akamai
techdocs

v2023-05-30 Property Manager Deprecated Rule Formats

November 6, 2023

Contents

Welcome

PAPI conventions

v2023-05-30 behaviors

cacheTagVisible

caching

centralAuthorization

chaseRedirects

clientCharacteristics

cloudInterconnects

cloudWrapper

cloudWrapperAdvanced

commonMediaClientData

constructResponse

contentCharacteristics

contentCharacteristicsAMD

contentCharacteristicsDD

contentCharacteristicsWsdLargeFile

contentCharacteristicsWsdLive

contentCharacteristicsWsdVod

contentTargetingProtection

corsSupport

cpCode

customBehavior

datastream

dcp

dcpAuthHMACTransformation

dcpAuthRegexTransformation

dcpAuthSubstringTransformation

dcpAuthVariableExtractor

dcpDefaultAuthzGroups

dcpDevRelations

deliveryReceipt

denyAccess

denyDirectFailoverAccess

deviceCharacteristicCacheId

deviceCharacteristicHeader

dnsAsyncRefresh

dnsPrefresh

downgradeProtocol

downloadCompleteMarker

downloadNotification

downstreamCache

dynamicThroughtputOptimization

dynamicThroughtputOptimizationOverride

dynamicWebContent

ecmsBulkUpload

ecmsDatabase

ecmsDataset

ecmsObjectKey

edgeConnect

edgeLoadBalancingAdvanced

edgeLoadBalancingDataCenter

edgeLoadBalancingOrigin

edgeOriginAuthorization

edgeRedirector

edgeScape

edgeSideIncludes

edgeWorker

enhancedAkamaiProtocol

enhancedProxyDetection

epdForwardHeaderEnrichment

failAction

failoverBotManagerFeatureCompatibility

fastInvalidate

firstPartyMarketing

firstPartyMarketingPlus

forwardRewrite

g2oheader

globalRequestNumber

graphqlCaching

gzipResponse

hdDataAdvanced

healthDetection

hsafEipBinding

http2

http3

httpStrictTransportSecurity

httpToHttpsUpgrade

inputValidation

imOverride

imageManager

imageManagerVideo

include

instant

instantConfig

largeFileOptimization

largeFileOptimizationAdvanced

limitBitRate

logCustom

mPulse

manifestPersonalization

manifestRerouting

manualServerPush

mediaAcceleration

mediaAccelerationQuicOptout

mediaClient

mediaFileRetrievalOptimization

mediaOriginFailover

metadataCaching

mobileSdkPerformance

modifyIncomingRequestHeader

modifyIncomingResponseHeader

modifyOutgoingRequestHeader

modifyOutgoingResponseHeader

modifyViaHeader

origin

originCharacteristics

originCharacteristicsWsd

originFailureRecoveryMethod

originFailureRecoveryPolicy

originIpAcl

persistentClientConnection

persistentConnection

personallyIdentifiableInformation

phasedRelease

preconnect

predictiveContentDelivery

predictivePrefetching

prefetch

prefetchable

prefreshCache

quicBeta

randomSeek

rapid

readTimeout

realTimeReporting

realUserMonitoring

redirect

redirectplus

refererChecking

removeQueryParameter

removeVary

report

requestControl

requestTypeMarker

resourceOptimizer

resourceOptimizerExtendedCompatibility

responseCode

responseCookie

restrictObjectCaching

returnCacheStatus

rewriteUrl

rumCustom

saasDefinitions

salesForceCommerceCloudClient

salesForceCommerceCloudProvider

salesForceCommerceCloudProviderHostHeade

r savePostDcaProcessing

scheduleInvalidation

shutr

scriptManagement

segmentedContentProtection

segmentedMediaOptimization

segmentedMediaStreamingPrefetch

setVariable

v2023-05-30 criteria

Notice

Welcome

Welcome

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

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

This guide provides details for all behaviors and criteria the Property Manager API supports in the v2022-05-30 **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.

PAPI conventions

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.

v2023-05-30 behaviors

v2023-05-30 behaviors

This section provides details for all behaviors the Property Manager API supports for the `v2023-05-30` 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 `v2023-05-30` 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 `v2023-05-30` rule format supports the `adScalerCircuitBreaker` behavior v1.2.
- **Rule format status**: [Deprecated, outdated rule format](#)
- **Access**: [Read-write](#)
- **Allowed in includes**: [No (temporarily)](#)

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
responseDelay Based	boolean	Triggers a fallback action based on the delayed response from the technology partner's server.	
responseDelay Threshold	enum	Specifies the maximum response delay that, if exceeded, triggers the fallback action.	`responseDelayBased` is `true`
		Supported values: 500ms	
responseCode Based	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.	`responseCodeBased` is `true`
fallbackAction ResponseCode Based	enum	Specifies the fallback action.	`responseDelayBased` is `true` OR `responseCodeBased` 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 ResponseCode Based	enum	Specifies the error to include in the response to the client.	`fallbackActionResponse CodeBased` is `RETURN_ ERROR`
	`SAME_ AS_ RECEIVED`	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 OwnResponse CodeBased	string	Defines a custom error response.	`returnErrorResponseCode Based` is `SPECIFY_YOUR_ OWN`

adaptiveAcceleration

- **Property Manager name**: [Adaptive Acceleration](#)

- **Behavior version**: The `v2023-05-30` rule format supports the `adaptiveAcceleration` behavior v2.1.
- **Rule format status**: Deprecated, outdated rule format
- **Access**: Read-write
- **Allowed in includes**: No (temporarily)

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

Option	Type	Description	Requires
source	string	The source Adaptive Acceleration uses to gather the real user monitoring timing data, either `mPulse` or `realUserMonitoring`. The recommended `mPulse` option supports all optimizations and requires the `mPulse` behavior added by default to new Ion properties. The classic `realUserMonitoring` method has been deprecated. If you set it as the data source, make sure you use it with the `realUserMonitoring` behavior.	
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.	
enable Preconnect	boolean	Allows browsers to anticipate what connections your site needs, and establishes those connections ahead of time. See Automatic Preconnect for more information.	
preload Enable	boolean	Allows browsers to preload necessary fonts before they fetch and process other resources. See Automatic Font Preload for more information.	
abLogic	enum	Specifies whether to use Adaptive Acceleration in an A/B testing environment. To include Adaptive Acceleration data in your A/B testing, specify the mode you want to apply. Otherwise, `DISABLED` by default. See Add A/B testing to A2 for details.	
	DISABLED	Disables the use of Adaptive Acceleration in the A/B testing environment. This is the default value.	
	CLOUDLETS	Applies A/B testing using Cloudlets.	
	MANUAL	Applies A/B testing by redirecting a request to one of two origin servers, based on the cookie included with the request.	
cookieName	string	This specifies the name of the cookie file used for redirecting the requests in the A/B testing environment.	`abLogic` is MANUAL
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. See the `resourceOptimizer` and `resourceOptimizerExtendedCompatibility` behaviors for more details.	
enableBrotli Compression	boolean	Applies Brotli compression, converting your origin content to cache on edge servers.	
enableFor Noncacheable	boolean	Applies Brotli compression to non-cacheable content.	`enableBrotli Compression` is `true`

adaptiveImageCompression

- **Property Manager name**: Adaptive Image Compression
- **Behavior version**: The `v2023-05-30` rule format supports the `adaptiveImageCompression` behavior v1.2.
- **Rule format status**: Deprecated, outdated rule format
- **Access**: Read-write
- **Allowed in includes**: Yes

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

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

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

Option	Type	Description	Requires
compressMobile	boolean	Adapts images served over cellular mobile networks.	
tier1MobileCompressionMethod	enum	Specifies tier-1 behavior.	`compressMobile` is `true`
		Supported values: BYPASS	
tier1MobileCompressionValue	number (0-100)	Specifies the compression percentage.	`tier1MobileCompressionMethod` is `COMPRESS`
tier2MobileCompressionMethod	enum	Specifies tier-2 cellular-network behavior.	`compressMobile` is `true`
		Supported values: BYPASS	
tier2MobileCompressionValue	number (0-100)	Specifies the compression percentage.	`tier2MobileCompressionMethod` is `COMPRESS`
tier3MobileCompressionMethod	enum	Specifies tier-3 cellular-network behavior.	`compressMobile` is `true`
		Supported values: BYPASS	
tier3MobileCompressionValue	number (0-100)	Specifies the compression percentage.	`tier3MobileCompressionMethod` is `COMPRESS`
compressStandard	boolean	Adapts images served over non-cellular networks.	
tier1StandardCompressionMethod	enum	Specifies tier-1 non-cellular network behavior.	`compressStandard` is `true`
		Supported values: BYPASS	

Option	Type	Description	Requires
tier1StandardCompression Value	number (0-100)	Specifies the compression percentage.	tier1StandardCompressionMethod is COMPRESS
tier2StandardCompression Method	enum	Specifies tier-2 non-cellular network behavior.	compressStandard is true
		Supported values: BYPASS	
tier2StandardCompression Value	number (0-100)	Specifies the compression percentage.	tier2StandardCompressionMethod is COMPRESS
tier3StandardCompression Method	enum	Specifies tier-3 non-cellular network behavior.	compressStandard is true
		Supported values: BYPASS	
tier3StandardCompression Value	number (0-100)	Specifies the compression percentage.	tier3StandardCompressionMethod is COMPRESS

advanced

- **Property Manager name**: Advanced
- **Behavior version**: The `v2023-05-30` rule format supports the `advanced` behavior v1.0.
- **Rule format status**: Deprecated, outdated rule format
- **Access**: Read-only
- **Allowed in includes**: No (temporarily)

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 `v2023-05-30` rule format supports the `aggregatedReporting` behavior v1.2.
- **Rule format status**: Deprecated, outdated rule format
- **Access**: Read-write
- **Allowed in includes**: No (temporarily)

Configure a custom report that collects traffic data. The data is based on one to four variables, such as `sum`, `average`, `min`, and `max`. These aggregation attributes help compile traffic data summaries.

This behavior is part of Internet of Things OTA Update, which allows users to securely download firmware to vehicle head units over cellular networks. Use this system to create statistical reports by defining PAPI variables, such as sum of requests sent by a specific car model. For example, you can send the sum of data in bytes, number of requests, and number of completed downloads based on the selected car model, campaign, and year.

To configure the behavior, see Configure the aggregated reporting behavior in the IoT OTA Updates documentation. For more information including accessing the report, see Aggregated Reporting. Also, you can configure variables with the `setVariable`, `requestTypeMarker`, and `downloadCompleteMarker` behaviors. To learn more about the combinations of OTA Updates behaviors, see Behaviors in reports.

Akamai also offers the `report` behavior to specify the HTTP request headers or cookies to include in your Log Delivery Service⬧ reports.

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)	The number of attributes to include in the report, ranging from 1 to 4.	
attribute1	string (allows variables)	Specify a previously user-defined variable name as a report attribute. The values extracted for all attributes range from 0 to 20 characters.	
attribute2	string (allows variables)	Specify a previously user-defined variable name as a report attribute. The values extracted for all attributes range from 0 to 20 characters.	attributes Count ≥ 2
attribute3	string (allows variables)	Specify a previously user-defined variable name as a report attribute. The values extracted for all attributes range from 0 to 20 characters.	attributes Count ≥ 3
attribute4	string (allows variables)	Specify a previously user-defined variable name as a report attribute. The values extracted for all attributes range from 0 to 20 characters.	attributes Count is 4

akamaizer

- **Property Manager name**: Akamaizer
- **Behavior version**: The `v2023-05-30` rule format supports the `akamaizer` behavior v1.1.
- **Rule format status**: Deprecated, outdated rule format

- **Access**: [Read-only](#)
- **Allowed in includes**: [Yes](#)

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 `akamaizer Tag` behavior.

Option	Type	Description
enabled	boolean	Enables the Akamaizer behavior.

akamaizerTag

- **Property Manager name**: [Akamaize Tag](#)
- **Behavior version**: The `v2023-05-30` rule format supports the `akamaizerTag` behavior v1.1.
- **Rule format status**: [Deprecated, outdated rule format](#)
- **Access**: [Read-only](#)
- **Allowed in includes**: [Yes](#)

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

Option	Type	Description	Requires
match Hostname	string	Specifies the hostname to match on as a Perl-compatible regular expression.	
replacement Hostname	string	Specifies the replacement hostname for the tag to use.	
scope	enum	Specifies the part of HTML content the `tagsAttribute` refers to.	
	ATTRIBUTE	When `tagsAttribute` refers to a tag/attribute pair, the match only applies to the attribute.	
	URL_ ATTRIBUTE	The same as an attribute but applies when the attribute value is a URL. In that case, it converts to an absolute URL prior to substitution.	
	BLOCK	Substitutes within the tag's contents, but not within any nested tags.	
	PAGE	Ignores the `tagsAttribute` field and performs the substitution on the entire page.	
tagsAttribute	enum	Specifies the tag or tag/attribute combination to operate on.	`scope` is not `PAGE`
		Supported values: A BASE IFRAME LINK AREA BASE_HREF IFRAME_SRC LINK_HREF AREA_HREF FORM IMG SCRIPT A_HREF FORM_ACTION IMG_SRC SCRIPT_SRC	
replaceAll	boolean	Replaces all matches when enabled, otherwise replaces only the first match.	

Option	Type	Description	Requires
includeTags Attribute	boolean	Whether to include the `tagsAttribute` value.	

allHttpInCacheHierarchy

- **Property Manager name**: [Allow All Methods on Parent Servers](#)
- **Behavior version**: The `v2023-05-30` rule format supports the `allHttpInCacheHierarchy` behavior v1.1.
- **Rule format status**: [Deprecated, outdated rule format](#)
- **Access**: [Read-write](#)
- **Allowed in includes**: [Yes](#)

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 `v2023-05-30` rule format supports the `allowCloudletsOrigins` behavior v1.4.
- **Rule format status**: [Deprecated, outdated rule format](#)
- **Access**: [Read-write](#)
- **Allowed in includes**: [No (temporarily)](#)

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

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

allowDelete

- **Property Manager name**: [Allow DELETE](#)
- **Behavior version**: The `v2023-05-30` rule format supports the `allowDelete` behavior v1.4.
- **Rule format status**: [Deprecated, outdated rule format](#)
- **Access**: [Read-write](#)
- **Allowed in includes**: [Yes](#)

Allow HTTP requests using the DELETE method. By default, GET, HEAD, and OPTIONS requests are allowed, and all other methods result in a 501 error. Such content does not cache, and any DELETE requests pass to the origin. See also the `allowOptions` , `allowPatch` , `allowPost` , and `allowPut` behaviors.

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

allowHTTPSCacheKeySharing

- **Property Manager name**: [HTTPS Cache Key Sharing](#)
- **Behavior version**: The `v2023-05-30` rule format supports the `allowHTTPSCacheKeySharing` behavior v1.0.
- **Rule format status**: [Deprecated, outdated rule format](#)
- **Access**: [Read-write](#)
- **Allowed in includes**: [Yes](#)

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

Option	Type	Description
enabled	boolean	Enables HTTPS cache key sharing.

allowHTTPSDowngrade

- **Property Manager name**: [Protocol Downgrade (HTTPS Downgrade to Origin)](#)
- **Behavior version**: The `v2023-05-30` rule format supports the `allowHTTPSDowngrade` behavior v1.0.
- **Rule format status**: [Deprecated, outdated rule format](#)
- **Access**: [Read-write](#)
- **Allowed in includes**: [Yes](#)

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 `v2023-05-30` rule format supports the `allowOptions` behavior v1.1.
- **Rule format status**: [Deprecated, outdated rule format](#)
- **Access**: [Read-write](#)
- **Allowed in includes**: [Yes](#)

GET, HEAD, and OPTIONS requests are allowed by default. All other HTTP methods result in a 501 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 `construct Response` behavior to send responses directly from the Akamai network. See also the `allowDelete` , `allowPatch` , `allow Post` , and `allowPut` behaviors.

Option	Type	Description
enabled	boolean	Set this to true to reflect the default policy where edge servers allow the OPTIONS method, without caching the response. Set this to false to deny OPTIONS requests and respond with a 501 error.

allowPatch

- **Property Manager name**: Allow PATCH
- **Behavior version**: The v2023-05-30 rule format supports the allowPatch behavior v1.2.
- **Rule format status**: Deprecated, outdated rule format
- **Access**: Read-write
- **Allowed in includes**: Yes

Allow HTTP requests using the PATCH method. By default, GET, HEAD, and OPTIONS requests are allowed, and all other methods result in a 501 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 *not* cache.

allowPost

- **Property Manager name**: Allow POST
- **Behavior version**: The v2023-05-30 rule format supports the allowPost behavior v1.3.
- **Rule format status**: Deprecated, outdated rule format
- **Access**: Read-write
- **Allowed in includes**: Yes

Allow HTTP requests using the POST method. By default, GET, HEAD, and OPTIONS requests are allowed, and POST requests are denied with 403 error. All other methods result in a 501 error. See also the allowDelete , allowOptions , allowPatch , and allowPut behaviors.

Option	Type	Description
enabled	boolean	Allows POST requests.

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

allowPut

- **Property Manager name**: Allow PUT
- **Behavior version**: The `v2023-05-30` rule format supports the `allowPut` behavior v1.2.
- **Rule format status**: Deprecated, outdated rule format
- **Access**: Read-write
- **Allowed in includes**: Yes

Allow HTTP requests using the PUT method. By default, GET, HEAD, and OPTIONS requests are allowed, and all other methods result in a 501 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 *not* cache.

allowTransferEncoding

- **Property Manager name**: Chunked Transfer Encoding
- **Behavior version**: The `v2023-05-30` rule format supports the `allowTransferEncoding` behavior v1.0.
- **Rule format status**: Deprecated, outdated rule format
- **Access**: Read-write
- **Allowed in includes**: Yes

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

Option	Type	Description
enabled	boolean	Allows Chunked Transfer Encoding requests.

altSvcHeader

- **Property Manager name**: Alt-Svc Header ⇱
- **Behavior version**: The `v2023-05-30` rule format supports the `altSvcHeader` behavior v1.0.
- **Rule format status**: Deprecated, outdated rule format
- **Access**: Read-write
- **Allowed in includes**: Yes

Sets the maximum age value for the Alternative Services (`Alt-Svc`) header.

Option	Type	Description
max Age	number	Specifies the `max-age` value in seconds for the `Alt-Svc` header. The default `max-age` for an `Alt-Svc` header is 93600 seconds (26 hours).

apiPrioritization

- **Property Manager name**: API Prioritization Cloudlet
- **Behavior version**: The `v2023-05-30` rule format supports the `apiPrioritization` behavior v3.0.
- **Rule format status**: Deprecated, outdated rule format
- **Access**: Read-write
- **Allowed in includes**: Yes

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.	

Option	Type	Description	Requires
isSharedPolicy	boolean	Whether you want to apply the Cloudlet shared policy to an unlimited number of properties within your account. Learn more about shared policies and how to create them in Cloudlets Policy Manager.	
cloudletPolicy	object	Identifies the Cloudlet policy.	isShared Policy is false
cloudletPolicy.id	number	Identifies the Cloudlet.	
cloudlet Policy.name	string	The Cloudlet's descriptive name.	
cloudletShared Policy	string	Identifies the Cloudlet shared policy to use with this behavior. Use the Cloudlets API to list available shared policies.	isShared Policy is true
label	string	A label to distinguish this API Prioritization policy from any others in the same property.	
useThrottledCp Code	boolean	Specifies whether to apply an alternative CP code for requests served the alternate response.	
throttledCpCode	object	Specifies the CP code as an object. You only need to provide the initial `id`, stripping any `cpc_` `prefix` to pass the integer to the rule tree. Additional CP code details may reflect back in subsequent read-only data.	use ThrottledCp Code is true
throttledCp Code.cpCode Limits	array	**Read-only**. Describes the current usage limit for the CP code.	
throttledCp Code.created Date	integer	**Read-only**. UNIX epoch timestamp reflecting when the CP code was originally created.	
throttledCp Code.description	string	**Read-only**. Additional description for the CP code.	
throttledCp Code.id	integer	Unique identifier for each CP code. Initially, you get this value when creating a new CP code in PAPI. You can also assign a `cpcodeId` value from the List CP codes operation.	
throttledCp Code.name	string	**Read-only**. The name of the CP code you specify as the `cpcodeName` when creating a new CP code in PAPI. You can modify this value with the PUT operation in the CP codes and Reporting Groups API.	
throttledCp Code.products	array	**Read-only**. The set of products the CP code is assigned to. This reflects `productId` values you specify when creating a new CP code in PAPI.	
useThrottled StatusCode	boolean	Allows you to assign a specific HTTP response code to a throttled request.	
throttledStatus Code	number	Specifies the HTTP response code for requests that receive the alternate response.	use Throttled StatusCode is true
netStorage	object	Specify the NetStorage domain that contains the alternate response.	
netStorage.cp Code	integer	Identifies a CP code assigned to this storage group.	
net Storage.download DomainName	string	Domain name from which content can be downloaded.	
netStorage.g2o Token	string	Signature Header Authentication key.	
netStorage.id	integer	Unique identifier for the storage group.	
net Storage.name	string	Name of the storage group.	

