

Amazon Key Management Service



Amazon Key Management Service: Developer Guide

Table of Contents

Amazon Key Management Service	1
Why use Amazon KMS?	1
Amazon KMS in Amazon Web Services Regions	2
Amazon KMS pricing	2
Amazon KMS service level agreement	2
Accessing Amazon Key Management Service	3
Amazon Web Services Management Console	3
Permissions required to use the Amazon KMS console	3
Amazon Command Line Interface	3
Amazon KMS REST API	4
Amazon SDKs	4
Working with Amazon SDKs	4
Amazon Encryption SDK	5
Amazon KMS eventual consistency	5
Hybrid post-quantum TLS	6
About post-quantum TLS	7
How to use it	8
Configure hybrid post-quantum TLS	9
Learn more	11
Connect to Amazon KMS through a VPC endpoint	11
Create a VPC endpoint for Amazon KMS	12
Connect to a VPC endpoint	13
Use VPC endpoints to control access to Amazon KMS resources	15
Logging Amazon KMS requests that use a VPC endpoint	18
Concepts	20
Introduction	20
Design goals	21
Amazon KMS keys	22
Customer managed keys	25
Amazon managed keys	26
Amazon owned keys	27
Amazon KMS key hierarchy	27
Key identifiers (KeyId)	29
Asymmetric keys	32

HMAC keys	34
Multi-Region keys	36
Imported key material	46
KMS keys in a CloudHSM key store	52
KMS keys in external key stores	54
Amazon KMS cryptography essentials	57
Entropy and random number generation	57
Symmetric key operations (encryption only)	57
Asymmetric key operations (encryption, digital signing and signature verification)	58
Key derivation functions	59
Amazon KMS internal use of digital signatures	59
Envelope encryption	59
Cryptographic operations	61
KMS key access and permissions	63
KMS key policies	63
KMS key grants	64
Key policies	65
Creating a key policy	65
Default key policy	72
View a key policies	87
Change a key policy	90
Permissions for Amazon services	93
IAM policies	93
Allowing multiple IAM principals to access a KMS key	95
Best practices for IAM policies	96
Specifying KMS keys in IAM policy statements	98
Examples	101
Resource control policies	107
Grants	109
Grant concepts	111
Best practices	115
Controlling access to grants	117
Creating grants	118
Viewing grants	126
Using a grant token	127
Retiring and revoking grants	128

Condition keys	129
Amazon global condition keys	130
Amazon KMS condition keys	132
Amazon KMS condition keys for Amazon Nitro Enclaves	199
Least-privilege permissions	203
Implementing least privileged permissions	204
Attribute-based access control (ABAC)	207
ABAC condition keys for Amazon KMS	208
Tags or aliases?	211
Troubleshooting ABAC for Amazon KMS	213
Role-based access control (RBAC)	217
Cross-account access	219
Step 1: Add a key policy statement in the local account	221
Step 2: Add IAM policies in the external account	225
Allowing use of external KMS keys with Amazon Web Services services	226
Using KMS keys in other accounts	226
Control access to multi-Region keys	227
Authorization basics for multi-Region keys	228
Authorizing multi-Region key administrators and users	230
Determining access	234
Examining the key policy	234
Examining IAM policies	237
Examining grants	239
Encryption context	241
Encryption context rules	242
Encryption context in policies	242
Encryption context in grants	243
Logging encryption context	244
Storing encryption context	244
Testing your permissions	244
What is DryRun?	245
Specifying DryRun with the API	246
Troubleshooting Amazon KMS permissions	246
Example 1: User is denied access to a KMS key in their Amazon Web Services account	248
Example 2: User assumes role with permission to use a KMS key in a different Amazon Web Services account	250

Glossary	253
Authentication	254
Authorization	254
Authenticating with identities	254
Managing access using policies	257
Amazon KMS resources	259
Create a KMS key	261
Permissions for creating KMS keys	263
Choosing what type of KMS key to create	264
Create a symmetric encryption KMS key	266
Create an asymmetric KMS key	271
Create an HMAC KMS key	277
Create multi-Region primary keys	282
Create multi-Region replica keys	287
Step 1: Choose replica Regions	288
Step 2: Create replica keys	288
Create a KMS key with imported key material	294
Permissions for importing key material	295
Requirements for imported key material	297
Step 1: Create an Amazon KMS key without key material	299
Step 2: Download the wrapping public key and import token	301
Step 3: Encrypt the key material	310
Step 4: Import the key material	319
Create a KMS key in an Amazon CloudHSM key store	323
Create a new KMS key in your CloudHSM key store	324
Create a KMS key in external key stores	330
Requirements for a KMS key in an external key store	332
Create a new KMS key in your external key store	333
Identify and view keys	341
Find the key ID and key ARN	341
Access and list KMS key details	343
Identify different key types	352
Identify asymmetric KMS keys	352
Identify HMAC KMS keys	353
Identify multi-Region KMS keys	354
Identify KMS keys with imported key material	355

Identify KMS keys in Amazon CloudHSM key stores	355
Identify KMS keys in external key stores	356
Customize your console view	357
Sort and filter your KMS keys	357
Customize your KMS key tables	360
Find KMS keys and key material in an Amazon CloudHSM key store	362
Find the KMS keys in an Amazon CloudHSM key store	362
Find all keys for an Amazon CloudHSM key store	364
Find the KMS key for an Amazon CloudHSM key	365
Find the Amazon CloudHSM key for a KMS key	370
Enable and disable keys	374
Rotate keys	377
Why rotate KMS keys?	379
How key rotation works	380
Enable automatic key rotation	384
Disable automatic key rotation	386
Perform on-demand key rotation	388
Initiating on-demand key rotation (console)	389
Initiating on-demand key rotation (Amazon KMS API)	390
Rotate keys manually	391
Change the primary key in a set of multi-Region keys	393
Update the primary Region	395
Delete keys	398
About the waiting period	399
Special considerations	399
Control access to key deletion	402
Allow key administrators to schedule and cancel key deletion	403
Schedule key deletion	405
.....	405
Cancel key deletion	407
Create an alarm	408
Determine past usage of a KMS key	410
Examine KMS key permissions to determine the scope of potential usage	410
Examine Amazon CloudTrail logs to determine actual usage	410
Delete imported key material	413
Generate data keys	416

Create a data key	416
How cryptographic operations with data keys work	417
Encrypt data with a data key	417
Decrypt data with a data key	418
How unusable KMS keys affect data keys	419
Generate data key pairs	421
Create a data key pair	421
How cryptographic operations with data key pairs work	422
Encrypt data with a data key pair	423
Decrypt data with a data key pair	423
Sign messages with a data key pair	424
Verify a signature with a data key pair	425
Derive a shared secret with data key pairs	426
Perform offline operations with public keys	427
Special considerations for downloading public keys	427
Download public key	429
Example offline operations	430
Deriving shared secrets offline	431
Offline verification with SM2 key pairs (China Regions only)	432
Monitor keys	438
Monitoring tools	439
Automated tools	439
Manual tools	439
Logging with Amazon CloudTrail	440
Finding Amazon KMS log entries in CloudTrail	441
Excluding Amazon KMS events from a trail	443
Examples of Amazon KMS log entries	444
Monitor keys with CloudWatch	524
Amazon KMS metrics and dimensions	525
Create a CloudWatch alarm for expiration of imported key material	533
Create CloudWatch alarms for external key stores	535
Monitor keys with Amazon EventBridge	539
KMS CMK Rotation	539
KMS Imported Key Material Expiration	540
KMS CMK Deletion	540
Aliases	542

How aliases work	542
Controlling access to aliases	546
kms:CreateAlias	546
kms:ListAliases	547
kms:UpdateAlias	548
kms>DeleteAlias	549
Limiting alias permissions	550
Create aliases	551
Find the alias name and alias ARN	554
Update aliases	559
Delete an alias	560
Use aliases to control access to KMS keys	561
kms:RequestAlias	563
kms:ResourceAliases	564
Learn how to use aliases in your applications	565
Find aliases in Amazon CloudTrail logs	567
Tags	569
Controlling access to tags	570
Tag permissions in policies	571
Limiting tag permissions	573
Add tags	574
Add tags while creating a KMS key	575
Add tags to existing KMS keys	576
Edit tags	577
Remove tags	579
View tags	580
Use tags to control access to KMS keys	581
Key stores	586
Amazon KMS standard key store	586
Amazon KMS standard key store with imported key material	586
Amazon KMS custom key stores	588
Amazon CloudHSM key store	588
External key store	589
Amazon CloudHSM key stores	589
Amazon CloudHSM key store concepts	592
Control access to your Amazon CloudHSM key store	595

Create an Amazon CloudHSM key store	597
View an Amazon CloudHSM key store	603
Edit Amazon CloudHSM key store settings	606
Connect an Amazon CloudHSM key store	610
Disconnect an Amazon CloudHSM key store	614
Delete an Amazon CloudHSM key store	617
Troubleshooting a custom key store	620
External key stores	635
External key store concepts	640
How external key stores work	648
Control access to your external key store	650
Choose a proxy connectivity option	655
Create an external key store	667
Edit external key store properties	679
View external key stores	686
Monitor external key stores	691
Connect and disconnect external key stores	704
Delete an external key store	714
Troubleshooting external key stores	716
Security	740
Data protection	740
Protecting key material	741
Data encryption	742
Internetwork privacy	744
Identity and access management	745
Amazon managed policies	745
Service-linked roles	749
Logging and monitoring	755
Compliance validation	756
Compliance and security documents	757
Learn more	757
Resilience	758
Regional isolation	758
Multi-tenant design	759
Resilience best practices in Amazon KMS	759
Infrastructure security	760

Isolation of Physical Hosts	761
Quotas	762
Resource quotas	762
Amazon KMS keys: 100,000	763
Aliases per KMS key: 50	763
Grants per KMS key: 50,000	764
Custom key stores resource quota: 10	764
On-demand rotation: 10	764
Request quotas	765
Request quotas for each Amazon KMS API operation	766
Applying request quotas	772
Shared quotas for cryptographic operations	773
API requests made on your behalf	774
Cross-account requests	775
Custom key store request quotas	775
Throttling requests	776
Code examples	779
Basics	783
Hello Amazon KMS	784
Learn the basics	787
Actions	860
Cryptographic attestation for Amazon Nitro Enclaves	1011
How to call Amazon KMS APIs for a Nitro enclave	1012
Monitoring requests for Nitro enclaves	1013
Decrypt (for an enclave)	1014
GenerateDataKey (for an enclave)	1015
GenerateDataKeyPair (for an enclave)	1016
GenerateRandom (for an enclave)	1017
Encrypting Amazon services	1019
Amazon Elastic Block Store (Amazon EBS)	1020
Amazon EBS encryption	1020
Using KMS keys and data keys	1021
Amazon EBS encryption context	1021
Detecting Amazon EBS failures	1022
Using Amazon CloudFormation to create encrypted Amazon EBS volumes	1023
Amazon EMR	1023

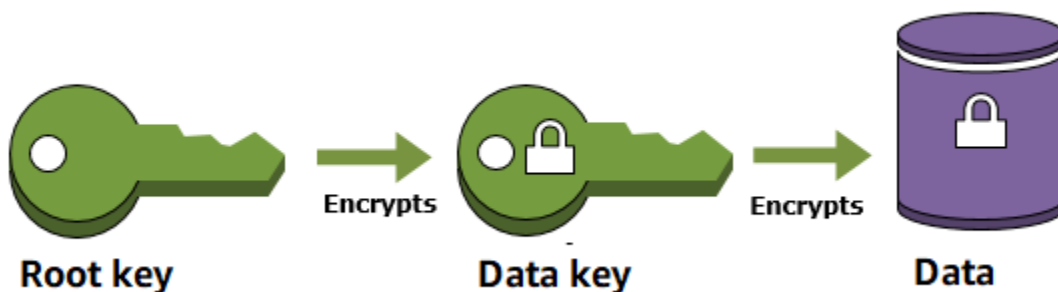
Encrypting data on the EMR file system (EMRFS)	1023
Encrypting data on the storage volumes of cluster nodes	1026
Encryption context	1027
Amazon Redshift	1028
Amazon Redshift encryption	1028
Encryption context	1029
Reference	1031
Key state reference	1032
Key states and KMS key types	1032
Key state table	1033
Key type reference	1040
Key type table	1040
Special features table	1047
Key spec reference	1055
SYMMETRIC_DEFAULT key spec	1057
RSA key specs	1058
Elliptic curve key specs	1061
SM2 key spec (China Regions only)	1063
Key specs for HMAC KMS keys	1064
Permissions reference	1065
Column descriptions	1112
Amazon KMS internal operations	1114
Domains and domain state	1115
Internal communication security	1118
Replication process for multi-Region keys	1122
Durability protection	1122
Document history	1124
Recent updates	1124
Earlier updates	1129

Amazon Key Management Service

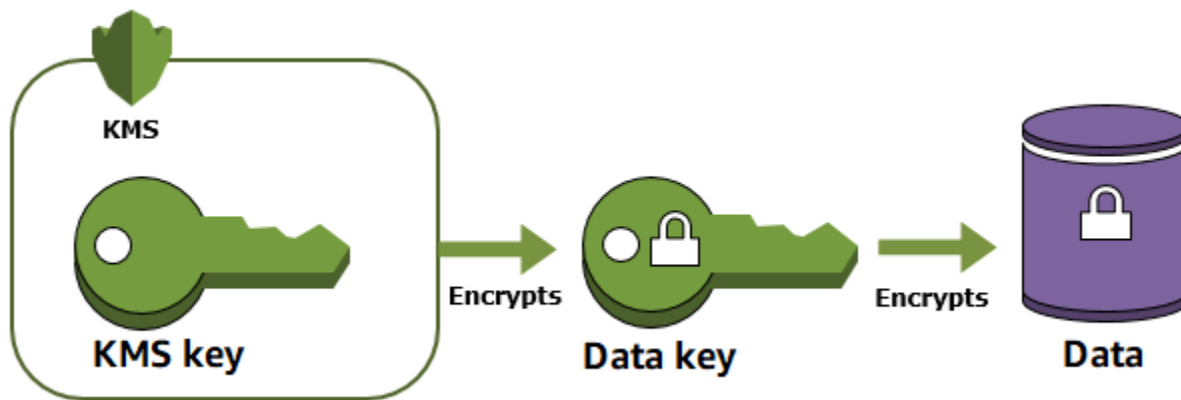
Amazon Key Management Service (Amazon KMS) is an Amazon managed service that makes it easy for you to create and control the encryption keys that are used to encrypt your data. The Amazon KMS keys that you create in Amazon KMS are protected by [FIPS 140-3 Security Level 3 validated hardware security modules \(HSM\)](#). They never leave Amazon KMS unencrypted. To use or manage your KMS keys, you interact with Amazon KMS.

Why use Amazon KMS?

When you encrypt data, you need to protect your encryption key. If you encrypt your key, you need to protect its encryption key. Eventually, you must protect the highest level encryption key (known as a *root key*) in the hierarchy that protects your data. That's where Amazon KMS comes in.



Amazon KMS protects your root keys. KMS keys are created, managed, used, and deleted entirely within Amazon KMS. They never leave the service unencrypted. To use or manage your KMS keys, you call Amazon KMS.



Additionally, you can create and manage [key policies](#) in Amazon KMS, ensuring that only trusted users have access to KMS keys.

Amazon KMS in Amazon Web Services Regions

The Amazon Web Services Regions in which Amazon KMS is supported are listed in [Amazon Key Management Service Endpoints and Quotas](#). If an Amazon KMS feature is not supported in an Amazon Web Services Region that Amazon KMS supports, the regional difference is described in the topic about the feature.

Amazon KMS pricing

As with other Amazon products, using Amazon KMS does not require contracts or minimum purchases. For more information about Amazon KMS pricing, see [Amazon Key Management Service Pricing](#).

Amazon KMS service level agreement

Amazon Key Management Service is backed by a [service level agreement](#) that defines our service availability policy.

Accessing Amazon Key Management Service

You can work with Amazon KMS in the following ways:

Amazon Web Services Management Console

The console is a web-based user interface for managing Amazon KMS and Amazon resources. If you've signed up for an Amazon Web Services account, you can access the Amazon KMS console by signing into the Amazon Web Services Management Console and choosing Amazon KMS from the Amazon Web Services Management Console home page.

Permissions required to use the Amazon KMS console

To work with the Amazon KMS console, users must have a minimum set of permissions that allow them to work with the Amazon KMS resources in their Amazon Web Services account. In addition to these Amazon KMS permissions, users must also have permissions to list IAM users and IAM roles. If you create an IAM policy that is more restrictive than the minimum required permissions, the Amazon KMS console won't function as intended for users with that IAM policy.

For the minimum permissions required to allow a user read-only access to the Amazon KMS console, see [Allow a user to view KMS keys in the Amazon KMS console](#).

To allow users to work with the Amazon KMS console to create and manage KMS keys, attach the **AWSKeyManagementServicePowerUser** managed policy to the user, as described in [Amazon managed policies for Amazon Key Management Service](#).

You don't need to allow minimum console permissions for users that are working with the Amazon KMS API through the [Amazon SDKs](#), [Amazon Command Line Interface](#), or [Amazon Tools for PowerShell](#). However, you do need to grant these users permission to use the API. For more information, see [Permissions reference](#).

Amazon Command Line Interface

You can use the Amazon CLI tools to issue commands or build scripts at your system's command line to perform Amazon (including Amazon KMS) tasks.

For more information about using Amazon KMS through the Amazon CLI, see the [Amazon CLI Command Reference](#)

Amazon KMS REST API

The architecture of Amazon KMS is designed to be programming language-neutral, using Amazon-supported interfaces to store and retrieve objects. You can access S3 and Amazon programmatically by using the Amazon KMS REST API. The REST API is an HTTP interface to Amazon KMS. With the REST API, you use standard HTTP requests to create, fetch, and delete buckets and objects.

For more information on using the Amazon KMS REST API, see the [Amazon Key Management Service API Reference](#)

Amazon SDKs

Amazon provides SDKs (software development kits) that consist of libraries and sample code for common programming languages and platforms (Java, JavaScript, C, Python, and so on). The Amazon SDKs provide a convenient way to create programmatic access to Amazon KMS and Amazon. Amazon KMS is a REST service. You can send requests to Amazon KMS using the Amazon SDK libraries, which wrap the underlying Amazon KMS REST API and simplify your programming tasks. For information about the Amazon SDKs, including how to download and install them, see [Tools to Build on Amazon](#).

The [Code examples for Amazon KMS using Amazon SDKs](#) provides a good starting point for using Amazon KMS through the Amazon SDKs.

Using this service with an Amazon SDK

Amazon software development kits (SDKs) are available for many popular programming languages. Each SDK provides an API, code examples, and documentation that make it easier for developers to build applications in their preferred language.

SDK documentation

[Amazon CLI](#)

[Amazon SDK for Java](#)

[Amazon SDK for JavaScript](#)

SDK documentation

[Amazon SDK for .NET](#)

[Amazon SDK for PHP](#)

[Amazon Tools for PowerShell](#)

[Amazon SDK for Python \(Boto3\)](#)

[Amazon SDK for Ruby](#)

[Amazon SDK for SAP ABAP](#)

Amazon Encryption SDK

The Amazon Encryption SDK is a tool for implementing client-side encryption in your application. It does not provide full access to KMS, but instead it integrates with Amazon KMS, or can be used as a stand-alone SDK without referencing KMS keys. Libraries are available for Java, JavaScript, C, Python, and other programming languages.

For more information, see the [Amazon Encryption SDK Developer Guide](#).

Amazon KMS key policies and IAM policies

Amazon KMS eventual consistency

The Amazon KMS API follows an [eventual consistency](#) model due to the distributed nature of the system. As a result, changes to Amazon KMS resources might not be immediately visible to the subsequent commands you run.

When you perform Amazon KMS API calls, there might be a brief delay before the change is available throughout Amazon KMS. It typically takes less than a few seconds for the change to propagate throughout the system, but in some cases it can take several minutes. You might get unexpected errors, such as a `NotFoundException` or an `InvalidStateException`, during this time. For example, Amazon KMS might return a `NotFoundException` if you call `GetParametersForImport` immediately after calling `CreateKey`.

We recommend that you configure a retry strategy on your Amazon KMS clients to automatically retry operations after a brief waiting period. For more information, see [Retry behavior](#) in the Amazon SDKs and Tools Reference Guide.

For grant related API calls, you can [use a grant token](#) to avoid any potential delay and use the permissions in a grant immediately. For more information, see [Eventual consistency \(for grants\)](#).

Using hybrid post-quantum TLS with Amazon KMS

Amazon Key Management Service (Amazon KMS) supports a hybrid post-quantum key exchange option for the Transport Layer Security (TLS) network encryption protocol. You can use this TLS option when you connect to Amazon KMS API endpoints. These optional hybrid post-quantum key exchange features are at least as secure as the TLS encryption we use today and are likely to provide additional long-term security benefits. However, they affect latency and throughput compared to the classic key exchange protocols in use today.

The data that you send to Amazon Key Management Service (Amazon KMS) is protected in transit by the encryption provided by a Transport Layer Security (TLS) connection. The classic cipher suites that Amazon KMS supports for TLS sessions make brute force attacks on the key exchange mechanisms infeasible with current technology. However, if large-scale quantum computing becomes practical in the future, the classic cipher suites used in TLS key exchange mechanisms will be susceptible to these attacks. If you're developing applications that rely on the long-term confidentiality of data passed over a TLS connection, you should consider a plan to migrate to post-quantum cryptography before large-scale quantum computers become available for use. Amazon is working to prepare for this future, and we want you to be well-prepared, too.

To protect data encrypted today against potential future attacks, Amazon is participating with the cryptographic community in the development of quantum-resistant or *post-quantum* algorithms. We've implemented *hybrid* post-quantum key exchange cipher suites in Amazon KMS that combine classic and post-quantum elements to ensure that your TLS connection is at least as strong as it would be with classic cipher suites.

These hybrid cipher suites are available for use on your production workloads in [most Amazon Web Services Regions](#). However, because the performance characteristics and bandwidth requirements of hybrid cipher suites are different from those of classic key exchange mechanisms, we recommend that you [test them on your Amazon KMS API calls](#) under different conditions.

Feedback

As always, we welcome your feedback and participation in our open-source repositories. We'd especially like to hear how your infrastructure interacts with this new variant of TLS traffic.

- To provide feedback on this topic, use the **Feedback** link in the upper right corner of this page.
- We're developing these hybrid cipher suites in open source in the [s2n-tls](#) repository on GitHub. To provide feedback on the usability of the cipher suites, or share novel test conditions or results, [create an issue](#) in the s2n-tls repository.
- We're writing code samples for using hybrid post-quantum TLS with Amazon KMS in the [aws-kms-pq-tls-example](#) GitHub repository. To ask questions or share ideas about configuring your HTTP client or Amazon KMS client to use the hybrid cipher suites, [create an issue](#) in the aws-kms-pq-tls-example repository.

Supported Amazon Web Services Regions

Post-quantum TLS for Amazon KMS is available in all Amazon Web Services Regions that Amazon KMS supports except for China (Beijing) and China (Ningxia).

Note

Amazon KMS does not support hybrid post-quantum TLS for FIPS endpoints in Amazon GovCloud (US).

For a list of Amazon KMS endpoints for each Amazon Web Services Region, see [Amazon Key Management Service endpoints and quotas](#) in the *Amazon Web Services General Reference*.

For information about FIPS endpoints, see [FIPS endpoints](#) in the *Amazon Web Services General Reference*.

About hybrid post-quantum key exchange in TLS

Amazon KMS supports hybrid post-quantum key exchange cipher suites. You can use the Amazon SDK for Java 2.x and Amazon Common Runtime on Linux systems to configure an HTTP client that uses these cipher suites. Then, whenever you connect to an Amazon KMS endpoint with your HTTP client, the hybrid cipher suites are used.

This HTTP client uses [s2n-tls](#), which is an open source implementation of the TLS protocol. The hybrid cipher suites that s2n-tls uses are implemented only for key exchange, not for direct data

encryption. During *key exchange*, the client and server calculate the key they will use to encrypt and decrypt the data on the wire.

The algorithms that s2n-tls uses are a *hybrid* that combines [Elliptic Curve Diffie-Hellman \(ECDH\)](#), a classic key exchange algorithm used today in TLS, with [Module-Lattice-Based Key-Encapsulation Mechanism \(ML-KEM\)](#), a public-key encryption and key-establishment algorithm that the National Institute for Standards and Technology (NIST) [has designated as its first standard](#) post-quantum key-agreement algorithm. This hybrid uses each of the algorithms independently to generate a key. Then it combines the two keys cryptographically. With s2n-tls, you can [configure an HTTP client](#) to prefer post-quantum TLS, which places ECDH with ML-KEM first in the preference list. Classic key exchange algorithms are included in the preference list to ensure compatibility, but they are lower in the preference order.

Using hybrid post-quantum TLS with Amazon KMS

You can use hybrid post-quantum TLS for your calls to Amazon KMS. When setting up your HTTP client test environment, be aware of the following information:

Encryption in Transit

The hybrid cipher suites in s2n-tls are used only for encryption in transit. They protect your data while it is traveling from your client to the Amazon KMS endpoint. Amazon KMS does not use these cipher suites to encrypt data under Amazon KMS keys.

Instead, when Amazon KMS encrypts your data under KMS keys, it uses symmetric cryptography with 256-bit keys and the Advanced Encryption Standard in Galois Counter Mode (AES-GCM) algorithm, which is already quantum resistant. Theoretical future, large-scale quantum computing attacks on ciphertexts created under 256-bit AES-GCM keys [reduce the effective security of the key to 128 bits](#). This security level is sufficient to make brute force attacks on Amazon KMS ciphertexts infeasible.

Supported Systems

Use of the hybrid cipher suites in s2n-tls is currently supported only on Linux systems. In addition, these cipher suites are supported only in SDKs that support the Amazon Common Runtime, such as the Amazon SDK for Java 2.x. For an example, see [Configure hybrid post-quantum TLS](#).

Amazon KMS Endpoints

When using the hybrid cipher suites, use the standard Amazon KMS endpoint. Amazon KMS does not support hybrid post-quantum TLS for [FIPS 140-3 validated endpoints](#).

When you configure a HTTP client to prefer post-quantum TLS connections with `s2n-tls`, the post-quantum ciphers are first in the cipher preference list. However, the preference list includes the classic, non-hybrid ciphers lower in the preference order for compatibility. When you configure an HTTP client to prefer post-quantum TLS with an Amazon KMS FIPS 140-3 validated endpoint, `s2n-tls` negotiates a classic, non-hybrid key exchange cipher.

For a list of Amazon KMS endpoints for each Amazon Web Services Region, see [Amazon Key Management Service endpoints and quotas](#) in the *Amazon Web Services General Reference*.

For information about FIPS endpoints, see [FIPS endpoints](#) in the *Amazon Web Services General Reference*.

Expected Performance

Our early benchmark testing shows that the hybrid cipher suites in `s2n-tls` are slower than classic TLS cipher suites. The effect varies based on the network profile, CPU speed, the number of cores, and your call rate. For more information, see [Amazon post-quantum cryptography migration plan](#).

Configure hybrid post-quantum TLS

In this procedure, add a Maven dependency for the Amazon Common Runtime HTTP Client. Next, configure an HTTP client that prefers post-quantum TLS. Then, create an Amazon KMS client that uses the HTTP client.

To see a complete working examples of configuring and using hybrid post-quantum TLS with Amazon KMS, see the [aws-kms-pq-tls-example](#) repository.

Note

The Amazon Common Runtime HTTP Client, which has been available as a preview, became generally available in February 2023. In that release, the `TlsCipherPreference` class and the `TlsCipherPreference()` method parameter are replaced by the `postQuantumTlsEnabled()` method parameter. If you were using this example during the preview, you need to update your code.

1. Add the Amazon Common Runtime client to your Maven dependencies. We recommend using the latest available version.

For example, this statement adds version `2.30.22` of the Amazon Common Runtime client to your Maven dependencies.

```
<dependency>
  <groupId>software.amazon.awssdk</groupId>
  <artifactId>aws-crt-client</artifactId>
  <version>2.30.22</version>
</dependency>
```

2. To enable the hybrid post-quantum cipher suites, add the Amazon SDK for Java 2.x to your project and initialize it. Then enable the hybrid post-quantum cipher suites on your HTTP client as shown in the following example.

This code uses the `postQuantumTlsEnabled()` method parameter to configure an [Amazon common runtime HTTP client](#) that prefers the recommended hybrid post-quantum cipher suite, ECDH with ML-KEM. Then it uses the configured HTTP client to build an instance of the Amazon KMS asynchronous client, [KmsAsyncClient](#). After this code completes, all [Amazon KMS API](#) requests on the `KmsAsyncClient` instance use hybrid post-quantum TLS.

```
// Configure HTTP client
SdkAsyncHttpClient awsCrtHttpClient = AwsCrtAsyncHttpClient.builder()
    .postQuantumTlsEnabled(true)
    .build();

// Create the Amazon KMS async client
KmsAsyncClient kmsAsync = KmsAsyncClient.builder()
    .httpClient(awsCrtHttpClient)
    .build();
```

3. Test your Amazon KMS calls with hybrid post-quantum TLS.

When you call Amazon KMS API operations on the configured Amazon KMS client, your calls are transmitted to the Amazon KMS endpoint using hybrid post-quantum TLS. To test your configuration, call an Amazon KMS API, such as [ListKeys](#).

```
ListKeysResponse keys = kmsAsync.listKeys().get();
```

Test your hybrid post-quantum TLS configuration

Consider running the following tests with hybrid cipher suites on your applications that call Amazon KMS.

- Run load tests and benchmarks. The hybrid cipher suites perform differently than traditional key exchange algorithms. You might need to adjust your connection timeouts to allow for the longer handshake times. If you're running inside an Amazon Lambda function, extend the execution timeout setting.
- Try connecting from different locations. Depending on the network path your request takes, you might discover that intermediate hosts, proxies, or firewalls with deep packet inspection (DPI) block the request. This might result from using the new cipher suites in the [ClientHello](#) part of the TLS handshake, or from the larger key exchange messages. If you have trouble resolving these issues, work with your security team or IT administrators to update the relevant configuration and unblock the new TLS cipher suites.

Learn more about post-quantum TLS in Amazon KMS

For more information about using hybrid post-quantum TLS in Amazon KMS, see the following resources.

- To learn about post-quantum cryptography at Amazon, including links to blog posts and research papers, see [Post-Quantum Cryptography](#).
- For information about s2n-tls, see [Introducing s2n-tls, a New Open Source TLS Implementation](#) and [Using s2n-tls](#).
- For information about the Amazon Common Runtime HTTP Client, see [Configuring the Amazon CRT-based HTTP client](#) in the *Amazon SDK for Java 2.x Developer Guide*.
- For information about the post-quantum cryptography project at the National Institute for Standards and Technology (NIST), see [Post-Quantum Cryptography](#).
- For information about NIST post-quantum cryptography standardization, see [Post-Quantum Cryptography Standardization](#).

Connect to Amazon KMS through a VPC endpoint

You can connect directly to Amazon KMS through a private interface endpoint in your virtual private cloud (VPC). When you use an interface VPC endpoint, communication between your VPC and Amazon KMS is conducted entirely within the Amazon network.

Amazon KMS supports Amazon Virtual Private Cloud (Amazon VPC) endpoints powered by [Amazon PrivateLink](#). Each VPC endpoint is represented by one or more [Elastic Network Interfaces](#) (ENIs) with private IP addresses in your VPC subnets.

The interface VPC endpoint connects your VPC directly to Amazon KMS without an internet gateway, NAT device, VPN connection, or Amazon Direct Connect connection. The instances in your VPC do not need public IP addresses to communicate with Amazon KMS.

Regions

Amazon KMS supports VPC endpoints and VPC endpoint policies in all Amazon Web Services Regions in which [Amazon KMS](#) is supported.

Considerations for Amazon KMS VPC endpoints

Before you set up an interface VPC endpoint for Amazon KMS, review the [Interface endpoint properties and limitations](#) topic in the *Amazon PrivateLink Guide*.

Amazon KMS support for a VPC endpoint includes the following.

- You can use your VPC endpoint to call all [Amazon KMS API operations](#) from your VPC.
- You can create an interface VPC endpoint that connects to an Amazon KMS region endpoint or an [Amazon KMS FIPS endpoint](#).
- You can use Amazon CloudTrail logs to audit your use of KMS keys through the VPC endpoint. For details, see [Logging Amazon KMS requests that use a VPC endpoint](#).

Topics

- [Create a VPC endpoint for Amazon KMS](#)
- [Connect to an Amazon KMS VPC endpoint](#)
- [Use VPC endpoints to control access to Amazon KMS resources](#)
- [Logging Amazon KMS requests that use a VPC endpoint](#)

Create a VPC endpoint for Amazon KMS

You can create a VPC endpoint for Amazon KMS by using the Amazon VPC console or the Amazon VPC API. Follow the procedures to [Create an interface endpoint](#) using one of the following values.

- To create a VPC endpoint for Amazon KMS, use the following service name:

```
com.amazonaws.region.kms
```

For example, in the US West (Oregon) Region (us-west-2), the service name would be:


```
com.amazonaws.us-west-2.kms
```

- To create a VPC endpoint that connects to an [Amazon KMS FIPS endpoint](#), use the following service name:

```
com.amazonaws.region.kms-fips
```

For example, in the US West (Oregon) Region (us-west-2), the service name would be:

```
com.amazonaws.us-west-2.kms-fips
```

To make it easier to use the VPC endpoint, you can enable a [private DNS name](#) for your VPC endpoint. If you select the **Enable DNS Name** option, the standard Amazon KMS DNS hostname resolves to your VPC endpoint. For example, `https://kms.us-west-2.amazonaws.com` would resolve to a VPC endpoint connected to service name `com.amazonaws.us-west-2.kms`.

This option makes it easier to use the VPC endpoint. The Amazon SDKs and Amazon CLI use the standard Amazon KMS DNS hostname by default, so you do not need to specify the VPC endpoint URL in applications and commands.

For more information, see [Accessing a service through an interface endpoint](#) in the *Amazon PrivateLink Guide*.

Connect to an Amazon KMS VPC endpoint

You can connect to Amazon KMS through the VPC endpoint by using an Amazon SDK, the Amazon CLI, or Amazon Tools for PowerShell. To specify the VPC endpoint, use its DNS name.

For example, this [list-keys](#) command uses the `endpoint-url` parameter to specify the VPC endpoint. To use a command like this, replace the example VPC endpoint ID with one in your account.

```
$ aws kms list-keys --endpoint-url https://vpce-1234abcd5678c90a-09p7654s-us-east-1a.ec2.us-east-1.vpce.amazonaws.com
```

Required permissions

For an Amazon KMS request that uses a VPC endpoint to be successful, the principal requires permissions from two sources:

- A [key policy](#), [IAM policy](#), or [grant](#) must give principal permission to call the operation on the resource (KMS key or alias).
- A VPC endpoint policy must give the principal permission to use the endpoint to make the request.

For example, a key policy might give a principal permission to call [Decrypt](#) on a particular KMS key. However, the VPC endpoint policy might not allow that principal to call `Decrypt` on that KMS key by using the endpoint.

Or a VPC endpoint policy might allow a principal to use the endpoint to call [DisableKey](#) on certain KMS keys. But if the principal doesn't have those permissions from a key policy, IAM policy, or grant, the request fails.

You can create a VPC endpoint policy when you create your endpoint, and you can change the VPC endpoint policy at any time. Use the VPC management console, or the [CreateVpcEndpoint](#) or [ModifyVpcEndpoint](#) operations. You can also create and change a VPC endpoint policy by [using an Amazon CloudFormation template](#). For help using the VPC management console, see [Create an interface endpoint](#) and [Modifying an interface endpoint](#) in the *Amazon PrivateLink Guide*.

Private hostnames

If you enabled private hostnames when you created your VPC endpoint, you do not need to specify the VPC endpoint URL in your CLI commands or application configuration. The standard Amazon KMS DNS hostname resolves to your VPC endpoint. The Amazon CLI and SDKs use this hostname by default, so you can begin using the VPC endpoint to connect to an Amazon KMS regional endpoint without changing anything in your scripts and applications.

To use private hostnames, the `enableDnsHostnames` and `enableDnsSupport` attributes of your VPC must be set to `true`. To set these attributes, use the [ModifyVpcAttribute](#) operation. For details, see [View and update DNS attributes for your VPC](#) in the *Amazon VPC User Guide*.

Use VPC endpoints to control access to Amazon KMS resources

You can control access to Amazon KMS resources and operations when the request comes from VPC or uses a VPC endpoint. To do so, use one of the following [global condition keys](#) in a [key policy](#) or [IAM policy](#).

- Use the `aws:sourceVpce` condition key to grant or restrict access based on the VPC endpoint.
- Use the `aws:sourceVpc` condition key to grant or restrict access based on the VPC that hosts the private endpoint.

Note

Use caution when creating key policies and IAM policies based on your VPC endpoint. If a policy statement requires that requests come from a particular VPC or VPC endpoint, requests from integrated Amazon services that use an Amazon KMS resource on your behalf might fail. For help, see [Using VPC endpoint conditions in policies with Amazon KMS permissions](#).

Also, the `aws:sourceIP` condition key is not effective when the request comes from an [Amazon VPC endpoint](#). To restrict requests to a VPC endpoint, use the `aws:sourceVpce` or `aws:sourceVpc` condition keys. For more information, see [Identity and access management for VPC endpoints and VPC endpoint services](#) in the *Amazon PrivateLink Guide*.

You can use these global condition keys to control access to Amazon KMS keys (KMS keys), aliases, and to operations like [CreateKey](#) that don't depend on any particular resource.

For example, the following sample key policy allows a user to perform some cryptographic operations with a KMS key only when the request uses the specified VPC endpoint. When a user makes a request to Amazon KMS, the VPC endpoint ID in the request is compared to the `aws:sourceVpce` condition key value in the policy. If they do not match, the request is denied.

To use a policy like this one, replace the placeholder Amazon Web Services account ID and VPC endpoint IDs with valid values for your account.

```
{
  "Id": "example-key-1",
  "Version": "2012-10-17",
```

```

"Statement": [
  {
    "Sid": "Enable IAM policies",
    "Effect": "Allow",
    "Principal": {"AWS":["111122223333"]},
    "Action": ["kms:*"],
    "Resource": "*"
  },
  {
    "Sid": "Restrict usage to my VPC endpoint",
    "Effect": "Deny",
    "Principal": "*",
    "Action": [
      "kms:Encrypt",
      "kms:Decrypt",
      "kms:ReEncrypt*",
      "kms:GenerateDataKey*"
    ],
    "Resource": "*",
    "Condition": {
      "StringNotEquals": {
        "aws:sourceVpce": "vpce-1234abcd5678c90a"
      }
    }
  }
]
}

```

You can also use the `aws:sourceVpce` condition key to restrict access to your KMS keys based on the VPC in which VPC endpoint resides.

The following sample key policy allows commands that manage the KMS key only when they come from `vpc-12345678`. In addition, it allows commands that use the KMS key for cryptographic operations only when they come from `vpc-2b2b2b2b`. You might use a policy like this one if an application is running in one VPC, but you use a second, isolated VPC for management functions.

To use a policy like this one, replace the placeholder Amazon Web Services account ID and VPC endpoint IDs with valid values for your account.

```

{
  "Id": "example-key-2",
  "Version": "2012-10-17",

```

```
"Statement": [
  {
    "Sid": "Allow administrative actions from vpc-12345678",
    "Effect": "Allow",
    "Principal": {"AWS": "111122223333"},
    "Action": [
      "kms:Create*", "kms:Enable*", "kms:Put*", "kms:Update*",
      "kms:Revoke*", "kms:Disable*", "kms>Delete*",
      "kms:TagResource", "kms:UntagResource"
    ],
    "Resource": "*",
    "Condition": {
      "StringEquals": {
        "aws:sourceVpc": "vpc-12345678"
      }
    }
  },
  {
    "Sid": "Allow key usage from vpc-2b2b2b2b",
    "Effect": "Allow",
    "Principal": {"AWS": "111122223333"},
    "Action": [
      "kms:Encrypt", "kms:Decrypt", "kms:GenerateDataKey*"
    ],
    "Resource": "*",
    "Condition": {
      "StringEquals": {
        "aws:sourceVpc": "vpc-2b2b2b2b"
      }
    }
  },
  {
    "Sid": "Allow read actions from everywhere",
    "Effect": "Allow",
    "Principal": {"AWS": "111122223333"},
    "Action": [
      "kms:Describe*", "kms:List*", "kms:Get*"
    ],
    "Resource": "*"
  }
]
```

Logging Amazon KMS requests that use a VPC endpoint

Amazon CloudTrail logs all operations that use the VPC endpoint. When a request to Amazon KMS uses a VPC endpoint, the VPC endpoint ID appears in the [Amazon CloudTrail log](#) entry that records the request. You can use the endpoint ID to audit the use of your Amazon KMS VPC endpoint.

However, your CloudTrail logs don't include operations requested by principals in other accounts or requests for Amazon KMS operations on KMS keys and aliases in other accounts. Also, to protect your VPC, requests that are denied by a VPC endpoint policy, but otherwise would have been allowed, are not recorded in [Amazon CloudTrail](#).

For example, this sample log entry records a [GenerateDataKey](#) request that used the VPC endpoint. The `vpcEndpointId` field appears at the end of the log entry.

```
{
  "eventVersion": "1.05",
  "userIdentity": {
    "type": "IAMUser",
    "principalId": "EX_PRINCIPAL_ID",
    "arn": "arn:aws:iam::111122223333:user/Alice",
    "accessKeyId": "EXAMPLE_KEY_ID",
    "accountId": "111122223333",
    "userName": "Alice"
  },
  "eventTime": "2018-01-16T05:46:57Z",
  "eventSource": "kms.amazonaws.com",
  "eventName": "GenerateDataKey",
  "awsRegion": "eu-west-1",
  "sourceIPAddress": "172.01.01.001",
  "userAgent": "aws-cli/1.14.23 Python/2.7.12 Linux/4.9.75-25.55.amzn1.x86_64
botocore/1.8.27",
  "requestParameters": {
    "keyId": "1234abcd-12ab-34cd-56ef-1234567890ab",
    "numberOfBytes": 128
  },
  "responseElements": null,
  "requestID": "a9fff0bf-fa80-11e7-a13c-afcabbff2f04c",
  "eventID": "77274901-88bc-4e3f-9bb6-acf1c16f6a7c",
  "readOnly": true,
  "resources": [
    {
      "ARN": "arn:aws:kms:eu-
west-1:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab",
```

```
    "accountId": "111122223333",
    "type": "AWS::KMS::Key"
  }],
  "eventType": "AwsApiCall",
  "recipientAccountId": "111122223333",
  "vpcEndpointId": "vpce-1234abcdef5678c90a"
}
```

Amazon KMS concepts

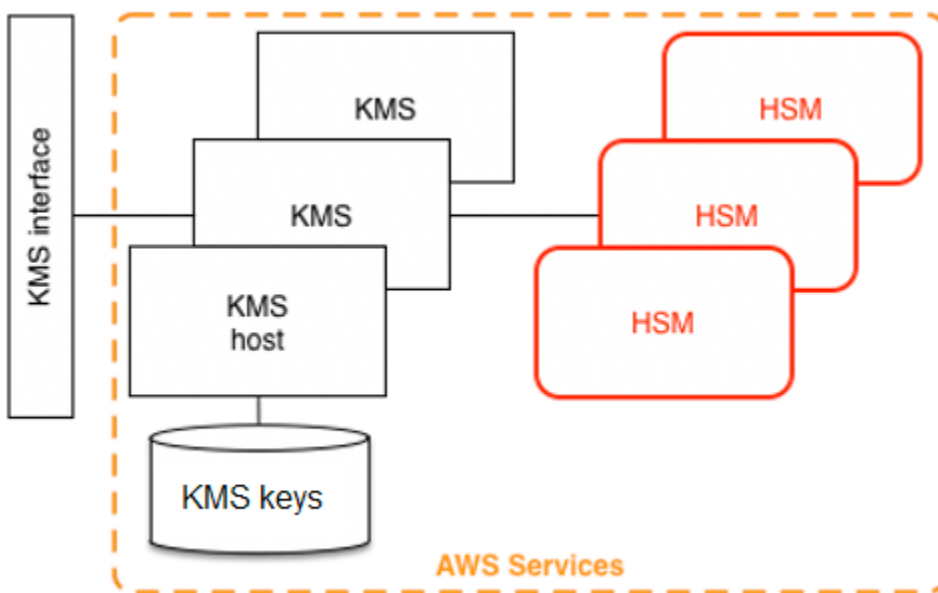
Learn the basic terms and concepts used in Amazon Key Management Service (Amazon KMS) and how they work together to help protect your data.

Introduction to Amazon KMS

Amazon Key Management Service (Amazon KMS) provides a web interface to generate and manage cryptographic keys and operates as a cryptographic service provider for protecting data. Amazon KMS offers traditional key management services integrated with Amazon services to provide a consistent view of customers' keys across Amazon, with centralized management and auditing.

Amazon KMS includes a web interface through the Amazon Web Services Management Console, command line interface, and RESTful API operations to request cryptographic operations of a distributed fleet of FIPS 140-3 validated hardware security modules (HSMs). The Amazon KMS HSM is a multichip standalone hardware cryptographic appliance designed to provide dedicated cryptographic functions to meet the security and scalability requirements of Amazon KMS. You can establish your own HSM-based cryptographic hierarchy under keys that you manage as Amazon KMS keys. These keys are made available only on the HSMs and only in memory for the necessary time needed to process your cryptographic request. You can create multiple KMS keys, each represented by its key ID. Only under Amazon IAM roles and accounts administered by each customer can customer managed KMS keys be created, deleted, or used to encrypt, decrypt, sign, or verify data. You can define access controls on who can manage and/or use KMS keys by creating a policy that is attached to the key. Such policies allow you to define application-specific uses for your keys for each API operation.

In addition, most Amazon services support encryption of data at rest using KMS keys. This capability allows customers to control how and when Amazon services can access encrypted data by controlling how and when KMS keys can be accessed.



Amazon KMS is a tiered service consisting of web-facing Amazon KMS hosts and a tier of HSMs. The grouping of these tiered hosts forms the Amazon KMS stack. All requests to Amazon KMS must be made over the Transport Layer Security protocol (TLS) and terminate on an Amazon KMS host. Amazon KMS hosts only allow TLS with a ciphersuite that provides perfect [forward secrecy](#). Amazon KMS authenticates and authorizes your requests using the same credential and policy mechanisms of Amazon Identity and Access Management (IAM) that are available for all other Amazon API operations.

Amazon KMS design goals

Amazon KMS is designed to meet the following requirements.

Durability

The durability of cryptographic keys is designed to equal that of the highest durability services in Amazon. A single cryptographic key can encrypt large volumes of your data that has accumulated over a long time.

Trustworthy

Use of keys is protected by access control policies that you define and manage. There is no mechanism to export plaintext KMS keys. The confidentiality of your cryptographic keys is crucial. Multiple Amazon employees with role-specific access to quorum-based access controls are required to perform administrative actions on the HSMs.

Low-latency and high throughput

Amazon KMS provides cryptographic operations at latency and throughput levels suitable for use by other services in Amazon.

Independent Regions

Amazon provides independent Regions for customers who need to restrict data access in different Regions. Key usage can be isolated within an Amazon Web Services Region.

Secure source of random numbers

Because strong cryptography depends on truly unpredictable random number generation, Amazon KMS provides a high-quality and validated source of random numbers.

Audit

Amazon KMS records the use and management of cryptographic keys in Amazon CloudTrail logs. You can use Amazon CloudTrail logs to inspect use of your cryptographic keys, including the use of keys by Amazon services on your behalf.

To achieve these goals, the Amazon KMS system includes a set of Amazon KMS operators and service host operators (collectively, “operators”) that administer “domains.” A domain is a Regionally defined set of Amazon KMS servers, HSMs, and operators. Each Amazon KMS operator has a hardware token that contains a private and public key pair that is used to authenticate its actions. The HSMs have an additional private and public key pair to establish encryption keys that protect HSM state synchronization.

Amazon KMS keys

The KMS keys that you create and manage for use in your own cryptographic applications are of a type known as *customer managed keys*. Customer managed keys can also be used in conjunction with Amazon services that use KMS keys to encrypt the data the service stores on your behalf. Customer managed keys are recommended for customers who want full control over the lifecycle and usage of their keys. There is a monthly cost to have a customer managed key in your account. In addition, requests use and/or manage the key incur a usage cost. See [Amazon Key Management Service Pricing](#) for more details.

There are cases where a customer might want an Amazon service to encrypt their data, but they don't want the overhead of managing keys and don't want to pay for a key. An *Amazon managed*

key is a KMS key that exists in your account, but can only be used under certain circumstances. Specifically, it can only be used in the context of the Amazon service you're operating in and it can only be used by principals within the account that the key exists. You cannot manage anything about the lifecycle or permissions of these keys. As you use encryption features in Amazon services, you may see Amazon managed keys; they use an alias of the form "aws<service code>". For example, an aws/ebs key can only be used to encrypt EBS volumes and only for volumes used by IAM principals in the same account as the key. Think of an Amazon managed key that is scoped down for use only by users in your account for resources in your account. You cannot share resources encrypted under an Amazon managed key with other accounts. While an Amazon managed key is free to exist in your account, you are charged for any use of this key type by the Amazon service that is assigned to the key.

Amazon managed keys are a legacy key type that is no longer being created for new Amazon services as of 2021. Instead, new (and legacy) Amazon services are using what's known as an *Amazon owned key* to encrypt customer data by default. An Amazon owned key is a KMS key that is in an account managed by the Amazon service, so the service operators have the ability to manage its lifecycle and usage permissions. By using Amazon owned keys, Amazon services can transparently encrypt your data and allow for easy cross-account or cross-region sharing of data without you needing to worry about key permissions. Use Amazon owned keys for encryption-by-default workloads that provide easier, more automated data protection. Because these keys are owned and managed by Amazon, you are not charged for their existence or their usage, you cannot change their policies, you cannot audit activities on these keys, and you cannot delete them. Use customer managed keys when control is important, but use Amazon owned keys when convenience is most important.

	Customer managed keys	Amazon managed keys	Amazon owned keys
Key policy	Exclusively controlled by the customer	Controlled by service; viewable by customer	Exclusively controlled and only viewable by the Amazon service that encrypts your data
Logging	CloudTrail customer trail or event data store	CloudTrail customer trail or event data store	Not viewable by the customer

Lifecycle management	Customer manages rotation, deletion and Regional location	Amazon KMS manages rotation (annual), deletion, and Regional location	Amazon Web Services service manages rotation, deletion, and Regional location
Pricing	Monthly fee for existence of keys (pro-rated hourly). Also charged for key usage	No monthly fee; but the caller is charged for API usage on these keys	No charges to customer

The KMS keys that you create are [customer managed keys](#). Amazon Web Services services that use KMS keys to encrypt your service resources often create keys for you. KMS keys that Amazon Web Services services create in your Amazon account are [Amazon managed keys](#). KMS keys that Amazon Web Services services create in a service account are [Amazon owned keys](#).

Type of KMS key	Can view KMS key metadata	Can manage KMS key	Used only for my Amazon Web Services account	Automatic rotation	Pricing
Customer managed key	Yes	Yes	Yes	Optional.	Monthly fee (pro-rated hourly) Per-use fee
Amazon managed key	Yes	No	Yes	Required. Every year (approximately 365 days).	No monthly fee Per-use fee (some Amazon Web Services services pay

Type of KMS key	Can view KMS key metadata	Can manage KMS key	Used only for my Amazon Web Services account	Automatic rotation	Pricing
Amazon owned key	No	No	No	The Amazon Web Services service manages the rotation strategy.	this fee for you) No fees

[Amazon services that integrate with Amazon KMS](#) differ in their support for KMS keys. Some Amazon services encrypt your data by default with an Amazon owned key or an Amazon managed key. Some Amazon services support customer managed keys. Other Amazon services support all types of KMS keys to allow you the ease of an Amazon owned key, the visibility of an Amazon managed key, or the control of a customer managed key. For detailed information about the encryption options that an Amazon service offers, see the *Encryption at Rest* topic in the user guide or the developer guide for the service.

Customer managed keys

The KMS keys that you create are *customer managed keys*. Customer managed keys are KMS keys in your Amazon Web Services account that you create, own, and manage. You have full control over these KMS keys, including establishing and maintaining their [key policies, IAM policies, and grants](#), [enabling and disabling](#) them, [rotating their cryptographic material](#), [adding tags](#), [creating aliases](#) that refer to the KMS keys, and [scheduling the KMS keys for deletion](#).

Customer managed keys appear on the **Customer managed keys** page of the Amazon Web Services Management Console for Amazon KMS. To definitively identify a customer managed key, use the [DescribeKey](#) operation. For customer managed keys, the value of the `KeyManager` field of the `DescribeKey` response is `CUSTOMER`.

You can use your customer managed key in cryptographic operations and audit usage in Amazon CloudTrail logs. In addition, many [Amazon services that integrate with Amazon KMS](#) let you specify a customer managed key to protect the data stored and managed for you.

Customer managed keys incur a monthly fee and a fee for use in excess of the free tier. They are counted against the Amazon KMS [quotas](#) for your account. For details, see [Amazon Key Management Service Pricing](#) and [Quotas](#).

Amazon managed keys

Amazon managed keys are KMS keys in your account that are created, managed, and used on your behalf by an [Amazon service integrated with Amazon KMS](#).

Some Amazon services let you choose an Amazon managed key or a customer managed key to protect your resources in that service. In general, unless you are required to control the encryption key that protects your resources, an Amazon managed key is a good choice. You don't have to create or maintain the key or its key policy, and there's never a monthly fee for an Amazon managed key.

You have permission to [view the Amazon managed keys](#) in your account, [view their key policies](#), and [audit their use](#) in Amazon CloudTrail logs. However, you cannot change any properties of Amazon managed keys, rotate them, change their key policies, or schedule them for deletion. And, you cannot use Amazon managed keys in cryptographic operations directly; the service that creates them uses them on your behalf.

[Resource control policies](#) in your organization do not apply to Amazon managed keys.

Amazon managed keys appear on the **Amazon managed keys** page of the Amazon Web Services Management Console for Amazon KMS. You can also identify Amazon managed keys by their aliases, which have the format `aws/service-name`, such as `aws/redshift`. To definitively identify an Amazon managed keys, use the [DescribeKey](#) operation. For Amazon managed keys, the value of the `KeyManager` field of the `DescribeKey` response is `Amazon`.

All Amazon managed keys are automatically rotated every year. You cannot change this rotation schedule.

Note

In May 2022, Amazon KMS changed the rotation schedule for Amazon managed keys from every three years (approximately 1,095 days) to every year (approximately 365 days).

New Amazon managed keys are automatically rotated one year after they are created, and approximately every year thereafter.

Existing Amazon managed keys are automatically rotated one year after their most recent rotation, and every year thereafter.

There is no monthly fee for Amazon managed keys. They can be subject to fees for use in excess of the free tier, but some Amazon services cover these costs for you. For details, see the *Encryption at Rest* topic in the user guide or developer guide for the service. For details, see [Amazon Key Management Service Pricing](#).

Amazon managed keys do not count against resource quotas on the number of KMS keys in each Region of your account. But when used on behalf of a principal in your account, the KMS keys count against request quotas. For details, see [Quotas](#).

Amazon owned keys

Amazon owned keys are a collection of KMS keys that an Amazon service owns and manages for use in multiple Amazon Web Services accounts. Although Amazon owned keys are not in your Amazon Web Services account, an Amazon service can use an Amazon owned key to protect the resources in your account.

Some Amazon services let you choose an Amazon owned key or a customer managed key. In general, unless you are required to audit or control the encryption key that protects your resources, an Amazon owned key is a good choice. Amazon owned keys are completely free of charge (no monthly fees or usage fees), they do not count against the [Amazon KMS quotas](#) for your account, and they're easy to use. You don't need to create or maintain the key or its key policy.

The rotation of Amazon owned keys varies across services. For information about the rotation of a particular Amazon owned key, see the *Encryption at Rest* topic in the user guide or developer guide for the service.

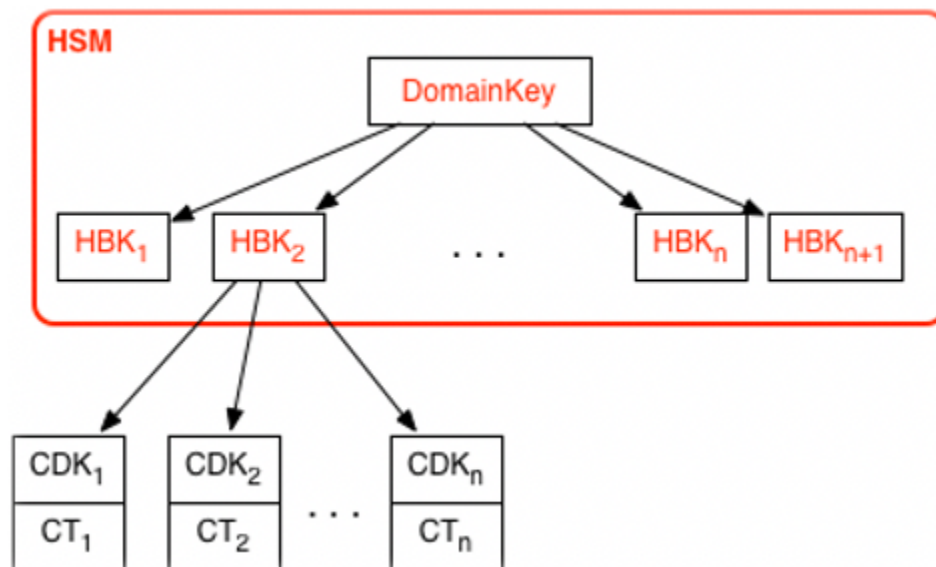
Amazon KMS key hierarchy

Your key hierarchy starts with a top-level logical key, an Amazon KMS key. A KMS key represents a container for top-level key material and is uniquely defined within the Amazon service namespace with an Amazon Resource Name (ARN). The ARN includes a uniquely generated key identifier, a *key ID*. A KMS key is created based on a user-initiated request through Amazon KMS. Upon reception, Amazon KMS requests the creation of an initial HSM backing key (HBK) to be placed into the

KMS key container. The HBK is generated on an HSM in the domain and is designed never to be exported from the HSM in plaintext. Instead, the HBK is exported encrypted under HSM-managed domain keys. These exported HBKs are referred to as exported key tokens (EKTs).

The EKT is exported to a highly durable, low-latency storage. For example, suppose you receive an ARN to the logical KMS key. This represents the top of a key hierarchy, or cryptographic context, for you. You can create multiple KMS keys within your account and set policies on your KMS keys like any other Amazon named resource.

Within the hierarchy of a specific KMS key, the HBK can be thought of as a version of the KMS key. When you want to rotate the KMS key through Amazon KMS, a new HBK is created and associated with the KMS key as the active HBK for the KMS key. The older HBKs are preserved and can be used to decrypt and verify previously protected data. But only the active cryptographic key can be used to protect new information.



You can make requests through Amazon KMS to use your KMS keys to directly protect information or request additional HSM-generated keys that are protected under your KMS key. These keys are called customer data keys, or CDKs. CDKs can be returned encrypted as ciphertext (CT), in plaintext, or both. All objects encrypted under a KMS key (either customer-supplied data or HSM-generated keys) can be decrypted only on an HSM via a call through Amazon KMS.

The returned ciphertext, or the decrypted payload, is never stored within Amazon KMS. The information is returned to you over your TLS connection to Amazon KMS. This also applies to calls made by Amazon services on your behalf.

The key hierarchy and the specific key properties appear in the following table.

Key	Description	Lifecycle
Domain key	A 256-bit AES-GCM key only in memory of an HSM used to wrap versions of the KMS keys, the HSM backing keys.	Rotated daily ¹
HSM backing key	A 256-bit symmetric key or RSA or elliptic curve private key, used to protect customer data and keys and stored encrypted under domain keys. One or more HSM backing keys comprise the KMS key, represented by the keyId.	Rotated yearly ² (optional config.)
Derived encryption key	A 256-bit AES-GCM key only in memory of an HSM used to encrypt customer data and keys. Derived from an HBK for each encryption.	Used once per encrypt and regenerated on decrypt
Customer data key	User-defined symmetric or asymmetric key exported from HSM in plaintext and ciphertext. Encrypted under an HSM backing key and returned to authorized users over TLS channel.	Rotation and use controlled by application

¹ Amazon KMS might from time to time relax domain key rotation to at most weekly to account for domain administration and configuration tasks.

² Default Amazon managed keys created and managed by Amazon KMS on your behalf are automatically rotated annually.

Key identifiers (KeyId)

Key identifiers act like names for your KMS keys. They help you to recognize your KMS keys in the console. You use them to indicate which KMS keys you want to use in Amazon KMS API operations,

key policies, IAM policies, and grants. The key identifier values are completely unrelated to the key material associated with the KMS key.

Amazon KMS defines several key identifiers. When you create a KMS key, Amazon KMS generates a key ARN and key ID, which are properties of the KMS key. When you create an [alias](#), Amazon KMS generates an alias ARN based on the alias name that you define. You can view the key and alias identifiers in the Amazon Web Services Management Console and in the Amazon KMS API.

In the Amazon KMS console, you can view and filter KMS keys by their key ARN, key ID, or alias name, and sort by key ID and alias name. For help finding the key identifiers in the console, see [the section called “Find the key ID and key ARN”](#).

In the Amazon KMS API, the parameters you use to identify a KMS key are named `KeyId` or a variation, such as `TargetKeyId` or `DestinationKeyId`. However, the values of those parameters are not limited to key IDs. Some can take any valid key identifier. For information about the values for each parameter, see the parameter description in the Amazon Key Management Service API Reference.

Note

When using the Amazon KMS API, be careful about the key identifier that you use. Different APIs require different key identifiers. In general, use the most complete and practical key identifier for your task.

Amazon KMS supports the following key identifiers.

Key ARN

The key ARN is the Amazon Resource Name (ARN) of a KMS key. It is a unique, fully qualified identifier for the KMS key. A key ARN includes the Amazon Web Services account, Region, and the key ID. For help finding the key ARN of a KMS key, see [the section called “Find the key ID and key ARN”](#).

The format of a key ARN is as follows:

```
arn:<partition>:kms:<region>:<account-id>:key/<key-id>
```

The following is an example key ARN for a single-Region KMS key.

```
arn:aws:kms:us-west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab
```

The *key-id* element of the key ARNs of [multi-Region keys](#) begin with the `mrk-` prefix. The following is an example key ARN for a multi-Region key.

```
arn:aws:kms:us-west-2:111122223333:key/mrk-1234abcd12ab34cd56ef1234567890ab
```

Key ID

The key ID uniquely identifies a KMS key within an account and Region. For help finding the key ID of a KMS key, see [the section called “Find the key ID and key ARN”](#).

The following is an example key ID for a single-Region KMS key.

```
1234abcd-12ab-34cd-56ef-1234567890ab
```

The key IDs of [multi-Region keys](#) begin with the `mrk-` prefix. The following is an example key ID for a multi-Region key.

```
mrk-1234abcd12ab34cd56ef1234567890ab
```

Alias ARN

The alias ARN is the Amazon Resource Name (ARN) of an Amazon KMS alias. It is a unique, fully qualified identifier for the alias, and for the KMS key it represents. An alias ARN includes the Amazon Web Services account, Region, and the alias name.

At any given time, an alias ARN identifies one particular KMS key. However, because you can change the KMS key associated with the alias, the alias ARN can identify different KMS keys at different times. For help finding the alias ARN of a KMS key, see [Find the alias name and alias ARN for a KMS key](#).

The format of an alias ARN is as follows:

```
arn:<partition>:kms:<region>:<account-id>:alias/<alias-name>
```

The following is the alias ARN for a fictitious `ExampleAlias`.

```
arn:aws:kms:us-west-2:111122223333:alias/ExampleAlias
```

Alias name

The alias name is a string of up to 256 characters. It uniquely identifies an associated KMS key within an account and Region. In the Amazon KMS API, alias names always begin with `alias/`. For help finding the alias name of a KMS key, see [Find the alias name and alias ARN for a KMS key](#).

The format of an alias name is as follows:

```
alias/<alias-name>
```

For example:

```
alias/ExampleAlias
```

The `aws/` prefix for an alias name is reserved for [Amazon managed keys](#). You cannot create an alias with this prefix. For example, the alias name of the Amazon managed key for Amazon Simple Storage Service (Amazon S3) is the following.

```
alias/aws/s3
```

Asymmetric keys in Amazon KMS

An *asymmetric KMS key* represents a mathematically related public key and private key pair. You can give the public key to anyone, even if they're not trusted, but the private key must be kept secret.

In an asymmetric KMS key, the private key is created in Amazon KMS and never leaves Amazon KMS unencrypted. To use the private key, you must call Amazon KMS. You can use the public key within Amazon KMS by calling the Amazon KMS API operations. Or, you can [download the public key](#) and use it outside of Amazon KMS.

If your use case requires encryption outside of Amazon by users who cannot call Amazon KMS, asymmetric KMS keys are a good choice. However, if you are creating a KMS key to encrypt the data that you store or manage in an Amazon service, use a symmetric encryption KMS key. [Amazon services that are integrated with Amazon KMS](#) use only symmetric encryption KMS keys to encrypt your data. These services do not support encryption with asymmetric KMS keys.

Amazon KMS supports three types of asymmetric KMS keys.

RSA KMS keys

A KMS key with an RSA key pair for encryption and decryption or signing and verification (but not both). Amazon KMS supports several key lengths for different security requirements.

For technical details about the encryption and signing algorithms that Amazon KMS supports for RSA KMS keys, see [RSA key specs](#).

Elliptic Curve (ECC) KMS keys

A KMS key with an elliptic curve key pair for signing and verification or deriving shared secrets (but not both). Amazon KMS supports several commonly-used curves.

For technical details about the signing algorithms that Amazon KMS supports for ECC KMS keys, see [Elliptic curve key specs](#).

SM2 KMS keys (China Regions only)

A KMS key with an SM2 key pair for encryption and decryption, signing and verification, or deriving shared secrets (you must choose one key usage type).

For technical details about the encryption and signing algorithms that Amazon KMS supports for SM2 KMS keys (China Regions only), see [SM2 key spec](#).

For help choosing your asymmetric key configuration, see [Choosing what type of KMS key to create](#).

Regions

Asymmetric KMS keys and asymmetric data key pairs are supported in all Amazon Web Services Regions that Amazon KMS supports.

Learn more

- To create asymmetric KMS keys, see [Create an asymmetric KMS key](#).
- To create multi-Region asymmetric KMS keys, see [Create multi-Region primary keys](#).
- To learn how to sign messages and verify signatures with asymmetric KMS keys, see [Digital signing with the new asymmetric keys feature of Amazon KMS](#) in the *Amazon Security Blog*.
- To learn about special considerations for deleting asymmetric KMS keys, see [Deleting asymmetric KMS keys](#).

- To identify and view asymmetric KMS keys, see [Identify asymmetric KMS keys](#).

HMAC keys in Amazon KMS

Hash-Based Message Authentication Code (HMAC) KMS keys are symmetric keys that you use to generate and verify HMACs within Amazon KMS. The unique key material associated with each HMAC KMS key provides the secret key that HMAC algorithms require. You can use an HMAC KMS key with the [GenerateMac](#) and [VerifyMac](#) operations to verify the integrity and authenticity of data within Amazon KMS.

HMAC algorithms combine a cryptographic hash function and a shared secret key. They take a message and a secret key, such as the key material in an HMAC KMS key, and return a unique, fixed-size code or *tag*. If even one character of the message changes, or if the secret key is not identical, the resulting tag is entirely different. By requiring a secret key, HMAC also provides authenticity; it is impossible to generate an identical HMAC tag without the secret key. HMACs are sometimes called *symmetric signatures*, because they work like digital signatures, but use a single key for both signing and verification.

HMAC KMS keys and the HMAC algorithms that Amazon KMS uses conform to industry standards defined in [RFC 2104](#). The Amazon KMS [GenerateMac](#) operation generates standard HMAC tags. HMAC KMS keys are generated in Amazon KMS hardware security modules that are certified under the [FIPS 140-3 Cryptographic Module Validation Program](#) (except in China (Beijing) and China (Ningxia) Regions) and never leave Amazon KMS unencrypted. To use an HMAC KMS key, you must call Amazon KMS.

You can use HMAC KMS keys to determine the authenticity of a message, such as a JSON Web Token (JWT), tokenized credit card information, or a submitted password. They can also be used as secure Key Derivation Functions (KDFs), especially in applications that require deterministic keys.

HMAC KMS keys provide an advantage over HMACs from application software because the key material is generated and used entirely within Amazon KMS, subject to the access controls that you set on the key.

Tip

Best practices recommend that you limit the time during which any signing mechanism, including an HMAC, is effective. This deters an attack where the actor uses a signed message to establish validity repeatedly or long after the message is superseded. HMAC

tags do not include a timestamp, but you can include a timestamp in the token or message to help you detect when its time to refresh the HMAC.

Supported cryptographic operations

HMAC KMS keys support only the [GenerateMac](#) and [VerifyMac](#) cryptographic operations. You cannot use HMAC KMS keys to encrypt data or sign messages, or use any other type of KMS key in HMAC operations. When you use the `GenerateMac` operation, you supply a message of up to 4,096 bytes, an HMAC KMS key, and the MAC algorithm that is compatible with the HMAC key spec, and `GenerateMac` computes the HMAC tag. To verify an HMAC tag, you must supply the HMAC tag, and the same message, HMAC KMS key, and MAC algorithm that `GenerateMac` used to compute the original HMAC tag. The `VerifyMac` operation computes the HMAC tag and verifies that it is identical to the supplied HMAC tag. If the input and computed HMAC tags are not identical, verification fails.

HMAC KMS keys *do not* support [automatic key rotation](#) and you cannot create an HMAC KMS key in a [custom key store](#).

If you are creating a KMS key to encrypt data in an Amazon service, use a symmetric encryption key. You cannot use an HMAC KMS key.

Regions

HMAC KMS keys are supported in all Amazon Web Services Regions that Amazon KMS supports.

Learn more

- To create HMAC KMS keys, see [Create an HMAC KMS key](#).
- To create multi-Region HMAC KMS keys, see [Multi-Region keys in Amazon KMS](#).
- To examine the difference in the default key policy that the Amazon KMS console sets for HMAC KMS keys, see [the section called “Allows key users to use a KMS key for cryptographic operations”](#).
- To identify and view HMAC KMS keys, see [Identify HMAC KMS keys](#).
- To learn about using HMACs to create JSON web tokens, see [How to protect HMACs inside Amazon KMS](#) in the *Amazon Security Blog*.
- Listen to a podcast: [Introducing HMACs for Amazon Key Management Service](#) on *The Official Amazon Podcast*.

Multi-Region keys in Amazon KMS

Amazon KMS supports *multi-Region keys*, which are Amazon KMS keys in different Amazon Web Services Regions that can be used interchangeably – as though you had the same key in multiple Regions. Each set of *related* multi-Region keys has the same key material and [key ID](#), so you can encrypt data in one Amazon Web Services Region and decrypt it in a different Amazon Web Services Region without re-encrypting or making a cross-Region call to Amazon KMS.

Like all KMS keys, multi-Region keys never leave Amazon KMS unencrypted. You can create symmetric or asymmetric multi-Region keys for encryption or signing, create HMAC multi-Region keys for generating and verifying HMAC tags, and create multi-Region keys with [imported key material](#) or key material that Amazon KMS generates. You must manage each multi-Region key independently, including creating aliases and tags, setting their key policies and grants, and enabling and disabling them selectively. You can use multi-Region keys in all cryptographic operations that you can do with single-Region keys.

Multi-Region keys are a flexible and powerful solution for many common data security scenarios.

Disaster recovery

In a backup and recovery architecture, multi-Region keys let you process encrypted data without interruption even in the event of an Amazon Web Services Region outage. Data maintained in backup Regions can be decrypted in the backup Region, and data newly encrypted in the backup Region can be decrypted in the primary Region when that Region is restored.

Global data management

Businesses that operate globally need globally distributed data that is available consistently across Amazon Web Services Regions. You can create multi-Region keys in all Regions where your data resides, then use the keys as though they were a single-Region key without the latency of a cross-Region call or the cost of re-encrypting data under a different key in each Region.

Distributed signing applications

Applications that require cross-Region signature capabilities can use multi-Region asymmetric signing keys to generate identical digital signatures consistently and repeatedly in different Amazon Web Services Regions.

If you use certificate chaining with a single global trust store (for a single root certificate authority (CA), and Regional intermediate CAs signed by the root CA, you don't need multi-Region keys. However, if your system doesn't support intermediate CAs, such as application signing, you can use multi-Region keys to bring consistency to Regional certifications.

Active-active applications that span multiple Regions

Some workloads and applications can span multiple Regions in active-active architectures. For these applications, multi-Region keys can reduce complexity by providing the same key material for concurrent encrypt and decrypt operations on data that might be moving across Region boundaries.

You can use multi-Region keys with client-side encryption libraries, such as the [Amazon Encryption SDK](#), the [Amazon Database Encryption SDK](#), and [Amazon S3 client-side encryption](#).

[Amazon services that integrate with Amazon KMS](#) for encryption at rest or digital signatures currently treat multi-Region keys as though they were single-Region keys. They might re-wrap or re-encrypt data moved between Regions. For example, Amazon S3 cross-region replication decrypts and re-encrypts data under a KMS key in the destination Region, even when replicating objects protected by a multi-Region key.

Multi-Region keys are not global. You create a multi-Region primary key and then replicate it into Regions that you select within an [Amazon partition](#). Then you manage the multi-Region key in each Region independently. Neither Amazon nor Amazon KMS ever automatically creates or replicates multi-Region keys into any Region on your behalf. [Amazon managed keys](#), the KMS keys that Amazon services create in your account for you, are always single-Region keys.

In China Regions, you can use the multi-Region key feature to replicate KMS keys within the China Regions partition (aws-cn). For example, you can replicate a key from the China (Beijing) Region to the China (Ningxia) Region, or the reverse. By replicating a key from one China region to another, you agree to use the Amazon Key Management Service of the destination region and comply with all applicable terms of agreement for the destination region. You cannot replicate a key from the Beijing and Ningxia Regions into an Amazon Region outside of the China Regions partition. Similarly, you cannot replicate a key from a region outside of the China Regions partition into the Beijing and Ningxia Regions.

You cannot convert an existing single-Region key to a multi-Region key. This design ensures that all data protected with existing single-Region keys maintain the same data residency and data sovereignty properties.

For most data security needs, the Regional isolation and fault tolerance of Regional resources make standard Amazon KMS single-Region keys a best-fit solution. However, when you need to encrypt or sign data in client-side applications across multiple Regions, multi-Region keys might be the solution.

Regions

Multi-Region keys are supported in all Amazon Web Services Regions that Amazon KMS supports.

Pricing and quotas

Every key in a set of related multi-Region keys counts as one KMS key for pricing and quotas. [Amazon KMS quotas](#) are calculated separately for each Region of an account. Use and management of the multi-Region keys in each Region count toward the quotas for that Region.

Supported KMS key types

You can create the following types of multi-Region KMS keys:

- Symmetric encryption KMS keys
- Asymmetric KMS keys
- HMAC KMS keys
- KMS keys with imported key material

You cannot create multi-Region keys in a custom key store.

Learn more

- To learn how to control access to multi-Region KMS keys, see [Control access to multi-Region keys](#).
- To create multi-Region primary KMS keys of any type, see [Create multi-Region primary keys](#).
- To create multi-Region replica KMS keys, see [Create multi-Region replica keys](#).
- To update the primary Region, see [Change the primary key in a set of multi-Region keys](#).
- To identify and view multi-Region KMS keys, see [Identify HMAC KMS keys](#).
- To learn about special considerations for deleting multi-Region KMS keys, see [Deleting multi-Region keys](#).

Terminology and concepts

The following terms and concepts are used with multi-Region keys.

Multi-Region key

A *multi-Region key* is one of a set of KMS keys with the same key ID and key material (and other [shared properties](#)) in different Amazon Web Services Regions. Each multi-Region key is a fully functioning KMS key that can be used entirely independently of its related multi-Region keys. Because all *related* multi-Region keys have the same key ID and key material, they are *interoperable*, that is, any related multi-Region key in any Amazon Web Services Region can decrypt ciphertext encrypted by any other related multi-Region key.

You set the multi-Region property of a KMS key when you create it. You cannot change the multi-Region property on an existing key. You cannot convert a single-Region key to multi-Region key or a convert a multi-Region key to a single-Region key. To move existing workloads into multi-Region scenarios, you must re-encrypt your data or create new signatures with new multi-Region keys.

A multi-Region key can be [symmetric or asymmetric](#) and it can use Amazon KMS key material or [imported key material](#). You cannot create multi-Region keys in a [custom key store](#).

In a set of related multi-Region keys, there is exactly one [primary key](#) at any time. You can create [replica keys](#) of that primary key in other Amazon Web Services Regions. You can also [update the primary region](#), which changes the primary key to a replica key and changes a specified replica key to the primary key. However, you can maintain only one primary key or replica key in each Amazon Web Services Region. All of the Regions must be in the same [Amazon partition](#).

You can have multiple sets of related multi-Region keys in the same or different Amazon Web Services Regions. Although related multi-Region keys are interoperable, unrelated multi-Region keys are not interoperable.

Primary key

A multi-Region *primary key* is a KMS key that can be replicated into other Amazon Web Services Regions in the same partition. Each set of multi-Region keys has just one primary key.

A primary key differs from a replica key in the following ways:

- Only a primary key can be [replicated](#).
- The primary key is the source for [shared properties](#) of its [replica keys](#), including the key material and key ID.

- You can enable and disable [automatic key rotation](#) only on a primary key.
- You can [schedule the deletion of a primary key](#) at any time. But Amazon KMS will not delete a primary key until all of its replica keys are deleted.

However, primary and replica keys don't differ in any cryptographic properties. You can use a primary key and its replica keys interchangeably.

You are not required to replicate a primary key. You can use it just as you would any KMS key and replicate it if and when it is useful. However, because multi-Region keys have different security properties than single-Region keys, we recommend that you create a multi-Region key only when you plan to replicate it.

Replica key

A multi-Region *replica key* is a KMS key that has the same [key ID](#) and key material as its [primary key](#) and related replica keys, but exists in a different Amazon Web Services Region.

A replica key is a fully functional KMS key with its own key policy, grants, alias, tags, and other properties. It is not a copy of or pointer to the primary key or any other key. You can use a replica key even if its primary key and all related replica keys are disabled. You can also convert a replica key to a primary key and a primary key to a replica key. Once it is created, a replica key relies on its primary key only for [key rotation](#) and [updating the primary Region](#).

Primary and replica keys don't differ in any cryptographic properties. You can use a primary key and its replica keys interchangeably. Data encrypted by a primary or replica key can be decrypted by the same key, or by any related primary or replica key.

Replicate

You can *replicate* a multi-Region [primary key](#) into a different Amazon Web Services Region in the same partition. When you do, Amazon KMS creates a multi-Region [replica key](#) in the specified Region with the same [key ID](#) and other [shared properties](#) as its primary key. Then it securely transports the key material across the Region boundary and associates it with the new replica key, all within Amazon KMS.

Shared properties

Shared properties are properties of a multi-Region primary key that are shared with its replica keys. Amazon KMS creates the replica keys with the same shared property values as those of the primary

key. Then, it periodically synchronizes the shared property values of the primary key to its replica keys. You cannot set these properties on a replica key.

The following are the shared properties of multi-Region keys.

- [Key ID](#) — (The `Region` element of the [key ARN](#) differs.)
- [Key material](#)
- [Key material origin](#)
- [Key spec](#) and encryption algorithms
- [Key usage](#)
- [Automatic key rotation](#) — You can enable and disable automatic key rotation only on the primary key. New replica keys are created with all versions of the shared key material. For details, see [Rotating multi-Region keys](#).
- [On-demand rotation](#) — You can perform on-demand rotation only on the primary key. New replica keys are created with all versions of the shared key material. For details, see [Rotating multi-Region keys](#).

You can also think of the primary and replica designations of related multi-Region keys as shared properties. When you [create new replica keys](#) or [update the primary key](#), Amazon KMS synchronizes the change to all related multi-Region keys. When these changes are complete, all related multi-Region keys list their primary key and replica keys accurately.

All other properties of multi-Region keys are *independent properties*, including the description, [key policy](#), [grants](#), [enabled and disabled key states](#), [aliases](#), and [tags](#). You can set the same values for these properties on all related multi-Region keys, but if you change the value of an independent property, Amazon KMS does not synchronize it.

You can track the synchronization of the shared properties of your multi-Region keys. In your Amazon CloudTrail log, look for the [SynchronizeMultiRegionKey](#) event.

Security considerations for multi-Region keys

Use an Amazon KMS multi-Region key only when you need one. Multi-Region keys provide a flexible and scalable solution for workloads that move encrypted data between Amazon Web Services Regions or need cross-Region access. Consider a multi-Region key if you must share, move, or back up protected data across Regions or need to create identical digital signatures of applications operating in different Regions.

However, the process of creating a multi-Region key moves your key material across Amazon Web Services Region boundaries within Amazon KMS. The ciphertext generated by a multi-Region key can potentially be decrypted by multiple related keys in multiple geographic locations. There are also significant benefits to Regionally-isolated services and resources. Each Amazon Web Services Region is isolated and independent of the other Regions. Regions provide fault tolerance, stability, and resilience, and can also reduce latency. They enable you to create redundant resources that remain available and unaffected by an outage in another Region. In Amazon KMS, they also ensure that every ciphertext can be decrypted by only one key.

Multi-Region keys also raise new security considerations:

- Controlling access and enforcing data security policy is more complex with multi-Region keys. You need to ensure that policy is audited consistently on key across multiple, isolated regions. And you need to use policy to enforce boundaries, instead of relying on separate keys.

For example, you need to set policy conditions on data to prevent payroll teams in one Region from being able to read payroll data for a different Region. Also, you must use access control to prevent a scenario where a multi-Region key in one Region protects one tenant's data and a related multi-Region key in another Region protects a different tenant's data.

- Auditing keys across Regions is also more complex. With multi-Region keys, you need to examine and reconcile audit activities across multiple Regions to gain a complete understanding of key activities on protected data.
- Compliance with data residency mandates can be more complex. With isolated Regions, you can ensure data residency and data sovereignty compliance. KMS keys in a given Region can decrypt sensitive data only in that Region. Data encrypted in one Region can remain completely protected and inaccessible in any other Region.

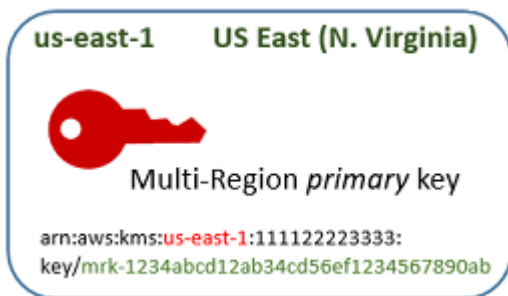
To verify data residency and data sovereignty with multi-Region keys, you need to implement access policies and compile Amazon CloudTrail events across multiple Regions.

To make it easier for you to manage access control on multi-Region keys, the permission to replicate a multi-Region key ([kms:ReplicateKey](#)) is separate from the standard permission to create keys ([kms:CreateKey](#)). Also, Amazon KMS supports several policy conditions for multi-Region keys, including `kms:MultiRegion`, which allows or denies permission to create, use, or manage multi-Region keys and `kms:ReplicaRegion`, which restricts the Regions into which a multi-Region key can be replicated. For details, see [Control access to multi-Region keys](#).

How multi-Region keys work

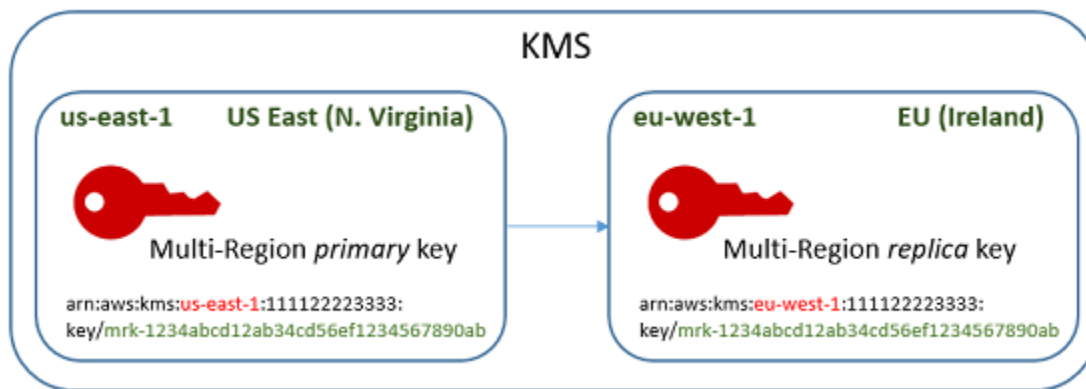
You begin by creating a symmetric or asymmetric [multi-Region primary key](#) in an Amazon Web Services Region that Amazon KMS supports, such as US East (N. Virginia). You decide whether a key is single-Region or multi-Region only when you create it; you can't change this property later. As with any KMS key, you set a key policy for the multi-Region key, and you can create grants, and add aliases and tags for categorization and authorization. (These are [independent properties](#) that aren't shared or synchronized with other keys.) You can use your multi-Region primary key in cryptographic operations for encryption or signing.

You can [create a multi-Region primary key](#) in the Amazon KMS console or by using the [CreateKey](#) API with the `MultiRegion` parameter set to `true`. Notice that multi-Region keys have a distinctive key ID that begins with `mrk-`. You can use the `mrk-` prefix to identify MRKs programmatically.



If you choose, you can [replicate](#) the multi-Region primary key into one or more different Amazon Web Services Regions in the same [Amazon partition](#), such as Europe (Ireland). When you do, Amazon KMS creates a [replica key](#) in the specified Region with the same key ID and other [shared properties](#) as the primary key. Then it securely transports the key material across the Region boundary and associates it with the new KMS key in the destination Region, all within Amazon KMS. The result is two *related* multi-Region keys — a primary key and a replica key — that can be used interchangeably.

You can [create a multi-Region replica key](#) in the Amazon KMS console or by using the [ReplicateKey](#) API.



The resulting [multi-Region replica key](#) is a fully-functional KMS key with the same [shared properties](#) as the primary key. In all other respects, it is an independent KMS key with its own description, key policy, grants, aliases, and tags. Enabling or disabling a multi-Region key has no effect on related multi-Region keys. You can use the primary and replica keys independently in cryptographic operations or coordinate their use. For example, you can encrypt data with the primary key in the US East (N. Virginia) Region, move the data to the Europe (Ireland) Region and use the replica key to decrypt the data.

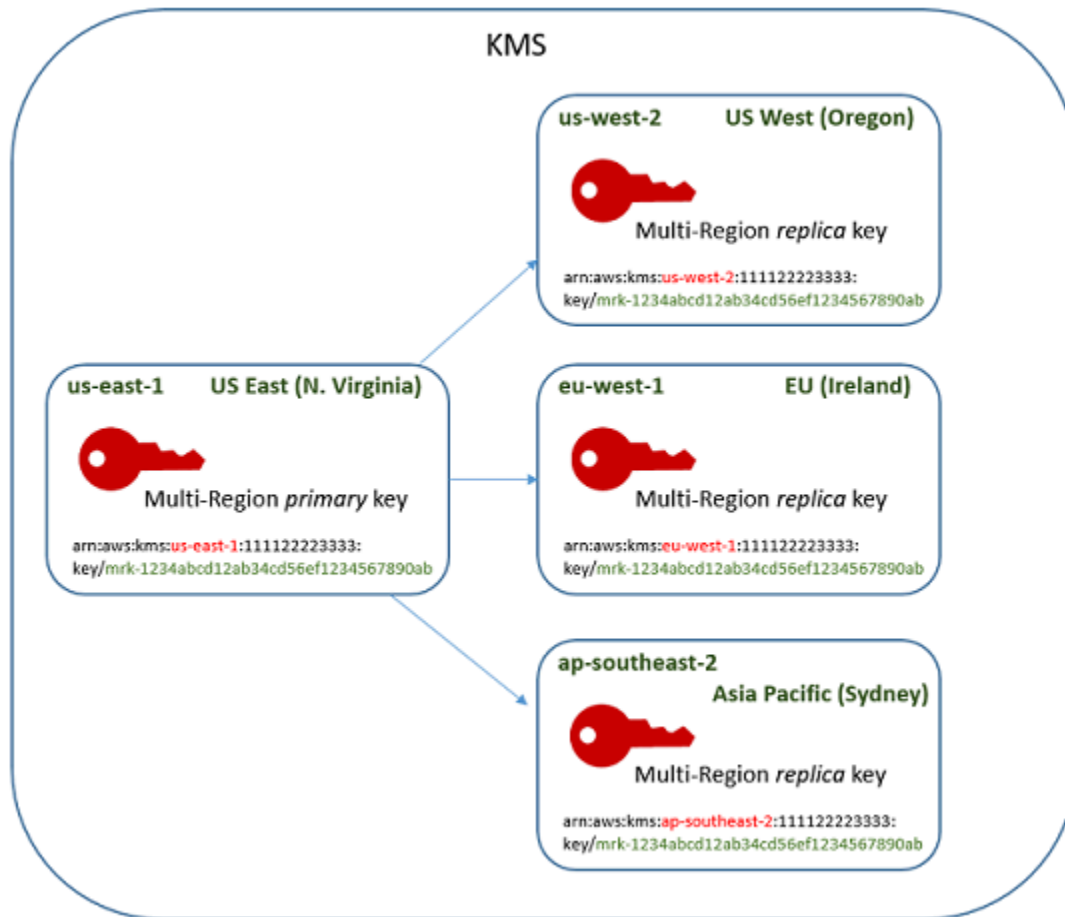
Related multi-Region keys have the same key ID. Their key ARNs (Amazon Resource Names) differ only in the Region field. For example, the multi-Region primary key and replica keys might have the following example key ARNs. The key ID – the last element in the key ARN – is identical. Both keys have the distinctive key ID of multi-Region keys, which begins with **mrk-**.

```
Primary key: arn:aws:kms:us-east-1:111122223333:key/mrk-1234abcd12ab34cd56ef12345678990ab
Replica key: arn:aws:kms:eu-west-1:111122223333:key/mrk-1234abcd12ab34cd56ef12345678990ab
```

Having the same key ID is required for interoperability. When encrypting, Amazon KMS binds the key ID of the KMS key to the ciphertext so the ciphertext can be decrypted only with that KMS key or a KMS key with the same key ID. This feature also makes related multi-Region keys easy to recognize, and it makes it easier to use them interchangeably. For example, when using them in an application, you can refer to related multi-Region keys by their shared key ID. Then, if necessary, specify the Region or ARN to distinguish them.

As your data needs change, you can replicate the primary key to other Amazon Web Services Regions in the same partition, such as US West (Oregon) and Asia Pacific (Sydney). The result is four *related* multi-Region keys with the same key material and key IDs, as shown in the following diagram. You manage the keys independently. You can use them independently or in a coordinated

fashion. For example, you can encrypt data with the replica key in Asia Pacific (Sydney), move the data to US West (Oregon), and decrypt it with the replica key in US West (Oregon).



Other considerations for multi-Region keys include the following.

Synchronizing shared properties — If a [shared property](#) of the multi-Region keys changes, Amazon KMS automatically synchronizes the change from the [primary key](#) to all of its [replica keys](#). You cannot request or force a synchronization of shared properties. Amazon KMS detects and synchronizes all changes for you. However, you can audit synchronization by using the [SynchronizeMultiRegionKey](#) event in CloudTrail logs.

For example, if you enable automatic key rotation on a symmetric multi-Region primary key, Amazon KMS copies that setting to all of its replica keys. When the key material is rotated, the rotation is synchronized among all of the related multi-Region keys, so they continue to have the same current key material, and access to all older versions of the key material. If you create a new replica key, it has the same current key material of all related multi-Region keys and access to all previous versions of the key material. For details, see [Rotating multi-Region keys](#).

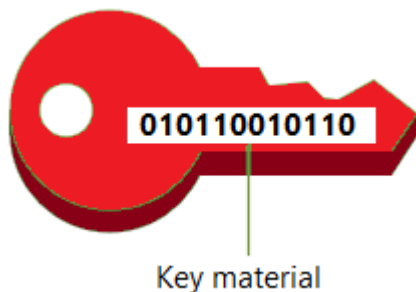
Changing the primary key — Every set of multi-Region keys must have exactly one primary key. The [primary key](#) is the only key that can be replicated. It's also the source of the shared properties of its replica keys. But you can change the primary key to a replica and promote one of the replica keys to primary. You might do this so you can delete a multi-Region primary key from a particular Region, or locate the primary key in a Region closer to project administrators. For details, see [Change the primary key in a set of multi-Region keys](#).

Deleting multi-Region keys — Like all KMS keys, you must schedule the deletion of multi-Region keys before Amazon KMS deletes them. While the key is pending deletion, you cannot use it in any cryptographic operations. However, Amazon KMS will not delete a multi-Region primary key until all of its replica keys are deleted. For details, see [Deleting multi-Region keys](#).

Importing key material for Amazon KMS keys

You can create an Amazon KMS keys (KMS key) with key material that you supply.

A KMS key is a logical representation of a data key. The metadata for a KMS key includes the ID of the key material used to perform cryptographic operations. When you [create a KMS key](#), by default, Amazon KMS generates the key material for that KMS key. But you can create a KMS key without key material and then import your own key material into that KMS key, a feature often known as "bring your own key" (BYOK).



Note

Amazon KMS does not support decrypting any Amazon KMS ciphertext encrypted by a symmetric encryption KMS key outside of Amazon KMS, even if the ciphertext was encrypted under a KMS key with imported key material. Amazon KMS does not publish the ciphertext format this task requires, and the format might change without notice.

When you use imported key material, you remain responsible for the key material while allowing Amazon KMS to use a copy of it. You might choose to do this for one or more of the following reasons:

- To prove the key material was generated using a source of entropy that meets your requirements.
- To use key material from your own infrastructure with Amazon services, and to use Amazon KMS to manage the lifecycle of that key material within Amazon.
- To use existing, well-established keys in Amazon KMS, such as keys for code signing, PKI certificate signing, and certificate pinned applications
- To set an expiration time for the key material in Amazon and to [manually delete it](#), but to also make it available again in the future. In contrast, [scheduling key deletion](#) requires a waiting period of 7 to 30 days, after which you cannot recover the deleted KMS key.
- To own the original copy of the key material, and to keep it outside of Amazon for additional durability and disaster recovery during the complete lifecycle of the key material.
- For asymmetric keys and HMAC keys, importing creates compatible and interoperable keys that operate within and outside of Amazon.

Supported KMS key types

Amazon KMS supports imported key material for the following types of KMS keys. You cannot import key material into KMS keys in [custom key stores](#).

- [Symmetric encryption KMS keys](#)
- [Asymmetric KMS keys](#)
- [HMAC KMS keys](#)
- [Multi-Region keys](#) of all supported types.

Regions

Imported key material is supported in all Amazon Web Services Regions that Amazon KMS supports.

In China Regions, the key material requirements for symmetric encryption KMS keys differ from other Regions. For details, see [Step 3: Encrypt the key material](#).

Learn more

- To create KMS keys with imported key material, see [Create a KMS key with imported key material](#).
- To create an alarm that notifies you when the imported key material in a KMS key is approaching its expiration time, see [Create a CloudWatch alarm for expiration of imported key material](#).
- To reimport key material into a KMS key, see [Reimport key material](#).
- To identify and view KMS keys with imported key material, see [Identify KMS keys with imported key material](#).
- To learn about special considerations for deleting KMS keys with imported key material, see [Deleting KMS keys with imported key material](#).

Special considerations for imported key material

Before you decide to import key material into Amazon KMS, you should understand the following characteristics of imported key material.

You generate the key material

You are responsible for generating the key material using a source of randomness that meets your security requirements.

You can delete the key material

You can [delete imported key material](#) from a KMS key, immediately rendering the KMS key unusable. Also, when you import key material into a KMS key, you can determine whether the key expires and [set its expiration time](#). When the expiration time arrives, Amazon KMS [deletes the key material](#). Without key material, the KMS key cannot be used in any cryptographic operation. To restore the key, you must reimport the same key material into the key.

You cannot change the key material

When you import key material into a KMS key, the KMS key is permanently associated with that key material. You can [reimport the same key material](#), but you cannot import different key material into that KMS key. Also, you cannot [enable automatic key rotation](#) for a KMS key with imported key material. However, you can [manually rotate a KMS key](#) with imported key material.

You cannot change the key material origin

KMS keys designed for imported key material have an [origin](#) value of EXTERNAL that cannot be changed. You cannot convert a KMS key for imported key material to use key material from

any other source, including Amazon KMS. Similarly, you cannot convert a KMS key with Amazon KMS key material into one designed for imported key material.

You cannot export key material

You cannot export any key material that you imported. Amazon KMS cannot return the imported key material to you in any form. You must maintain a copy of your imported key material outside of Amazon, preferably in a key manager, such as a hardware security module (HSM), so you can re-import the key material if you delete it or it expires.

You can create multi-Region keys with imported key material

Multi-Region with imported key material have the features of KMS keys with imported key material, and can interoperate between Amazon Web Services Regions. To create a multi-Region key with imported key material, you must import the same key material into the primary KMS key and into each replica key.

Asymmetric keys and HMAC keys are portable and interoperable

You can use your asymmetric key material and HMAC key material outside of Amazon to interoperate with Amazon KMS keys with the same imported key material.

Unlike the Amazon KMS symmetric ciphertext, which is inextricably bound to the KMS key used in the algorithm, Amazon KMS uses standard HMAC and asymmetric formats for encryption, signing, and MAC generation. As a result, the keys are portable and support traditional escrow key scenarios.

When your KMS key has imported key material, you can use the imported key material outside of Amazon to perform the following operations.

- **HMAC keys** — You can verify a HMAC tag that was generated by the HMAC KMS key with imported key material. You can also use the HMAC KMS key with the imported key material to verify an HMAC tag that was generated by the key material outside of Amazon.
- **Asymmetric encryption keys** — You can use your private asymmetric encryption key outside of Amazon to decrypt a ciphertext encrypted by the KMS key with the corresponding public key. You can also use your asymmetric KMS key to decrypt an asymmetric ciphertext that was generated outside of Amazon.
- **Asymmetric signing keys** — You can use your asymmetric signing KMS key with imported key material to verify digital signatures generated by your private signing key outside of Amazon. You can also use your asymmetric public signing key outside of Amazon to verify signatures generated by your asymmetric KMS key.

- Asymmetric key agreement keys — You can use your asymmetric key agreement KMS key with imported key material to derive shared secrets with a peer outside of Amazon.

If you import the same key material into different KMS keys in the same Amazon Web Services Region, those keys are also interoperable. To create interoperable KMS keys in different Amazon Web Services Regions, create a multi-Region key with imported key material.

Symmetric encryption keys are not portable or interoperable

The symmetric ciphertexts that Amazon KMS produces are not portable or interoperable. Amazon KMS does not publish the symmetric ciphertext format that portability requires, and the format might change without notice.

- Amazon KMS cannot decrypt symmetric ciphertexts that you encrypt outside of Amazon, even if you use key material that you have imported.
- Amazon KMS does not support decrypting any Amazon KMS symmetric ciphertext outside of Amazon KMS, even if the ciphertext was encrypted under a KMS key with imported key material.
- KMS keys with the same imported key material are not interoperable. The symmetric ciphertext that Amazon KMS generates ciphertext that is specific to each KMS key. This ciphertext format guarantees that only the KMS key that encrypted data can decrypt it.

Also, you cannot use any Amazon tools, such as the [Amazon Encryption SDK](#) or [Amazon S3 client-side encryption](#), to decrypt Amazon KMS symmetric ciphertexts.

As a result, you cannot use keys with imported key material to support key escrow arrangements where an authorized third party with conditional access to key material can decrypt certain ciphertexts outside of Amazon KMS. To support key escrow, use the [Amazon Encryption SDK](#) to encrypt your message under a key that is independent of Amazon KMS.

You're responsible for availability and durability

Amazon KMS is designed to keep imported key material highly available. But Amazon KMS does not maintain the durability of imported key material at the same level as key material that Amazon KMS generates. For details, see [Protecting imported key material](#).

Protecting imported key material

The key material that you import is protected in transit and at rest. Before importing the key material, you encrypt (or "wrap") the key material with the public key of an RSA key pair generated

in Amazon KMS hardware security modules (HSMs) validated under the [FIPS 140-3 Cryptographic Module Validation Program](#). You can encrypt the key material directly with the wrapping public key, or encrypt the key material with an AES symmetric key, and then encrypt the AES symmetric key with the RSA public key.

Upon receipt, Amazon KMS decrypts the key material with the corresponding private key in a Amazon KMS HSM and re-encrypts it under an AES symmetric key that exists only in the volatile memory of the HSM. Your key material never leaves the HSM in plain text. It is decrypted only while it is in use and only within Amazon KMS HSMs.

Use of your KMS key with imported key material is determined solely by the [access control policies](#) that you set on the KMS key. In addition, you can use [aliases](#) and [tags](#) to identify and [control access](#) to the KMS key. You can [enable and disable](#) the key, [view](#), and [monitor](#) it using services like Amazon CloudTrail.

However, you maintain the only failsafe copy of your key material. In return for this extra measure of control, you are responsible for durability and overall availability of the imported key material. Amazon KMS is designed to keep imported key material highly available. But Amazon KMS does not maintain the durability of imported key material at the same level as key material that Amazon KMS generates.

This difference in durability is meaningful in the following cases:

- When you [set an expiration time](#) for your imported key material, Amazon KMS deletes the key material after it expires. Amazon KMS does not delete the KMS key or its metadata. You can [create a Amazon CloudWatch alarm](#) that notifies you when imported key material is approaching its expiration date.

You cannot delete key material that Amazon KMS generates for a KMS key and you cannot set Amazon KMS key material to expire, although you can [rotate it](#).

- When you [manually delete imported key material](#), Amazon KMS deletes the key material but does not delete the KMS key or its metadata. In contrast, [scheduling key deletion](#) requires a waiting period of 7 to 30 days, after which Amazon KMS permanently deletes the KMS key, its metadata, and its key material.
- In the unlikely event of certain region-wide failures that affect Amazon KMS (such as a total loss of power), Amazon KMS cannot automatically restore your imported key material. However, Amazon KMS can restore the KMS key and its metadata.

You *must* retain a copy of the imported key material outside of Amazon in a system that you control. We recommend that you store an exportable copy of the imported key material in a key management system, such as an HSM. If your imported key material is deleted or expires, its associated KMS key becomes unusable until you reimport the same key material. If your imported key material is permanently lost, any ciphertext encrypted under the KMS key is unrecoverable.

KMS keys in a CloudHSM key store

You can create, view, manage, use, and schedule deletion of the Amazon KMS keys in an Amazon CloudHSM key store. The procedures that you use are very similar to those you use for other KMS keys. The only difference is that you specify an Amazon CloudHSM key store when you create the KMS key. Then, Amazon KMS creates non-extractable key material for the KMS key in the Amazon CloudHSM cluster that is associated with the Amazon CloudHSM key store. When you use a KMS key in an Amazon CloudHSM key store, the [cryptographic operations](#) are performed in the HSMs in the cluster.

Supported features

In addition to the procedures discussed in this section, you can do the following with KMS keys in an Amazon CloudHSM key store:

- Use key policies, IAM policies, and grants to [authorize access](#) to the KMS keys.
- [Enable and disable](#) the KMS keys.
- Assign [tags](#) and create [aliases](#), and use attribute-based access control (ABAC) to authorize access to the KMS keys.
- Use the KMS keys to perform the following cryptographic operations:
 - [Encrypt](#)
 - [Decrypt](#)
 - [GenerateDataKey](#)
 - [GenerateDataKeyWithoutPlaintext](#)
 - [ReEncrypt](#)

The operations that generate asymmetric data key pairs, [GenerateDataKeyPair](#) and [GenerateDataKeyPairWithoutPlaintext](#), are *not* supported in custom key stores.

- Use the KMS keys with [Amazon services that integrate with Amazon KMS](#) and support customer managed keys.

- Track use of your KMS keys in [Amazon CloudTrail logs](#) and [Amazon CloudWatch monitoring tools](#).

Unsupported features

- Amazon CloudHSM key stores support only symmetric encryption KMS keys. You cannot create HMAC KMS keys, asymmetric KMS keys, or asymmetric data key pairs in an Amazon CloudHSM key store.
- You cannot [import key material](#) into a KMS key in an Amazon CloudHSM key store. Amazon KMS generates the key material for the KMS key in the Amazon CloudHSM cluster.
- You cannot enable or disable [automatic rotation](#) of the key material for a KMS key in an Amazon CloudHSM key store.

Using KMS keys in an Amazon CloudHSM key store

When you use your KMS key in a request, identify the KMS key by its ID or alias; you do not need to specify the Amazon CloudHSM key store or Amazon CloudHSM cluster. The response includes the same fields that are returned for any symmetric encryption KMS key.

However, when you use a KMS key in an Amazon CloudHSM key store, the cryptographic operation is performed entirely within the Amazon CloudHSM cluster that is associated with the Amazon CloudHSM key store. The operation uses the key material in the cluster that is associated with the KMS key that you chose.

To make this possible, the following conditions are required.

- The [key state](#) of the KMS key must be Enabled. To find the key state, use the **Status** field in the [Amazon KMS console](#) or the `KeyState` field in the [DescribeKey](#) response.
- The Amazon CloudHSM key store must be connected to its Amazon CloudHSM cluster. Its **Status** in the [Amazon KMS console](#) or `ConnectionState` in the [DescribeCustomKeyStores](#) response must be CONNECTED.
- The Amazon CloudHSM cluster that is associated with the custom key store must contain at least one active HSM. To find the number of active HSMs in the cluster, use the [Amazon KMS console](#), the Amazon CloudHSM console, or the [DescribeClusters](#) operation.
- The Amazon CloudHSM cluster must contain the key material for the KMS key. If the key material was deleted from the cluster, or an HSM was created from a backup that did not include the key material, the cryptographic operation will fail.

If these conditions are not met, the cryptographic operation fails, and Amazon KMS returns a `KMSInvalidStateException` exception. Typically, you just need to [reconnect the Amazon CloudHSM key store](#). For additional help, see [How to fix a failing KMS key](#).

When using the KMS keys in an Amazon CloudHSM key store, be aware that the KMS keys in each Amazon CloudHSM key store share a [custom key store request quota](#) for cryptographic operations. If you exceed the quota, Amazon KMS returns a `ThrottlingException`. If the Amazon CloudHSM cluster that is associated with the Amazon CloudHSM key store is processing numerous commands, including those unrelated to the Amazon CloudHSM key store, you might get a `ThrottlingException` at an even lower rate. If you get a `ThrottlingException` for any request, lower your request rate and try the commands again. For details about the custom key store request quota, see [Custom key store request quotas](#).

Learn more

- To learn more about Amazon CloudHSM key stores, see [Amazon CloudHSM key stores](#).
- To create KMS keys in an Amazon CloudHSM key store, see [Create a KMS key in an Amazon CloudHSM key store](#).
- To identify and view KMS keys in an Amazon CloudHSM key store, see [Identify KMS keys in Amazon CloudHSM key stores](#).
- To find KMS keys and key material in an Amazon CloudHSM key store, see [Find KMS keys and key material in an Amazon CloudHSM key store](#).
- To learn about special considerations for deleting KMS keys in an Amazon CloudHSM key store, see [Deleting KMS keys from an Amazon CloudHSM key store](#).

KMS keys in external key stores

To create, view, manage, use, and schedule deletion of the KMS keys in an external key store, you use procedures that are very similar to those you use for other KMS keys. However, when you create a KMS key in an external key store, you specify an [external key store](#) and an [external key](#). When you use a KMS key in an external key store, [encryption and decryption operations](#) are performed by your external key manager using the specified external key.

Amazon KMS cannot create, view, update, or delete any cryptographic keys in your external key manager. Amazon KMS never directly accesses your external key manager or any external key. All requests for cryptographic operations are mediated by your [external key store proxy](#). To use a KMS key in an external key store, the external key store that hosts the KMS key must be [connected](#) to its external key store proxy.

Supported features

In addition to the procedures discussed in this section, you can do the following with KMS keys in an external key store:

- Use [key policies](#), [IAM policies](#), and [grants](#) to control access to the KMS keys.
- [Enable and disable](#) the KMS keys. These actions do not affect the external key in your external key manager.
- Assign [tags](#) and create [aliases](#), and use [attribute-based access control](#) (ABAC) to authorize access to the KMS keys.
- Use the KMS keys to perform the following cryptographic operations:
 - [Encrypt](#)
 - [Decrypt](#)
 - [GenerateDataKey](#)
 - [GenerateDataKeyWithoutPlaintext](#)
 - [ReEncrypt](#)

The operations that generate asymmetric data key pairs, [GenerateDataKeyPair](#) and [GenerateDataKeyPairWithoutPlaintext](#), are *not* supported in custom key stores.

- Use the KMS keys with [Amazon Web Services services that integrate with Amazon KMS](#) and support [customer managed keys](#).

Unsupported features

- External key stores support only [symmetric encryption KMS keys](#). You cannot create HMAC KMS keys or asymmetric KMS keys in an external key store.
- [GenerateDataKeyPair](#) and [GenerateDataKeyPairWithoutPlaintext](#) are not supported on KMS keys in an external key store.
- You cannot use an [AWS::KMS::Key Amazon CloudFormation template](#) to create an external key store or a KMS key in an external key store.
- [Multi-Region keys](#) are not supported in an external key store.
- KMS keys with [imported key material](#) are not supported in an external key store.
- [Automatic key rotation](#) is not supported for KMS keys in an external key store.

Using KMS keys in an external key store

When you use your KMS key in a request, identify the KMS key by its [key ID, key ARN, alias, or alias ARN](#). You do not need to specify the external key store. The response includes the same

fields that are returned for any symmetric encryption KMS key. However, when you use a KMS key in an external key store, encryption and decryption operations are performed by your external key manager using the external key that is associated with the KMS key.

To ensure that ciphertext encrypted by a KMS key in an external key store is at least as secure as any ciphertext encrypted by a standard KMS key, Amazon KMS uses [double encryption](#). Data is first encrypted in Amazon KMS using Amazon KMS key material. Then it is encrypted by your external key manager using the external key for the KMS key. To decrypt double-encrypted ciphertext, the ciphertext is first decrypted by your external key manager using the external key for the KMS key. Then it is decrypted in Amazon KMS using the Amazon KMS key material for the KMS key.

To make this possible, the following conditions are required.

- The [key state](#) of the KMS key must be Enabled. To find the key state, see the **Status** field for customer managed keys the [Amazon KMS console](#) or the `KeyState` field in the [DescribeKey](#) response.
- The external key store that hosts the KMS key must be connected to its [external key store proxy](#), that is, the [connection state](#) of the external key store must be CONNECTED.

You can view the connection state on the **External key stores** page in the Amazon KMS console or in the [DescribeCustomKeyStores](#) response. The connection state of the external key store is also displayed on the detail page for the KMS key in the Amazon KMS console. On the detail page, choose the **Cryptographic configuration** tab and see the **Connection state** field in the **Custom key store** section.

If the connection state is DISCONNECTED, you must first connect it. If the connection state is FAILED, you must resolve the problem, disconnect the external key store, and then connect it. For instructions, see [Connect and disconnect external key stores](#).

- The external key store proxy must be able to find the external key.
- The external key must be enabled and it must perform encryption and decryption.

The status of the external key is independent of and not affected by changes in the [key state](#) of the KMS key, including enabling and disabling the KMS key. Similarly, disabling or deleting the external key doesn't change the key state of the KMS key, but cryptographic operations using the associated KMS key will fail.

If these conditions are not met, the cryptographic operation fails, and Amazon KMS returns a `KMSInvalidStateException` exception. You might need to [reconnect the external key store](#)

or use your external key manager tools to reconfigure or repair your external key. For additional help, see [the section called “Troubleshooting external key stores”](#).

When using the KMS keys in an external key store, be aware that the KMS keys in each external key store share a [custom key store request quota](#) for cryptographic operations. If you exceed the quota, Amazon KMS returns a `ThrottlingException`. For details about the custom key store request quota, see [Custom key store request quotas](#).

Learn more

- To learn more about external key stores, see [External key stores](#).
- To learn more about key material in external key stores, see [External key](#).
- To create KMS keys in an external key store, see [Create a KMS key in external key stores](#).
- To identify and view KMS keys in an external key store, see [Identify KMS keys in external key stores](#).
- To learn about special considerations for deleting KMS keys in an external key store, see [Deleting KMS keys from an external key store](#).

Amazon KMS cryptography essentials

Amazon KMS uses configurable cryptographic algorithms so that the system can quickly migrate from one approved algorithm, or mode, to another. The initial default set of cryptographic algorithms has been selected from Federal Information Processing Standard (FIPS-approved) algorithms for their security properties and performance.

Entropy and random number generation

Amazon KMS key generation is performed in the Amazon KMS HSMs. The HSMs implement a hybrid random number generator that uses the [NIST SP800-90A Deterministic Random Bit Generator \(DRBG\) CTR_DRBG using AES-256](#). It is seeded with a nondeterministic random bit generator with 384-bits of entropy and updated with additional entropy to provide prediction resistance on every call for cryptographic material.

Symmetric key operations (encryption only)

All symmetric key encrypt commands used within HSMs use the [Advanced Encryption Standards \(AES\)](#), in [Galois Counter Mode \(GCM\)](#) using 256-bit keys. The analogous calls to decrypt use the inverse function.

AES-GCM is an authenticated encryption scheme. In addition to encrypting plaintext to produce ciphertext, it computes an authentication tag over the ciphertext and any additional data for which authentication is required (additionally authenticated data, or AAD). The authentication tag helps ensure that the data is from the purported source and that the ciphertext and AAD have not been modified.

Frequently, Amazon omits the inclusion of the AAD in our descriptions, especially when referring to the encryption of data keys. It is implied by surrounding text in these cases that the structure to be encrypted is partitioned between the plaintext to be encrypted and the cleartext AAD to be protected.

Amazon KMS provides an option for you to import key material into an Amazon KMS key instead of relying on Amazon KMS to generate the key material. This imported key material can be encrypted using [RSAES-OAEP](#) to protect the key during transport to the Amazon KMS HSM. The RSA key pairs are generated on Amazon KMS HSMs. The imported key material is decrypted on an Amazon KMS HSM and re-encrypted under AES-GCM before being stored by the service.

Asymmetric key operations (encryption, digital signing and signature verification)

Amazon KMS supports the use of asymmetric key operations for both encryption, digital signature, and key agreement operations. Asymmetric key operations rely on a mathematically related public key and private key pair that you can use for encryption and decryption, signing and signature verification, *or* deriving shared secrets. The private key never leaves Amazon KMS unencrypted. You can use the public key within Amazon KMS by calling the Amazon KMS API operations, or download the public key and use it outside of Amazon KMS.

Amazon KMS supports the following asymmetric ciphers.

- **RSA-OAEP (for encryption) & RSA-PSS and RSA-PKCS-#1-v1_5 (for signing and verification)** – Supports RSA key lengths (in bits): 2048, 3072, and 4096 for different security requirements.
- **Elliptic Curve (ECC)** – Used for signing and verification or deriving shared secrets, but not both. Supports ECC curves: NIST P256, P384, P521, SECP 256k1.
- **SM2 (China Regions only)** – Used for encryption and decryption, signing and verification, or deriving shared secrets, but you must choose one key usage. Supports SM2PKE for encryption and SM2DSA for signing.

Key derivation functions

A key derivation function is used to derive additional keys from an initial secret or key. Amazon KMS uses an key derivation function (KDF) to derive per-call keys for every encryption under an Amazon KMS key. All KDF operations use the [KDF in counter mode](#) using HMAC [\[FIPS197\]](#) with SHA256 [\[FIPS180\]](#). The 256-bit derived key is used with AES-GCM to encrypt or decrypt customer data and keys.

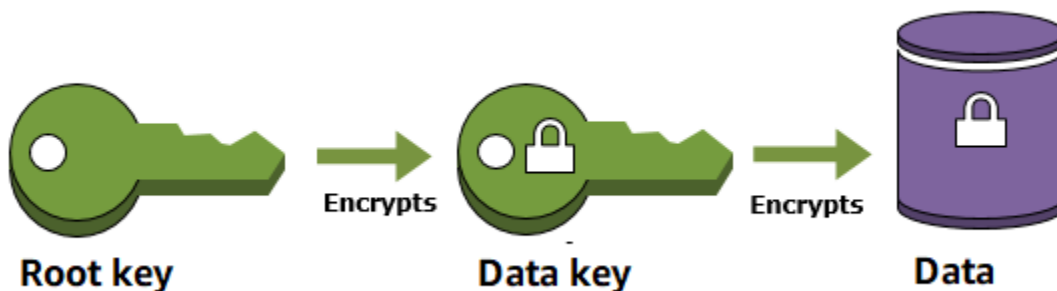
Amazon KMS internal use of digital signatures

Digital signatures are also used to authenticate commands and communications between Amazon KMS entities. All service entities have an elliptic curve digital signature algorithm (ECDSA) key pair. They perform ECDSA as defined in [Use of Elliptic Curve Cryptography \(ECC\) Algorithms in Cryptographic Message Syntax \(CMS\)](#) and [X9.62-2005: Public Key Cryptography for the Financial Services Industry: The Elliptic Curve Digital Signature Algorithm \(ECDSA\)](#). The entities use the secure hash algorithm defined in [Federal Information Processing Standards Publications, FIPS PUB 180-4](#), known as SHA384. The keys are generated on the curve `secp384r1` (NIST-P384).

Envelope encryption

When you encrypt your data, your data is protected, but you have to protect your encryption key. One strategy is to encrypt it. *Envelope encryption* is the practice of encrypting plaintext data with a data key, and then encrypting the data key under another key.

You can even encrypt the data encryption key under another encryption key, and encrypt that encryption key under another encryption key. But, eventually, one key must remain in plaintext so you can decrypt the keys and your data. This top-level plaintext key encryption key is known as the *root key*.



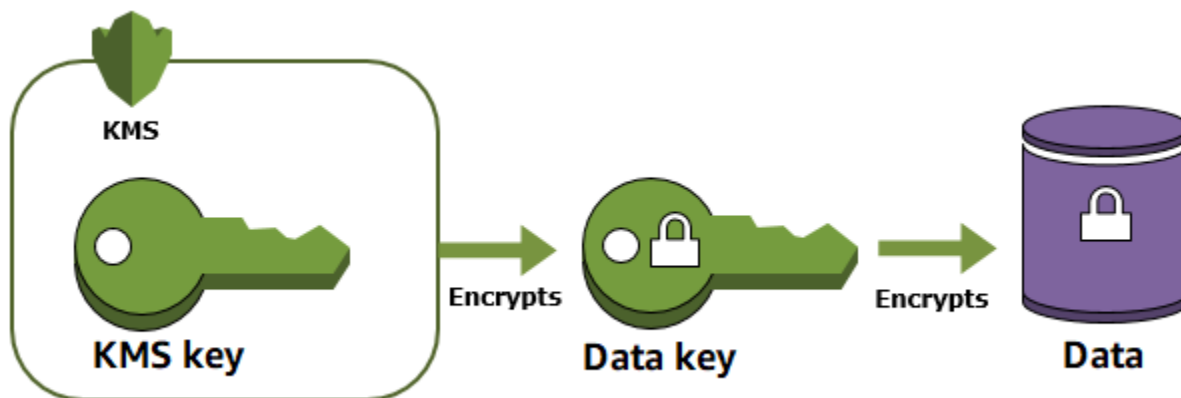
Amazon KMS helps you to protect your encryption keys by storing and managing them securely. Root key stored in Amazon KMS, known as Amazon KMS keys, never leave the Amazon KMS [FIPS 140-3 Security Level 3 validated hardware security modules](#) unencrypted. To use a KMS key, you must call Amazon KMS.

A basic construction used within many cryptographic systems is envelope encryption. Envelope encryption uses two or more cryptographic keys to secure a message. Typically, one key is derived from a longer-term static key k , and another key is a per-message key, $msgKey$, which is generated to encrypt the message. The envelope is formed by encrypting the message: $ciphertext = Encrypt(msgKey, message)$. Then the message key is encrypted with the long-term static key: $encKey = Encrypt(k, msgKey)$. Finally, the two values $(encKey, ciphertext)$ are packaged into a single structure, or envelope encrypted message.

The recipient, with access to k , can open the enveloped message by first decrypting the encrypted key and then decrypting the message.

Amazon KMS provides the ability to manage these longer-term static keys and automate the process of envelope encryption of your data.

In addition to the encryption capabilities provided within the Amazon KMS service, the [Amazon Encryption SDK](#) provides client-side envelope encryption libraries. You can use these libraries to protect your data and the encryption keys that are used to encrypt that data.



Envelope encryption offers several benefits:

- **Protecting data keys**

When you encrypt a data key, you don't have to worry about storing the encrypted data key, because the data key is inherently protected by encryption. You can safely store the encrypted data key alongside the encrypted data.

- **Encrypting the same data under multiple keys**

Encryption operations can be time consuming, particularly when the data being encrypted are large objects. Instead of re-encrypting raw data multiple times with different keys, you can re-encrypt only the data keys that protect the raw data.

- **Combining the strengths of multiple algorithms**

In general, symmetric key algorithms are faster and produce smaller ciphertexts than public key algorithms. But public key algorithms provide inherent separation of roles and easier key management. Envelope encryption lets you combine the strengths of each strategy.

Cryptographic operations

In Amazon KMS, *cryptographic operations* are API operations that use KMS keys to protect data. Because KMS keys remain within Amazon KMS, you must call Amazon KMS to use a KMS key in a cryptographic operation.

To perform cryptographic operations with KMS keys, use the Amazon SDKs, Amazon Command Line Interface (Amazon CLI), or the Amazon Tools for PowerShell. You cannot perform cryptographic operations in the Amazon KMS console. For examples of calling the cryptographic operations in several programming languages, see [Code examples for Amazon KMS using Amazon SDKs](#).

The following table lists the Amazon KMS cryptographic operations. It also shows the key type and [key usage](#) requirements for KMS keys used in the operation.

Operation	Key type	Key usage
Decrypt	Symmetric or asymmetric	ENCRYPT_DECRYPT
DeriveSharedSecret	Asymmetric	KEY_AGREEMENT
Encrypt	Symmetric or asymmetric	ENCRYPT_DECRYPT
GenerateDataKey	Symmetric	ENCRYPT_DECRYPT
GenerateDataKeyPair	Symmetric [1]	ENCRYPT_DECRYPT

Operation	Key type	Key usage
	Not supported on KMS keys in custom key stores.	
GenerateDataKeyPairWithoutPlaintext	Symmetric [1] Not supported on KMS keys in custom key stores.	ENCRYPT_DECRYPT
GenerateDataKeyWithoutPlaintext	Symmetric	ENCRYPT_DECRYPT
GenerateMac	HMAC	GENERATE_VERIFY_MAC
GenerateRandom	N/A. This operation doesn't use a KMS key.	N/A
ReEncrypt	Symmetric or asymmetric	ENCRYPT_DECRYPT
Sign	Asymmetric	SIGN_VERIFY
Verify	Asymmetric	SIGN_VERIFY
VerifyMac	HMAC	GENERATE_VERIFY_MAC

[1] Generates an asymmetric data key pair that is protected by a symmetric encryption KMS key.

For information about the permissions for cryptographic operations, see the [the section called "Permissions reference"](#).

To make Amazon KMS responsive and highly functional for all users, Amazon KMS establishes quotas on number of cryptographic operations called in each second. For details, see [the section called "Shared quotas for cryptographic operations"](#).

KMS key access and permissions

To use Amazon KMS, you must have credentials that Amazon can use to authenticate your requests. The credentials must include permissions to access Amazon resources: Amazon KMS keys and [aliases](#). No Amazon principal has any permissions to a KMS key unless that permission is provided explicitly and never denied. There are no implicit or automatic permission to use or manage a KMS key.

To control access to your KMS keys, you can use the following policy mechanisms.

- [Key policy](#) – Every KMS key has a key policy. It is the primary mechanism for controlling access to a KMS key. You can use the key policy alone to control access, which means the full scope of access to the KMS key is defined in a single document (the key policy). For more information about using key policies, see [Key policies](#).
- [IAM policies](#) – You can use IAM policies in combination with the key policy and grants to control access to a KMS key. Controlling access this way enables you to manage all of the permissions for your IAM identities in IAM. To use an IAM policy to allow access to a KMS key, the key policy must explicitly allow it. For more information about using IAM policies, see [IAM policies](#).
- [Grants](#) – You can use grants in combination with the key policy and IAM policies to allow access to a KMS key. Controlling access this way enables you to allow access to the KMS key in the key policy, and to allow identities to delegate their access to others. For more information about using grants, see [Grants in Amazon KMS](#).

KMS key policies

The primary way to manage access to your Amazon KMS resources is with *policies*. Policies are documents that describe which principals can access which resources. Policies attached to an IAM identity are called *identity-based policies* (or *IAM policies*), and policies attached to other kinds of resources are called *resource policies*. Amazon KMS resource policies for KMS keys are called *key policies*.

All KMS keys have a key policy. If you don't provide one, Amazon KMS creates one for you. The [default key policy](#) that Amazon KMS uses differs depending on whether you create the key in the Amazon KMS console or you use the Amazon KMS API. We recommend that you edit the default key policy to align with your organization's requirements for [least-privilege permissions](#).

You can use the key policy alone to control access if the key and the IAM principal are in the same Amazon account, which means the full scope of access to the KMS key is defined in a single document (the key policy). However, when a caller in one account must access a key in a different account, you cannot use key policy alone to grant access. In the cross-account scenario, an IAM policy must be attached to the caller's user or role that explicitly allows the caller to make the API call.

You can also use IAM policies in combination with key policies and grants to control access to a KMS key. To use an IAM policy to control access to a KMS key, the key policy must give the account permission to use IAM policies. You can either specify a [key policy statement that enables IAM policies](#), or you can explicitly [specify allowed principals](#) in the key policy.

When writing policies, ensure that you have strong controls restricting who can perform the following actions:

- Update, create, and delete IAM and KMS key policies
- Attach and detach IAM policies from users, roles, and groups
- Attach and detach KMS key policies from your KMS keys

KMS key grants

In addition to IAM and key policies, Amazon KMS supports [grants](#). Grants provide a flexible and powerful way to delegate permissions. You can use grants to issue time-bound KMS key access to IAM principals in your Amazon account, or in other Amazon accounts. We recommend issuing time-bound access if you don't know the names of the principals at the time that the policies are created, or if the principals that require access frequently change. The [grantee principal](#) can be in the same account as the KMS key or a different account. If the principal and KMS key are in different accounts, then you must specify an IAM policy in addition to the grant. Grants require additional management because you must call an API to create the grant and to retire or revoke the grant when it is no longer needed.

The following topics provide details about how you can use Amazon Identity and Access Management (IAM) and Amazon KMS permissions to help secure your resources by controlling who can access them.

Key policies in Amazon KMS

A key policy is a resource policy for an Amazon KMS key. Key policies are the primary way to control access to KMS keys. Every KMS key must have exactly one key policy. The statements in the key policy determine who has permission to use the KMS key and how they can use it. You can also use [IAM policies](#) and [grants](#) to control access to the KMS key, but every KMS key must have a key policy.

No Amazon principal, including the account root user or key creator, has any permissions to a KMS key unless they are explicitly allowed, and never denied, in a key policy, IAM policy, or grant.

Unless the key policy explicitly allows it, you cannot use IAM policies to *allow* access to a KMS key. Without permission from the key policy, IAM policies that allow permissions have no effect. (You can use an IAM policy to *deny* a permission to a KMS key without permission from a key policy.) The default key policy enables IAM policies. To enable IAM policies in your key policy, add the policy statement described in [Allows access to the Amazon Web Services account and enables IAM policies](#).

Unlike IAM policies, which are global, key policies are Regional. A key policy controls access only to a KMS key in the same Region. It has no effect on KMS keys in other Regions.

Topics

- [Creating a key policy](#)
- [Default key policy](#)
- [View a key policies](#)
- [Change a key policy](#)
- [Permissions for Amazon services in key policies](#)

Creating a key policy

You can create and manage key policies in the Amazon KMS console or by using Amazon KMS API operations, such as [CreateKey](#), [ReplicateKey](#), and [PutKeyPolicy](#).

When you create a KMS key in the Amazon KMS console, the console walks you through the steps of creating a key policy based on the [default key policy for the console](#). When you use the `CreateKey` or `ReplicateKey` APIs, if you don't specify a key policy, these APIs apply the [default key policy for keys created programmatically](#). When you use the `PutKeyPolicy` API, you are required to specify a key policy.

Each policy document can have one or more policy statements. The following example shows a valid key policy document with one policy statement.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "Describe the policy statement",
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::111122223333:user/Alice"
      },
      "Action": "kms:DescribeKey",
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "kms:KeySpec": "SYMMETRIC_DEFAULT"
        }
      }
    }
  ]
}
```

Topics

- [Key policy format](#)
- [Elements in a key policy](#)
- [Example key policy](#)

Key policy format

A key policy document must conform to the following rules:

- Up to 32 kilobytes (32,768 bytes)
- The Sid element in a key policy statement can include spaces. (Spaces are prohibited in the Sid element of an IAM policy document.)

A key policy document can include only the following characters:

- Printable ASCII characters

- Printable characters in the Basic Latin and Latin-1 Supplement character set
- The tab (`\u0009`), line feed (`\u000A`), and carriage return (`\u000D`) special characters

Elements in a key policy

A key policy document must have the following elements:

Version

Specifies the key policy document version. Set the version to `2012-10-17` (the latest version).

Statement

Encloses the policy statements. A key policy document must have at least one statement.

Each key policy statement consists of up to six elements. The `Effect`, `Principal`, `Action`, and `Resource` elements are required.

Sid

(Optional) The statement identifier (`Sid`) an arbitrary string you can use to describe the statement. The `Sid` in a key policy can include spaces. (You can't include spaces in an IAM policy `Sid` element.)

Effect

(Required) Determines whether to allow or deny the permissions in the policy statement. Valid values are `Allow` or `Deny`. If you don't explicitly allow access to a KMS key, access is implicitly denied. You can also explicitly deny access to a KMS key. You might do this to make sure that a user cannot access it, even when a different policy allows access.

Principal

(Required) The [principal](#) is the identity that gets the permissions specified in the policy statement. You can specify Amazon Web Services accounts, IAM users, IAM roles, and some Amazon services as principals in a key policy. IAM [user groups](#) are not a valid principal in any policy type.

An asterisk value, such as `"AWS": "*"` represents all Amazon identities in all accounts.

⚠ Important

Do not set the Principal to an asterisk (*) in any key policy statement that allows permissions unless you use [conditions](#) to limit the key policy. An asterisk gives every identity in every Amazon Web Services account permission to use the KMS key, unless another policy statement explicitly denies it. Users in other Amazon Web Services accounts can use your KMS key whenever they have corresponding permissions in their own account.

ℹ Note

IAM best practices discourage the use of IAM users with long-term credentials. Whenever possible, use IAM roles, which provide temporary credentials. For details, see [Security best practices in IAM](#) in the *IAM User Guide*.

When the principal in a key policy statement is an [Amazon Web Services account principal](#) expressed as `arn:aws:iam::111122223333:root`, the policy statement doesn't give permission to any IAM principal. Instead, it gives the Amazon Web Services account permission to use IAM policies to delegate the permissions specified in the key policy. (A principal in `arn:aws:iam::111122223333:root` format does *not* represent the [Amazon account root user](#), despite the use of "root" in the account identifier. However, the account principal represents the account and its administrators, including the account root user.)

When the principal is another Amazon Web Services account or its principals, the permissions are effective only when the account is enabled in the Region with the KMS key and key policy. For information about Regions that are not enabled by default ("opt-in Regions"), see [Managing Amazon Web Services Regions](#) in the *Amazon Web Services General Reference*.

To allow a different Amazon Web Services account or its principals to use a KMS key, you must provide permission in a key policy and in an IAM policy in the other account. For details, see [Allowing users in other accounts to use a KMS key](#).

Action

(Required) Specify the API operations to allow or deny. For example, the `kms:Encrypt` action corresponds to the Amazon KMS [Encrypt](#) operation. You can list more than one action in a policy statement. For more information, see [Permissions reference](#).

Note

If the required `Action` element is missing from a key policy statement, the policy statement has no effect. A key policy statement without an `Action` element doesn't apply to any KMS key.

When a key policy statement is missing its `Action` element, the Amazon KMS console correctly reports an error, but the [CreateKey](#) and [PutKeyPolicy](#) APIs succeed, even though the policy statement is ineffective.

Resource

(Required) In a key policy, the value of the `Resource` element is `"*"`, which means "this KMS key." The asterisk (`"*"`) identifies the KMS key to which the key policy is attached.

Note

If the required `Resource` element is missing from a key policy statement, the policy statement has no effect. A key policy statement without a `Resource` element doesn't apply to any KMS key.

When a key policy statement is missing its `Resource` element, the Amazon KMS console correctly reports an error, but the [CreateKey](#) and [PutKeyPolicy](#) APIs succeed, even though the policy statement is ineffective.

Condition

(Optional) Conditions specify requirements that must be met for a key policy to take effect. With conditions, Amazon can evaluate the context of an API request to determine whether or not the policy statement applies.

To specify conditions, you use predefined *condition keys*. Amazon KMS supports [Amazon global condition keys](#) and [Amazon KMS condition keys](#). To support attribute-based access

control (ABAC), Amazon KMS provides condition keys that control access to a KMS key based on tags and aliases. For details, see [ABAC for Amazon KMS](#).

The format for a condition is:

```
"Condition": {"condition operator": {"condition key": "condition value"}}
```

such as:

```
"Condition": {"StringEquals": {"kms:CallerAccount": "111122223333"}}
```

For more information about Amazon policy syntax, see [Amazon IAM Policy Reference](#) in the *IAM User Guide*.

Example key policy

The following example shows a complete key policy for a symmetric encryption KMS key. You can use it for reference as you read about the key policy concepts in this chapter. This key policy combines the example policy statements from the preceding [default key policy](#) section into a single key policy that accomplishes the following:

- Allows the example Amazon Web Services account, 111122223333, full access to the KMS key. It allows the account and its administrators, including the account root user (for emergencies), to use IAM policies in the account to allow access to the KMS key.
- Allows the ExampleAdminRole IAM role to administer the KMS key.
- Allows the ExampleUserRole IAM role to use the KMS key.

```
{
  "Id": "key-consolepolicy",
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "Enable IAM user Permissions",
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::111122223333:root"
      },
      "Action": "kms:*",
      "Resource": "*"
    }
  ]
}
```

```
    },
    {
      "Sid": "Allow access for Key Administrators",
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::111122223333:role/ExampleAdminRole"
      },
      "Action": [
        "kms:Create*",
        "kms:Describe*",
        "kms:Enable*",
        "kms:List*",
        "kms:Put*",
        "kms:Update*",
        "kms:Revoke*",
        "kms:Disable*",
        "kms:Get*",
        "kms>Delete*",
        "kms:TagResource",
        "kms:UntagResource",
        "kms:ScheduleKeyDeletion",
        "kms:CancelKeyDeletion",
        "kms:RotateKeyOnDemand"
      ],
      "Resource": "*"
    },
    {
      "Sid": "Allow use of the key",
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::111122223333:role/ExampleUserRole"
      },
      "Action": [
        "kms:Encrypt",
        "kms:Decrypt",
        "kms:ReEncrypt*",
        "kms:GenerateDataKey*",
        "kms:DescribeKey"
      ],
      "Resource": "*"
    },
    {
      "Sid": "Allow attachment of persistent resources",
      "Effect": "Allow",
```

```
    "Principal": {
      "AWS": "arn:aws:iam::111122223333:role/ExampleUserRole"
    },
    "Action": [
      "kms:CreateGrant",
      "kms:ListGrants",
      "kms:RevokeGrant"
    ],
    "Resource": "*",
    "Condition": {
      "Bool": {
        "kms:GrantIsForAWSResource": "true"
      }
    }
  }
]
```

Default key policy

When you create a KMS key, you can specify the key policy for the new KMS key. If you don't provide one, Amazon KMS creates one for you. The default key policy that Amazon KMS uses differs depending on whether you create the key in the Amazon KMS console or you use the Amazon KMS API.

Default key policy when you create a KMS key programmatically

When you create a KMS key programmatically with the [Amazon KMS API](#) (including by using the [Amazon SDKs](#), [Amazon Command Line Interface](#) or [Amazon Tools for PowerShell](#)), and you don't specify a key policy, Amazon KMS applies a very simple default key policy. This default key policy has one policy statement that gives the Amazon Web Services account that owns the KMS key permission to use IAM policies to allow access to all Amazon KMS operations on the KMS key. For more information about this policy statement, see [Allows access to the Amazon Web Services account and enables IAM policies](#).

Default key policy when you create a KMS key with the Amazon Web Services Management Console

When you [create a KMS key with the Amazon Web Services Management Console](#), the key policy begins with the policy statement that [allows access to the Amazon Web Services account and enables IAM policies](#). The console then adds a [key administrators statement](#), a [key users](#)

[statement](#), and (for most key types) a statement that allows principals to use the KMS key with [other Amazon services](#). You can use the features of the Amazon KMS console to specify the IAM users, IAM roles, and Amazon Web Services accounts who are key administrators and those who are key users (or both).

Permissions

- [Allows access to the Amazon Web Services account and enables IAM policies](#)
- [Allows key administrators to administer the KMS key](#)
- [Allows key users to use the KMS key](#)
 - [Allows key users to use a KMS key for cryptographic operations](#)
 - [Allows key users to use the KMS key with Amazon services](#)

Allows access to the Amazon Web Services account and enables IAM policies

The following default key policy statement is critical.

- It gives the Amazon Web Services account that owns the KMS key full access to the KMS key.

Unlike other Amazon resource policies, an Amazon KMS key policy does not automatically give permission to the account or any of its identities. To give permission to account administrators, the key policy must include an explicit statement that provides this permission, like this one.

- It allows the account to use IAM policies to allow access to the KMS key, in addition to the key policy.

Without this permission, IAM policies that allow access to the key are ineffective, although IAM policies that deny access to the key are still effective.

- It reduces the risk of the key becoming unmanageable by giving access control permission to the account administrators, including the account root user, which cannot be deleted.

The following key policy statement is the entire default key policy for KMS keys created programmatically. It's the first policy statement in the default key policy for KMS keys created in the Amazon KMS console.

```
{
  "Sid": "Enable IAM User Permissions",
```

```
"Effect": "Allow",
"Principal": {
  "AWS": "arn:aws:iam::111122223333:root"
},
"Action": "kms:*",
"Resource": "*"
}
```

Allows IAM policies to allow access to the KMS key.

The key policy statement shown above gives the Amazon Web Services account that owns the key permission to use IAM policies, as well as key policies, to allow all actions (`kms : *`) on the KMS key.

The principal in this key policy statement is the [account principal](#), which is represented by an ARN in this format: `arn:aws:iam::account-id:root`. The account principal represents the Amazon account and its administrators.

When the principal in a key policy statement is the account principal, the policy statement doesn't give any IAM principal permission to use the KMS key. Instead, it allows the account to use IAM policies to *delegate* the permissions specified in the policy statement. This default key policy statement allows the account to use IAM policies to delegate permission for all actions (`kms : *`) on the KMS key.

Reduces the risk of the KMS key becoming unmanageable.

Unlike other Amazon resource policies, an Amazon KMS key policy does not automatically give permission to the account or any of its principals. To give permission to any principal, including the [account principal](#), you must use a key policy statement that provides the permission explicitly. You are not required to give the account principal, or any principal, access to the KMS key. However, giving access to the account principal helps you prevent the key from becoming unmanageable.

For example, suppose you create a key policy that gives only one user access to the KMS key. If you then delete that user, the key becomes unmanageable and you must [contact Amazon Support](#) to regain access to the KMS key.

The key policy statement shown above gives permission to control the key to the [account principal](#), which represents the Amazon Web Services account and its administrators, including the [account root user](#). The account root user is the only principal that cannot be deleted unless

you delete the Amazon Web Services account. IAM best practices discourage acting on behalf of the account root user, except in an emergency. However, you might need to act as the account root user if you delete all other users and roles with access to the KMS key.

Allows key administrators to administer the KMS key

The default key policy created by the console allows you to choose IAM users and roles in the account and make them *key administrators*. This statement is called the *key administrators statement*. Key administrators have permissions to manage the KMS key, but do not have permissions to use the KMS key in [cryptographic operations](#). You can add IAM users and roles to the list of key administrators when you create the KMS key in the default view or the policy view.

Warning

Because key administrators have permission to change the key policy and create grants, they can give themselves and others Amazon KMS permissions not specified in this policy. Principals who have permission to manage tags and aliases can also control access to a KMS key. For details, see [ABAC for Amazon KMS](#).

Note

IAM best practices discourage the use of IAM users with long-term credentials. Whenever possible, use IAM roles, which provide temporary credentials. For details, see [Security best practices in IAM](#) in the *IAM User Guide*.

The following example shows the key administrators statement in the default view of the Amazon KMS console.

The screenshot shows the Amazon KMS console interface. At the top, there are two tabs: 'Key policy' (selected) and 'Tags'. Below the tabs, the 'Key policy' section has a 'Switch to policy view' button. The main content area is titled 'Key administrators' and includes a description: 'Choose the IAM users and roles who can administer this key through the KMS API. You might need to add additional permissions for the users or roles to administer this key from this console. [Learn more](#)'. There are 'Add' and 'Remove' buttons, a search input field, and a pagination indicator showing '1'. Below this is a table with columns 'Name', 'Path', and 'Type'. The table contains one row: 'ExampleAdminRole' with a path of '/' and a type of 'Role'. At the bottom, the 'Key deletion' section has a checked checkbox for 'Allow key administrators to delete this key'.

The following is an example key administrators statement in the policy view of the Amazon KMS console. This key administrators statement is for a single-region symmetric encryption KMS key.

Note

The Amazon KMS console adds key administrators to the key policy under the statement identifier "Allow access for Key Administrators". Modifying this statement identifier might impact how the console displays updates that you make to the statement.

```
{
  "Sid": "Allow access for Key Administrators",
  "Effect": "Allow",
  "Principal": {"AWS": "arn:aws:iam::111122223333:role/ExampleAdminRole"},
  "Action": [
    "kms:Create*",
  ]
}
```



```
"kms:Describe*",
"kms:Enable*",
"kms:List*",
"kms:Put*",
"kms:Update*",
"kms:Revoke*",
"kms:Disable*",
"kms:Get*",
"kms>Delete*",
"kms:TagResource",
"kms:UntagResource",
"kms:ScheduleKeyDeletion",
"kms:CancelKeyDeletion",
"kms:RotateKeyOnDemand"
],
"Resource": "*"
}
```

The default key administrators statement for the most common KMS key, a single-Region symmetric encryption KMS key, allows the following permissions. For detailed information about each permission, see the [Amazon KMS permissions](#).

When you use the Amazon KMS console to create a KMS key, the console adds the users and roles you specify to the `Principal` element in the key administrators statement.

Many of these permissions contain the wildcard character (*), which allows all permissions that begin with the specified verb. As a result, when Amazon KMS adds new API operations, key administrators are automatically allowed to use them. You don't have to update your key policies to include the new operations. If you prefer to limit your key administrators to a fixed set of API operations, you can [change your key policy](#).

kms:Create*

Allows [kms:CreateAlias](#) and [kms:CreateGrant](#). (The `kms:CreateKey` permission is valid only in an IAM policy.)

kms:Describe*

Allows [kms:DescribeKey](#). The `kms:DescribeKey` permission is required to view the key details page for a KMS key in the Amazon Web Services Management Console.

kms:Enable*

Allows [kms:EnableKey](#). For symmetric encryption KMS keys, it also allows [kms:EnableKeyRotation](#).

kms:List*

Allows [kms:ListGrants](#), [kms:ListKeyPolicies](#), and [kms:ListResourceTags](#). (The [kms:ListAliases](#) and [kms:ListKeys](#) permissions, which are required to view KMS keys in the Amazon Web Services Management Console, are valid only in IAM policies.)

kms:Put*

Allows [kms:PutKeyPolicy](#). This permission allows key administrators to change the key policy for this KMS key.

kms:Update*

Allows [kms:UpdateAlias](#) and [kms:UpdateKeyDescription](#). For multi-Region keys, it allows [kms:UpdatePrimaryRegion](#) on this KMS key.

kms:Revoke*

Allows [kms:RevokeGrant](#), which allows key administrators to [delete a grant](#) even if they are not a [retiring principal](#) in the grant.

kms:Disable*

Allows [kms:DisableKey](#). For symmetric encryption KMS keys, it also allows [kms:DisableKeyRotation](#).

kms:Get*

Allows [kms:GetKeyPolicy](#) and [kms:GetKeyRotationStatus](#). For KMS keys with imported key material, it allows [kms:GetParametersForImport](#). For asymmetric KMS keys, it allows [kms:GetPublicKey](#). The [kms:GetKeyPolicy](#) permission is required to view the key policy of a KMS key in the Amazon Web Services Management Console.

kms>Delete*

Allows [kms>DeleteAlias](#). For keys with imported key material, it allows [kms>DeleteImportedKeyMaterial](#). The [kms>Delete*](#) permission does not allow key administrators to delete the KMS key ([ScheduleKeyDeletion](#)).

kms:TagResource

Allows [kms:TagResource](#), which allows key administrators to add tags to the KMS key. Because tags can also be used to control access to the KMS key, this permission can allow administrators to allow or deny access to the KMS key. For details, see [ABAC for Amazon KMS](#).

kms:UntagResource

Allows [kms:UntagResource](#), which allows key administrators to delete tags from the KMS key. Because tags can be used to control access to the key, this permission can allow administrators to allow or deny access to the KMS key. For details, see [ABAC for Amazon KMS](#).

kms:ScheduleKeyDeletion

Allows [kms:ScheduleKeyDeletion](#), which allows key administrators to [delete this KMS key](#). To delete this permission, clear the **Allow key administrators to delete this key** option.

kms:CancelKeyDeletion

Allows [kms:CancelKeyDeletion](#), which allows key administrators to [cancel deletion of this KMS key](#). To delete this permission, clear the **Allow key administrators to delete this key** option.

kms:RotateKeyOnDemand

Allows [kms:RotateKeyOnDemand](#), which allows key administrators to [perform on-demand rotation of the key material in this KMS key](#).

Amazon KMS adds the following permissions to the default key administrators statement when you create special-purpose keys.

kms:ImportKeyMaterial

The [kms:ImportKeyMaterial](#) permission allows key administrators to import key material into the KMS key. This permission is included in the key policy only when you [create a KMS key with no key material](#).

kms:ReplicateKey

The [kms:ReplicateKey](#) permission allows key administrators to [create a replica of a multi-Region primary key](#) in a different Amazon Region. This permission is included in the key policy only when you create a multi-Region primary or replica key.

kms:UpdatePrimaryRegion

The [kms:UpdatePrimaryRegion](#) permission allows key administrators to [change a multi-Region replica key to a multi-Region primary key](#). This permission is included in the key policy only when you create a multi-Region primary or replica key.

Allows key users to use the KMS key

The default key policy that the console creates for KMS keys allows you to choose IAM users and IAM roles in the account, and external Amazon Web Services accounts, and make them *key users*.

The console adds two policy statements to the key policy for key users.


- [Use the KMS key directly](#) — The first key policy statement gives key users permission to use the KMS key directly for all supported [cryptographic operations](#) for that type of KMS key.
- [Use the KMS key with Amazon services](#) — The second policy statement gives key users permission to allow Amazon services that are integrated with Amazon KMS to use the KMS key on their behalf to protect resources, such as Amazon S3 buckets and Amazon DynamoDB tables.

You can add IAM users, IAM roles, and other Amazon Web Services accounts to the list of key users when you create the KMS key. You can also edit the list with the console's default view for key policies, as shown in the following image. The default view for key policies is on the key details page. For more information about allowing users in other Amazon Web Services accounts to use the KMS key, see [Allowing users in other accounts to use a KMS key](#).

Note

IAM best practices discourage the use of IAM users with long-term credentials. Whenever possible, use IAM roles, which provide temporary credentials. For details, see [Security best practices in IAM](#) in the *IAM User Guide*.

Key users

The following IAM users and roles can use this key for cryptographic operations. They can also allow Amazon services that are integrated with KMS to use the key on their behalf. [Learn more](#) 

< 1 >

<input type="checkbox"/>	Name	Path	Type
<input type="checkbox"/>	ExampleUser	/	User
<input type="checkbox"/>	ExampleRole	/	Role

Other Amazon accounts

- arn:aws:iam::444455556666:root

The default *key users statements* for a single-Region symmetric allows the following permissions. For detailed information about each permission, see the [Amazon KMS permissions](#).

When you use the Amazon KMS console to create a KMS key, the console adds the users and roles you specify to the `Principal` element in each key users statement.

Note

The Amazon KMS console adds key users to the key policy under the statement identifiers "Allow use of the key" and "Allow attachment of persistent resources". Modifying these statement identifiers might impact how the console displays updates that you make to the statement.

```
{
  "Sid": "Allow use of the key",
  "Effect": "Allow",
```

```

"Principal": {"AWS": [
  "arn:aws:iam::111122223333:role/ExampleRole",
  "arn:aws:iam::444455556666:root"
]},
"Action": [
  "kms:Encrypt",
  "kms:Decrypt",
  "kms:ReEncrypt*",
  "kms:GenerateDataKey*",
  "kms:DescribeKey"
],
"Resource": "*"
},
{
  "Sid": "Allow attachment of persistent resources",
  "Effect": "Allow",
  "Principal": {"AWS": [
    "arn:aws:iam::111122223333:role/ExampleRole",
    "arn:aws:iam::444455556666:root"
  ]},
  "Action": [
    "kms:CreateGrant",
    "kms:ListGrants",
    "kms:RevokeGrant"
  ],
  "Resource": "*",
  "Condition": {"Bool": {"kms:GrantIsForAWSResource": true}}
}

```

Allows key users to use a KMS key for cryptographic operations

Key users have permission to use the KMS key directly in all [cryptographic operations](#) supported on the KMS key. They can also use the [DescribeKey](#) operation to get detailed information about the KMS key in the Amazon KMS console or by using the Amazon KMS API operations.

By default, the Amazon KMS console adds key users statements like those in the following examples to the default key policy. Because they support different API operations, the actions in the policy statements for symmetric encryption KMS keys, HMAC KMS keys, asymmetric KMS keys for public key encryption, and asymmetric KMS keys for signing and verification are slightly different.

Symmetric encryption KMS keys

The console adds the following statement to the key policy for symmetric encryption KMS keys.

```
{
  "Sid": "Allow use of the key",
  "Effect": "Allow",
  "Principal": {"AWS": "arn:aws:iam::111122223333:role/ExampleKeyUserRole"},
  "Action": [
    "kms:Decrypt",
    "kms:DescribeKey",
    "kms:Encrypt",
    "kms:GenerateDataKey*",
    "kms:ReEncrypt*"
  ],
  "Resource": "*"
}
```

HMAC KMS keys

The console adds the following statement to the key policy for HMAC KMS keys.

```
{
  "Sid": "Allow use of the key",
  "Effect": "Allow",
  "Principal": {"AWS": "arn:aws:iam::111122223333:role/ExampleKeyUserRole"},
  "Action": [
    "kms:DescribeKey",
    "kms:GenerateMac",
    "kms:VerifyMac"
  ],
  "Resource": "*"
}
```

Asymmetric KMS keys for public key encryption

The console adds the following statement to the key policy for asymmetric KMS keys with a key usage of **Encrypt and decrypt**.

```
{
  "Sid": "Allow use of the key",
  "Effect": "Allow",
  "Principal": {
```

```

    "AWS": "arn:aws:iam::111122223333:role/ExampleKeyUserRole"
  },
  "Action": [
    "kms:Encrypt",
    "kms:Decrypt",
    "kms:ReEncrypt*",
    "kms:DescribeKey",
    "kms:GetPublicKey"
  ],
  "Resource": "*"
}

```

Asymmetric KMS keys for signing and verification

The console adds the following statement to the key policy for asymmetric KMS keys with a key usage of **Sign and verify**.

```

{
  "Sid": "Allow use of the key",
  "Effect": "Allow",
  "Principal": {"AWS": "arn:aws:iam::111122223333:role/ExampleKeyUserRole"},
  "Action": [
    "kms:DescribeKey",
    "kms:GetPublicKey",
    "kms:Sign",
    "kms:Verify"
  ],
  "Resource": "*"
}

```

Asymmetric KMS keys for deriving shared secrets

The console adds the following statement to the key policy for asymmetric KMS keys with a key usage of **Key agreement**.

```

{
  "Sid": "Allow use of the key",
  "Effect": "Allow",
  "Principal": {"AWS": "arn:aws:iam::111122223333:role/ExampleKeyUserRole"},
  "Action": [
    "kms:DescribeKey",
    "kms:GetPublicKey",
    "kms:DeriveSharedSecret"
  ]
}

```



```
],  
  "Resource": "*" }  
}
```

The actions in these statements give the key users the following permissions.

[kms:Encrypt](#)

Allows key users to encrypt data with this KMS key.

[kms:Decrypt](#)

Allows key users to decrypt data with this KMS key.

[kms:DeriveSharedSecret](#)

Allows key users to derive shared secrets with this KMS key.

[kms:DescribeKey](#)

Allows key users to get detailed information about this KMS key including its identifiers, creation date, and key state. It also allows the key users to display details about the KMS key in the Amazon KMS console.

kms:GenerateDataKey*

Allows key users to request a symmetric data key or an asymmetric data key pair for client-side cryptographic operations. The console uses the * wildcard character to represent permission for the following API operations: [GenerateDataKey](#), [GenerateDataKeyWithoutPlaintext](#), [GenerateDataKeyPair](#), and [GenerateDataKeyPairWithoutPlaintext](#). These permissions are valid only on the symmetric KMS keys that encrypt the data keys.

[kms:GenerateMac](#)

Allows key users to use an HMAC KMS key to generate an HMAC tag.

[kms:GetPublicKey](#)

Allows key users to download the public key of the asymmetric KMS key. Parties with whom you share this public key can encrypt data outside of Amazon KMS. However, those ciphertexts can be decrypted only by calling the [Decrypt](#) operation in Amazon KMS.

[kms:ReEncrypt*](#)

Allows key users to re-encrypt data that was originally encrypted with this KMS key, or to use this KMS key to re-encrypt previously encrypted data. The [ReEncrypt](#) operation requires

access to both source and destination KMS keys. To accomplish this, you can allow the `kms:ReEncryptFrom` permission on the source KMS key and `kms:ReEncryptTo` permission on the destination KMS key. However, for simplicity, the console allows `kms:ReEncrypt*` (with the `*` wildcard character) on both KMS keys.

[kms:Sign](#)

Allows key users to sign messages with this KMS key.

[kms:Verify](#)

Allows key users to verify signatures with this KMS key.

[kms:VerifyMac](#)

Allows key users to use an HMAC KMS key to verify an HMAC tag.

Allows key users to use the KMS key with Amazon services

The default key policy in the console also gives key users the grant permissions they need to protect their data in Amazon services that use grants. Amazon services often use grants to get specific and limited permission to use a KMS key.

This key policy statement allows the key user to create, view, and revoke grants on the KMS key, but only when the grant operation request comes from an [Amazon service integrated with Amazon KMS](#). The [kms:GrantIsForAWSResource](#) policy condition doesn't allow the user to call these grant operations directly. When the key user allows it, an Amazon service can create a grant on the user's behalf that allows the service to use the KMS key to protect the user's data.

Key users require these grant permissions to use their KMS key with integrated services, but these permissions are not sufficient. Key users also need permission to use the integrated services. For details about giving users access to an Amazon service that integrates with Amazon KMS, consult the documentation for the integrated service.

```
{
  "Sid": "Allow attachment of persistent resources",
  "Effect": "Allow",
  "Principal": {"AWS": "arn:aws:iam::111122223333:role/ExampleKeyUserRole"},
  "Action": [
    "kms:CreateGrant",
    "kms:ListGrants",
    "kms:RevokeGrant"
  ],
}
```

```
"Resource": "*",
"Condition": {"Bool": {"kms:GrantIsForAWSResource": true}}
}
```

For example, key users can use these permissions on the KMS key in the following ways.

- Use this KMS key with Amazon Elastic Block Store (Amazon EBS) and Amazon Elastic Compute Cloud (Amazon EC2) to attach an encrypted EBS volume to an EC2 instance. The key user implicitly gives Amazon EC2 permission to use the KMS key to attach the encrypted volume to the instance. For more information, see [How Amazon Elastic Block Store \(Amazon EBS\) uses Amazon KMS](#).
- Use this KMS key with Amazon Redshift to launch an encrypted cluster. The key user implicitly gives Amazon Redshift permission to use the KMS key to launch the encrypted cluster and create encrypted snapshots. For more information, see [How Amazon Redshift uses Amazon KMS](#).
- Use this KMS key with other [Amazon services integrated with Amazon KMS](#) that use grants to create, manage, or use encrypted resources with those services.

The default key policy allows key users to delegate their grant permission to *all* integrated services that use grants. However, you can create a custom key policy that restricts the permission to specified Amazon services. For more information, see the [kms:ViaService](#) condition key.

View a key policies

You can view the key policy for an Amazon KMS [customer managed key](#) or an [Amazon managed key](#) in your account by using the Amazon KMS console or the [GetKeyPolicy](#) operation in the Amazon KMS API. You cannot use these techniques to view the key policy of a KMS key in a different Amazon Web Services account.

To learn more about Amazon KMS key policies, see [Key policies in Amazon KMS](#). To learn how to determine which users and roles have access to a KMS key, see [the section called “Determining access”](#).

Using the Amazon KMS console

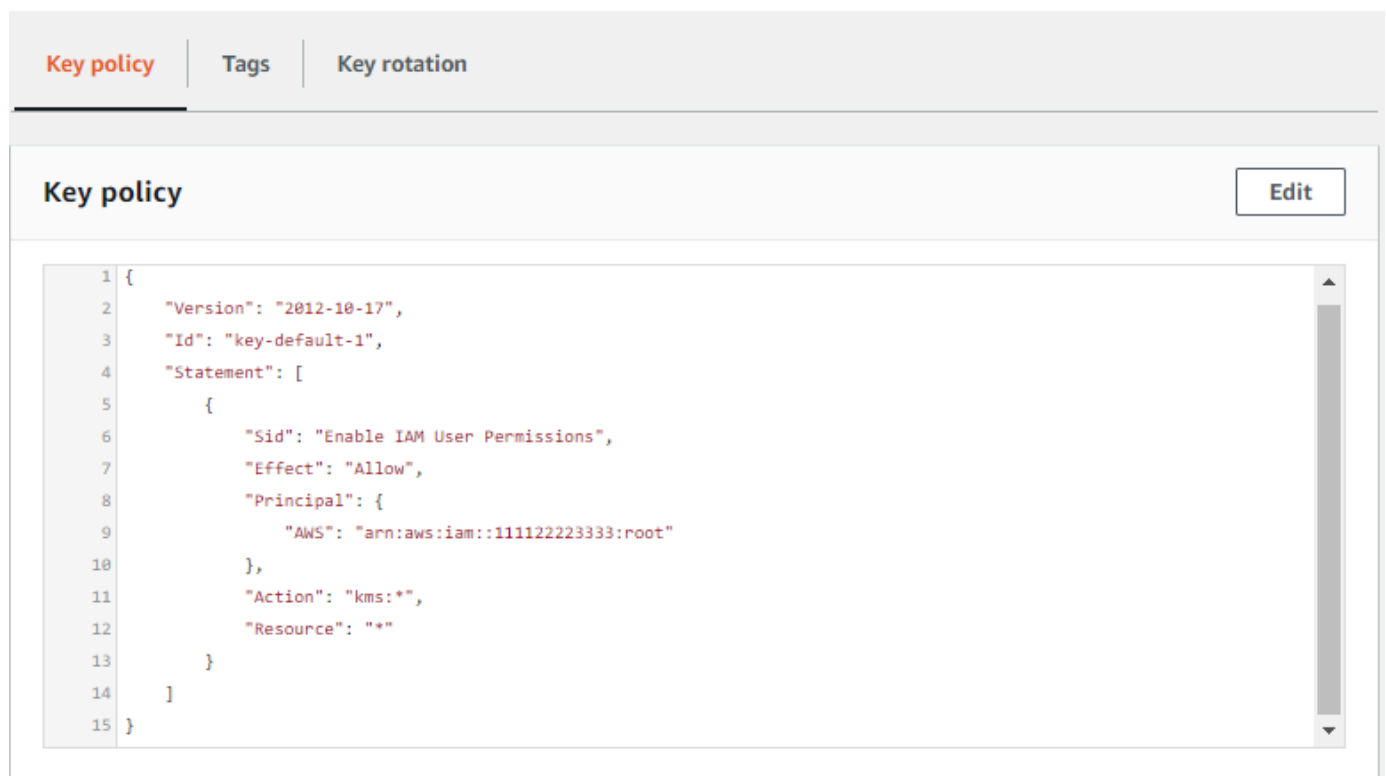
Authorized users can view the key policy for an [Amazon managed key](#) or a [customer managed key](#) on the **Key policy** tab of the Amazon Web Services Management Console.

To view the key policy for a KMS key in the Amazon Web Services Management Console, you must have [kms:ListAliases](#), [kms:DescribeKey](#), and [kms:GetKeyPolicy](#) permissions.

1. Sign in to the Amazon Web Services Management Console and open the Amazon Key Management Service (Amazon KMS) console at <https://console.amazonaws.cn/kms>.
2. To change the Amazon Web Services Region, use the Region selector in the upper-right corner of the page.
3. To view the keys in your account that Amazon creates and manages for you, in the navigation pane, choose **Amazon managed keys**. To view the keys in your account that you create and manage, in the navigation pane choose **Customer managed keys**.
4. In the list of KMS keys, choose the alias or key ID of the KMS key that you want to examine.
5. Choose the **Key policy** tab.

On the **Key policy** tab, you might see the key policy document. This is *policy view*. In the key policy statements, you can see the principals who have been given access to the KMS key by the key policy, and you can see the actions they can perform.

The following example shows the policy view for the [default key policy](#).



The screenshot shows the Amazon KMS console interface. At the top, there are three tabs: "Key policy" (selected), "Tags", and "Key rotation". Below the tabs, the "Key policy" section is visible, with an "Edit" button in the top right corner. The main content area displays a JSON policy document in a code editor with line numbers 1 through 15. The policy document is as follows:

```
1 {
2   "Version": "2012-10-17",
3   "Id": "key-default-1",
4   "Statement": [
5     {
6       "Sid": "Enable IAM User Permissions",
7       "Effect": "Allow",
8       "Principal": {
9         "AWS": "arn:aws:iam::111122223333:root"
10      },
11       "Action": "kms:*",
12       "Resource": "*"
13     }
14   ]
15 }
```

Or, if you created the KMS key in the Amazon Web Services Management Console, you will see the *default view* with sections for **Key administrators**, **Key deletion**, and **Key Users**. To see the key policy document, choose **Switch to policy view**.

The following example shows the default view for the [default key policy](#).

The screenshot displays the Amazon KMS console interface for a key policy. At the top, there are three tabs: 'Key policy' (selected), 'Tags', and 'Key rotation'. Below the tabs, the 'Key policy' section is visible, featuring a 'Switch to policy view' button. The 'Key administrators' section includes a description, 'Add' and 'Remove' buttons, a search bar, and a table with columns for Name, Path, and Type. The table is currently empty, displaying 'Empty Resources' and 'No resources to display'. The 'Key deletion' section has a checkbox labeled 'Allow key administrators to delete this key'. The 'Key users' section also includes a description, 'Add' and 'Remove' buttons, a search bar, and a table with columns for Name, Path, and Type, which is also empty.

Using the Amazon KMS API

To get the key policy for a KMS key in your Amazon Web Services account, use the [GetKeyPolicy](#) operation in the Amazon KMS API. You cannot use this operation to view a key policy in a different account.

The following example uses the [get-key-policy](#) command in the Amazon Command Line Interface (Amazon CLI), but you can use any Amazon SDK to make this request.

Note that the `PolicyName` parameter is required even though `default` is its only valid value. Also, this command requests the output in text, rather than JSON, to make it easier to view.

Before running this command, replace the example key ID with a valid one from your account.

```
$ aws kms get-key-policy --key-id 1234abcd-12ab-34cd-56ef-1234567890ab --policy-name default --output text
```

The response should be similar to the following one, which returns the [default key policy](#).

```
{
  "Version" : "2012-10-17",
  "Id" : "key-consolepolicy-3",
  "Statement" : [ {
    "Sid" : "Enable IAM User Permissions",
    "Effect" : "Allow",
    "Principal" : {
      "AWS" : "arn:aws:iam::111122223333:root"
    },
    "Action" : "kms:*",
    "Resource" : "*"
  } ]
}
```

Change a key policy

You can change the key policy for a KMS key in your Amazon Web Services account by using the Amazon Web Services Management Console or the [PutKeyPolicy](#) operation. You cannot use these techniques to change the key policy of a KMS key in a different Amazon Web Services account.

When changing a key policy, keep in mind the following rules:

- You can view the key policy for an [Amazon managed key](#) or a [customer managed key](#), but you can only change the key policy for a customer managed key. The policies of Amazon managed keys are created and managed by the Amazon service that created the KMS key in your account. You cannot view or change the key policy for an [Amazon owned key](#).

- You can add or remove IAM users, IAM roles, and Amazon Web Services accounts in the key policy, and change the actions that are allowed or denied for those principals. For more information about the ways to specify principals and permissions in a key policy, see [Key policies](#).
- You cannot add IAM groups to a key policy, but you can add multiple IAM users and IAM roles. For more information, see [Allowing multiple IAM principals to access a KMS key](#).
- If you add external Amazon Web Services accounts to a key policy, you must also use IAM policies in the external accounts to give permissions to IAM users, groups, or roles in those accounts. For more information, see [Allowing users in other accounts to use a KMS key](#).
- The resulting key policy document cannot exceed 32 KB (32,768 bytes).

How to change a key policy

You can change a key policy in three different ways as explained in the following sections.

Topics

- [Using the Amazon Web Services Management Console default view](#)
- [Using the Amazon Web Services Management Console policy view](#)
- [Using the Amazon KMS API](#)

Using the Amazon Web Services Management Console default view

You can use the console to change a key policy with a graphical interface called the *default view*.

If the following steps don't match what you see in the console, it might mean that this key policy was not created by the console. Or it might mean that the key policy has been modified in a way that the console's default view does not support. In that case, follow the steps at [Using the Amazon Web Services Management Console policy view](#) or [Using the Amazon KMS API](#).

1. View the key policy for a customer managed key as described in [Using the Amazon KMS console](#). (You cannot change the key policies of Amazon managed keys.)
2. Decide what to change.
 - To add or remove [key administrators](#), and to allow or prevent key administrators from [deleting the KMS key](#), use the controls in the **Key administrators** section of the page. Key administrators manage the KMS key, including enabling and disabling it, setting key policy, and [enabling key rotation](#).

- To add or remove [key users](#), and to allow or disallow external Amazon Web Services accounts to use the KMS key, use the controls in the **Key users** section of the page. Key users can use the KMS key in [cryptographic operations](#), such as encrypting, decrypting, re-encrypting, and generating data keys.

Using the Amazon Web Services Management Console policy view

You can use the console to change a key policy document with the console's *policy view*.

1. View the key policy for a customer managed key as described in [Using the Amazon KMS console](#). (You cannot change the key policies of Amazon managed keys.)
2. In the **Key Policy** section, choose **Switch to policy view**.
3. Choose **Edit**.
4. Decide what to change.
 - To add a new statement, choose **Add new statement**. Then, you can select the actions, principals, and conditions for your new key policy statement from the options listed in the statement builder panel, or manually enter the policy statement elements.
 - To remove a statement from your key policy, select the statement and then choose **Remove**. Review the selected policy statement and confirm that you want to remove it. If you decide that you do not want to proceed with removing the statement, choose **Cancel**.
 - To edit an existing key policy statement, select the statement. Then, you can use the statement builder panel to choose specific elements that you want to modify, or manually edit the statement.
5. Choose **Save changes**.

Using the Amazon KMS API

You can use the [PutKeyPolicy](#) operation to change the key policy of a KMS key in your Amazon Web Services account. You cannot use this API on a KMS key in a different Amazon Web Services account.

1. Use the [GetKeyPolicy](#) operation to get the existing key policy document, and then save the key policy document to a file. For sample code in multiple programming languages, see [Use GetKeyPolicy with an Amazon SDK or CLI](#).

2. Open the key policy document in your preferred text editor, edit the key policy document, and then save the file.
3. Use the [PutKeyPolicy](#) operation to apply the updated key policy document to the KMS key. For sample code in multiple programming languages, see [Use PutKeyPolicy with an Amazon SDK or CLI](#).

For an example of copying a key policy from one KMS key to another, see the [GetKeyPolicy example](#) in the Amazon CLI Command Reference.

Permissions for Amazon services in key policies

Many Amazon services use Amazon KMS keys to protect the resources they manage. When a service uses [Amazon owned keys](#) or [Amazon managed keys](#), the service establishes and maintains the key policies for these KMS keys.

However, when you use a [customer managed key](#) with an Amazon service, you set and maintain the key policy. That key policy must allow the service the minimum permissions that it requires to protect the resource on your behalf. We recommend that you follow the principle of least privilege: give the service only the permissions that it requires. You can do this effectively by learning which permissions the service needs and using [Amazon global condition keys](#) and [Amazon KMS condition keys](#) to refine the permissions.

To find the permissions that the service requires on a customer managed key, see the encryption documentation for the service. For example, for the permissions that Amazon Elastic Block Store (Amazon EBS) requires, see *Permissions for IAM users* in the [Amazon EC2 User Guide](#) and [Amazon EC2 User Guide](#). For the permissions that Secrets Manager requires, see [Authorizing use of the KMS key](#) in the *Amazon Secrets Manager User Guide*.

Using IAM policies with Amazon KMS

You can use IAM policies, along with [key policies](#), [grants](#), and [VPC endpoint policies](#), to control access to your Amazon KMS keys in Amazon KMS.

Note

To use an IAM policy to control access to a KMS key, the key policy for the KMS key must give the account permission to use IAM policies. Specifically, the key policy must include the [policy statement that enables IAM policies](#).

This section explains how to use IAM policies to control access to Amazon KMS operations. For more general information about IAM, see the [IAM User Guide](#).

All KMS keys must have a key policy. IAM policies are optional. To use an IAM policy to control access to a KMS key, the key policy for the KMS key must give the account permission to use IAM policies. Specifically, the key policy must include the [policy statement that enables IAM policies](#).

IAM policies can control access to any Amazon KMS operation. Unlike key policies, IAM policies can control access to multiple KMS keys and provide permissions for the operations of several related Amazon services. But IAM policies are particularly useful for controlling access to operations, such as [CreateKey](#), that can't be controlled by a key policy because they don't involve any particular KMS key.

If you access Amazon KMS through an Amazon Virtual Private Cloud (Amazon VPC) endpoint, you can also use a VPC endpoint policy to limit access to your Amazon KMS resources when using the endpoint. For example, when using the VPC endpoint, you might only allow the principals in your Amazon Web Services account to access your customer managed keys. For details, see [VPC endpoint policies](#).

For help writing and formatting a JSON policy document, see the [IAM JSON Policy Reference](#) in the *IAM User Guide*.

You can use IAM policies in the following ways:

- **Attach a permissions policy to a role for federation or cross-account permissions** – You can attach an IAM policy to an IAM role to enable identity federation, allow cross-account permissions, or give permissions to applications running on EC2 instances. For more information about the various use cases for IAM roles, see [IAM Roles](#) in the *IAM User Guide*.
- **Attach a permissions policy to a user or a group** – You can attach a policy that allows a user or group of users to call Amazon KMS operations. However, IAM best practices recommend that you use identities with temporary credentials, such as IAM roles, whenever possible.

The following example shows an IAM policy with Amazon KMS permissions. This policy allows the IAM identities to which it is attached to list all KMS keys and aliases.

```
{  
  "Version": "2012-10-17",
```

```
"Statement": {
  "Effect": "Allow",
  "Action": [
    "kms:ListKeys",
    "kms:ListAliases"
  ],
  "Resource": "*"
}
```

Like all IAM policies, this policy doesn't have a `Principal` element. When you attach an IAM policy to an IAM identity, that identity gets the permissions specified in the policy.

For a table showing all of the Amazon KMS API actions and the resources that they apply to, see the [Permissions reference](#).

Allowing multiple IAM principals to access a KMS key

IAM groups are not valid principals in a key policy. To allow multiple users and roles to access a KMS key, do one of the following:

- Use an IAM role as the principal in the key policy. Multiple authorized users can assume the role as needed. For details, see [IAM roles](#) in the *IAM User Guide*.

While you can list multiple IAM users in a key policy, this practice is not recommended because it requires that you update the key policy every time the list of authorized users changes. Also, IAM best practices discourage the use of IAM users with long-term credentials. For details, see [Security best practices in IAM](#) in the *IAM User Guide*.

- Use an IAM policy to give permission to an IAM group. To do this, ensure that the key policy includes the statement that [enables IAM policies to allow access to the KMS key](#), [create an IAM policy](#) that allows access to the KMS key, and then [attach that policy to an IAM group](#) that contains the authorized IAM users. Using this approach, you don't need to change any policies when the list of authorized users changes. Instead, you only need to add or remove those users from the appropriate IAM group. For details, see [IAM user groups](#) in the *IAM User Guide*

For more information about how Amazon KMS key policies and IAM policies work together, see [Troubleshooting Amazon KMS permissions](#).

Best practices for IAM policies

Securing access to Amazon KMS keys is critical to the security of all of your Amazon resources. KMS keys are used to protect many of the most sensitive resources in your Amazon Web Services account. Take the time to design the [key policies](#), IAM policies, [grants](#), and VPC endpoint policies that control access to your KMS keys.

In IAM policy statements that control access to KMS keys, use the [least privileged principle](#). Give IAM principals only the permissions they need on only the KMS keys they must use or manage.

The following best practices apply to IAM policies that control access to Amazon KMS keys and aliases. For general IAM policy best practice guidance, see [Security best practices in IAM](#) in the *IAM User Guide*.

Use key policies

Whenever possible, provide permissions in key policies that affect one KMS key, rather than in an IAM policy that can apply to many KMS keys, including those in other Amazon Web Services accounts. This is particularly important for sensitive permissions like [kms:PutKeyPolicy](#) and [kms:ScheduleKeyDeletion](#) but also for cryptographic operations that determine how your data is protected.

Limit CreateKey permission

Give permission to create keys ([kms:CreateKey](#)) only to principals who need it. Principals who create a KMS key also set its key policy, so they can give themselves and others permission to use and manage the KMS keys they create. When you allow this permission, consider limiting it by using [policy conditions](#). For example, you can use the [kms:KeySpec](#) condition to limit the permission to symmetric encryption KMS keys.

Specify KMS keys in an IAM policy

As a best practice, specify the [key ARN](#) of each KMS key to which the permission applies in the Resource element of the policy statement. This practice restricts the permission to the KMS keys that principal requires. For example, this Resource element lists only the KMS keys the principal needs to use.

```
"Resource": [  
  "arn:aws:kms:us-west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab",  
  "arn:aws:kms:us-west-2:111122223333:key/0987dcba-09fe-87dc-65ba-ab0987654321"
```

]

When specifying KMS keys is impractical, use a Resource value that limits access to KMS keys in a trusted Amazon Web Services account and Region, such as `arn:aws:kms:region:account:key/*`. Or limit access to KMS keys in all Regions (*) of a trusted Amazon Web Services account, such as `arn:aws:kms:*:account:key/*`.

You cannot use a [key ID](#), [alias name](#), or [alias ARN](#) to represent a KMS key in the Resource field of an IAM policy. If you specify an alias ARN, the policy applies to the alias, not to the KMS key. For information about IAM policies for aliases, see [Controlling access to aliases](#)

Avoid "Resource": "*" in an IAM policy

Use wildcard characters (*) judiciously. In a key policy, the wildcard character in the Resource element represents the KMS key to which the key policy is attached. But in an IAM policy, a wildcard character alone in the Resource element ("Resource": "*") applies the permissions to all KMS keys in all Amazon Web Services accounts that the principal's account has permission to use. This might include [KMS keys in other Amazon Web Services accounts](#), as well as KMS keys in the principal's account.

For example, to use a KMS key in another Amazon Web Services account, a principal needs permission from the key policy of the KMS key in the external account, and from an IAM policy in their own account. Suppose that an arbitrary account gave your Amazon Web Services account `kms:Decrypt` permission on their KMS keys. If so, an IAM policy in your account that gives a role `kms:Decrypt` permission on all KMS keys ("Resource": "*") would satisfy the IAM part of the requirement. As a result, principals who can assume that role can now decrypt ciphertexts using the KMS key in the untrusted account. Entries for their operations appear in the CloudTrail logs of both accounts.

In particular, avoid using "Resource": "*" in a policy statement that allows the following API operations. These operations can be called on KMS keys in other Amazon Web Services accounts.

- [DescribeKey](#)
- [GetKeyRotationStatus](#)
- [Cryptographic operations](#) ([Encrypt](#), [Decrypt](#), [GenerateDataKey](#), [GenerateDataKeyPair](#), [GenerateDataKeyWithoutPlaintext](#), [GenerateDataKeyPairWithoutPlaintext](#), [GetPublicKey](#), [ReEncrypt](#), [Sign](#), [Verify](#))
- [CreateGrant](#), [ListGrants](#), [ListRetirableGrants](#), [RetireGrant](#), [RevokeGrant](#)

When to use "Resource": "*"

In an IAM policy, use a wildcard character in the Resource element only for permissions that require it. Only the following permissions require the "Resource": "*" element.

- [kms:CreateKey](#)
- [kms:GenerateRandom](#)
- [kms:ListAliases](#)
- [kms:ListKeys](#)
- Permissions for custom key stores, such as [kms:CreateCustomKeyStore](#) and [kms:ConnectCustomKeyStore](#).

Note

Permissions for alias operations ([kms:CreateAlias](#), [kms:UpdateAlias](#), [kms>DeleteAlias](#)) must be attached to the alias and the KMS key. You can use "Resource": "*" in an IAM policy to represent the aliases and the KMS keys, or specify the aliases and KMS keys in the Resource element. For examples, see [Controlling access to aliases](#).

The examples in this topic provide more information and guidance for designing IAM policies for KMS keys. For IAM best practices for all Amazon resources, see [Security best practices in IAM](#) in the *IAM User Guide*.

Specifying KMS keys in IAM policy statements

You can use an IAM policy to allow a principal to use or manage KMS keys. KMS keys are specified in the Resource element of the policy statement.

- To specify a KMS key in an IAM policy statement, you must use its [key ARN](#). You cannot use a [key id](#), [alias name](#), or [alias ARN](#) to identify a KMS key in an IAM policy statement.

For example: "Resource": "arn:aws:kms:us-west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab"

To control access to a KMS key based on its aliases, use the [kms:RequestAlias](#) or [kms:ResourceAliases](#) condition keys. For details, see [ABAC for Amazon KMS](#).

Use an alias ARN as the resource only in a policy statement that controls access to alias operations, such as [CreateAlias](#), [UpdateAlias](#), or [DeleteAlias](#). For details, see [Controlling access to aliases](#).

- To specify multiple KMS keys in the account and Region, use wildcard characters (*) in the Region or resource ID positions of the key ARN.

For example, to specify all KMS keys in the US West (Oregon) Region of an account, use "Resource": "arn:aws:kms:us-west-2:111122223333:key/*". To specify all KMS keys in all Regions of the account, use "Resource": "arn:aws:kms:*:111122223333:key/*".

- To represent all KMS keys, use a wildcard character alone ("*"). Use this format for operations that don't use any particular KMS key, namely [CreateKey](#), [GenerateRandom](#), [ListAliases](#), and [ListKeys](#).

When writing your policy statements, it's a [best practice](#) to specify only the KMS keys that the principal needs to use, rather than giving them access to all KMS keys.

For example, the following IAM policy statement allows the principal to call the [DescribeKey](#), [GenerateDataKey](#), [Decrypt](#) operations only on the KMS keys listed in the Resource element of the policy statement. Specifying KMS keys by key ARN, which is a best practice, ensures that the permissions are limited only to the specified KMS keys.

```
{
  "Version": "2012-10-17",
  "Statement": {
    "Effect": "Allow",
    "Action": [
      "kms:DescribeKey",
      "kms:GenerateDataKey",
      "kms:Decrypt"
    ],
    "Resource": [
      "arn:aws:kms:us-west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab",
      "arn:aws:kms:us-west-2:111122223333:key/0987dcba-09fe-87dc-65ba-ab0987654321"
    ]
  }
}
```

To apply the permission to all KMS keys in a particular trusted Amazon Web Services account, you can use wildcard characters (*) in the Region and key ID positions. For example, the following policy statement allows the principal to call the specified operations on all KMS keys in two trusted example accounts.

```
{
  "Version": "2012-10-17",
  "Statement": {
    "Effect": "Allow",
    "Action": [
      "kms:DescribeKey",
      "kms:GenerateDataKey",
      "kms:GenerateDataKeyPair"
    ],
    "Resource": [
      "arn:aws:kms:*:111122223333:key/*",
      "arn:aws:kms:*:444455556666:key/*"
    ]
  }
}
```

You can also use a wildcard character ("*") alone in the Resource element. Because it allows access to all KMS keys the account has permission to use, it's recommended primarily for operations without a particular KMS key and for Deny statements. You can also use it in policy statements that allow only less sensitive read-only operations. To determine whether an Amazon KMS operation involves a particular KMS key, look for the **KMS key** value in the **Resources** column of the table in [the section called "Permissions reference"](#).

For example, the following policy statement uses a Deny effect to prohibit the principals from using the specified operations on any KMS key. It uses a wildcard character in the Resource element to represent all KMS keys.

```
{
  "Version": "2012-10-17",
  "Statement": {
    "Effect": "Deny",
    "Action": [
      "kms:CreateKey",
      "kms:PutKeyPolicy",
      "kms:CreateGrant",
      "kms:ScheduleKeyDeletion"
    ]
  }
}
```



```
    ],  
    "Resource": "*"    
  }  
}
```

The following policy statement uses a wildcard character alone to represent all KMS keys. But it allows only less sensitive read-only operations and operations that don't apply to any particular KMS key.

```
{  
  "Version": "2012-10-17",  
  "Statement": [  
    {  
      "Effect": "Allow",  
      "Action": [  
        "kms:CreateKey",  
        "kms:ListKeys",  
        "kms:ListAliases",  
        "kms:ListResourceTags"  
      ],  
      "Resource": "*"    
    }  
  ]  
}
```

IAM policy examples

In this section, you can find example IAM policies that allow permissions for various Amazon KMS actions.

Important

Some of the permissions in the following policies are allowed only when the KMS key's key policy also allows them. For more information, see [Permissions reference](#).

For help writing and formatting a JSON policy document, see the [IAM JSON Policy Reference](#) in the *IAM User Guide*.

Examples

- [Allow a user to view KMS keys in the Amazon KMS console](#)
- [Allow a user to create KMS keys](#)

- [Allow a user to encrypt and decrypt with any KMS key in a specific Amazon Web Services account](#)
- [Allow a user to encrypt and decrypt with any KMS key in a specific Amazon Web Services account and Region](#)
- [Allow a user to encrypt and decrypt with specific KMS keys](#)
- [Prevent a user from disabling or deleting any KMS keys](#)

Allow a user to view KMS keys in the Amazon KMS console

The following IAM policy allows users read-only access to the Amazon KMS console. Users with these permissions can view all KMS keys in their Amazon Web Services account, but they cannot create or change any KMS keys.

To view KMS keys on the **Amazon managed keys** and **Customer managed keys** pages, principals require [kms:ListKeys](#), [kms:ListAliases](#), and [tag:GetResources](#) permissions, even if the keys do not have tags or aliases. The remaining permissions, particularly [kms:DescribeKey](#), are required to view optional KMS key table columns and data on the KMS key detail pages. The [iam:ListUsers](#) and [iam:ListRoles](#) permissions are required to display the key policy in default view without error. To view data on the **Custom key stores** page and details about KMS keys in custom key stores, principals also need [kms:DescribeCustomKeyStores](#) permission.

If you limit a user's console access to particular KMS keys, the console displays an error for each KMS key that is not visible.

This policy includes of two policy statements. The Resource element in the first policy statement allows the specified permissions on all KMS keys in all Regions of the example Amazon Web Services account. Console viewers don't need additional access because the Amazon KMS console displays only KMS keys in the principal's account. This is true even if they have permission to view KMS keys in other Amazon Web Services accounts. The remaining Amazon KMS and IAM permissions require a "Resource": "*" element because they don't apply to any particular KMS key.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "ReadOnlyAccessForAllKMSKeysInAccount",
      "Effect": "Allow",
      "Action": [
        "kms:GetPublicKey",
```

```

        "kms:GetKeyRotationStatus",
        "kms:GetKeyPolicy",
        "kms:DescribeKey",
        "kms:ListKeyPolicies",
        "kms:ListResourceTags",
        "tag:GetResources"
    ],
    "Resource": "arn:aws:kms:*:111122223333:key/*"
},
{
    "Sid": "ReadOnlyAccessForOperationsWithNoKMSKey",
    "Effect": "Allow",
    "Action": [
        "kms:ListKeys",
        "kms:ListAliases",
        "iam:ListRoles",
        "iam:ListUsers"
    ],
    "Resource": "*"
}
]
}

```

Allow a user to create KMS keys

The following IAM policy allows a user to create all types of KMS keys. The value of the Resource element is * because the CreateKey operation does not use any particular Amazon KMS resources (KMS keys or aliases).

To restrict the user to particular types of KMS keys, use the [kms:KeySpec](#), [kms:KeyUsage](#), and [kms:KeyOrigin](#) condition keys.

```

{
    "Version": "2012-10-17",
    "Statement": {
        "Effect": "Allow",
        "Action": "kms:CreateKey",
        "Resource": "*"
    }
}

```

Principals who create keys might need some related permissions.

- **kms:PutKeyPolicy** — Principals who have `kms:CreateKey` permission can set the initial key policy for the KMS key. However, the `CreateKey` caller must have [kms:PutKeyPolicy](#) permission, which lets them change the KMS key policy, or they must specify the `BypassPolicyLockoutSafetyCheck` parameter of `CreateKey`, which is not recommended. The `CreateKey` caller can get `kms:PutKeyPolicy` permission for the KMS key from an IAM policy or they can include this permission in the key policy of the KMS key that they're creating.
- **kms:TagResource** — To add tags to the KMS key during the `CreateKey` operation, the `CreateKey` caller must have [kms:TagResource](#) permission in an IAM policy. Including this permission in the key policy of the new KMS key isn't sufficient. However, if the `CreateKey` caller includes `kms:TagResource` in the initial key policy, they can add tags in a separate call after the KMS key is created.
- **kms:CreateAlias** — Principals who create a KMS key in the Amazon KMS console must have [kms:CreateAlias](#) permission on the KMS key and on the alias. (The console makes two calls; one to `CreateKey` and one to `CreateAlias`). You must provide the alias permission in an IAM policy. You can provide the KMS key permission in a key policy or IAM policy. For details, see [Controlling access to aliases](#).

In addition to `kms:CreateKey`, the following IAM policy provides `kms:TagResource` permission on all KMS keys in the Amazon Web Services account and `kms:CreateAlias` permission on all aliases that the account. It also includes some useful read-only permissions that can be provided only in an IAM policy.

This IAM policy does not include `kms:PutKeyPolicy` permission or any other permissions that can be set in a key policy. It's a [best practice](#) to set these permissions in the key policy where they apply exclusively to one KMS key.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "IAMPermissionsForParticularKMSKeys",
      "Effect": "Allow",
      "Action": "kms:TagResource",
      "Resource": "arn:aws:kms:*:111122223333:key/*"
    },
    {
      "Sid": "IAMPermissionsForParticularAliases",
      "Effect": "Allow",
```

```
    "Action": "kms:CreateAlias",
    "Resource": "arn:aws:kms:*:111122223333:alias/*"
  },
  {
    "Sid": "IAMPermissionsForAllKMSKeys",
    "Effect": "Allow",
    "Action": [
      "kms:CreateKey",
      "kms:ListKeys",
      "kms:ListAliases"
    ],
    "Resource": "*"
  }
]
```

Allow a user to encrypt and decrypt with any KMS key in a specific Amazon Web Services account

The following IAM policy allows a user to encrypt and decrypt data with any KMS key in Amazon Web Services account 111122223333.

```
{
  "Version": "2012-10-17",
  "Statement": {
    "Effect": "Allow",
    "Action": [
      "kms:Encrypt",
      "kms:Decrypt"
    ],
    "Resource": "arn:aws:kms:*:111122223333:key/*"
  }
}
```

Allow a user to encrypt and decrypt with any KMS key in a specific Amazon Web Services account and Region

The following IAM policy allows a user to encrypt and decrypt data with any KMS key in Amazon Web Services account 111122223333 in the US West (Oregon) Region.

```
{
```

```
"Version": "2012-10-17",
"Statement": {
  "Effect": "Allow",
  "Action": [
    "kms:Encrypt",
    "kms:Decrypt"
  ],
  "Resource": [
    "arn:aws:kms:us-west-2:111122223333:key/*"
  ]
}
```

Allow a user to encrypt and decrypt with specific KMS keys

The following IAM policy allows a user to encrypt and decrypt data with the two KMS keys specified in the Resource element. When specifying a KMS key in an IAM policy statement, you must use the [key ARN](#) of the KMS key.

```
{
  "Version": "2012-10-17",
  "Statement": {
    "Effect": "Allow",
    "Action": [
      "kms:Encrypt",
      "kms:Decrypt"
    ],
    "Resource": [
      "arn:aws:kms:us-west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab",
      "arn:aws:kms:us-west-2:111122223333:key/0987dcba-09fe-87dc-65ba-ab0987654321"
    ]
  }
}
```

Prevent a user from disabling or deleting any KMS keys

The following IAM policy prevents a user from disabling or deleting any KMS keys, even when another IAM policy or a key policy allows these permissions. A policy that explicitly denies permissions overrides all other policies, even those that explicitly allow the same permissions. For more information, see [Troubleshooting Amazon KMS permissions](#).

```
{
```

```
"Version": "2012-10-17",
"Statement": {
  "Effect": "Deny",
  "Action": [
    "kms:DisableKey",
    "kms:ScheduleKeyDeletion"
  ],
  "Resource": "*"
}
```

Resource control policies in Amazon KMS

Resource control policies (RCPs) are a type of organization policy that you can use to enforce preventive controls on Amazon resources in your organization. RCPs help you to centrally restrict external access to your Amazon resources at scale. RCPs complement service control policies (SCPs). While, SCPs can be used to centrally set the maximum permissions on the IAM roles and users in your organization, RCPs can be used to centrally set the maximum permissions on Amazon resources in your organization.

You can use RCPs to manage permissions to the customer managed KMS keys in your organization. RCPs alone are not sufficient in granting permissions to your customer managed keys. No permissions are granted by an RCP. An RCP defines a permissions guardrail, or sets limits, on the actions that identities can take on resources in the affected accounts. The administrator must still attach identity-based policies to IAM roles or users, or key policies to actually grant permissions.

Note

Resource control policies in your organization do not apply to [Amazon managed keys](#). Amazon managed keys are created, managed, and used on your behalf by an Amazon service, you cannot change or manage their permissions.

Learn more

- For more general information on RCPs, see [Resource control policies](#) in the *Amazon Organizations User Guide*.
- For details on how to define RCPs, including examples, see [RCP syntax](#) in the *Amazon Organizations User Guide*.

The following example demonstrates how to use an RCP to prevent external principals from accessing customer managed keys in your organization. This policy is just a sample, and you should tailor it to meet your unique business and security needs. For example, you might want to customize your policy to allow access by your business partners. For more details, see the [data perimeter policy examples repository](#).

Note

The `kms:RetireGrant` permission is not effective in an RCP, even if the `Action` element specifies an asterisk (*) as a wildcard.

For more information on how permission to `kms:RetireGrant` is determined, see [Retiring and revoking grants](#).

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "RCPEnforceIdentityPerimeter",
      "Effect": "Deny",
      "Principal": "*",
      "Action": "kms:*",
      "Resource": "*",
      "Condition": {
        "StringNotEqualsIfExists": {
          "aws:PrincipalOrgID": "my-org-id"
        },
        "Bool": {
          "aws:PrincipalIsAWSService": "false"
        }
      }
    }
  ]
}
```

The following example RCP requires that Amazon service principals can only access your customer managed KMS keys when the request originates from your organization. This policy applies the control only on requests that have `aws:SourceAccount` present. This ensures that service integrations that don't require the use of `aws:SourceAccount` aren't affected. If

`aws:SourceAccount` is present in the request context, the `Null` condition evaluates to `true`, causing the `aws:SourceOrgID` key to be enforced.

For more information about the confused deputy problem, see [The confused deputy problem](#) in the *IAM User Guide*.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "RCPEnforceConfusedDeputyProtection",
      "Effect": "Deny",
      "Principal": "*",
      "Action": "kms:*",
      "Resource": "*",
      "Condition": {
        "StringNotEqualsIfExists": {
          "aws:SourceOrgID": "my-org-id"
        },
        "Bool": {
          "aws:PrincipalIsAWSService": "true"
        },
        "Null": {
          "aws:SourceAccount": "false"
        }
      }
    }
  ]
}
```

Grants in Amazon KMS

A *grant* is a policy instrument that allows [Amazon principals](#) to use KMS keys in cryptographic operations. It also can let them view a KMS key (`DescribeKey`) and create and manage grants. When authorizing access to a KMS key, grants are considered along with [key policies](#) and [IAM policies](#). Grants are often used for temporary permissions because you can create one, use its permissions, and delete it without changing your key policies or IAM policies.

Grants are commonly used by Amazon services that integrate with Amazon KMS to encrypt your data at rest. The service creates a grant on behalf of a user in the account, uses its permissions, and

retires the grant as soon as its task is complete. For details about how Amazon services, use grants, see the *Encryption at rest* topic in the service's user guide or developer guide.

Grants are a very flexible and useful access control mechanism. When you create a grant for a KMS key, the grant allows the grantee principal to call the specified grant operations on the KMS key provided that all conditions specified in the grant are met.

- Each grant allows access to exactly one KMS key. You can create a grant for a KMS key in a different Amazon Web Services account.
- A grant can allow access to a KMS key, but not deny access.
- Each grant has one [grantee principal](#). The grantee principal can represent one or more identities in the same Amazon Web Services account as the KMS key or in a different account.
- A grant can only allow [grant operations](#). The grant operations must be supported by the KMS key in the grant. If you specify an unsupported operation, the [CreateGrant](#) request fails with a `ValidationError` exception.
- The grantee principal can use the permissions that the grant gives them without specifying the grant, just as they would if the permissions came from a key policy or IAM policy. However, because the Amazon KMS API follows an [eventual consistency](#) model, when you create, retire, or revoke a grant, there might be a brief delay, before the change is available throughout Amazon KMS. To use the permissions in a grant immediately, [use a grant token](#).
- An authorized principal can delete the grant ([retire](#) or [revoke](#) it). Deleting a grant eliminates all permissions that the grant allowed. You do not have to figure out which policies to add or remove to undo the grant.
- Amazon KMS limits the number of grants on each KMS key. For details, see [Grants per KMS key: 50,000](#).

Be cautious when creating grants and when giving others permission to create grants. Permission to create grants has security implications, much like allowing the [kms:PutKeyPolicy](#) permission to set policies.

- Users with permission to create grants for a KMS key (`kms:CreateGrant`) can use a grant to allow users and roles, including Amazon services, to use the KMS key. The principals can be identities in your own Amazon Web Services account or identities in a different account or organization.
- Grants can allow only a subset of Amazon KMS operations. You can use grants to allow principals to view the KMS key, use it in cryptographic operations, and create and retire grants. For details,

see [Grant operations](#). You can also use [grant constraints](#) to limit the permissions in a grant for a symmetric encryption key.

- Principals can get permission to create grants from a key policy or IAM policy. Principals who get `kms:CreateGrant` permission from a policy can create grants for any [grant operation](#) on the KMS key. These principals are not required to have the permission that they are granting on the key. When you allow `kms:CreateGrant` permission in a policy, you can use [policy conditions](#) to limit this permission.
- Principals can also get permission to create grants from a grant. These principals can only delegate the permissions that they were granted, even if they have other permissions from a policy. For details, see [Granting CreateGrant permission](#).

Grant concepts

To use grants effectively, you'll need to understand the terms and concepts that Amazon KMS uses.

Grant constraint

A condition that limits the permissions in the grant. Currently, Amazon KMS supports grant constraints based on the [encryption context](#) in the request for a cryptographic operation. For details, see [Using grant constraints](#).

Grant ID

The unique identifier of a grant for a KMS key. You can use a grant ID, along with a [key identifier](#), to identify a grant in a [RetireGrant](#) or [RevokeGrant](#) request.

Grant operations

The Amazon KMS operations that you can allow in a grant. If you specify other operations, the [CreateGrant](#) request fails with a `ValidationError` exception. These are also the operations that accept a [grant token](#). For detailed information about these permissions, see the [Amazon KMS permissions](#).

These grant operations actually represent permission to use the operation. Therefore, for the `ReEncrypt` operation, you can specify `ReEncryptFrom`, `ReEncryptTo`, or both `ReEncrypt*`.

The grant operations are:

- Cryptographic operations
 - [Decrypt](#)

- [DeriveSharedSecret](#)
- [Encrypt](#)
- [GenerateDataKey](#)
- [GenerateDataKeyPair](#)
- [GenerateDataKeyPairWithoutPlaintext](#)
- [GenerateDataKeyWithoutPlaintext](#)
- [GenerateMac](#)
- [ReEncryptFrom](#)
- [ReEncryptTo](#)
- [Sign](#)
- [Verify](#)
- [VerifyMac](#)
- Other operations
 - [CreateGrant](#)
 - [DescribeKey](#)
 - [GetPublicKey](#)
 - [RetireGrant](#)

The grant operations that you allow must be supported by the KMS key in the grant. If you specify an unsupported operation, the [CreateGrant](#) request fails with a `ValidationError` exception. For example, grants for symmetric encryption KMS keys cannot allow the [Sign](#), [Verify](#), [GenerateMac](#) or [VerifyMac](#) operations. Grants for asymmetric KMS keys cannot allow any operations that generate data keys or data key pairs.

Grant token

The Amazon KMS API follows an [eventual consistency](#) model. When you create a grant, there might be a brief delay before the change is available throughout Amazon KMS. It typically takes less than a few seconds for the change to propagate throughout the system, but in some cases it can take several minutes. If you try to use a grant before it fully propagates through the system, you might get an access denied error. A grant token lets you refer to the grant and use the grant permissions immediately.

A *grant token* is a unique, nonsecret, variable-length, base64-encoded string that represents a grant. You can use the grant token to identify the grant in any [grant operation](#). However, because the token value is a hash digest, it doesn't reveal any details about the grant.

A grant token is designed to be used only until the grant has fully propagated throughout Amazon KMS. After that, the [grantee principal](#) can use the permission in the grant without providing a grant token or any other evidence of the grant. You can use a grant token at any time, but once the grant is eventually consistent, Amazon KMS uses the grant to determine permissions, not the grant token.

For example, the following command calls the [GenerateDataKey](#) operation. It uses a grant token to represent the grant that gives the caller (the grantee principal) permission to call `GenerateDataKey` on the specified KMS key.

```
$ aws kms generate-data-key \  
  --key-id 1234abcd-12ab-34cd-56ef-1234567890ab \  
  --key-spec AES_256 \  
  --grant-token $token
```

You can also use a grant token to identify a grant in operations that manage grants. For example, the [retiring principal](#) can use a grant token in a call to the [RetireGrant](#) operation.

```
$ aws kms retire-grant \  
  --grant-token $token
```

`CreateGrant` is the only operation that returns a grant token. You cannot get a grant token from any other Amazon KMS operation or from the [CloudTrail log event](#) for the `CreateGrant` operation. The [ListGrants](#) and [ListRetirableGrants](#) operations return the [grant ID](#), but not a grant token.

For details, see [Using a grant token](#).

Grantee principal

The identities that get the permissions specified in the grant. Each grant has one grantee principal, but the grantee principal can represent multiple identities.

The grantee principal can be any Amazon principal, including an Amazon Web Services account (root), an [IAM user](#), an [IAM role](#), a [federated role or user](#), or an assumed role user. The grantee principal can be in the same account as the KMS key or a different account. However, the grantee principal cannot be a [service principal](#), an [IAM group](#), or an [Amazon organization](#).

Note

IAM best practices discourage the use of IAM users with long-term credentials. Whenever possible, use IAM roles, which provide temporary credentials. For details, see [Security best practices in IAM](#) in the *IAM User Guide*.

Retire (a grant)

Terminates a grant. You retire a grant when you finish using the permissions.

Revoking and retiring a grant both delete the grant. But retiring is done by a principal specified in the grant. Revoking is typically done by a key administrator. For details, see [Retiring and revoking grants](#).

Retiring principal

A principal who can [retire a grant](#). You can specify a retiring principal in a grant, but it is not required. The retiring principal can be any Amazon principal, including Amazon Web Services accounts, IAM users, IAM roles, federated users, and assumed role users. The retiring principal can be in the same account as the KMS key or a different account.

Note

IAM best practices discourage the use of IAM users with long-term credentials. Whenever possible, use IAM roles, which provide temporary credentials. For details, see [Security best practices in IAM](#) in the *IAM User Guide*.

In addition to retiring principal specified in the grant, a grant can be retired by the Amazon Web Services account in which the grant was created. If the grant allows the `RetireGrant` operation, the [grantee principal](#) can retire the grant. Also, the Amazon Web Services account or an Amazon Web Services account that is the retiring principal can delegate the permission to retire a grant to an IAM principal in the same Amazon Web Services account. For details, see [Retiring and revoking grants](#).

Revoke (a grant)

Terminates a grant. You revoke a grant to actively deny the permissions that the grant allows.

Revoking and retiring a grant both delete the grant. But retiring is done by a principal specified in the grant. Revoking is typically done by a key administrator. For details, see [Retiring and revoking grants](#).

Eventual consistency (for grants)

The Amazon KMS API follows an [eventual consistency](#) model. When you create, retire, or revoke a grant, there might be a brief delay before the change is available throughout Amazon KMS. It typically takes less than a few seconds for the change to propagate throughout the system, but in some cases it can take several minutes.

You might become aware of this brief delay if you get unexpected errors. For example, If you try to manage a new grant or use the permissions in a new grant before the grant is known throughout Amazon KMS, you might get an access denied error. If you retire or revoke a grant, the grantee principal might still be able to use its permissions for a brief period until the grant is fully deleted. The typical strategy is to retry the request, and some Amazon SDKs include automatic backoff and retry logic.

Amazon KMS has features to mitigate this brief delay.

- To use the permissions in a new grant immediately, use a [grant token](#). You can use a grant token to refer to a grant in any [grant operation](#). For instructions, see [Using a grant token](#).
- The [CreateGrant](#) operation has a Name parameter that prevents retry operations from creating duplicate grants.

Note

Grant tokens supersede the validity of the grant until all endpoints in the service have been updated with the new grant state. In most cases, eventual consistency will be achieved within five minutes.

For more information, see [Amazon KMS eventual consistency](#).

Best practices for Amazon KMS grants

Amazon KMS recommends the following best practices when creating, using, and managing grants.


- Limit the permissions in the grant to those that the grantee principal requires. Use the principle of [least privileged access](#).

- Use a specific grantee principal, such as an IAM role, and give the grantee principal permission to use only the API operations that they require.
- Use the encryption context [grant constraints](#) to ensure that callers are using the KMS key for the intended purpose. For details about how to use the encryption context in a request to secure your data, see [How to Protect the Integrity of Your Encrypted Data by Using Amazon Key Management Service and EncryptionContext](#) in the *Amazon Security Blog*.

 Tip

Use the [EncryptionContextEqual](#) grant constraint whenever possible. The [EncryptionContextSubset](#) grant constraint is more difficult to use correctly. If you need to use it, read the documentation carefully and test the grant constraint to make sure it works as intended.

- Delete duplicate grants. Duplicate grants have the same key ARN, API actions, grantee principal, encryption context, and name. If you retire or revoke the original grant but leave the duplicates, the leftover duplicate grants constitute unintended escalations of privilege. To avoid duplicating grants when retrying a `CreateGrant` request, use the [Name parameter](#). To detect duplicate grants, use the [ListGrants](#) operation. If you accidentally create a duplicate grant, retire or revoke it as soon as possible.

 Note

Grants for [Amazon managed keys](#) might look like duplicates but have different grantee principals.

The `GranteePrincipal` field in the `ListGrants` response usually contains the grantee principal of the grant. However, when the grantee principal in the grant is an Amazon service, the `GranteePrincipal` field contains the [service principal](#), which might represent several different grantee principals.

- Remember that grants do not automatically expire. [Retire or revoke the grant](#) as soon as the permission is no longer needed. Grants that are not deleted might create a security risk for encrypted resources.

Controlling access to grants

You can control access to the operations that create and manage grants in key policies, IAM policies, and in grants. Principals who get CreateGrant permission from a grant have [more limited grant permissions](#).

API operation	Key policy or IAM policy	Grant
CreateGrant	✓	✓
ListGrants	✓	-
ListRetirableGrants	✓	-
Retire Grants	(Limited. See Retiring and revoking grants)	✓
RevokeGrant	✓	-

When you use a key policy or IAM policy to control access to operations that create and manage grants, you can use one or more of the following policy conditions to limit the permission. Amazon KMS supports all of the following grant-related condition keys. For detailed information and examples, see [Amazon KMS condition keys](#).

[kms:GrantConstraintType](#)

Allows principals to create a grant only when the grant includes the specified [grant constraint](#).

[kms:GrantsForAWSResource](#)

Allows principals to call CreateGrant, ListGrants, or RevokeGrant only when [an Amazon service that is integrated with Amazon KMS](#) sends the request on the principal's behalf.

[kms:GrantOperations](#)

Allows principals to create a grant, but limits the grant to the specified operations.

[kms:GranteePrincipal](#)

Allows principals to create a grant only for the specified [grantee principal](#).

[kms:RetiringPrincipal](#)

Allows principals to create a grant only when the grant specifies a particular [retiring principal](#).

Creating grants

Before creating a grant, learn about the options for customizing your grant. You can use *grant constraints* to limit the permissions in the grant. Also, learn about granting `CreateGrant` permission. Principals who get permission to create grants from a grant are limited in the grants that they can create.

Topics

- [Creating a grant](#)
- [Granting `CreateGrant` permission](#)

Creating a grant

To create a grant, call the [CreateGrant](#) operation. Specify a KMS key, a [grantee principal](#), and a list of allowed [grant operations](#). You can also designate an optional [retiring principal](#). To customize the grant, use optional `Constraints` parameters to define [grant constraints](#).

When you create, retire, or revoke a grant, there might be a brief delay, usually less than five minutes, before the change is available throughout Amazon KMS. For more information, see [Eventual consistency \(for grants\)](#).

For example, the following `CreateGrant` command creates a grant that allows users who are authorized to assume the `keyUserRole` role to call the [Decrypt](#) operation on the specified [symmetric KMS key](#). The grant uses the `RetiringPrincipal` parameter to designate a principal that can retire the grant. It also includes a grant constraint that allows the permission only when the [encryption context](#) in the request includes `"Department": "IT"`.

