<table>
<thead>
<tr>
<th>GenerateDataKey</th>
<th>Encrypt</th>
<th>EnableKeyRotation</th>
<th>DisableKey</th>
<th>EnableKey</th>
<th>Decrypt</th>
</tr>
</thead>
<tbody>
<tr>
<td>Request Syntax</td>
<td>Request Parameters</td>
<td>Request Syntax</td>
<td>Request Parameters</td>
<td>Request Syntax</td>
<td>Request Parameters</td>
</tr>
<tr>
<td>Response Syntax</td>
<td>Response Elements</td>
<td>Errors</td>
<td>Response Elements</td>
<td>Errors</td>
<td>Response Elements</td>
</tr>
<tr>
<td>Examples</td>
<td>Examples</td>
<td>See Also</td>
<td>Examples</td>
<td>See Also</td>
<td>Examples</td>
</tr>
<tr>
<td>See Also</td>
<td>See Also</td>
<td>See Also</td>
<td>See Also</td>
<td>See Also</td>
<td>See Also</td>
</tr>
</tbody>
</table>

API Version 2014-11-01
Welcome

AWS Key Management Service (AWS KMS) is an encryption and key management web service. This guide describes the AWS KMS operations that you can call programmatically. For general information about AWS KMS, see the AWS Key Management Service Developer Guide.

**Note**

AWS provides SDKs that consist of libraries and sample code for various programming languages and platforms (Java, Ruby, .Net, iOS, Android, etc.). The SDKs provide a convenient way to create programmatic access to AWS KMS and other AWS services. For example, the SDKs take care of tasks such as signing requests (see below), managing errors, and retrying requests automatically. For more information about the AWS SDKs, including how to download and install them, see Tools for Amazon Web Services.

We recommend that you use the AWS SDKs to make programmatic API calls to AWS KMS.

Clients must support TLS (Transport Layer Security) 1.0. We recommend TLS 1.2. 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.

**Signing Requests**

Requests must be signed by using an access key ID and a secret access key. We strongly recommend that you **do not** use your AWS account (root) access key ID and secret key for everyday work with AWS KMS. Instead, use the access key ID and secret access key for an IAM user, or you can use the AWS Security Token Service to generate temporary security credentials that you can use to sign requests.

All AWS KMS operations require **Signature Version 4**.

**Logging API Requests**

AWS KMS supports AWS CloudTrail, a service that logs AWS API calls and related events for your AWS account and delivers them to an Amazon S3 bucket that you specify. By using the information collected by CloudTrail, you can determine what requests were made to AWS KMS, who made the request, when it was made, and so on. To learn more about CloudTrail, including how to turn it on and find your log files, see the AWS CloudTrail User Guide.

**Additional Resources**

For more information about credentials and request signing, see the following:

- **AWS Security Credentials** - This topic provides general information about the types of credentials used for accessing AWS.
- **Temporary Security Credentials** - This section of the IAM User Guide describes how to create and use temporary security credentials.
- **Signature Version 4 Signing Process** - This set of topics walks you through the process of signing a request using an access key ID and a secret access key.

**Commonly Used APIs**

Of the APIs discussed in this guide, the following will prove the most useful for most applications. You will likely perform actions other than these, such as creating keys and assigning policies, by using the console.
• Encrypt (p. 46)
• Decrypt (p. 20)
• GenerateDataKey (p. 51)
• GenerateDataKeyWithoutPlaintext (p. 56)

This document was last published on December 20, 2017.
Actions

The following actions are supported:

- CancelKeyDeletion (p. 4)
- CreateAlias (p. 7)
- CreateGrant (p. 10)
- CreateKey (p. 15)
- Decrypt (p. 20)
- DeleteAlias (p. 24)
- DeleteImportedKeyMaterial (p. 27)
- DescribeKey (p. 30)
- DisableKey (p. 34)
- DisableKeyRotation (p. 37)
- EnableKey (p. 40)
- EnableKeyRotation (p. 43)
- Encrypt (p. 46)
- GenerateDataKey (p. 51)
- GenerateDataKeyWithoutPlaintext (p. 56)
- GenerateRandom (p. 61)
- GetKeyPolicy (p. 64)
- GetKeyRotationStatus (p. 67)
- GetParametersForImport (p. 70)
- ImportKeyMaterial (p. 75)
- ListAliases (p. 80)
- ListGrants (p. 84)
- ListKeyPolicies (p. 89)
- ListKeys (p. 93)
- ListResourceTags (p. 97)
- ListRetirableGrants (p. 101)
- PutKeyPolicy (p. 105)
- ReEncrypt (p. 110)
- RetireGrant (p. 115)
- RevokeGrant (p. 118)
- ScheduleKeyDeletion (p. 121)
- TagResource (p. 125)
- UntagResource (p. 128)
- UpdateAlias (p. 131)
- UpdateKeyDescription (p. 134)
CancelKeyDeletion

Cancels the deletion of a customer master key (CMK). When this operation is successful, the CMK is set to the Disabled state. To enable a CMK, use EnableKey (p. 40). You cannot perform this operation on a CMK in a different AWS account.

For more information about scheduling and canceling deletion of a CMK, see Deleting Customer Master Keys in the AWS Key Management Service Developer Guide.

Request Syntax

```
{
   "KeyId": "string"
}
```

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters (p. 147).

The request accepts the following data in JSON format.

**Note**
In the following list, the required parameters are described first.

**KeyId (p. 4)**

The unique identifier for the customer master key (CMK) for which to cancel deletion.

Specify the key ID or the Amazon Resource Name (ARN) of the CMK.

For example:
- Key ID: 1234abcd-12ab-34cd-56ef-1234567890ab
- Key ARN: arn:aws:kms:us-east-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab

To get the key ID and key ARN for a CMK, use ListKeys (p. 93) or DescribeKey (p. 30).

Type: String

Length Constraints: Minimum length of 1. Maximum length of 2048.

Required: Yes

Response Syntax

```
{
   "KeyId": "string"
}
```

Response Elements

If the action is successful, the service sends back an HTTP 200 response.
The following data is returned in JSON format by the service.

**KeyId (p. 4)**

The unique identifier of the master key for which deletion is canceled.

- **Type:** String
- **Length Constraints:** Minimum length of 1. Maximum length of 2048.

**Errors**

For information about the errors that are common to all actions, see [Common Errors (p. 149)](#).

- **DependencyTimeoutException**
  - The system timed out while trying to fulfill the request. The request can be retried.
  - **HTTP Status Code:** 500
- **InvalidArnException**
  - The request was rejected because a specified ARN was not valid.
  - **HTTP Status Code:** 400
- **KMSInternalException**
  - The request was rejected because an internal exception occurred. The request can be retried.
  - **HTTP Status Code:** 400
- **KMSInvalidStateException**
  - The request was rejected because the state of the specified resource is not valid for this request.
  - For more information about how key state affects the use of a CMK, see [How Key State Affects Use of a Customer Master Key](#) in the AWS Key Management Service Developer Guide.
  - **HTTP Status Code:** 400
- **NotFoundException**
  - The request was rejected because the specified entity or resource could not be found.
  - **HTTP Status Code:** 400

**Examples**

**Example Request**

The following example is formatted for legibility.

```bash
POST / HTTP/1.1
Host: kms.us-east-2.amazonaws.com
Content-Length: 48
X-Amz-Target: TrentService.CancelKeyDeletion
X-Amz-Date: 20161025T182658Z
Content-Type: application/x-amz-json-1.1
Authorization: AWS4-HMAC-SHA256
```

API Version 2014-11-01
Example Response

HTTP/1.1 200 OK
Server: Server
Date: Tue, 25 Oct 2016 18:27:01 GMT
Content-Type: application/x-amz-json-1.1
Content-Length: 87
Connection: keep-alive
x-amzn-RequestId: 9f3b3cb8-9ae0-11e6-ac6b-03478315fc57

{"KeyId":"arn:aws:kms:us-east-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab"}

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java
- AWS SDK for JavaScript
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V2
CreateAlias

Creates a display name for a customer master key (CMK). You can use an alias to identify a CMK in selected operations, such as Encrypt (p. 46) and GenerateDataKey (p. 51).

Each CMK can have multiple aliases, but each alias points to only one CMK. The alias name must be unique in the AWS account and region. To simplify code that runs in multiple regions, use the same alias name, but point it to a different CMK in each region.

Because an alias is not a property of a CMK, you can delete and change the aliases of a CMK without affecting the CMK. Also, aliases do not appear in the response from the DescribeKey (p. 30) operation. To get the aliases of all CMKs, use the ListAliases (p. 80) operation.

An alias must start with the word `alias` followed by a forward slash (`alias/`). The alias name can contain only alphanumeric characters, forward slashes (`/`), underscores (`_`), and dashes (`-`). Alias names cannot begin with `aws`; that alias name prefix is reserved by Amazon Web Services (AWS).

The alias and the CMK it is mapped to must be in the same AWS account and the same region. You cannot perform this operation on an alias in a different AWS account.

To map an existing alias to a different CMK, call UpdateAlias (p. 131).

**Request Syntax**

```
{
  "AliasName": "string",
  "TargetKeyId": "string"
}
```

**Request Parameters**

For information about the parameters that are common to all actions, see Common Parameters (p. 147).

The request accepts the following data in JSON format.

**Note**

In the following list, the required parameters are described first.

**AliasName (p. 7)**

String that contains the display name. The name must start with the word "alias" followed by a forward slash (`alias/`). Aliases that begin with "alias/AWS" are reserved.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 256.

Pattern: `^[a-zA-Z0-9:/_\-]+$`

Required: Yes

**TargetKeyId (p. 7)**

Identifies the CMK for which you are creating the alias. This value cannot be an alias.

Specify the key ID or the Amazon Resource Name (ARN) of the CMK.

For example:
• Key ID: 1234abcd-12ab-34cd-56ef-1234567890ab
• Key ARN: arn:aws:kms:us-east-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab

To get the key ID and key ARN for a CMK, use ListKeys (p. 93) or DescribeKey (p. 30).

Type: String

Length Constraints: Minimum length of 1. Maximum length of 2048.

Required: Yes

Response Elements

If the action is successful, the service sends back an HTTP 200 response with an empty HTTP body.

Errors

For information about the errors that are common to all actions, see Common Errors (p. 149).

AlreadyExistsException

The request was rejected because it attempted to create a resource that already exists.

HTTP Status Code: 400

DependencyTimeoutException

The system timed out while trying to fulfill the request. The request can be retried.

HTTP Status Code: 500

InvalidAliasNameException

The request was rejected because the specified alias name is not valid.

HTTP Status Code: 400

KMSInternalException

The request was rejected because an internal exception occurred. The request can be retried.

HTTP Status Code: 400

KMSInvalidStateException

The request was rejected because the state of the specified resource is not valid for this request.

For more information about how key state affects the use of a CMK, see How Key State Affects Use of a Customer Master Key in the AWS Key Management Service Developer Guide.

HTTP Status Code: 400

LimitExceededException

The request was rejected because a limit was exceeded. For more information, see Limits in the AWS Key Management Service Developer Guide.

HTTP Status Code: 400

NotFoundException

The request was rejected because the specified entity or resource could not be found.
HTTP Status Code: 400

Examples

Example Request

The following example is formatted for legibility.

```
POST / HTTP/1.1
Host: kms.us-west-2.amazonaws.com
Content-Length: 87
X-Amz-Target: TrentService.CreateAlias
X-Amz-Date: 20160517T204220Z
Content-Type: application/x-amz-json-1.1
Authorization: AWS4-HMAC-SHA256
  Credential=AKIAI44QH8DHBEXAMPLE/20160517/us-west-2/kms/aws4_request,
  SignedHeaders=content-type;host;x-amz-date;x-amz-target,
  Signature=ca7bcf1e8d5364dc3f0d881c05bdadf36f498c6c6a8b576a060142d9b2199123
{
  "TargetKeyId": "1234abcd-12ab-34cd-56ef-1234567890ab",
  "AliasName": "alias/ExampleAlias"
}
```

Example Response

```
HTTP/1.1 200 OK
Server: Server
Date: Tue, 17 May 2016 20:42:25 GMT
Content-Type: application/x-amz-json-1.1
Content-Length: 0
Connection: keep-alive
x-amzn-RequestId: dcb07ca7-1c6f-11e6-8540-77c363708b91
```

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java
- AWS SDK for JavaScript
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V2
CreateGrant

Adds a grant to a customer master key (CMK). The grant specifies who can use the CMK and under what conditions. When setting permissions, grants are an alternative to key policies.

To perform this operation on a CMK in a different AWS account, specify the key ARN in the value of the KeyId parameter. For more information about grants, see Grants in the AWS Key Management Service Developer Guide.

Request Syntax

```json
{
   "Constraints": {
      "EncryptionContextEquals": {
         "string" : "string"
      },
      "EncryptionContextSubset": {
         "string" : "string"
      }
   },
   "GranteePrincipal": "string",
   "GrantTokens": [ "string" ],
   "KeyId": "string",
   "Name": "string",
   "Operations": [ "string" ],
   "RetiringPrincipal": "string"
}
```

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters (p. 147).

The request accepts the following data in JSON format.

**Note**

In the following list, the required parameters are described first.

**GranteePrincipal (p. 10)**

The principal that is given permission to perform the operations that the grant permits.

To specify the principal, use the Amazon Resource Name (ARN) of an AWS principal. Valid AWS principals include AWS accounts (root), IAM users, IAM roles, federated users, and assumed role users. For examples of the ARN syntax to use for specifying a principal, see AWS Identity and Access Management (IAM) in the Example ARNs section of the AWS General Reference.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 256.

Required: Yes

**KeyId (p. 10)**

The unique identifier for the customer master key (CMK) that the grant applies to.

Specify the key ID or the Amazon Resource Name (ARN) of the CMK. To specify a CMK in a different AWS account, you must use the key ARN.
For example:

- Key ID: 1234abcd-12ab-34cd-56ef-1234567890ab
- Key ARN: arn:aws:kms:us-east-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab

To get the key ID and key ARN for a CMK, use ListKeys (p. 93) or DescribeKey (p. 30).

Type: String
Length Constraints: Minimum length of 1. Maximum length of 2048.
Required: Yes

**Operations (p. 10)**

A list of operations that the grant permits.

Type: Array of strings
Valid Values: Decrypt | Encrypt | GenerateDataKey | GenerateDataKeyWithoutPlaintext | ReEncryptFrom | ReEncryptTo | CreateGrant | RetireGrant | DescribeKey
Required: Yes

**Constraints (p. 10)**

A structure that you can use to allow certain operations in the grant only when the desired encryption context is present. For more information about encryption context, see Encryption Context in the AWS Key Management Service Developer Guide.

Type: GrantConstraints (p. 139) object
Required: No

**GrantTokens (p. 10)**

A list of grant tokens.

For more information, see Grant Tokens in the AWS Key Management Service Developer Guide.

Type: Array of strings
Array Members: Minimum number of 0 items. Maximum number of 10 items.
Required: No

**Name (p. 10)**

A friendly name for identifying the grant. Use this value to prevent unintended creation of duplicate grants when retrying this request.

When this value is absent, all CreateGrant requests result in a new grant with a unique GrantId even if all the supplied parameters are identical. This can result in unintended duplicates when you retry the CreateGrant request.

When this value is present, you can retry a CreateGrant request with identical parameters; if the grant already exists, the original GrantId is returned without creating a new grant. Note that the returned grant token is unique with every CreateGrant request, even when a duplicate GrantId is returned. All grant tokens obtained in this way can be used interchangeably.

Type: String
Length Constraints: Minimum length of 1. Maximum length of 256.

Pattern: ^[a-zA-Z0-9:/_\-]+$  
Required: No

RetiringPrincipal (p. 10)

The principal that is given permission to retire the grant by using RetireGrant (p. 115) operation.

To specify the principal, use the Amazon Resource Name (ARN) of an AWS principal. Valid AWS principals include AWS accounts (root), IAM users, federated users, and assumed role users. For examples of the ARN syntax to use for specifying a principal, see AWS Identity and Access Management (IAM) in the Example ARNs section of the AWS General Reference.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 256.

Required: No

Response Syntax

```json
{
  "GrantId": "string",
  "GrantToken": "string"
}
```

Response Elements

If the action is successful, the service sends back an HTTP 200 response.

The following data is returned in JSON format by the service.

GrantId (p. 12)

The unique identifier for the grant.

You can use the GrantId in a subsequent RetireGrant (p. 115) or RevokeGrant (p. 118) operation.

Type: String


GrantToken (p. 12)

The grant token.

For more information, see Grant Tokens in the AWS Key Management Service Developer Guide.

Type: String


Errors

For information about the errors that are common to all actions, see Common Errors (p. 149).
**Examples**

The following examples are formatted for legibility.

**Example Request**

```
POST / HTTP/1.1
Host: kms.us-east-2.amazonaws.com
Content-Length: 176
X-Amz-Target: TrentService.CreateGrant
X-Amz-Date: 20161031T202851Z
Content-Type: application/x-amz-json-1.1
```

**DependencyTimeoutException**

The system timed out while trying to fulfill the request. The request can be retried.

HTTP Status Code: 500

**DisabledException**

The request was rejected because the specified CMK is not enabled.

HTTP Status Code: 400

**InvalidArnException**

The request was rejected because a specified ARN was not valid.

HTTP Status Code: 400

**InvalidGrantTokenException**

The request was rejected because the specified grant token is not valid.

HTTP Status Code: 400

**KMSInternalException**

The request was rejected because an internal exception occurred. The request can be retried.

HTTP Status Code: 400

**KMSInvalidStateException**

The request was rejected because the state of the specified resource is not valid for this request.

For more information about how key state affects the use of a CMK, see [How Key State Affects Use of a Customer Master Key](https://docs.aws.amazon.com/kms/latest/developerguide/how-key-state-affects-use-of-cmk.html) in the *AWS Key Management Service Developer Guide*.

HTTP Status Code: 400

**LimitExceededException**

The request was rejected because a limit was exceeded. For more information, see [Limits](https://docs.aws.amazon.com/kms/latest/developerguide/limits.html) in the *AWS Key Management Service Developer Guide*.

HTTP Status Code: 400

**NotFoundException**

The request was rejected because the specified entity or resource could not be found.

HTTP Status Code: 400
Example Response

HTTP/1.1 200 OK
Server: Server
Date: Mon, 31 Oct 2016 20:28:51 GMT
Content-Type: application/x-amz-json-1.1
Content-Length: 585
Connection: keep-alive
x-amzn-RequestId: a2d8d452-9fa8-11e6-b30c-dbb8ea4d97c5

{
    "GrantId": "0c237476b39f8bc44e45212e08498fbe3151305030726c0590dd83e9f3d6a60",
    "GrantToken": "AQpAM2RhZTk1MGMyNTk2ZmZmMzEyYWWboWVWjN2I1MW4Mzc0MWYiYjc0DE1ODkyNGFlNTIzODZhMzgyZjBlNGY3NklAIAgEBAgB4Pa6VDCWW__MSrqnre1HIN ... kiiG9w0BBwaggc4wgcsCAQAwgcUGCSqGSIb3DQEHATAeBglghkgBZQMEAS4wEQQMmqLyBTAegIn9XlK5AgEQgIGXZQjkBcl1dykDdqZBUQ6L1OfUivQy7JVYO2-ZJP7m6f1g6G4v7HX5phdOtONAP7Y_HQ1fscqkoCqQd_fUnEl14mSmiaqWkbQ5aqAVV3ov-VeqgrvMezZFWLMsiuVBqdgjHEDMIkHMi1hlj4ENZbzeBfo9Wxk8b8SmwP4kc4gIvedzFXo-dwN8fxjjq_ZZ9JFOj2Li1bj5FyogDCN0d0rOifi8RORSEuCEmPv1jFRMFAwcmwFk2N2PpS9amA"
}

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java
- AWS SDK for JavaScript
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V2
CreateKey

Creates a customer master key (CMK) in the caller's AWS account.

You can use a CMK to encrypt small amounts of data (4 KiB or less) directly, but CMKs are more commonly used to encrypt data encryption keys (DEKs), which are used to encrypt raw data. For more information about DEKs and the difference between CMKs and DEKs, see the following:

- The GenerateDataKey (p. 51) operation
- AWS Key Management Service Concepts in the AWS Key Management Service Developer Guide

You cannot use this operation to create a CMK in a different AWS account.

Request Syntax

```json
{
    "BypassPolicyLockoutSafetyCheck": boolean,
    "Description": "string",
    "KeyUsage": "string",
    "Origin": "string",
    "Policy": "string",
    "Tags": [
        {
            "TagKey": "string",
            "TagValue": "string"
        }
    ]
}
```

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters (p. 147).

The request accepts the following data in JSON format.

**Note**

In the following list, the required parameters are described first.

**BypassPolicyLockoutSafetyCheck (p. 15)**

A flag to indicate whether to bypass the key policy lockout safety check.

**Important**

Setting this value to true increases the likelihood that the CMK becomes unmanageable. Do not set this value to true indiscriminately.

For more information, refer to the scenario in the Default Key Policy section in the AWS Key Management Service Developer Guide.

Use this parameter only when you include a policy in the request and you intend to prevent the principal that is making the request from making a subsequent PutKeyPolicy (p. 105) request on the CMK.

The default value is false.

