



v2018-09-12 Property Manager Deprecated Rule Formats

December 21, 2022

Contents

Welcome

[Welcome](#)

PAPI conventions

[API versioning](#)

[Advanced and locked features](#)

v2018-09-12 behaviors

[v2018-09-12 behaviors](#)

[adScalerCircuitBreaker](#)

[adaptiveImageCompression](#)

[adaptiveAcceleration](#)

[advanced](#)

[aggregatedReporting](#)

[akamaizer](#)

[akamaizerTag](#)

[allHttpInCacheHierarchy](#)

[allowCloudletsOrigins](#)

[allowDelete](#)

[allowHTTPSCacheKeySharing](#)

[allowHTTPSDowngrade](#)

[allowOptions](#)

[allowPatch](#)

[allowPost](#)

[allowPut](#)

[allowTransferEncoding](#)

[apiPrioritization](#)

[applicationLoadBalancer](#)

[autoDomainValidation](#)

[audienceSegmentation](#)

[baseDirectory](#)

[bossBeaconing](#)

[breakConnection](#)

[brotli](#)

[cacheError](#)

[cacheId](#)

[cacheKeyIgnoreCase](#)

[cacheKeyQueryParams](#)

[cacheKeyRewrite](#)

[cachePost](#)

[cacheRedirect](#)

[caching](#)

[centralAuthorization](#)

[chaseRedirects](#)

clientCharacteristics
constructResponse
contentCharacteristics
contentCharacteristicsAMD
contentCharacteristicsDD
contentCharacteristicsWsdLargeFile
contentCharacteristicsWsdLive
contentCharacteristicsWsdVod
contentTargetingProtection
cpCode
customBehavior
datastream
dcp
dcpAuthHMACTransformation
dcpAuthRegexTransformation
dcpAuthSubstringTransformation
dcpAuthVariableExtractor
dcpDefaultAuthzGroups
deliveryReceipt
denyDirectFailoverAccess
denyAccess
deviceCharacteristicCacheId
deviceCharacteristicHeader
dnsAsyncRefresh
dnsPrefresh
downgradeProtocol
downloadCompleteMarker
downloadNotification
downstreamCache
dynamicWebContent
edgeConnect
edgeImageConversion
edgeLoadBalancingAdvanced
edgeLoadBalancingDataCenter
edgeLoadBalancingOrigin
edgeOriginAuthorization
edgeRedirector
edgeScape
edgeSideIncludes
enhancedAkamaiProtocol
edgeWorker
failAction
fastInvalidate
firstPartyMarketing
firstPartyMarketingPlus
forwardRewrite
frontEndOptimization
g2oheader
hdDataAdvanced
gzipResponse
http2

healthDetection
imOverride
httpStrictTransportSecurity
imageManager
imageManagerVideo
inputValidation
injectReferenceld
instant
instantConfig
largeFileOptimization
largeFileOptimizationAdvanced
limitBitRate
mPulse
manifestPersonalization
manifestRerouting
manualServerPush
mediaAcceleration
mediaAccelerationQuicOptout
mediaClient
mediaFileRetrievalOptimization
mobileSdkPerformance
mediaOriginFailover
modifyIncomingRequestHeader
modifyIncomingResponseHeader
modifyOutgoingRequestHeader
netSession
modifyOutgoingResponseHeader
networkConditionsHeader
origin
originCharacteristics
originCharacteristicsWsd
persistentClientConnection
persistentConnection
personallyIdentifiableInformation
phasedRelease
preconnect
predictiveContentDelivery
predictivePrefetching
prefetch
prefetchable
prefreshCache
randomSeek
rapid
readTimeout
realUserMonitoring
redirect
redirectplus
referrerChecking
removeQueryParameter
removeVary
report

requestControl
requestTypeMarker
resourceOptimizer
responseCode
restrictObjectCaching
responseCookie
rmaOptimization
rewriteUrl
rumCustom
saasDefinitions
salesForceCommerceCloudClient
salesForceCommerceCloudProvider
savePostDcaProcessing
scheduleInvalidation
scriptManagement
segmentedContentProtection
shutr
segmentedMediaOptimization
setVariable
simulateErrorCode
siteShield
standardTLSMigrationOverride
standardTLSMigration
tcpOptimization
subCustomer
sureRoute
teaLeaf
tieredDistribution
tieredDistributionAdvanced
timeout
uidConfiguration
validateEntityTag
verifyJsonWebToken
verifyJsonWebTokenForDcp
verifyTokenAuthorization
visitorPrioritization
watermarkUrl
webApplicationFirewall
webSockets
webdav

v2018-09-12 criteria

v2018-09-12 criteria
advancedImMatch
bucket
cacheability
clientIp
clientIpVersion
cloudletsOrigin
contentDeliveryNetwork

contentType
deviceCharacteristic
fileExtension
filename
hostname
matchAdvanced
matchCpCode
matchResponseCode
matchVariable
metadataStage
originTimeout
path
queryStringParameter
random
regularExpression
requestCookie
requestHeader
requestMethod
requestProtocol
requestType
responseHeader
time
tokenAuthorization
userAgent
userLocation
userNetwork
variableError

Notice

Notice

Welcome

Welcome

Akamai often modifies Property Manager API (PAPI) features, each time deploying a new internal version of the feature. By default, the Property Manager interface in [Control Center](#)⁺ uses the latest available feature versions and you may be prompted to upgrade your configuration. In the interest of stability, PAPI does not support this system of selective updates for each feature. Instead, PAPI's rule objects are simply versioned as a whole. These versions, which update infrequently, are known as rule formats.

PAPI supports different dated versions for the set of features available within a property's rule tree. Akamai releases a new stable version of a rule format twice a year on average. As best practice, you should upgrade to the most recent dated rule format available. See [API versioning](#) for details.

This guide provides details for all behaviors and criteria the Property Manager API supports in the v2018-09-12 **deprecated** rule format version. The version available to you is determined by the product and modules assigned to the property. You can get it by running the [List available behaviors for a property](#) operation.

API versioning

The API exposes several different versioning systems:

- The version of the API is specified as part of the URL path. The current API version is `v1`.
- The API supports different dated versions for the set of features available within a property's rule tree. You can [freeze](#) and smoothly [update](#) the set of features that a property's rules apply to your content. Each behavior and criteria you invoke within your rules may independently increment versions from time to time, but you can only specify the most recent dated rule format to freeze the set of features. Otherwise, if you assign the `latest` rule format, features update automatically to their most recent version. This may abruptly result in errors if JSON in your rules no longer comply with the most recent feature's set of requirements.



Once you've frozen a rule format in PAPI, that state persists even if you use the Property Manager interface in [Control Center](#)[®]. You no longer get any feature upgrade prompts.

- The latest set of features are detailed in the [behavior](#) and [criteria](#) reference.
- PAPI lets you access your own set of property versions. Versions are available as URL resources that you can modify and activate independently, or perform roll-back if needed. This set is the only versioned object under your direct control.
- The API's [Build interface](#) also provides details on the current software release and its accompanying *catalog* of behaviors and criteria. These include version numbers and extraneous commit and build dates, which bear no relation to dated rule format versions. Don't rely on any of the internal version numbers this interface makes available.

Expect internal catalog release versions to update the most frequently, followed by less frequent rule format versions, followed by infrequent new API versions.

Advanced and locked features

In addition to its `name` and component `options`, special types of behavior and criteria objects may feature these additional members:

- A `uuid` string signifies an *advanced* feature. Advanced behaviors and criteria are read-only, and can only be modified by Akamai representatives. They typically deploy metadata customized for you, whose functionality falls outside the predefined guidelines of what other read/write behaviors can do. Such metadata might also cause problems if executed outside of

its intended context within the rule tree. Throughout the behavior and criteria reference, advanced features are identified as *read-only*.

- If a `locked` boolean member is `true`, it indicates a behavior or criteria that your Akamai representative has *locked* so that you can't modify it. You typically arrange with your representative to lock certain behaviors to protect sensitive data from erroneous changes. Any kind of behavior or criteria may be locked, including writable ones.

When modifying rule trees, you need to preserve the state of any `uuid` or `locked` members. You receive an error if you try to modify or delete either of these special types of feature. You can reposition regular features relative to these special ones, for example by inserting them within the same rule, but each rule's sequence of special features needs to remain unchanged.

Higher-level rule trees may also indicate the presence of these special features:

- A `uuid` member present on a rule object indicates that at least one of its component behaviors or criteria is advanced and read-only. You need to preserve this `uuid` as well when modifying the rule tree.
- A `criteriaLocked` member enabled on a criteria rule by your Akamai representative means that you may *not* insert additional criteria objects within the sequence. This typically keeps complex logical tests from breaking. Preserve the state of `criteriaLocked` when modifying the rule tree.

v2018-09-12 behaviors

v2018-09-12 behaviors

This section provides details for all behaviors the Property Manager API supports for the v2018-09-12 rule format version. The set available to you is determined by the product and modules assigned to the property. You can get it by running the [List available behaviors](#) operation.

This v2018-09-12 rule format provides an older deprecated set of PAPI features. You should use the most recent dated rule format available. See [API versioning](#) for details.

Option requirements

PAPI's behaviors and match criteria often include cross-dependent options, for which this reference documentation provides details in a *Requires* table column. For example, suppose documentation for a `cloudletSharedPolicy` option specifies this as *Requires*:

```
isSharedPolicy is true
```

That means for the `cloudletSharedPolicy` to appear in the object, you need to also have `isSharedPolicy` set to `true` :

```
{
  "isSharedPolicy": true,
  "cloudletSharedPolicy": 1000
}
```

Often you include options in behavior or criteria objects based on the match of a string value. Documentation also indicates any set of high-level logical *AND* and *OR* validation requirements.

adScalerCircuitBreaker

- **Property Manager name:** [Ad Scaler Circuit Breaker](#)✎
- **Behavior version:** The v2018-09-12 rule format supports the `adScalerCircuitBreaker` behavior v1.1.
- **Rule format status:** [Deprecated, outdated rule format](#)
- **Access:** [Read-write](#)

This behavior works with [manifestRerouting](#), to provide the scale and reliability of Akamai network while simultaneously allowing third party partners to modify the requested media content with value-added features. The `adScalerCircuitBreaker` behavior specifies the fallback action in case the technology partner encounters errors and can't modify the requested media object.

Option	Type	Description	Requires
--------	------	-------------	--------------------------

Option	Type	Description	Requires
<code>responseDelayBased</code>	boolean	Triggers a fallback action based on the delayed response from the technology partner's server.	
<code>responseDelayThreshold</code>	enum	Specifies the maximum response delay that, if exceeded, triggers the fallback action.	<code>responseDelayBased</code> is true
		Supported values: 500ms	
<code>responseCodeBased</code>	boolean	Triggers a fallback action based on the response code from the technology partner's server.	
<code>responseCodes</code>	string	Specifies the codes in the partner's response that trigger the fallback action, either 408 , 500 , 502 , 504 , SAME_AS_RECEIEVED , or SPECIFY_YOUR_OWN for a custom code.	<code>responseCodeBased</code> is true
<code>fallbackActionResponseCodeBased</code>	enum	Specifies the fallback action.	<code>responseDelayBased</code> is true OR <code>responseCodeBased</code> is true
	<code>RETURN_AKAMAI_COPY</code>	Return an unmodified Akamai copy of the manifest file to the requesting client.	
	<code>RETURN_ERROR</code>	Return an error as the server response.	
<code>returnErrorResponseCodeBased</code>	enum	Specifies the error to include in the response to the client.	<code>fallbackActionResponseCodeBased</code> is <code>RETURN_ERROR</code>
	<code>SAME_AS_RECEIEVED</code>	Return the same error received from the partner platform.	
	408	Return a 408 error.	
	500	Return a 500 error.	
	502	Return a 502 error.	
	504	Return a 504 error.	
	<code>SPECIFY_YOUR_OWN</code>	Customize the error.	
<code>specifyYourOwnResponseCodeBased</code>	string	Defines a custom error response.	<code>returnErrorResponseCodeBased</code> is <code>SPECIFY_YOUR_OWN</code>

adaptiveImageCompression

- **Property Manager name:** [Adaptive Image Compression](#) ^{*)}
- **Behavior version:** The `v2018-09-12` rule format supports the `adaptiveImageCompression` behavior v1.2.
- **Rule format status:** [Deprecated, outdated rule format](#)

- **Access:** [Read-write](#)

The Adaptive Image Compression feature compresses JPEG images depending on the requesting network's performance, thus improving response time. The behavior specifies three performance tiers based on round-trip tests: 1 for excellent, 2 for good, and 3 for poor. It assigns separate performance criteria for mobile (cellular) and non-mobile networks, which the `compressMobile` and `compressStandard` options enable independently.