```
$ aws kms create-grant \  
  --key-id 1234abcd-12ab-34cd-56ef-1234567890ab \  
  --grantee-principal arn:aws:iam::111122223333:role/keyUserRole \  
  --operations Decrypt \  
  --retiring-principal arn:aws:iam::111122223333:role/adminRole \  
  --constraints EncryptionContextSubset={Department=IT}
```

If your code retries the `CreateGrant` operation, or uses an [Amazon SDK that automatically retries requests](#), use the optional `Name` parameter to prevent the creation of duplicate grants. If Amazon KMS gets a `CreateGrant` request for a grant with the same properties as an existing grant, including the name, it recognizes the request as a retry, and does not create a new grant. You cannot use the `Name` value to identify the grant in any Amazon KMS operations.

Important

Do not include confidential or sensitive information in the grant name. It may appear in plain text in CloudTrail logs and other output.

```
$ aws kms create-grant \  
  --name IT-1234abcd-keyUserRole-decrypt \  
  --key-id 1234abcd-12ab-34cd-56ef-1234567890ab \  
  --grantee-principal arn:aws:iam::111122223333:role/keyUserRole \  
  --operations Decrypt \  
  --retiring-principal arn:aws:iam::111122223333:role/adminRole \  
  --constraints EncryptionContextSubset={Department=IT}
```

For code examples that demonstrate how to create grants in several programming languages, see [Use CreateGrant with an Amazon SDK or CLI](#).

Using grant constraints

[Grant constraints](#) set conditions on the permissions that the grant gives to the grantee principal. Grant constraints take the place of [condition keys](#) in a [key policy](#) or [IAM policy](#). Each grant constraint value can include up to 8 encryption context pairs. The encryption context value in each grant constraint cannot exceed 384 characters.

Important

Do not include confidential or sensitive information in this field. This field may be displayed in plaintext in CloudTrail logs and other output.

Amazon KMS supports two grant constraints, `EncryptionContextEquals` and `EncryptionContextSubset`, both of which establish requirements for the [encryption context](#) in a request for a cryptographic operation.

The encryption context grant constraints are designed to be used with [grant operations](#) that have an encryption context parameter.

- Encryption context constraints are valid only in a grant for a symmetric encryption KMS key. Cryptographic operations with other KMS keys don't support an encryption context.
- The encryption context constraint is ignored for `DescribeKey` and `RetireGrant` operations. `DescribeKey` and `RetireGrant` don't have an encryption context parameter, but you can include these operations in a grant that has an encryption context constraint.
- You can use an encryption context constraint in a grant for the `CreateGrant` operation. The encryption context constraint requires that any grants created with the `CreateGrant` permission have an equally strict or stricter encryption context constraint.

Amazon KMS supports the following encryption context grant constraints.

EncryptionContextEquals

Use `EncryptionContextEquals` to specify the exact encryption context for permitted requests.

`EncryptionContextEquals` requires that the encryption context pairs in the request are an exact, case-sensitive match for the encryption context pairs in the grant constraint. The pairs can appear in any order, but the keys and values in each pair cannot vary.

For example, if the `EncryptionContextEquals` grant constraint requires the `"Department": "IT"` encryption context pair, the grant allows requests of the specified type only when the encryption context in the request is exactly `"Department": "IT"`.

EncryptionContextSubset

Use `EncryptionContextSubset` to require that requests include particular encryption context pairs.

`EncryptionContextSubset` requires that the request include all encryption context pairs in the grant constraint (an exact, case-sensitive match), but the request can also have additional encryption context pairs. The pairs can appear in any order, but the keys and values in each pair cannot vary.

For example, if the `EncryptionContextSubset` grant constraint requires the `Department=IT` encryption context pair, the grant allows requests of the specified type when the encryption context in the request is `"Department": "IT"`, or includes `"Department":`

"IT" along with other encryption context pairs, such as "Department": "IT", "Purpose": "Test".

To specify an encryption context constraint in a grant for a symmetric encryption KMS key, use the `Constraints` parameter in the [CreateGrant](#) operation. The grant that this command creates gives users who are authorized to assume the `keyUserRole` role permission to call the [Decrypt](#) operation. But that permission is effective only when the encryption context in the Decrypt request is a "Department": "IT" encryption context pair.

```
$ aws kms create-grant \
  --key-id 1234abcd-12ab-34cd-56ef-1234567890ab \
  --grantee-principal arn:aws:iam::111122223333:role/keyUserRole \
  --operations Decrypt \
  --retiring-principal arn:aws:iam::111122223333:role/adminRole \
  --constraints EncryptionContextEquals={Department=IT}
```

The resulting grant looks like the following one. Notice that the permission granted to the `keyUserRole` role is effective only when the Decrypt request uses the same encryption context pair specified in the grant constraint. To find the grants on a KMS key, use the [ListGrants](#) operation.

```
$ aws kms list-grants --key-id 1234abcd-12ab-34cd-56ef-1234567890ab
{
  "Grants": [
    {
      "Name": "",
      "IssuingAccount": "arn:aws:iam::111122223333:root",
      "GrantId":
"abcde1237f76e4ba7987489ac329fbfba6ad343d6f7075dbd1ef191f0120514a",
      "Operations": [
        "Decrypt"
      ],
      "GranteePrincipal": "arn:aws:iam::111122223333:role/keyUserRole",
      "Constraints": {
        "EncryptionContextEquals": {
          "Department": "IT"
        }
      },
      "CreationDate": 1568565290.0,
      "KeyId": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab",
      "RetiringPrincipal": "arn:aws:iam::111122223333:role/adminRole"
```

```

    }
  ]
}

```

To satisfy the `EncryptionContextEquals` grant constraint, the encryption context in the request for the `Decrypt` operation must be a `"Department": "IT"` pair. A request like the following from the grantee principal would satisfy the `EncryptionContextEquals` grant constraint.

```

$ aws kms decrypt \
  --key-id arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab \
  --ciphertext-blob fileb://encrypted_msg \
  --encryption-context Department=IT

```

When the grant constraint is `EncryptionContextSubset`, the encryption context pairs in the request must include the encryption context pairs in the grant constraint, but the request can also include other encryption context pairs. The following grant constraint requires that one of encryption context pairs in the request is `"Department": "IT"`.

```

"Constraints": {
  "EncryptionContextSubset": {
    "Department": "IT"
  }
}

```

The following request from the grantee principal would satisfy both of the `EncryptionContextEqual` and `EncryptionContextSubset` grant constraints in this example.

```

$ aws kms decrypt \
  --key-id arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab \
  --ciphertext-blob fileb://encrypted_msg \
  --encryption-context Department=IT

```

However, a request like the following from the grantee principal would satisfy the `EncryptionContextSubset` grant constraint, but it would fail the `EncryptionContextEquals` grant constraint.

```

$ aws kms decrypt \

```

```
--key-id arn:aws:kms:us-west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab \  
--ciphertext-blob fileb://encrypted_msg \  
--encryption-context Department=IT,Purpose=Test
```

Amazon services often use encryption context constraints in the grants that give them permission to use KMS keys in your Amazon Web Services account. For example, Amazon DynamoDB uses a grant like the following one to get permission to use the [Amazon managed key](#) for DynamoDB in your account. The `EncryptionContextSubset` grant constraint in this grant makes the permissions in the grant effective only when the encryption context in the request includes `"subscriberID": "111122223333"` and `"tableName": "Services"` pairs. This grant constraint means that the grant allows DynamoDB to use the specified KMS key only for a particular table in your Amazon Web Services account.

To get this output, run the [ListGrants](#) operation on the Amazon managed key for DynamoDB in your account.

```
$ aws kms list-grants --key-id 0987dcba-09fe-87dc-65ba-ab0987654321  
  
{  
  "Grants": [  
    {  
      "Operations": [  
        "Decrypt",  
        "Encrypt",  
        "GenerateDataKey",  
        "ReEncryptFrom",  
        "ReEncryptTo",  
        "RetireGrant",  
        "DescribeKey"  
      ],  
      "IssuingAccount": "arn:aws:iam::111122223333:root",  
      "Constraints": {  
        "EncryptionContextSubset": {  
          "aws:dynamodb:tableName": "Services",  
          "aws:dynamodb:subscriberId": "111122223333"  
        }  
      },  
      "CreationDate": 1518567315.0,  
      "KeyId": "arn:aws:kms:us-west-2:111122223333:key/0987dcba-09fe-87dc-65ba-ab0987654321",  
      "GranteePrincipal": "dynamodb.us-west-2.amazonaws.com",
```

```
    "RetiringPrincipal": "dynamodb.us-west-2.amazonaws.com",
    "Name": "8276b9a6-6cf0-46f1-b2f0-7993a7f8c89a",
    "GrantId":
"1667b97d27cf748cf05b487217dd4179526c949d14fb3903858e25193253fe59"
  }
]
}
```

Granting CreateGrant permission

A grant can include permission to call the `CreateGrant` operation. But when a [grantee principal](#) gets permission to call `CreateGrant` from a grant, rather than from a policy, that permission is limited.

- The grantee principal can only create grants that allow some or all of the operations in the parent grant.
- The [grant constraints](#) in the grants they create must be at least as strict as those in the parent grant.

These limitations don't apply to principals who get `CreateGrant` permission from a policy, although their permissions can be limited by [policy conditions](#).

For example, consider a grant that allows the grantee principal to call the `GenerateDataKey`, `Decrypt`, and `CreateGrant` operations. We call a grant that allow `CreateGrant` permission a *parent grant*.

```
# The original grant in a ListGrants response.
{
  "Grants": [
    {
      "KeyId": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab",
      "CreationDate": 1572216195.0,
      "GrantId":
"abcde1237f76e4ba7987489ac329fbfba6ad343d6f7075dbd1ef191f0120514a",
      "Operations": [
        "GenerateDataKey",
        "Decrypt",
        "CreateGrant
      ]
      "RetiringPrincipal": "arn:aws:iam::111122223333:role/adminRole",
```



```

    "Name": "",
    "IssuingAccount": "arn:aws:iam::111122223333:root",
    "GranteePrincipal": "arn:aws:iam::111122223333:role/keyUserRole",
    "Constraints": {
      "EncryptionContextSubset": {
        "Department": "IT"
      }
    },
  ],
]
}

```

The grantee principal, `exampleUser`, can use this permission to create a grant that includes any subset of the operations specified in the original grant, such as `CreateGrant` and `Decrypt`. The *child grant* cannot include other operations, such as `ScheduleKeyDeletion` or `ReEncrypt`.

Also, the [grant constraints](#) in child grants must be as restrictive or more restrictive than those in the parent grant. For example, the child grant can add pairs to an `EncryptionContextSubset` constraint in the parent grant, but it cannot remove them. The child grant can change an `EncryptionContextSubset` constraint to an `EncryptionContextEquals` constraint, but not the reverse.

IAM best practices discourage the use of IAM users with long-term credentials. Whenever possible, use IAM roles, which provide temporary credentials. For details, see [Security best practices in IAM](#) in the *IAM User Guide*.

For example, the grantee principal can use the `CreateGrant` permission that it got from the parent grant to create the following child grant. The operations in the child grant are a subset of the operations in the parent grant and the grant constraints are more restrictive.

```

# The child grant in a ListGrants response.
{
  "Grants": [
    {
      "KeyId": "arn:aws:kms:us-west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab",
      "CreationDate": 1572249600.0,
      "GrantId": "fedcba9999c1e2e9876abcde6e9d6c9b6a1987650000abcee009abcdef40183f",
      "Operations": [
        "CreateGrant"
        "Decrypt"
      ]
    }
  ]
}

```

```

    ]
    "RetiringPrincipal": "arn:aws:iam::111122223333:user/exampleUser",
    "Name": "",
    "IssuingAccount": "arn:aws:iam::111122223333:root",
    "GranteePrincipal": "arn:aws:iam::111122223333:user/anotherUser",
    "Constraints": {
      "EncryptionContextEquals": {
        "Department": "IT"
      }
    },
  }
]
}

```

The grantee principal in the child grant, `anotherUser`, can use their `CreateGrant` permission to create grants. However, the grants that `anotherUser` creates must include the operations in its parent grant or a subset, and the grant constraints must be the same or stricter.

Viewing grants

To view the grant, use the [ListGrants](#) operation. You must specify the KMS key to which the grants apply. You can also filter the grant list by grant ID or grantee principal. For more examples, see [Use ListGrants with an Amazon SDK or CLI](#).

To view all grants in the Amazon Web Services account and Region with a particular [retiring principal](#), use [ListRetirableGrants](#). The responses include details about each grant.

Note

The `GranteePrincipal` field in the `ListGrants` response usually contains the grantee principal of the grant. However, when the grantee principal in the grant is an Amazon service, the `GranteePrincipal` field contains the [service principal](#), which might represent several different grantee principals.

For example, the following command lists all of the grants for a KMS key.

```

$ aws kms list-grants --key-id 1234abcd-12ab-34cd-56ef-1234567890ab
{
  "Grants": [

```

```
{
  "KeyId": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab",
  "CreationDate": 1572216195.0,
  "GrantId":
"abcde1237f76e4ba7987489ac329fbfba6ad343d6f7075dbd1ef191f0120514a",
  "Constraints": {
    "EncryptionContextSubset": {
      "Department": "IT"
    }
  },
  "RetiringPrincipal": "arn:aws:iam::111122223333:role/adminRole",
  "Name": "",
  "IssuingAccount": "arn:aws:iam::111122223333:root",
  "GranteePrincipal": "arn:aws:iam::111122223333:user/exampleUser",
  "Operations": [
    "Decrypt"
  ]
}
```

Using a grant token

The Amazon KMS API follows an [eventual consistency](#) model. When you create a grant, the grant might not be effective immediately. There might be a brief delay before the change is available throughout Amazon KMS. It typically takes less than a few seconds for the change to propagate throughout the system, but in some cases it can take several minutes. Once the change has fully propagated throughout the system, the grantee principal can use the permissions in the grant without specifying the grant token or any evidence of the grant. However, if a grant that is so new that it is not yet known to all of Amazon KMS, the request might fail with an `AccessDeniedException` error.

To use the permissions in a new grant immediately, use the [grant token](#) for the grant. Save the grant token that the [CreateGrant](#) operation returns. Then submit the grant token in the request for the Amazon KMS operation. You can submit a grant token to any Amazon KMS [grant operation](#) and you can submit multiple grant tokens in the same request.

The following example uses the `CreateGrant` operation to create a grant that allows the [GenerateDataKey](#) and [Decrypt](#) operations. It saves the grant token that `CreateGrant` returns in

the token variable. Then, in a call to the `GenerateDataKey` operation, it uses the grant token in the token variable.

```
# Create a grant; save the grant token
$ token=$(aws kms create-grant \
  --key-id 1234abcd-12ab-34cd-56ef-1234567890ab \
  --grantee-principal arn:aws:iam::111122223333:user/appUser \
  --retiring-principal arn:aws:iam::111122223333:user/acctAdmin \
  --operations GenerateDataKey Decrypt \
  --query GrantToken \
  --output text)

# Use the grant token in a request
$ aws kms generate-data-key \
  --key-id 1234abcd-12ab-34cd-56ef-1234567890ab \
  --key-spec AES_256 \
  --grant-tokens $token
```

Principals with permission can also use a grant token to retire a new grant even before the grant is available throughout Amazon KMS. (The `RevokeGrant` operation doesn't accept a grant token.) For details, see [Retiring and revoking grants](#).

```
# Retire the grant
$ aws kms retire-grant --grant-token $token
```

Retiring and revoking grants

To delete a grant, retire or revoke it.

The [RetireGrant](#) and [RevokeGrant](#) operations are very similar to each other. Both operations delete a grant, which eliminates the permissions the grant allows. The primary difference between these operations is how they are authorized.

RevokeGrant

Like most Amazon KMS operations, access to the `RevokeGrant` operation is controlled through [key policies](#) and [IAM policies](#). The [RevokeGrant](#) API can be called by any principal with `kms:RevokeGrant` permission. This permission is included in the standard permissions given to key administrators. Typically, administrators revoke a grant to deny permissions the grant allows.

RetireGrant

The grant determines who can retire it. This design allows you to control the lifecycle of a grant without changing key policies or IAM policies. Typically, you retire a grant when you are done using its permissions.

A grant can be retired by an optional [retiring principal](#) specified in the grant. The [grantee principal](#) can also retire the grant, but only if they are also a retiring principal or the grant includes the `RetireGrant` operation. As a backup, the Amazon Web Services account in which the grant was created can retire the grant.

There is a `kms:RetireGrant` permission that can be used in IAM policies, but it has limited utility. Principals specified in the grant can retire a grant without the `kms:RetireGrant` permission. The `kms:RetireGrant` permission alone does not allow principals to retire a grant. The `kms:RetireGrant` permission is not effective in a [key policy](#) or [resource control policy](#).

- To deny permission to retire a grant, you can use a Deny action with the `kms:RetireGrant` permission in your IAM policies.
- The Amazon Web Services account that owns the KMS key can delegate the `kms:RetireGrant` permission to an IAM principal in the account.
- If the retiring principal is a different Amazon Web Services account, administrators in the other account can use `kms:RetireGrant` to delegate permission to retire the grant to an IAM principal in that account.

The Amazon KMS API follows an [eventual consistency](#) model. When you create, retire, or revoke a grant, there might be a brief delay before the change is available throughout Amazon KMS. It typically takes less than a few seconds for the change to propagate throughout the system, but in some cases it can take several minutes. If you need to delete a new grant immediately, before it is available throughout Amazon KMS, [use a grant token](#) to retire the grant. You cannot use a grant token to revoke a grant.

Condition keys for Amazon KMS

You can specify conditions in the [key policies](#) and [IAM policies](#) that control access to Amazon KMS resources. The policy statement is effective only when the conditions are true. For example, you might want a policy statement to take effect only after a specific date. Or, you might want a policy statement to control access only when a specific value appears in an API request.

To specify conditions, you use *condition keys* in the [Condition element](#) of a policy statement with [IAM condition operators](#). Some condition keys apply generally to Amazon; others are specific to Amazon KMS.

Condition key values must adhere to the character and encoding rules for Amazon KMS key policies and IAM policies. For details about key policy document rules, see [Key policy format](#). For details about IAM policy document rules, see [IAM name requirements](#) in the *IAM User Guide*.

Topics

- [Amazon global condition keys](#)
- [Amazon KMS condition keys](#)
- [Amazon KMS condition keys for Amazon Nitro Enclaves](#)

Amazon global condition keys

Amazon defines [global condition keys](#), a set of policy conditions keys for all Amazon services that use IAM for access control. Amazon KMS supports all global condition keys. You can use them in Amazon KMS key policies and IAM policies.

For example, you can use the [aws:PrincipalArn](#) global condition key to allow access to an Amazon KMS key (KMS key) only when the principal in the request is represented by the Amazon Resource Name (ARN) in the condition key value. To support [attribute-based access control](#) (ABAC) in Amazon KMS, you can use the [aws:ResourceTag/tag-key](#) global condition key in an IAM policy to allow access to KMS keys with a particular tag.

To help prevent an Amazon service from being used as a confused deputy in a policy where the principal is an [Amazon service principal](#), you can use the [aws:SourceArn](#) or [aws:SourceAccount](#) global condition keys. For details, see [Using aws:SourceArn or aws:SourceAccount condition keys](#).

For information about Amazon global condition keys, including the types of requests in which they are available, see [Amazon Global Condition Context Keys](#) in the *IAM User Guide*. For examples of using global condition keys in IAM policies, see [Controlling Access to Requests](#) and [Controlling Tag Keys](#) in the *IAM User Guide*.

The following topics provide special guidance for using condition keys based on IP addresses and VPC endpoints.

Topics

- [Using the IP address condition in policies with Amazon KMS permissions](#)
- [Using VPC endpoint conditions in policies with Amazon KMS permissions](#)

Using the IP address condition in policies with Amazon KMS permissions

You can use Amazon KMS to protect your data in an [integrated Amazon service](#). But use caution when specifying the [IP address condition operators](#) or the `aws:SourceIp` condition key in the same policy statement that allows or denies access to Amazon KMS. For example, the policy in [Amazon: Denies Access to Amazon Based on the Source IP](#) restricts Amazon actions to requests from the specified IP range.

Consider this scenario:

1. You attach a policy like the one shown at [Amazon: Denies Access to Amazon Based on the Source IP](#) to an IAM identity. You set the value of the `aws:SourceIp` condition key to the range of IP addresses for the user's company. This IAM identity has other policies attached that allow it to use Amazon EBS, Amazon EC2, and Amazon KMS.
2. The identity attempts to attach an encrypted EBS volume to an EC2 instance. This action fails with an authorization error even though the user has permission to use all the relevant services.

Step 2 fails because the request to Amazon KMS to decrypt the volume's encrypted data key comes from an IP address that is associated with the Amazon EC2 infrastructure. To succeed, the request must come from the IP address of the originating user. Because the policy in step 1 explicitly denies all requests from IP addresses other than those specified, Amazon EC2 is denied permission to decrypt the EBS volume's encrypted data key.

Also, the `aws:sourceIP` condition key is not effective when the request comes from an [Amazon VPC endpoint](#). To restrict requests to a VPC endpoint, including an [Amazon KMS VPC endpoint](#), use the `aws:sourceVpce` or `aws:sourceVpc` condition keys. For more information, see [VPC Endpoints - Controlling the Use of Endpoints](#) in the *Amazon VPC User Guide*.

Using VPC endpoint conditions in policies with Amazon KMS permissions

[Amazon KMS supports Amazon Virtual Private Cloud \(Amazon VPC\) endpoints](#) that are powered by [Amazon PrivateLink](#). You can use the following [global condition keys](#) in key policies and IAM policies to control access to Amazon KMS resources when the request comes from a VPC or uses a VPC endpoint. For details, see [Use VPC endpoints to control access to Amazon KMS resources](#).

- `aws:SourceVpc` limits access to requests from the specified VPC.
- `aws:SourceVpce` limits access to requests from the specified VPC endpoint.

If you use these condition keys to control access to KMS keys, you might inadvertently deny access to Amazon services that use Amazon KMS on your behalf.

Take care to avoid a situation like the [IP address condition keys](#) example. If you restrict requests for a KMS key to a VPC or VPC endpoint, calls to Amazon KMS from an integrated service, such as Amazon S3 or Amazon EBS, might fail. This can happen even if the source request ultimately originates in the VPC or from the VPC endpoint.

Amazon KMS condition keys

Amazon KMS provides a set of condition keys that you can use in key policies and IAM policies. These condition keys are specific to Amazon KMS. For example, you can use the `kms:EncryptionContext:context-key` condition key to require a particular [encryption context](#) when controlling access to a symmetric encryption KMS key.

Conditions for an API operation request

Many Amazon KMS condition keys control access to a KMS key based on the value of a parameter in the request for an Amazon KMS operation. For example, you can use the `kms:KeySpec` condition key in an IAM policy to allow use of the [CreateKey](#) operation only when the value of the `KeySpec` parameter in the `CreateKey` request is `RSA_4096`.

This type of condition works even when the parameter doesn't appear in the request, such as when you use the parameter's default value. For example you can use the `kms:KeySpec` condition key to allow users to use the `CreateKey` operation only when the value of the `KeySpec` parameter is `SYMMETRIC_DEFAULT`, which is the default value. This condition allows requests that have the `KeySpec` parameter with the `SYMMETRIC_DEFAULT` value and requests that have no `KeySpec` parameter.

Conditions for KMS keys used in API operations

Some Amazon KMS condition keys can control access to operations based on a property of the KMS key that is used in the operation. For example, you can use the `kms:KeyOrigin` condition to allow principals to call [GenerateDataKey](#) on a KMS key only when the `Origin` of the KMS key is `AWS_KMS`. To find out if a condition key can be used in this way, see the description of the condition key.

The operation must be a *KMS key resource operation*, that is, an operation that is authorized for a particular KMS key. To identify the KMS key resource operations, in the [Actions and Resources Table](#), look for a value of `KMS key` in the Resources column for the operation. If you use this type of condition key with an operation that is not authorized for a particular KMS key resource, like [ListKeys](#), the permission is not effective because the condition can never be satisfied. There is no KMS key resource involved in authorizing the `ListKeys` operation and no `KeySpec` property.

The following topics describe each Amazon KMS condition key and include example policy statements that demonstrate policy syntax.

Using set operators with condition keys

When a policy condition compares two set of values, such as the set of tags in a request and the set of tags in a policy, you need tell Amazon how to compare the sets. IAM defines two set operators, `ForAnyValue` and `ForAllValues`, for this purpose. Use set operators only with *multi-valued condition keys*, which require them. Do not use set operators with *single-valued condition keys*. As always, test your policy statements thoroughly before using them in a production environment.

Condition keys are single-valued or multi-valued. To determine whether an Amazon KMS condition key is single-valued or multi-valued, see the **Value type** column in the condition key description.

- *Single-valued* condition keys have at most one value in the authorization context (the request or resource). For example, because each API call can originate from only one Amazon Web Services account, [kms:CallerAccount](#) is a single valued condition key. Do not use a set operator with a single-valued condition key.
- *Multi-valued* condition keys have multiple values in the authorization context (the request or resource). For example, because each KMS key can have multiple aliases, [kms:ResourceAliases](#) can have multiple values. Multi-valued condition keys require a set operator.

Note that the difference between single-valued and multi-valued condition keys depends on the number of values in the authorization context; not the number of values in the policy condition.

Warning

Using a set operator with a single-valued condition key can create a policy statement that is overly permissive (or overly restrictive). Use set operators only with multi-valued condition keys.

If you create or update a policy that includes a `ForAllValues` set operator with the `kms:EncryptionContext:context-key` or `aws:RequestTag/tag-key` condition keys, Amazon KMS returns the following error message:

`OverlyPermissiveCondition: Using the ForAllValues set operator with a single-valued condition key matches requests without the specified [encryption context or tag] or with an unspecified [encryption context or tag]. To fix, remove ForAllValues.`

For detailed information about the `ForAnyValue` and `ForAllValues` set operators, see [Using multiple keys and values](#) in the *IAM User Guide*. For information about the risk of using the `ForAllValues` set operator with a single-valued condition, see [Security Warning – ForAllValues with single valued key](#) in the *IAM User Guide*.

Topics

- [kms:BypassPolicyLockoutSafetyCheck](#)
- [kms:CallerAccount](#)
- [kms:CustomerMasterKeySpec \(deprecated\)](#)
- [kms:CustomerMasterKeyUsage \(deprecated\)](#)
- [kms:DataKeyPairSpec](#)
- [kms:EncryptionAlgorithm](#)
- [kms:EncryptionContext:context-key](#)
- [kms:EncryptionContextKeys](#)
- [kms:ExpirationModel](#)
- [kms:GrantConstraintType](#)
- [kms:GrantIsForAWSResource](#)
- [kms:GrantOperations](#)
- [kms:GranteePrincipal](#)
- [kms:KeyAgreementAlgorithm](#)
- [kms:KeyOrigin](#)
- [kms:KeySpec](#)
- [kms:KeyUsage](#)

- [kms:MacAlgorithm](#)
- [kms:MessageType](#)
- [kms:MultiRegion](#)
- [kms:MultiRegionKeyType](#)
- [kms:PrimaryRegion](#)
- [kms:ReEncryptOnSameKey](#)
- [kms:RequestAlias](#)
- [kms:ResourceAliases](#)
- [kms:ReplicaRegion](#)
- [kms:RetiringPrincipal](#)
- [kms:RotationPeriodInDays](#)
- [kms:ScheduleKeyDeletionPendingWindowInDays](#)
- [kms:SigningAlgorithm](#)
- [kms:ValidTo](#)
- [kms:ViaService](#)
- [kms:WrappingAlgorithm](#)
- [kms:WrappingKeySpec](#)

kms:BypassPolicyLockoutSafetyCheck

Amazon KMS condition keys	Condition type	Value type	API operations	Policy type
kms:BypassPolicyLockoutSafetyCheck	Boolean	Single-valued	CreateKey PutKeyPolicy	IAM policies only Key policies and IAM policies

The `kms:BypassPolicyLockoutSafetyCheck` condition key controls access to the [CreateKey](#) and [PutKeyPolicy](#) operations based on the value of the `BypassPolicyLockoutSafetyCheck` parameter in the request.

The following example IAM policy statement prevents users from bypassing the policy lockout safety check by denying them permission to create KMS keys when the value of the `BypassPolicyLockoutSafetyCheck` parameter in the `CreateKey` request is `true`.

```
{
  "Effect": "Deny",
  "Action": [
    "kms:CreateKey",
    "kms:PutKeyPolicy"
  ],
  "Resource": "*",
  "Condition": {
    "Bool": {
      "kms:BypassPolicyLockoutSafetyCheck": true
    }
  }
}
```

You can also use the `kms:BypassPolicyLockoutSafetyCheck` condition key in an IAM policy or key policy to control access to the `PutKeyPolicy` operation. The following example policy statement from a key policy prevents users from bypassing the policy lockout safety check when changing the policy of a KMS key.

Instead of using an explicit `Deny`, this policy statement uses `Allow` with the [Null condition operator](#) to allow access only when the request does not include the `BypassPolicyLockoutSafetyCheck` parameter. When the parameter is not used, the default value is `false`. This slightly weaker policy statement can be overridden in the rare case that a bypass is necessary.

```
{
  "Effect": "Allow",
  "Action": "kms:PutKeyPolicy",
  "Resource": "*",
  "Condition": {
    "Null": {
      "kms:BypassPolicyLockoutSafetyCheck": true
    }
  }
}
```

See also

- [kms:KeySpec](#)
- [kms:KeyOrigin](#)
- [kms:KeyUsage](#)

kms:CallerAccount

Amazon KMS condition keys	Condition type	Value type	API operations	Policy type
kms:CallerAccount	String	Single-valued	KMS key resource operations Custom key store operations	Key policies and IAM policies

You can use this condition key to allow or deny access to all identities (users and roles) in an Amazon Web Services account. In key policies, you use the `Principal` element to specify the identities to which the policy statement applies. The syntax for the `Principal` element does not provide a way to specify all identities in an Amazon Web Services account. But you can achieve this effect by combining this condition key with a `Principal` element that specifies all Amazon identities.

You can use it to control access to any *KMS key resource operation*, that is, any Amazon KMS operation that uses a particular KMS key. To identify the KMS key resource operations, in the [Actions and Resources Table](#), look for a value of `KMS key` in the `Resources` column for the operation. It is also valid for operations that manage [custom key stores](#).

For example, the following key policy statement demonstrates how to use the `kms:CallerAccount` condition key. This policy statement is in the key policy for the Amazon managed key for Amazon EBS. It combines a `Principal` element that specifies all Amazon identities with the `kms:CallerAccount` condition key to effectively allow access to all identities in Amazon Web Services account 111122223333. It contains an additional Amazon KMS condition key (`kms:ViaService`) to further limit the permissions by only allowing requests that come through Amazon EBS. For more information, see [kms:ViaService](#).

```
{
  "Sid": "Allow access through EBS for all principals in the account that are
authorized to use EBS",
  "Effect": "Allow",
  "Principal": {"AWS": "*"},
  "Condition": {
    "StringEquals": {
      "kms:CallerAccount": "111122223333",
      "kms:ViaService": "ec2.us-west-2.amazonaws.com"
    }
  },
  "Action": [
    "kms:Encrypt",
    "kms:Decrypt",
    "kms:ReEncrypt*",
    "kms:GenerateDataKey*",
    "kms:CreateGrant",
    "kms:DescribeKey"
  ],
  "Resource": "*"
}
```

kms:CustomerMasterKeySpec (deprecated)

The `kms:CustomerMasterKeySpec` condition key is deprecated. Instead, use the [kms:KeySpec](#) condition key.

The `kms:CustomerMasterKeySpec` and `kms:KeySpec` condition keys work the same way. Only the names differ. We recommend that you use `kms:KeySpec`. However, to avoid breaking changes, Amazon KMS supports both condition keys.

kms:CustomerMasterKeyUsage (deprecated)

The `kms:CustomerMasterKeyUsage` condition key is deprecated. Instead, use the [kms:KeyUsage](#) condition key.

The `kms:CustomerMasterKeyUsage` and `kms:KeyUsage` condition keys work the same way. Only the names differ. We recommend that you use `kms:KeyUsage`. However, to avoid breaking changes, Amazon KMS supports both condition keys.

kms:DataKeyPairSpec

Amazon KMS condition keys	Condition type	Value type	API operations	Policy type
kms:DataKeyPairSpec	String	Single-valued	GenerateDataKeyPair GenerateDataKeyPairWithoutPlaintext	Key policies and IAM policies

You can use this condition key to control access to the [GenerateDataKeyPair](#) and [GenerateDataKeyPairWithoutPlaintext](#) operations based on the value of the `KeyPairSpec` parameter in the request. For example, you can allow users to generate only particular types of data key pairs.

The following example key policy statement uses the `kms:DataKeyPairSpec` condition key to allow users to use the KMS key to generate only RSA data key pairs.

```
{
  "Effect": "Allow",
  "Principal": {
    "AWS": "arn:aws:iam::111122223333:role/ExampleRole"
  },
  "Action": [
    "kms:GenerateDataKeyPair",
    "kms:GenerateDataKeyPairWithoutPlaintext"
  ],
  "Resource": "*",
  "Condition": {
    "StringLike": {
      "kms:DataKeyPairSpec": "RSA*"
    }
  }
}
```

See also

- [kms:KeySpec](#)
- [the section called “kms:EncryptionAlgorithm”](#)
- [the section called “kms:EncryptionContext:context-key”](#)
- [the section called “kms:EncryptionContextKeys”](#)

kms:EncryptionAlgorithm

Amazon KMS condition keys	Condition type	Value type	API operations	Policy type
kms:EncryptionAlgorithm	String	Single-valued	Decrypt Encrypt GeneratedDataKey GeneratedDataKeyPair GeneratedDataKeyPairWithoutPlaintext GeneratedDataKeyWithoutPlaintext ReEncrypt	Key policies and IAM policies

You can use the `kms:EncryptionAlgorithm` condition key to control access to cryptographic operations based on the encryption algorithm that is used in the operation. For the [Encrypt](#), [Decrypt](#), and [ReEncrypt](#) operations, it controls access based on the value of the [EncryptionAlgorithm](#) parameter in the request. For operations that generate data keys and data key pairs, it controls access based on the encryption algorithm that is used to encrypt the data key.

This condition key has no effect on operations performed outside of Amazon KMS, such as encrypting with the public key in an asymmetric KMS key pair outside of Amazon KMS.

EncryptionAlgorithm parameter in a request

To allow users to use only a particular encryption algorithm with a KMS key, use a policy statement with a Deny effect and a `StringNotEquals` condition operator. For example, the following example key policy statement prohibits principals who can assume the `ExampleRole` role from using this KMS key in the specified cryptographic operations unless the encryption algorithm in the request is `RSAES_OAEP_SHA_256`, an asymmetric encryption algorithm used with RSA KMS keys.

Unlike a policy statement that allows a user to use a particular encryption algorithm, a policy statement with a double-negative like this one prevents other policies and grants for this KMS key from allowing this role to use other encryption algorithms. The Deny in this key policy statement takes precedence over any key policy or IAM policy with an Allow effect, and it takes precedence over all grants for this KMS key and its principals.

```
{
  "Sid": "Allow only one encryption algorithm with this asymmetric KMS key",
  "Effect": "Deny",
  "Principal": {
    "AWS": "arn:aws:iam::111122223333:role/ExampleRole"
  },
  "Action": [
    "kms:Encrypt",
    "kms:Decrypt",
    "kms:ReEncrypt*"
  ],
  "Resource": "*",
  "Condition": {
    "StringNotEquals": {
      "kms:EncryptionAlgorithm": "RSAES_OAEP_SHA_256"
    }
  }
}
```

Encryption algorithm used for the operation

You can also use the `kms:EncryptionAlgorithm` condition key to control access to operations based on the encryption algorithm used in the operation, even when the algorithm isn't specified

in the request. This allows you to require or forbid the `SYMMETRIC_DEFAULT` algorithm, which might not be specified in a request because it's the default value.

This feature lets you use the `kms:EncryptionAlgorithm` condition key to control access to the operations that generate data keys and data key pairs. These operations use only symmetric encryption KMS keys and the `SYMMETRIC_DEFAULT` algorithm.

For example, this IAM policy limits its principals to symmetric encryption. It denies access to any KMS key in the example account for cryptographic operations unless the encryption algorithm specified in the request or used in the operation is `SYMMETRIC_DEFAULT`.

Including `GenerateDataKey*` adds [GenerateDataKey](#), [GenerateDataKeyWithoutPlaintext](#), [GenerateDataKeyPair](#), and [GenerateDataKeyPairWithoutPlaintext](#) to the permissions. The condition has no effect on these operations because they always use a symmetric encryption algorithm.

```
{
  "Sid": "AllowOnlySymmetricAlgorithm",
  "Effect": "Deny",
  "Action": [
    "kms:Encrypt",
    "kms:Decrypt",
    "kms:ReEncrypt*",
    "kms:GenerateDataKey*"
  ],
  "Resource": "arn:aws:kms:us-west-2:111122223333:key/*",
  "Condition": {
    "StringNotEquals": {
      "kms:EncryptionAlgorithm": "SYMMETRIC_DEFAULT"
    }
  }
}
```

See also

- [the section called “kms:MacAlgorithm”](#)
- [kms:SigningAlgorithm](#)

kms:EncryptionContext:context-key

Amazon KMS condition keys	Condition type	Value type	API operations	Policy type
kms:EncryptionContext:context-key	String	Single-valued	CreateGrant Encrypt Decrypt GenerateDataKey GenerateDataKeyPair GenerateDataKeyPairWithoutPlaintext GenerateDataKeyWithoutPlaintext ReEncrypt RetireGrant	Key policies and IAM policies

You can use the `kms:EncryptionContext:context-key` condition key to control access to a [symmetric encryption KMS key](#) based on the [encryption context](#) in a request for a [cryptographic operation](#). Use this condition key to evaluate both the key and the value in the encryption context pair. To evaluate only the encryption context keys or require an encryption context regardless of keys or values, use the [kms:EncryptionContextKeys](#) condition key.

Note

Condition key values must conform to the character rules for key policies and IAM policies. Some characters that are valid in an encryption context are not valid in policies. You might not be able to use this condition key to express all valid encryption context values. For details about key policy document rules, see [Key policy format](#). For details about IAM policy document rules, see [IAM name requirements](#) in the *IAM User Guide*.

You cannot specify an encryption context in a cryptographic operation with an [asymmetric KMS key](#) or an [HMAC KMS key](#). Asymmetric algorithms and MAC algorithms do not support an encryption context.

To use the `kms:EncryptionContext:context-key` condition key, replace the *context-key* placeholder with the encryption context key. Replace the *context-value* placeholder with the encryption context value.

```
"kms:EncryptionContext:context-key": "context-value"
```

For example, the following condition key specifies an encryption context in which the key is `AppName` and the value is `ExampleApp` (`AppName = ExampleApp`).

```
"kms:EncryptionContext:AppName": "ExampleApp"
```

This is a [single-valued condition key](#). The key in the condition key specifies a particular encryption context key (*context-key*). Although you can include multiple encryption context pairs in each API request, the encryption context pair with the specified *context-key* can have only one value. For example, the `kms:EncryptionContext:Department` condition key applies only to encryption context pairs with a `Department` key, and any given encryption context pair with the `Department` key can have only one value.

Do not use a set operator with the `kms:EncryptionContext:context-key` condition key. If you create a policy statement with an `Allow` action, the `kms:EncryptionContext:context-key` condition key, and the `ForAllValues` set operator, the condition allows requests with no encryption context and requests with encryption context pairs that are not specified in the policy condition.

⚠ Warning

Do not use a `ForAnyValue` or `ForAllValues` set operator with this single-valued condition key. These set operators can create a policy condition that does not require values you intend to require and allows values you intend to forbid.

If you create or update a policy that includes a `ForAllValues` set operator with the `kms:EncryptionContext:context-key`, Amazon KMS returns the following error message: `OverlyPermissiveCondition:EncryptionContext: Using the ForAllValues set operator with a single-valued condition key matches requests without the specified encryption context or with an unspecified encryption context. To fix, remove ForAllValues.`

To require a particular encryption context pair, use the `kms:EncryptionContext:context-key` condition key with the `StringEquals` operator .

The following example key policy statement allows principals who can assume the role to use the KMS key in a `GenerateDataKey` request only when the encryption context in the request includes the `AppName:ExampleApp` pair. Other encryption context pairs are permitted.

The key name is not case sensitive. The case sensitivity of the value is determined by the condition operator, such as `StringEquals`. For details, see [Case sensitivity of the encryption context condition](#).

```
{
  "Effect": "Allow",
  "Principal": {
    "AWS": "arn:aws:iam::111122223333:role/RoleForExampleApp"
  },
  "Action": "kms:GenerateDataKey",
  "Resource": "*",
  "Condition": {
    "StringEquals": {
      "kms:EncryptionContext:AppName": "ExampleApp"
    }
  }
}
```

To require an encryption context pair and forbid all other encryption context pairs, use both `kms:EncryptionContext:context-key` and [kms:EncryptionContextKeys](#) in the policy statement.

The following key policy statement uses the `kms:EncryptionContext:AppName` condition to require the `AppName=ExampleApp` encryption context pair in the request. It also uses a `kms:EncryptionContextKeys` condition key with the `ForAllValues` set operator to allow only the `AppName` encryption context key.

The `ForAllValues` set operator limits encryption context keys in the request to `AppName`. If the `kms:EncryptionContextKeys` condition with the `ForAllValues` set operator was used alone in a policy statement, this set operator would allow requests with no encryption context. However, if the request had no encryption context, the `kms:EncryptionContext:AppName` condition would fail. For details about the `ForAllValues` set operator, see [Using multiple keys and values](#) in the *IAM User Guide*.

```
{
  "Effect": "Allow",
  "Principal": {
    "AWS": "arn:aws:iam::111122223333:role/KeyUsers"
  },
  "Action": "kms:GenerateDataKey",
  "Resource": "*",
  "Condition": {
    "StringEquals": {
      "kms:EncryptionContext:AppName": "ExampleApp"
    },
    "ForAllValues:StringEquals": {
      "kms:EncryptionContextKeys": [
        "AppName"
      ]
    }
  }
}
```

You can also use this condition key to deny access to a KMS key for a particular operation. The following example key policy statement uses a `Deny` effect to forbid the principal from using the KMS key if the encryption context in the request includes a `Stage=Restricted` encryption context pair. This condition allows a request with other encryption context pairs, including encryption context pairs with the `Stage` key and other values, such as `Stage=Test`.

```
{
  "Effect": "Deny",
  "Principal": {
    "AWS": "arn:aws:iam::111122223333:role/RoleForExampleApp"
  }
}
```

```
  },
  "Action": "kms:GenerateDataKey",
  "Resource": "*",
  "Condition": {
    "StringEquals": {
      "kms:EncryptionContext:Stage": "Restricted"
    }
  }
}
```

Using multiple encryption context pairs

You can require or forbid multiple encryption context pairs. You can also require one of several encryption context pairs. For details about the logic used to interpret these conditions, see [Creating a condition with multiple keys or values](#) in the IAM User Guide.

Note

Earlier versions of this topic displayed policy statements that used the `ForAnyValue` and `ForAllValues` set operators with the `kms:EncryptionContext:context-key` condition key. Using a set operator with a [single-valued condition key](#) can result in policies that allow requests with no encryption context and unspecified encryption context pairs.

For example, a policy condition with the `Allow` effect, the `ForAllValues` set operator, and the `"kms:EncryptionContext:Department": "IT"` condition key does not limit the encryption context to the `"Department=IT"` pair. It allows requests with no encryption context and requests with unspecified encryption context pairs, such as `Stage=Restricted`.

Please review your policies and eliminate the set operator from any condition with `kms:EncryptionContext:context-key`. Attempts to create or update a policy with this format fail with an `OverlyPermissiveCondition` exception. To resolve the error, delete the set operator.

To require multiple encryption context pairs, list the pairs in the same condition.

The following example key policy statement requires two encryption context pairs, `Department=IT` and `Project=Alpha`. Because the conditions have different keys (`kms:EncryptionContext:Department` and `kms:EncryptionContext:Project`), they are implicitly connected by an AND operator. Other encryption context pairs are permitted, but not required.

```
{
  "Effect": "Allow",
  "Principal": {
    "AWS": "arn:aws:iam::111122223333:role/RoleForExampleApp"
  },
  "Action": "kms:Decrypt",
  "Resource": "*",
  "Condition": {
    "StringEquals": {
      "kms:EncryptionContext:Department": "IT",
      "kms:EncryptionContext:Project": "Alpha"
    }
  }
}
```

To require one encryption context pair OR another pair, place each condition key in a separate policy statement. The following example key policy requires `Department=IT` or `Project=Alpha` pairs, or both. Other encryption context pairs are permitted, but not required.

```
{
  "Effect": "Allow",
  "Principal": {
    "AWS": "arn:aws:iam::111122223333:role/RoleForExampleApp"
  },
  "Action": "kms:GenerateDataKey",
  "Resource": "*",
  "Condition": {
    "StringEquals": {
      "kms:EncryptionContext:Department": "IT"
    }
  }
},
{
  "Effect": "Allow",
  "Principal": {
    "AWS": "arn:aws:iam::111122223333:role/RoleForExampleApp"
  },
  "Action": "kms:GenerateDataKey",
  "Resource": "*",
  "Condition": {
    "StringEquals": {
      "kms:EncryptionContext:Project": "Alpha"
    }
  }
}
```



```

}
}
}

```

To require particular encryption pairs and exclude all other encryption context pairs, use both `kms:EncryptionContext:context-key` and [kms:EncryptionContextKeys](#) in the policy statement. The following key policy statement uses the `kms:EncryptionContext:context-key` condition to require an encryption context with both `Department=IT` and `Project=Alpha` pairs. It uses a `kms:EncryptionContextKeys` condition key with the `ForAllValues` set operator to allow only the `Department` and `Project` encryption context keys.

The `ForAllValues` set operator limits encryption context keys in the request to `Department` and `Project`. If it were used alone in a condition, this set operator would allow requests with no encryption context, but in this configuration, the `kms:EncryptionContext:context-key` in this condition would fail.

```

{
  "Effect": "Allow",
  "Principal": {
    "AWS": "arn:aws:iam::111122223333:role/RoleForExampleApp"
  },
  "Action": "kms:GenerateDataKey",
  "Resource": "*",
  "Condition": {
    "StringEquals": {
      "kms:EncryptionContext:Department": "IT",
      "kms:EncryptionContext:Project": "Alpha"
    },
    "ForAllValues:StringEquals": {
      "kms:EncryptionContextKeys": [
        "Department",
        "Project"
      ]
    }
  }
}

```

You can also forbid multiple encryption context pairs. The following example key policy statement uses a `Deny` effect to forbid the principal from using the KMS keys if the encryption context in the request includes a `Stage=Restricted` or `Stage=Production` pair.

Multiple values (Restricted and Production) for the same key (kms:EncryptionContext:Stage) are implicitly connected by a OR. For details, see [Evaluation logic for conditions with multiple keys or values](#) in the *IAM User Guide*.

```
{
  "Effect": "Deny",
  "Principal": {
    "AWS": "arn:aws:iam::111122223333:role/RoleForExampleApp"
  },
  "Action": "kms:GenerateDataKey",
  "Resource": "*",
  "Condition": {
    "StringEquals": {
      "kms:EncryptionContext:Stage": [
        "Restricted",
        "Production"
      ]
    }
  }
}
```

Case sensitivity of the encryption context condition

The encryption context that is specified in a decryption operation must be an exact, case-sensitive match for the encryption context that is specified in the encryption operation. Only the order of pairs in an encryption context with multiple pair can vary.

However, in policy conditions, the condition key is not case sensitive. The case sensitivity of the condition value is determined by the [policy condition operator](#) that you use, such as `StringEquals` or `StringEqualsIgnoreCase`.

As such, the condition key, which consists of the `kms:EncryptionContext:` prefix and the *context-key* replacement, is not case sensitive. A policy that uses this condition does not check the case of either element of the condition key. The case sensitivity of the value, that is, the *context-value* replacement, is determined by the policy condition operator.

For example, the following policy statement allows the operation when the encryption context includes an Appname key, regardless of its capitalization. The `StringEquals` condition requires that `ExampleApp` be capitalized as it is specified.

```
{
```

```

"Effect": "Allow",
"Principal": {
  "AWS": "arn:aws:iam::111122223333:role/RoleForExampleApp"
},
"Action": "kms:Decrypt",
"Resource": "*",
"Condition": {
  "StringEquals": {
    "kms:EncryptionContext:Appname": "ExampleApp"
  }
}
}

```

To require a case-sensitive encryption context key, use the [kms:EncryptionContextKeys](#) policy condition with a case-sensitive condition operator, such as `StringEquals`. In this policy condition, because the encryption context key is the value in this policy condition, its case sensitivity is determined by the condition operator.

```

{
  "Effect": "Allow",
  "Principal": {
    "AWS": "arn:aws:iam::111122223333:role/RoleForExampleApp"
  },
  "Action": "kms:GenerateDataKey",
  "Resource": "*",
  "Condition": {
    "ForAnyValue:StringEquals": {
      "kms:EncryptionContextKeys": "AppName"
    }
  }
}

```

To require a case-sensitive evaluation of both the encryption context key and value, use the `kms:EncryptionContextKeys` and `kms:EncryptionContext:context-key` policy conditions together in the same policy statement. The case-sensitive condition operator (such as `StringEquals`) always applies to the value of the condition. The encryption context key (such as `AppName`) is the value of the `kms:EncryptionContextKeys` condition. The encryption context value (such as `ExampleApp`) is the value of the `kms:EncryptionContext:context-key` condition.

For example, in the following example key policy statement, because the `StringEquals` operator is case sensitive, both the encryption context key and the encryption context value are case sensitive.

```
{
  "Effect": "Allow",
  "Principal": {
    "AWS": "arn:aws:iam::111122223333:role/RoleForExampleApp"
  },
  "Action": "kms:GenerateDataKey",
  "Resource": "*",
  "Condition": {
    "ForAnyValue:StringEquals": {
      "kms:EncryptionContextKeys": "AppName"
    },
    "StringEquals": {
      "kms:EncryptionContext:AppName": "ExampleApp"
    }
  }
}
```

Using variables in an encryption context condition

The key and value in an encryption context pair must be simple literal strings. They cannot be integers or objects, or any type that is not fully resolved. If you use a different type, such as an integer or float, Amazon KMS interprets it as a literal string.

```
"encryptionContext": {
  "department": "10103.0"
}
```

However, the value of the `kms:EncryptionContext:context-key` condition key can be an [IAM policy variable](#). These policy variables are resolved at runtime based on values in the request. For example, `aws:CurrentTime` resolves to the time of the request and `aws:username` resolves to the friendly name of the caller.

You can use these policy variables to create a policy statement with a condition that requires very specific information in an encryption context, such as the caller's user name. Because it contains a variable, you can use the same policy statement for all users who can assume the role. You don't have to write a separate policy statement for each user.

Consider a situation where you want to all users who can assume a role to use the same KMS key to encrypt and decrypt their data. However, you want to allow them to decrypt only the data that they encrypted. Start by requiring that every request to Amazon KMS include an encryption context where the key is `user` and the value is the caller's Amazon user name, such as the following one.

```
"encryptionContext": {
  "user": "bob"
}
```

Then, to enforce this requirement, you can use a policy statement like the one in the following example. This policy statement gives the `TestTeam` role permission to encrypt and decrypt data with the KMS key. However, the permission is valid only when the encryption context in the request includes a `"user": "<username>"` pair. To represent the user name, the condition uses the [aws:username](#) policy variable.

When the request is evaluated, the caller's user name replaces the variable in the condition. As such, the condition requires an encryption context of `"user": "bob"` for "bob" and `"user": "alice"` for "alice."

```
{
  "Effect": "Allow",
  "Principal": {
    "AWS": "arn:aws:iam::111122223333:role/TestTeam"
  },
  "Action": [
    "kms:Decrypt",
    "kms:Encrypt"
  ],
  "Resource": "*",
  "Condition": {
    "StringEquals": {
      "kms:EncryptionContext:user": "${aws:username}"
    }
  }
}
```

You can use an IAM policy variable only in the value of the `kms:EncryptionContext:context-key` condition key. You cannot use a variable in the key.

You can also use [provider-specific context keys](#) in variables. These context keys uniquely identify users who logged into Amazon by using web identity federation.

Like all variables, these variables can be used only in the `kms:EncryptionContext:context-key` policy condition, not in the actual encryption context. And they can be used only in the value of the condition, not in the key.

For example, the following key policy statement is similar to the previous one. However, the condition requires an encryption context where the key is `sub` and the value uniquely identifies a user logged into an Amazon Cognito user pool. For details about identifying users and roles in Amazon Cognito, see [IAM Roles](#) in the [Amazon Cognito Developer Guide](#).

```
{
  "Effect": "Allow",
  "Principal": {
    "AWS": "arn:aws:iam::111122223333:role/TestTeam"
  },
  "Action": [
    "kms:Decrypt",
    "kms:Encrypt"
  ],
  "Resource": "*",
  "Condition": {
    "StringEquals": {
      "kms:EncryptionContext:sub": "${cognito-identity.amazonaws.com:sub}"
    }
  }
}
```

See also


- [the section called “kms:EncryptionContextKeys”](#)
- [the section called “kms:GrantConstraintType”](#)

kms:EncryptionContextKeys

Amazon KMS condition keys	Condition type	Value type	API operations	Policy type
kms:EncryptionContextKeys	String (list)	Multi-valued	CreateGrant Decrypt Encrypt GenerateDataKey GenerateDataKeyPair GenerateDataKeyPairWithoutPlaintext GenerateDataKeyWithoutPlaintext ReEncrypt RetireGrant	Key policies and IAM policies

You can use the `kms:EncryptionContextKeys` condition key to control access to a [symmetric encryption KMS key](#) based on the [encryption context](#) in a request for a cryptographic operation. Use this condition key to evaluate only the key in each encryption context pair. To evaluate both the key and the value in the encryption context, use the `kms:EncryptionContext:context-key` condition key.

You cannot specify an encryption context in a cryptographic operation with an [asymmetric KMS key](#) or an [HMAC KMS key](#). Asymmetric algorithms and MAC algorithms do not support an encryption context.

 **Note**

Condition key values, including an encryption context key, must conform to the character and encoding rules for Amazon KMS key policies. You might not be able to use this condition key to express all valid encryption context keys. For details about key policy document rules, see [Key policy format](#). For details about IAM policy document rules, see [IAM name requirements](#) in the *IAM User Guide*.

This is a [multi-valued condition key](#). You can specify multiple encryption context pairs in each API request. `kms:EncryptionContextKeys` compares the encryption context keys in the request to the set of encryption context keys in the policy. To determine how these sets are compared, you must provide a `ForAnyValue` or `ForAllValues` set operator in the policy condition. For details about the set operators, see [Using multiple keys and values](#) in the IAM User Guide.

- `ForAnyValue`: At least one encryption context key in the request must match an encryption context key in the policy condition. Other encryption context keys are permitted. If the request has no encryption context, the condition is not satisfied.
- `ForAllValues`: Every encryption context key in the request must match an encryption context key in the policy condition. This set operator limits the encryption context keys to those in the policy condition. It doesn't require any encryption context keys, but it forbids unspecified encryption context keys.

The following example key policy statement uses the `kms:EncryptionContextKeys` condition key with the `ForAnyValue` set operator. This policy statement allows use of a KMS key for the specified operations, but only when at least one of the encryption context pairs in the request includes the `AppName` key, regardless of its value.

For example, this key policy statement allows a `GenerateDataKey` request with two encryption context pairs, `AppName=Helper` and `Project=Alpha`, because the first encryption context pair satisfies the condition. A request with only `Project=Alpha` or with no encryption context would fail.

Because the [StringEquals](#) condition operation is case sensitive, this policy statement requires the spelling and case of the encryption context key. But you can use a condition operator that ignores the case of the key, such as `StringEqualsIgnoreCase`.

```
{
  "Effect": "Allow",
  "Principal": {
    "AWS": "arn:aws:iam::111122223333:role/RoleForExampleApp"
  },
  "Action": [
    "kms:Encrypt",
    "kms:GenerateDataKey*"
  ],
  "Resource": "*",
  "Condition": {
    "ForAnyValue:StringEquals": {
      "kms:EncryptionContextKeys": "AppName"
    }
  }
}
```

You can also use the `kms:EncryptionContextKeys` condition key to require an encryption context (any encryption context) in cryptographic operations that use the KMS key;

The following example key policy statement uses the `kms:EncryptionContextKeys` condition key with the [Null condition operator](#) to allow access to a KMS key only when encryption context in the API request is not null. This condition does not check the keys or values of the encryption context. It only verifies that the encryption context exists.

```
{
  "Effect": "Allow",
  "Principal": {
    "AWS": "arn:aws:iam::111122223333:role/RoleForExampleApp"
  },
  "Action": [
    "kms:Encrypt",
    "kms:GenerateDataKey*"
  ],
  "Resource": "*",
  "Condition": {
    "Null": {
      "kms:EncryptionContextKeys": false
    }
  }
}
```

```

    }
  }
}

```

See also

- [kms:EncryptionContext:context-key](#)
- [kms:GrantConstraintType](#)

kms:ExpirationModel

Amazon KMS condition keys	Condition type	Value type	API operations	Policy type
kms:ExpirationModel	String	Single-valued	ImportKeyMaterial	Key policies and IAM policies

The `kms:ExpirationModel` condition key controls access to the [ImportKeyMaterial](#) operation based on the value of the [ExpirationModel](#) parameter in the request.

`ExpirationModel` is an optional parameter that determines whether the imported key material expires. Valid values are `KEY_MATERIAL_EXPIRES` and `KEY_MATERIAL_DOES_NOT_EXPIRE`. `KEY_MATERIAL_EXPIRES` is the default value.

The expiration date and time is determined by the value of the [ValidTo](#) parameter. The `ValidTo` parameter is required unless the value of the `ExpirationModel` parameter is `KEY_MATERIAL_DOES_NOT_EXPIRE`. You can also use the [kms:ValidTo](#) condition key to require a particular expiration date as a condition for access.

The following example policy statement uses the `kms:ExpirationModel` condition key to allow users to import key material into a KMS key only when the request includes the `ExpirationModel` parameter and its value is `KEY_MATERIAL_DOES_NOT_EXPIRE`.

```

{
  "Effect": "Allow",
  "Principal": {
    "AWS": "arn:aws:iam::111122223333:role/RoleForExampleApp"
  }
}

```

```
  },
  "Action": "kms:ImportKeyMaterial",
  "Resource": "*",
  "Condition": {
    "StringEquals": {
      "kms:ExpirationModel": "KEY_MATERIAL_DOES_NOT_EXPIRE"
    }
  }
}
```

You can also use the `kms:ExpirationModel` condition key to allow users to import key material only when the key material expires. The following example key policy statement uses the `kms:ExpirationModel` condition key with the [Null condition operator](#) to allow users to import key material only when the request does not have an `ExpirationModel` parameter. The default value for `ExpirationModel` is `KEY_MATERIAL_EXPIRES`.

```
{
  "Effect": "Allow",
  "Principal": {
    "AWS": "arn:aws:iam::111122223333:role/RoleForExampleApp"
  },
  "Action": "kms:ImportKeyMaterial",
  "Resource": "*",
  "Condition": {
    "Null": {
      "kms:ExpirationModel": true
    }
  }
}
```

See also

- [kms:ValidTo](#)
- [kms:WrappingAlgorithm](#)
- [kms:WrappingKeySpec](#)

kms:GrantConstraintType

Amazon KMS condition keys	Condition type	Value type	API operations	Policy type
kms:GrantConstraintType	String	Single-valued	CreateGrant RetireGrant	Key policies and IAM policies

You can use this condition key to control access to the [CreateGrant](#) operation based on the type of [grant constraint](#) in the request.

When you create a grant, you can optionally specify a grant constraint to allow the operations that the grant permit only when a particular [encryption context](#) is present. The grant constraint can be one of two types: `EncryptionContextEquals` or `EncryptionContextSubset`. You can use this condition key to check that the request contains one type or the other.

Important

Do not include confidential or sensitive information in this field. This field may be displayed in plaintext in CloudTrail logs and other output.

The following example key policy statement uses the `kms:GrantConstraintType` condition key to allow users to create grants only when the request includes an `EncryptionContextEquals` grant constraint. The example shows a policy statement in a key policy.

```
{
  "Effect": "Allow",
  "Principal": {
    "AWS": "arn:aws:iam::111122223333:role/RoleForExampleApp"
  },
  "Action": "kms:CreateGrant",
  "Resource": "*",
  "Condition": {
    "StringEquals": {
      "kms:GrantConstraintType": "EncryptionContextEquals"
    }
  }
}
```

}

See also

- [kms:EncryptionContext:context-key](#)
- [kms:EncryptionContextKeys](#)
- [kms:GrantIsForAWSResource](#)
- [kms:GrantOperations](#)
- [kms:GranteePrincipal](#)
- [kms:RetiringPrincipal](#)

kms:GrantIsForAWSResource

Amazon KMS condition keys	Condition type	Value type	API operations	Policy type
<code>kms:GrantIsForAWSResource</code>	Boolean	Single-valued	<code>CreateGrant</code> <code>ListGrants</code> <code>RevokeGrant</code>	Key policies and IAM policies

Allows or denies permission for the [CreateGrant](#), [ListGrants](#), or [RevokeGrant](#) operations only when an [Amazon service integrated with Amazon KMS](#) calls the operation on the user's behalf. This policy condition doesn't allow the user to call these grant operations directly.

The following example key policy statement uses the `kms:GrantIsForAWSResource` condition key. It allows Amazon services that are integrated with Amazon KMS, such as Amazon EBS, to create grants on this KMS key on behalf of the specified principal.

```
{
  "Effect": "Allow",
  "Principal": {
    "AWS": "arn:aws:iam::111122223333:role/ExampleRole"
  },
  "Action": "kms:CreateGrant",
  "Resource": "*",
}
```

```

"Condition": {
  "Bool": {
    "kms:GrantIsForAWSResource": true
  }
}
}

```

See also

- [kms:GrantConstraintType](#)
- [kms:GrantOperations](#)
- [kms:GranteePrincipal](#)
- [kms:RetiringPrincipal](#)

kms:GrantOperations

Amazon KMS condition keys	Condition type	Value type	API operations	Policy type
kms:GrantOperations	String	Multi-valued	CreateGrant	Key policies and IAM policies

You can use this condition key to control access to the [CreateGrant](#) operation based on the [grant operations](#) in the request. For example, you can allow users to create grants that delegate permission to encrypt but not decrypt. For more information about grants, see [Using grants](#).

This is a [multi-valued condition key](#). `kms:GrantOperations` compares the set of grant operations in the `CreateGrant` request to the set of grant operations in the policy. To determine how these sets are compared, you must provide a `ForAnyValue` or `ForAllValues` set operator in the policy condition. For details about the set operators, see [Using multiple keys and values](#) in the IAM User Guide.

- `ForAnyValue`: At least one grant operation in the request must match one of the grant operations in the policy condition. Other grant operations are permitted.
- `ForAllValues`: Every grant operation in the request must match a grant operation in the policy condition. This set operator limits the grant operations to those specified in the policy condition. It doesn't require any grant operations, but it forbids unspecified grant operations.

`ForAllValues` also returns true when there are no grant operations in the request, but `CreateGrant` doesn't permit it. If the `Operations` parameter is missing or has a null value, the `CreateGrant` request fails.

The following example key policy statement uses the `kms:GrantOperations` condition key to create grants only when the grant operations are `Encrypt`, `ReEncryptTo`, or both. If the grant includes any other operations, the `CreateGrant` request fails.

```
{
  "Effect": "Allow",
  "Principal": {
    "AWS": "arn:aws:iam::111122223333:role/ExampleRole"
  },
  "Action": "kms:CreateGrant",
  "Resource": "*",
  "Condition": {
    "ForAllValues:StringEquals": {
      "kms:GrantOperations": [
        "Encrypt",
        "ReEncryptTo"
      ]
    }
  }
}
```

If you change the set operator in the policy condition to `ForAnyValue`, the policy statement would require that at least one of the grant operations in the grant is `Encrypt` or `ReEncryptTo`, but it would allow other grant operations, such as `Decrypt` or `ReEncryptFrom`.

See also

- [kms:GrantConstraintType](#)
- [kms:GrantIsForAWSResource](#)
- [kms:GranteePrincipal](#)
- [kms:RetiringPrincipal](#)

kms:GranteePrincipal

Amazon KMS condition keys	Condition type	Value type	API operations	Policy type
kms:GranteePrincipal	String	Single-valued	CreateGrant	IAM and key policies

You can use this condition key to control access to the [CreateGrant](#) operation based on the value of the [GranteePrincipal](#) parameter in the request. For example, you can to create grants to use a KMS key only when the grantee principal in the CreateGrant request matches the principal specified in the condition statement.

To specify the grantee principal, use the Amazon Resource Name (ARN) of an Amazon principal. Valid principals include Amazon Web Services accounts, IAM users, IAM roles, federated users, and assumed role users. For help with the ARN syntax for a principal, see [IAM ARNs](#) in the *IAM User Guide*.

The following example key policy statement uses the `kms:GranteePrincipal` condition key to to create grants for a KMS key only when the grantee principal in the grant is the `LimitedAdminRole`.

```
{
  "Effect": "Allow",
  "Principal": {
    "AWS": "arn:aws:iam::111122223333:role/ExampleRole"
  },
  "Action": "kms:CreateGrant",
  "Resource": "*",
  "Condition": {
    "StringEquals": {
      "kms:GranteePrincipal": "arn:aws:iam::111122223333:role/LimitedAdminRole"
    }
  }
}
```

See also

- [kms:GrantConstraintType](#)
- [kms:GrantIsForAWSResource](#)
- [kms:GrantOperations](#)
- [kms:RetiringPrincipal](#)

kms:KeyAgreementAlgorithm

Amazon KMS condition keys	Condition type	Value type	API operations	Policy type
kms:KeyAgreementAlgorithm	String	Single-valued	DeriveSharedSecret	Key policies and IAM policies

You can use the `kms:KeyAgreementAlgorithm` condition key to control access to the [DeriveSharedSecret](#) operation based on the value of the `KeyAgreementAlgorithm` parameter in the request. The only valid value for `KeyAgreementAlgorithm` is `ECDH`.

For example, the following key policy statement uses the `kms:KeyAgreementAlgorithm` condition key to deny all access to `DeriveSharedSecret` unless the `KeyAgreementAlgorithm` is `ECDH`.

```
{
  "Effect": "Deny",
  "Principal": {
    "AWS": "arn:aws:iam::111122223333:role/ExampleRole"
  },
  "Action": "kms:DeriveSharedSecret",
  "Resource": "*",
  "Condition": {
    "StringNotEquals": {
      "kms:KeyAgreementAlgorithm": "ECDH"
    }
  }
}
```

See also

- [the section called “kms:KeyUsage”](#)

kms:KeyOrigin

Amazon KMS condition keys	Condition type	Value type	API operations	Policy type
kms:KeyOrigin	String	Single-valued	CreateKey KMS key resource operations	IAM policies Key policies and IAM policies

The `kms:KeyOrigin` condition key controls access to operations based on the value of the `Origin` property of the KMS key that is created by or used in the operation. It works as a resource condition or a request condition.

You can use this condition key to control access to the [CreateKey](#) operation based on the value of the [Origin](#) parameter in the request. Valid values for `Origin` are `AWS_KMS`, `AWS_CLOUDHSM`, and `EXTERNAL`.

For example, you can create a KMS key only when the key material is generated in Amazon KMS (`AWS_KMS`), only when the key material is generated in an Amazon CloudHSM cluster that is associated with a [custom key store](#) (`AWS_CLOUDHSM`), or only when the [key material is imported](#) from an external source (`EXTERNAL`).

The following example key policy statement uses the `kms:KeyOrigin` condition key to create a KMS key only when Amazon KMS creates the key material.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::111122223333:role/ExampleRole"
      },
      "Action": "kms:CreateKey",
      "Resource": "*"
    }
  ]
}
```

```

    "Condition": {
      "StringEquals": {
        "kms:KeyOrigin": "AWS_KMS"
      }
    },
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::111122223333:role/ExampleRole"
      },
      "Action": [
        "kms:Encrypt",
        "kms:Decrypt",
        "kms:GenerateDataKey",
        "kms:GenerateDataKeyWithoutPlaintext",
        "kms:GenerateDataKeyPair",
        "kms:GenerateDataKeyPairWithoutPlaintext",
        "kms:ReEncrypt*"
      ],
      "Resource": "arn:aws:kms:us-west-2:111122223333:key/*",
      "Condition": {
        "StringEquals": {
          "kms:KeyOrigin": "AWS_CLOUDHSM"
        }
      }
    }
  ]
}

```

You can also use the `kms:KeyOrigin` condition key to control access to operations that use or manage a KMS key based on the `Origin` property of the KMS key used for the operation. The operation must be a *KMS key resource operation*, that is, an operation that is authorized for a particular KMS key. To identify the KMS key resource operations, in the [Actions and Resources Table](#), look for a value of `KMS key` in the Resources column for the operation.

For example, the following IAM policy allows principals to perform the specified KMS key resource operations, but only with KMS keys in the account that were created in a custom key store.

```

{
  "Effect": "Allow",
  "Action": [
    "kms:Encrypt",

```

```

    "kms:Decrypt",
    "kms:GenerateDataKey",
    "kms:GenerateDataKeyWithoutPlaintext",
    "kms:GenerateDataKeyPair",
    "kms:GenerateDataKeyPairWithoutPlaintext",
    "kms:ReEncrypt*"
  ],
  "Resource": "arn:aws:kms:us-west-2:111122223333:key/*",
  "Condition": {
    "StringEquals": {
      "kms:KeyOrigin": "AWS_CLOUDHSM"
    }
  }
}

```

See also

- [kms:ByPassPolicyLockoutSafetyCheck](#)
- [kms:KeySpec](#)
- [kms:KeyUsage](#)

kms:KeySpec

Amazon KMS condition keys	Condition type	Value type	API operations	Policy type
kms:KeySpec	String	Single-valued	CreateKey KMS key resource operations	IAM policies Key policies and IAM policies

The `kms:KeySpec` condition key controls access to operations based on the value of the `KeySpec` property of the KMS key that is created by or used in the operation.

You can use this condition key in an IAM policy to control access to the [CreateKey](#) operation based on the value of the [KeySpec](#) parameter in a `CreateKey` request. For example, you can use this condition to allow users to create only symmetric encryption KMS keys or only HMAC KMS keys.

The following example IAM policy statement uses the `kms:KeySpec` condition key to allow the principals to create only RSA asymmetric KMS keys. The permission is valid only when the `KeySpec` in the request begins with `RSA_`.

```
{
  "Effect": "Allow",
  "Action": "kms:CreateKey",
  "Resource": "*",
  "Condition": {
    "StringLike": {
      "kms:KeySpec": "RSA_*"
    }
  }
}
```

You can also use the `kms:KeySpec` condition key to control access to operations that use or manage a KMS key based on the `KeySpec` property of the KMS key used for the operation. The operation must be a *KMS key resource operation*, that is, an operation that is authorized for a particular KMS key. To identify the KMS key resource operations, in the [Actions and Resources Table](#), look for a value of `KMS key` in the `Resources` column for the operation.

For example, the following IAM policy allows principals to perform the specified KMS key resource operations, but only with symmetric encryption KMS keys in the account.

```
{
  "Effect": "Allow",
  "Action": [
    "kms:Encrypt",
    "kms:Decrypt",
    "kms:ReEncrypt*",
    "kms:DescribeKey"
  ],
  "Resource": "arn:aws:kms:us-west-2:111122223333:key/*",
  "Condition": {
    "StringEquals": {
      "kms:KeySpec": "SYMMETRIC_DEFAULT"
    }
  }
}
```

See also

- [kms:BypassPolicyLockoutSafetyCheck](#)
- [kms:CustomerMasterKeySpec](#) (deprecated)
- [kms:DataKeyPairSpec](#)
- [kms:KeyOrigin](#)
- [kms:KeyUsage](#)

kms:KeyUsage

Amazon KMS condition keys	Condition type	Value type	API operations	Policy type
kms : KeyUsage	String	Single-valued	CreateKey KMS key resource operations	IAM policies Key policies and IAM policies

The kms : KeyUsage condition key controls access to operations based on the value of the KeyUsage property of the KMS key that is created by or used in the operation.

You can use this condition key to control access to the [CreateKey](#) operation based on the value of the [KeyUsage](#) parameter in the request. Valid values for KeyUsage are ENCRYPT_DECRYPT, SIGN_VERIFY, GENERATE_VERIFY_MAC, and KEY_AGREEMENT.

For example, you can create a KMS key only when the KeyUsage is ENCRYPT_DECRYPT or deny a user permission when the KeyUsage is SIGN_VERIFY.

The following example IAM policy statement uses the kms : KeyUsage condition key to create a KMS key only when the KeyUsage is ENCRYPT_DECRYPT.

```
{
  "Effect": "Allow",
  "Action": "kms:CreateKey",
  "Resource": "*",
  "Condition": {
    "StringEquals": {
```

```
    "kms:KeyUsage": "ENCRYPT_DECRYPT"  
  }  
}  
}
```

You can also use the `kms:KeyUsage` condition key to control access to operations that use or manage a KMS key based on the `KeyUsage` property of the KMS key in the operation. The operation must be a *KMS key resource operation*, that is, an operation that is authorized for a particular KMS key. To identify the KMS key resource operations, in the [Actions and Resources Table](#), look for a value of `KMS` key in the Resources column for the operation.

For example, the following IAM policy allows principals to perform the specified KMS key resource operations, but only with KMS keys in the account that are used for signing and verification.

```
{  
  "Effect": "Allow",  
  "Action": [  
    "kms:CreateGrant",  
    "kms:DescribeKey",  
    "kms:GetPublicKey",  
    "kms:ScheduleKeyDeletion"  
  ],  
  "Resource": "arn:aws:kms:us-west-2:111122223333:key/*",  
  "Condition": {  
    "StringEquals": {  
      "kms:KeyUsage": "SIGN_VERIFY"  
    }  
  }  
}
```

See also

- [kms:BypassPolicyLockoutSafetyCheck](#)
- [kms:CustomerMasterKeyUsage \(deprecated\)](#)
- [kms:KeyOrigin](#)
- [kms:KeySpec](#)

kms:MacAlgorithm

Amazon KMS condition keys	Condition type	Value type	API operations	Policy type
kms:MacAlgorithm	String	Single-valued	GenerateMac VerifyMac	Key policies and IAM policies

You can use the `kms:MacAlgorithm` condition key to control access to the [GenerateMac](#) and [VerifyMac](#) operations based on the value of the `MacAlgorithm` parameter in the request.

The following example key policy allows users who can assume the `testers` role to use the HMAC KMS key to generate and verify HMAC tags only when the MAC algorithm in the request is `HMAC_SHA_384` or `HMAC_SHA_512`. This policy uses two separate policy statements each with its own condition. If you specify more than one MAC algorithm in a single condition statement, the condition requires both algorithms, instead of one or the other.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::111122223333:role/testers"
      },
      "Action": [
        "kms:GenerateMac",
        "kms:VerifyMac"
      ],
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "kms:MacAlgorithm": "HMAC_SHA_384"
        }
      }
    },
    {
      "Effect": "Allow",
      "Principal": {
```



```

    "AWS": "arn:aws:iam::111122223333:role/testers"
  },
  "Action": [
    "kms:GenerateMac",
    "kms:VerifyMac"
  ],
  "Resource": "*",
  "Condition": {
    "StringEquals": {
      "kms:MacAlgorithm": "HMAC_SHA_512"
    }
  }
}
]
}

```

See also

- [the section called “kms:EncryptionAlgorithm”](#)
- [kms:SigningAlgorithm](#)

kms:MessageType

Amazon KMS condition keys	Condition type	Value type	API operations	Policy type
kms:MessageType	String	Single-valued	Sign Verify	Key policies and IAM policies

The `kms:MessageType` condition key controls access to the [Sign](#) and [Verify](#) operations based on the value of the `MessageType` parameter in the request. Valid values for `MessageType` are `RAW` and `DIGEST`.

For example, the following key policy statement uses the `kms:MessageType` condition key to use an asymmetric KMS key to sign a message, but not a message digest.

```

{
  "Effect": "Allow",

```

```

"Principal": {
  "AWS": "arn:aws:iam::111122223333:role/ExampleRole"
},
"Action": "kms:Sign",
"Resource": "*",
"Condition": {
  "StringEquals": {
    "kms:MessageType": "RAW"
  }
}
}

```

See also

- [the section called “kms:SigningAlgorithm”](#)

kms:MultiRegion

Amazon KMS condition keys	Condition type	Value type	API operations	Policy type
kms:MultiRegion	Boolean	Single-valued	CreateKey KMS key resource operations	Key policies and IAM policies

You can use this condition key to allow operations only on single-Region keys or only on [multi-Region keys](#). The `kms:MultiRegion` condition key controls access to Amazon KMS operations on KMS keys and to the [CreateKey](#) operation based on the value of the `MultiRegion` property of the KMS key. Valid values are `true` (multi-Region), and `false` (single-Region). All KMS keys have a `MultiRegion` property.

For example, the following IAM policy statement uses the `kms:MultiRegion` condition key to allow principals to create only single-Region keys.

```

{
  "Effect": "Allow",
  "Action": "kms:CreateKey",

```

```

"Resource": "*",
"Condition": {
  "Bool": {
    "kms:MultiRegion": false
  }
}
}

```

kms:MultiRegionKeyType

Amazon KMS condition keys	Condition type	Value type	API operations	Policy type
kms:MultiRegionKeyType	String	Single-valued	CreateKey KMS key resource operations	Key policies and IAM policies

You can use this condition key to allow operations only on [multi-Region primary keys](#) or only on [multi-Region replica keys](#). The `kms:MultiRegionKeyType` condition key controls access to Amazon KMS operations on KMS keys and the [CreateKey](#) operation based on the `MultiRegionKeyType` property of the KMS key. The valid values are `PRIMARY` and `REPLICA`. Only multi-Region keys have a `MultiRegionKeyType` property.

Typically, you use the `kms:MultiRegionKeyType` condition key in an IAM policy to control access to multiple KMS keys. However, because a given multi-Region key can change to primary or replica, you might want to use this condition in a key policy to allow an operation only when the particular multi-Region key is a primary or replica key.

For example, the following IAM policy statement uses the `kms:MultiRegionKeyType` condition key to allow principals to schedule and cancel key deletion only on multi-Region replica keys in the specified Amazon Web Services account.

```

{
  "Effect": "Allow",
  "Action": [
    "kms:ScheduleKeyDeletion",

```

```

    "kms:CancelKeyDeletion"
  ],
  "Resource": "arn:aws:kms:*:111122223333:key/*",
  "Condition": {
    "StringEquals": {
      "kms:MultiRegionKeyType": "REPLICA"
    }
  }
}

```

To allow or deny access to all multi-Region keys, you can use both values or a null value with `kms:MultiRegionKeyType`. However, the [kms:MultiRegion](#) condition key is recommended for that purpose.

kms:PrimaryRegion

Amazon KMS condition keys	Condition type	Value type	API operations	Policy type
<code>kms:PrimaryRegion</code>	String (list)	Single-valued	<code>UpdatePrimaryRegion</code>	Key policies and IAM policies

You can use this condition key to limit the destination Regions in an [UpdatePrimaryRegion](#) operation. These are Amazon Web Services Regions that can host your multi-Region primary keys.

The `kms:PrimaryRegion` condition key controls access to the [UpdatePrimaryRegion](#) operation based on the value of the `PrimaryRegion` parameter. The `PrimaryRegion` parameter specifies the Amazon Web Services Region of the [multi-Region replica key](#) that is being promoted to primary. The value of the condition is one or more Amazon Web Services Region names, such as `us-east-1` or `ap-southeast-2`, or Region name patterns, such as `eu-*`

For example, the following key policy statement uses the `kms:PrimaryRegion` condition key to allow principals to update the primary region of a multi-Region key to one of the four specified Regions.

```

{
  "Effect": "Allow",
  "Action": "kms:UpdatePrimaryRegion",
  "Principal": {

```

```

    "AWS": "arn:aws:iam::111122223333:role/Developer"
  },
  "Resource": "*",
  "Condition": {
    "StringEquals": {
      "kms:PrimaryRegion": [
        "us-east-1",
        "us-west-2",
        "eu-west-3",
        "ap-southeast-2"
      ]
    }
  }
}

```

kms:ReEncryptOnSameKey

Amazon KMS condition keys	Condition type	Value type	API operations	Policy type
kms:ReEncryptOnSameKey	Boolean	Single-valued	ReEncrypt	Key policies and IAM policies

You can use this condition key to control access to the [ReEncrypt](#) operation based on whether the request specifies a destination KMS key that is the same one used for the original encryption.

For example, the following key policy statement uses the `kms:ReEncryptOnSameKey` condition key to to reencrypt only when the destination KMS key is the same one used for the original encryption.

```

{
  "Effect": "Allow",
  "Principal": {
    "AWS": "arn:aws:iam::111122223333:role/ExampleRole"
  },
  "Action": "kms:ReEncrypt*",
  "Resource": "*",
  "Condition": {
    "Bool": {

```

```

    "kms:ReEncryptOnSameKey": true
  }
}
}

```

kms:RequestAlias

Amazon KMS condition keys	Condition type	Value type	API operations	Policy type
kms:RequestAlias	String (list)	Single-valued	Cryptographic operations DescribeKey GetPublicKey	Key policies and IAM policies

You can use this condition key to allow an operation only when the request uses a particular alias to identify the KMS key. The `kms:RequestAlias` condition key controls access to a KMS key used in a cryptographic operation, `GetPublicKey`, or `DescribeKey` based on the [alias](#) that identifies that KMS key in the request. (This policy condition has no effect on the [GenerateRandom](#) operation because the operation doesn't use a KMS key or alias.)

This condition supports [attribute-based access control](#) (ABAC) in Amazon KMS, which lets you control access to KMS keys based on the tags and aliases of a KMS key. You can use tags and aliases to allow or deny access to a KMS key without changing policies or grants. For details, see [ABAC for Amazon KMS](#).

To specify the alias in this policy condition, use an [alias name](#), such as `alias/project-alpha`, or an alias name pattern, such as `alias/*test*`. You cannot specify an [alias ARN](#) in the value of this condition key.

To satisfy this condition, the value of the `KeyId` parameter in the request must be a matching alias name or alias ARN. If the request uses a different [key identifier](#), it does not satisfy the condition, even if it identifies the same KMS key.

For example, the following key policy statement allows the principal to call the [GenerateDataKey](#) operation on the KMS key. However this is permitted only when the value of the `KeyId`

parameter in the request is `alias/finance-key` or an alias ARN with that alias name, such as `arn:aws:kms:us-west-2:111122223333:alias/finance-key`.

```
{
  "Sid": "Key policy using a request alias condition",
  "Effect": "Allow",
  "Principal": {
    "AWS": "arn:aws:iam::111122223333:role/developer"
  },
  "Action": "kms:GenerateDataKey",
  "Resource": "*",
  "Condition": {
    "StringEquals": {
      "kms:RequestAlias": "alias/finance-key"
    }
  }
}
```

You cannot use this condition key to control access to alias operations, such as [CreateAlias](#) or [DeleteAlias](#). For information about controlling access to alias operations, see [Controlling access to aliases](#).

kms:ResourceAliases

Amazon KMS condition keys	Condition type	Value type	API operations	Policy type
<code>kms:ResourceAliases</code>	String (list)	Multi-valued	KMS key resource operations	IAM policies only

Use this condition key to control access to a KMS key based on the [aliases](#) that are associated with the KMS key. The operation must be a *KMS key resource operation*, that is, an operation that is authorized for a particular KMS key. To identify the KMS key resource operations, in the [Actions and Resources Table](#), look for a value of `KMS key` in the `Resources` column for the operation.

This condition supports attribute-based access control (ABAC) in Amazon KMS. With ABAC, you can control access to KMS keys based on the tags that are assigned to a KMS key and the aliases that

are associated with a KMS key. You can use tags and aliases to allow or deny access to a KMS key without changing policies or grants. For details, see [ABAC for Amazon KMS](#).

An alias must be unique in an Amazon Web Services account and Region, but this condition lets you control access to multiple KMS keys in the same Region (using the `StringLike` comparison operator) or to multiple KMS keys in different Amazon Web Services Regions of each account.

Note

The [kms:ResourceAliases](#) condition is effective only when the KMS key conforms to the [aliases per KMS key](#) quota. If a KMS key exceeds this quota, principals who are authorized to use the KMS key by the `kms:ResourceAliases` condition are denied access to the KMS key.

To specify the alias in this policy condition, use an [alias name](#), such as `alias/project-alpha`, or an alias name pattern, such as `alias/*test*`. You cannot specify an [alias ARN](#) in the value of this condition key. To satisfy the condition, the KMS key used in the operation must have the specified alias. It does not matter whether or how the KMS key is identified in the request for the operation.

This is a multivalued condition key that compares the set of aliases associated with a KMS key to the set of aliases in the policy. To determine how these sets are compared, you must provide a `ForAnyValue` or `ForAllValues` set operator in the policy condition. For details about the set operators, see [Using multiple keys and values](#) in the IAM User Guide.

- `ForAnyValue`: At least one alias associated with the KMS key must match an alias in the policy condition. Other aliases are permitted. If the KMS key has no aliases, the condition is not satisfied.
- `ForAllValues`: Every alias associated with the KMS key must match an alias in the policy. This set operator limits the aliases associated with the KMS key to those in the policy condition. It doesn't require any aliases, but it forbids unspecified aliases.

For example, the following IAM policy statement allows the principal to call the [GenerateDataKey](#) operation on any KMS key in the specified Amazon Web Services account that is associated with the `finance-key` alias. (The key policies of the affected KMS keys must also allow the principal's account to use them for this operation.) To indicate that the condition is satisfied when one of the many aliases that might be associated with the KMS key is `alias/finance-key`, the condition uses the `ForAnyValue` set operator.

Because the `kms:ResourceAliases` condition is based on the resource, not the request, a call to `GenerateDataKey` succeeds for any KMS key associated with the `finance-key` alias, even if the request uses a [key ID](#) or [key ARN](#) to identify the KMS key.

```
{
  "Sid": "AliasBasedIAMPolicy",
  "Effect": "Allow",
  "Action": "kms:GenerateDataKey",
  "Resource": [
    "arn:aws:kms:*:111122223333:key/*",
    "arn:aws:kms:*:444455556666:key/*"
  ],
  "Condition": {
    "ForAnyValue:StringEquals": {
      "kms:ResourceAliases": "alias/finance-key"
    }
  }
}
```

The following example IAM policy statement allows the principal to enable and disable KMS keys but only when all aliases of the KMS keys include "Test." This policy statement uses two conditions. The condition with the `ForAllValues` set operator requires that all aliases associated with the KMS key include "Test". The condition with the `ForAnyValue` set operator requires that the KMS key have at least one alias with "Test." Without the `ForAnyValue` condition, this policy statement would have allowed the principal to use KMS keys that had no aliases.

```
{
  "Sid": "AliasBasedIAMPolicy",
  "Effect": "Allow",
  "Action": [
    "kms:EnableKey",
    "kms:DisableKey"
  ],
  "Resource": "arn:aws:kms:*:111122223333:key/*",
  "Condition": {
    "ForAllValues:StringLike": {
      "kms:ResourceAliases": [
        "alias/*Test*"
      ]
    },
    "ForAnyValue:StringLike": {
      "kms:ResourceAliases": [
```

```

        "alias/*Test*"
    ]
}
}
}

```

kms:ReplicaRegion

Amazon KMS condition keys	Condition type	Value type	API operations	Policy type
kms:ReplicaRegion	String (list)	Single-valued	ReplicateKey	Key policies and IAM policies

You can use this condition key to limit the Amazon Web Services Regions in which a principal can replicate a [multi-Region key](#). The `kms:ReplicaRegion` condition key controls access to the [ReplicateKey](#) operation based on the value of the [ReplicaRegion](#) parameter in the request. This parameter specifies the Amazon Web Services Region for the new [replica key](#).

The value of the condition is one or more Amazon Web Services Region names, such as `us-east-1` or `ap-southeast-2`, or name patterns, such as `eu-*`. For a list of the names of Amazon Web Services Regions that Amazon KMS supports, see [Amazon Key Management Service endpoints and quotas](#) in the Amazon Web Services General Reference.

For example, the following key policy statement uses the `kms:ReplicaRegion` condition key to allow principals to call the [ReplicateKey](#) operation only when the value of the `ReplicaRegion` parameter is one of the specified Regions.

```

{
  "Effect": "Allow",
  "Principal": {
    "AWS": "arn:aws:iam::111122223333:role/Administrator"
  },
  "Action": "kms:ReplicateKey"
  "Resource": "*",
  "Condition": {
    "StringEquals": {
      "kms:ReplicaRegion": [
        "us-east-1",

```

```

        "eu-west-3",
        "ap-southeast-2"
    ]
}
}
}

```

This condition key controls access only to the [ReplicateKey](#) operation. To control access to the [UpdatePrimaryRegion](#) operation, use the [kms:PrimaryRegion](#) condition key.

kms:RetiringPrincipal

Amazon KMS condition keys	Condition type	Value type	API operations	Policy type
kms:RetiringPrincipal	String (list)	Single-valued	CreateGrant	Key policies and IAM policies

You can use this condition key to control access to the [CreateGrant](#) operation based on the value of the [RetiringPrincipal](#) parameter in the request. For example, you can to create grants to use a KMS key only when the `RetiringPrincipal` in the `CreateGrant` request matches the `RetiringPrincipal` in the condition statement.

To specify the retiring principal, use the Amazon Resource Name (ARN) of an Amazon principal. Valid principals include Amazon Web Services accounts, IAM users, IAM roles, federated users, and assumed role users. For help with the ARN syntax for a principal, see [IAM ARNs](#) in the *IAM User Guide*.

The following example key policy statement allows a user to create grants for the KMS key. The `kms:RetiringPrincipal` condition key restricts the permission to `CreateGrant` requests where the retiring principal in the grant is the `LimitedAdminRole`.

```

{
  "Effect": "Allow",
  "Principal": {
    "AWS": "arn:aws:iam::111122223333:role/ExampleRole"
  },
  "Action": "kms:CreateGrant",

```

```

"Resource": "*",
"Condition": {
  "StringEquals": {
    "kms:RetiringPrincipal": "arn:aws:iam::111122223333:role/LimitedAdminRole"
  }
}
}

```

See also

- [kms:GrantConstraintType](#)
- [kms:GrantIsForAWSResource](#)
- [kms:GrantOperations](#)
- [kms:GranteePrincipal](#)

kms:RotationPeriodInDays

Amazon KMS condition keys	Condition type	Value type	API operations	Policy type
kms:RotationPeriodInDays	Numeric	Single-valued	EnableKeyRotation	Key policies and IAM policies

You can use this condition key to limit the values that principals can specify in the `RotationPeriodInDays` parameter of a [EnableKeyRotation](#) request.

The `RotationPeriodInDays` specifies the number of days between each automatic key rotation date. Amazon KMS allows you to specify a rotation period between 90 and 2560 days, but you can use the `kms:RotationPeriodInDays` condition key to further constrain the rotation period, such as enforcing a minimum rotation period within the valid range.

For example, the following key policy statement uses the `kms:RotationPeriodInDays` condition key to prevent principals from enabling key rotation if the rotation period is less than or equal to 180 days.

```

{
  "Effect": "Deny",

```

```

"Action": "kms:EnableKeyRotation",
"Principal": "*",
"Resource": "*",
"Condition" : {
  "NumericLessThanEquals" : {
    "kms:RotationPeriodInDays" : "180"
  }
}
}

```

kms:ScheduleKeyDeletionPendingWindowInDays

Amazon KMS condition keys	Condition type	Value type	API operations	Policy type
kms:ScheduleKeyDeletionPendingWindowInDays	Numeric	Single-valued	ScheduleKeyDeletion	Key policies and IAM policies

You can use this condition key to limit the values that principals can specify in the `PendingWindowInDays` parameter of a [ScheduleKeyDeletion](#) request.

The `PendingWindowInDays` specifies the number of days that Amazon KMS will wait before deleting a key. Amazon KMS allows you to specify a waiting period between 7 and 30 days, but you can use the `kms:ScheduleKeyDeletionPendingWindowInDays` condition key to further constrain the waiting period, such as enforcing a minimum waiting period within the valid range.

For example, the following key policy statement uses the `kms:ScheduleKeyDeletionPendingWindowInDays` condition key to prevent principals from scheduling key deletion if the waiting period is less than or equal to 21 days.

```

{
  "Effect": "Deny",
  "Action": "kms:ScheduleKeyDeletion",
  "Principal": "*",
  "Resource": "*",
  "Condition" : {

```

```

    "NumericLessThanEquals" : {
      "kms:ScheduleKeyDeletionPendingWindowInDays" : "21"
    }
  }
}

```

kms:SigningAlgorithm

Amazon KMS condition keys	Condition type	Value type	API operations	Policy type
kms:SigningAlgorithm	String	Single-valued	Sign Verify	Key policies and IAM policies

You can use the `kms:SigningAlgorithm` condition key to control access to the [Sign](#) and [Verify](#) operations based on the value of the [SigningAlgorithm](#) parameter in the request. This condition key has no effect on operations performed outside of Amazon KMS, such as verifying signatures with the public key in an asymmetric KMS key pair outside of Amazon KMS.

The following example key policy allows users who can assume the `testers` role to use the KMS key to sign messages only when the signing algorithm used for the request is an `RSASSA_PSS` algorithm, such as `RSASSA_PSS_SHA512`.

```

{
  "Effect": "Allow",
  "Principal": {
    "AWS": "arn:aws:iam::111122223333:role/testers"
  },
  "Action": "kms:Sign",
  "Resource": "*",
  "Condition": {
    "StringLike": {
      "kms:SigningAlgorithm": "RSASSA_PSS*"
    }
  }
}

```

See also

- [kms:EncryptionAlgorithm](#)
- [the section called “kms:MacAlgorithm”](#)
- [the section called “kms:MessageType”](#)

kms:ValidTo

Amazon KMS condition keys	Condition type	Value type	API operations	Policy type
kms:ValidTo	Timestamp	Single-valued	ImportKeyMaterial	Key policies and IAM policies

The `kms:ValidTo` condition key controls access to the [ImportKeyMaterial](#) operation based on the value of the [ValidTo](#) parameter in the request, which determines when the imported key material expires. The value is expressed in [Unix time](#).

By default, the `ValidTo` parameter is required in an `ImportKeyMaterial` request. However, if the value of the [ExpirationModel](#) parameter is `KEY_MATERIAL_DOES_NOT_EXPIRE`, the `ValidTo` parameter is invalid. You can also use the [kms:ExpirationModel](#) condition key to require the `ExpirationModel` parameter or a specific parameter value.

The following example policy statement allows a user to import key material into a KMS key. The `kms:ValidTo` condition key limits the permission to `ImportKeyMaterial` requests where the `ValidTo` value is less than or equal to `1546257599.0` (December 31, 2018 11:59:59 PM).

```
{
  "Effect": "Allow",
  "Principal": {
    "AWS": "arn:aws:iam::111122223333:role/ExampleRole"
  },
  "Action": "kms:ImportKeyMaterial",
  "Resource": "*",
  "Condition": {
    "NumericLessThanEquals": {
      "kms:ValidTo": "1546257599.0"
    }
  }
}
```

See also

- [kms:ExpirationModel](#)
- [kms:WrappingAlgorithm](#)
- [kms:WrappingKeySpec](#)

kms:ViaService

Amazon KMS condition keys	Condition type	Value type	API operations	Policy type
kms:ViaService	String	Single-valued	KMS key resource operations	Key policies and IAM policies

The `kms:ViaService` condition key limits use of an KMS key to requests from specified Amazon services. You can specify one or more services in each `kms:ViaService` condition key. The operation must be a *KMS key resource operation*, that is, an operation that is authorized for a particular KMS key. To identify the KMS key resource operations, in the [Actions and Resources Table](#), look for a value of `KMS key` in the Resources column for the operation.

For example, the following key policy statement uses the `kms:ViaService` condition key to allow a [customer managed key](#) to be used for the specified actions only when the request comes from Amazon EC2 or Amazon RDS in the US West (Oregon) region on behalf of `ExampleRole`.

```
{
  "Effect": "Allow",
  "Principal": {
    "AWS": "arn:aws:iam::111122223333:role/ExampleRole"
  },
  "Action": [
    "kms:Encrypt",
    "kms:Decrypt",
    "kms:ReEncrypt*",
    "kms:GenerateDataKey*",
    "kms:CreateGrant",
    "kms:ListGrants",
    "kms:DescribeKey"
  ]
}
```



```

],
"Resource": "*",
"Condition": {
  "StringEquals": {
    "kms:ViaService": [
      "ec2.us-west-2.amazonaws.com",
      "rds.us-west-2.amazonaws.com"
    ]
  }
}
}

```

You can also use a `kms:ViaService` condition key to deny permission to use a KMS key when the request comes from particular services. For example, the following policy statement from a key policy uses a `kms:ViaService` condition key to prevent a customer managed key from being used for Encrypt operations when the request comes from Amazon Lambda on behalf of `ExampleRole`.

```

{
  "Effect": "Deny",
  "Principal": {
    "AWS": "arn:aws:iam::111122223333:role/ExampleRole"
  },
  "Action": [
    "kms:Encrypt"
  ],
  "Resource": "*",
  "Condition": {
    "StringEquals": {
      "kms:ViaService": [
        "lambda.us-west-2.amazonaws.com"
      ]
    }
  }
}

```

Important

When you use the `kms:ViaService` condition key, the service makes the request on behalf of a principal in the Amazon Web Services account. These principals must have the following permissions:

- Permission to use the KMS key. The principal needs to grant these permissions to the integrated service so the service can use the customer managed key on behalf of the principal. For more information, see [Using Amazon KMS encryption with Amazon services](#).
- Permission to use the integrated service. For details about giving users access to an Amazon service that integrates with Amazon KMS, consult the documentation for the integrated service.

All [Amazon managed keys](#) use a `kms:ViaService` condition key in their key policy document. This condition allows the KMS key to be used only for requests that come from the service that created the KMS key. To see the key policy for an Amazon managed key, use the [GetKeyPolicy](#) operation.

The `kms:ViaService` condition key is valid in IAM and key policy statements. The services that you specify must be [integrated with Amazon KMS](#) and support the `kms:ViaService` condition key.

Services that support the `kms:ViaService` condition key

The following table lists Amazon services that are integrated with Amazon KMS and support the use of the `kms:ViaService` condition key in customer managed keys. The services in this table might not be available in all regions. Use the `.amazonaws.com` suffix of the Amazon KMS `ViaService` name in all Amazon partitions.

Note

You might need to scroll horizontally or vertically to see all of the data in this table.

Service name	Amazon KMS <code>ViaService</code> name
Amazon AI Operations	<code>aiops.<i>AWS_region</i>.amazonaws.com</code>
Amazon App Runner	<code>apprunner.<i>AWS_region</i>.amazonaws.com</code>
Amazon AppFabric	<code>appfabric.<i>AWS_region</i>.amazonaws.com</code>

Service name	Amazon KMS ViaService name
Amazon AppFlow	appflow. <i>AWS_region</i> .amazonaws.com
Amazon Application Migration Service	mgn. <i>AWS_region</i> .amazonaws.com
Amazon Athena	athena. <i>AWS_region</i> .amazonaws.com
Amazon Audit Manager	auditmanager. <i>AWS_region</i> .amazonaws.com
Amazon Aurora	rds. <i>AWS_region</i> .amazonaws.com
Amazon Backup	backup. <i>AWS_region</i> .amazonaws.com
Amazon Backup Gateway	backup-gateway. <i>AWS_region</i> .amazonaws.com
Amazon Bedrock Model Copy	bedrock. <i>AWS_region</i> .amazonaws.com
Amazon Chime SDK	chimevoiceconnector. <i>AWS_region</i> .amazonaws.com
Amazon Clean Rooms ML	cleanrooms-ml. <i>AWS_region</i> .amazonaws.com
Amazon CodeArtifact	codeartifact. <i>AWS_region</i> .amazonaws.com
Amazon CodeGuru Reviewer	codeguru-reviewer. <i>AWS_region</i> .amazonaws.com
Amazon Comprehend	comprehend. <i>AWS_region</i> .amazonaws.com
Amazon Connect	connect. <i>AWS_region</i> .amazonaws.com
Amazon Connect Customer Profiles	profile. <i>AWS_region</i> .amazonaws.com
Amazon Q in Connect	wisdom. <i>AWS_region</i> .amazonaws.com

Service name	Amazon KMS ViaService name
Amazon Database Migration Service (Amazon DMS)	<code>dms.AWS_region .amazonaws.com</code>
Amazon DeepRacer	<code>deepracer.AWS_region .amazonaws.com</code>
Amazon Directory Service	<code>directoryservice.AWS_region .amazonaws.com</code>
Amazon DocumentDB	<code>docdb-elastic.AWS_region .amazonaws.com</code>
Amazon DynamoDB	<code>dynamodb.AWS_region .amazonaws.com</code>
Amazon EC2 Systems Manager (SSM)	<code>ssm.AWS_region .amazonaws.com</code>
Amazon Elastic Block Store (Amazon EBS)	<code>ec2.AWS_region .amazonaws.com</code> (EBS only)
Amazon Elastic Container Registry (Amazon ECR)	<code>ecr.AWS_region .amazonaws.com</code>
Amazon Elastic File System (Amazon EFS)	<code>elasticfilesystem.AWS_region .amazonaws.com</code>
Amazon ElastiCache	<p>Include both ViaService names in the condition key value:</p> <ul style="list-style-type: none"> <code>elasticache.AWS_region .amazonaws.com</code> <code>dax.AWS_region .amazonaws.com</code>
AWS Elemental MediaTailor	<code>mediatailor.AWS_region .amazonaws.com</code>

Service name	Amazon KMS ViaService name
Amazon Entity Resolution	entityresolution. <i>AWS_region</i> .amazonaws.com
Amazon EventBridge	events. <i>AWS_region</i> .amazonaws.com
Amazon FinSpace	finspace. <i>AWS_region</i> .amazonaws.com
Amazon Forecast	forecast. <i>AWS_region</i> .amazonaws.com
Amazon FSx	fsx. <i>AWS_region</i> .amazonaws.com
Amazon Glue	glue. <i>AWS_region</i> .amazonaws.com
Amazon Ground Station	groundstation. <i>AWS_region</i> .amazonaws.com
Amazon GuardDuty	malware-protection. <i>AWS_region</i> .amazonaws.com
Amazon HealthLake	healthlake. <i>AWS_region</i> .amazonaws.com
Amazon IoT SiteWise	iotsitewise. <i>AWS_region</i> .amazonaws.com
Amazon Kendra	kendra. <i>AWS_region</i> .amazonaws.com
Amazon Keyspaces (for Apache Cassandra)	cassandra. <i>AWS_region</i> .amazonaws.com
Amazon Kinesis	kinesis. <i>AWS_region</i> .amazonaws.com
Amazon Data Firehose	firehose. <i>AWS_region</i> .amazonaws.com

Service name	Amazon KMS ViaService name
Amazon Kinesis Video Streams	kinesisvideo. <i>AWS_region</i> .amazonaws.com
Amazon Lambda	lambda. <i>AWS_region</i> .amazonaws.com
Amazon Lex	lex. <i>AWS_region</i> .amazonaws.com
Amazon License Manager	license-manager. <i>AWS_region</i> .amazonaws.com
Amazon Location Service	geo. <i>AWS_region</i> .amazonaws.com
Amazon Lookout for Equipment	lookoutequipment. <i>AWS_region</i> .amazonaws.com
Amazon Lookout for Metrics	lookoutmetrics. <i>AWS_region</i> .amazonaws.com
Amazon Lookout for Vision	lookoutvision. <i>AWS_region</i> .amazonaws.com
Amazon Macie	macie. <i>AWS_region</i> .amazonaws.com
Amazon Mainframe Modernization	m2. <i>AWS_region</i> .amazonaws.com
Amazon Mainframe Modernization Application Testing	apptest. <i>AWS_region</i> .amazonaws.com
Amazon Managed Blockchain	managedblockchain. <i>AWS_region</i> .amazonaws.com
Amazon Managed Streaming for Apache Kafka (Amazon MSK)	kafka. <i>AWS_region</i> .amazonaws.com
Amazon Managed Workflows for Apache Airflow (MWAA)	airflow. <i>AWS_region</i> .amazonaws.com

Service name	Amazon KMS ViaService name
Amazon MemoryDB	memorydb. <i>AWS_region</i> .amazonaws.com
Amazon Monitron	monitron. <i>AWS_region</i> .amazonaws.com
Amazon MQ	mq. <i>AWS_region</i> .amazonaws.com
Amazon Neptune	ids. <i>AWS_region</i> .amazonaws.com
Amazon Nimble Studio	nimble. <i>AWS_region</i> .amazonaws.com
Amazon HealthOmics	omics. <i>AWS_region</i> .amazonaws.com
Amazon OpenSearch Service	es. <i>AWS_region</i> .amazonaws.com , aoss. <i>AWS_region</i> .amazonaws.com
Amazon OpenSearch Custom Packages	custom-packages. <i>AWS_region</i> .amazonaws.com
Amazon Proton	proton. <i>AWS_region</i> .amazonaws.com
Amazon Quantum Ledger Database (Amazon QLDB)	qldb. <i>AWS_region</i> .amazonaws.com
Amazon RDS Performance Insights	ids. <i>AWS_region</i> .amazonaws.com
Amazon Redshift	redshift. <i>AWS_region</i> .amazonaws.com
Amazon Redshift query editor V2	sqlworkbench. <i>AWS_region</i> .amazonaws.com
Amazon Redshift Serverless	redshift-serverless. <i>AWS_region</i> .amazonaws.com
Amazon Rekognition	rekognition. <i>AWS_region</i> .amazonaws.com

Service name	Amazon KMS ViaService name
Amazon Relational Database Service (Amazon RDS)	<code>rds.AWS_region .amazonaws.com</code>
Amazon Replicated Data Store	<code>ards.AWS_region .amazonaws.com</code>
Amazon SageMaker AI	<code>sagemaker.AWS_region .amazonaws.com</code>
Amazon Secrets Manager	<code>secretsmanager.AWS_region .amazonaws.com</code>
Amazon Security Lake	<code>securitylake.AWS_region .amazonaws.com</code>
Amazon Simple Email Service (Amazon SES)	<code>ses.AWS_region .amazonaws.com</code>
Amazon Simple Notification Service (Amazon SNS)	<code>sns.AWS_region .amazonaws.com</code>
Amazon Simple Queue Service (Amazon SQS)	<code>sqs.AWS_region .amazonaws.com</code>
Amazon Simple Storage Service (Amazon S3)	<code>s3.AWS_region .amazonaws.com</code>
Amazon S3 Tables	<code>s3tables.AWS_region .amazonaws.com</code>
Amazon Snowball Edge	<code>importexport.AWS_region .amazonaws.com</code>
Amazon Step Functions	<code>states.AWS_region .amazonaws.com</code>
Amazon Storage Gateway	<code>storagegateway.AWS_region .amazonaws.com</code>
Amazon Systems Manager Incident Manager	<code>ssm-incidents.AWS_region .amazonaws.com</code>

Service name	Amazon KMS ViaService name
Amazon Systems Manager Incident Manager Contacts	ssm-contacts. <i>AWS_region</i> .amazonaws.com
Amazon Timestream	timestream. <i>AWS_region</i> .amazonaws.com
Amazon Translate	translate. <i>AWS_region</i> .amazonaws.com
Amazon Verified Access	verified-access. <i>AWS_region</i> .amazonaws.com
Amazon WorkMail	workmail. <i>AWS_region</i> .amazonaws.com
Amazon WorkSpaces	workspaces. <i>AWS_region</i> .amazonaws.com
Amazon WorkSpaces Thin Client	thinclient. <i>AWS_region</i> .amazonaws.com
Amazon WorkSpaces Web	workspaces-web. <i>AWS_region</i> .amazonaws.com
Amazon X-Ray	xray. <i>AWS_region</i> .amazonaws.com

kms:WrappingAlgorithm

Amazon KMS condition keys	Condition type	Value type	API operations	Policy type
kms:WrappingAlgorithm	String	Single-valued	GetParametersForImport	Key policies and IAM policies

This condition key controls access to the [GetParametersForImport](#) operation based on the value of the [WrappingAlgorithm](#) parameter in the request. You can use this condition to require principals to use a particular algorithm to encrypt key material during the import process. Requests for the required public key and import token fail when they specify a different wrapping algorithm.

The following example key policy statement uses the `kms:WrappingAlgorithm` condition key to give the example user permission to call the `GetParametersForImport` operation, but prevents them from using the `RSAES_OAEP_SHA_1` wrapping algorithm. When the `WrappingAlgorithm` in the `GetParametersForImport` request is `RSAES_OAEP_SHA_1`, the operation fails.

```
{
  "Effect": "Allow",
  "Principal": {
    "AWS": "arn:aws:iam::111122223333:role/ExampleRole"
  },
  "Action": "kms:GetParametersForImport",
  "Resource": "*",
  "Condition": {
    "StringNotEquals": {
      "kms:WrappingAlgorithm": "RSAES_OAEP_SHA_1"
    }
  }
}
```

See also

- [kms:ExpirationModel](#)
- [kms:ValidTo](#)
- [kms:WrappingKeySpec](#)

kms:WrappingKeySpec

Amazon KMS condition keys	Condition type	Value type	API operations	Policy type
<code>kms:WrappingKeySpec</code>	String	Single-valued	<code>GetParametersForImport</code>	Key policies and IAM policies

This condition key controls access to the [GetParametersForImport](#) operation based on the value of the [WrappingKeySpec](#) parameter in the request. You can use this condition to require principals to use a particular type of public key during the import process. If the request specifies a different key type, it fails.

Because the only valid value for the `WrappingKeySpec` parameter value is `RSA_2048`, preventing users from using this value effectively prevents them from using the `GetParametersForImport` operation.

The following example policy statement uses the `kms:WrappingAlgorithm` condition key to require that the `WrappingKeySpec` in the request is `RSA_4096`.

```
{
  "Effect": "Allow",
  "Principal": {
    "AWS": "arn:aws:iam::111122223333:role/ExampleRole"
  },
  "Action": "kms:GetParametersForImport",
  "Resource": "*",
  "Condition": {
    "StringEquals": {
      "kms:WrappingKeySpec": "RSA_4096"
    }
  }
}
```

See also

- [kms:ExpirationModel](#)
- [kms:ValidTo](#)
- [kms:WrappingAlgorithm](#)

Amazon KMS condition keys for Amazon Nitro Enclaves

[Amazon Nitro Enclaves](#) is an Amazon EC2 capability that lets you create isolated compute environments called [enclaves](#) to protect and process highly sensitive data. Amazon KMS provides condition keys to support Amazon Nitro Enclaves. These conditions keys are effective only for requests to Amazon KMS for a Nitro Enclave.

When you call the [Decrypt](#), [DeriveSharedSecret](#), [GenerateDataKey](#), [GenerateDataKeyPair](#), or [GenerateRandom](#) API operations with the signed [attestation document](#) from an enclave, these APIs encrypt the plaintext in the response under the public key from the attestation document, and return ciphertext instead of plaintext. This ciphertext can be decrypted only by using the private key in the enclave. For more information, see [Cryptographic attestation for Amazon Nitro Enclaves](#).

The following condition keys let you limit the permissions for these operations based on the contents of the signed attestation document. Before allowing an operation, Amazon KMS compares the attestation document from the enclave to the values in these Amazon KMS condition keys.

kms:RecipientAttestation:ImageSha384

Amazon KMS Condition Keys	Condition Type	Value type	API Operations	Policy Type
kms:RecipientAttestation:ImageSha384	String	Single-valued	Decrypt DeriveSharedSecret GenerateDataKey GenerateDataKeyPair GenerateRandom	Key policies and IAM policies

The `kms:RecipientAttestation:ImageSha384` condition key controls access to `Decrypt`, `DeriveSharedSecret`, `GenerateDataKey`, `GenerateDataKeyPair`, and `GenerateRandom` with a KMS key when the image digest from the signed attestation document in the request matches the value in the condition key. The `ImageSha384` value corresponds to PCR0 in the attestation document. This condition key is effective only when the `Recipient` parameter in the request specifies a signed attestation document for an Amazon Nitro enclave.

This value is also included in [CloudTrail events](#) for requests to Amazon KMS for Nitro enclaves.

For example, the following key policy statement allows the data-processing role to use the KMS key for [Decrypt](#), [DeriveSharedSecret](#), [GenerateDataKey](#), [GenerateDataKeyPair](#), and [GenerateRandom](#) operations. The `kms:RecipientAttestation:ImageSha384` condition key allows the operations only when the image digest value (PCR0) of the attestation document in the request matches the image digest value in the condition. This condition key is effective only when the `Recipient` parameter in the request specifies a signed attestation document for an Amazon Nitro enclave.

If the request does not include a valid attestation document from an Amazon Nitro enclave, permission is denied because this condition is not satisfied.

```
{
  "Sid" : "Enable enclave data processing",
  "Effect" : "Allow",
  "Principal" : {
    "AWS" : "arn:aws:iam::111122223333:role/data-processing"
  },
  "Action": [
    "kms:Decrypt",
    "kms:DeriveSharedSecret",
    "kms:GenerateDataKey",
    "kms:GenerateDataKeyPair",
    "kms:GenerateRandom"
  ],
  "Resource" : "*",
  "Condition": {
    "StringEqualsIgnoreCase": {
      "kms:RecipientAttestation:ImageSha384":
      "9fedcba8abcdef7abcdef6abcdef5abcdef4abcdef3abcdef2abcdef1abcdef1abcdef0abcdef1abcdef2abcdef3a
    }
  }
}
```

`kms:RecipientAttestation:PCR<PCR_ID>`

Amazon KMS Condition Keys	Condition Type	Value type	API Operations	Policy Type
<code>kms:RecipientAttestation</code>	String	Single-valued	Decrypt	Key policies and IAM policies

Amazon KMS Condition Keys	Condition Type	Value type	API Operations	Policy Type
<code>kms:RecipientAttestation:PCR<PCR_ID></code>			DeriveSharedSecret GenerateDataKey GenerateDataKeyPair GenerateRandom	

The `kms:RecipientAttestation:PCR<PCR_ID>` condition key controls access to `Decrypt`, `DeriveSharedSecret`, `GenerateDataKey`, `GenerateDataKeyPair`, and `GenerateRandom` with a KMS key only when the platform configuration registers (PCRs) from the signed attestation document in the request match the PCRs in the condition key. This condition key is effective only when the `Recipient` parameter in the request specifies a signed attestation document from an Amazon Nitro enclave.

This value is also included in [CloudTrail events](#) that represent requests to Amazon KMS for Nitro enclaves.

To specify a PCR value, use the following format. Concatenate the PCR ID to the condition key name. You can specify a PCR ID that identifies one of the [six enclave measurements](#) or a custom PCR ID that you defined for a specific use case. The PCR value must be a lower-case hexadecimal string of up to 96 bytes.

```
"kms:RecipientAttestation:PCR<PCR_ID>": "<PCR_value>"
```

For example, the following condition key specifies a particular value for PCR1, which corresponds to the hash of the kernel used for the enclave and the bootstrap process.

```
kms:RecipientAttestation:PCR1:
  "0x1abcdef2abcdef3abcdef4abcdef5abcdef6abcdef7abcdef8abcdef9abcdef8abcdef7abcdef6abcdef5abcdef"
```

The following example key policy statement allows the data-processing role to use the KMS key for the [Decrypt](#) operation.

The `kms:RecipientAttestation:PCR` condition key in this statement allows the operation only when the PCR1 value in the signed attestation document in the request matches `kms:RecipientAttestation:PCR1` value in the condition. Use the `StringEqualsIgnoreCase` policy operator to require a case-insensitive comparison of the PCR values.

If the request does not include an attestation document, permission is denied because this condition is not satisfied.

```
{
  "Sid" : "Enable enclave data processing",
  "Effect" : "Allow",
  "Principal" : {
    "AWS" : "arn:aws:iam::111122223333:role/data-processing"
  },
  "Action": "kms:Decrypt",
  "Resource" : "*",
  "Condition": {
    "StringEqualsIgnoreCase": {
      "kms:RecipientAttestation:PCR1":
      "0x1de4f2dcf774f6e3b679f62e5f120065b2e408dcea327bd1c9dddaea6664e7af7935581474844767453082c6f15"
    }
  }
}
```

Least-privilege permissions

Since your KMS keys protect sensitive information, we recommend following the principle of least-privileged access. Delegate the minimum permissions required to perform a task when you define your key policies. Only allow all actions (`kms:*`) on a KMS key policy if you plan to further restrict permissions with additional IAM policies. If you plan to manage permissions with IAM policies, limit who has the ability to create and attach IAM policies to IAM principals and [monitor for policy changes](#).

If you allow all actions (`kms:*`) in both the key policy and the IAM policy, the principal has both administrative and usage permissions to the KMS key. As a security best practice, we recommend only delegating these permissions to specific principals. You can do this by explicitly naming the principal in the key policy or by limiting which principals the IAM policy is attached to. You can also

use [condition keys](#) to restrict permissions. For example, you can use the [aws:PrincipalTag](#) to allow all actions if the principal making the API call has the tag specified in the condition rule.

For help understanding how policy statements are evaluated in Amazon, see [Policy evaluation logic](#) in the *IAM User Guide*. We recommend reviewing this topic before writing policies to reduce the chance that your policy has unintended effects, such as providing access to principals that should not have access.

Tip

When testing an application in a non-production environment, use [IAM Access Analyzer](#) to help you apply least-privileges to your IAM policies.

If you use IAM users instead of IAM roles, we strongly recommend enabling Amazon [multi-factor authentication](#) (MFA) to mitigate the vulnerability of long-term credentials. You can use MFA to do the following:

- Require that users validate their credentials with MFA before performing privileged actions, such as scheduling key deletion.
- Split ownership of an administrator account password and MFA device between individuals to implement split authorization.

Learn more

- [Amazon managed policies for job functions](#)
- [Techniques for writing least privilege IAM policies](#)

Implementing least privileged permissions

When you give an Amazon service permission to use a KMS key, ensure that the permission is valid only for the resources that the service must access on your behalf. This least privilege strategy helps to prevent unauthorized use of a KMS key when requests are passed between Amazon services.

To implement a least privilege strategy, we recommend using Amazon KMS encryption context condition keys and the global source ARN or source account condition keys.

Using encryption context condition keys

The most effective way to implement least privileged permissions when using Amazon KMS resources is to include the [kms:EncryptionContext:context-key](#) or [kms:EncryptionContextKeys](#) condition keys in the policy that allows principals to call Amazon KMS cryptographic operations. These condition keys are particularly effective because they associate the permission with the [encryption context](#) that is bound to the ciphertext when the resource is encrypted.

Use encryption context conditions keys only when the action in the policy statement is [CreateGrant](#) or an Amazon KMS symmetric cryptographic operation that takes an `EncryptionContext` parameter, such as the operations like [GenerateDataKey](#) or [Decrypt](#). (For a list of supported operations, see [kms:EncryptionContext:context-key](#) or [kms:EncryptionContextKeys](#).) If you use these condition keys to allow other operations, such as [DescribeKey](#), permission will be denied.

Set the value to the encryption context that the service uses when it encrypts the resource. This information is typically available in the Security chapter of the service documentation. For example, the [encryption context for Amazon Proton](#) identifies the Amazon Proton resource and its associated template. The [Amazon Secrets Manager encryption context](#) identifies the secret and its version. The [encryption context for Amazon Location](#) identifies the tracker or collection.

The following example key policy statement allows Amazon Location Service to create grants on behalf of authorized users. This policy statement limits the permission by using the [kms:ViaService](#), [kms:CallerAccount](#), and `kms:EncryptionContext:context-key` condition keys to tie the permission to a particular tracker resource.

```
{
  "Sid": "Allow Amazon Location to create grants on behalf of authorized users",
  "Effect": "Allow",
  "Principal": {
    "AWS": "arn:aws:iam::111122223333:role/LocationTeam"
  },
  "Action": "kms:CreateGrant",
  "Resource": "*",
  "Condition": {
    "StringEquals": {
      "kms:ViaService": "geo.us-west-2.amazonaws.com",
      "kms:CallerAccount": "111122223333",
      "kms:EncryptionContext:aws:geo:arn": "arn:aws:geo:us-west-2:111122223333:tracker/SAMPLE-Tracker"
    }
  }
}
```

```
}
```

Using `aws:SourceArn` or `aws:SourceAccount` condition keys

When the principal in a key policy statement is an [Amazon service principal](#), we strongly recommend that you use the `aws:SourceArn` or `aws:SourceAccount` global condition keys, in addition to the `kms:EncryptionContext:context-key` condition key. The ARN and account values are included in the authorization context only when a request comes to Amazon KMS from another Amazon service. This combination of conditions implements least privileged permissions and avoids a potential [confused deputy scenario](#). Service principals are not typically used as principals in a key policy, but some Amazon services, such as Amazon CloudTrail, require it.

To use the `aws:SourceArn` or `aws:SourceAccount` global condition keys, set the value to the Amazon Resource Name (ARN) or account of the resource that is being encrypted. For example, in a key policy statement that gives Amazon CloudTrail permission to encrypt a trail, set the value of `aws:SourceArn` to the ARN of the trail. Whenever possible, use `aws:SourceArn`, which is more specific. Set the value to the ARN or an ARN pattern with wildcard characters. If you don't know the ARN of the resource, use `aws:SourceAccount` instead.

Note

If a resource ARN includes characters that are not permitted in an Amazon KMS key policy, you cannot use that resource ARN in the value of the `aws:SourceArn` condition key. Instead, use the `aws:SourceAccount` condition key. For details about key policy document rules, see [Key policy format](#).

In the following example key policy, the principal who gets the permissions is the Amazon CloudTrail service principal, `cloudtrail.amazonaws.com`. To implement least privilege, this policy uses the `aws:SourceArn` and `kms:EncryptionContext:context-key` condition keys. The policy statement allows CloudTrail to use the KMS key to [generate the data key](#) that it uses to encrypt a trail. The `aws:SourceArn` and `kms:EncryptionContext:context-key` conditions are evaluated independently. Any request to use the KMS key for the specified operation must satisfy both conditions.

To restrict the service's permission to the `finance` trail in the example account (111122223333) and `us-west-2` Region, this policy statement sets the `aws:SourceArn` condition key to the ARN of a particular trail. The condition statement uses the [ArnEquals](#) operator to ensure that

every element in the ARN is evaluated independently when matching. The example also uses the `kms:EncryptionContext:context-key` condition key to limit the permission to trails in a particular account and Region.

Before using this key policy, replace the example account ID, Region, and trail name with valid values from your account.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "Allow CloudTrail to encrypt logs",
      "Effect": "Allow",
      "Principal": {
        "Service": "cloudtrail.amazonaws.com"
      },
      "Action": "kms:GenerateDataKey",
      "Resource": "*",
      "Condition": {
        "ArnEquals": {
          "aws:SourceArn": [
            "arn:aws:cloudtrail:us-west-2:111122223333:trail/finance"
          ]
        },
        "StringLike": {
          "kms:EncryptionContext:aws:cloudtrail:arn": [
            "arn:aws:cloudtrail:*:111122223333:trail/*"
          ]
        }
      }
    }
  ]
}
```

ABAC for Amazon KMS

Attribute-based access control (ABAC) is an authorization strategy that defines permissions based on attributes. Amazon KMS supports ABAC by allowing you to control access to your customer managed keys based on the tags and aliases associated with the KMS keys. The tag and alias condition keys that enable ABAC in Amazon KMS provide a powerful and flexible way to authorize

principals to use KMS keys without editing policies or managing grants. But you should use these feature with care so principals aren't inadvertently allowed or denied access.

If you use ABAC, be aware that permission to manage tags and aliases is now an access control permission. Be sure that you know the existing tags and aliases on all KMS keys before you deploy a policy that depends on tags or aliases. Take reasonable precautions when adding, deleting, and updating aliases, and when tagging and untagging keys. Give permissions to manage tags and aliases only to principals who need them, and limit the tags and aliases they can manage.

Notes

When using ABAC for Amazon KMS, be cautious about giving principals permission to manage tags and aliases. Changing a tag or alias might allow or deny permission to a KMS key. Key administrators who don't have permission to change key policies or create grants can control access to KMS keys if they have permission to manage tags or aliases.

It might take up to five minutes for tag and alias changes to affect KMS key authorization. Recent changes might be visible in API operations before they affect authorization.

To control access to a KMS key based on its alias, you must use a condition key. You cannot use an alias to represent a KMS key in the `Resource` element of a policy statement. When an alias appears in the `Resource` element, the policy statement applies to the alias, not to the associated KMS key.

Learn more

- For details about Amazon KMS support for ABAC, including examples, see [Use aliases to control access to KMS keys](#) and [Use tags to control access to KMS keys](#).
- For more general information about using tags to control access to Amazon resources, see [What is ABAC for Amazon?](#) and [Controlling Access to Amazon Resources Using Resource Tags](#) in the *IAM User Guide*.

ABAC condition keys for Amazon KMS

To authorize access to KMS keys based on their tags and aliases, use the following condition keys in a key policy or IAM policy.

ABAC condition key	Description	Policy type	Amazon KMS operations
aws:ResourceTag	Tag (key and value) on the KMS key matches the tag (key and value) or tag pattern in the policy	IAM policy only	KMS key resource operations ²
aws:RequestTag/tag-key	Tag (key and value) in the request matches the tag (key and value) or tag pattern in the policy	Key policy and IAM policies ¹	TagResource , UntagResource
aws:TagKeys	Tag keys in the request match the tag keys in the policy	Key policy and IAM policies ¹	TagResource , UntagResource
kms:ResourceAliases	Aliases associated with the KMS key match the aliases or alias patterns in the policy	IAM policy only	KMS key resource operations ²
kms:RequestAlias	Alias that represents the KMS key in the request matches the alias or alias patterns in the policy.	Key policy and IAM policies ¹	Cryptographic operations , DescribeKey , GetPublicKey

¹Any condition key that can be used in a key policy can also be used in an IAM policy, but only if [the key policy allows it](#).

²A *KMS key resource operation* is an operation authorized for a particular KMS key. To identify the KMS key resource operations, in the [Amazon KMS permissions table](#), look for a value of KMS key in the Resources column for the operation.

For example, you can use these condition keys to create the following policies.

- An IAM policy with `kms:ResourceAliases` that allows permission to use KMS keys with a particular alias or alias pattern. This is a bit different from policies that rely on tags: Although you can use alias patterns in a policy, each alias must be unique in an Amazon Web Services account and Region. This allows you to apply a policy to a select set of KMS keys without listing the key ARNs of the KMS keys in the policy statement. To add or remove KMS keys from the set, change the alias of the KMS key.
- A key policy with `kms:RequestAlias` that allows principals to use a KMS key in a `Encrypt` operation, but only when the `Encrypt` request uses that alias to identify the KMS key.
- An IAM policy with `aws:ResourceTag/tag-key` that denies permission to use KMS keys with a particular tag key and tag value. This lets you apply a policy to a select set of KMS keys without listing the key ARNs of the KMS keys in the policy statement. To add or remove KMS keys from the set, tag or untag the KMS key.
- An IAM policy with `aws:RequestTag/tag-key` that allows principals to delete only "Purpose"="Test" KMS key tags.
- An IAM policy with `aws:TagKeys` that denies permission to tag or untag a KMS key with a Restricted tag key.

ABAC makes access management flexible and scalable. For example, you can use the `aws:ResourceTag/tag-key` condition key to create an IAM policy that allows principals to use a KMS key for specified operations only when the KMS key has a `Purpose=Test` tag. The policy applies to all KMS keys in all Regions of the Amazon Web Services account.

When attached to a user or role, the following IAM policy allows principals to use all existing KMS keys with a `Purpose=Test` tag for the specified operations. To provide this access to new or existing KMS keys, you don't need to change the policy. Just attach the `Purpose=Test` tag to the KMS keys. Similarly, to remove this access from KMS keys with a `Purpose=Test` tag, edit or delete the tag.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AliasBasedIAMPolicy",
      "Effect": "Allow",
      "Action": [
```

```
    "kms:Decrypt",
    "kms:Encrypt",
    "kms:GenerateDataKey*",
    "kms:DescribeKey"
  ],
  "Resource": "arn:aws:kms:*:111122223333:key/*",
  "Condition": {
    "StringEquals": {
      "aws:ResourceTag/Purpose": "Test"
    }
  }
}
```

However, if you use this feature, be careful when managing tags and aliases. Adding, changing, or deleting a tag or alias can inadvertently allow or deny access to a KMS key. Key administrators who don't have permission to change key policies or create grants can control access to KMS keys if they have permission to manage tags and aliases. To mitigate this risk, consider [limiting permissions to manage tags](#) and [aliases](#). For example, you might want to allow only select principals to manage Purpose=Test tags. For details, see [Use aliases to control access to KMS keys](#) and [Use tags to control access to KMS keys](#).

Tags or aliases?

Amazon KMS supports ABAC with tags and aliases. Both options provide a flexible, scalable access control strategy, but they're slightly different from each other.

You might decide to use tags or use aliases based on your particular Amazon use patterns. For example, if you have already given tagging permissions to most administrators, it might be easier to control an authorization strategy based on aliases. Or, if you are close to the quota for [aliases per KMS key](#), you might prefer an authorization strategy based on tags.

The following benefits are of general interest.

Benefits of tag-based access control

- Same authorization mechanism for different types of Amazon resources.

You can use the same tag or tag key to control access to multiple resource types, such as an Amazon Relational Database Service (Amazon RDS) cluster, an Amazon Elastic Block Store

(Amazon EBS) volume, and a KMS key. This feature enables several different authorization models that are more flexible than traditional role-based access control.

- Authorize access to a group of KMS keys.

You can use tags to manage access to a group of KMS keys in the same Amazon Web Services account and Region. Assign the same tag or tag key to the KMS keys that you choose. Then create a simple, easy-to-maintain policy statement that is based on the tag or tag key. To add or remove a KMS key from your authorization group, add or remove the tag; you don't need to edit the policy.

Benefits of alias-based access control

- Authorize access to cryptographic operations based on aliases.

Most request-based policy conditions for attributes, including [aws:RequestTag/tag-key](#), affect only operations that add, edit, or delete the attribute. But the [kms:RequestAlias](#) condition key controls access to cryptographic operations based on the alias used to identify the KMS key in the request. For example, you can give a principal permission to use a KMS key in a Encrypt operation but only when the value of the KeyId parameter is `alias/restricted-key-1`. To satisfy this condition requires all of the following:

- The KMS key must be associated with that alias.
- The request must use the alias to identify the KMS key.
- The principal must have permission to use the KMS key subject to the `kms:RequestAlias` condition.

This is particularly useful if your applications commonly use alias names or alias ARNs to refer to KMS keys.

- Provide very limited permissions.

An alias must be unique in an Amazon Web Services account and Region. As a result, giving principals access to a KMS key based on an alias can be much more restrictive than giving them access based on a tag. Unlike aliases, tags can be assigned to multiple KMS keys in the same account and Region. If you choose, you can use an alias pattern, such as `alias/test*`, to give principals access to a group of KMS keys in the same account and Region. However, allowing or denying access to a particular alias allows very strict control on KMS keys.

Troubleshooting ABAC for Amazon KMS

Controlling access to KMS keys based on their tags and aliases is convenient and powerful. However, it's prone to a few predictable errors that you'll want to prevent.

Access changed due to tag change

If a tag is deleted or its value is changed, principals who have access to a KMS key based only on that tag will be denied access to the KMS key. This can also happen when a tag that is included in a deny policy statement is added to a KMS key. Adding a policy-related tag to a KMS key can allow access to principals who should be denied access to a KMS key.

For example, suppose that a principal has access to a KMS key based on the `Project=Alpha` tag, such as the permission provided by the following example IAM policy statement.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "IAMPolicyWithTag",
      "Effect": "Allow",
      "Action": [
        "kms:GenerateDataKeyWithoutPlaintext",
        "kms:Decrypt"
      ],
      "Resource": "arn:aws:kms:ap-southeast-1:111122223333:key/*",
      "Condition": {
        "StringEquals": {
          "aws:ResourceTag/Project": "Alpha"
        }
      }
    }
  ]
}
```

If the tag is deleted from that KMS key or the tag value is changed, the principal no longer has permission to use the KMS key for the specified operations. This might become evident when the principal tries to read or write data in an Amazon service that uses a customer managed key. To trace the tag change, review your CloudTrail logs for [TagResource](#) or [UntagResource](#) entries.

To restore access without updating the policy, change the tags on the KMS key. This action has minimal impact other than a brief period while it is taking effect throughout Amazon KMS. To

prevent an error like this one, give tagging and untagging permissions only to principals who need it and [limit their tagging permissions](#) to tags they need to manage. Before changing a tag, search policies to detect access that depends on the tag, and get KMS keys in all Regions that have the tag. You might consider creating an Amazon CloudWatch alarm when particular tags are changed.

Access change due to alias change

If an alias is deleted or associated with a different KMS key, principals who have access to the KMS key based only on that alias will be denied access to the KMS key. This can also happen when an alias that is associated with a KMS key is included in a deny policy statement. Adding a policy-related alias to a KMS key can also allow access to principals who should be denied access to a KMS key.

For example, the following IAM policy statement uses the [kms:ResourceAliases](#) condition key to allow access to KMS keys in different Regions of the account with any of the specified aliases.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AliasBasedIAMPolicy",
      "Effect": "Allow",
      "Action": [
        "kms:List*",
        "kms:Describe*",
        "kms:Decrypt"
      ],
      "Resource": "arn:aws:kms:*:111122223333:key/*",
      "Condition": {
        "ForAnyValue:StringEquals": {
          "kms:ResourceAliases": [
            "alias/ProjectAlpha",
            "alias/ProjectAlpha_Test",
            "alias/ProjectAlpha_Dev"
          ]
        }
      }
    }
  ]
}
```

To trace the alias change, review your CloudTrail logs for [CreateAlias](#), [UpdateAlias](#), and [DeleteAlias](#) entries.

To restore access without updating the policy, change the alias associated with the KMS key. Because each alias can be associated with only one KMS key in an account and Region, managing aliases is a bit more difficult than managing tags. Restoring access to some principals on one KMS key can deny the same or other principals access to a different KMS key.

To prevent this error, give alias management permissions only to principals who need it and [limit their alias-management permissions](#) to aliases they need to manage. Before updating or deleting an alias, search policies to detect access that depends on the alias, and find KMS keys in all Regions that are associated with the alias.

Access denied due to alias quota

Users who are authorized to use a KMS key by an [kms:ResourceAliases](#) condition will get an `AccessDenied` exception if the KMS key exceeds the default [aliases per KMS key](#) quota for that account and Region.

To restore access, delete aliases that are associated with the KMS key so it complies with the quota. Or use an alternate mechanism to give users access to the KMS key.

Delayed authorization change

Changes that you make to tags and aliases might take up to five minutes to affect the authorization of KMS keys. As a result, a tag or alias change might be reflected in the responses from API operations before they affect authorization. This delay is likely to be longer than the brief eventual consistency delay that affects most Amazon KMS operations.

For example, you might have an IAM policy that allows certain principals to use any KMS key with a `"Purpose"="Test"` tag. Then you add the `"Purpose"="Test"` tag to a KMS key. Although the [TagResource](#) operation completes and [ListResourceTags](#) response confirms that the tag is assigned to the KMS key, the principals might not have access to the KMS key for up to five minutes.

To prevent errors, build this expected delay into your code.

Failed requests due to alias updates

When you update an alias, you associate an existing alias with a different KMS key.

[Decrypt](#) and [ReEncrypt](#) requests that specify the [alias name](#) or [alias ARN](#) might fail because the alias is now associated with a KMS key that didn't encrypt the ciphertext. This situation typically returns an `IncorrectKeyException` or `NotFoundException`. Or if the request has no `KeyId` or `DestinationKeyId` parameter, the operation might fail with `AccessDenied` exception because the caller no longer has access to the KMS key that encrypted the ciphertext.

You can trace the change by looking at CloudTrail logs for [CreateAlias](#), [UpdateAlias](#), and [DeleteAlias](#) log entries. You can also use the value of the `LastUpdatedDate` field in the [ListAliases](#) response to detect a change.

For example, the following [ListAliases](#) example response shows that the `ProjectAlpha_Test` alias in the `kms:ResourceAliases` condition was updated. As a result, the principals who have access based on the alias lose access to the previously associated KMS key. Instead, they have access to the newly associated KMS key.

```
$ aws kms list-aliases --query 'Aliases[?starts_with(AliasName, `alias/ProjectAlpha`)]'
```

```
{
  "Aliases": [
    {
      "AliasName": "alias/ProjectAlpha_Test",
      "AliasArn": "arn:aws:kms:us-west-2:111122223333:alias/ProjectAlpha_Test",
      "TargetKeyId": "0987dcba-09fe-87dc-65ba-ab0987654321",
      "CreationDate": 1566518783.394,
      "LastUpdatedDate": 1605308931.903
    },
    {
      "AliasName": "alias/ProjectAlpha_Restricted",
      "AliasArn": "arn:aws:kms:us-west-2:111122223333:alias/ProjectAlpha_Restricted",
      "TargetKeyId": "1234abcd-12ab-34cd-56ef-1234567890ab",
      "CreationDate": 1553410800.010,
      "LastUpdatedDate": 1553410800.010
    }
  ]
}
```

The remedy for this change isn't simple. You can update the alias again to associate it with the original KMS key. However, before you act, you need to consider the effect of that change on the currently associated KMS key. If principals used the latter KMS key in cryptographic operations,

they might need continued access to it. In this case, you might want to update the policy to ensure that principals have permission to use both of the KMS keys.

You can prevent an error like this one: Before updating an alias, search policies to detect access that depends on the alias. Then get KMS keys in all Regions that are associated with the alias. Give alias management permissions only to principals who need it and [limit their alias-management permissions](#) to aliases they need to manage.

RBAC for Amazon KMS

Role-based access control (RBAC) is an authorization strategy that only provides users with the permissions required to perform their job duties, and nothing more. Amazon KMS supports RBAC by allowing you to control access to your keys by specifying granular permissions on key usage within [key policies](#). Key policies specify a resource, action, effect, principal, and optional conditions to grant access to keys.

To implement RBAC in Amazon KMS, we recommend separating the permissions for key users and key administrators.

Key users

The following key policy example allows the `ExampleUserRole` IAM role to use the KMS key.

```
{
  "Sid": "Allow use of the key",
  "Effect": "Allow",
  "Principal": {
    "Amazon": "arn:aws-cn:iam::111122223333:role/ExampleUserRole"
  },
  "Action": [
    "kms:Encrypt",
    "kms:Decrypt",
    "kms:ReEncrypt*",
    "kms:GenerateDataKey*",
    "kms:DescribeKey"
  ],
  "Resource": "*"
}
```

Your key users might need fewer permissions than the user in this example. Only assign the permissions that the user needs. Use the following questions to help you further refine permissions.

- Which IAM principals (roles or users) need access to the key?
- Which actions does each principal need to perform with the key? For example, does the principal only need Encrypt and Sign permissions?
- Is the user a human or an Amazon service? If it's an Amazon service, you can use the [condition key](#) to restrict key usage to a specific Amazon service.

Key administrators

The following key policy example allows the `ExampleAdminRole` IAM role to administer the KMS key.

```
{
  "Sid": "Allow access for Key Administrators",
  "Effect": "Allow",
  "Principal": {
    "Amazon": "arn:aws-cn:iam::111122223333:role/ExampleAdminRole"
  },
  "Action": [
    "kms:Create*",
    "kms:Describe*",
    "kms:Enable*",
    "kms:List*",
    "kms:Put*",
    "kms:Update*",
    "kms:Revoke*",
    "kms:Disable*",
    "kms:Get*",
    "kms>Delete*",
    "kms:TagResource",
    "kms:UntagResource",
    "kms:ScheduleKeyDeletion",
    "kms:CancelKeyDeletion"
  ],
  "Resource": "*"
}
```

Your key administrators might need fewer permissions than the administrator in this example. Only assign the permissions that your key administrators need.

Only give users the permissions they need to fulfill their roles. A user's permissions might vary depending on whether the key is used in test or production environments. If you use less restrictive permissions in certain non-production environments, implement a process to test the policies before they're released to production.

Learn more

- [IAM identities \(users, user groups, and roles\)](#)
- [Types of access control](#)

Allowing users in other accounts to use a KMS key

You can allow users or roles in a different Amazon Web Services account to use a KMS key in your account. Cross-account access requires permission in the key policy of the KMS key and in an IAM policy in the external user's account.

Cross-account permission is effective only for the following operations:

- [Cryptographic operations](#)
- [CreateGrant](#)
- [DescribeKey](#)
- [GetKeyRotationStatus](#)
- [GetPublicKey](#)
- [ListGrants](#)
- [RetireGrant](#)
- [RevokeGrant](#)

If you give a user in a different account permission for other operations, those permissions have no effect. For example, if you give a principal in a different account [kms:ListKeys](#) permission in an IAM policy, or [kms:ScheduleKeyDeletion](#) permission on a KMS key in a key policy, the user's attempts to call those operations on your resources still fail.

For details about using KMS keys in different accounts for Amazon KMS operations, see the **Cross-account use** column in the [Amazon KMS permissions](#) and [Using KMS keys in other accounts](#). There is also a **Cross-account use** section in each API description in the [Amazon Key Management Service API Reference](#).

⚠ Warning

Be cautious about giving principals permissions to use your KMS keys. Whenever possible, follow the *least privilege* principle. Give users access only to the KMS keys they need for only the operations they require.

Also, be cautious about using any unfamiliar KMS key, especially a KMS key in a different account. Malicious users might give you permissions to use their KMS key to get information about you or your account.

For information about using policies to protect the resources in your account, see [Best practices for IAM policies](#).

To give permission to use a KMS key to users and roles in another account, you must use two different types of policies:

- The **key policy** for the KMS key must give the external account (or users and roles in the external account) permission to use the KMS key. The key policy is in the account that owns the KMS key.
- **IAM policies** in the external account must delegate the key policy permissions to its users and roles. These policies are set in the external account and give permissions to users and roles in that account.

The key policy determines who *can* have access to the KMS key. The IAM policy determines who *does* have access to the KMS key. Neither the key policy nor the IAM policy alone is sufficient—you must change both.

To edit the key policy, you can use the [Policy View](#) in the Amazon Web Services Management Console or use the [CreateKey](#) or [PutKeyPolicy](#) operations.

For help with editing IAM policies, see [Using IAM policies with Amazon KMS](#).

For an example that shows how the key policy and IAM policies work together to allow use of a KMS key in a different account, see [Example 2: User assumes role with permission to use a KMS key in a different Amazon Web Services account](#).

You can view the resulting cross-account Amazon KMS operations on the KMS key in your [Amazon CloudTrail logs](#). Operations that use KMS keys in other accounts are logged in both the caller's account and the KMS key owner account.

Topics

- [Step 1: Add a key policy statement in the local account](#)
- [Step 2: Add IAM policies in the external account](#)
- [Allowing use of external KMS keys with Amazon Web Services services](#)
- [Using KMS keys in other accounts](#)

Note

The examples in this topic show how to use a key policy and IAM policy together to provide and limit access to a KMS key. These generic examples are not intended to represent the permissions that any particular Amazon Web Services service requires on a KMS key. For information about the permissions that an Amazon Web Services service requires, see the encryption topic in the service documentation.

Step 1: Add a key policy statement in the local account

The key policy for a KMS key is the primary determinant of who can access the KMS key and which operations they can perform. The key policy is always in the account that owns the KMS key. Unlike IAM policies, key policies do not specify a resource. The resource is the KMS key that is associated with the key policy. When providing cross-account permission, the key policy for the KMS key must give the external account (or users and roles in the external account) permission to use the KMS key.

To give an external account permission to use the KMS key, add a statement to the key policy that specifies the external account. In the `Principal` element of the key policy, enter the Amazon Resource Name (ARN) of the external account.

When you specify an external account in a key policy, IAM administrators in the external account can use IAM policies to delegate those permissions to any users and roles in the external account. They can also decide which of the actions specified in the key policy the users and roles can perform.

Permissions given to the external account and its principals are effective only if the external account is enabled in the Region that hosts the KMS key and its key policy. For information about Regions that are not enabled by default ("opt-in Regions"), see [Managing Amazon Web Services Regions](#) in the *Amazon Web Services General Reference*.

For example, suppose you want to allow account 444455556666 to use a symmetric encryption KMS key in account 111122223333. To do that, add a policy statement like the one in the following example to the key policy for the KMS key in account 111122223333. This policy statement gives the external account, 444455556666, permission to use the KMS key in cryptographic operations for symmetric encryption KMS keys.

Note

The following example represents a sample key policy for sharing a KMS key with another account. Replace the example `Sid`, `Principal`, and `Action` values with valid values for the intended use of your KMS key.

```
{
  "Sid": "Allow an external account to use this KMS key",
  "Effect": "Allow",
  "Principal": {
    "AWS": [
      "arn:aws:iam::444455556666:root"
    ]
  },
  "Action": [
    "kms:Encrypt",
    "kms:Decrypt",
    "kms:ReEncrypt*",
    "kms:GenerateDataKey*",
    "kms:DescribeKey"
  ],
  "Resource": "*"
}
```

Instead of giving permission to the external account, you can specify particular external users and roles in the key policy. However, those users and roles cannot use the KMS key until IAM administrators in the external account attach the proper IAM policies to their identities. The IAM

policies can give permission to all or a subset of the external users and roles that are specified in the key policy. And they can allow all or a subset of the actions specified in the key policy.

Specifying identities in a key policy restricts the permissions that IAM administrators in the external account can provide. However, it makes policy management with two accounts more complex. For example, assume that you need to add a user or role. You must add that identity to the key policy in the account that owns the KMS key and create IAM policies in the identity's account.

To specify particular external users or roles in a key policy, in the `Principal` element, enter the Amazon Resource Name (ARN) of a user or role in the external account.

For example, the following example key policy statement allows `ExampleRole` in account 444455556666 to use a KMS key in account 111122223333. This key policy statement gives the external account, 444455556666, permission to use the KMS key in cryptographic operations for symmetric encryption KMS keys.

Note

The following example represents a sample key policy for sharing a KMS key with another account. Replace the example `Sid`, `Principal`, and `Action` values with valid values for the intended use of your KMS key.

```
{
  "Sid": "Allow an external account to use this KMS key",
  "Effect": "Allow",
  "Principal": {
    "AWS": "arn:aws:iam::444455556666:role/ExampleRole"
  },
  "Action": [
    "kms:Encrypt",
    "kms:Decrypt",
    "kms:ReEncrypt*",
    "kms:GenerateDataKey*",
    "kms:DescribeKey"
  ],
  "Resource": "*"
}
```

Note

Do not set the Principal to an asterisk (*) in any key policy statement that allows permissions unless you use [conditions](#) to limit the key policy. An asterisk gives every identity in every Amazon Web Services account permission to use the KMS key, unless another policy statement explicitly denies it. Users in other Amazon Web Services accounts can use your KMS key whenever they have corresponding permissions in their own account.

You also need to decide which permissions you want to give to the external account. For example, you might want to give users permission to decrypt but not encrypt, or permission to view the KMS key but not use it. For a list of permissions on KMS keys, see [Amazon KMS permissions](#).

Setting the key policy when you create a KMS key

When you use the [CreateKey](#) operation to create a KMS key, you can use its `Policy` parameter to specify a key policy that gives an external account, or external users and roles, permission to use the KMS key.

When you create a KMS key in the Amazon Web Services Management Console, you also create its key policy. When you select identities in the **Key Administrators** and **Key Users** sections, Amazon KMS adds policy statements for those identities to the KMS key's key policy. The **Key Users** section also lets you add external accounts as key users.

When you enter the account ID of an external account, Amazon KMS adds two statements to the key policy. This action only affects the key policy. Users and roles in the external account cannot use the KMS key until you attach IAM policies to give them some or all of these permissions.

The first key policy statement gives the external account permission to use the KMS key in cryptographic operations. The second key policy statement allows the external account to create, view, and revoke grants on the KMS key, but only when the request comes from an [Amazon service that is integrated with Amazon KMS](#). These permissions allow other Amazon services that encrypt user data to use the KMS key. These permissions are designed for KMS keys that encrypt user data in Amazon services

Step 2: Add IAM policies in the external account

The key policy in the account that owns the KMS key sets the valid range for permissions. But, users and roles in the external account cannot use the KMS key until you attach IAM policies that delegate those permissions, or use grants to manage access to the KMS key. The IAM policies are set in the external account.

If the key policy gives permission to the external account, you can attach IAM policies to any user or role in the account. But if the key policy gives permission to specified users or roles, the IAM policy can only give those permissions to all or a subset of the specified users and roles. If an IAM policy gives KMS key access to other external users or roles, it has no effect.

The key policy also limits the actions in the IAM policy. The IAM policy can delegate all or a subset of the actions specified in the key policy. If the IAM policy lists actions that are not specified in the key policy, those permissions are not effective.

The following example IAM policy allows the principal to use the KMS key in account 111122223333 for cryptographic operations. To give this permission to users and roles in account 444455556666, [attach the policy](#) to the users or roles in account 444455556666.

Note

The following example represents a sample IAM policy for sharing a KMS key with another account. Replace the example Sid, Resource, and Action values with valid values for the intended use of your KMS key.

```
{
  "Sid": "AllowUseOfKeyInAccount111122223333",
  "Effect": "Allow",
  "Action": [
    "kms:Encrypt",
    "kms:Decrypt",
    "kms:ReEncrypt*",
    "kms:GenerateDataKey*",
    "kms:DescribeKey"
  ],
  "Resource": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab"
}
```

Note the following details about this policy:

- Unlike key policies, IAM policy statements do not contain the `Principal` element. In IAM policies, the principal is the identity to which the policy is attached.
- The `Resource` element in the IAM policy identifies the KMS key that the principal can use. To specify a KMS key, add its [key ARN](#) to the `Resource` element.
- You can specify more than one KMS key in the `Resource` element. But if you don't specify particular KMS keys in the `Resource` element, you might inadvertently give access to more KMS keys than you intend.
- To allow the external user to use the KMS key with [Amazon services that integrate with Amazon KMS](#), you might need to add permissions to the key policy or the IAM policy. For details, see [Allowing use of external KMS keys with Amazon Web Services services](#).

For more information about working with IAM policies, see [IAM policies](#).

Allowing use of external KMS keys with Amazon Web Services services

You can give a user in a different account permission to use your KMS key with a service that is integrated with Amazon KMS. For example, a user in an external account can use your KMS key to encrypt the objects in an Amazon S3 bucket or to encrypt the secrets they store in Amazon Secrets Manager.

The key policy must give the external user or the external user's account permission to use the KMS key. In addition, you need to attach IAM policies to the identity that gives the user permission to use the Amazon Web Services service. The service might also require that users have additional permissions in the key policy or IAM policy. For a list of permissions that the Amazon Web Services service requires on a customer managed key, see the Data Protection topic in the Security chapter of the user guide or developer guide for the service.

Using KMS keys in other accounts

If you have permission to use a KMS key in a different Amazon Web Services account, you can use the KMS key in the Amazon Web Services Management Console, Amazon SDKs, Amazon CLI, and Amazon Tools for PowerShell.

To identify a KMS key in a different account in a shell command or API request, use the following [key identifiers](#).

- For [cryptographic operations](#), [DescribeKey](#), and [GetPublicKey](#), use the [key ARN](#) or [alias ARN](#) of the KMS key.
- For [CreateGrant](#), [GetKeyRotationStatus](#), [ListGrants](#), and [RevokeGrant](#), use the key ARN of the KMS key.

If you enter only a key ID or alias name, Amazon assumes the KMS key is in your account.

The Amazon KMS console does not display KMS keys in other accounts, even if you have permission to use them. Also, the lists of KMS keys displayed in the consoles of other Amazon services do not include KMS keys in other accounts.

To specify a KMS key in a different account in the console of an Amazon service, you must enter the key ARN or alias ARN of the KMS key. The required key identifier varies with the service, and might differ between the service console and its API operations. For details, see the service documentation.

Control access to multi-Region keys

You can use multi-Region keys in compliance, disaster recovery, and backup scenarios that would be more complex with single-Region keys. However, because the security properties of multi-Region keys are significantly different from those of single-Region keys, we recommend using caution when authorizing the creation, management, and use of multi-Region keys.

Note

Existing IAM policy statements with wildcard characters in the Resource field now apply to both single-Region and multi-Region keys. To restrict them to single-Region KMS keys or multi-Region keys, use the [kms:MultiRegion](#) condition key.

Use your authorization tools to prevent creation and use of multi-Region keys in any scenario where a single-Region will suffice. Allow principals to replicate a multi-Region key only into Amazon Web Services Regions that require them. Give permission for multi-Region keys only to principals who need them and only for tasks that require them.

You can use key policies, IAM policies, and grants to allow IAM principals to manage and use multi-Region keys in your Amazon Web Services account. Each multi-Region key is an independent

resource with a unique key ARN and key policy. You need to establish and maintain a key policy for each key and make sure that new and existing IAM policies implement your authorization strategy.

To support multi-Region keys, Amazon KMS uses an IAM service linked role. This role gives Amazon KMS the permissions it needs to synchronize [shared properties](#). For more information, see [Authorizing Amazon KMS to synchronize multi-Region keys](#).

Topics

- [Authorization basics for multi-Region keys](#)
- [Authorizing multi-Region key administrators and users](#)

Authorization basics for multi-Region keys

When designing key policies and IAM policies for multi-Region keys, consider the following principles.

- **Key policy** — Each multi-Region key is an independent KMS key resource with its own [key policy](#). You can apply the same or a different key policy to each key in the set of related multi-Region keys. Key policies are *not* [shared properties](#) of multi-Region keys. Amazon KMS does not copy or synchronize key policies among related multi-Region keys.

When you create a replica key in the Amazon KMS console, the console displays the current key policy of the primary key as a convenience. You can use this key policy, edit it, or delete and replace it. But even if you accept the primary key policy unchanged, Amazon KMS doesn't synchronize the policies. For example, if you change the key policy of the primary key, the key policy of the replica key remains the same.

- **Default key policy** — When you create multi-Region keys by using the [CreateKey](#) and [ReplicateKey](#) operations, the [default key policy](#) is applied unless you specify a key policy in the request. This is the same default key policy that is applied to single-Region keys.
- **IAM policies** — As with all KMS keys, you can use IAM policies to control access to multi-Region keys only when the [key policy allows it](#). [IAM policies](#) apply to all Amazon Web Services Regions by default. However, you can use condition keys, such as [aws:RequestedRegion](#), to limit permissions to a particular Region.

To create primary and replica keys, principals must have `kms:CreateKey` permission in an IAM policy that applies to the Region where the key is created.

- **Grants** — Amazon KMS [grants](#) are Regional. Each grant allows permissions to one KMS key. You can use grants to allow permissions to a multi-Region primary key or replica key. But you cannot use a single grant to allow permissions to multiple KMS keys, even if they are related multi-Region keys.
- **Key ARN** — Each multi-Region key has a [unique key ARN](#). The key ARNs of related multi-Region keys have the same partition, account, and key ID, but different Regions.

To apply an IAM policy statement to a particular multi-Region key, use its key ARN or a key ARN pattern that includes the Region. To apply an IAM policy statement to all related multi-Region keys, use a wildcard character (*) in the Region element of the ARN, as shown in the following example.

```
{
  "Effect": "Allow",
  "Action": [
    "kms:Describe*",
    "kms:List*"
  ],
  "Resource": {
    "arn:aws:kms:*::111122223333:key/mrk-1234abcd12ab34cd56ef1234567890ab"
  }
}
```

To apply a policy statement to all multi-Region keys in your Amazon Web Services account, you can use the [kms:MultiRegion](#) policy condition or a key ID pattern that includes the distinctive `mrk-` prefix.

- **Service-linked role** — Principals who create multi-Region primary keys must have [iam:CreateServiceLinkedRole](#) permission.

To synchronize the shared properties of related multi-Region keys, Amazon KMS assumes an IAM [service-linked role](#). Amazon KMS creates the service-linked role in the Amazon Web Services account whenever you create a multi-Region primary key. (If the role exists, Amazon KMS recreates it, which has no harmful effect.) The role is valid in all Regions. To allow Amazon KMS to create (or recreate) the service-linked role, principals who create multi-Region primary keys must have [iam:CreateServiceLinkedRole](#) permission.

Authorizing multi-Region key administrators and users

Principals who create and manage multi-Region keys need the following permissions in the primary and replica Regions:

- `kms:CreateKey`
- `kms:ReplicateKey`
- `kms:UpdatePrimaryRegion`
- `iam:CreateServiceLinkedRole`

Creating a primary key

To [create a multi-Region primary key](#), the principal needs [kms:CreateKey](#) and [iam:CreateServiceLinkedRole](#) permissions in an IAM policy that is effective in the primary key's Region. Principals who have these permissions can create single-Region and multi-Region keys unless you restrict their permissions.

The `iam:CreateServiceLinkedRole` permission allows Amazon KMS to create the [AWSServiceRoleForKeyManagementServiceMultiRegionKeys](#) role to synchronize the [shared properties](#) of related multi-Region keys.

For example, this IAM policy allows a principal to create any type of KMS key.

```
{
  "Version": "2012-10-17",
  "Statement": {
    "Action": [
      "kms:CreateKey",
      "iam:CreateServiceLinkedRole"
    ],
    "Effect": "Allow",
    "Resource": "*"
  }
}
```

To allow or deny permission to create multi-Region primary keys, use the [kms:MultiRegion](#) condition key. Valid values are `true` (multi-Region key) or `false` (single-Region key). For example, the following IAM policy statement uses a Deny action with the `kms:MultiRegion` condition key to prevent principals from creating multi-Region keys.

```
{
  "Version": "2012-10-17",
  "Statement": {
    "Action": "kms:CreateKey",
    "Effect": "Deny",
    "Resource": "*",
    "Condition": {
      "Bool": "kms:MultiRegion": true
    }
  }
}
```

Replicating keys

To [create a multi-Region replica key](#), the principal needs the following permissions:

- [kms:ReplicateKey](#) permission in the key policy of the primary key.
- [kms:CreateKey](#) permission in an IAM policy that is effective in the replica key Region.

Use caution when allowing these permissions. They allow principals to create KMS keys and the key policies that authorize their use. The `kms:ReplicateKey` permission also authorizes the transfer of key material across Region boundaries within Amazon KMS.

To restrict the Amazon Web Services Regions in which a multi-Region key can be replicated, use the [kms:ReplicaRegion](#) condition key. It limits only the `kms:ReplicateKey` permission. Otherwise, it has no effect. For example, the following key policy allows the principal to replicate this primary key, but only in the specified Regions.

```
{
  "Effect": "Allow",
  "Principal": {
    "AWS": "arn:aws:iam::111122223333:role/Administrator"
  },
  "Action": "kms:ReplicateKey",
  "Resource": "*",
  "Condition": {
    "StringEquals": {
      "kms:ReplicaRegion": [
        "us-east-1",
        "eu-west-3",
        "ap-southeast-2"
      ]
    }
  }
}
```

```
    ]
  }
}
```

Updating the primary Region

Authorized principals can convert a replica key to a primary key, which changes the former primary key into a replica. This action is known as [updating the primary Region](#). To update the primary Region, the principal needs [kms:UpdatePrimaryRegion](#) permission in both Regions. You can provide these permissions in a key policy or IAM policy.

- `kms:UpdatePrimaryRegion` on the primary key. This permission must be effective in the primary key Region.
- `kms:UpdatePrimaryRegion` on the replica key. This permission must be effective in the replica key Region.

For example, the following key policy gives users who can assume the Administrator role permission to update the primary Region of the KMS key. This KMS key can be the primary key or a replica key in this operation.

```
{
  "Effect": "Allow",
  "Resource": "*",
  "Principal": {
    "AWS": "arn:aws:iam::111122223333:role/Administrator"
  },
  "Action": "kms:UpdatePrimaryRegion"
}
```

To restrict the Amazon Web Services Regions that can host a primary key, use the [kms:PrimaryRegion](#) condition key. For example, the following IAM policy statement allows the principals to update the primary Region of the multi-Region keys in the Amazon Web Services account, but only when the new primary Region is one of the specified Regions.

```
{
  "Effect": "Allow",
  "Action": "kms:UpdatePrimaryRegion",
  "Resource": {
```

```

    "arn:aws:kms:*:111122223333:key/*"
  },
  "Condition": {
    "StringEquals": {
      "kms:PrimaryRegion": [
        "us-west-2",
        "sa-east-1",
        "ap-southeast-1"
      ]
    }
  }
}
}
}

```

Using and managing multi-Region keys

By default, principals who have permission to use and manage KMS keys in an Amazon Web Services account and Region also have permission to use and manage multi-Region keys. However, you can use the [kms:MultiRegion](#) condition key to allow only single-Region keys or only multi-Region keys. Or use the [kms:MultiRegionKeyType](#) condition key to allow only multi-Region primary keys or only replica keys. Both condition keys controls access to the [CreateKey](#) operation and to any operation that uses an existing KMS key, such as [Encrypt](#) or [EnableKey](#).

The following example IAM policy statement uses the `kms:MultiRegion` condition key to prevent the principals from using or managing any multi-Region key.

```

{
  "Effect": "Deny",
  "Action": "kms:*",
  "Resource": "*",
  "Condition": {
    "Bool": "kms:MultiRegion": true
  }
}
}

```

This example IAM policy statement uses the `kms:MultiRegionKeyType` condition to allow principals to schedule and cancel key deletion, but only on multi-Region replica keys.

```

{
  "Effect": "Allow",
  "Action": [
    "kms:ScheduleKeyDeletion",

```

```
    "kms:CancelKeyDeletion"
  ],
  "Resource": {
    "arn:aws:kms:us-west-2:111122223333:key/*"
  },
  "Condition": {
    "StringEquals": "kms:MultiRegionKeyType": "REPLICA"
  }
}
```

Determining access to Amazon KMS keys

To determine the full extent of who or what currently has access to an Amazon KMS key, you must examine the key policy of the KMS key, all [grants](#) that apply to the KMS key, and potentially all Amazon Identity and Access Management (IAM) policies. You might do this to determine the scope of potential usage of a KMS key, or to help you meet compliance or auditing requirements. The following topics can help you generate a complete list of the Amazon principals (identities) that currently have access to a KMS key.

Topics

- [Examining the key policy](#)
- [Examining IAM policies](#)
- [Examining grants](#)

Examining the key policy

[Key policies](#) are the primary way to control access to KMS keys. Every KMS key has exactly one key policy.

When a key policy consists of or includes the [default key policy](#), the key policy allows IAM administrators in the account to use IAM policies to control access to the KMS key. Also, if the key policy gives [another Amazon Web Services account](#) permission to use the KMS key, the IAM administrators in the external account can use IAM policies to delegate those permissions. To determine the complete list of principals that can access the KMS key, [examine the IAM policies](#).

To view the key policy of an Amazon KMS [customer managed key](#) or [Amazon managed key](#) in your account, use the Amazon Web Services Management Console or the [GetKeyPolicy](#) operation in the Amazon KMS API. To view the key policy, you must have `kms:GetKeyPolicy` permissions for the

KMS key. For instructions for viewing the key policy for a KMS key, see [the section called “View a key policies”](#).

Examine the key policy document and take note of all principals specified in each policy statement's `Principal` element. In a policy statement with an `Allow` effect, the IAM users, IAM roles, and Amazon Web Services accounts in the `Principal` element have access to this KMS key.

Note

Do not set the `Principal` to an asterisk (*) in any key policy statement that allows permissions unless you use [conditions](#) to limit the key policy. An asterisk gives every identity in every Amazon Web Services account permission to use the KMS key, unless another policy statement explicitly denies it. Users in other Amazon Web Services accounts can use your KMS key whenever they have corresponding permissions in their own account.

The following examples use the policy statements found in the [default key policy](#) to demonstrate how to do this.

Example Policy statement 1

```
{
  "Sid": "Enable IAM User Permissions",
  "Effect": "Allow",
  "Principal": {"AWS": "arn:aws:iam::111122223333:root"},
  "Action": "kms:*",
  "Resource": "*"
}
```

In policy statement 1, `arn:aws:iam::111122223333:root` is an [Amazon account principal](#) that refers to the Amazon Web Services account 111122223333. (It is not the account root user.) By default, a policy statement like this one is included in the key policy document when you create a new KMS key with the Amazon Web Services Management Console, or create a new KMS key programmatically but do not provide a key policy.

A key policy document with a statement that allows access to the Amazon Web Services account enables [IAM policies in the account to allow access to the KMS key](#). This means that users and roles in the account might have access to the KMS key even if they are not explicitly listed as principals in the key policy document. Take care to [examine all IAM policies](#) in all Amazon Web Services accounts listed as principals to determine whether they allow access to this KMS key.

Example Policy statement 2

```
{
  "Sid": "Allow access for Key Administrators",
  "Effect": "Allow",
  "Principal": {"AWS": "arn:aws:iam::111122223333:role/KMSKeyAdmins"},
  "Action": [
    "kms:Describe*",
    "kms:Put*",
    "kms:Create*",
    "kms:Update*",
    "kms:Enable*",
    "kms:Revoke*",
    "kms:List*",
    "kms:Disable*",
    "kms:Get*",
    "kms>Delete*",
    "kms:ScheduleKeyDeletion",
    "kms:CancelKeyDeletion"
  ],
  "Resource": "*"
}
```

In policy statement 2, `arn:aws:iam::111122223333:role/KMSKeyAdmins` refers to the IAM role named `KMSKeyAdmins` in Amazon Web Services account `111122223333`. Users who are authorized to assume this role are allowed to perform the actions listed in the policy statement, which are the administrative actions for managing a KMS key.

Example Policy statement 3

```
{
  "Sid": "Allow use of the key",
  "Effect": "Allow",
  "Principal": {"AWS": "arn:aws:iam::111122223333:role/EncryptionApp"},
  "Action": [
    "kms:DescribeKey",
    "kms:GenerateDataKey*",
    "kms:Encrypt",
    "kms:ReEncrypt*",
    "kms:Decrypt"
  ],
  "Resource": "*"
}
```



```
}
```

In policy statement 3, `arn:aws:iam::111122223333:role/EncryptionApp` refers to the IAM role named `EncryptionApp` in Amazon Web Services account `111122223333`. Principals who are authorized to assume this role are allowed to perform the actions listed in the policy statement, which include the [cryptographic operations](#) for a symmetric encryption KMS key.

Example Policy statement 4

```
{
  "Sid": "Allow attachment of persistent resources",
  "Effect": "Allow",
  "Principal": {"AWS": "arn:aws:iam::111122223333:role/EncryptionApp"},
  "Action": [
    "kms:ListGrants",
    "kms:CreateGrant",
    "kms:RevokeGrant"
  ],
  "Resource": "*",
  "Condition": {"Bool": {"kms:GrantIsForAWSResource": true}}
}
```

In policy statement 4, `arn:aws:iam::111122223333:role/EncryptionApp` refers to the IAM role named `EncryptionApp` in Amazon Web Services account `111122223333`. Principals who are authorized assume this role are allowed to perform the actions listed in the policy statement. These actions, when combined with the actions allowed in **Example policy statement 3**, are those necessary to delegate use of the KMS key to most [Amazon services that integrate with Amazon KMS](#), specifically the services that use [grants](#). The [kms:GrantIsForAWSResource](#) value in the `Condition` element ensures that the delegation is allowed only when the delegate is an Amazon service that integrates with Amazon KMS and uses grants for authorization.

To learn all the different ways you can specify a principal in a key policy document, see [Specifying a Principal](#) in the *IAM User Guide*.

To learn more about Amazon KMS key policies, see [Key policies in Amazon KMS](#).

Examining IAM policies

In addition to the key policy and grants, you can also use [IAM policies](#) to allow access to a KMS key. For more information about how IAM policies and key policies work together, see [Troubleshooting Amazon KMS permissions](#).

To determine which principals currently have access to a KMS key through IAM policies, you can use the browser-based [IAM Policy Simulator](#) tool, or you can make requests to the IAM API.

Ways to examine IAM policies

- [Examining IAM policies with the IAM policy simulator](#)
- [Examining IAM policies with the IAM API](#)

Examining IAM policies with the IAM policy simulator

The IAM Policy Simulator can help you learn which principals have access to a KMS key through an IAM policy.

To use the IAM policy simulator to determine access to a KMS key

1. Sign in to the Amazon Web Services Management Console and then open the IAM Policy Simulator at <https://policysim.aws.amazon.com/>.
2. In the **Users, Groups, and Roles** pane, choose the user, group, or role whose policies you want to simulate.
3. (Optional) Clear the check box next to any policies that you want to omit from the simulation. To simulate all policies, leave all policies selected.
4. In the **Policy Simulator** pane, do the following:
 - a. For **Select service**, choose **Key Management Service**.
 - b. To simulate specific Amazon KMS actions, for **Select actions**, choose the actions to simulate. To simulate all Amazon KMS actions, choose **Select All**.
5. (Optional) The Policy Simulator simulates access to all KMS keys by default. To simulate access to a specific KMS key, choose **Simulation Settings** and then type the Amazon Resource Name (ARN) of the KMS key to simulate.
6. Choose **Run Simulation**.

You can view the results of the simulation in the **Results** section. Repeat steps 2 through 6 for every user, group, and role in the Amazon Web Services account.

Examining IAM policies with the IAM API

You can use the IAM API to examine IAM policies programmatically. The following steps provide a general overview of how to do this:

1. For each Amazon Web Services account listed as a principal in the key policy (that is, each [Amazon account principal](#) specified in this format: "Principal": {"AWS": "arn:aws:iam::111122223333:root"}), use the [ListUsers](#) and [ListRoles](#) operations in the IAM API to get all users and roles in the account.
2. For each user and role in the list, use the [SimulatePrincipalPolicy](#) operation in the IAM API, passing in the following parameters:
 - For `PolicySourceArn`, specify the Amazon Resource Name (ARN) of a user or role from your list. You can specify only one `PolicySourceArn` for each `SimulatePrincipalPolicy` request, so you must call this operation multiple times, once for each user and role in your list.
 - For the `ActionNames` list, specify every Amazon KMS API action to simulate. To simulate all Amazon KMS API actions, use `kms:*`. To test individual Amazon KMS API actions, precede each API action with "kms:", for example "kms:ListKeys". For a complete list of Amazon KMS API actions, see [Actions](#) in the *Amazon Key Management Service API Reference*.
 - (Optional) To determine whether the users or roles have access to specific KMS keys, use the `ResourceArns` parameter to specify a list of the Amazon Resource Names (ARNs) of the KMS keys. To determine whether the users or roles have access to any KMS key, omit the `ResourceArns` parameter.

IAM responds to each `SimulatePrincipalPolicy` request with an evaluation decision: `allowed`, `explicitDeny`, or `implicitDeny`. For each response that contains an evaluation decision of `allowed`, the response includes the name of the specific Amazon KMS API operation that is allowed. It also includes the ARN of the KMS key that was used in the evaluation, if any.

Examining grants

Grants are advanced mechanisms for specifying permissions that you or an Amazon service integrated with Amazon KMS can use to specify how and when a KMS key can be used. Grants are attached to a KMS key, and each grant contains the principal who receives permission to use the KMS key and a list of operations that are allowed. Grants are an alternative to the key policy, and are useful for specific use cases. For more information, see [Grants in Amazon KMS](#).

To get a list of grants for a KMS key, use the Amazon KMS [ListGrants](#) operation. You can examine the grants for a KMS key to determine who or what currently has access to use the KMS key via those grants. For example, the following is a JSON representation of a grant that was obtained from the [list-grants](#) command in the Amazon CLI.

```
{"Grants": [{
```

```

"Operations": ["Decrypt"],
"KeyId": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab",
"Name": "0d8aa621-43ef-4657-b29c-3752c41dc132",
"RetiringPrincipal": "arn:aws:iam::123456789012:root",
"GranteePrincipal": "arn:aws:sts::111122223333:assumed-role/aws:ec2-infrastructure/
i-5d476fab",
"GrantId": "dc716f53c93acacf291b1540de3e5a232b76256c83b2ecb22cdefa26576a2d3e",
"IssuingAccount": "arn:aws:iam::111122223333:root",
"CreationDate": 1.444151834E9,
"Constraints": {"EncryptionContextSubset": {"aws:ebs:id": "vol-5cccfb4e"}}
}}

```

To find out who or what has access to use the KMS key, look for the `"GranteePrincipal"` element. In the preceding example, the grantee principal is an assumed role user that is associated with the EC2 instance `i-5d476fab`. The EC2 infrastructure uses this role to attach the encrypted EBS volume `vol-5cccfb4e` to the instance. In this case, the EC2 infrastructure role has permission to use the KMS key because you previously created an encrypted EBS volume that is protected by this KMS key. You then attached the volume to an EC2 instance.

The following is another example of a JSON representation of a grant that was obtained from the [list-grants](#) command in the Amazon CLI. In the following example, the grantee principal is another Amazon Web Services account.

```

{"Grants": [{
  "Operations": ["Encrypt"],
  "KeyId": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab",
  "Name": "",
  "GranteePrincipal": "arn:aws:iam::444455556666:root",
  "GrantId": "f271e8328717f8bde5d03f4981f06a6b3fc18bcae2da12ac38bd9186e7925d11",
  "IssuingAccount": "arn:aws:iam::111122223333:root",
  "CreationDate": 1.444151269E9
}]}

```

Encryption context

Note

You cannot specify an encryption context in a cryptographic operation with an [asymmetric KMS key](#) or an [HMAC KMS key](#). Asymmetric algorithms and MAC algorithms do not support an encryption context.

All Amazon KMS [cryptographic operations](#) with [symmetric encryption KMS keys](#) accept an *encryption context*, an optional set of non-secret key–value pairs that can contain additional contextual information about the data. You can insert encryption context in Encrypt operations in Amazon KMS to enhance the authorization and auditability of your Amazon KMS API decryption calls. Amazon KMS uses the encryption context as additional authenticated data (AAD) to support authenticated encryption. The encryption context is cryptographically bound to the ciphertext so that the same encryption context is required to decrypt the data.

The encryption context is not secret and not encrypted. It appears in plaintext in [Amazon CloudTrail Logs](#) so you can use it to identify and categorize your cryptographic operations. Your encryption context should not include sensitive information. We recommend that your encryption context describe the data being encrypted or decrypted. For example, when you encrypt a file, you might use part of the file path as encryption context.

```
"encryptionContext": {
  "department": "10103.0"
}
```

For example, when encrypting volumes and snapshots created with the [Amazon Elastic Block Store](#) (Amazon EBS) [CreateSnapshot](#) operation, Amazon EBS uses the volume ID as encryption context value.

```
"encryptionContext": {
  "aws:ebs:id": "vol-abcde12345abc1234"
}
```

You can also use the encryption context to refine or limit access to Amazon KMS keys in your account. You can use the encryption context [as a constraint in grants](#) and as a [condition in policy statements](#).

To learn how to use encryption context to protect the integrity of encrypted data, see the post [How to Protect the Integrity of Your Encrypted Data by Using Amazon Key Management Service and EncryptionContext](#) on the Amazon Security Blog.

Encryption context rules

Amazon KMS enforces the following rules for encryption context keys and values.

- The key and value in an encryption context pair must be simple literal strings. If you use a different type, such as an integer or float, Amazon KMS interprets it as a string.
- The keys and values in an encryption context can include Unicode characters. If an encryption context includes characters that are not permitted in key policies or IAM policies, you won't be able to specify the encryption context in policy condition keys, such as [kms:EncryptionContext:context-key](#) and [kms:EncryptionContextKeys](#). For details about key policy document rules, see [Key policy format](#). For details about IAM policy document rules, see [IAM name requirements](#) in the *IAM User Guide*.

Encryption context in policies

The encryption context is used primarily to verify integrity and authenticity. But you can also use the encryption context to control access to symmetric encryption Amazon KMS keys in key policies and IAM policies.

The [kms:EncryptionContext:](#) and [kms:EncryptionContextKeys](#) condition keys allow (or deny) a permission only when the request includes particular encryption context keys or key–value pairs.

For example, the following key policy statement allows the RoleForExampleApp role to use the KMS key in Decrypt operations. It uses the `kms:EncryptionContext:context-key` condition key to allow this permission only when the encryption context in the request includes an `AppName:ExampleApp` encryption context pair.

```
{
  "Effect": "Allow",
  "Principal": {
    "AWS": "arn:aws:iam::111122223333:role/RoleForExampleApp"
  },
  "Action": "kms:Decrypt",
  "Resource": "*",
  "Condition": {
```

```
"StringEquals": {
  "kms:EncryptionContext:AppName": "ExampleApp"
}
}
```

For more information about these encryption context condition keys, see [Condition keys for Amazon KMS](#).

Encryption context in grants

When you [create a grant](#), you can include [grant constraints](#) that establish conditions for the grant permissions. Amazon KMS supports two grant constraints, `EncryptionContextEquals` and `EncryptionContextSubset`, both of which involve the [encryption context](#) in a request for a cryptographic operation. When you use these grant constraints, the permissions in the grant are effective only when the encryption context in the request for the cryptographic operation satisfies the requirements of the grant constraints.

For example, you can add an `EncryptionContextEquals` grant constraint to a grant that allows the [GenerateDataKey](#) operation. With this constraint, the grant allows the operation only when the encryption context in the request is a case-sensitive match for the encryption context in the grant constraint.

```
$ aws kms create-grant \
  --key-id 1234abcd-12ab-34cd-56ef-1234567890ab \
  --grantee-principal arn:aws:iam::111122223333:user/exampleUser \
  --retiring-principal arn:aws:iam::111122223333:role/adminRole \
  --operations GenerateDataKey \
  --constraints EncryptionContextEquals={Purpose=Test}
```

A request like the following from the grantee principal would satisfy the `EncryptionContextEquals` constraint.

```
$ aws kms generate-data-key \
  --key-id 1234abcd-12ab-34cd-56ef-1234567890ab \
  --key-spec AES_256 \
  --encryption-context Purpose=Test
```

For details about the grant constraints, see [Using grant constraints](#). For detailed information about grants, see [the section called “Grants”](#).

Logging encryption context

Amazon KMS uses Amazon CloudTrail to log the encryption context so you can determine which KMS keys and data have been accessed. The log entry shows exactly which KMS keys was used to encrypt or decrypt specific data referenced by the encryption context in the log entry.

Important

Because the encryption context is logged, it must not contain sensitive information.

Storing encryption context

To simplify use of any encryption context when you call the [Decrypt](#) or [ReEncrypt](#) operations, you can store the encryption context alongside the encrypted data. We recommend that you store only enough of the encryption context to help you create the full encryption context when you need it for encryption or decryption.

For example, if the encryption context is the fully qualified path to a file, store only part of that path with the encrypted file contents. Then, when you need the full encryption context, reconstruct it from the stored fragment. If someone tampers with the file, such as renaming it or moving it to a different location, the encryption context value changes and the decryption request fails.

Testing your permissions

To use Amazon KMS, you must have credentials that Amazon can use to authenticate your API requests. The credentials must include the permission to access KMS keys and aliases. The permissions are determined by key policies, IAM policies, grants, and cross-account access controls. In addition to controlling access to KMS keys, you can control access to your CloudHSM, and to your custom key stores.

You can specify the `DryRun` API parameter to verify that you have the necessary permissions to use Amazon KMS keys. You can also use `DryRun` to verify that the request parameters in a Amazon KMS API call are correctly specified.

Topics

- [What is the DryRun parameter?](#)

- [Specifying DryRun with the API](#)

What is the DryRun parameter?

DryRun is an optional API parameter that you specify to verify that Amazon KMS API calls will succeed. Use DryRun to test your API call, before actually making the call to Amazon KMS. You can verify the following.

- That you have the necessary permissions to use Amazon KMS keys.
- That you have specified the parameters in the call correctly.

Amazon KMS supports using the DryRun parameter in certain API actions:

- [CreateGrant](#)
- [Decrypt](#)
- [DeriveSharedSecret](#)
- [Encrypt](#)
- [GenerateDataKey](#)
- [GenerateDataKeyPair](#)
- [GenerateDataKeyPairWithoutPlaintext](#)
- [GenerateDataKeyWithoutPlaintext](#)
- [GenerateMac](#)
- [ReEncrypt](#)
- [RetireGrant](#)
- [RevokeGrant](#)
- [Sign](#)
- [Verify](#)
- [VerifyMac](#)

Using the DryRun parameter will incur charges and will be billed as a standard API request. For more information about Amazon KMS pricing, see [Amazon Key Management Service Pricing](#).

All API requests using the DryRun parameter apply to the request quota of the API and can result in a throttling exception if you exceed an API request quota. For example, calling [Decrypt](#)

with `DryRun` or without `DryRun` counts against the same cryptographic operations quota. See [Throttling Amazon KMS requests](#) to learn more.

Every call to an Amazon KMS API operation is captured as an event and recorded in an Amazon CloudTrail log. The output of any operations that specify the `DryRun` parameter appear in your CloudTrail log. For more information, see [Logging Amazon KMS API calls with Amazon CloudTrail](#).

Specifying DryRun with the API

To use `DryRun`, specify the `--dry-run` parameter in Amazon CLI commands and Amazon KMS API calls that support the parameter. When you do, Amazon KMS will verify whether your call will succeed. Amazon KMS calls that use `DryRun` will always fail and return a message with information about reason why the call failed. The message can include the following exceptions:

- `DryRunOperationException` - The request would succeed if `DryRun` wasn't specified.
- `ValidationException` - The request failed from specifying an incorrect API parameter.
- `AccessDeniedException` - You do not have permissions to perform the specified API action on the KMS resource.

For example, the following command uses the [CreateGrant](#) operation and creates a grant that allows users who are authorized to assume the `keyUserRole` role to call the [Decrypt](#) operation on a specified [symmetric KMS key](#). The `DryRun` parameter is specified.

```
$ aws kms create-grant \  
  --key-id 1234abcd-12ab-34cd-56ef-1234567890ab \  
  --grantee-principal arn:aws:iam::111122223333:role/keyUserRole \  
  --operations Decrypt \  
  --dry-run
```

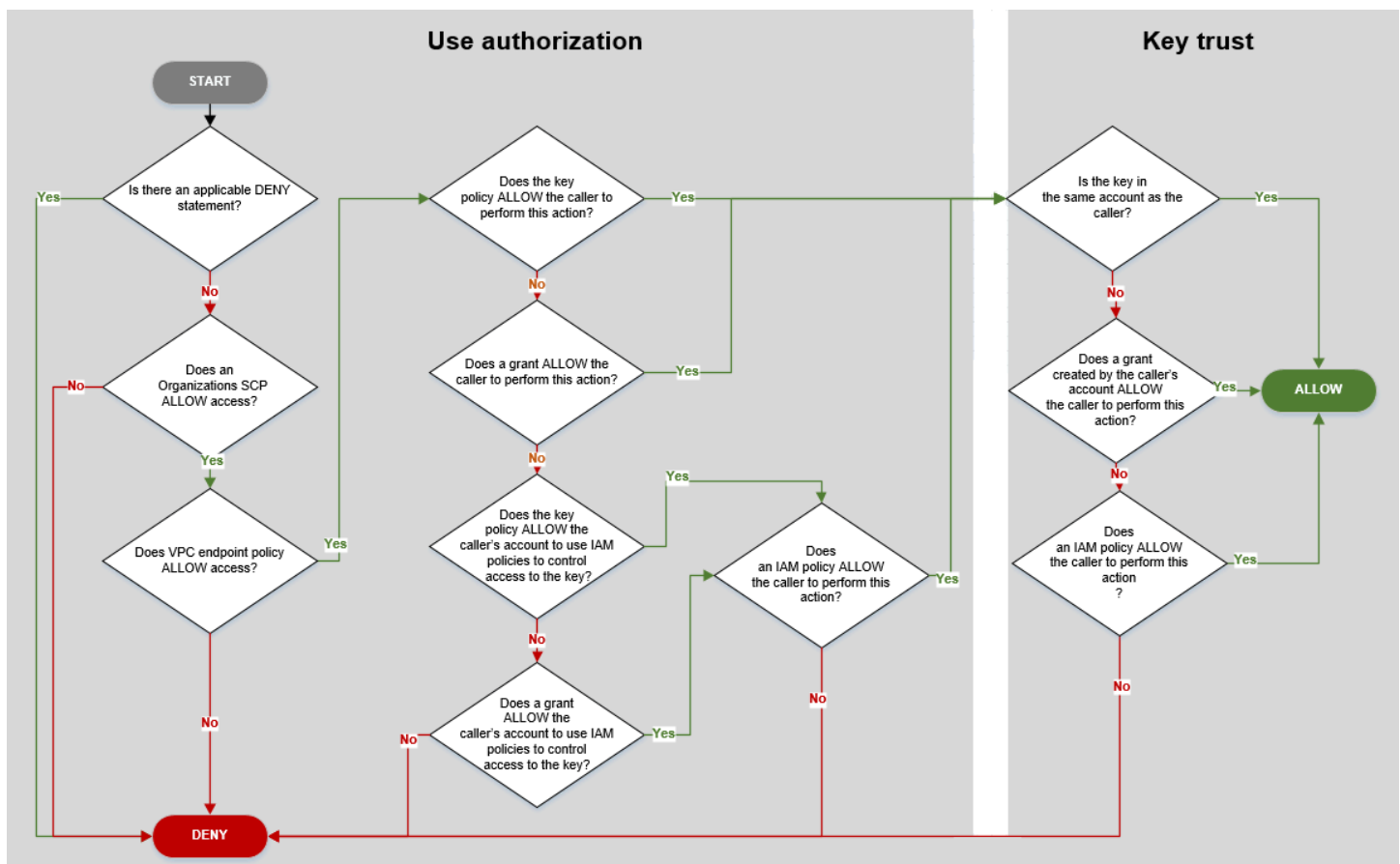
Troubleshooting Amazon KMS permissions

When authorizing access to a KMS key, Amazon KMS evaluates the following:

- The [key policy](#) that is attached to the KMS key. The key policy is always defined in the Amazon Web Services account and Region that owns the KMS key.
- All [IAM policies](#) that are attached to the user or role making the request. IAM policies that govern a principal's use of a KMS key are always defined in the principal's Amazon Web Services account.
- All [grants](#) that apply to the KMS key.

- Other types of policies that might apply to the request to use the KMS key, such as [Amazon Organizations service control policies](#) and [VPC endpoint policies](#). These policies are optional and allow all actions by default, but you can use them to restrict permissions otherwise given to principals.

Amazon KMS evaluates these policy mechanisms together to determine whether access to the KMS key is allowed or denied. To do this, Amazon KMS uses a process similar to the one depicted in the following flowchart. The following flowchart provides a visual representation of the policy evaluation process.



This flowchart is divided into two parts. The parts appear to be sequential, but they are typically evaluated at the same time.

- *Use authorization* determines whether you are permitted to use a KMS key based on its key policy, IAM policies, grants, and other applicable policies.
- *Key trust* determines whether you should trust a KMS key that you are permitted to use. In general, you trust the resources in your Amazon Web Services account. But, you can also feel

confident about using KMS keys in a different Amazon Web Services account if a grant or IAM policy in your account allows you to use the KMS key.

You can use this flowchart to discover why a caller was allowed or denied permission to use a KMS key. You can also use it to evaluate your policies and grants. For example, the flowchart shows that a caller can be denied access by an explicit DENY statement, or by the absence of an explicit ALLOW statement, in the key policy, IAM policy, or grant.

The flowchart can explain some common permission scenarios.

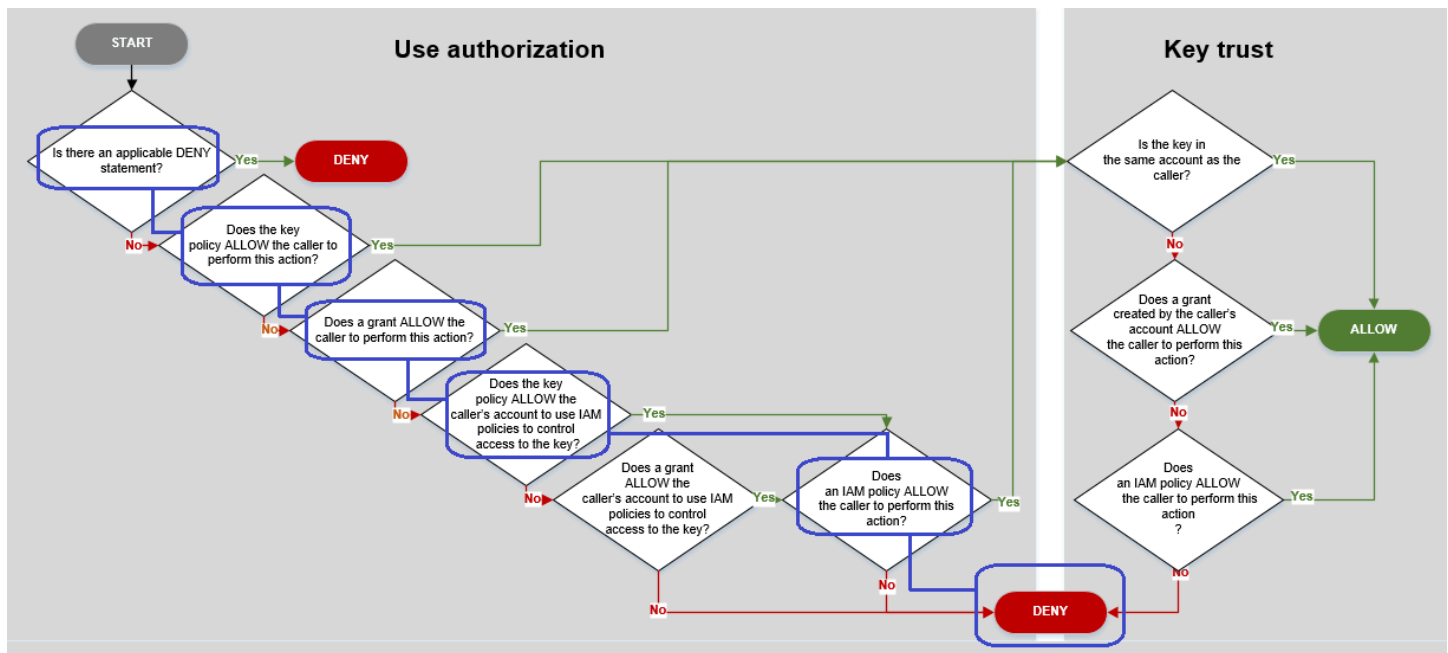
Permission Examples

- [Example 1: User is denied access to a KMS key in their Amazon Web Services account](#)
- [Example 2: User assumes role with permission to use a KMS key in a different Amazon Web Services account](#)

Example 1: User is denied access to a KMS key in their Amazon Web Services account

Alice is an IAM user in the 111122223333 Amazon Web Services account. She was denied access to a KMS key in same Amazon Web Services account. Why can't Alice use the KMS key?

In this case, Alice is denied access to the KMS key because there is no key policy, IAM policy, or grant that gives her the required permissions. The key policy of the KMS key allows the Amazon Web Services account to use IAM policies to control access to the KMS key, but no IAM policy gives Alice permission to use the KMS key.



Consider the relevant policies for this example.

- The KMS key that Alice wants to use has the [default key policy](#). This policy [allows the Amazon Web Services account](#) that owns the KMS key to use IAM policies to control access to the KMS key. This key policy satisfies the *Does the key policy ALLOW the callers account to use IAM policies to control access to the key?* condition in the flowchart.

```
{
  "Version" : "2012-10-17",
  "Id" : "key-test-1",
  "Statement" : [ {
    "Sid" : "Delegate to IAM policies",
    "Effect" : "Allow",
    "Principal" : {
      "AWS" : "arn:aws:iam::111122223333:root"
    },
    "Action" : "kms:*",
    "Resource" : "*"
  } ]
}
```

- However, no key policy, IAM policy, or grant gives Alice permission to use the KMS key. Therefore, Alice is denied permission to use the KMS key.

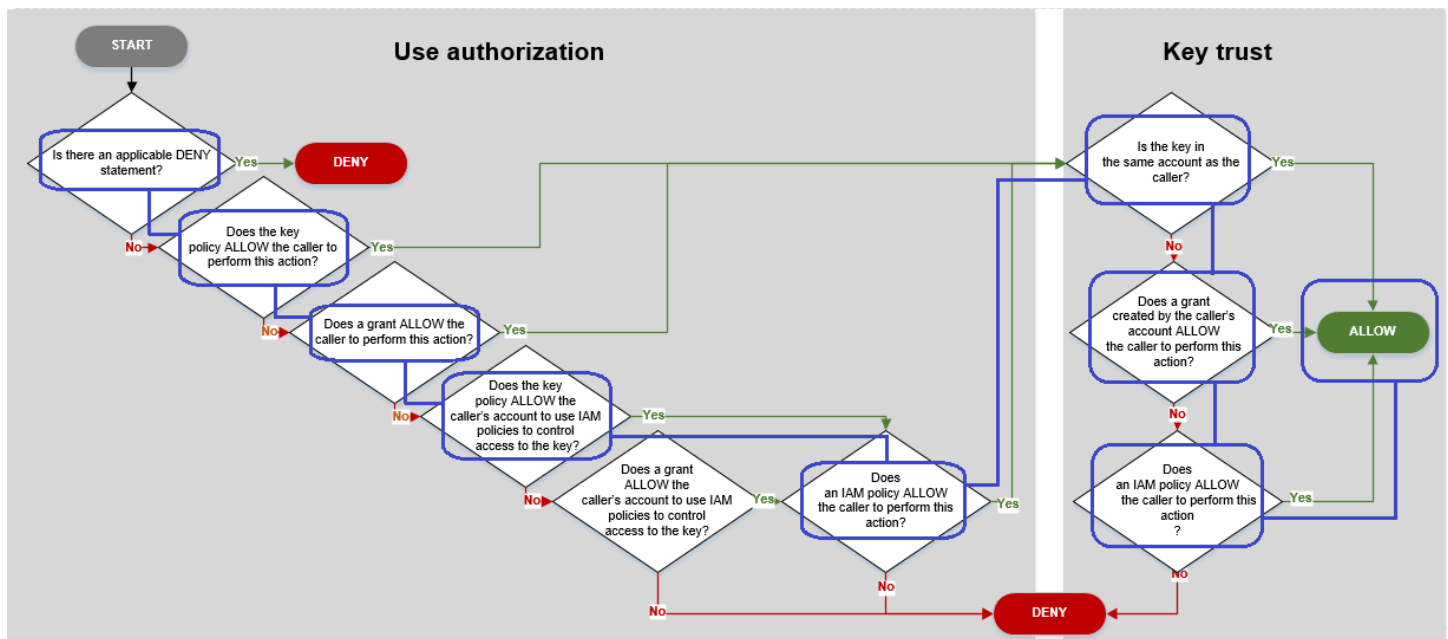
Example 2: User assumes role with permission to use a KMS key in a different Amazon Web Services account

Bob is a user in account 1 (111122223333). He is allowed to use a KMS key in account 2 (444455556666) in [cryptographic operations](#). How is this possible?

Tip

When evaluating cross-account permissions, remember that the key policy is specified in the KMS key's account. The IAM policy is specified in the caller's account, even when the caller is in a different account. For details about providing cross-account access to KMS keys, see [Allowing users in other accounts to use a KMS key](#).

- The key policy for the KMS key in account 2 allows account 2 to use IAM policies to control access to the KMS key.
- The key policy for the KMS key in account 2 allows account 1 to use the KMS key in cryptographic operations. However, account 1 must use IAM policies to give its principals access to the KMS key.
- An IAM policy in account 1 allows the `Engineering` role to use the KMS key in account 2 for cryptographic operations.
- Bob, a user in account 1, has permission to assume the `Engineering` role.
- Bob can trust this KMS key, because even though it is not in his account, an IAM policy in his account gives him explicit permission to use this KMS key.



Consider the policies that let Bob, a user in account 1, use the KMS key in account 2.

- The key policy for the KMS key allows account 2 (444455556666, the account that owns the KMS key) to use IAM policies to control access to the KMS key. This key policy also allows account 1 (111122223333) to use the KMS key in cryptographic operations (specified in the `Action` element of the policy statement). However, no one in account 1 can use the KMS key in account 2 until account 1 defines IAM policies that give the principals access to the KMS key.

In the flowchart, this key policy in account 2 satisfies the *Does the key policy ALLOW the caller's account to use IAM policies to control access to the key?* condition.

```

{
  "Id": "key-policy-acct-2",
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "Permission to use IAM policies",
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::444455556666:root"
      },
      "Action": "kms:*",
      "Resource": "*"
    }
  ],
}

```

```

    "Sid": "Allow account 1 to use this KMS key",
    "Effect": "Allow",
    "Principal": {
      "AWS": "arn:aws:iam::111122223333:root"
    },
    "Action": [
      "kms:Encrypt",
      "kms:Decrypt",
      "kms:ReEncryptFrom",
      "kms:ReEncryptTo",
      "kms:GenerateDataKey",
      "kms:GenerateDataKeyWithoutPlaintext",
      "kms:DescribeKey"
    ],
    "Resource": "*"
  }
]
}

```

- An IAM policy in the caller's Amazon Web Services account (account 1, 111122223333) gives the principal permission to perform cryptographic operations using the KMS key in account 2 (444455556666). The Action element delegates to the principal the same permissions that the key policy in account 2 gave to account 1. To give these permission to the Engineering role in account 1, [this inline policy is embedded](#) in the Engineering role.

Cross-account IAM policies like this one are effective only when the key policy for the KMS key in account 2 gives account 1 permission to use the KMS key. Also, account 1 can only give its principals permission to perform the actions that the key policy gave to the account.

In the flowchart, this satisfies the *Does an IAM policy allow the caller to perform this action?* condition.

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "kms:Encrypt",
        "kms:Decrypt",
        "kms:ReEncryptFrom",
        "kms:ReEncryptTo",

```



```

        "kms:GenerateDataKey",
        "kms:GenerateDataKeyWithoutPlaintext",
        "kms:DescribeKey"
    ],
    "Resource": [
        "arn:aws:kms:us-
west-2:444455556666:key/1234abcd-12ab-34cd-56ef-1234567890ab"
    ]
}

```

- The last required element is the definition of the Engineering role in account 1. The AssumeRolePolicyDocument in the role allows Bob to assume the Engineering role.

```

{
  "Role": {
    "Arn": "arn:aws:iam::111122223333:role/Engineering",
    "CreateDate": "2019-05-16T00:09:25Z",
    "AssumeRolePolicyDocument": {
      "Version": "2012-10-17",
      "Statement": {
        "Principal": {
          "AWS": "arn:aws:iam::111122223333:user/bob"
        },
        "Effect": "Allow",
        "Action": "sts:AssumeRole"
      }
    },
    "Path": "/",
    "RoleName": "Engineering",
    "RoleId": "AR0A4KJY2TU23Y7NK62MV"
  }
}

```

Amazon KMS access control glossary

The following topic describes important terms and concepts in Amazon KMS access control.

Authentication

Authentication is the process of verifying your identity. To send a request to Amazon KMS, you must sign into Amazon using your Amazon credentials.

Authorization

Authorization provides the permission to send requests to create, manage, or use Amazon KMS resources. For example, you must be authorized to use a KMS key in a cryptographic operation.

To control access to your Amazon KMS resources, use [key policies](#), [IAM policies](#), and [grants](#). Every KMS key must have a key policy. If the key policy allows it, you can also use IAM policies and grants to give principals access to the KMS key. To refine your authorization, you can use [condition keys](#) that allow or deny access only when a request or resource meets the conditions you specify. You can also allow access to principals you trust in [other Amazon Web Services accounts](#).

Authenticating with identities

Authentication is how you sign in to Amazon using your identity credentials. You must be *authenticated* (signed in to Amazon) as the Amazon Web Services account root user, as an IAM user, or by assuming an IAM role.

If you access Amazon programmatically, Amazon provides a software development kit (SDK) and a command line interface (CLI) to cryptographically sign your requests by using your credentials. If you don't use Amazon tools, you must sign requests yourself. For more information about using the recommended method to sign requests yourself, see [Amazon Signature Version 4 for API requests](#) in the *IAM User Guide*.

Regardless of the authentication method that you use, you might be required to provide additional security information. For example, Amazon recommends that you use multi-factor authentication (MFA) to increase the security of your account. To learn more, see [Amazon Multi-factor authentication in IAM](#) in the *IAM User Guide*.

Amazon Web Services account root user

When you create an Amazon Web Services account, you begin with one sign-in identity that has complete access to all Amazon Web Services services and resources in the account. This identity is called the Amazon Web Services account *root user* and is accessed by signing in with the email address and password that you used to create the account. We strongly recommend that you don't

use the root user for your everyday tasks. Safeguard your root user credentials and use them to perform the tasks that only the root user can perform. For the complete list of tasks that require you to sign in as the root user, see [Tasks that require root user credentials](#) in the *IAM User Guide*.

Federated identity

As a best practice, require human users, including users that require administrator access, to use federation with an identity provider to access Amazon Web Services services by using temporary credentials.

A *federated identity* is a user from your enterprise user directory, a web identity provider, the Amazon Directory Service, or any user that accesses Amazon Web Services services by using credentials provided through an identity source. When federated identities access Amazon Web Services accounts, they assume roles, and the roles provide temporary credentials.

IAM users and groups

An [IAM user](#) is an identity within your Amazon Web Services account that has specific permissions for a single person or application. Where possible, we recommend relying on temporary credentials instead of creating IAM users who have long-term credentials such as passwords and access keys. However, if you have specific use cases that require long-term credentials with IAM users, we recommend that you rotate access keys. For more information, see [Rotate access keys regularly for use cases that require long-term credentials](#) in the *IAM User Guide*.

An [IAM group](#) is an identity that specifies a collection of IAM users. You can't sign in as a group. You can use groups to specify permissions for multiple users at a time. Groups make permissions easier to manage for large sets of users. For example, you could have a group named *IAMAdmins* and give that group permissions to administer IAM resources.

Users are different from roles. A user is uniquely associated with one person or application, but a role is intended to be assumable by anyone who needs it. Users have permanent long-term credentials, but roles provide temporary credentials. To learn more, see [Use cases for IAM users](#) in the *IAM User Guide*.

IAM roles

An [IAM role](#) is an identity within your Amazon Web Services account that has specific permissions. It is similar to an IAM user, but is not associated with a specific person. To temporarily assume an IAM role in the Amazon Web Services Management Console, you can [switch from a user to an IAM role \(console\)](#). You can assume a role by calling an Amazon CLI or Amazon API operation or by

using a custom URL. For more information about methods for using roles, see [Methods to assume a role](#) in the *IAM User Guide*.

IAM roles with temporary credentials are useful in the following situations:

- **Federated user access** – To assign permissions to a federated identity, you create a role and define permissions for the role. When a federated identity authenticates, the identity is associated with the role and is granted the permissions that are defined by the role. For information about roles for federation, see [Create a role for a third-party identity provider \(federation\)](#) in the *IAM User Guide*.
- **Temporary IAM user permissions** – An IAM user or role can assume an IAM role to temporarily take on different permissions for a specific task.
- **Cross-account access** – You can use an IAM role to allow someone (a trusted principal) in a different account to access resources in your account. Roles are the primary way to grant cross-account access. However, with some Amazon Web Services services, you can attach a policy directly to a resource (instead of using a role as a proxy). To learn the difference between roles and resource-based policies for cross-account access, see [Cross account resource access in IAM](#) in the *IAM User Guide*.
- **Cross-service access** – Some Amazon Web Services services use features in other Amazon Web Services services. For example, when you make a call in a service, it's common for that service to run applications in Amazon EC2 or store objects in Amazon S3. A service might do this using the calling principal's permissions, using a service role, or using a service-linked role.
 - **Forward access sessions (FAS)** – When you use an IAM user or role to perform actions in Amazon, you are considered a principal. When you use some services, you might perform an action that then initiates another action in a different service. FAS uses the permissions of the principal calling an Amazon Web Services service, combined with the requesting Amazon Web Services service to make requests to downstream services. FAS requests are only made when a service receives a request that requires interactions with other Amazon Web Services services or resources to complete. In this case, you must have permissions to perform both actions. For policy details when making FAS requests, see [Forward access sessions](#).
 - **Service role** – A service role is an [IAM role](#) that a service assumes to perform actions on your behalf. An IAM administrator can create, modify, and delete a service role from within IAM. For more information, see [Create a role to delegate permissions to an Amazon Web Services service](#) in the *IAM User Guide*.
 - **Service-linked role** – A service-linked role is a type of service role that is linked to an Amazon Web Services service. The service can assume the role to perform an action on your behalf.

Service-linked roles appear in your Amazon Web Services account and are owned by the service. An IAM administrator can view, but not edit the permissions for service-linked roles.

- **Applications running on Amazon EC2** – You can use an IAM role to manage temporary credentials for applications that are running on an EC2 instance and making Amazon CLI or Amazon API requests. This is preferable to storing access keys within the EC2 instance. To assign an Amazon role to an EC2 instance and make it available to all of its applications, you create an instance profile that is attached to the instance. An instance profile contains the role and enables programs that are running on the EC2 instance to get temporary credentials. For more information, see [Use an IAM role to grant permissions to applications running on Amazon EC2 instances](#) in the *IAM User Guide*.

Managing access using policies

You control access in Amazon by creating policies and attaching them to Amazon identities or resources. A policy is an object in Amazon that, when associated with an identity or resource, defines their permissions. Amazon evaluates these policies when a principal (user, root user, or role session) makes a request. Permissions in the policies determine whether the request is allowed or denied. Most policies are stored in Amazon as JSON documents. For more information about the structure and contents of JSON policy documents, see [Overview of JSON policies](#) in the *IAM User Guide*.

Administrators can use Amazon JSON policies to specify who has access to what. That is, which **principal** can perform **actions** on what **resources**, and under what **conditions**.

By default, users and roles have no permissions. To grant users permission to perform actions on the resources that they need, an IAM administrator can create IAM policies. The administrator can then add the IAM policies to roles, and users can assume the roles.

IAM policies define permissions for an action regardless of the method that you use to perform the operation. For example, suppose that you have a policy that allows the `iam:GetRole` action. A user with that policy can get role information from the Amazon Web Services Management Console, the Amazon CLI, or the Amazon API.

