



v2018-02-27 Property Manager Deprecated Rule Formats

January 4, 2023

Contents

Welcome

[Welcome](#)

PAPI conventions

[API versioning](#)

[Advanced and locked features](#)

v2018-02-27 behaviors

[v2018-02-27 behaviors](#)

[adScalerCircuitBreaker](#)

[adaptiveImageCompression](#)

[adaptiveAcceleration](#)

[advanced](#)

[aggregatedReporting](#)

[akamaizer](#)

[akamaizerTag](#)

[allHttpInCacheHierarchy](#)

[allowCloudletsOrigins](#)

[allowDelete](#)

[allowHTTPSCacheKeySharing](#)

[allowHTTPSDowngrade](#)

[allowOptions](#)

[allowPatch](#)

[allowPost](#)

[allowPut](#)

[allowTransferEncoding](#)

[apiPrioritization](#)

[applicationLoadBalancer](#)

[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
deliveryReceipt
dcpDefaultAuthzGroups
denyAccess
denyDirectFailoverAccess
deviceCharacteristicCacheId
deviceCharacteristicHeader
dnsAsyncRefresh
dnsPrefresh
downgradeProtocol
downloadCompleteMarker
downloadNotification
downstreamCache
dynamicWebContent
edgeConnect
edgeImageConversion
edgeLoadBalancingAdvanced
edgeLoadBalancingDataCenter
edgeLoadBalancingOrigin
edgeOriginAuthorization
edgeRedirector
edgeScape
enhancedAkamaiProtocol
edgeSideIncludes
failAction
fastInvalidate
firstPartyMarketing
firstPartyMarketingPlus
forwardRewrite
frontEndOptimization
g2oheader
gzipResponse
hdDataAdvanced
http2
healthDetection
httpStrictTransportSecurity
imOverride
injectReferenceld
imageManager
inputValidation

instant
instantConfig
largeFileOptimization
largeFileOptimizationAdvanced
limitBitRate
mPulse
manifestRerouting
manualServerPush
mediaAccelerationQuicOptout
mediaAcceleration
mediaClient
mediaFileRetrievalOptimization
mediaOriginFailover
mobileSdkPerformance
modifyIncomingRequestHeader
modifyIncomingResponseHeader
modifyOutgoingRequestHeader
modifyOutgoingResponseHeader
netSession
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
restrictObjectCaching
responseCode
responseCookie
rmaOptimization
rewriteUrl

rumCustom
saasDefinitions
salesForceCommerceCloudClient
salesForceCommerceCloudProvider
savePostDcaProcessing
scheduleInvalidation
scriptManagement
segmentedContentProtection
shutr
segmentedMediaOptimization
setVariable
simulateErrorCode
siteShield
standardTLMigrationOverride
standardTLMigration
subCustomer
tcpOptimization
sureRoute
teaLeaf
tieredDistribution
tieredDistributionAdvanced
timeout
uidConfiguration
validateEntityTag
verifyJsonWebToken
verifyJsonWebTokenForDcp
verifyTokenAuthorization
visitorPrioritization
watermarkUrl
webApplicationFirewall
webSockets
webdav

v2018-02-27 criteria

v2018-02-27 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

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 v2018-02-27 **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.

v2018-02-27 behaviors

v2018-02-27 behaviors

This section provides details for all behaviors the Property Manager API supports for the v2018-02-27 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 v2018-02-27 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 v2018-02-27 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
response DelayBased	boolean	Triggers a fallback action based on the delayed response from the technology partner's server.	
response Delay Threshold	enum	Specifies the maximum response delay that, if exceeded, triggers the fallback action.	responseDelay Based is true
		Supported values: 500ms	
response CodeBased	boolean	Triggers a fallback action based on the response code from the technology partner's server.	
response Codes	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.	responseCode Based is true
fallback Action Response CodeBased	enum	Specifies the fallback action.	responseDelay Based is true OR responseCode Based is true
	RETURN_AKAMAI_COPY	Return an unmodified Akamai copy of the manifest file to the requesting client.	
	RETURN_ERROR	Return an error as the server response.	
returnError Response CodeBased	enum	Specifies the error to include in the response to the client.	fallbackAction ResponseCode Based is RETURN_ERROR
	SAME_AS_RECEIEVED	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.	
	SPECIFY_YOUR_OWN	Customize the error.	
specifyYour Own Response CodeBased	string	Defines a custom error response.	returnError ResponseCode Based is SPECIFY_YOUR_OWN

adaptiveImageCompression

- **Property Manager name:** [Adaptive Image Compression](#) ^{*)}
- **Behavior version:** The v2018-02-27 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`, `jiff`, 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 v2018-02-27 rule format supports the adaptiveAcceleration behavior v1.4.
- **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
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 v2018-02-27 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
description	string	Human-readable description of what the XML block does.
xml	string	Akamai XML metadata.


aggregatedReporting

- **Property Manager name:** [Aggregated Reporting](#)
- **Behavior version:** The v2018-02-27 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
enabled	boolean	Enables aggregated reporting.	
report Name	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.	
attributes Count	number (1-4)	Select the number of attributes by which your report is grouped. You can add up to four attributes.	
attribute1	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.	
attribute2	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 \geq 2
attribute3	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 \geq 3
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 `v2018-02-27` 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
<code>enabled</code>	boolean	Enables the Akamaizer behavior.

akamaizerTag

- **Property Manager name:** [Akamaize Tag](#) 
- **Behavior version:** The `v2018-02-27` 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
<code>match</code> Hostname	string	Specifies the hostname to match on as a Perl-compatible regular expression.	
<code>replacement</code> Hostname	string	Specifies the replacement hostname for the tag to use.	
<code>scope</code>	enum	Specifies the part of HTML content the <code>tagsAttribute</code> refers to.	
	ATTRIBUTE	When <code>tagsAttribute</code> 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.	
	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.	
<code>tags</code> Attribute	enum	Specifies the tag or tag/attribute combination to operate on.	<code>scope</code> is not <code>PAGE</code>

Option	Type	Description	Requires															
		<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.																
<code>includeTagsAttribute</code>	boolean	Whether to include the <code>tagsAttribute</code> value.																

allHttpInCacheHierarchy

- **Property Manager name:** [Allow All Methods on Parent Servers](#) [¶]
- **Behavior version:** The `v2018-02-27` 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 `v2018-02-27` 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 [cloudletsOrigin](#) criteria within sub-rules to override the prevailing origin.

Option	Type	Description
<code>enabled</code>	boolean	Allows you to assign custom origin definitions referenced in sub-rules by cloudletsOrigin labels. If disabled, all sub-rules are ignored.
<code>honor Base Directory</code>	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.
<code>purge Origin Query Parameter</code>	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 `v2018-02-27` rule format supports the `allowDelete` behavior v1.1.
- **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
<code>enabled</code>	boolean	Allows DELETE requests. Content does <i>not</i> cache.

allowHTTPSCacheKeySharing

- **Property Manager name:** [HTTPS Cache Key Sharing](#)
- **Behavior version:** The `v2018-02-27` 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 v2018-02-27 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
enabled	boolean	Downgrades to HTTP protocol for the origin server.

allowOptions

- **Property Manager name:** [Allow OPTIONS](#) [↗]
- **Behavior version:** The v2018-02-27 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
enabled	boolean	Allows OPTIONS requests. Content does <i>not</i> cache.

allowPatch

- **Property Manager name:** [Allow PATCH](#) [↗]
- **Behavior version:** The v2018-02-27 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 v2018-02-27 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 <code>Content-Length</code> header, or they result in a 411 error. With this option enabled with no specified <code>Content-Length</code> , the edge server relies on a <code>Transfer-Encoding</code> header to chunk the data. If neither header is present, it assumes the request has no body, and it adds a header with a <code>0</code> value to the forward request.

allowPut

- **Property Manager name:** [Allow PUT](#)*
- **Behavior version:** The v2018-02-27 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 v2018-02-27 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 v2018-02-27 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.	

Option	Type	Description	Requires
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 v2018-02-27 rule format supports the applicationLoadBalancer behavior v1.8.
- **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
enabled	boolean	Activates the Application Load Balancer Cloudlet.	
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 Application Load Balancer policy from any others within the same property.	
stickinessCookieType	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.	
stickinessExpirationDate	string (epoch timestamp)	Specifies when the cookie expires.	stickinessCookieType is FIXED_DATE
stickinessDuration	string (duration)	Sets how long it is before the cookie expires.	stickinessCookieType is DURATION
stickinessRefresh	boolean	Extends the duration of the cookie with each new request. When enabled, the DURATION thus specifies the latency between requests that would cause the cookie to expire.	stickinessCookieType is DURATION
specifyStickinessCookieDomain	boolean	Specifies whether to use a cookie domain with the stickiness cookie, to tell the browser to which domain to send the cookie.	stickinessCookieType is either: ON_BROWSER_CLOSE , FIXED_DATE , DURATION , NEVER
stickinessCookieDomain	string	Specifies the domain to track the stickiness cookie.	specifyStickinessCookieDomain is true
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
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

Option	Type	Description	Requires
stickinessCookie SetSecureFlag	boolean	Deploys the stickiness cookie as secure.	stickinessCookieType is either: ON_ BROWSER_CLOSE , FIXED_DATE , DURATION , NEVER
allDownNet Storage	object	Specifies a NetStorage account for a static maintenance page as a fallback when no origins are available.	
allDownNet Storage.cpCode List	array	A set of CP codes that apply to this storage group.	
allDownNet Storage.download DomainName	string	Domain name from which content can be downloaded.	
allDownNet Storage.id	number	Unique identifier for the storage group.	
allDownNet Storage.name	string	Name of the storage group.	
allDownNet Storage.upload DomainName	string	Domain name used to upload content.	
allDownNet StorageFile	string	Specifies the fallback maintenance page's filename, expressed as a full path from the root of the NetStorage server.	
allDownStatus Code	string	Specifies the HTTP response code when all load- balancing origins are unavailable.	
failoverStatus Codes	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.	
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.	
allowCache Prefresh	boolean	Allows the cache to prefetch. Only appropriate if all origins serve the same content for the same URL.	
failoverAttempts Threshold	number	Sets the number of failed requests that would trigger the failover process.	enableAdvanced Options is true

Option	Type	Description	Requires
originCookie Name	string	Specifies the name for your session cookie.	enableSession Synchronization is true

audienceSegmentation


- **Property Manager name:** [Audience Segmentation Cloudlet](#)
- **Behavior version:** The v2018-02-27 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: IN_COOKIE_HEADER	
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.	

Option	Type	Description	Requires
	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 PopulationCookie Domain 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.	
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 v2018-02-27 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
--------	------	-------------

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 v2018-02-27 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.
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.

Option	Type	Description
	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 <code>*CONNECT* *DENIED*</code> .

breakConnection

- **Property Manager name:** [Break Forward Connection](#) [↗]
- **Behavior version:** The `v2018-02-27` 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
enabled	boolean	Enables the break connection behavior.

brrotli

- **Property Manager name:** [Brotli Support](#) [↗]
- **Behavior version:** The `v2018-02-27` rule format supports the `brrotli` 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
enabled	boolean	Enables Brotli compression.

cacheError

- **Property Manager name:** [Cache HTTP Error Responses](#)
- **Behavior version:** The v2018-02-27 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
enabled	boolean	Activates the error-caching behavior.
ttl	string (duration)	Overrides the default caching duration of 10s . Note that if set to 0 , it is equivalent to no-cache , which forces revalidation and may cause a traffic spike. This can be counterproductive when, for example, the origin is producing an error code of 500 .
preserve Stale	boolean	When enabled, the edge server preserves stale cached objects when the origin returns 400 , 500 , 502 , 503 , and 504 error codes. This avoids re-fetching and re-caching content after transient errors.

cacheld

- **Property Manager name:** [Cache ID Modification](#)
- **Behavior version:** The v2018-02-27 rule format supports the `cacheld` 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 `cache id` behaviors within the same rule results in a system of forming cache keys that applies independently to the rule's content. If any `cacheld` 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 `cacheld` 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.	

Option	Type	Description	Requires
	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 <code>cacheid</code> 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
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 `v2018-02-27` 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
enabled	boolean	Ignores case when forming cache keys.

cacheKeyQueryParams

- **Property Manager name:** [Cache Key Query Parameters](#)
- **Behavior version:** The v2018-02-27 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 v2018-02-27 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 v2018-02-27 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 `v2018-02-27` 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
<code>enabled</code>	boolean	Enables the redirect caching behavior.

caching

- **Property Manager name:** [Caching](#)
- **Behavior version:** The `v2018-02-27` 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
<code>behavior</code>	enum	Specify the caching option.	
	<code>MAX_AGE</code>	Honor the origin's <code>MAX_AGE</code> header.	
	<code>NO_STORE</code>	Clears the cache and serves from the origin.	
	<code>BYPASS_CACHE</code>	Retains the cache but serves from the origin.	
	<code>CACHE_CONTROL_AND_EXPIRES</code>	Honor the origin's <code>CACHE_CONTROL</code> or <code>EXPIRES</code> header, whichever comes last. This adds support for the <code>s-maxage</code> response directive specified in RFC 7234 . Use this alternative value to instruct a downstream CDN how long to cache content.	
	<code>CACHE_CONTROL</code>	Honor the origin's <code>CACHE_CONTROL</code> header. This adds support for the <code>s-maxage</code> response directive specified in RFC 7234 . Use this alternative value to instruct a downstream CDN how long to cache content.	
	<code>EXPIRES</code>	Honor the origin's <code>EXPIRES</code> header.	
<code>must Revalidate</code>	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.	<code>behavior</code> is either: <code>CACHE_CONTROL_AND_EXPIRES</code> , <code>CACHE_CONTROL</code> , <code>EXPIRES</code> , <code>MAX_AGE</code>

Option	Type	Description	Requires
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 v2018-02-27 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
enabled	boolean	Enables the centralized authorization behavior.

chaseRedirects


- **Property Manager name:** [Chase Redirects](#)
- **Behavior version:** The v2018-02-27 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
enabled	boolean	Allows edge servers to chase redirects.
limit	string	Specifies, as a string, the maximum number of redirects to follow.

Option	Type	Description
serve404	boolean	Once the redirect limit is reached, enabling this option serves an HTTP 404 (Not Found) error instead of the last redirect.

clientCharacteristics

- **Property Manager name:** [Client Characteristics](#) 
- **Behavior version:** The v2018-02-27 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 v2018-02-27 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
<code>enabled</code>	boolean	Serves the custom response.
<code>body</code>	string (allows variables)	HTML response of up to 2000 characters to send to the end-user client.
<code>response Code</code>	enum	The HTTP response code to send to the end-user client.
		Supported values: 200 401 403 404 405 417
<code>forceEviction</code>	boolean	Removes the underlying object from the cache, since it is not being served.

contentCharacteristics

- **Property Manager name:** [Content Characteristics](#)[¶]
- **Behavior version:** The v2018-02-27 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
<code>objectSize</code>	enum	Optimize based on the size of the object retrieved from the origin.
	LESS_THAN_1MB	Less than 1Mb.

Option	Type	Description
	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.
	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 v2018-02-27 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.	
	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.	

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.	
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.	
	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.	

Option	Type	Description	Requires
	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
	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 `v2018-02-27` 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.
	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.
contentType	enum	Optimize based on the type of content.
	VIDEO	Video.
	SOFTWARE	Software.
	SOFTWARE_PATCH	Software patch.
	GAME	Game.
	GAME_PATCH	Game patch.

Option	Type	Description
	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 v2018-02-27 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.

Option	Type	Description
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 v2018-02-27 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.	

Option	Type	Description	Requires
	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.	
	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.	

Option	Type	Description	Requires
	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.	
	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.	

Option	Type	Description	Requires
	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 v2018-02-27 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.	

Option	Type	Description	Requires
	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.	
	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.	

Option	Type	Description	Requires
	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.	
	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.	

Option	Type	Description	Requires
	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 v2018-02-27 rule format supports the contentTargetingProtection behavior v1.0.
- **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
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
dmas	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.	

Option	Type	Description	Requires
ipProtection Mode	enum	Specifies how to handle requests.	enable IPProtection is true
	ALLOW	Allow requests.	
	DENY	Deny requests.	
ipAddresses	string array	Specify a set of IP addresses or CIDR blocks to allow or deny.	enable IPProtection is true
enable IPRedirectOn Deny	boolean	When enabled, redirects denied requests rather than responding with an error code.	enable IPProtection is true
ipRedirectUrl	string	This specifies the full URL to the redirect page for denied requests.	enableIPRedirect OnDeny is true
enable Referrer Protection	boolean	Allows you allow traffic from certain referring websites, and disallow traffic from unauthorized sites that hijack those links.	
referrer Protection Mode	enum	Specify the action to take.	enableReferrer Protection is true
	ALLOW	Allow requests.	
	DENY	Deny requests.	
referrer Domains	string array	Specifies the set of domains from which to allow or deny traffic.	enableReferrer Protection is true
enable Referrer RedirectOn Deny	boolean	When enabled, redirects denied requests rather than responding with an error code.	enableReferrer Protection is true
referrer RedirectUrl	string	This specifies the full URL to the redirect page for denied requests.	enableReferrer RedirectOnDeny is true

cpCode

- **Property Manager name:** [Content Provider Code](#)^{*)}
- **Behavior version:** The v2018-02-27 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 <code>value</code> object, which includes an <code>id</code> key and a descriptive <code>name</code> .
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 `v2018-02-27` 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
behaviorId	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 `v2018-02-27` 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
enabled	boolean	Enables DataStream reporting.

dcp

- **Property Manager name:** [IoT Edge Connect](#)
- **Behavior version:** The v2018-02-27 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
enabled	boolean	Enables IoT Edge Connect.
namespaceId	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.

deliveryReceipt

- **Property Manager name:** [Cloud Monitor Data Delivery](#)
- **Behavior version:** The v2018-02-27 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.

dcpDefaultAuthzGroups

- **Property Manager name:** [Default Authorization Groups](#) [↗]
- **Behavior version:** The v2018-02-27 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
groupNames	string array	Specifies the set of authorization groups to assign to all connecting devices.

denyAccess

- **Property Manager name:** [Control Access](#) [↗]
- **Behavior version:** The v2018-02-27 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
reason	string	Text message that keys why access is denied. Any subsequent denyaccess behaviors within the rule tree may refer to the same reason key to override the current behavior.
enabled	boolean	Denies access when enabled.

denyDirectFailoverAccess

- **Property Manager name:** [Security Failover Protection](#)✎
- **Behavior version:** The `v2018-02-27` 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.

deviceCharacteristicCached

- **Property Manager name:** [Device Characterization - Define Cached Content](#)✎
- **Behavior version:** The `v2018-02-27` rule format supports the `deviceCharacteristicCached` behavior v1.2.
- **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: <table><tr><td>ACCEPT_THIRD_PARTY_COOKIE</td><td>MOBILE_BROWSER</td></tr><tr><td>AJAX_PREFERRED_GEOLOC_API</td><td>MOBILE_BROWSER_VERSION</td></tr><tr><td>AJAX_SUPPORT_JAVASCRIPT</td><td>MODEL_NAME</td></tr><tr><td>BRAND_NAME</td><td>PDF_SUPPORT</td></tr><tr><td>COOKIE_SUPPORT</td><td>PHYSICAL_SCREEN_HEIGHT</td></tr><tr><td>DEVICE_OS</td><td>PHYSICAL_SCREEN_WIDTH</td></tr><tr><td>DEVICE_OS_VERSION</td><td>PNG</td></tr><tr><td>DUAL_ORIENTATION</td><td>PREFERRED_MARKUP</td></tr><tr><td>FLASH_LITE_VERSION</td><td>RESOLUTION_HEIGHT</td></tr><tr><td>FULL_FLASH_SUPPORT</td><td>RESOLUTION_WIDTH</td></tr><tr><td>GIF_ANIMATED</td><td>VIEWPORT_INITIAL_SCALE</td></tr><tr><td>HTML_PREFERRED_DTD</td><td>VIEWPORT_WIDTH</td></tr><tr><td>IS_MOBILE</td><td>XHTMLMP_PREFERRED_MIME_TYPE</td></tr><tr><td>IS_TABLET</td><td>XHTML_FILE_UPLOAD</td></tr><tr><td>IS_WIRELESS_DEVICE</td><td>XHTML_PREFERRED_CHARSET</td></tr><tr><td>JPG</td><td>XHTML_SUPPORTS_IFRAME</td></tr><tr><td>MARKETING_NAME</td><td>XHTML_SUPPORTS_TABLE_FOR_LAYOUT</td></tr><tr><td>MAX_IMAGE_HEIGHT</td><td>XHTML_SUPPORT_LEVEL</td></tr><tr><td>MAX_IMAGE_WIDTH</td><td>XHTML_TABLE_SUPPORT</td></tr></table>	ACCEPT_THIRD_PARTY_COOKIE	MOBILE_BROWSER	AJAX_PREFERRED_GEOLOC_API	MOBILE_BROWSER_VERSION	AJAX_SUPPORT_JAVASCRIPT	MODEL_NAME	BRAND_NAME	PDF_SUPPORT	COOKIE_SUPPORT	PHYSICAL_SCREEN_HEIGHT	DEVICE_OS	PHYSICAL_SCREEN_WIDTH	DEVICE_OS_VERSION	PNG	DUAL_ORIENTATION	PREFERRED_MARKUP	FLASH_LITE_VERSION	RESOLUTION_HEIGHT	FULL_FLASH_SUPPORT	RESOLUTION_WIDTH	GIF_ANIMATED	VIEWPORT_INITIAL_SCALE	HTML_PREFERRED_DTD	VIEWPORT_WIDTH	IS_MOBILE	XHTMLMP_PREFERRED_MIME_TYPE	IS_TABLET	XHTML_FILE_UPLOAD	IS_WIRELESS_DEVICE	XHTML_PREFERRED_CHARSET	JPG	XHTML_SUPPORTS_IFRAME	MARKETING_NAME	XHTML_SUPPORTS_TABLE_FOR_LAYOUT	MAX_IMAGE_HEIGHT	XHTML_SUPPORT_LEVEL	MAX_IMAGE_WIDTH	XHTML_TABLE_SUPPORT
ACCEPT_THIRD_PARTY_COOKIE	MOBILE_BROWSER																																							
AJAX_PREFERRED_GEOLOC_API	MOBILE_BROWSER_VERSION																																							
AJAX_SUPPORT_JAVASCRIPT	MODEL_NAME																																							
BRAND_NAME	PDF_SUPPORT																																							
COOKIE_SUPPORT	PHYSICAL_SCREEN_HEIGHT																																							
DEVICE_OS	PHYSICAL_SCREEN_WIDTH																																							
DEVICE_OS_VERSION	PNG																																							
DUAL_ORIENTATION	PREFERRED_MARKUP																																							
FLASH_LITE_VERSION	RESOLUTION_HEIGHT																																							
FULL_FLASH_SUPPORT	RESOLUTION_WIDTH																																							
GIF_ANIMATED	VIEWPORT_INITIAL_SCALE																																							
HTML_PREFERRED_DTD	VIEWPORT_WIDTH																																							
IS_MOBILE	XHTMLMP_PREFERRED_MIME_TYPE																																							
IS_TABLET	XHTML_FILE_UPLOAD																																							
IS_WIRELESS_DEVICE	XHTML_PREFERRED_CHARSET																																							
JPG	XHTML_SUPPORTS_IFRAME																																							
MARKETING_NAME	XHTML_SUPPORTS_TABLE_FOR_LAYOUT																																							
MAX_IMAGE_HEIGHT	XHTML_SUPPORT_LEVEL																																							
MAX_IMAGE_WIDTH	XHTML_TABLE_SUPPORT																																							

deviceCharacteristicHeader

- **Property Manager name:** [Device Characterization - Forward in Header](#)[↗]
- **Behavior version:** The v2018-02-27 rule format supports the deviceCharacteristicHeader behavior v1.2.
- **Rule format status:** [Deprecated, outdated rule format](#)
- **Access:** [Read-write](#)

Sends selected information about requesting devices to the origin server, in the form of an X-Akamai-Device-Characteristics HTTP header. Use in conjunction with the [deviceCharacteristicCacheId](#) behavior.

Option	Type	Description																																		
elements	string array	Specifies the set of information about the requesting device to send to the origin server.																																		
		Supported values: <table><tr><td>ACCEPT_THIRD_PARTY_COOKIE</td><td>MAX_IMAGE_HEIGHT</td></tr><tr><td>AJAX_PREFERRED_GEOLOC_API</td><td>MAX_IMAGE_WIDTH</td></tr><tr><td>AJAX_SUPPORT_JAVASCRIPT</td><td>MOBILE_BROWSER</td></tr><tr><td>BRAND_NAME</td><td>MOBILE_BROWSER_VERSION</td></tr><tr><td>COOKIE_SUPPORT</td><td>MODEL_NAME</td></tr><tr><td>DEVICE_OS</td><td>PDF_SUPPORT</td></tr><tr><td>DEVICE_OS_VERSION</td><td>PHYSICAL_SCREEN_HEIGHT</td></tr><tr><td>DUAL_ORIENTATION</td><td>PHYSICAL_SCREEN_WIDTH</td></tr><tr><td>FLASH_LITE_VERSION</td><td>PNG</td></tr><tr><td>FULL_FLASH_SUPPORT</td><td>PREFERRED_MARKUP</td></tr><tr><td>GIF_ANIMATED</td><td>RESOLUTION_HEIGHT</td></tr><tr><td>HTML_PREFERRED_DTD</td><td>RESOLUTION_WIDTH</td></tr><tr><td>IS_MOBILE</td><td>VIEWPORT_INITIAL_SCALE</td></tr><tr><td>IS_TABLET</td><td>VIEWPORT_WIDTH</td></tr><tr><td>IS_WIRELESS_DEVICE</td><td>XHTMLMP_PREFERRED_MIME_TYPE</td></tr><tr><td>JPG</td><td>XHTML_FILE_UPLOAD</td></tr><tr><td>MARKETING_NAME</td><td>XHTML_PREFERRED_CHARSET</td></tr></table>	ACCEPT_THIRD_PARTY_COOKIE	MAX_IMAGE_HEIGHT	AJAX_PREFERRED_GEOLOC_API	MAX_IMAGE_WIDTH	AJAX_SUPPORT_JAVASCRIPT	MOBILE_BROWSER	BRAND_NAME	MOBILE_BROWSER_VERSION	COOKIE_SUPPORT	MODEL_NAME	DEVICE_OS	PDF_SUPPORT	DEVICE_OS_VERSION	PHYSICAL_SCREEN_HEIGHT	DUAL_ORIENTATION	PHYSICAL_SCREEN_WIDTH	FLASH_LITE_VERSION	PNG	FULL_FLASH_SUPPORT	PREFERRED_MARKUP	GIF_ANIMATED	RESOLUTION_HEIGHT	HTML_PREFERRED_DTD	RESOLUTION_WIDTH	IS_MOBILE	VIEWPORT_INITIAL_SCALE	IS_TABLET	VIEWPORT_WIDTH	IS_WIRELESS_DEVICE	XHTMLMP_PREFERRED_MIME_TYPE	JPG	XHTML_FILE_UPLOAD	MARKETING_NAME	XHTML_PREFERRED_CHARSET
ACCEPT_THIRD_PARTY_COOKIE	MAX_IMAGE_HEIGHT																																			
AJAX_PREFERRED_GEOLOC_API	MAX_IMAGE_WIDTH																																			
AJAX_SUPPORT_JAVASCRIPT	MOBILE_BROWSER																																			
BRAND_NAME	MOBILE_BROWSER_VERSION																																			
COOKIE_SUPPORT	MODEL_NAME																																			
DEVICE_OS	PDF_SUPPORT																																			
DEVICE_OS_VERSION	PHYSICAL_SCREEN_HEIGHT																																			
DUAL_ORIENTATION	PHYSICAL_SCREEN_WIDTH																																			
FLASH_LITE_VERSION	PNG																																			
FULL_FLASH_SUPPORT	PREFERRED_MARKUP																																			
GIF_ANIMATED	RESOLUTION_HEIGHT																																			
HTML_PREFERRED_DTD	RESOLUTION_WIDTH																																			
IS_MOBILE	VIEWPORT_INITIAL_SCALE																																			
IS_TABLET	VIEWPORT_WIDTH																																			
IS_WIRELESS_DEVICE	XHTMLMP_PREFERRED_MIME_TYPE																																			
JPG	XHTML_FILE_UPLOAD																																			
MARKETING_NAME	XHTML_PREFERRED_CHARSET																																			

dnsAsyncRefresh

- **Property Manager name:** [DNS Asynchronous Refresh](#)[↗]
- **Behavior version:** The v2018-02-27 rule format supports the dnsAsyncRefresh behavior v1.1.
- **Rule format status:** [Deprecated, outdated rule format](#)
- **Access:** [Read-write](#)

Allow an edge server to use an expired DNS record when forwarding a request to your origin. The *type A* DNS record refreshes *after* content is served to the end user, so there is no wait for the DNS resolution. Avoid this behavior if you want to be able to disable a server immediately after its DNS record expires.

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

Option	Type	Description
enabled	boolean	Allows edge servers to refresh an expired DNS record after serving content.
timeout	string (duration)	Set the maximum allowed time an expired DNS record may be active.

dnsPrefresh

- **Property Manager name:** [DNS Prefresh](#)^{*}
- **Behavior version:** The v2018-02-27 rule format supports the dnsPrefresh behavior v1.1.
- **Rule format status:** [Deprecated, outdated rule format](#)
- **Access:** [Read-only](#)

Allows edge servers to refresh your origin's DNS record independently from end-user requests. The type A DNS record refreshes before the origin's DNS record expires.

Option	Type	Description
enabled	boolean	Allows edge servers to refresh DNS records before they expire.
delay	string (duration)	Specifies the amount of time following a DNS record's expiration to asynchronously prefetch it.
timeout	string (duration)	Specifies the amount of time to prefetch a DNS entry if there have been no requests to the domain name.


downgradeProtocol


- **Property Manager name:** [Protocol Downgrade](#)^{*}
- **Behavior version:** The v2018-02-27 rule format supports the downgradeProtocol behavior v1.1.
- **Rule format status:** [Deprecated, outdated rule format](#)
- **Access:** [Read-write](#)

Serve static objects to the end-user client over HTTPS, but fetch them from the origin via HTTP.

Option	Type	Description
enabled	boolean	Enables the protocol downgrading behavior.

downloadCompleteMarker


- **Property Manager name:** [Download Complete Marker](#) 
- **Behavior version:** The v2018-02-27 rule format supports the downloadCompleteMarker behavior v1.0.
- **Rule format status:** [Deprecated, outdated rule format](#)
- **Access:** [Read-write](#)



The [Internet of Things: OTA Updates](#)  product allows customers to securely distribute firmware to devices over cellular networks. Based on match criteria that executes a rule, this behavior logs requests to the OTA servers as completed in aggregated and individual reports.

See also the [downloadNotification](#) and [requestTypeMarker](#) behaviors.

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

downloadNotification


- **Property Manager name:** [Download Notification](#) 
- **Behavior version:** The v2018-02-27 rule format supports the downloadNotification behavior v1.0.
- **Rule format status:** [Deprecated, outdated rule format](#)
- **Access:** [Read-write](#)

The [Internet of Things: OTA Updates](#)  product allows customers to securely distribute firmware to devices over cellular networks. Based on match criteria that executes a rule, this behavior allows requests to the [OTA Updates API](#)  for a list of completed downloads to individual vehicles.

See also the [downloadCompleteMarker](#) behavior.

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

downstreamCache

- **Property Manager name:** [Downstream Cacheability](#) 
- **Behavior version:** The v2018-02-27 rule format supports the downstreamCache behavior v1.2.
- **Rule format status:** [Deprecated, outdated rule format](#)
- **Access:** [Read-write](#)

Specify the caching instructions the edge server sends to the end user's client or client proxies. By default, the cache's duration is whichever is less: the remaining lifetime of the edge cache, or what the origin's header specifies. If the origin is set to `no-store` or `bypass-cache`, edge servers send *cache-busting* headers downstream to prevent downstream caching.

Option	Type	Description	Requires
behavior	enum	Specify the caching instructions the edge server sends to the end user's client.	
	ALLOW	The value of <code>allowBehavior</code> chooses the caching method and headers to send to the client.	
	MUST_REVALIDATE	This equates to a <code>Cache-Control: no-cache</code> header, which allows caching but forces the client browser to send an <code>if-modified-since</code> request each time it requests the object.	
	BUST	Sends cache-busting headers downstream.	
	TUNNEL_ORIGIN	This passes <code>Cache-Control</code> and <code>Expires</code> headers from the origin to the downstream client.	
	NONE	Don't send any caching headers. Allow client browsers to cache content according to their own default settings.	
allowBehavior	enum	Specify how the edge server calculates the downstream cache by setting the value of the <code>Expires</code> header.	behavior is ALLOW
	LESSER	Sends the lesser value of what the origin specifies and the edge cache's remaining duration. This is the default behavior.	
	GREATER	Sends the greater value of what the origin specifies and the edge cache's remaining duration.	
	REMAINING_LIFETIME	Sends the value of the edge cache's remaining duration, without comparing it to the origin's headers.	
	FROM_MAX_AGE	Sends the <code>cache:max-age</code> value applied to the object, without evaluating the cache's duration.	
	FROM_VALUE	Sends the value of the edge cache's duration.	
	PASS_ORIGIN	Sends the value of the origin's header, without evaluating the edge cache's duration.	
ttl	string (duration)	Sets the duration of the cache. Setting the value to <code>0</code> equates to a <code>no-cache</code> header that forces revalidation.	allowBehavior is FROM_VALUE
sendHeaders	enum	Specifies the HTTP headers to include in the response to the client.	behavior is ALLOW
	CACHE_CONTROL_AND_EXPIRES	Sends both <code>Cache-Control</code> and <code>Expires</code> header.	
	CACHE_CONTROL	Sends only the origin's <code>Cache-Control</code> header.	
	EXPIRES	Sends only the origin's <code>Expires</code> header.	
	PASS_ORIGIN	Sends the same set of <code>Cache-Control</code> and <code>Expires</code> headers received from the origin.	
sendPrivate	boolean	Adds a <code>Cache-Control: private</code> header to prevent objects from being cached in a shared caching proxy.	behavior is either: ALLOW, MUST_REVALIDATE AND sendHeaders is not EXPIRES

dynamicWebContent

- **Property Manager name:** [Content Characteristics - Dynamic Web Content](#)
- **Behavior version:** The v2018-02-27 rule format supports the dynamicWebContent behavior v1.1.
- **Rule format status:** [Deprecated, outdated rule format](#)
- **Access:** [Read-write](#)

In conjunction with the [subCustomer](#) behavior, this optional behavior allows you to control how dynamic web content behaves for your subcustomers using [Akamai Cloud Embed](#).

