
AWS Certificate Manager

API Reference

API Version 2015-12-08



AWS Certificate Manager: API Reference

Copyright © 2017 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Amazon's trademarks and trade dress may not be used in connection with any product or service that is not Amazon's, in any manner that is likely to cause confusion among customers, or in any manner that disparages or discredits Amazon. All other trademarks not owned by Amazon are the property of their respective owners, who may or may not be affiliated with, connected to, or sponsored by Amazon.

Table of Contents

Welcome	1
Actions	2
AddTagsToCertificate	3
Request Syntax	3
Request Parameters	3
Response Elements	4
Errors	4
Example	4
See Also	5
DeleteCertificate	6
Request Syntax	6
Request Parameters	6
Response Elements	6
Errors	6
Example	7
See Also	7
DescribeCertificate	9
Request Syntax	9
Request Parameters	9
Response Syntax	9
Response Elements	10
Errors	10
Example	10
See Also	12
GetCertificate	13
Request Syntax	13
Request Parameters	13
Response Syntax	13
Response Elements	13
Errors	14
Example	14
See Also	16
ImportCertificate	17
Request Syntax	17
Request Parameters	17
Response Syntax	18
Response Elements	18
Errors	19
Example	19
See Also	19
ListCertificates	21
Request Syntax	21
Request Parameters	21
Response Syntax	22
Response Elements	22
Errors	22
Example	22
See Also	23
ListTagsForCertificate	24
Request Syntax	24
Request Parameters	24
Response Syntax	24
Response Elements	24
Errors	25

Example	25
See Also	25
RemoveTagsFromCertificate	27
Request Syntax	27
Request Parameters	27
Response Elements	28
Errors	28
Example	28
See Also	29
RequestCertificate	30
Request Syntax	30
Request Parameters	30
Response Syntax	31
Response Elements	31
Errors	32
Example	32
See Also	33
ResendValidationEmail	34
Request Syntax	34
Request Parameters	34
Response Elements	35
Errors	35
Example	36
See Also	36
Data Types	37
CertificateDetail	38
Contents	38
See Also	41
CertificateSummary	42
Contents	42
See Also	42
DomainValidation	43
Contents	43
See Also	43
DomainValidationOption	45
Contents	45
See Also	45
RenewalSummary	46
Contents	46
See Also	46
Tag	47
Contents	47
See Also	47
Common Parameters	48
Common Errors	50

Welcome

Welcome to the AWS Certificate Manager (ACM) API Reference. This guide provides descriptions, syntax, and usage examples for each ACM API operation.

You can use ACM to manage SSL/TLS certificates for your AWS-based websites and applications. For general information about using ACM, see the [AWS Certificate Manager User Guide](#).

Instead of using the ACM HTTP API directly, you can use one of the AWS SDKs or command line tools to interact with the ACM API. These tools are available for a variety of programming languages and platforms. For more information, see [Tools for Amazon Web Services](#).

Signing API Requests

You must sign your HTTP API requests to ACM. When you use the AWS SDKs and command line tools, they sign API requests for you. If you do not use these tools, you must calculate the signature yourself. For more information, see [Signature Version 4 Signing Process](#) in the *Amazon Web Services General Reference*. ACM requires signature version 4.

Actions

The following actions are supported:

- [AddTagsToCertificate](#) (p. 3)
- [DeleteCertificate](#) (p. 6)
- [DescribeCertificate](#) (p. 9)
- [GetCertificate](#) (p. 13)
- [ImportCertificate](#) (p. 17)
- [ListCertificates](#) (p. 21)
- [ListTagsForCertificate](#) (p. 24)
- [RemoveTagsFromCertificate](#) (p. 27)
- [RequestCertificate](#) (p. 30)
- [ResendValidationEmail](#) (p. 34)

AddTagsToCertificate

Adds one or more tags to an ACM Certificate. Tags are labels that you can use to identify and organize your AWS resources. Each tag consists of a `key` and an optional `value`. You specify the certificate on input by its Amazon Resource Name (ARN). You specify the tag by using a key-value pair.

You can apply a tag to just one certificate if you want to identify a specific characteristic of that certificate, or you can apply the same tag to multiple certificates if you want to filter for a common relationship among those certificates. Similarly, you can apply the same tag to multiple resources if you want to specify a relationship among those resources. For example, you can add the same tag to an ACM Certificate and an Elastic Load Balancing load balancer to indicate that they are both used by the same website. For more information, see [Tagging ACM Certificates](#).

To remove one or more tags, use the [RemoveTagsFromCertificate \(p. 27\)](#) action. To view all of the tags that have been applied to the certificate, use the [ListTagsForCertificate \(p. 24\)](#) action.

Request Syntax

```
{
  "CertificateArn": "string",
  "Tags": [
    {
      "Key": "string",
      "Value": "string"
    }
  ]
}
```

Request Parameters

For information about the parameters that are common to all actions, see [Common Parameters \(p. 48\)](#).

The request accepts the following data in JSON format.

Note

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

CertificateArn (p. 3)

String that contains the ARN of the ACM Certificate to which the tag is to be applied. This must be of the form:

```
arn:aws:acm:region:123456789012:certificate/12345678-1234-1234-1234-123456789012
```

For more information about ARNs, see [Amazon Resource Names \(ARNs\) and AWS Service Namespaces](#).

Type: String

Length Constraints: Minimum length of 20. Maximum length of 2048.

Pattern: `arn:[\w+=/, .@-]+:[\w+=/, .@-]+:[\w+=/, .@-]*:[0-9]+:[\w+=, .@-]+(/[\w+=/, .@-]+)*`

Required: Yes

Tags (p. 3)

The key-value pair that defines the tag. The tag value is optional.

Type: Array of [Tag \(p. 47\)](#) objects

Array Members: Minimum number of 1 item. Maximum number of 50 items.

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 \(p. 50\)](#).

InvalidArnException

The requested Amazon Resource Name (ARN) does not refer to an existing resource.

HTTP Status Code: 400

InvalidTagException

One or both of the values that make up the key-value pair is not valid. For example, you cannot specify a tag value that begins with `aws:`.

HTTP Status Code: 400

ResourceNotFoundException

The specified certificate cannot be found in the caller's account, or the caller's account cannot be found.

HTTP Status Code: 400

TooManyTagsException

The request contains too many tags. Try the request again with fewer tags.

HTTP Status Code: 400

Example

Add two tags to an ACM Certificate

Sample Request

```
POST / HTTP/1.1
Host: acm.us-east-1.amazonaws.com
X-Amz-Target: CertificateManager.AddTagsToCertificate
X-Amz-Date: 20160414T162438Z
User-Agent: aws-cli/1.10.20 Python/2.7.3 Linux/3.13.0-83-generic botocore/1.4.11
Content-Type: application/x-amz-json-1.1
Authorization: AWS4-HMAC-SHA256 Credential=AKIAI44QH8DHBEXAMPLE/20160414/us-east-1/
acm/aws4_request, SignedHeaders=content-type;host;user-agent;x-amz-date;x-amz-target,
Signature=370a583d3532f14e0cb34ea51de782e9e5138171184bfede740f5f150251fa2f

{"CertificateArn": "arn:aws:acm:us-
east-1:111122223333:certificate/12345678-1234-1234-1234-123456789012", "Tags": [{"Key":
"website", "Value": "example.com"}, {"Key": "stack", "Value": "production"}]}
```


Sample Response

```
HTTP/1.1 200 OK
x-amzn-RequestId: 640bd601-025d-11e6-baa2-cd9f4ef8cda6
Content-Type: application/x-amz-json-1.1
Content-Length: 0
Date: Thu, 14 Apr 2016 16:24:41 GMT
```

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](#)

DeleteCertificate

Deletes an ACM Certificate and its associated private key. If this action succeeds, the certificate no longer appears in the list of ACM Certificates that can be displayed by calling the [ListCertificates \(p. 21\)](#) action or be retrieved by calling the [GetCertificate \(p. 13\)](#) action. The certificate will not be available for use by other AWS services.

Note

You cannot delete an ACM Certificate that is being used by another AWS service. To delete a certificate that is in use, the certificate association must first be removed.

