Table of Contents

Welcome ........................................................................................................................................... 1
Actions ............................................................................................................................................. 2
  AssociateAlias ............................................................................................................................ 5
    Request Syntax ..................................................................................................................... 5
    URI Request Parameters ..................................................................................................... 5
    Request Body ....................................................................................................................... 5
    Response Syntax ................................................................................................................ 5
    Response Elements ............................................................................................................. 5
    Errors .................................................................................................................................. 5
    See Also ............................................................................................................................ 6
  CreateCachePolicy .................................................................................................................. 7
    Request Syntax ..................................................................................................................... 7
    URI Request Parameters ..................................................................................................... 8
    Request Body ....................................................................................................................... 8
    Response Syntax ................................................................................................................ 9
    Response Elements ............................................................................................................. 10
    Errors .................................................................................................................................. 10
    See Also ............................................................................................................................ 11
  CreateCloudFrontOriginAccessIdentity ............................................................................... 12
    Request Syntax ..................................................................................................................... 12
    URI Request Parameters ..................................................................................................... 12
    Request Body ....................................................................................................................... 12
    Response Syntax ................................................................................................................ 13
    Response Elements ............................................................................................................. 13
    Errors .................................................................................................................................. 13
    See Also ............................................................................................................................ 14
  CreateDistribution ................................................................................................................... 15
    Request Syntax ..................................................................................................................... 15
    URI Request Parameters ..................................................................................................... 19
    Request Body ....................................................................................................................... 19
    Response Syntax ................................................................................................................ 23
    Response Elements ............................................................................................................. 28
    Errors .................................................................................................................................. 30
    See Also ............................................................................................................................ 35
  CreateDistributionWithTags ............................................................................................... 37
    Request Syntax ..................................................................................................................... 37
    URI Request Parameters ..................................................................................................... 41
    Request Body ....................................................................................................................... 41
    Response Syntax ................................................................................................................ 42
    Response Elements ............................................................................................................. 47
    Errors .................................................................................................................................. 48
    See Also ............................................................................................................................ 54
  CreateFieldLevelEncryptionConfig .................................................................................. 55
    Request Syntax ..................................................................................................................... 55
    URI Request Parameters ..................................................................................................... 55
    Request Body ....................................................................................................................... 55
    Response Syntax ................................................................................................................ 56
    Response Elements ............................................................................................................. 57
    Errors .................................................................................................................................. 57
    See Also ............................................................................................................................ 58
  CreateFieldLevelEncryptionProfile ................................................................................ 59
    Request Syntax ..................................................................................................................... 59
    URI Request Parameters ..................................................................................................... 59
    Request Body ....................................................................................................................... 59

API Version 2020-05-31

iii
<table>
<thead>
<tr>
<th>Function</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>DeleteFieldLevelEncryptionProfile</td>
<td>111</td>
</tr>
<tr>
<td>Request Syntax</td>
<td>111</td>
</tr>
<tr>
<td>URI Request Parameters</td>
<td>111</td>
</tr>
<tr>
<td>Request Body</td>
<td>111</td>
</tr>
<tr>
<td>Response Syntax</td>
<td>111</td>
</tr>
<tr>
<td>Response Elements</td>
<td>111</td>
</tr>
<tr>
<td>Errors</td>
<td>111</td>
</tr>
<tr>
<td>See Also</td>
<td>112</td>
</tr>
<tr>
<td>DeleteFunction</td>
<td>113</td>
</tr>
<tr>
<td>Request Syntax</td>
<td>113</td>
</tr>
<tr>
<td>URI Request Parameters</td>
<td>113</td>
</tr>
<tr>
<td>Request Body</td>
<td>113</td>
</tr>
<tr>
<td>Response Syntax</td>
<td>113</td>
</tr>
<tr>
<td>Response Elements</td>
<td>113</td>
</tr>
<tr>
<td>Errors</td>
<td>113</td>
</tr>
<tr>
<td>See Also</td>
<td>114</td>
</tr>
<tr>
<td>DeleteKeyGroup</td>
<td>115</td>
</tr>
<tr>
<td>Request Syntax</td>
<td>115</td>
</tr>
<tr>
<td>URI Request Parameters</td>
<td>115</td>
</tr>
<tr>
<td>Request Body</td>
<td>115</td>
</tr>
<tr>
<td>Response Syntax</td>
<td>115</td>
</tr>
<tr>
<td>Response Elements</td>
<td>115</td>
</tr>
<tr>
<td>Errors</td>
<td>115</td>
</tr>
<tr>
<td>See Also</td>
<td>116</td>
</tr>
<tr>
<td>DeleteMonitoringSubscription</td>
<td>117</td>
</tr>
<tr>
<td>Request Syntax</td>
<td>117</td>
</tr>
<tr>
<td>URI Request Parameters</td>
<td>117</td>
</tr>
<tr>
<td>Request Body</td>
<td>117</td>
</tr>
<tr>
<td>Response Syntax</td>
<td>117</td>
</tr>
<tr>
<td>Response Elements</td>
<td>117</td>
</tr>
<tr>
<td>Errors</td>
<td>117</td>
</tr>
<tr>
<td>See Also</td>
<td>118</td>
</tr>
<tr>
<td>DeleteOriginRequestPolicy</td>
<td>119</td>
</tr>
<tr>
<td>Request Syntax</td>
<td>119</td>
</tr>
<tr>
<td>URI Request Parameters</td>
<td>119</td>
</tr>
<tr>
<td>Request Body</td>
<td>119</td>
</tr>
<tr>
<td>Response Syntax</td>
<td>119</td>
</tr>
<tr>
<td>Response Elements</td>
<td>119</td>
</tr>
<tr>
<td>Errors</td>
<td>119</td>
</tr>
<tr>
<td>See Also</td>
<td>120</td>
</tr>
<tr>
<td>DeletePublicKey</td>
<td>121</td>
</tr>
<tr>
<td>Request Syntax</td>
<td>121</td>
</tr>
<tr>
<td>URI Request Parameters</td>
<td>121</td>
</tr>
<tr>
<td>Request Body</td>
<td>121</td>
</tr>
<tr>
<td>Response Syntax</td>
<td>121</td>
</tr>
<tr>
<td>Response Elements</td>
<td>121</td>
</tr>
<tr>
<td>Errors</td>
<td>121</td>
</tr>
<tr>
<td>See Also</td>
<td>122</td>
</tr>
<tr>
<td>DeleteRealtimeLogConfig</td>
<td>123</td>
</tr>
<tr>
<td>Request Syntax</td>
<td>123</td>
</tr>
<tr>
<td>URI Request Parameters</td>
<td>123</td>
</tr>
<tr>
<td>Request Body</td>
<td>123</td>
</tr>
<tr>
<td>Response Syntax</td>
<td>123</td>
</tr>
<tr>
<td>Response Elements</td>
<td>124</td>
</tr>
<tr>
<td>Errors</td>
<td>124</td>
</tr>
<tr>
<td>Request Syntax</td>
<td>173</td>
</tr>
<tr>
<td>----------------</td>
<td>-----</td>
</tr>
<tr>
<td>URI Request Parameters</td>
<td>173</td>
</tr>
<tr>
<td>Request Body</td>
<td>173</td>
</tr>
<tr>
<td>Response Syntax</td>
<td>173</td>
</tr>
<tr>
<td>Response Elements</td>
<td>173</td>
</tr>
<tr>
<td>Errors</td>
<td>174</td>
</tr>
<tr>
<td>See Also</td>
<td>174</td>
</tr>
<tr>
<td>GetKeyGroup</td>
<td>176</td>
</tr>
<tr>
<td>Request Syntax</td>
<td>176</td>
</tr>
<tr>
<td>URI Request Parameters</td>
<td>176</td>
</tr>
<tr>
<td>Request Body</td>
<td>176</td>
</tr>
<tr>
<td>Response Syntax</td>
<td>176</td>
</tr>
<tr>
<td>Response Elements</td>
<td>176</td>
</tr>
<tr>
<td>Errors</td>
<td>177</td>
</tr>
<tr>
<td>See Also</td>
<td>177</td>
</tr>
<tr>
<td>GetKeyGroupConfig</td>
<td>178</td>
</tr>
<tr>
<td>Request Syntax</td>
<td>178</td>
</tr>
<tr>
<td>URI Request Parameters</td>
<td>178</td>
</tr>
<tr>
<td>Request Body</td>
<td>178</td>
</tr>
<tr>
<td>Response Syntax</td>
<td>178</td>
</tr>
<tr>
<td>Response Elements</td>
<td>178</td>
</tr>
<tr>
<td>Errors</td>
<td>179</td>
</tr>
<tr>
<td>See Also</td>
<td>179</td>
</tr>
<tr>
<td>GetMonitoringSubscription</td>
<td>180</td>
</tr>
<tr>
<td>Request Syntax</td>
<td>180</td>
</tr>
<tr>
<td>URI Request Parameters</td>
<td>180</td>
</tr>
<tr>
<td>Request Body</td>
<td>180</td>
</tr>
<tr>
<td>Response Syntax</td>
<td>180</td>
</tr>
<tr>
<td>Response Elements</td>
<td>180</td>
</tr>
<tr>
<td>Errors</td>
<td>180</td>
</tr>
<tr>
<td>See Also</td>
<td>181</td>
</tr>
<tr>
<td>GetOriginRequestPolicy</td>
<td>182</td>
</tr>
<tr>
<td>Request Syntax</td>
<td>182</td>
</tr>
<tr>
<td>URI Request Parameters</td>
<td>182</td>
</tr>
<tr>
<td>Request Body</td>
<td>182</td>
</tr>
<tr>
<td>Response Syntax</td>
<td>182</td>
</tr>
<tr>
<td>Response Elements</td>
<td>183</td>
</tr>
<tr>
<td>Errors</td>
<td>183</td>
</tr>
<tr>
<td>See Also</td>
<td>184</td>
</tr>
<tr>
<td>GetOriginRequestPolicyConfig</td>
<td>185</td>
</tr>
<tr>
<td>Request Syntax</td>
<td>185</td>
</tr>
<tr>
<td>URI Request Parameters</td>
<td>185</td>
</tr>
<tr>
<td>Request Body</td>
<td>185</td>
</tr>
<tr>
<td>Response Syntax</td>
<td>185</td>
</tr>
<tr>
<td>Response Elements</td>
<td>186</td>
</tr>
<tr>
<td>Errors</td>
<td>186</td>
</tr>
<tr>
<td>See Also</td>
<td>187</td>
</tr>
<tr>
<td>GetPublicKey</td>
<td>188</td>
</tr>
<tr>
<td>Request Syntax</td>
<td>188</td>
</tr>
<tr>
<td>URI Request Parameters</td>
<td>188</td>
</tr>
<tr>
<td>Request Body</td>
<td>188</td>
</tr>
<tr>
<td>Response Syntax</td>
<td>188</td>
</tr>
<tr>
<td>Response Elements</td>
<td>188</td>
</tr>
<tr>
<td>Errors</td>
<td>189</td>
</tr>
<tr>
<td>See Also</td>
<td>189</td>
</tr>
<tr>
<td>GetPublicKeyConfig</td>
<td>190</td>
</tr>
<tr>
<td>Request Syntax</td>
<td>190</td>
</tr>
<tr>
<td>Function</td>
<td>Page</td>
</tr>
<tr>
<td>----------------------------------</td>
<td>------</td>
</tr>
<tr>
<td>PublishFunction</td>
<td>284</td>
</tr>
<tr>
<td>ListTagsForResource</td>
<td>282</td>
</tr>
<tr>
<td>ListStreamingDistributions</td>
<td>279</td>
</tr>
<tr>
<td>ListRealtimeLogConfigs</td>
<td>272</td>
</tr>
<tr>
<td>ListResponseHeadersPolicies</td>
<td>275</td>
</tr>
<tr>
<td>ListPublicKeys</td>
<td>270</td>
</tr>
<tr>
<td>Request Syntax</td>
<td>270</td>
</tr>
<tr>
<td>URI Request Parameters</td>
<td>270</td>
</tr>
<tr>
<td>Request Body</td>
<td>270</td>
</tr>
<tr>
<td>Response Syntax</td>
<td>270</td>
</tr>
<tr>
<td>Response Elements</td>
<td>270</td>
</tr>
<tr>
<td>Errors</td>
<td>271</td>
</tr>
<tr>
<td>See Also</td>
<td>271</td>
</tr>
<tr>
<td>Request Syntax</td>
<td>275</td>
</tr>
<tr>
<td>URI Request Parameters</td>
<td>275</td>
</tr>
<tr>
<td>Request Body</td>
<td>275</td>
</tr>
<tr>
<td>Response Syntax</td>
<td>275</td>
</tr>
<tr>
<td>Response Elements</td>
<td>277</td>
</tr>
<tr>
<td>Errors</td>
<td>277</td>
</tr>
<tr>
<td>See Also</td>
<td>278</td>
</tr>
<tr>
<td>Request Syntax</td>
<td>279</td>
</tr>
<tr>
<td>URI Request Parameters</td>
<td>279</td>
</tr>
<tr>
<td>Request Body</td>
<td>279</td>
</tr>
<tr>
<td>Response Syntax</td>
<td>279</td>
</tr>
<tr>
<td>Response Elements</td>
<td>280</td>
</tr>
<tr>
<td>Errors</td>
<td>280</td>
</tr>
<tr>
<td>See Also</td>
<td>281</td>
</tr>
<tr>
<td>Request Syntax</td>
<td>282</td>
</tr>
<tr>
<td>URI Request Parameters</td>
<td>282</td>
</tr>
<tr>
<td>Request Body</td>
<td>282</td>
</tr>
<tr>
<td>Response Syntax</td>
<td>282</td>
</tr>
<tr>
<td>Response Elements</td>
<td>282</td>
</tr>
<tr>
<td>Errors</td>
<td>283</td>
</tr>
<tr>
<td>See Also</td>
<td>283</td>
</tr>
<tr>
<td>Request Syntax</td>
<td>284</td>
</tr>
<tr>
<td>URI Request Parameters</td>
<td>284</td>
</tr>
<tr>
<td>Request Body</td>
<td>284</td>
</tr>
<tr>
<td>Response Syntax</td>
<td>284</td>
</tr>
<tr>
<td>Response Elements</td>
<td>285</td>
</tr>
<tr>
<td>Errors</td>
<td>285</td>
</tr>
<tr>
<td>See Also</td>
<td>286</td>
</tr>
<tr>
<td>Request Syntax</td>
<td>287</td>
</tr>
<tr>
<td>URI Request Parameters</td>
<td>287</td>
</tr>
<tr>
<td>Request Body</td>
<td>287</td>
</tr>
<tr>
<td>Response Syntax</td>
<td>287</td>
</tr>
<tr>
<td>Response Elements</td>
<td>287</td>
</tr>
<tr>
<td>Function</td>
<td>Pages</td>
</tr>
<tr>
<td>-----------------------------------------------</td>
<td>---------</td>
</tr>
<tr>
<td>TestFunction</td>
<td>289</td>
</tr>
<tr>
<td>UpdateCloudFrontOriginAccessIdentity</td>
<td>300</td>
</tr>
<tr>
<td>UpdateDistribution</td>
<td>303</td>
</tr>
<tr>
<td>UpdateFieldLevelEncryptionConfig</td>
<td>325</td>
</tr>
<tr>
<td>UpdateFieldLevelEncryptionProfile</td>
<td>329</td>
</tr>
<tr>
<td>Errors</td>
<td>287</td>
</tr>
<tr>
<td>See Also</td>
<td>288</td>
</tr>
<tr>
<td>URI Request Parameters</td>
<td>289</td>
</tr>
<tr>
<td>Request Syntax</td>
<td>289</td>
</tr>
<tr>
<td>Request Body</td>
<td>289</td>
</tr>
<tr>
<td>Response Syntax</td>
<td>290</td>
</tr>
<tr>
<td>Response Elements</td>
<td>290</td>
</tr>
<tr>
<td>Errors</td>
<td>291</td>
</tr>
<tr>
<td>See Also</td>
<td>291</td>
</tr>
<tr>
<td>UpdateDistribution</td>
<td>293</td>
</tr>
<tr>
<td>URI Request Parameters</td>
<td>293</td>
</tr>
<tr>
<td>Request Syntax</td>
<td>293</td>
</tr>
<tr>
<td>Request Body</td>
<td>293</td>
</tr>
<tr>
<td>Response Syntax</td>
<td>293</td>
</tr>
<tr>
<td>Response Elements</td>
<td>293</td>
</tr>
<tr>
<td>Errors</td>
<td>293</td>
</tr>
<tr>
<td>See Also</td>
<td>294</td>
</tr>
<tr>
<td>UpdateCachePolicy</td>
<td>295</td>
</tr>
<tr>
<td>URI Request Parameters</td>
<td>295</td>
</tr>
<tr>
<td>Request Syntax</td>
<td>295</td>
</tr>
<tr>
<td>Request Body</td>
<td>296</td>
</tr>
<tr>
<td>Response Syntax</td>
<td>297</td>
</tr>
<tr>
<td>Response Elements</td>
<td>297</td>
</tr>
<tr>
<td>Errors</td>
<td>298</td>
</tr>
<tr>
<td>See Also</td>
<td>299</td>
</tr>
<tr>
<td>UpdateDistribution</td>
<td>300</td>
</tr>
<tr>
<td>URI Request Parameters</td>
<td>300</td>
</tr>
<tr>
<td>Request Syntax</td>
<td>300</td>
</tr>
<tr>
<td>Request Body</td>
<td>301</td>
</tr>
<tr>
<td>Response Syntax</td>
<td>301</td>
</tr>
<tr>
<td>Response Elements</td>
<td>301</td>
</tr>
<tr>
<td>Errors</td>
<td>301</td>
</tr>
<tr>
<td>See Also</td>
<td>302</td>
</tr>
<tr>
<td>UpdateCloudFrontOriginAccessIdentity</td>
<td>303</td>
</tr>
<tr>
<td>URI Request Parameters</td>
<td>308</td>
</tr>
<tr>
<td>Request Syntax</td>
<td>308</td>
</tr>
<tr>
<td>Request Body</td>
<td>312</td>
</tr>
<tr>
<td>Response Syntax</td>
<td>317</td>
</tr>
<tr>
<td>Response Elements</td>
<td>318</td>
</tr>
<tr>
<td>Errors</td>
<td>324</td>
</tr>
<tr>
<td>See Also</td>
<td>328</td>
</tr>
<tr>
<td>UpdateFieldLevelEncryptionConfig</td>
<td>325</td>
</tr>
<tr>
<td>URI Request Parameters</td>
<td>325</td>
</tr>
<tr>
<td>Request Syntax</td>
<td>325</td>
</tr>
<tr>
<td>Request Body</td>
<td>326</td>
</tr>
<tr>
<td>Response Syntax</td>
<td>327</td>
</tr>
<tr>
<td>Response Elements</td>
<td>327</td>
</tr>
<tr>
<td>Errors</td>
<td>328</td>
</tr>
<tr>
<td>See Also</td>
<td>328</td>
</tr>
<tr>
<td>UpdateFieldLevelEncryptionProfile</td>
<td>329</td>
</tr>
<tr>
<td>URI Request Parameters</td>
<td>329</td>
</tr>
<tr>
<td>Request Syntax</td>
<td>329</td>
</tr>
<tr>
<td>Request Body</td>
<td>330</td>
</tr>
<tr>
<td>Response Syntax</td>
<td>330</td>
</tr>
<tr>
<td>Response Elements</td>
<td>330</td>
</tr>
<tr>
<td>Errors</td>
<td>331</td>
</tr>
<tr>
<td>See Also</td>
<td>448</td>
</tr>
<tr>
<td>----------</td>
<td>----</td>
</tr>
<tr>
<td>Headers</td>
<td>450</td>
</tr>
<tr>
<td>Contents</td>
<td>450</td>
</tr>
<tr>
<td>See Also</td>
<td>450</td>
</tr>
<tr>
<td>Invalidation</td>
<td>451</td>
</tr>
<tr>
<td>Contents</td>
<td>451</td>
</tr>
<tr>
<td>See Also</td>
<td>451</td>
</tr>
<tr>
<td>InvalidationBatch</td>
<td>452</td>
</tr>
<tr>
<td>Contents</td>
<td>452</td>
</tr>
<tr>
<td>See Also</td>
<td>452</td>
</tr>
<tr>
<td>InvalidationList</td>
<td>453</td>
</tr>
<tr>
<td>Contents</td>
<td>453</td>
</tr>
<tr>
<td>See Also</td>
<td>453</td>
</tr>
<tr>
<td>InvalidationSummary</td>
<td>455</td>
</tr>
<tr>
<td>Contents</td>
<td>455</td>
</tr>
<tr>
<td>See Also</td>
<td>455</td>
</tr>
<tr>
<td>KeyGroup</td>
<td>456</td>
</tr>
<tr>
<td>Contents</td>
<td>456</td>
</tr>
<tr>
<td>See Also</td>
<td>456</td>
</tr>
<tr>
<td>KeyGroupConfig</td>
<td>457</td>
</tr>
<tr>
<td>Contents</td>
<td>457</td>
</tr>
<tr>
<td>See Also</td>
<td>457</td>
</tr>
<tr>
<td>KeyGroupList</td>
<td>458</td>
</tr>
<tr>
<td>Contents</td>
<td>458</td>
</tr>
<tr>
<td>See Also</td>
<td>458</td>
</tr>
<tr>
<td>KeyGroupSummary</td>
<td>459</td>
</tr>
<tr>
<td>Contents</td>
<td>459</td>
</tr>
<tr>
<td>See Also</td>
<td>459</td>
</tr>
<tr>
<td>KeyPairIds</td>
<td>460</td>
</tr>
<tr>
<td>Contents</td>
<td>460</td>
</tr>
<tr>
<td>See Also</td>
<td>460</td>
</tr>
<tr>
<td>KGKeyPairIds</td>
<td>461</td>
</tr>
<tr>
<td>Contents</td>
<td>461</td>
</tr>
<tr>
<td>See Also</td>
<td>461</td>
</tr>
<tr>
<td>KinesisStreamConfig</td>
<td>462</td>
</tr>
<tr>
<td>Contents</td>
<td>462</td>
</tr>
<tr>
<td>See Also</td>
<td>462</td>
</tr>
<tr>
<td>LambdaFunctionAssociation</td>
<td>463</td>
</tr>
<tr>
<td>Contents</td>
<td>463</td>
</tr>
<tr>
<td>See Also</td>
<td>463</td>
</tr>
<tr>
<td>LambdaFunctionAssociations</td>
<td>465</td>
</tr>
<tr>
<td>Contents</td>
<td>465</td>
</tr>
<tr>
<td>See Also</td>
<td>465</td>
</tr>
<tr>
<td>LoggingConfig</td>
<td>466</td>
</tr>
<tr>
<td>Contents</td>
<td>466</td>
</tr>
<tr>
<td>See Also</td>
<td>466</td>
</tr>
<tr>
<td>MonitoringSubscription</td>
<td>468</td>
</tr>
<tr>
<td>Contents</td>
<td>468</td>
</tr>
<tr>
<td>See Also</td>
<td>468</td>
</tr>
<tr>
<td>Origin</td>
<td>469</td>
</tr>
<tr>
<td>Contents</td>
<td>469</td>
</tr>
<tr>
<td>See Also</td>
<td>470</td>
</tr>
<tr>
<td>OriginCustomHeaderValue</td>
<td>472</td>
</tr>
<tr>
<td>Contents</td>
<td>472</td>
</tr>
<tr>
<td>See Also</td>
<td>472</td>
</tr>
<tr>
<td>OriginGroup</td>
<td>473</td>
</tr>
<tr>
<td>Contents</td>
<td>473</td>
</tr>
<tr>
<td>Contents</td>
<td>Page</td>
</tr>
<tr>
<td>-------------------------------------------------------------------------</td>
<td>------</td>
</tr>
<tr>
<td>OriginGroupFailoverCriteria</td>
<td>474</td>
</tr>
<tr>
<td>Contents</td>
<td>474</td>
</tr>
<tr>
<td>See Also</td>
<td>474</td>
</tr>
<tr>
<td>OriginGroupMember</td>
<td>475</td>
</tr>
<tr>
<td>Contents</td>
<td>475</td>
</tr>
<tr>
<td>See Also</td>
<td>475</td>
</tr>
<tr>
<td>OriginGroupMembers</td>
<td>476</td>
</tr>
<tr>
<td>Contents</td>
<td>476</td>
</tr>
<tr>
<td>See Also</td>
<td>476</td>
</tr>
<tr>
<td>OriginGroups</td>
<td>477</td>
</tr>
<tr>
<td>Contents</td>
<td>477</td>
</tr>
<tr>
<td>See Also</td>
<td>477</td>
</tr>
<tr>
<td>OriginRequestPolicy</td>
<td>478</td>
</tr>
<tr>
<td>Contents</td>
<td>478</td>
</tr>
<tr>
<td>See Also</td>
<td>478</td>
</tr>
<tr>
<td>OriginRequestPolicyConfig</td>
<td>479</td>
</tr>
<tr>
<td>Contents</td>
<td>479</td>
</tr>
<tr>
<td>See Also</td>
<td>480</td>
</tr>
<tr>
<td>OriginRequestPolicyCookiesConfig</td>
<td>481</td>
</tr>
<tr>
<td>Contents</td>
<td>481</td>
</tr>
<tr>
<td>See Also</td>
<td>481</td>
</tr>
<tr>
<td>OriginRequestPolicyHeadersConfig</td>
<td>482</td>
</tr>
<tr>
<td>Contents</td>
<td>482</td>
</tr>
<tr>
<td>See Also</td>
<td>482</td>
</tr>
<tr>
<td>OriginRequestPolicyList</td>
<td>483</td>
</tr>
<tr>
<td>Contents</td>
<td>483</td>
</tr>
<tr>
<td>See Also</td>
<td>483</td>
</tr>
<tr>
<td>OriginRequestPolicyQueryStringsConfig</td>
<td>484</td>
</tr>
<tr>
<td>Contents</td>
<td>484</td>
</tr>
<tr>
<td>See Also</td>
<td>484</td>
</tr>
<tr>
<td>OriginRequestPolicySummary</td>
<td>485</td>
</tr>
<tr>
<td>Contents</td>
<td>485</td>
</tr>
<tr>
<td>See Also</td>
<td>485</td>
</tr>
<tr>
<td>Origins</td>
<td>486</td>
</tr>
<tr>
<td>Contents</td>
<td>486</td>
</tr>
<tr>
<td>See Also</td>
<td>486</td>
</tr>
<tr>
<td>OriginShield</td>
<td>487</td>
</tr>
<tr>
<td>Contents</td>
<td>487</td>
</tr>
<tr>
<td>See Also</td>
<td>487</td>
</tr>
<tr>
<td>OriginSslProtocols</td>
<td>488</td>
</tr>
<tr>
<td>Contents</td>
<td>488</td>
</tr>
<tr>
<td>See Also</td>
<td>488</td>
</tr>
<tr>
<td>ParametersInCacheKeyAndForwardedToOrigin</td>
<td>489</td>
</tr>
<tr>
<td>Contents</td>
<td>489</td>
</tr>
<tr>
<td>See Also</td>
<td>490</td>
</tr>
<tr>
<td>Paths</td>
<td>491</td>
</tr>
<tr>
<td>Contents</td>
<td>491</td>
</tr>
<tr>
<td>See Also</td>
<td>491</td>
</tr>
<tr>
<td>PublicKey</td>
<td>492</td>
</tr>
<tr>
<td>Contents</td>
<td>492</td>
</tr>
<tr>
<td>See Also</td>
<td>492</td>
</tr>
<tr>
<td>PublicKeyConfig</td>
<td>493</td>
</tr>
<tr>
<td>Contents</td>
<td>493</td>
</tr>
<tr>
<td>See Also</td>
<td>493</td>
</tr>
<tr>
<td>PublicKeyList</td>
<td>494</td>
</tr>
<tr>
<td>Contents</td>
<td>494</td>
</tr>
</tbody>
</table>
See Also ........................................................................................................................ 516
ResponseHeadersPolicyCustomHeadersConfig ................................................................. 517
Contents ......................................................................................................................... 517
See Also ......................................................................................................................... 517
ResponseHeadersPolicyFrameOptions ............................................................................. 518
Contents ......................................................................................................................... 518
See Also ......................................................................................................................... 518
ResponseHeadersPolicyList ............................................................................................. 519
Contents ......................................................................................................................... 519
See Also ......................................................................................................................... 519
ResponseHeadersPolicyReferrerPolicy ......................................................................... 520
Contents ......................................................................................................................... 520
See Also ......................................................................................................................... 520
ResponseHeadersPolicySecurityHeadersConfig ............................................................. 521
Contents ......................................................................................................................... 521
See Also ......................................................................................................................... 522
ResponseHeadersPolicyServerTimingHeadersConfig ...................................................... 523
Contents ......................................................................................................................... 523
See Also ......................................................................................................................... 523
ResponseHeadersPolicyStrictTransportSecurity ............................................................ 524
Contents ......................................................................................................................... 524
See Also ......................................................................................................................... 524
ResponseHeadersPolicySummary .................................................................................... 525
Contents ......................................................................................................................... 525
See Also ......................................................................................................................... 525
ResponseHeadersPolicyXSSProtection ............................................................................ 526
Contents ......................................................................................................................... 526
See Also ......................................................................................................................... 526
Restrictions ..................................................................................................................... 528
Contents ......................................................................................................................... 528
See Also ......................................................................................................................... 528
S3Origin .......................................................................................................................... 529
Contents ......................................................................................................................... 529
See Also ......................................................................................................................... 529
S3OriginConfig .............................................................................................................. 530
Contents ......................................................................................................................... 530
See Also ......................................................................................................................... 530
Signer ............................................................................................................................... 531
Contents ......................................................................................................................... 531
See Also ......................................................................................................................... 531
StatusCodes .................................................................................................................... 532
Contents ......................................................................................................................... 532
See Also ......................................................................................................................... 532
StreamingDistribution .................................................................................................... 533
Contents ......................................................................................................................... 533
See Also ......................................................................................................................... 534
StreamingDistributionConfig ........................................................................................ 535
Contents ......................................................................................................................... 535
See Also ......................................................................................................................... 536
StreamingDistributionConfigWithTags .......................................................................... 537
Contents ......................................................................................................................... 537
See Also ......................................................................................................................... 537
StreamingDistributionList ............................................................................................. 538
Contents ......................................................................................................................... 538
See Also ......................................................................................................................... 538
StreamingDistributionSummary .................................................................................... 540
Contents ......................................................................................................................... 540

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>See Also</td>
<td>541</td>
</tr>
<tr>
<td>StreamingLoggingConfig</td>
<td>542</td>
</tr>
<tr>
<td>Contents</td>
<td>542</td>
</tr>
<tr>
<td>See Also</td>
<td>542</td>
</tr>
<tr>
<td>Tag</td>
<td>543</td>
</tr>
<tr>
<td>Contents</td>
<td>543</td>
</tr>
<tr>
<td>See Also</td>
<td>543</td>
</tr>
<tr>
<td>TagKeys</td>
<td>544</td>
</tr>
<tr>
<td>Contents</td>
<td>544</td>
</tr>
<tr>
<td>See Also</td>
<td>544</td>
</tr>
<tr>
<td>Tags</td>
<td>544</td>
</tr>
<tr>
<td>Contents</td>
<td>545</td>
</tr>
<tr>
<td>See Also</td>
<td>545</td>
</tr>
<tr>
<td>TestResult</td>
<td>546</td>
</tr>
<tr>
<td>Contents</td>
<td>546</td>
</tr>
<tr>
<td>See Also</td>
<td>546</td>
</tr>
<tr>
<td>TrustedKeyGroups</td>
<td>547</td>
</tr>
<tr>
<td>Contents</td>
<td>547</td>
</tr>
<tr>
<td>See Also</td>
<td>547</td>
</tr>
<tr>
<td>TrustedSigners</td>
<td>548</td>
</tr>
<tr>
<td>Contents</td>
<td>548</td>
</tr>
<tr>
<td>See Also</td>
<td>548</td>
</tr>
<tr>
<td>ViewerCertificate</td>
<td>549</td>
</tr>
<tr>
<td>Contents</td>
<td>549</td>
</tr>
<tr>
<td>See Also</td>
<td>552</td>
</tr>
<tr>
<td>Common Parameters</td>
<td>553</td>
</tr>
<tr>
<td>Common Errors</td>
<td>555</td>
</tr>
</tbody>
</table>
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 August 11, 2022.
Actions

The following actions are supported:

- AssociateAlias (p. 5)
- CreateCachePolicy (p. 7)
- CreateCloudFrontOriginAccessIdentity (p. 12)
- CreateDistribution (p. 15)
- CreateDistributionWithTags (p. 37)
- CreateFieldLevelEncryptionConfig (p. 55)
- CreateFieldLevelEncryptionProfile (p. 59)
- CreateFunction (p. 63)
- CreateInvalidation (p. 67)
- CreateKeyGroup (p. 70)
- CreateMonitoringSubscription (p. 73)
- CreateOriginRequestPolicy (p. 75)
- CreatePublicKey (p. 80)
- CreateRealtimeLogConfig (p. 83)
- CreateResponseHeadersPolicy (p. 86)
- CreateStreamingDistribution (p. 92)
- CreateStreamingDistributionWithTags (p. 98)
- DeleteCachePolicy (p. 103)
- DeleteCloudFrontOriginAccessIdentity (p. 105)
- DeleteDistribution (p. 107)
- DeleteFieldLevelEncryptionConfig (p. 109)
- DeleteFieldLevelEncryptionProfile (p. 111)
- DeleteFunction (p. 113)
- DeleteKeyGroup (p. 115)
- DeleteMonitoringSubscription (p. 117)
- DeleteOriginRequestPolicy (p. 119)
- DeletePublicKey (p. 121)
- DeleteRealtimeLogConfig (p. 123)
- DeleteResponseHeadersPolicy (p. 125)
- DeleteStreamingDistribution (p. 127)
- DescribeFunction (p. 130)
- GetCachePolicy (p. 133)
- GetCachePolicyConfig (p. 136)
- GetCloudFrontOriginAccessIdentity (p. 139)
- GetCloudFrontOriginAccessIdentityConfig (p. 141)
- GetDistribution (p. 143)
- GetDistributionConfig (p. 151)
- GetFieldLevelEncryption (p. 160)
- GetFieldLevelEncryptionConfig (p. 163)
- GetFieldLevelEncryptionProfile (p. 166)
• GetFieldLevelEncryptionProfileConfig (p. 169)
• GetFunction (p. 171)
• GetInvalidation (p. 173)
• GetKeyGroup (p. 176)
• GetKeyGroupConfig (p. 178)
• GetMonitoringSubscription (p. 180)
• GetOriginRequestPolicy (p. 182)
• GetOriginRequestPolicyConfig (p. 185)
• GetPublicKey (p. 188)
• GetPublicKeyConfig (p. 190)
• GetRealtimeLogConfig (p. 192)
• GetResponseHeadersPolicy (p. 195)
• GetResponseHeadersPolicyConfig (p. 199)
• GetStreamingDistribution (p. 203)
• GetStreamingDistributionConfig (p. 206)
• ListCachePolicies (p. 209)
• ListCloudFrontOriginAccessIdentities (p. 212)
• ListConflictingAliases (p. 215)
• ListDistributions (p. 218)
• ListDistributionsByCachePolicyId (p. 225)
• ListDistributionsByKeyGroup (p. 228)
• ListDistributionsByOriginRequestPolicyId (p. 231)
• ListDistributionsByRealtimeLogConfig (p. 234)
• ListDistributionsByResponseHeadersPolicyId (p. 242)
• ListDistributionsByWebACLId (p. 245)
• ListFieldLevelEncryptionConfigs (p. 252)
• ListFieldLevelEncryptionProfiles (p. 255)
• ListFunctions (p. 258)
• ListInvalidations (p. 261)
• ListKeyGroups (p. 264)
• ListOriginRequestPolicies (p. 267)
• ListPublicKeys (p. 270)
• ListRealtimeLogConfigs (p. 272)
• ListResponseHeadersPolicies (p. 275)
• ListStreamingDistributions (p. 279)
• ListTagsForResource (p. 282)
• PublishFunction (p. 284)
• TagResource (p. 287)
• TestFunction (p. 289)
• UntagResource (p. 293)
• UpdateCachePolicy (p. 295)
• UpdateCloudFrontOriginAccessIdentity (p. 300)
• UpdateDistribution (p. 303)
• UpdateFieldLevelEncryptionConfig (p. 325)
• UpdateFieldLevelEncryptionProfile (p. 329)
• UpdateFunction (p. 333)
• UpdateKeyGroup (p. 337)
• UpdateOriginRequestPolicy (p. 340)
• UpdatePublicKey (p. 345)
• UpdateRealtimeLogConfig (p. 348)
• UpdateResponseHeadersPolicy (p. 351)
• UpdateStreamingDistribution (p. 357)
AssociateAlias

Associates an alias (also known as a CNAME or an alternate domain name) with a CloudFront distribution.

With this operation you can move an alias that's already in use on a CloudFront distribution to a different distribution in one step. This prevents the downtime that could occur if you first remove the alias from one distribution and then separately add the alias to another distribution.

To use this operation to associate an alias with a distribution, you provide the alias and the ID of the target distribution for the alias. For more information, including how to set up the target distribution, prerequisites that you must complete, and other restrictions, see Moving an alternate domain name to a different distribution in the Amazon CloudFront Developer Guide.

Request Syntax

```
PUT /2020-05-31/distribution/TargetDistributionId/associate-alias?Alias=Alias HTTP/1.1
```

URI Request Parameters

The request uses the following URI parameters.

**Alias (p. 5)**

The alias (also known as a CNAME) to add to the target distribution.

Required: Yes

**TargetDistributionId (p. 5)**

The ID of the distribution that you’re associating the alias with.

Required: Yes

Request Body

The request does not have a request body.

Response Syntax

```
HTTP/1.1 200
```

Response Elements

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

Errors

For information about the errors that are common to all actions, see Common Errors (p. 555).

**AccessDenied**

Access denied.
HTTP Status Code: 403

IllegalUpdate
The update contains modifications that are not allowed.

HTTP Status Code: 400

InvalidArgument
An argument is invalid.

HTTP Status Code: 400

NoSuchDistribution
The specified distribution does not exist.

HTTP Status Code: 404

TooManyDistributionCNAMEs
Your request contains more CNAMEs than are allowed per distribution.

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

Creates a cache policy.

After you create a cache policy, you can attach it to one or more cache behaviors. When it's attached to a cache behavior, the cache policy determines the following:

- The values that CloudFront includes in the cache key. These values can include HTTP headers, cookies, and URL query strings. CloudFront uses the cache key to find an object in its cache that it can return to the viewer.
- The default, minimum, and maximum time to live (TTL) values that you want objects to stay in the CloudFront cache.

The headers, cookies, and query strings that are included in the cache key are automatically included in requests that CloudFront sends to the origin. CloudFront sends a request when it can't find an object in its cache that matches the request's cache key. If you want to send values to the origin but not include them in the cache key, use OriginRequestPolicy.

For more information about cache policies, see Controlling the cache key in the Amazon CloudFront Developer Guide.

Request Syntax

```
POST /2020-05-31/cache-policy HTTP/1.1
<?xml version="1.0" encoding="UTF-8"?>
  <Comment>string</Comment>
  <DefaultTTL>long</DefaultTTL>
  <MaxTTL>long</MaxTTL>
  <MinTTL>long</MinTTL>
  <Name>string</Name>
  <ParametersInCacheKeyAndForwardedToOrigin>
    <CookiesConfig>
      <CookieBehavior>string</CookieBehavior>
      <Cookies>
        <Items>
          <Name>string</Name>
        </Items>
        <Quantity>integer</Quantity>
      </Cookies>
    </CookiesConfig>
    <EnableAcceptEncodingBrotli>boolean</EnableAcceptEncodingBrotli>
    <EnableAcceptEncodingGzip>boolean</EnableAcceptEncodingGzip>
    <HeadersConfig>
      <HeaderBehavior>string</HeaderBehavior>
      <Headers>
        <Items>
          <Name>string</Name>
        </Items>
        <Quantity>integer</Quantity>
      </Headers>
    </HeadersConfig>
    <QueryStringsConfig>
      <QueryStringBehavior>string</QueryStringBehavior>
      <QueryStrings>
        <Items>
          <Name>string</Name>
        </Items>
        <Quantity>integer</Quantity>
      </QueryStrings>
    </QueryStringsConfig>
  </ParametersInCacheKeyAndForwardedToOrigin>
</CachePolicyConfig>
```
URI Request Parameters

The request does not use any URI parameters.

Request Body

The request accepts the following data in XML format.

CachePolicyConfig (p. 7)

Root level tag for the CachePolicyConfig parameters.

Required: Yes

Comment (p. 7)

A comment to describe the cache policy. The comment cannot be longer than 128 characters.

Type: String

Required: No

MaxTTL (p. 7)

The default amount of time, in seconds, that you want objects to stay in the CloudFront cache before CloudFront sends another request to the origin to see if the object has been updated. CloudFront uses this value as the object's time to live (TTL) only when the origin does not send Cache-Control or Expires headers with the object. For more information, see Managing How Long Content Stays in an Edge Cache (Expiration) in the Amazon CloudFront Developer Guide.

The default value for this field is 86400 seconds (one day). If the value of MinTTL is more than 86400 seconds, then the default value for this field is the same as the value of MinTTL.

Type: Long

Required: No

MinTTL (p. 7)

The minimum amount of time, in seconds, that you want objects to stay in the CloudFront cache before CloudFront sends another request to the origin to see if the object has been updated. For
more information, see Managing How Long Content Stays in an Edge Cache (Expiration) in the Amazon CloudFront Developer Guide.

Type: Long
Required: Yes

Name (p. 7)
A unique name to identify the cache policy.
Type: String
Required: Yes

ParametersInCacheKeyAndForwardedToOrigin (p. 7)
The HTTP headers, cookies, and URL query strings to include in the cache key. The values included in the cache key are automatically included in requests that CloudFront sends to the origin.
Type: ParametersInCacheKeyAndForwardedToOrigin (p. 489) object
Required: No

Response Syntax

```xml
HTTP/1.1 201
<?xml version="1.0" encoding="UTF-8"?>
<CachePolicy>
  <CachePolicyConfig>
    <Comment>string</Comment>
    <DefaultTTL>long</DefaultTTL>
    <MaxTTL>long</MaxTTL>
    <MinTTL>long</MinTTL>
    <Name>string</Name>
    <ParametersInCacheKeyAndForwardedToOrigin>
      <CookiesConfig>
        <CookieBehavior>string</CookieBehavior>
        <Cookies>
          <Items>
            <Name>string</Name>
          </Items>
        </Cookies>
      </CookiesConfig>
      <EnableAcceptEncodingBrotli>boolean</EnableAcceptEncodingBrotli>
      <EnableAcceptEncodingGzip>boolean</EnableAcceptEncodingGzip>
      <HeadersConfig>
        <HeaderBehavior>string</HeaderBehavior>
        <Headers>
          <Items>
            <Name>string</Name>
          </Items>
        </Headers>
      </HeadersConfig>
      <QueryStringsConfig>
        <QueryStringBehavior>string</QueryStringBehavior>
        <QueryStrings>
          <Items>
            <Name>string</Name>
          </Items>
        </QueryStrings>
      </QueryStringsConfig>
    </ParametersInCacheKeyAndForwardedToOrigin>
  </CachePolicyConfig>
</CachePolicy>
```
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.

**CachePolicy (p. 9)**

Root level tag for the CachePolicy parameters.

Required: Yes

**CachePolicyConfig (p. 9)**

The cache policy configuration.

Type: CachePolicyConfig (p. 381) object

**Id (p. 9)**

The unique identifier for the cache policy.

Type: String

**LastModifiedTime (p. 9)**

The date and time when the cache policy was last modified.

Type: Timestamp

Errors

For information about the errors that are common to all actions, see Common Errors (p. 555).

**AccessDenied**

Access denied.

HTTP Status Code: 403

**CachePolicyAlreadyExists**

A cache policy with this name already exists. You must provide a unique name. To modify an existing cache policy, use UpdateCachePolicy.

HTTP Status Code: 409

**InconsistentQuantities**

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

HTTP Status Code: 400

**InvalidArgument**

An argument is invalid.
HTTP Status Code: 400

**TooManyCachePolicies**

You have reached the maximum number of cache policies for this AWS account. For more information, see Quotas (formerly known as limits) in the Amazon CloudFront Developer Guide.

HTTP Status Code: 400

**TooManyCookiesInCachePolicy**

The number of cookies in the cache policy exceeds the maximum. For more information, see Quotas (formerly known as limits) in the Amazon CloudFront Developer Guide.

HTTP Status Code: 400

**TooManyHeadersInCachePolicy**

The number of headers in the cache policy exceeds the maximum. For more information, see Quotas (formerly known as limits) in the Amazon CloudFront Developer Guide.

HTTP Status Code: 400

**TooManyQueryStringsInCachePolicy**

The number of query strings in the cache policy exceeds the maximum. For more information, see Quotas (formerly known as limits) in the Amazon CloudFront Developer Guide.

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 V2
- AWS SDK for JavaScript
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3
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 /2020-05-31/origin-access-identity/cloudfront HTTP/1.1
<?xml version="1.0" encoding="UTF-8"?>
  <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. 12)**

Root level tag for the CloudFrontOriginAccessIdentityConfig parameters.

Required: Yes

**CallerReference (p. 12)**

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 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. 12)**

A comment to describe the origin access identity. The comment cannot be longer than 128 characters.

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</S3 CanonicalUserld>
</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. 13)

Root level tag for the CloudFrontOriginAccessIdentity parameters.

Required: Yes

CloudFrontOriginAccessIdentityConfig (p. 13)

The current configuration information for the identity.

Type: CloudFrontOriginAccessIdentityConfig (p. 389) object

Id (p. 13)

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

Type: String

S3CanonicalUserId (p. 13)

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. 555).

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

An 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

TooManyCloudFrontOriginAccessIdsentities

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

Creates a new web distribution. You create a CloudFront distribution to tell CloudFront where you want content to be delivered from, and the details about how to track and manage content delivery. Send a POST request to the `/CloudFront API version/distribution/distribution ID` resource.

**Important**
When you update a distribution, there are more required fields than when you create a distribution. When you update your distribution by using `UpdateDistribution`, follow the steps included in the documentation to get the current configuration and then make your updates. This helps to make sure that you include all of the required fields. To view a summary, see `Required Fields for Create Distribution and Update Distribution` in the *Amazon CloudFront Developer Guide*.

**Request Syntax**

```xml
POST /2020-05-31/distribution HTTP/1.1
<?xml version="1.0" encoding="UTF-8"?>
  <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>
        <CachePolicyId>string</CachePolicyId>
        <Compress>boolean</Compress>
        <DefaultTTL>long</DefaultTTL>
        <FieldLevelEncryptionId>string</FieldLevelEncryptionId>
      </CacheBehavior>
    </Items>
  </CacheBehaviors>
  <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>
  </ForwardedValues>
</DistributionConfig>
```

API Version 2020-05-31
<QueryStringCacheKeys>
  <Items>
    <Name>string</Name>
  </Items>
  <Quantity>integer</Quantity>
</QueryStringCacheKeys>

<ForwardedValues>
  <FunctionAssociations>
    <Items>
      <FunctionAssociation>
        <EventType>string</EventType>
        <FunctionARN>string</FunctionARN>
      </FunctionAssociation>
    </Items>
    <Quantity>integer</Quantity>
  </FunctionAssociations>
  <LambdaFunctionAssociations>
    <Items>
      <LambdaFunctionAssociation>
        <EventType>string</EventType>
        <IncludeBody>boolean</IncludeBody>
        <LambdaFunctionARN>string</LambdaFunctionARN>
      </LambdaFunctionAssociation>
    </Items>
    <Quantity>integer</Quantity>
  </LambdaFunctionAssociations>
  <MaxTTL>long</MaxTTL>
  <MinTTL>long</MinTTL>
  <OriginRequestPolicyId>string</OriginRequestPolicyId>
  <PathPattern>string</PathPattern>
  <RealtimeLogConfigArn>string</RealtimeLogConfigArn>
  <ResponseHeadersPolicyId>string</ResponseHeadersPolicyId>
  <SmoothStreaming>boolean</SmoothStreaming>
  <TargetOriginId>string</TargetOriginId>
  <TrustedKeyGroups>
    <Enabled>boolean</Enabled>
    <Items>
      <KeyGroup>string</KeyGroup>
    </Items>
    <Quantity>integer</Quantity>
  </TrustedKeyGroups>
  <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>
      <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>
  <CachePolicyId>string</CachePolicyId>
  <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>
  <FunctionAssociations>
    <Items>
      <FunctionAssociation>
        <EventType>string</EventType>
        <FunctionARN>string</FunctionARN>
      </FunctionAssociation>
    </Items>
    <Quantity>integer</Quantity>
  </FunctionAssociations>
  <LambdaFunctionAssociations>
    <Items>
      <LambdaFunctionAssociation>
        <EventType>string</EventType>
        <IncludeBody>boolean</IncludeBody>
        <LambdaFunctionARN>string</LambdaFunctionARN>
      </LambdaFunctionAssociation>
    </Items>
    <Quantity>integer</Quantity>
  </LambdaFunctionAssociations>
  <MaxTTL>long</MaxTTL>
  <MinTTL>long</MinTTL>
  <OriginRequestPolicyId>string</OriginRequestPolicyId>
  <RealtimeLogConfigArn>string</RealtimeLogConfigArn>
  <ResponseHeadersPolicyId>string</ResponseHeadersPolicyId>
</DefaultCacheBehavior>
<TargetOriginId>string</TargetOriginId>

<TrustedKeyGroups>
  <Enabled>boolean</Enabled>
  <Items>
    <KeyGroup>string</KeyGroup>
  </Items>
</TrustedKeyGroups>

<TrustedSigners>
  <Enabled>boolean</Enabled>
  <Items>
    <AwsAccountNumber>string</AwsAccountNumber>
  </Items>
</TrustedSigners>

<ViewerProtocolPolicy>string</ViewerProtocolPolicy>

<DefaultCacheBehavior>
  <DefaultRootObject>string</DefaultRootObject>
</DefaultCacheBehavior>

<HttpVersion>string</HttpVersion>

<IsIPV6Enabled>boolean</IsIPV6Enabled>

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

<Origins>
  <Items>
    <Origin>
      <ConnectionAttempts>integer</ConnectionAttempts>
      <ConnectionTimeout>integer</ConnectionTimeout>
      <CustomHeaders>
        <Items>
          <OriginCustomHeader>
            <HeaderName>string</HeaderName>
            <HeaderValue>string</HeaderValue>
          </OriginCustomHeader>
        </Items>
      </CustomHeaders>
    </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.