Option	Type	Description
sureRoute	boolean	Optimizes how subcustomer traffic routes from origin to edge servers. See the sureRoute behavior for more information.
prefetch	boolean	Allows subcustomer content to prefetch over HTTP/2.
realUserMonitoring	boolean	Allows Real User Monitoring (RUM) to collect performance data for subcustomer content. See the realUserMonitoring behavior for more information.
imageCompression	boolean	Enables image compression for subcustomer content.

edgeConnect

- **Property Manager name:** [Cloud Monitor Instrumentation](#)
- **Behavior version:** The v2018-02-27 rule format supports the edgeConnect behavior v1.1.
- **Rule format status:** [Deprecated, outdated rule format](#)
- **Access:** [Read-write](#)

Configures traffic logs for the Cloud Monitor push API.

Option	Type	Description	Requires
enabled	boolean	Enables Cloud Monitor's log-publishing behavior.	
apiConnector	enum	Describes the API connector type.	
		Supported values: BMC_APM	
apiDataElements	string array	Specifies the data set to log.	

Option	Type	Description	Requires
		Supported values: <pre> APM GEO HTTP NETWORK_PERFORMANCE NETWORK_V1 REQUEST_HEADER RESPONSE_HEADER SEC_APP_V2 SEC_RATE_DENY_V2 SEC_RATE_WARN_V2 </pre>	
destination Hostname	string	Specifies the target hostname accepting push API requests.	
destinationPath	string	Specifies the push API's endpoint.	
overrideAggregate Settings	boolean	When enabled, overrides default log settings.	
aggregateTime	string (duration)	Specifies how often logs are generated.	overrideAggregateSettings is true
aggregateLines	string	Specifies the maximum number of lines to include in each log.	overrideAggregateSettings is true
aggregateSize	string	Specifies the log's maximum size.	overrideAggregateSettings is true


edgeImageConversion

- **Property Manager name:** [Image Converter Settings](#)
- **Behavior version:** The v2018-02-27 rule format supports the edgeImageConversion behavior v1.2.
- **Rule format status:** [Deprecated, outdated rule format](#)
- **Access:** [Read-write](#)

The Edge Image Converter offloads various image manipulation tasks to edge servers. This behavior specifies various predefined policies to apply.

Option	Type	Description	Requires
enabled	boolean	Enables the edge image conversion behavior.	
failover	boolean	If the request results in a server error, enabling this forwards it to the origin.	
usePolicy	boolean	Enables a specified set of image conversion policies.	
policies	object array	Specifies commands that when present or not in the query string release an error code.	usePolicy is true
policy Responses	enum	Specifies the HTTP error code if any policies conditions match.	usePolicy is true
		Supported values: <pre> 400 403 404 409 </pre>	


edgeLoadBalancingAdvanced

- **Property Manager name:** [Edge Load Balancing: Advanced Metadata](#) 
- **Behavior version:** The `v2018-02-27` rule format supports the `edgeLoadBalancingAdvanced` behavior v1.0.
- **Rule format status:** [Deprecated, outdated rule format](#)
- **Access:** [Read-only](#)

This behavior implements customized Edge Load Balancing features. Contact Akamai Professional Services for help configuring it.

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

edgeLoadBalancingDataCenter

- **Property Manager name:** [Edge Load Balancing: Data Center](#) 
- **Behavior version:** The `v2018-02-27` rule format supports the `edgeLoadBalancingDataCenter` behavior v1.2.
- **Rule format status:** [Deprecated, outdated rule format](#)
- **Access:** [Read-write](#)

The Edge Load Balancing module allows you to specify groups of data centers that implement load balancing, session persistence, and real-time dynamic failover. Enabling ELB routes requests contextually based on location, device, or network, along with optional rules you specify.

This behavior specifies details about a data center, and needs to be paired in the same rule with an `edgeLoadBalancingOrigin` behavior, which specifies its origin. An *origin* is an abstraction that helps group a logical set of a website or application. It potentially includes information about many data centers and cloud providers, as well as many end points or IP addresses for each data center. More than one data center can thus refer to the same origin.

Option	Type	Description	Requires
originId	string	Corresponds to the <code>id</code> specified by the <code>edgeLoadBalancingOrigin</code> behavior associated with this data center.	
description	string	Provides a description for the ELB data center, for your own reference.	
hostname	string	Specifies the data center's hostname.	

Option	Type	Description	Requires
cookieName	string	If using session persistence, this specifies the value of the cookie named in the corresponding edgeLoadBalancingOrigin behavior's <code>cookie_name</code> option.	
enableFailover	boolean	Allows you to specify failover rules.	
ip	string	Specifies this data center's IP address.	enable Failover is true
failoverRules	object array	Provides up to four failover rules to apply in the specified order.	enable Failover is true
failover Rules[].failover Hostname	string	The hostname of the data center to fail over to.	
failover Rules[].modify Request	boolean	Allows you to modify the request's hostname or path.	
failover Rules[].override Hostname	boolean	Overrides the request's hostname with the <code>failover_hostname</code> .	modify Request is true
failover Rules[].context Root	string	Specifies the path to use in the forwarding request, typically the root (/) when failing over to a different data center, or a full path such as <code>/static/error.html</code> when failing over to an error page.	modify Request is true
failover Rules[].absolute Path	boolean	When enabled, interprets the path specified by <code>context_root</code> as an absolute server path, for example to reference a site-down page. Otherwise when disabled, the path is appended to the request.	modify Request is true

edgeLoadBalancingOrigin

- **Property Manager name:** [Edge Load Balancing: Origin Definition](#) [↗]
- **Behavior version:** The `v2018-02-27` rule format supports the `edgeLoadBalancingOrigin` behavior v1.2.
- **Rule format status:** [Deprecated, outdated rule format](#)
- **Access:** [Read-write](#)


The Edge Load Balancing module allows you to implement groups of data centers featuring load balancing, session persistence, and real-time dynamic failover. Enabling ELB routes requests contextually based on location, device, or network, along with optional rules you specify.

This behavior specifies the data center's origin, and needs to be paired in the same rule with at least one [edgeLoadBalancingDataCenter](#) behavior, which provides details about a particular data center. An *origin* is an abstraction that helps group a logical set of a website or application. It potentially includes information about many data centers and cloud providers, as well as many end points or IP addresses for each data center. To specify an ELB origin, you need to have configured an [origin](#) behavior whose `type` is set to `elb_origin_group` .

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

Option	Type	Description	Requires
id	string	Specifies a unique descriptive string for this ELB origin. The value needs to match the <code>origin_id</code> specified by the <code>edgeLoadBalancingDataCenter</code> behavior associated with this origin.	
description	string	Provides a description for the ELB origin, for your own reference.	
hostname	string	Specifies the hostname associated with the ELB rule.	
enable Session Persistence	boolean	Allows you to specify a cookie to pin the user's browser session to one data center. When disabled, ELB's default load balancing may send users to various data centers within the same session.	
cookie Name	string	This specifies the name of the cookie that marks users' persistent sessions. The accompanying <code>edgeLoadBalancingDataCenter</code> behavior's <code>description</code> option specifies the cookie's value.	enable Session Persistence is <code>true</code>

edgeOriginAuthorization


- **Property Manager name:** [Edge Server Identification](#) 
- **Behavior version:** The `v2018-02-27` rule format supports the `edgeOriginAuthorization` behavior `v1.1`.
- **Rule format status:** [Deprecated, outdated rule format](#)
- **Access:** [Read-write](#)

Allows the origin server to use a cookie to ensure requests from Akamai servers are genuine.

This behavior requires that you specify the cookie's domain name, so it is best to deploy within a match of the hostname. It does not work properly when the origin server accepts more than one hostname (for example, using virtual servers) that do not share the same top-level domain.

Option	Type	Description
enabled	boolean	Enables the cookie-authorization behavior.
cookie Name	string	Specifies the name of the cookie to use for authorization.
value	string	Specifies the value of the authorization cookie.
domain	string	Specify the cookie's domain, which needs to match the top-level domain of the <code>Host</code> header the origin server receives.

edgeRedirector

- **Property Manager name:** [Edge Redirector Cloudlet](#) 
- **Behavior version:** The `v2018-02-27` rule format supports the `edgeRedirector` behavior `v3.0`.

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

This behavior enables the [Edge Redirector Cloudlet](#) application, which helps you manage large numbers of redirects. With Cloudlets available on your contract, choose **Your services <> Edge logic Cloudlets** to control the Edge Redirector within [Control Center](#). Otherwise use the [Cloudlets API](#) to configure it programmatically.

Option	Type	Description
enabled	boolean	Enables the Edge Redirector Cloudlet.
cloudletPolicy	object	Specifies the Cloudlet policy as an object.
cloudletPolicy.id	number	Identifies the Cloudlet.
cloudletPolicy.name	string	The Cloudlet's descriptive name.

edgeScape

- **Property Manager name:** [Content Targeting_\(EdgeScape\)](#)
- **Behavior version:** The `v2018-02-27` rule format supports the `edgeScape` behavior v1.1.
- **Rule format status:** [Deprecated, outdated rule format](#)
- **Access:** [Read-write](#)

[EdgeScape](#) allows you to customize content based on the end user's geographic location or connection speed. When enabled, the edge server sends a special `X-Akamai-Edgescape` header to the origin server encoding relevant details about the end-user client as key-value pairs.

Option	Type	Description
enabled	boolean	When enabled, sends the <code>X-Akamai-Edgescape</code> request header to the origin.

enhancedAkamaiProtocol

- **Property Manager name:** [Enhanced Akamai Protocol](#)
- **Behavior version:** The `v2018-02-27` rule format supports the `enhancedAkamaiProtocol` behavior v1.1.
- **Rule format status:** [Deprecated, outdated rule format](#)
- **Access:** [Read-write](#)

Enables the Enhanced Akamai Protocol, a suite of advanced routing and transport optimizations that increase your website's performance and reliability. It is only available to specific

applications, and requires a special routing from edge to origin.

Warning. Disabling this behavior may significantly reduce a property's performance.

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

edgeSideIncludes

- **Property Manager name:** [ESI \(Edge Side Includes\)](#)^{*}
- **Behavior version:** The `v2018-02-27` rule format supports the `edgeSideIncludes` behavior v1.2.
- **Rule format status:** [Deprecated, outdated rule format](#)
- **Access:** [Read-write](#)

Allows edge servers to process edge side include (ESI) code to generate dynamic content. To apply this behavior, you need to match on a `contentType`, `path`, or `filename`. Since this behavior requires more parsing time, you should not apply it to pages that lack ESI code, or to any non-HTML content.

Option	Type	Description	Requires
<code>enabled</code>	boolean	Enables ESI processing.	
<code>enableViaHttp</code>	boolean	Enable ESI only for content featuring the <code>Edge-control: dca=esi</code> HTTP response header.	
<code>passSetCookie</code>	boolean	Allows edge servers to pass your origin server's cookies to the ESI processor.	<code>enableViaHttp</code> is <code>true</code>
<code>passClientIp</code>	boolean	Allows edge servers to pass the client IP header to the ESI processor.	<code>enableViaHttp</code> is <code>true</code>
<code>i18nStatus</code>	boolean	Provides internationalization support for ESI.	<code>enableViaHttp</code> is <code>true</code>
<code>i18nCharset</code>	string array	Specifies the character sets to use when transcoding the ESI language, UTF-8 and ISO-8859-1 for example.	<code>i18nStatus</code> is <code>true</code>

failAction

- **Property Manager name:** [Site Failover](#)^{*}
- **Behavior version:** The `v2018-02-27` rule format supports the `failAction` behavior v1.4.
- **Rule format status:** [Deprecated, outdated rule format](#)
- **Access:** [Read-write](#)

Specifies how to respond when the origin is not available: by serving stale content, by serving an error page, or by redirecting. To apply this behavior, you should match on an `originTimeout` or

[matchResponseCode](#) .

Option	Type	Description	Requires
enabled	boolean	When enabled in case of a failure to contact the origin, the current behavior applies.	
actionType	enum	Specifies the basic action to take when there is a failure to contact the origin.	
	SERVE_STALE	Serves content that is already in the cache.	
	REDIRECT	Specifies a redirect action. (Use with these options: redirectHostnameType , redirectHostname , redirectCustomPath , redirectPath , redirectMethod , modifyProtocol , and protocol .)	
	RECREATED_CO	Serves alternate content from your network. (Use with these options: contentHostname , contentCustomPath , and contentPath .)	
	RECREATED_CEX	Serves alternate content from an external network. (Use with these options: cexHostname , cexCustomPath , and cexPath .)	
	RECREATED_NS	Serves NetStorage content. (Use with these options: netStorageHostname , netStoragePath , and cpCode .)	
	DYNAMIC	Allows you to serve dynamic SaaS content if SaaS acceleration is available on your contract. (Use with these options: dynamicMethod , dynamicCustomPath , saasType , saasSuffix , saasRegex , and saasReplace .)	
saasType	enum	Identifies the component of the request that identifies the SaaS dynamic fail action.	actionType is DYNAMIC
		Supported values: COOKIE	
saasCnameEnabled	boolean	Specifies whether to use a CNAME chain to determine the hostname for the SaaS dynamic failaction.	saasType is HOSTNAME
saasCnameLevel	number	Specifies the number of elements in the CNAME chain backwards from the edge hostname that determines the hostname for the SaaS dynamic failaction.	saasCnameEnabled is true
saasCookie	string (allows variables)	Specifies the name of the cookie that identifies this SaaS dynamic failaction.	saasType is COOKIE
saasQueryString	string (allows variables)	Specifies the name of the query parameter that identifies this SaaS dynamic failaction.	saasType is QUERY_STRING
saasRegex	string	Specifies the substitution pattern (a Perl-compatible regular expression) that defines the SaaS dynamic failaction.	actionType is DYNAMIC
saasReplace	string (allows variables)	Specifies the replacement pattern that defines the SaaS dynamic failaction.	actionType is DYNAMIC
saasSuffix	string (allows variables)	Specifies the static portion of the SaaS dynamic failaction.	actionType is DYNAMIC
dynamicMethod	enum	Specifies the redirect method.	actionType is DYNAMIC
	SERVE_301	A 301 redirect response.	
	SERVE_302	A 302 redirect response.	
	SERVE_ALTERNATE	Serve an alternate response.	

Option	Type	Description	Requires
dynamicCustomPath	boolean	Allows you to modify the original requested path.	actionType is DYNAMIC
dynamicPath	string (allows variables)	Specifies the new path.	dynamicCustomPath is true
redirectHostnameType	enum	Whether to preserve or customize the hostname.	actionType is REDIRECT
	ORIGINAL	Preserve the original hostname in the redirect.	
	ALTERNATE	Specify a redirectHostname .	
redirectHostname	string (allows variables)	When the actionType is REDIRECT and the redirectHostnameType is ALTERNATE , this specifies the hostname for the redirect.	redirectHostnameType is ALTERNATE
redirectCustomPath	boolean	Uses the redirectPath to customize a new path.	actionType is REDIRECT
redirectPath	string (allows variables)	Specifies a new path.	redirectCustomPath is true
redirectMethod	enum	Specifies the HTTP response code.	actionType is REDIRECT
		Supported values: 301 302	
contentHostname	string (allows variables)	Specifies the static hostname for the alternate redirect.	actionType is RECREATED_CO
contentCustomPath	boolean	Specifies a custom redirect path.	actionType is RECREATED_CO
contentPath	string (allows variables)	Specifies a custom redirect path.	contentCustomPath is true
netStorageHostname	object	When the actionType is RECREATED_NS , specifies the Net Storage origin to serve the alternate content. Contact Akamai Professional Services for your NetStorage origin's id .	actionType is RECREATED_NS
netStorageHostname.cpCodeList	array	A set of CP codes that apply to this storage group.	
netStorageHostname.downloadDomainName	string	Domain name from which content can be downloaded.	
netStorageHostname.id	number	Unique identifier for the storage group.	
netStorageHostname.name	string	Name of the storage group.	
netStorageHostname.uploadDomainName	string	Domain name used to upload content.	

Option	Type	Description	Requires
netStoragePath	string (allows variables)	When the <code>actionType</code> is <code>RECREATED_NS</code> , specifies the path for the NetStorage request.	<code>actionType</code> is <code>RECREATED_NS</code>
cexHostname	string (allows variables)	Specifies a hostname.	<code>actionType</code> is <code>RECREATED_CEX</code>
cexCustomPath	boolean	Specifies a custom path.	<code>actionType</code> is <code>RECREATED_CEX</code>
cexPath	string (allows variables)	Specifies a custom path.	<code>cexCustomPath</code> is <code>true</code>
cpCode	object	Specifies a CP code for which to log errors for the Net Storage location.	<code>actionType</code> is <code>RECREATED_NS</code>
cp Code.description	string	Additional description for the CP code.	
cpCode.id	integer	Unique identifier for each CP code.	
cpCode.name	string	The name of the CP code.	
cpCode.products	array	The set of products the CP code is assigned to.	
preserveQuery String	boolean	When using either <code>contentCustomPath</code> , <code>cexCustomPath</code> , <code>dynamicCustomPath</code> , or <code>redirectCustomPath</code> to specify a custom path, enabling this passes in the original request's query string as part of the path.	<code>contentCustomPath</code> is <code>true</code> OR <code>cexCustomPath</code> is <code>true</code> OR <code>redirectCustomPath</code> is <code>true</code> OR <code>dynamicCustomPath</code> is <code>true</code>
modifyProtocol	boolean	Modifies the redirect's protocol using the value of the <code>protocol</code> field.	<code>actionType</code> is <code>REDIRECT</code> OR <code>dynamicMethod</code> is either: <code>SERVE_301</code> , <code>SERVE_302</code>
protocol	enum	When the <code>actionType</code> is <code>REDIRECT</code> and <code>modifyProtocol</code> is enabled, this specifies the redirect's protocol.	<code>modifyProtocol</code> is <code>true</code>
		Supported values: HTTP HTTPS	

fastInvalidDate

- **Property Manager name:** [Fast Invalidate \(Safe to remove\)](#) [ⓘ]
- **Behavior version:** The v2018-02-27 rule format supports the fastInvalidate behavior v1.0.
- **Rule format status:** [Deprecated, outdated rule format](#)
- **Access:** [Read-write](#)

Applies Akamai's *Fast Purge* feature to selected edge content, invalidating it within approximately five seconds. This behavior sends an If-Modified-Since request to the origin for subsequent requests, replacing it with origin content if its timestamp is more recent. Otherwise if the origin lacks a Last-Modified header, it sends a simple GET request. Note that this behavior does not simply delete content if more recent origin content is unavailable. See the [Fast Purge API](#) [ⓘ] for an independent way to invalidate selected sets of content, and for more information on the feature.

Option	Type	Description
enabled	boolean	When enabled, forces a validation test for all edge content to which the behavior applies.

firstPartyMarketing


- **Property Manager name:** [Cloud Marketing Cloudlet \(Beta\)](#) [ⓘ]
- **Behavior version:** The v2018-02-27 rule format supports the firstPartyMarketing behavior v1.0.
- **Rule format status:** [Deprecated, outdated rule format](#)
- **Access:** [Read-write](#)



Enables the [Cloud Marketing Cloudlet](#) [ⓘ], which helps MediaMath customers collect usage data and place corresponding tags for use in online advertising. You can configure tags using either the Cloudlets Policy Manager application or the [Cloudlets API](#) [ⓘ]. See also the [firstPartyMarketingPlus](#) behavior, which integrates better with both MediaMath and its partners. Both behaviors support the same set of options.

Option	Type	Description	Requires
enabled	boolean	Enables the Cloud Marketing Cloudlet.	
javascript Insertion Rule	enum	Select how to insert the MediaMath JavaScript reference script.	
	NEVER	Specify this if inserting the script at the origin.	
	POLICY	Allow the Cloudlet policy to determine when to insert it.	
	ALWAYS	Insert it for all edge requests.	
cloudlet Policy	object	Identifies the Cloudlet policy.	javascript Insertion Rule is POLICY
cloudlet Policy.id	number	Identifies the Cloudlet.	

Option	Type	Description	Requires
cloudlet Policy.name	string	The Cloudlet's descriptive name.	
mediaMath Prefix	string	Specify the URL path prefix that distinguishes Cloud Marketing requests from your other web traffic. Include the leading slash character, but no trailing slash. For example, if the path prefix is <code>/mmath</code> , and the request is for <code>www.example.com/dir</code> , the new URL is <code>www.example.com/mmath/dir</code> .	

firstPartyMarketingPlus

- **Property Manager name:** [Cloud Marketing Plus Cloudlet \(Beta\)](#) 
- **Behavior version:** The `v2018-02-27` rule format supports the `firstPartyMarketingPlus` behavior `v1.0`.
- **Rule format status:** [Deprecated, outdated rule format](#)
- **Access:** [Read-write](#)

Enables the [Cloud Marketing Plus Cloudlet](#) , which helps MediaMath customers collect usage data and place corresponding tags for use in online advertising. You can configure tags using either the Cloudlets Policy Manager application or the [Cloudlets API](#) . See also the [firstPartyMarketing](#) behavior, which integrates with MediaMath but not its partners. Both behaviors support the same set of options.

Option	Type	Description	Requires
enabled	boolean	Enables the Cloud Marketing Plus Cloudlet.	
javaScript Insertion Rule	enum	Select how to insert the MediaMath JavaScript reference script.	
	NEVER	Specify this if inserting the script at the origin.	
	POLICY	Allow the Cloudlet policy to determine when to insert it.	
	ALWAYS	Insert it for all edge requests.	
cloudlet Policy	object	Identifies the Cloudlet policy.	javaScript Insertion Rule is POLICY
cloudlet Policy.id	number	Identifies the Cloudlet.	
cloudlet Policy.name	string	The Cloudlet's descriptive name.	
mediaMath Prefix	string	Specify the URL path prefix that distinguishes Cloud Marketing requests from your other web traffic. Include the leading slash character, but no trailing slash. For example, if the path prefix is <code>/mmath</code> , and the request is for <code>www.example.com/dir</code> , the new URL is <code>www.example.com/mmath/dir</code> .	

forwardRewrite

- **Property Manager name:** [Forward Rewrite Cloudlet](#)[↗]
- **Behavior version:** The v2018-02-27 rule format supports the forwardRewrite behavior v3.1.
- **Rule format status:** [Deprecated, outdated rule format](#)
- **Access:** [Read-write](#)

The Forward Rewrite Cloudlet allows you to conditionally modify the forward path in edge content without affecting the URL that displays in the user's address bar. If Cloudlets are available on your contract, choose **Your services** <> **Edge logic Cloudlets** to control how this feature works within [Control Center](#)[↗], or use the [Cloudlets API](#)[↗] to configure it programmatically.

Option	Type	Description
enabled	boolean	Enables the Forward Rewrite Cloudlet behavior.
cloudletPolicy	object	Identifies the Cloudlet policy.
cloudletPolicy.id	number	Identifies the Cloudlet.
cloudletPolicy.name	string	The Cloudlet's descriptive name.

frontEndOptimization

- **Property Manager name:** [Front-End Optimization \(FEO\)](#)[↗]
- **Behavior version:** The v2018-02-27 rule format supports the frontEndOptimization behavior v1.1.
- **Rule format status:** [Deprecated, outdated rule format](#)
- **Access:** [Read-write](#)

This behavior enables [Front End Optimization](#)[↗], a suite of performance enhancements that accelerate page rendering and reduce download times, for example by *minifying* JavaScript and CSS.

Option	Type	Description
enabled	boolean	Enables the front-end optimization behavior.

g2oheader

- **Property Manager name:** [Signature Header Authentication](#)[↗]

- **Behavior version:** The `v2018-02-27` rule format supports the `g2oheader` behavior v1.1.
- **Rule format status:** [Deprecated, outdated rule format](#)
- **Access:** [Read-write](#)

The *signature header authentication* (g2o) security feature provides header-based verification of outgoing origin requests. Edge servers encrypt request data in a pre-defined header, which the origin uses to verify that the edge server processed the request. This behavior configures the request data, header names, encryption algorithm, and shared secret to use for verification.

Option	Type	Description	Requires
<code>enabled</code>	boolean	Enables the g2o verification behavior.	
<code>data Header</code>	string	Specifies the name of the header that contains the request data that needs to be encrypted.	
<code>signed Header</code>	string	Specifies the name of the header containing encrypted request data.	
<code>encoding Version</code>	enum	Specifies the version of the encryption algorithm as an integer from 1 through 5.	
		Supported values: <div>1 2 3 4 5</div>	
<code>use Custom Sign String</code>	boolean	When disabled, the encrypted string is based on the forwarded URL. If enabled, you can use <code>customSignString</code> to customize the set of data to encrypt.	
<code>custom Sign String</code>	string array	Specifies the set of data to be encrypted as a combination of concatenated strings.	<code>useCustom SignString</code> is <code>true</code>
	<code>AK_METHOD</code>	Incoming request method.	
	<code>AK_SCHEME</code>	Incoming request scheme (HTTP or HTTPS).	
	<code>AK_HOSTHEADER</code>	Incoming request hostname.	
	<code>AK_DOMAIN</code>	Incoming request domain.	
	<code>AK_URL</code>	Incoming request URL.	
	<code>AK_PATH</code>	Incoming request path.	
	<code>AK_QUERY</code>	Incoming request query string.	
	<code>AK_FILENAME</code>	Incoming request filename.	
	<code>AK_EXTENSION</code>	Incoming request filename extension.	
	<code>AK_CLIENT_REAL_IP</code>	Incoming client IP.	
<code>secret Key</code>	object array	Specifies the shared secret key.	
<code>nonce</code>	string	Specifies the cryptographic <i>nonce</i> string.	

gzipResponse

- **Property Manager name:** [Last Mile Acceleration \(Gzip Compression\)](#) [↗]
- **Behavior version:** The v2018-02-27 rule format supports the `gzipResponse` behavior v1.1.
- **Rule format status:** [Deprecated, outdated rule format](#)
- **Access:** [Read-write](#)

Apply *gzip* compression to speed transfer time. This behavior applies best to text-based content such as HTML, CSS, and JavaScript, especially once files exceed about 10KB. Do not apply it to already compressed image formats, or to small files that would add more time to uncompress. To apply this behavior, you should match on `contentType` or the content's `cacheability`.

Option	Type	Description	Requires
<code>behavior</code>	enum	Specify when to compress responses.	
	ORIGIN_RESPONSE	Compress for clients that send an <code>Accept-Encoding: gzip</code> header.	
	ALWAYS	Always compress.	
	NEVER	Never compress.	
<code>enable Compression</code>	boolean	Enables compression for all objects, regardless of their size.	<code>behavior</code> is ALWAYS
<code>threshold</code>	number	Specifies the maximum size of uncompressed files up to 25 KB. This behavior then only compresses objects that exceed the threshold.	<code>enable Compression</code> is false

hdDataAdvanced

- **Property Manager name:** [HD Data Override: Advanced Metadata](#) [↗]
- **Behavior version:** The v2018-02-27 rule format supports the `hdDataAdvanced` behavior v1.0.
- **Rule format status:** [Deprecated, outdated rule format](#)
- **Access:** [Read-only](#)

This behavior specifies Akamai XML metadata that can only be configured on your behalf by Akamai Professional Services. Unlike the [advanced](#) behavior, this may apply a different set of overriding metadata that executes in a post-processing phase.

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

http2

- **Property Manager name:** [HTTP/2](#)
- **Behavior version:** The `v2018-02-27` rule format supports the `http2` behavior v1.0.
- **Rule format status:** [Deprecated, outdated rule format](#)
- **Access:** [Read-write](#)

Enables the HTTP/2 protocol, which reduces latency and improves efficiency. 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.

healthDetection

- **Property Manager name:** [Origin Health Detection](#)
- **Behavior version:** The `v2018-02-27` rule format supports the `healthDetection` behavior v1.1.
- **Rule format status:** [Deprecated, outdated rule format](#)
- **Access:** [Read-write](#)

Monitors the health of your origin server by tracking unsuccessful attempts to contact it. Use this behavior to keep end users from having to wait several seconds before a forwarded request times out, or to reduce requests on the origin server when it is unavailable.

When client requests are forwarded to the origin, the edge server tracks the number of attempts to connect to each IP address. It cycles through IP addresses in least-recently-tested order to avoid hitting the same one twice in a row. If the number of consecutive unsuccessful tests reaches a threshold you specify, the behavior identifies the address as faulty and stops sending requests. The edge server returns an error message to the end user or else triggers any [failAction](#) behavior you specify.

Option	Type	Description
<code>retryCount</code>	number	The number of consecutive connection failures that mark an IP address as faulty.
<code>retryInterval</code>	string (duration)	Specifies the amount of time the edge server will wait before trying to reconnect to an IP address it has already identified as faulty.
<code>maximumReconnects</code>	number	Specifies the maximum number of times the edge server will contact your origin server. If your origin is associated with several IP addresses, <code>maximumReconnects</code> effectively overrides the value of <code>retryCount</code> .

httpStrictTransportSecurity

- **Property Manager name:** [HTTP Strict Transport Security \(HSTS\)](#) [↗]
- **Behavior version:** The `v2018-02-27` rule format supports the `httpStrictTransportSecurity` behavior v1.0.
- **Rule format status:** [Deprecated, outdated rule format](#)
- **Access:** [Read-write](#)

Applies HTTP Strict Transport Security (HSTS), disallowing insecure HTTP traffic. Apply this to hostnames managed with Standard TLS or Enhanced TLS certificates.

Option	Type	Description	Requires
<code>enable</code>	boolean	Applies HSTS to this set of requests.	
<code>maxAge</code>	enum	Specifies the duration for which to apply HSTS for new browser connections.	
	<code>ZERO_MINS</code>	This effectively disables HSTS, without affecting any existing browser connections.	
	<code>TEN_MINS</code>	10 minutes.	
	<code>ONE_DAY</code>	1 day.	
	<code>ONE_MONTH</code>	1 month.	
	<code>THREE_MONTHS</code>	3 months.	
	<code>SIX_MONTHS</code>	6 months.	
	<code>ONE_YEAR</code>	1 year.	
<code>includeSubDomains</code>	boolean	When enabled, applies HSTS to all subdomains.	<code>maxAge</code> is not <code>ZERO_MINS</code>
<code>preload</code>	boolean	When enabled, adds this domain to the browser's preload list. You still need to declare the domain at https://hstspreload.org [↗] .	<code>maxAge</code> is not <code>ZERO_MINS</code>
<code>redirect</code>	boolean	When enabled, redirects all HTTP requests to HTTPS.	<code>maxAge</code> is not <code>ZERO_MINS</code>
<code>redirectStatus Code</code>	enum	Specifies a response code.	<code>maxAge</code> is not <code>ZERO_MINS</code> AND <code>redirect</code> is <code>true</code>
		Supported values: <code>301</code> <code>302</code>	

imOverride

- **Property Manager name:** [Image and Video Manager: Set Parameter](#) [↗]
- **Behavior version:** The `v2018-02-27` rule format supports the `imOverride` behavior v1.0.

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

This specifies common query parameters that affect how [imageManager](#) transforms images, potentially overriding policy, width, format, or density request parameters. This also allows you to assign the value of one of the property's [rule tree variables](#) to one of Image and Video Manager's own policy variables.

Option	Type	Description	Requires
override	enum	Selects the type of query parameter you want to set.	
	POLICY	For the name of the Image and Video Manager policy you want to apply.	
	POLICY_VARIABLE	Specify that you want to set an Image and Video Manager policy variable from a rule tree variable defined in the property.	
	WIDTH	A predefined width to constrain the image to.	
	FORMAT	For browser types.	
	DPR	For pixel density.	
typesel	enum	Specifies how to set a query parameter.	override is not POLICY_VARIABLE
	VALUE	Assign a specific value.	
	VARIABLE	Assign a Property Manager rule tree VARIABLE .	
formatvar	string (variable name)	This selects the variable with the name of the browser you want to optimize images for. The variable specifies the same type of data as the format option below.	override is FORMAT AND typesel is VARIABLE
format	enum	Specifies the type of the browser you want to optimize images for.	override is FORMAT AND typesel is VALUE
	CHROME	Google Chrome.	
	IE	Internet Explorer.	
	SAFARI	Apple Safari.	
	GENERIC	Generic.	
dprvar	string (variable name)	This selects the variable with the desired pixel density. The variable specifies the same type of data as the dpr option below.	override is DPR AND typesel is VARIABLE
dpr	number	Directly specifies the pixel density. The numeric value is a scaling factor of 1, representing normal density.	override is DPR AND typesel is VALUE
widthvar	string (variable name)	Selects the variable with the desired width. If the Image and Video Manager policy doesn't define that width, it serves the next largest width.	override is WIDTH AND typesel is VARIABLE
width	number	Sets the image's desired pixel width directly. If the Image Manager policy doesn't define that width, it serves the next largest width.	override is WIDTH AND typesel is VALUE

Option	Type	Description	Requires
policyvar	string (variable name)	This selects the variable with the desired Image and Video Manager policy name to apply to image requests. If there is no policy by that name, Image and Video Manager serves the image unmodified.	override is POLICY AND typeset is VARIABLE
policy	string	This selects the desired Image and Video Manager policy name directly. If there is no policy by that name, Image and Video Manager serves the image unmodified.	override is POLICY AND typeset is VALUE
policyvar Name	string	This selects the name of one of the variables defined in an Image and Video Manager policy that you want to replace with the property's rule tree variable.	override is POLICY_ VARIABLE
policyvar IMvar	string (variable name)	This selects one of the property's rule tree variables to assign to the policyvarName variable within Image and Video Manager.	override is POLICY_ VARIABLE

injectReferenceld

- **Property Manager name:** [Inject Reference ID](#)
- **Behavior version:** The v2018-02-27 rule format supports the injectReferenceld behavior v1.0.
- **Rule format status:** [Deprecated, outdated rule format](#)
- **Access:** [Read-write](#)

Allows you to inject an Akamai reference ID, useful for troubleshooting, anywhere within the response body. With this feature enabled, any AKAM_REF string you specify is replaced with a unique identifier for each response.