Identity-based policies

Identity-based policies are JSON permissions policy documents that you can attach to an identity, such as an IAM user, group of users, or role. These policies control what actions users and roles can

perform, on which resources, and under what conditions. To learn how to create an identity-based policy, see [Define custom IAM permissions with customer managed policies](#) in the *IAM User Guide*.

Identity-based policies can be further categorized as *inline policies* or *managed policies*. Inline policies are embedded directly into a single user, group, or role. Managed policies are standalone policies that you can attach to multiple users, groups, and roles in your Amazon Web Services account. Managed policies include Amazon managed policies and customer managed policies. To learn how to choose between a managed policy or an inline policy, see [Choose between managed policies and inline policies](#) in the *IAM User Guide*.

Resource-based policies

An Amazon KMS [key policy](#) is a resource-based policy that controls access to a KMS key. Every KMS key must have a key policy. You can use other authorization mechanism to allow access to the KMS key, but only if the key policy allows it. (You can use an IAM policy to *deny* access to a KMS key even if the key policy doesn't explicitly permit it.)

Resource-based policies are JSON policy documents that you attach to a resource, such as a KMS key, to control access to the specific resource. The resource-based policy defines the actions that a specified principal can perform on that resource and under what conditions. You don't specify the resource in a resource-based policy, but you must specify a principal, such as accounts, users, roles, federated users, or Amazon Web Services services. Resource-based policies are inline policies that are located in that service that manages the resource. You can't use Amazon managed policies from IAM, such as the [AWSKeyManagementServicePowerUser managed policy](#), in a resource-based policy.

Other policy types

Amazon supports additional, less-common policy types. These policy types can set the maximum permissions granted to you by the more common policy types.

- **Permissions boundaries** – A permissions boundary is an advanced feature in which you set the maximum permissions that an identity-based policy can grant to an IAM entity (IAM user or role). You can set a permissions boundary for an entity. The resulting permissions are the intersection of an entity's identity-based policies and its permissions boundaries. Resource-based policies that specify the user or role in the `Principal` field are not limited by the permissions boundary. An explicit deny in any of these policies overrides the allow. For more information about permissions boundaries, see [Permissions boundaries for IAM entities](#) in the *IAM User Guide*.

- **Service control policies (SCPs)** – SCPs are JSON policies that specify the maximum permissions for an organization or organizational unit (OU) in Amazon Organizations. Amazon Organizations is a service for grouping and centrally managing multiple Amazon Web Services accounts that your business owns. If you enable all features in an organization, then you can apply service control policies (SCPs) to any or all of your accounts. The SCP limits permissions for entities in member accounts, including each Amazon Web Services account root user. For more information about Organizations and SCPs, see [Service control policies](#) in the *Amazon Organizations User Guide*.
- **Resource control policies (RCPs)** – RCPs are JSON policies that you can use to set the maximum available permissions for resources in your accounts without updating the IAM policies attached to each resource that you own. The RCP limits permissions for resources in member accounts and can impact the effective permissions for identities, including the Amazon Web Services account root user, regardless of whether they belong to your organization. For more information about Organizations and RCPs, including a list of Amazon Web Services services that support RCPs, see [Resource control policies \(RCPs\)](#) in the *Amazon Organizations User Guide*.
- **Session policies** – Session policies are advanced policies that you pass as a parameter when you programmatically create a temporary session for a role or federated user. The resulting session's permissions are the intersection of the user or role's identity-based policies and the session policies. Permissions can also come from a resource-based policy. An explicit deny in any of these policies overrides the allow. For more information, see [Session policies](#) in the *IAM User Guide*.

Multiple policy types

When multiple types of policies apply to a request, the resulting permissions are more complicated to understand. To learn how Amazon determines whether to allow a request when multiple policy types are involved, see [Policy evaluation logic](#) in the *IAM User Guide*.

Amazon KMS resources

In Amazon KMS, the primary resource is an Amazon KMS key. Amazon KMS also supports an [alias](#), an independent resource that provides a friendly name for a KMS key. Some Amazon KMS operations allow you to use an alias to identify a KMS key.

Each instance of a KMS key or alias has a unique [Amazon Resource Name](#) (ARN) with a standard format. In Amazon KMS resources, the Amazon service name is kms.

- **Amazon KMS key**

ARN format:

*arn:Amazon partition name:Amazon service name:Amazon Web Services
Region:Amazon Web Services account ID:key/key ID*

Example ARN:

```
arn:aws:kms:us-west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab
```

- **Alias**

ARN format:

*arn:Amazon partition name:Amazon service name:Amazon Web Services
Region:Amazon Web Services account ID:alias/alias name*

Example ARN:

```
arn:aws:kms:us-west-2:111122223333:alias/example-alias
```

Amazon KMS provides a set of API operations to work with your Amazon KMS resources. For more information about identifying KMS keys in the Amazon Web Services Management Console and Amazon KMS API operations, see [Key identifiers \(KeyId\)](#). For a list of Amazon KMS operations, see the [Amazon Key Management Service API Reference](#).

Create a KMS key

You can create Amazon KMS keys in the Amazon Web Services Management Console, or by using the [CreateKey](#) operation or the [AWS::KMS::Key Amazon CloudFormation resource](#). During this process, you set the key policy for the KMS key, which you can change at any time. You also select the following values that define the type of KMS key that you create. You cannot change these properties after the KMS key is created.

KMS key type

Key type is a property that determines what type of cryptographic key is created. Amazon KMS offers three key types to protect data:

- Advanced Encryption Standard (AES) symmetric keys

256-bit keys that are used under the Galois Counter Mode (GCM) mode of AES to provide authenticated encryption/decryption of data under 4KB in size. This is the most common type of key and is used to protect other data encryption keys used in your applications and by Amazon Web Services services that encrypt your data on your behalf.

- RSA, elliptic curve, or SM2 (China Regions only) asymmetric keys

These keys are available in various sizes and support many algorithms. They can be used for encryption and decryption, sign and verify, or derive shared secrets operations depending on the algorithm choice.

- Symmetric keys for performing hash-based message authentication codes (HMAC) operations

These keys are 256-bit keys used for sign and verify operations.

KMS keys cannot be exported from the service in plaintext. They are generated by and can only be used within the hardware security modules (HSMs) used by the service. This is the foundational security property of Amazon KMS to ensure that keys are not compromised.

Key usage

Key usage is a property that determines the cryptographic operations the key supports. KMS keys can have a key usage of ENCRYPT_DECRYPT, SIGN_VERIFY, GENERATE_VERIFY_MAC, or KEY_AGREEMENT. Each KMS key can have only one key usage. Using a KMS key for more than one type of operation makes the product of both operations more vulnerable to attack.

Key spec

Key spec is a property that represents the cryptographic configuration of a key. The meaning of the key spec differs with the key type.

For KMS keys, the *key spec* determines whether the KMS key is symmetric or asymmetric. It also determines the type of its key material, and the algorithms it supports.

The default key spec, [SYMMETRIC_DEFAULT](#), represents a 256-bit symmetric encryption key. For a detailed description of all supported key specs, see [Key spec reference](#).

Key material origin

Key material origin is a KMS key property that identifies the source of the key material in the KMS key. You choose the key material origin when you create the KMS key, and you cannot change it. The source of the key material affects the security, durability, availability, latency, and throughput characteristics of the KMS key.

Each KMS key includes a reference to its key material in its metadata. The key material origin of symmetric encryption KMS keys can vary. You can use key material that Amazon KMS generates, key material that is generated in a [custom key store](#), or [import your own key material](#).

By default, each KMS key has unique key material. However, you can create a set of [multi-Region keys](#) with the same key material.

KMS keys can have one of the following key material origin values: `AWS_KMS`, `EXTERNAL` ([imported key material](#)), `AWS_CLOUDHSM` ([KMS key in a Amazon CloudHSM key store](#)), or `EXTERNAL_KEY_STORE` ([KMS key in an external key store](#)).

Topics

- [Permissions for creating KMS keys](#)
- [Choosing what type of KMS key to create](#)
- [Create a symmetric encryption KMS key](#)
- [Create an asymmetric KMS key](#)
- [Create an HMAC KMS key](#)
- [Create multi-Region primary keys](#)
- [Create multi-Region replica keys](#)

- [Create a KMS key with imported key material](#)
- [Create a KMS key in an Amazon CloudHSM key store](#)
- [Create a KMS key in external key stores](#)

Permissions for creating KMS keys

To create a KMS key in the console or by using the APIs, you must have the following permission in an IAM policy. Whenever possible, use [condition keys](#) to limit the permissions. For example, you can use the [kms:KeySpec](#) condition key in an IAM policy to allow principals to create only symmetric encryption keys.

For an example of an IAM policy for principals who create keys, see [Allow a user to create KMS keys](#).

Note

Be cautious when giving principals permission to manage tags and aliases. Changing a tag or alias can allow or deny permission to the customer managed key. For details, see [ABAC for Amazon KMS](#).

- [kms:CreateKey](#) is required.
- [kms:CreateAlias](#) is required to create a KMS key in the console where an alias is required for every new KMS key.
- [kms:TagResource](#) is required to add tags while creating the KMS key.
- [iam:CreateServiceLinkedRole](#) is required to create multi-Region primary keys. For details, see [Control access to multi-Region keys](#).

The [kms:PutKeyPolicy](#) permission is not required to create the KMS key. The `kms:CreateKey` permission includes permission to set the initial key policy. But you must add this permission to the key policy while creating the KMS key to ensure that you can control access to the KMS key. The alternative is using the [BypassLockoutSafetyCheck](#) parameter, which is not recommended.

KMS keys belong to the Amazon account in which they were created. The IAM user who creates a KMS key is not considered to be the key owner and they don't automatically have permission to use or manage the KMS key that they created. Like any other principal, the key creator needs

to get permission through a key policy, IAM policy, or grant. However, principals who have the `kms:CreateKey` permission can set the initial key policy and give themselves permission to use or manage the key.

Choosing what type of KMS key to create

The type of KMS key that you create depends largely on how you plan to *use* the KMS key, your security requirements, and your authorization requirements. The key type and key usage of a KMS key determine what cryptographic operations the key can perform. Each KMS key has only one key usage. Using a KMS key for more than one type of operation makes the product of all operations more vulnerable to attack.

To allow principals to create KMS keys only for a particular key usage, use the [kms:KeyUsage](#) condition key. You can also use the `kms:KeyUsage` condition key to allow principals to call API operations for a KMS key based on its key usage. For example, you can allow permission to disable a KMS key only if its key usage is `SIGN_VERIFY`.

Use the following guidance to determine which type of KMS key you need based on your use case.

Encrypt and decrypt data

Use a [symmetric KMS key](#) for most use cases that require encrypting and decrypting data. The symmetric encryption algorithm that Amazon KMS uses is fast, efficient, and assures the confidentiality and authenticity of data. It supports authenticated encryption with additional authenticated data (AAD), defined as an [encryption context](#). This type of KMS key requires both the sender and recipient of encrypted data to have valid Amazon credentials to call Amazon KMS.

If your use case requires encryption outside of Amazon by users who cannot call Amazon KMS, [asymmetric KMS keys](#) are a good choice. You can distribute the public key of the asymmetric KMS key to allow these users to encrypt data. And your applications that need to decrypt that data can use the private key of the asymmetric KMS key within Amazon KMS.

Sign messages and verify signatures

To sign messages and verify signatures, you must use an [asymmetric KMS key](#). You can use a KMS key with a [key spec](#) that represents an RSA key pair, an elliptic curve (ECC) key pair, or an SM2 key pair (China Regions only). The key spec you choose is determined by the signing algorithm that you want to use. The ECDSA signing algorithms that ECC key pairs support are

recommended over the RSA signing algorithms. However, you might need to use a particular key spec and signing algorithm to support users who verify signatures outside of Amazon.

Encrypt with asymmetric key pairs

To encrypt data with an asymmetric key pair, you must use an [asymmetric KMS key](#) with an [RSA key spec](#) or an [SM2 key spec](#) (China Regions only). To encrypt data in Amazon KMS with the public key of a KMS key pair, use the [Encrypt](#) operation. You can also [download the public key](#) and share it with the parties that need to encrypt data outside of Amazon KMS.

When you download the public key of an asymmetric KMS key, you can use it outside of Amazon KMS. But it is no longer subject to the security controls that protect the KMS key in Amazon KMS. For example, you cannot use Amazon KMS key policies or grants to control use of the public key. Nor can you control whether the key is used only for encryption and decryption using the encryption algorithms that Amazon KMS supports. For more details, see [Special Considerations for Downloading Public Keys](#).

To decrypt data that was encrypted with the public key outside of Amazon KMS, call the [Decrypt](#) operation. The Decrypt operation fails if the data was encrypted under a public key from a KMS key with a key usage of SIGN_VERIFY. It will also fail if it was encrypted by using an algorithm that Amazon KMS does not support for the key spec you selected. For more information on key specs and supported algorithms, see [Key spec reference](#).

To avoid these errors, anyone using a public key outside of Amazon KMS must store the key configuration. The Amazon KMS console and the [GetPublicKey](#) response provide the information that you must include when you share the public key.

Derive shared secrets

To derive shared secrets, use a KMS key with [NIST-recommended elliptic curve](#) or [SM2](#) (China Regions only) key material. Amazon KMS uses the [Elliptic Curve Cryptography Cofactor Diffie-Hellman Primitive](#) (ECDH) to establish a key agreement between two peers by deriving a shared secret from their elliptic curve public-private key pairs. You can use the raw shared secret that the [DeriveSharedSecret](#) operation returns to derive a symmetric key that can encrypt and decrypt data that is sent between two parties, or generate and verify HMACs. Amazon KMS recommends that you follow [NIST recommendations for key derivation](#) when using the raw shared secret to derive a symmetric key.

Generate and verify HMAC codes

To generate and verify hash-based message authentication codes, use an HMAC KMS key. When you create an HMAC key in Amazon KMS, Amazon KMS creates and protects your key material

and ensures that you use the correct MAC algorithms for your key. HMAC codes can also be used as pseudo-random numbers, and in certain scenarios for symmetric signing and tokenizing.

HMAC KMS keys are symmetric keys. When creating an HMAC KMS key in the Amazon KMS console, choose the `Symmetric` key type.

Use with Amazon services

To create a KMS key for use with an [Amazon service that is integrated with Amazon KMS](#), consult the documentation for the service. Amazon services that encrypt your data require a [symmetric encryption KMS key](#).

In addition to these considerations, cryptographic operations on KMS keys with different key specs have different prices and different request quotas. For information about Amazon KMS pricing, see [Amazon Key Management Service Pricing](#). For information about request quotas, see [Request quotas](#).

Create a symmetric encryption KMS key

This topic explains how to create the basic KMS key, a [symmetric encryption KMS key](#) for a single Region with key material from Amazon KMS. You can use this KMS key to protect your resources in an Amazon Web Services service.

You can create symmetric encryption KMS keys in the Amazon KMS console, by using the [CreateKey](#) API, or by using the [AWS::KMS::Key Amazon CloudFormation template](#).

The default key spec, `SYMMETRIC_DEFAULT`, is the key spec for symmetric encryption KMS keys. When you select the **Symmetric** key type and the **Encrypt and decrypt** key usage in the Amazon KMS console, it selects the `SYMMETRIC_DEFAULT` key spec. In the [CreateKey](#) operation, if you don't specify a `KeySpec` value, `SYMMETRIC_DEFAULT` is selected. If you don't have a reason to use a different key spec, `SYMMETRIC_DEFAULT` is a good choice.

For information about quotas that apply to KMS keys, see [Quotas](#).

Using the Amazon KMS console

You can use the Amazon Web Services Management Console to create Amazon KMS keys (KMS keys).

⚠ Important

Do not include confidential or sensitive information in the alias, description, or tags. These fields may appear in plain text in CloudTrail logs and other output.

1. Sign in to the Amazon Web Services Management Console and open the Amazon Key Management Service (Amazon KMS) console at <https://console.amazonaws.cn/kms>.
2. To change the Amazon Web Services Region, use the Region selector in the upper-right corner of the page.
3. In the navigation pane, choose **Customer managed keys**.
4. Choose **Create key**.
5. To create a symmetric encryption KMS key, for **Key type** choose **Symmetric**.
6. In **Key usage**, the **Encrypt and decrypt** option is selected for you.
7. Choose **Next**.
8. Type an alias for the KMS key. The alias name cannot begin with **aws/**. The **aws/** prefix is reserved by Amazon Web Services to represent Amazon managed keys in your account.

ℹ Note

Adding, deleting, or updating an alias can allow or deny permission to the KMS key. For details, see [ABAC for Amazon KMS](#) and [Use aliases to control access to KMS keys](#).

An alias is a display name that you can use to identify the KMS key. We recommend that you choose an alias that indicates the type of data you plan to protect or the application you plan to use with the KMS key.


Aliases are required when you create a KMS key in the Amazon Web Services Management Console. They are optional when you use the [CreateKey](#) operation.

9. (Optional) Type a description for the KMS key.

You can add a description now or update it any time unless the [key state](#) is Pending Deletion or Pending Replica Deletion. To add, change, or delete the description of an

existing customer managed key, edit the description on the details page for the KMS key in the Amazon Web Services Management Console or use the [UpdateKeyDescription](#) operation.


10. (Optional) Type a tag key and an optional tag value. To add more than one tag to the KMS key, choose **Add tag**.

 **Note**

Tagging or untagging a KMS key can allow or deny permission to the KMS key. For details, see [ABAC for Amazon KMS](#) and [Use tags to control access to KMS keys](#).

When you add tags to your Amazon resources, Amazon generates a cost allocation report with usage and costs aggregated by tags. Tags can also be used to control access to a KMS key. For information about tagging KMS keys, see [Tags in Amazon KMS](#) and [ABAC for Amazon KMS](#).

11. Choose **Next**.
12. Select the IAM users and roles that can administer the KMS key.

 **Notes**

This key policy gives the Amazon Web Services account full control of this KMS key. It allows account administrators to use IAM policies to give other principals permission to manage the KMS key. For details, see [the section called "Default key policy"](#).

IAM best practices discourage the use of IAM users with long-term credentials.

Whenever possible, use IAM roles, which provide temporary credentials. For details, see [Security best practices in IAM](#) in the *IAM User Guide*.

The Amazon KMS console adds key administrators to the key policy under the statement identifier "Allow access for Key Administrators". Modifying this statement identifier might impact how the console displays updates that you make to the statement.

13. (Optional) To prevent the selected IAM users and roles from deleting this KMS key, in the **Key deletion** section at the bottom of the page, clear the **Allow key administrators to delete this key** check box.
14. Choose **Next**.
15. Select the IAM users and roles that can use the key in [cryptographic operations](#)

Notes

IAM best practices discourage the use of IAM users with long-term credentials. Whenever possible, use IAM roles, which provide temporary credentials. For details, see [Security best practices in IAM](#) in the *IAM User Guide*.

The Amazon KMS console adds key users to the key policy under the statement identifiers "Allow use of the key" and "Allow attachment of persistent resources". Modifying these statement identifiers might impact how the console displays updates that you make to the statement.

16. (Optional) You can allow other Amazon Web Services accounts to use this KMS key for cryptographic operations. To do so, in the **Other Amazon Web Services accounts** section at the bottom of the page, choose **Add another Amazon Web Services account** and enter the Amazon Web Services account identification number of an external account. To add multiple external accounts, repeat this step.

Note

To allow principals in the external accounts to use the KMS key, Administrators of the external account must create IAM policies that provide these permissions. For more information, see [Allowing users in other accounts to use a KMS key](#).

17. Choose **Next**.
18. Review the key policy statements for the key. To make changes to the key policy, select **Edit**.
19. Choose **Next**.
20. Review the key settings that you chose. You can still go back and change all settings.
21. Choose **Finish** to create the KMS key.

Using the Amazon KMS API

You can use the [CreateKey](#) operation to create Amazon KMS keys of all types. These examples use the [Amazon Command Line Interface \(Amazon CLI\)](#). For examples in multiple programming languages, see [Use CreateKey with an Amazon SDK or CLI](#).

⚠ Important

Do not include confidential or sensitive information in the `Description` or `Tags` fields. These fields may appear in plain text in CloudTrail logs and other output.

The following operation creates a symmetric encryption key in a single Region backed by key material generated by Amazon KMS. This operation has no required parameters. However, you might also want to use the `Policy` parameter to specify a key policy. You can change the key policy ([PutKeyPolicy](#)) and add optional elements, such as a [description](#) and [tags](#) at any time. You can also create [asymmetric keys](#), [multi-Region keys](#), keys with [imported key material](#), and keys in [custom key stores](#). To create data keys for client-side encryption, use the [GenerateDataKey](#) operation.

The `CreateKey` operation doesn't let you specify an alias, but you can use the [CreateAlias](#) operation to create an alias for your new KMS key.

The following is an example of a call to the `CreateKey` operation with no parameters. This command uses all of the default values. It creates a symmetric encryption KMS key with key material generated by Amazon KMS.

```
$ aws kms create-key
{
  "KeyMetadata": {
    "Origin": "AWS_KMS",
    "KeyId": "1234abcd-12ab-34cd-56ef-1234567890ab",
    "Description": "",
    "KeyManager": "CUSTOMER",
    "Enabled": true,
    "KeySpec": "SYMMETRIC_DEFAULT",
    "CustomerMasterKeySpec": "SYMMETRIC_DEFAULT",
    "KeyUsage": "ENCRYPT_DECRYPT",
    "KeyState": "Enabled",
    "CreationDate": 1502910355.475,
    "Arn": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab",
    "AWSAccountId": "111122223333",
    "MultiRegion": false
    "EncryptionAlgorithms": [
      "SYMMETRIC_DEFAULT"
    ],
  },
}
```

```
}  
}
```

If you do not specify a key policy for your new KMS key, the [default key policy](#) that `CreateKey` applies differs from the default key policy that the console applies when you use it to create a new KMS key.

For example, this call to the [GetKeyPolicy](#) operation returns the key policy that `CreateKey` applies. It gives the Amazon Web Services account access to the KMS key and allows it to create Amazon Identity and Access Management (IAM) policies for the KMS key. For detailed information about IAM policies and key policies for KMS keys, see [KMS key access and permissions](#)

```
$ aws kms get-key-policy --key-id 1234abcd-12ab-34cd-56ef-1234567890ab --policy-name  
default --output text  
{  
  "Version" : "2012-10-17",  
  "Id" : "key-default-1",  
  "Statement" : [ {  
    "Sid" : "Enable IAM User Permissions",  
    "Effect" : "Allow",  
    "Principal" : {  
      "AWS" : "arn:aws:iam::111122223333:root"  
    },  
    "Action" : "kms:*",  
    "Resource" : "*"   
  } ]  
}
```

Create an asymmetric KMS key

You can create [asymmetric KMS keys](#) in the Amazon KMS console, by using the [CreateKey](#) API, or by using the [AWS::KMS::Key Amazon CloudFormation template](#). An asymmetric KMS key represents a public and private key pair that can be used for encryption, signing, or deriving shared secrets. The private key remains within Amazon KMS. To download the public key for use outside of Amazon KMS, see [Download public key](#).

When you create an asymmetric KMS key, you must select a key spec. Often the key spec that you select is determined by regulatory, security, or business requirements. It might also be influenced by the size of messages that you need to encrypt or sign. In general, longer encryption keys are

more resistant to brute-force attacks. For a detailed description of all supported key specs, see [Key spec reference](#).

Amazon services that integrate with Amazon KMS do not support asymmetric KMS keys. If you want to create a KMS key that encrypts data that you store or manage in an Amazon service, [create a symmetric encryption KMS key](#).

For information about the permissions required to create KMS keys, see [Permissions for creating KMS keys](#).

Using the Amazon KMS console

You can use the Amazon Web Services Management Console to create asymmetric Amazon KMS keys (KMS keys). Each asymmetric KMS key represents a public and private key pair.

Important

Do not include confidential or sensitive information in the alias, description, or tags. These fields may appear in plain text in CloudTrail logs and other output.

1. Sign in to the Amazon Web Services Management Console and open the Amazon Key Management Service (Amazon KMS) console at <https://console.amazonaws.cn/kms>.
2. To change the Amazon Web Services Region, use the Region selector in the upper-right corner of the page.
3. In the navigation pane, choose **Customer managed keys**.
4. Choose **Create key**.
5. To create an asymmetric KMS key, in **Key type**, choose **Asymmetric**.
6. To create an asymmetric KMS key for public key encryption, in **Key usage**, choose **Encrypt and decrypt**.

To create an asymmetric KMS key for signing messages and verifying signatures, in **Key usage**, choose **Sign and verify**.

To create an asymmetric KMS key for deriving shared secrets, in **Key usage**, choose **Key agreement**.

For help choosing a key usage value, see [Choosing what type of KMS key to create](#).

7. Select a specification (**Key spec**) for your asymmetric KMS key.
8. Choose **Next**.
9. Type an [alias](#) for the KMS key. The alias name cannot begin with **aws/**. The **aws/** prefix is reserved by Amazon Web Services to represent Amazon managed keys in your account.

An *alias* is a friendly name that you can use to identify the KMS key in the console and in some Amazon KMS APIs. We recommend that you choose an alias that indicates the type of data you plan to protect or the application you plan to use with the KMS key.

Aliases are required when you create a KMS key in the Amazon Web Services Management Console. You cannot specify an alias when you use the [CreateKey](#) operation, but you can use the console or the [CreateAlias](#) operation to create an alias for an existing KMS key. For details, see [Aliases in Amazon KMS](#).

10. (Optional) Type a description for the KMS key.

Enter a description that explains the type of data you plan to protect or the application you plan to use with the KMS key.

You can add a description now or update it any time unless the [key state](#) is Pending Deletion or Pending Replica Deletion. To add, change, or delete the description of an existing customer managed key, edit the description on the details page for the KMS key in the Amazon Web Services Management Console or use the [UpdateKeyDescription](#) operation.

11. (Optional) Type a tag key and an optional tag value. To add more than one tag to the KMS key, choose **Add tag**.

When you add tags to your Amazon resources, Amazon generates a cost allocation report with usage and costs aggregated by tags. Tags can also be used to control access to a KMS key. For information about tagging KMS keys, see [Tags in Amazon KMS](#) and [ABAC for Amazon KMS](#).

12. Choose **Next**.
13. Select the IAM users and roles that can administer the KMS key.

Notes

This key policy gives the Amazon Web Services account full control of this KMS key. It allows account administrators to use IAM policies to give other principals permission to manage the KMS key. For details, see [the section called “Default key policy”](#).

IAM best practices discourage the use of IAM users with long-term credentials. Whenever possible, use IAM roles, which provide temporary credentials. For details, see [Security best practices in IAM](#) in the *IAM User Guide*.

The Amazon KMS console adds key administrators to the key policy under the statement identifier "Allow access for Key Administrators". Modifying this statement identifier might impact how the console displays updates that you make to the statement.

14. (Optional) To prevent the selected IAM users and roles from deleting this KMS key, in the **Key deletion** section at the bottom of the page, clear the **Allow key administrators to delete this key** check box.
15. Choose **Next**.
16. Select the IAM users and roles that can use the KMS key for [cryptographic operations](#).

Notes

IAM best practices discourage the use of IAM users with long-term credentials. Whenever possible, use IAM roles, which provide temporary credentials. For details, see [Security best practices in IAM](#) in the *IAM User Guide*.

The Amazon KMS console adds key users to the key policy under the statement identifiers "Allow use of the key" and "Allow attachment of persistent resources". Modifying these statement identifiers might impact how the console displays updates that you make to the statement.

17. (Optional) You can allow other Amazon Web Services accounts to use this KMS key for cryptographic operations. To do so, in the **Other Amazon Web Services accounts** section at the bottom of the page, choose **Add another Amazon Web Services account** and enter the Amazon Web Services account identification number of an external account. To add multiple external accounts, repeat this step.

Note

To allow principals in the external accounts to use the KMS key, administrators of the external account must create IAM policies that provide these permissions. For more information, see [Allowing users in other accounts to use a KMS key](#).

18. Choose **Next**.

19. Review the key policy statements for the key. To make changes to the key policy, select **Edit**.
20. Choose **Next**.
21. Review the key settings that you chose. You can still go back and change all settings.
22. Choose **Finish** to create the KMS key.

Using the Amazon KMS API

You can use the [CreateKey](#) operation to create an asymmetric Amazon KMS key. These examples use the [Amazon Command Line Interface \(Amazon CLI\)](#), but you can use any supported programming language.

When you create an asymmetric KMS key, you must specify the `KeySpec` parameter, which determines the type of keys you create. Also, you must specify a `KeyUsage` value of `ENCRYPT_DECRYPT`, `SIGN_VERIFY`, or `KEY_AGREEMENT`. You cannot change these properties after the KMS key is created.

The `CreateKey` operation doesn't let you specify an alias, but you can use the [CreateAlias](#) operation to create an alias for your new KMS key.

Important

Do not include confidential or sensitive information in the `Description` or `Tags` fields. These fields may appear in plain text in CloudTrail logs and other output.

Create an asymmetric KMS key pair for public encryption

The following example uses the `CreateKey` operation to create an asymmetric KMS key of 4096-bit RSA keys designed for public key encryption.

```
$ aws kms create-key --key-spec RSA_4096 --key-usage ENCRYPT_DECRYPT
{
  "KeyMetadata": {
    "KeyState": "Enabled",
    "KeyId": "1234abcd-12ab-34cd-56ef-1234567890ab",
    "KeyManager": "CUSTOMER",
    "Description": "",
    "Arn": "arn:aws:kms:us-west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab",
```

```

    "CreationDate": 1569973196.214,
    "MultiRegion": false,
    "KeySpec": "RSA_4096",
    "CustomerMasterKeySpec": "RSA_4096",
    "KeyUsage": "ENCRYPT_DECRYPT",
    "EncryptionAlgorithms": [
      "RSAES_OAEP_SHA_1",
      "RSAES_OAEP_SHA_256"
    ],
    "AWSAccountId": "111122223333",
    "Origin": "AWS_KMS",
    "Enabled": true
  }
}

```

Create an asymmetric KMS key pair for signing and verification

The following example command creates an asymmetric KMS key that represents a pair of ECC keys used for signing and verification. You cannot create an elliptic curve key pair for encryption and decryption.

```

$ aws kms create-key --key-spec ECC_NIST_P521 --key-usage SIGN_VERIFY
{
  "KeyMetadata": {
    "KeyState": "Enabled",
    "KeyId": "0987dcba-09fe-87dc-65ba-ab0987654321",
    "CreationDate": 1570824817.837,
    "Origin": "AWS_KMS",
    "SigningAlgorithms": [
      "ECDSA_SHA_512"
    ],
    "Arn": "arn:aws:kms:us-west-2:111122223333:key/0987dcba-09fe-87dc-65ba-ab0987654321",
    "AWSAccountId": "111122223333",
    "KeySpec": "ECC_NIST_P521",
    "CustomerMasterKeySpec": "ECC_NIST_P521",
    "KeyManager": "CUSTOMER",
    "Description": "",
    "Enabled": true,
    "MultiRegion": false,
    "KeyUsage": "SIGN_VERIFY"
  }
}

```


Create an asymmetric KMS key pair for deriving shared secrets

The following example command creates an asymmetric KMS key that represents a pair of ECDH keys used for deriving shared secrets. You cannot create an elliptic curve key pair for encryption and decryption.

```
$ aws kms create-key --key-spec ECC_NIST_P256 --key-usage KEY_AGREEMENT
{
  "KeyMetadata": {
    "AWSAccountId": "111122223333",
    "KeyId": "0987dcba-09fe-87dc-65ba-ab0987654321",
    "Arn": "arn:aws:kms:us-west-2:111122223333:key/0987dcba-09fe-87dc-65ba-
ab0987654321",
    "CreationDate": "2023-12-27T19:10:15.063000+00:00",
    "Enabled": true,
    "Description": "",
    "KeyUsage": "KEY_AGREEMENT",
    "KeyState": "Enabled",
    "Origin": "AWS_KMS",
    "KeyManager": "CUSTOMER",
    "CustomerMasterKeySpec": "ECC_NIST_P256",
    "KeySpec": "ECC_NIST_P256",
    "KeyAgreementAlgorithms": [
      "ECDH"
    ],
    "MultiRegion": false
  }
}
```

Create an HMAC KMS key

You can create HMAC KMS keys in the Amazon KMS console, by using the [CreateKey](#) API, or by using the [AWS::KMS::Key Amazon CloudFormation template](#).

When you create an HMAC KMS key, you must select a key spec. Amazon KMS supports multiple [key specs for HMAC KMS keys](#). The key spec that you select might be determined by regulatory, security, or business requirements. In general, longer keys are more resistant to brute-force attacks.

For information about the permissions required to create KMS keys, see [Permissions for creating KMS keys](#).

Using the Amazon KMS console

You can use the Amazon Web Services Management Console to create HMAC KMS keys. HMAC KMS keys are symmetric keys with a key usage of **Generate and verify MAC**. You can also create multi-Region HMAC keys.

1. Sign in to the Amazon Web Services Management Console and open the Amazon Key Management Service (Amazon KMS) console at <https://console.amazonaws.cn/kms>.
2. To change the Amazon Web Services Region, use the Region selector in the upper-right corner of the page.
3. In the navigation pane, choose **Customer managed keys**.
4. Choose **Create key**.
5. For **Key type**, choose **Symmetric**.

HMAC KMS keys are symmetric. You use the same key to generate and verify HMAC tags.

6. For **Key usage**, choose **Generate and verify MAC**.

Generate and verify MAC is the only valid key usage for HMAC KMS keys.

Note

Key usage is displayed for symmetric keys only when HMAC KMS keys are supported in your selected Region.

7. Select a specification (**Key spec**) for your HMAC KMS key.

The key spec that you select can be determined by regulatory, security, or business requirements. In general, longer keys are more secure.

8. To create a [multi-Region](#) *primary* HMAC key, in **Advanced options**, choose **Multi-Region key**. The [shared properties](#) that you define for this KMS key, such as its key type and key usage, will be shared with its replica keys.

You cannot use this procedure to create a replica key. To create a multi-Region *replica* HMAC key, follow the [instructions for creating a replica key](#).

9. Choose **Next**.
10. Enter an [alias](#) for the KMS key. The alias name cannot begin with **aws/**. The **aws/** prefix is reserved by Amazon Web Services to represent Amazon managed keys in your account.

We recommend that you use an alias that identifies the KMS key as an HMAC key, such as HMAC/test-key. This will make it easier for you to identify your HMAC keys in the Amazon KMS console where you can sort and filter keys by tags and aliases, but not by key spec or key usage.

Aliases are required when you create a KMS key in the Amazon Web Services Management Console. You cannot specify an alias when you use the [CreateKey](#) operation, but you can use the console or the [CreateAlias](#) operation to create an alias for an existing KMS key. For details, see [Aliases in Amazon KMS](#).

11. (Optional) Enter a description for the KMS key.

Enter a description that explains the type of data you plan to protect or the application you plan to use with the KMS key.

You can add a description now or update it any time unless the [key state](#) is Pending Deletion or Pending Replica Deletion. To add, change, or delete the description of an existing customer managed key, edit the description on the details page for the KMS key in the Amazon Web Services Management Console in the Amazon Web Services Management Console or use the [UpdateKeyDescription](#) operation.


12. (Optional) Enter a tag key and an optional tag value. To add more than one tag to the KMS key, choose **Add tag**.

Consider adding a tag that identifies the key as an HMAC key, such as Type=HMAC. This will make it easier for you to identify your HMAC keys in the Amazon KMS console where you can sort and filter keys by tags and aliases, but not by key spec or key usage.

When you add tags to your Amazon resources, Amazon generates a cost allocation report with usage and costs aggregated by tags. Tags can also be used to control access to a KMS key. For information about tagging KMS keys, see [Tags in Amazon KMS](#) and [ABAC for Amazon KMS](#).

13. Choose **Next**.

14. Select the IAM users and roles that can administer the KMS key.

 **Notes**

This key policy gives the Amazon Web Services account full control of this KMS key. It allows account administrators to use IAM policies to give other principals permission to manage the KMS key. For details, see [the section called "Default key policy"](#).

IAM best practices discourage the use of IAM users with long-term credentials. Whenever possible, use IAM roles, which provide temporary credentials. For details, see [Security best practices in IAM](#) in the *IAM User Guide*.

The Amazon KMS console adds key administrators to the key policy under the statement identifier "Allow access for Key Administrators". Modifying this statement identifier might impact how the console displays updates that you make to the statement.

15. (Optional) To prevent the selected IAM users and roles from deleting this KMS key, in the **Key deletion** section at the bottom of the page, clear the **Allow key administrators to delete this key** check box.
16. Choose **Next**.
17. Select the IAM users and roles that can use the KMS key for [cryptographic operations](#).

Notes

IAM best practices discourage the use of IAM users with long-term credentials. Whenever possible, use IAM roles, which provide temporary credentials. For details, see [Security best practices in IAM](#) in the *IAM User Guide*.

The Amazon KMS console adds key users to the key policy under the statement identifiers "Allow use of the key" and "Allow attachment of persistent resources". Modifying these statement identifiers might impact how the console displays updates that you make to the statement.

18. (Optional) You can allow other Amazon Web Services accounts to use this KMS key for cryptographic operations. To do so, in the **Other Amazon Web Services accounts** section at the bottom of the page, choose **Add another Amazon Web Services account** and enter the Amazon Web Services account identification number of an external account. To add multiple external accounts, repeat this step.

Note

To allow principals in the external accounts to use the KMS key, Administrators of the external account must create IAM policies that provide these permissions. For more information, see [Allowing users in other accounts to use a KMS key](#).

19. Choose **Next**.

20. Review the key policy statements for the key. To make changes to the key policy, select **Edit**.
21. Choose **Next**.
22. Review the key settings that you chose. You can still go back and change all settings.
23. Choose **Finish** to create the HMAC KMS key.

Using the Amazon KMS API

You can use the [CreateKey](#) operation to create an HMAC KMS key. These examples use the [Amazon Command Line Interface \(Amazon CLI\)](#), but you can use any supported programming language.

When you create an HMAC KMS key, you must specify the `KeySpec` parameter, which determines the type of the KMS key. Also, you must specify a `KeyUsage` value of `GENERATE_VERIFY_MAC`, even though it's the only valid key usage value for HMAC keys. To create a [multi-Region](#) HMAC KMS key, add the `MultiRegion` parameter with a value of `true`. You cannot change these properties after the KMS key is created.

The `CreateKey` operation doesn't let you specify an alias, but you can use the [CreateAlias](#) operation to create an alias for your new KMS key. We recommend that you use an alias that identifies the KMS key as an HMAC key, such as `HMAC/test-key`. This will make it easier for you to identify your HMAC keys in the Amazon KMS console where you can sort and filter keys by alias, but not by key spec or key usage.

If you try to create an HMAC KMS key in an Amazon Web Services Region in which HMAC keys are not supported, the `CreateKey` operation returns an `UnsupportedOperationException`.

The following example uses the `CreateKey` operation to create a 512-bit HMAC KMS key.

```
$ aws kms create-key --key-spec HMAC_512 --key-usage GENERATE_VERIFY_MAC
{
  "KeyMetadata": {
    "KeyState": "Enabled",
    "KeyId": "1234abcd-12ab-34cd-56ef-1234567890ab",
    "KeyManager": "CUSTOMER",
    "Description": "",
    "Arn": "arn:aws:kms:us-west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab",
    "CreationDate": 1669973196.214,
    "MultiRegion": false,
    "KeySpec": "HMAC_512",
```

```
    "CustomerMasterKeySpec": "HMAC_512",
    "KeyUsage": "GENERATE_VERIFY_MAC",
    "MacAlgorithms": [
      "HMAC_SHA_512"
    ],
    "AWSAccountId": "111122223333",
    "Origin": "AWS_KMS",
    "Enabled": true
  }
}
```

Create multi-Region primary keys

You can create a [multi-Region primary key](#) in the Amazon KMS console or by using the Amazon KMS API. You can create the primary key in any Amazon Web Services Region where Amazon KMS supports multi-Region keys.

To create a multi-Region primary key, the principal needs the [same permissions](#) that they need to create any KMS key, including the [kms:CreateKey](#) permission in an IAM policy. The principal also needs the [iam:CreateServiceLinkedRole](#) permission. You can use the [kms:MultiRegionKeyType](#) condition key to allow or deny permission to create multi-Region primary keys.

Note

When creating your multi-Region primary key, carefully consider the IAM users and roles that you select to administer and use the key. IAM policies can give other IAM users and roles permission to manage the KMS key.

IAM best practices discourage the use of IAM users with long-term credentials. Whenever possible, use IAM roles, which provide temporary credentials. For details, see [Security best practices in IAM](#) in the *IAM User Guide*.

Using the Amazon KMS console

To create a multi-Region primary key in the Amazon KMS console, use the same process that you would use to create any KMS key.. You select a multi-Region key in **Advanced options**. For complete instructions, see [Create a KMS key](#).

⚠ Important

Do not include confidential or sensitive information in the alias, description, or tags. These fields may appear in plain text in CloudTrail logs and other output.

1. Sign in to the Amazon Web Services Management Console and open the Amazon Key Management Service (Amazon KMS) console at <https://console.amazonaws.cn/kms>.
2. To change the Amazon Web Services Region, use the Region selector in the upper-right corner of the page.
3. In the navigation pane, choose **Customer managed keys**.
4. Choose **Create key**.
5. Select a [symmetric or asymmetric](#) key type. Symmetric keys are the default.

You can create multi-Region symmetric and asymmetric keys, including multi-Region HMAC KMS keys, which are symmetric.

6. Select your key usage. **Encrypt and decrypt** is the default.

For help, see [Create a KMS key](#), the section called “[Create an asymmetric KMS key](#)”, or [the section called “Create an HMAC KMS key”](#).

7. Expand **Advanced options**.
8. Under **Key material origin**, to have Amazon KMS generate the key material that your primary and replica keys will share, choose **KMS**. If you are [importing key material](#) into the primary and replica keys, choose **External (Import key material)**.
9. Under **Regionality**, choose **Multi-Region key**.

You can't change this setting after you create the KMS key.

10. Type an [alias](#) for the primary key.

Aliases are not a shared property of multi-Region keys. You can give your multi-Region primary key and its replicas the same alias or different aliases. Amazon KMS does not synchronize the aliases of multi-Region keys.

Note

Adding, deleting, or updating an alias can allow or deny permission to the KMS key. For details, see [ABAC for Amazon KMS](#) and [Use aliases to control access to KMS keys](#).

11. (Optional) Type a description of the primary key.

Descriptions are not a shared property of multi-Region keys. You can give your multi-Region primary key and its replicas the same description or different descriptions. Amazon KMS does not synchronize the key descriptions of multi-Region keys.

12. (Optional) Type a tag key and an optional tag value. To assign more than one tag to the primary key, choose **Add tag.**

Tags are not a shared property of multi-Region keys. You can give your multi-Region primary key and its replicas the same tags or different tags. Amazon KMS does not synchronize the tags of multi-Region keys. You can change the tags on KMS keys at any time.

Note

Tagging or untagging a KMS key can allow or deny permission to the KMS key. For details, see [ABAC for Amazon KMS](#) and [Use tags to control access to KMS keys](#).

13. Select the IAM users and roles that can administer the primary key.**Notes**

- This step starts the process of creating a [key policy](#) for the primary key. Key policies are not a shared property of multi-Region keys. You can give your multi-Region primary key and its replicas the same key policy or different key policies. Amazon KMS does not synchronize the key policies of multi-Region keys. You can change the key policy of a KMS key at any time.
- When creating a multi-Region primary key, consider using the [default key policy](#) generated by the console. If you modify this policy, the console won't provide steps to select key administrators and users when creating replica keys, nor will it add the corresponding policy statements. As a result, you'll need to add these manually.

- The Amazon KMS console adds key administrators to the key policy under the statement identifier "Allow access for Key Administrators". Modifying this statement identifier might impact how the console displays updates that you make to the statement.

14. (Optional) To prevent the selected IAM users and roles from deleting this KMS key, in the **Key deletion** section at the bottom of the page, clear the **Allow key administrators to delete this key** check box.
15. Choose **Next**.
16. Select the IAM users and roles that can use the KMS key for [cryptographic operations](#).

Notes

The Amazon KMS console adds key users to the key policy under the statement identifiers "Allow use of the key" and "Allow attachment of persistent resources". Modifying these statement identifiers might impact how the console displays updates that you make to the statement.

17. (Optional) You can allow other Amazon Web Services accounts to use this KMS key for cryptographic operations. To do so, in the **Other Amazon Web Services accounts** section at the bottom of the page, choose **Add another Amazon Web Services account** and enter the Amazon Web Services account identification number of an external account. To add multiple external accounts, repeat this step.

Note

To allow principals in the external accounts to use the KMS key, Administrators of the external account must create IAM policies that provide these permissions. For more information, see [Allowing users in other accounts to use a KMS key](#).

18. Choose **Next**.
19. Review the key policy statements for the key. To make changes to the key policy, select **Edit**.
20. Choose **Next**.
21. Review the key settings that you chose. You can still go back and change all settings.
22. Choose **Finish** to create the multi-Region primary key.

Using the Amazon KMS API

To create a multi-Region primary key, use the [CreateKey](#) operation. Use the `MultiRegion` parameter with a value of `True`.

For example, the following command creates a multi-Region primary key in the caller's Amazon Web Services Region (`us-east-1`). It accepts default values for all other properties, including the key policy. The default values for multi-Region primary keys are the same as the default values for all other KMS keys, including the [default key policy](#). This procedure creates a symmetric encryption key, the default KMS key.

The response includes the `MultiRegion` element and the `MultiRegionConfiguration` element with typical sub-elements and values for a multi-Region primary key with no replica keys. The [key ID](#) of a multi-Region key always begins with `mrk-`.

Important

Do not include confidential or sensitive information in the `Description` or `Tags` fields. These fields may appear in plain text in CloudTrail logs and other output.

```
$ aws kms create-key --multi-region
{
  "KeyMetadata": {
    "Origin": "AWS_KMS",
    "KeyId": "mrk-1234abcd12ab34cd56ef1234567890ab",
    "Description": "",
    "KeyManager": "CUSTOMER",
    "Enabled": true,
    "KeySpec": "SYMMETRIC_DEFAULT",
    "CustomerMasterKeySpec": "SYMMETRIC_DEFAULT",
    "KeyUsage": "ENCRYPT_DECRYPT",
    "KeyState": "Enabled",
    "CreationDate": 1606329032.475,
    "Arn": "arn:aws:kms:us-east-1:111122223333:key/
mrk-1234abcd12ab34cd56ef1234567890ab",
    "AWSAccountId": "111122223333",
    "EncryptionAlgorithms": [
      "SYMMETRIC_DEFAULT"
    ],
    "MultiRegion": true,
```

```
    "MultiRegionConfiguration": {
      "MultiRegionKeyType": "PRIMARY",
      "PrimaryKey": {
        "Arn": "arn:aws:kms:us-east-1:111122223333:key/
mrk-1234abcd12ab34cd56ef1234567890ab",
        "Region": "us-east-1"
      },
      "ReplicaKeys": [ ]
    }
  }
}
```

Create multi-Region replica keys

You can create a [multi-Region replica key](#) in the Amazon KMS console, by using the [ReplicateKey](#) operation, or by using a [AWS::KMS::ReplicaKey Amazon CloudFormation template](#). You cannot use the [CreateKey](#) operation to create a replica key.

You can use these procedures to replicate any multi-Region primary key, including a [symmetric encryption KMS key](#), an [asymmetric KMS key](#), or an [HMAC KMS key](#).

When this operation completes, the new replica key has a transient [key state](#) of `Creating`. This key state changes to `Enabled` (or `PendingImport` if you create a multi-Region key with [imported key material](#)) after a few seconds when the process of creating the new replica key is complete. While the key state is `Creating`, you can manage key, but you cannot yet use it in cryptographic operations. If you are creating and using the replica key programmatically, retry on `KMSInvalidStateException` or call [DescribeKey](#) to check its `KeyState` value before using it.

If you mistakenly delete a replica key, you can use this procedure to recreate it. If you replicate the same primary key in the same Region, the new replica key you create will have the same [shared properties](#) as the original replica key.

Important

Do not include confidential or sensitive information in the alias, description, or tags. These fields may appear in plain text in CloudTrail logs and other output.

To use a Amazon CloudFormation template to create a replica key, see [AWS::KMS::ReplicaKey](#) in the *Amazon CloudFormation User Guide*.

Step 1: Choose replica Regions

You typically choose to replicate a multi-Region key into an Amazon Web Services Region based on your business model and regulatory requirements. For example, you might replicate a key into Regions where you keep your resources. Or, to comply with a disaster recovery requirement, you might replicate a key into geographically distant Regions.

The following are the Amazon KMS requirements for replica Regions. If the Region that you choose doesn't comply with these requirements, attempts to replicate a key fail.

- **One related multi-Region key per Region** — You can't create a replica key in the same Region as its primary key, or in the same Region as another replica of the primary key.

If you try to replicate a primary key in a Region that already has a replica of that primary key, the attempt fails. If the current replica key in the Region is in the [PendingDeletion key state](#), you can [cancel the replica key deletion](#) or wait until the replica key is deleted.

- **Multiple unrelated multi-Region keys in the same Region** — You can have multiple unrelated multi-Region keys in the same Region. For example, you can have two multi-Region primary keys in the us-east-1 Region. Each of the primary keys can have a replica key in us-west-2 Region.
- **Regions in the same partition** — The replica key Region must be in the same [Amazon partition](#) as the primary key Region.
- **Region must be enabled** — If a Region is [disabled by default](#), you cannot create any resources in that Region until it is enabled for your Amazon Web Services account.

Step 2: Create replica keys

Note

When creating replica keys, carefully consider the IAM users and roles that you select to administer and use the replica key. IAM policies can give other IAM users and roles permission to manage the KMS key.

IAM best practices discourage the use of IAM users with long-term credentials. Whenever possible, use IAM roles, which provide temporary credentials. For details, see [Security best practices in IAM](#) in the *IAM User Guide*.

Using the Amazon KMS console

In the Amazon KMS console, you can create one or many replicas of a multi-Region primary key in the same operation.

This procedure is similar to creating a standard single-Region KMS key in the console. However, because a replica key is based on the primary key, you do not select values for [shared properties](#), such as the key spec (symmetric or asymmetric), key usage, or key origin.

You do specify properties that are not shared, including an alias, tags, a description, and a key policy. As a convenience, the console displays the current property values of the primary key, but you can change them. Even if you keep the primary key values, Amazon KMS does not keep these values synchronized.

Important

Do not include confidential or sensitive information in the alias, description, or tags. These fields may appear in plain text in CloudTrail logs and other output.

1. Sign in to the Amazon Web Services Management Console and open the Amazon Key Management Service (Amazon KMS) console at <https://console.amazonaws.cn/kms>.
2. To change the Amazon Web Services Region, use the Region selector in the upper-right corner of the page.
3. In the navigation pane, choose **Customer managed keys**.
4. Select the key ID or alias of a [multi-Region primary key](#). This opens the key details page for the KMS key.

To identify a multi-Region primary key, use the tool icon in the upper right corner to add the **Regionality** column to the table.

5. Choose the **Regionality** tab.
6. In the **Related multi-Region keys** section, choose **Create new replica keys**.

The **Related multi-Region keys** section displays the Region of the primary key and its replica keys. You can use this display to help you choose the Region for your new replica key.

7. Choose one or more Amazon Web Services Regions. This procedure creates a replica key in each of the Regions you select.

The menu includes only Regions in the same Amazon partition as the primary key. Regions that already have a related multi-Region key are displayed, but not selectable. You might not have permission to replicate a key into all of the Regions on the menu.

When you are finished choosing Regions, close the menu. The Regions you chose are displayed. To cancel replication into a Region, choose the **X** beside the Region name.

8. Type an [alias](#) for the replica key.

The console displays one of the current aliases of the primary key, but you can change it. You can give your multi-Region primary key and its replicas the same alias or different aliases. Aliases are not a [shared property](#) of multi-Region keys. Amazon KMS does not synchronize the aliases of multi-Region keys.

Adding, deleting, or updating an alias can allow or deny permission to the KMS key. For details, see [ABAC for Amazon KMS](#) and [Use aliases to control access to KMS keys](#).

9. (Optional) Type a description of the replica key.

The console displays the current description of the primary key, but you can change it. Descriptions are not a shared property of multi-Region keys. You can give your multi-Region primary key and its replicas the same description or different descriptions. Amazon KMS does not synchronize the key descriptions of multi-Region keys.

10. (Optional) Type a tag key and an optional tag value. To assign more than one tag to the replica key, choose **Add tag**.

The console displays the tags currently attached to the primary key, but you can change them. Tags are not a shared property of multi-Region keys. You can give your multi-Region primary key and its replicas the same tags or different tags. Amazon KMS does not synchronize the tags of multi-Region keys.

Tagging or untagging a KMS key can allow or deny permission to the KMS key. For details, see [ABAC for Amazon KMS](#) and [Use tags to control access to KMS keys](#).

11. Select the IAM users and roles that can administer the replica key.


Notes

- If you modified the default key policy when creating your multi-Region primary key, the console won't prompt you to select key administrators or key users (steps 11-15)

during replica key creation. In this case, you'll need to manually add the necessary permissions for key administrators and users to the key policy by selecting **Edit** in the **Edit key policy** step (Step 17).

- This step begins the process of creating a [key policy](#) for the replica key. The console displays the current key policy of the primary key, but you can change it. Key policies are not a shared property of multi-Region keys. You can give your multi-Region primary key and its replicas the same key policy or different key policies. Amazon KMS does not synchronize key policies. You can change the key policy of any KMS key at any time.
- The Amazon KMS console adds key administrators to the key policy under the statement identifier "Allow access for Key Administrators". Modifying this statement identifier might impact how the console displays updates that you make to the statement.

12. (Optional) To prevent the selected IAM users and roles from deleting this KMS key, in the **Key deletion** section at the bottom of the page, clear the **Allow key administrators to delete this key** check box.
13. Choose **Next**.
14. Select the IAM users and roles that can use the KMS key for [cryptographic operations](#).

 **Note**

The Amazon KMS console adds key users to the key policy under the statement identifiers "Allow use of the key" and "Allow attachment of persistent resources". Modifying these statement identifiers might impact how the console displays updates that you make to the statement.

15. (Optional) You can allow other Amazon Web Services accounts to use this KMS key for cryptographic operations. To do so, in the **Other Amazon Web Services accounts** section at the bottom of the page, choose **Add another Amazon Web Services account** and enter the Amazon Web Services account identification number of an external account. To add multiple external accounts, repeat this step.

Note

To allow principals in the external accounts to use the KMS key, Administrators of the external account must create IAM policies that provide these permissions. For more information, see [Allowing users in other accounts to use a KMS key](#).

16. Choose **Next**.
17. Review the key policy statements for the key. To make changes to the key policy, select **Edit**.
18. Choose **Next**.
19. Review the key settings that you chose. You can still go back and change all settings.
20. Choose **Finish** to create the multi-Region replica key.

Using the Amazon KMS API

To create a multi-Region replica key, use the [ReplicateKey](#) operation. You cannot use the [CreateKey](#) operation to create a replica key. This operation creates one replica key at a time. The Region that you specify must comply with the [Region requirements](#) for replica keys.

When you use the `ReplicateKey` operation, you don't specify values for any [shared properties](#) of multi-Region keys. Shared property values are copied from the primary key and kept synchronized. However, you can specify values for properties that are not shared. Otherwise, Amazon KMS applies the standard default values for KMS keys, not the values of the primary key.

Note

If you don't specify values for the `Description`, `KeyPolicy`, or `Tags` parameters, Amazon KMS creates the replica key with an empty string description, the [default key policy](#), and no tags.

Do not include confidential or sensitive information in the `Description` or `Tags` fields. These fields may appear in plain text in CloudTrail logs and other output.

For example, the following command creates a multi-Region replica key in the Asia Pacific (Sydney) Region (ap-southeast-2). This replica key is modeled on the primary key in the US East (N. Virginia) Region (us-east-1), which is identified by the value of the `KeyId` parameter. This example accepts default values for all other properties, including the key policy.

The response describes the new replica key. It includes fields for shared properties, such as the `KeyId`, `KeySpec`, `KeyUsage`, and key material origin (`Origin`). It also includes properties that are independent of the primary key, such as the `Description`, key policy (`ReplicaKeyPolicy`), and tags (`ReplicaTags`).

The response also includes the key ARN and region of the primary key and all of its replica keys, including the one that was just created in the `ap-southeast-2` Region. In this example, the `ReplicaKey` element shows that this primary key was already replicated in the Europe (Ireland) Region (`eu-west-1`).

```
$ aws kms replicate-key \
  --key-id arn:aws:kms:us-east-1:111122223333:key/
mrk-1234abcd12ab34cd56ef1234567890ab \
  --replica-region ap-southeast-2
{
  "ReplicaKeyMetadata": {
    "MultiRegion": true,
    "MultiRegionConfiguration": {
      "MultiRegionKeyType": "REPLICA",
      "PrimaryKey": {
        "Arn": "arn:aws:kms:us-east-1:111122223333:key/
mrk-1234abcd12ab34cd56ef1234567890ab",
        "Region": "us-east-1"
      },
      "ReplicaKeys": [
        {
          "Arn": "arn:aws:kms:ap-southeast-2:111122223333:key/
mrk-1234abcd12ab34cd56ef1234567890ab",
          "Region": "ap-southeast-2"
        },
        {
          "Arn": "arn:aws:kms:eu-west-1:111122223333:key/
mrk-1234abcd12ab34cd56ef1234567890ab",
          "Region": "eu-west-1"
        }
      ]
    },
    "AWSAccountId": "111122223333",
    "Arn": "arn:aws:kms:ap-southeast-2:111122223333:key/
mrk-1234abcd12ab34cd56ef1234567890ab",
    "CreationDate": 1607472987.918,
    "Description": ""
```

```
    "Enabled": true,
    "KeyId": "mrk-1234abcd12ab34cd56ef1234567890ab",
    "KeyManager": "CUSTOMER",
    "KeySpec": "SYMMETRIC_DEFAULT",
    "KeyState": "Enabled",
    "KeyUsage": "ENCRYPT_DECRYPT",
    "Origin": "AWS_KMS",
    "CustomerMasterKeySpec": "SYMMETRIC_DEFAULT",
    "EncryptionAlgorithms": [
      "SYMMETRIC_DEFAULT"
    ]
  },
  "ReplicaKeyPolicy": "{\n  \"Version\" : \"2012-10-17\",\n  \"Id\" : \"key-
default-1\",...
  \"ReplicaTags\": []
}
```

Create a KMS key with imported key material

Imported key material lets you protect your Amazon resources under cryptographic keys that you generate. The key material that you import is associated with a particular KMS key. You can reimport the same key material into the same KMS key, but you cannot import different key material into the KMS key and you cannot convert a KMS key designed for imported key material into a KMS key with Amazon KMS key material.

The following overview explains how to import your key material into Amazon KMS. For more details about each step in the process, see the corresponding topic.

1. [Create a KMS key with no key material](#) – The origin must be EXTERNAL. A key origin of EXTERNAL indicates that the key is designed for imported key material and prevents Amazon KMS from generating key material for the KMS key. In a later step you will import your own key material into this KMS key.

The key material that you import must be compatible with the key spec of the associated Amazon KMS key. For more information about compatibility, see [the section called “Requirements for imported key material”](#).

2. [Download the wrapping public key and import token](#) – After completing step 1, download a wrapping public key and an import token. These items protect your key material while it's imported to Amazon KMS.

In this step, you choose the type ("key spec") of the RSA wrapping key and the wrapping algorithm that you'll use to encrypt your data in transit to Amazon KMS. You can choose a different wrapping key spec and wrapping key algorithm each time you import or reimport the same key material.

3. [Encrypt the key material](#) – Use the wrapping public key that you downloaded in step 2 to encrypt the key material that you created on your own system.
4. [Import the key material](#) – Upload the encrypted key material that you created in step 3 and the import token that you downloaded in step 2.

At this stage, you can [set an optional expiration time](#). When imported key material expires, Amazon KMS deletes it, and the KMS key becomes unusable. To continue to use the KMS key, you must reimport the **same** key material.

When the import operation completes successfully, the key state of the KMS key changes from `PendingImport` to `Enabled`. You can now use the KMS key in cryptographic operations.

Amazon KMS records an entry in your Amazon CloudTrail log when you [create the KMS key](#), [download the wrapping public key and import token](#), and [import the key material](#). Amazon KMS also records an entry when you delete imported key material or when Amazon KMS [deletes expired key material](#).

Permissions for importing key material

To create and manage KMS keys with imported key material, the user needs permission for the operations in this process. You can provide the `kms:GetParametersForImport`, `kms:ImportKeyMaterial`, and `kms>DeleteImportedKeyMaterial` permissions in the key policy when you create the KMS key. In the Amazon KMS console, these permissions are added automatically for key administrators when you create a key with an **External** key material origin.

To create KMS keys with imported key material, the principal needs the following permissions.

- [kms:CreateKey](#) (IAM policy)
 - To limit this permission to KMS keys with imported key material, use the [kms:KeyOrigin](#) policy condition with a value of `EXTERNAL`.

```
{
  "Sid": "CreateKMSKeysWithoutKeyMaterial",
```

```

"Effect": "Allow",
"Resource": "*",
"Action": "kms:CreateKey",
"Condition": {
  "StringEquals": {
    "kms:KeyOrigin": "EXTERNAL"
  }
}
}
}

```

- [kms:GetParametersForImport](#) (Key policy or IAM policy)
 - To limit this permission to requests that use a particular wrapping algorithm and wrapping key spec, use the [kms:WrappingAlgorithm](#) and [kms:WrappingKeySpec](#) policy conditions.
- [kms:ImportKeyMaterial](#) (Key policy or IAM policy)
 - To allow or prohibit key material that expires and control the expiration date, use the [kms:ExpirationModel](#) and [kms:ValidTo](#) policy conditions.

To reimport imported key material, the principal needs the [kms:GetParametersForImport](#) and [kms:ImportKeyMaterial](#) permissions.

To delete imported key material, the principal needs [kms>DeleteImportedKeyMaterial](#) permission.

For example, to give the example `KMSAdminRole` permission to manage all aspects of a KMS key with imported key material, include a key policy statement like the following one in the key policy of the KMS key.

```

{
  "Sid": "Manage KMS keys with imported key material",
  "Effect": "Allow",
  "Resource": "*",
  "Principal": {
    "AWS": "arn:aws:iam::111122223333:role/KMSAdminRole"
  },
  "Action": [
    "kms:GetParametersForImport",
    "kms:ImportKeyMaterial",
    "kms>DeleteImportedKeyMaterial"
  ]
}

```

Requirements for imported key material

The key material that you import must be compatible with the [key spec](#) of the associated KMS key. For asymmetric key pairs, import only the private key of the pair. Amazon KMS derives the public key from the private key.

Amazon KMS supports the following key specs for KMS keys with imported key material.

KMS key key spec	Key material requirements
Symmetric encryption keys SYMMETRIC_DEFAULT	256-bits (32 bytes) of binary data In China Regions, it must be a 128-bits (16 bytes) of binary data.
HMAC keys HMAC_224 HMAC_256 HMAC_384 HMAC_512	HMAC key material must conform to RFC 2104 . The key length must match the length specified by the key spec.
RSA asymmetric private key RSA_2048 RSA_3072 RSA_4096	The RSA asymmetric private key that you import must be part of a key pair that conforms to RFC 3447 . Modulus: 2048 bits, 3072 bits or 4096 bits Number of primes: 2 (multi-prime RSA keys are not supported) Asymmetric key material must be BER-encoded or DER-encoded in Public-Key Cryptography Standards (PKCS) #8 format that complies with RFC 5208 .

KMS key key spec	Key material requirements
<p>Elliptic curve asymmetric private key</p> <p>ECC_NIST_P256 (secp256r1)</p> <p>ECC_NIST_P384 (secp384r1)</p> <p>ECC_NIST_P521 (secp521r1)</p> <p>ECC_SECG_P256K1 (secp256k1)</p>	<p>The ECC asymmetric private key that you import must be part of a key pair that conforms to RFC 5915.</p> <p>Curve: NIST P-256, NIST P-384, NIST P-521, or Secp256k1</p> <p>Parameters: Named curves only (ECC keys with explicit parameters are rejected)</p> <p>Public point coordinates: May be compressed, uncompressed, or projective</p> <p>Asymmetric key material must be BER-encoded or DER-encoded in Public-Key Cryptography Standards (PKCS) #8 format that complies with RFC 5208.</p>
<p>SM2 asymmetric private key (China Regions only)</p>	<p>The SM2 asymmetric private key that you import must be part of a key pair that conforms to GM/T 0003.</p> <p>Curve: SM2</p> <p>Parameters: Named curve only (SM2 keys with explicit parameters are rejected)</p> <p>Public point coordinates: May be compressed, uncompressed, or projective</p> <p>Asymmetric key material must be BER-encoded or DER-encoded in Public-Key Cryptography Standards (PKCS) #8 format that complies with RFC 5208.</p>

Step 1: Create an Amazon KMS key without key material

By default, Amazon KMS creates key material for you when you create a KMS key. To import your own key material instead, start by creating a KMS key with no key material. Then import the key material. To create a KMS key with no key material, use Amazon KMS console or the [CreateKey](#) operation.

To create a key with no key material, specify an [origin](#) of EXTERNAL. The origin property of a KMS key is immutable. Once you create it, you cannot convert a KMS key designed for imported key material into a KMS key with key material from Amazon KMS or any other source.

The [key state](#) of a KMS key with an EXTERNAL origin and no key material is PendingImport. A KMS key can remain in PendingImport state indefinitely. However, you cannot use a KMS key in PendingImport state in cryptographic operations. When you import key material, the key state of the KMS key changes to Enabled, and you can use it in cryptographic operations.

Amazon KMS records an event in your Amazon CloudTrail log when you [create the KMS key](#), [download the public key and import token](#), and [import the key material](#). Amazon KMS also records a CloudTrail event when you [delete imported key material](#) or when Amazon KMS [deletes expired key material](#).

Topics

- [Creating a KMS key with no key material \(console\)](#)
- [Creating a KMS key with no key material \(Amazon KMS API\)](#)

Creating a KMS key with no key material (console)

You only need to create a KMS key for the imported key material once. You can import and reimport the same key material into the existing KMS key as often as you need to, but you cannot import different key material into a KMS key. For details, see [Step 2: Download the wrapping public key and import token](#).

To find existing KMS keys with imported key material in your **Customer managed keys** table, use the gear icon in the upper right corner to show the **Origin** column in the list of KMS keys. Imported keys have an **Origin** value of **External (Import Key material)**.

To create a KMS key with imported key material, begin by following the [instructions for creating a KMS key of your preferred key type](#), with the following exception.

After choosing the key usage, do the following:

1. Expand **Advanced options**.
2. For **Key material origin**, choose **External (Import key material)**.
3. Choose the check box next to **I understand the security and durability implications of using an imported key** to indicate that you understand the implications of using imported key material. To read about these implications, see [Protecting imported key material](#).
4. Optional: To create a [multi-Region KMS key](#) with imported key material, under **Regionality** select **Multi-Region key**.
5. Return to the basic instructions. The remaining steps of the basic procedure are the same for all KMS keys of that type.

When you choose **Finish**, you have created a KMS key with no key material and a status ([key state](#)) of **Pending import**.

However, instead of returning to the **Customer managed keys** table, the console displays a page where you can download the public key and import token that you need to import your key material. You can continue with the download step now, or choose **Cancel** to stop at this point. You can return to this download step at any time.

Next: [Step 2: Download the wrapping public key and import token](#).

Creating a KMS key with no key material (Amazon KMS API)

To use the [Amazon KMS API](#) to create a symmetric encryption KMS key with no key material, send a [CreateKey](#) request with the `Origin` parameter set to `EXTERNAL`. The following example shows how to do this with the [Amazon Command Line Interface \(Amazon CLI\)](#).

```
$ aws kms create-key --origin EXTERNAL
```

When the command is successful, you see output similar to the following. The Amazon KMS key's `Origin` is `EXTERNAL` and its `KeyState` is `PendingImport`.

Tip

If the command does not succeed, you might see a `KMSInvalidStateException` or a `NotFoundException`. You can retry the request.


```
{
  "KeyMetadata": {
    "Origin": "EXTERNAL",
    "KeyId": "1234abcd-12ab-34cd-56ef-1234567890ab",
    "Description": "",
    "Enabled": false,
    "MultiRegion": false,
    "KeyUsage": "ENCRYPT_DECRYPT",
    "KeyState": "PendingImport",
    "CreationDate": 1568289600.0,
    "Arn": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab",
    "AWSAccountId": "111122223333",
    "KeyManager": "CUSTOMER",
    "KeySpec": "SYMMETRIC_DEFAULT",
    "CustomerMasterKeySpec": "SYMMETRIC_DEFAULT",
    "EncryptionAlgorithms": [
      "SYMMETRIC_DEFAULT"
    ]
  }
}
```

Copy the `KeyId` value from your command output to use in later steps, and then proceed to [Step 2: Download the wrapping public key and import token](#).

Note

This command creates a symmetric encryption KMS key with a `KeySpec` of `SYMMETRIC_DEFAULT` and `KeyUsage` of `ENCRYPT_DECRYPT`. You can use the optional parameters `--key-spec` and `--key-usage` to create an asymmetric or HMAC KMS key. For more information, see the [CreateKey](#) operation.

Step 2: Download the wrapping public key and import token

After you [create a Amazon KMS key with no key material](#), download a wrapping public key and an import token for that KMS key by using the Amazon KMS console or the [GetParametersForImport](#) API. The wrapping public key and import token are an indivisible set that must be used together.

You will use the wrapping public key to [encrypt your key material](#) for transport. Before downloading an RSA wrapping key pair, you select the length (key spec) of the RSA wrapping

key pair and the wrapping algorithm that you will use to encrypt your imported key material for transport in [step 3](#). Amazon KMS also supports the SM2 wrapping key spec (China Regions only).

Each wrapping public key and import token set is valid for 24 hours. If you don't use them to import key material within 24 hours of downloading them, you must download a new set. You can download new wrapping public key and import token sets at any time. This lets you change your RSA wrapping key length ("key spec") or replace a lost set.

You can also download a wrapping public key and import token set to [reimport the same key material](#) into a KMS key. You might do this to set or change the expiration time for the key material, or to restore expired or deleted key material. You must download and re-encrypt your key material every time you import it to Amazon KMS.

Use of the wrapping public key

The download includes a public key that is unique to your Amazon Web Services account, also called a *wrapping public key*.

Before you import key material, you encrypt the key material with the public wrapping key, and then upload the encrypted key material to Amazon KMS. When Amazon KMS receives your encrypted key material, it decrypts the key material with the corresponding private key, then reencrypts the key material under an AES symmetric key, all within an Amazon KMS hardware security module (HSM).

Use of the import token

The download includes an import token with metadata that ensures that your key material is imported correctly. When you upload your encrypted key material to Amazon KMS, you must upload the same import token that you downloaded in this step.

Select a wrapping public key spec

To protect your key material during import, you encrypt it using wrapping public key that you download from Amazon KMS, and a supported [wrapping algorithm](#). You select a key spec before you download your wrapping public key and import token. All wrapping key pairs are generated in Amazon KMS hardware security modules (HSMs). The private key never leaves the HSM in plain text.

RSA wrapping key specs

The *key spec* of the wrapping public key determines the length of the keys in the RSA key pair that protects your key material during its transport to Amazon KMS. In general, we recommend using the longest wrapping public key that is practical. We offer several wrapping public key specs to support a variety of HSMs and key managers.

Amazon KMS supports the following key specs for the RSA wrapping keys used to import key material of all types, except as noted.

- RSA_4096 (preferred)
- RSA_3072
- RSA_2048

Note

The following combination is NOT supported: ECC_NIST_P521 key material, the RSA_2048 public wrapping key spec, and an RSAES_OAEP_SHA_* wrapping algorithm.

You cannot directly wrap ECC_NIST_P521 key material with a RSA_2048 public wrapping key. Use a larger wrapping key or an RSA_AES_KEY_WRAP_SHA_* wrapping algorithm.

SM2 wrapping key spec (China Regions only)

Amazon KMS supports the following key spec for the SM2 wrapping keys used to import asymmetric key material.

- SM2

Select a wrapping algorithm

To protect your key material during import, you encrypt it using the downloaded wrapping public key and a supported wrapping algorithm.

Amazon KMS supports several standard RSA wrapping algorithms and a two-step hybrid wrapping algorithm. In general, we recommend using the most secure wrapping algorithm that is compatible with your imported key material and [wrapping key spec](#). Typically, you choose an algorithm that is supported by the hardware security module (HSM) or key management system that protects your key material.

The following table shows the wrapping algorithms that are supported for each type of key material and KMS key. The algorithms are listed in preference order.

Key material	Supported wrapping algorithm and spec
Symmetric encryption key 256-bit AES key 128-bit SM4 key (China Regions only)	Wrapping algorithms: RSAES_OAEP_SHA_256 RSAES_OAEP_SHA_1 Deprecated wrapping algorithms: RSAES_PKCS1_V1 <div data-bbox="878 751 1507 1066" style="border: 1px solid #add8e6; border-radius: 10px; padding: 10px;"> <p> Note As of October 10, 2023, Amazon KMS does not support the RSAES_PKCS1_V1_5 wrapping algorithm.</p> </div> Wrapping key specs: RSA_2048 RSA_3072 RSA_4096
Asymmetric RSA private key	Wrapping algorithms: RSA_AES_KEY_WRAP_SHA_256 RSA_AES_KEY_WRAP_SHA_1 SM2PKE (China Regions only) Wrapping key specs: RSA_2048

Key material	Supported wrapping algorithm and spec
<p data-bbox="110 449 732 485">Asymmetric elliptic curve (ECC) private key</p> <p data-bbox="110 562 737 737">You cannot use the RSAES_OAEP_SHA_* wrapping algorithms with the RSA_2048 wrapping key spec to wrap ECC_NIST_P521 key material.</p>	<p data-bbox="873 212 1029 247">RSA_3072</p> <p data-bbox="873 289 1029 325">RSA_4096</p> <p data-bbox="873 367 1247 403">SM2 (China Regions only)</p> <p data-bbox="824 449 1146 485">Wrapping algorithms:</p> <p data-bbox="873 527 1338 562">RSA_AES_KEY_WRAP_SHA_256</p> <p data-bbox="873 604 1295 640">RSA_AES_KEY_WRAP_SHA_1</p> <p data-bbox="873 682 1221 718">RSAES_OAEP_SHA_256</p> <p data-bbox="873 760 1179 795">RSAES_OAEP_SHA_1</p> <p data-bbox="873 842 1302 877">SM2PKE (China Regions only)</p> <p data-bbox="824 905 1123 940">Wrapping key specs:</p> <p data-bbox="873 982 1029 1018">RSA_2048</p> <p data-bbox="873 1060 1029 1096">RSA_3072</p> <p data-bbox="873 1138 1029 1173">RSA_4096</p> <p data-bbox="873 1220 1247 1255">SM2 (China Regions only)</p>

Key material	Supported wrapping algorithm and spec
Asymmetric SM2 private key (China Regions only)	Wrapping algorithms: <ul style="list-style-type: none"> RSAES_OAEP_SHA_256 RSAES_OAEP_SHA_1 SM2PKE (China Regions only) Wrapping key specs: <ul style="list-style-type: none"> RSA_2048 RSA_3072 RSA_4096 SM2 (China Regions only)
HMAC key	Wrapping algorithms: <ul style="list-style-type: none"> RSAES_OAEP_SHA_256 RSAES_OAEP_SHA_1 Wrapping key specs: <ul style="list-style-type: none"> RSA_2048 RSA_3072 RSA_4096

 **Note**

The RSA_AES_KEY_WRAP_SHA_256 and RSA_AES_KEY_WRAP_SHA_1 wrapping algorithms are not supported in China Regions.

- RSA_AES_KEY_WRAP_SHA_256 – A two-step hybrid wrapping algorithm that combines encrypting your key material with an AES symmetric key that you generate, and then

encrypting the AES symmetric key with the downloaded RSA public wrapping key and the RSAES_OAEP_SHA_256 wrapping algorithm.

An RSA_AES_KEY_WRAP_SHA_* wrapping algorithm is required for wrapping RSA private key material, except in China Regions, where you must use the SM2PKE wrapping algorithm.

- RSA_AES_KEY_WRAP_SHA_1 – A two-step hybrid wrapping algorithm that combines encrypting your key material with an AES symmetric key that you generate, and then encrypting the AES symmetric key with the downloaded RSA wrapping public key and the RSAES_OAEP_SHA_1 wrapping algorithm.

An RSA_AES_KEY_WRAP_SHA_* wrapping algorithm is required for wrapping RSA private key material, except in China Regions, where you must use the SM2PKE wrapping algorithm.

- RSAES_OAEP_SHA_256 – The RSA encryption algorithm with Optimal Asymmetric Encryption Padding (OAEP) with the SHA-256 hash function.
- RSAES_OAEP_SHA_1 – The RSA encryption algorithm with Optimal Asymmetric Encryption Padding (OAEP) with the SHA-1 hash function.
- RSAES_PKCS1_V1_5 (Deprecated; as of October 10, 2023, Amazon KMS does not support the RSAES_PKCS1_V1_5 wrapping algorithm) – The RSA encryption algorithm with the padding format defined in PKCS #1 Version 1.5.
- SM2PKE (China Regions only) – An elliptic curve based encryption algorithm defined by OSCCA in GM/T 0003.4-2012.

Topics

- [Downloading the wrapping public key and import token \(console\)](#)
- [Downloading the wrapping public key and import token \(Amazon KMS API\)](#)

Downloading the wrapping public key and import token (console)

You can use the Amazon KMS console to download the wrapping public key and import token.

1. If you just completed the steps to [create a KMS key with no key material](#) and you are on the **Download wrapping key and import token** page, skip to [Step 9](#).
2. Sign in to the Amazon Web Services Management Console and open the Amazon Key Management Service (Amazon KMS) console at <https://console.amazonaws.cn/kms>.

3. To change the Amazon Web Services Region, use the Region selector in the upper-right corner of the page.
4. In the navigation pane, choose **Customer managed keys**.

 **Tip**

You can import key material only into a KMS key with an **Origin** of **External (Import key material)**. This indicates that the KMS key was created with no key material. To add the **Origin** column to your table, in the upper-right corner of the page, choose the settings icon



Turn on **Origin**, and then choose **Confirm**.

5. Choose the alias or key ID of the KMS key that is pending import.
6. Choose the **Cryptographic configuration** tab and view its values. The tabs are below the **General configuration** section.

You can only import key material into KMS keys with an **Origin** of **External (Import Key material)**. For information about creating KMS keys with imported key material, see, [Importing key material for Amazon KMS keys](#).

7. Choose the **Key material** tab and then choose **Import key material**.

The **Key material** tab appears only for KMS keys that have an **Origin** value of **External (Import Key material)**.

8. For **Select wrapping key spec**, choose the configuration for your KMS key. After you create this key, you can't change the key spec.
9. For **Select wrapping algorithm**, choose the option that you will use to encrypt your key material. For more information about the options, see [Select a Wrapping Algorithm](#).
10. Choose **Download wrapping public key and import token**, and then save the file.

If you have a **Next** option, to continue the process now, choose **Next**. To continue later, choose **Cancel**.

11. Decompress the .zip file that you saved in the previous step (Import_Parameters_<key_id>_<timestamp>).

The folder contains the following files:

- A wrapping public key in a file named `WrappingPublicKey.bin`.
- An import token in a file named `ImportToken.bin`.
- A text file named `README.txt`. This file contains information about the wrapping public key, the wrapping algorithm to use to encrypt your key material, and the date and time when the wrapping public key and import token expire.

12. To continue the process, see [encrypt your key material](#).

Downloading the wrapping public key and import token (Amazon KMS API)

To download the public key and import token, use the [GetParametersForImport](#) API. Specify the KMS key that will be associated with the imported key material. This KMS key must have an [Origin](#) value of `EXTERNAL`.

This example specifies the `RSA_AES_KEY_WRAP_SHA_256` wrapping algorithm, the `RSA_3072` wrapping public key spec, and an example key ID. Replace these example values with valid values for your download. For the key ID, you can use a [key ID](#) or [key ARN](#), but you cannot use an [alias name](#) or [alias ARN](#) in this operation.

```
$ aws kms get-parameters-for-import \
  --key-id 1234abcd-12ab-34cd-56ef-1234567890ab \
  --wrapping-algorithm RSA_AES_KEY_WRAP_SHA_256 \
  --wrapping-key-spec RSA_3072
```

When the command is successful, you see output similar to the following:

```
{
  "ParametersValidTo": 1568290320.0,
  "PublicKey": "public key (base64 encoded)",
  "KeyId": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab",
  "ImportToken": "import token (base64 encoded)"
}
```

To prepare the data for the next step, base64 decode the public key and import token and save the decoded values in files.

To base64 decode the public key and import token:

1. Copy the base64 encoded public key (represented by *public key (base64 encoded)* in the example output), paste it into a new file, and then save the file. Give the file a descriptive name, such as `PublicKey.b64`.
2. Use [OpenSSL](#) to base64 decode the file's contents and save the decoded data to a new file. The following example decodes the data in the file that you saved in the previous step (`PublicKey.b64`) and saves the output to a new file named `WrappingPublicKey.bin`.

```
$ openssl enc -d -base64 -A -in PublicKey.b64 -out WrappingPublicKey.bin
```

3. Copy the base64 encoded import token (represented by *import token (base64 encoded)* in the example output), paste it into a new file, and then save the file. Give the file a descriptive name, for example `importtoken.b64`.
4. Use [OpenSSL](#) to base64 decode the file's contents and save the decoded data to a new file. The following example decodes the data in the file that you saved in the previous step (`ImportToken.b64`) and saves the output to a new file named `ImportToken.bin`.

```
$ openssl enc -d -base64 -A -in importtoken.b64 -out ImportToken.bin
```

Proceed to [Step 3: Encrypt the key material](#).

Step 3: Encrypt the key material

After you [download the public key and import token](#), encrypt your key material using the public key that you downloaded and the wrapping algorithm that you specified. If you need to replace the public key or import token, or change the wrapping algorithm, you must download a new public key and import token. For information about the public keys and wrapping algorithms that Amazon KMS supports, see [Select a wrapping public key spec](#) and [Select a wrapping algorithm](#).

The key material must be in binary format. For detailed information, see [Requirements for imported key material](#).

Note

For asymmetric key pairs, encrypt and import only the private key. Amazon KMS derives the public key from the private key.

The following combination is NOT supported: ECC_NIST_P521 key material, the RSA_2048 public wrapping key spec, and an RSAES_OAEP_SHA_* wrapping algorithm.

You cannot directly wrap ECC_NIST_P521 key material with a RSA_2048 public wrapping key. Use a larger wrapping key or an RSA_AES_KEY_WRAP_SHA_* wrapping algorithm. The RSA_AES_KEY_WRAP_SHA_256 and RSA_AES_KEY_WRAP_SHA_1 wrapping algorithms are not supported in China Regions.

Typically, you encrypt your key material when you export it from your hardware security module (HSM) or key management system. For information about how to export key material in binary format, see the documentation for your HSM or key management system. You can also refer to the following section that provides a proof of concept demonstration using OpenSSL.

When you encrypt your key material, use the same wrapping algorithm that you specified when you [downloaded the public key and import token](#). To find the wrapping algorithm that you specified, see the CloudTrail log event for the associated [GetParametersForImport](#) request.

Generate key material for testing

The following OpenSSL commands generate key material of each supported type for testing. These examples are provided only for testing and proof-of-concept demonstrations. For production systems, use a more secure method to generate your key material, such as a hardware security module or key management system.

To convert the private keys of asymmetric key pairs into DER-encoded format, pipe the key material generation command to the following `openssl pkcs8` command. The `topk8` parameter directs OpenSSL to take a private key as input and return a PKCS#8 formatted key. (The default behavior is the opposite.)

```
openssl pkcs8 -topk8 -outform der -nocrypt
```

The following commands generate test key material for each of the supported key types.

- Symmetric encryption key (32 bytes)

This command generates a 256-bit symmetric key (32-byte random string) and saves it in the `PlaintextKeyMaterial.bin` file. You do not need to encode this key material.

```
openssl rand -out PlaintextKeyMaterial.bin 32
```

In China Regions only, you must generate a 128-bit symmetric key (16-byte random string).

```
openssl rand -out PlaintextKeyMaterial.bin 16
```

- HMAC keys

This command generates a random byte string of the specified size. You do not need to encode this key material.

The length of your HMAC key must match the length defined by the key spec of the KMS key. For example, if the KMS key is HMAC_384, you must import a 384-bit (48-byte) key.

```
openssl rand -out HMAC_224_PlaintextKey.bin 28
openssl rand -out HMAC_256_PlaintextKey.bin 32
openssl rand -out HMAC_384_PlaintextKey.bin 48
openssl rand -out HMAC_512_PlaintextKey.bin 64
```

- RSA private keys

```
openssl genpkey -algorithm rsa -pkeyopt rsa_keygen_bits:2048 | openssl pkcs8 -topk8 -
outform der -nocrypt > RSA_2048_PrivateKey.der

openssl genpkey -algorithm rsa -pkeyopt rsa_keygen_bits:3072 | openssl pkcs8 -topk8 -
outform der -nocrypt > RSA_3072_PrivateKey.der

openssl genpkey -algorithm rsa -pkeyopt rsa_keygen_bits:4096 | openssl pkcs8 -topk8 -
outform der -nocrypt > RSA_4096_PrivateKey.der
```

- ECC private keys

```
openssl genpkey -algorithm ec -pkeyopt ec_paramgen_curve:P-256 | openssl pkcs8 -topk8
-outform der -nocrypt > ECC_NIST_P256_PrivateKey.der

openssl genpkey -algorithm ec -pkeyopt ec_paramgen_curve:P-384 | openssl pkcs8 -topk8
-outform der -nocrypt > ECC_NIST_P384_PrivateKey.der

openssl genpkey -algorithm ec -pkeyopt ec_paramgen_curve:P-521 | openssl pkcs8 -topk8
-outform der -nocrypt > ECC_NIST_P521_PrivateKey.der
```

```
openssl genpkey -algorithm ec -pkeyopt ec_paramgen_curve:secp256k1 | openssl pkcs8 -topk8 -outform der -nocrypt > ECC_SECG_P256K1_PrivateKey.der
```

- SM2 private keys (China Regions only)

```
openssl genpkey -algorithm ec -pkeyopt ec_paramgen_curve:sm2 | openssl pkcs8 -topk8 -outform der -nocrypt > SM2_PrivateKey.der
```

Examples of encrypting key material with OpenSSL

The following examples show how to use [OpenSSL](#) to encrypt your key material with the public key that you downloaded. To encrypt your key material using an SM2 public key (China Regions only), use the [SM2OfflineOperationHelper class](#). For more information on the key material types that each wrapping algorithm supports, see [the section called "Select a wrapping algorithm"](#).

Important

These examples are a proof of concept demonstration only. For production systems, use a more secure method (such as a commercial HSM or key management system) to generate and store your key material.

The following combination is NOT supported: ECC_NIST_P521 key material, the RSA_2048 public wrapping key spec, and an RSAES_OAEP_SHA_* wrapping algorithm.

You cannot directly wrap ECC_NIST_P521 key material with a RSA_2048 public wrapping key. Use a larger wrapping key or an RSA_AES_KEY_WRAP_SHA_* wrapping algorithm.

RSAES_OAEP_SHA_1

Amazon KMS supports the RSAES_OAEP_SHA_1 for symmetric encryption keys (SYMMETRIC_DEFAULT), elliptic curve (ECC) private keys, SM2 private keys, and HMAC keys.

RSAES_OAEP_SHA_1 is not supported for RSA private keys. Also, you cannot use an RSA_2048 public wrapping key with any RSAES_OAEP_SHA_* wrapping algorithm to wrap an ECC_NIST_P521 (secp521r1) private key. You must use a larger public wrapping key or an RSA_AES_KEY_WRAP wrapping algorithm.

The following example encrypts your key material with the [public key that you downloaded](#) and the RSAES_OAEP_SHA_1 wrapping algorithm, and saves it in the EncryptedKeyMaterial.bin file.

In this example:

- *WrappingPublicKey.bin* is the file that contains the downloaded wrapping public key.
- *PlaintextKeyMaterial.bin* is the file that contains the key material that you are encrypting, such as `PlaintextKeyMaterial.bin`, `HMAC_384_PlaintextKey.bin` or `ECC_NIST_P521_PrivateKey.der`.

```
$ openssl pkeyutl \  
-encrypt \  
-in PlaintextKeyMaterial.bin \  
-out EncryptedKeyMaterial.bin \  
-inkey WrappingPublicKey.bin \  
-keyform DER \  
-pubin \  
-pkeyopt rsa_padding_mode:oaep \  
-pkeyopt rsa_oaep_md:sha1
```

RSAES_OAEP_SHA_256

Amazon KMS supports the RSAES_OAEP_SHA_256 for symmetric encryption keys (SYMMETRIC_DEFAULT), elliptic curve (ECC) private keys, SM2 private keys, and HMAC keys.

RSAES_OAEP_SHA_256 is not supported for RSA private keys. Also, you cannot use an RSA_2048 public wrapping key with any RSAES_OAEP_SHA_* wrapping algorithm to wrap an ECC_NIST_P521 (secp521r1) private key. You must use a larger public key or an RSA_AES_KEY_WRAP wrapping algorithm.

The following example encrypts key material with the [public key that you downloaded](#) and the RSAES_OAEP_SHA_256 wrapping algorithm, and saves it in the `EncryptedKeyMaterial.bin` file.

In this example:

- *WrappingPublicKey.bin* is the file that contains the downloaded public wrapping key. If you downloaded the public key from the console, this file is named `wrappingKey_KMS_key_key_ID_timestamp` (for example, `wrappingKey_f44c4e20-f83c-48f4-adc6-a1ef38829760_0809092909`).

- *PlaintextKeyMaterial.bin* is the file that contains the key material that you are encrypting, such as `PlaintextKeyMaterial.bin`, `HMAC_384_PlaintextKey.bin`, or `ECC_NIST_P521_PrivateKey.der`.

```
$ openssl pkeyutl \  
-encrypt \  
-in PlaintextKeyMaterial.bin \  
-out EncryptedKeyMaterial.bin \  
-inkey WrappingPublicKey.bin \  
-keyform DER \  
-pubin \  
-pkeyopt rsa_padding_mode:oaep \  
-pkeyopt rsa_oaep_md:sha256 \  
-pkeyopt rsa_mgf1_md:sha256
```

RSA_AES_KEY_WRAP_SHA_1

The `RSA_AES_KEY_WRAP_SHA_1` wrapping algorithm involves two encryption operations.

1. Encrypt your key material with an AES symmetric key that you generate and an AES symmetric encryption algorithm.
2. Encrypt the AES symmetric key that you used with the public key that you downloaded and the `RSAES_OAEP_SHA_1` wrapping algorithm.

The `RSA_AES_KEY_WRAP_SHA_1` wrapping algorithm requires OpenSSL version 3.x or later.

1. Generate a 256-bit AES symmetric encryption key

This command generates an AES symmetric encryption key consisting of 256 random bits, and saves it in the `aes-key.bin` file

```
# Generate a 32-byte AES symmetric encryption key  
$ openssl rand -out aes-key.bin 32
```

2. Encrypt your key material with the AES symmetric encryption key

This command encrypts your key material with the AES symmetric encryption key and saves the encrypted key material in the `key-material-wrapped.bin` file.

In this example command:

- *PlaintextKeyMaterial.bin* is the file that contains the key material that you are importing, such as `PlaintextKeyMaterial.bin`, `HMAC_384_PlaintextKey.bin`, `RSA_3072_PrivateKey.der`, or `ECC_NIST_P521_PrivateKey.der`.
- *aes-key.bin* is the file that contains 256-bit AES symmetric encryption key that you generated in the previous command.

```
# Encrypt your key material with the AES symmetric encryption key
$ openssl enc -id-aes256-wrap-pad \
  -K "$(xxd -p < aes-key.bin | tr -d '\n')" \
  -iv A65959A6 \
  -in PlaintextKeyMaterial.bin \
  -out key-material-wrapped.bin
```

3. Encrypt your AES symmetric encryption key with the public key

This command encrypts your AES symmetric encryption key with the public key that you downloaded and the `RSAES_OAEP_SHA_1` wrapping algorithm, DER-encodes it, and save it in the `aes-key-wrapped.bin` file.

In this example command:

- *WrappingPublicKey.bin* is the file that contains the downloaded public wrapping key. If you downloaded the public key from the console, this file is named `wrappingKey_KMS_key_key_ID_timestamp` (for example, `wrappingKey_f44c4e20-f83c-48f4-adc6-a1ef38829760_0809092909`).
- *aes-key.bin* is the file that contains 256-bit AES symmetric encryption key that you generated in the first command in this example sequence.

```
# Encrypt your AES symmetric encryption key with the downloaded public key
$ openssl pkeyutl \
  -encrypt \
  -in aes-key.bin \
  -out aes-key-wrapped.bin \
  -inkey WrappingPublicKey.bin \
  -keyform DER \
  -pubin \
  -pkeyopt rsa_padding_mode:oaep \
  -pkeyopt rsa_oaep_md:sha1 \
```



```
-pkeyopt rsa_mgf1_md:sha1
```

4. Generate the file to import

Concatenate the file with the encrypted key material and the file with the encrypted AES key. Save them in the `EncryptedKeyMaterial.bin` file, which is the file that you'll import in the [Step 4: Import the key material](#).

In this example command:

- *key-material-wrapped.bin* is the file that contains your encrypted key material.
- *aes-key-wrapped.bin* is the file that contains the encrypted AES encryption key.

```
# Combine the encrypted AES key and encrypted key material in a file
$ cat aes-key-wrapped.bin key-material-wrapped.bin > EncryptedKeyMaterial.bin
```

RSA_AES_KEY_WRAP_SHA_256

The `RSA_AES_KEY_WRAP_SHA_256` wrapping algorithm involves two encryption operations.

1. Encrypt your key material with an AES symmetric key that you generate and an AES symmetric encryption algorithm.
2. Encrypt the AES symmetric key that you used with the public key that you downloaded and the `RSAES_OAEP_SHA_256` wrapping algorithm.

The `RSA_AES_KEY_WRAP_SHA_256` wrapping algorithm requires OpenSSL version 3.x or later.

1. Generate a 256-bit AES symmetric encryption key

This command generates an AES symmetric encryption key consisting of 256 random bits, and saves it in the `aes-key.bin` file

```
# Generate a 32-byte AES symmetric encryption key
$ openssl rand -out aes-key.bin 32
```

2. Encrypt your key material with the AES symmetric encryption key

This command encrypts your key material with the AES symmetric encryption key and saves the encrypted key material in the `key-material-wrapped.bin` file.

In this example command:

- *PlaintextKeyMaterial.bin* is the file that contains the key material that you are importing, such as `PlaintextKeyMaterial.bin`, `HMAC_384_PlaintextKey.bin`, `RSA_3072_PrivateKey.der`, or `ECC_NIST_P521_PrivateKey.der`.
- *aes-key.bin* is the file that contains 256-bit AES symmetric encryption key that you generated in the previous command.

```
# Encrypt your key material with the AES symmetric encryption key
$ openssl enc -id-aes256-wrap-pad \
  -K "$(xxd -p < aes-key.bin | tr -d '\n')" \
  -iv A65959A6 \
  -in PlaintextKeyMaterial.bin \
  -out key-material-wrapped.bin
```

3. Encrypt your AES symmetric encryption key with the public key

This command encrypts your AES symmetric encryption key with the public key that you downloaded and the `RSAES_OAEP_SHA_256` wrapping algorithm, DER-encodes it, and save it in the `aes-key-wrapped.bin` file.

In this example command:

- *WrappingPublicKey.bin* is the file that contains the downloaded public wrapping key. If you downloaded the public key from the console, this file is named `wrappingKey_KMS_key_key_ID_timestamp` (for example, `wrappingKey_f44c4e20-f83c-48f4-adc6-a1ef38829760_0809092909`).
- *aes-key.bin* is the file that contains 256-bit AES symmetric encryption key that you generated in the first command in this example sequence.

```
# Encrypt your AES symmetric encryption key with the downloaded public key
$ openssl pkeyutl \
  -encrypt \
```

```
-in aes-key.bin \  
-out aes-key-wrapped.bin \  
-inkey WrappingPublicKey.bin \  
-keyform DER \  
-pubin \  
-pkeyopt rsa_padding_mode:oaep \  
-pkeyopt rsa_oaep_md:sha256 \  
-pkeyopt rsa_mgf1_md:sha256
```

4. Generate the file to import

Concatenate the file with the encrypted key material and the file with the encrypted AES key. Save them in the `EncryptedKeyMaterial.bin` file, which is the file that you'll import in the [Step 4: Import the key material](#).

In this example command:

- *key-material-wrapped.bin* is the file that contains your encrypted key material.
- *aes-key-wrapped.bin* is the file that contains the encrypted AES encryption key.

```
# Combine the encrypted AES key and encrypted key material in a file  
$ cat aes-key-wrapped.bin key-material-wrapped.bin > EncryptedKeyMaterial.bin
```

Proceed to [Step 4: Import the key material](#).

Step 4: Import the key material

After you [encrypt your key material](#), you can import the key material to use with an Amazon KMS key. To import key material, you upload the encrypted key material from [Step 3: Encrypt the key material](#) and the import token that you downloaded at [Step 2: Download the wrapping public key and import token](#). You must import key material into the same KMS key that you specified when you [downloaded the public key and import token](#). When key material is successfully imported, the [key state](#) of the KMS key changes to `Enabled`, and you can use the KMS key in cryptographic operations.

When you import key material, you can [set an optional expiration time](#) for the key material. When the key material expires, Amazon KMS deletes the key material and the KMS key becomes unusable. To use the KMS key in cryptographic operations, you must reimport the same key material. After you import your key material, you cannot set, change, or cancel the expiration

date for the current import. To change these values, you must [delete](#) and [reimport](#) the same key material.

To import key material, you can use the Amazon KMS console or the [ImportKeyMaterial](#) API. You can use the API directly by making HTTP requests, or by using an [Amazon SDKs](#), [Amazon Command Line Interface](#) or [Amazon Tools for PowerShell](#).

When you import the key material, an [ImportKeyMaterial entry](#) is added to your Amazon CloudTrail log to record the `ImportKeyMaterial` operation. The CloudTrail entry is the same whether you use the Amazon KMS console or the Amazon KMS API.

Setting an expiration time (optional)

When you import the key material for your KMS key, you can set an optional expiration date and time for the key material of up to 365 days from the import date. When imported key material expires, Amazon KMS deletes it. This action changes the [key state](#) of the KMS key to `PendingImport`, which prevents it from being used in any cryptographic operation. To use the KMS key, you must [reimport a copy of the original key material](#).

Ensuring that imported key material expires frequently can help you to satisfy regulatory requirements, but it introduces an additional risk to data encrypted under the KMS key. Until you reimport a copy of the original key material, a KMS key with expired key material is unusable, and any data encrypted under the KMS key is inaccessible. If you fail to reimport the key material for any reason, including losing your copy of the original key material, the KMS key is permanently unusable, and data encrypted under the KMS key is unrecoverable.

To mitigate this risk, make sure that your copy of the imported key material is accessible, and design a system to delete and reimport the key material before it expires and interrupts your Amazon workload. We recommend that you [set an alarm](#) for the expiration of your imported key material that gives you plenty of time to reimport the key material before it expires. You can also use your CloudTrail logs to audit operations that [import \(and reimport\) key material](#) and [delete imported key material](#), and the Amazon KMS operation to [delete expired key material](#).

You cannot import different key material into the KMS key, and Amazon KMS cannot restore, recover, or reproduce the deleted key material. Instead of setting an expiration time, you can programmatically [delete](#) and [reimport](#) the imported key material periodically, but the requirements for retaining a copy of the original key material are the same.

You determine whether and when imported key material expires when you import the key material. But you can turn expiration on and off, or set a new expiration time by deleting and reimporting

the key material. Use the `ExpirationModel` parameter of [ImportKeyMaterial](#) to turn expiration on (`KEY_MATERIAL_EXPIRES`) and off (`KEY_MATERIAL_DOES_NOT_EXPIRE`) and the `ValidTo` parameter to set the expiration time. The maximum time is 365 days from the import data; there is no minimum, but the time must be in the future.

Reimport key material

If you manage a KMS key with imported key material, you might need to reimport the key material. You might reimport key material to replace expiring or deleted key material, or to change the expiration model or expiration date of the key material.

When you import key material into a KMS key, the KMS key is permanently associated with that key material. You can reimport the same key material, but you cannot import different key material into that KMS key. You cannot rotate the key material and Amazon KMS cannot create key material for a KMS key with imported key material.

You can reimport key material at any time, on any schedule that meets your security requirements. You do not have to wait until the key material is at or close to its expiration time.

The procedures to reimport key material are the same the same procedure that you use to import the key material the first time, with the following exceptions.

- Use an existing KMS key, instead of creating a new KMS key. You can skip [Step 1](#) of the import procedure.
- When you reimport key material, you can change the expiration model and expiration date.

Each time you import key material to a KMS key, you need to [download and use a new wrapping key and import token](#) for the KMS key. The wrapping procedure does not affect the content of the key material, so you can use different wrapping public keys and different wrapping algorithms to import the same key material.

Import key material (console)

You can use the Amazon Web Services Management Console to import key material.

1. If you are on the **Upload your wrapped key material** page, skip to [Step 8](#).
2. Sign in to the Amazon Web Services Management Console and open the Amazon Key Management Service (Amazon KMS) console at <https://console.amazonaws.cn/kms>.

3. To change the Amazon Web Services Region, use the Region selector in the upper-right corner of the page.
4. In the navigation pane, choose **Customer managed keys**.
5. Choose the key ID or alias of the KMS key for which you downloaded the public key and import token.
6. Choose the **Cryptographic configuration** tab and view its values. The tabs are on the detail page for a KMS key below the **General configuration** section.

You can only import key material into KMS keys with an **Origin** of **External (Import key material)**. For information about creating KMS keys with imported key material, see [Importing key material for Amazon KMS keys](#).

7. Choose the **Key material** tab and then choose **Import key material**. The **Key material** tab appears only for KMS keys with an **Origin** value of **External (Import key material)**.

If you downloaded the key material, import token, and encrypted the key material, choose **Next**.

8. In the **Encrypted key material and import token** section, do the following.
 - a. Under **Wrapped key material**, choose **Choose file**. Then upload the file that contains your wrapped (encrypted) key material.
 - b. Under **Import token**, choose **Choose file**. Upload the file that contains the import token that you [downloaded](#).
9. In the **Expiration option** section, you determine whether the key material expires. To set an expiration date and time, choose **Key material expires**, and use the calendar to select a date and time. You can specify a date up to 365 days from the current date and time.
10. Choose **Upload key material**.

Import key material (Amazon KMS API)

To import key material, use the [ImportKeyMaterial](#) operation. The following example uses the [Amazon CLI](#), but you can use any supported programming language.

To use this example:

1. Replace `1234abcd-12ab-34cd-56ef-1234567890ab` with a key ID of the KMS key that you specified when you downloaded the public key and import token. To identify the KMS key, use its [key ID](#) or [key ARN](#). You cannot use an [alias name](#) or [alias ARN](#) for this operation.

2. Replace `EncryptedKeyMaterial.bin` with the name of the file that contains the encrypted key material.
3. Replace `ImportToken.bin` with the name of the file that contains the import token.
4. If you want the imported key material to expire, set the value of the `expiration-model` parameter to its default value, `KEY_MATERIAL_EXPIRES`, or omit the `expiration-model` parameter. Then, replace the value of the `valid-to` parameter with the date and time that you want the key material to expire. The date and time can be up to 365 days from the time of the request.

```
$ aws kms import-key-material --key-id 1234abcd-12ab-34cd-56ef-1234567890ab \  
  --encrypted-key-material fileb://EncryptedKeyMaterial.bin \  
  --import-token fileb://ImportToken.bin \  
  --expiration-model KEY_MATERIAL_EXPIRES \  
  --valid-to 2023-06-17T12:00:00-08:00
```

If you do not want the imported key material to expire, set the value of the `expiration-model` parameter to `KEY_MATERIAL_DOES_NOT_EXPIRE` and omit the `valid-to` parameter from the command.

```
$ aws kms import-key-material --key-id 1234abcd-12ab-34cd-56ef-1234567890ab \  
  --encrypted-key-material fileb://EncryptedKeyMaterial.bin \  
  --import-token fileb://ImportToken.bin \  
  --expiration-model KEY_MATERIAL_DOES_NOT_EXPIRE
```

Tip

If the command does not succeed, you might see a `KMSInvalidStateException` or a `NotFoundException`. You can retry the request.

Create a KMS key in an Amazon CloudHSM key store

After you have created an Amazon CloudHSM key store, you can create Amazon KMS keys in your key store. They must be [symmetric encryption KMS keys](#) with key material that Amazon KMS generates. You cannot create [asymmetric KMS keys](#), [HMAC KMS keys](#) or KMS keys with [imported key material](#) in a custom key store. Also, you cannot use symmetric encryption KMS keys in a custom key store to generate asymmetric data key pairs.

To create a KMS key in an Amazon CloudHSM key store, the Amazon CloudHSM key store must be [connected to the associated Amazon CloudHSM cluster](#) and the cluster must contain at least two active HSMs in different Availability Zones. To find the connection state and number of HSMs, view the [Amazon CloudHSM key stores page](#) in the Amazon Web Services Management Console. When using the API operations, use the [DescribeCustomKeyStores](#) operation to verify that the Amazon CloudHSM key store is connected. To verify the number of active HSMs in the cluster and their Availability Zones, use the Amazon CloudHSM [DescribeClusters](#) operation.

When you create a KMS key in your Amazon CloudHSM key store, Amazon KMS creates the KMS key in Amazon KMS. But, it creates the key material for the KMS key in the associated Amazon CloudHSM cluster. Specifically, Amazon KMS signs into the cluster as the [kmsuser CU that you created](#). Then it creates a persistent, non-extractable, 256-bit Advanced Encryption Standard (AES) symmetric key in the cluster. Amazon KMS sets the value of the [key label attribute](#), which is visible only in the cluster, to Amazon Resource Name (ARN) of the KMS key.

When the command succeeds, the [key state](#) of the new KMS key is Enabled and its origin is AWS_CLOUDHSM. You cannot change the origin of any KMS key after you create it. When you view a KMS key in an Amazon CloudHSM key store in the Amazon KMS console or by using the [DescribeKey](#) operation, you can see typical properties, like its key ID, key state, and creation date. But you can also see the custom key store ID and (optionally) the Amazon CloudHSM cluster ID.

If your attempt to create a KMS key in your Amazon CloudHSM key store fails, use the error message to help you determine the cause. It might indicate that the Amazon CloudHSM key store is not connected (`CustomKeyStoreInvalidStateException`) or the associated Amazon CloudHSM cluster doesn't have the two active HSMs that are required for this operation (`CloudHsmClusterInvalidConfigurationException`). For help see [Troubleshooting a custom key store](#).

For an example of the Amazon CloudTrail log of the operation that creates a KMS key in an Amazon CloudHSM key store, see [CreateKey](#).

Create a new KMS key in your CloudHSM key store

You can create a symmetric encryption KMS key in your Amazon CloudHSM key store in the Amazon KMS console or by using the [CreateKey](#) operation.

Using the Amazon KMS console

Use the following procedure to create a symmetric encryption KMS key in an Amazon CloudHSM key store.

Note

Do not include confidential or sensitive information in the alias, description, or tags. These fields may appear in plain text in CloudTrail logs and other output.

1. Sign in to the Amazon Web Services Management Console and open the Amazon Key Management Service (Amazon KMS) console at <https://console.amazonaws.cn/kms>.
2. To change the Amazon Web Services Region, use the Region selector in the upper-right corner of the page.
3. In the navigation pane, choose **Customer managed keys**.
4. Choose **Create key**.
5. Choose **Symmetric**.
6. In **Key usage**, the **Encrypt and decrypt** option is selected for you. Do not change it.
7. Choose **Advanced options**.
8. For **Key material origin**, choose **Amazon CloudHSM key store**.

You cannot create a multi-Region key in an Amazon CloudHSM key store.

9. Choose **Next**.
10. Select an Amazon CloudHSM key store for your new KMS key. To create a new Amazon CloudHSM key store, choose **Create custom key store**.

The Amazon CloudHSM key store that you select must have a status of **Connected**. Its associated Amazon CloudHSM cluster must be active and contain at least two active HSMs in different Availability Zones.

For help with connecting an Amazon CloudHSM key store, see [Disconnect an Amazon CloudHSM key store](#). For help with adding HSMs, see [Adding an HSM](#) in the *Amazon CloudHSM User Guide*.

11. Choose **Next**.
12. Type an alias and an optional description for the KMS key.
13. (Optional). On the **Add Tags** page, add tags that identify or categorize your KMS key.

When you add tags to your Amazon resources, Amazon generates a cost allocation report with usage and costs aggregated by tags. Tags can also be used to control access to a KMS key. For information about tagging KMS keys, see [Tags in Amazon KMS](#) and [ABAC for Amazon KMS](#).

14. Choose **Next**.
15. In the **Key Administrators** section, select the IAM users and roles who can manage the KMS key. For more information, see [Allows key administrators to administer the KMS key](#).

Notes

IAM policies can give other IAM users and roles permission to use the KMS key. IAM best practices discourage the use of IAM users with long-term credentials. Whenever possible, use IAM roles, which provide temporary credentials. For details, see [Security best practices in IAM](#) in the *IAM User Guide*.

The Amazon KMS console adds key administrators to the key policy under the statement identifier "Allow access for Key Administrators". Modifying this statement identifier might impact how the console displays updates that you make to the statement.

16. (Optional) To prevent these key administrators from deleting this KMS key, clear the box at the bottom of the page for **Allow key administrators to delete this key**.
17. Choose **Next**.
18. In the **This account** section, select the IAM users and roles in this Amazon Web Services account that can use the KMS key in [cryptographic operations](#). For more information, see [Allows key users to use the KMS key](#).

Notes

IAM best practices discourage the use of IAM users with long-term credentials. Whenever possible, use IAM roles, which provide temporary credentials. For details, see [Security best practices in IAM](#) in the *IAM User Guide*.

The Amazon KMS console adds key users to the key policy under the statement identifiers "Allow use of the key" and "Allow attachment of persistent resources". Modifying these statement identifiers might impact how the console displays updates that you make to the statement.

19. (Optional) You can allow other Amazon Web Services accounts to use this KMS key for cryptographic operations. To do so, in the **Other Amazon Web Services accounts** section at the bottom of the page, choose **Add another Amazon Web Services account** and enter the Amazon Web Services account ID of an external account. To add multiple external accounts, repeat this step.

Note

Administrators of the other Amazon Web Services accounts must also allow access to the KMS key by creating IAM policies for their users. For more information, see [Allowing users in other accounts to use a KMS key](#).

20. Choose **Next**.
21. Review the key policy statements for the key. To make changes to the key policy, select **Edit**.
22. Choose **Next**.
23. Review the key settings that you chose. You can still go back and change all settings.
24. When you're done, choose **Finish** to create the key.

When the procedure succeeds, the display shows the new KMS key in the Amazon CloudHSM key store that you chose. When you choose the name or alias of the new KMS key, the **Cryptographic configuration** tab on its detail page displays the origin of the KMS key (**Amazon CloudHSM**), the name, ID, and type of the custom key store, and the ID of the Amazon CloudHSM cluster. If the procedure fails, an error message appears that describes the failure.

Tip

To make it easier to identify KMS keys in a custom key store, on the **Customer managed keys** page, add the **Custom key store ID** column to the display. Click the gear icon in the upper-right and select **Custom key store ID**. For details, see [Customize your console view](#).

Using the Amazon KMS API

To create a new Amazon KMS key (KMS key) in your Amazon CloudHSM key store, use the [CreateKey](#) operation. Use the `CustomKeyStoreId` parameter to identify your custom key store and specify an `Origin` value of `AWS_CLOUDHSM`.

You might also want to use the `Policy` parameter to specify a key policy. You can change the key policy ([PutKeyPolicy](#)) and add optional elements, such as a [description](#) and [tags](#) at any time.

The examples in this section use the [Amazon Command Line Interface \(Amazon CLI\)](#), but you can use any supported programming language.

The following example begins with a call to the [DescribeCustomKeyStores](#) operation to verify that the Amazon CloudHSM key store is connected to its associated Amazon CloudHSM cluster. By default, this operation returns all custom keys stores in your account and Region. To describe only a particular Amazon CloudHSM key store, use its CustomKeyId or CustomKeyName parameter (but not both).

Before running this command, replace the example custom key store ID with a valid ID.

Note

Do not include confidential or sensitive information in the Description or Tags fields. These fields may appear in plain text in CloudTrail logs and other output.

```
$ aws kms describe-custom-key-stores --custom-key-store-id cks-1234567890abcdef0
{
  "CustomKeyStores": [
    {
      "CustomKeyId": "cks-1234567890abcdef0",
      "CustomKeyName": "ExampleKeyStore",
      "CustomKeyType": "Amazon CloudHSM key store",
      "CloudHsmClusterId": "cluster-1a23b4cdefg",
      "TrustAnchorCertificate": "<certificate string appears here>",
      "CreationDate": "1.499288695918E9",
      "ConnectionState": "CONNECTED"
    }
  ],
}
```

The next example command uses the [DescribeClusters](#) operation to verify that the Amazon CloudHSM cluster that is associated with the ExampleKeyStore (cluster-1a23b4cdefg) has at least two active HSMs. If the cluster has fewer than two HSMs, the CreateKey operation fails.

```
$ aws cloudhsmv2 describe-clusters
{
  "Clusters": [
    {
      "SubnetMapping": {
        ...
      },
      "CreateTimestamp": 1507133412.351,
      "ClusterId": "cluster-1a23b4cdefg",
      "SecurityGroup": "sg-865af2fb",
    }
  ]
}
```



```
{
  "KeyMetadata": {
    "AWSAccountId": "111122223333",
    "Arn": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab",
    "CreationDate": 1.499288695918E9,
    "Description": "Example key",
    "Enabled": true,
    "MultiRegion": false,
    "KeyId": "1234abcd-12ab-34cd-56ef-1234567890ab",
    "KeyManager": "CUSTOMER",
    "KeyState": "Enabled",
    "KeyUsage": "ENCRYPT_DECRYPT",
    "Origin": "AWS_CLOUDHSM"
    "CloudHsmClusterId": "cluster-1a23b4cdefg",
    "CustomKeyStoreId": "cks-1234567890abcdef0"
    "KeySpec": "SYMMETRIC_DEFAULT",
    "CustomerMasterKeySpec": "SYMMETRIC_DEFAULT",
    "EncryptionAlgorithms": [
      "SYMMETRIC_DEFAULT"
    ]
  }
}
```

Create a KMS key in external key stores

After you have [created](#) and [connected](#) your external key store, you can create Amazon KMS keys in your key store. They must be [symmetric encryption KMS keys](#) with an origin value of **External key store** (EXTERNAL_KEY_STORE). You cannot create [asymmetric KMS keys](#), [HMAC KMS keys](#) or KMS keys with [imported key material](#) in a custom key store. Also, you cannot use symmetric encryption KMS keys in a custom key store to generate asymmetric data key pairs.

A KMS key in an external key store might have poorer latency, durability and availability than a standard KMS key because it depends on components located outside of Amazon. Before creating or using a KMS key in an external key store, verify that you require a key with external key store properties.

Note

Some external key managers provide a simpler method for creating KMS keys in an external key store. For details, see your external key manager documentation.

To create a KMS key in your external key store, you specify the following:

- The ID of your external key store.
- A [key material origin](#) of External key store (EXTERNAL_KEY_STORE).
- The ID of an existing [external key](#) in the [external key manager](#) associated with your external key store. This external key serves as key material for the KMS key. You cannot change the external key ID after you create the KMS key.

Amazon KMS provides the external key ID to your external key store proxy in requests for encryption and decryption operations. Amazon KMS cannot directly access your external key manager or any of its cryptographic keys.

In addition to the external key, a KMS key in an external key store also has Amazon KMS key material. All data encrypted under the KMS key is first encrypted in Amazon KMS using the key's Amazon KMS key material and then by your external key manager using your external key. This [double encryption](#) process ensures that ciphertext protected by a KMS key in an external key store is at least as strong as ciphertext protected only by Amazon KMS. For details, see [How external key stores work](#).

When the CreateKey operation succeeds, the [key state](#) of the new KMS key is Enabled. When you [view a KMS key in an external key store](#) you can see typical properties, like its key ID, [key spec](#), [key usage](#), [key state](#), and creation date. But you can also see the ID and [connection state](#) of the external key store and the ID of the external key.

If your attempt to create a KMS key in your external key store fails, use the error message to identify the cause. It might indicate that the external key store is not connected (`CustomKeyStoreInvalidStateException`), that your external key store proxy cannot find an external key with the specified external key ID (`XksKeyNotFoundException`), or that the external key is already associated with a KMS key in the same external key store (`XksKeyAlreadyInUseException`).

For an example of the Amazon CloudTrail log of the operation that creates a KMS key in an external key store, see [CreateKey](#).

Topics

- [Requirements for a KMS key in an external key store](#)
- [Create a new KMS key in your external key store](#)

Requirements for a KMS key in an external key store

To create a KMS key in an external key store, the following properties are required of the external key store, the KMS key, and the external key that serves as the external cryptographic key material for the KMS key.

External key store requirements

- Must be connected to its external key store proxy.

To view the [connection state](#) of your external key store, see [View external key stores](#). To connect your external key store, see [Connect and disconnect external key stores](#).

KMS key requirements

You cannot change these properties after you create the KMS key.

- Key spec: SYMMETRIC_DEFAULT
- Key usage: ENCRYPT_DECRYPT
- Key material origin: EXTERNAL_KEY_STORE
- Multi-Region: FALSE

External key requirements

- 256-bit AES cryptographic key (256 random bits). The KeySpec of the external key must be AES_256.
- Enabled and available for use. The Status of the external key must be ENABLED.
- Configured for encryption and decryption. The KeyUsage of the external key must include ENCRYPT and DECRYPT.

- Used only with this KMS key. Each KMS key in an external key store must be associated with a different external key.

Amazon KMS also recommends that the external key be used exclusively for the external key store. This restriction makes it easier to identify and resolve problems with the key.

- Accessible by the [external key store proxy](#) for the external key store.

If the external key store proxy can't find the key using the specified external key ID, the `CreateKey` operation fails.

- Can handle the anticipated traffic that your use of Amazon Web Services services generates. Amazon KMS recommends that external keys be prepared to handle up to 1800 requests per second.

Create a new KMS key in your external key store

You can create a new KMS key in your external key store in the Amazon KMS console or by using the [CreateKey](#) operation.

Using the Amazon KMS console

There are two ways to create a KMS key in an external key store.

- Method 1 (recommended): Choose an external key store, then create a KMS key in that external key store.
- Method 2: Create a KMS key, then indicate that it's in an external key store.

If you use Method 1, where you choose your external key store before you create your key, Amazon KMS chooses all required KMS key properties for you and fills in the ID of your external key store. This method avoids errors you might make when creating your KMS key.

Note

Do not include confidential or sensitive information in the alias, description, or tags. These fields may appear in plain text in CloudTrail logs and other output.

Method 1 (recommended): Start in your external key store

To use this method, choose your external key store, then create a KMS key. The Amazon KMS console chooses all required properties for you and fills in the ID of your external key store. This method avoids many errors you might make when creating your KMS key.

1. Sign in to the Amazon Web Services Management Console and open the Amazon Key Management Service (Amazon KMS) console at <https://console.amazonaws.cn/kms>.
2. To change the Amazon Web Services Region, use the Region selector in the upper-right corner of the page.
3. In the navigation pane, choose **Custom key stores, External key stores**.
4. Choose the name of your external key store.
5. In the top right corner, choose **Create a KMS key in this key store**.

If the external key store is *not* connected, you will be prompted to connect it. If the connection attempt fails, you need to resolve the problem and connect the external key store before you can create a new KMS key in it.

If the external key store is connected, you are redirected to the **Customer managed keys** page for creating a key. The required **Key configuration** values are already chosen for you. Also, the custom key store ID of your external key store is filled in, although you can change it.

6. Enter the key ID of an [external key](#) in your [external key manager](#). This external key must [fulfill the requirements](#) for use with a KMS key. You cannot change this value after the key is created.

If the external key has multiple IDs, enter the key ID that the external key store proxy uses to identify the external key.

7. Confirm that you intend to create a KMS key in the specified external key store.
8. Choose **Next**.


The remainder of this procedure is the same as [creating a standard KMS key](#).

9. Type an alias (required) and a description (optional) for the KMS key.
10. (Optional). On the **Add Tags** page, add tags that identify or categorize your KMS key.

When you add tags to your Amazon resources, Amazon generates a cost allocation report with usage and costs aggregated by tags. Tags can also be used to control access to a KMS key. For information about tagging KMS keys, see [Tags in Amazon KMS](#) and [ABAC for Amazon KMS](#).

11. Choose **Next**.

12. In the **Key Administrators** section, select the IAM users and roles who can manage the KMS key. For more information, see [Allows key administrators to administer the KMS key](#).

 **Note**


IAM policies can give other IAM users and roles permission to use the KMS key. IAM best practices discourage the use of IAM users with long-term credentials. Whenever possible, use IAM roles, which provide temporary credentials. For details, see [Security best practices in IAM](#) in the *IAM User Guide*.

13. (Optional) To prevent these key administrators from deleting this KMS key, clear **Allow key administrators to delete this key** check box.

Deleting a KMS key is a destructive and irreversible operation that can render ciphertext unrecoverable. You cannot recreate a symmetric KMS key in an external key store, even if you have the external key material. However, deleting a KMS key has no effect on its associated external key. For information about deleting a KMS key from an external key store, see [Special considerations for deleting keys](#).

14. Choose **Next**.

15. In the **This account** section, select the IAM users and roles in this Amazon Web Services account that can use the KMS key in [cryptographic operations](#). For more information, see [Allows key users to use the KMS key](#).

 **Note**

IAM policies can give other IAM users and roles permission to use the KMS key. IAM best practices discourage the use of IAM users with long-term credentials. Whenever possible, use IAM roles, which provide temporary credentials. For details, see [Security best practices in IAM](#) in the *IAM User Guide*.

16. (Optional) You can allow other Amazon Web Services accounts to use this KMS key for cryptographic operations. To do so, in the **Other Amazon Web Services accounts** section at the bottom of the page, choose **Add another Amazon Web Services account** and enter the Amazon Web Services account ID of an external account. To add multiple external accounts, repeat this step.

Note

Administrators of the other Amazon Web Services accounts must also allow access to the KMS key by creating IAM policies for their users. For more information, see [Allowing users in other accounts to use a KMS key](#).

17. Choose **Next**.
18. Review the key settings that you chose. You can still go back and change all settings.
19. When you're done, choose **Finish** to create the key.

Method 2: Start in Customer managed keys

This procedure is the same as the procedure to create a symmetric encryption key with Amazon KMS key material. But, in this procedure, you specify the custom key store ID of the external key store and the key ID of the external key. You must also specify the [required property values](#) for a KMS key in an external key store, such as the key spec and key usage.

1. Sign in to the Amazon Web Services Management Console and open the Amazon Key Management Service (Amazon KMS) console at <https://console.amazonaws.cn/kms>.
2. To change the Amazon Web Services Region, use the Region selector in the upper-right corner of the page.
3. In the navigation pane, choose **Customer managed keys**.
4. Choose **Create key**.
5. Choose **Symmetric**.
6. In **Key usage**, the **Encrypt and decrypt** option is selected for you. Do not change it.
7. Choose **Advanced options**.
8. For **Key material origin**, choose **External key store**.
9. Confirm that you intend to create a KMS key in the specified external key store.
10. Choose **Next**.
11. Choose the row that represents the external key store for your new KMS key.

You cannot choose a disconnected external key store. To connect a key store that is disconnected, choose the key store name, and then, from **Key store actions**, choose, **Connect**. For details, see [Using the Amazon KMS console](#).

12. Enter the key ID of an [external key](#) in your [external key manager](#). This external key must [fulfill the requirements](#) for use with a KMS key. You cannot change this value after the key is created.

If the external key has multiple IDs, enter the key ID that the external key store proxy uses to identify the external key.


13. Choose **Next**.

The remainder of this procedure is the same as [creating a standard KMS key](#).

14. Type an alias and an optional description for the KMS key.
15. (Optional). On the **Add Tags** page, add tags that identify or categorize your KMS key.

When you add tags to your Amazon resources, Amazon generates a cost allocation report with usage and costs aggregated by tags. Tags can also be used to control access to a KMS key. For information about tagging KMS keys, see [Tags in Amazon KMS](#) and [ABAC for Amazon KMS](#).

16. Choose **Next**.
17. In the **Key Administrators** section, select the IAM users and roles who can manage the KMS key. For more information, see [Allows key administrators to administer the KMS key](#).

 **Note**

IAM policies can give other IAM users and roles permission to use the KMS key.

18. (Optional) To prevent these key administrators from deleting this KMS key, clear **Allow key administrators to delete this key** check box.

Deleting a KMS key is a destructive and irreversible operation that can render ciphertext unrecoverable. You cannot recreate a symmetric KMS key in an external key store, even if you have the external key material. However, deleting a KMS key has no effect on its associated external key. For information about deleting a KMS key from an external key store, see [Delete an Amazon KMS key](#).

19. Choose **Next**.
20. In the **This account** section, select the IAM users and roles in this Amazon Web Services account that can use the KMS key in [cryptographic operations](#). For more information, see [Allows key users to use the KMS key](#).

Note

IAM policies can give other IAM users and roles permission to use the KMS key.

21. (Optional) You can allow other Amazon Web Services accounts to use this KMS key for cryptographic operations. To do so, in the **Other Amazon Web Services accounts** section at the bottom of the page, choose **Add another Amazon Web Services account** and enter the Amazon Web Services account ID of an external account. To add multiple external accounts, repeat this step.

Note

Administrators of the other Amazon Web Services accounts must also allow access to the KMS key by creating IAM policies for their users. For more information, see [Allowing users in other accounts to use a KMS key](#).

22. Choose **Next**.
23. Review the key settings that you chose. You can still go back and change all settings.
24. When you're done, choose **Finish** to create the key.

When the procedure succeeds, the display shows the new KMS key in the external key store that you chose. When you choose the name or alias of the new KMS key, the **Cryptographic configuration** tab on its detail page displays the origin of the KMS key (**External key store**), the name, ID, and type of the custom key store, and the ID, key usage, and status of the external key. If the procedure fails, an error message appears that describes the failure. For , see [Troubleshooting external key stores](#).

Tip

To make it easier to identify KMS keys in a custom key store, on the **Customer managed keys** page, add the **Origin** and **Custom key store ID** column to the display. To change the table fields, choose the gear icon in the upper right corner of the page. For details, see [Customize your console view](#).

Using the Amazon KMS API

To create a new KMS key in an external key store, use the [CreateKey](#) operation. The following parameters are required:

- The `Origin` value must be `EXTERNAL_KEY_STORE`.
- The `CustomKeyStoreId` parameter identifies your external key store. The [ConnectionState](#) of the specified external key store must be `CONNECTED`. To find the `CustomKeyStoreId` and `ConnectionState`, use the `DescribeCustomKeyStores` operation.
- The `XksKeyId` parameter identifies the external key. This external key must [fulfills the requirements](#) for association with a KMS key.

You can also use any of the optional parameters of the `CreateKey` operation, such as using the `Policy` or [Tags](#) parameters.

Note

Do not include confidential or sensitive information in the `Description` or `Tags` fields. These fields may appear in plain text in CloudTrail logs and other output.

The examples in this section use the [Amazon Command Line Interface \(Amazon CLI\)](#), but you can use any supported programming language.

This example command uses the [CreateKey](#) operation to create a KMS key in an external key store. The response includes the properties of the KMS keys, the ID of the external key store, and the ID, usage, and status of the external key.

Before running this command, replace the example custom key store ID with a valid ID.

```
$ aws kms create-key --origin EXTERNAL_KEY_STORE --custom-key-store-id cks-1234567890abcdef0 --xks-key-id bb8562717f809024
{
  "KeyMetadata": {
    "Arn": "arn:aws:kms:us-west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab",
    "AWSAccountId": "111122223333",
    "CreationDate": "2022-12-02T07:48:55-07:00",
    "CustomerMasterKeySpec": "SYMMETRIC_DEFAULT",
```

```
"CustomKeyStoreId": "cks-1234567890abcdef0",
"Description": "",
"Enabled": true,
"EncryptionAlgorithms": [
  "SYMMETRIC_DEFAULT"
],
"KeyId": "1234abcd-12ab-34cd-56ef-1234567890ab",
"KeyManager": "CUSTOMER",
"KeySpec": "SYMMETRIC_DEFAULT",
"KeyState": "Enabled",
"KeyUsage": "ENCRYPT_DECRYPT",
"MultiRegion": false,
"Origin": "EXTERNAL_KEY_STORE",
"XksKeyConfiguration": {
  "Id": "bb8562717f809024"
}
}
}
```


Identify and view keys

You can use [Amazon Web Services Management Console](#) or the [Amazon Key Management Service \(Amazon KMS\) API](#) to view Amazon KMS keys in each account and Region, including KMS keys that you manage and KMS keys that are managed by Amazon.

Topics

- [Find the key ID and key ARN](#)
- [Access and list KMS key details](#)
- [Identify different key types](#)
- [Customize your console view](#)
- [Find KMS keys and key material in an Amazon CloudHSM key store](#)

Find the key ID and key ARN

To identify an Amazon KMS key, you can use the [key ID](#) or the Amazon Resource Name ([key ARN](#)). In [cryptographic operations](#), you can also use the [alias name](#) or [alias ARN](#).

You can use the [Amazon KMS console](#) or the [ListKeys](#) operation to identify the key ID and key ARN of each KMS key in your account and Region.

For detailed information about the KMS key identifiers supported by Amazon KMS, see [Key identifiers \(KeyId\)](#). For help finding an alias name and alias ARN, see [Find the alias name and alias ARN for a KMS key](#).

Using the Amazon KMS console

1. Open the Amazon KMS console at <https://console.amazonaws.cn/kms>.
2. To change the Amazon Web Services Region, use the Region selector in the upper-right corner of the page.
3. To view the keys in your account that you create and manage, in the navigation pane choose **Customer managed keys**. To view the keys in your account that Amazon creates and manages for you, in the navigation pane, choose **Amazon managed keys**.
4. To find the [key ID](#) for a KMS key, see the row that begins with the KMS key alias.

The **Key ID** column appears in the tables by default. If the Key ID column doesn't appear in your table, use the procedure described in [the section called “Customize your console view”](#) to restore it. You can also view the key ID of a KMS key on its details page.

Customer managed keys				
Key actions ▼ Create key				
Search				
Aliases	Key ID	Status	Creation date	
<input type="checkbox"/> key-test	1234abcd-12ab-34cd-56ef-1234567890ab	Enabled	Oct 19, 2018 12:43 PDT	

- To find the Amazon Resource Name (ARN) of the KMS key, choose the key ID or alias. The [key ARN](#) appears in the **General Configuration** section.

General configuration		
Aliases key-test	Status Enabled	ARN arn:aws:kms:us-east-1:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab
Description -	Creation date Nov 06, 2018 15:11 PST	

Using the Amazon KMS API

To find the [key ID](#) and [key ARN](#) of an Amazon KMS key, use the [ListKeys](#) operation.

The ListKeys operation returns the key ID and Amazon Resource Name (ARN) of all KMS keys in the caller's account and Region.

For example, this call to the ListKeys operation returns the ID and ARN of each KMS key in this fictitious account. For examples in multiple programming languages, see [Use ListKeys with an Amazon SDK or CLI](#).

```
$ aws kms list-keys
{
  "Keys": [
    {
      "KeyId": "1234abcd-12ab-34cd-56ef-1234567890ab",
```

```
    "KeyArn": "arn:aws:kms:us-  
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab"  
  },  
  {  
    "KeyId": "0987dcba-09fe-87dc-65ba-ab0987654321",  
    "KeyArn": "arn:aws:kms:us-west-2:111122223333:key/0987dcba-09fe-87dc-65ba-  
ab0987654321"  
  }  
]  
}
```

Access and list KMS key details

You can use the [Amazon KMS console](#) or the [DescribeKey](#) operation to access and list detailed information about the KMS keys in the account and Region.

The following procedures demonstrate how to access KMS key details, such as the key ID, key spec, key usage, and more.

Using the Amazon KMS console

The details page for each KMS key displays the properties of the KMS key. It differs slightly for the different types of KMS keys.

To display detailed information about a KMS key, on the **Amazon managed keys** or **Customer managed keys** page, choose the alias or key ID of the KMS key.

The details page for a KMS key includes a **General Configuration** section that displays the basic properties of the KMS key. It also includes tabs on which you can view and edit properties of the KMS key, such as **Key policy**, **Cryptographic configuration**, **Tags**, **Key material** (for KMS keys with imported key material), **Key rotation** (for symmetric encryption KMS keys), **Regionality** (for multi-Region keys), and **Public key** (for asymmetric KMS keys).

Note

The Amazon KMS console displays the KMS keys that you have [permission to view](#) in your account and Region. KMS keys in other Amazon Web Services accounts do not appear in the console, even if you have permission to view, manage, and use them. To view KMS keys in other accounts, use the [DescribeKey](#) operation.

To navigate to the key details page for a KMS key.

1. Sign in to the Amazon Web Services Management Console and open the Amazon Key Management Service (Amazon KMS) console at <https://console.amazonaws.cn/kms>.
2. To change the Amazon Web Services Region, use the Region selector in the upper-right corner of the page.
3. To view the keys in your account that you create and manage, in the navigation pane choose **Customer managed keys**. To view the keys in your account that Amazon creates and manages for you, in the navigation pane, choose **Amazon managed keys**.
4. To open the key details page, in the key table, choose the key ID or alias of the KMS key.

If the KMS key has multiple aliases, an alias summary (**+n more**) appears beside the name of the one of the aliases. Choosing the alias summary takes you directly to the **Aliases** tab on the key details page.

KMS > Customer managed keys > Key ID: 0987dcba-09fe-87dc-65ba-ab0987654321

0987dcba-09fe-87dc-65ba-ab0987654321 Key actions ▼ Edit

General configuration

Aliases key-test	Status Enabled	ARN arn:aws:kms:us-east-1:111122223333:key/0987dcba-09fe-87dc-65ba-ab0987654321
Description -	Creation date Nov 06, 2018 15:11 PST	

Key policy | **Cryptographic configuration** | Tags | Key rotation | Aliases

Cryptographic configuration

Key Type Symmetric	Origin AWS_KMS	Key Spec SYMMETRIC_DEFAULT	Key Usage Encrypt and decrypt
-----------------------	-------------------	-------------------------------	----------------------------------

The following list describes the fields in the detailed display, including field in the tabs. Some of these fields are also available as columns in the table display.

Aliases

Where: Aliases tab

A friendly name for the KMS key. You can use an alias to identify the KMS key in the console and in some Amazon KMS APIs. For details, see [Aliases in Amazon KMS](#).

The **Aliases** tab displays all aliases associated with the KMS key in the Amazon Web Services account and Region.

ARN

Where: General configuration section

The Amazon Resource Name (ARN) of the KMS key. This value uniquely identifies the KMS key. You can use it to identify the KMS key in Amazon KMS API operations.

Connection state

Indicates whether a [custom key store](#) is connected to its backing key store. This field appears only when the KMS key is created in a custom key store.

For information about the values in this field, see [ConnectionState](#) in the *Amazon KMS API Reference*.

Creation date

Where: General configuration section

The date and time that the KMS key was created. This value is displayed in local time for the device. The time zone does not depend on the Region.

Unlike **Expiration**, the creation refers only to the KMS key, not its key material.

CloudHSM cluster ID

Where: Cryptographic configuration tab

The cluster ID of the Amazon CloudHSM cluster that contains the key material for the KMS key. This field appears only when the KMS key is created in a [custom key store](#).

If you choose the CloudHSM cluster ID, it opens the **Clusters** page in the Amazon CloudHSM console.

Custom key store ID

Where: Cryptographic configuration tab

The ID of the [custom key store](#) that contains the KMS key. This field appears only when the KMS key is created in a custom key store.

If you choose the custom key store ID, it opens the **Custom key stores** page in the Amazon KMS console.

Custom key store name

Where: Cryptographic configuration tab

The name of the [custom key store](#) that contains the KMS key. This field appears only when the KMS key is created in a custom key store.

Custom key store type

Where: Cryptographic configuration tab

Indicates whether the custom key store is an [Amazon CloudHSM key store](#) or an [external key store](#). This field appears only when the KMS key is created in a [custom key store](#).

Description

Where: General configuration section

A brief, optional description of the KMS key that you can write and edit. To add or update the description of a customer managed key, above **General Configuration**, choose **Edit**.

Encryption algorithms

Where: Cryptographic configuration tab

Lists the encryption algorithms that can be used with the KMS key in Amazon KMS. This field appears only when the **Key type** is **Asymmetric** and the **Key usage** is **Encrypt and decrypt**. For information about the encryption algorithms that Amazon KMS supports, see [SYMMETRIC_DEFAULT key spec](#) and [RSA key specs for encryption and decryption](#).

Expiration date

Where: Key material tab

The date and time when the key material for the KMS key expires. This field appears only for KMS keys with [imported key material](#), that is, when the **Origin** is **External** and the KMS key has key material that expires.

External key ID

Where: Cryptographic configuration tab

The ID of the [external key](#) that is associated with a KMS key in an [external key store](#). This field appears only for KMS keys in an external key store.

External key status

Where: Cryptographic configuration tab

The most recent status that the [external key store proxy](#) reported for the [external key](#) associated with the KMS key. This field appears only for KMS keys in an external key store.

External key usage

Where: Cryptographic configuration tab

The cryptographic operations that are enabled on the [external key](#) associated with the KMS key. This field appears only for KMS keys in an external key store.

Key policy

Where: Key policy tab

Controls access to the KMS key along with [IAM policies](#) and [grants](#). Every KMS key has one key policy. It is the only mandatory authorization element. To change the key policy of a customer managed key, on the **Key policy** tab, choose **Edit**. For details, see [the section called "Key policies"](#).

Key rotation

Where: Key rotation tab

Enables and disables [automatic rotation](#) of the key material in a [customer managed KMS key](#). To change the key rotation status of a [customer managed key](#), use the check box on the **Key rotation** tab.

You can't enable or disable rotation of the key material in an [Amazon managed key](#). Amazon managed keys are automatically rotated every year.

Key spec

Where: Cryptographic configuration tab

The type of key material in the KMS key. Amazon KMS supports symmetric encryption KMS keys (SYMMETRIC_DEFAULT), HMAC KMS keys of different lengths, KMS keys for RSA keys of different lengths, and elliptic curve keys with different curves. For details, see [Key spec](#).

Key type

Where: Cryptographic configuration tab

Indicates whether the KMS key is **Symmetric** or **Asymmetric**.

Key usage

Where: Cryptographic configuration tab

Indicates whether a KMS key can be used for **Encrypt and decrypt**, **Sign and verify** or **Generate and verify MAC**. For details, see [Key usage](#).

Origin

Where: Cryptographic configuration tab

The source of the key material for the KMS key. Valid values are:

- **Amazon KMS** for key material that Amazon KMS generates
- **Amazon CloudHSM** for KMS keys in [Amazon CloudHSM key store](#)
- **External** for [imported key material](#) (BYOK)
- **External key store** for KMS keys in an [external key store](#)

MAC algorithms

Where: Cryptographic configuration tab

Lists the MAC algorithms that can be used with an HMAC KMS key in Amazon KMS. This field appears only when the **Key spec** is an HMAC key spec (HMAC_*). For information about the MAC algorithms that Amazon KMS supports, see [Key specs for HMAC KMS keys](#).

Primary key

Where: Regionality tab

Indicates that this KMS key is a [multi-Region primary key](#). Authorized users can use this section to [change the primary key](#) to a different related multi-Region key. This field appears only when the KMS key is a multi-Region primary key.

Public key

Where: Public key tab

Displays the public key of an asymmetric KMS key. Authorized users can use this tab to [copy and download the public key](#).

Regionality

Where: General configuration section and Regionality tabs

Indicates whether a KMS key is a single-Region key, a [multi-Region primary key](#), or a [multi-Region replica key](#). This field appears only when the KMS key is a multi-Region key.

Related multi-Region keys

Where: Regionality tab

Displays all related [multi-Region primary and replica keys](#), except for the current KMS key. This field appears only when the KMS key is a multi-Region key.

In the **Related multi-Region keys** section of a primary key, authorized users can [create new replica keys](#).

Replica key

Where: Regionality tab

Indicates that this KMS key is a [multi-Region replica key](#). This field appears only when the KMS key is a multi-Region replica key.

Signing algorithms

Where: Cryptographic configuration tab

Lists the signing algorithms that can be used with the KMS key in Amazon KMS. This field appears only when the **Key type** is **Asymmetric** and the **Key usage** is **Sign and verify**. For information about the signing algorithms that Amazon KMS supports, see [RSA key specs for signing and verification](#) and [Elliptic curve key specs](#).

Status

Where: General configuration section

The key state of the KMS key. You can use the KMS key in [cryptographic operations](#) only when the status is **Enabled**. For a detailed description of each KMS key status and its effect on the operations that you can run on the KMS key, see [Key states of Amazon KMS keys](#).

Tags

Where: Tags tab

Optional key-value pairs that describe the KMS key. To add or change the tags for a KMS key, on the **Tags** tab, choose **Edit**.

When you add tags to your Amazon resources, Amazon generates a cost allocation report with usage and costs aggregated by tags. Tags can also be used to control access to a KMS key. For information about tagging KMS keys, see [Tags in Amazon KMS](#) and [ABAC for Amazon KMS](#).

Using the Amazon KMS API

The [DescribeKey](#) operation returns details about the specified KMS key. To identify the KMS key, use the [key ID](#), [key ARN](#), [alias name](#), or [alias ARN](#).

Unlike the [ListKeys](#) operation, which displays only KMS keys in the caller's account and Region, authorized users can use the DescribeKey operation to get details about KMS keys in other accounts.

Note

The DescribeKey response includes both KeySpec and CustomerMasterKeySpec members with the same values. The CustomerMasterKeySpec member is deprecated.

For example, this call to DescribeKey returns information about a symmetric encryption KMS key. The fields in the response vary with the [Amazon KMS key spec](#), [key state](#), and the [key material origin](#). For examples in multiple programming languages, see [Use DescribeKey with an Amazon SDK or CLI](#).

```
$ aws kms describe-key --key-id 1234abcd-12ab-34cd-56ef-1234567890ab

{
  "KeyMetadata": {
    "Origin": "AWS_KMS",
    "KeyId": "1234abcd-12ab-34cd-56ef-1234567890ab",
```

```

    "Description": "",
    "KeyManager": "CUSTOMER",
    "Enabled": true,
    "KeySpec": "SYMMETRIC_DEFAULT",
    "CustomerMasterKeySpec": "SYMMETRIC_DEFAULT",
    "KeyUsage": "ENCRYPT_DECRYPT",
    "KeyState": "Enabled",
    "CreationDate": 1499988169.234,
    "MultiRegion": false,
    "Arn": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab",
    "AWSAccountId": "111122223333",
    "EncryptionAlgorithms": [
        "SYMMETRIC_DEFAULT"
    ]
}
}

```

This example calls `DescribeKey` operation on an asymmetric KMS key used for signing and verification. The response includes the signing algorithms that Amazon KMS supports for this KMS key.

```

$ aws kms describe-key --key-id 0987dcba-09fe-87dc-65ba-ab0987654321

{
  "KeyMetadata": {
    "KeyId": "0987dcba-09fe-87dc-65ba-ab0987654321",
    "Origin": "AWS_KMS",
    "Arn": "arn:aws:kms:us-west-2:111122223333:key/0987dcba-09fe-87dc-65ba-
ab0987654321",
    "KeyState": "Enabled",
    "KeyUsage": "SIGN_VERIFY",
    "CreationDate": 1569973196.214,
    "Description": "",
    "KeySpec": "ECC_NIST_P521",
    "CustomerMasterKeySpec": "ECC_NIST_P521",
    "AWSAccountId": "111122223333",
    "Enabled": true,
    "MultiRegion": false,
    "KeyManager": "CUSTOMER",
    "SigningAlgorithms": [
        "ECDSA_SHA_512"
    ]
  }
}

```

```
}  
}
```

Identify different key types

The following topics explain how to identify different key types in the Amazon KMS console and [DescribeKey](#) responses.

For help navigating to the **Cryptographic configuration** tab on the details page for a KMS key, see [the section called “Access and list KMS key details”](#).

Topics

- [Identify asymmetric KMS keys](#)
- [Identify HMAC KMS keys](#)
- [Identify multi-Region KMS keys](#)
- [Identify KMS keys with imported key material](#)
- [Identify KMS keys in Amazon CloudHSM key stores](#)
- [Identify KMS keys in external key stores](#)

Identify asymmetric KMS keys

In the Amazon KMS console

The **Key type** column of the **Customer managed keys** table shows whether each KMS key is symmetric or asymmetric. You can filter the table by the **Key type** value to display only asymmetric KMS keys. For more information see [the section called “Sort and filter your KMS keys”](#).

The **Cryptographic configuration** tab on the details page for a KMS key displays the **Key Type**, which indicates whether the key is symmetric or asymmetric. It also displays the **Key Usage**, which indicates whether your asymmetric KMS key is used for encryption and decryption, signing and verification, or deriving shared secrets.

In DescribeKey responses

When you call the `DescribeKey` operation on an asymmetric KMS key the response includes the `KeySpec` and `KeyUsage` values, which can be used to determine if a KMS key is symmetric or asymmetric.

If the `KeySpec` value is `SYMMETRIC_DEFAULT`, the key is a symmetric encryption KMS key. For details on asymmetric key specs, see [Key spec reference](#).

If the `KeyUsage` value is `SIGN_VERIFY` or `KEY_AGREEMENT`, the key is an asymmetric KMS key.

The `DescribeKey` operation also returns the following details for asymmetric KMS keys.

- For asymmetric KMS keys with a `KeyUsage` value of `ENCRYPT_DECRYPT`, the operation returns the `EncryptionAlgorithms`, which lists the valid encryption algorithms for the key.
- For asymmetric KMS keys with a `KeyUsage` value of `SIGN_VERIFY`, the operation returns the `SigningAlgorithms`, which lists the valid signing algorithms for the key.
- For asymmetric KMS keys with a `KeyUsage` value of `KEY_AGREEMENT`, the operation returns the `KeyAgreementAlgorithms`, which lists the valid key agreement algorithms for the key.

For more information on asymmetric KMS keys, see [the section called “Asymmetric keys”](#).

Identify HMAC KMS keys

In the Amazon KMS console

HMAC KMS keys are included in the **Customer managed keys** table, but you cannot sort or filter this table by the key spec or key usage values that identify HMAC keys. To make it easier to find your HMAC keys, assign them a distinctive alias or tag. Then you can sort or filter by the alias or tag.

The **Cryptographic configuration** tab on the details page for a KMS key displays the **Key Type**, which indicates whether the key is symmetric or asymmetric. HMAC KMS keys are symmetric. The **Cryptographic configuration** tab also displays the **Key Usage**. For HMAC KMS keys the key usage value is always **Generate and verify MAC**.

In `DescribeKey` responses

When you call the `DescribeKey` operation on an HMAC KMS key the response includes the `KeySpec` and `KeyUsage` values. For HMAC KMS keys the key usage value is always `GENERATE_VERIFY_MAC` and the key spec value always starts with `HMAC_`.

For more information on HMAC KMS keys, see [the section called “HMAC keys”](#).

Identify multi-Region KMS keys

In the Amazon KMS console

The **Customer managed keys** table only displays KMS keys in the selected Region. You can view multi-Region primary and replica keys in the selected Region. To change the Amazon Region, use the Region selector in the upper-right corner of the console.

To make it easier to identify multi-Region keys in the **Customer managed keys** table, add the **Regionality** column to your table. For help, see [the section called “Customize your KMS key tables”](#).

The detail page for multi-Region KMS keys includes a **Regionality** tab. The **Regionality** tab for a primary key includes Change primary Region and Create new replica keys buttons. (The Regionality tab for a replica key has neither button.) The **Related multi-Region keys** section lists all multi-Region keys related to the current one. If the current key is a replica key, this list includes the primary key.

If you choose a related multi-Region key from the **Related multi-Region keys** table, the Amazon KMS console changes to the Region of the selected key and it opens the detail page for the key. For example, if you choose the replica key in the sa-east-1 Region from the example **Related multi-Region keys** section below, the Amazon KMS console changes to the sa-east-1 Region to display the detail page for that replica key. You might do this to view the alias or key policy for the replica key. To change the Region again, use the Region selector at the top right corner of the page.

In DescribeKey responses

By default, Amazon KMS API operations are Regional and only return the resources in the current or specified Region. But, when you call the DescribeKey operation on a multi-Region KMS key, the response includes all related multi-Region keys in other Amazon Regions in the MultiRegionConfiguration element.

For more information on multi-Region KMS keys, see [the section called “Multi-Region keys”](#).

Identify KMS keys with imported key material

In the Amazon KMS console

To make it easier to identify KMS keys with imported key material in the **Customer managed keys** table, add the **Origin** column to your table. The **Origin** column makes it easy to identify KMS keys with an **External (Import Key material)** origin property value. For help, see [the section called “Customize your KMS key tables”](#).

The **Cryptographic configuration** tab on the details page for a KMS key displays the **Origin**, which identifies the source of the key material for the KMS key. For KMS keys with imported key material, the origin value is always **External (Import Key material)**. The details page also includes a **Key material** tab that provides detailed information about the imported key material. The **Key material** tab only appears on the detail page for KMS keys with imported key material.

In DescribeKey responses

When you call the DescribeKey operation on a KMS key with imported key material the response includes the Origin, ExpirationModel, and ValidTo values. For KMS keys with imported key material the origin value is always EXTERNAL. The ExpirationModel value indicates whether or not the key material is set to expire, and the ValidTo value indicates when the key material will expire. For more information, see [the section called “Setting an expiration time \(optional\)”](#).

For more information on KMS keys with imported key material, see [the section called “Imported key material”](#).

Identify KMS keys in Amazon CloudHSM key stores

In the Amazon KMS console

To make it easier to identify KMS keys in Amazon CloudHSM key stores in the **Customer managed keys** table, add the **Origin** column to your table. The **Origin** column makes it easy to identify KMS keys with an **Amazon CloudHSM** origin property value. For help, see [the section called “Customize your KMS key tables”](#).

The **Cryptographic configuration** tab on the details page for a KMS key displays the **Origin**, which identifies the source of the key material for the KMS key. For KMS keys in Amazon CloudHSM key stores, the origin value is always **Amazon CloudHSM**.

For a KMS key in an Amazon CloudHSM key store, the **Cryptographic configuration** tab includes an additional section, **Custom key store**, that provides information about the Amazon CloudHSM key store and Amazon CloudHSM cluster associated with the KMS key.

In DescribeKey responses

When you call the DescribeKey operation on a KMS key in an Amazon CloudHSM key store the response includes the `Origin`, which identifies the source of the key material. For KMS keys in an Amazon CloudHSM key store the origin value is always `AWS_CLOUDHSM`. The operation also returns the following special fields for KMS keys in Amazon CloudHSM key stores:

- `CloudHsmClusterId`
- `CustomKeyStoreId`

For more information on Amazon CloudHSM key stores, see [the section called “Amazon CloudHSM key stores”](#).

Identify KMS keys in external key stores

In the Amazon KMS console

To make it easier to identify KMS keys in external key stores in the **Customer managed keys** table, add the **Origin** column to your table. The **Origin** column makes it easy to identify KMS keys with an **External key store** origin property value. For help, see [the section called “Customize your KMS key tables”](#).

The **Cryptographic configuration** tab on the details page for a KMS key displays the **Origin**, which identifies the source of the key material for the KMS key. For KMS keys in external key stores, the origin value is always **External key store**.

For a KMS key in an external key store, the **Cryptographic configuration** tab includes two additional sections, **Custom key store** and **External key**. The **Custom key store** table provides information about the external key store associated with the KMS key. The **External key** table appears in the Amazon KMS console only for KMS keys in external key stores. It provides information about the external key associated with the KMS key. The [external key](#) is a cryptographic key outside of Amazon that serves as the key material for the KMS key in the external key store. When you encrypt or decrypt with the KMS key, the operation is performed by your [external key manager](#) using the specified external key.

The following values appear in the **External key** section.

External key ID

The identifier for the external key in its external key manager. This is the value that the external key store proxy uses to identify the external key. You specify the ID of the external key when you create the KMS key and you cannot change it. If the external key ID value that you used to create the KMS key changes or becomes invalid, you must [schedule the KMS key for deletion](#) and [create a new KMS key](#) with the correct external key ID value.

In DescribeKey responses

When you call the DescribeKey operation on a KMS key in an external key store the response includes the `Origin`, which identifies the source of the key material. For KMS keys in an Amazon CloudHSM key store the origin value is always `EXTERNAL_KEY_STORE`. The operation also returns the `CustomKeyId` element, which identifies the external key store associated with the KMS keys.

For more information on external key stores, see [the section called “External key stores”](#).

Customize your console view

You can customize the view of the Amazon KMS console to make it easier to find your KMS keys. Customize the tables that appear on the **Amazon managed keys** and **Customer managed keys** pages to display the information that you need the most, or sort and filter the KMS keys returned in the tables.

Topics

- [Sort and filter your KMS keys](#)
- [Customize your KMS key tables](#)

Sort and filter your KMS keys

To make it easier to find your KMS keys in the console, you can sort and filter the key tables.

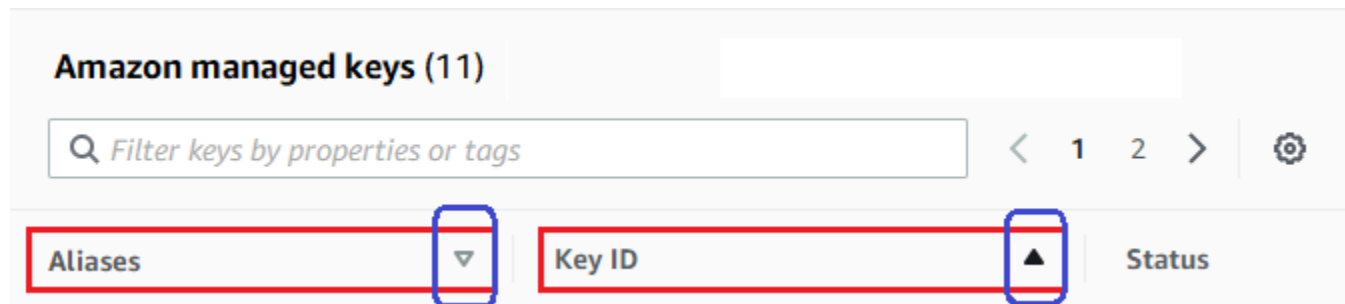
Sort

You can sort KMS keys in ascending or descending order by their column values. This feature sorts all KMS keys in the table, even if they don't appear on the current table page.

Sortable columns are indicated by an arrow beside the column name. On the **Amazon managed keys** page, you can sort by **Aliases** or **Key ID**. On the **Customer managed keys** page, you can sort by **Aliases**, **Key ID**, or **Key type**.

To sort in ascending order, choose the column heading until the arrow points upward. To sort in descending order, choose the column heading until the arrow points downward. You can sort by only one column at a time.

For example, you can sort KMS keys in ascending order by key ID, instead of aliases, which is the default.



When you sort KMS keys on the **Customer managed keys** page in ascending order by **Key type**, all asymmetric keys are displayed before all symmetric keys.

Filter

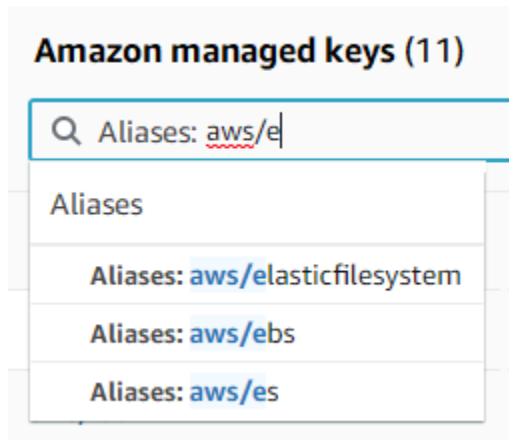
You can filter KMS keys by their property values or tags. The filter applies to all KMS keys in the table, even if they don't appear on the current table page. The filter is not case-sensitive.

Filterable properties are listed in the filter box. On the **Amazon managed keys** page, you can filter by alias and key ID. On the **Customer managed keys** page, you can filter by the alias, key ID, and key type properties, and by tags.

- On the **Amazon managed keys** page, you can filter by alias and key ID.
- On the **Customer managed keys** page, you can filter by tags, or by the alias, key ID, key type, or regionality properties.

To filter by a property value, choose the filter, choose the property name, and then choose from the list of actual property values. To filter by a tag, choose the tag key, and then choose from the list of actual tag values. After choosing a property or tag key, you can also type all or part of the property value or tag value. You'll see a preview of the results before you make your choice.

For example, to display KMS keys with an alias name that contains aws/e, choose the filter box, choose **Alias**, type aws/e, and then press Enter or Return to add the filter.



Suggested KMS key table filters

Filter for asymmetric KMS keys

To display only asymmetric KMS keys on the **Customer managed keys** page, click the filter box, choose **Key type** and then choose **Key type: Asymmetric**. The **Asymmetric** option appears only when you have asymmetric KMS keys in the table.

Filter for multi-Region keys

To display only multi-Region keys, on the **Customer managed keys** page, choose the filter box, choose **Regionality** and then choose **Regionality: Multi-Region**. The **Multi-Region** option appears only when you have multi-Region keys in the table.

Filter for tags

To display only KMS keys with a particular tag, choose the filter box, choose the tag key, and then choose from among the actual tag values. You can also type all or part of the tag value.

The resulting table displays all KMS keys with the chosen tag. However, it doesn't display the tag. To see the tag, choose the key ID or alias of the KMS key and on its detail page, choose the **Tags** tab. The tabs appear below the **General configuration** section.

This filter requires both the tag key and tag value. It won't find KMS keys by typing only the tag key or only its value. To filter tags by all or part of the tag key or value, use the [ListResourceTags](#) operation to get tagged KMS keys, then use the filtering features of your programming language.

Filter by text

To search for text, in the filter box, type all or part of an alias, key ID, key type, or tag key. (After you select the tag key, you can search for a tag value). You'll see a preview of the results before you make your choice.

For example, to display KMS keys with `test` in its tag keys or filterable properties, type `test` in the filter box. The preview shows the KMS keys that the filter will select. In this case, `test` appears only in the **Alias** property.

Customize your KMS key tables

You can customize the tables that appear on the **Amazon managed keys** and **Customer managed keys** pages in the Amazon Web Services Management Console to suit your needs. You can choose the table columns, the number of Amazon KMS keys on each page (**Page size**), and the text wrap. The configuration you choose is saved when you confirm it and reapplied whenever you open the pages.

To customize your KMS key tables

1. On the **Amazon managed keys** or **Customer managed keys** page, choose the settings icon



in the upper-right corner of the page.

2. On the **Preferences** page, choose your preferred settings, and then choose **Confirm**.

Consider using the **Page size** setting to increase the number of KMS keys displayed on each page, especially if you typically use a device that's easy to scroll.

The data columns that you display might vary depending on the table, your job role, and the types of KMS keys in the account and Region. The following table offers some suggested configurations. For descriptions of the columns, see [Using the Amazon KMS console](#).

Suggested KMS key table configurations

You can customize the columns that appear in your KMS key table to display the information you need about your KMS keys.

Amazon managed keys

By default, the **Amazon managed key** table displays the **Aliases**, **Key ID**, and **Status** columns. These columns are ideal for most use cases.

Symmetric encryption KMS keys

If you use only symmetric encryption KMS keys with key material generated by Amazon KMS, the **Aliases**, **Key ID**, **Status**, and **Creation date** columns are likely to be the most useful.

Asymmetric KMS keys

If you use asymmetric KMS keys, in addition to the **Aliases**, **Key ID**, and **Status** columns, consider adding the **Key type**, **Key spec**, and **Key usage** columns. These columns will show you whether a KMS key is symmetric or asymmetric, the type of key material, and whether the KMS key can be used for encryption or signing.

HMAC KMS keys

If you use HMAC KMS keys, in addition to the **Aliases**, **Key ID**, and **Status** columns, consider adding the **Key spec** and **Key usage** columns. These columns will show you whether a KMS key is an HMAC key. Because you can't sort KMS keys by key spec or key usage, use aliases and tags to identify your HMAC keys and then use the [filter features](#) of the Amazon KMS console to filter by aliases or tags.

Imported key material

If you have KMS keys with [imported key material](#), consider adding the **Origin** and **Expiration date** columns. These columns will show you whether the key material in a KMS key is imported or generated by Amazon KMS and when the key material expires, if at all. The **Creation date** field displays the date that the KMS key was created (without key material). It doesn't reflect any characteristic of the key material.

Keys in custom key stores

If you have KMS keys in [custom key stores](#), consider adding the **Origin** and **Custom key store ID** columns. These columns show that the KMS key is in a custom key store, display the custom key store type, and identify the custom key store.

Multi-Region keys

If you have [multi-Region keys](#), consider adding the **Regionality** column. This shows whether a KMS key is a single-Region key, a [multi-Region primary key](#) or a [multi-Region replica key](#).

Find KMS keys and key material in an Amazon CloudHSM key store

If you manage an Amazon CloudHSM key store, you might need to identify the KMS keys in each Amazon CloudHSM key store. For example, you might need to do some of the following tasks.

- Track the KMS keys in Amazon CloudHSM key store in Amazon CloudTrail logs.
- Predict the effect on KMS keys of disconnecting an Amazon CloudHSM key store.
- Schedule deletion of KMS keys before you delete an Amazon CloudHSM key store.

In addition, you might want to identify the keys in your Amazon CloudHSM cluster that serve as key material for your KMS keys. Although Amazon KMS manages the KMS keys and the key material, you still retain control of and responsibility for the management of your Amazon CloudHSM cluster, as well as the HSMs and backups and the keys in the HSMs. You might need to identify the keys in order to audit the key material, protect it from accidental deletion, or delete it from HSMs and cluster backups after deleting the KMS key.

All key material for the KMS keys in your Amazon CloudHSM key store is owned by the [kmsuser crypto user](#) (CU). Amazon KMS sets the key label attribute, which is viewable only in Amazon CloudHSM, to the Amazon Resource Name (ARN) of the KMS key.

To find KMS keys and key material, use any of the following techniques.

- [Find the KMS keys in an Amazon CloudHSM key store](#) — How to identify the KMS keys in one or all of your Amazon CloudHSM key stores.
- [Find all keys for an Amazon CloudHSM key store](#) — How to find all keys in your cluster that serve as key material for the KMS keys in your Amazon CloudHSM key store.
- [Find the Amazon CloudHSM key for a KMS key](#) — How to find the key in your cluster that serves as key material for a particular KMS key in your Amazon CloudHSM key store.
- [Find the KMS key for an Amazon CloudHSM key](#) — How to find the KMS key for a particular key in your cluster.

Find the KMS keys in an Amazon CloudHSM key store

If you manage an Amazon CloudHSM key store, you might need to identify the KMS keys in each Amazon CloudHSM key store. You can use this information to track the KMS key operations in

Amazon CloudTrail logs, predict the effect of disconnecting a custom key store on KMS keys, or schedule deletion of KMS keys before you delete an Amazon CloudHSM key store.

To find the KMS keys in an Amazon CloudHSM key store (console)

To find the KMS keys in a particular Amazon CloudHSM key store, on the **Customer managed keys** page, view the values in the **Custom Key Store Name** or **Custom Key Store ID** fields. To identify KMS keys in any Amazon CloudHSM key store, look for KMS keys with an **Origin** value of **Amazon CloudHSM**. To add optional columns to the display, choose the gear icon in the upper right corner of the page.

To find the KMS keys in an Amazon CloudHSM key store (API)

To find the KMS keys in an Amazon CloudHSM key store, use the [ListKeys](#) and [DescribeKey](#) operations and then filter by CustomKeyStoreId value. Before running the following examples, replace the fictitious custom key store ID values with a valid value.

Bash

To find KMS keys in a particular Amazon CloudHSM key store, get all of your KMS keys in the account and Region. Then filter by the custom key store ID.

```
for key in $(aws kms list-keys --query 'Keys[*].KeyId' --output text) ;  
do aws kms describe-key --key-id $key |  
grep '"CustomKeyStoreId": "cks-1234567890abcdef0"' --context 100; done
```

To get KMS keys in any Amazon CloudHSM key store in the account and Region, search for CustomKeyStoreType with a value of AWS_CloudHSM.

```
for key in $(aws kms list-keys --query 'Keys[*].KeyId' --output text) ;  
do aws kms describe-key --key-id $key |  
grep '"CustomKeyStoreType": "AWS_CloudHSM"' --context 100; done
```

PowerShell

To find KMS keys in a particular Amazon CloudHSM key store, use the [Get-KmsKeyList](#) and [Get-KmsKey](#) cmdlets to get all of your KMS keys in the account and Region. Then filter by the custom key store ID.

```
PS C:\> Get-KMSKeyList | Get-KMSKey | where CustomKeyStoreId -eq  
'cks-1234567890abcdef0'
```

To get KMS keys in any Amazon CloudHSM key store in the account and Region, filter for the `CustomKeyStoreType` value of `AWS_CLOUDHSM`.

```
PS C:\> Get-KMSKeyList | Get-KMSKey | where CustomKeyStoreType -eq 'AWS_CLOUDHSM'
```

Find all keys for an Amazon CloudHSM key store

You can identify the keys in your Amazon CloudHSM cluster that serve as key material for your Amazon CloudHSM key store. To do that, use the [key list](#) command in CloudHSM CLI.

You can also use the **key list** command to find the Amazon KMS for an Amazon CloudHSM key. When Amazon KMS creates the key material for a KMS key in your Amazon CloudHSM cluster, it writes the Amazon Resource Name (ARN) of the KMS key in the key label. The **key list** command returns the `key-reference` and the `label`.

Notes

The following procedures use the Amazon CloudHSM Client SDK 5 command line tool, [CloudHSM CLI](#). The CloudHSM CLI replaces `key-handle` with `key-reference`.

On January 1, 2025, Amazon CloudHSM will end support for the Client SDK 3 command line tools, the CloudHSM Management Utility (CMU) and the Key Management Utility (KMU). For more information on the differences between the Client SDK 3 command line tools and the Client SDK 5 command line tool, see [Migrate from Client SDK 3 CMU and KMU to Client SDK 5 CloudHSM CLI](#) in the *Amazon CloudHSM User Guide*.

To run this procedure you need to disconnect the Amazon CloudHSM key store temporarily so you can log in as the `kmsuser` CU.

1. Disconnect the Amazon CloudHSM key store, if it is not already disconnected, then log in as `kmsuser`, as explained in [How to disconnect and log in](#).

Note

While a custom key store is disconnected, all attempts to create KMS keys in the custom key store or to use existing KMS keys in cryptographic operations will fail. This action can prevent users from storing and accessing sensitive data.

2. Use the [key list](#) command in CloudHSM CLI to find all keys for the current user present in your Amazon CloudHSM cluster.

By default, only 10 keys of the currently logged in user are displayed, and only the key-reference and label are displayed as output. For more options, see [key list](#) in the *Amazon CloudHSM User Guide*.

```
aws-cloudhsm > key list
{
  "error_code": 0,
  "data": {
    "matched_keys": [
      {
        "key-reference": "0x00000000000000123",
        "attributes": {
          "label": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab"
        }
      },
      {
        "key-reference": "0x00000000000000456",
        "attributes": {
          "label": "arn:aws:kms:us-west-2:111122223333:key/0987dcba-09fe-87dc-65ba-
ab0987654321"
        }
      },
      ...8 keys later...
    ],
    "total_key_count": 56,
    "returned_key_count": 10,
    "next_token": "10"
  }
}
```

3. Log out and reconnect the Amazon CloudHSM key store as described in [How to log out and reconnect](#).

Find the KMS key for an Amazon CloudHSM key

If you know the key reference or ID of a key that the kmsuser owns in the cluster, you can use that value to identify the associated KMS key in your Amazon CloudHSM key store.

When Amazon KMS creates the key material for a KMS key in your Amazon CloudHSM cluster, it writes the Amazon Resource Name (ARN) of the KMS key in the key label. Unless you have changed the label value, you can use the [key list](#) command in CloudHSM CLI to identify the KMS key associated with the Amazon CloudHSM key.

Notes

The following procedures use the Amazon CloudHSM Client SDK 5 command line tool, [CloudHSM CLI](#). The CloudHSM CLI replaces `key-handle` with `key-reference`.

On January 1, 2025, Amazon CloudHSM will end support for the Client SDK 3 command line tools, the CloudHSM Management Utility (CMU) and the Key Management Utility (KMU). For more information on the differences between the Client SDK 3 command line tools and the Client SDK 5 command line tool, see [Migrate from Client SDK 3 CMU and KMU to Client SDK 5 CloudHSM CLI](#) in the *Amazon CloudHSM User Guide*.

To run these procedures you need to disconnect the Amazon CloudHSM key store temporarily so you can log in as the `kmsuser` CU.

Note

While a custom key store is disconnected, all attempts to create KMS keys in the custom key store or to use existing KMS keys in cryptographic operations will fail. This action can prevent users from storing and accessing sensitive data.

Topics

- [Identify the KMS key associated with a key reference](#)
- [Identify the KMS key associated with a backing key ID](#)

Identify the KMS key associated with a key reference

The following procedures demonstrate how to use the [key list](#) command in CloudHSM CLI with the `key-reference` attribute filter to find the key in your cluster that serves as key material for a particular KMS key in your Amazon CloudHSM key store.

1. Disconnect the Amazon CloudHSM key store, if it is not already disconnected, then log in as `kmsuser`, as explained in [How to disconnect and log in](#).

2. Use the [key list](#) command in CloudHSM CLI to filter by the `key-reference` attribute. Specify the `verbose` argument to include all attributes and key information for the matched key. If you don't specify the `verbose` argument, the `key list` operation only returns the matched key's `key-reference` and `label` attribute.

Before running this command, replace the example `key-reference` with a valid one from your account.

```
aws-cloudhsm > key list --filter attr.key-reference="0x0000000000120034" --verbose
{
  "error_code": 0,
  "data": {
    "matched_keys": [
      {
        "key-reference": "0x0000000000120034",
        "key-info": {
          "key-owners": [
            {
              "username": "kmsuser",
              "key-coverage": "full"
            }
          ],
          "shared-users": [],
          "cluster-coverage": "full"
        },
        "attributes": {
          "key-type": "aes",
          "label": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab",
          "id": "0xbacking-key-id",
          "check-value": "0x29bbd1",
          "class": "my_test_key",
          "encrypt": true,
          "decrypt": true,
          "token": true,
          "always-sensitive": true,
          "derive": false,
          "destroyable": true,
          "extractable": false,
          "local": true,
          "modifiable": true,
          "never-extractable": false,
          "private": true,
```

```
        "sensitive": true,  
        "sign": false,  
        "trusted": false,  
        "unwrap": true,  
        "verify": false,  
        "wrap": true,  
        "wrap-with-trusted": false,  
        "key-length-bytes": 32  
    }  
}  
],  
"total_key_count": 1,  
"returned_key_count": 1  
}  
}
```

3. Log out and reconnect the Amazon CloudHSM key store as described in [How to log out and reconnect](#).

Identify the KMS key associated with a backing key ID

All CloudTrail log entries for cryptographic operations with a KMS key in an Amazon CloudHSM key store include an `additionalEventData` field with the `customKeyStoreId` and `backingKeyId`. The value returned in the `backingKeyId` field correlates to the CloudHSM key `id` attribute. You can filter the [key list](#) operation by the `id` attribute to identify the KMS key associated with a specific `backingKeyId`.

1. Disconnect the Amazon CloudHSM key store, if it is not already disconnected, then log in as `kmsuser`, as explained in [How to disconnect and log in](#).
2. Use the [key list](#) command in CloudHSM CLI with the attribute filter to find the key in your cluster that serves as key material for a particular KMS key in your Amazon CloudHSM key store.

The following example demonstrates how to filter by the `id` attribute. Amazon CloudHSM recognizes the `id` value as a hexadecimal value. To filter the **key list** operation by the `id` attribute, you must first convert the `backingKeyId` value that you identified in your CloudTrail log entry into a format that Amazon CloudHSM recognizes.

- a. Use the following Linux command to convert the `backingKeyId` into a hexadecimal representation.

```
echo backingKeyId | tr -d '\n' | xxd -p
```

The following example demonstrates how to convert the `backingKeyId` byte array into a hexadecimal representation.

```
echo 5890723622dc15f699aa9ab2387a9f744b2b884c18b2186ee8ada4f556a2eb9d | tr -d
'\n' | xxd -p
353839303732333632326463313566363939616139616232333837613966373434623262383834633138623
```

- b. Prepend the hexadecimal representation of the `backingKeyId` with `0x`.

```
0x353839303732333632326463313566363939616139616232333837613966373434623262383834633138623
```

- c. Use the converted `backingKeyId` value to filter by the `id` attribute. Specify the `verbose` argument to include all attributes and key information for the matched key. If you don't specify the `verbose` argument, the `key list` operation only returns the matched key's key-reference and label attribute.

```
aws-cloudhsm > key list --filter
attr.id="0x353839303732333632326463313566363939616139616232333837613966373434623262383834633138623"
--verbose
{
  "error_code": 0,
  "data": {
    "matched_keys": [
      {
        "key-reference": "0x0000000000120034",
        "key-info": {
          "key-owners": [
            {
              "username": "kmsuser",
              "key-coverage": "full"
            }
          ],
          "shared-users": [],
          "cluster-coverage": "full"
        },
        "attributes": {
          "key-type": "aes",
          "label": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab",
```

```

    "id":
      "0x35383930373233363232646331356636393961613961623233383761396637343462326238383463313
      "check-value": "0x29bbd1",
      "class": "my_test_key",
      "encrypt": true,
      "decrypt": true,
      "token": true,
      "always-sensitive": true,
      "derive": false,
      "destroyable": true,
      "extractable": false,
      "local": true,
      "modifiable": true,
      "never-extractable": false,
      "private": true,
      "sensitive": true,
      "sign": false,
      "trusted": false,
      "unwrap": true,
      "verify": false,
      "wrap": true,
      "wrap-with-trusted": false,
      "key-length-bytes": 32
    }
  ],
  "total_key_count": 1,
  "returned_key_count": 1
}

```

3. Log out and reconnect the Amazon CloudHSM key store as described in [How to log out and reconnect](#).

Find the Amazon CloudHSM key for a KMS key

You can use the KMS key ID of a KMS key in an Amazon CloudHSM key store to identify the key in your Amazon CloudHSM cluster that serves as its key material.

When Amazon KMS creates the key material for a KMS key in your Amazon CloudHSM cluster, it writes the Amazon Resource Name (ARN) of the KMS key in the key label. Unless you have changed

the label value, you can use the [key list](#) command in CloudHSM CLI to find the key-resource and id of the key material for the KMS key.

All CloudTrail log entries for cryptographic operation with a KMS key in an Amazon CloudHSM key store include an additional `EventData` field with the `customKeyId` and `backingKeyId`. The value returned in the `backingKeyId` field is the `id` Amazon CloudHSM key attribute. You can filter the **key list** Amazon CloudHSM CLI operation by KMS key ARN to identify the CloudHSM key `id` attribute associated with a specific KMS key.

To run this procedure, you need to disconnect the Amazon CloudHSM key store temporarily so you can log in as the `kmsuser` CU.

Notes

The following procedures use the Amazon CloudHSM Client SDK 5 command line tool, [CloudHSM CLI](#). The CloudHSM CLI replaces `key-handle` with `key-reference`.

On January 1, 2025, Amazon CloudHSM will end support for the Client SDK 3 command line tools, the CloudHSM Management Utility (CMU) and the Key Management Utility (KMU). For more information on the differences between the Client SDK 3 command line tools and the Client SDK 5 command line tool, see [Migrate from Client SDK 3 CMU and KMU to Client SDK 5 CloudHSM CLI](#) in the *Amazon CloudHSM User Guide*.

1. Disconnect the Amazon CloudHSM key store, if it is not already disconnected, then log in as `kmsuser`, as explained in [How to disconnect and log in](#).

Note

While a custom key store is disconnected, all attempts to create KMS keys in the custom key store or to use existing KMS keys in cryptographic operations will fail. This action can prevent users from storing and accessing sensitive data.

2. Use the [key list](#) command in CloudHSM CLI and filter by `label` to find the KMS key for a particular key in your Amazon CloudHSM cluster. Specify the `verbose` argument to include all attributes and key information for the matched key. If you don't specify the `verbose` argument, the **key list** operation only returns the matched key's key-reference and label attributes.

The following example demonstrates how to filter by the `label` attribute that stores the KMS key ARN. Before running this command, replace the example KMS key ARN with a valid one from your account.

```
aws-cloudhsm > key list --filter attr.label="arn:aws:kms:us-  
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab" --verbose  
{  
  "error_code": 0,  
  "data": {  
    "matched_keys": [  
      {  
        "key-reference": "0x00000000000120034",  
        "key-info": {  
          "key-owners": [  
            {  
              "username": "kmsuser",  
              "key-coverage": "full"  
            }  
          ],  
          "shared-users": [],  
          "cluster-coverage": "full"  
        },  
        "attributes": {  
          "key-type": "aes",  
          "label": "arn:aws:kms:us-  
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab",  
          "id": "0xbacking-key-id",  
          "check-value": "0x29bbd1",  
          "class": "my_test_key",  
          "encrypt": true,  
          "decrypt": true,  
          "token": true,  
          "always-sensitive": true,  
          "derive": false,  
          "destroyable": true,  
          "extractable": false,  
          "local": true,  
          "modifiable": true,  
          "never-extractable": false,  
          "private": true,  
          "sensitive": true,  
          "sign": false,
```



```
        "trusted": false,  
        "unwrap": true,  
        "verify": false,  
        "wrap": true,  
        "wrap-with-trusted": false,  
        "key-length-bytes": 32  
    }  
  ],  
  "total_key_count": 1,  
  "returned_key_count": 1  
}
```

3. Log out and reconnect the Amazon CloudHSM key store as described in [How to log out and reconnect](#).

Enable and disable keys

You can disable and re-enable customer managed keys. When you create a KMS key, it is enabled by default. If you disable a KMS key, it cannot be used in any [cryptographic operation](#) until you re-enable it.

Because it's temporary and easily undone, disabling a KMS key is a safe alternative to deleting a KMS key, an action that is destructive and irreversible. If you are considering deleting a KMS key, disable it first and set a [CloudWatch alarm](#) or similar mechanism to be certain that you'll never need to use the key to decrypt encrypted data.

When you disable a KMS key, it becomes unusable right away (subject to eventual consistency). However, resources encrypted with [data keys](#) protected by the KMS key are not affected until the KMS key is used again, such as to decrypt the data key. This issue affects Amazon Web Services services, many of which use data keys to protect your resources. For details, see [How unusable KMS keys affect data keys](#).

You cannot enable or disable [Amazon managed keys](#) or [Amazon owned keys](#). Amazon managed keys are permanently enabled for use by [services that use Amazon KMS](#). Amazon owned keys are managed solely by the service that owns them.

Note

Amazon KMS does not rotate the key material of customer managed keys while they are disabled. For more information, see [How key rotation works](#).

Using the Amazon KMS console

You can use the Amazon KMS console to enable and disable [customer managed keys](#).

1. Sign in to the Amazon Web Services Management Console and open the Amazon Key Management Service (Amazon KMS) console at <https://console.amazonaws.cn/kms>.
2. To change the Amazon Web Services Region, use the Region selector in the upper-right corner of the page.
3. In the navigation pane, choose **Customer managed keys**.
4. Choose the check box for the KMS keys that you want to enable or disable.

5. To enable a KMS key, choose **Key actions, Enable**. To disable a KMS key, choose **Key actions, Disable**.

Using the Amazon KMS API

The [EnableKey](#) operation enables a disabled Amazon KMS key. These examples use the [Amazon Command Line Interface \(Amazon CLI\)](#), but you can use any supported programming language. The `key-id` parameter is required.

This operation does not return any output. To see the key status, use the [DescribeKey](#) operation.

```
$ aws kms enable-key --key-id 1234abcd-12ab-34cd-56ef-1234567890ab
```

The [DisableKey](#) operation disables an enabled KMS key. The `key-id` parameter is required.

```
$ aws kms disable-key --key-id 1234abcd-12ab-34cd-56ef-1234567890ab
```

This operation does not return any output. To see the key status, use the [DescribeKey](#) operation, and see the `Enabled` field.

```
$ aws kms describe-key --key-id 1234abcd-12ab-34cd-56ef-1234567890ab
{
  "KeyMetadata": {
    "Origin": "AWS_KMS",
    "KeyId": "1234abcd-12ab-34cd-56ef-1234567890ab",
    "Description": "",
    "KeyManager": "CUSTOMER",
    "MultiRegion": false,
    "Enabled": false,
    "KeyState": "Disabled",
    "KeyUsage": "ENCRYPT_DECRYPT",
    "CreationDate": 1502910355.475,
    "Arn": "arn:aws:kms:us-west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab",
    "AWSAccountId": "111122223333"
    "KeySpec": "SYMMETRIC_DEFAULT",
    "CustomerMasterKeySpec": "SYMMETRIC_DEFAULT",
    "EncryptionAlgorithms": [
      "SYMMETRIC_DEFAULT"
    ]
  }
}
```

```
}  
}
```

Rotate Amazon KMS keys

To create new cryptographic material for your [customer managed keys](#), you can create new KMS keys, and then change your applications or aliases to use the new KMS keys. Or, you can rotate the key material associated with an existing KMS key by enabling automatic key rotation or performing on-demand rotation.

By default, when you enable *automatic key rotation* for a KMS key, Amazon KMS generates new cryptographic material for the KMS key every year. You can also specify a custom [rotation-period](#) to define the number of days after you enable automatic key rotation that Amazon KMS will rotate your key material, and the number of days between each automatic rotation thereafter. If you need to immediately initiate key material rotation, you can perform *on-demand rotation*, regardless of whether or not automatic key rotation is enabled. On-demand rotations do not change existing automatic rotation schedules.

Amazon KMS saves all previous versions of the cryptographic material in perpetuity so you can decrypt any data encrypted with that KMS key. Amazon KMS does not delete any rotated key material until you [delete the KMS key](#). You can [track the rotation](#) of key material for your KMS keys in Amazon CloudWatch, Amazon CloudTrail, and the Amazon Key Management Service console. You can also use [GetKeyRotationStatus](#) operation to verify whether automatic rotation is enabled for a KMS key and identify any in progress on-demand rotations. You can use [ListKeyRotations](#) operation to view the details of completed rotations.

When you use a rotated KMS key to encrypt data, Amazon KMS uses the current key material. When you use the rotated KMS key to decrypt ciphertext, Amazon KMS uses the version of the key material that was used to encrypt it. You cannot select a particular version of the key material for decrypt operations, Amazon KMS automatically chooses the correct version. Because Amazon KMS transparently decrypts with the appropriate key material, you can safely use a rotated KMS key in applications and Amazon Web Services services without code changes.

However, automatic key rotation has no effect on the data that the KMS key protects. It does not rotate the [data keys](#) that the KMS key generated or re-encrypt any data protected by the KMS key, and it will not mitigate the effect of a compromised data key.

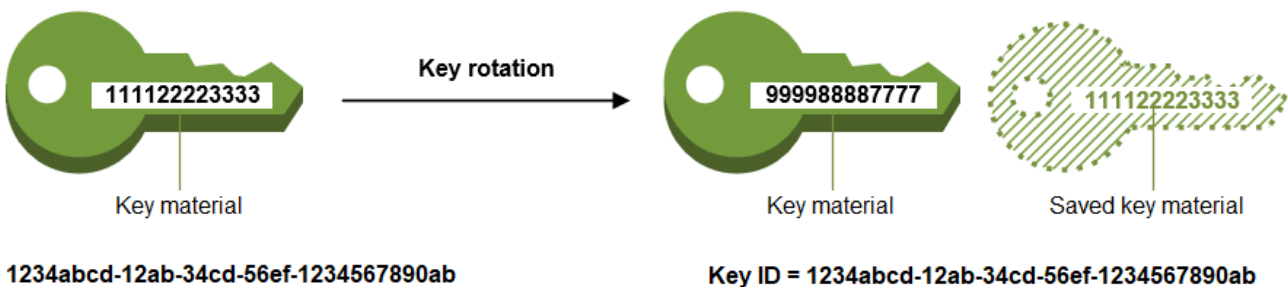
Amazon KMS supports automatic and on-demand key rotation only for [symmetric encryption KMS keys](#) with key material that Amazon KMS creates. Automatic rotation is optional for [customer managed KMS keys](#). Amazon KMS always rotates the key material for [Amazon managed KMS keys](#)

every year. Rotation of [Amazon owned KMS keys](#) is managed by the Amazon service that owns the key.

Note

The rotation period for Amazon managed keys changed in May 2022. For details, see [Amazon managed keys](#).

Key rotation changes only the *key material*, which is the cryptographic secret that is used in encryption operations. The KMS key is the same logical resource, regardless of whether or how many times its key material changes. The properties of the KMS key do not change, as shown in the following image.



You might decide to create a new KMS key and use it in place of the original KMS key. This has the same effect as rotating the key material in an existing KMS key, so it's often thought of as [manually rotating the key](#). Manual rotation is a good choice when you want to rotate KMS keys that are not eligible for automatic key rotation, including [asymmetric KMS keys](#), [HMAC KMS keys](#), KMS keys in [custom key stores](#), and KMS keys with [imported key material](#).

Key rotation and pricing

Amazon KMS charges a monthly fee for first and second rotation of key material maintained for your KMS key. This price increase is capped at the second rotation, and any subsequent rotations will not be billed. For details, see [Amazon Key Management Service Pricing](#).

Note

You can use the [Amazon Cost Explorer Service](#) to view a breakdown of your key storage charges. For example, you can filter your view to see the total charges for keys billed as current and rotated KMS keys by specifying \$REGION-KMS-Keys for the **Usage Type** and grouping the data by **API Operation**.

You might still see instances of the legacy Unknown API operation for historical dates.

Key rotation and quotas

Each KMS key counts as one key when calculating key resource quotas, regardless of the number of rotated key material versions.

For detailed information about key material and rotation, see [Amazon Key Management Service Cryptographic Details](#).

Topics

- [Why rotate KMS keys?](#)
- [How key rotation works](#)
- [Enable automatic key rotation](#)
- [Disable automatic key rotation](#)
- [Perform on-demand key rotation](#)
- [Rotate keys manually](#)
- [Change the primary key in a set of multi-Region keys](#)

Why rotate KMS keys?

Cryptographic best practices discourage extensive reuse of keys that encrypt data directly, such as the [data keys](#) that Amazon KMS generates. When 256-bit data keys encrypt millions of messages they can become exhausted and begin to produce ciphertext with subtle patterns that clever actors can exploit to discover the bits in the key. To avoid this key exhaustion, it's best to use data keys once, or just a few times, which effectively rotates the key material.

However, KMS keys are most often used as *wrapping keys*, also known as *key-encryption keys*. Instead of encrypting data, wrapping keys encrypt the data keys that encrypt your data. As such, they are used far less often than data keys, and are almost never reused enough to risk key exhaustion.

Despite this very low exhaustion risk, you might be required to rotate your KMS keys due to business or contract rules or government regulations. When you are compelled to rotate KMS keys, we recommend that you use automatic key rotation where it is supported, and manual key rotation when automatic key rotation is not supported.

You might consider performing on-demand rotations to demonstrate key material rotation capabilities or to validate automation scripts. We recommend using on-demand rotations for unplanned rotations, and using automatic key rotation with with a custom [rotation period](#) whenever possible.

How key rotation works

Key rotation in Amazon KMS is designed to be transparent and easy to use. Amazon KMS supports optional automatic and on-demand key rotation only for [customer managed keys](#).

Automatic key rotation

Amazon KMS rotates the KMS key automatically on the next rotation date defined by your rotation period. You don't need to remember or schedule the update.

On-demand rotation

Immediately initiate rotation of the key material associated with your KMS key, regardless of whether or not automatic key rotation is enabled.

Managing key material

Amazon KMS retains all key material for a KMS key, even if key rotation is disabled. Amazon KMS deletes key material only when you delete the KMS key.

Using key material

When you use a rotated KMS key to encrypt data, Amazon KMS uses the current key material. When you use the rotated KMS key to decrypt ciphertext, Amazon KMS uses the same version of the key material that was used to encrypt it. You cannot select a particular version of the key material for decrypt operations, Amazon KMS automatically chooses the correct version.

Rotation period

Rotation period defines the number of days after you enable automatic key rotation that Amazon KMS will rotate your key material, and the number of days between each automatic key rotation thereafter. If you do not specify a value for `RotationPeriodInDays` when you enable automatic key rotation, the default value is 365 days.

You can use the [kms:RotationPeriodInDays](#) condition key to further constrain the values that principals can specify in the `RotationPeriodInDays` parameter.

Rotation date

Amazon KMS automatically rotates the KMS key on the rotation date defined by your rotation period. The default rotation period is 365 days.

Customer managed keys

Because automatic key rotation is optional on [customer managed keys](#) and can be enabled and disabled at any time, the rotation date depends on the date that rotation was most recently enabled. The date can change if you modify the rotation period for a key that you previously enabled automatic key rotation on. The rotation date can change many times over the life of the key.

For example, if you create a customer managed key on January 1, 2022, and enable automatic key rotation with the default rotation period of 365 days on March 15, 2022, Amazon KMS rotates the key material on March 15, 2023, March 15, 2024, and every 365 days thereafter.

The following examples assume that automatic key rotation was enabled with the default rotation period of 365 days. These examples demonstrate special cases that might impact a key's rotation period.

- **Disable key rotation** — If you [disable automatic key rotation](#) at any point, the KMS key continues to use the version of the key material it was using when rotation was disabled. If you enable automatic key rotation again, Amazon KMS rotates the key material based on the new rotation-enable date.
- **Disabled KMS keys** — While a KMS key is disabled, Amazon KMS does not rotate it. However, the key rotation status does not change, and you cannot change it while the KMS key is disabled. When the KMS key is re-enabled, if the key material is past its last scheduled rotation date, Amazon KMS rotates it immediately. If the key material has not missed its last scheduled rotation date, Amazon KMS resumes the original key rotation schedule.
- **KMS keys pending deletion** — While a KMS key is pending deletion, Amazon KMS does not rotate it. The key rotation status is set to `false` and you cannot change it while deletion is pending. If deletion is canceled, the previous key rotation status is restored. If the key material is past its last scheduled rotation date, Amazon KMS rotates it immediately. If the key material has not missed its last scheduled rotation date, Amazon KMS resumes the original key rotation schedule.

Amazon managed keys

Amazon KMS automatically rotates Amazon managed keys every year (approximately 365 days). You cannot enable or disable key rotation for [Amazon managed keys](#).

The key material for an Amazon managed key is first rotated one year after its creation date, and every year (approximately 365 days from the last rotation) thereafter.

Note

In May 2022, Amazon KMS changed the rotation schedule for Amazon managed keys from every three years (approximately 1,095 days) to every year (approximately 365 days).

New Amazon managed keys are automatically rotated one year after they are created, and approximately every year thereafter.

Existing Amazon managed keys are automatically rotated one year after their most recent rotation, and every year thereafter.

Amazon owned keys

You cannot enable or disable key rotation for Amazon owned keys. The [key rotation](#) strategy for an Amazon owned key is determined by the Amazon service that creates and manages the key. For details, see the *Encryption at Rest* topic in the user guide or developer guide for the service.

Supported KMS key types

Automatic key rotation is supported only on [symmetric encryption KMS keys](#) with key material that Amazon KMS generates (Origin = AWS_KMS).

Automatic key rotation is *not* supported on the following types of KMS keys, but you can [rotate these KMS keys manually](#).

- [Asymmetric KMS keys](#)
- [HMAC KMS keys](#)
- KMS keys in [custom key stores](#)
- KMS keys with [imported key material](#)

Rotating multi-Region keys

You can enable and disable automatic rotation and perform on-demand rotation of the key material in symmetric encryption [multi-Region keys](#). Key rotation is a [shared property](#) of multi-Region keys.

You enable and disable automatic key rotation only on the primary key. You initiate on-demand rotation only on the primary key.

- When Amazon KMS synchronizes the multi-Region keys, it copies the key rotation property setting from the primary key to all of its related replica keys.
- When Amazon KMS rotates the key material, it creates new key material for the primary key and then copies the new key material across Region boundaries to all related replica keys. The key material never leaves Amazon KMS unencrypted. This step is carefully controlled to ensure that key material is fully synchronized before any key is used in a cryptographic operation.
- Amazon KMS does not encrypt any data with the new key material until that key material is available in the primary key and every one of its replica keys.
- When you replicate a primary key that has been rotated, the new replica key has the current key material and all previous versions of the key material for its related multi-Region keys.

This pattern ensures that related multi-Region keys are fully interoperable. Any multi-Region key can decrypt any ciphertext encrypted by a related multi-Region key, even if the ciphertext was encrypted before the key was created.

Amazon services

You can enable automatic key rotation on the [customer managed keys](#) that you use for server-side encryption in Amazon services. The annual rotation is transparent and compatible with Amazon services.

Monitoring key rotation

When Amazon KMS rotates the key material for an [Amazon managed key](#) or [customer managed key](#), it writes a KMS CMK Rotation event to Amazon EventBridge and a [RotateKey event](#) to your Amazon CloudTrail log. You can use these records to verify that the KMS key was rotated.

You can use the Amazon Key Management Service console to view the number of remaining on-demand rotations and a list of all completed key material rotations for a KMS key.

You can use [ListKeyRotations](#) operation to view the details of completed rotations.

Eventual consistency

Key rotation is subject to the same eventual consistency effects as other Amazon KMS management operations. There might be a slight delay before the new key material is available throughout Amazon KMS. However, rotating key material does not cause any interruption or delay in cryptographic operations. The current key material is used in cryptographic operations until the new key material is available throughout Amazon KMS. When key material for a multi-Region key is automatically rotated, Amazon KMS uses the current key material until the new key material is available in all Regions with a related multi-Region key.

Enable automatic key rotation

By default, when you enable *automatic key rotation* for a KMS key, Amazon KMS generates new cryptographic material for the KMS key every year. You can also specify a custom [rotation-period](#) to define the number of days after you enable automatic key rotation that Amazon KMS will rotate your key material, and the number of days between each automatic rotation thereafter.

Automatic key rotation has the following benefits:

- The properties of the KMS key, including its [key ID](#), [key ARN](#), region, policies, and permissions, do not change when the key is rotated.
- You do not need to change applications or aliases that refer to the key ID or key ARN of the KMS key.
- Rotating key material does not affect the use of the KMS key in any Amazon Web Services service.
- After you enable key rotation, Amazon KMS rotates the KMS key automatically on the next rotation date defined by your rotation period. You don't need to remember or schedule the update.

You can enable automatic key rotation in the Amazon KMS console or by using the [EnableKeyRotation](#) operation. To enable automatic key rotation, you need `kms:EnableKeyRotation` permissions. For more information about Amazon KMS permissions, see the [Permissions reference](#).

Using the Amazon KMS console

1. Sign in to the Amazon Web Services Management Console and open the Amazon Key Management Service (Amazon KMS) console at <https://console.amazonaws.cn/kms>.
2. To change the Amazon Web Services Region, use the Region selector in the upper-right corner of the page.
3. In the navigation pane, choose **Customer managed keys**. (You cannot enable or disable rotation of Amazon managed keys. They are automatically rotated every year.)
4. Choose the alias or key ID of a KMS key.
5. Choose the **Key rotation** tab.

The **Key rotation** tab appears only on the detail page of symmetric encryption KMS keys with key material that Amazon KMS generated (the **Origin** is **AWS_KMS**), including [multi-Region symmetric encryption KMS keys](#).

You cannot automatically rotate asymmetric KMS keys, HMAC KMS keys, KMS keys with [imported key material](#), or KMS keys in [custom key stores](#). However, you can [rotate them manually](#).

6. In the **Automatic key rotation** section, choose **Edit**.
7. For **Key rotation**, select **Enable**.

Note

If a KMS key is disabled or pending deletion, Amazon KMS does not rotate the key material and you cannot update the automatic key rotation status or rotation period. Enable the KMS key or cancel deletion to update the automatic key rotation configuration. For details, see [How key rotation works](#) and [Key states of Amazon KMS keys](#).

8. (Optional) Type a rotation period between 90 and 2560 days. The default value is 365 days. If you do not specify a custom rotation period, Amazon KMS will rotate the key material every year.

You can use the [kms:RotationPeriodInDays](#) condition key to limit the values that principals can specify for the rotation period.

9. Choose **Save**.

Using the Amazon KMS API

You can use the [Amazon Key Management Service \(Amazon KMS\) API](#) to enable automatic key rotation and view the current rotation status of any customer managed key. These examples use the [Amazon Command Line Interface \(Amazon CLI\)](#), but you can use any supported programming language.

The [EnableKeyRotation](#) operation enables automatic key rotation for the specified KMS key. To identify the KMS key in this operation, use its [key ID](#) or [key ARN](#). By default, key rotation is disabled for customer managed keys.

You can use the [kms:RotationPeriodInDays](#) condition key to limit the values that principals can specify for the `RotationPeriodInDays` parameter of an `EnableKeyRotation` request.

The following example enables key rotation with a rotation period of 180 days on the specified symmetric encryption KMS key and uses the [GetKeyRotationStatus](#) operation to see the result.

```
$ aws kms enable-key-rotation \
  --key-id 1234abcd-12ab-34cd-56ef-1234567890ab \
  --rotation-period-in-days 180

$ aws kms get-key-rotation-status --key-id 1234abcd-12ab-34cd-56ef-1234567890ab
{
  "KeyId": "1234abcd-12ab-34cd-56ef-1234567890ab",
  "KeyRotationEnabled": true,
  "RotationPeriodInDays": 180,
  "NextRotationDate": "2024-02-14T18:14:33.587000+00:00"
}
```

Disable automatic key rotation

After enabling automatic key rotation on a customer managed key, you can choose to disable it at any time.

If you disable automatic key rotation, the KMS key continues to use the version of the key material it was using when rotation was disabled. If you enable automatic key rotation again, Amazon KMS rotates the key material based on the new rotation-enable date.

Disabling automatic rotation does not impact your ability to [perform on-demand rotations](#), nor does it cancel any in progress on-demand rotations.

You can disable automatic key rotation in the Amazon KMS console or by using the [DisableKeyRotation](#) operation. To disable automatic key rotation, you need `kms:DisableKeyRotation` permissions. For more information about Amazon KMS permissions, see the [Permissions reference](#).

Using the Amazon KMS console

1. Sign in to the Amazon Web Services Management Console and open the Amazon Key Management Service (Amazon KMS) console at <https://console.amazonaws.cn/kms>.
2. To change the Amazon Web Services Region, use the Region selector in the upper-right corner of the page.
3. In the navigation pane, choose **Customer managed keys**. (You cannot enable or disable rotation of Amazon managed keys. They are automatically rotated every year.)
4. Choose the alias or key ID of a KMS key.
5. Choose the **Key rotation** tab.

The **Key rotation** tab appears only on the detail page of symmetric encryption KMS keys with key material that Amazon KMS generated (the **Origin** is **AWS_KMS**), including [multi-Region](#) symmetric encryption KMS keys.

You cannot automatically rotate asymmetric KMS keys, HMAC KMS keys, KMS keys with [imported key material](#), or KMS keys in [custom key stores](#). However, you can [rotate them manually](#).

6. In the **Automatic key rotation** section, choose **Edit**.
7. For **Key rotation**, select **Disable**.

Note

If a KMS key is disabled or pending deletion, Amazon KMS does not rotate the key material and you cannot update the automatic key rotation status or rotation period. Enable the KMS key or cancel deletion to update the automatic key rotation configuration. For details, see [How key rotation works](#) and [Key states of Amazon KMS keys](#).

8. Choose **Save**.

Using the Amazon KMS API

You can use the [Amazon Key Management Service \(Amazon KMS\) API](#) to disable automatic key rotation and view the current rotation status of any customer managed key. This example uses the [Amazon Command Line Interface \(Amazon CLI\)](#), but you can use any supported programming language.

The [DisableKeyRotation](#) operation disables automatic key rotation. To identify the KMS key in this operation, use its [key ID](#) or [key ARN](#). By default, key rotation is disabled for customer managed keys.

The following example disables automatic key rotation on the specified symmetric encryption KMS key and uses the [GetKeyRotationStatus](#) operation to see the result.

```
$ aws kms disable-key-rotation --key-id 1234abcd-12ab-34cd-56ef-1234567890ab

$ aws kms get-key-rotation-status --key-id 1234abcd-12ab-34cd-56ef-1234567890ab
{
  "KeyId": "1234abcd-12ab-34cd-56ef-1234567890ab",
  "KeyRotationEnabled": false
}
```

Perform on-demand key rotation

You can perform on-demand rotation of the key material in customer managed KMS keys, regardless of whether or not automatic key rotation is enabled. Disabling automatic rotation ([DisableKeyRotation](#)) does not impact your ability to perform on-demand rotations, nor does it cancel any in progress on-demand rotations. On-demand rotations do not change existing automatic rotation schedules. For example, consider a KMS key that has automatic key rotation enabled with a rotation period of 730 days. If the key is scheduled to automatically rotate on April 14, 2024, and you perform an on-demand rotation on April 10, 2024, the key will automatically rotate, as scheduled, on April 14, 2024 and every 730 days thereafter.

You can perform on-demand key rotation a maximum of 10 times per KMS key. You can use the Amazon KMS console to view the number of remaining on-demand rotations available for a KMS key.

On-demand key rotation is supported only on [symmetric encryption KMS keys](#). You cannot perform on-demand rotation of [asymmetric KMS keys](#), [HMAC KMS keys](#), KMS keys with [imported](#)

[key material](#), or KMS keys in a [custom key store](#). To perform on-demand rotation of a set of related [multi-Region keys](#), invoke the on-demand rotation on the primary key.

Authorized users can use the Amazon KMS console and the Amazon KMS API to initiate on-demand key rotation and view the key rotation status.

Topics

- [Initiating on-demand key rotation \(console\)](#)
- [Initiating on-demand key rotation \(Amazon KMS API\)](#)

Initiating on-demand key rotation (console)

1. Sign in to the Amazon Web Services Management Console and open the Amazon Key Management Service (Amazon KMS) console at <https://console.amazonaws.cn/kms>.
2. To change the Amazon Web Services Region, use the Region selector in the upper-right corner of the page.
3. In the navigation pane, choose **Customer managed keys**. (You cannot perform on-demand rotation of Amazon managed keys. They are automatically rotated every year.)
4. Choose the alias or key ID of a KMS key.
5. Choose the **Key rotation** tab.

The **Key rotation** tab appears only on the detail page of symmetric encryption KMS keys with key material that Amazon KMS generated (the **Origin** is **AWS_KMS**), including [multi-Region symmetric encryption KMS keys](#).

You cannot perform on-demand rotation of asymmetric KMS keys, HMAC KMS keys, KMS keys with [imported key material](#), or KMS keys in [custom key stores](#). However, you can [rotate them manually](#).

6. In the **On-demand key rotation** section, choose **Rotate key**.
7. Read and consider the warning and the information about the number of remaining on-demand rotations for the key. If you decide that you do not want to proceed with the on-demand rotation, choose **Cancel**.
8. Choose **Rotate key** to confirm on-demand rotation.

Note

On-demand rotation is subject to the same eventual consistency effects as other Amazon KMS management operations. There might be a slight delay before the new key material is available throughout Amazon KMS. The banner at the top of the console notifies you when the on-demand rotation is complete.

Initiating on-demand key rotation (Amazon KMS API)

You can use the [Amazon Key Management Service \(Amazon KMS\) API](#) to initiate on-demand key rotation, and view the current rotation status of any customer managed key. This example uses the [Amazon Command Line Interface \(Amazon CLI\)](#), but you can use any supported programming language.

The [RotateKeyOnDemand](#) operation immediately initiates on-demand key rotation for the specified KMS key. To identify the KMS key in these operations, use its [key ID](#) or [key ARN](#).

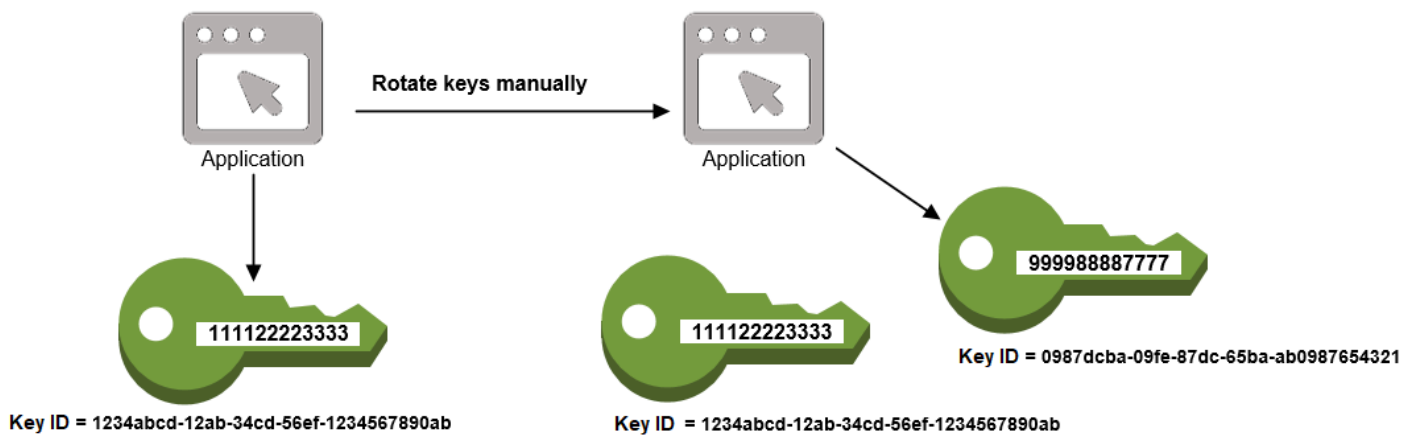
The following example initiates on-demand key rotation on the specified symmetric encryption KMS key and uses the [GetKeyRotationStatus](#) operation to verify that the on-demand rotation is in progress. The `OnDemandRotationStartDate` in the `kms:GetKeyRotationStatus` response identifies the date and time that an in progress on-demand rotation was initiated.

```
$ aws kms rotate-key-on-demand --key-id 1234abcd-12ab-34cd-56ef-1234567890ab
{
  "KeyId": "1234abcd-12ab-34cd-56ef-1234567890ab"
}

$ aws kms get-key-rotation-status --key-id 1234abcd-12ab-34cd-56ef-1234567890ab
{
  "KeyId": "1234abcd-12ab-34cd-56ef-1234567890ab",
  "KeyRotationEnabled": true,
  "NextRotationDate": "2024-03-14T18:14:33.587000+00:00",
  "OnDemandRotationStartDate": "2024-02-24T18:44:48.587000+00:00"
  "RotationPeriodInDays": 365
}
```

Rotate keys manually

You might want to create a new KMS key and use it in place of a current KMS key instead of enabling automatic key rotation. When the new KMS key has different cryptographic material than the current KMS key, using the new KMS key has the same effect as changing the key material in an existing KMS key. The process of replacing one KMS key with another is known as *manual key rotation*.