There are six `method` options, one for each tier and type of network. If the `method` is `COMPRESS`, choose from among the six corresponding `slider` options to specify a percentage. As an alternative to compression, setting the `method` to `STRIP` removes unnecessary application-generated metadata from the image. Setting the `method` to `BYPASS` serves clients the original image.

The behavior serves `ETags` headers as a data signature for each adapted variation. In case of error or if the file size increases, the behavior serves the original image file. Flushing the original image from the edge cache also flushes adapted variants. The behavior applies to the following image file extensions: `jpg`, `jpeg`, `jpe`, `jif`, `jfif`, and `jfi`.

Option	Type	Description	Requires
<code>compressMobile</code>	boolean	Adapts images served over cellular mobile networks.	
<code>tier1MobileCompressionMethod</code>	enum	Specifies tier-1 behavior.	<code>compressMobile</code> is <code>true</code>
		Supported values: <code>BYPASS</code>	
<code>tier1MobileCompressionValue</code>	number (0-100)	Specifies the compression percentage.	<code>tier1MobileCompressionMethod</code> is <code>COMPRESS</code>
<code>tier2MobileCompressionMethod</code>	enum	Specifies tier-2 cellular-network behavior.	<code>compressMobile</code> is <code>true</code>
		Supported values: <code>BYPASS</code>	
<code>tier2MobileCompressionValue</code>	number (0-100)	Specifies the compression percentage.	<code>tier2MobileCompressionMethod</code> is <code>COMPRESS</code>
<code>tier3MobileCompressionMethod</code>	enum	Specifies tier-5 cellular-network behavior.	<code>compressMobile</code> is <code>true</code>
		Supported values: <code>BYPASS</code>	
<code>tier3MobileCompressionValue</code>	number (0-100)	Specifies the compression percentage.	<code>tier3MobileCompressionMethod</code> is <code>COMPRESS</code>
<code>compressStandard</code>	boolean	Adapts images served over non-cellular networks.	
<code>tier1StandardCompressionMethod</code>	enum	Specifies tier-1 non-cellular network behavior.	<code>compressStandard</code> is <code>true</code>
		Supported values: <code>BYPASS</code>	
<code>tier1StandardCompressionValue</code>	number (0-100)	Specifies the compression percentage.	<code>tier1StandardCompressionMethod</code> is <code>COMPRESS</code>
<code>tier2StandardCompressionMethod</code>	enum	Specifies tier-2 non-cellular network behavior.	<code>compressStandard</code> is <code>true</code>

Option	Type	Description	Requires
		Supported values: BYPASS	
tier2StandardCompressionValue	number (0-100)	Specifies the compression percentage.	tier2StandardCompressionMethod is COMPRESS
tier3StandardCompressionMethod	enum	Specifies tier-5 non-cellular network behavior.	compressStandard is true
		Supported values: BYPASS	
tier3StandardCompressionValue	number (0-100)	Specifies the compression percentage.	tier3StandardCompressionMethod is COMPRESS

adaptiveAcceleration

- **Property Manager name:** [Adaptive Acceleration](#)✎
- **Behavior version:** The v2018-09-12 rule format supports the adaptiveAcceleration behavior v1.5.
- **Rule format status:** [Deprecated, outdated rule format](#)
- **Access:** [Read-write](#)

Adaptive Acceleration uses HTTP/2 server push functionality with Ion properties to pre-position content and improve the performance of HTML page loading based on real user monitoring (RUM) timing data. It also helps browsers to preconnect to content that's likely needed for upcoming requests. To use this behavior, make sure you enable the [http2](#) behavior. Use the [Adaptive Acceleration API](#) to report on the set of assets this feature optimizes.

Option	Type	Description	Requires
source	string	The source Adaptive Acceleration uses to gather the real user monitoring timing data, either mPulse or realUserMonitoring. The recommended mPulse option supports all optimizations and requires the mPulse behavior added by default to new Ion properties. The classic realUserMonitoring method has been deprecated. If you set it as the data source, make sure you use it with the realUserMonitoring behavior.	enablePreconnect is true OR enablePush is true
enablePush	boolean	Recognizes resources like JavaScript, CSS, and images based on gathered timing data and sends these resources to a browser as it's waiting for a response to the initial request for your website or app. See Automatic Server Push for more information.	
enablePreconnect	boolean	Allows browsers to anticipate what connections your site needs, and establishes those connections ahead of time. See Automatic Preconnect for more information.	
enableRo	boolean	Enables the Resource Optimizer, which automates the compression and delivery of your .css, .js, and .svg content using a combination of Brotli and Zopfli compressions. The compression is performed offline, during a time to live that the feature automatically sets.	

advanced

- **Property Manager name:** [Advanced](#) [✎]
- **Behavior version:** The `v2018-09-12` rule format supports the `advanced` behavior v1.0.
- **Rule format status:** [Deprecated, outdated rule format](#)
- **Access:** [Read-only](#)

This specifies Akamai XML metadata. It can only be configured on your behalf by Akamai Professional Services.

Option	Type	Description
<code>description</code>	string	Human-readable description of what the XML block does.
<code>xml</code>	string	Akamai XML metadata.

aggregatedReporting


- **Property Manager name:** [Aggregated Reporting](#) [✎]
- **Behavior version:** The `v2018-09-12` rule format supports the `aggregatedReporting` behavior v1.2.
- **Rule format status:** [Deprecated, outdated rule format](#)
- **Access:** [Read-write](#)

Configure attributes for your custom aggregated reports. You can configure up to four attributes.

Option	Type	Description	Requires
<code>enabled</code>	boolean	Enables aggregated reporting.	
<code>report Name</code>	string	The unique name of the aggregated report within the property. If you reconfigure any attributes or variables in the aggregated reporting behavior, update this field to a unique value to enable logging data in a new instance of the report.	
<code>attributes Count</code>	number (1-4)	Select the number of attributes by which your report is grouped. You can add up to four attributes.	
<code>attribute1</code>	string (allows variables)	Select a previously user-defined variable to be an attribute for the report. The values extracted for all attributes range from 0 to 20 characters.	
<code>attribute2</code>	string (allows variables)	Select a previously user-defined variable to be an attribute for the report. The values extracted for all attributes range from 0 to 20 characters.	<code>attributes Count</code> ≥ 2
<code>attribute3</code>	string (allows variables)	Select a previously user-defined variable to be an attribute for the report. The values extracted for all attributes range from 0 to 20 characters.	<code>attributes Count</code> ≥ 3

Option	Type	Description	Requires
attribute4	string (allows variables)	Select a previously user-defined variable to be an attribute for the report. The values extracted for all attributes range from 0 to 20 characters.	attributes Count is 4


akamaizer

- **Property Manager name:** [Akamaizer](#) 
- **Behavior version:** The v2018-09-12 rule format supports the akamaizer behavior v1.1.
- **Rule format status:** [Deprecated, outdated rule format](#)
- **Access:** [Read-only](#)

This allows you to run regular expression substitutions over web pages. To apply this behavior, you need to match on a `contentType`. Contact Akamai Professional Services for help configuring the Akamaizer. See also the [akamaizerTag](#) behavior.

Option	Type	Description
enabled	boolean	Enables the Akamaizer behavior.

akamaizerTag

- **Property Manager name:** [Akamaize Tag](#) 
- **Behavior version:** The v2018-09-12 rule format supports the akamaizerTag behavior v1.1.
- **Rule format status:** [Deprecated, outdated rule format](#)
- **Access:** [Read-only](#)

This specifies HTML tags and replacement rules for hostnames used in conjunction with the [akamaizer](#) behavior. Contact Akamai Professional Services for help configuring the Akamaizer.

Option	Type	Description	Requires
match Hostname	string	Specifies the hostname to match on as a Perl-compatible regular expression.	
replacement Hostname	string	Specifies the replacement hostname for the tag to use.	
scope	enum	Specifies the part of HTML content the tagsAttribute refers to.	
	ATTRIBUTE	When tagsAttribute refers to a tag/attribute pair, the match only applies to the attribute.	
	URL_ ATTRIBUTE	The same as an attribute but applies when the attribute value is a URL. In that case, it converts to an absolute URL prior to substitution.	

Option	Type	Description	Requires															
	BLOCK	Substitutes within the tag's contents, but not within any nested tags.																
	PAGE	Ignores the <code>tagsAttribute</code> field and performs the substitution on the entire page.																
tagsAttribute	enum	Specifies the tag or tag/attribute combination to operate on.	scope is not PAGE															
		<div>Supported values:<table><tr><td>A</td><td>BASE_HREF</td><td>IMG</td></tr><tr><td>AREA</td><td>FORM</td><td>IMG_SRC</td></tr><tr><td>AREA_HREF</td><td>FORM_ACTION</td><td>LINK</td></tr><tr><td>A_HREF</td><td>IFRAME</td><td>LINK_HREF</td></tr><tr><td>BASE</td><td>IFRAME_SRC</td><td>SCRIPT</td></tr></table></div>	A	BASE_HREF	IMG	AREA	FORM	IMG_SRC	AREA_HREF	FORM_ACTION	LINK	A_HREF	IFRAME	LINK_HREF	BASE	IFRAME_SRC	SCRIPT	
A	BASE_HREF	IMG																
AREA	FORM	IMG_SRC																
AREA_HREF	FORM_ACTION	LINK																
A_HREF	IFRAME	LINK_HREF																
BASE	IFRAME_SRC	SCRIPT																
replaceAll	boolean	Replaces all matches when enabled, otherwise replaces only the first match.																
includeTagsAttribute	boolean	Whether to include the <code>tagsAttribute</code> value.																

allHttpInCacheHierarchy

- **Property Manager name:** [Allow All Methods on Parent Servers](#) [↗]
- **Behavior version:** The `v2018-09-12` rule format supports the `allHttpInCacheHierarchy` behavior v1.1.
- **Rule format status:** [Deprecated, outdated rule format](#)
- **Access:** [Read-write](#)

Allow all HTTP request methods to be used for the edge's parent servers, useful to implement features such as [Site Shield](#) [↗], [SureRoute](#) [↗], and Tiered Distribution. (See the [siteShield](#), [sureRoute](#), and [tieredDistribution](#) behaviors.)

Option	Type	Description
enabled	boolean	Enables all HTTP requests for parent servers in the cache hierarchy.

allowCloudletsOrigins

- **Property Manager name:** [Allow Conditional Origins](#) [↗]
- **Behavior version:** The `v2018-09-12` rule format supports the `allowCloudletsOrigins` behavior v1.3.
- **Rule format status:** [Deprecated, outdated rule format](#)
- **Access:** [Read-write](#)

Allows Cloudlets Origins to determine the criteria, separately from the Property Manager, under which alternate [origin](#) definitions are assigned.

This behavior needs to appear alone within its own rule. When enabled, it allows any [cloudlets Origin](#) criteria within sub-rules to override the prevailing origin.

Option	Type	Description
enabled	boolean	Allows you to assign custom origin definitions referenced in sub-rules by cloudletsOrigin labels. If disabled, all sub-rules are ignored.
honor Base Directory	boolean	Prefixes any Cloudlet-generated origin path with a path defined by an Origin Base Path behavior. If no path is defined, it has no effect. If another Cloudlet policy already prepends the same Origin Base Path, the path is not duplicated.
purge Origin Query Parameter	string	When purging content from a Cloudlets Origin, this specifies a query parameter name whose value is the specific named origin to purge. Note that this only applies to content purge requests, for example when using the Content Control Utility API .

allowDelete

- **Property Manager name:** [Allow DELETE](#)
- **Behavior version:** The `v2018-09-12` rule format supports the `allowDelete` behavior v1.3.
- **Rule format status:** [Deprecated, outdated rule format](#)
- **Access:** [Read-write](#)

Allow HTTP requests using the DELETE method. By default, GET, HEAD, and OPTIONS requests are allowed, and all other methods result in a 403 error. Such content does not cache, and any DELETE requests pass to the origin. See also the [allowOptions](#), [allowPatch](#), [allowPost](#), and [allowPut](#) behaviors.