Request Syntax

```
{  
  "CertificateArn": "string"  
}
```

Request Parameters

For information about the parameters that are common to all actions, see [Common Parameters \(p. 48\)](#).

The request accepts the following data in JSON format.

Note

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

CertificateArn (p. 6)

String that contains the ARN of the ACM Certificate to be deleted. This must be of the form:

```
arn:aws:acm:region:123456789012:certificate/12345678-1234-1234-1234-123456789012
```

For more information about ARNs, see [Amazon Resource Names \(ARNs\) and AWS Service Namespaces](#).

Type: String

Length Constraints: Minimum length of 20. Maximum length of 2048.

Pattern: `arn:[\w+=/, .@-]+:[\w+=/, .@-]+:[\w+=/, .@-]*:[0-9]+:[\w+=, .@-]+(/[\w+=/, .@-]+)*`

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 \(p. 50\)](#).

InvalidArnException

The requested Amazon Resource Name (ARN) does not refer to an existing resource.

HTTP Status Code: 400

ResourceInUseException

The certificate is in use by another AWS service in the caller's account. Remove the association and try again.

HTTP Status Code: 400

ResourceNotFoundException

The specified certificate cannot be found in the caller's account, or the caller's account cannot be found.

HTTP Status Code: 400

Example

Delete an ACM Certificate

Sample Request

```
POST / HTTP/1.1
Host: acm.us-east-1.amazonaws.com
X-Amz-Target: CertificateManager.DeleteCertificate
X-Amz-Date: 20151222T164207Z
User-Agent: aws-cli/1.9.7 Python/2.7.3 Linux/3.13.0-73-generic botocore/1.3.7
Content-Type: application/x-amz-json-1.1
Authorization: AWS4-HMAC-SHA256 Credential=AKIAIOSFODNN7EXAMPLE/20151222/us-east-1/
acm/aws4_request, SignedHeaders=content-type;host;user-agent;x-amz-date;x-amz-target,
Signature=0b29b04bb5f1ebb5fe9e6b1cbcdeda903b4ed2e06f3abe8a092c0ed1193b4dfc

{
  "CertificateArn": "arn:aws:acm:us-
east-1:111122223333:certificate/12345678-1234-1234-1234-123456789012"
}
```

Sample Response

```
HTTP/1.1 200 OK
x-amzn-RequestId: ee2db085-a8ca-11e5-9561-b3f6248b5775
Content-Type: application/x-amz-json-1.1
Content-Length: 0
Date: Tue, 22 Dec 2015 16:42:03 GMT
```

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](#)

DescribeCertificate

Returns detailed metadata about the specified ACM Certificate.

Request Syntax

```
{  
  "CertificateArn": "string"  
}
```

Request Parameters

For information about the parameters that are common to all actions, see [Common Parameters](#) (p. 48).

The request accepts the following data in JSON format.

Note

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

CertificateArn (p. 9)

The Amazon Resource Name (ARN) of the ACM Certificate. The ARN must have the following form:

```
arn:aws:acm:region:123456789012:certificate/12345678-1234-1234-1234-123456789012
```

For more information about ARNs, see [Amazon Resource Names \(ARNs\) and AWS Service Namespaces](#).

Type: String

Length Constraints: Minimum length of 20. Maximum length of 2048.

Pattern: `arn:[\w+=/, .@-]+:[\w+=/, .@-]+:[\w+=/, .@-]*:[0-9]+:[\w+=/, .@-]+(<[/[\w+=/, .@-]+)*`

Required: Yes

Response Syntax

```
{  
  "Certificate": {  
    "CertificateArn": "string",  
    "CreatedAt": number,  
    "DomainName": "string",  
    "DomainValidationOptions": [  
      {  
        "DomainName": "string",  
        "ValidationDomain": "string",  
        "ValidationEmails": [ "string" ],  
        "ValidationStatus": "string"  
      }  
    ],  
    "FailureReason": "string",  
    "ImportedAt": number,  
    "InUseBy": [ "string" ],  
    "IssuedAt": number,  
    "Issuer": "string",  
    "KeyAlgorithm": "string",  
    "NotAfter": number,  
  }  
}
```

```
"NotBefore": number,
"RenewalSummary": {
  "DomainValidationOptions": [
    {
      "DomainName": "string",
      "ValidationDomain": "string",
      "ValidationEmails": [ "string" ],
      "ValidationStatus": "string"
    }
  ],
  "RenewalStatus": "string"
},
"RevocationReason": "string",
"RevokedAt": number,
"Serial": "string",
"SignatureAlgorithm": "string",
"Status": "string",
"Subject": "string",
"SubjectAlternativeNames": [ "string" ],
"Type": "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.

Certificate (p. 9)

Metadata about an ACM certificate.

Type: [CertificateDetail \(p. 38\)](#) object

Errors

For information about the errors that are common to all actions, see [Common Errors \(p. 50\)](#).

InvalidArnException

The requested Amazon Resource Name (ARN) does not refer to an existing resource.

HTTP Status Code: 400

ResourceNotFoundException

The specified certificate cannot be found in the caller's account, or the caller's account cannot be found.

HTTP Status Code: 400

Example

Describe an ACM Certificate

Sample Request

```
POST / HTTP/1.1
```

AWS Certificate Manager API Reference Example

```
Host: acm.us-east-1.amazonaws.com
X-Amz-Target: CertificateManager.DescribeCertificate
X-Amz-Date: 20151221T203246Z
User-Agent: aws-cli/1.9.7 Python/2.7.3 Linux/3.13.0-71-generic boto/1.3.7
Content-Type: application/x-amz-json-1.1
Authorization: AWS4-HMAC-SHA256 Credential=AKIAI44QH8DHBEXAMPLE/20151221/us-east-1/
acm/aws4_request, SignedHeaders=content-type;host;user-agent;x-amz-date;x-amz-target,
Signature=76913a7d6013d34afbdclbbd6c3e77d5edd3fa2d9883a94d946c6eeea5908d9e

{
  "CertificateArn": "arn:aws:acm:us-
east-1:111122223333:certificate/12345678-1234-1234-1234-123456789012"
}
```

Sample Response

```
HTTP/1.1 200 OK
x-amzn-RequestId: fd1e5a07-a821-11e5-845d-95c070464235
Content-Type: application/x-amz-json-1.1
Content-Length: 1035
Date: Mon, 21 Dec 2015 20:32:43 GMT

{
  "Certificate": {
    "CertificateArn": "arn:aws:acm:us-
east-1:111122223333:certificate/12345678-1234-1234-1234-123456789012",
    "CreatedAt": 1450212224.0,
    "DomainName": "example.com",
    "DomainValidationOptions": [
      {
        "DomainName": "example.com",
        "ValidationDomain": "example.com",
        "ValidationEmails": [
          "hostmaster@example.com",
          "admin@example.com",
          "admin@example.com.whoisprivacyservice.org",
          "tech@example.com.whoisprivacyservice.org",
          "owner@example.com.whoisprivacyservice.org",
          "postmaster@example.com",
          "webmaster@example.com",
          "administrator@example.com"
        ]
      }
    ],
    "DomainName": "www.example.com",
    "ValidationDomain": "www.example.com",
    "ValidationEmails": [
      "hostmaster@example.com",
      "admin@example.com",
      "admin@example.com.whoisprivacyservice.org",
      "tech@example.com.whoisprivacyservice.org",
      "owner@example.com.whoisprivacyservice.org",
      "postmaster@example.com",
      "webmaster@example.com",
      "administrator@example.com"
    ]
  },
  "InUseBy": [
    "arn:aws:cloudfront::111122223333:distribution/E12KXPQHVLVSVC"
  ],
  "IssuedAt": 1450212292.0,
  "Issuer": "Amazon",
  "KeyAlgorithm": "RSA-2048",
}
```