Type: Boolean

Required: No
Description (p. 15)

A description of the CMK.

Use a description that helps you decide whether the CMK is appropriate for a task.

Type: String

Length Constraints: Minimum length of 0. Maximum length of 8192.

Required: No

KeyUsage (p. 15)

The intended use of the CMK.

You can use CMKs only for symmetric encryption and decryption.

Type: String

Valid Values: ENCRYPT_DECRYPT

Required: No

Origin (p. 15)

The source of the CMK's key material.

The default is AWS_KMS, which means AWS KMS creates the key material. When this parameter is set to EXTERNAL, the request creates a CMK without key material so that you can import key material from your existing key management infrastructure. For more information about importing key material into AWS KMS, see Importing Key Material in the AWS Key Management Service Developer Guide.

The CMK's Origin is immutable and is set when the CMK is created.

Type: String

Valid Values: AWS_KMS | EXTERNAL

Required: No

Policy (p. 15)

The key policy to attach to the CMK.

If you specify a policy and do not set BypassPolicyLockoutSafetyCheck to true, the policy must meet the following criteria:

• It must allow the principal that is making the CreateKey request to make a subsequent PutKeyPolicy request on the CMK. This reduces the likelihood that the CMK becomes unmanageable. For more information, refer to the scenario in the Default Key Policy section in the AWS Key Management Service Developer Guide.

• The principals that are specified in the key policy must exist and be visible to AWS KMS. When you create a new AWS principal (for example, an IAM user or role), you might need to enforce a delay before specifying the new principal in a key policy because the new principal might not immediately be visible to AWS KMS. For more information, see Changes that I make are not always immediately visible in the IAM User Guide.

If you do not specify a policy, AWS KMS attaches a default key policy to the CMK. For more information, see Default Key Policy in the AWS Key Management Service Developer Guide.

The policy size limit is 32 kilobytes (32768 bytes).

Type: String

Pattern: \[\u0009\u000A\u000D\u0020-\u00FF]+

Required: No

**Tags (p. 15)**

One or more tags. Each tag consists of a tag key and a tag value. Tag keys and tag values are both required, but tag values can be empty (null) strings.

Use this parameter to tag the CMK when it is created. Alternately, you can omit this parameter and instead tag the CMK after it is created using TagResource (p. 125).

Type: Array of Tag (p. 146) objects

Required: No

### Response Syntax

```json
{
   "KeyMetadata": {
      "Arn": "string",
      "AWSAccountId": "string",
      "CreationDate": number,
      "DeletionDate": number,
      "Description": "string",
      "Enabled": boolean,
      "ExpirationModel": "string",
      "KeyId": "string",
      "KeyManager": "string",
      "KeyState": "string",
      "KeyUsage": "string",
      "Origin": "string",
      "ValidTo": number
   }
}
```

### Response Elements

If the action is successful, the service sends back an HTTP 200 response.

The following data is returned in JSON format by the service.

**KeyMetadata (p. 17)**

Metadata associated with the CMK.

Type: KeyMetadata (p. 143) object

### Errors

For information about the errors that are common to all actions, see Common Errors (p. 149).

**DependencyTimeoutException**

The system timed out while trying to fulfill the request. The request can be retried.
HTTP Status Code: 500
InvalidArnException
The request was rejected because a specified ARN was not valid.

HTTP Status Code: 400
KMSInternalException
The request was rejected because an internal exception occurred. The request can be retried.

HTTP Status Code: 400
LimitExceededException
The request was rejected because a limit was exceeded. For more information, see Limits in the AWS Key Management Service Developer Guide.

HTTP Status Code: 400
MalformedPolicyDocumentException
The request was rejected because the specified policy is not syntactically or semantically correct.

HTTP Status Code: 400
TagException
The request was rejected because one or more tags are not valid.

HTTP Status Code: 400
UnsupportedOperationException
The request was rejected because a specified parameter is not supported or a specified resource is not valid for this operation.

Examples
The following examples are formatted for legibility.

Example Request

```json
POST / HTTP/1.1
Host: kms.us-east-2.amazonaws.com
Content-Type: application/x-amz-json-1.1
Authorization: AWS4-HMAC-SHA256
  Credential=AKIAI44QH8DHBEXAMPLE/20170705/us-east-2/kms/aws4_request,\n  SignedHeaders=content-type;host;x-amz-date;x-amz-target,\n  Signature=8fb59aa17854a97df47aae69f560b66178ed0b51ebe334be516c4f3f9acedc
X-Amz-Target: TrentService.CreateKey
X-Amz-Date: 20170705T210455Z
Content-Length: 62

  {"Tags": ["TagValue": "ExampleUser", "TagKey": "CreatedBy"]}
```
Example Response

HTTP/1.1 200 OK
Server: Server
Date: Wed, 05 Jul 2017 21:04:55 GMT
Content-Type: application/x-amz-json-1.1
Content-Length: 335
Connection: keep-alive
x-amzn-RequestId: 98b2de61-61c5-11e7-bd87-9fc4a74e147b

{
    "KeyMetadata": {
        "AWSAccountId": "111122223333",
        "Arn": "arn:aws:kms:us-east-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab",
        "CreationDate": 1.499288695918E9,
        "Description": "",
        "Enabled": true,
        "KeyId": "1234abcd-12ab-34cd-56ef-1234567890ab",
        "KeyManager": "CUSTOMER",
        "KeyState": "Enabled",
        "KeyUsage": "ENCRYPT_DECRYPT",
        "Origin": "AWS_KMS"
    }
}

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java
- AWS SDK for JavaScript
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V2
Decrypt

Decrypts ciphertext. Ciphertext is plaintext that has been previously encrypted by using any of the following operations:

- GenerateDataKey (p. 51)
- GenerateDataKeyWithoutPlaintext (p. 56)
- Encrypt (p. 46)

Note that if a caller has been granted access permissions to all keys (through, for example, IAM user policies that grant Decrypt permission on all resources), then ciphertext encrypted by using keys in other accounts where the key grants access to the caller can be decrypted. To remedy this, we recommend that you do not grant Decrypt access in an IAM user policy. Instead grant Decrypt access only in key policies. If you must grant Decrypt access in an IAM user policy, you should scope the resource to specific keys or to specific trusted accounts.

Request Syntax

```json
{
    "CiphertextBlob": blob,
    "EncryptionContext": {
        "String": "string"
    },
    "GrantTokens": [ "string" ]
}
```

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters (p. 147).

The request accepts the following data in JSON format.

**Note**

In the following list, the required parameters are described first.

**CiphertextBlob (p. 20)**

Ciphertext to be decrypted. The blob includes metadata.

Type: Base64-encoded binary data object


Required: Yes

**EncryptionContext (p. 20)**

The encryption context. If this was specified in the Encrypt (p. 46) function, it must be specified here or the decryption operation will fail. For more information, see Encryption Context.

Type: String to string map

Required: No

**GrantTokens (p. 20)**

A list of grant tokens.
For more information, see Grant Tokens in the AWS Key Management Service Developer Guide.

Type: Array of strings

Array Members: Minimum number of 0 items. Maximum number of 10 items.


Required: No

Response Syntax

```
{
  "KeyId": "string",
  "Plaintext": blob
}
```

Response Elements

If the action is successful, the service sends back an HTTP 200 response.

The following data is returned in JSON format by the service.

**KeyId (p. 21)**

ARN of the key used to perform the decryption. This value is returned if no errors are encountered during the operation.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 2048.

**Plaintext (p. 21)**

Decrypted plaintext data. When you use the HTTP API or the AWS CLI, the value is Base64-encoded. Otherwise, it is not encoded.

Type: Base64-encoded binary data object


Errors

For information about the errors that are common to all actions, see Common Errors (p. 149).

**DependencyTimeoutException**

The system timed out while trying to fulfill the request. The request can be retried.

HTTP Status Code: 500

**DisabledException**

The request was rejected because the specified CMK is not enabled.

HTTP Status Code: 400
InvalidCiphertextException

The request was rejected because the specified ciphertext, or additional authenticated data incorporated into the ciphertext, such as the encryption context, is corrupted, missing, or otherwise invalid.

HTTP Status Code: 400

InvalidGrantTokenException

The request was rejected because the specified grant token is not valid.

HTTP Status Code: 400

KeyUnavailableException

The request was rejected because the specified CMK was not available. The request can be retried.

HTTP Status Code: 500

KMSInternalException

The request was rejected because an internal exception occurred. The request can be retried.

HTTP Status Code: 400

KMSInvalidStateException

The request was rejected because the state of the specified resource is not valid for this request.

For more information about how key state affects the use of a CMK, see How Key State Affects Use of a Customer Master Key in the AWS Key Management Service Developer Guide.

HTTP Status Code: 400

NotFoundException

The request was rejected because the specified entity or resource could not be found.

HTTP Status Code: 400

Examples

The following examples are formatted for legibility.

Example Request

```
POST / HTTP/1.1
Host: kms.us-west-2.amazonaws.com
Content-Length: 293
X-Amz-Target: TrentService.Decrypt
X-Amz-Date: 20160517T204035Z
Content-Type: application/x-amz-json-1.1
Authorization: AWS4-HMAC-SHA256
   Credential=AKIAI44QH8DHBEXAMPLE/20160517/us-west-2/kms/aws4_request,
   SignedHeaders=content-type;host;x-amz-date;x-amz-target,
   Signature=545b0c3bf6d9223b8ef7e6293ef3ccac37a83d415ee3112d2e5c70727d2a49c46

{"CiphertextBlob": "CiDPoCH188S65r5Cy7pAhIFJMXDL7mewhSl1YuQIVhrhKmAQEBAgB4z6Ah9fPEuua +QsuQ7ISB7Tw5V05siiUpWFKbkC7FqAa4AAAB9MHSgCScs81b3DPEH8BqBuMGCwCAQAwZwYJkoZ1hvcNAQcMBMB4GCWCGSAFLAwQBLjARBaZjYCARCAOt81a8qXL05wB3JH2N1wWwzWRU2RKgp09A/0psE5UWvkK6CnwoeC3Zj9Q0A66ap2kbRglFy11TY+Tc=
```
Example Response

HTTP/1.1 200 OK
Server: Server
Date: Tue, 17 May 2016 20:40:40 GMT
Content-Type: application/x-amz-json-1.1
Content-Length: 146
Connection: keep-alive
x-amzn-RequestId: 9e02f41f-1c6f-11e6-af63-ab8791945da7

{
  "KeyId": "arn:aws:kms:us-west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab",
  "Plaintext": "VGhpcyBpcyBEYXkgMSBmb3IgdGhlIEludGVybmV0Cg=="
}

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java
- AWS SDK for JavaScript
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V2
DeleteAlias

Deletes the specified alias. You cannot perform this operation on an alias in a different AWS account.

Because an alias is not a property of a CMK, you can delete and change the aliases of a CMK without affecting the CMK. Also, aliases do not appear in the response from the DescribeKey (p. 30) operation. To get the aliases of all CMKs, use the ListAliases (p. 80) operation.

Each CMK can have multiple aliases. To change the alias of a CMK, use DeleteAlias (p. 24) to delete the current alias and CreateAlias (p. 7) to create a new alias. To associate an existing alias with a different customer master key (CMK), call UpdateAlias (p. 131).

Request Syntax

```json
{
  "AliasName": "string"
}
```

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters (p. 147).

The request accepts the following data in JSON format.

**Note**

In the following list, the required parameters are described first.

**AliasName (p. 24)**

The alias to be deleted. The name must start with the word "alias" followed by a forward slash (alias/). Aliases that begin with "alias/aws" are reserved.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 256.

Pattern: `^[a-zA-Z0-9:/_\-]+$`

Required: Yes

Response Elements

If the action is successful, the service sends back an HTTP 200 response with an empty HTTP body.

Errors

For information about the errors that are common to all actions, see Common Errors (p. 149).

**DependencyTimeoutException**

The system timed out while trying to fulfill the request. The request can be retried.

HTTP Status Code: 500
KMSInternalException

The request was rejected because an internal exception occurred. The request can be retried.

HTTP Status Code: 400

KMSInvalidStateException

The request was rejected because the state of the specified resource is not valid for this request.

For more information about how key state affects the use of a CMK, see How Key State Affects Use of a Customer Master Key in the AWS Key Management Service Developer Guide.

HTTP Status Code: 400

NotFoundException

The request was rejected because the specified entity or resource could not be found.

HTTP Status Code: 400

Examples

Example Request

The following example is formatted for legibility.

```plaintext
POST / HTTP/1.1
Host: kms.us-east-2.amazonaws.com
Content-Length: 34
X-Amz-Target: TrentService.DeleteAlias
X-Amz-Date: 20161104T183415Z
Content-Type: application/x-amz-json-1.1
Authorization: AWS4-HMAC-SHA256
    Credential=AKIAI44QH8DHBEXAMPLE/20161104/us-east-2/kms/aws4_request,\
    SignedHeaders=content-type;host;x-amz-date;x-amz-target,\
    Signature=a57d9c76f60733ea93fe92ac4fa90ca83058a72913e4b8e52c262ff96704d53

{"AliasName": "alias/ExampleAlias"}
```

Example Response

```plaintext
HTTP/1.1 200 OK
Server: Server
Date: Fri, 04 Nov 2016 18:34:15 GMT
Content-Type: application/x-amz-json-1.1
Content-Length: 0
Connection: keep-alive
x-amzn-RequestId: 4a2313ae-a2bd-11e6-aea3-9bf897a0ae69
```

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
See Also

- AWS SDK for Go
- AWS SDK for Java
- AWS SDK for JavaScript
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V2
DeleteImportedKeyMaterial

Deletes key material that you previously imported. This operation makes the specified customer master key (CMK) unusable. For more information about importing key material into AWS KMS, see Importing Key Material in the AWS Key Management Service Developer Guide. You cannot perform this operation on a CMK in a different AWS account.

When the specified CMK is in the PendingDeletion state, this operation does not change the CMK's state. Otherwise, it changes the CMK's state to PendingImport.

After you delete key material, you can use ImportKeyMaterial (p. 75) to reimport the same key material into the CMK.

Request Syntax

```
{
  "KeyId": "string"
}
```

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters (p. 147).

The request accepts the following data in JSON format.

**Note**

In the following list, the required parameters are described first.

**KeyId (p. 27)**

The identifier of the CMK whose key material to delete. The CMK's Origin must be EXTERNAL. Specify the key ID or the Amazon Resource Name (ARN) of the CMK.

For example:

- Key ID: 1234abcd-12ab-34cd-56ef-1234567890ab
- Key ARN: arn:aws:kms:us-east-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab

To get the key ID and key ARN for a CMK, use ListKeys (p. 93) or DescribeKey (p. 30).

Type: String

Length Constraints: Minimum length of 1. Maximum length of 2048.

Required: Yes

Response Elements

If the action is successful, the service sends back an HTTP 200 response with an empty HTTP body.

Errors

For information about the errors that are common to all actions, see Common Errors (p. 149).
**DependencyTimeoutException**

The system timed out while trying to fulfill the request. The request can be retried.

HTTP Status Code: 500

**InvalidArnException**

The request was rejected because a specified ARN was not valid.

HTTP Status Code: 400

**KMSInternalException**

The request was rejected because an internal exception occurred. The request can be retried.

HTTP Status Code: 400

**KMSInvalidStateException**

The request was rejected because the state of the specified resource is not valid for this request.

For more information about how key state affects the use of a CMK, see How Key State Affects Use of a Customer Master Key in the AWS Key Management Service Developer Guide.

HTTP Status Code: 400

**NotFoundException**

The request was rejected because the specified entity or resource could not be found.

HTTP Status Code: 400

**UnsupportedOperationException**

The request was rejected because a specified parameter is not supported or a specified resource is not valid for this operation.

HTTP Status Code: 400

---

**Examples**

**Example Request**

The following example is formatted for legibility.

```plaintext
POST / HTTP/1.1
Host: kms.us-east-2.amazonaws.com
Content-Length: 48
X-Amz-Target: TrentService.DeleteImportedKeyMaterial
X-Amz-Date: 20161107T213532Z
Content-Type: application/x-amz-json-1.1
Authorization: AWS4-HMAC-SHA256
Credential=AKIAI44QH8DHBEXAMPLE/20161107/us-east-2/kms/aws4_request,\
SignedHeaders=content-type;host;x-amz-date;x-amz-target,\
Signature=2cea34fe55d5858295a377448ae053d0ed5e571da7c59b202905759f272
{"KeyId": "1234abcd-12ab-34cd-56ef-1234567890ab"}
```

**Example Response**

```
HTTP/1.1 200 OK
```

---

API Version 2014-11-01

28
See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java
- AWS SDK for JavaScript
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V2
DescribeKey

Provides detailed information about the specified customer master key (CMK).

To perform this operation on a CMK in a different AWS account, specify the key ARN or alias ARN in the value of the KeyId parameter.

Request Syntax

```
{
  "GrantTokens": [ "string" ],
  "KeyId": "string"
}
```

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters (p. 147).

The request accepts the following data in JSON format.

**Note**

In the following list, the required parameters are described first.

**KeyId (p. 30)**

A unique identifier for the customer master key (CMK).

To specify a CMK, use its key ID, Amazon Resource Name (ARN), alias name, or alias ARN. When using an alias name, prefix it with “alias/”. To specify a CMK in a different AWS account, you must use the key ARN or alias ARN.

For example:
- Key ID: 1234abcd-12ab-34cd-56ef-1234567890ab
- Key ARN: arn:aws:kms:us-east-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab
- Alias name: alias/ExampleAlias

To get the key ID and key ARN for a CMK, use ListKeys (p. 93) or DescribeKey (p. 30). To get the alias name and alias ARN, use ListAliases (p. 80).

Type: String

Length Constraints: Minimum length of 1. Maximum length of 2048.

Required: Yes

**GrantTokens (p. 30)**

A list of grant tokens.

For more information, see Grant Tokens in the AWS Key Management Service Developer Guide.

Type: Array of strings
Array Members: Minimum number of 0 items. Maximum number of 10 items.


Required: No

Response Syntax

```
{
    "KeyMetadata": {
        "Arn": "string",
        "AWSAccountId": "string",
        "CreationDate": number,
        "DeletionDate": number,
        "Description": "string",
        "Enabled": boolean,
        "ExpirationModel": "string",
        "KeyId": "string",
        "KeyManager": "string",
        "KeyState": "string",
        "KeyUsage": "string",
        "Origin": "string",
        "ValidTo": number
    }
}
```

Response Elements

If the action is successful, the service sends back an HTTP 200 response.

The following data is returned in JSON format by the service.

**KeyMetadata (p. 31)**

Metadata associated with the key.

Type: KeyMetadata (p. 143) object

Errors

For information about the errors that are common to all actions, see Common Errors (p. 149).

**DependencyTimeoutException**

The system timed out while trying to fulfill the request. The request can be retried.

HTTP Status Code: 500

**InvalidArnException**

The request was rejected because a specified ARN was not valid.

HTTP Status Code: 400

**KMSInternalException**

The request was rejected because an internal exception occurred. The request can be retried.

HTTP Status Code: 400
NotFoundException

The request was rejected because the specified entity or resource could not be found.

HTTP Status Code: 400

Examples

The following examples are formatted for legibility.

Example Request

```
POST / HTTP/1.1
Host: kms.us-east-2.amazonaws.com
Content-Length: 49
X-Amz-Target: TrentService.DescribeKey
X-Amz-Date: 20170705T211529Z
Authorization: AWS4-HMAC-SHA256
  Credential=AKIAI44QH8DHBEXAMPLE/20170705/us-east-2/kms/aws4_request,
  SignedHeaders=content-type;host;x-amz-date;x-amz-target,
  Signature=6bcb6a5ef9ee7585d83955e8a5c3f6d47cf581596208fc0e436fa1de26ef3f6a
Content-Type: application/x-amz-json-1.1

{"KeyId": "1234abcd-12ab-34cd-56ef-1234567890ab"}
```

Example Response

```
HTTP/1.1 200 OK
Server: Server
Date: Wed, 05 Jul 2017 21:15:30 GMT
Content-Type: application/x-amz-json-1.1
Content-Length: 335
Connection: keep-alive
x-amzn-RequestId: 13230ddb-61c7-11e7-af6f-c5b105d7a982

{
  "KeyMetadata": {
    "AWSAccountId": "111122223333",
    "Arn": "arn:aws:kms:us-east-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab",
    "CreationDate": 1.499288695918E9,
    "Description": "",
    "Enabled": true,
    "KeyId": "1234abcd-12ab-34cd-56ef-1234567890ab",
    "KeyManager": "CUSTOMER",
    "KeyState": "Enabled",
    "KeyUsage": "ENCRYPT_DECRYPT",
    "Origin": "AWS_KMS"
  }
}
```

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
• AWS SDK for Go
• AWS SDK for Java
• AWS SDK for JavaScript
• AWS SDK for PHP V3
• AWS SDK for Python
• AWS SDK for Ruby V2
DisableKey

Sets the state of a customer master key (CMK) to disabled, thereby preventing its use for cryptographic operations. You cannot perform this operation on a CMK in a different AWS account.

For more information about how key state affects the use of a CMK, see How Key State Affects the Use of a Customer Master Key in the AWS Key Management Service Developer Guide.

Request Syntax

```json
{
  "KeyId": "string"
}
```

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters (p. 147).