Manual rotation is a good choice when you want to rotate KMS keys that are not eligible for automatic key rotation, such as asymmetric KMS keys, HMAC KMS keys, KMS keys in [custom key stores](#), and KMS keys with [imported key material](#).

Note

When you begin using the new KMS key, be sure to keep the original KMS key enabled so that Amazon KMS can decrypt data that the original KMS key encrypted.

When you rotate KMS keys manually, you also need to update references to the KMS key ID or key ARN in your applications. [Aliases](#), which associate a friendly name with a KMS key, can make this process easier. Use an alias to refer to a KMS key in your applications. Then, when you want to change the KMS key that the application uses, instead of editing your application code, change the target KMS key of the alias. For details, see [Learn how to use aliases in your applications](#).

Note

Aliases that point to the latest version of a manually rotated KMS key are a good solution for the [DescribeKey](#), [Encrypt](#), [GenerateDataKey](#), [GenerateDataKeyPair](#), [GenerateMac](#), and

[Sign](#) operations. Aliases are not permitted in operations that manage KMS keys, such as [DisableKey](#) or [ScheduleKeyDeletion](#).

When calling the [Decrypt](#) operation on manually rotated symmetric encryption KMS keys, omit the `KeyId` parameter from the command. Amazon KMS automatically uses the KMS key that encrypted the ciphertext.

The `KeyId` parameter is required when calling `Decrypt` or [Verify](#) with an asymmetric KMS key, or calling [VerifyMac](#) with an HMAC KMS key. These requests fail when the value of the `KeyId` parameter is an alias that no longer points to the KMS key that performed the cryptographic operation, such as when a key is manually rotated. To avoid this error, you must track and specify the correct KMS key for each operation.

To change the target KMS key of an alias, use [UpdateAlias](#) operation in the Amazon KMS API. For example, this command updates the `alias/TestKey` alias to point to a new KMS key. Because the operation does not return any output, the example uses the [ListAliases](#) operation to show that the alias is now associated with a different KMS key and the `LastUpdatedDate` field is updated. The `ListAliases` commands use the [query parameter](#) in the Amazon CLI to get only the `alias/TestKey` alias.

```
$ aws kms list-aliases --query 'Aliases[?AliasName==`alias/TestKey`]'
{
  "Aliases": [
    {
      "AliasArn": "arn:aws:kms:us-west-2:111122223333:alias/TestKey",
      "AliasName": "alias/TestKey",
      "TargetKeyId": "1234abcd-12ab-34cd-56ef-1234567890ab",
      "CreationDate": 1521097200.123,
      "LastUpdatedDate": 1521097200.123
    },
  ]
}

$ aws kms update-alias --alias-name alias/TestKey --target-key-id
0987dcba-09fe-87dc-65ba-ab0987654321

$ aws kms list-aliases --query 'Aliases[?AliasName==`alias/TestKey`]'
{
  "Aliases": [
    {
```

```
    "AliasArn": "arn:aws:kms:us-west-2:111122223333:alias/TestKey",
    "AliasName": "alias/TestKey",
    "TargetKeyId": "0987dcba-09fe-87dc-65ba-ab0987654321",
    "CreationDate": 1521097200.123,
    "LastUpdatedDate": 1604958290.722
  },
]
}
```

Change the primary key in a set of multi-Region keys

Every set of related multi-Region keys must have a primary key. But you can change the primary key. This action, known as *updating the primary Region*, converts the current primary key to a replica key and converts one of the related replica keys to the primary key. You might do this if you need to delete the current primary key while maintaining the replica keys, or to locate the primary key in the same Region as your key administrators.

You can select any related replica key to be the new primary key. Both the primary key and the replica key must be in the Enabled [key state](#) when the operation starts.

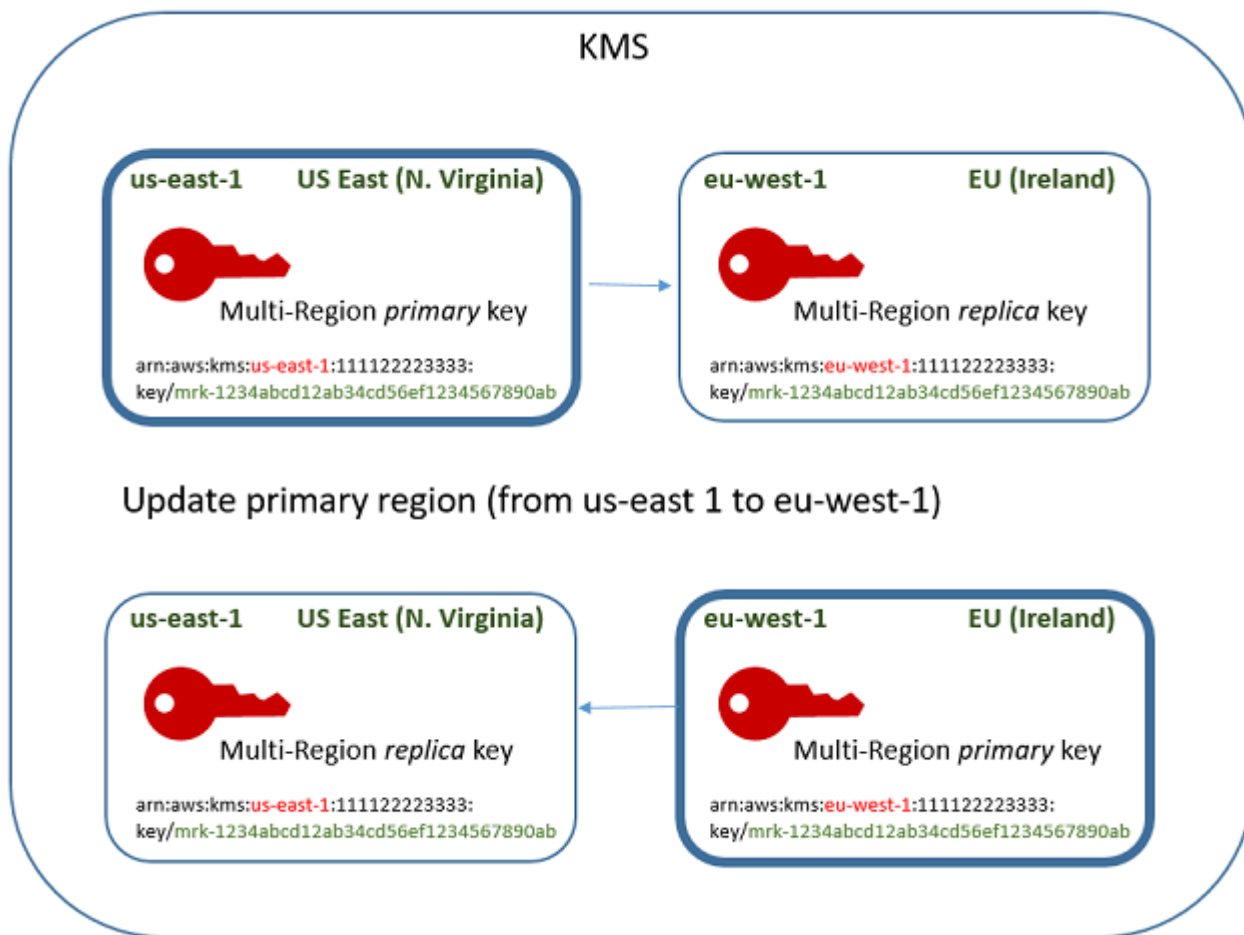
The Updating key state

Even after the `UpdatePrimaryRegion` operation completes, the process of updating the primary Region might still be in progress for a few more seconds. During this time, the old and new primary keys have a transient key state of [Updating](#). While the key state is `Updating`, you can use the keys in cryptographic operations, but you cannot replicate the new primary key or perform certain management operations, such as enabling or disabling these keys. Operations such as [DescribeKey](#) might display both the old and new primary keys as replicas. The Enabled key state is restored when the update is complete.

For information about the effect of the `Updating` key state, see [Key states of Amazon KMS keys](#).

How it works

Suppose you have a primary key in US East (N. Virginia) (`us-east-1`) and a replica key in Europe (Ireland) (`eu-west-1`). You can use the update feature to change the primary key in US East (N. Virginia) (`us-east-1`) to a replica key and change the replica key in Europe (Ireland) (`eu-west-1`) to the primary key.



When the update process completes, the multi-Region key in the Europe (Ireland) (eu-west-1) Region is a multi-Region primary key and the key in the US East (N. Virginia) (us-east-1) Region is its replica key. If there are other related replica keys, they become replicas of the new primary key. The next time that Amazon KMS synchronizes the shared properties of the multi-Region keys, it will get the [shared properties](#) from the new primary key and copy them to its replica keys, including the former primary key.

The update operation has no effect on the [key ARN](#) of any multi-Region key. It also has no effect on shared properties, such as the key material, or on independent properties, such as the key policy. However, you might want to [update the key policy](#) of the new primary key. For example, you might want to add [kms:ReplicateKey](#) permission for trusted principals to the new primary key and remove it from the new replica key.

Update the primary Region

You can convert a replica key to a primary key, which changes the former primary key into a replica. To update the primary Region, you need [kms:UpdatePrimaryRegion](#) permission in both Regions.

You can update the primary Region in the Amazon KMS console or by using the [UpdatePrimaryRegion](#) operation.

Using the Amazon KMS console

You can update the primary key in the Amazon KMS console. Start on the key details page for the current primary key.

1. Sign in to the Amazon Web Services Management Console and open the Amazon Key Management Service (Amazon KMS) console at <https://console.amazonaws.cn/kms>.
2. To change the Amazon Web Services Region, use the Region selector in the upper-right corner of the page.
3. In the navigation pane, choose **Customer managed keys**.
4. Select the key ID or alias of the [multi-Region primary key](#). This opens the key details page for the primary key.

To identify a multi-Region primary key, use the tool icon in the upper right corner to add the **Regionality** column to the table.

5. Choose the **Regionality** tab.
6. In the **Primary key** section, choose **Change primary Region**.
7. Choose the Region of the new primary key. You can choose only one Region from the menu.

The **Change primary Regions** menu includes only Regions that have a related multi-Region key. You might not have [permission to update the primary Region](#) in all of the Regions on the menu.

8. Choose **Change primary Region**.

Using the Amazon KMS API

To change the primary key in a set of related multi-Region keys, use the [UpdatePrimaryRegion](#) operation.

Use the `KeyId` parameter to identify the current primary key. Use the `PrimaryRegion` parameter to indicate the Amazon Web Services Region of the new primary key. If the primary key doesn't already have a replica in the new primary Region, the operation fails.

The following example changes the primary key from the multi-Region key in the `us-west-2` Region to its replica in the `eu-west-1` Region. The `KeyId` parameter identifies the current primary key in the `us-west-2` Region. The `PrimaryRegion` parameter specifies the Amazon Web Services Region of the new primary key, `eu-west-1`.

```
$ aws kms update-primary-region \  
    --key-id arn:aws:kms:us-west-2:111122223333:key/  
mrk-1234abcd12ab34cd56ef1234567890ab \  
    --primary-region eu-west-1
```

When successful, this operation doesn't return any output; just the HTTP status code. To see the effect, call the [DescribeKey](#) operation on either of the multi-Region keys. You might want to wait until the key state returns to `Enabled`. While the key state is [Updating](#), the values for the key might still be in flux.

For example, the following `DescribeKey` call gets the details about the multi-Region key in the `eu-west-1` Region. The output shows that the multi-Region key in the `eu-west-1` Region is now the primary key. The related multi-Region key (same key ID) in the `us-west-2` Region is now a replica key.

```
$ aws kms describe-key \  
    --key-id arn:aws:kms:eu-west-1:111122223333:key/  
mrk-1234abcd12ab34cd56ef1234567890ab \  
  
{  
  "KeyMetadata": {  
    "AWSAccountId": "111122223333",  
    "KeyId": "mrk-1234abcd12ab34cd56ef1234567890ab",  
    "Arn": "arn:aws:kms:eu-west-1:111122223333:key/  
mrk-1234abcd12ab34cd56ef1234567890ab",  
    "CreationDate": 1609193147.831,  
    "Enabled": true,  
    "Description": "multi-region-key",  
    "KeySpec": "SYMMETRIC_DEFAULT",  
    "KeyState": "Enabled",  
    "KeyUsage": "ENCRYPT_DECRYPT",  
    "Origin": "AWS_KMS",
```



```
    "KeyManager": "CUSTOMER",
    "CustomerMasterKeySpec": "SYMMETRIC_DEFAULT",
    "EncryptionAlgorithms": [
      "SYMMETRIC_DEFAULT"
    ],
    "MultiRegion": true,
    "MultiRegionConfiguration": {
      "MultiRegionKeyType": "PRIMARY",
      "PrimaryKey": {
        "Arn": "arn:aws:kms:eu-west-1:111122223333:key/
mrk-1234abcd12ab34cd56ef1234567890ab",
        "Region": "eu-west-1"
      },
      "ReplicaKeys": [
        {
          "Arn": "arn:aws:kms:us-west-2:111122223333:key/
mrk-1234abcd12ab34cd56ef1234567890ab",
          "Region": "us-west-2"
        }
      ]
    }
  }
}
```

Delete an Amazon KMS key

Deleting an Amazon KMS key is destructive and potentially dangerous. It deletes the key material and all metadata associated with the KMS key and is irreversible. After a KMS key is deleted, you can no longer decrypt the data that was encrypted under that KMS key, which means that data becomes unrecoverable. (The only exceptions are [multi-Region replica keys](#) and asymmetric and HMAC KMS keys with imported key material.) This risk is significant for [asymmetric KMS keys used for encryption](#) where, without warning or error, users can continue to generate ciphertexts with the public key that cannot be decrypted after the private key is deleted from Amazon KMS.

You should delete a KMS key only when you are sure that you don't need to use it anymore. If you are not sure, consider [disabling the KMS key](#) instead of deleting it. You can re-enable a disabled KMS key and [cancel the scheduled deletion](#) of a KMS key, but you cannot recover a deleted KMS key.

You can only schedule the deletion of a customer managed key. You cannot delete Amazon managed keys or Amazon owned keys.

Before deleting a KMS key, you might want to know how many ciphertexts were encrypted under that KMS key. Amazon KMS does not store this information and does not store any of the ciphertexts. To get this information, you must determine past usage of a KMS key. For help, go to [Determine past usage of a KMS key](#).

Amazon KMS never deletes your KMS keys unless you explicitly schedule them for deletion and the mandatory waiting period expires.

However, you might choose to delete a KMS key for one or more of the following reasons:

- To complete the key lifecycle for KMS keys that you no longer need
- To avoid the management overhead and [costs](#) associated with maintaining unused KMS keys
- To reduce the number of KMS keys that count against your [KMS key resource quota](#)

Note

If you [close your Amazon Web Services account](#), your KMS keys become inaccessible and you are no longer billed for them.

Amazon KMS records an entry in your Amazon CloudTrail log when you [schedule deletion](#) of the KMS key and when the [KMS key is actually deleted](#).

About the waiting period

Because it is destructive and potentially dangerous to delete a KMS key, Amazon KMS requires you to set a waiting period of 7 – 30 days. The default waiting period is 30 days.

However, the actual waiting period might be up to 24 hours longer than the one you scheduled. To get the actual date and time when the KMS key will be deleted, use the [DescribeKey](#) operation. Or in the Amazon KMS console, on [detail page](#) for the KMS key, in the **General configuration** section, see the **Scheduled deletion date**. Be sure to note the time zone.

During the waiting period, the KMS key status and key state is **Pending deletion**.

- A KMS key pending deletion cannot be used in any [cryptographic operations](#).
- Amazon KMS does not [rotate the key material](#) of KMS keys that are pending deletion.

After the waiting period ends, Amazon KMS deletes the KMS key, its aliases, and all related Amazon KMS metadata.

Scheduling the deletion of a KMS key might not immediately affect data keys encrypted by the KMS key. For details, see [How unusable KMS keys affect data keys](#).

Use the waiting period to ensure that you don't need the KMS key now or in the future. You can [configure an Amazon CloudWatch alarm](#) to warn you if a person or application attempts to use the KMS key during the waiting period. To recover the KMS key, you can cancel key deletion before the waiting period ends. After the waiting period ends you cannot cancel key deletion, and Amazon KMS deletes the KMS key.

Special considerations

Before you schedule your keys for deletion, review the following special considerations for deleting special purpose KMS keys.

Deleting asymmetric KMS keys

Users [who are authorized](#) can delete symmetric or asymmetric KMS keys. The procedure to schedule the deletion of these KMS keys is the same for both types of keys. However, because

the [public key of an asymmetric KMS key can be downloaded](#) and used outside of Amazon KMS, the operation poses significant additional risks, especially for asymmetric KMS keys used for encryption (the key usage is ENCRYPT_DECRYPT).

- When you schedule the deletion of a KMS key, the key state of KMS key changes to **Pending deletion**, and the KMS key cannot be used in [cryptographic operations](#). However, scheduling deletion has no effect on public keys outside of Amazon KMS. Users who have the public key can continue to use them to encrypt messages. They do not receive any notification that the key state is changed. Unless the deletion is canceled, ciphertext created with the public key cannot be decrypted.
- Alarms, logs, and other strategies that detect attempted use of KMS key that is pending deletion cannot detect use of the public key outside of Amazon KMS.
- When the KMS key is deleted, all Amazon KMS actions involving that KMS key fail. However, users who have the public key can continue to use them to encrypt messages. These ciphertexts cannot be decrypted.

If you must delete an asymmetric KMS key with a key usage of ENCRYPT_DECRYPT, use your CloudTrail Log entries to determine whether the public key has been downloaded and shared. If it has, verify that the public key is not being used outside of Amazon KMS. Then, consider [disabling the KMS key](#) instead of deleting it.

The risk posed by deleting an asymmetric KMS key is mitigated for asymmetric KMS keys with imported key material. For details, see [Deleting KMS keys with imported key material](#).

Deleting multi-Region keys

To delete a primary key, you must schedule the deletion all of its replica keys, and then wait for the replica keys to be deleted. The required waiting period for deleting a primary key begins when the last of its replica keys is deleted. If you must delete a primary key from a particular Region without deleting its replica keys, change the primary key to a replica key by [updating the primary Region](#).

You can delete a replica key at any time. It doesn't depend on the key state of any other KMS key. If you mistakenly delete a replica key, you can recreate it by replicating the same primary key in the same Region. The new replica key you create will have the same [shared properties](#) as the original replica key.

Deleting KMS keys with imported key material

Deleting the key material of a KMS key with imported key material is temporary and reversible. To restore the key, reimport its key material.

In contrast, deleting a KMS key is irreversible. If you [schedule key deletion](#) and the required waiting period expires, Amazon KMS permanently and irreversibly deletes the KMS key, its key material, and all metadata associated with the KMS key.

However, the risk and consequence of deleting a KMS key with imported key material depends on the type ("key spec") of the KMS key.

- **Symmetric encryption keys** — If you delete a symmetric encryption KMS key, all remaining ciphertexts encrypted by that key are unrecoverable. You cannot create a new symmetric encryption KMS key that can decrypt the ciphertexts of a deleted symmetric encryption KMS key, even if you have the same key material. Metadata unique to each KMS key is cryptographically bound to each symmetric ciphertext. This security feature guarantees that only the KMS key that encrypted the symmetric ciphertext can decrypt it, but it prevents you from recreating an equivalent KMS key.
- **Asymmetric and HMAC keys** — If you have the original key material, you can create a new KMS key with the same cryptographic properties as an asymmetric or HMAC KMS key that was deleted. Amazon KMS generates standard RSA ciphertexts and signatures, ECC signatures, and HMAC tags, which do not include any unique security features. Also, you can use an HMAC key or the private key of an asymmetric key pair outside of Amazon.

A new KMS key that you create with the same asymmetric or HMAC key material will have a different key identifier. You will have to create a new key policy, recreate any aliases, and update existing IAM policies and grants to refer to the new key.

Deleting KMS keys from an Amazon CloudHSM key stores

When you schedule deletion of a KMS key from an Amazon CloudHSM key store, its [key state](#) changes to **Pending deletion**. The KMS key remains in the **Pending deletion** state throughout the waiting period, even if the KMS key becomes unavailable because you have [disconnected the custom key store](#). This allows you to cancel the deletion of the KMS key at any time during the waiting period.

When the waiting period expires, Amazon KMS deletes the KMS key from Amazon KMS. Then Amazon KMS makes a best effort to delete the key material from the associated Amazon CloudHSM cluster. If Amazon KMS cannot delete the key material, such as when the key store is disconnected from Amazon KMS, you might need to manually [delete the orphaned key material](#) from the cluster.

Amazon KMS does not delete the key material from cluster backups. Even if you delete the KMS key from Amazon KMS and delete its key material from your Amazon CloudHSM cluster,

clusters created from backups might contain the deleted key material. To permanently delete the key material, use the [DescribeKey](#) operation to identify the creation date of the KMS key. Then [delete all cluster backups](#) that might contain the key material.

When you schedule the deletion of a KMS key from an Amazon CloudHSM key store, the KMS key becomes unusable right away (subject to eventual consistency). However, resources encrypted with [data keys](#) protected by the KMS key are not affected until the KMS key is used again, such to decrypt the data key. This issue affects Amazon Web Services services, many of which use data keys to protect your resources. For details, see [How unusable KMS keys affect data keys](#).

Deleting KMS keys from an external key store

Deleting a KMS key from an external key store has no effect on the [external key](#) that served as its key material.

When you schedule deletion of a KMS key from an external key store, its [key state](#) changes to **Pending deletion**. The KMS key remains in the **Pending deletion** state throughout the waiting period, even if the KMS key becomes unavailable because you have [disconnected the external key store](#). This allows you to cancel the deletion of the KMS key at any time during the waiting period. When the waiting period expires, Amazon KMS deletes the KMS key from Amazon KMS.

When you schedule the deletion of a KMS key from an external key store, the KMS key becomes unusable right away (subject to eventual consistency). However, resources encrypted with [data keys](#) protected by the KMS key are not affected until the KMS key is used again, such to decrypt the data key. This issue affects Amazon Web Services services, many of which use data keys to protect your resources. For details, see [How unusable KMS keys affect data keys](#).

Control access to key deletion

If you use IAM policies to allow Amazon KMS permissions, IAM identities that have Amazon administrator access (`"Action": "*"`) or Amazon KMS full access (`"Action": "kms:*"`) are already allowed to schedule and cancel key the deletion of KMS keys. To allow key administrators to schedule and cancel key deletion in the key policy, use the Amazon KMS console or the Amazon KMS API.

Typically, only key administrators have permission to schedule or cancel key deletion. However, you can give these permissions to other IAM identities by adding the `kms:ScheduleKeyDeletion` and `kms:CancelKeyDeletion` permission to the key policy or an IAM policy. You can also

use the [kms:ScheduleKeyDeletionPendingWindowInDays](#) condition key to further constrain the values that principals can specify in the `PendingWindowInDays` parameter of a [ScheduleKeyDeletion](#) request.

Allow key administrators to schedule and cancel key deletion

Using the Amazon KMS console

To give key administrators permission to schedule and cancel key deletion.

1. Sign in to the Amazon Web Services Management Console and open the Amazon Key Management Service (Amazon KMS) console at <https://console.amazonaws.cn/kms>.
2. To change the Amazon Web Services Region, use the Region selector in the upper-right corner of the page.
3. In the navigation pane, choose **Customer managed keys**.
4. Choose the alias or key ID of the KMS key whose permissions you want to change.
5. Choose the **key policy** tab.
6. The next step differs for the *default view* and *policy view* of your key policy. Default view is available only if you are using the default console key policy. Otherwise, only policy view is available.

When default view is available, a **Switch to policy view** or **Switch to default view** button appears on the **Key policy** tab.

- In default view:
 - Under **Key deletion**, choose **Allow key administrators to delete this key**.
- In policy view:
 - a. Choose **Edit**.
 - b. In the policy statement for key administrators, add the `kms:ScheduleKeyDeletion` and `kms:CancelKeyDeletion` permissions to the `Action` element.

```
{
  "Sid": "Allow access for Key Administrators",
  "Effect": "Allow",
  "Principal": {"AWS": "arn:aws:iam::111122223333:user/KMSKeyAdmin"},
  "Action": [
    "kms:Create*",
```

```
"kms:Describe*",
"kms:Enable*",
"kms:List*",
"kms:Put*",
"kms:Update*",
"kms:Revoke*",
"kms:Disable*",
"kms:Get*",
"kms>Delete*",
  "kms:ScheduleKeyDeletion",
  "kms:CancelKeyDeletion"
],
"Resource": "*"
}
```

- c. Choose **Save changes**.

Using the Amazon KMS API

You can use the Amazon Command Line Interface to add permissions for scheduling and canceling key deletion.

To add permission to schedule and cancel key deletion

1. Use the [aws kms get-key-policy](#) command to retrieve the existing key policy, and then save the policy document to a file.
2. Open the policy document in your preferred text editor. In the policy statement for key administrators, add the `kms:ScheduleKeyDeletion` and `kms:CancelKeyDeletion` permissions. The following example shows a policy statement with these two permissions:

```
{
  "Sid": "Allow access for Key Administrators",
  "Effect": "Allow",
  "Principal": {"AWS": "arn:aws:iam::111122223333:user/KMSKeyAdmin"},
  "Action": [
    "kms:Create*",
    "kms:Describe*",
    "kms:Enable*",
    "kms:List*",
    "kms:Put*",
    "kms:Update*",
    "kms:Revoke*",
```



```
"kms:Disable*",
"kms:Get*",
"kms:Delete*",
"kms:ScheduleKeyDeletion",
"kms:CancelKeyDeletion"
],
"Resource": "*"
}
```

3. Use the [aws kms put-key-policy](#) command to apply the key policy to the KMS key.

Schedule key deletion

The following procedures describe how to schedule key deletion and cancel key deletion of Amazon KMS keys (KMS keys) in Amazon KMS using the Amazon Web Services Management Console and the Amazon KMS API.

Warning

Deleting a KMS key is destructive and potentially dangerous. You should proceed only when you are sure that you don't need to use the KMS key anymore and won't need to use it in the future. If you are not sure, you should [disable the KMS key](#) instead of deleting it.

Before you can delete a KMS key, you must have permission to do so. For information about giving these permissions to key administrators, see [Control access to key deletion](#). You can also use the [kms:ScheduleKeyDeletionPendingWindowInDays](#) condition key to further constrain the waiting period, such as enforcing a minimum waiting period.

Amazon KMS records an entry in your Amazon CloudTrail log when you [schedule deletion](#) of the KMS key and when the [KMS key is actually deleted](#).

Using the Amazon KMS console

In the Amazon Web Services Management Console, you can schedule and cancel the deletion of multiple KMS keys at one time.

To schedule key deletion

1. Sign in to the Amazon Web Services Management Console and open the Amazon Key Management Service (Amazon KMS) console at <https://console.amazonaws.cn/kms>.
2. To change the Amazon Web Services Region, use the Region selector in the upper-right corner of the page.
3. In the navigation pane, choose **Customer managed keys**.

You cannot schedule the deletion of [Amazon managed keys](#) or [Amazon owned keys](#).

4. Choose the check box next to the KMS key that you want to delete.
5. Choose **Key actions, Schedule key deletion**.
6. Read and consider the warning, and the information about canceling the deletion during the waiting period. If you decide to cancel the deletion, at the bottom of the page, choose **Cancel**.
7. For **Waiting period (in days)**, enter a number of days between 7 and 30.
8. Review the KMS keys that you are deleting.
9. Choose the check box next to **Confirm you want to schedule this key for deletion in *<number of days>* days..**
10. Choose **Schedule deletion**.

The KMS key status changes to **Pending deletion**.

Using the Amazon KMS API

Use the [aws kms schedule-key-deletion](#) command to schedule key deletion of a [customer managed key](#), as shown in the following example.

You cannot schedule the deletion of an Amazon managed key or Amazon owned key.

```
$ aws kms schedule-key-deletion --key-id 1234abcd-12ab-34cd-56ef-1234567890ab --
pending-window-in-days 10
```

When used successfully, the Amazon CLI returns output like the output shown in the following example:

```
{
  "KeyId": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab",
```

```
"DeletionDate": 1598304792.0,  
"KeyState": "PendingDeletion",  
"PendingWindowInDays": 10  
}
```

Cancel key deletion

After you [schedule a KMS key for deletion](#), you can cancel the key deletion while it is still in the [pending deletion](#) state. You can cancel key deletion in the Amazon KMS console or by using the [CancelKeyDeletion](#) operation. After you cancel the pending deletion of a KMS key, the key state of the KMS key is Disabled. For more information on enabling the KMS key, see [Enable and disable keys](#).

Using the Amazon KMS console

To cancel key deletion

1. Open the Amazon KMS console at <https://console.amazonaws.cn/kms>.
2. To change the Amazon Web Services Region, use the Region selector in the upper-right corner of the page.
3. In the navigation pane, choose **Customer managed keys**.
4. Choose the check box next to the KMS key that you want to recover.
5. Choose **Key actions**, **Cancel key deletion**.

The KMS key status changes from **Pending deletion** to **Disabled**. To use the KMS key, you must [enable it](#).

Using the Amazon KMS API

Use the [aws kms cancel-key-deletion](#) command to cancel key deletion from the Amazon CLI as shown in the following example.

```
$ aws kms cancel-key-deletion --key-id 1234abcd-12ab-34cd-56ef-1234567890ab
```

When used successfully, the Amazon CLI returns output like the output shown in the following example:

```
{
```

```
"KeyId": "arn:aws:kms:us-west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab"
}
```

The status of the KMS key changes from **Pending Deletion** to **Disabled**. To use the KMS key, you must [enable it](#).

Create an alarm that detects use of a KMS key pending deletion

You can combine the features of Amazon CloudTrail, Amazon CloudWatch Logs, and Amazon Simple Notification Service (Amazon SNS) to create an Amazon CloudWatch alarm that notifies you when someone in your account tries to use a KMS key that is pending deletion. If you receive this notification, you might want to cancel deletion of the KMS key and reconsider your decision to delete it.

The following procedures create an alarm that notifies you whenever the "*Key ARN* is pending deletion" error message is written to your CloudTrail log files. This error message indicates that a person or application tried to use the KMS key in a [cryptographic operation](#). Because the notification is linked to the error message, it is not triggered when you use API operations that are permitted on KMS keys that are pending deletion, such as `ListKeys`, `CancelKeyDeletion`, and `PutKeyPolicy`. To see a list of the Amazon KMS API operations that return this error message, see [Key states of Amazon KMS keys](#).

The notification email that you receive does not list the KMS key or the cryptographic operation. You can find that information in [your CloudTrail log](#). Instead, the email reports that the alarm state changed from **OK** to **Alarm**. For more information about CloudWatch alarms and state changes, see [Using Amazon CloudWatch alarms](#) in the *Amazon CloudWatch User Guide*.

Warning

This Amazon CloudWatch alarm cannot detect use of the public key of an asymmetric KMS key outside of Amazon KMS. For details about the special risks of deleting asymmetric KMS keys used for public key cryptography, including creating ciphertexts that cannot be decrypted, see [Deleting asymmetric KMS keys](#).

In this procedure, you create a CloudWatch log group metric filter that finds instances of the pending deletion exception. Then, you create a CloudWatch alarm based on the log group metric.

For information about log group metric filters, see [Creating metrics from log events using filters](#) in the Amazon CloudWatch Logs User Guide.

1. Create a CloudWatch metric filter that parses CloudTrail logs.

Follow the instructions in [Create a metric filter for a log group](#) using the following required values. For other fields, accept the default values and provide names as requested.

Field	Value
Filter pattern	<code>{ \$.eventSource = kms* && \$.errorMessage = "* is pending deletion."}</code>
Metric value	1

2. Create a CloudWatch alarm based on the metric filter that you created in Step 1.

Follow the instructions in [Create a CloudWatch alarm based on a log group-metric filter](#) using the following required values. For other fields, accept the default values and provide names as requested.

Field	Value
Metric filter	The name of the metric filter that you created in Step 1.
Threshold type	Static
Conditions	Whenever <i>metric-name</i> is Greater/Equal than 1
Data points to alarm	1 out of 1
Missing data treatment	Treat missing data as good (not breaching threshold)

After you complete this procedure, you will receive a notification each time your new CloudWatch alarm enters the ALARM state. If you receive a notification for this alarm, it might mean that a KMS key that is scheduled for deletion is still needed to encrypt or decrypt data. In that case, [cancel deletion of the KMS key](#) and reconsider your decision to delete it.

Determine past usage of a KMS key

Before deleting a KMS key, you might want to know how many ciphertexts were encrypted under that key. Amazon KMS does not store this information, and does not store any of the ciphertexts. Knowing how a KMS key was used in the past might help you decide whether or not you will need it in the future. This topic suggest several strategies that can help you determine the past usage of a KMS key.

Warning

These strategies for determining past and actual usage are effective only for Amazon users and Amazon KMS operations. They cannot detect use of the public key of an asymmetric KMS key outside of Amazon KMS. For details about the special risks of deleting asymmetric KMS keys used for public key cryptography, including creating ciphertexts that cannot be decrypted, see [Deleting asymmetric KMS keys](#).

Topics

- [Examine KMS key permissions to determine the scope of potential usage](#)
- [Examine Amazon CloudTrail logs to determine actual usage](#)

Examine KMS key permissions to determine the scope of potential usage

Determining who or what currently has access to a KMS key might help you determine how widely the KMS key was used and whether it is still needed. To learn how to determine who or what currently has access to a KMS key, go to [Determining access to Amazon KMS keys](#).

Examine Amazon CloudTrail logs to determine actual usage

You might be able to use a KMS key usage history to help you determine whether you have ciphertexts encrypted under a particular KMS key.

All Amazon KMS API activity is recorded in Amazon CloudTrail log files. If you have [created a CloudTrail trail](#) in the region where your KMS key is located, you can examine your CloudTrail log files to view a history of all Amazon KMS API activity for a particular KMS key. If you don't have

a trail, you can still view recent events in your [CloudTrail event history](#). For details about how Amazon KMS uses CloudTrail, see [Logging Amazon KMS API calls with Amazon CloudTrail](#).

The following examples show CloudTrail log entries that are generated when a KMS key is used to protect an object stored in Amazon Simple Storage Service (Amazon S3). In this example, the object is uploaded to Amazon S3 using [Protecting data using server-side encryption with KMS keys \(SSE-KMS\)](#). When you upload an object to Amazon S3 with SSE-KMS, you specify the KMS key to use for protecting the object. Amazon S3 uses the Amazon KMS [GenerateDataKey](#) operation to request a unique data key for the object, and this request event is logged in CloudTrail with an entry similar to the following:

```
{
  "eventVersion": "1.02",
  "userIdentity": {
    "type": "AssumedRole",
    "principalId": "AROACKCEVSQ6C2EXAMPLE:example-user",
    "arn": "arn:aws:sts::111122223333:assumed-role/Admins/example-user",
    "accountId": "111122223333",
    "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
    "sessionContext": {
      "attributes": {
        "mfaAuthenticated": "false",
        "creationDate": "2015-09-10T23:12:48Z"
      },
      "sessionIssuer": {
        "type": "Role",
        "principalId": "AROACKCEVSQ6C2EXAMPLE",
        "arn": "arn:aws:iam::111122223333:role/Admins",
        "accountId": "111122223333",
        "userName": "Admins"
      }
    }
  },
  "invokedBy": "internal.amazonaws.com"
},
"eventTime": "2015-09-10T23:58:18Z",
"eventSource": "kms.amazonaws.com",
"eventName": "GenerateDataKey",
"awsRegion": "us-west-2",
"sourceIPAddress": "internal.amazonaws.com",
"userAgent": "internal.amazonaws.com",
"requestParameters": {
  "encryptionContext": {"aws:s3:arn": "arn:aws:s3:::example_bucket/example_object"},
```

```

    "keySpec": "AES_256",
    "keyId": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab"
  },
  "responseElements": null,
  "requestID": "cea04450-5817-11e5-85aa-97ce46071236",
  "eventID": "80721262-21a5-49b9-8b63-28740e7ce9c9",
  "readOnly": true,
  "resources": [{
    "ARN": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab",
    "accountId": "111122223333"
  }],
  "eventType": "AwsApiCall",
  "recipientAccountId": "111122223333"
}

```

When you later download this object from Amazon S3, Amazon S3 sends a Decrypt request to Amazon KMS to decrypt the object's data key using the specified KMS key. When you do this, your CloudTrail log files include an entry similar to the following:

```

{
  "eventVersion": "1.02",
  "userIdentity": {
    "type": "AssumedRole",
    "principalId": "AROACKCEVSQ6C2EXAMPLE:example-user",
    "arn": "arn:aws:sts::111122223333:assumed-role/Admins/example-user",
    "accountId": "111122223333",
    "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
    "sessionContext": {
      "attributes": {
        "mfaAuthenticated": "false",
        "creationDate": "2015-09-10T23:12:48Z"
      },
      "sessionIssuer": {
        "type": "Role",
        "principalId": "AROACKCEVSQ6C2EXAMPLE",
        "arn": "arn:aws:iam::111122223333:role/Admins",
        "accountId": "111122223333",
        "userName": "Admins"
      }
    }
  },
  "invokedBy": "internal.amazonaws.com"
}

```



```
},
"eventTime": "2015-09-10T23:58:39Z",
"eventSource": "kms.amazonaws.com",
"eventName": "Decrypt",
"awsRegion": "us-west-2",
"sourceIPAddress": "internal.amazonaws.com",
"userAgent": "internal.amazonaws.com",
"requestParameters": {
  "encryptionContext": {"aws:s3:arn": "arn:aws:s3:::example_bucket/example_object"}},
"responseElements": null,
"requestID": "db750745-5817-11e5-93a6-5b87e27d91a0",
"eventID": "ae551b19-8a09-4cfc-a249-205ddba330e3",
"readOnly": true,
"resources": [{
  "ARN": "arn:aws:kms:us-west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab",
  "accountId": "111122223333"
}],
"eventType": "AwsApiCall",
"recipientAccountId": "111122223333"
}
```

All Amazon KMS API activity is logged by CloudTrail. By evaluating these log entries, you might be able to determine the past usage of a particular KMS key, and this might help you determine whether or not you want to delete it.

To see more examples of how Amazon KMS API activity appears in your CloudTrail log files, go to [Logging Amazon KMS API calls with Amazon CloudTrail](#). For more information about CloudTrail go to the [Amazon CloudTrail User Guide](#).

Delete imported key material

You can delete the imported key material from a KMS key at any time. Also, when imported key material with an expiration date expires, Amazon KMS deletes the key material. In either case, when the key material is deleted, the [key state](#) of the KMS key changes to *pending import*, and the KMS key can't be used in any cryptographic operations until you [reimport the same key material](#). (You cannot import any other key material into the KMS key.)

Along with disabling the KMS key and withdrawing permissions, deleting key material can be used as a strategy to quickly, but temporarily, halt the use of the KMS key. In contrast, scheduling the deletion of a KMS key with imported key material also quickly halts the use of the KMS key.

However, if the deletion is not canceled during the waiting period, the KMS key, the key material, and all key metadata are permanently deleted. For details, see [Deleting KMS keys with imported key material](#).

To delete key material, you can use the Amazon KMS console or the [DeleteImportedKeyMaterial](#) API operation. Amazon KMS records an entry in your Amazon CloudTrail log when you [delete imported key material](#) and when [Amazon KMS deletes expired key material](#).

How deleting key material affects Amazon services

When you delete key material, the KMS key with no key material becomes unusable right away (subject to eventual consistency). However, resources encrypted with [data keys](#) protected by the KMS key are not affected until the KMS key is used again, such as to decrypt the data key. This issue affects Amazon Web Services services, many of which use data keys to protect your resources. For details, see [How unusable KMS keys affect data keys](#).

Using the Amazon KMS console

You can use the Amazon KMS console to delete key material.

1. Sign in to the Amazon Web Services Management Console and open the Amazon Key Management Service (Amazon KMS) console at <https://console.amazonaws.cn/kms>.
2. To change the Amazon Web Services Region, use the Region selector in the upper-right corner of the page.
3. In the navigation pane, choose **Customer managed keys**.
4. Do one of the following:
 - Select the check box for a KMS key with imported key material. Choose **Key actions**, **Delete key material**.
 - Choose the alias or key ID of a KMS key with imported key material. Choose the **Key material** tab and then choose **Delete key material**.
5. Confirm that you want to delete the key material and then choose **Delete key material**. The KMS key's status, which corresponds to its [key state](#), changes to **Pending import**.

Using the Amazon KMS API

To use the [Amazon KMS API](#) to delete key material, send a [DeleteImportedKeyMaterial](#) request. The following example shows how to do this with the [Amazon CLI](#).

Replace *1234abcd-12ab-34cd-56ef-1234567890ab* with the key ID of the KMS key whose key material you want to delete. You can use the KMS key's key ID or ARN but you cannot use an alias for this operation.

```
$ aws kms delete-imported-key-material --key-id 1234abcd-12ab-34cd-56ef-1234567890ab
```

Generate data keys

Data keys are symmetric keys you can use to encrypt data, including large amounts of data and other data encryption keys. Unlike symmetric KMS keys, which can't be downloaded, data keys are returned to you for use outside of Amazon KMS.

When Amazon KMS generates data keys, it returns a plaintext data key for immediate use (optional) and an encrypted copy of the data key that you can safely store with the data. When you are ready to decrypt the data, you first ask Amazon KMS to decrypt the encrypted data key.

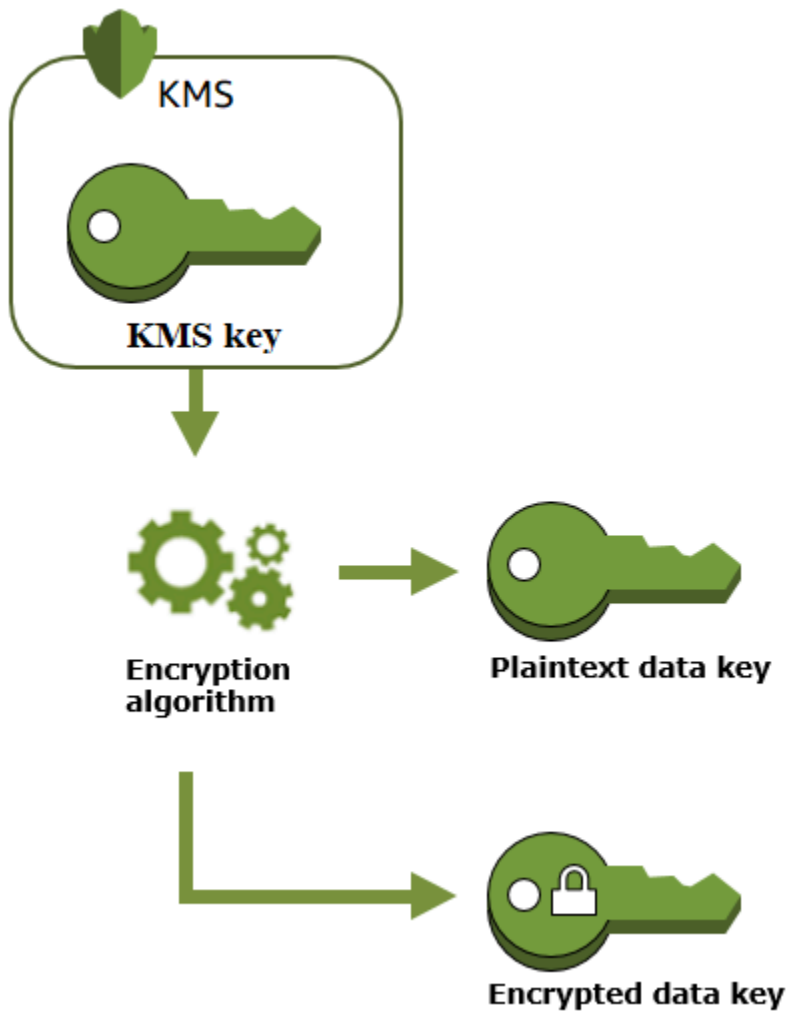
Amazon KMS generates, encrypts, and decrypts data keys. However, Amazon KMS does not store, manage, or track your data keys, or perform cryptographic operations with data keys. You must use and manage data keys outside of Amazon KMS. For help using the data keys securely, see the [Amazon Encryption SDK](#).

Topics

- [Create a data key](#)
- [How cryptographic operations with data keys work](#)
- [How unusable KMS keys affect data keys](#)

Create a data key

To create a data key, call the [GenerateDataKey](#) operation. Amazon KMS generates the data key. Then it encrypts a copy of the data key under a [symmetric encryption KMS key](#) that you specify. The operation returns a plaintext copy of the data key and the copy of the data key encrypted under the KMS key. The following image shows this operation.



Amazon KMS also supports the [GenerateDataKeyWithoutPlaintext](#) operation, which returns only an encrypted data key. When you need to use the data key, ask Amazon KMS to [decrypt](#) it.

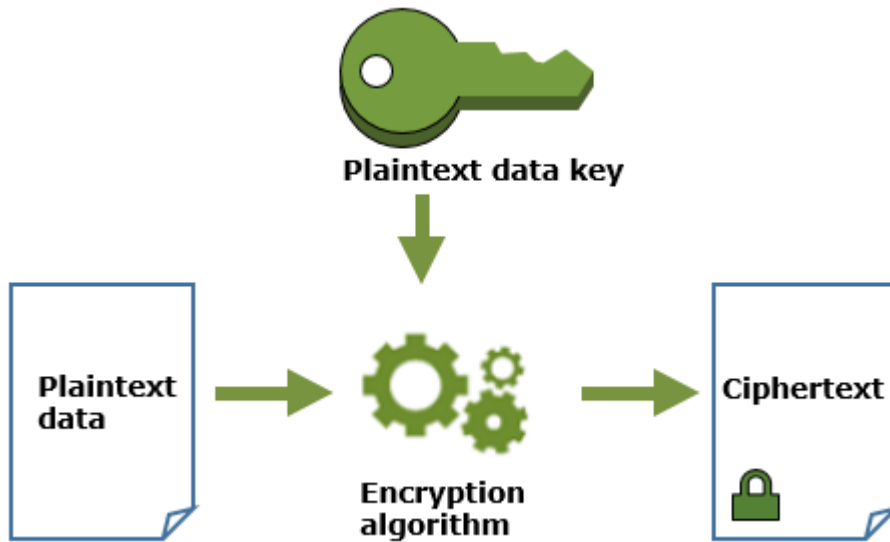
How cryptographic operations with data keys work

The following topics explain how data keys generated by a [GenerateDataKey](#) or [GenerateDataKeyWithoutPlaintext](#) operation work.

Encrypt data with a data key

Amazon KMS cannot use a data key to encrypt data. But you can use the data key outside of Amazon KMS, such as by using OpenSSL or a cryptographic library like the [Amazon Encryption SDK](#).

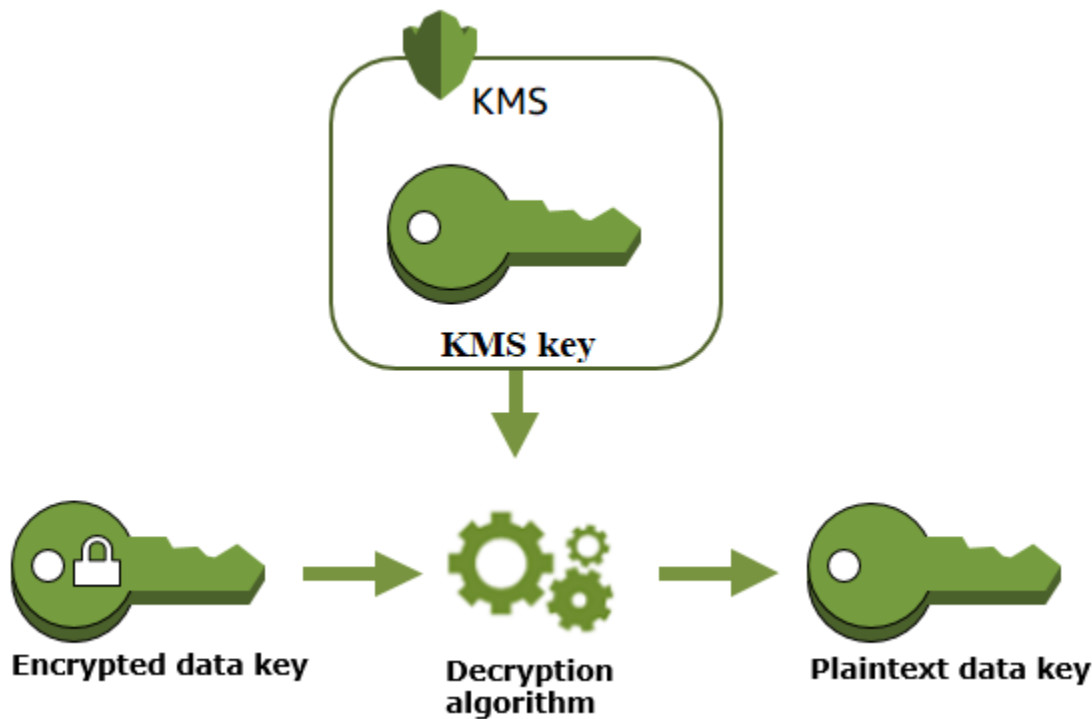
After using the plaintext data key to encrypt data, remove it from memory as soon as possible. You can safely store the encrypted data key with the encrypted data so it is available to decrypt the data.



Decrypt data with a data key

To decrypt your data, pass the encrypted data key to the [Decrypt](#) operation. Amazon KMS uses your KMS key to decrypt the data key and then returns the plaintext data key. Use the plaintext data key to decrypt your data and then remove the plaintext data key from memory as soon as possible.

The following diagram shows how to use the Decrypt operation to decrypt an encrypted data key.



How unusable KMS keys affect data keys

When a KMS key becomes unusable, the effect is almost immediate (subject to eventual consistency). The [key state](#) of the KMS key changes to reflect its new condition, and all requests to use the KMS key in [cryptographic operations](#) fail.

However, the effect on data keys encrypted by the KMS key, and on data encrypted by the data key, is delayed until the KMS key is used again, such as to decrypt the data key.

KMS keys can become unusable for a variety of reasons, including the following actions that you might perform.

- [Disabling the KMS key](#)
- [Scheduling the KMS key for deletion](#)
- [Deleting the key material](#) from a KMS key with imported key material, or allowing the imported key material to expire.
- [Disconnecting the Amazon CloudHSM key store](#) that hosts the KMS key, or [deleting the key from the Amazon CloudHSM cluster](#) that serves as key material for the KMS key.

- [Disconnecting the external key store](#) that hosts the KMS key, or any other action that interferes with encryption and decryption requests to the external key store proxy, including deleting the external key from its external key manager.

This effect is particularly important for the many Amazon Web Services services that use data keys to protect the resources that the service manages. The following example uses Amazon Elastic Block Store (Amazon EBS) and Amazon Elastic Compute Cloud (Amazon EC2). Different Amazon Web Services services use data keys in different ways. For details, see the Data protection section of the Security chapter for the Amazon Web Services service.

For example, consider this scenario:

1. You [create an encrypted EBS volume](#) and specify a KMS key to protect it. Amazon EBS asks Amazon KMS to use your KMS key to [generate an encrypted data key](#) for the volume. Amazon EBS stores the encrypted data key with the volume's metadata.
2. When you attach the EBS volume to an EC2 instance, Amazon EC2 uses your KMS key to decrypt the EBS volume's encrypted data key. Amazon EC2 uses the data key in the Nitro hardware, which is responsible for encrypting all disk I/O to the EBS volume. The data key persists in the Nitro hardware while the EBS volume is attached to the EC2 instance.
3. You perform an action that makes the KMS key unusable. This has no immediate effect on the EC2 instance or the EBS volume. Amazon EC2 uses the data key—not the KMS key—to encrypt all disk I/O while the volume is attached to the instance.
4. However, when the encrypted EBS volume is detached from the EC2 instance, Amazon EBS removes the data key from the Nitro hardware. The next time the encrypted EBS volume is attached to an EC2 instance, the attachment fails, because Amazon EBS cannot use the KMS key to decrypt the volume's encrypted data key. To use the EBS volume again, you must make the KMS key usable again.

Generate data key pairs

An asymmetric KMS key represents a *data key pair*. Data key pairs are asymmetric data keys consisting of a mathematically-related public key and private key. They are designed for use in client-side encryption and decryption, signing and verification outside of Amazon KMS, or to establish a shared secret between two peers.

Unlike the data key pairs that tools like OpenSSL generate, Amazon KMS protects the private key in each data key pair under a symmetric encryption KMS key in Amazon KMS that you specify. However, Amazon KMS does not store, manage, or track your data key pairs, or perform cryptographic operations with data key pairs. You must use and manage data key pairs outside of Amazon KMS.

Topics

- [Create a data key pair](#)
- [How cryptographic operations with data key pairs work](#)

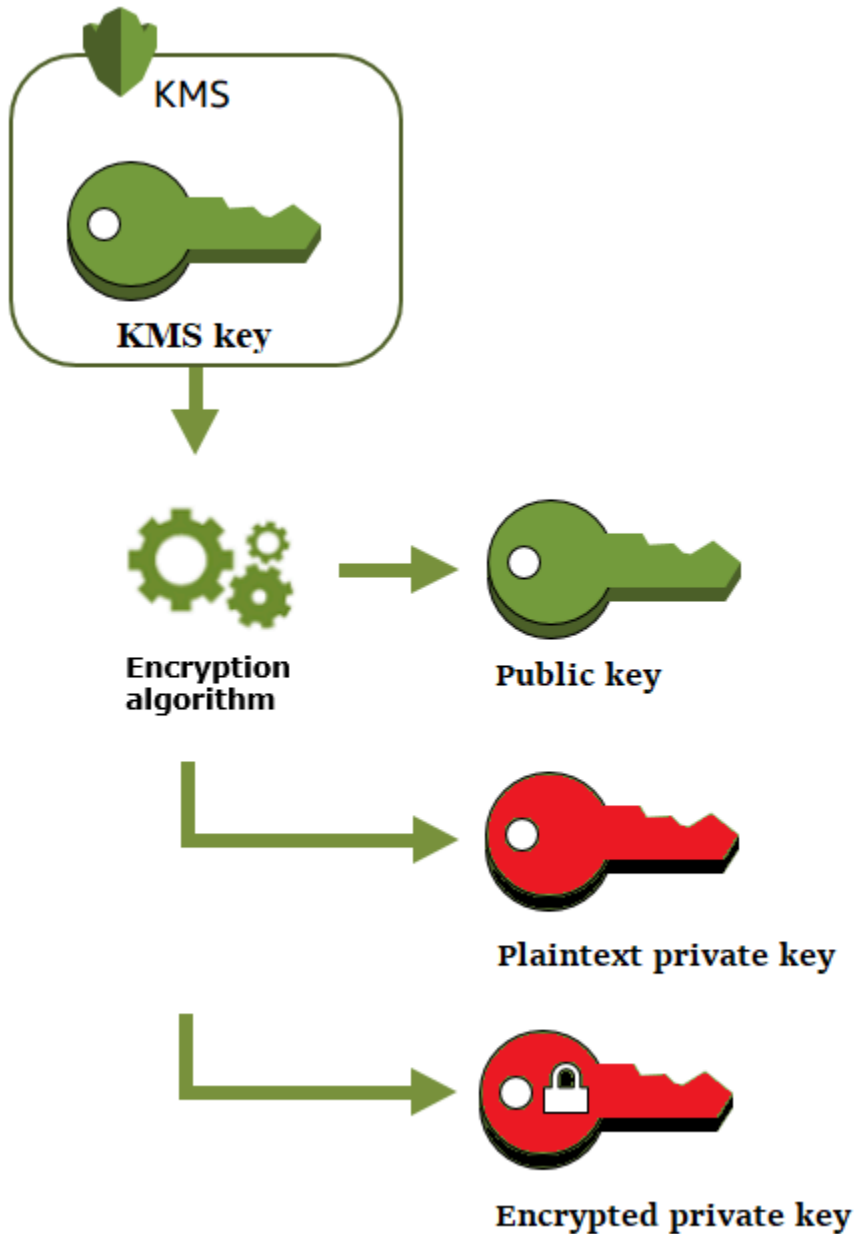
Create a data key pair

To create a data key pair, call the [GenerateDataKeyPair](#) or [GenerateDataKeyPairWithoutPlaintext](#) operations. Specify the [symmetric encryption KMS key](#) you want to use to encrypt the private key.

`GenerateDataKeyPair` returns a plaintext public key, a plaintext private key, and an encrypted private key. Use this operation when you need a plaintext private key immediately, such as to generate a digital signature.

`GenerateDataKeyPairWithoutPlaintext` returns a plaintext public key and an encrypted private key, but not a plaintext private key. Use this operation when you don't need a plaintext private key immediately, such as when you're encrypting with a public key. Later, when you need a plaintext private key to decrypt the data, you can call the [Decrypt](#) operation.

The following image shows the `GenerateDataKeyPair` operation. The `GenerateDataKeyPairWithoutPlaintext` operation omits the plaintext private key.



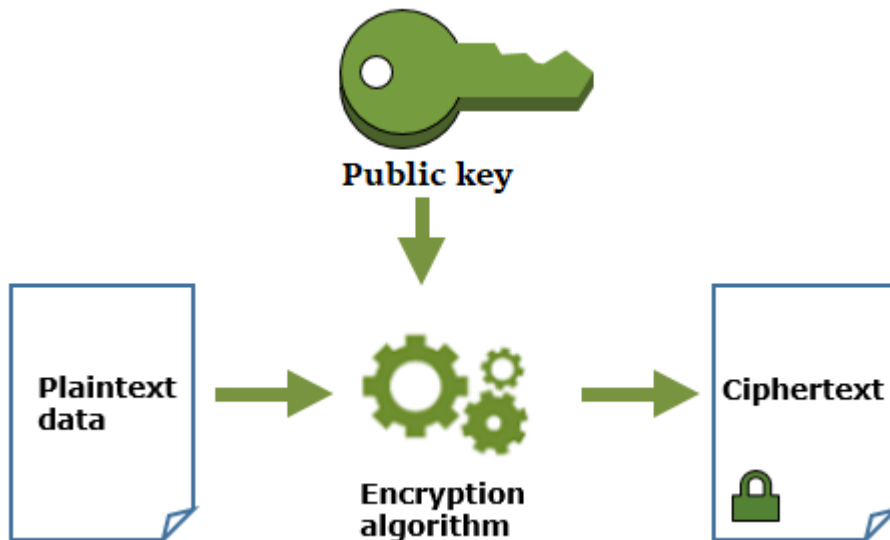
How cryptographic operations with data key pairs work

The following topics explain what cryptographic operations you can perform with data key pairs generated by a [GenerateDataKeyPair](#) or [GenerateDataKeyPairWithoutPlaintext](#) operation and how they work.

Encrypt data with a data key pair

When you encrypt with a data key pair, you use the public key of the pair to encrypt the data and the private key of the same pair to decrypt the data. Typically, you use data key pairs when many parties need to encrypt data that only the party with the private key can decrypt.

The parties with the public key use that key to encrypt data, as shown in the following diagram.

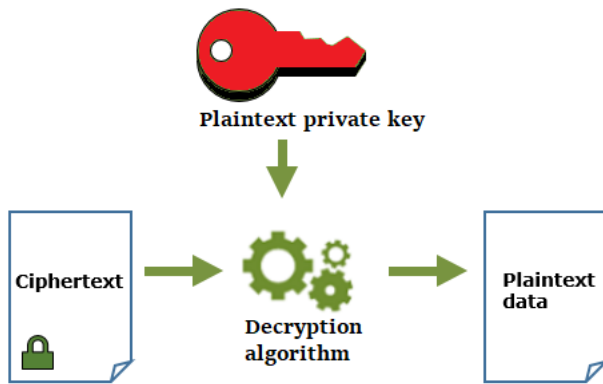


Decrypt data with a data key pair

To decrypt your data, use the private key in the data key pair. For the operation to succeed, the public and private keys must be from the same data key pair, and you must use the same encryption algorithm.

To decrypt the encrypted private key, pass it to the [Decrypt](#) operation. Use the plaintext private key to decrypt the data. Then remove the plaintext private key from memory as soon as possible.

The following diagram shows how to use the private key in a data key pair to decrypt ciphertext.



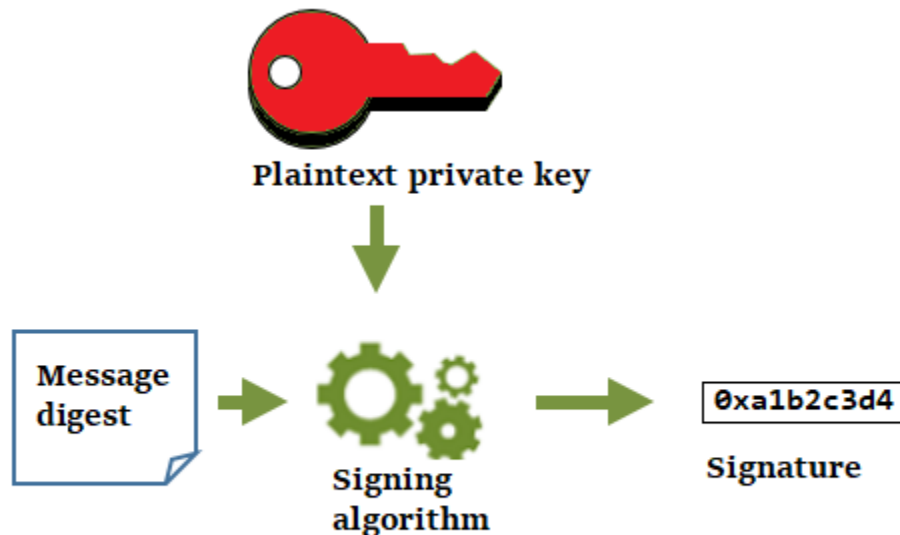
Sign messages with a data key pair

To generate a cryptographic signature for a message, use the private key in the data key pair. Anyone with the public key can use it to verify that the message was signed with your private key and that it has not changed since it was signed.

If you encrypt your private key, pass the encrypted private key to the [Decrypt](#) operation. Amazon KMS uses your KMS key to decrypt the data key and then it returns the plaintext private key. Use the plaintext private key to generate the signature. Then remove the plaintext private key from memory as soon as possible.

To sign a message, create a message digest using a cryptographic hash function, such as the [dgst](#) command in OpenSSL. Then, pass your plaintext private key to the signing algorithm. The result is a signature that represents the contents of the message. (You might be able to sign shorter messages without first creating a digest. The maximum message size varies with the signing tool you use.)

The following diagram shows how to use the private key in a data key pair to sign a message.

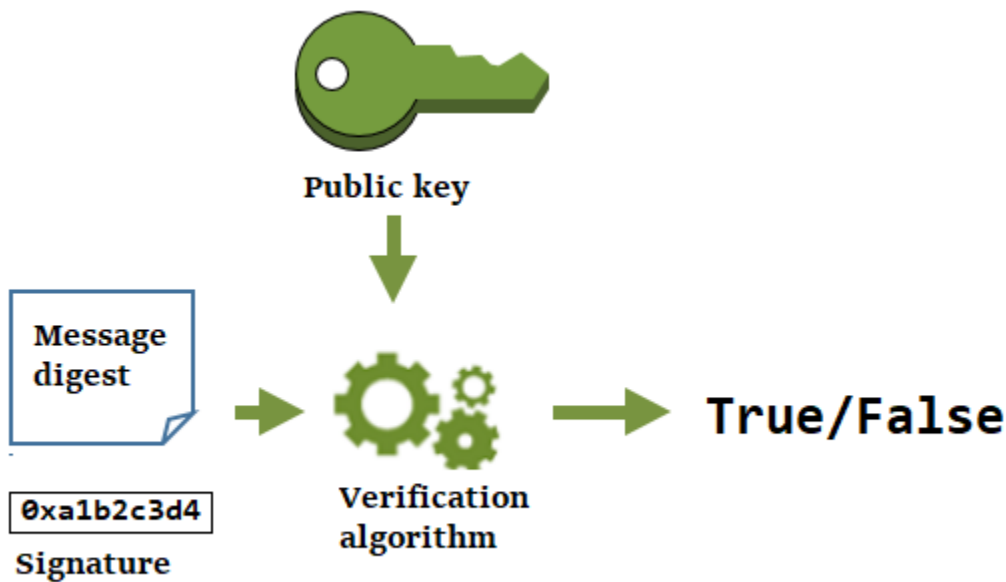


Verify a signature with a data key pair

Anyone who has the public key in your data key pair can use it to verify the signature that you generated with your private key. Verification confirms that an authorized user signed the message with the specified private key and signing algorithm, and the message hasn't changed since it was signed.

To be successful, the party verifying the signature must generate the same type of digest, use the same algorithm, and use the public key that corresponds to the private key used to sign the message.

The following diagram shows how to use the public key in a data key pair to verify a message signature.



Derive a shared secret with data key pairs

Key agreement enables two peers, each having an elliptic-curve public–private key pair, to establish a shared secret over an insecure channel. To [derive a shared secret](#), the two peers must exchange their public keys over the insecure communication channel (like the internet). Then, each party uses their *private key* and their peer's *public key* to calculate the same shared secret using a key agreement algorithm. You can use the shared secret value to derive a symmetric key that can encrypt and decrypt data that is sent between the two peers, or that can generate and verify HMACs.

Note

Amazon KMS strongly recommends verifying that the public key you receive came from the expected party before using it to derive a shared secret.

Perform offline operations with public keys

In an asymmetric KMS key, the private key is created in Amazon KMS and never leaves Amazon KMS unencrypted. To use the private key, you must call Amazon KMS. You can use the public key within Amazon KMS by calling the Amazon KMS API operations. Or, you can [download the public key](#) and share for use outside of Amazon KMS.

You might share a public key to let others encrypt data outside of Amazon KMS that you can decrypt only with your private key. Or, to allow others to verify a digital signature outside of Amazon KMS that you have generated with your private key. Or, to share your public key with a peer to derive a shared secret.

When you use the public key in your asymmetric KMS key within Amazon KMS, you benefit from the authentication, authorization, and logging that are part of every Amazon KMS operation. You also reduce the risk of encrypting data that cannot be decrypted. These features are not effective outside of Amazon KMS. For details, see [Special considerations for downloading public keys](#).

Tip

Looking for data keys or SSH keys? This topic explains how to manage asymmetric keys in Amazon Key Management Service, where the private key is not exportable. For exportable data key pairs where the private key is protected by a symmetric encryption KMS key, see [GenerateDataKeyPair](#). For help with downloading the public key associated with an Amazon EC2 instance, see *Retrieving the public key* in the [Amazon EC2 User Guide](#) and [Amazon EC2 User Guide](#).

Topics

- [Special considerations for downloading public keys](#)
- [Download public key](#)
- [Example offline operations](#)

Special considerations for downloading public keys

To protect your KMS keys, Amazon KMS provides access controls, authenticated encryption, and detailed logs of every operation. Amazon KMS also allows you to prevent the use of KMS keys,

temporarily or permanently. Finally, Amazon KMS operations are designed to minimize of risk of encrypting data that cannot be decrypted. These features are not available when you use downloaded public keys outside of Amazon KMS.

Authorization

[Key policies](#) and [IAM policies](#) that control access to the KMS key within Amazon KMS have no effect on operations performed outside of Amazon. Any user who can get the public key can use it outside of Amazon KMS even if they don't have permission to encrypt data or verify signatures with the KMS key.

Key usage restrictions

Key usage restrictions are not effective outside of Amazon KMS. If you call the [Encrypt](#) operation with a KMS key that has a KeyUsage of SIGN_VERIFY, the Amazon KMS operation fails. But if you encrypt data outside of Amazon KMS with a public key from a KMS key with a KeyUsage of SIGN_VERIFY or KEY_AGREEMENT, the data cannot be decrypted.

Algorithm restrictions

Restrictions on the encryption and signing algorithms that Amazon KMS supports are not effective outside of Amazon KMS. If you encrypt data with the public key from a KMS key outside of Amazon KMS, and use an encryption algorithm that Amazon KMS does not support, the data cannot be decrypted.

Disabling and deleting KMS keys

Actions that you can take to prevent the use of KMS key in a cryptographic operation within Amazon KMS do not prevent anyone from using the public key outside of Amazon KMS. For example, disabling a KMS key, scheduling deletion of a KMS key, deleting a KMS key, or deleting the key material from a KMS key have no effect on a public key outside of Amazon KMS. If you delete an asymmetric KMS key or delete or lose its key material, data that you encrypt with a public key outside of Amazon KMS is unrecoverable.

Logging

Amazon CloudTrail logs that record every Amazon KMS operation, including the request, response, date, time, and authorized user, do not record the use of the public key outside of Amazon KMS.

Offline verification with SM2 key pairs (China Regions only)

To verify a signature outside of Amazon KMS with an SM2 public key, you must specify the distinguishing ID. By default, Amazon KMS uses 1234567812345678 as the distinguishing ID. For more information, see [Offline verification with SM2 key pairs \(China Regions only\)](#).

Download public key

You can download the public key from an asymmetric KMS key pair in the Amazon KMS console or by using the [GetPublicKey](#) operation. To download the public key, you must have `kms:GetPublicKey` permission on the asymmetric KMS key.

The public key that Amazon KMS returns is a DER-encoded X.509 public key, also known as SubjectPublicKeyInfo (SPKI), as defined in [RFC 5280](#). When you use the HTTP API or the Amazon CLI, the value is Base64-encoded. Otherwise, it is not Base64-encoded.

To download the public key from an asymmetric KMS key pair, you need `kms:GetPublicKey` permissions. For more information about Amazon KMS permissions, see the [Permissions reference](#).

Using the Amazon KMS console

You can use the Amazon Web Services Management Console to view, copy, and download the public key from an asymmetric KMS key in your Amazon Web Services account. To download the public key from an asymmetric KMS key in different Amazon Web Services account, use the Amazon KMS API.

1. Sign in to the Amazon Web Services Management Console and open the Amazon Key Management Service (Amazon KMS) console at <https://console.amazonaws.cn/kms>.
2. To change the Amazon Web Services Region, use the Region selector in the upper-right corner of the page.
3. In the navigation pane, choose **Customer managed keys**.
4. Choose the alias or key ID of an asymmetric KMS key.
5. Choose the **Cryptographic configuration** tab. Record the values of the **Key spec**, **Key usage**, and **Encryption algorithms** or **Signing Algorithms** fields. You'll need to use these values to use the public key outside of Amazon KMS. Be sure to share this information when you share the public key.
6. Choose the **Public key** tab.

7. To copy the public key to your clipboard, choose **Copy**. To download the public key to a file, choose **Download**.

Using the Amazon KMS API

The [GetPublicKey](#) operation returns the public key in an asymmetric KMS key. It also returns critical information that you need to use the public key correctly outside of Amazon KMS, including the key usage and encryption algorithms. Be sure to save these values and share them whenever you share the public key.

The examples in this section use the [Amazon Command Line Interface \(Amazon CLI\)](#), but you can use any supported programming language.

To specify a KMS key, use its [key ID](#), [key ARN](#), [alias name](#), or [alias ARN](#). When using an alias name, prefix it with **alias/**. To specify a KMS key in a different Amazon Web Services account, you must use its key ARN or alias ARN.

Before running this command, replace the example alias name with a valid identifier for the KMS key. To run this command, you must have `kms:GetPublicKey` permissions on the KMS key.

```
$ aws kms get-public-key --key-id alias/example_RSA_3072

{
  "KeySpec": "RSA_3072",
  "KeyId": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab",
  "KeyUsage": "ENCRYPT_DECRYPT",
  "EncryptionAlgorithms": [
    "RSAES_OAEP_SHA_1",
    "RSAES_OAEP_SHA_256"
  ],
  "PublicKey": "MIIBojANBgkqhkiG..."
}
```

Example offline operations

After [downloading the public key](#) of your asymmetric KMS key pair, you can share it with others and use it to perform offline operations.

Amazon CloudTrail logs that record every Amazon KMS operation, including the request, response, date, time, and authorized user, do not record the use of the public key outside of Amazon KMS.

This topic provides example offline operations and details the tools Amazon KMS provides to make offline operations easier.

Topics

- [Deriving shared secrets offline](#)
- [Offline verification with SM2 key pairs \(China Regions only\)](#)

Deriving shared secrets offline

You can [download the public key](#) of your ECC key pair for use in offline operations, that is, operations outside of Amazon KMS.

The following [OpenSSL](#) walkthrough demonstrates one method of deriving a shared secret outside of Amazon KMS using the public key of an ECC KMS key pair and a private key created with OpenSSL.

1. Create an ECC key pair in OpenSSL and prepare it for use with Amazon KMS.

```
// Create an ECC key pair in OpenSSL and save the private key in
openssl_ecc_key_priv.pem
export OPENSSL_CURVE_NAME="P-256"
export KMS_CURVE_NAME="ECC_NIST_P256"

export OPENSSL_KEY1_PRIV_PEM="openssl_ecc_key1_priv.pem"
openssl ecparam -name ${OPENSSL_CURVE_NAME} -genkey -out ${OPENSSL_KEY1_PRIV_PEM}

// Derive the public key from the private key
export OPENSSL_KEY1_PUB_PEM="openssl_ecc_key1_pub.pem"
openssl ec -in ${OPENSSL_KEY1_PRIV_PEM} -pubout -outform pem \
  -out ${OPENSSL_KEY1_PUB_PEM}

// View the PEM file containing the public key and extract the public key as a
// Base64 encoded string into OPENSSL_KEY1_PUB_BASE64 for use with Amazon KMS
export OPENSSL_KEY1_PUB_BASE64=`cat ${OPENSSL_KEY1_PUB_PEM} | \
  tee /dev/stderr | grep -v "PUBLIC KEY" | tr -d "\n"`
```

2. Create an ECC key agreement key pair in Amazon KMS and prepare it for use with OpenSSL.

```
// Create a KMS key on the same curve as the key pair from step 1
// with a key usage of KEY_AGREEMENT
// Save its ARN in KMS_KEY1_ARN.
export KMS_KEY1_ARN=`aws kms create-key --key-spec ${KMS_CURVE_NAME} \
  --key-usage KEY_AGREEMENT | tee /dev/stderr | jq -r .KeyMetadata.Arn`

// Download the public key and save the Base64-encoded version in KMS_KEY1_PUB_BASE64

export KMS_KEY1_PUB_BASE64=`aws kms get-public-key --key-id ${KMS_KEY1_ARN} | \
  tee /dev/stderr | jq -r .PublicKey`

// Create a PEM file for the public KMS key for use with OpenSSL
export KMS_KEY1_PUB_PEM="aws_kms_ecdh_key1_pub.pem"
echo "-----BEGIN PUBLIC KEY-----" > ${KMS_KEY1_PUB_PEM}
echo ${KMS_KEY1_PUB_BASE64} | fold -w 64 >> ${KMS_KEY1_PUB_PEM}
echo "-----END PUBLIC KEY-----" >> ${KMS_KEY1_PUB_PEM}
```

3. Derive shared secret in OpenSSL using the private key in OpenSSL and the public KMS key.

```
export OPENSSL_SHARED_SECRET1_BIN="openssl_shared_secret1.bin"
openssl pkeyutl -derive -inkey ${OPENSSL_KEY1_PRIV_PEM} \
  -peerkey ${KMS_KEY1_PUB_PEM} -out ${OPENSSL_SHARED_SECRET1_BIN}
```

Offline verification with SM2 key pairs (China Regions only)

To verify a signature outside of Amazon KMS with an SM2 public key, you must specify the distinguishing ID. When you pass a raw message, [MessageType:RAW](#), to the [Sign](#) API, Amazon KMS uses the default distinguishing ID, 1234567812345678, defined by OSCCA in GM/T 0009-2012. You cannot specify your own distinguishing ID within Amazon KMS.

However, if you are generating a message digest outside of Amazon, you can specify your own distinguishing ID, then pass the message digest, [MessageType:DIGEST](#), to Amazon KMS to sign. To do this, change the `DEFAULT_DISTINGUISHING_ID` value in the `SM2OfflineOperationHelper` class. The distinguishing ID you specify can be any string up to 8,192 characters long. After Amazon KMS signs the message digest, you need either the message digest or the message and the distinguishing ID used to compute the digest to verify it offline.

⚠ Important

The `SM2OfflineOperationHelper` reference code is designed to be compatible with [Bouncy Castle](#) version 1.68. For help with other versions, contact [bouncycastle.org](https://www.bouncycastle.org).

SM2OfflineOperationHelper class

To help you with offline operations with SM2 keys, the `SM2OfflineOperationHelper` class for Java has methods that perform the tasks for you. You can use this helper class as a model for other cryptographic providers.

Within Amazon KMS, the raw ciphertext conversions and SM2DSA message digest calculations occur automatically. Not all cryptographic providers implement SM2 in the same way. Some libraries, like [OpenSSL](#) versions 1.1.1 and later, perform these actions automatically. Amazon KMS confirmed this behavior in testing with OpenSSL version 3.0. Use the following `SM2OfflineOperationHelper` class with libraries, like [Bouncy Castle](#), that require you to perform these conversions and calculations manually.

The `SM2OfflineOperationHelper` class provides methods for the following offline operations:

- **Message digest calculation**

To generate a message digest offline that you can use for offline verification, or that you can pass to Amazon KMS to sign, use the `calculateSM2Digest` method. The `calculateSM2Digest` method generates a message digest with the SM3 hashing algorithm. The [GetPublicKey](#) API returns your public key in binary format. You must parse the binary key into a Java `PublicKey`. Provide the parsed public key with the message. The method automatically combines your message with the default distinguishing ID, `1234567812345678`, but you can set your own distinguishing ID by changing the `DEFAULT_DISTINGUISHING_ID` value.

- **Verify**

To verify a signature offline, use the `offlineSM2DSAVerify` method. The `offlineSM2DSAVerify` method uses the message digest calculated from the specified distinguishing ID, and original message you provide to verify the digital signature. The [GetPublicKey](#) API returns your public key in binary format. You must parse the binary key into

a Java `PublicKey`. Provide the parsed public key with the original message and the signature you want to verify. For more details, see [Offline verification with SM2 key pairs](#).

- **Encrypt**

To encrypt plaintext offline, use the `offlineSM2PKEEncrypt` method. This method ensures the ciphertext is in a format Amazon KMS can decrypt. The `offlineSM2PKEEncrypt` method encrypts the plaintext, and then converts the raw ciphertext produced by SM2PKE to the ASN.1 format. The [GetPublicKey](#) API returns your public key in binary format. You must parse the binary key into a Java `PublicKey`. Provide the parsed public key with the plaintext that you want to encrypt.

If you're unsure whether you need to perform the conversion, use the following OpenSSL operation to test the format of your ciphertext. If the operation fails, you need to convert the ciphertext to the ASN.1 format.

```
openssl asn1parse -inform DER -in ciphertext.der
```

By default, the `SM2OfflineOperationHelper` class uses the default distinguishing ID, 1234567812345678, when generating message digests for SM2DSA operations.

```
package com.amazon.kms.utils;

import javax.crypto.BadPaddingException;
import javax.crypto.Cipher;
import javax.crypto.IllegalBlockSizeException;
import javax.crypto.NoSuchPaddingException;
import java.io.IOException;
import java.math.BigInteger;
import java.nio.ByteBuffer;
import java.nio.charset.StandardCharsets;
import java.security.InvalidKeyException;
import java.security.MessageDigest;
import java.security.NoSuchAlgorithmException;
import java.security.NoSuchProviderException;
import java.security.PrivateKey;
import java.security.PublicKey;

import org.bouncycastle.crypto.CryptoException;
import org.bouncycastle.jce.interfaces.ECPublicKey;
```

```
import java.util.Arrays;

import org.bouncycastle.asn1.ASN1EncodableVector;
import org.bouncycastle.asn1.ASN1Integer;
import org.bouncycastle.asn1.DEROctetString;
import org.bouncycastle.asn1.DERSequence;
import org.bouncycastle.asn1.gm.GMNamedCurves;
import org.bouncycastle.asn1.x9.X9ECParameters;
import org.bouncycastle.crypto.CipherParameters;
import org.bouncycastle.crypto.params.ParametersWithID;
import org.bouncycastle.crypto.params.ParametersWithRandom;
import org.bouncycastle.crypto.signers.SM2Signer;
import org.bouncycastle.jcajce.provider.asymmetric.util.ECUtil;

public class SM2OfflineOperationHelper {
    // You can change the DEFAULT_DISTINGUISHING_ID value to set your own
    // distinguishing ID,
    // the DEFAULT_DISTINGUISHING_ID can be any string up to 8,192 characters long.
    private static final byte[] DEFAULT_DISTINGUISHING_ID =
"1234567812345678".getBytes(StandardCharsets.UTF_8);
    private static final X9ECParameters SM2_X9EC_PARAMETERS =
GMNamedCurves.getByname("sm2p256v1");

    // ***calculateSM2Digest***
    // Calculate message digest
    public static byte[] calculateSM2Digest(final PublicKey publicKey, final byte[]
message) throws
        NoSuchProviderException, NoSuchAlgorithmException {
        final ECPublicKey ecPublicKey = (ECPublicKey) publicKey;

        // Generate SM3 hash of default distinguishing ID, 1234567812345678
        final int entlenA = DEFAULT_DISTINGUISHING_ID.length * 8;
        final byte [] entla = new byte[] { (byte) (entlenA & 0xFF00), (byte) (entlenA &
0x00FF) };
        final byte [] a = SM2_X9EC_PARAMETERS.getCurve().getA().getEncoded();
        final byte [] b = SM2_X9EC_PARAMETERS.getCurve().getB().getEncoded();
        final byte [] xg = SM2_X9EC_PARAMETERS.getG().getXCoord().getEncoded();
        final byte [] yg = SM2_X9EC_PARAMETERS.getG().getYCoord().getEncoded();
        final byte[] xa = ecPublicKey.getQ().getXCoord().getEncoded();
        final byte[] ya = ecPublicKey.getQ().getYCoord().getEncoded();
        final byte[] za = MessageDigest.getInstance("SM3", "BC")
            .digest(ByteBuffer.allocate(entla.length +
DEFAULT_DISTINGUISHING_ID.length + a.length + b.length + xg.length + yg.length +
```

```

        xa.length +
ya.length).put(entla).put(DEFAULT_DISTINGUISHING_ID).put(a).put(b).put(xg).put(yg).put(xa).put
        .array());

    // Combine hashed distinguishing ID with original message to generate final
digest
    return MessageDigest.getInstance("SM3", "BC")
        .digest(ByteBuffer.allocate(za.length +
message.length).put(za).put(message)
        .array());
}

// ***offlineSM2DSAVerify***
// Verify digital signature with SM2 public key
public static boolean offlineSM2DSAVerify(final PublicKey publicKey, final byte []
message,
    final byte [] signature) throws InvalidKeyException {
    final SM2Signer signer = new SM2Signer();
    CipherParameters cipherParameters =
ECUtil.generatePublicKeyParameter(publicKey);
    cipherParameters = new ParametersWithID(cipherParameters,
DEFAULT_DISTINGUISHING_ID);
    signer.init(false, cipherParameters);
    signer.update(message, 0, message.length);
    return signer.verifySignature(signature);
}

// ***offlineSM2PKEEncrypt***
// Encrypt data with SM2 public key
public static byte[] offlineSM2PKEEncrypt(final PublicKey publicKey, final byte []
plaintext) throws
    NoSuchPaddingException, NoSuchAlgorithmException, NoSuchProviderException,
InvalidKeyException,
    BadPaddingException, IllegalBlockSizeException, IOException {
    final Cipher sm2Cipher = Cipher.getInstance("SM2", "BC");
    sm2Cipher.init(Cipher.ENCRYPT_MODE, publicKey);

    // By default, Bouncy Castle returns raw ciphertext in the c1c2c3 format
    final byte [] cipherText = sm2Cipher.doFinal(plaintext);

    // Convert the raw ciphertext to the ASN.1 format before passing it to AWS KMS
    final ASN1EncodableVector asn1EncodableVector = new ASN1EncodableVector();
    final int coordinateLength = (SM2_X9EC_PARAMETERS.getCurve().getFieldSize() +
7) / 8 * 2 + 1;

```



```
    final int sm3HashLength = 32;
    final int xCoordinateInCipherText = 33;
    final int yCoordinateInCipherText = 65;
    byte[] coords = new byte[coordinateLength];
    byte[] sm3Hash = new byte[sm3HashLength];
    byte[] remainingCipherText = new byte[cipherText.length - coordinateLength -
sm3HashLength];

    // Split components out of the ciphertext
    System.arraycopy(cipherText, 0, coords, 0, coordinateLength);
    System.arraycopy(cipherText, cipherText.length - sm3HashLength, sm3Hash, 0,
sm3HashLength);
    System.arraycopy(cipherText, coordinateLength, remainingCipherText,
0,cipherText.length - coordinateLength - sm3HashLength);

    // Build standard SM2PKE ASN.1 ciphertext vector
    asn1EncodableVector.add(new ASN1Integer(new BigInteger(1,
Arrays.copyOfRange(coords, 1, xCoordinateInCipherText))));
    asn1EncodableVector.add(new ASN1Integer(new BigInteger(1,
Arrays.copyOfRange(coords, xCoordinateInCipherText, yCoordinateInCipherText))));
    asn1EncodableVector.add(new DEROctetString(sm3Hash));
    asn1EncodableVector.add(new DEROctetString(remainingCipherText));

    return new DERSequence(asn1EncodableVector).getEncoded("DER");
}
}
```

Monitor Amazon KMS keys

Monitoring is an important part of understanding the availability, state, and usage of your Amazon KMS keys in Amazon KMS and maintaining the reliability, availability, and performance of your Amazon solutions. Collecting monitoring data from all the parts of your Amazon solution will help you debug a multipoint failure if one occurs. Before you start monitoring your KMS keys, however, create a monitoring plan that includes answers to the following questions:

- What are your monitoring goals?
- What resources will you monitor?
- How often will you monitor these resources?
- What [monitoring tools](#) will you use?
- Who will perform the monitoring tasks?
- Who should be notified when something happens?

The next step is to monitor your KMS keys over time to establish a baseline for normal Amazon KMS usage and expectations in your environment. As you monitor your KMS keys, store historical monitoring data so that you can compare it with current data, identify normal patterns and anomalies, and devise methods to address issues.

For example, you can monitor Amazon KMS API activity and events that affect your KMS keys. When data falls above or below your established norms, you might need to investigate or take corrective action.

To establish a baseline for normal patterns, monitor the following items:

- Amazon KMS API activity for *data plane* operations. These are [cryptographic operations](#) that use a KMS key, such as [Decrypt](#), [Encrypt](#), [ReEncrypt](#), and [GenerateDataKey](#).
- Amazon KMS API activity for *control plane* operations that are important to you. These operations manage a KMS key, and you might want to monitor those that change a KMS key's availability (such as [ScheduleKeyDeletion](#), [CancelKeyDeletion](#), [DisableKey](#), [EnableKey](#), [ImportKeyMaterial](#), and [DeleteImportedKeyMaterial](#)) or change a KMS key's access control (such as [PutKeyPolicy](#) and [RevokeGrant](#)).
- Other Amazon KMS metrics (such as the amount of time remaining until your [imported key material](#) expires) and events (such as the expiration of imported key material or the deletion or key rotation of a KMS key).

Monitoring tools

Amazon provides various tools that you can use to monitor your KMS keys. You can configure some of these tools to do the monitoring for you, while some of the tools require manual intervention. We recommend that you automate monitoring tasks as much as possible.

Automated monitoring tools

You can use the following automated monitoring tools to watch your KMS keys and report when something has changed.

- **Amazon CloudTrail Log Monitoring** – Share log files between accounts, monitor CloudTrail log files in real time by sending them to CloudWatch Logs, write log processing applications with the [CloudTrail Processing Library](#), and validate that your log files have not changed after delivery by CloudTrail. For more information, see [Working with CloudTrail Log Files](#) in the *Amazon CloudTrail User Guide*.
- **Amazon CloudWatch Alarms** – Watch a single metric over a time period that you specify, and perform one or more actions based on the value of the metric relative to a given threshold over a number of time periods. The action is a notification sent to an Amazon Simple Notification Service (Amazon SNS) topic or Amazon EC2 Auto Scaling policy. CloudWatch alarms do not invoke actions simply because they are in a particular state; the state must have changed and been maintained for a specified number of periods. For more information, see [Monitor KMS keys with Amazon CloudWatch](#).
- **Amazon EventBridge** – Match events and route them to one or more target functions or streams to capture state information and, if necessary, make changes or take corrective action. For more information, see [Monitor KMS keys with Amazon EventBridge](#) and the [Amazon EventBridge User Guide](#).
- **Amazon CloudWatch Logs** – Monitor, store, and access your log files from Amazon CloudTrail or other sources. For more information, see the [Amazon CloudWatch Logs User Guide](#).

Manual monitoring tools

Another important part of monitoring KMS keys involves manually monitoring those items that the CloudWatch alarms and events don't cover. The Amazon KMS, CloudWatch, Amazon Trusted Advisor, and other Amazon dashboards provide an at-a-glance view of the state of your Amazon environment.

You can [customize](#) the **Amazon managed keys** and **Customer managed keys** pages of the [Amazon KMS console](#) to display the following information about each KMS key:

- Key ID
- Status
- Creation date
- Expiration date (for KMS keys with [imported key material](#))
- Origin
- Custom key store ID (for KMS keys in [custom key stores](#))

The [CloudWatch console dashboard](#) shows the following:

- Current alarms and status
- Graphs of alarms and resources
- Service health status

In addition, you can use CloudWatch to do the following:

- Create [customized dashboards](#) to monitor the services you care about
- Graph metric data to troubleshoot issues and discover trends
- Search and browse all your Amazon resource metrics
- Create and edit alarms to be notified of problems

Amazon Trusted Advisor can help you monitor your Amazon resources to improve performance, reliability, security, and cost effectiveness. Four Trusted Advisor checks are available to all users; more than 50 checks are available to users with a Business or Enterprise support plan. For more information, see [Amazon Trusted Advisor](#).

Logging Amazon KMS API calls with Amazon CloudTrail

Amazon KMS is integrated with [Amazon CloudTrail](#), a service that records all calls to Amazon KMS by users, roles, and other Amazon services. CloudTrail captures all API calls to Amazon KMS as events, including calls from the Amazon KMS console, Amazon KMS APIs, Amazon CloudFormation templates, the Amazon Command Line Interface (Amazon CLI), and Amazon Tools for PowerShell.

CloudTrail logs all Amazon KMS operations, including read-only operations, such as [ListAliases](#) and [GetKeyRotationStatus](#), operations that manage KMS keys, such as [CreateKey](#) and [PutKeyPolicy](#), and [cryptographic operations](#), such as [GenerateDataKey](#) and [Decrypt](#). It also logs internal operations that Amazon KMS calls for you, such as [DeleteExpiredKeyMaterial](#), [DeleteKey](#), [SynchronizeMultiRegionKey](#), and [RotateKey](#).

CloudTrail logs all successful operations and, in some scenarios, attempted calls that failed, such as when the caller is denied access to a resource. [Cross-account operations on KMS keys](#) are logged in both the caller account and the KMS key owner account. However, cross-account Amazon KMS requests that are rejected because access is denied are logged only in the caller's account.

For security reasons, some fields are omitted from Amazon KMS log entries, such as the Plaintext parameter of an [Encrypt](#) request, and the response to [GetKeyPolicy](#) or any cryptographic operation. To make it easier to search for CloudTrail log entries for particular KMS keys, Amazon KMS adds the [key ARN](#) of the affected KMS key to the responseElements field in the log entries for some Amazon KMS key management operations, even when the API operation doesn't return the key ARN.

Although by default, all Amazon KMS actions are logged as CloudTrail events, you can exclude Amazon KMS actions from a CloudTrail trail. For details, see [Excluding Amazon KMS events from a trail](#).

Learn more:

- For CloudTrail log examples of Amazon KMS operations for an Amazon Nitro enclave, see [Monitoring requests for Nitro enclaves](#).


Topics

- [Finding Amazon KMS log entries in CloudTrail](#)
- [Excluding Amazon KMS events from a trail](#)
- [Examples of Amazon KMS log entries](#)

Finding Amazon KMS log entries in CloudTrail

To search CloudTrail log entries, use the [CloudTrail console](#) or the [CloudTrail LookupEvents](#) operation. CloudTrail supports numerous [attribute values](#) for filtering your search, including event name, user name, and event source.

To help you search for Amazon KMS log entries in CloudTrail, Amazon KMS populates the following CloudTrail log entry fields.

 **Note**

Beginning in December 2022, Amazon KMS populates the **Resource type** and **Resource name** attributes in all management operations that change a particular KMS key. These attribute values might be null in older CloudTrail entries for the following operations: [CreateAlias](#), [CreateGrant](#), [DeleteAlias](#), [DeleteImportedKeyMaterial](#), [ImportKeyMaterial](#), [ReplicateKey](#), [RetireGrant](#), [RevokeGrant](#), [UpdateAlias](#), and [UpdatePrimaryRegion](#).

Attribute	Value	Log entries
Event source (EventSource)	kms.amazonaws.com	All operations.
Resource type (ResourceType)	AWS::KMS::Key	Management operations that change a particular KMS key, such as <code>CreateKey</code> and <code>EnableKey</code> , but not <code>ListKeys</code> .
Resource name (ResourceName)	Key ARN (or key ID and key ARN)	Management operations that change a particular KMS key, such as <code>CreateKey</code> and <code>EnableKey</code> , but not <code>ListKeys</code> .

To help you find log entries for management operations on particular KMS keys, Amazon KMS records the key ARN of the affected KMS key in the `responseElements.keyId` element of the log entry, even when the Amazon KMS API operation doesn't return the key ARN.

For example, a successful call to the [DisableKey](#) operation doesn't return any values in the response, but instead of a null value, the `responseElements.keyId` value in the [DisableKey log entry](#) includes the key ARN of the disabled KMS key.

This feature was added in December 2022 and affects the following CloudTrail log entries: [CreateAlias](#), [CreateGrant](#), [DeleteAlias](#), [DeleteKey](#), [DisableKey](#), [EnableKey](#), [EnableKeyRotation](#), [ImportKeyMaterial](#), [RotateKey](#), [SynchronizeMultiRegionKey](#), [TagResource](#), [UntagResource](#), [UpdateAlias](#), and [UpdatePrimaryRegion](#).

Excluding Amazon KMS events from a trail

To provide a record of the use and management of their Amazon KMS resources, most Amazon KMS users rely on the events in a CloudTrail trail. The trail can be an valuable source of data for auditing critical events, such as creating, disabling, and deleting Amazon KMS keys, changing key policy, and the use of your KMS keys by Amazon services on your behalf. In some cases, the metadata in a CloudTrail log entry, such as the [encryption context](#) in an encryption operation, can help you to avoid or resolve errors.

However, because Amazon KMS can generate a large number of events, Amazon CloudTrail lets you exclude Amazon KMS events from a trail. This per-trail setting excludes all Amazon KMS events; you cannot exclude particular Amazon KMS events.

Warning

Excluding Amazon KMS events from a CloudTrail Log can obscure actions that use your KMS keys. Be cautious when giving principals the `cloudtrail:PutEventSelectors` permission that is required to perform this operation.

To exclude Amazon KMS events from a trail:

- In the CloudTrail console, use the **Log Key Management Service events** setting when you [create a trail](#) or [update a trail](#). For instructions, see [Logging Management Events with the Amazon Web Services Management Console](#) in the Amazon CloudTrail User Guide.
- In the CloudTrail API, use the [PutEventSelectors](#) operation. Add the `ExcludeManagementEventSources` attribute to your event selectors with a value of `kms.amazonaws.com`. For an example, see [Example: A trail that does not log Amazon Key Management Service events](#) in the Amazon CloudTrail User Guide.

You can disable this exclusion at any time by changing the console setting or the event selectors for a trail. The trail will then start recording Amazon KMS events. However, it cannot recover Amazon KMS events that occurred while the exclusion was effective.

When you exclude Amazon KMS events by using the console or API, the resulting CloudTrail `PutEventSelectors` API operation is also logged in your CloudTrail Logs. If Amazon KMS events don't appear in your CloudTrail Logs, look for a `PutEventSelectors` event with the `ExcludeManagementEventSources` attribute set to `kms.amazonaws.com`.

Examples of Amazon KMS log entries

Amazon KMS writes entries to your CloudTrail log when you call an Amazon KMS operation and when an Amazon service calls an operation on your behalf. Amazon KMS also writes an entry when it calls an operation for you. For example, it writes an entry when it [deletes a KMS key](#) that you scheduled for deletion.

The following topics display examples of CloudTrail log entries for Amazon KMS operations.

For examples of CloudTrail log entries of requests to Amazon KMS from Amazon Nitro Enclaves, see [Monitoring requests for Nitro enclaves](#).

Topics

- [CancelKeyDeletion](#)
- [ConnectCustomKeyStore](#)
- [CreateAlias](#)
- [CreateCustomKeyStore](#)
- [CreateGrant](#)
- [CreateKey](#)
- [Decrypt](#)
- [DeleteAlias](#)
- [DeleteCustomKeyStore](#)
- [DeleteExpiredKeyMaterial](#)
- [DeleteImportedKeyMaterial](#)
- [DeleteKey](#)
- [DescribeCustomKeyStores](#)
- [DescribeKey](#)
- [DisableKey](#)
- [DisableKeyRotation](#)
- [DisconnectCustomKeyStore](#)

- [EnableKey](#)
- [EnableKeyRotation](#)
- [Encrypt](#)
- [GenerateDataKey](#)
- [GenerateDataKeyPair](#)
- [GenerateDataKeyPairWithoutPlaintext](#)
- [GenerateDataKeyWithoutPlaintext](#)
- [GenerateMac](#)
- [GenerateRandom](#)
- [GetKeyPolicy](#)
- [GetKeyRotationStatus](#)
- [GetParametersForImport](#)
- [ImportKeyMaterial](#)
- [ListAliases](#)
- [ListGrants](#)
- [ListKeyRotations](#)
- [PutKeyPolicy](#)
- [ReEncrypt](#)
- [ReplicateKey](#)
- [RetireGrant](#)
- [RevokeGrant](#)
- [RotateKey](#)
- [RotateKeyOnDemand](#)
- [ScheduleKeyDeletion](#)
- [Sign](#)
- [SynchronizeMultiRegionKey](#)
- [TagResource](#)
- [UntagResource](#)
- [UpdateAlias](#)
- [UpdateCustomKeyStore](#)

- [UpdateKeyDescription](#)
- [UpdatePrimaryRegion](#)
- [VerifyMac](#)
- [Verify](#)
- [Amazon EC2 example one](#)
- [Amazon EC2 example two](#)

CancelKeyDeletion

The following example shows an Amazon CloudTrail log entry generated by calling the [CancelKeyDeletion](#) operation. For information about deleting Amazon KMS keys, see [Delete an Amazon KMS key](#).

```
{
  "eventVersion": "1.05",
  "userIdentity": {
    "type": "IAMUser",
    "principalId": "EX_PRINCIPAL_ID",
    "arn": "arn:aws:iam::111122223333:user/Alice",
    "accountId": "111122223333",
    "accessKeyId": "EXAMPLE_KEY_ID",
    "userName": "Alice"
  },
  "eventTime": "2020-07-27T21:53:17Z",
  "eventSource": "kms.amazonaws.com",
  "eventName": "CancelKeyDeletion",
  "awsRegion": "us-west-2",
  "sourceIPAddress": "192.0.2.0",
  "userAgent": "Amazon Internal",
  "requestParameters": {
    "keyId": "1234abcd-12ab-34cd-56ef-1234567890ab"
  },
  "responseElements": {
    "keyId": "arn:aws:kms:us-west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab"
  },
  "requestID": "e3452e68-d4b0-4ec7-a768-7ae96c23764f",
  "eventID": "d818bf03-6655-48e9-8b26-f279a07075fd",
  "readOnly": false,
  "resources": [
```

```

    {
      "accountId": "111122223333",
      "type": "AWS::KMS::Key",
      "ARN": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab"
    }
  ],
  "eventType": "AwsApiCall",
  "recipientAccountId": "111122223333"
}

```

ConnectCustomKeyStore

The following example shows an Amazon CloudTrail log entry generated by calling the [ConnectCustomKeyStore](#) operation. For information about connecting a custom key store, see [Disconnect an Amazon CloudHSM key store](#).

```

{
  "eventVersion": "1.08",
  "userIdentity": {
    "type": "IAMUser",
    "principalId": "EX_PRINCIPAL_ID",
    "arn": "arn:aws:iam::111122223333:user/Alice",
    "accountId": "111122223333",
    "accessKeyId": "EXAMPLE_KEY_ID",
    "userName": "Alice"
  },
  "eventTime": "2021-10-21T20:17:32Z",
  "eventSource": "kms.amazonaws.com",
  "eventName": "ConnectCustomKeyStore",
  "awsRegion": "us-east-1",
  "sourceIPAddress": "192.0.2.0",
  "userAgent": "AWS Internal",
  "requestParameters": {
    "customKeyId": "cks-1234567890abcdef0"
  },
  "responseElements": null,
  "additionalEventData": {
    "customKeyName": "ExampleKeyStore",
    "clusterId": "cluster-1a23b4cdefg"
  },
  "requestID": "abcde9e1-f1a3-4460-a423-577fb6e695c9",
  "eventID": "114b61b9-0ea6-47f5-a9d2-4f2bdd0017d5",
}

```

```

    "readOnly": false,
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "111122223333"
  }

```

CreateAlias

The following example shows an Amazon CloudTrail log entry for the [CreateAlias](#) operation. The `resources` element includes fields for the alias and KMS key resources. For information about creating aliases in Amazon KMS, see [Create aliases](#).

CloudTrail log entries for this operation recorded on or after December 2022 include the key ARN of the affected KMS key in the `responseElements.keyId` value, even though this operation does not return the key ARN.

```

{
  "eventVersion": "1.08",
  "userIdentity": {
    "type": "IAMUser",
    "principalId": "EX_PRINCIPAL_ID",
    "arn": "arn:aws:iam::111122223333:user/Alice",
    "accountId": "111122223333",
    "accessKeyId": "EXAMPLE_KEY_ID",
    "userName": "Alice"
  },
  "eventTime": "2022-08-14T23:08:31Z",
  "eventSource": "kms.amazonaws.com",
  "eventName": "CreateAlias",
  "awsRegion": "us-west-2",
  "sourceIPAddress": "192.0.2.0",
  "userAgent": "Amazon Internal",
  "requestParameters": {
    "aliasName": "alias/ExampleAlias",
    "targetKeyId": "1234abcd-12ab-34cd-56ef-1234567890ab"
  },
  "responseElements": {
    "keyId": "arn:aws:kms:us-west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab"
  },
  "requestID": "caec1e0c-ce03-419e-bdab-6ab1f7c57c01",
  "eventID": "2dd6e784-8286-46a6-befd-d64e5a02fb28",
  "readOnly": false,

```

```

    "resources": [
      {
        "accountId": "111122223333",
        "type": "AWS::KMS::Key",
        "ARN": "arn:aws:kms:us-west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab"
      },
      {
        "accountId": "111122223333",
        "type": "AWS::KMS::Key",
        "ARN": "arn:aws:kms:us-west-2:111122223333:alias/ExampleAlias"
      }
    ],
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "111122223333",
    "eventCategory": "Management"
  }

```

CreateCustomKeyStore

The following example shows an Amazon CloudTrail log entry generated by calling the [CreateCustomKeyStore](#) operation on an Amazon CloudHSM key store. For information about creating custom key stores, see [Create an Amazon CloudHSM key store](#).

```

{
  "eventVersion": "1.08",
  "userIdentity": {
    "type": "IAMUser",
    "principalId": "EX_PRINCIPAL_ID",
    "arn": "arn:aws:iam::111122223333:user/Alice",
    "accountId": "111122223333",
    "accessKeyId": "EXAMPLE_KEY_ID",
    "userName": "Alice"
  },
  "eventTime": "2021-10-21T20:17:32Z",
  "eventSource": "kms.amazonaws.com",
  "eventName": "CreateCustomKeyStore",
  "awsRegion": "us-east-1",
  "sourceIPAddress": "192.0.2.0",
  "userAgent": "AWS Internal",
  "requestParameters": {
    "customKeyName": "ExampleKeyStore",

```

```
    "clusterId": "cluster-1a23b4cdefg"
  },
  "responseElements": {
    "customKeyStoreId": "cks-1234567890abcdef0"
  },
  "requestID": "abcde9e1-f1a3-4460-a423-577fb6e695c9",
  "eventID": "114b61b9-0ea6-47f5-a9d2-4f2bdd0017d5",
  "readOnly": false,
  "eventType": "AwsApiCall",
  "managementEvent": true,
  "recipientAccountId": "111122223333"
}
```

CreateGrant

The following example shows an Amazon CloudTrail log entry for the [CreateGrant](#) operation. For information about creating grants in Amazon KMS, see [Grants in Amazon KMS](#).

CloudTrail log entries for this operation recorded on or after December 2022 include the key ARN of the affected KMS key in the `responseElements.keyId` value, even though this operation does not return the key ARN.

```
{
  "eventVersion": "1.02",
  "userIdentity": {
    "type": "IAMUser",
    "principalId": "EX_PRINCIPAL_ID",
    "arn": "arn:aws:iam::111122223333:user/Alice",
    "accountId": "111122223333",
    "accessKeyId": "EXAMPLE_KEY_ID",
    "userName": "Alice"
  },
  "eventTime": "2014-11-04T00:53:12Z",
  "eventSource": "kms.amazonaws.com",
  "eventName": "CreateGrant",
  "awsRegion": "us-east-1",
  "sourceIPAddress": "192.0.2.0",
  "userAgent": "Amazon Internal",
  "requestParameters": {
    "keyId": "arn:aws:kms:us-west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab",
    "constraints": {
      "encryptionContextSubset": {
```

```

        "ContextKey1": "Value1"
      }
    },
    "operations": ["Encrypt",
    "RetireGrant"],
    "granteePrincipal": "EX_PRINCIPAL_ID"
  },
  "responseElements": {
    "grantId": "f020fe75197b93991dc8491d6f19dd3cebb24ee62277a05914386724f3d48758",
    "keyId": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab"
  },
  "requestID": "f3c08808-63bc-11e4-bc2b-4198b6150d5c",
  "eventID": "5d529779-2d27-42b5-92da-91aaea1fc4b5",
  "readOnly": false,
  "resources": [{
    "ARN": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab",
    "accountId": "111122223333"
  }],
  "eventType": "AwsApiCall",
  "recipientAccountId": "111122223333"
}

```

CreateKey

These examples show Amazon CloudTrail log entries for the [CreateKey](#) operation.

A CreateKey log entry can result from a CreateKey request or the CreateKey operation for a [ReplicateKey](#) request.

The following example shows an CloudTrail log entry for a [CreateKey](#) operation that creates a [symmetric encryption KMS key](#). For information about creating KMS keys, see [Create a KMS key](#).

```

{
  "eventVersion": "1.08",
  "userIdentity": {
    "type": "IAMUser",
    "principalId": "EX_PRINCIPAL_ID",
    "arn": "arn:aws:iam::111122223333:user/Alice",
    "accountId": "111122223333",
    "accessKeyId": "EXAMPLE_KEY_ID",
    "userName": "Alice"
  }
}

```

```
  },
  "eventTime": "2022-08-10T22:38:27Z",
  "eventSource": "kms.amazonaws.com",
  "eventName": "CreateKey",
  "awsRegion": "us-west-2",
  "sourceIPAddress": "192.0.2.0",
  "userAgent": "Amazon Internal",
  "requestParameters": {
    "description": "",
    "origin": "EXTERNAL",
    "bypassPolicyLockoutSafetyCheck": false,
    "customerMasterKeySpec": "SYMMETRIC_DEFAULT",
    "keySpec": "SYMMETRIC_DEFAULT",
    "keyUsage": "ENCRYPT_DECRYPT"
  },
  "responseElements": {
    "keyMetadata": {
      "AWSAccountId": "111122223333",
      "keyId": "1234abcd-12ab-34cd-56ef-1234567890ab",
      "arn": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab",
      "creationDate": "Aug 10, 2022, 10:38:27 PM",
      "enabled": false,
      "description": "",
      "keyUsage": "ENCRYPT_DECRYPT",
      "keyState": "PendingImport",
      "origin": "EXTERNAL",
      "keyManager": "CUSTOMER",
      "customerMasterKeySpec": "SYMMETRIC_DEFAULT",
      "keySpec": "SYMMETRIC_DEFAULT",
      "encryptionAlgorithms": [
        "SYMMETRIC_DEFAULT"
      ],
      "multiRegion": false
    }
  },
  "requestID": "1aef6713-0223-4ff7-9a6d-781360521930",
  "eventID": "36327b37-f4f6-40a9-92ab-48064ec905a2",
  "readOnly": false,
  "resources": [
    {
      "accountId": "111122223333",
      "type": "AWS::KMS::Key",
```



```

        "ARN": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab"
    }
],
"eventType": "AwsApiCall",
"managementEvent": true,
"recipientAccountId": "111122223333",
"eventCategory": "Management"
}

```

The following example shows the CloudTrail log of a CreateKey operation that creates a symmetric encryption KMS key in an [Amazon CloudHSM key store](#).

```

{
  "eventVersion": "1.08",
  "userIdentity": {
    "type": "IAMUser",
    "principalId": "EX_PRINCIPAL_ID",
    "arn": "arn:aws:iam::111122223333:user/Alice",
    "accountId": "111122223333",
    "accessKeyId": "EXAMPLE_KEY_ID",
    "userName": "Alice"
  },
  "eventTime": "2021-10-14T17:39:50Z",
  "eventSource": "kms.amazonaws.com",
  "eventName": "CreateKey",
  "awsRegion": "us-west-2",
  "sourceIPAddress": "192.0.2.0",
  "userAgent": "Amazon Internal",
  "requestParameters": {
    "keyUsage": "ENCRYPT_DECRYPT",
    "bypassPolicyLockoutSafetyCheck": false,
    "origin": "AWS_CLOUDHSM",
    "keySpec": "SYMMETRIC_DEFAULT",
    "customerMasterKeySpec": "SYMMETRIC_DEFAULT",
    "customKeyStoreId": "cks-1234567890abcdef0",
    "description": ""
  },
  "responseElements": {
    "keyMetadata": {
      "awsAccountId": "111122223333",
      "keyId": "0987dcba-09fe-87dc-65ba-ab0987654321",

```

```

    "arn": "arn:aws:kms:us-west-2:111122223333:key/0987dcba-09fe-87dc-65ba-
ab0987654321",
    "creationDate": "Oct 14, 2021, 5:39:50 PM",
    "enabled": true,
    "description": "",
    "keyUsage": "ENCRYPT_DECRYPT",
    "keyState": "Enabled",
    "origin": "AWS_CLOUDHSM",
    "customKeyStoreId": "cks-1234567890abcdef0",
    "cloudHsmClusterId": "cluster-1a23b4cdefg",
    "keyManager": "CUSTOMER",
    "customerMasterKeySpec": "SYMMETRIC_DEFAULT",
    "keySpec": "SYMMETRIC_DEFAULT",
    "encryptionAlgorithms": [
      "SYMMETRIC_DEFAULT"
    ],
    "multiRegion": false
  }
},
"additionalEventData": {
  "backingKey": "{\"backingKeyId\": \"backing-key-id\"}"
},
"requestID": "4f0b185c-588c-4767-9e90-c618f7e13cad",
"eventID": "c73964b8-703d-49e4-bd9e-f773d0ee1e65",
"readOnly": false,
"resources": [
  {
    "accountId": "111122223333",
    "type": "AWS::KMS::Key",
    "ARN": "arn:aws:kms:us-west-2:111122223333:key/0987dcba-09fe-87dc-65ba-
ab0987654321"
  }
],
"eventType": "AwsApiCall",
"managementEvent": true,
"recipientAccountId": "111122223333",
"eventCategory": "Management"
}

```

The following example shows the CloudTrail log of a `CreateKey` operation that creates a symmetric encryption KMS key in an [external key store](#).

```
{
```

```
"eventVersion": "1.08",
"userIdentity": {
  "type": "IAMUser",
  "principalId": "EX_PRINCIPAL_ID",
  "arn": "arn:aws:iam::111122223333:user/Alice",
  "accountId": "111122223333",
  "accessKeyId": "EXAMPLE_KEY_ID",
  "userName": "Alice"
},
"eventTime": "2022-09-07T22:37:45Z",
"eventSource": "kms.amazonaws.com",
"eventName": "CreateKey",
"awsRegion": "us-east-1",
"sourceIPAddress": "192.0.2.0",
"userAgent": "Amazon Internal",
"requestParameters": {
  "tags": [],
  "keyUsage": "ENCRYPT_DECRYPT",
  "description": "",
  "origin": "EXTERNAL_KEY_STORE",
  "multiRegion": false,
  "keySpec": "SYMMETRIC_DEFAULT",
  "customerMasterKeySpec": "SYMMETRIC_DEFAULT",
  "bypassPolicyLockoutSafetyCheck": false,
  "customKeyId": "cks-1234567890abcdef0",
  "xksKeyId": "bb8562717f809024"
},
"responseElements": {
  "keyMetadata": {
    "awsAccountId": "111122223333",
    "keyId": "1234abcd-12ab-34cd-56ef-1234567890ab",
    "arn": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab",
    "creationDate": "Dec 7, 2022, 10:37:45 PM",
    "enabled": true,
    "description": "",
    "keyUsage": "ENCRYPT_DECRYPT",
    "keyState": "Enabled",
    "origin": "EXTERNAL_KEY_STORE",
    "customKeyId": "cks-1234567890abcdef0",
    "keyManager": "CUSTOMER",
    "customerMasterKeySpec": "SYMMETRIC_DEFAULT",
    "keySpec": "SYMMETRIC_DEFAULT",
    "encryptionAlgorithms": [
```

```
        "SYMMETRIC_DEFAULT"
      ],
      "multiRegion": false,
      "xksKeyConfiguration": {
        "id": "bb8562717f809024"
      }
    }
  },
  "requestID": "ba197c82-3ac7-487a-8ff4-7736bbeb1316",
  "eventID": "838ad5f4-5fdd-4044-afd7-4dbd88c6af56",
  "readOnly": false,
  "resources": [
    {
      "accountId": "227179770375",
      "type": "AWS::KMS::Key",
      "ARN": "arn:aws:kms:us-east-1:227179770375:key/39c5eb22-
f37c-4956-92ca-89e8f8b57ab2"
    }
  ],
  "eventType": "AwsApiCall",
  "managementEvent": true,
  "recipientAccountId": "111122223333",
  "eventCategory": "Management"
}
```

Decrypt

These examples show Amazon CloudTrail log entries for the [Decrypt](#) operation.

The CloudTrail log entry for a Decrypt operation always includes the `encryptionAlgorithm` in the `requestParameters` even if the encryption algorithm wasn't specified in the request. The ciphertext in the request and the plaintext in the response are omitted.

Topics

- [Decrypt with a standard symmetric encryption key](#)
- [Decrypt failure with a standard symmetric encryption key](#)
- [Decrypt with a KMS key in an Amazon CloudHSM key store](#)
- [Decrypt with a KMS key in an external key store](#)
- [Decrypt failure with a KMS key in an external key store](#)

Decrypt with a standard symmetric encryption key

The following is an example CloudTrail log entry for a Decrypt operation with a standard symmetric encryption key.

```
{
  "eventVersion": "1.05",
  "userIdentity": {
    "type": "IAMUser",
    "principalId": "EX_PRINCIPAL_ID",
    "arn": "arn:aws:iam::111122223333:user/Alice",
    "accountId": "111122223333",
    "accessKeyId": "EXAMPLE_KEY_ID",
    "userName": "Alice"
  },
  "eventTime": "2020-07-27T22:58:24Z",
  "eventSource": "kms.amazonaws.com",
  "eventName": "Decrypt",
  "awsRegion": "us-west-2",
  "sourceIPAddress": "192.0.2.0",
  "userAgent": "Amazon Internal",
  "requestParameters": {
    "encryptionAlgorithm": "SYMMETRIC_DEFAULT",
    "keyId": "arn:aws:kms:us-west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab",
    "encryptionContext": {
      "Department": "Engineering",
      "Project": "Alpha"
    }
  },
  "responseElements": null,
  "requestID": "12345126-30d5-4b28-98b9-9153da559963",
  "eventID": "abcde202-ba1a-467c-b4ba-f729d45ae521",
  "readOnly": true,
  "resources": [
    {
      "accountId": "111122223333",
      "type": "AWS::KMS::Key",
      "ARN": "arn:aws:kms:us-west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab"
    }
  ],
  "eventType": "AwsApiCall",
  "recipientAccountId": "111122223333"
}
```

```
}
```

Decrypt failure with a standard symmetric encryption key

The following example CloudTrail log entry records a failed Decrypt operation with a standard symmetric encryption KMS key. The exception (`errorCode`) and error message (`errorMessage`) are included help you to resolve the error.

In this case, the symmetric encryption KMS key specified in the Decrypt request was not the symmetric encryption KMS key that was used to encrypt the data.

```
{
  "eventVersion": "1.08",
  "userIdentity": {
    "type": "IAMUser",
    "principalId": "EX_PRINCIPAL_ID",
    "arn": "arn:aws:iam::111122223333:user/Alice",
    "accountId": "111122223333",
    "accessKeyId": "EXAMPLE_KEY_ID",
    "userName": "Alice"
  },
  "eventTime": "2022-11-24T18:57:43Z",
  "eventSource": "kms.amazonaws.com",
  "eventName": "Decrypt",
  "awsRegion": "us-west-2",
  "sourceIPAddress": "192.0.2.0",
  "userAgent": "AWS Internal",
  "errorCode": "IncorrectKeyException"
  "errorMessage": "The key ID in the request does not identify a CMK that can perform
this operation.",
  "requestParameters": {
    "encryptionAlgorithm": "SYMMETRIC_DEFAULT",
    "keyId": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab",
    "encryptionContext": {
      "Department": "Engineering",
      "Project": "Alpha"
    }
  },
  "responseElements": null,
  "requestID": "22345126-30d5-4b28-98b9-9153da559963",
  "eventID": "abcde202-ba1a-467c-b4ba-f729d45ae521",
  "readOnly": true,
```

```

    "resources": [
      {
        "accountId": "111122223333",
        "type": "AWS::KMS::Key",
        "ARN": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab"
      }
    ],
    "eventType": "AwsApiCall",
    "recipientAccountId": "111122223333"
  }

```

Decrypt with a KMS key in an Amazon CloudHSM key store

The following example CloudTrail log entry records a Decrypt operation with a KMS key in an [Amazon CloudHSM key store](#). All log entries for cryptographic operations with a KMS key in a custom key store include an `additionalEventData` field with the `customKeyStoreId` and `backingKeyId`. The value returned in the `backingKeyId` field is the CloudHSM key id attribute. The `additionalEventData` isn't specified in the request.

```

{
  "eventVersion": "1.08",
  "userIdentity": {
    "type": "IAMUser",
    "principalId": "EX_PRINCIPAL_ID",
    "arn": "arn:aws:iam::111122223333:user/Alice",
    "accountId": "111122223333",
    "accessKeyId": "EXAMPLE_KEY_ID",
    "userName": "Alice"
  },
  "eventTime": "2021-10-26T23:41:27Z",
  "eventSource": "kms.amazonaws.com",
  "eventName": "Decrypt",
  "awsRegion": "us-west-2",
  "sourceIPAddress": "192.0.2.0",
  "requestParameters": {
    "encryptionAlgorithm": "SYMMETRIC_DEFAULT",
    "keyId": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab",
    "encryptionContext": {
      "Department": "Development",
      "Purpose": "Test"
    }
  }
}

```

```

    },
    "responseElements": null,
    "additionalEventData": {
        "customKeyId": "cks-1234567890abcdef0"
    },
    "requestID": "e1b881f8-2048-41f8-b6cc-382b7857ec61",
    "eventID": "a79603d5-4cde-46fc-819c-a7cf547b9df4",
    "readOnly": true,
    "resources": [
        {
            "accountId": "111122223333",
            "type": "AWS::KMS::Key",
            "ARN": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab"
        }
    ],
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "111122223333",
    "eventCategory": "Management"
}

```

Decrypt with a KMS key in an external key store

The following example CloudTrail log entry records a Decrypt operation with a KMS key in an [external key store](#). In addition to the `customKeyId`, the `additionalEventData` field includes the [external key ID](#) (`XksKeyId`). The `additionalEventData` isn't specified in the request.

```

{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "IAMUser",
        "principalId": "EX_PRINCIPAL_ID",
        "arn": "arn:aws:iam::111122223333:user/Alice",
        "accountId": "111122223333",
        "accessKeyId": "EXAMPLE_KEY_ID",
        "userName": "Alice"
    },
    "eventTime": "2022-11-24T00:26:58Z",
    "eventSource": "kms.amazonaws.com",
    "eventName": "Decrypt",
    "awsRegion": "us-west-2",

```



```

    "sourceIPAddress": "AWS Internal",
    "requestParameters": {
      "encryptionAlgorithm": "SYMMETRIC_DEFAULT",
      "keyId": "arn:aws:kms:us-west-2:111122223333:key/0987dcba-09fe-87dc-65ba-ab0987654321",
      "encryptionContext": {
        "Department": "Engineering",
        "Purpose": "Test"
      }
    },
    "responseElements": null,
    "additionalEventData": {
      "customKeyStoreId": "cks-9876543210fedcba9",
      "xksKeyId": "abc01234567890fe"
    },
    "requestID": "f1b881f8-2048-41f8-b6cc-382b7857ec61",
    "eventID": "b79603d5-4cde-46fc-819c-a7cf547b9df4",
    "readOnly": true,
    "resources": [
      {
        "accountId": "111122223333",
        "type": "AWS::KMS::Key",
        "ARN": "arn:aws:kms:us-west-2:111122223333:key/0987dcba-09fe-87dc-65ba-ab0987654321"
      }
    ],
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "111122223333",
    "eventCategory": "Management"
  }

```

Decrypt failure with a KMS key in an external key store

The following example CloudTrail log entry records a failed request for a Decrypt operation with a KMS key in an [external key store](#). CloudWatch logs requests that fail, in addition to successful requests. When recording a failure, the CloudTrail log entry includes the exception (errorCode) and the accompanying error message (errorMessage).

If the failed request reached your external key store proxy, as in this example, you can use the requestId value to associate the failed request with a corresponding request your external key store proxy logs, if your proxy provides them.

For help with Decrypt requests in external key stores, see [Decryption errors](#).

```
{
  "eventVersion": "1.08",
  "userIdentity": {
    "type": "IAMUser",
    "principalId": "EX_PRINCIPAL_ID",
    "arn": "arn:aws:iam::111122223333:user/Alice",
    "accountId": "111122223333",
    "accessKeyId": "EXAMPLE_KEY_ID",
    "userName": "Alice"
  },
  "eventTime": "2022-11-24T00:26:58Z",
  "eventSource": "kms.amazonaws.com",
  "eventName": "Decrypt",
  "awsRegion": "us-west-2",
  "sourceIPAddress": "AWS Internal",
  "userAgent": "AWS Internal",
  "errorCode": "KMSInvalidStateException",
  "errorMessage": "The external key store proxy rejected the request because the
specified ciphertext or additional authenticated data is corrupted, missing, or
otherwise invalid.",
  "requestParameters": {
    "encryptionAlgorithm": "SYMMETRIC_DEFAULT",
    "keyId": "arn:aws:kms:us-west-2:111122223333:key/0987dcba-09fe-87dc-65ba-
ab0987654321",
    "encryptionContext": {
      "Department": "Engineering",
      "Purpose": "Test"
    }
  },
  "responseElements": null,
  "additionalEventData": {
    "customKeyId": "cks-9876543210fedcba9",
    "xksKeyId": "abc01234567890fe"
  },
  "requestID": "f1b881f8-2048-41f8-b6cc-382b7857ec61",
  "eventID": "b79603d5-4cde-46fc-819c-a7cf547b9df4",
  "readOnly": true,
  "resources": [
    {
      "accountId": "111122223333",
      "type": "AWS::KMS::Key",

```

```

        "ARN": "arn:aws:kms:us-west-2:111122223333:key/0987dcba-09fe-87dc-65ba-
ab0987654321"
    }
  ],
  "eventType": "AwsApiCall",
  "managementEvent": true,
  "recipientAccountId": "111122223333",
  "eventCategory": "Management"
}

```

DeleteAlias

The following example shows an Amazon CloudTrail log entry for the [DeleteAlias](#) operation. For information about deleting aliases, see [Delete an alias](#).

CloudTrail log entries for this operation recorded on or after December 2022 include the key ARN of the affected KMS key in the `responseElements.keyId` value, even though this operation does not return the key ARN.

```

{
  "eventVersion": "1.02",
  "userIdentity": {
    "type": "IAMUser",
    "principalId": "EX_PRINCIPAL_ID",
    "arn": "arn:aws:iam::111122223333:user/Alice",
    "accountId": "111122223333",
    "accessKeyId": "EXAMPLE_KEY_ID",
    "userName": "Alice",
    "sessionContext": {
      "attributes": {
        "mfaAuthenticated": "false",
        "creationDate": "2014-11-04T00:52:27Z"
      }
    }
  },
  "eventTime": "2014-11-04T00:52:27Z",
  "eventSource": "kms.amazonaws.com",
  "eventName": "DeleteAlias",
  "awsRegion": "us-east-1",
  "sourceIPAddress": "192.0.2.0",
  "userAgent": "Amazon Internal",
  "requestParameters": {
    "aliasName": "alias/my_alias"
  }
}

```

```

    },
    "responseElements": {
      "keyId": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab"
    },
    "requestID": "d9542792-63bc-11e4-bc2b-4198b6150d5c",
    "eventID": "12f48554-bb04-4991-9cfc-e7e85f68eda0",
    "readOnly": false,
    "resources": [{
      "ARN": "arn:aws:kms:us-east-1:111122223333:alias/my_alias",
      "accountId": "111122223333"
    },
    {
      "ARN": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab",
      "accountId": "111122223333"
    }
  ],
  "eventType": "AwsApiCall",
  "recipientAccountId": "111122223333"
}

```

DeleteCustomKeyStore

The following example shows an Amazon CloudTrail log entry generated by calling the [DeleteCustomKeyStore](#) operation. For information about creating custom key stores, see [Delete an Amazon CloudHSM key store](#).

```

{
  "eventVersion": "1.08",
  "userIdentity": {
    "type": "IAMUser",
    "principalId": "EX_PRINCIPAL_ID",
    "arn": "arn:aws:iam::111122223333:user/Alice",
    "accountId": "111122223333",
    "accessKeyId": "EXAMPLE_KEY_ID",
    "userName": "Alice"
  },
  "eventTime": "2021-10-21T20:17:32Z",
  "eventSource": "kms.amazonaws.com",
  "eventName": "DeleteCustomKeyStore",
  "awsRegion": "us-east-1",
  "sourceIPAddress": "192.0.2.0",
  "userAgent": "AWS Internal",

```

```
"requestParameters": {
  "customKeyStoreId": "cks-1234567890abcdef0"
},
"responseElements": null,
"additionalEventData": {
  "customKeyStoreName": "ExampleKeyStore",
  "clusterId": "cluster-1a23b4cdefg"
},
"requestID": "abcde9e1-f1a3-4460-a423-577fb6e695c9",
"eventID": "114b61b9-0ea6-47f5-a9d2-4f2bdd0017d5",
"readOnly": false,
"eventType": "AwsApiCall",
"managementEvent": true,
"recipientAccountId": "111122223333"
}
```

DeleteExpiredKeyMaterial

When you import key material into an Amazon KMS key (KMS key), you can set an expiration date and time for that key material. Amazon KMS records an entry in your CloudTrail log when you [import the key material](#) (with the expiration settings) and when Amazon KMS deletes the expired key material. For information about creating KMS key with imported key material, see [Importing key material for Amazon KMS keys](#).

The following example shows an Amazon CloudTrail log entry generated when Amazon KMS deletes the expired key material.

```
{
  "eventVersion": "1.05",
  "userIdentity": {
    "accountId": "111122223333",
    "invokedBy": "Amazon Internal"
  },
  "eventTime": "2021-01-01T16:00:00Z",
  "eventSource": "kms.amazonaws.com",
  "eventName": "DeleteExpiredKeyMaterial",
  "awsRegion": "us-east-1",
  "sourceIPAddress": "Amazon Internal",
  "userAgent": "Amazon Internal",
  "requestParameters": null,
  "responseElements": null,
  "eventID": "cfa932fd-0d3a-4a76-a8b8-616863a2b547",
```

```
"readOnly": false,
"resources": [
  {
    "accountId": "111122223333",
    "type": "AWS::KMS::Key",
    "ARN": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab"
  }
],
"eventType": "AwsServiceEvent",
"recipientAccountId": "111122223333",
"serviceEventDetails": {
  "keyId": "1234abcd-12ab-34cd-56ef-1234567890ab"
}
}
```

DeleteImportedKeyMaterial

If you import key material into a KMS key, you can delete the imported key material at any time by using the [DeleteImportedKeyMaterial](#) operation. When you delete imported key material from a KMS key, the key state of the KMS key changes to `PendingImport` and the KMS key cannot be used in any cryptographic operations. For details, see [Delete imported key material](#).

The following example shows an Amazon CloudTrail log entry generated for the `DeleteImportedKeyMaterial` operation.

```
{
  "eventVersion": "1.08",
  "userIdentity": {
    "type": "IAMUser",
    "principalId": "EX_PRINCIPAL_ID",
    "arn": "arn:aws:iam::111122223333:user/Alice",
    "accountId": "111122223333",
    "accessKeyId": "EXAMPLE_KEY_ID",
    "userName": "Alice"
  },
  "eventTime": "2022-10-04T21:43:33Z",
  "eventSource": "kms.amazonaws.com",
  "eventName": "DeleteImportedKeyMaterial",
  "awsRegion": "us-west-2",
  "sourceIPAddress": "192.0.2.0",
  "userAgent": "Amazon Internal",
  "requestParameters": {
```

```

    "keyId": "1234abcd-12ab-34cd-56ef-1234567890ab"
  },
  "responseElements": {
    "keyId": "&example-key-arn-1;"
  },
  "requestID": "dcf0e82f-dad0-4622-a378-a5b964ad42c1",
  "eventID": "2afbb991-c668-4641-8a00-67d62e1fecbd",
  "readOnly": false,
  "resources": [
    {
      "accountId": "111122223333",
      "type": "AWS::KMS::Key",
      "ARN": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab"
    }
  ],
  "eventType": "AwsApiCall",
  "managementEvent": true,
  "recipientAccountId": "111122223333",
  "eventCategory": "Management"
}

```

DeleteKey

These examples show the Amazon CloudTrail log entry that is generated when a KMS key is deleted. To delete a KMS key, you use the [ScheduleKeyDeletion](#) operation. After the specified waiting period expires, Amazon KMS deletes the KMS key and records an entry like the following one in your CloudTrail log to record that event.

CloudTrail log entries for this operation recorded on or after December 2022 include the key ARN of the affected KMS key in the `responseElements.keyId` value, even though this operation does not return the key ARN.

For an example of the CloudTrail log entry for the `ScheduleKeyDeletion` operation, see [ScheduleKeyDeletion](#). For information about deleting KMS keys, see [Delete an Amazon KMS key](#).

The following example CloudTrail log entry records a `DeleteKey` operation of a KMS key with key material in Amazon KMS.

```

{
  "eventVersion": "1.08",
  "userIdentity": {

```

```

    "accountId": "111122223333",
    "invokedBy": "Amazon Internal"
  },
  "eventTime": "2020-07-31T00:07:00Z",
  "eventSource": "kms.amazonaws.com",
  "eventName": "DeleteKey",
  "awsRegion": "us-east-1",
  "sourceIPAddress": "Amazon Internal",
  "userAgent": "Amazon Internal",
  "requestParameters": null,
  "responseElements": null,
  "eventID": "b25f9cda-74e1-4458-847b-4972a0bf9668",
  "readOnly": false,
  "resources": [
    {
      "accountId": "111122223333",
      "type": "AWS::KMS::Key",
      "ARN": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab"
    }
  ],
  "eventType": "AwsServiceEvent",
  "recipientAccountId": "111122223333",
  "managementEvent": true,
  "eventCategory": "Management"
}

```

The following CloudTrail log entry records a DeleteKey operation of a KMS key in an Amazon CloudHSM [custom key store](#).

```

{
  "eventVersion": "1.08",
  "userIdentity": {
    "accountId": "111122223333",
    "invokedBy": "Amazon Internal"
  },
  "eventTime": "2021-10-26T23:41:27Z",
  "eventSource": "kms.amazonaws.com",
  "eventName": "DeleteKey",
  "awsRegion": "us-east-1",
  "sourceIPAddress": "Amazon Internal",
  "userAgent": "Amazon Internal",
  "requestParameters": null,

```



```

    "responseElements": {
      "keyId": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab"
    },
    "additionalEventData": {
      "customKeyId": "cks-1234567890abcdef0",
      "clusterId": "cluster-1a23b4cdefg",
      "backingKeys": "[{\\"backingKeyId\\":\\"backing-key-id\\"}]",
      "backingKeysDeletionStatus": "[{\\"backingKeyId\\":\\"backing-key-id\\",
\\"deletionStatus\\":\\"SUCCESS\\"}]"
    },
    "eventID": "1234585c-4b0c-4340-ab11-662414b79239",
    "readOnly": false,
    "resources": [
      {
        "accountId": "111122223333",
        "type": "AWS::KMS::Key",
        "ARN": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab"
      }
    ],
    "eventType": "AwsServiceEvent",
    "recipientAccountId": "111122223333",
    "managementEvent": true,
    "eventCategory": "Management"
  }
}

```

DescribeCustomKeyStores

The following example shows an Amazon CloudTrail log entry generated by calling the [DescribeCustomKeyStores](#) operation. For information about viewing custom key stores, see [View an Amazon CloudHSM key store](#).

```

{
  "eventVersion": "1.08",
  "userIdentity": {
    "type": "IAMUser",
    "principalId": "EX_PRINCIPAL_ID",
    "arn": "arn:aws:iam::111122223333:user/Alice",
    "accountId": "111122223333",
    "accessKeyId": "EXAMPLE_KEY_ID",
    "userName": "Alice"
  },

```

```
"eventTime": "2021-10-21T20:17:32Z",
"eventSource": "kms.amazonaws.com",
"eventName": "DescribeCustomKeyStores",
"awsRegion": "us-east-1",
"sourceIPAddress": "192.0.2.0",
"userAgent": "AWS Internal",
"requestParameters": {
  "customKeyStoreId": "cks-1234567890abcdef0"
},
"responseElements": null,
"requestID": "abcde9e1-f1a3-4460-a423-577fb6e695c9",
"eventID": "2ea1735f-628d-43e3-b2ee-486d02913a78",
"readOnly": true,
"eventType": "AwsApiCall",
"managementEvent": true,
"recipientAccountId": "111122223333"
}
```

DescribeKey

The following example shows an Amazon CloudTrail log entry for the [DescribeKey](#) operation. Amazon KMS records an entry like the following one when you call the DescribeKey operation or [view KMS keys](#) in the Amazon KMS console. This call is the result of viewing a key in the Amazon KMS management console.

```
{
  "eventVersion": "1.08",
  "userIdentity": {
    "type": "IAMUser",
    "principalId": "EX_PRINCIPAL_ID",
    "arn": "arn:aws:iam::111122223333:user/Alice",
    "accountId": "111122223333",
    "accessKeyId": "EXAMPLE_KEY_ID",
    "userName": "Alice"
  },
  "eventTime": "2022-09-26T18:01:36Z",
  "eventSource": "kms.amazonaws.com",
  "eventName": "DescribeKey",
  "awsRegion": "us-west-2",
  "sourceIPAddress": "192.0.2.0",
  "userAgent": "Amazon Internal",
  "requestParameters": {
    "keyId": "1234abcd-12ab-34cd-56ef-1234567890ab"
  }
}
```

```

    },
    "responseElements": null,
    "requestID": "12345126-30d5-4b28-98b9-9153da559963",
    "eventID": "abcde202-ba1a-467c-b4ba-f729d45ae521",
    "readOnly": true,
    "resources": [
      {
        "accountId": "111122223333",
        "type": "AWS::KMS::Key",
        "ARN": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab"
      }
    ],
    "eventType": "AwsApiCall",
    "recipientAccountId": "111122223333"
  }

```

DisableKey

The following example shows an Amazon CloudTrail log entry for the [DisableKey](#) operation. For information about enabling and disabling Amazon KMS keys in Amazon KMS, see [Enable and disable keys](#).

CloudTrail log entries for this operation recorded on or after December 2022 include the key ARN of the affected KMS key in the `responseElements.keyId` value, even though this operation does not return the key ARN.

```

{
  "eventVersion": "1.02",
  "userIdentity": {
    "type": "IAMUser",
    "principalId": "EX_PRINCIPAL_ID",
    "arn": "arn:aws:iam::111122223333:user/Alice",
    "accountId": "111122223333",
    "accessKeyId": "EXAMPLE_KEY_ID",
    "userName": "Alice"
  },
  "eventTime": "2014-11-04T00:52:43Z",
  "eventSource": "kms.amazonaws.com",
  "eventName": "DisableKey",
  "awsRegion": "us-east-1",
  "sourceIPAddress": "192.0.2.0",

```

```

    "userAgent": "Amazon Internal",
    "requestParameters": {
      "keyId": "1234abcd-12ab-34cd-56ef-1234567890ab"
    },
    "responseElements": {
      "keyId": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab"
    },
    "requestID": "12345126-30d5-4b28-98b9-9153da559963",
    "eventID": "abcde202-ba1a-467c-b4ba-f729d45ae521",
    "readOnly": false,
    "resources": [{
      "ARN": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab",
      "accountId": "111122223333"
    }],
    "eventType": "AwsApiCall",
    "recipientAccountId": "111122223333"
  }

```

DisableKeyRotation

The following example shows an Amazon CloudTrail log entry generated by calling the [DisableKeyRotation](#) operation. For information about automatic key rotation, see [Rotate Amazon KMS keys](#).

```

{
  "eventVersion": "1.08",
  "userIdentity": {
    "type": "IAMUser",
    "principalId": "EX_PRINCIPAL_ID",
    "arn": "arn:aws:iam::111122223333:user/Alice",
    "accountId": "111122223333",
    "accessKeyId": "EXAMPLE_KEY_ID",
    "userName": "Alice"
  },
  "eventTime": "2022-09-01T19:31:39Z",
  "eventSource": "kms.amazonaws.com",
  "eventName": "DisableKeyRotation",
  "awsRegion": "us-west-2",
  "sourceIPAddress": "192.0.2.0",
  "userAgent": "Amazon Internal",
  "requestParameters": {

```

```

    "keyId": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab"
  },
  "responseElements": null,
  "requestID": "d6a9351a-ed6e-4581-88d1-2a9a8a538497",
  "eventID": "6313164c-83aa-4cc3-9e1a-b7c426f7a5b1",
  "readOnly": false,
  "resources": [
    {
      "accountId": "111122223333",
      "type": "AWS::KMS::Key",
      "ARN": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab"
    }
  ],
  "eventType": "AwsApiCall",
  "managementEvent": true,
  "recipientAccountId": "111122223333",
  "eventCategory": "Management"
}

```

DisconnectCustomKeyStore

The following example shows an Amazon CloudTrail log entry generated by calling the [DisconnectCustomKeyStore](#) operation. For information about disconnecting a custom key store, see [Disconnect an Amazon CloudHSM key store](#).

```

{
  "eventVersion": "1.08",
  "userIdentity": {
    "type": "IAMUser",
    "principalId": "EX_PRINCIPAL_ID",
    "arn": "arn:aws:iam::111122223333:user/Alice",
    "accountId": "111122223333",
    "accessKeyId": "EXAMPLE_KEY_ID",
    "userName": "Alice"
  },
  "eventTime": "2021-10-21T20:17:32Z",
  "eventSource": "kms.amazonaws.com",
  "eventName": "DisconnectCustomKeyStore",
  "awsRegion": "us-east-1",
  "sourceIPAddress": "192.0.2.0",
  "userAgent": "AWS Internal",

```

```
"requestParameters": {
  "customKeyStoreId": "cks-1234567890abcdef0"
},
"responseElements": null,
"additionalEventData": {
  "customKeyStoreName": "ExampleKeyStore",
  "clusterId": "cluster-1a23b4cdefg"
},
"requestID": "abcde9e1-f1a3-4460-a423-577fb6e695c9",
"eventID": "114b61b9-0ea6-47f5-a9d2-4f2bdd0017d5",
"readOnly": false,
"eventType": "AwsApiCall",
"managementEvent": true,
"recipientAccountId": "111122223333"
}
```

EnableKey

The following example shows an Amazon CloudTrail log entry for the [EnableKey](#) operation. For information about enabling and disabling Amazon KMS keys in Amazon KMS, see [Enable and disable keys..](#)

CloudTrail log entries for this operation recorded on or after December 2022 include the key ARN of the affected KMS key in the `responseElements.keyId` value, even though this operation does not return the key ARN.

```
{
  "eventVersion": "1.02",
  "userIdentity": {
    "type": "IAMUser",
    "principalId": "EX_PRINCIPAL_ID",
    "arn": "arn:aws:iam::111122223333:user/Alice",
    "accountId": "111122223333",
    "accessKeyId": "EXAMPLE_KEY_ID",
    "userName": "Alice"
  },
  "eventTime": "2014-11-04T00:52:20Z",
  "eventSource": "kms.amazonaws.com",
  "eventName": "EnableKey",
  "awsRegion": "us-east-1",
  "sourceIPAddress": "192.0.2.0",
  "userAgent": "Amazon Internal",
  "requestParameters": {
```

```

    "keyId": "1234abcd-12ab-34cd-56ef-1234567890ab"
  },
  "responseElements": {
    "keyId": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab"
  },
  "requestID": "d528a6fb-63bc-11e4-bc2b-4198b6150d5c",
  "eventID": "be393928-3629-4370-9634-567f9274d52e",
  "readOnly": false,
  "resources": [{
    "ARN": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab",
    "accountId": "111122223333"
  }],
  "eventType": "AwsApiCall",
  "recipientAccountId": "111122223333"
}

```

EnableKeyRotation

The following example shows an Amazon CloudTrail log entry of a call to the [EnableKeyRotation](#) operation. For an example of the CloudTrail log entry that is written when the key is rotated, see [RotateKey](#). For information about rotating Amazon KMS keys, see [Rotate Amazon KMS keys](#).

Note

The [rotation-period](#) is an optional request parameter. If you do not specify a rotation period when you enable automatic key rotation, the default value is 365 days.

CloudTrail log entries for this operation recorded on or after December 2022 include the key ARN of the affected KMS key in the `responseElements.keyId` value, even though this operation does not return the key ARN.

```

{
  "eventVersion": "1.05",
  "userIdentity": {
    "type": "IAMUser",
    "principalId": "EX_PRINCIPAL_ID",
    "arn": "arn:aws:iam::111122223333:user/Alice",
    "accountId": "111122223333",
    "accessKeyId": "EXAMPLE_KEY_ID",

```

```

    "userName": "Alice"
  },
  "eventTime": "2020-07-25T23:41:56Z",
  "eventSource": "kms.amazonaws.com",
  "eventName": "EnableKeyRotation",
  "awsRegion": "us-west-2",
  "sourceIPAddress": "192.0.2.0",
  "userAgent": "Amazon Internal",
  "requestParameters": {
    "keyId": "1234abcd-12ab-34cd-56ef-1234567890ab",
    "rotationPeriodInDays": 180
  },
  "responseElements": {
    "keyId": "arn:aws:kms:us-west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab"
  },
  "requestID": "81f5b794-452b-4d6a-932b-68c188165273",
  "eventID": "fefc43a7-8e06-419f-bcab-b3bf18d6a401",
  "readOnly": false,
  "resources": [
    {
      "accountId": "111122223333",
      "type": "AWS::KMS::Key",
      "ARN": "arn:aws:kms:us-west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab"
    }
  ],
  "eventType": "AwsApiCall",
  "recipientAccountId": "111122223333"
}

```

Encrypt

The following example shows an Amazon CloudTrail log entry for the [Encrypt](#) operation.

```

{
  "eventVersion": "1.02",
  "userIdentity": {
    "type": "IAMUser",
    "principalId": "EX_PRINCIPAL_ID",
    "arn": "arn:aws:iam::111122223333:user/Alice",
    "accountId": "111122223333",
    "accessKeyId": "EXAMPLE_KEY_ID",

```



```

    "userName": "Alice"
  },
  "eventTime": "2022-07-14T20:17:42Z",
  "eventSource": "kms.amazonaws.com",
  "eventName": "Encrypt",
  "awsRegion": "us-east-1",
  "sourceIPAddress": "192.0.2.0",
  "userAgent": "Amazon Internal",
  "requestParameters": {
    "encryptionContext": {
      "Department": "Engineering"
    },
    "keyId": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab",
    "encryptionAlgorithm": "SYMMETRIC_DEFAULT",
  },
  "responseElements": null,
  "requestID": "f3423043-63bc-11e4-bc2b-4198b6150d5c",
  "eventID": "91235988-eb87-476a-ac2c-0cdc244e6dca",
  "readOnly": true,
  "resources": [{
    "ARN": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab",
    "accountId": "111122223333"
  }],
  "eventType": "AwsApiCall",
  "recipientAccountId": "111122223333"
}

```

GenerateDataKey

The following example shows an Amazon CloudTrail log entry for the [GenerateDataKey](#) operation.

```

{
  "eventVersion": "1.02",
  "userIdentity": {
    "type": "IAMUser",
    "principalId": "EX_PRINCIPAL_ID",
    "arn": "arn:aws:iam::111122223333:user/Alice",
    "accountId": "111122223333",
    "accessKeyId": "EXAMPLE_KEY_ID",
    "userName": "Alice"
  },

```

```

    "eventTime": "2014-11-04T00:52:40Z",
    "eventSource": "kms.amazonaws.com",
    "eventName": "GenerateDataKey",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "192.0.2.0",
    "userAgent": "Amazon Internal",
    "requestParameters": {
      "keyId": "1234abcd-12ab-34cd-56ef-1234567890ab",
      "keySpec": "AES_256",
      "encryptionContext": {
        "Department": "Engineering",
        "Project": "Alpha"
      }
    },
    "responseElements": null,
    "requestID": "e0eb83e3-63bc-11e4-bc2b-4198b6150d5c",
    "eventID": "a9dea4f9-8395-46c0-942c-f509c02c2b71",
    "readOnly": true,
    "resources": [{
      "ARN": "arn:aws:kms:us-west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab",
      "accountId": "111122223333"
    }],
    "eventType": "AwsApiCall",
    "recipientAccountId": "111122223333"
  }

```

GenerateDataKeyPair

The following example shows an Amazon CloudTrail log entry for the [GenerateDataKeyPair](#) operation. This example records an operation that generates an RSA key pair encrypted under a symmetric encryption Amazon KMS key.

```

{
  "eventVersion": "1.05",
  "userIdentity": {
    "type": "IAMUser",
    "principalId": "EX_PRINCIPAL_ID",
    "arn": "arn:aws:iam::111122223333:user/Alice",
    "accountId": "111122223333",
    "accessKeyId": "EXAMPLE_KEY_ID",
    "userName": "Alice"
  },

```

```

"eventTime": "2020-07-27T18:57:57Z",
"eventSource": "kms.amazonaws.com",
"eventName": "GenerateDataKeyPair",
"awsRegion": "us-west-2",
"sourceIPAddress": "192.0.2.0",
"userAgent": "Amazon Internal",
"requestParameters": {
  "keyPairSpec": "RSA_3072",
  "encryptionContext": {
    "Project": "Alpha"
  },
  "keyId": "1234abcd-12ab-34cd-56ef-1234567890ab"
},
"responseElements": null,
"requestID": "52fb127b-0fe5-42bb-8e5e-f560febde6b0",
"eventID": "9b6bd6d2-529d-4890-a949-593b13800ad7",
"readOnly": true,
"resources": [
  {
    "accountId": "111122223333",
    "type": "AWS::KMS::Key",
    "ARN": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab"
  }
],
"eventType": "AwsApiCall",
"recipientAccountId": "111122223333"
}

```

GenerateDataKeyPairWithoutPlaintext

The following example shows an Amazon CloudTrail log entry for the [GenerateDataKeyPairWithoutPlaintext](#) operation. This example records an operation that generates an RSA key pair that is encrypted under a symmetric encryption Amazon KMS key.

```

{
  "eventVersion": "1.05",
  "userIdentity": {
    "type": "IAMUser",
    "principalId": "EX_PRINCIPAL_ID",
    "arn": "arn:aws:iam::111122223333:user/Alice",
    "accountId": "111122223333",
    "accessKeyId": "EXAMPLE_KEY_ID",

```

```

        "userName": "Alice"
    },
    "eventTime": "2020-07-27T18:57:57Z",
    "eventSource": "kms.amazonaws.com",
    "eventName": "GenerateDataKeyPairWithoutPlaintext",
    "awsRegion": "us-west-2",
    "sourceIPAddress": "192.0.2.0",
    "userAgent": "Amazon Internal",
    "requestParameters": {
        "keyPairSpec": "RSA_4096",
        "encryptionContext": {
            "Index": "5"
        }
    },
    "keyId": "1234abcd-12ab-34cd-56ef-1234567890ab"
},
"responseElements": null,
"requestID": "52fb127b-0fe5-42bb-8e5e-f560febde6b0",
"eventID": "9b6bd6d2-529d-4890-a949-593b13800ad7",
"readOnly": true,
"resources": [
    {
        "accountId": "111122223333",
        "type": "AWS::KMS::Key",
        "ARN": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab"
    }
],
"eventType": "AwsApiCall",
"recipientAccountId": "111122223333"
}

```

GenerateDataKeyWithoutPlaintext

The following example shows an Amazon CloudTrail log entry for the [GenerateDataKeyWithoutPlaintext](#) operation.

```

{
    "eventVersion": "1.02",
    "userIdentity": {
        "type": "IAMUser",
        "principalId": "EX_PRINCIPAL_ID",
        "arn": "arn:aws:iam::111122223333:user/Alice",
        "accountId": "111122223333",

```

```

    "accessKeyId": "EXAMPLE_KEY_ID",
    "userName": "Alice"
  },
  "eventTime": "2014-11-04T00:52:23Z",
  "eventSource": "kms.amazonaws.com",
  "eventName": "GenerateDataKeyWithoutPlaintext",
  "awsRegion": "us-east-1",
  "sourceIPAddress": "192.0.2.0",
  "userAgent": "Amazon Internal",
  "errorCode": "InvalidKeyUsageException",
  "requestParameters": {
    "keyId": "1234abcd-12ab-34cd-56ef-1234567890ab",
    "keySpec": "AES_256",
    "encryptionContext": {
      "Project": "Alpha"
    }
  },
  "responseElements": null,
  "requestID": "d6b8e411-63bc-11e4-bc2b-4198b6150d5c",
  "eventID": "f7734272-9ec5-4c80-9f36-528ebbe35e4a",
  "readOnly": true,
  "resources": [{
    "ARN": "arn:aws:kms:us-west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab",
    "accountId": "111122223333"
  }],
  "eventType": "AwsApiCall",
  "recipientAccountId": "111122223333"
}

```

GenerateMac

The following example shows an Amazon CloudTrail log entry for the [GenerateMac](#) operation.

```

{
  "eventVersion": "1.08",
  "userIdentity": {
    "type": "IAMUser",
    "principalId": "EX_PRINCIPAL_ID",
    "arn": "arn:aws:iam::111122223333:user/Alice",
    "accountId": "111122223333",
    "accessKeyId": "EXAMPLE_KEY_ID",
    "userName": "Alice"
  }
}

```

```

    },
    "eventTime": "2022-12-23T19:26:54Z",
    "eventSource": "kms.amazonaws.com",
    "eventName": "GenerateMac",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "192.0.2.0",
    "userAgent": "Amazon Internal",
    "requestParameters": {
      "macAlgorithm": "HMAC_SHA_512",
      "keyId": "1234abcd-12ab-34cd-56ef-1234567890ab"
    },
    "responseElements": null,
    "requestID": "e0eb83e3-63bc-11e4-bc2b-4198b6150d5c",
    "eventID": "a9dea4f9-8395-46c0-942c-f509c02c2b71",
    "readOnly": true,
    "resources": [
      {
        "accountId": "111122223333",
        "ARN": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab"
      }
    ],
    "eventType": "AwsApiCall",
    "recipientAccountId": "111122223333",
    "eventCategory": "Management"
  }

```

GenerateRandom

The following example shows an Amazon CloudTrail log entry for the [GenerateRandom](#) operation. Because this operation doesn't use an Amazon KMS key, the `resources` field is empty.

```

{
  "eventVersion": "1.02",
  "userIdentity": {
    "type": "IAMUser",
    "principalId": "EX_PRINCIPAL_ID",
    "arn": "arn:aws:iam::111122223333:user/Alice",
    "accountId": "111122223333",
    "accessKeyId": "EXAMPLE_KEY_ID",
    "userName": "Alice"
  },
  "eventTime": "2014-11-04T00:52:37Z",

```

```

    "eventSource": "kms.amazonaws.com",
    "eventName": "GenerateRandom",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "192.0.2.0",
    "userAgent": "Amazon Internal",
    "requestParameters": null,
    "responseElements": null,
    "requestID": "df1e3de6-63bc-11e4-bc2b-4198b6150d5c",
    "eventID": "239cb9f7-ae05-4c94-9221-6ea30eef0442",
    "readOnly": true,
    "resources": [],
    "eventType": "AwsApiCall",
    "recipientAccountId": "111122223333"
  }

```

GetKeyPolicy

The following example shows an Amazon CloudTrail log entry for the [GetKeyPolicy](#) operation. For information about viewing the key policy for a KMS key, see [View a key policies](#).

```

{
  "eventVersion": "1.02",
  "userIdentity": {
    "type": "IAMUser",
    "principalId": "EX_PRINCIPAL_ID",
    "arn": "arn:aws:iam::111122223333:user/Alice",
    "accountId": "111122223333",
    "accessKeyId": "EXAMPLE_KEY_ID",
    "userName": "Alice"
  },
  "eventTime": "2014-11-04T00:50:30Z",
  "eventSource": "kms.amazonaws.com",
  "eventName": "GetKeyPolicy",
  "awsRegion": "us-east-1",
  "sourceIPAddress": "192.0.2.0",
  "userAgent": "Amazon Internal",
  "requestParameters": {
    "keyId": "1234abcd-12ab-34cd-56ef-1234567890ab",
    "policyName": "default"
  },
  "responseElements": null,
  "requestID": "93746dd6-63bc-11e4-bc2b-4198b6150d5c",
  "eventID": "4aa7e4d5-d047-452a-a5a6-2cce282a7e82",

```

```

    "readOnly": true,
    "resources": [{
      "ARN": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab",
      "accountId": "111122223333"
    }],
    "eventType": "AwsApiCall",
    "recipientAccountId": "111122223333"
  }

```

GetKeyRotationStatus

The following example shows an Amazon CloudTrail log entry for the [GetKeyRotationStatus](#) operation. For information about automatic and on-demand rotation of key material for a KMS key, see [Rotate Amazon KMS keys](#).

```

{
  "eventVersion": "1.08",
  "userIdentity": {
    "type": "IAMUser",
    "principalId": "EX_PRINCIPAL_ID",
    "arn": "arn:aws:iam::111122223333:user/Alice",
    "accountId": "111122223333",
    "accessKeyId": "EXAMPLE_KEY_ID",
    "userName": "Alice"
  },
  "eventTime": "2024-02-20T19:16:45Z",
  "eventSource": "kms.amazonaws.com",
  "eventName": "GetKeyRotationStatus",
  "awsRegion": "us-east-1",
  "sourceIPAddress": "192.0.2.0",
  "userAgent": "Amazon Internal",
  "requestParameters": {
    "keyId": "1234abcd-12ab-34cd-56ef-1234567890ab"
  },
  "responseElements": null,
  "requestID": "12f9b7e8-49b9-4c1c-a7e3-34ac0cdf0467",
  "eventID": "3d082126-9e7d-4167-8372-a6cfcbed4be6",
  "readOnly": true,
  "resources": [
    {
      "accountId": "111122223333",
      "type": "AWS::KMS::Key",

```



```

        "ARN": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab"
    }
  ],
  "eventType": "AwsApiCall",
  "managementEvent": true,
  "recipientAccountId": "111122223333",
  "eventCategory": "Management"
  "tlsDetails": {
    "tlsVersion": "TLSv1.2",
    "cipherSuite": "ECDHE-RSA-AES256-GCM-SHA384",
    "clientProvidedHostHeader": "kms.us-east-1.amazonaws.com"
  }
}

```

GetParametersForImport

The following example shows an Amazon CloudTrail log entry generated when you use the [GetParametersForImport](#) operation. This operation returns the public key and import token that you use when importing key material into a KMS key. The same CloudTrail entry is recorded when you use the `GetParametersForImport` operation or use the Amazon KMS console to [download the public key and import token](#).

```

{
  "eventVersion": "1.05",
  "userIdentity": {
    "type": "IAMUser",
    "principalId": "EX_PRINCIPAL_ID",
    "arn": "arn:aws:iam::111122223333:user/Alice",
    "accountId": "111122223333",
    "accessKeyId": "EXAMPLE_KEY_ID",
    "userName": "Alice"
  },
  "eventTime": "2020-07-25T23:58:23Z",
  "eventSource": "kms.amazonaws.com",
  "eventName": "GetParametersForImport",
  "awsRegion": "us-west-2",
  "sourceIPAddress": "192.0.2.0",
  "userAgent": "Amazon Internal",
  "requestParameters": {
    "keyId": "1234abcd-12ab-34cd-56ef-1234567890ab",
    "wrappingAlgorithm": "RSAES_OAEP_SHA_256",
    "wrappingKeySpec": "RSA_2048"
  }
}

```

```

    },
    "responseElements": null,
    "requestID": "b5786406-e3c7-43d6-8d3c-6d5ef96e2278",
    "eventID": "4023e622-0c3e-4324-bdef-7f58193bba87",
    "readOnly": true,
    "resources": [
      {
        "accountId": "111122223333",
        "type": "AWS::KMS::Key",
        "ARN": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab"
      }
    ],
    "eventType": "AwsApiCall",
    "recipientAccountId": "111122223333"
  }

```

ImportKeyMaterial

The following example shows an Amazon CloudTrail log entry generated when you use the [ImportKeyMaterial](#) operation. The same CloudTrail entry is recorded when you use the `ImportKeyMaterial` operation or use the Amazon KMS console to [import key material](#) into an Amazon KMS key.

CloudTrail log entries for this operation recorded on or after December 2022 include the key ARN of the affected KMS key in the `responseElements.keyId` value, even though this operation does not return the key ARN.

```

{
  "eventVersion": "1.05",
  "userIdentity": {
    "type": "IAMUser",
    "principalId": "EX_PRINCIPAL_ID",
    "arn": "arn:aws:iam::111122223333:user/Alice",
    "accountId": "111122223333",
    "accessKeyId": "EXAMPLE_KEY_ID",
    "userName": "Alice"
  },
  "eventTime": "2020-07-26T00:08:00Z",
  "eventSource": "kms.amazonaws.com",
  "eventName": "ImportKeyMaterial",
  "awsRegion": "us-west-2",

```

```

"sourceIPAddress": "192.0.2.0",
"userAgent": "Amazon Internal",
"requestParameters": {
  "keyId": "1234abcd-12ab-34cd-56ef-1234567890ab",
  "validTo": "Jan 1, 2021 8:00:00 PM",
  "expirationModel": "KEY_MATERIAL_EXPIRES"
},
"responseElements": {
  "keyId": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab"
},
"requestID": "89e10ee7-a612-414d-95a2-a128346969fd",
"eventID": "c7abd205-a5a2-4430-bbfa-fc10f3e2d79f",
"readOnly": false,
"resources": [
  {
    "accountId": "111122223333",
    "type": "AWS::KMS::Key",
    "ARN": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab"
  }
],
"eventType": "AwsApiCall",
"recipientAccountId": "111122223333"
}

```

ListAliases

The following example shows an Amazon CloudTrail log entry for the [ListAliases](#) operation. Because this operation doesn't use any particular alias or Amazon KMS key, the resources field is empty. For information about viewing aliases in Amazon KMS, see [Find the alias name and alias ARN for a KMS key](#).

```

{
  "eventVersion": "1.02",
  "userIdentity": {
    "type": "IAMUser",
    "principalId": "EX_PRINCIPAL_ID",
    "arn": "arn:aws:iam::111122223333:user/Alice",
    "accountId": "111122223333",
    "accessKeyId": "EXAMPLE_KEY_ID",
    "userName": "Alice"
  },

```

```

    "eventTime": "2014-11-04T00:51:45Z",
    "eventSource": "kms.amazonaws.com",
    "eventName": "ListAliases",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "192.0.2.0",
    "userAgent": "Amazon Internal",
    "requestParameters": {
      "limit": 5,
      "marker":
"eyJiIjojYWxpYXNvZTU0Y2MxOTMmYTMwNC00YzEwLTliZWItYTJjZjA3NjA2OTJhIiwieSI6ImFsaWFzL2U1NGNjMTkzL",
    },
    "responseElements": null,
    "requestID": "bfe6c190-63bc-11e4-bc2b-4198b6150d5c",
    "eventID": "a27dda7b-76f1-4ac3-8b40-42dfba77bcd6",
    "readOnly": true,
    "resources": [],
    "eventType": "AwsApiCall",
    "recipientAccountId": "111122223333"
  }
}

```

ListGrants

The following example shows an Amazon CloudTrail log entry for the [ListGrant](#) operation. For information about grants in Amazon KMS, see [Grants in Amazon KMS](#).

```

{
  "eventVersion": "1.02",
  "userIdentity": {
    "type": "IAMUser",
    "principalId": "EX_PRINCIPAL_ID",
    "arn": "arn:aws:iam::111122223333:user/Alice",
    "accountId": "111122223333",
    "accessKeyId": "EXAMPLE_KEY_ID",
    "userName": "Alice"
  },
  "eventTime": "2014-11-04T00:52:49Z",
  "eventSource": "kms.amazonaws.com",
  "eventName": "ListGrants",
  "awsRegion": "us-east-1",
  "sourceIPAddress": "192.0.2.0",
  "userAgent": "Amazon Internal",
  "requestParameters": {
    "keyId": "1234abcd-12ab-34cd-56ef-1234567890ab",

```



```

"responseElements": null,
"requestID": "99c88d32-f2db-455e-8a9a-23855258a452",
"eventID": "8ce0e74b-b9c7-45a2-96ef-83136d38068e",
"readOnly": true,
"resources": [
  {
    "accountId": "111122223333",
    "type": "AWS::KMS::Key",
    "ARN": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab"
  }
],
"eventType": "AwsApiCall",
"managementEvent": true,
"recipientAccountId": "111122223333",
"eventCategory": "Management",
"tlsDetails": {
  "tlsVersion": "TLSv1.2",
  "cipherSuite": "ECDHE-RSA-AES256-GCM-SHA384",
  "clientProvidedHostHeader": "kms.us-east-1.amazonaws.com"
}
}

```

PutKeyPolicy

The following example shows an Amazon CloudTrail log entry generated by calling the [PutKeyPolicy](#) operation. For information about updating a key policy, see [Change a key policy](#).

```

{
  "eventVersion": "1.08",
  "userIdentity": {
    "type": "IAMUser",
    "principalId": "EX_PRINCIPAL_ID",
    "arn": "arn:aws:iam::111122223333:user/Alice",
    "accountId": "111122223333",
    "accessKeyId": "EXAMPLE_KEY_ID",
    "userName": "Alice"
  },
  "eventTime": "2022-09-01T20:06:16Z",
  "eventSource": "kms.amazonaws.com",
  "eventName": "PutKeyPolicy",
  "awsRegion": "us-west-2",
  "sourceIPAddress": "192.0.2.0",

```

```

"userAgent": "Amazon Internal",
"requestParameters": {
  "keyId": "1234abcd-12ab-34cd-56ef-1234567890ab",
  "policyName": "default",
  "policy": "{\n  \"Version\" : \"2012-10-17\",\n  \"Id\" : \"key-default-1\",\n  \"Statement\" : [ {\n    \"Sid\" : \"Enable IAM User Permissions\",\n    \"Effect\" :\n  \"Allow\",\n    \"Principal\" : {\n      \"AWS\" : \"arn:aws:iam::111122223333:root\n    },\n    \"Action\" : \"kms:*\",\n    \"Resource\" : \"*\"\n  } ]\n}",
  "bypassPolicyLockoutSafetyCheck": false
},
"responseElements": null,
"requestID": "7bb906fa-dc21-4350-b65c-808ff0f72f55",
"eventID": "c217db1f-903f-4a2f-8f88-9580182d6313",
"readOnly": false,
"resources": [
  {
    "accountId": "111122223333",
    "type": "AWS::KMS::Key",
    "ARN": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab"
  }
],
"eventType": "AwsApiCall",
"managementEvent": true,
"recipientAccountId": "111122223333",
"eventCategory": "Management"
}

```

ReEncrypt

The following example shows an Amazon CloudTrail log entry for the [ReEncrypt](#) operation. The `resources` field in this log entry specifies two Amazon KMS keys, the source KMS key and the destination KMS key, in that order.

```

{
  "eventVersion": "1.05",
  "userIdentity": {
    "type": "IAMUser",
    "principalId": "EX_PRINCIPAL_ID",
    "arn": "arn:aws:iam::111122223333:user/Alice",
    "accountId": "111122223333",
    "accessKeyId": "EXAMPLE_KEY_ID",
    "userName": "Alice"
  }
}

```

```
  },
  "eventTime": "2020-07-27T23:09:13Z",
  "eventSource": "kms.amazonaws.com",
  "eventName": "ReEncrypt",
  "awsRegion": "us-west-2",
  "sourceIPAddress": "192.0.2.0",
  "userAgent": "Amazon Internal",
  "requestParameters": {
    "sourceEncryptionAlgorithm": "SYMMETRIC_DEFAULT",
    "sourceEncryptionContext": {
      "Project": "Alpha",
      "Department": "Engineering"
    },
    "destinationKeyId": "0987dcba-09fe-87dc-65ba-ab0987654321",
    "destinationEncryptionAlgorithm": "SYMMETRIC_DEFAULT",
    "destinationEncryptionContext": {
      "Level": "3A"
    }
  },
  "responseElements": null,
  "requestID": "03769fd4-acf9-4b33-adf3-2ab8ca73aadf",
  "eventID": "542d9e04-0e8d-4e05-bf4b-4bdeb032e6ec",
  "readOnly": true,
  "resources": [
    {
      "accountId": "111122223333",
      "type": "AWS::KMS::Key",
      "ARN": "arn:aws:kms:us-west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab"
    },
    {
      "accountId": "111122223333",
      "type": "AWS::KMS::Key",
      "ARN": "arn:aws:kms:us-west-2:111122223333:key/0987dcba-09fe-87dc-65ba-ab0987654321"
    }
  ],
  "eventType": "AwsApiCall",
  "recipientAccountId": "111122223333"
}
```


ReplicateKey

The following example shows an Amazon CloudTrail log entry generated by calling the [ReplicateKey](#) operation. A `ReplicateKey` request results in a `ReplicateKey` operation and a `CreateKey` operation.

For information about replicating multi-Region keys, see [Create multi-Region replica keys](#).

```
{
  "eventVersion": "1.08",
  "userIdentity": {
    "type": "IAMUser",
    "principalId": "EX_PRINCIPAL_ID",
    "arn": "arn:aws:iam::111122223333:user/Alice",
    "accountId": "111122223333",
    "accessKeyId": "EXAMPLE_KEY_ID",
    "userName": "Alice"
  },
  "eventTime": "2020-11-18T01:29:18Z",
  "eventSource": "kms.amazonaws.com",
  "eventName": "ReplicateKey",
  "awsRegion": "us-east-1",
  "sourceIPAddress": "192.0.2.0",
  "userAgent": "AWS Internal",
  "requestParameters": {
    "keyId": "1234abcd-12ab-34cd-56ef-1234567890ab",
    "replicaRegion": "us-west-2",
    "bypassPolicyLockoutSafetyCheck": false,
    "description": ""
  },
  "responseElements": {
    "replicaKeyMetadata": {
      "awsAccountId": "111122223333",
      "keyId": "1234abcd-12ab-34cd-56ef-1234567890ab",
      "arn": "arn:aws:kms:us-west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab",
      "creationDate": "Nov 18, 2020, 1:29:18 AM",
      "enabled": false,
      "description": "",
      "keyUsage": "ENCRYPT_DECRYPT",
      "keyState": "Creating",
      "origin": "AWS_KMS",
      "keyManager": "CUSTOMER",
```

```

    "keySpec": "SYMMETRIC_DEFAULT",
    "customerMasterKeySpec": "SYMMETRIC_DEFAULT",
    "encryptionAlgorithms": [
      "SYMMETRIC_DEFAULT"
    ],
    "multiRegion": true,
    "multiRegionConfiguration": {
      "multiRegionKeyType": "REPLICA",
      "primaryKey": {
        "arn": "arn:aws:kms:us-
east-1:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab",
        "region": "us-east-1"
      },
      "replicaKeys": [
        {
          "arn": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab",
          "region": "us-west-2"
        }
      ]
    },
    "replicaPolicy": "{\n  \"Version\": \"2012-10-17\", \n  \"Statement\": [{\n    \n    \"Effect\": \"Allow\", \n    \"Principal\": {\"AWS\": \"arn:aws:iam:123456789012:user/Alice\"}, \n    \"Action\": \"kms:*\", \n    \"Resource\": \"*\" \n  }, {\n    \"Effect\": \"Allow\", \n    \"Principal\": {\"AWS\": \"arn:aws:iam:012345678901:user/Bob\"}, \n    \"Action\": \"kms:CreateGrant\", \n    \"Resource\": \"*\" \n  }, {\n    \"Effect\": \"Allow\", \n    \"Principal\": {\"AWS\": \"arn:aws:iam:012345678901:user/Charlie\"}, \n    \"Action\": \"kms:Encrypt\", \n    \"Resource\": \"*\" \n  }]\n}",
    "requestID": "abcdef68-63bc-11e4-bc2b-4198b6150d5c",
    "eventID": "fedcba44-6773-4f96-8763-1993aec9ae6a",
    "readOnly": false,
    "resources": [
      {
        "accountId": "111122223333",
        "type": "AWS::KMS::Key",
        "ARN": "arn:aws:kms:us-
east-1:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab"
      }
    ],
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "111122223333",

```

```
"eventCategory": "Management"
}
```

RetireGrant

The following example shows an Amazon CloudTrail log entry generated by calling the [RetireGrant](#) operation. For information about retiring grants, see [Retiring and revoking grants](#).

```
{
  "eventVersion": "1.08",
  "userIdentity": {
    "type": "IAMUser",
    "principalId": "EX_PRINCIPAL_ID",
    "arn": "arn:aws:iam::111122223333:user/Alice",
    "accountId": "111122223333",
    "accessKeyId": "EXAMPLE_KEY_ID",
    "userName": "Alice"
  },
  "eventTime": "2022-09-01T19:39:33Z",
  "eventSource": "kms.amazonaws.com",
  "eventName": "RetireGrant",
  "awsRegion": "us-west-2",
  "sourceIPAddress": "192.0.2.0",
  "userAgent": "Amazon Internal",
  "requestParameters": null,
  "responseElements": null,
  "additionalEventData": {
    "grantId": "abcde1237f76e4ba7987489ac329fbfba6ad343d6f7075dbd1ef191f0120514a"
  },
  "requestID": "1d274d57-5697-462c-a004-f25fcc29fa26",
  "eventID": "0771bcfb-3e24-4332-9ac8-e1c06563eecf",
  "readOnly": false,
  "resources": [
    {
      "accountId": "111122223333",
      "type": "AWS::KMS::Key",
      "ARN": "arn:aws:kms:us-west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab"
    }
  ],
  "eventType": "AwsApiCall",
  "managementEvent": true,
  "recipientAccountId": "111122223333",
}
```

```
"eventCategory": "Management"
}
```

RevokeGrant

The following example shows an Amazon CloudTrail log entry generated by calling the [RevokeGrant](#) operation. For information about revoking grants, see [Retiring and revoking grants](#).

```
{
  "eventVersion": "1.08",
  "userIdentity": {
    "type": "IAMUser",
    "principalId": "EX_PRINCIPAL_ID",
    "arn": "arn:aws:iam::111122223333:user/Alice",
    "accountId": "111122223333",
    "accessKeyId": "EXAMPLE_KEY_ID",
    "userName": "Alice"
  },
  "eventTime": "2022-09-01T19:35:17Z",
  "eventSource": "kms.amazonaws.com",
  "eventName": "RevokeGrant",
  "awsRegion": "us-west-2",
  "sourceIPAddress": "192.0.2.0",
  "userAgent": "Amazon Internal",
  "requestParameters": {
    "keyId": "1234abcd-12ab-34cd-56ef-1234567890ab",
    "grantId": "abcde1237f76e4ba7987489ac329fbfba6ad343d6f7075dbd1ef191f0120514a"
  },
  "responseElements": null,
  "requestID": "59d94c03-c5b7-428d-ae6e-f2c4b47d2917",
  "eventID": "07a23a39-6526-4ae2-b31e-d35fbe9e24ee",
  "readOnly": false,
  "resources": [
    {
      "accountId": "111122223333",
      "type": "AWS::KMS::Key",
      "ARN": "arn:aws:kms:us-west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab"
    }
  ],
  "eventType": "AwsApiCall",
  "managementEvent": true,
  "recipientAccountId": "111122223333",
}
```

```
"eventCategory": "Management"
}
```

RotateKey

These examples show the Amazon CloudTrail log entries for the operations that rotate Amazon KMS keys. For information about rotating KMS keys, see [Rotate Amazon KMS keys](#).

The following example shows a CloudTrail log entry for the operation that rotates a symmetric encryption KMS key on which automatic key rotation is enabled. For information about enabling automatic rotation, see [Rotate Amazon KMS keys](#).

For an example of the CloudTrail log entry that records the EnableKeyRotation operation, see [EnableKeyRotation](#).

```
{
  "eventVersion": "1.08",
  "userIdentity": {
    "accountId": "111122223333",
    "invokedBy": "Amazon Internal"
  },
  "eventTime": "2021-01-14T01:41:59Z",
  "eventSource": "kms.amazonaws.com",
  "eventName": "RotateKey",
  "awsRegion": "us-west-2",
  "sourceIPAddress": "Amazon Internal",
  "userAgent": "Amazon Internal",
  "requestParameters": null,
  "responseElements": null,
  "eventID": "a24b3967-ddad-417f-9b22-2332b918db06",
  "readOnly": false,
  "resources": [
    {
      "accountId": "111122223333",
      "type": "AWS::KMS::Key",
      "ARN": "arn:aws:kms:us-west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab"
    }
  ],
  "eventType": "AwsServiceEvent",
  "recipientAccountId": "111122223333",
  "serviceEventDetails": {
    "rotationType": "AUTOMATIC",
```

```

    "keyId": "1234abcd-12ab-34cd-56ef-1234567890ab"
  },
  "eventCategory": "Management"
}

```

The following example shows a CloudTrail log entry for a [RotateKeyOnDemand](#) operation. For information about rotating symmetric encryption KMS keys on-demand, see [Perform on-demand key rotation](#).

For an example of the CloudTrail log entry that records the RotateKeyOnDemand operation, see [RotateKeyOnDemand](#).

```

{
  "eventVersion": "1.08",
  "userIdentity": {
    "accountId": "111122223333",
    "invokedBy": "Amazon Internal"
  },
  "eventTime": "2021-01-14T01:41:59Z",
  "eventSource": "kms.amazonaws.com",
  "eventName": "RotateKey",
  "awsRegion": "us-west-2",
  "sourceIPAddress": "Amazon Internal",
  "userAgent": "Amazon Internal",
  "requestParameters": null,
  "responseElements": null,
  "eventID": "a24b3967-ddad-417f-9b22-2332b918db06",
  "readOnly": false,
  "resources": [
    {
      "accountId": "111122223333",
      "type": "AWS::KMS::Key",
      "ARN": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab"
    }
  ],
  "eventType": "AwsServiceEvent",
  "recipientAccountId": "111122223333",
  "serviceEventDetails": {
    "rotationType": "ON_DEMAND",
    "keyId": "1234abcd-12ab-34cd-56ef-1234567890ab"
  },
  "eventCategory": "Management"
}

```

```
}
```

RotateKeyOnDemand

The following example shows an Amazon CloudTrail log entry for the [RotateKeyOnDemand](#) operation. For an example of the CloudTrail log entry that is written when the key is rotated, see [RotateKey](#). For more information about on-demand rotation of key material for a KMS key, see [Perform on-demand key rotation](#).

```
{
  "eventVersion": "1.08",
  "userIdentity": {
    "type": "IAMUser",
    "principalId": "EX_PRINCIPAL_ID",
    "arn": "arn:aws:iam::111122223333:user/Alice",
    "accountId": "111122223333",
    "accessKeyId": "EXAMPLE_KEY_ID",
    "userName": "Alice"
  },
  "eventTime": "2024-02-20T17:41:57Z",
  "eventSource": "kms.amazonaws.com",
  "eventName": "RotateKeyOnDemand",
  "awsRegion": "us-east-1",
  "sourceIPAddress": "192.0.2.0",
  "userAgent": "Amazon Internal",
  "requestParameters": {
    "keyId": "1234abcd-12ab-34cd-56ef-1234567890ab"
  },
  "responseElements": {
    "keyId": "1234abcd-12ab-34cd-56ef-1234567890ab"
  },
  "requestID": "9e1dee86-eb84-42fd-8f25-e3fc7dbb32c8",
  "eventID": "00a09fbc-20d6-4a58-9b92-7da85984ab77",
  "readOnly": false,
  "resources": [
    {
      "accountId": "111122223333",
      "type": "AWS::KMS::Key",
      "ARN": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab"
    }
  ],
  "eventType": "AwsApiCall",
```

```
"managementEvent": true,
"recipientAccountId": "111122223333",
"eventCategory": "Management",
"tlsDetails": {
  "tlsVersion": "TLSv1.2",
  "cipherSuite": "ECDHE-RSA-AES256-GCM-SHA384",
  "clientProvidedHostHeader": "kms.us-east-1.amazonaws.com"
}
}
```

ScheduleKeyDeletion

These examples show Amazon CloudTrail log entries for the [ScheduleKeyDeletion](#) operation.

For an example of the CloudTrail log entry that is written when the key is deleted, see [DeleteKey](#). For information about deleting Amazon KMS keys, see [Delete an Amazon KMS key](#).

The following example records a ScheduleKeyDeletion request for a single-Region KMS key.

```
{
  "eventVersion": "1.08",
  "userIdentity": {
    "type": "IAMUser",
    "principalId": "EX_PRINCIPAL_ID",
    "arn": "arn:aws:iam::111122223333:user/Alice",
    "accountId": "111122223333",
    "accessKeyId": "EXAMPLE_KEY_ID",
    "userName": "Alice"
  },
  "eventTime": "2021-03-23T18:58:30Z",
  "eventSource": "kms.amazonaws.com",
  "eventName": "ScheduleKeyDeletion",
  "awsRegion": "us-east-1",
  "sourceIPAddress": "192.0.2.0",
  "userAgent": "Amazon Internal",
  "requestParameters": {
    "pendingWindowInDays": 20,
    "keyId": "1234abcd-12ab-34cd-56ef-1234567890ab"
  },
  "responseElements": {
    "keyId": "arn:aws:kms:us-west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab",
    "keyState": "PendingDeletion",
  }
}
```



```

    "deletionDate": "Apr 12, 2021 18:58:30 PM"
  },
  "requestID": "ee408f36-ea01-422b-ac14-b0f147c68334",
  "eventID": "3c4226b0-1e81-48a8-a333-7fa5f3cbd118",
  "readOnly": false,
  "resources": [
    {
      "accountId": "111122223333",
      "type": "AWS::KMS::Key",
      "ARN": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab"
    }
  ],
  "eventType": "AwsApiCall",
  "recipientAccountId": "111122223333"
}

```

The following example records a `ScheduleKeyDeletion` request for a multi-Region KMS key with replica keys.

Because Amazon KMS won't delete a multi-Region key until all of its replica keys are deleted, in the `responseElements` field, the `keyState` is `PendingReplicaDeletion` and the `deletionDate` field is omitted.

```

{
  "eventVersion": "1.08",
  "userIdentity": {
    "type": "IAMUser",
    "principalId": "EX_PRINCIPAL_ID",
    "arn": "arn:aws:iam::111122223333:user/Alice",
    "accountId": "111122223333",
    "accessKeyId": "EXAMPLE_KEY_ID",
    "userName": "Alice"
  },
  "eventTime": "2021-10-28T17:59:05Z",
  "eventSource": "kms.amazonaws.com",
  "eventName": "ScheduleKeyDeletion",
  "awsRegion": "us-west-2",
  "sourceIPAddress": "192.0.2.0",
  "userAgent": "Amazon Internal",
  "requestParameters": {
    "pendingWindowInDays": 30,
    "keyId": "mrk-1234abcd12ab34cd56ef1234567890ab"
  }
}

```

```

    },
    "responseElements": {
      "keyId": "arn:aws:kms:us-west-2:111122223333:key/
mrk-1234abcd12ab34cd56ef1234567890ab",
      "keyState": "PendingReplicaDeletion",
      "pendingWindowInDays": 30
    },
    "requestID": "12341411-d846-42a6-a476-b1cbe3011f89",
    "eventID": "abcda5f-396d-494c-9380-0c47860df5f1",
    "readOnly": false,
    "resources": [
      {
        "accountId": "111122223333",
        "type": "AWS::KMS::Key",
        "ARN": "arn:aws:kms:us-west-2:111122223333:key/
mrk-1234abcd12ab34cd56ef1234567890ab"
      }
    ],
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "111122223333",
    "eventCategory": "Management"
  }
}

```

The following example records a `ScheduleKeyDeletion` request for a KMS key in an Amazon CloudHSM [custom key store](#).

```

{
  "eventVersion": "1.08",
  "userIdentity": {
    "type": "IAMUser",
    "principalId": "EX_PRINCIPAL_ID",
    "arn": "arn:aws:iam::111122223333:user/Alice",
    "accountId": "111122223333",
    "accessKeyId": "EXAMPLE_KEY_ID",
    "userName": "Alice"
  },
  "eventTime": "2021-10-26T23:25:25Z",
  "eventSource": "kms.amazonaws.com",
  "eventName": "ScheduleKeyDeletion",
  "awsRegion": "us-west-2",
  "sourceIPAddress": "192.0.2.0",
  "userAgent": "Amazon Internal",

```

```

    "requestParameters": {
      "keyId": "arn:aws:kms:us-west-2:111122223333:key/0987dcba-09fe-87dc-65ba-
ab0987654321",
      "pendingWindowInDays": 30
    },
    "responseElements": {
      "keyId": "arn:aws:kms:us-west-2:111122223333:key/0987dcba-09fe-87dc-65ba-
ab0987654321",
      "deletionDate": "Nov 2, 2021, 11:25:25 PM",
      "keyState": "PendingDeletion",
      "pendingWindowInDays": 30
    },
    "additionalEventData": {
      "customKeyId": "cks-1234567890abcdef0",
      "clusterId": "cluster-1a23b4cdefg",
      "backingKeys": "[{\\"backingKeyId\\":\\"backing-key-id\\"}]"
    },
    "requestID": "abcd9f60-2c9c-4a0b-a456-d5d998f7f321",
    "eventID": "ca01996a-01b0-4edd-bbbb-25d7b6d1a6fa",
    "readOnly": false,
    "resources": [
      {
        "accountId": "111122223333",
        "type": "AWS::KMS::Key",
        "ARN": "arn:aws:kms:us-west-2:111122223333:key/0987dcba-09fe-87dc-65ba-
ab0987654321"
      }
    ],
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "111122223333",
    "eventCategory": "Management"
  }
}

```

Sign

These examples show Amazon CloudTrail log entries for the [Sign](#) operation.

The following example shows an CloudTrail log entry for a [Sign](#) operation that uses an asymmetric RSA KMS key to generate a digital signature for a file.

```

{
  "eventVersion": "1.08",

```

```

"userIdentity": {
  "type": "IAMUser",
  "principalId": "EX_PRINCIPAL_ID",
  "arn": "arn:aws:iam::111122223333:user/Alice",
  "accountId": "111122223333",
  "accessKeyId": "EXAMPLE_KEY_ID",
  "userName": "Alice"
},
"eventTime": "2022-03-07T22:36:44Z",
"eventSource": "kms.amazonaws.com",
"eventName": "Sign",
"awsRegion": "us-west-2",
"sourceIPAddress": "192.0.2.0",
"userAgent": "Amazon Internal",
"requestParameters": {
  "messageType": "RAW",
  "keyId": "0987dcba-09fe-87dc-65ba-ab0987654321",
  "signingAlgorithm": "RSASSA_PKCS1_V1_5_SHA_256"
},
"responseElements": null,
"requestID": "8d0b35e0-46cf-48b9-be99-bf2ebc9ab9fb",
"eventID": "107b3cac-b125-4556-9702-12a2b9afc7f7",
"readOnly": true,
"resources": [
  {
    "accountId": "111122223333",
    "type": "AWS::KMS::Key",
    "ARN": "arn:aws:kms:us-west-2:111122223333:key/0987dcba-09fe-87dc-65ba-ab0987654321"
  }
],
"eventType": "AwsApiCall",
"managementEvent": true,
"recipientAccountId": "111122223333",
"eventCategory": "Management"
}

```

SynchronizeMultiRegionKey

The following example shows an Amazon CloudTrail log entry generated when Amazon KMS synchronizes a [multi-Region key](#). Synchronizing involves cross-Region calls to copy the [shared properties](#) of a multi-Region primary key to its replica keys. Amazon KMS synchronizes multi-Region keys periodically to assure that all related multi-Region keys have the same key material.

The `resources` element of the CloudTrail log entry includes the key ARN of the multi-Region primary key, including its Amazon Web Services Region. The related multi-Region replica keys and their Regions are not listed in this log entry.

CloudTrail log entries for this operation recorded on or after December 2022 include the key ARN of the affected KMS key in the `responseElements.keyId` value, even though this operation does not return the key ARN.

```
{
  "eventVersion": "1.08",
  "userIdentity": {
    "accountId": "111122223333",
    "invokedBy": "AWS Internal"
  },
  "eventTime": "2020-11-18T02:04:37Z",
  "eventSource": "kms.amazonaws.com",
  "eventName": "SynchronizeMultiRegionKey",
  "awsRegion": "us-west-2",
  "sourceIPAddress": "AWS Internal",
  "userAgent": "AWS Internal",
  "requestParameters": null,
  "responseElements": {
    "keyId": "arn:aws:kms:us-west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab"
  },
  "requestID": "12345681-de97-42e9-bed0-b02ae1abd8dc",
  "eventID": "abcdec99-2b5c-4670-9521-ddb8f031e146",
  "readOnly": false,
  "resources": [
    {
      "accountId": "111122223333",
      "type": "AWS::KMS::Key",
      "ARN": "arn:aws:kms:us-west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab"
    }
  ],
  "eventType": "AwsApiCall",
  "managementEvent": true,
  "recipientAccountId": "111122223333",
  "eventCategory": "Management"
}
```

TagResource

The following example shows an Amazon CloudTrail log entry of a call to the [TagResource](#) operation to add a tag with a tag key of Department and a tag value of IT.

For an example of an UntagResource CloudTrail log entry that is written when the key is rotated, see [UntagResource](#). For information about tagging Amazon KMS keys, see [Tags in Amazon KMS](#).

```
{
  "eventVersion": "1.05",
  "userIdentity": {
    "type": "IAMUser",
    "principalId": "EX_PRINCIPAL_ID",
    "arn": "arn:aws:iam::111122223333:user/Alice",
    "accountId": "111122223333",
    "accessKeyId": "EXAMPLE_KEY_ID",
    "userName": "Alice"
  },
  "eventTime": "2020-07-01T21:19:25Z",
  "eventSource": "kms.amazonaws.com",
  "eventName": "TagResource",
  "awsRegion": "us-west-2",
  "sourceIPAddress": "192.0.2.0",
  "userAgent": "Amazon Internal",
  "requestParameters": {
    "keyId": "arn:aws:kms:us-west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab",
    "tags": [
      {
        "tagKey": "Department",
        "tagValue": "IT"
      }
    ]
  },
  "responseElements": null,
  "requestID": "b942584a-f77d-4787-9feb-b9c5be6e746d",
  "eventID": "0a091b9b-0df5-4cf9-b667-6f2879532b8f",
  "readOnly": false,
  "resources": [
    {
      "accountId": "111122223333",
      "type": "AWS::KMS::Key",

```

```

        "ARN": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab"
    }
],
"eventType": "AwsApiCall",
"recipientAccountId": "111122223333"
}

```

UntagResource

The following example shows an Amazon CloudTrail log entry of a call to the [UntagResource](#) operation to delete a tag with a tag key of Dept.

CloudTrail log entries for this operation recorded on or after December 2022 include the key ARN of the affected KMS key in the `responseElements.keyId` value, even though this operation does not return the key ARN.

For an example of an `TagResource` CloudTrail log entry, see [TagResource](#). For information about tagging Amazon KMS keys, see [Tags in Amazon KMS](#).

```

{
  "eventVersion": "1.05",
  "userIdentity": {
    "type": "IAMUser",
    "principalId": "EX_PRINCIPAL_ID",
    "arn": "arn:aws:iam::111122223333:user/Alice",
    "accountId": "111122223333",
    "accessKeyId": "EXAMPLE_KEY_ID",
    "userName": "Alice"
  },
  "eventTime": "2020-07-01T21:19:19Z",
  "eventSource": "kms.amazonaws.com",
  "eventName": "UntagResource",
  "awsRegion": "us-west-2",
  "sourceIPAddress": "192.0.2.0",
  "userAgent": "Amazon Internal",
  "requestParameters": {
    "keyId": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab",
    "tagKeys": [
      "Dept"
    ]
  },
}

```

```

    "responseElements": {
      "keyId": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab"
    },
    "requestID": "cb1d507b-6015-47f4-812b-179713af8068",
    "eventID": "0b00f4b0-036e-411d-aa75-87eb4a35a4b3",
    "readOnly": false,
    "resources": [
      {
        "accountId": "111122223333",
        "type": "AWS::KMS::Key",
        "ARN": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab"
      }
    ],
    "eventType": "AwsApiCall",
    "recipientAccountId": "111122223333"
  }
}

```

UpdateAlias

The following example shows an Amazon CloudTrail log entry for the [UpdateAlias](#) operation. The resources element includes fields for the alias and KMS key resources. For information about creating aliases in Amazon KMS, see [Create aliases](#).

CloudTrail log entries for this operation recorded on or after December 2022 include the key ARN of the affected KMS key in the `responseElements.keyId` value, even though this operation does not return the key ARN.

```

{
  "eventVersion": "1.05",
  "userIdentity": {
    "type": "IAMUser",
    "principalId": "EX_PRINCIPAL_ID",
    "arn": "arn:aws:iam::111122223333:user/Alice",
    "accountId": "111122223333",
    "accessKeyId": "EXAMPLE_KEY_ID",
    "userName": "Alice"
  },
  "eventTime": "2020-11-13T23:18:15Z",
  "eventSource": "kms.amazonaws.com",
  "eventName": "UpdateAlias",
  "awsRegion": "us-west-2",

```



```

    "sourceIPAddress": "192.0.2.0",
    "userAgent": "Amazon Internal",
    "requestParameters": {
      "aliasName": "alias/my_alias",
      "targetKeyId": "1234abcd-12ab-34cd-56ef-1234567890ab"
    },
    "responseElements": {
      "keyId": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab"
    },
    "requestID": "d9472f40-63bc-11e4-bc2b-4198b6150d5c",
    "eventID": "f72d3993-864f-48d6-8f16-e26e1ae8dff0",
    "readOnly": false,
    "resources": [
      {
        "accountId": "111122223333",
        "type": "AWS::KMS::Key",
        "ARN": "arn:aws:kms:us-west-2:111122223333:alias/my_alias"
      },
      {
        "accountId": "111122223333",
        "type": "AWS::KMS::Key",
        "ARN": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab"
      }
    ],
    "eventType": "AwsApiCall",
    "recipientAccountId": "111122223333"
  }

```

UpdateCustomKeyStore

The following example shows an Amazon CloudTrail log entry generated by calling the [UpdateCustomKeyStore](#) operation to update the cluster ID for a custom key store. For information about editing custom key stores, see [Edit Amazon CloudHSM key store settings](#).

```

{
  "eventVersion": "1.08",
  "userIdentity": {
    "type": "IAMUser",
    "principalId": "EX_PRINCIPAL_ID",
    "arn": "arn:aws:iam::111122223333:user/Alice",
    "accountId": "111122223333",

```

```

    "accessKeyId": "EXAMPLE_KEY_ID",
    "userName": "Alice"
  },
  "eventTime": "2021-10-21T20:17:32Z",
  "eventSource": "kms.amazonaws.com",
  "eventName": "UpdateCustomKeyStore",
  "awsRegion": "us-east-1",
  "sourceIPAddress": "192.0.2.0",
  "userAgent": "AWS Internal",
  "requestParameters": {
    "customKeyId": "cks-1234567890abcdef0",
    "clusterId": "cluster-1a23b4cdefg"
  },
  "responseElements": null,
  "additionalEventData": {
    "customKeyName": "ExampleKeyStore",
    "clusterId": "cluster-1a23b4cdefg"
  },
  "requestID": "abcde9e1-f1a3-4460-a423-577fb6e695c9",
  "eventID": "114b61b9-0ea6-47f5-a9d2-4f2bdd0017d5",
  "readOnly": false,
  "eventType": "AwsApiCall",
  "managementEvent": true,
  "recipientAccountId": "111122223333"
}

```

UpdateKeyDescription

The following example shows an Amazon CloudTrail log entry generated by calling the [UpdateKeyDescription](#) operation.

```

{
  "eventVersion": "1.08",
  "userIdentity": {
    "type": "IAMUser",
    "principalId": "EX_PRINCIPAL_ID",
    "arn": "arn:aws:iam::111122223333:user/Alice",
    "accountId": "111122223333",
    "accessKeyId": "EXAMPLE_KEY_ID",
    "userName": "Alice"
  },
  "eventTime": "2022-09-01T19:22:40Z",
  "eventSource": "kms.amazonaws.com",

```

```
"eventName": "UpdateKeyDescription",
"awsRegion": "us-west-2",
"sourceIPAddress": "192.0.2.0",
"userAgent": "Amazon Internal",
"requestParameters": {
  "keyId": "1234abcd-12ab-34cd-56ef-1234567890ab",
  "description": "New key description"
},
"responseElements": null,
"requestID": "8c3c1f8b-336d-4896-b034-4eb9916bc9b3",
"eventID": "f5f3d548-2e9e-4658-8427-9dcb5b1ea791",
"readOnly": false,
"resources": [
  {
    "accountId": "111122223333",
    "type": "AWS::KMS::Key",
    "ARN": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab"
  }
],
"eventType": "AwsApiCall",
"managementEvent": true,
"recipientAccountId": "111122223333",
"eventCategory": "Management"
}
```

UpdatePrimaryRegion

The following example shows the Amazon CloudTrail log entries that are generated by calling the [UpdatePrimaryRegion](#) operation on a [multi-Region key](#).

The UpdatePrimaryRegion operation writes two CloudTrail log entries: one in the Region with the multi-Region primary key that is converted to a replica key, and one in the Region with a multi-Region replica key that is converted to a primary key.

CloudTrail log entries for this operation recorded on or after December 2022 include the key ARN of the affected KMS key in the responseElements.keyId value, even though this operation does not return the key ARN.

The following example shows a CloudTrail log entry for UpdatePrimaryRegion in the Region where the multi-Region key changed from a primary key to a replica key (us-west-2). The primaryRegion field shows the Region that now hosts the primary key (ap-northeast-1).

```
{
  "eventVersion": "1.08",
  "userIdentity": {
    "type": "IAMUser",
    "principalId": "EX_PRINCIPAL_ID",
    "arn": "arn:aws:iam::111122223333:user/Alice",
    "accountId": "111122223333",
    "accessKeyId": "EXAMPLE_KEY_ID",
    "userName": "Alice"
  },
  "eventTime": "2021-03-10T20:23:37Z",
  "eventSource": "kms.amazonaws.com",
  "eventName": "UpdatePrimaryRegion",
  "awsRegion": "us-west-2",
  "sourceIPAddress": "192.0.2.0",
  "userAgent": "AWS Internal",
  "requestParameters": {
    "keyId": "mrk-1234abcd12ab34cd56ef1234567890ab",
    "primaryRegion": "ap-northeast-1"
  },
  "responseElements": {
    "keyId": "arn:aws:kms:us-west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab"
  },
  "requestID": "ee408f36-ea01-422b-ac14-b0f147c68334",
  "eventID": "3c4226b0-1e81-48a8-a333-7fa5f3cbd118",
  "readOnly": false,
  "resources": [
    {
      "accountId": "111122223333",
      "type": "AWS::KMS::Key",
      "ARN": "arn:aws:kms:us-west-2:111122223333:key/mrk-1234abcd12ab34cd56ef1234567890ab"
    }
  ],
  "eventType": "AwsApiCall",
  "managementEvent": true,
  "eventCategory": "Management",
  "recipientAccountId": "111122223333"
}
```

The following example represents the CloudTrail log entry for UpdatePrimaryRegion in the Region where the multi-Region key changed from a replica key to a primary key (ap-northeast-1). This log entry doesn't identify the previous primary Region.

```
{
  "eventVersion": "1.08",
  "userIdentity": {
    "type": "IAMUser",
    "principalId": "EX_PRINCIPAL_ID",
    "arn": "arn:aws:iam::111122223333:user/Alice",
    "accountId": "111122223333",
    "accessKeyId": "EXAMPLE_KEY_ID",
    "userName": "Alice",
    "invokedBy": "kms.amazonaws.com"
  },
  "eventTime": "2021-03-10T20:23:37Z",
  "eventSource": "kms.amazonaws.com",
  "eventName": "UpdatePrimaryRegion",
  "awsRegion": "ap-northeast-1",
  "sourceIPAddress": "192.0.2.0",
  "userAgent": "AWS Internal",
  "requestParameters": {
    "keyId": "arn:aws:kms:ap-northeast-1:111122223333:key/mrk-1234abcd12ab34cd56ef1234567890ab",
    "primaryRegion": "ap-northeast-1"
  },
  "responseElements": {
    "keyId": "arn:aws:kms:us-west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab"
  },
  "requestID": "ee408f36-ea01-422b-ac14-b0f147c68334",
  "eventID": "091e6be5-737f-43c6-8431-e3679d6d0619",
  "readOnly": false,
  "eventType": "AwsApiCall",
  "managementEvent": true,
  "eventCategory": "Management",
  "recipientAccountId": "111122223333"
}
```

VerifyMac

The following example shows an Amazon CloudTrail log entry for the [VerifyMac](#) operation.

```

{
  "eventVersion": "1.08",
  "userIdentity": {
    "type": "IAMUser",
    "principalId": "EX_PRINCIPAL_ID",
    "arn": "arn:aws:iam::111122223333:user/Alice",
    "accountId": "111122223333",
    "accessKeyId": "EXAMPLE_KEY_ID",
    "userName": "Alice"
  },
  "eventTime": "2022-03-31T19:25:54Z",
  "eventSource": "kms.amazonaws.com",
  "eventName": "VerifyMac",
  "awsRegion": "us-east-1",
  "sourceIPAddress": "192.0.2.0",
  "userAgent": "Amazon Internal",
  "requestParameters": {
    "macAlgorithm": "HMAC_SHA_384",
    "keyId": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab"
  },
  "responseElements": null,
  "requestID": "f35da560-edff-4d6e-9b40-fb306fa9ef1e",
  "eventID": "6b464487-6dea-44cd-84ad-225d7450c975",
  "readOnly": true,
  "resources": [
    {
      "accountId": "111122223333",
      "ARN": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab"
    }
  ],
  "eventType": "AwsApiCall",
  "recipientAccountId": "111122223333",
  "eventCategory": "Management"
}

```

Verify

These examples show Amazon CloudTrail log entries for the [Verify](#) operation.

The following example shows an CloudTrail log entry for a [Verify](#) operation that uses an asymmetric RSA KMS key to verify a digital signature.

```
{
  "eventVersion": "1.08",
  "userIdentity": {
    "type": "IAMUser",
    "principalId": "EX_PRINCIPAL_ID",
    "arn": "arn:aws:iam::111122223333:user/Alice",
    "accountId": "111122223333",
    "accessKeyId": "EXAMPLE_KEY_ID",
    "userName": "Alice"
  },
  "eventTime": "2022-03-07T22:50:41Z",
  "eventSource": "kms.amazonaws.com",
  "eventName": "Verify",
  "awsRegion": "us-west-2",
  "sourceIPAddress": "192.0.2.0",
  "userAgent": "Amazon Internal",
  "requestParameters": {
    "signingAlgorithm": "RSASSA_PKCS1_V1_5_SHA_256",
    "keyId": "0987dcba-09fe-87dc-65ba-ab0987654321",
    "messageType": "RAW"
  },
  "responseElements": null,
  "requestID": "c73ab82a-af82-4750-ae2c-b6bb790e9c28",
  "eventID": "3b4331cd-5b7b-4de5-bf5f-82ec22f0dac0",
  "readOnly": true,
  "resources": [
    {
      "accountId": "111122223333",
      "type": "AWS::KMS::Key",
      "ARN": "arn:aws:kms:us-west-2:111122223333:key/0987dcba-09fe-87dc-65ba-ab0987654321"
    }
  ],
  "eventType": "AwsApiCall",
  "managementEvent": true,
  "recipientAccountId": "111122223333",
  "eventCategory": "Management"
}
```

Amazon EC2 example one

The following example records an IAM principal creating an encrypted volume using the default volume key in the Amazon EC2 management console.

The following example shows a CloudTrail log entry in which user Alice creates an encrypted volume with a default volume key in the Amazon EC2 management console. The EC2 log file record includes a `volumeId` field with a value of `"vol-13439757"`. The Amazon KMS record contains an `encryptionContext` field with a value of `"aws:ebs:id": "vol-13439757"`. Similarly, the `principalId` and `accountId` between the two records match. The records reflect the fact that creating an encrypted volume generates a data key that is used to encrypt the volume content.

```
{
  "Records": [
    {
      "eventVersion": "1.02",
      "userIdentity": {
        "type": "IAMUser",
        "principalId": "EX_PRINCIPAL_ID",
        "arn": "arn:aws:iam::111122223333:user/Alice",
        "accountId": "111122223333",
        "accessKeyId": "EXAMPLE_KEY_ID",
        "userName": "Alice"
      },
      "eventTime": "2014-11-05T20:50:18Z",
      "eventSource": "ec2.amazonaws.com",
      "eventName": "CreateVolume",
      "awsRegion": "us-east-1",
      "sourceIPAddress": "192.0.2.0",
      "userAgent": "Amazon Internal",
      "requestParameters": {
        "size": "10",
        "zone": "us-east-1a",
        "volumeType": "gp2",
        "encrypted": true
      },
      "responseElements": {
        "volumeId": "vol-13439757",
        "size": "10",
        "zone": "us-east-1a",
        "status": "creating",
        "createTime": 1415220618876,
        "volumeType": "gp2",
        "iops": 30,
        "encrypted": true
      },
      "requestID": "1565210e-73d0-4912-854c-b15ed349e526",
      "eventID": "a3447186-135f-4b00-8424-bc41f1a93b4f",
    }
  ]
}
```



```

    "eventType": "AwsApiCall",
    "recipientAccountId": "123456789012"
  },
  {
    "eventVersion": "1.02",
    "userIdentity": {
      "type": "IAMUser",
      "principalId": "EX_PRINCIPAL_ID",
      "arn": "arn:aws:iam::111122223333:user/Alice",
      "accountId": "111122223333",
      "accessKeyId": "EXAMPLE_KEY_ID",
      "userName": "Alice"
    },
    "eventTime": "2014-11-05T20:50:19Z",
    "eventSource": "kms.amazonaws.com",
    "eventName": "GenerateDataKeyWithoutPlaintext",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "192.0.2.0",
    "userAgent": "&AWS; Internal",
    "requestParameters": {
      "encryptionContext": {
        "aws:ebs:id": "vol-13439757"
      },
      "numberOfBytes": 64,
      "keyId": "alias/aws/ebs"
    },
    "responseElements": null,
    "requestID": "create-123456789012-758241111-1415220618",
    "eventID": "4bd2a696-d833-48cc-b72c-05e61b608399",
    "readOnly": true,
    "resources": [
      {
        "ARN": "arn:aws:kms:us-west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab",
        "accountId": "111122223333"
      }
    ],
    "eventType": "AwsApiCall",
    "recipientAccountId": "111122223333"
  }
]
}

```

Amazon EC2 example two

In the following example, an IAM principal running an Amazon EC2 instance creates and mounts a data volume that is encrypted under a KMS key. This action generates multiple CloudTrail log records.

When the volume is created, Amazon EC2, acting on behalf of the customer, gets an encrypted data key from Amazon KMS (`GenerateDataKeyWithoutPlaintext`). Then it creates a grant (`CreateGrant`) that allows it to decrypt the data key. When the volume is mounted, Amazon EC2 calls Amazon KMS to decrypt the data key (`Decrypt`).

The `instanceId` of the Amazon EC2 instance, `"i-81e2f56c"`, appears in the `RunInstances` event. The same instance ID qualifies the `granteePrincipal` of the grant that is created (`"111122223333:aws:ec2-infrastructure:i-81e2f56c"`) and the assumed role that is the principal in the `Decrypt` call (`"arn:aws:sts::111122223333:assumed-role/aws:ec2-infrastructure/i-81e2f56c"`).