**DistributionConfig (p. 15)**

Root level tag for the DistributionConfig parameters.

Required: Yes
**Aliases (p. 15)**

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

Type: Aliases (p. 369) object

Required: No

**CacheBehaviors (p. 15)**

A complex type that contains zero or more CacheBehavior elements.

Type: CacheBehaviors (p. 378) object

Required: No

**CallerReference (p. 15)**

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 that you already sent in a previous request to create a distribution, CloudFront returns a DistributionAlreadyExists error.

Type: String

Required: Yes

**Comment (p. 15)**

An optional comment to describe the distribution. The comment cannot be longer than 128 characters.

Type: String

Required: Yes

**CustomErrorResponses (p. 15)**

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. 403) object

Required: No

**DefaultCacheBehavior (p. 15)**

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. 407) object

Required: Yes
DefaultRootObject (p. 15)

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. 15)

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

Type: Boolean

Required: Yes

HttpVersion (p. 15)

(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. 15)

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

API Version 2020-05-31
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 AWS Integration 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 AWS Integration Developer Guide.

If you created a CNAME resource record set, either with Amazon Route 53 AWS Integration 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. 15)

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. 466) object

Required: No

OriginGroups (p. 15)

A complex type that contains information about origin groups for this distribution.

Type: OriginGroups (p. 477) object

Required: No

Origins (p. 15)

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

Type: Origins (p. 486) object

Required: Yes

PriceClass (p. 15)

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 (such as Price Class 100) map to CloudFront regions, see Amazon CloudFront Pricing.

Type: String

Valid Values: PriceClass_100 | PriceClass_200 | PriceClass_All
Required: No

**Restrictions (p. 15)**

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

Type: Restrictions (p. 528) object

Required: No

**ViewerCertificate (p. 15)**

A complex type that determines the distribution's SSL/TLS configuration for communicating with viewers.

Type: ViewerCertificate (p. 549) object

Required: No

**WebACLId (p. 15)**

A unique identifier that specifies the AWS WAF web ACL, if any, to associate with this distribution. To specify a web ACL created using the latest version of AWS WAF, use the ACL ARN, for example arn:aws:wafv2:us-east-1:123456789012:global/webacl/ExampleWebACL/473e64fd-f30b-4765-81a0-62ad96dd167a. To specify a web ACL created using AWS WAF Classic, use the ACL ID, for example 473e64fd-f30b-4765-81a0-62ad96dd167a.

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**

```xml
HTTP/1.1 201
<?xml version="1.0" encoding="UTF-8"?>
<Distribution>
  <ActiveTrustedKeyGroups>
    <Enabled>boolean</Enabled>
    <Items>
      <KeyGroup>
        <KeyGroupId>string</KeyGroupId>
        <KeyPairIds>
          <Items>
            <KeyPairId>string</KeyPairId>
          </Items>
        </KeyPairIds>
      </KeyGroup>
    </Items>
  </ActiveTrustedKeyGroups>
  <ActiveTrustedSigners>
    <Enabled>boolean</Enabled>
    <Items>
      <Signer>
        <AwsAccountNumber>string</AwsAccountNumber>
      </Signer>
    </Items>
  </ActiveTrustedSigners>
</Distribution>
```

API Version 2020-05-31
23
<KeyPairIds>
  <Items>
    <KeyPairId>string</KeyPairId>
  </Items>
  <Quantity>integer</Quantity>
</KeyPairIds>

<Signer>
  <Quantity>integer</Quantity>
</Signer>

<ActiveTrustedSigners>
  <AliasICPRecordals>
    <AliasICPRecordal>
      <CNAME>string</CNAME>
      <ICPRecordalStatus>string</ICPRecordalStatus>
    </AliasICPRecordal>
  </AliasICPRecordals>
  <ARN>string</ARN>
</DistributionConfig>

<Aliases>
  <Items>
    <CNAME>string</CNAME>
  </Items>
  <Quantity>integer</Quantity>
</Aliases>

<CacheBehaviors>
  <Items>
    <Method>string</Method>
    <CachedMethods>
      <Items>
        <Method>string</Method>
      </Items>
      <Quantity>integer</Quantity>
    </CachedMethods>
    <Quantity>integer</Quantity>
  </Items>
  <AllowedMethods>
    <CachePolicyId>string</CachePolicyId>
    <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>
  </AllowedMethods>
</CacheBehaviors>
Amazon CloudFront API Reference
Response Syntax

</ForwardedValues>
<FunctionAssociations>
<Items>
  <FunctionAssociation>
    <EventType>string</EventType>
    <FunctionARN>string</FunctionARN>
  </FunctionAssociation>
</Items>
<Quantity>integer</Quantity>
</FunctionAssociations>
<LambdaFunctionAssociations>
<Items>
  <LambdaFunctionAssociation>
    <EventType>string</EventType>
    <IncludeBody>boolean</IncludeBody>
    <LambdaFunctionARN>string</LambdaFunctionARN>
  </LambdaFunctionAssociation>
</Items>
<Quantity>integer</Quantity>
</LambdaFunctionAssociations>
<MaxTTL>long</MaxTTL>
<MinTTL>long</MinTTL>
<OriginRequestPolicyId>string</OriginRequestPolicyId>
<PathPattern>string</PathPattern>
<RealtimeLogConfigArn>string</RealtimeLogConfigArn>
<ResponseHeadersPolicyId>string</ResponseHeadersPolicyId>
<SmoothStreaming>boolean</SmoothStreaming>
<TargetOriginId>string</TargetOriginId>
<TrustedKeyGroups>
  <Enabled>boolean</Enabled>
  <Items>
    <KeyGroup>string</KeyGroup>
  </Items>
  <Quantity>integer</Quantity>
</TrustedKeyGroups>
<TrustedSigners>
  <Enabled>boolean</Enabled>
  <Items>
    <AwsAccountNumber>string</AwsAccountNumber>
  </Items>
  <Quantity>integer</Quantity>
</TrustedSigners>
<ViewerProtocolPolicy>string</ViewerProtocolPolicy>
</CacheBehavior>
<Quantity>integer</Quantity>
</CacheBehaviors>
<CallerReference>string</CallerReference>
<Comment>string</Comment>
<CustomErrorResponse>
<Items>
  <CustomErrorResponse>
    <ErrorCachingMinTTL>long</ErrorCachingMinTTL>
    <ErrorCode>integer</ErrorCode>
    <ResponseCode>string</ResponseCode>
    <ResponsePagePath>string</ResponsePagePath>
  </CustomErrorResponse>
</Items>
<Quantity>integer</Quantity>
</CustomErrorResponse>
<DefaultCacheBehavior>
<AllowedMethods>
<Items>
  <Method>string</Method>
</Items>
</AllowedMethods>
Amazon CloudFront API Reference
Response Syntax

<Quantity>integer</Quantity>
</CachedMethods>
<Items>
  <Method>string</Method>
</Items>
<Quantity>integer</Quantity>
</AllowedMethods>
<CachePolicyId>string</CachePolicyId>
<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>
<FunctionAssociations>
  <Items>
    <FunctionAssociation>
      <EventType>string</EventType>
      <FunctionARN>string</FunctionARN>
    </FunctionAssociation>
  </Items>
  <Quantity>integer</Quantity>
</FunctionAssociations>
<LambdaFunctionAssociations>
  <Items>
    <LambdaFunctionAssociation>
      <EventType>string</EventType>
      <IncludeBody>boolean</IncludeBody>
      <LambdaFunctionARN>string</LambdaFunctionARN>
    </LambdaFunctionAssociation>
  </Items>
  <Quantity>integer</Quantity>
</LambdaFunctionAssociations>
<MaxTTL>long</MaxTTL>
<MinTTL>long</MinTTL>
<OriginRequestPolicyId>string</OriginRequestPolicyId>
<RealtimeLogConfigArn>string</RealtimeLogConfigArn>
<ResponseHeadersPolicyId>string</ResponseHeadersPolicyId>
<SmoothStreaming>boolean</SmoothStreaming>
<TargetOriginId>string</TargetOriginId>
<TrustedKeyGroups>
  <Enabled>boolean</Enabled>
  <Items>
    <KeyGroup>string</KeyGroup>
  </Items>
</TrustedKeyGroups>
API Version 2020-05-31
26
<Quantity>integer</Quantity>
</TrustedKeyGroups>
<TrustedSigners>
  <Enabled>boolean</Enabled>
  <Items>
    <AwsAccountNumber>string</AwsAccountNumber>
  </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>
<OriginGroups>
  <Items>
    <OriginGroup>
      <FailoverCriteria>
        <StatusCodes>
          <Items>
            <StatusCode>integer</StatusCode>
          </Items>
        </StatusCodes>
      </FailoverCriteria>
      <Id>string</Id>
      <Members>
        <Items>
          <OriginGroupMember>
            <OriginId>string</OriginId>
          </OriginGroupMember>
        </Items>
      </Members>
    </OriginGroup>
  </Items>
</OriginGroups>
<Origins>
  <Items>
    <Origin>
      <ConnectionAttempts>integer</ConnectionAttempts>
      <ConnectionTimeout>integer</ConnectionTimeout>
      <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>
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. 23)

Root level tag for the Distribution parameters.

Required: Yes

ActiveTrustedKeyGroups (p. 23)

CloudFront automatically adds this field to the response if you've configured a cache behavior in this distribution to serve private content using key groups. This field contains a list of key groups and
the public keys in each key group that CloudFront can use to verify the signatures of signed URLs or signed cookies.

Type: `ActiveTrustedKeyGroups (p. 367)` object

**ActiveTrustedSigners (p. 23)**

**Important**

We recommend using `TrustedKeyGroups` instead of `TrustedSigners`.

CloudFront automatically adds this field to the response if you've configured a cache behavior in this distribution to serve private content using trusted signers. This field contains a list of AWS account IDs and the active CloudFront key pairs in each account that CloudFront can use to verify the signatures of signed URLs or signed cookies.

Type: `ActiveTrustedSigners (p. 368)` object

**AliasICPRecordals (p. 23)**

AWS services in China customers must file for an Internet Content Provider (ICP) recordal if they want to serve content publicly on an alternate domain name, also known as a CNAME, that they've added to CloudFront. AliasICPRecordal provides the ICP recordal status for CNAMEs associated with distributions.

For more information about ICP recordals, see  [Signup, Accounts, and Credentials in Getting Started with AWS services in China](#).

Type: Array of `AliasICPRecordal (p. 370)` objects

**ARN (p. 23)**

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. 23)**

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

Type: `DistributionConfig (p. 414)` object

**DomainName (p. 23)**

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

Type: String

**Id (p. 23)**

The identifier for the distribution. For example: `EDFDVBD632BHDSS`.

Type: String

**InProgressInvalidationBatches (p. 23)**

The number of invalidation batches currently in progress.

Type: Integer

**LastModifiedTime (p. 23)**

The date and time the distribution was last modified.

Type: Timestamp
Status (p. 23)

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. 555).

AccessDenied

Access denied.

HTTP Status Code: 403

CNAMEAlreadyExists

The CNAME specified is already defined for CloudFront.

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

An 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

An invalid error code was specified.

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
InvalidFunctionAssociation
A CloudFront function association is invalid.

HTTP Status Code: 400
InvalidGeoRestrictionParameter
The specified geo restriction parameter is not valid.

HTTP Status Code: 400
InvalidHeadersForS3Origin
The headers specified are not valid for an Amazon S3 origin.

HTTP Status Code: 400
InvalidLambdaFunctionAssociation
The specified Lambda@Edge function association is invalid.

HTTP Status Code: 400
InvalidLocationCode
The location code specified is not valid.

HTTP Status Code: 400
InvalidMinimumProtocolVersion
The minimum protocol version specified is not valid.

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
The keep alive timeout specified for the origin is not valid.

HTTP Status Code: 400
InvalidOriginReadTimeout
The read timeout specified for the origin is not valid.

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).
**InvalidQueryStringParameters**

The query string parameters specified are not valid.

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**

A response code is not valid.

HTTP Status Code: 400

**InvalidTTLOrder**

The TTL order specified is not valid.

HTTP Status Code: 400

**InvalidViewerCertificate**

A viewer certificate specified is not valid.

HTTP Status Code: 400

**InvalidWebACLId**

A web ACL ID specified is not valid. To specify a web ACL created using the latest version of AWS WAF, use the ACL ARN, for example `arn:aws:wafv2:us-east-1:123456789012:global/webacl/ExampleWebACL/473e64fd-f30b-4765-81a0-62ad96dd167a`. To specify a web ACL created using AWS WAF Classic, use the ACL ID, for example `473e64fd-f30b-4765-81a0-62ad96dd167a`.

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

**NoSuchCachePolicy**

The cache policy 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

**NoSuchOriginRequestPolicy**

The origin request policy does not exist.

HTTP Status Code: 404

**NoSuchRealtimeLogConfig**

The real-time log configuration does not exist.

HTTP Status Code: 404

**NoSuchResponseHeadersPolicy**

The response headers policy does not exist.

HTTP Status Code: 404

**RealtimeLogConfigOwnerMismatch**

The specified real-time log configuration belongs to a different AWS account.

HTTP Status Code: 401

**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

**TooManyDistributionsAssociatedToCachePolicy**

The maximum number of distributions have been associated with the specified cache policy. For more information, see **Quotas** (formerly known as limits) in the *Amazon CloudFront Developer Guide*.

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
TooManyDistributionsAssociatedToKeyGroup

The number of distributions that reference this key group is more than the maximum allowed. For more information, see Quotas (formerly known as limits) in the Amazon CloudFront Developer Guide.

HTTP Status Code: 400

TooManyDistributionsAssociatedToOriginRequestPolicy

The maximum number of distributions have been associated with the specified origin request policy. For more information, see Quotas (formerly known as limits) in the Amazon CloudFront Developer Guide.

HTTP Status Code: 400

TooManyDistributionsAssociatedToResponseHeadersPolicy

The maximum number of distributions have been associated with the specified response headers policy.

For more information, see Quotas (formerly known as limits) in the Amazon CloudFront Developer Guide.

HTTP Status Code: 400

TooManyDistributionsWithFunctionAssociations

You have reached the maximum number of distributions that are associated with a CloudFront function. For more information, see Quotas (formerly known as limits) in the Amazon CloudFront Developer Guide.

HTTP Status Code: 400

TooManyDistributionsWithLambdaAssociations

Processing your request would cause the maximum number of distributions with Lambda@Edge function associations per owner to be exceeded.

HTTP Status Code: 400

TooManyDistributionsWithSingleFunctionARN

The maximum number of distributions have been associated with the specified Lambda@Edge function.

HTTP Status Code: 400

TooManyFunctionAssociations

You have reached the maximum number of CloudFront function associations for this distribution. For more information, see Quotas (formerly known as limits) in the Amazon CloudFront Developer Guide.

HTTP Status Code: 400

TooManyHeadersInForwardedValues

Your request contains too many headers in forwarded values.

HTTP Status Code: 400

TooManyKeyGroupsAssociatedToDistribution

The number of key groups referenced by this distribution is more than the maximum allowed. For more information, see Quotas (formerly known as limits) in the Amazon CloudFront Developer Guide.

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

TooManyOriginCustomHeaders
Your request contains too many origin custom headers.
HTTP Status Code: 400

TooManyOriginGroupsPerDistribution
Processing your request would cause you to exceed the maximum number of origin groups allowed.
HTTP Status Code: 400

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

TooManyQueryStringParameters
Your request contains too many query string parameters.
HTTP Status Code: 400

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

TrustedKeyGroupDoesNotExist
The specified key group does not exist.
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 V2
- AWS SDK for JavaScript
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3
CreateDistributionWithTags

Create a new distribution with tags.

Request Syntax

POST /2020-05-31/distribution?WithTags HTTP/1.1
<?xml version="1.0" encoding="UTF-8"?>
  <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>
          <CachePolicyId>string</CachePolicyId>
          <Compress>boolean</Compress>
          <DefaultTTL>long</DefaultTTL>
          <FieldLevelEncryptionId>string</FieldLevelEncryptionId>
          <ForwardedValues>
            <Cookies>
              <Forward>string</Forward>
            </Cookies>
          </ForwardedValues>
          <FunctionAssociations>
            <Items>
              <FunctionAssociation>
                <EventType>string</EventType>
              </FunctionAssociation>
            </Items>
          </FunctionAssociations>
        </CacheBehavior>
      </Items>
    </CacheBehaviors>
    <ForwardedValues>
      <Cookies>
        <Forward>string</Forward>
      </Cookies>
    </ForwardedValues>
    <Headers>
      <Items>
        <Name>string</Name>
      </Items>
      <Quantity>integer</Quantity>
    </Headers>
    <QueryString>boolean</QueryString>
    <QueryStringCacheKeys>
      <Items>
        <Name>string</Name>
      </Items>
      <Quantity>integer</Quantity>
    </QueryStringCacheKeys>
    <ForwardedValues>
      <FunctionAssociations>
        <Items>
          <FunctionAssociation>
            <EventType>string</EventType>
          </FunctionAssociation>
        </Items>
      </FunctionAssociations>
    </ForwardedValues>
  </DistributionConfig>
</DistributionConfigWithTags>
<FunctionARN>string</FunctionARN>
</FunctionAssociation>
</Items>
<Quantity>integer</Quantity>
</FunctionAssociations>
<LambdaFunctionAssociations>
<Items>
<LambdaFunctionAssociation>
<EventType>string</EventType>
<IncludeBody>boolean</IncludeBody>
<LambdaFunctionARN>string</LambdaFunctionARN>
</LambdaFunctionAssociation>
</Items>
<Quantity>integer</Quantity>
</LambdaFunctionAssociations>
<MaxTTL>long</MaxTTL>
<MinTTL>long</MinTTL>
<OriginRequestPolicyId>string</OriginRequestPolicyId>
<PathPattern>string</PathPattern>
<RealtimeLogConfigArn>string</RealtimeLogConfigArn>
<ResponseHeadersPolicyId>string</ResponseHeadersPolicyId>
<SmoothStreaming>boolean</SmoothStreaming>
<TargetOriginId>string</TargetOriginId>
<TrustedKeyGroups>
<Items>
<KeyGroup>string</KeyGroup>
</Items>
<Quantity>integer</Quantity>
</TrustedKeyGroups>
<TrustedSigners>
<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>
<ResponsePagePath>string</ResponsePagePath>
</CustomErrorResponse>
</Items>
<Quantity>integer</Quantity>
</CustomErrorResponses>
<DefaultCacheBehavior>
<AllowedMethods>
<Items>
<Method>string</Method>
</Items>
<Quantity>integer</Quantity>
</AllowedMethods>
<CachedMethods>
<Items>
<Method>string</Method>
</Items>
</CachedMethods>
<Items>
</Method>string</Method>
</Items>
</DefaultCacheBehavior>
</Items>
<Quantity>integer</Quantity>
</CacheBehaviors>

Amazon CloudFront API Reference
Request Syntax

API Version 2020-05-31
38
<Quantity>integer</Quantity>
</AllowedMethods>
<CachePolicyId>string</CachePolicyId>
<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>
  </Headers>
  <QueryString>boolean</QueryString>
  <QueryStringCacheKeys>
    <Items>
      <Name>string</Name>
    </Items>
  </QueryStringCacheKeys>
</ForwardedValues>
<FunctionAssociations>
  <Items>
    <FunctionAssociation>
      <EventType>string</EventType>
      <FunctionARN>string</FunctionARN>
    </FunctionAssociation>
  </Items>
</FunctionAssociations>
</LambdaFunctionAssociations>
<MaxTTL>long</MaxTTL>
<MinTTL>long</MinTTL>
-OriginRequestPolicyId>string</OriginRequestPolicyId>
<RealtimeLogConfigArn>string</RealtimeLogConfigArn>
<ResponseHeadersPolicyId>string</ResponseHeadersPolicyId>
<SmoothStreaming>boolean</SmoothStreaming>
</TargetOriginId>
<TrustedKeyGroups>
  <Enabled>boolean</Enabled>
  <Items>
    <KeyGroup>string</KeyGroup>
  </Items>
</TrustedKeyGroups>
<TrustedSigners>
  <Enabled>boolean</Enabled>
  <Items>
<Items>
  <OriginGroup>
    <FailoverCriteria>
      <StatusCodes>
        <Items>
          <StatusCode>integer</StatusCode>
        </Items>
        <Quantity>integer</Quantity>
      </StatusCodes>
    </FailoverCriteria>
    <Id>string</Id>
    <Members>
      <Items>
        <OriginGroupMember>
          <OriginId>string</OriginId>
        </OriginGroupMember>
      </Items>
      <Quantity>integer</Quantity>
    </Members>
  </OriginGroup>
</Items>
</OriginGroups>
</Origins>
</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>
URI Request Parameters

The request does not use any URI parameters.

Request Body

The request accepts the following data in XML format.

**DistributionConfigWithTags (p. 37)**

Root level tag for the DistributionConfigWithTags parameters.

Required: Yes

**DistributionConfig (p. 37)**

A distribution configuration.
Type: DistributionConfig (p. 414) object

Required: Yes

**Tags (p. 37)**

A complex type that contains zero or more Tag elements.

Type: Tags (p. 545) object

Required: Yes

## Response Syntax

```
HTTP/1.1 201
<?xml version="1.0" encoding="UTF-8"?>
<Distribution>
  <ActiveTrustedKeyGroups>
    <Enabled>boolean</Enabled>
    <Items>
      <KeyGroup>
        <KeyGroupId>string</KeyGroupId>
        <KeyPairIds>
          <Items>
            <KeyId>string</KeyId>
            <Quantity>integer</Quantity>
          </Items>
          <Quantity>integer</Quantity>
        </KeyPairIds>
      </KeyGroup>
    </Items>
    <Quantity>integer</Quantity>
  </ActiveTrustedKeyGroups>
  <ActiveTrustedSigners>
    <Enabled>boolean</Enabled>
    <Items>
      <Signer>
        <AwsAccountNumber>string</AwsAccountNumber>
        <KeyPairIds>
          <Items>
            <KeyId>string</KeyId>
            <Quantity>integer</Quantity>
          </Items>
          <Quantity>integer</Quantity>
        </KeyPairIds>
      </Signer>
    </Items>
    <Quantity>integer</Quantity>
  </ActiveTrustedSigners>
  <AliasICPRecordals>
    <AliasICPRecordal>
      <CNAME>string</CNAME>
      <ICPRecordalStatus>string</ICPRecordalStatus>
    </AliasICPRecordal>
  </AliasICPRecordals>
  <ARN>string</ARN>
  <DistributionConfig>
    <Aliases>
      <Items>
        <CNAME>string</CNAME>
      </Items>
      <Quantity>integer</Quantity>
    </Aliases>
    <CacheBehaviors>
      <Items>
```

API Version 2020-05-31

42
<CacheBehavior>
  <AllowedMethods>
    <CachedMethods>
      <Items>
        <Method>string</Method>
      </Items>
      <Quantity>integer</Quantity>
    </CachedMethods>
    <Items>
      <Method>string</Method>
    </Items>
    <Quantity>integer</Quantity>
  </AllowedMethods>
  <CachePolicyId>string</CachePolicyId>
  <Compress>boolean</Compress>
  <DefaultTTL>long</DefaultTTL>
  <FieldLevelEncryptionId>string</FieldLevelEncryptionId>
  <ForwardedValues>
    <Cookies>
      <Forward>string</Forward>
      <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>
    </Cookies>
    <FunctionAssociations>
      <Items>
        <FunctionAssociation>
          <EventType>string</EventType>
          <FunctionARN>string</FunctionARN>
        </FunctionAssociation>
      </Items>
      <Quantity>integer</Quantity>
    </FunctionAssociations>
    <LambdaFunctionAssociations>
      <Items>
        <LambdaFunctionAssociation>
          <EventType>string</EventType>
          <IncludeBody>boolean</IncludeBody>
          <LambdaFunctionARN>string</LambdaFunctionARN>
        </LambdaFunctionAssociation>
      </Items>
      <Quantity>integer</Quantity>
    </LambdaFunctionAssociations>
    <MaxTTL>long</MaxTTL>
    <MinTTL>long</MinTTL>
    <OriginRequestPolicyId>string</OriginRequestPolicyId>
    <PathPattern>string</PathPattern>
    <RealtimeLogConfigArn>string</RealtimeLogConfigArn>
    <ResponseHeadersPolicyId>string</ResponseHeadersPolicyId>
  </ForwardedValues>
</CacheBehavior>

API Version 2020-05-31

43
<SmoothStreaming>boolean</SmoothStreaming>
<TargetOriginId>string</TargetOriginId>

<TrustedKeyGroups>
  <Enabled>boolean</Enabled>
  <Items>
    <KeyGroup>string</KeyGroup>
  </Items>
</TrustedKeyGroups>

<TrustedSigners>
  <Enabled>boolean</Enabled>
  <Items>
    <AwsAccountNumber>string</AwsAccountNumber>
  </Items>
  <Quantity>integer</Quantity>
</TrustedSigners>

<ViewerProtocolPolicy>string</ViewerProtocolPolicy>
</CacheBehavior>

<CallerReference>string</CallerReference>
<Comment>string</Comment>

<CustomErrorResponses>
  <Items>
    <CustomErrorResponse>
      <ErrorCachingMinTTL>long</ErrorCachingMinTTL>
      <ErrorCode>integer</ErrorCode>
      <ResponseCode>string</ResponseCode>
      <ResponsePagePath>string</ResponsePagePath>
    </CustomErrorResponse>
    <Quantity>integer</Quantity>
  </Items>
</CustomErrorResponses>

<DefaultCacheBehavior>
  <AllowedMethods>
    <CachedMethods>
      <Method>string</Method>
      <Items>
        <Quantity>integer</Quantity>
      </Items>
      <Method>string</Method>
    </CachedMethods>
    <Quantity>integer</Quantity>
  </AllowedMethods>
  <CachePolicyId>string</CachePolicyId>
  <Compress>boolean</Compress>
  <DefaultTTL>long</DefaultTTL>
  <FieldLevelEncryptionId>string</FieldLevelEncryptionId>
</DefaultCacheBehavior>

<ForwardedValues>
  <Cookies>
    <WhitelistedNames>
      <Items>
        <Name>string</Name>
        <Items>
          <Name>string</Name>
        </Items>
        <Quantity>integer</Quantity>
      </WhitelistedNames>
    </Cookies>
    <Headers>
      <Items>
        <Name>string</Name>
      </Items>
      <Quantity>integer</Quantity>
    </Headers>
  </ForwardedValues>
<Items>
  <StatusCode>integer</StatusCode>
</Items>
<Quantity>integer</Quantity>
</StatusCodes>
</FailoverCriteria>
<Id>string</Id>
<Members>
  <Items>
    <OriginGroupMember>
      <OriginId>string</OriginId>
    </OriginGroupMember>
  </Items>
  <Quantity>integer</Quantity>
</Members>
</OriginGroup>
<Quantity>integer</Quantity>
</OriginGroups>
<Origins>
  <Items>
    <Origin>
      <ConnectionAttempts>integer</ConnectionAttempts>
      <ConnectionTimeout>integer</ConnectionTimeout>
      <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>
      <OriginShield>
        <Enabled>boolean</Enabled>
        <OriginShieldRegion>string</OriginShieldRegion>
      </OriginShield>
      <S3OriginConfig>
        <OriginAccessIdentity>string</OriginAccessIdentity>
      </S3OriginConfig>
    </Origin>
  </Items>
  <Quantity>integer</Quantity>
</Origins>
<PriceClass>string</PriceClass>
<Restrictions>
  <GeoRestriction>
    <Items>
      <Location>string</Location>
    </Items>
  </GeoRestriction>
  <Items>
</Items>
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. 42)

Root level tag for the Distribution parameters.

Required: Yes

ActiveTrustedKeyGroups (p. 42)

CloudFront automatically adds this field to the response if you've configured a cache behavior in this distribution to serve private content using key groups. This field contains a list of key groups and the public keys in each key group that CloudFront can use to verify the signatures of signed URLs or signed cookies.

Type: ActiveTrustedKeyGroups (p. 367) object

ActiveTrustedSigners (p. 42)

Important

We recommend using TrustedKeyGroups instead of TrustedSigners.

CloudFront automatically adds this field to the response if you've configured a cache behavior in this distribution to serve private content using trusted signers. This field contains a list of AWS account IDs and the active CloudFront key pairs in each account that CloudFront can use to verify the signatures of signed URLs or signed cookies.

Type: ActiveTrustedSigners (p. 368) object

AliasICPRecordals (p. 42)

AWS services in China customers must file for an Internet Content Provider (ICP) recordal if they want to serve content publicly on an alternate domain name, also known as a CNAME, that they've added to CloudFront. AliasICPRecordal provides the ICP recordal status for CNAMEs associated with distributions.

For more information about ICP recordals, see Signup, Accounts, and Credentials in Getting Started with AWS services in China.
Type: Array of AliasICPRecordal (p. 370) objects

**ARN (p. 42)**

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. 42)**

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

Type: DistributionConfig (p. 414) object

**DomainName (p. 42)**

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

Type: String

**Id (p. 42)**

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

Type: String

**InProgressInvalidationBatches (p. 42)**

The number of invalidation batches currently in progress.

Type: Integer

**LastModifiedTime (p. 42)**

The date and time the distribution was last modified.

Type: Timestamp

**Status (p. 42)**

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. 555).

**AccessDenied**

Access denied.

HTTP Status Code: 403

**CNAMEAlreadyExists**

The CNAME specified is already defined for CloudFront.

HTTP Status Code: 409
Amazon CloudFront API Reference
Errors

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
An 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
An invalid error code was specified.
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

InvalidFunctionAssociation
A CloudFront function association is invalid.
HTTP Status Code: 400

InvalidGeoRestrictionParameter
The specified geo restriction parameter is not valid.
HTTP Status Code: 400

InvalidHeadersForS3Origin
The headers specified are not valid for an Amazon S3 origin.
HTTP Status Code: 400

InvalidLambdaFunctionAssociation
The specified Lambda@Edge function association is invalid.
HTTP Status Code: 400
**InvalidLocationCode**
The location code specified is not valid.

HTTP Status Code: 400
**InvalidMinimumProtocolVersion**
The minimum protocol version specified is not valid.

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**
The keep alive timeout specified for the origin is not valid.

HTTP Status Code: 400
**InvalidOriginReadTimeout**
The read timeout specified for the origin is not valid.

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**
The query string parameters specified are not valid.

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**
A response code is not valid.
Errors

InvalidTagging
The tagging specified is not valid.
HTTP Status Code: 400

InvalidTTLOrder
The TTL order specified is not valid.
HTTP Status Code: 400

InvalidViewerCertificate
A viewer certificate specified is not valid.
HTTP Status Code: 400

InvalidWebACLId
A web ACL ID specified is not valid. To specify a web ACL created using the latest version of AWS WAF, use the ACL ARN, for example `arn:aws:wafv2:us-east-1:123456789012:global/webacl/ExampleWebACL/473e64fd-f30b-4765-81a0-62ad96dd167a`. To specify a web ACL created using AWS WAF Classic, use the ACL ID, for example `473e64fd-f30b-4765-81a0-62ad96dd167a`.
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

NoSuchCachePolicy
The cache policy 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

NoSuchOriginRequestPolicy
The origin request policy does not exist.
HTTP Status Code: 404

NoSuchRealtimeLogConfig
The real-time log configuration does not exist.
HTTP Status Code: 404

NoSuchResponseHeadersPolicy
The response headers policy does not exist.
HTTP Status Code: 404
RealtimeLogConfigOwnerMismatch

The specified real-time log configuration belongs to a different AWS account.

HTTP Status Code: 401

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

TooManyDistributionsAssociatedToCachePolicy

The maximum number of distributions have been associated with the specified cache policy. For more information, see Quotas (formerly known as limits) in the Amazon CloudFront Developer Guide.

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

TooManyDistributionsAssociatedToKeyGroup

The number of distributions that reference this key group is more than the maximum allowed. For more information, see Quotas (formerly known as limits) in the Amazon CloudFront Developer Guide.

HTTP Status Code: 400

TooManyDistributionsAssociatedToOriginRequestPolicy

The maximum number of distributions have been associated with the specified origin request policy. For more information, see Quotas (formerly known as limits) in the Amazon CloudFront Developer Guide.

HTTP Status Code: 400

TooManyDistributionsAssociatedToResponseHeadersPolicy

The maximum number of distributions have been associated with the specified response headers policy.
For more information, see Quotas (formerly known as limits) in the Amazon CloudFront Developer Guide.

HTTP Status Code: 400

TooManyDistributionsWithFunctionAssociations

You have reached the maximum number of distributions that are associated with a CloudFront function. For more information, see Quotas (formerly known as limits) in the Amazon CloudFront Developer Guide.

HTTP Status Code: 400

TooManyDistributionsWithLambdaAssociations

Processing your request would cause the maximum number of distributions with Lambda@Edge function associations per owner to be exceeded.

HTTP Status Code: 400

TooManyDistributionsWithSingleFunctionARN

The maximum number of distributions have been associated with the specified Lambda@Edge function.

HTTP Status Code: 400

TooManyFunctionAssociations

You have reached the maximum number of CloudFront function associations for this distribution. For more information, see Quotas (formerly known as limits) in the Amazon CloudFront Developer Guide.

HTTP Status Code: 400

TooManyHeadersInForwardedValues

Your request contains too many headers in forwarded values.

HTTP Status Code: 400

TooManyKeyGroupsAssociatedToDistribution

The number of key groups referenced by this distribution is more than the maximum allowed. For more information, see Quotas (formerly known as limits) in the Amazon CloudFront Developer Guide.

HTTP Status Code: 400

TooManyLambdaFunctionAssociations

Your request contains more Lambda@Edge function associations than are allowed per distribution.

HTTP Status Code: 400

TooManyOriginCustomHeaders

Your request contains too many origin custom headers.

HTTP Status Code: 400

TooManyOriginGroupsPerDistribution

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

HTTP Status Code: 400

TooManyOrigins

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

**TooManyQueryStringParameters**

Your request contains too many query string parameters.

HTTP Status Code: 400

**TooManyTrustedSigners**

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

HTTP Status Code: 400

**TrustedKeyGroupDoesNotExist**

The specified key group does not exist.

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

Create a new field-level encryption configuration.

Request Syntax

```xml
POST /2020-05-31/field-level-encryption HTTP/1.1
<?xml version="1.0" encoding="UTF-8"?>
  <CallerReference>string</CallerReference>
  <Comment>string</Comment>
  <ContentTypeProfileConfig>
    <Items>
      <ContentTypeProfile>
        <ContentType>string</ContentType>
        <Format>string</Format>
        <ProfileId>string</ProfileId>
      </ContentTypeProfile>
    </Items>
    <Quantity>integer</Quantity>
  </ContentTypeProfileConfig>
  <QueryArgProfileConfig>
    <Items>
      <QueryArgProfile>
        <ProfileId>string</ProfileId>
        <QueryArg>string</QueryArg>
      </QueryArgProfile>
    </Items>
    <Quantity>integer</Quantity>
  </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. 55)**

Root level tag for the FieldLevelEncryptionConfig parameters.

Required: Yes

**CallerReference (p. 55)**

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

Type: String

Required: Yes
Comment (p. 55)

An optional comment about the configuration. The comment cannot be longer than 128 characters.

Type: String

Required: No

ContentTypeProfileConfig (p. 55)

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. 396) object

Required: No

QueryArgProfileConfig (p. 55)

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. 497) object

Required: No

Response Syntax

```
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>
```
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. 56)**

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

**FieldLevelEncryptionConfig (p. 56)**

- A complex data type that includes the profile configurations specified for field-level encryption.
- Type: FieldLevelEncryptionConfig (p. 431) object

**Id (p. 56)**

- 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. 56)**

- 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. 555).

**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**

- An 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 V2
- AWS SDK for JavaScript
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3
CreateFieldLevelEncryptionProfile

Create a field-level encryption profile.

Request Syntax

```xml
POST /2020-05-31/field-level-encryption-profile HTTP/1.1
<?xml version="1.0" encoding="UTF-8"?>
  <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. 59)**

Root level tag for the FieldLevelEncryptionProfileConfig parameters.

Required: Yes

**CallerReference (p. 59)**

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

Type: String

Required: Yes

**Comment (p. 59)**

An optional comment for the field-level encryption profile. The comment cannot be longer than 128 characters.

Type: String

Required: No
EncryptionEntities (p. 59)

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. 427) object

Required: Yes

Name (p. 59)

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. 60)

Root level tag for the FieldLevelEncryptionProfile parameters.

Required: Yes

FieldLevelEncryptionProfileConfig (p. 60)

A complex data type that includes the profile name and the encryption entities for the field-level encryption profile.
Type: FieldLevelEncryptionProfileConfig (p. 434) object

Id (p. 60)

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. 60)

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. 555).

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

An 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 V2
- AWS SDK for JavaScript
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3
CreateFunction

Creates a CloudFront function.

To create a function, you provide the function code and some configuration information about the function. The response contains an Amazon Resource Name (ARN) that uniquely identifies the function.

When you create a function, it's in the DEVELOPMENT stage. In this stage, you can test the function with TestFunction, and update it with UpdateFunction.

When you're ready to use your function with a CloudFront distribution, use PublishFunction to copy the function from the DEVELOPMENT stage to LIVE. When it's live, you can attach the function to a distribution's cache behavior, using the function's ARN.

Request Syntax

POST /2020-05-31/function HTTP/1.1
<?xml version="1.0" encoding="UTF-8"?>
  <FunctionCode>blob</FunctionCode>
  <FunctionConfig>
    <Comment>string</Comment>
    <Runtime>string</Runtime>
  </FunctionConfig>
  <Name>string</Name>
</CreateFunctionRequest>

URI Request Parameters

The request does not use any URI parameters.

Request Body

The request accepts the following data in XML format.

CreateFunctionRequest (p. 63)

Root level tag for the CreateFunctionRequest parameters.

Required: Yes

FunctionCode (p. 63)

The function code. For more information about writing a CloudFront function, see Writing function code for CloudFront Functions in the Amazon CloudFront Developer Guide.

Type: Base64-encoded binary data object


Required: Yes

FunctionConfig (p. 63)

Configuration information about the function, including an optional comment and the function's runtime.

Type: FunctionConfig (p. 444) object
Required: Yes

**Name (p. 63)**

A name to identify the function.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 64.

Pattern: ^[a-zA-Z0-9-_.]{1,64}$

Required: Yes

---

**Response Syntax**

```
HTTP/1.1 201
<?xml version="1.0" encoding="UTF-8"?>
<FunctionSummary>
  <FunctionConfig>
    <Comment>string</Comment>
    <Runtime>string</Runtime>
  </FunctionConfig>
  <FunctionMetadata>
    <CreatedTime>timestamp</CreatedTime>
    <FunctionARN>string</FunctionARN>
    <LastModifiedTime>timestamp</LastModifiedTime>
    <Stage>string</Stage>
  </FunctionMetadata>
  <Name>string</Name>
  <Status>string</Status>
</FunctionSummary>
```

---

**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.

*FunctionSummary (p. 64)*

Root level tag for the FunctionSummary parameters.

Required: Yes

*FunctionConfig (p. 64)*

Contains configuration information about a CloudFront function.

Type: FunctionConfig (p. 444) object

*FunctionMetadata (p. 64)*

Contains metadata about a CloudFront function.

Type: FunctionMetadata (p. 446) object

*Name (p. 64)*

The name of the CloudFront function.

Type: String
Length Constraints: Minimum length of 1. Maximum length of 64.

Pattern: ^[a-zA-Z0-9-_.]{1,64}$

**Status (p. 64)**

The status of the CloudFront function.

Type: String

**Errors**

For information about the errors that are common to all actions, see Common Errors (p. 555).

**FunctionAlreadyExists**

A function with the same name already exists in this AWS account. To create a function, you must provide a unique name. To update an existing function, use UpdateFunction.

HTTP Status Code: 409

**FunctionSizeLimitExceeded**

The function is too large. For more information, see Quotas (formerly known as limits) in the Amazon CloudFront Developer Guide.

HTTP Status Code: 413

**InvalidArgument**

An argument is invalid.

HTTP Status Code: 400

**TooManyFunctions**

You have reached the maximum number of CloudFront functions for this AWS account. For more information, see Quotas (formerly known as limits) in the Amazon CloudFront Developer Guide.

HTTP Status Code: 400

**UnsupportedOperation**

This operation is not supported in this region.

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 V2
- AWS SDK for JavaScript
- AWS SDK for PHP V3
- AWS SDK for Python
• AWS SDK for Ruby V3
CreateInvalidation

Create a new invalidation.

Request Syntax

```
POST /2020-05-31/distribution/DistributionId/invalidation HTTP/1.1
<?xml version="1.0" encoding="UTF-8"?>
  <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. 67)**

Root level tag for the InvalidationBatch parameters.

Required: Yes

**CallerReference (p. 67)**

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 InvalidationBatchAlreadyExists error.

Type: String

Required: Yes

**Paths (p. 67)**

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. 491) 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. 68)

Root level tag for the Invalidation parameters.

Required: Yes

CreateTime (p. 68)

The date and time the invalidation request was first made.

Type: Timestamp

Id (p. 68)

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

Type: String

InvalidationBatch (p. 68)

The current invalidation information for the batch request.

Type: InvalidationBatch (p. 452) object

Status (p. 68)

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. 555).
AccessDenied

Access denied.

HTTP Status Code: 403

BatchTooLarge

Invalidation batch specified is too large.

HTTP Status Code: 413

InconsistentQuantities

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

HTTP Status Code: 400

InvalidArgument

An 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 V2
- AWS SDK for JavaScript
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3
CreateKeyGroup

Creates a key group that you can use with CloudFront signed URLs and signed cookies.

To create a key group, you must specify at least one public key for the key group. After you create a key group, you can reference it from one or more cache behaviors. When you reference a key group in a cache behavior, CloudFront requires signed URLs or signed cookies for all requests that match the cache behavior. The URLs or cookies must be signed with a private key whose corresponding public key is in the key group. The signed URL or cookie contains information about which public key CloudFront should use to verify the signature. For more information, see Serving private content in the Amazon CloudFront Developer Guide.

Request Syntax

POST /2020-05-31/key-group HTTP/1.1
<?xml version="1.0" encoding="UTF-8"?>
<KeyGroupConfig xmlns="http://cloudfront.amazonaws.com/doc/2020-05-31/"
  <Comment>string</Comment>
  <Items>
    <PublicKey>string</PublicKey>
  </Items>
  <Name>string</Name>
</KeyGroupConfig>

URI Request Parameters

The request does not use any URI parameters.

Request Body

The request accepts the following data in XML format.

KeyGroupConfig (p. 70)

Root level tag for the KeyGroupConfig parameters.

Required: Yes

Comment (p. 70)

A comment to describe the key group. The comment cannot be longer than 128 characters.

Type: String

Required: No

Items (p. 70)

A list of the identifiers of the public keys in the key group.

Type: Array of strings

Required: Yes

Name (p. 70)

A name to identify the key group.
Type: String
Required: Yes

Response Syntax

HTTP/1.1 201
<?xml version="1.0" encoding="UTF-8"?>
<KeyGroup>
  <Id>string</Id>
  <KeyGroupConfig>
    <Comment>string</Comment>
    <Items>
      <PublicKey>string</PublicKey>
      <Name>string</Name>
    </Items>
  </KeyGroupConfig>
  <LastModifiedTime>timestamp</LastModifiedTime>
</KeyGroup>

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.

**KeyGroup** (p. 71)
- Root level tag for the KeyGroup parameters.
  - Required: Yes

**Id** (p. 71)
- The identifier for the key group.
  - Type: String

**KeyGroupConfig** (p. 71)
- The key group configuration.
  - Type: KeyGroupConfig (p. 457) object

**LastModifiedTime** (p. 71)
- The date and time when the key group was last modified.
  - Type: Timestamp

Errors

For information about the errors that are common to all actions, see [Common Errors (p. 555)](#).

**InvalidArgument**
- An argument is invalid.
  - HTTP Status Code: 400
KeyGroupAlreadyExists

A key group with this name already exists. You must provide a unique name. To modify an existing key group, use UpdateKeyGroup.

HTTP Status Code: 409

TooManyKeyGroups

You have reached the maximum number of key groups for this AWS account. For more information, see Quotas (formerly known as limits) in the Amazon CloudFront Developer Guide.

HTTP Status Code: 400

TooManyPublicKeysInKeyGroup

The number of public keys in this key group is more than the maximum allowed. For more information, see Quotas (formerly known as limits) in the Amazon CloudFront Developer Guide.

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

Enables additional CloudWatch metrics for the specified CloudFront distribution. The additional metrics incur an additional cost.

For more information, see Viewing additional CloudFront distribution metrics in the Amazon CloudFront Developer Guide.

Request Syntax

```
POST /2020-05-31/distributions/DistributionId/monitoring-subscription HTTP/1.1
<?xml version="1.0" encoding="UTF-8"?>
  <RealtimeMetricsSubscriptionConfig>
    <RealtimeMetricsSubscriptionStatus>string</RealtimeMetricsSubscriptionStatus>
  </RealtimeMetricsSubscriptionConfig>
</MonitoringSubscription>
```

URI Request Parameters

The request does not use any URI parameters.

Request Body

The request accepts the following data in XML format.

**MonitoringSubscription (p. 73)**

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

**RealtimeMetricsSubscriptionConfig (p. 73)**

- A subscription configuration for additional CloudWatch metrics.
  - Type: RealtimeMetricsSubscriptionConfig (p. 504) object
  - Required: No

Response Syntax

```
HTTP/1.1 200
<?xml version="1.0" encoding="UTF-8"?>
<MonitoringSubscription>
  <RealtimeMetricsSubscriptionConfig>
    <RealtimeMetricsSubscriptionStatus>string</RealtimeMetricsSubscriptionStatus>
  </RealtimeMetricsSubscriptionConfig>
</MonitoringSubscription>
```

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.
MonitoringSubscription (p. 73)

Root level tag for the MonitoringSubscription parameters.

Required: Yes

RealtimeMetricsSubscriptionConfig (p. 73)

A subscription configuration for additional CloudWatch metrics.

Type: RealtimeMetricsSubscriptionConfig (p. 504) object

Errors

For information about the errors that are common to all actions, see Common Errors (p. 555).

AccessDenied

Access denied.

HTTP Status Code: 403

NoSuchDistribution

The specified distribution does not exist.

HTTP Status Code: 404

UnsupportedOperation

This operation is not supported in this region.

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

Creates an origin request policy.

After you create an origin request policy, you can attach it to one or more cache behaviors. When it’s attached to a cache behavior, the origin request policy determines the values that CloudFront includes in requests that it sends to the origin. Each request that CloudFront sends to the origin includes the following:

- The request body and the URL path (without the domain name) from the viewer request.
- The headers that CloudFront automatically includes in every origin request, including Host, User-Agent, and X-Amz-Cf-Id.
- All HTTP headers, cookies, and URL query strings that are specified in the cache policy or the origin request policy. These can include items from the viewer request and, in the case of headers, additional ones that are added by CloudFront.

CloudFront sends a request when it can’t find a valid object in its cache that matches the request. If you want to send values to the origin and also include them in the cache key, use CachePolicy.

For more information about origin request policies, see Controlling origin requests in the Amazon CloudFront Developer Guide.

Request Syntax

```
POST /2020-05-31/origin-request-policy HTTP/1.1
<?xml version="1.0" encoding="UTF-8"?>
   <Comment>string</Comment>
   <CookiesConfig>
      <CookieBehavior>string</CookieBehavior>
      <Cookies>
         <Items>
            <Name>string</Name>
         </Items>
         <Quantity>integer</Quantity>
      </Cookies>
   </CookiesConfig>
   <HeadersConfig>
      <HeaderBehavior>string</HeaderBehavior>
      <Headers>
         <Items>
            <Name>string</Name>
         </Items>
         <Quantity>integer</Quantity>
      </Headers>
   </HeadersConfig>
   <Name>string</Name>
   <QueryStringsConfig>
      <QueryStringBehavior>string</QueryStringBehavior>
      <QueryStrings>
         <Items>
            <Name>string</Name>
         </Items>
         <Quantity>integer</Quantity>
      </QueryStrings>
   </QueryStringsConfig>
</OriginRequestPolicyConfig>
```
URI Request Parameters

The request does not use any URI parameters.

Request Body

The request accepts the following data in XML format.

**OriginRequestPolicyConfig** (p. 75)

Root level tag for the OriginRequestPolicyConfig parameters.

Required: Yes

**Comment** (p. 75)

A comment to describe the origin request policy. The comment cannot be longer than 128 characters.

Type: String

Required: No

**CookiesConfig** (p. 75)

The cookies from viewer requests to include in origin requests.

Type: **OriginRequestPolicyCookiesConfig** (p. 481) object

Required: Yes

**HeadersConfig** (p. 75)

The HTTP headers to include in origin requests. These can include headers from viewer requests and additional headers added by CloudFront.

Type: **OriginRequestPolicyHeadersConfig** (p. 482) object

Required: Yes

**Name** (p. 75)

A unique name to identify the origin request policy.

Type: String

Required: Yes

**QueryStringsConfig** (p. 75)

The URL query strings from viewer requests to include in origin requests.

Type: **OriginRequestPolicyQueryStringsConfig** (p. 484) object

Required: Yes

Response Syntax

```
HTTP/1.1 201
<?xml version="1.0" encoding="UTF-8"?>
<OriginRequestPolicy>
```

API Version 2020-05-31

76
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.

**OriginRequestPolicy (p. 76)**

Root level tag for the OriginRequestPolicy parameters.

Required: Yes

**Id (p. 76)**

The unique identifier for the origin request policy.

Type: String

**LastModifiedTime (p. 76)**

The date and time when the origin request policy was last modified.

Type: Timestamp

**OriginRequestPolicyConfig (p. 76)**

The origin request policy configuration.

Type: OriginRequestPolicyConfig (p. 479) object
Errors

For information about the errors that are common to all actions, see Common Errors (p. 555).

AccessDenied

Access denied.

HTTP Status Code: 403

InconsistentQuantities

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

HTTP Status Code: 400

InvalidArgument

An argument is invalid.

HTTP Status Code: 400

OriginRequestPolicyAlreadyExists

An origin request policy with this name already exists. You must provide a unique name. To modify an existing origin request policy, use UpdateOriginRequestPolicy.

HTTP Status Code: 409

TooManyCookiesInOriginRequestPolicy

The number of cookies in the origin request policy exceeds the maximum. For more information, see Quotas (formerly known as limits) in the Amazon CloudFront Developer Guide.

HTTP Status Code: 400

TooManyHeadersInOriginRequestPolicy

The number of headers in the origin request policy exceeds the maximum. For more information, see Quotas (formerly known as limits) in the Amazon CloudFront Developer Guide.

HTTP Status Code: 400

TooManyOriginRequestPolicies

You have reached the maximum number of origin request policies for this AWS account. For more information, see Quotas (formerly known as limits) in the Amazon CloudFront Developer Guide.

HTTP Status Code: 400

TooManyQueryStringsInOriginRequestPolicy

The number of query strings in the origin request policy exceeds the maximum. For more information, see Quotas (formerly known as limits) in the Amazon CloudFront Developer Guide.

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 V2
• AWS SDK for JavaScript
• AWS SDK for PHP V3
• AWS SDK for Python
• AWS SDK for Ruby V3
CreatePublicKey

Uploads a public key to CloudFront that you can use with signed URLs and signed cookies, or with field-level encryption.

**Request Syntax**

```xml
POST /2020-05-31/public-key HTTP/1.1
<?xml version="1.0" encoding="UTF-8"?>
<PublicKeyConfig xmlns="http://cloudfront.amazonaws.com/doc/2020-05-31/"
    <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. 80)**
  - Root level tag for the PublicKeyConfig parameters.
  - Required: Yes

- **CallerReference (p. 80)**
  - A string included in the request to help make sure that the request can't be replayed.
  - Type: String
  - Required: Yes

- **Comment (p. 80)**
  - A comment to describe the public key. The comment cannot be longer than 128 characters.
  - Type: String
  - Required: No

- **EncodedKey (p. 80)**
  - The public key that you can use with signed URLs and signed cookies, or with field-level encryption.
  - Type: String
  - Required: Yes

- **Name (p. 80)**
  - A name to help identify the public key.
  - Type: String
  - Required: Yes
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. 81)**

Root level tag for the PublicKey parameters.

