## Table of Contents

Welcome ........................................................................................................................................... 1
Actions ............................................................................................................................................... 2
CreateCloudFrontOriginAccessIdentity ........................................................................................... 4
  - Request Syntax .......................................................................................................................... 4
  - URI Request Parameters ........................................................................................................... 4
  - Request Body ............................................................................................................................ 4
  - Response Syntax ....................................................................................................................... 5
  - Response Elements .................................................................................................................... 5
  - Errors ......................................................................................................................................... 5
  - See Also .................................................................................................................................... 6
CreateDistribution ............................................................................................................................ 7
  - Request Syntax .......................................................................................................................... 7
  - URI Request Parameters ........................................................................................................... 10
  - Request Body ............................................................................................................................ 10
  - Response Syntax ....................................................................................................................... 15
  - Response Elements .................................................................................................................... 19
  - Errors ......................................................................................................................................... 20
  - See Also .................................................................................................................................... 23
CreateDistributionWithTags ............................................................................................................. 25
  - Request Syntax .......................................................................................................................... 25
  - URI Request Parameters ........................................................................................................... 28
  - Request Body ............................................................................................................................ 28
  - Response Syntax ....................................................................................................................... 29
  - Response Elements .................................................................................................................... 32
  - Errors ......................................................................................................................................... 33
  - See Also .................................................................................................................................... 37
CreateFieldLevelEncryptionConfig ................................................................................................. 38
  - Request Syntax .......................................................................................................................... 38
  - URI Request Parameters ........................................................................................................... 38
  - Request Body ............................................................................................................................ 38
  - Response Syntax ....................................................................................................................... 39
  - Response Elements .................................................................................................................... 40
  - Errors ......................................................................................................................................... 40
  - See Also .................................................................................................................................... 41
CreateFieldLevelEncryptionProfile ................................................................................................. 42
  - Request Syntax .......................................................................................................................... 42
  - URI Request Parameters ........................................................................................................... 42
  - Request Body ............................................................................................................................ 42
  - Response Syntax ....................................................................................................................... 43
  - Response Elements .................................................................................................................... 43
  - Errors ......................................................................................................................................... 44
  - See Also .................................................................................................................................... 45
CreateInvalidation ............................................................................................................................. 46
  - Request Syntax .......................................................................................................................... 46
  - URI Request Parameters ........................................................................................................... 46
  - Request Body ............................................................................................................................ 46
  - Response Syntax ....................................................................................................................... 47
  - Response Elements .................................................................................................................... 47
  - Errors ......................................................................................................................................... 47
  - See Also .................................................................................................................................... 48
CreatePublicKey ............................................................................................................................... 49
  - Request Syntax .......................................................................................................................... 49
  - URI Request Parameters ........................................................................................................... 49
  - Request Body ............................................................................................................................ 49

API Version 2017-10-30
Amazon CloudFront API Reference

Contents

ContentTypeProfileConfig ................................................................. 209
Contents ......................................................................................... 209
See Also ....................................................................................... 209
ContentTypeProfiles ......................................................................... 210
Contents ......................................................................................... 210
See Also ....................................................................................... 210
CookieNames .................................................................................. 211
Contents ......................................................................................... 211
See Also ....................................................................................... 211
CookiePreference ........................................................................... 212
Contents ......................................................................................... 212
See Also ....................................................................................... 212
CustomErrorResponse ..................................................................... 213
Contents ......................................................................................... 213
See Also ....................................................................................... 214
CustomErrorResponses ................................................................... 215
Contents ......................................................................................... 215
See Also ....................................................................................... 215
CustomHeaders .............................................................................. 216
Contents ......................................................................................... 216
See Also ....................................................................................... 216
CustomOriginConfig ....................................................................... 217
Contents ......................................................................................... 217
See Also ....................................................................................... 218
DefaultCacheBehavior .................................................................... 219
Contents ......................................................................................... 219
See Also ....................................................................................... 221
Distribution .................................................................................... 222
Contents ......................................................................................... 222
See Also ....................................................................................... 223
DistributionConfig ............................................................. 224
Contents ......................................................................................... 224
See Also ....................................................................................... 228
DistributionConfigWithTags .......................................................... 230
Contents ......................................................................................... 230
See Also ....................................................................................... 230
DistributionList ............................................................................. 231
Contents ......................................................................................... 231
See Also ....................................................................................... 231
DistributionSummary ............................................................... 233
Contents ......................................................................................... 233
See Also ....................................................................................... 236
EncryptionEntities ........................................................................... 237
Contents ......................................................................................... 237
See Also ....................................................................................... 237
EncryptionEntity ............................................................................ 238
Contents ......................................................................................... 238
See Also ....................................................................................... 238
FieldLevelEncryption ..................................................................... 239
Contents ......................................................................................... 239
See Also ....................................................................................... 239
FieldLevelEncryptionConfig ....................................................... 240
Contents ......................................................................................... 240
See Also ....................................................................................... 240
FieldLevelEncryptionList ............................................................. 241
Contents ......................................................................................... 241
See Also ....................................................................................... 241
FieldLevelEncryptionProfile ................................................................. 242
  Contents ............................................................................................... 242
  See Also ................................................................................................ 242
FieldLevelEncryptionProfileConfig ......................................................... 243
  Contents ............................................................................................... 243
  See Also ................................................................................................ 243
FieldLevelEncryptionProfileList ............................................................. 244
  Contents ............................................................................................... 244
  See Also ................................................................................................ 244
FieldLevelEncryptionProfileSummary .................................................... 245
  Contents ............................................................................................... 245
  See Also ................................................................................................ 245
FieldLevelEncryptionSummary ................................................................. 246
  Contents ............................................................................................... 246
  See Also ................................................................................................ 246
FieldPatterns .......................................................................................... 247
  Contents ............................................................................................... 247
  See Also ................................................................................................ 247
ForwardedValues ....................................................................................... 248
  Contents ............................................................................................... 248
  See Also ................................................................................................ 249
GeoRestriction ........................................................................................ 250
  Contents ............................................................................................... 250
  See Also ................................................................................................ 250
Headers ..................................................................................................... 252
  Contents ............................................................................................... 252
  See Also ................................................................................................ 252
Invalidation ............................................................................................. 254
  Contents ............................................................................................... 254
  See Also ................................................................................................ 254
InvalidationBatch ..................................................................................... 255
  Contents ............................................................................................... 255
  See Also ................................................................................................ 255
InvalidationList ......................................................................................... 256
  Contents ............................................................................................... 256
  See Also ................................................................................................ 256
InvalidationSummary ............................................................................... 258
  Contents ............................................................................................... 258
  See Also ................................................................................................ 258
KeyPairIds ............................................................................................... 259
  Contents ............................................................................................... 259
  See Also ................................................................................................ 259
LambdaFunctionAssociation ...................................................................... 260
  Contents ............................................................................................... 260
  See Also ................................................................................................ 260
LambdaFunctionAssociations ................................................................. 261
  Contents ............................................................................................... 261
  See Also ................................................................................................ 261
LoggingConfig ......................................................................................... 262
  Contents ............................................................................................... 262
  See Also ................................................................................................ 262
Origin ........................................................................................................ 264
  Contents ............................................................................................... 264
  See Also ................................................................................................ 265
OriginCustomHeader .............................................................................. 266
  Contents ............................................................................................... 266
  See Also ................................................................................................ 266
StreamingDistributionSummary ................................................................................................ 289
Contents .................................................................................................................................. 289
See Also .................................................................................................................................. 290
StreamingLoggingConfig ........................................................................................................... 291
Contents .................................................................................................................................. 291
See Also .................................................................................................................................. 291
Tag .......................................................................................................................................... 292
Contents .................................................................................................................................. 292
See Also .................................................................................................................................. 292
TagKeys ................................................................................................................................... 293
Contents .................................................................................................................................. 293
See Also .................................................................................................................................. 293
Tags ........................................................................................................................................ 294
Contents .................................................................................................................................. 294
See Also .................................................................................................................................. 294
TrustedSigners ............................................................................................................................ 295
Contents .................................................................................................................................. 295
See Also .................................................................................................................................. 295
ViewerCertificate ....................................................................................................................... 296
Contents .................................................................................................................................. 297
See Also .................................................................................................................................. 299
Common Parameters .................................................................................................................. 300
Common Errors ......................................................................................................................... 302
Welcome

This is the Amazon CloudFront API Reference. This guide is for developers who need detailed information about CloudFront API actions, data types, and errors. For detailed information about CloudFront features, see the Amazon CloudFront Developer Guide.

This document was last published on March 22, 2018.
Actions

The following actions are supported:

- CreateCloudFrontOriginAccessIdentity (p. 4)
- CreateDistribution (p. 7)
- CreateDistributionWithTags (p. 25)
- CreateFieldLevelEncryptionConfig (p. 38)
- CreateFieldLevelEncryptionProfile (p. 42)
- CreateInvalidation (p. 46)
- CreatePublicKey (p. 49)
- CreateStreamingDistribution (p. 52)
- CreateStreamingDistributionWithTags (p. 58)
- DeleteCloudFrontOriginAccessIdentity (p. 63)
- DeleteDistribution (p. 65)
- DeleteFieldLevelEncryptionConfig (p. 67)
- DeleteFieldLevelEncryptionProfile (p. 69)
- DeletePublicKey (p. 71)
- DeleteStreamingDistribution (p. 73)
- GetCloudFrontOriginAccessIdentity (p. 75)
- GetCloudFrontOriginAccessIdentityConfig (p. 77)
- GetDistribution (p. 79)
- GetDistributionConfig (p. 85)
- GetFieldLevelEncryption (p. 94)
- GetFieldLevelEncryptionConfig (p. 97)
- GetFieldLevelEncryptionProfile (p. 100)
- GetFieldLevelEncryptionProfileConfig (p. 102)
- GetInvalidation (p. 104)
- GetPublicKey (p. 107)
- GetPublicKeyConfig (p. 109)
- GetStreamingDistribution (p. 111)
- GetStreamingDistributionConfig (p. 114)
- ListCloudFrontOriginAccessIdentities (p. 117)
- ListDistributions (p. 120)
- ListDistributionsByWebACLId (p. 126)
- ListFieldLevelEncryptionConfigs (p. 132)
- ListFieldLevelEncryptionProfiles (p. 135)
- ListInvalidations (p. 138)
- ListPublicKeys (p. 141)
- ListStreamingDistributions (p. 143)
- ListTagsForResource (p. 146)
- TagResource (p. 148)
- UntagResource (p. 150)
- UpdateCloudFrontOriginAccessIdentity (p. 152)
- UpdateDistribution (p. 155)
- UpdateFieldLevelEncryptionConfig (p. 173)
- UpdateFieldLevelEncryptionProfile (p. 177)
- UpdatePublicKey (p. 181)
- UpdateStreamingDistribution (p. 184)
CreateCloudFrontOriginAccessIdentity

Creates a new origin access identity. If you're using Amazon S3 for your origin, you can use an origin access identity to require users to access your content using a CloudFront URL instead of the Amazon S3 URL. For more information about how to use origin access identities, see Serving Private Content through CloudFront in the Amazon CloudFront Developer Guide.

Request Syntax

POST /2017-10-30/origin-access-identity/cloudfront HTTP/1.1
<?xml version="1.0" encoding="UTF-8"?>
<CloudFrontOriginAccessIdentityConfig xmlns="http://cloudfront.amazonaws.com/doc/2017-10-30/"
  doc/2017-10-30/">
  <CallerReference>string</CallerReference>
  <Comment>string</Comment>
</CloudFrontOriginAccessIdentityConfig>

URI Request Parameters

The request does not use any URI parameters.

Request Body

The request accepts the following data in XML format.

CloudFrontOriginAccessIdentityConfig (p. 4)

Root level tag for the CloudFrontOriginAccessIdentityConfig parameters.

Required: Yes

CallerReference (p. 4)

A unique number that ensures the request can't be replayed.

If the CallerReference is new (no matter the content of the CloudFrontOriginAccessIdentityConfig object), a new origin access identity is created.

If the CallerReference is a value already sent in a previous identity request, and the content of the CloudFrontOriginAccessIdentityConfig is identical to the original request (ignoring white space), the response includes the same information returned to the original request.

If the CallerReference is a value you already sent in a previous request to create an identity, but the content of the CloudFrontOriginAccessIdentityConfig is different from the original request, CloudFront returns a CloudFrontOriginAccessIdentityAlreadyExists error.

Type: String

Required: Yes

Comment (p. 4)

Any comments you want to include about the origin access identity.

Type: String

Required: Yes
Response Syntax

HTTP/1.1 201
<?xml version="1.0" encoding="UTF-8"?>
<CloudFrontOriginAccessIdentity>
  <CloudFrontOriginAccessIdentityConfig>
    <CallerReference>string</CallerReference>
    <Comment>string</Comment>
  </CloudFrontOriginAccessIdentityConfig>
  <Id>string</Id>
  <S3CanonicalUserId>string</S3CanonicalUserId>
</CloudFrontOriginAccessIdentity>

Response Elements

If the action is successful, the service sends back an HTTP 201 response.

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

CloudFrontOriginAccessIdentity (p. 5)

Root level tag for the CloudFrontOriginAccessIdentity parameters.

Required: Yes

CloudFrontOriginAccessIdentityConfig (p. 5)

The current configuration information for the identity.

Type: CloudFrontOriginAccessIdentityConfig (p. 204) object

Id (p. 5)

The ID for the origin access identity, for example, E74FTE3AJFJ256A.

Type: String

S3CanonicalUserId (p. 5)

The Amazon S3 canonical user ID for the origin access identity, used when giving the origin access identity read permission to an object in Amazon S3.

Type: String

Errors

For information about the errors that are common to all actions, see Common Errors (p. 302).

CloudFrontOriginAccessIdentityAlreadyExists

If the CallerReference is a value you already sent in a previous request to create an identity but the content of the CloudFrontOriginAccessIdentityConfig is different from the original request, CloudFront returns a CloudFrontOriginAccessIdentityAlreadyExists error.

HTTP Status Code: 409

InconsistentQuantities

The value of Quantity and the size of Items don't match.

HTTP Status Code: 400
InvalidArgument

The argument is invalid.

HTTP Status Code: 400

MissingBody

This operation requires a body. Ensure that the body is present and the Content-Type header is set.

HTTP Status Code: 400

TooManyCloudFrontOriginAccessIdentities

Processing your request would cause you to exceed the maximum number of origin access identities allowed.

HTTP Status Code: 400

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
CreateDistribution

Creates a new web distribution. Send a POST request to the /CloudFront API version/distribution/distribution ID resource.

Request Syntax

POST /2017-10-30/distribution HTTP/1.1
<?xml version="1.0" encoding="UTF-8"?>
<DistributionConfig xmlns="http://cloudfront.amazonaws.com/doc/2017-10-30/"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  xsi:schemaLocation="http://cloudfront.amazonaws.com/doc/2017-10-30"
>
  <Aliases>
    <Items>
      <CNAME>string</CNAME>
    </Items>
    <Quantity>integer</Quantity>
  </Aliases>
  <CacheBehaviors>
    <Items>
      <CacheBehavior>
        <AllowedMethods>
          <CachedMethods>
            <Items>
              <Method>string</Method>
            </Items>
            <Quantity>integer</Quantity>
          </CachedMethods>
          <Items>
            <Method>string</Method>
          </Items>
          <Quantity>integer</Quantity>
        </AllowedMethods>
        <Compress>boolean</Compress>
        <DefaultTTL>long</DefaultTTL>
        <FieldLevelEncryptionId>string</FieldLevelEncryptionId>
        <ForwardedValues>
          <Cookies>
            <Forward>string</Forward>
            <WhitelistedNames>
              <Items>
                <Name>string</Name>
              </Items>
              <Quantity>integer</Quantity>
            </WhitelistedNames>
          </Cookies>
          <Headers>
            <Items>
              <Name>string</Name>
            </Items>
            <Quantity>integer</Quantity>
          </Headers>
          <QueryString>boolean</QueryString>
          <QueryStringCacheKeys>
            <Items>
              <Name>string</Name>
            </Items>
            <Quantity>integer</Quantity>
          </QueryStringCacheKeys>
        </ForwardedValues>
        <LambdaFunctionAssociations>
          <Items>
            <LambdaFunctionAssociation>
              <EventType>string</EventType>
            </LambdaFunctionAssociation>
          </Items>
        </LambdaFunctionAssociations>
      </CacheBehavior>
    </Items>
  </CacheBehaviors>
  <Compress>boolean</Compress>
  <DefaultTTL>long</DefaultTTL>
  <FieldLevelEncryptionId>string</FieldLevelEncryptionId>
  <ForwardedValues>
    <Cookies>
      <Forward>string</Forward>
      <WhitelistedNames>
        <Items>
          <Name>string</Name>
        </Items>
        <Quantity>integer</Quantity>
      </WhitelistedNames>
    </Cookies>
    <Headers>
      <Items>
        <Name>string</Name>
      </Items>
      <Quantity>integer</Quantity>
    </Headers>
  </ForwardedValues>
</DistributionConfig>
<LambdaFunctionARN>string</LambdaFunctionARN>  
</LambdaFunctionAssociation>
</Items>
</LambdaFunctionAssociations>
<MaxTTL>long</MaxTTL>
<MinTTL>long</MinTTL>
<PathPattern>string</PathPattern>
<SmoothStreaming>boolean</SmoothStreaming>
<TargetOriginId>string</TargetOriginId>
<TrustedSigners>
<Enabled>boolean</Enabled>
</Items>
<AwsAccountNumber>string</AwsAccountNumber>
</Items>
<Quantity>integer</Quantity>
</TrustedSigners>
</ViewerProtocolPolicy>
</CacheBehavior>
</Items>
<Quantity>integer</Quantity>
</CacheBehaviors>
<CallerReference>string</CallerReference>
<Comment>string</Comment>
</CustomErrorResponses>
</Items>
<CustomErrorResponse>
<ErrorCachingMinTTL>long</ErrorCachingMinTTL>
<ErrorCode>integer</ErrorCode>
<ResponseCode>string</ResponseCode>
<ResponsePagePath>string</ResponsePagePath>
</CustomErrorResponse>
</Items>
<Quantity>integer</Quantity>
</CustomErrorResponses>
</DefaultCacheBehavior>
<AllowedMethods>
<CachedMethods>
<Items>
<Method>string</Method>
</Items>
<Quantity>integer</Quantity>
</CachedMethods>
<Items>
<Method>string</Method>
</Items>
<Quantity>integer</Quantity>
</AllowedMethods>
<Compress>boolean</Compress>
<DefaultTTL>long</DefaultTTL>
<FieldLevelEncryptionId>string</FieldLevelEncryptionId>
<ForwardedValues>
<Cookies>
<Forward>string</Forward>
<WhitelistedNames>
<Items>
>Name>string</Name>
</Items>
<Quantity>integer</Quantity>
</WhitelistedNames>
</Cookies>
<Headers>
<Items>
>Name>string</Name>
</Items>
<Quantity>integer</Quantity>
</Headers>
<Headers>
  <QueryString>boolean</QueryString>
  <QueryStringCacheKeys>
    <Items>
      <Name>string</Name>
    </Items>
  </QueryStringCacheKeys>
  <ForwardedValues>
    <LambdaFunctionAssociations>
      <Items>
        <LambdaFunctionAssociation>
          <EventType>string</EventType>
          <LambdaFunctionARN>string</LambdaFunctionARN>
        </LambdaFunctionAssociation>
      </Items>
    </LambdaFunctionAssociations>
    <MaxTTL>long</MaxTTL>
    <MinTTL>long</MinTTL>
    <SmoothStreaming>boolean</SmoothStreaming>
    <TargetOriginId>string</TargetOriginId>
    <TrustedSigners>
      <Enabled>boolean</Enabled>
      <Items>
        <AwsAccountNumber>string</AwsAccountNumber>
      </Items>
    </TrustedSigners>
    <ViewerProtocolPolicy>string</ViewerProtocolPolicy>
  </ForwardedValues>
  <DefaultCacheBehavior>
    <DefaultRootObject>string</DefaultRootObject>
    <HttpVersion>string</HttpVersion>
    <IsIPV6Enabled>boolean</IsIPV6Enabled>
    <Logging>
      <Bucket>string</Bucket>
      <IncludeCookies>boolean</IncludeCookies>
      <Prefix>string</Prefix>
    </Logging>
    <Origins>
      <Items>
        <Origin>
          <CustomHeaders>
            <Items>
              <OriginCustomHeader>
                <HeaderValue>string</HeaderValue>
              </OriginCustomHeader>
            </Items>
          </CustomHeaders>
          <CustomOriginConfig>
            <HTTPPort>integer</HTTPPort>
            <HTTPSPort>integer</HTTPSPort>
            <OriginKeepaliveTimeout>integer</OriginKeepaliveTimeout>
            <OriginReadTimeout>integer</OriginReadTimeout>
            <OriginSslProtocols>
              <Items>
                <SslProtocol>string</SslProtocol>
              </Items>
            </OriginSslProtocols>
          </CustomOriginConfig>
        </Origin>
      </Items>
    </Origins>
  </DefaultCacheBehavior>
</Headers>

API Version 2017-10-30
## URI Request Parameters

The request does not use any URI parameters.

## Request Body

The request accepts the following data in XML format.

**DistributionConfig (p. 7)**

Root level tag for the DistributionConfig parameters.

- **Required:** Yes

**Aliases (p. 7)**

A complex type that contains information about CNAMEs (alternate domain names), if any, for this distribution.

- **Type:** Aliases (p. 194) object

- **Required:** No

**CacheBehaviors (p. 7)**

A complex type that contains zero or more CacheBehavior elements.

- **Type:** CacheBehaviors (p. 201) object

- **Required:** No
**CallerReference (p. 7)**

A unique value (for example, a date-time stamp) that ensures that the request can't be replayed.

If the value of `CallerReference` is new (regardless of the content of the `DistributionConfig` object), CloudFront creates a new distribution.

If `CallerReference` is a value you already sent in a previous request to create a distribution, and if the content of the `DistributionConfig` is identical to the original request (ignoring white space), CloudFront returns the same response that it returned to the original request.

If `CallerReference` is a value you already sent in a previous request to create a distribution but the content of the `DistributionConfig` is different from the original request, CloudFront returns a `DistributionAlreadyExists` error.

Type: String
Required: Yes

**Comment (p. 7)**

Any comments you want to include about the distribution.

If you don't want to specify a comment, include an empty `Comment` element.

To delete an existing comment, update the distribution configuration and include an empty `Comment` element.

To add or change a comment, update the distribution configuration and specify the new comment.

Type: String
Required: Yes

**CustomErrorResponses (p. 7)**

A complex type that controls the following:
- Whether CloudFront replaces HTTP status codes in the 4xx and 5xx range with custom error messages before returning the response to the viewer.
- How long CloudFront caches HTTP status codes in the 4xx and 5xx range.

For more information about custom error pages, see `Customizing Error Responses` in the Amazon CloudFront Developer Guide.

Type: `CustomErrorResponses (p. 215)` object
Required: No

**DefaultCacheBehavior (p. 7)**

A complex type that describes the default cache behavior if you don't specify a `CacheBehavior` element or if files don't match any of the values of `PathPattern` in `CacheBehavior` elements. You must create exactly one default cache behavior.

Type: `DefaultCacheBehavior (p. 219)` object
Required: Yes

**DefaultRootObject (p. 7)**

The object that you want CloudFront to request from your origin (for example, `index.html`) when a viewer requests the root URL for your distribution (`http://www.example.com`) instead

Specify only the object name, for example, index.html. Don't add a / before the object name.

If you don't want to specify a default root object when you create a distribution, include an empty DefaultRootObject element.

To delete the default root object from an existing distribution, update the distribution configuration and include an empty DefaultRootObject element.

To replace the default root object, update the distribution configuration and specify the new object.

For more information about the default root object, see Creating a Default Root Object in the Amazon CloudFront Developer Guide.

Type: String
Required: No

**Enabled (p. 7)**

From this field, you can enable or disable the selected distribution.

If you specify false for Enabled but you specify values for Bucket and Prefix, the values are automatically deleted.

Type: Boolean
Required: Yes

**HttpVersion (p. 7)**

(Optional) Specify the maximum HTTP version that you want viewers to use to communicate with CloudFront. The default value for new web distributions is http2. Viewers that don't support HTTP/2 automatically use an earlier HTTP version.

For viewers and CloudFront to use HTTP/2, viewers must support TLS 1.2 or later, and must support Server Name Identification (SNI).

In general, configuring CloudFront to communicate with viewers using HTTP/2 reduces latency. You can improve performance by optimizing for HTTP/2. For more information, do an Internet search for "http/2 optimization."

Type: String

Valid Values: http1.1 | http2

Required: No

**IsIPV6Enabled (p. 7)**

If you want CloudFront to respond to IPv6 DNS requests with an IPv6 address for your distribution, specify true. If you specify false, CloudFront responds to IPv6 DNS requests with the DNS response code NOERROR and with no IP addresses. This allows viewers to submit a second request, for an IPv4 address for your distribution.

In general, you should enable IPv6 if you have users on IPv6 networks who want to access your content. However, if you're using signed URLs or signed cookies to restrict access to your content, and if you're using a custom policy that includes the IPAddress parameter to restrict the IP addresses that can access your content, don't enable IPv6. If you want to restrict access to some content by IP address and not restrict access to other content (or restrict access but not by IP
address), you can create two distributions. For more information, see Creating a Signed URL Using a Custom Policy in the Amazon CloudFront Developer Guide.

If you're using an Amazon Route 53 alias resource record set to route traffic to your CloudFront distribution, you need to create a second alias resource record set when both of the following are true:

- You enable IPv6 for the distribution
- You're using alternate domain names in the URLs for your objects

For more information, see Routing Traffic to an Amazon CloudFront Web Distribution by Using Your Domain Name in the Amazon Route 53 Developer Guide.

If you created a CNAME resource record set, either with Amazon Route 53 or with another DNS service, you don't need to make any changes. A CNAME record will route traffic to your distribution regardless of the IP address format of the viewer request.

Type: Boolean

Required: No

Logging (p. 7)

A complex type that controls whether access logs are written for the distribution.

For more information about logging, see Access Logs in the Amazon CloudFront Developer Guide.

Type: LoggingConfig (p. 262) object

Required: No

Origins (p. 7)

A complex type that contains information about origins for this distribution.

Type: Origins (p. 267) object

Required: Yes

PriceClass (p. 7)

The price class that corresponds with the maximum price that you want to pay for CloudFront service. If you specify PriceClass_All, CloudFront responds to requests for your objects from all CloudFront edge locations.

If you specify a price class other than PriceClass_All, CloudFront serves your objects from the CloudFront edge location that has the lowest latency among the edge locations in your price class. Viewers who are in or near regions that are excluded from your specified price class may encounter slower performance.

For more information about price classes, see Choosing the Price Class for a CloudFront Distribution in the Amazon CloudFront Developer Guide. For information about CloudFront pricing, including how price classes map to CloudFront regions, see Amazon CloudFront Pricing.

Type: String

Valid Values: PriceClass_100 | PriceClass_200 | PriceClass_All

Required: No

Restrictions (p. 7)

A complex type that identifies ways in which you want to restrict distribution of your content.
Type: **Restrictions (p. 278) object**

Required: No

**ViewerCertificate (p. 7)**

A complex type that specifies the following:

- Whether you want viewers to use HTTP or HTTPS to request your objects.
- If you want viewers to use HTTPS, whether you're using an alternate domain name such as example.com or the CloudFront domain name for your distribution, such as d111111abcdef8.cloudfront.net.
- If you're using an alternate domain name, whether AWS Certificate Manager (ACM) provided the certificate, or you purchased a certificate from a third-party certificate authority and imported it into ACM or uploaded it to the IAM certificate store.

You must specify only one of the following values:

- **ViewerCertificate:ACMCertificateArn (p. 297)**
- **ViewerCertificate:IAMCertificateId (p. 298)**
- **ViewerCertificate:CloudFrontDefaultCertificate (p. 297)**

Don't specify `false` for `CloudFrontDefaultCertificate`.

**If you want viewers to use HTTP instead of HTTPS to request your objects:** Specify the following value:

```
<CloudFrontDefaultCertificate>true</CloudFrontDefaultCertificate>
```

In addition, specify `allow-all` for `ViewerProtocolPolicy` for all of your cache behaviors.

**If you want viewers to use HTTPS to request your objects:** Choose the type of certificate that you want to use based on whether you're using an alternate domain name for your objects or the CloudFront domain name:

- **If you're using an alternate domain name, such as example.com:** Specify one of the following values, depending on whether ACM provided your certificate or you purchased your certificate from third-party certificate authority:

  - `<ACMCertificateArn>ARN for ACM SSL/TLS certificate</ACMCertificateArn>` where `ARN for ACM SSL/TLS certificate` is the ARN for the ACM SSL/TLS certificate that you want to use for this distribution.
  - `<IAMCertificateId>IAM certificate ID</IAMCertificateId>` where `IAM certificate ID` is the ID that IAM returned when you added the certificate to the IAM certificate store.

  If you specify `ACMCertificateArn` or `IAMCertificateId`, you must also specify a value for `SSLSupportMethod`.

  If you choose to use an ACM certificate or a certificate in the IAM certificate store, we recommend that you use only an alternate domain name in your object URLs (https://example.com/logo.jpg). If you use the domain name that is associated with your CloudFront distribution (such as https://d111111abcdef8.cloudfront.net/logo.jpg) and the viewer supports SNI, then CloudFront behaves normally. However, if the browser does not support SNI, the user's experience depends on the value that you choose for `SSLSupportMethod`:

  - `vip`: The viewer displays a warning because there is a mismatch between the CloudFront domain name and the domain name in your SSL/TLS certificate.
  - `sni-only`: CloudFront drops the connection with the browser without returning the object.

  **If you're using the CloudFront domain name for your distribution, such as d111111abcdef8.cloudfront.net:** Specify the following value:
If you want viewers to use HTTPS, you must also specify one of the following values in your cache behaviors:

- `<ViewerProtocolPolicy>https-only</ViewerProtocolPolicy>`
- `<ViewerProtocolPolicy>redirect-to-https</ViewerProtocolPolicy>`

You can also optionally require that CloudFront use HTTPS to communicate with your origin by specifying one of the following values for the applicable origins:

- `<OriginProtocolPolicy>https-only</OriginProtocolPolicy>`

For more information, see Using Alternate Domain Names and HTTPS in the Amazon CloudFront Developer Guide.

**Type:** ViewerCertificate (p. 296) object

**Required:** No

### WebACLId (p. 7)

A unique identifier that specifies the AWS WAF web ACL, if any, to associate with this distribution.

AWS WAF is a web application firewall that lets you monitor the HTTP and HTTPS requests that are forwarded to CloudFront, and lets you control access to your content. Based on conditions that you specify, such as the IP addresses that requests originate from or the values of query strings, CloudFront responds to requests either with the requested content or with an HTTP 403 status code (Forbidden). You can also configure CloudFront to return a custom error page when a request is blocked. For more information about AWS WAF, see the AWS WAF Developer Guide.

**Type:** String

**Required:** No

---

**Response Syntax**

```
HTTP/1.1 201
<?xml version="1.0" encoding="UTF-8"?>
<Distribution>
  <ActiveTrustedSigners>
    <Enabled>boolean</Enabled>
    <Items>
      <Signer>
        <AwsAccountNumber>string</AwsAccountNumber>
        <KeyPairIds>
          <Items>
            <KeyPairId>string</KeyPairId>
          </Items>
          <Quantity>integer</Quantity>
        </KeyPairIds>
      </Signer>
    </Items>
  </ActiveTrustedSigners>
  <ARN>string</ARN>
  <DistributionConfig>
    <Aliases>
      <Items>
        <CNAME>string</CNAME>
      </Items>
    </Aliases>
  </DistributionConfig>
</Distribution>
```
<Items>
  <Quantity>integer</Quantity>
</Items>

<Aliases>
  <Quantity>integer</Quantity>
</Aliases>

<CacheBehaviors>
  <Items>
    <CacheBehavior>
      <AllowedMethods>
        <Items>
          <Quantity>integer</Quantity>
        </Items>
      </AllowedMethods>
      <CachedMethods>
        <Items>
          <Method>string</Method>
          <Quantity>integer</Quantity>
        </Items>
      </CachedMethods>
      <Compress>boolean</Compress>
      <DefaultTTL>long</DefaultTTL>
      <FieldLevelEncryptionId>string</FieldLevelEncryptionId>
      <ForwardedValues>
        <Cookies>
          <Forward>string</Forward>
          <WhitelistedNames>
            <Items>
              <Name>string</Name>
              <Quantity>integer</Quantity>
            </Items>
          </WhitelistedNames>
        </Cookies>
        <Headers>
          <Items>
            <Name>string</Name>
            <Quantity>integer</Quantity>
          </Items>
        </Headers>
        <QueryString>boolean</QueryString>
        <QueryStringCacheKeys>
          <Items>
            <Name>string</Name>
            <Quantity>integer</Quantity>
          </Items>
        </QueryStringCacheKeys>
      </ForwardedValues>
      <LambdaFunctionAssociations>
        <Items>
          <LambdaFunctionAssociation>
            <EventType>string</EventType>
            <LambdaFunctionARN>string</LambdaFunctionARN>
          </LambdaFunctionAssociation>
          <Quantity>integer</Quantity>
        </LambdaFunctionAssociations>
      </LambdaFunctionAssociations>
      <MaxTTL>long</MaxTTL>
      <MinTTL>long</MinTTL>
      <PathPattern>string</PathPattern>
      <SmoothStreaming>boolean</SmoothStreaming>
      <TargetOriginId>string</TargetOriginId>
      <TrustedSigners>
        <Enabled>boolean</Enabled>
        <Items>
          <AwsAccountNumber>string</AwsAccountNumber>
          <Quantity>integer</Quantity>
        </Items>
      </TrustedSigners>
    </CacheBehavior>
    <Quantity>integer</Quantity>
  </Items>
</CacheBehaviors>
<ViewerProtocolPolicy>string</ViewerProtocolPolicy>
</CacheBehavior>
</Items>
<CallerReference>string</CallerReference>
<Comment>string</Comment>
<CustomErrorResponses>
<Items>
<CustomErrorResponse>
<ErrorCachingMinTTL>long</ErrorCachingMinTTL>
<ErrorCode>integer</ErrorCode>
<ResponseCode>string</ResponseCode>
<ResponsePagePath>string</ResponsePagePath>
</CustomErrorResponse>
</Items>
<Quantity>integer</Quantity>
</CustomErrorResponses>
<DefaultCacheBehavior>
<AllowedMethods>
<CachedMethods>
<Items>
<Method>string</Method>
</Items>
<Quantity>integer</Quantity>
</CachedMethods>
<Items>
<Method>string</Method>
</Items>
<Quantity>integer</Quantity>
</AllowedMethods>
<Compress>boolean</Compress>
<DefaultTTL>long</DefaultTTL>
<FieldLevelEncryptionId>string</FieldLevelEncryptionId>
<ForwardedValues>
<Cookies>
<Forward>string</Forward>
<WhitelistedNames>
<Items>
<Name>string</Name>
</Items>
<Quantity>integer</Quantity>
</WhitelistedNames>
</Cookies>
<Headers>
<Items>
<Name>string</Name>
</Items>
<Quantity>integer</Quantity>
</Headers>
<QueryString>boolean</QueryString>
<queryStringCacheKeys>
<Items>
<Name>string</Name>
</Items>
<Quantity>integer</Quantity>
</queryStringCacheKeys>
</ForwardedValues>
</LambdaFunctionAssociations>
<Items>
<LambdaFunctionAssociation>
<EventType>string</EventType>
<LambdaFunctionARN>string</LambdaFunctionARN>
</LambdaFunctionAssociation>
</Items>
<Quantity>integer</Quantity>
<LambdaFunctionAssociations>
<MaxTTL>long</MaxTTL>
<MinTTL>long</MinTTL>
<SmoothStreaming>boolean</SmoothStreaming>
<TargetOriginId>string</TargetOriginId>
<TrustedSigners>
<Enabled>boolean</Enabled>
<Items>
<AwsAccountNumber>string</AwsAccountNumber>
<Quantity>integer</Quantity>
</Items>
</TrustedSigners>
<ViewerProtocolPolicy>string</ViewerProtocolPolicy>
</DefaultCacheBehavior>
<DefaultRootObject>string</DefaultRootObject>
<Enabled>boolean</Enabled>
<HttpVersion>string</HttpVersion>
<IsIPV6Enabled>boolean</IsIPV6Enabled>
<Logging>
<Bucket>string</Bucket>
<Enabled>boolean</Enabled>
<IncludeCookies>boolean</IncludeCookies>
<Prefix>string</Prefix>
</Logging>
<Origins>
<Items>
<Origin>
<CustomHeaders>
<Items>
<OriginCustomHeader>
<HeaderValue>string</HeaderValue>
</OriginCustomHeader>
<Quantity>integer</Quantity>
</Items>
</CustomHeaders>
<CustomOriginConfig>
<HTTPPort>integer</HTTPPort>
<HTTPSPort>integer</HTTPSPort>
<OriginKeepaliveTimeout>integer</OriginKeepaliveTimeout>
<OriginProtocolPolicy>string</OriginProtocolPolicy>
<OriginReadTimeout>integer</OriginReadTimeout>
<OriginSslProtocols>
<Items>
<SslProtocol>string</SslProtocol>
</Items>
<Quantity>integer</Quantity>
</OriginSslProtocols>
</CustomOriginConfig>
<DomainName>string</DomainName>
<Id>string</Id>
<OriginPath>string</OriginPath>
<S3OriginConfig>
<OriginAccessIdentity>string</OriginAccessIdentity>
</S3OriginConfig>
</Origin>
</Items>
<Quantity>integer</Quantity>
</Origins>
</PriceClass>
<Restrictions>
<GeoRestriction>
<Items>
<Location>string</Location>
</Items>
<Quantity>integer</Quantity>
</GeoRestriction>
</Restrictions>
</OriginGroupDescription>
Response Elements

If the action is successful, the service sends back an HTTP 201 response.

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

Distribution (p. 15)

Root level tag for the Distribution parameters.

Required: Yes

Active Trusted Signers (p. 15)

CloudFront automatically adds this element to the response only if you've set up the distribution to serve private content with signed URLs. The element lists the key pair IDs that CloudFront is aware of for each trusted signer. The `Signer` child element lists the AWS account number of the trusted signer (or an empty `Self` element if the signer is you). The `Signer` element also includes the IDs of any active key pairs associated with the trusted signer's AWS account. If no `KeyPairId` element appears for a `Signer`, that signer can't create working signed URLs.

Type: `ActiveTrustedSigners` (p. 192) object

ARN (p. 15)

The ARN (Amazon Resource Name) for the distribution. For example: `arn:aws:cloudfront::123456789012:distribution/EDFDVBD632BHDSS`, where 123456789012 is your AWS account ID.

Type: String

DistributionConfig (p. 15)

The current configuration information for the distribution. Send a GET request to the `/CloudFront API version/distribution ID/config` resource.

Type: `DistributionConfig` (p. 224) object

DomainName (p. 15)

The domain name corresponding to the distribution, for example, d111111abcdef8.cloudfront.net.
Type: String

**Id (p. 15)**

The identifier for the distribution. For example: EDFDVBD632BHDS5.

Type: String

**InProgressInvalidationBatches (p. 15)**

The number of invalidation batches currently in progress.

Type: Integer

**LastModifiedTime (p. 15)**

The date and time the distribution was last modified.

Type: Timestamp

**Status (p. 15)**

This response element indicates the current status of the distribution. When the status is **Deployed**, the distribution's information is fully propagated to all CloudFront edge locations.

Type: String

## Errors

For information about the errors that are common to all actions, see [Common Errors (p. 302)](#).

**AccessDenied**

Access denied.

HTTP Status Code: 403

**CNAMEAlreadyExists**

HTTP Status Code: 409

**DistributionAlreadyExists**

The caller reference you attempted to create the distribution with is associated with another distribution.