```
"NotAfter": 1484481600.0,  
"NotBefore": 1450137600.0,  
"Serial": "07:71:71:f4:6b:e7:bf:63:87:e6:ad:3c:b2:0f:d0:5b",  
"SignatureAlgorithm": "SHA256WITHRSA",  
"Status": "ISSUED",  
"Subject": "CN=example.com",  
"SubjectAlternativeNames": [  
  "example.com",  
  "www.example.com"  
]  
}  
}
```

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](#)

GetCertificate

Retrieves an ACM Certificate and certificate chain for the certificate specified by an ARN. The chain is an ordered list of certificates that contains the root certificate, intermediate certificates of subordinate CAs, and the ACM Certificate. The certificate and certificate chain are base64 encoded. If you want to decode the certificate chain to see the individual certificate fields, you can use OpenSSL.

Note

Currently, ACM Certificates can be used only with Elastic Load Balancing and Amazon CloudFront.

Request Syntax

```
{  
  "CertificateArn": "string"  
}
```

Request Parameters

For information about the parameters that are common to all actions, see [Common Parameters \(p. 48\)](#).

The request accepts the following data in JSON format.

Note

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

CertificateArn (p. 13)

String that contains a certificate ARN in the following format:

```
arn:aws:acm:region:123456789012:certificate/12345678-1234-1234-1234-123456789012
```

For more information about ARNs, see [Amazon Resource Names \(ARNs\) and AWS Service Namespaces](#).

Type: String

Length Constraints: Minimum length of 20. Maximum length of 2048.

Pattern: `arn:[\w+=/, .@-]+:[\w+=/, .@-]+:[\w+=/, .@-]*:[0-9]+:[\w+=, .@-]+(/[\w+=/, .@-]+)*`

Required: Yes

Response Syntax

```
{  
  "Certificate": "string",  
  "CertificateChain": "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.

Certificate (p. 13)

String that contains the ACM Certificate represented by the ARN specified at input.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 32768.

Pattern: `-{5}BEGIN CERTIFICATE-{5}\u000D?\u000A([A-Za-z0-9/+] {64}\u000D?\u000A)*[A-Za-z0-9/+] {1,64}={0,2}\u000D?\u000A-{5}END CERTIFICATE-{5}(\u000D?\u000A)?`

CertificateChain (p. 13)

The certificate chain that contains the root certificate issued by the certificate authority (CA).

Type: String

Length Constraints: Minimum length of 1. Maximum length of 2097152.

Pattern: `(-{5}BEGIN CERTIFICATE-{5}\u000D?\u000A([A-Za-z0-9/+] {64}\u000D?\u000A)*[A-Za-z0-9/+] {1,64}={0,2}\u000D?\u000A-{5}END CERTIFICATE-{5}\u000D?\u000A)*-{5}BEGIN CERTIFICATE-{5}\u000D?\u000A([A-Za-z0-9/+] {64}\u000D?\u000A)*[A-Za-z0-9/+] {1,64}={0,2}\u000D?\u000A-{5}END CERTIFICATE-{5}(\u000D?\u000A)?`

Errors

For information about the errors that are common to all actions, see [Common Errors \(p. 50\)](#).

InvalidArnException

The requested Amazon Resource Name (ARN) does not refer to an existing resource.

HTTP Status Code: 400

RequestInProgressException

The certificate request is in process and the certificate in your account has not yet been issued.

HTTP Status Code: 400

ResourceNotFoundException

The specified certificate cannot be found in the caller's account, or the caller's account cannot be found.

HTTP Status Code: 400

Example

Get an ACM Certificate

Sample Request

```
POST / HTTP/1.1
Host: acm.us-east-1.amazonaws.com
X-Amz-Target: CertificateManager.GetCertificate
X-Amz-Date: 20151221T210018Z
```

AWS Certificate Manager API Reference
Example

```
User-Agent: aws-cli/1.9.7 Python/2.7.3 Linux/3.13.0-71-generic botocore/1.3.7
Content-Type: application/x-amz-json-1.1
Authorization: AWS4-HMAC-SHA256 Credential=AKIAI44QH8DHBEXAMPLE/20151221/us-east-1/
acm/aws4_request, SignedHeaders=content-type;host;user-agent;x-amz-date;x-amz-target,
Signature=b51b4c2d5518473a8552fdab8e313c76254e9ca64e4d8ab69c2ebef83dbd459b

{
  "CertificateArn": "arn:aws:acm:us-
east-1:111122223333:certificate/12345678-1234-1234-1234-123456789012"
}
```