Option	Type	Description	Requires
netStoragePath	string	Specify the full NetStorage path for the alternate response, including trailing file name.	
alternate ResponseCache Ttl	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 `v2023-05-30` rule format supports the `applicationLoadBalancer` behavior v1.10.
- **Rule format status**: [Deprecated, outdated rule format](#)
- **Access**: [Read-write](#)
- **Allowed in includes**: [No (temporarily)](#)

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.	
cloudlet Policy.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.	
stickinessCookie Type	enum	Determines how a cookie persistently associates the client with a load-balanced origin.	
	`NONE`	Dynamically reassigns different load-balanced origins for each request.	
	`NEVER`	Preserves the cookie indefinitely.	
	`ON_BROWSER_ CLOSE`	Limit the cookie duration to browser sessions.	
	`FIXED_DATE`	Specify a specific time for when the cookie expires.	
	`DURATION`	Specify a delay for when the cookie expires.	
	`ORIGIN_SESSION`	Limit the cookie duration to when the `ORIGIN_SESSION` terminates. (After the cookie expires, the cookie type re-evaluates.)	
stickiness ExpirationDate	string (epoch timestamp)	Specifies when the cookie expires.	stickinessCookieType is `FIXED_ DATE`
stickiness Duration	string (duration)	Sets how long it is before the cookie expires.	stickinessCookieType is `DURATION`

Option	Type	Description	Requires
stickiness Refresh	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`
originCookie Name	string	Specifies the name for your session cookie.	`stickinessCookieType` is `ORIGIN_SESSION`
specifyStickiness CookieDomain	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`, `ORIGIN_SESSION`
stickinessCookie Domain	string	Specifies the domain to track the stickiness cookie.	`specifyStickinessCookieDomain` is `true`
stickinessCookie AutomaticSalt	boolean	Sets whether to assign a *salt* value automatically to the cookie to prevent manipulation by the user. You should not enable this if sharing the population cookie across more than one property.	`stickinessCookieType` is either: `ON_BROWSER_CLOSE`, `FIXED_DATE`, `DURATION`, `NEVER`, `ORIGIN_SESSION`
stickinessCookie Salt	string	Specifies the stickiness cookie's salt value. Use this option to share the cookie across many properties.	`stickinessCookieAutomaticSalt` is `false`
stickinessCookie SetHttpOnlyFlag	boolean	Ensures the cookie is transmitted only over HTTP.	`stickinessCookieType` is either: `ON_BROWSER_CLOSE`, `FIXED_DATE`, `DURATION`, `NEVER`, `ORIGIN_SESSION`
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.	

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

audienceSegmentation

- **Property Manager name**: Audience Segmentation Cloudlet
- **Behavior version**: The `v2023-05-30` rule format supports the `audienceSegmentation` behavior v3.0.
- **Rule format status**: Deprecated, outdated rule format
- **Access**: Read-write
- **Allowed in includes**: No (temporarily)

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.	
isShared Policy	boolean	Whether you want to use a shared policy for a Cloudlet. Learn more about shared policies and how to create them in Cloudlets Policy Manager.	
cloudlet Policy	object	Identifies the Cloudlet policy.	`isSharedPolicy` is false
cloudlet Policy.id	number	Identifies the Cloudlet.	
cloudlet Policy.name	string	The Cloudlet's descriptive name.	
cloudlet SharedPolicy	string	This identifies the Cloudlet shared policy to use with this behavior. You can list available shared policies with the Cloudlets API.	`isSharedPolicy` is true
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.	

Option	Type	Description	Requires
		Supported values: IN_COOKIE_HEADER	
segment TrackingQuery Param	string	This query parameter specifies the name of the segmentation rule.	segmentTracking Method is IN_ QUERY_PARAM
segment TrackingCookie Name	string	This cookie name specifies the name of the segmentation rule.	segmentTracking Method is IN_ COOKIE_HEADER
segment Tracking Custom Header	string	This custom HTTP header specifies the name of the segmentation rule.	segmentTracking Method is IN_ CUSTOM_HEADER
population CookieType	enum	Specifies when the segmentation cookie expires.	
	NEVER	Never expire.	
	ON_ BROWSER_ CLOSE	Expire at end of browser session.	
	DURATION	Specify a delay.	
population Duration	string (duration)	Specifies the lifetime of the segmentation cookie.	populationCookie Type is DURATION
population Refresh	boolean	If disabled, sets the expiration time only if the cookie is not yet present in the request.	populationCookie Type 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.	specifyPopulation CookieDomain is true
population Cookie AutomaticSalt	boolean	Whether to assign a *salt* 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.	populationCookie AutomaticSalt is false
population CookieInclude RuleName	boolean	When enabled, includes in the session cookie the name of the rule in which this behavior appears.	

autoDomainValidation

- **Property Manager name**: Auto Domain Validation

- **Behavior version**: The `v2023-05-30` rule format supports the `autoDomainValidation` behavior v1.0.
- **Rule format status**: Deprecated, outdated rule format
- **Access**: Read-write
- **Allowed in includes**: Yes

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

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

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

baseDirectory

- **Property Manager name**: Origin Base Path
- **Behavior version**: The `v2023-05-30` rule format supports the `baseDirectory` behavior v1.1.
- **Rule format status**: Deprecated, outdated rule format
- **Access**: Read-write
- **Allowed in includes**: Yes

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:

- Changing the origin's base path also changes the cache key, which makes any existing cached data inaccessible. This causes a spike in traffic to your origin until the cache repopulates with fresh content.
- You can't override the base path with other behaviors. For example, if in the `rewriteUrl` behavior you specify `targetPath` to `/gifs/hello.gif`, this gets appended to the base path: `example.com/images/gifs/hello.gif`.

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 `v2023-05-30` rule format supports the `bossBeaconing` behavior v1.0.
- **Rule format status**: [Deprecated, outdated rule format](#)
- **Access**: [Read-only](#)
- **Allowed in includes**: [Yes](#)

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.
request Type	enum	Specify when to trigger a beacon.
	EDGE	For edge requests only.
	EDGE_ MIDGRESS	Both end and midgress requests.
forward Type	enum	Specify when to trigger a beacon.
	MIDGRESS	For internal midgress forwards only.
	ORIGIN	For origin forwards only.
	MIDGRESS_ ORIGIN	Both.
sampling Frequency	enum	Specifies a sampling frequency or disables beacons.
	SAMPLING_ FREQ_0_0	Disables beacons altogether.
	SAMPLING_ FREQ_0_1	Specifies a sampling frequency.
conditional Sampling Frequency	enum	Specifies a conditional sampling frequency or disables beacons.
	CONDITIONAL_ SAMPLING_ FREQ_0_0	Disables beacons altogether.
	CONDITIONAL_ SAMPLING_ FREQ_0_1	Specifies a sampling frequency.
	CONDITIONAL_ SAMPLING_ FREQ_0_2	Specifies a sampling frequency.
	CONDITIONAL_ SAMPLING_ FREQ_0_3	Specifies a sampling frequency.
conditional HTTPStatus	string array	Specifies the set of response status codes or ranges that trigger the beacon.

Option	Type	Description
		Supported values:

		0xx	302	304	3xx	401	403	404	408	4xx

Option	Type	Description
conditional Error Pattern	string	A space-separated set of error patterns that trigger beacons to conditional feeds. Each pattern can include wildcards, where `?` matches a single character and `*` matches zero or more characters. For example, `*CONNECT* *DENIED*` matches two different words as substrings.

breadcrumbs

- **Property Manager name**: Breadcrumbs
- **Behavior version**: The `v2023-05-30` rule format supports the `breadcrumbs` behavior v1.1.
- **Rule format status**: Deprecated, outdated rule format
- **Access**: Read-write
- **Allowed in includes**: Yes

Provides per-HTTP transaction visibility into a request for content, regardless of how deep the request goes into the Akamai platform. The `Akamai-Request-BC` response header includes various data, such as network health and the location in the Akamai network used to serve content, which simplifies log review for troubleshooting.

Option	Type	Description
enabled	boolean	Enables the Breadcrumbs feature.
opt Mode	boolean	Specifies whether to include Breadcrumbs data in the response header. To bypass the current `optMode`, append the opposite `ak-bc` query string to each request from your player.
logging Enabled	boolean	Whether to collect all Breadcrumbs data in logs, including the response headers sent a requesting client. This can also be helpful if you're using DataStream 2 to retrieve log data. This way, all Breadcrumbs data is carried in the logs it uses.

breakConnection

- **Property Manager name**: Break Forward Connection
- **Behavior version**: The `v2023-05-30` rule format supports the `breakConnection` behavior v1.1.
- **Rule format status**: Deprecated, outdated rule format
- **Access**: Read-write
- **Allowed in includes**: Yes

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

Option	Type	Description
enabled	boolean	Enables the break connection behavior.

brotli

- **Property Manager name**: Brotli Support
- **Behavior version**: The `v2023-05-30` rule format supports the `brotli` behavior v1.1.
- **Rule format status**: Deprecated, outdated rule format
- **Access**: Read-write
- **Allowed in includes**: Yes

Accesses Brotli-compressed assets from your origin and caches them on edge servers. This doesn't compress resources within the content delivery network in real time. You need to set up Brotli compression separately on your origin. If a requesting client doesn't support Brotli, edge servers deliver non-Brotli resources.

Option	Type	Description
enabled	boolean	Fetches Brotli-compressed assets from your origin and caches them on edge servers.

cacheError

- **Property Manager name**: Cache HTTP Error Responses
- **Behavior version**: The `v2023-05-30` rule format supports the `cacheError` behavior v1.1.
- **Rule format status**: Deprecated, outdated rule format
- **Access**: Read-write
- **Allowed in includes**: Yes

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

This behavior no longer caches `400` error responses from the origin server. If you need to cache such errors, you can set up a custom variable. See Caching 400 responses for more information.

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 `500` , `502` , `503` , and `504` error codes. This avoids re-fetching and re-caching content after transient errors.

cacheId

- **Property Manager name**: Cache ID Modification⬚
- **Behavior version**: The `v2023-05-30` rule format supports the `cacheId` behavior v1.3.
- **Rule format status**: Deprecated, outdated rule format
- **Access**: Read-write
- **Allowed in includes**: Yes

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

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

Option	Type	Description	Requires
rule	enum	Specifies how to modify the cache ID.	
	INCLUDE_ QUERY_ PARAMS	Includes the specified set of query parameters when forming a cache ID.	
	INCLUDE_ COOKIES	Includes specified cookies in the cache ID.	
	INCLUDE_ HEADERS	Includes specified HTTP headers in the cache ID.	
	EXCLUDE_ QUERY_ PARAMS	Excludes the specified set of query parameters when forming a cache ID.	
	INCLUDE_ ALL_ QUERY_ PARAMS	Includes all query parameters when forming a cache ID.	
	INCLUDE_ VARIABLE	Includes a specific user variable in the cache ID.	

Option	Type	Description	Requires
	INCLUDE_URL	Includes the full URL, the same as the default without the `cacheid` behavior.	
include Value	boolean	Includes the value of the specified elements in the cache ID. Otherwise only their names are included.	`rule` is either: INCLUDE_COOKIES , INCLUDE_QUERY_PARAMS , INCLUDE_HEADERS
optional	boolean	Requires the behavior's specified elements to be present for content to cache. When disabled, requests that lack the specified elements are still cached.	`rule` is either: INCLUDE_COOKIES , INCLUDE_QUERY_PARAMS , INCLUDE_HEADERS , EXCLUDE_QUERY_PARAMS
elements	string array	Specifies the names of the query parameters, cookies, or headers to include or exclude from the cache ID.	`rule` is either: INCLUDE_COOKIES , INCLUDE_QUERY_PARAMS , INCLUDE_HEADERS , EXCLUDE_QUERY_PARAMS
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 `v2023-05-30` rule format supports the `cacheKeyIgnoreCase` behavior v1.2.
- **Rule format status**: Deprecated, outdated rule format
- **Access**: Read-write
- **Allowed in includes**: Yes

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 `v2023-05-30` rule format supports the `cacheKeyQueryParams` behavior v1.2.
- **Rule format status**: Deprecated, outdated rule format
- **Access**: Read-write
- **Allowed in includes**: Yes

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 *not* 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, `?q=akamai&state=ma` and `?state=ma&q=akamai` 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 `parameters` field.	
	IGNORE	Include all but the sequence of values in the `parameters` 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, `parameters` 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 `v2023-05-30` rule format supports the `cacheKeyRewrite` behavior v1.1.
- **Rule format status**: [Deprecated, outdated rule format](#)
- **Access**: [Read-only](#)
- **Allowed in includes**: [Yes](#)

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 `v2023-05-30` rule format supports the `cachePost` behavior v1.1.
- **Rule format status**: [Deprecated, outdated rule format](#)
- **Access**: [Read-write](#)
- **Allowed in includes**: [Yes](#)

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 Temporary Redirects](#)
- **Behavior version**: The `v2023-05-30` rule format supports the `cacheRedirect` behavior v1.0.
- **Rule format status**: [Deprecated, outdated rule format](#)
- **Access**: [Read-write](#)
- **Allowed in includes**: [Yes](#)

Controls the caching of HTTP 302 and 307 temporary redirects. By default, Akamai edge servers don't cache them. Enabling this behavior instructs edge servers to allow these redirects to be cached the same as HTTP 200 responses.

Use the `caching` behavior to separately control TTL for these redirects, either with a specific TTL value or based on `Cache-Control` or `Expires` response headers.

Option	Type	Description
`enabled`	boolean	Enables the redirect caching behavior.

cacheTag

- **Property Manager name**: [Cache Tag](#)
- **Behavior version**: The `v2023-05-30` rule format supports the `cacheTag` behavior v1.0.
- **Rule format status**: [Deprecated, outdated rule format](#)
- **Access**: [Read-write](#)
- **Allowed in includes**: [Yes](#)

This adds a cache tag to the requested object. With cache tags, you can flexibly fast purge tagged segments of your cached content. You can either define these tags with an `Edge-Cache-Tag` header at the origin server level, or use this behavior to directly add a cache tag to the object as the edge server caches it. The `cacheTag` behavior can only take a single value, including a variable. If you want to specify more tags for an object, add a few instances of this behavior to your configuration.

See [Fast Purge](#) for guidance on best practices to deploy cache tags. Use the [Fast Purge API](#) to purge by cache tag programmatically.

Note that this behavior is not compatible with the `dynamicThroughtputOptimization` behavior. Don't include both behaviors in a rule for the same request.

Option	Type	Description
`tag`	string (allows [variables](#))	Specifies the cache tag you want to add to your cached content. A cache tag is only added when the object is first added to cache. A single cache tag can't exceed 128 characters and can only include alphanumeric characters, plus this class of characters: `[!#$%'+./^_`|~-]`

cacheTagVisible

- **Property Manager name**: Cache Tag Visibility
- **Behavior version**: The `v2023-05-30` rule format supports the `cacheTagVisible` behavior v1.0.
- **Rule format status**: Deprecated, outdated rule format
- **Access**: Read-write
- **Allowed in includes**: Yes

Cache tags are comma-separated string values you define within an `Edge-Cache-Tag` header. You can use them to flexibly fast purge tagged segments of your cached content. You can either define these headers at the origin server level, or use the `modifyOutgoingResponseHeader` behavior to configure them at the edge. Apply this behavior to confirm you're deploying the intended set of cache tags to your content.

See Fast Purge for guidance on best practices to deploy cache tags. Use the Fast Purge API to purge by cache tag programmatically.

Option	Type	Description
behavior	enum	Specifies when to include the `Edge-Cache-Tag` in responses.
	NEVER	Strip out the `Edge-Cache-Tag` header, edge servers' default response.
	PRAGMA_HEADER	Edge servers respond with the `Edge-Cache-Tag` header only when you pass in a `Pragma: akamai-x-get-cache-tags` header as part of the request.
	ALWAYS	Include the `Edge-Cache-Tag` header in all responses.

caching

- **Property Manager name**: Caching
- **Behavior version**: The `v2023-05-30` rule format supports the `caching` behavior v1.12.
- **Rule format status**: Deprecated, outdated rule format
- **Access**: Read-write
- **Allowed in includes**: Yes

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 override this behavior. For more details on how caching works in Property Manager, see the Learn about caching section in the guide.

Option	Type	Description	Requires
behavior	enum	Specify the caching option.	

Option	Type	Description	Requires
	MAX_AGE	Honor the origin's `MAX_AGE` header.	
	NO_ STORE	Clears the cache and serves from the origin.	
	BYPASS_ CACHE	Retains the cache but serves from the origin.	
	CACHE_ CONTROL_ AND_ EXPIRES	Honor the origin's `CACHE_CONTROL` or `EXPIRES` header, whichever comes last. This adds support for the `s-maxage` response directive specified in [RFC 7234](#)⧉. Use this alternative value to instruct a downstream CDN how long to cache content.	
	CACHE_ CONTROL	Honor the origin's `CACHE_CONTROL` header. This adds support for the `s-maxage` response directive specified in [RFC 7234](#)⧉. Use this alternative value to instruct a downstream CDN how long to cache content.	
	EXPIRES	Honor the origin's `EXPIRES` header.	
must Revalidate	boolean	Determines what to do once the cached content has expired, by which time the Akamai platform should have re-fetched and validated content from the origin. If enabled, only allows the re-fetched content to be served. If disabled, may serve stale content if the origin is unavailable.	`behavior` is either: `CACHE_CONTROL_AND_ EXPIRES`, `CACHE_ CONTROL`, `EXPIRES`, `MAX_AGE`
ttl	string (duration)	The maximum time content may remain cached. Setting the value to `0` is the same as setting a `no-cache` header, which forces content to revalidate.	`behavior` is `MAX_AGE`
defaultTtl	string (duration)	Set the `MAX_AGE` header for the cached content.	`behavior` is either: `CACHE_CONTROL_AND_ EXPIRES`, `CACHE_ CONTROL`, `EXPIRES`
enhanced Rfc Support	boolean	This enables honoring particular `Cache-Control` header directives from the origin. Supports all official [RFC 7234](#)⧉ directives except for `no-transform`.	`behavior` is either: `CACHE_CONTROL`, `CACHE_CONTROL_AND_ EXPIRES`
honorNo Store	boolean	Instructs edge servers not to cache the response when the origin response includes the `no-store` directive.	`enhancedRfcSupport` is true
honor Private	boolean	Instructs edge servers not to cache the response when the origin response includes the `private` directive.	`behavior` is either: `CACHE_CONTROL`, `CACHE_CONTROL_AND_ EXPIRES`
honorNo Cache	boolean	With the `no-cache` directive present in the response, this instructs edge servers to validate or refetch the response for each request. Effectively, set the time to live `ttl` to zero seconds.	`enhancedRfcSupport` is true
honorMax Age	boolean	This instructs edge servers to cache the object for a length of time set by the `max-age` directive in the response. When present in the origin response, this directive takes precedence over the `max-age` directive and the `defaultTtl` setting.	`enhancedRfcSupport` is true
honor SMaxage	boolean	Instructs edge servers to cache the object for a length of time set by the `s-maxage` directive in the response. When present in the origin response, this directive takes precedence over the `max-age` directive and the `defaultTtl` setting.	`enhancedRfcSupport` is true
honor Must Revalidate	boolean	This instructs edge servers to successfully revalidate with the origin server before using stale objects in the cache to satisfy new requests.	`behavior` is either: `CACHE_CONTROL`, `CACHE_CONTROL_AND_ EXPIRES`
honor Proxy Revalidate	boolean	With the `proxy-revalidate` directive present in the response, this instructs edge servers to successfully revalidate with the origin server before using stale objects in the cache to satisfy new requests.	`enhancedRfcSupport` is true

centralAuthorization

- **Property Manager name**: Centralized Authorization
- **Behavior version**: The `v2023-05-30` rule format supports the `centralAuthorization` behavior v1.1.
- **Rule format status**: Deprecated, outdated rule format
- **Access**: Read-write
- **Allowed in includes**: Yes

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 `v2023-05-30` rule format supports the `chaseRedirects` behavior v1.1.
- **Rule format status**: Deprecated, outdated rule format
- **Access**: Read-write
- **Allowed in includes**: Yes

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

Note: Chase Redirects is not compatible with Amazon Web Services and Google Cloud Storage authentication methods in the `originCharacteristics` behavior. If you're using any of these authentication methods, Chase Redirects gets automatically disabled.

Option	Type	Description
enabled	boolean	Allows edge servers to chase redirects.
limit	string	Specifies, as a string, the maximum number of redirects to follow.
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 `v2023-05-30` rule format supports the `clientCharacteristics` behavior v1.0.
- **Rule format status**: Deprecated, outdated rule format
- **Access**: Read-write
- **Allowed in includes**: Yes

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 *content Characteristics*.

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.

cloudInterconnects

- **Property Manager name**: [Cloud Interconnects for Google Cloud (GCP)](#)
- **Behavior version**: The `v2023-05-30` rule format supports the `cloudInterconnects` behavior v1.1.
- **Rule format status**: [Deprecated, outdated rule format](#)
- **Access**: [Read-write](#)
- **Allowed in includes**: [No (temporarily)](#)

Cloud Interconnects forwards traffic from edge servers to your cloud origin through Private Network Interconnects (PNIs), helping to reduce the egress costs at the origin. Supports origins hosted by Google Cloud Provider (GCP).