HTTP Status Code: 409

**IllegalFieldLevelEncryptionConfigAssociationWithCacheBehavior**

The specified configuration for field-level encryption can't be associated with the specified cache behavior.

HTTP Status Code: 400

**InconsistentQuantities**

The value of **Quantity** and the size of **Items** don't match.

HTTP Status Code: 400

**InvalidArgument**

The argument is invalid.

HTTP Status Code: 400
InvalidDefaultRootObject

The default root object file name is too big or contains an invalid character.

HTTP Status Code: 400

InvalidErrorCode

HTTP Status Code: 400

InvalidForwardCookies

Your request contains forward cookies option which doesn't match with the expectation for the whitelisted list of cookie names. Either list of cookie names has been specified when not allowed or list of cookie names is missing when expected.

HTTP Status Code: 400

InvalidGeoRestrictionParameter

HTTP Status Code: 400

InvalidHeadersForS3Origin

HTTP Status Code: 400

InvalidLambdaFunctionAssociation

The specified Lambda function association is invalid.

HTTP Status Code: 400

InvalidLocationCode

HTTP Status Code: 400

InvalidMinimumProtocolVersion

HTTP Status Code: 400

InvalidOrigin

The Amazon S3 origin server specified does not refer to a valid Amazon S3 bucket.

HTTP Status Code: 400

InvalidOriginAccessIdentity

The origin access identity is not valid or doesn't exist.

HTTP Status Code: 400

InvalidOriginKeepaliveTimeout

HTTP Status Code: 400

InvalidOriginReadTimeout

HTTP Status Code: 400

InvalidProtocolSettings

You cannot specify SSLv3 as the minimum protocol version if you only want to support only clients that support Server Name Indication (SNI).

HTTP Status Code: 400

InvalidQueryStringParameters

HTTP Status Code: 400
InvalidRelativePath

The relative path is too big, is not URL-encoded, or does not begin with a slash (/).

HTTP Status Code: 400

InvalidRequiredProtocol

This operation requires the HTTPS protocol. Ensure that you specify the HTTPS protocol in your request, or omit the RequiredProtocols element from your distribution configuration.

HTTP Status Code: 400

InvalidResponseCode

HTTP Status Code: 400

InvalidTTLOrder

HTTP Status Code: 400

InvalidViewerCertificate

HTTP Status Code: 400

InvalidWebACLId

HTTP Status Code: 400

MissingBody

This operation requires a body. Ensure that the body is present and the Content-Type header is set.

HTTP Status Code: 400

NoSuchFieldLevelEncryptionConfig

The specified configuration for field-level encryption doesn't exist.

HTTP Status Code: 404

NoSuchOrigin

No origin exists with the specified Origin Id.

HTTP Status Code: 404

TooManyCacheBehaviors

You cannot create more cache behaviors for the distribution.

HTTP Status Code: 400

TooManyCertificates

You cannot create anymore custom SSL/TLS certificates.

HTTP Status Code: 400

TooManyCookieNamesInWhiteList

Your request contains more cookie names in the whitelist than are allowed per cache behavior.

HTTP Status Code: 400

TooManyDistributionCNAMEs

Your request contains more CNAMEs than are allowed per distribution.
HTTP Status Code: 400
**TooManyDistributions**
Processing your request would cause you to exceed the maximum number of distributions allowed.

HTTP Status Code: 400
**TooManyDistributionsAssociatedToFieldLevelEncryptionConfig**
The maximum number of distributions have been associated with the specified configuration for field-level encryption.

HTTP Status Code: 400
**TooManyDistributionsWithLambdaAssociations**
Processing your request would cause the maximum number of distributions with Lambda function associations per owner to be exceeded.

HTTP Status Code: 400
**TooManyHeadersInForwardedValues**

HTTP Status Code: 400
**TooManyLambdaFunctionAssociations**
Your request contains more Lambda function associations than are allowed per distribution.

HTTP Status Code: 400
**TooManyOriginCustomHeaders**

HTTP Status Code: 400
**TooManyOrigins**
You cannot create more origins for the distribution.

HTTP Status Code: 400
**TooManyQueryStringParameters**

HTTP Status Code: 400
**TooManyTrustedSigners**
Your request contains more trusted signers than are allowed per distribution.

HTTP Status Code: 400
**TrustedSignerDoesNotExist**
One or more of your trusted signers don't exist.

HTTP Status Code: 400

**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
CreateDistributionWithTags

Create a new distribution with tags.

Request Syntax

POST /2017-10-30/distribution?WithTags HTTP/1.1
<?xml version="1.0" encoding="UTF-8"?>
<DistributionConfigWithTags xmlns="http://cloudfront.amazonaws.com/doc/2017-10-30/">
    <DistributionConfig>
        <Aliases>
            <Items>
                <CNAME>string</CNAME>
            </Items>
            <Quantity>integer</Quantity>
        </Aliases>
        <CacheBehaviors>
            <Items>
                <CacheBehavior>
                    <AllowedMethods>
                        <CachedMethods>
                            <Items>
                                <Method>string</Method>
                            </Items>
                            <Quantity>integer</Quantity>
                        </CachedMethods>
                        <Items>
                            <Method>string</Method>
                        </Items>
                        <Quantity>integer</Quantity>
                    </AllowedMethods>
                    <Compress>boolean</Compress>
                    <DefaultTTL>long</DefaultTTL>
                    <FieldLevelEncryptionId>string</FieldLevelEncryptionId>
                </CacheBehavior>
            </Items>
            <ForwardedValues>
                <Cookies>
                    <Forward>string</Forward>
                </Cookies>
                <WhitelistedNames>
                    <Items>
                        <Name>string</Name>
                    </Items>
                    <Quantity>integer</Quantity>
                </WhitelistedNames>
                <Headers>
                    <Items>
                        <Name>string</Name>
                    </Items>
                    <Quantity>integer</Quantity>
                </Headers>
                <QueryString>boolean</QueryString>
                <QueryStringCacheKeys>
                    <Items>
                        <Name>string</Name>
                    </Items>
                    <Quantity>integer</Quantity>
                </QueryStringCacheKeys>
            </ForwardedValues>
            <LambdaFunctionAssociations>
                <Items>
                    <LambdaFunctionAssociation>
                        <EventType>string</EventType>
                    </LambdaFunctionAssociation>
                </Items>
            </LambdaFunctionAssociations>
        </CacheBehaviors>
    </DistributionConfig>
</DistributionConfigWithTags>
Amazon CloudFront API Reference

Request Syntax

</LambdaFunctionAssociation>
</Items>
</LambdaFunctionAssociations>
<MaxTTL>long</MaxTTL>
<MinTTL>long</MinTTL>
<PathPattern>string</PathPattern>
<SmoothStreaming>boolean</SmoothStreaming>
<TargetOriginId>string</TargetOriginId>
<TrustedSigners>
</Items>
</TrustedSigners>
</Viewe
<QueryString boolean>
 <Items>
  <Name>string</Name>
 </Items>
</QueryString>

<QueryStringCacheKeys>
 <Items>
  <Name>string</Name>
 </Items>
</QueryStringCacheKeys>

<ForwardedValues>
</ForwardedValues>

<LambdaFunctionAssociations>
 <Items>
  <LambdaFunctionAssociation>
   <EventType>string</EventType>
   <LambdaFunctionARN>string</LambdaFunctionARN>
  </LambdaFunctionAssociation>
 </Items>
</LambdaFunctionAssociations>

<MaxTTL>long</MaxTTL>

<MinTTL>long</MinTTL>

<SmoothStreaming>boolean</SmoothStreaming>

<TargetOriginId>string</TargetOriginId>

<TrustedSigners>
 <Items>
  <AwsAccountNumber>string</AwsAccountNumber>
 </Items>
</TrustedSigners>

<ViewerProtocolPolicy>string</ViewerProtocolPolicy>

<DefaultCacheBehavior>
</DefaultCacheBehavior>

<DefaultRootObject>string</DefaultRootObject>

<Enabled>boolean</Enabled>

<httpVersion>string</httpVersion>

<IsIPV6Enabled>boolean</IsIPV6Enabled>

<Logging>
 <Bucket>string</Bucket>
 <Enabled>boolean</Enabled>
 <IncludeCookies>boolean</IncludeCookies>
 <Prefix>string</Prefix>
</Logging>

<Origins>
 <Items>
  <Origin>
   <CustomOriginConfig>
    <HTTPPort>integer</HTTPPort>
    <HTTPSPort>integer</HTTPSPort>
    <OriginKeepaliveTimeout>integer</OriginKeepaliveTimeout>
    <OriginProtocolPolicy>string</OriginProtocolPolicy>
    <OriginReadTimeout>integer</OriginReadTimeout>
    <OriginSslProtocols>
     <Items>
      <SslProtocol>string</SslProtocol>
     </Items>
    </OriginSslProtocols>
   </CustomOriginConfig>
    <DomainName>string</DomainName>
   </Origin>
  </Items>
</Origins>
URI Request Parameters

The request does not use any URI parameters.

Request Body

The request accepts the following data in XML format.

**DistributionConfigWithTags (p. 25)**

Root level tag for the DistributionConfigWithTags parameters.

Required: Yes

**DistributionConfig (p. 224)**

A distribution configuration.

Type: DistributionConfig (p. 224) object

Required: Yes
**Tags (p. 25)**

A complex type that contains zero or more Tag elements.

Type: Tags (p. 294) object

Required: Yes

---

**Response Syntax**

```xml
HTTP/1.1 201
<?xml version="1.0" encoding="UTF-8"?>
<Distribution>
   <ActiveTrustedSigners>
      <Enabled>boolean</Enabled>
      <Items>
         <Signer>
            <AwsAccountNumber>string</AwsAccountNumber>
            <KeyPairIds>
               <Items>
                  <KeyPairId>string</KeyPairId>
               </Items>
            </KeyPairIds>
            <Quantity>integer</Quantity>
         </Signer>
      </Items>
      <Quantity>integer</Quantity>
   </ActiveTrustedSigners>
   <ARN>string</ARN>
   <DistributionConfig>
      <Aliases>
         <Items>
            <CNAME>string</CNAME>
         </Items>
      </Aliases>
      <CacheBehaviors>
         <Items>
            <CacheBehavior>
               <AllowedMethods>
                  <CachedMethods>
                     <Items>
                        <Method>string</Method>
                     </Items>
               </CachedMethods>
               <Compress>boolean</Compress>
               <DefaultTTL>long</DefaultTTL>
               <FieldLevelEncryptionId>string</FieldLevelEncryptionId>
               <ForwardedValues>
                  <Cookies>
                     <Forward>string</Forward>
                  </Cookies>
               </ForwardedValues>
               <WhitelistedNames>
                  <Items>
                     <Name>string</Name>
                  </Items>
               </WhitelistedNames>
            </CacheBehavior>
         </Items>
      </CacheBehaviors>
   </DistributionConfig>
</Distribution>
```

API Version 2017-10-30

29
</Cookies>
<Headers>
<Items>
>Name</name><string</Name>
</Items>
<Quantity>integer</Quantity>
</Headers>
<QueryString>boolean</QueryString>
<QueryStringCacheKeys>
<Items>
>Name</name><string</Name>
</Items>
<Quantity>integer</Quantity>
</QueryStringCacheKeys>
</ForwardedValues>
<LambdaFunctionAssociations>
<Items>
<LambdaFunctionAssociation>
<EventType>string</EventType>
<LambdaFunctionARN>string</LambdaFunctionARN>
</LambdaFunctionAssociation>
</Items>
<Quantity>integer</Quantity>
</LambdaFunctionAssociations>
<MaxTTL>long</MaxTTL>
<MinTTL>long</MinTTL>
<PathPattern>string</PathPattern>
<SmoothStreaming>boolean</SmoothStreaming>
<TargetOriginId>string</TargetOriginId>
<TrustedSigners>
<Enabled>boolean</Enabled>
<Items>
<AwsAccountNumber>string</AwsAccountNumber>
</Items>
<Quantity>integer</Quantity>
</TrustedSigners>
</CacheBehavior>
</Items>
<Quantity>integer</Quantity>
</CacheBehaviors>
</CallerReference>string</CallerReference>
</Comment>string</Comment>
</CustomErrorResponses>
<Items>
<CustomErrorResponse>
>ErrorCachingMinTTL>long</ErrorCachingMinTTL>
<ErrorCode>integer</ErrorCode>
<ResponseCode>string</ResponseCode>
<ResponsePagePath>string</ResponsePagePath>
</CustomErrorResponse>
</Items>
<Quantity>integer</Quantity>
</CustomErrorResponses>
</DefaultCacheBehavior>
<AllowedMethods>
</Items>
</AllowedMethods>
<CacheMethods>
<Items>
</Items>
<Quantity>integer</Quantity>
</CacheMethods>
</Items>
</Method>string</Method>
</Items>
<Quantity>integer</Quantity>
</CacheMethods>
</Items>
</Method>string</Method>
</Items>
<Quantity>integer</Quantity>
<AllowedMethods>
<Compress>boolean</Compress>
<DefaultTTL>long</DefaultTTL>
<FieldLevelEncryptionId>string</FieldLevelEncryptionId>
<ForwardedValues>
  <Cookies>
    <Forward>string</Forward>
    <WhitelistedNames>
      <Items>
        <Name>string</Name>
      </Items>
      <Quantity>integer</Quantity>
    </WhitelistedNames>
  </Cookies>
  <Headers>
    <Items>
      <Name>string</Name>
    </Items>
    <Quantity>integer</Quantity>
  </Headers>
  <QueryString>boolean</QueryString>
  <QueryStringCacheKeys>
    <Items>
      <Name>string</Name>
    </Items>
    <Quantity>integer</Quantity>
  </QueryStringCacheKeys>
</ForwardedValues>
<LambdaFunctionAssociations>
  <Items>
    <LambdaFunctionAssociation>
      <EventType>string</EventType>
      <LambdaFunctionARN>string</LambdaFunctionARN>
    </LambdaFunctionAssociation>
  </Items>
  <Quantity>integer</Quantity>
</LambdaFunctionAssociations>
<MaxTTL>long</MaxTTL>
<MinTTL>long</MinTTL>
<SmoothStreaming>boolean</SmoothStreaming>
<TargetOriginId>string</TargetOriginId>
<TrustedSigners>
  <Enabled>boolean</Enabled>
  <Items>
    <AwsAccountNumber>string</AwsAccountNumber>
  </Items>
  <Quantity>integer</Quantity>
</TrustedSigners>
<ViewerProtocolPolicy>string</ViewerProtocolPolicy>
</DefaultCacheBehavior>
<DefaultRootObject>string</DefaultRootObject>
<Enabled>boolean</Enabled>
<HttpVersion>string</HttpVersion>
<IsIPv6Enabled>boolean</IsIPv6Enabled>
<Logging>
  <Bucket>string</Bucket>
  <Enabled>boolean</Enabled>
  <IncludeCookies>boolean</IncludeCookies>
  <Prefix>string</Prefix>
</Logging>
<Origins>
  <Items>
    <Origin>
      <CustomHeaders>
        <Items>
          <OriginCustomHeader>
          </OriginCustomHeader>
        </Items>
      </CustomHeaders>
    </Origin>
  </Items>
</Origins>
Response Elements

If the action is successful, the service sends back an HTTP 201 response.

The following data is returned in XML format by the service.
Distribution (p. 29)

Root level tag for the Distribution parameters.

Required: Yes

ActiveTrustedSigners (p. 29)

CloudFront automatically adds this element to the response only if you've set up the distribution to serve private content with signed URLs. The element lists the key pair IDs that CloudFront is aware of for each trusted signer. The Signer child element lists the AWS account number of the trusted signer (or an empty Self element if the signer is you). The Signer element also includes the IDs of any active key pairs associated with the trusted signer's AWS account. If no KeyPairId element appears for a Signer, that signer can't create working signed URLs.

Type: ActiveTrustedSigners (p. 192) object

ARN (p. 29)

The ARN (Amazon Resource Name) for the distribution. For example:
arn:aws:cloudfront::123456789012:distribution/EDFDVBD632BHDS5, where 123456789012 is your AWS account ID.

Type: String

DistributionConfig (p. 29)

The current configuration information for the distribution. Send a GET request to the /CloudFront API version/distribution ID/config resource.

Type: DistributionConfig (p. 224) object

DomainName (p. 29)

The domain name corresponding to the distribution, for example, d111111abcdef8.cloudfront.net.

Type: String

Id (p. 29)

The identifier for the distribution. For example: EDFDVBD632BHDS5.

Type: String

InProgressInvalidationBatches (p. 29)

The number of invalidation batches currently in progress.

Type: Integer

LastModifiedTime (p. 29)

The date and time the distribution was last modified.

Type: Timestamp

Status (p. 29)

This response element indicates the current status of the distribution. When the status is Deployed, the distribution's information is fully propagated to all CloudFront edge locations.

Type: String

Errors

For information about the errors that are common to all actions, see Common Errors (p. 302).
Errors

AccessDenied

Access denied.

HTTP Status Code: 403

CNAMEAlreadyExists

HTTP Status Code: 409

DistributionAlreadyExists

The caller reference you attempted to create the distribution with is associated with another distribution.

HTTP Status Code: 409

IllegalFieldLevelEncryptionConfigAssociationWithCacheBehavior

The specified configuration for field-level encryption can't be associated with the specified cache behavior.

HTTP Status Code: 400

InconsistentQuantities

The value of Quantity and the size of Items don't match.

HTTP Status Code: 400

InvalidArgument

The argument is invalid.

HTTP Status Code: 400

InvalidDefaultRootObject

The default root object file name is too big or contains an invalid character.

HTTP Status Code: 400

InvalidErrorCode

HTTP Status Code: 400

InvalidForwardCookies

Your request contains forward cookies option which doesn't match with the expectation for the whitelisted list of cookie names. Either list of cookie names has been specified when not allowed or list of cookie names is missing when expected.

HTTP Status Code: 400

InvalidGeoRestrictionParameter

HTTP Status Code: 400

InvalidHeadersForS3Origin

HTTP Status Code: 400

InvalidLambdaFunctionAssociation

The specified Lambda function association is invalid.

HTTP Status Code: 400

InvalidLocationCode

HTTP Status Code: 400
InvalidMinimumProtocolVersion

HTTP Status Code: 400

InvalidOrigin

The Amazon S3 origin server specified does not refer to a valid Amazon S3 bucket.

HTTP Status Code: 400

InvalidOriginAccessIdentity

The origin access identity is not valid or doesn’t exist.

HTTP Status Code: 400

InvalidOriginKeepaliveTimeout

HTTP Status Code: 400

InvalidOriginReadTimeout

HTTP Status Code: 400

InvalidProtocolSettings

You cannot specify SSLv3 as the minimum protocol version if you only want to support only clients that support Server Name Indication (SNI).

HTTP Status Code: 400

InvalidQueryStringParameters

HTTP Status Code: 400

InvalidRelativePath

The relative path is too big, is not URL-encoded, or does not begin with a slash (/).

HTTP Status Code: 400

InvalidRequiredProtocol

This operation requires the HTTPS protocol. Ensure that you specify the HTTPS protocol in your request, or omit the RequiredProtocols element from your distribution configuration.

HTTP Status Code: 400

InvalidResponseCode

HTTP Status Code: 400

InvalidTagging

HTTP Status Code: 400

InvalidTTLOrder

HTTP Status Code: 400

InvalidViewerCertificate

HTTP Status Code: 400

InvalidWebACLId

HTTP Status Code: 400

MissingBody

This operation requires a body. Ensure that the body is present and the Content-Type header is set.
HTTP Status Code: 400
**NoSuchFieldLevelEncryptionConfig**
The specified configuration for field-level encryption doesn't exist.

HTTP Status Code: 404
**NoSuchOrigin**
No origin exists with the specified Origin Id.

HTTP Status Code: 404
**TooManyCacheBehaviors**
You cannot create more cache behaviors for the distribution.

HTTP Status Code: 400
**TooManyCertificates**
You cannot create anymore custom SSL/TLS certificates.

HTTP Status Code: 400
**TooManyCookieNamesInWhiteList**
Your request contains more cookie names in the whitelist than are allowed per cache behavior.

HTTP Status Code: 400
**TooManyDistributionCNAMEs**
Your request contains more CNAMEs than are allowed per distribution.

HTTP Status Code: 400
**TooManyDistributions**
Processing your request would cause you to exceed the maximum number of distributions allowed.

HTTP Status Code: 400
**TooManyDistributionsAssociatedToFieldLevelEncryptionConfig**
The maximum number of distributions have been associated with the specified configuration for field-level encryption.

HTTP Status Code: 400
**TooManyDistributionsWithLambdaAssociations**
Processing your request would cause the maximum number of distributions with Lambda function associations per owner to be exceeded.

HTTP Status Code: 400
**TooManyHeadersInForwardedValues**
HTTP Status Code: 400
**TooManyLambdaFunctionAssociations**
Your request contains more Lambda function associations than are allowed per distribution.

HTTP Status Code: 400
**TooManyOriginCustomHeaders**
HTTP Status Code: 400
TooManyOrigins

You cannot create more origins for the distribution.

HTTP Status Code: 400

TooManyQueryStringParameters

HTTP Status Code: 400

TooManyTrustedSigners

Your request contains more trusted signers than are allowed per distribution.

HTTP Status Code: 400

TrustedSignerDoesNotExist

One or more of your trusted signers don't exist.

HTTP Status Code: 400

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
CreateFieldLevelEncryptionConfig

Create a new field-level encryption configuration.

Request Syntax

POST /2017-10-30/field-level-encryption HTTP/1.1
<?xml version="1.0" encoding="UTF-8"?>
<FieldLevelEncryptionConfig xmlns="http://cloudfront.amazonaws.com/doc/2017-10-30/">
  <CallerReference>string</CallerReference>
  <Comment>string</Comment>
  <ContentTypeProfileConfig>
    <ContentTypeProfiles>
      <Items>
        <ContentTypeProfile>
          <ContentType>string</ContentType>
          <Format>string</Format>
          <ProfileId>string</ProfileId>
        </ContentTypeProfile>
      </Items>
      <Quantity>integer</Quantity>
    </ContentTypeProfiles>
    <ForwardWhenContentTypeIsUnknown>boolean</ForwardWhenContentTypeIsUnknown>
  </ContentTypeProfileConfig>
  <QueryArgProfileConfig>
    <ForwardWhenQueryArgProfileIsUnknown>boolean</ForwardWhenQueryArgProfileIsUnknown>
  </QueryArgProfileConfig>
</FieldLevelEncryptionConfig>

URI Request Parameters

The request does not use any URI parameters.

Request Body

The request accepts the following data in XML format.

FieldLevelEncryptionConfig (p. 38)

Root level tag for the FieldLevelEncryptionConfig parameters.

Required: Yes

CallerReference (p. 38)

A unique number that ensures the request can't be replayed.

Type: String

Required: Yes
Comment (p. 38)

An optional comment about the configuration.

Type: String
Required: No

ContentTypeProfileConfig (p. 38)

A complex data type that specifies when to forward content if a content type isn't recognized and profiles to use as by default in a request if a query argument doesn't specify a profile to use.

Type: ContentTypeProfileConfig (p. 209) object
Required: No

QueryArgProfileConfig (p. 38)

A complex data type that specifies when to forward content if a profile isn't found and the profile that can be provided as a query argument in a request.

Type: QueryArgProfileConfig (p. 275) object
Required: No

Response Syntax

```xml
HTTP/1.1 201
<?xml version="1.0" encoding="UTF-8"?>
<FieldLevelEncryption>
  <FieldLevelEncryptionConfig>
    <CallerReference>string</CallerReference>
    <Comment>string</Comment>
    <ContentTypeProfileConfig>
      <ContentTypeProfiles>
        <Items>
          <ContentTypeProfile>
            <ContentType>string</ContentType>
            <Format>string</Format>
            <ProfileId>string</ProfileId>
          </ContentTypeProfile>
        </Items>
        <Quantity>integer</Quantity>
      </ContentTypeProfiles>
      <ForwardWhenContentTypeIsUnknown>boolean</ForwardWhenContentTypeIsUnknown>
    </ContentTypeProfileConfig>
    <QueryArgProfileConfig>
      <QueryArgProfiles>
        <Items>
          <QueryArgProfile>
            <ProfileId>string</ProfileId>
            <QueryArg>string</QueryArg>
          </QueryArgProfile>
        </Items>
        <Quantity>integer</Quantity>
      </QueryArgProfiles>
    </QueryArgProfileConfig>
  </FieldLevelEncryptionConfig>
  <Id>string</Id>
  <LastModifiedTime>timestamp</LastModifiedTime>
</FieldLevelEncryption>
```

API Version 2017-10-30
Response Elements

If the action is successful, the service sends back an HTTP 201 response.

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

**FieldLevelEncryption (p. 39)**

Root level tag for the FieldLevelEncryption parameters.

Required: Yes

**FieldLevelEncryptionConfig (p. 39)**

A complex data type that includes the profile configurations specified for field-level encryption.

Type: FieldLevelEncryptionConfig (p. 240) object

**Id (p. 39)**

The configuration ID for a field-level encryption configuration which includes a set of profiles that specify certain selected data fields to be encrypted by specific public keys.

Type: String

**LastModifiedTime (p. 39)**

The last time the field-level encryption configuration was changed.

Type: Timestamp

Errors

For information about the errors that are common to all actions, see Common Errors (p. 302).

**FieldLevelEncryptionConfigAlreadyExists**

The specified configuration for field-level encryption already exists.

HTTP Status Code: 409

**InconsistentQuantities**

The value of Quantity and the size of Items don’t match.

HTTP Status Code: 400

**InvalidArgument**

The argument is invalid.

HTTP Status Code: 400

**NoSuchFieldLevelEncryptionProfile**

The specified profile for field-level encryption doesn’t exist.

HTTP Status Code: 404

**QueryArgProfileEmpty**

No profile specified for the field-level encryption query argument.

HTTP Status Code: 400
TooManyFieldLevelEncryptionConfigs

The maximum number of configurations for field-level encryption have been created.

HTTP Status Code: 400

TooManyFieldLevelEncryptionContentTypeProfiles

The maximum number of content type profiles for field-level encryption have been created.

HTTP Status Code: 400

TooManyFieldLevelEncryptionQueryArgProfiles

The maximum number of query arg profiles for field-level encryption have been created.

HTTP Status Code: 400

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
CreateFieldLevelEncryptionProfile

Create a field-level encryption profile.

Request Syntax

POST /2017-10-30/field-level-encryption-profile HTTP/1.1
<?xml version="1.0" encoding="UTF-8"?>
<FieldLevelEncryptionProfileConfig xmlns="http://cloudfront.amazonaws.com/doc/2017-10-30/">
    <CallerReference>string</CallerReference>
    <Comment>string</Comment>
    <EncryptionEntities>
        <Items>
            <EncryptionEntity>
                <FieldPatterns>
                    <Items>
                        <FieldPattern>string</FieldPattern>
                    </Items>
                    <Quantity>integer</Quantity>
                </FieldPatterns>
                <ProviderId>string</ProviderId>
                <PublicKeyId>string</PublicKeyId>
            </EncryptionEntity>
        </Items>
        <Quantity>integer</Quantity>
    </EncryptionEntities>
    <Name>string</Name>
</FieldLevelEncryptionProfileConfig>

URI Request Parameters

The request does not use any URI parameters.

Request Body

The request accepts the following data in XML format.

FieldLevelEncryptionProfileConfig (p. 42)

Root level tag for the FieldLevelEncryptionProfileConfig parameters.

Required: Yes

CallerReference (p. 42)

A unique number that ensures the request can't be replayed.

Type: String

Required: Yes

Comment (p. 42)

An optional comment for the field-level encryption profile.

Type: String

Required: No
**EncryptionEntities (p. 42)**

A complex data type of encryption entities for the field-level encryption profile that include the public key ID, provider, and field patterns for specifying which fields to encrypt with this key.

Type: EncryptionEntities (p. 237) object

Required: Yes

**Name (p. 42)**

Profile name for the field-level encryption profile.

Type: String

Required: Yes

---

**Response Syntax**

```
HTTP/1.1 201
<?xml version="1.0" encoding="UTF-8"?>
<FieldLevelEncryptionProfile>
  <FieldLevelEncryptionProfileConfig>
    <CallerReference>string</CallerReference>
    <Comment>string</Comment>
    <EncryptionEntities>
      <Items>
        <EncryptionEntity>
          <FieldPatterns>
            <Items>
              <FieldPattern>string</FieldPattern>
            </Items>
            <Quantity>integer</Quantity>
          </FieldPatterns>
          <ProviderId>string</ProviderId>
          <PublicKeyId>string</PublicKeyId>
        </EncryptionEntity>
      </Items>
      <Quantity>integer</Quantity>
    </EncryptionEntities>
    <Name>string</Name>
  </FieldLevelEncryptionProfileConfig>
  <Id>string</Id>
  <LastModifiedTime>timestamp</LastModifiedTime>
</FieldLevelEncryptionProfile>
```

---

**Response Elements**

If the action is successful, the service sends back an HTTP 201 response.

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

**FieldLevelEncryptionProfile (p. 43)**

Root level tag for the FieldLevelEncryptionProfile parameters.

Required: Yes

**FieldLevelEncryptionProfileConfig (p. 43)**

A complex data type that includes the profile name and the encryption entities for the field-level encryption profile.
Errors

For information about the errors that are common to all actions, see Common Errors (p. 302).

FieldLevelEncryptionProfileAlreadyExists

The specified profile for field-level encryption already exists.

HTTP Status Code: 409

FieldLevelEncryptionProfileSizeExceeded

The maximum size of a profile for field-level encryption was exceeded.

HTTP Status Code: 400

InconsistentQuantities

The value of Quantity and the size of Items don’t match.

HTTP Status Code: 400

InvalidArgument

The argument is invalid.

HTTP Status Code: 400

NoSuchPublicKey

The specified public key doesn’t exist.

HTTP Status Code: 404

TooManyFieldLevelEncryptionEncryptionEntities

The maximum number of encryption entities for field-level encryption have been created.

HTTP Status Code: 400

TooManyFieldLevelEncryptionFieldPatterns

The maximum number of field patterns for field-level encryption have been created.

HTTP Status Code: 400

TooManyFieldLevelEncryptionProfiles

The maximum number of profiles for field-level encryption have been created.

HTTP Status Code: 400
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
CreateInvalidation

Create a new invalidation.

Request Syntax

```
POST /2017-10-30/distribution/DistributionId/invalidation HTTP/1.1
<?xml version="1.0" encoding="UTF-8"?>
<InvalidationBatch xmlns="http://cloudfront.amazonaws.com/doc/2017-10-30/"
  <CallerReference>string</CallerReference>
  <Paths>
    <Items>
      <Path>string</Path>
    </Items>
    <Quantity>integer</Quantity>
  </Paths>
</InvalidationBatch>
```

URI Request Parameters

The request does not use any URI parameters.

Request Body

The request accepts the following data in XML format.

**InvalidationBatch (p. 46)**

Root level tag for the InvalidationBatch parameters.

Required: Yes

**CallerReference (p. 46)**

A value that you specify to uniquely identify an invalidation request. CloudFront uses the value to prevent you from accidentally resubmitting an identical request. Whenever you create a new invalidation request, you must specify a new value for CallerReference and change other values in the request as applicable. One way to ensure that the value of CallerReference is unique is to use a timestamp, for example, 20120301090000.

If you make a second invalidation request with the same value for CallerReference, and if the rest of the request is the same, CloudFront doesn't create a new invalidation request. Instead, CloudFront returns information about the invalidation request that you previously created with the same CallerReference.

If CallerReference is a value you already sent in a previous invalidation batch request but the content of any Path is different from the original request, CloudFront returns an InvalidationTokenAlreadyExists error.

Type: String

Required: Yes

**Paths (p. 46)**

A complex type that contains information about the objects that you want to invalidate. For more information, see Specifying the Objects to Invalidate in the Amazon CloudFront Developer Guide.

Type: Paths (p. 269) object
Response Syntax

```
HTTP/1.1 201
<?xml version="1.0" encoding="UTF-8"?>
<Invalidation>
  <CreateTime>timestamp</CreateTime>
  <Id>string</Id>
  <InvalidationBatch>
    <CallerReference>string</CallerReference>
    <Paths>
      <Items>
        <Path>string</Path>
      </Items>
      <Quantity>integer</Quantity>
    </Paths>
  </InvalidationBatch>
  <Status>string</Status>
</Invalidation>
```

Response Elements

If the action is successful, the service sends back an HTTP 201 response.

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

**Invalidation (p. 47)**

Root level tag for the Invalidation parameters.

Required: Yes

**CreateTime (p. 47)**

The date and time the invalidation request was first made.

Type: Timestamp

**Id (p. 47)**

The identifier for the invalidation request. For example: IDFDVBD632BHDS5.

Type: String

**InvalidationBatch (p. 47)**

The current invalidation information for the batch request.

Type: InvalidationBatch (p. 255) object

**Status (p. 47)**

The status of the invalidation request. When the invalidation batch is finished, the status is Completed.

Type: String

Errors

For information about the errors that are common to all actions, see Common Errors (p. 302).
AccessDenied
Access denied.
HTTP Status Code: 403

BatchTooLarge
HTTP Status Code: 413

InconsistentQuantities
The value of Quantity and the size of Items don't match.
HTTP Status Code: 400

InvalidArgument
The argument is invalid.
HTTP Status Code: 400

MissingBody
This operation requires a body. Ensure that the body is present and the Content-Type header is set.
HTTP Status Code: 400

NoSuchDistribution
The specified distribution does not exist.
HTTP Status Code: 404

TooManyInvalidationsInProgress
You have exceeded the maximum number of allowable InProgress invalidation batch requests, or invalidation objects.
HTTP Status Code: 400

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
CreatePublicKey

Add a new public key to CloudFront to use, for example, for field-level encryption. You can add a maximum of 10 public keys with one AWS account.

Request Syntax

POST /2017-10-30/public-key HTTP/1.1
<?xml version="1.0" encoding="UTF-8"?>
<PublicKeyConfig xmlns="http://cloudfront.amazonaws.com/doc/2017-10-30/"
  <CallerReference>string</CallerReference>
  <Comment>string</Comment>
  <EncodedKey>string</EncodedKey>
  <Name>string</Name>
</PublicKeyConfig>

URI Request Parameters

The request does not use any URI parameters.

Request Body

The request accepts the following data in XML format.

PublicKeyConfig (p. 49)

Root level tag for the PublicKeyConfig parameters.

Required: Yes

CallerReference (p. 49)

A unique number that ensures the request can't be replayed.

Type: String

Required: Yes

Comment (p. 49)

An optional comment about a public key.

Type: String

Required: No

EncodedKey (p. 49)

The encoded public key that you want to add to CloudFront to use with features like field-level encryption.

Type: String

Required: Yes

Name (p. 49)

The name for a public key you add to CloudFront to use with features like field-level encryption.
Response Syntax

HTTP/1.1 201
<?xml version="1.0" encoding="UTF-8"?>
<PublicKey>
    <CreatedTime>timestamp</CreatedTime>
    <Id>string</Id>
    <PublicKeyConfig>
        <CallerReference>string</CallerReference>
        <Comment>string</Comment>
        <EncodedKey>string</EncodedKey>
        <Name>string</Name>
    </PublicKeyConfig>
</PublicKey>

Response Elements

If the action is successful, the service sends back an HTTP 201 response.

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

PublicKey (p. 50)

Root level tag for the PublicKey parameters.

Required: Yes

CreatedTime (p. 50)

A time you added a public key to CloudFront.

Type: Timestamp

Id (p. 50)

A unique ID assigned to a public key you've added to CloudFront.

Type: String

PublicKeyConfig (p. 50)

A complex data type for a public key you add to CloudFront to use with features like field-level encryption.

Type: PublicKeyConfig (p. 271) object

Errors

For information about the errors that are common to all actions, see Common Errors (p. 302).

InvalidArgument

The argument is invalid.

HTTP Status Code: 400
PublicKeyAlreadyExists

The specified public key already exists.

HTTP Status Code: 409

TooManyPublicKeys

The maximum number of public keys for field-level encryption have been created. To create a new public key, delete one of the existing keys.

HTTP Status Code: 400

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
CreateStreamingDistribution

Create a new RTMP distribution. An RTMP distribution is similar to a web distribution, but an RTMP distribution streams media files using the Adobe Real-Time Messaging Protocol (RTMP) instead of serving files using HTTP.

To create a new web distribution, submit a POST request to the CloudFront API version/distribution resource. The request body must include a document with a StreamingDistributionConfig element. The response echoes the StreamingDistributionConfig element and returns other information about the RTMP distribution.

To get the status of your request, use the GET StreamingDistribution API action. When the value of Enabled is true and the value of Status is Deployed, your distribution is ready. A distribution usually deploys in less than 15 minutes.

For more information about web distributions, see Working with RTMP Distributions in the Amazon CloudFront Developer Guide.

Important
Beginning with the 2012-05-05 version of the CloudFront API, we made substantial changes to the format of the XML document that you include in the request body when you create or update a web distribution or an RTMP distribution, and when you invalidate objects. With previous versions of the API, we discovered that it was too easy to accidentally delete one or more values for an element that accepts multiple values, for example, CNAMEs and trusted signers. Our changes for the 2012-05-05 release are intended to prevent these accidental deletions and to notify you when there's a mismatch between the number of values you say you're specifying in the quantity element and the number of values specified.

Request Syntax

```xml
POST /2017-10-30/streaming-distribution HTTP/1.1
<?xml version="1.0" encoding="UTF-8"?>
<StreamingDistributionConfig xmlns="http://cloudfront.amazonaws.com/doc/2017-10-30/"
    xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
    xsi:schemaLocation="http://cloudfront.amazonaws.com/doc/2017-10-30/">
    <Aliases>
        <Items>
            <CNAME>string</CNAME>
        </Items>
        <Quantity>integer</Quantity>
    </Aliases>
    <CallerReference>string</CallerReference>
    <Comment>string</Comment>
    <Enabled>boolean</Enabled>
    <Logging>
        <Bucket>string</Bucket>
        <Enabled>boolean</Enabled>
        <Prefix>string</Prefix>
    </Logging>
    <PriceClass>string</PriceClass>
    <S3Origin>
        <DomainName>string</DomainName>
        <OriginAccessIdentity>string</OriginAccessIdentity>
    </S3Origin>
    <TrustedSigners>
        <Enabled>boolean</Enabled>
        <Items>
            <AwsAccountNumber>string</AwsAccountNumber>
        </Items>
        <Quantity>integer</Quantity>
    </TrustedSigners>
</StreamingDistributionConfig>
```
URI Request Parameters

The request does not use any URI parameters.

Request Body

The request accepts the following data in XML format.

StreamingDistributionConfig (p. 52)

  Root level tag for the StreamingDistributionConfig parameters.

  Required: Yes

Aliases (p. 52)

  A complex type that contains information about CNAMEs (alternate domain names), if any, for this
  streaming distribution.

  Type: Aliases (p. 194) object

  Required: No

CallerReference (p. 52)

  A unique number that ensures that the request can't be replayed. If the CallerReference is new
  (no matter the content of the StreamingDistributionConfig object), a new streaming distribution is created. If the CallerReference is a value that you already
  sent in a previous request to create a streaming distribution, and the content of the
  StreamingDistributionConfig is identical to the original request (ignoring white space), the
  response includes the same information returned to the original request. If the CallerReference is a value that you already sent in a previous request to create a streaming distribution but the
  content of the StreamingDistributionConfig is different from the original request, CloudFront
  returns a DistributionAlreadyExists error.

  Type: String

  Required: Yes

Comment (p. 52)

  Any comments you want to include about the streaming distribution.

  Type: String

  Required: Yes

Enabled (p. 52)

  Whether the streaming distribution is enabled to accept user requests for content.

  Type: Boolean

  Required: Yes

Logging (p. 52)

  A complex type that controls whether access logs are written for the streaming distribution.

  Type: StreamingLoggingConfig (p. 291) object

  Required: No
PriceClass (p. 52)

A complex type that contains information about price class for this streaming distribution.