The [key ARN](#) of the KMS key that protects the data volume, `arn:aws:kms:us-west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab`, appears in all three Amazon KMS calls (`CreateGrant`, `GenerateDataKeyWithoutPlaintext`, and `Decrypt`).

```
{
  "Records": [
    {
      "eventVersion": "1.02",
      "userIdentity": {
        "type": "IAMUser",
        "principalId": "EX_PRINCIPAL_ID",
        "arn": "arn:aws:iam::111122223333:user/Alice",
        "accountId": "111122223333",
        "accessKeyId": "EXAMPLE_KEY_ID",
        "userName": "Alice"
      },
      "eventTime": "2014-11-05T21:35:27Z",
      "eventSource": "ec2.amazonaws.com",
      "eventName": "RunInstances",
      "awsRegion": "us-west-2",
      "sourceIPAddress": "192.0.2.0",
      "userAgent": "Amazon Internal",
      "requestParameters": {
        "instancesSet": {
          "items": [
```

```
    {
      "imageId": "ami-b66ed3de",
      "minCount": 1,
      "maxCount": 1
    }
  ]
},
"groupSet": {
  "items": [
    {
      "groupId": "sg-98b6e0f2"
    }
  ]
},
"instanceType": "m3.medium",
"blockDeviceMapping": {
  "items": [
    {
      "deviceName": "/dev/xvda",
      "ebs": {
        "volumeSize": 8,
        "deleteOnTermination": true,
        "volumeType": "gp2"
      }
    },
    {
      "deviceName": "/dev/sdb",
      "ebs": {
        "volumeSize": 8,
        "deleteOnTermination": false,
        "volumeType": "gp2",
        "encrypted": true
      }
    }
  ]
},
"monitoring": {
  "enabled": false
},
"disableApiTermination": false,
"instanceInitiatedShutdownBehavior": "stop",
"clientToken": "XdKUT141516171819",
"ebsOptimized": false
},
```

```
"responseElements": {
  "reservationId": "r-5ebc9f74",
  "ownerId": "111122223333",
  "groupSet": {
    "items": [
      {
        "groupId": "sg-98b6e0f2",
        "groupName": "launch-wizard-2"
      }
    ]
  },
  "instancesSet": {
    "items": [
      {
        "instanceId": "i-81e2f56c",
        "imageId": "ami-b66ed3de",
        "instanceState": {
          "code": 0,
          "name": "pending"
        },
        "amiLaunchIndex": 0,
        "productCodes": {

        },
        "instanceType": "m3.medium",
        "launchTime": 1415223328000,
        "placement": {
          "availabilityZone": "us-east-1a",
          "tenancy": "default"
        },
        "monitoring": {
          "state": "disabled"
        },
        "stateReason": {
          "code": "pending",
          "message": "pending"
        },
        "architecture": "x86_64",
        "rootDeviceType": "ebs",
        "rootDeviceName": "/dev/xvda",
        "blockDeviceMapping": {

        },
        "virtualizationType": "hvm",
```

```
    "hypervisor": "xen",
    "clientToken": "XdKUT1415223327917",
    "groupSet": {
      "items": [
        {
          "groupId": "sg-98b6e0f2",
          "groupName": "launch-wizard-2"
        }
      ]
    },
    "networkInterfaceSet": {
    },
    "ebsOptimized": false
  }
]
},
"requestID": "41c4b4f7-8bce-4773-bf0e-5ae3bb5cbce2",
"eventID": "cd75a605-2fee-4fda-b847-9c3d330ebaae",
"eventType": "AwsApiCall",
"recipientAccountId": "111122223333"
},
{
  "eventVersion": "1.02",
  "userIdentity": {
    "type": "IAMUser",
    "principalId": "EX_PRINCIPAL_ID",
    "arn": "arn:aws:iam::111122223333:user/Alice",
    "accountId": "111122223333",
    "accessKeyId": "EXAMPLE_KEY_ID",
    "userName": "Alice"
  },
  "eventTime": "2014-11-05T21:35:35Z",
  "eventSource": "kms.amazonaws.com",
  "eventName": "CreateGrant",
  "awsRegion": "us-east-1",
  "sourceIPAddress": "192.0.2.0",
  "userAgent": "Amazon Internal",
  "requestParameters": {
    "constraints": {
      "encryptionContextSubset": {
        "aws:ebs:id": "vol-f67bafb2"
      }
    }
  }
}
```

```

    },
    "granteePrincipal": "111122223333:aws:ec2-infrastructure:i-81e2f56c",
    "keyId": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab"
  },
  "responseElements": {
    "grantId": "abcde1237f76e4ba7987489ac329fbfba6ad343d6f7075dbd1ef191f0120514a"
  },
  "requestID": "41c4b4f7-8bce-4773-bf0e-5ae3bb5cbce2",
  "eventID": "c1ad79e3-0d3f-402a-b119-d5c31d7c6a6c",
  "readOnly": false,
  "resources": [
    {
      "ARN": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab",
      "accountId": "111122223333"
    }
  ],
  "eventType": "AwsApiCall",
  "recipientAccountId": "111122223333"
},
{
  "eventVersion": "1.02",
  "userIdentity": {
    "type": "IAMUser",
    "principalId": "EX_PRINCIPAL_ID",
    "arn": "arn:aws:iam::111122223333:user/Alice",
    "accountId": "111122223333",
    "accessKeyId": "EXAMPLE_KEY_ID",
    "userName": "Alice"
  },
  "eventTime": "2014-11-05T21:35:32Z",
  "eventSource": "kms.amazonaws.com",
  "eventName": "GenerateDataKeyWithoutPlaintext",
  "awsRegion": "us-east-1",
  "sourceIPAddress": "192.0.2.0",
  "userAgent": "Amazon Internal",
  "requestParameters": {
    "encryptionContext": {
      "aws:ebs:id": "vol-f67bafb2"
    }
  },
  "numberOfBytes": 64,
  "keyId": "alias/aws/ebs"
},

```

```
"responseElements": null,
"requestID": "create-111122223333-758247346-1415223332",
"eventID": "ac3cab10-ce93-4953-9d62-0b6e5cba651d",
"readOnly": true,
"resources": [
  {
    "ARN": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab",
    "accountId": "111122223333"
  }
],
"eventType": "AwsApiCall",
"recipientAccountId": "111122223333"
},
{
  "eventVersion": "1.02",
  "userIdentity": {
    "type": "AssumedRole",
    "principalId": "111122223333:aws:ec2-infrastructure:i-81e2f56c",
    "arn": "arn:aws:sts::111122223333:assumed-role/aws:ec2-infrastructure/
i-81e2f56c",
    "accountId": "111122223333",
    "accessKeyId": "",
    "sessionContext": {
      "attributes": {
        "mfaAuthenticated": "false",
        "creationDate": "2014-11-05T21:35:38Z"
      },
      "sessionIssuer": {
        "type": "Role",
        "principalId": "111122223333:aws:ec2-infrastructure",
        "arn": "arn:aws:iam::111122223333:role/aws:ec2-infrastructure",
        "accountId": "111122223333",
        "userName": "aws:ec2-infrastructure"
      }
    }
  },
  "eventTime": "2014-11-05T21:35:47Z",
  "eventSource": "kms.amazonaws.com",
  "eventName": "Decrypt",
  "awsRegion": "us-east-1",
  "sourceIPAddress": "192.0.2.0",
  "requestParameters": {
    "encryptionContext": {
```

```
        "aws:ebs:id": "vol-f67bafb2"
      }
    },
    "responseElements": null,
    "requestID": "b4b27883-6533-11e4-b4d9-751f1761e9e5",
    "eventID": "edb65380-0a3e-4123-bbc8-3d1b7cff49b0",
    "readOnly": true,
    "resources": [
      {
        "ARN": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab",
        "accountId": "111122223333"
      }
    ],
    "eventType": "AwsApiCall",
    "recipientAccountId": "111122223333"
  }
]
}
```

Monitor KMS keys with Amazon CloudWatch

You can monitor your Amazon KMS keys using [Amazon CloudWatch](#), an Amazon service that collects and processes raw data from Amazon KMS into readable, near real-time metrics. These data are recorded for a period of two weeks so that you can access historical information and gain a better understanding of the usage of your KMS keys and their changes over time.

You can use Amazon CloudWatch to alert you to important events, such as the following ones.

- The imported key material in a KMS key is nearing its expiration date.
- A KMS key that is pending deletion is still being used.
- The key material in a KMS key was automatically rotated.
- A KMS key was deleted.

You can also create an [Amazon CloudWatch](#) alarm that alerts you when your request rate reaches a certain percentage of a quota value. For details, see [Manage your Amazon KMS API request rates using Service Quotas and Amazon CloudWatch](#) in the *Amazon Security Blog*.

Amazon KMS metrics and dimensions

Amazon KMS predefines Amazon CloudWatch metrics to make it easier for you to monitor critical data and create alarms. You can view the Amazon KMS metrics using the Amazon Web Services Management Console and the Amazon CloudWatch API.

This section lists each Amazon KMS metrics and the dimensions for each metric, and provides some basic guidance for creating CloudWatch alarms based on these metrics and dimensions.

Note

Dimension group name:

To view a metric in the Amazon CloudWatch console, in the **Metrics** section, select the dimension group name. Then you can filter by the **Metric name**. This topic includes the metric name and dimension group name for each Amazon KMS metric.

You can view Amazon KMS metrics using the Amazon Web Services Management Console and the Amazon CloudWatch API. For more information, see [View available metrics](#) in the *Amazon CloudWatch User Guide*.

Topics

- [SuccessfulRequest](#)
- [SecondsUntilKeyMaterialExpiration](#)
- [CloudHSMKeyStoreThrottle](#)
- [ExternalKeyStoreThrottle](#)
- [XksProxyCertificateDaysToExpire](#)
- [XksProxyCredentialAge](#)
- [XksProxyErrors](#)
- [XksExternalKeyManagerStates](#)
- [XksProxyLatency](#)

SuccessfulRequest

The number of successful requests for cryptographic operations on a specific KMS key. By using the SuccessfulRequest metric, you can apply key-level filtering to Amazon KMS API usage

in CloudWatch. The Sum statistic for this metric defines the total number of successful requests during the period.

Use this metric to identify which KMS keys consume the largest portion of your request quota or contribute the most to API charges. You can also create a CloudWatch alarm based on the `SuccessfulRequest` metric to notify you of anomalous Amazon KMS API usage patterns. These alerts can help identify inefficient workflows that might unintentionally exceed your request quotas or incur unexpected charges.

Dimensions for `SuccessfulRequest`

Dimension	Description
KeyArn	Value for each KMS key.
Operation	Value for each Amazon KMS API operation. This metric applies only to cryptographic operations.

For [ReEncrypt](#) operations, the `SuccessfulRequest` metric includes dimensions for both the source and destination KMS keys.

Dimension	Description
SourceKeyArn	Value for the KMS key that decrypted the ciphertext.
DestinationKeyArn	Value for the KMS key that re-encrypted the data.
Operation	Value for each Amazon KMS API operation, in this case, <code>ReEncrypt</code> .

`SecondsUntilKeyMaterialExpiration`

The number of seconds remaining until the [imported key material](#) in a KMS key expires. This metric is valid only for KMS keys with imported key material (a [key material origin](#) of `EXTERNAL`) and an expiration date.

Use this metric to track the time that remains until your imported key material expires. When that time falls below a threshold that you define, you might want to reimport the key material with a new expiration date. The `SecondsUntilKeyMaterialExpiration` metric is specific to a KMS key. You cannot use this metric to monitor multiple KMS keys or KMS keys that you might create in the future. For help with creating a CloudWatch alarm to monitor this metric, see [Create a CloudWatch alarm for expiration of imported key material](#).

The most useful statistic for this metric is `Minimum`, which tells you the smallest amount of time remaining for all data points in the specified statistical period. The only valid unit for this metric is `Seconds`.

Dimension group name: Per-Key Metrics

Dimensions for `SecondsUntilKeyMaterialExpiration`

Dimension	Description; related to Amazon
<code>KeyId</code>	Value for each KMS key.

When you [schedule deletion](#) of a KMS key, Amazon KMS enforces a waiting period before deleting the KMS key. You can use the waiting period to ensure that you don't need the KMS key now or in the future. You can also configure a CloudWatch alarm to warn you if a person or application attempts to use the KMS key in a [cryptographic operation](#) during the waiting period. If you receive a notification from such an alarm, you might want to cancel deletion of the KMS key.

For instructions, see [Create an alarm that detects use of a KMS key pending deletion](#).

CloudHSMKeyStoreThrottle

The number of requests for cryptographic operations on KMS keys in each Amazon CloudHSM key store that Amazon KMS throttles (responds with a `ThrottlingException`). This metric applies only to Amazon CloudHSM key stores.

The `CloudHSMKeyStoreThrottle` metric applies only to KMS keys in an Amazon CloudHSM key store and only to requests for [cryptographic operations](#). Amazon KMS [throttles these requests](#) when the request rate exceeds the [custom key store request quota](#) for your Amazon CloudHSM key store. This metric also includes throttling by the Amazon CloudHSM cluster.

Dimension group name: Keystore Throttle Metrics

Dimension	Description
CustomKeyStoreId	Value for each Amazon CloudHSM key store.
KmsOperation	Value for each Amazon KMS API operation. This metric applies only to cryptographic operations on KMS keys in an Amazon CloudHSM key store.
KeySpec	Value for each type of KMS key. The only supported key spec for KMS keys in an Amazon CloudHSM key store is SYMMETRIC_DEFAULT.

ExternalKeyStoreThrottle

The number of requests for cryptographic operations on KMS keys in each external key store that Amazon KMS throttles (responds with a `ThrottlingException`). This metric applies only to [external key stores](#).

The `ExternalKeyStoreThrottle` metric applies only to KMS keys in an external key store and only to requests for [cryptographic operations](#). Amazon KMS [throttles these requests](#) when the request rate exceeds the [custom key store request quota](#) for your external key store. This metric does not include throttling by your external key store proxy or external key manager.

Use this metric to review and adjust the value of your custom key store request quota. If this metric indicates that Amazon KMS is frequently throttling your requests for these KMS keys, you might consider requesting an increase in your custom key store request quota value. For help, see [Requesting a quota increase](#) in the *Service Quotas User Guide*.

If you are getting very frequent `KMSInvalidStateException` errors with a message that explains that the request was rejected "due to a very high request rate" or the request was rejected "because the external key store proxy did not respond in time," it might indicate that your external key manager or external key store proxy cannot keep pace with the current request rate. If possible, lower your request rate. You might also consider requesting a decrease in your custom key store request quota value. Decreasing this quota value might increase throttling (and the `ExternalKeyStoreThrottle` metric value), but it indicates that Amazon KMS is rejecting excess requests quickly before they are sent to your external key store proxy or external key manager. To request a quota decrease, please visit the [Amazon Web Services Support Center](#) and create a case.

Dimension group name: Keystore Throttle Metrics

Dimension	Description
CustomKeyStoreId	Value for each external key store.
KmsOperation	Value for each Amazon KMS API operation. This metric applies only to cryptographic operations on KMS keys in an external key store.
KeySpec	Value for each type of KMS key. The only supported key spec for KMS keys in an external key store is SYMMETRIC_DEFAULT.

XksProxyCertificateDaysToExpire

The number of days until the TLS certificate for your [external key store proxy endpoint](#) (`XksProxyUriEndpoint`) expires. This metric applies only to [external key stores](#).

Use this metric to create a CloudWatch alarm that notifies you about the upcoming expiration of your TLS certificate. When the certificate expires, Amazon KMS cannot communicate with the external key store proxy. All data protected by KMS keys in your external key store becomes inaccessible until you renew the certificate.

A certificate alarm prevents certificate expiration that might prevent you from accessing your encrypted resources. Set the alarm to give your organization time to renew the certificate before it expires.

Dimension group name: XKS Proxy Certificate Metrics

Dimension	Description
CustomKeyStoreId	Value for each external key store.
CertificateName	Subject name (CN) in the TLS certificate.

You can create CloudWatch alarms based on the metrics for external key stores and KMS keys in external key stores. For instructions, see [Monitor external key stores](#).

XksProxyCredentialAge

The number of days since the current external key store [proxy authentication credential](#) (XksProxyAuthenticationCredential) was associated with the external key store. This count begins when you enter the authentication credential as part of creating or updating your external key store. This metric applies only to [external key stores](#).

This value is designed to remind you about the age of your authentication credential. However, because we begin the count when you associate the credential with your external key store, not when you create your authentication credential on your external key store proxy, this might not be an accurate indicator of the credential age on the proxy.

Use this metric to create a CloudWatch alarm that reminds you to rotate your external key store proxy authentication credential.

Dimension group name: Per-Keystore Metrics

Dimension	Description
CustomKeyStoreId	Value for each external key store.

You can create CloudWatch alarms based on the metrics for external key stores and KMS keys in external key stores. For instructions, see [Monitor external key stores](#).

XksProxyErrors

The number of exceptions related to Amazon KMS requests to your [external key store proxy](#). This count includes exceptions that the external key store proxy returns to Amazon KMS and timeout errors that occur when the external key store proxy does not respond to Amazon KMS within the 250 millisecond timeout interval. This metric applies only to [external key stores](#).

Use this metric to track the error rate of KMS keys in your external key store. It reveals the most frequent errors, so you can prioritize your engineering effort. For example, KMS keys that are generating high rates of non-retryable errors might indicate a problem with the configuration of your external key store. To view your external key store configuration, see [View external key stores](#). To edit your external key store settings, see [Edit external key store properties](#).

Dimension group name: XKS Proxy Error Metrics

Dimension	Description
CustomKeyStoreId	Value for each external key store.
KmsOperation	Value for each Amazon KMS API operation that generated a request to the XKS proxy.
XksOperation	Value for each external key store proxy API operation .
KeySpec	Value for each type of KMS key. The only supported key spec for KMS keys in an external key store is SYMMETRIC_DEFAULT.
ErrorType	Values: <ul style="list-style-type: none"> • Retryable errors: Likely to be transient, such as networking errors. • Non-retryable errors: Likely to indicate a problem with the custom key store configuration or external components. • N/A: Successful request; no errors
ExceptionName	Values: <ul style="list-style-type: none"> • Name of the exception • None: Successful request; no errors

You can create CloudWatch alarms based on the metrics for external key stores and KMS keys in external key stores. For instructions, see [Monitor external key stores](#).

XksExternalKeyManagerStates

A count of the number of [external key manager instances](#) in each of the following health states: Active, Degraded, and Unavailable. The information for this metric comes from the external key store proxy associated with each external key store. This metric applies only to [external key stores](#).

The following are the health states for the external key manager instances associated with an external key store. Each external key store proxy might use different indicators to measure the

health states of your external key manager. For details, see the documentation for your external key store proxy.

- **Active:** The external key manager is healthy.
- **Degraded:** The external key manager is unhealthy, but can still serve traffic
- **Unavailable:** The external key manager cannot serve traffic.

Use this metric to create a CloudWatch alarm that alerts you to degraded and unavailable external key manager instances. To determine which external key manager instances are in each state, consult your external key store proxy logs.

Dimension group name: XKS External Key Manager Metrics

Dimension	Description
CustomKeyStoreId	Value for each external key store.
XksExternalKeyManagerState	Value for each health state.

You can create CloudWatch alarms based on the metrics for external key stores and KMS keys in external key stores. For instructions, see [Monitor external key stores](#).

XksProxyLatency

The number of milliseconds it takes for an external key store proxy to respond to an Amazon KMS request. If the request timed out, the recorded value is the 250 millisecond timeout limit. This metric applies only to [external key stores](#).

Use this metric to evaluate the performance of your external key store proxy and external key manager. For example, if the proxy is frequently timing out on encryption and decryption operations, consult your external proxy administrator.

Slow responses might also indicate that your external key manager cannot handle the current request traffic. Amazon KMS recommends that your external key manager be able to handle up to 1800 requests for cryptographic operations per second. If your external key manager cannot

handle the 1800 requests per second rate, consider requesting a decrease in your [request quota for KMS keys in a custom key store](#). Requests for cryptographic operations using the KMS keys in your external key store will fail fast with a [throttling exception](#), rather than being processed and later rejected by your external key store proxy or external key manager.

Dimension group name: XKS Proxy Latency Metrics

Dimension	Description
CustomKeyStoreId	Value for each external key store.
KmsOperation	Value for each Amazon KMS API operation that generated a request to the XKS proxy.
XksOperation	Value for each external key store proxy API operation .
KeySpec	Value for each type of KMS key. The only supported key spec for KMS keys in an external key store is SYMMETRIC_DEFAULT.

You can create CloudWatch alarms based on the metrics for external key stores and KMS keys in external key stores. For instructions, see [Monitor external key stores](#).

Create a CloudWatch alarm for expiration of imported key material

You can create a CloudWatch alarm that notifies you when the imported key material in a KMS key is approaching its expiration time. For example, the alarm can notify you when the time to expire is less than 30 days away.

When you [import key material into a KMS key](#), you can optionally specify a date and time when the key material expires. When the key material expires, Amazon KMS deletes the key material and the KMS key becomes unusable. To use the KMS key again, you must [reimport the key material](#). However, if you reimport the key material before it expires, you can avoid disrupting processes that use that KMS key.

This alarm uses the [SecondsUntilKeyMaterialExpires metric](#) that Amazon KMS publishes to CloudWatch for KMS keys with imported key material that expires. Each alarm uses this metric to

monitor the imported key material for a particular KMS key. You cannot create a single alarm for all KMS keys with expiring key material or an alarm for KMS keys that you might create in the future.

Requirements

The following resources are required for a CloudWatch alarm that monitors the expiration of imported key material.

- A KMS key with imported key material that expires.
- An Amazon SNS topic. For details, see [Creating an Amazon SNS topic](#) in the *Amazon CloudWatch User Guide*.

Create the alarm

Follow the instructions in [Create a CloudWatch alarm based on a static threshold](#) using the following required values. For other fields, accept the default values and provide names as requested.

Field	Value
Select metric	<p>Choose KMS, then choose Per-Key Metrics.</p> <p>Choose the row with the KMS key and the <code>SecondsUntilKeyMaterialExpires</code> metric. Then choose Select metric.</p> <p>The Metrics list displays the <code>SecondsUntilKeyMaterialExpires</code> metric only for KMS keys with imported key material that expires. If you don't have KMS keys with these properties in the account and Region, this list is empty.</p>
Statistic	Minimum
Period	1 minute
Threshold type	Static
Whenever ...	Whenever <i>metric-name</i> is Greater than 1

Create CloudWatch alarms for external key stores

You can create Amazon CloudWatch alarms based on external key store metrics to notify you when a metric value exceeds a threshold you specified. The alarm can send the message to an [Amazon Simple Notification Service \(Amazon SNS\) topic](#) or an [Amazon EC2 Auto Scaling policy](#). For detailed information about CloudWatch alarms, see [Using Amazon CloudWatch alarms](#) in the *Amazon CloudWatch User Guide*.

Before creating an Amazon CloudWatch alarm, you need an Amazon SNS topic. For details, see [Creating an Amazon SNS topic](#) in the *Amazon CloudWatch User Guide*.

Topics

- [Create an alarm for certificate expiration](#)
- [Create an alarm for response timeout](#)
- [Create an alarm for retryable errors](#)
- [Create an alarm for non-retryable errors](#)

Create an alarm for certificate expiration

This alarm uses the [XksProxyCertificateDaysToExpire](#) metric that Amazon KMS publishes to CloudWatch to record the anticipated expiration of the TLS certificate associated with your external key store proxy endpoint. You cannot create a single alarm for all external key stores in your account or an alarm for external key stores that you might create in the future.

We recommend setting the alarm to alert you 10 days before your certificate is set to expire, but you should set the threshold that best fits your needs.

Create the alarm

Follow the instructions in [Create a CloudWatch alarm based on a static threshold](#) using the following required values. For other fields, accept the default values and provide names as requested.

Field	Value
Select metric	Choose KMS , then choose XKS Proxy Certificate Metrics .

Field	Value
	Select the check box next to the <code>XksProxyCertificateName</code> that you want to monitor. Then choose Select metric .
Statistic	Minimum
Period	5 minutes
Threshold type	Static
Whenever ...	Whenever <code>XksProxyCertificateDaysToExpire</code> is Lower than 10.

Create an alarm for response timeout

This alarm uses the [XksProxyLatency](#) metric that Amazon KMS publishes to CloudWatch to record the number of milliseconds it takes for an external key store proxy to respond to an Amazon KMS request. You cannot create a single alarm for all external key stores in your account or an alarm for external key stores that you might create in the future.

Amazon KMS expects the external key store proxy to respond to each request within 250 milliseconds. We recommend setting an alarm to alert you when your external key store proxy takes longer than 200 milliseconds to respond, but you should set the threshold that best fits your needs.

Create the alarm

Follow the instructions in [Create a CloudWatch alarm based on a static threshold](#) using the following required values. For other fields, accept the default values and provide names as requested.

Field	Value
Select metric	Choose KMS , then choose XKS Proxy Latency Metrics . Select the check box next to the <code>KmsOperation</code> that you want to monitor. Then choose Select metric .

Field	Value
Statistic	Average
Period	5 minutes
Threshold type	Static
Whenever ...	Whenever XksProxyLatency is Greater than 200.

Create an alarm for retryable errors

This alarm uses the [XksProxyErrors](#) metric that Amazon KMS publishes to CloudWatch to record the number of exceptions related to Amazon KMS requests to your external key store proxy. You cannot create a single alarm for all external key stores in your account or an alarm for external key stores that you might create in the future.

Retryable errors will lower your reliability percentage and can indicate networking errors. We recommend setting an alarm to alert you when more than five retryable errors are recorded in a one minute period, but you should set the threshold that best fits your needs.

Follow the instructions in [Create a CloudWatch alarm based on a static threshold](#) using the following required values. For other fields, accept the default values and provide names as requested.

Field	Value
Select metric	Choose the Query tab. Choose AWS/KMS for Namespace . Enter SUM(XksProxyErrors) for Metric name . Enter ErrorType = Retryable for Filter by . Choose Run . Then choose Select metric .
Label	<i>Retryable errors</i>
Period	1 minute

Field	Value
Threshold type	Static
Whenever ...	Whenever q1 is Greater than 5.

Create an alarm for non-retryable errors

This alarm uses the [XksProxyErrors](#) metric that Amazon KMS publishes to CloudWatch to record the number of exceptions related to Amazon KMS requests to your external key store proxy. You cannot create a single alarm for all external key stores in your account or an alarm for external key stores that you might create in the future.

Non-retryable errors can indicate a problem with the configuration of your external key store. We recommend setting an alarm to alert you when more than five non-retryable errors are recorded in a one minute period, but you should set the threshold that best fits your needs.

Follow the instructions in [Create a CloudWatch alarm based on a static threshold](#) using the following required values. For other fields, accept the default values and provide names as requested.

Field	Value
Select metric	Choose the Query tab. Choose AWS/KMS for Namespace . Enter SUM(XksProxyErrors) for Metric name . Enter ErrorType = Non-retryable for Filter by . Choose Run . Then choose Select metric .
Label	<i>Non-retryable errors</i>
Period	1 minute
Threshold type	Static
Whenever ...	Whenever q1 is Greater than 5.

Monitor KMS keys with Amazon EventBridge

You can use Amazon EventBridge (formerly Amazon CloudWatch Events) to alert you to the following important events in the lifecycle of your KMS keys.

- The key material in a KMS key was automatically rotated.
- The imported key material in a KMS key expired.
- A KMS key that had been scheduled for deletion was deleted.

Amazon KMS integrates with Amazon EventBridge to notify you of important events that affect your KMS keys. Each event is represented in [JSON \(JavaScript Object Notation\)](#) and includes the event name, the date and time when the event occurred, and the affected. You can collect these events and establish rules that route them to one or more *targets* such as Amazon Lambda functions, Amazon SNS topics, Amazon SQS queues, streams in Amazon Kinesis Data Streams, or built-in targets.

For more information about using EventBridge with other kinds of events, including those emitted by Amazon CloudTrail when it records a read/write API request, see the [Amazon EventBridge User Guide](#).

The following topics describe the EventBridge events that Amazon KMS generates.

KMS CMK Rotation

Amazon KMS supports [automatic rotation](#) of the key material in symmetric encryption KMS keys. Annual key material rotation is optional for [customer managed keys](#). The key material for [Amazon managed keys](#) is automatically rotated every year.

Whenever Amazon KMS rotates key material, it sends a KMS CMK Rotation event to EventBridge. Amazon KMS generates this event on a best-effort basis.

The following is an example of this event.

```
{
  "version": "0",
  "id": "6a7e8feb-b491-4cf7-a9f1-bf3703467718",
  "detail-type": "KMS CMK Rotation",
  "source": "aws.kms",
  "account": "111122223333",
```

```
"time": "2022-08-10T16:37:50Z",
"region": "us-west-2",
"resources": [
  "arn:aws:kms:us-west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab"
],
"detail": {
  "key-id": "1234abcd-12ab-34cd-56ef-1234567890ab"
}
}
```

KMS Imported Key Material Expiration

When you [import key material into a KMS key](#), you can optionally specify a time at which the key material expires. When the key material expires, Amazon KMS deletes the key material and sends a corresponding KMS Imported Key Material Expiration event to EventBridge. Amazon KMS generates this event on a best-effort basis.

The following is an example of this event.

```
{
  "version": "0",
  "id": "9da9af57-9253-4406-87cb-7cc400e43465",
  "detail-type": "KMS Imported Key Material Expiration",
  "source": "aws.kms",
  "account": "111122223333",
  "time": "2022-08-10T16:37:50Z",
  "region": "us-west-2",
  "resources": [
    "arn:aws:kms:us-west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab"
  ],
  "detail": {
    "key-id": "1234abcd-12ab-34cd-56ef-1234567890ab"
  }
}
```

KMS CMK Deletion

When you [schedule deletion](#) of a KMS key, Amazon KMS enforces a waiting period before deleting the KMS key. After the waiting period ends, Amazon KMS deletes the KMS key and sends a KMS CMK Deletion event to EventBridge. Amazon KMS guarantees this EventBridge event. Due to retries, it might generate multiple events within a few seconds that delete the same KMS key.

The following is an example of this event.

```
{
  "version": "0",
  "id": "e9ce3425-7d22-412a-a699-e7a5fc3fbc9a",
  "detail-type": "KMS CMK Deletion",
  "source": "aws.kms",
  "account": "111122223333",
  "time": "2022-08-10T16:37:50Z",
  "region": "us-west-2",
  "resources": [
    "arn:aws:kms:us-west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab"
  ],
  "detail": {
    "key-id": "1234abcd-12ab-34cd-56ef-1234567890ab"
  }
}
```

Aliases in Amazon KMS

An *alias* is a friendly name for a Amazon KMS key. For example, an alias lets you refer to a KMS key as `test-key` instead of `1234abcd-12ab-34cd-56ef-1234567890ab`.

You can use an alias to identify a KMS key in the Amazon KMS console, in the [DescribeKey](#) operation, and in [cryptographic operations](#), such as [Encrypt](#) and [GenerateDataKey](#). Aliases also make it easy to recognize an [Amazon managed key](#). Aliases for these KMS keys always have the form `aws/<service-name>`. For example, the alias for the Amazon managed key for Amazon DynamoDB is `aws/dynamodb`. You can establish similar alias standards for your projects, such as prefacing your aliases with the name of a project or category.

You can also allow and deny access to KMS keys based on their aliases without editing policies or managing grants. This feature is part of Amazon KMS support for [attribute-based access control](#) (ABAC). For details, see [Use aliases to control access to KMS keys](#).

Much of the power of aliases come from your ability to change the KMS key associated with an alias at any time. Aliases can make your code easier to write and maintain. For example, suppose you use an alias to refer to a particular KMS key and you want to change the KMS key. In that case, just associate the alias with a different KMS key. You don't need to change your code.

Aliases also make it easier to reuse the same code in different Amazon Web Services Regions. Create aliases with the same name in multiple Regions and associate each alias with a KMS key in its Region. When the code runs in each Region, the alias refers to the associated KMS key in that Region. For an example, see [Learn how to use aliases in your applications](#).

You can create an alias for a KMS key in the Amazon KMS console, by using the [CreateAlias](#) API, or by using the [AWS::KMS::Alias Amazon CloudFormation template](#).

The Amazon KMS API provides full control of aliases in each account and Region. The API includes operations to create an alias ([CreateAlias](#)), view alias names and alias ARNs ([ListAliases](#)), change the KMS key associated with an alias ([UpdateAlias](#)), and delete an alias ([DeleteAlias](#)).

How aliases work

Learn how aliases work in Amazon KMS.

An alias is an independent Amazon resource

An alias is not a property of a KMS key. The actions that you take on the alias don't affect its associated KMS key. You can create an alias for a KMS key and then update the alias so it's associated with a different KMS key. You can even delete the alias without any effect on the associated KMS key. However, if you delete a KMS key, all aliases associated with that KMS key are deleted.

If you specify an alias as the resource in an IAM policy, the policy refers to the alias, not to the associated KMS key.

Each alias has two formats

When you create an alias, you specify the alias name. Amazon KMS creates the alias ARN for you.

- An [alias ARN](#) is an Amazon Resource Name (ARN) that uniquely identifies the alias.

```
# Alias ARN
arn:aws:kms:us-west-2:111122223333:alias/<alias-name>
```

- An [alias name](#) that is unique in the account and Region. In the Amazon KMS API, the alias name is always prefixed by `alias/`. That prefix is omitted in the Amazon KMS console.

```
# Alias name
alias/<alias-name>
```

Aliases are not secret

Aliases may be displayed in plaintext in CloudTrail logs and other output. Do not include confidential or sensitive information in the alias name.

Each alias is associated with one KMS key at a time

The alias and its KMS key must be in the same account and Region.

You can associate an alias with any [customer managed key](#) in the same Amazon Web Services account and Region. However, you do not have permission to associate an alias with an [Amazon managed key](#).

For example, this [ListAliases](#) output shows that the `test-key` alias is associated with exactly one target KMS key, which is represented by the `TargetKeyId` property.

```
{
  "AliasName": "alias/test-key",
  "AliasArn": "arn:aws:kms:us-west-2:111122223333:alias/test-key",
  "TargetKeyId": "1234abcd-12ab-34cd-56ef-1234567890ab",
  "CreationDate": 1593622000.191,
  "LastUpdatedDate": 1593622000.191
}
```

Multiple aliases can be associated with the same KMS key

For example, you can associate the `test-key` and `project-key` aliases with the same KMS key.

```
{
  "AliasName": "alias/test-key",
  "AliasArn": "arn:aws:kms:us-west-2:111122223333:alias/test-key",
  "TargetKeyId": "1234abcd-12ab-34cd-56ef-1234567890ab",
  "CreationDate": 1593622000.191,
  "LastUpdatedDate": 1593622000.191
},
{
  "AliasName": "alias/project-key",
  "AliasArn": "arn:aws:kms:us-west-2:111122223333:alias/project-key",
  "TargetKeyId": "1234abcd-12ab-34cd-56ef-1234567890ab",
  "CreationDate": 1516435200.399,
  "LastUpdatedDate": 1516435200.399
}
```

An alias must be unique in an account and Region

For example, you can have only one `test-key` alias in each account and Region. Aliases are case-sensitive, but aliases that differ only in their capitalization are very prone to error. You cannot change an alias name. However, you can delete the alias and create a new alias with the desired name.

You can create an alias with the same name in different Regions

For example, you can have a `finance-key` alias in US East (N. Virginia) and a `finance-key` alias in Europe (Frankfurt). Each alias would be associated with a KMS key in its Region. If your code refers to an alias name like `alias/finance-key`, you can run it in multiple Regions. In each Region, it uses a different KMS key. For details, see [Learn how to use aliases in your applications](#).

You can change the KMS key associated with an alias

You can use the [UpdateAlias](#) operation to associate an alias with a different KMS key. For example, if the `finance-key` alias is associated with the `1234abcd-12ab-34cd-56ef-1234567890ab` KMS key, you can update it so it is associated with the `0987dcba-09fe-87dc-65ba-ab0987654321` KMS key.

However, the current and new KMS key must be the same type (both symmetric or both asymmetric or both HMAC), and they must have the same [key usage](#) (`ENCRYPT_DECRYPT` or `SIGN_VERIFY` or `GENERATE_VERIFY_MAC`). This restriction prevents errors in code that uses aliases. If you must associate an alias with a different type of key, and you have mitigated the risks, you can delete and recreate the alias.

Some KMS keys don't have aliases

When you create a KMS key in the Amazon KMS console, you must give it a new alias. But an alias is not required when you use the [CreateKey](#) operation to create a KMS key. Also, you can use the [UpdateAlias](#) operation to change the KMS key associated with an alias and the [DeleteAlias](#) operation to delete an alias. As a result, some KMS keys might have several aliases, and some might have none.

Amazon creates aliases in your account

Amazon creates aliases in your account for [Amazon managed keys](#). These aliases have names of the form `alias/aws/<service-name>`, such as `alias/aws/s3`.

Some Amazon aliases have no KMS key. These predefined aliases are usually associated with an Amazon managed key when you start using the service.

Use aliases to identify KMS keys

You can use an [alias name](#) or [alias ARN](#) to identify a KMS key in [cryptographic operations](#), [DescribeKey](#), and [GetPublicKey](#). (If the [KMS key is in a different Amazon Web Services account](#), you must use its [key ARN](#) or alias ARN.) Aliases are not valid identifiers for KMS keys in other Amazon KMS operations. For information about the valid [key identifiers](#) for each Amazon KMS API operation, see the descriptions of the `KeyId` parameters in the *Amazon Key Management Service API Reference*.

You cannot use an alias name or alias ARN to [identify a KMS key in an IAM policy](#). To control access to a KMS key based on its aliases, use the [kms:RequestAlias](#) or [kms:ResourceAliases](#) condition keys. For details, see [ABAC for Amazon KMS](#).

Controlling access to aliases

When you create or change an alias, you affect the alias and its associated KMS key. Therefore, principals who manage aliases must have permission to call the alias operation on the alias and on all affected KMS keys. You can provide these permissions by using [key policies](#), [IAM policies](#) and [grants](#).

Note

Be cautious when giving principals permission to manage tags and aliases. Changing a tag or alias can allow or deny permission to the customer managed key. For details, see [ABAC for Amazon KMS](#) and [Use aliases to control access to KMS keys](#).

For information about controlling access to all Amazon KMS operations, see [Permissions reference](#).

Permissions to create and manage aliases work as follows.

kms:CreateAlias

To create an alias, the principal needs the following permissions for both the alias and for the associated KMS key.

- `kms:CreateAlias` for the alias. Provide this permission in an IAM policy that is attached to the principal who is allowed to create the alias.

The following example policy statement specifies a particular alias in a Resource element. But you can list multiple alias ARNs or specify an alias pattern, such as "test*". You can also specify a Resource value of "*" to allow the principal to create any alias in the account and Region. Permission to create an alias can also be included in a `kms:Create*` permission for all resources in an account and Region.

```
{
  "Sid": "IAMPolicyForAnAlias",
  "Effect": "Allow",
  "Action": [
    "kms:CreateAlias",
    "kms:UpdateAlias",
    "kms>DeleteAlias"
  ]
}
```

```

    ],
    "Resource": "arn:aws:kms:us-west-2:111122223333:alias/test-key"
  }

```

- `kms:CreateAlias` for the KMS key. This permission must be provided in a key policy or in an IAM policy that is delegated from the key policy.

```

{
  "Sid": "Key policy for 1234abcd-12ab-34cd-56ef-1234567890ab",
  "Effect": "Allow",
  "Principal": {"AWS": "arn:aws:iam::111122223333:user/KMSAdminUser"},
  "Action": [
    "kms:CreateAlias",
    "kms:DescribeKey"
  ],
  "Resource": "*"
}

```

You can use condition keys to limit the KMS keys that you can associate with an alias. For example, you can use the [kms:KeySpec](#) condition key to allow the principal to create aliases only on asymmetric KMS keys. For a full list of conditions keys that you can use to limit the `kms:CreateAlias` permission on KMS key resources, see [Amazon KMS permissions](#).

kms:ListAliases

To list aliases in the account and Region, the principal must have `kms:ListAliases` permission in an IAM policy. Because this policy isn't related to any particular KMS key or alias resource, the value of the resource element in the policy must be "*" .

For example, the following IAM policy statement gives the principal permission to list all KMS keys and aliases in the account and Region.

```

{
  "Version": "2012-10-17",
  "Statement": {
    "Effect": "Allow",
    "Action": [
      "kms:ListKeys",
      "kms:ListAliases"
    ],
    "Resource": "*"
  }
}

```

```
}  
}
```

kms:UpdateAlias

To change the KMS key that is associated with an alias, the principal needs three permission elements: one for the alias, one for the current KMS key, and one for the new KMS key.

For example, suppose you want to change the test-key alias from the KMS key with key ID 1234abcd-12ab-34cd-56ef-1234567890ab to the KMS key with key ID 0987dcba-09fe-87dc-65ba-ab0987654321. In that case, include policy statements similar to the examples in this section.

- `kms:UpdateAlias` for the alias. You provide this permission in an IAM policy that is attached to the principal. The following IAM policy specifies a particular alias. But you can list multiple alias ARNs or specify an alias pattern, such as `"test*"`. You can also specify a `Resource` value of `"*"` to allow the principal to update any alias in the account and Region.

```
{  
  "Sid": "IAMPolicyForAnAlias",  
  "Effect": "Allow",  
  "Action": [  
    "kms:UpdateAlias",  
    "kms:ListAliases",  
    "kms:ListKeys"  
  ],  
  "Resource": "arn:aws:kms:us-west-2:111122223333:alias/test-key"  
}
```

- `kms:UpdateAlias` for the KMS key that is currently associated with the alias. This permission must be provided in a key policy or in an IAM policy that is delegated from the key policy.

```
{  
  "Sid": "Key policy for 1234abcd-12ab-34cd-56ef-1234567890ab",  
  "Effect": "Allow",  
  "Principal": {"AWS": "arn:aws:iam::111122223333:user/KMSAdminUser"},  
  "Action": [  
    "kms:UpdateAlias",  
    "kms:DescribeKey"  
  ],  
  "Resource": "*"  
}
```


- `kms:UpdateAlias` for the KMS key that the operation associates with the alias. This permission must be provided in a key policy or in an IAM policy that is delegated from the key policy.

```
{
  "Sid": "Key policy for 0987dcba-09fe-87dc-65ba-ab0987654321",
  "Effect": "Allow",
  "Principal": {"AWS": "arn:aws:iam::111122223333:user/KMSAdminUser"},
  "Action": [
    "kms:UpdateAlias",
    "kms:DescribeKey"
  ],
  "Resource": "*"
}
```

You can use condition keys to limit either or both of KMS keys in an `UpdateAlias` operation. For example, you can use a [kms:ResourceAliases](#) condition key to allow the principal to update aliases only when the target KMS key already has a particular alias. For a full list of conditions keys that you can use to limit the `kms:UpdateAlias` permission on a KMS key resource, see [Amazon KMS permissions](#).

kms:DeleteAlias

To delete an alias, the principal needs permission for the alias and for the associated KMS key.

As always, you should exercise caution when giving principals permission to delete a resource. However, deleting an alias has no effect on the associated KMS key. Although it might cause a failure in an application that relies on the alias, if you mistakenly delete an alias, you can recreate it.

- `kms:DeleteAlias` for the alias. Provide this permission in an IAM policy attached to the principal who is allowed to delete the alias.

The following example policy statement specifies the alias in a `Resource` element. But you can list multiple alias ARNs or specify an alias pattern, such as `"test*"`. You can also specify a `Resource` value of `"*"` to allow the principal to delete any alias in the account and Region.

```
{
  "Sid": "IAMPolicyForAnAlias",
  "Effect": "Allow",
  "Action": [
```

```

    "kms:CreateAlias",
    "kms:UpdateAlias",
    "kms:DeleteAlias"
  ],
  "Resource": "arn:aws:kms:us-west-2:111122223333:alias/test-key"
}

```

- `kms:DeleteAlias` for the associated KMS key. This permission must be provided in a key policy or in an IAM policy that is delegated from the key policy.

```

{
  "Sid": "Key policy for 1234abcd-12ab-34cd-56ef-1234567890ab",
  "Effect": "Allow",
  "Principal": {
    "AWS": "arn:aws:iam::111122223333:user/KMSAdminUser"
  },
  "Action": [
    "kms:CreateAlias",
    "kms:UpdateAlias",
    "kms:DeleteAlias",
    "kms:DescribeKey"
  ],
  "Resource": "*"
}

```

Limiting alias permissions

You can use condition keys to limit alias permissions when the resource is a KMS key. For example, the following IAM policy allows the alias operations on KMS keys in a particular account and Region. However, it uses the [kms:KeyOrigin](#) condition key to further limit the permissions to KMS keys with key material from Amazon KMS.

For a full list of conditions keys that you can use to limit alias permission on a KMS key resource, see [Amazon KMS permissions](#).

```

{
  "Sid": "IAMPolicyKeyPermissions",
  "Effect": "Allow",
  "Resource": "arn:aws:kms:us-west-2:111122223333:key/*",
  "Action": [
    "kms:CreateAlias",

```

```

    "kms:UpdateAlias",
    "kms>DeleteAlias"
  ],
  "Condition": {
    "StringEquals": {
      "kms:KeyOrigin": "AWS_KMS"
    }
  }
}

```

You can't use condition keys in a policy statement where the resource is an alias. To limit the aliases that a principal can manage, use the value of the `Resource` element of the IAM policy statement that controls access to the alias. For example, the following policy statements allow the principal to create, update, or delete any alias in the Amazon Web Services account and Region unless the alias begins with `Restricted`.

```

{
  "Sid": "IAMPolicyForAnAliasAllow",
  "Effect": "Allow",
  "Action": [
    "kms:CreateAlias",
    "kms:UpdateAlias",
    "kms>DeleteAlias"
  ],
  "Resource": "arn:aws:kms:us-west-2:111122223333:alias/*"
},
{
  "Sid": "IAMPolicyForAnAliasDeny",
  "Effect": "Deny",
  "Action": [
    "kms:CreateAlias",
    "kms:UpdateAlias",
    "kms>DeleteAlias"
  ],
  "Resource": "arn:aws:kms:us-west-2:111122223333:alias/Restricted*"
}

```

Create aliases

You can create aliases in the Amazon KMS console or by using Amazon KMS API operations.

The alias must be string of 1–256 characters. It can contain only alphanumeric characters, forward slashes (/), underscores (_), and dashes (-). The alias name for a [customer managed key](#) cannot begin with `alias/aws/`. The `alias/aws/` prefix is reserved for [Amazon managed key](#).

You can create an alias for a new KMS key or for an existing KMS key. You might add an alias so that a particular KMS key is used in a project or application.

You can also use a Amazon CloudFormation template to create an alias for a KMS key. For more information, see [AWS::KMS::Alias](#) in the *Amazon CloudFormation User Guide*.

Using the Amazon KMS console

When you [create a KMS key](#) in the Amazon KMS console, you must create an alias for the new KMS key. To create an alias for an existing KMS key, use the **Aliases** tab on the detail page for the KMS key.

1. Sign in to the Amazon Web Services Management Console and open the Amazon Key Management Service (Amazon KMS) console at <https://console.amazonaws.cn/kms>.
2. To change the Amazon Web Services Region, use the Region selector in the upper-right corner of the page.
3. In the navigation pane, choose **Customer managed keys**. You cannot manage aliases for Amazon managed keys or Amazon owned keys.
4. In the table, choose the key ID or alias of the KMS key. Then, on the KMS key detail page, choose the **Aliases** tab.

If a KMS key has multiple aliases, the **Aliases** column in the table displays one alias and an alias summary, such as **(+n more)**. Choosing the alias summary takes you directly to the **Aliases** tab on the KMS key detail page.

5. On the **Aliases** tab, choose **Create alias**. Enter an alias name and choose **Create alias**.

Important

Do not include confidential or sensitive information in this field. This field may be displayed in plaintext in CloudTrail logs and other output.

Note

Do not add the `alias/` prefix. The console automatically adds it for you. If you enter `alias/ExampleAlias`, the actual alias name will be `alias/alias/ExampleAlias`.

Using the Amazon KMS API

To create an alias, use the [CreateAlias](#) operation. Unlike the process of creating KMS keys in the console, the [CreateKey](#) operation doesn't create an alias for a new KMS key.

Important

Do not include confidential or sensitive information in this field. This field may be displayed in plaintext in CloudTrail logs and other output.

You can use the `CreateAlias` operation to create an alias for a new KMS key with no alias. You can also use the `CreateAlias` operation to add an alias to any existing KMS key or to recreate an alias that was accidentally deleted.

In the Amazon KMS API operations, the alias name must begin with `alias/` followed by a name, such as `alias/ExampleAlias`. The alias must be unique in the account and Region. To find the alias names that are already in use, use the [ListAliases](#) operation. The alias name is case sensitive.

The `TargetKeyId` can be any [customer managed key](#) in the same Amazon Web Services Region. To identify the KMS key, use its [key ID](#) or [key ARN](#). You cannot use another alias.

The following example creates the `example-key` alias and associates it with the specified KMS key. These examples use the Amazon Command Line Interface (Amazon CLI). For examples in multiple programming languages, see [Use CreateAlias with an Amazon SDK or CLI](#).

```
$ aws kms create-alias \  
  --alias-name alias/example-key \  
  --target-key-id 1234abcd-12ab-34cd-56ef-1234567890ab
```

`CreateAlias` does not return any output. To see the new alias, use the `ListAliases` operation. For details, see [Using the Amazon KMS API](#).

Find the alias name and alias ARN for a KMS key

Aliases make it easy to recognize KMS keys in the Amazon KMS console. You can view the aliases for a KMS key in the Amazon KMS console or by using the [ListAliases](#) operation. The [DescribeKey](#) operation, which returns the properties of a KMS key, does not include aliases.

The following procedures demonstrate how to view and identify the aliases associated with a KMS key using the Amazon KMS console and Amazon KMS API. The Amazon KMS API examples use the [Amazon Command Line Interface \(Amazon CLI\)](#), but you can use any supported programming language.

Using the Amazon KMS console

The Amazon KMS console displays the aliases associated with the KMS key.

1. Open the Amazon KMS console at <https://console.amazonaws.cn/kms>.
2. To change the Amazon Web Services Region, use the Region selector in the upper-right corner of the page.
3. To view the keys in your account that you create and manage, in the navigation pane choose **Customer managed keys**. To view the keys in your account that Amazon creates and manages for you, in the navigation pane, choose **Amazon managed keys**.
4. The **Aliases** column displays the alias for each KMS key. If a KMS key does not have an alias, a dash (-) appears in the **Aliases** column.

If a KMS key has multiple aliases, the **Aliases** column also has an alias summary, such as **(+n more)**. For example, the following KMS key has two aliases, one of which is key-test.

To find the alias name and alias ARN of all aliases for the KMS key, use the **Aliases** tab.

- To go directly to the **Aliases** tab, in the **Aliases** column, choose the alias summary **(+n more)**. An alias summary appears only if the KMS key has more than one alias.
- Or, choose the alias or key ID of the KMS key (which opens the detail page for the KMS key) and then choose the **Aliases** tab. The tabs are under the **General configuration** section.

Customer managed keys (16) Key actions ▾ Create key

Filter keys by aliases, key ID, or key type < 1 2 > ⚙

<input type="checkbox"/>	Aliases ▾	Key ID ▾	Status
<input type="checkbox"/>	key-test (+1 more)	1234abcd-12ab-34cd-56ef-1234567890ab	Enabled
<input type="checkbox"/>	-	1a2b3c4d-5e6f-1a2b-3c4d-5e6f1a2b3c4d	Enabled

5. The **Aliases** tab displays the alias name and alias ARN of all aliases for a KMS key. You can also create and delete aliases for the KMS key on this tab.

Key policy | Cryptographic configuration | Key material | Tags | Public key | **Aliases**

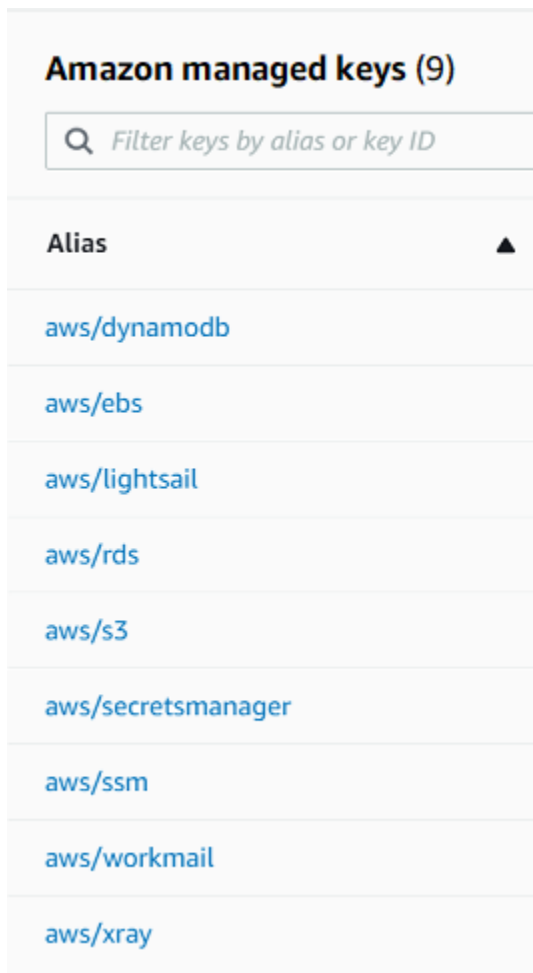
Aliases [Info](#) Delete Create new alias

Filter by Alias name < 1 >

<input type="checkbox"/>	Alias name	Alias ARN
<input type="checkbox"/>	key-test	arn:aws:kms:us-east-1:111122223333:alias/key-test
<input type="checkbox"/>	project-key	arn:aws:kms:us-east-1:111122223333:alias/project-key

Amazon managed keys

You can use the alias to recognize an Amazon managed key, as shown in this example **Amazon managed keys** page. The aliases for Amazon managed keys always have the format: `aws/<service-name>`. For example, the alias for the Amazon managed key for Amazon DynamoDB is `aws/dynamodb`.



Using the Amazon KMS API

The [ListAliases](#) operation returns the alias name and alias ARN of aliases in the account and Region. The output includes aliases for Amazon managed keys and for customer managed keys. The aliases for Amazon managed keys have the format `aws/<service-name>`, such as `aws/dynamodb`.

The response might also include aliases that have no `TargetKeyId` field. These are predefined aliases that Amazon has created but has not yet associated with a KMS key.

```
$ aws kms list-aliases
{
  "Aliases": [
    {
      "AliasName": "alias/access-key",
      "AliasArn": "arn:aws:kms:us-west-2:111122223333:alias/access-key",
      "TargetKeyId": "0987dcba-09fe-87dc-65ba-ab0987654321",
      "CreationDate": 1516435200.399,
```



```

    "LastUpdatedDate": 1516435200.399
  },
  {
    "AliasName": "alias/ECC-P521-Sign",
    "AliasArn": "arn:aws:kms:us-west-2:111122223333:alias/ECC-P521-Sign",
    "TargetKeyId": "1234abcd-12ab-34cd-56ef-1234567890ab",
    "CreationDate": 1693622000.704,
    "LastUpdatedDate": 1693622000.704
  },
  {
    "AliasName": "alias/ImportedKey",
    "AliasArn": "arn:aws:kms:us-west-2:111122223333:alias/ImportedKey",
    "TargetKeyId": "1a2b3c4d-5e6f-1a2b-3c4d-5e6f1a2b3c4d",
    "CreationDate": 1493622000.704,
    "LastUpdatedDate": 1521097200.235
  },
  {
    "AliasName": "alias/finance-project",
    "AliasArn": "arn:aws:kms:us-west-2:111122223333:alias/finance-project",
    "TargetKeyId": "0987dcba-09fe-87dc-65ba-ab0987654321",
    "CreationDate": 1604958290.014,
    "LastUpdatedDate": 1604958290.014
  },
  {
    "AliasName": "alias/aws/dynamodb",
    "AliasArn": "arn:aws:kms:us-west-2:111122223333:alias/aws/dynamodb",
    "TargetKeyId": "0987ab65-43cd-21ef-09ab-87654321cdef",
    "CreationDate": 1521097200.454,
    "LastUpdatedDate": 1521097200.454
  },
  {
    "AliasName": "alias/aws/ebs",
    "AliasArn": "arn:aws:kms:us-west-2:111122223333:alias/aws/ebs",
    "TargetKeyId": "abcd1234-09fe-ef90-09fe-ab0987654321",
    "CreationDate": 1466518990.200,
    "LastUpdatedDate": 1466518990.200
  }
]
}

```

To get all aliases that are associated with a particular KMS key, use the optional `KeyId` parameter of the `ListAliases` operation. The `KeyId` parameter takes the [key ID](#) or [key ARN](#) of the KMS key.

This example gets all aliases associated with the 0987dcba-09fe-87dc-65ba-ab0987654321 KMS key.

```
$ aws kms list-aliases --key-id 0987dcba-09fe-87dc-65ba-ab0987654321
{
  "Aliases": [
    {
      "AliasName": "alias/access-key",
      "AliasArn": "arn:aws:kms:us-west-2:111122223333:alias/access-key",
      "TargetKeyId": "0987dcba-09fe-87dc-65ba-ab0987654321",
      "CreationDate": "2018-01-20T15:23:10.194000-07:00",
      "LastUpdatedDate": "2018-01-20T15:23:10.194000-07:00"
    },
    {
      "AliasName": "alias/finance-project",
      "AliasArn": "arn:aws:kms:us-west-2:111122223333:alias/finance-project",
      "TargetKeyId": "0987dcba-09fe-87dc-65ba-ab0987654321",
      "CreationDate": 1604958290.014,
      "LastUpdatedDate": 1604958290.014
    }
  ]
}
```

The `KeyId` parameter doesn't take wildcard characters, but you can use the features of your programming language to filter the response.

For example, the following Amazon CLI command gets only the aliases for Amazon managed keys.

```
$ aws kms list-aliases --query 'Aliases[?starts_with(AliasName, `alias/aws/`)]'
```

The following command gets only the access-key alias. The alias name is case-sensitive.

```
$ aws kms list-aliases --query 'Aliases[?AliasName==`alias/access-key`]'
[
  {
    "AliasName": "alias/access-key",
    "AliasArn": "arn:aws:kms:us-west-2:111122223333:alias/access-key",
    "TargetKeyId": "0987dcba-09fe-87dc-65ba-ab0987654321",
    "CreationDate": "2018-01-20T15:23:10.194000-07:00",
    "LastUpdatedDate": "2018-01-20T15:23:10.194000-07:00"
  }
]
```

Update aliases

Because an alias is an independent resource, you can change the KMS key associated with an alias. For example, if the `test-key` alias is associated with one KMS key, you can use the [UpdateAlias](#) operation to associate it with a different KMS key. This is one of several ways to [manually rotate a KMS key](#) without changing its key material. You might also update a KMS key so that an application that was using one KMS key for new resources is now using a different KMS key.

You cannot update an alias in the Amazon KMS console. Also, you cannot use `UpdateAlias` (or any other operation) to change an alias name. To change an alias name, delete the current alias and then create a new alias for the KMS key.

When you update an alias, the current KMS key and the new KMS key must be the same type (both symmetric or asymmetric or HMAC). They must also have the same key usage (`ENCRYPT_DECRYPT` or `SIGN_VERIFY` or `GENERATE_VERIFY_MAC`). This restriction prevents cryptographic errors in code that uses aliases.

The following example begins by using the [ListAliases](#) operation to show that the `test-key` alias is currently associated with KMS key `1234abcd-12ab-34cd-56ef-1234567890ab`.

```
$ aws kms list-aliases --key-id 1234abcd-12ab-34cd-56ef-1234567890ab
{
  "Aliases": [
    {
      "AliasName": "alias/test-key",
      "AliasArn": "arn:aws:kms:us-west-2:111122223333:alias/test-key",
      "TargetKeyId": "1234abcd-12ab-34cd-56ef-1234567890ab",
      "CreationDate": 1593622000.191,
      "LastUpdatedDate": 1593622000.191
    }
  ]
}
```

Next, it uses the `UpdateAlias` operation to change the KMS key that is associated with the `test-key` alias to KMS key `0987dcba-09fe-87dc-65ba-ab0987654321`. You don't need to specify the currently associated KMS key, only the new ("target") KMS key. The alias name is case sensitive.

```
$ aws kms update-alias --alias-name 'alias/test-key' --target-key-id
0987dcba-09fe-87dc-65ba-ab0987654321
```

To verify that the alias is now associated with the target KMS key, use the `ListAliases` operation again. This Amazon CLI command uses the `--query` parameter to get only the `test-key` alias. The `TargetKeyId` and `LastUpdatedDate` fields are updated.

```
$ aws kms list-aliases --query 'Aliases[?AliasName==`alias/test-key`]'
[
  {
    "AliasName": "alias/test-key",
    "AliasArn": "arn:aws:kms:us-west-2:111122223333:alias/test-key",
    "TargetKeyId": "0987dcba-09fe-87dc-65ba-ab0987654321",
    "CreationDate": 1593622000.191,
    "LastUpdatedDate": 1604958290.154
  }
]
```

Delete an alias

You can delete an alias in the Amazon KMS console or by using the [DeleteAlias](#) operation. Before deleting an alias, make sure that it's not in use. Although deleting an alias doesn't affect the associated KMS key, it might create problems for any application that uses the alias. If you delete an alias by mistake, you can create a new alias with the same name and associate it with the same or a different KMS key.

If you delete a KMS key, all aliases associated with that KMS key are deleted.

Using the Amazon KMS console

To delete an alias in the Amazon KMS console, use the **Aliases** tab on the detail page for the KMS key. You can delete multiple aliases for a KMS key at one time.

1. Sign in to the Amazon Web Services Management Console and open the Amazon Key Management Service (Amazon KMS) console at <https://console.amazonaws.cn/kms>.
2. To change the Amazon Web Services Region, use the Region selector in the upper-right corner of the page.
3. In the navigation pane, choose **Customer managed keys**. You cannot manage aliases for Amazon managed keys or Amazon owned keys.
4. In the table, choose the key ID or alias of the KMS key. Then, on the KMS key detail page, choose the **Aliases** tab.

If a KMS key has multiple aliases, the **Aliases** column in the table displays one alias and an alias summary, such as **(+n more)**. Choosing the alias summary takes you directly to the **Aliases** tab on the KMS key detail page.

5. On the **Aliases** tab, select the check box next to the aliases that you want to delete. Then choose **Delete**.

Using the Amazon KMS API

To delete an alias, use the [DeleteAlias](#) operation. This operation deletes one alias at a time. The alias name is case-sensitive and it must be preceded by the `alias/` prefix.

For example, the following command deletes the `test-key` alias. This command does not return any output.

```
$ aws kms delete-alias --alias-name alias/test-key
```

To verify that the alias is deleted, use the [ListAliases](#) operation. The following command uses the `--query` parameter in the Amazon CLI to get only the `test-key` alias. The empty brackets in the response indicate that the `ListAliases` response didn't include a `test-key` alias. To eliminate the brackets, use the `--output text` parameter and value.

```
$ aws kms list-aliases --query 'Aliases[?AliasName==`alias/test-key`]'
[]
```

Use aliases to control access to KMS keys

You can control access to KMS keys based on the aliases that are associated with the KMS key. To do so, use the [kms:RequestAlias](#) and [kms:ResourceAliases](#) condition keys. This feature is part of Amazon KMS support for [attribute-based access control](#) (ABAC).

The `kms:RequestAlias` condition key allows or denies access to a KMS key based on the alias in a request. The `kms:ResourceAliases` condition key allows or denies access to a KMS key based on the aliases associated with the KMS key.

These features do not allow you to identify a KMS key by using an alias in the `resource` element of a policy statement. When an alias is the value of a `resource` element, the policy applies to the alias resource, not to any KMS key that might be associated with it.

Note

It might take up to five minutes for tag and alias changes to affect KMS key authorization. Recent changes might be visible in API operations before they affect authorization.

When using aliases to control access to KMS keys, consider the following:

- Use aliases to reinforce the best practice of [least privileged access](#). Give IAM principals only the permissions that they need for only the KMS keys that they must use or manage. For example, use aliases to identify the KMS keys used for a project. Then give the project team permission to use only KMS keys with the project aliases.
- Be cautious about giving principals the `kms:CreateAlias`, `kms:UpdateAlias`, or `kms>DeleteAlias` permissions that let them add, edit, and delete aliases. When you use aliases to control access to KMS keys, changing an alias can give principals permission to use KMS keys that they didn't otherwise have permission to use. It can also deny access to KMS keys that other principals require to do their jobs.
- Review the principals in your Amazon Web Services account that currently have permission to manage aliases and adjust the permissions, if necessary. Key administrators who don't have permission to change key policies or create grants can control access to KMS keys if they have permission to manage aliases.

For example, the console [default key policy for key administrators](#) includes `kms:CreateAlias`, `kms>DeleteAlias`, and `kms:UpdateAlias` permission. IAM policies might give alias permissions for all KMS keys in your Amazon Web Services account. For example, the [AWSKeyManagementServicePowerUser](#) managed policy allows principals to create, delete, and list aliases for all KMS keys but not update them.

- Before setting a policy that depends on an alias, review the aliases on the KMS keys in your Amazon Web Services account. Make sure that your policy applies only to the aliases that you intend to include. Use [CloudTrail logs](#) and [CloudWatch alarms](#) to alert you to alias changes that might affect access to your KMS keys. Also, the [ListAliases](#) response includes the creation date and last updated date for each alias.
- The alias policy conditions use pattern matching; they aren't tied to a particular instance of an alias. A policy that uses alias-based condition keys affects all new and existing aliases that match the pattern. If you delete and recreate an alias that matches a policy condition, the condition applies to the new alias, just as it did to the old one.

The `kms:RequestAlias` condition key relies on the alias specified explicitly in an operation request. The `kms:ResourceAliases` condition key depends on the aliases that are associated with a KMS key, even if they don't appear in the request.

kms:RequestAlias

Allow or deny access to a KMS key based on the alias that identifies the KMS key in a request. You can use the [kms:RequestAlias](#) condition key in a [key policy](#) or IAM policy. It applies to operations that use an alias to identify a KMS key in a request, namely [cryptographic operations](#), [DescribeKey](#), and [GetPublicKey](#). It is not valid for alias operations, such as [CreateAlias](#) or [DeleteAlias](#).

In the condition key, specify an [alias name](#) or alias name pattern. You cannot specify an [alias ARN](#).

For example, the following key policy statement allows principals to use the specified operations on the KMS key. The permission is effective only when the request uses an alias that includes alpha to identify the KMS key.

```
{
  "Sid": "Key policy using a request alias condition",
  "Effect": "Allow",
  "Principal": {
    "AWS": "arn:aws:iam::111122223333:role/alpha-developer"
  },
  "Action": [
    "kms:Decrypt",
    "kms:GenerateDataKey*",
    "kms:DescribeKey"
  ],
  "Resource": "*",
  "Condition": {
    "StringLike": {
      "kms:RequestAlias": "alias/*alpha*"
    }
  }
}
```

The following example request from an authorized principal would fulfill the condition. However, a request that used a [key ID](#), a [key ARN](#), or a different alias would not fulfill the condition, even if these values identified the same KMS key.

```
$ aws kms describe-key --key-id "arn:aws:kms:us-west-2:111122223333:alias/project-alpha"
```

kms:ResourceAliases

Allow or deny access to a KMS key based on the aliases associated with the KMS key, even if the alias isn't used in a request. The [kms:ResourceAliases](#) condition key lets you specify an alias or alias pattern, such as `alias/test*`, so you can use it in an IAM policy to control access to several KMS keys in the same Region. It's valid for any Amazon KMS operation that uses a KMS key.

For example, the following IAM policy lets the principals call the specified operations on the KMS keys in two Amazon Web Services accounts. However, the permission applies only to KMS keys associated with aliases that begin with `restricted`.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AliasBasedIAMPolicy",
      "Effect": "Allow",
      "Action": [
        "kms:Decrypt",
        "kms:GenerateDataKey*",
        "kms:DescribeKey"
      ],
      "Resource": [
        "arn:aws:kms:*:111122223333:key/*",
        "arn:aws:kms:*:444455556666:key/*"
      ],
      "Condition": {
        "ForAnyValue:StringLike": {
          "kms:ResourceAliases": "alias/restricted*"
        }
      }
    }
  ]
}
```

The `kms:ResourceAliases` condition is a condition of the resource, not the request. As such, a request that doesn't specify the alias can still satisfy the condition.

The following example request, which specifies a matching alias, satisfies the condition.

```
$ aws kms enable-key-rotation --key-id "alias/restricted-project"
```

However, the following example request also satisfies the condition, provided that the specified KMS key has an alias that begins with `restricted`, even if that alias isn't used in the request.

```
$ aws kms enable-key-rotation --key-id "1234abcd-12ab-34cd-56ef-1234567890ab"
```

Learn how to use aliases in your applications

You can use an alias to represent a KMS key in your application code. The `KeyId` parameter in Amazon KMS [cryptographic operations](#), [DescribeKey](#), and [GetPublicKey](#) accepts an alias name or alias ARN.

For example, the following `GenerateDataKey` command uses an alias name (`alias/finance`) to identify a KMS key. The alias name is the value of the `KeyId` parameter.

```
$ aws kms generate-data-key --key-id alias/finance --key-spec AES_256
```

If the KMS key is in a different Amazon Web Services account, you must use a key ARN or alias ARN in these operations. When using an alias ARN, remember that the alias for a KMS key is defined in the account that owns the KMS key and might differ in each Region. For help finding the alias ARN, see [Find the alias name and alias ARN for a KMS key](#).

For example, the following `GenerateDataKey` command uses a KMS key that's not in the caller's account. The `ExampleAlias` alias is associated with the KMS key in the specified account and Region.

```
$ aws kms generate-data-key --key-id arn:aws:kms:us-west-2:444455556666:alias/  
ExampleAlias --key-spec AES_256
```

One of the most powerful uses of aliases is in applications that run in multiple Amazon Web Services Regions. For example, you might have a global application that uses an RSA [asymmetric KMS key](#) for signing and verification.

- In US West (Oregon) (`us-west-2`), you want to use `arn:aws:kms:us-west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab`.

- In Europe (Frankfurt) (eu-central-1), you want to use `arn:aws:kms:eu-central-1:111122223333:key/0987dcba-09fe-87dc-65ba-ab0987654321`
- In Asia Pacific (Singapore) (ap-southeast-1), you want to use `arn:aws:kms:ap-southeast-1:111122223333:key/1a2b3c4d-5e6f-1a2b-3c4d-5e6f1a2b3c4d`.

You could create a different version of your application in each Region or use a dictionary or switch statement to select the right KMS key for each Region. But it's much easier to create an alias with the same alias name in each Region. Remember that the alias name is case-sensitive.

```
aws --region us-west-2 kms create-alias \  
  --alias-name alias/new-app \  
  --key-id arn:aws:kms:us-  
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab  
  
aws --region eu-central-1 kms create-alias \  
  --alias-name alias/new-app \  
  --key-id arn:aws:kms:eu-central-1:111122223333:key/0987dcba-09fe-87dc-65ba-  
ab0987654321  
  
aws --region ap-southeast-1 kms create-alias \  
  --alias-name alias/new-app \  
  --key-id arn:aws:kms:ap-  
southeast-1:111122223333:key/1a2b3c4d-5e6f-1a2b-3c4d-5e6f1a2b3c4d
```

Then, use the alias in your code. When your code runs in each Region, the alias will refer to its associated KMS key in that Region. For example, this code calls the [Sign](#) operation with an alias name.

```
aws kms sign --key-id alias/new-app \  
  --message $message \  
  --message-type RAW \  
  --signing-algorithm RSASSA_PSS_SHA_384
```

However, there is a risk that the alias might be deleted or updated to be associated with a different KMS key. In that case, the application's attempts to verify signatures using the alias name will fail, and you might need to recreate or update the alias.

To mitigate this risk, be cautious about giving principals permission to manage the aliases that you use in your application. For details, see [Controlling access to aliases](#).

There are several other solutions for applications that encrypt data in multiple Amazon Web Services Regions, including the [Amazon Encryption SDK](#).

Find aliases in Amazon CloudTrail logs

You can use an alias to represent an Amazon KMS key in an Amazon KMS API operation. When you do, the alias and the key ARN of the KMS key are recorded in the Amazon CloudTrail log entry for the event. The alias appears in the `requestParameters` field. The key ARN appears in the `resources` field. This is true even when an Amazon service uses an Amazon managed key in your account.

For example, the following [GenerateDataKey](#) request uses the `project-key` alias to represent a KMS key.

```
$ aws kms generate-data-key --key-id alias/project-key --key-spec AES_256
```

When this request is recorded in the CloudTrail log, the log entry includes both the alias and the key ARN of the actual KMS key that was used.

```
{
  "eventVersion": "1.05",
  "userIdentity": {
    "type": "IAMUser",
    "principalId": "ABCDE",
    "arn": "arn:aws:iam::111122223333:role/ProjectDev",
    "accountId": "111122223333",
    "accessKeyId": "FFHIJ",
    "userName": "example-dev"
  },
  "eventTime": "2020-06-29T23:36:41Z",
  "eventSource": "kms.amazonaws.com",
  "eventName": "GenerateDataKey",
  "awsRegion": "us-west-2",
  "sourceIPAddress": "205.205.123.000",
  "userAgent": "aws-cli/1.18.89 Python/3.6.10
Linux/4.9.217-0.1.ac.205.84.332.metal1.x86_64 boto3/1.17.12",
  "requestParameters": {
    "keyId": "alias/project-key",
    "keySpec": "AES_256"
  },
  "responseElements": null,
```

```
"requestID": "d93f57f5-d4c5-4bab-8139-5a1f7824a363",
"eventID": "d63001e2-dbc6-4aae-90cb-e5370aca7125",
"readOnly": true,
"resources": [
  {
    "accountId": "111122223333",
    "type": "AWS::KMS::Key",
    "ARN": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab"
  }
],
"eventType": "AwsApiCall",
"recipientAccountId": "111122223333"
}
```

For details about logging Amazon KMS operations in CloudTrail logs, see [Logging Amazon KMS API calls with Amazon CloudTrail](#).

Tags in Amazon KMS

A *tag* is an optional metadata label that you can assign (or Amazon can assign) to an Amazon resource. Each tag consists of a *tag key* and a *tag value*, both of which are case-sensitive strings. The tag value can be an empty (null) string. Each tag on a resource must have a different tag key, but you can add the same tag to multiple Amazon resources. Each resource can have up to 50 user-created tags.

Do not include confidential or sensitive information in the tag key or tag value. Tags are accessible to many Amazon Web Services services, including billing.

In Amazon KMS, you can add tags to a customer managed key when you create the KMS key, and tag or untag existing KMS keys unless they are [pending deletion](#). You cannot tag aliases, custom key stores, Amazon managed keys, Amazon owned keys, or KMS keys in other Amazon Web Services accounts. Tags are optional, but they can be very useful.

For example, you can add a "Project"="Alpha" tag to all KMS keys and Amazon S3 buckets that you use for the Alpha project.

```
TagKey    = "Project"  
TagValue  = "Alpha"
```

For general information about tags, including the format and syntax, see [Tagging Amazon resources](#) in the *Amazon Web Services General Reference*.

Tags help you do the following:

- Identify and organize your Amazon resources. Many Amazon services support tagging, so you can assign the same tag to resources from different services to indicate that the resources are related. For example, you can assign the same tag to a KMS key and an Amazon Elastic Block Store (Amazon EBS) volume or Amazon Secrets Manager secret. You can also use tags to identify KMS keys for automation.
- Track your Amazon costs. When you add tags to your Amazon resources, Amazon generates a cost allocation report with usage and costs aggregated by tags. You can use this feature to track Amazon KMS costs for a project, application, or cost center.

For more information about using tags for cost allocation, see [Using Cost Allocation Tags](#) in the *Amazon Billing User Guide*. For information about the rules for tag keys and tag values, see [User-Defined Tag Restrictions](#) in the *Amazon Billing User Guide*.

- Control access to your Amazon resources. Allowing and denying access to KMS keys based on their tags is part of Amazon KMS support for [attribute-based access control](#) (ABAC). For information about controlling access to Amazon KMS keys based on their tags, see [Use tags to control access to KMS keys](#). For more general information about using tags to control access to Amazon resources, see [Controlling Access to Amazon Resources Using Resource Tags](#) in the *IAM User Guide*.

Amazon KMS writes an entry to your Amazon CloudTrail log when you use the [TagResource](#), [UntagResource](#), or [ListResourceTags](#) operations.

Topics

- [Controlling access to tags](#)
- [Add tags to a KMS key](#)
- [Edit tags associated with a KMS key](#)
- [Remove tags associated with a KMS key](#)
- [View tags associated with a KMS key](#)
- [Use tags to control access to KMS keys](#)

Controlling access to tags

To add, view, and delete tags, either in the Amazon KMS console or by using the API, principals need tagging permissions. You can provide these permissions in [key policies](#). You can also provide them in IAM policies (including [VPC endpoint policies](#)), but only if [the key policy allows it](#). The [AWSKeyManagementServicePowerUser](#) managed policy allows principals to tag, untag, and list tags on all KMS keys the account can access.

You can also limit these permissions by using Amazon global condition keys for tags. In Amazon KMS, these conditions can control access to tagging operations, such as [TagResource](#) and [UntagResource](#).

Note

Be cautious when giving principals permission to manage tags and aliases. Changing a tag or alias can allow or deny permission to the customer managed key. For details, see [ABAC for Amazon KMS](#) and [Use tags to control access to KMS keys](#).

For example policies and more information, see [Controlling Access Based on Tag Keys](#) in the *IAM User Guide*.

Permissions to create and manage tags work as follows.

kms:TagResource

Allows principals to add or edit tags. To add tags while creating a KMS key, the principal must have permission in an IAM policy that isn't restricted to particular KMS keys.

kms:ListResourceTags

Allows principals to view tags on KMS keys.

kms:UntagResource

Allows principals to delete tags from KMS keys.

Tag permissions in policies

You can provide tagging permissions in a key policy or IAM policy. For example, the following example key policy gives select users tagging permission on the KMS key. It gives all users who can assume the example Administrator or Developer roles permission to view tags.

```
{
  "Version": "2012-10-17",
  "Id": "example-key-policy",
  "Statement": [
    {
      "Sid": "Enable IAM User Permissions",
      "Effect": "Allow",
      "Principal": {"AWS": "arn:aws:iam::111122223333:root"},
      "Action": "kms:*",
      "Resource": "*"
    },
    {
      "Sid": "Allow all tagging permissions",
      "Effect": "Allow",
      "Principal": {"AWS": [
        "arn:aws:iam::111122223333:user/LeadAdmin",
        "arn:aws:iam::111122223333:user/SupportLead"
      ]}
    }
  ]
}
```

```

    "Action": [
      "kms:TagResource",
      "kms:ListResourceTags",
      "kms:UntagResource"
    ],
    "Resource": "*"
  },
  {
    "Sid": "Allow roles to view tags",
    "Effect": "Allow",
    "Principal": {"AWS": [
      "arn:aws:iam::111122223333:role/Administrator",
      "arn:aws:iam::111122223333:role/Developer"
    ]},
    "Action": "kms:ListResourceTags",
    "Resource": "*"
  }
]
}

```

To give principals tagging permission on multiple KMS keys, you can use an IAM policy. For this policy to be effective, the key policy for each KMS key must allow the account to use IAM policies to control access to the KMS key.

For example, the following IAM policy allows the principals to create KMS keys. It also allows them to create and manage tags on all KMS keys in the specified account. This combination allows the principals to use the [Tags](#) parameter of the [CreateKey](#) operation to add tags to a KMS key while they are creating it.

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "IAMPolicyCreateKeys",
      "Effect": "Allow",
      "Action": "kms:CreateKey",
      "Resource": "*"
    },
    {
      "Sid": "IAMPolicyTags",
      "Effect": "Allow",
      "Action": [
        "kms:TagResource",

```



```
        "kms:UntagResource",
        "kms:ListResourceTags"
    ],
    "Resource": "arn:aws:kms:*:111122223333:key/*"
}
]
```

Limiting tag permissions

You can limit tagging permissions by using [policy conditions](#). The following policy conditions can be applied to the `kms:TagResource` and `kms:UntagResource` permissions. For example, you can use the `aws:RequestTag/tag-key` condition to allow a principal to add only particular tags, or prevent a principal from adding tags with particular tag keys. Or, you can use the `kms:KeyOrigin` condition to prevent principals from tagging or untagging KMS keys with [imported key material](#).

- [aws:RequestTag](#)
- [aws:ResourceTag/tag-key](#) (IAM policies only)
- [aws:TagKeys](#)
- [kms:CallerAccount](#)
- [kms:KeySpec](#)
- [kms:KeyUsage](#)
- [kms:KeyOrigin](#)
- [kms:ViaService](#)

As a best practice when you use tags to control access to KMS keys, use the `aws:RequestTag/tag-key` or `aws:TagKeys` condition key to determine which tags (or tag keys) are allowed.

For example, the following IAM policy is similar to the previous one. However, this policy allows the principals to create tags (`TagResource`) and delete tags `UntagResource` only for tags with a `Project` tag key.

Because `TagResource` and `UntagResource` requests can include multiple tags, you must specify a `ForAllValues` or `ForAnyValue` set operator with the [aws:TagKeys](#) condition. The

ForAnyValue operator requires that at least one of the tag keys in the request matches one of the tag keys in the policy. The ForAllValues operator requires that all of the tag keys in the request match one of the tag keys in the policy. The ForAllValues operator also returns true if there are no tags in the request, but TagResource and UntagResource fail when no tags are specified. For details about the set operators, see [Use multiple keys and values](#) in the *IAM User Guide*.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "IAMPolicyCreateKey",
      "Effect": "Allow",
      "Action": "kms:CreateKey",
      "Resource": "*"
    },
    {
      "Sid": "IAMPolicyViewAllTags",
      "Effect": "Allow",
      "Action": "kms:ListResourceTags",
      "Resource": "arn:aws:kms:*:111122223333:key/*"
    },
    {
      "Sid": "IAMPolicyManageTags",
      "Effect": "Allow",
      "Action": [
        "kms:TagResource",
        "kms:UntagResource"
      ],
      "Resource": "arn:aws:kms:*:111122223333:key/*",
      "Condition": {
        "ForAllValues:StringEquals": {"aws:TagKeys": "Project"}
      }
    }
  ]
}
```

Add tags to a KMS key

Tags help identify and organize your Amazon resources. You can add tags to a customer managed key when you [create the KMS key](#), or add tags to existing KMS keys. You cannot tag Amazon managed keys.

The following procedures demonstrate how to add tags to customer managed keys using the Amazon KMS console and Amazon KMS API. The Amazon KMS API examples use the [Amazon Command Line Interface \(Amazon CLI\)](#), but you can use any supported programming language.

Topics

- [Add tags while creating a KMS key](#)
- [Add tags to existing KMS keys](#)

Add tags while creating a KMS key

You can add tags to a KMS key as you create the key using the Amazon KMS console or the [CreateKey](#) operation. To add tags when creating a KMS key, you must have `kms:TagResource` permission in an IAM policy in addition to the permissions required to create KMS keys. At a minimum, the permission must cover all KMS keys in the account and Region. For details, see [Controlling access to tags](#).

Using the Amazon KMS console

To add tags when creating a KMS key in the console, you must have the permissions required to view KMS keys in the console in addition to the permissions required to tag and create KMS keys. At a minimum, the permission must cover all KMS keys in the account and Region.

1. Sign in to the Amazon Web Services Management Console and open the Amazon Key Management Service (Amazon KMS) console at <https://console.amazonaws.cn/kms>.
2. To change the Amazon Web Services Region, use the Region selector in the upper-right corner of the page.
3. In the navigation pane, choose **Customer managed keys**. (You cannot manage the tags of an Amazon managed key)
4. Choose the key type, then choose **Next**.
5. Enter an alias and optional description.
6. Enter a tag key and, optionally, a tag value. To add additional tags, choose **Add tag**. To delete a tag, choose **Remove**. When you're done tagging your new KMS key, choose **Next**.
7. Finish creating your KMS key.

Using the Amazon KMS API

To specify tags when creating keys using the [CreateKey](#) operation, use the Tags parameter of the operation.

The value of the Tags parameter of `CreateKey` is a collection of case-sensitive tag key and tag value pairs. Each tag on a KMS key must have a different tag name. The tag value can be a null or empty string.

For example, the following Amazon CLI command creates a symmetric encryption KMS key with a `Project:Alpha` tag. When specifying more than one key-value pair, use a space to separate each pair.

```
$ aws kms create-key --tags TagKey=Project,TagValue=Alpha
```

When this command is successful, it returns a `KeyMetadata` object with information about the new KMS key. However, the `KeyMetadata` does not include tags. To get the tags, use the [ListResourceTags](#) operation.

Add tags to existing KMS keys

You can add tags to your existing customer managed KMS keys in the Amazon KMS console or by using the [TagResource](#) operation. To add tags, you need tagging permission on the KMS key. You can get this permission from the key policy for the KMS key or, if the key policy allows it, from an IAM policy that includes the KMS key.

Using the Amazon KMS console

1. Sign in to the Amazon Web Services Management Console and open the Amazon Key Management Service (Amazon KMS) console at <https://console.amazonaws.cn/kms>.
2. To change the Amazon Web Services Region, use the Region selector in the upper-right corner of the page.
3. In the navigation pane, choose **Customer managed keys**. (You cannot manage the tags of an Amazon managed key)
4. You can use the table filter to display only KMS keys with particular tags. For details, see [View tags using the Amazon KMS console](#).
5. Select the check box next to the alias of a KMS key.
6. Choose **Key actions, Add or edit tags**.

7. On the details page for KMS key, choose the **Tags** tab.
 - To create your first tag, choose **Create tag**, type a tag key (required) and tag value (optional), and then choose **Save**.

If you leave the tag value blank, the actual tag value is a null or empty string.
 - To add a tag, choose **Edit**, choose **Add tag**, type a tag key and tag value, and then choose **Save**.
8. To save your changes, choose **Save changes**.

Using the Amazon KMS API

The [TagResource](#) operation adds one or more tags to a KMS key. You cannot use this operation to add tags in a different Amazon Web Services account. You can also use the TagResource operation to edit existing tags. For more information, see [the section called “Edit tags”](#).

To add a tag, specify a new tag key and a tag value. Each tag on a KMS key must have a different tag key. The tag value can be a null or empty string.

For example, the following command adds **Purpose** and **Department** tags to an example KMS key.

```
$ aws kms tag-resource \  
    --key-id 1234abcd-12ab-34cd-56ef-1234567890ab \  
    --tags TagKey=Purpose,TagValue=Pretest TagKey=Department,TagValue=Finance
```

When this command is successful, it does not return any output. To view the tags on a KMS key, use the [ListResourceTags](#) operation.

Edit tags associated with a KMS key

Tags help identify and organize your Amazon resources. You can edit the tags associated with your customer managed KMS keys in the Amazon KMS console or by using the [TagResource](#) operation. You cannot edit the tags of an Amazon managed key.

The following procedures demonstrate how to edit the tags associated with a KMS key. The Amazon KMS API examples use the [Amazon Command Line Interface \(Amazon CLI\)](#), but you can use any supported programming language.

Using the Amazon KMS console

1. Sign in to the Amazon Web Services Management Console and open the Amazon Key Management Service (Amazon KMS) console at <https://console.amazonaws.cn/kms>.
2. To change the Amazon Web Services Region, use the Region selector in the upper-right corner of the page.
3. In the navigation pane, choose **Customer managed keys**. (You cannot edit the tags of an Amazon managed key)
4. You can use the table filter to display only KMS keys with particular tags. For details, see [View tags using the Amazon KMS console](#).
5. Select the check box next to the alias of a KMS key.
6. Choose **Key actions, Add or edit tags**.
7. On the details page for KMS key, choose the **Tags** tab.
 - To change the name or value of a tag, choose **Edit**, make your changes, and then choose **Save**.
8. To save your changes, choose **Save changes**.

Using the Amazon KMS API

The [TagResource](#) operation add one or more tags to a customer managed key;. However, you can also use **TagResource** to change the tag value of an existing tag. You cannot use this operation to add or edit tags in a different Amazon Web Services account.

To edit a tag, specify an existing tag key and a new tag value. Each tag on a KMS key must have a different tag key. The tag value can be a null or empty string.

For example, this command changes the value of the Purpose tag from Pretest to Test.

```
$ aws kms tag-resource \  
    --key-id 1234abcd-12ab-34cd-56ef-1234567890ab \  
    --tags TagKey=Purpose,TagValue=Test
```

Remove tags associated with a KMS key

Tags help identify and organize your Amazon resources. You can remove the tags associated with your customer managed KMS keys in the Amazon KMS console or by using the [UntagResource](#) operation. You cannot edit or remove the tags of an Amazon managed key.

The following procedures demonstrate how to remove tags from a KMS key. The Amazon KMS API examples use the [Amazon Command Line Interface \(Amazon CLI\)](#), but you can use any supported programming language.

Using the Amazon KMS console

1. Sign in to the Amazon Web Services Management Console and open the Amazon Key Management Service (Amazon KMS) console at <https://console.amazonaws.cn/kms>.
2. To change the Amazon Web Services Region, use the Region selector in the upper-right corner of the page.
3. In the navigation pane, choose **Customer managed keys**. (You cannot manage the tags of an Amazon managed key)
4. You can use the table filter to display only KMS keys with particular tags. For details, see [View tags using the Amazon KMS console](#).
5. Select the check box next to the alias of a KMS key.
6. Choose **Key actions, Add or edit tags**.
7. On the details page for KMS key, choose the **Tags** tab.
 - To delete a tag, choose **Edit**. On the tag row, choose **Remove**, and then choose **Save**.
8. To save your changes, choose **Save changes**.

Using the Amazon KMS API

The [UntagResource](#) operation deletes tags from a KMS key. To identify the tags to delete, specify the tag keys. You cannot use this operation to delete tags from KMS keys a different Amazon Web Services account.

When it succeeds, the `UntagResource` operation doesn't return any output. Also, if the specified tag key isn't found on the KMS key, it doesn't throw an exception or return a response. To confirm that the operation worked, use the [ListResourceTags](#) operation.

For example, this command deletes the **Purpose** tag and its value from the specified KMS key.

```
$ aws kms untag-resource --key-id 1234abcd-12ab-34cd-56ef-1234567890ab --tag-keys Purpose
```

View tags associated with a KMS key

Tags help identify and organize your Amazon resources. You can view the tags associated with your customer managed KMS keys in the Amazon KMS console or by using the [ListResourceTags](#) operation.

The following procedures demonstrate how to find the tags associated with a specific KMS key. The Amazon KMS API examples use the [Amazon Command Line Interface \(Amazon CLI\)](#), but you can use any supported programming language.

Using the Amazon KMS console

1. Sign in to the Amazon Web Services Management Console and open the Amazon Key Management Service (Amazon KMS) console at <https://console.amazonaws.cn/kms>.
2. To change the Amazon Web Services Region, use the Region selector in the upper-right corner of the page.
3. In the navigation pane, choose **Customer managed keys**. (You cannot manage the tags of an Amazon managed key)
4. You can use the table filter to display only KMS keys with particular tags.

To display only KMS keys with a particular tag, choose the filter box, choose the tag key, and then choose from among the actual tag values. You can also type all or part of the tag value.

The resulting table displays all KMS keys with the chosen tag. However, it doesn't display the tag. To see the tag, choose the key ID or alias of the KMS key and on its detail page, choose the **Tags** tab. The tabs appear below the **General configuration** section.

This filter requires both the tag key and tag value. It won't find KMS keys by typing only the tag key or only its value. To filter tags by all or part of the tag key or value, use the [ListResourceTags](#) operation to get tagged KMS keys, then use the filtering features of your programming language.

5. Select the check box next to the alias of a KMS key.

6. Choose **Key actions, Add or edit tags**.
7. On the details page for KMS key, choose the **Tags** tab.

Using the Amazon KMS API

The [ListResourceTags](#) operation gets the tags for a KMS key. The `KeyId` parameter is required. You cannot use this operation to view the tags on KMS keys in a different Amazon Web Services account.

For example, the following command gets the tags for an example KMS key.

```
$ aws kms list-resource-tags --key-id 1234abcd-12ab-34cd-56ef-1234567890ab

{"Truncated": false,
 "Tags": [
   {
     "TagKey": "Project",
     "TagValue": "Alpha"
   },
   {
     "TagKey": "Purpose",
     "TagValue": "Test"
   },
   {
     "TagKey": "Department",
     "TagValue": "Finance"
   }
 ]
}
```

Use tags to control access to KMS keys

You can control access to Amazon KMS keys based on the tags on the KMS key. For example, you can write an IAM policy that allows principals to enable and disable only the KMS keys that have a particular tag. Or you can use an IAM policy to prevent principals from using KMS keys in cryptographic operations unless the KMS key has a particular tag.

This feature is part of Amazon KMS support for [attribute-based access control](#) (ABAC). For information about using tags to control access to Amazon resources, see [What is ABAC for](#)

[Amazon?](#) and [Controlling Access to Amazon Resources Using Resource Tags](#) in the *IAM User Guide*. For help resolving access issues related to ABAC, see [Troubleshooting ABAC for Amazon KMS](#).

Note

It might take up to five minutes for tag and alias changes to affect KMS key authorization. Recent changes might be visible in API operations before they affect authorization.

Amazon KMS supports the [aws:ResourceTag/tag-key global condition context key](#), which lets you control access to KMS keys based on the tags on the KMS key. Because multiple KMS keys can have the same tag, this feature lets you apply the permission to a select set of KMS keys. You can also easily change the KMS keys in the set by changing their tags.

In Amazon KMS, the `aws:ResourceTag/tag-key` condition key is supported only in IAM policies. It isn't supported in key policies, which apply only to one KMS key, or on operations that don't use a particular KMS key, such as the [ListKeys](#) or [ListAliases](#) operations.

Controlling access with tags provides a simple, scalable, and flexible way to manage permissions. However, if not properly designed and managed, it can allow or deny access to your KMS keys inadvertently. If you are using tags to control access, consider the following practices.

- Use tags to reinforce the best practice of [least privileged access](#). Give IAM principals only the permissions they need on only the KMS keys they must use or manage. For example, use tags to label the KMS keys used for a project. Then give the project team permission to use only KMS keys with the project tag.
- Be cautious about giving principals the `kms:TagResource` and `kms:UntagResource` permissions that let them add, edit, and delete tags. When you use tags to control access to KMS keys, changing a tag can give principals permission to use KMS keys that they didn't otherwise have permission to use. It can also deny access to KMS keys that other principals require to do their jobs. Key administrators who don't have permission to change key policies or create grants can control access to KMS keys if they have permission to manage tags.

Whenever possible, use a policy condition, such as `aws:RequestTag/tag-key` or `aws:TagKeys` to [limit a principal's tagging permissions](#) to particular tags or tag patterns on particular KMS keys.

- Review the principals in your Amazon Web Services account that currently have tagging and untagging permissions and adjust them, if necessary. For example, the console [default key policy](#)

[for key administrators](#) includes `kms:TagResource` and `kms:UntagResource` permission on that KMS key. IAM policies might allow tag and untag permissions on all KMS keys. For example, the [AWSKeyManagementServicePowerUser](#) managed policy allows principals to tag, untag, and list tags on all KMS keys.

- Before setting a policy that depends on a tag, review the tags on the KMS keys in your Amazon Web Services account. Make sure that your policy applies only to the tags you intend to include. Use [CloudTrail logs](#) and [CloudWatch alarms](#) to alert you to tag changes that might affect access to your KMS keys.
- The tag-based policy conditions use pattern matching; they aren't tied to a particular instance of a tag. A policy that uses tag-based condition keys affects all new and existing tags that match the pattern. If you delete and recreate a tag that matches a policy condition, the condition applies to the new tag, just as it did to the old one.

For example, consider the following IAM policy. It allows the principals to call the [GenerateDataKeyWithoutPlaintext](#) and [Decrypt](#) operations only on KMS keys in your account that are the Asia Pacific (Singapore) Region and have a "Project"="Alpha" tag. You might attach this policy to roles in the example Alpha project.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "IAMPolicyWithResourceTag",
      "Effect": "Allow",
      "Action": [
        "kms:GenerateDataKeyWithoutPlaintext",
        "kms:Decrypt"
      ],
      "Resource": "arn:aws:kms:ap-southeast-1:111122223333:key/*",
      "Condition": {
        "StringEquals": {
          "aws:ResourceTag/Project": "Alpha"
        }
      }
    }
  ]
}
```

The following example IAM policy allows the principals to use any KMS key in the account for certain cryptographic operations. But it prohibits the principals from using these cryptographic operations on KMS keys with a "Type"="Reserved" tag or no "Type" tag.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "IAMAllowCryptographicOperations",
      "Effect": "Allow",
      "Action": [
        "kms:Encrypt",
        "kms:GenerateDataKey*",
        "kms:Decrypt",
        "kms:ReEncrypt*"
      ],
      "Resource": "arn:aws:kms:*:111122223333:key/*"
    },
    {
      "Sid": "IAMDenyOnTag",
      "Effect": "Deny",
      "Action": [
        "kms:Encrypt",
        "kms:GenerateDataKey*",
        "kms:Decrypt",
        "kms:ReEncrypt*"
      ],
      "Resource": "arn:aws:kms:*:111122223333:key/*",
      "Condition": {
        "StringEquals": {
          "aws:ResourceTag/Type": "Reserved"
        }
      }
    },
    {
      "Sid": "IAMDenyNoTag",
      "Effect": "Deny",
      "Action": [
        "kms:Encrypt",
        "kms:GenerateDataKey*",
        "kms:Decrypt",
        "kms:ReEncrypt*"
      ],
    },
  ]
}
```

```
    "Resource": "arn:aws:kms:*:111122223333:key/*",
    "Condition": {
      "Null": {
        "aws:ResourceTag/Type": "true"
      }
    }
  ]
}
```

Key stores

A *key store* is a secure location for storing and using cryptographic keys. The default key store in Amazon KMS also supports methods for generating and managing the keys that it stores. By default, the cryptographic key material for the Amazon KMS keys that you create in Amazon KMS is generated in and protected by hardware security modules (HSMs) that are [FIPS 140-3 Cryptographic Module Validation Program](#). Key material for your KMS keys never leave the HSMs unencrypted.

Amazon KMS supports several types of key stores to protect your key material when using Amazon KMS to create and manage your encryption keys. All of the key store options supplied by Amazon KMS are continually validated under FIPS 140-3 at Security Level 3 and are designed to prevent anyone, including Amazon operators, from accessing your plaintext keys or using them without your permission.

Amazon KMS standard key store

By default, a KMS key is created using the standard Amazon KMS HSM. This HSM type can be thought of as a multi-tenant fleet of HSMs that allows for the most scalable, lowest cost and easiest key store to manage from your perspective. If you are creating a KMS key for use within one or more Amazon Web Services services so that service can encrypt your data on your behalf, you will create a symmetric key. If you are using a KMS key for your own application design, you may choose to create a symmetric encryption key, asymmetric key, or HMAC key.

In the standard key store option, Amazon KMS creates your key, then encrypts it under keys that the service manages internally. Multiple copies of encrypted versions of your keys are then stored in systems that are designed for durability. Generating and protecting your key material in the standard key store type lets you take full advantage of the scalability, availability, and durability of Amazon KMS with the lowest operational burden and cost of the Amazon key stores.

Amazon KMS standard key store with imported key material

Instead of asking Amazon KMS to both generate and store the only copies of a given key, you can choose to import key material into Amazon KMS, allowing you to generate your own 256-bit symmetric encryption key, RSA or elliptic curve (ECC) key, or Hash-Based Message Authentication Code (HMAC) key, and apply it to a KMS key identifier (keyId). This is sometimes referred to as

bring your own key (BYOK). Imported key material from your local key management system must be protected by using a public key issued by Amazon KMS, a supported cryptographic wrapping algorithm, and a time-based import token provided by Amazon KMS. This process verifies that your encrypted, imported key can only ever be decrypted by an Amazon KMS HSM once it has left your environment.

Imported key material may be useful if you have specific requirements around the system that generates keys, or want a copy of your key outside of Amazon as a backup. Note that you are responsible for an imported key material's overall availability and durability. While Amazon KMS has a copy of your imported key and will keep highly available while you need it, imported keys offer a special API for deletion – `DeleteImportedKeyMaterial`. This API will immediately delete all copies of the imported key material that Amazon KMS has, with no option for Amazon to recover the key. In addition, you can set an expiration time on an imported key, after which the key will be unusable. To make the key useful again in Amazon KMS, you will have to re-import the key material and assign it to the same keyId. This deletion action for imported keys is different than standard keys that Amazon KMS generates and stored for you on your behalf. In the standard case, the key deletion process has a mandatory waiting period where a key scheduled for deletion is first blocked from usage. This action allows you to see access denied errors in logs from any application or Amazon service that might need that key to access data. If you see such access requests, you can choose to cancel the scheduled deletion and re-enable the key. After a configurable waiting period (between 7 and 30 days), only then will KMS actually delete the key material, the keyId and all metadata associated with the key. For more information about availability and durability, see [Protecting imported key material](#) in the *Amazon KMS Developer Guide*.

There are some additional limitations with imported key material to be aware of. Since Amazon KMS cannot generate new key material, there is no way to configure automatic rotation of imported keys. You will need to create a new KMS key with a new keyId, then import new key material to achieve an effective rotation. Also, ciphertexts created in Amazon KMS under an imported symmetric key cannot be easily decrypted using your local copy of the key outside of Amazon. This is because the authenticated encryption format used by Amazon KMS appends additional metadata to the ciphertext to provide assurances during the decryption operation that the ciphertext was created by the expected KMS key under a previous encrypt operation. Most external cryptographic systems won't understand how to parse this metadata to gain access to the raw ciphertext to be able to use their copy of a symmetric key. Ciphertexts created under imported asymmetric keys (e.g. RSA or ECC) can be used outside of Amazon KMS with the matching (public or private) portion of the key because there is no additional metadata added by Amazon KMS to the ciphertext.

Amazon KMS custom key stores

However, if you require even more control of the HSMs, you can create a custom key store.

A *custom key store* is a key store within Amazon KMS that is backed by a key manager outside of Amazon KMS, which you own and manage. Custom key stores combine the convenient and comprehensive key management interface of Amazon KMS with the ability to own and control the key material and cryptographic operations. When you use a KMS key in a custom key store, the cryptographic operations are performed by your key manager using your cryptographic keys. As a result, you assume more responsibility for the availability and durability of cryptographic keys, and for the operation of the HSMs.

Owning your HSMs may be useful to help meet certain regulatory requirements that don't yet allow multi-tenant web services like the standard KMS key store to hold your cryptographic keys. Custom key stores are not more secure than KMS key store that use Amazon-managed HSMs, but they have different (and higher) management and cost implications. As a result, you assume more responsibility for the availability and durability of cryptographic keys and for the operation of the HSMs. Regardless of whether you use the standard key store with Amazon KMS HSMs or a custom key store, the service is designed so that no one, including Amazon employees, can retrieve your plaintext keys or use them without your permission. Amazon KMS supports two types of custom key stores, Amazon CloudHSM key stores and external key stores.

Unsupported features

Amazon KMS does not support the following features in custom key stores.

- [Asymmetric KMS keys](#)
- [HMAC KMS keys](#)
- [KMS keys with imported key material](#)
- [Automatic key rotation](#)
- [Multi-Region keys](#)

Amazon CloudHSM key store

You can create a KMS key in an [Amazon CloudHSM](#) key store, where root user keys are generated, stored and used in a Amazon CloudHSM cluster that you own and manage. Requests to Amazon KMS to use a key for some cryptographic operation are forwarded to your Amazon CloudHSM cluster to perform the operation. While a Amazon CloudHSM cluster is hosted by Amazon, it is

a single-tenant solution that is directly managed and operated by you. You own much of the availability and performance of KMS keys in a Amazon CloudHSM cluster. To see if a Amazon CloudHSM custom key store is a good fit for your requirements, read [Are Amazon KMS custom key stores right for you?](#) on the Amazon security blog.

External key store

You can configure Amazon KMS to use an External Key Store (XKS), where root user keys are generated, stored and used in a key management system outside the Amazon Web Services Cloud. Requests to Amazon KMS to use a key for some cryptographic operation are forwarded to your externally hosted system to perform the operation. Specifically, requests are forwarded to an XKS Proxy in your network, which then forwards the request to whichever cryptographic system you use. The XKS Proxy is an open-source specification that anyone can integrate with. Many commercial key management vendors support the XKS Proxy specification. Because an External Key Store is hosted by you or some third party, you own all of the availability, durability, and performance of the keys in the system. To see if an External Key Store is a good fit for your requirements, read [Announcing Amazon KMS External Key Store \(XKS\)](#) on the Amazon News blog.

Amazon CloudHSM key stores

An Amazon CloudHSM key store is a [custom key store](#) backed by a [Amazon CloudHSM cluster](#). When you create an Amazon KMS key in a custom key store, Amazon KMS generates and stores non-extractable key material for the KMS key in an Amazon CloudHSM cluster that you own and manage. When you use a KMS key in a custom key store, the [cryptographic operations](#) are performed in the HSMs in the cluster. This feature combines the convenience and widespread integration of Amazon KMS with the added control of an Amazon CloudHSM cluster in your Amazon Web Services account.

Amazon KMS provides full console and API support for creating, using, and managing your custom key stores. You can use the KMS keys in your custom key store the same way that you use any KMS key. For example, you can use the KMS keys to generate data keys and encrypt data. You can also use the KMS keys in your custom key store with Amazon services that support customer managed keys.

Do I need a custom key store?

For most users, the default Amazon KMS key store, which is protected by [FIPS 140-3 validated cryptographic modules](#), fulfills their security requirements. There is no need to add an extra layer of maintenance responsibility or a dependency on an additional service.

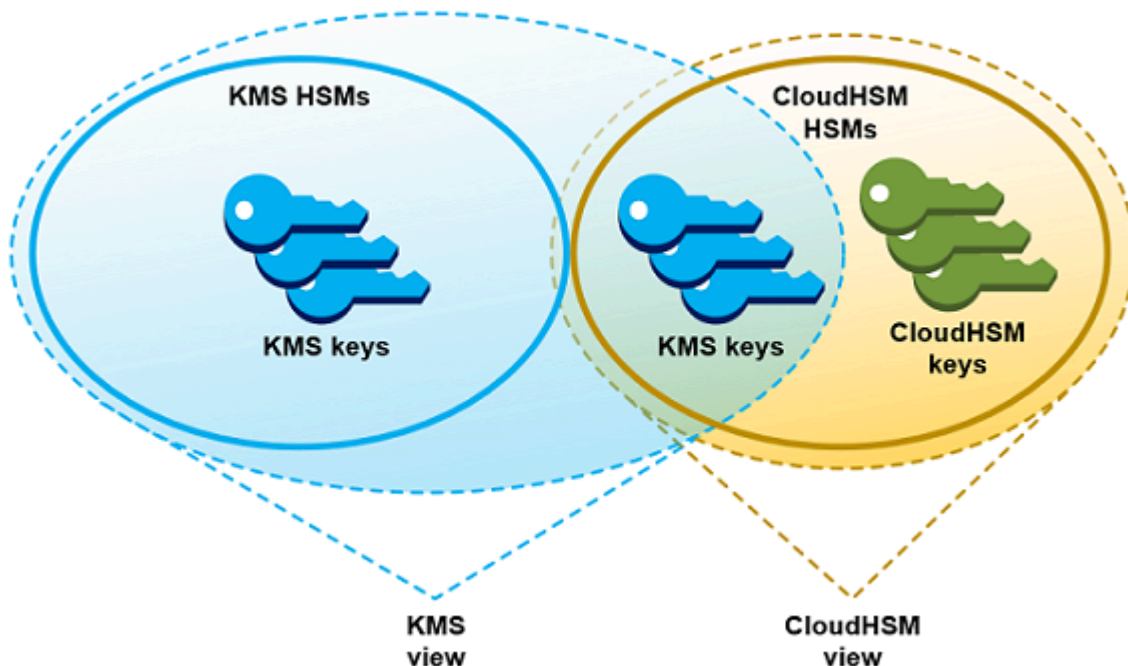
However, you might consider creating a custom key store if your organization has any of the following requirements:

- You have keys that are explicitly required to be protected in a single tenant HSM or in an HSM that you have direct control over.
- You need the ability to immediately remove key material from Amazon KMS.
- You need to be able to audit all use of your keys independently of Amazon KMS or Amazon CloudTrail.

How do custom key stores work?

Each custom key store is associated with an Amazon CloudHSM cluster in your Amazon Web Services account. When you connect the custom key store to its cluster, Amazon KMS creates the network infrastructure to support the connection. Then it logs into the key Amazon CloudHSM client in the cluster using the credentials of a [dedicated crypto user](#) in the cluster.

You create and manage your custom key stores in Amazon KMS and create and manage your HSM clusters in Amazon CloudHSM. When you create Amazon KMS keys in an Amazon KMS custom key store, you view and manage the KMS keys in Amazon KMS. But you can also view and manage their key material in Amazon CloudHSM, just as you would do for other keys in the cluster.



You can [create symmetric encryption KMS keys](#) with key material generated by Amazon KMS in your custom key store. Then use the same techniques to view and manage the KMS keys in your custom key store that you use for KMS keys in the Amazon KMS key store. You can control access with IAM and key policies, create tags and aliases, enable and disable the KMS keys, and schedule key deletion. You can use the KMS keys for [cryptographic operations](#) and use them with Amazon services that integrate with Amazon KMS.

In addition, you have full control over the Amazon CloudHSM cluster, including creating and deleting HSMs and managing backups. You can use the Amazon CloudHSM client and supported software libraries to view, audit, and manage the key material for your KMS keys. While the custom key store is disconnected, Amazon KMS cannot access it, and users cannot use the KMS keys in the custom key store for cryptographic operations. This added layer of control makes custom key stores a powerful solution for organizations that require it.

Where do I start?

To create and manage an Amazon CloudHSM key store, you use features of Amazon KMS and Amazon CloudHSM.

1. Start in Amazon CloudHSM. [Create an active Amazon CloudHSM cluster](#) or select an existing cluster. The cluster must have at least two active HSMs in different Availability Zones. Then create a [dedicated crypto user \(CU\) account](#) in that cluster for Amazon KMS.
2. In Amazon KMS, [create a custom key store](#) that is associated with your selected Amazon CloudHSM cluster. Amazon KMS provides a complete management interface that lets you create, view, edit, and delete your custom key stores.
3. When you're ready to use your custom key store, [connect it to its associated Amazon CloudHSM cluster](#). Amazon KMS creates the network infrastructure that it needs to support the connection. It then logs in to the cluster using the dedicated crypto user account credentials so it can generate and manage key material in the cluster.
4. Now, you can [create symmetric encryption KMS keys in your custom key store](#). Just specify the custom key store when you create the KMS key.

If you get stuck at any point, you can find help in the [Troubleshooting a custom key store](#) topic. If your question is not answered, use the feedback link at the bottom of each page of this guide or post a question on the [Amazon Key Management Service Discussion Forum](#).

Quotas

Amazon KMS allows up to [10 custom key stores](#) in each Amazon Web Services account and Region, including both [Amazon CloudHSM key stores](#) and [external key stores](#), regardless of their connection state. In addition, there are Amazon KMS request quotas on the [use of KMS keys in an Amazon CloudHSM key store](#).

Pricing

For information on the cost of Amazon KMS custom key stores and customer managed keys in a custom key store, see [Amazon Key Management Service pricing](#). For information about the cost of Amazon CloudHSM clusters and HSMs, see [Amazon CloudHSM Pricing](#).

Regions

Amazon KMS supports Amazon CloudHSM key stores in all Amazon Web Services Regions where Amazon KMS is supported, except for Asia Pacific (Melbourne), China (Beijing), China (Ningxia), and Europe (Spain).

Unsupported features

Amazon KMS does not support the following features in custom key stores.

- [Asymmetric KMS keys](#)
- [HMAC KMS keys](#)
- [KMS keys with imported key material](#)
- [Automatic key rotation](#)
- [Multi-Region keys](#)

Amazon CloudHSM key store concepts

This topic explains some of the terms and concepts used in Amazon CloudHSM key stores.

Amazon CloudHSM key store

An *Amazon CloudHSM key store* is a [custom key store](#) associated with an Amazon CloudHSM cluster that you own and manage. Amazon CloudHSM clusters are backed by hardware security modules (HSMs) certified at [FIPS 140-2 or FIPS 140-3 Level 3](#).

When you create a KMS key in your Amazon CloudHSM key store, Amazon KMS generates a 256-bit, persistent, non-exportable Advanced Encryption Standard (AES) symmetric key in the

associated Amazon CloudHSM cluster. This key material never leaves your HSMs unencrypted. When you use a KMS key in an Amazon CloudHSM key store, the cryptographic operations are performed in the HSMs in the cluster.

Amazon CloudHSM key stores combine the convenient and comprehensive key management interface of Amazon KMS with the additional controls provided by an Amazon CloudHSM cluster in your Amazon Web Services account. This integrated feature lets you create, manage, and use KMS keys in Amazon KMS while maintaining full control of the HSMs that store their key material, including managing clusters, HSMs, and backups. You can use the Amazon KMS console and APIs to manage the Amazon CloudHSM key store and its KMS keys. You can also use the Amazon CloudHSM console, APIs, client software, and associated software libraries to manage the associated cluster.

You can [view and manage](#) your Amazon CloudHSM key store, [edit its properties](#), and [connect](#) and [disconnect](#) it from its associated Amazon CloudHSM cluster. If you need to [delete an Amazon CloudHSM key store](#), you must first delete the KMS keys in the Amazon CloudHSM key store by scheduling their deletion and waiting until the grace period expires. Deleting the Amazon CloudHSM key store removes the resource from Amazon KMS, but it does not affect your Amazon CloudHSM cluster.

Amazon CloudHSM cluster

Every Amazon CloudHSM key store is associated with one *Amazon CloudHSM cluster*. When you create an Amazon KMS key in your Amazon CloudHSM key store, Amazon KMS creates its key material in the associated cluster. When you use a KMS key in your Amazon CloudHSM key store, the cryptographic operation is performed in the associated cluster.

Each Amazon CloudHSM cluster can be associated with only one Amazon CloudHSM key store. The cluster that you choose cannot be associated with another Amazon CloudHSM key store or share a backup history with a cluster that is associated with another Amazon CloudHSM key store. The cluster must be initialized and active, and it must be in the same Amazon Web Services account and Region as the Amazon CloudHSM key store. You can create a new cluster or use an existing one. Amazon KMS does not need exclusive use of the cluster. To create KMS keys in the Amazon CloudHSM key store, its associated cluster it must contain at least two active HSMs. All other operations require only one HSM.

You specify the Amazon CloudHSM cluster when you create the Amazon CloudHSM key store, and you cannot change it. However, you can substitute any cluster that shares a backup history with the

original cluster. This lets you delete the cluster, if necessary, and replace it with a cluster created from one of its backups. You retain full control of the associated Amazon CloudHSM cluster so you can manage users and keys, create and delete HSMs, and use and manage backups.

When you are ready to use your Amazon CloudHSM key store, you connect it to its associated Amazon CloudHSM cluster. You can connect and disconnect your custom key store at any time. When a custom key store is connected, you can create and use its KMS keys. When it is disconnected, you can view and manage the Amazon CloudHSM key store and its KMS keys. But you cannot create new KMS keys or use the KMS keys in the Amazon CloudHSM key store for cryptographic operations.

kmsuser Crypto user

To create and manage key material in the associated Amazon CloudHSM cluster on your behalf, Amazon KMS uses a dedicated *Amazon CloudHSM [crypto user](#) (CU)* in the cluster named `kmsuser`. The `kmsuser` CU is a standard CU account that is automatically synchronized to all HSMs in the cluster and is saved in cluster backups.

Before you create your Amazon CloudHSM key store, you [create a `kmsuser` CU account](#) in your Amazon CloudHSM cluster using the [user create](#) command in CloudHSM CLI. Then when you [create the Amazon CloudHSM key store](#), you provide the `kmsuser` account password to Amazon KMS. When you [connect the custom key store](#), Amazon KMS logs into the cluster as the `kmsuser` CU and rotates its password. Amazon KMS encrypts your `kmsuser` password before it stores it securely. When the password is rotated, the new password is encrypted and stored in the same way.

Amazon KMS remains logged in as `kmsuser` as long as the Amazon CloudHSM key store is connected. You should not use this CU account for other purposes. However, you retain ultimate control of the `kmsuser` CU account. At any time, you can [find the keys](#) that `kmsuser` owns. If necessary, you can [disconnect the custom key store](#), change the `kmsuser` password, [log into the cluster as `kmsuser`](#), and view and manage the keys that `kmsuser` owns.

For instructions on creating your `kmsuser` CU account, see [Create the `kmsuser` Crypto User](#).

KMS keys in an Amazon CloudHSM key store

You can use the Amazon KMS or Amazon KMS API to create a Amazon KMS keys in an Amazon CloudHSM key store. You use the same technique that you would use on any KMS key. The only difference is that you must identify the Amazon CloudHSM key store and specify that the origin of the key material is the Amazon CloudHSM cluster.

When you [create a KMS key in an Amazon CloudHSM key store](#), Amazon KMS creates the KMS key in Amazon KMS and it generates a 256-bit, persistent, non-exportable Advanced Encryption Standard (AES) symmetric key material in its associated cluster. When you use the Amazon KMS key in a cryptographic operation, the operation is performed in the Amazon CloudHSM cluster using the cluster-based AES key. Although Amazon CloudHSM supports symmetric and asymmetric keys of different types, Amazon CloudHSM key stores support only AES symmetric encryption keys.

You can view the KMS keys in an Amazon CloudHSM key store in the Amazon KMS console, and use the console options to display the custom key store ID. You can also use the [DescribeKey](#) operation to find the Amazon CloudHSM key store ID and Amazon CloudHSM cluster ID.

The KMS keys in an Amazon CloudHSM key store work just like any KMS keys in Amazon KMS. Authorized users need the same permissions to use and manage the KMS keys. You use the same console procedures and API operations to view and manage the KMS keys in an Amazon CloudHSM key store. These include enabling and disabling KMS keys, creating and using tags and aliases, and setting and changing IAM and key policies. You can use the KMS keys in an Amazon CloudHSM key store for cryptographic operations, and use them with [integrated Amazon services](#) that support the use of customer managed keys. However, you cannot enable [automatic key rotation](#) or [import key material](#) into a KMS key in an Amazon CloudHSM key store.

You also use the same process to [schedule deletion](#) of a KMS key in an Amazon CloudHSM key store. After the waiting period expires, Amazon KMS deletes the KMS key from KMS. Then it makes a best effort to delete the key material for the KMS key from the associated Amazon CloudHSM cluster. However, you might need to manually [delete the orphaned key material](#) from the cluster and its backups.

Control access to your Amazon CloudHSM key store

You use IAM policies to control access to your Amazon CloudHSM key store and your Amazon CloudHSM cluster. You can use key policies, IAM policies, and grants to control access to the Amazon KMS keys in your Amazon CloudHSM key store. We recommend that you provide users, groups, and roles only the permissions that they require for the tasks that they are likely to perform.

To support your Amazon CloudHSM key stores, Amazon KMS needs permission to get information about your Amazon CloudHSM clusters. It also needs permission to create the network infrastructure that connects your Amazon CloudHSM key store to its Amazon CloudHSM cluster. To get these permissions, Amazon KMS creates the

AWSServiceRoleForKeyManagementServiceCustomKeyStores service-linked role in your Amazon Web Services account. For more information, see [Authorizing Amazon KMS to manage Amazon CloudHSM and Amazon EC2 resources](#).

When designing your Amazon CloudHSM key store, be sure that the principals who use and manage it have only the permissions that they require. The following list describes the minimum permissions required for Amazon CloudHSM key store managers and users.

- Principals who create and manage your Amazon CloudHSM key store require the following permission to use the Amazon CloudHSM key store API operations.
 - `cloudhsm:DescribeClusters`
 - `kms:CreateCustomKeyStore`
 - `kms:ConnectCustomKeyStore`
 - `kms>DeleteCustomKeyStore`
 - `kms:DescribeCustomKeyStores`
 - `kms:DisconnectCustomKeyStore`
 - `kms:UpdateCustomKeyStore`
 - `iam:CreateServiceLinkedRole`
- Principals who create and manage the Amazon CloudHSM cluster that is associated with your Amazon CloudHSM key store need permission to create and initialize an Amazon CloudHSM cluster. This includes permission to create or use an Amazon Virtual Private Cloud (VPC), create subnets, and create an Amazon EC2 instance. They might also need to create and delete HSMs, and manage backups. For lists of the required permissions, see [Identity and access management for Amazon CloudHSM](#) in the *Amazon CloudHSM User Guide*.
- Principals who create and manage Amazon KMS keys in your Amazon CloudHSM key store require [the same permissions](#) as those who create and manage any KMS key in Amazon KMS. The [default key policy](#) for a KMS key in an Amazon CloudHSM key store is identical to the default key policy for KMS keys in Amazon KMS. [Attribute-based access control](#) (ABAC), which uses tags and aliases to control access to KMS keys, is also effective on KMS keys in Amazon CloudHSM key stores.
- Principals who use the KMS keys in your Amazon CloudHSM key store for [cryptographic operations](#) need permission to perform the cryptographic operation with the KMS key, such as [kms:Decrypt](#). You can provide these permissions in a key policy, IAM policy. But, they do not need any additional permissions to use a KMS key in an Amazon CloudHSM key store.

Create an Amazon CloudHSM key store

You can create one or several Amazon CloudHSM key stores in your account. Each Amazon CloudHSM key store is associated with one Amazon CloudHSM cluster in the same Amazon Web Services account and Region. Before you create your Amazon CloudHSM key store, you need to [assemble the prerequisites](#). Then, before you can use your Amazon CloudHSM key store, you must [connect it](#) to its Amazon CloudHSM cluster.

Notes

If you try to create an Amazon CloudHSM key store with all of the same property values as an existing *disconnected* Amazon CloudHSM key store, Amazon KMS does not create a new Amazon CloudHSM key store, and it does not throw an exception or display an error. Instead, Amazon KMS recognizes the duplicate as the likely consequence of a retry, and it returns the ID of the existing Amazon CloudHSM key store.

You do not have to connect your Amazon CloudHSM key store immediately. You can leave it in a disconnected state until you are ready to use it. However, to verify that it is configured properly, you might want to [connect it](#), [view its connection state](#), and then [disconnect it](#).

Topics

- [Assemble the prerequisites](#)
- [Create a new Amazon CloudHSM key store](#)

Assemble the prerequisites

Each Amazon CloudHSM key store is backed by an Amazon CloudHSM cluster. To create an Amazon CloudHSM key store, you must specify an active Amazon CloudHSM cluster that is not already associated with another key store. You also need to create a dedicated crypto user (CU) in the cluster's HSMs that Amazon KMS can use to create and manage keys on your behalf.

Before you create an Amazon CloudHSM key store, do the following:

Select an Amazon CloudHSM cluster

Every Amazon CloudHSM key store is [associated with exactly one Amazon CloudHSM cluster](#). When you create Amazon KMS keys in your Amazon CloudHSM key store, Amazon KMS creates the KMS key metadata, such as an ID and Amazon Resource Name (ARN) in Amazon KMS.

It then creates the key material in the HSMs of the associated cluster. You can [create a new Amazon CloudHSM](#) cluster or use an existing one. Amazon KMS does not require exclusive access to the cluster.

The Amazon CloudHSM cluster that you select is permanently associated with the Amazon CloudHSM key store. After you create the Amazon CloudHSM key store, you can [change the cluster ID](#) of the associated cluster, but the cluster that you specify must share a backup history with the original cluster. To use an unrelated cluster, you need to create a new Amazon CloudHSM key store.

The Amazon CloudHSM cluster that you select must have the following characteristics:

- **The cluster must be active.**

You must create the cluster, initialize it, install the Amazon CloudHSM client software for your platform, and then activate the cluster. For detailed instructions, see [Getting started with Amazon CloudHSM](#) in the *Amazon CloudHSM User Guide*.

- **The cluster must be in the same account and Region** as the Amazon CloudHSM key store. You cannot associate an Amazon CloudHSM key store in one Region with a cluster in a different Region. To create a key infrastructure in multiple Regions, you must create Amazon CloudHSM key stores and clusters in each Region.
- **The cluster cannot be associated with another custom key store** in the same account and Region. Each Amazon CloudHSM key store in the account and Region must be associated with a different Amazon CloudHSM cluster. You cannot specify a cluster that is already associated with a custom key store or a cluster that shares a backup history with an associated cluster. Clusters that share a backup history have the same cluster certificate. To view the cluster certificate of a cluster, use the Amazon CloudHSM console or the [DescribeClusters](#) operation.

If you [back up an Amazon CloudHSM cluster to a different Region](#), it is considered to be different cluster, and you can associate the backup with a custom key store in its Region. However, KMS keys in the two custom key stores are not interoperable, even if they have the same backing key. Amazon KMS binds metadata to the ciphertext so it can be decrypted only by the KMS key that encrypted it.

- The cluster must be configured with [private subnets](#) in **at least two Availability Zones** in the Region. Because Amazon CloudHSM is not supported in all Availability Zones, we recommend that you create private subnets in all Availability Zones in the region. You cannot reconfigure the subnets for an existing cluster, but you can [create a cluster from a backup](#) with different subnets in the cluster configuration.

⚠ Important

After you create your Amazon CloudHSM key store, do not delete any of the private subnets configured for its Amazon CloudHSM cluster. If Amazon KMS cannot find all of the subnets in the cluster configuration, attempts to [connect to the custom key store](#) fail with a SUBNET_NOT_FOUND connection error state. For details, see [How to fix a connection failure](#).

- The [security group for the cluster](#) (cloudhsm-cluster-*<cluster-id>*-sg) must include inbound rules and outbound rules that allow TCP traffic on ports 2223-2225. The **Source** in the inbound rules and the **Destination** in the outbound rules must match the security group ID. These rules are set by default when you create the cluster. Do not delete or change them.
- **The cluster must contain at least two active HSMs** in different Availability Zones. To verify the number of HSMs, use the Amazon CloudHSM console or the [DescribeClusters](#) operation. If necessary, you can [add an HSM](#).

Find the trust anchor certificate

When you create a custom key store, you must upload the trust anchor certificate for the Amazon CloudHSM cluster to Amazon KMS. Amazon KMS needs the trust anchor certificate to connect the Amazon CloudHSM key store to its associated Amazon CloudHSM cluster.

Every active Amazon CloudHSM cluster has a *trust anchor certificate*. When you [initialize the cluster](#), you generate this certificate, save it in the customerCA.crt file, and copy it to hosts that connect to the cluster.

Create the kmsuser crypto user for Amazon KMS

To administer your Amazon CloudHSM key store, Amazon KMS logs into the [kmsuser crypto user](#) (CU) account in the selected cluster. Before you create your Amazon CloudHSM key store, you must create the kmsuser CU. Then when you create your Amazon CloudHSM key store, you provide the password for kmsuser to Amazon KMS. Whenever you connect the Amazon CloudHSM key store to its associated Amazon CloudHSM cluster, Amazon KMS logs in as the kmsuser and rotates the kmsuser password

⚠ Important

Do not specify the 2FA option when you create the kmsuser CU. If you do, Amazon KMS cannot log in and your Amazon CloudHSM key store cannot be connected to this

Amazon CloudHSM cluster. Once you specify 2FA, you cannot undo it. Instead, you must delete the CU and recreate it.

Notes

The following procedures use the Amazon CloudHSM Client SDK 5 command line tool, [CloudHSM CLI](#). The CloudHSM CLI replaces `key-handle` with `key-reference`. On January 1, 2025, Amazon CloudHSM will end support for the Client SDK 3 command line tools, the CloudHSM Management Utility (CMU) and the Key Management Utility (KMU). For more information on the differences between the Client SDK 3 command line tools and the Client SDK 5 command line tool, see [Migrate from Client SDK 3 CMU and KMU to Client SDK 5 CloudHSM CLI](#) in the *Amazon CloudHSM User Guide*.

1. Follow the getting started procedures as described in the [Getting started with CloudHSM Command Line Interface \(CLI\)](#) topic of the *Amazon CloudHSM User Guide*.
2. Use the [user create](#) command to create a CU named `kmsuser`.

The password must consist of 7-32 alphanumeric characters. It is case-sensitive and cannot contain any special characters.

The following example command creates a `kmsuser` CU.

```
aws-cloudhsm > user create --username kmsuser --role crypto-user
Enter password:
Confirm password:
{
  "error_code": 0,
  "data": {
    "username": "kmsuser",
    "role": "crypto-user"
  }
}
```

Create a new Amazon CloudHSM key store

After [assembling the prerequisites](#), you can create a new Amazon CloudHSM key store in the Amazon KMS console or by using the [CreateCustomKeyStore](#) operation.

Using the Amazon KMS console

When you create an Amazon CloudHSM key store in the Amazon Web Services Management Console, you can add and create the [prerequisites](#) as part of your workflow. However, the process is quicker when you have assembled them in advance.

1. Sign in to the Amazon Web Services Management Console and open the Amazon Key Management Service (Amazon KMS) console at <https://console.amazonaws.cn/kms>.
2. To change the Amazon Web Services Region, use the Region selector in the upper-right corner of the page.
3. In the navigation pane, choose **Custom key stores, Amazon CloudHSM key stores**.
4. Choose **Create a key store**.
5. Enter a friendly name for the custom key store. The name must be unique among all custom key stores in your account.

Important

Do not include confidential or sensitive information in this field. This field may be displayed in plaintext in CloudTrail logs and other output.

6. Select [an Amazon CloudHSM cluster](#) for the Amazon CloudHSM key store. Or, to create a new Amazon CloudHSM cluster, choose the **Create an Amazon CloudHSM cluster** link.

The menu displays the Amazon CloudHSM clusters in your account and region that are not already associated with an Amazon CloudHSM key store. The cluster must [fulfill the requirements](#) for association with a custom key store.

7. Choose **Choose file**, and then upload the trust anchor certificate for the Amazon CloudHSM cluster that you chose. This is the `customerCA.crt` file that you created when you [initialized the cluster](#).
8. Enter the password of [the kmsuser crypto user](#) (CU) that you created in the selected cluster.
9. Choose **Create**.

When the procedure is successful, the new Amazon CloudHSM key store appears in the list of Amazon CloudHSM key stores in the account and Region. If it is unsuccessful, an error message appears that describes the problem and provides help on how to fix it. If you need more help, see [Troubleshooting a custom key store](#).

If you try to create an Amazon CloudHSM key store with all of the same property values as an existing *disconnected* Amazon CloudHSM key store, Amazon KMS does not create a new Amazon CloudHSM key store, and it does not throw an exception or display an error. Instead, Amazon KMS recognizes the duplicate as the likely consequence of a retry, and it returns the ID of the existing Amazon CloudHSM key store.

Next: New Amazon CloudHSM key stores are not automatically connected. Before you can create Amazon KMS keys in the Amazon CloudHSM key store, you must [connect the custom key store](#) to its associated Amazon CloudHSM cluster.

Using the Amazon KMS API

You can use the [CreateCustomKeyStore](#) operation to create a new Amazon CloudHSM key store that is associated with an Amazon CloudHSM cluster in the account and Region. These examples use the Amazon Command Line Interface (Amazon CLI), but you can use any supported programming language.

The `CreateCustomKeyStore` operation requires the following parameter values.

- `CustomKeyName` – A friendly name for the custom key store that is unique in the account.

Important

Do not include confidential or sensitive information in this field. This field may be displayed in plaintext in CloudTrail logs and other output.

- `CloudHsmClusterId` – The cluster ID of an Amazon CloudHSM cluster that [fulfills the requirements](#) for an Amazon CloudHSM key store.
- `KeyStorePassword` – The password of `kmsuser` CU account in the specified cluster.
- `TrustAnchorCertificate` – The content of the `customerCA.crt` file that you created when you [initialized the cluster](#).

The following example uses a fictitious cluster ID. Before running the command, replace it with a valid cluster ID.

```
$ aws kms create-custom-key-store
  --custom-key-store-name ExampleCloudHSMKeyStore \
  --cloud-hsm-cluster-id cluster-1a23b4cdefg \
  --key-store-password kmsPswd \
  --trust-anchor-certificate <certificate-goes-here>
```

If you are using the Amazon CLI, you can specify the trust anchor certificate file, instead of its contents. In the following example, the `customerCA.crt` file is in the root directory.

```
$ aws kms create-custom-key-store
  --custom-key-store-name ExampleCloudHSMKeyStore \
  --cloud-hsm-cluster-id cluster-1a23b4cdefg \
  --key-store-password kmsPswd \
  --trust-anchor-certificate file://customerCA.crt
```

When the operation is successful, `CreateCustomKeyStore` returns the custom key store ID, as shown in the following example response.

```
{
  "CustomKeyStoreId": cks-1234567890abcdef0
}
```

If the operation fails, correct the error indicated by the exception, and try again. For additional help, see [Troubleshooting a custom key store](#).

If you try to create an Amazon CloudHSM key store with all of the same property values as an existing *disconnected* Amazon CloudHSM key store, Amazon KMS does not create a new Amazon CloudHSM key store, and it does not throw an exception or display an error. Instead, Amazon KMS recognizes the duplicate as the likely consequence of a retry, and it returns the ID of the existing Amazon CloudHSM key store.

Next: To use the Amazon CloudHSM key store, [connect it to its Amazon CloudHSM cluster](#).

View an Amazon CloudHSM key store

You can view the Amazon CloudHSM key stores in each account and Region by using the Amazon KMS console or the [DescribeCustomKeyStores](#) operation.

Using the Amazon KMS console

When you view the Amazon CloudHSM key stores in the Amazon Web Services Management Console, you can see the following:

- The custom key store name and ID
- The ID of associated Amazon CloudHSM cluster
- The number of HSMs in the cluster
- The current connection state

A connection state (**Status**) value of **Disconnected** indicates that the custom key store is new and has never been connected, or it was intentionally [disconnected from its Amazon CloudHSM cluster](#). However, if your attempts to use a KMS key in a connected custom key store fail, that might indicate a problem with the custom key store or its Amazon CloudHSM cluster. For help, see [How to fix a failing KMS key](#).

To view the Amazon CloudHSM key stores in a given account and Region, use the following procedure.

1. Sign in to the Amazon Web Services Management Console and open the Amazon Key Management Service (Amazon KMS) console at <https://console.amazonaws.cn/kms>.
2. To change the Amazon Web Services Region, use the Region selector in the upper-right corner of the page.
3. In the navigation pane, choose **Custom key stores, Amazon CloudHSM key stores**.

To customize the display, click the gear icon that appears below the **Create key store** button.

Using the Amazon KMS API

To view your Amazon CloudHSM key stores, use the [DescribeCustomKeyStores](#) operation. By default, this operation returns all custom key stores in the account and Region. But you can use either the `CustomKeyId` or `CustomKeyName` parameter (but not both) to limit the output to a particular custom key store. For Amazon CloudHSM key stores, the output consists of the custom key store ID and name, the custom key store type, the ID of the associated Amazon CloudHSM cluster, and the connection state. If the connection state indicates an error, the output also includes an error code that describes the reason for the error.

The examples in this section use the [Amazon Command Line Interface \(Amazon CLI\)](#), but you can use any supported programming language.

For example, the following command returns all custom key stores in the account and Region. You can use the `Limit` and `Marker` parameters to page through the custom key stores in the output.

```
$ aws kms describe-custom-key-stores
```

The following example command uses the `CustomKeyStoreName` parameter to get only the custom key store with the `ExampleCloudHSMKeyStore` friendly name. You can use either the `CustomKeyStoreName` or `CustomKeyStoreId` parameter (but not both) in each command.

The following example output represents an Amazon CloudHSM key store that is connected to its Amazon CloudHSM cluster.

Note

The `CustomKeyStoreType` field was added to the `DescribeCustomKeyStores` response to distinguish Amazon CloudHSM key stores from external key stores.

```
$ aws kms describe-custom-key-stores --custom-key-store-name ExampleCloudHSMKeyStore
{
  "CustomKeyStores": [
    {
      "CloudHsmClusterId": "cluster-1a23b4cdefg",
      "ConnectionState": "CONNECTED",
      "CreationDate": "1.499288695918E9",
      "CustomKeyStoreId": "cks-1234567890abcdef0",
      "CustomKeyStoreName": "ExampleCloudHSMKeyStore",
      "CustomKeyStoreType": "AWS_CLOUDHSM",
      "TrustAnchorCertificate": "<certificate appears here>"
    }
  ]
}
```

A `ConnectionState` of `Disconnected` indicates that a custom key store has never been connected or it was intentionally [disconnected from its Amazon CloudHSM cluster](#). However, if attempts to use a KMS key in a connected Amazon CloudHSM key store fail, that might indicate a

problem with the Amazon CloudHSM key store or its Amazon CloudHSM cluster. For help, see [How to fix a failing KMS key](#).

If the `ConnectionState` of the custom key store is `FAILED`, the `DescribeCustomKeyStores` response includes a `ConnectionErrorCode` element that explains the reason for the error.

For example, in the following output, the `INVALID_CREDENTIALS` value indicates that the custom key store connection failed because the [kmsuser password is invalid](#). For help with this and other connection error failures, see [Troubleshooting a custom key store](#).

```
$ aws kms describe-custom-key-stores --custom-key-store-id cks-1234567890abcdef0
{
  "CustomKeyStores": [
    {
      "CloudHsmClusterId": "cluster-1a23b4cdefg",
      "ConnectionErrorCode": "INVALID_CREDENTIALS",
      "ConnectionState": "FAILED",
      "CustomKeyId": "cks-1234567890abcdef0",
      "CustomKeyName": "ExampleCloudHSMKeyStore",
      "CustomKeyType": "AWS_CLOUDHSM",
      "CreationDate": "1.499288695918E9",
      "TrustAnchorCertificate": "<certificate appears here>"
    }
  ]
}
```

Learn more:

- [View external key stores](#)
- [Identify KMS keys in Amazon CloudHSM key stores](#)
- [Logging Amazon KMS API calls with Amazon CloudTrail](#)

Edit Amazon CloudHSM key store settings

You can change the settings of an existing Amazon CloudHSM key store. The custom key store must be disconnected its Amazon CloudHSM cluster.

To edit Amazon CloudHSM key store settings:

1. [Disconnect the custom key store](#) from its Amazon CloudHSM cluster.

While the custom key store is disconnected, you cannot create Amazon KMS keys (KMS keys) in the custom key store and you cannot use the KMS keys it contains for [cryptographic operations](#).

2. Edit one or more of the Amazon CloudHSM key store settings.

You can edit the following settings in a custom key store:

The friendly name of the custom key store.

Enter a new friendly name. The new name must be unique among all custom key stores in your Amazon Web Services account.

 **Important**

Do not include confidential or sensitive information in this field. This field may be displayed in plaintext in CloudTrail logs and other output.

The cluster ID of the associated Amazon CloudHSM cluster.

Edit this value to substitute a related Amazon CloudHSM cluster for the original one. You can use this feature to repair a custom key store if its Amazon CloudHSM cluster becomes corrupted or is deleted.

Specify an Amazon CloudHSM cluster that shares a backup history with the original cluster and [fulfills the requirements](#) for association with a custom key store, including two active HSMs in different Availability Zones. Clusters that share a backup history have the same cluster certificate. To view the cluster certificate of a cluster, use the [DescribeClusters](#) operation. You cannot use the edit feature to associate the custom key store with an unrelated Amazon CloudHSM cluster.

The current password of the [kmsuser1 crypto user](#) (CU).

Tells Amazon KMS the current password of the kmsuser1 CU in the Amazon CloudHSM cluster. This action does not change the password of the kmsuser1 CU in the Amazon CloudHSM cluster.

If you change the password of the `kmsuser` CU in the Amazon CloudHSM cluster, use this feature to tell Amazon KMS the new `kmsuser` password. Otherwise, Amazon KMS cannot log into the cluster and all attempts to connect the custom key store to the cluster fail.

3. [Reconnect the custom key store](#) to its Amazon CloudHSM cluster.

Edit your key store settings

You can edit your Amazon CloudHSM key store settings in the Amazon KMS console or by using the [UpdateCustomKeyStore](#) operation.

Using the Amazon KMS console

When you edit an Amazon CloudHSM key store, you can change any or of the configurable values.

1. Sign in to the Amazon Web Services Management Console and open the Amazon Key Management Service (Amazon KMS) console at <https://console.amazonaws.cn/kms>.
2. To change the Amazon Web Services Region, use the Region selector in the upper-right corner of the page.
3. In the navigation pane, choose **Custom key stores, Amazon CloudHSM key stores**.
4. Choose the row of the Amazon CloudHSM key store you want to edit.

If the value in the **Connection state** column is not **Disconnected**, you must disconnect the custom key store before you can edit it. (From the **Key store actions** menu, choose **Disconnect**.)

While an Amazon CloudHSM key store is disconnected, you can manage the Amazon CloudHSM key store and its KMS keys, but you cannot create or use KMS keys in the Amazon CloudHSM key store.

5. From the **Key store actions** menu, choose **Edit**.
6. Do one or more of the following actions.
 - Type a new friendly name for the custom key store.
 - Type the cluster ID of a related Amazon CloudHSM cluster.
 - Type the current password of the `kmsuser` crypto user in the associated Amazon CloudHSM cluster.
7. Choose **Save**.

When the procedure is successful, a message describes the settings that you edited. When it is unsuccessful, an error message appears that describes the problem and provides help on how to fix it. If you need more help, see [Troubleshooting a custom key store](#).

8. [Reconnect the custom key store](#).

To use the Amazon CloudHSM key store, you must reconnect it after editing. You can leave the Amazon CloudHSM key store disconnected. But while it is disconnected, you cannot create KMS keys in the Amazon CloudHSM key store or use the KMS keys in the Amazon CloudHSM key store in [cryptographic operations](#).

Using the Amazon KMS API

To change the properties of an Amazon CloudHSM key store, use the [UpdateCustomKeyStore](#) operation. You can change multiple properties of a custom key store in the same command. If the operation is successful, Amazon KMS returns an HTTP 200 response and a JSON object with no properties. To verify that the changes are effective, use the [DescribeCustomKeyStores](#) operation.

The examples in this section use the [Amazon Command Line Interface \(Amazon CLI\)](#), but you can use any supported programming language.

Begin by using [DisconnectCustomKeyStore](#) to [disconnect the custom key store](#) from its Amazon CloudHSM cluster. Replace the example custom key store ID, `cks-1234567890abcdef0`, with an actual ID.

```
$ aws kms disconnect-custom-key-store --custom-key-store-id cks-1234567890abcdef0
```

The first example uses [UpdateCustomKeyStore](#) to change the friendly name of the Amazon CloudHSM key store to `DevelopmentKeys`. The command uses the `CustomKeyId` parameter to identify the Amazon CloudHSM key store and the `CustomKeyName` to specify the new name for the custom key store.

```
$ aws kms update-custom-key-store --custom-key-store-id cks-1234567890abcdef0 --new-custom-key-store-name DevelopmentKeys
```

The following example changes the cluster that is associated with an Amazon CloudHSM key store to another backup of the same cluster. The command uses the `CustomKeyId` parameter to identify the Amazon CloudHSM key store and the `CloudHsmClusterId` parameter to specify the new cluster ID.

```
$ aws kms update-custom-key-store --custom-key-store-id cks-1234567890abcdef0 --cloud-hsm-cluster-id cluster-1a23b4cdefg
```

The following example tells Amazon KMS that the current `kmsuser` password is `ExamplePassword`. The command uses the `CustomKeyStoreId` parameter to identify the Amazon CloudHSM key store and the `KeyStorePassword` parameter to specify the current password.

```
$ aws kms update-custom-key-store --custom-key-store-id cks-1234567890abcdef0 --key-store-password ExamplePassword
```

The final command reconnects the Amazon CloudHSM key store to its Amazon CloudHSM cluster. You can leave the custom key store in the disconnected state, but you must connect it before you can create new KMS keys or use existing KMS keys for [cryptographic operations](#). Replace the example custom key store ID with an actual ID.

```
$ aws kms connect-custom-key-store --custom-key-store-id cks-1234567890abcdef0
```

Connect an Amazon CloudHSM key store

New Amazon CloudHSM key stores are not connected. Before you can create and use Amazon KMS keys in your Amazon CloudHSM key store, you need to connect it to its associated Amazon CloudHSM cluster. You can connect and disconnect your Amazon CloudHSM key store at any time, and [view its connection state](#).

You are not required to connect your Amazon CloudHSM key store. You can leave an Amazon CloudHSM key store in a disconnected state indefinitely and connect it only when you need to use it. However, you might want to test the connection periodically to verify that the settings are correct and it can be connected.

Note

Amazon CloudHSM key stores have a `DISCONNECTED` connection state only when the key store has never been connected or you explicitly disconnect it. If your Amazon CloudHSM key store connection state is `CONNECTED` but you are having trouble using it, make sure that its associated Amazon CloudHSM cluster is active and contains at least one active

HSMs. For help with connection failures, see [the section called “Troubleshooting a custom key store”](#).

When you connect an Amazon CloudHSM key store, Amazon KMS finds the associated Amazon CloudHSM cluster, connects to it, logs into the Amazon CloudHSM client as the [kmsuser crypto user](#) (CU), and then rotates the `kmsuser` password. Amazon KMS remains logged into the Amazon CloudHSM client as long as the Amazon CloudHSM key store is connected.

To establish the connection, Amazon KMS creates a [security group](#) named `kms-<custom key store ID>` in the virtual private cloud (VPC) of the cluster. The security group has a single rule that allows inbound traffic from the cluster security group. Amazon KMS also creates an [elastic network interface](#) (ENI) in each Availability Zone of the private subnet for the cluster. Amazon KMS adds the ENIs to the `kms-<cluster ID>` security group and the security group for the cluster. The description of each ENI is `KMS managed ENI for cluster <cluster-ID>`.

The connection process can take an extended amount of time to complete; up to 20 minutes.

Before you connect the Amazon CloudHSM key store, verify that it meets the requirements.

- Its associated Amazon CloudHSM cluster must contain at least one active HSM. To find the number of HSMs in the cluster, view the cluster in the Amazon CloudHSM console or use the [DescribeClusters](#) operation. If necessary, you can [add an HSM](#).
- The cluster must have a [kmsuser crypto user](#) (CU) account, but that CU cannot be logged into the cluster when you connect the Amazon CloudHSM key store. For help with logging out, see [How to log out and reconnect](#).
- The connection state of the Amazon CloudHSM key store cannot be DISCONNECTING or FAILED. To view the connection state, use the Amazon KMS console or the [DescribeCustomKeyStores](#) response. If the connection state is FAILED, disconnect the custom key store, fix the problem, and then connect it.

For help with connection failures, see [How to fix a connection failure](#).

When your Amazon CloudHSM key store is connected, you can [create KMS keys in it](#) and use existing KMS keys in [cryptographic operations](#).

Connect and reconnect to your Amazon CloudHSM key store

You can connect, or reconnect, your Amazon CloudHSM key store in the Amazon KMS console or by using the [ConnectCustomKeyStore](#) operation.

Using the Amazon KMS console

To connect an Amazon CloudHSM key store in the Amazon Web Services Management Console, begin by selecting the Amazon CloudHSM key store from the **Custom key stores** page. The connection process can take up to 20 minutes to complete.

1. Sign in to the Amazon Web Services Management Console and open the Amazon Key Management Service (Amazon KMS) console at <https://console.amazonaws.cn/kms>.
2. To change the Amazon Web Services Region, use the Region selector in the upper-right corner of the page.
3. In the navigation pane, choose **Custom key stores, Amazon CloudHSM key stores**.
4. Choose the row of the Amazon CloudHSM key store you want to connect.

If the connection state of the Amazon CloudHSM key store is **Failed**, you must [disconnect the custom key store](#) before you connect it.

5. From the **Key store actions** menu, choose **Connect**.

Amazon KMS begins the process of connecting your custom key store. It finds the associated Amazon CloudHSM cluster, builds the required network infrastructure, connects to it, logs into the Amazon CloudHSM cluster as the `kmsuser1` CU, and rotates the `kmsuser1` password. When the operation completes, the connection state changes to **Connected**.

If the operation fails, an error message appears that describes the reason for the failure. Before you try to connect again, [view the connection state](#) of your Amazon CloudHSM key store. If it is **Failed**, you must [disconnect the custom key store](#) before you connect it again. If you need help, see [Troubleshooting a custom key store](#).

Next: [the section called "Create a KMS key in an Amazon CloudHSM key store"](#).

Using the Amazon KMS API

To connect a disconnected Amazon CloudHSM key store, use the [ConnectCustomKeyStore](#) operation. The associated Amazon CloudHSM cluster must contain at least one active HSM and the connection state cannot be FAILED.

The connection process takes an extended amount of time to complete; up to 20 minutes. Unless it fails quickly, the operation returns an HTTP 200 response and a JSON object with no properties. However, this initial response does not indicate that the connection was successful. To determine the connection state of the custom key store, see the [DescribeCustomKeyStores](#) response.

The examples in this section use the [Amazon Command Line Interface \(Amazon CLI\)](#), but you can use any supported programming language.

To identify the Amazon CloudHSM key store, use its custom key store ID. You can find the ID on the **Custom key stores** page in the console or by using the [DescribeCustomKeyStores](#) operation with no parameters. Before running this example, replace the example ID with a valid one.

```
$ aws kms connect-custom-key-store --custom-key-store-id cks-1234567890abcdef0
```

To verify that the Amazon CloudHSM key store is connected, use the [DescribeCustomKeyStores](#) operation. By default, this operation returns all custom key stores in your account and Region. But you can use either the `CustomKeyStoreId` or `CustomKeyStoreName` parameter (but not both) to limit the response to particular custom key stores. The `ConnectionState` value of `CONNECTED` indicates that the custom key store is connected to its Amazon CloudHSM cluster.

Note

The `CustomKeyStoreType` field was added to the `DescribeCustomKeyStores` response to distinguish Amazon CloudHSM key stores from external key stores.

```
$ aws kms describe-custom-key-stores --custom-key-store-id cks-1234567890abcdef0
{
  "CustomKeyStores": [
    {
      "CustomKeyStoreId": "cks-1234567890abcdef0",
      "CustomKeyStoreName": "ExampleCloudHSMKeyStore",
      "CloudHsmClusterId": "cluster-1a23b4cdefg",
      "CustomKeyStoreType": "AWS_CLOUDHSM",
      "TrustAnchorCertificate": "<certificate string appears here>",
      "CreationDate": "1.499288695918E9",
      "ConnectionState": "CONNECTED"
    }
  ],
}
```

If the `ConnectionState` value is failed, the `ConnectionErrorCode` element indicates the reason for the failure. In this case, Amazon KMS could not find an Amazon CloudHSM cluster in your account with the cluster ID `cluster-1a23b4cdefg`. If you deleted the cluster, you can [restore it from a backup](#) of the original cluster and then [edit the cluster ID](#) for the custom key store. For help responding to a connection error code, see [How to fix a connection failure](#).

```
$ aws kms describe-custom-key-stores --custom-key-store-id cks-1234567890abcdef0
{
  "CustomKeyStores": [
    "CustomKeyId": "cks-1234567890abcdef0",
    "CustomKeyName": "ExampleKeyStore",
    "CloudHsmClusterId": "cluster-1a23b4cdefg",
    "CustomKeyType": "AWS_CLOUDHSM",
    "TrustAnchorCertificate": "<certificate string appears here>",
    "CreationDate": "1.499288695918E9",
    "ConnectionState": "FAILED"
    "ConnectionErrorCode": "CLUSTER_NOT_FOUND"
  ],
}
```

Disconnect an Amazon CloudHSM key store

When you disconnect an Amazon CloudHSM key store, Amazon KMS logs out of the Amazon CloudHSM client, disconnects from the associated Amazon CloudHSM cluster, and removes the network infrastructure that it created to support the connection.


While an Amazon CloudHSM key store is disconnected, you can manage the Amazon CloudHSM key store and its KMS keys, but you cannot create or use KMS keys in the Amazon CloudHSM key store. The connection state of the key store is `DISCONNECTED` and the [key state](#) of KMS keys in the custom key store is `Unavailable`, unless they are `PendingDeletion`. You can reconnect the Amazon CloudHSM key store at any time.

Note

Amazon CloudHSM key stores have a `DISCONNECTED` connection state only when the key store has never been connected or you explicitly disconnect it. If your Amazon CloudHSM key store connection state is `CONNECTED` but you are having trouble using it, make sure that its associated Amazon CloudHSM cluster is active and contains at least one active

HSMs. For help with connection failures, see [the section called “Troubleshooting a custom key store”](#).

When you disconnect a custom key store, the KMS keys in the key store become unusable right away (subject to eventual consistency). However, resources encrypted with [data keys](#) protected by the KMS key are not affected until the KMS key is used again, such as to decrypt the data key. This issue affects Amazon Web Services services, many of which use data keys to protect your resources. For details, see [How unusable KMS keys affect data keys](#).

 **Note**

While a custom key store is disconnected, all attempts to create KMS keys in the custom key store or to use existing KMS keys in cryptographic operations will fail. This action can prevent users from storing and accessing sensitive data.

To better estimate the effect of disconnecting your custom key store, [identify the KMS keys](#) in the custom key store and [determine their past use](#).

You might disconnect an Amazon CloudHSM key store for reasons such as the following:

- **To rotate of the `kmsuser` password.** Amazon KMS changes the `kmsuser` password each time that it connects to the Amazon CloudHSM cluster. To force a password rotation, just disconnect and reconnect.
- **To audit the key material** for the KMS keys in the Amazon CloudHSM cluster. When you disconnect the custom key store, Amazon KMS logs out of the [kmsuser crypto user](#) account in the Amazon CloudHSM client. This allows you to log into the cluster as the `kmsuser` CU and audit and manage the key material for the KMS key.
- **To immediately disable all KMS keys** in the Amazon CloudHSM key store. You can [disable and re-enable KMS keys](#) in an Amazon CloudHSM key store by using the Amazon Web Services Management Console or the [DisableKey](#) operation. These operations complete quickly, but they act on one KMS key at a time. Disconnecting the Amazon CloudHSM key store immediately changes the key state of all KMS keys in the Amazon CloudHSM key store to `Unavailable`, which prevents them from being used in any cryptographic operation.

- **To repair a failed connection attempt.** If an attempt to connect an Amazon CloudHSM key store fails (the connection state of the custom key store is FAILED), you must disconnect the Amazon CloudHSM key store before you try to connect it again.

Disconnect your Amazon CloudHSM key store

You can disconnect your Amazon CloudHSM key store in the Amazon KMS console or by using the [DisconnectCustomKeyStore](#) operation.

Disconnect using the Amazon KMS console

To disconnect a connected Amazon CloudHSM key store in the Amazon KMS console, begin by choosing the Amazon CloudHSM key store from the **Custom Key Stores** page.

1. Sign in to the Amazon Web Services Management Console and open the Amazon Key Management Service (Amazon KMS) console at <https://console.amazonaws.cn/kms>.
2. To change the Amazon Web Services Region, use the Region selector in the upper-right corner of the page.
3. In the navigation pane, choose **Custom key stores, Amazon CloudHSM key stores**.
4. Choose the row of the external key store you want to disconnect.
5. From the **Key store actions** menu, choose **Disconnect**.

When the operation completes, the connection state changes from **Disconnecting** to **Disconnected**. If the operation fails, an error message appears that describes the problem and provides help on how to fix it. If you need more help, see [Troubleshooting a custom key store](#).

Disconnect using the Amazon KMS API

To disconnect a connected Amazon CloudHSM key store, use the [DisconnectCustomKeyStore](#) operation. If the operation is successful, Amazon KMS returns an HTTP 200 response and a JSON object with no properties.

The examples in this section use the [Amazon Command Line Interface \(Amazon CLI\)](#), but you can use any supported programming language.

This example disconnects an Amazon CloudHSM key store. Before running this example, replace the example ID with a valid one.

```
$ aws kms disconnect-custom-key-store --custom-key-store-id cks-1234567890abcdef0
```

To verify that the Amazon CloudHSM key store is disconnected, use the [DescribeCustomKeyStores](#) operation. By default, this operation returns all custom key stores in your account and Region. But you can use either the `CustomKeyId` and `CustomKeyName` parameter (but not both) to limit the response to particular custom key stores. The `ConnectionState` value of `DISCONNECTED` indicates that this example Amazon CloudHSM key store is not connected to its Amazon CloudHSM cluster.

```
$ aws kms describe-custom-key-stores --custom-key-store-id cks-1234567890abcdef0
{
  "CustomKeyStores": [
    "CloudHsmClusterId": "cluster-1a23b4cdefg",
    "ConnectionState": "DISCONNECTED",
    "CreationDate": "1.499288695918E9",
    "CustomKeyId": "cks-1234567890abcdef0",
    "CustomKeyName": "ExampleKeyStore",
    "CustomKeyType": "AWS_CLOUDHSM",
    "TrustAnchorCertificate": "<certificate string appears here>"
  ],
}
```

Delete an Amazon CloudHSM key store

When you delete an Amazon CloudHSM key store, Amazon KMS deletes all metadata about the Amazon CloudHSM key store from KMS, including information about its association with an Amazon CloudHSM cluster. This operation does not affect the Amazon CloudHSM cluster, its HSMs, or its users. You can create a new Amazon CloudHSM key store that is associated with the same Amazon CloudHSM cluster, but you cannot undo the delete operation.

You can only delete an Amazon CloudHSM key store that is disconnected from its Amazon CloudHSM cluster and does not contain any Amazon KMS keys. Before you delete a custom key store, do the following.

- Verify that you will never need to use any of the KMS keys in the key store for any [cryptographic operations](#). Then [schedule deletion](#) of all of the KMS keys from the key store. For help finding the KMS keys in an Amazon CloudHSM key store, see [Find the KMS keys in an Amazon CloudHSM key store](#).

- Confirm that all KMS keys have been deleted. To view the KMS keys in an Amazon CloudHSM key store, see [the section called “Identify KMS keys in Amazon CloudHSM key stores”](#).
- [Disconnect the Amazon CloudHSM key store](#) from its Amazon CloudHSM cluster.

Instead of deleting the Amazon CloudHSM key store, consider [disconnecting it](#) from its associated Amazon CloudHSM cluster. While an Amazon CloudHSM key store is disconnected, you can manage the Amazon CloudHSM key store and its Amazon KMS keys. But you cannot create or use KMS keys in the Amazon CloudHSM key store. You can reconnect the Amazon CloudHSM key store at any time.

Delete your Amazon CloudHSM key store

You can delete your Amazon CloudHSM key store in the Amazon KMS console or by using the [DeleteCustomKeyStore](#) operation.

Using the Amazon KMS console

To delete an Amazon CloudHSM key store in the Amazon Web Services Management Console, begin by selecting the Amazon CloudHSM key store from the **Custom key stores** page.

1. Sign in to the Amazon Web Services Management Console and open the Amazon Key Management Service (Amazon KMS) console at <https://console.amazonaws.cn/kms>.
2. To change the Amazon Web Services Region, use the Region selector in the upper-right corner of the page.
3. In the navigation pane, choose **Custom key stores, Amazon CloudHSM key stores**.
4. Find the row that represents the Amazon CloudHSM key store that you want to delete. If the **Connection state** of the Amazon CloudHSM key store is not **Disconnected**, you must [disconnect the Amazon CloudHSM key store](#) before you delete it.
5. From the **Key store actions** menu, choose **Delete**.

When the operation completes, a success message appears and the Amazon CloudHSM key store no longer appears in the key stores list. If the operation is unsuccessful, an error message appears that describes the problem and provides help on how to fix it. If you need more help, see [Troubleshooting a custom key store](#).

Using the Amazon KMS API

To delete an Amazon CloudHSM key store, use the [DeleteCustomKeyStore](#) operation. If the operation is successful, Amazon KMS returns an HTTP 200 response and a JSON object with no properties.

To begin, verify that the Amazon CloudHSM key store does not contain any Amazon KMS keys. You cannot delete a custom key store that contains KMS keys. The first example command uses [ListKeys](#) and [DescribeKey](#) to search for Amazon KMS keys in the Amazon CloudHSM key store with the example `cks-1234567890abcdef0` custom key store ID. In this case, the command does not return any KMS keys. If it does, use the [ScheduleKeyDeletion](#) operation to schedule deletion of each of the KMS keys.

Bash

```
for key in $(aws kms list-keys --query 'Keys[*].KeyId' --output text) ;  
do aws kms describe-key --key-id $key |  
grep '"CustomKeyId": "cks-1234567890abcdef0"' --context 100; done
```

PowerShell

```
PS C:\> Get-KMSKeyList | Get-KMSKey | where CustomKeyId -eq  
'cks-1234567890abcdef0'
```

Next, disconnect the Amazon CloudHSM key store. This example command uses the [DisconnectCustomKeyStore](#) operation to disconnect an Amazon CloudHSM key store from its Amazon CloudHSM cluster. Before running this command, replace the example custom key store ID with a valid one.

Bash

```
$ aws kms disconnect-custom-key-store --custom-key-store-id cks-1234567890abcdef0
```

PowerShell

```
PS C:\> Disconnect-KMSCustomKeyStore -CustomKeyId cks-1234567890abcdef0
```

After the custom key store is disconnected, you can use the [DeleteCustomKeyStore](#) operation to delete it.

Bash

```
$ aws kms delete-custom-key-store --custom-key-store-id cks-1234567890abcdef0
```

PowerShell

```
PS C:\> Remove-KMSCustomKeyStore -CustomKeyStoreId cks-1234567890abcdef0
```

Troubleshooting a custom key store

Amazon CloudHSM key stores are designed to be available and resilient. However, there are some error conditions that you might have to repair to keep your Amazon CloudHSM key store operational.

Topics

- [How to fix unavailable KMS keys](#)
- [How to fix a failing KMS key](#)
- [How to fix a connection failure](#)
- [How to respond to a cryptographic operation failure](#)
- [How to fix invalid kmsuser credentials](#)
- [How to delete orphaned key material](#)
- [How to recover deleted key material for a KMS key](#)
- [How to log in as kmsuser](#)

How to fix unavailable KMS keys

The [key state](#) of Amazon KMS keys in an Amazon CloudHSM key store is typically Enabled. Like all KMS keys, the key state changes when you disable the KMS keys in an Amazon CloudHSM key store or schedule them for deletion. However, unlike other KMS keys, the KMS keys in a custom key store can also have a [key state](#) of Unavailable.

A key state of Unavailable indicates that the KMS key is in a custom key store that was intentionally [disconnected](#) and attempts to reconnect it, if any, failed. While a KMS key is

unavailable, you can view and manage the KMS key, but you cannot use it for [cryptographic operations](#).

To find the key state of a KMS key, on the **Customer managed keys** page, view the **Status** field of the KMS key. Or, use the [DescribeKey](#) operation and view the KeyState element in the response. For details, see [Identify and view keys](#).

The KMS keys in a disconnected custom key store will have a key state of `Unavailable` or `PendingDeletion`. KMS keys that are scheduled for deletion from a custom key store have a `Pending Deletion` key state, even when the custom key store is disconnected. This allows you to cancel the scheduled key deletion without reconnecting the custom key store.

To fix an unavailable KMS key, [reconnect the custom key store](#). After the custom key store is reconnected, the key state of the KMS keys in the custom key store is automatically restored to its previous state, such as `Enabled` or `Disabled`. KMS keys that are pending deletion remain in the `PendingDeletion` state. However, while the problem persists, [enabling and disabling an unavailable KMS key](#) does not change its key state. The enable or disable action takes effect only when the key becomes available.

For help with failed connections, see [How to fix a connection failure](#).

How to fix a failing KMS key

Problems with creating and using KMS keys in Amazon CloudHSM key stores can be caused by a problem with your Amazon CloudHSM key store, its associated Amazon CloudHSM cluster, the KMS key, or its key material.

When an Amazon CloudHSM key store is disconnected from its Amazon CloudHSM cluster, the key state of KMS keys in the custom key store is `Unavailable`. All requests to create KMS keys in a disconnected Amazon CloudHSM key store return a `CustomKeyStoreInvalidStateException` exception. All requests to encrypt, decrypt, re-encrypt, or generate data keys return a `KMSInvalidStateException` exception. To fix the problem, [reconnect the Amazon CloudHSM key store](#).

However, your attempts to use a KMS key in an Amazon CloudHSM key store for [cryptographic operations](#) might fail even when its key state is `Enabled` and the connection state of the Amazon CloudHSM key store is `Connected`. This might be caused by any of the following conditions.

- The key material for the KMS key might have been deleted from the associated Amazon CloudHSM cluster. To investigate, [find the key id](#) of the key material for a KMS key and, if necessary, try to [recover the key material](#).
- All HSMs were deleted from the Amazon CloudHSM cluster that is associated with the Amazon CloudHSM key store. To use a KMS key in an Amazon CloudHSM key store in a cryptographic operation, its Amazon CloudHSM cluster must contain at least one active HSM. To verify the number and state of HSMs in an Amazon CloudHSM cluster, [use the Amazon CloudHSM console](#) or the [DescribeClusters](#) operation. To add an HSM to the cluster, use the Amazon CloudHSM console or the [CreateHsm](#) operation.
- The Amazon CloudHSM cluster associated with the Amazon CloudHSM key store was deleted. To fix the problem, [create a cluster from a backup](#) that is related to the original cluster, such as a backup of the original cluster, or a backup that was used to create the original cluster. Then, [edit the cluster ID](#) in the custom key store settings. For instructions, see [How to recover deleted key material for a KMS key](#).
- The Amazon CloudHSM cluster associated with the custom key store did not have any available PKCS #11 sessions. This typically occurs during periods of high burst traffic when additional sessions are needed to service the traffic. To respond to a `KMSInternalException` with an error message about PKCS #11 sessions, back off and retry the request again.

How to fix a connection failure

If you try to [connect an Amazon CloudHSM key store](#) to its Amazon CloudHSM cluster, but the operation fails, the connection state of the Amazon CloudHSM key store changes to FAILED. To find the connection state of an Amazon CloudHSM key store, use the Amazon KMS console or the [DescribeCustomKeyStores](#) operation.

Alternatively, some connection attempts fail quickly due to easily detected cluster configuration errors. In this case, the connection state is still DISCONNECTED. These failures return an error message or [exception](#) that explains why the attempt failed. Review the exception description and [cluster requirements](#), fix the problem, [update the Amazon CloudHSM key store](#), if necessary, and try to connect again.

When the connection state is FAILED, run the [DescribeCustomKeyStores](#) operation and see the `ConnectionErrorCode` element in the response.

Note

When the connection state of an Amazon CloudHSM key store is FAILED, you must [disconnect the Amazon CloudHSM key store](#) before attempting to reconnect it. You cannot connect an Amazon CloudHSM key store with a FAILED connection state.

- CLUSTER_NOT_FOUND indicates that Amazon KMS cannot find an Amazon CloudHSM cluster with the specified cluster ID. This might occur because the wrong cluster ID was provided to an API operation or the cluster was deleted and not replaced. To fix this error, verify the cluster ID, such as by using the Amazon CloudHSM console or the [DescribeClusters](#) operation. If the cluster was deleted, [create a cluster from a recent backup](#) of the original. Then, [disconnect the Amazon CloudHSM key store](#), [edit the Amazon CloudHSM key store](#) cluster ID setting, and [reconnect the Amazon CloudHSM key store](#) to the cluster.
- INSUFFICIENT_CLOUDHSM_HSMS indicates that the associated Amazon CloudHSM cluster does not contain any HSMS. To connect, the cluster must have at least one HSM. To find the number of HSMS in the cluster, use the [DescribeClusters](#) operation. To resolve this error, [add at least one HSM](#) to the cluster. If you add multiple HSMS, it's best to create them in different Availability Zones.
- INSUFFICIENT_FREE_ADDRESSES_IN_SUBNET indicates that Amazon KMS could not connect the Amazon CloudHSM key store to its Amazon CloudHSM cluster because at least one [private subnet associated with the cluster](#) doesn't have any available IP addresses. An Amazon CloudHSM key store connection requires one free IP address in each of the associated private subnets, although two are preferable.

You [can't add IP addresses](#) (CIDR blocks) to an existing subnet. If possible, move or delete other resources that are using the IP addresses in the subnet, such as unused EC2 instances or elastic network interfaces. Otherwise, you can [create a cluster from a recent backup](#) of the Amazon CloudHSM cluster with new or existing private subnets that have [more free address space](#). Then, to associate the new cluster with your Amazon CloudHSM key store, [disconnect the custom key store](#), [change the cluster ID](#) of the Amazon CloudHSM key store to the ID of the new cluster, and try to connect again.

Tip

To avoid [resetting the kmsuser password](#), use the most recent backup of the Amazon CloudHSM cluster.

- INTERNAL_ERROR indicates that Amazon KMS could not complete the request due to an internal error. Retry the request. For ConnectCustomKeyStore requests, disconnect the Amazon CloudHSM key store before trying to connect again.
- INVALID_CREDENTIALS indicates that Amazon KMS cannot log into the associated Amazon CloudHSM cluster because it doesn't have the correct kmsuser account password. For help with this error, see [How to fix invalid kmsuser credentials](#).
- NETWORK_ERRORS usually indicates transient network issues. [Disconnect the Amazon CloudHSM key store](#), wait a few minutes, and try to connect again.
- SUBNET_NOT_FOUND indicates that at least one subnet in the Amazon CloudHSM cluster configuration was deleted. If Amazon KMS cannot find all of the subnets in the cluster configuration, attempts to connect the Amazon CloudHSM key store to the Amazon CloudHSM cluster fail.

To fix this error, [create a cluster from a recent backup](#) of the same Amazon CloudHSM cluster. (This process creates a new cluster configuration with a VPC and private subnets.) Verify that the new cluster meets the [requirements for a custom key store](#), and note the new cluster ID. Then, to associate the new cluster with your Amazon CloudHSM key store, [disconnect the custom key store](#), [change the cluster ID](#) of the Amazon CloudHSM key store to the ID of the new cluster, and try to connect again.

Tip

To avoid [resetting the kmsuser password](#), use the most recent backup of the Amazon CloudHSM cluster.

- USER_LOCKED_OUT indicates that the [kmsuser crypto user \(CU\) account](#) is locked out of the associated Amazon CloudHSM cluster due to too many failed password attempts. For help with this error, see [How to fix invalid kmsuser credentials](#).

To fix this error, [disconnect the Amazon CloudHSM key store](#) and use the [user change-password](#) command in CloudHSM CLI to change the kmsuser account password. Then, [edit the kmsuser](#)

[password setting](#) for the custom key store, and try to connect again. For help, use the procedure described in the [How to fix invalid kmsuser credentials](#) topic.

- `USER_LOGGED_IN` indicates that the `kmsuser` CU account is logged into the associated Amazon CloudHSM cluster. This prevents Amazon KMS from rotating the `kmsuser` account password and logging into the cluster. To fix this error, log the `kmsuser` CU out of the cluster. If you changed the `kmsuser` password to log into the cluster, you must also update the key store password value for the Amazon CloudHSM key store. For help, see [How to log out and reconnect](#).
- `USER_NOT_FOUND` indicates that Amazon KMS cannot find a `kmsuser` CU account in the associated Amazon CloudHSM cluster. To fix this error, [create a kmsuser CU account](#) in the cluster, and then [update the key store password value](#) for the Amazon CloudHSM key store. For help, see [How to fix invalid kmsuser credentials](#).

How to respond to a cryptographic operation failure

A cryptographic operation that uses a KMS key in a custom key store might fail with a `KMSInvalidStateException`. The following error messages might accompany the `KMSInvalidStateException`.

KMS cannot communicate with your CloudHSM cluster. This might be a transient network issue. If you see this error repeatedly, verify that the Network ACLs and the security group rules for the VPC of your Amazon CloudHSM cluster are correct.

- Although this is an HTTPS 400 error, it might result from transient network issues. To respond, begin by retrying the request. However, if it continues to fail, examine the configuration of your networking components. This error is most likely caused by the misconfiguration of a networking component, such as a firewall rule or VPC security group rule that is blocking outgoing traffic.

KMS cannot communicate with your Amazon CloudHSM cluster because the `kmsuser` is locked out. If you see this error repeatedly, disconnect the Amazon CloudHSM key store and reset the `kmsuser` account password. Update the `kmsuser` password for the custom key store and try the request again.

- This error message indicates that the [kmsuser crypto user \(CU\) account](#) is locked out of the associated Amazon CloudHSM cluster due to too many failed password attempts. For help with this error, see [How to disconnect and log in](#).

How to fix invalid kmsuser credentials

When you [connect an Amazon CloudHSM key store](#), Amazon KMS logs into the associated Amazon CloudHSM cluster as the [kmsuser crypto user](#) (CU). It remains logged in until the Amazon CloudHSM key store is disconnected. The [DescribeCustomKeyStores](#) response shows a `ConnectionState` of `FAILED` and `ConnectionErrorCode` value of `INVALID_CREDENTIALS`, as shown in the following example.

If you disconnect the Amazon CloudHSM key store and change the `kmsuser` password, Amazon KMS cannot log into the Amazon CloudHSM cluster with the credentials of the `kmsuser` CU account. As a result, all attempts to connect the Amazon CloudHSM key store fail. The `DescribeCustomKeyStores` response shows a `ConnectionState` of `FAILED` and `ConnectionErrorCode` value of `INVALID_CREDENTIALS`, as shown in the following example.

```
$ aws kms describe-custom-key-stores --custom-key-store-name ExampleKeyStore
{
  "CustomKeyStores": [
    {
      "CloudHsmClusterId": "cluster-1a23b4cdefg",
      "ConnectionErrorCode": "INVALID_CREDENTIALS"
      "CustomKeyId": "cks-1234567890abcdef0",
      "CustomKeyName": "ExampleKeyStore",
      "TrustAnchorCertificate": "<certificate string appears here>",
      "CreationDate": "1.499288695918E9",
      "ConnectionState": "FAILED"
    }
  ],
}
```

Also, after five failed attempts to log into the cluster with an incorrect password, Amazon CloudHSM locks the user account. To log into the cluster, you must change the account password.

If Amazon KMS gets a lockout response when it tries to log into the cluster as the `kmsuser` CU, the request to connect the Amazon CloudHSM key store fails. The [DescribeCustomKeyStores](#) response includes a `ConnectionState` of `FAILED` and `ConnectionErrorCode` value of `USER_LOCKED_OUT`, as shown in the following example.

```
$ aws kms describe-custom-key-stores --custom-key-store-name ExampleKeyStore
```

```
{
  "CustomKeyStores": [
    {
      "CloudHsmClusterId": "cluster-1a23b4cdefg",
      "ConnectionErrorCode": "USER_LOCKED_OUT",
      "CustomKeyStoreId": "cks-1234567890abcdef0",
      "CustomKeyStoreName": "ExampleKeyStore",
      "TrustAnchorCertificate": "<certificate string appears here>",
      "CreationDate": "1.499288695918E9",
      "ConnectionState": "FAILED"
    }
  ],
}
```

To repair any of these conditions, use the following procedure.

1. [Disconnect the Amazon CloudHSM key store.](#)
2. Run the [DescribeCustomKeyStores](#) operation and view the value of the `ConnectionErrorCode` element in the response.
 - If the `ConnectionErrorCode` value is `INVALID_CREDENTIALS`, determine the current password for the `kmsuser` account. If necessary, use the [user change-password](#) command in CloudHSM CLI to set the password to a known value.
 - If the `ConnectionErrorCode` value is `USER_LOCKED_OUT`, you must use the [user change-password](#) command in CloudHSM CLI to change the `kmsuser` password.
3. [Edit the kmsuser password setting](#) so it matches the current `kmsuser` password in the cluster. This action tells Amazon KMS which password to use to log into the cluster. It does not change the `kmsuser` password in the cluster.
4. [Connect the custom key store.](#)

How to delete orphaned key material

After scheduling deletion of a KMS key from an Amazon CloudHSM key store, you might need to manually delete the corresponding key material from the associated Amazon CloudHSM cluster.

When you create a KMS key in an Amazon CloudHSM key store, Amazon KMS creates the KMS key metadata in Amazon KMS and generates the key material in the associated Amazon CloudHSM cluster. When you schedule deletion of a KMS key in an Amazon CloudHSM key store, after the waiting period, Amazon KMS deletes the KMS key metadata. Then Amazon KMS makes a best effort to delete the corresponding key material from the Amazon CloudHSM cluster. The attempt might fail if Amazon KMS cannot access the cluster, such as when it's disconnected from the

Amazon CloudHSM key store or the kmsuser password changes. Amazon KMS does not attempt to delete key material from cluster backups.

Amazon KMS reports the results of its attempt to delete the key material from the cluster in the DeleteKey event entry of your Amazon CloudTrail logs. It appears in the backingKeysDeletionStatus element of the additionalEventData element, as shown in the following example entry. The entry also includes the KMS key ARN, the Amazon CloudHSM cluster ID, and the ID (backing-key-id) of the key material.

```
{
  "eventVersion": "1.08",
  "userIdentity": {
    "accountId": "111122223333",
    "invokedBy": "Amazon Internal"
  },
  "eventTime": "2021-12-10T14:23:51Z",
  "eventSource": "kms.amazonaws.com",
  "eventName": "DeleteKey",
  "awsRegion": "us-west-2",
  "sourceIPAddress": "Amazon Internal",
  "userAgent": "AWS Internal",
  "requestParameters": null,
  "responseElements": {
    "keyId": "arn:aws:kms:us-west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab"
  },
  "additionalEventData": {
    "customKeyStoreId": "cks-1234567890abcdef0",
    "clusterId": "cluster-1a23b4cdefg",
    "backingKeys": "[{\"backingKeyId\": \"backing-key-id\"}]",
    "backingKeysDeletionStatus": "[{\"backingKeyId\": \"backing-key-id\", \"deletionStatus\": \"FAILURE\"}]"
  },
  "eventID": "c21f1f47-f52b-4ffe-bff0-6d994403cf40",
  "readOnly": false,
  "resources": [
    {
      "accountId": "111122223333",
      "type": "AWS::KMS::Key",
      "ARN": "arn:aws:kms:eu-west-1:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab"
    }
  ],
}
```



```
"eventType": "AwsServiceEvent",
"recipientAccountId": "111122223333",
"managementEvent": true,
"eventCategory": "Management"
}
```

Notes

The following procedures use the Amazon CloudHSM Client SDK 5 command line tool, [CloudHSM CLI](#). The CloudHSM CLI replaces `key-handle` with `key-reference`.

On January 1, 2025, Amazon CloudHSM will end support for the Client SDK 3 command line tools, the CloudHSM Management Utility (CMU) and the Key Management Utility (KMU). For more information on the differences between the Client SDK 3 command line tools and the Client SDK 5 command line tool, see [Migrate from Client SDK 3 CMU and KMU to Client SDK 5 CloudHSM CLI](#) in the *Amazon CloudHSM User Guide*.

The following procedures demonstrate how to delete the orphaned key material from the associated Amazon CloudHSM cluster.

1. Disconnect the Amazon CloudHSM key store, if it is not already disconnected, then [login](#), as explained in [How to disconnect and log in](#).

Note

While a custom key store is disconnected, all attempts to create KMS keys in the custom key store or to use existing KMS keys in cryptographic operations will fail. This action can prevent users from storing and accessing sensitive data.

2. Use the [key delete](#) command in CloudHSM CLI to delete the key from the HSMs in the cluster.

All CloudTrail log entries for cryptographic operation with a KMS key in a Amazon CloudHSM key store include an `additionalEventData` field with the `customKeyStoreId` and `backingKey`. The value returned in the `backingKeyId` field is the CloudHSM key `id` attribute. We recommend filtering the **key delete** operation by `id` to delete the orphaned key material you identified in your CloudTrail logs.

Amazon CloudHSM recognizes the `backingKeyId` value as a hexadecimal value. To filter by `id`, you must prepend the `backingKeyId` with `0x`. For example, if the `backingKeyId` in your CloudTrail log is `1a2b3c45678abcdef`, you would filter by `0x1a2b3c45678abcdef`.

The following example deletes a key from the HSMs in your cluster. The `backing-key-id` is listed in the CloudTrail log entry. Before running this command, replace the example `backing-key-id` with a valid one from your account.

```
aws-cloudhsm key delete --filter attr.id="0x<backing-key-id>"
{
  "error_code": 0,
  "data": {
    "message": "Key deleted successfully"
  }
}
```

3. Log out and reconnect the Amazon CloudHSM key store as described in [How to log out and reconnect](#).

How to recover deleted key material for a KMS key

If the key material for an Amazon KMS key is deleted, the KMS key is unusable and all ciphertext that was encrypted under the KMS key cannot be decrypted. This can happen if the key material for a KMS key in an Amazon CloudHSM key store is deleted from the associated Amazon CloudHSM cluster. However, it might be possible to recover the key material.

When you create an Amazon KMS key (KMS key) in an Amazon CloudHSM key store, Amazon KMS logs into the associated Amazon CloudHSM cluster and creates the key material for the KMS key. It also changes the password to a value that only it knows and remains logged in as long as the Amazon CloudHSM key store is connected. Because only the key owner, that is, the CU who created a key, can delete the key, it is unlikely that the key will be deleted from the HSMs accidentally.

However, if the key material for a KMS key is deleted from the HSMs in a cluster, the key state of the KMS key eventually changes to `UNAVAILABLE`. If you attempt to use the KMS key for a cryptographic operation, the operation fails with a `KMSInvalidStateException` exception. Most importantly, any data that was encrypted under the KMS key cannot be decrypted.

Under certain circumstances, you can recover deleted key material by [creating a cluster from a backup](#) that contains the key material. This strategy works only when at least one backup was created while the key existed and before it was deleted.

Use the following process to recover the key material.

1. Find a cluster backup that contains the key material. The backup must also contain all users and keys that you need to support the cluster and its encrypted data.

Use the [DescribeBackups](#) operation to list the backups for a cluster. Then use the backup timestamp to help you select a backup. To limit the output to the cluster that is associated with the Amazon CloudHSM key store, use the `Filters` parameter, as shown in the following example.

```
$ aws cloudhsmv2 describe-backups --filters clusterIds=<cluster ID>
{
  "Backups": [
    {
      "ClusterId": "cluster-1a23b4cdefg",
      "BackupId": "backup-9g87f6edcba",
      "CreateTimestamp": 1536667238.328,
      "BackupState": "READY"
    },
    ...
  ]
}
```

2. [Create a cluster from the selected backup](#). Verify that the backup contains the deleted key and other users and keys that the cluster requires.
3. [Disconnect the Amazon CloudHSM key store](#) so you can edit its properties.
4. [Edit the cluster ID](#) of the Amazon CloudHSM key store. Enter the cluster ID of the cluster that you created from the backup. Because the cluster shares a backup history with the original cluster, the new cluster ID should be valid.
5. [Reconnect the Amazon CloudHSM key store](#).

How to log in as kmsuser

To create and manage the key material in the Amazon CloudHSM cluster for your Amazon CloudHSM key store, Amazon KMS uses the [kmsuser crypto user \(CU\) account](#). You [create the](#)

[kmsuser CU account](#) in your cluster and provide its password to Amazon KMS when you create your Amazon CloudHSM key store.

In general, Amazon KMS manages the `kmsuser` account. However, for some tasks, you need to disconnect the Amazon CloudHSM key store, log into the cluster as the `kmsuser` CU, and use the [CloudHSM Command Line Interface \(CLI\)](#).

Note

While a custom key store is disconnected, all attempts to create KMS keys in the custom key store or to use existing KMS keys in cryptographic operations will fail. This action can prevent users from storing and accessing sensitive data.

This topic explains how to [disconnect your Amazon CloudHSM key store and log in](#) as `kmsuser`, run the Amazon CloudHSM command line tool, and [log out and reconnect your Amazon CloudHSM key store](#).

Topics

- [How to disconnect and log in](#)
- [How to log out and reconnect](#)

How to disconnect and log in

Use the following procedure each time you need to log into an associated cluster as the `kmsuser` crypto user.

Notes

The following procedures use the Amazon CloudHSM Client SDK 5 command line tool, [CloudHSM CLI](#). The CloudHSM CLI replaces `key-handle` with `key-reference`.

On January 1, 2025, Amazon CloudHSM will end support for the Client SDK 3 command line tools, the CloudHSM Management Utility (CMU) and the Key Management Utility (KMU). For more information on the differences between the Client SDK 3 command line tools and the Client SDK 5 command line tool, see [Migrate from Client SDK 3 CMU and KMU to Client SDK 5 CloudHSM CLI](#) in the *Amazon CloudHSM User Guide*.

1. Disconnect the Amazon CloudHSM key store, if it is not already disconnected. You can use the Amazon KMS console or Amazon KMS API.

While your Amazon CloudHSM key is connected, Amazon KMS is logged in as the `kmsuser`. This prevents you from logging in as `kmsuser` or changing the `kmsuser` password.

For example, this command uses [DisconnectCustomKeyStore](#) to disconnect an example key store. Replace the example Amazon CloudHSM key store ID with a valid one.

```
$ aws kms disconnect-custom-key-store --custom-key-store-id cks-1234567890abcdef0
```

2. Use the `login` command to login as an admin. Use the procedures described in the [Using CloudHSM CLI](#) section of the *Amazon CloudHSM User Guide*.

```
aws-cloudhsm > login --username admin --role admin
Enter password:
{
  "error_code": 0,
  "data": {
    "username": "admin",
    "role": "admin"
  }
}
```

3. Use the [user change-password](#) command in CloudHSM CLI to change the password of the `kmsuser` account to one that you know. (Amazon KMS rotates the password when you connect your Amazon CloudHSM key store.) The password must consist of 7-32 alphanumeric characters. It is case-sensitive and cannot contain any special characters.
4. Login as `kmsuser` using the password that you set. For detailed instructions, see the [Using CloudHSM CLI](#) section of the *Amazon CloudHSM User Guide*.

```
aws-cloudhsm > login --username kmsuser --role crypto-user
Enter password:
{
  "error_code": 0,
  "data": {
    "username": "kmsuser",
    "role": "crypto-user"
  }
}
```

How to log out and reconnect

Use the following procedure each time you need to log out as the `kmsuser` crypto user and reconnect your key store.

Notes

The following procedures use the Amazon CloudHSM Client SDK 5 command line tool, [CloudHSM CLI](#). The CloudHSM CLI replaces `key-handle` with `key-reference`.

On January 1, 2025, Amazon CloudHSM will end support for the Client SDK 3 command line tools, the CloudHSM Management Utility (CMU) and the Key Management Utility (KMU). For more information on the differences between the Client SDK 3 command line tools and the Client SDK 5 command line tool, see [Migrate from Client SDK 3 CMU and KMU to Client SDK 5 CloudHSM CLI](#) in the *Amazon CloudHSM User Guide*.

1. Perform the task, then use the [logout](#) command in CloudHSM CLI to log out. If you do not log out, attempts to reconnect your Amazon CloudHSM key store will fail.

```
aws-cloudhsm logout
{
  "error_code": 0,
  "data": "Logout successful"
}
```

2. [Edit the `kmsuser` password setting](#) for the custom key store.

This tells Amazon KMS the current password for `kmsuser` in the cluster. If you omit this step, Amazon KMS will not be able to log into the cluster as `kmsuser`, and all attempts to reconnect your custom key store will fail. You can use the Amazon KMS console or the `KeyStorePassword` parameter of the [UpdateCustomKeyStore](#) operation.

For example, this command tells Amazon KMS that the current password is `tempPassword`. Replace the example password with the actual one.

```
$ aws kms update-custom-key-store --custom-key-store-id cks-1234567890abcdef0 --
key-store-password tempPassword
```

3. Reconnect the Amazon KMS key store to its Amazon CloudHSM cluster. Replace the example Amazon CloudHSM key store ID with a valid one. During the connection process, Amazon KMS changes the `kmsuser` password to a value that only it knows.

The [ConnectCustomKeyStore](#) operation returns quickly, but the connection process can take an extended period of time. The initial response does not indicate the success of the connection process.

```
$ aws kms connect-custom-key-store --custom-key-store-id cks-1234567890abcdef0
```

4. Use the [DescribeCustomKeyStores](#) operation to verify that the Amazon CloudHSM key store is connected. Replace the example Amazon CloudHSM key store ID with a valid one.

In this example, the connection state field shows that the Amazon CloudHSM key store is now connected.

```
$ aws kms describe-custom-key-stores --custom-key-store-  
id cks-1234567890abcdef0  
{  
  "CustomKeyStores": [  
    "CustomKeyId": "cks-1234567890abcdef0",  
    "CustomKeyName": "ExampleKeyStore",  
    "CloudHsmClusterId": "cluster-1a23b4cdefg",  
    "TrustAnchorCertificate": "<certificate string appears here>",  
    "CreationDate": "1.499288695918E9",  
    "ConnectionState": "CONNECTED"  
  ],  
}
```

External key stores

External key stores allow you to protect your Amazon resources using cryptographic keys outside of Amazon. This advanced feature is designed for regulated workloads that you must protect with encryption keys stored in an external key management system that you control. External key stores support the [Amazon digital sovereignty pledge](#) to give you sovereign control over your data in Amazon, including the ability to encrypt with key material that you own and control outside of Amazon.

An *external key store* is a [custom key store](#) backed by an *external key manager* that you own and manage outside of Amazon. Your external key manager can be a physical or virtual hardware security modules (HSMs), or any hardware-based or software-based system capable of generating and using cryptographic keys. Encryption and decryption operations that use a KMS key in an external key store are performed by your external key manager using your cryptographic key material, a feature known as *hold your own keys* (HYOKs).

Amazon KMS never interacts directly with your external key manager, and cannot create, view, manage, or delete your keys. Instead, Amazon KMS interacts only with [external key store proxy](#) (XKS proxy) software that you provide. Your external key store proxy mediates all communication between Amazon KMS and your external key manager. It transmits all requests from Amazon KMS to your external key manager, and transmits responses from your external key manager back to Amazon KMS. The external key store proxy also translates generic requests from Amazon KMS into a vendor-specific format that your external key manager can understand, allowing you to use external key stores with key managers from a variety of vendors.

You can use KMS keys in an external key store for client-side encryption, including with the [Amazon Encryption SDK](#). But external key stores are an important resource for server-side encryption, allowing you to protect your Amazon resources in multiple Amazon Web Services services with your cryptographic keys outside of Amazon. Amazon Web Services services that support [customer managed keys](#) for symmetric encryption also support KMS keys in an external key store. For service support details, see [Amazon Service Integration](#).

External key stores allow you to use Amazon KMS for regulated workloads where encryption keys must be stored and used outside of Amazon. But they are a major departure from the standard shared responsibility model, and require additional operational burdens. The greater risk to availability and latency will, for most customers, exceed the perceived security benefits of external key stores.

External key stores let you control the root of trust. Data encrypted under KMS keys in your external key store can be decrypted only by using the external key manager that you control. If you temporarily revoke access to your external key manager, such as by disconnecting the external key store or disconnecting your external key manager from the external key store proxy, Amazon loses all access to your cryptographic keys until you restore it. During that interval, ciphertext encrypted under your KMS keys can't be decrypted. If you permanently revoke access to your external key manager, all ciphertext encrypted under a KMS key in your external key store becomes unrecoverable. The only exceptions are Amazon services that briefly cache the [data keys](#) protected

by your KMS keys. These data keys continue to work until you deactivate the resource or the cache expires. For details, see [How unusable KMS keys affect data keys](#).

External key stores unblock the few use cases for regulated workloads where encryption keys must remain solely under your control and inaccessible to Amazon. But this is a major change in the way you operate cloud-based infrastructure and a significant shift in the shared responsibility model. For most workloads, the additional operational burden and greater risks to availability and performance will exceed the perceived security benefits of external key stores.

Do I need an external key store?

For most users, the default Amazon KMS key store, which is protected by [FIPS 140-3 Security Level 3 validated hardware security modules](#), fulfills their security, control, and regulatory requirements. External key store users incur substantial cost, maintenance, and troubleshooting burden, and risks to latency, availability and reliability.

When considering an external key store, take some time to understand the alternatives, including an [Amazon CloudHSM key store](#) backed by an Amazon CloudHSM cluster that you own and manage, and KMS keys with [imported key material](#) that you generate in your own HSMs and can delete from KMS keys on demand. In particular, importing key material with a very brief expiration interval might provide a similar level of control without the performance or availability risks.

An external key store might be the right solution for your organization if you have the following requirements:

- You are required to use cryptographic keys in your on-premises key manager or a key manager outside of Amazon that you control.
- You must demonstrate that your cryptographic keys are retained solely under your control outside of the cloud.
- You must encrypt and decrypt using cryptographic keys with independent authorization.
- Key material must be subject to a secondary, independent audit path.

If you choose an external key store, limit its use to workloads that require protection with cryptographic keys outside of Amazon.

Shared responsibility model

Standard KMS keys use key material that is generated and used in HSMs that Amazon KMS owns and manages. You establish the access control policies on your KMS keys and configure Amazon Web Services services that use KMS keys to protect your resources. Amazon KMS assumes responsibility for the security, availability, latency, and durability of the key material in your KMS keys.

KMS keys in external key stores rely on key material and operations in your external key manager. As such, the balance of responsibility shifts in your direction. You are responsible for the security, reliability, durability, and performance of the cryptographic keys in your external key manager. Amazon KMS is responsible for responding promptly to requests and communicating with your external key store proxy, and for maintaining our security standards. To ensure that every external key store ciphertext at least as strong than standard Amazon KMS ciphertext, Amazon KMS first encrypts all plaintext with Amazon KMS key material specific to your KMS key, and then sends it to your external key manager for encryption with your external key, a procedure known as [double encryption](#). As a result, neither Amazon KMS nor the owner of the external key material can decrypt double-encrypted ciphertext alone.

You are responsible for maintaining an external key manager that meet your regulatory and performance standards, for supplying and maintaining an external key store proxy that conforms to the [Amazon KMS External Key Store Proxy API Specification](#), and for ensuring the availability and durability of your key material. You must also create, configure, and maintain an external key store. When errors arise that are caused by components that you maintain, you must be prepared to identify and resolve the errors so that Amazon services can access your resources without undue disruption. Amazon KMS provides [troubleshooting guidance](#) to help you determine the cause of problems and the most likely resolutions.

Review the [Amazon CloudWatch metrics and dimensions](#) that Amazon KMS records for external key stores. Amazon KMS strongly recommends that you create CloudWatch alarms to monitor your external key store so you can detect the early signs of performance and operational problems before they occur.

What is changing?

External key stores support only symmetric encryption KMS keys. Within Amazon KMS, you use and manage KMS keys in an external key store in much the same way that you manage other [customer managed keys](#), including [setting access control policies](#) and [monitoring key use](#). You use the same APIs with the same parameters to request a cryptographic operation with a KMS key in an external key store that you use for any KMS key. Pricing is also the same as for standard KMS keys. For details, see [KMS keys in external key stores](#) and [Amazon Key Management Service Pricing](#).

However, with external key stores the following principles change:

- You are responsible for the availability, durability, and latency of key operations.
- You are responsible for all costs for developing, purchasing, operating, and licensing your external key manager system.
- You can implement [independent authorization](#) of all requests from Amazon KMS to your external key store proxy.
- You can monitor, audit, and log all operations of your external key store proxy, and all operations of your external key manager related to Amazon KMS requests.

Where do I start?

To create and manage an external key store, you need to [choose your external key store proxy connectivity option](#), [assemble the prerequisites](#), and [create and configure your external key store](#).

Quotas

Amazon KMS allows up to [10 custom key stores](#) in each Amazon Web Services account and Region, including both [Amazon CloudHSM key stores](#) and [external key stores](#), regardless of their connection state. In addition, there are Amazon KMS request quotas on the [use of KMS keys in an external key store](#).

If you choose [VPC proxy connectivity](#) for your external key store proxy, there might also be quotas on the required components, such as VPCs, subnets, and network load balancers. For information about these quotas, use the [Service Quotas console](#).

Regions

To minimize network latency, create your external key store components in the Amazon Web Services Region closest to your [external key manager](#). If possible, choose a Region with a network round-trip time (RTT) of 35 milliseconds or less.

External key stores are supported in all Amazon Web Services Regions in which Amazon KMS is supported except for China (Beijing) and China (Ningxia).

Unsupported features

Amazon KMS does not support the following features in custom key stores.

- [Asymmetric KMS keys](#)
- [HMAC KMS keys](#)
- [KMS keys with imported key material](#)
- [Automatic key rotation](#)
- [Multi-Region keys](#)

Learn more:

- [Announcing Amazon KMS External Key Store](#) in the *Amazon News Blog*.

External key store concepts

Learn the basic terms and concepts used in external key stores.

External key store

An *external key store* is an Amazon KMS [custom key store](#) backed by an external key manager outside of Amazon that you own and manage. Each KMS key in an external key store is associated with an [external key](#) in your external key manager. When you use a KMS key in an external key store for encryption or decryption, the operation is performed in your external key manager using your external key, an arrangement known as *Hold your Own Keys* (HYOK). This feature is designed for organizations that are required to maintain their cryptographic keys in their own external key manager.

External key stores ensure that the cryptographic keys and operations that protect your Amazon resources remain in your external key manager under your control. Amazon KMS sends requests to your external key manager to encrypt and decrypt data, but Amazon KMS cannot create, delete, or manage any external keys. All requests from Amazon KMS to your external key manager are mediated by an [external key store proxy](#) software component that you supply, own, and manage.

Amazon services that support Amazon KMS [customer managed keys](#) can use the KMS keys in your external key store to protect your data. As a result, your data is ultimately protected by your keys using your encryption operations in your external key manager.

The KMS keys in an external key store have fundamentally different trust models, [shared responsibility arrangements](#), and performance expectations than standard KMS keys. With external key stores, you are responsible for the security and integrity of the key material and the

cryptographic operations. The availability and latency of KMS keys in an external key store are affected by the hardware, software, networking components, and the distance between Amazon KMS and your external key manager. You are also likely to incur additional costs for your external key manager and for the networking and load balancing infrastructure you need for your external key manager to communicate with Amazon KMS.

You can use your external key store as part of your broader data protection strategy. For each Amazon resource that you protect, you can decide which require a KMS key in an external key store and which can be protected by a standard KMS key. This gives you the flexibility to choose KMS keys for specific data classifications, applications, or projects.

External key manager

An *external key manager* is a component outside of Amazon that can generate 256-bit AES symmetric keys and perform symmetric encryption and decryption. The external key manager for an external key store can be a physical hardware security module (HSM), a virtual HSM, or a software key manager with or without an HSM component. It can be located anywhere outside of Amazon, including on your premises, in a local or remote data center, or in any cloud. Your external key store can be backed by a single external key manager or multiple related key manager instances that share cryptographic keys, such as an HSM cluster. External key stores are designed to support a variety of external managers from different vendors. For details about connecting to your external key manager, see [Choose an external key store proxy connectivity option](#).

External key

Each KMS key in an external key store is associated with a cryptographic key in your [external key manager](#) known as an *external key*. When you encrypt or decrypt with a KMS key in your external key store, the cryptographic operation is performed in your [external key manager](#) using your external key.

Warning

The external key is essential to the operation of the KMS key. If the external key is lost or deleted, ciphertext encrypted under the associated KMS key is unrecoverable.

For external key stores, an external key must be a 256-bit AES key that is enabled and can perform encryption and decryption. For detailed external key requirements, see [Requirements for a KMS key in an external key store](#).

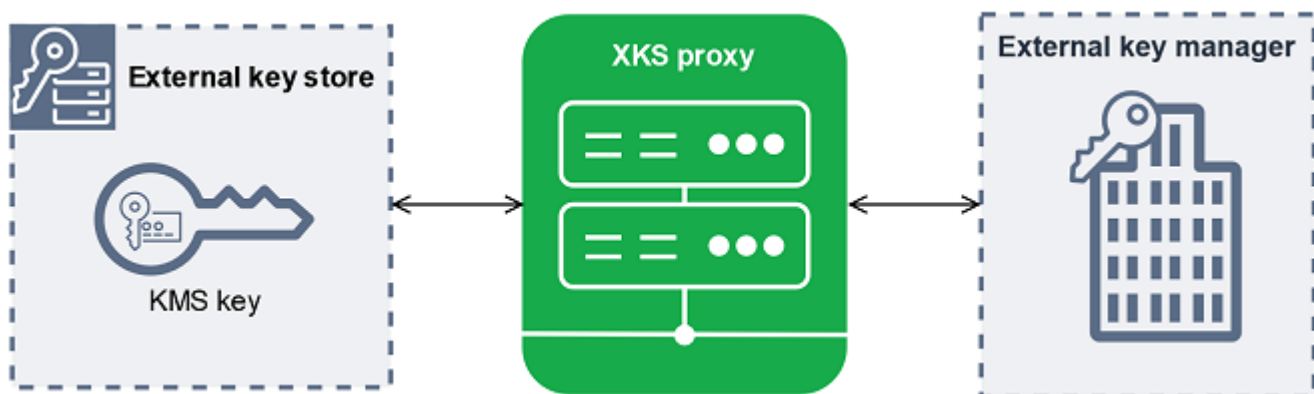
Amazon KMS cannot create, delete, or manage any external keys. Your cryptographic key material never leaves your external key manager. When you create a KMS key in an external key store, you provide the ID of an external key (XksKeyId). You cannot change the external key ID associated with a KMS key, although your external key manager can rotate the key material associated with the external key ID.

In addition to your external key, a KMS key in an external key store also has Amazon KMS key material. Data protected by the KMS key is encrypted first by Amazon KMS using the Amazon KMS key material, and then by your external key manager using your external key. This [double encryption](#) process ensures that ciphertext protected by your KMS key is always at least as strong as ciphertext protected only by Amazon KMS.

Many cryptographic keys have different types of identifiers. When creating a KMS key in an external key store, provide the ID of the external key that the [external key store proxy](#) uses to refer to the external key. If you use the wrong identifier, your attempt to create a KMS key in your external key store fails.

External key store proxy

The *external key store proxy* ("XKS proxy") is a customer-owned and customer-managed software application that mediates all communication between Amazon KMS and your external key manager. It also translates generic Amazon KMS requests into a format that your vendor-specific external key manager understand. An external key store proxy is required for an external key store. Each external key store is associated with one external key store proxy.



Amazon KMS cannot create, delete, or manage any external keys. Your cryptographic key material never leaves your external key manager. All communication between Amazon KMS and your external key manager is mediated by your external key store proxy. Amazon KMS sends requests to the external key store proxy and receives responses from the external key store proxy. The external

key store proxy is responsible for transmitting requests from Amazon KMS to your external key manager and transmitting responses from your external key manager back to Amazon KMS

You own and manage the external key store proxy for your external key store, and you are responsible for its maintenance and operation. You can develop your external key store proxy based on the open-source [external key store proxy API specification](#) that Amazon KMS publishes or purchase a proxy application from a vendor. Your external key store proxy might be included in your external key manager. To support proxy development, Amazon KMS also provides a sample external key store proxy ([aws-kms-xks-proxy](#)) and a test client ([xks-kms-xksproxy-test-client](#)) that verifies that your external key store proxy conforms to the specification.

To authenticate to Amazon KMS, the proxy uses server-side TLS certificates. To authenticate to your proxy, Amazon KMS signs all requests to your external key store proxy with a SigV4 [proxy authentication credential](#). Optionally, your proxy can enable mutual TLS (mTLS) for additional assurance that it only accepts requests from Amazon KMS.

Your external key store proxy must support HTTP/1.1 or later and TLS 1.2 or later with at least one of the following cipher suites:

- TLS_AES_256_GCM_SHA384 (TLS 1.3)
- TLS_CHACHA20_POLY1305_SHA256 (TLS 1.3)

Note

The Amazon GovCloud (US) Region does not support TLS_CHACHA20_POLY1305_SHA256.

- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (TLS 1.2)
- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 (TLS 1.2)

To create and use the KMS keys in your external key store, you must first [connect the external key store](#) to its external key store proxy. You can also disconnect your external key store from its proxy on demand. When you do, all KMS keys in the external key store become [unavailable](#); they cannot be used in any cryptographic operation.

External key store proxy connectivity

The external key store proxy connectivity ("XKS proxy connectivity") describes the method that Amazon KMS uses to communicate with your external key store proxy.

You specify your proxy connectivity option when you create your external key store, and it becomes a property of the external key store. You can change your proxy connectivity option by updating the custom key store property, but you must be certain that your external key store proxy can still access the same external keys.

Amazon KMS supports the following connectivity options:

- [Public endpoint connectivity](#) — Amazon KMS sends requests for your external key store proxy over the internet to a public endpoint that you control. This option is simple to create and maintain, but it might not fulfill the security requirements for every installation.
- [VPC endpoint service connectivity](#) — Amazon KMS sends requests to a Amazon Virtual Private Cloud (Amazon VPC) endpoint service that you create and maintain. You can host your external key store proxy inside your Amazon VPC, or host your external key store proxy outside of Amazon and use the Amazon VPC only for communication.

For details about the external key store proxy connectivity options, see [Choose an external key store proxy connectivity option](#).

External key store proxy authentication credential

To authenticate to your external key store proxy, Amazon KMS signs all requests to your external key store proxy with a [Signature V4 \(SigV4\)](#) authentication credential. You establish and maintain the authentication credential on your proxy, then provide this credential to Amazon KMS when you create your external store.

Note

The SigV4 credential that Amazon KMS uses to sign requests to the XKS proxy is unrelated to any SigV4 credentials associated with Amazon Identity and Access Management principals in your Amazon Web Services accounts. Do not reuse any IAM SigV4 credentials for your external key store proxy.

Each proxy authentication credential has two parts. You must provide both parts when creating an external key store or updating the authentication credential for your external key store.

- Access key ID: Identifies the secret access key. You can provide this ID in plaintext.

- **Secret access key:** The secret part of the credential. Amazon KMS encrypts the secret access key in the credential before storing it.

You can [edit the credential setting](#) at any time, such as when you enter incorrect values, when you change your credential on the proxy, or when your proxy rotates the credential. For technical details about Amazon KMS authentication to the external key store proxy, see [Authentication](#) in the Amazon KMS External Key Store Proxy API Specification.

To allow you to rotate your credential without disrupting the Amazon Web Services services that use KMS keys in your external key store, we recommend that the external key store proxy support at least two valid authentication credentials for Amazon KMS. This ensures that your previous credential continues to work while you provide your new credential to Amazon KMS.

To help you track the age of your proxy authentication credential, Amazon KMS defines an Amazon CloudWatch metric, [XksProxyCredentialAge](#). You can use this metric to create a CloudWatch alarm that notifies you when the age of your credential reaches a threshold you establish.

To provide additional assurance that your external key store proxy responds only to Amazon KMS, some external key proxies support mutual Transport Layer Security (mTLS). For details, see [mTLS authentication \(optional\)](#).

Proxy APIs

To support an Amazon KMS external key store, an [external key store proxy](#) must implement the required proxy APIs as described in the [Amazon KMS External Key Store Proxy API Specification](#). These proxy API requests are the only requests that Amazon KMS sends to the proxy. Although you never send these requests directly, knowing about them might help you fix any issues that might arise with your external key store or its proxy. For example, Amazon KMS includes information about the latency and success rates of these API calls in its [Amazon CloudWatch metrics](#) for external key stores. For details, see [Monitor external key stores](#).

The following table lists and describes each of the proxy APIs. It also includes the Amazon KMS operations that trigger a call to the proxy API and any Amazon KMS operation exceptions related to the proxy API.

Proxy API	Description	Related Amazon KMS operations
Decrypt	Amazon KMS sends the ciphertext to be decrypted, and the ID of the	Decrypt , ReEncrypt

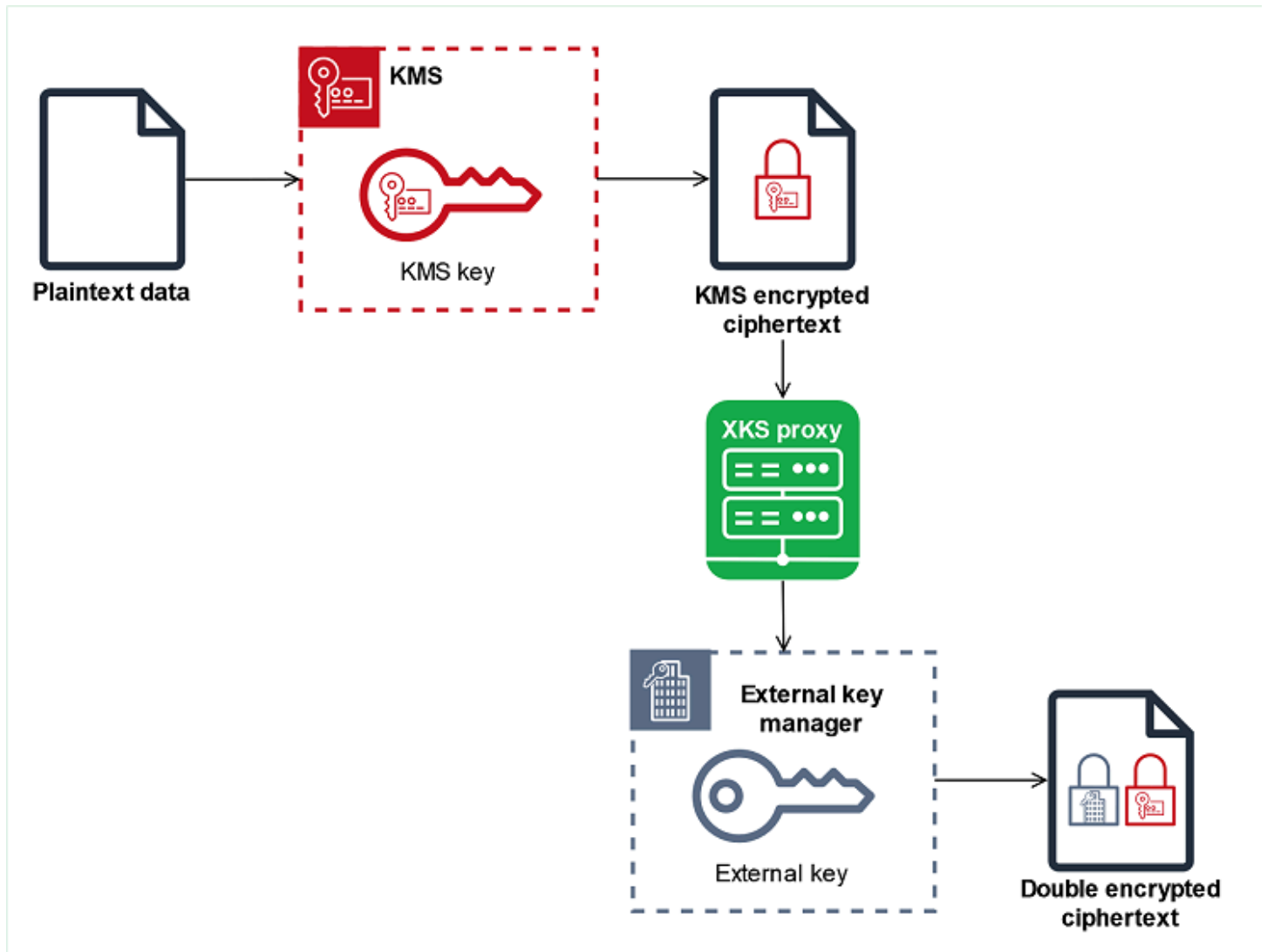
Proxy API	Description	Related Amazon KMS operations
	<p>external key to use. The required encryption algorithm is AES_GCM.</p>	
Encrypt	<p>Amazon KMS sends data to be encrypted, and the ID of the external key to use. The required encryption algorithm is AES_GCM.</p>	<p>Encrypt, GenerateDataKey, GenerateDataKeyWithoutPlaintext, ReEncrypt</p>
GetHealth Status	<p>Amazon KMS requests information about the status of the proxy and your external key manager.</p> <p>The status of each external key manager can be one of the following.</p> <ul style="list-style-type: none"> • Active: Healthy; can serve traffic • Degraded: Unhealthy, but can serve traffic • Unavailable : Unhealthy; cannot serve traffic 	<p>CreateCustomKeyStore (for public endpoint connectivity), ConnectCustomKeyStore (for VPC endpoint service connectivity)</p> <p>If all external key manager instances are Unavailable , attempts to create or connect the key store fail with XksProxyUriUnreachableException .</p>
GetKeyMetadata	<p>Amazon KMS requests information about the external key associated with a KMS key in your external key store.</p> <p>The response includes the key spec (AES_256), the key usage ([ENCRYPT, DECRYPT]), and the whether the external key is ENABLED or DISABLED.</p>	<p>CreateKey</p> <p>If the key spec is not AES_256, or the key usage is not [ENCRYPT, DECRYPT], or the status is DISABLED, the CreateKey operation fails with XksKeyInvalidConfigurationException .</p>

Double encryption

Data encrypted by a KMS key in an external key store is encrypted twice. First, Amazon KMS encrypts the data with Amazon KMS key material specific to the KMS key. Then the Amazon KMS-

encrypted ciphertext is encrypted by your [external key manager](#) using your [external key](#). This process is known as *double encryption*.

Double encryption ensures that data encrypted by a KMS key in an external key store is at least as strong as ciphertext encrypted by a standard KMS key. It also protects your plaintext in transit from Amazon KMS to your external key store proxy. With double encryption, you retain full control of your ciphertexts. If you permanently revoke Amazon access to your external key through your external proxy, any ciphertext remaining in Amazon is effectively crypto-shredded.



To enable double encryption, each KMS key in an external key store has *two* cryptographic backing keys:

- An Amazon KMS key material unique to the KMS key. This key material is generated and only used in Amazon KMS [FIPS 140-3 Security Level 3](#) certified hardware security modules (HSMs).

- An [external key](#) in your external key manager.

Double encryption has the following effects:

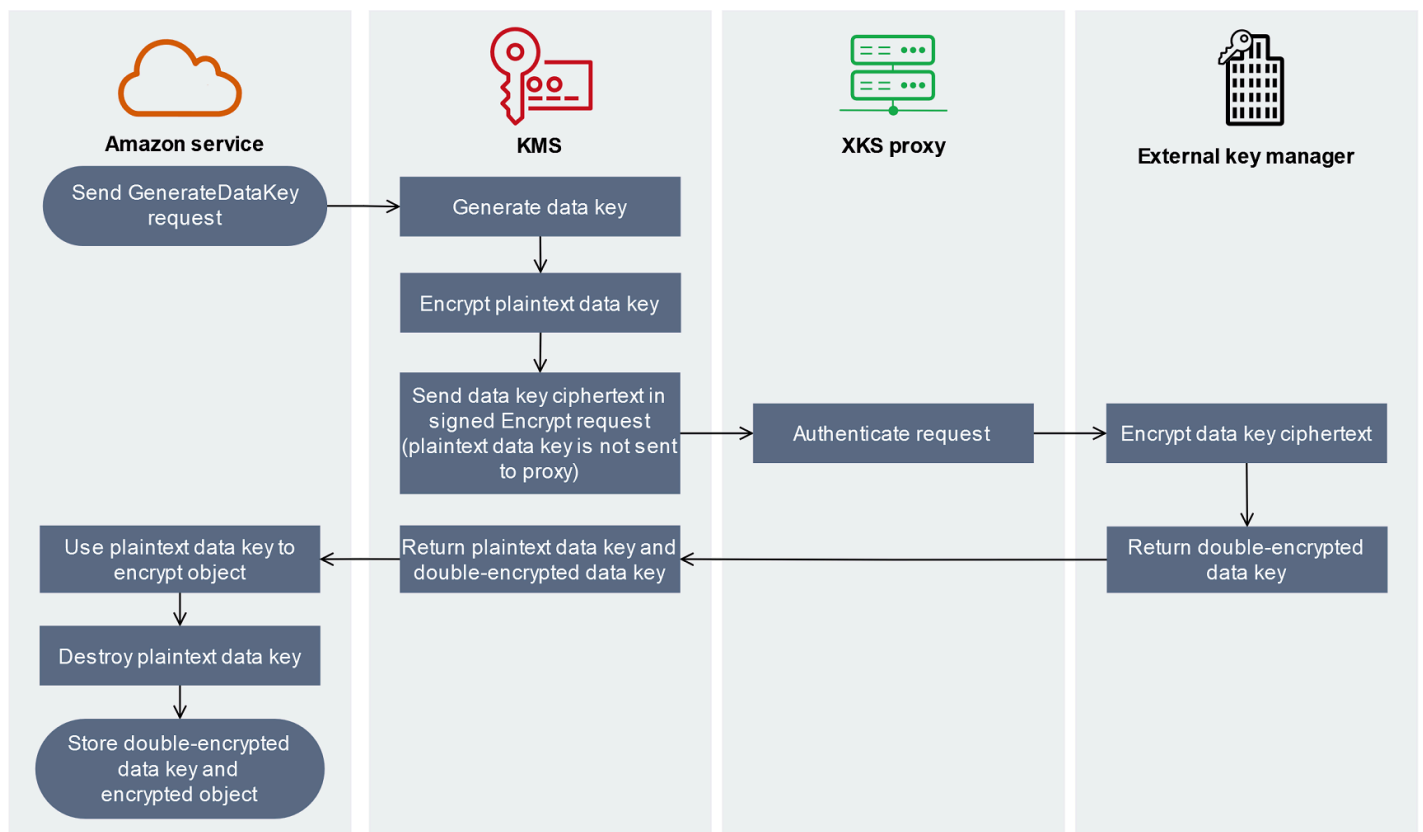
- Amazon KMS cannot decrypt any ciphertext encrypted by a KMS key in an external key store without access to your external keys via your external key store proxy.
- You cannot decrypt any ciphertext encrypted by a KMS key in an external key store outside of Amazon, even if you have its external key material.
- You cannot recreate a KMS key that was deleted from an external key store, even if you have its external key material. Each KMS key has unique metadata that it includes in the symmetric ciphertext. A new KMS key would not be able to decrypt ciphertext encrypted by the original key, even if it used the same external key material.

For an example of double encryption in practice, see [How external key stores work](#).

How external key stores work

Your [external key store](#), [external key store proxy](#), and [external key manager](#) work together to protect your Amazon resources. The following procedure depicts the encryption workflow of a typical Amazon Web Services service that encrypts each object under a unique data key protected by a KMS key. In this case, you've chosen a KMS key in an external key store to protect the object. The example shows how Amazon KMS uses [double encryption](#) to protect the data key in transit and ensure that ciphertext generated by a KMS key in an external key store is always at least as strong as ciphertext encrypted by a standard symmetric KMS key with key material in Amazon KMS.

The encryption methods used by each actual Amazon Web Services service that integrates with Amazon KMS vary. For details, see the "Data protection" topic in the Security chapter of the Amazon Web Services service documentation.



1. You add a new object to your Amazon Web Services service resource. To encrypt the object, the Amazon Web Services service sends a [GenerateDataKey](#) request to Amazon KMS using a KMS key in your external key store.
2. Amazon KMS generates a 256-bit symmetric [data key](#) and prepares to send a copy of the plaintext data key to your external key manager via your external key store proxy. Amazon KMS begins the [double encryption](#) process by encrypting the plaintext data key with the [Amazon KMS key material](#) associated with the KMS key in the external key store.
3. Amazon KMS sends an [encrypt](#) request to the external key store proxy associated with the external key store. The request includes the data key ciphertext to be encrypted and the ID of the [external key](#) that is associated with the KMS key. Amazon KMS signs the request using the [proxy authentication credential](#) for your external key store proxy.

The plaintext copy of the data key is not sent to the external key store proxy.

4. The external key store proxy authenticates the request, and then passes the encrypt request to your external key manager.

Some external key store proxies also implement an optional [authorization policy](#) that allows only selected principals to perform operations under specific conditions.

5. Your external key manager encrypts the data key ciphertext using the specified external key. The external key manager returns the double-encrypted data key to your external key store proxy, which returns it to Amazon KMS.
6. Amazon KMS returns the plaintext data key and the double-encrypted copy of that data key to the Amazon Web Services service.
7. The Amazon Web Services service uses the plaintext data key to encrypt the resource object, destroys the plaintext data key, and stores the encrypted data key with the encrypted object.

Some Amazon Web Services services might cache the plaintext data key to use for multiple objects, or to reuse while the resource is in use. For details, see [How unusable KMS keys affect data keys](#).

To decrypt the encrypted object, the Amazon Web Services service must send the encrypted data key back to Amazon KMS in a [Decrypt](#) request. To decrypt the encrypted data key, Amazon KMS must send the encrypted data key back to your external key store proxy with the ID of the external key. If the decrypt request to the external key store proxy fails for any reason, Amazon KMS cannot decrypt the encrypted data key, and the Amazon Web Services service cannot decrypt the encrypted object.

Control access to your external key store

All Amazon KMS access control features — [key policies](#), [IAM policies](#), and [grants](#) — that you use with standard KMS keys, work the same way for KMS keys in an external key store. You can use IAM policies to control access to the API operations that create and manage external key stores. You use IAM policies and key policies to control access to the Amazon KMS keys in your external key store. You can also use [service control policies](#) for your Amazon organization and [VPC endpoint policies](#) to control access to KMS keys in your external key store.

We recommend that you provide users and roles only the permissions that they require for the tasks that they are likely to perform.

Topics

- [Authorizing external key store managers](#)
- [Authorizing users of KMS keys in external key stores](#)

- [Authorizing Amazon KMS to communicate with your external key store proxy](#)
- [External key store proxy authorization \(optional\)](#)
- [mTLS authentication \(optional\)](#)

Authorizing external key store managers

Principals who create and manage an external key store need permissions to the custom key store operations. The following list describes the minimum permissions required for external key store managers. Because a custom key store is not an Amazon resource, you cannot provide permission to an external key store for principals in other Amazon Web Services accounts.

- `kms:CreateCustomKeyStore`
- `kms:DescribeCustomKeyStores`
- `kms:ConnectCustomKeyStore`
- `kms:DisconnectCustomKeyStore`
- `kms:UpdateCustomKeyStore`
- `kms>DeleteCustomKeyStore`

Principals who create an external key store need permission to create and configure the external key store components. Principals can create external key stores only in their own accounts. To create an external key store with [VPC endpoint service connectivity](#), principals must have permission to create the following components:

- An Amazon VPC
- Public and private subnets
- A network load balancer and target group
- An Amazon VPC endpoint service

For details, see [Identity and access management for Amazon VPC](#), [Identity and access management for VPC endpoints and VPC endpoint services](#) and [Elastic Load Balancing API permissions](#).

Authorizing users of KMS keys in external key stores

Principals who create and manage Amazon KMS keys in your external key store require [the same permissions](#) as those who create and manage any KMS key in Amazon KMS. The [default key policy](#)

for KMS key in an external key store is identical to the default key policy for KMS keys in Amazon KMS. [Attribute-based access control](#) (ABAC), which uses tags and aliases to control access to KMS keys, is also effective on KMS keys in an external key stores.

Principals who use the KMS keys in your custom key store for [cryptographic operations](#) need permission to perform the cryptographic operation with the KMS key, such as [kms:Decrypt](#). You can provide these permissions in an IAM or key policy. But, they do not need any additional permissions to use a KMS key in a custom key store.

To set a permission that applies only to KMS keys in an external key store, use the [kms:KeyOrigin](#) policy condition with a value of `EXTERNAL_KEY_STORE`. You can use this condition to limit the [kms:CreateKey](#) permission or any permission that is specific to a KMS key resource. For example, the following IAM policy allows the identity to which it is attached to call the specified operations on all KMS keys in the account, provided that the KMS keys are in an external key store. Notice that you can limit the permission to KMS keys in an external key store, and KMS keys in an Amazon Web Services account, but not to any particular external key store in the account.