Option	Type	Description
referenceld	boolean	Enables injection of reference ID values.

imageManager

- **Property Manager name:** [Image and Video Manager \(Images\)](#)
- **Behavior version:** The v2018-02-27 rule format supports the imageManager behavior v1.6.
- **Rule format status:** [Deprecated, outdated rule format](#)
- **Access:** [Read-write](#)

Optimizes images' size or file type for the requesting device. You can also use this behavior to generate API tokens to apply your own policies to matching images using the [Image and Video Manager API](#). To apply this behavior, you need to match on a [fileExtension](#). Once you apply

Image and Video Manager to traffic, you can add the [advancedImMatch](#) to ensure the behavior applies to the requests from the Image and Video Manager backend.

Option	Type	Description	Requires
<code>enabled</code>	boolean	Enable image management capabilities and generate a corresponding API token.	
<code>resize</code>	boolean	Specify whether to scale down images to the maximum screen resolution, as determined by the rendering device's user agent. Note that enabling this may affect screen layout in unexpected ways.	
<code>applyBestFileType</code>	boolean	Specify whether to convert images to the best file type for the requesting device, based on its user agent and the initial image file. This produces the smallest file size possible that retains image quality.	
<code>superCacheRegion</code>	enum	Specifies a location for your site's heaviest traffic, for use in caching derivatives on edge servers.	
	<code>US</code>	United States.	
	<code>ASIA</code>	Asia.	
	<code>AUSTRALIA</code>	Australia.	
	<code>EMEA</code>	Europe, Middle East, and Africa.	
	<code>JAPAN</code>	Japan.	
<code>cpCodeOriginal</code>	object	Assigns a CP code to track traffic and billing for original images that the Image and Video Manager has not modified.	
<code>cpCodeOriginal.description</code>	string	Additional description for the CP code.	
<code>cpCodeOriginal.id</code>	integer	Unique identifier for each CP code.	
<code>cpCodeOriginal.name</code>	string	The name of the CP code.	
<code>cpCodeOriginal.products</code>	array	The set of products the CP code is assigned to.	
<code>cpCodeTransformed</code>	object	Assigns a separate CP code to track traffic and billing for derived images.	
<code>cpCodeTransformed.description</code>	string	Additional description for the CP code.	
<code>cpCodeTransformed.id</code>	integer	Unique identifier for each CP code.	
<code>cpCodeTransformed.name</code>	string	The name of the CP code.	
<code>cpCodeTransformed.products</code>	array	The set of products the CP code is assigned to.	
<code>advanced</code>	boolean	Generates a custom Image and Video Manager API token to apply a corresponding policy to this set of images. The token consists of a descriptive label (the <code>policyToken</code>) concatenated with a property-specific identifier that's generated when you save the property. The API registers the token when you activate the property.	
<code>policyToken</code>	string	Assign a prefix label to help match the policy token to this set of images, limited to 32 alphanumeric or underscore characters. If you don't specify a label, <i>default</i> becomes the prefix.	<code>advanced</code> is <code>true</code>
<code>policyTokenDefault</code>	string	Specify the default policy identifier, which is registered with the Image and Video Manager API once you activate this property. The <code>advanced</code> option needs to be inactive.	<code>advanced</code> is <code>false</code>

inputValidation

- **Property Manager name:** [Input Validation Cloudlet](#)
- **Behavior version:** The v2018-02-27 rule format supports the inputValidation behavior v1.5.
- **Rule format status:** [Deprecated, outdated rule format](#)
- **Access:** [Read-write](#)

The Input Validation Cloudlet detects anomalous edge requests and helps mitigate repeated invalid requests. You can configure it using either the Cloudlets Policy Manager application, available within [Control Center](#) under **Your services <> Edge logic Cloudlets**, or the [Cloudlets API](#).

Use this behavior to specify criteria that identifies each unique end user, and optionally supplement the Input Validation policy with additional criteria your origin uses to identify invalid requests. Specify the threshold number of invalid requests that triggers a penalty, and the subsequent response. Also specify an ordinary failure response for those who have not yet met the threshold, which should not conflict with any other behavior that defines a failure response.

Option	Type	Description	Requires
enabled	boolean	Applies the Input Validation Cloudlet behavior.	
cloudletPolicy	object	Identifies the Cloudlet policy.	
cloudletPolicy.id	number	Identifies the Cloudlet.	
cloudletPolicy.name	string	The Cloudlet's descriptive name.	
label	string	Distinguishes this Input Validation policy from any others within the same property.	
userIdentificationByCookie	boolean	When enabled, identifies users by the value of a cookie.	
userIdentificationKeyCookie	string	This specifies the cookie name whose value needs to remain constant across requests to identify a user.	userIdentificationByCookie is true
userIdentificationByIp	boolean	When enabled, identifies users by specific IP address. Do not enable this if you are concerned about DDoS attacks from many different IP addresses.	
userIdentificationByHeaders	boolean	When enabled, identifies users by specific HTTP headers on GET or POST requests.	
userIdentificationKeyHeaders	string array	This specifies the HTTP headers whose combined set of values identify each end user.	userIdentificationByHeaders is true
userIdentificationByParams	boolean	When enabled, identifies users by specific query parameters on GET or POST requests.	

Option	Type	Description	Requires
userIdentificationKeyParams	string array	This specifies the query parameters whose combined set of values identify each end user.	userIdentificationByParams is true
allowLargePostBody	boolean	Fails POST request bodies that exceed 16 KB when enabled, otherwise allows them to pass with no validation for policy compliance.	
resetOnValid	boolean	Upon receiving a valid request, enabling this resets the <code>penaltyThreshold</code> counter to zero. Otherwise, even those series of invalid requests that are interrupted by valid requests may trigger the <code>penaltyAction</code> .	
validateOnOriginWith	enum	For any validation that edge servers can't perform alone, this specifies additional validation steps based on how the origin identifies an invalid request. If a request is invalid, the origin can indicate this to the edge server.	
	DISABLED	Specify if no additional validation is necessary.	
	RESPONSE_CODE	Use a response code.	
	RESPONSE_CODE_AND_HEADER	Use a response code and header.	
validateOnOriginHeaderName	string	If <code>validateOnOriginWith</code> is set to <code>RESPONSE_CODE_AND_HEADER</code> , this specifies the header name for a request that the origin identifies as invalid.	<code>validateOnOriginWith</code> is <code>RESPONSE_CODE_AND_HEADER</code>
validateOnOriginHeaderValue	string	If <code>validateOnOriginWith</code> is set to <code>RESPONSE_CODE_AND_HEADER</code> , this specifies an invalid request's header value that corresponds to the <code>validateOnOriginHeaderName</code> .	<code>validateOnOriginWith</code> is <code>RESPONSE_CODE_AND_HEADER</code>
validateOnOriginResponseCode	number	Unless <code>validateOnOriginWith</code> is <code>DISABLED</code> , this identifies the integer response code for requests the origin identifies as invalid.	<code>validateOnOriginWith</code> is either: <code>RESPONSE_CODE</code> , <code>RESPONSE_CODE_AND_HEADER</code>
failure302Uri	string	Specifies the redirect link for invalid requests that have not yet triggered a penalty.	
penaltyThreshold	number	Specifies the number of invalid requests permitted before executing the <code>penaltyAction</code> .	
penaltyAction	enum	Once the <code>penaltyThreshold</code> of invalid requests is met, this specifies the response.	
	REDIRECT_302	A 302 redirect response.	
	BLANK_403	A 403 response with no body content.	
	BRANDED_403	A custom 403 response.	
penalty302Uri	string	Specifies the redirect link for end users who trigger the penalty.	<code>penaltyAction</code> is <code>REDIRECT_302</code>
penaltyNetStorage	object	Specifies the NetStorage account that serves out the penalty's static 403 response content. Details appear in an object featuring a <code>downloadDomainName</code> string member that identifies the NetStorage hostname, and an integer <code>cpCode</code> to track the traffic.	<code>penaltyAction</code> is <code>BRANDED_403</code>

Option	Type	Description	Requires
penaltyNetStorage.cpCodeList	array	A set of CP codes that apply to this storage group.	
penaltyNetStorage.downloadDomainName	string	Domain name from which content can be downloaded.	
penaltyNetStorage.id	number	Unique identifier for the storage group.	
penaltyNetStorage.name	string	Name of the storage group.	
penaltyNetStorage.uploadDomainName	string	Domain name used to upload content.	
penalty403NetStoragePath	string	Specifies the full path to the static 403 response content relative to the <code>downloadDomainName</code> in the <code>penaltyNetStorage</code> object.	<code>penaltyAction</code> is <code>BRANDED_403</code>
penaltyBrandedDenyCacheTtl	number (5-30)	Specifies the penalty response's time to live in the cache, 5 minutes by default.	<code>penaltyAction</code> is <code>BRANDED_403</code>

instant

- **Property Manager name:** [Akamai Instant \(Prefetching\)](#) [↗]
- **Behavior version:** The `v2018-02-27` rule format supports the `instant` behavior v1.1.
- **Rule format status:** [Deprecated, outdated rule format](#)
- **Access:** [Read-write](#)

The Instant feature allows you to prefetch content to the edge cache by adding link relation attributes to markup. For example:

```
xml <a href="page2.html" rel="Akamai-prefetch">Page 2</a>
```

Default link relation values are `prefetch` and `Akamai-prefetch`. Applies only to HTML elements that may specify an external file: `<a>`, `<base>`, ``, `<script>`, `<input>`, `<link>`, `<table>`, `<td>`, or `<th>`. (For the latter three, some legacy browsers support a nonstandard `background` image attribute.)

This behavior provides an alternative to the [prefetch](#) and [prefetchable](#) behaviors, which allow you to configure more general prefetching behavior outside of markup.

Option	Type	Description	Requires
prefetchCacheable	boolean	When enabled, applies prefetching only to objects already set to be cacheable, for example using the caching behavior. Only applies to content with the tieredDistribution behavior enabled.	
prefetchNoStore	boolean	Allows otherwise non-cacheable <code>no-store</code> content to prefetch if the URL path ends with <code>/</code> to indicate a request for a default file, or if the extension matches the value of the <code>prefetchNoStoreExtensions</code> option. Only applies to content with the sureRoute behavior enabled.	

Option	Type	Description	Requires
prefetchNoStoreExtensions	string array	Specifies a set of file extensions for which the prefetchNoStore option is allowed.	prefetchNoStore is true
prefetchHtml	boolean	Allows edge servers to prefetch additional HTML pages while pages that link to them are being delivered. This only applies to links from <a> or <link> tags with the appropriate link relation attribute.	prefetchCacheable is true OR prefetchNoStore is true
customLinkRelations	string array	Specify link relation values that activate the prefetching behavior. For example, specifying fetch allows you to use shorter rel="fetch" markup.	prefetchHtml is true

instantConfig

- **Property Manager name:** [InstantConfig](#)
- **Behavior version:** The v2018-02-27 rule format supports the instantConfig behavior v1.1.
- **Rule format status:** [Deprecated, outdated rule format](#)
- **Access:** [Read-write](#)

Multi-Domain Configuration, also known as *InstantConfig*, allows you to apply property settings to all incoming hostnames based on a DNS lookup, without explicitly listing them among the property's hostnames.

Option	Type	Description
enabled	boolean	Enables the InstantConfig behavior.

largeFileOptimization

- **Property Manager name:** [Large File Optimization](#)
- **Behavior version:** The v2018-02-27 rule format supports the largeFileOptimization behavior v1.2.
- **Rule format status:** [Deprecated, outdated rule format](#)
- **Access:** [Read-write](#)

The [Large File Optimization](#) feature improves performance and reliability when delivering large files. You need this behavior for objects larger than 1.8GB, and it's recommended for anything over 100MB. You should apply it only to the specific content to be optimized, such as a download directory's .gz files, and enable the useVersioning option while enforcing your own filename versioning policy. Note that it is best to use [NetStorage](#) for objects larger than 1.8GB.

See also the [largeFileOptimizationAdvanced](#) behavior, which provides additional options for to configure partial object caching and HTTP/2 prefetching.

Option	Type	Description	Requires
enabled	boolean	Enables the file optimization behavior.	
enablePartialObjectCaching	enum	Specifies whether to cache partial objects.	
	PARTIAL_OBJECT_CACHING	Allows <i>partial-object caching</i> , which always applies to large objects served from NetStorage . To enable this, the origin needs to support byte range requests.	
	NON_PARTIAL_OBJECT_CACHING	Caches entire objects.	
minimumSize	string	Optimization only applies to files larger than this, expressed as a number suffixed with a unit string such as MB or GB .	enablePartialObjectCaching is PARTIAL_OBJECT_CACHING
maximumSize	string	Optimization does not apply to files larger than this, expressed as a number suffixed with a unit string such as MB or GB .	enablePartialObjectCaching is PARTIAL_OBJECT_CACHING
useVersioning	boolean	When enablePartialObjectCaching is set to PARTIAL_OBJECT_CACHING , enabling this option signals your intention to vary filenames by version, strongly recommended to avoid serving corrupt content when chunks come from different versions of the same file.	enablePartialObjectCaching is PARTIAL_OBJECT_CACHING

largeFileOptimizationAdvanced

- **Property Manager name:** [Large File Optimization \(Advanced\)](#)
- **Behavior version:** The v2018-02-27 rule format supports the largeFileOptimizationAdvanced behavior v1.0.
- **Rule format status:** [Deprecated, outdated rule format](#)
- **Access:** [Read-only](#)

The [Large File Optimization](#) feature improves performance and reliability when delivering large files. You need this behavior for objects larger than 1.8GB, and it's recommended for anything over 100MB. You should apply it only to the specific content to be optimized, such as a download directory's .gz files. Note that it is best to use [NetStorage](#) for objects larger than 1.8GB.

This advanced behavior provides additional HTTP/2 options not present in the [largeFileOptimization](#) behavior.

Option	Type	Description
enabled	boolean	Enables the file optimization behavior.
objectSize	string	Specifies the size of the file at which point to apply partial object (POC) caching. Append a numeric value with a MB or GB suffix.
fragmentSize	enum	Specifies the size of each fragment used for partial object caching.
		Supported values: <div>FOUR_MB HALF_MB ONE_MB TWO_MB</div>
prefetchDuring Request	number	The number of POC fragments to prefetch during the request.
prefetchAfter Request	number	The number of POC fragments to prefetch after the request.

limitBitRate

- **Property Manager name:** [Bit Rate Limiting](#)
- **Behavior version:** The v2018-02-27 rule format supports the limitBitRate behavior v1.1.
- **Rule format status:** [Deprecated, outdated rule format](#)
- **Access:** [Read-write](#)

Control the rate at which content serves out to end users, optionally varying the speed depending on the file size or elapsed download time. Each bit rate specified in the bitrateTable array corresponds to a thresholdTable entry that activates it. You can use this behavior to prevent media downloads from progressing faster than they are viewed, for example, or to differentiate various tiers of end-user experience. To apply this behavior, you should match on a [contentType](#) , [path](#) , or [filename](#) .

Option	Type	Description
enabled	boolean	When enabled, activates the bit rate limiting behavior.
bitrateTable	object array	Specifies a download rate that corresponds to a thresholdTable entry. The bit rate appears as a two-member object consisting of a numeric bitrateValue and a bitrateUnit string, with allowed values of Kbps , Mbps , and Gbps .
bitrateTable[].bitrateValue	number	The numeric indicator of the download rate.
bitrateTable[].bitrateUnit	enum	The unit of measurement, either KBPS , MBPS , or GBPS .
		Supported values: <div>GBPS KBPS MBPS</div>
thresholdTable	object array	Specifies the minimum size of the file or the amount of elapsed download time before applying the bit rate limit from the corresponding bitrateTable entry. The threshold appears as a two-member object consisting of a numeric thresholdValue and thresholdUnit string, with allowed values of SECONDS or BYTES .

Option	Type	Description
threshold Table[].threshold Value	number	The numeric indicator of the minimum file size or elapsed download time.
threshold Table[].threshold Unit	enum	The unit of measurement, either SECONDS of the elapsed download time, or BYTES of the file size.
		Supported values: <div>BYTESSECONDS</div>

mPulse

- **Property Manager name:** [mPulse](#)
- **Behavior version:** The v2018-02-27 rule format supports the mPulse behavior v1.1.
- **Rule format status:** [Deprecated, outdated rule format](#)
- **Access:** [Read-write](#)

[mPulse](#) provides high-level performance analytics and predictive recommendations based on real end user data. See the [mPulse Quick Start](#) to set up mPulse on your website.

Option	Type	Description
enabled	boolean	Applies performance monitoring to this behavior's set of content.
apiKey	string	This generated value uniquely identifies sections of your website for you to analyze independently. To access this value, see Enable mPulse in Property Manager .
buffer Size	string	Allows you to override the browser's default (150) maximum number of reported performance timeline entries.

manifestRerouting

- **Property Manager name:** [Manifest Rerouting](#)
- **Behavior version:** The v2018-02-27 rule format supports the manifestRerouting behavior v1.0.
- **Rule format status:** [Deprecated, outdated rule format](#)
- **Access:** [Read-write](#)

This behavior works with [adScalerCircuitBreaker](#). It delegates parts of the media delivery workflow, like ad insertion, to other technology partners. Akamai reroutes manifest file requests to partner platforms for processing prior to being delivered. Rerouting simplifies the workflow and improves the media streaming experience.

Option	Type	Description
partner	enum	Set this value to <code>adobe_primetime</code> , which is an external technology partner that provides value added offerings, like advertisement integration, to the requested media objects.
	adobe_primetime	This is currently the only supported value.
username	string	The user name for your Adobe Primetime account.

manualServerPush

- **Property Manager name:** [Manual Server Push](#) [↗]
- **Behavior version:** The `v2018-02-27` rule format supports the `manualServerPush` behavior v1.0.
- **Rule format status:** [Deprecated, outdated rule format](#)
- **Access:** [Read-write](#)

With the `http2` behavior enabled, this loads a specified set of objects into the client browser's cache. To apply this behavior, you should match on a `path` or `filename`.

Option	Type	Description
serverpushlist	string array	Specifies the set of objects to load into the client browser's cache over HTTP2. Each value in the array represents a hostname and full path to the object, such as <code>www.example.com/js/site.js</code> .


mediaAccelerationQuicOptout

- **Property Manager name:** [Media Acceleration \(QUIC Protocol\) Opt-Out](#) [↗]
- **Behavior version:** The `v2018-02-27` rule format supports the `mediaAccelerationQuicOptout` behavior v1.0.
- **Rule format status:** [Deprecated, outdated rule format](#)
- **Access:** [Read-write](#)

When enabled, disables use of QUIC protocol for this set of accelerated media content.

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


mediaAcceleration

- **Property Manager name:** [Media Acceleration](#) 
- **Behavior version:** The v2018-02-27 rule format supports the `mediaAcceleration` behavior v1.1.
- **Rule format status:** [Deprecated, outdated rule format](#)
- **Access:** [Read-write](#)

Enables Accelerated Media Delivery for this set of requests.

Option	Type	Description
<code>enabled</code>	boolean	Enables Media Acceleration.


mediaClient

- **Property Manager name:** [Media Client](#) 
- **Behavior version:** The v2018-02-27 rule format supports the `mediaClient` behavior v1.1.
- **Rule format status:** [Deprecated, outdated rule format](#)
- **Access:** [Read-write](#)

Enables client-side reporting through analytics beacon requests.

Option	Type	Description
<code>enabled</code>	boolean	Enables client-side download analytics.
<code>beaconId</code>	string	Specifies the ID of data source's beacon.
<code>useHybridHttpUdp</code>	boolean	Enables the hybrid HTTP/UDP protocol.

mediaFileRetrievalOptimization

- **Property Manager name:** [Media File Retrieval Optimization](#) 
- **Behavior version:** The v2018-02-27 rule format supports the `mediaFileRetrievalOptimization` behavior v1.1.
- **Rule format status:** [Deprecated, outdated rule format](#)
- **Access:** [Read-write](#)

Media File Retrieval Optimization (MFRO) speeds the delivery of large media files by relying on caches of partial objects. You should use it for files larger than 100 MB. It's required for files

larger than 1.8 GB, and works best with [NetStorage](#)[↗]. To apply this behavior, you should match on a [fileExtension](#) .

Option	Type	Description
enabled	boolean	Enables the partial-object caching behavior.

mediaOriginFailover

- **Property Manager name:** [Media Origin Failover](#)[↗]
- **Behavior version:** The `v2018-02-27` rule format supports the `mediaOriginFailover` behavior v1.0.
- **Rule format status:** [Deprecated, outdated rule format](#)
- **Access:** [Read-write](#)

Specifies how edge servers respond when the origin is unresponsive, or suffers from server or content errors. You can specify how many times to retry, switch to a backup origin hostname, or configure a redirect.

Option	Type	Description	Requires
detectOriginUnresponsive	boolean	Allows you to configure what happens when the origin is unresponsive.	
originUnresponsiveDetectionLevel	enum	Specify the level of response to slow origin connections.	detectOriginUnresponsive is true
	AGGRESSIVE	Aggressive response.	
	CONSERVATIVE	Conservative response.	
	MODERATE	Moderate response.	
originUnresponsiveBlacklistOriginIp	boolean	Enabling this blacklists the origin's IP address.	detectOriginUnresponsive is true
originUnresponsiveBlacklistWindow	enum	This sets the delay before blacklisting an IP address.	originUnresponsiveBlacklistOriginIp is true
	TEN_S	10 seconds.	
	THIRTY_S	30 seconds.	
originUnresponsiveRecovery	enum	This sets the recovery option.	detectOriginUnresponsive is true
	RETRY_X_TIMES	Retry.	
	SWITCH_TO_BACKUP_ORIGIN	Switch to a backup origin.	
	REDIRECT_TO_DIFFERENT_ORIGIN_LOCATION	Redirect to a different origin.	

Option	Type	Description	Requires
origin Unresponsive RetryLimit	enum	Sets how many times to retry.	originUnresponsiveRecovery is RETRY_X_TIMES
		Supported values: ONE THREE	
origin Unresponsive BackupHost	string	This specifies the origin hostname.	originUnresponsiveRecovery is SWITCH_TO_BACKUP_ORIGIN
origin Unresponsive AlternateHost	string	This specifies the redirect's destination hostname.	originUnresponsiveRecovery is REDIRECT_TO_DIFFERENT_ORIGIN_ LOCATION
origin Unresponsive ModifyRequest Path	boolean	Modifies the request path.	originUnresponsiveRecovery is SWITCH_TO_BACKUP_ORIGIN OR originUnresponsiveRecovery is REDIRECT_TO_DIFFERENT_ORIGIN_ LOCATION
origin Unresponsive ModifiedPath	string	This specifies the path to form the new URL.	originUnresponsiveModifyRequest Path is true
origin Unresponsive IncludeQuery String	boolean	Enabling this includes the original set of query parameters.	originUnresponsiveModifyRequest Path is true
origin Unresponsive RedirectMethod	enum	Specifies the redirect response code.	originUnresponsiveRecovery is REDIRECT_TO_DIFFERENT_ORIGIN_ LOCATION
		Supported values: 301 302	
origin Unresponsive ChangeProtocol	boolean	This allows you to change the request protocol.	originUnresponsiveRecovery is SWITCH_TO_BACKUP_ORIGIN OR originUnresponsiveRecovery is REDIRECT_TO_DIFFERENT_ORIGIN_ LOCATION
origin Unresponsive Protocol	enum	Specifies which protocol to use.	originUnresponsiveChangeProtocol is true
		Supported values: HTTP HTTPS	
detectOrigin Unavailable	boolean	Allows you to configure failover settings when the origin server responds with errors.	
origin Unavailable DetectionLevel	enum	Specify RESPONSE_CODES , the only available option.	detectOriginUnavailable is true
	RESPONSE_CODES	This is the only value currently available.	
origin Unavailable ResponseCodes	string array	Specifies the set of response codes identifying when the origin responds with errors.	detectOriginUnavailable is true
origin Unavailable BlacklistOriginIp	boolean	Enabling this blacklists the origin's IP address.	detectOriginUnavailable is true

Option	Type	Description	Requires
origin Unavailable BlacklistWindow	enum	This sets the delay before blacklisting an IP address.	originUnavailableBlacklistOriginIp is true
	TEN_S	10 seconds.	
	THIRTY_S	30 seconds.	
origin Unavailable Recovery	enum	This sets the recovery option.	detectOriginUnavailable is true
	RETRY_X_TIMES	Retry.	
	SWITCH_TO_BACKUP_ORIGIN	Switch to a backup origin.	
	REDIRECT_TO_DIFFERENT_ORIGIN_LOCATION	Redirect to a different origin.	
origin UnavailableRetry Limit	enum	Sets how many times to retry.	originUnavailableRecovery is RETRY_X_TIMES
		Supported values: ONE THREE	
origin Unavailable BackupHost	string	This specifies the origin hostname.	originUnavailableRecovery is SWITCH_TO_BACKUP_ORIGIN
origin Unavailable AlternateHost	string	This specifies the redirect's destination hostname.	originUnavailableRecovery is REDIRECT_TO_DIFFERENT_ORIGIN_LOCATION
origin Unavailable ModifyRequest Path	boolean	Modifies the request path.	originUnavailableRecovery is SWITCH_TO_BACKUP_ORIGIN OR originUnavailableRecovery is REDIRECT_TO_DIFFERENT_ORIGIN_LOCATION
origin Unavailable ModifiedPath	string	This specifies the path to form the new URL.	originUnavailableModifyRequestPath is true
origin Unavailable IncludeQuery String	boolean	Enabling this includes the original set of query parameters.	originUnavailableModifyRequestPath is true
origin Unavailable RedirectMethod	enum	Specifies either a redirect response code.	originUnavailableRecovery is REDIRECT_TO_DIFFERENT_ORIGIN_LOCATION
		Supported values: 301 302	
origin Unavailable ChangeProtocol	boolean	Modifies the request protocol.	originUnavailableRecovery is SWITCH_TO_BACKUP_ORIGIN OR originUnavailableRecovery is REDIRECT_TO_DIFFERENT_ORIGIN_LOCATION
origin Unavailable Protocol	enum	Specifies either the HTTP or HTTPS protocol.	originUnavailableChangeProtocol is true

Option	Type	Description	Requires
		Supported values: <div>HTTP HTTPS</div>	
detectObjectUnavailable	boolean	Allows you to configure failover settings when the origin has content errors.	
objectUnavailableDetectionLevel	enum	Specify <code>RESPONSE_CODES</code> , the only available option.	detectObjectUnavailable is true
	<code>RESPONSE_CODES</code>	This is the only value currently available.	
objectUnavailableResponseCodes	string array	Specifies the set of response codes identifying when there are content errors.	detectObjectUnavailable is true
objectUnavailableBlacklistOriginIp	boolean	Enabling this blacklists the origin's IP address.	detectObjectUnavailable is true
objectUnavailableBlacklistWindow	enum	This sets the delay before blacklisting an IP address.	objectUnavailableBlacklistOriginIp is true
	<code>TEN_S</code>	10 seconds.	
	<code>THIRTY_S</code>	30 seconds.	
objectUnavailableRecovery	enum	This sets the recovery option.	detectObjectUnavailable is true
	<code>RETRY_X_TIMES</code>	Retry.	
	<code>SWITCH_TO_BACKUP_ORIGIN</code>	Switch to a backup origin.	
	<code>REDIRECT_TO_DIFFERENT_ORIGIN_LOCATION</code>	Redirect to a different origin.	
objectUnavailableRetryLimit	enum	Sets how many times to retry.	objectUnavailableRecovery is <code>RETRY_X_TIMES</code>
		Supported values: <div>ONE THREE</div>	
objectUnavailableBackupHost	string	This specifies the origin hostname.	objectUnavailableRecovery is <code>SWITCH_TO_BACKUP_ORIGIN</code>
objectUnavailableAlternateHost	string	This specifies the redirect's destination hostname.	objectUnavailableRecovery is <code>REDIRECT_TO_DIFFERENT_ORIGIN_LOCATION</code>
objectUnavailableModifyRequestPath	boolean	Enabling this allows you to modify the request path.	objectUnavailableRecovery is <code>SWITCH_TO_BACKUP_ORIGIN</code> OR objectUnavailableRecovery is <code>REDIRECT_TO_DIFFERENT_ORIGIN_LOCATION</code>
objectUnavailableModifiedPath	string	This specifies the path to form the new URL.	objectUnavailableModifyRequestPath is true

Option	Type	Description	Requires
object Unavailable IncludeQuery String	boolean	Enabling this includes the original set of query parameters.	objectUnavailableModifyRequestPath is true
object Unavailable RedirectMethod	enum	Specifies a redirect response code.	objectUnavailableRecovery is REDIRECT_TO_DIFFERENT_ORIGIN_LOCATION
		Supported values: 301 302	
object Unavailable ChangeProtocol	boolean	Changes the request protocol.	objectUnavailableRecovery is SWITCH_TO_BACKUP_ORIGIN OR objectUnavailableRecovery is REDIRECT_TO_DIFFERENT_ORIGIN_LOCATION
object Unavailable Protocol	enum	Specifies either the HTTP or HTTPS protocol.	objectUnavailableChangeProtocol is true
		Supported values: HTTP HTTPS	
clientResponse Code	string	Specifies the response code served to the client.	
cacheError Response	boolean	When enabled, caches the error response.	
cacheWindow	enum	This sets error response's TTL.	cacheErrorResponse is true
	ONE_S	1 second.	
	TEN_S	10 seconds.	
	THIRTY_S	30 seconds.	

mobileSdkPerformance

- **Property Manager name:** [Mobile App Performance SDK](#)
- **Behavior version:** The v2018-02-27 rule format supports the mobileSdkPerformance behavior v1.0.
- **Rule format status:** [Deprecated, outdated rule format](#)
- **Access:** [Read-write](#)

The Mobile Application Performance software development kit allows you to optimize native iOS and Android apps, effectively extending Akamai's intelligent edge platform's advantages to mobile devices operation in poor network conditions. This behavior enables the SDK's features for this set of requests.

Option	Type	Description
enabled	boolean	Enables the Mobile App Performance SDK.

Option	Type	Description
secondaryMultipathToOrigin	boolean	When enabled, sends secondary multi-path requests to the origin server.

modifyIncomingRequestHeader

- **Property Manager name:** [Modify Incoming Request Header](#) [↗]
- **Behavior version:** The v2018-02-27 rule format supports the `modifyIncomingRequestHeader` behavior v1.2.
- **Rule format status:** [Deprecated, outdated rule format](#)
- **Access:** [Read-write](#)

Modify, add, remove, or pass along specific request headers coming upstream from the client.


Depending on the type of `action` you want to perform, specify the corresponding *standard* header name, or a `customHeaderName` if the standard name is set to `OTHER`. The `headerValue` serves as a match condition when the action is `DELETE` or `MODIFY`, and the `newHeaderValue` applies when the action is `ADD` or `MODIFY`.

See also [modifyIncomingResponseHeader](#), [modifyOutgoingRequestHeader](#), and [modifyOutgoingResponseHeader](#).

Option	Type	Description	Requires
<code>action</code>	enum	Either <code>ADD</code> , <code>DELETE</code> , <code>MODIFY</code> , or <code>PASS</code> incoming HTTP request headers.	
	<code>ADD</code>	Add the header.	
	<code>DELETE</code>	Delete the header.	
	<code>MODIFY</code>	Modify the header.	
	<code>PASS</code>	Pass through the header.	
<code>standardAddHeaderName</code>	enum	If the value of <code>action</code> is <code>ADD</code> , this specifies the name of the field to add.	<code>action</code> is <code>ADD</code>
	<code>ACCEPT_ENCODING</code>	Add an <code>Accept-Encoding</code> header.	
	<code>ACCEPT_LANGUAGE</code>	Add an <code>Accept-Language</code> header.	
	<code>OTHER</code>	Specify another header to add.	
<code>standardDeleteHeaderName</code>	enum	If the value of <code>action</code> is <code>DELETE</code> , this specifies the name of the field to remove.	<code>action</code> is <code>DELETE</code>
	<code>IF_MODIFIED_SINCE</code>	The <code>If-Modified-Since</code> header.	
	<code>VIA</code>	The <code>Via</code> header.	
	<code>OTHER</code>	Specify another header to remove.	