Type: String

Valid Values: PriceClass_100 | PriceClass_200 | PriceClass_All

Required: No

S3Origin (p. 52)

A complex type that contains information about the Amazon S3 bucket from which you want CloudFront to get your media files for distribution.

Type: S3Origin (p. 279) object

Required: Yes

TrustedSigners (p. 52)

A complex type that specifies any AWS accounts that you want to permit to create signed URLs for private content. If you want the distribution to use signed URLs, include this element; if you want the distribution to use public URLs, remove this element. For more information, see Serving Private Content through CloudFront in the Amazon CloudFront Developer Guide.

Type: TrustedSigners (p. 295) object

Required: Yes

Response Syntax

HTTP/1.1 201
<?xml version="1.0" encoding="UTF-8"?>
<StreamingDistribution>
  <ActiveTrustedSigners>
    <Enabled>boolean</Enabled>
    <Items>
      <Signer>
        <AwsAccountNumber>string</AwsAccountNumber>
        <KeyPairIds>
          <Items>
            <KeyPairId>string</KeyPairId>
          </Items>
          <Quantity>integer</Quantity>
        </KeyPairIds>
      </Signer>
    </Items>
    <Quantity>integer</Quantity>
  </ActiveTrustedSigners>
  <ARN>string</ARN>
  <DomainName>string</DomainName>
  <Id>string</Id>
  <LastModifiedTime>timestamp</LastModifiedTime>
  <Status>string</Status>
  <StreamingDistributionConfig>
    <Aliases>
      <Items>
        <CNAME>string</CNAME>
      </Items>
      <Quantity>integer</Quantity>
    </Aliases>
    <CallerReference>string</CallerReference>
Response Elements

If the action is successful, the service sends back an HTTP 201 response.

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

**StreamingDistribution (p. 54)**

Root level tag for the StreamingDistribution parameters.

Required: Yes

**ActiveTrustedSigners (p. 54)**

A complex type that lists the AWS accounts, if any, that you included in the TrustedSigners complex type for this distribution. These are the accounts that you want to allow to create signed URLs for private content.

The Signer complex type lists the AWS account number of the trusted signer or self if the signer is the AWS account that created the distribution. The Signer element also includes the IDs of any active CloudFront key pairs that are associated with the trusted signer's AWS account. If no KeyPairId element appears for a Signer, that signer can't create signed URLs.

For more information, see Serving Private Content through CloudFront in the Amazon CloudFront Developer Guide.

Type: ActiveTrustedSigners (p. 192) object

**ARN (p. 54)**

Type: String

**DomainName (p. 54)**

The domain name that corresponds to the streaming distribution, for example, s5c39gqb8ow64r.cloudfront.net.

Type: String

**Id (p. 54)**

The identifier for the RTMP distribution. For example: EGTXBD79EXAMPLE.
Type: String

**LastModifiedTime (p. 54)**

The date and time that the distribution was last modified.

Type: Timestamp

**Status (p. 54)**

The current status of the RTMP distribution. When the status is deployed, the distribution’s information is propagated to all CloudFront edge locations.

Type: String

**StreamingDistributionConfig (p. 54)**

The current configuration information for the RTMP distribution.

Type: `StreamingDistributionConfig (p. 284)` object

---

**Errors**

For information about the errors that are common to all actions, see Common Errors (p. 302).

**AccessDenied**

Access denied.

HTTP Status Code: 403

**CNAMEAlreadyExists**

HTTP Status Code: 409

**InconsistentQuantities**

The value of `Quantity` and the size of `Items` don’t match.

HTTP Status Code: 400

**InvalidArgument**

The argument is invalid.

HTTP Status Code: 400

**InvalidOrigin**

The Amazon S3 origin server specified does not refer to a valid Amazon S3 bucket.

HTTP Status Code: 400

**InvalidOriginAccessIdentity**

The origin access identity is not valid or doesn’t exist.

HTTP Status Code: 400

**MissingBody**

This operation requires a body. Ensure that the body is present and the `Content-Type` header is set.

HTTP Status Code: 400
StreamingDistributionAlreadyExists

HTTP Status Code: 409

TooManyStreamingDistributionCNAMEs

HTTP Status Code: 400

TooManyStreamingDistributions

Processing your request would cause you to exceed the maximum number of streaming distributions allowed.

HTTP Status Code: 400

TooManyTrustedSigners

Your request contains more trusted signers than are allowed per distribution.

HTTP Status Code: 400

TrustedSignerDoesNotExist

One or more of your trusted signers don't exist.

HTTP Status Code: 400

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
CreateStreamingDistributionWithTags

Create a new streaming distribution with tags.

**Request Syntax**

```xml
POST /2017-10-30/streaming-distribution?WithTags HTTP/1.1
<?xml version="1.0" encoding="UTF-8"?>
<StreamingDistributionConfigWithTags xmlns="http://cloudfront.amazonaws.com/doc/2017-10-30/">
  <StreamingDistributionConfig>
    <Aliases>
      <Items>
        <CNAME>string</CNAME>
      </Items>
    </Aliases>
    <CallerReference>string</CallerReference>
    <Comment>string</Comment>
    <Enabled>boolean</Enabled>
    <Logging>
      <Bucket>string</Bucket>
      <Enabled>boolean</Enabled>
      <Prefix>string</Prefix>
    </Logging>
    <PriceClass>string</PriceClass>
    <S3Origin>
      <DomainName>string</DomainName>
    </S3Origin>
    <TrustedSigners>
      <Enabled>boolean</Enabled>
      <Items>
        <AwsAccountNumber>string</AwsAccountNumber>
      </Items>
    </TrustedSigners>
  </StreamingDistributionConfig>
  <Tags>
    <Items>
      <Tag>
        <Key>string</Key>
        <Value>string</Value>
      </Tag>
    </Items>
  </Tags>
</StreamingDistributionConfigWithTags>
```

**URI Request Parameters**

The request does not use any URI parameters.

**Request Body**

The request accepts the following data in XML format.

**StreamingDistributionConfigWithTags (p. 58)**

Root level tag for the StreamingDistributionConfigWithTags parameters.
Required: Yes

**StreamingDistributionConfig (p. 58)**

A streaming distribution configuration.

Type: **StreamingDistributionConfig (p. 284)** object

Required: Yes

**Tags (p. 58)**

A complex type that contains zero or more `<Tag>` elements.

Type: **Tags (p. 294)** object

Required: Yes

**Response Syntax**

```
HTTP/1.1 201
<?xml version="1.0" encoding="UTF-8"?>
<StreamingDistribution>
  <ActiveTrustedSigners>
    <Enabled>boolean</Enabled>
    <Items>
      <Signer>
        <AwsAccountNumber>string</AwsAccountNumber>
        <KeyPairIds>
          <Items>
            <KeyPairId>string</KeyPairId>
          </Items>
        </KeyPairIds>
        <Quantity>integer</Quantity>
      </Signer>
    </Items>
  </ActiveTrustedSigners>
  <ARN>string</ARN>
  <DomainName>string</DomainName>
  <Id>string</Id>
  <LastModifiedTime>timestamp</LastModifiedTime>
  <Status>string</Status>
  <StreamingDistributionConfig>
    <Aliases>
      <Items>
        <CNAME>string</CNAME>
      </Items>
    </Aliases>
    <CallerReference>string</CallerReference>
    <Comment>string</Comment>
    <Enabled>boolean</Enabled>
    <Logging>
      <Bucket>string</Bucket>
      <Enabled>boolean</Enabled>
      <Prefix>string</Prefix>
    </Logging>
    <PriceClass>string</PriceClass>
    <S3Origin>
      <DomainName>string</DomainName>
      <OriginAccessIdentity>string</OriginAccessIdentity>
    </S3Origin>
    <TrustedSigners>
```

API Version 2017-10-30
Response Elements

If the action is successful, the service sends back an HTTP 201 response.

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

**StreamingDistribution (p. 59)**

Root level tag for the StreamingDistribution parameters.

Required: Yes

**ActiveTrustedSigners (p. 59)**

A complex type that lists the AWS accounts, if any, that you included in the TrustedSigners complex type for this distribution. These are the accounts that you want to allow to create signed URLs for private content.

The Signer complex type lists the AWS account number of the trusted signer or self if the signer is the AWS account that created the distribution. The Signer element also includes the IDs of any active CloudFront key pairs that are associated with the trusted signer's AWS account. If no KeyPairId element appears for a Signer, that signer can't create signed URLs.

For more information, see Serving Private Content through CloudFront in the *Amazon CloudFront Developer Guide*.

Type: ActiveTrustedSigners (p. 192) object

**ARN (p. 59)**

Type: String

**DomainName (p. 59)**

The domain name that corresponds to the streaming distribution, for example, s5c39gb8ow64r.cloudfront.net.

Type: String

**Id (p. 59)**

The identifier for the RTMP distribution. For example: EGTXBD79EXAMPLE.

Type: String

**LastModifiedTime (p. 59)**

The date and time that the distribution was last modified.

Type: Timestamp

**Status (p. 59)**

The current status of the RTMP distribution. When the status is Deployed, the distribution's information is propagated to all CloudFront edge locations.
Type: String

`StreamingDistributionConfig (p. 59)`

The current configuration information for the RTMP distribution.

Type: `StreamingDistributionConfig (p. 284)` object

---

**Errors**

For information about the errors that are common to all actions, see [Common Errors (p. 302)](#).

**AccessDenied**

Access denied.

HTTP Status Code: 403

**CNAMEAlreadyExists**

HTTP Status Code: 409

**InconsistentQuantities**

The value of `Quantity` and the size of `Items` don't match.

HTTP Status Code: 400

**InvalidArgument**

The argument is invalid.

HTTP Status Code: 400

**InvalidOrigin**

The Amazon S3 origin server specified does not refer to a valid Amazon S3 bucket.

HTTP Status Code: 400

**InvalidOriginAccessIdentity**

The origin access identity is not valid or doesn't exist.

HTTP Status Code: 400

**InvalidTagging**

HTTP Status Code: 400

**MissingBody**

This operation requires a body. Ensure that the body is present and the `Content-Type` header is set.

HTTP Status Code: 400

**StreamingDistributionAlreadyExists**

HTTP Status Code: 409

**TooManyStreamingDistributionCNAMEs**

HTTP Status Code: 400

**TooManyStreamingDistributions**

Processing your request would cause you to exceed the maximum number of streaming distributions allowed.
HTTP Status Code: 400

**TooManyTrustedSigners**

Your request contains more trusted signers than are allowed per distribution.

HTTP Status Code: 400

**TrustedSignerDoesNotExist**

One or more of your trusted signers don't exist.

HTTP Status Code: 400

---

**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
DeleteCloudFrontOriginAccessIdentity

Delete an origin access identity.

Request Syntax

DELETE /2017-10-30/origin-access-identity/cloudfront/Id HTTP/1.1
If-Match: IfMatch

URI Request Parameters

The request requires the following URI parameters.

Id (p. 63)

The origin access identity's ID.

If-Match (p. 63)

The value of the ETag header you received from a previous GET or PUT request. For example: E2QWRSAPMQW9L.

Request Body

The request does not have a request body.

Response Syntax

HTTP/1.1 204

Response Elements

If the action is successful, the service sends back an HTTP 204 response with an empty HTTP body.

Errors

For information about the errors that are common to all actions, see Common Errors (p. 302).

AccessDenied

Access denied.

HTTP Status Code: 403

CloudFrontOriginAccessIdentityInUse

HTTP Status Code: 409

InvalidIfMatchVersion

The If-Match version is missing or not valid for the distribution.

HTTP Status Code: 400
NoSuchCloudFrontOriginAccessIdentity

The specified origin access identity does not exist.

HTTP Status Code: 404

PreconditionFailed

The precondition given in one or more of the request-header fields evaluated to false.

HTTP Status Code: 412

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
DeleteDistribution

Delete a distribution.

Request Syntax

```plaintext
DELETE /2017-10-30/distribution/Id HTTP/1.1
If-Match: IfMatch
```

URI Request Parameters

The request requires the following URI parameters.

Id (p. 65)

The distribution ID.

If-Match (p. 65)

The value of the `ETag` header that you received when you disabled the distribution. For example: `E2QWRIHAPOMQZL`.

Request Body

The request does not have a request body.

Response Syntax

```
HTTP/1.1 204
```

Response Elements

If the action is successful, the service sends back an HTTP 204 response with an empty HTTP body.

Errors

For information about the errors that are common to all actions, see Common Errors (p. 302).

AccessDenied

Access denied.

HTTP Status Code: 403

DistributionNotDisabled

HTTP Status Code: 409

InvalidIfMatchVersion

The `If-Match` version is missing or not valid for the distribution.

HTTP Status Code: 400
Unexpected error encountered while processing request.

**NoSuchDistribution**

The specified distribution does not exist.

HTTP Status Code: 404

**PreconditionFailed**

The precondition given in one or more of the request-header fields evaluated to false.

HTTP Status Code: 412

---

**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
DeleteFieldLevelEncryptionConfig

Remove a field-level encryption configuration.

Request Syntax

DELETE /2017-10-30/field-level-encryption/Id HTTP/1.1
If-Match: IfMatch

URI Request Parameters

The request requires the following URI parameters.

Id (p. 67)

The ID of the configuration you want to delete from CloudFront.

If-Match (p. 67)

The value of the ETag header that you received when retrieving the configuration identity to delete. For example: E2QWRUHAPOMQZL.

Request Body

The request does not have a request body.

Response Syntax

HTTP/1.1 204

Response Elements

If the action is successful, the service sends back an HTTP 204 response with an empty HTTP body.

Errors

For information about the errors that are common to all actions, see Common Errors (p. 302).

AccessDenied

Access denied.

HTTP Status Code: 403

FieldLevelEncryptionConfigInUse

The specified configuration for field-level encryption is in use.

HTTP Status Code: 409

InvalidIfMatchVersion

The If-Match version is missing or not valid for the distribution.
HTTP Status Code: 400

**NoSuchFieldLevelEncryptionConfig**

The specified configuration for field-level encryption doesn't exist.

HTTP Status Code: 404

**PreconditionFailed**

The precondition given in one or more of the request-header fields evaluated to false.

HTTP Status Code: 412

**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
DeleteFieldLevelEncryptionProfile

Remove a field-level encryption profile.

**Request Syntax**

```
DELETE /2017-10-30/field-level-encryption-profile/{id} HTTP/1.1
If-Match: {IfMatch}
```

**URI Request Parameters**

The request requires the following URI parameters.

- **Id (p. 69)**
  
  Request the ID of the profile you want to delete from CloudFront.

- **If-Match (p. 69)**
  
  The value of the ETag header that you received when retrieving the profile to delete. For example: E2QWRUHAPMQZL.

**Request Body**

The request does not have a request body.

**Response Syntax**

```
HTTP/1.1 204
```

**Response Elements**

If the action is successful, the service sends back an HTTP 204 response with an empty HTTP body.

**Errors**

For information about the errors that are common to all actions, see Common Errors (p. 302).

- **AccessDenied**
  
  Access denied.
  
  HTTP Status Code: 403

- **FieldLevelEncryptionProfileInUse**
  
  The specified profile for field-level encryption is in use.
  
  HTTP Status Code: 409

- **InvalidIfMatchVersion**
  
  The If-Match version is missing or not valid for the distribution.
HTTP Status Code: 400

**NoSuchFieldLevelEncryptionProfile**

The specified profile for field-level encryption doesn’t exist.

HTTP Status Code: 404

**PreconditionFailed**

The precondition given in one or more of the request-header fields evaluated to false.

HTTP Status Code: 412

**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
DeletePublicKey

Remove a public key you previously added to CloudFront.

Request Syntax

DELETE /2017-10-30/public-key/Id HTTP/1.1
If-Match: IfMatch

URI Request Parameters

The request requires the following URI parameters.

Id (p. 71)

The ID of the public key you want to remove from CloudFront.

If-Match (p. 71)

The value of the ETag header that you received when retrieving the public key identity to delete. For example: E2QNEUHAPMQZL.

Request Body

The request does not have a request body.

Response Syntax

HTTP/1.1 204

Response Elements

If the action is successful, the service sends back an HTTP 204 response with an empty HTTP body.

Errors

For information about the errors that are common to all actions, see Common Errors (p. 302).

AccessDenied

Access denied.

HTTP Status Code: 403

InvalidIfMatchVersion

The If-Match version is missing or not valid for the distribution.

HTTP Status Code: 400

NoSuchPublicKey

The specified public key doesn't exist.
HTTP Status Code: 404

_PreconditionFailed_

The precondition given in one or more of the request-header fields evaluated to false.

HTTP Status Code: 412

_PublicKeyInUse_

The specified public key is in use.

HTTP Status Code: 409

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
DeleteStreamingDistribution

Delete a streaming distribution. To delete an RTMP distribution using the CloudFront API, perform the following steps.

**To delete an RTMP distribution using the CloudFront API:**

1. Disable the RTMP distribution.
2. Submit a GET Streaming Distribution Config request to get the current configuration and the Etag header for the distribution.
3. Update the XML document that was returned in the response to your GET Streaming Distribution Config request to change the value of Enabled to false.
4. Submit a PUT Streaming Distribution Config request to update the configuration for your distribution. In the request body, include the XML document that you updated in Step 3. Then set the value of the HTTP If-Match header to the value of the ETag header that CloudFront returned when you submitted the GET Streaming Distribution Config request in Step 2.
5. Review the response to the PUT Streaming Distribution Config request to confirm that the distribution was successfully disabled.
6. Submit a GET Streaming Distribution Config request to confirm that your changes have propagated. When propagation is complete, the value of Status is Deployed.
7. Submit a DELETE Streaming Distribution request. Set the value of the HTTP If-Match header to the value of the ETag header that CloudFront returned when you submitted the GET Streaming Distribution Config request in Step 2.
8. Review the response to your DELETE Streaming Distribution request to confirm that the distribution was successfully deleted.

For information about deleting a distribution using the CloudFront console, see Deleting a Distribution in the Amazon CloudFront Developer Guide.

**Request Syntax**

```
DELETE /2017-10-30/streaming-distribution/Id HTTP/1.1
If-Match: IfMatch
```

**URI Request Parameters**

The request requires the following URI parameters.

**Id (p. 73)**

The distribution ID.

**If-Match (p. 73)**

The value of the ETag header that you received when you disabled the streaming distribution. For example: EZQWRUHAPOMQZL.

**Request Body**

The request does not have a request body.
Response Syntax

HTTP/1.1 204

Response Elements

If the action is successful, the service sends back an HTTP 204 response with an empty HTTP body.

Errors

For information about the errors that are common to all actions, see Common Errors (p. 302).

AccessDenied

Access denied.

HTTP Status Code: 403

InvalidIfMatchVersion

The If-Match version is missing or not valid for the distribution.

HTTP Status Code: 400

NoSuchStreamingDistribution

The specified streaming distribution does not exist.

HTTP Status Code: 404

PreconditionFailed

The precondition given in one or more of the request-header fields evaluated to false.

HTTP Status Code: 412

StreamingDistributionNotDisabled

HTTP Status Code: 409

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
GetCloudFrontOriginAccessIdentity

Get the information about an origin access identity.

Request Syntax

GET /2017-10-30/origin-access-identity/cloudfront/Id HTTP/1.1

URI Request Parameters

The request requires the following URI parameters.

Id (p. 75)

The identity's ID.

Request Body

The request does not have a request body.

Response Syntax

HTTP/1.1 200
<?xml version="1.0" encoding="UTF-8"?>
<CloudFrontOriginAccessIdentity>
  <CloudFrontOriginAccessIdentityConfig>
    <CallerReference>string</CallerReference>
    <Comment>string</Comment>
  </CloudFrontOriginAccessIdentityConfig>
  <Id>string</Id>
  <S3CanonicalUserId>string</S3CanonicalUserId>
</CloudFrontOriginAccessIdentity>

Response Elements

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

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

CloudFrontOriginAccessIdentity (p. 75)

Root level tag for the CloudFrontOriginAccessIdentity parameters.

Required: Yes

CloudFrontOriginAccessIdentityConfig (p. 75)

The current configuration information for the identity.

Type: CloudFrontOriginAccessIdentityConfig (p. 204) object

Id (p. 75)

The ID for the origin access identity, for example, E74FTE3AJFJ256A.
Type: String

**S3CanonicalUserId (p. 75)**

The Amazon S3 canonical user ID for the origin access identity, used when giving the origin access identity read permission to an object in Amazon S3.

Type: String

---

**Errors**

For information about the errors that are common to all actions, see Common Errors (p. 302).

**AccessDenied**

Access denied.

HTTP Status Code: 403

**NoSuchCloudFrontOriginAccessIdentity**

The specified origin access identity does not exist.

HTTP Status Code: 404

---

**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
GetCloudFrontOriginAccessIdentityConfig

Get the configuration information about an origin access identity.

**Request Syntax**

```
GET /2017-10-30/origin-access-identity/cloudfront/Id/config HTTP/1.1
```

**URI Request Parameters**

The request requires the following URI parameters.

Id (p. 77)

The identity's ID.

**Request Body**

The request does not have a request body.

**Response Syntax**

```
HTTP/1.1 200
<?xml version="1.0" encoding="UTF-8"?>
<CloudFrontOriginAccessIdentityConfig>
  <CallerReference>string</CallerReference>
  <Comment>string</Comment>
</CloudFrontOriginAccessIdentityConfig>
```

**Response Elements**

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

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

CloudFrontOriginAccessIdentityConfig (p. 77)

Root level tag for the CloudFrontOriginAccessIdentityConfig parameters.

Required: Yes

**CallerReference (p. 77)**

A unique number that ensures the request can't be replayed.

If the CallerReference is new (no matter the content of the CloudFrontOriginAccessIdentityConfig object), a new origin access identity is created.

If the CallerReference is a value already sent in a previous identity request, and the content of the CloudFrontOriginAccessIdentityConfig is identical to the original request (ignoring white space), the response includes the same information returned to the original request.

If the CallerReference is a value you already sent in a previous request to create an identity, but the content of the CloudFrontOriginAccessIdentityConfig is different from the original request, CloudFront returns a CloudFrontOriginAccessIdentityAlreadyExists error.
Type: String

Comment (p. 77)

Any comments you want to include about the origin access identity.

Type: String

Errors

For information about the errors that are common to all actions, see Common Errors (p. 302).

AccessDenied

Access denied.

HTTP Status Code: 403

NoSuchCloudFrontOriginAccessIdentity

The specified origin access identity does not exist.

HTTP Status Code: 404

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
GetDistribution

Get the information about a distribution.

Request Syntax

```
GET /2017-10-30/distribution/Id HTTP/1.1
```

URI Request Parameters

The request requires the following URI parameters.

Id (p. 79)

The distribution's ID.

Request Body

The request does not have a request body.

Response Syntax

```
HTTP/1.1 200
<?xml version="1.0" encoding="UTF-8"?>
<Distribution>
  <ActiveTrustedSigners>
    <Enabled>boolean</Enabled>
    <Items>
      <Signer>
        <AwsAccountNumber>string</AwsAccountNumber>
        <KeyPairIds>
          <Items>
            <KeyPairId>string</KeyPairId>
          </Items>
        </KeyPairIds>
        <Quantity>integer</Quantity>
      </Signer>
    </Items>
    <Quantity>integer</Quantity>
  </ActiveTrustedSigners>
  <ARN>string</ARN>
  <DistributionConfig>
    <Aliases>
      <Items>
        <CNAME>string</CNAME>
      </Items>
    </Aliases>
  </DistributionConfig>
</Distribution>
```
<Quantity>integer</Quantity>
</CachedMethods>
<Items>
  <Method>string</Method>
</Items>
<Quantity>integer</Quantity>
</AllowedMethods>
<Compress>boolean</Compress>
<DefaultTTL>long</DefaultTTL>
<FieldLevelEncryptionId>string</FieldLevelEncryptionId>
<ForwardedValues>
  <Cookies>
    <Forward>string</Forward>
  </Cookies>
  <WhitelistedNames>
    <Items>
      <Name>string</Name>
    </Items>
    <Quantity>integer</Quantity>
  </WhitelistedNames>
  <Headers>
    <Items>
      <Name>string</Name>
    </Items>
    <Quantity>integer</Quantity>
  </Headers>
  <QueryStrings>boolean</QueryStrings>
  <QueryStringCacheKeys>
    <Items>
      <Name>string</Name>
    </Items>
    <Quantity>integer</Quantity>
  </QueryStringCacheKeys>
</ForwardedValues>
<LambdaFunctionAssociations>
  <Items>
    <LambdaFunctionAssociation>
      <EventType>string</EventType>
      <LambdaFunctionARN>string</LambdaFunctionARN>
    </LambdaFunctionAssociation>
    <Quantity>integer</Quantity>
  </LambdaFunctionAssociations>
<MaxTTL>long</MaxTTL>
<MinTTL>long</MinTTL>
<PathPattern>string</PathPattern>
<SmoothStreaming>boolean</SmoothStreaming>
<TargetOriginId>string</TargetOriginId>
<TrustedSigners>
  <Enabled>boolean</Enabled>
  <Items>
    <AwsAccountNumber>string</AwsAccountNumber>
  </Items>
  <Quantity>integer</Quantity>
</TrustedSigners>
<ViewerProtocolPolicy>string</ViewerProtocolPolicy>
</CacheBehavior>
</CacheBehaviors>
<CallerReference>string</CallerReference>
<Comment>string</Comment>
<CustomErrorResponses>
  <Items>
    <CustomErrorResponse>
      <ErrorCachingMinTTL>long</ErrorCachingMinTTL>
    </CustomErrorResponse>
    <Quantity>integer</Quantity>
  </Items>
</CustomErrorResponses>

API Version 2017-10-30

80
</TrustedSigners>
</ViewerProtocolPolicy>
</DefaultCacheBehavior>
</DefaultRootObject>
</Enabled>
</HttpVersion>
</IsIPV6Enabled>
</Logging>
</Bucket>
</Enabled>
</IncludeCookies>
</Prefix>
</Logging>
</Origins>
</Items>
<Origin>
<CustomHeaders>
<Items>
<OriginCustomHeader>
<HeaderName>
</HeaderValue>
</OriginCustomHeader>
</Items>
</CustomHeaders>
</CustomOriginConfig>
</DomainName>
</Id>
</OriginPath>
</S3OriginConfig>
</OriginAccessIdentity>
</S3OriginConfig>
</Origin>
</Origins>
</PriceClass>
</Restrictions>
</GeoRestriction>
</Restrictions>
</ViewerCertificate>
</ACMCertificateArn>
</Certificate>
</CertificateSource>
</CloudFrontDefaultCertificate>
</IAMCertificateId>
</MinimumProtocolVersion>
</SSLSupportMethod>
API Version 2017-10-30
82
### Response Elements

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

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

**Distribution (p. 79)**

- Root level tag for the Distribution parameters.
- Required: Yes

**ActiveTrustedSigners (p. 79)**

CloudFront automatically adds this element to the response only if you've set up the distribution to serve private content with signed URLs. The element lists the key pair IDs that CloudFront is aware of for each trusted signer. The `Signer` child element lists the AWS account number of the trusted signer (or an empty `Self` element if the signer is you). The `Signer` element also includes the IDs of any active key pairs associated with the trusted signer's AWS account. If no `KeyPairId` element appears for a `Signer`, that signer can't create working signed URLs.

- Type: `ActiveTrustedSigners (p. 192)` object

**ARN (p. 79)**

- The ARN (Amazon Resource Name) for the distribution. For example: `arn:aws:cloudfront::123456789012:distribution/EDFDVBD632BHDS5`, where `123456789012` is your AWS account ID.

- Type: String

**DistributionConfig (p. 79)**

- The current configuration information for the distribution. Send a GET request to the `/CloudFront API version/distribution ID/config` resource.

- Type: `DistributionConfig (p. 224)` object

**DomainName (p. 79)**

- The domain name corresponding to the distribution, for example, `d111111abcdef8.cloudfront.net`.

- Type: String

**Id (p. 79)**

- The identifier for the distribution. For example: `EDFDVBD632BHDS5`.

- Type: String

**InProgressInvalidationBatches (p. 79)**

- The number of invalidation batches currently in progress.
Errors

For information about the errors that are common to all actions, see Common Errors (p. 302).

AccessDenied

Access denied.

HTTP Status Code: 403

NoSuchDistribution

The specified distribution does not exist.

HTTP Status Code: 404

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
GetDistributionConfig

Get the configuration information about a distribution.

**Request Syntax**

```
GET /2017-10-30/distribution/Id/config HTTP/1.1
```

**URI Request Parameters**

The request requires the following URI parameters.

*Id* (p. 85)

The distribution's ID.

**Request Body**

The request does not have a request body.

**Response Syntax**

```
HTTP/1.1 200
<?xml version="1.0" encoding="UTF-8"?>
<DistributionConfig>
  <Aliases>
    <Items>
      <CNAME>string</CNAME>
    </Items>
    <Quantity>integer</Quantity>
  </Aliases>
  <CacheBehaviors>
    <Items>
      <Method>string</Method>
      <Quantity>integer</Quantity>
    </Items>
    <CachedMethods>
      <Items>
        <Method>string</Method>
        <Quantity>integer</Quantity>
      </Items>
      <AllowedMethods>
        <Items>
          <Method>string</Method>
          <Quantity>integer</Quantity>
        </Items>
        <Compress>boolean</Compress>
        <DefaultTTL>long</DefaultTTL>
      </CachedMethods>
      <ForwardedValues>
        <Cookies>
          <Forward>string</Forward>
        </Cookies>
        <WhitelistedNames>
          <Items>
            <Name>string</Name>
          </Items>
        </WhitelistedNames>
      </ForwardedValues>
      <FieldLevelEncryptionId>string</FieldLevelEncryptionId>
    </Items>
  </CacheBehaviors>
  <DefaultTTL>long</DefaultTTL>
  <FieldLevelEncryptionId>string</FieldLevelEncryptionId>
  <Id>Id</Id>
```

API Version 2017-10-30

85
<Quantity>integer</Quantity>
</WhitelistedNames>
</Cookies>
</Headers>
<Items>
  <Name>string</Name>
</Items>
</Headers>
</QueryStrings>
<QueryStringCacheKeys>
<Items>
  <Name>string</Name>
</Items>
</QueryStringCacheKeys>
</ForwardedValues>
</LambdaFunctionAssociations>
<Items>
  <LambdaFunctionAssociation>
    <EventType>string</EventType>
    <LambdaFunctionARN>string</LambdaFunctionARN>
  </LambdaFunctionAssociation>
</Items>
</LambdaFunctionAssociations>
<MaxTTL>long</MaxTTL>
<MinTTL>long</MinTTL>
<PathPattern>string</PathPattern>
<SmoothStreaming>boolean</SmoothStreaming>
<TargetOriginId>string</TargetOriginId>
<TrustedSigners>
  <Enabled>boolean</Enabled>
  <Items>
    <AwsAccountNumber>string</AwsAccountNumber>
  </Items>
</TrustedSigners>
</ViewerProtocolPolicy>
</CacheBehavior>
</Items>
</CacheBehaviors>
<CallerReference>string</CallerReference>
<Comment>string</Comment>
</CustomErrorResponses>
<Items>
  <CustomErrorResponse>
    <ErrorCachingMinTTL>long</ErrorCachingMinTTL>
    <ErrorCode>integer</ErrorCode>
    <ResponseCode>string</ResponseCode>
    <ResponsePagePath>string</ResponsePagePath>
  </CustomErrorResponse>
</Items>
</CustomErrorResponses>
<DefaultCacheBehavior>
<AllowedMethods>
<Items>
  <Method>string</Method>
</Items>
</AllowedMethods>
<CacheMethods>
<Items>
  <Method>string</Method>
</Items>
</CacheMethods>
</CacheBehaviors>
</CallerReference>
<Comment>string</Comment>
</CustomErrorResponses>
Response Elements

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

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

**DistributionConfig (p. 85)**

Root level tag for the DistributionConfig parameters.

Required: Yes
**Aliases (p. 85)**

A complex type that contains information about CNAMEs (alternate domain names), if any, for this distribution.

Type: Aliases (p. 194) object

**CacheBehaviors (p. 85)**

A complex type that contains zero or more CacheBehavior elements.

Type: CacheBehaviors (p. 201) object

**CallerReference (p. 85)**

A unique value (for example, a date-time stamp) that ensures that the request can't be replayed.

If the value of CallerReference is new (regardless of the content of the DistributionConfig object), CloudFront creates a new distribution.

If CallerReference is a value you already sent in a previous request to create a distribution, and if the content of the DistributionConfig is identical to the original request (ignoring white space), CloudFront returns the same the response that it returned to the original request.

If CallerReference is a value you already sent in a previous request to create a distribution but the content of the DistributionConfig is different from the original request, CloudFront returns a DistributionAlreadyExists error.

Type: String

**Comment (p. 85)**

Any comments you want to include about the distribution.

If you don't want to specify a comment, include an empty Comment element.

To delete an existing comment, update the distribution configuration and include an empty Comment element.

To add or change a comment, update the distribution configuration and specify the new comment.

Type: String

**CustomErrorResponses (p. 85)**

A complex type that controls the following:

- Whether CloudFront replaces HTTP status codes in the 4xx and 5xx range with custom error messages before returning the response to the viewer.
- How long CloudFront caches HTTP status codes in the 4xx and 5xx range.

For more information about custom error pages, see Customizing Error Responses in the Amazon CloudFront Developer Guide.

Type: CustomErrorResponses (p. 215) object

**DefaultCacheBehavior (p. 85)**

A complex type that describes the default cache behavior if you don't specify a CacheBehavior element or if files don't match any of the values of PathPattern in CacheBehavior elements. You must create exactly one default cache behavior.

Type: DefaultCacheBehavior (p. 219) object
DefaultRootObject (p. 85)

The object that you want CloudFront to request from your origin (for example, index.html) when a viewer requests the root URL for your distribution (http://www.example.com) instead of an object in your distribution (http://www.example.com/product-description.html). Specifying a default root object avoids exposing the contents of your distribution.

Specify only the object name, for example, index.html. Don't add a / before the object name.

If you don't want to specify a default root object when you create a distribution, include an empty DefaultRootObject element.

To delete the default root object from an existing distribution, update the distribution configuration and include an empty DefaultRootObject element.

To replace the default root object, update the distribution configuration and specify the new object.

For more information about the default root object, see Creating a Default Root Object in the Amazon CloudFront Developer Guide.

Type: String

Enabled (p. 85)

From this field, you can enable or disable the selected distribution.

If you specify false for Enabled but you specify values for Bucket and Prefix, the values are automatically deleted.

Type: Boolean

HttpVersion (p. 85)

(Optional) Specify the maximum HTTP version that you want viewers to use to communicate with CloudFront. The default value for new web distributions is http2. Viewers that don't support HTTP/2 automatically use an earlier HTTP version.

For viewers and CloudFront to use HTTP/2, viewers must support TLS 1.2 or later, and must support Server Name Identification (SNI).

In general, configuring CloudFront to communicate with viewers using HTTP/2 reduces latency. You can improve performance by optimizing for HTTP/2. For more information, do an Internet search for "http/2 optimization."

Type: String

Valid Values: http1.1 | http2

IsIPV6Enabled (p. 85)

If you want CloudFront to respond to IPv6 DNS requests with an IPv6 address for your distribution, specify true. If you specify false, CloudFront responds to IPv6 DNS requests with the DNS response code NOERROR and with no IP addresses. This allows viewers to submit a second request, for an IPv4 address for your distribution.

In general, you should enable IPv6 if you have users on IPv6 networks who want to access your content. However, if you're using signed URLs or signed cookies to restrict access to your content, and if you're using a custom policy that includes the IpAddress parameter to restrict the IP addresses that can access your content, don't enable IPv6. If you want to restrict access to some content by IP address and not restrict access to other content (or restrict access but not by IP address), you can create two distributions. For more information, see Creating a Signed URL Using a Custom Policy in the Amazon CloudFront Developer Guide.
If you're using an Amazon Route 53 alias resource record set to route traffic to your CloudFront distribution, you need to create a second alias resource record set when both of the following are true:

- You enable IPv6 for the distribution
- You're using alternate domain names in the URLs for your objects

For more information, see Routing Traffic to an Amazon CloudFront Web Distribution by Using Your Domain Name in the Amazon Route 53 Developer Guide.

If you created a CNAME resource record set, either with Amazon Route 53 or with another DNS service, you don't need to make any changes. A CNAME record will route traffic to your distribution regardless of the IP address format of the viewer request.

Type: Boolean

Logging (p. 85)

A complex type that controls whether access logs are written for the distribution.

For more information about logging, see Access Logs in the Amazon CloudFront Developer Guide.

Type: LoggingConfig (p. 262) object

Origins (p. 85)

A complex type that contains information about origins for this distribution.

Type: Origins (p. 267) object

PriceClass (p. 85)

The price class that corresponds with the maximum price that you want to pay for CloudFront service. If you specify PriceClass_All, CloudFront responds to requests for your objects from all CloudFront edge locations.

If you specify a price class other than PriceClass_All, CloudFront serves your objects from the CloudFront edge location that has the lowest latency among the edge locations in your price class. Viewers who are in or near regions that are excluded from your specified price class may encounter slower performance.

For more information about price classes, see Choosing the Price Class for a CloudFront Distribution in the Amazon CloudFront Developer Guide. For information about CloudFront pricing, including how price classes map to CloudFront regions, see Amazon CloudFront Pricing.

Type: String

Valid Values: PriceClass_100 | PriceClass_200 | PriceClass_All

Restrictions (p. 85)

A complex type that identifies ways in which you want to restrict distribution of your content.

Type: Restrictions (p. 278) object

ViewerCertificate (p. 85)

A complex type that specifies the following:

- Whether you want viewers to use HTTP or HTTPS to request your objects.
- If you want viewers to use HTTPS, whether you're using an alternate domain name such as example.com or the CloudFront domain name for your distribution, such as d111111abcdef8.cloudfront.net.
• If you're using an alternate domain name, whether AWS Certificate Manager (ACM) provided the certificate, or you purchased a certificate from a third-party certificate authority and imported it into ACM or uploaded it to the IAM certificate store.

You must specify only one of the following values:

• ViewerCertificate:ACMCertificateArn (p. 297)
• ViewerCertificate:IAMCertificateId (p. 298)
• ViewerCertificate:CloudFrontDefaultCertificate (p. 297)

Don't specify false for CloudFrontDefaultCertificate.

If you want viewers to use HTTP instead of HTTPS to request your objects: Specify the following value:

<CloudFrontDefaultCertificate>true<CloudFrontDefaultCertificate>

In addition, specify allow-all for ViewerProtocolPolicy for all of your cache behaviors.

If you want viewers to use HTTPS to request your objects: Choose the type of certificate that you want to use based on whether you're using an alternate domain name for your objects or the CloudFront domain name:

• If you're using an alternate domain name, such as example.com: Specify one of the following values, depending on whether ACM provided your certificate or you purchased your certificate from third-party certificate authority:

  • <ACMCertificateArn>ARN for ACM SSL/TLS certificate<ACMCertificateArn>
    where ARN for ACM SSL/TLS certificate is the ARN for the ACM SSL/TLS certificate that you want to use for this distribution.
  • <IAMCertificateId>IAM certificate ID<IAMCertificateId>
    where IAM certificate ID is the ID that IAM returned when you added the certificate to the IAM certificate store.

If you specify ACMCertificateArn or IAMCertificateId, you must also specify a value for SSLSupportMethod.

If you choose to use an ACM certificate or a certificate in the IAM certificate store, we recommend that you use only an alternate domain name in your object URLs (https://example.com/logo.jpg). If you use the domain name that is associated with your CloudFront distribution (such as https://d111111abcdef8.cloudfront.net/logo.jpg) and the viewer supports SNI, then CloudFront behaves normally. However, if the browser does not support SNI, the user's experience depends on the value that you choose for SSLSupportMethod:

• vip: The viewer displays a warning because there is a mismatch between the CloudFront domain name and the domain name in your SSL/TLS certificate.
• sni-only: CloudFront drops the connection with the browser without returning the object.