Required: Yes

**CreatedTime (p. 81)**

The date and time when the public key was uploaded.

Type: Timestamp

**Id (p. 81)**

The identifier of the public key.

Type: String

**PublicKeyConfig (p. 81)**

Configuration information about a public key that you can use with signed URLs and signed cookies, or with field-level encryption.

Type: PublicKeyConfig (p. 493) object

Errors

For information about the errors that are common to all actions, see Common Errors (p. 555).

**InvalidArgument**

An 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 V2
- AWS SDK for JavaScript
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3
CreateRealtimeLogConfig

Creates a real-time log configuration.

After you create a real-time log configuration, you can attach it to one or more cache behaviors to send real-time log data to the specified Amazon Kinesis data stream.

For more information about real-time log configurations, see Real-time logs in the Amazon CloudFront Developer Guide.

Request Syntax

```xml
POST /2020-05-31/realtime-log-config HTTP/1.1
<?xml version="1.0" encoding="UTF-8"?>
  <EndPoints>
    <EndPoint>
      <KinesisStreamConfig>
        <RoleARN>string</RoleARN>
        <StreamARN>string</StreamARN>
      </KinesisStreamConfig>
      <StreamType>string</StreamType>
    </EndPoint>
  </EndPoints>
  <Fields>
    <Field>string</Field>
  </Fields>
  <Name>string</Name>
  <SamplingRate>long</SamplingRate>
</CreateRealtimeLogConfigRequest>
```

URI Request Parameters

The request does not use any URI parameters.

Request Body

The request accepts the following data in XML format.

CreateRealtimeLogConfigRequest (p. 83)

Root level tag for the CreateRealtimeLogConfigRequest parameters.

Required: Yes

EndPoints (p. 83)

Contains information about the Amazon Kinesis data stream where you are sending real-time log data.

Type: Array of EndPoint (p. 429) objects

Required: Yes

Fields (p. 83)

A list of fields to include in each real-time log record.

For more information about fields, see Real-time log configuration fields in the Amazon CloudFront Developer Guide.
Type: Array of strings
Required: Yes

**Name (p. 83)**
A unique name to identify this real-time log configuration.
Type: String
Required: Yes

**SamplingRate (p. 83)**
The sampling rate for this real-time log configuration. The sampling rate determines the percentage of viewer requests that are represented in the real-time log data. You must provide an integer between 1 and 100, inclusive.
Type: Long
Required: Yes

### Response Syntax

```
HTTP/1.1 201
<?xml version="1.0" encoding="UTF-8"?>
<CreateRealtimeLogConfigResult>
  <RealtimeLogConfig>
    <ARN>string</ARN>
    <EndPoints>
      <EndPoint>
        <KinesisStreamConfig>
          <RoleARN>string</RoleARN>
          <StreamARN>string</StreamARN>
        </KinesisStreamConfig>
        <StreamType>string</StreamType>
      </EndPoint>
    </EndPoints>
    <Fields>
      <Field>string</Field>
    </Fields>
    <Name>string</Name>
    <SamplingRate>long</SamplingRate>
  </RealtimeLogConfig>
</CreateRealtimeLogConfigResult>
```

### 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.

**CreateRealtimeLogConfigResult (p. 84)**
Root level tag for the CreateRealtimeLogConfigResult parameters.
Required: Yes

**RealtimeLogConfig (p. 84)**
A real-time log configuration.
Errors

For information about the errors that are common to all actions, see Common Errors (p. 555).

AccessDenied

Access denied.

HTTP Status Code: 403

InvalidArgument

An argument is invalid.

HTTP Status Code: 400

RealtimeLogConfigAlreadyExists

A real-time log configuration with this name already exists. You must provide a unique name. To modify an existing real-time log configuration, use UpdateRealtimeLogConfig.

HTTP Status Code: 409

TooManyRealtimeLogConfigs

You have reached the maximum number of real-time log configurations for this AWS account. For more information, see Quotas (formerly known as limits) in the Amazon CloudFront Developer Guide.

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

Creates a response headers policy.

A response headers policy contains information about a set of HTTP response headers and their values. To create a response headers policy, you provide some metadata about the policy, and a set of configurations that specify the response headers.

After you create a response headers policy, you can use its ID to attach it to one or more cache behaviors in a CloudFront distribution. When it’s attached to a cache behavior, CloudFront adds the headers in the policy to HTTP responses that it sends for requests that match the cache behavior.

Request Syntax

```
POST /2020-05-31/response-headers-policy HTTP/1.1
<?xml version="1.0" encoding="UTF-8"?>
    <Comment>string</Comment>
  <CorsConfig>
    <AccessControlAllowCredentials>boolean</AccessControlAllowCredentials>
    <AccessControlAllowHeaders>
      <Items>
        <Header>string</Header>
      </Items>
      <Quantity>integer</Quantity>
    </AccessControlAllowHeaders>
    <AccessControlAllowMethods>
      <Items>
        <Method>string</Method>
      </Items>
      <Quantity>integer</Quantity>
    </AccessControlAllowMethods>
    <AccessControlAllowOrigins>
      <Items>
        <Origin>string</Origin>
      </Items>
      <Quantity>integer</Quantity>
    </AccessControlAllowOrigins>
    <AccessControlExposeHeaders>
      <Items>
        <Header>string</Header>
      </Items>
      <Quantity>integer</Quantity>
    </AccessControlExposeHeaders>
    <AccessControlMaxAgeSec>integer</AccessControlMaxAgeSec>
    <OriginOverride>boolean</OriginOverride>
  </CorsConfig>
  <CustomHeadersConfig>
    <Items>
      <ResponseHeadersPolicyCustomHeader>
        <Header>string</Header>
        <Override>boolean</Override>
        <Value>string</Value>
      </ResponseHeadersPolicyCustomHeader>
    </Items>
    <Quantity>integer</Quantity>
  </CustomHeadersConfig>
  <Name>string</Name>
  <SecurityHeadersConfig>
    <ContentSecurityPolicy>string</ContentSecurityPolicy>
    <Override>boolean</Override>
  </SecurityHeadersConfig>
</ResponseHeadersPolicyConfig>
```
URI Request Parameters

The request does not use any URI parameters.

Request Body

The request accepts the following data in XML format.

**ResponseHeadersPolicyConfig (p. 86)**

Root level tag for the ResponseHeadersPolicyConfig parameters.

Required: Yes

**Comment (p. 86)**

A comment to describe the response headers policy.

The comment cannot be longer than 128 characters.

Type: String

Required: No

**CorsConfig (p. 86)**

A configuration for a set of HTTP response headers that are used for cross-origin resource sharing (CORS).

Type: ResponseHeadersPolicyCorsConfig (p. 514) object

Required: No
**CustomHeadersConfig (p. 86)**

A configuration for a set of custom HTTP response headers.

Type: `ResponseHeadersPolicyCustomHeadersConfig (p. 517)` object

Required: No

**Name (p. 86)**

A name to identify the response headers policy.

The name must be unique for response headers policies in this AWS account.

Type: String

Required: Yes

**SecurityHeadersConfig (p. 86)**

A configuration for a set of security-related HTTP response headers.

Type: `ResponseHeadersPolicySecurityHeadersConfig (p. 521)` object

Required: No

**ServerTimingHeadersConfig (p. 86)**

A configuration for enabling the `Server-Timing` header in HTTP responses sent from CloudFront.

Type: `ResponseHeadersPolicyServerTimingHeadersConfig (p. 523)` object

Required: No

## Response Syntax

```
HTTP/1.1 201
<?xml version="1.0" encoding="UTF-8"?>
<ResponseHeadersPolicy>
  <Id>string</Id>
  <LastModifiedTime>timestamp</LastModifiedTime>
  <ResponseHeadersPolicyConfig>
    <Comment>string</Comment>
    <CorsConfig>
      <AccessControlAllowCredentials>boolean</AccessControlAllowCredentials>
      <AccessControlAllowHeaders>
        <Items>
          <Header>string</Header>
        </Items>
        <Quantity>integer</Quantity>
      </AccessControlAllowHeaders>
      <AccessControlAllowMethods>
        <Items>
          <Method>string</Method>
        </Items>
        <Quantity>integer</Quantity>
      </AccessControlAllowMethods>
      <AccessControlAllowOrigins>
        <Items>
          <Origin>string</Origin>
        </Items>
        <Quantity>integer</Quantity>
      </AccessControlAllowOrigins>
      <AccessControlExposeHeaders>
```

```
```
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.

ResponseHeadersPolicy (p. 88)

Root level tag for the ResponseHeadersPolicy parameters.
The Amazon CloudFront API Reference

Errors

**Required: Yes**

**Id (p. 88)**

The identifier for the response headers policy.

Type: String

**LastModifiedTime (p. 88)**

The date and time when the response headers policy was last modified.

Type: Timestamp

**ResponseHeadersPolicyConfig (p. 88)**

A response headers policy configuration.

A response headers policy contains information about a set of HTTP response headers and their values. CloudFront adds the headers in the policy to HTTP responses that it sends for requests that match a cache behavior that's associated with the policy.

Type: `ResponseHeadersPolicyConfig (p. 510)` object

---

**Errors**

For information about the errors that are common to all actions, see [Common Errors (p. 555)](#).

**AccessDenied**

Access denied.

HTTP Status Code: 403

**InconsistentQuantities**

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

HTTP Status Code: 400

**InvalidArgument**

An argument is invalid.

HTTP Status Code: 400

**ResponseHeadersPolicyAlreadyExists**

A response headers policy with this name already exists. You must provide a unique name. To modify an existing response headers policy, use `UpdateResponseHeadersPolicy`.

HTTP Status Code: 409

**TooManyCustomHeadersInResponseHeadersPolicy**

The number of custom headers in the response headers policy exceeds the maximum.

For more information, see [Quotas (formerly known as limits)](https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/quotas.html) in the Amazon CloudFront Developer Guide.

HTTP Status Code: 400

**TooManyResponseHeadersPolicies**

You have reached the maximum number of response headers policies for this AWS account.
For more information, see Quotas (formerly known as limits) in the Amazon CloudFront Developer Guide.

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

This API is deprecated. Amazon CloudFront is deprecating real-time messaging protocol (RTMP) distributions on December 31, 2020. For more information, read the announcement on the Amazon CloudFront discussion forum.

Request Syntax

POST /2020-05-31/streaming-distribution HTTP/1.1
<?xml version="1.0" encoding="UTF-8"?>
  <Aliases>
    <CNAME>string</CNAME>
  </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>
  </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. 92)

  Root level tag for the StreamingDistributionConfig parameters.
  Required: Yes

Aliases (p. 92)

  A complex type that contains information about CNAMEs (alternate domain names), if any, for this streaming distribution.
  Type: Aliases (p. 369) object

API Version 2020-05-31
**Request Body**

**CallerReference (p. 92)**

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 StreamingDistributionConfig object), CloudFront creates a new distribution.

If CallerReference is a value that you already sent in a previous request to create a distribution, CloudFront returns a DistributionAlreadyExists error.

Type: String

Required: Yes

**Comment (p. 92)**

Any comments you want to include about the streaming distribution.

Type: String

Required: Yes

**Enabled (p. 92)**

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

Type: Boolean

Required: Yes

**Logging (p. 92)**

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

Type: StreamingLoggingConfig (p. 542) object

Required: No

**PriceClass (p. 92)**

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. 92)**

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. 529) object

Required: Yes

**TrustedSigners (p. 92)**

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. 548) 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>
    <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 201 response.

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

**StreamingDistribution (p. 94)**

Root level tag for the StreamingDistribution parameters.

Required: Yes

**ActiveTrustedSigners (p. 94)**

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. 368) object

**ARN (p. 94)**

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

**DomainName (p. 94)**

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

Type: String

**Id (p. 94)**

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

Type: String

**LastModifiedTime (p. 94)**

The date and time that the distribution was last modified.

Type: Timestamp

**Status (p. 94)**

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. 94)**

The current configuration information for the RTMP distribution.
Errors

For information about the errors that are common to all actions, see Common Errors (p. 555).

AccessDenied

Access denied.

HTTP Status Code: 403

CNAMEAlreadyExists

The CNAME specified is already defined for CloudFront.

HTTP Status Code: 409

InconsistentQuantities

The value of quantity and the size of items don't match.

HTTP Status Code: 400

InvalidArgument

An 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

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

HTTP Status Code: 409

TooManyStreamingDistributionCNAMEs

Your request contains more CNAMEs than are allowed per distribution.

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

This API is deprecated. Amazon CloudFront is deprecating real-time messaging protocol (RTMP) distributions on December 31, 2020. For more information, read the announcement on the Amazon CloudFront discussion forum.

Request Syntax

```
POST /2020-05-31/streaming-distribution?WithTags HTTP/1.1
<?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>
            <Items>
                <AwsAccountNumber>string</AwsAccountNumber>
            </Items>
            <Quantity>integer</Quantity>
        </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. 98)

Root level tag for the StreamingDistributionConfigWithTags parameters.

Required: Yes

StreamingDistributionConfig (p. 98)

A streaming distribution Configuration.

Type: StreamingDistributionConfig (p. 535) object

Required: Yes

Tags (p. 98)

A complex type that contains zero or more Tag elements.

Type: Tags (p. 545) 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>
    <Comment>string</Comment>
    <Enabled>boolean</Enabled>
    <Logging>
      <Bucket>string</Bucket>
      <Enabled>boolean</Enabled>
      <Prefix>string</Prefix>
    </Logging>
    <PriceClass>string</PriceClass>
  </StreamingDistributionConfig>
</StreamingDistribution>
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. 99)**

Root level tag for the StreamingDistribution parameters.

Required: Yes

**ActiveTrustedSigners (p. 99)**

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. 368) object

**ARN (p. 99)**

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

**DomainName (p. 99)**

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

Type: String

**Id (p. 99)**

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

Type: String
LastModifiedTime (p. 99)

The date and time that the distribution was last modified.

Type: Timestamp

Status (p. 99)

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. 99)

The current configuration information for the RTMP distribution.

Type: StreamingDistributionConfig (p. 535) object

Errors

For information about the errors that are common to all actions, see Common Errors (p. 555).

AccessDenied

Access denied.

HTTP Status Code: 403

CNAMEAlreadyExists

The CNAME specified is already defined for CloudFront.

HTTP Status Code: 409

InconsistentQuantities

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

HTTP Status Code: 400

InvalidArgument

An 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

The tagging specified is not valid.

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**

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

HTTP Status Code: 409

**TooManyStreamingDistributionCNAMEs**

Your request contains more CNAMEs than are allowed per distribution.

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

Deletes a cache policy.

You cannot delete a cache policy if it’s attached to a cache behavior. First update your distributions to remove the cache policy from all cache behaviors, then delete the cache policy.

To delete a cache policy, you must provide the policy’s identifier and version. To get these values, you can use ListCachePolicies or GetCachePolicy.

Request Syntax

```
DELETE /2020-05-31/cache-policy/Id HTTP/1.1
If-Match: IfMatch
```

URI Request Parameters

The request uses the following URI parameters.

**Id (p. 103)**

The unique identifier for the cache policy that you are deleting. To get the identifier, you can use ListCachePolicies.

Required: Yes

**If-Match (p. 103)**

The version of the cache policy that you are deleting. The version is the cache policy’s ETag value, which you can get using ListCachePolicies, GetCachePolicy, or GetCachePolicyConfig.

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. 555).

**AccessDenied**

Access denied.

HTTP Status Code: 403
CachePolicyInUse

Cannot delete the cache policy because it is attached to one or more cache behaviors.

HTTP Status Code: 409

IllegalDelete

You cannot delete a managed policy.

HTTP Status Code: 400

InvalidIfMatchVersion

The If-Match version is missing or not valid.

HTTP Status Code: 400

NoSuchCachePolicy

The cache policy does not exist.

HTTP Status Code: 404

PreconditionFailed

The precondition in one or more of the request 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 V2
- AWS SDK for JavaScript
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3
DeleteCloudFrontOriginAccessIdentity

Delete an origin access identity.

**Request Syntax**

```
DELETE /2020-05-31/origin-access-identity/cloudfront/Id HTTP/1.1
If-Match: IfMatch
```

**URI Request Parameters**

The request uses the following URI parameters.

- **Id** *(p. 105)*
  
  The origin access identity's ID.
  
  Required: Yes

- **If-Match** *(p. 105)*
  
  The value of the ETag header you received from a previous GET or PUT request. For example: E2QWRUHAPOMQ2L.

**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. 555).*

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

- **CloudFrontOriginAccessIdentityInUse**
  
  The Origin Access Identity specified is already in use.
  
  HTTP Status Code: 409

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

**NoSuchCloudFrontOriginAccessIdentity**

The specified origin access identity does not exist.

HTTP Status Code: 404

**PreconditionFailed**

The precondition in one or more of the request 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 V2
- AWS SDK for JavaScript
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3
DeleteDistribution

Delete a distribution.

Request Syntax

DELETE /2020-05-31/distribution/Id HTTP/1.1
If-Match: IfMatch

URI Request Parameters

The request uses the following URI parameters.

Id (p. 107)

The distribution ID.

Required: Yes

If-Match (p. 107)

The value of the ETag header that you received when you disabled the distribution. For example: E2QWRUHAPOMG2L.

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. 555).

AccessDenied

Access denied.

HTTP Status Code: 403

DistributionNotDisabled

The specified CloudFront distribution is not disabled. You must disable the distribution before you can delete it.

HTTP Status Code: 409
InvalidIfMatchVersion

The If-Match version is missing or not valid.

HTTP Status Code: 400

NoSuchDistribution

The specified distribution does not exist.

HTTP Status Code: 404

PreconditionFailed

The precondition in one or more of the request 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 V2
- AWS SDK for JavaScript
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3
DeleteFieldLevelEncryptionConfig

Remove a field-level encryption configuration.

Request Syntax

DELETE /2020-05-31/field-level-encryption/Id HTTP/1.1
If-Match: IfMatch

URI Request Parameters

The request uses the following URI parameters.

Id (p. 109)

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

Required: Yes

If-Match (p. 109)

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

For example: E2QWRUHAPOMQ2L.

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. 555).

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.
HTTP Status Code: 400

NoSuchFieldLevelEncryptionConfig

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

HTTP Status Code: 404

PreconditionFailed

The precondition in one or more of the request 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 V2
- AWS SDK for JavaScript
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3
DeleteFieldLevelEncryptionProfile

Remove a field-level encryption profile.

Request Syntax

```
DELETE /2020-05-31/field-level-encryption-profile/Id HTTP/1.1
If-Match: IfMatch
```

URI Request Parameters

The request uses the following URI parameters.

Id (p. 111)

Request the ID of the profile you want to delete from CloudFront.

Required: Yes

If-Match (p. 111)

The value of the ETag header that you received when retrieving the profile to delete. For example: E2QWRUHAPOMQ2L.

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. 555).

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.
HTTP Status Code: 400

NoSuchFieldLevelEncryptionProfile

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

HTTP Status Code: 404

PreconditionFailed

The precondition in one or more of the request 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 V2
- AWS SDK for JavaScript
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3
DeleteFunction

Deletes a CloudFront function.

You cannot delete a function if it’s associated with a cache behavior. First, update your distributions to remove the function association from all cache behaviors, then delete the function.

To delete a function, you must provide the function's name and version (ETag value). To get these values, you can use ListFunctions and DescribeFunction.

Request Syntax

DELETE /2020-05-31/function/Name HTTP/1.1
If-Match: IfMatch

URI Request Parameters

The request uses the following URI parameters.

If-Match (p. 113)

The current version (ETag value) of the function that you are deleting, which you can get using DescribeFunction.

Required: Yes

Name (p. 113)

The name of the function that you are deleting.

Required: Yes

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. 555).

FunctionInUse

Cannot delete the function because it's attached to one or more cache behaviors.

HTTP Status Code: 409
InvalidIfMatchVersion
   The If-Match version is missing or not valid.
   HTTP Status Code: 400

NoSuchFunctionExists
   The function does not exist.
   HTTP Status Code: 404

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

UnsupportedOperation
   This operation is not supported in this region.
   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 V2
- AWS SDK for JavaScript
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3
DeleteKeyGroup

Deletes a key group.

You cannot delete a key group that is referenced in a cache behavior. First update your distributions to remove the key group from all cache behaviors, then delete the key group.

To delete a key group, you must provide the key group's identifier and version. To get these values, use ListKeyGroups followed by GetKeyGroup or GetKeyGroupConfig.

_requestSyntax

DELETE /2020-05-31/key-group/Id HTTP/1.1
If-Match: IfMatch

_URIRequestParameters

The request uses the following URI parameters.

**Id (p. 115)**

The identifier of the key group that you are deleting. To get the identifier, use ListKeyGroups.

Required: Yes

**If-Match (p. 115)**

The version of the key group that you are deleting. The version is the key group's ETag value. To get the ETag, use GetKeyGroup or GetKeyGroupConfig.

_requestBody

The request does not have a request body.

_responseSyntax

HTTP/1.1 204

_responseElements

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. 555).

**InvalidIfMatchVersion**

The If-Match version is missing or not valid.

HTTP Status Code: 400
NoSuchResource

A resource that was specified is not valid.

HTTP Status Code: 404

PreconditionFailed

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

HTTP Status Code: 412

ResourceInUse

Cannot delete this resource because it 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 V2
- AWS SDK for JavaScript
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3
DeleteMonitoringSubscription

Disables additional CloudWatch metrics for the specified CloudFront distribution.

Request Syntax

DELETE /2020-05-31/distributions/DistributionId/monitoring-subscription HTTP/1.1

URI Request Parameters

The request uses the following URI parameters.

DistributionId (p. 117)

The ID of the distribution that you are disabling metrics for.

Required: Yes

Request Body

The request does not have a request body.

Response Syntax

HTTP/1.1 200

Response Elements

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

Errors

For information about the errors that are common to all actions, see Common Errors (p. 555).

AccessDenied

Access denied.

HTTP Status Code: 403

NoSuchDistribution

The specified distribution does not exist.

HTTP Status Code: 404

UnsupportedOperation

This operation is not supported in this region.

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

Deletes an origin request policy.

You cannot delete an origin request policy if it's attached to any cache behaviors. First update your distributions to remove the origin request policy from all cache behaviors, then delete the origin request policy.

To delete an origin request policy, you must provide the policy's identifier and version. To get the identifier, you can use ListOriginRequestPolicies or GetOriginRequestPolicy.

Request Syntax

DELETE /2020-05-31/origin-request-policy/Id HTTP/1.1
If-Match: IfMatch

URI Request Parameters

The request uses the following URI parameters.

Id (p. 119)

The unique identifier for the origin request policy that you are deleting. To get the identifier, you can use ListOriginRequestPolicies.

Required: Yes

If-Match (p. 119)

The version of the origin request policy that you are deleting. The version is the origin request policy's ETag value, which you can get using ListOriginRequestPolicies, GetOriginRequestPolicy, or GetOriginRequestPolicyConfig.

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. 555).

AccessDenied

Access denied.
HTTP Status Code: 403

**IllegalDelete**

You cannot delete a managed policy.

HTTP Status Code: 400

**InvalidIfMatchVersion**

The If-Match version is missing or not valid.

HTTP Status Code: 400

**NoSuchOriginRequestPolicy**

The origin request policy does not exist.

HTTP Status Code: 404

**OriginRequestPolicyInUse**

Cannot delete the origin request policy because it is attached to one or more cache behaviors.

HTTP Status Code: 409

**PreconditionFailed**

The precondition in one or more of the request 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 V2
- AWS SDK for JavaScript
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3
DeletePublicKey

Remove a public key you previously added to CloudFront.

Request Syntax

```
DELETE /2020-05-31/public-key/Id HTTP/1.1
If-Match: IfMatch
```

URI Request Parameters

The request uses the following URI parameters.

**Id (p. 121)**

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

- Required: Yes

**If-Match (p. 121)**

The value of the ETag header that you received when retrieving the public key 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. 555).

**AccessDenied**

- Access denied.
  - HTTP Status Code: 403

**InvalidIfMatchVersion**

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

**NoSuchPublicKey**

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

**PreconditionFailed**

The precondition in one or more of the request 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 V2
- AWS SDK for JavaScript
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3
DeleteRealtimeLogConfig

Deletes a real-time log configuration.

You cannot delete a real-time log configuration if it’s attached to a cache behavior. First update your distributions to remove the real-time log configuration from all cache behaviors, then delete the real-time log configuration.

To delete a real-time log configuration, you can provide the configuration’s name or its Amazon Resource Name (ARN). You must provide at least one. If you provide both, CloudFront uses the name to identify the real-time log configuration to delete.

Request Syntax

```
POST /2020-05-31/delete-realtime-log-config/ HTTP/1.1
<?xml version="1.0" encoding="UTF-8"?>
  <ARN>string</ARN>
  <Name>string</Name>
</DeleteRealtimeLogConfigRequest>
```

URI Request Parameters

The request does not use any URI parameters.

Request Body

The request accepts the following data in XML format.

```
DeleteRealtimeLogConfigRequest (p. 123)
```

Root level tag for the DeleteRealtimeLogConfigRequest parameters.

Required: Yes

```
ARN (p. 123)
```

The Amazon Resource Name (ARN) of the real-time log configuration to delete.

Type: String

Required: No

```
Name (p. 123)
```

The name of the real-time log configuration to delete.

Type: String

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. 555).

AccessDenied

Access denied.

HTTP Status Code: 403

InvalidArgument

An argument is invalid.

HTTP Status Code: 400

NoSuchRealtimeLogConfig

The real-time log configuration does not exist.

HTTP Status Code: 404

RealtimeLogConfigInUse

Cannot delete the real-time log configuration because it is attached to one or more cache behaviors.

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

Deletes a response headers policy.

You cannot delete a response headers policy if it's attached to a cache behavior. First update your distributions to remove the response headers policy from all cache behaviors, then delete the response headers policy.

To delete a response headers policy, you must provide the policy's identifier and version. To get these values, you can use ListResponseHeadersPolicies or GetResponseHeadersPolicy.

Request Syntax

```plaintext
DELETE /2020-05-31/response-headers-policy/Id HTTP/1.1
If-Match: IfMatch
```

URI Request Parameters

The request uses the following URI parameters.

**Id (p. 125)**

The identifier for the response headers policy that you are deleting.

To get the identifier, you can use ListResponseHeadersPolicies.

Required: Yes

**If-Match (p. 125)**

The version of the response headers policy that you are deleting.

The version is the response headers policy's ETag value, which you can get using ListResponseHeadersPolicies, GetResponseHeadersPolicy, or GetResponseHeadersPolicyConfig.

Request Body

The request does not have a request body.

Response Syntax

```plaintext
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. 555).
AccessDenied

Access denied.

HTTP Status Code: 403

IllegalDelete

You cannot delete a managed policy.

HTTP Status Code: 400

InvalidIfMatchVersion

The If-Match version is missing or not valid.

HTTP Status Code: 400

NoSuchResponseHeadersPolicy

The response headers policy does not exist.

HTTP Status Code: 404

PreconditionFailed

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

HTTP Status Code: 412

ResponseHeadersPolicyInUse

Cannot delete the response headers policy because it is attached to one or more cache behaviors in a CloudFront distribution.

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 V2
- AWS SDK for JavaScript
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3
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 /2020-05-31/streaming-distribution/Id HTTP/1.1
If-Match: IfMatch
```

URI Request Parameters

The request uses the following URI parameters.

**Id (p. 127)**

The distribution ID.

Required: Yes

**If-Match (p. 127)**

The value of the ETag header that you received when you disabled the streaming distribution. For example: E2QWRHUAPOMQZL.

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. 555).

**AccessDenied**

Access denied.

HTTP Status Code: 403

**InvalidIfMatchVersion**

The If-Match version is missing or not valid.

HTTP Status Code: 400

**NoSuchStreamingDistribution**

The specified streaming distribution does not exist.

HTTP Status Code: 404

**PreconditionFailed**

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

HTTP Status Code: 412

**StreamingDistributionNotDisabled**

The specified CloudFront distribution is not disabled. You must disable the distribution before you can delete it.

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

Gets configuration information and metadata about a CloudFront function, but not the function's code. To get a function's code, use GetFunction.

To get configuration information and metadata about a function, you must provide the function's name and stage. To get these values, you can use ListFunctions.

Request Syntax

```
GET /2020-05-31/function/Name?Stage=Stage HTTP/1.1
```

URI Request Parameters

The request uses the following URI parameters.

Name (p. 130)

The name of the function that you are getting information about.

Required: Yes

Stage (p. 130)

The function's stage, either DEVELOPMENT or LIVE.

Valid Values: DEVELOPMENT | LIVE

Request Body

The request does not have a request body.

Response Syntax

```
HTTP/1.1 200
<?xml version="1.0" encoding="UTF-8"?>
<FunctionSummary>
  <FunctionConfig>
    <Comment>string</Comment>
    <Runtime>string</Runtime>
  </FunctionConfig>
  <FunctionMetadata>
    <CreatedTime>timestamp</CreatedTime>
    <FunctionARN>string</FunctionARN>
    <LastModifiedTime>timestamp</LastModifiedTime>
  </FunctionMetadata>
  <Name>string</Name>
  <Status>string</Status>
</FunctionSummary>
```

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.

**FunctionSummary (p. 130)**

Root level tag for the FunctionSummary parameters.

Required: Yes

**FunctionConfig (p. 130)**

Contains configuration information about a CloudFront function.

Type: FunctionConfig (p. 444) object

**FunctionMetadata (p. 130)**

Contains metadata about a CloudFront function.

Type: FunctionMetadata (p. 446) object

**Name (p. 130)**

The name of the CloudFront function.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 64.

Pattern: ^[a-zA-Z0-9-]{1,64}$

**Status (p. 130)**

The status of the CloudFront function.

Type: String

---

**Errors**

For information about the errors that are common to all actions, see [Common Errors (p. 555)](#).

**NoSuchFunctionExists**

The function does not exist.

HTTP Status Code: 404

**UnsupportedOperation**

This operation is not supported in this region.

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](#)
See Also

- AWS SDK for Java V2
- AWS SDK for JavaScript
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3
GetCachePolicy

Gets a cache policy, including the following metadata:

- The policy's identifier.
- The date and time when the policy was last modified.

To get a cache policy, you must provide the policy's identifier. If the cache policy is attached to a distribution's cache behavior, you can get the policy's identifier using ListDistributions or GetDistribution. If the cache policy is not attached to a cache behavior, you can get the identifier using ListCachePolicies.

Request Syntax

```
GET /2020-05-31/cache-policy/Id HTTP/1.1
```

URI Request Parameters

The request uses the following URI parameters.

**Id (p. 133)**

The unique identifier for the cache policy. If the cache policy is attached to a distribution's cache behavior, you can get the policy's identifier using ListDistributions or GetDistribution. If the cache policy is not attached to a cache behavior, you can get the identifier using ListCachePolicies.

Required: Yes

Request Body

The request does not have a request body.

Response Syntax

```
HTTP/1.1 200
<?xml version="1.0" encoding="UTF-8"?>
<CachePolicy>
  <CachePolicyConfig>
    <Comment>string</Comment>
    <DefaultTTL>long</DefaultTTL>
    <MaxTTL>long</MaxTTL>
    <MinTTL>long</MinTTL>
    <Name>string</Name>
    <ParametersInCacheKeyAndForwardedToOrigin>
      <CookieBehavior>string</CookieBehavior>
      <Cookies>
        <Items>
          <Name>string</Name>
        </Items>
        <Quantity>integer</Quantity>
      </Cookies>
    </ParametersInCacheKeyAndForwardedToOrigin>
  </CachePolicyConfig>
</CachePolicy>
```

API Version 2020-05-31
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.

**CachePolicy** *(p. 133)*

Root level tag for the CachePolicy parameters.

Required: Yes

**CachePolicyConfig** *(p. 133)*

The cache policy configuration.

Type: CachePolicyConfig *(p. 381)* object

**Id** *(p. 133)*

The unique identifier for the cache policy.

Type: String

**LastModifiedTime** *(p. 133)*

The date and time when the cache policy was last modified.

Type: Timestamp

**Errors**

For information about the errors that are common to all actions, see Common Errors *(p. 555)*.

**AccessDenied**

Access denied.
HTTP Status Code: 403
**NoSuchCachePolicy**

The cache policy 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 V2
- AWS SDK for JavaScript
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3
GetCachePolicyConfig

Gets a cache policy configuration.

To get a cache policy configuration, you must provide the policy's identifier. If the cache policy is attached to a distribution's cache behavior, you can get the policy's identifier using ListDistributions or GetDistribution. If the cache policy is not attached to a cache behavior, you can get the identifier using ListCachePolicies.

**Request Syntax**

```
GET /2020-05-31/cache-policy/Id/config HTTP/1.1
```

**URI Request Parameters**

The request uses the following URI parameters.

**Id (p. 136)**

The unique identifier for the cache policy. If the cache policy is attached to a distribution's cache behavior, you can get the policy's identifier using ListDistributions or GetDistribution. If the cache policy is not attached to a cache behavior, you can get the identifier using ListCachePolicies.

Required: Yes

**Request Body**

The request does not have a request body.

**Response Syntax**

```
HTTP/1.1 200
<?xml version="1.0" encoding="UTF-8"?>
<CachePolicyConfig>
  <Comment>string</Comment>
  <DefaultTTL>long</DefaultTTL>
  <MaxTTL>long</MaxTTL>
  <MinTTL>long</MinTTL>
  <Name>string</Name>
  <ParametersInCacheKeyAndForwardedToOrigin>
    <CookiesConfig>
      <CookieBehavior>string</CookieBehavior>
      <Cookies>
        <Items>
          <Name>string</Name>
        </Items>
        <Quantity>integer</Quantity>
      </Cookies>
    </CookiesConfig>
    <EnableAcceptEncodingBrotli>boolean</EnableAcceptEncodingBrotli>
    <EnableAcceptEncodingGzip>boolean</EnableAcceptEncodingGzip>
    <HeadersConfig>
      <HeaderBehavior>string</HeaderBehavior>
      <Headers>
```

API Version 2020-05-31

136
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.

**CachePolicyConfig (p. 136)**

Root level tag for the CachePolicyConfig parameters.

Required: Yes

**Comment (p. 136)**

A comment to describe the cache policy. The comment cannot be longer than 128 characters.

Type: String

**DefaultTTL (p. 136)**

The default amount of time, in seconds, that you want objects to stay in the CloudFront cache before CloudFront sends another request to the origin to see if the object has been updated. CloudFront uses this value as the object’s time to live (TTL) only when the origin does not send Cache-Control or Expires headers with the object. For more information, see Managing How Long Content Stays in an Edge Cache (Expiration) in the Amazon CloudFront Developer Guide.

The default value for this field is 86400 seconds (one day). If the value of MinTTL is more than 86400 seconds, then the default value for this field is the same as the value of MinTTL.

Type: Long

**MaxTTL (p. 136)**

The maximum amount of time, in seconds, that objects stay in the CloudFront cache before CloudFront sends another request to the origin to see if the object has been updated. CloudFront uses this value only when the origin sends Cache-Control or Expires headers with the object. For more information, see Managing How Long Content Stays in an Edge Cache (Expiration) in the Amazon CloudFront Developer Guide.

The default value for this field is 31536000 seconds (one year). If the value of MinTTL or DefaultTTL is more than 31536000 seconds, then the default value for this field is the same as the value of DefaultTTL.

Type: Long
**MinTTL (p. 136)**

The minimum amount of time, in seconds, that you want objects to stay in the CloudFront cache before CloudFront sends another request to the origin to see if the object has been updated. For more information, see Managing How Long Content Stays in an Edge Cache (Expiration) in the Amazon CloudFront Developer Guide.

Type: Long

**Name (p. 136)**

A unique name to identify the cache policy.

Type: String

**ParametersInCacheKeyAndForwardedToOrigin (p. 136)**

The HTTP headers, cookies, and URL query strings to include in the cache key. The values included in the cache key are automatically included in requests that CloudFront sends to the origin.

Type: ParametersInCacheKeyAndForwardedToOrigin (p. 489) object

---

**Errors**

For information about the errors that are common to all actions, see Common Errors (p. 555).

**AccessDenied**

Access denied.

HTTP Status Code: 403

**NoSuchCachePolicy**

The cache policy 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 V2
- AWS SDK for JavaScript
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3
GetCloudFrontOriginAccessIdentity

Get the information about an origin access identity.

Request Syntax

```
GET /2020-05-31/origin-access-identity/cloudfront/Id HTTP/1.1
```

URI Request Parameters

The request uses the following URI parameters.

**Id (p. 139)**

The identity's ID.

Required: Yes

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. 139)**

Root level tag for the CloudFrontOriginAccessIdentity parameters.

Required: Yes

**CloudFrontOriginAccessIdentityConfig (p. 139)**

The current configuration information for the identity.

Type: CloudFrontOriginAccessIdentityConfig (p. 389) object

**Id (p. 139)**

The ID for the origin access identity, for example, E74FTE3A7FJ256A.
Type: String

**S3CanonicalUserId (p. 139)**

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. 555).

**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 V2
- AWS SDK for JavaScript
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3
GetCloudFrontOriginAccessIdentityConfig

Get the configuration information about an origin access identity.

Request Syntax

GET /2020-05-31/origin-access-identity/cloudfront/<Id>/config HTTP/1.1

URI Request Parameters

The request uses the following URI parameters.

Id (p. 141)

The identity’s ID.

Required: Yes

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. 141)

Root level tag for the CloudFrontOriginAccessIdentityConfig parameters.

Required: Yes

CallerReference (p. 141)

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 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.

API Version 2020-05-31

141
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. 141)

A comment to describe the origin access identity. The comment cannot be longer than 128 characters.

Type: String

Errors

For information about the errors that are common to all actions, see Common Errors (p. 555).

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

Get the information about a distribution.

Request Syntax

GET /2020-05-31/distribution/Id HTTP/1.1

URI Request Parameters

The request uses the following URI parameters.

Id (p. 143)

The distribution's ID. If the ID is empty, an empty distribution configuration is returned.

Required: Yes

Request Body

The request does not have a request body.

Response Syntax

HTTP/1.1 200
<?xml version="1.0" encoding="UTF-8"?>
<Distribution>
  <ActiveTrustedKeyGroups>
    <Enabled>boolean</Enabled>
    <Items>
      <KeyGroup>
        <KeyGroupId>string</KeyGroupId>
        <KeyPairIds>
          <Items>
            <KeyPairId>string</KeyPairId>
          </Items>
        </KeyPairIds>
        <Quantity>integer</Quantity>
      </KeyGroup>
    </Items>
    <Quantity>integer</Quantity>
  </ActiveTrustedKeyGroups>
  <ActiveTrustedSigners>
    <Enabled>boolean</Enabled>
    <Items>
      <Signer>
        <AwsAccountNumber>string</AwsAccountNumber>
      </Signer>
      <KeyPairIds>
        <Items>
          <KeyPairId>string</KeyPairId>
        </Items>
      </KeyPairIds>
      <Quantity>integer</Quantity>
    </Items>
    <Quantity>integer</Quantity>
  </ActiveTrustedSigners>
</Distribution>
</FunctionAssociations>
</LambdaFunctionAssociations>
<Items>
  <LambdaFunctionAssociation>
    <EventType>string</EventType>
    <IncludeBody>boolean</IncludeBody>
    <LambdaFunctionARN>string</LambdaFunctionARN>
  </LambdaFunctionAssociation>
</Items>
<Quantity>integer</Quantity>
</LambdaFunctionAssociations>
</MaxTTL>long</MaxTTL>
</MinTTL>long</MinTTL>
<OriginRequestPolicyId>string</OriginRequestPolicyId>
<PathPattern>string</PathPattern>
<RealtimeLogConfigArn>string</RealtimeLogConfigArn>
<ResponseHeadersPolicyId>string</ResponseHeadersPolicyId>
<SmoothStreaming>boolean</SmoothStreaming>
<TargetOriginId>string</TargetOriginId>
<TrustedKeyGroups>
  <Enabled>boolean</Enabled>
  <Items>
    <KeyGroup>string</KeyGroup>
  </Items>
  <Quantity>integer</Quantity>
</TrustedKeyGroups>
<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>
    <Quantity>integer</Quantity>
  </Items>
</AllowedMethods>
<CachePolicyId>string</CachePolicyId>
<Compress>boolean</Compress>

API Version 2020-05-31
145
<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>
  <QueryString>boolean</QueryString>
  <QueryStringCacheKeys>
    <Items>
      <Name>string</Name>
    </Items>
  </QueryStringCacheKeys>
</ForwardedValues>

<FunctionAssociations>
  <Items>
    <FunctionAssociation>
      <eventType>string</EventType>
      <FunctionARN>string</FunctionARN>
    </FunctionAssociation>
  </Items>
</FunctionAssociations>

<LambdaFunctionAssociations>
  <Items>
    <LambdaFunctionAssociation>
      <eventType>string</EventType>
      <IncludeBody>boolean</IncludeBody>
      <LambdaFunctionARN>string</LambdaFunctionARN>
    </LambdaFunctionAssociation>
  </Items>
</LambdaFunctionAssociations>

<MaxTTL>long</MaxTTL>
<MinTTL>long</MinTTL>
<OriginRequestPolicyId>string</OriginRequestPolicyId>
<RealtimeLogConfigArn>string</RealtimeLogConfigArn>
<ResponseHeadersPolicyId>string</ResponseHeadersPolicyId>
<SmoothStreaming>boolean</SmoothStreaming>
<TargetOriginId>string</TargetOriginId>

<TrustedKeyGroups>
  <Enabled>boolean</Enabled>
  <Items>
    <KeyGroup>string</KeyGroup>
  </Items>
</TrustedKeyGroups>

<TrustedSigners>
  <Enabled>boolean</Enabled>
  <Items>
    <AwsAccountNumber>string</AwsAccountNumber>
  </Items>
</TrustedSigners>
<ViewerProtocolPolicy>string</ViewerProtocolPolicy>

<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>

<OriginGroups>
  <Items>
    <OriginGroup>
      <FailoverCriteria>
        <StatusCodes>
          <Items>
            <StatusCode>integer</StatusCode>
          </Items>
        </StatusCodes>
        <Quantity>integer</Quantity>
      </FailoverCriteria>

      <Id>string</Id>

      <Members>
        <Items>
          <OriginGroupMember>
            <OriginId>string</OriginId>
          </OriginGroupMember>
        </Items>
        <Quantity>integer</Quantity>
      </Members>

      <Id>string</Id>

      <Quantity>integer</Quantity>
    </OriginGroups>
  </Items>
</OriginGroups>

<Origins>
  <Items>
  </Items>
</Origins>

<ConnectionAttempts>integer</ConnectionAttempts>

<ConnectionTimeout>integer</ConnectionTimeout>

<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>
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. 143)

Root level tag for the Distribution parameters.

Required: Yes

ActiveTrustedKeyGroups (p. 143)

CloudFront automatically adds this field to the response if you’ve configured a cache behavior in this distribution to serve private content using key groups. This field contains a list of key groups and the public keys in each key group that CloudFront can use to verify the signatures of signed URLs or signed cookies.

Type: ActiveTrustedKeyGroups (p. 367) object

Important
We recommend using TrustedKeyGroups instead of TrustedSigners.
CloudFront automatically adds this field to the response if you've configured a cache behavior in this distribution to serve private content using trusted signers. This field contains a list of AWS account IDs and the active CloudFront key pairs in each account that CloudFront can use to verify the signatures of signed URLs or signed cookies.

Type: `ActiveTrustedSigners (p. 368)` object

**AliasICPRecordals (p. 143)**

AWS services in China customers must file for an Internet Content Provider (ICP) recordal if they want to serve content publicly on an alternate domain name, also known as a CNAME, that they've added to CloudFront. `AliasICPRecordal` provides the ICP recordal status for CNAMEs associated with distributions.

For more information about ICP recordals, see [Signup, Accounts, and Credentials](https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/ICP-recordals.html) in the *Getting Started with AWS services in China*.

Type: Array of `AliasICPRecordal (p. 370)` objects

**ARN (p. 143)**

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. 143)**

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

Type: `DistributionConfig (p. 414)` object

**DomainName (p. 143)**

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

Type: String

**Id (p. 143)**

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

Type: String

**InProgressInvalidationBatches (p. 143)**

The number of invalidation batches currently in progress.

Type: Integer

**LastModifiedTime (p. 143)**

The date and time the distribution was last modified.

Type: Timestamp

**Status (p. 143)**

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. 555).

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

Get the configuration information about a distribution.

**Request Syntax**

```
GET /2020-05-31/distribution/Id/config HTTP/1.1
```

**URI Request Parameters**

The request uses the following URI parameters.

**Id (p. 151)**

The distribution's ID. If the ID is empty, an empty distribution configuration is returned.

Required: Yes

**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>
      <Compress>boolean</Compress>
    </CachedMethods>
    <FieldLevelEncryptionId>string</FieldLevelEncryptionId>
    <ForwardedValues>
      <Cookies>
        <Forward>string</Forward>
        <WhitelistedNames>
```

API Version 2020-05-31
<Items>
  <Name>string</Name>
</Items>
<Quantity>integer</Quantity>
</WhitelistedNames>
</Cookies>
<Headers>
  <Items>
    <Name>string</Name>
  </Items>
  <Quantity>integer</Quantity>
</Headers>
<QueryStringBoolean>boolean</QueryStringBoolean>
<QueryStringCacheKeys>
  <Items>
    <Name>string</Name>
  </Items>
  <Quantity>integer</Quantity>
</QueryStringCacheKeys>
</ForwardedValues>
<FunctionAssociations>
  <Items>
    <FunctionAssociation>
      <EventType>string</EventType>
      <FunctionARN>string</FunctionARN>
    </FunctionAssociation>
  </Items>
  <Quantity>integer</Quantity>
</FunctionAssociations>
<LambdaFunctionAssociations>
  <Items>
    <LambdaFunctionAssociation>
      <EventType>string</EventType>
      <IncludeBody>boolean</IncludeBody>
      <LambdaFunctionARN>string</LambdaFunctionARN>
    </LambdaFunctionAssociation>
  </Items>
  <Quantity>integer</Quantity>
</LambdaFunctionAssociations>
<MaxTTL>long</MaxTTL>
<MinTTL>long</MinTTL>
-OriginRequestPolicyId>string</OriginRequestPolicyId>
<PathPattern>string</PathPattern>
<RealtimeLogConfigArn>string</RealtimeLogConfigArn>
<ResponseHeadersPolicyId>string</ResponseHeadersPolicyId>
<SmoothStreaming>boolean</SmoothStreaming>
<TargetOriginId>string</TargetOriginId>
<TrustedKeyGroups>
  <Enabled>boolean</Enabled>
  <Items>
    <KeyGroup>string</KeyGroup>
  </Items>
  <Quantity>integer</Quantity>
</TrustedKeyGroups>
<TrustedSigners>
  <Enabled>boolean</Enabled>
  <Items>
    <AwsAccountNumber>string</AwsAccountNumber>
  </Items>
  <Quantity>integer</Quantity>
</TrustedSigners>
</ViewerProtocolPolicy>string</ViewerProtocolPolicy>
</CacheBehavior>
</Items>
<Quantity>integer</Quantity>
</CacheBehaviors>
Amazon CloudFront API Reference

Response Syntax

```xml
<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>
      <Method>string</Method>
    </Items>
    <Quantity>integer</Quantity>
  </AllowedMethods>
  <CachePolicyId>string</CachePolicyId>
  <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>
  <FunctionAssociations>
    <Items>
      <FunctionAssociation>
        <EventType>string</EventType>
        <FunctionARN>string</FunctionARN>
      </FunctionAssociation>
    </Items>
    <Quantity>integer</Quantity>
  </FunctionAssociations>
  <LambdaFunctionAssociations>
    <Items>
      <LambdaFunctionAssociation>
        <FunctionARN>string</FunctionARN>
      </LambdaFunctionAssociation>
    </Items>
    <Quantity>integer</Quantity>
  </LambdaFunctionAssociations>
</DefaultCacheBehavior>
```

API Version 2020-05-31

153
<EventType>string</EventType>
<IncludeBody>boolean</IncludeBody>
<LambdaFunctionARN>string</LambdaFunctionARN>
</LambdaFunctionAssociation>
</Items>
<Quantity>integer</Quantity>
</LambdaFunctionAssociations>
<MaxTTL>long</MaxTTL>
<MinTTL>long</MinTTL>
-OriginRequestPolicyId>string</OriginRequestPolicyId>
<RealtimeLogConfigArn>string</RealtimeLogConfigArn>
<ResponseHeadersPolicyId>string</ResponseHeadersPolicyId>
<SmoothStreaming>boolean</SmoothStreaming>
<TargetOriginId>string</TargetOriginId>
</TrustedKeyGroups>
<Enabled>boolean</Enabled>
</Items>
<Quantity>integer</Quantity>
</TrustedSigners>
<Enabled>boolean</Enabled>
</Items>
<Quantity>integer</Quantity>
</TrustedSigners>
</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>
</OriginGroups>
<Items>
-OriginGroup>
<FailoverCriteria>
>StatusCodes>
<Items>
<StatusCode>integer</StatusCode>
</Items>
<Quantity>integer</Quantity>
</StatusCodes>
</FailoverCriteria>
<Id>string</Id>
<Members>
<Items>
-OriginGroupMember>
-OriginId>string</OriginId>
</OriginGroupMember>
</Items>
<Quantity>integer</Quantity>
</Members>
</OriginGroup>
</Items>
</Origins>
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. 151)**

Root level tag for the DistributionConfig parameters.