The request accepts the following data in JSON format.

**Note**
In the following list, the required parameters are described first.

**KeyId (p. 34)**

A unique identifier for the customer master key (CMK).

Specify the key ID or the Amazon Resource Name (ARN) of the CMK.

For example:

- Key ID: 1234abcd-12ab-34cd-56ef-1234567890ab
- Key ARN: arn:aws:kms:us-east-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab

To get the key ID and key ARN for a CMK, use ListKeys (p. 93) or DescribeKey (p. 30).

Type: String

Length Constraints: Minimum length of 1. Maximum length of 2048.

Required: Yes

Response Elements

If the action is successful, the service sends back an HTTP 200 response with an empty HTTP body.

Errors

For information about the errors that are common to all actions, see Common Errors (p. 149).

**DependencyTimeoutException**

The system timed out while trying to fulfill the request. The request can be retried.

Http Status Code: 500
InvalidArnException
The request was rejected because a specified ARN was not valid.
HTTP Status Code: 400

KMSInternalException
The request was rejected because an internal exception occurred. The request can be retried.
HTTP Status Code: 400

KMSInvalidStateException
The request was rejected because the state of the specified resource is not valid for this request.
For more information about how key state affects the use of a CMK, see How Key State Affects Use of a Customer Master Key in the AWS Key Management Service Developer Guide.
HTTP Status Code: 400

NotFoundException
The request was rejected because the specified entity or resource could not be found.
HTTP Status Code: 400

Examples

Example Request
The following example is formatted for legibility.

```
POST / HTTP/1.1
Host: kms.us-east-2.amazonaws.com
Content-Length: 48
X-Amz-Target: TrentService.DisableKey
X-Amz-Date: 20161107T221459Z
Content-Type: application/x-amz-json-1.1
Authorization: AWS4-HMAC-SHA256
    Credential=AKIAI44QH8DH8EXAMPLE/20161107/us-east-2/kms/aws4_request,\n    SignedHeaders=content-type;host;x-amz-date;x-amz-target,\n    Signature=de4ddbea732953d60c07d835a5d6e9037c484ee3bec9313cbec1d9420b41a7a

{"KeyId": "1234abcd-12ab-34cd-56ef-1234567890ab"}
```

Example Response

```
HTTP/1.1 200 OK
Server: Server
Date: Mon, 07 Nov 2016 22:14:59 GMT
Content-Type: application/x-amz-json-1.1
Content-Length: 0
Connection: keep-alive
x-amzn-RequestId: 9f5f3560-a537-11e6-8185-8df6f2682323
```

See Also
For more information about using this API in one of the language-specific AWS SDKs, see the following:
- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java
- AWS SDK for JavaScript
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V2
DisableKeyRotation

Disables automatic rotation of the key material for the specified customer master key (CMK). You cannot perform this operation on a CMK in a different AWS account.

Request Syntax

```
{
   "KeyId": "string"
}
```

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters (p. 147).

The request accepts the following data in JSON format.

**Note**

In the following list, the required parameters are described first.

**KeyId (p. 37)**

A unique identifier for the customer master key (CMK).

Specify the key ID or the Amazon Resource Name (ARN) of the CMK.

For example:

- Key ID: 1234abcd-12ab-34cd-56ef-1234567890ab
- Key ARN: arn:aws:kms:us-east-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab

To get the key ID and key ARN for a CMK, use ListKeys (p. 93) or DescribeKey (p. 30).

Type: String

Length Constraints: Minimum length of 1. Maximum length of 2048.

Required: Yes

Response Elements

If the action is successful, the service sends back an HTTP 200 response with an empty HTTP body.

Errors

For information about the errors that are common to all actions, see Common Errors (p. 149).

**DependencyTimeoutException**

The system timed out while trying to fulfill the request. The request can be retried.

HTTP Status Code: 500
Examples

Example Request

The following example is formatted for legibility.

```
POST / HTTP/1.1
Host: kms.us-east-2.amazonaws.com
Content-Length: 48
X-Amz-Target: TrentService.DisableKeyRotation
X-Amz-Date: 20161107T222236Z
Content-Type: application/x-amz-json-1.1
Authorization: AWS4-HMAC-SHA256
    Credential=AKIAI44QH8DHBEXAMPLE/20161107/us-east-2/kms/aws4_request,
    SignedHeaders=content-type;host;x-amz-date;x-amz-target,
    Signature=2304622be05af2afa8c75bf784fb87b280c194746418b05d7af947c8c2bd8f04
{"KeyId": "1234abcd-12ab-34cd-56ef-1234567890ab"}
```

Example Response

```
HTTP/1.1 200 OK
```
See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java
- AWS SDK for JavaScript
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V2
EnableKey

Sets the state of a customer master key (CMK) to enabled, thereby permitting its use for cryptographic operations. You cannot perform this operation on a CMK in a different AWS account.

Request Syntax

```json
{
    "KeyId": "string"
}
```

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters (p. 147).

The request accepts the following data in JSON format.

**Note**
In the following list, the required parameters are described first.

**KeyId (p. 40)**
A unique identifier for the customer master key (CMK).

Specify the key ID or the Amazon Resource Name (ARN) of the CMK.

For example:
- Key ID: 1234abcd-12ab-34cd-56ef-1234567890ab
- Key ARN: arn:aws:kms:us-east-2:1234567890abcd-12ab-34cd-56ef-1234567890ab

To get the key ID and key ARN for a CMK, use ListKeys (p. 93) or DescribeKey (p. 30).

Type: String

Length Constraints: Minimum length of 1. Maximum length of 2048.

Required: Yes

Response Elements

If the action is successful, the service sends back an HTTP 200 response with an empty HTTP body.

Errors

For information about the errors that are common to all actions, see Common Errors (p. 149).

**DependencyTimeoutException**

The system timed out while trying to fulfill the request. The request can be retried.

HTTP Status Code: 500
InvalidArnException
The request was rejected because a specified ARN was not valid.
HTTP Status Code: 400

KMSInternalException
The request was rejected because an internal exception occurred. The request can be retried.
HTTP Status Code: 400

KMSInvalidStateException
The request was rejected because the state of the specified resource is not valid for this request.
For more information about how key state affects the use of a CMK, see How Key State Affects Use of a Customer Master Key in the AWS Key Management Service Developer Guide.
HTTP Status Code: 400

LimitExceededException
The request was rejected because a limit was exceeded. For more information, see Limits in the AWS Key Management Service Developer Guide.
HTTP Status Code: 400

NotFoundException
The request was rejected because the specified entity or resource could not be found.
HTTP Status Code: 400

Examples

Example Request
The following example is formatted for legibility.

```plaintext
POST / HTTP/1.1
Host: kms.us-east-2.amazonaws.com
Content-Length: 48
X-Amz-Target: TrentService.EnableKey
X-Amz-Date: 20161107T221800Z
Content-Type: application/x-amz-json-1.1
Authorization: AWS4-HMAC-SHA256
  Credential=AKIAI44QH8DHBEXAMPLE/20161107/us-east-2/kms/aws4_request,\n  SignedHeaders=content-type;host;x-amz-date;x-amz-target,\n  Signature=74d02e36580c1759255dfef66f1e51f3542e469de8c7c8fa5fb21c042e518295

{"KeyId": "1234abcd-12ab-34cd-56ef-1234567890ab"}
```

Example Response

```
HTTP/1.1 200 OK
Server: Server
Date: Mon, 07 Nov 2016 22:18:00 GMT
Content-Type: application/x-amz-json-1.1
Content-Length: 0
Connection: keep-alive
```

API Version 2014-11-01

41
See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java
- AWS SDK for JavaScript
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V2
EnableKeyRotation

Enables automatic rotation of the key material for the specified customer master key (CMK). You cannot perform this operation on a CMK in a different AWS account.

Request Syntax

```json
{
    "KeyId": "string"
}
```

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters (p. 147).

The request accepts the following data in JSON format.

**Note**

In the following list, the required parameters are described first.

**KeyId (p. 43)**

A unique identifier for the customer master key (CMK).

Specify the key ID or the Amazon Resource Name (ARN) of the CMK.

For example:

- Key ID: 1234abcd-12ab-34cd-56ef-1234567890ab
- Key ARN: arn:aws:kms:us-east-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab

To get the key ID and key ARN for a CMK, use ListKeys (p. 93) or DescribeKey (p. 30).

Type: String

Length Constraints: Minimum length of 1. Maximum length of 2048.

Required: Yes

Response Elements

If the action is successful, the service sends back an HTTP 200 response with an empty HTTP body.

Errors

For information about the errors that are common to all actions, see Common Errors (p. 149).

**DependencyTimeoutException**

The system timed out while trying to fulfill the request. The request can be retried.

HTTP Status Code: 500
**DisabledException**

The request was rejected because the specified CMK is not enabled.

HTTP Status Code: 400

**InvalidArnException**

The request was rejected because a specified ARN was not valid.

HTTP Status Code: 400

**KMSInternalException**

The request was rejected because an internal exception occurred. The request can be retried.

HTTP Status Code: 400

**KMSInvalidStateException**

The request was rejected because the state of the specified resource is not valid for this request.

For more information about how key state affects the use of a CMK, see [How Key State Affects Use of a Customer Master Key](https://docs.aws.amazon.com/kms/latest/developerguide/how-key-state-affects-use-cmk.html) in the *AWS Key Management Service Developer Guide*.

HTTP Status Code: 400

**NotFoundException**

The request was rejected because the specified entity or resource could not be found.

HTTP Status Code: 400

**UnsupportedOperationException**

The request was rejected because a specified parameter is not supported or a specified resource is not valid for this operation.

HTTP Status Code: 400

## Examples

### Example Request

The following example is formatted for legibility.

```plaintext
POST / HTTP/1.1
Host: kms.us-east-2.amazonaws.com
Content-Length: 48
X-Amz-Target: TrentService.EnableKeyRotation
X-Amz-Date: 20161107T221835Z
Content-Type: application/x-amz-json-1.1
Authorization: AWS4-HMAC-SHA256
  Credential=AKIAI44QH8DHBEXAMPLE/20161107/us-east-2/kms/aws4_request,\n  SignedHeaders=content-type;host;x-amz-date;x-amz-target,\n  Signature=4783e177036ca78627fe0cda9d9dfad4ad7c8312d0e73d71d814b0c4c0c9b8160b
"KeyId": "1234abcd-12ab-34cd-56ef-1234567890ab"
```

### Example Response

HTTP/1.1 200 OK
See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java
- AWS SDK for JavaScript
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V2
Encrypt

Encrypts plaintext into ciphertext by using a customer master key (CMK). The `Encrypt` operation has two primary use cases:

- You can encrypt up to 4 kilobytes (4096 bytes) of arbitrary data such as an RSA key, a database password, or other sensitive information.
- To move encrypted data from one AWS region to another, you can use this operation to encrypt in the new region the plaintext data key that was used to encrypt the data in the original region. This provides you with an encrypted copy of the data key that can be decrypted in the new region and used there to decrypt the encrypted data.

To perform this operation on a CMK in a different AWS account, specify the key ARN or alias ARN in the value of the `KeyId` parameter.

Unless you are moving encrypted data from one region to another, you don't use this operation to encrypt a generated data key within a region. To get data keys that are already encrypted, call the `GenerateDataKey (p. 51)` or `GenerateDataKeyWithoutPlaintext (p. 56)` operation. Data keys don't need to be encrypted again by calling `Encrypt`.

To encrypt data locally in your application, use the `GenerateDataKey (p. 51)` operation to return a plaintext data encryption key and a copy of the key encrypted under the CMK of your choosing.

Request Syntax

```json
{
  "EncryptionContext": {
    "string": "string"
  },
  "GrantTokens": [ "string" ],
  "KeyId": "string",
  "Plaintext": blob
}
```

Request Parameters

For information about the parameters that are common to all actions, see [Common Parameters (p. 147)](https://docs.aws.amazon.com/kms/latest/developerguide/common-parameters.html).

The request accepts the following data in JSON format.

**Note**

In the following list, the required parameters are described first.

**KeyId (p. 46)**

A unique identifier for the customer master key (CMK).

To specify a CMK, use its key ID, Amazon Resource Name (ARN), alias name, or alias ARN. When using an alias name, prefix it with "alias/". To specify a CMK in a different AWS account, you must use the key ARN or alias ARN.

For example:
- Key ID: 1234abcd-12ab-34cd-56ef-1234567890ab
- Key ARN: arn:aws:kms:us-east-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab
• Alias name: alias/ExampleAlias

To get the key ID and key ARN for a CMK, use ListKeys (p. 93) or DescribeKey (p. 30). To get the alias name and alias ARN, use ListAliases (p. 80).

Type: String
Length Constraints: Minimum length of 1. Maximum length of 2048.
Required: Yes

Plaintext (p. 46)
Data to be encrypted.
Type: Base64-encoded binary data object
Required: Yes

EncryptionContext (p. 46)
Name-value pair that specifies the encryption context to be used for authenticated encryption. If used here, the same value must be supplied to the Decrypt API or decryption will fail. For more information, see Encryption Context.

Type: String to string map
Required: No

GrantTokens (p. 46)
A list of grant tokens.
For more information, see Grant Tokens in the AWS Key Management Service Developer Guide.

Type: Array of strings
Array Members: Minimum number of 0 items. Maximum number of 10 items.
Required: No

Response Syntax

```json
{
  "CiphertextBlob": blob,
  "KeyId": "string"
}
```

Response Elements

If the action is successful, the service sends back an HTTP 200 response.

The following data is returned in JSON format by the service.
**CiphertextBlob (p. 47)**

The encrypted plaintext. When you use the HTTP API or the AWS CLI, the value is Base64-encoded. Otherwise, it is not encoded.

Type: Base64-encoded binary data object


**KeyId (p. 47)**

The ID of the key used during encryption.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 2048.

**Errors**

For information about the errors that are common to all actions, see [Common Errors (p. 149)](https://docs.aws.amazon.com/kms/latest/APIReference/API_Error_Codes.html).

**DependencyTimeoutException**

The system timed out while trying to fulfill the request. The request can be retried.

HTTP Status Code: 500

**DisabledException**

The request was rejected because the specified CMK is not enabled.

HTTP Status Code: 400

**InvalidGrantTokenException**

The request was rejected because the specified grant token is not valid.

HTTP Status Code: 400

**InvalidKeyUsageException**

The request was rejected because the specified KeySpec value is not valid.

HTTP Status Code: 400

**KeyUnavailableException**

The request was rejected because the specified CMK was not available. The request can be retried.

HTTP Status Code: 500

**KMSInternalException**

The request was rejected because an internal exception occurred. The request can be retried.

HTTP Status Code: 400

**KMSInvalidStateException**

The request was rejected because the state of the specified resource is not valid for this request.

For more information about how key state affects the use of a CMK, see [How Key State Affects Use of a Customer Master Key](https://docs.aws.amazon.com/kms/latest/developerguide/key-state.html) in the AWS Key Management Service Developer Guide.

HTTP Status Code: 400
NotFoundException

The request was rejected because the specified entity or resource could not be found.

HTTP Status Code: 400

Examples

The following examples are formatted for legibility.

Example Request

POST / HTTP/1.1
Host: kms.us-west-2.amazonaws.com
Content-Length: 107
X-Amz-Target: TrentService.Encrypt
X-Amz-Date: 20160517T203825Z
Content-Type: application/x-amz-json-1.1
Authorization: AWS4-HMAC-SHA256
    Credential=AKIAI44QH8DHEXAMPLE/20160517/us-west-2/kms/aws4_request,
    SignedHeaders=content-type;host;x-amz-date;x-amz-target,
    Signature=67ccaa73731af7fe83973ce8139104d55f3bdcebee323d2fe65996d9015ace2
{
    "Plaintext": "VGhpcyBpcyBEYXkgMSBmb3IgdGhlIEludGVybmV0Cg==",
    "KeyId": "1234abcd-12ab-34cd-56ef-1234567890ab"
}

Example Response

HTTP/1.1 200 OK
Server: Server
Date: Tue, 17 May 2016 20:38:30 GMT
Content-Type: application/x-amz-json-1.1
Content-Length: 379
Connection: keep-alive
x-amzn-RequestId: 50a0c603-1c6f-11e6-bb9e-3fadd80ce75
{
    "CiphertextBlob": "CiDPoCH188S65r5Cy7pAhIFJMXDLU7mewhSlYUpuQIVBrhKmAQEBAgB4z6Ah9fPEuua
+Qsu6QISB0TfW5VO5nsIUpwFkbkCFQa4AAAB9MHSgCSCqS1b3DQE1HQBqUcGwCAQAwzYWJKoZIhvcNAQcMBM4CWCXGSAF3AwQB1jAARB
ZjYCAkA0t8la8qXLO5wB3JH2NIwWwWzWRU2Rkgp09A/OpsE5UWwK6CnwoeC3Zj9Q0A66apZkBkgFlFy11TY+Tc=",
    "KeyId": "arn:aws:kms:us-east-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab"
}

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java
- AWS SDK for JavaScript

API Version 2014-11-01

49
See Also

- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V2
GenerateDataKey

Returns a data encryption key that you can use in your application to encrypt data locally.

You must specify the customer master key (CMK) under which to generate the data key. You must also specify the length of the data key using either the KeySpec or NumberOfBytes field. You must specify one field or the other, but not both. For common key lengths (128-bit and 256-bit symmetric keys), we recommend that you use KeySpec. To perform this operation on a CMK in a different AWS account, specify the key ARN or alias ARN in the value of the KeyId parameter.

This operation returns a plaintext copy of the data key in the Plaintext field of the response, and an encrypted copy of the data key in the CiphertextBlob field. The data key is encrypted under the CMK specified in the KeyId field of the request.

We recommend that you use the following pattern to encrypt data locally in your application:

1. Use this operation (GenerateDataKey) to get a data encryption key.
2. Use the plaintext data encryption key (returned in the Plaintext field of the response) to encrypt data locally, then erase the plaintext data key from memory.
3. Store the encrypted data key (returned in the CiphertextBlob field of the response) alongside the locally encrypted data.

To decrypt data locally:

1. Use the Decrypt (p. 20) operation to decrypt the encrypted data key into a plaintext copy of the data key.
2. Use the plaintext data key to decrypt data locally, then erase the plaintext data key from memory.

To return only an encrypted copy of the data key, use GenerateDataKeyWithoutPlaintext (p. 56). To return a random byte string that is cryptographically secure, use GenerateRandom (p. 61).

If you use the optional EncryptionContext field, you must store at least enough information to be able to reconstruct the full encryption context when you later send the ciphertext to the Decrypt (p. 20) operation. It is a good practice to choose an encryption context that you can reconstruct on the fly to better secure the ciphertext. For more information, see Encryption Context in the AWS Key Management Service Developer Guide.

Request Syntax

```
{
  "EncryptionContext": {
    "string": "string"
  },
  "GrantTokens": [ "string" ],
  "KeyId": "string",
  "KeySpec": "string",
  "NumberOfBytes": number
}
```

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters (p. 147).

The request accepts the following data in JSON format.
Note
In the following list, the required parameters are described first.

KeyId (p. 51)
The identifier of the CMK under which to generate and encrypt the data encryption key.

To specify a CMK, use its key ID, Amazon Resource Name (ARN), alias name, or alias ARN. When using an alias name, prefix it with "alias/". To specify a CMK in a different AWS account, you must use the key ARN or alias ARN.

For example:
- Key ID: 1234abcd-12ab-34cd-56ef-1234567890ab
- Key ARN: arn:aws:kms:us-east-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab
- Alias name: alias/ExampleAlias

To get the key ID and key ARN for a CMK, use ListKeys (p. 93) or DescribeKey (p. 30). To get the alias name and alias ARN, use ListAliases (p. 80).

Type: String
Length Constraints: Minimum length of 1. Maximum length of 2048.
Required: Yes

EncryptionContext (p. 51)
A set of key-value pairs that represents additional authenticated data.

For more information, see Encryption Context in the AWS Key Management Service Developer Guide.

Type: String to string map
Required: No

GrantTokens (p. 51)
A list of grant tokens.

For more information, see Grant Tokens in the AWS Key Management Service Developer Guide.

Type: Array of strings
Array Members: Minimum number of 0 items. Maximum number of 10 items.
Required: No

KeySpec (p. 51)
The length of the data encryption key. Use AES_128 to generate a 128-bit symmetric key, or AES_256 to generate a 256-bit symmetric key.

Type: String
Valid Values: AES_256 | AES_128
Required: No
NumberOfBytes (p. 51)

The length of the data encryption key in bytes. For example, use the value 64 to generate a 512-bit data key (64 bytes is 512 bits). For common key lengths (128-bit and 256-bit symmetric keys), we recommend that you use the KeySpec field instead of this one.

Type: Integer

Valid Range: Minimum value of 1. Maximum value of 1024.

Required: No

Response Syntax

```json
{
  "CiphertextBlob": blob,
  "KeyId": "string",
  "Plaintext": blob
}
```

Response Elements

If the action is successful, the service sends back an HTTP 200 response.

The following data is returned in JSON format by the service.

CiphertextBlob (p. 53)

The encrypted data encryption key. When you use the HTTP API or the AWS CLI, the value is Base64-encoded. Otherwise, it is not encoded.

Type: Base64-encoded binary data object


KeyId (p. 53)

The identifier of the CMK under which the data encryption key was generated and encrypted.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 2048.