• If you're using the CloudFront domain name for your distribution, such as d111111abcdef8.cloudfront.net: Specify the following value:

  <CloudFrontDefaultCertificate>true<CloudFrontDefaultCertificate>

If you want viewers to use HTTPS, you must also specify one of the following values in your cache behaviors:

• <ViewerProtocolPolicy>https-only<ViewerProtocolPolicy>
• <ViewerProtocolPolicy>redirect-to-https<ViewerProtocolPolicy>

You can also optionally require that CloudFront use HTTPS to communicate with your origin by specifying one of the following values for the applicable origins:

• <OriginProtocolPolicy>https-only<OriginProtocolPolicy>
• `<OriginProtocolPolicy>match-viewer<OriginProtocolPolicy>`

For more information, see Using Alternate Domain Names and HTTPS in the Amazon CloudFront Developer Guide.

Type: ViewerCertificate (p. 296) object

WebACLId (p. 85)

A unique identifier that specifies the AWS WAF web ACL, if any, to associate with this distribution.

AWS WAF is a web application firewall that lets you monitor the HTTP and HTTPS requests that are forwarded to CloudFront, and lets you control access to your content. Based on conditions that you specify, such as the IP addresses that requests originate from or the values of query strings, CloudFront responds to requests either with the requested content or with an HTTP 403 status code (Forbidden). You can also configure CloudFront to return a custom error page when a request is blocked. For more information about AWS WAF, see the AWS WAF Developer Guide.

Type: String

Errors

For information about the errors that are common to all actions, see Common Errors (p. 302).

AccessDenied

Access denied.

HTTP Status Code: 403

NoSuchDistribution

The specified distribution does not exist.

HTTP Status Code: 404

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
GetFieldLevelEncryption

Get the field-level encryption configuration information.

Request Syntax

GET /2017-10-30/field-level-encryption/Id HTTP/1.1

URI Request Parameters

The request requires the following URI parameters.

Id (p. 94)
Request the ID for the field-level encryption configuration information.

Request Body

The request does not have a request body.

Response Syntax

HTTP/1.1 200
<?xml version="1.0" encoding="UTF-8"?>
<FieldLevelEncryption>
    <FieldLevelEncryptionConfig>
        <CallerReference>string</CallerReference>
        <Comment>string</Comment>
        <ContentTypeProfileConfig>
            <ContainsTypeProfiles>integer</ContainsTypeProfiles>
            <ContentTypeProfile>
                <ContentType>string</ContentType>
                <Format>string</Format>
                <ProfileId>string</ProfileId>
            </ContentTypeProfile>
        </ContentTypeProfileConfig>
        <ForwardWhenContentTypeIsUnknown>boolean</ForwardWhenContentTypeIsUnknown>
        <QueryArgProfileConfig>
            <ForwardWhenQueryArgProfileIsUnknown>boolean</ForwardWhenQueryArgProfileIsUnknown>
            <QueryArgProfiles>
                <QueryArgProfile>
                    <ProfileId>string</ProfileId>
                    <QueryArg>string</QueryArg>
                </QueryArgProfile>
            </QueryArgProfiles>
        </QueryArgProfileConfig>
    </FieldLevelEncryptionConfig>
    <Id>string</Id>
    <LastModifiedTime>timestamp</LastModifiedTime>
</FieldLevelEncryption>

API Version 2017-10-30
Response Elements

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

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

**FieldLevelEncryption (p. 94)**

Root level tag for the FieldLevelEncryption parameters.

Required: Yes

**FieldLevelEncryptionConfig (p. 94)**

A complex data type that includes the profile configurations specified for field-level encryption.

Type: FieldLevelEncryptionConfig (p. 240) object

**Id (p. 94)**

The configuration ID for a field-level encryption configuration which includes a set of profiles that specify certain selected data fields to be encrypted by specific public keys.

Type: String

**LastModifiedTime (p. 94)**

The last time the field-level encryption configuration was changed.

Type: Timestamp

Errors

For information about the errors that are common to all actions, see Common Errors (p. 302).

**AccessDenied**

Access denied.

HTTP Status Code: 403

**NoSuchFieldLevelEncryptionConfig**

The specified configuration for field-level encryption doesn't exist.

HTTP Status Code: 404

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
See Also

- AWS SDK for JavaScript
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V2
GetFieldLevelEncryptionConfig

Get the field-level encryption configuration information.

Request Syntax

GET /2017-10-30/field-level-encryption/Id/config HTTP/1.1

URI Request Parameters

The request requires the following URI parameters.

Id (p. 97)

Request the ID for the field-level encryption configuration information.

Request Body

The request does not have a request body.

Response Syntax

HTTP/1.1 200
<?xml version="1.0" encoding="UTF-8"?>
<FieldLevelEncryptionConfig>
  <CallerReference>string</CallerReference>
  <Comment>string</Comment>
  <ContentTypeProfileConfig>
    <ContentTypeProfiles>
      <Items>
        <ContentTypeProfile>
          <ContentType>string</ContentType>
          <Format>string</Format>
          <ProfileId>string</ProfileId>
        </ContentTypeProfile>
      </Items>
    </ContentTypeProfiles>
    <Quantity>integer</Quantity>
  </ContentTypeProfileConfig>
  <QueryArgProfileConfig>
    <ForwardWhenQueryArgProfileIsUnknown>boolean</ForwardWhenQueryArgProfileIsUnknown>
    <QueryArgProfiles>
      <Items>
        <QueryArgProfile>
          <ProfileId>string</ProfileId>
          <QueryArg>string</QueryArg>
        </QueryArgProfile>
      </Items>
    </QueryArgProfiles>
    <Quantity>integer</Quantity>
  </QueryArgProfileConfig>
</FieldLevelEncryptionConfig>
Response Elements

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

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

FieldLevelEncryptionConfig (p. 97)

Root level tag for the FieldLevelEncryptionConfig parameters.

Required: Yes

CallerReference (p. 97)

A unique number that ensures the request can't be replayed.

Type: String

Comment (p. 97)

An optional comment about the configuration.

Type: String

ContentTypeProfileConfig (p. 97)

A complex data type that specifies when to forward content if a content type isn't recognized and profiles to use as by default in a request if a query argument doesn't specify a profile to use.

Type: ContentTypeProfileConfig (p. 209) object

QueryArgProfileConfig (p. 97)

A complex data type that specifies when to forward content if a profile isn't found and the profile that can be provided as a query argument in a request.

Type: QueryArgProfileConfig (p. 275) object

Errors

For information about the errors that are common to all actions, see Common Errors (p. 302).

AccessDenied

Access denied.

HTTP Status Code: 403

NoSuchFieldLevelEncryptionConfig

The specified configuration for field-level encryption doesn't exist.

HTTP Status Code: 404

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
GetFieldLevelEncryptionProfile

Get the field-level encryption profile information.

Request Syntax

GET /2017-10-30/field-level-encryption-profile/Id HTTP/1.1

URI Request Parameters

The request requires the following URI parameters.

Id (p. 100)

Get the ID for the field-level encryption profile information.

Request Body

The request does not have a request body.

Response Syntax

HTTP/1.1 200
<?xml version="1.0" encoding="UTF-8"?>
<FieldLevelEncryptionProfile>
  <FieldLevelEncryptionProfileConfig>
    <CallerReference>string</CallerReference>
    <Comment>string</Comment>
    <EncryptionEntities>
      <Items>
        <EncryptionEntity>
          <FieldPatterns>
            <Items>
              <FieldPattern>string</FieldPattern>
            </Items>
            <Quantity>integer</Quantity>
          </FieldPatterns>
          <ProviderId>string</ProviderId>
          <PublicKeyId>string</PublicKeyId>
        </EncryptionEntity>
      </Items>
      <Quantity>integer</Quantity>
    </EncryptionEntities>
    <Name>string</Name>
  </FieldLevelEncryptionProfileConfig>
  <Id>string</Id>
  <LastModifiedTime>timestamp</LastModifiedTime>
</FieldLevelEncryptionProfile>

Response Elements

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

The following data is returned in XML format by the service.
FieldLevelEncryptionProfile (p. 100)

Root level tag for the FieldLevelEncryptionProfile parameters.

Required: Yes

FieldLevelEncryptionProfileConfig (p. 100)

A complex data type that includes the profile name and the encryption entities for the field-level encryption profile.

Type: FieldLevelEncryptionProfileConfig (p. 243) object

Id (p. 100)

The ID for a field-level encryption profile configuration which includes a set of profiles that specify certain selected data fields to be encrypted by specific public keys.

Type: String

LastModifiedTime (p. 100)

The last time the field-level encryption profile was updated.

Type: Timestamp

Errors

For information about the errors that are common to all actions, see Common Errors (p. 302).

AccessDenied

Access denied.

HTTP Status Code: 403

NoSuchFieldLevelEncryptionProfile

The specified profile for field-level encryption doesn’t exist.

HTTP Status Code: 404

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
GetFieldLevelEncryptionProfileConfig

Get the field-level encryption profile configuration information.

Request Syntax

```
GET /2017-10-30/field-level-encryption-profile/Id/config HTTP/1.1
```

URI Request Parameters

The request requires the following URI parameters.

**Id (p. 102)**

Get the ID for the field-level encryption profile configuration information.

Request Body

The request does not have a request body.

Response Syntax

```
HTTP/1.1 200
<?xml version="1.0" encoding="UTF-8"?>
<FieldLevelEncryptionProfileConfig>
  <CallerReference>string</CallerReference>
  <Comment>string</Comment>
  <EncryptionEntities>
    <Items>
      <EncryptionEntity>
        <FieldPatterns>
          <Items>
            <FieldPattern>string</FieldPattern>
          </Items>
        </FieldPatterns>
        <ProviderId>string</ProviderId>
        <PublicKeyId>string</PublicKeyId>
      </EncryptionEntity>
    </Items>
    <Quantity>integer</Quantity>
  </EncryptionEntities>
  <Name>string</Name>
</FieldLevelEncryptionProfileConfig>
```

Response Elements

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

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

**FieldLevelEncryptionProfileConfig (p. 102)**

Root level tag for the FieldLevelEncryptionProfileConfig parameters.
Required: Yes

**CallerReference (p. 102)**

A unique number that ensures the request can't be replayed.

Type: String

**Comment (p. 102)**

An optional comment for the field-level encryption profile.

Type: String

**EncryptionEntities (p. 102)**

A complex data type of encryption entities for the field-level encryption profile that include the public key ID, provider, and field patterns for specifying which fields to encrypt with this key.

Type: EncryptionEntities (p. 237) object

**Name (p. 102)**

Profile name for the field-level encryption profile.

Type: String

---

**Errors**

For information about the errors that are common to all actions, see Common Errors (p. 302).

**AccessDenied**

Access denied.

HTTP Status Code: 403

**NoSuchFieldLevelEncryptionProfile**

The specified profile for field-level encryption doesn't exist.

HTTP Status Code: 404

---

**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
GetInvalidation

Get the information about an invalidation.

Request Syntax

GET /2017-10-30/distribution/DistributionId/invalidation/Id HTTP/1.1

URI Request Parameters

The request requires the following URI parameters.

DistributionId (p. 104)
   The distribution's ID.

Id (p. 104)
   The identifier for the invalidation request, for example, IDFDVBD632BHDS5.

Request Body

The request does not have a request body.

Response Syntax

HTTP/1.1 200
<?xml version="1.0" encoding="UTF-8"?>
<Invalidation>
   <CreateTime>timestamp</CreateTime>
   <Id>string</Id>
   <InvalidationBatch>
      <CallerReference>string</CallerReference>
      <Paths>
         <Items>
            <Path>string</Path>
         </Items>
         <Quantity>integer</Quantity>
      </Paths>
   </InvalidationBatch>
   <Status>string</Status>
</Invalidation>

Response Elements

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

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

Invalidation (p. 104)
   Root level tag for the Invalidation parameters.
   Required: Yes
CreateTime (p. 104)
The date and time the invalidation request was first made.
Type: Timestamp

Id (p. 104)
The identifier for the invalidation request. For example: IDFDVB632BHDS5.
Type: String

InvalidationBatch (p. 104)
The current invalidation information for the batch request.
Type: InvalidationBatch (p. 255) object

Status (p. 104)
The status of the invalidation request. When the invalidation batch is finished, the status is Completed.
Type: String

Errors
For information about the errors that are common to all actions, see Common Errors (p. 302).

AccessDenied
Access denied.
HTTP Status Code: 403

NoSuchDistribution
The specified distribution does not exist.
HTTP Status Code: 404

NoSuchInvalidation
The specified invalidation does not exist.
HTTP Status Code: 404

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
See Also

- AWS SDK for Ruby V2
GetPublicKey

Get the public key information.

Request Syntax

GET /2017-10-30/public-key/Id HTTP/1.1

URI Request Parameters

The request requires the following URI parameters.

Id (p. 107)

Request the ID for the public key.

Request Body

The request does not have a request body.

Response Syntax

HTTP/1.1 200
<?xml version="1.0" encoding="UTF-8"?>
<PublicKey>
  <CreatedTime>timestamp</CreatedTime>
  <Id>string</Id>
  <PublicKeyConfig>
    <CallerReference>string</CallerReference>
    <Comment>string</Comment>
    <EncodedKey>string</EncodedKey>
    <Name>string</Name>
  </PublicKeyConfig>
</PublicKey>

Response Elements

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

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

PublicKey (p. 107)

Root level tag for the PublicKey parameters.

Required: Yes

CreatedTime (p. 107)

A time you added a public key to CloudFront.

Type: Timestamp

Id (p. 107)

A unique ID assigned to a public key you've added to CloudFront.
Errors

For information about the errors that are common to all actions, see Common Errors (p. 302).

AccessDenied

Access denied.

HTTP Status Code: 403

NoSuchPublicKey

The specified public key doesn’t exist.

HTTP Status Code: 404

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
GetPublicKeyConfig

Return public key configuration information

Request Syntax

GET /2017-10-30/public-key/Id/config HTTP/1.1

URI Request Parameters

The request requires the following URI parameters.

Id (p. 109)

Request the ID for the public key configuration.

Request Body

The request does not have a request body.

Response Syntax

HTTP/1.1 200
<?xml version="1.0" encoding="UTF-8"?>
<PublicKeyConfig>
  <CallerReference>string</CallerReference>
  <Comment>string</Comment>
  <EncodedKey>string</EncodedKey>
  <Name>string</Name>
</PublicKeyConfig>

Response Elements

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

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

PublicKeyConfig (p. 109)

Root level tag for the PublicKeyConfig parameters.

Required: Yes

CallerReference (p. 109)

A unique number that ensures the request can't be replayed.

Type: String

Comment (p. 109)

An optional comment about a public key.

Type: String
EncodedKey (p. 109)

The encoded public key that you want to add to CloudFront to use with features like field-level encryption.

Type: String

Name (p. 109)

The name for a public key you add to CloudFront to use with features like field-level encryption.

Type: String

Errors

For information about the errors that are common to all actions, see Common Errors (p. 302).

AccessDenied

Access denied.

HTTP Status Code: 403

NoSuchPublicKey

The specified public key doesn't exist.

HTTP Status Code: 404

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
GetStreamingDistribution

Gets information about a specified RTMP distribution, including the distribution configuration.

**Request Syntax**

```
GET /2017-10-30/streaming-distribution/Id HTTP/1.1
```

**URI Request Parameters**

The request requires the following URI parameters.

**Id (p. 111)**

The streaming distribution's ID.

**Request Body**

The request does not have a request body.

**Response Syntax**

```
HTTP/1.1 200
<?xml version="1.0" encoding="UTF-8"?>
<StreamingDistribution>
  <ActiveTrustedSigners>
    <Enabled>boolean</Enabled>
    <Items>
      <Signer>
        <AwsAccountNumber>string</AwsAccountNumber>
        <KeyPairIds>
          <Items>
            <KeyPairId>string</KeyPairId>
          </Items>
          <Quantity>integer</Quantity>
        </KeyPairIds>
      </Signer>
      <Items>
        <Signer>
          <AwsAccountNumber>string</AwsAccountNumber>
          <KeyPairIds>
            <Items>
              <KeyPairId>string</KeyPairId>
            </Items>
            <Quantity>integer</Quantity>
          </KeyPairIds>
        </Signer>
      </Items>
    </Items>
    <Quantity>integer</Quantity>
  </ActiveTrustedSigners>
  <ARN>string</ARN>
  <DomainName>string</DomainName>
  <Id>string</Id>
  <LastModifiedTime>timestamp</LastModifiedTime>
  <Status>string</Status>
  <StreamingDistributionConfig>
    <Aliases>
      <Items>
        <CNAME>string</CNAME>
      </Items>
      <Quantity>integer</Quantity>
    </Aliases>
    <CallerReference>string</CallerReference>
    <Comment>string</Comment>
    <Enabled>boolean</Enabled>
    <Logging>
```

API Version 2017-10-30

111
Response Elements

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

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

**StreamingDistribution (p. 111)**

Root level tag for the StreamingDistribution parameters.

Required: Yes

**ActiveTrustedSigners (p. 111)**

A complex type that lists the AWS accounts, if any, that you included in the TrustedSigners complex type for this distribution. These are the accounts that you want to allow to create signed URLs for private content.

The Signer complex type lists the AWS account number of the trusted signer or self if the signer is the AWS account that created the distribution. The Signer element also includes the IDs of any active CloudFront key pairs that are associated with the trusted signer's AWS account. If no KeyPairId element appears for a Signer, that signer can't create signed URLs.

For more information, see Serving Private Content through CloudFront in the Amazon CloudFront Developer Guide.

Type: ActiveTrustedSigners (p. 192) object

**ARN (p. 111)**

Type: String

**DomainName (p. 111)**

The domain name that corresponds to the streaming distribution, for example, s5c39gqb8ow64r.cloudfront.net.

Type: String

**Id (p. 111)**

The identifier for the RTMP distribution. For example: EGTXBD79EXAMPLE.

Type: String
LastModifiedTime (p. 111)

The date and time that the distribution was last modified.

Type: Timestamp

Status (p. 111)

The current status of the RTMP distribution. When the status is Deployed, the distribution's information is propagated to all CloudFront edge locations.

Type: String

StreamingDistributionConfig (p. 111)

The current configuration information for the RTMP distribution.

Type: StreamingDistributionConfig (p. 284) object

Errors

For information about the errors that are common to all actions, see Common Errors (p. 302).

AccessDenied

Access denied.

HTTP Status Code: 403

NoSuchStreamingDistribution

The specified streaming distribution does not exist.

HTTP Status Code: 404

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
GetStreamingDistributionConfig

Get the configuration information about a streaming distribution.

Request Syntax

GET /2017-10-30/streaming-distribution/Id/config HTTP/1.1

URI Request Parameters

The request requires the following URI parameters.

Id (p. 114)

The streaming distribution's ID.

Request Body

The request does not have a request body.

Response Syntax

HTTP/1.1 200
<?xml version="1.0" encoding="UTF-8"?>
<StreamingDistributionConfig>
  <Aliases>
    <Items>
      <CNAME>string</CNAME>
    </Items>
    <Quantity>integer</Quantity>
  </Aliases>
  <CallerReference>string</CallerReference>
  <Comment>string</Comment>
  <Enabled>boolean</Enabled>
  <Logging>
    <Bucket>string</Bucket>
    <Enabled>boolean</Enabled>
    <Prefix>string</Prefix>
  </Logging>
  <PriceClass>string</PriceClass>
  <S3Origin>
    <DomainName>string</DomainName>
    <OriginAccessIdentity>string</OriginAccessIdentity>
  </S3Origin>
  <TrustedSigners>
    <Enabled>boolean</Enabled>
    <Items>
      <AwsAccountNumber>string</AwsAccountNumber>
    </Items>
    <Quantity>integer</Quantity>
  </TrustedSigners>
</StreamingDistributionConfig>

Response Elements

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

**StreamingDistributionConfig (p. 114)**

Root level tag for the StreamingDistributionConfig parameters.

Required: Yes

**Aliases (p. 114)**

A complex type that contains information about CNAMEs (alternate domain names), if any, for this streaming distribution.

Type: Aliases (p. 194) object

**CallerReference (p. 114)**

A unique number that ensures that the request can't be replayed. If the CallerReference is new (no matter the content of the StreamingDistributionConfig object), a new streaming distribution is created. If the CallerReference is a value that you already sent in a previous request to create a streaming distribution, and the content of the StreamingDistributionConfig is identical to the original request (ignoring white space), the response includes the same information returned to the original request. If the CallerReference is a value that you already sent in a previous request to create a streaming distribution but the content of the StreamingDistributionConfig is different from the original request, CloudFront returns a DistributionAlreadyExists error.

Type: String

**Comment (p. 114)**

Any comments you want to include about the streaming distribution.

Type: String

**Enabled (p. 114)**

Whether the streaming distribution is enabled to accept user requests for content.

Type: Boolean

**Logging (p. 114)**

A complex type that controls whether access logs are written for the streaming distribution.

Type: StreamingLoggingConfig (p. 291) object

**PriceClass (p. 114)**

A complex type that contains information about price class for this streaming distribution.

Type: String

Valid Values: PriceClass_100 | PriceClass_200 | PriceClass_All

**S3Origin (p. 114)**

A complex type that contains information about the Amazon S3 bucket from which you want CloudFront to get your media files for distribution.

Type: S3Origin (p. 279) object

**TrustedSigners (p. 114)**

A complex type that specifies any AWS accounts that you want to permit to create signed URLs for private content. If you want the distribution to use signed URLs, include this element; if you want
the distribution to use public URLs, remove this element. For more information, see Serving Private Content through CloudFront in the Amazon CloudFront Developer Guide.

Type: TrustedSigners (p. 295) object

Errors

For information about the errors that are common to all actions, see Common Errors (p. 302).

AccessDenied

Access denied.

HTTP Status Code: 403

NoSuchStreamingDistribution

The specified streaming distribution does not exist.

HTTP Status Code: 404

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
ListCloudFrontOriginAccessIdentities

Lists origin access identities.

**Request Syntax**

```
GET /2017-10-30/origin-access-identity/cloudfront?Marker=Marker&MaxItems=MaxItems HTTP/1.1
```

**URI Request Parameters**

The request requires the following URI parameters.

**Marker (p. 117)**

Use this when paginating results to indicate where to begin in your list of origin access identities. The results include identities in the list that occur after the marker. To get the next page of results, set the `Marker` to the value of the `NextMarker` from the current page's response (which is also the ID of the last identity on that page).

**MaxItems (p. 117)**

The maximum number of origin access identities you want in the response body.

**Request Body**

The request does not have a request body.

**Response Syntax**

```
HTTP/1.1 200
<?xml version="1.0" encoding="UTF-8"?>
<CloudFrontOriginAccessIdentityList>
    <IsTruncated>boolean</IsTruncated>
    <Items>
        <CloudFrontOriginAccessIdentitySummary>
            <Comment>string</Comment>
            <Id>string</Id>
            <S3CanonicalUserId>string</S3CanonicalUserId>
        </CloudFrontOriginAccessIdentitySummary>
    </Items>
    <Marker>string</Marker>
    <MaxItems>integer</MaxItems>
    <NextMarker>string</NextMarker>
    <Quantity>integer</Quantity>
</CloudFrontOriginAccessIdentityList>
```

**Response Elements**

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

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

**CloudFrontOriginAccessIdentityList (p. 117)**

Root level tag for the CloudFrontOriginAccessIdentityList parameters.
Required: Yes

**IsTruncated (p. 117)**

A flag that indicates whether more origin access identities remain to be listed. If your results were truncated, you can make a follow-up pagination request using the Marker request parameter to retrieve more items in the list.

Type: Boolean

**Items (p. 117)**

A complex type that contains one CloudFrontOriginAccessIdentitySummary element for each origin access identity that was created by the current AWS account.

Type: Array of CloudFrontOriginAccessIdentitySummary (p. 207) objects

**Marker (p. 117)**

Use this when paginating results to indicate where to begin in your list of origin access identities. The results include identities in the list that occur after the marker. To get the next page of results, set the Marker to the value of the NextMarker from the current page's response (which is also the ID of the last identity on that page).

Type: String

**MaxItems (p. 117)**

The maximum number of origin access identities you want in the response body.

Type: Integer

**NextMarker (p. 117)**

If IsTruncated is true, this element is present and contains the value you can use for the Marker request parameter to continue listing your origin access identities where they left off.

Type: String

**Quantity (p. 117)**

The number of CloudFront origin access identities that were created by the current AWS account.

Type: Integer

---

**Errors**

For information about the errors that are common to all actions, see Common Errors (p. 302).

**InvalidArgument**

The argument is invalid.

HTTP Status Code: 400

---

**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
ListDistributions

List distributions.

Request Syntax

```
GET /2017-10-30/distribution?Marker=Marker&MaxItems=MaxItems HTTP/1.1
```

URI Request Parameters

The request requires the following URI parameters.

**Marker (p. 120)**

Use this when paginating results to indicate where to begin in your list of distributions. The results include distributions in the list that occur after the marker. To get the next page of results, set the Marker to the value of the NextMarker from the current page's response (which is also the ID of the last distribution on that page).

**MaxItems (p. 120)**

The maximum number of distributions you want in the response body.

Request Body

The request does not have a request body.

Response Syntax

```
HTTP/1.1 200
<?xml version="1.0" encoding="UTF-8"?>
<DistributionList>
  <IsTruncated>boolean</IsTruncated>
  <Items>
    <DistributionSummary>
      <Aliases>
        <Items>
          <CNAME>string</CNAME>
          <Quantity>integer</Quantity>
        </Items>
      </Aliases>
      <ARN>string</ARN>
      <CacheBehaviors>
        <Items>
          <CacheBehavior>
            <AllowedMethods>
              <CachedMethods>
                <Items>
                  <Method>string</Method>
                  <Quantity>integer</Quantity>
                </Items>
              </CachedMethods>
              <Items>
                <Method>string</Method>
                <Quantity>integer</Quantity>
              </Items>
            </AllowedMethods>
            <Compress>boolean</Compress>
          </CacheBehavior>
        </Items>
      </CacheBehaviors>
    </DistributionSummary>
  </Items>
</DistributionList>
```
<DefaultTTL>long</DefaultTTL>
<FieldLevelEncryptionId>string</FieldLevelEncryptionId>
<ForwardedValues>
  <Cookies>
    <Forward>string</Forward>
  </Cookies>
  <WhitelistedNames>
    <Items>
      <Name>string</Name>
    </Items>
  </WhitelistedNames>
  <Headers>
    <Items>
      <Name>string</Name>
    </Items>
  </Headers>
  <QueryStringCacheKeys>
    <Items>
      <Name>string</Name>
    </Items>
  </QueryStringCacheKeys>
</ForwardedValues>
<LambdaFunctionAssociations>
  <Items>
    <LambdaFunctionAssociation>
      <EventType>string</EventType>
      <LambdaFunctionARN>string</LambdaFunctionARN>
    </LambdaFunctionAssociation>
  </Items>
</LambdaFunctionAssociations>
<MaxTTL>long</MaxTTL>
<MinTTL>long</MinTTL>
<PathPattern>string</PathPattern>
<SmoothStreaming>boolean</SmoothStreaming>
<TargetOriginId>string</TargetOriginId>
<TrustedSigners>
  <Enabled>boolean</Enabled>
  <Items>
    <AwsAccountNumber>string</AwsAccountNumber>
  </Items>
</TrustedSigners>
<ViewerProtocolPolicy>string</ViewerProtocolPolicy>
</CacheBehavior>
</Items>
<Quantity>integer</Quantity>
</CacheBehaviors>
<Comment>string</Comment>
<CustomErrorResponses>
  <Items>
    <CustomErrorResponse>
      <ErrorCachingMinTTL>long</ErrorCachingMinTTL>
      <ErrorCode>integer</ErrorCode>
      <ResponseCode>string</ResponseCode>
      <ResponsePagePath>string</ResponsePagePath>
    </CustomErrorResponse>
  </Items>
  <Quantity>integer</Quantity>
</CustomErrorResponses>
<DefaultCacheBehavior>
  <AllowedMethods>
<CachedMethods>
  <Items>
    <Method>string</Method>
  </Items>
  <Quantity>integer</Quantity>
</CachedMethods>
<AllowedMethods>
  <Compress>boolean</Compress>
  <DefaultTTL>long</DefaultTTL>
  <FieldLevelEncryptionId>string</FieldLevelEncryptionId>
  <ForwardedValues>
    <Cookies>
      <Forward>string</Forward>
      <WhitelistedNames>
        <Items>
          <Name>string</Name>
        </Items>
        <Quantity>integer</Quantity>
      </WhitelistedNames>
    </Cookies>
    <Headers>
      <Items>
        <Name>string</Name>
      </Items>
      <Quantity>integer</Quantity>
    </Headers>
    <QueryString>boolean</QueryString>
    <QueryStringCacheKeys>
      <Items>
        <Name>string</Name>
      </Items>
      <Quantity>integer</Quantity>
    </QueryStringCacheKeys>
  </ForwardedValues>
  <LambdaFunctionAssociations>
    <Items>
      <LambdaFunctionAssociation>
        <EventType>string</EventType>
        <LambdaFunctionARN>string</LambdaFunctionARN>
      </LambdaFunctionAssociation>
      <Quantity>integer</Quantity>
    </LambdaFunctionAssociations>
    <MaxTTL>long</MaxTTL>
    <MinTTL>long</MinTTL>
    <SmoothStreaming>boolean</SmoothStreaming>
    <TargetOriginId>string</TargetOriginId>
    <TrustedSigners>
      <Enabled>boolean</Enabled>
      <Items>
        <AwsAccountNumber>string</AwsAccountNumber>
      </Items>
      <Quantity>integer</Quantity>
    </TrustedSigners>
    <ViewerProtocolPolicy>string</ViewerProtocolPolicy>
  </LambdaFunctionAssociations>
</DefaultCacheBehavior>
<DomainName>string</DomainName>
<Enabled>boolean</Enabled>
<HttpVersion>string</HttpVersion>
<Id>string</Id>
<IsIPV6Enabled>boolean</IsIPV6Enabled>
<LastModifiedTime>timestamp</LastModifiedTime>
<Origins>
  <Items>
    <Origin>
      <CustomHeaders>
        <Items>
          <OriginCustomHeader>
            <HeaderName>string</HeaderName>
            <HeaderValue>string</HeaderValue>
          </OriginCustomHeader>
        </Items>
      </CustomHeaders>
      <CustomOriginConfig>
        <HTTPPort>integer</HTTPPort>
        <HTTPSPort>integer</HTTPSPort>
        <OriginKeepaliveTimeout>integer</OriginKeepaliveTimeout>
        <OriginProtocolPolicy>string</OriginProtocolPolicy>
        <OriginReadTimeout>integer</OriginReadTimeout>
        <OriginSslProtocols>
          <Items>
            <SslProtocol>string</SslProtocol>
          </Items>
        </OriginSslProtocols>
      </CustomOriginConfig>
      <DomainName>string</DomainName>
      <Id>string</Id>
      <OriginPath>string</OriginPath>
      <S3OriginConfig>
        <OriginAccessIdentity>string</OriginAccessIdentity>
      </S3OriginConfig>
    </Origin>
  </Items>
  <Quantity>integer</Quantity>
</Origins>

<PriceClass>string</PriceClass>

<Restrictions>
  <GeoRestriction>
    <Items>
      <Location>string</Location>
    </Items>
  </GeoRestriction>
  <RestrictionType>string</RestrictionType>
</Restrictions>

<Status>string</Status>

<ViewerCertificate>
  <ACMCertificateArn>string</ACMCertificateArn>
  <Certificate>string</Certificate>
  <CertificateSource>string</CertificateSource>
  <CloudFrontDefaultCertificate>boolean</CloudFrontDefaultCertificate>
  <IAMCertificateId>string</IAMCertificateId>
  <MinimumProtocolVersion>string</MinimumProtocolVersion>
  <SSLSupportMethod>string</SSLSupportMethod>
</ViewerCertificate>

<WebACLId>string</WebACLId>

</DistributionSummary>

<Marker>string</Marker>

<MaxItems>integer</MaxItems>

<NextMarker>string</NextMarker>

<Quantity>integer</Quantity>

</DistributionList>
Response Elements

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

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

**DistributionList (p. 120)**

Root level tag for the DistributionList parameters.

- Required: Yes

**IsTruncated (p. 120)**

A flag that indicates whether more distributions remain to be listed. If your results were truncated, you can make a follow-up pagination request using the Marker request parameter to retrieve more distributions in the list.

- Type: Boolean

**Items (p. 120)**

A complex type that contains one DistributionSummary element for each distribution that was created by the current AWS account.

- Type: Array of DistributionSummary (p. 233) objects

**Marker (p. 120)**

The value you provided for the Marker request parameter.

- Type: String

**MaxItems (p. 120)**

The value you provided for the MaxItems request parameter.

- Type: Integer

**NextMarker (p. 120)**

If IsTruncated is true, this element is present and contains the value you can use for the Marker request parameter to continue listing your distributions where they left off.

- Type: String

**Quantity (p. 120)**

The number of distributions that were created by the current AWS account.

- Type: Integer

Errors

For information about the errors that are common to all actions, see Common Errors (p. 302).

**InvalidArgument**

- The argument is invalid.

  HTTP Status Code: 400
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
ListDistributionsByWebACLId

List the distributions that are associated with a specified AWS WAF web ACL.

Request Syntax

GET /2017-10-30/distributionsByWebACLId/WebACLId?Marker=Marker&MaxItems=MaxItems HTTP/1.1

URI Request Parameters

The request requires the following URI parameters.

Marker (p. 126)

Use Marker and MaxItems to control pagination of results. If you have more than MaxItems distributions that satisfy the request, the response includes a NextMarker element. To get the next page of results, submit another request. For the value of Marker, specify the value of NextMarker from the last response. (For the first request, omit Marker.)

MaxItems (p. 126)

The maximum number of distributions that you want CloudFront to return in the response body. The maximum and default values are both 100.

WebACLId (p. 126)

The ID of the AWS WAF web ACL that you want to list the associated distributions. If you specify "null" for the ID, the request returns a list of the distributions that aren't associated with a web ACL.

Request Body

The request does not have a request body.

Response Syntax

HTTP/1.1 200
<?xml version="1.0" encoding="UTF-8"?>
<DistributionList>
  <IsTruncated>boolean</IsTruncated>
  <Items>
    <DistributionSummary>
      <Aliases>
        <Items>
          <CNAME>string</CNAME>
        </Items>
        <Quantity>integer</Quantity>
      </Aliases>
      <ARN>string</ARN>
      <CacheBehaviors>
        <Items>
          <CacheBehavior>
            <AllowedMethods>
              <CachedMethods>
                <Items>
                  <Method>string</Method>
                </Items>
              </CachedMethods>
            </AllowedMethods>
          </CacheBehavior>
        </Items>
      </CacheBehaviors>
    </DistributionSummary>
  </Items>
</DistributionList>
<Quantity>integer</Quantity>
</CachedMethods>
<Items>
  <Method>string</Method>
</Items>
<Quantity>integer</Quantity>
</AllowedMethods>
<Compress>boolean</Compress>
<DefaultTTL>long</DefaultTTL>
<FieldLevelEncryptionId>string</FieldLevelEncryptionId>
</ForwardedValues>
<Cookies>
  <Forward>string</Forward>
  <WhitelistedNames>
    <Items>
      <Name>string</Name>
    </Items>
    <Quantity>integer</Quantity>
  </WhitelistedNames>
</Cookies>
-Headers>
  <Items>
    <Name>string</Name>
  </Items>
  <Quantity>integer</Quantity>
</Headers>
<QueryString>boolean</QueryString>
<QueryStringCacheKeys>
  <Items>
    <Name>string</Name>
  </Items>
  <Quantity>integer</Quantity>
</QueryStringCacheKeys>
</ForwardedValues>
<LambdaFunctionAssociations>
  <Items>
    <LambdaFunctionAssociation>
      <EventType>string</EventType>
      <LambdaFunctionARN>string</LambdaFunctionARN>
    </LambdaFunctionAssociation>
  </Items>
  <Quantity>integer</Quantity>
</LambdaFunctionAssociations>
<MaxTTL>long</MaxTTL>
<MinTTL>long</MinTTL>
<PathPattern>string</PathPattern>
<SmoothStreaming>boolean</SmoothStreaming>
<TargetOriginId>string</TargetOriginId>
<TrustedSigners>
  <Enabled>boolean</Enabled>
  <Items>
    <AwsAccountNumber>string</AwsAccountNumber>
  </Items>
  <Quantity>integer</Quantity>
</TrustedSigners>
</CacheBehaviors>
<Comment>string</Comment>
<CustomErrorResponses>
  <Items>
    <CustomErrorResponse>
      <ErrorCachingMinTTL>long</ErrorCachingMinTTL>
      <ErrorCode>integer</ErrorCode>
    </CustomErrorResponse>
  </Items>
</CustomErrorResponses>
Amazon CloudFront API Reference
Response Syntax

API Version 2017-10-30
128
<ViewerProtocolPolicy>string</ViewerProtocolPolicy>
</DefaultCacheBehavior>
<DomainName>string</DomainName>
<Enabled>boolean</Enabled>
<HttpVersion>string</HttpVersion>
<Id>string</Id>
<IsIPV6Enabled>boolean</IsIPV6Enabled>
<LastModifiedTime>timestamp</LastModifiedTime>
<Origins>
<Items>
<Origin>
<CustomHeaders>
<Items>
<OriginCustomHeader>
<HeaderName>string</HeaderName>
<HeaderValue>string</HeaderValue>
</OriginCustomHeader>
</Items>
<Quantity>integer</Quantity>
</CustomHeaders>
<CustomOriginConfig>
<HTTPPort>integer</HTTPPort>
<HTTPSPort>integer</HTTPSPort>
<OriginKeepaliveTimeout>integer</OriginKeepaliveTimeout>
<OriginProtocolPolicy>string</OriginProtocolPolicy>
<OriginReadTimeout>integer</OriginReadTimeout>
<OriginSslProtocols>
<Items>
<SslProtocol>string</SslProtocol>
</Items>
<Quantity>integer</Quantity>
</OriginSslProtocols>
</CustomOriginConfig>
<DomainName>string</DomainName>
<Id>string</Id>
<OriginPath>string</OriginPath>
<S3OriginConfig>
<OriginAccessIdentity>string</OriginAccessIdentity>
</S3OriginConfig>
</Origin>
</Items>
<Quantity>integer</Quantity>
</Origins>
<PriceClass>string</PriceClass>
<Restrictions>
<GeoRestriction>
<Items>
<Location>string</Location>
</Items>
<Quantity>integer</Quantity>
<RestrictionType>string</RestrictionType>
</GeoRestriction>
</Restrictions>
>Status>string</Status>
</ViewerCertificate>
<ACMCertificateArn>string</ACMCertificateArn>
<Certificate>string</Certificate>
<CertificateSource>string</CertificateSource>
<CloudFrontDefaultCertificate>boolean</CloudFrontDefaultCertificate>
<IAMCertificateId>string</IAMCertificateId>
<MinimumProtocolVersion>string</MinimumProtocolVersion>
<SSLSupportMethod>string</SSLSupportMethod>
</ViewerCertificate>
</WebACLId>string</WebACLId>
</Items>
Response Elements

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

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

DistributionList (p. 126)

Root level tag for the DistributionList parameters.

Required: Yes

IsTruncated (p. 126)

A flag that indicates whether more distributions remain to be listed. If your results were truncated, you can make a follow-up pagination request using the Marker request parameter to retrieve more distributions in the list.

Type: Boolean

Items (p. 126)

A complex type that contains one DistributionSummary element for each distribution that was created by the current AWS account.

Type: Array of DistributionSummary (p. 233) objects

Marker (p. 126)

The value you provided for the Marker request parameter.

Type: String

MaxItems (p. 126)

The value you provided for the MaxItems request parameter.

Type: Integer

NextMarker (p. 126)

If IsTruncated is true, this element is present and contains the value you can use for the Marker request parameter to continue listing your distributions where they left off.