Required: Yes

**Aliases (p. 151)**

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

Type: Aliases (p. 369) object

**CacheBehaviors (p. 151)**

A complex type that contains zero or more CacheBehavior elements.

Type: CacheBehaviors (p. 378) object

**CallerReference (p. 151)**

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 that you already sent in a previous request to create a distribution, CloudFront returns a DistributionAlreadyExists error.

Type: String

**Comment (p. 151)**

An optional comment to describe the distribution. The comment cannot be longer than 128 characters.

Type: String

**CustomErrorResponses (p. 151)**

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. 403) object

**DefaultCacheBehavior (p. 151)**

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. 407) object

**DefaultRootObject (p. 151)**

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. 151)

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

Type: Boolean

HttpVersion (p. 151)

(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. 151)

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 AWS Integration 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 AWS Integration Developer Guide.
If you created a CNAME resource record set, either with Amazon Route 53 AWS Integration 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. 151)

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. 466) object

OriginGroups (p. 151)

A complex type that contains information about origin groups for this distribution.

Type: OriginGroups (p. 477) object

Origins (p. 151)

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

Type: Origins (p. 486) object

PriceClass (p. 151)

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 (such as Price Class 100) map to CloudFront regions, see Amazon CloudFront Pricing.

Type: String

Valid Values: PriceClass_100 | PriceClass_200 | PriceClass_All

Restrictions (p. 151)

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

Type: Restrictions (p. 528) object

ViewerCertificate (p. 151)

A complex type that determines the distribution’s SSL/TLS configuration for communicating with viewers.

Type: ViewerCertificate (p. 549) object

WebACLId (p. 151)

A unique identifier that specifies the AWS WAF web ACL, if any, to associate with this distribution. To specify a web ACL created using the latest version of AWS WAF, use the ACL ARN, for example arn:aws:wafv2:us-east-1:123456789012:global/webacl/ExampleWebACL/473e64fd-f30b-4765-81a0-62ad96dd167a. To specify a web ACL created using AWS WAF Classic, use the ACL ID, for example 473e64fd-f30b-4765-81a0-62ad96dd167a.
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. 555).

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

Get the field-level encryption configuration information.

Request Syntax

GET /2020-05-31/field-level-encryption/Id HTTP/1.1

URI Request Parameters

The request uses the following URI parameters.

Id (p. 160)

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

Required: Yes

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>
      <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>
</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. 160)

Root level tag for the FieldLevelEncryption parameters.

Required: Yes

FieldLevelEncryptionConfig (p. 160)

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

Type: FieldLevelEncryptionConfig (p. 431) object

Id (p. 160)

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. 160)

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. 555).

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
See Also

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

Get the field-level encryption configuration information.

Request Syntax

```
GET /2020-05-31/field-level-encryption/Id/config HTTP/1.1
```

URI Request Parameters

The request uses the following URI parameters.

Id (p. 163)

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

Required: Yes

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>
      <Quantity>integer</Quantity>
    </ContentTypeProfiles>
  </ContentTypeProfileConfig>
  <QueryArgProfileConfig>
    <ForwardWhenQueryArgProfileIsUnknown>boolean</ForwardWhenQueryArgProfileIsUnknown>
    <QueryArgProfiles>
      <Items>
        <QueryArgProfile>
          <ProfileId>string</ProfileId>
          <QueryArg>string</QueryArg>
        </QueryArgProfile>
      </Items>
      <Quantity>integer</Quantity>
    </QueryArgProfiles>
  </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. 163)**

Root level tag for the FieldLevelEncryptionConfig parameters.

Required: Yes

**CallerReference (p. 163)**

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

Type: String

**Comment (p. 163)**

An optional comment about the configuration. The comment cannot be longer than 128 characters.

Type: String

**ContentTypeProfileConfig (p. 163)**

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. 396) object

**QueryArgProfileConfig (p. 163)**

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. 497) object

Errors

For information about the errors that are common to all actions, see Common Errors (p. 555).

**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 V2
• AWS SDK for JavaScript
• AWS SDK for PHP V3
• AWS SDK for Python
• AWS SDK for Ruby V3
GetFieldLevelEncryptionProfile

Get the field-level encryption profile information.

**Request Syntax**

```
GET /2020-05-31/field-level-encryption-profile/Id HTTP/1.1
```

**URI Request Parameters**

The request uses the following URI parameters.

**Id (p. 166)**

- Get the ID for the field-level encryption profile information.
- Required: Yes

**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. 166)**

Root level tag for the FieldLevelEncryptionProfile parameters.

Required: Yes

**FieldLevelEncryptionProfileConfig (p. 166)**

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

Type: FieldLevelEncryptionProfileConfig (p. 434) object

**Id (p. 166)**

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. 166)**

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. 555).

**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 V2
- AWS SDK for JavaScript
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3
GetFieldLevelEncryptionProfileConfig

Get the field-level encryption profile configuration information.

Request Syntax

GET /2020-05-31/field-level-encryption-profile/Id/config HTTP/1.1

URI Request Parameters

The request uses the following URI parameters.

Id (p. 169)

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

Required: Yes

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>
  </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. 169)

Root level tag for the FieldLevelEncryptionProfileConfig parameters.
Required: Yes

**CallerReference (p. 169)**

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

Type: String

**Comment (p. 169)**

An optional comment for the field-level encryption profile. The comment cannot be longer than 128 characters.

Type: String

**EncryptionEntities (p. 169)**

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. 427)` object

**Name (p. 169)**

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. 555)](#).

**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 V2
- AWS SDK for JavaScript
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3
GetFunction

Gets the code of a CloudFront function. To get configuration information and metadata about a function, use DescribeFunction.

To get a function’s code, you must provide the function’s name and stage. To get these values, you can use ListFunctions.

Request Syntax

GET /2020-05-31/function/Name?Stage=Stage HTTP/1.1

URI Request Parameters

The request uses the following URI parameters.

Name (p. 171)

The name of the function whose code you are getting.

Required: Yes

Stage (p. 171)

The function’s stage, either DEVELOPMENT or LIVE.

Valid Values: DEVELOPMENT | LIVE

Request Body

The request does not have a request body.

Response Syntax

HTTP/1.1 200

Response Elements

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

Errors

For information about the errors that are common to all actions, see Common Errors (p. 555).

NoSuchFunctionExists

The function does not exist.

HTTP Status Code: 404

UnsupportedOperation

This operation is not supported in this region.
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 V2
- AWS SDK for JavaScript
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3
GetInvalidation

Get the information about an invalidation.

Request Syntax

GET /2020-05-31/distribution/DistributionId/invalidation/Id HTTP/1.1

URI Request Parameters

The request uses the following URI parameters.

DistributionId (p. 173)

The distribution's ID.

Required: Yes

Id (p. 173)

The identifier for the invalidation request, for example, IDFDVBD632BHDSS.

Required: Yes

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. 173)

Root level tag for the Invalidation parameters.
Required: Yes

CreateTime (p. 173)

The date and time the invalidation request was first made.
Type: Timestamp

Id (p. 173)

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

InvalidationBatch (p. 173)

The current invalidation information for the batch request.
Type: InvalidationBatch (p. 452) object

Status (p. 173)

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. 555).

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 V2
- AWS SDK for JavaScript
- AWS SDK for PHP V3
• AWS SDK for Python
• AWS SDK for Ruby V3
GetKeyGroup

Gets a key group, including the date and time when the key group was last modified.

To get a key group, you must provide the key group's identifier. If the key group is referenced in a distribution's cache behavior, you can get the key group's identifier using ListDistributions or GetDistribution. If the key group is not referenced in a cache behavior, you can get the identifier using ListKeyGroups.

Request Syntax

GET /2020-05-31/key-group/Id HTTP/1.1

URI Request Parameters

The request uses the following URI parameters.

Id (p. 176)

The identifier of the key group that you are getting. To get the identifier, use ListKeyGroups.

Required: Yes

Request Body

The request does not have a request body.

Response Syntax

HTTP/1.1 200
<?xml version="1.0" encoding="UTF-8"?>
<KeyGroup>
  <Id>string</Id>
  <KeyGroupConfig>
    <Comment>string</Comment>
    <Items>
      <PublicKey>string</PublicKey>
    </Items>
    <Name>string</Name>
  </KeyGroupConfig>
  <LastModifiedTime>timestamp</LastModifiedTime>
</KeyGroup>

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.

KeyGroup (p. 176)

Root level tag for the KeyGroup parameters.

Required: Yes
Id (p. 176)
The identifier for the key group.
Type: String

KeyGroupConfig (p. 176)
The key group configuration.
Type: KeyGroupConfig (p. 457) object

LastModifiedTime (p. 176)
The date and time when the key group was last modified.
Type: Timestamp

Errors

For information about the errors that are common to all actions, see Common Errors (p. 555).

NoSuchResource
A resource that was specified is not valid.
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 V2
- AWS SDK for JavaScript
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3
GetKeyGroupConfig

Gets a key group configuration.

To get a key group configuration, you must provide the key group's identifier. If the key group is referenced in a distribution’s cache behavior, you can get the key group’s identifier using ListDistributions or GetDistribution. If the key group is not referenced in a cache behavior, you can get the identifier using ListKeyGroups.

Request Syntax

```
GET /2020-05-31/key-group/Id/config HTTP/1.1
```

URI Request Parameters

The request uses the following URI parameters.

**Id (p. 178)**

The identifier of the key group whose configuration you are getting. To get the identifier, use ListKeyGroups.

Required: Yes

Request Body

The request does not have a request body.

Response Syntax

```
HTTP/1.1 200
<?xml version="1.0" encoding="UTF-8"?>
<KeyGroupConfig>
  <Comment>string</Comment>
  <Items>
    <PublicKey>string</PublicKey>
  </Items>
  <Name>string</Name>
</KeyGroupConfig>
```

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.

**KeyGroupConfig (p. 178)**

Root level tag for the KeyGroupConfig parameters.

Required: Yes

**Comment (p. 178)**

A comment to describe the key group. The comment cannot be longer than 128 characters.
Errors

For information about the errors that are common to all actions, see Common Errors (p. 555).

NoSuchResource

A resource that was specified is not valid.

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

Gets information about whether additional CloudWatch metrics are enabled for the specified CloudFront distribution.

Request Syntax

```
GET /2020-05-31/distributions/DistributionId/monitoring-subscription HTTP/1.1
```

URI Request Parameters

The request uses the following URI parameters.

- **DistributionId** (p. 180)
  - The ID of the distribution that you are getting metrics information for.
  - Required: Yes

Request Body

The request does not have a request body.

Response Syntax

```
HTTP/1.1 200
<?xml version="1.0" encoding="UTF-8"?>
<MonitoringSubscription>
  <RealtimeMetricsSubscriptionConfig>
    <RealtimeMetricsSubscriptionStatus>string</RealtimeMetricsSubscriptionStatus>
  </RealtimeMetricsSubscriptionConfig>
</MonitoringSubscription>
```

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.

- **MonitoringSubscription** (p. 180)
  - Root level tag for the MonitoringSubscription parameters.
  - Required: Yes
- **RealtimeMetricsSubscriptionConfig** (p. 180)
  - A subscription configuration for additional CloudWatch metrics.
  - Type: `RealtimeMetricsSubscriptionConfig` (p. 504) object

Errors

For information about the errors that are common to all actions, see `Common Errors (p. 555)`.
**AccessDenied**

Access denied.

HTTP Status Code: 403

**NoSuchDistribution**

The specified distribution does not exist.

HTTP Status Code: 404

**UnsupportedOperation**

This operation is not supported in this region.

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

Gets an origin request policy, including the following metadata:

- The policy's identifier.
- The date and time when the policy was last modified.

To get an origin request policy, you must provide the policy's identifier. If the origin request policy is attached to a distribution's cache behavior, you can get the policy's identifier using ListDistributions or GetDistribution. If the origin request policy is not attached to a cache behavior, you can get the identifier using ListOriginRequestPolicies.

**Request Syntax**

GET /2020-05-31/origin-request-policy/[Id] HTTP/1.1

**URI Request Parameters**

The request uses the following URI parameters.

**Id (p. 182)**

The unique identifier for the origin request policy. If the origin request policy is attached to a distribution's cache behavior, you can get the policy's identifier using ListDistributions or GetDistribution. If the origin request policy is not attached to a cache behavior, you can get the identifier using ListOriginRequestPolicies.

Required: Yes

**Request Body**

The request does not have a request body.

**Response Syntax**

```
HTTP/1.1 200
<?xml version="1.0" encoding="UTF-8"?>
<OriginRequestPolicy>
  <Id>string</Id>
  <LastModifiedTime>timestamp</LastModifiedTime>
  <OriginRequestPolicyConfig>
    <Comment>string</Comment>
    <CookiesConfig>
      <CookieBehavior>string</CookieBehavior>
      <Cookies>
        <Items>
          <Name>string</Name>
        </Items>
        <Quantity>integer</Quantity>
      </Cookies>
    </CookiesConfig>
    <HeadersConfig>
      <HeaderBehavior>string</HeaderBehavior>
      <Headers/>
    </HeadersConfig>
  </OriginRequestPolicyConfig>
</OriginRequestPolicy>
```
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.

**OriginRequestPolicy (p. 182)**

Root level tag for the OriginRequestPolicy parameters.

Required: Yes
Id (p. 182)

The unique identifier for the origin request policy.

Type: String

**LastModifiedTime (p. 182)**

The date and time when the origin request policy was last modified.

Type: Timestamp

**OriginRequestPolicyConfig (p. 182)**

The origin request policy configuration.

Type: OriginRequestPolicyConfig (p. 479) object

**Errors**

For information about the errors that are common to all actions, see Common Errors (p. 555).

**AccessDenied**

Access denied.

HTTP Status Code: 403

**NoSuchOriginRequestPolicy**

The origin request policy 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 V2
- AWS SDK for JavaScript
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3
GetOriginRequestPolicyConfig

Gets an origin request policy configuration.

To get an origin request policy configuration, you must provide the policy's identifier. If the origin request policy is attached to a distribution's cache behavior, you can get the policy's identifier using ListDistributions or GetDistribution. If the origin request policy is not attached to a cache behavior, you can get the identifier using ListOriginRequestPolicies.

Request Syntax

GET /2020-05-31/origin-request-policy/Id/config HTTP/1.1

URI Request Parameters

The request uses the following URI parameters.

Id (p. 185)

The unique identifier for the origin request policy. If the origin request policy is attached to a distribution's cache behavior, you can get the policy's identifier using ListDistributions or GetDistribution. If the origin request policy is not attached to a cache behavior, you can get the identifier using ListOriginRequestPolicies.

Required: Yes

Request Body

The request does not have a request body.

Response Syntax

HTTP/1.1 200
<?xml version="1.0" encoding="UTF-8"?>
<OriginRequestPolicyConfig>
  <Comment>string</Comment>
  <CookiesConfig>
    <CookieBehavior>string</CookieBehavior>
    <Cookies>
      <Items>
        <Name>string</Name>
      </Items>
      <Quantity>integer</Quantity>
    </Cookies>
  </CookiesConfig>
  <HeadersConfig>
    <HeaderBehavior>string</HeaderBehavior>
    <Headers>
      <Items>
        <Name>string</Name>
      </Items>
      <Quantity>integer</Quantity>
    </Headers>
  </HeadersConfig>
</OriginRequestPolicyConfig>
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.

**OriginRequestPolicyConfig (p. 185)**

Root level tag for the OriginRequestPolicyConfig parameters.

Required: Yes

**Comment (p. 185)**

A comment to describe the origin request policy. The comment cannot be longer than 128 characters.

Type: String

**CookiesConfig (p. 185)**

The cookies from viewer requests to include in origin requests.

Type: OriginRequestPolicyCookiesConfig (p. 481) object

**HeadersConfig (p. 185)**

The HTTP headers to include in origin requests. These can include headers from viewer requests and additional headers added by CloudFront.

Type: OriginRequestPolicyHeadersConfig (p. 482) object

**Name (p. 185)**

A unique name to identify the origin request policy.

Type: String

**QueryStringsConfig (p. 185)**

The URL query strings from viewer requests to include in origin requests.

Type: OriginRequestPolicyQueryStringsConfig (p. 484) object

**Errors**

For information about the errors that are common to all actions, see Common Errors (p. 555).

**AccessDenied**

Access denied.
HTTP Status Code: 403

NoSuchOriginRequestPolicy

The origin request policy 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 V2
- AWS SDK for JavaScript
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3
GetPublicKeyp

Gets a public key.

**Request Syntax**

```
GET /2020-05-31/public-key/Id HTTP/1.1
```

**URI Request Parameters**

The request uses the following URI parameters.

**Id** *(p. 188)*

The identifier of the public key you are getting.

Required: Yes

**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. 188)*

Root level tag for the PublicKey parameters.

Required: Yes

**CreatedTime** *(p. 188)*

The date and time when the public key was uploaded.

Type: Timestamp
Id (p. 188)

The identifier of the public key.

Type: String

PublicKeyConfig (p. 188)

Configuration information about a public key that you can use with signed URLs and signed cookies, or with field-level encryption.

Type: PublicKeyConfig (p. 493) object

Errors

For information about the errors that are common to all actions, see Common Errors (p. 555).

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

Gets a public key configuration.

Request Syntax

```
GET /2020-05-31/public-key/Id/config HTTP/1.1
```

URI Request Parameters

The request uses the following URI parameters.

**Id (p. 190)**

The identifier of the public key whose configuration you are getting.

Required: Yes

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. 190)**

Root level tag for the PublicKeyConfig parameters.

Required: Yes

**CallerReference (p. 190)**

A string included in the request to help make sure that the request can’t be replayed.

Type: String

**Comment (p. 190)**

A comment to describe the public key. The comment cannot be longer than 128 characters.
Type: String

EncodedKey (p. 190)

The public key that you can use with signed URLs and signed cookies, or with field-level encryption.

Type: String

Name (p. 190)

A name to help identify the public key.

Type: String

Errors

For information about the errors that are common to all actions, see Common Errors (p. 555).

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

Gets a real-time log configuration.

To get a real-time log configuration, you can provide the configuration's name or its Amazon Resource Name (ARN). You must provide at least one. If you provide both, CloudFront uses the name to identify the real-time log configuration to get.

Request Syntax

```
POST /2020-05-31/get-realtime-log-config/ HTTP/1.1
<?xml version="1.0" encoding="UTF-8"?>
  <ARN>string</ARN>
  <Name>string</Name>
</GetRealtimeLogConfigRequest>
```

URI Request Parameters

The request does not use any URI parameters.

Request Body

The request accepts the following data in XML format.

GetRealtimeLogConfigRequest (p. 192)

Root level tag for the GetRealtimeLogConfigRequest parameters.

Required: Yes

ARN (p. 192)

The Amazon Resource Name (ARN) of the real-time log configuration to get.

Type: String

Required: No

Name (p. 192)

The name of the real-time log configuration to get.

Type: String

Required: No

Response Syntax

```
HTTP/1.1 200
<?xml version="1.0" encoding="UTF-8"?>
<GetRealtimeLogConfigResult>
  <RealtimeLogConfig>
    <ARN>string</ARN>
    <EndPoints>
      <EndPoint>
      ...
      </EndPoint>
    </EndPoints>
  </RealtimeLogConfig>
</GetRealtimeLogConfigResult>
```
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.

GetRealtimeLogConfigResult (p. 192)

Root level tag for the GetRealtimeLogConfigResult parameters.

Required: Yes

RealtimeLogConfig (p. 192)

A real-time log configuration.

Type: RealtimeLogConfig (p. 501) object

Errors

For information about the errors that are common to all actions, see Common Errors (p. 555).

AccessDenied

Access denied.

HTTP Status Code: 403

InvalidArgument

An argument is invalid.

HTTP Status Code: 400

NoSuchRealtimeLogConfig

The real-time log configuration 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 V2
• AWS SDK for JavaScript
• AWS SDK for PHP V3
• AWS SDK for Python
• AWS SDK for Ruby V3
GetResponseHeadersPolicy

Gets a response headers policy, including metadata (the policy's identifier and the date and time when
the policy was last modified).

To get a response headers policy, you must provide the policy's identifier. If the response headers
policy is attached to a distribution's cache behavior, you can get the policy's identifier using
ListDistributions or GetDistribution. If the response headers policy is not attached to a cache
behavior, you can get the identifier using ListResponseHeadersPolicies.

Request Syntax

GET /2020-05-31/response-headers-policy/Id HTTP/1.1

URI Request Parameters

The request uses the following URI parameters.

Id (p. 195)

The identifier for the response headers policy.

If the response headers policy is attached to a distribution's cache behavior, you can get the policy's
identifier using ListDistributions or GetDistribution. If the response headers policy is not
attached to a cache behavior, you can get the identifier using ListResponseHeadersPolicies.

Required: Yes

Request Body

The request does not have a request body.

Response Syntax

HTTP/1.1 200
<?xml version="1.0" encoding="UTF-8"?>
<ResponseHeadersPolicy>
  <Id>string</Id>
  <LastModifiedTime>timestamp</LastModifiedTime>
  <ResponseHeadersPolicyConfig>
    <Comment>string</Comment>
    <CorsConfig>
      <AccessControlAllowCredentials>boolean</AccessControlAllowCredentials>
      <AccessControlAllowHeaders>
        <Items>
          <Header>string</Header>
        </Items>
      </AccessControlAllowHeaders>
      <AccessControlAllowMethods>
        <Items>
          <Method>string</Method>
        </Items>
      </AccessControlAllowMethods>
      <AccessControlAllowOrigins>
      </AccessControlAllowOrigins>
    </CorsConfig>
  </ResponseHeadersPolicyConfig>
</ResponseHeadersPolicy>
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.

**ResponseHeadersPolicy (p. 195)**

Root level tag for the ResponseHeadersPolicy parameters.

Required: Yes

**Id (p. 195)**

The identifier for the response headers policy.

Type: String

**LastModifiedTime (p. 195)**

The date and time when the response headers policy was last modified.

Type: Timestamp

**ResponseHeadersPolicyConfig (p. 195)**

A response headers policy configuration.

A response headers policy contains information about a set of HTTP response headers and their values. CloudFront adds the headers in the policy to HTTP responses that it sends for requests that match a cache behavior that's associated with the policy.

Type: ResponseHeadersPolicyConfig (p. 510) object

---

**Errors**

For information about the errors that are common to all actions, see Common Errors (p. 555).

**AccessDenied**

Access denied.

HTTP Status Code: 403

**NoSuchResponseHeadersPolicy**

The response headers policy 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 V2
- AWS SDK for JavaScript
- AWS SDK for PHP V3
- AWS SDK for Python
• AWS SDK for Ruby V3
GetResponseHeadersPolicyConfig

Gets a response headers policy configuration.

To get a response headers policy configuration, you must provide the policy's identifier. If the response headers policy is attached to a distribution's cache behavior, you can get the policy's identifier using ListDistributions or GetDistribution. If the response headers policy is not attached to a cache behavior, you can get the identifier using ListResponseHeadersPolicies.

Request Syntax

GET /2020-05-31/response-headers-policy/Id/config HTTP/1.1

URI Request Parameters

The request uses the following URI parameters.

Id (p. 199)

The identifier for the response headers policy.

If the response headers policy is attached to a distribution's cache behavior, you can get the policy's identifier using ListDistributions or GetDistribution. If the response headers policy is not attached to a cache behavior, you can get the identifier using ListResponseHeadersPolicies.

Required: Yes

Request Body

The request does not have a request body.

Response Syntax

HTTP/1.1 200
<?xml version="1.0" encoding="UTF-8"?>
<ResponseHeadersPolicyConfig>
  <Comment>string</Comment>
  <CorsConfig>
    <AccessControlAllowCredentials>boolean</AccessControlAllowCredentials>
    <AccessControlAllowHeaders>
      <Items>
        <Header>string</Header>
      </Items>
    </AccessControlAllowHeaders>
    <AccessControlAllowMethods>
      <Items>
        <Method>string</Method>
      </Items>
    </AccessControlAllowMethods>
    <AccessControlAllowOrigins>
      <Items>
        <Origin>string</Origin>
      </Items>
    </AccessControlAllowOrigins>
  </CorsConfig>
</ResponseHeadersPolicyConfig>
<AccessControlExposeHeaders>
  <Items>
    <Header>string</Header>
  </Items>
  <Quantity>integer</Quantity>
</AccessControlExposeHeaders>

<AccessControlMaxAgeSec>integer</AccessControlMaxAgeSec>

<OriginOverride>boolean</OriginOverride>

</CorsConfig>

<CustomHeadersConfig>
  <Items>
    <ResponseHeadersPolicyCustomHeader>
      <Header>string</Header>
      <Override>boolean</Override>
      <Value>string</Value>
    </ResponseHeadersPolicyCustomHeader>
  </Items>
  <Quantity>integer</Quantity>
</CustomHeadersConfig>

<Name>string</Name>

<SecurityHeadersConfig>
  <ContentSecurityPolicy>
    <ContentSecurityPolicy>string</ContentSecurityPolicy>
    <Override>boolean</Override>
  </ContentSecurityPolicy>
  <ContentTypeOptions>
    <Override>boolean</Override>
  </ContentTypeOptions>
  <FrameOptions>
    <FrameOption>string</FrameOption>
    <Override>boolean</Override>
  </FrameOptions>
  <ReferrerPolicy>
    <Override>boolean</Override>
  </ReferrerPolicy>
  <StrictTransportSecurity>
    <AccessControlMaxAgeSec>integer</AccessControlMaxAgeSec>
    <IncludeSubdomains>boolean</IncludeSubdomains>
    <Override>boolean</Override>
    <Preload>boolean</Preload>
  </StrictTransportSecurity>
  <XSSProtection>
    <ModeBlock>boolean</ModeBlock>
    <Override>boolean</Override>
    <Protection>boolean</Protection>
    <ReportUri>string</ReportUri>
  </XSSProtection>
</SecurityHeadersConfig>

<ServerTimingHeadersConfig>
  <Enabled>boolean</Enabled>
  <SamplingRate>double</SamplingRate>
</ServerTimingHeadersConfig>

</ResponseHeadersPolicyConfig>

---

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.

**ResponseHeadersPolicyConfig (p. 199)**

Root level tag for the ResponseHeadersPolicyConfig parameters.
Required: Yes

**Comment (p. 199)**

A comment to describe the response headers policy.

The comment cannot be longer than 128 characters.

Type: String

**CorsConfig (p. 199)**

A configuration for a set of HTTP response headers that are used for cross-origin resource sharing (CORS).

Type: ResponseHeadersPolicyCorsConfig (p. 514) object

**CustomHeadersConfig (p. 199)**

A configuration for a set of custom HTTP response headers.

Type: ResponseHeadersPolicyCustomHeadersConfig (p. 517) object

**Name (p. 199)**

A name to identify the response headers policy.

The name must be unique for response headers policies in this AWS account.

Type: String

**SecurityHeadersConfig (p. 199)**

A configuration for a set of security-related HTTP response headers.

Type: ResponseHeadersPolicySecurityHeadersConfig (p. 521) object

**ServerTimingHeadersConfig (p. 199)**

A configuration for enabling the Server-Timing header in HTTP responses sent from CloudFront.

Type: ResponseHeadersPolicyServerTimingHeadersConfig (p. 523) object

---

**Errors**

For information about the errors that are common to all actions, see [Common Errors (p. 555)].

**AccessDenied**

Access denied.

HTTP Status Code: 403

**NoSuchResponseHeadersPolicy**

The response headers policy 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:
See Also

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

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

Request Syntax

```
GET /2020-05-31/streaming-distribution/Id HTTP/1.1
```

URI Request Parameters

The request uses the following URI parameters.

**Id (p. 203)**

The streaming distribution's ID.

Required: Yes

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>
        </KeyPairIds>
        <Quantity>integer</Quantity>
      </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>
```

API Version 2020-05-31

203
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. 203)

Root level tag for the StreamingDistribution parameters.

Required: Yes

ActiveTrustedSigners (p. 203)

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. 368) object

ARN (p. 203)

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

DomainName (p. 203)

The domain name that corresponds to the streaming distribution, for example, s5c39ggb8ow64r.cloudfront.net.

Type: String
Id (p. 203)

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

Type: String

LastModifiedTime (p. 203)

The date and time that the distribution was last modified.

Type: Timestamp

Status (p. 203)

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. 203)

The current configuration information for the RTMP distribution.

Type: StreamingDistributionConfig (p. 535) object

Errors

For information about the errors that are common to all actions, see Common Errors (p. 555).

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

Get the configuration information about a streaming distribution.

Request Syntax

GET /2020-05-31/streaming-distribution/Id/config HTTP/1.1

URI Request Parameters

The request uses the following URI parameters.

Id (p. 206)

The streaming distribution's ID.

Required: Yes

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. 206)

Root level tag for the StreamingDistributionConfig parameters.

Required: Yes

Aliases (p. 206)

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

Type: Aliases (p. 369) object

CallerReference (p. 206)

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 StreamingDistributionConfig object), CloudFront creates a new distribution.

If CallerReference is a value that you already sent in a previous request to create a distribution, CloudFront returns a DistributionAlreadyExists error.

Type: String

Comment (p. 206)

Any comments you want to include about the streaming distribution.

Type: String

Enabled (p. 206)

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

Type: Boolean

Logging (p. 206)

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

Type: StreamingLoggingConfig (p. 542) object

PriceClass (p. 206)

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. 206)

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. 529) object

TrustedSigners (p. 206)

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

API Version 2020-05-31

207
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. 548) object

Errors

For information about the errors that are common to all actions, see Common Errors (p. 555).

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

Gets a list of cache policies.

You can optionally apply a filter to return only the managed policies created by AWS, or only the custom policies created in your AWS account.

You can optionally specify the maximum number of items to receive in the response. If the total number of items in the list exceeds the maximum that you specify, or the default maximum, the response is paginated. To get the next page of items, send a subsequent request that specifies the NextMarker value from the current response as the Marker value in the subsequent request.

Request Syntax

GET /2020-05-31/cache-policy?Marker=Marker&MaxItems=MaxItems&Type=Type HTTP/1.1

URI Request Parameters

The request uses the following URI parameters.

**Marker (p. 209)**

Use this field when paginating results to indicate where to begin in your list of cache policies. The response includes cache policies in the list that occur after the marker. To get the next page of the list, set this field's value to the value of NextMarker from the current page's response.

**MaxItems (p. 209)**

The maximum number of cache policies that you want in the response.

**Type (p. 209)**

A filter to return only the specified kinds of cache policies. Valid values are:

- managed – Returns only the managed policies created by AWS.
- custom – Returns only the custom policies created in your AWS account.

Valid Values: managed | custom

Request Body

The request does not have a request body.

Response Syntax

```
HTTP/1.1 200
<?xml version="1.0" encoding="UTF-8"?>
<CachePolicyList>
  <Items>
    <CachePolicySummary>
      <CachePolicy>
        <CachePolicyConfig>
          <Comment>string</Comment>
          <DefaultTTL>long</DefaultTTL>
          <MaxTTL>long</MaxTTL>
          <MinTTL>long</MinTTL>
          <Name>string</Name>
```
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.

**CachePolicyList (p. 209)**

Root level tag for the CachePolicyList parameters.

Required: Yes

**Items (p. 209)**

Contains the cache policies in the list.

Type: Array of CachePolicySummary (p. 387) objects

**MaxItems (p. 209)**

The maximum number of cache policies requested.
Type: Integer

NextMarker (p. 209)

If there are more items in the list than are in this response, this element is present. It contains the value that you should use in the Marker field of a subsequent request to continue listing cache policies where you left off.

Type: String

Quantity (p. 209)

The total number of cache policies returned in the response.

Type: Integer

Errors

For information about the errors that are common to all actions, see Common Errors (p. 555).

AccessDenied

Access denied.

HTTP Status Code: 403

InvalidArgument

An argument is invalid.

HTTP Status Code: 400

NoSuchCachePolicy

The cache policy 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 V2
- AWS SDK for JavaScript
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3
ListCloudFrontOriginAccessIdentities

Lists origin access identities.

Request Syntax

GET /2020-05-31/origin-access-identity/cloudfront?Marker=Marker&MaxItems=MaxItems HTTP/1.1

URI Request Parameters

The request uses the following URI parameters.

Marker (p. 212)

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. 212)

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. 212)

Root level tag for the CloudFrontOriginAccessIdentityList parameters.
Required: Yes

**IsTruncated (p. 212)**

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. 212)**

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. 392) objects

**Marker (p. 212)**

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. 212)**

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

Type: Integer

**NextMarker (p. 212)**

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. 212)**

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. 555)].

**InvalidArgument**

An 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 V2
- AWS SDK for JavaScript
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3
ListConflictingAliases

Gets a list of aliases (also called CNAMEs or alternate domain names) that conflict or overlap with the provided alias, and the associated CloudFront distributions and AWS accounts for each conflicting alias. In the returned list, the distribution and account IDs are partially hidden, which allows you to identify the distributions and accounts that you own, but helps to protect the information of ones that you don’t own.

Use this operation to find aliases that are in use in CloudFront that conflict or overlap with the provided alias. For example, if you provide `www.example.com` as input, the returned list can include `www.example.com` and the overlapping wildcard alternate domain name (`*.example.com`), if they exist. If you provide `*.example.com` as input, the returned list can include `*.example.com` and any alternate domain names covered by that wildcard (for example, `www.example.com`, `test.example.com`, `dev.example.com`, and so on), if they exist.

To list conflicting aliases, you provide the alias to search and the ID of a distribution in your account that has an attached SSL/TLS certificate that includes the provided alias. For more information, including how to set up the distribution and certificate, see Moving an alternate domain name to a different distribution in the Amazon CloudFront Developer Guide.

You can optionally specify the maximum number of items to receive in the response. If the total number of items in the list exceeds the maximum that you specify, or the default maximum, the response is paginated. To get the next page of items, send a subsequent request that specifies the `NextMarker` value from the current response as the `Marker` value in the subsequent request.

**Request Syntax**

```
GET /2020-05-31/conflicting-alias?
Alias=Alias&DistributionId=DistributionId&Marker=Marker&MaxItems=MaxItems HTTP/1.1
```

**URI Request Parameters**

The request uses the following URI parameters.

**Alias (p. 215)**

The alias (also called a CNAME) to search for conflicting aliases.

Length Constraints: Maximum length of 253.

Required: Yes

**DistributionId (p. 215)**

The ID of a distribution in your account that has an attached SSL/TLS certificate that includes the provided alias.

Length Constraints: Maximum length of 25.

Required: Yes

**Marker (p. 215)**

Use this field when paginating results to indicate where to begin in the list of conflicting aliases. The response includes conflicting aliases in the list that occur after the marker. To get the next page of the list, set this field’s value to the value of `NextMarker` from the current page’s response.

**MaxItems (p. 215)**

The maximum number of conflicting aliases that you want in the response.
Valid Range: Maximum value of 100.

**Request Body**

The request does not have a request body.

**Response Syntax**

```
HTTP/1.1 200
<?xml version="1.0" encoding="UTF-8"?>
<ConflictingAliasesList>
  <Items>
    <ConflictingAlias>
      <AccountId>string</AccountId>
      <Alias>string</Alias>
      <DistributionId>string</DistributionId>
    </ConflictingAlias>
  </Items>
  <MaxItems>integer</MaxItems>
  <NextMarker>string</NextMarker>
  <Quantity>integer</Quantity>
</ConflictingAliasesList>
```

**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.

**ConflictingAliasesList (p. 216)**

Root level tag for the ConflictingAliasesList parameters.

- Required: Yes

**Items (p. 216)**

Contains the conflicting aliases in the list.

- Type: Array of ConflictingAlias (p. 393) objects

**MaxItems (p. 216)**

The maximum number of conflicting aliases requested.

- Type: Integer

**NextMarker (p. 216)**

If there are more items in the list than are in this response, this element is present. It contains the value that you should use in the Marker field of a subsequent request to continue listing conflicting aliases where you left off.

- Type: String

**Quantity (p. 216)**

The number of conflicting aliases returned in the response.

- Type: Integer
Errors

For information about the errors that are common to all actions, see Common Errors (p. 555).

InvalidArgument

An 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 V2
- AWS SDK for JavaScript
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3
ListDistributions

List CloudFront distributions.

Request Syntax

GET /2020-05-31/distribution?Marker=Marker&MaxItems=MaxItems HTTP/1.1

URI Request Parameters

The request uses the following URI parameters.

**Marker (p. 218)**

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. 218)**

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>
        </Items>
        <Quantity>integer</Quantity>
      </Aliases>
      <AliasICPRecordals>
        <AliasICPRecordal>
          <CNAME>string</CNAME>
          <ICPRecordalStatus>string</ICPRecordalStatus>
        </AliasICPRecordal>
      </AliasICPRecordals>
      <ARN>string</ARN>
      <CacheBehaviors>
        <Items>
          <AllowedMethods>
            <CachedMethods>
              <Items>
                <Method>string</Method>
              </Items>
            </CachedMethods>
          </AllowedMethods>
        </Items>
      </CacheBehaviors>
    </DistributionSummary>
  </Items>
</DistributionList>
```
API Version 2020-05-31

219
Response Syntax

```xml
<Items>
<Quantity>integer</Quantity>
</Items>
<TrustedKeyGroups>
<Items>
<Enabled>boolean</Enabled>
<Items>
<AwsAccountNumber>string</AwsAccountNumber>
</Items>
<Quantity>integer</Quantity>
</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>
<Items>
<Method>string</Method>
</Items>
<Quantity>integer</Quantity>
</CachedMethods>
<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>
</AllowedMethods>
</CachePolicyId>string</CachePolicyId>
</Compress>boolean</Compress>
</DefaultTTL>long</DefaultTTL>
</FieldLevelEncryptionId>string</FieldLevelEncryptionId>
</ForwardedValues>
```

API Version 2020-05-31
220
XML Response Syntax

```xml
<OriginGroupMembers>
  <OriginGroup>
    <Items>
      <OriginGroupMember>
        <Items>
          <Quantity>integer</Quantity>
        </Items>
        <Members>
          <Items>
            <Quantity>integer</Quantity>
          </Items>
          <OriginGroups>
            <Items>
              <Origin>
                <ConnectionAttempts>integer</ConnectionAttempts>
                <ConnectionTimeout>integer</ConnectionTimeout>
                <CustomHeaders>
                  <Items>
                    <OriginCustomHeader>
                      <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>
                <OriginShield>
                  <Enabled>boolean</Enabled>
                  <OriginShieldRegion>string</OriginShieldRegion>
                </OriginShield>
                <S3OriginConfig>
                  <OriginAccessIdentity>string</OriginAccessIdentity>
                </S3OriginConfig>
              </Origin>
            </Items>
            <Quantity>integer</Quantity>
          </OriginGroups>
        </Items>
        <PriceClass>string</PriceClass>
      </OriginGroupMembers>
    </Items>
  </OriginGroups>
</Origins>
<PriceClass>string</PriceClass>
<Restrictions>
  <GeoRestriction>
    <Items>
      <Location>string</Location>
    </Items>
    <Quantity>integer</Quantity>
  </GeoRestriction>
</Restrictions>
>Status>string</Status>
</ViewerCertificate>
<ACMCertificateArn>string</ACMCertificateArn>
<Certificate>string</Certificate>
<CertificateSource>string</CertificateSource>
<CloudFrontDefaultCertificate>boolean</CloudFrontDefaultCertificate>
<IAMCertificateId>string</IAMCertificateId>
```
### 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.

<table>
<thead>
<tr>
<th>Tag</th>
<th>Description</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>DistributionList (p. 218)</td>
<td>Root level tag for the DistributionList parameters.</td>
<td></td>
</tr>
<tr>
<td>IsTruncated (p. 218)</td>
<td>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.</td>
<td>Boolean</td>
</tr>
<tr>
<td>Items (p. 218)</td>
<td>A complex type that contains one DistributionSummary element for each distribution that was created by the current AWS account.</td>
<td>Array of DistributionSummary (p. 423) objects</td>
</tr>
<tr>
<td>Marker (p. 218)</td>
<td>The value you provided for the Marker request parameter.</td>
<td>String</td>
</tr>
<tr>
<td>MaxItems (p. 218)</td>
<td>The value you provided for the MaxItems request parameter.</td>
<td>Integer</td>
</tr>
<tr>
<td>NextMarker (p. 218)</td>
<td>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.</td>
<td>String</td>
</tr>
<tr>
<td>Quantity (p. 218)</td>
<td>The number of distributions that were created by the current AWS account.</td>
<td>Integer</td>
</tr>
</tbody>
</table>
Errors

For information about the errors that are common to all actions, see Common Errors (p. 555).

InvalidArgument

An 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 V2
- AWS SDK for JavaScript
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3
ListDistributionsByCachePolicyId

Gets a list of distribution IDs for distributions that have a cache behavior that's associated with the specified cache policy.

You can optionally specify the maximum number of items to receive in the response. If the total number of items in the list exceeds the maximum that you specify, or the default maximum, the response is paginated. To get the next page of items, send a subsequent request that specifies the NextMarker value from the current response as the Marker value in the subsequent request.

Request Syntax

GET /2020-05-31/distributionsByCachePolicyId/CachePolicyId?Marker=Marker&MaxItems=MaxItems
HTTP/1.1

URI Request Parameters

The request uses the following URI parameters.

CachePolicyId (p. 225)

The ID of the cache policy whose associated distribution IDs you want to list.

Required: Yes

Marker (p. 225)

Use this field when paginating results to indicate where to begin in your list of distribution IDs. The response includes distribution IDs in the list that occur after the marker. To get the next page of the list, set this field's value to the value of NextMarker from the current page's response.

MaxItems (p. 225)

The maximum number of distribution IDs that you want in the response.

Request Body

The request does not have a request body.

Response Syntax

HTTP/1.1 200
<?xml version="1.0" encoding="UTF-8"?>
<DistributionIdList>
<IsTruncated>boolean</IsTruncated>
<Items>
  <DistributionId>string</DistributionId>
</Items>
<Marker>string</Marker>
<MaxItems>integer</MaxItems>
<NextMarker>string</NextMarker>
<Quantity>integer</Quantity>
</DistributionIdList>
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.

**DistributionIdList (p. 225)**

Root level tag for the DistributionIdList parameters.

Required: Yes

**IsTruncated (p. 225)**

A flag that indicates whether more distribution IDs remain to be listed. If your results were truncated, you can make a subsequent request using the Marker request field to retrieve more distribution IDs in the list.

Type: Boolean

**Items (p. 225)**

Contains the distribution IDs in the list.

Type: Array of strings

**Marker (p. 225)**

The value provided in the Marker request field.

Type: String

**MaxItems (p. 225)**

The maximum number of distribution IDs requested.

Type: Integer

**NextMarker (p. 225)**

Contains the value that you should use in the Marker field of a subsequent request to continue listing distribution IDs where you left off.

Type: String

**Quantity (p. 225)**

The total number of distribution IDs returned in the response.

Type: Integer

Errors

For information about the errors that are common to all actions, see Common Errors (p. 555).

**AccessDenied**

Access denied.

HTTP Status Code: 403

**InvalidArgument**

An argument is invalid.
HTTP Status Code: 400

NoSuchCachePolicy

The cache policy 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 V2
- AWS SDK for JavaScript
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3
ListDistributionsByKeyGroup

Gets a list of distribution IDs for distributions that have a cache behavior that references the specified key group.

You can optionally specify the maximum number of items to receive in the response. If the total number of items in the list exceeds the maximum that you specify, or the default maximum, the response is paginated. To get the next page of items, send a subsequent request that specifies the NextMarker value from the current response as the Marker value in the subsequent request.

Request Syntax

GET /2020-05-31/distributionsByKeyGroupId/KeyGroupId?Marker=Marker&MaxItems=MaxItems
HTTP/1.1

URI Request Parameters

The request uses the following URI parameters.

KeyGroupId (p. 228)

The ID of the key group whose associated distribution IDs you are listing.

Required: Yes

Marker (p. 228)

Use this field when paginating results to indicate where to begin in your list of distribution IDs. The response includes distribution IDs in the list that occur after the marker. To get the next page of the list, set this field's value to the value of NextMarker from the current page's response.

MaxItems (p. 228)

The maximum number of distribution IDs that you want in the response.

Request Body

The request does not have a request body.

Response Syntax

HTTP/1.1 200
<?xml version="1.0" encoding="UTF-8"?>
<DistributionIdList>
  <IsTruncated>boolean</IsTruncated>
  <Items>
    <DistributionId>string</DistributionId>
  </Items>
  <Marker>string</Marker>
  <MaxItems>integer</MaxItems>
  <NextMarker>string</NextMarker>
  <Quantity>integer</Quantity>
</DistributionIdList>
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.

DistributionIdList (p. 228)

Root level tag for the DistributionIdList parameters.

Required: Yes

IsTruncated (p. 228)

A flag that indicates whether more distribution IDs remain to be listed. If your results were truncated, you can make a subsequent request using the Marker request field to retrieve more distribution IDs in the list.

Type: Boolean

Items (p. 228)

Contains the distribution IDs in the list.

Type: Array of strings

Marker (p. 228)

The value provided in the Marker request field.

Type: String

MaxItems (p. 228)

The maximum number of distribution IDs requested.

Type: Integer

NextMarker (p. 228)

Contains the value that you should use in the Marker field of a subsequent request to continue listing distribution IDs where you left off.

Type: String

Quantity (p. 228)

The total number of distribution IDs returned in the response.

Type: Integer

Errors

For information about the errors that are common to all actions, see Common Errors (p. 555).

InvalidArgument

An argument is invalid.

HTTP Status Code: 400

NoSuchResource

A resource that was specified is not valid.
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 V2
- AWS SDK for JavaScript
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3
ListDistributionsByOriginRequestPolicyId

Gets a list of distribution IDs for distributions that have a cache behavior that's associated with the specified origin request policy.

You can optionally specify the maximum number of items to receive in the response. If the total number of items in the list exceeds the maximum that you specify, or the default maximum, the response is paginated. To get the next page of items, send a subsequent request that specifies the NextMarker value from the current response as the Marker value in the subsequent request.

Request Syntax

GET /2020-05-31/distributionsByOriginRequestPolicyId/OriginRequestPolicyId?Marker=Marker&MaxItems=MaxItems HTTP/1.1

URI Request Parameters

The request uses the following URI parameters.

**Marker (p. 231)**

Use this field when paginating results to indicate where to begin in your list of distribution IDs. The response includes distribution IDs in the list that occur after the marker. To get the next page of the list, set this field's value to the value of NextMarker from the current page's response.

**MaxItems (p. 231)**

The maximum number of distribution IDs that you want in the response.

**OriginRequestPolicyId (p. 231)**

The ID of the origin request policy whose associated distribution IDs you want to list.

Required: Yes

Request Body

The request does not have a request body.

Response Syntax

```xml
HTTP/1.1 200
<?xml version="1.0" encoding="UTF-8"?>
<DistributionIdList>
  <IsTruncated>boolean</IsTruncated>
  <Items>
    <DistributionId>string</DistributionId>
  </Items>
  <Marker>string</Marker>
  <MaxItems>integer</MaxItems>
  <NextMarker>string</NextMarker>
  <Quantity>integer</Quantity>
</DistributionIdList>
```
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.

DistributionIdList (p. 231)

Root level tag for the DistributionIdList parameters.

Required: Yes

IsTruncated (p. 231)

A flag that indicates whether more distribution IDs remain to be listed. If your results were truncated, you can make a subsequent request using the Marker request field to retrieve more distribution IDs in the list.

Type: Boolean

Items (p. 231)

Contains the distribution IDs in the list.

Type: Array of strings

Marker (p. 231)

The value provided in the Marker request field.

Type: String

MaxItems (p. 231)

The maximum number of distribution IDs requested.

Type: Integer

NextMarker (p. 231)

Contains the value that you should use in the Marker field of a subsequent request to continue listing distribution IDs where you left off.

Type: String

Quantity (p. 231)

The total number of distribution IDs returned in the response.

Type: Integer

Errors

For information about the errors that are common to all actions, see Common Errors (p. 555).