Option	Type	Description
enabled	boolean	Allows DELETE requests. Content does <i>not</i> cache.
allowBody	boolean	Allows data in the body of the DELETE request.

allowHTTPSCacheKeySharing

- **Property Manager name:** [HTTPS Cache Key Sharing](#)
- **Behavior version:** The `v2018-09-12` rule format supports the `allowHTTPSCacheKeySharing` behavior v1.0.
- **Rule format status:** [Deprecated, outdated rule format](#)
- **Access:** [Read-write](#)

HTTPS cache key sharing allows HTTP requests to be served from an HTTPS cache.

Option	Type	Description
<code>enabled</code>	boolean	Enables HTTPS cache key sharing.

allowHTTPSDowngrade

- **Property Manager name:** [Protocol Downgrade \(HTTPS Downgrade to Origin\)](#)^{*}
- **Behavior version:** The `v2018-09-12` rule format supports the `allowHTTPSDowngrade` behavior v1.0.
- **Rule format status:** [Deprecated, outdated rule format](#)
- **Access:** [Read-write](#)

Passes HTTPS requests to origin as HTTP. This is useful when incorporating Standard TLS or Akamai's shared certificate delivery security with an origin that serves HTTP traffic.

Option	Type	Description
<code>enabled</code>	boolean	Downgrades to HTTP protocol for the origin server.

allowOptions

- **Property Manager name:** [Allow OPTIONS](#)^{*}
- **Behavior version:** The `v2018-09-12` rule format supports the `allowOptions` behavior v1.0.
- **Rule format status:** [Deprecated, outdated rule format](#)
- **Access:** [Read-write](#)

GET, HEAD, and OPTIONS requests are allowed by default. All other HTTP methods result in a 403 error. For full support of Cross-Origin Resource Sharing (CORS), you need to allow requests that use the OPTIONS method. If you're using the [corsSupport](#) behavior, do not disable OPTIONS requests. The response to an OPTIONS request is not cached, so the request always goes through the Akamai network to your origin, unless you use the [constructResponse](#) behavior to send responses directly from the Akamai network. See also the [allowDelete](#), [allowPatch](#), [allowPost](#), and [allowPut](#) behaviors.

Option	Type	Description
<code>enabled</code>	boolean	Allows OPTIONS requests. Content does <i>not</i> cache.

allowPatch

- **Property Manager name:** [Allow PATCH](#)✎
- **Behavior version:** The v2018-09-12 rule format supports the allowPatch behavior v1.1.
- **Rule format status:** [Deprecated, outdated rule format](#)
- **Access:** [Read-write](#)

Allow HTTP requests using the PATCH method. By default, GET, HEAD, and OPTIONS requests are allowed, and all other methods result in a 403 error. Such content does not cache, and any PATCH requests pass to the origin. See also the [allowDelete](#) , [allowOptions](#) , [allowPost](#) , and [allowPut](#) behaviors.

Option	Type	Description
enabled	boolean	Allows PATCH requests. Content does <i>not</i> cache.

allowPost

- **Property Manager name:** [Allow POST](#)✎
- **Behavior version:** The v2018-09-12 rule format supports the allowPost behavior v1.2.
- **Rule format status:** [Deprecated, outdated rule format](#)
- **Access:** [Read-write](#)

Allow HTTP requests using the POST method. By default, GET, HEAD, and OPTIONS requests are allowed, and all other methods result in a 403 error. See also the [allowDelete](#) , [allowOptions](#) , [allowPatch](#) , and [allowPut](#) behaviors.

Option	Type	Description
enabled	boolean	Allows POST requests.
allow Without Content Length	boolean	By default, POST requests also require a Content-Length header, or they result in a 411 error. With this option enabled with no specified Content-Length , the edge server relies on a Transfer-Encoding header to chunk the data. If neither header is present, it assumes the request has no body, and it adds a header with a 0 value to the forward request.

allowPut


- **Property Manager name:** [Allow PUT](#)✎
- **Behavior version:** The v2018-09-12 rule format supports the allowPut behavior v1.1.

- **Rule format status:** [Deprecated, outdated rule format](#)
- **Access:** [Read-write](#)

Allow HTTP requests using the PUT method. By default, GET, HEAD, and OPTIONS requests are allowed, and all other methods result in a 403 error. Such content does not cache, and any PUT requests pass to the origin. See also the [allowDelete](#) , [allowOptions](#) , [allowPatch](#) , and [allowPost](#) behaviors.

Option	Type	Description
enabled	boolean	Allows PUT requests. Content does <i>not</i> cache.


allowTransferEncoding


- **Property Manager name:** [Chunked Transfer Encoding](#) 
- **Behavior version:** The `v2018-09-12` rule format supports the `allowTransferEncoding` behavior v1.0.
- **Rule format status:** [Deprecated, outdated rule format](#)
- **Access:** [Read-write](#)

Controls whether to allow or deny Chunked Transfer Encoding (CTE) requests to pass to your origin. If your origin supports CTE, you should enable this behavior. This behavior also protects against a known issue when pairing [http2](#) and [webdav](#) behaviors within the same rule tree, in which case it's required.

Option	Type	Description
enabled	boolean	Allows Chunked Transfer Encoding requests.

apiPrioritization

- **Property Manager name:** [API Prioritization Cloudlet](#) 
- **Behavior version:** The `v2018-09-12` rule format supports the `apiPrioritization` behavior v2.2.
- **Rule format status:** [Deprecated, outdated rule format](#)
- **Access:** [Read-write](#)

Enables the API Prioritization Cloudlet, which maintains continuity in user experience by serving an alternate static response when load is too high. You can configure rules using either the Cloudlets Policy Manager application or the [Cloudlets API](#) . Use this feature serve static API content, such as fallback JSON data. To serve non-API HTML content, use the [visitorPrioritization](#) behavior.

Option	Type	Description	Requires
enabled	boolean	Activates the API Prioritization feature.	
cloudletPolicy	object	Identifies the Cloudlet policy.	
cloudletPolicy.id	number	Identifies the Cloudlet.	
cloudletPolicy.name	string	The Cloudlet's descriptive name.	
label	string	A label to distinguish this API Prioritization policy from any others in the same property.	
useThrottledCpCode	boolean	Specifies whether to apply an alternative CP code for requests served the alternate response.	
throttledCpCode	object	Specifies the CP code as an object.	useThrottledCpCode is true
throttledCpCode.description	string	Additional description for the CP code.	
throttledCpCode.id	integer	Unique identifier for each CP code.	
throttledCpCode.name	string	The name of the CP code.	
throttledCpCode.products	array	The set of products the CP code is assigned to.	
useThrottledStatusCode	boolean	Allows you to assign a specific HTTP response code to a throttled request.	
throttledStatusCode	number	Specifies the HTTP response code for requests that receive the alternate response.	useThrottledStatusCode is true
netStorage	object	Specify the NetStorage domain that contains the alternate response.	
netStorage.cpCodeList	array	A set of CP codes that apply to this storage group.	
netStorage.downloadDomainName	string	Domain name from which content can be downloaded.	
netStorage.id	number	Unique identifier for the storage group.	
netStorage.name	string	Name of the storage group.	
netStorage.uploadDomainName	string	Domain name used to upload content.	
netStoragePath	string	Specify the full NetStorage path for the alternate response, including trailing file name.	
alternateResponseCacheTtl	number (5-30)	Specifies the alternate response's time to live in the cache, 5 minutes by default.	

applicationLoadBalancer

- **Property Manager name:** [Application Load Balancer Cloudlet](#)
- **Behavior version:** The v2018-09-12 rule format supports the applicationLoadBalancer behavior v1.9.

- **Rule format status:** [Deprecated, outdated rule format](#)
- **Access:** [Read-write](#)

Enables the Application Load Balancer Cloudlet, which automates load balancing based on configurable criteria. To configure this behavior, use either the Cloudlets Policy Manager or the [Cloudlets API](#) to set up a policy.

Option	Type	Description	Requires
<code>enabled</code>	boolean	Activates the Application Load Balancer Cloudlet.	
<code>cloudletPolicy</code>	object	Identifies the Cloudlet policy.	
<code>cloudletPolicy.id</code>	number	Identifies the Cloudlet.	
<code>cloudletPolicy.name</code>	string	The Cloudlet's descriptive name.	
<code>label</code>	string	A label to distinguish this Application Load Balancer policy from any others within the same property.	
<code>stickinessCookieType</code>	enum	Determines how a cookie persistently associates the client with a load-balanced origin.	
	NONE	Dynamically reassigns different load-balanced origins for each request.	
	NEVER	Preserves the cookie indefinitely.	
	ON_BROWSER_CLOSE	Limit the cookie duration to browser sessions.	
	FIXED_DATE	Specify a specific time for when the cookie expires.	
	DURATION	Specify a delay for when the cookie expires.	
	ORIGIN_SESSION	Limit the cookie duration to when the ORIGIN_SESSION terminates. (After the cookie expires, the cookie type re-evaluates.)	
<code>stickinessExpirationDate</code>	string (epoch timestamp)	Specifies when the cookie expires.	<code>stickinessCookieType</code> is <code>FIXED_DATE</code>
<code>stickinessDuration</code>	string (duration)	Sets how long it is before the cookie expires.	<code>stickinessCookieType</code> is <code>DURATION</code>
<code>stickinessRefresh</code>	boolean	Extends the duration of the cookie with each new request. When enabled, the <code>DURATION</code> thus specifies the latency between requests that would cause the cookie to expire.	<code>stickinessCookieType</code> is <code>DURATION</code>
<code>originCookieName</code>	string	Specifies the name for your session cookie.	<code>stickinessCookieType</code> is <code>ORIGIN_SESSION</code>
<code>specifyStickinessCookieDomain</code>	boolean	Specifies whether to use a cookie domain with the stickiness cookie, to tell the browser to which domain to send the cookie.	<code>stickinessCookieType</code> is either: <code>ON_BROWSER_CLOSE</code> , <code>FIXED_DATE</code> , <code>DURATION</code> , <code>NEVER</code> , <code>ORIGIN_SESSION</code>
<code>stickinessCookieDomain</code>	string	Specifies the domain to track the stickiness cookie.	<code>specifyStickinessCookieDomain</code> is <code>true</code>

Option	Type	Description	Requires
stickinessCookieAutomaticSalt	boolean	Sets whether to assign a <i>salt</i> value automatically to the cookie to prevent manipulation by the user. You should not enable this if sharing the population cookie across more than one property.	stickinessCookieType is either: ON_BROWSER_CLOSE, FIXED_DATE, DURATION, NEVER, ORIGIN_SESSION
stickinessCookieSalt	string	Specifies the stickiness cookie's salt value. Use this option to share the cookie across many properties.	stickinessCookieAutomaticSalt is false
stickinessCookieSetHttpOnlyFlag	boolean	Ensures the cookie is transmitted only over HTTP.	stickinessCookieType is either: ON_BROWSER_CLOSE, FIXED_DATE, DURATION, NEVER, ORIGIN_SESSION
stickinessCookieSetSecureFlag	boolean	Deploys the stickiness cookie as secure.	stickinessCookieType is either: ON_BROWSER_CLOSE, FIXED_DATE, DURATION, NEVER, ORIGIN_SESSION
allDownNetStorage	object	Specifies a NetStorage account for a static maintenance page as a fallback when no origins are available.	
allDownNetStorage.cpCodeList	array	A set of CP codes that apply to this storage group.	
allDownNetStorage.downloadDomainName	string	Domain name from which content can be downloaded.	
allDownNetStorage.id	number	Unique identifier for the storage group.	
allDownNetStorage.name	string	Name of the storage group.	
allDownNetStorage.uploadDomainName	string	Domain name used to upload content.	
allDownNetStorageFile	string	Specifies the fallback maintenance page's filename, expressed as a full path from the root of the NetStorage server.	
allDownStatusCode	string	Specifies the HTTP response code when all load-balancing origins are unavailable.	
failoverStatusCodes	string array	Specifies a set of HTTP status codes that signal a failure on the origin, in which case the cookie that binds the client to that origin is invalidated and the client is rerouted to another available origin.	
failoverMode	enum	Determines what to do if an origin fails.	
	AUTOMATIC	Automatically determines which origin in the policy to try next.	
	MANUAL	You define a sequence of failover origins. (If failover runs out of origins, requests are sent to NetStorage.)	
	DISABLED	Turns off failover, but maintains origin stickiness even when the origin goes down.	