Option	Type	Description
enabled	boolean	Channels the traffic to maximize the egress discount at the origin.
cloud Locations	string array	Specifies the geographical locations of your cloud origin. You should enable Cloud Interconnects only if your origin is in one of these locations, since GCP doesn't provide a discount for egress traffic for any other regions.
	AS	Asia.
	EU	Europe.
	NA	North America.

cloudWrapper

- **Property Manager name**: [Cloud Wrapper](#)⬈
- **Behavior version**: The `v2023-05-30` rule format supports the `cloudWrapper` behavior v1.0.
- **Rule format status**: [Deprecated, outdated rule format](#)
- **Access**: [Read-write](#)
- **Allowed in includes**: [No (temporarily)](#)

[Cloud Wrapper](#) maximizes origin offload for large libraries of video, game, and software downloads by optimizing data caches in regions nearest to your origin. You can't use this behavior in conjunction with `sureRoute` or `tiered Distribution` .

Option	Type	Description
enabled	boolean	Enables Cloud Wrapper behavior.
location	string	The location you want to distribute your Cloud Wrapper cache space to. This behavior allows all locations configured in your Cloud Wrapper configuration.

cloudWrapperAdvanced

- **Property Manager name**: [Cloud Wrapper Advanced](#)
- **Behavior version**: The `v2023-05-30` rule format supports the `cloudWrapperAdvanced` behavior v1.0.
- **Rule format status**: [Deprecated, outdated rule format](#)
- **Access**: [Read-only](#)
- **Allowed in includes**: [No (temporarily)](#)

Your account representative uses this behavior to implement a customized failover configuration on your behalf. Use Cloud Wrapper Advanced with an enabled `cloudWrapper` behavior in the same rule.

Option	Type	Description	[Requires](#)
enabled	boolean	Enables failover for Cloud Wrapper.	
failover Map	string	Specifies the failover map to handle Cloud Wrapper failures. Contact your account representative for more information.	
custom FailoverMap	string (allows [variables](#))	Specifies the custom failover map to handle Cloud Wrapper failures. Contact your account representative for more information.	`failoverMap` is Custom

commonMediaClientData

- **Property Manager name**: [Common Media Client Data support](#)
- **Behavior version**: The `v2023-05-30` rule format supports the `commonMediaClientData` behavior v1.0.
- **Rule format status**: [Deprecated, outdated rule format](#)
- **Access**: [Read-write](#)
- **Allowed in includes**: [Yes](#)

Use this behavior to send expanded playback information as CMCD metadata in requests from a media player. Edge servers may use this metadata for segment prefetching to optimize your content's delivery, or for logging. For more details and additional property requirements, see the [Adaptive Media Delivery](#) documentation.

Option	Type	Description
enableCMCDSegment Prefetch	boolean	Uses Common Media Client Data (CMCD) metadata to determine the segment URLs your origin server prefetches to speed up content delivery.

constructResponse

- **Property Manager name**: Construct Response
- **Behavior version**: The v2023-05-30 rule format supports the constructResponse behavior v1.3.
- **Rule format status**: Deprecated, outdated rule format
- **Access**: Read-write
- **Allowed in includes**: Yes

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 .

Don't use this behavior with Bot Manager when you set up alternate hostnames↗ to send bot traffic to an alternate page or site. Make sure the constructResponse behavior is disabled in that case.

Option	Type	Description
enabled	boolean	Serves the custom response.
body	string (allows variables)	HTML response of up to 2000 characters to send to the end-user client.
responseCode	enum	The HTTP response code to send to the end-user client.
		Supported values: 200 401 403 404 405 417 500
forceEviction	boolean	Removes the underlying object from the cache, since it is not being served.
ignorePurge	boolean	Whether to ignore the custom response when purging.

contentCharacteristics

- **Property Manager name**: Content Characteristics
- **Behavior version**: The v2023-05-30 rule format supports the contentCharacteristics behavior v1.1.
- **Rule format status**: Deprecated, outdated rule format
- **Access**: Read-write
- **Allowed in includes**: Yes

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

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

Option	Type	Description
objectSize	enum	Optimize based on the size of the object retrieved from the origin.
	LESS_THAN_1MB	Less than 1Mb.
	ONE_MB_TO_TEN_MB	1-10 Mb.
	TEN_MB_TO_100_MB	10-100 Mb.
	OTHER	A fallback value.
	UNKNOWN	Defer this optimization.
popularityDistribution	enum	Optimize based on the content's expected popularity.
	LONG_TAIL	A low volume of requests over a long period.
	ALL_POPULAR	A high volume of requests over a short period.
	OTHER	A fallback value.
	UNKNOWN	Defer this optimization.
catalogSize	enum	Optimize based on the total size of the content library delivered.
	SMALL	Under 100GB.
	MEDIUM	100GB-1TB.
	LARGE	1TB-100TB.
	EXTRA_LARGE	More than 100TB.
	OTHER	A fallback value.
	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 `v2023-05-30` rule format supports the `contentCharacteristicsAMD` behavior v1.1.
- **Rule format status**: Deprecated, outdated rule format
- **Access**: Read-write
- **Allowed in includes**: Yes

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.	
segmentDuration HLSCustom	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.	

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.	
`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.	
`segmentDuration HDSCustom`	number	Customizes the number of seconds for the fragment.	`segmentDurationHDS` is `OTHER`
`segmentSizeHDS`	enum	Specifies the size of the media object retrieved from the origin.	`hds` is `true`
	`LESS_THAN_1MB`	Less than 1Mb.	
	`ONE_MB_TO_TEN_MB`	1-10Mb.	
	`TEN_MB_TO_100_MB`	10-100Mb.	
	`GREATER_THAN_100MB`	More than 100Mb.	
	`UNKNOWN`	Defer this optimization.	
	`OTHER`	Customize the value.	
`dash`	boolean	Enable delivery of DASH media.	
`segmentDurationDASH`	enum	Specifies the duration of individual segments.	`dash` is `true`
	`SEGMENT_DURATION_2S`	2 seconds.	
	`SEGMENT_DURATION_4S`	4 seconds.	
	`SEGMENT_DURATION_6S`	6 seconds.	
	`SEGMENT_DURATION_8S`	8 seconds.	
	`SEGMENT_DURATION_10S`	10 seconds.	
	`OTHER`	Customize the value.	
`segmentDuration DASHCustom`	number	Customizes the number of seconds for the segment.	`segmentDurationDASH` is `OTHER`

Option	Type	Description	Requires
segmentSizeDASH	enum	Specifies the size of the media object retrieved from the origin.	dash is true
	LESS_THAN_1MB	Less than 1Mb.	
	ONE_MB_TO_TEN_MB	1-10Mb.	
	TEN_MB_TO_100_MB	10-100Mb.	
	GREATER_THAN_100MB	More than 100Mb.	
	UNKNOWN	Defer this optimization.	
	OTHER	Sizes 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 v2023-05-30 rule format supports the contentCharacteristicsDD behavior v1.0.

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

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.
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	Less than 100Gb.
	MEDIUM	100Gb-1Tb.
	LARGE	1-100Tb.
	EXTRA_LARGE	More than 100Tb.
	OTHER	A fallback value.
	UNKNOWN	Defer this optimization.
contentType	enum	Optimize based on the type of content.
	VIDEO	Video.
	SOFTWARE	Software.
	SOFTWARE_PATCH	Software patch.
	GAME	Game.
	GAME_PATCH	Game patch.
	OTHER_DOWNLOADS	Other downloads that don't fall into these categories.
	UNKNOWN	Defer this optimization.
optimizeOption	boolean	Optimizes the delivery throughput and download times for large files.

contentCharacteristicsWsdLargeFile

- **Property Manager name**: Content Characteristics - Large File
- **Behavior version**: The `v2023-05-30` rule format supports the `contentCharacteristicsWsdLargeFile` behavior v1.0.
- **Rule format status**: Deprecated, outdated rule format
- **Access**: Read-write
- **Allowed in includes**: Yes

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

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

Option	Type	Description
objectSize	enum	Optimize based on the size of the object retrieved from the origin.
	LESS_THAN_1MB	Less than 1Mb.
	ONE_MB_TO_TEN_MB	1-10Mb.
	TEN_MB_TO_100_MB	10-100Mb.
	GREATER_THAN_100MB	More than 100Mb.
	UNKNOWN	Defer this optimization.
popularityDistribution	enum	Optimize based on the content's expected popularity.
	LONG_TAIL	A low volume of requests over a long period.
	ALL_POPULAR	A high volume of requests over a short period.
	UNKNOWN	Defer this optimization.
catalogSize	enum	Optimize based on the total size of the content library delivered.
	SMALL	Less than 100Gb.
	MEDIUM	100Gb-1Tb.
	LARGE	1-100Tb.
	EXTRA_LARGE	More than 100Tb.
	UNKNOWN	Defer this optimization.
contentType	enum	Optimize based on the type of content.
	VIDEO	Video.
	SOFTWARE	Software.
	SOFTWARE_PATCH	Software patch.
	GAME	Game.
	GAME_PATCH	Game patch.

Option	Type	Description
	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 `v2023-05-30` rule format supports the `contentCharacteristicsWsdLive` behavior v1.0.
- **Rule format status**: Deprecated, outdated rule format
- **Access**: Read-write
- **Allowed in includes**: Yes

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

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

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

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

Option	Type	Description	Requires
	GREATER_THAN_100MB	More than 100Mb.	
	UNKNOWN	Defer this optimization.	
	OTHER	Sizes 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.	
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 that straddle these ranges.	

contentCharacteristicsWsdVod

- **Property Manager name**: [Content Characteristics - Streaming Video On-demand](#)⇗
- **Behavior version**: The `v2023-05-30` rule format supports the `contentCharacteristicsWsdVod` behavior v1.0.
- **Rule format status**: [Deprecated, outdated rule format](#)
- **Access**: [Read-write](#)
- **Allowed in includes**: [Yes](#)

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.	

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

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.	
`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.	
`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.	
`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.	
`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.	

contentTargetingProtection

- **Property Manager name**: Content Targeting - Protection
- **Behavior version**: The `v2023-05-30` rule format supports the `contentTargetingProtection` behavior v1.1.
- **Rule format status**: Deprecated, outdated rule format
- **Access**: Read-write
- **Allowed in includes**: Yes

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.	
enableGeo Protection	boolean	When enabled, verifies IP addresses are unique to specific geographic regions.	
geoProtection Mode	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
override IPAddresses	string array	Specify a set of IP addresses or CIDR blocks that exceptions to the set of included or excluded areas.	enableGeoProtection is true
enableGeo RedirectOnDeny	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.	enableGeoRedirectOn Deny is true
enable IPProtection	boolean	Allows you to control access to your content from specific sets of IP addresses and CIDR blocks.	
ipProtectionMode	enum	Specifies how to handle requests.	enableIPProtection is true
	ALLOW	Allow requests.	
	DENY	Deny requests.	
ipAddresses	string array	Specify a set of IP addresses or CIDR blocks to allow or deny.	enableIPProtection is true
enableIPRedirect OnDeny	boolean	When enabled, redirects denied requests rather than responding with an error code.	enableIPProtection is true
ipRedirectUrl	string	This specifies the full URL to the redirect page for denied requests.	enableIPRedirectOn Deny is true
enableReferrer Protection	boolean	Allows you allow traffic from certain referring websites, and disallow traffic from unauthorized sites that hijack those links.	
referrerProtection Mode	enum	Specify the action to take.	enableReferrer Protection is true
	ALLOW	Allow requests.	

Option	Type	Description	Requires
	DENY	Deny requests.	
referrerDomains	string array	Specifies the set of domains from which to allow or deny traffic.	enableReferrer Protection is true
enableReferrer RedirectOnDeny	boolean	When enabled, redirects denied requests rather than responding with an error code.	enableReferrer Protection is true
referrerRedirect Url	string	This specifies the full URL to the redirect page for denied requests.	enableReferrerRedirect OnDeny is true

corsSupport

- **Property Manager name**: CORS Protocol Support
- **Behavior version**: The `v2023-05-30` rule format supports the `corsSupport` behavior v1.0.
- **Rule format status**: Deprecated, outdated rule format
- **Access**: Read-write
- **Allowed in includes**: Yes

Cross-origin resource sharing (CORS) allows web pages in one domain to access restricted resources from your domain. Specify external origin hostnames, methods, and headers that you want to accept via HTTP response headers. Full support of CORS requires allowing requests that use the OPTIONS method. See `allowOptions` .

Option	Type	Description	Requires
enabled	boolean	Enables CORS feature.	
allow Origins	enum	In responses to preflight requests, sets which origin hostnames to accept requests from.	
	ANY	Accept from any origin hostname.	
	SPECIFIED	Accept from a set of origin hostnames.	
origins	string array	Defines the origin hostnames to accept requests from. The hostnames that you enter need to start with `http` or `https` . For detailed hostname syntax requirements, refer to RFC-952 and RFC-1123 specifications.	allow Origins is SPECIFIED
allow Credentials	boolean	Accepts requests made using credentials, like cookies or TLS client certificates.	
allow Headers	enum	In responses to preflight requests, defines which headers to allow when making the actual request.	
	ANY	Allow any headers.	
	SPECIFIED	Allow a specific set of headers.	
headers	string array	Defines the supported request headers.	allow Headers is SPECIFIED
methods	string array	Specifies any combination of the following methods: `DELETE` , `GET` , `PATCH` , `POST` , and `PUT` that are allowed when accessing the resource from an external domain.	

Option	Type	Description	Requires
expose Headers	string array (allows variables)	In responses to preflight requests, lists names of headers that clients can access. By default, clients can access the following simple response headers: `Cache-Control` , `Content-Language` , `Content-Type` , `Expires` , `Last-Modified` , and `Pragma` . You can add other header names to make them accessible to clients.	
preflight MaxAge	string (duration)	Defines the number of seconds that the browser should cache the response to a preflight request.	

cpCode

- **Property Manager name**: Content Provider Code
- **Behavior version**: The `v2023-05-30` rule format supports the `cpCode` behavior v1.1.
- **Rule format status**: Deprecated, outdated rule format
- **Access**: Read-write
- **Allowed in includes**: Yes

Content Provider Codes (CP codes) allow you to distinguish various reporting and billing traffic segments, and you need them to access properties. You receive an initial CP code when purchasing Akamai, and you can run the Create a new CP code operation to generate more. This behavior applies any valid CP code, either as required as a default at the top of the rule tree, or subsequently to override the default. For a CP code to be valid, it needs to be assigned the same contract and product as the property, and the group needs access to it. For available values, run the List CP codes operation.

Option	Type	Description
value	object	Specifies the CP code as an object. You only need to provide the initial `id` , stripping any `cpc_` `prefix` to pass the integer to the rule tree. Additional CP code details may reflect back in subsequent read-only data.
value.cpCode Limits	array	**Read-only**. Describes the current usage limit for the CP code.
value.created Date	integer	**Read-only**. UNIX epoch timestamp reflecting when the CP code was originally created.
value.description	string	**Read-only**. Additional description for the CP code.
value.id	integer	Unique identifier for each CP code. Initially, you get this value when creating a new CP code in PAPI. You can also assign a `cpcodeId` value from the List CP codes operation.
value.name	string	**Read-only**. The name of the CP code you specify as the `cpcodeName` when creating a new CP code in PAPI. You can modify this value with the PUT operation in the CP codes and Reporting Groups API.
value.products	array	**Read-only**. The set of products the CP code is assigned to. This reflects `productId` values you specify when creating a new CP code in PAPI.

customBehavior

- **Property Manager name**: Custom Behavior
- **Behavior version**: The `v2023-05-30` rule format supports the `customBehavior` behavior v1.0.
- **Rule format status**: Deprecated, outdated rule format
- **Access**: Read-write
- **Allowed in includes**: Yes

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 `v2023-05-30` rule format supports the `datastream` behavior v1.8.
- **Rule format status**: Deprecated, outdated rule format
- **Access**: Read-write
- **Allowed in includes**: No (temporarily)

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.

In the latest rule format, `logStreamName` is an array of string values, such as `["1234", "5678"]` instead of a single `1234` integer value. Make sure your property accepts the single integer for the previous rule format, otherwise use an array to prevent errors.

Option	Type	Description	Requires
stream Type	enum	Specify the DataStream type.	
	BEACON	Low latency streaming of raw or aggregated data for push delivery or through the pull API.	
	LOG	Scalable, low latency streaming of raw data for push delivery.	
	BEACON_ AND_LOG	Specify both.	

Option	Type	Description	Requires
enabled	boolean	Enables DataStream reporting.	
datastream Ids	string	A set of dash-separated DataStream ID values to limit the scope of reported data. By default, all active streams report. Use the DataStream application to gather stream ID values that apply to this property configuration. Specifying IDs for any streams that don't apply to this property has no effect, and results in no data reported.	
log Enabled	boolean	Enables log collection for the property by associating it with DataStream configurations.	stream Type is either: LOG , BEACON_ AND_LOG
logStream Name	string	Specifies the unique IDs of streams configured for the property. For properties created with the previous version of the rule format, this option contains a string instead of an array of strings. You can use the List streams operation to get stream IDs.	log Enabled is true
sampling Percentage	number	Specifies the percentage of log data you want to collect for this property.	log Enabled is true
collect Midgress Traffic	boolean	If enabled, gathers midgress traffic data within the Akamai platform, such as between two edge servers, for all streams configured.	log Enabled is true

dcp

- **Property Manager name**: IoT Edge Connect
- **Behavior version**: The v2023-05-30 rule format supports the dcp behavior v1.0.
- **Rule format status**: Deprecated, outdated rule format
- **Access**: Read-write
- **Allowed in includes**: No (temporarily)

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.
namespace Id	string	Specifies the globally reserved name for a specific configuration. It includes authorization rules over publishing and subscribing to logical categories known as *topics*. 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.

Option	Type	Description
gwenabled	boolean	When enabled, you can publish and receive messages over a secured HTTP connection on port 443.
anonymous	boolean	When enabled, you don't need to pass the JWT token with the mqtt request, and JWT validation is skipped.

dcpAuthHMACTransformation

- **Property Manager name**: Variable Hash Transformation ⬈
- **Behavior version**: The `v2023-05-30` rule format supports the `dcpAuthHMACTransformation` behavior v1.0.
- **Rule format status**: Deprecated, outdated rule format
- **Access**: Read-write
- **Allowed in includes**: No (temporarily)

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

Note that you can apply this hash transformation, or either of the `dcpAuthRegexTransformation` or `dcpAuthSubstring Transformation` behaviors.

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

dcpAuthRegexTransformation

- **Property Manager name**: Variable Regex Transformation ⬈
- **Behavior version**: The `v2023-05-30` rule format supports the `dcpAuthRegexTransformation` behavior v1.0.
- **Rule format status**: Deprecated, outdated rule format

- **Access**: Read-write
- **Allowed in includes**: No (temporarily)

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

Note that you can apply this regular expression transformation, or either of the `dcpAuthHMACTransformation` or `dcpAuthSubstringTransformation` behaviors.

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

dcpAuthSubstringTransformation

- **Property Manager name**: Variable Substring Transformation
- **Behavior version**: The `v2023-05-30` rule format supports the `dcpAuthSubstringTransformation` behavior v1.0.
- **Rule format status**: Deprecated, outdated rule format
- **Access**: Read-write
- **Allowed in includes**: No (temporarily)

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

Note that you can apply this substring transformation, or either of the `dcpAuthHMACTransformation` or `dcpAuthRegexTransformation` behaviors.

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

dcpAuthVariableExtractor

- **Property Manager name**: Mutual Authentication
- **Behavior version**: The `v2023-05-30` rule format supports the `dcpAuthVariableExtractor` behavior v1.0.
- **Rule format status**: Deprecated, outdated rule format
- **Access**: Read-write
- **Allowed in includes**: No (temporarily)

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

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

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

dcpDefaultAuthzGroups

- **Property Manager name**: [Default Authorization Groups](#)
- **Behavior version**: The `v2023-05-30` rule format supports the `dcpDefaultAuthzGroups` behavior v1.0.
- **Rule format status**: [Deprecated, outdated rule format](#)
- **Access**: [Read-write](#)
- **Allowed in includes**: [No (temporarily)](#)

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.

dcpDevRelations

- **Property Manager name**: [IoT Edge Connect Dev Relations](#)
- **Behavior version**: The `v2023-05-30` rule format supports the `dcpDevRelations` behavior v1.0.
- **Rule format status**: [Deprecated, outdated rule format](#)
- **Access**: [Read-write](#)
- **Allowed in includes**: [No (temporarily)](#)

The [Internet of Things: Edge Connect](#) product allows connected users and devices to communicate on a publish-subscribe basis within reserved namespaces. This behavior allows Akamai-external clients to use developer test accounts in a shared environment. In conjunction with `verifyJsonWebTokenForDcp`, this behavior allows you to use your own JWTs in your requests, or those generated by Akamai. It lets you either enable the default JWT server for your test configuration by setting the authentication endpoint to a default path, or specify custom settings for your JWT server and the authentication endpoint.