Sample Response

```
HTTP/1.1 200 OK
x-amzn-RequestId: d5300b5a-a825-11e5-9141-fbb8a078e3eb
Content-Type: application/x-amz-json-1.1
Content-Length: 6506
Date: Mon, 21 Dec 2015 21:00:15 GMT

{
  "Certificate":
  "-----BEGIN CERTIFICATE-----
MIICiTCcAfICcQD6m7oRw0uXOjANBgkqhkiG9w0BAQUFADCBiDELMAkGA1UEBhMC
VVMxCzAJBgNVBAGTALdBMRAdDgYDVQHEwdTZWF0dGxLMQ8wDQYDVQKewZBbWF6
b24xFDASBgNVBAsTC0lBTSBDb25zb2x1MRIwEAYDVQDEwLUZXN0Q21sYWMxHzAd
BgkqhkiG9w0BCQEWEG5vb25lQGFTYXpvi5jb20wHhcNMTEwNDI1MjA0NTIxWjcN
MTIwNDIOMjA0NTIxWjCBiDELMAkGA1UEBhMCVVMxCzAJBgNVBAGTALdBMRAdDgYD
VQHEwdTZWF0dGxLMQ8wDQYDVQKewZBbWF6b24xFDASBgNVBAsTC0lBTSBDb25z
b2x1MRIwEAYDVQDEwLUZXN0Q21sYWMxHzAdBgkqhkiG9w0BCQEWEG5vb25lQGFT
YXpvi5jb20wZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJAoGBAMaK0dn+a4GmWIWJ
21uUSfwfEvySwTc2XADZ4nB+BLyGVik60CpiwsZ3G93vUEIO3IyNoH/f0wYK8m9T
rDHudUZg3qX4waLG5M43q7Wgc/MbQITxOUSQv7c7ugFFDzQGBzZswY6786m86gpE
Ibb30hjZnczvQAaRHhdLQWIMm2nrAgMBAAEwDQYJKoZIhvcNAQEFBQADgYEAAtCu4
nUhVVxYUntneD9+h8Mg9q6q+auNKyExzyLwax1Aoo7TJHidbtS4J5iNmZgXLOFkb
FFBjvSfpJlJ00zbhNYS5f6GuoEDmFJl0ZxBHjJnyp378OD8uTs7fLvJx79LjStB
NYiytVbZPQUQ5Yaxu2jXnimvw3rrszlaEXAMPLE=
-----END CERTIFICATE-----\n",

  "CertificateChain":
  "-----BEGIN CERTIFICATE-----
MIICiTCcAfICcQD6m7oRw0uXOjANBgkqhkiG9w0BAQUFADCBiDELMAkGA1UEBhMC
VVMxCzAJBgNVBAGTALdBMRAdDgYDVQHEwdTZWF0dGxLMQ8wDQYDVQKewZBbWF6
b24xFDASBgNVBAsTC0lBTSBDb25zb2x1MRIwEAYDVQDEwLUZXN0Q21sYWMxHzAd
BgkqhkiG9w0BCQEWEG5vb25lQGFTYXpvi5jb20wHhcNMTEwNDI1MjA0NTIxWjcN
MTIwNDIOMjA0NTIxWjCBiDELMAkGA1UEBhMCVVMxCzAJBgNVBAGTALdBMRAdDgYD
VQHEwdTZWF0dGxLMQ8wDQYDVQKewZBbWF6b24xFDASBgNVBAsTC0lBTSBDb25z
b2x1MRIwEAYDVQDEwLUZXN0Q21sYWMxHzAdBgkqhkiG9w0BCQEWEG5vb25lQGFT
YXpvi5jb20wZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJAoGBAMaK0dn+a4GmWIWJ
21uUSfwfEvySwTc2XADZ4nB+BLyGVik60CpiwsZ3G93vUEIO3IyNoH/f0wYK8m9T
rDHudUZg3qX4waLG5M43q7Wgc/MbQITxOUSQv7c7ugFFDzQGBzZswY6786m86gpE
Ibb30hjZnczvQAaRHhdLQWIMm2nrAgMBAAEwDQYJKoZIhvcNAQEFBQADgYEAAtCu4
nUhVVxYUntneD9+h8Mg9q6q+auNKyExzyLwax1Aoo7TJHidbtS4J5iNmZgXLOFkb
FFBjvSfpJlJ00zbhNYS5f6GuoEDmFJl0ZxBHjJnyp378OD8uTs7fLvJx79LjStB
NYiytVbZPQUQ5Yaxu2jXnimvw3rrszlaEXAMPLE=
-----END CERTIFICATE-----\n
-----BEGIN CERTIFICATE-----
MIICiTCcAfICcQD6m7oRw0uXOjANBgkqhkiG9w0BAQUFADCBiDELMAkGA1UEBhMC
VVMxCzAJBgNVBAGTALdBMRAdDgYDVQHEwdTZWF0dGxLMQ8wDQYDVQKewZBbWF6
b24xFDASBgNVBAsTC0lBTSBDb25zb2x1MRIwEAYDVQDEwLUZXN0Q21sYWMxHzAd
BgkqhkiG9w0BCQEWEG5vb25lQGFTYXpvi5jb20wHhcNMTEwNDI1MjA0NTIxWjcN
MTIwNDIOMjA0NTIxWjCBiDELMAkGA1UEBhMCVVMxCzAJBgNVBAGTALdBMRAdDgYD
VQHEwdTZWF0dGxLMQ8wDQYDVQKewZBbWF6b24xFDASBgNVBAsTC0lBTSBDb25z
b2x1MRIwEAYDVQDEwLUZXN0Q21sYWMxHzAdBgkqhkiG9w0BCQEWEG5vb25lQGFT
YXpvi5jb20wZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJAoGBAMaK0dn+a4GmWIWJ
```

```
21uUSfwfEvySWtC2XADZ4nB+BLYgVIk60CpiwsZ3G93vUEIO3IyNoH/f0wYK8m9T
rDHudUZg3qX4waLG5M43q7Wgc/MbQITxOUSQv7c7ugFFDzQGBzZswY6786m86gpE
Ibb3OhjZnzcVQAaRHhdlQWIMm2nrAgMBAAEwDQYJKoZIhvcNAQEFBQADgYEAtCu4
nUhVVxYUntneD9+h8Mg9q6q+auNKyExzyLwaxLAoo7TJHidbtS4J5iNmZgXLOFkb
FFBjvSfpJlJ00zbhNYS5f6GuoEDmFJl0ZxBHjJnyp378OD8uTs7fLvJx79LjSTb
NYiytVbZPQUQ5Yaxu2jXnimvw3rrszlaEXAMPLE=
-----END CERTIFICATE-----\n
-----BEGIN CERTIFICATE-----
MIICiTCcAfICCD6m7oRw0uXOjANBgkqhkiG9w0BAQUFADCBiDELMAkGA1UEBhMC
VVMxCzAJBgNVBAGTAldBMRAwDgYDVOQHEwdTZWF0dGx1MQ8wDQYDVOQKEwZBbWF6
b24xFDASBgNVBASTC0lBTsBDb25zb2x1MRIwEAYDVOQDEwLUZXNOQ2lsYWMxHZAAd
BgkqhkiG9w0BCQEWEG5vb25lQGFTYXpvi5jb20wHhcNMTEwNDI1MjAONTIxWhcN
MTIwNDIOMjAONTIxwJCBiDELMAkGA1UEBhMCVVMxCzAJBgNVBAGTAldBMRAwDgYD
VOQHEwdTZWF0dGx1MQ8wDQYDVOQKEwZBbWF6b24xFDASBgNVBASTC0lBTsBDb25z
b2x1MRIwEAYDVOQDEwLUZXNOQ2lsYWMxHZAAdBgkqhkiG9w0BCQEWEG5vb25lQGFT
YXpvi5jb20wZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJAoGBAMaK0dn+a4GmWIWJ
21uUSfwfEvySWtC2XADZ4nB+BLYgVIk60CpiwsZ3G93vUEIO3IyNoH/f0wYK8m9T
rDHudUZg3qX4waLG5M43q7Wgc/MbQITxOUSQv7c7ugFFDzQGBzZswY6786m86gpE
Ibb3OhjZnzcVQAaRHhdlQWIMm2nrAgMBAAEwDQYJKoZIhvcNAQEFBQADgYEAtCu4
nUhVVxYUntneD9+h8Mg9q6q+auNKyExzyLwaxLAoo7TJHidbtS4J5iNmZgXLOFkb
FFBjvSfpJlJ00zbhNYS5f6GuoEDmFJl0ZxBHjJnyp378OD8uTs7fLvJx79LjSTb
NYiytVbZPQUQ5Yaxu2jXnimvw3rrszlaEXAMPLE=
-----END CERTIFICATE-----"
}
```

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](#)

ImportCertificate

Imports an SSL/TLS certificate into AWS Certificate Manager (ACM) to use with [ACM's integrated AWS services](#).

Note

ACM does not provide [managed renewal](#) for certificates that you import.

For more information about importing certificates into ACM, including the differences between certificates that you import and those that ACM provides, see [Importing Certificates](#) in the *AWS Certificate Manager User Guide*.

To import a certificate, you must provide the certificate and the matching private key. When the certificate is not self-signed, you must also provide a certificate chain. You can omit the certificate chain when importing a self-signed certificate.

The certificate, private key, and certificate chain must be PEM-encoded. For more information about converting these items to PEM format, see [Importing Certificates Troubleshooting](#) in the *AWS Certificate Manager User Guide*.

To import a new certificate, omit the `certificateArn` field. Include this field only when you want to replace a previously imported certificate.

This operation returns the [Amazon Resource Name \(ARN\)](#) of the imported certificate.

Request Syntax

```
{
  "Certificate": blob,
  "CertificateArn": "string",
  "CertificateChain": blob,
  "PrivateKey": blob
}
```

Request Parameters

For information about the parameters that are common to all actions, see [Common Parameters \(p. 48\)](#).

The request accepts the following data in JSON format.

Note

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

[Certificate \(p. 17\)](#)

The certificate to import. It must meet the following requirements:

- Must be PEM-encoded.
- Must contain a 1024-bit or 2048-bit RSA public key.
- Must be valid at the time of import. You cannot import a certificate before its validity period begins (the certificate's `NotBefore` date) or after it expires (the certificate's `NotAfter` date).

Type: Base64-encoded binary data object

Length Constraints: Minimum length of 1. Maximum length of 32768.

Required: Yes

PrivateKey (p. 17)

The private key that matches the public key in the certificate. It must meet the following requirements:

- Must be PEM-encoded.
- Must be unencrypted. You cannot import a private key that is protected by a password or passphrase.

Type: Base64-encoded binary data object

Length Constraints: Minimum length of 1. Maximum length of 524288.

Required: Yes

CertificateArn (p. 17)

The [Amazon Resource Name \(ARN\)](#) of an imported certificate to replace. To import a new certificate, omit this field.

Type: String

Length Constraints: Minimum length of 20. Maximum length of 2048.

Pattern: `arn:[\w+=/, .@-]+:[\w+=/, .@-]+:[\w+=/, .@-]*:[0-9]+:[\w+=, .@-]+(</[\w+=/, .@-]+)*`

Required: No

CertificateChain (p. 17)

The certificate chain. It must be PEM-encoded.

Type: Base64-encoded binary data object

Length Constraints: Minimum length of 1. Maximum length of 2097152.