Option	Type	Description	Requires
standard ModifyHeader Name	enum	If the value of <code>action</code> is <code>MODIFY</code> , this specifies the name of the field to modify.	<code>action</code> is <code>MODIFY</code>
	<code>ACCEPT_ENCODING</code>	Add an <code>Accept-Encoding</code> header.	
	<code>ACCEPT_LANGUAGE</code>	Add an <code>Accept-Language</code> header.	
	<code>OTHER</code>	Specify another header to add.	
standardPass HeaderName	enum	If the value of <code>action</code> is <code>PASS</code> , this specifies the name of the field to pass through.	<code>action</code> is <code>PASS</code>
	<code>ACCEPT_ENCODING</code>	Add an <code>Accept-Encoding</code> header.	
	<code>ACCEPT_LANGUAGE</code>	Add an <code>Accept-Language</code> header.	
	<code>OTHER</code>	Specify another header to add.	
custom HeaderName	string (allows variables)	Specifies a custom field name that applies when the relevant <i>standard</i> header name is set to <code>OTHER</code> .	<code>standardAddHeaderName</code> is <code>OTHER</code> OR <code>standardDeleteHeaderName</code> is <code>OTHER</code> OR <code>standardModifyHeaderName</code> is <code>OTHER</code> OR <code>standardPassHeaderName</code> is <code>OTHER</code>
<code>headerValue</code>	string (allows variables)	Specifies the new header value.	<code>action</code> is <code>ADD</code>
<code>newHeaderValue</code>	string (allows variables)	Supplies an HTTP header replacement value.	<code>action</code> is <code>MODIFY</code>
<code>avoidDuplicateHeaders</code>	boolean	When enabled with the <code>action</code> set to <code>MODIFY</code> , prevents creation of more than one instance of a header.	<code>action</code> is <code>MODIFY</code>

modifyIncomingResponseHeader

- **Property Manager name:** [Modify Incoming Response Header](#) 
- **Behavior version:** The `v2018-02-27` rule format supports the `modifyIncomingResponseHeader` behavior v1.2.
- **Rule format status:** [Deprecated, outdated rule format](#)
- **Access:** [Read-write](#)

Modify, add, remove, or pass along specific response headers coming downstream from the origin.

Depending on the type of `action` you want to perform, specify the corresponding *standard* header name, or a `customHeaderName` if the standard name is set to `OTHER` . The `headerValue` serves as a match condition when the action is `DELETE` or `MODIFY` , and the `newHeaderValue` applies when the action is `ADD` or `MODIFY` .

See also [modifyIncomingRequestHeader](#) , [modifyOutgoingRequestHeader](#) , and [modifyOutgoingResponseHeader](#) .

Option	Type	Description	Requires
<code>action</code>	enum	Either <code>ADD</code> , <code>DELETE</code> , <code>MODIFY</code> , or <code>PASS</code> incoming HTTP response headers.	
	<code>ADD</code>	Add the header.	
	<code>DELETE</code>	Delete the header.	
	<code>MODIFY</code>	Modify the header.	
	<code>PASS</code>	Pass through the header.	
<code>standardAddHeaderName</code>	enum	If the value of <code>action</code> is <code>ADD</code> , this specifies the name of the field to add.	<code>action</code> is <code>ADD</code>
	<code>CACHE_CONTROL</code>	The <code>Cache-Control</code> header.	
	<code>CONTENT_TYPE</code>	The <code>Content-Type</code> header.	
	<code>EDGE_CONTROL</code>	The <code>Edge-Control</code> header.	
	<code>EXPIRES</code>	The <code>Expires</code> header.	
	<code>LAST_MODIFIED</code>	The <code>Last-Modified</code> header.	
	<code>OTHER</code>	Specify another header to add.	
<code>standardDeleteHeaderName</code>	enum	If the value of <code>action</code> is <code>DELETE</code> , this specifies the name of the field to remove.	<code>action</code> is <code>DELETE</code>
	<code>CACHE_CONTROL</code>	The <code>Cache-Control</code> header.	
	<code>CONTENT_TYPE</code>	The <code>Content-Type</code> header.	
	<code>VARY</code>	The <code>Vary</code> header.	
	<code>OTHER</code>	Specify another header to remove.	
<code>standardModifyHeaderName</code>	enum	If the value of <code>action</code> is <code>MODIFY</code> , this specifies the name of the field to modify.	<code>action</code> is <code>MODIFY</code>
	<code>CACHE_CONTROL</code>	The <code>Cache-Control</code> header.	
	<code>CONTENT_TYPE</code>	The <code>Content-Type</code> header.	
	<code>EDGE_CONTROL</code>	The <code>Edge-Control</code> header.	
	<code>OTHER</code>	Specify another header to modify.	
<code>standardPassHeaderName</code>	enum	If the value of <code>action</code> is <code>PASS</code> , this specifies the name of the field to pass through.	<code>action</code> is <code>PASS</code>
	<code>CACHE_CONTROL</code>	Pass through the <code>Cache-Control</code> header.	
	<code>EXPIRES</code>	Pass through the <code>Expires</code> header.	
	<code>PRAGMA</code>	Pass through the <code>Pragma</code> header.	
	<code>OTHER</code>	Specify another header to pass.	

Option	Type	Description	Requires
custom HeaderName	string (allows variables)	Specifies a custom field name that applies when the relevant <i>standard</i> header name is set to <code>OTHER</code> .	standardAddHeader Name is <code>OTHER</code> OR standardDelete HeaderName is <code>OTHER</code> OR standardModify HeaderName is <code>OTHER</code> OR standardPass HeaderName is <code>OTHER</code>
headerValue	string (allows variables)	Specifies the header's new value.	action is <code>ADD</code>
newHeader Value	string (allows variables)	Specifies an HTTP header replacement value.	action is <code>MODIFY</code>
avoid Duplicate Headers	boolean	When enabled with the <code>action</code> set to <code>MODIFY</code> , prevents creation of more than one instance of a header.	action is <code>MODIFY</code>

modifyOutgoingRequestHeader

- **Property Manager name:** [Modify Outgoing Request Header](#) [↗]
- **Behavior version:** The `v2018-02-27` rule format supports the `modifyOutgoingRequestHeader` behavior v1.2.
- **Rule format status:** [Deprecated, outdated rule format](#)
- **Access:** [Read-write](#)

Modify, add, remove, or pass along specific request headers going upstream towards the origin.

Depending on the type of `action` you want to perform, specify the corresponding *standard* header name, or a `customHeaderName` if the standard name is set to `OTHER` . The `headerValue` serves as a match condition when the action is `DELETE` or `MODIFY` , and the `newHeaderValue` applies when the action is `ADD` or `MODIFY` . Whole-text replacements apply when the action is `MODIFY` , and substitutions apply when set to `REGEX` .

See also [modifyIncomingRequestHeader](#) , [modifyIncomingResponseHeader](#) , and [modifyOutgoingResponseHeader](#) .

Option	Type	Description	Requires
action	enum	Either <code>ADD</code> or <code>DELETE</code> outgoing HTTP request headers, <code>MODIFY</code> their fixed values, or specify a <code>REGEX</code> pattern to transform them.	
	<code>ADD</code>	Add the header.	
	<code>DELETE</code>	Delete the header.	
	<code>MODIFY</code>	Modify the header.	
	<code>REGEX</code>	Specify another header to modify.	

Option	Type	Description	Requires
standard AddHeader Name	enum	If the value of <code>action</code> is <code>ADD</code> , this specifies the name of the field to add.	<code>action</code> is <code>ADD</code>
	<code>USER_AGENT</code>	The <code>User-Agent</code> header.	
	<code>OTHER</code>	Specify another header to add.	
standard Delete Header Name	enum	If the value of <code>action</code> is <code>DELETE</code> , this specifies the name of the field to remove.	<code>action</code> is <code>DELETE</code>
	<code>PRAGMA</code>	The <code>Pragma</code> header.	
	<code>USER_AGENT</code>	The <code>User-Agent</code> header.	
	<code>VIA</code>	The <code>Via</code> header.	
	<code>OTHER</code>	Specify another header to remove.	
standard Modify Header Name	enum	If the value of <code>action</code> is <code>MODIFY</code> or <code>REGEX</code> , this specifies the name of the field to modify.	<code>action</code> is <code>MODIFY</code> OR <code>action</code> is <code>REGEX</code>
	<code>USER_AGENT</code>	The <code>User-Agent</code> header.	
	<code>OTHER</code>	Specify another header to modify.	
custom Header Name	string (allows variables)	Specifies a custom field name that applies when the relevant <i>standard</i> header name is set to <code>OTHER</code> .	<code>standardAddHeaderName</code> is <code>OTHER</code> OR <code>standardDeleteHeaderName</code> is <code>OTHER</code> OR <code>standardModifyHeaderName</code> is <code>OTHER</code>
header Value	string (allows variables)	Specifies the new header value.	<code>action</code> is <code>ADD</code>
new Header Value	string (allows variables)	Specifies an HTTP header replacement value.	<code>action</code> is <code>MODIFY</code>
regex Header Match	string (allows variables)	Specifies a Perl-compatible regular expression to match within the header value.	<code>action</code> is <code>REGEX</code>
regex Header Replace	string (allows variables)	Specifies text that replaces the <code>regexHeaderMatch</code> pattern within the header value.	<code>action</code> is <code>REGEX</code>
match Multiple	boolean	When enabled with the <code>action</code> set to <code>REGEX</code> , replaces all occurrences of the matched regular expression, otherwise only the first match if disabled.	<code>action</code> is <code>REGEX</code>
avoid Duplicate Headers	boolean	When enabled with the <code>action</code> set to <code>MODIFY</code> , prevents creation of more than one instance of a header.	<code>action</code> is <code>MODIFY</code>

modifyOutgoingResponseHeader

- **Property Manager name:** [Modify Outgoing Response Header](#)¹
- **Behavior version:** The `v2018-02-27` rule format supports the `modifyOutgoingResponseHeader` behavior v1.2.
- **Rule format status:** [Deprecated, outdated rule format](#)
- **Access:** [Read-write](#)

Modify, add, remove, or pass along specific response headers going downstream towards the client.

Depending on the type of `action` you want to perform, specify the corresponding *standard* header name, or a `customHeaderName` if the standard name is set to `OTHER`. The `headerValue` serves as a match condition when the action is `DELETE` or `MODIFY`, and the `newHeaderValue` applies when the action is `ADD` or `MODIFY`. Whole-text replacements apply when the action is `MODIFY`, and substitutions apply when set to `REGEX`.

See also [modifyIncomingRequestHeader](#), [modifyIncomingResponseHeader](#), and [modifyOutgoingRequestHeader](#)

Option	Type	Description	Requires
<code>action</code>	enum	Either <code>ADD</code> or <code>DELETE</code> outgoing HTTP response headers, <code>MODIFY</code> their fixed values, or specify a <code>REGEX</code> pattern to transform them.	
	<code>ADD</code>	Add the header.	
	<code>DELETE</code>	Delete the header.	
	<code>MODIFY</code>	Modify the header.	
	<code>REGEX</code>	Specify another header to modify.	
<code>standardAddHeaderName</code>	enum	If the value of <code>action</code> is <code>ADD</code> , this specifies the name of the field to add.	<code>action</code> is <code>ADD</code>
	<code>CACHE_CONTROL</code>	The <code>Cache-Control</code> header.	
	<code>CONTENT_DISPOSITION</code>	The <code>Content-Disposition</code> header.	
	<code>CONTENT_TYPE</code>	The <code>Content-Type</code> header.	
	<code>EDGE_CONTROL</code>	The <code>Edge-Control</code> header.	
	<code>P3P</code>	Specify another header to add.	
	<code>PRAGMA</code>	The <code>Pragma</code> header.	
	<code>ACCESS_CONTROL_ALLOW_ORIGIN</code>	The <code>Access-Control-Allow-Origin</code> header.	
	<code>ACCESS_CONTROL_ALLOW_METHODS</code>	The <code>Access-Control-Allow-Methods</code> header.	
	<code>ACCESS_CONTROL_ALLOW_HEADERS</code>	The <code>Access-Control-Allow-Headers</code> header.	
	<code>ACCESS_CONTROL_EXPOSE_HEADERS</code>	The <code>Access-Control-Expose-Headers</code> header.	

Option	Type	Description	Requires
	ACCESS_CONTROL_ALLOW_CREDENTIALS	The Access-Control-Allow-Credentials header.	
	ACCESS_CONTROL_MAX_AGE	The Access-Control-Max-Age header.	
	OTHER	Specify another header to add.	
standard Delete Header Name	enum	If the value of action is DELETE , this specifies the name of the field to remove.	action is DELETE
	CACHE_CONTROL	The Cache-Control header.	
	CONTENT_DISPOSITION	The Content-Disposition header.	
	CONTENT_TYPE	The Content-Type header.	
	EXPIRES	The Expires header.	
	P3P	The P3P header.	
	PRAGMA	The Pragma header.	
	ACCESS_CONTROL_ALLOW_ORIGIN	The Access-Control-Allow-Origin header.	
	ACCESS_CONTROL_ALLOW_METHODS	The Access-Control-Allow-Methods header.	
	ACCESS_CONTROL_ALLOW_HEADERS	The Access-Control-Allow-Headers header.	
	ACCESS_CONTROL_EXPOSE_HEADERS	The Access-Control-Expose-Headers header.	
	ACCESS_CONTROL_ALLOW_CREDENTIALS	The Access-Control-Allow-Credentials header.	
	ACCESS_CONTROL_MAX_AGE	The Access-Control-Max-Age header.	
	OTHER	Specify another header to remove.	
standard Modify Header Name	enum	If the value of action is MODIFY or REGEX , this specifies the name of the field to modify.	action is MODIFY OR action is REGEX
	CACHE_CONTROL	The Cache-Control header.	
	CONTENT_DISPOSITION	The Content-Disposition header.	
	CONTENT_TYPE	The Content-Type header.	
	P3P	The P3P header.	
	PRAGMA	The Pragma header.	
	ACCESS_CONTROL_ALLOW_ORIGIN	The Access-Control-Allow-Origin header.	
	ACCESS_CONTROL_ALLOW_METHODS	The Access-Control-Allow-Methods header.	
	ACCESS_CONTROL_ALLOW_HEADERS	The Access-Control-Allow-Headers header.	

Option	Type	Description	Requires
	ACCESS_CONTROL_EXPOSE_HEADERS	The <code>Access-Control-Expose-Headers</code> header.	
	ACCESS_CONTROL_ALLOW_CREDENTIALS	The <code>Access-Control-Allow-Credentials</code> header.	
	ACCESS_CONTROL_MAX_AGE	The <code>Access-Control-Max-Age</code> header.	
	OTHER	Specify another header to modify.	
custom Header Name	string (allows variables)	Specifies a custom field name that applies when the relevant <i>standard</i> header name is set to <code>OTHER</code> .	<code>standardAddHeaderName</code> is <code>OTHER</code> OR <code>standardDeleteHeaderName</code> is <code>OTHER</code> OR <code>standardModifyHeaderName</code> is <code>OTHER</code>
header Value	string (allows variables)	Specifies the existing value of the header to match.	<code>action</code> is <code>ADD</code>
new Header Value	string (allows variables)	Specifies the new HTTP header replacement value.	<code>action</code> is <code>MODIFY</code>
regex Header Match	string	Specifies a Perl-compatible regular expression to match within the header value.	<code>action</code> is <code>REGEX</code>
regex Header Replace	string (allows variables)	Specifies text that replaces the <code>regexHeaderMatch</code> pattern within the header value.	<code>action</code> is <code>REGEX</code>
match Multiple	boolean	When enabled with the <code>action</code> set to <code>REGEX</code> , replaces all occurrences of the matched regular expression, otherwise only the first match if disabled.	<code>action</code> is <code>REGEX</code>
avoid Duplicate Headers	boolean	When enabled with the <code>action</code> set to <code>MODIFY</code> , prevents creation of more than one instance of a header. The last header clobbers others with the same name. This option affects the entire set of outgoing headers, and is not confined to the subset of regular expression matches.	<code>action</code> is <code>MODIFY</code>


netSession

- **Property Manager name:** [NetSession](#) [↗]
- **Behavior version:** The `v2018-02-27` rule format supports the `netSession` behavior v1.1.
- **Rule format status:** [Deprecated, outdated rule format](#)
- **Access:** [Read-write](#)

Deprecated This behavior enables various features of NetSession, a client-side download manager application that's especially appropriate for large file downloads. For the feature to work, the end user needs to download the DLM client.

Option	Type	Description
enabled	boolean	Enables NetSession DLM capabilities for this content.
enable Domain	boolean	Enables Download Manager domains.
enable Download Manager	boolean	When enabled, launches files once they are fully downloaded. For example, specify this option to run an executable application.
enable Download Clients	boolean	Allows download clients to form a peer-to-peer network to reduce transmission time.
disable Reporting	boolean	Disable download state reporting via HTTP beacon messages. Otherwise when enabled, you can view the state of each download by choosing Monitor <> Download Analytics on the DLM client.
resumeUrl	string array	Specify an alternate domain from which to resume a paused download. This generates a corresponding shortcut link on the end user's desktop that disappears after the download is complete.
organization Name	string	The name of the organization that displays in the NetSession client DLM interface.
supportUrl	string	A supporting link to the <code>organizationName</code> that displays in the NetSession client DLM interface.

networkConditionsHeader

- **Property Manager name:** [Network Conditions Header](#) 
- **Behavior version:** The `v2018-02-27` rule format supports the `networkConditionsHeader` behavior v1.1.
- **Rule format status:** [Deprecated, outdated rule format](#)
- **Access:** [Read-write](#)

Instructs edge servers to send an `X-Akamai-Network-Condition` header to the origin assessing the quality of the network.

Option	Type	Description
behavior	enum	Specifies either two or three quality levels.
	TWO_TIER	The assessment is either <code>Excellent</code> or <code>Poor</code> .
	THREE_TIER	The assessment can also be <code>Fair</code> .

origin

- **Property Manager name:** [Origin Server](#)[↗]
- **Behavior version:** The v2018-02-27 rule format supports the `origin` behavior v1.17.
- **Rule format status:** [Deprecated, outdated rule format](#)
- **Access:** [Read-write](#)

Specify the hostname and settings used to contact the origin once service begins. You can use your own origin, [NetStorage](#)[↗], an Edge Load Balancing origin, or a SaaS dynamic origin.

Option	Type	Description	Requires
<code>originType</code>	enum	Choose where your content is retrieved from.	
	CUSTOMER	From your own server.	
	NET_STORAGE	From your NetStorage [↗] account. This option is most appropriate for static content.	
	MEDIA_SERVICE_LIVE	From a Media Services Live origin.	
	EDGE_LOAD_BALANCING_ORIGIN_GROUP	From any available Edge Load Balancing origin.	
	SAAS_DYNAMIC_ORIGIN	From a SaaS dynamic origin if SaaS acceleration is available on your contract.	
<code>netStorage</code>	object	Specifies the details of the NetStorage server.	<code>originType</code> is NET_STORAGE
<code>netStorage.cpCodeList</code>	array	A set of CP codes that apply to this storage group.	
<code>netStorage.downloadDomainName</code>	string	Domain name from which content can be downloaded.	
<code>netStorage.id</code>	number	Unique identifier for the storage group.	
<code>netStorage.name</code>	string	Name of the storage group.	
<code>netStorage.uploadDomainName</code>	string	Domain name used to upload content.	
<code>originId</code>	string	Identifies the Edge Load Balancing origin. This needs to correspond to an edgeLoadBalancingOrigin behavior's <code>id</code> attribute within the same property.	<code>originType</code> is EDGE_LOAD_BALANCING_ORIGIN_GROUP
<code>hostname</code>	string (allows variables)	Specifies the hostname or IPv4 address of your origin server, from which edge servers can retrieve your content.	<code>originType</code> is CUSTOMER
<code>mslorigin</code>	string	This specifies the media's origin server.	<code>originType</code> is MEDIA_SERVICE_LIVE
<code>saasType</code>	enum	Specifies the part of the request that identifies this SaaS dynamic origin.	<code>originType</code> is SAAS_DYNAMIC_ORIGIN

Option	Type	Description	Requires
		Supported values: <div>COOKIE</div>	
saasCname Enabled	boolean	Enabling this allows you to use a <i>CNAME chain</i> to determine the hostname for this SaaS dynamic origin.	saasType is HOSTNAME
saasCname Level	number	Specifies the desired number of hostnames to use in the <i>CNAME chain</i> , starting backwards from the edge server.	saasCname Enabled is true
saasCookie	string	Specifies the name of the cookie that identifies this SaaS dynamic origin.	saasType is COOKIE
saasQueryString	string	Specifies the name of the query parameter that identifies this SaaS dynamic origin.	saasType is QUERY_STRING
saasRegex	string	Specifies the Perl-compatible regular expression match that identifies this SaaS dynamic origin.	originType is SAAS_DYNAMIC_ORIGIN
saasReplace	string	Specifies replacement text for what <code>saasRegex</code> matches.	originType is SAAS_DYNAMIC_ORIGIN
saasSuffix	string	Specifies the static part of the SaaS dynamic origin.	originType is SAAS_DYNAMIC_ORIGIN
forwardHost Header	enum	When the <code>originType</code> is set to either <code>CUSTOMER</code> or <code>SAAS_DYNAMIC_ORIGIN</code> , this specifies which <code>Host</code> header to pass to the origin.	originType is either: <code>CUSTOMER</code> , <code>SAAS_DYNAMIC_ORIGIN</code>
	REQUEST_HOST_HEADER	Passes the original request's header.	
	ORIGIN_HOSTNAME	Passes the current origin's <code>HOSTNAME</code> .	
	CUSTOM	Passes the value of <code>customForwardHostHeader</code> . Use this option if you want requests handled by different properties to converge on the same cached object.	
customForward HostHeader	string (allows variables)	This specifies the name of the custom host header the edge server should pass to the origin.	forwardHost Header is CUSTOM
cacheKey Hostname	enum	Specifies the hostname to use when forming a cache key.	originType is either: <code>CUSTOMER</code> , <code>SAAS_DYNAMIC_ORIGIN</code>
	REQUEST_HOST_HEADER	Specify when using a virtual server.	
	ORIGIN_HOSTNAME	Specify if your origin server's responses do not depend on the hostname.	
useUniqueCache Key	boolean	With a shared <code>hostname</code> such as provided by Amazon AWS, sets a unique cache key for your content.	

Option	Type	Description	Requires
compress	boolean	Enables <i>gzip</i> compression for non-NetStorage origins.	originType is either: CUSTOMER , EDGE_LOAD_BALANCING_ORIGIN_GROUP , SAAS_DYNAMIC_ORIGIN
enableTrueClientIp	boolean	When enabled on non-NetStorage origins, allows you to send a custom header (the trueClientIpHeader) identifying the IP address of the immediate client connecting to the edge server. This may provide more useful information than the standard X-Forward-For header, which proxies may modify.	originType is either: CUSTOMER , EDGE_LOAD_BALANCING_ORIGIN_GROUP , SAAS_DYNAMIC_ORIGIN
trueClientIpHeader	string	This specifies the name of the field that identifies the end client's IP address, for example True-Client-IP .	enableTrueClientIp is true
trueClientIpClientSetting	boolean	If a client sets the True-Client-IP header, the edge server allows it and passes the value to the origin. Otherwise the edge server removes it and sets the value itself.	enableTrueClientIp is true
verificationMode	enum	For non-NetStorage origins, maximize security by controlling which certificates edge servers should trust.	originType is either: CUSTOMER , EDGE_LOAD_BALANCING_ORIGIN_GROUP , SAAS_DYNAMIC_ORIGIN AND is_secure is true in top-level rule
	PLATFORM_SETTINGS	Trust platform settings.	
	CUSTOM	Only applies if the property is marked as secure. See Secure property requirements for guidance. Under some products, you may also need to enable the <i>Secure Delivery - Customer Cert</i> module. Contact your Akamai representative for details.	
	THIRD_PARTY	When your origin server references certain types of third-party hostname.	
originSni	boolean	For non-NetStorage origins, enabling this adds a Server Name Indication (SNI) header in the SSL request sent to the origin, with the origin hostname as the value. Contact your Akamai representative for more information.	is_secure is true in top-level rule AND originType is either: CUSTOMER , EDGE_LOAD_BALANCING_ORIGIN_GROUP , SAAS_DYNAMIC_ORIGIN AND verificationMode is either: PLATFORM_SETTINGS , CUSTOM , THIRD_PARTY

Option	Type	Description	Requires
customValidCnValues	string array	Specifies values to look for in the origin certificate's Subject Alternate Name or Common Name fields. Specify {{Origin Hostname}} and {{Forward Host Header}} within the text in the order you want them to be evaluated. (Note that these two template items are not the same as in-line variables , which use the same curly-brace syntax.)	verification Mode is CUSTOM
originCertsToHonor	enum	Specifies which certificate to trust.	verification Mode is CUSTOM
	COMBO	May rely on all three other inputs.	
	STANDARD_CERTIFICATE_AUTHORITIES	Any certificate signed by an Akamai-managed authority set.	
	CUSTOM_CERTIFICATE_AUTHORITIES	Any certificate signed by a custom authority set you manage.	
	CUSTOM_CERTIFICATES	Pinned origin server certificates.	
customCertificateAuthorities	object array	Specifies an array of certification objects. Contact your Akamai representative for details on this object's requirements.	originCertsToHonor is either: CUSTOM_CERTIFICATE_AUTHORITIES , COMBO
customCertificates	object array	Specifies an array of certification objects. Contact your Akamai representative for details on this object's requirements.	originCertsToHonor is either: CUSTOM_CERTIFICATES , COMBO
httpPort	number	Specifies the port on your origin server to which edge servers should connect for HTTP requests, customarily 80 .	originType is either: CUSTOMER , SAAS_DYNAMIC_ORIGIN
httpsPort	number	Specifies the port on your origin server to which edge servers should connect for secure HTTPS requests, customarily 443 . This option only applies if the property is marked as secure. See Secure property requirements for guidance.	originType is either: CUSTOMER , SAAS_DYNAMIC_ORIGIN AND is_secure is true in top-level rule

originCharacteristics

- **Property Manager name:** [Origin Characteristics](#) [ⓘ]
- **Behavior version:** The v2018-02-27 rule format supports the originCharacteristics behavior v1.1.
- **Rule format status:** [Deprecated, outdated rule format](#)

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

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

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

Option	Type	Description	Requires
country	enum	Specifies the origin's geographic region.	
	EUROPE	Europe.	
	NORTH_AMERICA	North America.	
	LATIN_AMERICA	Latin America.	
	SOUTH_AMERICA	South America.	
	NORDICS	Northern Europe.	
	ASIA_PACIFIC	Asia and Pacific Islands.	
	OTHER_AMERICAS	Other Americas.	
	OTHER_APJ	Asia, Pacific, Japan.	
	OTHER_EMEA	Europe, Middle East, Africa.	
	AUSTRALIA	Australia.	
	GERMANY	Germany.	
	INDIA	India.	
	ITALY	Italy.	
	JAPAN	Japan.	
	MEXICO	Mexico.	
	TAIWAN	Taiwan.	
	UNITED_KINGDOM	United Kingdom.	
	US_EAST	Eastern United States.	
	US_CENTRAL	Central United States.	
	US_WEST	Western United States.	
	GLOBAL_MULTI_GEO	Global.	
	OTHER	A fallback value.	
	UNKNOWN	Defer this optimization.	
authentication Method	enum	Specifies the authentication method.	
	AUTOMATIC	Use default authentication.	
	SIGNATURE_HEADER_AUTHENTICATION	Available with the Adaptive Media Delivery product.	
	MSL_AUTHENTICATION	Available with the Adaptive Media Delivery product.	

Option	Type	Description	Requires
	GCP	Google Cloud Platform.	
	AWSV4	Amazon Web Services v4.	
encodingVersion	enum	Specifies the version of the encryption algorithm, an integer from 1 to 5 .	authenticationMethod is SIGNATURE_HEADER_AUTHENTICATION
useCustomSignString	boolean	Specifies whether to customize your signed string.	authenticationMethod is SIGNATURE_HEADER_AUTHENTICATION
customSignString	string array	Specifies the data to be encrypted as a series of enumerated variable names. See Built-in system variables for guidance on each.	authenticationMethod is SIGNATURE_HEADER_AUTHENTICATION AND useCustomSignString is true
		Supported values: AK_CLIENT_REAL_IP AK_FILENAME AK_DOMAIN AK_HOSTHEADER AK_EXTENSION AK_METHOD	
secretKey	object array	Specifies the shared secret key.	authenticationMethod is SIGNATURE_HEADER_AUTHENTICATION
nonce	string	Specifies the nonce.	authenticationMethod is SIGNATURE_HEADER_AUTHENTICATION
mslkey	string	Specifies the access key provided by the hosting service.	authenticationMethod is MSL_AUTHENTICATION
mslname	string	Specifies the origin name provided by the hosting service.	authenticationMethod is MSL_AUTHENTICATION
gcsAccessKeyId	string	Specifies the access key ID provided by Google Cloud Platform.	authenticationMethod is GCP
gcsSecretKey	string	Specifies the bucket name for your Google Cloud Platform service.	authenticationMethod is GCP
gcsBucket	string	Specifies the secret key used to compute the signature.	authenticationMethod is GCP
awsv4AccessKeyId	string	Specifies the access key used to compute the signature.	authenticationMethod is AWSV4
awsv4SecretKey	string	Specifies the secret key AWS uses to compute the signature.	authenticationMethod is AWSV4
awsv4Region	string	Specifies the region on the AWS service.	authenticationMethod is AWSV4
awsv4Host	string	Specifies the AWS hostname, with no http:// or https:// prefix.	authenticationMethod is AWSV4
awsv4Service	string	Specifies the AWS service name, the hostname segment that precedes amazon.com .	authenticationMethod is AWSV4

originCharacteristicsWsd

- **Property Manager name:** [Origin Characteristics](#) [↗]
- **Behavior version:** The `v2018-02-27` rule format supports the `originCharacteristicsWsd` behavior v1.0.
- **Rule format status:** [Deprecated, outdated rule format](#)
- **Access:** [Read-write](#)

Specifies characteristics of the origin, for use in Akamai's Wholesale Delivery product.

Option	Type	Description
<code>origintype</code>	enum	Specifies an origin type.
	AZURE	An Azure origin type.
	UNKNOWN	An unknown origin type.

persistentClientConnection

- **Property Manager name:** [Persistent Connections: Client to Edge](#) [↗]
- **Behavior version:** The `v2018-02-27` rule format supports the `persistentClientConnection` behavior v1.1.
- **Rule format status:** [Deprecated, outdated rule format](#)
- **Access:** [Read-only](#)

This behavior activates *persistent connections* between edge servers and clients, which allow for better performance and more efficient use of resources. Compare with the [persistentConnection](#) behavior, which configures persistent connections for the entire journey from origin to edge to client. Contact Akamai Professional Services for help configuring either.

Warning. Disabling or removing this behavior may negatively affect performance.

Option	Type	Description
<code>enabled</code>	boolean	Enables the persistent connections behavior.
<code>timeout</code>	string (duration)	Specifies the timeout period after which edge server closes the persistent connection with the client, 500 seconds by default.

persistentConnection

- **Property Manager name:** [Persistent Connections: Edge to Origin](#) [↗]
- **Behavior version:** The `v2018-02-27` rule format supports the `persistentConnection` behavior v1.1.


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

This behavior enables more efficient *persistent connections* from origin to edge server to client. Compare with the [persistentClientConnection](#) behavior, which customizes persistent connections from edge to client. Contact Akamai Professional Services for help configuring either.

Warning. Disabling this behavior wastes valuable browser resources. Leaving connections open too long makes them vulnerable to attack. Avoid both of these scenarios.

Option	Type	Description
enabled	boolean	Enables persistent connections.
timeout	string (duration)	Specifies the timeout period after which edge server closes a persistent connection.

personallyIdentifiableInformation


- **Property Manager name:** [Personally Identifiable Information \(PII\)](#) 
- **Behavior version:** The `v2018-02-27` rule format supports the `personallyIdentifiableInformation` behavior v1.1.
- **Rule format status:** [Deprecated, outdated rule format](#)
- **Access:** [Read-write](#)

Marks content covered by the current rule as sensitive *personally identifiable information* that needs to be treated as secure and private. That includes anything involving personal information: name, social security number, date and place of birth, mother's maiden name, biometric data, or any other data linked to an individual. If you attempt to save a property with such a rule that also caches or logs sensitive content, the added behavior results in a validation error.

Warning. This feature only identifies some vulnerabilities. For example, it does not prevent you from including secure information in a query string or writing it to an origin folder. It also can't tell whether the SSL protocol is in effect.

Option	Type	Description
enabled	boolean	When enabled, marks content as personally identifiable information (PII).

phasedRelease


- **Property Manager name:** [Phased Release Cloudlet](#) 
- **Behavior version:** The `v2018-02-27` rule format supports the `phasedRelease` behavior v1.2.
- **Rule format status:** [Deprecated, outdated rule format](#)

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

The Phased Release Cloudlet provides gradual and granular traffic management to an alternate origin in near real time. Use the [Cloudlets API](#) or the Cloudlets Policy Manager application within [Control Center](#) to set up your Cloudlets policies.