Option	Type	Description	Requires
enabled	boolean	Enables the default JWT server and sets the authentication endpoint to a default path.	
customValues	boolean	Allows you to specify custom JWT server connection values.	
hostname	string	Specifies the JWT server's hostname.	customValues is true
path	string	Specifies the path to your JWT server's authentication endpoint. This lets you generate JWTs to sign your requests.	customValues is true

deliveryReceipt

- **Property Manager name**: [Cloud Monitor Data Delivery](#)
- **Behavior version**: The `v2023-05-30` rule format supports the `deliveryReceipt` behavior v1.1.
- **Rule format status**: [Deprecated, outdated rule format](#)
- **Access**: [Read-write](#)
- **Allowed in includes**: [Yes](#)

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.

denyAccess

- **Property Manager name**: [Control Access](#)
- **Behavior version**: The `v2023-05-30` rule format supports the `denyAccess` behavior v1.2.
- **Rule format status**: [Deprecated, outdated rule format](#)
- **Access**: [Read-write](#)
- **Allowed in includes**: [Yes](#)

Assuming a condition in the rule matches, this denies access to the requested content. For example, a `userLocation` match paired with this 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 `v2023-05-30` rule format supports the `denyDirectFailoverAccess` behavior v1.1.
- **Rule format status**: [Deprecated, outdated rule format](#)
- **Access**: [Read-write](#)
- **Allowed in includes**: [Yes](#)

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.

deviceCharacteristicCacheId

- **Property Manager name**: [Device Characterization - Define Cached Content](#)
- **Behavior version**: The `v2023-05-30` rule format supports the `deviceCharacteristicCacheId` behavior v1.4.
- **Rule format status**: [Deprecated, outdated rule format](#)
- **Access**: [Read-write](#)
- **Allowed in includes**: [Yes](#)

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.

Option	Type	Description
		Supported values:

		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 `v2023-05-30` rule format supports the `deviceCharacteristicHeader` behavior v1.3.
- **Rule format status**: Deprecated, outdated rule format
- **Access**: Read-write
- **Allowed in includes**: Yes

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.

Option	Type	Description
		Supported values:

ACCEPT_THIRD_PARTY_COOKIE
AJAX_PREFERRED_GEOLOC_API
AJAX_SUPPORT_JAVASCRIPT
BRAND_NAME
COOKIE_SUPPORT
DEVICE_OS
DEVICE_OS_VERSION
DUAL_ORIENTATION
FLASH_LITE_VERSION
FULL_FLASH_SUPPORT
GIF_ANIMATED
HTML_PREFERRED_DTD
IS_MOBILE
IS_TABLET
IS_WIRELESS_DEVICE
JPG
MARKETING_NAME

MAX_IMAGE_HEIGHT
MAX_IMAGE_WIDTH
MOBILE_BROWSER
MOBILE_BROWSER_VERSION
MODEL_NAME
PDF_SUPPORT
PHYSICAL_SCREEN_HEIGHT
PHYSICAL_SCREEN_WIDTH
PNG
PREFERRED_MARKUP
RESOLUTION_HEIGHT
RESOLUTION_WIDTH
VIEWPORT_INITIAL_SCALE
VIEWPORT_WIDTH
XHTMLMP_PREFERRED_MIME_TYPE
XHTML_FILE_UPLOAD
XHTML_PREFERRED_CHARSET

dnsAsyncRefresh

- **Property Manager name**: DNS Asynchronous Refresh
- **Behavior version**: The `v2023-05-30` rule format supports the `dnsAsyncRefresh` behavior v1.1.
- **Rule format status**: Deprecated, outdated rule format
- **Access**: Read-write
- **Allowed in includes**: Yes

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
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 `v2023-05-30` rule format supports the `dnsPrefresh` behavior v1.1.
- **Rule format status**: [Deprecated, outdated rule format](#)
- **Access**: [Read-only](#)
- **Allowed in includes**: [Yes](#)

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 prefresh it.
timeout	string (duration)	Specifies the amount of time to prefresh a DNS entry if there have been no requests to the domain name.

downgradeProtocol

- **Property Manager name**: [Protocol Downgrade](#)
- **Behavior version**: The `v2023-05-30` rule format supports the `downgradeProtocol` behavior v1.1.
- **Rule format status**: [Deprecated, outdated rule format](#)
- **Access**: [Read-write](#)
- **Allowed in includes**: [No (temporarily)](#)

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 `v2023-05-30` rule format supports the `downloadCompleteMarker` behavior v1.0.
- **Rule format status**: [Deprecated, outdated rule format](#)
- **Access**: [Read-write](#)
- **Allowed in includes**: [Yes](#)

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 `v2023-05-30` rule format supports the `downloadNotification` behavior v1.0.
- **Rule format status**: [Deprecated, outdated rule format](#)
- **Access**: [Read-write](#)
- **Allowed in includes**: [No (temporarily)](#)

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 `v2023-05-30` rule format supports the `downstreamCache` behavior v1.2.
- **Rule format status**: [Deprecated, outdated rule format](#)
- **Access**: [Read-write](#)
- **Allowed in includes**: [Yes](#)

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 `allowBehavior` chooses the caching method and headers to send to the client.	
	MUST_ REVALIDATE	This equates to a `Cache-Control: no-cache` header, which allows caching but forces the client browser to send an `if-modified-since` request each time it requests the object.	
	BUST	Sends cache-busting headers downstream.	
	TUNNEL_ ORIGIN	This passes `Cache-Control` and `Expires` 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.	
allow Behavior	enum	Specify how the edge server calculates the downstream cache by setting the value of the `Expires` 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 `cache:max-age` 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 `0` equates to a `no-cache` header that forces revalidation.	`allowBehavior` is `FROM_VALUE`
send Headers	enum	Specifies the HTTP headers to include in the response to the client.	`behavior` is `ALLOW`
	CACHE_ CONTROL_ AND_EXPIRES	Sends both `Cache-Control` and `Expires` header.	
	CACHE_ CONTROL	Sends only the origin's `Cache-Control` header.	
	EXPIRES	Sends only the origin's `Expires` header.	
	PASS_ORIGIN	Sends the same set of `Cache-Control` and `Expires` headers received from the origin.	
send Private	boolean	Adds a `Cache-Control: private` header to prevent objects from being cached in a shared caching proxy.	`behavior` is either: `ALLOW`, `MUST_ REVALIDATE` AND `sendHeaders` is not `EXPIRES`

dynamicThroughtputOptimization

- **Property Manager name**: Quick Retry
- **Behavior version**: The `v2023-05-30` rule format supports the `dynamicThroughtputOptimization` behavior v1.0.
- **Rule format status**: Deprecated, outdated rule format
- **Access**: Read-write
- **Allowed in includes**: Yes

Enables *quick retry*, which detects slow forward throughput while fetching an object, and attempts a different forward connection path to avoid congestion. By default, connections under 5 mbps trigger this behavior. When the transfer rate drops below this rate during a connection attempt, quick retry is enabled and a different forward connection path is used. Contact Akamai Professional Services to override this threshold.

Note that there are certain limitations to how you can use this behavior. See the Object Delivery documentation for more information.

Option	Type	Description
enabled	boolean	Enables the quick retry feature.

dynamicThroughtputOptimizationOverride

- **Property Manager name**: Quick Retry Override
- **Behavior version**: The `v2023-05-30` rule format supports the `dynamicThroughtputOptimizationOverride` behavior v1.1.
- **Rule format status**: Deprecated, outdated rule format
- **Access**: Read-only
- **Allowed in includes**: Yes

This overrides the default threshold of 5 Mbps that triggers the `dynamicThroughtputOptimization` behavior, which enables the quick retry feature. Quick retry detects slow forward throughput while fetching an object, and attempts a different forward connection path to avoid congestion. This behavior can only be configured on your behalf by Akamai Professional Services.

Option	Type	Description
throughput	string	Specifies the default target forward throughput in Mbps, ranging from 2 to 50 Mbps. If this time is exceeded during a connection attempt, quick retry is enabled and a different forward connection path is used.

dynamicWebContent

- **Property Manager name**: [Content Characteristics - Dynamic Web Content](#)
- **Behavior version**: The `v2023-05-30` rule format supports the `dynamicWebContent` behavior v1.1.
- **Rule format status**: [Deprecated, outdated rule format](#)
- **Access**: [Read-write](#)
- **Allowed in includes**: [Yes](#)

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.
realUser Monitoring	boolean	Allows Real User Monitoring (RUM) to collect performance data for subcustomer content. See the `realUser Monitoring` behavior for more information.
image Compression	boolean	Enables image compression for subcustomer content.

ecmsBulkUpload

- **Property Manager name**: [Message Store bulk upload](#)
- **Behavior version**: The `v2023-05-30` rule format supports the `ecmsBulkUpload` behavior v1.0.
- **Rule format status**: [Deprecated, outdated rule format](#)
- **Access**: [Read-write](#)
- **Allowed in includes**: [No (temporarily)](#)

Uploads a ZIP archive with objects to an existing data set. The target data set stores objects as key-value pairs. The path to an object in the ZIP archive is a key, and the content of an object is a value. For an overview, see `ecms Database`.

Option	Type	Description
enabled	boolean	Enables sending a compressed archive file with objects. Sends the archive file to the default path of the target data set: `<hostname>/bulk/<database_name>/<dataset_name>` .

ecmsDatabase

- **Property Manager name**: [Message Store database selection](#)
- **Behavior version**: The `v2023-05-30` rule format supports the `ecmsDatabase` behavior v1.0.
- **Rule format status**: [Deprecated, outdated rule format](#)
- **Access**: [Read-write](#)
- **Allowed in includes**: [No (temporarily)](#)

Edge Connect Message Store is available for [Internet of Things: Edge Connect](#) users. It lets you create databases and data sets within these databases. You can use this object store to save files smaller than 2 GB. `ecmsDatabase` specifies a default database for requests to this property, unless indicated otherwise in the URL. To access objects in the default database, you can skip its name in the URLs. To access objects in a different database, pass its name in the header, query parameter, or a regular expression matching a URL segment. You can also configure the `ecms Dataset` behavior to specify a default data set for requests.

Option	Type	Description	Requires
database	string	Specifies a default database for this property. If you don't configure a default data set in the `ecmsDataset` behavior, requests to objects in this database follow the pattern: `<hostname>/datastore/<data_set_name>/<object_key>`.	
extractLocation	enum	Specifies where to pass a database name in requests. If the specified location doesn't include the database name or the name doesn't match the regular expression, the default database is used.	
	`CLIENT_REQUEST_HEADER`	Name is a request header.	
	`QUERY_STRING`	Name is a query parameter.	
	`REGEX`	Name matches the URL.	
headerName	string	Specifies the request header that passed the database name. By default, it points to `X-KV-Database`.	`extractLocation` is `CLIENT_REQUEST_HEADER`
queryParameterName	string	Specifies the query string parameter that passed the database name. By default, it points to `database`.	`extractLocation` is `QUERY_STRING`
regexPattern	string	Specifies the regular expression that matches the database name in the URL.	`extractLocation` is `REGEX`

ecmsDataset

- **Property Manager name**: [Message Store data set selection](#)⟶
- **Behavior version**: The `v2023-05-30` rule format supports the `ecmsDataset` behavior v1.0.
- **Rule format status**: [Deprecated, outdated rule format](#)
- **Access**: [Read-write](#)
- **Allowed in includes**: [No (temporarily)](#)

Specifies a default data set for requests to this property unless indicated otherwise in the URL. To access objects in this data set, you can skip the data set name in the URLs. To access objects in a different data set within a database, pass the data set name in the header, query parameter, or a regular expression pattern matching a URL segment. You can also configure the `ecmsDatabase` behavior to specify a default database for requests.

Option	Type	Description	Requires
dataset	string	Specifies a default data set for this property. If you don't configure a default database in the `ecmsDatabase` behavior, requests to objects in this data set follow the pattern: `<hostname>/datastore/<database_name>/<object_key>`.	
extractLocation	enum	Specifies where to pass a data set name in requests. If the specified location doesn't include the data set name or the name doesn't match the regular expression pattern, the default data set is used.	
	CLIENT_REQUEST_HEADER	Name is a request header.	
	QUERY_STRING	Name is a query parameter.	
	REGEX	Name matches the URL.	
headerName	string	Specifies the request header that passed the data set name. By default, it points to `X-KV-Dataset`.	extractLocation is CLIENT_REQUEST_HEADER
queryParameterName	string	Specifies the query string parameter that passed the data set name. By default, it points to `dataset`.	extractLocation is QUERY_STRING
regexPattern	string	Specifies the regular expression that matches the data set name in the URL.	extractLocation is REGEX

ecmsObjectKey

- **Property Manager name**: [Message Store object key selection](#)⟶

- **Behavior version**: The `v2023-05-30` rule format supports the `ecmsObjectKey` behavior v1.0.
- **Rule format status**: Deprecated, outdated rule format
- **Access**: Read-write
- **Allowed in includes**: No (temporarily)

Defines a regular expression to match object keys in custom URLs and to access objects in a data set. You can point custom URLs to access proper values in the target data set. For an overview, see `ecmsDatabase` .

Option	Type	Description
regex	string	Enables sending a compressed archive file with objects to the default path of the target data set: `<hostname>/bulk/<database_name>/<dataset_name>` .

edgeConnect

- **Property Manager name**: Cloud Monitor Instrumentation
- **Behavior version**: The `v2023-05-30` rule format supports the `edgeConnect` behavior v1.2.
- **Rule format status**: Deprecated, outdated rule format
- **Access**: Read-write
- **Allowed in includes**: Yes

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 DEFAULT	
apiDataElements	string array	Specifies the data set to log.	
		Supported values: APM NETWORK_PERFORMANCE GEO NETWORK_V1 HTTP REQUEST_HEADER	
destinationHostname	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

Option	Type	Description	Requires
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

edgeLoadBalancingAdvanced

- **Property Manager name**: Edge Load Balancing: Advanced Metadata
- **Behavior version**: The v2023-05-30 rule format supports the edgeLoadBalancingAdvanced behavior v1.0.
- **Rule format status**: Deprecated, outdated rule format
- **Access**: Read-only
- **Allowed in includes**: No (temporarily)

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 xml block does.
xml	string	A block of Akamai XML metadata.

edgeLoadBalancingDataCenter

- **Property Manager name**: Edge Load Balancing: Data Center
- **Behavior version**: The v2023-05-30 rule format supports the edgeLoadBalancingDataCenter behavior v1.2.
- **Rule format status**: Deprecated, outdated rule format
- **Access**: Read-write
- **Allowed in includes**: No (temporarily)

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 `id` specified by the `edgeLoadBalancingOrigin` 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.	
cookieName	string	If using session persistence, this specifies the value of the cookie named in the corresponding `edgeLoadBalancingOrigin` behavior's `cookie_name` option.	
enableFailover	boolean	Allows you to specify failover rules.	
ip	string	Specifies this data center's IP address.	`enableFailover` is true
failoverRules	object array	Provides up to four failover rules to apply in the specified order.	`enableFailover` is true
failoverRules[].failoverHostname	string	The hostname of the data center to fail over to.	
failoverRules[].modifyRequest	boolean	Allows you to modify the request's hostname or path.	
failoverRules[].overrideHostname	boolean	Overrides the request's hostname with the `failover_hostname`.	`modifyRequest` is true
failoverRules[].contextRoot	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 `/static/error.html` when failing over to an error page.	`modifyRequest` is true
failoverRules[].absolutePath	boolean	When enabled, interprets the path specified by `context_root` as an absolute server path, for example to reference a site-down page. Otherwise when disabled, the path is appended to the request.	`modifyRequest` is true

edgeLoadBalancingOrigin

- **Property Manager name**: [Edge Load Balancing: Origin Definition](#)
- **Behavior version**: The `v2023-05-30` rule format supports the `edgeLoadBalancingOrigin` behavior v1.2.
- **Rule format status**: [Deprecated, outdated rule format](#)
- **Access**: [Read-write](#)
- **Allowed in includes**: [No (temporarily)](#)

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
id	string	Specifies a unique descriptive string for this ELB origin. The value needs to match the `origin_id` specified by the `edgeLoadBalancingDataCenter` 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 `edgeLoadBalancingDataCenter` behavior's `description` option specifies the cookie's value.	enableSession Persistence is true

edgeOriginAuthorization

- **Property Manager name**: Edge Server Identification
- **Behavior version**: The `v2023-05-30` rule format supports the `edgeOriginAuthorization` behavior v1.1.
- **Rule format status**: Deprecated, outdated rule format
- **Access**: Read-write
- **Allowed in includes**: Yes

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 `Host` header the origin server receives.

edgeRedirector

- **Property Manager name**: [Edge Redirector Cloudlet](#)
- **Behavior version**: The `v2023-05-30` rule format supports the `edgeRedirector` behavior v4.0.
- **Rule format status**: [Deprecated, outdated rule format](#)
- **Access**: [Read-write](#)
- **Allowed in includes**: [No (temporarily)](#)

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	Requires
enabled	boolean	Enables the Edge Redirector Cloudlet.	
isShared Policy	boolean	Whether you want to apply the Cloudlet shared policy to an unlimited number of properties within your account. Learn more about shared policies and how to create them in [Cloudlets Policy Manager](#).	
cloudlet Policy	object	Specifies the Cloudlet policy as an object.	isShared Policy is false
cloudlet Policy.id	number	Identifies the Cloudlet.	
cloudlet Policy.name	string	The Cloudlet's descriptive name.	
cloudlet Shared Policy	string	Identifies the Cloudlet shared policy to use with this behavior. Use the [Cloudlets API](#) to list available shared policies.	isShared Policy is true

edgeScape

- **Property Manager name**: [Content Targeting (EdgeScape)](#)
- **Behavior version**: The `v2023-05-30` rule format supports the `edgeScape` behavior v1.1.
- **Rule format status**: [Deprecated, outdated rule format](#)
- **Access**: [Read-write](#)
- **Allowed in includes**: [Yes](#)

[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 `X-Akamai-Edgescape` request header to the origin.

edgeSideIncludes

- **Property Manager name**: [ESI (Edge Side Includes)](#)
- **Behavior version**: The `v2023-05-30` rule format supports the `edgeSideIncludes` behavior v1.3.
- **Rule format status**: [Deprecated, outdated rule format](#)
- **Access**: [Read-write](#)
- **Allowed in includes**: [Yes](#)

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](#)
enabled	boolean	Enables ESI processing.	
enableVia Http	boolean	Enable ESI only for content featuring the `Edge-control: dca=esi` HTTP response header.	
passSet Cookie	boolean	Allows edge servers to pass your origin server's cookies to the ESI processor.	`enableViaHttp` is true
passClient Ip	boolean	Allows edge servers to pass the client IP header to the ESI processor.	`enableViaHttp` is true
i18nStatus	boolean	Provides internationalization support for ESI.	`enableViaHttp` is true
i18n Charset	string array	Specifies the character sets to use when transcoding the ESI language, `UTF-8` and `ISO-8859-1` for example.	`i18nStatus` is true
detect Injection	boolean	Denies attempts to inject ESI code.	

edgeWorker

- **Property Manager name**: [EdgeWorkers](#)
- **Behavior version**: The `v2023-05-30` rule format supports the `edgeWorker` behavior v1.7.
- **Rule format status**: [Deprecated, outdated rule format](#)
- **Access**: [Read-write](#)
- **Allowed in includes**: [Yes](#)

[EdgeWorkers](#) are JavaScript applications that allow you to manipulate your web traffic on edge servers outside of Property Manager behaviors, and deployed independently from your configuration's logic. This behavior applies an EdgeWorker to a set of edge requests.

Option	Type	Description
enabled	boolean	When enabled, applies specified EdgeWorker functionality to this rule's web traffic.
edgeWorker Id	string	Identifies the EdgeWorker application to apply to this rule's web traffic. You can use the [EdgeWorkers API](#) to get this value.

enhancedAkamaiProtocol

- **Property Manager name**: [Enhanced Akamai Protocol](#)
- **Behavior version**: The `v2023-05-30` rule format supports the `enhancedAkamaiProtocol` behavior v1.1.
- **Rule format status**: [Deprecated, outdated rule format](#)
- **Access**: [Read-write](#)
- **Allowed in includes**: [Yes](#)

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.

enhancedProxyDetection

- **Property Manager name**: [Enhanced Proxy Detection with GeoGuard](#)

- **Behavior version**: The `v2023-05-30` rule format supports the `enhancedProxyDetection` behavior v1.2.
- **Rule format status**: Deprecated, outdated rule format
- **Access**: Read-write
- **Allowed in includes**: Yes

Enhanced Proxy Detection (EPD) leverages the GeoGuard service provided by GeoComply to add proxy detection and location spoofing protection. It identifies requests for your content that have been redirected from an unwanted source through a proxy. You can then allow, deny, or redirect these requests.

Include this behavior in the same rule as `epdForwardHeaderEnrichment`. The `epdForwardHeaderEnrichment` behavior sends the Enhanced Proxy Detection (`Akamai-EPD`) header in the forward request to determine whether the connecting IP address is an anonymous proxy.