Plaintext (p. 53)

The data encryption key. When you use the HTTP API or the AWS CLI, the value is Base64-encoded. Otherwise, it is not encoded. Use this data key for local encryption and decryption, then remove it from memory as soon as possible.

Type: Base64-encoded binary data object


Errors

For information about the errors that are common to all actions, see Common Errors (p. 149).
DependencyTimeoutException

The system timed out while trying to fulfill the request. The request can be retried.

HTTP Status Code: 500

DisabledException

The request was rejected because the specified CMK is not enabled.

HTTP Status Code: 400

InvalidGrantTokenException

The request was rejected because the specified grant token is not valid.

HTTP Status Code: 400

InvalidKeyUsageException

The request was rejected because the specified KeySpec value is not valid.

HTTP Status Code: 400

KeyUnavailableException

The request was rejected because the specified CMK was not available. The request can be retried.

HTTP Status Code: 500

KMSInternalException

The request was rejected because an internal exception occurred. The request can be retried.

HTTP Status Code: 400

KMSInvalidStateException

The request was rejected because the state of the specified resource is not valid for this request.

For more information about how key state affects the use of a CMK, see How Key State Affects Use of a Customer Master Key in the AWS Key Management Service Developer Guide.

HTTP Status Code: 400

NotFoundException

The request was rejected because the specified entity or resource could not be found.

HTTP Status Code: 400

Examples

The following examples are formatted for legibility.

Example Request

<table>
<thead>
<tr>
<th>POST / HTTP/1.1</th>
</tr>
</thead>
<tbody>
<tr>
<td>Host: kms.us-east-2.amazonaws.com</td>
</tr>
<tr>
<td>Content-Length: 50</td>
</tr>
<tr>
<td>X-Amz-Target: TrentService.GenerateDataKey</td>
</tr>
<tr>
<td>X-Amz-Date: 20161112T000940Z</td>
</tr>
<tr>
<td>Content-Type: application/x-amz-json-1.1</td>
</tr>
<tr>
<td>Authorization: AWS4-HMAC-SHA256</td>
</tr>
</tbody>
</table>
Credential=AKIAI44QH8DHBEXAMPLE/20161112/us-east-2/kms/aws4_request,\
SignedHeaders=content-type;host;x-amz-date;x-amz-target,\
Signature=815ac4ccbb5c53b8ca015f979704c7953bb0068bf53f4e0b7c6886ed5b0a8fe4

{
  "KeyId": "alias/ExampleAlias",
  "KeySpec": "AES_256"
}

Example Response

HTTP/1.1 200 OK
Server: Server
Date: Sat, 12 Nov 2016 00:09:40 GMT
Content-Type: application/x-amz-json-1.1
Content-Length: 390
Connection: keep-alive
x-amzn-RequestId: 4e6fc242-a86c-11e6-aff0-8333261e2fbd

{
  "CiphertextBlob": "AQEDAHjRYf5WytIc0C857tFSnBaNp2F8DgfcmThbJlGfr8PjlwAAAH4wfAYJKoZIhvcNAQcGoG8wbQIBADBoRgkqhkiG9w0BBwEwHgYJYIZIAWUDBAEuMBEEDEFogLqPWZconQhwHAIBEIA7d9AC7GeJJM34njQvg4Wf1d5sw0NIo1MrBqZa+YdhV8MrkBQPeac0ReRVNDt9qleAt+SHgIRF8POH+7U=",
  "KeyId": "arn:aws:kms:us-east-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab",
  "Plaintext": "VdzKNHGzUAzJeRBVY+uUmofUGGlDzyB3+i9fVkh3piw="
}

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java
- AWS SDK for JavaScript
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V2
GenerateDataKeyWithoutPlaintext

Returns a data encryption key encrypted under a customer master key (CMK). This operation is identical to GenerateDataKey (p. 51) but returns only the encrypted copy of the data key.

To perform this operation on a CMK in a different AWS account, specify the key ARN or alias ARN in the value of the KeyId parameter.

This operation is useful in a system that has multiple components with different degrees of trust. For example, consider a system that stores encrypted data in containers. Each container stores the encrypted data and an encrypted copy of the data key. One component of the system, called the control plane, creates new containers. When it creates a new container, it uses this operation (GenerateDataKeyWithoutPlaintext) to get an encrypted data key and then stores it in the container. Later, a different component of the system, called the data plane, puts encrypted data into the containers. To do this, it passes the encrypted data key to the Decrypt (p. 20) operation, then uses the returned plaintext data key to encrypt data, and finally stores the encrypted data in the container. In this system, the control plane never sees the plaintext data key.

Request Syntax

```
{
    "EncryptionContext": {
        "String": "string"
    },
    "GrantTokens": [ "string" ],
    "KeyId": "string",
    "KeySpec": "string",
    "NumberOfBytes": number
}
```

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters (p. 147).

The request accepts the following data in JSON format.

**Note**

In the following list, the required parameters are described first.

**KeyId (p. 56)**

The identifier of the customer master key (CMK) under which to generate and encrypt the data encryption key.

To specify a CMK, use its key ID, Amazon Resource Name (ARN), alias name, or alias ARN. When using an alias name, prefix it with "alias/". To specify a CMK in a different AWS account, you must use the key ARN or alias ARN.

For example:
- Key ID: 1234abcd-12ab-34cd-56ef-1234567890ab
- Key ARN: arn:aws:kms:us-east-2:11112223333:key/1234abcd-12ab-34cd-56ef-1234567890ab
- Alias name: alias/ExampleAlias
To get the key ID and key ARN for a CMK, use ListKeys (p. 93) or DescribeKey (p. 30). To get the alias name and alias ARN, use ListAliases (p. 80).

Type: String

Length Constraints: Minimum length of 1. Maximum length of 2048.

Required: Yes

EncryptionContext (p. 56)

A set of key-value pairs that represents additional authenticated data.

For more information, see Encryption Context in the AWS Key Management Service Developer Guide.

Type: String to string map

Required: No

GrantTokens (p. 56)

A list of grant tokens.

For more information, see Grant Tokens in the AWS Key Management Service Developer Guide.

Type: Array of strings

Array Members: Minimum number of 0 items. Maximum number of 10 items.


Required: No

KeySpec (p. 56)

The length of the data encryption key. Use AES_128 to generate a 128-bit symmetric key, or AES_256 to generate a 256-bit symmetric key.

Type: String

Valid Values: AES_256 | AES_128

Required: No

NumberOfBytes (p. 56)

The length of the data encryption key in bytes. For example, use the value 64 to generate a 512-bit data key (64 bytes is 512 bits). For common key lengths (128-bit and 256-bit symmetric keys), we recommend that you use the KeySpec field instead of this one.

Type: Integer

Valid Range: Minimum value of 1. Maximum value of 1024.

Required: No

Response Syntax

```json
{
  "CiphertextBlob": blob,
  "KeyId": "string"
}
```
Response Elements

If the action is successful, the service sends back an HTTP 200 response.

The following data is returned in JSON format by the service.

CiphertextBlob (p. 57)

The encrypted data encryption key. When you use the HTTP API or the AWS CLI, the value is Base64-encoded. Otherwise, it is not encoded.

Type: Base64-encoded binary data object


KeyId (p. 57)

The identifier of the CMK under which the data encryption key was generated and encrypted.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 2048.

Errors

For information about the errors that are common to all actions, see Common Errors (p. 149).

DependencyTimeoutException

The system timed out while trying to fulfill the request. The request can be retried.

HTTP Status Code: 500

DisabledException

The request was rejected because the specified CMK is not enabled.

HTTP Status Code: 400

InvalidGrantTokenException

The request was rejected because the specified grant token is not valid.

HTTP Status Code: 400

InvalidKeySpec

The request was rejected because the specified KeySpec value is not valid.

HTTP Status Code: 400

KeyUnavailableException

The request was rejected because the specified CMK was not available. The request can be retried.

HTTP Status Code: 500

KMSInternalException

The request was rejected because an internal exception occurred. The request can be retried.

HTTP Status Code: 400
**KMSInvalidStateException**

The request was rejected because the state of the specified resource is not valid for this request.

For more information about how key state affects the use of a CMK, see How Key State Affects Use of a Customer Master Key in the AWS Key Management Service Developer Guide.

HTTP Status Code: 400

**NotFoundException**

The request was rejected because the specified entity or resource could not be found.

HTTP Status Code: 400

---

**Examples**

The following examples are formatted for legibility.

**Example Request**

```plaintext
POST / HTTP/1.1
Host: kms.us-east-2.amazonaws.com
Content-Length: 50
X-Amz-Target: TrentService.GenerateDataKeyWithoutPlaintext
X-Amz-Date: 20161112T001941Z
Content-Type: application/x-amz-json-1.1
Authorization: AWS4-HMAC-SHA256
Credential=AKIAI44QH8DHBEXAMPLE/20161112/us-east-2/kms/aws4_request,
SignedHeaders=content-type;host;x-amz-date;x-amz-target,
Signature=c86e7fc0218461e537c0d06ac29d865d94dba6fbfad00a844f61200e651df483
{
"KeyId": "alias/ExampleAlias",
"KeySpec": "AES_256"
}
```

**Example Response**

```plaintext
HTTP/1.1 200 OK
Server: Server
Date: Sat, 12 Nov 2016 00:19:41 GMT
Content-Type: application/x-amz-json-1.1
Content-Length: 331
Connection: keep-alive
x-amzn-RequestId: b4ca7ee7-a86d-11e6-8a4e-2f341b963ed6
{
  "CiphertextBlob": "AQEDAHjRYf5WytIc0C857tFSnBaPn2F8Dgfmtbhbj1OFR8F3WlwAAH4wFAJJKoZIhvcNAQcGoG8wqIgADBoBkgkhkG9w0BBwEwF
ntdQ2ZL6wqZElA7BEJ/LB7T1meU8z4e1vEKBGZgXFwMVkZXhKrj3CDR4H29r1i4euOQxp8E5b
+7C9N9f1r75ac3",
  "KeyId": "arn:aws:kms:us-east-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab"
}
```

**See Also**

For more information about using this API in one of the language-specific AWS SDKs, see the following:
See Also

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java
- AWS SDK for JavaScript
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V2
GenerateRandom

Returns a random byte string that is cryptographically secure.

For more information about entropy and random number generation, see the AWS Key Management Service Cryptographic Details whitepaper.

Request Syntax

```json
{
   "NumberOfBytes": number
}
```

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters (p. 147).

The request accepts the following data in JSON format.

**Note**

In the following list, the required parameters are described first.

**NumberOfBytes (p. 61)**

The length of the byte string.

Type: Integer

Valid Range: Minimum value of 1. Maximum value of 1024.

Required: No

Response Syntax

```json
{
   "Plaintext": blob
}
```

Response Elements

If the action is successful, the service sends back an HTTP 200 response.

The following data is returned in JSON format by the service.

**Plaintext (p. 61)**

The random byte string. When you use the HTTP API or the AWS CLI, the value is Base64-encoded. Otherwise, it is not encoded.

Type: Base64-encoded binary data object

Errors

For information about the errors that are common to all actions, see Common Errors (p. 149).

**DependencyTimeoutException**

The system timed out while trying to fulfill the request. The request can be retried.

HTTP Status Code: 500

**KMSInternalException**

The request was rejected because an internal exception occurred. The request can be retried.

HTTP Status Code: 400

Examples

Example Request

The following example is formatted for legibility.

```
POST / HTTP/1.1
Host: kms.us-east-2.amazonaws.com
Content-Length: 21
X-Amz-Target: TrentService.GenerateRandom
X-Amz-Date: 20161114T215101Z
Content-Type: application/x-amz-json-1.1
Authorization: AWS4-HMAC-SHA256
    Credential=AKIAI44QH8DHBEXAMPLE/20161114/us-east-2/kms/aws4_request,
    SignedHeaders=content-type;host;x-amz-date;x-amz-target,
    Signature=e3a0cfdbfb71fae5c89e422ad8322b6a44aed85bf68e3d11f3f315bbaa82ad22
{"NumberOfBytes": 32}
```

Example Response

```
HTTP/1.1 200 OK
Server: Server
Date: Mon, 14 Nov 2016 21:51:02 GMT
Content-Type: application/x-amz-json-1.1
Content-Length: 60
Connection: keep-alive
x-amzn-RequestId: 6f79b0ad-aab4-11e6-971f-0f7b7e5b6782
{"Plaintext":"+Q2hxK60BuU6K6ZIBucFMCW2NJkhISWDaSSQyWp9zA="}
```

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java
- AWS SDK for JavaScript
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V2
GetKeyPolicy

Gets a key policy attached to the specified customer master key (CMK). You cannot perform this operation on a CMK in a different AWS account.

Request Syntax

```
{
    "KeyId": "string",
    "PolicyName": "string"
}
```

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters (p. 147).

The request accepts the following data in JSON format.

**Note**

In the following list, the required parameters are described first.

**KeyId (p. 64)**

A unique identifier for the customer master key (CMK).

Specify the key ID or the Amazon Resource Name (ARN) of the CMK.

For example:
- Key ID: 1234abcd-12ab-34cd-56ef-1234567890ab
- Key ARN: arn:aws:kms:us-east-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab

To get the key ID and key ARN for a CMK, use ListKeys (p. 93) or DescribeKey (p. 30).

Type: String

Length Constraints: Minimum length of 1. Maximum length of 2048.

Required: Yes

**PolicyName (p. 64)**

Specifies the name of the policy. The only valid name is default. To get the names of key policies, use ListKeyPolicies (p. 89).

Type: String


Pattern: \[\w]+

Required: Yes

Response Syntax

```
{
}
```
Response Elements

If the action is successful, the service sends back an HTTP 200 response.

The following data is returned in JSON format by the service.

Policy (p. 64)

A policy document in JSON format.

Type: String


Pattern: [	
 -ÿ]+

Errors

For information about the errors that are common to all actions, see Common Errors (p. 149).

DependencyTimeoutException

The system timed out while trying to fulfill the request. The request can be retried.

HTTP Status Code: 500

InvalidArnException

The request was rejected because a specified ARN was not valid.

HTTP Status Code: 400

KMSInternalException

The request was rejected because an internal exception occurred. The request can be retried.

HTTP Status Code: 400

KMSInvalidStateException

The request was rejected because the state of the specified resource is not valid for this request.

For more information about how key state affects the use of a CMK, see How Key State Affects Use of a Customer Master Key in the AWS Key Management Service Developer Guide.

HTTP Status Code: 400

NotFoundException

The request was rejected because the specified entity or resource could not be found.

HTTP Status Code: 400

Examples

The following examples are formatted for legibility.
Example Request

POST / HTTP/1.1
Host: kms.us-east-2.amazonaws.com
Content-Length: 74
X-Amz-Target: TrentService.GetKeyPolicy
X-Amz-Date: 20161114T225546Z
Content-Type: application/x-amz-json-1.1
Authorization: AWS4-HMAC-SHA256
Credential=AKIAI44QH8DHBEXAMPLE/20161114/us-east-2/kms/aws4_request,\
SignedHeaders=content-type;host;x-amz-date;x-amz-target,\
Signature=a88e20eebfbea3bf62d1512d0d2987e2d233becc7631a442237d1661df623a40

{
  "PolicyName": "default",
  "KeyId": "1234abcd-12ab-34cd-56ef-1234567890ab"
}

Example Response

HTTP/1.1 200 OK
Server: Server
Date: Mon, 14 Nov 2016 22:55:47 GMT
Content-Type: application/x-amz-json-1.1
Content-Length: 326
Connection: keep-alive
x-amzn-RequestId: 7b105e7b-aabd-11e6-8039-3123b558b719

{"Policy":"{
  "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" : "*"
  } ]
}

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java
- AWS SDK for JavaScript
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V2
GetKeyRotationStatus

Gets a Boolean value that indicates whether automatic rotation of the key material is enabled for the specified customer master key (CMK).

To perform this operation on a CMK in a different AWS account, specify the key ARN in the value of the KeyId parameter.

Request Syntax

```
{
  "KeyId": "string"
}
```

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters (p. 147).

The request accepts the following data in JSON format.

**Note**

In the following list, the required parameters are described first.

**KeyId** (p. 67)

A unique identifier for the customer master key (CMK).

Specify the key ID or the Amazon Resource Name (ARN) of the CMK. To specify a CMK in a different AWS account, you must use the key ARN.

For example:

- Key ID: 1234abcd-12ab-34cd-56ef-1234567890ab
- Key ARN: arn:aws:kms:us-east-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab

To get the key ID and key ARN for a CMK, use ListKeys (p. 93) or DescribeKey (p. 30).

Type: String

Length Constraints: Minimum length of 1. Maximum length of 2048.

Required: Yes

Response Syntax

```
{
  "KeyRotationEnabled": boolean
}
```

Response Elements

If the action is successful, the service sends back an HTTP 200 response.
The following data is returned in JSON format by the service.

**KeyRotationEnabled (p. 67)**

A Boolean value that specifies whether key rotation is enabled.

Type: Boolean

**Errors**

For information about the errors that are common to all actions, see Common Errors (p. 149).

**DependencyTimeoutException**

The system timed out while trying to fulfill the request. The request can be retried.

HTTP Status Code: 500

**InvalidArnException**

The request was rejected because a specified ARN was not valid.

HTTP Status Code: 400

**KMSInternalException**

The request was rejected because an internal exception occurred. The request can be retried.

HTTP Status Code: 400

**KMSInvalidStateException**

The request was rejected because the state of the specified resource is not valid for this request.

For more information about how key state affects the use of a CMK, see How Key State Affects Use of a Customer Master Key in the AWS Key Management Service Developer Guide.

HTTP Status Code: 400

**NotFoundException**

The request was rejected because the specified entity or resource could not be found.

HTTP Status Code: 400

**UnsupportedOperationException**

The request was rejected because a specified parameter is not supported or a specified resource is not valid for this operation.

HTTP Status Code: 400

**Examples**

**Example Request**

The following example is formatted for legibility.

```plaintext
POST / HTTP/1.1
Host: kms.us-east-2.amazonaws.com
Content-Length: 49
```
X-Amz-Target: TrentService.GetKeyRotationStatus
X-Amz-Date: 20161115T005817Z
Content-Type: application/x-amz-json-1.1
Authorization: AWS4-HMAC-SHA256\n   Credential=AKIAI44QH8DHBBEXAM/20161115/us-east-2/kms/aws4_request,\n   SignedHeaders=content-type;host;x-amz-date;x-amz-target,\n   Signature=282cb3a4a5d10684ff6c363300c34569a0707c4d50b88778e78cc51ea52f9be
{"KeyId": "1234abcd-12ab-34cd-56ef-1234567890ab"}

Example Response

HTTP/1.1 200 OK
Server: Server
Date: Tue, 15 Nov 2016 00:58:18 GMT
Content-Type: application/x-amz-json-1.1
Content-Length: 28
Connection: keep-alive
x-amzn-RequestId: 98b59330-aace-11e6-aff0-8333261e2fbd
{"KeyRotationEnabled":false}

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java
- AWS SDK for JavaScript
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V2
GetParametersForImport

Returns the items you need in order to import key material into AWS KMS from your existing key management infrastructure. For more information about importing key material into AWS KMS, see Importing Key Material in the AWS Key Management Service Developer Guide.

You must specify the key ID of the customer master key (CMK) into which you will import key material. This CMK's Origin must be EXTERNAL. You must also specify the wrapping algorithm and type of wrapping key (public key) that you will use to encrypt the key material. You cannot perform this operation on a CMK in a different AWS account.

This operation returns a public key and an import token. Use the public key to encrypt the key material. Store the import token to send with a subsequent ImportKeyMaterial (p. 75) request. The public key and import token from the same response must be used together. These items are valid for 24 hours. When they expire, they cannot be used for a subsequent ImportKeyMaterial (p. 75) request. To get new ones, send another GetParametersForImport request.

Request Syntax

```json
{
  "KeyId": "string",
  "WrappingAlgorithm": "string",
  "WrappingKeySpec": "string"
}
```

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters (p. 147).

The request accepts the following data in JSON format.

**Note**

In the following list, the required parameters are described first.

**KeyId (p. 70)**

The identifier of the CMK into which you will import key material. The CMK's Origin must be EXTERNAL.

Specify the key ID or the Amazon Resource Name (ARN) of the CMK.

For example:

- Key ID: 1234abcd-12ab-34cd-56ef-1234567890ab
- Key ARN: arn:aws:kms:us-east-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab

To get the key ID and key ARN for a CMK, use ListKeys (p. 93) or DescribeKey (p. 30).

Type: String

Length Constraints: Minimum length of 1. Maximum length of 2048.

Required: Yes
WrappingAlgorithm (p. 70)

The algorithm you will use to encrypt the key material before importing it with ImportKeyMaterial (p. 75). For more information, see Encrypt the Key Material in the AWS Key Management Service Developer Guide.

Type: String

Valid Values: RSAES_PKCS1_V1_5 | RSAES_OAEP_SHA_1 | RSAES_OAEP_SHA_256

Required: Yes

WrappingKeySpec (p. 70)

The type of wrapping key (public key) to return in the response. Only 2048-bit RSA public keys are supported.