Option	Type	Description	Requires
failoverOrigin Map	object array	Specifies a fixed set of failover mapping rules.	failoverMode is MANUAL
failoverOrigin Map[].fromOrigin Id	string	Specifies the origin whose failure triggers the mapping rule.	
failoverOrigin Map[].toOriginIds	string array	Requests stuck to the fromOriginId origin retry for each alternate origin toOriginIds , until one succeeds.	
failoverAttempts Threshold	number	Sets the number of failed requests that would trigger the failover process.	failoverMode is either: MANUAL , AUTOMATIC
allowCache Prefresh	boolean	Allows the cache to prefresh. Only appropriate if all origins serve the same content for the same URL.	

autoDomainValidation

- **Property Manager name:** [Auto Domain Validation](#) [†]
- **Behavior version:** The v2018-09-12 rule format supports the autoDomainValidation behavior v1.0.
- **Rule format status:** [Deprecated, outdated rule format](#)
- **Access:** [Read-write](#)

This behavior allows standard TLS domain validated certificates to renew automatically. Apply it after using the [Certificate Provisioning System](#) [↗] to request a certificate for a hostname. To provision certificates programmatically, see the [Certificate Provisioning System API](#) [↗].

This behavior does not affect hostnames that use enhanced TLS certificates.

This behavior object does not support any options. Specifying the behavior enables it.

audienceSegmentation

- **Property Manager name:** [Audience Segmentation Cloudlet](#) [†]
- **Behavior version:** The v2018-09-12 rule format supports the audienceSegmentation behavior v2.3.
- **Rule format status:** [Deprecated, outdated rule format](#)
- **Access:** [Read-write](#)

Allows you to divide your users into different segments based on a persistent cookie. You can configure rules using either the Cloudlets Policy Manager application or the [Cloudlets API](#) [↗].

Option	Type	Description	Requires
enabled	boolean	Enables the Audience Segmentation cloudlet feature.	
cloudlet Policy	object	Identifies the Cloudlet policy.	
cloudlet Policy.id	number	Identifies the Cloudlet.	
cloudlet Policy.name	string	The Cloudlet's descriptive name.	
label	string	Specifies a suffix to append to the cookie name. This helps distinguish this audience segmentation policy from any others within the same property.	
segment Tracking Method	enum	Specifies the method to pass segment information to the origin. The Cloudlet passes the rule applied to a given request location.	
		Supported values: <div>IN_COOKIE_HEADER</div>	
segment Tracking Query Param	string	This query parameter specifies the name of the segmentation rule.	segment TrackingMethod is IN_QUERY_PARAM
segment Tracking Cookie Name	string	This cookie name specifies the name of the segmentation rule.	segment TrackingMethod is IN_COOKIE_HEADER
segment Tracking Custom Header	string	This custom HTTP header specifies the name of the segmentation rule.	segment TrackingMethod is IN_CUSTOM_HEADER
population CookieType	enum	Specifies when the segmentation cookie expires.	
	NEVER	Never expire.	
	ON_BROWSER_CLOSE	Expire at end of browser session.	
	DURATION	Specify a delay.	
population Duration	string (duration)	Specifies the lifetime of the segmentation cookie.	population CookieType is DURATION
population Refresh	boolean	If disabled, sets the expiration time only if the cookie is not yet present in the request.	population CookieType is DURATION
specify Population Cookie Domain	boolean	Whether to specify a cookie domain with the population cookie. It tells the browser to which domain to send the cookie.	
population Cookie Domain	string	Specifies the domain to track the population cookie.	specify PopulationCookieDomain is true
population Cookie Automatic Salt	boolean	Whether to assign a <i>salt</i> value automatically to the cookie to prevent manipulation by the user. You should not enable if sharing the population cookie across more than one property.	

Option	Type	Description	Requires
population CookieSalt	string	Specifies the cookie's salt value. Use this option to share the cookie across many properties.	population CookieAutomatic Salt is false
population Cookie IncludeRule Name	boolean	When enabled, includes in the session cookie the name of the rule in which this behavior appears.	

baseDirectory

- **Property Manager name:** [Origin Base Path](#)
- **Behavior version:** The v2018-09-12 rule format supports the baseDirectory behavior v1.1.
- **Rule format status:** [Deprecated, outdated rule format](#)
- **Access:** [Read-write](#)

Prefix URLs sent to the origin with a base path.

For example, with an origin of example.com , setting the value to /images sets the origin's base path to example.com/images . Any request for a my_pics/home.jpg file resolves on the origin server to example.com/images/my_pics/home.jpg .

Note that changing the origin's base path also causes a change to the cache key. Until that resolves, it may cause a traffic spike to your origin server.

Option	Type	Description
value	string (allows variables)	Specifies the base path of content on your origin server. The value needs to begin and end with a slash (/) character, for example /parent/child/ .

bossBeaconing

- **Property Manager name:** [Diagnostic data beacons \(Ex. BOSS\)](#)
- **Behavior version:** The v2018-09-12 rule format supports the bossBeaconing behavior v1.0.
- **Rule format status:** [Deprecated, outdated rule format](#)
- **Access:** [Read-only](#)

Triggers diagnostic data beacons for use with BOSS, Akamai's monitoring and diagnostics system.

Option	Type	Description
enabled	boolean	Enable diagnostic data beacons.

Option	Type	Description
cpcodes	string	The space-separated list of CP codes that trigger the beacons. You need to specify the same set of CP codes within BOSS.
requestType	enum	Specify when to trigger a beacon.
	EDGE	For edge requests only.
	EDGE_ MIDGRESS	Both end and midgress requests.
forwardType	enum	Specify when to trigger a beacon.
	MIDGRESS	For internal midgress forwards only.
	ORIGIN	For origin forwards only.
	MIDGRESS_ ORIGIN	Both.
sampling Frequency	enum	Specifies a sampling frequency or disables beacons.
	SAMPLING_ FREQ_0_0	Disables beacons altogether.
	SAMPLING_ FREQ_0_1	Specifies a sampling frequency.
conditional Sampling Frequency	enum	Specifies a conditional sampling frequency or disables beacons.
	CONDITIONAL_ SAMPLING_ FREQ_0_0	Disables beacons altogether.
	CONDITIONAL_ SAMPLING_ FREQ_0_1	Specifies a sampling frequency.
	CONDITIONAL_ SAMPLING_ FREQ_0_2	Specifies a sampling frequency.
	CONDITIONAL_ SAMPLING_ FREQ_0_3	Specifies a sampling frequency.
conditional HTTPStatus	string array	Specifies the set of response status codes or ranges that trigger the beacon.
		Supported values: <div>0xx 302 304 3xx 401 403 404</div>
conditional ErrorPattern	string	A space-separated set of error patterns that trigger beacons to conditional feeds. Each pattern can include wildcards, such as *CONNECT* *DENIED* .

breakConnection

- **Property Manager name:** [Break Forward Connection](#) [ⓘ]
- **Behavior version:** The v2018-09-12 rule format supports the breakConnection behavior v1.1.

- **Rule format status:** [Deprecated, outdated rule format](#)
- **Access:** [Read-write](#)

This behavior simulates an origin connection problem, typically to test an accompanying `fail Action` policy.

Option	Type	Description
<code>enabled</code>	boolean	Enables the break connection behavior.

brotnli

- **Property Manager name:** [Brotli Support](#)
- **Behavior version:** The `v2018-09-12` rule format supports the `brotnli` behavior v1.1.
- **Rule format status:** [Deprecated, outdated rule format](#)
- **Access:** [Read-write](#)

Applies Brotli compression, converting your origin content to cache on edge servers.

Option	Type	Description
<code>enabled</code>	boolean	Enables Brotli compression.

cacheError

- **Property Manager name:** [Cache HTTP Error Responses](#)
- **Behavior version:** The `v2018-09-12` rule format supports the `cacheError` behavior v1.1.
- **Rule format status:** [Deprecated, outdated rule format](#)
- **Access:** [Read-write](#)

Caches the origin's error responses to decrease server load. Applies for 10 seconds by default to the following HTTP codes: `204` , `305` , `400` , `404` , `405` , `501` , `502` , `503` , `504` , and `505` .

Option	Type	Description
<code>enabled</code>	boolean	Activates the error-caching behavior.
<code>tll</code>	string (duration)	Overrides the default caching duration of <code>10s</code> . Note that if set to <code>0</code> , it is equivalent to <code>no-cache</code> , which forces revalidation and may cause a traffic spike. This can be counterproductive when, for example, the origin is producing an error code of <code>500</code> .
<code>preserve Stale</code>	boolean	When enabled, the edge server preserves stale cached objects when the origin returns <code>400</code> , <code>500</code> , <code>502</code> , <code>503</code> , and <code>504</code> error codes. This avoids re-fetching and re-caching content after transient errors.

cacheId

- **Property Manager name:** [Cache ID Modification](#)
- **Behavior version:** The v2018-09-12 rule format supports the cacheId behavior v1.2.
- **Rule format status:** [Deprecated, outdated rule format](#)
- **Access:** [Read-write](#)

Controls which query parameters, headers, and cookies are included in or excluded from the cache key identifier.

Note that this behavior executes differently than usual within rule trees. Applying a set of cacheId behaviors within the same rule results in a system of forming cache keys that applies independently to the rule's content. If any cacheId behaviors are present in a rule, any others specified in parent rules or prior executing sibling rules no longer apply. Otherwise for any rule that lacks a cacheId behavior, the set of behaviors specified in an ancestor or prior sibling rule determines how to form cache keys for that content.

Option	Type	Description	Requires
rule	enum	Specifies how to modify the cache ID.	
	INCLUDE_QUERY_PARAMS	Includes the specified set of query parameters when forming a cache ID.	
	INCLUDE_COOKIES	Includes specified cookies in the cache ID.	
	INCLUDE_HEADERS	Includes specified HTTP headers in the cache ID.	
	EXCLUDE_QUERY_PARAMS	Excludes the specified set of query parameters when forming a cache ID.	
	INCLUDE_ALL_QUERY_PARAMS	Includes all query parameters when forming a cache ID.	
	INCLUDE_VARIABLE	Includes a specific user variable in the cache ID.	
	INCLUDE_URL	Includes the full URL, the same as the default without the cacheId behavior.	
include Value	boolean	Includes the value of the specified elements in the cache ID. Otherwise only their names are included.	rule is either: INCLUDE_COOKIES , INCLUDE_QUERY_PARAMS , INCLUDE_HEADERS
optional	boolean	Requires the behavior's specified elements to be present for content to cache. When disabled, requests that lack the specified elements are still cached.	rule is either: INCLUDE_COOKIES , INCLUDE_QUERY_PARAMS , INCLUDE_HEADERS , EXCLUDE_QUERY_PARAMS
elements	string array	Specifies the names of the query parameters, cookies, or headers to include or exclude from the cache ID.	rule is either: INCLUDE_COOKIES , INCLUDE_QUERY_PARAMS , INCLUDE_HEADERS , EXCLUDE_QUERY_PARAMS

Option	Type	Description	Requires
variable Name	string (variable name)	Specifies the name of the variable you want to include in the cache key.	rule is INCLUDE_VARIABLE

cacheKeyIgnoreCase

- **Property Manager name:** [Ignore Case In Cache Key](#) [↗]
- **Behavior version:** The v2018-09-12 rule format supports the `cacheKeyIgnoreCase` behavior v1.2.
- **Rule format status:** [Deprecated, outdated rule format](#)
- **Access:** [Read-write](#)

By default, cache keys are generated under the assumption that path and filename components are case-sensitive, so that `File.html` and `file.html` use separate cache keys. Enabling this behavior forces URL components whose case varies to resolve to the same cache key. Enable this behavior if your origin server is already case-insensitive, such as those based on Microsoft IIS.

With this behavior enabled, make sure any child rules do not match case-sensitive path components, or you may apply different settings to the same cached object.

Note that if already enabled, disabling this behavior potentially results in new sets of cache keys. Until these new caches are built, your origin server may experience traffic spikes as requests pass through. It may also result in *cache pollution*, excess cache space taken up with redundant content.

If you're using [NetStorage](#) [↗] in conjunction with this behavior, enable its **Force Case** option to match it, and make sure you name the original files consistently as either upper- or lowercase.