Option	Type	Description	Requires
enabled	boolean	Applies GeoGuard proxy detection.	
forward Header Enrichment	boolean	Whether the Enhanced Proxy Detection (Akamai-EPD) header is included in the forward request to mark a connecting IP address as an anonymous proxy, with a two-letter designation. See the `epdForwardHeaderEnrichment` behavior for details.	
enable Configuration Mode	enum	Specifies how to field the proxy request.	
	BEST_PRACTICE	GeoComply maintains a fixed list of categories for their GeoGuard service. Select this mode to automatically apply their primary, "must-have" categories for proxy detection.	
	ADVANCED	Use this mode to selectively apply GeoGuard categories ⏎ and customize the applied action. Make sure you include at least the categories GeoGuard considers "must-have." Akamai can't guarantee optimal proxy protection if you leave them out.	
bestPractice Action	enum	Specifies how to field the proxy request.	enable Configuration Mode is BEST_ PRACTICE
	ALLOW	Allow the request.	
	DENY	Deny the request.	
	REDIRECT	Respond with a redirect.	
bestPractice Redirecturl	string (allows variables)	This specifies the URL to which to redirect requests.	bestPractice Action is REDIRECT
detect Anonymous Vpn	boolean	This enables detection of requests from anonymous VPNs.	enable Configuration Mode is ADVANCED
detect Anonymous VpnAction	enum	Specifies how to field anonymous VPN requests.	detect Anonymous Vpn is true
	ALLOW	Allow the request.	
	DENY	Deny the request.	
	REDIRECT	Respond with a redirect.	
detect Anonymous Vpn Redirecturl	string (allows variables)	This specifies the URL to which to redirect anonymous VPN requests.	detect Anonymous VpnAction is REDIRECT

Option	Type	Description	Requires
detectPublic Proxy	boolean	This enables detection of requests from public proxies.	enable Configuration Mode is ADVANCED
detectPublic ProxyAction	enum	Specifies how to field public proxy requests.	detectPublic Proxy is true
	ALLOW	Allow the request.	
	DENY	Deny the request.	
	REDIRECT	Respond with a redirect.	
detectPublic Proxy Redirecturl	string (allows variables)	This specifies the URL to which to redirect public proxy requests.	detectPublic ProxyAction is REDIRECT
detectTor ExitNode	boolean	This enables detection of requests from Tor exit nodes.	enable Configuration Mode is ADVANCED
detectTor ExitNode Action	enum	This specifies whether to DENY , ALLOW , or REDIRECT requests from Tor exit nodes.	detectTorExit Node is true
	ALLOW	Allow the request.	
	DENY	Deny the request.	
	REDIRECT	Respond with a redirect.	
detectTor ExitNode Redirecturl	string (allows variables)	This specifies the URL to which to redirect requests from Tor exit nodes.	detectTorExit NodeAction is REDIRECT
detectSmart DNSProxy	boolean	This enables detection of requests from smart DNS proxies.	enable Configuration Mode is ADVANCED
detectSmart DNSProxy Action	enum	Specifies whether to DENY , ALLOW , or REDIRECT smart DNS proxy requests.	detectSmart DNSProxy is true
	ALLOW	Allow the request.	
	DENY	Deny the request.	
	REDIRECT	Respond with a redirect.	
detectSmart DNSProxy Redirecturl	string (allows variables)	This specifies the URL to which to redirect DNS proxy requests.	detectSmart DNSProxy Action is REDIRECT
detect Hosting Provider	boolean	This detects requests from a hosting provider.	enable Configuration Mode is ADVANCED
detect Hosting Provider Action	enum	This specifies whether to DENY , ALLOW , or REDIRECT requests from hosting providers.	detect Hosting Provider is true
	ALLOW	Allow the request.	
	DENY	Deny the request.	

Option	Type	Description	Requires
	`REDIRECT`	Respond with a redirect.	
detect Hosting Provider Redirecturl	string (allows [variables](#))	This specifies the absolute URL to which to redirect requests from hosting providers.	detect Hosting Provider Action is `REDIRECT`
detectVpn DataCenter	boolean	This enables detection of requests from VPN data centers.	enable Configuration Mode is `ADVANCED`
detectVpn DataCenter Action	enum	This specifies whether to `DENY`, `ALLOW`, or `REDIRECT` requests from VPN data centers.	detectVpn DataCenter is `true`
	`ALLOW`	Allow the request.	
	`DENY`	Deny the request.	
	`REDIRECT`	Respond with a redirect.	
detectVpn DataCenter Redirecturl	string (allows [variables](#))	This specifies the URL to which to redirect requests from VPN data centers.	detectVpn DataCenter Action is `REDIRECT`
detect Residential Proxy	boolean	This enables detection of requests from a residential proxy. See [Enhanced Proxy Detection with GeoGuard](#) and learn more about this GeoGuard category before enabling it.	enable Configuration Mode is `ADVANCED`
detect Residential ProxyAction	enum	This specifies whether to `DENY`, `ALLOW`, or `REDIRECT` requests from residential proxies.	detect Residential Proxy is `true`
	`ALLOW`	Allow the request.	
	`DENY`	Deny the request.	
	`REDIRECT`	Respond with a redirect.	
detect Residential Proxy Redirecturl	string (allows [variables](#))	This specifies the URL to which to redirect requests.	detect Residential ProxyAction is `REDIRECT`

epdForwardHeaderEnrichment

- **Property Manager name**: [Enhanced Proxy Detection with GeoGuard - Forward Header Enrichment](#)
- **Behavior version**: The `v2023-05-30` rule format supports the `epdForwardHeaderEnrichment` behavior v1.0.
- **Rule format status**: [Deprecated, outdated rule format](#)
- **Access**: [Read-write](#)
- **Allowed in includes**: [Yes](#)

This behavior identifies unwanted requests from an anonymous proxy. This and the enhancedProxyDetection behavior work together and need to be included either in the same rule, or in the default one.

Option	Type	Description
enabled	boolean	Sends the Enhanced Proxy Detection (Akamai-EPD) header in the forward request to determine whether the connecting IP address is an anonymous proxy. The header can contain one or more two-letter codes that indicate the IP address type detected by edge servers: • av for is_anonymous_vpn • hp for is_hosting_provider • pp for is_public_proxy • dp for is_smart_dns_proxy • tn for is_tor_exit_node • vc for is_vpn_datacentre • rp for is_residential_proxy

failAction

- **Property Manager name**: Site Failover
- **Behavior version**: The v2023-05-30 rule format supports the failAction behavior v1.7.
- **Rule format status**: Deprecated, outdated rule format
- **Access**: Read-write
- **Allowed in includes**: Yes

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 , modify Protocol , and protocol .)	
	RECREATED_CO	Serves alternate content from your network. (Use with these options: content Hostname , 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 , net StoragePath , 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 .)	

Option	Type	Description	Requires
saasType	enum	Identifies the component of the request that identifies the SaaS dynamic fail action.	`actionType` is `DYNAMIC`
		Supported values: COOKIE HOSTNAME	
saasCname Enabled	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.	`saasCname Enabled` 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.	
dynamicCustom Path	boolean	Allows you to modify the original requested path.	`actionType` is `DYNAMIC`
dynamicPath	string (allows [variables](#))	Specifies the new path.	`dynamic CustomPath` is `true`
redirectHostname Type	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.	`redirect HostnameType` is `ALTERNATE`
redirectCustom Path	boolean	Uses the `redirectPath` to customize a new path.	`actionType` is `REDIRECT`
redirectPath	string (allows [variables](#))	Specifies a new path.	`redirectCustom Path` 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`

Option	Type	Description	Requires
contentCustom Path	boolean	Specifies a custom redirect path.	`actionType` is `RECREATED_CO`
contentPath	string (allows [variables](#))	Specifies a custom redirect path.	`contentCustom Path` is `true`
netStorage Hostname	object	When the `actionType` is `RECREATED_NS`, specifies the [NetStorage](#) origin to serve the alternate content. Contact Akamai Professional Services for your NetStorage origin's `id`.	`actionType` is `RECREATED_NS`
netStorage Hostname.cpCode	integer	Identifies a CP code assigned to this storage group.	
netStorage Hostname.download DomainName	string	Domain name from which content can be downloaded.	
netStorage Hostname.g2o Token	string	Signature Header Authentication key.	
netStorage Hostname.id	integer	Unique identifier for the storage group.	
netStorage Hostname.name	string	Name of the storage group.	
netStoragePath	string (allows [variables](#))	When the `actionType` is `RECREATED_NS`, specifies the path for the [NetStorage](#) request.	`actionType` is `RECREATED_NS`
cexHostname	string (allows [variables](#))	Specifies a hostname.	`actionType` is `RECREATED_CEX`
cexCustomPath	boolean	Specifies a custom path.	`actionType` is `RECREATED_CEX`
cexPath	string (allows [variables](#))	Specifies a custom path.	`cexCustom Path` is `true`
cpCode	object	Specifies a CP code for which to log errors for the NetStorage location. You only need to provide the initial `id`, stripping any `cpc_` [prefix](#) to pass the integer to the rule tree. Additional CP code details may reflect back in subsequent read-only data.	`actionType` is `RECREATED_NS`
cpCode.cpCode Limits	array	**Read-only**. Describes the current usage limit for the CP code.	
cpCode.created Date	integer	**Read-only**. UNIX epoch timestamp reflecting when the CP code was originally created.	
cp Code.description	string	**Read-only**. Additional description for the CP code.	
cpCode.id	integer	Unique identifier for each CP code. Initially, you get this value when [creating a new CP code](#) in PAPI. You can also assign a `cpcodeId` value from the [List CP codes](#) operation.	
cpCode.name	string	**Read-only**. The name of the CP code you specify as the `cpcodeName` when [creating a new CP code](#) in PAPI. You can modify this value with the [PUT operation](#) in the CP codes and Reporting Groups API.	
cpCode.products	array	**Read-only**. The set of products the CP code is assigned to. This reflects `productId` values you specify when [creating a new CP code](#) in PAPI.	
statusCode	enum	Assigns a new HTTP status code to the failure response.	`actionType` is `RECREATED_NS`

Option	Type	Description	Requires
		Supported values: 100 102 122 201 203 205 207 400 402 404 406 408 410 412 101 103 200 202 204 206 226 401 403 405 407 409 411 413	
preserveQuery String	boolean	When using either `contentCustomPath`, `cexCustomPath`, `dynamicCustomPath`, or `redirectCustomPath` to specify a custom path, enabling this passes in the original request's query string as part of the path.	`contentCustom Path` is `true` OR `cexCustom Path` is `true` OR `redirect CustomPath` is `true` OR `dynamic CustomPath` is `true`
modifyProtocol	boolean	Modifies the redirect's protocol using the value of the `protocol` field.	`actionType` is `REDIRECT` OR `dynamic Method` is either: `SERVE_301`, `SERVE_302`
protocol	enum	When the `actionType` is `REDIRECT` and `modifyProtocol` is enabled, this specifies the redirect's protocol.	`modifyProtocol` is `true`
		Supported values: HTTP HTTPS	

failoverBotManagerFeatureCompatibility

- **Property Manager name**: Security Failover Feature Compatibility
- **Behavior version**: The `v2023-05-30` rule format supports the `failoverBotManagerFeatureCompatibility` behavior v1.0.
- **Rule format status**: [Deprecated, outdated rule format](#)
- **Access**: [Read-write](#)
- **Allowed in includes**: [Yes](#)

Ensures that functionality such as challenge authentication and reset protocol work with a failover product property you use to create an alternate hostname. Apply it to any properties that implement a failover under the Cloud Security Failover product.

Option	Type	Description
compatibility	boolean	This behavior does not include any options. Specifying the behavior itself enables it.

fastInvalidate

- **Property Manager name**: [Fast Invalidate (Safe to remove)](#)
- **Behavior version**: The `v2023-05-30` rule format supports the `fastInvalidate` behavior v1.0.
- **Rule format status**: [Deprecated, outdated rule format](#)
- **Access**: [Read-write](#)
- **Allowed in includes**: [Yes](#)

This behavior is deprecated, but you should not disable or remove it if present.

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 `v2023-05-30` rule format supports the `firstPartyMarketing` behavior v1.0.
- **Rule format status**: [Deprecated, outdated rule format](#)
- **Access**: [Read-write](#)
- **Allowed in includes**: [No (temporarily)](#)

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.	

Option	Type	Description	Requires
	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 `/mmath`, and the request is for `www.example.com/dir`, the new URL is `www.example.com/mmath/dir`.	

firstPartyMarketingPlus

- **Property Manager name**: Cloud Marketing Plus Cloudlet (Beta)
- **Behavior version**: The `v2023-05-30` rule format supports the `firstPartyMarketingPlus` behavior v1.0.
- **Rule format status**: Deprecated, outdated rule format
- **Access**: Read-write
- **Allowed in includes**: No (temporarily)

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

Option	Type	Description	Requires
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 `/mmath` , and the request is for `www.example.com/dir` , the new URL is `www.example.com/mmath/dir` .	

forwardRewrite

- **Property Manager name**: Forward Rewrite Cloudlet
- **Behavior version**: The `v2023-05-30` rule format supports the `forwardRewrite` behavior v4.0.
- **Rule format status**: Deprecated, outdated rule format
- **Access**: Read-write
- **Allowed in includes**: No (temporarily)

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	Requires
enabled	boolean	Enables the Forward Rewrite Cloudlet behavior.	
isShared Policy	boolean	Whether you want to use a shared policy for a Cloudlet. Learn more about shared policies and how to create them in Cloudlets Policy Manager.	
cloudlet Policy	object	Identifies the Cloudlet policy.	isShared Policy is false
cloudlet Policy.id	number	Identifies the Cloudlet.	
cloudlet Policy.name	string	The Cloudlet's descriptive name.	
cloudlet SharedPolicy	string	This identifies the Cloudlet shared policy to use with this behavior. You can list available shared policies with the Cloudlets API.	isShared Policy is true

g2oheader

- **Property Manager name**: [Signature Header Authentication](#)
- **Behavior version**: The `v2023-05-30` rule format supports the `g2oheader` behavior v1.1.
- **Rule format status**: [Deprecated, outdated rule format](#)
- **Access**: [Read-write](#)
- **Allowed in includes**: [Yes](#)

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
enabled	boolean	Enables the g2o verification behavior.	
data Header	string	Specifies the name of the header that contains the request data that needs to be encrypted.	
signed Header	string	Specifies the name of the header containing encrypted request data.	
encoding Version	enum	Specifies the version of the encryption algorithm as an integer from `1` through `5`.	
		Supported values: 1 2 3 4 5	
useCustom SignString	boolean	When disabled, the encrypted string is based on the forwarded URL. If enabled, you can use `customSignString` to customize the set of data to encrypt.	
custom SignString	string array	Specifies the set of data to be encrypted as a combination of concatenated strings.	useCustomSign String `is` `true`
	AK_METHOD	Incoming request method.	
	AK_SCHEME	Incoming request scheme (HTTP or HTTPS).	
	AK_ HOSTHEADER	Incoming request hostname.	
	AK_DOMAIN	Incoming request domain.	
	AK_URL	Incoming request URL.	
	AK_PATH	Incoming request path.	
	AK_QUERY	Incoming request query string.	
	AK_ FILENAME	Incoming request filename.	
	AK_ EXTENSION	Incoming request filename extension.	
	AK_CLIENT_ REAL_IP	Incoming client IP.	
secretKey	object array	Specifies the shared secret key.	
nonce	string	Specifies the cryptographic *nonce* string.	

globalRequestNumber

- **Property Manager name**: Global Request Number
- **Behavior version**: The `v2023-05-30` rule format supports the `globalRequestNumber` behavior v1.0.
- **Rule format status**: Deprecated, outdated rule format
- **Access**: Read-write
- **Allowed in includes**: Yes

Generates a unique identifier for each request on the Akamai edge network, for use in logging and debugging. GRN identifiers follow the same format as Akamai's error reference strings, for example: `0.05313217.1567801841.1457a3`. You can use the Edge Diagnostics API's Translate error string operation to get low-level details about any request.

Option	Type	Description	Requires
output Option	enum	Specifies how to report the GRN value.	
	`RESPONSE_ HEADER`	Use a response header.	
	`REQUEST_ HEADER`	Use a request header.	
	`BOTH_ HEADERS`	Use both headers.	
	`ASSIGN_ VARIABLE`	Process the value in some other way as a variable.	
header Name	string	With `outputOption` set to specify any set of headers, this specifies the name of the header to report the GRN value.	`outputOption` is either: `RESPONSE_ HEADER`, `REQUEST_HEADER`, `BOTH_ HEADERS`
variable Name	string (variable name)	This specifies the name of the variable to assign the GRN value to. You need to pre-declare any variable you specify within the rule tree.	`outputOption` is `ASSIGN_VARIABLE`

graphqlCaching

- **Property Manager name**: GraphQL Caching
- **Behavior version**: The `v2023-05-30` rule format supports the `graphqlCaching` behavior v1.1.
- **Rule format status**: Deprecated, outdated rule format
- **Access**: Read-write
- **Allowed in includes**: Yes

This behavior configures how to cache GraphQL-based API traffic. Enable `caching` for your GraphQL API traffic, along with `allowPost` to cache POST responses. To configure REST API traffic, use the `rapid` behavior.

Option	Type	Description
enabled	boolean	Enables GraphQL caching.
cacheResponses WithErrors	boolean	When enabled, caches responses that include an `error` field at the top of the response body object. Disable this if your GraphQL server yields temporary errors with success codes in the 2xx range.
postRequest ProcessingError Handling	enum	Specify what happens if GraphQL query processing fails on POST requests.
	APPLY_ CACHING_ BEHAVIOR	If your GraphQL server does not allow mutations and subscriptions, this offloads requests.
	NO_STORE	Pass requests to the origin.
operationsUrl QueryParameter Name	string	Specifies the name of a query parameter that identifies requests as GraphQL queries.
operationsJson BodyParameter Name	string	The name of the JSON body parameter that identifies GraphQL POST requests.

gzipResponse

- **Property Manager name**: Last Mile Acceleration (Gzip Compression)
- **Behavior version**: The `v2023-05-30` rule format supports the `gzipResponse` behavior v1.2.
- **Rule format status**: Deprecated, outdated rule format
- **Access**: Read-write
- **Allowed in includes**: Yes

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
behavior	enum	Specify when to compress responses.
	ORIGIN_RESPONSE	Compress for clients that send an `Accept-Encoding: gzip` header.
	ALWAYS	Always compress.
	NEVER	Never compress.

hdDataAdvanced

- **Property Manager name**: HD Data Override: Advanced Metadata
- **Behavior version**: The `v2023-05-30` rule format supports the `hdDataAdvanced` behavior v1.0.
- **Rule format status**: Deprecated, outdated rule format
- **Access**: Read-only
- **Allowed in includes**: Yes

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
description	string	Human-readable description of what the XML block does.
xml	string	A block of Akamai XML metadata.

healthDetection

- **Property Manager name**: Origin Health Detection
- **Behavior version**: The `v2023-05-30` rule format supports the `healthDetection` behavior v1.1.
- **Rule format status**: Deprecated, outdated rule format
- **Access**: Read-write
- **Allowed in includes**: Yes

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
retryCount	number	The number of consecutive connection failures that mark an IP address as faulty.

Option	Type	Description
retry Interval	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.
maximum Reconnects	number	Specifies the maximum number of times the edge server will contact your origin server. If your origin is associated with several IP addresses, `maximumReconnects` effectively overrides the value of `retryCount`.

hsafEipBinding

- **Property Manager name**: [HSAF for Edge IP Binding](#)
- **Behavior version**: The `v2023-05-30` rule format supports the `hsafEipBinding` behavior v1.0.
- **Rule format status**: [Deprecated, outdated rule format](#)
- **Access**: [Read-only](#)
- **Allowed in includes**: [No (temporarily)](#)

Edge IP Binding works with a limited set of static IP addresses to distribute your content, which can be limiting in large footprint environments. This behavior sets Hash Serial and Forward (HSAF) for Edge IP Binding to deal with larger footprints. It can only be configured on your behalf by Akamai Professional Services. For more information, see the [Edge IP Binding documentation](#).

Option	Type	Description	Requires
enabled	boolean	Enables HSAF for Edge IP Binding customers with a large footprint.	
custom Extracted Serial	boolean	Whether to pull the serial number from the variable value set in the `advanced` behavior. Work with your Akamai Services team to add the `advanced` behavior earlier in your property to extract and apply the `AKA_PM_EIP_HSAF_SERIAL` variable.	
hashMin Value	number	Specifies the minimum value for the HSAF hash range, from 2 through 2045. This needs to be lower than `hashMaxValue`.	custom Extracted Serial is false
hashMax Value	number	Specifies the maximum value for the hash range, from 3 through 2046. This needs to be higher than `hashMinValue`.	custom Extracted Serial is false
tier	enum	Specifies where the behavior is applied.	
	EDGE	Applies Hash Serial and Forward only at edge regions.	
	PARENT	Applies Hash Serial and Forward using tiers. For more details, see the [Edge IP Binding documentation](#).	
	BOTH	Applies Hash Serial and Forward in both environments.	

http2

- **Property Manager name**: [HTTP/2](#)
- **Behavior version**: The `v2023-05-30` rule format supports the `http2` behavior v1.0.
- **Rule format status**: [Deprecated, outdated rule format](#)
- **Access**: [Read-write](#)
- **Allowed in includes**: [No (temporarily)](#)

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.

http3

- **Property Manager name**: [HTTP/3](#)
- **Behavior version**: The `v2023-05-30` rule format supports the `http3` behavior v1.0.
- **Rule format status**: [Deprecated, outdated rule format](#)
- **Access**: [Read-write](#)
- **Allowed in includes**: [No (temporarily)](#)

This enables the HTTP/3 protocol that uses QUIC. The behavior allows for improved performance and faster connection setup. You can only apply this behavior if the property is marked as secure. See [Secure property requirements](#) and the [Property Manager documentation](#) for guidance.