Required: No

Response Syntax

```
{  
  "CertificateArn": "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.

CertificateArn (p. 18)

The [Amazon Resource Name \(ARN\)](#) of the imported certificate.

Type: String

Length Constraints: Minimum length of 20. Maximum length of 2048.

Pattern: `arn:[\w+=/, .@-]+:[\w+=/, .@-]+:[\w+=/, .@-]*:[0-9]+:[\w+=, .@-]+(</[\w+=/, .@-]+)*`

Errors

For information about the errors that are common to all actions, see [Common Errors \(p. 50\)](#).

LimitExceededException

An ACM limit has been exceeded. For example, you may have input more domains than are allowed or you've requested too many certificates for your account. See the exception message returned by ACM to determine which limit you have violated. For more information about ACM limits, see the [Limits](#) topic.

HTTP Status Code: 400

ResourceNotFoundException

The specified certificate cannot be found in the caller's account, or the caller's account cannot be found.

HTTP Status Code: 400

Example

Import a certificate

Sample Request

```
POST / HTTP/1.1
Host: acm.us-east-1.amazonaws.com
X-Amz-Target: CertificateManager.ImportCertificate
X-Amz-Date: 20161011T184744Z
Content-Type: application/x-amz-json-1.1
Authorization: AWS4-HMAC-SHA256\
  Credential=AKIAI44QH8DHBEXAMPLE/20161011/us-east-1/acm/aws4_request,\
  SignedHeaders=content-type;host;x-amz-date;x-amz-target,\
  Signature=60f965247476c4672c498c24ba255e52a62a7e4bd8678d8ee788af5ffe42f377

{
  "CertificateChain": "Base64-encoded blob",
  "PrivateKey": "Base64-encoded blob",
  "Certificate": "Base64-encoded blob"
}
```

Sample Response

```
HTTP/1.1 200 OK
x-amzn-RequestId: 32f9ab0a-8fe3-11e6-8d69-c91606b24a3f
Content-Type: application/x-amz-json-1.1
Content-Length: 104
Date: Tue, 11 Oct 2016 18:47:46 GMT

{"CertificateArn": "arn:aws:acm:us-east-1:111122223333:certificate/91228a40-ad89-4ce0-9f6c-07009fc8fdfb"}
```

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](#)

ListCertificates

Retrieves a list of ACM Certificates and the domain name for each. You can optionally filter the list to return only the certificates that match the specified status.

Request Syntax

```
{
  "CertificateStatuses": [ "string" ],
  "MaxItems": number,
  "NextToken": "string"
}
```

Request Parameters

For information about the parameters that are common to all actions, see [Common Parameters \(p. 48\)](#).

The request accepts the following data in JSON format.

Note

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

CertificateStatuses (p. 21)

The status or statuses on which to filter the list of ACM Certificates.

Type: Array of strings

Valid Values: PENDING_VALIDATION | ISSUED | INACTIVE | EXPIRED | VALIDATION_TIMED_OUT | REVOKED | FAILED

Required: No

MaxItems (p. 21)

Use this parameter when paginating results to specify the maximum number of items to return in the response. If additional items exist beyond the number you specify, the `NextToken` element is sent in the response. Use this `NextToken` value in a subsequent request to retrieve additional items.

Type: Integer

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

Required: No

NextToken (p. 21)

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

Type: String

Length Constraints: Minimum length of 1. Maximum length of 320.

Pattern: `[\u0009\u000A\u000D\u0020-\u00FF]*`

Required: No

Response Syntax

```
{
  "CertificateSummaryList": [
    {
      "CertificateArn": "string",
      "DomainName": "string"
    }
  ],
  "NextToken": "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.

CertificateSummaryList (p. 22)

A list of ACM Certificates.

Type: Array of [CertificateSummary](#) (p. 42) objects

NextToken (p. 22)

When the list is truncated, this value is present and contains the value to use for the `NextToken` parameter in a subsequent pagination request.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 320.

Pattern: [`\u0009\u000A\u000D\u0020-\u00FF`]*

Errors

For information about the errors that are common to all actions, see [Common Errors](#) (p. 50).

Example

List Certificates

Sample Request

```
POST / HTTP/1.1
Host: acm.us-east-1.amazonaws.com
Content-Length: 2
X-Amz-Target: CertificateManager.ListCertificates
X-Amz-Date: 20160602T185849Z
Content-Type: application/x-amz-json-1.1
Authorization: AWS4-HMAC-SHA256\
  Credential=AKIAI44QH8DHBEXAMPLE/20160602/us-east-1/acm/aws4_request,\
  SignedHeaders=content-type;host;x-amz-date;x-amz-target,\
  Signature=13cfab2fbac91594da31999325c8a64da70a053a731fd237501bfbc10a24e311
```

```
{}
```

Sample Response

```
HTTP/1.1 200 OK
x-amzn-RequestId: 0be6b8db-28f4-11e6-87c4-d92106aa4389
Content-Type: application/x-amz-json-1.1
Date: Thu, 02 Jun 2016 18:58:51 GMT

{"CertificateSummaryList": [
  {
    "CertificateArn": "arn:aws:acm:us-
east-1:111122223333:certificate/12345678-1234-1234-1234-123456789012",
    "DomainName": "www.example.com"
  },
  {
    "CertificateArn": "arn:aws:acm:us-
east-1:111122223333:certificate/87654321-5678-5678-5678-210987654321",
    "DomainName": "www.example.net"
  }
]}
```

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](#)

ListTagsForCertificate

Lists the tags that have been applied to the ACM Certificate. Use the certificate's Amazon Resource Name (ARN) to specify the certificate. To add a tag to an ACM Certificate, use the [AddTagsToCertificate](#) (p. 3) action. To delete a tag, use the [RemoveTagsFromCertificate](#) (p. 27) action.

Request Syntax

```
{  
  "CertificateArn": "string"  
}
```

Request Parameters

For information about the parameters that are common to all actions, see [Common Parameters](#) (p. 48).

The request accepts the following data in JSON format.

Note

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

CertificateArn (p. 24)

String that contains the ARN of the ACM Certificate for which you want to list the tags. This has the following form:

```
arn:aws:acm:region:123456789012:certificate/12345678-1234-1234-1234-123456789012
```

For more information about ARNs, see [Amazon Resource Names \(ARNs\) and AWS Service Namespaces](#).

Type: String

Length Constraints: Minimum length of 20. Maximum length of 2048.

Pattern: `arn:[\w+=/, .@-]+:[\w+=/, .@-]+:[\w+=/, .@-]*:[0-9]+:[\w+=, .@-]+(/[\w+=/, .@-]+)*`

Required: Yes

Response Syntax

```
{  
  "Tags": [  
    {  
      "Key": "string",  
      "Value": "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.

Tags (p. 24)

The key-value pairs that define the applied tags.

Type: Array of [Tag \(p. 47\)](#) objects

Array Members: Minimum number of 1 item. Maximum number of 50 items.

Errors

For information about the errors that are common to all actions, see [Common Errors \(p. 50\)](#).

InvalidArnException

The requested Amazon Resource Name (ARN) does not refer to an existing resource.

HTTP Status Code: 400

ResourceNotFoundException

The specified certificate cannot be found in the caller's account, or the caller's account cannot be found.

HTTP Status Code: 400

Example

List tags for an ACM Certificate

Sample Request

```
POST / HTTP/1.1
Host: acm.us-east-1.amazonaws.com
X-Amz-Target: CertificateManager.ListTagsForCertificate
X-Amz-Date: 20160414T162913Z
User-Agent: aws-cli/1.10.20 Python/2.7.3 Linux/3.13.0-83-generic botocore/1.4.11
Content-Type: application/x-amz-json-1.1
Authorization: AWS4-HMAC-SHA256 Credential=AKIAI44QH8DHBEXAMPLE/20160414/us-east-1/
acm/aws4_request, SignedHeaders=content-type;host;user-agent;x-amz-date;x-amz-target,
Signature=c1b80f2b1b6c73c39e1a9594e621648e673b1419101809239b9a5dd8c397953a

{"CertificateArn": "arn:aws:acm:us-
east-1:111122223333:certificate/12345678-1234-1234-1234-123456789012"}
```

Sample Response

```
HTTP/1.1 200 OK
x-amzn-RequestId: 07c10419-025e-11e6-baa2-cd9f4ef8cda6
Content-Type: application/x-amz-json-1.1
Content-Length: 87
Date: Thu, 14 Apr 2016 16:29:16 GMT

{"Tags": [{"Key": "stack", "Value": "production"}, {"Key": "website", "Value": "example.com"}]}
```

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](#)

RemoveTagsFromCertificate

Remove one or more tags from an ACM Certificate. A tag consists of a key-value pair. If you do not specify the value portion of the tag when calling this function, the tag will be removed regardless of value. If you specify a value, the tag is removed only if it is associated with the specified value.

To add tags to a certificate, use the [AddTagsToCertificate \(p. 3\)](#) action. To view all of the tags that have been applied to a specific ACM Certificate, use the [ListTagsForCertificate \(p. 24\)](#) action.

Request Syntax