Option	Type	Description	Requires
enabled	boolean	Enables the Phased Release Cloudlet.	
cloudlet Policy	object	Specifies the Cloudlet policy as an object.	
cloudlet Policy.id	number	Identifies the Cloudlet.	
cloudlet Policy.name	string	The Cloudlet's descriptive name.	
label	string	A label to distinguish this Phased Release policy from any others within the same property.	
population CookieType	enum	Select when to assign a cookie to the population of users the Cloudlet defines. If you select the Cloudlet's <i>random</i> membership option, it overrides this option's value so that it is effectively <i>NONE</i> .	
	NONE	Do not expire the cookie.	
	NEVER	Never assign a cookie.	
	ON_BROWSER_CLOSE	Once the browser session ends.	
	FIXED_DATE	Specify a time when the cookie expires.	
	DURATION	Specify a delay before the cookie expires.	
population Expiration Date	string (epoch timestamp)	Specifies the date and time when membership expires, and the browser no longer sends the cookie. Subsequent requests re-evaluate based on current membership settings.	population Cookie Type is FIXED_DATE
population Duration	string (duration)	Sets the lifetime of the cookie from the initial request. Subsequent requests re-evaluate based on current membership settings.	population Cookie Type is DURATION
population Refresh	boolean	Enabling this option resets the original duration of the cookie if the browser refreshes before the cookie expires.	population Cookie Type is DURATION
failover Enabled	boolean	Allows failure responses at the origin defined by the Cloudlet to fail over to the prevailing origin defined by the property.	
failover Response Code	string array	Defines the set of failure codes that initiate the failover response.	failover Enabled is true
failover Duration	number (0-300)	Specifies the number of seconds to wait until the client tries to access the failover origin after the initial failure is detected. Set the value to 0 to immediately request the alternate origin upon failure.	failover Enabled is true


preconnect

- **Property Manager name:** [Manual Preconnect](#) 
- **Behavior version:** The `v2018-02-27` rule format supports the `preconnect` behavior v1.0.
- **Rule format status:** [Deprecated, outdated rule format](#)
- **Access:** [Read-write](#)

With the `http2` behavior enabled, this requests a specified set of domains that relate to your property hostname, and keeps the connection open for faster loading of content from those domains.

Option	Type	Description
<code>preconnectlist</code>	string array	Specifies the set of hostnames to which to preconnect over HTTP2.


predictiveContentDelivery

- **Property Manager name:** [Predictive Content Delivery](#) 
- **Behavior version:** The `v2018-02-27` rule format supports the `predictiveContentDelivery` behavior v1.0.
- **Rule format status:** [Deprecated, outdated rule format](#)
- **Access:** [Read-write](#)

Improves user experience and reduces the cost of downloads by enabling mobile devices to predictively fetch and cache content from catalogs managed by Akamai servers. You can't use this feature if in the `segmentedMediaOptimization` behavior, the value for `behavior` is set to `LIVE`.

Option	Type	Description
<code>enabled</code>	boolean	Enables the predictive content delivery behavior.

predictivePrefetching

- **Property Manager name:** [Predictive Prefetching](#) 
- **Behavior version:** The `v2018-02-27` rule format supports the `predictivePrefetching` behavior v1.1.
- **Rule format status:** [Deprecated, outdated rule format](#)
- **Access:** [Read-write](#)

This behavior potentially reduces the client's page load time by pre-caching objects based on historical data for the page, not just its current set of referenced objects. It also detects second-level dependencies, such as objects retrieved by JavaScript.

Option	Type	Description
enabled	boolean	Enables the predictive prefetching behavior.
accuracy Target	enum	The level of prefetching. A higher level results in better client performance, but potentially greater load on the origin.
	LOW	Low.
	MEDIUM	Medium.
	HIGH	High.


prefetch

- **Property Manager name:** [Prefetch Objects](#) 
- **Behavior version:** The v2018-02-27 rule format supports the prefetch behavior v1.1.
- **Rule format status:** [Deprecated, outdated rule format](#)
- **Access:** [Read-write](#)

Instructs edge servers to retrieve content linked from requested pages as they load, rather than waiting for separate requests for the linked content. This behavior applies depending on the rule's set of matching conditions. Use in conjunction with the [prefetchable](#) behavior, which specifies the set of objects to prefetch.

Option	Type	Description
enabled	boolean	Applies prefetching behavior when enabled.

prefetchable

- **Property Manager name:** [Prefetchable Objects](#) 
- **Behavior version:** The v2018-02-27 rule format supports the prefetchable behavior v1.1.
- **Rule format status:** [Deprecated, outdated rule format](#)
- **Access:** [Read-write](#)

Allow matching objects to prefetch into the edge cache as the parent page that links to them loads, rather than waiting for a direct request. This behavior applies depending on the rule's set of matching conditions. Use [prefetch](#) to enable the overall behavior for parent pages that contain links to the object. To apply this behavior, you need to match on a [filename](#) or [fileExtension](#).

Option	Type	Description
enabled	boolean	Allows matching content to prefetch when referenced on a requested parent page.

prefreshCache

- **Property Manager name:** [Cache Prefreshing](#) [↗]
- **Behavior version:** The v2018-02-27 rule format supports the `prefreshCache` behavior v1.1.
- **Rule format status:** [Deprecated, outdated rule format](#)
- **Access:** [Read-write](#)

Refresh cached content before its time-to-live (TTL) expires, to keep end users from having to wait for the origin to provide fresh content.

Prefreshing starts asynchronously based on a percentage of remaining TTL. The edge serves the prefreshed content only after the TTL expires. If the percentage is set too high, and there is not enough time to retrieve the object, the end user waits for it to refresh from the origin, as is true by default without this prefetch behavior enabled. The edge does not serve stale content.

Option	Type	Description
enabled	boolean	Enables the cache prefreshing behavior.
prefreshval	number (0-99)	Specifies when the prefetch occurs as a percentage of the TTL. For example, for an object whose cache has 10 minutes left to live, and an origin response that is routinely less than 30 seconds, a percentage of 95 prefetches the content without unnecessarily increasing load on the origin.

randomSeek

- **Property Manager name:** [Random Seek](#) [↗]
- **Behavior version:** The v2018-02-27 rule format supports the `randomSeek` behavior v1.2.
- **Rule format status:** [Deprecated, outdated rule format](#)
- **Access:** [Read-write](#)

Optimizes `.flv` and `.mp4` files to allow random jump-point navigation.

Option	Type	Description	Requires
flv	boolean	Enables random seek optimization in FLV files.	
mp4	boolean	Enables random seek optimization in MP4 files.	
maximum Size	string	Sets the maximum size of the MP4 file to optimize, expressed as a number suffixed with a unit string such as <code>MB</code> or <code>GB</code> .	<code>mp4</code> is true

rapid

- **Property Manager name:** [Akamai API Gateway](#) [↗]
- **Behavior version:** The `v2018-02-27` rule format supports the `rapid` behavior v1.0.
- **Rule format status:** [Deprecated, outdated rule format](#)
- **Access:** [Read-write](#)

The [Akamai API Gateway](#) [↗] allows you to configure API traffic delivered over the Akamai network. Apply this behavior to a set of API assets, then use Akamai's [API Endpoints API](#) [↗] to configure how the traffic responds. Use the [API Keys and Traffic Management API](#) [↗] to control access to your APIs.

Option	Type	Description
<code>enabled</code>	boolean	Enables API Gateway for the current set of content.

readTimeout

- **Property Manager name:** [Read Timeout](#) [↗]
- **Behavior version:** The `v2018-02-27` rule format supports the `readTimeout` behavior v1.1.
- **Rule format status:** [Deprecated, outdated rule format](#)
- **Access:** [Read-write](#)

This behavior specifies how long the edge server should wait for a response from the requesting forward server after a connection has already been established. Any failure to read aborts the request and sends a `504` Gateway Timeout error to the client. Contact Akamai Professional Services for help configuring this behavior.

Option	Type	Description
<code>value</code>	string (duration)	Specifies the read timeout necessary before failing with a <code>504</code> error. This value should never be zero.

realUserMonitoring

- **Property Manager name:** [Real User Monitoring \(RUM\)](#) [↗]

- **Behavior version:** The `v2018-02-27` rule format supports the `realUserMonitoring` behavior v1.2.
- **Rule format status:** [Deprecated, outdated rule format](#)
- **Access:** [Read-write](#)

Real User Monitoring (RUM) injects JavaScript into HTML pages served to end-user clients that monitors page-load performance and reports on various data, such as browser type and geographic location. The [report](#) behavior allows you to configure logs.

Option	Type	Description
<code>enabled</code>	boolean	When enabled, activates real-use monitoring.

redirect

- **Property Manager name:** [Redirect](#)
- **Behavior version:** The `v2018-02-27` rule format supports the `redirect` behavior v1.4.
- **Rule format status:** [Deprecated, outdated rule format](#)
- **Access:** [Read-write](#)

Respond to the client request with a redirect without contacting the origin. Specify the redirect as a path expression starting with a `/` character relative to the current root, or as a fully qualified URL. This behavior relies primarily on `destinationHostname` and `destinationPath` to manipulate the hostname and path independently.

See also the [redirectplus](#) behavior, which allows you to use [variables](#) more flexibly to express the redirect's destination.

Option	Type	Description	Requires
<code>mobileDefaultChoice</code>	enum	Either specify a default response for mobile browsers, or customize your own.	
	DEFAULT	Allows all other <code>responseCode</code> values.	
	MOBILE	Allows only a 302 response code.	
<code>destinationProtocol</code>	enum	Choose the protocol for the redirect URL.	
	SAME_AS_REQUEST	Pass through the original protocol.	
	HTTP	Use <code>http</code> .	
	HTTPS	Use <code>https</code> .	
<code>destinationHostname</code>	enum	Specify how to change the requested hostname, independently from the pathname.	
	SAME_AS_REQUEST	Preserves the hostname unchanged.	

Option	Type	Description	Requires
	SUBDOMAIN	Prepends a subdomain from the <code>destinationHostnameSubdomain</code> field.	
	SIBLING	Replaces the leftmost subdomain with the <code>destinationHostnameSibling</code> field.	
	OTHER	Specifies a static domain in the <code>destinationHostnameOther</code> field.	
<code>destinationHostnameOther</code>	string (allows variables)	Specifies the full hostname with which to replace the current hostname.	<code>destinationHostname</code> is OTHER
<code>destinationPath</code>	enum	Specify how to change the requested pathname, independently from the hostname.	
	SAME_AS_REQUEST	Preserves the current path unchanged.	
	PREFIX_REQUEST	Prepends a path with the <code>destinationPathPrefix</code> field. You also have the option to specify a suffix using <code>destinationPathSuffix</code> and <code>destinationPathSuffixStatus</code> .	
	OTHER	Replaces the current path with the <code>destinationPathOther</code> field.	
<code>destinationPathPrefix</code>	string (allows variables)	When <code>destinationPath</code> is set to <code>PREFIX_REQUEST</code> , this prepends the current path. For example, a value of <code>/prefix/path</code> changes <code>/example/index.html</code> to <code>/prefix/path/example/index.html</code> .	<code>destinationPath</code> is <code>PREFIX_REQUEST</code>
<code>destinationPathSuffixStatus</code>	enum	When <code>destinationPath</code> is set to <code>PREFIX_REQUEST</code> , this gives you the option of adding a suffix.	<code>destinationPath</code> is <code>PREFIX_REQUEST</code>
	NO_SUFFIX	Specify if you want to preserve the end of the path unchanged.	
	SUFFIX	The <code>destinationPathSuffix</code> provides the value.	
<code>destinationPathSuffix</code>	string (allows variables)	When <code>destinationPath</code> is set to <code>PREFIX_REQUEST</code> and <code>destinationPathSuffixStatus</code> is set to <code>SUFFIX</code> , this specifies the suffix to append to the path.	<code>destinationPathSuffixStatus</code> is <code>SUFFIX</code>
<code>destinationPathOther</code>	string (allows variables)	When <code>destinationPath</code> is set to <code>PREFIX_REQUEST</code> , this replaces the current path.	<code>destinationPath</code> is <code>OTHER</code>
<code>queryString</code>	boolean	When set to <code>APPEND</code> , passes incoming query string parameters as part of the redirect URL. Otherwise set this to <code>IGNORE</code> .	
<code>responseCode</code>	enum	Specify the redirect's response code.	
		Supported values: 301 302 303 307	

redirectplus


- **Property Manager name:** [Redirect Plus](#)
- **Behavior version:** The `v2018-02-27` rule format supports the `redirectplus` behavior v1.2.

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

Respond to the client request with a redirect without contacting the origin. This behavior fills the same need as [redirect](#) , but allows you to use [variables](#) to express the redirect [destination](#) 's component values more concisely.

Option	Type	Description
<code>enabled</code>	boolean	Enables the redirect feature.
<code>destination</code>	string (allows variables)	Specifies the redirect as a path expression starting with a <code>/</code> character relative to the current root, or as a fully qualified URL. Optionally inject variables, as in this example that refers to the original request's filename: <code>/path/to/{{builtin.AK_FILENAME}}</code> .
<code>response Code</code>	enum	Assigns the status code for the redirect response.
		Supported values: <div>301 302 303 307</div>

referrerChecking

- **Property Manager name:** [Legacy Referrer Checking](#) 
- **Behavior version:** The `v2018-02-27` rule format supports the `referrerChecking` behavior v1.1.
- **Rule format status:** [Deprecated, outdated rule format](#)
- **Access:** [Read-write](#)

Limits allowed requests to a set of domains you specify.

Option	Type	Description
<code>enabled</code>	boolean	Enables the referrer-checking behavior.
<code>strict</code>	boolean	When enabled, excludes requests whose <code>Referer</code> header include a relative path, or that are missing a <code>Referer</code> . When disabled, only excludes requests whose <code>Referer</code> hostname is not part of the <code>domains</code> set.
<code>domains</code>	string array	Specifies the set of allowed domains. With <code>allowChildren</code> disabled, prefixing values with <code>*</code> specifies domains for which subdomains are allowed.
<code>allow Children</code>	boolean	Allows all subdomains for the <code>domains</code> set, just like adding a <code>*</code> prefix to each.

removeQueryParameter

- **Property Manager name:** [Remove Outgoing Request Parameters](#) [↗]
- **Behavior version:** The v2018-02-27 rule format supports the removeQueryParam behavior v1.1.
- **Rule format status:** [Deprecated, outdated rule format](#)
- **Access:** [Read-write](#)

Remove named query parameters before forwarding the request to the origin.

Option	Type	Description
parameters	string array	Specifies parameters to remove from the request.

removeVary

- **Property Manager name:** [Remove Vary Header](#) [↗]
- **Behavior version:** The v2018-02-27 rule format supports the removeVary behavior v1.1.
- **Rule format status:** [Deprecated, outdated rule format](#)
- **Access:** [Read-write](#)

By default, responses that feature a Vary header value of anything other than Accept-Encoding and a corresponding Content-Encoding: gzip header aren't cached on edge servers. Vary headers indicate when a URL's content varies depending on some variable, such as which User-Agent requests it. This behavior simply removes the Vary header to make responses cacheable.

Warning. If your site relies on Vary: User-Agent to customize content, removing the header may lead the edge to serve content inappropriate for specific devices.

Option	Type	Description
enabled	boolean	When enabled, removes the Vary header to ensure objects can be cached.

report

- **Property Manager name:** [Log Request Details](#) [↗]
- **Behavior version:** The v2018-02-27 rule format supports the report behavior v1.3.
- **Rule format status:** [Deprecated, outdated rule format](#)
- **Access:** [Read-write](#)

Specify the HTTP request headers or cookie names to log in your Log Delivery Service reports.

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

Option	Type	Description	Requires
logHost	boolean	Log the Host header.	
logReferer	boolean	Log the Referer header.	
logUserAgent	boolean	Log the User-Agent header.	
logAcceptLanguage	boolean	Log the Accept-Language header.	
logCookies	enum	Specifies the set of cookies to log.	
	OFF	Do not log cookies.	
	ALL	Log all cookies.	
	SOME	A specific set of cookies .	
cookies	string array	This specifies the set of cookies names whose values you want to log.	logCookies is SOME
logCustomLogField	boolean	Whether to append additional custom data to each log line.	
customLogField	string (allows variables)	Specifies an additional data field to append to each log line, maximum 40 bytes, typically based on a dynamically generated built-in system variable. For example, round-trip: {{builtin.AK_CLIENT_TURNAROUND_TIME}}ms logs the total time to complete the response. See Support for variables for more information. If you enable the logCustom behavior, it overrides the customLogField option.	logCustomLogField is true

requestControl

- **Property Manager name:** [Request Control Cloudlet](#)
- **Behavior version:** The v2018-02-27 rule format supports the requestControl behavior v3.3.
- **Rule format status:** [Deprecated, outdated rule format](#)
- **Access:** [Read-write](#)

The Request Control Cloudlet allows you to control access to your web content based on the incoming request's IP or geographic location. With Cloudlets available on your contract, choose **Your services <> Edge logic Cloudlets** to control how the feature works within [Control Center](#), or use the [Cloudlets API](#) to configure it programmatically.

Option	Type	Description	Requires
enabled	boolean	Enables the Request Control Cloudlet.	
cloudletPolicy	object	Identifies the Cloudlet policy.	
cloudletPolicy.id	number	Identifies the Cloudlet.	
cloudletPolicy.name	string	The Cloudlet's descriptive name.	

Option	Type	Description	Requires
enableBranded403	boolean	If enabled, serves a branded 403 page for this Cloudlet instance.	
branded403Status Code	enum	Specifies the response status code for the branded deny action.	enableBranded403 is true
		Supported values: <div>200 302 403 503</div>	
netStorage	object	Specifies the NetStorage domain that contains the branded 403 page.	enableBranded403 is true AND branded403Status Code is not 302
netStorage.cp CodeList	array	A set of CP codes that apply to this storage group.	
netStorage.download DomainName	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.upload DomainName	string	Domain name used to upload content.	
branded403File	string	Specifies the full path of the branded 403 page, including the filename, but excluding the NetStorage CP code path component.	enableBranded403 is true AND branded403Status Code is not 302
branded403Url	string	Specifies the redirect URL for the branded deny action.	enableBranded403 is true AND branded403Status Code is 302
brandedDeny CacheTtl	number (5-30)	Specifies the branded response page's time to live in the cache, 5 minutes by default.	enableBranded403 is true AND branded403Status Code is not 302


requestTypeMarker

- **Property Manager name:** [Request Type Marker](#)
- **Behavior version:** The v2018-02-27 rule format supports the requestTypeMarker behavior v1.0.
- **Rule format status:** [Deprecated, outdated rule format](#)
- **Access:** [Read-write](#)

The [Internet of Things: OTA Updates](#) product allows customers to securely distribute firmware to devices over cellular networks. When using the [downloadCompleteMarker](#) behavior to log successful downloads, this related behavior identifies download or campaign server types in aggregated and individual reports.

Option	Type	Description
requestType	enum	Specifies the type of request.
	DOWNLOAD	Download.
	CAMPAIGN_SERVER	Campaign server.


resourceOptimizer

- **Property Manager name:** [Resource Optimizer](#) 
- **Behavior version:** The v2018-02-27 rule format supports the resourceOptimizer behavior v1.1.
- **Rule format status:** [Deprecated, outdated rule format](#)
- **Access:** [Read-write](#)

The Resource Optimizer helps compress and cache web resources such as JavaScript, CSS, and font files.

Option	Type	Description
enabled	boolean	Enables the Resource Optimizer feature.

restrictObjectCaching

- **Property Manager name:** [Object Caching](#) 
- **Behavior version:** The v2018-02-27 rule format supports the restrictObjectCaching behavior v1.2.
- **Rule format status:** [Deprecated, outdated rule format](#)
- **Access:** [Read-only](#)

You need this behavior to deploy the Object Caching product. It disables serving HTML content and limits the maximum object size to 100MB. Contact Akamai Professional Services for help configuring it.

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

responseCode

- **Property Manager name:** [Set Response Code](#)
- **Behavior version:** The v2018-02-27 rule format supports the `responseCode` behavior v1.1.
- **Rule format status:** [Deprecated, outdated rule format](#)
- **Access:** [Read-write](#)

Change the existing response code. For example, if your origin sends a `301` permanent redirect, this behavior can change it on the edge to a temporary `302` redirect.

Option	Type	Description	Requires
<code>statusCode</code>	enum	The HTTP status code to replace the existing one.	
		Supported values: <div> 100 103 201 204 207 301 304 307 401 404 407 410 413 101 122 202 205 226 302 305 308 402 405 408 411 414 102 200 203 206 300 303 306 400 403 406 409 412 415 </div>	
<code>override206</code>	boolean	Allows any specified <code>200</code> success code to override a <code>206</code> partial-content code, in which case the response's content length matches the requested range length.	<code>statusCode</code> is <code>200</code>

responseCookie

- **Property Manager name:** [Set Response Cookie](#)
- **Behavior version:** The v2018-02-27 rule format supports the `responseCookie` behavior v1.2.
- **Rule format status:** [Deprecated, outdated rule format](#)
- **Access:** [Read-write](#)

Set a cookie to send downstream to the client with either a fixed value or a unique stamp.

Option	Type	Description	Requires
<code>cookieName</code>	string (allows variables)	Specifies the name of the cookie, which serves as a key to determine if the cookie is set.	
<code>enabled</code>	boolean	Allows you to set a response cookie.	
<code>type</code>	enum	What type of value to assign.	
	<code>FIXED</code>	Assign a <code>FIXED</code> value based on the <code>value</code> field.	
	<code>UNIQUE</code>	Assign a unique value.	
<code>value</code>	string (allows variables)	If the cookie <code>type</code> is <code>FIXED</code> , this specifies the cookie value.	<code>type</code> is <code>FIXED</code>
<code>format</code>	enum	When the <code>type</code> of cookie is set to <code>UNIQUE</code> , this sets the date format.	<code>type</code> is <code>UNIQUE</code>
	<code>AKAMAI</code>	Akamai format, which adds milliseconds to the date stamp.	
	<code>APACHE</code>	Apache format.	
<code>defaultDomain</code>	boolean	When enabled, uses the default domain value, otherwise the set specified in the <code>domain</code> field.	

Option	Type	Description	Requires
default Path	boolean	When enabled, uses the default path value, otherwise the set specified in the <code>path</code> field.	
domain	string (allows variables)	If the <code>defaultDomain</code> is disabled, this sets the domain for which the cookie is valid. For example, <code>example.com</code> makes the cookie valid for that hostname and all subdomains.	default Domain is false
path	string (allows variables)	If the <code>defaultPath</code> is disabled, sets the path component for which the cookie is valid.	default Path is false
expires	enum	Sets various ways to specify when the cookie expires.	
	ON_BROWSER_CLOSE	Limit the cookie to the duration of the session.	
	FIXED_DATE	Requires a corresponding <code>expirationDate</code> field value.	
	DURATION	Requires a corresponding <code>duration</code> field value.	
	NEVER	Let the cookie persist indefinitely.	
expiration Date	string (epoch timestamp)	If <code>expires</code> is set to <code>FIXED_DATE</code> , this sets when the cookie expires as a UTC date and time.	<code>expires</code> is <code>FIXED_DATE</code>
duration	string (duration)	If <code>expires</code> is set to <code>DURATION</code> , this sets the cookie's lifetime.	<code>expires</code> is <code>DURATION</code>
secure	boolean	When enabled, sets the cookie's <code>Secure</code> flag to transmit it with <code>HTTPS</code> .	

rmaOptimization

- **Property Manager name:** [RMA Optimizations \(RMA\)](#) [↗]
- **Behavior version:** The `v2018-02-27` rule format supports the `rmaOptimization` behavior v1.1.
- **Rule format status:** [Deprecated, outdated rule format](#)
- **Access:** [Read-write](#)

This behavior is deprecated. Do not add it to any properties.

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

rewriteUrl

- **Property Manager name:** [Modify Outgoing Request Path](#) [↗]
- **Behavior version:** The `v2018-02-27` rule format supports the `rewriteUrl` behavior v1.3.
- **Rule format status:** [Deprecated, outdated rule format](#)

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

Modifies the path of incoming requests to forward to the origin. This helps you offload URL-rewriting tasks to the edge to increase the origin server's performance, allows you to redirect links to different targets without changing markup, and hides your original directory structure.

Except for regular expression replacements, this behavior manipulates *path expressions*, which start and end with a `/` character.

Option	Type	Description	Requires
behavior	enum	The action to perform on the path.	
	REPLACE	Specify the <code>match</code> and <code>targetPath</code> . For example, a <code>match</code> of <code>/path1/</code> and a <code>targetPath</code> of <code>/path1/path2/</code> changes <code>/path1/page.html</code> to <code>/path1/path2/page.html</code> .	
	REMOVE	Specify the <code>match</code> . For example, a <code>match</code> of <code>/path2/</code> changes <code>/path1/path2/page.html</code> to <code>/path1/page.html</code> .	
	REWRITE	Specify the <code>targetUrl</code> . For example, you can direct traffic to <code>/error/restricted.html</code> .	
	PREPEND	Specify the <code>targetPathPrepend</code> . For example, if set to <code>/prefix/</code> , <code>/path1/page.html</code> changes to <code>/prefix/path1/page.html</code> .	
	REGEX_REPLACE	Specify the <code>matchRegex</code> and <code>targetRegex</code> . For example, specifying <code>logo\.(png gif jpe?g)</code> and <code>brand\$1</code> changes <code>logo.png</code> to <code>brand.png</code> .	
match	string	When <code>behavior</code> is <code>REMOVE</code> or <code>REPLACE</code> , specifies the part of the incoming path you'd like to remove or modify.	<code>behavior</code> is either: <code>REMOVE</code> , <code>REPLACE</code>
match Regex	string	When <code>behavior</code> is set to <code>REGEX_REPLACE</code> , specifies the Perl-compatible regular expression to replace with <code>targetRegex</code> .	<code>behavior</code> is <code>REGEX_REPLACE</code>
target Regex	string (allows variables)	When <code>behavior</code> is set to <code>REGEX_REPLACE</code> , this replaces whatever the <code>matchRegex</code> field matches, along with any captured sequences from <code>\\$1</code> through <code>\\$9</code> .	<code>behavior</code> is <code>REGEX_REPLACE</code>
target Path	string (allows variables)	When <code>behavior</code> is set to <code>REPLACE</code> , this path replaces whatever the <code>match</code> field matches in the incoming request's path.	<code>behavior</code> is <code>REPLACE</code>
target Path Prepend	string (allows variables)	When <code>behavior</code> is set to <code>PREPEND</code> , specifies a path to prepend to the incoming request's URL.	<code>behavior</code> is <code>PREPEND</code>
target Url	string (allows variables)	When <code>behavior</code> is set to <code>REWRITE</code> , specifies the full path to request from the origin.	<code>behavior</code> is <code>REWRITE</code>
match Multiple	boolean	When enabled, replaces all potential matches rather than only the first.	<code>behavior</code> is either: <code>REMOVE</code> , <code>REPLACE</code> , <code>REGEX_REPLACE</code>
keep Query String	boolean	When enabled, retains the original path's query parameters.	<code>behavior</code> is not <code>REWRITE</code>

rumCustom

- **Property Manager name:** [RUM SampleRate](#)
- **Behavior version:** The v2018-02-27 rule format supports the rumCustom behavior v1.0.
- **Rule format status:** [Deprecated, outdated rule format](#)
- **Access:** [Read-only](#)

With `realUserMonitoring` enabled, this configures the sample of data to include in your RUM report.

Option	Type	Description
rumSampleRate	number (0-100)	Specifies the percentage of web traffic to include in your RUM report.
rumGroupName	string	A deprecated option to specify an alternate name under which to batch this set of web traffic in your report. Do not use it.

saasDefinitions

- **Property Manager name:** [SaaS Definitions](#)
- **Behavior version:** The v2018-02-27 rule format supports the saasDefinitions behavior v3.1.
- **Rule format status:** [Deprecated, outdated rule format](#)
- **Access:** [Read-write](#)

Configures how the Software as a Service feature identifies *customers*, *applications*, and *users*. A different set of options is available for each type of targeted request, each enabled with the `action`-suffixed option. In each case, you can use `PATH`, `COOKIE`, `QUERY_STRING`, or `HOSTNAME` components as identifiers, or `disable` the SaaS behavior for certain targets. If you rely on a `HOSTNAME`, you also have the option of specifying a *CNAME chain* rather than an individual hostname. The various options suffixed `regex` and `replace` subsequently remove the identifier from the request. This behavior requires a sibling `origin` behavior whose `originType` option is set to `SAAS_DYNAMIC_ORIGIN`.

Option	Type	Description	Requires
customerAction	enum	Specifies the request component that identifies a SaaS customer.	
	DISABLED	This effectively ignores customers.	
	HOSTNAME	In a hostname.	
	PATH	In the URL path.	
	QUERY_STRING	In a query parameter.	
	COOKIE	In a cookie.	
customerCnameEnabled	boolean	Enabling this allows you to identify customers using a <i>CNAME chain</i> rather than a single hostname.	customerAction is HOSTNAME
customerCnameLevel	number	Specifies the number of CNAMEs to use in the chain.	customerCnameEnabled is true

Option	Type	Description	Requires
customer Cookie	string	This specifies the name of the cookie that identifies the customer.	customerAction is COOKIE
customer Query String	string	This names the query parameter that identifies the customer.	customerAction is QUERY_STRING
customer Regex	string	Specifies a Perl-compatible regular expression with which to substitute the request's customer ID.	customerAction is either: HOSTNAME , PATH , COOKIE , QUERY_STRING
customer Replace	string	Specifies a string to replace the request's customer ID matched by customerRegex .	customerAction is either: HOSTNAME , PATH , COOKIE , QUERY_STRING
application Action	enum	Specifies the request component that identifies a SaaS application.	
	DISABLED	This effectively ignores applications.	
	HOSTNAME	In the hostname.	
	PATH	In the URL path.	
	QUERY_ STRING	In a query parameter.	
	COOKIE	In a cookie.	
application Cname Enabled	boolean	Enabling this allows you to identify applications using a <i>CNAME chain</i> rather than a single hostname.	applicationAction is HOSTNAME
application Cname Level	number	Specifies the number of CNAMEs to use in the chain.	applicationCnameEnabled is true
application Cookie	string	This specifies the name of the cookie that identifies the application.	applicationAction is COOKIE
application Query String	string	This names the query parameter that identifies the application.	applicationAction is QUERY_STRING
application Regex	string	Specifies a Perl-compatible regular expression with which to substitute the request's application ID.	applicationAction is either: HOSTNAME , PATH , COOKIE , QUERY_STRING
application Replace	string	Specifies a string to replace the request's application ID matched by applicationRegex .	applicationAction is either: HOSTNAME , PATH , COOKIE , QUERY_STRING
users Action	enum	Specifies the request component that identifies a SaaS user.	
	DISABLED	This effectively ignores users.	
	HOSTNAME	In a hostname.	
	PATH	In the URL path.	
	QUERY_ STRING	In a query parameter.	
	COOKIE	In a cookie.	
users Cname Enabled	boolean	Enabling this allows you to identify users using a <i>CNAME chain</i> rather than a single hostname.	usersAction is HOSTNAME

Option	Type	Description	Requires
usersCnameLevel	number	Specifies the number of CNAMEs to use in the chain.	usersCnameEnabled is true
usersCookie	string	This specifies the name of the cookie that identifies the user.	usersAction is COOKIE
usersQueryString	string	This names the query parameter that identifies the user.	usersAction is QUERY_STRING
usersRegex	string	Specifies a Perl-compatible regular expression with which to substitute the request's user ID.	usersAction is either: HOSTNAME , PATH , COOKIE , QUERY_STRING
usersReplace	string	Specifies a string to replace the request's user ID matched by usersRegex .	usersAction is either: HOSTNAME , PATH , COOKIE , QUERY_STRING

salesForceCommerceCloudClient

- **Property Manager name:** [Akamai Connector for Salesforce Commerce Cloud](#)
- **Behavior version:** The v2018-02-27 rule format supports the salesForceCommerceCloudClient behavior v1.2.
- **Rule format status:** [Deprecated, outdated rule format](#)
- **Access:** [Read-write](#)

If you use the Salesforce Commerce Cloud platform for your origin content, this behavior allows your edge content managed by Akamai to contact directly to origin.

Option	Type	Description	Requires
enabled	boolean	Enables the Akamai Connector for Salesforce Commerce Cloud.	
connectorId	string (allows variables)	An ID value that helps distinguish different types of traffic sent from Akamai to the Salesforce Commerce Cloud. Form the value as <i>instance-realm-customer</i> , where <i>instance</i> is either <code>production</code> or <code>development</code> , <i>realm</i> is your Salesforce Commerce Cloud service \$REALM value, and <i>customer</i> is the name for your organization in Salesforce Commerce Cloud. You can use alphanumeric characters, underscores, or dot characters within dash-delimited segment values.	
originType	enum	Specifies where the origin is.	
	DEFAULT	Use a default Salesforce origin.	
	CUSTOMER	Customize the origin.	
sf3cOriginHost	string (allows variables)	This specifies the hostname or IP address of the custom Salesforce origin.	originType is CUSTOMER
originHostHeader	enum	Specifies where the Host header is defined.	
	DEFAULT	Use the default Salesforce header.	
	CUSTOMER	Customize the header.	

Option	Type	Description	Requires
sf3cOrigin Host Header	string (allows variables)	This specifies the hostname or IP address of the custom Salesforce host header.	originHost Header is CUSTOMER
allow Override Origin CacheKey	boolean	When enabled, overrides the forwarding origin's cache key.	

salesForceCommerceCloudProvider

- **Property Manager name:** [Akamai Provider for Salesforce Commerce Cloud](#)^{*)}
- **Behavior version:** The v2018-02-27 rule format supports the salesForceCommerceCloudProvider behavior v1.0.
- **Rule format status:** [Deprecated, outdated rule format](#)
- **Access:** [Read-write](#)

This manages traffic between mutual customers and the Salesforce Commerce Cloud platform.

Option	Type	Description
enabled	boolean	Enables Akamai Provider for Salesforce Commerce Cloud.

savePostDcaProcessing

- **Property Manager name:** [Save POST DCA processing result](#)^{*)}
- **Behavior version:** The v2018-02-27 rule format supports the savePostDcaProcessing behavior v1.1.
- **Rule format status:** [Deprecated, outdated rule format](#)
- **Access:** [Read-only](#)

Used in conjunction with the [cachePost](#) behavior, this behavior allows the body of POST requests to be processed through Dynamic Content Assembly. Contact Akamai Professional Services for help configuring it.