Option	Type	Description
<code>enabled</code>	boolean	Ignores case when forming cache keys.

cacheKeyQueryParams

- **Property Manager name:** [Cache Key Query Parameters](#) [↗]
- **Behavior version:** The v2018-09-12 rule format supports the `cacheKeyQueryParams` behavior v1.2.
- **Rule format status:** [Deprecated, outdated rule format](#)
- **Access:** [Read-write](#)

By default, cache keys are formed as URLs with full query strings. This behavior allows you to consolidate cached objects based on specified sets of query parameters.

Note also that whenever you apply behavior that generates new cache keys, your origin server may experience traffic spikes before the new cache starts to serve out.

Option	Type	Description	Requires
behavior	enum	Configures how sets of query string parameters translate to cache keys. Be careful not to ignore any parameters that result in substantially different content, as it is <i>not</i> reflected in the cached object.	
	INCLUDE_ ALL_ PRESERVE_ ORDER	Forms a separate key for the entire set of query parameters, but sensitive to the order in which they appear. (For example, <code>?q=akamai&state=ma</code> and <code>?state=ma&q=akamai</code> cache separately.)	
	INCLUDE_ ALL_ ALPHABETIZE_ ORDER	Forms keys for the entire set of parameters, but the order doesn't matter. The examples above both use the same cache key.	
	IGNORE_ALL	Causes query string parameters to be ignored when forming cache keys.	
	INCLUDE	Include the sequence of values in the <code>parameters</code> field.	
	IGNORE	Include all but the sequence of values in the <code>parameters</code> field.	
parameters	string array	Specifies the set of parameter field names to include in or exclude from the cache key. By default, these match the field names as string prefixes.	behavior is either: INCLUDE , IGNORE
exactMatch	boolean	When enabled, <code>parameters</code> needs to match exactly. Keep disabled to match string prefixes.	behavior is either: INCLUDE , IGNORE


cacheKeyRewrite

- **Property Manager name:** [Cache Key Path Rewrite \(Beta\)](#) [🔒]
- **Behavior version:** The `v2018-09-12` rule format supports the `cacheKeyRewrite` behavior v1.1.
- **Rule format status:** [Deprecated, outdated rule format](#)
- **Access:** [Read-only](#)

This behavior rewrites a default cache key's path. Contact Akamai Professional Services for help configuring it.

Option	Type	Description
purgeKey	string	Specifies the new cache key path as an alphanumeric value.


cachePost

- **Property Manager name:** [Cache POST Responses](#) 
- **Behavior version:** The v2018-09-12 rule format supports the cachePost behavior v1.1.
- **Rule format status:** [Deprecated, outdated rule format](#)
- **Access:** [Read-write](#)

By default, POST requests are passed to the origin. This behavior overrides the default, and allows you to cache POST responses.

Option	Type	Description
enabled	boolean	Enables caching of POST responses.
use Body	enum	Define how and whether to use the POST message body as a cache key.
	IGNORE	Uses only the URL to cache the response.
	MD5	Adds a string digest of the data as a query parameter to the cache URL.
	QUERY	Adds the raw request body as a query parameter to the cache key, but only if the POST request's Content-Type is application/x-www-form-urlencoded . (Use this in conjunction with cacheId to define relevant query parameters.)

cacheRedirect

- **Property Manager name:** [Cache HTTP Redirects](#) 
- **Behavior version:** The v2018-09-12 rule format supports the cacheRedirect behavior v1.0.
- **Rule format status:** [Deprecated, outdated rule format](#)
- **Access:** [Read-write](#)

Caches HTTP 302 redirect responses. By default, Akamai edge servers cache HTTP 302 redirects depending on their Cache-Control or Expires headers. Enabling this behavior instructs edge servers to cache 302 redirects the same as they would for HTTP 200 responses.

Option	Type	Description
enabled	boolean	Enables the redirect caching behavior.

caching

- **Property Manager name:** [Caching](#)
- **Behavior version:** The v2018-09-12 rule format supports the caching behavior v1.5.
- **Rule format status:** [Deprecated, outdated rule format](#)
- **Access:** [Read-write](#)

Control content caching on edge servers: whether or not to cache, whether to honor the origin's caching headers, and for how long to cache. Note that any NO_STORE or BYPASS_CACHE HTTP headers set on the origin's content overrides this behavior.

Option	Type	Description	Requires
behavior	enum	Specify the caching option.	
	MAX_AGE	Honor the origin's MAX_AGE header.	
	NO_STORE	Clears the cache and serves from the origin.	
	BYPASS_CACHE	Retains the cache but serves from the origin.	
	CACHE_CONTROL_AND_EXPIRES	Honor the origin's CACHE_CONTROL or EXPIRES header, whichever comes last. This adds support for the s-maxage response directive specified in RFC 7234 . Use this alternative value to instruct a downstream CDN how long to cache content.	
	CACHE_CONTROL	Honor the origin's CACHE_CONTROL header. This adds support for the s-maxage response directive specified in RFC 7234 . Use this alternative value to instruct a downstream CDN how long to cache content.	
	EXPIRES	Honor the origin's EXPIRES header.	
must Revalidate	boolean	Determines what to do once the cached content has expired, by which time the Akamai platform should have re-fetched and validated content from the origin. If enabled, only allows the re-fetched content to be served. If disabled, may serve stale content if the origin is unavailable.	behavior is either: CACHE_CONTROL_AND_EXPIRES , CACHE_CONTROL , EXPIRES , MAX_AGE
ttl	string (duration)	The maximum time content may remain cached. Setting the value to 0 is the same as setting a no-cache header, which forces content to revalidate.	behavior is MAX_AGE
defaultTtl	string (duration)	Set the MAX_AGE header for the cached content.	behavior is either: CACHE_CONTROL_AND_EXPIRES , CACHE_CONTROL , EXPIRES

centralAuthorization


- **Property Manager name:** [Centralized Authorization](#)
- **Behavior version:** The v2018-09-12 rule format supports the centralAuthorization behavior v1.1.
- **Rule format status:** [Deprecated, outdated rule format](#)

- **Access:** [Read-write](#)

Forward client requests to the origin server for authorization, along with optional `Set-Cookie` headers, useful when you need to maintain tight access control. The edge server forwards an `If-Modified-Since` header, to which the origin needs to respond with a `304` (Not-Modified) HTTP status when authorization succeeds. If so, the edge server responds to the client with the cached object, since it does not need to be re-acquired from the origin.

Option	Type	Description
<code>enabled</code>	boolean	Enables the centralized authorization behavior.


chaseRedirects

- **Property Manager name:** [Chase Redirects](#) 
- **Behavior version:** The `v2018-09-12` rule format supports the `chaseRedirects` behavior v1.1.
- **Rule format status:** [Deprecated, outdated rule format](#)
- **Access:** [Read-write](#)

Controls whether the edge server chases any redirects served from the origin.

Option	Type	Description
<code>enabled</code>	boolean	Allows edge servers to chase redirects.
<code>limit</code>	string	Specifies, as a string, the maximum number of redirects to follow.
<code>serve404</code>	boolean	Once the redirect <code>limit</code> is reached, enabling this option serves an HTTP <code>404</code> (Not Found) error instead of the last redirect.

clientCharacteristics

- **Property Manager name:** [Client Characteristics](#) 
- **Behavior version:** The `v2018-09-12` rule format supports the `clientCharacteristics` behavior v1.0.
- **Rule format status:** [Deprecated, outdated rule format](#)
- **Access:** [Read-write](#)

Specifies characteristics of the client ecosystem. Akamai uses this information to optimize your metadata configuration, which may result in better end-user performance.

See also [originCharacteristics](#) and various product-specific behaviors whose names are prefixed *contentCharacteristics*.

Option	Type	Description
country	enum	Specifies the client request's geographic region.
	GLOBAL	Global.
	GLOBAL_US_CENTRIC	Regional.
	GLOBAL_EU_CENTRIC	Regional.
	GLOBAL_ASIA_CENTRIC	Regional.
	EUROPE	Europe.
	NORTH_AMERICA	North America.
	SOUTH_AMERICA	South America.
	NORDICS	Northern Europe.
	ASIA_PACIFIC	Asia and Pacific Islands.
	AUSTRALIA	Australia.
	GERMANY	Germany.
	INDIA	India.
	ITALY	Italy.
	JAPAN	Japan.
	TAIWAN	Taiwan.
	UNITED_KINGDOM	United Kingdom.
	OTHER	A fallback value.
	UNKNOWN	Defer any optimizations.

constructResponse

- **Property Manager name:** [Construct Response](#)
- **Behavior version:** The v2018-09-12 rule format supports the constructResponse behavior v1.2.
- **Rule format status:** [Deprecated, outdated rule format](#)
- **Access:** [Read-write](#)

This behavior constructs an HTTP response, complete with HTTP status code and body, to serve from the edge independently of your origin. It supports all request methods except for POST .

Option	Type	Description
enabled	boolean	Serves the custom response.
body	string (allows variables)	HTML response of up to 2000 characters to send to the end-user client.
response Code	enum	The HTTP response code to send to the end-user client.

Option	Type	Description
		Supported values: 200 401 403 404 405 417
forceEviction	boolean	Removes the underlying object from the cache, since it is not being served.

contentCharacteristics

- **Property Manager name:** [Content Characteristics](#) [↗]
- **Behavior version:** The v2018-09-12 rule format supports the contentCharacteristics behavior v1.1.
- **Rule format status:** [Deprecated, outdated rule format](#)
- **Access:** [Read-write](#)

Specifies characteristics of the delivered content. Akamai uses this information to optimize your metadata configuration, which may result in better origin offload and end-user performance.

Along with other behaviors whose names are prefixed *contentCharacteristics*, this behavior is customized for a specific product set. Use PAPI's [List available behaviors](#) operation to determine the set available to you. See also the related [clientCharacteristics](#) and [originCharacteristics](#) behaviors.

Option	Type	Description
objectSize	enum	Optimize based on the size of the object retrieved from the origin.
	LESS_THAN_1MB	Less than 1Mb.
	ONE_MB_TO_TEN_MB	1-10 Mb.
	TEN_MB_TO_100_MB	10-100 Mb.
	OTHER	A fallback value.
	UNKNOWN	Defer this optimization.
popularityDistribution	enum	Optimize based on the content's expected popularity.
	LONG_TAIL	A low volume of requests over a long period.
	ALL_POPULAR	A high volume of requests over a short period.
	OTHER	A fallback value.
	UNKNOWN	Defer this optimization.
catalogSize	enum	Optimize based on the total size of the content library delivered.
	SMALL	Under 100GB.
	MEDIUM	100GB-1TB.
	LARGE	1TB-100TB.
	EXTRA_LARGE	More than 100TB.
	OTHER	A fallback value.

Option	Type	Description
	UNKNOWN	Defer this optimization.
contentType	enum	Optimize based on the type of content.
	USER_GENERATED	Generally, user-generated media.
	WEB_OBJECTS	Generally, media delivered for websites.
	SOFTWARE	Software.
	IMAGES	Images.
	OTHER_OBJECTS	Content that doesn't fall under any of these categories.
	UNKNOWN	Defer this optimization.

contentCharacteristicsAMD

- **Property Manager name:** [Content Characteristics](#) ⁺
- **Behavior version:** The v2018-09-12 rule format supports the contentCharacteristicsAMD behavior v1.1.
- **Rule format status:** [Deprecated, outdated rule format](#)
- **Access:** [Read-write](#)

Specifies characteristics of the delivered content. Akamai uses this information to optimize your metadata configuration, which may result in better origin offload and end-user performance.

Along with other behaviors whose names are prefixed *contentCharacteristics*, this behavior is customized for a specific product set. Use PAPI's [List available behaviors](#) operation to determine the set available to you. See also the related [clientCharacteristics](#) and [originCharacteristics](#) behaviors.

Option	Type	Description	Requires
catalogSize	enum	Optimize based on the total size of the content library delivered.	
	SMALL	Less than 100Gb.	
	MEDIUM	100Gb-1Tb.	
	LARGE	1-100Tb.	
	EXTRA_LARGE	More than 100Tb.	
	OTHER	Customize the value.	
	UNKNOWN	Defer this optimization.	
contentType	enum	Optimize based on the quality of media content.	
	SD	Standard definition.	
	HD	High definition.	
	ULTRA_HD	Ultra high definition.	