If you want all requests processed by a property to support HTTP/3 for transfer, add the behavior to the default rule. If you add the behavior to a custom rule, use it with the `bucket` match so that it applies to a specific percentage of the HTTP/3 requests.

Option	Type	Description
enable	boolean	This enables HTTP/3 connections between requesting clients and Akamai edge servers. You also need to enable QUIC and TLS 1.3 in your certificate deployment settings. See the [Property Manager documentation](#) for more details.

httpStrictTransportSecurity

- **Property Manager name**: HTTP Strict Transport Security (HSTS)
- **Behavior version**: The `v2023-05-30` rule format supports the `httpStrictTransportSecurity` behavior v1.0.
- **Rule format status**: Deprecated, outdated rule format
- **Access**: Read-write
- **Allowed in includes**: No (temporarily)

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

httpToHttpsUpgrade

- **Property Manager name**: [HTTP to HTTPS Upgrade](#)
- **Behavior version**: The `v2023-05-30` rule format supports the `httpToHttpsUpgrade` behavior v1.0.
- **Rule format status**: [Deprecated, outdated rule format](#)
- **Access**: [Read-write](#)
- **Allowed in includes**: [Yes](#)

Upgrades an HTTP edge request to HTTPS for the remainder of the request flow. Enable this behavior only if your origin supports HTTPS, and if your `origin` behavior is configured with `originCertsToHonor` to verify SSL certificates.

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

inputValidation

- **Property Manager name**: [Input Validation Cloudlet](#)
- **Behavior version**: The `v2023-01-05` rule format supports the `inputValidation` behavior v1.5.
- **Rule format status**: [Deprecated, outdated rule format](#)
- **Access**: [Read-write](#)
- **Allowed in includes**: [No (temporarily)](#)

This behavior is deprecated, but you should not disable or remove it if present.

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.	
cloudlet Policy.name	string	The Cloudlet's descriptive name.	
label	string	Distinguishes this Input Validation policy from any others within the same property.	
user IdentificationBy Cookie	boolean	When enabled, identifies users by the value of a cookie.	

Option	Type	Description	Requires
user IdentificationKey Cookie	string	This specifies the cookie name whose value needs to remain constant across requests to identify a user.	`userIdentificationBy Cookie` is `true`
user IdentificationBy Ip	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.	
user IdentificationBy Headers	boolean	When enabled, identifies users by specific HTTP headers on GET or POST requests.	
user IdentificationKey Headers	string array	This specifies the HTTP headers whose combined set of values identify each end user.	`userIdentificationBy Headers` is `true`
user IdentificationBy Params	boolean	When enabled, identifies users by specific query parameters on GET or POST requests.	
user IdentificationKey Params	string array	This specifies the query parameters whose combined set of values identify each end user.	`userIdentificationBy Params` is `true`
allowLargePost Body	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 `penaltyThreshold` counter to zero. Otherwise, even those series of invalid requests that are interrupted by valid requests may trigger the `penaltyAction`.	
validateOnOrigin With	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.	
validateOnOrigin HeaderName	string	If `validateOnOriginWith` is set to `RESPONSE_CODE_AND_HEADER`, this specifies the header name for a request that the origin identifies as invalid.	`validateOnOriginWith` is `RESPONSE_CODE_ AND_HEADER`
validateOnOrigin HeaderValue	string	If `validateOnOriginWith` is set to `RESPONSE_CODE_AND_HEADER`, this specifies an invalid request's header value that corresponds to the `validateOnOriginHeader Name`.	`validateOnOriginWith` is `RESPONSE_CODE_ AND_HEADER`
validateOnOrigin ResponseCode	number	Unless `validateOnOriginWith` is `DISABLED`, this identifies the integer response code for requests the origin identifies as invalid.	`validateOnOriginWith` is either: `RESPONSE_ CODE`, `RESPONSE_ CODE_AND_HEADER`
failure302Uri	string	Specifies the redirect link for invalid requests that have not yet triggered a penalty.	
penalty Threshold	number	Specifies the number of invalid requests permitted before executing the `penaltyAction`.	
penaltyAction	enum	Once the `penaltyThreshold` 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.	

Option	Type	Description	Requires
penalty302Uri	string	Specifies the redirect link for end users who trigger the penalty.	`penaltyAction` is `REDIRECT_302`
penaltyNet Storage	object	Specifies the NetStorage account that serves out the penalty's static 403 response content. Details appear in an object featuring a `downloadDomain Name` string member that identifies the NetStorage hostname, and an integer `cpCode` to track the traffic.	`penaltyAction` is `BRANDED_403`
penaltyNet Storage.cpCode List	array	A set of CP codes that apply to this storage group.	
penaltyNet Storage.download DomainName	string	Domain name from which content can be downloaded.	
penaltyNet Storage.id	number	Unique identifier for the storage group.	
penaltyNet Storage.name	string	Name of the storage group.	
penaltyNet Storage.upload DomainName	string	Domain name used to upload content.	
penalty403Net StoragePath	string	Specifies the full path to the static 403 response content relative to the `downloadDomainName` in the `penaltyNetStorage` object.	`penaltyAction` is `BRANDED_403`
penaltyBranded DenyCacheTtl	number (5-30)	Specifies the penalty response's time to live in the cache, `5` minutes by default.	`penaltyAction` is `BRANDED_403`

imOverride

- **Property Manager name**: Image and Video Manager: Set Parameter
- **Behavior version**: The `v2023-05-30` rule format supports the `imOverride` behavior v1.0.
- **Rule format status**: Deprecated, outdated rule format
- **Access**: Read-write
- **Allowed in includes**: Yes

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.	

Option	Type	Description	Requires
	FORMAT	For browser types.	
	DPR	For pixel density.	
	EXCLUDE_ QUERY	Excludes the specified query parameters from the cache key.	
typesel	enum	Specifies how to set a query parameter.	override is not POLICY_ VARIABLE AND override is not EXCLUDE_ QUERY
	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, or the encodings passed in the Accept header, that you want to optimize images for.	override is FORMAT AND typesel is VALUE
	CHROME	Google Chrome.	
	IE	Internet Explorer.	
	SAFARI	Apple Safari.	
	GENERIC	Generic.	
	AVIF_ WEBP_ JPEG_PNG_ GIF	Best of AVIF, WebP, JPEG, PNG, and GIF.	
	JP2_WEBP_ JPEG_PNG_ GIF	Best of JP2, WebP, JPEG, PNG, and GIF.	
	WEBP_ JPEG_PNG_ GIF	Best of WebP, JPEG, PNG, and GIF.	
	JPEG_PNG_ GIF	Best of JPEG, PNG, GIF.	
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 `typesel` 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 `typesel` 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`
excludeAll Query Parameters	boolean	Whether to exclude all query parameters from the Image and Video Manager cache key.	`override` is `EXCLUDE_ QUERY`
excluded Query Parameters	string array	Specifies individual query parameters to exclude from the Image and Video Manager cache key.	`override` is `EXCLUDE_ QUERY` AND `excludeAll QueryParameters` is `false`

imageManager

- **Property Manager name**: Image and Video Manager (Images)
- **Behavior version**: The `v2023-05-30` rule format supports the `imageManager` behavior v2.0.
- **Rule format status**: Deprecated, outdated rule format
- **Access**: Read-write
- **Allowed in includes**: Yes

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 `advancedIm Match` to ensure the behavior applies to the requests from the Image and Video Manager backend.

Option	Type	Description	Requires
enabled	boolean	Enable image management capabilities and generate a corresponding API token.	
resize	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.	

Option	Type	Description	Requires
applyBestFileType	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.	
superCacheRegion	enum	Specifies a location for your site's heaviest traffic, for use in caching derivatives on edge servers.	use Existing PolicySet is not true
	US	United States.	
	ASIA	Asia.	
	AUSTRALIA	Australia.	
	EMEA	Europe, Middle East, and Africa.	
	JAPAN	Japan.	
	CHINA	China.	
cpCodeOriginal	object	Assigns a CP code to track traffic and billing for original images that the Image and Video Manager has not modified. You only need to provide the initial `id`, stripping any `cpc_` [prefix](#) to pass the integer to the rule tree. Additional CP code details may reflect back in subsequent read-only data.	
cpCodeOriginal.cpCodeLimits	array	**Read-only**. Describes the current usage limit for the CP code.	
cpCodeOriginal.createdDate	integer	**Read-only**. UNIX epoch timestamp reflecting when the CP code was originally created.	
cpCodeOriginal.description	string	**Read-only**. Additional description for the CP code.	
cpCodeOriginal.id	integer	Unique identifier for each CP code. Initially, you get this value when [creating a new CP code](#) in PAPI. You can also assign a `cpcodeId` value from the [List CP codes](#) operation.	
cpCodeOriginal.name	string	**Read-only**. The name of the CP code you specify as the `cpcodeName` when [creating a new CP code](#) in PAPI. You can modify this value with the [PUT operation](#) in the CP codes and Reporting Groups API.	
cpCodeOriginal.products	array	**Read-only**. The set of products the CP code is assigned to. This reflects `productId` values you specify when [creating a new CP code](#) in PAPI.	
cpCodeTransformed	object	Assigns a separate CP code to track traffic and billing for derived images. You only need to provide the initial `id`, stripping any `cpc_` [prefix](#) to pass the integer to the rule tree. Additional CP code details may reflect back in subsequent read-only data.	
cpCodeTransformed.cpCodeLimits	array	**Read-only**. Describes the current usage limit for the CP code.	
cpCodeTransformed.createdDate	integer	**Read-only**. UNIX epoch timestamp reflecting when the CP code was originally created.	
cpCodeTransformed.description	string	**Read-only**. Additional description for the CP code.	
cpCodeTransformed.id	integer	Unique identifier for each CP code. Initially, you get this value when [creating a new CP code](#) in PAPI. You can also assign a `cpcodeId` value from the [List CP codes](#) operation.	
cpCodeTransformed.name	string	**Read-only**. The name of the CP code you specify as the `cpcodeName` when [creating a new CP code](#) in PAPI. You can modify this value with the [PUT operation](#) in the CP codes and Reporting Groups API.	
cpCodeTransformed.products	array	**Read-only**. The set of products the CP code is assigned to. This reflects `productId` values you specify when [creating a new CP code](#) in PAPI.	

Option	Type	Description	Requires
useExistingPolicySet	boolean	Whether to use a previously created policy set that may be referenced in other properties, or create a new policy set to use with this property. A policy set can be shared across multiple properties belonging to the same contract. The behavior populates any changes to the policy set across all properties that reference that set.	
policySet	object	Identifies the existing policy set configured with Image and Video Manager API.	use Existing PolicySet is true
advanced	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 policyToken) concatenated with a property-specific identifier that's generated when you save the property. The API registers the token when you activate the property.	use Existing PolicySet is false
policyToken	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, *default* becomes the prefix.	advanced is true
policyTokenDefault	string	Specify the default policy identifier, which is registered with the Image and Video Manager API once you activate this property. The advanced option needs to be inactive.	advanced is false

imageManagerVideo

- **Property Manager name**: Image and Video Manager (Videos)
- **Behavior version**: The v2023-05-30 rule format supports the imageManagerVideo behavior v2.0.
- **Rule format status**: Deprecated, outdated rule format
- **Access**: Read-write
- **Allowed in includes**: Yes

Optimizes videos managed by Image and Video Manager for the requesting device. You can also use this behavior to generate API tokens to apply your own policies to matching videos using the Image and Video Manager API. To apply this behavior, you need to match on a fileExtension .

Option	Type	Description	Requires
enabled	boolean	Applies Image and Video Manager's video optimization to the current content.	
resize	boolean	When enabled, scales down video for smaller mobile screens, based on the device's User-Agent header.	
applyBestFileType	boolean	When enabled, automatically converts videos to the best file type for the requesting device. This produces the smallest file size that retains image quality, based on the user agent and the initial image file.	
superCacheRegion	enum	To optimize caching, assign a region close to your site's heaviest traffic.	use Existing PolicySet is not true
	US	United States.	

Option	Type	Description	Requires
	ASIA	Asia.	
	AUSTRALIA	Australia.	
	EMEA	Europe, Middle East, and Africa.	
	JAPAN	Japan.	
	CHINA	China.	
cpCodeOriginal	object	Specifies the CP code for which to track Image and Video Manager video traffic. Use this along with `cpCodeTransformed` to track traffic to derivative video content. You only need to provide the initial `id`, stripping any `cpc_` `prefix` to pass the integer to the rule tree. Additional CP code details may reflect back in subsequent read-only data.	
cpCodeOriginal.cpCode Limits	array	**Read-only**. Describes the current usage limit for the CP code.	
cpCodeOriginal.created Date	integer	**Read-only**. UNIX epoch timestamp reflecting when the CP code was originally created.	
cpCode Original.description	string	**Read-only**. Additional description for the CP code.	
cpCodeOriginal.id	integer	Unique identifier for each CP code. Initially, you get this value when creating a new CP code in PAPI. You can also assign a `cpcodeId` value from the List CP codes operation.	
cpCodeOriginal.name	string	**Read-only**. The name of the CP code you specify as the `cpcodeName` when creating a new CP code in PAPI. You can modify this value with the PUT operation in the CP codes and Reporting Groups API.	
cpCode Original.products	array	**Read-only**. The set of products the CP code is assigned to. This reflects `productId` values you specify when creating a new CP code in PAPI.	
cpCodeTransformed	object	Specifies the CP code to identify derivative transformed video content. You only need to provide the initial `id`, stripping any `cpc_` `prefix` to pass the integer to the rule tree. Additional CP code details may reflect back in subsequent read-only data.	
cpCodeTransformed.cp CodeLimits	array	**Read-only**. Describes the current usage limit for the CP code.	
cpCode Transformed.created Date	integer	**Read-only**. UNIX epoch timestamp reflecting when the CP code was originally created.	
cpCode Transformed.description	string	**Read-only**. Additional description for the CP code.	
cpCodeTransformed.id	integer	Unique identifier for each CP code. Initially, you get this value when creating a new CP code in PAPI. You can also assign a `cpcodeId` value from the List CP codes operation.	
cpCode Transformed.name	string	**Read-only**. The name of the CP code you specify as the `cpcodeName` when creating a new CP code in PAPI. You can modify this value with the PUT operation in the CP codes and Reporting Groups API.	
cpCode Transformed.products	array	**Read-only**. The set of products the CP code is assigned to. This reflects `productId` values you specify when creating a new CP code in PAPI.	
useExistingPolicySet	boolean	Whether to use a previously created policy set that may be referenced in other properties, or create a new policy set to use with this property. A policy set can be shared across multiple properties belonging to the same contract. The behavior populates any changes to the policy set across all properties that reference that set.	
policySet	object	Identifies the existing policy set configured with Image and Video Manager API.	`use Existing PolicySet` is `true`

Option	Type	Description	Requires
advanced	boolean	When disabled, applies a single standard policy based on your property name. Allows you to reference a rule-specific `policyToken` for videos with different match criteria.	use Existing PolicySet is `false`
policyToken	string	Specifies a custom policy defined in the Image and Video Manager Policy Manager or the [Image and Video Manager API](#). The policy name can include up to 64 alphanumeric, dash, or underscore characters.	advanced is `true`
policyTokenDefault	string	Specifies the default policy identifier, which is registered with the [Image and Video Manager API](#) once you activate this property.	advanced is `false`

include

- **Property Manager name**: [Include](#)
- **Behavior version**: The `v2023-05-30` rule format supports the `include` behavior v1.0.
- **Rule format status**: [Deprecated, outdated rule format](#)
- **Access**: [Read-write](#)
- **Allowed in includes**: [No (temporarily)](#)

Includes let you reuse chunks of a property configuration that you can manage separately from the rest of the property rule tree.

Option	Type	Description
id	string	Identifies the include you want to add to your rule tree. You can get the include ID using [PAPI](#). This option only accepts digits, without the `inc_` [ID prefix](#).

instant

- **Property Manager name**: [Akamai Instant (Prefetching)](#)
- **Behavior version**: The `v2023-05-30` rule format supports the `instant` behavior v1.1.
- **Rule format status**: [Deprecated, outdated rule format](#)
- **Access**: [Read-write](#)
- **Allowed in includes**: [Yes](#)

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>` , `<img>` , `<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
prefetch Cacheable	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.	
prefetch NoStore	boolean	Allows otherwise non-cacheable `no-store` content to prefetch if the URL path ends with `/` to indicate a request for a default file, or if the extension matches the value of the `prefetchNoStore Extensions` option. Only applies to content with the `sureRoute` behavior enabled.	
prefetch NoStore Extensions	string array	Specifies a set of file extensions for which the `prefetchNoStore` option is allowed.	prefetchNo Store is true
prefetch Html	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.	prefetch Cacheable is true OR prefetch NoStore is true
custom Link Relations	string array	Specify link relation values that activate the prefetching behavior. For example, specifying `fetch` allows you to use shorter `rel="fetch"` markup.	prefetch Html is true

instantConfig

- **Property Manager name**: InstantConfig
- **Behavior version**: The `v2023-05-30` rule format supports the `instantConfig` behavior v1.1.
- **Rule format status**: Deprecated, outdated rule format
- **Access**: Read-write
- **Allowed in includes**: No (temporarily)

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 `v2023-05-30` rule format supports the `largeFileOptimization` behavior v1.2.
- **Rule format status**: Deprecated, outdated rule format
- **Access**: Read-write
- **Allowed in includes**: Yes

The Large File Optimization (LFO) feature improves performance and reliability when delivering large files. You need this behavior for objects larger than 1.8GB, and you should apply it to 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. Make sure you meet all the requirements and best practices for the LFO delivery.

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 *partial-object caching*, which always applies to large objects served from NetStorage. The size of the object to be cached can't be greater than 323 GB. To enable this, the origin needs to support byte range requests.	
	NON_PARTIAL_OBJECT_CACHING	Caches entire objects. The size of the object to be cached can't be greater than 1800 MB.	
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`. The size of a file can't be greater than 323 GB. If you need to optimize a larger file, contact Akamai Professional Services for help.	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 `v2023-05-30` rule format supports the `largeFileOptimizationAdvanced` behavior v1.0.
- **Rule format status**: Deprecated, outdated rule format
- **Access**: Read-only
- **Allowed in includes**: Yes

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: FOUR_MB HALF_MB ONE_MB TWO_MB
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 `v2023-05-30` rule format supports the `limitBitRate` behavior v1.2.
- **Rule format status**: Deprecated, outdated rule format
- **Access**: Read-write
- **Allowed in includes**: Yes

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` .
bitrate Table[].bitrate Value	number	The numeric indicator of the download rate.
bitrate Table[].bitrate Unit	enum	The unit of measurement, either `KBPS` , `MBPS` , or `GBPS` .
		Supported values: 　　　GBPS　　　　　KBPS　　　　　MBPS
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` .
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: 　　　BYTES　　　　　　　　SECONDS

logCustom

- **Property Manager name**: Log Custom Details
- **Behavior version**: The `v2023-05-30` rule format supports the `logCustom` behavior v1.1.
- **Rule format status**: Deprecated, outdated rule format
- **Access**: Read-write
- **Allowed in includes**: Yes

Logs custom details from the origin response in the Log Delivery Service⬈ report.

Option	Type	Description	Requires
log Custom LogField	boolean	Whether to append additional custom data to each log line.	

Option	Type	Description	Requires
custom LogField	string (allows variables)	Specifies an additional data field to append to each log line, maximum 1000 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. Since this option can specify both a request and response, it overrides any `customLogField` settings in the `report` behavior.	logCustom LogField is true

mPulse

- **Property Manager name**: mPulse
- **Behavior version**: The `v2023-05-30` rule format supports the `mPulse` behavior v1.4.
- **Rule format status**: Deprecated, outdated rule format
- **Access**: Read-write
- **Allowed in includes**: No (temporarily)

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.
require Pci	boolean	Suppresses gathering metrics for potentially sensitive end-user interactions. Enabling this omits data from some older browsers.
loader Version	enum	Specifies the version of the Boomerang JavaScript loader snippet. See mPulse Loader Snippets for more information.
	V10	Use version 10.
	V12	Use version 12.
	LATEST	Automatically update to the latest available production version.
	BETA	Use the latest version, including beta releases.
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.
config Override	string	A JSON string representing a configuration object passed to the JavaScript library under which mPulse runs. It corresponds at run-time to the `window.BOOMR_config` object. For example, this turns on monitoring of Single Page App frameworks: `"{\"history\": {\"enabled\": true, \"auto\": true}}"` . See Configuration Overrides for more information.

manifestPersonalization

- **Property Manager name**: [Manifest Personalization](#)
- **Behavior version**: The `v2023-05-30` rule format supports the `manifestPersonalization` behavior v1.0.
- **Rule format status**: [Deprecated, outdated rule format](#)
- **Access**: [Read-write](#)
- **Allowed in includes**: [Yes](#)

Allows customers who use the Adaptive Media Delivery product to enhance content based on the capabilities of each end user's device. This behavior configures a *manifest* for both HLS Live and on-demand streaming. For more information, see [Adaptive Media Delivery](#).