```
{
  "CertificateArn": "string",
  "Tags": [
    {
      "Key": "string",
      "Value": "string"
    }
  ]
}
```

Request Parameters

For information about the parameters that are common to all actions, see [Common Parameters \(p. 48\)](#).

The request accepts the following data in JSON format.

Note

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

CertificateArn (p. 27)

String that contains the ARN of the ACM Certificate with one or more tags that you want to remove. This must be of the form:

```
arn:aws:acm:region:123456789012:certificate/12345678-1234-1234-1234-123456789012
```

For more information about ARNs, see [Amazon Resource Names \(ARNs\) and AWS Service Namespaces](#).

Type: String

Length Constraints: Minimum length of 20. Maximum length of 2048.

Pattern: `arn:[\w+=/, .@-]+:[\w+=/, .@-]+:[\w+=/, .@-]*:[0-9]+:[\w+=, .@-]+(/[\w+=/, .@-]+)*`

Required: Yes

Tags (p. 27)

The key-value pair that defines the tag to remove.

Type: Array of [Tag \(p. 47\)](#) objects

Array Members: Minimum number of 1 item. Maximum number of 50 items.

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 \(p. 50\)](#).

InvalidArnException

The requested Amazon Resource Name (ARN) does not refer to an existing resource.

HTTP Status Code: 400

InvalidTagException

One or both of the values that make up the key-value pair is not valid. For example, you cannot specify a tag value that begins with `aws:`.

HTTP Status Code: 400

ResourceNotFoundException

The specified certificate cannot be found in the caller's account, or the caller's account cannot be found.

HTTP Status Code: 400

Example

Remove two tags from an ACM Certificate

Sample Request

```
POST / HTTP/1.1
Host: acm.us-east-1.amazonaws.com
X-Amz-Target: CertificateManager.RemoveTagsFromCertificate
X-Amz-Date: 20160414T163042Z
User-Agent: aws-cli/1.10.20 Python/2.7.3 Linux/3.13.0-83-generic botocore/1.4.11
Content-Type: application/x-amz-json-1.1
Authorization: AWS4-HMAC-SHA256 Credential=AKIAI44QH8DHBEXAMPLE/20160414/us-east-1/
acm/aws4_request, SignedHeaders=content-type;host;user-agent;x-amz-date;x-amz-target,
Signature=379429306c5e89b9b4be5b35e29c26cc1da38215d8055a5ed0bdda57bcc881cc

{"CertificateArn": "arn:aws:acm:us-
east-1:111122223333:certificate/12345678-1234-1234-1234-123456789012", "Tags": [{"Key":
"website", "Value": "example.com"}, {"Key": "stack", "Value": "production"}]}
```

Sample Response

```
HTTP/1.1 200 OK
x-amzn-RequestId: 3c8d676d-025e-11e6-8823-93164b47113c
Content-Type: application/x-amz-json-1.1
Content-Length: 0
Date: Thu, 14 Apr 2016 16:30:44 GMT
```


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](#)

RequestCertificate

Requests an ACM Certificate for use with other AWS services. To request an ACM Certificate, you must specify the fully qualified domain name (FQDN) for your site. You can also specify additional FQDNs if users can reach your site by using other names. For each domain name you specify, email is sent to the domain owner to request approval to issue the certificate. After receiving approval from the domain owner, the ACM Certificate is issued. For more information, see the [AWS Certificate Manager User Guide](#).

Request Syntax

```
{
  "DomainName": "string",
  "DomainValidationOptions": [
    {
      "DomainName": "string",
      "ValidationDomain": "string"
    }
  ],
  "IdempotencyToken": "string",
  "SubjectAlternativeNames": [ "string" ]
}
```

Request Parameters

For information about the parameters that are common to all actions, see [Common Parameters](#) (p. 48).

The request accepts the following data in JSON format.

Note

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

DomainName (p. 30)

Fully qualified domain name (FQDN), such as `www.example.com`, of the site that you want to secure with an ACM Certificate. Use an asterisk (*) to create a wildcard certificate that protects several sites in the same domain. For example, `*.example.com` protects `www.example.com`, `site.example.com`, and `images.example.com`.

The maximum length of a DNS name is 253 octets. The name is made up of multiple labels separated by periods. No label can be longer than 63 octets. Consider the following examples:

`(63 octets).(63 octets).(63 octets).(61 octets)` is legal because the total length is 253 octets ($63+1+63+1+63+1+61$) and no label exceeds 63 octets.

`(64 octets).(63 octets).(63 octets).(61 octets)` is not legal because the total length exceeds 253 octets ($64+1+63+1+63+1+61$) and the first label exceeds 63 octets.

`(63 octets).(63 octets).(63 octets).(62 octets)` is not legal because the total length of the DNS name ($63+1+63+1+63+1+62$) exceeds 253 octets.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 253.

Pattern: `^(*\.\.)?(((?!-)[A-Za-z0-9-]{0,62}[A-Za-z0-9])\.)+((?!-)[A-Za-z0-9-]{1,62}[A-Za-z0-9])$`

Required: Yes

[DomainValidationOptions \(p. 30\)](#)

The domain name that you want ACM to use to send you emails to validate your ownership of the domain.

Type: Array of [DomainValidationOption \(p. 45\)](#) objects

Array Members: Minimum number of 1 item. Maximum number of 100 items.

Required: No

[IdempotencyToken \(p. 30\)](#)

Customer chosen string that can be used to distinguish between calls to `RequestCertificate`. Idempotency tokens time out after one hour. Therefore, if you call `RequestCertificate` multiple times with the same idempotency token within one hour, ACM recognizes that you are requesting only one certificate and will issue only one. If you change the idempotency token for each call, ACM recognizes that you are requesting multiple certificates.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 32.

Pattern: `\w+`

Required: No

[SubjectAlternativeNames \(p. 30\)](#)

Additional FQDNs to be included in the Subject Alternative Name extension of the ACM Certificate. For example, add the name `www.example.net` to a certificate for which the `DomainName` field is `www.example.com` if users can reach your site by using either name.

Type: Array of strings

Array Members: Minimum number of 1 item. Maximum number of 100 items.

Length Constraints: Minimum length of 1. Maximum length of 253.

Pattern: `^(*\.\.?)?(((?!-)[A-Za-z0-9-]{0,62}[A-Za-z0-9])\.\.)*((?!-)[A-Za-z0-9-]{1,62}[A-Za-z0-9])$`

Required: No

Response Syntax

```
{
  "CertificateArn": "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.

[CertificateArn \(p. 31\)](#)

String that contains the ARN of the issued certificate. This must be of the form:

```
arn:aws:acm:us-east-1:123456789012:certificate/12345678-1234-1234-1234-123456789012
```

Type: String

Length Constraints: Minimum length of 20. Maximum length of 2048.

Pattern: `arn:[\w+=/, .@-]+:[\w+=/, .@-]+:[\w+=/, .@-]*:[0-9]+:[\w+=/, .@-]+(/[\w+=/, .@-]+)*`

Errors

For information about the errors that are common to all actions, see [Common Errors \(p. 50\)](#).

InvalidDomainValidationOptionsException

One or more values in the [DomainValidationOption \(p. 45\)](#) structure is incorrect.

HTTP Status Code: 400

LimitExceededException

An ACM limit has been exceeded. For example, you may have input more domains than are allowed or you've requested too many certificates for your account. See the exception message returned by ACM to determine which limit you have violated. For more information about ACM limits, see the [Limits](#) topic.