Type: String

Quantity (p. 126)

The number of distributions that were created by the current AWS account.

Type: Integer

Errors

For information about the errors that are common to all actions, see Common Errors (p. 302).
InvalidArgument

The argument is invalid.

HTTP Status Code: 400

InvalidWebACLId

HTTP Status Code: 400

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
ListFieldLevelEncryptionConfigs

List all field-level encryption configurations that have been created in CloudFront for this account.

**Request Syntax**

```
GET /2017-10-30/field-level-encryption?Marker=Marker&MaxItems=MaxItems HTTP/1.1
```

**URI Request Parameters**

The request requires the following URI parameters.

**Marker (p. 132)**

Use this when paginating results to indicate where to begin in your list of configurations. The results include configurations in the list that occur after the marker. To get the next page of results, set the `Marker` to the value of the `NextMarker` from the current page's response (which is also the ID of the last configuration on that page).

**MaxItems (p. 132)**

The maximum number of field-level encryption configurations you want in the response body.

**Request Body**

The request does not have a request body.

**Response Syntax**

HTTP/1.1 200
<?xml version="1.0" encoding="UTF-8"?>
<FieldLevelEncryptionList>
    <Items>
        <FieldLevelEncryptionSummary>
            <Comment>string</Comment>
            <ContentTypeProfileConfig>
                <ContentTypeProfiles>
                    <Items>
                        <ContentTypeProfile>
                            <ContentType>string</ContentType>
                            <Format>string</Format>
                            <ProfileId>string</ProfileId>
                        </ContentTypeProfile>
                    </Items>
                    <Quantity>integer</Quantity>
                </ContentTypeProfiles>
                <ForwardWhenContentTypeIsUnknown>boolean</ForwardWhenContentTypeIsUnknown>
            </ContentTypeProfileConfig>
            <Id>string</Id>
            <LastModifiedTime>timestamp</LastModifiedTime>
            <QueryArgProfileConfig>
                <ForwardWhenQueryArgProfileIsUnknown>boolean</ForwardWhenQueryArgProfileIsUnknown>
                <QueryArgProfiles>
                    <Items>
                    </QueryArgProfiles>
            </QueryArgProfileConfig>
    </Items>
</FieldLevelEncryptionList>
Response Elements

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

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

FieldLevelEncryptionList (p. 132)

Root level tag for the FieldLevelEncryptionList parameters.

Required: Yes

Items (p. 132)

An array of field-level encryption items.

Type: Array of FieldLevelEncryptionSummary (p. 246) objects

MaxItems (p. 132)

The maximum number of elements you want in the response body.

Type: Integer

NextMarker (p. 132)

If there are more elements to be listed, this element is present and contains the value that you can use for the Marker request parameter to continue listing your configurations where you left off.

Type: String

Quantity (p. 132)

The number of field-level encryption items.

Type: Integer

Errors

For information about the errors that are common to all actions, see Common Errors (p. 302).

InvalidArgument

The argument is invalid.

HTTP Status Code: 400
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
ListFieldLevelEncryptionProfiles

Request a list of field-level encryption profiles that have been created in CloudFront for this account.

Request Syntax

GET /2017-10-30/field-level-encryption-profile?Marker=Marker&MaxItems=MaxItems HTTP/1.1

URI Request Parameters

The request requires the following URI parameters.

**Marker (p. 135)**

Use this when paginating results to indicate where to begin in your list of profiles. The results include profiles in the list that occur after the marker. To get the next page of results, set the Marker to the value of the NextMarker from the current page's response (which is also the ID of the last profile on that page).

**MaxItems (p. 135)**

The maximum number of field-level encryption profiles you want in the response body.

Request Body

The request does not have a request body.

Response Syntax

HTTP/1.1 200
<?xml version="1.0" encoding="UTF-8"?>
<FieldLevelEncryptionProfileList>
  <Items>
    <FieldLevelEncryptionProfileSummary>
      <Comment>string</Comment>
      <EncryptionEntities>
        <Items>
          <EncryptionEntity>
            <FieldPatterns>
              <Items>
                <FieldPattern>string</FieldPattern>
              </Items>
            </FieldPatterns>
            <ProviderId>string</ProviderId>
            <PublicKeyId>string</PublicKeyId>
          </EncryptionEntity>
        </Items>
        <Quantity>integer</Quantity>
      </EncryptionEntities>
      <Id>string</Id>
      <LastModifiedTime>timestamp</LastModifiedTime>
      <Name>string</Name>
    </FieldLevelEncryptionProfileSummary>
  </Items>
  <MaxItems>integer</MaxItems>
</FieldLevelEncryptionProfileList>
Response Elements

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

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

**FieldLevelEncryptionProfileList (p. 135)**

Root level tag for the FieldLevelEncryptionProfileList parameters.

Required: Yes

**Items (p. 135)**

The field-level encryption profile items.

Type: Array of FieldLevelEncryptionProfileSummary (p. 245) objects

**MaxItems (p. 135)**

The maximum number of field-level encryption profiles you want in the response body.

Type: Integer

**NextMarker (p. 135)**

If there are more elements to be listed, this element is present and contains the value that you can use for the Marker request parameter to continue listing your profiles where you left off.

Type: String

**Quantity (p. 135)**

The number of field-level encryption profiles.

Type: Integer

Errors

For information about the errors that are common to all actions, see Common Errors (p. 302).

**InvalidArgument**

The argument is invalid.

HTTP Status Code: 400

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
ListInvalidations

Lists invalidation batches.

Request Syntax

```
GET /2017-10-30/distribution/DistributionId/invalidation?Marker=Marker&MaxItems=MaxItems
HTTP/1.1
```

URI Request Parameters

The request requires the following URI parameters.

**DistributionId (p. 138)**

The distribution's ID.

**Marker (p. 138)**

Use this parameter when paginating results to indicate where to begin in your list of invalidation batches. Because the results are returned in decreasing order from most recent to oldest, the most recent results are on the first page, the second page will contain earlier results, and so on. To get the next page of results, set `Marker` to the value of the `NextMarker` from the current page's response. This value is the same as the ID of the last invalidation batch on that page.

**MaxItems (p. 138)**

The maximum number of invalidation batches that you want in the response body.

Request Body

The request does not have a request body.

Response Syntax

```
HTTP/1.1 200
<?xml version="1.0" encoding="UTF-8"?>
<InvalidationList>
  <IsTruncated>boolean</IsTruncated>
  <Items>
    <InvalidationSummary>
      <CreateTime>timestamp</CreateTime>
      <Id>string</Id>
      <Status>string</Status>
    </InvalidationSummary>
  </Items>
  <Marker>string</Marker>
  <MaxItems>integer</MaxItems>
  <NextMarker>string</NextMarker>
  <Quantity>integer</Quantity>
</InvalidationList>
```

Response Elements

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

**InvalidationList (p. 138)**

- Root level tag for the InvalidationList parameters.
- Required: Yes

**IsTruncated (p. 138)**

- A flag that indicates whether more invalidation batch requests remain to be listed. If your results were truncated, you can make a follow-up pagination request using the Marker request parameter to retrieve more invalidation batches in the list.
- Type: Boolean

**Items (p. 138)**

- A complex type that contains one InvalidationSummary element for each invalidation batch created by the current AWS account.
- Type: Array of InvalidationSummary (p. 258) objects

**Marker (p. 138)**

- The value that you provided for the Marker request parameter.
- Type: String

**MaxItems (p. 138)**

- The value that you provided for the MaxItems request parameter.
- Type: Integer

**NextMarker (p. 138)**

- If IsTruncated is true, this element is present and contains the value that you can use for the Marker request parameter to continue listing your invalidation batches where they left off.
- Type: String

**Quantity (p. 138)**

- The number of invalidation batches that were created by the current AWS account.
- Type: Integer

## Errors

For information about the errors that are common to all actions, see Common Errors (p. 302).

**AccessDenied**

- Access denied.
- HTTP Status Code: 403

**InvalidArgument**

- The argument is invalid.
- HTTP Status Code: 400
NoSuchDistribution

The specified distribution does not exist.

HTTP Status Code: 404

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
ListPublicKeys

List all public keys that have been added to CloudFront for this account.

Request Syntax

GET /2017-10-30/public-key?Marker=Marker&MaxItems=MaxItems HTTP/1.1

URI Request Parameters

The request requires the following URI parameters.

Marker (p. 141)

Use this when paginating results to indicate where to begin in your list of public keys. The results include public keys in the list that occur after the marker. To get the next page of results, set the Marker to the value of the NextMarker from the current page's response (which is also the ID of the last public key on that page).

MaxItems (p. 141)

The maximum number of public keys you want in the response body.

Request Body

The request does not have a request body.

Response Syntax

HTTP/1.1 200
<?xml version="1.0" encoding="UTF-8"?>
<PublicKeyList>
  <Items>
    <PublicKeySummary>
      <Comment>string</Comment>
      <CreatedTime>timestamp</CreatedTime>
      <EncodedKey>string</EncodedKey>
      <Id>string</Id>
      <Name>string</Name>
    </PublicKeySummary>
  </Items>
  <MaxItems>integer</MaxItems>
  <NextMarker>string</NextMarker>
  <Quantity>integer</Quantity>
</PublicKeyList>

Response Elements

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

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

PublicKeyList (p. 141)

Root level tag for the PublicKeyList parameters.
**Required**: Yes

**Items (p. 141)**

An array of information about a public key you add to CloudFront to use with features like field-level encryption.

Type: Array of PublicKeySummary (p. 273) objects

**MaxItems (p. 141)**

The maximum number of public keys you want in the response body.

Type: Integer

**NextMarker (p. 141)**

If there are more elements to be listed, this element is present and contains the value that you can use for the Marker request parameter to continue listing your public keys where you left off.

Type: String

**Quantity (p. 141)**

The number of public keys you added to CloudFront to use with features like field-level encryption.

Type: Integer

---

**Errors**

For information about the errors that are common to all actions, see Common Errors (p. 302).

**InvalidArgument**

The argument is invalid.

HTTP Status Code: 400

---

**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
ListStreamingDistributions

List streaming distributions.

Request Syntax

```
GET /2017-10-30/streaming-distribution?Marker=Marker&MaxItems=MaxItems HTTP/1.1
```

URI Request Parameters

The request requires the following URI parameters.

**Marker (p. 143)**

The value that you provided for the `Marker` request parameter.

**MaxItems (p. 143)**

The value that you provided for the `MaxItems` request parameter.

Request Body

The request does not have a request body.

Response Syntax

```
HTTP/1.1 200
<?xml version="1.0" encoding="UTF-8"?>
<StreamingDistributionList>
  <IsTruncated>boolean</IsTruncated>
  <Items>
    <StreamingDistributionSummary>
      <Aliases>
        <Items>
          <CNAME>string</CNAME>
        </Items>
      </Aliases>
      <ARN>string</ARN>
      <Comment>string</Comment>
      <DomainName>string</DomainName>
      <Enabled>boolean</Enabled>
      <Id>string</Id>
      <LastModifiedTime>timestamp</LastModifiedTime>
      <PriceClass>string</PriceClass>
      <S3Origin>
        <DomainName>string</DomainName>
        <OriginAccessIdentity>string</OriginAccessIdentity>
      </S3Origin>
      <Status>string</Status>
      <TrustedSigners>
        <Enabled>boolean</Enabled>
        <Items>
          <AwsAccountNumber>string</AwsAccountNumber>
        </Items>
      </TrustedSigners>
    </StreamingDistributionSummary>
  </Items>
</StreamingDistributionList>
```

API Version 2017-10-30

143
Response Elements

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

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

**StreamingDistributionList (p. 143)**

- Root level tag for the StreamingDistributionList parameters.
- Required: Yes

**IsTruncated (p. 143)**

- A flag that indicates whether more streaming distributions remain to be listed. If your results were truncated, you can make a follow-up pagination request using the Marker request parameter to retrieve more distributions in the list.
- Type: Boolean

**Items (p. 143)**

- A complex type that contains one StreamingDistributionSummary element for each distribution that was created by the current AWS account.
- Type: Array of StreamingDistributionSummary (p. 289) objects

**Marker (p. 143)**

- The value you provided for the Marker request parameter.
- Type: String

**MaxItems (p. 143)**

- The value you provided for the MaxItems request parameter.
- Type: Integer

**NextMarker (p. 143)**

- If IsTruncated is true, this element is present and contains the value you can use for the Marker request parameter to continue listing your RTMP distributions where they left off.
- Type: String

**Quantity (p. 143)**

- The number of streaming distributions that were created by the current AWS account.
- Type: Integer

**Errors**

For information about the errors that are common to all actions, see Common Errors (p. 302).
InvalidArgument

The argument is invalid.

HTTP Status Code: 400

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
## ListTagsForResource

List tags for a CloudFront resource.

### Request Syntax

```plaintext
GET /2017-10-30/tagging?Resource=Resource HTTP/1.1
```

### URI Request Parameters

The request requires the following URI parameters.

**Resource (p. 146)**

An ARN of a CloudFront resource.

**Pattern:** `arn:aws:cloudfront::[0-9]+:*`

### Request Body

The request does not have a request body.

### Response Syntax

```
HTTP/1.1 200
<?xml version="1.0" encoding="UTF-8"?>
<Tags>
  <Items>
    <Tag>
      <Key>string</Key>
      <Value>string</Value>
    </Tag>
  </Items>
</Tags>
```

### Response Elements

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

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

**Tags (p. 146)**

Root level tag for the Tags parameters.

Required: Yes

**Items (p. 146)**

A complex type that contains Tag elements.

Type: Array of Tag (p. 292) objects
Errors

For information about the errors that are common to all actions, see Common Errors (p. 302).

AccessDenied

Access denied.

HTTP Status Code: 403

InvalidArgument

The argument is invalid.

HTTP Status Code: 400

InvalidTagging

HTTP Status Code: 400

NoSuchResource

HTTP Status Code: 404

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
TagResource

Add tags to a CloudFront resource.

Request Syntax

POST /2017-10-30/tagging?Operation=Tag HTTP/1.1
<?xml version="1.0" encoding="UTF-8"?>
<Tags xmlns="http://cloudfront.amazonaws.com/doc/2017-10-30/">
  <Items>
    <Tag>
      <Key>string</Key>
      <Value>string</Value>
    </Tag>
  </Items>
</Tags>

URI Request Parameters

The request does not use any URI parameters.

Request Body

The request accepts the following data in XML format.

Tags (p. 148)

Root level tag for the Tags parameters.
Required: Yes

Items (p. 148)

A complex type that contains Tag elements.
Type: Array of Tag (p. 292) objects
Required: No

Response Syntax

HTTP/1.1 204

Response Elements

If the action is successful, the service sends back an HTTP 204 response with an empty HTTP body.

Errors

For information about the errors that are common to all actions, see Common Errors (p. 302).

AccessDenied

Access denied.
HTTP Status Code: 403
InvalidArgument
The argument is invalid.

HTTP Status Code: 400
InvalidTagging

HTTP Status Code: 400
NoSuchResource

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

Remove tags from a CloudFront resource.

Request Syntax

POST /2017-10-30/tagging?Operation=Untag HTTP/1.1
<?xml version="1.0" encoding="UTF-8"?>
<TagKeys xmlns="http://cloudfront.amazonaws.com/doc/2017-10-30/"
    <Items>
        <Key>string</Key>
    </Items>
</TagKeys>

URI Request Parameters

The request does not use any URI parameters.

Request Body

The request accepts the following data in XML format.

TagKeys (p. 150)

Root level tag for the TagKeys parameters.

Required: Yes

Items (p. 150)

A complex type that contains Tag key elements.

Type: Array of strings


Pattern: ^([\p{L}\p{Z}\p{N}_.:/=+-@]*)$

Required: No

Response Syntax

HTTP/1.1 204

Response Elements

If the action is successful, the service sends back an HTTP 204 response with an empty HTTP body.

Errors

For information about the errors that are common to all actions, see Common Errors (p. 302).
AccessDenied

Access denied.

HTTP Status Code: 403

InvalidArgument

The argument is invalid.

HTTP Status Code: 400

InvalidTagging

HTTP Status Code: 400

NoSuchResource

HTTP Status Code: 404

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
UpdateCloudFrontOriginAccessIdentity

Update an origin access identity.

Request Syntax

```
PUT /2017-10-30/origin-access-identity/cloudfront/Id/config HTTP/1.1
<?xml version="1.0" encoding="UTF-8"?>
<CloudFrontOriginAccessIdentityConfig xmlns="http://cloudfront.amazonaws.com/doc/2017-10-30/">
  <CallerReference>string</CallerReference>
  <Comment>string</Comment>
</CloudFrontOriginAccessIdentityConfig>
```

URI Request Parameters

The request does not use any URI parameters.

Request Body

The request accepts the following data in XML format.

CloudFrontOriginAccessIdentityConfig (p. 152)

Root level tag for the CloudFrontOriginAccessIdentityConfig parameters.

Required: Yes

CallerReference (p. 152)

A unique number that ensures the request can't be replayed.

If the CallerReference is new (no matter the content of the CloudFrontOriginAccessIdentityConfig object), a new origin access identity is created.

If the CallerReference is a value already sent in a previous identity request, and the content of the CloudFrontOriginAccessIdentityConfig is identical to the original request (ignoring white space), the response includes the same information returned to the original request.

If the CallerReference is a value you already sent in a previous request to create an identity, but the content of the CloudFrontOriginAccessIdentityConfig is different from the original request, CloudFront returns a CloudFrontOriginAccessIdentityAlreadyExists error.

Type: String

Required: Yes

Comment (p. 152)

Any comments you want to include about the origin access identity.

Type: String

Required: Yes

Response Syntax

```
HTTP/1.1 200
```

API Version 2017-10-30

152
Response Elements

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

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

CloudFrontOriginAccessIdentity (p. 152)

Root level tag for the CloudFrontOriginAccessIdentity parameters.

Required: Yes

CloudFrontOriginAccessIdentityConfig (p. 152)

The current configuration information for the identity.

Type: CloudFrontOriginAccessIdentityConfig (p. 204) object

Id (p. 152)

The ID for the origin access identity, for example, E74FTE3AJFJ256A.

Type: String

S3CanonicalUserId (p. 152)

The Amazon S3 canonical user ID for the origin access identity, used when giving the origin access identity read permission to an object in Amazon S3.

Type: String

Errors

For information about the errors that are common to all actions, see Common Errors (p. 302).

AccessDenied

Access denied.

HTTP Status Code: 403

IllegalUpdate

Origin and CallerReference cannot be updated.

HTTP Status Code: 400

InconsistentQuantities

The value of Quantity and the size of Items don't match.

HTTP Status Code: 400
InvalidArgument

The argument is invalid.

HTTP Status Code: 400

InvalidIfMatchVersion

The If-Match version is missing or not valid for the distribution.

HTTP Status Code: 400

MissingBody

This operation requires a body. Ensure that the body is present and the Content-Type header is set.

HTTP Status Code: 400

NoSuchCloudFrontOriginAccessIdentity

The specified origin access identity does not exist.

HTTP Status Code: 404

PreconditionFailed

The precondition given in one or more of the request-header fields evaluated to false.

HTTP Status Code: 412

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
UpdateDistribution

Updates the configuration for a web distribution. Perform the following steps.

For information about updating a distribution using the CloudFront console, see Creating or Updating a Web Distribution Using the CloudFront Console in the Amazon CloudFront Developer Guide.

To update a web distribution using the CloudFront API

1. Submit a GetDistributionConfig (p. 85) request to get the current configuration and an Etag header for the distribution.

   **Note**
   If you update the distribution again, you need to get a new Etag header.

2. Update the XML document that was returned in the response to your GetDistributionConfig request to include the desired changes. You can't change the value of CallerReference. If you try to change this value, CloudFront returns an IllegalUpdate error.

   **Important**
   The new configuration replaces the existing configuration; the values that you specify in an UpdateDistribution request are not merged into the existing configuration. When you add, delete, or replace values in an element that allows multiple values (for example, CNAME), you must specify all of the values that you want to appear in the updated distribution. In addition, you must update the corresponding Quantity element.

3. Submit an UpdateDistribution request to update the configuration for your distribution:
   - In the request body, include the XML document that you updated in Step 2. The request body must include an XML document with a DistributionConfig element.
   - Set the value of the HTTP If-Match header to the value of the ETag header that CloudFront returned when you submitted the GetDistributionConfig request in Step 1.

4. Review the response to the UpdateDistribution request to confirm that the configuration was successfully updated.

5. Optional: Submit a GetDistribution (p. 79) request to confirm that your changes have propagated. When propagation is complete, the value of Status is Deployed.

   **Important**
   Beginning with the 2012-05-05 version of the CloudFront API, we made substantial changes to the format of the XML document that you include in the request body when you create or update a distribution. With previous versions of the API, we discovered that it was too easy to accidentally delete one or more values for an element that accepts multiple values, for example, CNAMEs and trusted signers. Our changes for the 2012-05-05 release are intended to prevent these accidental deletions and to notify you when there's a mismatch between the number of values you say you're specifying in the Quantity element and the number of values you're actually specifying.

Request Syntax

```
PUT /2017-10-30/distribution/Id/config HTTP/1.1
<?xml version="1.0" encoding="UTF-8"?>
<DistributionConfig xmlns="http://cloudfront.amazonaws.com/doc/2017-10-30/"
  <Aliases>
    <Items>
      <CNAME>string</CNAME>
    </Items>
    <Quantity>integer</Quantity>
  </Aliases>
```
<Items>
  <CacheBehavior>
    <AllowedMethods>
      <CachedMethods>
        <Items>
          <Method>string</Method>
        </Items>
        <Quantity>integer</Quantity>
      </CachedMethods>
      <Items>
        <Method>string</Method>
      </Items>
      <Quantity>integer</Quantity>
    </AllowedMethods>
    <Compress>boolean</Compress>
    <DefaultTTL>long</DefaultTTL>
    <FieldLevelEncryptionId>string</FieldLevelEncryptionId>
    <ForwardedValues>
      <Cookies>
        <Forward>string</Forward>
        <WhitelistedNames>
          <Items>
            <Name>string</Name>
          </Items>
          <Quantity>integer</Quantity>
        </WhitelistedNames>
      </Cookies>
      <Headers>
        <Items>
          <Name>string</Name>
        </Items>
        <Quantity>integer</Quantity>
      </Headers>
      <QueryString>boolean</QueryString>
      <QueryStringCacheKeys>
        <Items>
          <Name>string</Name>
        </Items>
        <Quantity>integer</Quantity>
      </QueryStringCacheKeys>
    </ForwardedValues>
    <LambdaFunctionAssociations>
      <Items>
        <LambdaFunctionAssociation>
          <EventType>string</EventType>
          <LambdaFunctionARN>string</LambdaFunctionARN>
        </LambdaFunctionAssociation>
      </Items>
      <Quantity>integer</Quantity>
    </LambdaFunctionAssociations>
    <MaxTTL>long</MaxTTL>
    <MinTTL>long</MinTTL>
    <PathPattern>string</PathPattern>
    <SmoothStreaming>boolean</SmoothStreaming>
    <TargetOriginId>string</TargetOriginId>
    <TrustedSigners>
      <Enabled>boolean</Enabled>
      <Items>
        <AwsAccountNumber>string</AwsAccountNumber>
      </Items>
      <Quantity>integer</Quantity>
    </TrustedSigners>
    <ViewerProtocolPolicy>string</ViewerProtocolPolicy>
  </CacheBehavior>
</Items>
<Quantity>integer</Quantity>
</CacheBehaviors>
<CallerReference>string</CallerReference>
<Comment>string</Comment>
<CustomErrorResponses>
 <Items>
  <CustomErrorResponse>
   <ErrorCachingMinTTL>long</ErrorCachingMinTTL>
   <ErrorCode>integer</ErrorCode>
   <ResponseCode>string</ResponseCode>
   <ResponsePagePath>string</ResponsePagePath>
  </CustomErrorResponse>
 </Items>
<Quantity>integer</Quantity>
</CustomErrorResponses>

<DefaultCacheBehavior>
<AllowedMethods>
 <CachedMethods>
  <Items>
   <Method>string</Method>
  </Items>
<Quantity>integer</Quantity>
</CachedMethods>
 <Items>
  <Method>string</Method>
 </Items>
<Quantity>integer</Quantity>
</AllowedMethods>
<Compress>boolean</Compress>
<DefaultTTL>long</DefaultTTL>
<FieldLevelEncryptionId>string</FieldLevelEncryptionId>
<ForwardedValues>
 <Cookies>
  <Forward>string</Forward>
  <WhitelistedNames>
   <Items>
    <Name>string</Name>
   </Items>
<Quantity>integer</Quantity>
  </WhitelistedNames>
 </Cookies>
 <Headers>
  <Items>
   <Name>string</Name>
  </Items>
<Quantity>integer</Quantity>
</Headers>
<QueryString>boolean</QueryString>
<QueryStringLengthCacheKeys>
 <Items>
  <Name>string</Name>
 </Items>
<Quantity>integer</Quantity>
</QueryStringLengthCacheKeys>
</ForwardedValues>
<LambdaFunctionAssociations>
 <Items>
  <LambdaFunctionAssociation>
   <EventType>string</EventType>
   <LambdaFunctionARN>string</LambdaFunctionARN>
  </LambdaFunctionAssociation>
 </Items>
<Quantity>integer</Quantity>
</LambdaFunctionAssociations>
</MaxTTL>long</MaxTTL>
<MinTTL>long</MinTTL>
<SmoothStreaming>boolean</SmoothStreaming>
<TargetOriginId>string</TargetOriginId>
<TrustedSigners>
  <Enabled>boolean</Enabled>
  <Items>
    <AwsAccountNumber>string</AwsAccountNumber>
  </Items>
</TrustedSigners>
<ViewerProtocolPolicy>string</ViewerProtocolPolicy>
</DefaultCacheBehavior>
(DefaultRootObject)string
<Enabled>boolean</Enabled>
<HttpVersion>string</HttpVersion>
<IsIPV6Enabled>boolean</IsIPV6Enabled>
<Logging>
  <Bucket>string</Bucket>
  <Enabled>boolean</Enabled>
  <IncludeCookies>boolean</IncludeCookies>
  <Prefix>string</Prefix>
</Logging>
<Origins>
  <Items>
    <Origin>
      <CustomHeaders>
        <Items>
          <OriginCustomHeader>
            <HeaderValue>string</HeaderValue>
            <HeaderName>string</HeaderName>
          </OriginCustomHeader>
        </Items>
      </CustomHeaders>
      <CustomOriginConfig>
        <HTTPPort>integer</HTTPPort>
        <HTTPSPort>integer</HTTPSPort>
        <OriginKeepaliveTimeout>integer</OriginKeepaliveTimeout>
        <OriginReadTimeout>integer</OriginReadTimeout>
        <OriginSslProtocols>
          <Items>
            <SslProtocol>string</SslProtocol>
          </Items>
        </OriginSslProtocols>
        <DomainName>string</DomainName>
        <Id>string</Id>
        <OriginPath>string</OriginPath>
      </CustomOriginConfig>
    </Origin>
  </Items>
</Origins>
<PriceClass>string</PriceClass>
<Restrictions>
  <GeoRestriction>
    <Items>
      <Location>string</Location>
    </Items>
  </GeoRestriction>
  <RestrictionType>string</RestrictionType>
</Restrictions>
<ViewerCertificate>
URI Request Parameters

The request does not use any URI parameters.

Request Body

The request accepts the following data in XML format.

DistributionConfig (p. 155)

Root level tag for the DistributionConfig parameters.

Required: Yes

Aliases (p. 155)

A complex type that contains information about CNAMEs (alternate domain names), if any, for this distribution.

Type: Aliases (p. 194) object

Required: No

CacheBehaviors (p. 155)

A complex type that contains zero or more CacheBehavior elements.

Type: CacheBehaviors (p. 201) object

Required: No

CallerReference (p. 155)

A unique value (for example, a date-time stamp) that ensures that the request can't be replayed.

If the value of CallerReference is new (regardless of the content of the DistributionConfig object), CloudFront creates a new distribution.

If CallerReference is a value you already sent in a previous request to create a distribution, and if the content of the DistributionConfig is identical to the original request (ignoring white space), CloudFront returns the same the response that it returned to the original request.

If CallerReference is a value you already sent in a previous request to create a distribution but the content of the DistributionConfig is different from the original request, CloudFront returns a DistributionAlreadyExists error.

Type: String

Required: Yes

Comment (p. 155)

Any comments you want to include about the distribution.
If you don't want to specify a comment, include an empty `Comment` element.

To delete an existing comment, update the distribution configuration and include an empty `Comment` element.

To add or change a comment, update the distribution configuration and specify the new comment.

Type: String  
Required: Yes

**CustomErrorResponses (p. 155)**

A complex type that controls the following:

- Whether CloudFront replaces HTTP status codes in the 4xx and 5xx range with custom error messages before returning the response to the viewer.
- How long CloudFront caches HTTP status codes in the 4xx and 5xx range.

For more information about custom error pages, see Customizing Error Responses in the Amazon CloudFront Developer Guide.

Type: `CustomErrorResponses (p. 215)` object  
Required: No

**DefaultCacheBehavior (p. 155)**

A complex type that describes the default cache behavior if you don't specify a `CacheBehavior` element or if files don't match any of the values of `PathPattern` in `CacheBehavior` elements. You must create exactly one default cache behavior.

Type: `DefaultCacheBehavior (p. 219)` object  
Required: Yes

**DefaultRootObject (p. 155)**

The object that you want CloudFront to request from your origin (for example, `index.html`) when a viewer requests the root URL for your distribution (http://www.example.com) instead of an object in your distribution (http://www.example.com/product-description.html). Specifying a default root object avoids exposing the contents of your distribution.

Specify only the object name, for example, `index.html`. Don't add a `/` before the object name.

If you don't want to specify a default root object when you create a distribution, include an empty `DefaultRootObject` element.

To delete the default root object from an existing distribution, update the distribution configuration and include an empty `DefaultRootObject` element.

To replace the default root object, update the distribution configuration and specify the new object.

For more information about the default root object, see Creating a Default Root Object in the Amazon CloudFront Developer Guide.

Type: String  
Required: No

**Enabled (p. 155)**

From this field, you can enable or disable the selected distribution.
If you specify `false` for `Enabled` but you specify values for `Bucket` and `Prefix`, the values are automatically deleted.

Type: Boolean

Required: Yes

**HttpVersion (p. 155)**

(Optional) Specify the maximum HTTP version that you want viewers to use to communicate with CloudFront. The default value for new web distributions is `http2`. Viewers that don’t support HTTP/2 automatically use an earlier HTTP version.

For viewers and CloudFront to use HTTP/2, viewers must support TLS 1.2 or later, and must support Server Name Identification (SNI).

In general, configuring CloudFront to communicate with viewers using HTTP/2 reduces latency. You can improve performance by optimizing for HTTP/2. For more information, do an Internet search for "HTTP/2 optimization."

Type: String

Valid Values: http1.1 | http2

Required: No

**IsIPV6Enabled (p. 155)**

If you want CloudFront to respond to IPv6 DNS requests with an IPv6 address for your distribution, specify `true`. If you specify `false`, CloudFront responds to IPv6 DNS requests with the DNS response code `NOERROR` and with no IP addresses. This allows viewers to submit a second request, for an IPv4 address for your distribution.

In general, you should enable IPv6 if you have users on IPv6 networks who want to access your content. However, if you're using signed URLs or signed cookies to restrict access to your content, and if you're using a custom policy that includes the `IpAddress` parameter to restrict the IP addresses that can access your content, don't enable IPv6. If you want to restrict access to some content by IP address and not restrict access to other content (or restrict access but not by IP address), you can create two distributions. For more information, see Creating a Signed URL Using a Custom Policy in the Amazon CloudFront Developer Guide.

If you're using an Amazon Route 53 alias resource record set to route traffic to your CloudFront distribution, you need to create a second alias resource record set when both of the following are true:

- You enable IPv6 for the distribution
- You're using alternate domain names in the URLs for your objects

For more information, see Routing Traffic to an Amazon CloudFront Web Distribution by Using Your Domain Name in the Amazon Route 53 Developer Guide.

If you created a CNAME resource record set, either with Amazon Route 53 or with another DNS service, you don’t need to make any changes. A CNAME record will route traffic to your distribution regardless of the IP address format of the viewer request.

Type: Boolean

Required: No

**Logging (p. 155)**

A complex type that controls whether access logs are written for the distribution.
For more information about logging, see Access Logs in the Amazon CloudFront Developer Guide.

Type: LoggingConfig (p. 262) object

Required: No

**Origins (p. 155)**

A complex type that contains information about origins for this distribution.

Type: Origins (p. 267) object

Required: Yes

**PriceClass (p. 155)**

The price class that corresponds with the maximum price that you want to pay for CloudFront service. If you specify PriceClass_All, CloudFront responds to requests for your objects from all CloudFront edge locations.

If you specify a price class other than PriceClass_All, CloudFront serves your objects from the CloudFront edge location that has the lowest latency among the edge locations in your price class. Viewers who are in or near regions that are excluded from your specified price class may encounter slower performance.

For more information about price classes, see Choosing the Price Class for a CloudFront Distribution in the Amazon CloudFront Developer Guide. For information about CloudFront pricing, including how price classes map to CloudFront regions, see Amazon CloudFront Pricing.

Type: String

Valid Values: PriceClass_100 | PriceClass_200 | PriceClass_All

Required: No

**Restrictions (p. 155)**

A complex type that identifies ways in which you want to restrict distribution of your content.

Type: Restrictions (p. 278) object

Required: No

**ViewerCertificate (p. 155)**

A complex type that specifies the following:

- Whether you want viewers to use HTTP or HTTPS to request your objects.
- If you want viewers to use HTTPS, whether you're using an alternate domain name such as example.com or the CloudFront domain name for your distribution, such as d11111abcdef8.cloudfront.net.
- If you're using an alternate domain name, whether AWS Certificate Manager (ACM) provided the certificate, or you purchased a certificate from a third-party certificate authority and imported it into ACM or uploaded it to the IAM certificate store.

You must specify only one of the following values:

- ViewerCertificate:ACMCertificateArn (p. 297)
- ViewerCertificate:IAMCertificateId (p. 298)
- ViewerCertificate:CloudFrontDefaultCertificate (p. 297)

Don't specify false for CloudFrontDefaultCertificate.
If you want viewers to use HTTP instead of HTTPS to request your objects: Specify the following value:

```xml
<CloudFrontDefaultCertificate>true</CloudFrontDefaultCertificate>
```

In addition, specify allow-all for ViewerProtocolPolicy for all of your cache behaviors.

If you want viewers to use HTTPS to request your objects: Choose the type of certificate that you want to use based on whether you're using an alternate domain name for your objects or the CloudFront domain name:

- If you're using an alternate domain name, such as example.com: Specify one of the following values, depending on whether ACM provided your certificate or you purchased your certificate from third-party certificate authority:
  - `<ACMCertificateArn>`
  
  where **ARN for ACM SSL/TLS certificate** is the ARN for the ACM SSL/TLS certificate that you want to use for this distribution.
  - `<IAMCertificateId>`

  where **IAM certificate ID** is the ID that IAM returned when you added the certificate to the IAM certificate store.

If you specify `ACMCertificateArn` or `IAMCertificateId`, you must also specify a value for `SSLSupportMethod`.

If you choose to use an ACM certificate or a certificate in the IAM certificate store, we recommend that you use only an alternate domain name in your object URLs (https://example.com/logo.jpg). If you use the domain name that is associated with your CloudFront distribution (such as https://d111111abcdef8.cloudfront.net/logo.jpg) and the viewer supports SNI, then CloudFront behaves normally. However, if the browser does not support SNI, the user's experience depends on the value that you choose for `SSLSupportMethod`:

- `vip`: The viewer displays a warning because there is a mismatch between the CloudFront domain name and the domain name in your SSL/TLS certificate.
- `sni-only`: CloudFront drops the connection with the browser without returning the object.

- If you're using the CloudFront domain name for your distribution, such as `d111111abcdef8.cloudfront.net`: Specify the following value:

  ```xml
  <CloudFrontDefaultCertificate>true</CloudFrontDefaultCertificate>
  ```

If you want viewers to use HTTPS, you must also specify one of the following values in your cache behaviors:

- `<ViewerProtocolPolicy>`
  
  ```xml
  https-only
  ```

- `<ViewerProtocolPolicy>`
  
  ```xml
  redirect-to-https
  ```

You can also optionally require that CloudFront use HTTPS to communicate with your origin by specifying one of the following values for the applicable origins:

- `<OriginProtocolPolicy>`
  
  ```xml
  https-only
  ```

- `<OriginProtocolPolicy>`
  
  ```xml
  match-viewer
  ```

For more information, see Using Alternate Domain Names and HTTPS in the Amazon CloudFront Developer Guide.

Type: `ViewerCertificate` (p. 296) object

Required: No

`WebACLId` (p. 155)

A unique identifier that specifies the AWS WAF web ACL, if any, to associate with this distribution.
AWS WAF is a web application firewall that lets you monitor the HTTP and HTTPS requests that are forwarded to CloudFront, and lets you control access to your content. Based on conditions that you specify, such as the IP addresses that requests originate from or the values of query strings, CloudFront responds to requests either with the requested content or with an HTTP 403 status code (Forbidden). You can also configure CloudFront to return a custom error page when a request is blocked. For more information about AWS WAF, see the AWS WAF Developer Guide.