Option	Type	Description
enabled	boolean	Enables processing of POST requests.

scheduleInvalidation

- **Property Manager name:** [Scheduled Invalidation](#)[↗]
- **Behavior version:** The v2018-02-27 rule format supports the `scheduleInvalidation` behavior v1.2.
- **Rule format status:** [Deprecated, outdated rule format](#)
- **Access:** [Read-write](#)

Specifies when cached content that satisfies a rule's criteria expires, optionally at repeating intervals. In addition to periodic cache flushes, you can use this behavior to minimize potential conflicts when related objects expire at different times.

Warning. scheduled invalidations can significantly increase origin servers' load when matching content expires simultaneously across all edge servers. As best practice, schedule expirations during periods of lowest traffic.

Option	Type	Description	Requires
start	string (timestamp)	The UTC date and time when matching cached content is to expire.	
repeat	boolean	When enabled, invalidation recurs periodically from the <code>start</code> time based on the <code>repeatInterval</code> time.	
repeat Interval	string (duration)	Specifies how often to invalidate content from the <code>start</code> time, expressed in seconds. For example, an expiration set to midnight and an interval of <code>86400</code> seconds invalidates content once a day. Repeating intervals of less than 5 minutes are not allowed for NetStorage [↗] origins.	<code>repeat</code> is <code>true</code>
refresh Method	enum	Specifies how to invalidate the content.	
	INVALIDATE	Sends an <code>If-Modified-Since</code> request to the origin, re-caching the content only if it is fresher.	
	PURGE	Re-caches content regardless of its freshness, potentially creating more traffic at the origin.	

scriptManagement

- **Property Manager name:** [Script Management](#)[↗]
- **Behavior version:** The v2018-02-27 rule format supports the `scriptManagement` behavior v1.0.
- **Rule format status:** [Deprecated, outdated rule format](#)
- **Access:** [Read-write](#)

Ensures unresponsive linked JavaScript files do not prevent HTML pages from loading.

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

Option	Type	Description
enabled	boolean	Enables the Script Management feature.

segmentedContentProtection

- **Property Manager name:** [Segmented Media Protection](#)
- **Behavior version:** The v2018-02-27 rule format supports the segmentedContentProtection behavior v1.2.
- **Rule format status:** [Deprecated, outdated rule format](#)
- **Access:** [Read-write](#)

Validates authorization tokens at the edge server to prevent unauthorized link sharing.

Option	Type	Description	Requires
enabled	boolean	Enables the segmented content protection behavior.	
key	object array	Specifies the encryption key to use as a shared secret to validate tokens.	
use Advanced	boolean	Allows you to specify advanced transitionKey and salt options.	
transition Key	object array	An alternate encryption key to match along with the key field, allowing you to rotate keys with no down time.	useAdvanced is true
salt	object array	Specifies a salt as input into the token for added security. This value needs to match the salt used in the token generation code.	useAdvanced is true
hlsMedia Encryption	boolean	Enables HLS Segment Encryption.	
encryption Mode	enum	Specifies the encryption algorithm.	hlsMedia Encryption is true
	AES128	This is currently the only available value.	
use Advanced Option	boolean	Allows you to use advanced encryption options.	hlsMedia Encryption is true
iv	object array	Specifies the initialization vector used to generate the encryption key.	useAdvanced Option is true

shutr

- **Property Manager name:** [SHUTR](#)
- **Behavior version:** The v2018-02-27 rule format supports the shutr behavior v1.1.

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

The SHUTR protocol extends HTTP to reduce the amount of header data necessary for web transactions with mobile devices.

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

segmentedMediaOptimization

- **Property Manager name:** [Segmented Media Delivery Mode](#) [↗]
- **Behavior version:** The `v2018-02-27` rule format supports the `segmentedMediaOptimization` behavior v1.2.
- **Rule format status:** [Deprecated, outdated rule format](#)
- **Access:** [Read-write](#)

Optimizes segmented media for live or streaming delivery contexts.

Option	Type	Description	Requires
behavior	enum	Sets the type of media content to optimize.	
	ON_DEMAND	Media is available on demand. This is the only option allowed for NetStorage [↗] origins.	
	LIVE	Media is streaming live.	
show Advanced	boolean	Allows you to configure advanced media options.	behavior is LIVE
liveType	enum	The type of live media.	showAdvanced is true
	CONTINUOUS	Not confined to a range of time.	
	EVENT	An event for a range of time.	
start Time	string (epoch timestamp)	This specifies when the live media event begins.	showAdvanced is true AND liveType is EVENT
endTime	string (epoch timestamp)	This specifies when the live media event ends.	showAdvanced is true AND liveType is EVENT
dvrType	enum	The type of DVR.	showAdvanced is true
	CONFIGURABLE	A configurable DVR.	
	UNKNOWN	An unknown DVR.	
dvr Window	string (duration)	Set the duration for your media, or <code>0m</code> if a DVR is not required.	showAdvanced is true AND dvrType is CONFIGURABLE

setVariable

- **Property Manager name:** [Set Variable](#)
- **Behavior version:** The v2018-02-27 rule format supports the `setVariable` behavior v1.1.
- **Rule format status:** [Deprecated, outdated rule format](#)
- **Access:** [Read-write](#)

Modify a variable to insert into subsequent fields within the rule tree. Use this behavior to specify the predeclared `variableName` and determine from where to derive its new value. Based on this `valueSource`, you can either generate the value, extract it from some part of the incoming request, assign it from another variable (including a set of built-in system variables), or directly specify its text. Optionally choose a `transform` function to modify the value once. See [Support for variables](#) for more information.

Option	Type	Description	Requires
variable Name	string (variable name)	Specifies the predeclared root name of the variable to modify. When you declare a variable name such as <code>VAR</code> , its name is prepended with <code>PMUSER_</code> and accessible in a <code>user</code> namespace, so that you invoke it in subsequent text fields within the rule tree as <code>{{user.PMUSER_VAR}}</code> . In deployed XML metadata , it appears as <code>%(PMUSER_VAR)</code> .	
valueSource	enum	Determines how you want to set the value.	
	EXPRESSION	Specify your own string expression.	
	EXTRACT	Extract it from another value.	
	GENERATE	Generate the value.	
variable Value	string (allows variables)	This directly specifies the value to assign to the variable. The expression may include a mix of static text and other variables, such as <code>new_filename.{{builtin.AK_EXTENSION}}</code> to embed a system variable.	<code>valueSource</code> is <code>EXPRESSION</code>
extract Location	enum	This specifies from where to get the value.	<code>valueSource</code> is <code>EXTRACT</code>
	CLIENT_CERTIFICATE	Client certificate.	
	CLIENT_REQUEST_HEADER	Client request header.	
	COOKIE	Cookie.	
	EDGESCAPE	For location or network data.	
	PATH_COMPONENT_OFFSET	Substring within the URL path.	
	QUERY_STRING	A query parameter.	
certificate FieldName	enum	Specifies the certificate's content.	<code>extractLocation</code> is <code>CLIENT_CERTIFICATE</code>
	VERSION	The certificate's X509 version number.	

Option	Type	Description	Requires
	SERIAL	The serial number, expressed in hex.	
	FINGERPRINT_MD5	The hex-encoded MD5 fingerprint.	
	FINGERPRINT_SHA1	The hex-encoded SHA1 fingerprint.	
	FINGERPRINT_DYN	The hex-encoded fingerprint generated based on the SIGNATURE_ALGORITHM .	
	ISSUER_DN	The <i>distinguished name</i> field for the certificate's issuer.	
	SUBJECT_DN	The <i>distinguished name</i> field for the user.	
	NOT_BEFORE	The start of the time range, expressed in YYYY/MM/DD HH:MI:SS ZONE format, where the zone is optional.	
	NOT_AFTER	The end of the time range, expressed in YYYY/MM/DD HH:MI:SS ZONE format, where the zone is optional.	
	SIGNATURE_ALGORITHM	The algorithm used to generate the certificate's signature.	
	SIGNATURE	The certificate's signature, expressed in hex.	
	CONTENTS_DER	The entire DER-encoded certificate, expressed in hex.	
	CONTENTS_PEM	The PEM-formatted certificate encoded as a single line of base64 characters.	
	CONTENTS_PEM_NO_LABELS	Same as CONTENTS_PEM , but not including the certificate's header and footer.	
	COUNT	The number of client certificates received.	
	STATUS_MSG	A short message indicating the status of a certificate's validation, such as ok or missing .	
	KEY_LENGTH	The size of the key in bits.	
header Name	string	Specifies the case-insensitive name of the HTTP header to extract.	extractLocation is CLIENT_REQUEST_HEADER
cookieName	string	Specifies the name of the cookie to extract.	extractLocation is COOKIE
locationId	enum	Specifies the X-Akamai-Edgescape header's field name. Possible values specify basic geolocation, various geographic standards, and information about the client's network. For details on EdgeScape header fields, see the EdgeScape User Guide .	extractLocation is EDGESCAPE
	GEOREGION	Region.	
	COUNTRY_CODE	ISO-3166 country code.	
	REGION_CODE	ISO-3166 region code.	
	CITY	City.	
	DMA	Designated Market Area.	
	PMSA	Primary Metropolitan Statistical Area.	
	MSA	Metropolitan Statistical Area.	
	AREACODE	Area code.	
	COUNTY	County.	
	FIPS	Federal Information Processing System code.	

Option	Type	Description	Requires
	LAT	Latitude.	
	LONG	Longitude.	
	TIMEZONE	Time zone.	
	ZIP	Zip code.	
	CONTINENT	Two-letter continent code.	
	NETWORK	Network name.	
	NETWORK_TYPE	Network type.	
	ASNUM	Autonomous System Number.	
	THROUGHPUT	Tiered throughput level.	
	BW	Tiered bandwidth level.	
path Component Offset	string	This specifies a portion of the path. The indexing starts from 1 , so a value of /path/to/nested/filename.html and an offset of 1 yields path , and 3 yields nested . Negative indexes offset from the right, so -2 also yields nested .	extractLocation is PATH_ COMPONENT_ OFFSET
query Parameter Name	string	Specifies the name of the query parameter from which to extract the value.	extractLocation is QUERY_STRING
generator	enum	This specifies the type of value to generate.	valueSource is GENERATE
	HEXRAND	A random hex sequence.	
	RAND	A random number.	
numberOf Bytes	number (1-16)	Specifies the number of random hex bytes to generate.	generator is HEXRAND
minRandom Number	string (allows variables)	Specifies the lower bound of the random number.	generator is RAND
maxRandom Number	string (allows variables)	Specifies the upper bound of the random number.	generator is RAND
transform	enum	Specifies a function to transform the value. For more details on each transform function, see Set Variable: Operations .	
	NONE	No transformation.	
	ADD	Arithmetic function.	
	BASE_64_DECODE	String encoding.	
	BASE_64_ENCODE	String encoding.	
	BITWISE_AND	Bitwise operation.	
	BITWISE_NOT	Bitwise operation.	
	BITWISE_OR	Bitwise operation.	
	BITWISE_XOR	Bitwise operation.	
	DECIMAL_TO_HEX	Numeric conversion.	
	DECRYPT	String encoding.	
	DIVIDE	Arithmetic function.	
	ENCRYPT	String encoding.	

Option	Type	Description	Requires
	EPOCH_TO_STRING	Time format.	
	EXTRACT_PARAM	String format.	
	HASH	Integer data digest.	
	HEX_TO_DECIMAL	Numeric conversion.	
	HEX_DECODE	String conversion.	
	HEX_ENCODE	String conversion.	
	HMAC	Data digest.	
	LOWER	String function.	
	MD5	Data digest.	
	MINUS	Arithmetic function, reverse sign.	
	MODULO	Arithmetic function, get remainder.	
	MULTIPLY	Arithmetic function.	
	NORMALIZE_PATH_WIN	Convert Windows paths to Unix format and remove relative path syntax.	
	REMOVE_WHITESPACE	String conversion.	
	SHA_1	Data digest.	
	SHA_256	Data digest.	
	STRING_INDEX	String function: locate substring.	
	STRING_LENGTH	String function.	
	STRING_TO_EPOCH	Time format.	
	SUBSTITUTE	String function.	
	SUBSTRING	String function: locate index.	
	SUBTRACT	Arithmetic function.	
	TRIM	Trim surrounding whitespace in string.	
	UPPER	String function.	
	URL_DECODE	String conversion.	
	URL_ENCODE	Unicode string conversion.	
	URL_DECODE_UNI	String conversion.	
	UTC_SECONDS	Time format.	
	XML_DECODE	String conversion.	
	XML_ENCODE	String conversion.	
operandOne	string (allows variables)	Specifies an additional operand when the transform function is set to various arithmetic functions (ADD , SUBTRACT , MULTIPLY , DIVIDE , or MODULO) or bitwise functions (BITWISE_AND , BITWISE_OR , or BITWISE_XOR).	transform is either: ADD , BITWISE_AND , BITWISE_OR , BITWISE_XOR , DIVIDE , MODULO , MULTIPLY , SUBTRACT

Option	Type	Description	Requires
algorithm	enum	Specifies the algorithm to apply.	transform is either: ENCRYPT , DECRYPT
	ALG_3DES	Triple DES.	
	ALG_AES128	Advanced Encryption Standard, 128 bits.	
	ALG_AES256	Advanced Encryption Standard, 256 bits.	
encryption Key	string (allows variables)	Specifies the encryption hex key. For ALG_3DES it needs to be 48 characters long, 32 characters for ALG_AES128 , and 64 characters for ALG_AES256 .	transform is either: ENCRYPT , DECRYPT
initialization Vector	string	Specifies a one-time number as an initialization vector. It needs to be 15 characters long for ALG_3DES , and 32 characters for both ALG_AES128 and ALG_AES256 .	transform is either: ENCRYPT , DECRYPT
encryption Mode	enum	Specifies the encryption mode.	transform is either: ENCRYPT , DECRYPT
	CBC	Cipher Block Chaining.	
	ECB	Electronic Codebook.	
nonce	string (allows variables)	Specifies the one-time number used for encryption.	transform is either: ENCRYPT , DECRYPT
prepend Bytes	boolean	Specifies a number of random bytes to prepend to the key.	transform is either: ENCRYPT , DECRYPT
formatString	string	Specifies an optional format string for the conversion, using format codes such as %m/%d/%y as specified by strftime . A blank value defaults to RFC-2616 format.	transform is either: EPOCH_TO_STRING , STRING_TO_EPOCH
paramName	string (allows variables)	Extracts the value for the specified parameter name from a string that contains key/value pairs. (Use separator below to parse them.)	transform is EXTRACT_PARAM
separator	string	Specifies the character that separates pairs of values within the string.	transform is EXTRACT_PARAM
min	number	Specifies a minimum value for the generated integer.	transform is HASH
max	number	Specifies a maximum value for the generated integer.	transform is HASH
hmacKey	string (allows variables)	Specifies the secret to use in generating the base64-encoded digest.	transform is HMAC
hmac Algorithm	enum	Specifies the algorithm to use to generate the base64-encoded digest.	transform is HMAC
	SHA1	SHA-1.	
	SHA256	SHA-256.	
	MD5	MD5.	

Option	Type	Description	Requires
ipVersion	enum	Specifies the IP version under which a subnet mask generates.	transform is NETMASK
	IPv4	Use IPv4.	
	IPv6	Use IPv6.	
ipv6Prefix	number (0-128)	Specifies the prefix of the IPV6 address, a value between 0 and 128.	ipVersion is IPV6
ipv4Prefix	number (0-32)	Specifies the prefix of the IPV4 address, a value between 0 and 32.	ipVersion is IPV4
subString	string (allows variables)	Specifies a substring for which the returned value represents a zero-based offset of where it appears in the original string, or -1 if there's no match.	transform is STRING_INDEX
regex	string	Specifies the regular expression pattern (PCRE) to match the value.	transform is SUBSTITUTE
replacement	string (allows variables)	Specifies the replacement string. Reinsert grouped items from the match into the replacement using \$1 , \$2 ... \$n .	transform is SUBSTITUTE
case Sensitive	boolean	Enabling this makes all matches case sensitive.	transform is either: EXTRACT_PARAM , SUBSTITUTE
global Substitution	boolean	Replaces all matches in the string, not just the first.	transform is SUBSTITUTE
startIndex	string (allows variables)	Specifies the zero-based character offset at the start of the substring. Negative indexes specify the offset from the end of the string.	transform is SUBSTRING
endIndex	string (allows variables)	Specifies the zero-based character offset at the end of the substring, without including the character at that index position. Negative indexes specify the offset from the end of the string.	transform is SUBSTRING
exceptChars	string	Specifies characters <i>not</i> to encode, possibly overriding the default set.	transform is URL_ENCODE
forceChars	string	Specifies characters to encode, possibly overriding the default set.	transform is URL_ENCODE

simulateErrorCode

- **Property Manager name:** [Simulate Error Response Code](#) [↗]
- **Behavior version:** The v2018-02-27 rule format supports the simulateErrorCode behavior v1.1.
- **Rule format status:** [Deprecated, outdated rule format](#)
- **Access:** [Read-write](#)

This behavior simulates various error response codes. Contact Akamai Professional Services for help configuring it.

Option	Type	Description	Requires
<code>errorType</code>	enum	Specifies the type of error.	
		Supported values: ERR_CONNECT_FAIL ERR_CONNECT_TIMEOUT ERR_DNS_FAIL ERR_DNS_IN_REGION ERR_DNS_TIMEOUT ERR_NO_GOOD_FWD_IP ERR_READ_ERROR ERR_READ_TIMEOUT ERR_SUREROUTE_DNS_FAIL ERR_WRITE_ERROR	
<code>timeout</code>	string (duration)	When the <code>errorType</code> is <code>ERR_CONNECT_TIMEOUT</code> , <code>ERR_DNS_TIMEOUT</code> , <code>ERR_SUREROUTE_DNS_FAIL</code> , or <code>ERR_READ_TIMEOUT</code> , generates an error after the specified amount of time from the initial request.	<code>errorType</code> is either: <code>ERR_DNS_TIMEOUT</code> , <code>ERR_SUREROUTE_DNS_FAIL</code> , <code>ERR_READ_TIMEOUT</code> , or <code>ERR_CONNECT_TIMEOUT</code>

siteShield

- **Property Manager name:** [SiteShield](#) [↗]
- **Behavior version:** The `v2018-02-27` rule format supports the `siteShield` behavior v1.3.
- **Rule format status:** [Deprecated, outdated rule format](#)
- **Access:** [Read-write](#)

This behavior implements the [Site Shield](#) [↗] feature, which helps prevent non-Akamai machines from contacting your origin. Your service representative periodically sends you a list of Akamai servers allowed to contact your origin, with which you establish an Access Control List on your firewall to prevent any other requests.

Option	Type	Description
<code>ssmap</code>	object	Identifies the hostname for the Site Shield map, available from your Akamai representative. Form an object with a <code>value</code> key that references the hostname, for example: <code>"ssmap": {"value": "ss.akamai.net"}</code> .

standardTLSMigrationOverride

- **Property Manager name:** [Standard TLS Migration Override](#) [↗]
- **Behavior version:** The `v2018-02-27` rule format supports the `standardTLSMigrationOverride` behavior v1.0.
- **Rule format status:** [Deprecated, outdated rule format](#)
- **Access:** [Read-only](#)

When applying `standardTLSMigration`, add this behavior if your new certificate is SNI-only, if your property includes any [advanced features](#), any Edge IP Binding enabled hosts, or if any foreground downloads are configured.

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

standardTLSMigration


- **Property Manager name:** [Standard TLS Migration](#) ➦
- **Behavior version:** The `v2018-02-27` rule format supports the `standardTLSMigration` behavior v1.0.
- **Rule format status:** [Deprecated, outdated rule format](#)
- **Access:** [Read-write](#)



Migrates traffic to Standard TLS. Apply this behavior within the default rule or any `hostname` match. In some cases you may need to apply this along with the [standardTLSMigrationOverride](#) behavior.

Option	Type	Description	Requires
<code>enabled</code>	boolean	Allows migration to Standard TLS.	
<code>migrationFrom</code>	enum	What kind of traffic you're migrating from.	
	<code>SHARED_CERT</code>	A shared certificate.	
	<code>NON_SECURE</code>	Non-secure traffic.	
	<code>ENHANCED_SECURE</code>	Enhanced Secure TLS.	
<code>allow HTTPUpgrade</code>	boolean	Allows temporary upgrade of HTTP traffic to HTTPS.	<code>migrationFrom</code> is <code>NON_SECURE</code>
<code>allow HTTPSDowngrade</code>	boolean	Allow temporary downgrade of HTTPS traffic to HTTP. This removes various <code>Origin</code> , <code>Referer</code> , <code>Cookie</code> , <code>Cookie2</code> , <code>sec-*</code> and <code>proxy-*</code> headers from the request to origin.	<code>migrationFrom</code> is <code>NON_SECURE</code>
<code>migrationStartTime</code>	string (epoch timestamp)	Specifies when to start migrating the cache.	<code>allow HTTPUpgrade</code> is <code>true</code> OR <code>allow HTTPSDowngrade</code> is <code>true</code>
<code>migrationDuration</code>	number	Specifies the number of days to migrate the cache.	<code>allow HTTPUpgrade</code> is <code>true</code> OR <code>allow HTTPSDowngrade</code> is <code>true</code>
<code>cacheSharingStartTime</code>	string (epoch timestamp)	Specifies when to start cache sharing.	<code>migrationFrom</code> is <code>ENHANCED_SECURE</code>

Option	Type	Description	Requires
cacheSharing Duration	number	Specifies the number cache sharing days.	migrationFrom is ENHANCED_ SECURE
isCertificate SNIOnly	boolean	Sets whether your new certificate is SNI-only.	migrationFrom is ENHANCED_ SECURE
isTiered DistributionUsed	boolean	Allows you to align traffic to various tieredDistribution areas.	migrationFrom is NON_SECURE
tdLocation	enum	Specifies the tieredDistribution location.	isTiered DistributionUsed is true
	GLOBAL	Global.	
	APAC	Asia and Pacific.	
	EUROPE	Europe.	
	US_EAST	Eastern United States.	
	US_CENTRAL	Central United States.	
	US_WEST	Western United States.	
	AUSTRALIA	Australia.	
	GLOBAL_LEGACY	Global.	

subCustomer

- **Property Manager name:** [Subcustomer Enablement](#) 
- **Behavior version:** The v2018-02-27 rule format supports the subCustomer behavior v1.5.
- **Rule format status:** [Deprecated, outdated rule format](#)
- **Access:** [Read-write](#)

When positioned in a property's top-level default rule, enables various [Cloud Embed](#)  features that allow you to leverage Akamai's CDN architecture for your own subcustomers. This behavior's options allow you to use Cloud Embed to configure your subcustomers' content. Once enabled, you can use the [Akamai Cloud Embed API](#)  (ACE) to assign subcustomers to this base configuration, and to customize policies for them. See also the [dynamicWebContent](#) behavior to configure subcustomers' dynamic web content.

Option	Type	Description	Requires
enabled	boolean	Allows Cloud Embed to dynamically modify your subcustomers' content.	
origin	boolean	Allows you to assign origin hostnames for customers.	

Option	Type	Description	Requires
partner DomainSuffix	string	This specifies the appropriate domain suffix, which you should typically match with your property hostname. It identifies the domain as trustworthy on the Akamai network, despite being defined within Cloud Embed, outside of your base property configuration. Include this domain suffix if you want to purge subcustomer URLs. For example, if you provide a value of <code>suffix.example.com</code> , then to purge <code>subcustomer.com/some/path</code> , specify <code>subcustomer.com.suffix.example.com/some/path</code> as the purge request's URL.	<code>origin</code> is <code>true</code>
cacheing	boolean	Modifies content caching rules.	
referrer	boolean	Sets subcustomers' referrer whitelists or blacklist.	
ip	boolean	Sets subcustomers' IP whitelists or blacklists.	
geoLocation	boolean	Sets subcustomers' location-based whitelists or blacklists.	
refresh Content	boolean	Allows you to reschedule when content validates for subcustomers.	
modifyPath	boolean	Modifies a subcustomer's request path.	
cacheKey	boolean	Allows you to set which query parameters are included in the cache key.	
token Authorization	boolean	When enabled, this allows you to configure edge servers to use tokens to control access to subcustomer content. Use Cloud Embed to configure the token to appear in a cookie, header, or query parameter.	
siteFailover	boolean	Allows you to configure unique failover sites for each subcustomer's policy.	
content Compressor	boolean	Allows compression of subcustomer content.	
access Control	boolean	When enabled, this allows you to deny requests to a subcustomer's content based on specific match conditions, which you use Cloud Embed to configure in each subcustomer's policy.	
dynamicWeb Content	boolean	Allows you to apply the dynamicWebContent behavior to further modify how dynamic content behaves for subcustomers.	
onDemand Video Delivery	boolean	Enables delivery of media assets to subcustomers.	
largeFile Delivery	boolean	Enables large file delivery for subcustomers.	

tcpOptimization

- **Property Manager name:** [TCP Optimizations](#) [🔗]
- **Behavior version:** The `v2018-02-27` rule format supports the `tcpOptimization` behavior v1.1.
- **Rule format status:** [Deprecated, outdated rule format](#)
- **Access:** [Read-write](#)

Enables a suite of optimizations targeting buffers, time-outs, and packet loss that improve transmission performance. This behavior is deprecated, but you should not disable or remove it if present.

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

sureRoute

- **Property Manager name:** [SureRoute](#)^{*)}
- **Behavior version:** The `v2018-02-27` rule format supports the `sureRoute` behavior v1.5.
- **Rule format status:** [Deprecated, outdated rule format](#)
- **Access:** [Read-write](#)

The [SureRoute](#)[↗] feature continually tests different routes between origin and edge servers to identify the optimal path. By default, it conducts *rac*es to identify alternative paths to use in case of a transmission failure. These races increase origin traffic slightly.

This behavior allows you to configure SureRoute along with a test object to improve delivery of non-cacheable `no-store` or `bypass-cache` content. Since edge servers are already positioned as close as possible to requesting clients, the behavior does not apply to cacheable content.

Option	Type	Description	Requires
<code>enabled</code>	boolean	Enables the SureRoute behavior, to optimize delivery of non-cached content.	
<code>type</code>	enum	Specifies the set of edge servers used to test routes.	
	<code>PERFORMANCE</code>	Use the default set of edge servers.	
	<code>CUSTOM_MAP</code>	A custom map that you need to get from Akamai Professional Services.	
<code>custom Map</code>	string	If <code>type</code> is <code>CUSTOM_MAP</code> , this specifies the map string provided to you by Akamai Professional Services, or included as part of the Site Shield [↗] product.	<code>type</code> is <code>CUSTOM_MAP</code>
<code>test Object Uri</code>	string	<p>Specifies the path and filename for your origin's test object to use in races to test routes.</p> <p>Akamai provides sample test objects for the Dynamic Site Accelerator[↗] and Web Application Accelerator products. If you want to use your own test object, it needs to be on the same origin server as the traffic being served through SureRoute. Make sure it returns a <code>200</code> HTTP response and does not require authentication. The file should be an average-sized static HTML file (<code>Content-Type: text/html</code>) that is no smaller than 8KB, with no back-end processing.</p> <p>If you have more than one origin server deployed behind a load balancer, you can configure it to serve the test object directly on behalf of the origin, or route requests to the same origin server to avoid deploying the test object on each origin server.</p>	
<code>toHost Status</code>	enum	Specifies which hostname to use.	
	<code>INCOMING_HH</code>	Use the incoming <code>Host</code> header when requesting the SureRoute test object.	
	<code>OTHER</code>	Use <code>toHost</code> to specify a custom <code>Host</code> header.	
<code>toHost</code>	string	If <code>toHostStatus</code> is <code>OTHER</code> , this specifies the custom <code>Host</code> header to use when requesting the SureRoute test object.	<code>toHost Status</code> is <code>OTHER</code>

Option	Type	Description	Requires
raceStat Ttl	string (duration)	Specifies the time-to-live to preserve SureRoute race results, typically 30m . If traffic exceeds a certain threshold after TTL expires, the overflow is routed directly to the origin, not necessarily optimally. If traffic remains under the threshold, the route is determined by the winner of the most recent race.	
forceSsl Forward	boolean	Forces SureRoute to use SSL when requesting the origin's test object, appropriate if your origin does not respond to HTTP requests, or responds with a redirect to HTTPS.	
enable Custom Key	boolean	When disabled, caches race results under the race destination's hostname. If enabled, use <code>customStatKey</code> to specify a custom hostname.	
custom StatKey	string	This specifies a hostname under which to cache race results. This may be useful when a property corresponds to many origin hostnames. By default, SureRoute would launch races for each origin, but consolidating under a single hostname runs only one race.	enable Custom Key is true

teaLeaf

- **Property Manager name:** [IBM Tealeaf Connector](#)^{*}
- **Behavior version:** The `v2018-02-27` rule format supports the `teaLeaf` behavior v1.0.
- **Rule format status:** [Deprecated, outdated rule format](#)
- **Access:** [Read-write](#)

Allows IBM Tealeaf Customer Experience on Cloud to record HTTPS requests and responses for Akamai-enabled properties. Recorded data becomes available in your IBM Tealeaf account.

Option	Type	Description
enabled	boolean	When enabled, capture HTTPS requests and responses, and send the data to your IBM Tealeaf account.
limitTo Dynamic	boolean	Limit traffic to dynamic, uncached (No-Store) content.
ibmCustomer Id	number	The integer identifier for the IBM Tealeaf Connector account.

tieredDistribution

- **Property Manager name:** [Tiered Distribution](#)^{*}
- **Behavior version:** The `v2018-02-27` rule format supports the `tieredDistribution` behavior v1.2.
- **Rule format status:** [Deprecated, outdated rule format](#)
- **Access:** [Read-write](#)

This behavior allows Akamai edge servers to retrieve cached content from other Akamai servers, rather than directly from the origin. These interim *parent* servers in the *cache hierarchy* (CH) are positioned close to the origin, and fall along the path from the origin to the edge server. Tiered Distribution typically reduces the origin server's load, and reduces the time it takes for edge servers to refresh content.

See also the [tieredDistributionAdvanced](#) behavior.

Option	Type	Description	Requires
enabled	boolean	When enabled, activates tiered distribution.	
tiered Distribution Map	enum	Optionally map the tiered parent server's location close to your origin. A narrower local map minimizes the origin server's load, and increases the likelihood the requested object is cached. A wider global map reduces end-user latency, but decreases the likelihood the requested object is in any given parent server's cache. This option cannot apply if the property is marked as secure. See Secure property requirements for guidance.	is_secure is false in top-level rule
	CH2	A global map.	
	CHAPAC	China and the Asian Pacific area.	
	CHEU2	Europe.	
	CHEUS2	Eastern United States.	
	CHCUS2	Central United States.	
	CHWUS2	Western United States.	
	CH AUS	Australia.	
	CH	A global map.	

tieredDistributionAdvanced


- **Property Manager name:** [Tiered Distribution \(Advanced\)](#) [✎]
- **Behavior version:** The v2018-02-27 rule format supports the `tieredDistributionAdvanced` behavior v1.0.
- **Rule format status:** [Deprecated, outdated rule format](#)
- **Access:** [Read-only](#)

This behavior allows Akamai edge servers to retrieve cached content from other Akamai servers, rather than directly from the origin. These interim *parent* servers in the *cache hierarchy* (CH) are positioned close to the origin, and fall along the path from the origin to the edge server. Tiered Distribution typically reduces the origin server's load, and reduces the time it takes for edge servers to refresh content. This advanced behavior provides a wider set of options than [tiered Distribution](#) .

Option	Type	Description
enabled	boolean	When enabled, activates tiered distribution.

Option	Type	Description
tiered Distribution Map	string	Optionally map the tiered parent server's location close to your origin: CHEU2 for Europe; CHAUS for Australia; CHAPAC for China and the Asian Pacific area; CHWUS2 , CHCUS2 , and CHEUS2 for different parts of the United States. Choose CH or CH2 for a more global map. A narrower local map minimizes the origin server's load, and increases the likelihood the requested object is cached. A wider global map reduces end-user latency, but decreases the likelihood the requested object is in any given parent server's cache. This option cannot apply if the property is marked as secure. See Secure property requirements for guidance.


timeout

- **Property Manager name:** [Connect Timeout](#) 
- **Behavior version:** The v2018-02-27 rule format supports the timeout behavior v1.1.
- **Rule format status:** [Deprecated, outdated rule format](#)
- **Access:** [Read-write](#)

Sets the HTTP connect timeout.

Option	Type	Description
value	string (duration)	Specifies the timeout, for example 10s .

uidConfiguration

- **Property Manager name:** [UID Configuration](#) 
- **Behavior version:** The v2018-02-27 rule format supports the uidConfiguration behavior v1.0.
- **Rule format status:** [Deprecated, outdated rule format](#)
- **Access:** [Read-write](#)

This behavior allows you to extract unique identifier (UID) values from live traffic, for use in OTA applications. Note that you are responsible for maintaining the security of any data that may identify individual users.

Option	Type	Description	Requires
enabled	boolean	Allows you to extract UIDs from client requests.	
extract Location	enum	Where to extract the UID value from.	
	CLIENT_ REQUEST_ HEADER	From a client request header.	

Option	Type	Description	Requires
	QUERY_STRING	From the request query string.	
	VARIABLE	From a rule tree VARIABLE . You should mark these variables as sensitive . See also Support for variables .	
header Name	string	This specifies the name of the HTTP header from which to extract the UID value.	extractLocation is CLIENT_REQUEST_HEADER
query Parameter Name	string	This specifies the name of the query parameter from which to extract the UID value.	extractLocation is QUERY_STRING
variable Name	string (variable name)	This specifies the name of the rule tree variable from which to extract the UID value.	extractLocation is VARIABLE

validateEntityTag

- **Property Manager name:** [Validate Entity Tag \(ETag\)](#) [↗]
- **Behavior version:** The v2018-02-27 rule format supports the validateEntityTag behavior v1.1.
- **Rule format status:** [Deprecated, outdated rule format](#)
- **Access:** [Read-write](#)

Instructs edge servers to compare the request's ETag header with that of the cached object. If they differ, the edge server sends a new copy of the object. This validation occurs in addition to the default validation of Last-Modified and If-Modified-Since headers.