Option	Type	Description	Requires
enabled	boolean	Enables the Manifest Personalization feature.	
hls Enabled	boolean	Allows you to customize the HLS master manifest that's sent to the requesting client.	
hlsMode	enum	Applies with `hlsEnabled` on.	`hlsEnabled` is `true`
	BEST_ PRACTICE	Specify the default best practice mode.	
	CUSTOM	Specify a custom manifest.	
hls Preferred Bitrate	string	Sets the preferred bit rate in Kbps. This causes the media playlist specified in the `#EXT-X-STREAM-INF` tag that most closely matches the value to list first. All other playlists maintain their current position in the manifest.	`hlsMode` is CUSTOM
hlsFilterIn Bitrates	string	Specifies a comma-delimited set of preferred bit rates, such as `100,200,400`. Playlists specified in the `#EXT-X-STREAM-INF` tag with bit rates outside of any of those values by up to 100 Kbps are excluded from the manifest.	`hlsMode` is CUSTOM
hlsFilterIn Bitrate Ranges	string	Specifies a comma-delimited set of bit rate ranges, such as `100-400,1000-4000`. Playlists specified in the `#EXT-X-STREAM-INF` tag with bit rates outside of any of those ranges are excluded from the manifest.	`hlsMode` is CUSTOM
hlsQuery Param Enabled	boolean	Specifies query parameters for the HLS master manifest to customize the manifest's content. Any settings specified in the query string override those already configured in Property Manager.	`hlsEnabled` is `true`
hlsQuery Param SecretKey	object array	Specifies a primary key as a token to accompany the request.	`hlsQuery Param Enabled` is true
hlsQuery Param Transition Key	object array	Specifies a transition key as a token to accompany the request.	`hlsQuery Param Enabled` is true
hlsShow Advanced	boolean	Allows you to configure advanced settings.	`hlsEnabled` is `true`
hlsEnable Debug Headers	boolean	Includes additional `Akamai-Manifest-Personalization` and `Akamai-Manifest-Personalization-Config-Source` debugging headers.	`hlsShow Advanced` is `true`

manifestRerouting

- **Property Manager name**: Manifest Rerouting
- **Behavior version**: The `v2023-05-30` rule format supports the `manifestRerouting` behavior v1.0.
- **Rule format status**: Deprecated, outdated rule format
- **Access**: Read-write
- **Allowed in includes**: No (temporarily)

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 `adobe_primetime` , 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 `v2023-05-30` rule format supports the `manualServerPush` behavior v1.0.
- **Rule format status**: Deprecated, outdated rule format
- **Access**: Read-write
- **Allowed in includes**: No (temporarily)

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 `www.example.com/js/site.js` .

mediaAcceleration

- **Property Manager name**: [Media Acceleration](#)
- **Behavior version**: The `v2023-05-30` rule format supports the `mediaAcceleration` behavior v1.1.
- **Rule format status**: [Deprecated, outdated rule format](#)
- **Access**: [Read-write](#)
- **Allowed in includes**: [No (temporarily)](#)

Enables Accelerated Media Delivery for this set of requests.

Option	Type	Description
enabled	boolean	Enables Media Acceleration.

mediaAccelerationQuicOptout

- **Property Manager name**: [Media Acceleration (QUIC Protocol) Opt-Out](#)
- **Behavior version**: The `v2023-05-30` rule format supports the `mediaAccelerationQuicOptout` behavior v1.0.
- **Rule format status**: [Deprecated, outdated rule format](#)
- **Access**: [Read-write](#)
- **Allowed in includes**: [No (temporarily)](#)

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.

mediaClient

- **Property Manager name**: [Media Client](#)
- **Behavior version**: The `v2023-05-30` rule format supports the `mediaClient` behavior v1.1.
- **Rule format status**: [Deprecated, outdated rule format](#)
- **Access**: [Read-write](#)

- **Allowed in includes**: [No (temporarily)](#)

This behavior is deprecated, but you should not disable or remove it if present.

Enables client-side reporting through analytics beacon requests.

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

mediaFileRetrievalOptimization

- **Property Manager name**: [Media File Retrieval Optimization](#)
- **Behavior version**: The `v2023-05-30` rule format supports the `mediaFileRetrievalOptimization` behavior v1.1.
- **Rule format status**: [Deprecated, outdated rule format](#)
- **Access**: [Read-write](#)
- **Allowed in includes**: [Yes](#)

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 `v2023-05-30` rule format supports the `mediaOriginFailover` behavior v1.0.
- **Rule format status**: [Deprecated, outdated rule format](#)
- **Access**: [Read-write](#)
- **Allowed in includes**: [Yes](#)

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
detectOrigin Unresponsive	boolean	Allows you to configure what happens when the origin is unresponsive.	
originUnresponsive DetectionLevel	enum	Specify the level of response to slow origin connections.	detectOriginUnresponsive is true
	AGGRESSIVE	Aggressive response.	
	CONSERVATIVE	Conservative response.	
	MODERATE	Moderate response.	
originUnresponsive BlacklistOriginIp	boolean	Enabling this blacklists the origin's IP address.	detectOriginUnresponsive is true
originUnresponsive BlacklistWindow	enum	This sets the delay before blacklisting an IP address.	originUnresponsiveBlacklistOriginIp is true
	TEN_S	10 seconds.	
	THIRTY_S	30 seconds.	
originUnresponsive Recovery	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.	
originUnresponsive RetryLimit	enum	Sets how many times to retry.	originUnresponsiveRecovery is RETRY_ X_TIMES
		Supported values: ONE THREE	
originUnresponsive BackupHost	string	This specifies the origin hostname.	originUnresponsiveRecovery is SWITCH_TO_ BACKUP_ORIGIN
originUnresponsive AlternateHost	string	This specifies the redirect's destination hostname.	originUnresponsiveRecovery is REDIRECT_ TO_DIFFERENT_ORIGIN_LOCATION
originUnresponsive ModifyRequestPath	boolean	Modifies the request path.	originUnresponsiveRecovery is SWITCH_TO_ BACKUP_ORIGIN OR originUnresponsiveRecovery is REDIRECT_TO_DIFFERENT_ORIGIN_LOCATION
originUnresponsive ModifiedPath	string	This specifies the path to form the new URL.	originUnresponsiveModifyRequestPath is true
originUnresponsive IncludeQueryString	boolean	Enabling this includes the original set of query parameters.	originUnresponsiveModifyRequestPath is true
originUnresponsive RedirectMethod	enum	Specifies the redirect response code.	originUnresponsiveRecovery is REDIRECT_ TO_DIFFERENT_ORIGIN_LOCATION
		Supported values: 301 302	
originUnresponsive ChangeProtocol	boolean	This allows you to change the request protocol.	originUnresponsiveRecovery is SWITCH_TO_ BACKUP_ORIGIN OR originUnresponsiveRecovery is REDIRECT_TO_DIFFERENT_ORIGIN_LOCATION

Option	Type	Description	Requires
originUnresponsiveProtocol	enum	Specifies which protocol to use.	originUnresponsiveChangeProtocol is true
		Supported values: HTTP HTTPS	
detectOriginUnavailable	boolean	Allows you to configure failover settings when the origin server responds with errors.	
originUnavailableDetectionLevel	enum	Specify `RESPONSE_CODES`, the only available option.	detectOriginUnavailable is true
	`RESPONSE_CODES`	This is the only value currently available.	
originUnavailableResponseCodes	string array	Specifies the set of response codes identifying when the origin responds with errors.	detectOriginUnavailable is true
originUnavailableBlacklistOriginIp	boolean	Enabling this blacklists the origin's IP address.	detectOriginUnavailable is true
originUnavailableBlacklistWindow	enum	This sets the delay before blacklisting an IP address.	originUnavailableBlacklistOriginIp is true
	`TEN_S`	10 seconds.	
	`THIRTY_S`	30 seconds.	
originUnavailableRecovery	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.	
originUnavailableRetryLimit	enum	Sets how many times to retry.	originUnavailableRecovery is `RETRY_X_TIMES`
		Supported values: ONE THREE	
originUnavailableBackupHost	string	This specifies the origin hostname.	originUnavailableRecovery is `SWITCH_TO_BACKUP_ORIGIN`
originUnavailableAlternateHost	string	This specifies the redirect's destination hostname.	originUnavailableRecovery is `REDIRECT_TO_DIFFERENT_ORIGIN_LOCATION`
originUnavailableModifyRequestPath	boolean	Modifies the request path.	originUnavailableRecovery is `SWITCH_TO_BACKUP_ORIGIN` OR originUnavailableRecovery is `REDIRECT_TO_DIFFERENT_ORIGIN_LOCATION`
originUnavailableModifiedPath	string	This specifies the path to form the new URL.	originUnavailableModifyRequestPath is true
originUnavailableIncludeQueryString	boolean	Enabling this includes the original set of query parameters.	originUnavailableModifyRequestPath is true
originUnavailableRedirectMethod	enum	Specifies either a redirect response code.	originUnavailableRecovery is `REDIRECT_TO_DIFFERENT_ORIGIN_LOCATION`
		Supported values: 301 302	

Option	Type	Description	Requires
originUnavailable ChangeProtocol	boolean	Modifies the request protocol.	originUnavailableRecovery is SWITCH_TO_ BACKUP_ORIGIN OR originUnavailableRecovery is REDIRECT_TO_DIFFERENT_ORIGIN_LOCATION
originUnavailable Protocol	enum	Specifies either the HTTP or HTTPS protocol.	originUnavailableChangeProtocol is true
		Supported values: HTTP　　　　HTTPS	
detectObject Unavailable	boolean	Allows you to configure failover settings when the origin has content errors.	
objectUnavailable DetectionLevel	enum	Specify RESPONSE_CODES , the only available option.	detectObjectUnavailable is true
	RESPONSE_CODES	This is the only value currently available.	
objectUnavailable ResponseCodes	string array	Specifies the set of response codes identifying when there are content errors.	detectObjectUnavailable is true
objectUnavailable BlacklistOriginIp	boolean	Enabling this blacklists the origin's IP address.	detectObjectUnavailable is true
objectUnavailable BlacklistWindow	enum	This sets the delay before blacklisting an IP address.	objectUnavailableBlacklistOriginIp is true
	TEN_S	10 seconds.	
	THIRTY_S	30 seconds.	
objectUnavailable Recovery	enum	This sets the recovery option.	detectObjectUnavailable 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.	
objectUnavailable RetryLimit	enum	Sets how many times to retry.	objectUnavailableRecovery is RETRY_ X_TIMES
		Supported values: ONE　　　　THREE	
objectUnavailable BackupHost	string	This specifies the origin hostname.	objectUnavailableRecovery is SWITCH_TO_ BACKUP_ORIGIN
objectUnavailable AlternateHost	string	This specifies the redirect's destination hostname.	objectUnavailableRecovery is REDIRECT_ TO_DIFFERENT_ORIGIN_LOCATION
objectUnavailable ModifyRequestPath	boolean	Enabling this allows you to modify the request path.	objectUnavailableRecovery is SWITCH_TO_ BACKUP_ORIGIN OR objectUnavailableRecovery is REDIRECT_TO_DIFFERENT_ORIGIN_LOCATION
objectUnavailable ModifiedPath	string	This specifies the path to form the new URL.	objectUnavailableModifyRequestPath is true
objectUnavailable IncludeQueryString	boolean	Enabling this includes the original set of query parameters.	objectUnavailableModifyRequestPath is true
objectUnavailable RedirectMethod	enum	Specifies a redirect response code.	objectUnavailableRecovery is REDIRECT_ TO_DIFFERENT_ORIGIN_LOCATION

Option	Type	Description	Requires
		Supported values: 301 302	
objectUnavailableChangeProtocol	boolean	Changes the request protocol.	objectUnavailableRecovery is SWITCH_TO_BACKUP_ORIGIN OR objectUnavailableRecovery is REDIRECT_TO_DIFFERENT_ORIGIN_LOCATION
objectUnavailableProtocol	enum	Specifies either the HTTP or HTTPS protocol.	objectUnavailableChangeProtocol is true
		Supported values: HTTP HTTPS	
clientResponseCode	string	Specifies the response code served to the client.	
cacheErrorResponse	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.	

metadataCaching

- **Property Manager name**: Metadata Caching
- **Behavior version**: The v2023-05-30 rule format supports the metadataCaching behavior v1.0.
- **Rule format status**: Deprecated, outdated rule format
- **Access**: Read-only
- **Allowed in includes**: Yes

This behavior reduces time spent waiting for the initial response, also known as time to first byte, during peak traffic events. Contact Akamai Professional Services for help configuring it.

Option	Type	Description
enabled	boolean	Enables metadata caching.

mobileSdkPerformance

- **Property Manager name**: [Mobile App Performance SDK](#)
- **Behavior version**: The `v2023-05-30` rule format supports the `mobileSdkPerformance` behavior v1.0.
- **Rule format status**: [Deprecated, outdated rule format](#)
- **Access**: [Read-write](#)
- **Allowed in includes**: [Yes](#)

This behavior is deprecated, but you should not disable or remove it if present.

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

modifyIncomingRequestHeader

- **Property Manager name**: [Modify Incoming Request Header](#)
- **Behavior version**: The `v2023-05-30` rule format supports the `modifyIncomingRequestHeader` behavior v1.2.
- **Rule format status**: [Deprecated, outdated rule format](#)
- **Access**: [Read-write](#)
- **Allowed in includes**: [Yes](#)

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](#)
action	enum	Either `ADD` , `DELETE` , `MODIFY` , or `PASS` incoming HTTP request headers.	
	ADD	Add the header.	
	DELETE	Delete the header.	
	MODIFY	Modify the header.	
	PASS	Pass through the header.	

Option	Type	Description	Requires
standardAdd HeaderName	enum	If the value of `action` is `ADD` , this specifies the name of the field to add.	`action` is `ADD`
	`ACCEPT_ ENCODING`	Add an `Accept-Encoding` header.	
	`ACCEPT_ LANGUAGE`	Add an `Accept-Language` header.	
	`OTHER`	Specify another header to add.	
standardDelete HeaderName	enum	If the value of `action` is `DELETE` , this specifies the name of the field to remove.	`action` is `DELETE`
	`IF_MODIFIED_ SINCE`	The `If-Modified-Since` header.	
	`VIA`	The `Via` header.	
	`OTHER`	Specify another header to remove.	
standardModify HeaderName	enum	If the value of `action` is `MODIFY` , this specifies the name of the field to modify.	`action` is `MODIFY`
	`ACCEPT_ ENCODING`	Add an `Accept-Encoding` header.	
	`ACCEPT_ LANGUAGE`	Add an `Accept-Language` header.	
	`OTHER`	Specify another header to add.	
standardPass HeaderName	enum	If the value of `action` is `PASS` , this specifies the name of the field to pass through.	`action` is `PASS`
	`ACCEPT_ ENCODING`	Add an `Accept-Encoding` header.	
	`ACCEPT_ LANGUAGE`	Add an `Accept-Language` header.	
	`OTHER`	Specify another header to add.	
customHeader Name	string (allows [variables](#))	Specifies a custom field name that applies when the relevant *standard* header name is set to `OTHER` .	standardAddHeaderName is `OTHER` OR `standardDeleteHeader Name` is `OTHER` OR `standardModifyHeader Name` is `OTHER` OR `standardPassHeader Name` is `OTHER`
headerValue	string (allows [variables](#))	Specifies the new header value.	`action` is `ADD`
newHeaderValue	string (allows [variables](#))	Supplies an HTTP header replacement value.	`action` is `MODIFY`
avoidDuplicate Headers	boolean	When enabled with the `action` set to `MODIFY` , prevents creation of more than one instance of a header.	`action` is `MODIFY`

modifyIncomingResponseHeader

- **Property Manager name**: [Modify Incoming Response Header](#)
- **Behavior version**: The `v2023-05-30` rule format supports the `modifyIncomingResponseHeader` behavior v1.2.
- **Rule format status**: [Deprecated, outdated rule format](#)
- **Access**: [Read-write](#)
- **Allowed in includes**: [Yes](#)

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
action	enum	Either `ADD`, `DELETE`, `MODIFY`, or `PASS` incoming HTTP response headers.	
	ADD	Add the header.	
	DELETE	Delete the header.	
	MODIFY	Modify the header.	
	PASS	Pass through the header.	
standardAdd HeaderName	enum	If the value of `action` is `ADD`, this specifies the name of the field to add.	action is ADD
	CACHE_CONTROL	The `Cache-Control` header.	
	CONTENT_TYPE	The `Content-Type` header.	
	EDGE_CONTROL	The `Edge-Control` header.	
	EXPIRES	The `Expires` header.	
	LAST_MODIFIED	The `Last-Modified` header.	
	OTHER	Specify another header to add.	
standardDelete HeaderName	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_TYPE	The `Content-Type` header.	
	VARY	The `Vary` header.	
	OTHER	Specify another header to remove.	
standardModify HeaderName	enum	If the value of `action` is `MODIFY`, this specifies the name of the field to modify.	action is MODIFY
	CACHE_CONTROL	The `Cache-Control` header.	
	CONTENT_TYPE	The `Content-Type` header.	
	EDGE_CONTROL	The `Edge-Control` header.	
	OTHER	Specify another header to modify.	
standardPass HeaderName	enum	If the value of `action` is `PASS`, this specifies the name of the field to pass through.	action is PASS
	CACHE_CONTROL	Pass through the `Cache-Control` header.	

Option	Type	Description	Requires
	EXPIRES	Pass through the `Expires` header.	
	PRAGMA	Pass through the `Pragma` header.	
	OTHER	Specify another header to pass.	
customHeaderName	string (allows [variables](#))	Specifies a custom field name that applies when the relevant *standard* header name is set to `OTHER` .	standardAddHeaderName is `OTHER` OR standardDeleteHeaderName is `OTHER` OR standardModifyHeaderName is `OTHER` OR standardPassHeaderName is `OTHER`
headerValue	string (allows [variables](#))	Specifies the header's new value.	action is `ADD`
newHeaderValue	string (allows [variables](#))	Specifies an HTTP header replacement value.	action is `MODIFY`
avoidDuplicateHeaders	boolean	When enabled with the `action` set to `MODIFY` , prevents creation of more than one instance of a header.	action is `MODIFY`

modifyOutgoingRequestHeader

- **Property Manager name**: [Modify Outgoing Request Header](#)
- **Behavior version**: The `v2023-05-30` rule format supports the `modifyOutgoingRequestHeader` behavior v1.2.
- **Rule format status**: [Deprecated, outdated rule format](#)
- **Access**: [Read-write](#)
- **Allowed in includes**: [Yes](#)

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 `ADD` or `DELETE` outgoing HTTP request headers, `MODIFY` their fixed values, or specify a `REGEX` pattern to transform them.	
	ADD	Add the header.	
	DELETE	Delete the header.	
	MODIFY	Modify the header.	
	REGEX	Specify another header to modify.	

Option	Type	Description	Requires
standardAddHeaderName	enum	If the value of `action` is `ADD`, this specifies the name of the field to add.	`action` is `ADD`
	USER_AGENT	The `User-Agent` header.	
	OTHER	Specify another header to add.	
standardDeleteHeaderName	enum	If the value of `action` is `DELETE`, this specifies the name of the field to remove.	`action` is `DELETE`
	PRAGMA	The `Pragma` header.	
	USER_AGENT	The `User-Agent` header.	
	VIA	The `Via` header.	
	OTHER	Specify another header to remove.	
standardModifyHeaderName	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`
	USER_AGENT	The `User-Agent` header.	
	OTHER	Specify another header to modify.	
customHeaderName	string (allows [variables](#))	Specifies a custom field name that applies when the relevant *standard* header name is set to `OTHER`.	standardAddHeaderName is `OTHER` OR standardDeleteHeaderName is `OTHER` OR standardModifyHeaderName is `OTHER`
headerValue	string (allows [variables](#))	Specifies the new header value.	`action` is `ADD`
newHeaderValue	string (allows [variables](#))	Specifies an HTTP header replacement value.	`action` is `MODIFY`
regexHeaderMatch	string (allows [variables](#))	Specifies a Perl-compatible regular expression to match within the header value.	`action` is `REGEX`
regexHeaderReplace	string (allows [variables](#))	Specifies text that replaces the `regexHeaderMatch` pattern within the header value.	`action` is `REGEX`
matchMultiple	boolean	When enabled with the `action` set to `REGEX`, replaces all occurrences of the matched regular expression, otherwise only the first match if disabled.	`action` is `REGEX`
avoidDuplicateHeaders	boolean	When enabled with the `action` set to `MODIFY`, prevents creation of more than one instance of a header.	`action` is `MODIFY`

modifyOutgoingResponseHeader

- **Property Manager name**: [Modify Outgoing Response Header](#)

- **Behavior version**: The `v2023-05-30` rule format supports the `modifyOutgoingResponseHeader` behavior v1.6.
- **Rule format status**: Deprecated, outdated rule format
- **Access**: Read-write
- **Allowed in includes**: Yes

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
action	enum	Either `ADD` or `DELETE` outgoing HTTP response headers, `MODIFY` their fixed values, or specify a `REGEX` pattern to transform them.	
	ADD	Add the header.	
	DELETE	Delete the header.	
	MODIFY	Modify the header.	
	REGEX	Specify another header to modify.	
standard Add Header Name	enum	If the value of `action` is `ADD`, this specifies the name of the field to add.	`action` is `ADD`
	CACHE_CONTROL	The `Cache-Control` header.	
	CONTENT_ DISPOSITION	The `Content-Disposition` header.	
	CONTENT_TYPE	The `Content-Type` header.	
	EDGE_CONTROL	The `Edge-Control` header.	
	P3P	Specify another header to add.	
	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 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`

Option	Type	Description	Requires
	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.	
	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 modify.	