Type: String

Required: No

Response Syntax

HTTP/1.1 200
<?xml version="1.0" encoding="UTF-8"?>
<Distribution>
  <ActiveTrustedSigners>
    <Enabled>boolean</Enabled>
    <Items>
      <Signer>
        <AwsAccountNumber>string</AwsAccountNumber>
        <KeyPairIds>
          <Items>
            <KeyPairId>string</KeyPairId>
          </Items>
          <Quantity>integer</Quantity>
        </KeyPairIds>
      </Signer>
    </Items>
    <Quantity>integer</Quantity>
  </ActiveTrustedSigners>
  <ARN>string</ARN>
  <DistributionConfig>
    <Aliases>
      <Items>
        <CNAME>string</CNAME>
      </Items>
      <Quantity>integer</Quantity>
    </Aliases>
    <CacheBehaviors>
      <Items>
        <CacheBehavior>
          <AllowedMethods>
            <CachedMethods>
              <Items>
                <Method>string</Method>
              </Items>
              <Quantity>integer</Quantity>
            </CachedMethods>
          </AllowedMethods>
          <Compress>boolean</Compress>
          <DefaultTTL>long</DefaultTTL>
          <FieldLevelEncryptionId>string</FieldLevelEncryptionId>
          <ForwardedValues>
            <Cookies>
              <Forward>string</Forward>
            </Cookies>
          </ForwardedValues>
        </CacheBehavior>
      </Items>
    </CacheBehaviors>
  </DistributionConfig>
</Distribution>
<Name>string</Name>
</Items>
<Quantity>integer</Quantity>
</WhitelistedNames>
</Cookies>
<Headers>
<Items>
<Name>string</Name>
</Items>
<Quantity>integer</Quantity>
</Headers>
<QueryString>boolean</QueryString>
<QueryStringCacheKeys>
<Items>
<Name>string</Name>
</Items>
<Quantity>integer</Quantity>
</QueryStringCacheKeys>
</ForwardedValues>
<LambdaFunctionAssociations>
<Items>
<LambdaFunctionAssociation>
<EventType>string</EventType>
<LambdaFunctionARN>string</LambdaFunctionARN>
</LambdaFunctionAssociation>
</Items>
<Quantity>integer</Quantity>
</LambdaFunctionAssociations>
<MaxTTL>long</MaxTTL>
<MinTTL>long</MinTTL>
<PathPattern>string</PathPattern>
<SmoothStreaming>boolean</SmoothStreaming>
<TargetOriginId>string</TargetOriginId>
<TrustedSigners>
<Enabled>boolean</Enabled>
<Items>
<AwsAccountNumber>string</AwsAccountNumber>
</Items>
<Quantity>integer</Quantity>
</TrustedSigners>
</CacheBehavior>
</Items>
<Quantity>integer</Quantity>
</CacheBehaviors>
<CallerReference>string</CallerReference>
<Comment>string</Comment>
<CustomErrorResponses>
<Items>
<CustomErrorResponse>
<ErrorCachingMinTTL>long</ErrorCachingMinTTL>
<ErrorCode>integer</ErrorCode>
<ResponseCode>string</ResponseCode>
<ResponsePagePath>string</ResponsePagePath>
</CustomErrorResponse>
</Items>
<Quantity>integer</Quantity>
</CustomErrorResponses>
<DefaultCacheBehavior>
<AllowedMethods>
<CachedMethods>
<Items>
<Method>string</Method>
</Items>
<Quantity>integer</Quantity>
</CachedMethods>
<Items>
  <Method>string</Method>
  <Quantity>integer</Quantity>
</Items>
<AllowedMethods>
<Compress>boolean</Compress>
<DefaultTTL>long</DefaultTTL>
<FieldLevelEncryptionId>string</FieldLevelEncryptionId>
<ForwardedValues>
  <Cookies>
    <Forward>string</Forward>
    <WhitelistedNames>
      <Items>
        <Name>string</Name>
      </Items>
    </WhitelistedNames>
  </Cookies>
  <Headers>
    <Items>
      <Name>string</Name>
    </Items>
    <Quantity>integer</Quantity>
  </Headers>
  <QueryString>boolean</QueryString>
  <QueryStringCacheKeys>
    <Items>
      <Name>string</Name>
    </Items>
    <Quantity>integer</Quantity>
  </QueryStringCacheKeys>
</ForwardedValues>
<LambdaFunctionAssociations>
  <Items>
    <LambdaFunctionAssociation>
      <EventType>string</EventType>
      <LambdaFunctionARN>string</LambdaFunctionARN>
    </LambdaFunctionAssociation>
  </Items>
  <Quantity>integer</Quantity>
</LambdaFunctionAssociations>
<MaxTTL>long</MaxTTL>
<MinTTL>long</MinTTL>
<SmoothStreaming>boolean</SmoothStreaming>
<TargetOriginId>string</TargetOriginId>
<TrustedSigners>
  <Enabled>boolean</Enabled>
  <Items>
    <AwsAccountNumber>string</AwsAccountNumber>
  </Items>
  <Quantity>integer</Quantity>
</TrustedSigners>
<ViewerProtocolPolicy>string</ViewerProtocolPolicy>
</DefaultCacheBehavior>
<DefaultRootObject>string</DefaultRootObject>
<Enabled>boolean</Enabled>
<HttpVersion>string</HttpVersion>
<IsIPV6Enabled>boolean</IsIPV6Enabled>
<Logging>
  <Bucket>string</Bucket>
  <Enabled>boolean</Enabled>
  <IncludeCookies>boolean</IncludeCookies>
  <Prefix>string</Prefix>
</Logging>
<Origins>
  <Items>
  </Items>
Response Elements

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

**Distribution (p. 164)**

Root level tag for the Distribution parameters.

Required: Yes

**ActiveTrustedSigners (p. 164)**

CloudFront automatically adds this element to the response only if you've set up the distribution to serve private content with signed URLs. The element lists the key pair IDs that CloudFront is aware of for each trusted signer. The `Signer` child element lists the AWS account number of the trusted signer (or an empty `Self` element if the signer is you). The `Signer` element also includes the IDs of any active key pairs associated with the trusted signer's AWS account. If no `KeyPairId` element appears for a `Signer`, that signer can't create working signed URLs.

Type: `ActiveTrustedSigners (p. 192)` object

**ARN (p. 164)**

The ARN (Amazon Resource Name) for the distribution. For example: `arn:aws:cloudfront::123456789012:distribution/EDFDVBD632BHDS5`, where `123456789012` is your AWS account ID.

Type: String

**DistributionConfig (p. 164)**

The current configuration information for the distribution. Send a GET request to the `/CloudFront API version/distribution ID/config` resource.

Type: `DistributionConfig (p. 224)` object

**DomainName (p. 164)**

The domain name corresponding to the distribution, for example, `d111111abcdef8.cloudfront.net`.

Type: String

**Id (p. 164)**

The identifier for the distribution. For example: `EDFDVBD632BHDS5`.

Type: String

**InProgressInvalidationBatches (p. 164)**

The number of invalidation batches currently in progress.

Type: Integer

**LastModifiedTime (p. 164)**

The date and time the distribution was last modified.

Type: Timestamp

**Status (p. 164)**

This response element indicates the current status of the distribution. When the status is `Deployed`, the distribution's information is fully propagated to all CloudFront edge locations.

Type: String
Errors

For information about the errors that are common to all actions, see Common Errors (p. 302).

AccessDenied

Access denied.

HTTP Status Code: 403

CNAMEAlreadyExists

HTTP Status Code: 409

IllegalFieldLevelEncryptionConfigAssociationWithCacheBehavior

The specified configuration for field-level encryption can't be associated with the specified cache behavior.

HTTP Status Code: 400

IllegalUpdate

Origin and CallerReference cannot be updated.

HTTP Status Code: 400

InconsistentQuantities

The value of Quantity and the size of Items don't match.

HTTP Status Code: 400

InvalidArgument

The argument is invalid.

HTTP Status Code: 400

InvalidDefaultRootObject

The default root object file name is too big or contains an invalid character.

HTTP Status Code: 400

InvalidErrorCode

HTTP Status Code: 400

InvalidForwardCookies

Your request contains forward cookies option which doesn't match with the expectation for the whitelisted list of cookie names. Either list of cookie names has been specified when not allowed or list of cookie names is missing when expected.

HTTP Status Code: 400

InvalidGeoRestrictionParameter

HTTP Status Code: 400

InvalidHeadersForS3Origin

HTTP Status Code: 400

InvalidIfMatchVersion

The If-Match version is missing or not valid for the distribution.
HTTP Status Code: 400
InvalidLambdaFunctionAssociation
The specified Lambda function association is invalid.

HTTP Status Code: 400
InvalidLocationCode
HTTP Status Code: 400
InvalidMinimumProtocolVersion
HTTP Status Code: 400
InvalidOriginAccessIdentity
The origin access identity is not valid or doesn't exist.

HTTP Status Code: 400
InvalidOriginKeepaliveTimeout
HTTP Status Code: 400
InvalidOriginReadTimeout
HTTP Status Code: 400
InvalidQueryStringParameters
HTTP Status Code: 400
InvalidRelativePath
The relative path is too big, is not URL-encoded, or does not begin with a slash (/).

HTTP Status Code: 400
InvalidRequiredProtocol
This operation requires the HTTPS protocol. Ensure that you specify the HTTPS protocol in your request, or omit the RequiredProtocols element from your distribution configuration.

HTTP Status Code: 400
InvalidResponseCode
HTTP Status Code: 400
InvalidTTLOrder
HTTP Status Code: 400
InvalidViewerCertificate
HTTP Status Code: 400
InvalidWebACLId
HTTP Status Code: 400
MissingBody
This operation requires a body. Ensure that the body is present and the Content-Type header is set.

HTTP Status Code: 400
NoSuchDistribution
The specified distribution does not exist.
HTTP Status Code: 404
**NoSuchFieldLevelEncryptionConfig**
The specified configuration for field-level encryption doesn't exist.

HTTP Status Code: 404
**NoSuchOrigin**
No origin exists with the specified Origin Id.

HTTP Status Code: 404
**PreconditionFailed**
The precondition given in one or more of the request-header fields evaluated to false.

HTTP Status Code: 412
**TooManyCacheBehaviors**
You cannot create more cache behaviors for the distribution.

HTTP Status Code: 400
**TooManyCertificates**
You cannot create anymore custom SSL/TLS certificates.

HTTP Status Code: 400
**TooManyCookieNamesInWhiteList**
Your request contains more cookie names in the whitelist than are allowed per cache behavior.

HTTP Status Code: 400
**TooManyDistributionCNAMEs**
Your request contains more CNAMEs than are allowed per distribution.

HTTP Status Code: 400
**TooManyDistributionsAssociatedToFieldLevelEncryptionConfig**
The maximum number of distributions have been associated with the specified configuration for field-level encryption.

HTTP Status Code: 400
**TooManyDistributionsWithLambdaAssociations**
Processing your request would cause the maximum number of distributions with Lambda function associations per owner to be exceeded.

HTTP Status Code: 400
**TooManyHeadersInForwardedValues**

HTTP Status Code: 400
**TooManyLambdaFunctionAssociations**
Your request contains more Lambda function associations than are allowed per distribution.

HTTP Status Code: 400
**TooManyOriginCustomHeaders**

HTTP Status Code: 400
TooManyOrigins
You cannot create more origins for the distribution.
HTTP Status Code: 400

TooManyQueryStringParameters
HTTP Status Code: 400

TooManyTrustedSigners
Your request contains more trusted signers than are allowed per distribution.
HTTP Status Code: 400

TrustedSignerDoesNotExist
One or more of your trusted signers don't exist.
HTTP Status Code: 400

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
UpdateFieldLevelEncryptionConfig

Update a field-level encryption configuration.

Request Syntax

PUT /2017-10-30/field-level-encryption/Id/config HTTP/1.1
<?xml version="1.0" encoding="UTF-8"?>
<FieldLevelEncryptionConfig xmlns="http://cloudfront.amazonaws.com/doc/2017-10-30/">
  <CallerReference>string</CallerReference>
  <Comment>string</Comment>
  <ContentTypeProfileConfig>
    <ContentTypeProfiles>
      <Items>
        <ContentTypeProfile>
          <ContentType>string</ContentType>
          <Format>string</Format>
          <ProfileId>string</ProfileId>
        </ContentTypeProfile>
      </Items>
      <Quantity>integer</Quantity>
    </ContentTypeProfiles>
    <ForwardWhenContentTypeIsUnknown>boolean</ForwardWhenContentTypeIsUnknown>
  </ContentTypeProfileConfig>
  <QueryArgProfileConfig>
    <QueryArgProfiles>
      <Items>
        <QueryArgProfile>
          <ProfileId>string</ProfileId>
          <QueryArg>string</QueryArg>
        </QueryArgProfile>
      </Items>
      <Quantity>integer</Quantity>
    </QueryArgProfiles>
  </QueryArgProfileConfig>
</FieldLevelEncryptionConfig>

URI Request Parameters

The request does not use any URI parameters.

Request Body

The request accepts the following data in XML format.

FieldLevelEncryptionConfig (p. 173)

  Root level tag for the FieldLevelEncryptionConfig parameters.

  Required: Yes

CallerReference (p. 173)

  A unique number that ensures the request can't be replayed.

  Type: String

  Required: Yes
Comment (p. 173)

An optional comment about the configuration.

Type: String
Required: No

ContentTypeProfileConfig (p. 173)

A complex data type that specifies when to forward content if a content type isn't recognized and profiles to use as by default in a request if a query argument doesn't specify a profile to use.

Type: ContentTypeProfileConfig (p. 209) object
Required: No

QueryArgProfileConfig (p. 173)

A complex data type that specifies when to forward content if a profile isn't found and the profile that can be provided as a query argument in a request.

Type: QueryArgProfileConfig (p. 275) object
Required: No

Response Syntax

```xml
HTTP/1.1 200
<?xml version="1.0" encoding="UTF-8"?>
<FieldLevelEncryption>
  <FieldLevelEncryptionConfig>
    <CallerReference>string</CallerReference>
    <Comment>string</Comment>
    <ContentTypeProfileConfig>
      <ContentTypeProfiles>
        <Items>
          <ContentTypeProfile>
            <ContentType>string</ContentType>
            <Format>string</Format>
            <ProfileId>string</ProfileId>
          </ContentTypeProfile>
        </Items>
        <Quantity>integer</Quantity>
      </ContentTypeProfiles>
    </ContentTypeProfileConfig>
    <QueryArgProfileConfig>
      <QueryArgProfiles>
        <Items>
          <QueryArgProfile>
            <ProfileId>string</ProfileId>
            <QueryArg>string</QueryArg>
          </QueryArgProfile>
        </Items>
        <Quantity>integer</Quantity>
      </QueryArgProfiles>
    </QueryArgProfileConfig>
  </FieldLevelEncryptionConfig>
  <Id>string</Id>
  <LastModifiedTime>timestamp</LastModifiedTime>
</FieldLevelEncryption>
```
Response Elements

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

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

FieldLevelEncryption (p. 174)

Root level tag for the FieldLevelEncryption parameters.

Required: Yes

FieldLevelEncryptionConfig (p. 174)

A complex data type that includes the profile configurations specified for field-level encryption.

Type: FieldLevelEncryptionConfig (p. 240) object

Id (p. 174)

The configuration ID for a field-level encryption configuration which includes a set of profiles that specify certain selected data fields to be encrypted by specific public keys.

Type: String

LastModifiedTime (p. 174)

The last time the field-level encryption configuration was changed.

Type: Timestamp

Errors

For information about the errors that are common to all actions, see Common Errors (p. 302).

AccessDenied

Access denied.

HTTP Status Code: 403

IllegalUpdate

Origin and CallerReference cannot be updated.

HTTP Status Code: 400

InconsistentQuantities

The value of Quantity and the size of Items don’t match.

HTTP Status Code: 400

InvalidArgument

The argument is invalid.

HTTP Status Code: 400

InvalidIfMatchVersion

The If-Match version is missing or not valid for the distribution.

HTTP Status Code: 400
**NoSuchFieldLevelEncryptionConfig**

The specified configuration for field-level encryption doesn't exist.

HTTP Status Code: 404

**NoSuchFieldLevelEncryptionProfile**

The specified profile for field-level encryption doesn't exist.

HTTP Status Code: 404

**PreconditionFailed**

The precondition given in one or more of the request-header fields evaluated to false.

HTTP Status Code: 412

**QueryArgProfileEmpty**

No profile specified for the field-level encryption query argument.

HTTP Status Code: 400

**TooManyFieldLevelEncryptionContentTypeProfiles**

The maximum number of content type profiles for field-level encryption have been created.

HTTP Status Code: 400

**TooManyFieldLevelEncryptionQueryArgProfiles**

The maximum number of query arg profiles for field-level encryption have been created.

HTTP Status Code: 400

**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
UpdateFieldLevelEncryptionProfile

Update a field-level encryption profile.

Request Syntax

PUT /2017-10-30/field-level-encryption-profile/Id/config HTTP/1.1
<?xml version="1.0" encoding="UTF-8"?>
<FieldLevelEncryptionProfileConfig xmlns="http://cloudfront.amazonaws.com/doc/2017-10-30/">
  <CallerReference>
    <string/></CallerReference>
  <Comment>
    string</Comment>
  <EncryptionEntities>
    <Items>
      <EncryptionEntity>
        <FieldPatterns>
          <Items>
            <FieldPattern>
              string</FieldPattern>
          </Items>
        </FieldPatterns>
      </Items>
      <ProviderId>
        string</ProviderId>
      <PublicKeyId>
        string</PublicKeyId>
    </EncryptionEntity>
    <Items>
      <EncryptionEntity>
        <FieldPatterns>
          <Items>
            <FieldPattern>
              string</FieldPattern>
          </Items>
        </FieldPatterns>
      </Items>
      <ProviderId>
        string</ProviderId>
      <PublicKeyId>
        string</PublicKeyId>
    </EncryptionEntity>
  </Items>
  <Name>
    string</Name>
</FieldLevelEncryptionProfileConfig>

URI Request Parameters

The request does not use any URI parameters.

Request Body

The request accepts the following data in XML format.

FieldLevelEncryptionProfileConfig (p. 177)

Root level tag for the FieldLevelEncryptionProfileConfig parameters.

Required: Yes

CallerReference (p. 177)

A unique number that ensures the request can't be replayed.

Type: String

Required: Yes

Comment (p. 177)

An optional comment for the field-level encryption profile.

Type: String

Required: No
EncryptionEntities (p. 177)

A complex data type of encryption entities for the field-level encryption profile that include the public key ID, provider, and field patterns for specifying which fields to encrypt with this key.

Type: EncryptionEntities (p. 237) object

Required: Yes

Name (p. 177)

Profile name for the field-level encryption profile.

Type: String

Required: Yes

Response Syntax

HTTP/1.1 200
<?xml version="1.0" encoding="UTF-8"?><FieldLevelEncryptionProfile><FieldLevelEncryptionProfileConfig><CallerReference>string</CallerReference><Comment>string</Comment><EncryptionEntities><Items><EncryptionEntity><FieldPatterns><Items><FieldPattern>string</FieldPattern></Items><Quantity>integer</Quantity></FieldPatterns><ProviderId>string</ProviderId><PublicKeyId>string</PublicKeyId></EncryptionEntity></Items><Quantity>integer</Quantity></EncryptionEntities><Name>string</Name></FieldLevelEncryptionProfileConfig><Id>string</Id><LastModifiedTime>timestamp</LastModifiedTime></FieldLevelEncryptionProfile>

Response Elements

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

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

FieldLevelEncryptionProfile (p. 178)

Root level tag for the FieldLevelEncryptionProfile parameters.

Required: Yes

FieldLevelEncryptionProfileConfig (p. 178)

A complex data type that includes the profile name and the encryption entities for the field-level encryption profile.
Type: FieldLevelEncryptionProfileConfig (p. 243) object

Id (p. 178)

The ID for a field-level encryption profile configuration which includes a set of profiles that specify certain selected data fields to be encrypted by specific public keys.

Type: String

LastModifiedTime (p. 178)

The last time the field-level encryption profile was updated.

Type: Timestamp

Errors

For information about the errors that are common to all actions, see Common Errors (p. 302).

AccessDenied

Access denied.

HTTP Status Code: 403

FieldLevelEncryptionProfileAlreadyExists

The specified profile for field-level encryption already exists.

HTTP Status Code: 409

FieldLevelEncryptionProfileSizeExceeded

The maximum size of a profile for field-level encryption was exceeded.

HTTP Status Code: 400

IllegalUpdate

Origin and CallerReference cannot be updated.

HTTP Status Code: 400

InconsistentQuantities

The value of Quantity and the size of Items don't match.

HTTP Status Code: 400

InvalidArgument

The argument is invalid.

HTTP Status Code: 400

InvalidIfMatchVersion

The If-Match version is missing or not valid for the distribution.

HTTP Status Code: 400

NoSuchFieldLevelEncryptionProfile

The specified profile for field-level encryption doesn't exist.

HTTP Status Code: 404
NoSuchPublicKey

The specified public key doesn't exist.

HTTP Status Code: 404

PreconditionFailed

The precondition given in one or more of the request-header fields evaluated to false.

HTTP Status Code: 412

TooManyFieldLevelEncryptionEncryptionEntities

The maximum number of encryption entities for field-level encryption have been created.

HTTP Status Code: 400

TooManyFieldLevelEncryptionFieldPatterns

The maximum number of field patterns for field-level encryption have been created.

HTTP Status Code: 400

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
UpdatePublicKey

Update public key information. Note that the only value you can change is the comment.

Request Syntax

```
PUT /2017-10-30/public-key/Id/config HTTP/1.1
<?xml version="1.0" encoding="UTF-8"?>
<PublicKeyConfig xmlns="http://cloudfront.amazonaws.com/doc/2017-10-30/">
  <CallerReference>string</CallerReference>
  <Comment>string</Comment>
  <EncodedKey>string</EncodedKey>
  <Name>string</Name>
</PublicKeyConfig>
```

URI Request Parameters

The request does not use any URI parameters.

Request Body

The request accepts the following data in XML format.

**PublicKeyConfig (p. 181)**

Root level tag for the PublicKeyConfig parameters.

Required: Yes

**CallerReference (p. 181)**

A unique number that ensures the request can't be replayed.

Type: String

Required: Yes

**Comment (p. 181)**

An optional comment about a public key.

Type: String

Required: No

**EncodedKey (p. 181)**

The encoded public key that you want to add to CloudFront to use with features like field-level encryption.

Type: String

Required: Yes

**Name (p. 181)**

The name for a public key you add to CloudFront to use with features like field-level encryption.

Type: String

Required: Yes
Response Syntax

```
HTTP/1.1 200
<?xml version="1.0" encoding="UTF-8"?>
<PublicKey>
    <CreatedTime>timestamp</CreatedTime>
    <Id>string</Id>
    <PublicKeyConfig>
        <CallerReference>string</CallerReference>
        <Comment>string</Comment>
        <EncodedKey>string</EncodedKey>
        <Name>string</Name>
    </PublicKeyConfig>
</PublicKey>
```

Response Elements

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

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

**PublicKey (p. 182)**

Root level tag for the PublicKey parameters.

Required: Yes

**CreatedTime (p. 182)**

A time you added a public key to CloudFront.

Type: Timestamp

**Id (p. 182)**

A unique ID assigned to a public key you've added to CloudFront.

Type: String

**PublicKeyConfig (p. 182)**

A complex data type for a public key you add to CloudFront to use with features like field-level encryption.

Type: PublicKeyConfig (p. 271) object

Errors

For information about the errors that are common to all actions, see Common Errors (p. 302).

**AccessDenied**

Access denied.

HTTP Status Code: 403

**CannotChangeImmutablePublicKeyFields**

You can't change the value of a public key.

HTTP Status Code: 400
IllegalUpdate
Origin and CallerReference cannot be updated.
HTTP Status Code: 400

InvalidArgument
The argument is invalid.
HTTP Status Code: 400

InvalidIfMatchVersion
The If-Match version is missing or not valid for the distribution.
HTTP Status Code: 400

NoSuchPublicKey
The specified public key doesn't exist.
HTTP Status Code: 404

PreconditionFailed
The precondition given in one or more of the request-header fields evaluated to false.
HTTP Status Code: 412

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
UpdateStreamingDistribution

Update a streaming distribution.

Request Syntax

PUT /2017-10-30/streaming-distribution/Id/config HTTP/1.1
<?xml version="1.0" encoding="UTF-8"?>
<StreamingDistributionConfig xmlns="http://cloudfront.amazonaws.com/doc/2017-10-30/">
  <Aliases>
    <CNAME>string</CNAME>
  </Aliases>
  <CallerReference>string</CallerReference>
  <Comment>string</Comment>
  <Enabled>true</Enabled>
  <Logging>
    <Bucket>string</Bucket>
    <Enabled>true</Enabled>
    <Prefix>string</Prefix>
  </Logging>
  <PriceClass>string</PriceClass>
  <S3Origin>
    <DomainName>string</DomainName>
    <OriginAccessIdentity>string</OriginAccessIdentity>
  </S3Origin>
  <TrustedSigners>
    <Enabled>true</Enabled>
    <Items>
      <AwsAccountNumber>string</AwsAccountNumber>
    </Items>
  </TrustedSigners>
</StreamingDistributionConfig>

URI Request Parameters

The request does not use any URI parameters.

Request Body

The request accepts the following data in XML format.

StreamingDistributionConfig (p. 184)

Root level tag for the StreamingDistributionConfig parameters.

Required: Yes

Aliases (p. 184)

A complex type that contains information about CNAMEs (alternate domain names), if any, for this streaming distribution.

Type: Aliases (p. 194) object

Required: No
**CallerReference (p. 184)**

A unique number that ensures that the request can't be replayed. If the CallerReference is new (no matter the content of the StreamingDistributionConfig object), a new streaming distribution is created. If the CallerReference is a value that you already sent in a previous request to create a streaming distribution, and the content of the StreamingDistributionConfig is identical to the original request (ignoring white space), the response includes the same information returned to the original request. If the CallerReference is a value that you already sent in a previous request to create a streaming distribution but the content of the StreamingDistributionConfig is different from the original request, CloudFront returns a DistributionAlreadyExists error.

Type: String

Required: Yes

**Comment (p. 184)**

Any comments you want to include about the streaming distribution.

Type: String

Required: Yes

**Enabled (p. 184)**

Whether the streaming distribution is enabled to accept user requests for content.

Type: Boolean

Required: Yes

**Logging (p. 184)**

A complex type that controls whether access logs are written for the streaming distribution.

Type: StreamingLoggingConfig (p. 291) object

Required: No

**PriceClass (p. 184)**

A complex type that contains information about price class for this streaming distribution.

Type: String

Valid Values: PriceClass_100 | PriceClass_200 | PriceClass_All

Required: No

**S3Origin (p. 184)**

A complex type that contains information about the Amazon S3 bucket from which you want CloudFront to get your media files for distribution.

Type: S3Origin (p. 279) object

Required: Yes

**TrustedSigners (p. 184)**

A complex type that specifies any AWS accounts that you want to permit to create signed URLs for private content. If you want the distribution to use signed URLs, include this element; if you want
the distribution to use public URLs, remove this element. For more information, see Serving Private Content through CloudFront in the Amazon CloudFront Developer Guide.

Type: TrustedSigners (p. 295) object

Required: Yes

**Response Syntax**

```
HTTP/1.1 200
<?xml version="1.0" encoding="UTF-8"?>
<StreamingDistribution>
  <ActiveTrustedSigners>
    <Enabled>boolean</Enabled>
    <Items>
      <Signer>
        <AwsAccountNumber>string</AwsAccountNumber>
        <KeyPairIds>
          <Items>
            <KeyPairId>string</KeyPairId>
          </Items>
          <Quantity>integer</Quantity>
        </KeyPairIds>
        </Signer>
      </Items>
      <Quantity>integer</Quantity>
    </ActiveTrustedSigners>
    <ARN>string</ARN>
    <DomainName>string</DomainName>
    <Id>string</Id>
    <LastModifiedTime>timestamp</LastModifiedTime>
    <Status>string</Status>
    <StreamingDistributionConfig>
      <Aliases>
        <Items>
          <CNAME>string</CNAME>
        </Items>
        <Quantity>integer</Quantity>
      </Aliases>
      <CallerReference>string</CallerReference>
      <Comment>string</Comment>
      <Enabled>boolean</Enabled>
      <Logging>
        <Bucket>string</Bucket>
        <Enabled>boolean</Enabled>
        <Prefix>string</Prefix>
      </Logging>
      <PriceClass>string</PriceClass>
      <S3Origin>
        <DomainName>string</DomainName>
        <OriginAccessIdentity>string</OriginAccessIdentity>
      </S3Origin>
      <TrustedSigners>
        <Enabled>boolean</Enabled>
        <Items>
          <AwsAccountNumber>string</AwsAccountNumber>
        </Items>
        <Quantity>integer</Quantity>
      </TrustedSigners>
    </StreamingDistributionConfig>
  </StreamingDistribution>
```
Response Elements

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

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

**StreamingDistribution** (p. 186)

Root level tag for the StreamingDistribution parameters.

Required: Yes

**ActiveTrustedSigners** (p. 186)

A complex type that lists the AWS accounts, if any, that you included in the TrustedSigners complex type for this distribution. These are the accounts that you want to allow to create signed URLs for private content.

The Signer complex type lists the AWS account number of the trusted signer or self if the signer is the AWS account that created the distribution. The Signer element also includes the IDs of any active CloudFront key pairs that are associated with the trusted signer's AWS account. If no KeyPairId element appears for a Signer, that signer can't create signed URLs.

For more information, see Serving Private Content through CloudFront in the *Amazon CloudFront Developer Guide*.

Type: `ActiveTrustedSigners (p. 192)` object

**ARN** (p. 186)

Type: String

**DomainName** (p. 186)

The domain name that corresponds to the streaming distribution, for example, `s5c39gqb8ow64r.cloudfront.net`.

Type: String

**Id** (p. 186)

The identifier for the RTMP distribution. For example: `EGTXBD79EXAMPLE`.

Type: String

**LastModifiedTime** (p. 186)

The date and time that the distribution was last modified.

Type: Timestamp

**Status** (p. 186)

The current status of the RTMP distribution. When the status is `Deployed`, the distribution's information is propagated to all CloudFront edge locations.

Type: String

**StreamingDistributionConfig** (p. 186)

The current configuration information for the RTMP distribution.

Type: `StreamingDistributionConfig (p. 284)` object
Errors

For information about the errors that are common to all actions, see Common Errors (p. 302).

AccessDenied

Access denied.

HTTP Status Code: 403

CNAMEAlreadyExists

HTTP Status Code: 409

IllegalUpdate

Origin and CallerReference cannot be updated.

HTTP Status Code: 400

InconsistentQuantities

The value of Quantity and the size of Items don't match.

HTTP Status Code: 400

InvalidArgument

The argument is invalid.

HTTP Status Code: 400

InvalidIfMatchVersion

The If-Match version is missing or not valid for the distribution.

HTTP Status Code: 400

InvalidOriginAccessIdentity

The origin access identity is not valid or doesn't exist.

HTTP Status Code: 400

MissingBody

This operation requires a body. Ensure that the body is present and the Content-Type header is set.

HTTP Status Code: 400

NoSuchStreamingDistribution

The specified streaming distribution does not exist.

HTTP Status Code: 404

PreconditionFailed

The precondition given in one or more of the request-header fields evaluated to false.

HTTP Status Code: 412

TooManyStreamingDistributionCNAMEs

HTTP Status Code: 400
TooManyTrustedSigners

Your request contains more trusted signers than are allowed per distribution.

HTTP Status Code: 400

TrustedSignerDoesNotExist

One or more of your trusted signers don't exist.

HTTP Status Code: 400

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 Amazon CloudFront 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:

- `ActiveTrustedSigners` (p. 192)
- `Aliases` (p. 194)
- `AllowedMethods` (p. 195)
- `CacheBehavior` (p. 197)
- `CacheBehaviors` (p. 201)
- `CachedMethods` (p. 202)
- `CloudFrontOriginAccessIdentity` (p. 203)
- `CloudFrontOriginAccessIdentityConfig` (p. 204)
- `CloudFrontOriginAccessIdentityList` (p. 205)
- `CloudFrontOriginAccessIdentitySummary` (p. 207)
- `ContentTypeProfile` (p. 208)
- `ContentTypeProfileConfig` (p. 209)
- `ContentTypeProfiles` (p. 210)
- `CookieNames` (p. 211)
- `CookiePreference` (p. 212)
- `CustomErrorResponse` (p. 213)
- `CustomErrorResponses` (p. 215)
- `CustomHeaders` (p. 216)
- `CustomOriginConfig` (p. 217)
- `DefaultCacheBehavior` (p. 219)
- `Distribution` (p. 222)
- `DistributionConfig` (p. 224)
- `DistributionConfigWithTags` (p. 230)
- `DistributionList` (p. 231)
- `DistributionSummary` (p. 233)
- `EncryptionEntities` (p. 237)
- `EncryptionEntity` (p. 238)
- `FieldLevelEncryption` (p. 239)
- `FieldLevelEncryptionConfig` (p. 240)
- `FieldLevelEncryptionList` (p. 241)
- `FieldLevelEncryptionProfile` (p. 242)
- `FieldLevelEncryptionProfileConfig` (p. 243)
- `FieldLevelEncryptionProfileList` (p. 244)
- `FieldLevelEncryptionProfileSummary` (p. 245)
- `FieldLevelEncryptionSummary` (p. 246)
• FieldPatterns (p. 247)
• ForwardedValues (p. 248)
• GeoRestriction (p. 250)
• Headers (p. 252)
• Invalidation (p. 254)
• InvalidationBatch (p. 255)
• InvalidationList (p. 256)
• InvalidationSummary (p. 258)
• KeyPairIds (p. 259)
• LambdaFunctionAssociation (p. 260)
• LambdaFunctionAssociations (p. 261)
• LoggingConfig (p. 262)
• Origin (p. 264)
• OriginCustomHeader (p. 266)
• Origins (p. 267)
• OriginSslProtocols (p. 268)
• Paths (p. 269)
• PublicKey (p. 270)
• PublicKeyConfig (p. 271)
• PublicKeyList (p. 272)
• PublicKeySummary (p. 273)
• QueryArgProfile (p. 274)
• QueryArgProfileConfig (p. 275)
• QueryArgProfiles (p. 276)
• QueryStringCacheKeys (p. 277)
• Restrictions (p. 278)
• S3Origin (p. 279)
• S3OriginConfig (p. 280)
• Signer (p. 281)
• StreamingDistribution (p. 282)
• StreamingDistributionConfig (p. 284)
• StreamingDistributionConfigWithTags (p. 286)
• StreamingDistributionList (p. 287)
• StreamingDistributionSummary (p. 289)
• StreamingLoggingConfig (p. 291)
• Tag (p. 292)
• TagKeys (p. 293)
• Tags (p. 294)
• TrustedSigners (p. 295)
• ViewerCertificate (p. 296)
ActiveTrustedSigners

A complex type that lists the AWS accounts, if any, that you included in the TrustedSigners complex type for this distribution. These are the accounts that you want to allow to create signed URLs for private content.

The Signer complex type lists the AWS account number of the trusted signer or self if the signer is the AWS account that created the distribution. The Signer element also includes the IDs of any active CloudFront key pairs that are associated with the trusted signer's AWS account. If no KeyPairId element appears for a Signer, that signer can't create signed URLs.

For more information, see Serving Private Content through CloudFront in the Amazon CloudFront Developer Guide.

Contents

Enabled

Enabled is true if any of the AWS accounts listed in the TrustedSigners complex type for this RTMP distribution have active CloudFront key pairs. If not, Enabled is false.

For more information, see ActiveTrustedSigners (p. 192).

Type: Boolean

Required: Yes

Items

A complex type that contains one Signer complex type for each trusted signer that is specified in the TrustedSigners complex type.

For more information, see ActiveTrustedSigners (p. 192).

Type: Array of Signer (p. 281) objects

Required: No

Quantity

A complex type that contains one Signer complex type for each trusted signer specified in the TrustedSigners complex type.

For more information, see ActiveTrustedSigners (p. 192).

Type: Integer

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
**Aliases**

A complex type that contains information about CNAMEs (alternate domain names), if any, for this distribution.

**Contents**

**Items**

A complex type that contains the CNAME aliases, if any, that you want to associate with this distribution.

Type: Array of strings

Required: No

**Quantity**

The number of CNAME aliases, if any, that you want to associate with this distribution.

Type: Integer

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
AllowedMethods

A complex type that controls which HTTP methods CloudFront processes and forwards to your Amazon S3 bucket or your custom origin. There are three choices:

- CloudFront forwards only GET and HEAD requests.
- CloudFront forwards only GET, HEAD, and OPTIONS requests.
- CloudFront forwards GET, HEAD, OPTIONS, PUT, PATCH, POST, and DELETE requests.

If you pick the third choice, you may need to restrict access to your Amazon S3 bucket or to your custom origin so users can't perform operations that you don't want them to. For example, you might not want users to have permissions to delete objects from your origin.

Contents

CachedMethods

A complex type that controls whether CloudFront caches the response to requests using the specified HTTP methods. There are two choices:

- CloudFront caches responses to GET and HEAD requests.
- CloudFront caches responses to GET, HEAD, and OPTIONS requests.

If you pick the second choice for your Amazon S3 Origin, you may need to forward Access-Control-Request-Method, Access-Control-Request-Headers, and Origin headers for the responses to be cached correctly.

Type: CachedMethods (p. 202) object

Required: No

Items

A complex type that contains the HTTP methods that you want CloudFront to process and forward to your origin.

Type: Array of strings

Valid Values: GET | HEAD | POST | PUT | PATCH | OPTIONS | DELETE

Required: Yes

Quantity

The number of HTTP methods that you want CloudFront to forward to your origin. Valid values are 2 (for GET and HEAD requests), 3 (for GET, HEAD, and OPTIONS requests) and 7 (for GET, HEAD, OPTIONS, PUT, PATCH, POST, and DELETE requests).

Type: Integer

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
CacheBehavior

A complex type that describes how CloudFront processes requests.

You must create at least as many cache behaviors (including the default cache behavior) as you have origins if you want CloudFront to distribute objects from all of the origins. Each cache behavior specifies the one origin from which you want CloudFront to get objects. If you have two origins and only the default cache behavior, the default cache behavior will cause CloudFront to get objects from one of the origins, but the other origin is never used.

For the current limit on the number of cache behaviors that you can add to a distribution, see Amazon CloudFront Limits in the AWS General Reference.

If you don't want to specify any cache behaviors, include only an empty CacheBehaviors element. Don't include an empty CacheBehavior element, or CloudFront returns a MalformedXML error.

To delete all cache behaviors in an existing distribution, update the distribution configuration and include only an empty CacheBehaviors element.

To add, change, or remove one or more cache behaviors, update the distribution configuration and specify all of the cache behaviors that you want to include in the updated distribution.

For more information about cache behaviors, see Cache Behaviors in the Amazon CloudFront Developer Guide.

Contents

AllowedMethods

A complex type that controls which HTTP methods CloudFront processes and forwards to your Amazon S3 bucket or your custom origin. There are three choices:

- CloudFront forwards only GET and HEAD requests.
- CloudFront forwards only GET, HEAD, and OPTIONS requests.
- CloudFront forwards GET, HEAD, OPTIONS, PUT, PATCH, POST, and DELETE requests.

If you pick the third choice, you may need to restrict access to your Amazon S3 bucket or to your custom origin so users can't perform operations that you don't want them to. For example, you might not want users to have permissions to delete objects from your origin.

Type: AllowedMethods (p. 195) object

Required: No

Compress

Whether you want CloudFront to automatically compress certain files for this cache behavior. If so, specify true; if not, specify false. For more information, see Serving Compressed Files in the Amazon CloudFront Developer Guide.

Type: Boolean

Required: No

DefaultTTL

The default amount of time that you want objects to stay in CloudFront caches before CloudFront forwards another request to your origin to determine whether the object has been updated. The value that you specify applies only when your origin does not add HTTP headers such as Cache-Control max-age, Cache-Control s-maxage, and Expires to objects. For more information,
FieldLevelEncryptionId

A complex type that specifies how CloudFront handles query strings and cookies.

Type: FieldLevelEncryptionId

Required: No

ForwardedValues

A complex type that specifies how CloudFront handles query strings and cookies.

Type: ForwardedValues

Required: Yes

LambdaFunctionAssociations

A complex type that contains zero or more Lambda function associations for a cache behavior.

Type: LambdaFunctionAssociations

Required: No

MaxTTL

The maximum amount of time that you want objects to stay in CloudFront caches before CloudFront forwards another request to your origin to determine whether the object has been updated. The value that you specify applies only when your origin adds HTTP headers such as Cache-Control max-age, Cache-Control s-maxage, and Expires to objects. For more information, see Specifying How Long Objects and Errors Stay in a CloudFront Edge Cache (Expiration) in the Amazon CloudFront Developer Guide.

Type: Long

Required: No

MinTTL

The minimum amount of time that you want objects to stay in CloudFront caches before CloudFront forwards another request to your origin to determine whether the object has been updated. For more information, see Specifying How Long Objects and Errors Stay in a CloudFront Edge Cache (Expiration) in the Amazon CloudFront Developer Guide.

You must specify 0 for MinTTL if you configure CloudFront to forward all headers to your origin (under Headers, if you specify 1 for Quantity and * for Name).

Type: Long

Required: Yes

PathPattern

The pattern (for example, images/*.jpg) that specifies which requests to apply the behavior to. When CloudFront receives a viewer request, the requested path is compared with path patterns in the order in which cache behaviors are listed in the distribution.

Note
You can optionally include a slash (/) at the beginning of the path pattern. For example, / images/*.jpg. CloudFront behavior is the same with or without the leading /.
The path pattern for the default cache behavior is * and cannot be changed. If the request for an object does not match the path pattern for any cache behaviors, CloudFront applies the behavior in the default cache behavior.

For more information, see Path Pattern in the Amazon CloudFront Developer Guide.

Type: String
Required: Yes

SmoothStreaming

Indicates whether you want to distribute media files in the Microsoft Smooth Streaming format using the origin that is associated with this cache behavior. If so, specify true; if not, specify false. If you specify true for SmoothStreaming, you can still distribute other content using this cache behavior if the content matches the value of PathPattern.

Type: Boolean
Required: No

TargetOriginId

The value of ID for the origin that you want CloudFront to route requests to when a request matches the path pattern either for a cache behavior or for the default cache behavior.