```
{
  "Sid": "AllowKeysInExternalKeyStores",
  "Effect": "Allow",
  "Action": [
    "kms:Encrypt",
    "kms:Decrypt",
    "kms:ReEncrypt*",
    "kms:GenerateDataKey*",
    "kms:DescribeKey"
  ],
  "Resource": "arn:aws:kms:us-west-2:111122223333:key/*",
  "Condition": {
    "StringEquals": {
      "kms:KeyOrigin": "EXTERNAL_KEY_STORE"
    }
  }
}
```

Authorizing Amazon KMS to communicate with your external key store proxy

Amazon KMS communicates with your external key manager only through the [external key store proxy](#) that you provide. Amazon KMS authenticates to your proxy by signing its requests using the [Signature Version 4 \(SigV4\) process](#) with the [external key store proxy authentication credential](#) that

you specify. If you are using [public endpoint connectivity](#) for your external key store proxy, Amazon KMS does not require any additional permissions.

However, if you are using [VPC endpoint service connectivity](#), you must give Amazon KMS permission to create an interface endpoint to your Amazon VPC endpoint service. This permission is required regardless of whether the external key store proxy is in your VPC or the external key store proxy is located elsewhere, but uses the VPC endpoint service to communicate with Amazon KMS.

To allow Amazon KMS to create an interface endpoint, use the [Amazon VPC console](#) or the [ModifyVpcEndpointServicePermissions](#) operation. Allow permissions for the following principal: `cks.kms.<region>.amazonaws.com`.

For example, the following Amazon CLI command allows Amazon KMS to connect to the specified VPC endpoint service in the US West (Oregon) (us-west-2) Region. Before using this command, replace the Amazon VPC service ID and Amazon Web Services Region with valid values for your configuration.

```
modify-vpc-endpoint-service-permissions
--service-id vpce-svc-12abc34567def0987
--add-allowed-principals '["cks.kms.us-west-2.amazonaws.com"]'
```

To remove this permission, use the [Amazon VPC console](#) or the [ModifyVpcEndpointServicePermissions](#) with the `RemoveAllowedPrincipals` parameter.

External key store proxy authorization (optional)

Some external key store proxies implement authorization requirements for the use of its external keys. An external key store proxy is permitted, but not required, to design and implement an authorization scheme that allows particular users to request particular operations only under certain conditions. For example, a proxy might be configured to allow user A to encrypt with a particular external key, but not to decrypt with it.

Proxy authorization is independent of the [SigV4-based proxy authentication](#) that Amazon KMS requires for all external key store proxies. It is also independent of the key policies, IAM policies, and grants that authorize access to operations affecting the external key store or its KMS keys.

To enable authorization by the external key store proxy, Amazon KMS includes metadata in each [proxy API request](#), including the caller, the KMS key, the Amazon KMS operation, the Amazon Web

Services service (if any). The request metadata for version 1 (v1) of the external key proxy API is as follows.

```
"requestMetadata": {
  "awsPrincipalArn": string,
  "awsSourceVpc": string, // optional
  "awsSourceVpce": string, // optional
  "kmsKeyArn": string,
  "kmsOperation": string,
  "kmsRequestId": string,
  "kmsViaService": string // optional
}
```

For example, you might configure your proxy to allow requests from a particular principal (`awsPrincipalArn`), but only when the request is made on the principal's behalf by a particular Amazon Web Services service (`kmsViaService`).

If proxy authorization fails, the related Amazon KMS operation fails with a message that explains the error. For details, see [Proxy authorization issues](#).

mTLS authentication (optional)

To enable your external key store proxy to authenticate requests from Amazon KMS, Amazon KMS signs all requests to your external key store proxy with the Signature V4 (SigV4) [proxy authentication credential](#) for your external key store.

To provide additional assurance that your external key store proxy responds only to Amazon KMS requests, some external key proxies support *mutual Transport Layer Security* (mTLS), in which both parties to a transaction use certificates to authenticate to each other. mTLS adds client-side authentication — where the external key store proxy server authenticates the Amazon KMS client — to the server-side authentication that standard TLS provides. In the rare case that your proxy authentication credential is compromised, mTLS prevents a third party from making successful API requests to the external key store proxy.

To implement mTLS, configure your external key store proxy to accept only client-side TLS certificates with the following properties:

- The subject common name on the TLS certificate must be `cks.kms.<Region>.amazonaws.com`, for example, `cks.kms.eu-west-3.amazonaws.com`.
- The certificate must be chained to a certificate authority associated with [Amazon Trust Services](#).

Choose an external key store proxy connectivity option

Before creating your external key store, choose the connectivity option that determines how Amazon KMS communicates with your external key store components. The connectivity option that you choose determines the remainder of the planning process.

If you are creating an external key store, you need to determine how Amazon KMS communicates with your [external key store proxy](#). This choice will determine which components you need and how you configure them. Amazon KMS supports the following connectivity options. Choose the option that meets your performance and security goals.

Before you begin, [confirm that you need an external key store](#). Most customer can use KMS keys backed by Amazon KMS key material.

Note

If your external key store proxy is built into your external key manager, your connectivity might be predetermined. For guidance, consult the documentation for your external key manager or external key store proxy.

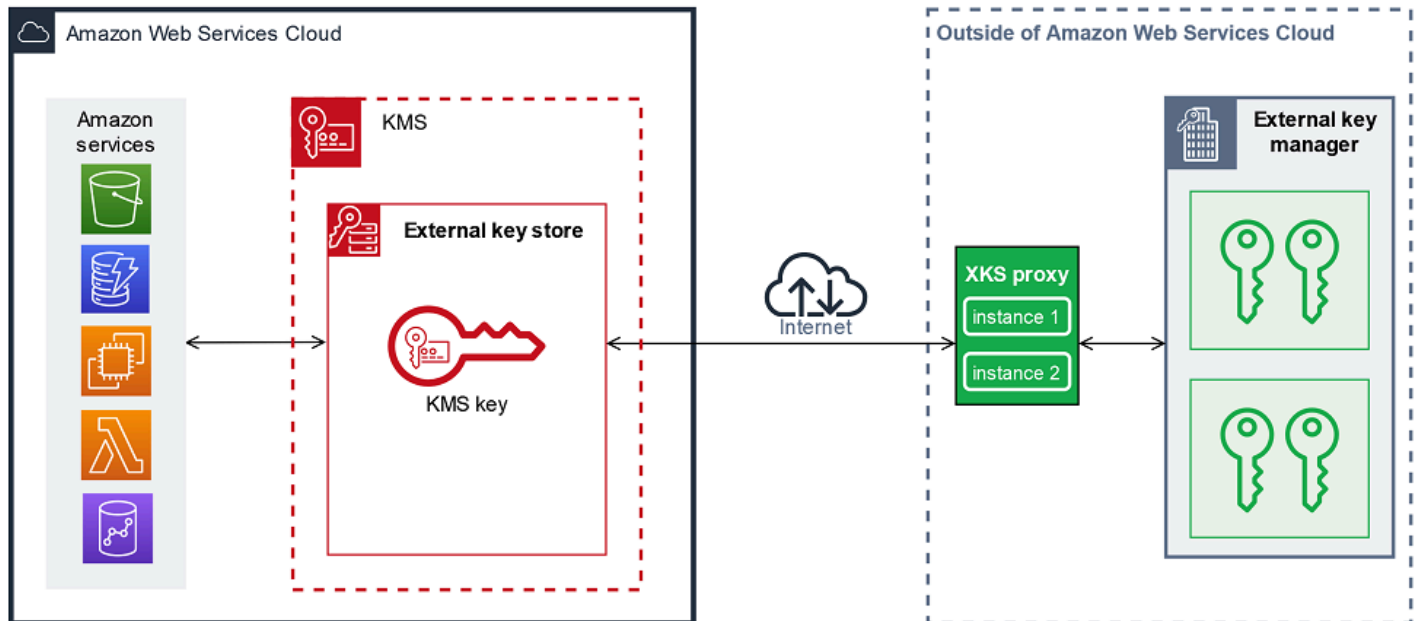
You can [change your external key store proxy connectivity option](#) even on an operating external key store. However, the process must be carefully planned and executed to minimize disruption, avoid errors, and ensure continued access to the cryptographic keys that encrypt your data.

Public endpoint connectivity

Amazon KMS connects to the external key store proxy (XKS proxy) over the internet using a public endpoint.

This connectivity option is easier to set up and maintain, and it aligns well with some models of key management. However, it might not fulfill the security requirements of some organizations.

XKS proxy connected by a public endpoint



Requirements

If you choose public endpoint connectivity, the following are required.

- Your external key store proxy must be reachable at a publicly routable endpoint.
- You can use the same public endpoint for multiple external key stores provided that they use different [proxy URI path](#) values.
- You cannot use the same endpoint for an external key store with public endpoint connectivity and any external key store with VPC endpoint services connectivity in the same Amazon Web Services Region, even if the key stores are in different Amazon Web Services accounts.
- You must obtain a TLS certificate issued by a public certificate authority supported for external key stores. For a list, see [Trusted Certificate Authorities](#).

The subject common name (CN) on the TLS certificate must match the domain name in the [proxy URI endpoint](#) for the external key store proxy. For example, if the public endpoint is `https://myproxy.xks.example.com`, the TLS, the CN on the TLS certificate must be `myproxy.xks.example.com` or `*.xks.example.com`.

- Ensure that any firewalls between Amazon KMS and the external key store proxy allow traffic to and from port 443 on the proxy. Amazon KMS communicates on port 443. This value is not configurable.

For all requirements for an external key store, see the [Assemble the prerequisites](#).

VPC endpoint service connectivity

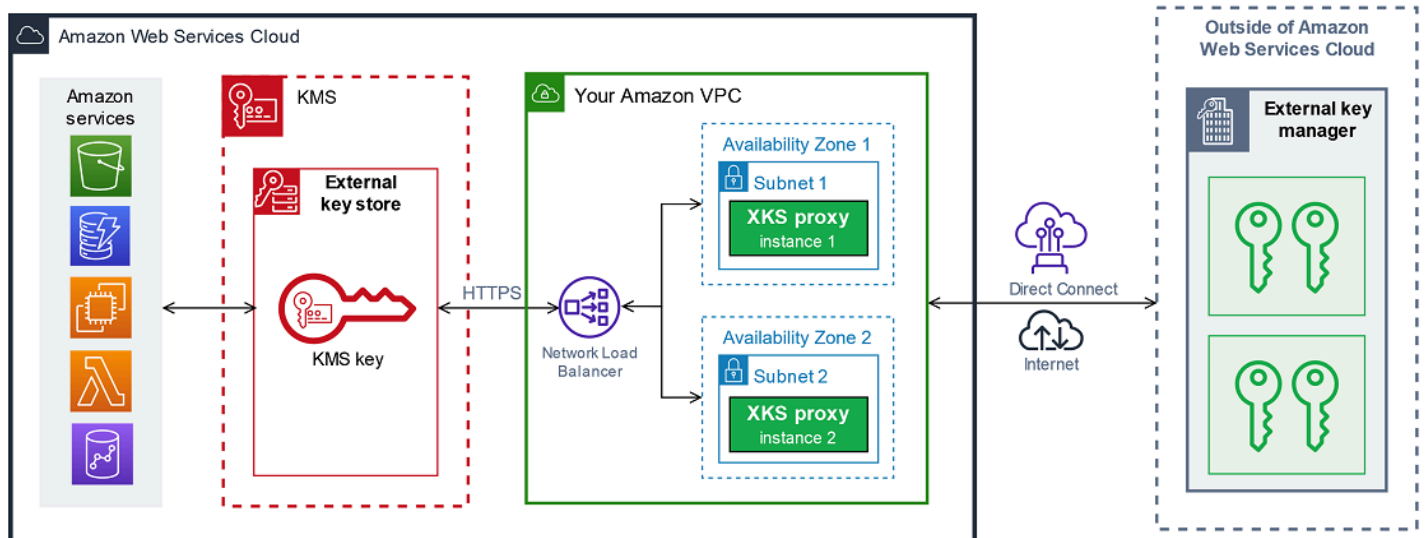
Amazon KMS connects to the external key store proxy (XKS proxy) by creating an interface endpoint to an Amazon VPC endpoint service that you create and configure. You are responsible for [creating the VPC endpoint service](#) and for connecting your VPC to your external key manager.

Your endpoint service can use any of the [supported network-to-Amazon VPC options](#) for communications, including [Amazon Direct Connect](#).

This connectivity option is more complicated to set up and maintain. But it uses Amazon PrivateLink, which enables Amazon KMS to privately connect to your Amazon VPC and your external key store proxy without using the public internet.

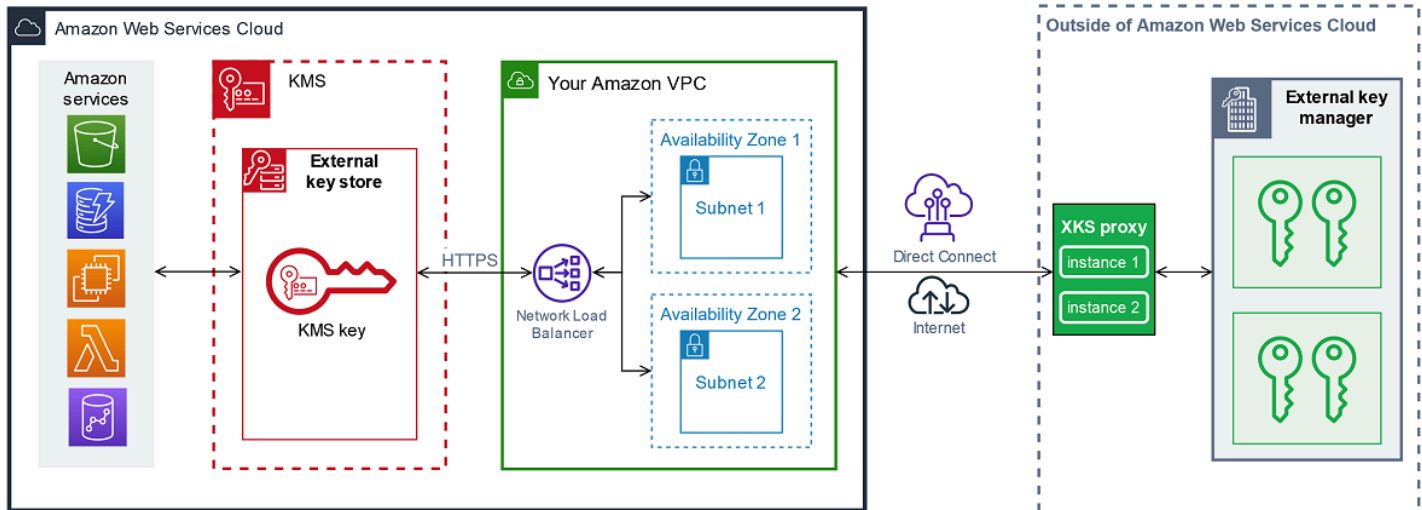
You can locate your external key store proxy in your Amazon VPC.

XKS proxy hosted in Amazon VPC



Or, locate your external key store proxy outside of Amazon and use your Amazon VPC endpoint service only for secure communication with Amazon KMS.

XKS proxy connected via Amazon VPC endpoint service



Learn more:

- Review the process for creating an external key store, including [assembling the prerequisites](#). It will help you to ensure that you have all of the components you need when you create your external key store.
- Learn how to [control access to your external key store](#), including the permissions that external key store administrators and users require.
- Learn about the [Amazon CloudWatch metrics and dimensions](#) that Amazon KMS records for external key stores. We strongly recommend that you create alarms to monitor your external key store so you can detect the early signs of performance and operational problems.

Configure VPC endpoint service connectivity

Use the guidance in this section to create and configure the Amazon resources and related components that are required for an external key store that uses [VPC endpoint service connectivity](#). The resources listed for this connectivity option are a supplement to the [resources required for all external key stores](#). After you create and configure the required resources, you can [create your external key store](#).

You can locate your external key store proxy in your Amazon VPC or locate the proxy outside of Amazon and use your VPC endpoint service for communication.

Before you begin, [confirm that you need an external key store](#). Most customer can use KMS keys backed by Amazon KMS key material.

Note

Some of the elements required for VPC endpoint service connectivity might be included in your external key manager. Also, your software might have additional configuration requirements. Before creating and configuring the Amazon resources in this section, consult your proxy and key manager documentation.

Topics

- [Requirements for VPC endpoint service connectivity](#)
- [Step 1: Create an Amazon VPC and subnets](#)
- [Step 2: Create a target group](#)
- [Step 3: Create a network load balancer](#)
- [Step 4: Create a VPC endpoint service](#)
- [Step 5: Verify your private DNS name domain](#)
- [Step 6: Authorize Amazon KMS to connect to the VPC endpoint service](#)

Requirements for VPC endpoint service connectivity

If you choose VPC endpoint service connectivity for your external key store, the following resources are required.

To minimize network latency, create your Amazon components in the [supported Amazon Web Services Region](#) that is closest to your [external key manager](#). If possible, choose a Region with a network round-trip time (RTT) of 35 milliseconds or less.

- An Amazon VPC that is connected to your external key manager. It must have at least two private [subnets](#) in two different Availability Zones.

You can use an existing Amazon VPC for your external key store, provided that it [fulfills the requirements](#) for use with an external key store. Multiple external key stores can share an Amazon VPC, but each external key store must have its own VPC endpoint service and private DNS name.

- An [Amazon VPC endpoint service powered by Amazon PrivateLink](#) with a [network load balancer](#) and [target group](#).

The endpoint service cannot require acceptance. Also, you must add Amazon KMS as an allowed principal. This allows Amazon KMS to create interface endpoints so it can communicate with your external key store proxy.

- A private DNS name for the VPC endpoint service that is unique in its Amazon Web Services Region.

The private DNS name must be a subdomain of a higher-level public domain. For example, if the private DNS name is `myproxy-private.xks.example.com`, it must be a subdomain of a public domain such as `xks.example.com` or `example.com`.

You must [verify ownership](#) of the DNS domain for private DNS name.

- A TLS certificate issued by a [supported public certificate authority](#) for your external key store proxy.

The subject common name (CN) on the TLS certificate must match the private DNS name. For example, if the private DNS name is `myproxy-private.xks.example.com`, the CN on the TLS certificate must be `myproxy-private.xks.example.com` or `*.xks.example.com`.

For all requirements for an external key store, see the [Assemble the prerequisites](#).

Step 1: Create an Amazon VPC and subnets

VPC endpoint service connectivity requires an Amazon VPC that is connected to your external key manager with at least two private subnets. You can create an Amazon VPC or use an existing Amazon VPC that fulfills the requirements for external key stores. For help with creating a new Amazon VPC, see [Create a VPC](#) in the *Amazon Virtual Private Cloud User Guide*.

Requirements for your Amazon VPC

To work with external key stores using VPC endpoint service connectivity, the Amazon VPC must have the following properties:

- Must be in the same Amazon Web Services account and [supported Region](#) as your external key store.
- Requires at least two private subnets, each in a different Availability Zone.
- The private IP address range of your Amazon VPC must not overlap with the private IP address range of the data center hosting your [external key manager](#).

- All components must use IPv4.

You have many options for connecting the Amazon VPC to your external key store proxy. Choose an option that meets your performance and security needs. For a list, see [Connect your VPC to other networks](#) and [Network-to-Amazon VPC connectivity options](#). For more details, see [Amazon Direct Connect](#), and the [Amazon Site-to-Site VPN User Guide](#).

Creating an Amazon VPC for your external key store

Use the following instructions to create the Amazon VPC for your external key store. An Amazon VPC is required only if you choose the [VPC endpoint service connectivity](#) option. You can use an existing Amazon VPC that fulfills the requirements for an external key store.

Follow the instructions in the [Create a VPC, subnets, and other VPC resources](#) topic using the following required values. For other fields, accept the default values and provide names as requested.

Field	Value
IPv4 CIDR block	Enter the IP addresses for your VPC. The private IP address range of your Amazon VPC must not overlap with the private IP address range of the data center hosting your external key manager .
Number of Availability Zones (AZs)	2 or more
Number of public subnets	None are required (0)
Number of private subnets	One for each AZ
NAT gateways	None are required.
VPC endpoints	None are required.
Enable DNS hostnames	Yes

Field	Value
Enable DNS resolution	Yes

Be sure to test your VPC communication. For example, if your external key store proxy is not located in your Amazon VPC, create an Amazon EC2 instance in your Amazon VPC, verify that the Amazon VPC can communicate with your external key store proxy.

Connecting the VPC to the external key manager

Connect the VPC to the data center that hosts your external key manager using any of the [network connectivity options](#) that Amazon VPC supports. Ensure that the Amazon EC2 instance in the VPC (or the external key store proxy, if it is in the VPC), can communicate with the data center and the external key manager.

Step 2: Create a target group

Before you create the required VPC endpoint service, create its required components, a network load balancer (NLB) and a target group. The network load balancer (NLB) distributes requests among multiple healthy targets, any of which can service the request. In this step, you create a target group with at least two hosts for your external key store proxy, and register your IP addresses with the target group.

Follow the instructions in the [Configure a target group](#) topic using the following required values. For other fields, accept the default values and provide names as requested.

Field	Value
Target type	IP addresses
Protocol	TCP
Port	443
IP address type	IPv4
VPC	Choose the VPC where you will create the VPC endpoint service for your external key store.

Field	Value
Health check protocol and path	Your health check protocol and path will differ with your external key store proxy configuration. Consult the documentation for your external key manager or external key store proxy. For general information about configuring health checks for your target groups, see Health checks for your target groups in the <i>Elastic Load Balancing User Guide for Network Load Balancers</i> .
Network	Other private IP address
IPv4 address	The private addresses of your external key store proxy
Ports	443

Step 3: Create a network load balancer

The network load balancer distributes the network traffic, including requests from Amazon KMS to your external key store proxy, to the configured targets.

Follow the instructions in the [Configure a load balancer and a listener](#) topic to configure and add a listener and create a load balancer using the following required values. For other fields, accept the default values and provide names as requested.

Field	Value
Scheme	Internal
IP address type	IPv4
Network mapping	Choose the VPC where you will create the VPC endpoint service for your external key store.
Mapping	Choose both of the availability zones (at least two) that you configured for your VPC subnets. Verify the subnet names and private IP address.
Protocol	TCP
Port	443

Field	Value
Default action: Forward to	Choose the target group for your network load balancer.

Step 4: Create a VPC endpoint service

Typically, you create an endpoint to a service. However, when you create a VPC endpoint service, you are the provider, and Amazon KMS creates an endpoint to your service. For an external key store, create a VPC endpoint service with the network load balancer that you created in the previous step. The VPC endpoint service must be in the same Amazon Web Services account and [supported Region](#) as your external key store.

Multiple external key stores can share an Amazon VPC, but each external key store must have its own VPC endpoint service and private DNS name.

Follow the instructions in the [Create an endpoint service](#) topic to create your VPC endpoint service with the following required values. For other fields, accept the default values and provide names as requested.

Field	Value
Load balancer type	Network
Available load balancers	Choose the network load balancer that you created in the previous step. If your new load balancer does not appear in the list, verify that its state is active. It might take a few minutes for the load balancer state to change from provisioning to active.
Acceptance required	False. Uncheck the check box. <i>Do not require acceptance.</i> Amazon KMS cannot connect to the VPC endpoint service without a manual acceptance. If acceptance is required, attempts to create the external key store fail with an <code>XksProxyInvalidConfigurationException</code> exception.

Field	Value
Enable private DNS name	Associate a private DNS name with the service
Private DNS name	<p>Enter a private DNS name that is unique in its Amazon Web Services Region.</p> <p>The private DNS name must be a subdomain of a higher level public domain. For example, if the private DNS name is <code>myproxy-private.xks.example.com</code>, it must be a subdomain of a public domain such as <code>xks.example.com</code> or <code>example.com</code>.</p> <p>This private DNS name must match the subject common name (CN) in the TLS certificate configured on your external key store proxy. For example, if the private DNS name is <code>myproxy-private.xks.example.com</code>, the CN on the TLS certificate must be <code>myproxy-private.xks.example.com</code> or <code>*.xks.example.com</code>.</p> <p>If the certificate and private DNS name do not match, attempts to connect an external key store to its external key store proxy fail with a connection error code of <code>XKS_PROXY_INVALID_TLS_CONFIGURATION</code>. For details, see General configuration errors.</p>
Supported IP address types	IPv4

Step 5: Verify your private DNS name domain

When you create your VPC endpoint service, its domain verification status is `pendingVerification`. Before using the VPC endpoint service to create an external key store, this status must be `verified`. To verify that you own the domain associated with your private DNS name, you must create a TXT record in a public DNS server.

For example, if the private DNS name for your VPC endpoint service is `myproxy-private.xks.example.com`, you must create a TXT record in a public domain, such as `xks.example.com` or `example.com`, whichever is public. Amazon PrivateLink looks for the TXT record first on `xks.example.com` and then on `example.com`.

Tip

After you add a TXT record, it might take a few minutes for the **Domain verification status** value to change from `pendingVerification` to `verify`.

To begin, find the verification status of your domain using either of the following methods. Valid values are `verified`, `pendingVerification`, and `failed`.

- In the [Amazon VPC console](#), choose **Endpoint services**, and choose your endpoint service. In the detail pane, see **Domain verification status**.
- Use the [DescribeVpcEndpointServiceConfigurations](#) operation. The `State` value is in the `ServiceConfigurations.PrivateDnsNameConfiguration.State` field.

If the verification status is not `verified`, follow the instructions in the [Domain ownership verification](#) topic to add a TXT record to your domain's DNS server and verify that the TXT record is published. Then check your verification status again.

You are not required to create an A record for the private DNS domain name. When Amazon KMS creates an interface endpoint to your VPC endpoint service, Amazon PrivateLink automatically creates a hosted zone with the required A record for the private domain name in the Amazon KMS VPC. For external key stores with VPC endpoint service connectivity, this happens when you [connect your external key store](#) to its external key store proxy.

Step 6: Authorize Amazon KMS to connect to the VPC endpoint service

You must add Amazon KMS to the **Allow principals** list for your VPC endpoint service. This allows Amazon KMS to create interface endpoints to your VPC endpoint service. If Amazon KMS is not an allowed principal, attempts to create an external key store will fail with an `XksProxyVpcEndpointServiceNotFoundException` exception.

Follow the instructions in the [Manage permissions](#) topic in the *Amazon PrivateLink Guide*. Use the following required value.

Field	Value
ARN	<code>cks.kms.<region>.amazonaws.com</code>

Field	Value
	For example, <code>cks.kms.us-east-1.amazonaws.com</code>

Next: [Create an external key store](#)

Create an external key store

You can create one or many external key stores in each Amazon Web Services account and Region. Each external key store must be associated with an external key manager outside of Amazon, and an external key store proxy (XKS proxy) that mediates communication between Amazon KMS and your external key manager. For details, see [Choose an external key store proxy connectivity option](#). Before you begin, [confirm that you need an external key store](#). Most customer can use KMS keys backed by Amazon KMS key material.

Tip

Some external key managers provide a simpler method for creating an external key store. For details, see your external key manager documentation.

Before you create your external key store, you need to [assemble the prerequisites](#). During the creation process, you specify the properties of your external key store. Most importantly, you indicate whether your external key store in Amazon KMS uses a [public endpoint](#) or a [VPC endpoint service](#) to connect to its external key store proxy. You also specify the connection details, including the URI endpoint of the proxy and the path within that proxy endpoint where Amazon KMS sends API requests to the proxy.

- If you use public endpoint connectivity, make sure that Amazon KMS can communicate with your proxy over the internet using an HTTPS connection. This includes configuring TLS on the external key store proxy and ensuring that any firewalls between Amazon KMS and the proxy allow traffic to and from port 443 on the proxy. While creating an external key store with public endpoint connectivity, Amazon KMS tests the connection by sending a status request to the external key store proxy. This test verifies that the endpoint is reachable and that your external key store proxy will accept a request signed with your [external key store proxy authentication credential](#). If this test request fails, the operation to create the external key store fails.

- If you use VPC endpoint service connectivity, make sure that the network load balancer, private DNS name, and VPC endpoint service are configured correctly and operational. If the external key store proxy isn't in the VPC, you need to ensure that the VPC endpoint service can communicate with the external key store proxy. (Amazon KMS tests VPC endpoint service connectivity when you [connect the external key store](#) to its external key store proxy.)

Additional considerations:

- Amazon KMS records [Amazon CloudWatch metrics and dimensions](#) especially for external key stores. Monitoring graphs based on some of these metrics appear in the Amazon KMS console for each external key store. We strongly recommend that you use these metrics to create alarms that monitor your external key store. These alarms alert you to early signs of performance and operational problems before they occur. For instructions, see [Monitor external key stores](#).
- External key stores are subject to [resource quotas](#). Use of KMS keys in an external key store are subject to [request quotas](#). Review these quotas before designing your external key store implementation.

Note

Review your configuration for circular dependencies that might prevent it from working. For example, if you create your external key store proxy using Amazon resources, make sure that operating the proxy does not require the availability of a KMS key in an external key store that is accessed via that proxy.

All new external key stores are created in a disconnected state. Before you can create KMS keys your external key store, you must [connect it](#) to its external key store proxy. To change the properties of your external key store, [edit your external key store settings](#).

Topics

- [Assemble the prerequisites](#)
- [Create a new external key store](#)

Assemble the prerequisites

Before you create an external key store, you need to assemble the required components, including the [external key manager](#) that you will use to support the external key store and the [external key store proxy](#) that translates Amazon KMS requests into a format that your external key manager can understand.

The following components are required for all external key stores. In addition to these components, you need to provide the components to support the [external key store proxy connectivity option](#) that you choose.

Tip

Your external key manager might include some of these components, or they might be configured for you. For details, see your external key manager documentation.

If you are creating your external key store in the Amazon KMS console, you have the option to upload a JSON-based [proxy configuration file](#) that specifies the [proxy URI path](#) and [proxy authentication credential](#). Some external key store proxies generate this file for you. For details, see the documentation for your external key store proxy or external key manager.

External key manager

Each external key store requires at least one [external key manager](#) instance. This can be a physical or virtual hardware security module (HSM), or key management software.

You can use a single key manager, but we recommend at least two related key manager instances that share cryptographic keys for redundancy. The external key store does not require exclusive use of the external key manager. However, the external key manager must have the capacity to handle the expected frequency of encryption and decryption requests from the Amazon services that use KMS keys in the external key store to protect your resources. Your external key manager should be configured to handle up to 1800 requests per second and to respond within the 250 millisecond timeout for each request. We recommend that you locate the external key manager close to an Amazon Web Services Region so that the network round-trip time (RTT) is 35 milliseconds or less.

If your external key store proxy allows it, you can change the external key manager that you associate with your external key store proxy, but the new external key manager must be a backup or snapshot with the same key material. If the external key that you associate with a KMS key is

no longer available to your external key store proxy, Amazon KMS cannot decrypt the ciphertext encrypted with the KMS key.

The external key manager must be accessible to the external key store proxy. If the [GetHealthStatus](#) response from the proxy reports that all external key manager instances are `Unavailable`, all attempts to create an external key store fail with an [XksProxyUriUnreachableException](#).

External key store proxy

You must specify an [external key store proxy](#) (XKS proxy) that conforms to the design requirements in the [Amazon KMS External Key Store Proxy API Specification](#). You can develop or buy an external key store proxy, or use an external key store proxy provided by or built into your external key manager. Amazon KMS recommends that your external key store proxy be configured to handle up to 1800 requests per second and respond within the 250 millisecond timeout for each request. We recommend that you locate the external key manager close to an Amazon Web Services Region so that the network round-trip time (RTT) is 35 milliseconds or less.

You can use an external key store proxy for more than one external key store, but each external key store must have a unique URI endpoint and path within the external key store proxy for its requests.

If you are using VPC endpoint service connectivity, you can locate your external key store proxy in your Amazon VPC, but that is not required. You can locate your proxy outside of Amazon, such as in your private data center, and use the VPC endpoint service only to communicate with the proxy.

Proxy authentication credential

To create an external key store, you must specify your external key store proxy authentication credential (`XksProxyAuthenticationCredential`).

You must establish an [authentication credential](#) (`XksProxyAuthenticationCredential`) for Amazon KMS on your external key store proxy. Amazon KMS authenticates to your proxy by signing its requests using the [Signature Version 4 \(SigV4\) process](#) with the external key store proxy authentication credential. You specify the authentication credential when you create your external key store and [you can change it](#) at any time. If your proxy rotates your credential, be sure to update the credential values for your external key store.

The proxy authentication credential has two parts. You must provide both parts for your external key store.

- **Access key ID:** Identifies the secret access key. You can provide this ID in plain text.
- **Secret access key:** The secret part of the credential. Amazon KMS encrypts the secret access key in the credential before storing it.

The SigV4 credential that Amazon KMS uses to sign requests to the external key store proxy are unrelated to any SigV4 credentials associated with any Amazon Identity and Access Management principals in your Amazon accounts. Do not reuse any IAM SigV4 credentials for your external key store proxy.

Proxy connectivity

To create an external key store, you must specify your external key store proxy connectivity option (`XksProxyConnectivity`).

Amazon KMS can communicate with your external key store proxy by using a [public endpoint](#) or an [Amazon Virtual Private Cloud \(Amazon VPC\) endpoint service](#). While a public endpoint is simpler to configure and maintain, it might not meet the security requirements for every installation. If you choose the Amazon VPC endpoint service connectivity option, you must create and maintain the required components, including an Amazon VPC with at least two subnets in two different Availability Zones, a VPC endpoint service with a network load balancer and target group, and a private DNS name for the VPC endpoint service.

You can [change the proxy connectivity option](#) for your external key store. However, you must ensure that the continued availability of the key material associated with the KMS keys in your external key store. Otherwise, Amazon KMS cannot decrypt any ciphertext encrypted with those KMS keys.

For help deciding which proxy connectivity option is best for your external key store, see [Choose an external key store proxy connectivity option](#). For help creating an configuring VPC endpoint service connectivity, see [Configure VPC endpoint service connectivity](#).

Proxy URI endpoint

To create an external key store, you must specify the endpoint (`XksProxyUriEndpoint`) that Amazon KMS uses to send requests to the external key store proxy.

The protocol must be HTTPS. Amazon KMS communicates on port 443. Do not specify the port in the proxy URI endpoint value.

- [Public endpoint connectivity](#) — Specify the publicly available endpoint for your external key store proxy. This endpoint must be reachable before you create your external key store.
- [VPC endpoint service connectivity](#) — Specify `https://` followed by the private DNS name of the VPC endpoint service.

The TLS server certificate configured on the external key store proxy must match the domain name in the external key store proxy URI endpoint and be issued by a certificate authority supported for external key stores. For a list, see [Trusted Certificate Authorities](#). Your certificate authority will require proof of domain ownership before issuing the TLS certificate.

The subject common name (CN) on the TLS certificate must match the private DNS name. For example, if the private DNS name is `myproxy-private.xks.example.com`, the CN on the TLS certificate must be `myproxy-private.xks.example.com` or `*.xks.example.com`.

You can [change your proxy URI endpoint](#), but be sure that the external key store proxy has access to the key material associated with the KMS keys in your external key store. Otherwise, Amazon KMS cannot decrypt any ciphertext encrypted with those KMS keys.

Uniqueness requirements

- The combined proxy URI endpoint (`XksProxyUriEndpoint`) and proxy URI path (`XksProxyUriPath`) value must be unique in the Amazon Web Services account and Region.
- External key stores with public endpoint connectivity can share the same proxy URI endpoint, provided that they have different proxy URI path values.
- An external key store with public endpoint connectivity cannot use the same proxy URI endpoint value as any external key store with VPC endpoint services connectivity in the same Amazon Web Services Region, even if the key stores are in different Amazon Web Services accounts.
- Each external key store with VPC endpoint connectivity must have its own private DNS name. The proxy URI endpoint (private DNS name) must be unique in the Amazon Web Services account and Region.

Proxy URI path

To create an external key store, you must specify the base path in your external key store proxy to the [required proxy APIs](#). The value must start with `/` and must end with `/kms/xks/v1` where `v1` represents the version of the Amazon KMS API for the external key store proxy. This path can

include an optional prefix between the required elements such as `/example-prefix/kms/xks/v1`. To find this value, see the documentation for your external key store proxy.

Amazon KMS sends proxy requests to the address specified by the concatenation of the proxy URI endpoint and proxy URI path. For example, if the proxy URI endpoint is `https://myproxy.xks.example.com` and the proxy URI path is `/kms/xks/v1`, Amazon KMS sends its proxy API requests to `https://myproxy.xks.example.com/kms/xks/v1`.

You can [change your proxy URI path](#), but be sure that the external key store proxy has access to the key material associated with the KMS keys in your external key store. Otherwise, Amazon KMS cannot decrypt any ciphertext encrypted with those KMS keys.

Uniqueness requirements

- The combined proxy URI endpoint (`XksProxyUriEndpoint`) and proxy URI path (`XksProxyUriPath`) value must be unique in the Amazon Web Services account and Region.

VPC endpoint service

Specifies the name of the Amazon VPC endpoint service that is used to communicate with your external key store proxy. This component is required only for external key stores that use VPC endpoint service connectivity. For help setting up and configuring your VPC endpoint service for an external key store, see [Configure VPC endpoint service connectivity](#).

The VPC endpoint service must have the following properties:

- The VPC endpoint service must be in the same Amazon Web Services account and Region as the external key store.
- It must have a network load balancer (NLB) connected to at least two subnets, each in a different Availability Zone.
- The *allow principals list* for the VPC endpoint service must include the Amazon KMS service principal for the Region: `cks.kms.<region>.amazonaws.com`, such as `cks.kms.us-east-1.amazonaws.com`.
- It must not require acceptance of connection requests.
- It must have a private DNS name within a higher level public domain. For example, you could have a private DNS name of `myproxy-private.xks.example.com` in the public `xks.example.com` domain.

The private DNS name for an external key store with VPC endpoint service connectivity must be unique in its Amazon Web Services Region.

- The [domain verification status](#) of the private DNS name domain must be verified.
- The TLS server certificate configured on the external key store proxy must specify the private DNS hostname at which the endpoint is reachable.

Uniqueness requirements

- External key stores with VPC endpoint connectivity can share an Amazon VPC, but each external key store must have its own VPC endpoint service and private DNS name.

Proxy configuration file

A *proxy configuration file* is an optional JSON-based file that contains values for the [proxy URI path](#) and [proxy authentication credential](#) properties of your external key store. When creating or [editing an external key store](#) in the Amazon KMS console, you can upload a proxy configuration file to supply configuration values for your external key store. Using this file avoids typing and pasting errors, and ensures that the values in your external key store match the values in your external key store proxy.

Proxy configuration files are generated by the external key store proxy. To learn whether your external key store proxy offers a proxy configuration file, see your external key store proxy documentation.

The following is an example of a well-formed proxy configuration file with fictitious values.

```
{
  "XksProxyUriPath": "/example-prefix/kms/xks/v1",
  "XksProxyAuthenticationCredential": {
    "AccessKeyId": "ABCDE12345670EXAMPLE",
    "RawSecretAccessKey": "0000EXAMPLEFA5FT0mCc3DrGUe2sti527BitkQ0Zr9M09+vE="
  }
}
```

You can upload a proxy configuration file only when creating or editing an external key store in the Amazon KMS console. You cannot use it with the [CreateCustomKeyStore](#) or [UpdateCustomKeyStore](#) operations, but you can use the values in the proxy configuration file to ensure that your parameter values are correct.

Create a new external key store

Once you've assembled the necessary prerequisites, you can create a new external key store in the Amazon KMS console or by using the [CreateCustomKeyStore](#) operation.

Using the Amazon KMS console

Before creating an external key store, [choose your proxy connectivity type](#) and ensure that you have created and configured all of the [required components](#). If you need help finding any of the required values, consult the documentation for your external key store proxy or key management software.

Note

When you create an external key store in the Amazon Web Services Management Console, you can upload a JSON-based *proxy configuration file* with values for the [proxy URI path](#) and [proxy authentication credential](#). Some proxies generate this file for you. It is not required.

1. Sign in to the Amazon Web Services Management Console and open the Amazon Key Management Service (Amazon KMS) console at <https://console.amazonaws.cn/kms>.
2. To change the Amazon Web Services Region, use the Region selector in the upper-right corner of the page.
3. In the navigation pane, choose **Custom key stores, External key stores**.
4. Choose **Create external key store**.
5. Enter a friendly name for the external key store. The name must be unique among all external key stores in your account.

Important

Do not include confidential or sensitive information in this field. This field may be displayed in plaintext in CloudTrail logs and other output.

6. Choose your [proxy connectivity](#) type.

Your proxy connectivity choice determines the [components required](#) for your external key store proxy. For help making this choice, see [Choose an external key store proxy connectivity option](#).

7. Choose or enter the name of the [VPC endpoint service](#) for this external key store. This step appears only when your external key store proxy connectivity type is **VPC endpoint service**.

The VPC endpoint service and its VPCs must fulfill the requirements for an external key store. For details, see [the section called "Assemble the prerequisites"](#).

8. Enter your [proxy URI endpoint](#). The protocol must be HTTPS. Amazon KMS communicates on port 443. Do not specify the port in the proxy URI endpoint value.

If Amazon KMS recognizes the VPC endpoint service that you specified in the previous step, it completes this field for you.

For public endpoint connectivity, enter a publicly available endpoint URI. For VPC endpoint connectivity, enter `https://` followed by the private DNS name of the VPC endpoint service.

9. To enter the values for the [proxy URI path](#) prefix and [proxy authentication credential](#), upload a proxy configuration file, or enter the values manually.
 - If you have an optional [proxy configuration file](#) that contains values for your [proxy URI path](#) and [proxy authentication credential](#), choose **Upload configuration file**. Follow the steps to upload the file.

When the file is uploaded, the console displays the values from the file in editable fields. You can change the values now or [edit these values](#) after the external key store is created.

To display the value of the secret access key, choose **Show secret access key**.

- If you don't have a proxy configuration file, you can enter the proxy URI path and proxy authentication credential values manually.
 - a. If you don't have a proxy configuration file, you can enter your proxy URI manually. The console supplies the required `/kms/xks/v1` value.

If your [proxy URI path](#) includes an optional prefix, such as the `example-prefix` in `/example-prefix/kms/xks/v1`, enter the prefix in the **Proxy URI path prefix** field. Otherwise, leave the field empty.

- b. If you don't have a proxy configuration file, you can enter your [proxy authentication credential](#) manually. Both the access key ID and secret access key are required.

- In **Proxy credential: Access key ID**, enter the access key ID of the proxy authentication credential. The access key ID identifies the secret access key.
- In **Proxy credential: Secret access key**, enter the secret access key of the proxy authentication credential.

To display the value of the secret access key, choose **Show secret access key**.

This procedure does not set or change the authentication credential you established on your external key store proxy. It just associates these values with your external key store. For information about setting, changing, and your rotating proxy authentication credential, see the documentation for your external key store proxy or key management software.

If your proxy authentication credential changes, [edit the credential setting](#) for your external key store.

10. Choose **Create external key store**.

When the procedure is successful, the new external key store appears in the list of external key stores in the account and Region. If it is unsuccessful, an error message appears that describes the problem and provides help on how to fix it. If you need more help, see [CreateKey errors for the external key](#).

Next: New external key stores are not automatically connected. Before you can create Amazon KMS keys in your external key store, you must [connect the external key store](#) to its external key store proxy.

Using the Amazon KMS API

You can use the [CreateCustomKeyStore](#) operation to create a new external key store. For help finding the values for the required parameters, see the documentation for your external key store proxy or key management software.

Tip

You cannot upload a [proxy configuration file](#) when using the `CreateCustomKeyStore` operation. However, you can use the values in the proxy configuration file to ensure that your parameter values are correct.

To create an external key store, the `CreateCustomKeyStore` operation requires the following parameter values.

- `CustomKeyStoreName` – A friendly name for the external key store that is unique in the account.

Important

Do not include confidential or sensitive information in this field. This field may be displayed in plaintext in CloudTrail logs and other output.

- `CustomKeyStoreType` — Specify `EXTERNAL_KEY_STORE`.
- [XksProxyConnectivity](#) – Specify `PUBLIC_ENDPOINT` or `VPC_ENDPOINT_SERVICE`.
- [XksProxyAuthenticationCredential](#) — Specify both the access key ID and the secret access key.
- [XksProxyUriEndpoint](#) — The endpoint that Amazon KMS uses to communicate with your external key store proxy.
- [XksProxyUriPath](#) — The path within the proxy to the proxy APIs.
- [XksProxyVpcEndpointServiceName](#) — Required only when your `XksProxyConnectivity` value is `VPC_ENDPOINT_SERVICE`.

Note

If you use Amazon CLI version 1.0, run the following command before specifying a parameter with an HTTP or HTTPS value, such as the `XksProxyUriEndpoint` parameter.

```
aws configure set cli_follow_urlparam false
```

Otherwise, Amazon CLI version 1.0 replaces the parameter value with the content found at that URI address, causing the following error:

```
Error parsing parameter '--xks-proxy-uri-endpoint': Unable to retrieve  
https:// : received non 200 status code of 404
```

The following examples use fictitious values. Before running the command, replace them with valid values for your external key store.

Create an external key store with public endpoint connectivity.

```
$ aws kms create-custom-key-store
  --custom-key-store-name ExampleExternalKeyStorePublic \
  --custom-key-store-type EXTERNAL_KEY_STORE \
  --xks-proxy-connectivity PUBLIC_ENDPOINT \
  --xks-proxy-uri-endpoint https://myproxy.xks.example.com \
  --xks-proxy-uri-path /kms/xks/v1 \
  --xks-proxy-authentication-credential
  AccessKeyId=<value>,RawSecretAccessKey=<value>
```

Create an external key store with VPC endpoint service connectivity.

```
$ aws kms create-custom-key-store
  --custom-key-store-name ExampleExternalKeyStoreVPC \
  --custom-key-store-type EXTERNAL_KEY_STORE \
  --xks-proxy-connectivity VPC_ENDPOINT_SERVICE \
  --xks-proxy-vpc-endpoint-service-name com.amazonaws.vpce.us-east-1.vpce-svc-
example \
  --xks-proxy-uri-endpoint https://myproxy-private.xks.example.com \
  --xks-proxy-uri-path /kms/xks/v1 \
  --xks-proxy-authentication-credential
  AccessKeyId=<value>,RawSecretAccessKey=<value>
```

When the operation is successful, `CreateCustomKeyStore` returns the custom key store ID, as shown in the following example response.

```
{
  "CustomKeyId": cks-1234567890abcdef0
}
```

If the operation fails, correct the error indicated by the exception, and try again. For additional help, see [Troubleshooting external key stores](#).

Next: To use the external key store, [connect it to its external key store proxy](#).

Edit external key store properties

You can edit selected properties of an existing external key store.

You can edit some properties while the external key store is connected or disconnected. For other properties, you must first [disconnect your external key store](#) from its external key store proxy. The [connection state](#) of the external key store must be DISCONNECTED. While your external key store is disconnected, you can manage the key store and its KMS keys, but you cannot create or use KMS keys in the external key store. To find the [connection state](#) of your external key store, use the [DescribeCustomKeyStores](#) operation or see the **General configuration** section on the detail page for the external key store.

Before updating the properties your external key store, Amazon KMS sends a [GetHealthStatus](#) request to the external key store proxy using the new values. If the request succeeds, it indicates that you can connect and authenticate to an external key store proxy with the updated property values. If the request fails, the edit operation fails with an exception that identifies the error.

When the edit operation completes, the updated property values for your external key store appear in the Amazon KMS console and the `DescribeCustomKeyStores` response. However, it can take up to five minutes for the changes to be fully effective.

If you edit your external key store in the Amazon KMS console, you have the option to upload a JSON-based [proxy configuration file](#) that specifies the [proxy URI path](#) and [proxy authentication credential](#). Some external key store proxies generate this file for you. For details, see the documentation for your external key store proxy or external key manager.







Warning

The updated property values must connect your external key store to a proxy for the same external key manager as the previous values, or for a backup or snapshot of the external key manager with the same cryptographic keys. If your external key store permanently loses its access to the external keys associated with its KMS keys, ciphertext encrypted under those external keys is unrecoverable. In particular, changing the proxy connectivity of an external key store can prevent Amazon KMS from accessing your external keys.

Tip

Some external key managers provide a simpler method for editing external key store properties. For details, see your external key manager documentation.

You can change the following properties of an external key store.

Editable external key store properties	Any connection state	Require Disconnected state
<p>Custom key store name</p> <p>A required friendly name for a custom key store.</p> <div data-bbox="115 457 847 772" style="border: 1px solid #f08080; border-radius: 10px; padding: 10px; margin: 10px 0;"> <p>⚠ Important</p> <p>Do not include confidential or sensitive information in this field. This field may be displayed in plaintext in CloudTrail logs and other output.</p> </div>		
<p>Proxy authentication credential (XksProxyAuthenticationCredential)</p> <p>(You must specify both the access key ID and the secret access key, even if you are changing only one element.)</p>		
<p>Proxy URI path (XksProxyUriPath)</p>		
<p>Proxy connectivity (XksProxyConnectivity)</p> <p>(You must also update the proxy URI endpoint. If you are changing to VPC endpoint service connectivity, you must specify a proxy VPC endpoint service name.)</p>		
<p>Proxy URI endpoint (XksProxyUriEndpoint)</p> <p>If you change the proxy endpoint URI, you might also need to change the associated TLS certificate.</p>		
<p>Proxy VPC endpoint service name (XksProxyVpcEndpointServiceName)</p>		

Editable external key store properties	Any connection state	Require Disconnected state
(This field is required for VPC endpoint service connectivity)		

Edit your external key store's properties

You can edit your external key store's properties in the Amazon KMS console or by using the [UpdateCustomKeyStore](#) operation.

Using the Amazon KMS console

When you edit an key store, you can change any or of the editable values. Some changes require that the external key store be disconnected from its external key store proxy.

If you are editing the proxy URI path or proxy authentication credential, you can enter the new values or upload an external key store [proxy configuration file](#) that includes the new values.

1. Sign in to the Amazon Web Services Management Console and open the Amazon Key Management Service (Amazon KMS) console at <https://console.amazonaws.cn/kms>.
2. To change the Amazon Web Services Region, use the Region selector in the upper-right corner of the page.
3. In the navigation pane, choose **Custom key stores, External key stores**.
4. Choose the row of the external key store you want to edit.
5. If necessary, disconnect the external key store from its external key store proxy. From the **Key store actions** menu, choose **Disconnect**.
6. From the **Key store actions** menu, choose **Edit**.
7. Change one or more of the editable external key store properties. You can also upload an external key store [proxy configuration file](#) with values for the proxy URI path and proxy authentication credential. You can use a proxy configuration file even if some values specified in the file haven't changed.
8. Choose **Update external key store**.
9. Review the warning, and if you decide to continue, confirm the warning, and then choose **Update external key store**.

When the procedure is successful, a message describes the properties that you edited. When it is unsuccessful, an error message appears that describes the problem and provides help on how to fix it.

10. If necessary, reconnect the external key store. From the **Key store actions** menu, choose **Connect**.

You can leave the external key store disconnected. But while it is disconnected, you cannot create KMS keys in the external key store or use the KMS keys in the external key store in [cryptographic operations](#).

Using the Amazon KMS API

To change the properties of an external key store, use the [UpdateCustomKeyStore](#) operation. You can change multiple properties of an external key store in the same operation. If the operation is successful, Amazon KMS returns an HTTP 200 response and a JSON object with no properties.

Use the `CustomKeyId` parameter to identify the external key store. Use the other parameters to change the properties. You cannot use a [proxy configuration file](#) with the `UpdateCustomKeyStore` operation. The proxy configuration file is supported only by the Amazon KMS console. However, you can use the proxy configuration file to help you determine the correct parameter values for your external key store proxy.

The examples in this section use the [Amazon Command Line Interface \(Amazon CLI\)](#), but you can use any supported programming language.

Before you begin, [if necessary, disconnect the external key store](#) from its external key store proxy. After updating, if necessary, you can [reconnect the external key store](#) to its external key store proxy. You can leave the external key store in the disconnected state, but you must reconnect it before you can create new KMS keys in the key store or use existing KMS keys in the key store for cryptographic operations.

Note

If you use Amazon CLI version 1.0, run the following command before specifying a parameter with an HTTP or HTTPS value, such as the `XksProxyUriEndpoint` parameter.

```
aws configure set cli_follow_urlparam false
```

Otherwise, Amazon CLI version 1.0 replaces the parameter value with the content found at that URI address, causing the following error:

```
Error parsing parameter '--xks-proxy-uri-endpoint': Unable to retrieve
https:// : received non 200 status code of 404
```

Change the name of the external key store

The first example uses the [UpdateCustomKeyStore](#) operation to change the friendly name of the external key store to `XksKeyStore`. The command uses the `CustomKeyStoreId` parameter to identify the custom key store and the `CustomKeyStoreName` to specify the new name for the custom key store. Replace all example values with actual values for your external key store.

```
$ aws kms update-custom-key-store --custom-key-store-id cks-1234567890abcdef0 --new-
custom-key-store-name XksKeyStore
```

Change the proxy authentication credential

The following example updates the proxy authentication credential that Amazon KMS uses to authenticate to the external key store proxy. You can use a command like this one to update the credential if it is rotated on your proxy.

Update the credential on your external key store proxy first. Then use this feature to report the change to Amazon KMS. (Your proxy will briefly support both the old and new credential so you have time to update your credential in Amazon KMS.)

You must always specify both the access key ID and the secret access key in the credential, even if only one value is changed.

The first two commands set variables to hold the credential values. The `UpdateCustomKeyStore` operations uses the `CustomKeyStoreId` parameter to identify the external key store. It uses the `XksProxyAuthenticationCredential` parameter with its `AccessKeyId` and `RawSecretAccessKey` fields to specify the new credential. Replace all example values with actual values for your external key store.

```
$ accessKeyId=access key id
$ secretAccessKey=secret access key
```



```
$ aws kms update-custom-key-store --custom-key-store-id cks-1234567890abcdef0 \  
  --xks-proxy-authentication-credential \  
    AccessKeyId=$accessKeyId,RawSecretAccessKey=$secretAccessKey
```

Change the proxy URI path

The following example updates the proxy URI path (XksProxyUriPath). The combination of the proxy URI endpoint and the proxy URI path must be unique in the Amazon Web Services account and Region. Replace all example values with actual values for your external key store.

```
$ aws kms update-custom-key-store --custom-key-store-id cks-1234567890abcdef0 \  
  --xks-proxy-uri-path /kms/xks/v1
```

Change to VPC endpoint service connectivity

The following example uses the [UpdateCustomKeyStore](#) operation to change the external key store proxy connectivity type to VPC_ENDPOINT_SERVICE. To make this change, you must specify the required values for VPC endpoint service connectivity, including the VPC endpoint service name (XksProxyVpcEndpointServiceName) and a proxy URI endpoint (XksProxyUriEndpoint) value that includes the private DNS name for the VPC endpoint service. Replace all example values with actual values for your external key store.

```
$ aws kms update-custom-key-store --custom-key-store-id cks-1234567890abcdef0 \  
  --xks-proxy-connectivity "VPC_ENDPOINT_SERVICE" \  
  --xks-proxy-uri-endpoint https://myproxy-private.xks.example.com \  
  --xks-proxy-vpc-endpoint-service-name com.amazonaws.vpce.us-east-1.vpce-  
svc-example
```

Change to public endpoint connectivity

The following example changes the external key store proxy connectivity type to PUBLIC_ENDPOINT. When you make this change, you must update the proxy URI endpoint (XksProxyUriEndpoint) value. Replace all example values with actual values for your external key store.

Note

VPC endpoint connectivity provides greater security than public endpoint connectivity. Before changing to public endpoint connectivity, consider other options, including locating your external key store proxy on premises and using the VPC only for communication.

```
$ aws kms update-custom-key-store --custom-key-store-id cks-1234567890abcdef0 \  
  --xks-proxy-connectivity "PUBLIC_ENDPOINT" \  
  --xks-proxy-uri-endpoint https://myproxy.xks.example.com
```

View external key stores

You can view external key stores in each account and Region by using the Amazon KMS console or by using the [DescribeCustomKeyStores](#) operation.

When you view an external key store, you can see the following:

- Basic information about the key store, including its friendly name, ID, key store type, and creation date.
- Configuration information for the [external key store proxy](#), including the [connectivity type](#), [proxy URI endpoint](#) and [path](#), and the [access key ID](#) of your current [proxy authentication credential](#).
- If the external key store proxy uses [VPC endpoint service connectivity](#), the console displays the name of the VPC endpoint service.
- The current [connection state](#).

Note

A connection state value of **Disconnected** indicates that the external key store has never been connected, or it was intentionally disconnected from its external key store proxy. However, if your attempts to use a KMS key in a connected external key store fail, that might indicate a problem with the external key store or its proxy. For help, see [External key store connection errors](#).

- A [Monitoring](#) section with graphs of [Amazon CloudWatch metrics](#) designed to help you detect and resolve issues with your external key store. For help interpreting the graphs, using them in

your planning and troubleshooting, and creating CloudWatch alarms based on the metrics in the graphs, see [Monitor external key stores](#).

External key store properties

The following properties of an external key store are visible in the Amazon KMS console and the [DescribeCustomKeyStores](#) response.

Custom key store properties

The following values appear in the **General configuration** section of the detail page for each custom key store. These properties apply to all custom key stores, including Amazon CloudHSM key stores and external key stores.

Custom key store ID

A unique ID that Amazon KMS assigns to the custom key store.

Custom key store name

A friendly name that you assign to the custom key store when you create it. You can change this value at any time.

Custom key store type

The type of custom key store. Valid values are Amazon CloudHSM (AWS_CLOUDHSM) or External key store (EXTERNAL_KEY_STORE). You cannot change the type after you create the custom key store.

Creation date

The date that the custom key store was created. This date is displayed in local time for the Amazon Web Services Region.

Connection state

Indicates whether the custom key store is connected to its backing key store. The connection state is DISCONNECTED only if the custom key store has never been connected to its backing key store, or it has been intentionally disconnected. For details, see [the section called "Connection state"](#).

External key store configuration properties

The following values appear in the **External key store proxy configuration** section of the detail page for each external key store and in the `XksProxyConfiguration` element of the [DescribeCustomKeyStores](#) response. For a detailed description of each field, including uniqueness requirements and help with determining the correct value for each field, see [the section called “Assemble the prerequisites”](#) in the *Creating an external key store* topic.

Proxy connectivity

Indicates whether the external key store uses [public endpoint connectivity](#) or [VPC endpoint service connectivity](#).

Proxy URI endpoint

The endpoint that Amazon KMS uses to connect to your [external key store proxy](#).

Proxy URI path

The path from the proxy URI endpoint where Amazon KMS sends [proxy API requests](#).

Proxy credential: Access key ID

Part of the [proxy authentication credential](#) that you establish on your external key store proxy. The access key ID identifies the secret access key in the credential.

Amazon KMS uses the SigV4 signing process and the proxy authentication credential to sign its requests to your external key store proxy. The credential in the signature allows the external key store proxy to authenticate requests on your behalf from Amazon KMS.

VPC endpoint service name

The name of the Amazon VPC endpoint service that supports your external key store. This value appears only when the external key store uses [VPC endpoint service connectivity](#). You can locate your external key store proxy in the VPC or use the VPC endpoint service to communicate securely with your external key store proxy.

View your external key store properties

You can view your external key store and its associated properties in the Amazon KMS console or by using the [DescribeCustomKeyStores](#) operation.

Using the Amazon KMS console

To view the external key stores in a given account and Region, use the following procedure.

1. Sign in to the Amazon Web Services Management Console and open the Amazon Key Management Service (Amazon KMS) console at <https://console.amazonaws.cn/kms>.
2. To change the Amazon Web Services Region, use the Region selector in the upper-right corner of the page.
3. In the navigation pane, choose **Custom key stores, External key stores**.
4. To view detailed information about an external key store, choose the key store name.

Using the Amazon KMS API

To view your external key stores, use the [DescribeCustomKeyStores](#) operation. By default, this operation returns all custom key stores in the account and Region. But you can use either the `CustomKeyId` or `CustomKeyName` parameter (but not both) to limit the output to a particular custom key store.

For custom key stores, the output consists of the custom key store ID, name, and type, and the [connection state](#) of the key store. If the connection state is `FAILED`, the output also includes a `ConnectionErrorCode` that describes the reason for the error. For help interpreting the `ConnectionErrorCode` for an external key store, see [Connection error codes for external key stores](#).

For external key stores, the output also includes the `XksProxyConfiguration` element. This element includes the [connectivity type](#), [proxy URI endpoint](#), [proxy URI path](#), and the access key ID of the [proxy authentication credential](#).

The examples in this section use the [Amazon Command Line Interface \(Amazon CLI\)](#), but you can use any supported programming language.

For example, the following command returns all custom key stores in the account and Region. You can use the `Limit` and `Marker` parameters to page through the custom key stores in the output.

```
$ aws kms describe-custom-key-stores
```

The following command uses the `CustomKeyName` parameter to get only the example external key store with the `ExampleXksPublic` friendly name. This example key store uses public endpoint connectivity. It is connected to its external key store proxy.

```
$ aws kms describe-custom-key-stores --custom-key-store-name ExampleXksPublic
{
  "CustomKeyStores": [
    {
      "CustomKeyStoreId": "cks-1234567890abcdef0",
      "CustomKeyStoreName": "ExampleXksPublic",
      "ConnectionState": "CONNECTED",
      "CreationDate": "2022-12-14T20:17:36.419000+00:00",
      "CustomKeyStoreType": "EXTERNAL_KEY_STORE",
      "XksProxyConfiguration": {
        "AccessKeyId": "ABCDE12345670EXAMPLE",
        "Connectivity": "PUBLIC_ENDPOINT",
        "UriEndpoint": "https://xks.example.com:6443",
        "UriPath": "/example/prefix/kms/xks/v1"
      }
    }
  ]
}
```

The following command gets an example external key store with VPC endpoint service connectivity. In this example, the external key store is connected to its external key store proxy.

```
$ aws kms describe-custom-key-stores --custom-key-store-name ExampleXksVpc
{
  "CustomKeyStores": [
    {
      "CustomKeyStoreId": "cks-9876543210fedcba9",
      "CustomKeyStoreName": "ExampleXksVpc",
      "ConnectionState": "CONNECTED",
      "CreationDate": "2022-12-13T18:34:10.675000+00:00",
      "CustomKeyStoreType": "EXTERNAL_KEY_STORE",
      "XksProxyConfiguration": {
        "AccessKeyId": "ABCDE98765432EXAMPLE",
        "Connectivity": "VPC_ENDPOINT_SERVICE",
        "UriEndpoint": "https://example-proxy-uri-endpoint-vpc",
        "UriPath": "/example/prefix/kms/xks/v1",
        "VpcEndpointServiceName": "com.amazonaws.vpce.us-east-1.vpce-svc-example"
      }
    }
  ]
}
```

A [ConnectionState](#) of `Disconnected` indicates that an external key store has never been connected or it was intentionally disconnected from its external key store proxy. However, if attempts to use a KMS key in a connected external key store fail, that might indicate a problem with the external key store proxy or other external components.

If the `ConnectionState` of the external key store is `FAILED`, the `DescribeCustomKeyStores` response includes a `ConnectionErrorCode` element that explains the reason for the error.

For example, in the following output, the `XKS_PROXY_TIMED_OUT` value indicates Amazon KMS can connect to the external key store proxy, but the connection failed because the external key store proxy did not respond to Amazon KMS in the time allotted. If you see this connection error code repeatedly, notify your external key store proxy vendor. For help with this and other connection error failures, see [Troubleshooting external key stores](#).

```
$ aws kms describe-custom-key-stores --custom-key-store-name ExampleXksVpc
{
  "CustomKeyStores": [
    {
      "CustomKeyId": "cks-9876543210fedcba9",
      "CustomKeyName": "ExampleXksVpc",
      "ConnectionState": "FAILED",
      "ConnectionErrorCode": "XKS_PROXY_TIMED_OUT",
      "CreationDate": "2022-12-13T18:34:10.675000+00:00",
      "CustomKeyType": "EXTERNAL_KEY_STORE",
      "XksProxyConfiguration": {
        "AccessKeyId": "ABCDE98765432EXAMPLE",
        "Connectivity": "VPC_ENDPOINT_SERVICE",
        "UriEndpoint": "https://example-proxy-uri-endpoint-vpc",
        "UriPath": "/example/prefix/kms/xks/v1",
        "VpcEndpointServiceName": "com.amazonaws.vpce.us-east-1.vpce-svc-example"
      }
    }
  ]
}
```

Monitor external key stores

Amazon KMS collects metrics for each interaction with an external key store and publishes them in your CloudWatch account. These metrics are used to generate the graphs in the monitoring section of the detail page for each external key store. The following topic details how to use the graphs to identify and troubleshoot operational and configuration issues impacting your external

key store. We recommend using the CloudWatch metrics to set alarms that notify you when your external key store isn't performing as expected. For more information, see [Monitoring with Amazon CloudWatch](#).

Topics

- [Viewing the graphs](#)
- [Interpreting the graphs](#)

Viewing the graphs

You can view the graphs at different levels of detail. By default, each graph uses a three hour time range and five minute aggregation [period](#). You can adjust the graph view within the console, but your changes will revert to the default settings when the external key store detail page is closed or the browser is refreshed. For help with Amazon CloudWatch terminology, see [Amazon CloudWatch concepts](#).

View data point details

The data in each graph is collected by [Amazon KMS metrics](#). To view more information about a specific data point, pause the mouse over the data point on the line graph. This will display a pop-up with more information about the metric that the graph was derived from. Each list item displays the [dimension](#) value recorded at that data point. The pop-up displays a null value (–) if there is no metric data available for the dimension value at that data point. Some graphs record multiple dimensions and values for a single data point. Other graphs, like the [reliability graph](#), use the data collected by the metric to calculate a unique value. Each list item is associated with a different line graph color.

Modify the time range

To modify the [time range](#), select one of the predefined time ranges in the upper right corner of the monitoring section. The predefined time ranges span from 1 hour to 1 week (**1h**, **3h**, **12h**, **1d**, **3d**, or **1w**). This adjusts the time range for all graphs. If you want to view one specific graph in a different time range, or if you want to set a custom time range, enlarge the graph or view it in the Amazon CloudWatch console.

Zoom in on graphs

You can use the [mini-map zoom feature](#) to focus on sections of line graphs and stacked portions of the graphs without changing between zoomed-in and zoomed-out views. For example, you can

use the mini-map zoom feature to focus on a peak in a graph, so that you can compare the spike against other graphs in the monitoring section from the same timeline.

1. Choose and drag on the area of the graph that you want to focus on, and then release the drag.
2. To reset the zoom, choose the **Reset zoom** icon, which looks like a magnifying glass with a minus (-) symbol inside.

Enlarge a graph

To enlarge a graph, select the menu icon in the upper right corner of an individual graph and choose **Enlarge**. You can also select the enlarge icon that appears next to the menu icon when you hover over a graph.

Enlarging a graph enables you to further modify the view of a graph by specifying a different period, custom time range, or refresh interval. These changes will revert to the default settings when you close the enlarged view.

Modify the period

1. Choose the **Period options** menu. By default, this menu displays the value: **5 minutes**.
2. Choose a period, the predefined periods span from 1 second to 30 days.

For example, you can choose a one-minute view, which can be useful when troubleshooting. Or, choose a less detailed, one-hour view. That can be useful when viewing a broader time range (for example, 3 days) so that you can see trends over time. For more information, see [Periods](#) in the *Amazon CloudWatch User Guide*.

Modify the time range or time zone

1. Select one of the predefined time ranges, which span from 1 hour to 1 week (**1h**, **3h**, **12h**, **1d**, **3d**, or **1w**). Alternatively, you can choose **Custom** to set your own time range.
2. Choose **Custom**
 - a. *Time range*: select the **Absolute** tab in the upper left corner of the box. Use the calendar picker or text field boxes to specify a time range.
 - b. *Time zone*: choose the dropdown in the upper right corner of the box. You can change the time zone to **UTC** or **Local time zone**.
3. After you specify a time range, choose **Apply**.

Modify how often the data in your graph is refreshed

1. Choose the **Refresh options** menu in the upper-right corner.
2. Choose a refresh interval (**Off**, **10 Seconds**, **1 Minute**, **2 Minutes**, **5 Minutes**, or **15 Minutes**).

View graphs in the Amazon CloudWatch console

The graphs in the monitoring section are derived from predefined metrics that Amazon KMS publishes to Amazon CloudWatch. You can open them within the CloudWatch console and save them to CloudWatch dashboards. If you have multiple external key stores, you can open their respective graphs in CloudWatch and save them to a single dashboard to compare their health and usage.

Add to CloudWatch dashboard

Select **Add to dashboard** in the upper right corner to add all of the graphs to an Amazon CloudWatch dashboard. You can either select an existing dashboard or create a new one. For information on using this dashboard to create customized views of the graphs and alarms, see [Using Amazon CloudWatch dashboards](#) in the *Amazon CloudWatch User Guide*.

View in CloudWatch metrics

Select the menu icon in the upper right corner of an individual graph and choose **View in metrics** to view this graph in the Amazon CloudWatch console. From the CloudWatch console, you can add this single graph to a dashboard and modify time ranges, periods, and refresh intervals. For more information see, [Graphing metrics](#) in the *Amazon CloudWatch User Guide*.

Interpreting the graphs

Amazon KMS provides several graphs to monitor the health of your external key store within the Amazon KMS console. These graphs are automatically configured and derived from [Amazon KMS metrics](#).

The graph data is collected as part of the calls you make to your external key store and external keys. You might see data populating graphs during a time range that you did not make any calls, this data comes from the periodic `GetHealthStatus` calls that Amazon KMS makes on your behalf to check the status of your external key store proxy and external key manager. If your graphs display the message **No data available**, then there were no calls recorded during that time range or your external key store is in a [DISCONNECTED](#) state. You might be able to identify the time your external key store disconnected by [adjusting your view](#) to a broader time range.

Topics

- [Total requests](#)
- [Reliability](#)
- [Latency](#)
- [Top 5 exceptions](#)
- [Certificate days to expire](#)

Total requests

The total number of Amazon KMS requests being received for a specific external key store during a given time range. Use this graph to determine if you are at risk of throttling.

Amazon KMS recommends that your external key manager be able to handle up to 1800 requests for cryptographic operations per second. If you approach 540,000 calls in a five-minute period, you are at risk of throttling.

You can monitor the number of requests for cryptographic operations on KMS keys in your external key store that Amazon KMS throttles with the [ExternalKeyStoreThrottle](#) metric.

If you are getting very frequent `KMSInvalidStateException` errors with a message that explains that the request was rejected "due to a very high request rate," it might indicate that your external key manager or external key store proxy cannot keep pace with the current request rate. If possible, lower your request rate. You might also consider requesting a decrease in your custom key store request quota value. Decreasing this quota value might increase throttling, but it indicates that Amazon KMS is rejecting excess requests quickly before they are sent to your external key store proxy or external key manager. To request a quota decrease, please visit [Amazon Web Services Support Center](#) and create a case.

The total requests graph is derived from the [XksProxyErrors](#) metric, which collects data on both the successful and unsuccessful responses that Amazon KMS receives from your external key store proxy. When you [view a specific data point](#), the pop-up displays the value of the `CustomKeyId` dimension alongside the total number of Amazon KMS requests recorded at that data point. The `CustomKeyId` will always be the same.

Reliability

The percentage of Amazon KMS requests for which the external key store proxy returned either a successful response or a non-retryable error. Use this graph to evaluate the operational health of your external key store proxy.

When the graph displays a value less than 100%, it indicates cases where the proxy either did not respond or responded with a retryable error. This can indicate problems with the network, slowness of the external key store proxy or external key manager, or implementation bugs.

If the request includes a bad credential and your proxy responds with an `AuthenticationFailedException`, the graph will still indicate 100% reliability because the proxy identified an incorrect value in the [external key store proxy API request](#), and therefore the failure is expected. If the percentage of your reliability graph is 100%, then your external key store proxy is responding as expected. If the graph displays a value less than 100%, then the proxy either responded with a retryable error or timed out. For example, if the proxy responds with a `ThrottlingException` due to a very high request rate, it will display a lower reliability percentage because the proxy was unable to identify a specific problem in the request that caused it to fail. This is because retryable errors are likely transient problems that can be resolved by retrying the request.

The following error responses will lower the reliability percentage. You can use the [Top 5 exceptions](#) graph and the [XksProxyErrors](#) metric to further monitor how frequently your proxy returns each retryable error.

- `InternalException`
- `DependencyTimeoutException`
- `ThrottlingException`
- `XksProxyUnreachableException`

The reliability graph is derived from the [XksProxyErrors](#) metric, which collects data on both the successful and unsuccessful responses that Amazon KMS receives from your external key store proxy. The reliability percentage will only lower if the response has an `ErrorType` value of `Retryable`. When you [view a specific data point](#), the pop-up displays the value of the `CustomKeyStoreId` dimension alongside the reliability percentage for Amazon KMS requests recorded at that data point. The `CustomKeyStoreId` will always be the same.

We recommend using the [XksProxyErrors](#) metric to create a CloudWatch alarm that notifies you of potential networking problems by alerting you when more than five retryable errors are recorded in a one minute period. For more information, see [Create an alarm for retryable errors](#).

Latency

The number of milliseconds it takes for an external key store proxy to respond to an Amazon KMS request. Use this graph to evaluate the performance of your external key store proxy and external key manager.

Amazon KMS expects the external key store proxy to respond to each request within 250 milliseconds. In the case of network timeouts, Amazon KMS will retry the request once. If the proxy fails a second time, the recorded latency is the combined timeout limit for both request attempts and the graph will display approximately 500 milliseconds. In all other cases where the proxy doesn't respond within the 250 millisecond timeout limit, the recorded latency is 250 milliseconds. If the proxy is frequently timing out on encryption and decryption operations, consult your external proxy administrator. For help troubleshooting latency problems, see [Latency and timeout errors](#).

Slow responses might also indicate that your external key manager cannot handle the current request traffic. Amazon KMS recommends that your external key manager be able to handle up to 1800 requests for cryptographic operations per second. If your external key manager cannot handle the 1800 requests per second rate, consider requesting a decrease in your [request quota for KMS keys in a custom key store](#). Requests for cryptographic operations using the KMS keys in your external key store will fail fast with a [throttling exception](#), rather than being processed and later rejected by your external key store proxy or external key manager.

The latency graph is derived from the [XksProxyLatency](#) metric. When you [view a specific data point](#), the pop-up displays the corresponding `KmsOperation` and `XksOperation` dimension values alongside the average latency recorded for the operations at that data point. The list items are ordered from highest latency to lowest.

We recommend using the [XksProxyLatency](#) metric to create a CloudWatch alarm that notifies you when your latency is approaching the timeout limit. For more information, see [Create an alarm for response timeout](#).

Top 5 exceptions

The top five exceptions for failed cryptographic and management operations during a given time range. Use this graph to track the most frequent errors, so you can prioritize your engineering effort.

This count includes exceptions that Amazon KMS received from the external key store proxy and the `XksProxyUnreachableException` that Amazon KMS returns internally when it cannot establish communication with the external key store proxy.

High rates of retryable errors might indicate networking errors, while high rates of non-retryable errors might indicate a problem with the configuration of your external key store. For example, a spike in `AuthenticationFailedExceptions` indicates a discrepancy between the authentication credentials configured in Amazon KMS and the external key store proxy. To view your external key store configuration, see [View external key stores](#). To edit your external key store settings, see [Edit external key store properties](#).

The exceptions that Amazon KMS receives from the external key store proxy are different from the exceptions that Amazon KMS returns when an operation fails. Amazon KMS cryptographic operations return an `KMSInvalidStateException` for all failures related to the external configuration or connection state of the external key store. To identify the problem, use the accompanying error message text.

The following table shows the exceptions that can appear in the top 5 exceptions graph and the corresponding exceptions that Amazon KMS returns to you.

Error type	Exception displayed in the graph	Exception that Amazon KMS returned to you
Non-retryable	<p>AccessDeniedException</p> <p>For troubleshooting help, see Proxy authorization issues.</p>	<p>CustomKeyStoreInvalidStateException in response to <code>CreateKey</code> operations.</p> <p>KMSInvalidStateException in response to cryptographic operations.</p>

Error type	Exception displayed in the graph	Exception that Amazon KMS returned to you
Non-retryable	<p>AuthenticationFailedException</p> <p>For troubleshooting help, see Authentication credential errors.</p>	<p>XksProxyIncorrectAuthenticationCredentialException in response to <code>CreateCustomKeyStore</code> and <code>UpdateCustomKeyStore</code> operations.</p> <p>CustomKeyStoreInvalidStateException in response to <code>CreateKey</code> operations.</p> <p>KMSInvalidStateException in response to cryptographic operations.</p>
Retryable	<p>DependencyTimeoutException</p> <p>For troubleshooting help, see Latency and timeout errors.</p>	<p>XksProxyUriUnreachableException in response to <code>CreateCustomKeyStore</code> and <code>UpdateCustomKeyStore</code> operations.</p> <p>CustomKeyStoreInvalidStateException in response to <code>CreateKey</code> operations.</p> <p>KMSInvalidStateException in response to cryptographic operations.</p>

Error type	Exception displayed in the graph	Exception that Amazon KMS returned to you
Retryable	<p>InternalException</p> <p>The external key store proxy rejected the request because it cannot communicate with the external key manager. Verify that the external key store proxy configuration is correct and that the external key manager is available.</p>	<p>XksProxyInvalidResponseException in response to <code>CreateCustomKeyStore</code> and <code>UpdateCustomKeyStore</code> operations.</p> <p>CustomKeyStoreInvalidStateException in response to <code>CreateKey</code> operations.</p> <p>KMSInvalidStateException in response to cryptographic operations.</p>
Non-retryable	<p>InvalidCiphertextException</p> <p>For troubleshooting help, see Decryption errors.</p>	<p>KMSInvalidStateException in response to cryptographic operations.</p>
Non-retryable	<p>InvalidKeyUsageException</p> <p>For troubleshooting help, see Cryptographic operation errors for the external key.</p>	<p>XksKeyInvalidConfigurationException in response to <code>CreateKey</code> operations.</p> <p>KMSInvalidStateException in response to cryptographic operations.</p>

Error type	Exception displayed in the graph	Exception that Amazon KMS returned to you
Non-retryable	<p>InvalidStateException</p> <p>For troubleshooting help, see Cryptographic operation errors for the external key.</p>	<p>XksKeyInvalidConfigurationException in response to CreateKey operations.</p> <p>KMSInvalidStateException in response to cryptographic operations.</p>
Non-retryable	<p>InvalidUriPathException</p> <p>For troubleshooting help, see General configuration errors.</p>	<p>XksProxyInvalidConfigurationException in response to CreateCustomKeyStore and UpdateCustomKeyStore operations.</p> <p>CustomKeyStoreInvalidStateException in response to CreateKey operations.</p> <p>KMSInvalidStateException in response to cryptographic operations.</p>
Non-retryable	<p>KeyNotFoundException</p> <p>For troubleshooting help, see External key errors.</p>	<p>XksKeyNotFoundException in response to CreateKey operations.</p> <p>KMSInvalidStateException in response to cryptographic operations.</p>

Error type	Exception displayed in the graph	Exception that Amazon KMS returned to you
Retryable	<p>ThrottlingException</p> <p>The external key store proxy rejected the request due to a very high request rate. Reduce the frequency of your calls using KMS keys in this external key store.</p>	<p>XksProxyUriUnreachableException in response to <code>CreateCustomKeyStore</code> and <code>UpdateCustomKeyStore</code> operations.</p> <p>CustomKeyStoreInvalidStateException in response to <code>CreateKey</code> operations.</p> <p>KMSInvalidStateException in response to cryptographic operations.</p>
Non-retryable	<p>UnsupportedOperationException</p> <p>For troubleshooting help, see Cryptographic operation errors for the external key.</p>	<p>XksKeyInvalidResponseException in response to <code>CreateKey</code> operations.</p> <p>KMSInvalidStateException in response to cryptographic operations.</p>

Error type	Exception displayed in the graph	Exception that Amazon KMS returned to you
Non-retryable	<p>ValidationException</p> <p>For troubleshooting help, see Proxy issues.</p>	<p>XksProxyInvalidResponseException in response to CreateCustomKeyStore and UpdateCustomKeyStore operations.</p> <p>CustomKeyStoreInvalidStateException in response to CreateKey operations.</p> <p>KMSInvalidStateException in response to cryptographic operations.</p>
Retryable	<p>XksProxyUnreachableException</p> <p>If you see this error repeatedly, verify that your external key store proxy is active and is connected to the network, and that its URI path and endpoint URI or VPC service name are correct in your external key store.</p>	<p>XksProxyUriUnreachableException in response to CreateCustomKeyStore and UpdateCustomKeyStore operations.</p> <p>CustomKeyStoreInvalidStateException in response to CreateKey operations.</p> <p>KMSInvalidStateException in response to cryptographic operations.</p>

The top 5 exceptions graph is derived from the [XksProxyErrors](#) metric. When you [view a specific data point](#), the pop-up displays the value of the ExceptionName dimension alongside the number

of times that the exception was recorded at that data point. The five list items are ordered from most frequent exception to least.

We recommend using the [XksProxyErrors](#) metric to create a CloudWatch alarm that notifies you of potential configuration problems by alerting you when more than five non-retryable errors are recorded in a one minute period. For more information, see [Create an alarm for non-retryable errors](#).

Certificate days to expire

The number of days until the TLS certificate for your external key store proxy endpoint (`XksProxyUriEndpoint`) expires. Use this graph to monitor upcoming expiration of your TLS certificate.

When the certificate expires, Amazon KMS cannot communicate with the external key store proxy. All data protected by KMS keys in your external key store becomes inaccessible until you renew the certificate.

The certificate days to expire graph is derived from the [XksProxyCertificateDaysToExpire](#) metric. We strongly recommend using this metric to create a CloudWatch alarm that notifies you about the upcoming expiration. Certificate expiration might prevent you from accessing your encrypted resources. Set the alarm to give your organization time to renew the certificate before it expires. For more information, see [Create an alarm for certificate expiration](#).

Connect and disconnect external key stores

New external key stores are not connected. To create and use Amazon KMS keys in your external key store, you need to connect your external key store to its [external key store proxy](#). You can connect and disconnect your external key store at any time, and [view its connection state](#).

While your external key store is disconnected, Amazon KMS cannot communicate with your external key store proxy. As a result, you can view and manage your external key store and its existing KMS keys. However, you cannot create KMS keys in your external key store, or use its KMS keys in cryptographic operations. You might need to disconnect your external key store at some point, such as when editing its properties, but plan accordingly. Disconnecting the key store might disrupt the operation of Amazon services that use its KMS keys.

You are not required to connect your external key store. You can leave an external key store in a disconnected state indefinitely and connect it only when you need to use it. However, you

might want to test the connection periodically to verify that the settings are correct and it can be connected.

When you disconnect a custom key store, the KMS keys in the key store become unusable right away (subject to eventual consistency). However, resources encrypted with [data keys](#) protected by the KMS key are not affected until the KMS key is used again, such as to decrypt the data key. This issue affects Amazon Web Services services, many of which use data keys to protect your resources. For details, see [How unusable KMS keys affect data keys](#).

Note

External key stores are in a DISCONNECTED state only when the key store has never been connected or you explicitly disconnect it. A CONNECTED state does not indicate that external key store or its supporting components are operating efficiently. For information about the performance of your external key store components, see the graphs in **Monitoring** section of the detail page for each external key store. For details, see [Monitor external key stores](#).

Your external key manager might provide additional methods of stopping and restarting communication between your Amazon KMS external key store and your external key store proxy, or between your external key store proxy and external key manager. For details, see your external key manager documentation.

Topics

- [Connection state](#)
- [Connect an external key store](#)
- [Disconnect an external key store](#)

Connection state

Connecting and disconnecting changes the *connection state* of your custom key store. Connection state values are the same for Amazon CloudHSM key stores and external key stores.

To view the connection state of your custom key store, use the [DescribeCustomKeyStores](#) operation or Amazon KMS console. **Connection state** appears in each custom key store table, in the **General configuration** section of the detail page for each custom key store, and on the **Cryptographic**

configuration tab of KMS keys in a custom key store. For details, see [View an Amazon CloudHSM key store](#) and [View external key stores](#).

An custom key store can have one of the following connection states:

- **CONNECTED:** The custom key store is connected to its backing key store. You can create and use KMS keys in the custom key store.

The *backing key store* for an Amazon CloudHSM key store is its associated Amazon CloudHSM cluster. The *backing key store* for an external key store is external key store proxy and the external key manager that it supports.

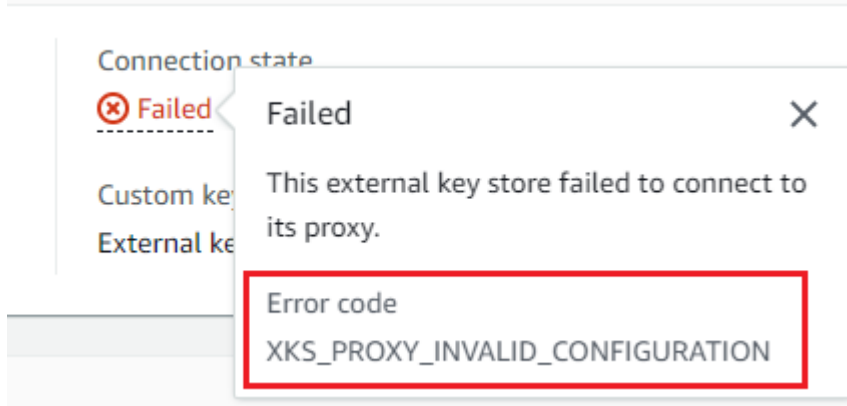
A **CONNECTED** state means that a connection succeeded and the custom key store has not been intentionally disconnected. It does not indicate that the connection is operating properly. For information about the status of the Amazon CloudHSM cluster associated with your Amazon CloudHSM key store, see [Getting CloudWatch metrics for Amazon CloudHSM](#) in the Amazon CloudHSM User Guide. For information about the status and operation of your external key store, see the graphs in the **Monitoring** section of the detail page for each external key store. For details, see [Monitor external key stores](#).

- **CONNECTING:** The process of connecting an custom key store is in progress. This is a transient state.
- **DISCONNECTED:** The custom key store has never been connected to its backing, or it was intentionally disconnected by using the Amazon KMS console or the [DisconnectCustomKeyStore](#) operation.
- **DISCONNECTING:** The process of disconnecting an custom key store is in progress. This is a transient state.
- **FAILED:** An attempt to connect the custom key store failed. The `ConnectionErrorCode` in the [DescribeCustomKeyStores](#) response indicates the problem.

To connect an custom key store, its connection state must be **DISCONNECTED**. If the connection state is **FAILED**, use the `ConnectionErrorCode` to identify and resolve the problem. Then disconnect the custom key store before trying to connect it again. For help with connection failures, see [External key store connection errors](#). For help responding to a connection error code, see [Connection error codes for external key stores](#).

To view the connection error code:

- In the [DescribeCustomKeyStores](#) response, view the value of the `ConnectionErrorCode` element. This element appears in the `DescribeCustomKeyStores` response only when the `ConnectionState` is `FAILED`.
- To view the connection error code in the Amazon KMS console, on detail page for the external key store and hover over the **Failed** value.



Connect an external key store

When your external key store is connected to its external key store proxy, you can [create KMS keys in your external key store](#) and use its existing KMS keys in [cryptographic operations](#).

The process that connects an external key store to its external key store proxy differs based on the connectivity of the external key store.

- When you connect an external key store with [public endpoint connectivity](#), Amazon KMS sends a [GetHealthStatus request](#) to the external key store proxy to validate the [proxy URI endpoint](#), [proxy URI path](#), and [proxy authentication credential](#). A successful response from the proxy confirms that the [proxy URI endpoint](#) and [proxy URI path](#) are accurate and accessible, and that the proxy authenticated the request signed with the [proxy authentication credential](#) for the external key store.
- When you connect an external key store with [VPC endpoint service connectivity](#) to its external key store proxy, Amazon KMS does the following:
 - Confirms that the domain for the private DNS name specified in the [proxy URI endpoint](#) is [verified](#).
 - Creates an interface endpoint from an Amazon KMS VPC to your VPC endpoint service.
 - Creates a private hosted zone for the private DNS name specified in the proxy URI endpoint

- Sends a [GetHealthStatus request](#) to the external key store proxy. A successful response from the proxy confirms that the [proxy URI endpoint](#) and [proxy URI path](#) are accurate and accessible, and that the proxy authenticated the request signed with the [proxy authentication credential](#) for the external key store.

The connect operation begins the process of connecting your custom key store, but connecting an external key store to its external proxy takes approximately five minutes. A success response from the connect operation does not indicate that the external key store is connected. To confirm that the connection was successful, use the Amazon KMS console or the [DescribeCustomKeyStores](#) operation to view the [connection state](#) of external your key store.

When the connection state is FAILED, a connection error code is displayed in the Amazon KMS console and is added to the DescribeCustomKeyStore response. For help interpreting connection error codes, see [Connection error codes for external key stores](#).

Connect and reconnect to your external key store

You can connect, or reconnect, your external key store in the Amazon KMS console or by using the [ConnectCustomKeyStore](#) operation.

Using the Amazon KMS console

You can use the Amazon KMS console to connect an external key store to its external key store proxy.

1. Sign in to the Amazon Web Services Management Console and open the Amazon Key Management Service (Amazon KMS) console at <https://console.amazonaws.cn/kms>.
2. To change the Amazon Web Services Region, use the Region selector in the upper-right corner of the page.
3. In the navigation pane, choose **Custom key stores, External key stores**.
4. Choose the row of the external key store you want to connect.

If the [connection state](#) of the external key store is **FAILED**, you must [disconnect the external key store](#) before you connect it.

5. From the **Key store actions** menu, choose **Connect**.

The connection process typically takes about five minutes to complete. When the operation completes, the [connection state](#) changes to **CONNECTED**.

If the connection state is **Failed**, hover over the connection state to see the *connection error code*, which explains the cause of the error. For help responding to a connection error code, see [Connection error codes for external key stores](#). To connect an external key store with a **Failed** connection state, you must first [disconnect the custom key store](#).

Using the Amazon KMS API

To connect a disconnected external key store, use the [ConnectCustomKeyStore](#) operation.

Before connecting, the [connection state](#) of the external key store must be DISCONNECTED. If the current connection state is FAILED, [disconnect the external key store](#), and then connect it.

The connection process takes about five minutes to complete. Unless it fails quickly, `ConnectCustomKeyStore` returns an HTTP 200 response and a JSON object with no properties. However, this initial response does not indicate that the connection was successful. To determine whether the external key store is connected, see the connection state in the [DescribeCustomKeyStores](#) response.

The examples in this section use the [Amazon Command Line Interface \(Amazon CLI\)](#), but you can use any supported programming language.

To identify the external key store, use its custom key store ID. You can find the ID on the **Custom key stores** page in the console or by using the [DescribeCustomKeyStores](#) operation. Before running this example, replace the example ID with a valid one.

```
$ aws kms connect-custom-key-store --custom-key-store-id cks-1234567890abcdef0
```

The `ConnectCustomKeyStore` operation does not return the `ConnectionState` in its response. To verify that the external key store is connected, use the [DescribeCustomKeyStores](#) operation. By default, this operation returns all custom keys stores in your account and Region. But you can use either the `CustomKeyStoreId` or `CustomKeyStoreName` parameter (but not both) to limit the response to particular custom key stores. A `ConnectionState` value of `CONNECTED` indicates that the external key store is connected to its external key store proxy.

```
$ aws kms describe-custom-key-stores --custom-key-store-name ExampleXksVpc
{
  "CustomKeyStores": [
    {
      "CustomKeyStoreId": "cks-9876543210fedcba9",
      "CustomKeyStoreName": "ExampleXksVpc",
```

```

    "ConnectionState": "CONNECTED",
    "CreationDate": "2022-12-13T18:34:10.675000+00:00",
    "CustomKeyStoreType": "EXTERNAL_KEY_STORE",
    "XksProxyConfiguration": {
      "AccessKeyId": "ABCDE98765432EXAMPLE",
      "Connectivity": "VPC_ENDPOINT_SERVICE",
      "UriEndpoint": "https://example-proxy-uri-endpoint-vpc",
      "UriPath": "/example/prefix/kms/xks/v1",
      "VpcEndpointServiceName": "com.amazonaws.vpce.us-east-1.vpce-svc-example"
    }
  }
]
}

```

If the `ConnectionState` value in the `DescribeCustomKeyStores` response is `FAILED`, the `ConnectionErrorCode` element indicates the reason for the failure.

In the following example, the `XKS_VPC_ENDPOINT_SERVICE_NOT_FOUND` value for the `ConnectionErrorCode` indicates that Amazon KMS can't find the VPC endpoint service that it uses to communicate with the external key store proxy. Verify that the `XksProxyVpcEndpointServiceName` is correct, the Amazon KMS service principal is an allowed principal on the Amazon VPC endpoint service, and that the VPC endpoint service does not require acceptance of connection requests. For help responding to a connection error code, see [Connection error codes for external key stores](#).

```

$ aws kms describe-custom-key-stores --custom-key-store-name ExampleXksVpc
{
  "CustomKeyStores": [
    {
      "CustomKeyId": "cks-9876543210fedcba9",
      "CustomKeyName": "ExampleXksVpc",
      "ConnectionState": "FAILED",
      "ConnectionErrorCode": "XKS_VPC_ENDPOINT_SERVICE_NOT_FOUND",
      "CreationDate": "2022-12-13T18:34:10.675000+00:00",
      "CustomKeyStoreType": "EXTERNAL_KEY_STORE",
      "XksProxyConfiguration": {
        "AccessKeyId": "ABCDE98765432EXAMPLE",
        "Connectivity": "VPC_ENDPOINT_SERVICE",
        "UriEndpoint": "https://example-proxy-uri-endpoint-vpc",
        "UriPath": "/example/prefix/kms/xks/v1",
        "VpcEndpointServiceName": "com.amazonaws.vpce.us-east-1.vpce-svc-example"
      }
    }
  ]
}

```

```
    }  
  ]  
}
```

Disconnect an external key store

When you disconnect an external key store with [VPC endpoint service connectivity](#) from its external key store proxy, Amazon KMS deletes its interface endpoint to the VPC endpoint service and removes the network infrastructure that it created to support the connection. No equivalent process is required for external key stores with public endpoint connectivity. This action does not affect the VPC endpoint service or any of its supporting components, and it does not affect the external key store proxy or any external components.

While the external key store is disconnected, Amazon KMS does not send any requests to the external key store proxy. The connection state of the external key store is `DISCONNECTED`. The KMS keys in the disconnected external key store are in an [UNAVAILABLE key state](#) (unless they are [pending deletion](#)), which means that they cannot be used in cryptographic operations. However, you can still view and manage your external key store and its existing KMS keys.

The disconnected state is designed to be temporary and reversible. You can reconnect your external key store at any time. Typically, no reconfiguration is necessary. However, if any properties of the associated external key store proxy have changed while it was disconnected, such as rotation of its [proxy authentication credential](#), you must [edit the external key store settings](#) before reconnecting.

Note

While a custom key store is disconnected, all attempts to create KMS keys in the custom key store or to use existing KMS keys in cryptographic operations will fail. This action can prevent users from storing and accessing sensitive data.

To better estimate the effect of disconnecting your external key store, identify the KMS keys in the external key store and [determine their past use](#).

You might disconnect an external key store for reasons such as the following:

- **To edit its properties.** You can edit the custom key store name, proxy URI path, and proxy authentication credential while the external key store is connected. However, to edit the proxy

connectivity type, proxy URI endpoint, or VPC endpoint service name, you must first disconnect the external key store. For details, see [Edit external key store properties](#).

- **To stop all communication** between Amazon KMS and the external key store proxy. You can also stop communication between Amazon KMS and your proxy by disabling your endpoint or VPC endpoint service. In addition, your external key store proxy or key management software might provide additional mechanisms to prevent Amazon KMS from communicating with the proxy or to prevent the proxy from accessing your external key manager.
- **To disable all KMS keys** in the external key store. You can [disable and re-enable KMS keys](#) in an external key store by using the Amazon KMS console or the [DisableKey](#) operation. These operations complete quickly (subject to eventual consistency), but they act on one KMS key at a time. Disconnecting the external key store changes the key state of all KMS keys in the external key store to `Unavailable`, which prevents them from being used in any cryptographic operation.
- **To repair a failed connection attempt.** If an attempt to connect an external key store fails (the connection state of the custom key store is `FAILED`), you must disconnect the external key store before you try to connect it again.

Disconnect your external key store

You can disconnect your external key store in the Amazon KMS console or by using the [DisconnectCustomKeyStore](#) operation.

Using the Amazon KMS console

You can use the Amazon KMS console to connect an external key store to its external key store proxy. This process takes about 5 minutes to complete.

1. Sign in to the Amazon Web Services Management Console and open the Amazon Key Management Service (Amazon KMS) console at <https://console.amazonaws.cn/kms>.
2. To change the Amazon Web Services Region, use the Region selector in the upper-right corner of the page.
3. In the navigation pane, choose **Custom key stores, External key stores**.
4. Choose the row of the external key store you want to disconnect.
5. From the **Key store actions** menu, choose **Disconnect**.

When the operation completes, the connection state changes from **DISCONNECTING** to **DISCONNECTED**. If the operation fails, an error message appears that describes the problem and provides help on how to fix it. If you need more help, see [External key store connection errors](#).

Using the Amazon KMS API

To disconnect a connected external key store, use the [DisconnectCustomKeyStore](#) operation. If the operation is successful, Amazon KMS returns an HTTP 200 response and a JSON object with no properties. The process takes about five minutes to complete. To find the connection state of the external key store, use the [DescribeCustomKeyStores](#) operation.

The examples in this section use the [Amazon Command Line Interface \(Amazon CLI\)](#), but you can use any supported programming language.

This example disconnects an external key store with VPC endpoint service connectivity. Before running this example, replace the example custom key store ID with a valid one.

```
$ aws kms disconnect-custom-key-store --custom-key-store-id cks-1234567890abcdef0
```

To verify that the external key store is disconnected, use the [DescribeCustomKeyStores](#) operation. By default, this operation returns all custom keys stores in your account and Region. But you can use either the `CustomKeyId` and `CustomKeyName` parameter (but not both) to limit the response to particular custom key stores. The `ConnectionState` value of `DISCONNECTED` indicates that this example external key store is no longer connected to its external key store proxy.

```
$ aws kms describe-custom-key-stores --custom-key-store-name ExampleXksVpc
{
  "CustomKeyStores": [
    {
      "CustomKeyId": "cks-9876543210fedcba9",
      "CustomKeyName": "ExampleXksVpc",
      "ConnectionState": "DISCONNECTED",
      "CreationDate": "2022-12-13T18:34:10.675000+00:00",
      "CustomKeyType": "EXTERNAL_KEY_STORE",
      "XksProxyConfiguration": {
        "AccessKeyId": "ABCDE98765432EXAMPLE",
        "Connectivity": "VPC_ENDPOINT_SERVICE",
        "UriEndpoint": "https://example-proxy-uri-endpoint-vpc",
        "UriPath": "/example/prefix/kms/xks/v1",
        "VpcEndpointServiceName": "com.amazonaws.vpce.us-east-1.vpce-svc-example"
      }
    }
  ]
}
```

```
    }  
  ]  
}
```

Delete an external key store

When you delete an external key store, Amazon KMS deletes all metadata about the external key store from Amazon KMS, including information about its external key store proxy. This operation does not affect the [external key store proxy](#), [external key manager](#), [external keys](#), or any Amazon resources that you created to support the external key store, such as an Amazon VPC or a VPC endpoint service.

Before you delete an external key store, you must [delete all of the KMS keys](#) from the key store and [disconnect the key store](#) from its external key store proxy. Otherwise, attempts to delete the key store fail.

Deleting an external key store is irreversible, but you can create a new external key store and associate it with the same external key store proxy and external key manager. However, you cannot recreate the symmetric encryption KMS keys in the external key store, even you have access to the same external key material. Amazon KMS includes metadata in the symmetric ciphertext unique to each KMS key. This security feature ensures that only the KMS key that encrypted the data can decrypt it.

Instead of deleting the external key store, consider disconnecting it. While an external key store is disconnected, you can manage the external key store and its Amazon KMS keys but you cannot create or use KMS keys in the external key store. You can reconnect the external key store at any time and resume using its KMS keys to encrypt and decrypt data. There is no cost for a disconnected external key store proxy or its unavailable KMS keys.

You can delete your external key store in the Amazon KMS console or by using the [DeleteCustomKeyStore](#) operation.

Using the Amazon KMS console

You can use the Amazon KMS console to delete an external key store.

1. Sign in to the Amazon Web Services Management Console and open the Amazon Key Management Service (Amazon KMS) console at <https://console.amazonaws.cn/kms>.
2. To change the Amazon Web Services Region, use the Region selector in the upper-right corner of the page.

3. In the navigation pane, choose **Custom key stores, External key stores**.
4. Find the row that represents the external key store that you want to delete. If the **Connection state** of the external key store is not **DISCONNECTED**, you must [disconnect the external key store](#) before you delete it.
5. From the **Key store actions** menu, choose **Delete**.

When the operation completes, a success message appears and the external key store no longer appears in the key store list. If the operation is unsuccessful, an error message appears that describes the problem and provides help on how to fix it. If you need more help, see [Troubleshooting external key stores](#).

Using the Amazon KMS API

To delete an external key store, use the [DeleteCustomKeyStore](#) operation. If the operation is successful, Amazon KMS returns an HTTP 200 response and a JSON object with no properties.

To begin, disconnect the external key store. Before running this command, replace the example custom key store ID with a valid one.

```
$ aws kms disconnect-custom-key-store --custom-key-store-id cks-1234567890abcdef0
```

After the external key store is disconnected, you can use the [DeleteCustomKeyStore](#) operation to delete it.

```
$ aws kms delete-custom-key-store --custom-key-store-id cks-1234567890abcdef0
```

To confirm that the external key store is deleted, use the [DescribeCustomKeyStores](#) operation.

```
$ aws kms describe-custom-key-stores  
  
{  
  "CustomKeyStores": []  
}
```

If you specify a custom key store name or ID that no longer exists, Amazon KMS returns a `CustomKeyStoreNotFoundException` exception.

```
$ aws kms describe-custom-key-stores --custom-key-store-id cks-1234567890abcdef0
```

An error occurred (CustomKeyStoreNotFoundException) when calling the DescribeCustomKeyStore operation:

Troubleshooting external key stores

The resolution for most problems with external key stores are indicated by the error message that Amazon KMS displays with each exception, or by the [connection error code](#) that Amazon KMS returns when an attempt to [connect the external key store](#) to its external key store proxy fails. However, some issues are a bit more complex.

When diagnosing an issue with an external key store, first locate the cause. This will narrow the range of remedies and make your troubleshooting more efficient.

- Amazon KMS — The problem might be within Amazon KMS, such as an incorrect value in your [external key store configuration](#).
- External — The problem might originate outside of Amazon KMS, including problems with the configuration or operation of the external key store proxy, external key manager, external keys, or VPC endpoint service.
- Networking — It might be a problem with connectivity or networking, such as a problem with your proxy endpoint, port, or your private DNS name or domain.

Note

When management operations on external key stores fail, they generate several different exceptions. But Amazon KMS cryptographic operations return `KMSInvalidStateException` for all failures related to the external configuration or connection state of the external key store. To identify the problem, use the accompanying error message text.

The [ConnectCustomKeyStore](#) operation succeeds quickly before the connection process is complete. To determine whether the connection process is successful, view the [connection state](#) of the external key store. If the connection process fails, Amazon KMS returns a [connection error code](#) that explains the cause and suggests a remedy.

Topics

- [Troubleshooting tools for external key stores](#)
- [Configuration errors](#)

- [External key store connection errors](#)
- [Latency and timeout errors](#)
- [Authentication credential errors](#)
- [Key state errors](#)
- [Decryption errors](#)
- [External key errors](#)
- [Proxy issues](#)
- [Proxy authorization issues](#)

Troubleshooting tools for external key stores

Amazon KMS provides several tools to help you identify and resolve problems with your external key store and its keys. Use these tools in conjunction with the tools provided with your external key store proxy and external key manager.

Note

Your external key store proxy and external key manager might provide easier methods of creating and maintaining your external key store and its KMS keys. For details, see the documentation for your external tools.

Amazon KMS exceptions and error messages

Amazon KMS provides a detailed error message about any problem it encounters. You can find additional information about Amazon KMS exceptions in the [Amazon Key Management Service API Reference](#) and Amazon SDKs. Even if you are using the Amazon KMS console, you might find these references to be helpful. For example, see the [Errors](#) list for the `CreateCustomKeyStores` operation.

To optimize the performance of your external key store proxy, Amazon KMS returns exceptions based on your proxy's reliability within a given aggregation period of 5 minutes. In the event of a 500 Internal Server Error, 503 Service Unavailable, or connection timeout, a proxy with high reliability returns `KMSInternalException` and triggers an automatic retry to ensure that requests eventually succeed. However, a proxy with low reliability returns `KMSInvalidStateException`. For more information, see [Monitoring an external key store](#).

If the problem surfaces in a different Amazon service, such as when you use a KMS key in your external key store to protect a resource in another Amazon service, the Amazon service might provide additional information to help you identify the problem. If the Amazon service doesn't provide the message, you can view the error message in the [CloudTrail logs](#) that record the use of your KMS key.

[CloudTrail logs](#)

Every Amazon KMS API operation, including actions in the Amazon KMS console, is recorded in Amazon CloudTrail logs. Amazon KMS records a log entry for successful and failed operations. For failed operations, the log entry includes the Amazon KMS exception name (`errorCode`) and the error message (`errorMessage`). You can use this information to help you identify and resolve the error. For an example, see [Decrypt failure with a KMS key in an external key store](#).

The log entry also includes the request ID. If the request reached your external key store proxy, you can use the request ID in the log entry to find the corresponding request in your proxy logs, if your proxy provides them.

[CloudWatch metrics](#)

Amazon KMS records detailed Amazon CloudWatch metrics about the operation and performance of your external key store, including latency, throttling, proxy errors, external key manager status, the number of days until your TLS certificate expires, and the reported age of your proxy authentication credentials. You can use these metrics to develop data models for the operation of your external key store and CloudWatch alarms that alert you to impending problems before they occur.

Important

Amazon KMS recommends that you create CloudWatch alarms to monitor the external key store metrics. These alarms will alert you to early signs of problems before they develop.

[Monitoring graphs](#)

Amazon KMS displays graphs of the external key store CloudWatch metrics on the detail page for each external key store in the Amazon KMS console. You can use the data in the graphs to help locate the source of errors, detect impending problems, establish baselines, and refine your CloudWatch alarm thresholds. For details about interpreting the monitoring graphs and using their data, see [Monitor external key stores](#).

Displays of external key stores and KMS keys

Amazon KMS displays detailed information about your external key stores and the KMS keys in the external key store in the Amazon KMS console, and in the response to the [DescribeCustomKeyStores](#) and [DescribeKey](#) operations. These displays include special fields for external key stores and KMS keys with information that you can use for troubleshooting, such as the [connection state](#) of the external key store and the ID of the external key that is associated with the KMS key. For details, see [View external key stores](#).

[XKS Proxy Test Client](#)

Amazon KMS provides an open source test client that verifies that your external key store proxy conforms to the [Amazon KMS External Key Store Proxy API Specification](#). You can use this test client to identify and resolve problems with your external key store proxy.

Configuration errors

When you create an external key store, you specify property values that comprise the *configuration* of your external key store, such as the [proxy authentication credential](#), [proxy URI endpoint](#), [proxy URI path](#), and [VPC endpoint service name](#). When Amazon KMS detects an error in a property value, the operation fails and returns an error that indicates the faulty value.

Many configuration issues can be resolved by fixing the incorrect value. You can fix an invalid proxy URI path or proxy authentication credential without disconnecting the external key store. For definitions of these values, including uniqueness requirements, see [Assemble the prerequisites](#). For instructions about updating these values, see [Edit external key store properties](#).

To avoid errors with your proxy URI path and proxy authentication credential values, when creating or updating your external key store, upload a [proxy configuration file](#) to the Amazon KMS console. This is a JSON-based file with proxy URI path and proxy authentication credential values that is provided by your external key store proxy or external key manager. You can't use a proxy configuration file with Amazon KMS API operations, but you can use the values in the file to help you provide parameter values for your API requests that match the values in your proxy.

General configuration errors

Exceptions: `CustomKeyStoreInvalidStateException` (`CreateKey`),
`KMSInvalidStateException` (cryptographic operations),
`XksProxyInvalidConfigurationException` (management operations, except for `CreateKey`)

Connection error codes: XKS_PROXY_INVALID_CONFIGURATION,
XKS_PROXY_INVALID_TLS_CONFIGURATION

For external key stores with [public endpoint connectivity](#), Amazon KMS tests the property values when you create and update the external key store. For external key stores with [VPC endpoint service connectivity](#), Amazon KMS tests the property values when you connect and update the external key store.

Note

The ConnectCustomKeyStore operation, which is asynchronous, might succeed even though the attempt to connect the external key store to its external key store proxy fails. In that case, there is no exception, but the connection state of the external key store is Failed, and a connection error code explains the error message. For more information, see [External key store connection errors](#).

If Amazon KMS detects an error in a property value, the operation fails and returns XksProxyInvalidConfigurationException with one of the following error messages.

The external key store proxy rejected the request because of an invalid URI path. Verify the URI path for your external key store and update if necessary.

- The [proxy URI path](#) is the base path for Amazon KMS requests to the proxy APIs. If this path is incorrect, all requests to the proxy fail. To [view the current proxy URI path](#) for your external key store, use the Amazon KMS console or the DescribeCustomKeyStores operation. To find the correct proxy URI path, see your external key store proxy documentation. For help correcting your proxy URI path value, see [Edit external key store properties](#).
- The proxy URI path for your external key store proxy can change with updates to your external key store proxy or external key manager. For information about these changes, see the documentation for your external key store proxy or external key manager.

XKS_PROXY_INVALID_TLS_CONFIGURATION

Amazon KMS cannot establish a TLS connection to the external key store proxy. Verify the TLS configuration, including its certificate.

- All external key store proxies require a TLS certificate. The TLS certificate must be issued by a public certificate authority (CA) that is supported for external key stores. For list of supported CAs, see [Trusted Certificate Authorities](#) in the Amazon KMS External Key Store Proxy API Specification.
- For public endpoint connectivity, the subject common name (CN) on the TLS certificate must match the domain name in the [proxy URI endpoint](#) for the external key store proxy. For example, if the public endpoint is `https://myproxy.xks.example.com`, the CN on the TLS certificate must be `myproxy.xks.example.com` or `*.xks.example.com`.
- For VPC endpoint service connectivity, the subject common name (CN) on the TLS certificate must match the private DNS name for your [VPC endpoint service](#). For example, if the private DNS name is `myproxy-private.xks.example.com`, the CN on the TLS certificate must be `myproxy-private.xks.example.com` or `*.xks.example.com`.
- The TLS certificate cannot be expired. To get the expiration date of a TLS certificate, use SSL tools, such as [OpenSSL](#). To monitor the expiration date of a TLS certificate associated with an external key store, use the [XksProxyCertificateDaysToExpire](#) CloudWatch metric. The number of days to your TLS certification expiration date also appears in the [Monitoring section](#) of the Amazon KMS console.
- If you are using [public endpoint connectivity](#), use SSL test tools to test your SSL configuration. TLS connection errors can result from incorrect certificate chaining.

VPC endpoint service connectivity configuration errors

Exceptions: `XksProxyVpcEndpointServiceNotFoundException`,
`XksProxyVpcEndpointServiceInvalidConfigurationException`

In addition to general connectivity issues, you might encounter the following issues while creating, connecting, or updating an external key store with VPC endpoint service connectivity. Amazon KMS tests the property values of an external key store with VPC endpoint service connectivity while [creating](#), [connecting](#), and [updating](#) the external key store. When management operations fail due to configuration errors, they generate the following exceptions:

```
XksProxyVpcEndpointServiceNotFoundException
```

The cause might be one of the following:

- An incorrect VPC endpoint service name. Verify that the VPC endpoint service name for the external key store is correct and matches the proxy URI endpoint value for the external key store. To find the VPC endpoint service name, use the [Amazon VPC console](#) or the [DescribeVpcEndpointServices](#) operation. To find the VPC endpoint service name and proxy URI endpoint of an existing external key store, use the Amazon KMS console or the [DescribeCustomKeyStores](#) operation. For details, see [View external key stores](#).
- The VPC endpoint service might be in a different Amazon Web Services Region than the external key store. Verify that the VPC endpoint service and external key store are in same Region. (The external name of the Region name, such as us-east-1, is part of the VPC endpoint service name, such as com.amazonaws.vpce.us-east-1.vpce-svc-example.) For a list of requirements for the VPC endpoint service for an external key store, see [VPC endpoint service](#). You cannot move a VPC endpoint service or an external key store to a different Region. However, you can create a new external key store in the same Region as the VPC endpoint service. For details, see [Configure VPC endpoint service connectivity](#) and [Create an external key store](#).
- Amazon KMS is not an allowed principal for the VPC endpoint service. The **Allow principals** list for the VPC endpoint service must include the `cks.kms.<region>.amazonaws.com` value, such as `cks.kms.eu-west-3.amazonaws.com`. For instructions about adding this value, see [Manage permissions](#) in the *Amazon PrivateLink Guide*.

XksProxyVpcEndpointServiceInvalidConfigurationException

This error occurs when the VPC endpoint service fails to meet one of the following requirements:

- The VPC requires at least two private subnets, each in a different Availability Zone. For help adding a subnet to your VPC, see [Create a subnet in your VPC](#) in the *Amazon VPC User Guide*.
- Your [VPC endpoint service type](#) must use a network load balancer, not a gateway load balancer.
- Acceptance must not be required for the VPC endpoint service (**Acceptance required** must be false.). If manual acceptance of each connection request is required, Amazon KMS cannot use the VPC endpoint service to connect to the external key store proxy. For details, see [Accept or reject connection requests](#) in the *Amazon PrivateLink Guide*.
- The VPC endpoint service must have a private DNS name that is a subdomain of a public domain. For example, if the private DNS name is `https://myproxy-private.xks.example.com`, the `xks.example.com` or `example.com` domains must have a public DNS server. To view or change

the private DNS name for your VPC endpoint service, see [Manage DNS names for VPC endpoint services](#) in the *Amazon PrivateLink Guide*.

- The **Domain verification status** of the domain for your private DNS name must be verified. To view and update the verification status of the private DNS name domain, see [Step 5: Verify your private DNS name domain](#). It might take a few minutes for the updated verification status to appear after you've added the required text record.

Note

A private DNS domain can be verified only if it is the subdomain of a public domain. Otherwise, the verification status of the private DNS domain does not change, even after you add the required TXT record.

- The private DNS name of the VPC endpoint service must match the [proxy URI endpoint](#) value for the external key store. For an external key store with VPC endpoint service connectivity, the proxy URI endpoint must be `https://` followed by the private DNS name of the VPC endpoint service. To view the proxy URI endpoint value, see [View external key stores](#). To change the proxy URI endpoint value, see [Edit external key store properties](#).

External key store connection errors

The [process of connecting an external key store](#) to its external key store proxy takes about five minutes to complete. Unless it fails quickly, the `ConnectCustomKeyStore` operation returns an HTTP 200 response and a JSON object with no properties. However, this initial response does not indicate that the connection was successful. To determine whether the external key store is connected, see its [connection state](#). If the connection fails, the connection state of the external key store changes to `FAILED` and Amazon KMS returns a [connection error code](#) that explains the cause of the failure.

Note

When the connection state of a custom key store is `FAILED`, you must disconnect the custom key store before attempting to reconnect it. You cannot connect a custom key store with a `FAILED` connection status.

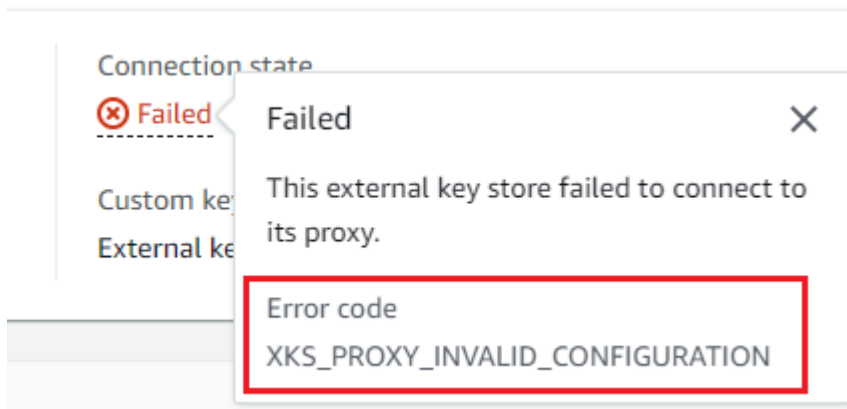
To view the connection state of an external key store:

- In the [DescribeCustomKeyStores](#) response, view the value of the `ConnectionState` element.
- In the Amazon KMS console, the **Connection state** appears in the external key store table. Also, on the detail page for each external key store, the **Connection state** appears in the **General configuration** section.

When the connection state is `FAILED`, the connection error code helps to explain the error.

To view the connection error code:

- In the [DescribeCustomKeyStores](#) response, view the value of the `ConnectionErrorCode` element. This element appears in the `DescribeCustomKeyStores` response only when the `ConnectionState` is `FAILED`.
- To view the connection error code in the Amazon KMS console, on the detail page for the external key store and hover over the **Failed** value.



Connection error codes for external key stores

The following connection error codes apply to external key stores

INTERNAL_ERROR

Amazon KMS could not complete the request due to an internal error. Retry the request. For `ConnectCustomKeyStore` requests, disconnect the custom key store before trying to connect again.

INVALID_CREDENTIALS

One or both of the `XksProxyAuthenticationCredential` values is not valid on the specified external key store proxy.

NETWORK_ERRORS

Network errors are preventing Amazon KMS from connecting the custom key store to its backing key store.

XKS_PROXY_ACCESS_DENIED

Amazon KMS requests are denied access to the external key store proxy. If the external key store proxy has authorization rules, verify that they permit Amazon KMS to communicate with the proxy on your behalf.

XKS_PROXY_INVALID_CONFIGURATION

A configuration error is preventing the external key store from connecting to its proxy. Verify the value of the `XksProxyUriPath`.

XKS_PROXY_INVALID_RESPONSE

Amazon KMS cannot interpret the response from the external key store proxy. If you see this connection error code repeatedly, notify your external key store proxy vendor.

XKS_PROXY_INVALID_TLS_CONFIGURATION

Amazon KMS cannot connect to the external key store proxy because the TLS configuration is invalid. Verify that the external key store proxy supports TLS 1.2 or 1.3. Also, verify that the TLS certificate is not expired, that it matches the hostname in the `XksProxyUriEndpoint` value, and that it is signed by a trusted certificate authority included in the [Trusted Certificate Authorities](#) list.

XKS_PROXY_NOT_REACHABLE

Amazon KMS can't communicate with your external key store proxy. Verify that the `XksProxyUriEndpoint` and `XksProxyUriPath` are correct. Use the tools for your external key store proxy to verify that the proxy is active and available on its network. Also, verify that your external key manager instances are operating properly. Connection attempts fail with this connection error code if the proxy reports that all external key manager instances are unavailable.

XKS_PROXY_TIMED_OUT

Amazon KMS can connect to the external key store proxy, but the proxy does not respond to Amazon KMS in the time allotted. If you see this connection error code repeatedly, notify your external key store proxy vendor.

XKS_VPC_ENDPOINT_SERVICE_INVALID_CONFIGURATION

The Amazon VPC endpoint service configuration doesn't conform to the requirements for an Amazon KMS external key store.

- The VPC endpoint service must be an endpoint service for interface endpoints in the caller's Amazon Web Services account.
- It must have a network load balancer (NLB) connected to at least two subnets, each in a different Availability Zone.
- The `Allow principals` list must include the Amazon KMS service principal for the Region, `cks.kms.<region>.amazonaws.com`, such as `cks.kms.us-east-1.amazonaws.com`.
- It must *not* require [acceptance](#) of connection requests.
- It must have a private DNS name. The private DNS name for an external key store with `VPC_ENDPOINT_SERVICE` connectivity must be unique in its Amazon Web Services Region.
- The domain of the private DNS name must have a [verification status](#) of verified.
- The [TLS certificate](#) specifies the private DNS hostname at which the endpoint is reachable.

XKS_VPC_ENDPOINT_SERVICE_NOT_FOUND

Amazon KMS can't find the VPC endpoint service that it uses to communicate with the external key store proxy. Verify that the `XksProxyVpcEndpointServiceName` is correct and the Amazon KMS service principal has service consumer permissions on the Amazon VPC endpoint service.

Latency and timeout errors

Exceptions: `CustomKeyStoreInvalidStateException (CreateKey)`,
`KMSInvalidStateException (cryptographic operations)`,
`XksProxyUriUnreachableException (management operations)`

[Connection error codes:](#) `XKS_PROXY_NOT_REACHABLE`, `XKS_PROXY_TIMED_OUT`

When Amazon KMS can't contact the proxy within the 250 millisecond timeout interval, it returns an exception. `CreateCustomKeyStore` and `UpdateCustomKeyStore` return `XksProxyUriUnreachableException`. Cryptographic operations return the standard `KMSInvalidStateException` with an error message that describes the problem. If `ConnectCustomKeyStore` fails, Amazon KMS returns a [connection error code](#) that describes the problem.

Timeout errors might be transient issues that can be resolved by retrying the request. If the problem persists, verify that your external key store proxy is active and is connected to the network, and that its proxy URI endpoint, proxy URI path, and VPC endpoint service name (if any) are correct in your external key store. Also, verify that your external key manager is close to the Amazon Web Services Region for your external key store. If you need to update any of these values, see [Edit external key store properties](#).

To track latency patterns, use the [XksProxyLatency](#) CloudWatch metric and the **Average latency** graph (based on that metric) in the [Monitoring section](#) of the Amazon KMS console. Your external key store proxy might also generate logs and metrics that track latency and timeouts.

XksProxyUriUnreachableException

Amazon KMS cannot communicate with the external key store proxy. This might be a transient network issue. If you see this error repeatedly, verify that your external key store proxy is active and is connected to the network, and that its endpoint URI is correct in your external key store.

- The external key store proxy didn't respond to an Amazon KMS proxy API request within the 250 millisecond timeout interval. This might indicate a transient network problem or an operational or performance problem with the proxy. If retrying doesn't solve the problem, notify your external key store proxy administrator.

Latency and timeout errors often manifest as connection failures. When the [ConnectCustomKeyStore](#) operation fails, the *connection state* of the external key store changes to FAILED and Amazon KMS returns a *connection error code* that explains the error. For a list of connection error codes and suggestions for resolving the errors, see [Connection error codes for external key stores](#). The connection codes lists for **All custom key stores** and **External key stores** apply to external key stores. The following connection errors are related to latency and timeouts.

XKS_PROXY_NOT_REACHABLE

-or-

CustomKeyStoreInvalidStateException , KMSInvalidStateException ,
XksProxyUriUnreachableException

Amazon KMS cannot communicate with the external key store proxy. Verify that your external key store proxy is active and is connected to the network, and that its URI path and endpoint URI or VPC service name are correct in your external key store.

This error might occur for the following reasons:

- The external key store proxy is not active and or not connected to the network.
- There is an error in the [proxy URI endpoint](#), [proxy URI path](#), or [VPC endpoint service name](#) (if applicable) values in the external key store configuration. To view the external key store configuration, use the [DescribeCustomKeyStores](#) operation or [view the detail page](#) for the external key store in the Amazon KMS console.
- There might be a network configuration error, such as a port error, on the network path between Amazon KMS and the external key store proxy. Amazon KMS communicates with the external key store proxy on port 443. This value is not configurable.
- When the external key store proxy reports (in a [GetHealthStatus](#) response) that all external key manager instances are UNAVAILABLE, the [ConnectCustomKeyStore](#) operation fails with a `ConnectionErrorCode` of `XKS_PROXY_NOT_REACHABLE`. For help, see your external key manager documentation.
- This error can result from a long physical distance between the external key manager and the Amazon Web Services Region with the external key store. The ping latency (network round-trip time (RTT)) between the Amazon Web Services Region and the external key manager must be no more than 35 milliseconds. You might have to create an external key store in an Amazon Web Services Region that is closer to the external key manager, or move the external key manager to a data center that is closer to the Amazon Web Services Region.

XKS_PROXY_TIMED_OUT

-or-

`CustomKeyStoreInvalidStateException` , `KMSInvalidStateException` ,
`XksProxyUriUnreachableException`

Amazon KMS rejected the request because the external key store proxy did not respond in time. Retry the request. If you see this error repeatedly, report it to your external key store proxy administrator.

This error might occur for the following reasons:

- This error can result from a long physical distance between the external key manager and the external key store proxy. If possible, move the external key store proxy closer to the external key manager.
- Timeout errors can occur when the proxy is not designed to handle the volume and frequency of requests from Amazon KMS. If your CloudWatch metrics indicate a persistent problem, notify your external key store proxy administrator.
- Timeout errors can occur when the connection between the external key manager and the Amazon VPC for the external key store is not operating properly. If you are using Amazon Direct Connect, verify that your VPC and external key manager can communicate effectively. For help resolving any issues, see [Troubleshooting Amazon Direct Connect](#) in the Amazon Direct Connect User Guide.

```
XKS_PROXY_TIMED_OUT
```

-or-

```
CustomKeyStoreInvalidStateException , KMSInvalidStateException ,  
XksProxyUriUnreachableException
```

The external key store proxy did not respond to the request in the time allotted. Retry the request. If you see this error repeatedly, report it to your external key store proxy administrator.

- This error can result from a long physical distance between the external key manager and the external key store proxy. If possible, move the external key store proxy closer to the external key manager.

Authentication credential errors

Exceptions: `CustomKeyStoreInvalidStateException (CreateKey)`,
`KMSInvalidStateException (cryptographic operations)`,
`XksProxyIncorrectAuthenticationCredentialException (management operations other than CreateKey)`

You establish and maintain an authentication credential for Amazon KMS on your external key store proxy. Then you tell Amazon KMS the credential values when you create an external key

store. To change the authentication credential, make the change on your external key store proxy. Then [update the credential](#) for your external key store. If your proxy rotates the credential, you must [update the credential](#) for your external key store.

If the external key store proxy won't authenticate a request signed with the [proxy authentication credential](#) for your external key store, the effect depends on the request:

- `CreateCustomKeyStore` and `UpdateCustomKeyStore` fail with an `XksProxyIncorrectAuthenticationCredentialException`.
- `ConnectCustomKeyStore` succeeds, but the connection fails. The connection state is `FAILED` and the connection error code is `INVALID_CREDENTIALS`. For details, see [External key store connection errors](#).
- Cryptographic operations return `KMSInvalidStateException` for all external configuration errors and connection state errors in an external key store. The accompanying error message describes the problem.

The external key store proxy rejected the request because it could not authenticate Amazon KMS. Verify the credentials for your external key store and update if necessary.

This error might occur for the following reasons:

- The access key ID or the secret access key for the external key store doesn't match the values established on the external key store proxy.

To fix this error, [update the proxy authentication credential](#) for your external key store. You can make this change without disconnecting your external key store.

- A reverse proxy between Amazon KMS and the external key store proxy could be manipulating HTTP headers in a manner that invalidates the SigV4 signatures. To fix this error, notify your proxy administrator.

Key state errors

Exceptions: `KMSInvalidStateException`

`KMSInvalidStateException` is used for two distinct purposes for KMS keys in custom key stores.

- When a management operation, such as `CancelKeyDeletion`, fails and returns this exception, it indicates that the [key state](#) of the KMS key is not compatible with the operation.
- When a [cryptographic operation](#) on a KMS key in a custom key store fails with `KMSInvalidStateException`, it can indicate a problem with the key state of the KMS key. But Amazon KMS cryptographic operation return `KMSInvalidStateException` for all external configuration errors and connection state errors in an external key store. To identify the problem, use the error message that accompanies the exception.

To find the required key state for an Amazon KMS API operations, see [Key states of Amazon KMS keys](#). To find the key state of a KMS key, on the **Customer managed keys** page, view the **Status** field of the KMS key. Or, use the [DescribeKey](#) operation and view the `KeyState` element in the response. For details, see [Identify and view keys](#).

Note

The key state of a KMS key in an external key store does not indicate anything about the status of its associated [external key](#). For information about the external key status, use your external key manager and external key store proxy tools.

The `CustomKeyStoreInvalidStateException` refers to the [connection state](#) of the external key store, not the [key state](#) of a KMS key.

A cryptographic operation on a KMS key in a custom store might fail because the key state of the KMS key is `Unavailable` or `PendingDeletion`. (Disabled keys return `DisabledException`.)

- A KMS key has a `Disabled` key state only when you intentionally disable the KMS key in the Amazon KMS console or by using the [DisableKey](#) operation. While a KMS key is disabled, you can view and manage the key, but you cannot use it in cryptographic operations. To fix this problem, enable the key. For details, see [Enable and disable keys](#).
- A KMS key has an `Unavailable` key state when the external key store is disconnected from its external key store proxy. To fix an unavailable KMS key, [reconnect the external key store](#). After the external key store is reconnected, the key state of the KMS keys in the external key store is automatically restored to its previous state, such as `Enabled` or `Disabled`.

A KMS key has a `PendingDeletion` key state when it has been scheduled for deletion and is in its waiting period. A key state error on a KMS key that is pending deletion indicates that the key should not be deleted, either because it's being used for encryption, or it is required for

decryption. To re-enable the KMS key, cancel the scheduled deletion, and then [enable the key](#). For details, see [Schedule key deletion](#).

Decryption errors

Exceptions: `KMSInvalidStateException`

When a [Decrypt](#) operation with a KMS key in an external key store fails, Amazon KMS returns the standard `KMSInvalidStateException` that cryptographic operations use for all external configuration errors and connection state errors on an external key store. The error message indicates the problem.

To decrypt a ciphertext that was encrypted using [double encryption](#), the external key manager first uses the external key to decrypt the outer layer of ciphertext. Then Amazon KMS uses the Amazon KMS key material in the KMS key to decrypt the inner layer of ciphertext. An invalid or corrupt ciphertext can be rejected by the external key manager or Amazon KMS.

The following error messages accompany the `KMSInvalidStateException` when decryption fails. It indicates a problem with the ciphertext or the optional encryption context in the request.

The external key store proxy rejected the request because the specified ciphertext or additional authenticated data is corrupted, missing, or otherwise invalid.

- When the external key store proxy or external key manager report that a ciphertext or its encryption context is invalid, it typically indicates a problem with the ciphertext or encryption context in the `Decrypt` request sent to Amazon KMS. For `Decrypt` operations, Amazon KMS sends the proxy the same ciphertext and encryption context it receives in the `Decrypt` request.

This error might be caused by a networking problem in transit, such as a flipped bit. Retry the `Decrypt` request. If the problem persists, verify that the ciphertext was not altered or corrupted. Also, verify that the encryption context in the `Decrypt` request to Amazon KMS matches the encryption context in the request that encrypted the data.

The ciphertext that the external key store proxy submitted for decryption, or the encryption context, is corrupted, missing, or otherwise invalid.

- When Amazon KMS rejects the ciphertext that it received from the proxy, it indicates that the external key manager or proxy returned an invalid or corrupt ciphertext to Amazon KMS.

This error might be caused by a networking problem in transit, such as a flipped bit. Retry the Decrypt request. If the problem persists, verify that the external key manager is operating properly, and that the external key store proxy does not alter the ciphertext that it receives from the external key manager before it returns it to Amazon KMS.

External key errors

An [external key](#) is a cryptographic key in the external key manager that serves as the external key material for a KMS key. Amazon KMS cannot directly access the external key. It must ask the external key manager (via the external key store proxy) to use the external key to encrypt data or decrypt a ciphertext.

You specify the ID of the external key in its external key manager when you create a KMS key in your external key store. You cannot change the external key ID after the KMS key is created. To prevent problems with the KMS key, the CreateKey operation asks the external key store proxy to verify the ID and configuration of the external key. If the external key doesn't [fulfill the requirements](#) for use with a KMS key, the CreateKey operation fails with an exception and error message that identifies the problem.

However, issues can occur after the KMS key is created. If a cryptographic operation fails because of a problem with the external key, the operation fails and returns a `KMSInvalidStateException` with an error message that indicates the problem.

CreateKey errors for the external key

Exceptions: `XksKeyAlreadyInUseException`, `XksKeyNotFoundException`, `XksKeyInvalidConfigurationException`

The [CreateKey](#) operation attempts to verify the ID and properties of the external key that you provide in the **External key ID** (console) or `XksKeyId` (API) parameter. This practice is designed to detect errors early before you try to use the external key with the KMS key.

External key in use

Each KMS key in an external key store must use a different external key. When `CreateKey` recognizes that the external key ID (`XksKeyId`) for a KMS key is not unique in the external key store, it fails with an `XksKeyAlreadyInUseException`.

If you use multiple IDs for the same external key, `CreateKey` won't recognize the duplicate. However, KMS keys with the same external key are not interoperable because they have different Amazon KMS key material and metadata.

External key not found

When the external key store proxy reports that it cannot find the external key using the external key ID (`XksKeyId`) for the KMS key, the `CreateKey` operation fails and returns `XksKeyNotFoundException` with the following error message.

The external key store proxy rejected the request because it could not find the external key.

This error might occur for the following reasons:

- The ID of the external key (`XksKeyId`) for the KMS key might be invalid. To find the ID for your external key proxy uses to identify the external key, see your external key store proxy or external key manager documentation.
- The external key might have been deleted from your external key manager. To investigate, use your external key manager tools. If the external key is permanently deleted, use a different external key with the KMS key. For a list or requirements for the external key, see [Requirements for a KMS key in an external key store](#).

External key requirements not met

When the external key store proxy reports that the external key does not [fulfill the requirements](#) for use with a KMS key, the `CreateKey` operation fails and returns `XksKeyInvalidConfigurationException` with one of the following error messages.

The key spec of the external key must be `AES_256`. The key spec of specified external key is `<key-spec>` .

- The external key must be a 256-bit symmetric encryption key with a key spec of `AES_256`. If the specified external key is a different type, specify the ID of an external key that fulfills this requirement.

The status of the external key must be ENABLED. The status of specified external key is *<status>*.

- The external key must be enabled in the external key manager. If the specified external key is not enabled, use your external key manager tools to enable it, or specify an enabled external key.

The key usage of the external key must include ENCRYPT and DECRYPT. The key use of specified external key is *<key-usage >*.

- The external key must be configured for encryption and decryption in the external key manager. If the specified external key does not include these operations, use your external key manager tools to change the operations, or specify a different external key.

Cryptographic operation errors for the external key

Exceptions: `KMSInvalidStateException`

When the external key store proxy cannot find the external key associated with the KMS key, or the external key doesn't [fulfill the requirements](#) for use with a KMS key, the cryptographic operation fails.

External key issues that are detected during a cryptographic operation are more difficult to resolve than external key issues detected before creating the KMS key. You cannot change the external key ID after the KMS key is created. If the KMS key has not yet encrypted any data, you can delete the KMS key and create a new one with a different external key ID. However, ciphertext generated with the KMS key cannot be decrypted by any other KMS key, even one with the same external key, because keys will have different key metadata and different Amazon KMS key material. Instead, to the extent possible, use your external key manager tools to resolve the problem with the external key.

When the external key store proxy reports a problem with the external key, cryptographic operations return `KMSInvalidStateException` with an error message that identifies the problem.

External key not found

When the external key store proxy reports that it cannot find the external key using the external key ID (XksKeyId) for the KMS key, cryptographic operations return a `KMSInvalidStateException` with the following error message.

The external key store proxy rejected the request because it could not find the external key.

This error might occur for the following reasons:

- The ID of the external key (XksKeyId) for the KMS key is no longer valid.

To find the external key ID associated with your KMS key, [view the details of the KMS key](#). To find the ID that your external key proxy uses to identify the external key, see your external key store proxy or external key manager documentation.

Amazon KMS verifies the external key ID when it creates a KMS key in an external key store. However, the ID might become invalid, especially if the external key ID value is an alias or mutable name. You cannot change the external key ID associated with an existing KMS key. To decrypt any ciphertext encrypted under the KMS key, you must re-associate the external key with the existing external key ID.

If you have not yet used the KMS key to encrypt data, you can create a new KMS key with a valid external key ID. However, if you have generated ciphertext with the KMS key, you cannot use any other KMS key to decrypt the ciphertext, even if it uses the same external key.

- The external key might have been deleted from your external key manager. To investigate, use your external key manager tools. If possible, try to [recover the key material](#) from a copy or backup of your external key manager. If the external key is permanently deleted, any ciphertext encrypted under the associated KMS key is unrecoverable.

External key configuration errors

When the external key store proxy reports that the external key doesn't [fulfill the requirements](#) for use with a KMS key, the cryptographic operation returns `KMSInvalidStateException` with the one of the following error messages.

The external key store proxy rejected the request because the external key does not support the requested operation.

- The external key must support both encryption and decryption. If the key usage does not include encryption and decryption, use your external key manager tools to change the key usage.

The external key store proxy rejected the request because the external key is not enabled in the external key manager.

- The external key must be enabled and available for use in the external key manager. If the status of the external key is not Enabled, use your external key manager tools to enable it.

Proxy issues

Exceptions:

`CustomKeyStoreInvalidStateException` (`CreateKey`), `KMSInvalidStateException` (cryptographic operations), `UnsupportedOperationException`, `XksProxyUriUnreachableException`, `XksProxyInvalidResponseException` (management operations other than `CreateKey`)

The external key store proxy mediates all communication between Amazon KMS and the external key manager. It translates generic Amazon KMS requests into a format that your external key manager can understand. If the external key store proxy doesn't conform to the [Amazon KMS External Key Store Proxy API Specification](#), or if isn't operating properly, or can't communicate with Amazon KMS, you won't be able to create or use KMS keys in your external key store.

While many errors mention the external key store proxy because of its critical role in the external key store architecture, those problem might originate in the external key manager or external key.

The issues in this section relate to problems with the design or operation of the external key store proxy. Resolving these issues might require a change to the proxy software. Consult your proxy administrator. To help diagnose proxy issues, Amazon KMS provides [XKS Proxy Text Client](#), an open source test client that verifies that your external key store proxy conforms to the [Amazon KMS External Key Store Proxy API Specification](#).

`CustomKeyStoreInvalidStateException` , `KMSInvalidStateException` or `XksProxyUriUnreachableException`

The external key store proxy is in an unhealthy state. If you see this message repeatedly, notify your external key store proxy administrator.

- This error can indicate an operational problem or software error in the external key store proxy. You can find CloudTrail log entries for the Amazon KMS API operation that generated each error. This error might be resolved by retrying the operation. However, if it persists, notify your external key store proxy administrator.
- When the external key store proxy reports (in a [GetHealthStatus](#) response) that all external key manager instances are UNAVAILABLE, attempts to create or update an external key store fail with this exception. If this error persists, consult your external key manager documentation.

`CustomKeyStoreInvalidStateException` , `KMSInvalidStateException` or `XksProxyInvalidResponseException`

Amazon KMS cannot interpret the response from the external key store proxy. If you see this error repeatedly, consult your external key store proxy administrator.

- Amazon KMS operations generate this exception when the proxy returns an undefined response that Amazon KMS cannot parse or interpret. This error might occur occasionally due to temporarily external issues or sporadic network errors. However, if it persists, it might indicate that the external key store proxy doesn't conform to the [Amazon KMS External Key Store Proxy API Specification](#). Notify your external key store administrator or vendor.

`CustomKeyStoreInvalidStateException` , `KMSInvalidStateException` or `UnsupportedOperationException`

The external key store proxy rejected the request because it does not support the requested cryptographic operation.

- The external key store proxy should support all [proxy APIs](#) defined in the [Amazon KMS External Key Store Proxy API Specification](#). This error indicates that the proxy does not support the operation that is related to the request. Notify your external key store administrator or vendor.

Proxy authorization issues

Exceptions: CustomKeyStoreInvalidStateException, KMSInvalidStateException

Some external key store proxies implement authorization requirements for the use of its external keys. An external key store proxy is permitted, but not required, to design and implement an authorization scheme that allows particular users to request particular operations under certain conditions. For example, a proxy might allow a user to encrypt with a particular external key, but not to decrypt with it. For more information, see [External key store proxy authorization \(optional\)](#).

Proxy authorization is based on metadata that Amazon KMS includes in its requests to the proxy. The `awsSourceVpc` and `awsSourceVpce` fields are included in the metadata only when the request is from a VPC endpoint and only when the caller is in the same account as the KMS key.

```
"requestMetadata": {
  "awsPrincipalArn": string,
  "awsSourceVpc": string, // optional
  "awsSourceVpce": string, // optional
  "kmsKeyArn": string,
  "kmsOperation": string,
  "kmsRequestId": string,
  "kmsViaService": string // optional
}
```

When the proxy rejects a request due to an authorization failure, the related Amazon KMS operation fails. `CreateKey` returns `CustomKeyStoreInvalidStateException`. Amazon KMS cryptographic operations return `KMSInvalidStateException`. Both use the following error message:

The external key store proxy denied access to the operation. Verify that the user and the external key are both authorized for this operation, and try the request again.

- To resolve the error, use your external key manager or external key store proxy tools to determine why authorization failed. Then, update the procedure that caused the unauthorized request or use your external key store proxy tools to update the authorization policy. You cannot resolve this error in Amazon KMS.

Security of Amazon Key Management Service

Cloud security at Amazon is the highest priority. As an Amazon customer, you benefit from a data center and network architecture that are built to meet the requirements of the most security-sensitive organizations.

Security is a shared responsibility between Amazon and you. The [shared responsibility model](#) describes this as security of the cloud and security in the cloud:

- **Security of the cloud** – Amazon is responsible for protecting the infrastructure that runs Amazon services in the Amazon Cloud. Amazon also provides you with services that you can use securely. Third-party auditors regularly test and verify the effectiveness of our security as part of the [Amazon Compliance Programs](#). To learn about the compliance programs that apply to Amazon Key Management Service (Amazon KMS), see [Amazon Services in Scope by Compliance Program](#).
- **Security in the cloud** – Your responsibility is determined by the Amazon service that you use. In Amazon KMS, in addition to your configuration and use of Amazon KMS keys, you are responsible for other factors including the sensitivity of your data, your company's requirements, and applicable laws and regulations

This documentation helps you understand how to apply the shared responsibility model when using Amazon Key Management Service. It shows you how to configure Amazon KMS to meet your security and compliance objectives.

Topics

- [Data protection in Amazon Key Management Service](#)
- [Identity and access management for Amazon Key Management Service](#)
- [Logging and monitoring in Amazon Key Management Service](#)
- [Compliance validation for Amazon Key Management Service](#)
- [Resilience in Amazon Key Management Service](#)
- [Infrastructure security in Amazon Key Management Service](#)

Data protection in Amazon Key Management Service

Amazon Key Management Service stores and protects your encryption keys to make them highly available while providing you with strong and flexible access control.

Topics

- [Protecting key material](#)
- [Data encryption](#)
- [Internet network traffic privacy](#)

Protecting key material

By default, Amazon KMS generates and protects the cryptographic key material for KMS keys. In addition, Amazon KMS offers options for key material that is created and protected outside of Amazon KMS.

Protecting key material generated in Amazon KMS

When you create a KMS key, by default, Amazon KMS generates and protects the cryptographic material for the KMS key.

To safeguard key material for KMS keys, Amazon KMS relies on a distributed fleet of [FIPS 140-3 Security Level 3–validated](#) hardware security modules (HSMs). Each Amazon KMS HSM is a dedicated, standalone hardware appliance designed to provide dedicated cryptographic functions to meet the security and scalability requirements of Amazon KMS. (The HSMs that Amazon KMS uses in China Regions are certified by [OSCCA](#) and comply with all pertinent Chinese regulations, but are not validated under the FIPS 140-3 Cryptographic Module Validation Program.)

The key material for a KMS key is encrypted by default when it is generated in the HSM. The key material is decrypted only within HSM volatile memory and only for the few milliseconds that it takes to use it in a cryptographic operation. Whenever the key material is not in active use, it is encrypted within the HSM and transferred to [highly durable](#) (99.999999999%), low-latency persistent storage where it remains separate and isolated from the HSMs. Plaintext key material never leaves the HSM [security boundary](#); it is never written to disk or persisted in any storage medium. (The only exception is the public key of an asymmetric key pair, which is not secret.)

Amazon asserts as a fundamental security principle that there is no human interaction with plaintext cryptographic key material of any type in any Amazon Web Services service. There is no mechanism for anyone, including Amazon Web Services service operators, to view, access, or export plaintext key material. This principle applies even during catastrophic failures and disaster recovery events. Plaintext customer key material in Amazon KMS is used for cryptographic operations within Amazon KMS FIPS 140-3 validated HSMs only in response to authorized requests made to the service by the customer or their delegate.

For [customer managed keys](#), the Amazon Web Services account that creates the key is the sole and non-transferable owner of the key. The owning account has complete and exclusive control over the authorization policies that control access to the key. For Amazon managed keys, the Amazon Web Services account has complete control over the IAM policies that authorize requests to the Amazon Web Services service.

Protecting key material generated outside of Amazon KMS

Amazon KMS provides alternatives to key material generated in Amazon KMS.

[Custom key stores](#), an optional Amazon KMS feature, let you create KMS keys backed by key material that is generated and used outside of Amazon KMS. KMS keys in [Amazon CloudHSM key stores](#) are backed by keys in Amazon CloudHSM hardware security modules that you control. These HSMs are certified at [FIPS 140-2 Security Level 3 or 140-3 Security Level 3](#). KMS keys in [external key stores](#) are backed by keys in an external key manager that you control and manage outside of Amazon, such as a physical HSM in your private data center.

Another optional feature lets you [import the key material](#) for a KMS key. To protect imported key material while it is in transit to Amazon KMS, you encrypt the key material using a public key from an RSA key pair generated in an Amazon KMS HSM. The imported key material is decrypted in an Amazon KMS HSM and re-encrypted under a symmetric key in the HSM. Like all Amazon KMS key material, plaintext imported key material never leaves the HSMs unencrypted. However, the customer who provided the key material is responsible for secure use, durability, and maintenance of the key material outside of Amazon KMS.

Data encryption

The data in Amazon KMS consists of Amazon KMS keys and the encryption key material they represent. This key material exists in plaintext only within Amazon KMS hardware security modules (HSMs) and only when in use. Otherwise, the key material is encrypted and stored in durable persistent storage.

The key material that Amazon KMS generates for KMS keys never leaves the boundary of Amazon KMS HSMs unencrypted. It is not exported or transmitted in any Amazon KMS API operations. The exception is for [multi-Region keys](#), where Amazon KMS uses a cross-Region replication mechanism to copy the key material for a multi-Region key from an HSM in one Amazon Web Services Region to an HSM in a different Amazon Web Services Region. For details, see [Replication process for multi-Region keys](#) in Amazon Key Management Service Cryptographic Details.

Topics

- [Encryption at rest](#)
- [Encryption in transit](#)

Encryption at rest

Amazon KMS generates key material for Amazon KMS keys in [FIPS 140-3 Security Level 3](#)-compliant hardware security modules (HSMs). The only exception is China Regions, where the HSMs that Amazon KMS uses to generate KMS keys comply with all pertinent Chinese regulations, but are not validated under the FIPS 140-3 Cryptographic Module Validation Program. When not in use, key material is encrypted by an HSM key and written to durable, persistent storage. The key material for KMS keys and the encryption keys that protect the key material never leave the HSMs in plaintext form.

Encryption and management of key material for KMS keys is handled entirely by Amazon KMS.

For more details, see [Working with Amazon KMS keys](#) in Amazon Key Management Service Cryptographic Details.

Encryption in transit

Key material that Amazon KMS generates for KMS keys is never exported or transmitted in Amazon KMS API operations. Amazon KMS uses [key identifiers](#) to represent the KMS keys in API operations. Similarly, key material for KMS keys in Amazon KMS [custom key stores](#) is non-exportable and never transmitted in Amazon KMS or Amazon CloudHSM API operations.

However, some Amazon KMS API operations return [data keys](#). Also, customers can use API operations to [import key material](#) for selected KMS keys.

All Amazon KMS API calls must be signed and transmitted using Transport Layer Security (TLS). Amazon KMS requires TLS 1.2 and recommends TLS 1.3 in all regions. Amazon KMS also supports hybrid post-quantum TLS for Amazon KMS service endpoints in all regions, except China Regions. Amazon KMS does not support hybrid post-quantum TLS for FIPS endpoints in Amazon GovCloud (US). Calls to Amazon KMS also require a modern cipher suite that supports *perfect forward secrecy*, which means that compromise of any secret, such as a private key, does not also compromise the session key.

If you require FIPS 140-3 validated cryptographic modules when accessing Amazon through a command line interface or an API, use a FIPS endpoint. To use standard Amazon KMS endpoints

or Amazon KMS FIPS endpoints, clients must support TLS 1.2 or later. For more information about the available FIPS endpoints, see [Federal Information Processing Standard \(FIPS\) 140-3](#). For a list of Amazon KMS FIPS endpoints, see [Amazon Key Management Service endpoints and quotas](#) in the Amazon Web Services General Reference.

Communications between Amazon KMS service hosts and HSMs are protected using Elliptic Curve Cryptography (ECC) and Advanced Encryption Standard (AES) in an authenticated encryption scheme. For more details, see [Internal communication security](#) in Amazon Key Management Service Cryptographic Details.

Internetwork traffic privacy

Amazon KMS supports an Amazon Web Services Management Console and a set of API operations that enable you to create and manage Amazon KMS keys and use them in cryptographic operations.

Amazon KMS supports two network connectivity options from your private network to Amazon.

- An IPsec VPN connection over the internet
- [Amazon Direct Connect](#), which links your internal network to an Amazon Direct Connect location over a standard Ethernet fiber-optic cable.

All Amazon KMS API calls must be signed and be transmitted using Transport Layer Security (TLS). The calls also require a modern cipher suite that supports [perfect forward secrecy](#). Traffic to the hardware security modules (HSMs) that store key material for KMS keys is permitted only from known Amazon KMS API hosts over the Amazon internal network.

To connect directly to Amazon KMS from your virtual private cloud (VPC) without sending traffic over the public internet, use VPC endpoints, powered by [Amazon PrivateLink](#). For more information, see [Connect to Amazon KMS through a VPC endpoint](#).

Amazon KMS also supports a [hybrid post-quantum key exchange](#) option for the Transport Layer Security (TLS) network encryption protocol. You can use this option with TLS when you connect to Amazon KMS API endpoints.

Identity and access management for Amazon Key Management Service

Amazon Identity and Access Management (IAM) helps you securely control access to Amazon resources. Administrators control who can be *authenticated* (signed in) and *authorized* (have permissions) to use Amazon KMS resources. For more information, see [Using IAM policies with Amazon KMS](#).

[Key policies](#) are the primary mechanism for controlling access to KMS keys in Amazon KMS. Every KMS key must have a key policy. You can also use [IAM policies](#) and [grants](#), along with key policies, to control access to your KMS keys. For more information, see [KMS key access and permissions](#).

If you are using an Amazon Virtual Private Cloud (Amazon VPC), you can [create an interface VPC endpoint](#) to Amazon KMS powered by [Amazon PrivateLink](#). You can also use VPC endpoint policies to determine which principals can access your Amazon KMS endpoint, which API calls they can make, and which KMS key they can access.

Topics

- [Amazon managed policies for Amazon Key Management Service](#)
- [Using service-linked roles for Amazon KMS](#)

Amazon managed policies for Amazon Key Management Service

An Amazon managed policy is a standalone policy that is created and administered by Amazon. Amazon managed policies are designed to provide permissions for many common use cases so that you can start assigning permissions to users, groups, and roles.

Keep in mind that Amazon managed policies might not grant least-privilege permissions for your specific use cases because they're available for all Amazon customers to use. We recommend that you reduce permissions further by defining [customer managed policies](#) that are specific to your use cases.

You cannot change the permissions defined in Amazon managed policies. If Amazon updates the permissions defined in an Amazon managed policy, the update affects all principal identities (users, groups, and roles) that the policy is attached to. Amazon is most likely to update an Amazon managed policy when a new Amazon Web Services service is launched or new API operations become available for existing services.

For more information, see [Amazon managed policies](#) in the *IAM User Guide*.

Amazon managed policy: `AWSKeyManagementServicePowerUser`

You can attach the `AWSKeyManagementServicePowerUser` policy to your IAM identities.

You can use the `AWSKeyManagementServicePowerUser` managed policy to give IAM principals in your account the permissions of a power user. Power users can create KMS keys, use and manage the KMS keys they create, and view all KMS keys and IAM identities. Principals who have the `AWSKeyManagementServicePowerUser` managed policy can also get permissions from other sources, including key policies, other IAM policies, and grants.

`AWSKeyManagementServicePowerUser` is an Amazon managed IAM policy. For more information about Amazon managed policies, see [Amazon managed policies](#) in the *IAM User Guide*.

Note

Permissions in this policy that are specific to a KMS key, such as `kms:TagResource` and `kms:GetKeyRotationStatus`, are effective only when the key policy for that KMS key [explicitly allows the Amazon Web Services account to use IAM policies](#) to control access to the key. To determine whether a permission is specific to a KMS key, see [Amazon KMS permissions](#) and look for a value of **KMS key** in the **Resources** column.

This policy gives a power user permissions on any KMS key with a key policy that permits the operation. For cross-account permissions, such as `kms:DescribeKey` and `kms:ListGrants`, this might include KMS keys in untrusted Amazon Web Services accounts. For details, see [Best practices for IAM policies](#) and [Allowing users in other accounts to use a KMS key](#). To determine whether a permission is valid on KMS keys in other accounts, see [Amazon KMS permissions](#) and look for a value of **Yes** in the **Cross-account use** column.

To allow principals to view the Amazon KMS console without errors, the principal needs the `tag:GetResources` permission, which is not included in the `AWSKeyManagementServicePowerUser` policy. You can allow this permission in a separate IAM policy.

The [AWSKeyManagementServicePowerUser](#) managed IAM policy includes the following permissions.

- Allows principals to create KMS keys. Because this process includes setting the key policy, power users can give themselves and others permission to use and manage the KMS keys they create.
- Allows principals to create and delete [aliases](#) and [tags](#) on all KMS keys. Changing a tag or alias can allow or deny permission to use and manage the KMS key. For details, see [ABAC for Amazon KMS](#).
- Allows principals to get detailed information about all KMS keys, including their key ARN, cryptographic configuration, key policy, aliases, tags, and [rotation status](#).
- Allows principals to list IAM users, groups, and roles.
- This policy does not allow principals to use or manage KMS keys that they didn't create. However, they can change aliases and tags on all KMS keys, which might allow or deny them permission to use or manage a KMS key.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "kms:CreateAlias",
        "kms:CreateKey",
        "kms>DeleteAlias",
        "kms:Describe*",
        "kms:GenerateRandom",
        "kms:Get*",
        "kms:List*",
        "kms:TagResource",
        "kms:UntagResource",
        "iam:ListGroups",
        "iam:ListRoles",
        "iam:ListUsers"
      ],
      "Resource": "*"
    }
  ]
}
```

Amazon managed policy:**`AWSServiceRoleForKeyManagementServiceCustomKeyStores`**

You can't attach `AWSServiceRoleForKeyManagementServiceCustomKeyStores` to your IAM entities. This policy is attached to a service-linked role that gives Amazon KMS permission to view the Amazon CloudHSM clusters associated with your Amazon CloudHSM key store and create the network to support a connection between your custom key store and its Amazon CloudHSM cluster. For more information, see [Authorizing Amazon KMS to manage Amazon CloudHSM and Amazon EC2 resources](#).

Amazon managed policy:**`AWSServiceRoleForKeyManagementServiceMultiRegionKeys`**

You can't attach `AWSServiceRoleForKeyManagementServiceMultiRegionKeys` to your IAM entities. This policy is attached to a service-linked role that gives Amazon KMS permission to synchronize any changes to the key material of a multi-Region primary key to its replica keys. For more information, see [Authorizing Amazon KMS to synchronize multi-Region keys](#).

Amazon KMS updates to Amazon managed policies

View details about updates to Amazon managed policies for Amazon KMS since this service began tracking these changes. For automatic alerts about changes to this page, subscribe to the RSS feed on the Amazon KMS [Document history](#) page.

Change	Description	Date
AWSKeyManagementServiceMultiRegionKeysServiceRolePolicy – Update to existing policy	Amazon KMS added a statement ID (Sid) field to the managed policy in policy version v2.	November 21, 2024
AWSKeyManagementServiceCustomKeyStoresServiceRolePolicy – Update to existing policy	Amazon KMS added the <code>ec2:DescribeVpcs</code> , <code>ec2:DescribeNetworkAcls</code> , and <code>ec2:DescribeNetworkInterfaces</code> permissions to monitor changes in the VPC that	November 10, 2023

Change	Description	Date
	contains your Amazon CloudHSM cluster so that Amazon KMS can provide clear error messages in the case of failures.	
Amazon KMS started tracking changes	Amazon KMS started tracking changes for its Amazon managed policies.	November 10, 2023

Using service-linked roles for Amazon KMS

Amazon Key Management Service uses Amazon Identity and Access Management (IAM) [service-linked roles](#). A service-linked role is a unique type of IAM role that is linked directly to Amazon KMS. Service-linked roles are defined by Amazon KMS and include all the permissions that the service requires to call other Amazon services on your behalf.

A service-linked role makes setting up Amazon KMS easier because you don't have to manually add the necessary permissions. Amazon KMS defines the permissions of its service-linked roles, and unless defined otherwise, only Amazon KMS can assume its roles. The defined permissions include the trust policy and the permissions policy, and that permissions policy cannot be attached to any other IAM entity.

You can delete a service-linked role only after first deleting the related resources. This protects your Amazon KMS resources because you can't inadvertently remove permission to access the resources.

For information about other services that support service-linked roles, see [Amazon Services That Work with IAM](#) and look for the services that have **Yes** in the **Service-Linked Role** column. Choose a **Yes** with a link to view the service-linked role documentation for that service.

To view details about updates to the service-linked roles discussed in this topic, see [Amazon KMS updates to Amazon managed policies](#).

Topics

- [Authorizing Amazon KMS to manage Amazon CloudHSM and Amazon EC2 resources](#)

- [Authorizing Amazon KMS to synchronize multi-Region keys](#)

Authorizing Amazon KMS to manage Amazon CloudHSM and Amazon EC2 resources

To support your Amazon CloudHSM key stores, Amazon KMS needs permission to get information about your Amazon CloudHSM clusters. It also needs permission to create the network infrastructure that connects your Amazon CloudHSM key store to its Amazon CloudHSM cluster. To get these permissions, Amazon KMS creates the **AWSServiceRoleForKeyManagementServiceCustomKeyStores** service-linked role in your Amazon Web Services account. Users who create Amazon CloudHSM key stores must have the `iam:CreateServiceLinkedRole` permission that allows them to create service-linked roles.

To view details about updates to the **AWSKeyManagementServiceCustomKeyStoresServiceRolePolicy** managed policy, see [Amazon KMS updates to Amazon managed policies](#).

Topics

- [About the Amazon KMS service-linked role](#)
- [Create the service-linked role](#)
- [Edit the service-linked role description](#)
- [Delete the service-linked role](#)

About the Amazon KMS service-linked role

A [service-linked role](#) is an IAM role that gives one Amazon service permission to call other Amazon services on your behalf. It's designed to make it easier for you to use the features of multiple integrated Amazon services without having to create and maintain complex IAM policies. For more information, see [Using service-linked roles for Amazon KMS](#).

For Amazon CloudHSM key stores, Amazon KMS creates the **AWSServiceRoleForKeyManagementServiceCustomKeyStores** service-linked role with the **AWSKeyManagementServiceCustomKeyStoresServiceRolePolicy** managed policy. This policy grants the role the following permissions:

- [cloudhsm:Describe*](#) – detects changes in the Amazon CloudHSM cluster that is attached to your custom key store.

- [ec2:CreateSecurityGroup](#) – used when you [connect an Amazon CloudHSM key store](#) to create the security group that enables network traffic flow between Amazon KMS and your Amazon CloudHSM cluster.
- [ec2:AuthorizeSecurityGroupIngress](#) – used when you [connect an Amazon CloudHSM key store](#) to allow network access from Amazon KMS into the VPC that contains your Amazon CloudHSM cluster.
- [ec2:CreateNetworkInterface](#) – used when you [connect an Amazon CloudHSM key store](#) to create the network interface used for communication between Amazon KMS and the Amazon CloudHSM cluster.
- [ec2:RevokeSecurityGroupEgress](#) – used when you [connect an Amazon CloudHSM key store](#) to remove all outbound rules from the security group that Amazon KMS created.
- [ec2>DeleteSecurityGroup](#) – used when you [disconnect an Amazon CloudHSM key store](#) to delete security groups that were created when you connected the Amazon CloudHSM key store.
- [ec2:DescribeSecurityGroups](#) – used to monitor changes in the security group that Amazon KMS created in the VPC that contains your Amazon CloudHSM cluster so that Amazon KMS can provide clear error messages in case of failures.
- [ec2:DescribeVpcs](#) – used to monitor changes in the VPC that contains your Amazon CloudHSM cluster so that Amazon KMS can provide clear error messages in case of failures.
- [ec2:DescribeNetworkAcls](#) – used to monitor changes in the network ACLs for the VPC that contains your Amazon CloudHSM cluster so that Amazon KMS can provide clear error messages in case of failures.
- [ec2:DescribeNetworkInterfaces](#) – used to monitor changes in the network interfaces that Amazon KMS created in the VPC that contains your Amazon CloudHSM cluster so that Amazon KMS can provide clear error messages in case of failures.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "cloudhsm:Describe*",
        "ec2:CreateNetworkInterface",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:CreateSecurityGroup",
        "ec2:DescribeSecurityGroups",
```

```
        "ec2:RevokeSecurityGroupEgress",
        "ec2:DeleteSecurityGroup",
        "ec2:DescribeVpcs",
        "ec2:DescribeNetworkAcls",
        "ec2:DescribeNetworkInterfaces"
    ],
    "Resource": "*"
}
]
```

Because the **AWSServiceRoleForKeyManagementServiceCustomKeyStores** service-linked role trusts only `cks.kms.amazonaws.com`, only Amazon KMS can assume this service-linked role. This role is limited to the operations that Amazon KMS needs to view your Amazon CloudHSM clusters and to connect an Amazon CloudHSM key store to its associated Amazon CloudHSM cluster. It does not give Amazon KMS any additional permissions. For example, Amazon KMS does not have permission to create, manage, or delete your Amazon CloudHSM clusters, HSMs, or backups.

Regions

Like the Amazon CloudHSM key stores feature, the

AWSServiceRoleForKeyManagementServiceCustomKeyStores role is supported in all Amazon Web Services Regions where Amazon KMS and Amazon CloudHSM are available. For a list of Amazon Web Services Regions that each service supports, see [Amazon Key Management Service Endpoints and Quotas](#) and [Amazon CloudHSM endpoints and quotas](#) in the *Amazon Web Services General Reference*.

For more information about how Amazon services use service-linked roles, see [Using service-linked roles](#) in the IAM User Guide.

Create the service-linked role

Amazon KMS automatically creates the

AWSServiceRoleForKeyManagementServiceCustomKeyStores service-linked role in your Amazon Web Services account when you create an Amazon CloudHSM key store, if the role does not already exist. You cannot create or re-create this service-linked role directly.

Edit the service-linked role description

You cannot edit the role name or the policy statements in the **AWSServiceRoleForKeyManagementServiceCustomKeyStores** service-linked role, but you can edit role description. For instructions, see [Editing a service-linked role](#) in the *IAM User Guide*.

Delete the service-linked role

Amazon KMS does not delete the **AWSServiceRoleForKeyManagementServiceCustomKeyStores** service-linked role from your Amazon Web Services account even if you have [deleted all of your Amazon CloudHSM key stores](#). Although there is currently no procedure for deleting the **AWSServiceRoleForKeyManagementServiceCustomKeyStores** service-linked role, Amazon KMS does not assume this role or use its permissions unless you have active Amazon CloudHSM key stores.

Authorizing Amazon KMS to synchronize multi-Region keys

To support [multi-Region keys](#), Amazon KMS needs permission to synchronize the [shared properties](#) of a multi-Region primary key with its replica keys. To get these permissions, Amazon KMS creates the **AWSServiceRoleForKeyManagementServiceMultiRegionKeys** service-linked role in your Amazon Web Services account. Users who create multi-Region keys must have the `iam:CreateServiceLinkedRole` permission that allows them to create service-linked roles.

You can view the [SynchronizeMultiRegionKey](#) CloudTrail event that records Amazon KMS synchronizing shared properties in your Amazon CloudTrail logs.

To view details about updates to the **AWSKeyManagementServiceMultiRegionKeysServiceRolePolicy** managed policy, see [Amazon KMS updates to Amazon managed policies](#).

Topics

- [About the service-linked role for multi-Region keys](#)
- [Create the service-linked role](#)
- [Edit the service-linked role description](#)
- [Delete the service-linked role](#)

About the service-linked role for multi-Region keys

A [service-linked role](#) is an IAM role that gives one Amazon service permission to call other Amazon services on your behalf. It's designed to make it easier for you to use the features of multiple integrated Amazon services without having to create and maintain complex IAM policies.

For multi-Region keys, Amazon KMS creates the

AWSServiceRoleForKeyManagementServiceMultiRegionKeys service-linked role with the **AWSKeyManagementServiceMultiRegionKeysServiceRolePolicy** managed policy. This policy gives the role the `kms:SynchronizeMultiRegionKey` permission, which allows it to synchronize the shared properties of multi-Region keys.

Because the **AWSServiceRoleForKeyManagementServiceMultiRegionKeys** service-linked role trusts only `mrk.kms.amazonaws.com`, only Amazon KMS can assume this service-linked role. This role is limited to the operations that Amazon KMS needs to synchronize multi-Region shared properties. It does not give Amazon KMS any additional permissions. For example, Amazon KMS does not have permission to create, replicate, or delete any KMS keys.

For more information about how Amazon services use service-linked roles, see [Using Service-Linked Roles](#) in the IAM User Guide.

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "KMSSynchronizeMultiRegionKey",
      "Effect" : "Allow",
      "Action" : [
        "kms:SynchronizeMultiRegionKey"
      ],
      "Resource" : "*"
    }
  ]
}
```

Create the service-linked role

Amazon KMS automatically creates the

AWSServiceRoleForKeyManagementServiceMultiRegionKeys service-linked role in your Amazon Web Services account when you create a multi-Region key, if the role does not already exist. You cannot create or re-create this service-linked role directly.

Edit the service-linked role description

You cannot edit the role name or the policy statements in the **AWSServiceRoleForKeyManagementServiceMultiRegionKeys** service-linked role, but you can edit the role description. For instructions, see [Editing a Service-Linked Role](#) in the *IAM User Guide*.

Delete the service-linked role

Amazon KMS does not delete the **AWSServiceRoleForKeyManagementServiceMultiRegionKeys** service-linked role from your Amazon Web Services account and you cannot delete it. However, Amazon KMS does not assume the **AWSServiceRoleForKeyManagementServiceMultiRegionKeys** role or use any of its permissions unless you have multi-Region keys in your Amazon Web Services account and Region.

Logging and monitoring in Amazon Key Management Service

Monitoring is an important part of understanding the availability, state, and usage of your Amazon KMS keys in Amazon KMS. Monitoring helps maintain the security, reliability, availability, and performance of your Amazon solutions. Amazon provides several tools for monitoring your KMS keys.

Amazon CloudTrail Logs

Every call to an Amazon KMS API operation is captured as an event in an Amazon CloudTrail log. These logs record all API calls from the Amazon KMS console, and calls made by Amazon KMS and other Amazon services. Cross-account API calls, such as a call to use a KMS key in a different Amazon Web Services account, are recorded in the CloudTrail logs of both accounts.

When troubleshooting or auditing, you can use the log to reconstruct the lifecycle of a KMS key. You can also view its management and use of the KMS key in cryptographic operations. For more information, see [the section called “Logging with Amazon CloudTrail”](#).

Amazon CloudWatch Logs

Monitor, store, and access your log files from Amazon CloudTrail and other sources. For more information, see the [Amazon CloudWatch User Guide](#).

For Amazon KMS, CloudWatch stores useful information that helps you to prevent problems with your KMS keys and the resources that they protect. For more information, see [the section called “Monitor keys with CloudWatch”](#).

Amazon EventBridge

Amazon KMS generates EventBridge events when your KMS key is [rotated](#) or [deleted](#) or the [imported key material](#) in your KMS key expires. Search for Amazon KMS events (API operations) and route them to one or more target functions or streams to capture state information. For more information, see [the section called “Monitor keys with Amazon EventBridge”](#) and the [Amazon EventBridge User Guide](#).

Amazon CloudWatch Metrics

You can monitor your KMS keys using CloudWatch metrics, which collects and processes raw data from Amazon KMS into performance metrics. The data are recorded in two-week intervals so you can view trends of current and historical information. This helps you to understand how your KMS keys are used and how their use changes over time. For information about using CloudWatch metrics to monitor KMS keys, see [Amazon KMS metrics and dimensions](#).

Amazon CloudWatch Alarms

Watch a single metric change over a time period that you specify. Then perform actions based on the value of the metric relative to a threshold over a number of time periods. For example, you can create a CloudWatch alarm that is triggered when someone tries to use a KMS key that is scheduled to be deleted in a cryptographic operation. This indicates that the KMS key is still being used and probably should not be deleted. For more information, see [the section called “Create an alarm”](#).

Amazon Security Hub

You can monitor your Amazon KMS usage for security industry standards and best practices compliance using Amazon Security Hub. Security Hub uses security controls to evaluate resource configurations and security standards to help you comply with various compliance frameworks. For more information, see [Amazon Key Management Service controls](#) in the *Amazon Security Hub User Guide*.

Compliance validation for Amazon Key Management Service

Third-party auditors assess the security and compliance of Amazon Key Management Service as part of multiple Amazon compliance programs. These include SOC, PCI, FedRAMP, HIPAA, and others.

Topics

- [Compliance and security documents](#)
- [Learn more](#)

Compliance and security documents

The following compliance and security documents cover Amazon KMS. To view them, use [Amazon Artifact](#).

- Cloud Computing Compliance Controls Catalogue (C5)
- ISO 27001:2013 Statement of Applicability (SoA)
- ISO 27001:2013 Certification
- ISO 27017:2015 Statement of Applicability (SoA)
- ISO 27017:2015 Certification
- ISO 27018:2015 Statement of Applicability (SoA)
- ISO 27018:2014 Certification
- ISO 9001:2015 Certification
- PCI DSS Attestation of Compliance (AOC) and Responsibility Summary
- Service Organization Controls (SOC) 1 Report
- Service Organization Controls (SOC) 2 Report
- Service Organization Controls (SOC) 2 Report For Confidentiality
- FedRAMP-High

For help using Amazon Artifact, see [Downloading Reports in Amazon Artifact](#).

Learn more

Your compliance responsibility when using Amazon KMS is determined by the sensitivity of your data, your company's compliance objectives, and applicable laws and regulations. If your use of Amazon KMS is subject to compliance with a published standard, Amazon provides resources to help:

- [Amazon Services in Scope by Compliance Program](#) – This page lists Amazon services that are in scope of specific compliance programs. For general information, see [Amazon Compliance Programs](#).

- [Security and Compliance Quick Start Guides](#) – These deployment guides discuss architectural considerations and provide steps for deploying security- and compliance-focused baseline environments on Amazon.
- [Amazon Compliance Resources](#) – This collection of workbooks and guides might apply to your industry and location.
- [Amazon Config](#) – This Amazon service assesses how well your resource configurations comply with internal practices, industry guidelines, and regulations.
- [Amazon Security Hub](#) – This Amazon service provides a comprehensive view of your security state within Amazon. Security Hub uses security controls to evaluate your Amazon resources and to check your compliance against security industry standards and best practices. For a list of supported services and controls, see [Security Hub controls reference](#).

Resilience in Amazon Key Management Service

The Amazon global infrastructure is built around Amazon Web Services Regions and Availability Zones. Amazon Web Services Regions provide multiple physically separated and isolated Availability Zones, which are connected with low-latency, high-throughput, and highly redundant networking. With Availability Zones, you can design and operate applications and databases that automatically fail over between Availability Zones without interruption. Availability Zones are more highly available, fault tolerant, and scalable than traditional single or multiple data center infrastructures.

In addition to the Amazon global infrastructure, Amazon KMS offers several features to help support your data resiliency and backup needs. For more information about Amazon Web Services Regions and Availability Zones, see [Amazon Global Infrastructure](#).

Regional isolation

Amazon Key Management Service (Amazon KMS) is a self-sustaining Regional service that is available in all Amazon Web Services Regions. The Regionally isolated design of Amazon KMS ensures that an availability issue in one Amazon Web Services Region cannot affect Amazon KMS operation in any other Region. Amazon KMS is designed to ensure *zero planned downtime*, with all software updates and scaling operations performed seamlessly and imperceptibly.

The Amazon KMS [Service Level Agreement](#) (SLA) includes a service commitment of 99.999% for all KMS APIs. To fulfill this commitment, Amazon KMS ensures that all data and authorization

information required to execute an API request is available on all regional hosts that receive the request.

The Amazon KMS infrastructure is replicated in at least three Availability Zones (AZs) in each Region. To ensure that multiple host failures do not affect Amazon KMS performance, Amazon KMS is designed to service customer traffic from any of the AZs in a Region.

Changes that you make to the properties or permissions of a KMS key are replicated to all hosts in the Region to ensure that subsequent request can be processed correctly by any host in the Region. Requests for [cryptographic operations](#) using your KMS key are forwarded to a fleet of Amazon KMS hardware security modules (HSMs), any of which can perform the operation with the KMS key.

Multi-tenant design

The multi-tenant design of Amazon KMS enables it to fulfill the 99.999% availability SLA, and to sustain high request rates, while protecting the confidentiality of your keys and data.

Multiple integrity-enforcing mechanisms are deployed to ensure that the KMS key that you specified for the cryptographic operation is always the one that is used.

The plaintext key material for your KMS keys is protected extensively. The key material is encrypted in the HSM as soon as it is created, and the encrypted key material is immediately moved to secure, low latency storage. The encrypted key is retrieved and decrypted within the HSM just in time for use. The plaintext key remains in HSM memory only for the time needed to complete the cryptographic operation. Then it is re-encrypted in the HSM and the encrypted key is returned to storage. Plaintext key material never leaves the HSMs; it is never written to persistent storage.

Resilience best practices in Amazon KMS

To optimize resilience for your Amazon KMS resources, consider the following strategies.

- To support your backup and disaster recovery strategy, consider *multi-Region keys*, which are KMS keys created in one Amazon Web Services Region and replicated only to Regions that you specify. With multi-Region keys, you can move encrypted resources between Amazon Web Services Regions (within the same partition) without ever exposing the plaintext, and decrypt the resource, when needed, in any of its destination Regions. Related multi-Region keys are interoperable because they share the same key material and key ID, but they have independent key policies for high-resolution access control. For details, see [Multi-Region keys in Amazon KMS](#).
- To protect your keys in a multi-tenant service like Amazon KMS, be sure to use access controls, including [key policies](#) and [IAM policies](#). In addition, you can send your requests to Amazon KMS

using a *VPC interface endpoint* powered by Amazon PrivateLink. When you do, all communication between your Amazon VPC and Amazon KMS is conducted entirely within the Amazon network using a dedicated Amazon KMS endpoint restricted to your VPC. You can further secure these requests by creating an additional authorization layer using [VPC endpoint policies](#). For details, see [Connecting to Amazon KMS through a VPC endpoint](#).

Infrastructure security in Amazon Key Management Service

As a managed service, Amazon Key Management Service (Amazon KMS) is protected by the Amazon global network security procedures that are described in the [Amazon Web Services: Overview of Security Processes](#).

To access Amazon KMS over the network, you can call the Amazon KMS API operations that are described in the [Amazon Key Management Service API Reference](#). Amazon KMS requires TLS 1.2 and recommends TLS 1.3 in all regions. Amazon KMS also supports hybrid post-quantum TLS for Amazon KMS service endpoints in all regions, except China Regions. Amazon KMS does not support hybrid post-quantum TLS for FIPS endpoints in Amazon GovCloud (US). To use [standard Amazon KMS endpoints](#) or [Amazon KMS FIPS endpoints](#), clients must support TLS 1.2 or later. Clients must also support cipher suites with perfect forward secrecy (PFS) such as Ephemeral Diffie-Hellman (DHE) or Elliptic Curve Ephemeral Diffie-Hellman (ECDHE). Most modern systems, such as Java 7 and later, support these modes.

Additionally, requests must be signed by using an access key ID and a secret access key that is associated with an IAM principal. Or you can use the [Amazon Security Token Service](#) (Amazon STS) to generate temporary security credentials to sign requests.

You can call these API operations from any network location, but Amazon KMS supports global policy conditions that let you control access to a KMS key based on the source IP address, VPC, and VPC endpoint. You can use these condition keys in key policies and IAM policies. However, these conditions can prevent Amazon from using the KMS key on your behalf. For details, see [Amazon global condition keys](#).

For example, the following key policy statement allows users who can assume the `KMSTestRole` role to use this Amazon KMS key for the specified [cryptographic operations](#) unless the source IP address is one of the IP addresses specified in the policy.

```
{
  "Version": "2012-10-17",
```

```
"Statement": {
  "Effect": "Allow",
  "Principal": {"AWS":
    "arn:aws:iam::111122223333:role/KMSTestRole"},
  "Action": [
    "kms:Encrypt",
    "kms:Decrypt",
    "kms:ReEncrypt*",
    "kms:GenerateDataKey*",
    "kms:DescribeKey"
  ],
  "Resource": "*",
  "Condition": {
    "NotIpAddress": {
      "aws:SourceIp": [
        "192.0.2.0/24",
        "203.0.113.0/24"
      ]
    }
  }
}
```

Isolation of Physical Hosts

The security of the physical infrastructure that Amazon KMS uses is subject to the controls described in the **Physical and Environmental Security** section of the [Amazon Web Services: Overview of Security Processes](#). You can find more detail in compliance reports and third-party audit findings listed in the previous section.

Amazon KMS is supported by dedicated hardened hardware security modules (HSMs) designed with specific controls to resist physical attacks. The HSMs are physical devices that *do not* have a virtualization layer, such as a hypervisor, that shares the physical device among several logical tenants. The key material for Amazon KMS keys is stored only in volatile memory on the HSMs, and only while the KMS key is in use. This memory is erased when the HSM moves out of the operational state, including intended and unintended shutdowns and resets. For detailed information about the operation of Amazon KMS HSMs, see [Amazon Key Management Service Cryptographic Details](#).

Quotas

To make Amazon KMS responsive and performant for all users, Amazon KMS applies two types of quotas, resource quotas and request quotas. Each quota is calculated independently for each Region of each Amazon Web Services account.

All Amazon KMS quotas are adjustable, except for the [on-demand rotation resource quota](#) and the [Amazon CloudHSM key store request quota](#). To request a quota increase, see [Requesting a quota increase](#) in the *Service Quotas User Guide*. To request a quota decrease, to change a quota that is not listed in Service Quotas, or to change a quota in an Amazon Web Services Region where Service Quotas for Amazon KMS is not available, please visit [Amazon Web Services Support Center](#) and create a case.

Topics

- [Resource quotas](#)
- [Request quotas](#)
- [Throttling Amazon KMS requests](#)

Resource quotas

Amazon KMS establishes resource quotas to ensure that it can provide fast and resilient service to all of our customers. Some resource quotas apply only to resources that you create, but not to resources that Amazon services create for you. Resources that you use, but that aren't in your Amazon Web Services account, such as [Amazon owned keys](#), do not count against these quotas.

If you have exceeded a resource limit, requests to create an additional resource of that type generate an `LimitExceededException` error message.

All Amazon KMS resource quotas are adjustable, except for the [on-demand rotation resource quota](#). To request a quota increase, see [Requesting a quota increase](#) in the *Service Quotas User Guide*. To request a quota decrease, to change a quota that is not listed in Service Quotas, or to change a quota in an Amazon Web Services Region where Service Quotas for Amazon KMS is not available, please visit [Amazon Web Services Support Center](#) and create a case.

The following table lists and describes the Amazon KMS resource quotas in each Amazon Web Services account and Region.

Quota name	Default value	Applies to	Adjustable
Amazon KMS keys	100,000	Customer managed keys	Yes
Aliases per KMS key	50	Customer created aliases	Yes
Grants per KMS key	50,000	Customer managed keys	Yes
Custom key store resource quota	10	Amazon Web Services account and Region	Yes
On-demand rotation	10	Customer managed keys	No

In addition to resource quotas, Amazon KMS uses request quotas to ensure the responsiveness of the service. For details, see [the section called “Request quotas”](#).

Amazon KMS keys: 100,000

You can have up to 100,000 [customer managed keys](#) in each Region of your Amazon Web Services account. This quota applies to all customer managed keys in all Amazon Web Services Regions regardless of their [key spec](#) or [key state](#). Each KMS key is considered to be one resource. [Amazon managed keys](#) and [Amazon owned keys](#) do not count against this quota.

Aliases per KMS key: 50

You can associate up to 50 [aliases](#) with each [customer managed key](#). Aliases that Amazon associates with [Amazon managed keys](#) do not count against this quota. You might encounter this quota when you [create](#) or [update](#) an alias.

Note

The [kms:ResourceAliases](#) condition is effective only when the KMS key conforms to this quota. If a KMS key exceeds this quota, principals who are authorized to use the KMS key

by the `kms:ResourceAliases` condition are denied access to the KMS key. For details, see [Access denied due to alias quota](#).

The Aliases per KMS key quota replaces the Aliases per Region quota that limited the total number of aliases in each Region of an Amazon Web Services account. Amazon KMS has eliminated the Aliases per Region quota.

Grants per KMS key: 50,000

Each [customer managed key](#) can have up to 50,000 [grants](#), including the grants created by [Amazon services that are integrated with Amazon KMS](#). This quota does not apply to [Amazon managed keys](#) or [Amazon owned keys](#).

One effect of this quota is that you cannot perform more than 50,000 grant-authorized operations that use the same KMS key at the same time. After you reach the quota, you can create new grants on the KMS key only when an active grant is retired or revoked.

For example, when you attach an Amazon Elastic Block Store (Amazon EBS) volume to an Amazon Elastic Compute Cloud (Amazon EC2) instance, the volume is decrypted so you can read it. To get permission to decrypt the data, Amazon EBS creates a grant for each volume. Therefore, if all of your Amazon EBS volumes use the same KMS key, you cannot attach more than 50,000 volumes at one time.

Custom key stores resource quota: 10

You can create up to 10 [custom key stores](#) in each Amazon Web Services account and Region. If you try to create more, the [CreateCustomKeyStore](#) operation fails.

This quota applies to the total number of custom key stores in each account and region, including all [Amazon CloudHSM key stores](#) and [external key stores](#), regardless of their connection state.

On-demand rotation: 10

You can perform [on-demand key rotation](#) a maximum of 10 times per KMS key. If you try to perform more on-demand rotations, the [RotateKeyOnDemand](#) operation fails.

This quota is not adjustable. You cannot increase it by using Service Quotas or by creating a case in Amazon Web Services Support. To prevent reaching the on-demand rotation quota, we recommend using [automatic key rotation](#) whenever possible.

Request quotas

Amazon KMS establishes quotas for the number of API operations requested in each second. The request quotas differ with the API operation, the Amazon Web Services Region, and other factors, such as the KMS key type. When you exceed an API request quota, Amazon KMS [throttles the request](#).

All Amazon KMS request quotas are adjustable, except for the [Amazon CloudHSM key store request quota](#). To request a quota increase, see [Requesting a quota increase](#) in the *Service Quotas User Guide*. To request a quota decrease, to change a quota that is not listed in Service Quotas, or to change a quota in an Amazon Web Services Region where Service Quotas for Amazon KMS is not available, please visit [Amazon Web Services Support Center](#) and create a case.

If you are exceeding the request quota for the [GenerateDataKey](#) operation, consider using the [data key caching](#) feature of the Amazon Encryption SDK. Reusing data keys might reduce the frequency of your requests to Amazon KMS.

In addition to request quotas, Amazon KMS uses resource quotas to ensure capacity for all users. For details, see [Resource quotas](#).

To view trends in your request rates, use the [Service Quotas console](#). You can also create an [Amazon CloudWatch](#) alarm that alerts you when your request rate reaches a certain percentage of a quota value. For details, see [Manage your Amazon KMS API request rates using Service Quotas and Amazon CloudWatch](#) in the *Amazon Security Blog*.

Topics

- [Request quotas for each Amazon KMS API operation](#)
- [Applying request quotas](#)
- [Shared quotas for cryptographic operations](#)
- [API requests made on your behalf](#)
- [Cross-account requests](#)
- [Custom key store request quotas](#)

Request quotas for each Amazon KMS API operation

This table lists the [Service Quotas](#) quota code and the default value for each Amazon KMS request quota. All Amazon KMS request quotas are adjustable, except for the [Amazon CloudHSM key store request quota](#).

Note

You might need to scroll horizontally or vertically to see all of the data in this table.

Quota name	Default value (requests per second)
Cryptographic operations (symmetric) request rate Applies to: <ul style="list-style-type: none"> • Decrypt • Encrypt • GenerateDataKey • GenerateDataKeyWithoutPlainText • GenerateMac • GenerateRandom • ReEncrypt • VerifyMac 	These shared quotas vary with the Amazon Web Services Region and the type of KMS key used in the request. Each quota is calculated separately. <ul style="list-style-type: none"> • 10,000 (shared) • 20,000 (shared) in the following Regions: <ul style="list-style-type: none"> • US East (Ohio), us-east-2 • Asia Pacific (Singapore), ap-southeast-1 • Asia Pacific (Sydney), ap-southeast-2 • Asia Pacific (Tokyo), ap-northeast-1 • Europe (Frankfurt), eu-central-1 • Europe (London), eu-west-2 • 100,000 (shared) in the following Regions: <ul style="list-style-type: none"> • US East (N. Virginia), us-east-1 • US West (Oregon), us-west-2 • Europe (Ireland), eu-west-1
Cryptographic operations (RSA) request rate Applies to:	1,000 (shared) for RSA KMS keys

Quota name	Default value (requests per second)
<ul style="list-style-type: none"> • Decrypt • Encrypt • ReEncrypt • Sign • Verify 	
<p>Cryptographic operations (ECC and SM2) request rate</p> <p>Applies to:</p> <ul style="list-style-type: none"> • Decrypt—only supported for SM2 (China Regions only) KMS keys • DeriveSharedSecret • Encrypt—only supported for SM2 (China Regions only) KMS keys • ReEncrypt —only supported for SM2 (China Regions only) KMS keys • Sign • Verify 	<p>1,000 (shared) for elliptic curve (ECC) and SM2 (China Regions only) KMS keys</p>
<p>Custom key store request quotas</p> <p>Applies to:</p> <ul style="list-style-type: none"> • Decrypt • DeriveSharedSecret • Encrypt • GenerateDataKey • GenerateDataKeyWithoutPlain text • GenerateRandom • ReEncrypt 	<p>Custom key store request quotas are calculated separately for each custom key store</p> <ul style="list-style-type: none"> • 1,800 (shared) for each Amazon CloudHSM key store • 1,800 (shared) for each external key store

Quota name	Default value (requests per second)
CancelKeyDeletion request rate	5
ConnectCustomKeyStore request rate	5
CreateAlias request rate	5
CreateCustomKeyStore request rate	5
CreateGrant request rate	50
CreateKey request rate	5
DeleteAlias request rate	15
DeleteCustomKeyStore request rate	5
DeleteImportedKeyMaterial request rate	15
DescribeCustomKeyStores request rate	5
DescribeKey request rate	2000
DisableKey request rate	5
DisableKeyRotation request rate	5
DisconnectCustomKeyStore request rate	5
EnableKey request rate	5
EnableKeyRotation request rate	15

Quota name	Default value (requests per second)
GenerateDataKeyPair (ECC_NIST_P256) request rate Applies to: <ul style="list-style-type: none">GenerateDataKeyPairGenerateDataKeyPairWithoutPlaintext	100
GenerateDataKeyPair (ECC_NIST_P384) request rate Applies to: <ul style="list-style-type: none">GenerateDataKeyPairGenerateDataKeyPairWithoutPlaintext	100
GenerateDataKeyPair (ECC_NIST_P521) request rate Applies to: <ul style="list-style-type: none">GenerateDataKeyPairGenerateDataKeyPairWithoutPlaintext	100
GenerateDataKeyPair (ECC_SECG_P256K1) request rate Applies to: <ul style="list-style-type: none">GenerateDataKeyPairGenerateDataKeyPairWithoutPlaintext	100

Quota name	Default value (requests per second)
GenerateDataKeyPair (RSA_2048) request rate Applies to: <ul style="list-style-type: none"> • GenerateDataKeyPair • GenerateDataKeyPairWithoutPlaintext 	1
GenerateDataKeyPair (RSA_3072) request rate Applies to: <ul style="list-style-type: none"> • GenerateDataKeyPair • GenerateDataKeyPairWithoutPlaintext 	0.5 (1 in each 2-second interval)
GenerateDataKeyPair (RSA_4096) request rate Applies to: <ul style="list-style-type: none"> • GenerateDataKeyPair • GenerateDataKeyPairWithoutPlaintext 	0.1 (1 in each 10-second interval)
GenerateDataKeyPair (SM2 – China Regions only) request rate Applies to: <ul style="list-style-type: none"> • GenerateDataKeyPair • GenerateDataKeyPairWithoutPlaintext 	25
GetKeyPolicy request rate	1000

Quota name	Default value (requests per second)
GetKeyRotationStatus request rate	1000
GetParametersForImport request rate	0.25 (1 in each 4-second interval)
GetPublicKey request rate	2000
ImportKeyMaterial request rate	15
ListAliases request rate	500
ListGrants request rate	100
ListKeyPolicies request rate	100
ListKeys request rate	500
ListKeyRotations request rate	100
ListResourceTags request rate	2000
ListRetirableGrants request rate	100
PutKeyPolicy request rate	15
ReplicateKey request rate	5
A <code>ReplicateKey</code> operation counts as one <code>ReplicateKey</code> request in the primary key's Region and two <code>CreateKey</code> requests in the replica's Region. One of the <code>CreateKey</code> requests is a dry run to detect potential problems before creating the key.	
RetireGrant request rate	50
RevokeGrant request rate	50
RotateKeyOnDemand request rate	5

Quota name	Default value (requests per second)
ScheduleKeyDeletion request rate	15
TagResource request rate	10
UntagResource request rate	5
UpdateAlias request rate	5
UpdateCustomKeyStore request rate	5
UpdateKeyDescription request rate	5
UpdatePrimaryRegion request rate An UpdatePrimaryRegion operation counts as two UpdatePrimaryRegion requests; one request in each of the two affected Regions.	5

Applying request quotas

When reviewing request quotas, keep in mind the following information.