Option	Type	Description
enabled	boolean	Enables the ETag validation behavior.

verifyJsonWebToken

- **Property Manager name:** [JWT verification](#) [↗]
- **Behavior version:** The v2018-02-27 rule format supports the verifyJsonWebToken behavior v1.0.
- **Rule format status:** [Deprecated, outdated rule format](#)
- **Access:** [Read-write](#)

This behavior allows you to use JSON Web Tokens (JWT) to verify requests.

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

Option	Type	Description
headerName	string	This specifies the name of the header from which to extract the JWT value.
jwt	string	An identifier for the JWT keys collection.

verifyJsonWebTokenForDcp

- **Property Manager name:** [JWT](#)
- **Behavior version:** The v2018-02-27 rule format supports the verifyJsonWebTokenForDcp behavior v1.0.
- **Rule format status:** [Deprecated, outdated rule format](#)
- **Access:** [Read-write](#)

This behavior allows you to use JSON web tokens (JWT) to verify requests for use in implementing [IoT Edge Connect](#), which you use the [dcp](#) behavior to configure. You can specify the location in a request to pass a JSON web token (JWT), collections of public keys to verify the integrity of this token, and specific claims to extract from it. Use the [verifyJsonWebToken](#) behavior for other JWT validation.

When authenticating to edge servers with both JWT and mutual authentication (using the [dcpAuthVariableExtractor](#) behavior), the JWT method is ignored, and you need to authenticate with a client authentication certificate.

Option	Type	Description	Requires
extract Location	enum	Specifies where to get the JWT value from.	
	CLIENT_REQUEST_HEADER	From the client request header.	
	QUERY_STRING	From the query string.	
	CLIENT_REQUEST_HEADER_AND_QUERY_STRING	From both.	
primary Location	enum	Specifies the primary location to extract the JWT value from. If the specified option doesn't include the JWTs, the system checks the secondary one.	extractLocation is CLIENT_REQUEST_HEADER_AND_QUERY_STRING
	CLIENT_REQUEST_HEADER	Get the JWT value from the request header.	
	QUERY_STRING	Get the JWT value from the query string.	
custom Header	boolean	The JWT value comes from the X-Akamai-DCP-Token header by default. Enabling this option allows you to extract it from another header name that you specify.	extractLocation is either: CLIENT_REQUEST_HEADER, CLIENT_REQUEST_HEADER_AND_QUERY_STRING

Option	Type	Description	Requires
headerName	string	This specifies the name of the header to extract the JWT value from.	customHeader is true
queryParameterName	string	Specifies the name of the query parameter from which to extract the JWT value.	extractLocation is either: QUERY_STRING, CLIENT_REQUEST_HEADER_AND_QUERY_STRING
jwt	string	An identifier for the JWT keys collection.	
extractClientId	boolean	Allows you to extract the client ID claim name stored in JWT.	
clientId	string	This specifies the claim name.	extractClientId is true
extractAuthorizations	boolean	Allows you to extract the authorization groups stored in the JWT.	
authorizations	string	This specifies the authorization group name.	extractAuthorizations is true
extractUserName	boolean	Allows you to extract the user name stored in the JWT.	
userName	string	This specifies the user name.	extractUserName is true
enableRS256	boolean	Verifies JWTs signed with the RS256 algorithm. This signature helps to ensure that the token hasn't been tampered with.	
enableES256	boolean	Verifies JWTs signed with the ES256 algorithm. This signature helps to ensure that the token hasn't been tampered with.	

verifyTokenAuthorization

- **Property Manager name:** [Auth Token 2.0 Verification](#)
- **Behavior version:** The v2018-02-27 rule format supports the verifyTokenAuthorization behavior v1.4.
- **Rule format status:** [Deprecated, outdated rule format](#)
- **Access:** [Read-write](#)

Verifies Auth 2.0 tokens.

Option	Type	Description	Requires
useAdvanced	boolean	If enabled, allows you to specify advanced options such as algorithm , escapeHmacInputs , ignoreQueryString , transitionKey , and salt .	
location	enum	Specifies where to find the token in the incoming request.	
		Supported values: <div> CLIENT_REQUEST_HEADER COOKIE QUERY_STRING </div>	
locationId	string	When location is CLIENT_REQUEST_HEADER , specifies the name of the incoming request's header where to find the token.	

Option	Type	Description	Requires
algorithm	enum	Specifies the algorithm that generates the token. It needs to match the method chosen in the token generation code.	use Advanced is true
		Supported values: MD5 SHA1 SHA256	
escape Hmac Inputs	boolean	URL-escapes HMAC inputs passed in as query parameters.	use Advanced is true
ignore Query String	boolean	Enabling this removes the query string from the URL used to form an encryption key.	use Advanced is true
key	object array	The shared secret used to validate tokens, which needs to match the key used in the token generation code.	
transition Key	object array	Specifies a transition key as a hex value.	use Advanced is true
salt	object array	Specifies a salt string for input when generating the token, which needs to match the salt value used in the token generation code.	use Advanced is true
failure Response	boolean	When enabled, sends an HTTP error when an authentication test fails.	

visitorPrioritization

- **Property Manager name:** [Visitor Prioritization Cloudlet](#)
- **Behavior version:** The v2018-02-27 rule format supports the visitorPrioritization behavior v3.5.
- **Rule format status:** [Deprecated, outdated rule format](#)
- **Access:** [Read-write](#)

The [Visitor Prioritization Cloudlet](#) decreases abandonment by providing a user-friendly waiting room experience. With Cloudlets available on your contract, choose **Your services <> Edge logic Cloudlets** to control Visitor Prioritization within [Control Center](#). Otherwise use the [Cloudlets API](#) to configure it programmatically. To serve non-HTML API content such as JSON blocks, see the [apiPrioritization](#) behavior.

Option	Type	Description	Requires
enabled	boolean	Enables the Visitor Prioritization behavior.	
cloudletPolicy	object	Identifies the Cloudlet policy.	
cloudletPolicy.id	number	Identifies the Cloudlet.	
cloudlet Policy.name	string	The Cloudlet's descriptive name.	

Option	Type	Description	Requires
user IdentificationBy Cookie	boolean	When enabled, identifies users by the value of a cookie.	
user IdentificationKey Cookie	string	Specifies the name of the cookie whose value identifies users. To match a user, the value of the cookie needs to remain constant across all requests.	user IdentificationBy Cookie is true
user IdentificationBy Headers	boolean	When enabled, identifies users by the values of GET or POST request headers.	
user IdentificationKey Headers	string array	Specifies names of request headers whose values identify users. To match a user, values for all the specified headers need to remain constant across all requests.	user IdentificationBy Headers is true
user IdentificationBy Ip	boolean	Allows IP addresses to identify users.	
user IdentificationBy Params	boolean	When enabled, identifies users by the values of GET or POST request parameters.	
user IdentificationKey Params	string array	Specifies names of request parameters whose values identify users. To match a user, values for all the specified parameters need to remain constant across all requests. Parameters that are absent or blank may also identify users.	user IdentificationBy Params is true
allowedUser CookieEnabled	boolean	Sets a cookie for users who have been allowed through to the site.	
allowedUser CookieLabel	string	Specifies a label to distinguish this cookie for an allowed user from others. The value appends to the cookie's name, and helps you to maintain the same user assignment across behaviors within a property, and across properties.	allowedUser CookieEnabled is true
allowedUser CookieDuration	number (0-600)	Sets the number of seconds for the allowed user's session once allowed through to the site.	allowedUser CookieEnabled is true
allowedUser CookieRefresh	boolean	Resets the duration of an allowed cookie with each request, so that it only expires if the user doesn't make any requests for the specified duration. Do not enable this option if you want to set a fixed time for all users.	allowedUser CookieEnabled is true
allowedUser CookieAdvanced	boolean	Sets advanced configuration options for the allowed user's cookie.	allowedUser CookieEnabled is true
allowedUser CookieAutomatic Salt	boolean	Sets an automatic <i>salt</i> value to verify the integrity of the cookie for an allowed user. Disable this if you want to share the cookie across properties.	allowedUser CookieEnabled is true AND allowed UserCookie Advanced is true

Option	Type	Description	Requires
allowedUser CookieSalt	string	Specifies a fixed <i>salt</i> value, which is incorporated into the cookie's value to prevent users from manipulating it. You can use the same salt string across different behaviors or properties to apply a single cookie to all allowed users.	allowedUser CookieEnabled is true AND allowed UserCookie Advanced is true AND allowed UserCookie AutomaticSalt is false
allowedUser CookieDomain Type	enum	Specify with allowedUserCookieAdvanced enabled.	allowedUser CookieEnabled is true AND allowed UserCookie Advanced is true
	DYNAMIC	Use the dynamic incoming host header.	
	CUSTOMER	Use a customer-defined cookie domain.	
allowedUser CookieDomain	string	Specifies a domain for an allowed user cookie.	allowedUser CookieEnabled is true AND allowed UserCookie Advanced is true AND allowed UserCookie DomainType is CUSTOMER
allowedUser CookieHttpOnly	boolean	Applies the HttpOnly flag to the allowed user's cookie to ensure it's accessed over HTTP and not manipulated by the client.	allowedUser CookieEnabled is true AND allowed UserCookie Advanced is true
allowedUser CookieSecure	boolean	Applies the Secure flag to the allowed user's cookie to transmit it over a secure connection. You can apply this option only if the property itself is secure. See Secure property requirements for guidance.	allowedUser CookieEnabled is true AND allowed UserCookie Advanced is true AND is_secure is true in top- level rule
waitingRoom CookieEnabled	boolean	Enables a cookie to track a waiting room assignment.	
waitingRoom CookieShare Label	boolean	Enabling this option shares the same allowedUserCookieLabel string. If disabled, specify a different waitingRoomCookieLabel .	waitingRoom CookieEnabled is true AND allowed UserCookie Enabled is true

Option	Type	Description	Requires
waitingRoom CookieLabel	string	Specifies a label to distinguish this waiting room cookie from others. The value appends to the cookie's name, and helps you to maintain the same waiting room assignment across behaviors within a property, and across properties.	waitingRoom CookieEnabled is true
waitingRoom CookieDuration	number (0-120)	Sets the number of seconds for which users remain in the waiting room. During this time, users who refresh the waiting room page remain there.	waitingRoom CookieEnabled is true
waitingRoom CookieAdvanced	boolean	When enabled along with waitingRoomCookieEnabled , sets advanced configuration options for the waiting room cookie.	waitingRoom CookieEnabled is true
waitingRoom CookieAutomatic Salt	boolean	Sets an automatic salt value to verify the integrity of the waiting room cookie. Disable this if you want to share the cookie across properties.	waitingRoom CookieEnabled is true AND waiting RoomCookie Advanced is true
waitingRoom CookieSalt	string	Specifies a fixed salt value, which is incorporated into the cookie's value to prevent users from manipulating it. You can use the same salt string across different behaviors or properties to apply a single cookie for the waiting room session.	waitingRoom CookieEnabled is true AND waiting RoomCookie Advanced is true AND waiting RoomCookie AutomaticSalt is false
waitingRoom CookieDomain Type	enum	Specify with waitingRoomCookieAdvanced enabled, selects whether to use the DYNAMIC incoming host header, or a CUSTOMER -defined cookie domain.	waitingRoom CookieEnabled is true AND waiting RoomCookie Advanced is true
	DYNAMIC	Use the dynamic incoming host header.	
	CUSTOMER	Use a customer-defined cookie domain.	
waitingRoom CookieDomain	string	Specifies a domain for the waiting room cookie.	waitingRoom CookieEnabled is true AND waiting RoomCookie Advanced is true AND waiting RoomCookie DomainType is CUSTOMER
waitingRoom CookieHttpOnly	boolean	Applies the HttpOnly flag to the waiting room cookie to ensure it's accessed over HTTP and not manipulated by the client.	waitingRoom CookieEnabled is true AND waiting RoomCookie Advanced is true

Option	Type	Description	Requires
waitingRoom CookieSecure	boolean	Applies the <code>Secure</code> flag to the waiting room cookie to transmit it over a secure connection. You can apply this option only if the property itself is secure. See Secure property requirements for guidance.	waitingRoom CookieEnabled is <code>true</code> AND waiting RoomCookie Advanced is <code>true</code> AND <code>is_secure</code> is <code>true</code> in top- level rule
waitingRoom StatusCode	number	Specifies the response code for requests sent to the waiting room.	
waitingRoomUse CpCode	boolean	Allows you to assign a different CP code that tracks any requests that are sent to the waiting room.	
waitingRoomCp Code	object	Specifies a <code>cpcode</code> object for requests sent to the waiting room, including a numeric <code>id</code> key and a descriptive <code>name</code> .	waitingRoom UseCpCode is <code>true</code>
waitingRoomCp Code.description	string	Additional description for the CP code.	
waitingRoomCp Code.id	integer	Unique identifier for each CP code.	
waitingRoomCp Code.name	string	The name of the CP code.	
waitingRoomCp Code.products	array	The set of products the CP code is assigned to.	
waitingRoomNet Storage	object	Specifies the NetStorage domain for the waiting room page.	
waitingRoomNet Storage.cpCode List	array	A set of CP codes that apply to this storage group.	
waitingRoomNet Storage.download DomainName	string	Domain name from which content can be downloaded.	
waitingRoomNet Storage.id	number	Unique identifier for the storage group.	
waitingRoomNet Storage.name	string	Name of the storage group.	
waitingRoomNet Storage.upload DomainName	string	Domain name used to upload content.	
waitingRoom Directory	string (allows variables)	Specifies the NetStorage directory that contains the static waiting room page, with no trailing slash character.	
waitingRoom CacheTtl	number (5-30)	Specifies the waiting room page's time to live in the cache, 5 minutes by default.	

watermarkUrl

- **Property Manager name:** [Watermark Token](#)
- **Behavior version:** The v2018-02-27 rule format supports the watermarkUrl behavior v1.1.
- **Rule format status:** [Deprecated, outdated rule format](#)
- **Access:** [Read-write](#)

Aliases a token to a watermark image URL.

Option	Type	Description
token	string	Specifies the string token.
imageUrl	string	Specifies the URL for the watermark image.

webApplicationFirewall

- **Property Manager name:** [Web Application Firewall \(WAF\)](#)
- **Behavior version:** The v2018-02-27 rule format supports the webApplicationFirewall behavior v1.1.
- **Rule format status:** [Deprecated, outdated rule format](#)
- **Access:** [Read-write](#)

This behavior implements a suite of security features that blocks threatening HTTP and HTTPS requests. Use it as your primary firewall, or in addition to existing security measures. Only one referenced configuration is allowed per property, so this behavior typically belongs as part of its default rule.

Option	Type	Description
firewallConfiguration	object	An object featuring details about your firewall configuration.

webSockets

- **Property Manager name:** [WebSockets](#)
- **Behavior version:** The v2018-02-27 rule format supports the webSockets behavior v1.1.
- **Rule format status:** [Deprecated, outdated rule format](#)
- **Access:** [Read-write](#)

The WebSocket protocol allows web applications real-time bidirectional communication between clients and servers.

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

Option	Type	Description
enabled	boolean	Enables WebSocket traffic.

webdav

- **Property Manager name:** [WebDAV](#)✎
- **Behavior version:** The v2018-02-27 rule format supports the webdav behavior v1.1.
- **Rule format status:** [Deprecated, outdated rule format](#)
- **Access:** [Read-write](#)

Web-based Distributed Authoring and Versioning (WebDAV) is a set of extensions to the HTTP protocol that allows users to collaboratively edit and manage files on remote web servers. This behavior enables WebDAV, and provides support for the following additional request methods: PROPFIND, PROPPATCH, MKCOL, COPY, MOVE, LOCK, and UNLOCK. To apply this behavior, you need to match on a [requestMethod](#) .

Option	Type	Description
enabled	boolean	Enables the WebDAV behavior.

v2018-02-27 criteria

v2018-02-27 criteria

This section provides details for all criteria the Property Manager API supports for the v2018-02-27 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 criteria](#) operation.

This v2018-02-27 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.

advancedImMatch

- **Property Manager name:** [Image and Video Manager](#) [↗]
- **Criteria version:** The v2018-02-27 rule format supports the `advancedImMatch` criteria v1.0.
- **Rule format status:** [Deprecated, outdated rule format](#)
- **Access:** [Read-write](#)

Matches whether the `imageManager` behavior already applies to the current set of requests.

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

bucket

- **Property Manager name:** [Percentage of Clients](#)[¶]
- **Criteria version:** The v2018-02-27 rule format supports the bucket criteria v1.1.
- **Rule format status:** [Deprecated, outdated rule format](#)
- **Access:** [Read-write](#)

This matches a specified percentage of requests when used with the required accompanying [spdy](#) behavior. Contact Akamai Professional Services for help configuring it.

Option	Type	Description
percentage	number (0-100)	Specifies the percentage of SPDY requests to match.

cacheability

- **Property Manager name:** [Response Cacheability](#)[¶]
- **Criteria version:** The v2018-02-27 rule format supports the cacheability criteria v1.1.
- **Rule format status:** [Deprecated, outdated rule format](#)
- **Access:** [Read-write](#)

Matches the current cache state. Note that any NO_STORE or BYPASS_CACHE HTTP headers set on the origin's content overrides properties' [caching](#) instructions, in which case this criteria does not apply.

Option	Type	Description
match Operator	enum	Specifies the match's logic.
	IS	Cache state matches the value .
	IS_NOT	Cache state does not match the value .
value	enum	Content's cache is enabled (CACHEABLE) or not (NO_STORE), or else is ignored (BYPASS_CACHE).
	NO_STORE	Content cache is disabled.
	BYPASS_CACHE	Content cache is ignored.
	CACHEABLE	Content cache is enabled.

clientIp

- **Property Manager name:** [Client IP](#)
- **Criteria version:** The v2018-02-27 rule format supports the clientIp criteria v1.1.
- **Rule format status:** [Deprecated, outdated rule format](#)
- **Access:** [Read-write](#)

Matches the IP number of the requesting client.

Option	Type	Description
match Operator	enum	Matches the contents of values if set to IS_ONE_OF , otherwise IS_NOT_ONE_OF reverses the match.
	IS_ONE_OF	Matches any of the specified values .
	IS_NOT_ONE_OF	Does not match any of the specified values .
values	string array	IP or CIDR block, for example: 71.92.0.0/14 .
use Headers	boolean	When connecting via a proxy server as determined by the X-Forwarded-For header, enabling this option matches the connecting client's IP address rather than the original end client specified in the header.

clientIpVersion

- **Property Manager name:** [Client IP Version](#)
- **Criteria version:** The v2018-02-27 rule format supports the clientIpVersion criteria v1.1.
- **Rule format status:** [Deprecated, outdated rule format](#)
- **Access:** [Read-write](#)

Matches the version of the IP protocol used by the requesting client.

Option	Type	Description
value	enum	The IP version of the client request, either IPV4 or IPV6 .
	IPV4	Matches the IPv4 protocol.
	IPV6	Matches the IPv6 protocol.
use XForwarded For	boolean	When connecting via a proxy server as determined by the X-Forwarded-For header, enabling this option matches the connecting client's IP address rather than the original end client specified in the header.

cloudletsOrigin

- **Property Manager name:** [Conditional Origin ID](#)
- **Criteria version:** The v2018-02-27 rule format supports the cloudletsOrigin criteria v1.2.
- **Rule format status:** [Deprecated, outdated rule format](#)
- **Access:** [Read-write](#)

Allows Cloudlets Origins, referenced by label, to define their own criteria to assign custom origin definitions. The criteria may match, for example, for a specified percentage of requests defined by the cloudlet to use an alternative version of a website.

You need to pair this criteria with a sibling [origin](#) definition. It should not appear with any other criteria, and an [allowCloudletsOrigins](#) behavior needs to appear within a parent rule.

Option	Type	Description
originId	string	The Cloudlets Origins identifier, limited to alphanumeric and underscore characters.

contentDeliveryNetwork

- **Property Manager name:** CDN Network
- **Criteria version:** The v2018-02-27 rule format supports the contentDeliveryNetwork criteria v1.2.
- **Rule format status:** [Deprecated, outdated rule format](#)
- **Access:** [Read-write](#)

Specifies the type of Akamai network handling the request.

Option	Type	Description
match Operator	enum	Matches the specified network if set to IS , otherwise IS_NOT reverses the match.
	IS	Matches the specified network .
	IS_NOT	Does not match the specified network .
network	enum	Match the network.
	STAGING	Match the staging network.
	PRODUCTION	Match the production network.

contentType

- **Property Manager name:** [Content Type](#)
- **Criteria version:** The v2018-02-27 rule format supports the contentType criteria v1.1.

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

Matches the HTTP response header's `Content-Type` .

Option	Type	Description
<code>match</code> Operator	enum	Matches any <code>Content-Type</code> among specified <code>values</code> when set to <code>IS_ONE_OF</code> , otherwise <code>IS_NOT_ONE_OF</code> reverses the match.
	<code>IS_ONE_OF</code>	Matches any <code>Content-Type</code> among the specified <code>values</code> .
	<code>IS_NOT_ONE_OF</code>	Matches none of the specified <code>values</code> .
<code>values</code>	string array	<code>Content-Type</code> response header value, for example <code>text/html</code> .
<code>match</code> Wildcard	boolean	Allows <code>*</code> and <code>?</code> wildcard matches among the <code>values</code> , so that specifying <code>text/*</code> matches both <code>text/html</code> and <code>text/css</code> .
<code>matchCase</code> Sensitive	boolean	Sets a case-sensitive match for all <code>values</code> .

deviceCharacteristic

- **Property Manager name:** [Device Characteristics](#)[↗]
- **Criteria version:** The `v2018-02-27` rule format supports the `deviceCharacteristic` criteria v1.3.
- **Rule format status:** [Deprecated, outdated rule format](#)
- **Access:** [Read-write](#)

Match various aspects of the device or browser making the request. Based on the value of the `characteristic` option, the expected value is either a boolean, a number, or a string, possibly representing a version number. Each type of value requires a different field.

Option	Type	Description	Requires
<code>characteristic</code>	enum	Aspect of the device or browser to match.	
	<code>BRAND_NAME</code>	String value such as <code>Samsung</code> or <code>Apple</code> .	
	<code>MODEL_NAME</code>	String value such as <code>SCH-I110</code> .	
	<code>MARKETING_NAME</code>	String value such as <code>Samsung Illusion</code> .	
	<code>IS_WIRELESS_DEVICE</code>	Boolean value.	
	<code>IS_TABLET</code>	Boolean value, subset of <code>IS_MOBILE</code> .	
	<code>DEVICE_OS</code>	String value.	

Option	Type	Description	Requires
	DEVICE_OS_VERSION	Version string value.	
	MOBILE_BROWSER	String value.	
	MOBILE_BROWSER_VERSION	Version string value.	
	RESOLUTION_WIDTH	Number of pixels wide.	
	RESOLUTION_HEIGHT	Number of pixels high.	
	PHYSICAL_SCREEN_HEIGHT	Number of millimeters high.	
	PHYSICAL_SCREEN_WIDTH	Number of millimeters wide.	
	COOKIE_SUPPORT	Boolean value.	
	AJAX_SUPPORT_JAVASCRIPT	Boolean value.	
	FULL_FLASH_SUPPORT	Boolean value.	
	ACCEPT_THIRD_PARTY_COOKIE	Boolean value.	
	XHTML_SUPPORT_LEVEL	Numeric value.	
	IS_MOBILE	Boolean value.	
stringMatch Operator	enum	When the <code>characteristic</code> expects a string value, set this to <code>MATCHES_ONE_OF</code> to match against the <code>stringValue</code> set, otherwise set to <code>DOES_NOT_MATCH_ONE_OF</code> to exclude that set of values.	<code>characteristic</code> is either: <code>BRAND_NAME</code> , <code>MODEL_NAME</code> , <code>MARKETING_NAME</code> , <code>DEVICE_OS</code> , <code>MOBILE_BROWSER</code> , <code>PREFERRED_MARKUP</code> , <code>HTML_PREFERRED_DTD</code> , <code>XHTML_PREFERRED_CHARSET</code> , <code>VIEWPORT_WIDTH</code> , <code>XHTMLMP_PREFERRED_MIME_TYPE</code> , <code>AJAX_PREFERRED_GEOLOC_API</code> , <code>XHTML_FILE_UPLOAD</code> , <code>XHTML_SUPPORTS_IFRAME</code> , <code>FLASH_LITE_VERSION</code>
	MATCHES_ONE_OF	The value is included as a string Value .	
	DOES_NOT_MATCH_ONE_OF	The value is not included as a <code>stringValue</code> .	
numericMatch Operator	enum	When the <code>characteristic</code> expects a numeric value, compares the specified <code>numericValue</code> against the matched client.	<code>characteristic</code> is either: <code>RESOLUTION_WIDTH</code> , <code>RESOLUTION_HEIGHT</code> , <code>PHYSICAL_SCREEN_HEIGHT</code> , <code>PHYSICAL_SCREEN_WIDTH</code> , <code>XHTML_SUPPORT_LEVEL</code> , <code>MAX_IMAGE_WIDTH</code> , <code>MAX_IMAGE_HEIGHT</code> , <code>VIEWPORT_INITIAL_SCALE</code>
	IS	Values are equal.	
	IS_NOT	Values are not equal.	

Option	Type	Description	Requires
	IS_LESS_THAN	The numericValue is less than the matched client.	
	IS_LESS_THAN_OR_EQUAL	The numericValue is less than or equal to the matched client.	
	IS_MORE_THAN	The numericValue is more than the matched client.	
	IS_MORE_THAN_OR_EQUAL	The numericValue is more than or equal to the matched client.	
versionMatch Operator	enum	When the characteristic expects a version string value, compares the specified versionValue against the matched client, using the following operators: IS, IS_MORE_THAN_OR_EQUAL, IS_MORE_THAN, IS_LESS_THAN_OR_EQUAL, IS_LESS_THAN, IS_NOT.	characteristic is either: DEVICE_OS_VERSION, MOBILE_BROWSER_VERSION
	IS	The versionValue equals the matched client.	
	IS_NOT	The versionValue does not equal the matched client.	
	IS_LESS_THAN	The versionValue is less than the matched client.	
	IS_LESS_THAN_OR_EQUAL	The versionValue is less than or equal to the matched client.	
	IS_MORE_THAN	The versionValue is more than the matched client.	
	IS_MORE_THAN_OR_EQUAL	The versionValue is more than or equal to the matched client.	
booleanValue	boolean	When the characteristic expects a boolean value, this specifies the value.	characteristic is either: IS_WIRELESS_DEVICE, IS_TABLET, COOKIE_SUPPORT, AJAX_SUPPORT, JAVASCRIPT, FULL_FLASH_SUPPORT, DUAL_ORIENTATION, ACCEPT_THIRD_PARTY_COOKIE, GIF_ANIMATED, JPG, PNG, XHTML_SUPPORTS_TABLE_FOR_LAYOUT, XHTML_TABLE_SUPPORT, PDF_SUPPORT, IS_MOBILE
stringValue	string array	When the characteristic expects a string, this specifies the set of values.	stringMatchOperator is either: MATCHES_ONE_OF, DOES_NOT_MATCH_ONE_OF
numericValue	number	When the characteristic expects a numeric value, this specifies the number.	numericMatchOperator is either: IS, IS_NOT, IS_LESS_THAN, IS_LESS_THAN_OR_EQUAL, IS_MORE_THAN, IS_MORE_THAN_OR_EQUAL
versionValue	string	When the characteristic expects a version number, this specifies it as a string.	versionMatchOperator is either: IS, IS_NOT, IS_LESS_THAN, IS_LESS_THAN_OR_EQUAL, IS_MORE_THAN, IS_MORE_THAN_OR_EQUAL
matchCase Sensitive	boolean	Sets a case-sensitive match for the stringValue field.	stringMatchOperator is either: MATCHES_ONE_OF, DOES_NOT_MATCH_ONE_OF
match Wildcard	boolean	Allows * and ? wildcard matches in the stringValue field.	stringMatchOperator is either: MATCHES_ONE_OF, DOES_NOT_MATCH_ONE_OF

fileExtension

- **Property Manager name:** [File Extension](#)
- **Criteria version:** The v2018-02-27 rule format supports the fileExtension criteria v1.1.
- **Rule format status:** [Deprecated, outdated rule format](#)
- **Access:** [Read-write](#)

Matches the requested filename's extension, if present.

Option	Type	Description
match Operator	enum	Matches the contents of values if set to IS_ONE_OF , otherwise IS_NOT_ONE_OF reverses the match.
	IS_ONE_OF	Matches any of the specified values .
	IS_NOT_ONE_OF	Does not match any of the specified values .
values	string array	An array of file extension strings, with no leading dot characters, for example png , jpg , jpeg , and gif .
matchCase Sensitive	boolean	Sets a case-sensitive match.

filename

- **Property Manager name:** [Filename](#)
- **Criteria version:** The v2018-02-27 rule format supports the filename criteria v1.1.
- **Rule format status:** [Deprecated, outdated rule format](#)
- **Access:** [Read-write](#)

Matches the requested filename, or test whether it is present.

Option	Type	Description	Requires
match Operator	enum	If set to IS_ONE_OF or IS_NOT_ONE_OF , matches whether the filename matches one of the values . If set to IS_EMPTY or IS_NOT_EMPTY , matches whether the specified filename is part of the path.	
	IS_ONE_OF	The filename matches one of the values .	
	IS_NOT_ONE_OF	The filename does not match one of the values .	
	IS_EMPTY	The filename is not part of the path.	
	IS_NOT_EMPTY	The filename is part of the path.	

Option	Type	Description	Requires
values	string array	Matches the filename component of the request URL. Wildcards are allowed, where ? matches a single character and * matches more than one. For example, specify filename.* to accept any extension.	matchOperator is either: IS_ONE_OF , IS_NOT_ONE_OF
match Case Sensitive	boolean	Sets a case-sensitive match for the value field.	matchOperator is either: IS_ONE_OF , IS_NOT_ONE_OF

hostname

- **Property Manager name:** [Hostname](#)
- **Criteria version:** The v2018-02-27 rule format supports the hostname criteria v1.1.
- **Rule format status:** [Deprecated, outdated rule format](#)
- **Access:** [Read-write](#)

Matches the requested hostname.

Option	Type	Description
match Operator	enum	Matches the contents of values when set to IS_ONE_OF , otherwise IS_NOT_ONE_OF reverses the match.
	IS_ONE_OF	Matches the contents of values .
	IS_NOT_ONE_OF	Does not match the contents of values .
values	string array	A list of hostnames. Wildcards match, so *.example.com matches both m.example.com and www.example.com .

matchAdvanced

- **Property Manager name:** Advanced Match
- **Criteria version:** The v2018-02-27 rule format supports the matchAdvanced criteria v1.1.
- **Rule format status:** [Deprecated, outdated rule format](#)
- **Access:** [Read-only](#)

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

Option	Type	Description
description	string	A human-readable description of what the XML block does.

Option	Type	Description
openXml	string	An XML string that opens the relevant block.
closeXml	string	An XML string that closes the relevant block.

matchCpCode

- **Property Manager name:** [Content Provider Code](#)^{*)}
- **Criteria version:** The v2018-02-27 rule format supports the matchCpCode criteria v1.1.
- **Rule format status:** [Deprecated, outdated rule format](#)
- **Access:** [Read-write](#)

Match the assigned content provider code.

Option	Type	Description
value	object	Specifies an object that encodes the matching value , including 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.

matchResponseCode


- **Property Manager name:** [Response Status Code](#)^{*)}
- **Criteria version:** The v2018-02-27 rule format supports the matchResponseCode criteria v1.2.
- **Rule format status:** [Deprecated, outdated rule format](#)
- **Access:** [Read-write](#)

Match a set or range of HTTP response codes.

Option	Type	Description	Requires
match Operator	enum	Matches numeric range or a specified set of values .	
	IS_ONE_OF	Matches the contents of values .	
	IS_NOT_ONE_OF	Does not match the contents of values .	

Option	Type	Description	Requires
	IS_BETWEEN	Matches the numeric range between <code>lowerBound</code> and <code>upperBound</code> .	
	IS_NOT_BETWEEN	Does not match the numeric range between <code>lowerBound</code> and <code>upperBound</code> .	
values	string array	A set of response codes to match, for example <code>["404","500"]</code> .	<code>matchOperator</code> is either: IS_ONE_OF , IS_NOT_ONE_OF
lower Bound	number	Specifies the start of a range of responses. For example, <code>400</code> to match anything from <code>400</code> to <code>500</code> .	<code>matchOperator</code> is either: IS_BETWEEN , IS_NOT_BETWEEN
upper Bound	number	Specifies the end of a range of responses. For example, <code>500</code> to match anything from <code>400</code> to <code>500</code> .	<code>matchOperator</code> is either: IS_BETWEEN , IS_NOT_BETWEEN

matchVariable

- **Property Manager name:** [Variable](#) 
- **Criteria version:** The `v2018-02-27` rule format supports the `matchVariable` criteria v1.2.
- **Rule format status:** [Deprecated, outdated rule format](#)
- **Access:** [Read-write](#)

Matches a built-in variable, or a custom variable pre-declared within the rule tree by the [set Variable](#) behavior. See [Support for variables](#) for more information on this feature.