AccessDenied

Access denied.

HTTP Status Code: 403

InvalidArgument

An argument is invalid.
HTTP Status Code: 400

NoSuchOriginRequestPolicy

The origin request policy 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 V2
- AWS SDK for JavaScript
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3
ListDistributionsByRealtimeLogConfig

Gets a list of distributions that have a cache behavior that's associated with the specified real-time log configuration.

You can specify the real-time log configuration by its name or its Amazon Resource Name (ARN). You must provide at least one. If you provide both, CloudFront uses the name to identify the real-time log configuration to list distributions for.

You can optionally specify the maximum number of items to receive in the response. If the total number of items in the list exceeds the maximum that you specify, or the default maximum, the response is paginated. To get the next page of items, send a subsequent request that specifies the NextMarker value from the current response as the Marker value in the subsequent request.

**Request Syntax**

```xml
POST /2020-05-31/distributionsByRealtimeLogConfig/ HTTP/1.1
<?xml version="1.0" encoding="UTF-8"?>
  <Marker>string</Marker>
  <MaxItems>string</MaxItems>
  <RealtimeLogConfigArn>string</RealtimeLogConfigArn>
  <RealtimeLogConfigName>string</RealtimeLogConfigName>
</ListDistributionsByRealtimeLogConfigRequest>
```

**URI Request Parameters**

The request does not use any URI parameters.

**Request Body**

The request accepts the following data in XML format.

- **ListDistributionsByRealtimeLogConfigRequest (p. 234)**
  
  Root level tag for the ListDistributionsByRealtimeLogConfigRequest parameters.
  
  Required: Yes

- **Marker (p. 234)**
  
  Use this field when paginating results to indicate where to begin in your list of distributions. The response includes distributions in the list that occur after the marker. To get the next page of the list, set this field's value to the value of NextMarker from the current page's response.
  
  Type: String
  
  Required: No

- **MaxItems (p. 234)**
  
  The maximum number of distributions that you want in the response.
  
  Type: String
  
  Required: No
RealtimeLogConfigArn (p. 234)

The Amazon Resource Name (ARN) of the real-time log configuration whose associated distributions you want to list.

Type: String
Required: No

RealtimeLogConfigName (p. 234)

The name of the real-time log configuration whose associated distributions you want to list.

Type: String
Required: No

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>
      <AliasICPRecordals>
        <AliasICPRecordal>
          <CNAME>string</CNAME>
          <ICPRecordalStatus>string</ICPRecordalStatus>
        </AliasICPRecordal>
      </AliasICPRecordals>
      <ARN>string</ARN>
      <CacheBehaviors>
        <Items>
          <CacheBehavior>
            <AllowedMethods>
              <CachedMethods>
                <Items>
                  <Method>string</Method>
                </Items>
                <Quantity>integer</Quantity>
              </CachedMethods>
              <Items>
                <Method>string</Method>
                <Quantity>integer</Quantity>
              </AllowedMethods>
              <CachePolicyId>string</CachePolicyId>
              <Compress>boolean</Compress>
              <DefaultTLT>long</DefaultTLT>
              <FieldLevelEncryptionId>string</FieldLevelEncryptionId>
              <ForwardedValues>
                <Cookies>
                  <Forward>string</Forward>
                  <WhitelistedNames>
                    <Items>
                      <Name>string</Name>
                    </Items>
                  </WhitelistedNames>
                </Cookies>
              </ForwardedValues>
            </AllowedMethods>
            <Compress>boolean</Compress>
            <DefaultTLT>long</DefaultTLT>
            <FieldLevelEncryptionId>string</FieldLevelEncryptionId>
            <ForwardedValues>
              <Cookies>
                <Forward>string</Forward>
                <WhitelistedNames>
                  <Items>
                    <Name>string</Name>
                  </Items>
                </WhitelistedNames>
              </Cookies>
            </ForwardedValues>
          </CacheBehavior>
        </Items>
      </CacheBehaviors>
    </DistributionSummary>
  </Items>
</DistributionList>
<Items>
  <CustomErrorResponse>
    <ErrorCachingMinTTL>long</ErrorCachingMinTTL>
    <ErrorCode>integer</ErrorCode>
    <ResponseCode>string</ResponseCode>
    <ResponsePagePath>string</ResponsePagePath>
  </CustomErrorResponse>
  <Quantity>integer</Quantity>
</CustomErrorResponses>
<DefaultCacheBehavior>
  <AllowedMethods>
    <CachedMethods>
      <Items>
        <Method>string</Method>
      </Items>
      <Quantity>integer</Quantity>
    </CachedMethods>
    <Items>
      <Method>string</Method>
      <Quantity>integer</Quantity>
    </Items>
    <Compress>boolean</Compress>
    <DefaultTTL>long</DefaultTTL>
    <FieldLevelEncryptionId>string</FieldLevelEncryptionId>
  </AllowedMethods>
  <CachePolicyId>string</CachePolicyId>
  <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>
  <FunctionAssociations>
    <Items>
      <FunctionAssociation>
        <EventType>string</EventType>
        <FunctionARN>string</FunctionARN>
      </FunctionAssociation>
      <Quantity>integer</Quantity>
    </FunctionAssociations>
  <LambdaFunctionAssociations>
    <Items>
      <LambdaFunctionAssociation>
        <EventType>string</EventType>
        <IncludeBody>boolean</IncludeBody>
        <LambdaFunctionARN>string</LambdaFunctionARN>
      </LambdaFunctionAssociation>
      <Quantity>integer</Quantity>
    </LambdaFunctionAssociations>
</Items>

API Version 2020-05-31
237
<LambdaFunctionAssociations>
  <Items>
    <Quantity>integer</Quantity>
  </Items>
</LambdaFunctionAssociations>

<MaxTTL>long</MaxTTL>
<MinTTL>long</MinTTL>
<OriginRequestPolicyId>string</OriginRequestPolicyId>
<RealtimeLogConfigArn>string</RealtimeLogConfigArn>
steller</ResponseHeadersPolicyId>
<SmoothingStream>boolean</SmoothingStream>
<TargetOriginId>string</TargetOriginId>

<TrustedKeyGroups>
  <Enabled>boolean</Enabled>
  <Items>
    <KeyGroup>string</KeyGroup>
  </Items>
  <Quantity>integer</Quantity>
</TrustedKeyGroups>

<TrustedSigners>
  <Enabled>boolean</Enabled>
  <Items>
    <AwsAccountNumber>string</AwsAccountNumber>
  </Items>
  <Quantity>integer</Quantity>
</TrustedSigners>

<ViewerProtocolPolicy>string</ViewerProtocolPolicy>

<DefaultCacheBehavior>
  <DomainName>string</DomainName>
  <Enabled>boolean</Enabled>
  <HttpVersion>string</HttpVersion>
  <Id>string</Id>
  <IsIPV6Enabled>boolean</IsIPV6Enabled>
  <LastModifiedTime>timestamp</LastModifiedTime>
</DefaultCacheBehavior>

<Origins>
  <Items>
    <Origin>
      <ConnectionAttempts>integer</ConnectionAttempts>
      <ConnectionTimeout>integer</ConnectionTimeout>
      <CustomHeaders>
        <Items>
          <OriginCustomHeader>
            <HeaderValue>string</HeaderValue>
          </OriginCustomHeader>
        </Items>
      </CustomHeaders>
    </Origin>
  </Items>
  <Quantity>integer</Quantity>
</Origins>

<OriginGroups>
  <Items>
    <OriginGroup>
      <FailoverCriteria>
        <StatusCodes>
          <Items>
            <StatusCode>integer</StatusCode>
          </Items>
        </StatusCodes>
        <Id>string</Id>
        <Members>
          <Items>
            <OriginGroupMember>
              <GroupId>string</GroupId>
            </OriginGroupMember>
          </Items>
        </Members>
      </FailoverCriteria>
    </OriginGroup>
  </Items>
  <Quantity>integer</Quantity>
</OriginGroups>

API Version 2020-05-31
238
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. 235)**

Root level tag for the DistributionList parameters.

Required: Yes

**IsTruncated (p. 235)**

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. 235)**

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

Type: Array of DistributionSummary (p. 423) objects

**Marker (p. 235)**

The value you provided for the Marker request parameter.

Type: String

**MaxItems (p. 235)**

The value you provided for the MaxItems request parameter.

Type: Integer

**NextMarker (p. 235)**

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. 235)**

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. 555).

**InvalidArgument**

An 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:
See Also

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

Gets a list of distribution IDs for distributions that have a cache behavior that's associated with the specified response headers policy.

You can optionally specify the maximum number of items to receive in the response. If the total number of items in the list exceeds the maximum that you specify, or the default maximum, the response is paginated. To get the next page of items, send a subsequent request that specifies the NextMarker value from the current response as the Marker value in the subsequent request.

**Request Syntax**

```
GET /2020-05-31/distributionsByResponseHeadersPolicyId/ResponseHeadersPolicyId?
Marker=Marker&MaxItems=MaxItems HTTP/1.1
```

**URI Request Parameters**

The request uses the following URI parameters.

**Marker (p. 242)**

Use this field when paginating results to indicate where to begin in your list of distribution IDs. The response includes distribution IDs in the list that occur after the marker. To get the next page of the list, set this field's value to the value of NextMarker from the current page's response.

**MaxItems (p. 242)**

The maximum number of distribution IDs that you want to get in the response.

**ResponseHeadersPolicyId (p. 242)**

The ID of the response headers policy whose associated distribution IDs you want to list.

Required: Yes

**Request Body**

The request does not have a request body.

**Response Syntax**

```
HTTP/1.1 200
<?xml version="1.0" encoding="UTF-8"?>
<DistributionIdList>
  <IsTruncated>boolean</IsTruncated>
  <Items>
    <DistributionId>string</DistributionId>
  </Items>
  <Marker>string</Marker>
  <MaxItems>integer</MaxItems>
  <NextMarker>string</NextMarker>
  <Quantity>integer</Quantity>
</DistributionIdList>
```
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.

**DistributionIdList (p. 242)**

Root level tag for the DistributionIdList parameters.

Required: Yes

**IsTruncated (p. 242)**

A flag that indicates whether more distribution IDs remain to be listed. If your results were truncated, you can make a subsequent request using the Marker request field to retrieve more distribution IDs in the list.

Type: Boolean

**Items (p. 242)**

Contains the distribution IDs in the list.

Type: Array of strings

**Marker (p. 242)**

The value provided in the Marker request field.

Type: String

**MaxItems (p. 242)**

The maximum number of distribution IDs requested.

Type: Integer

**NextMarker (p. 242)**

Contains the value that you should use in the Marker field of a subsequent request to continue listing distribution IDs where you left off.

Type: String

**Quantity (p. 242)**

The total number of distribution IDs returned in the response.

Type: Integer

Errors

For information about the errors that are common to all actions, see Common Errors (p. 555).

**AccessDenied**

Access denied.

HTTP Status Code: 403

**InvalidArgument**

An argument is invalid.
HTTP Status Code: 400

**NoSuchResponseHeadersPolicy**

The response headers policy 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 V2
- AWS SDK for JavaScript
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3
ListDistributionsByWebACLId

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

Request Syntax

GET /2020-05-31/distributionsByWebACLId/WebACLId?Marker=Marker&MaxItems=MaxItems HTTP/1.1

URI Request Parameters

The request uses the following URI parameters.

Marker (p. 245)

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. 245)

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. 245)

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.

Required: Yes

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>
      <AliasICPRecordals>
        <AliasICPRecordal>
          <CNAME>string</CNAME>
          <ICPRecordalStatus>string</ICPRecordalStatus>
        </AliasICPRecordal>
      </AliasICPRecordals>
      <ARN>string</ARN>
    </DistributionSummary>
  </Items>
</DistributionList>
<CacheBehaviors>
  <Items>
    <CacheBehavior>
      <AllowedMethods>
        <Items>
          <Method>string</Method>
          <Items>
            <Method>string</Method>
          </Items>
          <Quantity>integer</Quantity>
        </AllowedMethods>
        <CachePolicyId>string</CachePolicyId>
        <Compress>boolean</Compress>
        <DefaultTTL>long</DefaultTTL>
      </CacheBehavior>
    </Items>
  </Items>
  <CachePolicyId>string</CachePolicyId>
  <Compress>boolean</Compress>
  <DefaultTTL>long</DefaultTTL>
  <FieldLevelEncryptionId>string</FieldLevelEncryptionId>
  <ForwardedValues>
    <Cookies>
      <Forward>string</Forward>
    </Cookies>
    <WhitelistedNames>
      <Name>string</Name>
      <Items>
        <Name>string</Name>
        <Quantity>integer</Quantity>
      </Items>
    </WhitelistedNames>
    <Headers>
      <Name>string</Name>
      <Items>
        <Name>string</Name>
        <Quantity>integer</Quantity>
      </Items>
    </Headers>
    <QueryString>boolean</QueryString>
    <QueryStringCacheKeys>
      <Name>string</Name>
      <Items>
        <Name>string</Name>
        <Quantity>integer</Quantity>
      </Items>
    </QueryStringCacheKeys>
  </ForwardedValues>
  <FunctionAssociations>
    <Items>
      <FunctionAssociation>
        <EventType>string</EventType>
        <FunctionARN>string</FunctionARN>
      </FunctionAssociation>
    </Items>
    <Quantity>integer</Quantity>
  </FunctionAssociations>
  <LambdaFunctionAssociations>
    <Items>
      <LambdaFunctionAssociation>
        <EventType>string</EventType>
        <FunctionARN>string</FunctionARN>
        <IncludeBody>boolean</IncludeBody>
      </LambdaFunctionAssociation>
    </Items>
    <Quantity>integer</Quantity>
  </LambdaFunctionAssociations>
  <MaxTTL>long</MaxTTL>
  <MinTTL>long</MinTTL>
  <OriginRequestPolicyId>string</OriginRequestPolicyId>
  <PathPattern>string</PathPattern>
</CacheBehaviors>
Amazon CloudFront API Reference
Response Syntax

API Version 2020-05-31
247

<ResponseSyntax>

// RealtimeLogConfigArn
<string>/RealtimeLogConfigArn</string>

// ResponseHeadersPolicyId
<string>/ResponseHeadersPolicyId</string>

// SmoothStreaming
<boolean>/SmoothStreaming</boolean>

// TargetOriginId
<string>/TargetOriginId</string>

// TrustedKeyGroups
<Enabled boolean/>
  <Items>
    <KeyGroup>
      <string>/KeyGroup</string>
    </Items>
    <Quantity integer/></Quantity>
  </TrustedKeyGroups>

// TrustedSigners
<Enabled boolean/>
  <Items>
    <AwsAccountNumber>
      <string>/AwsAccountNumber</string>
    </Items>
    <Quantity integer/></Quantity>
  </TrustedSigners>

// ViewerProtocolPolicy
<string>/ViewerProtocolPolicy</string>

// CacheBehavior
  <AllowedMethods>
    <CachedMethods>
      <Items>
        <Method>
          <string>/Method</string>
        </Items>
        <Quantity integer/></Quantity>
      </CachedMethods>
    </AllowedMethods>
    <CachePolicyId>
      <string>/CachePolicyId</string>
    </CachePolicyId>
    <Compress boolean/>
    <DefaultTTL long/>
    <FieldLevelEncryptionId>
      <string>/FieldLevelEncryptionId</string>
    </FieldLevelEncryptionId>
    <ForwardedValues>
      <Cookies>
        <Forward>
          <string>/Forward</string>
        </Forward>
        <WhitelistedNames>
          <Items>
            <Name>
              <string>/Name</string>
            </Items>
            <Quantity integer/></Quantity>
          </WhitelistedNames>
        </Cookies>
        <Headers>
          <Items>
            <Name>
              <string>/Name</string>
            </Items>
          </Headers>
      </Cookies>
    </ForwardedValues>
  </CacheBehavior>
  <Comment>
    <string>/Comment</string>
  </Comment>
  <CustomErrorResponses>
    <Items>
      <CustomErrorResponse>
        <ErrorCachingMinTTL long/>
        <ErrorCode integer/>
        <ResponseCode string/>
        <ResponsePagePath>
          <string>/ResponsePagePath</string>
        </ResponsePagePath>
      </CustomErrorResponse>
      <Quantity integer/></Quantity>
    </CustomErrorResponses>
  </CacheBehaviors>
</ResponseSyntax>
<Quantity>integer</Quantity>
</Headers>
<QueryString>boolean</QueryString>
<QueryStringCacheKeys>
  <Items>
    <Name>string</Name>
  </Items>
</QueryStringCacheKeys>
</ForwardedValues>
</FunctionAssociations>
</Items>
</FunctionAssociations>
</LambdaFunctionAssociations>
</Items>
</LambdaFunctionAssociations>
<MaxTTL>long</MaxTTL>
<MinTTL>long</MinTTL>
<OriginRequestPolicyId>string</OriginRequestPolicyId>
<RealtimeLogConfigArn>string</RealtimeLogConfigArn>
<ResponseHeadersPolicyId>string</ResponseHeadersPolicyId>
<SmoothStreaming>boolean</SmoothStreaming>
<TargetOriginId>string</TargetOriginId>
</DefaultCacheBehavior>
<DomainName>string</DomainName>
<Enabled>boolean</Enabled>
<HttpVersion>string</HttpVersion>
<ID>string</ID>
<IsIPV6Enabled>boolean</IsIPV6Enabled>
<LastModifiedTime>timestamp</LastModifiedTime>
</OriginGroups>
</Items>
</FailoverCriteria>
<StatusCodes>
  <Items>
    <StatusCode>integer</StatusCode>
  </Items>
</StatusCodes>
</Items>
<Quantity>integer</Quantity>
</StatusCodes>
</FailoverCriteria>
<Id>string</Id>
<Members>
<Items>
<OriginGroupMember>
<OriginId>string</OriginId>
</OriginGroupMember>
</Items>
<Quantity>integer</Quantity>
</Members>
</OriginGroup>
</Items>
</OriginGroups>
<Origins>
<Items>
<Origin>
<ConnectionAttempts>integer</ConnectionAttempts>
<ConnectionTimeout>integer</ConnectionTimeout>
<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>
<OriginShield>
<Enabled>boolean</Enabled>
<OriginShieldRegion>string</OriginShieldRegion>
</OriginShield>
<S3OriginConfig>
<OriginAccessIdentity>string</OriginAccessIdentity>
</S3OriginConfig>
</Origin>
</Items>
<Quantity>integer</Quantity>
</Origins>
<PriceClass>string</PriceClass>
<Restrictions>
<GeoRestriction>
<Items>
<Location>string</Location>
</Items>
<Quantity>integer</Quantity>
</GeoRestriction>
</Restrictions>
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. 245)**

Root level tag for the DistributionList parameters.

Required: Yes

**IsTruncated (p. 245)**

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. 245)**

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

Type: Array of DistributionSummary (p. 423) objects

**Marker (p. 245)**

The value you provided for the Marker request parameter.

Type: String

**MaxItems (p. 245)**

The value you provided for the MaxItems request parameter.

Type: Integer

**NextMarker (p. 245)**

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. 245)

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. 555).

InvalidArgument

An argument is invalid.

HTTP Status Code: 400

InvalidWebACLId

A web ACL ID specified is not valid. To specify a web ACL created using the latest version of AWS WAF, use the ACL ARN, for example arn:aws:wafv2:us-east-1:123456789012:global/webacl/ExampleWebACL/473e64fd-f30b-4765-81a0-62ad96dd167a. To specify a web ACL created using AWS WAF Classic, use the ACL ID, for example 473e64fd-f30b-4765-81a0-62ad96dd167a.

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

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

Request Syntax

```
GET /2020-05-31/field-level-encryption?Marker=Marker&MaxItems=MaxItems HTTP/1.1
```

URI Request Parameters

The request uses the following URI parameters.

**Marker (p. 252)**

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. 252)**

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>
        </ContentTypeProfiles>
        <Quantity>integer</Quantity>
      </ContentTypeProfileConfig>
      <Id>string</Id>
      <ForwardWhenContentTypeIsUnknown>boolean</ForwardWhenContentTypeIsUnknown>
      <LastModifiedTime>timestamp</LastModifiedTime>
    </FieldLevelEncryptionSummary>
    <QueryArgProfileConfig>
      <ForwardWhenQueryArgProfileIsUnknown>boolean</ForwardWhenQueryArgProfileIsUnknown>
      <QueryArgProfiles>
        <Items>
          <QueryArgProfile>
```

API Version 2020-05-31

252
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. 252)

Root level tag for the FieldLevelEncryptionList parameters.

Required: Yes

Items (p. 252)

An array of field-level encryption items.

Type: Array of FieldLevelEncryptionSummary (p. 437) objects

MaxItems (p. 252)

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

Type: Integer

NextMarker (p. 252)

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. 252)

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. 555).

InvalidArgument

An 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 V2
- AWS SDK for JavaScript
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3
ListFieldLevelEncryptionProfiles

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

Request Syntax

GET /2020-05-31/field-level-encryption-profile?Marker=Marker&MaxItems=MaxItems HTTP/1.1

URI Request Parameters

The request uses the following URI parameters.

**Marker (p. 255)**

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. 255)**

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

```xml
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>
      </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. 255)

Root level tag for the FieldLevelEncryptionProfileList parameters.

Required: Yes

Items (p. 255)

The field-level encryption profile items.

Type: Array of FieldLevelEncryptionProfileSummary (p. 436) objects

MaxItems (p. 255)

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

Type: Integer

NextMarker (p. 255)

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. 255)

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. 555).

InvalidArgument

An 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 V2
• AWS SDK for JavaScript
• AWS SDK for PHP V3
• AWS SDK for Python
• AWS SDK for Ruby V3
ListFunctions

Gets a list of all CloudFront functions in your AWS account.

You can optionally apply a filter to return only the functions that are in the specified stage, either DEVELOPMENT or LIVE.

You can optionally specify the maximum number of items to receive in the response. If the total number of items in the list exceeds the maximum that you specify, or the default maximum, the response is paginated. To get the next page of items, send a subsequent request that specifies the NextMarker value from the current response as the Marker value in the subsequent request.

Request Syntax

```
GET /2020-05-31/function?Marker=Marker&MaxItems=MaxItems&Stage=Stage HTTP/1.1
```

URI Request Parameters

The request uses the following URI parameters.

**Marker (p. 258)**

Use this field when paginating results to indicate where to begin in your list of functions. The response includes functions in the list that occur after the marker. To get the next page of the list, set this field's value to the value of NextMarker from the current page's response.

**MaxItems (p. 258)**

The maximum number of functions that you want in the response.

**Stage (p. 258)**

An optional filter to return only the functions that are in the specified stage, either DEVELOPMENT or LIVE.

Valid Values: DEVELOPMENT | LIVE

Request Body

The request does not have a request body.

Response Syntax

```
HTTP/1.1 200
<?xml version="1.0" encoding="UTF-8"?>
<FunctionList>
  <Items>
    <FunctionSummary>
      <FunctionConfig>
        <Comment>string</Comment>
        <Runtime>string</Runtime>
      </FunctionConfig>
      <FunctionMetadata>
        <CreatedTime>timestamp</CreatedTime>
        <FunctionARN>string</FunctionARN>
        <LastModifiedTime>timestamp</LastModifiedTime>
      </FunctionMetadata>
    </FunctionSummary>
  </Items>
</FunctionList>
```

API Version 2020-05-31
258
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.

**FunctionList (p. 258)**

Root level tag for the FunctionList parameters.

Required: Yes

**Items (p. 258)**

Contains the functions in the list.

Type: Array of FunctionSummary (p. 447) objects

**MaxItems (p. 258)**

The maximum number of functions requested.

Type: Integer

**NextMarker (p. 258)**

If there are more items in the list than are in this response, this element is present. It contains the value that you should use in the Marker field of a subsequent request to continue listing functions where you left off.

Type: String

**Quantity (p. 258)**

The number of functions returned in the response.

Type: Integer

**Errors**

For information about the errors that are common to all actions, see Common Errors (p. 555).

**InvalidArgument**

An argument is invalid.

HTTP Status Code: 400

**UnsupportedOperation**

This operation is not supported in this region.
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 V2
- AWS SDK for JavaScript
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3
## ListInvalidations

Lists invalidation batches.

### Request Syntax

```
GET /2020-05-31/distribution/DistributionId/invalidation?Marker=Marker&MaxItems=MaxItems
HTTP/1.1
```

### URI Request Parameters

The request uses the following URI parameters.

- **DistributionId (p. 261)**
  - The distribution's ID.
  - Required: Yes

- **Marker (p. 261)**
  - 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. 261)**
  - 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. 261)**

Root level tag for the InvalidationList parameters.

Required: Yes

**IsTruncated (p. 261)**

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. 261)**

A complex type that contains one InvalidationSummary element for each invalidation batch created by the current AWS account.

Type: Array of InvalidationSummary (p. 455) objects

**Marker (p. 261)**

The value that you provided for the Marker request parameter.

Type: String

**MaxItems (p. 261)**

The value that you provided for the MaxItems request parameter.

Type: Integer

**NextMarker (p. 261)**

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. 261)**

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. 555).

**AccessDenied**

Access denied.

HTTP Status Code: 403

**InvalidArgument**

An 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 V2
- AWS SDK for JavaScript
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3
ListKeyGroups

Gets a list of key groups.

You can optionally specify the maximum number of items to receive in the response. If the total number of items in the list exceeds the maximum that you specify, or the default maximum, the response is paginated. To get the next page of items, send a subsequent request that specifies the NextMarker value from the current response as the Marker value in the subsequent request.

Request Syntax

```
GET /2020-05-31/key-group?Marker=Marker&MaxItems=MaxItems HTTP/1.1
```

URI Request Parameters

The request uses the following URI parameters.

**Marker (p. 264)**

Use this field when paginating results to indicate where to begin in your list of key groups. The response includes key groups in the list that occur after the marker. To get the next page of the list, set this field's value to the value of NextMarker from the current page's response.

**MaxItems (p. 264)**

The maximum number of key groups that you want in the response.

Request Body

The request does not have a request body.

Response Syntax

```xml
HTTP/1.1 200
<?xml version="1.0" encoding="UTF-8"?>
<KeyGroupList>
  <Items>
    <KeyGroupSummary>
      <KeyGroup>
        <Id>string</Id>
        <KeyGroupConfig>
          <Comment>string</Comment>
          <Items>
            <PublicKey>string</PublicKey>
            </Items>
        </KeyGroupConfig>
        <Name>string</Name>
      </KeyGroup>
    </KeyGroupSummary>
  </Items>
  <MaxItems>integer</MaxItems>
  <NextMarker>string</NextMarker>
  <Quantity>integer</Quantity>
</KeyGroupList>
```
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.

**KeyGroupList (p. 264)**

Root level tag for the KeyGroupList parameters.

Required: Yes

**Items (p. 264)**

A list of key groups.

Type: Array of **KeyGroupSummary (p. 459) objects**

**MaxItems (p. 264)**

The maximum number of key groups requested.

Type: Integer

**NextMarker (p. 264)**

If there are more items in the list than are in this response, this element is present. It contains the value that you should use in the Marker field of a subsequent request to continue listing key groups.

Type: String

**Quantity (p. 264)**

The number of key groups returned in the response.

Type: Integer

Errors

For information about the errors that are common to all actions, see Common Errors (p. 555).

**InvalidArgument**

An 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 V2
- AWS SDK for JavaScript
See Also

- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3
ListOriginRequestPolicies

Gets a list of origin request policies.

You can optionally apply a filter to return only the managed policies created by AWS, or only the custom policies created in your AWS account.

You can optionally specify the maximum number of items to receive in the response. If the total number of items in the list exceeds the maximum that you specify, or the default maximum, the response is paginated. To get the next page of items, send a subsequent request that specifies the `NextMarker` value from the current response as the `Marker` value in the subsequent request.

Request Syntax

```plaintext
GET /2020-05-31/origin-request-policy?Marker=Marker&MaxItems=MaxItems&Type=Type HTTP/1.1
```

URI Request Parameters

The request uses the following URI parameters.

**Marker (p. 267)**

Use this field when paginating results to indicate where to begin in your list of origin request policies. The response includes origin request policies in the list that occur after the marker. To get the next page of the list, set this field's value to the value of `NextMarker` from the current page's response.

**MaxItems (p. 267)**

The maximum number of origin request policies that you want in the response.

**Type (p. 267)**

A filter to return only the specified kinds of origin request policies. Valid values are:

- managed – Returns only the managed policies created by AWS.
- custom – Returns only the custom policies created in your AWS account.

Valid Values: managed | custom

Request Body

The request does not have a request body.

Response Syntax

```
HTTP/1.1 200
<?xml version="1.0" encoding="UTF-8"?>
<OriginRequestPolicyList>
  <Items>
    <OriginRequestPolicySummary>
      <OriginRequestPolicy>
        <Id>string</Id>
        <LastModifiedTime>timestamp</LastModifiedTime>
      </OriginRequestPolicy>
    </OriginRequestPolicySummary>
  </Items>
</OriginRequestPolicyList>
```
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.

OriginRequestPolicyList (p. 267)

Root level tag for the OriginRequestPolicyList parameters.

Required: Yes

Items (p. 267)

Contains the origin request policies in the list.

Type: Array of OriginRequestPolicySummary (p. 485) objects

MaxItems (p. 267)

The maximum number of origin request policies requested.

Type: Integer
**NextMarker (p. 267)**

If there are more items in the list than are in this response, this element is present. It contains the value that you should use in the Marker field of a subsequent request to continue listing origin request policies where you left off.

Type: String

**Quantity (p. 267)**

The total number of origin request policies returned in the response.

Type: Integer

**Errors**

For information about the errors that are common to all actions, see Common Errors (p. 555).

- **AccessDenied**
  
  Access denied.

  HTTP Status Code: 403

- **InvalidArgument**
  
  An argument is invalid.

  HTTP Status Code: 400

- **NoSuchOriginRequestPolicy**
  
  The origin request policy 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 V2
- AWS SDK for JavaScript
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3
ListPublicKeys

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

Request Syntax

```
GET /2020-05-31/public-key?Marker=Marker&MaxItems=MaxItems HTTP/1.1
```

URI Request Parameters

The request uses the following URI parameters.

**Marker (p. 270)**

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. 270)**

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. 270)**

Root level tag for the PublicKeyList parameters.
Required: Yes

**Items (p. 270)**

A list of public keys.

Type: Array of PublicKeySummary (p. 495) objects

**MaxItems (p. 270)**

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

Type: Integer

**NextMarker (p. 270)**

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. 270)**

The number of public keys in the list.

Type: Integer

---

**Errors**

For information about the errors that are common to all actions, see Common Errors (p. 555).

**InvalidArgument**

An 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 V2
- AWS SDK for JavaScript
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3
ListRealtimeLogConfigs

Gets a list of real-time log configurations.

You can optionally specify the maximum number of items to receive in the response. If the total number of items in the list exceeds the maximum that you specify, or the default maximum, the response is paginated. To get the next page of items, send a subsequent request that specifies the NextMarker value from the current response as the Marker value in the subsequent request.

Request Syntax

GET /2020-05-31/realtime-log-config?Marker=Marker&MaxItems=MaxItems HTTP/1.1

URI Request Parameters

The request uses the following URI parameters.

Marker (p. 272)

Use this field when paginating results to indicate where to begin in your list of real-time log configurations. The response includes real-time log configurations in the list that occur after the marker. To get the next page of the list, set this field's value to the value of NextMarker from the current page's response.

MaxItems (p. 272)

The maximum number of real-time log configurations that you want in the response.

Request Body

The request does not have a request body.

Response Syntax

HTTP/1.1 200
<?xml version="1.0" encoding="UTF-8"?>
<RealtimeLogConfigs>
  <IsTruncated>boolean</IsTruncated>
  <Items>
    <RealtimeLogConfig>
      <ARN>string</ARN>
      <EndPoints>
        <EndPoint>
          <KinesisStreamConfig>
            <RoleARN>string</RoleARN>
            <StreamARN>string</StreamARN>
          </KinesisStreamConfig>
        </EndPoint>
      </EndPoints>
      <Fields>
        <Field>string</Field>
      </Fields>
      <Name>string</Name>
      <SamplingRate>long</SamplingRate>
    </RealtimeLogConfig>
  </Items>
</RealtimeLogConfigs>
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.

RealtimeLogConfigs (p. 272)

Root level tag for the RealtimeLogConfigs parameters.

Required: Yes

IsTruncated (p. 272)

A flag that indicates whether there are more real-time log configurations than are contained in this list.

Type: Boolean

Items (p. 272)

Contains the list of real-time log configurations.

Type: Array of RealtimeLogConfig (p. 501) objects

Marker (p. 272)

This parameter indicates where this list of real-time log configurations begins. This list includes real-time log configurations that occur after the marker.

Type: String

MaxItems (p. 272)

The maximum number of real-time log configurations requested.

Type: Integer

NextMarker (p. 272)

If there are more items in the list than are in this response, this element is present. It contains the value that you should use in the Marker field of a subsequent request to continue listing real-time log configurations where you left off.

Type: String

Errors

For information about the errors that are common to all actions, see Common Errors (p. 555).

AccessDenied

Access denied.

HTTP Status Code: 403
InvalidArgument

An argument is invalid.

HTTP Status Code: 400

NoSuchRealtimeLogConfig

The real-time log configuration 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 V2
- AWS SDK for JavaScript
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3
ListResponseHeadersPolicies

Gets a list of response headers policies.

You can optionally apply a filter to get only the managed policies created by AWS, or only the custom policies created in your AWS account.

You can optionally specify the maximum number of items to receive in the response. If the total number of items in the list exceeds the maximum that you specify, or the default maximum, the response is paginated. To get the next page of items, send a subsequent request that specifies the NextMarker value from the current response as the Marker value in the subsequent request.

Request Syntax

```
GET /2020-05-31/response-headers-policy?Marker=Marker&MaxItems=MaxItems&Type=Type  HTTP/1.1
```

URI Request Parameters

The request uses the following URI parameters.

**Marker (p. 275)**

Use this field when paginating results to indicate where to begin in your list of response headers policies. The response includes response headers policies in the list that occur after the marker. To get the next page of the list, set this field’s value to the value of NextMarker from the current page’s response.

**MaxItems (p. 275)**

The maximum number of response headers policies that you want to get in the response.

**Type (p. 275)**

A filter to get only the specified kind of response headers policies. Valid values are:

- managed – Gets only the managed policies created by AWS.
- custom – Gets only the custom policies created in your AWS account.

Valid Values: managed | custom

Request Body

The request does not have a request body.

Response Syntax

```xml
<xml version="1.0" encoding="UTF-8">
<ResponseHeadersPolicyList>
  <Items>
    <ResponseHeadersPolicySummary>
      <ResponseHeadersPolicy>
        <Id>string</Id>
        <LastModifiedTime>timestamp</LastModifiedTime>
        <ResponseHeadersPolicyConfig>
        </ResponseHeadersPolicyConfig>
        <Comment>string</Comment>
      </ResponseHeadersPolicy>
    </ResponseHeadersPolicySummary>
  </Items>
</ResponseHeadersPolicyList>
```

API Version 2020-05-31

275
```xml
<CorsConfig>
  <AccessControlAllowCredentials>boolean</AccessControlAllowCredentials>
  <AccessControlAllowHeaders>
    <Items>
      <Header>string</Header>
    </Items>
  </AccessControlAllowHeaders>
  <AccessControlAllowMethods>
    <Items>
      <Method>string</Method>
    </Items>
  </AccessControlAllowMethods>
  <AccessControlAllowOrigins>
    <Items>
      <Origin>string</Origin>
    </Items>
  </AccessControlAllowOrigins>
  <AccessControlExposeHeaders>
    <Items>
      <Header>string</Header>
    </Items>
  </AccessControlExposeHeaders>
  <AccessControlMaxAgeSec>integer</AccessControlMaxAgeSec>
  <OriginOverride>boolean</OriginOverride>
</CorsConfig>

<CustomHeadersConfig>
  <Items>
    <ResponseHeadersPolicyCustomHeader>
      <Header>string</Header>
      <Override>boolean</Override>
      <Value>string</Value>
    </ResponseHeadersPolicyCustomHeader>
  </Items>
</CustomHeadersConfig>

<SecurityHeadersConfig>
  <ContentSecurityPolicy>string</ContentSecurityPolicy>
  <Override>boolean</Override>
  <ContentTypeOptions>
    <Override>boolean</Override>
  </ContentTypeOptions>
  <FrameOptions>
    <FrameOption>string</FrameOption>
    <Override>boolean</Override>
  </FrameOptions>
  <ReferrerPolicy>
    <Override>boolean</Override>
  </ReferrerPolicy>
  <StrictTransportSecurity>
    <AccessControlMaxAgeSec>integer</AccessControlMaxAgeSec>
    <IncludeSubdomains>boolean</IncludeSubdomains>
    <Override>boolean</Override>
    <Preload>boolean</Preload>
  </StrictTransportSecurity>
  <XSSProtection>
    <ModeBlock>boolean</ModeBlock>
    <Override>boolean</Override>
    <Protection>boolean</Protection>
  </XSSProtection>
</SecurityHeadersConfig>
```

API Version 2020-05-31

276
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.

**ResponseHeadersPolicyList (p. 275)**

Root level tag for the ResponseHeadersPolicyList parameters.

**Items (p. 275)**

The response headers policies in the list.

**MaxItems (p. 275)**

The maximum number of response headers policies requested.

**NextMarker (p. 275)**

If there are more items in the list than are in this response, this element is present. It contains the value that you should use in the Marker field of a subsequent request to continue listing response headers policies where you left off.

**Quantity (p. 275)**

The number of response headers policies returned.

Errors

For information about the errors that are common to all actions, see Common Errors (p. 555).

**AccessDenied**

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

HTTP Status Code: 400
**NoSuchResponseHeadersPolicy**
The response headers policy 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 V2
- AWS SDK for JavaScript
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3
ListStreamingDistributions

List streaming distributions.

Request Syntax

```
GET /2020-05-31/streaming-distribution?Marker=Marker&MaxItems=MaxItems HTTP/1.1
```

URI Request Parameters

The request uses the following URI parameters.

**Marker (p. 279)**

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

**MaxItems (p. 279)**

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>
        <Quantity>integer</Quantity>
      </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>
        <Quantity>integer</Quantity>
      </TrustedSigners>
    </StreamingDistributionSummary>
  </Items>
</StreamingDistributionList>
```
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. 279)**

Root level tag for the StreamingDistributionList parameters.

- **Required:** Yes
- **IsTruncated (p. 279)**
  
  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. 279)**
  
  A complex type that contains one StreamingDistributionSummary element for each distribution that was created by the current AWS account.
  
  - **Type:** Array of StreamingDistributionSummary (p. 540) objects
- **Marker (p. 279)**
  
  The value you provided for the Marker request parameter.
  
  - **Type:** String
- **MaxItems (p. 279)**
  
  The value you provided for the MaxItems request parameter.
  
  - **Type:** Integer
- **NextMarker (p. 279)**
  
  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. 279)**
  
  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. 555).
**InvalidArgument**

An 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 V2
- AWS SDK for JavaScript
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3
ListTagsForResource

List tags for a CloudFront resource.

Request Syntax

GET /2020-05-31/tagging?Resource=Resource HTTP/1.1

URI Request Parameters

The request uses the following URI parameters.

Resource (p. 282)

An ARN of a CloudFront resource.

Pattern: arn:aws(-cn)?:cloudfront::[0-9]+:.*

Required: Yes

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. 282)

Root level tag for the Tags parameters.

Required: Yes

Items (p. 282)

A complex type that contains Tag elements.

Type: Array of Tag (p. 543) objects
Errors

For information about the errors that are common to all actions, see Common Errors (p. 555).

**AccessDenied**

Access denied.

HTTP Status Code: 403

**InvalidArgument**

An argument is invalid.

HTTP Status Code: 400

**InvalidTagging**

The tagging specified is not valid.

HTTP Status Code: 400

**NoSuchResource**

A resource that was specified is not valid.

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

Publishes a CloudFront function by copying the function code from the DEVELOPMENT stage to LIVE. This automatically updates all cache behaviors that are using this function to use the newly published copy in the LIVE stage.

When a function is published to the LIVE stage, you can attach the function to a distribution’s cache behavior, using the function’s Amazon Resource Name (ARN).

To publish a function, you must provide the function’s name and version (ETag value). To get these values, you can use ListFunctions and DescribeFunction.

Request Syntax

```
POST /2020-05-31/function/Name/publish HTTP/1.1
If-Match: IfMatch
```

URI Request Parameters

The request uses the following URI parameters.

**If-Match (p. 284)**

- The current version (ETag value) of the function that you are publishing, which you can get using DescribeFunction.
  - Required: Yes

**Name (p. 284)**

- The name of the function that you are publishing.
  - Required: Yes

Request Body

The request does not have a request body.

Response Syntax

```
HTTP/1.1 200
<?xml version="1.0" encoding="UTF-8"?>
<FunctionSummary>
  <FunctionConfig>
    <Comment>string</Comment>
    <Runtime>string</Runtime>
  </FunctionConfig>
  <FunctionMetadata>
    <CreatedTime>timestamp</CreatedTime>
    <FunctionARN>string</FunctionARN>
    <LastModifiedTime>timestamp</LastModifiedTime>
    <Stage>string</Stage>
  </FunctionMetadata>
  <Name>string</Name>
  <Status>string</Status>
</FunctionSummary>
```
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.

**FunctionSummary (p. 284)**

Root level tag for the FunctionSummary parameters.

Required: Yes

**FunctionConfig (p. 284)**

Contains configuration information about a CloudFront function.

Type: FunctionConfig (p. 444) object

**FunctionMetadata (p. 284)**

Contains metadata about a CloudFront function.

Type: FunctionMetadata (p. 446) object

**Name (p. 284)**

The name of the CloudFront function.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 64.

Pattern: ^[a-zA-Z0-9-\_]{1,64}$

**Status (p. 284)**

The status of the CloudFront function.

Type: String

Errors

For information about the errors that are common to all actions, see Common Errors (p. 555).

**InvalidArgument**

An argument is invalid.

HTTP Status Code: 400

**InvalidIfMatchVersion**

The If-Match version is missing or not valid.

HTTP Status Code: 400

**NoSuchFunctionExists**

The function does not exist.

HTTP Status Code: 404
PreconditionFailed

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

HTTP Status Code: 412

UnsupportedOperation

This operation is not supported in this region.

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

Add tags to a CloudFront resource.

Request Syntax

```
POST /2020-05-31/tagging?Operation=Tag HTTP/1.1
<?xml version="1.0" encoding="UTF-8"?>
  <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. 287)**

Root level tag for the Tags parameters.

Required: Yes

**Items (p. 287)**

A complex type that contains Tag elements.

Type: Array of Tag (p. 543) 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. 555).

**AccessDenied**

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

HTTP Status Code: 400
InvalidTagging
The tagging specified is not valid.

HTTP Status Code: 400
NoSuchResource
A resource that was specified is not valid.

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

Tests a CloudFront function.

To test a function, you provide an event object that represents an HTTP request or response that your CloudFront distribution could receive in production. CloudFront runs the function, passing it the event object that you provided, and returns the function's result (the modified event object) in the response. The response also contains function logs and error messages, if any exist. For more information about testing functions, see Testing functions in the Amazon CloudFront Developer Guide.

To test a function, you provide the function's name and version (ETag value) along with the event object. To get the function's name and version, you can use ListFunctions and DescribeFunction.

Request Syntax

| POST /2020-05-31/function/Name/test HTTP/1.1 |
| If-Match: IfMatch |
| <?xml version="1.0" encoding="UTF-8"?> |
|   <EventObject>blob</EventObject> |
|   <Stage>string</Stage> |
| </TestFunctionRequest> |

URI Request Parameters

The request uses the following URI parameters.

If-Match (p. 289)

The current version (ETag value) of the function that you are testing, which you can get using DescribeFunction.

Required: Yes

Name (p. 289)

The name of the function that you are testing.

Required: Yes

Request Body

The request accepts the following data in XML format.

TestFunctionRequest (p. 289)

Root level tag for the TestFunctionRequest parameters.

Required: Yes

EventObject (p. 289)

The event object to test the function with. For more information about the structure of the event object, see Testing functions in the Amazon CloudFront Developer Guide.

Type: Base64-encoded binary data object

Length Constraints: Maximum length of 40960.
Stage (p. 289)

The stage of the function that you are testing, either DEVELOPMENT or LIVE.

Type: String

Valid Values: DEVELOPMENT | LIVE

Required: No

Response Syntax

HTTP/1.1 200
<?xml version="1.0" encoding="UTF-8"?>
<TestResult>
  <ComputeUtilization>string</ComputeUtilization>
  <FunctionErrorMessage>string</FunctionErrorMessage>
  <FunctionExecutionLogs>
    <INVALID-TYPE-NAME>string</INVALID-TYPE-NAME>
  </FunctionExecutionLogs>
  <FunctionOutput>string</FunctionOutput>
  <FunctionSummary>
    <FunctionConfig>
      <Comment>string</Comment>
      <Runtime>string</Runtime>
    </FunctionConfig>
    <FunctionMetadata>
      <CreatedTime>timestamp</CreatedTime>
      <FunctionARN>string</FunctionARN>
      <LastModifiedTime>timestamp</LastModifiedTime>
      <Stage>string</Stage>
    </FunctionMetadata>
    <Name>string</Name>
    <Status>string</Status>
  </FunctionSummary>
</TestResult>

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.

TestResult (p. 290)

Root level tag for the TestResult parameters.

Required: Yes

ComputeUtilization (p. 290)

The amount of time that the function took to run as a percentage of the maximum allowed time. For example, a compute utilization of 35 means that the function completed in 35% of the maximum allowed time.

Type: String

FunctionErrorMessage (p. 290)

If the result of testing the function was an error, this field contains the error message.
Type: String

**FunctionExecutionLogs (p. 290)**

Contains the log lines that the function wrote (if any) when running the test.

Type: Array of strings

**FunctionOutput (p. 290)**

The event object returned by the function. For more information about the structure of the event object, see Event object structure in the *Amazon CloudFront Developer Guide*.

Type: String

**FunctionSummary (p. 290)**

Contains configuration information and metadata about the CloudFront function that was tested.

Type: FunctionSummary (p. 447) object

---

**Errors**

For information about the errors that are common to all actions, see Common Errors (p. 555).

**InvalidArgument**

An argument is invalid.

HTTP Status Code: 400

**InvalidIfMatchVersion**

The If-Match version is missing or not valid.

HTTP Status Code: 400

**NoSuchFunctionExists**

The function does not exist.

HTTP Status Code: 404

**TestFunctionFailed**

The CloudFront function failed.

HTTP Status Code: 500

**UnsupportedOperation**

This operation is not supported in this region.

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 V2
• AWS SDK for JavaScript
• AWS SDK for PHP V3
• AWS SDK for Python
• AWS SDK for Ruby V3
UntagResource

Remove tags from a CloudFront resource.

Request Syntax

POST /2020-05-31/tagging?Operation=Untag HTTP/1.1
<?xml version="1.0" encoding="UTF-8"?>
  <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. 293)

Root level tag for the TagKeys parameters.

Required: Yes

Items (p. 293)

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. 555).
AccessDenied

Access denied.

HTTP Status Code: 403

InvalidArgument

An argument is invalid.

HTTP Status Code: 400

InvalidTagging

The tagging specified is not valid.

HTTP Status Code: 400

NoSuchResource

A resource that was specified is not valid.

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

Updates a cache policy configuration.

When you update a cache policy configuration, all the fields are updated with the values provided in the request. You cannot update some fields independent of others. To update a cache policy configuration:

1. Use GetCachePolicyConfig to get the current configuration.
2. Locally modify the fields in the cache policy configuration that you want to update.
3. Call UpdateCachePolicy by providing the entire cache policy configuration, including the fields that you modified and those that you didn't.

Request Syntax

```
PUT /2020-05-31/cache-policy/Id HTTP/1.1
<?xml version="1.0" encoding="UTF-8"?>
  <Comment>string</Comment>
  <DefaultTTL>long</DefaultTTL>
  <MaxTTL>long</MaxTTL>
  <MinTTL>long</MinTTL>
  <Name>string</Name>
  <ParametersInCacheKeyAndForwardedToOrigin>
    <CookiesConfig>
      <CookieBehavior>string</CookieBehavior>
      <Cookies>
        <Items>
          <Name>string</Name>
        </Items>
        <Quantity>integer</Quantity>
      </Cookies>
    </CookiesConfig>
    <EnableAcceptEncodingBrotli>boolean</EnableAcceptEncodingBrotli>
    <EnableAcceptEncodingGzip>boolean</EnableAcceptEncodingGzip>
    <HeadersConfig>
      <HeaderBehavior>string</HeaderBehavior>
      <Headers>
        <Items>
          <Name>string</Name>
        </Items>
        <Quantity>integer</Quantity>
      </Headers>
    </HeadersConfig>
    <QueryStringsConfig>
      <QueryStringBehavior>string</QueryStringBehavior>
      <QueryStrings>
        <Items>
          <Name>string</Name>
        </Items>
        <Quantity>integer</Quantity>
      </QueryStrings>
    </QueryStringsConfig>
  </ParametersInCacheKeyAndForwardedToOrigin>
</CachePolicyConfig>
```

URI Request Parameters

The request does not use any URI parameters.
Request Body

The request accepts the following data in XML format.

**CachePolicyConfig (p. 295)**

Root level tag for the CachePolicyConfig parameters.

- **Required:** Yes

**Comment (p. 295)**

A comment to describe the cache policy. The comment cannot be longer than 128 characters.

- **Type:** String
- **Required:** No

**DefaultTTL (p. 295)**

The default amount of time, in seconds, that you want objects to stay in the CloudFront cache before CloudFront sends another request to the origin to see if the object has been updated. CloudFront uses this value as the object's time to live (TTL) only when the origin does not send Cache-Control or Expires headers with the object. For more information, see Managing How Long Content Stays in an Edge Cache (Expiration) in the Amazon CloudFront Developer Guide.

The default value for this field is 86400 seconds (one day). If the value of MinTTL is more than 86400 seconds, then the default value for this field is the same as the value of MinTTL.