HTTP Status Code: 400

Example

Request an ACM Certificate

Sample Request

```
POST / HTTP/1.1
Host: acm.us-east-1.amazonaws.com
Accept-Encoding: identity
Content-Length: 75
X-Amz-Target: CertificateManager.RequestCertificate
X-Amz-Date: 20151222T165732Z
User-Agent: aws-cli/1.9.7 Python/2.7.3 Linux/3.13.0-73-generic botocore/1.3.7
Content-Type: application/x-amz-json-1.1
Authorization: AWS4-HMAC-SHA256 Credential=AKIAIOSFODNN7EXAMPLE/20151222/us-east-1/
acm/aws4_request, SignedHeaders=content-type;host;user-agent;x-amz-date;x-amz-target,
Signature=dbba4b1fa1199c011c0b781b94c97b14cbe75fa64dc6424232c903798d2a83b5

{
  "SubjectAlternativeNames": ["example.com"],
  "DomainName": "www.example.com"
}
```

Sample Response

```
HTTP/1.1 200 OK
x-amzn-RequestId: 15320637-a8cd-11e5-9141-fbb8a078e3eb
Content-Type: application/x-amz-json-1.1
Content-Length: 104
Date: Tue, 22 Dec 2015 16:57:28 GMT
```

```
{  
  "CertificateArn": "arn:aws:acm:us-east-1:493619779192:certificate/1ad574bd-eeb0-466e-  
b961-74ec8b405093"  
}
```

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](#)

ResendValidationEmail

Resends the email that requests domain ownership validation. The domain owner or an authorized representative must approve the ACM Certificate before it can be issued. The certificate can be approved by clicking a link in the mail to navigate to the Amazon certificate approval website and then clicking **I Approve**. However, the validation email can be blocked by spam filters. Therefore, if you do not receive the original mail, you can request that the mail be resent within 72 hours of requesting the ACM Certificate. If more than 72 hours have elapsed since your original request or since your last attempt to resend validation mail, you must request a new certificate. For more information about setting up your contact email addresses, see [Configure Email for your Domain](#).

Request Syntax

```
{
  "CertificateArn": "string",
  "Domain": "string",
  "ValidationDomain": "string"
}
```

Request Parameters

For information about the parameters that are common to all actions, see [Common Parameters \(p. 48\)](#).

The request accepts the following data in JSON format.

Note

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

CertificateArn (p. 34)

String that contains the ARN of the requested certificate. The certificate ARN is generated and returned by the [RequestCertificate \(p. 30\)](#) action as soon as the request is made. By default, using this parameter causes email to be sent to all top-level domains you specified in the certificate request.

The ARN must be of the form:

```
arn:aws:acm:us-east-1:123456789012:certificate/12345678-1234-1234-1234-123456789012
```

Type: String

Length Constraints: Minimum length of 20. Maximum length of 2048.

Pattern: `arn:[\w+=/, .@-]+:[\w+=/, .@-]+:[\w+=/, .@-]*:[0-9]+:[\w+=, .@-]+(</[\w+=/, .@-]+)*`

Required: Yes

Domain (p. 34)

The fully qualified domain name (FQDN) of the certificate that needs to be validated.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 253.

Pattern: `^(*\.\.?)?(((?!-)[A-Za-z0-9-]{0,62}[A-Za-z0-9])\.\.)(?!-)[A-Za-z0-9-]{1,62}[A-Za-z0-9])$`

Required: Yes

ValidationDomain (p. 34)

The base validation domain that will act as the suffix of the email addresses that are used to send the emails. This must be the same as the `Domain` value or a superdomain of the `Domain` value. For example, if you requested a certificate for `site.subdomain.example.com` and specify a **ValidationDomain** of `subdomain.example.com`, ACM sends email to the domain registrant, technical contact, and administrative contact in WHOIS and the following five addresses:

- `admin@subdomain.example.com`
- `administrator@subdomain.example.com`
- `hostmaster@subdomain.example.com`
- `postmaster@subdomain.example.com`
- `webmaster@subdomain.example.com`

Type: String

Length Constraints: Minimum length of 1. Maximum length of 253.

Pattern: `^(*\.\.?)?(((?!-)[A-Za-z0-9-]{0,62}[A-Za-z0-9])\.\.)+(?!-)[A-Za-z0-9-]{1,62}[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. 50).

InvalidArnException

The requested Amazon Resource Name (ARN) does not refer to an existing resource.

HTTP Status Code: 400

InvalidDomainValidationOptionsException

One or more values in the [DomainValidationOption](#) (p. 45) structure is incorrect.

HTTP Status Code: 400

InvalidStateException

Processing has reached an invalid state. For example, this exception can occur if the specified domain is not using email validation, or the current certificate status does not permit the requested operation. See the exception message returned by ACM to determine which state is not valid.

HTTP Status Code: 400

ResourceNotFoundException

The specified certificate cannot be found in the caller's account, or the caller's account cannot be found.

HTTP Status Code: 400

Example

Resend Validation Email

Sample Request

```
POST / HTTP/1.1
Host: acm.us-east-1.amazonaws.com
Accept-Encoding: identity
Content-Length: 167
X-Amz-Target: CertificateManager.ResendValidationEmail
X-Amz-Date: 20151222T170722Z
User-Agent: aws-cli/1.9.7 Python/2.7.3 Linux/3.13.0-73-generic boto/1.3.7
Content-Type: application/x-amz-json-1.1
Authorization: AWS4-HMAC-SHA256 Credential=AKIAIOSFODNN7EXAMPLE/20151222/us-east-1/
acm/aws_request, SignedHeaders=content-type;host;user-agent;x-amz-date;x-amz-target,
Signature=7ec7e70cd614724945545b22bc28296f77803d0c2524573d41c994668f07f435

{
  "CertificateArn": "arn:aws:acm:us-
east-1:111122223333 :certificate/12345678-1234-1234-1234-1234567890912",
  "Domain": "www.example.com",
  "ValidationDomain": "example.com"
}
```

Sample Response

```
HTTP/1.1 200 OK
x-amzn-RequestId: 74bada6d-a8ce-11e5-82ad-d565a2aaa0b3
Content-Type: application/x-amz-json-1.1
Content-Length: 0
Date: Tue, 22 Dec 2015 17:07:18 GMT
```

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 Certificate Manager 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:

- [CertificateDetail](#) (p. 38)
- [CertificateSummary](#) (p. 42)
- [DomainValidation](#) (p. 43)
- [DomainValidationOption](#) (p. 45)
- [RenewalSummary](#) (p. 46)
- [Tag](#) (p. 47)

CertificateDetail

Contains metadata about an ACM certificate. This structure is returned in the response to a [DescribeCertificate \(p. 9\)](#) request.

Contents

Note

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

CertificateArn

The Amazon Resource Name (ARN) of the certificate. For more information about ARNs, see [Amazon Resource Names \(ARNs\) and AWS Service Namespaces](#) in the *AWS General Reference*.

Type: String

Length Constraints: Minimum length of 20. Maximum length of 2048.

Pattern: `arn:[\w+=/, .@-]+:[\w+=/, .@-]+:[\w+=/, .@-]*:[0-9]+:[\w+=, .@-]+(<[/[\w+=/, .@-]+>)*`

Required: No

CreatedAt

The time at which the certificate was requested. This value exists only when the certificate type is `AMAZON_ISSUED`.

Type: Timestamp

Required: No

DomainName

The fully qualified domain name for the certificate, such as `www.example.com` or `example.com`.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 253.

Pattern: `^(*\.\.?)?(((?!-)[A-Za-z0-9-]{0,62}[A-Za-z0-9])\.\.)(?!-)[A-Za-z0-9-]{1,62}[A-Za-z0-9])$`

Required: No

DomainValidationOptions

Contains information about the initial validation of each domain name that occurs as a result of the [RequestCertificate \(p. 30\)](#) request. This field exists only when the certificate type is `AMAZON_ISSUED`.

Type: Array of [DomainValidation \(p. 43\)](#) objects

Array Members: Minimum number of 1 item. Maximum number of 1000 items.

Required: No

FailureReason

The reason the certificate request failed. This value exists only when the certificate status is `FAILED`. For more information, see [Certificate Request Failed](#) in the *AWS Certificate Manager User Guide*.

Type: String

Valid Values: NO_AVAILABLE_CONTACTS | ADDITIONAL_VERIFICATION_REQUIRED | DOMAIN_NOT_ALLOWED | INVALID_PUBLIC_DOMAIN | OTHER

Required: No

ImportedAt

The date and time at which the certificate was imported. This value exists only when the certificate type is `IMPORTED`.