Option	Type	Description	Requires
	OTHER	More than one level of quality.	
	UNKNOWN	Defer this optimization.	
popularityDistribution	enum	Optimize based on the content's expected popularity.	
	LONG_TAIL	A low volume of requests over a long period.	
	ALL_POPULAR	A high volume of requests over a short period.	
	OTHER	Customize the value.	
	UNKNOWN	Defer this optimization.	
hls	boolean	Enable delivery of HLS media.	
segmentDurationHLS	enum	Specifies the duration of individual segments.	hls is true
	SEGMENT_DURATION_2S	2 seconds.	
	SEGMENT_DURATION_4S	4 seconds.	
	SEGMENT_DURATION_6S	6 seconds.	
	SEGMENT_DURATION_8S	8 seconds.	
	SEGMENT_DURATION_10S	10 seconds.	
	OTHER	Customize the value.	
segmentDurationHLSCustom	number	Customizes the number of seconds for the segment.	segmentDurationHLS is OTHER
segmentSizeHLS	enum	Specifies the size of the media object retrieved from the origin.	hls is true
	LESS_THAN_1MB	Less than 1Mb.	
	ONE_MB_TO_TEN_MB	1-10Mb.	
	TEN_MB_TO_100_MB	10-100Mb.	
	GREATER_THAN_100MB	More than 100Mb.	
	UNKNOWN	Defer this optimization.	
	OTHER	Sizes straddle these ranges.	
hds	boolean	Enable delivery of HDS media.	
segmentDurationHDS	enum	Specifies the duration of individual fragments.	hds is true
	SEGMENT_DURATION_2S	2 seconds.	
	SEGMENT_DURATION_4S	4 seconds.	
	SEGMENT_DURATION_6S	6 seconds.	
	SEGMENT_DURATION_8S	8 seconds.	

Option	Type	Description	Requires
	SEGMENT_DURATION_10S	10 seconds.	
	OTHER	Customize the value.	
segmentDurationHDSCustom	number	Customizes the number of seconds for the fragment.	segmentDurationHDS is OTHER
segmentSizeHDS	enum	Specifies the size of the media object retrieved from the origin.	hds is true
	LESS_THAN_1MB	Less than 1Mb.	
	ONE_MB_TO_TEN_MB	1-10Mb.	
	TEN_MB_TO_100_MB	10-100Mb.	
	GREATER_THAN_100MB	More than 100Mb.	
	UNKNOWN	Defer this optimization.	
	OTHER	Customize the value.	
dash	boolean	Enable delivery of DASH media.	
segmentDurationDASH	enum	Specifies the duration of individual segments.	dash is true
	SEGMENT_DURATION_2S	2 seconds.	
	SEGMENT_DURATION_4S	4 seconds.	
	SEGMENT_DURATION_6S	6 seconds.	
	SEGMENT_DURATION_8S	8 seconds.	
	SEGMENT_DURATION_10S	10 seconds.	
	OTHER	Customize the value.	
segmentDurationDASHCustom	number	Customizes the number of seconds for the segment.	segmentDurationDASH is OTHER
segmentSizeDASH	enum	Specifies the size of the media object retrieved from the origin.	dash is true
	LESS_THAN_1MB	Less than 1Mb.	
	ONE_MB_TO_TEN_MB	1-10Mb.	
	TEN_MB_TO_100_MB	10-100Mb.	
	GREATER_THAN_100MB	More than 100Mb.	
	UNKNOWN	Defer this optimization.	
	OTHER	Sizes that straddle these ranges.	
smooth	boolean	Enable delivery of Smooth media.	
segmentDurationSmooth	enum	Specifies the duration of individual fragments.	smooth is true

Option	Type	Description	Requires
	SEGMENT_DURATION_2S	2 seconds.	
	SEGMENT_DURATION_4S	4 seconds.	
	SEGMENT_DURATION_6S	6 seconds.	
	SEGMENT_DURATION_8S	8 seconds.	
	SEGMENT_DURATION_10S	10 seconds.	
	OTHER	Customize the value.	
segmentDurationSmoothCustom	number	Customizes the number of seconds for the fragment.	segmentDurationSmooth is OTHER
segmentSizeSmooth	enum	Specifies the size of the media object retrieved from the origin.	smooth is true
	LESS_THAN_1MB	Less than 1Mb.	
	ONE_MB_TO_TEN_MB	1-10Mb.	
	TEN_MB_TO_100_MB	10-100Mb.	
	GREATER_THAN_100MB	More than 100Mb.	
	UNKNOWN	Defer this optimization.	
	OTHER	Sizes straddle these ranges.	

contentCharacteristicsDD

- **Property Manager name:** [Content Characteristics](#)
- **Behavior version:** The v2018-09-12 rule format supports the contentCharacteristicsDD behavior v1.0.
- **Rule format status:** [Deprecated, outdated rule format](#)
- **Access:** [Read-write](#)

Specifies characteristics of the delivered content. Akamai uses this information to optimize your metadata configuration, which may result in better origin offload and end-user performance.

Along with other behaviors whose names are prefixed *contentCharacteristics*, this behavior is customized for a specific product set. Use PAPI's [List available behaviors](#) operation to determine the set available to you. See also the related [clientCharacteristics](#) and [originCharacteristics](#) behaviors.

Option	Type	Description
objectSize	enum	Optimize based on the size of the object retrieved from the origin.

Option	Type	Description
	LESS_THAN_1MB	Less than 1Mb.
	ONE_MB_TO_TEN_MB	1-10Mb.
	TEN_MB_TO_100_MB	10-100Mb.
	GREATER_THAN_100MB	More than 100Mb.
	OTHER	A fallback value.
	UNKNOWN	Defer this optimization.
popularity Distribution	enum	Optimize based on the content's expected popularity.
	LONG_TAIL	A low volume of requests over a long period.
	ALL_POPULAR	A high volume of requests over a short period.
	OTHER	A fallback value.
	UNKNOWN	Defer this optimization.
catalogSize	enum	Optimize based on the total size of the content library delivered.
	SMALL	Less than 100Gb.
	MEDIUM	100Gb-1Tb.
	LARGE	1-100Tb.
	EXTRA_LARGE	More than 100Tb.
	OTHER	A fallback value.
	UNKNOWN	Defer this optimization.
contentType	enum	Optimize based on the type of content.
	VIDEO	Video.
	SOFTWARE	Software.
	SOFTWARE_PATCH	Software patch.
	GAME	Game.
	GAME_PATCH	Game patch.
	OTHER_DOWNLOADS	Other downloads that don't fall into these categories.
	UNKNOWN	Defer this optimization.
optimizeOption	boolean	Optimizes the delivery throughput and download times for large files.

contentCharacteristicsWsdLargeFile

- **Property Manager name:** [Content Characteristics - Large File](#)
- **Behavior version:** The v2018-09-12 rule format supports the contentCharacteristicsWsdLargeFile behavior v1.0.
- **Rule format status:** [Deprecated, outdated rule format](#)

- **Access:** [Read-write](#)

Specifies characteristics of the delivered content, specifically targeted to delivering large files. Akamai uses this information to optimize your metadata configuration, which may result in better origin offload and end-user performance.

Along with other behaviors whose names are prefixed *contentCharacteristics*, this behavior is customized for a specific product set. Use PAPI's [List available behaviors](#) operation to determine the set available to you. See also the related [clientCharacteristics](#) and [originCharacteristics](#) behaviors.

Option	Type	Description
objectSize	enum	Optimize based on the size of the object retrieved from the origin.
	LESS_THAN_1MB	Less than 1Mb.
	ONE_MB_TO_TEN_MB	1-10Mb.
	TEN_MB_TO_100_MB	10-100Mb.
	GREATER_THAN_100MB	More than 100Mb.
	UNKNOWN	Defer this optimization.
popularityDistribution	enum	Optimize based on the content's expected popularity.
	LONG_TAIL	A low volume of requests over a long period.
	ALL_POPULAR	A high volume of requests over a short period.
	UNKNOWN	Defer this optimization.
catalogSize	enum	Optimize based on the total size of the content library delivered.
	SMALL	Less than 100Gb.
	MEDIUM	100Gb-1Tb.
	LARGE	1-100Tb.
	EXTRA_LARGE	More than 100Tb.
	UNKNOWN	Defer this optimization.
contentType	enum	Optimize based on the type of content.
	VIDEO	Video.
	SOFTWARE	Software.
	SOFTWARE_PATCH	Software patch.
	GAME	Game.
	GAME_PATCH	Game patch.
	OTHER_DOWNLOADS	Other downloads that don't fall into these categories.
	UNKNOWN	Defer this optimization.

contentCharacteristicsWsdLive

- **Property Manager name:** [Content Characteristics - Streaming Video Live](#) [↗]
- **Behavior version:** The v2018-09-12 rule format supports the contentCharacteristicsWsdLive behavior v1.0.
- **Rule format status:** [Deprecated, outdated rule format](#)
- **Access:** [Read-write](#)

Specifies characteristics of the delivered content, specifically targeted to delivering live video. Akamai uses this information to optimize your metadata configuration, which may result in better origin offload and end-user performance.

Along with other behaviors whose names are prefixed *contentCharacteristics*, this behavior is customized for a specific product set. Use PAPI's [List available behaviors](#) operation to determine the set available to you. See also the related [clientCharacteristics](#) and [originCharacteristics](#) behaviors.

Option	Type	Description	Requires
catalogSize	enum	Optimize based on the total size of the content library delivered.	
	SMALL	Less than 100Gb.	
	MEDIUM	100Gb-1Tb.	
	LARGE	1-100Tb.	
	EXTRA_LARGE	More than 100Tb.	
	UNKNOWN	Defer this optimization.	
contentType	enum	Optimize based on the quality of media content.	
	SD	Standard definition.	
	HD	High definition.	
	ULTRA_HD	Ultra high definition.	
	OTHER	More than one level of quality.	
	UNKNOWN	Defer this optimization.	
popularity Distribution	enum	Optimize based on the content's expected popularity.	
	LONG_TAIL	A low volume of requests over a long period.	
	ALL_POPULAR	A high volume of requests over a short period.	
	UNKNOWN	Defer this optimization.	
hls	boolean	Enable delivery of HLS media.	
segmentDuration HLS	enum	Specifies the duration of individual segments.	hls is true
	SEGMENT_DURATION_2S	2 seconds.	
	SEGMENT_DURATION_4S	4 seconds.	
	SEGMENT_DURATION_6S	6 seconds.	
	SEGMENT_DURATION_8S	8 seconds.	
	SEGMENT_DURATION_10S	10 seconds.	

Option	Type	Description	Requires
segmentSizeHLS	enum	Specifies the size of the media object retrieved from the origin.	hls is true
	LESS_THAN_1MB	Less than 1Mb.	
	ONE_MB_TO_TEN_MB	1-10Mb.	
	TEN_MB_TO_100_MB	10-100Mb.	
	GREATER_THAN_100MB	More than 100Mb.	
	UNKNOWN	Defer this optimization.	
	OTHER	Sizes straddle these ranges.	
hds	boolean	Enable delivery of HDS media.	
segmentDuration HDS	enum	Specifies the duration of individual fragments.	hds is true
	SEGMENT_DURATION_2S	2 seconds.	
	SEGMENT_DURATION_4S	4 seconds.	
	SEGMENT_DURATION_6S	6 seconds.	
	SEGMENT_DURATION_8S	8 seconds.	
	SEGMENT_DURATION_10S	10 seconds.	
segmentSizeHDS	enum	Specifies the size of the media object retrieved from the origin.	hds is true
	LESS_THAN_1MB	Less than 1Mb.	
	ONE_MB_TO_TEN_MB	1-10Mb.	
	TEN_MB_TO_100_MB	10-100Mb.	
	GREATER_THAN_100MB	More than 100Mb.	
	UNKNOWN	Defer this optimization.	
	OTHER	Sizes straddle these ranges.	
dash	boolean	Enable delivery of DASH media.	
segmentDuration DASH	enum	Specifies the duration of individual segments.	dash is true
	SEGMENT_DURATION_2S	2 seconds.	
	SEGMENT_DURATION_4S	4 seconds.	
	SEGMENT_DURATION_6S	6 seconds.	
	SEGMENT_DURATION_8S	8 seconds.	
	SEGMENT_DURATION_10S	10 seconds.	