- **Type:** Long
- **Required:** No

**MaxTTL (p. 295)**

The maximum amount of time, in seconds, that objects stay in the CloudFront cache before CloudFront sends another request to the origin to see if the object has been updated. CloudFront uses this value only when the origin sends Cache-Control or Expires headers with the object. For more information, see Managing How Long Content Stays in an Edge Cache (Expiration) in the Amazon CloudFront Developer Guide.

The default value for this field is 31536000 seconds (one year). If the value of MinTTL or DefaultTTL is more than 31536000 seconds, then the default value for this field is the same as the value of DefaultTTL.

- **Type:** Long
- **Required:** No

**MinTTL (p. 295)**

The minimum amount of time, in seconds, that you want objects to stay in the CloudFront cache before CloudFront sends another request to the origin to see if the object has been updated. For more information, see Managing How Long Content Stays in an Edge Cache (Expiration) in the Amazon CloudFront Developer Guide.

- **Type:** Long
- **Required:** Yes

**Name (p. 295)**

A unique name to identify the cache policy.

- **Type:** String
Required: Yes

**ParametersInCacheKeyAndForwardedToOrigin (p. 295)**

The HTTP headers, cookies, and URL query strings to include in the cache key. The values included in the cache key are automatically included in requests that CloudFront sends to the origin.

Type: **ParametersInCacheKeyAndForwardedToOrigin (p. 489)** object

Required: No

### Response Syntax

```
HTTP/1.1 200
<?xml version="1.0" encoding="UTF-8"?>
<CachePolicy>
  <CachePolicyConfig>
    <Comment>string</Comment>
    <DefaultTTL>long</DefaultTTL>
    <MaxTTL>long</MaxTTL>
    <MinTTL>long</MinTTL>
    <Name>string</Name>
    <ParametersInCacheKeyAndForwardedToOrigin>
      <CookiesConfig>
        <CookieBehavior>string</CookieBehavior>
        <Cookies>
          <Items>
            <Name>string</Name>
          </Items>
          <Quantity>integer</Quantity>
        </Cookies>
      </CookiesConfig>
      <EnableAcceptEncodingBrotli>boolean</EnableAcceptEncodingBrotli>
      <EnableAcceptEncodingGzip>boolean</EnableAcceptEncodingGzip>
      <HeadersConfig>
        <HeaderBehavior>string</HeaderBehavior>
        <Headers>
          <Items>
            <Name>string</Name>
          </Items>
          <Quantity>integer</Quantity>
        </Headers>
      </HeadersConfig>
      <QueryStringsConfig>
        <QueryStringBehavior>string</QueryStringBehavior>
        <QueryStrings>
          <Items>
            <Name>string</Name>
          </Items>
          <Quantity>integer</Quantity>
        </QueryStrings>
      </QueryStringsConfig>
    </ParametersInCacheKeyAndForwardedToOrigin>
  </CachePolicyConfig>
  <Id>string</Id>
  <LastModifiedTime>timestamp</LastModifiedTime>
</CachePolicy>
```

### 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.

**CachePolicy (p. 297)**
Root level tag for the CachePolicy parameters.
Required: Yes

**CachePolicyConfig (p. 297)**
The cache policy configuration.
Type: CachePolicyConfig (p. 381) object

**Id (p. 297)**
The unique identifier for the cache policy.
Type: String

**LastModifiedTime (p. 297)**
The date and time when the cache policy was last modified.
Type: Timestamp

## Errors
For information about the errors that are common to all actions, see **Common Errors (p. 555)**.

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

**CachePolicyAlreadyExists**
A cache policy with this name already exists. You must provide a unique name. To modify an existing cache policy, use UpdateCachePolicy.
HTTP Status Code: 409

**IllegalUpdate**
The update contains modifications that are not allowed.
HTTP Status Code: 400

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

**InvalidArgument**
An argument is invalid.
HTTP Status Code: 400

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

The cache policy does not exist.

HTTP Status Code: 404

PreconditionFailed

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

HTTP Status Code: 412

TooManyCookiesInCachePolicy

The number of cookies in the cache policy exceeds the maximum. For more information, see Quotas (formerly known as limits) in the Amazon CloudFront Developer Guide.

HTTP Status Code: 400

TooManyHeadersInCachePolicy

The number of headers in the cache policy exceeds the maximum. For more information, see Quotas (formerly known as limits) in the Amazon CloudFront Developer Guide.

HTTP Status Code: 400

TooManyQueryStringsInCachePolicy

The number of query strings in the cache policy exceeds the maximum. For more information, see Quotas (formerly known as limits) in the Amazon CloudFront Developer Guide.

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

Update an origin access identity.

Request Syntax

```
PUT /2020-05-31/origin-access-identity/cloudfront/Id/config HTTP/1.1
<?xml version="1.0" encoding="UTF-8"?>
  doc/2020-05-31/"/>
  <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. 300)

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

CallerReference (p. 300)

- 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 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. 300)

- A comment to describe the origin access identity. The comment cannot be longer than 128 characters.
  - Type: String
  - Required: Yes
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. 301)

Root level tag for the CloudFrontOriginAccessIdentity parameters.

Required: Yes

CloudFrontOriginAccessIdentityConfig (p. 301)

The current configuration information for the identity.

Type: CloudFrontOriginAccessIdentityConfig (p. 389) object

Id (p. 301)

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

Type: String

S3CanonicalUserld (p. 301)

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. 555).

AccessDenied

Access denied.

HTTP Status Code: 403

IllegalUpdate

The update contains modifications that are not allowed.

HTTP Status Code: 400
InconsistentQuantities

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

HTTP Status Code: 400

InvalidArgument

An argument is invalid.

HTTP Status Code: 400

InvalidIfMatchVersion

The If-Match version is missing or not valid.

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 in one or more of the request 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 V2
- AWS SDK for JavaScript
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3
UpdateDistribution

Updates the configuration for a web distribution.

Important
When you update a distribution, there are more required fields than when you create a distribution. When you update your distribution by using this API action, follow the steps here to get the current configuration and then make your updates, to make sure that you include all of the required fields. To view a summary, see Required Fields for Create Distribution and Update Distribution in the Amazon CloudFront Developer Guide.

The update process includes getting the current distribution configuration, updating the XML document that is returned to make your changes, and then submitting an UpdateDistribution request to make the updates.

For information about updating a distribution using the CloudFront console instead, see Creating a Distribution in the Amazon CloudFront Developer Guide.

To update a web distribution using the CloudFront API

1. Submit a GetDistributionConfig request to get the current configuration and an ETag header for the distribution.

   Note
   If you update the distribution again, you must get a new ETag header.

2. Update the XML document that was returned in the response to your GetDistributionConfig request to include your changes.

   Important
   When you edit the XML file, be aware of the following:
   • You must strip out the ETag parameter that is returned.
   • Additional fields are required when you update a distribution. There may be fields included in the XML file for features that you haven't configured for your distribution. This is expected and required to successfully update the distribution.
   • You can't change the value of CallerReference. If you try to change this value, CloudFront returns an IllegalUpdate error.
   • The new configuration replaces the existing configuration; the values that you specify in an UpdateDistribution request are not merged into your 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 request to confirm that your changes have propagated. When propagation is complete, the value of Status is Deployed.

Request Syntax

```
PUT /2020-05-31/distribution/Id/config HTTP/1.1
```
API Version 2020-05-31
305
Request Syntax

```xml
<Name>string</Name>
</Items>
<Quantity>integer</Quantity>
</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>
<FunctionAssociations>
<Items>
<FunctionAssociation>
<EventType>string</EventType>
<FunctionARN>string</FunctionARN>
</FunctionAssociation>
</Items>
<Quantity>integer</Quantity>
</FunctionAssociations>
<LambdaFunctionAssociations>
<Items>
<LambdaFunctionAssociation>
<EventType>string</EventType>
<IncludeBody>boolean</IncludeBody>
<LambdaFunctionARN>string</LambdaFunctionARN>
</LambdaFunctionAssociation>
</Items>
<Quantity>integer</Quantity>
</LambdaFunctionAssociations>
<MaxTTL>long</MaxTTL>
<MinTTL>long</MinTTL>
<OriginRequestPolicyId>string</OriginRequestPolicyId>
<RealtimeLogConfigArn>string</RealtimeLogConfigArn>
<ResponseHeadersPolicyId>string</ResponseHeadersPolicyId>
<SmoothStreaming>boolean</SmoothStreaming>
<TargetOriginId>string</TargetOriginId>
<TrustedKeyGroups>
<Items>
<KeyGroup>string</KeyGroup>
</Items>
<Quantity>integer</Quantity>
</TrustedKeyGroups>
<TrustedSigners>
<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>
<OriginGroups>
<Items>
-OriginGroup>
-FailoverCriteria>
-StatusCodes>
-Quantity>integer</Quantity>
</StatusCodes>
</FailoverCriteria>
<Id>string</Id>
<Members>
<Items>
-OriginGroupMember>
-OriginId>string</OriginId>
</Items>
</Members>
</OriginGroup>
</Items>
<OriginGroups>
<Items>
-Origin>
-ConnectionAttempts>integer</ConnectionAttempts>
-ConnectionTimeout>integer</ConnectionTimeout>
</CustomHeaders>
</OriginCustomHeader>
<Items>
-OriginCustomHeader>
-HeaderName>string</HeaderName>
-HeaderValue>string</HeaderValue>
</Items>
</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>
-OriginShield>
-Enabled>boolean</Enabled>
-OriginShieldRegion>string</OriginShieldRegion>
</OriginShield>
</S3OriginConfig>
-OriginAccessIdentity>string</OriginAccessIdentity>
</S3OriginConfig>
URI Request Parameters

The request does not use any URI parameters.

Request Body

The request accepts the following data in XML format.

**DistributionConfig (p. 303)**

Root level tag for the DistributionConfig parameters.

Required: Yes

**Aliases (p. 303)**

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

Type: Aliases (p. 369) object

Required: No

**CacheBehaviors (p. 303)**

A complex type that contains zero or more CacheBehavior elements.

Type: CacheBehaviors (p. 378) object

Required: No

**CallerReference (p. 303)**

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 that you already sent in a previous request to create a distribution, CloudFront returns a `DistributionAlreadyExists` error.

Type: String
Required: Yes

**Comment (p. 303)**

An optional comment to describe the distribution. The comment cannot be longer than 128 characters.

Type: String
Required: Yes

**CustomErrorResponses (p. 303)**

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. 403)` object
Required: No

**DefaultCacheBehavior (p. 303)**

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. 407)` object
Required: Yes

**DefaultRootObject (p. 303)**

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. 303)
From this field, you can enable or disable the selected distribution.
Type: Boolean
Required: Yes

HttpVersion (p. 303)
(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 "http2 optimization."
Type: String
Valid Values: http1.1 | http2
Required: No

IsIPV6Enabled (p. 303)
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 AWS Integration 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 AWS Integration Developer Guide.

If you created a CNAME resource record set, either with Amazon Route 53 AWS Integration 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. 303)
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. 466) object

Required: No

OriginGroups (p. 303)

A complex type that contains information about origin groups for this distribution.

Type: OriginGroups (p. 477) object

Required: No

Origins (p. 303)

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

Type: Origins (p. 486) object

Required: Yes

PriceClass (p. 303)

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 (such as Price Class 100) map to CloudFront regions, see Amazon CloudFront Pricing.

Type: String

Valid Values: PriceClass_100 | PriceClass_200 | PriceClass_All

Required: No

Restrictions (p. 303)

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

Type: Restrictions (p. 528) object

Required: No

ViewerCertificate (p. 303)

A complex type that determines the distribution's SSL/TLS configuration for communicating with viewers.

Type: ViewerCertificate (p. 549) object

Required: No

WebACLId (p. 303)

A unique identifier that specifies the AWS WAF web ACL, if any, to associate with this distribution. To specify a web ACL created using the latest version of AWS WAF, use the ACL ARN, for example arn:aws:wafv2:us-east-1:123456789012:global/webacl/ExampleWebACL/473e64fd-
f30b-4765-81a0-62ad96dd167a. To specify a web ACL created using AWS WAF Classic, use the ACL ID, for example 473e64fd-f30b-4765-81a0-62ad96dd167a.

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>
  <ActiveTrustedKeyGroups>
    <Enabled>boolean</Enabled>
    <Items>
      <KeyGroup>
        <KeyGroupId>string</KeyGroupId>
        <KeyPairIds>
          <Items>
            <KeyPairId>string</KeyPairId>
          </Items>
          <Quantity>integer</Quantity>
        </KeyPairIds>
      </KeyGroup>
    </Items>
    <Quantity>integer</Quantity>
  </ActiveTrustedKeyGroups>
  <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>
  <AliasICPRecordals>
    <AliasICPRecordal>
      <CNAME>string</CNAME>
      <ICPRecordalStatus>string</ICPRecordalStatus>
    </AliasICPRecordal>
  </AliasICPRecordals>
  <ARN>string</ARN>
  <DistributionConfig>
    <Aliases>
      <Items>
        <CNAME>string</CNAME>
      </Items>
      <Quantity>integer</Quantity>
    </Aliases>
```
</Aliases>
<CacheBehaviors>
  <Items>
    <CacheBehavior>
      <AllowedMethods>
        <CachedMethods>
          <Items>
            <Method>string</Method>
            <Quantity>integer</Quantity>
          </Items>
        </CachedMethods>
        <Items>
          <Method>string</Method>
          <Quantity>integer</Quantity>
        </Items>
      </AllowedMethods>
      <CachePolicyId>string</CachePolicyId>
      <Compress>boolean</Compress>
      <DefaultTTL>long</DefaultTTL>
      <FieldLevelEncryptionId>string</FieldLevelEncryptionId>
      <ForwardedValues>
        <Cookies>
          <WhitelistedNames>
            <Items>
              <Name>string</Name>
            </Items>
            <Quantity>integer</Quantity>
          </WhitelistedNames>
        </Cookies>
        <Headers>
          <Items>
            <Name>string</Name>
            <Quantity>integer</Quantity>
          </Items>
        </Headers>
        <QueryString>boolean</QueryString>
        <QueryStringCacheKeys>
          <Items>
            <Name>string</Name>
          </Items>
          <Quantity>integer</Quantity>
        </QueryStringCacheKeys>
      </ForwardedValues>
      <FunctionAssociations>
        <Items>
          <FunctionAssociation>
            <EventType>string</EventType>
            <FunctionARN>string</FunctionARN>
          </FunctionAssociation>
        </Items>
        <Quantity>integer</Quantity>
      </FunctionAssociations>
      <LambdaFunctionAssociations>
        <Items>
          <LambdaFunctionAssociation>
            <EventType>string</EventType>
            <IncludeBody>boolean</IncludeBody>
            <LambdaFunctionARN>string</LambdaFunctionARN>
          </LambdaFunctionAssociation>
        </Items>
        <Quantity>integer</Quantity>
      </LambdaFunctionAssociations>
    </CacheBehavior>
  </Items>
</CacheBehaviors>
<PathPattern>string</PathPattern>
<RealtimeLogConfigArn>string</RealtimeLogConfigArn>
<ResponseHeadersPolicyId>string</ResponseHeadersPolicyId>
<SmoothStreaming>boolean</SmoothStreaming>
<TargetOriginId>string</TargetOriginId>
<TrustedKeyGroups>
  <Enabled>boolean</Enabled>
  <Items>
    <KeyGroup>string</KeyGroup>
  </Items>
</TrustedKeyGroups>
<TrustedSigners>
  <Enabled>boolean</Enabled>
  <Items>
    <AwsAccountNumber>string</AwsAccountNumber>
  </Items>
</TrustedSigners>
<ViewerProtocolPolicy>string</ViewerProtocolPolicy>
</CacheBehavior>
</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>
  <CachePolicyId>string</CachePolicyId>
  <Compress>boolean</Compress>
  <DefaultTTL>long</DefaultTTL>
  <FieldLevelEncryptionId>string</FieldLevelEncryptionId>
  <ForwardedValues>
    <Cookies>
      <Forward>string</Forward>
    </Cookies>
  </ForwardedValues>
  <Headers>
    <Items>
      <Name>string</Name>
    </Items>
  </Headers>
</DefaultCacheBehavior>
<Name>string</Name>
</Items>
<Quantity>integer</Quantity>
</Headers>
<QueryString>boolean</QueryString>
<QueryStringCacheKeys>
<Items>
</Items>
<Quantity>integer</Quantity>
</QueryStringCacheKeys>
</ForwardedValues>
<FunctionAssociations>
<Items>
</Items>
<Quantity>integer</Quantity>
</FunctionAssociations>
<LambdaFunctionAssociations>
<Items>
</Items>
<Quantity>integer</Quantity>
</LambdaFunctionAssociations>
<MaxTTL>long</MaxTTL>
<MinTTL>long</MinTTL>
-OriginRequestPolicyId>string</OriginRequestPolicyId>
<RealtimeLogConfigArn>string</RealtimeLogConfigArn>
<ResponseHeadersPolicyId>string</ResponseHeadersPolicyId>
<SmoothStreaming>boolean</SmoothStreaming>
<TargetOriginId>string</TargetOriginId>
<TrustedKeyGroups>
<Enabled>boolean</Enabled>
<Items>
</Items>
<Quantity>integer</Quantity>
</TrustedKeyGroups>
<TrustedSigners>
<Enabled>boolean</Enabled>
<Items>
</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>
<OriginGroups>
<Items>
Amazon CloudFront API Reference
Response Syntax

```xml
<OriginGroup>
  <FailoverCriteria>
    <StatusCodes>
      <Items>
        <StatusCode>integer</StatusCode>
      </Items>
      <Quantity>integer</Quantity>
    </StatusCodes>
    <FailoverCriteria>
      <Id>string</Id>
      <Members>
        <Items>
          <OriginGroupMember>
            <OriginId>string</OriginId>
          </OriginGroupMember>
        </Items>
        <Quantity>integer</Quantity>
      </Members>
    </FailoverCriteria>
    <Id>string</Id>
    <Members>
      <Items>
        <OriginGroupMember>
          <OriginId>string</OriginId>
        </OriginGroupMember>
      </Items>
      <Quantity>integer</Quantity>
    </Members>
  </FailoverCriteria>
  <Quantity>integer</Quantity>
</OriginGroups>
<Origins>
  <Items>
    <Origin>
      <ConnectionAttempts>integer</ConnectionAttempts>
      <ConnectionTimeout>integer</ConnectionTimeout>
      <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>
      <OriginShield>
        <Enabled>boolean</Enabled>
        <OriginShieldRegion>string</OriginShieldRegion>
      </OriginShield>
    </Origin>
  </Items>
  <Quantity>integer</Quantity>
</Origins>
<PriceClass>string</PriceClass>
<Restrictions>
  <GeoRestriction>
  </GeoRestriction>
</ResponseSyntax>
```
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. 312)**

Root level tag for the Distribution parameters.

Required: Yes

**ActiveTrustedKeyGroups (p. 312)**

CloudFront automatically adds this field to the response if you've configured a cache behavior in this distribution to serve private content using key groups. This field contains a list of key groups and the public keys in each key group that CloudFront can use to verify the signatures of signed URLs or signed cookies.

Type: ActiveTrustedKeyGroups (p. 367) object

**ActiveTrustedSigners (p. 312)**

**Important**

We recommend using TrustedKeyGroups instead of TrustedSigners.

CloudFront automatically adds this field to the response if you've configured a cache behavior in this distribution to serve private content using trusted signers. This field contains a list of AWS account IDs and the active CloudFront key pairs in each account that CloudFront can use to verify the signatures of signed URLs or signed cookies.

Type: ActiveTrustedSigners (p. 368) object

**AliasICPRecordals (p. 312)**

AWS services in China customers must file for an Internet Content Provider (ICP) recordal if they want to serve content publicly on an alternate domain name, also known as a CNAME, that they've added to CloudFront. AliasICPRecordal provides the ICP recordal status for CNAMEs associated with distributions.
Errors

For more information about ICP recordals, see Signup, Accounts, and Credentials in Getting Started with AWS services in China.

Type: Array of AliasICPRecordal (p. 370) objects

ARN (p. 312)

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. 312)

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

Type: DistributionConfig (p. 414) object

DomainName (p. 312)

The domain name corresponding to the distribution, for example, d111111abcde8.cloudfront.net.

Type: String

Id (p. 312)

The identifier for the distribution. For example: EDFDVBD632BHDS5.

Type: String

InProgressInvalidationBatches (p. 312)

The number of invalidation batches currently in progress.

Type: Integer

LastModifiedTime (p. 312)

The date and time the distribution was last modified.

Type: Timestamp

Status (p. 312)

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. 555).

AccessDenied

Access denied.

HTTP Status Code: 403

CNAMEAlreadyExists

The CNAME specified is already defined for CloudFront.
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
The update contains modifications that are not allowed.

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

HTTP Status Code: 400
InvalidArgument
An 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
An invalid error code was specified.

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
InvalidFunctionAssociation
A CloudFront function association is invalid.

HTTP Status Code: 400
InvalidGeoRestrictionParameter
The specified geo restriction parameter is not valid.

HTTP Status Code: 400
InvalidHeadersForS3Origin
The headers specified are not valid for an Amazon S3 origin.

HTTP Status Code: 400
InvalidIfMatchVersion
The If-Match version is missing or not valid.
HTTP Status Code: 400
**InvalidLambdaFunctionAssociation**
The specified Lambda@Edge function association is invalid.

HTTP Status Code: 400
**InvalidLocationCode**
The location code specified is not valid.

HTTP Status Code: 400
**InvalidMinimumProtocolVersion**
The minimum protocol version specified is not valid.

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

HTTP Status Code: 400
**InvalidOriginKeepaliveTimeout**
The keep alive timeout specified for the origin is not valid.

HTTP Status Code: 400
**InvalidOriginReadTimeout**
The read timeout specified for the origin is not valid.

HTTP Status Code: 400
**InvalidQueryStringParameters**
The query string parameters specified are not valid.

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**
A response code is not valid.

HTTP Status Code: 400
**InvalidTTLOrder**
The TTL order specified is not valid.

HTTP Status Code: 400
InvalidViewerCertificate

A viewer certificate specified is not valid.

HTTP Status Code: 400

InvalidWebACLId

A web ACL ID specified is not valid. To specify a web ACL created using the latest version of AWS WAF, use the ACL ARN, for example `arn:aws:wafv2:us-east-1:123456789012:global/webacl/ExampleWebACL/473e64fd-f30b-4765-81a0-62ad96dd167a`. To specify a web ACL created using AWS WAF Classic, use the ACL ID, for example `473e64fd-f30b-4765-81a0-62ad96dd167a`.

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

NoSuchCachePolicy

The cache policy does not exist.

HTTP Status Code: 404

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

NoSuchOriginRequestPolicy

The origin request policy does not exist.

HTTP Status Code: 404

NoSuchRealtimeLogConfig

The real-time log configuration does not exist.

HTTP Status Code: 404

NoSuchResponseHeadersPolicy

The response headers policy does not exist.

HTTP Status Code: 404

PreconditionFailed

The precondition in one or more of the request fields evaluated to false.
HTTP Status Code: 412
**RealtimeLogConfigOwnerMismatch**

The specified real-time log configuration belongs to a different AWS account.

HTTP Status Code: 401
**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
**TooManyDistributionsAssociatedToCachePolicy**

The maximum number of distributions have been associated with the specified cache policy. For more information, see Quotas (formerly known as limits) in the Amazon CloudFront Developer Guide.

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
**TooManyDistributionsAssociatedToKeyGroup**

The number of distributions that reference this key group is more than the maximum allowed. For more information, see Quotas (formerly known as limits) in the Amazon CloudFront Developer Guide.

HTTP Status Code: 400
**TooManyDistributionsAssociatedToOriginRequestPolicy**

The maximum number of distributions have been associated with the specified origin request policy. For more information, see Quotas (formerly known as limits) in the Amazon CloudFront Developer Guide.

HTTP Status Code: 400
**TooManyDistributionsAssociatedToResponseHeadersPolicy**

The maximum number of distributions have been associated with the specified response headers policy.

For more information, see Quotas (formerly known as limits) in the Amazon CloudFront Developer Guide.
HTTP Status Code: 400
TooManyDistributionsWithFunctionAssociations
You have reached the maximum number of distributions that are associated with a CloudFront function. For more information, see Quotas (formerly known as limits) in the Amazon CloudFront Developer Guide.

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

HTTP Status Code: 400
TooManyDistributionsWithSingleFunctionARN
The maximum number of distributions have been associated with the specified Lambda@Edge function.

HTTP Status Code: 400
TooManyFunctionAssociations
You have reached the maximum number of CloudFront function associations for this distribution. For more information, see Quotas (formerly known as limits) in the Amazon CloudFront Developer Guide.

HTTP Status Code: 400
TooManyHeadersInForwardedValues
Your request contains too many headers in forwarded values.

HTTP Status Code: 400
TooManyKeyGroupsAssociatedToDistribution
The number of key groups referenced by this distribution is more than the maximum allowed. For more information, see Quotas (formerly known as limits) in the Amazon CloudFront Developer Guide.

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

HTTP Status Code: 400
TooManyOriginCustomHeaders
Your request contains too many origin custom headers.

HTTP Status Code: 400
TooManyOriginGroupsPerDistribution
Processing your request would cause you to exceed the maximum number of origin groups allowed.

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

Your request contains too many query string parameters.

HTTP Status Code: 400

TooManyTrustedSigners

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

HTTP Status Code: 400

TrustedKeyGroupDoesNotExist

The specified key group does not exist.

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

Update a field-level encryption configuration.

Request Syntax

PUT /2020-05-31/field-level-encryption/Id/config HTTP/1.1
<?xml version="1.0" encoding="UTF-8"?>
  <CallerReference>string</CallerReference>
  <Comment>string</Comment>
  <ContentTypeProfileConfig>
    <contentTypeProfileConfig>
      <contentTypeProfile>
        <contentType>string</contentType>
        <Format>string</Format>
        <ProfileId>string</ProfileId>
      </contentTypeProfile>
    </contentTypeProfileConfig>
    <Quantity>integer</Quantity>
  </ContentTypeProfiles>
  <ForwardWhenContentTypeIsUnknown>boolean</ForwardWhenContentTypeIsUnknown>
</ContentTypeProfileConfig>
  <QueryArgProfileConfig>
    <QueryArgProfileConfig>
      <QueryArgProfileIsUnknown>boolean</QueryArgProfileIsUnknown>
    <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. 325)

Root level tag for the FieldLevelEncryptionConfig parameters.

  Required: Yes

CallerReference (p. 325)

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

  Type: String
  Required: Yes
Comment (p. 325)

An optional comment about the configuration. The comment cannot be longer than 128 characters.

Type: String
Required: No

ContentTypeProfileConfig (p. 325)

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. 396) object
Required: No

QueryArgProfileConfig (p. 325)

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. 497) object
Required: No

Response Syntax

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>
      </ContentTypeProfiles>
      <ForwardWhenContentTypeIsUnknown>boolean</ForwardWhenContentTypeIsUnknown>
    </ContentTypeProfileConfig>
    <QueryArgProfileConfig>
      <QueryArgProfiles>
        <Items>
          <QueryArgProfile>
            <ProfileId>string</ProfileId>
            <QueryArg>string</QueryArg>
          </QueryArgProfile>
        </Items>
      </QueryArgProfiles>
      <ForwardWhenQueryArgProfileIsUnknown>boolean</ForwardWhenQueryArgProfileIsUnknown>
    </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. 326)

Root level tag for the FieldLevelEncryption parameters.
Required: Yes

FieldLevelEncryptionConfig (p. 326)

A complex data type that includes the profile configurations specified for field-level encryption.
Type: FieldLevelEncryptionConfig (p. 431) object

Id (p. 326)

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. 326)

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. 555).

AccessDenied

Access denied.
HTTP Status Code: 403

IllegalUpdate

The update contains modifications that are not allowed.
HTTP Status Code: 400

InconsistentQuantities

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

InvalidArgument

An argument is invalid.
HTTP Status Code: 400

InvalidIfMatchVersion

The If-Match version is missing or not valid.
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 in one or more of the request 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 V2
- AWS SDK for JavaScript
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3
UpdateFieldLevelEncryptionProfile

Update a field-level encryption profile.

Request Syntax

PUT /2020-05-31/field-level-encryption-profile/Id/config HTTP/1.1
<?xml version="1.0" encoding="UTF-8"?>
  <CallerReference>string</CallerReference>
  <Comment>string</Comment>
  <EncryptionEntities>
    <Items>
      <EncryptionEntity>
        <FieldPatterns>
          <Fields>
            <FieldPattern>string</FieldPattern>
          </Fields>
          <Quantity>integer</Quantity>
        </FieldPatterns>
        <ProviderId>string</ProviderId>
        <PublicKeyId>string</PublicKeyId>
      </EncryptionEntity>
    </Items>
  </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. 329)

Root level tag for the FieldLevelEncryptionProfileConfig parameters.

Required: Yes

CallerReference (p. 329)

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

Type: String

Required: Yes

Comment (p. 329)

An optional comment for the field-level encryption profile. The comment cannot be longer than 128 characters.

Type: String

Required: No
EncryptionEntities (p. 329)

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. 427) object

Required: Yes

Name (p. 329)

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. 330)

Root level tag for the FieldLevelEncryptionProfile parameters.

Required: Yes

FieldLevelEncryptionProfileConfig (p. 330)

A complex data type that includes the profile name and the encryption entities for the field-level
encryption profile.
Type: FieldLevelEncryptionProfileConfig (p. 434) object

**Id (p. 330)**

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. 330)**

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. 555).

**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**

The update contains modifications that are not allowed.

HTTP Status Code: 400

**InconsistentQuantities**

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

HTTP Status Code: 400

**InvalidArgument**

An argument is invalid.

HTTP Status Code: 400

**InvalidIfMatchVersion**

The If-Match version is missing or not valid.

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 in one or more of the request 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 V2
- AWS SDK for JavaScript
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3
UpdateFunction

Updates a CloudFront function.

You can update a function's code or the comment that describes the function. You cannot update a function's name.

To update a function, you provide the function's name and version (ETag value) along with the updated function code. To get the name and version, you can use ListFunctions and DescribeFunction.

Request Syntax

```
PUT /2020-05-31/function/Name HTTP/1.1
If-Match: IfMatch
<?xml version="1.0" encoding="UTF-8"?>
    <FunctionCode>blob</FunctionCode>
    <FunctionConfig>
        <Comment>string</Comment>
        <Runtime>string</Runtime>
    </FunctionConfig>
</UpdateFunctionRequest>
```

URI Request Parameters

The request uses the following URI parameters.

- **If-Match (p. 333)**
  The current version (ETag value) of the function that you are updating, which you can get using DescribeFunction.
  
  Required: Yes

- **Name (p. 333)**
  The name of the function that you are updating.

  Required: Yes

Request Body

The request accepts the following data in XML format.

- **UpdateFunctionRequest (p. 333)**
  Root level tag for the UpdateFunctionRequest parameters.

  Required: Yes

- **FunctionCode (p. 333)**
  The function code. For more information about writing a CloudFront function, see Writing function code for CloudFront Functions in the Amazon CloudFront Developer Guide.

  Type: Base64-encoded binary data object

Required: Yes

**FunctionConfig (p. 333)**

Configuration information about the function.

Type: FunctionConfig (p. 444) object

Required: Yes

### Response Syntax

```xml
HTTP/1.1 200
<?xml version="1.0" encoding="UTF-8"?>
 FunctionSummary
  FunctionConfig
    Comment</string>
    Runtime</string>
  </FunctionConfig>
  FunctionMetadata
    CreatedTime</timestamp>
    FunctionARN</string>
    LastModifiedTime</timestamp>
    Stage</string>
  </FunctionMetadata>
  Name</string>
  Status</string>
 </FunctionSummary>
```

### 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.

**FunctionSummary (p. 334)**

Root level tag for the FunctionSummary parameters.

Required: Yes

**FunctionConfig (p. 334)**

Contains configuration information about a CloudFront function.

Type: FunctionConfig (p. 444) object

**FunctionMetadata (p. 334)**

Contains metadata about a CloudFront function.

Type: FunctionMetadata (p. 446) object

**Name (p. 334)**

The name of the CloudFront function.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 64.

Pattern: ^[a-zA-Z0-9-]{1,64}$

---

API Version 2020-05-31

334
Status (p. 334)
The status of the CloudFront function.
Type: String

Errors
For information about the errors that are common to all actions, see Common Errors (p. 555).

FunctionSizeLimitExceeded
The function is too large. For more information, see Quotas (formerly known as limits) in the Amazon CloudFront Developer Guide.

HTTP Status Code: 413

InvalidArgument
An argument is invalid.

HTTP Status Code: 400

InvalidIfMatchVersion
The If-Match version is missing or not valid.

HTTP Status Code: 400

NoSuchFunctionExists
The function does not exist.

HTTP Status Code: 404

PreconditionFailed
The precondition in one or more of the request fields evaluated to false.

HTTP Status Code: 412

UnsupportedOperation
This operation is not supported in this region.

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 V2
- AWS SDK for JavaScript
- AWS SDK for PHP V3
- AWS SDK for Python
• AWS SDK for Ruby V3
UpdateKeyGroup

Updates a key group.

When you update a key group, all the fields are updated with the values provided in the request. You cannot update some fields independent of others. To update a key group:

1. Get the current key group with GetKeyGroup or GetKeyGroupConfig.
2. Locally modify the fields in the key group that you want to update. For example, add or remove public key IDs.
3. Call UpdateKeyGroup with the entire key group object, including the fields that you modified and those that you didn’t.

Request Syntax

```xml
PUT /2020-05-31/key-group/Id HTTP/1.1
<?xml version="1.0" encoding="UTF-8"?>
<KeyGroupConfig xmlns="http://cloudfront.amazonaws.com/doc/2020-05-31/">
  <Comment>string</Comment>
  <Items>
    <PublicKey>string</PublicKey>
  </Items>
  <Name>string</Name>
</KeyGroupConfig>
```

URI Request Parameters

The request does not use any URI parameters.

Request Body

The request accepts the following data in XML format.

KeyGroupConfig (p. 337)

Root level tag for the KeyGroupConfig parameters.

Required: Yes

Comment (p. 337)

A comment to describe the key group. The comment cannot be longer than 128 characters.

Type: String

Required: No

Items (p. 337)

A list of the identifiers of the public keys in the key group.

Type: Array of strings

Required: Yes

Name (p. 337)

A name to identify the key group.
Response Syntax

HTTP/1.1 200
<?xml version="1.0" encoding="UTF-8"?>
<KeyGroup>
  <Id>string</Id>
  <KeyGroupConfig>
    <Comment>string</Comment>
    <Items>
      <PublicKey>string</PublicKey>
      <Name>string</Name>
    </Items>
  </KeyGroupConfig>
  <LastModifiedTime>timestamp</LastModifiedTime>
</KeyGroup>

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.

KeyGroup (p. 338)
  Root level tag for the KeyGroup parameters.
  Required: Yes

Id (p. 338)
  The identifier for the key group.
  Type: String

KeyGroupConfig (p. 338)
  The key group configuration.
  Type: KeyGroupConfig (p. 457) object

LastModifiedTime (p. 338)
  The date and time when the key group was last modified.
  Type: Timestamp

Errors

For information about the errors that are common to all actions, see Common Errors (p. 555).

InvalidArgument
  An argument is invalid.
  HTTP Status Code: 400
InvalidIfMatchVersion

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

HTTP Status Code: 400

**KeyGroupAlreadyExists**

A key group with this name already exists. You must provide a unique name. To modify an existing key group, use `UpdateKeyGroup`.

HTTP Status Code: 409

**NoSuchResource**

A resource that was specified is not valid.

HTTP Status Code: 404

**PreconditionFailed**

The precondition in one or more of the request fields evaluated to `false`.

HTTP Status Code: 412

**TooManyPublicKeysInKeyGroup**

The number of public keys in this key group is more than the maximum allowed. For more information, see Quotas (formerly known as limits) in the Amazon CloudFront Developer Guide.

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

Updates an origin request policy configuration.

When you update an origin request policy configuration, all the fields are updated with the values provided in the request. You cannot update some fields independent of others. To update an origin request policy configuration:

1. Use GetOriginRequestPolicyConfig to get the current configuration.
2. Locally modify the fields in the origin request policy configuration that you want to update.
3. Call UpdateOriginRequestPolicy by providing the entire origin request policy configuration, including the fields that you modified and those that you didn't.

Request Syntax

```
PUT /2020-05-31/origin-request-policy/Id HTTP/1.1
<?xml version="1.0" encoding="UTF-8"?>
  <Comment>string</Comment>
  <CookiesConfig>
    <CookieBehavior>string</CookieBehavior>
    <Cookies>
      <Items>
        <Name>string</Name>
      </Items>
      <Quantity>integer</Quantity>
    </Cookies>
  </CookiesConfig>
  <HeadersConfig>
    <HeaderBehavior>string</HeaderBehavior>
    <Headers>
      <Items>
        <Name>string</Name>
      </Items>
      <Quantity>integer</Quantity>
    </Headers>
  </HeadersConfig>
  <Name>string</Name>
  <QueryStringsConfig>
    <QueryStringBehavior>string</QueryStringBehavior>
    <QueryStrings>
      <Items>
        <Name>string</Name>
      </Items>
      <Quantity>integer</Quantity>
    </QueryStrings>
  </QueryStringsConfig>
</OriginRequestPolicyConfig>
```

URI Request Parameters

The request does not use any URI parameters.

Request Body

The request accepts the following data in XML format.
**OriginRequestPolicyConfig (p. 340)**

Root level tag for the OriginRequestPolicyConfig parameters.

Required: Yes

**Comment (p. 340)**

A comment to describe the origin request policy. The comment cannot be longer than 128 characters.

Type: String

Required: No

**CookiesConfig (p. 340)**

The cookies from viewer requests to include in origin requests.

Type: OriginRequestPolicyCookiesConfig (p. 481) object

Required: Yes

**HeadersConfig (p. 340)**

The HTTP headers to include in origin requests. These can include headers from viewer requests and additional headers added by CloudFront.

Type: OriginRequestPolicyHeadersConfig (p. 482) object

Required: Yes

**Name (p. 340)**

A unique name to identify the origin request policy.

Type: String

Required: Yes

**QueryStringsConfig (p. 340)**

The URL query strings from viewer requests to include in origin requests.

Type: OriginRequestPolicyQueryStringsConfig (p. 484) object

Required: Yes

**Response Syntax**

```
HTTP/1.1 200
<?xml version="1.0" encoding="UTF-8"?>
<OriginRequestPolicy>
  <Id><string /></Id>
  <LastModifiedTime><timestamp /></LastModifiedTime>
  <OriginRequestPolicyConfig>
    <Comment><string /></Comment>
    <CookiesConfig>
      <CookieBehavior><string /></CookieBehavior>
      <Cookies>
        <Items>
          <Name><string /></Name>
        </Items>
      </Cookies>
      <Quantity><integer /></Quantity>
    </CookiesConfig>
  </OriginRequestPolicyConfig>
</OriginRequestPolicy>
```
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.

**OriginRequestPolicy (p. 341)**

Root level tag for the OriginRequestPolicy parameters.

Required: Yes

**Id (p. 341)**

The unique identifier for the origin request policy.

Type: String

**LastModifiedTime (p. 341)**

The date and time when the origin request policy was last modified.

Type: Timestamp

**OriginRequestPolicyConfig (p. 341)**

The origin request policy configuration.

Type: OriginRequestPolicyConfig (p. 479) object

**Errors**

For information about the errors that are common to all actions, see Common Errors (p. 555).

**AccessDenied**

Access denied.

HTTP Status Code: 403
**IllegalUpdate**

The update contains modifications that are not allowed.

HTTP Status Code: 400

**InconsistentQuantities**

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

HTTP Status Code: 400

**InvalidArgument**

An argument is invalid.

HTTP Status Code: 400

**InvalidIfMatchVersion**

The If-Match version is missing or not valid.

HTTP Status Code: 400

**NoSuchOriginRequestPolicy**

The origin request policy does not exist.

HTTP Status Code: 404

**OriginRequestPolicyAlreadyExists**

An origin request policy with this name already exists. You must provide a unique name. To modify an existing origin request policy, use UpdateOriginRequestPolicy.

HTTP Status Code: 409

**PreconditionFailed**

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

HTTP Status Code: 412

**TooManyCookiesInOriginRequestPolicy**

The number of cookies in the origin request policy exceeds the maximum. For more information, see Quotas (formerly known as limits) in the Amazon CloudFront Developer Guide.

HTTP Status Code: 400

**TooManyHeadersInOriginRequestPolicy**

The number of headers in the origin request policy exceeds the maximum. For more information, see Quotas (formerly known as limits) in the Amazon CloudFront Developer Guide.

HTTP Status Code: 400

**TooManyQueryStringsInOriginRequestPolicy**

The number of query strings in the origin request policy exceeds the maximum. For more information, see Quotas (formerly known as limits) in the Amazon CloudFront Developer Guide.

HTTP Status Code: 400

**See Also**

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

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

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

Request Syntax

```
PUT /2020-05-31/public-key/Id/config HTTP/1.1
<?xml version="1.0" encoding="UTF-8"?>
<PublicKeyConfig xmlns="http://cloudfront.amazonaws.com/doc/2020-05-31/">
  <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.

PublicConfig (p. 345)

Root level tag for the PublicKeyConfig parameters.

- Required: Yes

CallerReference (p. 345)

A string included in the request to help make sure that the request can't be replayed.

- Type: String
- Required: Yes

Comment (p. 345)

A comment to describe the public key. The comment cannot be longer than 128 characters.

- Type: String
- Required: No

EncodedKey (p. 345)

The public key that you can use with signed URLs and signed cookies, or with field-level encryption.

- Type: String
- Required: Yes

Name (p. 345)

A name to help identify the public key.

- 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. 346)
  Root level tag for the PublicKey parameters.
  Required: Yes
CREATEDTIME (p. 346)
  The date and time when the public key was uploaded.
  Type: Timestamp
ID (p. 346)
  The identifier of the public key.
  Type: String
PUBLICKEYCONFIG (p. 346)
  Configuration information about a public key that you can use with signed URLs and signed cookies, or with field-level encryption.
  Type: PublicKeyConfig (p. 493) object

Errors

For information about the errors that are common to all actions, see Common Errors (p. 555).

AccessDenied
  Access denied.
  HTTP Status Code: 403
CannotChangeImmutablePublicKeyFields
  You can't change the value of a public key.
  HTTP Status Code: 400
IllegalUpdate

The update contains modifications that are not allowed.

HTTP Status Code: 400

InvalidArgument

An argument is invalid.

HTTP Status Code: 400

InvalidIfMatchVersion

The If-Match version is missing or not valid.

HTTP Status Code: 400

NoSuchPublicKey

The specified public key doesn't exist.

HTTP Status Code: 404

PreconditionFailed

The precondition in one or more of the request 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 V2
- AWS SDK for JavaScript
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3
UpdateRealtimeLogConfig

Updates a real-time log configuration.

When you update a real-time log configuration, all the parameters are updated with the values provided in the request. You cannot update some parameters independent of others. To update a real-time log configuration:

1. Call GetRealtimeLogConfig to get the current real-time log configuration.
2. Locally modify the parameters in the real-time log configuration that you want to update.
3. Call this API (UpdateRealtimeLogConfig) by providing the entire real-time log configuration, including the parameters that you modified and those that you didn’t.

You cannot update a real-time log configuration’s Name or ARN.

Request Syntax

```
PUT /2020-05-31/realtime-log-config/ HTTP/1.1
<?xml version="1.0" encoding="UTF-8"?>
  <ARN>string</ARN>
  <EndPoints>
    <EndPoint>
      <KinesisStreamConfig>
        <RoleARN>string</RoleARN>
        <StreamARN>string</StreamARN>
      </KinesisStreamConfig>
      <StreamType>string</StreamType>
    </EndPoint>
  </EndPoints>
  <Fields>
    <Field>string</Field>
  </Fields>
  <Name>string</Name>
  <SamplingRate>long</SamplingRate>
</UpdateRealtimeLogConfigRequest>
```

URI Request Parameters

The request does not use any URI parameters.

Request Body

The request accepts the following data in XML format.

**UpdateRealtimeLogConfigRequest** (p. 348)

Root level tag for the UpdateRealtimeLogConfigRequest parameters.

Required: Yes

**ARN** (p. 348)

The Amazon Resource Name (ARN) for this real-time log configuration.

Type: String
Required: No

**EndPoints (p. 348)**

Contains information about the Amazon Kinesis data stream where you are sending real-time log data.

Type: Array of [EndPoint (p. 429)] objects

Required: No

**Fields (p. 348)**

A list of fields to include in each real-time log record.


Type: Array of strings

Required: No

**Name (p. 348)**

The name for this real-time log configuration.

Type: String

Required: No

**SamplingRate (p. 348)**

The sampling rate for this real-time log configuration. The sampling rate determines the percentage of viewer requests that are represented in the real-time log data. You must provide an integer between 1 and 100, inclusive.

Type: Long

Required: No

---

**Response Syntax**

```xml
HTTP/1.1 200
<?xml version="1.0" encoding="UTF-8"?>
<UpdateRealtimeLogConfigResult>
  <RealtimeLogConfig>
    <ARN>string</ARN>
    <EndPoints>
      <EndPoint>
        <KinesisStreamConfig>
          <RoleARN>string</RoleARN>
          <StreamARN>string</StreamARN>
        </KinesisStreamConfig>
        <StreamType>string</StreamType>
      </EndPoint>
    </EndPoints>
    <Fields>
      <Field>string</Field>
    </Fields>
    <Name>string</Name>
    <SamplingRate>long</SamplingRate>
  </RealtimeLogConfig>
</UpdateRealtimeLogConfigResult>
```
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.

**UpdateRealtimeLogConfigResult (p. 349)**

Root level tag for the UpdateRealtimeLogConfigResult parameters.

- Required: Yes
- **RealtimeLogConfig (p. 349)**
  - A real-time log configuration.
  - Type: RealtimeLogConfig (p. 501) object

Errors

For information about the errors that are common to all actions, see Common Errors (p. 555).

**AccessDenied**

Access denied.

- HTTP Status Code: 403

**InvalidArgument**

An argument is invalid.

- HTTP Status Code: 400

**NoSuchRealtimeLogConfig**

The real-time log configuration 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 V2
- AWS SDK for JavaScript
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3
UpdateResponseHeadersPolicy

Updates a response headers policy.

When you update a response headers policy, the entire policy is replaced. You cannot update some policy fields independent of others. To update a response headers policy configuration:

1. Use GetResponseHeadersPolicyConfig to get the current policy’s configuration.
2. Modify the fields in the response headers policy configuration that you want to update.
3. Call UpdateResponseHeadersPolicy, providing the entire response headers policy configuration, including the fields that you modified and those that you didn’t.

Request Syntax

```
PUT /2020-05-31/response-headers-policy/Id HTTP/1.1
<?xml version="1.0" encoding="UTF-8"?>
  <Comment>string</Comment>
  <CorsConfig>
    <AccessControlAllowCredentials>boolean</AccessControlAllowCredentials>
    <AccessControlAllowHeaders>
      <Items>
        <Header>string</Header>
      </Items>
      <Quantity>integer</Quantity>
    </AccessControlAllowHeaders>
    <AccessControlAllowMethods>
      <Items>
        <Method>string</Method>
      </Items>
      <Quantity>integer</Quantity>
    </AccessControlAllowMethods>
    <AccessControlAllowOrigins>
      <Items>
        <Origin>string</Origin>
      </Items>
      <Quantity>integer</Quantity>
    </AccessControlAllowOrigins>
    <AccessControlExposeHeaders>
      <Items>
        <Header>string</Header>
      </Items>
      <Quantity>integer</Quantity>
    </AccessControlExposeHeaders>
    <AccessControlMaxAgeSec>integer</AccessControlMaxAgeSec>
    <OriginOverride>boolean</OriginOverride>
  </CorsConfig>
  <CustomHeadersConfig>
    <Items>
      <ResponseHeadersPolicyCustomHeader>
        <Header>string</Header>
        <Override>boolean</Override>
        <Value>string</Value>
      </ResponseHeadersPolicyCustomHeader>
    </Items>
    <Quantity>integer</Quantity>
  </CustomHeadersConfig>
  <Name>string</Name>
  <SecurityHeadersConfig>
    <ContentSecurityPolicy>
```
URI Request Parameters

The request does not use any URI parameters.

Request Body

The request accepts the following data in XML format.

**ResponseHeadersPolicyConfig (p. 351)**

Root level tag for the ResponseHeadersPolicyConfig parameters.

Required: Yes

**Comment (p. 351)**

A comment to describe the response headers policy.

The comment cannot be longer than 128 characters.

Type: String

Required: No

**CorsConfig (p. 351)**

A configuration for a set of HTTP response headers that are used for cross-origin resource sharing (CORS).

Type: `ResponseHeadersPolicyCorsConfig (p. 514)` object
Required: No

**CustomHeadersConfig (p. 351)**

A configuration for a set of custom HTTP response headers.

Type: `ResponseHeadersPolicyCustomHeadersConfig (p. 517)` object

Required: No

**Name (p. 351)**

A name to identify the response headers policy.

The name must be unique for response headers policies in this AWS account.

Type: String

Required: Yes

**SecurityHeadersConfig (p. 351)**

A configuration for a set of security-related HTTP response headers.

Type: `ResponseHeadersPolicySecurityHeadersConfig (p. 521)` object

Required: No

**ServerTimingHeadersConfig (p. 351)**

A configuration for enabling the `Server-Timing` header in HTTP responses sent from CloudFront.