- Request quotas apply to both [customer managed keys](#) and [Amazon managed keys](#). The use of [Amazon owned keys](#) does not count against request quotas for your Amazon Web Services account, even when they are used to protect resources in your account.
- Request quotas apply to requests sent to FIPS endpoints and non-FIPS endpoints. For a list of Amazon KMS service endpoints, see [Amazon Key Management Service endpoints and quotas](#) in the Amazon Web Services General Reference.
- Throttling is based on all requests on KMS keys of all types in the Region. This total includes requests from all principals in the Amazon Web Services account, including requests from Amazon services on your behalf.
- Each request quota is calculated independently. For example, requests for the [CreateKey](#) operation have no effect on the request quota for the [CreateAlias](#) operation. If your CreateAlias requests are throttled, your CreateKey requests can still complete successfully.

- Although cryptographic operations share a quota, the shared quota is calculated independently of quotas for other operations. For example, calls to the [Encrypt](#) and [Decrypt](#) operations share a request quota, but that quota is independent of the quota for management operations, such as [EnableKey](#). For example, in the Europe (London) Region, you can perform 10,000 cryptographic operations on symmetric KMS keys *plus* 5 [EnableKey](#) operations per second without being throttled.

Shared quotas for cryptographic operations

Amazon KMS [cryptographic operations](#) share request quotas. You can request any combination of the cryptographic operations that are supported by the KMS key, just so the total number of cryptographic operations doesn't exceed the request quota for that type of KMS key. The exceptions are [GenerateDataKeyPair](#) and [GenerateDataKeyPairWithoutPlaintext](#), which share a separate quota.

The quotas for different types of KMS keys are calculated independently. Each quota applies to all requests for these operations in the Amazon Web Services account and Region with the given key type in each one-second interval.

- *Cryptographic operations (symmetric) request rate* is the shared request quota for cryptographic operations using symmetric KMS keys in an account and region. This quota applies to cryptographic operations with symmetric encryption keys and HMAC keys, which are also symmetric.

For example, you might be using [symmetric KMS keys](#) in an Amazon Web Services Region with a shared quota of 10,000 requests per second. When you make 7,000 [GenerateDataKey](#) requests per second and 2,000 [Decrypt](#) requests per second, Amazon KMS doesn't throttle your requests. However, when you make 9,500 [GenerateDataKey](#) requests and 1,000 [Encrypt](#) requests per second, Amazon KMS throttles your requests because they exceed the shared quota.

Cryptographic operations on the [symmetric encryption KMS keys](#) in a [custom key store](#) count toward both the *Cryptographic operations (symmetric) request rate* for the account and the [custom key store request quota](#) for the custom key store.

- *Cryptographic operations (RSA) request rate* is the shared request quota for cryptographic operations using [RSA asymmetric KMS keys](#).

For example, with a request quota of 1,000 operations per second, you can make 400 [Encrypt](#) requests and 200 [Decrypt](#) requests with RSA KMS keys that can encrypt and decrypt, plus 250 [Sign](#) requests and 150 [Verify](#) requests with RSA KMS keys that can sign and verify.

- *Cryptographic operations (ECC) request rate* is the shared request quota for cryptographic operations using [elliptic curve \(ECC\) asymmetric KMS keys](#) and [SM asymmetric KMS keys](#).

For example, with a request quota of 1,000 operations per second, you can make 400 Sign requests and 200 Verify requests with ECC KMS keys that can sign and verify, plus 250 [Sign](#) requests and 150 [Verify](#) requests with SM2 KMS keys that can sign and verify.

- *Custom key store request quota* is the shared request quota for cryptographic operations on KMS keys in a custom key store. This quota is calculated separately for each custom key store.

Cryptographic operations on the [symmetric encryption KMS keys](#) in a [custom key store](#) count toward both the *Cryptographic operations (symmetric) request rate* for the account and the [custom key store request quota](#) for the custom key store.

The quotas for different key types are also calculated independently. For example, in the Asia Pacific (Singapore) Region, if you use both symmetric and asymmetric KMS keys, you can make up to 10,000 calls per second with symmetric KMS keys (including HMAC keys) *plus* up to 500 additional calls per second with your RSA asymmetric KMS keys, *plus* up to 300 additional requests per second with your ECC-based KMS keys.

API requests made on your behalf

You can make API requests directly or by using an integrated Amazon service that makes API requests to Amazon KMS on your behalf. The quota applies to both kinds of requests.

For example, you might store data in Amazon S3 using server-side encryption with a KMS key (SSE-KMS). Each time you upload or download an S3 object that's encrypted with SSE-KMS, Amazon S3 makes a `GenerateDataKey` (for uploads) or `Decrypt` (for downloads) request to Amazon KMS on your behalf. These requests count toward your quota, so Amazon KMS throttles the requests if you exceed a combined total of 5,500 (or 10,000 or 50,000 depending upon your Amazon Web Services Region) uploads or downloads per second of S3 objects encrypted with SSE-KMS.

Cross-account requests

When an application in one Amazon Web Services account uses a KMS key owned by a different account, it's known as a *cross-account request*. For cross-account requests, Amazon KMS throttles the account that makes the requests, not the account that owns the KMS key. For example, if an application in account A uses a KMS key in account B, the KMS key use applies only to the quotas in account A.

Custom key store request quotas

Amazon KMS maintains request quotas for [cryptographic operations](#) on the KMS keys in a [custom key store](#). These request quotas are calculated separately for each custom key store.

Custom key store request quota	Default value (requests per second) for each custom key store	Adjustable
Amazon CloudHSM key store request quota	1800	No
External key store request quota	1800	Yes

Note

Amazon KMS [custom key store request quotas](#) do not appear in the Service Quotas console. You cannot view or manage these quotas by using Service Quotas API operations. To request a change to your external key store request quota, visit the [Amazon Web Services Support Center](#) and create a case.

If the Amazon CloudHSM cluster associated with an Amazon CloudHSM key store is processing numerous commands, including those unrelated to the custom key store, you might get an Amazon KMS `ThrottlingException` at a lower-than-expected rate. If this occurs, lower your request rate to Amazon KMS, reduce the unrelated load, or use a dedicated Amazon CloudHSM cluster for your Amazon CloudHSM key store.

Amazon KMS reports throttling of external key store requests in the [ExternalKeyStoreThrottle](#) CloudWatch metric. You can use this metric to view throttling patterns, create alarms, and adjust your external key store request quota.

A request for a [cryptographic operation](#) on a KMS key in a custom key store counts toward two quotas:

- Cryptographic operations (symmetric) request rate quota (per account)

Requests for cryptographic operations on KMS keys in a custom key store count toward the `Cryptographic operations (symmetric) request rate quota` for each Amazon Web Services account and Region. For example, in US East (N. Virginia) (us-east-1), each Amazon Web Services account can have up to 100,000 requests per second on symmetric encryption KMS keys, including requests that use a KMS key in a custom key store.

- Custom key store request quota (per custom key store)

Requests for cryptographic operations on KMS keys in a custom key store also count toward a `Custom key store request quota` of 1,800 operations per second. These quotas are calculated separately for each custom key store. They might include requests from multiple Amazon Web Services accounts that use KMS keys in the custom key store.

For example, an [Encrypt](#) operation on a KMS key in a custom key store (either type) in the US East (N. Virginia) (us-east-1) Region counts toward the `Cryptographic operations (symmetric) request rate account-level quota` (100,000 requests per second) for its account and Region, and toward a `Custom key store request quota` (1,800 requests per second) for its custom key store. However, a request for a management operation, such as [PutKeyPolicy](#), on a KMS key in a custom key store applies only to its account-level quota (15 requests per second).

Throttling Amazon KMS requests

To ensure that Amazon KMS can provide fast and reliable responses to API requests from all customers, it throttles API requests that exceed certain boundaries.

Throttling occurs when Amazon KMS rejects a request that might otherwise be valid, and returns a `ThrottlingException` error like the following one.

```
You have exceeded the rate at which you may call KMS. Reduce the frequency of your
calls.
(Service: AWSKMS; Status Code: 400; Error Code: ThrottlingException; Request ID: <ID>
```

Amazon KMS throttles requests for the following conditions.

- The rate of requests per second exceeds the Amazon KMS [request quota](#) for an account and Region.

For example, if users in your account submit 1000 DescribeKey requests in a second, Amazon KMS throttles all subsequent DescribeKey requests in that second.

To respond to throttling, use a [backoff and retry strategy](#). This strategy is implemented automatically for HTTP 400 errors in some Amazon SDKs.

- A burst or sustained high rate of requests to change the state of the same KMS key. This condition is often known as a "hot key."

For example, if an application in your account sends a persistent volley of EnableKey and DisableKey requests for the same KMS key, Amazon KMS throttles the requests. This throttling occurs even if the requests don't exceed the request-per-second request limit for the EnableKey and DisableKey operations.


To respond to throttling, adjust your application logic so it makes only required requests or it consolidates the requests of multiple functions.

- Requests for operations on KMS keys in a [Amazon CloudHSM key store](#) might be throttled at a lower-than-expected rate when the Amazon CloudHSM cluster associated with the Amazon CloudHSM key store is processing numerous commands, including those unrelated to the Amazon CloudHSM key store.

(Amazon KMS no longer throttles requests for operations on KMS keys in a Amazon CloudHSM key store when there are no available PKCS #11 sessions for the Amazon CloudHSM cluster. Instead, it throws a `KMSInternalException` and recommends that you retry your request.)

To view trends in your request rates, use the [Service Quotas console](#). You can also create an [Amazon CloudWatch](#) alarm that alerts you when your request rate reaches a certain percentage of a quota value. For details, see [Manage your Amazon KMS API request rates using Service Quotas and Amazon CloudWatch](#) in the *Amazon Security Blog*.

All Amazon KMS quotas are adjustable, except for the [on-demand rotation resource quota](#) and the [Amazon CloudHSM key store request quota](#). To request a quota increase, see [Requesting a quota increase](#) in the *Service Quotas User Guide*. To request a quota decrease, to change a quota that is not listed in Service Quotas, or to change a quota in an Amazon Web Services Region where Service Quotas for Amazon KMS is not available, please visit [Amazon Web Services Support Center](#) and create a case.

 **Note**

Amazon KMS [custom key store request quotas](#) do not appear in the Service Quotas console. You cannot view or manage these quotas by using Service Quotas API operations. To request a change to your external key store request quota, visit the [Amazon Web Services Support Center](#) and create a case.

Code examples for Amazon KMS using Amazon SDKs

The following code examples show how to use Amazon KMS with an Amazon software development kit (SDK).

Basics are code examples that show you how to perform the essential operations within a service.

Actions are code excerpts from larger programs and must be run in context. While actions show you how to call individual service functions, you can see actions in context in their related scenarios.

For a complete list of Amazon SDK developer guides and code examples, see [Using this service with an Amazon SDK](#). This topic also includes information about getting started and details about previous SDK versions.

Get started

Hello Amazon Key Management Service

The following code examples show how to get started using Amazon Key Management Service.

Java

SDK for Java 2.x

Note

There's more on GitHub. Find the complete example and learn how to set up and run in the [Amazon Code Examples Repository](#).

```
import software.amazon.awssdk.services.kms.KmsAsyncClient;
import software.amazon.awssdk.services.kms.model.ListKeysRequest;
import software.amazon.awssdk.services.kms.paginators.ListKeysPublisher;
import java.util.concurrent.CompletableFuture;

/**
 * Before running this Java V2 code example, set up your development
 * environment, including your credentials.
 *
 * For more information, see the following documentation topic:
 *
 */
```

```
* https://docs.aws.amazon.com/sdk-for-java/latest/developer-guide/get-started.html
*/
public class HelloKMS {
    public static void main(String[] args) {
        listAllKeys();
    }

    public static void listAllKeys() {
        KmsAsyncClient kmsAsyncClient = KmsAsyncClient.builder()
            .build();
        ListKeysRequest listKeysRequest = ListKeysRequest.builder()
            .limit(15)
            .build();

        /*
         * The `subscribe` method is required when using paginator methods in the
        AWS SDK
         * because paginator methods return an instance of a `ListKeysPublisher`,
        which is
         * based on a reactive stream. This allows asynchronous retrieval of
        paginated
         * results as they become available. By subscribing to the stream, we can
        process
         * each page of results as they are emitted.
        */
        ListKeysPublisher keysPublisher =
        kmsAsyncClient.listKeysPaginator(listKeysRequest);
        CompletableFuture<Void> future = keysPublisher
            .subscribe(r -> r.keys().forEach(key ->
                System.out.println("The key ARN is: " + key.keyArn() + ". The key
        Id is: " + key.keyId()))
            .whenComplete((result, exception) -> {
                if (exception != null) {
                    System.err.println("Error occurred: " +
        exception.getMessage());
                } else {
                    System.out.println("Successfully listed all keys.");
                }
            });

        try {
            future.join();
        } catch (Exception e) {
```



```
        System.err.println("Failed to list keys: " + e.getMessage());
    }
}
}
```

- For API details, see [ListKeys](#) in *Amazon SDK for Java 2.x API Reference*.

PHP

SDK for PHP

Note

There's more on GitHub. Find the complete example and learn how to set up and run in the [Amazon Code Examples Repository](#).

```
include "vendor/autoload.php";

use Aws\Kms\KmsClient;

echo "This file shows how to connect to the KmsClient, uses a paginator to get
the keys for the account, and lists the KeyIds for up to 10 keys.\n";

$client = new KmsClient([]);

$pageLength = 10; // Change this value to change the number of records shown, or
to break up the result into pages.

$keys = [];
$keysPaginator = $client->getPaginator("ListKeys", ['Limit' => $pageLength]);
foreach($keysPaginator as $page){
    foreach($page['Keys'] as $index => $key){
        echo "The $index index Key's ID is: {$key['KeyId']}\n";
    }
    echo "End of page one of results. Alter the \$pageLength variable to see more
results.\n";
    break;
}
```

- For API details, see [ListKeys](#) in *Amazon SDK for PHP API Reference*.

Code examples

- [Basic examples for Amazon KMS using Amazon SDKs](#)
 - [Hello Amazon Key Management Service](#)
 - [Learn the basics of Amazon KMS with an Amazon SDK](#)
 - [Actions for Amazon KMS using Amazon SDKs](#)
 - [Use CreateAlias with an Amazon SDK or CLI](#)
 - [Use CreateGrant with an Amazon SDK or CLI](#)
 - [Use CreateKey with an Amazon SDK or CLI](#)
 - [Use Decrypt with an Amazon SDK or CLI](#)
 - [Use DeleteAlias with an Amazon SDK or CLI](#)
 - [Use DescribeKey with an Amazon SDK or CLI](#)
 - [Use DisableKey with an Amazon SDK or CLI](#)
 - [Use EnableKey with an Amazon SDK or CLI](#)
 - [Use EnableKeyRotation with an Amazon SDK or CLI](#)
 - [Use Encrypt with an Amazon SDK or CLI](#)
 - [Use GenerateDataKey with an Amazon SDK or CLI](#)
 - [Use GenerateDataKeyWithoutPlaintext with an Amazon SDK or CLI](#)
 - [Use GenerateRandom with an Amazon SDK or CLI](#)
 - [Use GetKeyPolicy with an Amazon SDK or CLI](#)
 - [Use ListAliases with an Amazon SDK or CLI](#)
 - [Use ListGrants with an Amazon SDK or CLI](#)
 - [Use ListKeyPolicies with an Amazon SDK or CLI](#)
 - [Use ListKeys with an Amazon SDK or CLI](#)
 - [Use PutKeyPolicy with an Amazon SDK or CLI](#)
 - [Use ReEncrypt with an Amazon SDK or CLI](#)
 - [Use RetireGrant with an Amazon SDK or CLI](#)
 - [Use RevokeGrant with an Amazon SDK or CLI](#)

- [Use ScheduleKeyDeletion with an Amazon SDK or CLI](#)
- [Use Sign with an Amazon SDK or CLI](#)
- [Use TagResource with an Amazon SDK or CLI](#)
- [Use UpdateAlias with an Amazon SDK or CLI](#)
- [Use Verify with an Amazon SDK or CLI](#)

Basic examples for Amazon KMS using Amazon SDKs

The following code examples show how to use the basics of Amazon Key Management Service with Amazon SDKs.

Examples

- [Hello Amazon Key Management Service](#)
- [Learn the basics of Amazon KMS with an Amazon SDK](#)
- [Actions for Amazon KMS using Amazon SDKs](#)
 - [Use CreateAlias with an Amazon SDK or CLI](#)
 - [Use CreateGrant with an Amazon SDK or CLI](#)
 - [Use CreateKey with an Amazon SDK or CLI](#)
 - [Use Decrypt with an Amazon SDK or CLI](#)
 - [Use DeleteAlias with an Amazon SDK or CLI](#)
 - [Use DescribeKey with an Amazon SDK or CLI](#)
 - [Use DisableKey with an Amazon SDK or CLI](#)
 - [Use EnableKey with an Amazon SDK or CLI](#)
 - [Use EnableKeyRotation with an Amazon SDK or CLI](#)
 - [Use Encrypt with an Amazon SDK or CLI](#)
 - [Use GenerateDataKey with an Amazon SDK or CLI](#)
 - [Use GenerateDataKeyWithoutPlaintext with an Amazon SDK or CLI](#)
 - [Use GenerateRandom with an Amazon SDK or CLI](#)
 - [Use GetKeyPolicy with an Amazon SDK or CLI](#)
 - [Use ListAliases with an Amazon SDK or CLI](#)
 - [Use ListGrants with an Amazon SDK or CLI](#)

- [Use ListKeyPolicies with an Amazon SDK or CLI](#)
- [Use ListKeys with an Amazon SDK or CLI](#)
- [Use PutKeyPolicy with an Amazon SDK or CLI](#)
- [Use ReEncrypt with an Amazon SDK or CLI](#)
- [Use RetireGrant with an Amazon SDK or CLI](#)
- [Use RevokeGrant with an Amazon SDK or CLI](#)
- [Use ScheduleKeyDeletion with an Amazon SDK or CLI](#)
- [Use Sign with an Amazon SDK or CLI](#)
- [Use TagResource with an Amazon SDK or CLI](#)
- [Use UpdateAlias with an Amazon SDK or CLI](#)
- [Use Verify with an Amazon SDK or CLI](#)

Hello Amazon Key Management Service

The following code examples show how to get started using Amazon Key Management Service.

Java

SDK for Java 2.x

Note

There's more on GitHub. Find the complete example and learn how to set up and run in the [Amazon Code Examples Repository](#).

```
import software.amazon.awssdk.services.kms.KmsAsyncClient;
import software.amazon.awssdk.services.kms.model.ListKeysRequest;
import software.amazon.awssdk.services.kms.paginators.ListKeysPublisher;
import java.util.concurrent.CompletableFuture;

/**
 * Before running this Java V2 code example, set up your development
 * environment, including your credentials.
 *
 * For more information, see the following documentation topic:
 *
 */
```

```
* https://docs.aws.amazon.com/sdk-for-java/latest/developer-guide/get-started.html
*/
public class HelloKMS {
    public static void main(String[] args) {
        listAllKeys();
    }

    public static void listAllKeys() {
        KmsAsyncClient kmsAsyncClient = KmsAsyncClient.builder()
            .build();
        ListKeysRequest listKeysRequest = ListKeysRequest.builder()
            .limit(15)
            .build();

        /*
         * The `subscribe` method is required when using paginator methods in the
        AWS SDK
         * because paginator methods return an instance of a `ListKeysPublisher`,
        which is
         * based on a reactive stream. This allows asynchronous retrieval of
        paginated
         * results as they become available. By subscribing to the stream, we can
        process
         * each page of results as they are emitted.
        */
        ListKeysPublisher keysPublisher =
        kmsAsyncClient.listKeysPaginator(listKeysRequest);
        CompletableFuture<Void> future = keysPublisher
            .subscribe(r -> r.keys().forEach(key ->
                System.out.println("The key ARN is: " + key.keyArn() + ". The key
        Id is: " + key.keyId()))
            .whenComplete((result, exception) -> {
                if (exception != null) {
                    System.err.println("Error occurred: " +
        exception.getMessage());
                } else {
                    System.out.println("Successfully listed all keys.");
                }
            });

        try {
            future.join();
        } catch (Exception e) {
```

```
        System.err.println("Failed to list keys: " + e.getMessage());
    }
}
}
```

- For API details, see [ListKeys](#) in *Amazon SDK for Java 2.x API Reference*.

PHP

SDK for PHP

Note

There's more on GitHub. Find the complete example and learn how to set up and run in the [Amazon Code Examples Repository](#).

```
include "vendor/autoload.php";

use Aws\Kms\KmsClient;

echo "This file shows how to connect to the KmsClient, uses a paginator to get
the keys for the account, and lists the KeyIds for up to 10 keys.\n";

$client = new KmsClient([]);

$pageLength = 10; // Change this value to change the number of records shown, or
to break up the result into pages.

$keys = [];
$keysPaginator = $client->getPaginator("ListKeys", ['Limit' => $pageLength]);
foreach($keysPaginator as $page){
    foreach($page['Keys'] as $index => $key){
        echo "The $index index Key's ID is: {$key['KeyId']}\n";
    }
    echo "End of page one of results. Alter the \$pageLength variable to see more
results.\n";
    break;
}
```

- For API details, see [ListKeys](#) in *Amazon SDK for PHP API Reference*.

For a complete list of Amazon SDK developer guides and code examples, see [Using this service with an Amazon SDK](#). This topic also includes information about getting started and details about previous SDK versions.

Learn the basics of Amazon KMS with an Amazon SDK

The following code examples show how to:

- Create a KMS key.
- List KMS keys for your account and get details about them.
- Enable and disable KMS keys.
- Generate a symmetric data key that can be used for client-side encryption.
- Generate an asymmetric key used to digitally sign data.
- Tag keys.
- Delete KMS keys.

Java

SDK for Java 2.x

Note

There's more on GitHub. Find the complete example and learn how to set up and run in the [Amazon Code Examples Repository](#).

Run a scenario at a command prompt.

```
import software.amazon.awssdk.core.SdkBytes;
import software.amazon.awssdk.regions.Region;
import org.slf4j.Logger;
import org.slf4j.LoggerFactory;
import software.amazon.awssdk.services.kms.model.AlreadyExistsException;
import software.amazon.awssdk.services.kms.model.DisabledException;
```

```
import software.amazon.awssdk.services.kms.model.EnableKeyRotationResponse;
import software.amazon.awssdk.services.kms.model.KmsException;
import software.amazon.awssdk.services.kms.model.NotFoundException;
import software.amazon.awssdk.services.kms.model.RevokeGrantResponse;
import java.util.List;
import java.util.Scanner;
import java.util.concurrent.CompletableFuture;
import java.util.concurrent.CompletionException;

/**
 * Before running this Java V2 code example, set up your development
 * environment, including your credentials.
 *
 * For more information, see the following documentation topic:
 *
 * https://docs.aws.amazon.com/sdk-for-java/latest/developer-guide/get-started.html
 */

public class KMSScenario {
    public static final String DASHES = new String(new char[80]).replace("\0",
"-");
    private static String accountId = "";

    private static final Logger logger =
LoggerFactory.getLogger(KMSScenario.class);

    static KMSActions kmsActions = new KMSActions();

    static Scanner scanner = new Scanner(System.in);

    static String aliasName = "alias/dev-encryption-key";

    public static void main(String[] args) {
        final String usage = ""
Usage: <granteePrincipal>

        Where:
            granteePrincipal - The principal (user, service account, or group)
to whom the grant or permission is being given.
        """;

        if (args.length != 1) {
            logger.info(usage);
        }
    }
}
```



```
        return;
    }
    String granteePrincipal = args[0];
    String policyName = "default";

    accountId = kmsActions.getAccountId();
    String keyDesc = "Created by the AWS KMS API";

    logger.info(DASHES);
    logger.info("""
        Welcome to the AWS Key Management SDK Basics scenario.

        This program demonstrates how to interact with AWS Key Management
        using the AWS SDK for Java (v2).
        The AWS Key Management Service (KMS) is a secure and highly available
        service that allows you to create
        and manage AWS KMS keys and control their use across a wide range of
        AWS services and applications.
        KMS provides a centralized and unified approach to managing
        encryption keys, making it easier to meet your
        data protection and regulatory compliance requirements.

        This Basics scenario creates two key types:

        - A symmetric encryption key is used to encrypt and decrypt data.
        - An asymmetric key used to digitally sign data.

        Let's get started...
        """);
    waitForInputToContinue(scanner);

    try {
        // Run the methods that belong to this scenario.
        String targetKeyId = runScenario(granteePrincipal, keyDesc, policyName);
        requestDeleteResources(aliasName, targetKeyId);
    } catch (Throwable rt) {
        Throwable cause = rt.getCause();
        if (cause instanceof KmsException kmsEx) {
            logger.info("KMS error occurred: Error message: {}, Error code
        {}", kmsEx.getMessage(), kmsEx.awsErrorDetails().errorCode());
        } else {
            logger.info("An unexpected error occurred: " + rt.getMessage());
        }
    }
}
```

```

    }
}

private static String runScenario(String granteePrincipal, String keyDesc,
String policyName) throws Throwable {
    logger.info(DASHES);
    logger.info("1. Create a symmetric KMS key\n");
    logger.info("First, the program will creates a symmetric KMS key that you
can used to encrypt and decrypt data.");
    waitForInputToContinue(scanner);
    String targetKeyId;
    try {
        CompletableFuture<String> futureKeyId =
kmsActions.createKeyAsync(keyDesc);
        targetKeyId = futureKeyId.join();
        logger.info("A symmetric key was successfully created " +
targetKeyId);

    } catch (RuntimeException rt) {
        Throwable cause = rt.getCause();
        if (cause instanceof KmsException kmsEx) {
            logger.info("KMS error occurred: Error message: {}, Error code
{}", kmsEx.getMessage(), kmsEx.awsErrorDetails().errorCode());
        } else {
            logger.info("An unexpected error occurred: " + rt.getMessage());
        }
        throw cause;
    }
    waitForInputToContinue(scanner);

    logger.info(DASHES);
    logger.info("""
        2. Enable a KMS key

        By default, when the SDK creates an AWS key, it is enabled. The next
bit of code checks to
        determine if the key is enabled.
        """);
    waitForInputToContinue(scanner);
    boolean isEnabled;
    try {
        CompletableFuture<Boolean> futureIsKeyEnabled =
kmsActions.isKeyEnabledAsync(targetKeyId);
        isEnabled = futureIsKeyEnabled.join();
    }
}

```

```

        logger.info("Is the key enabled? {}", isEnabled);

    } catch (RuntimeException rt) {
        Throwable cause = rt.getCause();
        if (cause instanceof KmsException kmsEx) {
            logger.info("KMS error occurred: Error message: {}, Error code
{}", kmsEx.getMessage(), kmsEx.awsErrorDetails().errorCode());
        } else {
            logger.info("An unexpected error occurred: " + rt.getMessage());
        }
        throw cause;
    }

    if (!isEnabled)
        try {
            CompletableFuture<Void> future =
kmsActions.enableKeyAsync(targetKeyId);
            future.join();

        } catch (RuntimeException rt) {
            Throwable cause = rt.getCause();
            if (cause instanceof KmsException kmsEx) {
                logger.info("KMS error occurred: Error message: {}, Error
code {}", kmsEx.getMessage(), kmsEx.awsErrorDetails().errorCode());
            } else {
                logger.info("An unexpected error occurred: " +
rt.getMessage());
            }
            throw cause;
        }
    waitForInputToContinue(scanner);

    logger.info(DASHES);
    logger.info("3. Encrypt data using the symmetric KMS key");
    String plaintext = "Hello, AWS KMS!";
    logger.info("""
        One of the main uses of symmetric keys is to encrypt and decrypt
data.

        Next, the code encrypts the string {} with the SYMMETRIC_DEFAULT
encryption algorithm.
        """, plaintext);
    waitForInputToContinue(scanner);
    SdkBytes encryptedData;
    try {

```

```
        CompletableFuture<SdkBytes> future =
kmsActions.encryptDataAsync(targetKeyId, plaintext);
        encryptedData = future.join();

    } catch (RuntimeException rt) {
        Throwable cause = rt.getCause();
        if (cause instanceof DisabledException kmsDisabledEx) {
            logger.info("KMS error occurred due to a disabled
key: Error message: {}, Error code {}", kmsDisabledEx.getMessage(),
kmsDisabledEx.awsErrorDetails().errorCode());
        } else {
            logger.info("An unexpected error occurred: " + rt.getMessage());
        }
        deleteKey(targetKeyId);
        throw cause;
    }
    waitForInputToContinue(scanner);

    logger.info(DASHES);
    logger.info("4. Create an alias");
    logger.info("""

        The alias name should be prefixed with 'alias/'.
        The default, 'alias/dev-encryption-key'.
        """);
    waitForInputToContinue(scanner);

    try {
        CompletableFuture<Void> future =
kmsActions.createCustomAliasAsync(targetKeyId, aliasName);
        future.join();

    } catch (RuntimeException rt) {
        Throwable cause = rt.getCause();
        if (cause instanceof AlreadyExistsException kmsExistsEx) {
            if (kmsExistsEx.getMessage().contains("already exists")) {
                logger.info("The alias '" + aliasName + "' already exists.
Moving on...");
            }
        } else {
            logger.error("An unexpected error occurred: " + rt.getMessage(),
rt);

            deleteKey(targetKeyId);
            throw cause;
        }
    }
}
```

```

    }
}
waitForInputToContinue(scanner);

logger.info(DASHES);
logger.info("5. List all of your aliases");
waitForInputToContinue(scanner);
try {
    CompletableFuture<Object> future = kmsActions.listAllAliasesAsync();
    future.join();

} catch (RuntimeException rt) {
    Throwable cause = rt.getCause();
    if (cause instanceof KmsException kmsEx) {
        logger.info("KMS error occurred: Error message: {}, Error code
{}", kmsEx.getMessage(), kmsEx.awsErrorDetails().errorCode());
    } else {
        logger.info("An unexpected error occurred: " + rt.getMessage());
    }
    deleteAliasName(aliasName);
    deleteKey(targetKeyId);
    throw cause;
}
waitForInputToContinue(scanner);

logger.info(DASHES);
logger.info("6. Enable automatic rotation of the KMS key");
logger.info("""

    By default, when the SDK enables automatic rotation of a KMS key,
    KMS rotates the key material of the KMS key one year (approximately
365 days) from the enable date and every year
    thereafter.
    """);
waitForInputToContinue(scanner);
try {
    CompletableFuture<EnableKeyRotationResponse> future =
kmsActions.enableKeyRotationAsync(targetKeyId);
    future.join();

} catch (RuntimeException rt) {
    Throwable cause = rt.getCause();
    if (cause instanceof KmsException kmsEx) {

```

```

        logger.info("KMS error occurred: Error message: {}, Error code
{}", kmsEx.getMessage(), kmsEx.awsErrorDetails().errorCode());
    } else {
        logger.info("An unexpected error occurred: " + rt.getMessage());
    }
    deleteAliasName(aliasName);
    deleteKey(targetKeyId);
    throw cause;
}
waitForInputToContinue(scanner);

logger.info(DASHES);
logger.info("""
    7. Create a grant

    A grant is a policy instrument that allows Amazon Web Services
principals to use KMS keys.
    It also can allow them to view a KMS key (DescribeKey) and create and
manage grants.
    When authorizing access to a KMS key, grants are considered along
with key policies and IAM policies.
    """);

waitForInputToContinue(scanner);
String grantId = null;
try {
    CompletableFuture<String> futureGrantId =
kmsActions.grantKeyAsync(targetKeyId, granteePrincipal);
    grantId = futureGrantId.join();

} catch (RuntimeException rt) {
    Throwable cause = rt.getCause();
    if (cause instanceof KmsException kmsEx) {
        logger.info("KMS error occurred: Error message: {}, Error code
{}", kmsEx.getMessage(), kmsEx.awsErrorDetails().errorCode());
    } else {
        logger.info("An unexpected error occurred: " + rt.getMessage());
    }
    deleteKey(targetKeyId);
    throw cause;
}
waitForInputToContinue(scanner);
logger.info(DASHES);

```

```

    logger.info(DASHES);
    logger.info("8. List grants for the KMS key");
    waitForInputToContinue(scanner);
    try {
        CompletableFuture<Object> future =
kmsActions.displayGrantIdsAsync(targetKeyId);
        future.join();

    } catch (RuntimeException rt) {
        Throwable cause = rt.getCause();
        if (cause instanceof KmsException kmsEx) {
            logger.info("KMS error occurred: Error message: {}, Error code
{}", kmsEx.getMessage(), kmsEx.awsErrorDetails().errorCode());
        } else {
            logger.info("An unexpected error occurred: " + rt.getMessage());
        }
        deleteAliasName(aliasName);
        deleteKey(targetKeyId);
        throw cause;
    }
    waitForInputToContinue(scanner);

    logger.info(DASHES);
    logger.info("9. Revoke the grant");
    logger.info("""
        The revocation of a grant immediately removes the permissions and
access that the grant had provided.
        This means that any principal (user, role, or service) that was
granted access to perform specific
        KMS operations on a KMS key will no longer be able to perform those
operations.
        """);
    waitForInputToContinue(scanner);
    try {
        CompletableFuture<RevokeGrantResponse> future =
kmsActions.revokeKeyGrantAsync(targetKeyId, grantId);
        future.join();

    } catch (RuntimeException rt) {
        Throwable cause = rt.getCause();
        if (cause instanceof KmsException kmsEx) {
            if (kmsEx.getMessage().contains("Grant does not exist")) {
                logger.info("The grant ID '" + grantId + "' does not exist.
Moving on...");
            }
        }
    }

```

```
        } else {
            logger.info("KMS error occurred: Error message: {}, Error
code {}", kmsEx.getMessage(), kmsEx.awsErrorDetails().errorCode());
            throw cause;
        }
    } else {
        logger.info("An unexpected error occurred: " + rt.getMessage());
        deleteAliasName(aliasName);
        deleteKey(targetKeyId);
        throw cause;
    }
}
waitForInputToContinue(scanner);

logger.info(DASHES);
logger.info("10. Decrypt the data\n");
logger.info("""
    Lets decrypt the data that was encrypted in an early step.
    The code uses the same key to decrypt the string that we encrypted
earlier in the program.
    """);
waitForInputToContinue(scanner);
String decryptedData = "";
try {
    CompletableFuture<String> future =
kmsActions.decryptDataAsync(encryptedData, targetKeyId);
    decryptedData = future.join();
    logger.info("Decrypted data: " + decryptedData);

} catch (RuntimeException rt) {
    Throwable cause = rt.getCause();
    if (cause instanceof KmsException kmsEx) {
        logger.info("KMS error occurred: Error message: {}, Error code
{}", kmsEx.getMessage(), kmsEx.awsErrorDetails().errorCode());
    } else {
        logger.info("An unexpected error occurred: " + rt.getMessage());
    }
    deleteAliasName(aliasName);
    deleteKey(targetKeyId);
    throw cause;
}
logger.info("Decrypted text is: " + decryptedData);
waitForInputToContinue(scanner);
```



```
logger.info(DASHES);
logger.info("11. Replace a key policy\n");
logger.info("""
```

A key policy is a resource policy for a KMS key. Key policies are the primary way to control

access to KMS keys. Every KMS key must have exactly one key policy. The statements in the key policy determine who has permission to use the KMS key and how they can use it.

You can also use IAM policies and grants to control access to the KMS key, but every KMS key must have a key policy.

By default, when you create a key by using the SDK, a policy is created that

gives the AWS account that owns the KMS key full access to the KMS key.

Let's try to replace the automatically created policy with the following policy.

```
        "Version": "2012-10-17",
        "Statement": [{
            "Effect": "Allow",
            "Principal": {"AWS": "arn:aws:iam::000000000000:root"},
            "Action": "kms:*",
            "Resource": "*"
        }]
    """);
```

```
waitForInputToContinue(scanner);
try {
    CompletableFuture<Boolean> future =
kmsActions.replacePolicyAsync(targetKeyId, policyName, accountId);
    boolean success = future.join();
    if (success) {
        logger.info("Key policy replacement succeeded.");
    } else {
        logger.error("Key policy replacement failed.");
    }
} catch (RuntimeException rt) {
    Throwable cause = rt.getCause();
    if (cause instanceof KmsException kmsEx) {
```

```
        logger.info("KMS error occurred: Error message: {}, Error code
{}", kmsEx.getMessage(), kmsEx.awsErrorDetails().errorCode());
    } else {
        logger.info("An unexpected error occurred: " + rt.getMessage());
    }
    deleteAliasName(aliasName);
    deleteKey(targetKeyId);
    throw cause;
}
waitForInputToContinue(scanner);

logger.info(DASHES);
logger.info("12. Get the key policy\n");
logger.info("The next bit of code that runs gets the key policy to make
sure it exists.");
waitForInputToContinue(scanner);
try {
    CompletableFuture<String> future =
kmsActions.getKeyPolicyAsync(targetKeyId, policyName);
    String policy = future.join();
    if (!policy.isEmpty()) {
        logger.info("Retrieved policy: " + policy);
    }

} catch (RuntimeException rt) {
    Throwable cause = rt.getCause();
    if (cause instanceof KmsException kmsEx) {
        logger.info("KMS error occurred: Error message: {}, Error code
{}", kmsEx.getMessage(), kmsEx.awsErrorDetails().errorCode());
    } else {
        logger.info("An unexpected error occurred: " + rt.getMessage());
    }
    deleteAliasName(aliasName);
    deleteKey(targetKeyId);
    throw cause;
}
waitForInputToContinue(scanner);

logger.info(DASHES);
logger.info("13. Create an asymmetric KMS key and sign your data\n");
logger.info("""
    Signing your data with an AWS key can provide several benefits that
make it an attractive option
```

```

        for your data signing needs. By using an AWS KMS key, you can
    leverage the
        security controls and compliance features provided by AWS,
        which can help you meet various regulatory requirements and enhance
    the overall security posture
        of your organization.
    """);
    waitForInputToContinue(scanner);
    try {
        CompletableFuture<Boolean> future = kmsActions.signVerifyDataAsync();
        boolean success = future.join();
        if (success) {
            logger.info("Sign and verify data operation succeeded.");
        } else {
            logger.error("Sign and verify data operation failed.");
        }
    } catch (RuntimeException rt) {
        Throwable cause = rt.getCause();
        if (cause instanceof KmsException kmsEx) {
            logger.info("KMS error occurred: Error message: {}, Error code
{}", kmsEx.getMessage(), kmsEx.awsErrorDetails().errorCode());
        } else {
            logger.info("An unexpected error occurred: " + rt.getMessage());
        }
        deleteAliasName(aliasName);
        deleteKey(targetKeyId);
        throw cause;
    }
    waitForInputToContinue(scanner);

    logger.info(DASHES);
    logger.info("14. Tag your symmetric KMS Key\n");
    logger.info("""
        By using tags, you can improve the overall management, security, and
    governance of your
        KMS keys, making it easier to organize, track, and control access to
    your encrypted data within
        your AWS environment
    """);
    waitForInputToContinue(scanner);
    try {
        CompletableFuture<Void> future =
    kmsActions.tagKMSKeyAsync(targetKeyId);

```

```
        future.join();

    } catch (RuntimeException rt) {
        Throwable cause = rt.getCause();
        if (cause instanceof KmsException kmsEx) {
            logger.info("KMS error occurred: Error message: {}, Error code
{}", kmsEx.getMessage(), kmsEx.awsErrorDetails().errorCode());
        } else {
            logger.info("An unexpected error occurred: " + rt.getMessage());
        }
        deleteAliasName(aliasName);
        deleteKey(targetKeyId);
        throw cause;
    }
    waitForInputToContinue(scanner);
    return targetKeyId;
}

// Deletes KMS resources with user input.
private static void requestDeleteResources(String aliasName, String
targetKeyId) {
    logger.info(DASHES);
    logger.info("15. Schedule the deletion of the KMS key\n");
    logger.info("
By default, KMS applies a waiting period of 30 days,
but you can specify a waiting period of 7-30 days. When this
operation is successful,
the key state of the KMS key changes to PendingDeletion and the key
can't be used in any
cryptographic operations. It remains in this state for the duration
of the waiting period.

Deleting a KMS key is a destructive and potentially dangerous
operation. When a KMS key is deleted,
all data that was encrypted under the KMS key is unrecoverable.
");
    logger.info("Would you like to delete the Key Management resources? (y/
n)");
    String delAns = scanner.nextLine().trim();
    if (delAns.equalsIgnoreCase("y")) {
        logger.info("You selected to delete the AWS KMS resources.");
        waitForInputToContinue(scanner);
        try {
```

```
        CompletableFuture<Void> future =
kmsActions.deleteSpecificAliasAsync(aliasName);
        future.join();

    } catch (RuntimeException rt) {
        Throwable cause = rt.getCause();
        if (cause instanceof KmsException kmsEx) {
            logger.info("KMS error occurred: Error message: {}, Error
code {}", kmsEx.getMessage(), kmsEx.awsErrorDetails().errorCode());
        } else {
            logger.info("An unexpected error occurred: " +
rt.getMessage());
        }
    }
    }
    waitForInputToContinue(scanner);
    try {
        CompletableFuture<Void> future =
kmsActions.disableKeyAsync(targetKeyId);
        future.join();

    } catch (RuntimeException rt) {
        Throwable cause = rt.getCause();
        if (cause instanceof KmsException kmsEx) {
            logger.info("KMS error occurred: Error message: {}, Error
code {}", kmsEx.getMessage(), kmsEx.awsErrorDetails().errorCode());
        } else {
            logger.info("An unexpected error occurred: " +
rt.getMessage());
        }
    }
    }
    try {
        CompletableFuture<Void> future =
kmsActions.deleteKeyAsync(targetKeyId);
        future.join();

    } catch (RuntimeException rt) {
        Throwable cause = rt.getCause();
        if (cause instanceof KmsException kmsEx) {
            logger.info("KMS error occurred: Error message: {}, Error
code {}", kmsEx.getMessage(), kmsEx.awsErrorDetails().errorCode());
        } else {
            logger.info("An unexpected error occurred: " +
rt.getMessage());
        }
    }
    }
```

```
        }
    }

    } else {
        logger.info("The Key Management resources will not be deleted");
    }

    logger.info(DASHES);
    logger.info("This concludes the AWS Key Management SDK scenario");
    logger.info(DASHES);
}

// This method is invoked from Exceptions to clean up the resources.
private static void deleteKey(String targetKeyId) {
    try {
        CompletableFuture<Void> future =
kmsActions.disableKeyAsync(targetKeyId);
        future.join();

    } catch (RuntimeException rt) {
        Throwable cause = rt.getCause();
        if (cause instanceof KmsException kmsEx) {
            logger.info("KMS error occurred: Error message: {}, Error code
{}", kmsEx.getMessage(), kmsEx.awsErrorDetails().errorCode());
        } else {
            logger.info("An unexpected error occurred: " + rt.getMessage());
        }
    }

    try {
        CompletableFuture<Void> future =
kmsActions.deleteKeyAsync(targetKeyId);
        future.join();

    } catch (RuntimeException rt) {
        Throwable cause = rt.getCause();
        if (cause instanceof KmsException kmsEx) {
            logger.info("KMS error occurred: Error message: {}, Error code
{}", kmsEx.getMessage(), kmsEx.awsErrorDetails().errorCode());
        } else {
            logger.info("An unexpected error occurred: " + rt.getMessage());
        }
    }
}
```

```
// This method is invoked from Exceptions to clean up the resources.
private static void deleteAliasName(String aliasName) {
    try {
        CompletableFuture<Void> future =
kmsActions.deleteSpecificAliasAsync(aliasName);
        future.join();

    } catch (RuntimeException rt) {
        Throwable cause = rt.getCause();
        if (cause instanceof KmsException kmsEx) {
            logger.info("KMS error occurred: Error message: {}, Error code
{}", kmsEx.getMessage(), kmsEx.awsErrorDetails().errorCode());
        } else {
            logger.info("An unexpected error occurred: " + rt.getMessage());
        }
    }
}

private static void waitForInputToContinue(Scanner scanner) {
    while (true) {
        logger.info("");
        logger.info("Enter 'c' followed by <ENTER> to continue:");
        String input = scanner.nextLine();

        if (input.trim().equalsIgnoreCase("c")) {
            logger.info("Continuing with the program...");
            logger.info("");
            break;
        } else {
            // Handle invalid input.
            logger.info("Invalid input. Please try again.");
        }
    }
}
}
```

Define a class that wraps KMS actions.

```
public class KMSActions {
    private static final Logger logger =
LoggerFactory.getLogger(KMSActions.class);
```

```
private static KmsAsyncClient kmsAsyncClient;

/**
 * Retrieves an asynchronous AWS Key Management Service (KMS) client.
 * <p>
 * This method creates and returns a singleton instance of the KMS async
 client, with the following configurations:
 * <ul>
 * <li>Max concurrency: 100</li>
 * <li>Connection timeout: 60 seconds</li>
 * <li>Read timeout: 60 seconds</li>
 * <li>Write timeout: 60 seconds</li>
 * <li>API call timeout: 2 minutes</li>
 * <li>API call attempt timeout: 90 seconds</li>
 * <li>Retry policy: up to 3 retries</li>
 * <li>Credentials provider: environment variable credentials provider</li>
 * </ul>
 * <p>
 * If the client instance has already been created, it is returned instead of
 creating a new one.
 *
 * @return the KMS async client instance
 */
private static KmsAsyncClient getAsyncClient() {
    if (kmsAsyncClient == null) {
        SdkAsyncHttpClient httpClient = NettyNioAsyncHttpClient.builder()
            .maxConcurrency(100)
            .connectionTimeout(Duration.ofSeconds(60))
            .readTimeout(Duration.ofSeconds(60))
            .writeTimeout(Duration.ofSeconds(60))
            .build();

        ClientOverrideConfiguration overrideConfig =
ClientOverrideConfiguration.builder()
            .apiCallTimeout(Duration.ofMinutes(2))
            .apiCallAttemptTimeout(Duration.ofSeconds(90))
            .retryPolicy(RetryPolicy.builder()
                .numRetries(3)
                .build())
            .build();

        kmsAsyncClient = KmsAsyncClient.builder()
            .httpClient(httpClient)
            .overrideConfiguration(overrideConfig)
```



```
        .build();
    }
    return kmsAsyncClient;
}

/**
 * Creates a new symmetric encryption key asynchronously.
 *
 * @param keyDesc the description of the key to be created
 * @return a {@link CompletableFuture} that completes with the ID of the
newly created key
 * @throws RuntimeException if an error occurs while creating the key
 */
public CompletableFuture<String> createKeyAsync(String keyDesc) {
    CreateKeyRequest keyRequest = CreateKeyRequest.builder()
        .description(keyDesc)
        .keySpec(KeySpec.SYMMETRIC_DEFAULT)
        .keyUsage(KeyUsageType.ENCRYPT_DECRYPT)
        .build();

    return getAsyncClient().createKey(keyRequest)
        .thenApply(resp -> resp.keyMetadata().keyId())
        .exceptionally(ex -> {
            throw new RuntimeException("An error occurred while creating the
key: " + ex.getMessage(), ex);
        });
}

/**
 * Asynchronously checks if a specified key is enabled.
 *
 * @param keyId the ID of the key to check
 * @return a {@link CompletableFuture} that, when completed, indicates
whether the key is enabled or not
 *
 * @throws RuntimeException if an exception occurs while checking the key
state
 */
public CompletableFuture<Boolean> isKeyEnabledAsync(String keyId) {
    DescribeKeyRequest keyRequest = DescribeKeyRequest.builder()
        .keyId(keyId)
        .build();
}
```

```

        CompletableFuture<DescribeKeyResponse> responseFuture =
getAsyncClient().describeKey(keyRequest);
        return responseFuture.whenComplete((resp, ex) -> {
            if (resp != null) {
                KeyState keyState = resp.keyMetadata().keyState();
                if (keyState == KeyState.ENABLED) {
                    logger.info("The key is enabled.");
                } else {
                    logger.info("The key is not enabled. Key state: {}",
keyState);
                }
            } else {
                throw new RuntimeException(ex);
            }
        }).thenApply(resp -> resp.keyMetadata().keyState() == KeyState.ENABLED);
    }

/**
 * Asynchronously enables the specified key.
 *
 * @param keyId the ID of the key to enable
 * @return a {@link CompletableFuture} that completes when the key has been
enabled
 */
public CompletableFuture<Void> enableKeyAsync(String keyId) {
    EnableKeyRequest enableKeyRequest = EnableKeyRequest.builder()
        .keyId(keyId)
        .build();

    CompletableFuture<EnableKeyResponse> responseFuture =
getAsyncClient().enableKey(enableKeyRequest);
    responseFuture.whenComplete((response, exception) -> {
        if (exception == null) {
            logger.info("Key with ID [{}] has been enabled.", keyId);
        } else {
            if (exception instanceof KmsException kmsEx) {
                throw new RuntimeException("KMS error occurred while enabling
key: " + kmsEx.getMessage(), kmsEx);
            } else {
                throw new RuntimeException("An unexpected error occurred
while enabling key: " + exception.getMessage(), exception);
            }
        }
    });
}

```

```
        return responseFuture.thenApply(response -> null);
    }

    /**
     * Encrypts the given text asynchronously using the specified KMS client and
     * key ID.
     *
     * @param keyId the ID of the KMS key to use for encryption
     * @param text the text to encrypt
     * @return a CompletableFuture that completes with the encrypted data as an
     * SdkBytes object
     */
    public CompletableFuture<SdkBytes> encryptDataAsync(String keyId, String
    text) {
        SdkBytes myBytes = SdkBytes.fromUtf8String(text);
        EncryptRequest encryptRequest = EncryptRequest.builder()
            .keyId(keyId)
            .plaintext(myBytes)
            .build();

        CompletableFuture<EncryptResponse> responseFuture =
    getAsyncClient().encrypt(encryptRequest).toCompletableFuture();
        return responseFuture.whenComplete((response, ex) -> {
            if (response != null) {
                String algorithm = response.encryptionAlgorithm().toString();
                logger.info("The string was encrypted with algorithm {}.\"",
    algorithm);
            } else {
                throw new RuntimeException(ex);
            }
        }).thenApply(EncryptResponse::ciphertextBlob);
    }

    /**
     * Creates a custom alias for the specified target key asynchronously.
     *
     * @param targetKeyId the ID of the target key for the alias
     * @param aliasName the name of the alias to create
     * @return a {@link CompletableFuture} that completes when the alias creation
     * operation is finished
     */
    public CompletableFuture<Void> createCustomAliasAsync(String targetKeyId,
    String aliasName) {
```

```
        CreateAliasRequest aliasRequest = CreateAliasRequest.builder()
            .aliasName(aliasName)
            .targetKeyId(targetKeyId)
            .build();

        CompletableFuture<CreateAliasResponse> responseFuture =
getAsyncClient().createAlias(aliasRequest);
        responseFuture.whenComplete((response, exception) -> {
            if (exception == null) {
                logger.info("{} was successfully created.", aliasName);
            } else {
                if (exception instanceof ResourceExistsException) {
                    logger.info("Alias [{}] already exists. Moving on...",
aliasName);
                } else if (exception instanceof KmsException kmsEx) {
                    throw new RuntimeException("KMS error occurred while creating
alias: " + kmsEx.getMessage(), kmsEx);
                } else {
                    throw new RuntimeException("An unexpected error occurred
while creating alias: " + exception.getMessage(), exception);
                }
            }
        });

        return responseFuture.thenApply(response -> null);
    }

    /**
     * Asynchronously lists all the aliases in the current AWS account.
     *
     * @return a {@link CompletableFuture} that completes when the list of
aliases has been processed
     */
    public CompletableFuture<Object> listAllAliasesAsync() {
        ListAliasesRequest aliasesRequest = ListAliasesRequest.builder()
            .limit(15)
            .build();

        ListAliasesPublisher paginator =
getAsyncClient().listAliasesPaginator(aliasesRequest);
        return paginator.subscribe(response -> {
            response.aliases().forEach(alias ->
                logger.info("The alias name is: " + alias.aliasName())
            );
        });
    }
}
```

```

    })
    .thenApply(v -> null)
    .exceptionally(ex -> {
        if (ex.getCause() instanceof KmsException) {
            KmsException e = (KmsException) ex.getCause();
            throw new RuntimeException("A KMS exception occurred: " +
e.getMessage());
        } else {
            throw new RuntimeException("An unexpected error occurred: " +
ex.getMessage());
        }
    });
}

/**
 * Enables key rotation asynchronously for the specified key ID.
 *
 * @param keyId the ID of the key for which to enable key rotation
 * @return a CompletableFuture that represents the asynchronous operation of
enabling key rotation
 * @throws RuntimeException if there was an error enabling key rotation,
either due to a KMS exception or an unexpected error
 */
public CompletableFuture<EnableKeyRotationResponse>
enableKeyRotationAsync(String keyId) {
    EnableKeyRotationRequest enableKeyRotationRequest =
EnableKeyRotationRequest.builder()
        .keyId(keyId)
        .build();

    CompletableFuture<EnableKeyRotationResponse> responseFuture =
getAsyncClient().enableKeyRotation(enableKeyRotationRequest);
    responseFuture.whenComplete((response, exception) -> {
        if (exception == null) {
            logger.info("Key rotation has been enabled for key with id [{}]",
keyId);
        } else {
            if (exception instanceof KmsException kmsEx) {
                throw new RuntimeException("Failed to enable key rotation: "
+ kmsEx.getMessage(), kmsEx);
            } else {
                throw new RuntimeException("An unexpected error occurred: " +
exception.getMessage(), exception);
            }
        }
    });
}

```

```
        }
    });

    return responseFuture;
}

/**
 * Grants permissions to a specified principal on a customer master key (CMK)
 * asynchronously.
 *
 * @param keyId          The unique identifier for the customer master key
 * (CMK) that the grant applies to.
 * @param granteePrincipal The principal that is given permission to perform
 * the operations that the grant permits on the CMK.
 * @return A {@link CompletableFuture} that, when completed, contains the ID
 * of the created grant.
 * @throws RuntimeException If an error occurs during the grant creation
 * process.
 */
public CompletableFuture<String> grantKeyAsync(String keyId, String
granteePrincipal) {
    List<GrantOperation> grantPermissions = List.of(
        GrantOperation.ENCRYPT,
        GrantOperation.DECRYPT,
        GrantOperation.DESCRIBE_KEY
    );

    CreateGrantRequest grantRequest = CreateGrantRequest.builder()
        .keyId(keyId)
        .name("grant1")
        .granteePrincipal(granteePrincipal)
        .operations(grantPermissions)
        .build();

    CompletableFuture<CreateGrantResponse> responseFuture =
getAsyncClient().createGrant(grantRequest);
    responseFuture.whenComplete((response, ex) -> {
        if (ex == null) {
            logger.info("Grant created successfully with ID: " +
response.grantId());
        } else {
            if (ex instanceof KmsException kmsEx) {
                throw new RuntimeException("Failed to create grant: " +
kmsEx.getMessage(), kmsEx);
            }
        }
    });
}
```

```
        } else {
            throw new RuntimeException("An unexpected error occurred: " +
ex.getMessage(), ex);
        }
    }
});

return responseFuture.thenApply(CreateGrantResponse::grantId);
}

/**
 * Asynchronously displays the grant IDs for the specified key ID.
 *
 * @param keyId the ID of the AWS KMS key for which to list the grants
 * @return a {@link CompletableFuture} that, when completed, will be null
if the operation succeeded, or will throw a {@link RuntimeException} if the
operation failed
 * @throws RuntimeException if there was an error listing the grants, either
due to an {@link KmsException} or an unexpected error
 */
public CompletableFuture<Object> displayGrantIdsAsync(String keyId) {
    ListGrantsRequest grantsRequest = ListGrantsRequest.builder()
        .keyId(keyId)
        .limit(15)
        .build();

    ListGrantsPublisher paginator =
getAsyncClient().listGrantsPaginator(grantsRequest);
    return paginator.subscribe(response -> {
        response.grants().forEach(grant -> {
            logger.info("The grant Id is: " + grant.grantId());
        });
    })
        .thenApply(v -> null)
        .exceptionally(ex -> {
            Throwable cause = ex.getCause();
            if (cause instanceof KmsException) {
                throw new RuntimeException("Failed to list grants: " +
cause.getMessage(), cause);
            } else {
                throw new RuntimeException("An unexpected error occurred: " +
cause.getMessage(), cause);
            }
        });
}
```

```
    }

    /**
     * Revokes a grant for the specified AWS KMS key asynchronously.
     *
     * @param keyId The ID or key ARN of the AWS KMS key.
     * @param grantId The identifier of the grant to be revoked.
     * @return A {@link CompletableFuture} representing the asynchronous
     operation of revoking the grant.
     *
     * The {@link CompletableFuture} will complete with a {@link
     RevokeGrantResponse} object
     *
     * if the operation is successful, or with a {@code null} value if an
     error occurs.
     */
    public CompletableFuture<RevokeGrantResponse> revokeKeyGrantAsync(String
    keyId, String grantId) {
        RevokeGrantRequest grantRequest = RevokeGrantRequest.builder()
            .keyId(keyId)
            .grantId(grantId)
            .build();

        CompletableFuture<RevokeGrantResponse> responseFuture =
    getAsyncClient().revokeGrant(grantRequest);
        responseFuture.whenComplete((response, exception) -> {
            if (exception == null) {
                logger.info("Grant ID: [" + grantId + "] was successfully
    revoked!");
            } else {
                if (exception instanceof KmsException kmsEx) {
                    if (kmsEx.getMessage().contains("Grant does not exist")) {
                        logger.info("The grant ID '" + grantId + "' does not
    exist. Moving on...");
                    } else {
                        throw new RuntimeException("KMS error occurred: " +
    kmsEx.getMessage(), kmsEx);
                    }
                } else {
                    throw new RuntimeException("An unexpected error occurred: " +
    exception.getMessage(), exception);
                }
            }
        });

        return responseFuture;
    }
}
```



```
    }

    /**
     * Asynchronously decrypts the given encrypted data using the specified key
     ID.
     *
     * @param encryptedData The encrypted data to be decrypted.
     * @param keyId The ID of the key to be used for decryption.
     * @return A CompletableFuture that, when completed, will contain the
     decrypted data as a String.
     *
     * If an error occurs during the decryption process, the
     CompletableFuture will complete
     *
     * exceptionally with the error, and the method will return an empty
     String.
     */
    public CompletableFuture<String> decryptDataAsync(SdkBytes encryptedData,
String keyId) {
        DecryptRequest decryptRequest = DecryptRequest.builder()
            .ciphertextBlob(encryptedData)
            .keyId(keyId)
            .build();

        CompletableFuture<DecryptResponse> responseFuture =
getAsyncClient().decrypt(decryptRequest);
        responseFuture.whenComplete((decryptResponse, exception) -> {
            if (exception == null) {
                logger.info("Data decrypted successfully for key ID: " + keyId);
            } else {
                if (exception instanceof KmsException kmsEx) {
                    throw new RuntimeException("KMS error occurred while
decrypting data: " + kmsEx.getMessage(), kmsEx);
                } else {
                    throw new RuntimeException("An unexpected error occurred
while decrypting data: " + exception.getMessage(), exception);
                }
            }
        });

        return responseFuture.thenApply(decryptResponse ->
decryptResponse.plaintext().asString(StandardCharsets.UTF_8));
    }

    /**
```

```

* Asynchronously replaces the policy for the specified KMS key.
*
* @param keyId      the ID of the KMS key to replace the policy for
* @param policyName the name of the policy to be replaced
* @param accountId  the AWS account ID to be used in the policy
* @return a {@link CompletableFuture} that completes with a boolean
indicating
*         whether the policy replacement was successful or not
*/
public CompletableFuture<Boolean> replacePolicyAsync(String keyId, String
policyName, String accountId) {
    String policy = ""
    {
        "Version": "2012-10-17",
        "Statement": [{
            "Effect": "Allow",
            "Principal": {"AWS": "arn:aws:iam::%s:root"},
            "Action": "kms:*",
            "Resource": "*"
        }]
    }
    """".formatted(accountId);

    PutKeyPolicyRequest keyPolicyRequest = PutKeyPolicyRequest.builder()
        .keyId(keyId)
        .policyName(policyName)
        .policy(policy)
        .build();

    // First, get the current policy to check if it exists
    return getAsyncClient().getKeyPolicy(r ->
r.keyId(keyId).policyName(policyName))
        .thenCompose(response -> {
            logger.info("Current policy exists. Replacing it...");
            return getAsyncClient().putKeyPolicy(keyPolicyRequest);
        })
        .thenApply(putPolicyResponse -> {
            logger.info("The key policy has been replaced.");
            return true;
        })
        .exceptionally(throwable -> {
            if (throwable.getCause() instanceof LimitExceededException) {
                logger.error("Cannot replace policy, as only one policy is
allowed per key.");
            }
        });
}

```

```
        return false;
    }
    throw new RuntimeException("Error replacing policy", throwable);
});
}

/**
 * Asynchronously retrieves the key policy for the specified key ID and
 * policy name.
 *
 * @param keyId      the ID of the AWS KMS key for which to retrieve the
 * policy
 * @param policyName the name of the key policy to retrieve
 * @return a {@link CompletableFuture} that, when completed, contains the key
 * policy as a {@link String}
 */
public CompletableFuture<String> getKeyPolicyAsync(String keyId, String
policyName) {
    GetKeyPolicyRequest policyRequest = GetKeyPolicyRequest.builder()
        .keyId(keyId)
        .policyName(policyName)
        .build();

    return getAsyncClient().getKeyPolicy(policyRequest)
        .thenApply(response -> {
            String policy = response.policy();
            logger.info("The response is: " + policy);
            return policy;
        })
        .exceptionally(ex -> {
            throw new RuntimeException("Failed to get key policy", ex);
        });
}

/**
 * Asynchronously signs and verifies data using AWS KMS.
 *
 * <p>The method performs the following steps:</p>
 * <ol>
 * <li>Creates an AWS KMS key with the specified key spec, key usage, and
 * origin.</li>
 * <li>Signs the provided message using the created KMS key and the
 * RSASSA-PSS-SHA-256 algorithm.</li>
 * </ol>
 */
```

```
    *    <li>Verifies the signature of the message using the created KMS key
and the RSASSA-PSS-SHA-256 algorithm.</li>
    * </ol>
    *
    * @return a {@link CompletableFuture} that completes with the result of the
signature verification,
    *     {@code true} if the signature is valid, {@code false} otherwise.
    * @throws KmsException if any error occurs during the KMS operations.
    * @throws RuntimeException if an unexpected error occurs.
    */
public CompletableFuture<Boolean> signVerifyDataAsync() {
    String signMessage = "Here is the message that will be digitally signed";

    // Create an AWS KMS key used to digitally sign data.
    CreateKeyRequest createKeyRequest = CreateKeyRequest.builder()
        .keySpec(KeySpec.RSA_2048)
        .keyUsage(KeyUsageType.SIGN_VERIFY)
        .origin(OriginType.AWS_KMS)
        .build();

    return getAsyncClient().createKey(createKeyRequest)
        .thenCompose(createKeyResponse -> {
            String keyId = createKeyResponse.keyMetadata().keyId();

            SdkBytes messageBytes = SdkBytes.fromString(signMessage,
Charset.defaultCharset());
            SignRequest signRequest = SignRequest.builder()
                .keyId(keyId)
                .message(messageBytes)
                .signingAlgorithm(SigningAlgorithmSpec.RSASSA_PSS_SHA_256)
                .build();

            return getAsyncClient().sign(signRequest)
                .thenCompose(signResponse -> {
                    byte[] signedBytes =
signResponse.signature().asByteArray();

                    VerifyRequest verifyRequest = VerifyRequest.builder()
                        .keyId(keyId)

                        .message(SdkBytes.fromByteArray(signMessage.getBytes(Charset.defaultCharset())))

                        .signature(SdkBytes.fromByteBuffer(ByteBuffer.wrap(signedBytes)))
```

```
.signingAlgorithm(SigningAlgorithmSpec.RSASSA_PSS_SHA_256)
    .build();

    return getAsyncClient().verify(verifyRequest)
        .thenApply(verifyResponse -> {
            return (boolean) verifyResponse.signatureValid();
        });
});

})
.exceptionally(throwable -> {
    throw new RuntimeException("Failed to sign or verify data",
throwable);
});
}

/**
 * Asynchronously tags a KMS key with a specific tag.
 *
 * @param keyId the ID of the KMS key to be tagged
 * @return a {@link CompletableFuture} that completes when the tagging
operation is finished
 */
public CompletableFuture<Void> tagKMSKeyAsync(String keyId) {
    Tag tag = Tag.builder()
        .tagKey("Environment")
        .tagValue("Production")
        .build();

    TagResourceRequest tagResourceRequest = TagResourceRequest.builder()
        .keyId(keyId)
        .tags(tag)
        .build();

    return getAsyncClient().tagResource(tagResourceRequest)
        .thenRun(() -> {
            logger.info("{} key was tagged", keyId);
        })
        .exceptionally(throwable -> {
            throw new RuntimeException("Failed to tag the KMS key",
throwable);
        });
}
```

```
/**
 * Deletes a specific KMS alias asynchronously.
 *
 * @param aliasName the name of the alias to be deleted
 * @return a {@link CompletableFuture} representing the asynchronous
operation of deleting the specified alias
 */
public CompletableFuture<Void> deleteSpecificAliasAsync(String aliasName) {
    DeleteAliasRequest deleteAliasRequest = DeleteAliasRequest.builder()
        .aliasName(aliasName)
        .build();

    return getAsyncClient().deleteAlias(deleteAliasRequest)
        .thenRun(() -> {
            logger.info("Alias {} has been deleted successfully", aliasName);
        })
        .exceptionally(throwable -> {
            throw new RuntimeException("Failed to delete alias: " +
aliasName, throwable);
        });
}

/**
 * Asynchronously disables the specified AWS Key Management Service (KMS)
key.
 *
 * @param keyId the ID or Amazon Resource Name (ARN) of the KMS key to be
disabled
 * @return a CompletableFuture that, when completed, indicates that the key
has been disabled successfully
 */
public CompletableFuture<Void> disableKeyAsync(String keyId) {
    DisableKeyRequest keyRequest = DisableKeyRequest.builder()
        .keyId(keyId)
        .build();

    return getAsyncClient().disableKey(keyRequest)
        .thenRun(() -> {
            logger.info("Key {} has been disabled successfully", keyId);
        })
        .exceptionally(throwable -> {
            throw new RuntimeException("Failed to disable key: " + keyId,
throwable);
        });
}
```

```
    }

    /**
     * Deletes a KMS key asynchronously.
     *
     * 

Warning: Deleting a KMS key is a destructive and
     potentially dangerous operation.
     * When a KMS key is deleted, all data that was encrypted under the KMS key
     becomes unrecoverable.
     * This means that any files, databases, or other data that were encrypted
     using the deleted KMS key
     * will become permanently inaccessible. Exercise extreme caution when
     deleting KMS keys.


     *
     * @param keyId the ID of the KMS key to delete
     * @return a CompletableFuture that completes when the key deletion
     is scheduled
     */
    public CompletableFuture<Void> deleteKeyAsync(String keyId) {
        ScheduleKeyDeletionRequest deletionRequest =
        ScheduleKeyDeletionRequest.builder()
            .keyId(keyId)
            .pendingWindowInDays(7)
            .build();

        return getAsyncClient().scheduleKeyDeletion(deletionRequest)
            .thenRun(() -> {
                logger.info("Key {} will be deleted in 7 days", keyId);
            })
            .exceptionally(throwable -> {
                throw new RuntimeException("Failed to schedule key deletion for
                key ID: " + keyId, throwable);
            });
    }

    public String getAccountId(){
        try (StsClient stsClient = StsClient.create()){
            GetCallerIdentityResponse callerIdentity =
            stsClient.getCallerIdentity();
            return callerIdentity.account();
        }
    }
}
```

- For API details, see the following topics in *Amazon SDK for Java 2.x API Reference*.
 - [CreateAlias](#)
 - [CreateGrant](#)
 - [CreateKey](#)
 - [Decrypt](#)
 - [DescribeKey](#)
 - [DisableKey](#)
 - [EnableKey](#)
 - [Encrypt](#)
 - [GetKeyPolicy](#)
 - [ListAliases](#)
 - [ListGrants](#)
 - [ListKeys](#)
 - [RevokeGrant](#)
 - [ScheduleKeyDeletion](#)
 - [Sign](#)
 - [TagResource](#)

PHP

SDK for PHP

Note

There's more on GitHub. Find the complete example and learn how to set up and run in the [Amazon Code Examples Repository](#).

```
echo "\n";  
echo "-----\n";  
echo <<<WELCOME  
Welcome to the AWS Key Management Service SDK Basics scenario.
```


This program demonstrates how to interact with AWS Key Management Service using the AWS SDK for PHP (v3).

The AWS Key Management Service (KMS) is a secure and highly available service that allows you to create and manage AWS KMS keys and control their use across a wide range of AWS services and applications.

KMS provides a centralized and unified approach to managing encryption keys, making it easier to meet your data protection and regulatory compliance requirements.

This KMS Basics scenario creates two key types:

- A symmetric encryption key is used to encrypt and decrypt data.
- An asymmetric key used to digitally sign data.

Let's get started...\n

```
WELCOME;
```

```
    echo "-----\n";  
    $this->pressEnter();
```

```
    $this->kmsClient = new KmsClient([]);  
    // Initialize the KmsService class with the client. This allows you to  
    // override any defaults in the client before giving it to the service class.  
    $this->kmsService = new KmsService($this->kmsClient);
```

```
    // 1. Create a symmetric KMS key.  
    echo "\n";  
    echo "1. Create a symmetric KMS key.\n";  
    echo "First, we will create a symmetric KMS key that is used to encrypt  
    and decrypt data by invoking createKey().\n";  
    $this->pressEnter();
```

```
    $key = $this->kmsService->createKey();  
    $this->resources['symmetricKey'] = $key['KeyId'];  
    echo "Created a customer key with ARN {$key['Arn']}. \n";  
    $this->pressEnter();
```

```
    // 2. Enable a KMS key.  
    echo "\n";  
    echo "2. Enable a KMS key.\n";  
    echo "By default when you create an AWS key, it is enabled. The code  
    checks to  
    determine if the key is enabled. If it is not enabled, the code enables it.\n";  
    $this->pressEnter();
```

```
$keyInfo = $this->kmsService->describeKey($key['KeyId']);
if(!$keyInfo['Enabled']){
    echo "The key was not enabled, so we will enable it.\n";
    $this->pressEnter();
    $this->kmsService->enableKey($key['KeyId']);
    echo "The key was successfully enabled.\n";
}else{
    echo "The key was already enabled, so there was no need to enable it.
\n";
}
$this->pressEnter();

// 3. Encrypt data using the symmetric KMS key.
echo "\n";
echo "3. Encrypt data using the symmetric KMS key.\n";
echo "One of the main uses of symmetric keys is to encrypt and decrypt
data.\n";
echo "Next, we'll encrypt the string 'Hello, AWS KMS!' with the
SYMMETRIC_DEFAULT encryption algorithm.\n";
$this->pressEnter();
$text = "Hello, AWS KMS!";
$encryption = $this->kmsService->encrypt($key['KeyId'], $text);
echo "The plaintext data was successfully encrypted with the algorithm:
{$encryption['EncryptionAlgorithm']}. \n";
$this->pressEnter();

// 4. Create an alias.
echo "\n";
echo "4. Create an alias.\n";
$aliasInput = testable_readline("Please enter an alias prefixed with
\"alias/\" or press enter to use a default value: ");
if($aliasInput == ""){
    $aliasInput = "alias/dev-encryption-key";
}
$this->kmsService->createAlias($key['KeyId'], $aliasInput);
$this->resources['alias'] = $aliasInput;
echo "The alias \"$aliasInput\" was successfully created.\n";
$this->pressEnter();

// 5. List all of your aliases.
$aliasPageSize = 10;
echo "\n";
echo "5. List all of your aliases, up to $aliasPageSize.\n";
```

```
$this->pressEnter();
$aliasPaginator = $this->kmsService->listAliases();
foreach($aliasPaginator as $pages){
    foreach($pages['Aliases'] as $alias){
        echo $alias['AliasName'] . "\n";
    }
    break;
}
$this->pressEnter();

// 6. Enable automatic rotation of the KMS key.
echo "\n";
echo "6. Enable automatic rotation of the KMS key.\n";
echo "By default, when the SDK enables automatic rotation of a KMS key,
KMS rotates the key material of the KMS key one year (approximately 365 days)
from the enable date and every year
thereafter.";
$this->pressEnter();
$this->kmsService->enableKeyRotation($key['KeyId']);
echo "The key's rotation was successfully set for key:
{$key['KeyId']}\n";
$this->pressEnter();

// 7. Create a grant.
echo "7. Create a grant.\n";
echo "\n";
echo "A grant is a policy instrument that allows Amazon Web Services
principals to use KMS keys.
It also can allow them to view a KMS key (DescribeKey) and create and manage
grants.
When authorizing access to a KMS key, grants are considered along with key
policies and IAM policies.\n";
$granteeARN = testable_readline("Please enter the Amazon Resource Name
(ARN) of an Amazon Web Services principal. Valid principals include Amazon
Web Services accounts, IAM users, IAM roles, federated users, and assumed
role users. For help with the ARN syntax for a principal, see IAM ARNs in the
Identity and Access Management User Guide. \nTo skip this step, press enter
without any other values: ");
if($granteeARN){
    $operations = [
        "ENCRYPT",
        "DECRYPT",
        "DESCRIBE_KEY",
    ];
};
```

```
        $grant = $this->kmsService->createGrant($key['KeyId'], $granteeARN,
$operations);
        echo "The grant Id is: {$grant['GrantId']}\n";
    }else{
        echo "Steps 7, 8, and 9 will be skipped.\n";
    }
    $this->pressEnter();

// 8. List grants for the KMS key.
if($granteeARN){
    echo "8. List grants for the KMS key.\n\n";
    $grantsPaginator = $this->kmsService->listGrants($key['KeyId']);
    foreach($grantsPaginator as $page){
        foreach($page['Grants'] as $grant){
            echo $grant['GrantId'] . "\n";
        }
    }
}else{
    echo "Skipping step 8...\n";
}
$this->pressEnter();

// 9. Revoke the grant.
if($granteeARN) {
    echo "\n";
    echo "9. Revoke the grant.\n";
    $this->pressEnter();
    $this->kmsService->revokeGrant($grant['GrantId'], $keyInfo['KeyId']);
    echo "{$grant['GrantId']} was successfully revoked!\n";
}else{
    echo "Skipping step 9...\n";
}
$this->pressEnter();

// 10. Decrypt the data.
echo "\n";
echo "10. Decrypt the data.\n";
echo "Let's decrypt the data that was encrypted before.\n";
echo "We'll use the same key to decrypt the string that we encrypted
earlier in the program.\n";
$this->pressEnter();
$decryption = $this->kmsService->decrypt($keyInfo['KeyId'],
$encryption['CiphertextBlob'], $encryption['EncryptionAlgorithm']);
echo "The decrypted text is: {$decryption['Plaintext']}\n";
```

```
$this->pressEnter();

// 11. Replace a Key Policy.
echo "\n";
echo "11. Replace a Key Policy.\n";
echo "A key policy is a resource policy for a KMS key. Key policies are
the primary way to control access to KMS keys.\n";
echo "Every KMS key must have exactly one key policy. The statements in
the key policy determine who has permission to use the KMS key and how they can
use it.\n";
echo " You can also use IAM policies and grants to control access to the
KMS key, but every KMS key must have a key policy.\n";
echo "We will replace the key's policy with a new one:\n";
$stsClient = new StsClient([]);
$result = $stsClient->getCallerIdentity();
$accountId = $result['Account'];
$keyPolicy = <<< KEYPOLICY
{
  "Version": "2012-10-17",
  "Statement": [{
    "Effect": "Allow",
    "Principal": {"AWS": "arn:aws:iam::$accountId:root"},
    "Action": "kms:*",
    "Resource": "*"
  }]
}
KEYPOLICY;
echo $keyPolicy;
$this->pressEnter();
$this->kmsService->putKeyPolicy($keyInfo['KeyId'], $keyPolicy);
echo "The Key Policy was successfully replaced!\n";
$this->pressEnter();

// 12. Retrieve the key policy.
echo "\n";
echo "12. Retrieve the key policy.\n";
echo "Let's get some information about the new policy and print it to the
screen.\n";
$this->pressEnter();
$policyInfo = $this->kmsService->getKeyPolicy($keyInfo['KeyId']);
echo "We got the info! Here is the policy: \n";
echo $policyInfo['Policy'] . "\n";
$this->pressEnter();
```

```
// 13. Create an asymmetric KMS key and sign data.
echo "\n";
echo "13. Create an asymmetric KMS key and sign data.\n";
echo "Signing your data with an AWS key can provide several benefits that
make it an attractive option for your data signing needs.\n";
echo "By using an AWS KMS key, you can leverage the security controls and
compliance features provided by AWS, which can help you meet various regulatory
requirements and enhance the overall security posture of your organization.\n";
echo "First we'll create the asymmetric key.\n";
$this->pressEnter();
$keySpec = "RSA_2048";
$keyUsage = "SIGN_VERIFY";
$asymmetricKey = $this->kmsService->createKey($keySpec, $keyUsage);
$this->resources['asymmetricKey'] = $asymmetricKey['KeyId'];
echo "Created the key with ID: {$asymmetricKey['KeyId']}\n";
echo "Next, we'll sign the data.\n";
$this->pressEnter();
$algorithm = "RSASSA_PSS_SHA_256";
$sign = $this->kmsService->sign($asymmetricKey['KeyId'], $text,
$algorithm);
$verify = $this->kmsService->verify($asymmetricKey['KeyId'], $text,
$sign['Signature'], $algorithm);
echo "Signature verification result: {$sign['signature']}\n";
$this->pressEnter();

// 14. Tag the symmetric KMS key.
echo "\n";
echo "14. Tag the symmetric KMS key.\n";
echo "By using tags, you can improve the overall management, security,
and governance of your KMS keys, making it easier to organize, track, and
control access to your encrypted data within your AWS environment.\n";
echo "Let's tag our symmetric key as Environment->Production\n";
$this->pressEnter();
$this->kmsService->tagResource($key['KeyId'], [
    [
        'TagKey' => "Environment",
        'TagValue' => "Production",
    ],
]);
echo "The key was successfully tagged!\n";
$this->pressEnter();

// 15. Schedule the deletion of the KMS key
echo "\n";
```

```
    echo "15. Schedule the deletion of the KMS key.\n";
    echo "By default, KMS applies a waiting period of 30 days, but you can
specify a waiting period of 7-30 days.\n";
    echo "When this operation is successful, the key state of the KMS key
changes to PendingDeletion and the key can't be used in any cryptographic
operations.\n";
    echo "It remains in this state for the duration of the waiting period.\n
\n";

    echo "Deleting a KMS key is a destructive and potentially dangerous
operation. When a KMS key is deleted, all data that was encrypted under the KMS
key is unrecoverable.\n\n";

    $cleanUp = testable_readline("Would you like to delete the resources
created during this scenario, including the keys? (y/n): ");
    if($cleanUp == "Y" || $cleanUp == "y"){
        $this->cleanUp();
    }

    echo
    "-----
\n";
    echo "This concludes the AWS Key Management SDK Basics scenario\n";
    echo
    "-----
\n";

namespace Kms;

use Aws\Kms\Exception\KmsException;
use Aws\Kms\KmsClient;
use Aws\Result;
use Aws\ResultPaginator;
use AwsUtilities\AWSServiceClass;

class KmsService extends AWSServiceClass
{

    protected KmsClient $client;
    protected bool $verbose;

    /**
```

```
* @param KmsClient|null $client
* @param bool $verbose
*/
public function __construct(KmsClient $client = null, bool $verbose = false)
{
    $this->verbose = $verbose;
    if($client){
        $this->client = $client;
        return;
    }
    $this->client = new KmsClient([]);
}

/**
 * @param string $keySpec
 * @param string $keyUsage
 * @param string $description
 * @return array
 */
public function createKey(string $keySpec = "", string $keyUsage = "", string
 $description = "Created by the SDK for PHP")
{
    $parameters = ['Description' => $description];
    if($keySpec && $keyUsage){
        $parameters['KeySpec'] = $keySpec;
        $parameters['KeyUsage'] = $keyUsage;
    }
    try {
        $result = $this->client->createKey($parameters);
        return $result['KeyMetadata'];
    }catch(KmsException $caught){
        // Check for error specific to createKey operations
        if ($caught->getAwsErrorMessage() == "LimitExceededException"){
            echo "The request was rejected because a quota was exceeded. For
 more information, see Quotas in the Key Management Service Developer Guide.";
        }
        throw $caught;
    }
}

/**
```



```
    * @param string $keyId
    * @param string $ciphertext
    * @param string $algorithm
    * @return Result
    */
    public function decrypt(string $keyId, string $ciphertext, string $algorithm
= "SYMMETRIC_DEFAULT")
    {
        try{
            return $this->client->decrypt([
                'CiphertextBlob' => $ciphertext,
                'EncryptionAlgorithm' => $algorithm,
                'KeyId' => $keyId,
            ]);
        }catch(KmsException $caught){
            echo "There was a problem decrypting the data: {"$caught-
>getAwsErrorMessage()}\n";
            throw $caught;
        }
    }

    /**
    * @param string $keyId
    * @param string $text
    * @return Result
    */
    public function encrypt(string $keyId, string $text)
    {
        try {
            return $this->client->encrypt([
                'KeyId' => $keyId,
                'Plaintext' => $text,
            ]);
        }catch(KmsException $caught){
            if($caught->getAwsErrorMessage() == "DisabledException"){
                echo "The request was rejected because the specified KMS key is
not enabled.\n";
            }
            throw $caught;
        }
    }
}
```

```
/**
 * @param string $keyId
 * @param int $limit
 * @return ResultPaginator
 */
public function listAliases(string $keyId = "", int $limit = 0)
{
    $args = [];
    if($keyId){
        $args['KeyId'] = $keyId;
    }
    if($limit){
        $args['Limit'] = $limit;
    }
    try{
        return $this->client->getPaginator("ListAliases", $args);
    }catch(KmsException $caught){
        if($caught->getAwsErrorMessage() == "InvalidMarkerException"){
            echo "The request was rejected because the marker that specifies
where pagination should next begin is not valid.\n";
        }
        throw $caught;
    }
}

/**
 * @param string $keyId
 * @param string $alias
 * @return void
 */
public function createAlias(string $keyId, string $alias)
{
    try{
        $this->client->createAlias([
            'TargetKeyId' => $keyId,
            'AliasName' => $alias,
        ]);
    }catch (KmsException $caught){
        if($caught->getAwsErrorMessage() == "InvalidAliasNameException"){
```

```
        echo "The request was rejected because the specified alias name
is not valid.";
    }
    throw $caught;
}
}

/**
 * @param string $keyId
 * @param string $granteePrincipal
 * @param array $operations
 * @param array $grantTokens
 * @return Result
 */
public function createGrant(string $keyId, string $granteePrincipal, array
$operations, array $grantTokens = [])
{
    $args = [
        'KeyId' => $keyId,
        'GranteePrincipal' => $granteePrincipal,
        'Operations' => $operations,
    ];
    if($grantTokens){
        $args['GrantTokens'] = $grantTokens;
    }
    try{
        return $this->client->createGrant($args);
    }catch(KmsException $caught){
        if($caught->getAwsErrorMessage() == "InvalidGrantTokenException"){
            echo "The request was rejected because the specified grant token
is not valid.\n";
        }
        throw $caught;
    }
}

/**
 * @param string $keyId
 * @return array
 */
```

```
public function describeKey(string $keyId)
{
    try {
        $result = $this->client->describeKey([
            "KeyId" => $keyId,
        ]);
        return $result['KeyMetadata'];
    } catch (KmsException $caught){
        if($caught->getAwsErrorMessage() == "NotFoundException"){
            echo "The request was rejected because the specified entity or
resource could not be found.\n";
        }
        throw $caught;
    }
}

/**
 * @param string $keyId
 * @return void
 */
public function disableKey(string $keyId)
{
    try {
        $this->client->disableKey([
            'KeyId' => $keyId,
        ]);
    } catch (KmsException $caught){
        echo "There was a problem disabling the key: {$caught-
>getAwsErrorMessage()}\n";
        throw $caught;
    }
}

/**
 * @param string $keyId
 * @return void
 */
public function enableKey(string $keyId)
{
    try {
```

```
        $this->client->enableKey([
            'KeyId' => $keyId,
        ]);
    }catch(KmsException $caught){
        if($caught->getAwsErrorMessage() == "NotFoundException"){
            echo "The request was rejected because the specified entity or
resource could not be found.\n";
        }
        throw $caught;
    }
}

/**
 * @return array
 */
public function listKeys()
{
    try {
        $contents = [];
        $paginator = $this->client->getPaginator("ListKeys");
        foreach($paginator as $result){
            foreach ($result['Content'] as $object) {
                $contents[] = $object;
            }
        }
        return $contents;
    }catch(KmsException $caught){
        echo "There was a problem listing the keys: {$caught-
>getAwsErrorMessage()}\n";
        throw $caught;
    }
}

/**
 * @param string $keyId
 * @return Result
 */
public function listGrants(string $keyId)
{
    try{
```

```
        return $this->client->listGrants([
            'KeyId' => $keyId,
        ]);
    }catch(KmsException $caught){
        if($caught->getAwsErrorMessage() == "NotFoundException"){
            echo "    The request was rejected because the specified entity
or resource could not be found.\n";
        }
        throw $caught;
    }
}

/**
 * @param string $keyId
 * @return Result
 */
public function getKeyPolicy(string $keyId)
{
    try {
        return $this->client->getKeyPolicy([
            'KeyId' => $keyId,
        ]);
    }catch(KmsException $caught){
        echo "There was a problem getting the key policy: {$caught-
>getAwsErrorMessage()}\n";
        throw $caught;
    }
}

/**
 * @param string $grantId
 * @param string $keyId
 * @return void
 */
public function revokeGrant(string $grantId, string $keyId)
{
    try{
        $this->client->revokeGrant([
            'GrantId' => $grantId,
            'KeyId' => $keyId,
        ]);
    }catch(KmsException $caught){
```

```
        echo "There was a problem with revoking the grant: {$caught-
>getAwsErrorMessage()}\n";
        throw $caught;
    }
}

/**
 * @param string $keyId
 * @param int $pendingWindowInDays
 * @return void
 */
public function scheduleKeyDeletion(string $keyId, int $pendingWindowInDays =
7)
{
    try {
        $this->client->scheduleKeyDeletion([
            'KeyId' => $keyId,
            'PendingWindowInDays' => $pendingWindowInDays,
        ]);
    } catch(KmsException $caught){
        echo "There was a problem scheduling the key deletion: {$caught-
>getAwsErrorMessage()}\n";
        throw $caught;
    }
}

/**
 * @param string $keyId
 * @param array $tags
 * @return void
 */
public function tagResource(string $keyId, array $tags)
{
    try {
        $this->client->tagResource([
            'KeyId' => $keyId,
            'Tags' => $tags,
        ]);
    } catch(KmsException $caught){
```

```
        echo "There was a problem applying the tag(s): {$caught-
>getAwsErrorMessage()}\n";
        throw $caught;
    }
}

/**
 * @param string $keyId
 * @param string $message
 * @param string $algorithm
 * @return Result
 */
public function sign(string $keyId, string $message, string $algorithm)
{
    try {
        return $this->client->sign([
            'KeyId' => $keyId,
            'Message' => $message,
            'SigningAlgorithm' => $algorithm,
        ]);
    } catch (KmsException $caught){
        echo "There was a problem signing the data: {$caught-
>getAwsErrorMessage()}\n";
        throw $caught;
    }
}

/**
 * @param string $keyId
 * @param int $rotationPeriodInDays
 * @return void
 */
public function enableKeyRotation(string $keyId, int $rotationPeriodInDays =
365)
{
    try{
        $this->client->enableKeyRotation([
            'KeyId' => $keyId,
            'RotationPeriodInDays' => $rotationPeriodInDays,
        ]);
    }
}
```



```
        }catch(KmsException $caught){
            if($caught->getAwsErrorMessage() == "NotFoundException"){
                echo "The request was rejected because the specified entity or
resource could not be found.\n";
            }
            throw $caught;
        }
    }

    /**
     * @param string $keyId
     * @param string $policy
     * @return void
     */
    public function putKeyPolicy(string $keyId, string $policy)
    {
        try {
            $this->client->putKeyPolicy([
                'KeyId' => $keyId,
                'Policy' => $policy,
            ]);
        }catch(KmsException $caught){
            echo "There was a problem replacing the key policy: {$caught-
>getAwsErrorMessage()}\n";
            throw $caught;
        }
    }

    /**
     * @param string $aliasName
     * @return void
     */
    public function deleteAlias(string $aliasName)
    {
        try {
            $this->client->deleteAlias([
                'AliasName' => $aliasName,
            ]);
        }catch(KmsException $caught){
```

```
        echo "There was a problem deleting the alias: {$caught-
>getAwsErrorMessage()}\n";
        throw $caught;
    }
}

/**
 * @param string $keyId
 * @param string $message
 * @param string $signature
 * @param string $signingAlgorithm
 * @return bool
 */
public function verify(string $keyId, string $message, string $signature,
string $signingAlgorithm)
{
    try {
        $result = $this->client->verify([
            'KeyId' => $keyId,
            'Message' => $message,
            'Signature' => $signature,
            'SigningAlgorithm' => $signingAlgorithm,
        ]);
        return $result['SignatureValid'];
    } catch (KmsException $caught){
        echo "There was a problem verifying the signature: {$caught-
>getAwsErrorMessage()}\n";
        throw $caught;
    }
}
}
```

- For API details, see the following topics in *Amazon SDK for PHP API Reference*.
 - [CreateAlias](#)
 - [CreateGrant](#)
 - [CreateKey](#)

- [Decrypt](#)
- [DescribeKey](#)
- [DisableKey](#)
- [EnableKey](#)
- [Encrypt](#)
- [GetKeyPolicy](#)
- [ListAliases](#)
- [ListGrants](#)
- [ListKeys](#)
- [RevokeGrant](#)
- [ScheduleKeyDeletion](#)
- [Sign](#)
- [TagResource](#)

Python

SDK for Python (Boto3)

Note

There's more on GitHub. Find the complete example and learn how to set up and run in the [Amazon Code Examples Repository](#).

```
class KMSScenario:
    """Runs an interactive scenario that shows how to get started with KMS."""

    def __init__(
        self,
        key_manager: KeyManager,
        key_encryption: KeyEncrypt,
        alias_manager: AliasManager,
        grant_manager: GrantManager,
        key_policy: KeyPolicy,
    ):
        self.key_manager = key_manager
```

```
self.key_encryption = key_encryption
self.alias_manager = alias_manager
self.grant_manager = grant_manager
self.key_policy = key_policy
self.key_id = ""
self.alias_name = ""
self.asymmetric_key_id = ""

def kms_scenario(self):
    key_description = "Created by the AWS KMS API"

    print(DASHES)
    print(
        """
Welcome to the AWS Key Management SDK Basics scenario.

This program demonstrates how to interact with AWS Key Management using the AWS
SDK for Python (Boto3).
The AWS Key Management Service (KMS) is a secure and highly available service
that allows you to create
and manage AWS KMS keys and control their use across a wide range of AWS services
and applications.
KMS provides a centralized and unified approach to managing encryption keys,
making it easier to meet your
data protection and regulatory compliance requirements.

This Basics scenario creates two key types:

- A symmetric encryption key is used to encrypt and decrypt data.
- An asymmetric key used to digitally sign data.

Let's get started...
        """
    )
    q.ask("Press Enter to continue...")

    print(DASHES)
    print(f"1. Create a symmetric KMS key\n")
    print(
        f"First, the program will creates a symmetric KMS key that you can
used to encrypt and decrypt data."
    )
    q.ask("Press Enter to continue...")
    self.key_id = self.key_manager.create_key(key_description)["KeyId"]
```

```

print(f"A symmetric key was successfully created {self.key_id}.")
q.ask("Press Enter to continue...")
print(DASHES)
print(
    """

```

2. Enable a KMS key

By default, when the SDK creates an AWS key, it is enabled. The next bit of code checks to determine if the key is enabled.

```

    """
)
q.ask("Press Enter to continue...")
is_enabled = self.is_key_enabled(self.key_id)
print(f"Is the key enabled? {is_enabled}")
if not is_enabled:
    self.key_manager.enable_key(self.key_id)
q.ask("Press Enter to continue...")
print(DASHES)
print(f"3. Encrypt data using the symmetric KMS key")
plain_text = "Hello, AWS KMS!"
print(
    f"""

```

One of the main uses of symmetric keys is to encrypt and decrypt data. Next, the code encrypts the string "{plain_text}" with the SYMMETRIC_DEFAULT encryption algorithm.

```

    """
)
q.ask("Press Enter to continue...")
encrypted_text = self.key_encryption.encrypt(self.key_id, plain_text)
print(DASHES)
print(f"4. Create an alias")
print(
    """

```

Now, the program will create an alias for the KMS key. An alias is a friendly name that you can associate with a KMS key. The alias name should be prefixed with 'alias/'.

```

    """
)
alias_name = q.ask("Enter an alias name: ", q.non_empty)
self.alias_manager.create_alias(self.key_id, alias_name)
print(f"{alias_name} was successfully created.")
self.alias_name = alias_name
print(DASHES)

```

```

print(f"5. List all of your aliases")
q.ask("Press Enter to continue...")
self.alias_manager.list_aliases(10)
q.ask("Press Enter to continue...")
print(DASHES)
print(f"6. Enable automatic rotation of the KMS key")
print(
    """

```

By default, when the SDK enables automatic rotation of a KMS key, KMS rotates the key material of the KMS key one year (approximately 365 days) from the enable date and every year

thereafter.

```

    """
)
q.ask("Press Enter to continue...")
self.key_manager.enable_key_rotation(self.key_id)
print(DASHES)
print(f"Key rotation has been enabled for key with id {self.key_id}")
print(
    """

```

7. Create a grant

A grant is a policy instrument that allows Amazon Web Services principals to use KMS keys.

It also can allow them to view a KMS key (DescribeKey) and create and manage grants.

When authorizing access to a KMS key, grants are considered along with key policies and IAM policies.

```

    """
)
print(
    """

```

To create a grant you must specify a `account_id`. To specify the grantee `account_id`, use the Amazon Resource Name (ARN) of an AWS `account_id`. Valid principals include AWS accounts, IAM users, IAM roles, federated users, and assumed role users.

```

    """
)
account_id = q.ask(
    "Enter an account_id, or press enter to skip creating a grant... "
)
grant = None

```

```

    if account_id != "":
        grant = self.grant_manager.create_grant(
            self.key_id,
            account_id,
            [
                "Encrypt",
                "Decrypt",
                "DescribeKey",
            ],
        )
        print(f"Grant created successfully with ID: {grant['GrantId']}")

```

```

q.ask("Press Enter to continue...")
print(DASHES)
print(DASHES)
print(f"8. List grants for the KMS key")
q.ask("Press Enter to continue...")
self.grant_manager.list_grants(self.key_id)
q.ask("Press Enter to continue...")
print(DASHES)
print(f"9. Revoke the grant")
print(
    """"

```

The revocation of a grant immediately removes the permissions and access that the grant had provided.

This means that any `account_id` (user, role, or service) that was granted access to perform specific

KMS operations on a KMS key will no longer be able to perform those operations.

```

    """"
    )
    q.ask("Press Enter to continue...")

    if grant is not None:
        self.grant_manager.revoke_grant(self.key_id, grant["GrantId"])
        print(f"Grant ID: {grant['GrantId']} was successfully revoked!")

```

```

q.ask("Press Enter to continue...")
print(DASHES)
print(f"10. Decrypt the data\n")
print(
    """"

```

Lets decrypt the data that was encrypted in an early step.

The code uses the same key to decrypt the string that we encrypted earlier in the program.

```

    """
    )
    q.ask("Press Enter to continue...")
    decrypted_data = self.key_encryption.decrypt(self.key_id, encrypted_text)
    print(f"Data decrypted successfully for key ID: {self.key_id}")
    print(f"Decrypted data: {decrypted_data}")

    q.ask("Press Enter to continue...")
    print(DASHES)
    print(f"11. Replace a key policy\n")
    print(
        """

```

A key policy is a resource policy for a KMS key. Key policies are the primary way to control access to KMS keys. Every KMS key must have exactly one key policy. The statements in the key policy determine who has permission to use the KMS key and how they can use it. You can also use IAM policies and grants to control access to the KMS key, but every KMS key must have a key policy.

By default, when you create a key by using the SDK, a policy is created that gives the AWS account that owns the KMS key full access to the KMS key.

Let's try to replace the automatically created policy with the following policy.

```

{
  "Version": "2012-10-17",
  "Statement": [{
    "Effect": "Allow",
    "Principal": {"AWS": "arn:aws:iam::0000000000:root"},
    "Action": "kms:*",
    "Resource": "*"
  }]
}
    """
    )
    account_id = q.ask("Enter your account ID or press enter to skip: ")
    if account_id != "":
        policy = {
            "Version": "2012-10-17",
            "Statement": [
                {
                    "Effect": "Allow",
                    "Principal": {"AWS": f"arn:aws:iam::{account_id}:root"},

```



```
        "Action": "kms:*",
        "Resource": "*",
    }
    ],
}

self.key_policy.set_new_policy(self.key_id, policy)
print("Key policy replacement succeeded.")
q.ask("Press Enter to continue...")
else:
    print("Skipping replacing the key policy.")

print(DASHES)
print(f"12. Get the key policy\n")
print(
    f"The next bit of code that runs gets the key policy to make sure it
exists."
)
q.ask("Press Enter to continue...")
policy = self.key_policy.get_policy(self.key_id)
print(f"The key policy is: {policy}")

q.ask("Press Enter to continue...")
print(DASHES)
print(f"13. Create an asymmetric KMS key and sign your data\n")
print(
    """
    Signing your data with an AWS key can provide several benefits that make
it an attractive option
    for your data signing needs. By using an AWS KMS key, you can leverage
the
    security controls and compliance features provided by AWS,
    which can help you meet various regulatory requirements and enhance the
overall security posture
    of your organization.
    """
)
q.ask("Press Enter to continue...")
print(f"Sign and verify data operation succeeded.")
self.asymmetric_key_id = self.key_manager.create_asymmetric_key()
message = "Here is the message that will be digitally signed"
signature = self.key_encryption.sign(self.asymmetric_key_id, message)
if self.key_encryption.verify(self.asymmetric_key_id, message,
signature):
```

```

        print("Signature verification succeeded.")
    else:
        print("Signature verification failed.")

    q.ask("Press Enter to continue...")
    print(DASHES)
    print(f"14. Tag your symmetric KMS Key\n")
    print(
        """
        By using tags, you can improve the overall management, security, and
        governance of your
        KMS keys, making it easier to organize, track, and control access to your
        encrypted data within
        your AWS environment
        """
    )
    q.ask("Press Enter to continue...")
    self.key_manager.tag_resource(self.key_id, "Environment", "Production")
    self.clean_up()

def is_key_enabled(self, key_id: str) -> bool:
    """
    Check if the key is enabled or not.

    :param key_id: The key to check.
    :return: True if the key is enabled, otherwise False.
    """
    response = self.key_manager.describe_key(key_id)
    return response["Enabled"] is True

def clean_up(self):
    """
    Delete resources created by this scenario.
    """
    if self.alias_name != "":
        print(f"Deleting the alias {self.alias_name}.")
        self.alias_manager.delete_alias(self.alias_name)
    window = 7 # The window in days for a scheduled deletion.
    if self.key_id != "":
        print(
            """

```

Warning:

Deleting a KMS key is a destructive and potentially dangerous operation. When a KMS key is deleted,

```
all data that was encrypted under the KMS key is unrecoverable.
    """
    )
    if q.ask(
        f"Do you want to delete the key with ID {self.key_id} (y/n)?",
        q.is_yesno,
    ):
        print(
            f"The key {self.key_id} will be deleted with a window of
{window} days. You can cancel the deletion before"
        )
        print("the window expires.")
        self.key_manager.delete_key(self.key_id, window)
        self.key_id = ""

    if self.asymmetric_key_id != "":
        if q.ask(
            f"Do you want to delete the asymmetric key with ID
{self.asymmetric_key_id} (y/n)?",
            q.is_yesno,
        ):
            print(
                f"The key {self.asymmetric_key_id} will be deleted with a
window of {window} days. You can cancel the deletion before"
            )
            print("the window expires.")
            self.key_manager.delete_key(self.asymmetric_key_id, window)
            self.asymmetric_key_id = ""

if __name__ == "__main__":
    kms_scenario = None
    try:
        kms_client = boto3.client("kms")
        a_key_manager = KeyManager(kms_client)
        a_key_encrypt = KeyEncrypt(kms_client)
        an_alias_manager = AliasManager(kms_client)
        a_grant_manager = GrantManager(kms_client)
        a_key_policy = KeyPolicy(kms_client)
        kms_scenario = KMSScenario(
            key_manager=a_key_manager,
            key_encryption=a_key_encrypt,
            alias_manager=an_alias_manager,
            grant_manager=a_grant_manager,
```

```

        key_policy=a_key_policy,
    )
    kms_scenario.kms_scenario()
except Exception:
    logging.exception("Something went wrong with the demo!")
if kms_scenario is not None:
    kms_scenario.clean_up()

```

Wrapper class and methods for KMS key management.

```

class KeyManager:
    def __init__(self, kms_client):
        self.kms_client = kms_client
        self.created_keys = []

    @classmethod
    def from_client(cls) -> "KeyManager":
        """
        Creates a KeyManager instance with a default KMS client.

        :return: An instance of KeyManager initialized with the default KMS
        client.
        """
        kms_client = boto3.client("kms")
        return cls(kms_client)

    def create_key(self, key_description: str) -> dict[str, any]:
        """
        Creates a key with a user-provided description.

        :param key_description: A description for the key.
        :return: The key ID.
        """
        try:
            key = self.kms_client.create_key(Description=key_description)
            ["KeyMetadata"]
            self.created_keys.append(key)
            return key
        except ClientError as err:
            logging.error(

```

```
        "Couldn't create your key. Here's why: %s",
        err.response["Error"]["Message"],
    )
    raise

def describe_key(self, key_id: str) -> dict[str, any]:
    """
    Describes a key.

    :param key_id: The ARN or ID of the key to describe.
    :return: Information about the key.
    """

    try:
        key = self.kms_client.describe_key(KeyId=key_id)["KeyMetadata"]
        return key
    except ClientError as err:
        logging.error(
            "Couldn't get key '%s'. Here's why: %s",
            key_id,
            err.response["Error"]["Message"],
        )
        raise

def enable_key_rotation(self, key_id: str) -> None:
    """
    Enables rotation for a key.

    :param key_id: The ARN or ID of the key to enable rotation for.
    """

    try:
        self.kms_client.enable_key_rotation(KeyId=key_id)
    except ClientError as err:
        logging.error(
            "Couldn't enable rotation for key '%s'. Here's why: %s",
            key_id,
            err.response["Error"]["Message"],
        )
        raise

def create_asymmetric_key(self) -> str:
```

```
"""
Creates an asymmetric key in AWS KMS for signing messages.

:return: The ID of the created key.
"""
try:
    key = self.kms_client.create_key(
        KeySpec="RSA_2048", KeyUsage="SIGN_VERIFY", Origin="AWS_KMS"
    )["KeyMetadata"]
    self.created_keys.append(key)
    return key["KeyId"]
except ClientError as err:
    logger.error(
        "Couldn't create your key. Here's why: %s",
        err.response["Error"]["Message"],
    )
    raise

def tag_resource(self, key_id: str, tag_key: str, tag_value: str) -> None:
    """
    Add or edit tags on a customer managed key.

    :param key_id: The ARN or ID of the key to enable rotation for.
    :param tag_key: Key for the tag.
    :param tag_value: Value for the tag.
    """
    try:
        self.kms_client.tag_resource(
            KeyId=key_id, Tags=[{"TagKey": tag_key, "TagValue": tag_value}]
        )
    except ClientError as err:
        logging.error(
            "Couldn't add a tag for the key '%s'. Here's why: %s",
            key_id,
            err.response["Error"]["Message"],
        )
        raise

def delete_key(self, key_id: str, window: int) -> None:
    """
    Deletes a list of keys.
```

```

Warning:
Deleting a KMS key is a destructive and potentially dangerous operation.
When a KMS key is deleted,
all data that was encrypted under the KMS key is unrecoverable.

:param key_id: The ARN or ID of the key to delete.
:param window: The waiting period, in days, before the KMS key is
deleted.
"""

try:
    self.kms_client.schedule_key_deletion(
        KeyId=key_id, PendingWindowInDays=window
    )
except ClientError as err:
    logging.error(
        "Couldn't delete key %s. Here's why: %s",
        key_id,
        err.response["Error"]["Message"],
    )
    raise

```

Wrapper class and methods for KMS key aliases.

```

class AliasManager:
    def __init__(self, kms_client):
        self.kms_client = kms_client
        self.created_key = None

    @classmethod
    def from_client(cls) -> "AliasManager":
        """
        Creates an AliasManager instance with a default KMS client.

        :return: An instance of AliasManager initialized with the default KMS
client.
        """
        kms_client = boto3.client("kms")
        return cls(kms_client)

```

```
def create_alias(self, key_id: str, alias: str) -> None:
    """
    Creates an alias for the specified key.

    :param key_id: The ARN or ID of a key to give an alias.
    :param alias: The alias to assign to the key.
    """
    try:
        self.kms_client.create_alias(AliasName=alias, TargetKeyId=key_id)
    except ClientError as err:
        if err.response["Error"]["Code"] == "AlreadyExistsException":
            logger.error(
                "Could not create the alias %s because it already exists.",
                key_id
            )
        else:
            logger.error(
                "Couldn't encrypt text. Here's why: %s",
                err.response["Error"]["Message"],
            )
            raise

def list_aliases(self, page_size: int) -> None:
    """
    Lists aliases for the current account.
    :param page_size: The number of aliases to list per page.
    """
    try:
        alias_paginator = self.kms_client.get_paginator("list_aliases")
        for alias_page in alias_paginator.paginate(
            PaginationConfig={"PageSize": page_size}
        ):
            print(f"Here are {page_size} aliases:")
            pprint(alias_page["Aliases"])
            if alias_page["Truncated"]:
                answer = input(
                    f"Do you want to see the next {page_size} aliases (y/n)?
                "
                )
                if answer.lower() != "y":
                    break
            else:
                print("That's all your aliases!")
```



```

except ClientError as err:
    logging.error(
        "Couldn't list your aliases. Here's why: %s",
        err.response["Error"]["Message"],
    )
    raise

def delete_alias(self, alias: str) -> None:
    """
    Deletes an alias.

    :param alias: The alias to delete.
    """
    try:
        self.kms_client.delete_alias(AliasName=alias)
    except ClientError as err:
        logger.error(
            "Couldn't delete alias %s. Here's why: %s",
            alias,
            err.response["Error"]["Message"],
        )
        raise

```

Wrapper class and methods for KMS key encryption.

```

class KeyEncrypt:
    def __init__(self, kms_client):
        self.kms_client = kms_client

    @classmethod
    def from_client(cls) -> "KeyEncrypt":
        """
        Creates a KeyEncrypt instance with a default KMS client.

        :return: An instance of KeyEncrypt initialized with the default KMS
        client.
        """
        kms_client = boto3.client("kms")
        return cls(kms_client)

```

```
def encrypt(self, key_id: str, text: str) -> str:
    """
    Encrypts text by using the specified key.

    :param key_id: The ARN or ID of the key to use for encryption.
    :param text: The text to encrypt.
    :return: The encrypted version of the text.
    """
    try:
        response = self.kms_client.encrypt(KeyId=key_id,
Plaintext=text.encode())
        print(
            f"The string was encrypted with algorithm
{response['EncryptionAlgorithm']}"
        )
        return response["CiphertextBlob"]
    except ClientError as err:
        if err.response["Error"]["Code"] == "DisabledException":
            logger.error(
                "Could not encrypt because the key %s is disabled.", key_id
            )
        else:
            logger.error(
                "Couldn't encrypt text. Here's why: %s",
                err.response["Error"]["Message"],
            )
        raise

def decrypt(self, key_id: str, cipher_text: str) -> bytes:
    """
    Decrypts text previously encrypted with a key.

    :param key_id: The ARN or ID of the key used to decrypt the data.
    :param cipher_text: The encrypted text to decrypt.
    :return: The decrypted text.
    """
    try:
        return self.kms_client.decrypt(KeyId=key_id,
CiphertextBlob=cipher_text)[
            "Plaintext"
        ]
```

```
except ClientError as err:
    logger.error(
        "Couldn't decrypt your ciphertext. Here's why: %s",
        err.response["Error"]["Message"],
    )
    raise

def sign(self, key_id: str, message: str) -> str:
    """
    Signs a message with a key.

    :param key_id: The ARN or ID of the key to use for signing.
    :param message: The message to sign.
    :return: The signature of the message.
    """
    try:
        return self.kms_client.sign(
            KeyId=key_id,
            Message=message.encode(),
            SigningAlgorithm="RSASSA_PSS_SHA_256",
        )["Signature"]
    except ClientError as err:
        logger.error(
            "Couldn't sign your message. Here's why: %s",
            err.response["Error"]["Message"],
        )
        raise

def verify(self, key_id: str, message: str, signature: str) -> bool:
    """
    Verifies a signature against a message.

    :param key_id: The ARN or ID of the key used to sign the message.
    :param message: The message to verify.
    :param signature: The signature to verify.
    :return: True when the signature matches the message, otherwise False.
    """
    try:
        response = self.kms_client.verify(
            KeyId=key_id,
            Message=message.encode(),
            Signature=signature,
```

```

        SigningAlgorithm="RSASSA_PSS_SHA_256",
    )
    valid = response["SignatureValid"]
    print(f"The signature is {'valid' if valid else 'invalid'}.")
    return valid
except ClientError as err:
    if err.response["Error"]["Code"] == "SignatureDoesNotMatchException":
        print("The signature is not valid.")
    else:
        logger.error(
            "Couldn't verify your signature. Here's why: %s",
            err.response["Error"]["Message"],
        )
    raise

```

Wrapper class and methods for KMS key grants.

```

class GrantManager:
    def __init__(self, kms_client):
        self.kms_client = kms_client

    @classmethod
    def from_client(cls) -> "GrantManager":
        """
        Creates a GrantManager instance with a default KMS client.

        :return: An instance of GrantManager initialized with the default KMS
        client.
        """
        kms_client = boto3.client("kms")
        return cls(kms_client)

    def create_grant(
        self, key_id: str, principal: str, operations: [str]
    ) -> dict[str, str]:
        """
        Creates a grant for a key that lets a principal generate a symmetric data
        encryption key.

        :param key_id: The ARN or ID of the key.

```

```
:param principal: The principal to grant permission to.
:param operations: The operations to grant permission for.
:return: The grant that is created.
"""
try:
    return self.kms_client.create_grant(
        KeyId=key_id,
        GranteePrincipal=principal,
        Operations=operations,
    )
except ClientError as err:
    logger.error(
        "Couldn't create a grant on key %s. Here's why: %s",
        key_id,
        err.response["Error"]["Message"],
    )
    raise

def list_grants(self, key_id):
    """
    Lists grants for a key.

    :param key_id: The ARN or ID of the key to query.
    :return: The grants for the key.
    """
    try:
        paginator = self.kms_client.get_paginator("list_grants")
        grants = []
        page_iterator = paginator.paginate(KeyId=key_id)
        for page in page_iterator:
            grants.extend(page["Grants"])

        print(f"Grants for key {key_id}:")
        pprint(grants)
        return grants
    except ClientError as err:
        logger.error(
            "Couldn't list grants for key %s. Here's why: %s",
            key_id,
            err.response["Error"]["Message"],
        )
        raise
```

```

def revoke_grant(self, key_id: str, grant_id: str) -> None:
    """
    Revokes a grant so that it can no longer be used.

    :param key_id: The ARN or ID of the key associated with the grant.
    :param grant_id: The ID of the grant to revoke.
    """
    try:
        self.kms_client.revoke_grant(KeyId=key_id, GrantId=grant_id)
    except ClientError as err:
        logger.error(
            "Couldn't revoke grant %s. Here's why: %s",
            grant_id,
            err.response["Error"]["Message"],
        )
        raise

```

Wrapper class and methods for KMS key policies.

```

class KeyPolicy:
    def __init__(self, kms_client):
        self.kms_client = kms_client

    @classmethod
    def from_client(cls) -> "KeyPolicy":
        """
        Creates a KeyPolicy instance with a default KMS client.

        :return: An instance of KeyPolicy initialized with the default KMS
        client.
        """
        kms_client = boto3.client("kms")
        return cls(kms_client)

    def set_new_policy(self, key_id: str, policy: dict[str, any]) -> None:
        """
        Sets the policy of a key. Setting a policy entirely overwrites the
        existing

```

```
    policy, so care is taken to add a statement to the existing list of
statements
    rather than simply writing a new policy.

    :param key_id: The ARN or ID of the key to set the policy to.
    :param policy: A new key policy. The key policy must allow the calling
principal to make a subsequent
        PutKeyPolicy request on the KMS key. This reduces the risk
that the KMS key becomes unmanageable
    """

    try:
        self.kms_client.put_key_policy(KeyId=key_id,
Policy=json.dumps(policy))
    except ClientError as err:
        logger.error(
            "Couldn't set policy for key %s. Here's why %s",
            key_id,
            err.response["Error"]["Message"],
        )
        raise

def get_policy(self, key_id: str) -> dict[str, str]:
    """
    Gets the policy of a key.

    :param key_id: The ARN or ID of the key to query.
    :return: The key policy as a dict.
    """
    if key_id != "":
        try:
            response = self.kms_client.get_key_policy(
                KeyId=key_id,
            )
            policy = json.loads(response["Policy"])
        except ClientError as err:
            logger.error(
                "Couldn't get policy for key %s. Here's why: %s",
                key_id,
                err.response["Error"]["Message"],
            )
            raise
```

```
        else:
            pprint(policy)
            return policy
    else:
        print("Skipping get policy demo.")
```

- For API details, see the following topics in *Amazon SDK for Python (Boto3) API Reference*.
 - [CreateAlias](#)
 - [CreateGrant](#)
 - [CreateKey](#)
 - [Decrypt](#)
 - [DescribeKey](#)
 - [DisableKey](#)
 - [EnableKey](#)
 - [Encrypt](#)
 - [GetKeyPolicy](#)
 - [ListAliases](#)
 - [ListGrants](#)
 - [ListKeys](#)
 - [RevokeGrant](#)
 - [ScheduleKeyDeletion](#)
 - [Sign](#)
 - [TagResource](#)

For a complete list of Amazon SDK developer guides and code examples, see [Using this service with an Amazon SDK](#). This topic also includes information about getting started and details about previous SDK versions.

Actions for Amazon KMS using Amazon SDKs

The following code examples demonstrate how to perform individual Amazon KMS actions with Amazon SDKs. Each example includes a link to GitHub, where you can find instructions for setting up and running the code.

The following examples include only the most commonly used actions. For a complete list, see the [Amazon Key Management Service API Reference](#).

Examples

- [Use CreateAlias with an Amazon SDK or CLI](#)
- [Use CreateGrant with an Amazon SDK or CLI](#)
- [Use CreateKey with an Amazon SDK or CLI](#)
- [Use Decrypt with an Amazon SDK or CLI](#)
- [Use DeleteAlias with an Amazon SDK or CLI](#)
- [Use DescribeKey with an Amazon SDK or CLI](#)
- [Use DisableKey with an Amazon SDK or CLI](#)
- [Use EnableKey with an Amazon SDK or CLI](#)
- [Use EnableKeyRotation with an Amazon SDK or CLI](#)
- [Use Encrypt with an Amazon SDK or CLI](#)
- [Use GenerateDataKey with an Amazon SDK or CLI](#)
- [Use GenerateDataKeyWithoutPlaintext with an Amazon SDK or CLI](#)
- [Use GenerateRandom with an Amazon SDK or CLI](#)
- [Use GetKeyPolicy with an Amazon SDK or CLI](#)
- [Use ListAliases with an Amazon SDK or CLI](#)
- [Use ListGrants with an Amazon SDK or CLI](#)
- [Use ListKeyPolicies with an Amazon SDK or CLI](#)
- [Use ListKeys with an Amazon SDK or CLI](#)
- [Use PutKeyPolicy with an Amazon SDK or CLI](#)
- [Use ReEncrypt with an Amazon SDK or CLI](#)
- [Use RetireGrant with an Amazon SDK or CLI](#)
- [Use RevokeGrant with an Amazon SDK or CLI](#)
- [Use ScheduleKeyDeletion with an Amazon SDK or CLI](#)
- [Use Sign with an Amazon SDK or CLI](#)
- [Use TagResource with an Amazon SDK or CLI](#)

- [Use UpdateAlias with an Amazon SDK or CLI](#)
- [Use Verify with an Amazon SDK or CLI](#)

Use CreateAlias with an Amazon SDK or CLI

The following code examples show how to use CreateAlias.

Action examples are code excerpts from larger programs and must be run in context. You can see this action in context in the following code example:

- [Learn the basics](#)

.NET

Amazon SDK for .NET

Note

There's more on GitHub. Find the complete example and learn how to set up and run in the [Amazon Code Examples Repository](#).

```
using System;
using System.Threading.Tasks;
using Amazon.KeyManagementService;
using Amazon.KeyManagementService.Model;

/// <summary>
/// Creates an alias for an AWS Key Management Service (AWS KMS) key.
/// </summary>
public class CreateAlias
{
    public static async Task Main()
    {
        var client = new AmazonKeyManagementServiceClient();

        // The alias name must start with alias/ and can be
        // up to 256 alphanumeric characters long.
        var aliasName = "alias/ExampleAlias";
```

```
// The value supplied as the TargetKeyId can be either
// the key ID or key Amazon Resource Name (ARN) of the
// AWS KMS key.
var keyId = "1234abcd-12ab-34cd-56ef-1234567890ab";

var request = new CreateAliasRequest
{
    AliasName = aliasName,
    TargetKeyId = keyId,
};

var response = await client.CreateAliasAsync(request);

if (response.HttpStatusCode == System.Net.HttpStatusCode.OK)
{
    Console.WriteLine($"Alias, {aliasName}, successfully created.");
}
else
{
    Console.WriteLine($"Could not create alias.");
}
}
```

- For API details, see [CreateAlias](#) in *Amazon SDK for .NET API Reference*.

CLI

Amazon CLI

To create an alias for a KMS key

The following `create-alias` command creates an alias named `example-alias` for the KMS key identified by key ID `1234abcd-12ab-34cd-56ef-1234567890ab`.

Alias names must begin with `alias/`. Do not use alias names that begin with `alias/aws/`; these are reserved for use by Amazon.

```
aws kms create-alias \  
    --alias-name alias/example-alias \  
    --target-key-id 1234abcd-12ab-34cd-56ef-1234567890ab
```

```
--target-key-id 1234abcd-12ab-34cd-56ef-1234567890ab
```

This command doesn't return any output. To see the new alias, use the `list-aliases` command.

For more information, see [Using aliases](#) in the *Amazon Key Management Service Developer Guide*.

- For API details, see [CreateAlias](#) in *Amazon CLI Command Reference*.

Java

SDK for Java 2.x

Note

There's more on GitHub. Find the complete example and learn how to set up and run in the [Amazon Code Examples Repository](#).

```
/**
 * Creates a custom alias for the specified target key asynchronously.
 *
 * @param targetKeyId the ID of the target key for the alias
 * @param aliasName the name of the alias to create
 * @return a {@link CompletableFuture} that completes when the alias creation
 * operation is finished
 */
public CompletableFuture<Void> createCustomAliasAsync(String targetKeyId,
String aliasName) {
    CreateAliasRequest aliasRequest = CreateAliasRequest.builder()
        .aliasName(aliasName)
        .targetKeyId(targetKeyId)
        .build();

    CompletableFuture<CreateAliasResponse> responseFuture =
getAsyncClient().createAlias(aliasRequest);
    responseFuture.whenComplete((response, exception) -> {
        if (exception == null) {
            logger.info("{} was successfully created.", aliasName);
        } else {
```

```

        if (exception instanceof ResourceExistsException) {
            logger.info("Alias [{}] already exists. Moving on...",
aliasName);
        } else if (exception instanceof KmsException kmsEx) {
            throw new RuntimeException("KMS error occurred while creating
alias: " + kmsEx.getMessage(), kmsEx);
        } else {
            throw new RuntimeException("An unexpected error occurred
while creating alias: " + exception.getMessage(), exception);
        }
    }
});

return responseFuture.thenApply(response -> null);
}

```

- For API details, see [CreateAlias](#) in *Amazon SDK for Java 2.x API Reference*.

Kotlin

SDK for Kotlin

Note

There's more on GitHub. Find the complete example and learn how to set up and run in the [Amazon Code Examples Repository](#).

```

suspend fun createCustomAlias(
    targetKeyIdVal: String?,
    aliasNameVal: String?,
) {
    val request =
        CreateAliasRequest {
            aliasName = aliasNameVal
            targetKeyId = targetKeyIdVal
        }

    KmsClient { region = "us-west-2" }.use { kmsClient ->
        kmsClient.createAlias(request)
        println("$aliasNameVal was successfully created")
    }
}

```

```
}  
}
```

- For API details, see [CreateAlias](#) in *Amazon SDK for Kotlin API reference*.

PHP

SDK for PHP

Note


There's more on GitHub. Find the complete example and learn how to set up and run in the [Amazon Code Examples Repository](#).

```
/**  
 * @param string $keyId  
 * @param string $alias  
 * @return void  
 */  
public function createAlias(string $keyId, string $alias)  
{  
    try{  
        $this->client->createAlias([  
            'TargetKeyId' => $keyId,  
            'AliasName' => $alias,  
        ]);  
    }catch (KmsException $caught){  
        if($caught->getAwsErrorMessage() == "InvalidAliasNameException"){  
            echo "The request was rejected because the specified alias name  
is not valid."  
        }  
        throw $caught;  
    }  
}
```

- For API details, see [CreateAlias](#) in *Amazon SDK for PHP API Reference*.

Python

SDK for Python (Boto3)

 **Note**

There's more on GitHub. Find the complete example and learn how to set up and run in the [Amazon Code Examples Repository](#).

```
class AliasManager:
    def __init__(self, kms_client):
        self.kms_client = kms_client
        self.created_key = None

    @classmethod
    def from_client(cls) -> "AliasManager":
        """
        Creates an AliasManager instance with a default KMS client.

        :return: An instance of AliasManager initialized with the default KMS
        client.
        """
        kms_client = boto3.client("kms")
        return cls(kms_client)

    def create_alias(self, key_id: str, alias: str) -> None:
        """
        Creates an alias for the specified key.

        :param key_id: The ARN or ID of a key to give an alias.
        :param alias: The alias to assign to the key.
        """
        try:
            self.kms_client.create_alias(AliasName=alias, TargetKeyId=key_id)
        except ClientError as err:
            if err.response["Error"]["Code"] == "AlreadyExistsException":
                logger.error(
                    "Could not create the alias %s because it already exists.",
                    key_id
                )
```

```
else:
    logger.error(
        "Couldn't encrypt text. Here's why: %s",
        err.response["Error"]["Message"],
    )
    raise
```

- For API details, see [CreateAlias](#) in *Amazon SDK for Python (Boto3) API Reference*.

For a complete list of Amazon SDK developer guides and code examples, see [Using this service with an Amazon SDK](#). This topic also includes information about getting started and details about previous SDK versions.

Use CreateGrant with an Amazon SDK or CLI

The following code examples show how to use CreateGrant.

Action examples are code excerpts from larger programs and must be run in context. You can see this action in context in the following code example:

- [Learn the basics](#)

.NET

Amazon SDK for .NET

Note

There's more on GitHub. Find the complete example and learn how to set up and run in the [Amazon Code Examples Repository](#).

```
public static async Task Main()
{
    var client = new AmazonKeyManagementServiceClient();

    // The identity that is given permission to perform the operations
    // specified in the grant.
```



```

        var grantee = "arn:aws:iam::111122223333:role/ExampleRole";

        // The identifier of the AWS KMS key to which the grant applies. You
        // can use the key ID or the Amazon Resource Name (ARN) of the KMS
key.
        var keyId = "7c9eccc2-38cb-4c4f-9db3-766ee8dd3ad4";

        var request = new CreateGrantRequest
        {
            GranteePrincipal = grantee,
            KeyId = keyId,

            // A list of operations that the grant allows.
            Operations = new List<string>
            {
                "Encrypt",
                "Decrypt",
            },
        };

        var response = await client.CreateGrantAsync(request);

        string grantId = response.GrantId; // The unique identifier of the
grant.
        string grantToken = response.GrantToken; // The grant token.

        Console.WriteLine($"Id: {grantId}, Token: {grantToken}");
    }
}

```

- For API details, see [CreateGrant](#) in *Amazon SDK for .NET API Reference*.

CLI

Amazon CLI

To create a grant

The following `create-grant` example creates a grant that allows the `exampleUser` user to use the `decrypt` command on the `1234abcd-12ab-34cd-56ef-1234567890ab` example KMS key. The retiring principal is the `adminRole` role. The grant uses the

EncryptionContextSubset grant constraint to allow this permission only when the encryption context in the decrypt request includes the "Department": "IT" key-value pair.

```
aws kms create-grant \  
  --key-id 1234abcd-12ab-34cd-56ef-1234567890ab \  
  --grantee-principal arn:aws:iam::123456789012:user/exampleUser \  
  --operations Decrypt \  
  --constraints EncryptionContextSubset={Department=IT} \  
  --retiring-principal arn:aws:iam::123456789012:role/adminRole
```

Output:

```
{  
  "GrantId":  
    "1a2b3c4d2f5e69f440bae30eaec9570bb1fb7358824f9ddfa1aa5a0dab1a59b2",  
  "GrantToken": "<grant token here>"  
}
```

To view detailed information about the grant, use the `list-grants` command.

For more information, see [Grants in Amazon KMS](#) in the *Amazon Key Management Service Developer Guide*.

- For API details, see [CreateGrant](#) in *Amazon CLI Command Reference*.

Java

SDK for Java 2.x

Note

There's more on GitHub. Find the complete example and learn how to set up and run in the [Amazon Code Examples Repository](#).

```
/**  
 * Grants permissions to a specified principal on a customer master key (CMK)  
 asynchronously.  
 */
```

```
    * @param keyId          The unique identifier for the customer master key
(CMK) that the grant applies to.
    * @param granteePrincipal The principal that is given permission to perform
the operations that the grant permits on the CMK.
    * @return A {@link CompletableFuture} that, when completed, contains the ID
of the created grant.
    * @throws RuntimeException If an error occurs during the grant creation
process.
    */
    public CompletableFuture<String> grantKeyAsync(String keyId, String
granteePrincipal) {
        List<GrantOperation> grantPermissions = List.of(
            GrantOperation.ENCRYPT,
            GrantOperation.DECRYPT,
            GrantOperation.DESCRIBE_KEY
        );

        CreateGrantRequest grantRequest = CreateGrantRequest.builder()
            .keyId(keyId)
            .name("grant1")
            .granteePrincipal(granteePrincipal)
            .operations(grantPermissions)
            .build();

        CompletableFuture<CreateGrantResponse> responseFuture =
getAsyncClient().createGrant(grantRequest);
        responseFuture.whenComplete((response, ex) -> {
            if (ex == null) {
                logger.info("Grant created successfully with ID: " +
response.grantId());
            } else {
                if (ex instanceof KmsException kmsEx) {
                    throw new RuntimeException("Failed to create grant: " +
kmsEx.getMessage(), kmsEx);
                } else {
                    throw new RuntimeException("An unexpected error occurred: " +
ex.getMessage(), ex);
                }
            }
        });

        return responseFuture.thenApply(CreateGrantResponse::grantId);
    }
}
```

- For API details, see [CreateGrant](#) in *Amazon SDK for Java 2.x API Reference*.

Kotlin

SDK for Kotlin

Note

There's more on GitHub. Find the complete example and learn how to set up and run in the [Amazon Code Examples Repository](#).

```
suspend fun createNewGrant(
    keyIdVal: String?,
    granteePrincipalVal: String?,
    operation: String,
): String? {
    val operationObj = GrantOperation.fromValue(operation)
    val grantOperationList = ArrayList<GrantOperation>()
    grantOperationList.add(operationObj)


    val request =
        CreateGrantRequest {
            keyId = keyIdVal
            granteePrincipal = granteePrincipalVal
            operations = grantOperationList
        }

    KmsClient { region = "us-west-2" }.use { kmsClient ->
        val response = kmsClient.createGrant(request)
        return response.grantId
    }
}
```

- For API details, see [CreateGrant](#) in *Amazon SDK for Kotlin API reference*.

PHP

SDK for PHP

 **Note**

There's more on GitHub. Find the complete example and learn how to set up and run in the [Amazon Code Examples Repository](#).

```
/**
 * @param string $keyId
 * @param string $granteePrincipal
 * @param array $operations
 * @param array $grantTokens
 * @return Result
 */
public function createGrant(string $keyId, string $granteePrincipal, array
$operations, array $grantTokens = [])
{
    $args = [
        'KeyId' => $keyId,
        'GranteePrincipal' => $granteePrincipal,
        'Operations' => $operations,
    ];
    if($grantTokens){
        $args['GrantTokens'] = $grantTokens;
    }
    try{
        return $this->client->createGrant($args);
    }catch(KmsException $caught){
        if($caught->getAwsErrorMessage() == "InvalidGrantTokenException"){
            echo "The request was rejected because the specified grant token
is not valid.\n";
        }
        throw $caught;
    }
}
```

- For API details, see [CreateGrant](#) in *Amazon SDK for PHP API Reference*.

Python

SDK for Python (Boto3)

Note

There's more on GitHub. Find the complete example and learn how to set up and run in the [Amazon Code Examples Repository](#).

```
class GrantManager:
    def __init__(self, kms_client):
        self.kms_client = kms_client

    @classmethod
    def from_client(cls) -> "GrantManager":
        """
        Creates a GrantManager instance with a default KMS client.

        :return: An instance of GrantManager initialized with the default KMS
client.
        """
        kms_client = boto3.client("kms")
        return cls(kms_client)

    def create_grant(
        self, key_id: str, principal: str, operations: [str]
    ) -> dict[str, str]:
        """
        Creates a grant for a key that lets a principal generate a symmetric data
encryption key.

        :param key_id: The ARN or ID of the key.
        :param principal: The principal to grant permission to.
        :param operations: The operations to grant permission for.
        :return: The grant that is created.
        """
        try:
            return self.kms_client.create_grant(
```

```
        KeyId=key_id,
        GranteePrincipal=principal,
        Operations=operations,
    )
except ClientError as err:
    logger.error(
        "Couldn't create a grant on key %s. Here's why: %s",
        key_id,
        err.response["Error"]["Message"],
    )
    raise
```

- For API details, see [CreateGrant](#) in *Amazon SDK for Python (Boto3) API Reference*.

For a complete list of Amazon SDK developer guides and code examples, see [Using this service with an Amazon SDK](#). This topic also includes information about getting started and details about previous SDK versions.

Use CreateKey with an Amazon SDK or CLI

The following code examples show how to use CreateKey.

Action examples are code excerpts from larger programs and must be run in context. You can see this action in context in the following code example:

- [Learn the basics](#)

.NET

Amazon SDK for .NET

Note

There's more on GitHub. Find the complete example and learn how to set up and run in the [Amazon Code Examples Repository](#).

```
using System;
```

```
using System.Threading.Tasks;
using Amazon.KeyManagementService;
using Amazon.KeyManagementService.Model;

/// <summary>
/// Shows how to create a new AWS Key Management Service (AWS KMS)
/// key.
/// </summary>
public class CreateKey
{
    public static async Task Main()
    {
        // Note that if you need to create a Key in an AWS Region
        // other than the Region defined for the default user, you need to
        // pass the Region to the client constructor.
        var client = new AmazonKeyManagementServiceClient();

        // The call to CreateKeyAsync will create a symmetrical AWS KMS
        // key. For more information about symmetrical and asymmetrical
        // keys, see:
        //
        // https://docs.aws.amazon.com/kms/latest/developerguide/symm-asymm-
choose.html
        var response = await client.CreateKeyAsync(new CreateKeyRequest());

        // The KeyMetadata object contains information about the new AWS KMS
key.
        KeyMetadata keyMetadata = response.KeyMetadata;

        if (keyMetadata is not null)
        {
            Console.WriteLine($"KMS Key: {keyMetadata.KeyId} was successfully
created.");
        }
        else
        {
            Console.WriteLine("Could not create KMS Key.");
        }
    }
}
```

- For API details, see [CreateKey](#) in *Amazon SDK for .NET API Reference*.

CLI

Amazon CLI

Example 1: To create a customer managed KMS key in Amazon KMS

The following `create-key` example creates a symmetric encryption KMS key.

To create the basic KMS key, a symmetric encryption key, you do not need to specify any parameters. The default values for those parameters create a symmetric encryption key.

Because this command doesn't specify a key policy, the KMS key gets the [default key policy](#) for programmatically created KMS keys. To view the key policy, use the `get-key-policy` command. To change the key policy, use the `put-key-policy` command.

```
aws kms create-key
```

The `create-key` command returns the key metadata, including the key ID and ARN of the new KMS key. You can use these values to identify the KMS key in other Amazon KMS operations. The output does not include the tags. To view the tags for a KMS key, use the `list-resource-tags` command.

Output:

```
{
  "KeyMetadata": {
    "AWSAccountId": "111122223333",
    "Arn": "arn:aws:kms:us-west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab",
    "CreationDate": "2017-07-05T14:04:55-07:00",
    "CustomerMasterKeySpec": "SYMMETRIC_DEFAULT",
    "Description": "",
    "Enabled": true,
    "KeyId": "1234abcd-12ab-34cd-56ef-1234567890ab",
    "KeyManager": "CUSTOMER",
    "KeySpec": "SYMMETRIC_DEFAULT",
    "KeyState": "Enabled",
    "KeyUsage": "ENCRYPT_DECRYPT",
    "MultiRegion": false,
    "Origin": "AWS_KMS"
    "EncryptionAlgorithms": [
      "SYMMETRIC_DEFAULT"
    ]
  }
}
```

```
}  
}
```

Note: The `create-key` command does not let you specify an alias. To create an alias for the new KMS key, use the `create-alias` command.

For more information, see [Creating keys](#) in the *Amazon Key Management Service Developer Guide*.

Example 2: To create an asymmetric RSA KMS key for encryption and decryption

The following `create-key` example creates a KMS key that contains an asymmetric RSA key pair for encryption and decryption.

```
aws kms create-key \  
  --key-spec RSA_4096 \  
  --key-usage ENCRYPT_DECRYPT
```

Output:

```
{  
  "KeyMetadata": {  
    "Arn": "arn:aws:kms:us-  
east-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab",  
    "AWSAccountId": "111122223333",  
    "CreationDate": "2021-04-05T14:04:55-07:00",  
    "CustomerMasterKeySpec": "RSA_4096",  
    "Description": "",  
    "Enabled": true,  
    "EncryptionAlgorithms": [  
      "RSAES_OAEP_SHA_1",  
      "RSAES_OAEP_SHA_256"  
    ],  
    "KeyId": "1234abcd-12ab-34cd-56ef-1234567890ab",  
    "KeyManager": "CUSTOMER",  
    "KeySpec": "RSA_4096",  
    "KeyState": "Enabled",  
    "KeyUsage": "ENCRYPT_DECRYPT",  
    "MultiRegion": false,  
    "Origin": "AWS_KMS"  
  }  
}
```

For more information, see [Asymmetric keys in Amazon KMS](#) in the *Amazon Key Management Service Developer Guide*.

Example 3: To create an asymmetric elliptic curve KMS key for signing and verification

To create an asymmetric KMS key that contains an asymmetric elliptic curve (ECC) key pair for signing and verification. The `--key-usage` parameter is required even though `SIGN_VERIFY` is the only valid value for ECC KMS keys.

```
aws kms create-key \  
  --key-spec ECC_NIST_P521 \  
  --key-usage SIGN_VERIFY
```

Output:

```
{  
  "KeyMetadata": {  
    "Arn": "arn:aws:kms:us-  
east-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab",  
    "AWSAccountId": "111122223333",  
    "CreationDate": "2019-12-02T07:48:55-07:00",  
    "CustomerMasterKeySpec": "ECC_NIST_P521",  
    "Description": "",  
    "Enabled": true,  
    "KeyId": "1234abcd-12ab-34cd-56ef-1234567890ab",  
    "KeyManager": "CUSTOMER",  
    "KeySpec": "ECC_NIST_P521",  
    "KeyState": "Enabled",  
    "KeyUsage": "SIGN_VERIFY",  
    "MultiRegion": false,  
    "Origin": "AWS_KMS",  
    "SigningAlgorithms": [  
      "ECDSA_SHA_512"  
    ]  
  }  
}
```

For more information, see [Asymmetric keys in Amazon KMS](#) in the *Amazon Key Management Service Developer Guide*.

Example 4: To create an HMAC KMS key

The following `create-key` example creates a 384-bit HMAC KMS key. The `GENERATE_VERIFY_MAC` value for the `--key-usage` parameter is required even though it's the only valid value for HMAC KMS keys.

```
aws kms create-key \  
  --key-spec HMAC_384 \  
  --key-usage GENERATE_VERIFY_MAC
```

Output:

```
{  
  "KeyMetadata": {  
    "Arn": "arn:aws:kms:us-  
east-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab",  
    "AWSAccountId": "111122223333",  
    "CreationDate": "2022-04-05T14:04:55-07:00",  
    "CustomerMasterKeySpec": "HMAC_384",  
    "Description": "",  
    "Enabled": true,  
    "KeyId": "1234abcd-12ab-34cd-56ef-1234567890ab",  
    "KeyManager": "CUSTOMER",  
    "KeySpec": "HMAC_384",  
    "KeyState": "Enabled",  
    "KeyUsage": "GENERATE_VERIFY_MAC",  
    "MacAlgorithms": [  
      "HMAC_SHA_384"  
    ],  
    "MultiRegion": false,  
    "Origin": "AWS_KMS"  
  }  
}
```

For more information, see [HMAC keys in Amazon KMS](#) in the *Amazon Key Management Service Developer Guide*.

Example 4: To create a multi-Region primary KMS key

The following `create-key` example creates a multi-Region primary symmetric encryption key. Because the default values for all parameters create a symmetric encryption key, only the `--multi-region` parameter is required for this KMS key. In the Amazon CLI, to indicate that a Boolean parameter is true, just specify the parameter name.

```
aws kms create-key \  
  --multi-region
```

Output:

```
{  
  "KeyMetadata": {  
    "Arn": "arn:aws:kms:us-west-2:111122223333:key/  
mrk-1234abcd12ab34cd56ef12345678990ab",  
    "AWSAccountId": "111122223333",  
    "CreationDate": "2021-09-02T016:15:21-09:00",  
    "CustomerMasterKeySpec": "SYMMETRIC_DEFAULT",  
    "Description": "",  
    "Enabled": true,  
    "EncryptionAlgorithms": [  
      "SYMMETRIC_DEFAULT"  
    ],  
    "KeyId": "mrk-1234abcd12ab34cd56ef12345678990ab",  
    "KeyManager": "CUSTOMER",  
    "KeySpec": "SYMMETRIC_DEFAULT",  
    "KeyState": "Enabled",  
    "KeyUsage": "ENCRYPT_DECRYPT",  
    "MultiRegion": true,  
    "MultiRegionConfiguration": {  
      "MultiRegionKeyType": "PRIMARY",  
      "PrimaryKey": {  
        "Arn": "arn:aws:kms:us-west-2:111122223333:key/  
mrk-1234abcd12ab34cd56ef12345678990ab",  
        "Region": "us-west-2"  
      },  
      "ReplicaKeys": []  
    },  
    "Origin": "AWS_KMS"  
  }  
}
```

For more information, see [Asymmetric keys in Amazon KMS](#) in the *Amazon Key Management Service Developer Guide*.

Example 5: To create a KMS key for imported key material

The following `create-key` example creates a KMS key with no key material. When the operation is complete, you can import your own key material into the KMS key. To create this KMS key, set the `--origin` parameter to `EXTERNAL`.

```
aws kms create-key \  
  --origin EXTERNAL
```

Output:

```
{  
  "KeyMetadata": {  
    "Arn": "arn:aws:kms:us-  
east-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab",  
    "AWSAccountId": "111122223333",  
    "CreationDate": "2019-12-02T07:48:55-07:00",  
    "CustomerMasterKeySpec": "SYMMETRIC_DEFAULT",  
    "Description": "",  
    "Enabled": false,  
    "EncryptionAlgorithms": [  
      "SYMMETRIC_DEFAULT"  
    ],  
    "KeyId": "1234abcd-12ab-34cd-56ef-1234567890ab",  
    "KeyManager": "CUSTOMER",  
    "KeySpec": "SYMMETRIC_DEFAULT",  
    "KeyState": "PendingImport",  
    "KeyUsage": "ENCRYPT_DECRYPT",  
    "MultiRegion": false,  
    "Origin": "EXTERNAL"  
  }  
}
```

For more information, see [Importing key material in Amazon KMS keys](#) in the *Amazon Key Management Service Developer Guide*.

Example 6: To create a KMS key in an Amazon CloudHSM key store

The following `create-key` example creates a KMS key in the specified Amazon CloudHSM key store. The operation creates the KMS key and its metadata in Amazon KMS and creates the key material in the Amazon CloudHSM cluster associated with the custom key store. The `--custom-key-store-id` and `--origin` parameters are required.

```
aws kms create-key \  
  --custom-key-store-id EXAMPLE-KEY-STORE-ID
```

```
--origin AWS_CLOUDHSM \  
--custom-key-store-id cks-1234567890abcdef0
```

Output:

```
{  
  "KeyMetadata": {  
    "Arn": "arn:aws:kms:us-  
east-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab",  
    "AWSAccountId": "111122223333",  
    "CloudHsmClusterId": "cluster-1a23b4cdefg",  
    "CreationDate": "2019-12-02T07:48:55-07:00",  
    "CustomerMasterKeySpec": "SYMMETRIC_DEFAULT",  
    "CustomKeyId": "cks-1234567890abcdef0",  
    "Description": "",  
    "Enabled": true,  
    "EncryptionAlgorithms": [  
      "SYMMETRIC_DEFAULT"  
    ],  
    "KeyId": "1234abcd-12ab-34cd-56ef-1234567890ab",  
    "KeyManager": "CUSTOMER",  
    "KeySpec": "SYMMETRIC_DEFAULT",  
    "KeyState": "Enabled",  
    "KeyUsage": "ENCRYPT_DECRYPT",  
    "MultiRegion": false,  
    "Origin": "AWS_CLOUDHSM"  
  }  
}
```

For more information, see [Amazon CloudHSM key stores](#) in the *Amazon Key Management Service Developer Guide*.

Example 7: To create a KMS key in an external key store

The following create-key example creates a KMS key in the specified external key store. The --custom-key-store-id, --origin, and --xks-key-id parameters are required in this command.

The --xks-key-id parameter specifies the ID of an existing symmetric encryption key in your external key manager. This key serves as the external key material for the KMS key. The value of the --origin parameter must be EXTERNAL_KEY_STORE. The custom-key-

`store-id` parameter must identify an external key store that is connected to its external key store proxy.

```
aws kms create-key \  
  --origin EXTERNAL_KEY_STORE \  
  --custom-key-store-id cks-9876543210fedcba9 \  
  --xks-key-id bb8562717f809024
```

Output:


```
{  
  "KeyMetadata": {  
    "Arn": "arn:aws:kms:us-  
east-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab",  
    "AWSAccountId": "111122223333",  
    "CreationDate": "2022-12-02T07:48:55-07:00",  
    "CustomerMasterKeySpec": "SYMMETRIC_DEFAULT",  
    "CustomKeyId": "cks-9876543210fedcba9",  
    "Description": "",  
    "Enabled": true,  
    "EncryptionAlgorithms": [  
      "SYMMETRIC_DEFAULT"  
    ],  
    "KeyId": "1234abcd-12ab-34cd-56ef-1234567890ab",  
    "KeyManager": "CUSTOMER",  
    "KeySpec": "SYMMETRIC_DEFAULT",  
    "KeyState": "Enabled",  
    "KeyUsage": "ENCRYPT_DECRYPT",  
    "MultiRegion": false,  
    "Origin": "EXTERNAL_KEY_STORE",  
    "XksKeyConfiguration": {  
      "Id": "bb8562717f809024"  
    }  
  }  
}
```

For more information, see [External key stores](#) in the *Amazon Key Management Service Developer Guide*.

- For API details, see [CreateKey](#) in *Amazon CLI Command Reference*.

Java

SDK for Java 2.x

 **Note**

There's more on GitHub. Find the complete example and learn how to set up and run in the [Amazon Code Examples Repository](#).

```
/**
 * Creates a new symmetric encryption key asynchronously.
 *
 * @param keyDesc the description of the key to be created
 * @return a {@link CompletableFuture} that completes with the ID of the
 * newly created key
 * @throws RuntimeException if an error occurs while creating the key
 */
public CompletableFuture<String> createKeyAsync(String keyDesc) {
    CreateKeyRequest keyRequest = CreateKeyRequest.builder()
        .description(keyDesc)
        .keySpec(KeySpec.SYMMETRIC_DEFAULT)
        .keyUsage(KeyUsageType.ENCRYPT_DECRYPT)
        .build();

    return getAsyncClient().createKey(keyRequest)
        .thenApply(resp -> resp.keyMetadata().keyId())
        .exceptionally(ex -> {
            throw new RuntimeException("An error occurred while creating the
key: " + ex.getMessage(), ex);
        });
}
```

- For API details, see [CreateKey](#) in *Amazon SDK for Java 2.x API Reference*.

Kotlin

SDK for Kotlin

Note

There's more on GitHub. Find the complete example and learn how to set up and run in the [Amazon Code Examples Repository](#).

```
suspend fun createKey(keyDesc: String?): String? {
    val request =
        CreateKeyRequest {
            description = keyDesc
            customerMasterKeySpec = CustomerMasterKeySpec.SymmetricDefault
            keyUsage = KeyUsageType.fromValue("ENCRYPT_DECRYPT")
        }

    KmsClient { region = "us-west-2" }.use { kmsClient ->
        val result = kmsClient.createKey(request)
        println("Created a customer key with id " + result.keyMetadata?.arn)
        return result.keyMetadata?.keyId
    }
}
```

- For API details, see [CreateKey](#) in *Amazon SDK for Kotlin API reference*.

PHP

SDK for PHP

Note

There's more on GitHub. Find the complete example and learn how to set up and run in the [Amazon Code Examples Repository](#).

```
/**
```

```

    * @param string $keySpec
    * @param string $keyUsage
    * @param string $description
    * @return array
    */
    public function createKey(string $keySpec = "", string $keyUsage = "", string
    $description = "Created by the SDK for PHP")
    {
        $parameters = ['Description' => $description];
        if($keySpec && $keyUsage){
            $parameters['KeySpec'] = $keySpec;
            $parameters['KeyUsage'] = $keyUsage;
        }
        try {
            $result = $this->client->createKey($parameters);
            return $result['KeyMetadata'];
        }catch(KmsException $caught){
            // Check for error specific to createKey operations
            if ($caught->getAwsErrorMessage() == "LimitExceededException"){
                echo "The request was rejected because a quota was exceeded. For
                more information, see Quotas in the Key Management Service Developer Guide.";
            }
            throw $caught;
        }
    }
}

```

- For API details, see [CreateKey](#) in *Amazon SDK for PHP API Reference*.

Python

SDK for Python (Boto3)

Note

There's more on GitHub. Find the complete example and learn how to set up and run in the [Amazon Code Examples Repository](#).

```

class KeyManager:
    def __init__(self, kms_client):

```

```
        self.kms_client = kms_client
        self.created_keys = []

    @classmethod
    def from_client(cls) -> "KeyManager":
        """
        Creates a KeyManager instance with a default KMS client.

        :return: An instance of KeyManager initialized with the default KMS
client.
        """
        kms_client = boto3.client("kms")
        return cls(kms_client)

    def create_key(self, key_description: str) -> dict[str, any]:
        """
        Creates a key with a user-provided description.

        :param key_description: A description for the key.
        :return: The key ID.
        """
        try:
            key = self.kms_client.create_key(Description=key_description)
["KeyMetadata"]
            self.created_keys.append(key)
            return key
        except ClientError as err:
            logging.error(
                "Couldn't create your key. Here's why: %s",
                err.response["Error"]["Message"],
            )
            raise
```

- For API details, see [CreateKey](#) in *Amazon SDK for Python (Boto3) API Reference*.

Ruby

SDK for Ruby

Note

There's more on GitHub. Find the complete example and learn how to set up and run in the [Amazon Code Examples Repository](#).

```
require 'aws-sdk-kms' # v2: require 'aws-sdk'

# Create a AWS KMS key.
# As long we are only encrypting small amounts of data (4 KiB or less) directly,
# a KMS key is fine for our purposes.
# For larger amounts of data,
# use the KMS key to encrypt a data encryption key (DEK).

client = Aws::KMS::Client.new

resp = client.create_key({
  tags: [
    {
      tag_key: 'CreatedBy',
      tag_value: 'ExampleUser'
    }
  ]
})

puts resp.key_metadata.key_id
```

- For API details, see [CreateKey](#) in *Amazon SDK for Ruby API Reference*.

Rust

SDK for Rust

Note

There's more on GitHub. Find the complete example and learn how to set up and run in the [Amazon Code Examples Repository](#).

```
async fn make_key(client: &Client) -> Result<(), Error> {
    let resp = client.create_key().send().await?;

    let id = resp.key_metadata.as_ref().unwrap().key_id();

    println!("Key: {}", id);

    Ok(())
}
```

- For API details, see [CreateKey](#) in *Amazon SDK for Rust API reference*.

For a complete list of Amazon SDK developer guides and code examples, see [Using this service with an Amazon SDK](#). This topic also includes information about getting started and details about previous SDK versions.

Use Decrypt with an Amazon SDK or CLI

The following code examples show how to use Decrypt.

Action examples are code excerpts from larger programs and must be run in context. You can see this action in context in the following code example:

- [Learn the basics](#)

CLI

Amazon CLI

Example 1: To decrypt an encrypted message with a symmetric KMS key (Linux and macOS)

The following decrypt command example demonstrates the recommended way to decrypt data with the Amazon CLI. This version shows how to decrypt data under a symmetric KMS key.

Provide the ciphertext in a file. In the value of the `--ciphertext-blob` parameter, use the `fileb://` prefix, which tells the CLI to read the data from a binary file. If the file is not in the current directory, type the full path to file. For more information about reading Amazon CLI parameter values from a file, see [Loading Amazon CLI parameters from a file](https://docs.aws.amazon.com/cli/latest/userguide/cli-usage-parameters-file.html) in the *Amazon Command Line Interface User Guide* and [Best Practices for Local File Parameters](https://aws.amazon.com/blogs/developer/best-practices-for-local-file-parameters/) in the *Amazon Command Line Tool Blog*. Specify the KMS key to decrypt the ciphertext. The `--key-id` parameter is not required when decrypting with a symmetric KMS key. Amazon KMS can get the key ID of the KMS key that was used to encrypt the data from the metadata in the ciphertext. But it's always a best practice to specify the KMS key you are using. This practice ensures that you use the KMS key that you intend, and prevents you from inadvertently decrypting a ciphertext using a KMS key you do not trust. Request the plaintext output as a text value. The `--query` parameter tells the CLI to get only the value of the `Plaintext` field from the output. The `--output` parameter returns the output as text. Base64-decode the plaintext and save it in a file. The following example pipes (`|`) the value of the `Plaintext` parameter to the Base64 utility, which decodes it. Then, it redirects (`>`) the decoded output to the `ExamplePlaintext` file.

Before running this command, replace the example key ID with a valid key ID from your Amazon account.

```
aws kms decrypt \  
  --ciphertext-blob fileb://ExampleEncryptedFile \  
  --key-id 1234abcd-12ab-34cd-56ef-1234567890ab \  
  --output text \  
  --query Plaintext | base64 \  
  --decode > ExamplePlaintextFile
```

This command produces no output. The output from the decrypt command is base64-decoded and saved in a file.

For more information, see [Decrypt](#) in the *Amazon Key Management Service API Reference*.

Example 2: To decrypt an encrypted message with a symmetric KMS key (Windows command prompt)

The following example is the same as the previous one except that it uses the `certutil` utility to Base64-decode the plaintext data. This procedure requires two commands, as shown in the following examples.

Before running this command, replace the example key ID with a valid key ID from your Amazon account.

```
aws kms decrypt ^
  --ciphertext-blob fileb://ExampleEncryptedFile ^
  --key-id 1234abcd-12ab-34cd-56ef-1234567890ab ^
  --output text ^
  --query Plaintext > ExamplePlaintextFile.base64
```

Run the `certutil` command.

```
certutil -decode ExamplePlaintextFile.base64 ExamplePlaintextFile
```

Output:

```
Input Length = 18
Output Length = 12
CertUtil: -decode command completed successfully.
```

For more information, see [Decrypt](#) in the *Amazon Key Management Service API Reference*.

Example 3: To decrypt an encrypted message with an asymmetric KMS key (Linux and macOS)

The following `decrypt` command example shows how to decrypt data encrypted under an RSA asymmetric KMS key.

When using an asymmetric KMS key, the `encryption-algorithm` parameter, which specifies the algorithm used to encrypt the plaintext, is required.

Before running this command, replace the example key ID with a valid key ID from your Amazon account.

```
aws kms decrypt \  
  --ciphertext-blob fileb://ExampleEncryptedFile \  
  --key-id 0987dcb-a-09fe-87dc-65ba-ab0987654321 \  
  --encryption-algorithm RSAES_OAEP_SHA_256 \  
  --output text \  
  --query Plaintext | base64 \  
  --decode > ExamplePlaintextFile
```

This command produces no output. The output from the decrypt command is base64-decoded and saved in a file.

For more information, see [Asymmetric keys in Amazon KMS](#) in the *Amazon Key Management Service Developer Guide*.

- For API details, see [Decrypt](#) in *Amazon CLI Command Reference*.

Java

SDK for Java 2.x

Note

There's more on GitHub. Find the complete example and learn how to set up and run in the [Amazon Code Examples Repository](#).

```
/**  
 * Asynchronously decrypts the given encrypted data using the specified key  
 ID.  
 *  
 * @param encryptedData The encrypted data to be decrypted.  
 * @param keyId The ID of the key to be used for decryption.  
 * @return A CompletableFuture that, when completed, will contain the  
 decrypted data as a String.  
 *         If an error occurs during the decryption process, the  
 CompletableFuture will complete  
 *         exceptionally with the error, and the method will return an empty  
 String. */
```

```

    */
    public CompletableFuture<String> decryptDataAsync(SdkBytes encryptedData,
String keyId) {
        DecryptRequest decryptRequest = DecryptRequest.builder()
            .ciphertextBlob(encryptedData)
            .keyId(keyId)
            .build();

        CompletableFuture<DecryptResponse> responseFuture =
getAsyncClient().decrypt(decryptRequest);
        responseFuture.whenComplete((decryptResponse, exception) -> {
            if (exception == null) {
                logger.info("Data decrypted successfully for key ID: " + keyId);
            } else {
                if (exception instanceof KmsException kmsEx) {
                    throw new RuntimeException("KMS error occurred while
decrypting data: " + kmsEx.getMessage(), kmsEx);
                } else {
                    throw new RuntimeException("An unexpected error occurred
while decrypting data: " + exception.getMessage(), exception);
                }
            }
        });

        return responseFuture.thenApply(decryptResponse ->
decryptResponse.plaintext().asString(StandardCharsets.UTF_8));
    }
}

```

- For API details, see [Decrypt](#) in *Amazon SDK for Java 2.x API Reference*.

Kotlin

SDK for Kotlin

Note

There's more on GitHub. Find the complete example and learn how to set up and run in the [Amazon Code Examples Repository](#).

```
suspend fun encryptData(keyIdValue: String): ByteArray? {
```

```
val text = "This is the text to encrypt by using the AWS KMS Service"
val myBytes: ByteArray = text.toByteArray()

val encryptRequest =
    EncryptRequest {
        keyId = keyIdValue
        plaintext = myBytes
    }

KmsClient { region = "us-west-2" }.use { kmsClient ->
    val response = kmsClient.encrypt(encryptRequest)
    val algorithm: String = response.encryptionAlgorithm.toString()
    println("The encryption algorithm is $algorithm")

    // Return the encrypted data.
    return response.ciphertextBlob
}

suspend fun decryptData(
    encryptedDataVal: ByteArray?,
    keyIdVal: String?,
) {
    val decryptRequest =
        DecryptRequest {
            ciphertextBlob = encryptedDataVal
            keyId = keyIdVal
        }
    KmsClient { region = "us-west-2" }.use { kmsClient ->
        val decryptResponse = kmsClient.decrypt(decryptRequest)
        val myVal = decryptResponse.plaintext

        // Print the decrypted data.
        print(myVal)
    }
}
```

- For API details, see [Decrypt](#) in *Amazon SDK for Kotlin API reference*.

PHP

SDK for PHP

 **Note**


There's more on GitHub. Find the complete example and learn how to set up and run in the [Amazon Code Examples Repository](#).

```
/**
 * @param string $keyId
 * @param string $ciphertext
 * @param string $algorithm
 * @return Result
 */
public function decrypt(string $keyId, string $ciphertext, string $algorithm
= "SYMMETRIC_DEFAULT")
{
    try{
        return $this->client->decrypt([
            'CiphertextBlob' => $ciphertext,
            'EncryptionAlgorithm' => $algorithm,
            'KeyId' => $keyId,
        ]);
    }catch(KmsException $caught){
        echo "There was a problem decrypting the data: {$caught-
>getAwsErrorMessage()}\n";
        throw $caught;
    }
}
```

- For API details, see [Decrypt](#) in *Amazon SDK for PHP API Reference*.

Python

SDK for Python (Boto3)

 **Note**

There's more on GitHub. Find the complete example and learn how to set up and run in the [Amazon Code Examples Repository](#).

```
class KeyEncrypt:
    def __init__(self, kms_client):
        self.kms_client = kms_client

    @classmethod
    def from_client(cls) -> "KeyEncrypt":
        """
        Creates a KeyEncrypt instance with a default KMS client.

        :return: An instance of KeyEncrypt initialized with the default KMS
client.
        """
        kms_client = boto3.client("kms")
        return cls(kms_client)

    def decrypt(self, key_id: str, cipher_text: str) -> bytes:
        """
        Decrypts text previously encrypted with a key.

        :param key_id: The ARN or ID of the key used to decrypt the data.
        :param cipher_text: The encrypted text to decrypt.
        :return: The decrypted text.
        """
        try:
            return self.kms_client.decrypt(KeyId=key_id,
CiphertextBlob=cipher_text)[
                "Plaintext"
            ]
        except ClientError as err:
            logger.error(
                "Couldn't decrypt your ciphertext. Here's why: %s",
```

```
        err.response["Error"]["Message"],
    )
    raise
```

- For API details, see [Decrypt](#) in *Amazon SDK for Python (Boto3) API Reference*.

Ruby

SDK for Ruby

Note

There's more on GitHub. Find the complete example and learn how to set up and run in the [Amazon Code Examples Repository](#).

```
require 'aws-sdk-kms' # v2: require 'aws-sdk'

# Decrypted blob

blob =
  '01020200785d68faeec386af1057904926253051eb2919d3c16078badf65b808b26dd057c101747cadf3593'
blob_packed = [blob].pack('H*')

client = Aws::KMS::Client.new(region: 'us-west-2')

resp = client.decrypt({
  ciphertext_blob: blob_packed
})

puts 'Raw text: '
puts resp.plaintext
```

- For API details, see [Decrypt](#) in *Amazon SDK for Ruby API Reference*.

Rust

SDK for Rust

Note

There's more on GitHub. Find the complete example and learn how to set up and run in the [Amazon Code Examples Repository](#).

```
async fn decrypt_key(client: &Client, key: &str, filename: &str) -> Result<(),
Error> {
    // Open input text file and get contents as a string
    // input is a base-64 encoded string, so decode it:
    let data = fs::read_to_string(filename)
        .map(|input| {
            base64::decode(input).expect("Input file does not contain valid base
64 characters.")
        })
        .map(Blob::new);

    let resp = client
        .decrypt()
        .key_id(key)
        .ciphertext_blob(data.unwrap())
        .send()
        .await?;

    let inner = resp.plaintext.unwrap();
    let bytes = inner.as_ref();

    let s = String::from_utf8(bytes.to_vec()).expect("Could not convert to
UTF-8");

    println!();
    println!("Decoded string:");
    println!("{}", s);

    Ok(())
}
```

- For API details, see [Decrypt](#) in *Amazon SDK for Rust API reference*.

For a complete list of Amazon SDK developer guides and code examples, see [Using this service with an Amazon SDK](#). This topic also includes information about getting started and details about previous SDK versions.

Use DeleteAlias with an Amazon SDK or CLI

The following code examples show how to use DeleteAlias.

CLI

Amazon CLI

To delete an Amazon KMS alias

The following delete-alias example deletes the alias alias/example-alias. The alias name must begin with alias/.

```
aws kms delete-alias \  
  --alias-name alias/example-alias
```

This command produces no output. To find the alias, use the list-aliases command.

For more information, see [Deleting an alias](#) in the *Amazon Key Management Service Developer Guide*.

- For API details, see [DeleteAlias](#) in *Amazon CLI Command Reference*.

Java

SDK for Java 2.x

Note

There's more on GitHub. Find the complete example and learn how to set up and run in the [Amazon Code Examples Repository](#).

```
/**  
 * Deletes a specific KMS alias asynchronously. */
```



```

    *
    * @param aliasName the name of the alias to be deleted
    * @return a {@link CompletableFuture} representing the asynchronous
operation of deleting the specified alias
    */
    public CompletableFuture<Void> deleteSpecificAliasAsync(String aliasName) {
        DeleteAliasRequest deleteAliasRequest = DeleteAliasRequest.builder()
            .aliasName(aliasName)
            .build();

        return getAsyncClient().deleteAlias(deleteAliasRequest)
            .thenRun(() -> {
                logger.info("Alias {} has been deleted successfully", aliasName);
            })
            .exceptionally(throwable -> {
                throw new RuntimeException("Failed to delete alias: " +
aliasName, throwable);
            });
    }
}

```

- For API details, see [DeleteAlias](#) in *Amazon SDK for Java 2.x API Reference*.

PHP

SDK for PHP

Note

There's more on GitHub. Find the complete example and learn how to set up and run in the [Amazon Code Examples Repository](#).

```

/**
 * @param string $aliasName
 * @return void
 */
public function deleteAlias(string $aliasName)
{
    try {
        $this->client->deleteAlias([

```

```

        'AliasName' => $aliasName,
    ]);
}catch(KmsException $caught){
    echo "There was a problem deleting the alias: {$caught-
>getAwsErrorMessage()}\n";
    throw $caught;
}
}

```

- For API details, see [DeleteAlias](#) in *Amazon SDK for PHP API Reference*.

Python

SDK for Python (Boto3)

Note

There's more on GitHub. Find the complete example and learn how to set up and run in the [Amazon Code Examples Repository](#).

```

class AliasManager:
    def __init__(self, kms_client):
        self.kms_client = kms_client
        self.created_key = None

    @classmethod
    def from_client(cls) -> "AliasManager":
        """
        Creates an AliasManager instance with a default KMS client.

        :return: An instance of AliasManager initialized with the default KMS
client.
        """
        kms_client = boto3.client("kms")
        return cls(kms_client)

    def delete_alias(self, alias: str) -> None:
        """

```

```
Deletes an alias.

:param alias: The alias to delete.
"""
try:
    self.kms_client.delete_alias(AliasName=alias)
except ClientError as err:
    logger.error(
        "Couldn't delete alias %s. Here's why: %s",
        alias,
        err.response["Error"]["Message"],
    )
    raise
```

- For API details, see [DeleteAlias](#) in *Amazon SDK for Python (Boto3) API Reference*.

For a complete list of Amazon SDK developer guides and code examples, see [Using this service with an Amazon SDK](#). This topic also includes information about getting started and details about previous SDK versions.

Use DescribeKey with an Amazon SDK or CLI

The following code examples show how to use DescribeKey.

Action examples are code excerpts from larger programs and must be run in context. You can see this action in context in the following code example:

- [Learn the basics](#)

.NET

Amazon SDK for .NET

Note

There's more on GitHub. Find the complete example and learn how to set up and run in the [Amazon Code Examples Repository](#).

```
using System;
using System.Threading.Tasks;
using Amazon.KeyManagementService;
using Amazon.KeyManagementService.Model;

/// <summary>
/// Retrieve information about an AWS Key Management Service (AWS KMS) key.
/// You can supply either the key Id or the key Amazon Resource Name (ARN)
/// to the DescribeKeyRequest KeyId property.
/// </summary>
public class DescribeKey
{
    public static async Task Main()
    {
        var keyId = "7c9eccc2-38cb-4c4f-9db3-766ee8dd3ad4";
        var request = new DescribeKeyRequest
        {
            KeyId = keyId,
        };

        var client = new AmazonKeyManagementServiceClient();

        var response = await client.DescribeKeyAsync(request);
        var metadata = response.KeyMetadata;

        Console.WriteLine($"{metadata.KeyId} created on:
{metadata.CreationDate}");
        Console.WriteLine($"State: {metadata.KeyState}");
        Console.WriteLine($"{metadata.Description}");
    }
}
```

- For API details, see [DescribeKey](#) in *Amazon SDK for .NET API Reference*.

CLI

Amazon CLI

Example 1: To find detailed information about a KMS key

The following `describe-key` example gets detailed information about the Amazon managed key for Amazon S3 in the example account and Region. You can use this command to find details about Amazon managed keys and customer managed keys.

To specify the KMS key, use the `key-id` parameter. This example uses an alias name value, but you can use a key ID, key ARN, alias name, or alias ARN in this command.

```
aws kms describe-key \  
  --key-id alias/aws/s3
```

Output:

```
{  
  "KeyMetadata": {  
    "AWSAccountId": "846764612917",  
    "KeyId": "b8a9477d-836c-491f-857e-07937918959b",  
    "Arn": "arn:aws:kms:us-west-2:846764612917:key/  
b8a9477d-836c-491f-857e-07937918959b",  
    "CreationDate": 2017-06-30T21:44:32.140000+00:00,  
    "Enabled": true,  
    "Description": "Default KMS key that protects my S3 objects when no other  
key is defined",  
    "KeyUsage": "ENCRYPT_DECRYPT",  
    "KeyState": "Enabled",  
    "Origin": "AWS_KMS",  
    "KeyManager": "AWS",  
    "CustomerMasterKeySpec": "SYMMETRIC_DEFAULT",  
    "EncryptionAlgorithms": [  
      "SYMMETRIC_DEFAULT"  
    ]  
  }  
}
```

For more information, see [Viewing keys](#) in the *Amazon Key Management Service Developer Guide*.

Example 2: To get details about an RSA asymmetric KMS key

The following `describe-key` example gets detailed information about an asymmetric RSA KMS key used for signing and verification.

```
aws kms describe-key \  
  --key-id alias/aws/s3
```

```
--key-id 1234abcd-12ab-34cd-56ef-1234567890ab
```

Output:

```
{
  "KeyMetadata": {
    "AWSAccountId": "111122223333",
    "KeyId": "1234abcd-12ab-34cd-56ef-1234567890ab",
    "Arn": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab",
    "CreationDate": "2019-12-02T19:47:14.861000+00:00",
    "CustomerMasterKeySpec": "RSA_2048",
    "Enabled": false,
    "Description": "",
    "KeyState": "Disabled",
    "Origin": "AWS_KMS",
    "MultiRegion": false,
    "KeyManager": "CUSTOMER",
    "KeySpec": "RSA_2048",
    "KeyUsage": "SIGN_VERIFY",
    "SigningAlgorithms": [
      "RSASSA_PKCS1_V1_5_SHA_256",
      "RSASSA_PKCS1_V1_5_SHA_384",
      "RSASSA_PKCS1_V1_5_SHA_512",
      "RSASSA_PSS_SHA_256",
      "RSASSA_PSS_SHA_384",
      "RSASSA_PSS_SHA_512"
    ]
  }
}
```

Example 3: To get details about a multi-Region replica key

The following `describe-key` example gets metadata for a multi-Region replica key. This multi-Region key is a symmetric encryption key. The output of a `describe-key` command for any multi-Region key returns information about the primary key and all of its replicas.

```
aws kms describe-key \
  --key-id arn:aws:kms:ap-northeast-1:111122223333:key/  
mrk-1234abcd12ab34cd56ef1234567890ab
```

Output:

```
{
  "KeyMetadata": {
    "MultiRegion": true,
    "AWSAccountId": "111122223333",
    "Arn": "arn:aws:kms:ap-northeast-1:111122223333:key/
mrk-1234abcd12ab34cd56ef1234567890ab",
    "CreationDate": "2021-06-28T21:09:16.114000+00:00",
    "Description": "",
    "Enabled": true,
    "KeyId": "mrk-1234abcd12ab34cd56ef1234567890ab",
    "KeyManager": "CUSTOMER",
    "KeyState": "Enabled",
    "KeyUsage": "ENCRYPT_DECRYPT",
    "Origin": "AWS_KMS",
    "CustomerMasterKeySpec": "SYMMETRIC_DEFAULT",
    "EncryptionAlgorithms": [
      "SYMMETRIC_DEFAULT"
    ],
    "MultiRegionConfiguration": {
      "MultiRegionKeyType": "PRIMARY",
      "PrimaryKey": {
        "Arn": "arn:aws:kms:us-west-2:111122223333:key/
mrk-1234abcd12ab34cd56ef1234567890ab",
        "Region": "us-west-2"
      },
      "ReplicaKeys": [
        {
          "Arn": "arn:aws:kms:eu-west-1:111122223333:key/
mrk-1234abcd12ab34cd56ef1234567890ab",
          "Region": "eu-west-1"
        },
        {
          "Arn": "arn:aws:kms:ap-northeast-1:111122223333:key/
mrk-1234abcd12ab34cd56ef1234567890ab",
          "Region": "ap-northeast-1"
        },
        {
          "Arn": "arn:aws:kms:sa-east-1:111122223333:key/
mrk-1234abcd12ab34cd56ef1234567890ab",
          "Region": "sa-east-1"
        }
      ]
    }
  }
}
```

```
}  
}
```

Example 4: To get details about an HMAC KMS key

The following describe-key example gets detailed information about an HMAC KMS key.

```
aws kms describe-key \  
  --key-id 1234abcd-12ab-34cd-56ef-1234567890ab
```


Output:

```
{  
  "KeyMetadata": {  
    "AWSAccountId": "123456789012",  
    "KeyId": "1234abcd-12ab-34cd-56ef-1234567890ab",  
    "Arn": "arn:aws:kms:us-  
west-2:123456789012:key/1234abcd-12ab-34cd-56ef-1234567890ab",  
    "CreationDate": "2022-04-03T22:23:10.194000+00:00",  
    "Enabled": true,  
    "Description": "Test key",  
    "KeyUsage": "GENERATE_VERIFY_MAC",  
    "KeyState": "Enabled",  
    "Origin": "AWS_KMS",  
    "KeyManager": "CUSTOMER",  
    "CustomerMasterKeySpec": "HMAC_256",  
    "MacAlgorithms": [  
      "HMAC_SHA_256"  
    ],  
    "MultiRegion": false  
  }  
}
```

- For API details, see [DescribeKey](#) in *Amazon CLI Command Reference*.

Java

SDK for Java 2.x

 **Note**

There's more on GitHub. Find the complete example and learn how to set up and run in the [Amazon Code Examples Repository](#).

```
/**
 * Asynchronously checks if a specified key is enabled.
 *
 * @param keyId the ID of the key to check
 * @return a {@link CompletableFuture} that, when completed, indicates
whether the key is enabled or not
 *
 * @throws RuntimeException if an exception occurs while checking the key
state
 */
public CompletableFuture<Boolean> isKeyEnabledAsync(String keyId) {
    DescribeKeyRequest keyRequest = DescribeKeyRequest.builder()
        .keyId(keyId)
        .build();

    CompletableFuture<DescribeKeyResponse> responseFuture =
getAsyncClient().describeKey(keyRequest);
    return responseFuture.whenComplete((resp, ex) -> {
        if (resp != null) {
            KeyState keyState = resp.keyMetadata().keyState();
            if (keyState == KeyState.ENABLED) {
                logger.info("The key is enabled.");
            } else {
                logger.info("The key is not enabled. Key state: {}",
keyState);
            }
        } else {
            throw new RuntimeException(ex);
        }
    }).thenApply(resp -> resp.keyMetadata().keyState() == KeyState.ENABLED);
}
```

- For API details, see [DescribeKey](#) in *Amazon SDK for Java 2.x API Reference*.

Kotlin

SDK for Kotlin

Note

There's more on GitHub. Find the complete example and learn how to set up and run in the [Amazon Code Examples Repository](#).

```
suspend fun describeSpecifcKey(keyIdVal: String?) {
    val request =
        DescribeKeyRequest {
            keyId = keyIdVal
        }

    KmsClient { region = "us-west-2" }.use { kmsClient ->
        val response = kmsClient.describeKey(request)
        println("The key description is ${response.keyMetadata?.description}")
        println("The key ARN is ${response.keyMetadata?.arn}")
    }
}
```

- For API details, see [DescribeKey](#) in *Amazon SDK for Kotlin API reference*.

PHP

SDK for PHP

Note

There's more on GitHub. Find the complete example and learn how to set up and run in the [Amazon Code Examples Repository](#).

```
/**
 * @param string $keyId
 * @return array
 */
public function describeKey(string $keyId)
{
    try {
        $result = $this->client->describeKey([
            "KeyId" => $keyId,
        ]);
        return $result['KeyMetadata'];
    } catch (KmsException $caught){
        if($caught->getAwsErrorMessage() == "NotFoundException"){
            echo "The request was rejected because the specified entity or
resource could not be found.\n";
        }
        throw $caught;
    }
}
```

- For API details, see [DescribeKey](#) in *Amazon SDK for PHP API Reference*.

Python

SDK for Python (Boto3)

Note

There's more on GitHub. Find the complete example and learn how to set up and run in the [Amazon Code Examples Repository](#).

```
class KeyManager:
    def __init__(self, kms_client):
        self.kms_client = kms_client
        self.created_keys = []

    @classmethod
    def from_client(cls) -> "KeyManager":
        """
```

```
Creates a KeyManager instance with a default KMS client.

:return: An instance of KeyManager initialized with the default KMS
client.
"""
kms_client = boto3.client("kms")
return cls(kms_client)

def describe_key(self, key_id: str) -> dict[str, any]:
    """
    Describes a key.

    :param key_id: The ARN or ID of the key to describe.
    :return: Information about the key.
    """

    try:
        key = self.kms_client.describe_key(KeyId=key_id)["KeyMetadata"]
        return key
    except ClientError as err:
        logging.error(
            "Couldn't get key '%s'. Here's why: %s",
            key_id,
            err.response["Error"]["Message"],
        )
        raise
```

- For API details, see [DescribeKey](#) in *Amazon SDK for Python (Boto3) API Reference*.

For a complete list of Amazon SDK developer guides and code examples, see [Using this service with an Amazon SDK](#). This topic also includes information about getting started and details about previous SDK versions.

Use DisableKey with an Amazon SDK or CLI

The following code examples show how to use DisableKey.

Action examples are code excerpts from larger programs and must be run in context. You can see this action in context in the following code example:

- [Learn the basics](#)

.NET

Amazon SDK for .NET

Note

There's more on GitHub. Find the complete example and learn how to set up and run in the [Amazon Code Examples Repository](#).

```
using System;
using System.Threading.Tasks;
using Amazon.KeyManagementService;
using Amazon.KeyManagementService.Model;

/// <summary>
/// Disable an AWS Key Management Service (AWS KMS) key and then retrieve
/// the key's status to show that it has been disabled.
/// </summary>
public class DisableKey
{
    public static async Task Main()
    {
        var client = new AmazonKeyManagementServiceClient();

        // The identifier of the AWS KMS key to disable. You can use the
        // key Id or the Amazon Resource Name (ARN) of the AWS KMS key.
        var keyId = "1234abcd-12ab-34cd-56ef-1234567890ab";

        var request = new DisableKeyRequest
        {
            KeyId = keyId,
        };

        var response = await client.DisableKeyAsync(request);

        if (response.HttpStatusCode == System.Net.HttpStatusCode.OK)
        {
            // Retrieve information about the key to show that it has now
            // been disabled.
        }
    }
}
```

```
        var describeResponse = await client.DescribeKeyAsync(new
DescribeKeyRequest
        {
            KeyId = keyId,
        });
        Console.WriteLine($"{describeResponse.KeyMetadata.KeyId} - state:
{describeResponse.KeyMetadata.KeyState}");
    }
}
}
```

- For API details, see [DisableKey](#) in *Amazon SDK for .NET API Reference*.

CLI

Amazon CLI

To temporarily disable a KMS key

The following example uses the `disable-key` command to disable a customer managed KMS key. To re-enable the KMS key, use the `enable-key` command.

```
aws kms disable-key \
  --key-id 1234abcd-12ab-34cd-56ef-1234567890ab
```


This command produces no output.

For more information, see [Enabling and Disabling Keys](#) in the *Amazon Key Management Service Developer Guide*.

- For API details, see [DisableKey](#) in *Amazon CLI Command Reference*.

Java

SDK for Java 2.x

 **Note**

There's more on GitHub. Find the complete example and learn how to set up and run in the [Amazon Code Examples Repository](#).

```
/**
 * Asynchronously disables the specified AWS Key Management Service (KMS)
 * key.
 *
 * @param keyId the ID or Amazon Resource Name (ARN) of the KMS key to be
 * disabled
 * @return a CompletableFuture that, when completed, indicates that the key
 * has been disabled successfully
 */
public CompletableFuture<Void> disableKeyAsync(String keyId) {
    DisableKeyRequest keyRequest = DisableKeyRequest.builder()
        .keyId(keyId)
        .build();

    return getAsyncClient().disableKey(keyRequest)
        .thenRun(() -> {
            logger.info("Key {} has been disabled successfully",keyId);
        })
        .exceptionally(throwable -> {
            throw new RuntimeException("Failed to disable key: " + keyId,
throwable);
        });
}
```

- For API details, see [DisableKey](#) in *Amazon SDK for Java 2.x API Reference*.

Kotlin

SDK for Kotlin

Note

There's more on GitHub. Find the complete example and learn how to set up and run in the [Amazon Code Examples Repository](#).

```
suspend fun disableKey(keyIdVal: String?) {
    val request =
        DisableKeyRequest {
            keyId = keyIdVal
        }

    KmsClient { region = "us-west-2" }.use { kmsClient ->
        kmsClient.disableKey(request)
        println("$keyIdVal was successfully disabled")
    }
}
```

- For API details, see [DisableKey](#) in *Amazon SDK for Kotlin API reference*.

PHP

SDK for PHP

Note

There's more on GitHub. Find the complete example and learn how to set up and run in the [Amazon Code Examples Repository](#).

```
/**
 * @param string $keyId
 * @return void
 */
```



```
public function disableKey(string $keyId)
{
    try {
        $this->client->disableKey([
            'KeyId' => $keyId,
        ]);
    } catch (KmsException $caught){
        echo "There was a problem disabling the key: {$caught-
>getAwsErrorMessage()}\n";
        throw $caught;
    }
}
```

- For API details, see [DisableKey](#) in *Amazon SDK for PHP API Reference*.

Python

SDK for Python (Boto3)

Note

There's more on GitHub. Find the complete example and learn how to set up and run in the [Amazon Code Examples Repository](#).

```
class KeyManager:
    def __init__(self, kms_client):
        self.kms_client = kms_client
        self.created_keys = []

    @classmethod
    def from_client(cls) -> "KeyManager":
        """
        Creates a KeyManager instance with a default KMS client.

        :return: An instance of KeyManager initialized with the default KMS
        client.
        """
        kms_client = boto3.client("kms")
        return cls(kms_client)
```

```
def disable_key(self, key_id: str) -> None:
    try:
        self.kms_client.disable_key(KeyId=key_id)
    except ClientError as err:
        logging.error(
            "Couldn't disable key '%s'. Here's why: %s",
            key_id,
            err.response["Error"]["Message"],
        )
        raise
```

- For API details, see [DisableKey](#) in *Amazon SDK for Python (Boto3) API Reference*.

For a complete list of Amazon SDK developer guides and code examples, see [Using this service with an Amazon SDK](#). This topic also includes information about getting started and details about previous SDK versions.

Use EnableKey with an Amazon SDK or CLI

The following code examples show how to use EnableKey.

Action examples are code excerpts from larger programs and must be run in context. You can see this action in context in the following code example:

- [Learn the basics](#)

.NET

Amazon SDK for .NET

Note

There's more on GitHub. Find the complete example and learn how to set up and run in the [Amazon Code Examples Repository](#).

```
using System;
using System.Threading.Tasks;
using Amazon.KeyManagementService;
using Amazon.KeyManagementService.Model;

/// <summary>
/// Enable an AWS Key Management Service (AWS KMS) key.
/// </summary>
public class EnableKey
{
    public static async Task Main()
    {
        var client = new AmazonKeyManagementServiceClient();

        // The identifier of the AWS KMS key to enable. You can use the
        // key Id or the Amazon Resource Name (ARN) of the AWS KMS key.
        var keyId = "1234abcd-12ab-34cd-56ef-1234567890ab";

        var request = new EnableKeyRequest
        {
            KeyId = keyId,
        };

        var response = await client.EnableKeyAsync(request);
        if (response.HttpStatusCode == System.Net.HttpStatusCode.OK)
        {
            // Retrieve information about the key to show that it has now
            // been enabled.
            var describeResponse = await client.DescribeKeyAsync(new
DescribeKeyRequest
            {
                KeyId = keyId,
            });
            Console.WriteLine($"{describeResponse.KeyMetadata.KeyId} - state:
{describeResponse.KeyMetadata.KeyState}");
        }
    }
}
```

- For API details, see [EnableKey](#) in *Amazon SDK for .NET API Reference*.

CLI

Amazon CLI**To enable a KMS key**

The following `enable-key` example enables a customer managed key. You can use a command like this one to enable a KMS key that you temporarily disabled by using the `disable-key` command. You can also use it to enable a KMS key that is disabled because it was scheduled for deletion and the deletion was canceled.

To specify the KMS key, use the `key-id` parameter. This example uses an key ID value, but you can use a key ID or key ARN value in this command.

Before running this command, replace the example key ID with a valid one.

```
aws kms enable-key \  
  --key-id 1234abcd-12ab-34cd-56ef-1234567890ab
```

This command produces no output. To verify that the KMS key is enabled, use the `describe-key` command. See the values of the `KeyState` and `Enabled` fields in the `describe-key` output.

For more information, see [Enabling and Disabling Keys](#) in the *Amazon Key Management Service Developer Guide*.

- For API details, see [EnableKey](#) in *Amazon CLI Command Reference*.

Java

SDK for Java 2.x **Note**

There's more on GitHub. Find the complete example and learn how to set up and run in the [Amazon Code Examples Repository](#).

```
/**  
 * Asynchronously enables the specified key.  
 */
```

```
    * @param keyId the ID of the key to enable
    * @return a {@link CompletableFuture} that completes when the key has been
    enabled
    */
    public CompletableFuture<Void> enableKeyAsync(String keyId) {
        EnableKeyRequest enableKeyRequest = EnableKeyRequest.builder()
            .keyId(keyId)
            .build();

        CompletableFuture<EnableKeyResponse> responseFuture =
            getAsyncClient().enableKey(enableKeyRequest);
        responseFuture.whenComplete((response, exception) -> {
            if (exception == null) {
                logger.info("Key with ID [{}] has been enabled.", keyId);
            } else {
                if (exception instanceof KmsException kmsEx) {
                    throw new RuntimeException("KMS error occurred while enabling
key: " + kmsEx.getMessage(), kmsEx);
                } else {
                    throw new RuntimeException("An unexpected error occurred
while enabling key: " + exception.getMessage(), exception);
                }
            }
        });

        return responseFuture.thenApply(response -> null);
    }
}
```

- For API details, see [EnableKey](#) in *Amazon SDK for Java 2.x API Reference*.

Kotlin

SDK for Kotlin

Note

There's more on GitHub. Find the complete example and learn how to set up and run in the [Amazon Code Examples Repository](#).

```
suspend fun enableKey(keyIdVal: String?) {
```

```
val request =
    EnableKeyRequest {
        keyId = keyIdVal
    }

KmsClient { region = "us-west-2" }.use { kmsClient ->
    kmsClient.enableKey(request)
    println("$keyIdVal was successfully enabled.")
}
}
```

- For API details, see [EnableKey](#) in *Amazon SDK for Kotlin API reference*.

PHP

SDK for PHP

Note

There's more on GitHub. Find the complete example and learn how to set up and run in the [Amazon Code Examples Repository](#).

```
/**
 * @param string $keyId
 * @return void
 */
public function enableKey(string $keyId)
{
    try {
        $this->client->enableKey([
            'KeyId' => $keyId,
        ]);
    } catch (KmsException $caught){
        if($caught->getAwsErrorMessage() == "NotFoundException"){
            echo "The request was rejected because the specified entity or
resource could not be found.\n";
        }
        throw $caught;
    }
}
```

```
}
```

- For API details, see [EnableKey](#) in *Amazon SDK for PHP API Reference*.

Python

SDK for Python (Boto3)

Note

There's more on GitHub. Find the complete example and learn how to set up and run in the [Amazon Code Examples Repository](#).

```
class KeyManager:
    def __init__(self, kms_client):
        self.kms_client = kms_client
        self.created_keys = []

    @classmethod
    def from_client(cls) -> "KeyManager":
        """
        Creates a KeyManager instance with a default KMS client.

        :return: An instance of KeyManager initialized with the default KMS
client.
        """
        kms_client = boto3.client("kms")
        return cls(kms_client)

    def enable_key(self, key_id: str) -> None:
        """
        Enables a key. Gets the key state after each state change.

        :param key_id: The ARN or ID of the key to enable.
        """
        try:
            self.kms_client.enable_key(KeyId=key_id)
        except ClientError as err:
```

```
logging.error(  
    "Couldn't enable key '%s'. Here's why: %s",  
    key_id,  
    err.response["Error"]["Message"],  
)  
raise
```

- For API details, see [EnableKey](#) in *Amazon SDK for Python (Boto3) API Reference*.

For a complete list of Amazon SDK developer guides and code examples, see [Using this service with an Amazon SDK](#). This topic also includes information about getting started and details about previous SDK versions.

Use EnableKeyRotation with an Amazon SDK or CLI

The following code examples show how to use EnableKeyRotation.

CLI

Amazon CLI

To enable automatic rotation of a KMS key

The following `enable-key-rotation` example enables automatic rotation of a customer managed KMS key with a rotation period of 180 days. The KMS key will be rotated one year (approximate 365 days) from the date that this command completes and every year thereafter.

The `--key-id` parameter identifies the KMS key. This example uses a key ARN value, but you can use either the key ID or the ARN of the KMS key. The `--rotation-period-in-days` parameter specifies the number of days between each rotation date. Specify a value between 90 and 2560 days. If no value is specified, the default value is 365 days.

```
aws kms enable-key-rotation \  
    --key-id arn:aws:kms:us-  
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab \  
    --rotation-period-in-days 180
```


This command produces no output. To verify that the KMS key is enabled, use the `get-key-rotation-status` command.

For more information, see [Rotating keys](#) in the *Amazon Key Management Service Developer Guide*.

- For API details, see [EnableKeyRotation](#) in *Amazon CLI Command Reference*.

Python

SDK for Python (Boto3)

Note

There's more on GitHub. Find the complete example and learn how to set up and run in the [Amazon Code Examples Repository](#).

```
class KeyManager:
    def __init__(self, kms_client):
        self.kms_client = kms_client
        self.created_keys = []

    @classmethod
    def from_client(cls) -> "KeyManager":
        """
        Creates a KeyManager instance with a default KMS client.

        :return: An instance of KeyManager initialized with the default KMS
        client.
        """
        kms_client = boto3.client("kms")
        return cls(kms_client)

    def enable_key_rotation(self, key_id: str) -> None:
        """
        Enables rotation for a key.

        :param key_id: The ARN or ID of the key to enable rotation for.
        """
        try:
```

```
        self.kms_client.enable_key_rotation(KeyId=key_id)
    except ClientError as err:
        logging.error(
            "Couldn't enable rotation for key '%s'. Here's why: %s",
            key_id,
            err.response["Error"]["Message"],
        )
        raise
```

- For API details, see [EnableKeyRotation](#) in *Amazon SDK for Python (Boto3) API Reference*.

For a complete list of Amazon SDK developer guides and code examples, see [Using this service with an Amazon SDK](#). This topic also includes information about getting started and details about previous SDK versions.

Use Encrypt with an Amazon SDK or CLI

The following code examples show how to use Encrypt.

Action examples are code excerpts from larger programs and must be run in context. You can see this action in context in the following code example:

- [Learn the basics](#)

CLI

Amazon CLI

Example 1: To encrypt the contents of a file on Linux or MacOS

The following encrypt command demonstrates the recommended way to encrypt data with the Amazon CLI.

```
aws kms encrypt \  
  --key-id 1234abcd-12ab-34cd-56ef-1234567890ab \  
  --plaintext fileb://ExamplePlaintextFile \  
  --output text \  
  --query CiphertextBlob | base64 \  
  --decode > ExampleEncryptedFile
```

The command does several things:

Uses the `--plaintext` parameter to indicate the data to encrypt. This parameter value must be base64-encoded. The value of the `plaintext` parameter must be base64-encoded, or you must use the `fileb://` prefix, which tells the Amazon CLI to read binary data from the file. If the file is not in the current directory, type the full path to file. For example: `fileb:///var/tmp/ExamplePlaintextFile` or `fileb://C:\Temp\ExamplePlaintextFile`. For more information about reading Amazon CLI parameter values from a file, see [Loading Parameters from a File](#) in the *Amazon Command Line Interface User Guide* and [Best Practices for Local File Parameters](#) on the Amazon Command Line Tool Blog. Uses the `--output` and `--query` parameters to control the command's output. These parameters extract the encrypted data, called the *ciphertext*, from the command's output. For more information about controlling output, see [Controlling Command Output](#) in the *Amazon Command Line Interface User Guide*. Uses the `base64` utility to decode the extracted output into binary data. The ciphertext that is returned by a successful `encrypt` command is base64-encoded text. You must decode this text before you can use the Amazon CLI to decrypt it. Saves the binary ciphertext to a file. The final part of the command (`> ExampleEncryptedFile`) saves the binary ciphertext to a file to make decryption easier. For an example command that uses the Amazon CLI to decrypt data, see the `decrypt` examples.

Example 2: Using the Amazon CLI to encrypt data on Windows

This example is the same as the previous one, except that it uses the `certutil` tool instead of `base64`. This procedure requires two commands, as shown in the following example.

```
aws kms encrypt \  
  --key-id 1234abcd-12ab-34cd-56ef-1234567890ab \  
  --plaintext fileb://ExamplePlaintextFile \  
  --output text \  
  --query CiphertextBlob > C:\Temp\ExampleEncryptedFile.base64  
  
certutil -decode C:\Temp\ExampleEncryptedFile.base64 C:\Temp\ExampleEncryptedFile
```

Example 3: Encrypting with an asymmetric KMS key

The following `encrypt` command shows how to encrypt plaintext with an asymmetric KMS key. The `--encryption-algorithm` parameter is required. As in all `encrypt` CLI

commands, the `plaintext` parameter must be base64-encoded, or you must use the `fileb://` prefix, which tells the Amazon CLI to read binary data from the file.

```
aws kms encrypt \
  --key-id 1234abcd-12ab-34cd-56ef-1234567890ab \
  --encryption-algorithm RSAES_OAEP_SHA_256 \
  --plaintext fileb://ExamplePlaintextFile \
  --output text \
  --query CiphertextBlob | base64 \
  --decode > ExampleEncryptedFile
```

This command produces no output.

- For API details, see [Encrypt](#) in *Amazon CLI Command Reference*.

Java

SDK for Java 2.x

Note

There's more on GitHub. Find the complete example and learn how to set up and run in the [Amazon Code Examples Repository](#).

```
/**
 * Encrypts the given text asynchronously using the specified KMS client and
 * key ID.
 *
 * @param keyId the ID of the KMS key to use for encryption
 * @param text the text to encrypt
 * @return a CompletableFuture that completes with the encrypted data as an
 * SdkBytes object
 */
public CompletableFuture<SdkBytes> encryptDataAsync(String keyId, String
text) {
    SdkBytes myBytes = SdkBytes.fromUtf8String(text);
    EncryptRequest encryptRequest = EncryptRequest.builder()
        .keyId(keyId)
        .plaintext(myBytes)
        .build();
```

```
CompletableFuture<EncryptResponse> responseFuture =
getAsyncClient().encrypt(encryptRequest).toCompletableFuture();
return responseFuture.whenComplete((response, ex) -> {
    if (response != null) {
        String algorithm = response.encryptionAlgorithm().toString();
        logger.info("The string was encrypted with algorithm {}.\"",
algorithm);
    } else {
        throw new RuntimeException(ex);
    }
}).thenApply(EncryptResponse::ciphertextBlob);
}
```

- For API details, see [Encrypt](#) in *Amazon SDK for Java 2.x API Reference*.

Kotlin

SDK for Kotlin

Note

There's more on GitHub. Find the complete example and learn how to set up and run in the [Amazon Code Examples Repository](#).

```
suspend fun encryptData(keyIdValue: String): ByteArray? {
    val text = "This is the text to encrypt by using the AWS KMS Service"
    val myBytes: ByteArray = text.toByteArray()

    val encryptRequest =
        EncryptRequest {
            keyId = keyIdValue
            plaintext = myBytes
        }

    KmsClient { region = "us-west-2" }.use { kmsClient ->
        val response = kmsClient.encrypt(encryptRequest)
        val algorithm: String = response.encryptionAlgorithm.toString()
        println("The encryption algorithm is $algorithm")
    }
}
```

```
        // Return the encrypted data.
        return response.ciphertextBlob
    }
}

suspend fun decryptData(
    encryptedDataVal: ByteArray?,
    keyIdVal: String?,
) {
    val decryptRequest =
        DecryptRequest {
            ciphertextBlob = encryptedDataVal
            keyId = keyIdVal
        }
    KmsClient { region = "us-west-2" }.use { kmsClient ->
        val decryptResponse = kmsClient.decrypt(decryptRequest)
        val myVal = decryptResponse.plaintext

        // Print the decrypted data.
        print(myVal)
    }
}
```

- For API details, see [Encrypt](#) in *Amazon SDK for Kotlin API reference*.

PHP

SDK for PHP

Note

There's more on GitHub. Find the complete example and learn how to set up and run in the [Amazon Code Examples Repository](#).

```
/**
 * @param string $keyId
 * @param string $text
 * @return Result
 */
```

```
public function encrypt(string $keyId, string $text)
{
    try {
        return $this->client->encrypt([
            'KeyId' => $keyId,
            'Plaintext' => $text,
        ]);
    } catch(KmsException $caught){
        if($caught->getAwsErrorMessage() == "DisabledException"){
            echo "The request was rejected because the specified KMS key is
not enabled.\n";
        }
        throw $caught;
    }
}
```

- For API details, see [Encrypt](#) in *Amazon SDK for PHP API Reference*.

Python

SDK for Python (Boto3)

Note

There's more on GitHub. Find the complete example and learn how to set up and run in the [Amazon Code Examples Repository](#).

```
class KeyEncrypt:
    def __init__(self, kms_client):
        self.kms_client = kms_client

    @classmethod
    def from_client(cls) -> "KeyEncrypt":
        """
        Creates a KeyEncrypt instance with a default KMS client.

        :return: An instance of KeyEncrypt initialized with the default KMS
client.
        """
```

```
kms_client = boto3.client("kms")
return cls(kms_client)

def encrypt(self, key_id: str, text: str) -> str:
    """
    Encrypts text by using the specified key.

    :param key_id: The ARN or ID of the key to use for encryption.
    :param text: The text to encrypt.
    :return: The encrypted version of the text.
    """
    try:
        response = self.kms_client.encrypt(KeyId=key_id,
Plaintext=text.encode())
        print(
            f"The string was encrypted with algorithm
{response['EncryptionAlgorithm']}"
        )
        return response["CiphertextBlob"]
    except ClientError as err:
        if err.response["Error"]["Code"] == "DisabledException":
            logger.error(
                "Could not encrypt because the key %s is disabled.", key_id
            )
        else:
            logger.error(
                "Couldn't encrypt text. Here's why: %s",
                err.response["Error"]["Message"],
            )
        raise
```

- For API details, see [Encrypt](#) in *Amazon SDK for Python (Boto3) API Reference*.

Ruby

SDK for Ruby

Note

There's more on GitHub. Find the complete example and learn how to set up and run in the [Amazon Code Examples Repository](#).

```
require 'aws-sdk-kms' # v2: require 'aws-sdk'

# ARN of the AWS KMS key.
#
# Replace the fictitious key ARN with a valid key ID

keyId = 'arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab'

text = '1234567890'

client = Aws::KMS::Client.new(region: 'us-west-2')

resp = client.encrypt({
    key_id: keyId,
    plaintext: text
})

# Display a readable version of the resulting encrypted blob.
puts 'Blob:'
puts resp.ciphertext_blob.unpack('H*')
```

- For API details, see [Encrypt](#) in *Amazon SDK for Ruby API Reference*.

Rust

SDK for Rust

Note

There's more on GitHub. Find the complete example and learn how to set up and run in the [Amazon Code Examples Repository](#).

```
async fn encrypt_string(
    verbose: bool,
    client: &Client,
    text: &str,
    key: &str,
    out_file: &str,
) -> Result<(), Error> {
    let blob = Blob::new(text.as_bytes());

    let resp = client.encrypt().key_id(key).plaintext(blob).send().await?;

    // Did we get an encrypted blob?
    let blob = resp.ciphertext_blob.expect("Could not get encrypted text");
    let bytes = blob.as_ref();

    let s = base64::encode(bytes);

    let mut ofile = File::create(out_file).expect("unable to create file");
    ofile.write_all(s.as_bytes()).expect("unable to write");

    if verbose {
        println!("Wrote the following to {:?}" , out_file);
        println!("{}", s);
    }

    Ok(())
}
```

- For API details, see [Encrypt](#) in *Amazon SDK for Rust API reference*.

For a complete list of Amazon SDK developer guides and code examples, see [Using this service with an Amazon SDK](#). This topic also includes information about getting started and details about previous SDK versions.

Use `GenerateDataKey` with an Amazon SDK or CLI

The following code examples show how to use `GenerateDataKey`.

CLI

Amazon CLI

Example 1: To generate a 256-bit symmetric data key

The following `generate-data-key` example requests a 256-bit symmetric data key for use outside of Amazon. The command returns a plaintext data key for immediate use and deletion, and a copy of that data key encrypted under the specified KMS key. You can safely store the encrypted data key with the encrypted data.

To request a 256-bit data key, use the `key-spec` parameter with a value of `AES_256`. To request a 128-bit data key, use the `key-spec` parameter with a value of `AES_128`. For all other data key lengths, use the `number-of-bytes` parameter.

The KMS key you specify must be a symmetric encryption KMS key, that is, a KMS key with a key spec value of `SYMMETRIC_DEFAULT`.

```
aws kms generate-data-key \  
  --key-id alias/ExampleAlias \  
  --key-spec AES_256
```

Output:

```
{  
  "Plaintext": "VdzKNHGzUAzJeRBVY+uUmofUGGiDzyB3+i9fVkh3piw=",  
  "KeyId": "arn:aws:kms:us-  
east-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab",  
  "CiphertextBlob":  
  "AQEDA HjRYf5WytIc0C857tFSnBaPn2F8DgfmThbJ1GfR8P3WlwAAAH4wfAYJKoZIHvcNAQcGoG8wbQIBADBoBgl  
+YdhV8MrkBQPeac0ReRVNDt9qleAt+SHgIRF8P0H+7U="
```

The `Plaintext` (plaintext data key) and the `CiphertextBlob` (encrypted data key) are returned in base64-encoded format.

For more information, see [Data keys](https://docs.aws.amazon.com/kms/latest/developerguide/concepts.html#data-keys) <<https://docs.aws.amazon.com/kms/latest/developerguide/concepts.html#data-keys>> in the *Amazon Key Management Service Developer Guide*.

Example 2: To generate a 512-bit symmetric data key

The following `generate-data-key` example requests a 512-bit symmetric data key for encryption and decryption. The command returns a plaintext data key for immediate use and deletion, and a copy of that data key encrypted under the specified KMS key. You can safely store the encrypted data key with the encrypted data.

To request a key length other than 128 or 256 bits, use the `number-of-bytes` parameter. To request a 512-bit data key, the following example uses the `number-of-bytes` parameter with a value of 64 (bytes).

The KMS key you specify must be a symmetric encryption KMS key, that is, a KMS key with a `key spec` value of `SYMMETRIC_DEFAULT`.

NOTE: The values in the output of this example are truncated for display.

```
aws kms generate-data-key \
  --key-id 1234abcd-12ab-34cd-56ef-1234567890ab \
  --number-of-bytes 64
```

Output:

```
{
  "CiphertextBlob": "AQIBAHi6LtupRpdK12aJTzkkK6Fbh0tQkMlQJJH3PdtHvS/y+hAEnX/
QQNmMwDfg2koirNMEc8AAACaDCCAmQGCSqGSiB3DQEHbqCCA1UwggJRAgEAMIICSgYJKoZ...",
  "Plaintext": "ty8Lr0Bk60F07M2Bwt6qbFdNB
+G00ZLtf5MSEb4a13R2UKWGOp06njAwy2n72VRm2m7z/
Pm9Wpbvttz6a4lSo9hgPvKhZ5y6RTm40ovEXiVfBveyX3DQxDzRSwbKDPk/...",
  "KeyId": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab"
}
```

The `Plaintext` (plaintext data key) and `CiphertextBlob` (encrypted data key) are returned in base64-encoded format.

For more information, see Data keys <<https://docs.aws.amazon.com/kms/latest/developerguide/concepts.html#data-keys>> in the *Amazon Key Management Service Developer Guide*.

- For API details, see [GenerateDataKey](#) in *Amazon CLI Command Reference*.

Python

SDK for Python (Boto3)

Note

There's more on GitHub. Find the complete example and learn how to set up and run in the [Amazon Code Examples Repository](#).

```
class KeyManager:
    def __init__(self, kms_client):
        self.kms_client = kms_client
        self.created_keys = []

    @classmethod
    def from_client(cls) -> "KeyManager":
        """
        Creates a KeyManager instance with a default KMS client.

        :return: An instance of KeyManager initialized with the default KMS
        client.
        """
        kms_client = boto3.client("kms")
        return cls(kms_client)

    def generate_data_key(self, key_id):
        """
        Generates a symmetric data key that can be used for client-side
        encryption.
        """
        answer = input(
            f"Do you want to generate a symmetric data key from key {key_id} (y/
n)? "
        )
```

```
if answer.lower() == "y":
    try:
        data_key = self.kms_client.generate_data_key(
            KeyId=key_id, KeySpec="AES_256"
        )
    except ClientError as err:
        logger.error(
            "Couldn't generate a data key for key %s. Here's why: %s",
            key_id,
            err.response["Error"]["Message"],
        )
    else:
        pprint(data_key)
```

- For API details, see [GenerateDataKey](#) in *Amazon SDK for Python (Boto3) API Reference*.

Rust

SDK for Rust

Note

There's more on GitHub. Find the complete example and learn how to set up and run in the [Amazon Code Examples Repository](#).

```
async fn make_key(client: &Client, key: &str) -> Result<(), Error> {
    let resp = client
        .generate_data_key()
        .key_id(key)
        .key_spec(DataKeySpec::Aes256)
        .send()
        .await?;

    // Did we get an encrypted blob?
    let blob = resp.ciphertext_blob.expect("Could not get encrypted text");
    let bytes = blob.as_ref();

    let s = base64::encode(bytes);
```

```
println!();
println!("Data key:");
println!("{}", s);

Ok(())
}
```

- For API details, see [GenerateDataKey](#) in *Amazon SDK for Rust API reference*.

For a complete list of Amazon SDK developer guides and code examples, see [Using this service with an Amazon SDK](#). This topic also includes information about getting started and details about previous SDK versions.

Use `GenerateDataKeyWithoutPlaintext` with an Amazon SDK or CLI

The following code examples show how to use `GenerateDataKeyWithoutPlaintext`.

CLI

Amazon CLI

To generate a 256-bit symmetric data key without a plaintext key

The following `generate-data-key-without-plaintext` example requests an encrypted copy of a 256-bit symmetric data key for use outside of Amazon. You can call Amazon KMS to decrypt the data key when you are ready to use it.

To request a 256-bit data key, use the `key-spec` parameter with a value of `AES_256`. To request a 128-bit data key, use the `key-spec` parameter with a value of `AES_128`. For all other data key lengths, use the `number-of-bytes` parameter.

The KMS key you specify must be a symmetric encryption KMS key, that is, a KMS key with a key spec value of `SYMMETRIC_DEFAULT`.

```
aws kms generate-data-key-without-plaintext \
  --key-id "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab" \
  --key-spec AES_256
```

Output:

```
{
  "CiphertextBlob":
  "AQEDAHjRYf5WytIc0C857tFSnBaPn2F8DgfmThbJlGfR8P3WlwAAAH4wfAYJKoZlIhvcNAQcGoG8wbQIBADBoBgk
  "KeyId": "arn:aws:kms:us-
east-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab"
}
```

The `CiphertextBlob` (encrypted data key) is returned in base64-encoded format.

For more information, see [Data keys](#) in the *Amazon Key Management Service Developer Guide*.

- For API details, see [GenerateDataKeyWithoutPlaintext](#) in *Amazon CLI Command Reference*.

Rust

SDK for Rust

Note

There's more on GitHub. Find the complete example and learn how to set up and run in the [Amazon Code Examples Repository](#).

```
async fn make_key(client: &Client, key: &str) -> Result<(), Error> {
    let resp = client
        .generate_data_key_without_plaintext()
        .key_id(key)
        .key_spec(DataKeySpec::Aes256)
        .send()
        .await?;

    // Did we get an encrypted blob?
    let blob = resp.ciphertext_blob.expect("Could not get encrypted text");
    let bytes = blob.as_ref();

    let s = base64::encode(bytes);

    println!();
    println!("Data key:");
    println!("{}", s);
}
```



```
    Ok(())  
}
```

- For API details, see [GenerateDataKeyWithoutPlaintext](#) in *Amazon SDK for Rust API reference*.

For a complete list of Amazon SDK developer guides and code examples, see [Using this service with an Amazon SDK](#). This topic also includes information about getting started and details about previous SDK versions.

Use GenerateRandom with an Amazon SDK or CLI

The following code examples show how to use GenerateRandom.