Option	Type	Description	Requires
segmentSizeDASH	enum	Specifies the size of the media object retrieved from the origin.	dash is true
	LESS_THAN_1MB	Less than 1Mb.	
	ONE_MB_TO_TEN_MB	1-10Mb.	
	TEN_MB_TO_100_MB	10-100Mb.	
	GREATER_THAN_100MB	More than 100Mb.	
	UNKNOWN	Defer this optimization.	
	OTHER	Sizes straddle these ranges.	
smooth	boolean	Enable delivery of Smooth media.	
segmentDuration Smooth	enum	Specifies the duration of individual fragments.	smooth is true
	SEGMENT_DURATION_2S	2 seconds.	
	SEGMENT_DURATION_4S	4 seconds.	
	SEGMENT_DURATION_6S	6 seconds.	
	SEGMENT_DURATION_8S	8 seconds.	
	SEGMENT_DURATION_10S	10 seconds.	
segmentSize Smooth	enum	Specifies the size of the media object retrieved from the origin.	smooth is true
	LESS_THAN_1MB	Less than 1Mb.	
	ONE_MB_TO_TEN_MB	1-10Mb.	
	TEN_MB_TO_100_MB	10-100Mb.	
	GREATER_THAN_100MB	More than 100Mb.	
	UNKNOWN	Defer this optimization.	
	OTHER	Sizes that straddle these ranges.	

contentCharacteristicsWsdVod

- **Property Manager name:** [Content Characteristics - Streaming Video On-demand](#)
- **Behavior version:** The `v2018-09-12` rule format supports the `contentCharacteristicsWsdVod` behavior v1.0.
- **Rule format status:** [Deprecated, outdated rule format](#)
- **Access:** [Read-write](#)

Specifies characteristics of the delivered content, specifically targeted to delivering on-demand video. Akamai uses this information to optimize your metadata configuration, which may result in better origin offload and end-user performance.

Along with other behaviors whose names are prefixed *contentCharacteristics*, this behavior is customized for a specific product set. Use PAPI's [List available behaviors](#) operation to determine the set available to you. See also the related [clientCharacteristics](#) and [originCharacteristics](#) behaviors.

Option	Type	Description	Requires
catalogSize	enum	Optimize based on the total size of the content library delivered.	
	SMALL	Less than 100Gb.	
	MEDIUM	100Gb-1Tb.	
	LARGE	1-100Tb.	
	EXTRA_LARGE	More than 100Tb.	
	UNKNOWN	Defer this optimization.	
contentType	enum	Optimize based on the quality of media content.	
	SD	Standard definition.	
	HD	High definition.	
	ULTRA_HD	Ultra high definition.	
	OTHER	More than one level of quality.	
	UNKNOWN	Defer this optimization.	
popularity Distribution	enum	Optimize based on the content's expected popularity.	
	LONG_TAIL	A low volume of requests over a long period.	
	ALL_POPULAR	A high volume of requests over a short period.	
	UNKNOWN	Defer this optimization.	
hls	boolean	Enable delivery of HLS media.	
segmentDuration HLS	enum	Specifies the duration of individual segments.	hls is true
	SEGMENT_DURATION_2S	2 seconds.	
	SEGMENT_DURATION_4S	4 seconds.	
	SEGMENT_DURATION_6S	6 seconds.	
	SEGMENT_DURATION_8S	8 seconds.	
	SEGMENT_DURATION_10S	10 seconds.	
segmentSizeHLS	enum	Specifies the size of the media object retrieved from the origin.	hls is true
	LESS_THAN_1MB	Less than 1Mb.	
	ONE_MB_TO_TEN_MB	1-10Mb.	

Option	Type	Description	Requires
	TEN_MB_TO_100_MB	10-100Mb.	
	GREATER_THAN_100MB	More than 100Mb.	
	UNKNOWN	Defer this optimization.	
	OTHER	Sizes straddle these ranges.	
hds	boolean	Enable delivery of HDS media.	
segmentDuration HDS	enum	Specifies the duration of individual fragments.	hds is true
	SEGMENT_DURATION_2S	2 seconds.	
	SEGMENT_DURATION_4S	4 seconds.	
	SEGMENT_DURATION_6S	6 seconds.	
	SEGMENT_DURATION_8S	8 seconds.	
	SEGMENT_DURATION_10S	10 seconds.	
segmentSizeHDS	enum	Specifies the size of the media object retrieved from the origin.	hds is true
	LESS_THAN_1MB	Less than 1Mb.	
	ONE_MB_TO_TEN_MB	1-10Mb.	
	TEN_MB_TO_100_MB	10-100Mb.	
	GREATER_THAN_100MB	More than 100Mb.	
	UNKNOWN	Defer this optimization.	
	OTHER	Sizes straddle these ranges.	
dash	boolean	Enable delivery of DASH media.	
segmentDuration DASH	enum	Specifies the duration of individual segments.	dash is true
	SEGMENT_DURATION_2S	2 seconds.	
	SEGMENT_DURATION_4S	4 seconds.	
	SEGMENT_DURATION_6S	6 seconds.	
	SEGMENT_DURATION_8S	8 seconds.	
	SEGMENT_DURATION_10S	10 seconds.	
segmentSizeDASH	enum	Specifies the size of the media object retrieved from the origin.	dash is true
	LESS_THAN_1MB	Less than 1Mb.	
	ONE_MB_TO_TEN_MB	1-10Mb.	

Option	Type	Description	Requires
	TEN_MB_TO_100_MB	10-100Mb.	
	GREATER_THAN_100MB	More than 100Mb.	
	UNKNOWN	Defer this optimization.	
	OTHER	Values straddle these ranges.	
smooth	boolean	Enable delivery of Smooth media.	
segmentDuration Smooth	enum	Specifies the duration of individual fragments.	smooth is true
	SEGMENT_DURATION_2S	2 seconds.	
	SEGMENT_DURATION_4S	4 seconds.	
	SEGMENT_DURATION_6S	6 seconds.	
	SEGMENT_DURATION_8S	8 seconds.	
	SEGMENT_DURATION_10S	10 seconds.	
segmentSize Smooth	enum	Specifies the size of the media object retrieved from the origin.	smooth is true
	LESS_THAN_1MB	Less than 1Mb.	
	ONE_MB_TO_TEN_MB	1-10Mb.	
	TEN_MB_TO_100_MB	10-100Mb.	
	GREATER_THAN_100MB	More than 100Mb.	
	UNKNOWN	Defer this optimization.	
	OTHER	Sizes straddle these ranges.	

contentTargetingProtection

- **Property Manager name:** [Content Targeting - Protection](#)
- **Behavior version:** The v2018-09-12 rule format supports the contentTargetingProtection behavior v1.1.
- **Rule format status:** [Deprecated, outdated rule format](#)
- **Access:** [Read-write](#)

Content Targeting is based on [EdgeScape](#), Akamai's location-based access control system. You can use it to allow or deny access to a set of geographic regions or IP addresses.

Option	Type	Description	Requires
--------	------	-------------	--------------------------

Option	Type	Description	Requires
enabled	boolean	Enables the Content Targeting feature.	
enableGeoProtection	boolean	When enabled, verifies IP addresses are unique to specific geographic regions.	
geoProtectionMode	enum	Specifies how to handle requests.	enableGeoProtection is true
	ALLOW	Allow requests.	
	DENY	Deny requests.	
countries	string array	Specifies a set of two-character ISO 3166 country codes from which to allow or deny traffic. See EdgeScape Data Codes for a list.	enableGeoProtection is true
regions	string array	Specifies a set of ISO 3166-2 regional codes from which to allow or deny traffic. See EdgeScape Data Codes for a list.	enableGeoProtection is true
dmaz	string array	Specifies the set of Designated Market Area codes from which to allow or deny traffic. See EdgeScape Data Codes for a list.	enableGeoProtection is true
overrideIPAddresses	string array	Specify a set of IP addresses or CIDR blocks that exceptions to the set of included or excluded areas.	enableGeoProtection is true
enableGeoRedirectOnDeny	boolean	When enabled, redirects denied requests rather than responding with an error code.	enableGeoProtection is true
geoRedirectUrl	string	This specifies the full URL to the redirect page for denied requests.	enableGeoRedirectOnDeny is true
enableIPProtection	boolean	Allows you to control access to your content from specific sets of IP addresses and CIDR blocks.	
ipProtectionMode	enum	Specifies how to handle requests.	enableIPProtection is true
	ALLOW	Allow requests.	
	DENY	Deny requests.	
ipAddresses	string array	Specify a set of IP addresses or CIDR blocks to allow or deny.	enableIPProtection is true
enableIPRedirectOnDeny	boolean	When enabled, redirects denied requests rather than responding with an error code.	enableIPProtection is true
ipRedirectUrl	string	This specifies the full URL to the redirect page for denied requests.	enableIPRedirectOnDeny is true
enableReferrerProtection	boolean	Allows you allow traffic from certain referring websites, and disallow traffic from unauthorized sites that hijack those links.	
referrerProtectionMode	enum	Specify the action to take.	enableReferrerProtection is true
	ALLOW	Allow requests.	
	DENY	Deny requests.	
referrerDomains	string array	Specifies the set of domains from which to allow or deny traffic.	enableReferrerProtection is true

Option	Type	Description	Requires
enableReferrerRedirectOnDeny	boolean	When enabled, redirects denied requests rather than responding with an error code.	enableReferrerProtection is true
referrerRedirectUrl	string	This specifies the full URL to the redirect page for denied requests.	enableReferrerRedirectOnDeny is true

cpCode

- **Property Manager name:** [Content Provider Code](#)^{*)}
- **Behavior version:** The v2018-09-12 rule format supports the cpCode behavior v1.1.
- **Rule format status:** [Deprecated, outdated rule format](#)
- **Access:** [Read-write](#)

Content Provider Codes (CP codes) allow you to distinguish various reporting and billing segments. You receive a CP code when purchasing Akamai service, and you need it to access properties. This behavior allows you to apply any valid CP code, including additional ones you may request from Akamai Professional Services. For a CP code to be valid, it needs to belong to the same contract and be associated with the same product as the property, and the group needs access to it.

Option	Type	Description
value	object	Specifies a value object, which includes an id key and a descriptive name .
value.description	string	Additional description for the CP code.
value.id	integer	Unique identifier for each CP code.
value.name	string	The name of the CP code.
value.products	array	The set of products the CP code is assigned to.

customBehavior

- **Property Manager name:** [Custom Behavior](#)^{*)}
- **Behavior version:** The v2018-09-12 rule format supports the customBehavior behavior v1.0.
- **Rule format status:** [Deprecated, outdated rule format](#)
- **Access:** [Read-write](#)

Allows you to insert a customized XML metadata behavior into any property's rule tree. Talk to your Akamai representative to implement the customized behavior. Once it's ready, run PAPI's

[List custom behaviors](#) operation, then apply the relevant `behaviorId` value from the response within the current `customBehavior`. See [Custom behaviors and overrides](#) for guidance on custom metadata behaviors.

Option	Type	Description
<code>behaviorId</code>	string	The unique identifier for the predefined custom behavior you want to insert into the current rule.

datastream

- **Property Manager name:** [DataStream](#)
- **Behavior version:** The `v2018-09-12` rule format supports the `datastream` behavior v1.2.
- **Rule format status:** [Deprecated, outdated rule format](#)
- **Access:** [Read-write](#)

The [DataStream](#) reporting service provides real-time logs on application activity, including aggregated metrics on complete request and response cycles and origin response times. Apply this behavior to report on this set of traffic. Use the [DataStream API](#) to aggregate the data.

Option	Type	Description
<code>enabled</code>	boolean	Enables DataStream reporting.

dcp

- **Property Manager name:** [IoT Edge Connect](#)
- **Behavior version:** The `v2018-09-12` rule format supports the `dcp` behavior v1.0.
- **Rule format status:** [Deprecated, outdated rule format](#)
- **Access:** [Read-write](#)

The [Internet of Things: Edge Connect](#) product allows connected users and devices to communicate on a publish-subscribe basis within reserved namespaces. (The [IoT Edge Connect API](#) allows programmatic access.) This behavior allows you to select previously reserved namespaces and set the protocols for users to publish and receive messages within these namespaces. Use the [verifyJsonWebTokenForDcp](#) behavior to control access.

Option	Type	Description
<code>enabled</code>	boolean	Enables IoT Edge Connect.