Type: `ResponseHeadersPolicyServerTimingHeadersConfig (p. 523)` object

Required: No

---

**Response Syntax**

```xml
HTTP/1.1 200
<?xml version="1.0" encoding="UTF-8"?>
<ResponseHeadersPolicy>
  <Id>string</Id>
  <LastModifiedTime>timestamp</LastModifiedTime>
  <Comment>string</Comment>
  <CorsConfig>
    <AccessControlAllowCredentials>boolean</AccessControlAllowCredentials>
    <AccessControlAllowHeaders>
      <Items>
        <Header>string</Header>
      </Items>
      <Quantity>integer</Quantity>
    </AccessControlAllowHeaders>
    <AccessControlAllowMethods>
      <Items>
        <Method>string</Method>
      </Items>
      <Quantity>integer</Quantity>
    </AccessControlAllowMethods>
    <AccessControlAllowOrigins>
      <Items>
        <Origin>string</Origin>
      </Items>
    </AccessControlAllowOrigins>
  </CorsConfig>
</ResponseHeadersPolicy>
```

API Version 2020-05-31
353
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.
**ResponseHeadersPolicy (p. 353)**

Root level tag for the ResponseHeadersPolicy parameters.

Required: Yes

**Id (p. 353)**

The identifier for the response headers policy.

Type: String

**LastModifiedTime (p. 353)**

The date and time when the response headers policy was last modified.

Type: Timestamp

**ResponseHeadersPolicyConfig (p. 353)**

A response headers policy configuration.

A response headers policy contains information about a set of HTTP response headers and their values. CloudFront adds the headers in the policy to HTTP responses that it sends for requests that match a cache behavior that's associated with the policy.

Type: ResponseHeadersPolicyConfig (p. 510) object

---

**Errors**

For information about the errors that are common to all actions, see [Common Errors (p. 555)](#).

**AccessDenied**

Access denied.

HTTP Status Code: 403

**IllegalUpdate**

The update contains modifications that are not allowed.

HTTP Status Code: 400

**InconsistentQuantities**

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

HTTP Status Code: 400

**InvalidArgument**

An argument is invalid.

HTTP Status Code: 400

**InvalidIfMatchVersion**

The If-Match version is missing or not valid.

HTTP Status Code: 400

**NoSuchResponseHeadersPolicy**

The response headers policy does not exist.
HTTP Status Code: 404

**PreconditionFailed**

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

HTTP Status Code: 412

**ResponseHeadersPolicyAlreadyExists**

A response headers policy with this name already exists. You must provide a unique name. To modify an existing response headers policy, use `UpdateResponseHeadersPolicy`.

HTTP Status Code: 409

**TooManyCustomHeadersInResponseHeadersPolicy**

The number of custom headers in the response headers policy exceeds the maximum.

For more information, see [Quotas](https://docs.aws.amazon.com/cloudfront/latest/developerguide/quotas.html) (formerly known as limits) in the *Amazon CloudFront Developer Guide*.

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

Update a streaming distribution.