CLI

Amazon CLI

Example 1: To generate a 256-bit random byte string (Linux or macOS)

The following generate-random example generates a 256-bit (32-byte), base64-encoded random byte string. The example decodes the byte string and saves it in the random file.

When you run this command, you must use the number-of-bytes parameter to specify the length of the random value in bytes.

You don't specify a KMS key when you run this command. The random byte string is unrelated to any KMS key.

By default, Amazon KMS generates the random number. However, if you specify a custom key store <<https://docs.aws.amazon.com/kms/latest/developerguide/custom-key-store-overview.html>>, the random byte string is generated in the Amazon CloudHSM cluster associated with the custom key store.

This example uses the following parameters and values:

It uses the required --number-of-bytes parameter with a value of 32 to request a 32-byte (256-bit) string. It uses the --output parameter with a value of text to direct the Amazon CLI to return the output as text, instead of JSON. It uses the --query parameter

to extract the value of the `Plaintext` property from the response. It pipes (`|`) the output of the command to the `base64` utility, which decodes the extracted output. It uses the redirection operator (`>`) to save decoded byte string to the `ExampleRandom` file. It uses the redirection operator (`>`) to save the binary ciphertext to a file.

```
aws kms generate-random \  
  --number-of-bytes 32 \  
  --output text \  
  --query Plaintext | base64 --decode > ExampleRandom
```

This command produces no output.

For more information, see [GenerateRandom](#) in the *Amazon Key Management Service API Reference*.

Example 2: To generate a 256-bit random number (Windows Command Prompt)

The following example uses the `generate-random` command to generate a 256-bit (32-byte), base64-encoded random byte string. The example decodes the byte string and saves it in the `random` file. This example is the same as the previous example, except that it uses the `certutil` utility in Windows to base64-decode the random byte string before saving it in a file.

First, generate a base64-encoded random byte string and saves it in a temporary file, `ExampleRandom.base64`.

```
aws kms generate-random \  
  --number-of-bytes 32 \  
  --output text \  
  --query Plaintext > ExampleRandom.base64
```

Because the output of the `generate-random` command is saved in a file, this example produces no output.

Now use the `certutil -decode` command to decode the base64-encoded byte string in the `ExampleRandom.base64` file. Then, it saves the decoded byte string in the `ExampleRandom` file.

```
certutil -decode ExampleRandom.base64 ExampleRandom
```

Output:

```
Input Length = 18
Output Length = 12
CertUtil: -decode command completed successfully.
```

For more information, see [GenerateRandom](#) in the *Amazon Key Management Service API Reference*.

- For API details, see [GenerateRandom](#) in *Amazon CLI Command Reference*.

Rust**SDK for Rust****Note**

There's more on GitHub. Find the complete example and learn how to set up and run in the [Amazon Code Examples Repository](#).

```
async fn make_string(client: &Client, length: i32) -> Result<(), Error> {
    let resp = client
        .generate_random()
        .number_of_bytes(length)
        .send()
        .await?;

    // Did we get an encrypted blob?
    let blob = resp.plaintext.expect("Could not get encrypted text");
    let bytes = blob.as_ref();

    let s = base64::encode(bytes);

    println!();
    println!("Data key:");
    println!("{}", s);

    Ok(())
}
```

- For API details, see [GenerateRandom](#) in *Amazon SDK for Rust API reference*.

For a complete list of Amazon SDK developer guides and code examples, see [Using this service with an Amazon SDK](#). This topic also includes information about getting started and details about previous SDK versions.

Use GetKeyPolicy with an Amazon SDK or CLI

The following code examples show how to use GetKeyPolicy.

Action examples are code excerpts from larger programs and must be run in context. You can see this action in context in the following code example:

- [Learn the basics](#)

CLI

Amazon CLI

To copy a key policy from one KMS key to another KMS key

The following `get-key-policy` example gets the key policy from one KMS key and saves it in a text file. Then, it replaces the policy of a different KMS key using the text file as the policy input.

Because the `--policy` parameter of `put-key-policy` requires a string, you must use the `--output text` option to return the output as a text string instead of JSON.

```
aws kms get-key-policy \
  --policy-name default \
  --key-id 1234abcd-12ab-34cd-56ef-1234567890ab \
  --query Policy \
  --output text > policy.txt

aws kms put-key-policy \
  --policy-name default \
  --key-id 0987dcba-09fe-87dc-65ba-ab0987654321 \
  --policy file://policy.txt
```

This command produces no output.

For more information, see [PutKeyPolicy](#) in the *Amazon KMS API Reference*.

- For API details, see [GetKeyPolicy](#) in *Amazon CLI Command Reference*.

Python

SDK for Python (Boto3)

Note

There's more on GitHub. Find the complete example and learn how to set up and run in the [Amazon Code Examples Repository](#).

```
class KeyPolicy:
    def __init__(self, kms_client):
        self.kms_client = kms_client

    @classmethod
    def from_client(cls) -> "KeyPolicy":
        """
        Creates a KeyPolicy instance with a default KMS client.

        :return: An instance of KeyPolicy initialized with the default KMS
        client.
        """
        kms_client = boto3.client("kms")
        return cls(kms_client)

    def get_policy(self, key_id: str) -> dict[str, str]:
        """
        Gets the policy of a key.

        :param key_id: The ARN or ID of the key to query.
        :return: The key policy as a dict.
        """
        if key_id != "":
            try:
                response = self.kms_client.get_key_policy(
                    KeyId=key_id,
                )
```

```
        policy = json.loads(response["Policy"])
    except ClientError as err:
        logger.error(
            "Couldn't get policy for key %s. Here's why: %s",
            key_id,
            err.response["Error"]["Message"],
        )
        raise
    else:
        pprint(policy)
        return policy
else:
    print("Skipping get policy demo.")
```

- For API details, see [GetKeyPolicy](#) in *Amazon SDK for Python (Boto3) API Reference*.

For a complete list of Amazon SDK developer guides and code examples, see [Using this service with an Amazon SDK](#). This topic also includes information about getting started and details about previous SDK versions.

Use ListAliases with an Amazon SDK or CLI

The following code examples show how to use ListAliases.

Action examples are code excerpts from larger programs and must be run in context. You can see this action in context in the following code example:

- [Learn the basics](#)

.NET

Amazon SDK for .NET

Note

There's more on GitHub. Find the complete example and learn how to set up and run in the [Amazon Code Examples Repository](#).

```
using System;
using System.Threading.Tasks;
using Amazon.KeyManagementService;
using Amazon.KeyManagementService.Model;

/// <summary>
/// List the AWS Key Management Service (AWS KMS) aliases that have been
defined for
/// the keys in the same AWS Region as the default user. If you want to list
/// the aliases in a different Region, pass the Region to the client
/// constructor.
/// </summary>
public class ListAliases
{
    public static async Task Main()
    {
        var client = new AmazonKeyManagementServiceClient();
        var request = new ListAliasesRequest();
        var response = new ListAliasesResponse();

        do
        {
            response = await client.ListAliasesAsync(request);

            response.Aliases.ForEach(alias =>
            {
                Console.WriteLine($"Created: {alias.CreationDate} Last
Update: {alias.LastUpdatedDate} Name: {alias.AliasName}");
            });

            request.Marker = response.NextMarker;
        }
        while (response.Truncated);
    }
}
```

- For API details, see [ListAliases](#) in *Amazon SDK for .NET API Reference*.

CLI

Amazon CLI

Example 1: To list all aliases in an Amazon account and Region

The following example uses the `list-aliases` command to list all aliases in the default Region of the Amazon account. The output includes aliases associated with Amazon managed KMS keys and customer managed KMS keys.

```
aws kms list-aliases
```

Output:

```
{
  "Aliases": [
    {
      "AliasArn": "arn:aws:kms:us-west-2:111122223333:alias/testKey",
      "AliasName": "alias/testKey",
      "TargetKeyId": "1234abcd-12ab-34cd-56ef-1234567890ab"
    },
    {
      "AliasArn": "arn:aws:kms:us-west-2:111122223333:alias/FinanceDept",
      "AliasName": "alias/FinanceDept",
      "TargetKeyId": "0987dcba-09fe-87dc-65ba-ab0987654321"
    },
    {
      "AliasArn": "arn:aws:kms:us-west-2:111122223333:alias/aws/dynamodb",
      "AliasName": "alias/aws/dynamodb",
      "TargetKeyId": "1a2b3c4d-5e6f-1a2b-3c4d-5e6f1a2b3c4d"
    },
    {
      "AliasArn": "arn:aws:kms:us-west-2:111122223333:alias/aws/ebs",
      "AliasName": "alias/aws/ebs",
      "TargetKeyId": "0987ab65-43cd-21ef-09ab-87654321cdef"
    },
    ...
  ]
}
```

Example 2: To list all aliases for a particular KMS key

The following example uses the `list-aliases` command and its `key-id` parameter to list all aliases that are associated with a particular KMS key.

Each alias is associated with only one KMS key, but a KMS key can have multiple aliases. This command is very useful because the Amazon KMS console lists only one alias for each KMS key. To find all aliases for a KMS key, you must use the `list-aliases` command.

This example uses the key ID of the KMS key for the `--key-id` parameter, but you can use a key ID, key ARN, alias name, or alias ARN in this command.

```
aws kms list-aliases --key-id 1234abcd-12ab-34cd-56ef-1234567890ab
```

Output:


```
{
  "Aliases": [
    {
      "TargetKeyId": "1234abcd-12ab-34cd-56ef-1234567890ab",
      "AliasArn": "arn:aws:kms:us-west-2:111122223333:alias/oregon-test-key",
      "AliasName": "alias/oregon-test-key"
    },
    {
      "TargetKeyId": "1234abcd-12ab-34cd-56ef-1234567890ab",
      "AliasArn": "arn:aws:kms:us-west-2:111122223333:alias/project121-test",
      "AliasName": "alias/project121-test"
    }
  ]
}
```

For more information, see [Working with Aliases](#) in the *Amazon Key Management Service Developer Guide*.

- For API details, see [ListAliases](#) in *Amazon CLI Command Reference*.

Java

SDK for Java 2.x

 **Note**

There's more on GitHub. Find the complete example and learn how to set up and run in the [Amazon Code Examples Repository](#).

```
/**
 * Asynchronously lists all the aliases in the current AWS account.
 *
 * @return a {@link CompletableFuture} that completes when the list of
 * aliases has been processed
 */
public CompletableFuture<Object> listAllAliasesAsync() {
    ListAliasesRequest aliasesRequest = ListAliasesRequest.builder()
        .limit(15)
        .build();

    ListAliasesPublisher paginator =
getAsyncClient().listAliasesPaginator(aliasesRequest);
    return paginator.subscribe(response -> {
        response.aliases().forEach(alias ->
            logger.info("The alias name is: " + alias.aliasName())
        );
    })
        .thenApply(v -> null)
        .exceptionally(ex -> {
            if (ex.getCause() instanceof KmsException) {
                KmsException e = (KmsException) ex.getCause();
                throw new RuntimeException("A KMS exception occurred: " +
e.getMessage());
            } else {
                throw new RuntimeException("An unexpected error occurred: " +
ex.getMessage());
            }
        });
}
```

- For API details, see [ListAliases](#) in *Amazon SDK for Java 2.x API Reference*.

Kotlin

SDK for Kotlin

Note

There's more on GitHub. Find the complete example and learn how to set up and run in the [Amazon Code Examples Repository](#).

```
suspend fun listAllAliases() {
    val request =
        ListAliasesRequest {
            limit = 15
        }

    KmsClient { region = "us-west-2" }.use { kmsClient ->
        val response = kmsClient.listAliases(request)
        response.aliases?.forEach { alias ->
            println("The alias name is ${alias.aliasName}")
        }
    }
}
```

- For API details, see [ListAliases](#) in *Amazon SDK for Kotlin API reference*.

PHP

SDK for PHP

Note

There's more on GitHub. Find the complete example and learn how to set up and run in the [Amazon Code Examples Repository](#).

```
/**
 * @param string $keyId
 * @param int $limit
 * @return ResultPaginator
 */
public function listAliases(string $keyId = "", int $limit = 0)
{
    $args = [];
    if($keyId){
        $args['KeyId'] = $keyId;
    }
    if($limit){
        $args['Limit'] = $limit;
    }
    try{
        return $this->client->getPaginator("ListAliases", $args);
    }catch(KmsException $caught){
        if($caught->getAwsErrorMessage() == "InvalidMarkerException"){
            echo "The request was rejected because the marker that specifies
where pagination should next begin is not valid.\n";
        }
        throw $caught;
    }
}
```

- For API details, see [ListAliases](#) in *Amazon SDK for PHP API Reference*.

Python

SDK for Python (Boto3)

Note

There's more on GitHub. Find the complete example and learn how to set up and run in the [Amazon Code Examples Repository](#).

```
class AliasManager:
```

```
def __init__(self, kms_client):
    self.kms_client = kms_client
    self.created_key = None

    @classmethod
    def from_client(cls) -> "AliasManager":
        """
        Creates an AliasManager instance with a default KMS client.

        :return: An instance of AliasManager initialized with the default KMS
client.
        """
        kms_client = boto3.client("kms")
        return cls(kms_client)

    def list_aliases(self, page_size: int) -> None:
        """
        Lists aliases for the current account.
        :param page_size: The number of aliases to list per page.
        """
        try:
            alias_paginator = self.kms_client.get_paginator("list_aliases")
            for alias_page in alias_paginator.paginate(
                PaginationConfig={"PageSize": page_size}
            ):
                print(f"Here are {page_size} aliases:")
                pprint(alias_page["Aliases"])
                if alias_page["Truncated"]:
                    answer = input(
                        f"Do you want to see the next {page_size} aliases (y/n)?
"
                    )
                    if answer.lower() != "y":
                        break
                else:
                    print("That's all your aliases!")
        except ClientError as err:
            logging.error(
                "Couldn't list your aliases. Here's why: %s",
                err.response["Error"]["Message"],
            )
            raise
```

- For API details, see [ListAliases](#) in *Amazon SDK for Python (Boto3) API Reference*.

For a complete list of Amazon SDK developer guides and code examples, see [Using this service with an Amazon SDK](#). This topic also includes information about getting started and details about previous SDK versions.

Use ListGrants with an Amazon SDK or CLI

The following code examples show how to use ListGrants.

Action examples are code excerpts from larger programs and must be run in context. You can see this action in context in the following code example:

- [Learn the basics](#)

.NET

Amazon SDK for .NET

Note

There's more on GitHub. Find the complete example and learn how to set up and run in the [Amazon Code Examples Repository](#).

```
using System;
using System.Threading.Tasks;
using Amazon.KeyManagementService;
using Amazon.KeyManagementService.Model;

/// <summary>
/// List the AWS Key Management Service (AWS KMS) grants that are associated
with
/// a specific key.
/// </summary>
public class ListGrants
{
    public static async Task Main()
```

```
{
    // The identifier of the AWS KMS key to disable. You can use the
    // key Id or the Amazon Resource Name (ARN) of the AWS KMS key.
    var keyId = "1234abcd-12ab-34cd-56ef-1234567890ab";
    var client = new AmazonKeyManagementServiceClient();
    var request = new ListGrantsRequest
    {
        KeyId = keyId,
    };

    var response = new ListGrantsResponse();

    do
    {
        response = await client.ListGrantsAsync(request);

        response.Grants.ForEach(grant =>
        {
            Console.WriteLine($"{grant.GrantId}");
        });

        request.Marker = response.NextMarker;
    }
    while (response.Truncated);
}
```

- For API details, see [ListGrants](#) in *Amazon SDK for .NET API Reference*.

CLI

Amazon CLI

To view the grants on an Amazon KMS key

The following `list-grants` example displays all of the grants on the specified Amazon managed KMS key for Amazon DynamoDB in your account. This grant allows DynamoDB to use the KMS key on your behalf to encrypt a DynamoDB table before writing it to disk. You can use a command like this one to view the grants on the Amazon managed KMS keys and customer managed KMS keys in the Amazon account and Region.

This command uses the `key-id` parameter with a key ID to identify the KMS key. You can use a key ID or key ARN to identify the KMS key. To get the key ID or key ARN of an Amazon managed KMS key, use the `list-keys` or `list-aliases` command.

```
aws kms list-grants \  
  --key-id 1234abcd-12ab-34cd-56ef-1234567890ab
```

The output shows that the grant gives Amazon DynamoDB permission to use the KMS key for cryptographic operations, and gives it permission to view details about the KMS key (`DescribeKey`) and to retire grants (`RetireGrant`). The `EncryptionContextSubset` constraint limits these permission to requests that include the specified encryption context pairs. As a result, the permissions in the grant are effective only on specified account and DynamoDB table.

```
{  
  "Grants": [  
    {  
      "Constraints": {  
        "EncryptionContextSubset": {  
          "aws:dynamodb:subscriberId": "123456789012",  
          "aws:dynamodb:tableName": "Services"  
        }  
      },  
      "IssuingAccount": "arn:aws:iam::123456789012:root",  
      "Name": "8276b9a6-6cf0-46f1-b2f0-7993a7f8c89a",  
      "Operations": [  
        "Decrypt",  
        "Encrypt",  
        "GenerateDataKey",  
        "ReEncryptFrom",  
        "ReEncryptTo",  
        "RetireGrant",  
        "DescribeKey"  
      ],  
      "GrantId":  
        "1667b97d27cf748cf05b487217dd4179526c949d14fb3903858e25193253fe59",  
      "KeyId": "arn:aws:kms:us-  
west-2:123456789012:key/1234abcd-12ab-34cd-56ef-1234567890ab",  
      "RetiringPrincipal": "dynamodb.us-west-2.amazonaws.com",  
      "GranteePrincipal": "dynamodb.us-west-2.amazonaws.com",  
      "CreationDate": "2021-05-13T18:32:45.144000+00:00"  
    }  
  ]  
}
```



```
]
}
```

For more information, see [Grants in Amazon KMS](#) in the *Amazon Key Management Service Developer Guide*.

- For API details, see [ListGrants](#) in *Amazon CLI Command Reference*.

Java

SDK for Java 2.x

Note

There's more on GitHub. Find the complete example and learn how to set up and run in the [Amazon Code Examples Repository](#).

```
/**
 * Asynchronously displays the grant IDs for the specified key ID.
 *
 * @param keyId the ID of the AWS KMS key for which to list the grants
 * @return a {@link CompletableFuture} that, when completed, will be null
 * if the operation succeeded, or will throw a {@link RuntimeException} if the
 * operation failed
 * @throws RuntimeException if there was an error listing the grants, either
 * due to an {@link KmsException} or an unexpected error
 */
public CompletableFuture<Object> displayGrantIdsAsync(String keyId) {
    ListGrantsRequest grantsRequest = ListGrantsRequest.builder()
        .keyId(keyId)
        .limit(15)
        .build();

    ListGrantsPublisher paginator =
getAsyncClient().listGrantsPaginator(grantsRequest);
    return paginator.subscribe(response -> {
        response.grants().forEach(grant -> {
            logger.info("The grant Id is: " + grant.grantId());
        });
    })
        .thenApply(v -> null)
```

```
        .exceptionally(ex -> {
            Throwable cause = ex.getCause();
            if (cause instanceof KmsException) {
                throw new RuntimeException("Failed to list grants: " +
                    cause.getMessage(), cause);
            } else {
                throw new RuntimeException("An unexpected error occurred: " +
                    cause.getMessage(), cause);
            }
        });
    }
}
```

- For API details, see [ListGrants](#) in *Amazon SDK for Java 2.x API Reference*.

Kotlin

SDK for Kotlin

Note

There's more on GitHub. Find the complete example and learn how to set up and run in the [Amazon Code Examples Repository](#).

```
suspend fun displayGrantIds(keyIdVal: String?) {
    val request =
        ListGrantsRequest {
            keyId = keyIdVal
            limit = 15
        }

    KmsClient { region = "us-west-2" }.use { kmsClient ->
        val response = kmsClient.listGrants(request)
        response.grants?.forEach { grant ->
            println("The grant Id is ${grant.grantId}")
        }
    }
}
```

- For API details, see [ListGrants](#) in *Amazon SDK for Kotlin API reference*.

PHP

SDK for PHP

Note

There's more on GitHub. Find the complete example and learn how to set up and run in the [Amazon Code Examples Repository](#).

```
/**
 * @param string $keyId
 * @return Result
 */
public function listGrants(string $keyId)
{
    try{
        return $this->client->listGrants([
            'KeyId' => $keyId,
        ]);
    }catch(KmsException $caught){
        if($caught->getAwsErrorMessage() == "NotFoundException"){
            echo "    The request was rejected because the specified entity
or resource could not be found.\n";
        }
        throw $caught;
    }
}
```

- For API details, see [ListGrants](#) in *Amazon SDK for PHP API Reference*.

Python

SDK for Python (Boto3)

 **Note**

There's more on GitHub. Find the complete example and learn how to set up and run in the [Amazon Code Examples Repository](#).

```
class GrantManager:
    def __init__(self, kms_client):
        self.kms_client = kms_client

    @classmethod
    def from_client(cls) -> "GrantManager":
        """
        Creates a GrantManager instance with a default KMS client.

        :return: An instance of GrantManager initialized with the default KMS
client.
        """
        kms_client = boto3.client("kms")
        return cls(kms_client)

    def list_grants(self, key_id):
        """
        Lists grants for a key.

        :param key_id: The ARN or ID of the key to query.
        :return: The grants for the key.
        """
        try:
            paginator = self.kms_client.get_paginator("list_grants")
            grants = []
            page_iterator = paginator.paginate(KeyId=key_id)
            for page in page_iterator:
                grants.extend(page["Grants"])

            print(f"Grants for key {key_id}:")
            pprint(grants)
```

```
        return grants
    except ClientError as err:
        logger.error(
            "Couldn't list grants for key %s. Here's why: %s",
            key_id,
            err.response["Error"]["Message"],
        )
        raise
```

- For API details, see [ListGrants](#) in *Amazon SDK for Python (Boto3) API Reference*.

For a complete list of Amazon SDK developer guides and code examples, see [Using this service with an Amazon SDK](#). This topic also includes information about getting started and details about previous SDK versions.

Use ListKeyPolicies with an Amazon SDK or CLI

The following code examples show how to use ListKeyPolicies.

CLI

Amazon CLI

To get the names of key policies for a KMS key

The following `list-key-policies` example gets the names of the key policies for a customer managed key in the example account and Region. You can use this command to find the names of key policies for Amazon managed keys and customer managed keys.

Because the only valid key policy name is `default`, this command is not useful.

To specify the KMS key, use the `key-id` parameter. This example uses a key ID value, but you can use a key ID or key ARN in this command.

```
aws kms list-key-policies \
    --key-id 1234abcd-12ab-34cd-56ef-1234567890ab
```

Output:

```
{
  "PolicyNames": [
    "default"
  ]
}
```

For more information about Amazon KMS key policies, see [Using Key Policies in Amazon KMS](#) in the *Amazon Key Management Service Developer Guide*.

- For API details, see [ListKeyPolicies](#) in *Amazon CLI Command Reference*.

Java

SDK for Java 2.x

Note

There's more on GitHub. Find the complete example and learn how to set up and run in the [Amazon Code Examples Repository](#).

```
/**
 * Asynchronously retrieves the key policy for the specified key ID and
 * policy name.
 *
 * @param keyId      the ID of the AWS KMS key for which to retrieve the
 * policy
 * @param policyName the name of the key policy to retrieve
 * @return a {@link CompletableFuture} that, when completed, contains the key
 * policy as a {@link String}
 */
public CompletableFuture<String> getKeyPolicyAsync(String keyId, String
policyName) {
    GetKeyPolicyRequest policyRequest = GetKeyPolicyRequest.builder()
        .keyId(keyId)
        .policyName(policyName)
        .build();

    return getAsyncClient().getKeyPolicy(policyRequest)
        .thenApply(response -> {
            String policy = response.policy();
        });
}
```

```

        logger.info("The response is: " + policy);
        return policy;
    })
    .exceptionally(ex -> {
        throw new RuntimeException("Failed to get key policy", ex);
    });
}

```

- For API details, see [ListKeyPolicies](#) in *Amazon SDK for Java 2.x API Reference*.

Python

SDK for Python (Boto3)

Note

There's more on GitHub. Find the complete example and learn how to set up and run in the [Amazon Code Examples Repository](#).

```

class KeyPolicy:
    def __init__(self, kms_client):
        self.kms_client = kms_client

    @classmethod
    def from_client(cls) -> "KeyPolicy":
        """
        Creates a KeyPolicy instance with a default KMS client.

        :return: An instance of KeyPolicy initialized with the default KMS
client.
        """
        kms_client = boto3.client("kms")
        return cls(kms_client)

    def list_policies(self, key_id):
        """
        Lists the names of the policies for a key.

        :param key_id: The ARN or ID of the key to query.

```

```
"""
try:
    policy_names = self.kms_client.list_key_policies(KeyId=key_id)[
        "PolicyNames"
    ]
except ClientError as err:
    logging.error(
        "Couldn't list your policies. Here's why: %s",
        err.response["Error"]["Message"],
    )
    raise
else:
    print(f"The policies for key {key_id} are:")
    pprint(policy_names)
```

- For API details, see [ListKeyPolicies](#) in *Amazon SDK for Python (Boto3) API Reference*.

For a complete list of Amazon SDK developer guides and code examples, see [Using this service with an Amazon SDK](#). This topic also includes information about getting started and details about previous SDK versions.

Use ListKeys with an Amazon SDK or CLI

The following code examples show how to use ListKeys.

Action examples are code excerpts from larger programs and must be run in context. You can see this action in context in the following code example:

- [Learn the basics](#)

.NET

Amazon SDK for .NET

Note

There's more on GitHub. Find the complete example and learn how to set up and run in the [Amazon Code Examples Repository](#).


```
using System;
using System.Threading.Tasks;
using Amazon.KeyManagementService;
using Amazon.KeyManagementService.Model;

/// <summary>
/// List the AWS Key Managements Service (AWS KMS) keys for the AWS Region
/// of the default user. To list keys in another AWS Region, supply the
Region
/// as a parameter to the client constructor.
/// </summary>
public class ListKeys
{
    public static async Task Main()
    {
        var client = new AmazonKeyManagementServiceClient();
        var request = new ListKeysRequest();
        var response = new ListKeysResponse();

        do
        {
            response = await client.ListKeysAsync(request);

            response.Keys.ForEach(key =>
            {
                Console.WriteLine($"ID: {key.KeyId}, {key.KeyArn}");
            });

            // Set the Marker property when response.Truncated is true
            // in order to get the next keys.
            request.Marker = response.NextMarker;
        }
        while (response.Truncated);
    }
}
```

- For API details, see [ListKeys](#) in *Amazon SDK for .NET API Reference*.

CLI

Amazon CLI

To get the KMS keys in an account and Region

The following `list-keys` example gets the KMS keys in an account and Region. This command returns both Amazon managed keys and customer managed keys.

```
aws kms list-keys
```

Output:

```
{
  "Keys": [
    {
      "KeyArn": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab",
      "KeyId": "1234abcd-12ab-34cd-56ef-1234567890ab"
    },
    {
      "KeyArn": "arn:aws:kms:us-
west-2:111122223333:key/0987dcba-09fe-87dc-65ba-ab0987654321",
      "KeyId": "0987dcba-09fe-87dc-65ba-ab0987654321"
    },
    {
      "KeyArn": "arn:aws:kms:us-
east-2:111122223333:key/1a2b3c4d-5e6f-1a2b-3c4d-5e6f1a2b3c4d",
      "KeyId": "1a2b3c4d-5e6f-1a2b-3c4d-5e6f1a2b3c4d"
    }
  ]
}
```

For more information, see [Viewing Keys](#) in the *Amazon Key Management Service Developer Guide*.

- For API details, see [ListKeys](#) in *Amazon CLI Command Reference*.

Java

SDK for Java 2.x

 **Note**

There's more on GitHub. Find the complete example and learn how to set up and run in the [Amazon Code Examples Repository](#).

```
import software.amazon.awssdk.services.kms.KmsAsyncClient;
import software.amazon.awssdk.services.kms.model.ListKeysRequest;
import software.amazon.awssdk.services.kms.paginators.ListKeysPublisher;
import java.util.concurrent.CompletableFuture;

/**
 * Before running this Java V2 code example, set up your development
 * environment, including your credentials.
 *
 * For more information, see the following documentation topic:
 *
 * https://docs.aws.amazon.com/sdk-for-java/latest/developer-guide/get-
 * started.html
 */
public class HelloKMS {
    public static void main(String[] args) {
        listAllKeys();
    }

    public static void listAllKeys() {
        KmsAsyncClient kmsAsyncClient = KmsAsyncClient.builder()
            .build();
        ListKeysRequest listKeysRequest = ListKeysRequest.builder()
            .limit(15)
            .build();

        /**
         * The `subscribe` method is required when using paginator methods in the
         * AWS SDK
         * because paginator methods return an instance of a `ListKeysPublisher`,
         * which is

```

```
    * based on a reactive stream. This allows asynchronous retrieval of
    paginated
    * results as they become available. By subscribing to the stream, we can
    process
    * each page of results as they are emitted.
    */
    ListKeysPublisher keysPublisher =
kmsAsyncClient.listKeysPaginator(listKeysRequest);
    CompletableFuture<Void> future = keysPublisher
        .subscribe(r -> r.keys().forEach(key ->
            System.out.println("The key ARN is: " + key.keyArn() + ". The key
    Id is: " + key.keyId()))
        .whenComplete((result, exception) -> {
            if (exception != null) {
                System.err.println("Error occurred: " +
exception.getMessage());
            } else {
                System.out.println("Successfully listed all keys.");
            }
        });

    try {
        future.join();
    } catch (Exception e) {
        System.err.println("Failed to list keys: " + e.getMessage());
    }
}
```

- For API details, see [ListKeys](#) in *Amazon SDK for Java 2.x API Reference*.

Kotlin

SDK for Kotlin

Note

There's more on GitHub. Find the complete example and learn how to set up and run in the [Amazon Code Examples Repository](#).

```
suspend fun listAllKeys() {
    val request =
        ListKeysRequest {
            limit = 15
        }

    KmsClient { region = "us-west-2" }.use { kmsClient ->
        val response = kmsClient.listKeys(request)
        response.keys?.forEach { key ->
            println("The key ARN is ${key.keyArn}")
            println("The key Id is ${key.keyId}")
        }
    }
}
```

- For API details, see [ListKeys](#) in *Amazon SDK for Kotlin API reference*.

PHP

SDK for PHP

Note

There's more on GitHub. Find the complete example and learn how to set up and run in the [Amazon Code Examples Repository](#).

```
/**
 * @return array
 */
public function listKeys()
{
    try {
        $contents = [];
        $paginator = $this->client->getPaginator("ListKeys");
        foreach($paginator as $result){
            foreach ($result['Content'] as $object) {
                $contents[] = $object;
            }
        }
    }
}
```

```
        }
        return $contents;
    }catch(KmsException $caught){
        echo "There was a problem listing the keys: {$caught-
>getAwsErrorMessage()}\n";
        throw $caught;
    }
}
```

- For API details, see [ListKeys](#) in *Amazon SDK for PHP API Reference*.

Python

SDK for Python (Boto3)

Note

There's more on GitHub. Find the complete example and learn how to set up and run in the [Amazon Code Examples Repository](#).

```
class KeyManager:
    def __init__(self, kms_client):
        self.kms_client = kms_client
        self.created_keys = []

    @classmethod
    def from_client(cls) -> "KeyManager":
        """
        Creates a KeyManager instance with a default KMS client.

        :return: An instance of KeyManager initialized with the default KMS
client.
        """
        kms_client = boto3.client("kms")
        return cls(kms_client)

    def list_keys(self):
        """
```

```

Lists the keys for the current account by using a paginator.
"""
try:
    page_size = 10
    print("\nLet's list your keys.")
    key_paginator = self.kms_client.get_paginator("list_keys")
    for key_page in key_paginator.paginate(PaginationConfig={"PageSize":
10}):
        print(f"Here are {len(key_page['Keys'])} keys:")
        pprint(key_page["Keys"])
        if key_page["Truncated"]:
            answer = input(
                f"Do you want to see the next {page_size} keys (y/n)? "
            )
            if answer.lower() != "y":
                break
        else:
            print("That's all your keys!")
except ClientError as err:
    logging.error(
        "Couldn't list your keys. Here's why: %s",
        err.response["Error"]["Message"],
    )

```

- For API details, see [ListKeys](#) in *Amazon SDK for Python (Boto3) API Reference*.

Rust

SDK for Rust

Note

There's more on GitHub. Find the complete example and learn how to set up and run in the [Amazon Code Examples Repository](#).

```

async fn show_keys(client: &Client) -> Result<(), Error> {
    let resp = client.list_keys().send().await?;

    let keys = resp.keys.unwrap_or_default();

```

```
let len = keys.len();

for key in keys {
    println!("Key ARN: {}", key.key_arn.as_deref().unwrap_or_default());
}

println!();
println!("Found {} keys", len);

Ok(())
}
```

- For API details, see [ListKeys](#) in *Amazon SDK for Rust API reference*.

For a complete list of Amazon SDK developer guides and code examples, see [Using this service with an Amazon SDK](#). This topic also includes information about getting started and details about previous SDK versions.

Use PutKeyPolicy with an Amazon SDK or CLI

The following code examples show how to use PutKeyPolicy.

CLI

Amazon CLI

To change the key policy for a KMS key

The following `put-key-policy` example changes the key policy for a customer managed key.

To begin, create a key policy and save it in a local JSON file. In this example, the file is `key_policy.json`. You can also specify the key policy as a string value of the `policy` parameter.

The first statement in this key policy gives the Amazon account permission to use IAM policies to control access to the KMS key. The second statement gives the `test-user` user permission to run the `describe-key` and `list-keys` commands on the KMS key.

Contents of `key_policy.json`:


```
{
  "Version" : "2012-10-17",
  "Id" : "key-default-1",
  "Statement" : [
    {
      "Sid" : "Enable IAM User Permissions",
      "Effect" : "Allow",
      "Principal" : {
        "AWS" : "arn:aws:iam::111122223333:root"
      },
      "Action" : "kms:*",
      "Resource" : "*"
    },
    {
      "Sid" : "Allow Use of Key",
      "Effect" : "Allow",
      "Principal" : {
        "AWS" : "arn:aws:iam::111122223333:user/test-user"
      },
      "Action" : [
        "kms:DescribeKey",
        "kms:ListKeys"
      ],
      "Resource" : "*"
    }
  ]
}
```

To identify the KMS key, this example uses the key ID, but you can also use a key ARN. To specify the key policy, the command uses the `policy` parameter. To indicate that the policy is in a file, it uses the required `file://` prefix. This prefix is required to identify files on all supported operating systems. Finally, the command uses the `policy-name` parameter with a value of `default`. If no policy name is specified, the default value is `default`. The only valid value is `default`.

```
aws kms put-key-policy \
  --policy-name default \
  --key-id 1234abcd-12ab-34cd-56ef-1234567890ab \
  --policy file://key_policy.json
```

This command does not produce any output. To verify that the command was effective, use the `get-key-policy` command. The following example command gets the key policy for the same KMS key. The output parameter with a value of `text` returns a text format that is easy to read.

```
aws kms get-key-policy \  
  --policy-name default \  
  --key-id 1234abcd-12ab-34cd-56ef-1234567890ab \  
  --output text
```

Output:

```
{  
  "Version" : "2012-10-17",  
  "Id" : "key-default-1",  
  "Statement" : [  
    {  
      "Sid" : "Enable IAM User Permissions",  
      "Effect" : "Allow",  
      "Principal" : {  
        "AWS" : "arn:aws:iam::111122223333:root"  
      },  
      "Action" : "kms:*",  
      "Resource" : "*"   
    },  
    {  
      "Sid" : "Allow Use of Key",  
      "Effect" : "Allow",  
      "Principal" : {  
        "AWS" : "arn:aws:iam::111122223333:user/test-user"  
      },  
      "Action" : [ "kms:Describe", "kms:List" ],  
      "Resource" : "*"   
    }  
  ]  
}
```

For more information, see [Changing a Key Policy](#) in the *Amazon Key Management Service Developer Guide*.

- For API details, see [PutKeyPolicy](#) in *Amazon CLI Command Reference*.

PHP

SDK for PHP

 **Note**


There's more on GitHub. Find the complete example and learn how to set up and run in the [Amazon Code Examples Repository](#).

```
/**
 * @param string $keyId
 * @param string $policy
 * @return void
 */
public function putKeyPolicy(string $keyId, string $policy)
{
    try {
        $this->client->putKeyPolicy([
            'KeyId' => $keyId,
            'Policy' => $policy,
        ]);
    } catch (KmsException $caught){
        echo "There was a problem replacing the key policy: {$caught-
>getAwsErrorMessage()}\n";
        throw $caught;
    }
}
```

- For API details, see [PutKeyPolicy](#) in *Amazon SDK for PHP API Reference*.

Python

SDK for Python (Boto3)

 **Note**

There's more on GitHub. Find the complete example and learn how to set up and run in the [Amazon Code Examples Repository](#).

```
class KeyPolicy:
    def __init__(self, kms_client):
        self.kms_client = kms_client

    @classmethod
    def from_client(cls) -> "KeyPolicy":
        """
        Creates a KeyPolicy instance with a default KMS client.

        :return: An instance of KeyPolicy initialized with the default KMS
client.
        """
        kms_client = boto3.client("kms")
        return cls(kms_client)

    def set_policy(self, key_id: str, policy: dict[str, any]) -> None:
        """
        Sets the policy of a key. Setting a policy entirely overwrites the
existing
policy, so care is taken to add a statement to the existing list of
statements
rather than simply writing a new policy.

:param key_id: The ARN or ID of the key to set the policy to.
:param policy: The existing policy of the key.
:return: None
        """
        principal = input(
            "Enter the ARN of an IAM role to set as the principal on the policy:
"
        )
    )
```

```
    if key_id != "" and principal != "":
        # The updated policy replaces the existing policy. Add a new
statement to
        # the list along with the original policy statements.
        policy["Statement"].append(
            {
                "Sid": "Allow access for ExampleRole",
                "Effect": "Allow",
                "Principal": {"AWS": principal},
                "Action": [
                    "kms:Encrypt",
                    "kms:GenerateDataKey*",
                    "kms:Decrypt",
                    "kms:DescribeKey",
                    "kms:ReEncrypt*",
                ],
                "Resource": "*",
            }
        )
    try:
        self.kms_client.put_key_policy(KeyId=key_id,
Policy=json.dumps(policy))
    except ClientError as err:
        logger.error(
            "Couldn't set policy for key %s. Here's why %s",
            key_id,
            err.response["Error"]["Message"],
        )
        raise
    else:
        print(f"Set policy for key {key_id}.")
else:
    print("Skipping set policy demo.")
```

- For API details, see [PutKeyPolicy](#) in *Amazon SDK for Python (Boto3) API Reference*.

For a complete list of Amazon SDK developer guides and code examples, see [Using this service with an Amazon SDK](#). This topic also includes information about getting started and details about previous SDK versions.

Use ReEncrypt with an Amazon SDK or CLI

The following code examples show how to use ReEncrypt.

CLI

Amazon CLI

Example 1: To re-encrypt an encrypted message under a different symmetric KMS key (Linux and macOS).

The following `re-encrypt` command example demonstrates the recommended way to re-encrypt data with the Amazon CLI.

Provide the ciphertext in a file. In the value of the `--ciphertext-blob` parameter, use the `fileb://` prefix, which tells the CLI to read the data from a binary file. If the file is not in the current directory, type the full path to file. For more information about reading Amazon CLI parameter values from a file, see [Loading Amazon CLI parameters from a file <https://docs.aws.amazon.com/cli/latest/userguide/cli-usage-parameters-file.html>](https://docs.aws.amazon.com/cli/latest/userguide/cli-usage-parameters-file.html) in the *Amazon Command Line Interface User Guide* and [Best Practices for Local File Parameters<https://aws.amazon.com/blogs/developer/best-practices-for-local-file-parameters/>](https://aws.amazon.com/blogs/developer/best-practices-for-local-file-parameters/) in the *Amazon Command Line Tool Blog*. Specify the source KMS key, which decrypts the ciphertext. The `--source-key-id` parameter is not required when decrypting with symmetric encryption KMS keys. Amazon KMS can get the KMS key that was used to encrypt the data from the metadata in the ciphertext blob. But it's always a best practice to specify the KMS key you are using. This practice ensures that you use the KMS key that you intend, and prevents you from inadvertently decrypting a ciphertext using a KMS key you do not trust. Specify the destination KMS key, which re-encrypts the data. The `--destination-key-id` parameter is always required. This example uses a key ARN, but you can use any valid key identifier. Request the plaintext output as a text value. The `--query` parameter tells the CLI to get only the value of the `Plaintext` field from the output. The `--output` parameter returns the output as text. Base64-decode the plaintext and save it in a file. The following example pipes (`|`) the value of the `Plaintext` parameter to the `Base64` utility, which decodes it. Then, it redirects (`>`) the decoded output to the `ExamplePlaintext` file.

Before running this command, replace the example key IDs with valid key identifiers from your Amazon account.

```
aws kms re-encrypt \
```

```
--ciphertext-blob fileb://ExampleEncryptedFile \  
--source-key-id 1234abcd-12ab-34cd-56ef-1234567890ab \  
--destination-key-id 0987dcba-09fe-87dc-65ba-ab0987654321 \  
--query CiphertextBlob \  
--output text | base64 --decode > ExampleReEncryptedFile
```

This command produces no output. The output from the re-encrypt command is base64-decoded and saved in a file.

For more information, see ReEncrypt <https://docs.aws.amazon.com/kms/latest/APIReference/API_ReEncrypt.html> in the *Amazon Key Management Service API Reference*.

Example 2: To re-encrypt an encrypted message under a different symmetric KMS key (Windows command prompt).

The following re-encrypt command example is the same as the previous one except that it uses the `certutil` utility to Base64-decode the plaintext data. This procedure requires two commands, as shown in the following examples.

Before running this command, replace the example key ID with a valid key ID from your Amazon account.

```
aws kms re-encrypt ^  
--ciphertext-blob fileb://ExampleEncryptedFile ^  
--source-key-id 1234abcd-12ab-34cd-56ef-1234567890ab ^  
--destination-key-id 0987dcba-09fe-87dc-65ba-ab0987654321 ^  
--query CiphertextBlob ^  
--output text > ExampleReEncryptedFile.base64
```

Then use the `certutil` utility

```
certutil -decode ExamplePlaintextFile.base64 ExamplePlaintextFile
```

Output:

```
Input Length = 18  
Output Length = 12  
CertUtil: -decode command completed successfully.
```

For more information, see ReEncrypt <https://docs.aws.amazon.com/kms/latest/APIReference/API_ReEncrypt.html> in the *Amazon Key Management Service API Reference*.

- For API details, see [ReEncrypt](#) in *Amazon CLI Command Reference*.

Python

SDK for Python (Boto3)

Note

There's more on GitHub. Find the complete example and learn how to set up and run in the [Amazon Code Examples Repository](#).

```
class KeyEncrypt:
    def __init__(self, kms_client):
        self.kms_client = kms_client

    @classmethod
    def from_client(cls) -> "KeyEncrypt":
        """
        Creates a KeyEncrypt instance with a default KMS client.

        :return: An instance of KeyEncrypt initialized with the default KMS
client.
        """
        kms_client = boto3.client("kms")
        return cls(kms_client)

    def re_encrypt(self, source_key_id, cipher_text):
        """
        Takes ciphertext previously encrypted with one key and reencrypt it by
using
        another key.

        :param source_key_id: The ARN or ID of the original key used to encrypt
the
                ciphertext.
        :param cipher_text: The encrypted ciphertext.
        :return: The ciphertext encrypted by the second key.
        """
        destination_key_id = input(
            f"Your ciphertext is currently encrypted with key {source_key_id}. "
```



```

        f"Enter another key ID or ARN to reencrypt it: "
    )
    if destination_key_id != "":
        try:
            cipher_text = self.kms_client.re_encrypt(
                SourceKeyId=source_key_id,
                DestinationKeyId=destination_key_id,
                CiphertextBlob=cipher_text,
            )["CiphertextBlob"]
        except ClientError as err:
            logger.error(
                "Couldn't reencrypt your ciphertext. Here's why: %s",
                err.response["Error"]["Message"],
            )
        else:
            print(f"Reencrypted your ciphertext as: {cipher_text}")
            return cipher_text
    else:
        print("Skipping reencryption demo.")

```

- For API details, see [ReEncrypt](#) in *Amazon SDK for Python (Boto3) API Reference*.

Ruby

SDK for Ruby

Note

There's more on GitHub. Find the complete example and learn how to set up and run in the [Amazon Code Examples Repository](#).

```

require 'aws-sdk-kms' # v2: require 'aws-sdk'

# Human-readable version of the ciphertext of the data to reencrypt.

blob =
  '01020200785d68faeec386af1057904926253051eb2919d3c16078badf65b808b26dd057c101747cadf3593'
sourceCiphertextBlob = [blob].pack('H*')

```

```
# Replace the fictitious key ARN with a valid key ID

destinationKeyId = 'arn:aws:kms:us-
west-2:111122223333:key/0987dcba-09fe-87dc-65ba-ab0987654321'

client = Aws::KMS::Client.new(region: 'us-west-2')

resp = client.re_encrypt({
    ciphertext_blob: sourceCiphertextBlob,
    destination_key_id: destinationKeyId
})

# Display a readable version of the resulting re-encrypted blob.
puts 'Blob:'
puts resp.ciphertext_blob.unpack('H*')
```

- For API details, see [ReEncrypt](#) in *Amazon SDK for Ruby API Reference*.

Rust

SDK for Rust

Note

There's more on GitHub. Find the complete example and learn how to set up and run in the [Amazon Code Examples Repository](#).

```
async fn reencrypt_string(
    verbose: bool,
    client: &Client,
    input_file: &str,
    output_file: &str,
    first_key: &str,
    new_key: &str,
) -> Result<(), Error> {
    // Get blob from input file
    // Open input text file and get contents as a string
    // input is a base-64 encoded string, so decode it:
    let data = fs::read_to_string(input_file)
```

```
        .map(|input_file| base64::decode(input_file).expect("invalid base 64"))
        .map(Blob::new);

let resp = client
    .re_encrypt()
    .ciphertext_blob(data.unwrap())
    .source_key_id(first_key)
    .destination_key_id(new_key)
    .send()
    .await?;

// Did we get an encrypted blob?
let blob = resp.ciphertext_blob.expect("Could not get encrypted text");
let bytes = blob.as_ref();

let s = base64::encode(bytes);
let o = &output_file;

let mut ofile = File::create(o).expect("unable to create file");
ofile.write_all(s.as_bytes()).expect("unable to write");

if verbose {
    println!("Wrote the following to {:}", output_file);
    println!("{}", s);
} else {
    println!("Wrote base64-encoded output to {}", output_file);
}

Ok(())
}
```

- For API details, see [ReEncrypt](#) in *Amazon SDK for Rust API reference*.

For a complete list of Amazon SDK developer guides and code examples, see [Using this service with an Amazon SDK](#). This topic also includes information about getting started and details about previous SDK versions.

Use RetireGrant with an Amazon SDK or CLI

The following code examples show how to use RetireGrant.

CLI

Amazon CLI**To retire a grant on a customer master key**

The following `retire-grant` example deletes a grant from a KMS key.

The following example command specifies the `grant-id` and the `key-id` parameters. The value of the `key-id` parameter must be the key ARN of the KMS key.

```
aws kms retire-grant \  
  --grant-id 1234a2345b8a4e350500d432bccf8ecd6506710e1391880c4f7f7140160c9af3 \  
  --key-id arn:aws:kms:us-  
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab
```

This command produces no output. To confirm that the grant was retired, use the `list-grants` command.

For more information, see [Retiring and revoking grants](#) in the *Amazon Key Management Service Developer Guide*.

- For API details, see [RetireGrant](#) in *Amazon CLI Command Reference*.

Python

SDK for Python (Boto3)**Note**

There's more on GitHub. Find the complete example and learn how to set up and run in the [Amazon Code Examples Repository](#).

```
class GrantManager:  
    def __init__(self, kms_client):  
        self.kms_client = kms_client  
  
    @classmethod  
    def from_client(cls) -> "GrantManager":  
        """
```

```

    Creates a GrantManager instance with a default KMS client.

    :return: An instance of GrantManager initialized with the default KMS
client.
    """
    kms_client = boto3.client("kms")
    return cls(kms_client)

def retire_grant(self, grant):
    """
    Retires a grant so that it can no longer be used.

    :param grant: The grant to retire.
    """
    try:
        self.kms_client.retire_grant(GrantToken=grant["GrantToken"])
    except ClientError as err:
        logger.error(
            "Couldn't retire grant %s. Here's why: %s",
            grant["GrantId"],
            err.response["Error"]["Message"],
        )
    else:
        print(f"Grant {grant['GrantId']} retired.")

```

- For API details, see [RetireGrant](#) in *Amazon SDK for Python (Boto3) API Reference*.

For a complete list of Amazon SDK developer guides and code examples, see [Using this service with an Amazon SDK](#). This topic also includes information about getting started and details about previous SDK versions.

Use RevokeGrant with an Amazon SDK or CLI

The following code examples show how to use RevokeGrant.

Action examples are code excerpts from larger programs and must be run in context. You can see this action in context in the following code example:

- [Learn the basics](#)

CLI

Amazon CLI

To revoke a grant on a customer master key

The following `revoke-grant` example deletes a grant from a KMS key. The following example command specifies the `grant-id` and the `key-id` parameters. The value of the `key-id` parameter can be the key ID or key ARN of the KMS key.

```
aws kms revoke-grant \  
  --grant-id 1234a2345b8a4e350500d432bccf8ecd6506710e1391880c4f7f7140160c9af3 \  
  --key-id 1234abcd-12ab-34cd-56ef-1234567890ab
```

This command produces no output. To confirm that the grant was revoked, use the `list-grants` command.

For more information, see [Retiring and revoking grants](#) in the *Amazon Key Management Service Developer Guide*.

- For API details, see [RevokeGrant](#) in *Amazon CLI Command Reference*.

Java

SDK for Java 2.x

 **Note**

There's more on GitHub. Find the complete example and learn how to set up and run in the [Amazon Code Examples Repository](#).

```
/**  
 * Revokes a grant for the specified AWS KMS key asynchronously.  
 *  
 * @param keyId The ID or key ARN of the AWS KMS key.  
 * @param grantId The identifier of the grant to be revoked.  
 * @return A {@link CompletableFuture} representing the asynchronous  
 operation of revoking the grant.  
 * The {@link CompletableFuture} will complete with a {@link  
 RevokeGrantResponse} object
```

```
    *         if the operation is successful, or with a {@code null} value if an
error occurs.
    */
    public CompletableFuture<RevokeGrantResponse> revokeKeyGrantAsync(String
keyId, String grantId) {
        RevokeGrantRequest grantRequest = RevokeGrantRequest.builder()
            .keyId(keyId)
            .grantId(grantId)
            .build();

        CompletableFuture<RevokeGrantResponse> responseFuture =
getAsyncClient().revokeGrant(grantRequest);
        responseFuture.whenComplete((response, exception) -> {
            if (exception == null) {
                logger.info("Grant ID: [" + grantId + "] was successfully
revoked!");
            } else {
                if (exception instanceof KmsException kmsEx) {
                    if (kmsEx.getMessage().contains("Grant does not exist")) {
                        logger.info("The grant ID '" + grantId + "' does not
exist. Moving on...");
                    } else {
                        throw new RuntimeException("KMS error occurred: " +
kmsEx.getMessage(), kmsEx);
                    }
                } else {
                    throw new RuntimeException("An unexpected error occurred: " +
exception.getMessage(), exception);
                }
            }
        });

        return responseFuture;
    }
}
```

- For API details, see [RevokeGrant](#) in *Amazon SDK for Java 2.x API Reference*.

PHP

SDK for PHP

 **Note**

There's more on GitHub. Find the complete example and learn how to set up and run in the [Amazon Code Examples Repository](#).

```
/**
 * @param string $grantId
 * @param string $keyId
 * @return void
 */
public function revokeGrant(string $grantId, string $keyId)
{
    try{
        $this->client->revokeGrant([
            'GrantId' => $grantId,
            'KeyId' => $keyId,
        ]);
    }catch(KmsException $caught){
        echo "There was a problem with revoking the grant: {$caught-
>getAwsErrorMessage()}.\\n";
        throw $caught;
    }
}
```

- For API details, see [RevokeGrant](#) in *Amazon SDK for PHP API Reference*.

Python

SDK for Python (Boto3)

 **Note**

There's more on GitHub. Find the complete example and learn how to set up and run in the [Amazon Code Examples Repository](#).

```
class GrantManager:
    def __init__(self, kms_client):
        self.kms_client = kms_client

    @classmethod
    def from_client(cls) -> "GrantManager":
        """
        Creates a GrantManager instance with a default KMS client.

        :return: An instance of GrantManager initialized with the default KMS
client.
        """
        kms_client = boto3.client("kms")
        return cls(kms_client)

    def revoke_grant(self, key_id: str, grant_id: str) -> None:
        """
        Revokes a grant so that it can no longer be used.

        :param key_id: The ARN or ID of the key associated with the grant.
        :param grant_id: The ID of the grant to revoke.
        """
        try:
            self.kms_client.revoke_grant(KeyId=key_id, GrantId=grant_id)
        except ClientError as err:
            logger.error(
                "Couldn't revoke grant %s. Here's why: %s",
                grant_id,
                err.response["Error"]["Message"],
            )
            raise
```

- For API details, see [RevokeGrant](#) in *Amazon SDK for Python (Boto3) API Reference*.

For a complete list of Amazon SDK developer guides and code examples, see [Using this service with an Amazon SDK](#). This topic also includes information about getting started and details about previous SDK versions.

Use `ScheduleKeyDeletion` with an Amazon SDK or CLI

The following code examples show how to use `ScheduleKeyDeletion`.

Action examples are code excerpts from larger programs and must be run in context. You can see this action in context in the following code example:

- [Learn the basics](#)

CLI

Amazon CLI

To schedule the deletion of a customer managed KMS key.

The following `schedule-key-deletion` example schedules the specified customer managed KMS key to be deleted in 15 days.

The `--key-id` parameter identifies the KMS key. This example uses a key ARN value, but you can use either the key ID or the ARN of the KMS key. The `--pending-window-in-days` parameter specifies the length of the 7-30 day waiting period. By default, the waiting period is 30 days. This example specifies a value of 15, which tells Amazon to permanently delete the KMS key 15 days after the command completes.

```
aws kms schedule-key-deletion \  
  --key-id arn:aws:kms:us-  
west-2:123456789012:key/1234abcd-12ab-34cd-56ef-1234567890ab \  
  --pending-window-in-days 15
```

The response includes the key ARN, key state, waiting period (`PendingWindowInDays`), and the deletion date in Unix time. To view the deletion date in local time, use the Amazon KMS console. KMS keys in the `PendingDeletion` key state cannot be used in cryptographic operations.

```
{
  "KeyId": "arn:aws:kms:us-
west-2:123456789012:key/1234abcd-12ab-34cd-56ef-1234567890ab",
  "DeletionDate": "2022-06-18T23:43:51.272000+00:00",
  "KeyState": "PendingDeletion",
  "PendingWindowInDays": 15
}
```

For more information, see [Deleting keys](#) in the *Amazon Key Management Service Developer Guide*.

- For API details, see [ScheduleKeyDeletion](#) in *Amazon CLI Command Reference*.

Java

SDK for Java 2.x

Note

There's more on GitHub. Find the complete example and learn how to set up and run in the [Amazon Code Examples Repository](#).

```
/**
 * Deletes a KMS key asynchronously.
 *
 * <p><strong>Warning:</strong> Deleting a KMS key is a destructive and
potentially dangerous operation.
 * When a KMS key is deleted, all data that was encrypted under the KMS key
becomes unrecoverable.
 * This means that any files, databases, or other data that were encrypted
using the deleted KMS key
 * will become permanently inaccessible. Exercise extreme caution when
deleting KMS keys.</p>
 *
 * @param keyId the ID of the KMS key to delete
```

```

    * @return a {@link CompletableFuture} that completes when the key deletion
    is scheduled
    */
    public CompletableFuture<Void> deleteKeyAsync(String keyId) {
        ScheduleKeyDeletionRequest deletionRequest =
        ScheduleKeyDeletionRequest.builder()
            .keyId(keyId)
            .pendingWindowInDays(7)
            .build();

        return getAsyncClient().scheduleKeyDeletion(deletionRequest)
            .thenRun(() -> {
                logger.info("Key {} will be deleted in 7 days", keyId);
            })
            .exceptionally(throwable -> {
                throw new RuntimeException("Failed to schedule key deletion for
key ID: " + keyId, throwable);
            });
    }
}

```

- For API details, see [ScheduleKeyDeletion](#) in *Amazon SDK for Java 2.x API Reference*.

PHP

SDK for PHP

Note

There's more on GitHub. Find the complete example and learn how to set up and run in the [Amazon Code Examples Repository](#).

```

/**
 * @param string $keyId
 * @param int $pendingWindowInDays
 * @return void
 */
public function scheduleKeyDeletion(string $keyId, int $pendingWindowInDays =
7)
{

```

```
try {
    $this->client->scheduleKeyDeletion([
        'KeyId' => $keyId,
        'PendingWindowInDays' => $pendingWindowInDays,
    ]);
} catch (KmsException $caught){
    echo "There was a problem scheduling the key deletion: {"$caught->getAwsErrorMessage()}\n";
    throw $caught;
}
```

- For API details, see [ScheduleKeyDeletion](#) in *Amazon SDK for PHP API Reference*.

Python

SDK for Python (Boto3)

Note

There's more on GitHub. Find the complete example and learn how to set up and run in the [Amazon Code Examples Repository](#).

```
class KeyManager:
    def __init__(self, kms_client):
        self.kms_client = kms_client
        self.created_keys = []

    @classmethod
    def from_client(cls) -> "KeyManager":
        """
        Creates a KeyManager instance with a default KMS client.

        :return: An instance of KeyManager initialized with the default KMS
        client.
        """
        kms_client = boto3.client("kms")
        return cls(kms_client)
```

```
def delete_key(self, key_id: str, window: int) -> None:
    """
    Deletes a list of keys.

    Warning:
    Deleting a KMS key is a destructive and potentially dangerous operation.
    When a KMS key is deleted,
    all data that was encrypted under the KMS key is unrecoverable.

    :param key_id: The ARN or ID of the key to delete.
    :param window: The waiting period, in days, before the KMS key is
    deleted.
    """

    try:
        self.kms_client.schedule_key_deletion(
            KeyId=key_id, PendingWindowInDays=window
        )
    except ClientError as err:
        logging.error(
            "Couldn't delete key %s. Here's why: %s",
            key_id,
            err.response["Error"]["Message"],
        )
        raise
```

- For API details, see [ScheduleKeyDeletion](#) in *Amazon SDK for Python (Boto3) API Reference*.

For a complete list of Amazon SDK developer guides and code examples, see [Using this service with an Amazon SDK](#). This topic also includes information about getting started and details about previous SDK versions.

Use Sign with an Amazon SDK or CLI

The following code examples show how to use Sign.

Action examples are code excerpts from larger programs and must be run in context. You can see this action in context in the following code example:

- [Learn the basics](#)

CLI

Amazon CLI

Example 1: To generate a digital signature for a message

The following `sign` example generates a cryptographic signature for a short message. The output of the command includes a base-64 encoded `Signature` field that you can verify by using the `verify` command.

You must specify a message to sign and a signing algorithm that your asymmetric KMS key supports. To get the signing algorithms for your KMS key, use the `describe-key` command.

In Amazon CLI 2.0, the value of the `message` parameter must be Base64-encoded. Or, you can save the message in a file and use the `fileb://` prefix, which tells the Amazon CLI to read binary data from the file.

Before running this command, replace the example key ID with a valid key ID from your Amazon account. The key ID must represent an asymmetric KMS key with a key usage of `SIGN_VERIFY`.

```
msg=(echo 'Hello World' | base64)

aws kms sign \
  --key-id 1234abcd-12ab-34cd-56ef-1234567890ab \
  --message fileb://UnsignedMessage \
  --message-type RAW \
  --signing-algorithm RSASSA_PKCS1_V1_5_SHA_256
```

Output:

```
{
  "KeyId": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab",
  "Signature": "ABCDEFhpyVYyTxbafE74ccSvEJLJr3zuoV1Hfymz4qv+
fxmxNLA7SE1SiF8lHw80fKZZ3bJ...",
  "SigningAlgorithm": "RSASSA_PKCS1_V1_5_SHA_256"
```

```
}
```

For more information about using asymmetric KMS keys in Amazon KMS, see [Asymmetric keys in Amazon KMS](#) in the *Amazon Key Management Service Developer Guide*.

Example 2: To save a digital signature in a file (Linux and macOS)

The following `sign` example generates a cryptographic signature for a short message stored in a local file. The command also gets the `Signature` property from the response, Base64-decodes it and saves it in the `ExampleSignature` file. You can use the signature file in a `verify` command that verifies the signature.

The `sign` command requires a Base64-encoded message and a signing algorithm that your asymmetric KMS key supports. To get the signing algorithms that your KMS key supports, use the `describe-key` command.

Before running this command, replace the example key ID with a valid key ID from your Amazon account. The key ID must represent an asymmetric KMS key with a key usage of `SIGN_VERIFY`.

```
echo 'hello world' | base64 > EncodedMessage

aws kms sign \
  --key-id 1234abcd-12ab-34cd-56ef-1234567890ab \
  --message fileb://EncodedMessage \
  --message-type RAW \
  --signing-algorithm RSASSA_PKCS1_V1_5_SHA_256 \
  --output text \
  --query Signature | base64 --decode > ExampleSignature
```


This command produces no output. This example extracts the `Signature` property of the output and saves it in a file.

For more information about using asymmetric KMS keys in Amazon KMS, see [Asymmetric keys in Amazon KMS](#) in the *Amazon Key Management Service Developer Guide*.

- For API details, see [Sign](#) in *Amazon CLI Command Reference*.

Java

SDK for Java 2.x

 **Note**

There's more on GitHub. Find the complete example and learn how to set up and run in the [Amazon Code Examples Repository](#).

```
/**
 * Asynchronously signs and verifies data using AWS KMS.
 *
 * <p>The method performs the following steps:
 * <ol>
 *   <li>Creates an AWS KMS key with the specified key spec, key usage, and
origin.</li>
 *   <li>Signs the provided message using the created KMS key and the
RSASSA-PSS-SHA-256 algorithm.</li>
 *   <li>Verifies the signature of the message using the created KMS key
and the RSASSA-PSS-SHA-256 algorithm.</li>
 * </ol>
 *
 * @return a {@link CompletableFuture} that completes with the result of the
signature verification,
 *         {@code true} if the signature is valid, {@code false} otherwise.
 * @throws KmsException if any error occurs during the KMS operations.
 * @throws RuntimeException if an unexpected error occurs.
 */
public CompletableFuture<Boolean> signVerifyDataAsync() {
    String signMessage = "Here is the message that will be digitally signed";

    // Create an AWS KMS key used to digitally sign data.
    CreateKeyRequest createKeyRequest = CreateKeyRequest.builder()
        .keySpec(KeySpec.RSA_2048)
        .keyUsage(KeyUsageType.SIGN_VERIFY)
        .origin(OriginType.AWS_KMS)
        .build();

    return getAsyncClient().createKey(createKeyRequest)
        .thenCompose(createKeyResponse -> {
            String keyId = createKeyResponse.keyMetadata().keyId();
```

```
        SdkBytes messageBytes = SdkBytes.fromString(signMessage,
Charset.defaultCharset());
        SignRequest signRequest = SignRequest.builder()
            .keyId(keyId)
            .message(messageBytes)
            .signingAlgorithm(SigningAlgorithmSpec.RSASSA_PSS_SHA_256)
            .build();

        return getAsyncClient().sign(signRequest)
            .thenCompose(signResponse -> {
                byte[] signedBytes =
signResponse.signature().asByteArray();

                VerifyRequest verifyRequest = VerifyRequest.builder()
                    .keyId(keyId)

.message(SdkBytes.fromByteArray(signMessage.getBytes(Charset.defaultCharset()))))

.signature(SdkBytes.fromByteBuffer(ByteBuffer.wrap(signedBytes)))

.signingAlgorithm(SigningAlgorithmSpec.RSASSA_PSS_SHA_256)
                    .build();

                return getAsyncClient().verify(verifyRequest)
                    .thenApply(verifyResponse -> {
                        return (boolean) verifyResponse.signatureValid();
                    });
            });
    })
    .exceptionally(throwable -> {
        throw new RuntimeException("Failed to sign or verify data",
throwable);
    });
}
```

- For API details, see [Sign](#) in *Amazon SDK for Java 2.x API Reference*.

PHP

SDK for PHP

 **Note**

There's more on GitHub. Find the complete example and learn how to set up and run in the [Amazon Code Examples Repository](#).

```
/**
 * @param string $keyId
 * @param string $message
 * @param string $algorithm
 * @return Result
 */
public function sign(string $keyId, string $message, string $algorithm)
{
    try {
        return $this->client->sign([
            'KeyId' => $keyId,
            'Message' => $message,
            'SigningAlgorithm' => $algorithm,
        ]);
    } catch (KmsException $caught){
        echo "There was a problem signing the data: {$caught-
>getAwsErrorMessage()}\n";
        throw $caught;
    }
}
```

- For API details, see [Sign](#) in *Amazon SDK for PHP API Reference*.

Python

SDK for Python (Boto3)

 **Note**

There's more on GitHub. Find the complete example and learn how to set up and run in the [Amazon Code Examples Repository](#).

```
class KeyEncrypt:
    def __init__(self, kms_client):
        self.kms_client = kms_client

    @classmethod
    def from_client(cls) -> "KeyEncrypt":
        """
        Creates a KeyEncrypt instance with a default KMS client.

        :return: An instance of KeyEncrypt initialized with the default KMS
client.
        """
        kms_client = boto3.client("kms")
        return cls(kms_client)

    def sign(self, key_id: str, message: str) -> str:
        """
        Signs a message with a key.

        :param key_id: The ARN or ID of the key to use for signing.
        :param message: The message to sign.
        :return: The signature of the message.
        """
        try:
            return self.kms_client.sign(
                KeyId=key_id,
                Message=message.encode(),
                SigningAlgorithm="RSASSA_PSS_SHA_256",
            )["Signature"]
        except ClientError as err:
            logger.error(
```

```
        "Couldn't sign your message. Here's why: %s",
        err.response["Error"]["Message"],
    )
    raise
```

- For API details, see [Sign](#) in *Amazon SDK for Python (Boto3) API Reference*.

For a complete list of Amazon SDK developer guides and code examples, see [Using this service with an Amazon SDK](#). This topic also includes information about getting started and details about previous SDK versions.

Use TagResource with an Amazon SDK or CLI

The following code examples show how to use TagResource.

Action examples are code excerpts from larger programs and must be run in context. You can see this action in context in the following code example:

- [Learn the basics](#)

CLI

Amazon CLI

To add a tag to a KMS key

The following tag-resource example adds "Purpose": "Test" and "Dept": "IT" tags to a customer managed KMS key. You can use tags like these to label KMS keys and create categories of KMS keys for permissions and auditing.

To specify the KMS key, use the key-id parameter. This example uses a key ID value, but you can use a key ID or key ARN in this command.

```
aws kms tag-resource \  
  --key-id 1234abcd-12ab-34cd-56ef-1234567890ab \  
  --tags TagKey='Purpose',TagValue='Test' TagKey='Dept',TagValue='IT'
```

This command produces no output. To view the tags on an Amazon KMS KMS key, use the list-resource-tags command.

For more information about using tags in Amazon KMS, see [Tagging keys](#) in the *Amazon Key Management Service Developer Guide*.

- For API details, see [TagResource](#) in *Amazon CLI Command Reference*.

Java

SDK for Java 2.x

Note

There's more on GitHub. Find the complete example and learn how to set up and run in the [Amazon Code Examples Repository](#).

```
/**
 * Asynchronously tags a KMS key with a specific tag.
 *
 * @param keyId the ID of the KMS key to be tagged
 * @return a {@link CompletableFuture} that completes when the tagging
operation is finished
 */
public CompletableFuture<Void> tagKMSKeyAsync(String keyId) {
    Tag tag = Tag.builder()
        .tagKey("Environment")
        .tagValue("Production")
        .build();

    TagResourceRequest tagResourceRequest = TagResourceRequest.builder()
        .keyId(keyId)
        .tags(tag)
        .build();

    return getAsyncClient().tagResource(tagResourceRequest)
        .thenRun(() -> {
            logger.info("{} key was tagged", keyId);
        })
        .exceptionally(throwable -> {
            throw new RuntimeException("Failed to tag the KMS key",
throwable);
        });
}
```

- For API details, see [TagResource](#) in *Amazon SDK for Java 2.x API Reference*.

PHP

SDK for PHP

Note


There's more on GitHub. Find the complete example and learn how to set up and run in the [Amazon Code Examples Repository](#).

```
/**
 * @param string $keyId
 * @param array $tags
 * @return void
 */
public function tagResource(string $keyId, array $tags)
{
    try {
        $this->client->tagResource([
            'KeyId' => $keyId,
            'Tags' => $tags,
        ]);
    } catch (KmsException $caught){
        echo "There was a problem applying the tag(s): {$caught-
>getAwsErrorMessage()}\n";
        throw $caught;
    }
}
```

- For API details, see [TagResource](#) in *Amazon SDK for PHP API Reference*.

Python

SDK for Python (Boto3)

 **Note**

There's more on GitHub. Find the complete example and learn how to set up and run in the [Amazon Code Examples Repository](#).

```
class KeyManager:
    def __init__(self, kms_client):
        self.kms_client = kms_client
        self.created_keys = []

    @classmethod
    def from_client(cls) -> "KeyManager":
        """
        Creates a KeyManager instance with a default KMS client.

        :return: An instance of KeyManager initialized with the default KMS
        client.
        """
        kms_client = boto3.client("kms")
        return cls(kms_client)

    def tag_resource(self, key_id: str, tag_key: str, tag_value: str) -> None:
        """
        Add or edit tags on a customer managed key.

        :param key_id: The ARN or ID of the key to enable rotation for.
        :param tag_key: Key for the tag.
        :param tag_value: Value for the tag.
        """
        try:
            self.kms_client.tag_resource(
                KeyId=key_id, Tags=[{"TagKey": tag_key, "TagValue": tag_value}]
            )
        except ClientError as err:
            logging.error(
                "Couldn't add a tag for the key '%s'. Here's why: %s",
```



```
        key_id,  
        err.response["Error"]["Message"],  
    )  
    raise
```

- For API details, see [TagResource](#) in *Amazon SDK for Python (Boto3) API Reference*.

For a complete list of Amazon SDK developer guides and code examples, see [Using this service with an Amazon SDK](#). This topic also includes information about getting started and details about previous SDK versions.

Use UpdateAlias with an Amazon SDK or CLI

The following code examples show how to use UpdateAlias.

CLI

Amazon CLI

To associate an alias with a different KMS key

The following update-alias example associates the alias alias/test-key with a different KMS key.

The --alias-name parameter specifies the alias. The alias name value must begin with alias/.The --target-key-id parameter specifies the KMS key to associate with the alias. You don't need to specify the current KMS key for the alias.

```
aws kms update-alias \  
  --alias-name alias/test-key \  
  --target-key-id 1234abcd-12ab-34cd-56ef-1234567890ab
```


This command produces no output. To find the alias, use the list-aliases command.

For more information, see [Updating aliases](#) in the *Amazon Key Management Service Developer Guide*.

- For API details, see [UpdateAlias](#) in *Amazon CLI Command Reference*.

Python

SDK for Python (Boto3)

 **Note**

There's more on GitHub. Find the complete example and learn how to set up and run in the [Amazon Code Examples Repository](#).

```
class AliasManager:
    def __init__(self, kms_client):
        self.kms_client = kms_client
        self.created_key = None

    @classmethod
    def from_client(cls) -> "AliasManager":
        """
        Creates an AliasManager instance with a default KMS client.

        :return: An instance of AliasManager initialized with the default KMS
        client.
        """
        kms_client = boto3.client("kms")
        return cls(kms_client)

    def update_alias(self, alias, current_key_id):
        """
        Updates an alias by assigning it to another key.

        :param alias: The alias to reassign.
        :param current_key_id: The ARN or ID of the key currently associated with
        the alias.
        """
        new_key_id = input(
            f"Alias {alias} is currently associated with {current_key_id}. "
            f"Enter another key ID or ARN that you want to associate with
        {alias}: "
        )
        if new_key_id != "":
            try:
```

```
        self.kms_client.update_alias(AliasName=alias,
TargetKeyId=new_key_id)
    except ClientError as err:
        logger.error(
            "Couldn't associate alias %s with key %s. Here's why: %s",
            alias,
            new_key_id,
            err.response["Error"]["Message"],
        )
    else:
        print(f"Alias {alias} is now associated with key {new_key_id}.")
else:
    print("Skipping alias update.")
```

- For API details, see [UpdateAlias](#) in *Amazon SDK for Python (Boto3) API Reference*.

For a complete list of Amazon SDK developer guides and code examples, see [Using this service with an Amazon SDK](#). This topic also includes information about getting started and details about previous SDK versions.

Use Verify with an Amazon SDK or CLI

The following code examples show how to use `Verify`.

CLI

Amazon CLI

To verify a digital signature

The following `verify` example verifies a cryptographic signature for a short, Base64-encoded message. The key ID, message, message type, and signing algorithm must be same ones that were used to sign the message. The signature that you specify cannot be base64-encoded. For help decoding the signature that the `sign` command returns, see the `sign` command examples.

The output of the command includes a Boolean `SignatureValid` field that indicates that the signature was verified. If the signature validation fails, the `verify` command fails, too.

Before running this command, replace the example key ID with a valid key ID from your Amazon account.

```
aws kms verify \  
  --key-id 1234abcd-12ab-34cd-56ef-1234567890ab \  
  --message fileb://EncodedMessage \  
  --message-type RAW \  
  --signing-algorithm RSASSA_PKCS1_V1_5_SHA_256 \  
  --signature fileb://ExampleSignature
```

Output:

```
{  
  "KeyId": "arn:aws:kms:us-  
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab",  
  "SignatureValid": true,  
  "SigningAlgorithm": "RSASSA_PKCS1_V1_5_SHA_256"  
}
```

For more information about using asymmetric KMS keys in Amazon KMS, see [Using asymmetric keys](#) in the *Amazon Key Management Service Developer Guide*.

- For API details, see [Verify](#) in *Amazon CLI Command Reference*.

Python

SDK for Python (Boto3)

Note

There's more on GitHub. Find the complete example and learn how to set up and run in the [Amazon Code Examples Repository](#).

```
class KeyEncrypt:  
    def __init__(self, kms_client):  
        self.kms_client = kms_client  
  
    @classmethod  
    def from_client(cls) -> "KeyEncrypt":
```

```
"""
Creates a KeyEncrypt instance with a default KMS client.

:return: An instance of KeyEncrypt initialized with the default KMS
client.
"""
kms_client = boto3.client("kms")
return cls(kms_client)

def verify(self, key_id: str, message: str, signature: str) -> bool:
    """
    Verifies a signature against a message.

    :param key_id: The ARN or ID of the key used to sign the message.
    :param message: The message to verify.
    :param signature: The signature to verify.
    :return: True when the signature matches the message, otherwise False.
    """
    try:
        response = self.kms_client.verify(
            KeyId=key_id,
            Message=message.encode(),
            Signature=signature,
            SigningAlgorithm="RSASSA_PSS_SHA_256",
        )
        valid = response["SignatureValid"]
        print(f"The signature is {'valid' if valid else 'invalid'}.")
        return valid
    except ClientError as err:
        if err.response["Error"]["Code"] == "SignatureDoesNotMatchException":
            print("The signature is not valid.")
        else:
            logger.error(
                "Couldn't verify your signature. Here's why: %s",
                err.response["Error"]["Message"],
            )
        raise
```

- For API details, see [Verify](#) in *Amazon SDK for Python (Boto3) API Reference*.

For a complete list of Amazon SDK developer guides and code examples, see [Using this service with an Amazon SDK](#). This topic also includes information about getting started and details about previous SDK versions.

Cryptographic attestation for Amazon Nitro Enclaves

Amazon KMS supports *cryptographic attestation* for [Amazon Nitro Enclaves](#). Applications that support Amazon Nitro Enclaves call the following Amazon KMS cryptographic operations with a signed attestation document for the enclave. These Amazon KMS APIs verify that the attestation document came from a Nitro enclave. Then, instead of returning plaintext data in the response, these APIs encrypt the plaintext with the public key from the attestation document and return ciphertext that can be decrypted only by the corresponding private key in the enclave.

- [Decrypt](#)
- [DeriveSharedSecret](#)
- [GenerateDataKey](#)
- [GenerateDataKeyPair](#)
- [GenerateRandom](#)

The following table shows how the response to Nitro enclave requests differs from the standard response for each API operation.

Amazon KMS operation	Standard response	Response for Amazon Nitro Enclaves
Decrypt	Returns plaintext data	Returns the plaintext data encrypted by the public key from the attestation document
DeriveSharedSecret	Returns raw shared secret	Returns the raw shared secret encrypted by the public key from the attestation document
GenerateDataKey	Returns a plaintext copy of the data key	Returns a copy of the data key encrypted by the public key from the attestation document

Amazon KMS operation	Standard response	Response for Amazon Nitro Enclaves
	(Also returns a copy of the data key encrypted by a KMS key)	(Also returns a copy of the data key encrypted by a KMS key)
GenerateDataKeyPair	Returns a plaintext copy of the private key (Also returns the public key and a copy of the private key encrypted by a KMS key)	Returns a copy of the private key encrypted by the public key from the attestation document (Also returns the public key and a copy of the private key encrypted by a KMS key)
GenerateRandom	Returns a random byte string	Returns the random byte string encrypted by the public key from the attestation document

Amazon KMS supports [policy condition keys](#) that you can use to allow or deny enclave operations with an Amazon KMS key based on the content of the attestation document. You can also [monitor requests to Amazon KMS for your Nitro enclave](#) in your Amazon CloudTrail logs.

Learn more

- [Cryptographic attestation](#)
- [Amazon KMS condition keys for Amazon Nitro Enclaves](#)
- [How to call Amazon KMS APIs for a Nitro enclave](#)
- [Monitoring requests for Nitro enclaves](#)

How to call Amazon KMS APIs for a Nitro enclave

To call Amazon KMS APIs for a Nitro enclave, use the `Recipient` parameter in the request to provide the signed attestation document for the enclave and the encryption algorithm to use with the enclave's public key. When a request includes the `Recipient` parameter with a

signed attestation document, the response includes a `CiphertextForRecipient` field with the ciphertext encrypted by the public key. The plaintext field is null or empty.

The `Recipient` parameter must specify a signed attestation document from an Amazon Nitro enclave. Amazon KMS relies on the digital signature for the enclave's attestation document to prove that the public key in the request came from a valid enclave. You cannot supply your own certificate to digitally sign the attestation document.

To specify the `Recipient` parameter, use the [Amazon Nitro Enclaves SDK](#) or any Amazon SDK. The Amazon Nitro Enclaves SDK, which is supported only within a Nitro enclave, automatically adds the `Recipient` parameter and its values to every Amazon KMS request. To make requests for Nitro enclaves in the Amazon SDKs, you have to specify the `Recipient` parameter and its values. Support for Nitro enclave cryptographic attestation in the Amazon SDKs was introduced in March 2023.

Amazon KMS supports [policy condition keys](#) that you can use to allow or deny enclave operations with an Amazon KMS key based on the content of the attestation document. You can also [monitor requests to Amazon KMS for your Nitro enclave](#) in your Amazon CloudTrail logs.

For detailed information about the `Recipient` parameter and the AWS `CiphertextForRecipient` response field, see the [Decrypt](#), [DeriveSharedSecret](#), [GenerateDataKey](#), [GenerateDataKeyPair](#), and [GenerateRandom](#) topics in the *Amazon Key Management Service API Reference*, the [Amazon Nitro Enclaves SDK](#), or any Amazon SDK. For information about setting up your data and data keys for encryption, see [Using cryptographic attestation with Amazon KMS](#).

Monitoring requests for Nitro enclaves

You can use your Amazon CloudTrail logs to monitor [Decrypt](#), [DeriveSharedSecret](#), [GenerateDataKey](#), [GenerateDataKeyPair](#), and [GenerateRandom](#) operations for an Amazon Nitro enclave. In these log entries, the `additionalEventData` field has a `recipient` field with the module ID (`attestationDocumentModuleId`), image digest (`attestationDocumentEnclaveImageDigest`), and platform configuration registers (PCRs) from the attestation document in the request. These fields are included only when the `Recipient` parameter in the request specifies a signed attestation document from an Amazon Nitro enclave.

The module ID is the [enclave ID](#) of the Nitro enclave. The image digest is the SHA384 hash of the enclave image. You can use the image digest and PCR values in [conditions for key policies and](#)

[IAM policies](#). For information about the PCRs, see [Where to get an enclave's measurements](#) in the *Amazon Nitro Enclaves User Guide*.

This section shows an example CloudTrail log entry for each of the supported Nitro enclave requests to Amazon KMS.

Decrypt (for an enclave)

The following example shows an Amazon CloudTrail log entry of a [Decrypt](#) operation for an Amazon Nitro enclave.

```
{
  "eventVersion": "1.05",
  "userIdentity": {
    "type": "IAMUser",
    "principalId": "EX_PRINCIPAL_ID",
    "arn": "arn:aws:iam::111122223333:user/Alice",
    "accountId": "111122223333",
    "accessKeyId": "EXAMPLE_KEY_ID",
    "userName": "Alice"
  },
  "eventTime": "2020-07-27T22:58:24Z",
  "eventSource": "kms.amazonaws.com",
  "eventName": "Decrypt",
  "awsRegion": "us-west-2",
  "sourceIPAddress": "192.0.2.0",
  "userAgent": "Amazon Internal",
  "requestParameters": {
    "encryptionAlgorithm": "SYMMETRIC_DEFAULT",
    "keyId": "arn:aws:kms:us-west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab"
  },
  "responseElements": null,
  "additionalEventData": {
    "recipient": {
      "attestationDocumentModuleId": "i-123456789abcde123-enc123456789abcde12",
      "attestationDocumentEnclaveImageDigest": "<AttestationDocument.PCR0>",
      "attestationDocumentEnclavePCR1": "<AttestationDocument.PCR1>",
      "attestationDocumentEnclavePCR2": "<AttestationDocument.PCR2>",
      "attestationDocumentEnclavePCR3": "<AttestationDocument.PCR3>",
      "attestationDocumentEnclavePCR4": "<AttestationDocument.PCR4>",
      "attestationDocumentEnclavePCR8": "<AttestationDocument.PCR8>"
    }
  }
}
```

```

    },
    "requestID": "b4a65126-30d5-4b28-98b9-9153da559963",
    "eventID": "e5a2f202-ba1a-467c-b4ba-f729d45ae521",
    "readOnly": true,
    "resources": [
      {
        "accountId": "111122223333",
        "type": "AWS::KMS::Key",
        "ARN": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab"
      }
    ],
    "eventType": "AwsApiCall",
    "recipientAccountId": "111122223333"
  }
}

```

GenerateDataKey (for an enclave)

The following example shows an Amazon CloudTrail log entry of a [GenerateDataKey](#) operation for an Amazon Nitro enclave.

```

{
  "eventVersion": "1.02",
  "userIdentity": {
    "type": "IAMUser",
    "principalId": "EX_PRINCIPAL_ID",
    "arn": "arn:aws:iam::111122223333:user/Alice",
    "accountId": "111122223333",
    "accessKeyId": "EXAMPLE_KEY_ID",
    "userName": "Alice"
  },
  "eventTime": "2014-11-04T00:52:40Z",
  "eventSource": "kms.amazonaws.com",
  "eventName": "GenerateDataKey",
  "awsRegion": "us-east-1",
  "sourceIPAddress": "192.0.2.0",
  "userAgent": "Amazon Internal",
  "requestParameters": {
    "keyId": "1234abcd-12ab-34cd-56ef-1234567890ab",
    "numberOfBytes": 32
  },
  "responseElements": null,
  "additionalEventData": {

```

```

    "recipient": {
      "attestationDocumentModuleId": "i-123456789abcde123-enc123456789abcde12",
      "attestationDocumentEnclaveImageDigest": "<AttestationDocument.PCR0>",
      "attestationDocumentEnclavePCR1": "<AttestationDocument.PCR1>",
      "attestationDocumentEnclavePCR2": "<AttestationDocument.PCR2>",
      "attestationDocumentEnclavePCR3": "<AttestationDocument.PCR3>",
      "attestationDocumentEnclavePCR4": "<AttestationDocument.PCR4>",
      "attestationDocumentEnclavePCR8": "<AttestationDocument.PCR8>"
    }
  },
  "requestID": "e0eb83e3-63bc-11e4-bc2b-4198b6150d5c",
  "eventID": "a9dea4f9-8395-46c0-942c-f509c02c2b71",
  "readOnly": true,
  "resources": [{
    "ARN": "arn:aws:kms:us-west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab",
    "accountId": "111122223333"
  }],
  "eventType": "AwsApiCall",
  "recipientAccountId": "111122223333"
}

```

GenerateDataKeyPair (for an enclave)

The following example shows an Amazon CloudTrail log entry of a [GenerateDataKeyPair](#) operation for an Amazon Nitro enclave.

```

{
  "eventVersion": "1.05",
  "userIdentity": {
    "type": "IAMUser",
    "principalId": "EX_PRINCIPAL_ID",
    "arn": "arn:aws:iam::111122223333:user/Alice",
    "accountId": "111122223333",
    "accessKeyId": "EXAMPLE_KEY_ID",
    "userName": "Alice"
  },
  "eventTime": "2020-07-27T18:57:57Z",
  "eventSource": "kms.amazonaws.com",
  "eventName": "GenerateDataKeyPair",
  "awsRegion": "us-west-2",
  "sourceIPAddress": "192.0.2.0",
  "userAgent": "Amazon Internal",

```

```

"requestParameters": {
  "keyPairSpec": "RSA_3072",
  "encryptionContext": {
    "Project": "Alpha"
  },
  "keyId": "1234abcd-12ab-34cd-56ef-1234567890ab"
},
"responseElements": null,
"additionalEventData": {
  "recipient": {
    "attestationDocumentModuleId": "i-123456789abcde123-enc123456789abcde12",
    "attestationDocumentEnclaveImageDigest": "<AttestationDocument.PCR0>",
    "attestationDocumentEnclavePCR1": "<AttestationDocument.PCR1>",
    "attestationDocumentEnclavePCR2": "<AttestationDocument.PCR2>",
    "attestationDocumentEnclavePCR3": "<AttestationDocument.PCR3>",
    "attestationDocumentEnclavePCR4": "<AttestationDocument.PCR4>",
    "attestationDocumentEnclavePCR8": "<AttestationDocument.PCR8>"
  }
},
"requestID": "52fb127b-0fe5-42bb-8e5e-f560febde6b0",
"eventID": "9b6bd6d2-529d-4890-a949-593b13800ad7",
"readOnly": true,
"resources": [
  {
    "accountId": "111122223333",
    "type": "AWS::KMS::Key",
    "ARN": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab"
  }
],
"eventType": "AwsApiCall",
"recipientAccountId": "111122223333"
}

```

GenerateRandom (for an enclave)

The following example shows an Amazon CloudTrail log entry of a [GenerateRandom](#) operation for an Amazon Nitro enclave.

```

{
  "eventVersion": "1.02",
  "userIdentity": {
    "type": "IAMUser",

```

```
    "principalId": "EX_PRINCIPAL_ID",
    "arn": "arn:aws:iam::111122223333:user/Alice",
    "accountId": "111122223333",
    "accessKeyId": "EXAMPLE_KEY_ID",
    "userName": "Alice"
  },
  "eventTime": "2014-11-04T00:52:37Z",
  "eventSource": "kms.amazonaws.com",
  "eventName": "GenerateRandom",
  "awsRegion": "us-east-1",
  "sourceIPAddress": "192.0.2.0",
  "userAgent": "Amazon Internal",
  "requestParameters": null,
  "responseElements": null,
  "additionalEventData": {
    "recipient": {
      "attestationDocumentModuleId": "i-123456789abcde123-enc123456789abcde12",
      "attestationDocumentEnclaveImageDigest": "<AttestationDocument.PCR0>",
      "attestationDocumentEnclavePCR1": "<AttestationDocument.PCR1>",
      "attestationDocumentEnclavePCR2": "<AttestationDocument.PCR2>",
      "attestationDocumentEnclavePCR3": "<AttestationDocument.PCR3>",
      "attestationDocumentEnclavePCR4": "<AttestationDocument.PCR4>",
      "attestationDocumentEnclavePCR8": "<AttestationDocument.PCR8>"
    }
  },
  "requestID": "df1e3de6-63bc-11e4-bc2b-4198b6150d5c",
  "eventID": "239cb9f7-ae05-4c94-9221-6ea30eef0442",
  "readOnly": true,
  "resources": [],
  "eventType": "AwsApiCall",
  "recipientAccountId": "111122223333"
}
```

Using Amazon KMS encryption with Amazon services

With Amazon Key Management Service, you can provide encryption keys for protecting data in other Amazon services. Using Amazon KMS encryption with Amazon services refers to the process of integrating Amazon KMS with other Amazon services to encrypt and decrypt data at rest or in transit. Developers, system administrators, and security professionals might be interested in this topic to secure sensitive data stored or transmitted through Amazon services, meet regulatory compliance requirements, or implement encryption best practices. Common use cases include encrypting Amazon EBS volumes, Amazon S3 buckets, and Amazon RDS databases. The following sections will cover the steps to configure and manage Amazon KMS encryption keys for specific Amazon services, ensuring data confidentiality and integrity across your Amazon environment. For the complete list of Amazon services integrated with Amazon KMS, see [Amazon Service Integration](#).

The following topics discuss in detail how particular services use Amazon KMS, including the KMS keys they support, how they manage data keys, the permissions they require, and how to track each service's use of the KMS keys in your account.

Important

[Amazon services that are integrated with Amazon KMS](#) use only symmetric encryption KMS keys to encrypt your data. These services do not support encryption with asymmetric KMS keys. For help determining whether a KMS key is symmetric or asymmetric, see [Identify different key types](#).

Topics

- [How Amazon Elastic Block Store \(Amazon EBS\) uses Amazon KMS](#)
- [How Amazon EMR uses Amazon KMS](#)
- [How Amazon Redshift uses Amazon KMS](#)

How Amazon Elastic Block Store (Amazon EBS) uses Amazon KMS

This topic discusses in detail how [Amazon Elastic Block Store \(Amazon EBS\)](#) uses Amazon KMS to encrypt volumes and snapshots. For basic instructions about encrypting Amazon EBS volumes, see [Amazon EBS Encryption](#).

Topics

- [Amazon EBS encryption](#)
- [Using KMS keys and data keys](#)
- [Amazon EBS encryption context](#)
- [Detecting Amazon EBS failures](#)
- [Using Amazon CloudFormation to create encrypted Amazon EBS volumes](#)

Amazon EBS encryption

When you attach an encrypted Amazon EBS volume to a [supported Amazon Elastic Compute Cloud \(Amazon EC2\) instance type](#), data stored at rest on the volume, disk I/O, and snapshots created from the volume are all encrypted. The encryption occurs on the servers that host Amazon EC2 instances.

This feature is supported on all [Amazon EBS volume types](#). You access encrypted volumes the same way you access other volumes; encryption and decryption are handled transparently and they require no additional action from you, your EC2 instance, or your application. Snapshots of encrypted volumes are automatically encrypted, and volumes that are created from encrypted snapshots are also automatically encrypted.

The encryption status of an EBS volume is determined when you create the volume. You cannot change the encryption status of an existing volume. However, you can [migrate data](#) between encrypted and unencrypted volumes and apply a new encryption status while copying a snapshot.

Amazon EBS supports optional encryption by default. You can enable encryption automatically on all new EBS volumes and snapshot copies in your Amazon Web Services account and Region. This configuration setting doesn't affect existing volumes or snapshots. For details, see [Amazon EBS encryption](#) in the *Amazon EBS User Guide*.

Using KMS keys and data keys

When you [create an encrypted Amazon EBS volume](#), you specify an Amazon KMS key. By default, Amazon EBS uses the [Amazon managed key](#) for Amazon EBS in your account (aws/ebs). However, you can specify a [customer managed key](#) that you create and manage.

To use a customer managed key, you must give Amazon EBS permission to use the KMS key on your behalf. For a list of required permissions, see *Permissions for IAM users* in the [Amazon EC2 User Guide](#) or [Amazon EC2 User Guide](#).

Important

Amazon EBS supports only [symmetric KMS keys](#). You cannot use an [asymmetric KMS key](#) to encrypt an Amazon EBS volume. For help determining whether a KMS key is symmetric or asymmetric, see [Identify different key types](#).

For each volume, Amazon EBS asks Amazon KMS to generate a unique data key encrypted under the KMS key that you specify. Amazon EBS stores the encrypted data key with the volume. Then, when you attach the volume to an Amazon EC2 instance, Amazon EBS calls Amazon KMS to decrypt the data key. Amazon EBS uses the plaintext data key in hypervisor memory to encrypt all disk I/O to the volume. For details, see *How EBS encryption works* in the [Amazon EC2 User Guide](#) or [Amazon EC2 User Guide](#).

Amazon EBS encryption context

In its [GenerateDataKeyWithoutPlaintext](#) and [Decrypt](#) requests to Amazon KMS, Amazon EBS uses an encryption context with a name-value pair that identifies the volume or snapshot in the request. The name in the encryption context does not vary.

An [encryption context](#) is a set of key-value pairs that contain arbitrary nonsecret data. When you include an encryption context in a request to encrypt data, Amazon KMS cryptographically binds the encryption context to the encrypted data. To decrypt the data, you must pass in the same encryption context.

For all volumes and for encrypted snapshots created with the Amazon EBS [CreateSnapshot](#) operation, Amazon EBS uses the volume ID as encryption context value. In the `requestParameters` field of a CloudTrail log entry, the encryption context looks similar to the following:

```
"encryptionContext": {  
  "aws:ebs:id": "vol-0cfb133e847d28be9"  
}
```

For encrypted snapshots created with the Amazon EC2 [CopySnapshot](#) operation, Amazon EBS uses the snapshot ID as encryption context value. In the `requestParameters` field of a CloudTrail log entry, the encryption context looks similar to the following:

```
"encryptionContext": {  
  "aws:ebs:id": "snap-069a655b568de654f"  
}
```

Detecting Amazon EBS failures

To create an encrypted EBS volume or attach the volume to an EC2 instance, Amazon EBS and the Amazon EC2 infrastructure must be able to use the KMS key that you specified for EBS volume encryption. When the KMS key is not usable—for example, when its [key state](#) is not `Enabled`—the volume creation or volume attachment fails.

In this case, Amazon EBS sends an *event* to Amazon EventBridge (formerly CloudWatch Events) to notify you about the failure. In EventBridge, you can establish rules that trigger automatic actions in response to these events. For more information, see [Amazon CloudWatch Events for Amazon EBS](#) in the *Amazon EC2 User Guide*, especially the following sections:

- [Invalid Encryption Key on Volume Attach or Reattach](#)
- [Invalid Encryption Key on Create Volume](#)

To fix these failures, ensure that the KMS key that you specified for EBS volume encryption is enabled. To do this, first [view the KMS key](#) to determine its current key state (the **Status** column in the Amazon Web Services Management Console). Then, see the information at one of the following links:

- If the KMS key's key state is disabled, [enable it](#).
- If the KMS key's key state is pending import, [import key material](#).
- If the KMS key's key state is pending deletion, [cancel key deletion](#).

Using Amazon CloudFormation to create encrypted Amazon EBS volumes

You can use [Amazon CloudFormation](#) to create encrypted Amazon EBS volumes. For more information, see [AWS::EC2::Volume](#) in the *Amazon CloudFormation User Guide*.

How Amazon EMR uses Amazon KMS

When you use an [Amazon EMR](#) cluster, you can configure the cluster to encrypt data *at rest* before saving it to a persistent storage location. You can encrypt data at rest on the EMR File System (EMRFS), on the storage volumes of cluster nodes, or both. To encrypt data at rest, you can use an Amazon KMS key. The following topics explain how an Amazon EMR cluster uses a KMS key to encrypt data at rest.

Important

Amazon EMR supports only [symmetric KMS keys](#). You cannot use an [asymmetric KMS key](#) to encrypt data at rest in an Amazon EMR cluster. For help determining whether a KMS key is symmetric or asymmetric, see [Identify different key types](#).

Amazon EMR clusters also encrypt data *in transit*, which means the cluster encrypts data before sending it through the network. You cannot use a KMS key to encrypt data in transit. For more information, see [In-Transit Data Encryption](#) in the *Amazon EMR Management Guide*.

For more information about all the encryption options available in Amazon EMR, see [Encryption Options](#) in the *Amazon EMR Management Guide*.

Topics

- [Encrypting data on the EMR file system \(EMRFS\)](#)
- [Encrypting data on the storage volumes of cluster nodes](#)
- [Encryption context](#)

Encrypting data on the EMR file system (EMRFS)

Amazon EMR clusters use two distributed files systems:

- The Hadoop Distributed File System (HDFS). HDFS encryption does not use a KMS key in Amazon KMS.
- The EMR File System (EMRFS). EMRFS is an implementation of HDFS that allows Amazon EMR clusters to store data in Amazon Simple Storage Service (Amazon S3). EMRFS supports four encryption options, two of which use a KMS key in Amazon KMS. For more information about all four of the EMRFS encryption options, see [Encryption Options](#) in the *Amazon EMR Management Guide*.

The two EMRFS encryption options that use a KMS key use the following encryption features offered by Amazon S3:

- [Protecting data using server-side encryption with Amazon Key Management Service \(SSE-KMS\)](#). The Amazon EMR cluster sends data to Amazon S3. Amazon S3 uses a KMS key to encrypt the data before saving it to an S3 bucket. For more information about how this works, see [Process for encrypting data on EMRFS with SSE-KMS](#).
- [Protecting data using client-side encryption](#) (CSE-KMS). Data in an Amazon EMR is encrypted under an Amazon KMS key before it's sent to Amazon S3 for storage. For more information about how this works, see [Process for encrypting data on EMRFS with CSE-KMS](#).

When you configure an Amazon EMR cluster to encrypt data on EMRFS with a KMS key, you choose the KMS key that you want Amazon S3 or the Amazon EMR cluster to use. With SSE-KMS, you can choose the Amazon managed key for Amazon S3 with the alias `aws/s3`, or a symmetric customer managed key that you create. With client-side encryption, you must choose a symmetric customer managed key that you create. When you choose a customer managed key, you must ensure that your Amazon EMR cluster has permission to use the KMS key. For more information, see [Using Amazon KMS keys for encryption](#) in the *Amazon EMR Management Guide*.

For both server-side and client-side encryption, the KMS key you choose is the root key in an [envelope encryption](#) workflow. The data is encrypted with a unique [data key](#) that is encrypted under the KMS key in Amazon KMS. The encrypted data and an encrypted copy of its data key are stored together as a single encrypted object in an S3 bucket. For more information about how this works, see the following topics.

Topics

- [Process for encrypting data on EMRFS with SSE-KMS](#)
- [Process for encrypting data on EMRFS with CSE-KMS](#)

Process for encrypting data on EMRFS with SSE-KMS

When you configure an Amazon EMR cluster to use SSE-KMS, the encryption process works like this:

1. The cluster sends data to Amazon S3 for storage in an S3 bucket.
2. Amazon S3 sends a [GenerateDataKey](#) request to Amazon KMS, specifying the key ID of the KMS key that you chose when you configured the cluster to use SSE-KMS. The request includes encryption context; for more information, see [Encryption context](#).
3. Amazon KMS generates a unique data encryption key (data key) and then sends two copies of this data key to Amazon S3. One copy is unencrypted (plaintext), and the other copy is encrypted under the KMS key.
4. Amazon S3 uses the plaintext data key to encrypt the data that it received in step 1, and then removes the plaintext data key from memory as soon as possible after use.
5. Amazon S3 stores the encrypted data and the encrypted copy of the data key together as a single encrypted object in an S3 bucket.

The decryption process works like this:

1. The cluster requests an encrypted data object from an S3 bucket.
2. Amazon S3 extracts the encrypted data key from the S3 object, and then sends the encrypted data key to Amazon KMS with a [Decrypt](#) request. The request includes an [encryption context](#).
3. Amazon KMS decrypts the encrypted data key using the same KMS key that was used to encrypt it, and then sends the decrypted (plaintext) data key to Amazon S3.
4. Amazon S3 uses the plaintext data key to decrypt the encrypted data, and then removes the plaintext data key from memory as soon as possible after use.
5. Amazon S3 sends the decrypted data to the cluster.

Process for encrypting data on EMRFS with CSE-KMS

When you configure an Amazon EMR cluster to use CSE-KMS, the encryption process works like this:

1. When it's ready to store data in Amazon S3, the cluster sends a [GenerateDataKey](#) request to Amazon KMS, specifying the key ID of the KMS key that you chose when you configured the

- cluster to use CSE-KMS. The request includes encryption context; for more information, see [Encryption context](#).
2. Amazon KMS generates a unique data encryption key (data key) and then sends two copies of this data key to the cluster. One copy is unencrypted (plaintext), and the other copy is encrypted under the KMS key.
 3. The cluster uses the plaintext data key to encrypt the data, and then removes the plaintext data key from memory as soon as possible after use.
 4. The cluster combines the encrypted data and the encrypted copy of the data key together into a single encrypted object.
 5. The cluster sends the encrypted object to Amazon S3 for storage.

The decryption process works like this:

1. The cluster requests the encrypted data object from an S3 bucket.
2. Amazon S3 sends the encrypted object to the cluster.
3. The cluster extracts the encrypted data key from the encrypted object, and then sends the encrypted data key to Amazon KMS with a [Decrypt](#) request. The request includes [encryption context](#).
4. Amazon KMS decrypts the encrypted data key using the same KMS key that was used to encrypt it, and then sends the decrypted (plaintext) data key to the cluster.
5. The cluster uses the plaintext data key to decrypt the encrypted data, and then removes the plaintext data key from memory as soon as possible after use.

Encrypting data on the storage volumes of cluster nodes

An Amazon EMR cluster is a collection of Amazon Elastic Compute Cloud (Amazon EC2) instances. Each instance in the cluster is called a *cluster node* or *node*. Each node can have two types of storage volumes: instance store volumes, and Amazon Elastic Block Store (Amazon EBS) volumes. You can configure the cluster to use [Linux Unified Key Setup \(LUKS\)](#) to encrypt both types of storage volumes on the nodes (but not the boot volume of each node). This is called *local disk encryption*.

When you enable local disk encryption for a cluster, you can choose to encrypt the LUKS key with a KMS key in Amazon KMS. You must choose a [customer managed key](#) that you create; you cannot use an [Amazon managed key](#). If you choose a customer managed key, you must ensure that your

Amazon EMR cluster has permission to use the KMS key. For more information, see [Using Amazon KMS keys for encryption](#) in the *Amazon EMR Management Guide*.

When you enable local disk encryption using a KMS key, the encryption process works like this:

1. When each cluster node launches, it sends a [GenerateDataKey](#) request to Amazon KMS, specifying the key ID of the KMS key that you chose when you enabled local disk encryption for the cluster.
2. Amazon KMS generates a unique data encryption key (data key) and then sends two copies of this data key to the node. One copy is unencrypted (plaintext), and the other copy is encrypted under the KMS key.
3. The node uses a base64-encoded version of the plaintext data key as the password that protects the LUKS key. The node saves the encrypted copy of the data key on its boot volume.
4. If the node reboots, the rebooted node sends the encrypted data key to Amazon KMS with a [Decrypt](#) request.
5. Amazon KMS decrypts the encrypted data key using the same KMS key that was used to encrypt it, and then sends the decrypted (plaintext) data key to the node.
6. The node uses the base64-encoded version of the plaintext data key as the password to unlock the LUKS key.

Encryption context

Each Amazon service integrated with Amazon KMS can specify an [encryption context](#) when the service uses Amazon KMS to generate data keys or to encrypt or decrypt data. Encryption context is additional authenticated information that Amazon KMS uses to check for data integrity. When a service specifies encryption context for an encryption operation, it must specify the same encryption context for the corresponding decryption operation or decryption will fail. Encryption context is also written to Amazon CloudTrail log files, which can help you understand why a specific KMS key was used.

The following section explain the encryption context that is used in each Amazon EMR encryption scenario that uses a KMS key.

Encryption context for EMRFS encryption with SSE-KMS

With SSE-KMS, the Amazon EMR cluster sends data to Amazon S3, and then Amazon S3 uses a KMS key to encrypt the data before saving it to an S3 bucket. In this case, Amazon S3 uses the

Amazon Resource Name (ARN) of the S3 object as encryption context with each [GenerateDataKey](#) and [Decrypt](#) request that it sends to Amazon KMS. The following example shows a JSON representation of the encryption context that Amazon S3 uses.

```
{ "aws:s3:arn" : "arn:aws:s3:::S3_bucket_name/S3_object_key" }
```

Encryption context for EMRFS encryption with CSE-KMS

With CSE-KMS, the Amazon EMR cluster uses a KMS key to encrypt data before sending it to Amazon S3 for storage. In this case, the cluster uses the Amazon Resource Name (ARN) of the KMS key as encryption context with each [GenerateDataKey](#) and [Decrypt](#) request that it sends to Amazon KMS. The following example shows a JSON representation of the encryption context that the cluster uses.

```
{ "kms_cmk_id" : "arn:aws:kms:us-east-2:111122223333:key/0987ab65-43cd-21ef-09ab-87654321cdef" }
```

Encryption context for local disk encryption with LUKS

When an Amazon EMR cluster uses local disk encryption with LUKS, the cluster nodes do not specify encryption context with the [GenerateDataKey](#) and [Decrypt](#) requests that they send to Amazon KMS.

How Amazon Redshift uses Amazon KMS

This topic discusses how Amazon Redshift uses Amazon KMS to encrypt data.

Topics

- [Amazon Redshift encryption](#)
- [Encryption context](#)

Amazon Redshift encryption

An Amazon Redshift data warehouse is a collection of computing resources called nodes, which are organized into a group called a cluster. Each cluster runs an Amazon Redshift engine and contains one or more databases.

Amazon Redshift uses a four-tier, key-based architecture for encryption. The architecture consists of data encryption keys, a database key, a cluster key, and a root key. You can use an Amazon KMS key as the root key.

Data encryption keys encrypt data blocks in the cluster. Each data block is assigned a randomly-generated AES-256 key. These keys are encrypted by using the database key for the cluster.

The database key encrypts data encryption keys in the cluster. The database key is a randomly-generated AES-256 key. It is stored on disk in a separate network from the Amazon Redshift cluster and passed to the cluster across a secure channel.

The cluster key encrypts the database key for the Amazon Redshift cluster. You can use Amazon KMS, Amazon CloudHSM, or an external hardware security module (HSM) to manage the cluster key. See the [Amazon Redshift Database Encryption](#) documentation for more details.

You can request encryption by checking the appropriate box in the Amazon Redshift console. You can specify a [customer managed key](#) by choosing one from the list that appears below the encryption box. If you do not specify a customer managed key, Amazon Redshift uses the [Amazon managed key](#) for Amazon Redshift under your account.

Important

Amazon Redshift supports only symmetric encryption KMS keys. You cannot use an asymmetric KMS key in an Amazon Redshift encryption workflow. For help determining whether a KMS key is symmetric or asymmetric, see [Identify different key types](#).

Encryption context

Each service that is integrated with Amazon KMS specifies an [encryption context](#) when requesting data keys, encrypting, and decrypting. The encryption context is additional authenticated data (AAD) that Amazon KMS uses to check for data integrity. That is, when an encryption context is specified for an encryption operation, the service also specifies it for the decryption operation or decryption will not succeed. Amazon Redshift uses the cluster ID and the creation time for the encryption context. In the `requestParameters` field of a CloudTrail log file, the encryption context will look similar to this.

```
"encryptionContext": {
```

```
"aws:redshift:arn": "arn:aws:redshift:region:account_ID:cluster:cluster_name",  
"aws:redshift:createtime": "20150206T1832Z"  
},
```

You can search on the cluster name in your CloudTrail logs to understand what operations were performed by using an Amazon KMS key (KMS key). The operations include cluster encryption, cluster decryption, and generating data keys.

Amazon KMS Reference

The following reference material provide useful information about using and managing KMS keys.

- [Key type reference](#). Lists the type of KMS key that supports each Amazon KMS API operation.

To find: Can I enable and disable an RSA signing KMS key?

- [Key state table](#). Shows how the key state of a KMS key affects its use in Amazon KMS API operations.

To find: Can I change the alias of a KMS key that is pending deletion?

- [Amazon KMSAPI permissions reference](#). Provides information about the permissions required for each Amazon KMS API operation.

To find: Can I run [GetKeyPolicy](#) on a key in a different Amazon account? Can I allow `kms:Decrypt` permission in an IAM policy?

- [ViaService reference](#). Lists the Amazon services that support the `kms:ViaService` condition key.

To find: Can I use the `kms:ViaService` condition key to allow a permission only when it comes from Amazon ElastiCache? What about Amazon Neptune?

- [Amazon KMS pricing](#). Lists and explains the price of KMS keys.

To find: How much does it cost to use my asymmetric keys?

- [Amazon KMS request quotas](#). Lists the per-second quotas for Amazon KMS API requests in each account and Region.

To find: How many [Decrypt](#) requests can I run in each second? How many [Decrypt](#) requests can I run on KMS keys in my custom key store?

- [Amazon KMS resource quotas](#). Lists the quotas on Amazon KMS resources.

To find: How many KMS key can I have in each Region of my account? How many aliases can I have on each KMS key?

- [Amazon services integrated with Amazon KMS](#). Lists the Amazon services that use KMS keys to protect the resources that they create, store, and manage.

To find: Does Amazon Connect use KMS keys to protect my Connect resources?

Key states of Amazon KMS keys

An Amazon KMS key always has a key state. Operations on the KMS key and its environment can change that key state, either transiently, or until another operation changes its key state.

The table in this section shows how key states affect calls to Amazon KMS API operations. As a result of its key state, an operation on a KMS key is expected to succeed (#), fail (X), or succeed only under certain conditions (?). The result often differs for KMS keys with imported key material.

This table includes only the API operations that use an existing KMS key. Other operations, such as [CreateKey](#) and [ListKeys](#), are omitted.

Topics

- [Key states and KMS key types](#)
- [Key state table](#)

Key states and KMS key types

The type of the KMS key determines the key states it can have.

- All KMS keys can be in the Enabled, Disabled, and PendingDeletion states.
- Most KMS keys are created in the Enabled state. Keys with imported key material are created in the PendingImport state.
- The PendingImport state applies only to KMS keys with [imported key material](#).
- The Unavailable state applies only to a KMS key in a [custom key store](#). A KMS key in an [Amazon CloudHSM key store](#) is Unavailable when the custom key store is intentionally disconnected from its Amazon CloudHSM cluster. A KMS key in an [external key store](#) is Unavailable when the custom key store is intentionally disconnected from its [external key store proxy](#). You can view and manage unavailable KMS keys, but you cannot use them in cryptographic operations.

The key state of a KMS key in a custom key store is not affected by changes to its backing key. A KMS key in a Amazon CloudHSM key store is not affected by changes to its [associated key material](#) in the Amazon CloudHSM cluster. A KMS key in an external key store is not affected by changes to its [external key](#) in an external key manager. If the backing key is disabled or deleted, the KMS key state doesn't change, but cryptographic operations using the KMS key fail.

- The `Creating`, `Updating`, and `PendingReplicaDeletion` key states apply only to [multi-Region keys](#).
 - A multi-Region replica key is in the transient `Creating` key state while it is being created. This process might still be in progress when the [ReplicateKey](#) operation completes. When the replicate process completes, the replica key is in the `Enabled` or `PendingImport` state.
 - Multi-Region keys are in the transient `Updating` key state while the primary Region is being updated. This process might still be in progress when the [UpdatePrimaryRegion](#) operation completes. When the update process completes, the primary and replica keys resume the `Enabled` key state.
 - When you schedule deletion of a multi-Region primary key that has replica keys, the primary key is in the `PendingReplicaDeletion` state until all of its replica keys are deleted. Then its key state changes to `PendingDeletion`. For details, see [Deleting multi-Region keys](#).















Key state table

The following table shows how the key state of a KMS key affects Amazon KMS operations.

The descriptions of the numbered footnotes ([n]) are at the end of this topic.

Note

You might need to scroll horizontally or vertically to see all of the data in this table.










API	Enabled	Disabled	Pending deletion Pending replica deletion	Pending import	Unavailable	Creating	Updating
CancelKey Deletion	 [4]	 [4]		 [4]	 [4], [13]	 [4]	 [4]
CreateAlias							

API	Enabled	Disabled	Pending deletion Pending replica deletion	Pending import	Unavailable	Creating	Updating
			[3]				
CreateGrant							
		[1]	[2] or [3]	[5]		[14]	
Decrypt							
		[1]	[2] or [3]	[5]	[11]	[14]	
DeleteAlias							
DeleteImportedKeyMaterial					N/A		
	[9]	[9]	[9]	(No effect)		[14]	[15]
DescribeKey							
DisableKey							
			[3]	[5]	[12]	[14]	[15]
DisableKeyRotation							
	[7]	[1] or [7]	[3] or [7]	[6]	[7]	[14]	[7]

API	Enabled	Disabled	Pending deletion Pending replica deletion	Pending import	Unavailable	Creating	Updating
EnableKey			 [3]	 [5]	 [12]	 [14]	 [15]
EnableKeyRotation	 [7]	 [1] or [7]	 [3] or [7]	 [6]	 [7]	 [14]	 [7]
Encrypt		 [1]	 [2] or [3]	 [5]	 [11]	 [14]	
GenerateDataKey		 [1]	 [2] or [3]	 [5]	 [11]	 [14]	
GenerateDataKeyPair		 [1]	 [2] or [3]	 [5]	 [11]	 [14]	
GenerateDataKeyPairWithoutPlaintext		 [1]	 [2] or [3]	 [5]	 [11]	 [14]	
GenerateDataKeyWithoutPlaintext		 [1]	 [2] or [3]	 [5]	 [11]	 [14]	

API	Enabled	Disabled	Pending deletion Pending replica deletion	Pending import	Unavailable	Creating	Updating
GenerateMac	✓	✗ [1]	✗ [2] or [3]	N/A	N/A	✗ [14]	✓
GetKeyPolicy	✓	✓	✓	✓	✓	✓	✓
GetKeyRotationStatus	⊛ [7]	⊛ [7]	⊛ [7]	✗ [6]	✗ [7]	⊛ [7]	⊛ [7]
GetParametersForImport	⊛ [9]	⊛ [9]	✗ [8] or [9]	✓	✗ [9]	✗ [14]	✗ [15]
GetPublicKey	✓	✓	✗ [2] or [3]	N/A	N/A	✗ [14]	✓
ImportKeyMaterial	⊛ [9]	⊛ [9]	✗ [8] or [9]	✓	✗ [9]	✗ [14]	✓
ListAliases	✓	✓	✓	✓	✓	✓	✓
ListGrants	✓	✓	✓	✓	✓	✓	✓

API	Enabled	Disabled	Pending deletion Pending replica deletion	Pending import	Unavailable	Creating	Updating
ListKeyPolicies	✓	✓	✓	✓	✓	✓	✓
ListKeyRotations	⓪ [7]	⓪ [7]	⓪ [7]	ⓧ [6]	ⓧ [7]	⓪ [7]	⓪ [7]
ListResourceTags	✓	✓	✓	✓	✓	✓	✓
PutKeyPolicy	✓	✓	✓	✓	✓	✓	✓
ReEncrypt	✓	ⓧ [1]	ⓧ [2] or [3]	ⓧ [5]	ⓧ [11]	ⓧ [14]	✓
Replicate Key	✓	ⓧ [1]	ⓧ [2] or [3]	ⓧ [5]	N/A	ⓧ [14]	ⓧ [15]
RetireGrant	✓	✓	✓	✓	✓	✓	✓
RevokeGrant	✓	✓	✓	✓	✓	✓	✓
RotateKey OnDemand	⓪ [7]	ⓧ [1] or [7]	ⓧ [3] or [7]	ⓧ [6]	ⓧ [7]	ⓧ [14]	⓪ [7]

API	Enabled	Disabled	Pending deletion Pending replica deletion	Pending import	Unavailable	Creating	Updating
ScheduleKeyDeletion	✓	✓	 [3]	✓	✓	✓	 [15]
Sign	✓	 [1]	 [2] or [3]	N/A	N/A	 [14]	✓
TagResource	✓	✓	 [3]	✓	✓	✓	✓
UntagResource	✓	✓	 [3]	✓	✓	✓	✓
UpdateAlias	✓	✓	 [10]	✓	✓	✓	✓
UpdateKeyDescription	✓	✓	 [3]	✓	✓	✓	✓
UpdatePrimaryRegion	✓	 [1]	 [2] or [3]	 [5]	N/A	 [14]	✓

API	Enabled	Disabled	Pending deletion Pending replica deletion	Pending import	Unavailable	Creating	Updating
Verify	✓	✗ [1]	✗ [2] or [3]	N/A	N/A	✗ [14]	✓
VerifyMac	✓	✗ [1]	✗ [2] or [3]	N/A	N/A	✗ [14]	✓

Table Details

- [1] DisabledException: *<key ARN>* is disabled.
- [2] DisabledException: *<key ARN>* is pending deletion (or pending replica deletion).
- [3] KMSInvalidStateException: *<key ARN>* is pending deletion (or pending replica deletion).
- [4] KMSInvalidStateException: *<key ARN>* is not pending deletion (or pending replica deletion).
- [5] KMSInvalidStateException: *<key ARN>* is pending import.
- [6] UnsupportedOperationException: *<key ARN>* origin is EXTERNAL which is not valid for this operation.
- [7] If the KMS key has imported key material or is in a custom key store: UnsupportedOperationException.
- [8] If the KMS key has imported key material: KMSInvalidStateException
- [9] If the KMS key cannot or does not have imported key material: UnsupportedOperationException.

- [10] If the source KMS key is pending deletion, the command succeeds. If the destination KMS key is pending deletion, the command fails with error: `KMSInvalidStateException : <key ARN> is pending deletion.`
- [11] `KMSInvalidStateException: <key ARN> is unavailable.` You cannot perform this operation on an unavailable KMS key.
- [12] The operation succeeds, but the key state of the KMS key does not change until it becomes available.
- [13] While a KMS key in a custom key store is pending deletion, its key state remains `PendingDeletion` even if the KMS key becomes unavailable. This allows you to cancel deletion of the KMS key at any time during the waiting period.
- [14] `KMSInvalidStateException: <key ARN> is creating.` Amazon KMS throws this exception while it is replicating a multi-Region key (`ReplicateKey`).
- [15] `KMSInvalidStateException: <key ARN> is updating.` Amazon KMS throws this exception while it is updating the primary Region of a multi-Region key (`UpdatePrimaryRegion`).

Key type reference

Amazon KMS supports different features for different *types* of KMS keys. For example, you can only use [symmetric encryption KMS keys](#) to [generate symmetric data keys](#) and [asymmetric data key pairs](#). Also, [importing key material](#) and [automatic key rotation](#) are supported only for symmetric encryption KMS keys, and you can create only symmetric encryption KMS keys in a [custom key store](#).

This reference includes two tables.

- The [Key type table](#) lists the Amazon KMS operations that are valid for symmetric encryption KMS keys, asymmetric KMS keys, and HMAC KMS keys.
- The [Special features table](#) lists the Amazon KMS operations that are valid for multi-Region KMS keys, KMS keys with imported key material, and KMS keys in custom key stores.

Key type table

You might need to scroll horizontally or vertically to see all of the data in this table.

Amazon KMS API operation	Symmetric encryption KMS keys	HMAC KMS keys	Asymmetric KMS keys (ENCRYPT/DECRYPT)	Asymmetric KMS keys (SIGN_VERIFY)	Asymmetric KMS keys (KEY_AGREEMENT)
CancelKeyDeletion	Yes	Yes	Yes	Yes	Yes
CreateAlias	Yes	Yes	Yes	Yes	Yes
CreateGrant	Yes	Yes	Yes	Yes	Yes
CreateKey	Yes	Yes	Yes	Yes	Yes
Decrypt	Yes	No	Yes	No	No
DeleteAlias	Yes	Yes	Yes	Yes	Yes
DeleteImportedKeyMaterial	Yes	Yes	Yes	Yes	Yes
Valid only on KMS keys with imported key material (Origin is EXTERNAL).					
DeriveSharedSecret	No	No	No	No	Yes
DescribeKey	Yes	Yes	Yes	Yes	Yes
DisableKey	Yes	Yes	Yes	Yes	Yes
DisableKeyRotation	Yes	No	No	No	No
	Valid only on KMS keys				

Amazon KMS API operation	Symmetric encryption KMS keys	HMAC KMS keys	Asymmetric KMS keys (ENCRYPT, DECRYPT)	Asymmetric KMS keys (SIGN_VERIFY)	Asymmetric KMS keys (KEY_AGREEMENT)
	with Amazon KMS key material (Origin is AWS_KMS)				
EnableKey	Yes	Yes	Yes	Yes	Yes
EnableKeyRotation	Yes	No	No	No	No
	Valid only on KMS keys with Amazon KMS key material (Origin is AWS_KMS)				
Encrypt	Yes	No	Yes	No	No
GenerateDataKey	Yes	No	No	No	No

Amazon KMS API operation	Symmetric encryption KMS keys	HMAC KMS keys	Asymmetric KMS keys (ENCRYPT/DECRYPT)	Asymmetric KMS keys (SIGN_VERIFY)	Asymmetric KMS keys (KEY_AGREEMENT)
GenerateDataKeyPair Generates an asymmetric data key pair that is protected by a symmetric encryption KMS key.	Yes Not valid on KMS keys in custom key stores.	No	No	No	No
GenerateDataKeyPairWithoutPlaintext Generates an asymmetric data key pair that is protected by a symmetric encryption KMS key.	Yes Not valid on KMS keys in custom key stores.	No	No	No	No
GenerateDataKeyWithoutPlaintext	Yes	No	No	No	No
GenerateMac	No	Yes	No	No	No
GetKeyPolicy	Yes	Yes	Yes	Yes	Yes

Amazon KMS API operation	Symmetric encryption KMS keys	HMAC KMS keys	Asymmetric KMS keys (ENCRYPT, DECRYPT)	Asymmetric KMS keys (SIGN_VERIFY)	Asymmetric KMS keys (KEY_AGREEMENT)
GetKeyRotationStatus	Yes	Yes (KeyRotationEnabled will always be false.)	Yes (KeyRotationEnabled will always be false.)	Yes (KeyRotationEnabled will always be false.)	Yes (KeyRotationEnabled will always be false.)
GetParametersForImport Valid only on KMS keys with imported key material (Origin is EXTERNAL).	Yes	Yes	Yes	Yes	Yes
GetPublicKey	No	No	Yes	Yes	Yes
ImportKeyMaterial Valid only on KMS keys with imported key material (Origin is EXTERNAL).	Yes	Yes	Yes	Yes	Yes
ListAliases	Yes	Yes	Yes	Yes	Yes
ListGrants	Yes	Yes	Yes	Yes	Yes
ListKeyPolicies	Yes	Yes	Yes	Yes	Yes

Amazon KMS API operation	Symmetric encryption KMS keys	HMAC KMS keys	Asymmetric KMS keys (ENCRYPT/DECRYPT)	Asymmetric KMS keys (SIGN_VERIFY)	Asymmetric KMS keys (KEY_AGREEMENT)
ListKeyRotations	Yes	Yes (The Rotations field will always be null or empty.)	Yes (The Rotations field will always be null or empty.)	Yes (The Rotations field will always be null or empty.)	Yes (The Rotations field will always be null or empty.)
ListResourceTags	Yes	Yes	Yes	Yes	Yes
ListRetirableGrants	Yes	Yes	Yes	Yes	Yes
PutKeyPolicy	Yes	Yes	Yes	Yes	Yes
ReEncrypt	Yes	No	Yes	No	No
ReplicateKey	Yes	Yes	Yes	Yes	Yes
- Valid only on multi-Region keys					
RetireGrant	Yes	Yes	Yes	Yes	Yes
RevokeGrant	Yes	Yes	Yes	Yes	Yes

Amazon KMS API operation	Symmetric encryption KMS keys	HMAC KMS keys	Asymmetric KMS keys (ENCRYPT/DECRYPT)	Asymmetric KMS keys (SIGN_VERIFY)	Asymmetric KMS keys (KEY_AGREEMENT)
RotateKeyOnDemand	Yes Valid only on KMS keys with Amazon KMS key material (Origin is AWS_KMS)	No	No	No	No
ScheduleKeyDeletion	Yes	Yes	Yes	Yes	Yes
Sign	No	No	No	Yes	No
TagResource	Yes	Yes	Yes	Yes	Yes
UntagResource	Yes	Yes	Yes	Yes	Yes

Amazon KMS API operation	Symmetric encryption KMS keys	HMAC KMS keys	Asymmetric KMS keys (ENCRYPT/DECRYPT)	Asymmetric KMS keys (SIGN_VERIFY)	Asymmetric KMS keys (KEY_AGREEMENT)
UpdateAlias The current KMS key and the new KMS key must be the same type (both symmetric or both asymmetric or both HMAC) and they must have the same key usage .	Yes	Yes	Yes	Yes	Yes
UpdateKeyDescription	Yes	Yes	Yes	Yes	Yes
UpdateReplicaRegion - Valid only on multi-Region keys	Yes	Yes	Yes	Yes	Yes
Verify	No	No	No	Yes	No
VerifyMac	No	Yes	No	No	No

Special features table

This table shows the Amazon KMS API operations that are supported on each type of *special-purpose key*.









While reading this table, be aware of the following interactions:













- [Multi-Region keys](#):
 - Multi-Region keys can be symmetric encryption KMS keys, asymmetric KMS keys, HMAC KMS keys, and KMS keys with imported key material.
 - You cannot create multi-Region keys in a custom key store.
- [Imported key material](#)
 - You can import key material for symmetric encryption KMS keys, asymmetric KMS keys, and HMAC KMS keys.
 - You can create [multi-Region keys with imported key material](#).
 - You cannot create keys with imported key material in a custom key store.
 - Automatic key rotation (`EnableKeyRotation`, `DisableKeyRotation`) is not supported for KMS keys with imported key material.
- [Custom key stores](#)
 - Custom key stores support only symmetric encryption KMS keys.
 - Symmetric operations on asymmetric key pairs (`GenerateDataKeyPair`, `GenerateDataKeyPairWithoutPlaintext`) are not supported on KMS keys in custom key stores.
 - Automatic key rotation (`EnableKeyRotation`, `DisableKeyRotation`) is not supported on KMS keys in custom key stores.
 - You cannot create multi-Region keys in custom key stores.

You might need to scroll horizontally or vertically to see all of the data in this table.

Amazon KMS API operation	Multi-Region keys	Imported key material	KMS keys in a custom key store
CancelKeyDeletion	✓	✓	✓
CreateAlias	✓	✓	✓
CreateGrant	✓	✓	✓

Amazon KMS API operation	Multi-Region keys	Imported key material	KMS keys in a custom key store
CreateKey You can use <code>CreateKey</code> to create a multi-Region primary key, a KMS key with imported key material, or a KMS key in a custom key store. To create a multi-Region replica key, use <code>ReplicateKey</code> .	✓	✓	✓
Decrypt	✓ Valid only when <code>KeyUsage</code> is <code>ENCRYPT_D</code> <code>ECRYPT</code>	✓	✓
DeleteAlias	✓	✓	✓
DeleteImportedKeyMaterial	✓ Valid only for keys with imported key material (<code>Origin</code> is <code>EXTERNAL</code>)	✓	✗
DescribeKey	✓	✓	✓
DisableKey	✓	✓	✓

Amazon KMS API operation	Multi-Region keys	Imported key material	KMS keys in a custom key store
DisableKeyRotation	 Valid only on symmetric encryption keys with Amazon KMS key material (Origin is AWS_KMS).		
EnableKey	 Valid only on symmetric encryption KMS keys		
EnableKeyRotation	 Valid only on symmetric encryption keys with Amazon KMS key material (Origin is AWS_KMS).		

Amazon KMS API operation	Multi-Region keys	Imported key material	KMS keys in a custom key store
Encrypt	 Valid only when KeyUsage is ENCRYPT_D ECRYPT		
GenerateDataKey	 Valid only on symmetric encryption KMS keys		
GenerateDataKeyPair	 Valid only on symmetric encryption KMS keys		
GenerateDataKeyPairWithoutPlaintext	 Valid only on symmetric encryption KMS keys		

Amazon KMS API operation	Multi-Region keys	Imported key material	KMS keys in a custom key store
GenerateDataKeyWithoutPlaintext	✓ Valid only on symmetric encryption KMS keys	✓	✓
GenerateMac Valid only on HMAC KMS keys	✓	✓	✗
GetKeyPolicy	✓	✓	✓
GetKeyRotationStatus	✓	✓ (KeyRotationEnabled will always be false.)	✗
GetParametersForImport	✓ Valid only for keys with imported key material (Origin is EXTERNAL).	✓	✗
GetPublicKey Valid only for asymmetric KMS keys .	✓	✓	✗

Amazon KMS API operation	Multi-Region keys	Imported key material	KMS keys in a custom key store
ImportKeyMaterial	 Valid only for keys with imported key material (Origin is EXTERNAL).		
ListAliases			
ListGrants			
ListKeyPolicies			
ListResourceTags			
ListRetirableGrants			
PutKeyPolicy			
ReEncrypt	 Valid only when KeyUsage is ENCRYPT_DECRYPT		

Amazon KMS API operation	Multi-Region keys	Imported key material	KMS keys in a custom key store
ReplicateKey	✓ Valid only on multi-Region primary keys.	✓ Valid only on multi-Region primary keys.	✗
RetireGrant	✓	✓	✓
RevokeGrant	✓	✓	✓
ScheduleKeyDeletion	✓	✓	✓
Sign Valid only on when KeyUsage is SIGN_VERIFY .	✓	✓	✗
TagResource	✓	✓	✓
UntagResource	✓	✓	✓
UpdateAlias - The current KMS key and the new KMS key must be the same type (both symmetric or both asymmetric or both HMAC) and they must have the same key usage .	✓	✓	✓
UpdateKeyDescription	✓	✓	✓

Amazon KMS API operation	Multi-Region keys	Imported key material	KMS keys in a custom key store
UpdateReplicaRegion	✓	✓ Valid only on multi-Region keys.	✗
Verify Valid only when KeyUsage is SIGN_VERIFY .	✓	✓	✗
VerifyMac Valid only on HMAC KMS keys	✓	✓	✗

Key spec reference

When you create an asymmetric KMS key or an HMAC KMS key, you select its [key spec](#). The *key spec*, which is a property of every Amazon KMS key, represents the cryptographic configuration of your KMS key. You choose the key spec when you create the KMS key, and you cannot change it. If you've selected the wrong key spec, [delete the KMS key](#), and create a new one.

Note

The key spec for a KMS key was known as a "customer master key spec." The `CustomerMasterKeySpec` parameter of the [CreateKey](#) operation is deprecated. Instead, use the `KeySpec` parameter. The response of the `CreateKey` and [DescribeKey](#) operations includes a `KeySpec` and `CustomerMasterKeySpec` member with the same value.

The key spec determines whether the KMS key is symmetric or asymmetric, the type of key material in the KMS key, and the encryption algorithms, signing algorithms, or message authentication code (MAC) algorithms that Amazon KMS supports for the KMS key. The key spec

that you choose is typically determined by your use case and regulatory requirements. However, cryptographic operations on KMS keys with different key specs are priced differently and are subject to different quotas. For pricing details, see [Amazon Key Management Service Pricing](#). For information about request quotas, see [Request quotas](#).

To limit the key specs that principals can use when creating KMS keys, use the [kms:KeySpec](#) condition key. You can also use the `kms:KeySpec` condition key to allow principals to call Amazon KMS operations only on KMS keys with a particular key spec. For example, you can deny permission to schedule deletion of any KMS key with an `RSA_4096` key spec.

Amazon KMS supports the following key specs for KMS keys:

[Symmetric encryption key spec](#) (default)

- `SYMMETRIC_DEFAULT`

[RSA key specs](#) (encryption and decryption -or- signing and verification)

- `RSA_2048`
- `RSA_3072`
- `RSA_4096`

[Elliptic curve key specs](#)

- Asymmetric NIST-recommended [elliptic curve key pairs](#) (signing and verification -or- deriving shared secrets)
 - `ECC_NIST_P256` (`secp256r1`)
 - `ECC_NIST_P384` (`secp384r1`)
 - `ECC_NIST_P521` (`secp521r1`)
- Other asymmetric elliptic curve key pairs (signing and verification)
 - `ECC_SECG_P256K1` ([secp256k1](#)), commonly used for cryptocurrency.

[SM2 key spec](#) (encryption and decryption -or- signing and verification -or- deriving shared secrets)

- `SM2` (China Regions only)

[HMAC key specs](#)

- `HMAC_224`
- `HMAC_256`
- `HMAC_384`
- `HMAC_512`

SYMMETRIC_DEFAULT key spec

The default key spec, SYMMETRIC_DEFAULT, is the key spec for symmetric encryption KMS keys. When you select the **Symmetric** key type and the **Encrypt and decrypt** key usage in the Amazon KMS console, it selects the SYMMETRIC_DEFAULT key spec. In the [CreateKey](#) operation, if you don't specify a KeySpec value, SYMMETRIC_DEFAULT is selected. If you don't have a reason to use a different key spec, SYMMETRIC_DEFAULT is a good choice.

SYMMETRIC_DEFAULT represents AES-256-GCM, a symmetric algorithm based on [Advanced Encryption Standard](#) (AES) in [Galois Counter Mode](#) (GCM) with 256-bit keys, an industry standard for secure encryption. The ciphertext that this algorithm generates supports additional authenticated data (AAD), such as an [encryption context](#), and GCM provides an additional integrity check on the ciphertext.

Data encrypted under AES-256-GCM is protected now and in the future. Cryptographers consider this algorithm to be *quantum resistant*. Theoretical future, large-scale quantum computing attacks on ciphertexts created under 256-bit AES-GCM keys [reduce the effective security of the key to 128 bits](#). But, this security level is sufficient to make brute force attacks on Amazon KMS ciphertexts infeasible.

The only exception in China Regions, where SYMMETRIC_DEFAULT represents a 128-bit symmetric key that uses SM4 encryption. You can only create a 128-bit SM4 key within China Regions. You cannot create a 256-bit AES-GCM KMS key in China Regions.

You can use a symmetric encryption KMS key in Amazon KMS to encrypt, decrypt, and re-encrypt data, and to protect generated data keys and data key pairs. Amazon services that are integrated with Amazon KMS use symmetric encryption KMS keys to encrypt your data at rest. You can [import your own key material](#) into a symmetric encryption KMS key and create symmetric encryption KMS keys in [custom key stores](#). For a table comparing the operations that you can perform on symmetric and asymmetric KMS keys, see [Comparing Symmetric and Asymmetric KMS keys](#).

You can use a symmetric encryption KMS key in Amazon KMS to encrypt, decrypt, and re-encrypt data, and generate data keys and data key pairs. You can create [multi-Region](#) symmetric encryption KMS keys, [import your own key material](#) into a symmetric encryption KMS key, and create symmetric encryption KMS keys in [custom key stores](#). For a table comparing the operations that you can perform on KMS keys of different types, see [Key type reference](#).

RSA key specs

When you use an RSA key spec, Amazon KMS creates an asymmetric KMS key with an RSA key pair. The private key never leaves Amazon KMS unencrypted. You can use the public key within Amazon KMS, or download the public key for use outside of Amazon KMS.

Warning

When you encrypt data outside of Amazon KMS, be sure that you can decrypt your ciphertext. If you use the public key from a KMS key that has been deleted from Amazon KMS, the public key from a KMS key configured for signing and verification, or an encryption algorithm that is not supported by the KMS key, the data is unrecoverable.

In Amazon KMS, you can use asymmetric KMS keys with RSA key pairs for encryption and decryption, or signing and verification, but not both. This property, known as *key usage*, is determined separately from the key spec, but you should make that decision before you select a key spec.

Amazon KMS supports the following RSA key specs for encryption and decryption or signing and verification:

- RSA_2048
- RSA_3072
- RSA_4096

RSA key specs differ by the length of the RSA key in bits. The RSA key spec that you choose might be determined by your security standards or the requirements of your task. In general, use the largest key that is practical and affordable for your task. Cryptographic operations on KMS keys with different RSA key specs are priced differently. For information about Amazon KMS pricing, see [Amazon Key Management Service Pricing](#). For information about request quotas, see [Request quotas](#).

RSA key specs for encryption and decryption

When an RSA asymmetric KMS key is used for encryption and decryption, you encrypt with the public key and decrypt with the private key. When you call the `Encrypt` operation in Amazon

KMS for an RSA KMS key, Amazon KMS uses the public key in the RSA key pair and the encryption algorithm you specify to encrypt your data. To decrypt the ciphertext, call the `Decrypt` operation and specify the same KMS key and encryption algorithm. Amazon KMS then uses the private key in the RSA key pair to decrypt your data.

You can also download the public key and use it to encrypt data outside of Amazon KMS. Be sure to use an encryption algorithm that Amazon KMS supports for RSA KMS keys. To decrypt the ciphertext, call the `Decrypt` function with the same KMS key and encryption algorithm.

Amazon KMS supports two encryption algorithms for KMS keys with RSA key specs. These algorithms, which are defined in [PKCS #1 v2.2](#), differ in the hash function they use internally. In Amazon KMS, the `RSAES_OAEP` algorithms always use the same hash function for both hashing purposes and for the [mask generation function](#) (MGF1). You are required to specify an encryption algorithm when you call the `Encrypt` and `Decrypt` operations. You can choose a different algorithm for each request.

Supported encryption algorithms for RSA key specs

Encryption algorithm	Algorithm description
<code>RSAES_OAEP_SHA_1</code>	PKCS #1 v2.2, Section 7.1. RSA encryption with OAEP Padding using SHA-1 for both the hash and in the MGF1 mask generation function along with an empty label.
<code>RSAES_OAEP_SHA_256</code>	PKCS #1, Section 7.1. RSA encryption with OAEP Padding using SHA-256 for both the hash and in the MGF1 mask generation function along with an empty label.

You cannot configure a KMS key to use a particular encryption algorithm. However, you can use the [kms:EncryptionAlgorithm](#) policy condition to specify the encryption algorithms that principals are allowed to use with the KMS key.

To get the encryption algorithms for a KMS key, [view the cryptographic configuration](#) of the KMS key in the Amazon KMS console or use the `DescribeKey` operation. Amazon KMS also provides the key spec and encryption algorithms when you download your public key, either in the Amazon KMS console or by using the `GetPublicKey` operation.

You might choose an RSA key spec based on the length of the plaintext data that you can encrypt in each request. The following table shows the maximum size, in bytes, of the plaintext that you can encrypt in a single call to the [Encrypt](#) operation. The values differ with the key spec and encryption algorithm. To compare, you can use a symmetric encryption KMS key to encrypt up to 4096 bytes at one time.

To compute the maximum plaintext length in bytes for these algorithms, use the following formula: $(key_size_in_bits / 8) - (2 * hash_length_in_bits / 8) - 2$. For example, for RSA_2048 with SHA-256, the maximum plaintext size in bytes is $(2048/8) - (2 * 256/8) - 2 = 190$.

Maximum plaintext size (in bytes) in an Encrypt operation

Key spec	Encryption algorithm	
	RSAES_OAEP_SHA_1	RSAES_OAEP_SHA_256
RSA_2048	214	190
RSA_3072	342	318
RSA_4096	470	446

RSA key specs for signing and verification

When an RSA asymmetric KMS key is used for signing and verification, you generate the signature for a message with the private key and verify the signature with the public key.

When you call the Sign operation in Amazon KMS for an asymmetric KMS key, Amazon KMS uses the private key in the RSA key pair, the message, and the signing algorithm you specify, to generate a signature. To verify the signature, call the [Verify](#) operation. Specify the signature, plus the same KMS key, message, and signing algorithm. Amazon KMS then uses the public key in the RSA key pair to verify the signature. You can also download the public key and use it to verify the signature outside of Amazon KMS.

Amazon KMS supports the following signing algorithms for all KMS keys with an RSA key spec. You are required to specify a signing algorithm when you call the [Sign](#) and [Verify](#) operations. You can choose a different algorithm for each request. When signing with RSA key pairs, RSASSA-PSS algorithms are preferred. We include RSASSA-PKCS1-v1_5 algorithms for compatibility with existing applications.

Supported signing algorithms for RSA key specs

Signing algorithm	Algorithm description
RSASSA_PSS_SHA_256	PKCS #1 v2.2, Section 8.1, RSA signature with PSS padding using SHA-256 for both the message digest and the MGF1 mask generation function along with a 256-bit salt
RSASSA_PSS_SHA_384	PKCS #1 v2.2, Section 8.1, RSA signature with PSS padding using SHA-384 for both the message digest and the MGF1 mask generation function along with a 384-bit salt
RSASSA_PSS_SHA_512	PKCS #1 v2.2, Section 8.1, RSA signature with PSS padding using SHA-512 for both the message digest and the MGF1 mask generation function along with a 512-bit salt
RSASSA_PKCS1_V1_5_SHA_256	PKCS #1 v2.2, Section 8.2, RSA signature with PKCS #1v1.5 Padding and SHA-256
RSASSA_PKCS1_V1_5_SHA_384	PKCS #1 v2.2, Section 8.2, RSA signature with PKCS #1v1.5 Padding and SHA-384
RSASSA_PKCS1_V1_5_SHA_512	PKCS #1 v2.2, Section 8.2, RSA signature with PKCS #1v1.5 Padding and SHA-512

You cannot configure a KMS key to use particular signing algorithms. However, you can use the [kms:SigningAlgorithm](#) policy condition to specify the signing algorithms that principals are allowed to use with the KMS key.

To get the signing algorithms for a KMS key, [view the cryptographic configuration](#) of the KMS key in the Amazon KMS console or by using the [DescribeKey](#) operation. Amazon KMS also provides the key spec and signing algorithms when you download your public key, either in the Amazon KMS console or by using the [GetPublicKey](#) operation.

Elliptic curve key specs

When you use an elliptic curve (ECC) key spec, Amazon KMS creates an asymmetric KMS key with an ECC key pair for signing and verification or deriving shared secrets (but not both). The private key that generates signatures or derives shared secrets never leaves Amazon KMS unencrypted. You can use the public key to [verify signatures](#) within Amazon KMS, or [download the public key](#) for use outside of Amazon KMS.

Amazon KMS supports the following ECC key specs for asymmetric KMS keys.

- Asymmetric NIST-recommended elliptic curve key pairs (signing and verification -or- deriving shared secrets)
 - ECC_NIST_P256 (secp256r1)
 - ECC_NIST_P384 (secp384r1)
 - ECC_NIST_P521 (secp521r1)
- Other asymmetric elliptic curve key pairs (signing and verification)
 - ECC_SECG_P256K1 ([secp256k1](#)), commonly used for cryptocurrencies.

The ECC key spec that you choose might be determined by your security standards or the requirements of your task. In general, use the curve with the most points that is practical and affordable for your task.

If you're creating an asymmetric KMS key to [derive shared secrets](#), use one of the NIST-recommended elliptic curve key specs. The only supported key agreement algorithm for deriving shared secrets is the [Elliptic Curve Cryptography Cofactor Diffie-Hellman Primitive](#) (ECDH). For an example of how to derive shared secrets offline, see [the section called "Deriving shared secrets offline"](#).

If you're creating an asymmetric KMS key to use with cryptocurrencies, use the ECC_SECG_P256K1 key spec. You can also use this key spec for other purposes, but it is required for Bitcoin, and other cryptocurrencies.

KMS keys with different ECC key specs are priced differently and are subject to different request quotas. For information about Amazon KMS pricing, see [Amazon Key Management Service Pricing](#). For information about request quotas, see [Request quotas](#).

The following table shows the signing algorithms that Amazon KMS supports for each of the ECC key specs. You cannot configure a KMS key to use particular signing algorithms. However, you can use the [kms:SigningAlgorithm](#) policy condition to specify the signing algorithms that principals are allowed to use with the KMS key.

Supported signing algorithms for ECC key specs

Key spec	Signing algorithm	Algorithm description
ECC_NIST_P256	ECDSA_SHA_256	NIST FIPS 186-4, Section 6.4, ECDSA signature using the curve specified by the key and SHA-256 for the message digest.
ECC_NIST_P384	ECDSA_SHA_384	NIST FIPS 186-4, Section 6.4, ECDSA signature using the curve specified by the key and SHA-384 for the message digest.
ECC_NIST_P521	ECDSA_SHA_512	NIST FIPS 186-4, Section 6.4, ECDSA signature using the curve specified by the key and SHA-512 for the message digest.
ECC_SECG_P256K1	ECDSA_SHA_256	NIST FIPS 186-4, Section 6.4, ECDSA signature using the curve specified by the key and SHA-256 for the message digest.

SM2 key spec (China Regions only)

The SM2 key spec is an elliptic curve key spec defined within the GM/T series of specifications published by [China's Office of State Commercial Cryptography Administration \(OSCCA\)](#). The SM2 key spec is available only in China Regions. When you use the SM2 key spec, Amazon KMS creates an asymmetric KMS key with an SM2 key pair. You can use your SM2 key pair within Amazon KMS, or download the public key for use outside of Amazon KMS. For more information, see [the section called "Offline verification with SM2 key pairs \(China Regions only\)"](#).

Each KMS key can have only one key usage. You can use an SM2 KMS key for signing and verification, encryption and decryption, *or* deriving shared secrets. You must specify the key usage when you create the KMS key, and you cannot change it after the key is created.

If you're creating an asymmetric KMS key to [derive shared secrets](#), use the SM2 key spec. The only supported key agreement algorithm for deriving shared secrets is the [Elliptic Curve Cryptography Cofactor Diffie-Hellman Primitive](#) (ECDH).

Amazon KMS supports the following SM2 encryption and signing algorithms:

- **SM2PKE** encryption algorithm

SM2PKE is an elliptic curve based encryption algorithm defined by OSCCA in GM/T 0003.4-2012.

- **SM2DSA** signing algorithm

SM2DSA is an elliptic curve based signing algorithm defined by OSCCA in GM/T 0003.2-2012. SM2DSA requires a distinguishing ID that is hashed with the SM3 hashing algorithm and then combined with the message, or message digest, that you passed to Amazon KMS. This concatenated value is then hashed and signed by Amazon KMS.

Key specs for HMAC KMS keys

Amazon KMS supports symmetric HMAC keys in varying lengths. The key spec that you select can depend on your security, regulatory, or business requirements. The length of the key determines the MAC algorithm that is used in [GenerateMac](#) and [VerifyMac](#) operations. In general, longer keys are more secure. Use the longest key that is practical for your use case.

HMAC key spec	MAC algorithm
HMAC_224	HMAC_SHA_224
HMAC_256	HMAC_SHA_256
HMAC_384	HMAC_SHA_384
HMAC_512	HMAC_SHA_512

Amazon KMS permissions

This table is designed to help you understand Amazon KMS permissions so you can control access to your Amazon KMS resources. Definitions of the column headings appear below the table.

You can also learn about Amazon KMS permissions in the [Actions, resources, and condition keys for Amazon Key Management Service](#) topic of the *Service Authorization Reference*. However, that topic doesn't list all of the condition keys that you can use to refine each permission.

For more information on which Amazon KMS operations are valid for symmetric encryption KMS keys, asymmetric KMS keys, and HMAC KMS keys, see the [Key type reference](#).

Note

You might have to scroll horizontally or vertically to see all of the data in the table.

Actions and permissions	Policy type	Cross-account use	Resources (for IAM policies)	Amazon KMS condition keys
CancelKeyDeletion kms:CancelKeyDeletion	Key policy	No	KMS key	<i>Conditions for KMS key operations:</i> kms:CallerAccount kms:KeySpec kms:KeyUsage kms:KeyOrigin kms:MultiRegion kms:MultiRegionKeyType kms:ResourceAliases

Actions and permissions	Policy type	Cross-account use	Resources (for IAM policies)	Amazon KMS condition keys
				aws:ResourceTag/tag-key (Amazon global condition key) kms:ViaService
ConnectCustomKeyStore kms:ConnectCustomKeyStore	IAM policy	No	*	kms:CallerAccount
CreateAlias kms:CreateAlias	IAM policy (for the alias)	No	Alias	None (when controlling access to the alias)
<p>To use this operation, the caller needs kms:CreateAlias permission on two resources:</p> <ul style="list-style-type: none"> The alias (in an IAM policy) The KMS key (in a key policy) <p>For details, see Controlling access to aliases.</p>	Key policy (for the KMS key)	No	KMS key	<i>Conditions for KMS key operations:</i> kms:CallerAccount kms:KeySpec kms:KeyUsage kms:KeyOrigin kms:MultiRegion kms:MultiRegionKeyType kms:ResourceAliases aws:ResourceTag/tag-key (Amazon global condition key) kms:ViaService

Actions and permissions	Policy type	Cross-account use	Resources (for IAM policies)	Amazon KMS condition keys
CreateCustomKeyStore kms:CreateCustomKeyStore	IAM policy	No	*	kms:CallerAccount

Actions and permissions	Policy type	Cross-account use	Resources (for IAM policies)	Amazon KMS condition keys
<p>CreateGrant</p> <p>kms:CreateGrant</p>	Key policy	Yes	KMS key	<p><i>Encryption context conditions:</i></p> <p>kms:EncryptionContext:context-key</p> <p>kms:EncryptionContextKeys</p> <p><i>Grant conditions:</i></p> <p>kms:GrantConstraintType</p> <p>kms:GranteePrincipal</p> <p>kms:GrantIsForAWSResource</p> <p>kms:GrantOperations</p> <p>kms:RetiringPrincipal</p> <p><i>Conditions for KMS key operations:</i></p> <p>kms:CallerAccount</p> <p>kms:KeySpec</p> <p>kms:KeyUsage</p> <p>kms:KeyOrigin</p> <p>kms:MultiRegion</p> <p>kms:MultiRegionKeyType</p> <p>kms:ResourceAliases</p>

Actions and permissions	Policy type	Cross-account use	Resources (for IAM policies)	Amazon KMS condition keys
				aws:ResourceTag/tag-key (Amazon global condition key) kms:ViaService
CreateKey kms:CreateKey	IAM policy	No	*	kms:BypassPolicyLockoutSafetyCheck kms:CallerAccount kms:KeySpec kms:KeyUsage kms:KeyOrigin kms:MultiRegion kms:MultiRegionKeyType kms:ViaService aws:RequestTag/tag-key (Amazon global condition key) aws:ResourceTag/tag-key (Amazon global condition key) aws:TagKeys (Amazon global condition key)

Actions and permissions	Policy type	Cross-account use	Resources (for IAM policies)	Amazon KMS condition keys
<p>Decrypt</p> <p>kms:Decrypt</p>	Key policy	Yes	KMS key	<p><i>Conditions for cryptographic operations</i></p> <p>kms:EncryptionAlgorithm</p> <p>kms:RequestAlias</p> <p><i>Encryption context conditions:</i></p> <p>kms:EncryptionContext:context-key</p> <p>kms:EncryptionContextKeys</p> <p><i>Conditions for KMS key operations:</i></p> <p>kms:CallerAccount</p> <p>kms:KeySpec</p> <p>kms:KeyUsage</p> <p>kms:KeyOrigin</p> <p>kms:MultiRegion</p> <p>kms:MultiRegionKeyType</p> <p>kms:ResourceAliases</p> <p>aws:ResourceTag/tag-key (Amazon global condition key)</p>

Actions and permissions	Policy type	Cross-account use	Resources (for IAM policies)	Amazon KMS condition keys
				kms:ViaService
<p>DeleteAlias</p> <p><code>kms:DeleteAlias</code></p> <p>To use this operation, the caller needs <code>kms:DeleteAlias</code> permission on two resources:</p> <ul style="list-style-type: none"> The alias (in an IAM policy) The KMS key (in a key policy) <p>For details, see Controlling access to aliases.</p>	<p>IAM policy (for the alias)</p> <p>Key policy (for the KMS key)</p>	No	Alias	<p>None (when controlling access to the alias)</p> <p><i>Conditions for KMS key operations:</i></p> <p>kms:CallerAccount</p> <p>kms:KeySpec</p> <p>kms:KeyUsage</p> <p>kms:KeyOrigin</p> <p>kms:MultiRegion</p> <p>kms:MultiRegionKeyType</p> <p>kms:ResourceAliases</p> <p>aws:ResourceTag/tag-key (Amazon global condition key)</p> <p>kms:ViaService</p>
<p>DeleteCustomKeyStore</p> <p><code>kms:DeleteCustomKeyStore</code></p>	IAM policy	No	*	kms:CallerAccount

Actions and permissions	Policy type	Cross-account use	Resources (for IAM policies)	Amazon KMS condition keys
<p>DeleteImportedKeyMaterial</p> <p>kms:DeleteImportedKeyMaterial</p>	Key policy	No	KMS key	<p><i>Conditions for KMS key operations:</i></p> <p>kms:CallerAccount</p> <p>kms:KeySpec</p> <p>kms:KeyUsage</p> <p>kms:KeyOrigin</p> <p>kms:MultiRegion</p> <p>kms:MultiRegionKeyType</p> <p>kms:ResourceAliases</p> <p>aws:ResourceTag/tag-key (Amazon global condition key)</p> <p>kms:ViaService</p>

Actions and permissions	Policy type	Cross-account use	Resources (for IAM policies)	Amazon KMS condition keys
<p>DeriveSharedSecret</p> <p>kms:DeriveSharedSecret</p>	Key policy	Yes	KMS key	<p><i>Conditions for KMS key operations:</i></p> <p>kms:CallerAccount</p> <p>kms:KeySpec</p> <p>kms:KeyUsage</p> <p>kms:KeyOrigin</p> <p>kms:MultiRegion</p> <p>kms:MultiRegionKeyType</p> <p>kms:ResourceAliases</p> <p>aws:ResourceTag/tag-key (Amazon global condition key)</p> <p>kms:ViaService</p> <p><i>Conditions for cryptographic operations:</i></p> <p>kms:KeyAgreementAlgorithm</p>
<p>DescribeCustomKeyStores</p> <p>kms:DescribeCustomKeyStores</p>	IAM policy	No	*	<p>kms:CallerAccount</p>

Actions and permissions	Policy type	Cross-account use	Resources (for IAM policies)	Amazon KMS condition keys
DescribeKey kms:DescribeKey	Key policy	Yes	KMS key	<p><i>Conditions for KMS key operations:</i></p> <p>kms:CallerAccount</p> <p>kms:KeySpec</p> <p>kms:KeyUsage</p> <p>kms:KeyOrigin</p> <p>kms:MultiRegion</p> <p>kms:MultiRegionKeyType</p> <p>kms:ResourceAliases</p> <p>aws:ResourceTag/tag-key (Amazon global condition key)</p> <p>kms:ViaService</p> <p><i>Other conditions:</i></p> <p>kms:RequestAlias</p>

Actions and permissions	Policy type	Cross-account use	Resources (for IAM policies)	Amazon KMS condition keys
DisableKey kms:DisableKey	Key policy	No	KMS key	<i>Conditions for KMS key operations:</i> kms:CallerAccount kms:KeySpec kms:KeyUsage kms:KeyOrigin kms:MultiRegion kms:MultiRegionKeyType kms:ResourceAliases aws:ResourceTag/tag-key (Amazon global condition key) kms:ViaService

Actions and permissions	Policy type	Cross-account use	Resources (for IAM policies)	Amazon KMS condition keys
<p>DisableKeyRotation</p> <p>kms:DisableKeyRotation</p>	Key policy	No	KMS key	<p><i>Conditions for KMS key operations:</i></p> <p>kms:CallerAccount</p> <p>kms:KeySpec</p> <p>kms:KeyUsage</p> <p>kms:KeyOrigin</p> <p>kms:MultiRegion</p> <p>kms:MultiRegionKeyType</p> <p>kms:ResourceAliases</p> <p>aws:ResourceTag/tag-key (Amazon global condition key)</p> <p>kms:ViaService</p>
<p>DisconnectCustomKeyStore</p> <p>kms:DisconnectCustomKeyStore</p>	IAM policy	No	*	<p>kms:CallerAccount</p>

Actions and permissions	Policy type	Cross-account use	Resources (for IAM policies)	Amazon KMS condition keys
EnableKey kms:EnableKey	Key policy	No	KMS key	<i>Conditions for KMS key operations:</i> kms:CallerAccount kms:KeySpec kms:KeyUsage kms:KeyOrigin kms:MultiRegion kms:MultiRegionKeyType kms:ResourceAliases aws:ResourceTag/tag-key (Amazon global condition key) kms:ViaService

Actions and permissions	Policy type	Cross-account use	Resources (for IAM policies)	Amazon KMS condition keys
<p>EnableKeyRotation</p> <p>kms:EnableKeyRotation</p>	Key policy	No	KMS key	<p><i>Conditions for KMS key operations:</i></p> <p>kms:CallerAccount</p> <p>kms:KeySpec</p> <p>kms:KeyUsage</p> <p>kms:KeyOrigin</p> <p>kms:MultiRegion</p> <p>kms:MultiRegionKeyType</p> <p>kms:ResourceAliases</p> <p>aws:ResourceTag/tag-key (Amazon global condition key)</p> <p>kms:ViaService</p> <p><i>Automatic key rotation conditions:</i></p> <p>kms:RotationPeriodInDays</p>

Actions and permissions	Policy type	Cross-account use	Resources (for IAM policies)	Amazon KMS condition keys
<p>Encrypt</p> <p>kms:Encrypt</p>	Key policy	Yes	KMS key	<p><i>Conditions for cryptographic operations</i></p> <p>kms:EncryptionAlgorithm</p> <p>kms:RequestAlias</p> <p><i>Encryption context conditions:</i></p> <p>kms:EncryptionContext:context-key</p> <p>kms:EncryptionContextKeys</p> <p><i>Conditions for KMS key operations:</i></p> <p>kms:CallerAccount</p> <p>kms:KeySpec</p> <p>kms:KeyUsage</p> <p>kms:KeyOrigin</p> <p>kms:MultiRegion</p> <p>kms:MultiRegionKeyType</p> <p>kms:ResourceAliases</p> <p>aws:ResourceTag/tag-key (Amazon global condition key)</p>

Actions and permissions	Policy type	Cross-account use	Resources (for IAM policies)	Amazon KMS condition keys
				kms:ViaService

Actions and permissions	Policy type	Cross-account use	Resources (for IAM policies)	Amazon KMS condition keys
<p>GenerateDataKey</p> <p>kms:GenerateDataKey</p>	Key policy	Yes	KMS key	<p><i>Conditions for cryptographic operations</i></p> <p>kms:EncryptionAlgorithm</p> <p>kms:RequestAlias</p> <p><i>Encryption context conditions:</i></p> <p>kms:EncryptionContext:key</p> <p>kms:EncryptionContextKeys</p> <p><i>Conditions for KMS key operations:</i></p> <p>kms:CallerAccount</p> <p>kms:KeySpec</p> <p>kms:KeyUsage</p> <p>kms:KeyOrigin</p> <p>kms:MultiRegion</p> <p>kms:MultiRegionKeyType</p> <p>kms:ResourceAliases</p> <p>aws:ResourceTag/tag-key (Amazon global condition key)</p>

Actions and permissions	Policy type	Cross-account use	Resources (for IAM policies)	Amazon KMS condition keys
				kms:ViaService

Actions and permissions	Policy type	Cross-account use	Resources (for IAM policies)	Amazon KMS condition keys
<p>GenerateDataKeyPair</p> <p><code>kms:GenerateDataKeyPair</code></p>	Key policy	Yes	<p>KMS key</p> <p>Generates an asymmetric data key pair that is protected by a symmetric encryption KMS key.</p>	<p><i>Conditions for data key pairs:</i></p> <p>kms:DataKeyPairSpec</p> <p><i>Conditions for cryptographic operations</i></p> <p>kms:EncryptionAlgorithm</p> <p>kms:RequestAlias</p> <p><i>Encryption context conditions:</i></p> <p>kms:EncryptionContext:context-key</p> <p>kms:EncryptionContextKeys</p> <p><i>Conditions for KMS key operations:</i></p> <p>kms:CallerAccount</p> <p>kms:KeySpec</p> <p>kms:KeyUsage</p> <p>kms:KeyOrigin</p> <p>kms:MultiRegion</p> <p>kms:MultiRegionKeyType</p>

Actions and permissions	Policy type	Cross-account use	Resources (for IAM policies)	Amazon KMS condition keys
				kms:ResourceAliases aws:ResourceTag/tag-key (Amazon global condition key) kms:ViaService

Actions and permissions	Policy type	Cross-account use	Resources (for IAM policies)	Amazon KMS condition keys
<p>GenerateDataKeyPairWithoutPlaintext</p> <p><code>kms:GenerateDataKeyPairWithoutPlaintext</code></p>	Key policy	Yes	<p>KMS key</p> <p>Generates an asymmetric data key pair that is protected by a symmetric encryption KMS key.</p>	<p><i>Conditions for data key pairs:</i></p> <p>kms:DataKeyPairSpec</p> <p><i>Conditions for cryptographic operations</i></p> <p>kms:EncryptionAlgorithm</p> <p>kms:RequestAlias</p> <p><i>Encryption context conditions:</i></p> <p>kms:EncryptionContext:key</p> <p>kms:EncryptionContextKeys</p> <p><i>Conditions for KMS key operations:</i></p> <p>kms:CallerAccount</p> <p>kms:KeySpec</p> <p>kms:KeyUsage</p> <p>kms:KeyOrigin</p> <p>kms:MultiRegion</p> <p>kms:MultiRegionKeyType</p>

Actions and permissions	Policy type	Cross-account use	Resources (for IAM policies)	Amazon KMS condition keys
				kms:ResourceAliases aws:ResourceTag/tag-key (Amazon global condition key) kms:ViaService

Actions and permissions	Policy type	Cross-account use	Resources (for IAM policies)	Amazon KMS condition keys
<p>GenerateDataKeyWithoutPlaintext</p> <p>kms:GenerateDataKeyWithoutPlaintext</p>	Key policy	Yes	KMS key	<p><i>Conditions for cryptographic operations</i></p> <p>kms:EncryptionAlgorithm</p> <p>kms:RequestAlias</p> <p><i>Encryption context conditions:</i></p> <p>kms:EncryptionContext:context-key</p> <p>kms:EncryptionContextKeys</p> <p><i>Conditions for KMS key operations:</i></p> <p>kms:CallerAccount</p> <p>kms:KeySpec</p> <p>kms:KeyUsage</p> <p>kms:KeyOrigin</p> <p>kms:MultiRegion</p> <p>kms:MultiRegionKeyType</p> <p>kms:ResourceAliases</p> <p>aws:ResourceTag/tag-key (Amazon global condition key)</p>

Actions and permissions	Policy type	Cross-account use	Resources (for IAM policies)	Amazon KMS condition keys
				kms:ViaService
GenerateMac kms:GenerateMac	Key policy	Yes	KMS key	<i>Conditions for KMS key operations:</i> kms:CallerAccount kms:KeySpec kms:KeyUsage kms:KeyOrigin kms:MultiRegion kms:MultiRegionKeyType kms:ResourceAliases aws:ResourceTag/tag-key (Amazon global condition key) kms:ViaService <i>Conditions for cryptographic operations:</i> kms:MacAlgorithm kms:RequestAlias
GenerateRandom kms:GenerateRandom	IAM policy	N/A	*	None

Actions and permissions	Policy type	Cross-account use	Resources (for IAM policies)	Amazon KMS condition keys
GetKeyPolicy kms:GetKeyPolicy	Key policy	No	KMS key	<i>Conditions for KMS key operations:</i> kms:CallerAccount kms:KeySpec kms:KeyUsage kms:KeyOrigin kms:MultiRegion kms:MultiRegionKeyType kms:ResourceAliases aws:ResourceTag/tag-key (Amazon global condition key) kms:ViaService

Actions and permissions	Policy type	Cross-account use	Resources (for IAM policies)	Amazon KMS condition keys
GetKeyRotationStatus kms:GetKeyRotationStatus	Key policy	Yes	KMS key	Conditions for KMS key operations: kms:CallerAccount kms:KeySpec kms:KeyUsage kms:KeyOrigin kms:MultiRegion kms:MultiRegionKeyType kms:ResourceAliases aws:ResourceTag/tag-key (Amazon global condition key) kms:ViaService

Actions and permissions	Policy type	Cross-account use	Resources (for IAM policies)	Amazon KMS condition keys
GetParametersForImport kms:GetParametersForImport	Key policy	No	KMS key	kms:WrappingAlgorithm kms:WrappingKeySpec <i>Conditions for KMS key operations:</i> kms:CallerAccount kms:KeySpec kms:KeyUsage kms:KeyOrigin kms:MultiRegion kms:MultiRegionKeyType kms:ResourceAliases aws:ResourceTag/tag-key (Amazon global condition key) kms:ViaService

Actions and permissions	Policy type	Cross-account use	Resources (for IAM policies)	Amazon KMS condition keys
GetPublicKey kms:GetPublicKey	Key policy	Yes	KMS key	<p><i>Conditions for KMS key operations:</i></p> <p>kms:CallerAccount</p> <p>kms:KeySpec</p> <p>kms:KeyUsage</p> <p>kms:KeyOrigin</p> <p>kms:MultiRegion</p> <p>kms:MultiRegionKeyType</p> <p>kms:ResourceAliases</p> <p>aws:ResourceTag/tag-key (Amazon global condition key)</p> <p>kms:ViaService</p> <p><i>Other conditions:</i></p> <p>kms:RequestAlias</p>

Actions and permissions	Policy type	Cross-account use	Resources (for IAM policies)	Amazon KMS condition keys
ImportKeyMaterial kms:ImportKeyMaterial	Key policy	No	KMS key	<p><i>Conditions for KMS key operations:</i></p> <p>kms:CallerAccount</p> <p>kms:KeySpec</p> <p>kms:KeyUsage</p> <p>kms:KeyOrigin</p> <p>kms:MultiRegion</p> <p>kms:MultiRegionKeyType</p> <p>kms:ResourceAliases</p> <p>aws:ResourceTag/tag-key (Amazon global condition key)</p> <p>kms:ViaService</p> <p><i>Other conditions:</i></p> <p>kms:ExpirationModel</p> <p>kms:ValidTo</p>
ListAliases kms:ListAliases	IAM policy	No	*	None

Actions and permissions	Policy type	Cross-account use	Resources (for IAM policies)	Amazon KMS condition keys
<p>ListGrants</p> <p>kms:ListGrants</p>	Key policy	Yes	KMS key	<p><i>Conditions for KMS key operations:</i></p> <p>kms:CallerAccount</p> <p>kms:KeySpec</p> <p>kms:KeyUsage</p> <p>kms:KeyOrigin</p> <p>kms:MultiRegion</p> <p>kms:MultiRegionKeyType</p> <p>kms:ResourceAliases</p> <p>aws:ResourceTag/tag-key (Amazon global condition key)</p> <p>kms:ViaService</p> <p><i>Other conditions:</i></p> <p>kms:GrantIsForResource</p>

Actions and permissions	Policy type	Cross-account use	Resources (for IAM policies)	Amazon KMS condition keys
ListKeyPolicies kms:ListKeyPolicies	Key policy	No	KMS key	<i>Conditions for KMS key operations:</i> kms:CallerAccount kms:KeySpec kms:KeyUsage kms:KeyOrigin kms:MultiRegion kms:MultiRegionKeyType kms:ResourceAliases aws:ResourceTag/tag-key (Amazon global condition key) kms:ViaService

Actions and permissions	Policy type	Cross-account use	Resources (for IAM policies)	Amazon KMS condition keys
ListKeyRotations kms:ListKeyRotations	Key policy	No	KMS key	Conditions for KMS key operations: kms:CallerAccount kms:KeySpec kms:KeyUsage kms:KeyOrigin kms:MultiRegion kms:MultiRegionKeyType kms:ResourceAliases aws:ResourceTag/tag-key (Amazon global condition key) kms:ViaService
ListKeys kms:ListKeys	IAM policy	No	*	None

Actions and permissions	Policy type	Cross-account use	Resources (for IAM policies)	Amazon KMS condition keys
ListResourceTags kms:ListResourceTags	Key policy	No	KMS key	<i>Conditions for KMS key operations:</i> kms:CallerAccount kms:KeySpec kms:KeyUsage kms:KeyOrigin kms:MultiRegion kms:MultiRegionKeyType kms:ResourceAliases aws:ResourceTag/tag-key (Amazon global condition key) kms:ViaService
ListRetirableGrants kms:ListRetirableGrants	IAM policy	The specified principal must be in the local account, but the operation returns grants in all accounts.	*	None

Actions and permissions	Policy type	Cross-account use	Resources (for IAM policies)	Amazon KMS condition keys
PutKeyPolicy kms:PutKeyPolicy	Key policy	No	KMS key	<p><i>Conditions for KMS key operations:</i></p> <p>kms:CallerAccount</p> <p>kms:KeySpec</p> <p>kms:KeyUsage</p> <p>kms:KeyOrigin</p> <p>kms:MultiRegion</p> <p>kms:MultiRegionKeyType</p> <p>kms:ResourceAliases</p> <p>aws:ResourceTag/tag-key (Amazon global condition key)</p> <p>kms:ViaService</p> <p><i>Other conditions:</i></p> <p>kms:BypassPolicyLockoutSafetyCheck</p>

Actions and permissions	Policy type	Cross-account use	Resources (for IAM policies)	Amazon KMS condition keys
<p>ReEncrypt</p> <p><code>kms:ReEncryptFrom</code></p> <p><code>kms:ReEncryptTo</code></p> <p>To use this operation, the caller needs permission on two KMS keys:</p> <ul style="list-style-type: none"> <code>kms:ReEncryptFrom</code> on the KMS key used to decrypt <code>kms:ReEncryptTo</code> on the KMS key used to encrypt 	Key policy	Yes	KMS key	<p><i>Conditions for cryptographic operations</i></p> <p>kms:EncryptionAlgorithm</p> <p>kms:RequestAlias</p> <p><i>Encryption context conditions:</i></p> <p>kms:EncryptionContext:key</p> <p>kms:EncryptionContextKeys</p> <p><i>Conditions for KMS key operations:</i></p> <p>kms:CallerAccount</p> <p>kms:KeySpec</p> <p>kms:KeyUsage</p> <p>kms:KeyOrigin</p> <p>kms:MultiRegion</p> <p>kms:MultiRegionKeyType</p> <p>kms:ResourceAliases</p> <p>aws:ResourceTag/tag-key (Amazon global condition key)</p>

Actions and permissions	Policy type	Cross-account use	Resources (for IAM policies)	Amazon KMS condition keys
				kms:ViaService <i>Other conditions:</i> kms:ReEncryptOnSameKey
<p>ReplicateKey</p> <p><code>kms:ReplicateKey</code></p> <p>To use this operation, the caller needs the following permissions:</p> <ul style="list-style-type: none"> <code>kms:ReplicateKey</code> on the multi-Region primary key <code>kms:CreateKey</code> in an IAM policy in the replica Region 	Key policy	No	KMS key	<p><i>Conditions for KMS key operations:</i></p> <p>kms:CallerAccount</p> <p>kms:KeySpec</p> <p>kms:KeyUsage</p> <p>kms:KeyOrigin</p> <p>kms:MultiRegion</p> <p>kms:MultiRegionKeyType</p> <p>kms:ResourceAliases</p> <p>aws:ResourceTag/tag-key (Amazon global condition key)</p> <p>kms:ViaService</p> <p><i>Other conditions:</i></p> <p>kms:ReplicaRegion</p>

Actions and permissions	Policy type	Cross-account use	Resources (for IAM policies)	Amazon KMS condition keys
<p>RetireGrant</p> <p><code>kms:RetireGrant</code></p> <p>Permission to retire a grant is determined primarily by the grant. A policy alone cannot allow access to this operation. For more information, see Retiring and revoking grants.</p>	<p>IAM policy</p> <p>(This permission is not effective in a key policy.)</p>	<p>Yes</p>	<p>KMS key</p>	<p><i>Encryption context conditions:</i></p> <p>kms:EncryptionContext:context-key</p> <p>kms:EncryptionContextKeys</p> <p><i>Grant conditions:</i></p> <p>kms:GrantConstraintType</p> <p><i>Conditions for KMS key operations:</i></p> <p>kms:CallerAccount</p> <p>kms:ResourceAliases</p> <p>aws:ResourceTag/tag-key (Amazon global condition key)</p> <p>kms:ViaService</p>

Actions and permissions	Policy type	Cross-account use	Resources (for IAM policies)	Amazon KMS condition keys
RevokeGrant kms:RevokeGrant	Key policy	Yes	KMS key	<p><i>Conditions for KMS key operations:</i></p> <p>kms:CallerAccount</p> <p>kms:KeySpec</p> <p>kms:KeyUsage</p> <p>kms:KeyOrigin</p> <p>kms:MultiRegion</p> <p>kms:MultiRegionKeyType</p> <p>kms:ResourceAliases</p> <p>aws:ResourceTag/tag-key (Amazon global condition key)</p> <p>kms:ViaService</p> <p><i>Other conditions:</i></p> <p>kms:GrantIsForResource</p>

Actions and permissions	Policy type	Cross-account use	Resources (for IAM policies)	Amazon KMS condition keys
<p>RotateKeyOnDemand</p> <p>kms:RotateKeyOnDemand</p>	Key policy	No	KMS key	<p><i>Conditions for KMS key operations:</i></p> <p>kms:CallerAccount</p> <p>kms:KeySpec</p> <p>kms:KeyUsage</p> <p>kms:KeyOrigin</p> <p>kms:MultiRegion</p> <p>kms:MultiRegionKeyType</p> <p>kms:ResourceAliases</p> <p>aws:ResourceTag/tag-key (Amazon global condition key)</p> <p>kms:ViaService</p>

Actions and permissions	Policy type	Cross-account use	Resources (for IAM policies)	Amazon KMS condition keys
ScheduleKeyDeletion kms:ScheduleKeyDeletion	Key policy	No	KMS key	<i>Conditions for KMS key operations:</i> kms:CallerAccount kms:KeySpec kms:KeyUsage kms:KeyOrigin kms:MultiRegion kms:MultiRegionKeyType kms:ResourceAliases aws:ResourceTag/tag-key (Amazon global condition key) kms:ViaService

Actions and permissions	Policy type	Cross-account use	Resources (for IAM policies)	Amazon KMS condition keys
<p>Sign</p> <p>kms:Sign</p>	Key policy	Yes	KMS key	<p><i>Conditions for signing and verification:</i></p> <p>kms:MessageType kms:RequestAlias</p> <p>kms:SigningAlgorithm</p> <p><i>Conditions for KMS key operations:</i></p> <p>kms:CallerAccount</p> <p>kms:KeySpec</p> <p>kms:KeyUsage</p> <p>kms:KeyOrigin</p> <p>kms:MultiRegion</p> <p>kms:MultiRegionKeyType</p> <p>kms:ResourceAliases</p> <p>aws:ResourceTag/tag-key (Amazon global condition key)</p> <p>kms:ViaService</p>

Actions and permissions	Policy type	Cross-account use	Resources (for IAM policies)	Amazon KMS condition keys
TagResource kms:TagResource	Key policy	No	KMS key	<p><i>Conditions for KMS key operations:</i></p> <p>kms:CallerAccount</p> <p>kms:KeySpec</p> <p>kms:KeyUsage</p> <p>kms:KeyOrigin</p> <p>kms:MultiRegion</p> <p>kms:MultiRegionKeyType</p> <p>kms:ResourceAliases</p> <p>aws:ResourceTag/tag-key (Amazon global condition key)</p> <p>kms:ViaService</p> <p><i>Conditions for tagging:</i></p> <p>aws:RequestTag/tag-key (Amazon global condition key)</p> <p>aws:TagKeys (Amazon global condition key)</p>

Actions and permissions	Policy type	Cross-account use	Resources (for IAM policies)	Amazon KMS condition keys
<p>UntagResource</p> <p>kms:UntagResource</p>	Key policy	No	KMS key	<p><i>Conditions for KMS key operations:</i></p> <p>kms:CallerAccount</p> <p>kms:KeySpec</p> <p>kms:KeyUsage</p> <p>kms:KeyOrigin</p> <p>kms:MultiRegion</p> <p>kms:MultiRegionKeyType</p> <p>kms:ResourceAliases</p> <p>aws:ResourceTag/tag-key (Amazon global condition key)</p> <p>kms:ViaService</p> <p><i>Conditions for tagging:</i></p> <p>aws:RequestTag/tag-key (Amazon global condition key)</p> <p>aws:TagKeys (Amazon global condition key)</p>

Actions and permissions	Policy type	Cross-account use	Resources (for IAM policies)	Amazon KMS condition keys
<p>UpdateAlias</p> <p><code>kms:UpdateAlias</code></p> <p>To use this operation, the caller needs <code>kms:UpdateAlias</code> permission on three resources:</p> <ul style="list-style-type: none"> The alias The currently associated KMS key The newly associated KMS key <p>For details, see Controlling access to aliases.</p>	IAM policy (for the alias)	No	Alias	None (when controlling access to the alias)
	Key policy (for the KMS keys)	No	KMS key	<p><i>Conditions for KMS key operations:</i></p> <p>kms:CallerAccount</p> <p>kms:KeySpec</p> <p>kms:KeyUsage</p> <p>kms:KeyOrigin</p> <p>kms:MultiRegion</p> <p>kms:MultiRegionKeyType</p> <p>kms:ResourceAliases</p> <p>aws:ResourceTag/tag-key (Amazon global condition key)</p> <p>kms:ViaService</p>
<p>UpdateCustomKeyStore</p> <p><code>kms:UpdateCustomKeyStore</code></p>	IAM policy	No	*	kms:CallerAccount

Actions and permissions	Policy type	Cross-account use	Resources (for IAM policies)	Amazon KMS condition keys
<p>UpdateKeyDescription</p> <p>kms:UpdateKeyDescription</p>	Key policy	No	KMS key	<p><i>Conditions for KMS key operations:</i></p> <p>kms:CallerAccount</p> <p>kms:KeySpec</p> <p>kms:KeyUsage</p> <p>kms:KeyOrigin</p> <p>kms:MultiRegion</p> <p>kms:MultiRegionKeyType</p> <p>kms:ResourceAliases</p> <p>aws:ResourceTag/tag-key (Amazon global condition key)</p> <p>kms:ViaService</p>

Actions and permissions	Policy type	Cross-account use	Resources (for IAM policies)	Amazon KMS condition keys
<p>UpdatePrimaryRegion</p> <p><code>kms:UpdatePrimaryRegion</code></p> <p>To use this operation, the caller needs <code>kms:UpdatePrimaryRegion</code> permission on both the multi-Region primary key that will become a replica key and the multi-Region replica key that will become the primary key.</p>	Key policy	No	KMS key	<p><i>Conditions for KMS key operations:</i></p> <p>kms:CallerAccount</p> <p>kms:KeySpec</p> <p>kms:KeyUsage</p> <p>kms:KeyOrigin</p> <p>kms:MultiRegion</p> <p>kms:MultiRegionKeyType</p> <p>kms:ResourceAliases</p> <p>aws:ResourceTag/tag-key (Amazon global condition key)</p> <p>kms:ViaService</p> <p><i>Other conditions</i></p> <p>kms:PrimaryRegion</p>

Actions and permissions	Policy type	Cross-account use	Resources (for IAM policies)	Amazon KMS condition keys
Verify kms:Verify	Key policy	Yes	KMS key	<p><i>Conditions for signing and verification:</i></p> <p>kms:MessageType kms:RequestAlias kms:SigningAlgorithm</p> <p><i>Conditions for KMS key operations:</i></p> <p>kms:CallerAccount kms:KeySpec kms:KeyUsage kms:KeyOrigin kms:MultiRegion kms:MultiRegionKeyType kms:ResourceAliases aws:ResourceTag/tag-key (Amazon global condition key) kms:ViaService</p>

Actions and permissions	Policy type	Cross-account use	Resources (for IAM policies)	Amazon KMS condition keys
VerifyMac kms:VerifyMac	Key policy	Yes	KMS key	<p><i>Conditions for KMS key operations:</i></p> <p>kms:CallerAccount</p> <p>kms:KeySpec</p> <p>kms:KeyUsage</p> <p>kms:KeyOrigin</p> <p>kms:MultiRegion</p> <p>kms:MultiRegionKeyType</p> <p>kms:ResourceAliases</p> <p>aws:ResourceTag/tag-key (Amazon global condition key)</p> <p><i>Conditions for cryptographic operations:</i></p> <p>kms:ViaService</p> <p>kms:MacAlgorithm</p> <p>kms:RequestAlias</p>

Column descriptions

The columns in this table provide the following information:

- **Actions and permissions** lists each Amazon KMS API operation and the permission that allows the operation. You specify the operation in Action element of a policy statement.
- **Policy type** indicates whether the permission can be used in a key policy or IAM policy.

Key policy means that you can specify the permission in the key policy. When the key policy contains the [policy statement that enables IAM policies](#), you can specify the permission in an IAM policy.

IAM policy means that you can specify the permission only in an IAM policy.

- **Cross-account use** shows the operations that authorized users can perform on resources in a different Amazon Web Services account.

A value of *Yes* means that principals can perform the operation on resources in a different Amazon Web Services account.

A value of *No* means that principals can perform the operation only on resources in their own Amazon Web Services account.

If you give a principal in a different account a permission that can't be used on a cross-account resource, the permission is not effective. For example, if you give a principal in a different account [kms:TagResource](#) permission to a KMS key in your account, their attempts to tag the KMS key in your account will fail.

- **Resources** lists the Amazon KMS resources to which the permissions apply. Amazon KMS supports two resource types: a KMS key and an alias. In a key policy, the value of the Resource element is always `*`, which indicates the KMS key to which the key policy is attached.

Use the following values to represent an Amazon KMS resource in an IAM policy.

KMS key

When the resource is a KMS key, use its [key ARN](#). For help, see [the section called "Find the key ID and key ARN"](#).

```
arn:Amazon_partition_name:kms:Amazon_Region:Amazon_account_ID:key/key_ID
```

For example:

```
arn:aws:kms:us-west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab
```

Alias

When the resource is an alias, use its [alias ARN](#). For help, see [the section called "Find the alias name and alias ARN"](#).

```
arn:Amazon_partition_name:kms:Amazon_region:Amazon_account_ID:alias/alias_name
```

For example:

```
arn:aws:kms:us-west-2:111122223333:alias/ExampleAlias
```

* (asterisk)

When the permission doesn't apply to a particular resource (KMS key or alias), use an asterisk (*).

In an IAM policy for an Amazon KMS permission, an asterisk in the `Resource` element indicates all Amazon KMS resources (KMS keys and aliases). You can also use an asterisk in the `Resource` element when the Amazon KMS permission doesn't apply to any particular KMS keys or aliases. For example, when allowing or denying `kms:CreateKey` or `kms:ListKeys` permission, you must set the `Resource` element to `*`.

- **Amazon KMS condition keys** lists the Amazon KMS condition keys that you can use to control access to the operation. You specify conditions in a policy's `Condition` element. For more information, see [Amazon KMS condition keys](#). This column also includes [Amazon global condition keys](#) that are supported by Amazon KMS, but not by all Amazon services.

Amazon KMS internal operations

Amazon Key Management Service (Amazon KMS) provides cryptographic keys and operations secured by [FIPS 140-3 Security Level 3 validated hardware security modules \(HSM\)](#) scaled for the cloud. Amazon KMS keys and functionality are used by multiple Amazon cloud services, and you can use them to protect data in your applications. This technical guide provides details on the cryptographic operations that are run within Amazon when you use Amazon KMS.

Amazon KMS internals are required to scale and secure HSMs for a globally distributed key management service.

Topics

- [Domains and domain state](#)
- [Internal communication security](#)
- [Replication process for multi-Region keys](#)
- [Durability protection](#)

Domains and domain state

A cooperative collection of trusted internal Amazon KMS entities within an Amazon Web Services Region is referred to as a domain. A domain includes a set of trusted entities, a set of rules, and a set of secret keys, called domain keys. The domain keys are shared among HSMs that are members of the domain. A domain state consists of the following fields.

Name

A domain name to identify this domain.

Members

A list of HSMs that are members of the domain, including their public signing key and public agreement keys.

Operators

A list of entities, public signing keys, and a role (Amazon KMS operator or service host) that represents the operators of this service.

Rules

A list of quorum rules for each command that must be satisfied to run a command on the HSM.

Domain keys

A list of domain keys (symmetric keys) currently in use within the domain.

The full domain state is available only on the HSM. The domain state is synchronized between HSM domain members as an exported domain token.

Domain keys

All the HSMs in a domain share a set of domain keys, $\{DK_r\}$. These keys are shared through a domain state export routine. The exported domain state can be imported into any HSM that is a member of the domain.

The set of domain keys, $\{DK_r\}$, always includes one active domain key, and several deactivated domain keys. Domain keys are rotated daily to ensure that Amazon complies with [Recommendation for Key Management - Part 1](#). During domain key rotation, all existing KMS keys encrypted under the outgoing domain key are re-encrypted under the new active domain key. The active domain key is used to encrypt any new EKTs. The expired domain keys can be used only

to decrypt previously encrypted EKTs for a number of days equivalent to the number of recently rotated domain keys.

Exported domain tokens

There is a regular need to synchronize state between domain participants. This is accomplished through exporting the domain state whenever a change is made to the domain. The domain state is exported as an exported domain token.

Name

A domain name to identify this domain.

Members

A list of HSMs that are members of the domain, including their signing and agreement public keys.

Operators

A list of entities, public signing keys, and a role that represents the operators of this service.

Rules

A list of quorum rules for each command that must be satisfied to run a command on an HSM domain member.

Encrypted domain keys

Envelope-encrypted domain keys. The domain keys are encrypted by the signing member for each of the members listed above, enveloped to their public agreement key.

Signature

A signature on the domain state produced by an HSM, necessarily a member of the domain that exported the domain state.

The exported domain token forms the fundamental source of trust for entities operating within the domain.

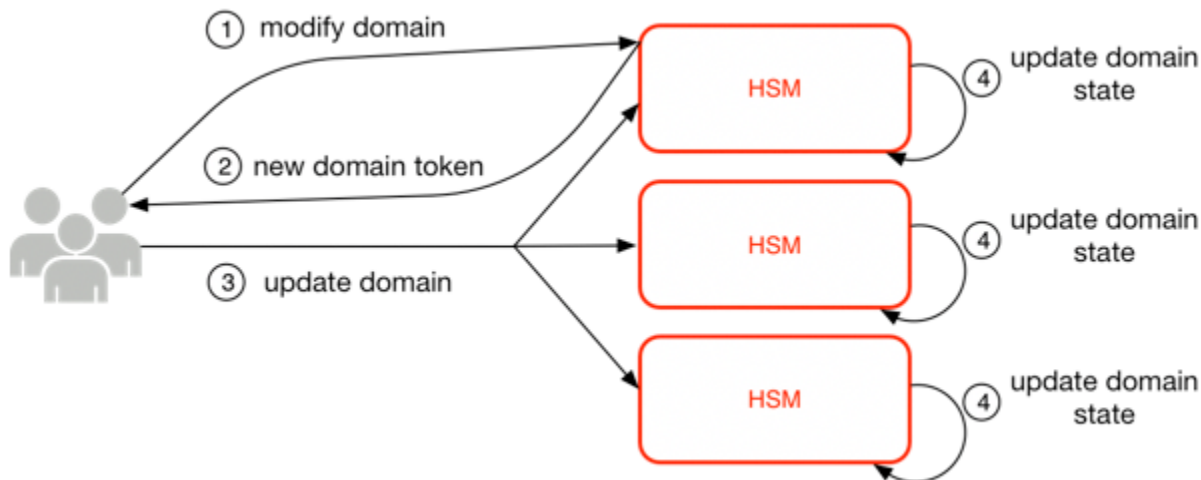
Managing domain states

The domain state is managed through quorum-authenticated commands. These changes include modifying the list of trusted participants in the domain, modifying the quorum rules for running

HSM commands, and periodically rotating the domain keys. These commands are authenticated on a per-command basis as opposed to authenticated session operations, as shown in the following image.

In its initialized and operational state, an HSM contains a set of self-generated asymmetric identity keys, a signing key pair, and a key-establishment key pair. Through a manual process, an Amazon KMS operator can establish an initial domain to be created on a first HSM in a Region. This initial domain consists of a full domain state as defined previously in this topic. It is installed through a join command to each of the defined HSM members in the domain.

After an HSM has joined an initial domain, it is bound to the rules that are defined in that domain. These rules govern the commands that use customer cryptographic keys or make changes to the host or domain state. The authenticated session API operations that use your cryptographic keys have been defined earlier.



The foregoing image depicts how a domain state gets modified. The process consists of four steps:

1. A quorum-based command is sent to an HSM to modify the domain.
2. A new domain state is generated and exported as a new exported domain token. The state on the HSM is not modified, meaning that the change is not enacted on the HSM.
3. A second command is sent to each of the HSMs in the newly exported domain token to update their domain state with the new domain token.
4. The HSMs listed in the new exported domain token can authenticate the command and the domain token. They can also unpack the domain keys to update the domain state on all HSMs in the domain.

HSMs do not communicate directly with one another. Instead, a quorum of operators requests a change to the domain state that results in a new exported domain token. A service host member of the domain is used to distribute the new domain state to every HSM in the domain.

The leaving and joining of a domain are done through the HSM management functions. The modification of the domain state is done through the domain management functions.

Leave domain

Causes an HSM to leave a domain, deleting all remnants and keys of that domain from memory.

Join domain

Causes an HSM to join a new domain or update its current domain state to the new domain state. The existing domain is used as source of the initial set of rules to authenticate this message.

Create domain

Causes a new domain to be created on an HSM. Returns a first domain token that can be distributed to member HSMs of the domain.

Modify operators

Adds or removes operators from the list of authorized operators and their roles in the domain.

Modify members

Adds or removes an HSM from the list of authorized HSMs in the domain.

Modify rules

Modifies the set of quorum rules that are required to run commands on an HSM.

Rotate domain keys

Causes a new domain key to be created and marked as the active domain key. This moves the existing active key to a deactivated key and removes the oldest deactivated key from the domain state.

Internal communication security

Commands between the service hosts or Amazon KMS operators and the HSMs are secured through two mechanisms depicted in [Authenticated sessions](#): a quorum-signed request method and an authenticated session using an HSM-service host protocol.

The quorum-signed commands are designed so that no single operator can modify the critical security protections that the HSMs provide. The commands that run over the authenticated sessions help ensure that only authorized service operators can perform operations involving KMS keys. All customer-bound secret information is secured across the Amazon infrastructure.

Key establishment

To secure internal communications, Amazon KMS uses two different *key establishment* methods. The first is defined as C(1, 2, ECC DH) in [Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography \(Revision 2\)](#). This scheme has an initiator with a static signing key. The initiator generates and signs an ephemeral elliptic curve Diffie-Hellman (ECDH) key, intended for a recipient with a static ECDH agreement key. This method uses one ephemeral key and two static keys using ECDH. That is the derivation of the label C(1, 2, ECC DH). This method is sometimes called one-pass ECDH.

The second key establishment method is [C\(2, 2, ECC, DH\)](#). In this scheme, both parties have a static signing key, and they generate, sign, and exchange an ephemeral ECDH key. This method uses two static keys and two ephemeral keys, each using ECDH. That is the derivation of the label C(2, 2, ECC, DH). This method is sometimes called ECDH ephemeral or ECDHE. All ECDH keys are generated on the curve secp384r1 (NIST-P384).

HSM security boundary

The inner *security boundary* of Amazon KMS is the HSM. The HSM has a proprietary interface and no other active physical interfaces in its operational state. An operational HSM is provisioned during initialization with the necessary cryptographic keys to establish its role in the domain. Sensitive cryptographic materials of the HSM are only stored in volatile memory and erased when the HSM moves out of the operational state, including intended or unintended shutdowns or resets.

The HSM API operations are authenticated either by individual commands or over a mutually authenticated confidential session established by a service host.



Quorum-signed commands

Quorum-signed commands are issued by operators to HSMs. This section describes how quorum-based commands are created, signed, and authenticated. These rules are fairly simple. For example, command *Foo* requires two members from role *Bar* to be authenticated. There are three steps in the creation and verification of a quorum-based command. The first step is the initial command creation; the second is the submission to additional operators to sign; and the third is the verification and execution.

For the purpose of introducing the concepts, assume that there is an authentic set of operator's public keys and roles $\{QOS_s\}$, and a set of quorum-rules $QR = \{Command_i, Rule_{\{i, t\}}\}$ where each *Rule* is a set of roles and minimum number $N \{Role_t, N_t\}$. For a command to satisfy the quorum rule, the command dataset must be signed by a set of operators listed in $\{QOS_s\}$ such that they meet one of the rules listed for that command. As mentioned earlier, the set of quorum rules and operators are stored in the domain state and the exported domain token.

In practice, an initial signer signs the command $Sig_1 = Sign(dO_{p1}, Command)$. A second operator also signs the command $Sig_2 = Sign(dO_{p2}, Command)$. The doubly signed message is sent to an HSM for execution. The HSM performs the following:

1. For each signature, it extracts the signer's public key from the domain state and verifies the signature on the command.
2. It verifies that the set of signers satisfies a rule for the command.

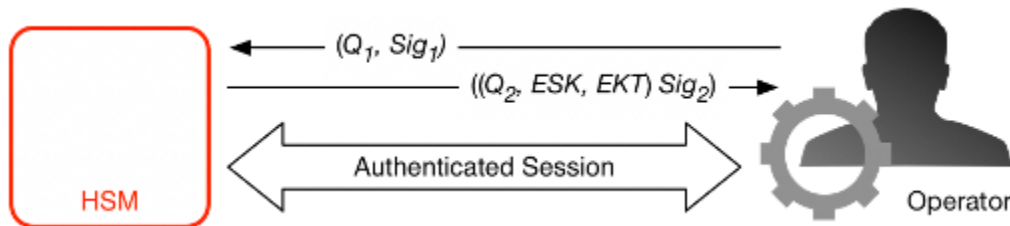
Authenticated sessions

Your key operations run between the externally facing Amazon KMS hosts and the HSMs. These commands pertain to the creation and use of cryptographic keys and secure random number generation. The commands run over a session-authenticated channel between the service hosts and the HSMs. In addition to the need for authenticity, these sessions require confidentiality. Commands running over these sessions include the returning of cleartext data keys and decrypted messages intended for you. To ensure that these sessions cannot be subverted through man-in-the-middle attacks, sessions are authenticated.

This protocol performs a mutually authenticated ECDHE key agreement between the HSM and the service host. The exchange is initiated by the service host and completed by the HSM. The HSM also returns a session key (SK) encrypted by the negotiated key and an exported key token that

contains the session key. The exported key token contains a validity period, after which the service host must renegotiate a session key.

A service host is a member of the domain and has an identity-signing key pair $(dHOS_i, QHOS_i)$ and an authentic copy of the HSMs' identity public keys. It uses its set of identity-signing keys to securely negotiate a session key that can be used between the service host and any HSM in the domain. The exported key tokens have a validity period associated with them, after which a new key must be negotiated.



The process begins with the service host recognition that it requires a session key to send and receive sensitive communication flows between itself and an HSM member of the domain.

1. A service host generates an ECDH ephemeral key pair (d_1, Q_1) and signs it with its identity key $Sig1 = Sign(dOS, Q_1)$.
2. The HSM verifies the signature on the received public key using its current domain token and creates an ECDH ephemeral key pair (d_2, Q_2) . It then completes the ECDH-key-exchange according to [Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography \(Revised\)](#) to form a negotiated 256-bit AES-GCM key. The HSM generates a fresh 256-bit AES-GCM session key. It encrypts the session key with the negotiated key to form the encrypted session key (ESK). It also encrypts the session key under the domain key as an exported key token EKT . Finally, it signs a return value with its identity key pair $Sig_2 = Sign(dHSM, (Q_2, ESK, EKT))$.
3. The service host verifies the signature on the received keys using its current domain token. The service host then completes the ECDH key exchange according to [Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography \(Revised\)](#). It next decrypts the ESK to obtain the session key SK.

During the validity period in the EKT , the service host can use the negotiated session key SK to send envelope-encrypted commands to the HSM. Every service-host-initiated command over this authenticated session includes the EKT . The HSM responds using the same negotiated session key SK.

Replication process for multi-Region keys

Amazon KMS uses a cross-Region replication mechanism to copy the key material in a KMS key from an HSM in one Amazon Web Services Region to an HSM in a different Amazon Web Services Region. For this mechanism to work, the KMS key that is being replicated must be a multi-Region key. When replicating a KMS key from one Region to another, the HSMs in the Regions cannot communicate directly, because they're in isolated networks. Instead, the messages exchanged during the cross-Region replication are delivered by a proxy service.

During cross-Region replication, every message generated by an Amazon KMS HSM is cryptographically signed using a *replication signing key*. Replication signing keys (RSKs) are ECDSA keys on the NIST P-384 curve. Every Region owns at least one RSK, and the public component of each RSK is shared with every other Region in the same Amazon partition.

The cross-Region replication process to copy key material from Region A to Region B works as follows:

1. The HSM in Region B generates an ephemeral ECDH key on the NIST P-384 curve, *Replication Agreement Key B* (RAKB). The public component of RAKB is sent to an HSM in Region A by the proxy service.
2. The HSM in Region A receives the public component of RAKB and then generates another ephemeral ECDH key on the NIST P-384 curve, *Replication Agreement Key A* (RAKA). The HSM runs the ECDH key establishment scheme on RAKA and the public component of RAKB, and derives a symmetric key from the output, the *Replication Wrapping Key* (RWK). The RWK is used to encrypt the key material of the multi-Region KMS key that is being replicated.
3. The public component of RAKA and the key material encrypted with the RWK are sent to the HSM in Region B through the proxy service.
4. The HSM in Region B receives the public component of RAKA and the key material encrypted using the RWK. The HSM derives by RWK by running the ECDH key establishment scheme on RAKB and the public component of RAKA.
5. The HSM in Region B use the RWK to decrypt the key material from Region A.

Durability protection

Additional service durability for keys generated by the service is provided by the use of offline HSMs, multiple nonvolatile storage of exported domain tokens, and redundant storage of encrypted KMS keys. The offline HSMs are members of the existing domains. With the exception

of not being online and participating in the regular domain operations, the offline HSMs appear identically in the domain state as the existing HSM members.

The durability design is intended to protect all KMS keys in a Region should Amazon experience a wide-scale loss of either the online HSMs or the set of KMS keys stored within our primary storage system. Amazon KMS keys with imported key material are not included under the durability protections afforded other KMS keys. In the event of a Regionwide failure in Amazon KMS, imported key material may need to be reimported into a KMS key.

The offline HSMs, and the credentials to access them, are stored in safes within monitored safe rooms in multiple independent geographical locations. Each safe requires at least one Amazon security officer and one Amazon KMS operator, from two independent teams in Amazon, to obtain these materials. The use of these materials is governed by internal policy requiring a quorum of Amazon KMS operators to be present.

Document history

This topic describes significant updates to the *Amazon Key Management Service Developer Guide*.

Topics

- [Recent updates](#)
- [Earlier updates](#)

Recent updates

The following table describes significant changes to this documentation since January 2018. In addition to major changes listed here, we also update the documentation frequently to improve the descriptions and examples, and to address the feedback that you send to us. To be notified about significant changes, subscribe to the RSS feed.

You might need to scroll horizontally or vertically to see all of the data in this table.

Change	Description	Date
Feature update	Added support for multi-Region KMS keys in China Regions.	November 21, 2024
Amazon managed policy update	Updated the AWSKeyManagementServiceMultiRegionKeysServiceRolePolicy service-linked role by adding a statement ID (Sid) to the managed policy with policy version v2.	November 21, 2024
Quota change	Increased the default request rate for ImportKeyMaterial and DeleteImportedKeyMaterial requests.	July 23, 2024

Quota change	Increased the default cryptographic operations request rate for symmetric encryption KMS keys, RSA KMS keys, and ECC and SM2 KMS keys.	July 8, 2024
New feature	Added new KeyUsage type KEY_AGREEMENT for NIST-recommended elliptic curve (ECC) and SM2 (China Regions only) KMS keys and added support to derive shared secrets .	June 13, 2024
Updates to key rotation	Added support for custom rotation periods for automatic key rotations, on-demand key rotations, and visibility into your key material rotations.	April 12, 2024
Updates to managed policy	Added new permissions to AWSKeyManagementServiceCustomKeyStoresServiceRolePolicy that allow Amazon KMS to monitor changes in the VPC that contains your Amazon CloudHSM cluster so that Amazon KMS can provide clear error messages in the case of failures.	November 10, 2023
Feature update	Added support for the DryRun API parameter.	July 5, 2023

Feature update	Added support for importing key material for all types of Amazon KMS keys, except custom key stores.	June 5, 2023
Feature update	Updates to Amazon KMS APIs for Nitro Enclaves	March 10, 2023
Feature update	The RSAES_PKCS1_V1_5 wrapping algorithm is deprecated. Amazon KMS will end all support for RSAES_PKCS1_V1_5 by October 1, 2023 pursuant to cryptographic key management guidance from the National Institute of Standards and Technology (NIST). We recommend that you begin using a different wrapping algorithm immediately.	February 28, 2023
Feature update	Added support for External key stores, a feature that lets you protect your Amazon resources using cryptographic keys outside of Amazon.	November 29, 2022
Quota change	Increased the Amazon KMS keys resource quota to 100,000 KMS keys in each account and Region.	July 8, 2022
Feature update	Added support for HMAC KMS keys in more Amazon Web Services Regions	July 8, 2022

New topic	Added the Resilience in Amazon Key Management Service topic to the Security chapter of the Amazon KMS Developer Guide.	June 14, 2022
New feature	Added support for Amazon KMS keys and API operations that generate and verify HMAC codes.	April 19, 2022
Documentation change	Replace the term <i>customer master key (CMK)</i> with <i>Amazon KMS key</i> and <i>KMS key</i> .	August 30, 2021
New feature	Added support for multi-Region keys , a set of interoperable KMS keys in different Regions that have the same key ID and key material. You can use multi-Region keys to encrypt data in one Region and decrypt data in a different Region.	June 8, 2021
New feature	Added support for attribute based access control (ABAC). You can use tags and aliases to control access to your Amazon KMS keys.	December 17, 2020
New feature	Added support for VPC endpoint policies.	July 9, 2020
New content	Explains the security properties of Amazon KMS.	June 18, 2020

New feature	Added support for asymmetric Amazon KMS keys and asymmetric data keys.	November 25, 2019
Updated feature	You can view the key policy of Amazon managed keys in the Amazon KMS console. This feature used to be limited to customer managed keys.	November 15, 2019
New feature	Explains how to use hybrid post-quantum key exchange algorithms in TLS for your calls to Amazon KMS.	November 4, 2019
Quota change	Increased the resource quotas for some APIs that manage KMS keys.	September 18, 2019
Quota change	Changed the resource quotas for KMS keys, aliases, and grants per KMS key.	March 27, 2019
Quota change	Changed the shared per-second request quota for cryptographic operations that use Amazon KMS keys in a custom key store.	March 7, 2019
New feature	Explains how to create and manage Amazon KMS custom key stores . Each key store is backed by an Amazon CloudHSM cluster that you own and control.	November 26, 2018

New console	Explains how to use the new Amazon KMS console, which is independent of the IAM console. The original console, and instructions for using it, will remain available for a brief period to give you time to familiarize yourself with the new console.	November 7, 2018
Quota change	Changed the shared request quota for use of Amazon KMS keys.	August 21, 2018
New content	Explains how Amazon Secrets Manager uses Amazon KMS keys to encrypt the secret value in a secret.	July 13, 2018
New content	Explains how DynamoDB uses Amazon KMS Amazon KMS keys to support its server-side encryption option.	May 23, 2018
New feature	Explains how to use a private endpoint in your VPC to connect directly to Amazon KMS, instead of connecting over the internet.	January 22, 2018

Earlier updates

The following table describes the important changes to the Amazon Key Management Service Developer Guide prior to 2018.

You might need to scroll horizontally or vertically to see all of the data in this table.

Change	Description	Date
New content	Added documentation about Tags in Amazon KMS .	February 15, 2017
New content	Added documentation about Monitor Amazon KMS keys and Monitor KMS keys with Amazon CloudWatch .	August 31, 2016
New content	Added documentation about Imported key material .	August 11, 2016
New content	Added the following documentation: IAM policies , Permissions reference , and Condition keys .	July 5, 2016
Update	Updated portions of the documentation in the KMS key access and permissions chapter.	July 5, 2016
Update	Updated the Quotas page to reflect new default quotas.	May 31, 2016
Update	Updated the Quotas page to reflect new default quotas, and updated the grant token documentation to improve clarity and accuracy.	April 11, 2016
New content	Added documentation about Allowing multiple IAM principals to access a KMS key and Using the IP address condition .	February 17, 2016

Change	Description	Date
Update	Updated the Key policies in Amazon KMS and Change a key policy pages to improve clarity and accuracy.	February 17, 2016
Update	Updated the Managing KMS keys topic pages to improve clarity.	January 5, 2016
New content	Added documentation about CloudTrail.	November 18, 2015
New content	Added instructions for Change a key policy .	November 18, 2015
Update	Updated the documentation about How Amazon Relational Database Service uses Amazon KMS.	November 18, 2015
New content	Added documentation about Amazon WorkSpaces.	November 6, 2015
Update	Updated the Key policies in Amazon KMS page to improve clarity.	October 22, 2015
New content	Added documentation about Delete an Amazon KMS key , including supporting documentation about Create an alarm and Determine past usage of a KMS key .	October 15, 2015
New content	Added documentation about Determining access to Amazon KMS keys .	October 15, 2015

Change	Description	Date
New content	Added documentation about Key states of Amazon KMS keys .	October 15, 2015
New content	Added documentation about Amazon Simple Email Service.	October 1, 2015
Update	Updated the Quotas page to explain the new request quotas.	August 31, 2015
New content	Added information about the charges for using Amazon KMS. See Amazon KMS Pricing .	August 14, 2015
New content	Added request quotas to the Amazon KMS Quotas .	June 11, 2015
New content	Added a new Java code sample demonstrating use of the UpdateAlias operation .	June 1, 2015
Update	Moved the Amazon Key Management Service regions table to the <i>Amazon Web Services General Reference</i> .	May 29, 2015
New content	Added documentation about How Amazon EMR uses Amazon KMS .	January 28, 2015
New content	Added documentation about Amazon WorkMail.	January 28, 2015

Change	Description	Date
New content	Added documentation about How Amazon Relational Database Service uses Amazon KMS.	January 6, 2015
New content	Added documentation about Amazon Elastic Transcoder.	November 24, 2014
New guide	Introduced the <i>Amazon Key Management Service Developer Guide</i> .	November 12, 2014