Option	Type	Description
namespace id	string	Specifies the globally reserved name for a specific configuration. It includes authorization rules over publishing and subscribing to logical categories known as <i>topics</i> . This provides a root path for all topics defined within a namespace configuration. You can use the IoT Edge Connect API to configure access control lists for your namespace configuration.
tlsenabled	boolean	When enabled, you can publish and receive messages over a secured MQTT connection on port 8883.
wsenabled	boolean	When enabled, you can publish and receive messages through a secured MQTT connection over WebSockets on port 443.
gwenabled	boolean	When enabled, you can publish and receive messages over a secured HTTP connection on port 443.
anonymous	boolean	When enabled, you don't need to pass the JWT token with the mqtt request, and JWT validation is skipped.

dcpAuthHMACTransformation

- **Property Manager name:** [Variable Hash Transformation](#)
- **Behavior version:** The v2018-09-12 rule format supports the dcpAuthHMACTransformation behavior v1.0.
- **Rule format status:** [Deprecated, outdated rule format](#)
- **Access:** [Read-write](#)

The [Internet of Things: Edge Connect](#) product allows connected users and devices to communicate on a publish-subscribe basis within reserved namespaces. In conjunction with [dcpAuthVariableExtractor](#), this behavior affects how clients can authenticate themselves to edge servers, and which groups within namespaces are authorized to access topics. It transforms a source string value extracted from the client certificate and stored as a variable, then generates a hash value based on the selected algorithm, for use in authenticating the client request.

Note that you can apply this hash transformation, or either of the [dcpAuthRegexTransformation](#) or [dcpAuthSubstringTransformation](#) behaviors.

Option	Type	Description
hashConversion Algorithm	enum	Specifies the hash algorithm.
	SHA256	Use SHA-256.
	MD5	Use MD5.
	SHA384	Use SHA-384.
hashConversionKey	string	Specifies the key to generate the hash, ideally a long random string to ensure adequate security.

dcpAuthRegexTransformation

- **Property Manager name:** [Variable Regex Transformation](#)
- **Behavior version:** The v2018-09-12 rule format supports the dcpAuthRegexTransformation behavior v1.0.
- **Rule format status:** [Deprecated, outdated rule format](#)
- **Access:** [Read-write](#)

The [Internet of Things: Edge Connect](#) product allows connected users and devices to communicate on a publish-subscribe basis within reserved namespaces. In conjunction with [dcpAuthVariableExtractor](#), this behavior affects how clients can authenticate themselves to edge servers, and which groups within namespaces are authorized to access topics. It transforms a source string value extracted from the client certificate and stored as a variable, then transforms the string based on a regular expression search pattern, for use in authenticating the client request.

Note that you can apply this regular expression transformation, or either of the [dcpAuthHMACTransformation](#) or [dcpAuthSubstringTransformation](#) behaviors.

Option	Type	Description
regex Pattern	string	Specifies a Perl-compatible regular expression with a single grouping to capture the text. For example, a value of <code>^(.{0,10})</code> omits the first character, but then captures up to 10 characters after that. If the regular expression does not capture a substring, authentication may fail.

dcpAuthSubstringTransformation

- **Property Manager name:** [Variable Substring Transformation](#)
- **Behavior version:** The v2018-09-12 rule format supports the dcpAuthSubstringTransformation behavior v1.0.
- **Rule format status:** [Deprecated, outdated rule format](#)
- **Access:** [Read-write](#)


The [Internet of Things: Edge Connect](#) product allows connected users and devices to communicate on a publish-subscribe basis within reserved namespaces. In conjunction with [dcpAuthVariableExtractor](#), this behavior affects how clients can authenticate themselves to edge servers, and which groups within namespaces are authorized to access topics. It transforms a source string value extracted from the client certificate and stored as a variable, then extracts a substring, for use in authenticating the client request.


Note that you can apply this substring transformation, or either of the [dcpAuthHMACTransformation](#) or [dcpAuthRegexTransformation](#) behaviors.

Option	Type	Description
substring Start	string	The zero-based index offset of the first character to extract. If the index is out of bound from the string's length, authentication may fail.

Option	Type	Description
substring End	string	The zero-based index offset of the last character to extract, where -1 selects the remainder of the string. If the index is out of bound from the string's length, authentication may fail.

dcpAuthVariableExtractor

- **Property Manager name:** [Mutual Authentication](#) 
- **Behavior version:** The v2018-09-12 rule format supports the dcpAuthVariableExtractor behavior v1.0.
- **Rule format status:** [Deprecated, outdated rule format](#)
- **Access:** [Read-write](#)

The [Internet of Things: Edge Connect](#)  product allows connected users and devices to communicate on a publish-subscribe basis within reserved namespaces. This behavior affects how clients can authenticate themselves to edge servers, and which groups within namespaces are authorized to access topics. When enabled, this behavior allows end users to authenticate their requests with valid x509 client certificates. Either a client identifier or access authorization groups are required to make the request valid.

The behavior extracts the value from the specified field in the client certificate and stores it as a variable for a client identifier or access authorization groups. You can then apply any of these behaviors to transform the value: [dcpAuthHMACTransformation](#) , [dcpAuthRegexTransformation](#) , or [dcpAuthSubstringTransformation](#) .

Option	Type	Description
certificateField	enum	Specifies the field in the client certificate to extract the variable from.
	SUBJECT_DN	Subject distinguished name.
	V3_SUBJECT_ALT_NAME	Subject alternative name.
	SERIAL	Serial number.
	FINGERPRINT_DYN	The fingerprint hashed based on the algorithm that was used to generate the signature in the certificate.
	FINGERPRINT_MD5	Fingerprint MD5.
	FINGERPRINT_SHA1	Fingerprint SHA1.
	V3_NETSCAPE_COMMENT	An X.509 v3 certificate extension used to include comments inside certificates.
dcpMutualAuth ProcessingVariableId	enum	Where to store the value.
	VAR_DCP_CLIENT_ID	Variable for the client ID.
	VAR_DCP_AUTH_GROUP	Variable for the access authorization groups.

dcpDefaultAuthzGroups

- **Property Manager name:** [Default Authorization Groups](#) [↗]
- **Behavior version:** The `v2018-09-12` rule format supports the `dcpDefaultAuthzGroups` behavior v1.0.
- **Rule format status:** [Deprecated, outdated rule format](#)
- **Access:** [Read-write](#)

The [Internet of Things: Edge Connect](#) [↗] product allows connected users and devices to communicate on a publish-subscribe basis within reserved namespaces. This behavior defines a set of default authorization groups to add to each request the property configuration controls. These groups have access regardless of the authentication method you use, either JWT using the [verifyJsonWebTokenForDcp](#) behavior, or mutual authentication using the [dcpAuthVariableExtractor](#) behavior to control where authorization groups are extracted from within certificates.

Option	Type	Description
<code>groupNames</code>	string array	Specifies the set of authorization groups to assign to all connecting devices.

deliveryReceipt

- **Property Manager name:** [Cloud Monitor Data Delivery](#) [↗]
- **Behavior version:** The `v2018-09-12` rule format supports the `deliveryReceipt` behavior v1.1.
- **Rule format status:** [Deprecated, outdated rule format](#)
- **Access:** [Read-write](#)

A static behavior that's required when specifying the Cloud Monitor module's ([edgeConnect](#)) behavior. You can only apply this behavior if the property is marked as secure. See [Secure property requirements](#) for guidance.

This behavior object does not support any options. Specifying the behavior enables it.

denyDirectFailoverAccess

- **Property Manager name:** [Security Failover Protection](#) [↗]

- **Behavior version:** The `v2018-09-12` rule format supports the `denyDirectFailoverAccess` behavior v1.0.
- **Rule format status:** [Deprecated, outdated rule format](#)
- **Access:** [Read-write](#)

A static behavior required for all properties that implement a failover under the Cloud Security Failover product.

This behavior object does not support any options. Specifying the behavior enables it.

denyAccess

- **Property Manager name:** [Control Access](#)
- **Behavior version:** The `v2018-09-12` rule format supports the `denyAccess` behavior v1.2.
- **Rule format status:** [Deprecated, outdated rule format](#)
- **Access:** [Read-write](#)

Assuming a condition in the rule matches, this denies access to the requested content. For example, a `userLocation` match paired with the `denyaccess` behavior would deny requests from a specified part of the world.

By keying on the value of the `reason` option, `denyaccess` behaviors may override each other when called from nested rules. For example, a parent rule might deny access to a certain geographic area, citing "location" as the `reason`, but another nested rule can then allow access for a set of IPs within that area, so long as the `reason` matches.

Option	Type	Description
<code>reason</code>	string	Text message that keys why access is denied. Any subsequent <code>denyaccess</code> behaviors within the rule tree may refer to the same <code>reason</code> key to override the current behavior.
<code>enabled</code>	boolean	Denies access when enabled.

deviceCharacteristicCached

- **Property Manager name:** [Device Characterization - Define Cached Content](#)
- **Behavior version:** The `v2018-09-12` rule format supports the `deviceCharacteristicCached` behavior v1.3.
- **Rule format status:** [Deprecated, outdated rule format](#)
- **Access:** [Read-write](#)

By default, source URLs serve as cache IDs on edge servers. Electronic Data Capture allows you to specify an additional set of device characteristics to generate separate cache keys. Use this in conjunction with the [deviceCharacteristicHeader](#) behavior.

Option	Type	Description
elements	string array	Specifies a set of information about the device with which to generate a separate cache key.
		Supported values: <div><div>ACCEPT_THIRD_PARTY_COOKIE AJAX_PREFERRED_GEOLOC_API AJAX_SUPPORT_JAVASCRIPT BRAND_NAME COOKIE_SUPPORT DEVICE_OS DEVICE_OS_VERSION DUAL_ORIENTATION FLASH_LITE_VERSION FULL_FLASH_SUPPORT GIF_ANIMATED HTML_PREFERRED_DTD IS_MOBILE IS_TABLET IS_WIRELESS_DEVICE JPG MARKETING_NAME</div><div>MAX_IMAGE_HEIGHT MAX_IMAGE_WIDTH MOBILE_BROWSER MOBILE_BROWSER_VERSION MODEL_NAME PDF_SUPPORT PHYSICAL_SCREEN_HEIGHT PHYSICAL_SCREEN_WIDTH PNG PREFERRED_MARKUP RESOLUTION_HEIGHT RESOLUTION_WIDTH VIEWPORT_INITIAL_SCALE VIEWPORT_WIDTH XHTMLMP_PREFERRED_MIME_TYPE XHTML_FILE_UPLOAD XHTML_PREFERRED_CHARSET</div></div>

Notice

Akamai secures and delivers digital experiences for the world's largest companies. Akamai's Intelligent Edge Platform surrounds everything, from the enterprise to the cloud, so customers and their businesses can be fast, smart, and secure. Top brands globally rely on Akamai to help them realize competitive advantage through agile solutions that extend the power of their multi-cloud architectures. Akamai keeps decisions, apps, and experiences closer to users than anyone — and attacks and threats far away. Akamai's portfolio of edge security, web and mobile performance, enterprise access, and video delivery solutions is supported by unmatched customer service, analytics, and 24/7/365 monitoring. To learn why the world's top brands trust Akamai, visit www.akamai.com, blogs.akamai.com, or [@Akamai](https://twitter.com/Akamai) on Twitter. You can find our global contact information at www.akamai.com/locations.

Akamai is headquartered in Cambridge, Massachusetts in the United States with operations in more than 57 offices around the world. Our services and renowned customer care are designed to enable businesses to provide an unparalleled Internet experience for their customers worldwide. Addresses, phone numbers, and contact information for all locations are listed on www.akamai.com/locations.

© 2022 Akamai Technologies, Inc. All Rights Reserved. No part of this publication may be reproduced, transmitted, transcribed, stored in a retrieval system or translated into any language in any form by any means without the written permission of Akamai Technologies, Inc. While precaution has been taken in the preparation of this document, Akamai Technologies, Inc. assumes no responsibility for errors, omissions, or for damages resulting from the use of the information herein. The information in this document is subject to change without notice. Without limitation of the foregoing, if this document discusses a product or feature in beta or limited availability, such information is provided with no representation or guarantee as to the matters discussed, as such products/features may have bugs or other issues.

Akamai and the Akamai wave logo are registered trademarks or service marks in the United States (Reg. U.S. Pat. & Tm. Off). Akamai Intelligent Edge Platform is a trademark in the United States. Products or corporate names may be trademarks or registered trademarks of other companies and are used only for explanation and to the owner's benefit, without intent to infringe.

Published December 21, 2022