Type: String
Required: Yes

TrustedSigners

A complex type that specifies the AWS accounts, if any, that you want to allow to create signed URLs for private content.

If you want to require signed URLs in requests for objects in the target origin that match the PathPattern for this cache behavior, specify true for Enabled, and specify the applicable values for Quantity and Items. For more information, see Serving Private Content through CloudFront in the Amazon Amazon CloudFront Developer Guide.

If you don't want to require signed URLs in requests for objects that match PathPattern, specify false for Enabled and 0 for Quantity. Omit Items.

To add, change, or remove one or more trusted signers, change Enabled to true (if it's currently false), change Quantity as applicable, and specify all of the trusted signers that you want to include in the updated distribution.

Type: TrustedSigners (p. 295) object
Required: Yes

ViewerProtocolPolicy

The protocol that viewers can use to access the files in the origin specified by TargetOriginId when a request matches the path pattern in PathPattern. You can specify the following options:

- allow-all: Viewers can use HTTP or HTTPS.
- redirect-to-https: If a viewer submits an HTTP request, CloudFront returns an HTTP status code of 301 (Moved Permanently) to the viewer along with the HTTPS URL. The viewer then resubmits the request using the new URL.
- https-only: If a viewer sends an HTTP request, CloudFront returns an HTTP status code of 403 (Forbidden).
For more information about requiring the HTTPS protocol, see Using an HTTPS Connection to Access Your Objects in the Amazon CloudFront Developer Guide.

**Note**
The only way to guarantee that viewers retrieve an object that was fetched from the origin using HTTPS is never to use any other protocol to fetch the object. If you have recently changed from HTTP to HTTPS, we recommend that you clear your objects' cache because cached objects are protocol agnostic. That means that an edge location will return an object from the cache regardless of whether the current request protocol matches the protocol used previously. For more information, see Specifying How Long Objects and Errors Stay in a CloudFront Edge Cache (Expiration) in the Amazon CloudFront Developer Guide.

Type: String

Valid Values: allow-all | https-only | redirect-to-https

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
CacheBehaviors

A complex type that contains zero or more CacheBehavior elements.

Contents

Items

Optional: A complex type that contains cache behaviors for this distribution. If quantity is 0, you can omit Items.

Type: Array of CacheBehavior (p. 197) objects

Required: No

Quantity

The number of cache behaviors for this distribution.

Type: Integer

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
CachedMethods

A complex type that controls whether CloudFront caches the response to requests using the specified HTTP methods. There are two choices:

- CloudFront caches responses to GET and HEAD requests.
- CloudFront caches responses to GET, HEAD, and OPTIONS requests.

If you pick the second choice for your Amazon S3 Origin, you may need to forward Access-Control-Request-Method, Access-Control-Request-Headers, and Origin headers for the responses to be cached correctly.

Contents

Items

A complex type that contains the HTTP methods that you want CloudFront to cache responses to.

Type: Array of strings

Valid Values: GET | HEAD | POST | PUT | PATCH | OPTIONS | DELETE

Required: Yes

Quantity

The number of HTTP methods for which you want CloudFront to cache responses. Valid values are 2 (for caching responses to GET and HEAD requests) and 3 (for caching responses to GET, HEAD, and OPTIONS requests).

Type: Integer

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
CloudFrontOriginAccessIdentity

CloudFront origin access identity.

Contents

CloudFrontOriginAccessIdentityConfig

The current configuration information for the identity.

Type: CloudFrontOriginAccessIdentityConfig (p. 204) object

Required: No

Id

The ID for the origin access identity, for example, E74FTE3AJFJ256A.

Type: String

Required: Yes

S3CanonicalUserId

The Amazon S3 canonical user ID for the origin access identity, used when giving the origin access identity read permission to an object in Amazon S3.

Type: String

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
CloudFrontOriginAccessIdentityConfig

Origin access identity configuration. Send a GET request to the /CloudFront API version/CloudFront/identity ID/config resource.

Contents

CallerReference

A unique number that ensures the request can't be replayed.

If the CallerReference is new (no matter the content of the CloudFrontOriginAccessIdentityConfig object), a new origin access identity is created.

If the CallerReference is a value already sent in a previous identity request, and the content of the CloudFrontOriginAccessIdentityConfig is identical to the original request (ignoring white space), the response includes the same information returned to the original request.

If the CallerReference is a value you already sent in a previous request to create an identity, but the content of the CloudFrontOriginAccessIdentityConfig is different from the original request, CloudFront returns a CloudFrontOriginAccessIdentityAlreadyExists error.

Type: String
Required: Yes

Comment

Any comments you want to include about the origin access identity.

Type: String
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
CloudFrontOriginAccessIdentityList

Lists the origin access identities for CloudFront. Send a GET request to the `/CloudFront API version/origin-access-identity/cloudfront` resource. The response includes a `CloudFrontOriginAccessIdentityList` element with zero or more `CloudFrontOriginAccessIdentitySummary` child elements. By default, your entire list of origin access identities is returned in one single page. If the list is long, you can paginate it using the `MaxItems` and `Marker` parameters.

## Contents

**IsTruncated**

A flag that indicates whether more origin access identities remain to be listed. If your results were truncated, you can make a follow-up pagination request using the `Marker` request parameter to retrieve more items in the list.

Type: Boolean

Required: Yes

**Items**

A complex type that contains one `CloudFrontOriginAccessIdentitySummary` element for each origin access identity that was created by the current AWS account.

Type: Array of `CloudFrontOriginAccessIdentitySummary` (p. 207) objects

Required: No

**Marker**

Use this when paginating results to indicate where to begin in your list of origin access identities. The results include identities in the list that occur after the marker. To get the next page of results, set the `Marker` to the value of the `NextMarker` from the current page's response (which is also the ID of the last identity on that page).

Type: String

Required: Yes

**MaxItems**

The maximum number of origin access identities you want in the response body.

Type: Integer

Required: Yes

**NextMarker**

If `IsTruncated` is true, this element is present and contains the value you can use for the `Marker` request parameter to continue listing your origin access identities where they left off.

Type: String

Required: No

**Quantity**

The number of CloudFront origin access identities that were created by the current AWS account.

Type: Integer
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
CloudFrontOriginAccessIdentitySummary

Summary of the information about a CloudFront origin access identity.

Contents

Comment

The comment for this origin access identity, as originally specified when created.

Type: String
Required: Yes

Id

The ID for the origin access identity. For example: E74FTE3AJFJ256A.

Type: String
Required: Yes

S3CanonicalUserId

The Amazon S3 canonical user ID for the origin access identity, which you use when giving the origin access identity read permission to an object in Amazon S3.

Type: String
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
ContentTypeProfile

A field-level encryption content type profile.

Contents

ContentType

The content type for a field-level encryption content type-profile mapping.

Type: String
Required: Yes

Format

The format for a field-level encryption content type-profile mapping.

Type: String
Valid Values: URLencoded
Required: Yes

ProfileId

The profile ID for a field-level encryption content type-profile mapping.

Type: String
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
ContentTypeProfileConfig

The configuration for a field-level encryption content type-profile mapping.

Contents

ContentTypeProfiles

The configuration for a field-level encryption content type-profile.

Type: ContentTypeProfiles (p. 210) object

Required: No

ForwardWhenContentTypeIsUnknown

The setting in a field-level encryption content type-profile mapping that specifies what to do when an unknown content type is provided for the profile. If true, content is forwarded without being encrypted when the content type is unknown. If false (the default), an error is returned when the content type is unknown.

Type: Boolean

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
ContentTypeProfiles

Field-level encryption content type-profile.

Contents

Items

Items in a field-level encryption content type-profile mapping.

Type: Array of ContentTypeProfile (p. 208) objects

Required: No

Quantity

The number of field-level encryption content type-profile mappings.

Type: Integer

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
CookieNames

A complex type that specifies whether you want CloudFront to forward cookies to the origin and, if so, which ones. For more information about forwarding cookies to the origin, see How CloudFront Forwards, Caches, and Logs Cookies in the Amazon CloudFront Developer Guide.

Contents

Items

A complex type that contains one Name element for each cookie that you want CloudFront to forward to the origin for this cache behavior.

Type: Array of strings

Required: No

Quantity

The number of different cookies that you want CloudFront to forward to the origin for this cache behavior.

Type: Integer

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
CookiePreference

A complex type that specifies whether you want CloudFront to forward cookies to the origin and, if so, which ones. For more information about forwarding cookies to the origin, see How CloudFront Forwards, Caches, and Logs Cookies in the Amazon CloudFront Developer Guide.

Contents

Forward

Specifies which cookies to forward to the origin for this cache behavior: all, none, or the list of cookies specified in the WhitelistedNames complex type.

Amazon S3 doesn't process cookies. When the cache behavior is forwarding requests to an Amazon S3 origin, specify none for the Forward element.

Type: String

Valid Values: none | whitelist | all

Required: Yes

WhitelistedNames

Required if you specify whitelist for the value of Forward: A complex type that specifies how many different cookies you want CloudFront to forward to the origin for this cache behavior and, if you want to forward selected cookies, the names of those cookies.

If you specify all or none for the value of Forward, omit WhitelistedNames. If you change the value of Forward from whitelist to all or none and you don't delete the WhitelistedNames element and its child elements, CloudFront deletes them automatically.

For the current limit on the number of cookie names that you can whitelist for each cache behavior, see Amazon CloudFront Limits in the AWS General Reference.

Type: CookieNames (p. 211) object

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
CustomErrorResponse

A complex type that controls:

- Whether CloudFront replaces HTTP status codes in the 4xx and 5xx range with custom error messages before returning the response to the viewer.
- How long CloudFront caches HTTP status codes in the 4xx and 5xx range.

For more information about custom error pages, see Customizing Error Responses in the Amazon CloudFront Developer Guide.

Contents

ErrorCachingMinTTL

The minimum amount of time, in seconds, that you want CloudFront to cache the HTTP status code specified in ErrorCode. When this time period has elapsed, CloudFront queries your origin to see whether the problem that caused the error has been resolved and the requested object is now available.

If you don't want to specify a value, include an empty element, <ErrorCachingMinTTL>, in the XML document.

For more information, see Customizing Error Responses in the Amazon CloudFront Developer Guide.

Type: Long
Required: No

ErrorCode

The HTTP status code for which you want to specify a custom error page and/or a caching duration.

Type: Integer
Required: Yes

ResponseCode

The HTTP status code that you want CloudFront to return to the viewer along with the custom error page. There are a variety of reasons that you might want CloudFront to return a status code different from the status code that your origin returned to CloudFront, for example:

- Some Internet devices (some firewalls and corporate proxies, for example) intercept HTTP 4xx and 5xx and prevent the response from being returned to the viewer. If you substitute 200, the response typically won't be intercepted.
- If you don't care about distinguishing among different client errors or server errors, you can specify 400 or 500 as the ResponseCode for all 4xx or 5xx errors.
- You might want to return a 200 status code (OK) and static website so your customers don't know that your website is down.

If you specify a value for ResponseCode, you must also specify a value for ResponsePagePath.
If you don't want to specify a value, include an empty element, <ResponseCode>, in the XML document.

Type: String
Required: No
ResponsePagePath

The path to the custom error page that you want CloudFront to return to a viewer when your origin returns the HTTP status code specified by ErrorCode, for example, /4xx-errors/403-forbidden.html. If you want to store your objects and your custom error pages in different locations, your distribution must include a cache behavior for which the following is true:

- The value of PathPattern matches the path to your custom error messages. For example, suppose you saved custom error pages for 4xx errors in an Amazon S3 bucket in a directory named /4xx-errors. Your distribution must include a cache behavior for which the path pattern routes requests for your custom error pages to that location, for example, /4xx-errors/*.
- The value of TargetOriginId specifies the value of the ID element for the origin that contains your custom error pages.

If you specify a value for ResponsePagePath, you must also specify a value for ResponseCode. If you don't want to specify a value, include an empty element, <ResponsePagePath>, in the XML document.

We recommend that you store custom error pages in an Amazon S3 bucket. If you store custom error pages on an HTTP server and the server starts to return 5xx errors, CloudFront can't get the files that you want to return to viewers because the origin server is unavailable.

Type: String

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
CustomErrorResponses

A complex type that controls:

- Whether CloudFront replaces HTTP status codes in the 4xx and 5xx range with custom error messages before returning the response to the viewer.
- How long CloudFront caches HTTP status codes in the 4xx and 5xx range.

For more information about custom error pages, see Customizing Error Responses in the Amazon CloudFront Developer Guide.

Contents

Items

A complex type that contains a CustomErrorResponse element for each HTTP status code for which you want to specify a custom error page and/or a caching duration.

Type: Array of CustomErrorResponse objects

Required: No

Quantity

The number of HTTP status codes for which you want to specify a custom error page and/or a caching duration. If Quantity is 0, you can omit Items.

Type: Integer

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
CustomHeaders

A complex type that contains the list of Custom Headers for each origin.

Contents

Items

Optional: A list that contains one OriginCustomHeader element for each custom header that you want CloudFront to forward to the origin. If Quantity is 0, omit Items.

Type: Array of OriginCustomHeader (p. 266) objects

Required: No

Quantity

The number of custom headers, if any, for this distribution.

Type: Integer

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
CustomOriginConfig

A customer origin.

Contents

HTTPPort

The HTTP port the custom origin listens on.

Type: Integer

Required: Yes

HTTPSPort

The HTTPS port the custom origin listens on.

Type: Integer

Required: Yes

OriginKeepaliveTimeout

You can create a custom keep-alive timeout. All timeout units are in seconds. The default keep-alive timeout is 5 seconds, but you can configure custom timeout lengths using the CloudFront API. The minimum timeout length is 1 second; the maximum is 60 seconds.

If you need to increase the maximum time limit, contact the AWS Support Center.

Type: Integer

Required: No

OriginProtocolPolicy

The origin protocol policy to apply to your origin.

Type: String

Valid Values: http-only | match-viewer | https-only

Required: Yes

OriginReadTimeout

You can create a custom origin read timeout. All timeout units are in seconds. The default origin read timeout is 30 seconds, but you can configure custom timeout lengths using the CloudFront API. The minimum timeout length is 4 seconds; the maximum is 60 seconds.

If you need to increase the maximum time limit, contact the AWS Support Center.

Type: Integer

Required: No

OriginSslProtocols

The SSL/TLS protocols that you want CloudFront to use when communicating with your origin over HTTPS.

Type: OriginSslProtocols (p. 268) object
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
DefaultCacheBehavior

A complex type that describes the default cache behavior if you don't specify a CacheBehavior element or if files don't match any of the values of PathPattern in CacheBehavior elements. You must create exactly one default cache behavior.

Contents

AllowedMethods

A complex type that controls which HTTP methods CloudFront processes and forwards to your Amazon S3 bucket or your custom origin. There are three choices:

- CloudFront forwards only GET and HEAD requests.
- CloudFront forwards only GET, HEAD, and OPTIONS requests.
- CloudFront forwards GET, HEAD, OPTIONS, PUT, PATCH, POST, and DELETE requests.

If you pick the third choice, you may need to restrict access to your Amazon S3 bucket or to your custom origin so users can't perform operations that you don't want them to. For example, you might not want users to have permissions to delete objects from your origin.

Type: AllowedMethods (p. 195) object

Required: No

Compress

Whether you want CloudFront to automatically compress certain files for this cache behavior. If so, specify true; if not, specify false. For more information, see Serving Compressed Files in the Amazon CloudFront Developer Guide.

Type: Boolean

Required: No

DefaultTTL

The default amount of time that you want objects to stay in CloudFront caches before CloudFront forwards another request to your origin to determine whether the object has been updated. The value that you specify applies only when your origin does not add HTTP headers such as Cache-Control max-age, Cache-Control s-maxage, and Expires to objects. For more information, see Specifying How Long Objects and Errors Stay in a CloudFront Edge Cache (Expiration) in the Amazon CloudFront Developer Guide.

Type: Long

Required: No

FieldLevelEncryptionId

Type: String

Required: No

ForwardedValues

A complex type that specifies how CloudFront handles query strings and cookies.

Type: ForwardedValues (p. 248) object

Required: Yes
LambdaFunctionAssociations

A complex type that contains zero or more Lambda function associations for a cache behavior.

Type: LambdaFunctionAssociations (p. 261) object

Required: No

MaxTTL

Type: Long

Required: No

MinTTL

The minimum amount of time that you want objects to stay in CloudFront caches before CloudFront forwards another request to your origin to determine whether the object has been updated. For more information, see Specifying How Long Objects and Errors Stay in a CloudFront Edge Cache (Expiration) in the Amazon Amazon CloudFront Developer Guide.

You must specify 0 for MinTTL if you configure CloudFront to forward all headers to your origin (under Headers, if you specify 1 for Quantity and * for Name).

Type: Long

Required: Yes

SmoothStreaming

Indicates whether you want to distribute media files in the Microsoft Smooth Streaming format using the origin that is associated with this cache behavior. If so, specify true; if not, specify false. If you specify true for SmoothStreaming, you can still distribute other content using this cache behavior if the content matches the value of PathPattern.

Type: Boolean

Required: No

TargetOriginId

The value of ID for the origin that you want CloudFront to route requests to when a request matches the path pattern either for a cache behavior or for the default cache behavior.

Type: String

Required: Yes

TrustedSigners

A complex type that specifies the AWS accounts, if any, that you want to allow to create signed URLs for private content.

If you want to require signed URLs in requests for objects in the target origin that match the PathPattern for this cache behavior, specify true for Enabled, and specify the applicable values for Quantity and Items. For more information, see Serving Private Content through CloudFront in the Amazon Amazon CloudFront Developer Guide.

If you don't want to require signed URLs in requests for objects that match PathPattern, specify false for Enabled and 0 for Quantity. Omit Items.

To add, change, or remove one or more trusted signers, change Enabled to true (if it's currently false), change Quantity as applicable, and specify all of the trusted signers that you want to include in the updated distribution.
Type: TrustedSigners (p. 295) object

Required: Yes

ViewerProtocolPolicy

The protocol that viewers can use to access the files in the origin specified by TargetOriginId when a request matches the path pattern in PathPattern. You can specify the following options:

- **allow-all**: Viewers can use HTTP or HTTPS.
- **redirect-to-https**: If a viewer submits an HTTP request, CloudFront returns an HTTP status code of 301 (Moved Permanently) to the viewer along with the HTTPS URL. The viewer then resubmits the request using the new URL.
- **https-only**: If a viewer sends an HTTP request, CloudFront returns an HTTP status code of 403 (Forbidden).

For more information about requiring the HTTPS protocol, see Using an HTTPS Connection to Access Your Objects in the Amazon CloudFront Developer Guide.

**Note**

The only way to guarantee that viewers retrieve an object that was fetched from the origin using HTTPS is never to use any other protocol to fetch the object. If you have recently changed from HTTP to HTTPS, we recommend that you clear your objects' cache because cached objects are protocol agnostic. That means that an edge location will return an object from the cache regardless of whether the current request protocol matches the protocol used previously. For more information, see Specifying How Long Objects and Errors Stay in a CloudFront Edge Cache (Expiration) in the Amazon CloudFront Developer Guide.

Type: String

Valid Values: allow-all | https-only | redirect-to-https

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
Distribution

The distribution's information.

Contents

ActiveTrustedSigners

CloudFront automatically adds this element to the response only if you've set up the distribution to serve private content with signed URLs. The element lists the key pair IDs that CloudFront is aware of for each trusted signer. The `Signer` child element lists the AWS account number of the trusted signer (or an empty `Self` element if the signer is you). The `Signer` element also includes the IDs of any active key pairs associated with the trusted signer's AWS account. If no `KeyPairId` element appears for a `Signer`, that signer can't create working signed URLs.

Type: ActiveTrustedSigners (p. 192) object

Required: Yes

ARN

The ARN (Amazon Resource Name) for the distribution. For example: arn:aws:cloudfront::123456789012:distribution/EDFDVBD632BHDS5, where 123456789012 is your AWS account ID.

Type: String

Required: Yes

DistributionConfig

The current configuration information for the distribution. Send a GET request to the `/CloudFront API version/distribution ID/config` resource.

Type: DistributionConfig (p. 224) object

Required: Yes

DomainName

The domain name corresponding to the distribution, for example, d111111abcdef8.cloudfront.net.

Type: String

Required: Yes

Id

The identifier for the distribution. For example: EDFDVBD632BHDS5.

Type: String

Required: Yes

InProgressInvalidationBatches

The number of invalidation batches currently in progress.

Type: Integer

Required: Yes
LastModifiedTime
The date and time the distribution was last modified.
Type: Timestamp
Required: Yes

Status
This response element indicates the current status of the distribution. When the status is Deployed, the distribution's information is fully propagated to all CloudFront edge locations.
Type: String
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
DistributionConfig

A distribution configuration.

Contents

Aliases

A complex type that contains information about CNAMEs (alternate domain names), if any, for this distribution.

Type: Aliases (p. 194) object

Required: No

CacheBehaviors

A complex type that contains zero or more CacheBehavior elements.

Type: CacheBehaviors (p. 201) object

Required: No

CallerReference

A unique value (for example, a date-time stamp) that ensures that the request can't be replayed.

If the value of CallerReference is new (regardless of the content of the DistributionConfig object), CloudFront creates a new distribution.

If CallerReference is a value you already sent in a previous request to create a distribution, and if the content of the DistributionConfig is identical to the original request (ignoring white space), CloudFront returns the same the response that it returned to the original request.

If CallerReference is a value you already sent in a previous request to create a distribution but the content of the DistributionConfig is different from the original request, CloudFront returns a DistributionAlreadyExists error.

Type: String

Required: Yes

Comment

Any comments you want to include about the distribution.

If you don't want to specify a comment, include an empty Comment element.

To delete an existing comment, update the distribution configuration and include an empty Comment element.

To add or change a comment, update the distribution configuration and specify the new comment.

Type: String

Required: Yes

CustomErrorResponses

A complex type that controls the following:

• Whether CloudFront replaces HTTP status codes in the 4xx and 5xx range with custom error messages before returning the response to the viewer.

• How long CloudFront caches HTTP status codes in the 4xx and 5xx range.
For more information about custom error pages, see Customizing Error Responses in the Amazon CloudFront Developer Guide.

Type: CustomErrorResponses (p. 215) object

Required: No

**DefaultCacheBehavior**

A complex type that describes the default cache behavior if you don't specify a CacheBehavior element or if files don't match any of the values of PathPattern in CacheBehavior elements. You must create exactly one default cache behavior.

Type: DefaultCacheBehavior (p. 219) object

Required: Yes

**DefaultRootObject**

The object that you want CloudFront to request from your origin (for example, index.html) when a viewer requests the root URL for your distribution (http://www.example.com) instead of an object in your distribution (http://www.example.com/product-description.html). Specifying a default root object avoids exposing the contents of your distribution.

Specify only the object name, for example, index.html. Don't add a / before the object name.

If you don't want to specify a default root object when you create a distribution, include an empty DefaultRootObject element.

To delete the default root object from an existing distribution, update the distribution configuration and include an empty DefaultRootObject element.

To replace the default root object, update the distribution configuration and specify the new object.

For more information about the default root object, see Creating a Default Root Object in the Amazon CloudFront Developer Guide.

Type: String

Required: No

**Enabled**

From this field, you can enable or disable the selected distribution.

If you specify false for Enabled but you specify values for Bucket and Prefix, the values are automatically deleted.

Type: Boolean

Required: Yes

**HttpVersion**

(Optional) Specify the maximum HTTP version that you want viewers to use to communicate with CloudFront. The default value for new web distributions is http2. Viewers that don't support HTTP/2 automatically use an earlier HTTP version.

For viewers and CloudFront to use HTTP/2, viewers must support TLS 1.2 or later, and must support Server Name Identification (SNI).

In general, configuring CloudFront to communicate with viewers using HTTP/2 reduces latency. You can improve performance by optimizing for HTTP/2. For more information, do an Internet search for "http/2 optimization."
Type: String

Valid Values: http1.1 | http2

Required: No

IsIPV6Enabled

If you want CloudFront to respond to IPv6 DNS requests with an IPv6 address for your distribution, specify true. If you specify false, CloudFront responds to IPv6 DNS requests with the DNS response code NOERROR and with no IP addresses. This allows viewers to submit a second request, for an IPv4 address for your distribution.

In general, you should enable IPv6 if you have users on IPv6 networks who want to access your content. However, if you're using signed URLs or signed cookies to restrict access to your content, and if you're using a custom policy that includes the IpAddress parameter to restrict the IP addresses that can access your content, don't enable IPv6. If you want to restrict access to some content by IP address and not restrict access to other content (or restrict access but not by IP address), you can create two distributions. For more information, see Creating a Signed URL Using a Custom Policy in the Amazon CloudFront Developer Guide.

If you're using an Amazon Route 53 alias resource record set to route traffic to your CloudFront distribution, you need to create a second alias resource record set when both of the following are true:

- You enable IPv6 for the distribution
- You're using alternate domain names in the URLs for your objects

For more information, see Routing Traffic to an Amazon CloudFront Web Distribution by Using Your Domain Name in the Amazon Route 53 Developer Guide.

If you created a CNAME resource record set, either with Amazon Route 53 or with another DNS service, you don't need to make any changes. A CNAME record will route traffic to your distribution regardless of the IP address format of the viewer request.

Type: Boolean

Required: No

Logging

A complex type that controls whether access logs are written for the distribution.

For more information about logging, see Access Logs in the Amazon CloudFront Developer Guide.

Type: LoggingConfig (p. 262) object

Required: No

Origins

A complex type that contains information about origins for this distribution.

Type: Origins (p. 267) object

Required: Yes

PriceClass

The price class that corresponds with the maximum price that you want to pay for CloudFront service. If you specify PriceClass_All, CloudFront responds to requests for your objects from all CloudFront edge locations.

If you specify a price class other than PriceClass_All, CloudFront serves your objects from the CloudFront edge location that has the lowest latency among the edge locations in your price class.
Viewers who are in or near regions that are excluded from your specified price class may encounter slower performance.

For more information about price classes, see Choosing the Price Class for a CloudFront Distribution in the Amazon CloudFront Developer Guide. For information about CloudFront pricing, including how price classes map to CloudFront regions, see Amazon CloudFront Pricing.

Type: String

Valid Values: PriceClass_100 | PriceClass_200 | PriceClass_All

Required: No

Restrictions

A complex type that identifies ways in which you want to restrict distribution of your content.

Type: Restrictions (p. 278) object

Required: No

ViewerCertificate

A complex type that specifies the following:

- Whether you want viewers to use HTTP or HTTPS to request your objects.
- If you want viewers to use HTTPS, whether you're using an alternate domain name such as example.com or the CloudFront domain name for your distribution, such as d1111111abcdef8.cloudfront.net.
- If you're using an alternate domain name, whether AWS Certificate Manager (ACM) provided the certificate, or you purchased a certificate from a third-party certificate authority and imported it into ACM or uploaded it to the IAM certificate store.

You must specify only one of the following values:

- ViewerCertificate:ACMCertificateArn (p. 297)
- ViewerCertificate:IAMCertificateId (p. 298)
- ViewerCertificate:CloudFrontDefaultCertificate (p. 297)

Don't specify false for CloudFrontDefaultCertificate.

If you want viewers to use HTTP instead of HTTPS to request your objects: Specify the following value:

<CloudFrontDefaultCertificate>true<CloudFrontDefaultCertificate>

In addition, specify allow-all for ViewerProtocolPolicy for all of your cache behaviors.

If you want viewers to use HTTPS to request your objects: Choose the type of certificate that you want to use based on whether you're using an alternate domain name for your objects or the CloudFront domain name:

- If you're using an alternate domain name, such as example.com: Specify one of the following values, depending on whether ACM provided your certificate or you purchased your certificate from third-party certificate authority:
  - <ACMCertificateArn>ARN for ACM SSL/TLS certificate</ACMCertificateArn>
    where ARN for ACM SSL/TLS certificate is the ARN for the ACM SSL/TLS certificate that you want to use for this distribution.
  - <IAMCertificateId>IAM certificate ID</IAMCertificateId> where IAM certificate ID is the ID that IAM returned when you added the certificate to the IAM certificate store.
If you specify ACMCertificateArn or IAMCertificateId, you must also specify a value for SSLSupportMethod.

If you choose to use an ACM certificate or a certificate in the IAM certificate store, we recommend that you use only an alternate domain name in your object URLs (https://example.com/logo.jpg). If you use the domain name that is associated with your CloudFront distribution (such as https://d111111abcdef8.cloudfront.net/logo.jpg) and the viewer supports SNI, then CloudFront behaves normally. However, if the browser does not support SNI, the user's experience depends on the value that you choose for SSLSupportMethod:

- **vip**: The viewer displays a warning because there is a mismatch between the CloudFront domain name and the domain name in your SSL/TLS certificate.
- **sni-only**: CloudFront drops the connection with the browser without returning the object.

**If you're using the CloudFront domain name for your distribution, such as d111111abcdef8.cloudfront.net**: Specify the following value:

```xml
<CloudFrontDefaultCertificate>true</CloudFrontDefaultCertificate>
```

If you want viewers to use HTTPS, you must also specify one of the following values in your cache behaviors:

- `<ViewerProtocolPolicy>https-only</ViewerProtocolPolicy>`
- `<ViewerProtocolPolicy>redirect-to-https</ViewerProtocolPolicy>`

You can also optionally require that CloudFront use HTTPS to communicate with your origin by specifying one of the following values for the applicable origins:

- `<OriginProtocolPolicy>https-only</OriginProtocolPolicy>`

For more information, see Using Alternate Domain Names and HTTPS in the *Amazon CloudFront Developer Guide*.

Type: ViewerCertificate (p. 296) object

Required: No

### WebACLId

A unique identifier that specifies the AWS WAF web ACL, if any, to associate with this distribution.

AWS WAF is a web application firewall that lets you monitor the HTTP and HTTPS requests that are forwarded to CloudFront, and lets you control access to your content. Based on conditions that you specify, such as the IP addresses that requests originate from or the values of query strings, CloudFront responds to requests either with the requested content or with an HTTP 403 status code (Forbidden). You can also configure CloudFront to return a custom error page when a request is blocked. For more information about AWS WAF, see the *AWS WAF Developer Guide*.

Type: String

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
DistributionConfigWithTags

A distribution Configuration and a list of tags to be associated with the distribution.

Contents

DistributionConfig

A distribution configuration.

Type: DistributionConfig (p. 224) object

Required: Yes

Tags

A complex type that contains zero or more Tag elements.

Type: Tags (p. 294) object

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
DistributionList

A distribution list.

Contents

IsTruncated

A flag that indicates whether more distributions remain to be listed. If your results were truncated, you can make a follow-up pagination request using the Marker request parameter to retrieve more distributions in the list.

Type: Boolean
Required: Yes

Items

A complex type that contains one DistributionSummary element for each distribution that was created by the current AWS account.

Type: Array of DistributionSummary (p. 233) objects
Required: No

Marker

The value you provided for the Marker request parameter.

Type: String
Required: Yes

MaxItems

The value you provided for the MaxItems request parameter.

Type: Integer
Required: Yes

NextMarker

If IsTruncated is true, this element is present and contains the value you can use for the Marker request parameter to continue listing your distributions where they left off.

Type: String
Required: No

Quantity

The number of distributions that were created by the current AWS account.

Type: Integer
Required: Yes

See Also

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

- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java
- AWS SDK for Ruby V2
DistributionSummary

A summary of the information about a CloudFront distribution.

Contents

Aliases

A complex type that contains information about CNAMEs (alternate domain names), if any, for this distribution.

Type: Aliases (p. 194) object

Required: Yes

ARN

The ARN (Amazon Resource Name) for the distribution. For example: arn:aws:cloudfront::123456789012:distribution/EDFDVBD632BHDS5, where 123456789012 is your AWS account ID.

Type: String

Required: Yes

CacheBehaviors

A complex type that contains zero or more CacheBehavior elements.

Type: CacheBehaviors (p. 201) object

Required: Yes

Comment

The comment originally specified when this distribution was created.

Type: String

Required: Yes

CustomErrorResponses

A complex type that contains zero or more CustomErrorResponses elements.

Type: CustomErrorResponses (p. 215) object

Required: Yes

DefaultCacheBehavior

A complex type that describes the default cache behavior if you don't specify a CacheBehavior element or if files don't match any of the values of PathPattern in CacheBehavior elements. You must create exactly one default cache behavior.

Type: DefaultCacheBehavior (p. 219) object

Required: Yes

DomainName

The domain name that corresponds to the distribution, for example, d111111abcdef8.cloudfront.net.
Type: String
Required: Yes

**Enabled**
Whether the distribution is enabled to accept user requests for content.
Type: Boolean
Required: Yes

**HttpVersion**
Specify the maximum HTTP version that you want viewers to use to communicate with CloudFront. The default value for new web distributions is `http2`. Viewers that don't support `HTTP/2` will automatically use an earlier version.
Type: String
Valid Values: `http1.1` | `http2`
Required: Yes

**Id**
The identifier for the distribution. For example: `EDFDVBD632BHDS5`.
Type: String
Required: Yes

**IsIPV6Enabled**
Whether CloudFront responds to IPv6 DNS requests with an IPv6 address for your distribution.
Type: Boolean
Required: Yes

**LastModifiedTime**
The date and time the distribution was last modified.
Type: Timestamp
Required: Yes

**Origins**
A complex type that contains information about origins for this distribution.
Type: Origins (p. 267) object
Required: Yes

**PriceClass**
Type: String
Valid Values: `PriceClass_100` | `PriceClass_200` | `PriceClass_All`
Required: Yes

**Restrictions**
A complex type that identifies ways in which you want to restrict distribution of your content.
Type: **Restrictions (p. 278)** object

Required: Yes

**Status**

The current status of the distribution. When the status is Deployed, the distribution's information is propagated to all CloudFront edge locations.

Type: String

Required: Yes

**ViewerCertificate**

A complex type that specifies the following:

- Whether you want viewers to use HTTP or HTTPS to request your objects.
- If you want viewers to use HTTPS, whether you're using an alternate domain name such as example.com or the CloudFront domain name for your distribution, such as d111111abcdef8.cloudfront.net.
- If you're using an alternate domain name, whether AWS Certificate Manager (ACM) provided the certificate, or you purchased a certificate from a third-party certificate authority and imported it into ACM or uploaded it to the IAM certificate store.

You must specify only one of the following values:

- **ViewerCertificate:ACMCertificateArn (p. 297)**
- **ViewerCertificate:IAMCertificateId (p. 298)**
- **ViewerCertificate:CloudFrontDefaultCertificate (p. 297)**

Don't specify false for **CloudFrontDefaultCertificate**.

**If you want viewers to use HTTP instead of HTTPS to request your objects:** Specify the following value:

```
<CloudFrontDefaultCertificate>true<CloudFrontDefaultCertificate>
```

In addition, specify allow-all for **ViewerProtocolPolicy** for all of your cache behaviors.

**If you want viewers to use HTTPS to request your objects:** Choose the type of certificate that you want to use based on whether you're using an alternate domain name for your objects or the CloudFront domain name:

- **If you're using an alternate domain name, such as example.com:** Specify one of the following values, depending on whether ACM provided your certificate or you purchased your certificate from third-party certificate authority:

  - `<ACMCertificateArn>ARN for ACM SSL/TLS certificate<ACMCertificateArn>` where **ARN for ACM SSL/TLS certificate** is the ARN for the ACM SSL/TLS certificate that you want to use for this distribution.

  - `<IAMCertificateId>IAM certificate ID<IAMCertificateId>` where **IAM certificate ID** is the ID that IAM returned when you added the certificate to the IAM certificate store.

  If you specify **ACMCertificateArn** or **IAMCertificateId**, you must also specify a value for **SSLSupportMethod**.

  If you choose to use an ACM certificate or a certificate in the IAM certificate store, we recommend that you use only an alternate domain name in your object URLs (https://example.com/logo.jpg). If you use the domain name that is associated with your CloudFront distribution (such as https://d111111abcdef8.cloudfront.net/logo.jpg) and the viewer supports
SNI, then CloudFront behaves normally. However, if the browser does not support SNI, the user's experience depends on the value that you choose for `SSLSupportMethod`:

- **vip**: The viewer displays a warning because there is a mismatch between the CloudFront domain name and the domain name in your SSL/TLS certificate.
- **sni-only**: CloudFront drops the connection with the browser without returning the object.

**If you're using the CloudFront domain name for your distribution, such as d11111abcdef8.cloudfront.net**: Specify the following value:

```
<CloudFrontDefaultCertificate>true</CloudFrontDefaultCertificate>
```

If you want viewers to use HTTPS, you must also specify one of the following values in your cache behaviors:

- `<ViewerProtocolPolicy>https-only</ViewerProtocolPolicy>`
- `<ViewerProtocolPolicy>redirect-to-https</ViewerProtocolPolicy>`

You can also optionally require that CloudFront use HTTPS to communicate with your origin by specifying one of the following values for the applicable origins:

- `<OriginProtocolPolicy>https-only</OriginProtocolPolicy>`

For more information, see Using Alternate Domain Names and HTTPS in the Amazon CloudFront Developer Guide.

Type: `ViewerCertificate (p. 296)` object

Required: Yes

**WebACLId**

The Web ACL Id (if any) associated with the distribution.

Type: String

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
EncryptionEntities

Complex data type for field-level encryption profiles that includes all of the encryption entities.

Contents

Items

An array of field patterns in a field-level encryption content type-profile mapping.

Type: Array of EncryptionEntity (p. 238) objects

Required: No

Quantity

Number of field pattern items in a field-level encryption content type-profile mapping.

Type: Integer

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
EncryptionEntity

Complex data type for field-level encryption profiles that includes the encryption key and field pattern specifications.

Contents

FieldPatterns

Field patterns in a field-level encryption content type profile specify the fields that you want to be encrypted. You can provide the full field name, or any beginning characters followed by a wildcard (*). You can't overlap field patterns. For example, you can't have both ABC* and AB*. Note that field patterns are case-sensitive.

Type: FieldPatterns (p. 247) object

Required: Yes

ProviderId

The provider associated with the public key being used for encryption. This value must also be provided with the private key for applications to be able to decrypt data.

Type: String

Required: Yes

PublicKeyId

The public key associated with a set of field-level encryption patterns, to be used when encrypting the fields that match the patterns.

Type: String

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
FieldLevelEncryption

A complex data type that includes the profile configurations and other options specified for field-level encryption.

Contents

FieldLevelEncryptionConfig

A complex data type that includes the profile configurations specified for field-level encryption.

Type: FieldLevelEncryptionConfig (p. 240) object

Required: Yes

Id

The configuration ID for a field-level encryption configuration which includes a set of profiles that specify certain selected data fields to be encrypted by specific public keys.

Type: String

Required: Yes

LastModifiedTime

The last time the field-level encryption configuration was changed.

Type: Timestamp

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
FieldLevelEncryptionConfig

A complex data type that includes the profile configurations specified for field-level encryption.

Contents

CallerReference

A unique number that ensures the request can't be replayed.
Type: String
Required: Yes

Comment

An optional comment about the configuration.
Type: String
Required: No

ContentTypeProfileConfig

A complex data type that specifies when to forward content if a content type isn't recognized and profiles to use as by default in a request if a query argument doesn't specify a profile to use.
Type: ContentTypeProfileConfig (p. 209) object
Required: No

QueryArgProfileConfig

A complex data type that specifies when to forward content if a profile isn't found and the profile that can be provided as a query argument in a request.
Type: QueryArgProfileConfig (p. 275) object
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
FieldLevelEncryptionList

List of field-level encryption configurations.

Contents

Items

An array of field-level encryption items.

Type: Array of FieldLevelEncryptionSummary (p. 246) objects

Required: No

MaxItems

The maximum number of elements you want in the response body.

Type: Integer

Required: Yes

NextMarker

If there are more elements to be listed, this element is present and contains the value that you can use for the Marker request parameter to continue listing your configurations where you left off.

Type: String

Required: No

Quantity

The number of field-level encryption items.

Type: Integer

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
FieldLevelEncryptionProfile

A complex data type for field-level encryption profiles.