Type: String

Valid Values: RSA_2048

Required: Yes

Response Syntax

```json
{
    "ImportToken": blob,
    "KeyId": "string",
    "ParametersValidTo": number,
    "PublicKey": blob
}
```

Response Elements

If the action is successful, the service sends back an HTTP 200 response.

The following data is returned in JSON format by the service.

ImportToken (p. 71)

The import token to send in a subsequent ImportKeyMaterial (p. 75) request.

Type: Base64-encoded binary data object


KeyId (p. 71)

The identifier of the CMK to use in a subsequent ImportKeyMaterial (p. 75) request. This is the same CMK specified in the GetParametersForImport request.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 2048.

ParametersValidTo (p. 71)

The time at which the import token and public key are no longer valid. After this time, you cannot use them to make an ImportKeyMaterial (p. 75) request and you must send another GetParametersForImport request to get new ones.
Type: Timestamp

**PublicKey (p. 71)**

The public key to use to encrypt the key material before importing it with ImportKeyMaterial (p. 75).

Type: Base64-encoded binary data object


## Errors

For information about the errors that are common to all actions, see Common Errors (p. 149).

**DependencyTimeoutException**

The system timed out while trying to fulfill the request. The request can be retried.

HTTP Status Code: 500

**InvalidArnException**

The request was rejected because a specified ARN was not valid.

HTTP Status Code: 400

**KMSInternalException**

The request was rejected because an internal exception occurred. The request can be retried.

HTTP Status Code: 400

**KMSInvalidStateException**

The request was rejected because the state of the specified resource is not valid for this request.

For more information about how key state affects the use of a CMK, see How Key State Affects Use of a Customer Master Key in the AWS Key Management Service Developer Guide.

HTTP Status Code: 400

**NotFoundException**

The request was rejected because the specified entity or resource could not be found.

HTTP Status Code: 400

**UnsupportedOperationException**

The request was rejected because a specified parameter is not supported or a specified resource is not valid for this operation.

HTTP Status Code: 400

## Examples

The following examples are formatted for legibility.

### Example Request

```
POST / HTTP/1.1
```
Example Response

HTTP/1.1 200 OK
Server: Server
Date: Wed, 30 Nov 2016 22:52:17 GMT
Content-Type: application/x-amz-json-1.1
Content-Length: 2892
Connection: keep-alive
x-amzn-RequestId: a46d61e0-b74f-11e6-b0c0-3343f53dee45

{
    "ImportToken": "AQECAHgyb1x2X9LNas5DpvmFmS5V//
daUB92EcCokiXmwi097OAAABQwggawBqkgkhiG9w08BBwaggahMIIgNgQJADBDCBpYGCSqGSIb3DQEHTAABgglbghkBEQMAE54wEQQWU4ngNV+MAqEgQr1g/PGOyGZslrjopP6W63j1LYYn
g+07lJ8bftTCTCQYTTj81sESOOGf71t7wBrhctg3zKwwAqVrxaW6vmeW6iZz1PeNu1AJTjX9t72vzyEYYgFvBeraO9V5tK1CQwZ2fJ5ba529ZkQ51f8qk+38E3CA2j5a52a262o5r
"KeyId": "arn:aws:kms:us-east-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab",
"ParametersValidTo": 1.480632737044E9,
"PublicKey":
"MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA3eh8nWZo2M8N+t49sZn6cBAKsBc5sOeS5dJLIrJ0w1O+e4ymoI7y/eQ5fR1dO/aUzy6U3x5qN+a+2wWxqWvlwK0L
+e5+n674A7R7YHkq4tGQmOv8yvpZ37Ko97mVX4wQbXy2vFZa7T9L6z5/AKjvPQX1gMf+2vOuZlCMQsV+9v3muVeDlY/Df1mPN5x32ez4
"}
See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java
- AWS SDK for JavaScript
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V2
**ImportKeyMaterial**

Imports key material into an existing AWS KMS customer master key (CMK) that was created without key material. You cannot perform this operation on a CMK in a different AWS account. For more information about creating CMKs with no key material and then importing key material, see Importing Key Material in the AWS Key Management Service Developer Guide.

Before using this operation, call GetParametersForImport (p. 70). Its response includes a public key and an import token. Use the public key to encrypt the key material. Then, submit the import token from the same GetParametersForImport response.

When calling this operation, you must specify the following values:

- The key ID or key ARN of a CMK with no key material. Its Origin must be EXTERNAL.
  
  To create a CMK with no key material, call CreateKey (p. 15) and set the value of its Origin parameter to EXTERNAL. To get the Origin of a CMK, call DescribeKey (p. 30).

- The encrypted key material. To get the public key to encrypt the key material, call GetParametersForImport (p. 70).

- The import token that GetParametersForImport (p. 70) returned. This token and the public key used to encrypt the key material must have come from the same response.

- Whether the key material expires and if so, when. If you set an expiration date, you can change it only by reimporting the same key material and specifying a new expiration date. If the key material expires, AWS KMS deletes the key material and the CMK becomes unusable. To use the CMK again, you must reimport the same key material.

When this operation is successful, the CMK's key state changes from PendingImport to Enabled, and you can use the CMK. After you successfully import key material into a CMK, you can reimport the same key material into that CMK, but you cannot import different key material.

**Request Syntax**

```json
{
  "EncryptedKeyMaterial": blob,
  "ExpirationModel": "string",
  "ImportToken": blob,
  "KeyId": "string",
  "ValidTo": number
}
```

**Request Parameters**

For information about the parameters that are common to all actions, see Common Parameters (p. 147).

The request accepts the following data in JSON format.

**Note**

In the following list, the required parameters are described first.

**EncryptedKeyMaterial (p. 75)**

The encrypted key material to import. It must be encrypted with the public key that you received in the response to a previous GetParametersForImport (p. 70) request, using the wrapping algorithm that you specified in that request.
Response Elements

If the action is successful, the service sends back an HTTP 200 response with an empty HTTP body.
Errors

For information about the errors that are common to all actions, see Common Errors (p. 149).

**DependencyTimeoutException**

The system timed out while trying to fulfill the request. The request can be retried.

HTTP Status Code: 500

**ExpiredImportTokenException**

The request was rejected because the provided import token is expired. Use GetParametersForImport (p. 70) to get a new import token and public key, use the new public key to encrypt the key material, and then try the request again.

HTTP Status Code: 400

**IncorrectKeyMaterialException**

The request was rejected because the provided key material is invalid or is not the same key material that was previously imported into this customer master key (CMK).

HTTP Status Code: 400

**InvalidArnException**

The request was rejected because a specified ARN was not valid.

HTTP Status Code: 400

**InvalidCiphertextException**

The request was rejected because the specified ciphertext, or additional authenticated data incorporated into the ciphertext, such as the encryption context, is corrupted, missing, or otherwise invalid.

HTTP Status Code: 400

**InvalidImportTokenException**

The request was rejected because the provided import token is invalid or is associated with a different customer master key (CMK).

HTTP Status Code: 400

**KMSInternalException**

The request was rejected because an internal exception occurred. The request can be retried.

HTTP Status Code: 400

**KMSInvalidStateException**

The request was rejected because the state of the specified resource is not valid for this request.

For more information about how key state affects the use of a CMK, see How Key State Affects Use of a Customer Master Key in the AWS Key Management Service Developer Guide.

HTTP Status Code: 400

**NotFoundException**

The request was rejected because the specified entity or resource could not be found.

HTTP Status Code: 400
UnsupportedOperationException

The request was rejected because a specified parameter is not supported or a specified resource is not valid for this operation.

HTTP Status Code: 400

Examples

Example Request

The following example is formatted for legibility.

POST / HTTP/1.1
Host: kms.us-east-2.amazonaws.com
Content-Length: 2835
X-Amz-Target: TrentService.ImportKeyMaterial
X-Amz-Date: 20161201T212609Z
Content-Type: application/x-amz-json-1.1
Authorization: AWS4-HMAC-SHA256

{
    "ExpirationModel": "KEY_MATERIAL_DOES_NOT_EXPIRE",
    "KeyId": "1234abcd-12ab-34cd-56ef-1234567890ab",
    "ImportToken": "AQECAHgybIx2X9LNs5ADpvmFm5Sv//daUB9ZeCKoiJxmiw09YQAABrQwggawBgkqhkiG9w0BBwagggahMIIGnQIBADCCBpGyGCSqGSIb3DQHE
    aTATBQCBKmgwggE4MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQAx
    
    "EncryptedKeyMaterial": "CubeyZ4cm/xMEA0UG5jP1iBzh/0E+uUg407JDcXhIC+iuMm+wPgITaEby+Y3nM/e6gjUls5vy9TdBRFv4+JtksvB5hW4Znb2lUQhTUv+SSAZpaI14kAgTq/jC2GTLkaC6Vf5zJx2xaLrOKGV2Xu4YgONIGslubHNffTC3aL/YBJ/FXTXaVu7rS2phOFCrZATittS03w4DiCVoNwo2v0QE0+dVoUNjXNQC1veWxhPlC7FezfK7AIsBSSXotJfANxRkybg8KcnkSoYdzr3N0L0v7oMorgbTgaTvdrLXu/PzphK6RWJGJig4tk/1xUT8h7vXilkFskgJHFmp6Xbonw8==",
}

Examples
Example Response

HTTP/1.1 200 OK
Server: Server
Date: Thu, 01 Dec 2016 21:26:10 GMT
Content-Type: application/x-amz-json-1.1
Content-Length: 2
Connection: keep-alive
x-amzn-RequestId: c72fb6ff-b80c-11e6-ae07-61b14fe11739

{}

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java
- AWS SDK for JavaScript
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V2
ListAliases

Gets a list of all aliases in the caller’s AWS account and region. You cannot list aliases in other accounts. For more information about aliases, see CreateAlias (p. 7).

The response might include several aliases that do not have a TargetKeyId field because they are not associated with a CMK. These are predefined aliases that are reserved for CMKs managed by AWS services. If an alias is not associated with a CMK, the alias does not count against the alias limit for your account.

Request Syntax

```json
{
    "Limit": number,
    "Marker": "string"
}
```

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters (p. 147).

The request accepts the following data in JSON format.

**Note**
In the following list, the required parameters are described first.

**Limit (p. 80)**

Use this parameter to specify the maximum number of items to return. When this value is present, AWS KMS does not return more than the specified number of items, but it might return fewer.

This value is optional. If you include a value, it must be between 1 and 100, inclusive. If you do not include a value, it defaults to 50.

Type: Integer

Valid Range: Minimum value of 1. Maximum value of 100.

Required: No

**Marker (p. 80)**

Use this parameter in a subsequent request after you receive a response with truncated results. Set it to the value of NextMarker from the truncated response you just received.

Type: String


Pattern: [\u0020-\u00FF]*

Required: No

Response Syntax

```json
{
}
```
"Aliases": [
    {
        "AliasArn": "string",
        "AliasName": "string",
        "TargetKeyId": "string"
    }
],
"NextMarker": "string",
"Truncated": boolean

Response Elements

If the action is successful, the service sends back an HTTP 200 response.

The following data is returned in JSON format by the service.

Aliases (p. 80)
A list of aliases.
Type: Array of AliasListEntry (p. 138) objects

NextMarker (p. 80)
When Truncated is true, this element is present and contains the value to use for the Marker parameter in a subsequent request.
Type: String
Pattern: [\u0020-\u00FF]*

Truncated (p. 80)
A flag that indicates whether there are more items in the list. When this value is true, the list in this response is truncated. To get more items, pass the value of the NextMarker element in this response to the Marker parameter in a subsequent request.
Type: Boolean

Errors

For information about the errors that are common to all actions, see Common Errors (p. 149).

DependencyTimeoutException
The system timed out while trying to fulfill the request. The request can be retried.
HTTP Status Code: 500

InvalidMarkerException
The request was rejected because the marker that specifies where pagination should next begin is not valid.
HTTP Status Code: 400

KMSInternalException
The request was rejected because an internal exception occurred. The request can be retried.
HTTP Status Code: 400

Examples

The following examples are formatted for legibility.

Example Request

POST / HTTP/1.1
Host: kms.us-east-2.amazonaws.com
Content-Length: 2
X-Amz-Target: TrentService.ListAliases
X-Amz-Date: 20161203T011453Z
Content-Type: application/x-amz-json-1.1
Authorization: AWS4-HMAC-SHA256\n   Credential=AKIAI44QH8DHBEEXAMPLE/20161203/us-east-2/kms/aws4_request,\n   SignedHeaders=content-type;host;x-amz-date;x-amz-target,\n   Signature=c2867e5f45167bf713e8f2c9998772ad72a20958db2cc0ef46bfba1632ca4d62
{}

Example Response

HTTP/1.1 200 OK
Server: Server
Date: Sat, 03 Dec 2016 01:14:55 GMT
Content-Type: application/x-amz-json-1.1
Content-Length: 2874
Connection: keep-alive
x-amzn-RequestId: e6196175-b8f5-11e6-b404-15dcd0a7add5
{}

"Aliases": [ }
     "AliasName": "alias/aws/acm",
     "TargetKeyId": "da03f6f7-d279-427a-9cae-de48d07e5b66"
   },
     "AliasName": "alias/aws/ebs",
     "TargetKeyId": "25a217e7-7170-4b8c-8bf6-045ea5f70e5b"
   },
     "AliasName": "alias/aws/rds",
     "TargetKeyId": "7ec3104e-c3f2-4b5c-bf42-bfc4772c6685"
   },
     "AliasName": "alias/aws/redshift",
     "TargetKeyId": "08f7a25a-69e2-4fb5-8f10-393db27326fa"
   },
     "AliasName": "alias/aws/s3",
     "TargetKeyId": "d2b0f1a3-580d-4f79-b836-bc983be8cfa5"
   },
   { "AliasArn": "arn:aws:kms:us-east-2:111122223333:alias/example1",}
"AliasName": "alias/example1",
"TargetKeyId": "4da1e216-62d0-46c5-a7c0-5f3a3d2f8046"
},
{
"AliasName": "alias/example2",
"TargetKeyId": "f32fef59-2cc2-445b-8573-2d73328acbee"
},
{
"AliasName": "alias/example3",
"TargetKeyId": "1374ef38-d34e-4d5f-b2c9-4e0daee38855"
}
],
"Truncated": false

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java
- AWS SDK for JavaScript
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V2
ListGrants

Gets a list of all grants for the specified customer master key (CMK).

To perform this operation on a CMK in a different AWS account, specify the key ARN in the value of the KeyId parameter.

Request Syntax

```
{
    "KeyId": "string",
    "Limit": number,
    "Marker": "string"
}
```

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters (p. 147).

The request accepts the following data in JSON format.

**Note**

In the following list, the required parameters are described first.

**KeyId (p. 84)**

A unique identifier for the customer master key (CMK).

Specify the key ID or the Amazon Resource Name (ARN) of the CMK. To specify a CMK in a different AWS account, you must use the key ARN.

For example:

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

To get the key ID and key ARN for a CMK, use ListKeys (p. 93) or DescribeKey (p. 30).

Type: String

Length Constraints: Minimum length of 1. Maximum length of 2048.

Required: Yes

**Limit (p. 84)**

Use this parameter to specify the maximum number of items to return. When this value is present, AWS KMS does not return more than the specified number of items, but it might return fewer.

This value is optional. If you include a value, it must be between 1 and 100, inclusive. If you do not include a value, it defaults to 50.

Type: Integer

Valid Range: Minimum value of 1. Maximum value of 100.

Required: No
Marker (p. 84)

Use this parameter in a subsequent request after you receive a response with truncated results. Set it to the value of NextMarker from the truncated response you just received.

Type: String
Pattern: [\u0020-\u00FF]*
Required: No

Response Syntax

```
{  
  "Grants": [ 
    {  
      "Constraints": {  
        "EncryptionContextEquals": {  
          "string": "string"
        },  
        "EncryptionContextSubset": {  
          "string": "string"
        }  
      },  
      "CreationDate": number,  
      "GranteePrincipal": "string",  
      "GrantId": "string",  
      "IssuingAccount": "string",  
      "KeyId": "string",  
      "Name": "string",  
      "Operations": [ "string" ],  
      "RetiringPrincipal": "string"
    }  
  ],  
  "NextMarker": "string",  
  "Truncated": boolean
}
```

Response Elements

If the action is successful, the service sends back an HTTP 200 response.

The following data is returned in JSON format by the service.

Grants (p. 85)

A list of grants.

Type: Array of GrantListEntry (p. 140) objects

NextMarker (p. 85)

When Truncated is true, this element is present and contains the value to use for the Marker parameter in a subsequent request.

Type: String
Errors

For information about the errors that are common to all actions, see Common Errors (p. 149).

DependencyTimeoutException

The system timed out while trying to fulfill the request. The request can be retried.

HTTP Status Code: 500

InvalidArnException

The request was rejected because a specified ARN was not valid.

HTTP Status Code: 400

InvalidMarkerException

The request was rejected because the marker that specifies where pagination should next begin is not valid.

HTTP Status Code: 400

KMSInternalException

The request was rejected because an internal exception occurred. The request can be retried.

HTTP Status Code: 400

KMSInvalidStateException

The request was rejected because the state of the specified resource is not valid for this request.

For more information about how key state affects the use of a CMK, see How Key State Affects Use of a Customer Master Key in the AWS Key Management Service Developer Guide.

HTTP Status Code: 400

NotFoundException

The request was rejected because the specified entity or resource could not be found.

HTTP Status Code: 400

Examples

The following examples are formatted for legibility.

Example Request

```
POST / HTTP/1.1
```

API Version 2014-11-01

86
Example Response

HTTP/1.1 200 OK
Server: Server
Date: Tue, 06 Dec 2016 23:11:34 GMT
Content-Type: application/x-amz-json-1.1
Content-Length: 1652
Connection: keep-alive
x-amzn-RequestId: 54ee4e2f-bc09-11e6-8073-89d6c33fcd1f

{
  "Grants": [
    {
      "CreationDate": 1477431461499,
      "GrantId": "a5d67d9e037a8f0409d9f82f9db6ea95e10908113f6d7f0c655be2a172",
      "GranteePrincipal": "acm.us-east-2.amazonaws.com",
      "IssuingAccount": "arn:aws:iam::111122223333:root",
      "KeyId": "arn:aws:kms:us-east-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab",
      "Name": "",
      "Operations": [
        "Encrypt",
        "ReEncryptFrom",
        "ReEncryptTo"
      ],
      "RetiringPrincipal": "acm.us-east-2.amazonaws.com"
    },
    {
      "CreationDate": 1477431461499,
      "GrantId": "a5d67d9e037a8f0409d9f82f9db6ea95e10908113f6d7f0c655be2a172",
      "GranteePrincipal": "acm.us-east-2.amazonaws.com",
      "IssuingAccount": "arn:aws:iam::111122223333:root",
      "KeyId": "arn:aws:kms:us-east-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab",
      "Name": "",
      "Operations": [
        "Encrypt",
        "ReEncryptFrom",
        "ReEncryptTo"
      ],
      "RetiringPrincipal": "acm.us-east-2.amazonaws.com"
    },
    {
      "CreationDate": 1477431461499,
      "GrantId": "a5d67d9e037a8f0409d9f82f9db6ea95e10908113f6d7f0c655be2a172",
      "GranteePrincipal": "acm.us-east-2.amazonaws.com",
      "IssuingAccount": "arn:aws:iam::111122223333:root",
      "KeyId": "arn:aws:kms:us-east-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab",
      "Name": "",
      "Operations": [
        "Encrypt",
        "ReEncryptFrom",
        "ReEncryptTo"
      ],
      "RetiringPrincipal": "acm.us-east-2.amazonaws.com"
    }
  ]
}
"ReEncryptTo"
],
"RetiringPrincipal": "acm.us-east-2.amazonaws.com"
},
{
"CreationDate": 1.477431461E9,
"GrantId": "dd2052c67b4c76ee45caf1dc6a1e2d24e8dc744a51b36ae2f067dc540ce0105c",
"GranteePrincipal": "acm.us-east-2.amazonaws.com",
"IssuingAccount": "arn:aws:iam::111122223333:root",
"KeyId": "arn:aws:kms:us-east-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab",
"Name": "",
"Operations": [
"Encrypt",
"ReEncryptFrom",
"ReEncryptTo"
],
"RetiringPrincipal": "acm.us-east-2.amazonaws.com"
}
],
"Truncated": false

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java
- AWS SDK for JavaScript
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V2
ListKeyPolicies

Gets the names of the key policies that are attached to a customer master key (CMK). This operation is designed to get policy names that you can use in a GetKeyPolicy (p. 64) operation. However, the only valid policy name is default. You cannot perform this operation on a CMK in a different AWS account.

Request Syntax

```json
{
    "KeyId": "string",
    "Limit": number,
    "Marker": "string"
}
```

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters (p. 147).

The request accepts the following data in JSON format.

**Note**

In the following list, the required parameters are described first.

**KeyId (p. 89)**

A unique identifier for the customer master key (CMK).

Specify the key ID or the Amazon Resource Name (ARN) of the CMK.

For example:

- Key ID: 1234abcd-12ab-34cd-56ef-1234567890ab
- Key ARN: arn:aws:kms:us-east-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab

To get the key ID and key ARN for a CMK, use ListKeys (p. 93) or DescribeKey (p. 30).

Type: String

Length Constraints: Minimum length of 1. Maximum length of 2048.