Request Syntax

```
PUT /2020-05-31/streaming-distribution/Id/config HTTP/1.1
<?xml version="1.0" encoding="UTF-8"?>
  <Aliases>
    <Items>
      <CNAME>string</CNAME>
    </Items>
  </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. 357)**

Root level tag for the StreamingDistributionConfig parameters.

Required: Yes

**Aliases (p. 357)**

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

Type: Aliases (p. 369) object
Required: No

**CallerReference (p. 357)**

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 `StreamingDistributionConfig` object), CloudFront creates a new distribution.

If `CallerReference` is a value that you already sent in a previous request to create a distribution, CloudFront returns a `DistributionAlreadyExists` error.

Type: String

Required: Yes

**Comment (p. 357)**

Any comments you want to include about the streaming distribution.

Type: String

Required: Yes

**Enabled (p. 357)**

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

Type: Boolean

Required: Yes

**Logging (p. 357)**

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

Type: `StreamingLoggingConfig (p. 542)` object

Required: No

**PriceClass (p. 357)**

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. 357)**

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. 529)` object

Required: Yes

**TrustedSigners (p. 357)**

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. 548) 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>
  </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. 359)**

Root level tag for the StreamingDistribution parameters.

Required: Yes

**ActiveTrustedSigners (p. 359)**

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. 368) object

**ARN (p. 359)**

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

**DomainName (p. 359)**

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

Type: String

**Id (p. 359)**

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

Type: String

**LastModifiedTime (p. 359)**

The date and time that the distribution was last modified.

Type: Timestamp

**Status (p. 359)**

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. 359)**

The current configuration information for the RTMP distribution.
Errors

For information about the errors that are common to all actions, see Common Errors (p. 555).

AccessDenied
Access denied.
HTTP Status Code: 403

CNAMEAlreadyExists
The CNAME specified is already defined for CloudFront.
HTTP Status Code: 409

IllegalUpdate
The update contains modifications that are not allowed.
HTTP Status Code: 400

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

InvalidArgument
An argument is invalid.
HTTP Status Code: 400

InvalidIfMatchVersion
The If-Match version is missing or not valid.
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 in one or more of the request fields evaluated to false.
HTTP Status Code: 412
**TooManyStreamingDistributionCNAMEs**

Your request contains more CNAMEs than are allowed per distribution.

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

- `ActiveTrustedKeyGroups` (p. 367)
- `ActiveTrustedSigners` (p. 368)
- `Aliases` (p. 369)
- `AliasICPRecordal` (p. 370)
- `AllowedMethods` (p. 371)
- `CacheBehavior` (p. 373)
- `CacheBehaviors` (p. 378)
- `CachedMethods` (p. 379)
- `CachePolicy` (p. 380)
- `CachePolicyConfig` (p. 381)
- `CachePolicyCookiesConfig` (p. 383)
- `CachePolicyHeadersConfig` (p. 384)
- `CachePolicyList` (p. 385)
- `CachePolicyQueryStringsConfig` (p. 386)
- `CachePolicySummary` (p. 387)
- `CloudFrontOriginAccessIdentity` (p. 388)
- `CloudFrontOriginAccessIdentityConfig` (p. 389)
- `CloudFrontOriginAccessIdentityList` (p. 390)
- `CloudFrontOriginAccessIdentitySummary` (p. 392)
- `ConflictingAlias` (p. 393)
- `ConflictingAliasesList` (p. 394)
- `ContentTypeProfile` (p. 395)
- `ContentTypeProfileConfig` (p. 396)
- `ContentTypeProfiles` (p. 397)
- `CookieNames` (p. 398)
- `CookiePreference` (p. 399)
- `CustomErrorResponse` (p. 401)
- `CustomErrorResponses` (p. 403)
- `CustomHeaders` (p. 404)
- `CustomOriginConfig` (p. 405)
- `DefaultCacheBehavior` (p. 407)
- `Distribution` (p. 412)
- `DistributionConfig` (p. 414)
- `DistributionConfigWithTags` (p. 418)
- `DistributionIdList` (p. 419)
• DistributionList (p. 421)
• DistributionSummary (p. 423)
• EncryptionEntities (p. 427)
• EncryptionEntity (p. 428)
• EndPoint (p. 429)
• FieldLevelEncryption (p. 430)
• FieldLevelEncryptionConfig (p. 431)
• FieldLevelEncryptionList (p. 432)
• FieldLevelEncryptionProfile (p. 433)
• FieldLevelEncryptionProfileConfig (p. 434)
• FieldLevelEncryptionProfileList (p. 435)
• FieldLevelEncryptionProfileSummary (p. 436)
• FieldLevelEncryptionSummary (p. 437)
• FieldPatterns (p. 438)
• ForwardedValues (p. 439)
• FunctionAssociation (p. 442)
• FunctionAssociations (p. 443)
• FunctionConfig (p. 444)
• FunctionList (p. 445)
• FunctionMetadata (p. 446)
• FunctionSummary (p. 447)
• GeoRestriction (p. 448)
• Headers (p. 450)
• Invalidation (p. 451)
• InvalidationBatch (p. 452)
• InvalidationList (p. 453)
• InvalidationSummary (p. 455)
• KeyGroup (p. 456)
• KeyGroupConfig (p. 457)
• KeyGroupList (p. 458)
• KeyGroupSummary (p. 459)
• KeyPairIds (p. 460)
• KGKeyPairIds (p. 461)
• KinesisStreamConfig (p. 462)
• LambdaFunctionAssociation (p. 463)
• LambdaFunctionAssociations (p. 465)
• LoggingConfig (p. 466)
• MonitoringSubscription (p. 468)
• Origin (p. 469)
• OriginCustomHeader (p. 472)
• OriginGroup (p. 473)
• OriginGroupFailoverCriteria (p. 474)
• OriginGroupMember (p. 475)
• OriginGroupMembers (p. 476)
• OriginGroups (p. 477)
• OriginRequestPolicy (p. 478)
• StatusCodes (p. 532)
• StreamingDistribution (p. 533)
• StreamingDistributionConfig (p. 535)
• StreamingDistributionConfigWithTags (p. 537)
• StreamingDistributionList (p. 538)
• StreamingDistributionSummary (p. 540)
• StreamingLoggingConfig (p. 542)
• Tag (p. 543)
• TagKeys (p. 544)
• Tags (p. 545)
• TestResult (p. 546)
• TrustedKeyGroups (p. 547)
• TrustedSigners (p. 548)
• ViewerCertificate (p. 549)
ActiveTrustedKeyGroups

A list of key groups, and the public keys in each key group, that CloudFront can use to verify the signatures of signed URLs and signed cookies.

Contents

Enabled

This field is true if any of the key groups have public keys that CloudFront can use to verify the signatures of signed URLs and signed cookies. If not, this field is false.

Type: Boolean
Required: Yes

Items

A list of key groups, including the identifiers of the public keys in each key group that CloudFront can use to verify the signatures of signed URLs and signed cookies.

Type: Array of KGKeyPairIds (p. 461) objects
Required: No

Quantity

The number of key groups in the list.

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 V2
- AWS SDK for Ruby V3
ActiveTrustedSigners

A list of AWS accounts and the active CloudFront key pairs in each account that CloudFront can use to verify the signatures of signed URLs and signed cookies.

Contents

Enabled

This field is `true` if any of the AWS accounts in the list have active CloudFront key pairs that CloudFront can use to verify the signatures of signed URLs and signed cookies. If not, this field is `false`.

Type: Boolean

Required: Yes

Items

A list of AWS accounts and the identifiers of active CloudFront key pairs in each account that CloudFront can use to verify the signatures of signed URLs and signed cookies.

Type: Array of Signer (p. 531) objects

Required: No

Quantity

The number of AWS accounts in the list.

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 V2
- AWS SDK for Ruby V3
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 V2
- AWS SDK for Ruby V3
AWS services in China customers must file for an Internet Content Provider (ICP) recordal if they want to serve content publicly on an alternate domain name, also known as a CNAME, that they've added to CloudFront. AliasICPRecordal provides the ICP recordal status for CNAMEs associated with distributions. The status is returned in the CloudFront response; you can't configure it yourself.

For more information about ICP recordals, see Signup, Accounts, and Credentials in Getting Started with AWS services in China.

### Contents

**CNAME**

A domain name associated with a distribution.

Type: String

Required: No

**ICPRecordalStatus**

The Internet Content Provider (ICP) recordal status for a CNAME. The ICPRecordalStatus is set to APPROVED for all CNAMEs (aliases) in regions outside of China.

The status values returned are the following:

- **APPROVED** indicates that the associated CNAME has a valid ICP recordal number. Multiple CNAMEs can be associated with a distribution, and CNAMEs can correspond to different ICP recordals. To be marked as APPROVED, that is, valid to use with China region, a CNAME must have one ICP recordal number associated with it.

- **SUSPENDED** indicates that the associated CNAME does not have a valid ICP recordal number.

- **PENDING** indicates that CloudFront can't determine the ICP recordal status of the CNAME associated with the distribution because there was an error in trying to determine the status. You can try again to see if the error is resolved in which case CloudFront returns an APPROVED or SUSPENDED status.

Type: String

Valid Values: APPROVED | SUSPENDED | PENDING

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 V2
- AWS SDK for Ruby V3

API Version 2020-05-31
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. 379) 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 V2
• AWS SDK for Ruby V3
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 serve 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 quota (formerly known as limit) on the number of cache behaviors that you can add to a distribution, see Quotas in the Amazon CloudFront Developer Guide.

If you don't want to specify any cache behaviors, include only an empty CacheBehaviors element. Don't include an empty CacheBehavior element because this is invalid.

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 Behavior Settings 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. 371) object

Required: No

CachePolicyId

The unique identifier of the cache policy that is attached to this cache behavior. For more information, see Creating cache policies or Using the managed cache policies in the Amazon CloudFront Developer Guide.

A CacheBehavior must include either a CachePolicyId or ForwardedValues. We recommend that you use a CachePolicyId.

Type: String

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.
**DefaultTTL**

This field is deprecated. We recommend that you use the `DefaultTTL` field in a cache policy instead of this field. For more information, see Creating cache policies or Using the managed cache policies in the *Amazon CloudFront Developer Guide*.

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 Managing How Long Content Stays in an Edge Cache (Expiration) in the *Amazon CloudFront Developer Guide*.

Type: Long

Required: No

**FieldLevelEncryptionId**

The value of `ID` for the field-level encryption configuration that you want CloudFront to use for encrypting specific fields of data for this cache behavior.

Type: String

Required: No

**ForwardedValues**

This field is deprecated. We recommend that you use a cache policy or an origin request policy instead of this field. For more information, see Working with policies in the *Amazon CloudFront Developer Guide*.

If you want to include values in the cache key, use a cache policy. For more information, see Creating cache policies or Using the managed cache policies in the *Amazon CloudFront Developer Guide*.

If you want to send values to the origin but not include them in the cache key, use an origin request policy. For more information, see Creating origin request policies or Using the managed origin request policies in the *Amazon CloudFront Developer Guide*.

A `CacheBehavior` must include either a `CachePolicyId` or `ForwardedValues`. We recommend that you use a `CachePolicyId`.

A complex type that specifies how CloudFront handles query strings, cookies, and HTTP headers.

Type: `ForwardedValues (p. 439)` object

Required: No

**FunctionAssociations**

A list of CloudFront functions that are associated with this cache behavior. CloudFront functions must be published to the `LIVE` stage to associate them with a cache behavior.

Type: `FunctionAssociations (p. 443)` object

Required: No

**LambdaFunctionAssociations**

A complex type that contains zero or more Lambda@Edge function associations for a cache behavior.
Type: LambdaFunctionAssociations (p. 465) object

Required: No

MaxTTL

This field is deprecated. We recommend that you use the MaxTTL field in a cache policy instead of this field. For more information, see Creating cache policies or Using the managed cache policies in the Amazon CloudFront Developer Guide.

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 Managing How Long Content Stays in an Edge Cache (Expiration) in the Amazon CloudFront Developer Guide.

Type: Long

Required: No

MinTTL

This field is deprecated. We recommend that you use the MinTTL field in a cache policy instead of this field. For more information, see Creating cache policies or Using the managed cache policies in the Amazon CloudFront Developer Guide.

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 Managing How Long Content Stays in an 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: No

OriginRequestPolicyId

The unique identifier of the origin request policy that is attached to this cache behavior. For more information, see Creating origin request policies or Using the managed origin request policies in the Amazon CloudFront Developer Guide.

Type: String

Required: No

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
RealtimeLogConfigArn
The Amazon Resource Name (ARN) of the real-time log configuration that is attached to this cache behavior. For more information, see Real-time logs in the Amazon CloudFront Developer Guide.

Type: String
Required: No
ResponseHeadersPolicyId
The identifier for a response headers policy.

Type: String
Required: No
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 they match this cache behavior.

Type: String
Required: Yes
TrustedKeyGroups
A list of key groups that CloudFront can use to validate signed URLs or signed cookies.

When a cache behavior contains trusted key groups, CloudFront requires signed URLs or signed cookies for all requests that match the cache behavior. The URLs or cookies must be signed with a private key whose corresponding public key is in the key group. The signed URL or cookie contains information about which public key CloudFront should use to verify the signature. For more information, see Serving private content in the Amazon CloudFront Developer Guide.

Type: TrustedKeyGroups (p. 547) object
Required: No
TrustedSigners

Important
We recommend using TrustedKeyGroups instead of TrustedSigners.

A list of AWS account IDs whose public keys CloudFront can use to validate signed URLs or signed cookies.

When a cache behavior contains trusted signers, CloudFront requires signed URLs or signed cookies for all requests that match the cache behavior. The URLs or cookies must be signed with the
private key of a CloudFront key pair in the trusted signer's AWS account. The signed URL or cookie contains information about which public key CloudFront should use to verify the signature. For more information, see Serving private content in the Amazon CloudFront Developer Guide.

Type: TrustedSigners (p. 548) object

Required: No

**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 Requiring HTTPS Between Viewers and CloudFront 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 Managing 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 V2
- AWS SDK for Ruby V3
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. 373) 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 V2
- AWS SDK for Ruby V3
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 V2
- AWS SDK for Ruby V3
CachePolicy

A cache policy.

When it’s attached to a cache behavior, the cache policy determines the following:

- The values that CloudFront includes in the cache key. These values can include HTTP headers, cookies, and URL query strings. CloudFront uses the cache key to find an object in its cache that it can return to the viewer.
- The default, minimum, and maximum time to live (TTL) values that you want objects to stay in the CloudFront cache.

The headers, cookies, and query strings that are included in the cache key are automatically included in requests that CloudFront sends to the origin. CloudFront sends a request when it can’t find a valid object in its cache that matches the request’s cache key. If you want to send values to the origin but not include them in the cache key, use OriginRequestPolicy.

Contents

CachePolicyConfig

The cache policy configuration.

Type: CachePolicyConfig (p. 381) object

Required: Yes

Id

The unique identifier for the cache policy.

Type: String

Required: Yes

LastModifiedTime

The date and time when the cache policy was last modified.

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 V2
- AWS SDK for Ruby V3
CachePolicyConfig

A cache policy configuration.

This configuration determines the following:

- The values that CloudFront includes in the cache key. These values can include HTTP headers, cookies, and URL query strings. CloudFront uses the cache key to find an object in its cache that it can return to the viewer.
- The default, minimum, and maximum time to live (TTL) values that you want objects to stay in the CloudFront cache.

The headers, cookies, and query strings that are included in the cache key are automatically included in requests that CloudFront sends to the origin. CloudFront sends a request when it can't find a valid object in its cache that matches the request's cache key. If you want to send values to the origin but not include them in the cache key, use OriginRequestPolicy.

Contents

Comment

A comment to describe the cache policy. The comment cannot be longer than 128 characters.

Type: String
Required: No

DefaultTTL

The default amount of time, in seconds, that you want objects to stay in the CloudFront cache before CloudFront sends another request to the origin to see if the object has been updated. CloudFront uses this value as the object's time to live (TTL) only when the origin does not send Cache-Control or Expires headers with the object. For more information, see Managing How Long Content Stays in an Edge Cache (Expiration) in the Amazon CloudFront Developer Guide.

The default value for this field is 86400 seconds (one day). If the value of MinTTL is more than 86400 seconds, then the default value for this field is the same as the value of MinTTL.

Type: Long
Required: No

MaxTTL

The maximum amount of time, in seconds, that objects stay in the CloudFront cache before CloudFront sends another request to the origin to see if the object has been updated. CloudFront uses this value only when the origin sends Cache-Control or Expires headers with the object. For more information, see Managing How Long Content Stays in an Edge Cache (Expiration) in the Amazon CloudFront Developer Guide.

The default value for this field is 31536000 seconds (one year). If the value of MinTTL or DefaultTTL is more than 31536000 seconds, then the default value for this field is the same as the value of DefaultTTL.

Type: Long
Required: No
MinTTL

The minimum amount of time, in seconds, that you want objects to stay in the CloudFront cache before CloudFront sends another request to the origin to see if the object has been updated. For more information, see Managing How Long Content Stays in an Edge Cache (Expiration) in the Amazon CloudFront Developer Guide.

Type: Long
Required: Yes

Name

A unique name to identify the cache policy.

Type: String
Required: Yes

ParametersInCacheKeyAndForwardedToOrigin

The HTTP headers, cookies, and URL query strings to include in the cache key. The values included in the cache key are automatically included in requests that CloudFront sends to the origin.

Type: ParametersInCacheKeyAndForwardedToOrigin (p. 489) 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 V2
- AWS SDK for Ruby V3
CachePolicyCookiesConfig

An object that determines whether any cookies in viewer requests (and if so, which cookies) are included in the cache key and automatically included in requests that CloudFront sends to the origin.

Contents

CookieBehavior

Determines whether any cookies in viewer requests are included in the cache key and automatically included in requests that CloudFront sends to the origin. Valid values are:

- **none** – Cookies in viewer requests are not included in the cache key and are not automatically included in requests that CloudFront sends to the origin. Even when this field is set to **none**, any cookies that are listed in an OriginRequestPolicy are included in origin requests.
- **whitelist** – The cookies in viewer requests that are listed in the CookieNames type are included in the cache key and automatically included in requests that CloudFront sends to the origin.
- **allExcept** – All cookies in viewer requests that are **not** listed in the CookieNames type are included in the cache key and automatically included in requests that CloudFront sends to the origin.
- **all** – All cookies in viewer requests are included in the cache key and are automatically included in requests that CloudFront sends to the origin.

Type: String

Valid Values: none | whitelist | allExcept | all

Required: Yes

Cookies

Contains a list of cookie names.

Type: CookieNames (p. 398) 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 V2
- AWS SDK for Ruby V3
CachePolicyHeadersConfig

An object that determines whether any HTTP headers (and if so, which headers) are included in the cache key and automatically included in requests that CloudFront sends to the origin.

Contents

HeaderBehavior

Determines whether any HTTP headers are included in the cache key and automatically included in requests that CloudFront sends to the origin. Valid values are:

- none – HTTP headers are not included in the cache key and are not automatically included in requests that CloudFront sends to the origin. Even when this field is set to none, any headers that are listed in an OriginRequestPolicy are included in origin requests.
- whitelist – The HTTP headers that are listed in the Headers type are included in the cache key and are automatically included in requests that CloudFront sends to the origin.

Type: String
Valid Values: none | whitelist
Required: Yes

Headers

Contains a list of HTTP header names.

Type: Headers (p. 450) 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 V2
- AWS SDK for Ruby V3
CachePolicyList

A list of cache policies.

Contents

Items

Contains the cache policies in the list.

Type: Array of CachePolicySummary (p. 387) objects

Required: No

MaxItems

The maximum number of cache policies requested.

Type: Integer

Required: Yes

NextMarker

If there are more items in the list than are in this response, this element is present. It contains the value that you should use in the Marker field of a subsequent request to continue listing cache policies where you left off.

Type: String

Required: No

Quantity

The total number of cache policies returned in the response.

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 V2
- AWS SDK for Ruby V3
CachePolicyQueryStringsConfig

An object that determines whether any URL query strings in viewer requests (and if so, which query strings) are included in the cache key and automatically included in requests that CloudFront sends to the origin.

Contents

QueryStringBehavior

Determines whether any URL query strings in viewer requests are included in the cache key and automatically included in requests that CloudFront sends to the origin. Valid values are:

- **none** – Query strings in viewer requests are not included in the cache key and are not automatically included in requests that CloudFront sends to the origin. Even when this field is set to **none**, any query strings that are listed in an OriginRequestPolicy are included in origin requests.
- **whitelist** – The query strings in viewer requests that are listed in the QueryStringNames type are included in the cache key and automatically included in requests that CloudFront sends to the origin.
- **allExcept** – All query strings in viewer requests that are **not** listed in the QueryStringNames type are included in the cache key and automatically included in requests that CloudFront sends to the origin.
- **all** – All query strings in viewer requests are included in the cache key and are automatically included in requests that CloudFront sends to the origin.

Type: String

Valid Values: none | whitelist | allExcept | all

Required: Yes

QueryString

Contains the specific query strings in viewer requests that either **are** or **are not** included in the cache key and automatically included in requests that CloudFront sends to the origin. The behavior depends on whether the QueryStringBehavior field in the CachePolicyQueryStringsConfig type is set to whitelist (the listed query strings are included) or allExcept (the listed query strings not included, but all other query strings are).

Type: QueryStringNames (p. 500) 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 V2
- AWS SDK for Ruby V3
CachePolicySummary

Contains a cache policy.

Contents

CachePolicy

The cache policy.

Type: CachePolicy (p. 380) object

Required: Yes

Type

The type of cache policy, either managed (created by AWS) or custom (created in this AWS account).

Type: String

Valid Values: managed | custom

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 V2
- AWS SDK for Ruby V3
CloudFrontOriginAccessIdentity

CloudFront origin access identity.

Contents

CloudFrontOriginAccessIdentityConfig

The current configuration information for the identity.

Type: CloudFrontOriginAccessIdentityConfig (p. 389) 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 V2
- AWS SDK for Ruby V3
CloudFrontOriginAccessIdentityConfig

Origin access identity configuration. Send a GET request to the /CloudFront API version/CloudFront/identity ID/config resource.

Contents

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 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

A comment to describe the origin access identity. The comment cannot be longer than 128 characters.

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 V2
- AWS SDK for Ruby V3
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. 392) 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
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 V2
- AWS SDK for Ruby V3
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 V2
- AWS SDK for Ruby V3
ConflictingAlias

An alias (also called a CNAME) and the CloudFront distribution and AWS account ID that it’s associated with. The distribution and account IDs are partially hidden, which allows you to identify the distributions and accounts that you own, but helps to protect the information of ones that you don’t own.

Contents

AccountId

The (partially hidden) ID of the AWS account that owns the distribution that’s associated with the alias.

Type: String

Required: No

Alias

An alias (also called a CNAME).

Type: String

Required: No

DistributionId

The (partially hidden) ID of the CloudFront distribution associated with the alias.

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 V2
- AWS SDK for Ruby V3
ConflictingAliasesList

A list of aliases (also called CNAMEs) and the CloudFront distributions and AWS accounts that they are associated with. In the list, the distribution and account IDs are partially hidden, which allows you to identify the distributions and accounts that you own, but helps to protect the information of ones that you don't own.

Contents

Items

Contains the conflicting aliases in the list.

Type: Array of ConflictingAlias (p. 393) objects

Required: No

MaxItems

The maximum number of conflicting aliases requested.

Type: Integer

Required: No

NextMarker

If there are more items in the list than are in this response, this element is present. It contains the value that you should use in the Marker field of a subsequent request to continue listing conflicting aliases where you left off.

Type: String

Required: No

Quantity

The number of conflicting aliases returned in the response.

Type: Integer

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 V2
- AWS SDK for Ruby V3
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 V2
- AWS SDK for Ruby V3
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. 397) 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 V2
• AWS SDK for Ruby V3
ContentTypeProfiles

Field-level encryption content type-profile.

Contents

Items

Items in a field-level encryption content type-profile mapping.

Type: Array of ContentTypeProfile (p. 395) 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 V2
- AWS SDK for Ruby V3
### CookieNames

Contains a list of cookie names.

#### Contents

**Items**

A list of cookie names.

Type: Array of strings

Required: No

**Quantity**

The number of cookie names in the `Items` list.

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 V2
- AWS SDK for Ruby V3
CookiePreference

This field is deprecated. We recommend that you use a cache policy or an origin request policy instead of this field.

If you want to include cookies in the cache key, use CookiesConfig in a cache policy. See CachePolicy.

If you want to send cookies to the origin but not include them in the cache key, use CookiesConfig in an origin request policy. See OriginRequestPolicy.

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 Caching Content Based on Cookies in the Amazon CloudFront Developer Guide.

Contents

Forward

This field is deprecated. We recommend that you use a cache policy or an origin request policy instead of this field.

If you want to include cookies in the cache key, use a cache policy. For more information, see Creating cache policies in the Amazon CloudFront Developer Guide.

If you want to send cookies to the origin but not include them in the cache key, use origin request policy. For more information, see Creating origin request policies in the Amazon CloudFront Developer Guide.

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

This field is deprecated. We recommend that you use a cache policy or an origin request policy instead of this field.

If you want to include cookies in the cache key, use a cache policy. For more information, see Creating cache policies in the Amazon CloudFront Developer Guide.

If you want to send cookies to the origin but not include them in the cache key, use origin request policy. For more information, see Creating origin request policies in the Amazon CloudFront Developer Guide.

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 CloudFront Limits in the AWS General Reference.

Type: CookieNames (p. 398) 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 V2
- AWS SDK for Ruby V3
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.

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.

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.

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.

**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 V2
- AWS SDK for Ruby V3
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 (p. 401) 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 V2
- AWS SDK for Ruby V3
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. 472) 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 V2
- AWS SDK for Ruby V3
CustomOriginConfig

A custom origin. A custom origin is any origin that is not an Amazon S3 bucket, with one exception. An Amazon S3 bucket that is configured with static website hosting is a custom origin.

Contents

HTTPPort
The HTTP port that CloudFront uses to connect to the origin. Specify the HTTP port that the origin listens on.
Type: Integer
Required: Yes

HTTPSPort
The HTTPS port that CloudFront uses to connect to the origin. Specify the HTTPS port that the origin listens on.
Type: Integer
Required: Yes

OriginKeepaliveTimeout
Specifies how long, in seconds, CloudFront persists its connection to the origin. The minimum timeout is 1 second, the maximum is 60 seconds, and the default (if you don’t specify otherwise) is 5 seconds.
For more information, see Origin Keep-alive Timeout in the Amazon CloudFront Developer Guide.
Type: Integer
Required: No

OriginProtocolPolicy
Specifies the protocol (HTTP or HTTPS) that CloudFront uses to connect to the origin. Valid values are:
- http-only – CloudFront always uses HTTP to connect to the origin.
- match-viewer – CloudFront connects to the origin using the same protocol that the viewer used to connect to CloudFront.
- https-only – CloudFront always uses HTTPS to connect to the origin.
Type: String
Valid Values: http-only | match-viewer | https-only
Required: Yes

OriginReadTimeout
Specifies how long, in seconds, CloudFront waits for a response from the origin. This is also known as the origin response timeout. The minimum timeout is 1 second, the maximum is 60 seconds, and the default (if you don’t specify otherwise) is 30 seconds.
For more information, see Origin Response Timeout in the Amazon CloudFront Developer Guide.
Type: Integer
Required: No

**OriginSslProtocols**

Specifies the minimum SSL/TLS protocol that CloudFront uses when connecting to your origin over HTTPS. Valid values include SSLv3, TLSv1, TLSv1.1, and TLSv1.2.

For more information, see Minimum Origin SSL Protocol in the Amazon CloudFront Developer Guide.

Type: OriginSslProtocols (p. 488) 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 V2
- AWS SDK for Ruby V3
DefaultCacheBehavior

A complex type that describes the default cache behavior if you don’t specify a CacheBehavior element or if request URLs 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 \texttt{GET} and \texttt{HEAD} requests.
- CloudFront forwards only \texttt{GET}, \texttt{HEAD}, and \texttt{OPTIONS} requests.
- CloudFront forwards \texttt{GET}, \texttt{HEAD}, \texttt{OPTIONS}, \texttt{PUT}, \texttt{PATCH}, \texttt{POST}, and \texttt{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: \texttt{AllowedMethods (p. 371) object}

Required: No

CachePolicyId

The unique identifier of the cache policy that is attached to the default cache behavior. For more information, see \textit{Creating cache policies} or \textit{Using the managed cache policies} in the \textit{Amazon CloudFront Developer Guide}.

A DefaultCacheBehavior must include either a CachePolicyId or ForwardedValues. We recommend that you use a CachePolicyId.

Type: String

Required: No

Compress

Whether you want CloudFront to automatically compress certain files for this cache behavior. If so, specify \texttt{true}; if not, specify \texttt{false}. For more information, see \textit{Serving Compressed Files} in the \textit{Amazon CloudFront Developer Guide}.

Type: Boolean

Required: No

DefaultTTL

This field is deprecated. We recommend that you use the DefaultTTL field in a cache policy instead of this field. For more information, see \textit{Creating cache policies} or \textit{Using the managed cache policies} in the \textit{Amazon CloudFront Developer Guide}.

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 \texttt{Cache-Control max-age}, \texttt{Cache-Control s-maxage}, and \texttt{Expires} to objects. For more information, see \textit{Managing How Long Content Stays in an Edge Cache (Expiration)} in the \textit{Amazon CloudFront Developer Guide}.
FieldLevelEncryptionId

The value of ID for the field-level encryption configuration that you want CloudFront to use for encrypting specific fields of data for the default cache behavior.

Type: String
Required: No

ForwardedValues

This field is deprecated. We recommend that you use a cache policy or an origin request policy instead of this field. For more information, see Working with policies in the Amazon CloudFront Developer Guide.

If you want to include values in the cache key, use a cache policy. For more information, see Creating cache policies or Using the managed cache policies in the Amazon CloudFront Developer Guide.

If you want to send values to the origin but not include them in the cache key, use an origin request policy. For more information, see Creating origin request policies or Using the managed origin request policies in the Amazon CloudFront Developer Guide.

A DefaultCacheBehavior must include either a CachePolicyId or ForwardedValues. We recommend that you use a CachePolicyId.

A complex type that specifies how CloudFront handles query strings, cookies, and HTTP headers.
Type: ForwardedValues (p. 439) object
Required: No

FunctionAssociations

A list of CloudFront functions that are associated with this cache behavior. CloudFront functions must be published to the LIVE stage to associate them with a cache behavior.
Type: FunctionAssociations (p. 443) object
Required: No

LambdaFunctionAssociations

A complex type that contains zero or more Lambda@Edge function associations for a cache behavior.
Type: LambdaFunctionAssociations (p. 465) object
Required: No

MaxTTL

This field is deprecated. We recommend that you use the MaxTTL field in a cache policy instead of this field. For more information, see Creating cache policies or Using the managed cache policies in the Amazon CloudFront Developer Guide.

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 Managing How Long Content Stays in an Edge Cache (Expiration) in the Amazon CloudFront Developer Guide.
MinTTL

This field is deprecated. We recommend that you use the MinTTL field in a cache policy instead of this field. For more information, see Creating cache policies or Using the managed cache policies in the Amazon CloudFront Developer Guide.

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 Managing How Long Content Stays in an 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: No

OriginRequestPolicyId

The unique identifier of the origin request policy that is attached to the default cache behavior. For more information, see Creating origin request policies or Using the managed origin request policies in the Amazon CloudFront Developer Guide.

Type: String
Required: No

RealtimeLogConfigArn

The Amazon Resource Name (ARN) of the real-time log configuration that is attached to this cache behavior. For more information, see Real-time logs in the Amazon CloudFront Developer Guide.

Type: String
Required: No

ResponseHeadersPolicyId

The identifier for a response headers policy.

Type: String
Required: No

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 they use the default cache behavior.

Type: String
**Required: Yes**

**TrustedKeyGroups**

A list of key groups that CloudFront can use to validate signed URLs or signed cookies.

When a cache behavior contains trusted key groups, CloudFront requires signed URLs or signed cookies for all requests that match the cache behavior. The URLs or cookies must be signed with a private key whose corresponding public key is in the key group. The signed URL or cookie contains information about which public key CloudFront should use to verify the signature. For more information, see Serving private content in the Amazon CloudFront Developer Guide.

Type: TrustedKeyGroups (p. 547) object

**Required: No**

**TrustedSigners**

Important

We recommend using TrustedKeyGroups instead of TrustedSigners.

A list of AWS account IDs whose public keys CloudFront can use to validate signed URLs or signed cookies.

When a cache behavior contains trusted signers, CloudFront requires signed URLs or signed cookies for all requests that match the cache behavior. The URLs or cookies must be signed with the private key of a CloudFront key pair in a trusted signer’s AWS account. The signed URL or cookie contains information about which public key CloudFront should use to verify the signature. For more information, see Serving private content in the Amazon CloudFront Developer Guide.

Type: TrustedSigners (p. 548) object

**Required: No**

**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 Requiring HTTPS Between Viewers and CloudFront 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 Managing 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 V2
- AWS SDK for Ruby V3
Distribution

A distribution tells CloudFront where you want content to be delivered from, and the details about how to track and manage content delivery.

Contents

ActiveTrustedKeyGroups

CloudFront automatically adds this field to the response if you've configured a cache behavior in this distribution to serve private content using key groups. This field contains a list of key groups and the public keys in each key group that CloudFront can use to verify the signatures of signed URLs or signed cookies.

Type: ActiveTrustedKeyGroups (p. 367) object

Required: No

ActiveTrustedSigners

Important
We recommend using TrustedKeyGroups instead of TrustedSigners.

CloudFront automatically adds this field to the response if you've configured a cache behavior in this distribution to serve private content using trusted signers. This field contains a list of AWS account IDs and the active CloudFront key pairs in each account that CloudFront can use to verify the signatures of signed URLs or signed cookies.

Type: ActiveTrustedSigners (p. 368) object

Required: No

AliasICPRecordals

AWS services in China customers must file for an Internet Content Provider (ICP) recordal if they want to serve content publicly on an alternate domain name, also known as a CNAME, that they've added to CloudFront. AliasICPRecordal provides the ICP recordal status for CNAMEs associated with distributions.

For more information about ICP recordals, see Signup, Accounts, and Credentials in Getting Started with AWS services in China.

Type: Array of AliasICPRecordal (p. 370) objects

Required: No

ARN

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

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. 414) 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 V2
- AWS SDK for Ruby V3
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. 369) object

Required: No

CacheBehaviors

A complex type that contains zero or more CacheBehavior elements.

Type: CacheBehaviors (p. 378) 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 that you already sent in a previous request to create a distribution, CloudFront returns a DistributionAlreadyExists error.

Type: String

Required: Yes

Comment

An optional comment to describe the distribution. The comment cannot be longer than 128 characters.

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. 403) 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. 407) 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.

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 AWS Integration 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 AWS Integration Developer Guide.

If you created a CNAME resource record set, either with Amazon Route 53 AWS Integration 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. 466) object

Required: No

OriginGroups

A complex type that contains information about origin groups for this distribution.

Type: OriginGroups (p. 477) object

Required: No

Origins

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

Type: Origins (p. 486) 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 (such as Price Class 100) 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. 528) object

Required: No

**ViewerCertificate**

A complex type that determines the distribution's SSL/TLS configuration for communicating with viewers.

Type: ViewerCertificate (p. 549) object

Required: No

**WebACLId**

A unique identifier that specifies the AWS WAF web ACL, if any, to associate with this distribution. To specify a web ACL created using the latest version of AWS WAF, use the ACL ARN, for example arn:aws:wafv2:us-east-1:123456789012:global/webacl/ExampleWebACL/473e64fd-f30b-4765-81a0-62ad96dd167a. To specify a web ACL created using AWS WAF Classic, use the ACL ID, for example 473e64fd-f30b-4765-81a0-62ad96dd167a.

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 V2
- AWS SDK for Ruby V3
DistributionConfigWithTags

A distribution Configuration and a list of tags to be associated with the distribution.

Contents

DistributionConfig

A distribution configuration.

Type: DistributionConfig (p. 414) object

Required: Yes

Tags

A complex type that contains zero or more Tag elements.

Type: Tags (p. 545) 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 V2
- AWS SDK for Ruby V3
DistributionIdList

A list of distribution IDs.

Contents

IsTruncated

A flag that indicates whether more distribution IDs remain to be listed. If your results were truncated, you can make a subsequent request using the Marker request field to retrieve more distribution IDs in the list.

Type: Boolean
Required: Yes

Items

Contains the distribution IDs in the list.

Type: Array of strings
Required: No

Marker

The value provided in the Marker request field.

Type: String
Required: Yes

MaxItems

The maximum number of distribution IDs requested.

Type: Integer
Required: Yes

NextMarker

Contains the value that you should use in the Marker field of a subsequent request to continue listing distribution IDs where you left off.

Type: String
Required: No

Quantity

The total number of distribution IDs returned in the response.

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 V2
• AWS SDK for Ruby V3
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. 423) 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:
• AWS SDK for C++
• AWS SDK for Go
• AWS SDK for Java V2
• AWS SDK for Ruby V3
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. 369) object

Required: Yes

AliasICPRecordals

AWS services in China customers must file for an Internet Content Provider (ICP) recordal if they want to serve content publicly on an alternate domain name, also known as a CNAME, that they've added to CloudFront. AliasICPRecordal provides the ICP recordal status for CNAMEs associated with distributions.

For more information about ICP recordals, see Signup, Accounts, and Credentials in Getting Started with AWS services in China.

Type: Array of AliasICPRecordal (p. 370) objects

Required: No

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. 378) 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. 403) 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. 407) 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

OriginGroups

A complex type that contains information about origin groups for this distribution.
Type: **OriginGroups (p. 477) object**

Required: No

**Origins**

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

Type: **Origins (p. 486) object**

Required: Yes

**PriceClass**

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

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. 528) 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 determines the distribution's SSL/TLS configuration for communicating with viewers.

Type: **ViewerCertificate (p. 549) 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 V2
• AWS SDK for Ruby V3
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. 428) 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 V2
- AWS SDK for Ruby V3
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. 438) 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 V2
- AWS SDK for Ruby V3
EndPoint

Contains information about the Amazon Kinesis data stream where you are sending real-time log data in a real-time log configuration.

Contents

KinesisStreamConfig

Contains information about the Amazon Kinesis data stream where you are sending real-time log data.

Type: KinesisStreamConfig (p. 462) object

Required: No

StreamType

The type of data stream where you are sending real-time log data. The only valid value is Kinesis.

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 V2
- AWS SDK for Ruby V3
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. 431) 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 V2
- AWS SDK for Ruby V3
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. The comment cannot be longer than 128 characters.
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. 396) 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. 497) 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 V2
- AWS SDK for Ruby V3
FieldLevelEncryptionList

List of field-level encryption configurations.

Contents

Items

An array of field-level encryption items.

Type: Array of FieldLevelEncryptionSummary (p. 437) 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 V2
- AWS SDK for Ruby V3
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. 434) 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 V2
- AWS SDK for Ruby V3
FieldLevelEncryptionProfileConfig

A complex data type of profiles for the field-level encryption.

Contents

**CallerReference**

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

Type: String  
Required: Yes

**Comment**

An optional comment for the field-level encryption profile. The comment cannot be longer than 128 characters.

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. 427) 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 V2
- AWS SDK for Ruby V3
FieldLevelEncryptionProfileList

List of field-level encryption profiles.

Contents

Items

The field-level encryption profile items.

Type: Array of FieldLevelEncryptionProfileSummary (p. 436) 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 V2
- AWS SDK for Ruby V3
FieldLevelEncryptionProfileSummary

The field-level encryption profile summary.

Contents

Comment

An optional comment for the field-level encryption profile summary. The comment cannot be longer than 128 characters.

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. 427) 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 V2
- AWS SDK for Ruby V3
FieldLevelEncryptionSummary

A summary of a field-level encryption item.

Contents

Comment

An optional comment about the field-level encryption item. The comment cannot be longer than 128 characters.

Type: String

Required: No

ContentTypeProfileConfig

A summary of a content type-profile mapping.

Type: ContentTypeProfileConfig (p. 396) 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. 497) 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 V2
- AWS SDK for Ruby V3
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 V2
- AWS SDK for Ruby V3
ForwardedValues

This field is deprecated. We recommend that you use a cache policy or an origin request policy instead of this field.

If you want to include values in the cache key, use a cache policy. For more information, see Creating cache policies in the Amazon CloudFront Developer Guide.

If you want to send values to the origin but not include them in the cache key, use an origin request policy. For more information, see Creating origin request policies in the Amazon CloudFront Developer Guide.

A complex type that specifies how CloudFront handles query strings, cookies, and HTTP headers.

Contents

Cookies

This field is deprecated. We recommend that you use a cache policy or an origin request policy instead of this field.

If you want to include cookies in the cache key, use a cache policy. For more information, see Creating cache policies in the Amazon CloudFront Developer Guide.

If you want to send cookies to the origin but not include them in the cache key, use an origin request policy. For more information, see Creating origin request policies in the Amazon CloudFront Developer Guide.

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. 399) object

Required: Yes

Headers

This field is deprecated. We recommend that you use a cache policy or an origin request policy instead of this field.

If you want to include headers in the cache key, use a cache policy. For more information, see Creating cache policies in the Amazon CloudFront Developer Guide.

If you want to send headers to the origin but not include them in the cache key, use an origin request policy. For more information, see Creating origin request policies in the Amazon CloudFront Developer Guide.

A complex type that specifies the Headers, if any, that you want CloudFront to forward to the origin for this cache behavior (whitelisted headers). For the headers that you specify, CloudFront also caches separate versions of a specified object that is based on the header values in viewer requests.

For more information, see Caching Content Based on Request Headers in the Amazon CloudFront Developer Guide.

Type: Headers (p. 450) object

Required: No
QueryString

This field is deprecated. We recommend that you use a cache policy or an origin request policy instead of this field.

If you want to include query strings in the cache key, use a cache policy. For more information, see Creating cache policies in the Amazon CloudFront Developer Guide.

If you want to send query strings to the origin but not include them in the cache key, use an origin request policy. For more information, see Creating origin request policies in the Amazon CloudFront Developer Guide.

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

This field is deprecated. We recommend that you use a cache policy or an origin request policy instead of this field.

If you want to include query strings in the cache key, use a cache policy. For more information, see Creating cache policies in the Amazon CloudFront Developer Guide.

If you want to send query strings to the origin but not include them in the cache key, use an origin request policy. For more information, see Creating origin request policies in the Amazon CloudFront Developer Guide.

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. 499) 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++
See Also

- AWS SDK for Go
- AWS SDK for Java V2
- AWS SDK for Ruby V3
FunctionAssociation

A CloudFront function that is associated with a cache behavior in a CloudFront distribution.

Contents

**EventType**

The event type of the function, either viewer-request or viewer-response. You cannot use origin-facing event types (origin-request and origin-response) with a CloudFront function.

Type: String

Valid Values: viewer-request | viewer-response | origin-request | origin-response

Required: Yes

**FunctionARN**

The Amazon Resource Name (ARN) of the function.

Type: String

Length Constraints: Maximum length of 108.

Pattern: `arn:aws:cloudfront::[0-9]{12}:function\/[a-zA-Z0-9-]{1,64}`

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 V2
- AWS SDK for Ruby V3
FunctionAssociations

A list of CloudFront functions that are associated with a cache behavior in a CloudFront distribution. CloudFront functions must be published to the **LIVE** stage to associate them with a cache behavior.

Contents

**Items**

The CloudFront functions that are associated with a cache behavior in a CloudFront distribution. CloudFront functions must be published to the **LIVE** stage to associate them with a cache behavior.

Type: Array of FunctionAssociation (p. 442) objects

Required: No

**Quantity**

The number of CloudFront functions in the list.

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 V2
- AWS SDK for Ruby V3
FunctionConfig

Contains configuration information about a CloudFront function.

Contents

Comment

A comment to describe the function.

Type: String

Required: Yes

Runtime

The function's runtime environment. The only valid value is cloudfront-js-1.0.

Type: String

Valid Values: cloudfront-js-1.0

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 V2
- AWS SDK for Ruby V3
FunctionList

A list of CloudFront functions.

Contents

Items

Contains the functions in the list.

Type: Array of FunctionSummary (p. 447) objects

Required: No

MaxItems

The maximum number of functions requested.

Type: Integer

Required: Yes

NextMarker

If there are more items in the list than are in this response, this element is present. It contains the value that you should use in the Marker field of a subsequent request to continue listing functions where you left off.

Type: String

Required: No

Quantity

The number of functions returned in the response.

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 V2
- AWS SDK for Ruby V3
FunctionMetadata

Contains metadata about a CloudFront function.

Contents

CreatedTime

The date and time when the function was created.

Type: Timestamp

Required: No

FunctionARN

The Amazon Resource Name (ARN) of the function. The ARN uniquely identifies the function.

Type: String

Required: Yes

LastModifiedTime

The date and time when the function was most recently updated.

Type: Timestamp

Required: Yes

Stage

The stage that the function is in, either DEVELOPMENT or LIVE.

When a function is in the DEVELOPMENT stage, you can test the function with TestFunction, and update it with UpdateFunction.

When a function is in the LIVE stage, you can attach the function to a distribution's cache behavior, using the function's ARN.

Type: String

Valid Values: DEVELOPMENT | LIVE

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 V2
- AWS SDK for Ruby V3
FunctionSummary

Contains configuration information and metadata about a CloudFront function.

Contents

FunctionConfig

Contains configuration information about a CloudFront function.

Type: FunctionConfig (p. 444) object

Required: Yes

FunctionMetadata

Contains metadata about a CloudFront function.

Type: FunctionMetadata (p. 446) object

Required: Yes

Name

The name of the CloudFront function.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 64.

Pattern: ^[a-zA-Z0-9-_]{1,64}$

Required: Yes

Status

The status of the CloudFront function.

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 V2
- AWS SDK for Ruby V3
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 V2
• AWS SDK for Ruby V3
Headers

Contains a list of HTTP header names.

Contents

Items

A list of HTTP header names.

Type: Array of strings

Required: No

Quantity

The number of header names in the Items list.

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 V2
- AWS SDK for Ruby V3
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. 452) 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 V2
- AWS SDK for Ruby V3
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 InvalidationBatchAlreadyExists 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. 491) 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 V2
- AWS SDK for Ruby V3
InvalidationList

The **InvalidationList** complex type describes the list of invalidation objects. For more information about invalidation, see [Invalidating Objects (Web Distributions Only)](https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/invalidating-objects.html) 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` 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:
See Also

- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2
- AWS SDK for Ruby V3
InvalidationSummary

A summary of an invalidation request.

Contents

CreateTime

The time that an invalidation request was created.

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 V2
- AWS SDK for Ruby V3
KeyGroup

A key group.

A key group contains a list of public keys that you can use with CloudFront signed URLs and signed cookies.

Contents

Id

The identifier for the key group.

Type: String

Required: Yes

KeyGroupConfig

The key group configuration.

Type: KeyGroupConfig (p. 457) object

Required: Yes

LastModifiedTime

The date and time when the key group was last modified.

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 V2
- AWS SDK for Ruby V3
KeyGroupConfig

A key group configuration.

A key group contains a list of public keys that you can use with CloudFront signed URLs and signed cookies.

Contents

Comment

A comment to describe the key group. The comment cannot be longer than 128 characters.

Type: String

Required: No

Items

A list of the identifiers of the public keys in the key group.

Type: Array of strings

Required: Yes

Name

A name to identify the key group.

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 V2
- AWS SDK for Ruby V3
KeyGroupList

A list of key groups.

Contents

Items

A list of key groups.

Type: Array of KeyGroupSummary (p. 459) objects

Required: No

MaxItems

The maximum number of key groups requested.

Type: Integer

Required: Yes

NextMarker

If there are more items in the list than are in this response, this element is present. It contains the value that you should use in the Marker field of a subsequent request to continue listing key groups.

Type: String

Required: No

Quantity

The number of key groups returned in the response.

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 V2
- AWS SDK for Ruby V3
KeyGroupSummary

Contains information about a key group.

Contents

KeyGroup

A key group.

Type: KeyGroup (p. 456) 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 V2
- AWS SDK for Ruby V3
KeyPairIds

A list of CloudFront key pair identifiers.

Contents

Items

A list of CloudFront key pair identifiers.

Type: Array of strings

Required: No

Quantity

The number of key pair identifiers in the list.

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 V2
- AWS SDK for Ruby V3
KGKeyPairIds

A list of identifiers for the public keys that CloudFront can use to verify the signatures of signed URLs and signed cookies.

Contents

KeyGroupId

The identifier of the key group that contains the public keys.

Type: String
Required: No

KeyPairIds

A list of CloudFront key pair identifiers.

Type: KeyPairIds (p. 460) 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 V2
- AWS SDK for Ruby V3
KinesisStreamConfig

Contains information about the Amazon Kinesis data stream where you are sending real-time log data.

Contents

RoleARN

The Amazon Resource Name (ARN) of an AWS Identity and Access Management (IAM) role that
CloudFront can use to send real-time log data to your Kinesis data stream.

For more information the IAM role, see Real-time log configuration IAM role in the Amazon
CloudFront Developer Guide.

Type: String
Required: Yes

StreamARN

The Amazon Resource Name (ARN) of the Kinesis data stream where you are sending real-time log
data.

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 V2
- AWS SDK for Ruby V3
LambdaFunctionAssociation

A complex type that contains a Lambda@Edge function association.

Contents

EventType

Specifies the event type that triggers a Lambda@Edge 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 sends 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.
- 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

IncludeBody

A flag that allows a Lambda@Edge function to have read access to the body content. For more information, see Accessing the Request Body by Choosing the Include Body Option in the Amazon CloudFront Developer Guide.

Type: Boolean

Required: No

LambdaFunctionARN

The ARN of the Lambda@Edge function. You must specify the ARN of a function version; you can't specify an 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 V2
- AWS SDK for Ruby V3
LambdaFunctionAssociations

A complex type that specifies a list of Lambda@Edge functions associations for a cache behavior.

If you want to invoke one or more Lambda@Edge 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 only one function.

If you don’t want to invoke any Lambda@Edge 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. 463) objects

Required: No

Quantity

The number of Lambda@Edge 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 V2
- AWS SDK for Ruby V3
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 V2
- AWS SDK for Ruby V3
MonitoringSubscription

A monitoring subscription. This structure contains information about whether additional CloudWatch metrics are enabled for a given CloudFront distribution.

Contents

RealtimeMetricsSubscriptionConfig

A subscription configuration for additional CloudWatch metrics.

Type: RealtimeMetricsSubscriptionConfig (p. 504) 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 V2
- AWS SDK for Ruby V3
Origin

An origin.

An origin is the location where content is stored, and from which CloudFront gets content to serve to viewers. To specify an origin:

- Use `S3OriginConfig` to specify an Amazon S3 bucket that is not configured with static website hosting.
- Use `CustomOriginConfig` to specify all other kinds of origins, including:
  - An Amazon S3 bucket that is configured with static website hosting
  - An Elastic Load Balancing load balancer
  - An AWS Elemental MediaPackage endpoint
  - An AWS Elemental MediaStore container
  - Any other HTTP server, running on an Amazon EC2 instance or any other kind of host

For the current maximum number of origins that you can specify per distribution, see General Quotas on Web Distributions in the Amazon CloudFront Developer Guide (quotas were formerly referred to as limits).

Contents

ConnectionAttempts

The number of times that CloudFront attempts to connect to the origin. The minimum number is 1, the maximum is 3, and the default (if you don't specify otherwise) is 3.

For a custom origin (including an Amazon S3 bucket that's configured with static website hosting), this value also specifies the number of times that CloudFront attempts to get a response from the origin, in the case of an Origin Response Timeout.

For more information, see Origin Connection Attempts in the Amazon CloudFront Developer Guide.

Type: Integer

Required: No

ConnectionTimeout

The number of seconds that CloudFront waits when trying to establish a connection to the origin. The minimum timeout is 1 second, the maximum is 10 seconds, and the default (if you don't specify otherwise) is 10 seconds.

For more information, see Origin Connection Timeout in the Amazon CloudFront Developer Guide.

Type: Integer

Required: No

CustomHeaders

A list of HTTP header names and values that CloudFront adds to the requests that it sends to the origin.

For more information, see Adding Custom Headers to Origin Requests in the Amazon CloudFront Developer Guide.

Type: CustomHeaders (p. 404) object
CustomOriginConfig

Use this type to specify an origin that is not an Amazon S3 bucket, with one exception. If the Amazon S3 bucket is configured with static website hosting, use this type. If the Amazon S3 bucket is not configured with static website hosting, use the S3OriginConfig type instead.

Type: CustomOriginConfig (p. 405) object

Required: No

DomainName

The domain name for the origin.

For more information, see Origin Domain Name in the Amazon CloudFront Developer Guide.

Type: String

Required: Yes

Id

A unique identifier for the origin. This value must be unique within the distribution.

Use this value to specify the TargetOriginId in a CacheBehavior or DefaultCacheBehavior.

Type: String

Required: Yes

OriginPath

An optional path that CloudFront appends to the origin domain name when CloudFront requests content from the origin.

For more information, see Origin Path in the Amazon CloudFront Developer Guide.

Type: String

Required: No

OriginShield

CloudFront Origin Shield. Using Origin Shield can help reduce the load on your origin.

For more information, see Using Origin Shield in the Amazon CloudFront Developer Guide.

Type: OriginShield (p. 487) object

Required: No

S3OriginConfig

Use this type to specify an origin that is an Amazon S3 bucket that is not configured with static website hosting. To specify any other type of origin, including an Amazon S3 bucket that is configured with static website hosting, use the CustomOriginConfig type instead.

Type: S3OriginConfig (p. 530) 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 V2
• AWS SDK for Ruby V3
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 send to your origin. For more information, see Adding Custom Headers to Origin Requests 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 V2
- AWS SDK for Ruby V3
OriginGroup

An origin group includes two origins (a primary origin and a second origin to failover to) and a failover criteria that you specify. You create an origin group to support origin failover in CloudFront. When you create or update a distribution, you can specify the origin group instead of a single origin, and CloudFront will failover from the primary origin to the second origin under the failover conditions that you've chosen.

Contents

FailoverCriteria

A complex type that contains information about the failover criteria for an origin group.

Type: OriginGroupFailoverCriteria (p. 474) object

Required: Yes

Id

The origin group's ID.

Type: String

Required: Yes

Members

A complex type that contains information about the origins in an origin group.

Type: OriginGroupMembers (p. 476) 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 V2
- AWS SDK for Ruby V3
OriginGroupFailoverCriteria

A complex data type that includes information about the failover criteria for an origin group, including the status codes for which CloudFront will failover from the primary origin to the second origin.

Contents

StatusCodes

The status codes that, when returned from the primary origin, will trigger CloudFront to failover to the second origin.

Type: StatusCodes (p. 532) 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 V2
- AWS SDK for Ruby V3
OriginGroupMember

An origin in an origin group.

Contents

OriginId

The ID for an origin in an origin group.

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 V2
- AWS SDK for Ruby V3
OriginGroupMembers

A complex data type for the origins included in an origin group.

Contents

Items

Items (origins) in an origin group.
Type: Array of OriginGroupMember (p. 475) objects
Array Members: Fixed number of 2 items.
Required: Yes

Quantity

The number of origins in an origin group.
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 V2
- AWS SDK for Ruby V3
OriginGroups

A complex data type for the origin groups specified for a distribution.

Contents

Items

The items (origin groups) in a distribution.

Type: Array of OriginGroup (p. 473) objects

Required: No

Quantity

The number of origin groups.

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 V2
- AWS SDK for Ruby V3
OriginRequestPolicy

An origin request policy.

When it's attached to a cache behavior, the origin request policy determines the values that CloudFront includes in requests that it sends to the origin. Each request that CloudFront sends to the origin includes the following:

- The request body and the URL path (without the domain name) from the viewer request.
- The headers that CloudFront automatically includes in every origin request, including Host, User-Agent, and X-Amz-Cf-Id.
- All HTTP headers, cookies, and URL query strings that are specified in the cache policy or the origin request policy. These can include items from the viewer request and, in the case of headers, additional ones that are added by CloudFront.

CloudFront sends a request when it can't find an object in its cache that matches the request. If you want to send values to the origin and also include them in the cache key, use CachePolicy.

Contents

Id

The unique identifier for the origin request policy.

Type: String

Required: Yes

LastModifiedTime

The date and time when the origin request policy was last modified.

Type: Timestamp

Required: Yes

OriginRequestPolicyConfig

The origin request policy configuration.

Type: OriginRequestPolicyConfig (p. 479) 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 V2
- AWS SDK for Ruby V3
OriginRequestPolicyConfig

An origin request policy configuration.

This configuration determines the values that CloudFront includes in requests that it sends to the origin. Each request that CloudFront sends to the origin includes the following:

- The request body and the URL path (without the domain name) from the viewer request.
- The headers that CloudFront automatically includes in every origin request, including Host, User-Agent, and X-Amz-Cf-Id.
- All HTTP headers, cookies, and URL query strings that are specified in the cache policy or the origin request policy. These can include items from the viewer request and, in the case of headers, additional ones that are added by CloudFront.

CloudFront sends a request when it can't find an object in its cache that matches the request. If you want to send values to the origin and also include them in the cache key, use CachePolicy.

Contents

Comment

A comment to describe the origin request policy. The comment cannot be longer than 128 characters.

Type: String

Required: No

CookiesConfig

The cookies from viewer requests to include in origin requests.

Type: OriginRequestPolicyCookiesConfig (p. 481) object

Required: Yes

HeadersConfig

The HTTP headers to include in origin requests. These can include headers from viewer requests and additional headers added by CloudFront.

Type: OriginRequestPolicyHeadersConfig (p. 482) object

Required: Yes

Name

A unique name to identify the origin request policy.

Type: String

Required: Yes

QueryStringsConfig

The URL query strings from viewer requests to include in origin requests.

Type: OriginRequestPolicyQueryStringsConfig (p. 484) 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 V2
- AWS SDK for Ruby V3
OriginRequestPolicyCookiesConfig

An object that determines whether any cookies in viewer requests (and if so, which cookies) are included in requests that CloudFront sends to the origin.

Contents

CookieBehavior

Determines whether cookies in viewer requests are included in requests that CloudFront sends to the origin. Valid values are:

- **none** – Cookies in viewer requests are not included in requests that CloudFront sends to the origin. Even when this field is set to `none`, any cookies that are listed in a `CachePolicy` are included in origin requests.
- **whitelist** – The cookies in viewer requests that are listed in the `CookieNames` type are included in requests that CloudFront sends to the origin.
- **all** – All cookies in viewer requests are included in requests that CloudFront sends to the origin.

Type: String

Valid Values: none | whitelist | all

Required: Yes

Cookies

Contains a list of cookie names.

Type: [CookieNames](p. 398) 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 V2
- AWS SDK for Ruby V3
OriginRequestPolicyHeadersConfig

An object that determines whether any HTTP headers (and if so, which headers) are included in requests that CloudFront sends to the origin.

Contents

HeaderBehavior

Determines whether any HTTP headers are included in requests that CloudFront sends to the origin. Valid values are:

- none – HTTP headers are not included in requests that CloudFront sends to the origin. Even when this field is set to none, any headers that are listed in a CachePolicy are included in origin requests.
- whitelist – The HTTP headers that are listed in the Headers type are included in requests that CloudFront sends to the origin.
- allViewer – All HTTP headers in viewer requests are included in requests that CloudFront sends to the origin.
- allViewerAndWhitelistCloudFront – All HTTP headers in viewer requests and the additional CloudFront headers that are listed in the Headers type are included in requests that CloudFront sends to the origin. The additional headers are added by CloudFront.

Type: String

Valid Values: none | whitelist | allViewer | allViewerAndWhitelistCloudFront

Required: Yes

Headers

Contains a list of HTTP header names.

Type: Headers (p. 450) 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 V2
- AWS SDK for Ruby V3
OriginRequestPolicyList

A list of origin request policies.

Contents

Items

Contains the origin request policies in the list.

Type: Array of OriginRequestPolicySummary (p. 485) objects

Required: No

MaxItems

The maximum number of origin request policies requested.

Type: Integer

Required: Yes

NextMarker

If there are more items in the list than are in this response, this element is present. It contains the value that you should use in the Marker field of a subsequent request to continue listing origin request policies where you left off.

Type: String

Required: No

Quantity

The total number of origin request policies returned in the response.

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 V2
- AWS SDK for Ruby V3
OriginRequestPolicyQueryStringsConfig

An object that determines whether any URL query strings in viewer requests (and if so, which query strings) are included in requests that CloudFront sends to the origin.

**Contents**

**QueryStringBehavior**

Determines whether any URL query strings in viewer requests are included in requests that CloudFront sends to the origin. Valid values are:

- **none** – Query strings in viewer requests are not included in requests that CloudFront sends to the origin. Even when this field is set to none, any query strings that are listed in a CachePolicy are included in origin requests.
- **whitelist** – The query strings in viewer requests that are listed in the QueryStringNames type are included in requests that CloudFront sends to the origin.
- **all** – All query strings in viewer requests are included in requests that CloudFront sends to the origin.

Type: String

Valid Values: none | whitelist | all

Required: Yes

**QueryStrings**

Contains a list of the query strings in viewer requests that are included in requests that CloudFront sends to the origin.

Type: [QueryStringNames](#) 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 V2
- AWS SDK for Ruby V3
OriginRequestPolicySummary

Contains an origin request policy.

Contents

OriginRequestPolicy

The origin request policy.

Type: OriginRequestPolicy (p. 478) object

Required: Yes

Type

The type of origin request policy, either managed (created by AWS) or custom (created in this AWS account).

Type: String

Valid Values: managed | custom

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 V2
- AWS SDK for Ruby V3
Origins

Contains information about the origins for this distribution.

Contents

Items

A list of origins.

Type: Array of Origin (p. 469) objects

Array Members: Minimum number of 1 item.

Required: Yes

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 V2
- AWS SDK for Ruby V3
OriginShield

CloudFront Origin Shield.

Using Origin Shield can help reduce the load on your origin. For more information, see Using Origin Shield in the Amazon CloudFront Developer Guide.

Contents

Enabled

A flag that specifies whether Origin Shield is enabled.

When it's enabled, CloudFront routes all requests through Origin Shield, which can help protect your origin. When it's disabled, CloudFront might send requests directly to your origin from multiple edge locations or regional edge caches.

Type: Boolean

Required: Yes

OriginShieldRegion

The AWS Region for Origin Shield.

Specify the AWS Region that has the lowest latency to your origin. To specify a region, use the region code, not the region name. For example, specify the US East (Ohio) region as us-east-2.

When you enable CloudFront Origin Shield, you must specify the AWS Region for Origin Shield. For the list of AWS Regions that you can specify, and for help choosing the best Region for your origin, see Choosing the AWS Region for Origin Shield in the Amazon CloudFront Developer Guide.

Type: String


Pattern: [a-z]{2}-[a-z]+-\d

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 V2
- AWS SDK for Ruby V3
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 V2
- AWS SDK for Ruby V3
ParametersInCacheKeyAndForwardedToOrigin

This object determines the values that CloudFront includes in the cache key. These values can include HTTP headers, cookies, and URL query strings. CloudFront uses the cache key to find an object in its cache that it can return to the viewer.

The headers, cookies, and query strings that are included in the cache key are automatically included in requests that CloudFront sends to the origin. CloudFront sends a request when it can’t find an object in its cache that matches the request’s cache key. If you want to send values to the origin but not include them in the cache key, use OriginRequestPolicy.

Contents

CookiesConfig

An object that determines whether any cookies in viewer requests (and if so, which cookies) are included in the cache key and automatically included in requests that CloudFront sends to the origin.

Type: CachePolicyCookiesConfig (p. 383) object

Required: Yes

EnableAcceptEncodingBrotli

A flag that can affect whether the Accept-Encoding HTTP header is included in the cache key and included in requests that CloudFront sends to the origin.

This field is related to the EnableAcceptEncodingGzip field. If one or both of these fields is true and the viewer request includes the Accept-Encoding header, then CloudFront does the following:
- Normalizes the value of the viewer’s Accept-Encoding header
- Includes the normalized header in the cache key
- Includes the normalized header in the request to the origin, if a request is necessary

For more information, see Compression support in the Amazon CloudFront Developer Guide.

If you set this value to true, and this cache behavior also has an origin request policy attached, do not include the Accept-Encoding header in the origin request policy. CloudFront always includes the Accept-Encoding header in origin requests when the value of this field is true, so including this header in an origin request policy has no effect.

If both of these fields are false, then CloudFront treats the Accept-Encoding header the same as any other HTTP header in the viewer request. By default, it’s not included in the cache key and it’s not included in origin requests. In this case, you can manually add Accept-Encoding to the headers whitelist like any other HTTP header.

Type: Boolean

Required: No

EnableAcceptEncodingGzip

A flag that can affect whether the Accept-Encoding HTTP header is included in the cache key and included in requests that CloudFront sends to the origin.

This field is related to the EnableAcceptEncodingBrotli field. If one or both of these fields is true and the viewer request includes the Accept-Encoding header, then CloudFront does the following:
- Normalizes the value of the viewer’s Accept-Encoding header
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 V2
- AWS SDK for Ruby V3
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

Quantity

The number of invalidation paths specified for the 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 V2
- AWS SDK for Ruby V3
PublicKey

A public key that you can use with signed URLs and signed cookies, or with field-level encryption.

Contents

**CreatedAtTime**

The date and time when the public key was uploaded.

Type: Timestamp

Required: Yes

**Id**

The identifier of the public key.

Type: String

Required: Yes

**PublicKeyConfig**

Configuration information about a public key that you can use with signed URLs and signed cookies, or with field-level encryption.

Type: PublicKeyConfig (p. 493) 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 V2
- AWS SDK for Ruby V3
PublickeyConfig

Configuration information about a public key that you can use with signed URLs and signed cookies, or with field-level encryption.

Contents

CallerReference

A string included in the request to help make sure that the request can't be replayed.

Type: String

Required: Yes

Comment

A comment to describe the public key. The comment cannot be longer than 128 characters.

Type: String

Required: No

EncodedKey

The public key that you can use with signed URLs and signed cookies, or with field-level encryption.

Type: String

Required: Yes

Name

A name to help identify the public key.

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 V2
- AWS SDK for Ruby V3
PublicKeyList

A list of public keys that you can use with signed URLs and signed cookies, or with field-level encryption.

Contents

Items

A list of public keys.

Type: Array of PublicKeySummary (p. 495) objects

Required: No

MaxItems

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

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 in the list.

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 V2
- AWS SDK for Ruby V3
PublicKeySummary

Contains information about a public key.

Contents

Comment

A comment to describe the public key. The comment cannot be longer than 128 characters.

Type: String
Required: No

CreatedTime

The date and time when the public key was uploaded.

Type: Timestamp
Required: Yes

EncodedKey

The public key.

Type: String
Required: Yes

Id

The identifier of the public key.

Type: String
Required: Yes

Name

A name to help identify the public key.

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 V2
- AWS SDK for Ruby V3
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 V2
- AWS SDK for Ruby V3
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. 498) 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 V2
- AWS SDK for Ruby V3
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. 496) 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 V2
- AWS SDK for Ruby V3
QueryStringCacheKeys

This field is deprecated. We recommend that you use a cache policy or an origin request policy instead of this field.

If you want to include query strings in the cache key, use QueryStringsConfig in a cache policy. See CachePolicy.

If you want to send query strings to the origin but not include them in the cache key, use QueryStringsConfig in an origin request policy. See OriginRequestPolicy.

A complex type that contains information about the query string parameters that you want CloudFront to use for caching for a cache behavior.

Contents

Items

A list that contains the query string parameters that you want CloudFront to use as a basis for caching for a 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 a 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 V2
- AWS SDK for Ruby V3
QueryStringNames

Contains a list of query string names.

Contents

Items

A list of query string names.
Type: Array of strings
Required: No

Quantity

The number of query string names in the Items list.
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 V2
- AWS SDK for Ruby V3
RealtimeLogConfig

A real-time log configuration.

Contents

ARN

The Amazon Resource Name (ARN) of this real-time log configuration.

Type: String

Required: Yes

EndPoint

Contains information about the Amazon Kinesis data stream where you are sending real-time log data for this real-time log configuration.

Type: Array of EndPoint (p. 429) objects

Required: Yes

Fields

A list of fields that are included in each real-time log record. In an API response, the fields are provided in the same order in which they are sent to the Amazon Kinesis data stream.

For more information about fields, see Real-time log configuration fields in the Amazon CloudFront Developer Guide.

Type: Array of strings

Required: Yes

Name

The unique name of this real-time log configuration.

Type: String

Required: Yes

SamplingRate

The sampling rate for this real-time log configuration. The sampling rate determines the percentage of viewer requests that are represented in the real-time log data. The sampling rate is an integer between 1 and 100, inclusive.

Type: Long

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 V2

API Version 2020-05-31

501
• AWS SDK for Ruby V3
RealtimeLogConfigs

A list of real-time log configurations.

Contents

IsTruncated

A flag that indicates whether there are more real-time log configurations than are contained in this list.

Type: Boolean

Required: Yes

Items

Contains the list of real-time log configurations.

Type: Array of RealtimeLogConfig (p. 501) objects

Required: No

Marker

This parameter indicates where this list of real-time log configurations begins. This list includes real-time log configurations that occur after the marker.

Type: String

Required: Yes

MaxItems

The maximum number of real-time log configurations requested.

Type: Integer

Required: Yes

NextMarker

If there are more items in the list than are in this response, this element is present. It contains the value that you should use in the Marker field of a subsequent request to continue listing real-time log configurations where you left off.

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 V2
- AWS SDK for Ruby V3
RealtimeMetricsSubscriptionConfig

A subscription configuration for additional CloudWatch metrics.

Contents

RealtimeMetricsSubscriptionStatus

A flag that indicates whether additional CloudWatch metrics are enabled for a given CloudFront distribution.

Type: String

Valid Values: Enabled | Disabled

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 V2
- AWS SDK for Ruby V3
ResponseHeadersPolicy

A response headers policy.

A response headers policy contains information about a set of HTTP response headers and their values.

After you create a response headers policy, you can use its ID to attach it to one or more cache behaviors in a CloudFront distribution. When it's attached to a cache behavior, CloudFront adds the headers in the policy to HTTP responses that it sends for requests that match the cache behavior.

For more information, see Adding HTTP headers to CloudFront responses in the Amazon CloudFront Developer Guide.

Contents

Id

The identifier for the response headers policy.

Type: String

Required: Yes

LastModifiedTime

The date and time when the response headers policy was last modified.

Type: Timestamp

Required: Yes

ResponseHeadersPolicyConfig

A response headers policy configuration.

A response headers policy contains information about a set of HTTP response headers and their values. CloudFront adds the headers in the policy to HTTP responses that it sends for requests that match a cache behavior that's associated with the policy.

Type: ResponseHeadersPolicyConfig (p. 510) 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 V2
- AWS SDK for Ruby V3
ResponseHeadersPolicyAccessControlAllowHeaders

A list of HTTP header names that CloudFront includes as values for the Access-Control-Allow-Headers HTTP response header.

For more information about the Access-Control-Allow-Headers HTTP response header, see Access-Control-Allow-Headers in the MDN Web Docs.

Contents

Items

The list of HTTP header names. You can specify * to allow all headers.

Type: Array of strings

Required: Yes

Quantity

The number of HTTP header names in the list.

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 V2
- AWS SDK for Ruby V3
ResponseHeadersPolicyAccessControlAllowMethods

A list of HTTP methods that CloudFront includes as values for the Access-Control-Allow-Methods HTTP response header.

For more information about the Access-Control-Allow-Methods HTTP response header, see Access-Control-Allow-Methods in the MDN Web Docs.

Contents

Items

The list of HTTP methods. Valid values are:

- GET
- DELETE
- HEAD
- OPTIONS
- PATCH
- POST
- PUT
- ALL

ALL is a special value that includes all of the listed HTTP methods.

Type: Array of strings

Valid Values: GET | POST | OPTIONS | PUT | DELETE | PATCH | HEAD | ALL

Required: Yes

Quantity

The number of HTTP methods in the list.

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 V2
- AWS SDK for Ruby V3
ResponseHeadersPolicyAccessControlAllowOrigins

A list of origins (domain names) that CloudFront can use as the value for the Access-Control-Allow-Origin HTTP response header.

For more information about the Access-Control-Allow-Origin HTTP response header, see Access-Control-Allow-Origin in the MDN Web Docs.

Contents

Items

The list of origins (domain names). You can specify * to allow all origins.

Type: Array of strings

Required: Yes

Quantity

The number of origins in the list.

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 V2
- AWS SDK for Ruby V3
ResponseHeadersPolicyAccessControlExposeHeaders

A list of HTTP headers that CloudFront includes as values for the Access-Control-Expose-Headers HTTP response header.

For more information about the Access-Control-Expose-Headers HTTP response header, see Access-Control-Expose-Headers in the MDN Web Docs.

**Contents**

**Items**

The list of HTTP headers. You can specify * to expose all headers.

- Type: Array of strings
- Required: No

**Quantity**

The number of HTTP headers in the list.

- 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 V2
- AWS SDK for Ruby V3
ResponseHeadersPolicyConfig

A response headers policy configuration.

A response headers policy configuration contains metadata about the response headers policy, and configurations for sets of HTTP response headers and their values. CloudFront adds the headers in the policy to HTTP responses that it sends for requests that match a cache behavior associated with the policy.

Contents

Comment

A comment to describe the response headers policy.

The comment cannot be longer than 128 characters.

Type: String

Required: No

CorsConfig

A configuration for a set of HTTP response headers that are used for cross-origin resource sharing (CORS).

Type: ResponseHeadersPolicyCorsConfig (p. 514) object

Required: No

CustomHeadersConfig

A configuration for a set of custom HTTP response headers.

Type: ResponseHeadersPolicyCustomHeadersConfig (p. 517) object

Required: No

Name

A name to identify the response headers policy.

The name must be unique for response headers policies in this AWS account.

Type: String

Required: Yes

SecurityHeadersConfig

A configuration for a set of security-related HTTP response headers.

Type: ResponseHeadersPolicySecurityHeadersConfig (p. 521) object

Required: No

ServerTimingHeadersConfig

A configuration for enabling the Server-Timing header in HTTP responses sent from CloudFront.

Type: ResponseHeadersPolicyServerTimingHeadersConfig (p. 523) 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 V2
- AWS SDK for Ruby V3
The policy directives and their values that CloudFront includes as values for the `Content-Security-Policy` HTTP response header.


### Contents

**ContentSecurityPolicy**

The policy directives and their values that CloudFront includes as values for the `Content-Security-Policy` HTTP response header.

Type: String

Required: Yes

**Override**

A Boolean that determines whether CloudFront overrides the `Content-Security-Policy` HTTP response header received from the origin with the one specified in this response headers policy.

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 V2
- AWS SDK for Ruby V3
ResponseHeadersPolicyContentTypeOptions

Determines whether CloudFront includes the X-Content-Type-Options HTTP response header with its value set to nosniff.

For more information about the X-Content-Type-Options HTTP response header, see X-Content-Type-Options in the MDN Web Docs.

Contents

Override

A Boolean that determines whether CloudFront overrides the X-Content-Type-Options HTTP response header received from the origin with the one specified in this response headers policy.

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 V2
- AWS SDK for Ruby V3
ResponseHeadersPolicyCorsConfig

A configuration for a set of HTTP response headers that are used for cross-origin resource sharing (CORS). CloudFront adds these headers to HTTP responses that it sends for CORS requests that match a cache behavior associated with this response headers policy.

For more information about CORS, see Cross-Origin Resource Sharing (CORS) in the MDN Web Docs.

Contents

AccessControlAllowCredentials

A Boolean that CloudFront uses as the value for the Access-Control-Allow-Credentials HTTP response header.

For more information about the Access-Control-Allow-Credentials HTTP response header, see Access-Control-Allow-Credentials in the MDN Web Docs.

Type: Boolean
Required: Yes

AccessControlAllowHeaders

A list of HTTP header names that CloudFront includes as values for the Access-Control-Allow-Headers HTTP response header.

For more information about the Access-Control-Allow-Headers HTTP response header, see Access-Control-Allow-Headers in the MDN Web Docs.

Type: ResponseHeadersPolicyAccessControlAllowHeaders (p. 506) object
Required: Yes

AccessControlAllowMethods

A list of HTTP methods that CloudFront includes as values for the Access-Control-Allow-Methods HTTP response header.

For more information about the Access-Control-Allow-Methods HTTP response header, see Access-Control-Allow-Methods in the MDN Web Docs.

Type: ResponseHeadersPolicyAccessControlAllowMethods (p. 507) object
Required: Yes

AccessControlAllowOrigins

A list of origins (domain names) that CloudFront can use as the value for the Access-Control-Allow-Origin HTTP response header.

For more information about the Access-Control-Allow-Origin HTTP response header, see Access-Control-Allow-Origin in the MDN Web Docs.

Type: ResponseHeadersPolicyAccessControlAllowOrigins (p. 508) object
Required: Yes

AccessControlExposeHeaders

A list of HTTP headers that CloudFront includes as values for the Access-Control-Expose-Headers HTTP response header.

**Type**: `ResponseHeadersPolicyAccessControlExposeHeaders (p. 509)` object

**Required**: No

---

**AccessControlMaxAgeSec**

A number that CloudFront uses as the value for the `Access-Control-Max-Age` HTTP response header.

For more information about the `Access-Control-Max-Age` HTTP response header, see [Access-Control-Max-Age](https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Acces) in the MDN Web Docs.

**Type**: Integer

**Required**: No

---

**OriginOverride**

A Boolean that determines whether CloudFront overrides HTTP response headers received from the origin with the ones specified in this response headers policy.

**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 V2
- AWS SDK for Ruby V3
ResponseHeadersPolicyCustomHeader

An HTTP response header name and its value. CloudFront includes this header in HTTP responses that it sends for requests that match a cache behavior that's associated with this response headers policy.

Contents

Header

The HTTP response header name.

Type: String

Required: Yes

Override

A Boolean that determines whether CloudFront overrides a response header with the same name received from the origin with the header specified here.

Type: Boolean

Required: Yes

Value

The value for the HTTP response header.

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 V2
- AWS SDK for Ruby V3
ResponseHeadersPolicyCustomHeadersConfig

A list of HTTP response header names and their values. CloudFront includes these headers in HTTP responses that it sends for requests that match a cache behavior that's associated with this response headers policy.

Contents

Items

The list of HTTP response headers and their values.

Type: Array of ResponseHeadersPolicyCustomHeader (p. 516) objects

Required: No

Quantity

The number of HTTP response headers in the list.

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 V2
- AWS SDK for Ruby V3
ResponseHeadersPolicyFrameOptions

Determines whether CloudFront includes the X-Frame-Options HTTP response header and the header’s value.

For more information about the X-Frame-Options HTTP response header, see X-Frame-Options in the MDN Web Docs.

Contents

FrameOption

The value of the X-Frame-Options HTTP response header. Valid values are DENY and SAMEORIGIN.

For more information about these values, see X-Frame-Options in the MDN Web Docs.

Type: String

Valid Values: DENY | SAMEORIGIN

Required: Yes

Override

A Boolean that determines whether CloudFront overrides the X-Frame-Options HTTP response header received from the origin with the one specified in this response headers policy.

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 V2
- AWS SDK for Ruby V3
ResponseHeadersPolicyList

A list of response headers policies.

**Contents**

**Items**

The response headers policies in the list.

Type: Array of ResponseHeadersPolicySummary (p. 525) objects

Required: No

**MaxItems**

The maximum number of response headers policies requested.

Type: Integer

Required: Yes

**NextMarker**

If there are more items in the list than are in this response, this element is present. It contains the value that you should use in the Marker field of a subsequent request to continue listing response headers policies where you left off.

Type: String

Required: No

**Quantity**

The number of response headers policies returned.

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 V2
- AWS SDK for Ruby V3
ResponseHeadersPolicyReferrerPolicy

Determines whether CloudFront includes the `Referrer-Policy` HTTP response header and the header's value.

For more information about the `Referrer-Policy` HTTP response header, see `Referrer-Policy` in the MDN Web Docs.

Contents

Override

A Boolean that determines whether CloudFront overrides the `Referrer-Policy` HTTP response header received from the origin with the one specified in this response headers policy.

Type: Boolean

Required: Yes

ReferrerPolicy

The value of the `Referrer-Policy` HTTP response header. Valid values are:

- no-referrer
- no-referrer-when-downgrade
- origin
- origin-when-cross-origin
- same-origin
- strict-origin
- strict-origin-when-cross-origin
- unsafe-url

For more information about these values, see `Referrer-Policy` in the MDN Web Docs.

Type: String

Valid Values: no-referrer | no-referrer-when-downgrade | origin | origin-when-cross-origin | same-origin | strict-origin | strict-origin-when-cross-origin | unsafe-url

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 V2
- AWS SDK for Ruby V3
ResponseHeadersPolicySecurityHeadersConfig

A configuration for a set of security-related HTTP response headers. CloudFront adds these headers to HTTP responses that it sends for requests that match a cache behavior associated with this response headers policy.

Contents

ContentSecurityPolicy

The policy directives and their values that CloudFront includes as values for the Content-Security-Policy HTTP response header.

For more information about the Content-Security-Policy HTTP response header, see Content-Security-Policy in the MDN Web Docs.

Type: ResponseHeadersPolicyContentSecurityPolicy (p. 512) object

Required: No

ContentTypeOptions

Determines whether CloudFront includes the X-Content-Type-Options HTTP response header with its value set to nosniff.

For more information about the X-Content-Type-Options HTTP response header, see X-Content-Type-Options in the MDN Web Docs.

Type: ResponseHeadersPolicyContentTypeOptions (p. 513) object

Required: No

FrameOptions

Determines whether CloudFront includes the X-Frame-Options HTTP response header and the header's value.

For more information about the X-Frame-Options HTTP response header, see X-Frame-Options in the MDN Web Docs.

Type: ResponseHeadersPolicyFrameOptions (p. 518) object

Required: No

ReferrerPolicy

Determines whether CloudFront includes the Referrer-Policy HTTP response header and the header's value.

For more information about the Referrer-Policy HTTP response header, see Referrer-Policy in the MDN Web Docs.

Type: ResponseHeadersPolicyReferrerPolicy (p. 520) object

Required: No

StrictTransportSecurity

Determines whether CloudFront includes the Strict-Transport-Security HTTP response header and the header's value.

Type: **ResponseHeadersPolicyStrictTransportSecurity** (p. 524) object

Required: No

**XSSProtection**

Determines whether CloudFront includes the X-XSS-Protection HTTP response header and the header's value.

For more information about the X-XSS-Protection HTTP response header, see [X-XSS-Protection](https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-XSS-Protection) in the MDN Web Docs.

Type: **ResponseHeadersPolicyXSSProtection** (p. 526) 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 V2
- AWS SDK for Ruby V3
ResponseHeadersPolicyServerTimingHeadersConfig

A configuration for enabling the Server-Timing header in HTTP responses sent from CloudFront. CloudFront adds this header to HTTP responses that it sends in response to requests that match a cache behavior that's associated with this response headers policy.

You can use the Server-Timing header to view metrics that can help you gain insights about the behavior and performance of CloudFront. For example, you can see which cache layer served a cache hit, or the first byte latency from the origin when there was a cache miss. You can use the metrics in the Server-Timing header to troubleshoot issues or test the efficiency of your CloudFront configuration. For more information, see Server-Timing header in the Amazon CloudFront Developer Guide.

Contents

Enabled

A Boolean that determines whether CloudFront adds the Server-Timing header to HTTP responses that it sends in response to requests that match a cache behavior that's associated with this response headers policy.

Type: Boolean

Required: Yes

SamplingRate

A number 0–100 (inclusive) that specifies the percentage of responses that you want CloudFront to add the Server-Timing header to. When you set the sampling rate to 100, CloudFront adds the Server-Timing header to the HTTP response for every request that matches the cache behavior that this response headers policy is attached to. When you set it to 50, CloudFront adds the header to 50% of the responses for requests that match the cache behavior. You can set the sampling rate to any number 0–100 with up to four decimal places.

Type: Double

Valid Range: Minimum value of 0.0. Maximum value of 100.0.

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 V2
- AWS SDK for Ruby V3
ResponseHeadersPolicyStrictTransportSecurity

Determines whether CloudFront includes the Strict-Transport-Security HTTP response header and the header’s value.


Contents

AccessControlMaxAgeSec

A number that CloudFront uses as the value for the max-age directive in the Strict-Transport-Security HTTP response header.

Type: Integer

Required: Yes

IncludeSubdomains

A Boolean that determines whether CloudFront includes the includeSubDomains directive in the Strict-Transport-Security HTTP response header.

Type: Boolean

Required: No

Override

A Boolean that determines whether CloudFront overrides the Strict-Transport-Security HTTP response header received from the origin with the one specified in this response headers policy.

Type: Boolean

Required: Yes

Preload

A Boolean that determines whether CloudFront includes the preload directive in the Strict-Transport-Security HTTP response header.

Type: Boolean

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 V2
- AWS SDK for Ruby V3
ResponseHeadersPolicySummary

Contains a response headers policy.

Contents

ResponseHeadersPolicy

The response headers policy.

Type: ResponseHeadersPolicy (p. 505) object

Required: Yes

Type

The type of response headers policy, either managed (created by AWS) or custom (created in this AWS account).

Type: String

Valid Values: managed | custom

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 V2
- AWS SDK for Ruby V3
ResponseHeadersPolicyXSSProtection

Determines whether CloudFront includes the X-XSS-Protection HTTP response header and the header's value.

For more information about the X-XSS-Protection HTTP response header, see X-XSS-Protection in the MDN Web Docs.

Contents

ModeBlock

A Boolean that determines whether CloudFront includes the mode=block directive in the X-XSS-Protection header.

For more information about this directive, see X-XSS-Protection in the MDN Web Docs.

Type: Boolean

Required: No

Override

A Boolean that determines whether CloudFront overrides the X-XSS-Protection HTTP response header received from the origin with the one specified in this response headers policy.

Type: Boolean

Required: Yes

Protection

A Boolean that determines the value of the X-XSS-Protection HTTP response header. When this setting is true, the value of the X-XSS-Protection header is 1. When this setting is false, the value of the X-XSS-Protection header is 0.

For more information about these settings, see X-XSS-Protection in the MDN Web Docs.

Type: Boolean

Required: Yes

ReportUri

A reporting URI, which CloudFront uses as the value of the report directive in the X-XSS-Protection header.

You cannot specify a ReportUri when ModeBlock is true.

For more information about using a reporting URL, see X-XSS-Protection in the MDN Web Docs.

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 V2
• AWS SDK for Ruby V3
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. 448) 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 V2
- AWS SDK for Ruby V3
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 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 V2
- AWS SDK for Ruby V3
S3OriginConfig

A complex type that contains information about the Amazon S3 origin. If the origin is a custom origin or an S3 bucket that is configured as a website endpoint, 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 V2
- AWS SDK for Ruby V3
Signer

A list of AWS accounts and the active CloudFront key pairs in each account that CloudFront can use to verify the signatures of signed URLs and signed cookies.

Contents

**AwsAccountNumber**

An AWS account number that contains active CloudFront key pairs that CloudFront can use to verify the signatures of signed URLs and signed cookies. If the AWS account that owns the key pairs is the same account that owns the CloudFront distribution, the value of this field is `self`.

Type: String
Required: No

**KeyPairIds**

A list of CloudFront key pair identifiers.

Type: *KeyPairIds (p. 460)* 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 V2
- AWS SDK for Ruby V3
StatusCodes

A complex data type for the status codes that you specify that, when returned by a primary origin, trigger CloudFront to failover to a second origin.

Contents

Items

The items (status codes) for an origin group.

Type: Array of integers

Array Members: Minimum number of 1 item.

Required: Yes

Quantity

The number of status codes.

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 V2
- AWS SDK for Ruby V3
StreamingDistribution

A streaming distribution tells CloudFront where you want RTMP content to be delivered from, and the details about how to track and manage content delivery.

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. 368) object

Required: Yes

ARN

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

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.
Amazon CloudFront API Reference

See Also

Type: String
Required: Yes

StreamingDistributionConfig

The current configuration information for the RTMP distribution.

Type: StreamingDistributionConfig (p. 535) 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 V2
- AWS SDK for Ruby V3
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. 369) 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 StreamingDistributionConfig object), CloudFront creates a new distribution.

If CallerReference is a value that you already sent in a previous request to create a distribution, 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. 542) 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

Required: No
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. 529) 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. 548) 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 V2
- AWS SDK for Ruby V3
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. 535) object

Required: Yes

Tags

A complex type that contains zero or more Tag elements.

Type: Tags (p. 545) 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 V2
- AWS SDK for Ruby V3
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. 540) 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:
- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2
- AWS SDK for Ruby V3
StreamingDistributionSummary

A summary of the information for a 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. 369) 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**

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

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. 529) 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.

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

Type: TrustedSigners (p. 548) 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 V2
- AWS SDK for Ruby V3
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 V2
- AWS SDK for Ruby V3
**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 V2
- AWS SDK for Ruby V3
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}\p{.}\p{_:\p{N}\p{=}\p{+}\p{-}\p{@}}\^\d\*]`*

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 V2
- AWS SDK for Ruby V3
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. 543) 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 V2
- AWS SDK for Ruby V3
TestResult

Contains the result of testing a CloudFront function with TestFunction.

Contents

ComputeUtilization

The amount of time that the function took to run as a percentage of the maximum allowed time. For example, a compute utilization of 35 means that the function completed in 35% of the maximum allowed time.

Type: String
Required: No

FunctionErrorMessage

If the result of testing the function was an error, this field contains the error message.

Type: String
Required: No

FunctionExecutionLogs

Contains the log lines that the function wrote (if any) when running the test.

Type: Array of strings
Required: No

FunctionOutput

The event object returned by the function. For more information about the structure of the event object, see Event object structure in the Amazon CloudFront Developer Guide.

Type: String
Required: No

FunctionSummary

Contains configuration information and metadata about the CloudFront function that was tested.

Type: FunctionSummary (p. 447) 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 V2
- AWS SDK for Ruby V3
TrustedKeyGroups

A list of key groups whose public keys CloudFront can use to verify the signatures of signed URLs and signed cookies.

Contents

Enabled

This field is true if any of the key groups in the list have public keys that CloudFront can use to verify the signatures of signed URLs and signed cookies. If not, this field is false.

Type: Boolean

Required: Yes

Items

A list of key groups identifiers.

Type: Array of strings

Required: No

Quantity

The number of key groups in the list.

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 V2
- AWS SDK for Ruby V3
**TrustedSigners**

A list of AWS accounts whose public keys CloudFront can use to verify the signatures of signed URLs and signed cookies.

**Contents**

**Enabled**

This field is `true` if any of the AWS accounts have public keys that CloudFront can use to verify the signatures of signed URLs and signed cookies. If not, this field is `false`.

Type: Boolean  
Required: Yes

**Items**

A list of AWS account identifiers.

Type: Array of strings  
Required: No

**Quantity**

The number of AWS accounts in the list.

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 V2
- AWS SDK for Ruby V3
ViewerCertificate

A complex type that determines the distribution’s SSL/TLS configuration for communicating with viewers.

If the distribution doesn’t use Aliases (also known as alternate domain names or CNAMEs)—that is, if the distribution uses the CloudFront domain name such as d111111abcdef8.cloudfront.net—set CloudFrontDefaultCertificate to true and leave all other fields empty.

If the distribution uses aliases (alternate domain names or CNAMEs), use the fields in this type to specify the following settings:

- Which viewers the distribution accepts HTTPS connections from: only viewers that support server name indication (SNI) (recommended), or all viewers including those that don’t support SNI.
  - To accept HTTPS connections from only viewers that support SNI, set SSLSupportMethod to sni-only. This is recommended. Most browsers and clients support SNI. (In CloudFormation, the field name is SslSupportMethod. Note the different capitalization.)
  - To accept HTTPS connections from all viewers, including those that don’t support SNI, set SSLSupportMethod to vip. This is not recommended, and results in additional monthly charges from CloudFront. (In CloudFormation, the field name is SslSupportMethod. Note the different capitalization.)
- The minimum SSL/TLS protocol version that the distribution can use to communicate with viewers. To specify a minimum version, choose a value for MinimumProtocolVersion. For more information, see Security Policy in the Amazon CloudFront Developer Guide.
- The location of the SSL/TLS certificate, AWS Certificate Manager (ACM) (recommended) or AWS Identity and Access Management (IAM). You specify the location by setting a value in one of the following fields (not both):
  - ACMCertificateArn (In CloudFormation, this field name is AcmCertificateArn. Note the different capitalization.)
  - IAMCertificateId (In CloudFormation, this field name is IamCertificateId. Note the different capitalization.)

All distributions support HTTPS connections from viewers. To require viewers to use HTTPS only, or to redirect them from HTTP to HTTPS, use ViewerProtocolPolicy in the CacheBehavior or DefaultCacheBehavior. To specify how CloudFront should use SSL/TLS to communicate with your custom origin, use CustomOriginConfig.

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

Contents

ACMCertificateArn

Note

In CloudFormation, this field name is AcmCertificateArn. Note the different capitalization.

If the distribution uses Aliases (alternate domain names or CNAMEs) and the SSL/TLS certificate is stored in AWS Certificate Manager (ACM), provide the Amazon Resource Name (ARN) of the ACM certificate. CloudFront only supports ACM certificates in the US East (N. Virginia) Region (us-east-1).

If you specify an ACM certificate ARN, you must also specify values for MinimumProtocolVersion and SSLSupportMethod. (In CloudFormation, the field name is SslSupportMethod. Note the different capitalization.)
Certificate

This field is deprecated. Use one of the following fields instead:

- ACMCertificateArn (In CloudFormation, this field name is AcmCertificateArn. Note the different capitalization.)
- IAMCertificateId (In CloudFormation, this field name is IamCertificateId. Note the different capitalization.)
- CloudFrontDefaultCertificate

Type: String
Required: No

CertificateSource

This field is deprecated. Use one of the following fields instead:

- ACMCertificateArn (In CloudFormation, this field name is AcmCertificateArn. Note the different capitalization.)
- IAMCertificateId (In CloudFormation, this field name is IamCertificateId. Note the different capitalization.)
- CloudFrontDefaultCertificate

Type: String
Valid Values: cloudfront | iam | acm
Required: No

CloudFrontDefaultCertificate

If the distribution uses the CloudFront domain name such as d111111abcdef8.cloudfront.net, set this field to true.

If the distribution uses Aliases (alternate domain names or CNAMEs), set this field to false and specify values for the following fields:

- ACMCertificateArn or IAMCertificateId (specify a value for one, not both)

In CloudFormation, these field names are AcmCertificateArn and IamCertificateId. Note the different capitalization.

Type: Boolean
Required: No

IAMCertificateId

Note
In CloudFormation, this field name is IamCertificateId. Note the different capitalization.

If the distribution uses Aliases (alternate domain names or CNAMEs) and the SSL/TLS certificate is stored in AWS Identity and Access Management (IAM), provide the ID of the IAM certificate.
If you specify an IAM certificate ID, you must also specify values for `MinimumProtocolVersion` and `SSLSupportMethod`. (In CloudFormation, the field name is `SslSupportMethod`. Note the different capitalization.)

Type: String

Required: No

**MinimumProtocolVersion**

If the distribution uses `Aliases` (alternate domain names or CNAMEs), specify the security policy that you want CloudFront to use for HTTPS connections with viewers. The security policy determines two settings:

- The minimum SSL/TLS protocol that CloudFront can use to communicate with viewers.
- The ciphers that CloudFront can use to encrypt the content that it returns to viewers.

For more information, see Security Policy and Supported Protocols and Ciphers Between Viewers and CloudFront in the *Amazon CloudFront Developer Guide*.

**Note**

On the CloudFront console, this setting is called **Security Policy**.

When you’re using SNI only (you set `SSLSupportMethod` to `sni-only`), you must specify TLSv1 or higher. (In CloudFormation, the field name is `SslSupportMethod`. Note the different capitalization.)

If the distribution uses the CloudFront domain name such as `d111111abcdef8.cloudfront.net` (you set `CloudFrontDefaultCertificate` to `true`), CloudFront automatically sets the security policy to TLSv1 regardless of the value that you set here.

Type: String

Valid Values: `SSLv3` | `TLSv1` | `TLSv1_2016` | `TLSv1.1_2016` | `TLSv1.2_2018` | `TLSv1.2_2019` | `TLSv1.2_2021`

Required: No

**SSLSupportMethod**

**Note**

In CloudFormation, this field name is `SslSupportMethod`. Note the different capitalization.

If the distribution uses `Aliases` (alternate domain names or CNAMEs), specify which viewers the distribution accepts HTTPS connections from.

- `sni-only` – The distribution accepts HTTPS connections from only viewers that support server name indication (SNI). This is recommended. Most browsers and clients support SNI.
- `vip` – The distribution accepts HTTPS connections from all viewers including those that don’t support SNI. This is not recommended, and results in additional monthly charges from CloudFront.
- `static-ip` - Do not specify this value unless your distribution has been enabled for this feature by the CloudFront team. If you have a use case that requires static IP addresses for a distribution, contact CloudFront through the AWS Support Center.

If the distribution uses the CloudFront domain name such as `d111111abcdef8.cloudfront.net`, don’t set a value for this field.

Type: String

Valid Values: `sni-only` | `vip` | `static-ip`

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 V2
- AWS SDK for Ruby V3
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

**NotAuthorized**

You do not have permission to perform this action.

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

**ValidationException**

The input fails to satisfy the constraints specified by an AWS service.

HTTP Status Code: 400