Option	Type	Description	Requires
variable Name	string (variable name)	The name of the variable to match.	
match Operator	enum	The type of match, based on which you use different options to specify the match criteria.	
	IS	Matches the <code>variableExpression</code> string.	
	IS_NOT	Does not match the <code>variable Expression</code> string.	
	IS_ONE_OF	Matches any of an array of string <code>variableValues</code> .	
	IS_NOT_ONE_OF	Does not match any of an array of string <code>variableValues</code> .	
	IS_EMPTY	Matches if a defined variable does not contain a value. You can't activate a rule that matches an undefined variable.	
	IS_NOT_EMPTY	Matches if a defined variable contains a value. You can't activate a rule that matches an undefined variable.	
	IS_BETWEEN	Is between the numeric <code>lowerBound</code> and <code>upperBound</code> values.	

Option	Type	Description	Requires
	IS_NOT_BETWEEN	Is outside the numeric lowerBound and upperBound range.	
	IS_GREATER_THAN	Is greater than the variable Expression string-formatted number.	
	IS_GREATER_THAN_OR_EQUAL_TO	Is greater than or equal to the variableExpression string-formatted number.	
	IS_LESS_THAN	Is less than the variableExpression string-formatted number.	
	IS_LESS_THAN_OR_EQUAL_TO	Is less than or equal to the variable Expression string-formatted number.	
variable Values	string array	Specifies an array of matching strings.	matchOperator is either: IS_ONE_OF, IS_NOT_ONE_OF
variable Expression	string (allows variables)	Specifies a single matching string.	matchOperator is either: IS, IS_NOT, IS_GREATER_THAN, IS_GREATER_THAN_OR_EQUAL_TO, IS_LESS_THAN, IS_LESS_THAN_OR_EQUAL_TO
lower Bound	string	Specifies the range's numeric minimum value.	matchOperator is either: IS_BETWEEN, IS_NOT_BETWEEN
upper Bound	string	Specifies the range's numeric maximum value.	matchOperator is either: IS_BETWEEN, IS_NOT_BETWEEN
match Wildcard	boolean	When matching string expressions, enabling this matches wildcard metacharacters such as * and ? .	matchOperator is either: IS, IS_NOT, IS_ONE_OF, IS_NOT_ONE_OF
match Case Sensitive	boolean	When matching string expressions, enabling this performs a case-sensitive match.	matchOperator is either: IS, IS_NOT, IS_ONE_OF, IS_NOT_ONE_OF

metadataStage

- **Property Manager name:** [Metadata Stage](#)
- **Criteria version:** The v2018-02-27 rule format supports the metadataStage criteria v1.0.
- **Rule format status:** [Deprecated, outdated rule format](#)
- **Access:** [Read-write](#)

Matches how the current rule corresponds to low-level syntax elements in translated XML metadata, indicating progressive stages as each edge server handles the request and response. To use this match, you need to be thoroughly familiar with how Akamai edge servers process requests. Contact your Akamai Technical representative if you need help, and test thoroughly on staging before activating on production.

Option	Type	Description
match Operator	enum	Compares the current rule with the specified metadata stage.
	IS	The current rule is at the specified metadata stage.

Option	Type	Description
	IS_NOT	The current rule is not at the specified metadata stage.
value	enum	Specifies the metadata stage.
	cache-hit	Content is cacheable and is already cached, but not yet tested for freshness.
	client-done	Occurs after the response completes and the response has been sent to the requesting client Only used for receipt requests and products like Cloud Monitor and Datastream.
	client-request	When the Akamai server receives the request. Most processing happens in this stage, including determining the object's cacheability and cache key.
	client-request-body	Runs when the Akamai server inspects the contents of a request POST body, typically as a security check.
	client-response	Occurs after the full response has been returned from the forward server or retrieved from Akamai's cache, prior to constructing a response.
	content-policy	This stage determines whether any Cloudlets or security products are associated with the request. It gets ignored in requests for other products.
	forward-request	Immediately before the Akamai server tries to connect to a forward server (either an Akamai parent server or a customer origin). Doesn't run for the content retrieved from Akamai's cache.
	forward-response	After the forward server responds and all response headers have been read. Doesn't run for the content retrieved from Akamai's cache.
	forward-start	Immediately before the <code>forward-request</code> stage, while the Akamai server selects a forward server or persistent connection. Doesn't run for the content retrieved from Akamai's cache.
	ipa-response	Runs when a response is received from an intermediate processing agent (IPA) server, called at the end of the <code>client-request</code> stage.

originTimeout

- **Property Manager name:** [Origin Timeout](#)
- **Criteria version:** The `v2018-02-27` rule format supports the `originTimeout` criteria v1.1.
- **Rule format status:** [Deprecated, outdated rule format](#)
- **Access:** [Read-write](#)

Matches when the origin responds with a timeout error.

Option	Type	Description
matchOperator	enum	Specifies a single required <code>ORIGIN_TIMED_OUT</code> value.
	ORIGIN_TIMED_OUT	This is currently the only supported value.

path

- **Property Manager name:** [Path](#) [↗]
- **Criteria version:** The v2018-02-27 rule format supports the path criteria v1.1.
- **Rule format status:** [Deprecated, outdated rule format](#)
- **Access:** [Read-write](#)

Matches the URL's non-hostname path component.

Option	Type	Description
match Operator	enum	Matches the contents of the values array.
	MATCHES_ONE_OF	Matches any of the values array.
	DOES_NOT_MATCH_ONE_OF	Matches none of the values array.
values	string array	Matches the URL path, excluding leading hostname and trailing query parameters. The path is relative to the server root, for example /blog . The value accepts * or ? wildcard characters, for example /blog/*/2014 .
match Case Sensitive	boolean	Sets a case-sensitive match.

queryStringParameter

- **Property Manager name:** [Query String Parameter](#) [↗]
- **Criteria version:** The v2018-02-27 rule format supports the queryStringParameter criteria v1.1.
- **Rule format status:** [Deprecated, outdated rule format](#)
- **Access:** [Read-write](#)

Matches query string field names or values.

Option	Type	Description	Requires
parameter Name	string	The name of the query field, for example, q in ?q=string .	
match Operator	enum	Narrows the match criteria.	
	IS_ONE_OF	Tests whether the field's value string matches.	
	IS_NOT_ONE_OF	Tests whether the field's value string does not match.	
	EXISTS	Whether the query field's parameterName is present in the requesting URL.	

Option	Type	Description	Requires
	DOES_NOT_EXIST	Whether the query field's <code>parameterName</code> is absent from the requesting URL.	
	IS_LESS_THAN	Matches a range when the <code>value</code> is numeric.	
	IS_MORE_THAN	Matches a range when the <code>value</code> is numeric.	
	IS_BETWEEN	Is between the numeric <code>lowerBound</code> and <code>upperBound</code> values.	
<code>values</code>	string array	The value of the query field, for example, <code>string</code> in <code>?q=string</code> .	<code>matchOperator</code> is either: <code>IS_ONE_OF</code> , <code>IS_NOT_ONE_OF</code>
<code>lowerBound</code>	number	Specifies the match's minimum value.	<code>matchOperator</code> is either: <code>IS_MORE_THAN</code> , <code>IS_BETWEEN</code>
<code>upperBound</code>	number	When the <code>value</code> is numeric, this field specifies the match's maximum value.	<code>matchOperator</code> is either: <code>IS_LESS_THAN</code> , <code>IS_BETWEEN</code>
<code>matchWildcardName</code>	boolean	Allows <code>*</code> and <code>?</code> wildcard matches in the <code>parameterName</code> field.	
<code>matchCaseSensitiveName</code>	boolean	Sets a case-sensitive match for the <code>parameterName</code> field.	
<code>matchWildcardValue</code>	boolean	Allows <code>*</code> and <code>?</code> wildcard matches in the <code>value</code> field.	<code>matchOperator</code> is either: <code>IS_ONE_OF</code> , <code>IS_NOT_ONE_OF</code>
<code>matchCaseSensitiveValue</code>	boolean	Sets a case-sensitive match for the <code>value</code> field.	<code>matchOperator</code> is either: <code>IS_ONE_OF</code> , <code>IS_NOT_ONE_OF</code>
<code>escapeValue</code>	boolean	Matches when the <code>value</code> is URL-escaped.	<code>matchOperator</code> is either: <code>IS_ONE_OF</code> , <code>IS_NOT_ONE_OF</code>

random

- **Property Manager name:** [Sample Percentage](#)^{*}
- **Criteria version:** The `v2018-02-27` rule format supports the `random` criteria v1.0.
- **Rule format status:** [Deprecated, outdated rule format](#)
- **Access:** [Read-write](#)

Matches a specified percentage of requests. Use this match to apply behaviors to a percentage of your incoming requests that differ from the remainder, useful for A/b testing, or to offload traffic onto different servers.

Option	Type	Description
<code>bucket</code>	number (0-100)	Specify a percentage of random requests to which to apply a behavior. Any remainders do not match.

regularExpression

- **Property Manager name:** [Regex](#)
- **Criteria version:** The v2018-02-27 rule format supports the `regularExpression` criteria v1.0.
- **Rule format status:** [Deprecated, outdated rule format](#)
- **Access:** [Read-write](#)

Matches a regular expression against a string, especially to apply behaviors flexibly based on the contents of dynamic [variables](#).

Option	Type	Description
<code>matchString</code>	string (allows variables)	The string to match, typically the contents of a dynamic variable.
<code>regex</code>	string	The regular expression (PCRE) to match against the string.
<code>caseSensitive</code>	boolean	Sets a case-sensitive regular expression match.

requestCookie

- **Property Manager name:** [Request Cookie](#)
- **Criteria version:** The v2018-02-27 rule format supports the `requestCookie` criteria v1.1.
- **Rule format status:** [Deprecated, outdated rule format](#)
- **Access:** [Read-write](#)

Match the cookie name or value passed with the request.

Option	Type	Description	Requires
<code>cookieName</code>	string	The name of the cookie, for example, <code>visitor</code> in <code>visitor:anon</code> .	
<code>matchOperator</code>	enum	Narrows the match criteria.	
	IS	If the field's <code>value</code> string matches.	
	IS_NOT	If the field's <code>value</code> string does not match.	
	EXISTS	Matches if the <code>cookieName</code> cookie exists.	
	DOES_NOT_EXIST	Matches if the <code>cookieName</code> cookie does not exist.	
	IS_BETWEEN	Is between the numeric <code>lowerBound</code> and <code>upperBound</code> values.	
<code>value</code>	string	The cookie's value, for example, <code>anon</code> in <code>visitor:anon</code> .	<code>matchOperator</code> is either: <code>IS</code> , <code>IS_NOT</code>
<code>lowerBound</code>	number	When the <code>value</code> is numeric, this field specifies the match's minimum value.	<code>matchOperator</code> is <code>IS_BETWEEN</code>
<code>upperBound</code>	number	When the <code>value</code> is numeric, this field specifies the match's maximum value.	<code>matchOperator</code> is <code>IS_BETWEEN</code>

Option	Type	Description	Requires
matchWildcard Name	boolean	Allows * and ? wildcard matches in the cookieName field.	
matchCase SensitiveName	boolean	Sets a case-sensitive match for the cookieName field.	
matchWildcard Value	boolean	Allows * and ? wildcard matches in the value field.	matchOperator is either: IS , IS_NOT
matchCase SensitiveValue	boolean	Sets a case-sensitive match for the value field.	matchOperator is either: IS , IS_NOT

requestHeader

- **Property Manager name:** [Request Header](#)*
- **Criteria version:** The v2018-02-27 rule format supports the requestHeader criteria v1.1.
- **Rule format status:** [Deprecated, outdated rule format](#)
- **Access:** [Read-write](#)

Match HTTP header names or values.

Option	Type	Description	Requires
header Name	string	The name of the request header, for example Accept-Language .	
match Operator	enum	Narrows the match criteria.	
	IS_ONE_OF	Tests whether the field's value string matches.	
	IS_NOT_ONE_OF	Tests whether the field's value string does not match.	
	EXISTS	Tests if the headerName field exists.	
	DOES_NOT_EXIST	Tests if the headerName field is absent.	
values	string array	The request header's value, for example en-US when the header headerName is Accept-Language .	matchOperator is either: IS_ONE_OF , IS_NOT_ONE_OF
match Wildcard Name	boolean	Allows * and ? wildcard matches in the headerName field.	
match Wildcard Value	boolean	Allows * and ? wildcard matches in the value field.	matchOperator is either: IS_ONE_OF , IS_NOT_ONE_OF
matchCase Sensitive Value	boolean	Sets a case-sensitive match for the value field.	matchOperator is either: IS_ONE_OF , IS_NOT_ONE_OF

requestMethod

- **Property Manager name:** [Request Method](#)
- **Criteria version:** The v2018-02-27 rule format supports the requestMethod criteria v1.3.
- **Rule format status:** [Deprecated, outdated rule format](#)
- **Access:** [Read-write](#)

Specify the request's HTTP verb. Also supports WebDAV methods and common Akamai operations.

Option	Type	Description
matchOperator	enum	Matches the value when set to IS , otherwise IS_NOT reverses the match.
	IS	Matches the value .
	IS_NOT	Does not match the value .
value	enum	Any of these HTTP methods, WebDAV methods, or Akamai operations.
	GET	Standard HTTP method.
	POST	Standard HTTP method.
	HEAD	Standard HTTP method.
	PUT	Standard HTTP method.
	PATCH	Standard HTTP method.
	HTTP_DELETE	Standard HTTP method. Note the additional prefix.
	AKAMAI_TRANSLATE	Akamai operation.
	AKAMAI_PURGE	Akamai operation.
	OPTIONS	Standard HTTP method.
	DAV_ACL	WebDAV method.
	DAV_CHECKOUT	WebDAV method.
	DAV_COPY	WebDAV method.
	DAV_DMCREATE	WebDAV method.
	DAV_DMINDEX	WebDAV method.
	DAV_DMMKPATH	WebDAV method.
	DAV_DMMKPATHS	WebDAV method.
	DAV_DMOVERLAY	WebDAV method.
	DAV_DMPATCHPATHS	WebDAV method.
	DAV_LOCK	WebDAV method.
	DAV_MERGE	WebDAV method.
	DAV_MKACTIVITY	WebDAV method.
	DAV_MKCALENDAR	WebDAV method.
	DAV_MKCOL	WebDAV method.
	DAV_MOVE	WebDAV method.

Option	Type	Description
	DAV_PROPFIND	WebDAV method.
	DAV_PROPPATCH	WebDAV method.
	DAV_REPORT	WebDAV method.
	DAV_SETPROCESS	WebDAV method.
	DAV_SETREDIRECT	WebDAV method.
	DAV_TRUTHGET	WebDAV method.
	DAV_UNLOCK	WebDAV method.

requestProtocol

- **Property Manager name:** [Request Protocol](#)
- **Criteria version:** The v2018-02-27 rule format supports the requestProtocol criteria v1.0.
- **Rule format status:** [Deprecated, outdated rule format](#)
- **Access:** [Read-write](#)

Matches whether the request uses the HTTP or HTTPS protocol.

Option	Type	Description
value	enum	Specifies the protocol.
		Supported values: HTTP HTTPS

requestType

- **Property Manager name:** [Request Type](#)
- **Criteria version:** The v2018-02-27 rule format supports the requestType criteria v1.1.
- **Rule format status:** [Deprecated, outdated rule format](#)
- **Access:** [Read-write](#)

Matches the basic type of request. To use this match, you need to be thoroughly familiar with how Akamai edge servers process requests. Contact your Akamai Technical representative if you need help, and test thoroughly on staging before activating on production.

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

Option	Type	Description
match Operator	enum	Specifies whether the request <code>IS</code> or <code>IS_NOT</code> the type of specified <code>value</code> .
	<code>IS</code>	The request is the type of specified <code>value</code> .
	<code>IS_NOT</code>	The request is not the type of specified <code>value</code> .
value	enum	Specifies the type of request, either a standard <code>CLIENT_REQ</code> , an <code>ESI_FRAGMENT</code> , or an <code>EW_SUBREQUEST</code> .
	<code>CLIENT_REQ</code>	A client request.
	<code>ESI_FRAGMENT</code>	An Edge Side Include fragment.
	<code>EW_SUBREQUEST</code>	An EdgeWorkers sub-request.

responseHeader


- **Property Manager name:** [Response Header](#)
- **Criteria version:** The `v2018-02-27` rule format supports the `responseHeader` criteria v1.1.
- **Rule format status:** [Deprecated, outdated rule format](#)
- **Access:** [Read-write](#)

Match HTTP header names or values.

Option	Type	Description	Requires
header Name	string	The name of the response header, for example <code>Content-Type</code> .	
match Operator	enum	Narrows the match according to various criteria.	
	<code>IS_ONE_OF</code>	The field's <code>value</code> string matches.	
	<code>IS_NOT_ONE_OF</code>	The field's <code>value</code> string does not match.	
	<code>EXISTS</code>	The HTTP field <code>headerName</code> is present.	
	<code>DOES_NOT_EXIST</code>	The HTTP field <code>headerName</code> is absent.	
	<code>IS_LESS_THAN</code>	Matches ranges when the <code>value</code> is numeric.	
	<code>IS_MORE_THAN</code>	Matches ranges when the <code>value</code> is numeric.	
	<code>IS_BETWEEN</code>	Is between the numeric <code>lowerBound</code> and <code>upperBound</code> values.	
values	string array	The response header's value, for example <code>application/x-www-form-urlencoded</code> when the header <code>headerName</code> is <code>Content-Type</code> .	<code>matchOperator</code> is either: <code>IS_ONE_OF</code> , <code>IS_NOT_ONE_OF</code>

Option	Type	Description	Requires
lower Bound	number	When the <code>value</code> is numeric, this field specifies the match's minimum value.	<code>matchOperator</code> is either: <code>IS_MORE_THAN</code> , <code>IS_BETWEEN</code>
upper Bound	number	When the <code>value</code> is numeric, this field specifies the match's maximum value.	<code>matchOperator</code> is either: <code>IS_LESS_THAN</code> , <code>IS_BETWEEN</code>
match Wildcard Name	boolean	Allows <code>*</code> and <code>?</code> wildcard matches in the <code>headerName</code> field.	
match Wildcard Value	boolean	Allows <code>*</code> and <code>?</code> wildcard matches in the <code>value</code> field.	<code>matchOperator</code> is either: <code>IS_ONE_OF</code> , <code>IS_NOT_ONE_OF</code>
match Case Sensitive Value	boolean	When enabled, the match is case-sensitive for the <code>value</code> field.	<code>matchOperator</code> is either: <code>IS_ONE_OF</code> , <code>IS_NOT_ONE_OF</code>

time

- **Property Manager name:** [Time Interval](#) 
- **Criteria version:** The `v2018-02-27` rule format supports the `time` criteria v1.1.
- **Rule format status:** [Deprecated, outdated rule format](#)
- **Access:** [Read-write](#)

Specifies ranges of times during which the request occurred.

Option	Type	Description	Requires
match Operator	enum	Specifies how to define the range of time.	
	BEGINNING	The duration is indefinite, using the value of <code>beginDate</code> .	
	BETWEEN	Sets a single range between two dates, using the values of <code>beginDate</code> and <code>endDate</code> .	
	LASTING	Sets a single range, but based on duration relative to the starting time. It relies on the values of <code>lastingDate</code> and <code>lastingDuration</code> .	
	REPEATING	Allows a <code>LASTING</code> -style range to repeat at regular intervals. It relies on the values of <code>repeatBeginDate</code> , <code>repeatDuration</code> , and <code>repeatInterval</code> .	
repeat Interval	string (duration)	Sets the time between each repeating time period's starting points.	<code>match Operator</code> is <code>REPEATING</code>
repeat Duration	string (duration)	Sets the duration of each repeating time period.	<code>match Operator</code> is <code>REPEATING</code>
lasting Duration	string (duration)	Specifies the end of a time period as a duration relative to the <code>lasting Date</code> .	<code>match Operator</code> is <code>LASTING</code>

Option	Type	Description	Requires
lasting Date	string (timestamp)	Sets the start of a fixed time period.	match Operator is LASTING
repeat Begin Date	string (timestamp)	Sets the start of the initial time period.	match Operator is REPEATING
apply Daylight Savings Time	boolean	Adjusts the start time plus repeat interval to account for daylight saving time. Applies when the current time and the start time use different systems, daylight and standard, and the two values are in conflict.	match Operator is REPEATING
begin Date	string (timestamp)	Sets the start of a time period.	match Operator is BEGINNING OR match Operator is BETWEEN
end Date	string (timestamp)	Sets the end of a fixed time period.	match Operator is BETWEEN

tokenAuthorization

- **Property Manager name:** Token Verification Result
- **Criteria version:** The v2018-02-27 rule format supports the tokenAuthorization criteria v1.2.
- **Rule format status:** [Deprecated, outdated rule format](#)
- **Access:** [Read-write](#)

Match on Auth Token 2.0 verification results.

Option	Type	Description	Requires
matchOperator	enum	Error match scope.	
	IS_SUCCESS	No errors occurred.	
	IS_CUSTOM_FAILURE	Match any error in statusList .	
	IS_ANY_FAILURE	Any error occurred.	

userAgent

- **Property Manager name:** [User Agent](#)
- **Criteria version:** The v2018-02-27 rule format supports the userAgent criteria v1.1.

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

Matches the user agent string that helps identify the client browser and device.

Option	Type	Description
match Operator	enum	Matches the specified set of values when set to IS_ONE_OF , otherwise IS_NOT_ONE_OF reverses the match.
	IS_ONE_OF	Matches any of the specified values .
	IS_NOT_ONE_OF	Does not match any of the specified values .
values	string array	The User-Agent header's value. For example, Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1) .
match Wildcard	boolean	Allows * and ? wildcard matches in the value field. For example, *Android* , *iPhone5* , *Firefox* , or *Chrome* .
matchCase Sensitive	boolean	Sets a case-sensitive match for the value field.

userLocation

- **Property Manager name:** [User Location Data](#)✎
- **Criteria version:** The v2018-02-27 rule format supports the userLocation criteria v1.1.
- **Rule format status:** [Deprecated, outdated rule format](#)
- **Access:** [Read-write](#)

The client browser's approximate geographic location, determined by looking up the IP address in a database.

Option	Type	Description	Requires
field	enum	Indicates the geographic scope.	
	COUNTRY	Country.	
	CONTINENT	Continent.	
	REGION	States or provinces within a country.	
match Operator	enum	Matches the specified set of values when set to IS_ONE_OF , otherwise IS_NOT_ONE_OF reverses the match.	
	IS_ONE_OF	Matches any of the specified values .	
	IS_NOT_ONE_OF	Does not match any of the specified values .	
country Values	string array	ISO 3166-1 country codes, such as US or CN .	field is COUNTRY
continent Values	string array	Continent codes.	field is CONTINENT

Option	Type	Description	Requires
	AF	Africa.	
	AS	Asia.	
	EU	Europe.	
	NA	North America.	
	OC	Oceania.	
	OT	Antarctica.	
	SA	South America.	
region Values	string array	ISO 3166 country and region codes, for example US:MA for Massachusetts or JP:13 for Tokyo.	field is REGION
checkIps	enum	Specifies which IP addresses determine the user's location.	
	BOTH	Behaves like HEADERS , but also considers the connecting client's IP address.	
	CONNECTING	Considers the connecting client's IP address.	
	HEADERS	Considers IP addresses specified in the X-Forwarded-For header, succeeding if any of them match.	
useOnlyFirstXForwardedForIp	boolean	When connecting via a proxy server as determined by the x-Forwarded-For header, enabling this option matches the end client specified in the header. Disabling it matches the connecting client's IP address.	checkIps is either: BOTH , HEADERS

userNetwork

- **Property Manager name:** [User Network Data](#)
- **Criteria version:** The v2018-02-27 rule format supports the userNetwork criteria v1.1.
- **Rule format status:** [Deprecated, outdated rule format](#)
- **Access:** [Read-write](#)

Matches details of the network over which the request was made, determined by looking up the IP address in a database.

Option	Type	Description	Requires
field	enum	The type of information to match.	
	NETWORK	A specific network.	
	NETWORK_TYPE	A more general NETWORK_TYPE .	
	BANDWIDTH	Bandwidth.	
match Operator	enum	Matches the specified set of values when set to IS_ONE_OF , otherwise IS_NOT_ONE_OF reverses the match.	
	IS_ONE_OF	Matches any of the specified values .	

Option	Type	Description	Requires																																																																																																															
	IS_NOT_ONE_OF	Does not match any of the specified values .																																																																																																																
network Values	string array	Any set of specific networks.	field is NETWORK																																																																																																															
		<div>Supported values:</div> <div><table><tbody><tr><td>@NIFTY</td><td>EARTHLINK</td><td>QWEST</td></tr><tr><td>AIRTEL</td><td>EASYPNET</td><td>RCN</td></tr><tr><td>ALPHA_INTERNET</td><td>EITC</td><td>REDIRIS</td></tr><tr><td>ALTITUDE_TELECOM</td><td>ETISALAT</td><td>RENATER</td></tr><tr><td>AOL</td><td>EUROCIBER</td><td>RESERVED</td></tr><tr><td>ARNET</td><td>FASTWEB</td><td>RETEVISION</td></tr><tr><td>ASAHI</td><td>FIBERTEL</td><td>ROAD_RUNNER</td></tr><tr><td>ATT</td><td>FRANCE_TELECOM</td><td>ROGERS</td></tr><tr><td>AWS</td><td>FREE</td><td>SASKTEL</td></tr><tr><td>BELLALIAN</td><td>FREECOM</td><td>SEEDNET</td></tr><tr><td>BELL_CANADA</td><td>FRONTIER</td><td>SEIKYO_INTERNET</td></tr><tr><td>BIGLOBE</td><td>GOOGLECLOUD</td><td>SFR</td></tr><tr><td>BITMAILER</td><td>H3G</td><td>SHAW</td></tr><tr><td>BOUYGUES</td><td>HINET</td><td>SOFTLAYER</td></tr><tr><td>BRIGHT_HOUSE</td><td>IBM</td><td>SO_NET</td></tr><tr><td>BSKYB</td><td>IDECNET</td><td>SPRINT</td></tr><tr><td>BT</td><td>IJ4U</td><td>SUDDENLINK</td></tr><tr><td>CABLEONE</td><td>INFOSPHERE</td><td>TALKTALK</td></tr><tr><td>CABLEVISION</td><td>JANET</td><td>TEKSAVY</td></tr><tr><td>CERNET</td><td>JAZZTELL</td><td>TELEFONICA</td></tr><tr><td>CHARTER</td><td>JUSTNET</td><td>TELSTRA</td></tr><tr><td>CHINANET</td><td>LIVEDOOR</td><td>TERRA_MEXICO</td></tr><tr><td>CHINA_MOBILE</td><td>MCI</td><td>TI</td></tr><tr><td>CHINA_UNICOM</td><td>MEDIACOM</td><td>TIKITIKI</td></tr><tr><td>CLEARWIRE</td><td>MEDIA_ONE</td><td>TIME_WARNER</td></tr><tr><td>COGECO</td><td>MICROSOFT</td><td>TISCALI</td></tr><tr><td>COLOCROSSING</td><td>MIL</td><td>TURK_TELEKOM</td></tr><tr><td>COLT</td><td>NERIM</td><td>T_MOBILE</td></tr><tr><td>COMCAST</td><td>NEWNET</td><td>UNI2</td></tr><tr><td>COMPLETEL</td><td>NUMERICABLE</td><td>UNINET</td></tr><tr><td>COMPUSERVE</td><td>OCN</td><td>UPC</td></tr><tr><td>COVAD</td><td>ODN</td><td>USEMB</td></tr><tr><td>DION</td><td>ONO</td><td>UUNET</td></tr><tr><td>DIRECTV</td><td>PANASONIC_HI_HO</td><td>VERIZON</td></tr><tr><td>DREAMNET</td><td>PLALA</td><td>VIRGIN_MEDIA</td></tr><tr><td>DTAG</td><td>PLUSNET</td><td>VODAFONE</td></tr><tr><td>DTI</td><td>PRODIGY</td><td>WAKWAK</td></tr></tbody></table></div>	@NIFTY	EARTHLINK	QWEST	AIRTEL	EASYPNET	RCN	ALPHA_INTERNET	EITC	REDIRIS	ALTITUDE_TELECOM	ETISALAT	RENATER	AOL	EUROCIBER	RESERVED	ARNET	FASTWEB	RETEVISION	ASAHI	FIBERTEL	ROAD_RUNNER	ATT	FRANCE_TELECOM	ROGERS	AWS	FREE	SASKTEL	BELLALIAN	FREECOM	SEEDNET	BELL_CANADA	FRONTIER	SEIKYO_INTERNET	BIGLOBE	GOOGLECLOUD	SFR	BITMAILER	H3G	SHAW	BOUYGUES	HINET	SOFTLAYER	BRIGHT_HOUSE	IBM	SO_NET	BSKYB	IDECNET	SPRINT	BT	IJ4U	SUDDENLINK	CABLEONE	INFOSPHERE	TALKTALK	CABLEVISION	JANET	TEKSAVY	CERNET	JAZZTELL	TELEFONICA	CHARTER	JUSTNET	TELSTRA	CHINANET	LIVEDOOR	TERRA_MEXICO	CHINA_MOBILE	MCI	TI	CHINA_UNICOM	MEDIACOM	TIKITIKI	CLEARWIRE	MEDIA_ONE	TIME_WARNER	COGECO	MICROSOFT	TISCALI	COLOCROSSING	MIL	TURK_TELEKOM	COLT	NERIM	T_MOBILE	COMCAST	NEWNET	UNI2	COMPLETEL	NUMERICABLE	UNINET	COMPUSERVE	OCN	UPC	COVAD	ODN	USEMB	DION	ONO	UUNET	DIRECTV	PANASONIC_HI_HO	VERIZON	DREAMNET	PLALA	VIRGIN_MEDIA	DTAG	PLUSNET	VODAFONE	DTI	PRODIGY	WAKWAK	
@NIFTY	EARTHLINK	QWEST																																																																																																																
AIRTEL	EASYPNET	RCN																																																																																																																
ALPHA_INTERNET	EITC	REDIRIS																																																																																																																
ALTITUDE_TELECOM	ETISALAT	RENATER																																																																																																																
AOL	EUROCIBER	RESERVED																																																																																																																
ARNET	FASTWEB	RETEVISION																																																																																																																
ASAHI	FIBERTEL	ROAD_RUNNER																																																																																																																
ATT	FRANCE_TELECOM	ROGERS																																																																																																																
AWS	FREE	SASKTEL																																																																																																																
BELLALIAN	FREECOM	SEEDNET																																																																																																																
BELL_CANADA	FRONTIER	SEIKYO_INTERNET																																																																																																																
BIGLOBE	GOOGLECLOUD	SFR																																																																																																																
BITMAILER	H3G	SHAW																																																																																																																
BOUYGUES	HINET	SOFTLAYER																																																																																																																
BRIGHT_HOUSE	IBM	SO_NET																																																																																																																
BSKYB	IDECNET	SPRINT																																																																																																																
BT	IJ4U	SUDDENLINK																																																																																																																
CABLEONE	INFOSPHERE	TALKTALK																																																																																																																
CABLEVISION	JANET	TEKSAVY																																																																																																																
CERNET	JAZZTELL	TELEFONICA																																																																																																																
CHARTER	JUSTNET	TELSTRA																																																																																																																
CHINANET	LIVEDOOR	TERRA_MEXICO																																																																																																																
CHINA_MOBILE	MCI	TI																																																																																																																
CHINA_UNICOM	MEDIACOM	TIKITIKI																																																																																																																
CLEARWIRE	MEDIA_ONE	TIME_WARNER																																																																																																																
COGECO	MICROSOFT	TISCALI																																																																																																																
COLOCROSSING	MIL	TURK_TELEKOM																																																																																																																
COLT	NERIM	T_MOBILE																																																																																																																
COMCAST	NEWNET	UNI2																																																																																																																
COMPLETEL	NUMERICABLE	UNINET																																																																																																																
COMPUSERVE	OCN	UPC																																																																																																																
COVAD	ODN	USEMB																																																																																																																
DION	ONO	UUNET																																																																																																																
DIRECTV	PANASONIC_HI_HO	VERIZON																																																																																																																
DREAMNET	PLALA	VIRGIN_MEDIA																																																																																																																
DTAG	PLUSNET	VODAFONE																																																																																																																
DTI	PRODIGY	WAKWAK																																																																																																																
bandwidth Values	string array	Bandwidth range in bits per second, either 1 , 57 , 257 , 1000 , 2000 , or 5000 .	field is BANDWIDTH																																																																																																															
checkIps	enum	Specifies which IP addresses determine the user's network.																																																																																																																
	BOTH	Behaves like HEADERS , but also considers the connecting client's IP address.																																																																																																																
	CONNECTING	Considers the connecting client's IP address.																																																																																																																
	HEADERS	Considers IP addresses specified in the X-Forwarded-For header, succeeding if any of them match.																																																																																																																
useOnlyFirstXForwardedForIp	boolean	When connecting via a proxy server as determined by the X-Forwarded-For header, enabling this option matches the end client specified in the header. Disabling it matches the connecting client's IP address.	checkIps is either: BOTH , HEADERS																																																																																																															

variableError

- **Property Manager name:** [Variable Error](#)
- **Criteria version:** The v2018-02-27 rule format supports the variableError criteria v1.1.
- **Rule format status:** [Deprecated, outdated rule format](#)
- **Access:** [Read-write](#)

Matches any runtime errors that occur on edge servers based on the configuration of a [setVariable](#) behavior. See [Support for variables](#) section for more information on this feature.

Option	Type	Description
result	boolean	Matches errors for the specified set of <code>variableNames</code> , otherwise matches errors from variables outside that set.
variableNames	string array	The name of the variable whose error triggers the match, or a space- or comma-delimited list of more than one variable name. Note that if you define a variable named <code>VAR</code> , the name in this field needs to appear with its added prefix as <code>PMUSER_VAR</code> . When such a variable is inserted into other fields, it appears with an additional namespace as <code>{{user.PMUSER_VAR}}</code> . See the setVariable behavior for details on variable names.

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.

© 2023 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 January 4, 2023