Required: Yes

**Limit (p. 89)**

Use this parameter to specify the maximum number of items to return. When this value is present, AWS KMS does not return more than the specified number of items, but it might return fewer.

This value is optional. If you include a value, it must be between 1 and 1000, inclusive. If you do not include a value, it defaults to 100.

Currently only 1 policy can be attached to a key.

Type: Integer

Valid Range: Minimum value of 1. Maximum value of 1000.

Required: No
Marker (p. 89)

Use this parameter in a subsequent request after you receive a response with truncated results. Set it to the value of NextMarker from the truncated response you just received.

Type: String


Pattern: [ -ÿ]*

Required: No

Response Syntax

```json
{
    "NextMarker": "string",
    "PolicyNames": [ "string" ],
    "Truncated": boolean
}
```

Response Elements

If the action is successful, the service sends back an HTTP 200 response.

The following data is returned in JSON format by the service.

NextMarker (p. 90)

When Truncated is true, this element is present and contains the value to use for the Marker parameter in a subsequent request.

Type: String


Pattern: [ -ÿ]*

PolicyNames (p. 90)

A list of policy names. Currently, there is only one policy and it is named "Default".

Type: Array of strings


Pattern: [\w]+

Truncated (p. 90)

A flag that indicates whether there are more items in the list. When this value is true, the list in this response is truncated. To get more items, pass the value of the NextMarker element in this response to the Marker parameter in a subsequent request.

Type: Boolean

Errors

For information about the errors that are common to all actions, see Common Errors (p. 149).
DependencyTimeoutException

The system timed out while trying to fulfill the request. The request can be retried.

HTTP Status Code: 500

InvalidArnException

The request was rejected because a specified ARN was not valid.

HTTP Status Code: 400

KMSInternalException

The request was rejected because an internal exception occurred. The request can be retried.

HTTP Status Code: 400

KMSInvalidStateException

The request was rejected because the state of the specified resource is not valid for this request.

For more information about how key state affects the use of a CMK, see How Key State Affects Use of a Customer Master Key in the AWS Key Management Service Developer Guide.

HTTP Status Code: 400

NotFoundException

The request was rejected because the specified entity or resource could not be found.

HTTP Status Code: 400

Examples

The following examples are formatted for legibility.

Example Request

```plaintext
POST / HTTP/1.1
Host: kms.us-east-2.amazonaws.com
Content-Length: 49
X-Amz-Target: TrentService.ListKeyPolicies
X-Amz-Date: 20161206T235923Z
Content-Type: application/x-amz-json-1.1
Authorization: AWS4-HMAC-SHA256\
    Credential=AKIAI44QH8DHBEXAMPLE/20161206/us-east-2/kms/aws4_request,\
    SignedHeaders=content-type;host;x-amz-date;x-amz-target,\
    Signature=82fe067c53d0dfff36793b506ef2d82d6af0f1c05016bf4b4d650563ec7033

{"KeyId": "1234abcd-12ab-34cd-56ef-1234567890ab"}
```

Example Response

```plaintext
HTTP/1.1 200 OK
Server: Server
Date: Tue, 06 Dec 2016 23:59:24 GMT
Content-Type: application/x-amz-json-1.1
Content-Length: 45
Connection: keep-alive
x-amzn-RequestId: 036f8e4b-bc10-11e6-b60b-ff5eb2d1d15
```

API Version 2014-11-01
See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java
- AWS SDK for JavaScript
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V2
ListKeys

Gets a list of all customer master keys (CMKs) in the caller's AWS account and region.

Request Syntax

```
{
   "Limit": number,
   "Marker": "string"
}
```

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters (p. 147).

The request accepts the following data in JSON format.

**Note**

In the following list, the required parameters are described first.

**Limit (p. 93)**

Use this parameter to specify the maximum number of items to return. When this value is present, AWS KMS does not return more than the specified number of items, but it might return fewer.

This value is optional. If you include a value, it must be between 1 and 1000, inclusive. If you do not include a value, it defaults to 100.

Type: Integer

Valid Range: Minimum value of 1. Maximum value of 1000.

Required: No

**Marker (p. 93)**

Use this parameter in a subsequent request after you receive a response with truncated results. Set it to the value of `NextMarker` from the truncated response you just received.

Type: String


Pattern: `/\u0020-\u00FF`*

Required: No

Response Syntax

```
{
   "Keys": [
      {
         "KeyArn": "string",
         "KeyId": "string"
      }
   ]
}
```
Response Elements

If the action is successful, the service sends back an HTTP 200 response.

The following data is returned in JSON format by the service.

**Keys (p. 93)**

A list of customer master keys (CMKs).

Type: Array of KeyListEntry (p. 142) objects

**NextMarker (p. 93)**

When `Truncated` is true, this element is present and contains the value to use for the `Marker` parameter in a subsequent request.

Type: String


Pattern: `[ -ÿ]*`

**Truncated (p. 93)**

A flag that indicates whether there are more items in the list. When this value is true, the list in this response is truncated. To get more items, pass the value of the `NextMarker` element in this response to the `Marker` parameter in a subsequent request.

Type: Boolean

Errors

For information about the errors that are common to all actions, see Common Errors (p. 149).

**DependencyTimeoutException**

The system timed out while trying to fulfill the request. The request can be retried.

HTTP Status Code: 500

**InvalidMarkerException**

The request was rejected because the marker that specifies where pagination should next begin is not valid.

HTTP Status Code: 400

**KMSInternalException**

The request was rejected because an internal exception occurred. The request can be retried.

HTTP Status Code: 400
Examples

The following examples are formatted for legibility.

Example Request

POST / HTTP/1.1
Host: kms.us-east-2.amazonaws.com
Content-Length: 2
X-Amz-Target: TrentService.ListKeys
X-Amz-Date: 20161207003550Z
Content-Type: application/x-amz-json-1.1
Authorization: AWS4-HMAC-SHA256
Credential=AKIAI44QH8DBEXAMPLE/20161207/us-east-2/kms/aws4_request,
SignedHeaders=content-type;host;x-amz-date;x-amz-target,
Signature=2196a20c1a139ae8f6fe070881f41954616c775bb5a484814c35f8ee35cfa448

{}

Example Response

HTTP/1.1 200 OK
Server: Server
Date: Wed, 07 Dec 2016 00:35:50 GMT
Content-Type: application/x-amz-json-1.1
Content-Length: 980
Connection: keep-alive
x-amzn-RequestId: 1a5f0a53-bc15-11e6-82b3-e9e4af764a06

{
    "Keys": [
        {
            "KeyArn": "arn:aws:kms:us-east-2:111122223333:key/0d990263-018e-4e65-a703-eff731de951e",
            "KeyId": "0d990263-018e-4e65-a703-eff731de951e"
        },
        {
            "KeyArn": "arn:aws:kms:us-east-2:111122223333:key/144be297-0ae1-44ac-9c8f-93cd8c82f841",
            "KeyId": "144be297-0ae1-44ac-9c8f-93cd8c82f841"
        },
        {
            "KeyArn": "arn:aws:kms:us-east-2:111122223333:key/21184251-b765-428e-b852-2c7353e72571",
            "KeyId": "21184251-b765-428e-b852-2c7353e72571"
        },
        {
            "KeyArn": "arn:aws:kms:us-east-2:111122223333:key/214fe92f-5b03-4ae1-b350-db2a45dbe10c",
            "KeyId": "214fe92f-5b03-4ae1-b350-db2a45dbe10c"
        },
        {
            "KeyArn": "arn:aws:kms:us-east-2:111122223333:key/339963f2-e523-49d3-af24-a0fe752aa458",
            "KeyId": "339963f2-e523-49d3-af24-a0fe752aa458"
        },
        {
            "KeyArn": "arn:aws:kms:us-east-2:111122223333:key/b776a44b-df37-4438-9be4-a27494e271a",
            "KeyId": "b776a44b-df37-4438-9be4-a27494e271a"
        }
    ]
}
See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java
- AWS SDK for JavaScript
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V2
ListResourceTags

Returns a list of all tags for the specified customer master key (CMK).

You cannot perform this operation on a CMK in a different AWS account.

Request Syntax

```
{
    "KeyId": "string",
    "Limit": number,
    "Marker": "string"
}
```

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters (p. 147).

The request accepts the following data in JSON format.

**Note**

In the following list, the required parameters are described first.

**KeyId (p. 97)**

A unique identifier for the customer master key (CMK).

Specify the key ID or the Amazon Resource Name (ARN) of the CMK.

For example:

- Key ID: 1234abcd-12ab-34cd-56ef-1234567890ab
- Key ARN: arn:aws:kms:us-east-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab

To get the key ID and key ARN for a CMK, use ListKeys (p. 93) or DescribeKey (p. 30).

Type: String

Length Constraints: Minimum length of 1. Maximum length of 2048.

Required: Yes

**Limit (p. 97)**

Use this parameter to specify the maximum number of items to return. When this value is present, AWS KMS does not return more than the specified number of items, but it might return fewer.

This value is optional. If you include a value, it must be between 1 and 50, inclusive. If you do not include a value, it defaults to 50.

Type: Integer

Valid Range: Minimum value of 1. Maximum value of 1000.

Required: No
Response Syntax

```
{
    "NextMarker": "string",
    "Tags": [
        {
            "TagKey": "string",
            "TagValue": "string"
        }
    ],
    "Truncated": boolean
}
```

Response Elements

If the action is successful, the service sends back an HTTP 200 response.

The following data is returned in JSON format by the service.

**NextMarker (p. 98)**

When `Truncated` is true, this element is present and contains the value to use for the `Marker` parameter in a subsequent request.

Do not assume or infer any information from this value.

Type: String


Pattern: [ -ÿ]*

**Tags (p. 98)**

A list of tags. Each tag consists of a tag key and a tag value.

Type: Array of Tag (p. 146) objects

**Truncated (p. 98)**

A flag that indicates whether there are more items in the list. When this value is true, the list in this response is truncated. To get more items, pass the value of the `NextMarker` element in this response to the `Marker` parameter in a subsequent request.
Errors

For information about the errors that are common to all actions, see Common Errors (p. 149).

InvalidArnException

The request was rejected because a specified ARN was not valid.

HTTP Status Code: 400

InvalidMarkerException

The request was rejected because the marker that specifies where pagination should next begin is not valid.

HTTP Status Code: 400

KMSInternalException

The request was rejected because an internal exception occurred. The request can be retried.

HTTP Status Code: 400

NotFoundException

The request was rejected because the specified entity or resource could not be found.

HTTP Status Code: 400

Examples

The following examples are formatted for legibility.

Example Request

```plaintext
POST / HTTP/1.1
Host: kms.us-east-2.amazonaws.com
Content-Length: 49
X-Amz-Target: TrentService.ListResourceTags
X-Amz-Date: 20170109T200421Z
Content-Type: application/x-amz-json-1.1
Authorization: AWS4-HMAC-SHA256
Credential=AKIAI44QH8DHBEXAMPLE/20170109/us-east-2/kms/aws4_request,
SignedHeaders=content-type;host;x-amz-date;x-amz-target,
Signature=17706fce40fda00c6768b3297355c353490c1ddf3b3a9591193612961cd2cb4

{"KeyId": "1234abcd-12ab-34cd-56ef-1234567890ab"}
```

Example Response

```plaintext
HTTP/1.1 200 OK
Server: Server
Date: Mon, 09 Jan 2017 20:04:22 GMT
Content-Type: application/x-amz-json-1.1
Content-Length: 158
Connection: keep-alive
```
See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java
- AWS SDK for JavaScript
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V2
ListRetirableGrants

Returns a list of all grants for which the grant's RetiringPrincipal matches the one specified.

A typical use is to list all grants that you are able to retire. To retire a grant, use RetireGrant (p. 115).

Request Syntax

```json
{
  "Limit": number,
  "Marker": "string",
  "RetiringPrincipal": "string"
}
```

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters (p. 147).

The request accepts the following data in JSON format.

Note
In the following list, the required parameters are described first.

**RetiringPrincipal (p. 101)**

The retiring principal for which to list grants.

To specify the retiring principal, use the Amazon Resource Name (ARN) of an AWS principal. Valid AWS principals include AWS accounts (root), IAM users, federated users, and assumed role users. For examples of the ARN syntax for specifying a principal, see AWS Identity and Access Management (IAM) in the Example ARNs section of the Amazon Web Services General Reference.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 256.

Required: Yes

**Limit (p. 101)**

Use this parameter to specify the maximum number of items to return. When this value is present, AWS KMS does not return more than the specified number of items, but it might return fewer.

This value is optional. If you include a value, it must be between 1 and 100, inclusive. If you do not include a value, it defaults to 50.

Type: Integer

Valid Range: Minimum value of 1. Maximum value of 100.

Required: No

**Marker (p. 101)**

Use this parameter in a subsequent request after you receive a response with truncated results. Set it to the value of NextMarker from the truncated response you just received.

Type: String
Response Syntax

```json
{
    "Grants": [
        {
            "Constraints": {
                "EncryptionContextEquals": {
                    "string": "string"
                },
                "EncryptionContextSubset": {
                    "string": "string"
                }
            },
            "CreationDate": number,
            "GranteePrincipal": "string",
            "GrantId": "string",
            "IssuingAccount": "string",
            "KeyId": "string",
            "Name": "string",
            "Operations": ["string"],
            "RetiringPrincipal": "string"
        }
    ],
    "NextMarker": "string",
    "Truncated": boolean
}
```

Response Elements

If the action is successful, the service sends back an HTTP 200 response.

The following data is returned in JSON format by the service.

**Grants (p. 102)**

A list of grants.

Type: Array of GrantListEntry (p. 140) objects

**NextMarker (p. 102)**

When Truncated is true, this element is present and contains the value to use for the Marker parameter in a subsequent request.

Type: String


Pattern: [\u0020-\u00FF]*

**Truncated (p. 102)**

A flag that indicates whether there are more items in the list. When this value is true, the list in this response is truncated. To get more items, pass the value of the NextMarker element in this response to the Marker parameter in a subsequent request.
Type: Boolean

Errors

For information about the errors that are common to all actions, see Common Errors (p. 149).

DependencyTimeoutException

The system timed out while trying to fulfill the request. The request can be retried.

HTTP Status Code: 500

InvalidArnException

The request was rejected because a specified ARN was not valid.

HTTP Status Code: 400

InvalidMarkerException

The request was rejected because the marker that specifies where pagination should next begin is not valid.

HTTP Status Code: 400

KMSInternalException

The request was rejected because an internal exception occurred. The request can be retried.

HTTP Status Code: 400

NotFoundException

The request was rejected because the specified entity or resource could not be found.

HTTP Status Code: 400

Examples

The following examples are formatted for legibility.

Example Request

```plaintext
POST / HTTP/1.1
Host: kms.us-east-2.amazonaws.com
Content-Length: 61
X-Amz-Target: TrentService.ListRetirableGrants
X-Amz-Date: 20161207T191040Z
Content-Type: application/x-amz-json-1.1
Authorization: AWS4-HMAC-SHA256
  Credential=AKIAI44QH8DHBEROLE/20161207/us-east-2/kms/aws4_request,\n  SignedHeaders=content-type;host;x-amz-date;x-amz-target,\n  Signature=d5e43f0cfdfb75a3251f40b47e76f83b3110b33e9d972142ae118b2c0f67b39

{"RetiringPrincipal": "arn:aws:iam::111122223333:role/ExampleRole"}
```

Example Response

```
HTTP/1.1 200 OK
```

API Version 2014-11-01

103
See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java
- AWS SDK for JavaScript
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V2
PutKeyPolicy

Attaches a key policy to the specified customer master key (CMK). You cannot perform this operation on a CMK in a different AWS account.

For more information about key policies, see Key Policies in the AWS Key Management Service Developer Guide.

Request Syntax

```json
{
  "BypassPolicyLockoutSafetyCheck": boolean,
  "KeyId": "string",
  "Policy": "string",
  "PolicyName": "string"
}
```

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters (p. 147).

The request accepts the following data in JSON format.

**Note**
In the following list, the required parameters are described first.

**KeyId (p. 105)**

A unique identifier for the customer master key (CMK).

Specify the key ID or the Amazon Resource Name (ARN) of the CMK.

For example:
- Key ID: 1234abcd-12ab-34cd-56ef-1234567890ab
- Key ARN: arn:aws:kms:us-east-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab

To get the key ID and key ARN for a CMK, use ListKeys (p. 93) or DescribeKey (p. 30).

Type: String

Length Constraints: Minimum length of 1. Maximum length of 2048.

Required: Yes

**Policy (p. 105)**

The key policy to attach to the CMK.

If you do not set BypassPolicyLockoutSafetyCheck to true, the policy must meet the following criteria:
- It must allow the principal that is making the PutKeyPolicy request to make a subsequent PutKeyPolicy request on the CMK. This reduces the likelihood that the CMK becomes unmanageable. For more information, refer to the scenario in the Default Key Policy section in the AWS Key Management Service Developer Guide.
The principals that are specified in the key policy must exist and be visible to AWS KMS. When you create a new AWS principal (for example, an IAM user or role), you might need to enforce a delay before specifying the new principal in a key policy because the new principal might not immediately be visible to AWS KMS. For more information, see Changes that I make are not always immediately visible in the IAM User Guide.

The policy size limit is 32 kilobytes (32768 bytes).

Type: String
Pattern: [	
 -ÿ]+
Required: Yes

**PolicyName (p. 105)**

The name of the key policy. The only valid value is default.

Type: String
Pattern: [\w]+
Required: Yes

**BypassPolicyLockoutSafetyCheck (p. 105)**

A flag to indicate whether to bypass the key policy lockout safety check.

**Important**
Setting this value to true increases the likelihood that the CMK becomes unmanageable. Do not set this value to true indiscriminately. For more information, refer to the scenario in the Default Key Policy section in the AWS Key Management Service Developer Guide.

Use this parameter only when you intend to prevent the principal that is making the request from making a subsequent PutKeyPolicy request on the CMK.

The default value is false.

Type: Boolean
Required: No

**Response Elements**

If the action is successful, the service sends back an HTTP 200 response with an empty HTTP body.

**Errors**

For information about the errors that are common to all actions, see Common Errors (p. 149).

**DependencyTimeoutException**

The system timed out while trying to fulfill the request. The request can be retried.

HTTP Status Code: 500
InvalidArnException

The request was rejected because a specified ARN was not valid.

HTTP Status Code: 400

KMSInternalException

The request was rejected because an internal exception occurred. The request can be retried.

HTTP Status Code: 400

KMSInvalidStateException

The request was rejected because the state of the specified resource is not valid for this request.

For more information about how key state affects the use of a CMK, see How Key State Affects Use of a Customer Master Key in the AWS Key Management Service Developer Guide.

HTTP Status Code: 400

LimitExceededException

The request was rejected because a limit was exceeded. For more information, see Limits in the AWS Key Management Service Developer Guide.

HTTP Status Code: 400

MalformedPolicyDocumentException

The request was rejected because the specified policy is not syntactically or semantically correct.

HTTP Status Code: 400

NotFoundException

The request was rejected because the specified entity or resource could not be found.

HTTP Status Code: 400

UnsupportedOperationException

The request was rejected because a specified parameter is not supported or a specified resource is not valid for this operation.

HTTP Status Code: 400

Examples

Example Request

The following example is formatted for legibility.

```
POST / HTTP/1.1
Host: kms.us-east-2.amazonaws.com
Content-Length: 2396
X-Amz-Target: TrentService.PutKeyPolicy
X-Amz-Date: 20161207T203023Z
Content-Type: application/x-amz-json-1.1
Authorization: AWS4-HMAC-SHA256
Credential=AKIAI44QH8DHBEXAMPLE/20161207/us-east-2/kms/aws4_request,
SignedHeaders=content-type;host;x-amz-date;x-amz-target,
Signature=e58ea91db06af11bc7a1f204769cf6bc4d003ee090095a13caef361c69739ede
```
{
  "Policy": {
    "Version": "2012-10-17",
    "Id": "custom-policy-2016-12-07",
    "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:user/ExampleAdminUser",
            "arn:aws:iam::111122223333:role/ExampleAdminRole"
          ]
        },
      ],
        "Resource": "*"
      },
      {
        "Sid": "Allow use of the key",
        "Effect": "Allow",
        "Principal": {
          "AWS": "arn:aws:iam::111122223333:role/ExamplePowerUserRole"
        },
        "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/ExamplePowerUserRole"
      },
      "Action": ["kms:CreateGrant", "kms:ListGrants", "kms:RevokeGrant"]
    }
  }
}
"Resource": "+",
"Condition": {
  "Bool": {
    "kms:GrantIsForAWSResource": "true"
  }
}
],

"PolicyName": "default",
"KeyId": "1234abcd-12ab-34cd-56ef-1234567890ab"
}

### Example Response

HTTP/1.1 200 OK
Server: Server
Date: Wed, 07 Dec 2016 20:30:23 GMT
Content-Type: application/x-amz-json-1.1
Content-Length: 0
Connection: keep-alive
x-amzn-RequestId: fb114d4c-bcbb-11e6-82b3-e9e4af764a06

### See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java
- AWS SDK for JavaScript
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V2
ReEncrypt

Encrypts data on the server side with a new customer master key (CMK) without exposing the plaintext of the data on the client side. The data is first decrypted and then reencrypted. You can also use this operation to change the encryption context of a ciphertext.