Contents

FieldLevelEncryptionProfileConfig

A complex data type that includes the profile name and the encryption entities for the field-level encryption profile.

Type: FieldLevelEncryptionProfileConfig (p. 243) object

Required: Yes

Id

The ID for a field-level encryption profile configuration which includes a set of profiles that specify certain selected data fields to be encrypted by specific public keys.

Type: String

Required: Yes

LastModifiedTime

The last time the field-level encryption profile was updated.

Type: Timestamp

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
FieldLevelEncryptionProfileConfig

A complex data type of profiles for the field-level encryption.

Contents

CallerReference

A unique number that ensures the request can't be replayed.

Type: String

Required: Yes

Comment

An optional comment for the field-level encryption profile.

Type: String

Required: No

EncryptionEntities

A complex data type of encryption entities for the field-level encryption profile that include the public key ID, provider, and field patterns for specifying which fields to encrypt with this key.

Type: EncryptionEntities (p. 237) object

Required: Yes

Name

Profile name for the field-level encryption profile.

Type: String

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
FieldLevelEncryptionProfileList

List of field-level encryption profiles.

Contents

Items

The field-level encryption profile items.

Type: Array of FieldLevelEncryptionProfileSummary (p. 245) objects

Required: No

MaxItems

The maximum number of field-level encryption profiles you want in the response body.

Type: Integer

Required: Yes

NextMarker

If there are more elements to be listed, this element is present and contains the value that you can use for the Marker request parameter to continue listing your profiles where you left off.

Type: String

Required: No

Quantity

The number of field-level encryption profiles.

Type: Integer

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
FieldLevelEncryptionProfileSummary

The field-level encryption profile summary.

Contents

Comment

An optional comment for the field-level encryption profile summary.

Type: String

Required: No

EncryptionEntities

A complex data type of encryption entities for the field-level encryption profile that include the public key ID, provider, and field patterns for specifying which fields to encrypt with this key.

Type: EncryptionEntities (p. 237) object

Required: Yes

Id

ID for the field-level encryption profile summary.

Type: String

Required: Yes

LastModifiedTime

The time when the the field-level encryption profile summary was last updated.

Type: Timestamp

Required: Yes

Name

Name for the field-level encryption profile summary.

Type: String

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
FieldLevelEncryptionSummary

A summary of a field-level encryption item.

Contents

Comment
An optional comment about the field-level encryption item.
Type: String
Required: No

ContentTypeProfileConfig
A summary of a content type-profile mapping.
Type: ContentTypeProfileConfig (p. 209) object
Required: No

Id
The unique ID of a field-level encryption item.
Type: String
Required: Yes

LastModifiedTime
The last time that the summary of field-level encryption items was modified.
Type: Timestamp
Required: Yes

QueryArgProfileConfig
A summary of a query argument-profile mapping.
Type: QueryArgProfileConfig (p. 275) object
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
FieldPatterns

A complex data type that includes the field patterns to match for field-level encryption.

Contents

Items

An array of the field-level encryption field patterns.

Type: Array of strings

Required: No

Quantity

The number of field-level encryption field patterns.

Type: Integer

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
ForwardedValues

A complex type that specifies how CloudFront handles query strings and cookies.

Contents

Cookies

A complex type that specifies whether you want CloudFront to forward cookies to the origin and, if so, which ones. For more information about forwarding cookies to the origin, see How CloudFront Forwards, Caches, and Logs Cookies in the Amazon CloudFront Developer Guide.

Type: CookiePreference (p. 212) object

Required: Yes

Headers

A complex type that specifies the Headers, if any, that you want CloudFront to base caching on for this cache behavior.

Type: Headers (p. 252) object

Required: No

QueryString

Indicates whether you want CloudFront to forward query strings to the origin that is associated with this cache behavior and cache based on the query string parameters. CloudFront behavior depends on the value of QueryString and on the values that you specify for QueryStringCacheKeys, if any:

If you specify true for QueryString and you don't specify any values for QueryStringCacheKeys, CloudFront forwards all query string parameters to the origin and caches based on all query string parameters. Depending on how many query string parameters and values you have, this can adversely affect performance because CloudFront must forward more requests to the origin.

If you specify true for QueryString and you specify one or more values for QueryStringCacheKeys, CloudFront forwards all query string parameters to the origin, but it only caches based on the query string parameters that you specify.

If you specify false for QueryString, CloudFront doesn't forward any query string parameters to the origin, and doesn't cache based on query string parameters.

For more information, see Configuring CloudFront to Cache Based on Query String Parameters in the Amazon CloudFront Developer Guide.

Type: Boolean

Required: Yes

QueryStringCacheKeys

A complex type that contains information about the query string parameters that you want CloudFront to use for caching for this cache behavior.

Type: QueryStringCacheKeys (p. 277) object

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
GeoRestriction

A complex type that controls the countries in which your content is distributed. CloudFront determines the location of your users using MaxMind GeoIP databases.

Contents

Items

A complex type that contains a Location element for each country in which you want CloudFront either to distribute your content (whitelist) or not distribute your content (blacklist).

The Location element is a two-letter, uppercase country code for a country that you want to include in your blacklist or whitelist. Include one Location element for each country.

CloudFront and MaxMind both use ISO 3166 country codes. For the current list of countries and the corresponding codes, see ISO 3166-1-alpha-2 code on the International Organization for Standardization website. You can also refer to the country list on the CloudFront console, which includes both country names and codes.

Type: Array of strings

Required: No

Quantity

When geo restriction is enabled, this is the number of countries in your whitelist or blacklist. Otherwise, when it is not enabled, Quantity is 0, and you can omit Items.

Type: Integer

Required: Yes

RestrictionType

The method that you want to use to restrict distribution of your content by country:

- none: No geo restriction is enabled, meaning access to content is not restricted by client geo location.
- blacklist: The Location elements specify the countries in which you don't want CloudFront to distribute your content.
- whitelist: The Location elements specify the countries in which you want CloudFront to distribute your content.

Type: String

Valid Values: blacklist | whitelist | none

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
Headers

A complex type that specifies the request headers, if any, that you want CloudFront to base caching on for this cache behavior.

For the headers that you specify, CloudFront caches separate versions of a specified object based on the header values in viewer requests. For example, suppose viewer requests for logo.jpg contain a custom product header that has a value of either acme or apex, and you configure CloudFront to cache your content based on values in the product header. CloudFront forwards the product header to the origin and caches the response from the origin once for each header value. For more information about caching based on header values, see How CloudFront Forwards and Caches Headers in the Amazon CloudFront Developer Guide.

Contents

Items

A list that contains one Name element for each header that you want CloudFront to use for caching in this cache behavior. If Quantity is 0, omit Items.

Type: Array of strings

Required: No

Quantity

The number of different headers that you want CloudFront to base caching on for this cache behavior. You can configure each cache behavior in a web distribution to do one of the following:

- **Forward all headers to your origin**: Specify 1 for Quantity and * for Name.
  
  **Important**
  
  CloudFront doesn’t cache the objects that are associated with this cache behavior. Instead, CloudFront sends every request to the origin.

- **Forward a whitelist of headers you specify**: Specify the number of headers that you want CloudFront to base caching on. Then specify the header names in Name elements. CloudFront caches your objects based on the values in the specified headers.

- **Forward only the default headers**: Specify 0 for Quantity and omit Items. In this configuration, CloudFront doesn’t cache based on the values in the request headers.

Regardless of which option you choose, CloudFront forwards headers to your origin based on whether the origin is an S3 bucket or a custom origin. See the following documentation:

- **S3 bucket**: See HTTP Request Headers That CloudFront Removes or Updates
- **Custom origin**: See HTTP Request Headers and CloudFront Behavior

Type: Integer

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
Invalidation

An invalidation.

Contents

CreateTime

The date and time the invalidation request was first made.

Type: Timestamp

Required: Yes

Id

The identifier for the invalidation request. For example: IDFDVBD632BHDS5.

Type: String

Required: Yes

InvalidationBatch

The current invalidation information for the batch request.

Type: InvalidationBatch (p. 255) object

Required: Yes

Status

The status of the invalidation request. When the invalidation batch is finished, the status is Completed.

Type: String

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
InvalidationBatch

An invalidation batch.

Contents

CallerReference

A value that you specify to uniquely identify an invalidation request. CloudFront uses the value to prevent you from accidentally resubmitting an identical request. Whenever you create a new invalidation request, you must specify a new value for CallerReference and change other values in the request as applicable. One way to ensure that the value of CallerReference is unique is to use a timestamp, for example, 20120301090000.

If you make a second invalidation request with the same value for CallerReference, and if the rest of the request is the same, CloudFront doesn't create a new invalidation request. Instead, CloudFront returns information about the invalidation request that you previously created with the same CallerReference.

If CallerReference is a value you already sent in a previous invalidation batch request but the content of any Path is different from the original request, CloudFront returns an InvalidBatchAlreadyExists error.

Type: String
Required: Yes

Paths

A complex type that contains information about the objects that you want to invalidate. For more information, see Specifying the Objects to Invalidate in the Amazon CloudFront Developer Guide.

Type: Paths (p. 269) object
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
InvalidationList

The **InvalidationList** complex type describes the list of invalidation objects. For more information about invalidation, see [Invalidating Objects (Web Distributions Only)] in the *Amazon CloudFront Developer Guide*.

## Contents

### IsTruncated

A flag that indicates whether more invalidation batch requests remain to be listed. If your results were truncated, you can make a follow-up pagination request using the **Marker** request parameter to retrieve more invalidation batches in the list.

- **Type:** Boolean
- **Required:** Yes

### Items

A complex type that contains one **InvalidationSummary** element for each invalidation batch created by the current AWS account.

- **Type:** Array of **InvalidationSummary** (p. 258) objects
- **Required:** No

### Marker

The value that you provided for the **Marker** request parameter.

- **Type:** String
- **Required:** Yes

### MaxItems

The value that you provided for the **MaxItems** request parameter.

- **Type:** Integer
- **Required:** Yes

### NextMarker

If **IsTruncated** is true, this element is present and contains the value that you can use for the **Marker** request parameter to continue listing your invalidation batches where they left off.

- **Type:** String
- **Required:** No

### Quantity

The number of invalidation batches that were created by the current AWS account.

- **Type:** Integer
- **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
InvalidationSummary

A summary of an invalidation request.

Contents

CreateTime

   Type: Timestamp
   Required: Yes

Id

   The unique ID for an invalidation request.
   Type: String
   Required: Yes

Status

   The status of an invalidation request.
   Type: String
   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
KeyPairIds

A complex type that lists the active CloudFront key pairs, if any, that are associated with AwsAccountNumber.

For more information, see ActiveTrustedSigners (p. 192).

Contents

Items

A complex type that lists the active CloudFront key pairs, if any, that are associated with AwsAccountNumber.

For more information, see ActiveTrustedSigners (p. 192).

Type: Array of strings

Required: No

Quantity

The number of active CloudFront key pairs for AwsAccountNumber.

For more information, see ActiveTrustedSigners (p. 192).

Type: Integer

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
LambdaFunctionAssociation

A complex type that contains a Lambda function association.

Contents

EventType

Specifies the event type that triggers a Lambda function invocation. You can specify the following values:

- **viewer-request**: The function executes when CloudFront receives a request from a viewer and before it checks to see whether the requested object is in the edge cache.
- **origin-request**: The function executes only when CloudFront forwards a request to your origin. When the requested object is in the edge cache, the function doesn't execute.
- **origin-response**: The function executes after CloudFront receives a response from the origin and before it caches the object in the response. When the requested object is in the edge cache, the function doesn't execute.

If the origin returns an HTTP status code other than HTTP 200 (OK), the function doesn't execute.

- **viewer-response**: The function executes before CloudFront returns the requested object to the viewer. The function executes regardless of whether the object was already in the edge cache.

If the origin returns an HTTP status code other than HTTP 200 (OK), the function doesn't execute.

Type: String

Valid Values: viewer-request | viewer-response | origin-request | origin-response

Required: Yes

LambdaFunctionARN

The ARN of the Lambda function. You must specify the ARN of a function version; you can't specify a Lambda alias or $LATEST.

Type: String

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
LambdaFunctionAssociations

A complex type that specifies a list of Lambda functions associations for a cache behavior.

If you want to invoke one or more Lambda functions triggered by requests that match the PathPattern of the cache behavior, specify the applicable values for Quantity and Items. Note that there can be up to 4 LambdaFunctionAssociation items in this list (one for each possible value of EventType) and each EventType can be associated with the Lambda function only once.

If you don't want to invoke any Lambda functions for the requests that match PathPattern, specify 0 for Quantity and omit Items.

Contents

Items

Optional: A complex type that contains LambdaFunctionAssociation items for this cache behavior. If Quantity is 0, you can omit Items.

Type: Array of LambdaFunctionAssociation (p. 260) objects

Required: No

Quantity

The number of Lambda function associations for this cache behavior.

Type: Integer

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
LoggingConfig

A complex type that controls whether access logs are written for the distribution.

Contents

Bucket

The Amazon S3 bucket to store the access logs in, for example, myawslogbucket.s3.amazonaws.com.

Type: String

Required: Yes

Enabled

Specifies whether you want CloudFront to save access logs to an Amazon S3 bucket. If you don't want to enable logging when you create a distribution or if you want to disable logging for an existing distribution, specify false for Enabled, and specify empty Bucket and Prefix elements. If you specify false for Enabled but you specify values for Bucket, prefix, and IncludeCookies, the values are automatically deleted.

Type: Boolean

Required: Yes

IncludeCookies

Specifies whether you want CloudFront to include cookies in access logs, specify true for IncludeCookies. If you choose to include cookies in logs, CloudFront logs all cookies regardless of how you configure the cache behaviors for this distribution. If you don't want to include cookies when you create a distribution or if you want to disable include cookies for an existing distribution, specify false for IncludeCookies.

Type: Boolean

Required: Yes

Prefix

An optional string that you want CloudFront to prefix to the access log filenames for this distribution, for example, myprefix/. If you want to enable logging, but you don't want to specify a prefix, you still must include an empty Prefix element in the Logging element.

Type: String

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
Origin

A complex type that describes the Amazon S3 bucket or the HTTP server (for example, a web server) from which CloudFront gets your files. You must create at least one origin.

For the current limit on the number of origins that you can create for a distribution, see Amazon CloudFront Limits in the AWS General Reference.

Contents

**CustomHeaders**

A complex type that contains names and values for the custom headers that you want.

Type: CustomHeaders (p. 216) object

Required: No

**CustomOriginConfig**

A complex type that contains information about a custom origin. If the origin is an Amazon S3 bucket, use the S3OriginConfig element instead.

Type: CustomOriginConfig (p. 217) object

Required: No

**DomainName**

Amazon S3 origins: The DNS name of the Amazon S3 bucket from which you want CloudFront to get objects for this origin, for example, myawsbucket.s3.amazonaws.com.

Constraints for Amazon S3 origins:
- If you configured Amazon S3 Transfer Acceleration for your bucket, don't specify the s3-accelerate endpoint for DomainName.
- The bucket name must be between 3 and 63 characters long (inclusive).
- The bucket name must contain only lowercase characters, numbers, periods, underscores, and dashes.
- The bucket name must not contain adjacent periods.

Custom Origins: The DNS domain name for the HTTP server from which you want CloudFront to get objects for this origin, for example, www.example.com.

Constraints for custom origins:
- DomainName must be a valid DNS name that contains only a-z, A-Z, 0-9, dot (.), hyphen (-), or underscore (_) characters.
- The name cannot exceed 128 characters.

Type: String

Required: Yes

**Id**

A unique identifier for the origin. The value of Id must be unique within the distribution.

When you specify the value of TargetOriginId for the default cache behavior or for another cache behavior, you indicate the origin to which you want the cache behavior to route requests by specifying the value of the Id element for that origin. When a request matches the path pattern for
that cache behavior, CloudFront routes the request to the specified origin. For more information, see Cache Behavior Settings in the Amazon CloudFront Developer Guide.

Type: String
Required: Yes

OriginPath

An optional element that causes CloudFront to request your content from a directory in your Amazon S3 bucket or your custom origin. When you include the OriginPath element, specify the directory name, beginning with a /. CloudFront appends the directory name to the value of DomainName, for example, example.com/production. Do not include a / at the end of the directory name.

For example, suppose you've specified the following values for your distribution:

- DomainName: An Amazon S3 bucket named myawsbucket.
- OriginPath: /production
- CNAME: example.com

When a user enters example.com/index.html in a browser, CloudFront sends a request to Amazon S3 for myawsbucket/production/index.html.

When a user enters example.com/acme/index.html in a browser, CloudFront sends a request to Amazon S3 for myawsbucket/production/acme/index.html.

Type: String
Required: No

S3OriginConfig

A complex type that contains information about the Amazon S3 origin. If the origin is a custom origin, use the CustomOriginConfig element instead.

Type: S3OriginConfig (p. 280) object
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
OriginCustomHeader

A complex type that contains HeaderName and HeaderValue elements, if any, for this distribution.

Contents

**HeaderName**

The name of a header that you want CloudFront to forward to your origin. For more information, see [Forwarding Custom Headers to Your Origin (Web Distributions Only)](https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/forward-custom-headers-web-distributions.html) in the *Amazon CloudFront Developer Guide*.

Type: String

Required: Yes

**HeaderValue**

The value for the header that you specified in the HeaderName field.

Type: String

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
Origins

A complex type that contains information about origins for this distribution.

Contents

Items

A complex type that contains origins for this distribution.

Type: Array of Origin (p. 264) objects

Array Members: Minimum number of 1 item.

Required: No

Quantity

The number of origins for this distribution.

Type: Integer

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
OriginSslProtocols

A complex type that contains information about the SSL/TLS protocols that CloudFront can use when establishing an HTTPS connection with your origin.

Contents

Items

A list that contains allowed SSL/TLS protocols for this distribution.

Type: Array of strings

Valid Values: SSLv3 | TLSv1 | TLSv1.1 | TLSv1.2

Required: Yes

Quantity

The number of SSL/TLS protocols that you want to allow CloudFront to use when establishing an HTTPS connection with this origin.

Type: Integer

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
Paths

A complex type that contains information about the objects that you want to invalidate. For more information, see Specifying the Objects to Invalidate in the Amazon CloudFront Developer Guide.

Contents

Items

A complex type that contains a list of the paths that you want to invalidate.

Type: Array of strings

Required: No

Quantity

The number of objects that you want to invalidate.

Type: Integer

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
PublicKey

A complex data type of public keys you add to CloudFront to use with features like field-level encryption.

Contents

CreatedTime

A time you added a public key to CloudFront.
Type: Timestamp
Required: Yes

Id

A unique ID assigned to a public key you’ve added to CloudFront.
Type: String
Required: Yes

PublicKeyConfig

A complex data type for a public key you add to CloudFront to use with features like field-level encryption.
Type: PublicKeyConfig (p. 271) object
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
PublicKeyConfig

Information about a public key you add to CloudFront to use with features like field-level encryption.

Contents

CallerReference

A unique number that ensures the request can't be replayed.

Type: String
Required: Yes

Comment

An optional comment about a public key.

Type: String
Required: No

EncodedKey

The encoded public key that you want to add to CloudFront to use with features like field-level encryption.

Type: String
Required: Yes

Name

The name for a public key you add to CloudFront to use with features like field-level encryption.

Type: String
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
PublicKeyList

A list of public keys you’ve added to CloudFront to use with features like field-level encryption.

Contents

Items

An array of information about a public key you add to CloudFront to use with features like field-level encryption.

Type: Array of PublicKeySummary (p. 273) objects

Required: No

MaxItems

The maximum number of public keys you want in the response body.

Type: Integer

Required: Yes

NextMarker

If there are more elements to be listed, this element is present and contains the value that you can use for the Marker request parameter to continue listing your public keys where you left off.

Type: String

Required: No

Quantity

The number of public keys you added to CloudFront to use with features like field-level encryption.

Type: Integer

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
PublicKeySummary

Public key information summary.

Contents

Comment
Comment for public key information summary.
Type: String
Required: No

CreatedTime
Creation time for public key information summary.
Type: Timestamp
Required: Yes

EncodedKey
Encoded key for public key information summary.
Type: String
Required: Yes

Id
ID for public key information summary.
Type: String
Required: Yes

Name
Name for public key information summary.
Type: String
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
QueryArgProfile

Query argument-profile mapping for field-level encryption.

Contents

ProfileId

ID of profile to use for field-level encryption query argument-profile mapping

Type: String

Required: Yes

QueryArg

Query argument for field-level encryption query argument-profile mapping.

Type: String

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
QueryArgProfileConfig

Configuration for query argument-profile mapping for field-level encryption.

Contents

ForwardWhenQueryArgProfileIsUnknown

Flag to set if you want a request to be forwarded to the origin even if the profile specified by the field-level encryption query argument, fle-profile, is unknown.

Type: Boolean

Required: Yes

QueryArgProfiles

Profiles specified for query argument-profile mapping for field-level encryption.

Type: QueryArgProfiles (p. 276) object

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
QueryArgProfiles

Query argument-profile mapping for field-level encryption.

Contents

Items

Number of items for query argument-profile mapping for field-level encryption.

Type: Array of QueryArgProfile (p. 274) objects

Required: No

Quantity

Number of profiles for query argument-profile mapping for field-level encryption.

Type: Integer

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
QueryStringCacheKeys

Contents

Items

(Optional) A list that contains the query string parameters that you want CloudFront to use as a basis for caching for this cache behavior. If Quantity is 0, you can omit Items.

Type: Array of strings
Required: No

Quantity

The number of whitelisted query string parameters for this cache behavior.

Type: Integer
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
Restrictions

A complex type that identifies ways in which you want to restrict distribution of your content.

Contents

GeoRestriction

A complex type that controls the countries in which your content is distributed. CloudFront determines the location of your users using MaxMind GeoIP databases.

Type: GeoRestriction (p. 250) object

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
S3Origin

A complex type that contains information about the Amazon S3 bucket from which you want CloudFront to get your media files for distribution.

Contents

DomainName

The DNS name of the Amazon S3 origin.
Type: String
Required: Yes

OriginAccessIdentity

The CloudFront origin access identity to associate with the RTMP distribution. Use an origin access identity to configure the distribution so that end users can only access objects in an Amazon S3 bucket through CloudFront.

If you want end users to be able to access objects using either the CloudFront URL or the Amazon S3 URL, specify an empty OriginAccessIdentity element.

To delete the origin access identity from an existing distribution, update the distribution configuration and include an empty OriginAccessIdentity element.

To replace the origin access identity, update the distribution configuration and specify the new origin access identity.

For more information, see Using an Origin Access Identity to Restrict Access to Your Amazon S3 Content in the Amazon CloudFront Developer Guide.
Type: String
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
S3OriginConfig

A complex type that contains information about the Amazon S3 origin. If the origin is a custom origin, use the CustomOriginConfig element instead.

Contents

OriginAccessIdentity

The CloudFront origin access identity to associate with the origin. Use an origin access identity to configure the origin so that viewers can only access objects in an Amazon S3 bucket through CloudFront. The format of the value is:

origin-access-identity/cloudfront/ID-of-origin-access-identity

where ID-of-origin-access-identity is the value that CloudFront returned in the ID element when you created the origin access identity.

If you want viewers to be able to access objects using either the CloudFront URL or the Amazon S3 URL, specify an empty OriginAccessIdentity element.

To delete the origin access identity from an existing distribution, update the distribution configuration and include an empty OriginAccessIdentity element.

To replace the origin access identity, update the distribution configuration and specify the new origin access identity.

For more information about the origin access identity, see Serving Private Content through CloudFront in the Amazon CloudFront Developer Guide.

Type: String

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
Signer

A complex type that lists the AWS accounts that were included in the TrustedSigners complex type, as well as their active CloudFront key pair IDs, if any.

Contents

AwsAccountNumber

An AWS account that is included in the TrustedSigners complex type for this RTMP distribution. Valid values include:

- `self`, which is the AWS account used to create the distribution.
- An AWS account number.

Type: String

Required: No

KeyPairIds

A complex type that lists the active CloudFront key pairs, if any, that are associated with AwsAccountNumber.

Type: KeyPairIds (p. 259) object

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
StreamingDistribution

A streaming distribution.

Contents

ActiveTrustedSigners

A complex type that lists the AWS accounts, if any, that you included in the TrustedSigners complex type for this distribution. These are the accounts that you want to allow to create signed URLs for private content.

The Signer complex type lists the AWS account number of the trusted signer or self if the signer is the AWS account that created the distribution. The Signer element also includes the IDs of any active CloudFront key pairs that are associated with the trusted signer's AWS account. If no KeyPairId element appears for a Signer, that signer can't create signed URLs.

For more information, see Serving Private Content through CloudFront in the Amazon CloudFront Developer Guide.

Type: ActiveTrustedSigners (p. 192) object

Required: Yes

ARN

Type: String

Required: Yes

DomainName

The domain name that corresponds to the streaming distribution, for example, s5c39gqb8ow64r.cloudfront.net.

Type: String

Required: Yes

Id

The identifier for the RTMP distribution. For example: EGTXBD79EXAMPLE.

Type: String

Required: Yes

LastModifiedTime

The date and time that the distribution was last modified.

Type: Timestamp

Required: No

Status

The current status of the RTMP distribution. When the status is Deployed, the distribution's information is propagated to all CloudFront edge locations.

Type: String

Required: Yes
**StreamingDistributionConfig**

The current configuration information for the RTMP distribution.

Type: `StreamingDistributionConfig (p. 284)` object

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
StreamingDistributionConfig

The RTMP distribution's configuration information.

Contents

Aliases

A complex type that contains information about CNAMEs (alternate domain names), if any, for this streaming distribution.

Type: Aliases (p. 194) object

Required: No

CallerReference

A unique number that ensures that the request can't be replayed. If the CallerReference is new (no matter the content of the StreamingDistributionConfig object), a new streaming distribution is created. If the CallerReference is a value that you already sent in a previous request to create a streaming distribution, and the content of the StreamingDistributionConfig is identical to the original request (ignoring white space), the response includes the same information returned to the original request. If the CallerReference is a value that you already sent in a previous request to create a streaming distribution but the content of the StreamingDistributionConfig is different from the original request, CloudFront returns a DistributionAlreadyExists error.

Type: String

Required: Yes

Comment

Any comments you want to include about the streaming distribution.

Type: String

Required: Yes

Enabled

Whether the streaming distribution is enabled to accept user requests for content.

Type: Boolean

Required: Yes

Logging

A complex type that controls whether access logs are written for the streaming distribution.

Type: StreamingLoggingConfig (p. 291) object

Required: No

PriceClass

A complex type that contains information about price class for this streaming distribution.

Type: String

Valid Values: PriceClass_100 | PriceClass_200 | PriceClass_All
S3Origin

A complex type that contains information about the Amazon S3 bucket from which you want CloudFront to get your media files for distribution.

Type: S3Origin (p. 279) object

Required: Yes

TrustedSigners

A complex type that specifies any AWS accounts that you want to permit to create signed URLs for private content. If you want the distribution to use signed URLs, include this element; if you want the distribution to use public URLs, remove this element. For more information, see Serving Private Content through CloudFront in the Amazon CloudFront Developer Guide.

Type: TrustedSigners (p. 295) object

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
StreamingDistributionConfigWithTags

A streaming distribution Configuration and a list of tags to be associated with the streaming distribution.

Contents

StreamingDistributionConfig

A streaming distribution Configuration.

Type: StreamingDistributionConfig (p. 284) object

Required: Yes

Tags

A complex type that contains zero or more Tag elements.

Type: Tags (p. 294) object

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
StreamingDistributionList

A streaming distribution list.

Contents

IsTruncated

A flag that indicates whether more streaming distributions remain to be listed. If your results were truncated, you can make a follow-up pagination request using the Marker request parameter to retrieve more distributions in the list.

Type: Boolean
Required: Yes

Items

A complex type that contains one StreamingDistributionSummary element for each distribution that was created by the current AWS account.

Type: Array of StreamingDistributionSummary (p. 289) objects
Required: No

Marker

The value you provided for the Marker request parameter.

Type: String
Required: Yes

MaxItems

The value you provided for the MaxItems request parameter.

Type: Integer
Required: Yes

NextMarker

If IsTruncated is true, this element is present and contains the value you can use for the Marker request parameter to continue listing your RTMP distributions where they left off.

Type: String
Required: No

Quantity

The number of streaming distributions that were created by the current AWS account.

Type: Integer
Required: Yes

See Also

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

- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java
- AWS SDK for Ruby V2
StreamingDistributionSummary

A summary of the information for an Amazon CloudFront streaming distribution.

Contents

**Aliases**

A complex type that contains information about CNAMEs (alternate domain names), if any, for this streaming distribution.

Type: Aliases (p. 194) object

Required: Yes

**ARN**

The ARN (Amazon Resource Name) for the streaming distribution. For example: `arn:aws:cloudfront::123456789012:streaming-distribution/EDFDVBD632BHDS5`, where 123456789012 is your AWS account ID.

Type: String

Required: Yes

**Comment**

The comment originally specified when this distribution was created.

Type: String

Required: Yes

**DomainName**

The domain name corresponding to the distribution, for example, `d111111abcdef8.cloudfront.net`.

Type: String

Required: Yes

**Enabled**

Whether the distribution is enabled to accept end user requests for content.

Type: Boolean

Required: Yes

**Id**

The identifier for the distribution, for example, `EDFDVBD632BHDS5`.

Type: String

Required: Yes

**LastModifiedTime**

The date and time the distribution was last modified.

Type: Timestamp
Required: Yes

**PriceClass**

Type: String

Valid Values: PriceClass_100 | PriceClass_200 | PriceClass_All

Required: Yes

**S3Origin**

A complex type that contains information about the Amazon S3 bucket from which you want CloudFront to get your media files for distribution.

Type: S3Origin (p. 279) object

Required: Yes

**Status**

Indicates the current status of the distribution. When the status is Deployed, the distribution's information is fully propagated throughout the Amazon CloudFront system.

Type: String

Required: Yes

**TrustedSigners**

A complex type that specifies the AWS accounts, if any, that you want to allow to create signed URLs for private content. If you want to require signed URLs in requests for objects in the target origin that match the PathPattern for this cache behavior, specify true for Enabled, and specify the applicable values for Quantity and Items. If you don't want to require signed URLs in requests for objects that match PathPattern, specify false for Enabled and 0 for Quantity. Omit Items. To add, change, or remove one or more trusted signers, change Enabled to true (if it's currently false), change Quantity as applicable, and specify all of the trusted signers that you want to include in the updated distribution.

Type: TrustedSigners (p. 295) object

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
StreamingLoggingConfig

A complex type that controls whether access logs are written for this streaming distribution.

**Contents**

**Bucket**

The Amazon S3 bucket to store the access logs in, for example, myawslogbucket.s3.amazonaws.com.

Type: String
Required: Yes

**Enabled**

Specifies whether you want CloudFront to save access logs to an Amazon S3 bucket. If you don't want to enable logging when you create a streaming distribution or if you want to disable logging for an existing streaming distribution, specify false for Enabled, and specify empty Bucket and Prefix elements. If you specify false for Enabled but you specify values for Bucket and Prefix, the values are automatically deleted.

Type: Boolean
Required: Yes

**Prefix**

An optional string that you want CloudFront to prefix to the access log filenames for this streaming distribution, for example, myprefix/. If you want to enable logging, but you don't want to specify a prefix, you still must include an empty Prefix element in the Logging element.

Type: String
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 complex type that contains `Tag` key and `Tag` value.

Contents

**Key**

A string that contains `Tag` key.

The string length should be between 1 and 128 characters. Valid characters include `a-z`, `A-Z`, `0-9`, space, and the special characters `_ - . : / = + @`.

Type: String


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

Required: Yes

**Value**

A string that contains an optional `Tag` value.

The string length should be between 0 and 256 characters. Valid characters include `a-z`, `A-Z`, `0-9`, space, and the special characters `_ - . : / = + @`.

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
TagKeys

A complex type that contains zero or more Tag elements.

Contents

Items

A complex type that contains Tag key elements.

Type: Array of strings


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
Tags

A complex type that contains zero or more Tag elements.

Contents

Items

A complex type that contains Tag elements.

Type: Array of Tag (p. 292) objects

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
TrustedSigners

A complex type that specifies the AWS accounts, if any, that you want to allow to create signed URLs for private content.

If you want to require signed URLs in requests for objects in the target origin that match the PathPattern for this cache behavior, specify true for Enabled, and specify the applicable values for Quantity and Items. For more information, see Serving Private Content through CloudFront in the Amazon CloudFront Developer Guide.

If you don't want to require signed URLs in requests for objects that match PathPattern, specify false for Enabled and 0 for Quantity. Omit Items.

To add, change, or remove one or more trusted signers, change Enabled to true (if it's currently false), change Quantity as applicable, and specify all of the trusted signers that you want to include in the updated distribution.

For more information about updating the distribution configuration, see DistributionConfig (p. 224).

Contents

Enabled

Specifies whether you want to require viewers to use signed URLs to access the files specified by PathPattern and TargetOriginId.

Type: Boolean

Required: Yes

Items

Optional: A complex type that contains trusted signers for this cache behavior. If Quantity is 0, you can omit Items.

Type: Array of strings

Required: No

Quantity

The number of trusted signers for this cache behavior.

Type: Integer

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
**ViewerCertificate**

A complex type that specifies the following:

- Whether you want viewers to use HTTP or HTTPS to request your objects.
- If you want viewers to use HTTPS, whether you're using an alternate domain name such as example.com or the CloudFront domain name for your distribution, such as d111111abcdef8.cloudfront.net.
- If you're using an alternate domain name, whether AWS Certificate Manager (ACM) provided the certificate, or you purchased a certificate from a third-party certificate authority and imported it into ACM or uploaded it to the IAM certificate store.

You must specify only one of the following values:

- ViewerCertificate:ACMCertificateArn (p. 297)
- ViewerCertificate:IAMCertificateId (p. 298)
- ViewerCertificate:CloudFrontDefaultCertificate (p. 297)

Don't specify false for CloudFrontDefaultCertificate.

**If you want viewers to use HTTP instead of HTTPS to request your objects:** Specify the following value:

```
<CloudFrontDefaultCertificate>true</CloudFrontDefaultCertificate>
```

In addition, specify allow-all for ViewerProtocolPolicy for all of your cache behaviors.

**If you want viewers to use HTTPS to request your objects:** Choose the type of certificate that you want to use based on whether you're using an alternate domain name for your objects or the CloudFront domain name:

- **If you're using an alternate domain name, such as example.com:** Specify one of the following values, depending on whether ACM provided your certificate or you purchased your certificate from third-party certificate authority:
  - `<ACMCertificateArn>ARN for ACM SSL/TLS certificate</ACMCertificateArn>` where ARN for ACM SSL/TLS certificate is the ARN for the ACM SSL/TLS certificate that you want to use for this distribution.
  - `<IAMCertificateId>IAM certificate ID</IAMCertificateId>` where IAM certificate ID is the ID that IAM returned when you added the certificate to the IAM certificate store.

If you specify ACMCertificateArn or IAMCertificateId, you must also specify a value for SSLSupportMethod.

If you choose to use an ACM certificate or a certificate in the IAM certificate store, we recommend that you use only an alternate domain name in your object URLs (https://example.com/logo.jpg). If you use the domain name that is associated with your CloudFront distribution (such as https://d111111abcdef8.cloudfront.net/logo.jpg) and the viewer supports SNI, then CloudFront behaves normally. However, if the browser does not support SNI, the user's experience depends on the value that you choose for SSLSupportMethod:

- **vip:** The viewer displays a warning because there is a mismatch between the CloudFront domain name and the domain name in your SSL/TLS certificate.
- **sni-only:** CloudFront drops the connection with the browser without returning the object.

**If you're using the CloudFront domain name for your distribution, such as d111111abcdef8.cloudfront.net:** Specify the following value:
If you want viewers to use HTTPS, you must also specify one of the following values in your cache behaviors:

- `<ViewerProtocolPolicy>https-only</ViewerProtocolPolicy>`
- `<ViewerProtocolPolicy>redirect-to-https</ViewerProtocolPolicy>`

You can also optionally require that CloudFront use HTTPS to communicate with your origin by specifying one of the following values for the applicable origins:

- `<OriginProtocolPolicy>https-only</OriginProtocolPolicy>`

For more information, see Using Alternate Domain Names and HTTPS in the *Amazon CloudFront Developer Guide*.

### Contents

**ACMCertificateArn**

For information about how and when to use `ACMCertificateArn`, see [ViewerCertificate (p. 296)](#).

Type: String

Required: No

**Certificate**

This field has been deprecated. Use one of the following fields instead:

- [ViewerCertificate:ACMCertificateArn (p. 297)](#)
- [ViewerCertificate:IAMCertificateId (p. 298)](#)
- [ViewerCertificate:CloudFrontDefaultCertificate (p. 297)](#)

Type: String

Required: No

**CertificateSource**

This field has been deprecated. Use one of the following fields instead:

- [ViewerCertificate:ACMCertificateArn (p. 297)](#)
- [ViewerCertificate:IAMCertificateId (p. 298)](#)
- [ViewerCertificate:CloudFrontDefaultCertificate (p. 297)](#)

Type: String

Valid Values: cloudfront | iam | acm

Required: No

**CloudFrontDefaultCertificate**

For information about how and when to use `CloudFrontDefaultCertificate`, see [ViewerCertificate (p. 296)](#).

Type: Boolean
IAMCertificateId

For information about how and when to use IAMCertificateId, see ViewerCertificate (p. 296).

Type: String

Required: No

MinimumProtocolVersion

Specify the security policy that you want CloudFront to use for HTTPS connections. A security policy determines two settings:

- The minimum SSL/TLS protocol that CloudFront uses to communicate with viewers
- The cipher that CloudFront uses to encrypt the content that it returns to viewers

Note

On the CloudFront console, this setting is called Security policy.

We recommend that you specify TLSv1.1_2016 unless your users are using browsers or devices that do not support TLSv1.1 or later.

When both of the following are true, you must specify TLSv1 or later for the security policy:

- You're using a custom certificate: you specified a value for ACMCertificateArn or for IAMCertificateId
- You're using SNI: you specified sni-only for SSLSupportMethod

If you specify true for CloudFrontDefaultCertificate, CloudFront automatically sets the security policy to TLSv1 regardless of the value that you specify for MinimumProtocolVersion.

For information about the relationship between the security policy that you choose and the protocols and ciphers that CloudFront uses to communicate with viewers, see Supported SSL/TLS Protocols and Ciphers for Communication Between Viewers and CloudFront in the Amazon CloudFront Developer Guide.

Type: String

Valid Values: SSLv3 | TLSv1 | TLSv1_2016 | TLSv1.1_2016 | TLSv1.2_2018

Required: No

SSLSupportMethod

If you specify a value for ViewerCertificate:ACMCertificateArn (p. 297) or for ViewerCertificate:IAMCertificateId (p. 298), you must also specify how you want CloudFront to serve HTTPS requests: using a method that works for all clients or one that works for most clients:

- vip: CloudFront uses dedicated IP addresses for your content and can respond to HTTPS requests from any viewer. However, you will incur additional monthly charges.
- sni-only: CloudFront can respond to HTTPS requests from viewers that support Server Name Indication (SNI). All modern browsers support SNI, but some browsers still in use don't support SNI. If some of your users' browsers don't support SNI, we recommend that you do one of the following:
  - Use the vip option (dedicated IP addresses) instead of sni-only.
  - Use the CloudFront SSL/TLS certificate instead of a custom certificate. This requires that you use the CloudFront domain name of your distribution in the URLs for your objects, for example, https://d111111abcdef8.cloudfront.net/logo.png.
  - If you can control which browser your users use, upgrade the browser to one that supports SNI.
  - Use HTTP instead of HTTPS.
Don't specify a value for SSLSupportMethod if you specified `<CloudFrontDefaultCertificate>true<CloudFrontDefaultCertificate>`. For more information, see Using Alternate Domain Names and HTTPS in the Amazon CloudFront Developer Guide.

Type: String

Valid Values: sni-only | vip

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