Type: Timestamp

Required: No

InUseBy

A list of ARNs for the AWS resources that are using the certificate. A certificate can be used by multiple AWS resources.

Type: Array of strings

Required: No

IssuedAt

The time at which the certificate was issued. This value exists only when the certificate type is `AMAZON_ISSUED`.

Type: Timestamp

Required: No

Issuer

The name of the certificate authority that issued and signed the certificate.

Type: String

Required: No

KeyAlgorithm

The algorithm that was used to generate the key pair (the public and private key).

Type: String

Valid Values: `RSA_2048` | `RSA_1024` | `EC_prime256v1`

Required: No

NotAfter

The time after which the certificate is not valid.

Type: Timestamp

Required: No

NotBefore

The time before which the certificate is not valid.

Type: Timestamp

Required: No

RenewalSummary

Contains information about the status of ACM's [managed renewal](#) for the certificate. This field exists only when the certificate type is `AMAZON_ISSUED`.

Type: [RenewalSummary \(p. 46\)](#) object

Required: No

RevocationReason

The reason the certificate was revoked. This value exists only when the certificate status is `REVOKED`.

Type: String

Valid Values: `UNSPECIFIED` | `KEY_COMPROMISE` | `CA_COMPROMISE` | `AFFILIATION_CHANGED` | `SUPERCEDED` | `CESSATION_OF_OPERATION` | `CERTIFICATE_HOLD` | `REMOVE_FROM_CRL` | `PRIVILEGE_WITHDRAWN` | `A_A_COMPROMISE`

Required: No

RevokedAt

The time at which the certificate was revoked. This value exists only when the certificate status is `REVOKED`.

Type: Timestamp

Required: No

Serial

The serial number of the certificate.

Type: String

Required: No

SignatureAlgorithm

The algorithm that was used to sign the certificate.

Type: String

Required: No

Status

The status of the certificate.

Type: String

Valid Values: `PENDING_VALIDATION` | `ISSUED` | `INACTIVE` | `EXPIRED` | `VALIDATION_TIMED_OUT` | `REVOKED` | `FAILED`

Required: No

Subject

The name of the entity that is associated with the public key contained in the certificate.

Type: String

Required: No

SubjectAlternativeNames

One or more domain names (subject alternative names) included in the certificate. This list contains the domain names that are bound to the public key that is contained in the certificate. The subject alternative names include the canonical domain name (CN) of the certificate and additional domain names that can be used to connect to the website.

Type: Array of strings

Array Members: Minimum number of 1 item. Maximum number of 100 items.

Length Constraints: Minimum length of 1. Maximum length of 253.

Pattern: `^(*\.\.?)?(((?!-)[A-Za-z0-9-]{0,62}[A-Za-z0-9])\.\.)*((?!-)[A-Za-z0-9-]{1,62}[A-Za-z0-9])$`

Required: No

Type

The source of the certificate. For certificates provided by ACM, this value is `AMAZON_ISSUED`. For certificates that you imported with [ImportCertificate \(p. 17\)](#), this value is `IMPORTED`. ACM does not provide [managed renewal](#) for imported certificates. For more information about the differences between certificates that you import and those that ACM provides, see [Importing Certificates](#) in the *AWS Certificate Manager User Guide*.

Type: String

Valid Values: `IMPORTED` | `AMAZON_ISSUED`

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](#)

CertificateSummary

This structure is returned in the response object of [ListCertificates \(p. 21\)](#) action.

Contents

Note

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

CertificateArn

Amazon Resource Name (ARN) of the certificate. This is of the form:

```
arn:aws:acm:region:123456789012:certificate/12345678-1234-1234-1234-123456789012
```

For more information about ARNs, see [Amazon Resource Names \(ARNs\) and AWS Service Namespaces](#).

Type: String

Length Constraints: Minimum length of 20. Maximum length of 2048.

Pattern: `arn:[\w+=/, .@-]+:[\w+=/, .@-]+:[\w+=/, .@-]*:[0-9]+:[\w+=, .@-]+(/[\w+=/, .@-]+)*`

Required: No

DomainName

Fully qualified domain name (FQDN), such as `www.example.com` or `example.com`, for the certificate.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 253.

Pattern: `^(*\.\.?)?(((?!-)[A-Za-z0-9-]{0,62}[A-Za-z0-9])\.)+((?!-)[A-Za-z0-9-]{1,62}[A-Za-z0-9])$`

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](#)

DomainValidation

Contains information about the validation of each domain name in the certificate.

Contents

Note

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

DomainName

A fully qualified domain name (FQDN) in the certificate. For example, `www.example.com` or `example.com`.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 253.

Pattern: `^(*\.\.?)?(((?!-)[A-Za-z0-9-]{0,62}[A-Za-z0-9])\.\.)*((?!-)[A-Za-z0-9-]{1,62}[A-Za-z0-9])$`

Required: Yes

ValidationDomain

The domain name that ACM used to send domain validation emails.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 253.

Pattern: `^(*\.\.?)?(((?!-)[A-Za-z0-9-]{0,62}[A-Za-z0-9])\.\.)*((?!-)[A-Za-z0-9-]{1,62}[A-Za-z0-9])$`

Required: No

ValidationEmails

A list of email addresses that ACM used to send domain validation emails.

Type: Array of strings

Required: No

ValidationStatus

The validation status of the domain name.

Type: String

Valid Values: `PENDING_VALIDATION` | `SUCCESS` | `FAILED`

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](#)

DomainValidationOption

Contains information about the domain names that you want ACM to use to send you emails to validate your ownership of the domain.

Contents

Note

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

DomainName

A fully qualified domain name (FQDN) in the certificate request.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 253.

Pattern: `^(*\.\.?)?(((?!-)[A-Za-z0-9-]{0,62}[A-Za-z0-9])\.)+((?!-)[A-Za-z0-9-]{1,62}[A-Za-z0-9])$`

Required: Yes

ValidationDomain

The domain name that you want ACM to use to send you validation emails. This domain name is the suffix of the email addresses that you want ACM to use. This must be the same as the `DomainName` value or a superdomain of the `DomainName` value. For example, if you request a certificate for `testing.example.com`, you can specify `example.com` for this value. In that case, ACM sends domain validation emails to the following five addresses:

- `admin@example.com`
- `administrator@example.com`
- `hostmaster@example.com`
- `postmaster@example.com`
- `webmaster@example.com`

Type: String

Length Constraints: Minimum length of 1. Maximum length of 253.

Pattern: `^(*\.\.?)?(((?!-)[A-Za-z0-9-]{0,62}[A-Za-z0-9])\.)+((?!-)[A-Za-z0-9-]{1,62}[A-Za-z0-9])$`

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](#)

RenewalSummary

Contains information about the status of ACM's [managed renewal](#) for the certificate. This structure exists only when the certificate type is `AMAZON_ISSUED`.

Contents

Note

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

DomainValidationOptions

Contains information about the validation of each domain name in the certificate, as it pertains to ACM's [managed renewal](#). This is different from the initial validation that occurs as a result of the [RequestCertificate \(p. 30\)](#) request. This field exists only when the certificate type is `AMAZON_ISSUED`.

Type: Array of [DomainValidation \(p. 43\)](#) objects

Array Members: Minimum number of 1 item. Maximum number of 1000 items.

Required: Yes

RenewalStatus

The status of ACM's [managed renewal](#) of the certificate.

Type: String

Valid Values: `PENDING_AUTO_RENEWAL` | `PENDING_VALIDATION` | `SUCCESS` | `FAILED`

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](#)

Tag

A key-value pair that identifies or specifies metadata about an ACM resource.

Contents

Note

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

Key

The key of the tag.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 128.

Pattern: `[\p{L}\p{Z}\p{N}_ :\/=+\-@]*`

Required: Yes

Value

The value of the tag.

Type: String

Length Constraints: Minimum length of 0. Maximum length of 256.

Pattern: `[\p{L}\p{Z}\p{N}_ :\/=+\-@]*`

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](#)

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`.

For more information, see [Task 2: Create a String to Sign 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

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