You can reencrypt data using CMKs in different AWS accounts.

Unlike other operations, ReEncrypt is authorized twice, once as ReEncryptFrom on the source CMK and once as ReEncryptTo on the destination CMK. We recommend that you include the "kms:ReEncrypt*" permission in your key policies to permit reencryption from or to the CMK. This permission is automatically included in the key policy when you create a CMK through the console, but you must include it manually when you create a CMK programmatically or when you set a key policy with the PutKeyPolicy (p. 105) operation.

Request Syntax

```json
{
    "CiphertextBlob": blob,
    "DestinationEncryptionContext": {
        "string": "string"
    },
    "DestinationKeyId": "string",
    "GrantTokens": [ "string" ],
    "SourceEncryptionContext": {
        "string": "string"
    }
}
```

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters (p. 147).

The request accepts the following data in JSON format.

**Note**

In the following list, the required parameters are described first.

**CiphertextBlob (p. 110)**

Ciphertext of the data to reencrypt.

Type: Base64-encoded binary data object


Required: Yes

**DestinationKeyId (p. 110)**

A unique identifier for the CMK that is used to reencrypt the data.

To specify a CMK, use its key ID, Amazon Resource Name (ARN), alias name, or alias ARN. When using an alias name, prefix it with "alias/". To specify a CMK in a different AWS account, you must use the key ARN or alias ARN.

For example:
Key ID: 1234abcd-12ab-34cd-56ef-1234567890ab
Key ARN: arn:aws:kms:us-east-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab
Alias name: alias/ExampleAlias

To get the key ID and key ARN for a CMK, use ListKeys (p. 93) or DescribeKey (p. 30). To get the alias name and alias ARN, use ListAliases (p. 80).

Type: String
Length Constraints: Minimum length of 1. Maximum length of 2048.
Required: Yes

DestinationEncryptionContext (p. 110)
Encryption context to use when the data is reencrypted.
Type: String to string map
Required: No

GrantTokens (p. 110)
A list of grant tokens.
For more information, see Grant Tokens in the AWS Key Management Service Developer Guide.
Type: Array of strings
Array Members: Minimum number of 0 items. Maximum number of 10 items.
Required: No

SourceEncryptionContext (p. 110)
Encryption context used to encrypt and decrypt the data specified in the CiphertextBlob parameter.
Type: String to string map
Required: No

Response Syntax

```json
{
  "CiphertextBlob": blob,
  "KeyId": "string",
  "SourceKeyId": "string"
}
```

Response Elements
If the action is successful, the service sends back an HTTP 200 response.
The following data is returned in JSON format by the service.
CiphertextBlob (p. 111)

The reencrypted data. When you use the HTTP API or the AWS CLI, the value is Base64-encoded. Otherwise, it is not encoded.

Type: Base64-encoded binary data object


KeyId (p. 111)

Unique identifier of the CMK used to reencrypt the data.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 2048.

SourceKeyId (p. 111)

Unique identifier of the CMK used to originally encrypt the data.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 2048.

Errors

For information about the errors that are common to all actions, see Common Errors (p. 149).

DependencyTimeoutException

The system timed out while trying to fulfill the request. The request can be retried.

HTTP Status Code: 500

DisabledException

The request was rejected because the specified CMK is not enabled.

HTTP Status Code: 400

InvalidCiphertextException

The request was rejected because the specified ciphertext, or additional authenticated data incorporated into the ciphertext, such as the encryption context, is corrupted, missing, or otherwise invalid.

HTTP Status Code: 400

InvalidGrantTokenException

The request was rejected because the specified grant token is not valid.

HTTP Status Code: 400

InvalidKeySpecException

The request was rejected because the specified KeySpec value is not valid.

HTTP Status Code: 400

KeyUnavailableException

The request was rejected because the specified CMK was not available. The request can be retried.

HTTP Status Code: 500
KMSInternalException
The request was rejected because an internal exception occurred. The request can be retried.
HTTP Status Code: 400

KMSInvalidStateException
The request was rejected because the state of the specified resource is not valid for this request.
For more information about how key state affects the use of a CMK, see How Key State Affects Use of a Customer Master Key in the AWS Key Management Service Developer Guide.
HTTP Status Code: 400

NotFoundException
The request was rejected because the specified entity or resource could not be found.
HTTP Status Code: 400

Examples
The following examples are formatted for legibility.

Example Request

```plaintext
POST / HTTP/1.1
Host: kms.us-east-2.amazonaws.com
Content-Length: 306
X-Amz-Target: TrentService.ReEncrypt
X-Amz-Date: 20161207T225816Z
Content-Type: application/x-amz-json-1.1
Authorization: AWS4-HMAC-SHA256
  Credential=AKIAI44QH8DHBEXAMPLE/20161207/us-east-2/kms/aws4_request,\n  SignedHeaders=content-type;host;x-amz-date;x-amz-target,\n  Signature=7afd339e2a680e0726592ddf687aaee8e18d8a7933a60ebbd0054b82936ef2
{
  "DestinationKeyId": "0987dcba-09fe-87dc-65ba-ab0987654321",
  "CiphertextBlob": "AQECAHj/M9MyvNsMT8kW
  +K5DVkMfunTHzGw6crnuAgW80uRwAAAH0wwyJYoNZhvcNAQcGoG4wbAIAIBABnBkgkqhkiG9w0BBwEwHgYJYIIZIAWUDBAsMBEBDFX
  +F5KUmNmmE0HOaHHRYRDR6XqUnaCNznAuhhq4YTGBfii6eWtjYU83pGmradVUwX8E/tbCg=="
}
```

Example Response

```plaintext
HTTP/1.1 200 OK
Server: Server
Date: Wed, 07 Dec 2016 22:58:17 GMT
Content-Type: application/x-amz-json-1.1
Content-Length: 423
Connection: keep-alive
x-amzn-RequestId: a434eca2-bcd0-11e6-b60b-ff95eb2d1d15
{
  "CiphertextBlob": "AQECAHjRYf5Wyt1cOC857tFSnBapn2F8DgfmThbJlfRE83WiAAMH0wwyJYoNZhvcNAQcGoG4wbAIAIBADBnBkgkqhkiG9w0BBwEwHgYJYIIZIAWUDBAsMBEBDFX
  +F5KUmNmmE0HOaHHRYRDR6XqUnaCNznAuhhq4YTGBfii6eWtjYU83pGmradVUwX8E/tbCg==",
```

113
"KeyId": "arn:aws:kms:us-east-2:111122223333:key/0987dcba-09fe-87dc-65ba-ab0987654321",
"SourceKeyId": "arn:aws:kms:us-east-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab"
}

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java
- AWS SDK for JavaScript
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V2
RetireGrant

Retires a grant. To clean up, you can retire a grant when you’re done using it. You should revoke a grant when you intend to actively deny operations that depend on it. The following are permitted to call this API:

- The AWS account (root user) under which the grant was created
- The RetiringPrincipal, if present in the grant
- The GranteePrincipal, if RetireGrant is an operation specified in the grant

You must identify the grant to retire by its grant token or by a combination of the grant ID and the Amazon Resource Name (ARN) of the customer master key (CMK). A grant token is a unique variable-length base64-encoded string. A grant ID is a 64 character unique identifier of a grant. The CreateGrant (p. 10) operation returns both.

Request Syntax

```json
{
  "GrantId": "string",
  "GrantToken": "string",
  "KeyId": "string"
}
```

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters (p. 147).

The request accepts the following data in JSON format.

**Note**
In the following list, the required parameters are described first.

**GrantId (p. 115)**

Unique identifier of the grant to retire. The grant ID is returned in the response to a CreateGrant operation.

- Grant ID Example -
  0123456789012345678901234567890123456789012345678901234567890123456789

  Type: String


  Required: No

**GrantToken (p. 115)**

Token that identifies the grant to be retired.

- Type: String


  Required: No

**KeyId (p. 115)**

The Amazon Resource Name (ARN) of the CMK associated with the grant.
For example: arn:aws:kms:us-east-2:444455556666:key/1234abcd-12ab-34cd-56ef-1234567890ab

Type: String
Length Constraints: Minimum length of 1. Maximum length of 2048.
Required: No

**Response Elements**

If the action is successful, the service sends back an HTTP 200 response with an empty HTTP body.

**Errors**

For information about the errors that are common to all actions, see Common Errors (p. 149).

**DependencyTimeoutException**

The system timed out while trying to fulfill the request. The request can be retried.

HTTP Status Code: 500

**InvalidGrantIdException**

The request was rejected because the specified GrantId is not valid.

HTTP Status Code: 400

**InvalidGrantTokenException**

The request was rejected because the specified grant token is not valid.

HTTP Status Code: 400

**KMSInternalException**

The request was rejected because an internal exception occurred. The request can be retried.

HTTP Status Code: 400

**KMSInvalidStateException**

The request was rejected because the state of the specified resource is not valid for this request.

For more information about how key state affects the use of a CMK, see How Key State Affects Use of a Customer Master Key in the AWS Key Management Service Developer Guide.

HTTP Status Code: 400

**NotFoundException**

The request was rejected because the specified entity or resource could not be found.

HTTP Status Code: 400

**Examples**

**Example Request**

The following example is formatted for legibility.
Example Response

HTTP/1.1 200 OK
Server: Server
Date: Thu, 08 Dec 2016 23:32:38 GMT
Content-Type: application/x-amz-json-1.1
Content-Length: 0
Connection: keep-alive
x-amzn-RequestId: 9ad2b038-bd9e-11e6-ace2-6fb96f685e31

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java
- AWS SDK for JavaScript
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V2
RevokeGrant

RevokeGrant

RevokeGrant

Revokes the specified grant for the specified customer master key (CMK). You can revoke a grant to actively deny operations that depend on it.

To perform this operation on a CMK in a different AWS account, specify the key ARN in the value of the KeyId parameter.

Request Syntax

```json
{
   "GrantId": "string",
   "KeyId": "string"
}
```

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters (p. 147).

The request accepts the following data in JSON format.

**Note**

In the following list, the required parameters are described first.

**GrantId (p. 118)**

Identifier of the grant to be revoked.

Type: String


Required: Yes

**KeyId (p. 118)**

A unique identifier for the customer master key associated with the grant.

Specify the key ID or the Amazon Resource Name (ARN) of the CMK. To specify a CMK in a different AWS account, you must use the key ARN.

For example:

- Key ID: 1234abcd-12ab-34cd-56ef-1234567890ab
- Key ARN: arn:aws:kms:us-east-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab

To get the key ID and key ARN for a CMK, use ListKeys (p. 93) or DescribeKey (p. 30).

Type: String

Length Constraints: Minimum length of 1. Maximum length of 2048.

Required: Yes

Response Elements

If the action is successful, the service sends back an HTTP 200 response with an empty HTTP body.
Errors

For information about the errors that are common to all actions, see Common Errors (p. 149).

**DependencyTimeoutException**

The system timed out while trying to fulfill the request. The request can be retried.

HTTP Status Code: 500

**InvalidArnException**

The request was rejected because a specified ARN was not valid.

HTTP Status Code: 400

**InvalidGrantIdException**

The request was rejected because the specified GrantId is not valid.

HTTP Status Code: 400

**KMSInternalException**

The request was rejected because an internal exception occurred. The request can be retried.

HTTP Status Code: 400

**KMSInvalidStateException**

The request was rejected because the state of the specified resource is not valid for this request.

For more information about how key state affects the use of a CMK, see How Key State Affects Use of a Customer Master Key in the AWS Key Management Service Developer Guide.

HTTP Status Code: 400

**NotFoundException**

The request was rejected because the specified entity or resource could not be found.

HTTP Status Code: 400

Examples

Example Request

The following example is formatted for legibility.

```json
POST / HTTP/1.1
Host: kms.us-west-2.amazonaws.com
Content-Length: 128
X-Amz-Target: TrentService.RevokeGrant
X-Amz-Date: 20161210T000739Z
Content-Type: application/x-amz-json-1.1
Authorization: AWS4-HMAC-SHA256
Credential=AKIAI44QH8DHBEXAMPLE/20161210/us-west-2/kms/aws4_request,
SignedHeaders=content-type;host;x-amz-date;x-amz-target,
Signature=3f4073c96c38c38c8bc006b3a74a67fb2108cfe2d6f23f96f09047924919806a7d

{
    "KeyId": "1234abcd-12ab-34cd-56ef-1234567890ab",
```
"GrantId": "f271e8328717f8bde5d03f4981f06a6b3fc18bcaee2da12ac38bd9186e7925d11"
}

Example Response

HTTP/1.1 200 OK
Server: Server
Date: Sat, 10 Dec 2016 00:07:40 GMT
Content-Type: application/x-amz-json-1.1
Content-Length: 0
Connection: keep-alive
x-amzn-RequestId: aa49887b-be6c-11e6-b749-7394871b1b43

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java
- AWS SDK for JavaScript
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V2
ScheduleKeyDeletion

Schedules the deletion of a customer master key (CMK). You may provide a waiting period, specified in days, before deletion occurs. If you do not provide a waiting period, the default period of 30 days is used. When this operation is successful, the state of the CMK changes to `PendingDeletion`. Before the waiting period ends, you can use `CancelKeyDeletion (p. 4)` to cancel the deletion of the CMK. After the waiting period ends, AWS KMS deletes the CMK and all AWS KMS data associated with it, including all aliases that refer to it.

You cannot perform this operation on a CMK in a different AWS account.

**Important**

Deleting a CMK is a destructive and potentially dangerous operation. When a CMK is deleted, all data that was encrypted under the CMK is rendered unrecoverable. To restrict the use of a CMK without deleting it, use `DisableKey (p. 34)`.

For more information about scheduling a CMK for deletion, see Deleting Customer Master Keys in the AWS Key Management Service Developer Guide.

**Request Syntax**

```json
{
  "KeyId": "string",
  "PendingWindowInDays": number
}
```

**Request Parameters**

For information about the parameters that are common to all actions, see Common Parameters (p. 147).

The request accepts the following data in JSON format.

**Note**

In the following list, the required parameters are described first.

**KeyId (p. 121)**

The unique identifier of the customer master key (CMK) to delete.

Specify the key ID or the Amazon Resource Name (ARN) of the CMK.

For example:

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

To get the key ID and key ARN for a CMK, use `ListKeys (p. 93)` or `DescribeKey (p. 30)`.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 2048.

Required: Yes

**PendingWindowInDays (p. 121)**

The waiting period, specified in number of days. After the waiting period ends, AWS KMS deletes the customer master key (CMK).
This value is optional. If you include a value, it must be between 7 and 30, inclusive. If you do not include a value, it defaults to 30.

Type: Integer


Required: No

Response Syntax

```json
{
  "DeletionDate": number,
  "KeyId": "string"
}
```

Response Elements

If the action is successful, the service sends back an HTTP 200 response.

The following data is returned in JSON format by the service.

**DeletionDate (p. 122)**

The date and time after which AWS KMS deletes the customer master key (CMK).

Type: Timestamp

**KeyId (p. 122)**

The unique identifier of the customer master key (CMK) for which deletion is scheduled.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 2048.

Errors

For information about the errors that are common to all actions, see Common Errors (p. 149).

**DependencyTimeoutException**

The system timed out while trying to fulfill the request. The request can be retried.

HTTP Status Code: 500

**InvalidArnException**

The request was rejected because a specified ARN was not valid.

HTTP Status Code: 400

**KMSInternalException**

The request was rejected because an internal exception occurred. The request can be retried.

HTTP Status Code: 400
KMSInvalidStateException

The request was rejected because the state of the specified resource is not valid for this request.

For more information about how key state affects the use of a CMK, see How Key State Affects Use of a Customer Master Key in the AWS Key Management Service Developer Guide.

HTTP Status Code: 400

NotFoundException

The request was rejected because the specified entity or resource could not be found.

HTTP Status Code: 400

Examples

The following examples are formatted for legibility.

Example Request

```
POST / HTTP/1.1
Host: kms.us-east-2.amazonaws.com
Content-Length: 75
X-Amz-Target: TrentService.ScheduleKeyDeletion
X-Amz-Date: 20161210T003358Z
Content-Type: application/x-amz-json-1.1
Authorization: AWS4-HMAC-SHA256
Credential=AKIAI44QH8DHBEXAMPLE/20161210/us-east-2/kms/aws4_request,
SignedHeaders=content-type;host;x-amz-date;x-amz-target,
Signature=c42c52cf0e4057e004b73a905b0e5da215f63d33117e7316f760e6223433abb
{
  "PendingWindowInDays": 7,
  "KeyId": "1234abcd-12ab-34cd-56ef-1234567890ab"
}
```

Example Response

```
HTTP/1.1 200 OK
Server: Server
Date: Sat, 10 Dec 2016 00:33:58 GMT
Content-Type: application/x-amz-json-1.1
Content-Length: 114
Connection: keep-alive
x-amzn-RequestId: 5704ddf7-be70-11e6-b0c0-3343f53dee45
{
  "DeletionDate": 1.4820192E9,
  "KeyId": "arn:aws:kms:us-east-2:11112223333:key/1234abcd-12ab-34cd-56ef-1234567890ab"
}
```

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface
- AWS SDK for .NET
See Also

- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java
- AWS SDK for JavaScript
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V2
TagResource

Adds or overwrites one or more tags for the specified customer master key (CMK). You cannot perform this operation on a CMK in a different AWS account.

Each tag consists of a tag key and a tag value. Tag keys and tag values are both required, but tag values can be empty (null) strings.

You cannot use the same tag key more than once per CMK. For example, consider a CMK with one tag whose tag key is `Purpose` and tag value is `Test`. If you send a `TagResource` request for this CMK with a tag key of `Purpose` and a tag value of `Prod`, it does not create a second tag. Instead, the original tag is overwritten with the new tag value.

For information about the rules that apply to tag keys and tag values, see User-Defined Tag Restrictions in the AWS Billing and Cost Management User Guide.

Request Syntax

```
{
  "KeyId": "string",
  "Tags": [
    {
      "TagKey": "string",
      "TagValue": "string"
    }
  ]
}
```

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters (p. 147).

The request accepts the following data in JSON format.

**Note**

In the following list, the required parameters are described first.

**KeyId (p. 125)**

A unique identifier for the CMK you are tagging.

Specify the key ID or the Amazon Resource Name (ARN) of the CMK.

For example:

- Key ID: 1234abcd-12ab-34cd-56ef-1234567890ab
- Key ARN: arn:aws:kms:us-east-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab

To get the key ID and key ARN for a CMK, use ListKeys (p. 93) or DescribeKey (p. 30).

Type: String

Length Constraints: Minimum length of 1. Maximum length of 2048.

Required: Yes
Tags (p. 125)

One or more tags. Each tag consists of a tag key and a tag value.

Type: Array of Tag (p. 146) objects

Required: Yes

Response Elements

If the action is successful, the service sends back an HTTP 200 response with an empty HTTP body.

Errors

For information about the errors that are common to all actions, see Common Errors (p. 149).

InvalidArnException

The request was rejected because a specified ARN was not valid.

HTTP Status Code: 400

KMSInternalException

The request was rejected because an internal exception occurred. The request can be retried.

HTTP Status Code: 400

KMSInvalidStateException

The request was rejected because the state of the specified resource is not valid for this request.

For more information about how key state affects the use of a CMK, see How Key State Affects Use of a Customer Master Key in the AWS Key Management Service Developer Guide.

HTTP Status Code: 400

LimitExceededException

The request was rejected because a limit was exceeded. For more information, see Limits in the AWS Key Management Service Developer Guide.

HTTP Status Code: 400

NotFoundException

The request was rejected because the specified entity or resource could not be found.

HTTP Status Code: 400

TagException

The request was rejected because one or more tags are not valid.

HTTP Status Code: 400

Examples

Example Request

The following example is formatted for legibility.
POST / HTTP/1.1
Host: kms.us-east-2.amazonaws.com
Content-Length: 102
X-Amz-Target: TrentService.TagResource
X-Amz-Date: 20170109T200202Z
Content-Type: application/x-amz-json-1.1
Authorization: AWS4-HMAC-SHA256
Credential=AKIAI44QH8DHBEXAMPLE/20170109/us-east-2/kms/aws4_request,\nSignedHeaders=content-type;host;x-amz-date;x-amz-target,\nSignature=5a5e6b9950567ea2b9ead41df706fd8f3e4a900553957c5c7f1992daaa67b8ff
{
    "KeyId": "1234abcd-12ab-34cd-56ef-1234567890ab",
    "Tags": [{
        "TagKey": "Purpose",
        "TagValue": "Test"
    }]
}

Example Response

HTTP/1.1 200 OK
Server: Server
Date: Mon, 09 Jan 2017 20:02:03 GMT
Content-Type: application/x-amz-json-1.1
Content-Length: 0
Connection: keep-alive
x-amzn-RequestId: 7ce02bcb-d6a6-11e6-bfed-ebe31947a596

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java
- AWS SDK for JavaScript
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V2
UntagResource

Removes the specified tag or tags from the specified customer master key (CMK). You cannot perform this operation on a CMK in a different AWS account.

To remove a tag, you specify the tag key for each tag to remove. You do not specify the tag value. To overwrite the tag value for an existing tag, use TagResource (p. 125).

Request Syntax

```json
{
  "KeyId": "string",
  "TagKeys": [ "string" ]
}
```

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters (p. 147).

The request accepts the following data in JSON format.

**Note**
In the following list, the required parameters are described first.

**KeyId (p. 128)**

A unique identifier for the CMK from which you are removing tags.

Specify the key ID or the Amazon Resource Name (ARN) of the CMK.

For example:
- Key ID: 1234abcd-12ab-34cd-56ef-1234567890ab
- Key ARN: arn:aws:kms:us-east-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab

To get the key ID and key ARN for a CMK, use ListKeys (p. 93) or DescribeKey (p. 30).

Type: String

Length Constraints: Minimum length of 1. Maximum length of 2048.

Required: Yes

**TagKeys (p. 128)**

One or more tag keys. Specify only the tag keys, not the tag values.

Type: Array of strings


Required: Yes

Response Elements

If the action is successful, the service sends back an HTTP 200 response with an empty HTTP body.
Errors

For information about the errors that are common to all actions, see Common Errors (p. 149).

InvalidArnException

The request was rejected because a specified ARN was not valid.

HTTP Status Code: 400

KMSInternalException

The request was rejected because an internal exception occurred. The request can be retried.

HTTP Status Code: 400

KMSInvalidStateException

The request was rejected because the state of the specified resource is not valid for this request.

For more information about how key state affects the use of a CMK, see How Key State Affects Use of a Customer Master Key in the AWS Key Management Service Developer Guide.

HTTP Status Code: 400

NotFoundException

The request was rejected because the specified entity or resource could not be found.

HTTP Status Code: 400

TagException

The request was rejected because one or more tags are not valid.

HTTP Status Code: 400

Examples

Example Request

The following example is formatted for legibility.

```plaintext
POST / HTTP/1.1
Host: kms.us-east-2.amazonaws.com
Content-Length: 87
X-Amz-Target: TrentService.UntagResource
X-Amz-Date: 20170109T200704Z
Content-Type: application/x-amz-json-1.1
Authorization: AWS4-HMAC-SHA256
   Credential=AKIAI44QH8DHBEXAMPLE/20170109/us-east-2/kms/aws4_request,
   SignedHeaders=content-type;host;x-amz-date;x-amz-target,
   Signature=f1c9c01e545fa02e2db0a96b66d5f6978001b8e06a1776058206dc393b8d1b4

{  
   "KeyId": "1234abcd-12ab-34cd-56ef-1234567890ab",  
   "TagKeys": [  
      "Purpose",  
      "CostCenter"  
   ]
}
```
Example Response

```
HTTP/1.1 200 OK
Server: Server
Date: Mon, 09 Jan 2017 20:07:04 GMT
Content-Type: application/x-amz-json-1.1
Content-Length: 0
Connection: keep-alive
x-amzn-RequestId: 30b417a1-d6a7-11e6-a164-b5365990e84e
```

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java
- AWS SDK for JavaScript
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V2
UpdateAlias

Associates an existing alias with a different customer master key (CMK). Each CMK can have multiple aliases, but the aliases must be unique within the account and region. You cannot perform this operation on an alias in a different AWS account.

This operation works only on existing aliases. To change the alias of a CMK to a new value, use CreateAlias (p. 7) to create a new alias and DeleteAlias (p. 24) to delete the old alias.

Because an alias is not a property of a CMK, you can create, update, and delete the aliases of a CMK without affecting the CMK. Also, aliases do not appear in the response from the DescribeKey (p. 30) operation. To get the aliases of all CMKs in the account, use the ListAliases (p. 80) operation.

An alias name can contain only alphanumeric characters, forward slashes (/), underscores (_), and dashes (-). An alias must start with the word alias followed by a forward slash (alias/). The alias name can contain only alphanumeric characters, forward slashes (/), underscores (_), and dashes (-). Alias names cannot begin with aws; that alias name prefix is reserved by Amazon Web Services (AWS).

Request Syntax

```
{
  "AliasName": "string",
  "TargetKeyId": "string"
}
```

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters (p. 147).

The request accepts the following data in JSON format.

**Note**
In the following list, the required parameters are described first.

**AliasName (p. 131)**

String that contains the name of the alias to be modified. The name must start with the word "alias" followed by a forward slash (alias/). Aliases that begin with "alias/aws" are reserved.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 256.

Pattern: `^[a-zA-Z0-9:/_\-]+$`

Required: Yes

**TargetKeyId (p. 131)**

Unique identifier of the customer master key to be mapped to the alias.

Specify the key ID or the Amazon Resource Name (ARN) of the CMK.

For example:
- Key ID: 1234abcd-12ab-34cd-56ef-1234567890ab
- Key ARN: arn:aws:kms:us-east-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab
To get the key ID and key ARN for a CMK, use `ListKeys` (p. 93) or `DescribeKey` (p. 30).

To verify that the alias is mapped to the correct CMK, use `ListAliases` (p. 80).

Type: String

Length Constraints: Minimum length of 1. Maximum length of 2048.

Required: Yes

**Response Elements**

If the action is successful, the service sends back an HTTP 200 response with an empty HTTP body.

**Errors**

For information about the errors that are common to all actions, see Common Errors (p. 149).

**DependencyTimeoutException**

The system timed out while trying to fulfill the request. The request can be retried.

HTTP Status Code: 500

**KMSInternalException**

The request was rejected because an internal exception occurred. The request can be retried.

HTTP Status Code: 400

**KMSInvalidStateException**

The request was rejected because the state of the specified resource is not valid for this request.

For more information about how key state affects the use of a CMK, see How Key State Affects Use of a Customer Master Key in the AWS Key Management Service Developer Guide.

HTTP Status Code: 400

**NotFoundException**

The request was rejected because the specified entity or resource could not be found.

HTTP Status Code: 400

**Examples**

**Example Request**

The following example is formatted for legibility.

```plaintext
POST / HTTP/1.1
Host: kms.us-east-2.amazonaws.com
Content-Length: 90
X-Amz-Target: TrentService.UpdateAlias
X-Amz-Date: 20161212T193252Z
Content-Type: application/x-amz-json-1.1
Authorization: AWS4-HMAC-SHA256
    Credential=AKIAI44QH8DHBEXAMPLE/20161212/us-east-2/kms/aws4_request,

```
SignedHeaders=content-type;host;x-amz-date;x-amz-target,\
Signature=3d6375048a5917aff38f25b92e66bceb16b29562193f7ab7f869b4c53f115c20
{
  "TargetKeyId": "1234abcd-12ab-34cd-56ef-1234567890ab",
  "AliasName": "alias/ExampleAlias"
}

Example Response

HTTP/1.1 200 OK
Server: Server
Date: Mon, 12 Dec 2016 19:32:53 GMT
Content-Type: application/x-amz-json-1.1
Content-Length: 0
Connection: keep-alive
x-amzn-RequestId: c64706c8-c0a1-11e6-b0c0-3343f53dee45

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java
- AWS SDK for JavaScript
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V2
UpdateKeyDescription

Updates the description of a customer master key (CMK). To see the description of a CMK, use DescribeKey (p. 30).

You cannot perform this operation on a CMK in a different AWS account.

Request Syntax

```
{
    "Description": "string",
    "KeyId": "string"
}
```

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters (p. 147).

The request accepts the following data in JSON format.

**Note**

In the following list, the required parameters are described first.

**Description (p. 134)**

New description for the CMK.

Type: String

Length Constraints: Minimum length of 0. Maximum length of 8192.

Required: Yes

**KeyId (p. 134)**

A unique identifier for the customer master key (CMK).

Specify the key ID or the Amazon Resource Name (ARN) of the CMK.

For example:

- Key ID: 1234abcd-12ab-34cd-56ef-1234567890ab
- Key ARN: arn:aws:kms:us-east-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab

To get the key ID and key ARN for a CMK, use ListKeys (p. 93) or DescribeKey (p. 30).

Type: String

Length Constraints: Minimum length of 1. Maximum length of 2048.

Required: Yes

Response Elements

If the action is successful, the service sends back an HTTP 200 response with an empty HTTP body.
Errors

For information about the errors that are common to all actions, see Common Errors (p. 149).

DependencyTimeoutException

The system timed out while trying to fulfill the request. The request can be retried.

HTTP Status Code: 500

InvalidArnException

The request was rejected because a specified ARN was not valid.

HTTP Status Code: 400

KMSInternalException

The request was rejected because an internal exception occurred. The request can be retried.

HTTP Status Code: 400

KMSInvalidStateException

The request was rejected because the state of the specified resource is not valid for this request.

For more information about how key state affects the use of a CMK, see How Key State Affects Use of a Customer Master Key in the AWS Key Management Service Developer Guide.

HTTP Status Code: 400

NotFoundException

The request was rejected because the specified entity or resource could not be found.

HTTP Status Code: 400

Examples

Example Request

The following example is formatted for legibility.

```plaintext
POST / HTTP/1.1
Host: kms.us-east-2.amazonaws.com
Content-Length: 150
X-Amz-Target: TrentService.UpdateKeyDescription
X-Amz-Date: 20161212T201249Z
Content-Type: application/x-amz-json-1.1
Authorization: AWS4-HMAC-SHA256
Credential=AKIAI44QH8DHBEXAMPLE/20161212/us-east-2/kms/aws4_request,\nSignedHeaders=content-type;host;x-amz-date;x-amz-target,\nSignature=cd81d09965e5df1156eb0416ec8b2e3f9de9db4ca9285b472c319bcbbac71

{"KeyId": "1234abcd-12ab-34cd-56ef-1234567890ab","Description": "Example description that explains what this CMK is used for."}
```

Example Response
See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java
- AWS SDK for JavaScript
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V2
Data Types

The AWS Key Management Service API contains several data types that various actions use. This section describes each data type in detail.

**Note**
The order of each element in a data type structure is not guaranteed. Applications should not assume a particular order.

The following data types are supported:

- **AliasListEntry** (p. 138)
- **GrantConstraints** (p. 139)
- **GrantListEntry** (p. 140)
- **KeyListEntry** (p. 142)
- **KeyMetadata** (p. 143)
- **Tag** (p. 146)
 AliasListEntry

Contains information about an alias.

Contents

Note
In the following list, the required parameters are described first.

AliasArn

String that contains the key ARN.

Type: String


Required: No

AliasName

String that contains the alias.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 256.

Pattern: ^[a-zA-Z0-9:/_\-]+$

Required: No

TargetKeyId

String that contains the key identifier referred to by the alias.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 2048.

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java
- AWS SDK for Ruby V2
GrantConstraints

A structure that you can use to allow certain operations in the grant only when the desired encryption context is present. For more information about encryption context, see Encryption Context in the AWS Key Management Service Developer Guide.

Grant constraints apply only to operations that accept encryption context as input. For example, the DescribeKey operation does not accept encryption context as input. A grant that allows the DescribeKey operation does so regardless of the grant constraints. In contrast, the Encrypt operation accepts encryption context as input. A grant that allows the Encrypt operation does so only when the encryption context of the Encrypt operation satisfies the grant constraints.

Contents

Note
In the following list, the required parameters are described first.

EncryptionContextEquals
A list of key-value pairs that must be present in the encryption context of certain subsequent operations that the grant allows. When certain subsequent operations allowed by the grant include encryption context that matches this list, the grant allows the operation. Otherwise, the grant does not allow the operation.

Type: String to string map

Required: No

EncryptionContextSubset
A list of key-value pairs, all of which must be present in the encryption context of certain subsequent operations that the grant allows. When certain subsequent operations allowed by the grant include encryption context that matches this list or is a superset of this list, the grant allows the operation. Otherwise, the grant does not allow the operation.

Type: String to string map

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java
- AWS SDK for Ruby V2
GrantListEntry

Contains information about an entry in a list of grants.

Contents

Note
In the following list, the required parameters are described first.

Constraints
A list of key-value pairs that must be present in the encryption context of certain subsequent operations that the grant allows.
Type: GrantConstraints (p. 139) object
Required: No

CreationDate
The date and time when the grant was created.
Type: Timestamp
Required: No

GranteePrincipal
The principal that receives the grant's permissions.
Type: String
Length Constraints: Minimum length of 1. Maximum length of 256.
Required: No

GrantId
The unique identifier for the grant.
Type: String
Required: No

IssuingAccount
The AWS account under which the grant was issued.
Type: String
Length Constraints: Minimum length of 1. Maximum length of 256.
Required: No

KeyId
The unique identifier for the customer master key (CMK) to which the grant applies.
Type: String
Length Constraints: Minimum length of 1. Maximum length of 2048.
Required: No

Name

The friendly name that identifies the grant. If a name was provided in the CreateGrant (p. 10) request, that name is returned. Otherwise this value is null.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 256.

Pattern: ^[a-zA-Z0-9:/_-]+$

Required: No

Operations

The list of operations permitted by the grant.

Type: Array of strings

Valid Values: Decrypt | Encrypt | GenerateDataKey | GenerateDataKeyWithoutPlaintext | ReEncryptFrom | ReEncryptTo | CreateGrant | RetireGrant | DescribeKey

Required: No

RetiringPrincipal

The principal that can retire the grant.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 256.

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java
- AWS SDK for Ruby V2
KeyListEntry

Contains information about each entry in the key list.

Contents

**Note**

In the following list, the required parameters are described first.

**KeyArn**

ARN of the key.

Type: String


Required: No

**KeyId**

Unique identifier of the key.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 2048.

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java
- AWS SDK for Ruby V2
KeyMetadata

Contains metadata about a customer master key (CMK).

This data type is used as a response element for the CreateKey (p. 15) and DescribeKey (p. 30) operations.

Contents

Note
In the following list, the required parameters are described first.

KeyId
The globally unique identifier for the CMK.
Type: String
Length Constraints: Minimum length of 1. Maximum length of 2048.
Required: Yes

Arn
The Amazon Resource Name (ARN) of the CMK. For examples, see AWS Key Management Service (AWS KMS) in the Example ARNs section of the AWS General Reference.
Type: String
Required: No

AWSAccountId
The twelve-digit account ID of the AWS account that owns the CMK.
Type: String
Required: No

CreationDate
The date and time when the CMK was created.
Type: Timestamp
Required: No

DeletionDate
The date and time after which AWS KMS deletes the CMK. This value is present only when KeyState is PendingDeletion, otherwise this value is omitted.
Type: Timestamp
Required: No

Description
The description of the CMK.
Type: String
Length Constraints: Minimum length of 0. Maximum length of 8192.

**Enabled**

Specifies whether the CMK is enabled. When `KeyState` is `Enabled` this value is true, otherwise it is false.

Type: Boolean

Required: No

**ExpirationModel**

Specifies whether the CMK's key material expires. This value is present only when `Origin` is `EXTERNAL`, otherwise this value is omitted.

Type: String

Valid Values: `KEY_MATERIAL_EXPIRES` | `KEY_MATERIAL_DOES_NOT_EXPIRE`

Required: No

**KeyManager**

The CMK's manager. CMKs are either customer-managed or AWS-managed. For more information about the difference, see Customer Master Keys in the AWS Key Management Service Developer Guide.

Type: String

Valid Values: `AWS` | `CUSTOMER`

Required: No

**KeyState**

The state of the CMK.

For more information about how key state affects the use of a CMK, see How Key State Affects the Use of a Customer Master Key in the AWS Key Management Service Developer Guide.

Type: String

Valid Values: `Enabled` | `Disabled` | `PendingDeletion` | `PendingImport`

Required: No

**KeyUsage**

The cryptographic operations for which you can use the CMK. Currently the only allowed value is `ENCRYPT_DECRYPT`, which means you can use the CMK for the Encrypt (p. 46) and Decrypt (p. 20) operations.

Type: String

Valid Values: `ENCRYPT_DECRYPT`

Required: No

**Origin**

The source of the CMK's key material. When this value is `AWS_KMS`, AWS KMS created the key material. When this value is `EXTERNAL`, the key material was imported from your existing key management infrastructure or the CMK lacks key material.
Type: String

Valid Values: AWS_KMS | EXTERNAL

Required: No

ValidTo

The time at which the imported key material expires. When the key material expires, AWS KMS deletes the key material and the CMK becomes unusable. This value is present only for CMKs whose Origin is EXTERNAL and whose ExpirationModel is KEY_MATERIAL_EXPIRES, otherwise this value is omitted.

Type: Timestamp

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java
- AWS SDK for Ruby V2
Tag

A key-value pair. A tag consists of a tag key and a tag value. Tag keys and tag values are both required, but tag values can be empty (null) strings.

For information about the rules that apply to tag keys and tag values, see User-Defined Tag Restrictions in the AWS Billing and Cost Management User Guide.

Contents

**Note**

In the following list, the required parameters are described first.

**TagKey**

The key of the tag.

Type: String


Required: Yes

**TagValue**

The value of the tag.

Type: String

Length Constraints: Minimum length of 0. Maximum length of 256.

Required: Yes

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java
- AWS SDK for Ruby V2
Common Parameters

The following list contains the parameters that all actions use for signing Signature Version 4 requests with a query string. Any action-specific parameters are listed in the topic for that action. For more information about Signature Version 4, see Signature Version 4 Signing Process in the Amazon Web Services General Reference.

**Action**

The action to be performed.

*Type:* string

*Required:* Yes

**Version**

The API version that the request is written for, expressed in the format YYYY-MM-DD.

*Type:* string

*Required:* Yes

**X-Amz-Algorithm**

The hash algorithm that you used to create the request signature.

*Condition:* Specify this parameter when you include authentication information in a query string instead of in the HTTP authorization header.

*Type:* string

*Valid Values:* AWS4-HMAC-SHA256

*Required:* Conditional

**X-Amz-Credential**

The credential scope value, which is a string that includes your access key, the date, the region you are targeting, the service you are requesting, and a termination string ("aws4_request"). The value is expressed in the following format: access_key/YYYYMMDD/region/service/aws4_request.

*Condition:* Specify this parameter when you include authentication information in a query string instead of in the HTTP authorization header.

*Type:* string

*Required:* Conditional

**X-Amz-Date**

The date that is used to create the signature. The format must be ISO 8601 basic format (YYYYMMDD'T'HHMMSS'Z'). For example, the following date time is a valid X-Amz-Date value:

20120325T120000Z.

*Condition:* X-Amz-Date is optional for all requests; it can be used to override the date used for signing requests. If the Date header is specified in the ISO 8601 basic format, X-Amz-Date is
not required. When X-Amz-Date is used, it always overrides the value of the Date header. For more information, see Handling Dates in Signature Version 4 in the Amazon Web Services General Reference.

Type: string
Required: Conditional

**X-Amz-Security-Token**

The temporary security token that was obtained through a call to AWS Security Token Service (AWS STS). For a list of services that support temporary security credentials from AWS Security Token Service, go to AWS Services That Work with IAM in the IAM User Guide.

Condition: If you're using temporary security credentials from the AWS Security Token Service, you must include the security token.

Type: string
Required: Conditional

**X-Amz-Signature**

Specifies the hex-encoded signature that was calculated from the string to sign and the derived signing key.

Condition: Specify this parameter when you include authentication information in a query string instead of in the HTTP authorization header.

Type: string
Required: Conditional

**X-Amz-SignedHeaders**

Specifies all the HTTP headers that were included as part of the canonical request. For more information about specifying signed headers, see Task 1: Create a Canonical Request For Signature Version 4 in the Amazon Web Services General Reference.

Condition: Specify this parameter when you include authentication information in a query string instead of in the HTTP authorization header.

Type: string
Required: Conditional
Common Errors

This section lists the errors common to the API actions of all AWS services. For errors specific to an API action for this service, see the topic for that API action.

**AccessDeniedException**

You do not have sufficient access to perform this action.

HTTP Status Code: 400

**IncompleteSignature**

The request signature does not conform to AWS standards.

HTTP Status Code: 400

**InternalFailure**

The request processing has failed because of an unknown error, exception or failure.

HTTP Status Code: 500

**InvalidAction**

The action or operation requested is invalid. Verify that the action is typed correctly.

HTTP Status Code: 400

**InvalidClientTokenId**

The X.509 certificate or AWS access key ID provided does not exist in our records.

HTTP Status Code: 403

**InvalidParameterCombination**

Parameters that must not be used together were used together.

HTTP Status Code: 400

**InvalidParameterValue**

An invalid or out-of-range value was supplied for the input parameter.

HTTP Status Code: 400

**InvalidQueryParameter**

The AWS query string is malformed or does not adhere to AWS standards.

HTTP Status Code: 400

**MalformedQueryString**

The query string contains a syntax error.

HTTP Status Code: 404

**MissingAction**

The request is missing an action or a required parameter.

HTTP Status Code: 400
MissingAuthenticationToken

The request must contain either a valid (registered) AWS access key ID or X.509 certificate.

HTTP Status Code: 403

MissingParameter

A required parameter for the specified action is not supplied.

HTTP Status Code: 400

OptInRequired

The AWS access key ID needs a subscription for the service.

HTTP Status Code: 403

RequestExpired

The request reached the service more than 15 minutes after the date stamp on the request or more
than 15 minutes after the request expiration date (such as for pre-signed URLs), or the date stamp
on the request is more than 15 minutes in the future.

HTTP Status Code: 400

ServiceUnavailable

The request has failed due to a temporary failure of the server.

HTTP Status Code: 503

ThrottlingException

The request was denied due to request throttling.

HTTP Status Code: 400

ValidationError

The input fails to satisfy the constraints specified by an AWS service.

HTTP Status Code: 400