Option	Type	Description	Requires
custom Header Name	string (allows variables)	Specifies a custom field name that applies when the relevant *standard* header name is set to `OTHER` .	`standardAdd Header Name` is `OTHER` OR `standard DeleteHeader Name` is `OTHER` OR `standard ModifyHeader Name` is `OTHER`
header Value	string (allows variables)	Specifies the existing value of the header to match.	`action` is `ADD`
new Header Value	string (allows variables)	Specifies the new HTTP header replacement value.	`action` is `MODIFY`
regex Header Match	string	Specifies a Perl-compatible regular expression to match within the header value.	`action` is `REGEX`
regex Header Replace	string (allows variables)	Specifies text that replaces the `regexHeaderMatch` pattern within the header value.	`action` is `REGEX`
match Multiple	boolean	When enabled with the `action` set to `REGEX` , replaces all occurrences of the matched regular expression, otherwise only the first match if disabled.	`action` is `REGEX`
avoid Duplicate Headers	boolean	When enabled with the `action` set to `MODIFY` , 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.	`action` is `MODIFY`

modifyViaHeader

- **Property Manager name**: Modify Via Header
- **Behavior version**: The `v2023-05-30` rule format supports the `modifyViaHeader` behavior v1.0.
- **Rule format status**: Deprecated, outdated rule format
- **Access**: Read-write
- **Allowed in includes**: Yes

Removes or renames the HTTP `Via` headers used to inform the server of proxies through which the request was sent to the origin.

Option	Type	Description	Requires
enabled	boolean	Enables `Via` header modifications.	
modification Option	enum	Specify how you want to handle the header.	

Option	Type	Description	Requires
	REMOVE_ HEADER	Remove the header.	
	RENAME_HEADER	Rename the header.	
renameHeaderTo	string	Specifies a new name to replace the existing Via header.	modificationOption is RENAME_HEADER

origin

- **Property Manager name**: Origin Server
- **Behavior version**: The v2023-05-30 rule format supports the origin behavior v1.21.
- **Rule format status**: Deprecated, outdated rule format
- **Access**: Read-write
- **Allowed in includes**: Yes

Specify the hostname and settings used to contact the origin once service begins. You can use your own origin, Net Storage, an Edge Load Balancing origin, or a SaaS dynamic origin.

Option	Type	Description	Requires
originType	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.	
netStorage	object	Specifies the details of the NetStorage server.	originType is NET_ STORAGE
netStorage.cp Code	integer	Identifies a CP code assigned to this storage group.	
net Storage.download DomainName	string	Domain name from which content can be downloaded.	
netStorage.g2o Token	string	Signature Header Authentication key.	
netStorage.id	integer	Unique identifier for the storage group.	

Option	Type	Description	Requires
netStorage.name	string	Name of the storage group.	
originId	string	Identifies the Edge Load Balancing origin. This needs to correspond to an `edgeLoadBalancingOrigin` behavior's `id` attribute within the same property.	`originType` is `EDGE_LOAD_BALANCING_ORIGIN_GROUP`
hostname	string (allows [variables](#))	Specifies the hostname or IPv4 address of your origin server, from which edge servers can retrieve your content.	`originType` is `CUSTOMER`
secondHostnameEnabled	boolean	Available only for certain products. This specifies whether you want to use an additional origin server address.	
secondHostname	string (allows [variables](#))	Specifies the origin server's hostname, IPv4 address, or IPv6 address. Edge servers retrieve your content from this origin server.	`secondHostnameEnabled` is `true`
mslorigin	string	This specifies the media's origin server.	`originType` is `MEDIA_SERVICE_LIVE`
saasType	enum	Specifies the part of the request that identifies this SaaS dynamic origin.	`originType` is `SAAS_DYNAMIC_ORIGIN`
		Supported values: COOKIE HOSTNAME	
saasCnameEnabled	boolean	Enabling this allows you to use a *CNAME chain* to determine the hostname for this SaaS dynamic origin.	`saasType` is `HOSTNAME`
saasCnameLevel	number	Specifies the desired number of hostnames to use in the *CNAME chain*, starting backwards from the edge server.	`saasCnameEnabled` 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 `saasRegex` matches.	`originType` is `SAAS_DYNAMIC_ORIGIN`
saasSuffix	string	Specifies the static part of the SaaS dynamic origin.	`originType` is `SAAS_DYNAMIC_ORIGIN`
forwardHostHeader	enum	When the `originType` is set to either `CUSTOMER` or `SAAS_DYNAMIC_ORIGIN`, this specifies which `Host` header to pass to the origin.	`originType` is either: `CUSTOMER`, `SAAS_DYNAMIC_ORIGIN`
	`REQUEST_HOST_HEADER`	Passes the original request's header.	
	`ORIGIN_HOSTNAME`	Passes the current origin's `HOSTNAME`.	
	`CUSTOM`	Passes the value of `customForwardHostHeader`. Use this option if you want requests handled by different properties to converge on the same cached object.	
customForwardHostHeader	string (allows [variables](#))	This specifies the name of the custom host header the edge server should pass to the origin.	`forwardHostHeader` is `CUSTOM`

Option	Type	Description	Requires
cacheKey Hostname	enum	Specifies the hostname to use when forming a cache key.	`originType` is either: `CUSTOMER`, `SAAS_DYNAMIC_ORIGIN`
	`REQUEST_HOST_ HEADER`	Specify when using a virtual server.	
	`ORIGIN_ HOSTNAME`	Specify if your origin server's responses do not depend on the hostname.	
ipVersion	enum	Specifies which IP version to use when getting content from the origin.	`originType` is either: `CUSTOMER`, `EDGE_ LOAD_BALANCING_ ORIGIN_GROUP`
	`IPV4`	Use IPv4.	
	`DUALSTACK`	Use both versions.	
	`IPV6`	Use IPv6.	
useUniqueCache Key	boolean	With a shared `hostname` such as provided by Amazon AWS, sets a unique cache key for your content.	
compress	boolean	Enables *gzip* compression for non-NetStorage origins.	`originType` is either: `CUSTOMER`, `EDGE_ LOAD_BALANCING_ ORIGIN_GROUP`, `SAAS_DYNAMIC_ ORIGIN`
enableTrueClient Ip	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`
trueClientIp Header	string	This specifies the name of the field that identifies the end client's IP address, for example `True-Client-IP`.	`enableTrueClientIp` is `true`
trueClientIp ClientSetting	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`
	`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 *Secure Delivery - Customer Cert* module. See the verification settings in the Origin Server behavior or contact your Akamai representative for details.	
	`THIRD_PARTY`	When your origin server references certain types of third-party hostname.	

Option	Type	Description	Requires
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. See the [verification settings in the Origin Server behavior](#) or contact your Akamai representative for more information.	`originType` is either: `CUSTOMER`, `EDGE_LOAD_BALANCING_ORIGIN_GROUP`, `SAAS_DYNAMIC_ORIGIN` AND `verificationMode` is either: `PLATFORM_SETTINGS`, `CUSTOM`, `THIRD_PARTY`
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.)	`verificationMode` is `CUSTOM`
originCertsToHonor	enum	Specifies which certificate to trust.	`verificationMode` 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. See the [verification settings in the Origin Server behavior](#) or 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. See the [verification settings in the Origin Server behavior](#) or 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`

originCharacteristics

- **Property Manager name**: Origin Characteristics
- **Behavior version**: The `v2023-05-30` rule format supports the `originCharacteristics` behavior v1.7.
- **Rule format status**: Deprecated, outdated rule format
- **Access**: Read-write
- **Allowed in includes**: No (temporarily)

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 *content Characteristics*.

Option	Type	Description	Requires
authentication Method	enum	Specifies the authentication method.	
	`AUTOMATIC`	Use default authentiation.	
	`SIGNATURE_ HEADER_ AUTHENTICATION`	Available with the Adaptive Media Delivery product.	
	`MSL_ AUTHENTICATION`	Available with the Adaptive Media Delivery product.	
	`AWS`	Amazon Web Services. If you're using this authentication method, any `chase Redirects` behavior you specify gets automatically disabled.	
	`GCS_HMAC_ AUTHENTICATION`	Google Cloud Platform. If you're using this authentication method, any `chase Redirects` behavior you specify gets automatically disabled.	
encoding Version	enum	Specifies the version of the encryption algorithm, an integer from `1` to `5`.	authentication Method is `SIGNATURE_ HEADER_ AUTHENTICATION`
useCustom SignString	boolean	Specifies whether to customize your signed string.	authentication Method is `SIGNATURE_ HEADER_ AUTHENTICATION`
customSign String	string array	Specifies the data to be encrypted as a series of enumerated variable names. See Built-in system variables for guidance on each.	authentication Method is `SIGNATURE_ HEADER_ AUTHENTICATION` AND `useCustom SignString` is `true`
		Supported values: AK_CLIENT_REAL_IP AK_DOMAIN AK_EXTENSION	
secretKey	object array	Specifies the shared secret key.	authentication Method is `SIGNATURE_ HEADER_ AUTHENTICATION`

Option	Type	Description	Requires
nonce	string	Specifies the nonce.	authentication Method is SIGNATURE_ HEADER_ AUTHENTICATION
mslkey	string	Specifies the access key provided by the hosting service.	authentication Method is MSL_ AUTHENTICATION
mslname	string	Specifies the origin name provided by the hosting service.	authentication Method is MSL_ AUTHENTICATION
accessKey Encrypted Storage	boolean	Enables secure use of access keys defined in Cloud Access Manager. Access keys store encrypted authentication details required to sign requests to cloud origins. If you disable this option, you'll need to store the authentication details unencrypted.	authentication Method is either: AWS , GCS_HMAC_ AUTHENTICATION
gcsAccessKey VersionGuid	string	Identifies the unique gcsAccessKeyVersionGuid access key created in Cloud Access Manager to sign your requests to Google Cloud Storage in interoperability mode.	authentication Method is GCS_ HMAC_ AUTHENTICATION AND accessKey EncryptedStorage is true
gcsHmacKey AccessId	string	Specifies the active access ID linked to your Google account.	authentication Method is GCS_ HMAC_ AUTHENTICATION AND accessKey EncryptedStorage is not true
gcsHmacKey Secret	string	Specifies the secret linked to the access ID that you want to use to sign requests to Google Cloud Storage.	authentication Method is GCS_ HMAC_ AUTHENTICATION AND accessKey EncryptedStorage is not true
awsAccessKey VersionGuid	string	Identifies the unique awsAccessKeyVersionGuid access key created in Cloud Access Manager to sign your requests to AWS S3.	authentication Method is AWS AND accessKey EncryptedStorage is true
awsAccessKey Id	string	Specifies active access key ID linked to your AWS account.	authentication Method is AWS AND accessKey EncryptedStorage is not true
awsSecret AccessKey	string	Specifies the secret linked to the access key identifier that you want to use to sign requests to AWS.	authentication Method is AWS AND accessKey EncryptedStorage is not true
awsRegion	string	This specifies the AWS region code of the location where your bucket resides.	authentication Method is AWS
awsHost	string	This specifies the AWS hostname, without http:// or https:// prefixes. If you leave this option empty, it inherits the hostname from the origin behavior.	authentication Method is AWS
awsService	string	This specifies the subdomain of your AWS service. It precedes amazonaws.com or the region code in the AWS hostname. For example, s3.amazonaws.com .	authentication Method is AWS

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.	
	ADC	Akamai Direct Connection, available to Adaptive Media Delivery customers.	
directConnectGeo	string	Provides a region used by Akamai Direct Connection.	country is ADC

originCharacteristicsWsd

- **Property Manager name**: Origin Characteristics

- **Behavior version**: The `v2023-05-30` rule format supports the `originCharacteristicsWsd` behavior v1.0.
- **Rule format status**: Deprecated, outdated rule format
- **Access**: Read-write
- **Allowed in includes**: Yes

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

Option	Type	Description
origintype	enum	Specifies an origin type.
	AZURE	An Azure origin type.
	UNKNOWN	An unknown origin type.

originFailureRecoveryMethod

- **Property Manager name**: Origin Failure Recovery Method
- **Behavior version**: The `v2023-05-30` rule format supports the `originFailureRecoveryMethod` behavior v1.0.
- **Rule format status**: Deprecated, outdated rule format
- **Access**: Read-write
- **Allowed in includes**: Yes

Origin Failover requires that you set up a separate rule containing origin failure recovery methods. You also need to set up the Origin Failure Recovery Policy behavior in a separate rule with a desired match criteria, and select the desired failover method. You can do this using Property Manager. Learn more about this process in Adaptive Media Delivery Implementation Guide. You can use the `originFailureRecoveryPolicy` member to edit existing instances of the Origin Failure Recover Policy behavior.

Option	Type	Description	Requires
recoveryMethod	enum	Specifies the recovery method.	
	RETRY_ALTERNATE_ ORIGIN	Retry with the alternate origin.	
	RESPOND_CUSTOM_ STATUS	Customize the response.	
customStatus Code	string	Specifies the custom status code to be sent to the client.	`recoveryMethod` is `RESPOND_CUSTOM_ STATUS`

originFailureRecoveryPolicy

- **Property Manager name**: [Origin Failure Recovery Policy](#)
- **Behavior version**: The `v2023-05-30` rule format supports the `originFailureRecoveryPolicy` behavior v1.0.
- **Rule format status**: [Deprecated, outdated rule format](#)
- **Access**: [Read-write](#)
- **Allowed in includes**: [Yes](#)

Configures how to detect an origin failure, in which case the `originFailureRecoveryMethod` behavior applies. You can also define up to three sets of criteria to detect origin failure based on specific response codes. Use it to apply specific retry or recovery actions. You can do this using Property Manager. Learn more about this process in [Adaptive Media Delivery Implementation Guide](#). You can use the `originFailureRecoveryMethod` member to edit existing instances of the Origin Failure Recover Method behavior.

Option	Type	Description	Requires
enabled	boolean	Activates and configures a recovery policy.	
enable IPAvoidance	boolean	Temporarily blocks an origin IP address that experienced a certain number of failures. When an IP address is blocked, the `configName` established for `origin ResponsivenessRecoveryConfigName` is applied.	
ipAvoidance ErrorThreshold	number	Defines the number of failures that need to occur to an origin address before it's blocked.	enable IPAvoidance is true
ipAvoidance RetryInterval	number	Defines the number of seconds after which the IP address is removed from the blocklist.	enable IPAvoidance is true
binary Equivalent Content	boolean	Synchronizes content between the primary and backup origins, byte for byte.	
monitorOrigin Responsiveness	boolean	Enables continuous monitoring of connectivity to the origin. If necessary, applies retry or recovery actions.	
origin Responsiveness Timeout	enum	The timeout threshold that triggers a retry or recovery action.	monitorOrigin Responsiveness is true
	AGGRESSIVE	A 2 second threshold.	
	MODERATE	3 seconds.	
	CONSERVATIVE	4 seconds.	
	USER_ SPECIFIED	Specify your own timeout.	
origin Responsiveness CustomTimeout	number	Specify a custom timeout, from 1 to 10 seconds.	origin Responsiveness Timeout is USER_ SPECIFIED
origin Responsiveness EnableRetry	boolean	If a specific failure condition applies, attempts a retry on the same origin before executing the recovery method.	monitorOrigin Responsiveness is true
origin Responsiveness EnableRecovery	boolean	Enables a recovery action for a specific failure condition.	monitorOrigin Responsiveness is true

Option	Type	Description	Requires
origin Responsiveness RecoveryConfig Name	string	Specifies a recovery configuration using the `configName` you defined in the `recovery Config` match criteria. Specify 3 to 20 alphanumeric characters or dashes. Ensure that you use the `recoveryConfig` match criteria to apply this option.	origin Responsiveness EnableRecovery is `true`
monitorStatus Codes1	boolean	Enables continuous monitoring for the specific origin status codes that trigger retry or recovery actions.	
monitor Response Codes1	string array	Defines the origin response codes that trigger a subsequent retry or recovery action. Specify a single code entry (`501`) or a range (`501:504`). If you configure other `monitorStatusCodes*` and `monitorResponseCodes*` options, you can't use the same codes here.	monitorStatus Codes1 is `true`
monitorStatus Codes1Enable Retry	boolean	When the defined response codes apply, attempts a retry on the same origin before executing the recovery method.	monitorStatus Codes1 is `true`
monitorStatus Codes1Enable Recovery	boolean	Enables the recovery action for the response codes you define.	monitorStatus Codes1 is `true`
monitorStatus Codes1Recovery ConfigName	string	Specifies a recovery configuration using the `configName` you defined in the `recovery Config` match criteria. Specify 3 to 20 alphanumeric characters or dashes. Ensure that you use the `recoveryConfig` match criteria to apply this option.	monitorStatus Codes1Enable Recovery is `true`
monitorStatus Codes2	boolean	Enables continuous monitoring for the specific origin status codes that trigger retry or recovery actions.	
monitor Response Codes2	string array	Defines the origin response codes that trigger a subsequent retry or recovery action. Specify a single code entry (`501`) or a range (`501:504`). If you configure other `monitorStatusCodes*` and `monitorResponseCodes*` options, you can't use the same codes here.	monitorStatus Codes2 is `true`
monitorStatus Codes2Enable Retry	boolean	When the defined response codes apply, attempts a retry on the same origin before executing the recovery method.	monitorStatus Codes2 is `true`
monitorStatus Codes2Enable Recovery	boolean	Enables the recovery action for the response codes you define.	monitorStatus Codes2 is `true`
monitorStatus Codes2Recovery ConfigName	string	Specifies a recovery configuration using the `configName` you defined in the `recovery Config` match criteria. Specify 3 to 20 alphanumeric characters or dashes. Ensure that you use the `recoveryConfig` match criteria to apply this option.	monitorStatus Codes2Enable Recovery is `true`
monitorStatus Codes3	boolean	Enables continuous monitoring for the specific origin status codes that trigger retry or recovery actions.	
monitor Response Codes3	string array	Defines the origin response codes that trigger a subsequent retry or recovery action. Specify a single code entry (`501`) or a range (`501:504`). If you configure other `monitorStatusCodes*` and `monitorResponseCodes*` options, you can't use the same codes here..	monitorStatus Codes3 is `true`
monitorStatus Codes3Enable Retry	boolean	When the defined response codes apply, attempts a retry on the same origin before executing the recovery method.	monitorStatus Codes3 is `true`
monitorStatus Codes3Enable Recovery	boolean	Enables the recovery action for the response codes you define.	monitorStatus Codes3 is `true`
monitorStatus Codes3Recovery ConfigName	string	Specifies a recovery configuration using the `configName` you defined in the `recovery Config` match criteria. Specify 3 to 20 alphanumeric characters or dashes. Ensure that you use the `recoveryConfig` match criteria to apply this option.	monitorStatus Codes3Enable Recovery is `true`

originIpAcl

- **Property Manager name**: Origin IP Access Control List
- **Behavior version**: The `v2023-05-30` rule format supports the `originIpAcl` behavior v1.0.
- **Rule format status**: Deprecated, outdated rule format
- **Access**: Read-write
- **Allowed in includes**: Yes

Origin IP Access Control List limits the traffic to your origin. It only allows requests from specific edge servers that are configured as part of a supernet defined by CIDR blocks.

Option	Type	Description
enable	boolean	Enables the Origin IP Access Control List behavior.

persistentClientConnection

- **Property Manager name**: Persistent Connections: Client to Edge
- **Behavior version**: The `v2023-05-30` rule format supports the `persistentClientConnection` behavior v1.1.
- **Rule format status**: Deprecated, outdated rule format
- **Access**: Read-only
- **Allowed in includes**: Yes

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.

This behavior is only supported with the HTTP/1.1 networking protocol that's automatically enabled in all properties. If you include this behavior in the same rule with `http2` or `http3`, edge servers honor requests using either of these protocols, but the settings specified in the `persistentClientConnection` behavior won't apply. Both `http2` and `http3` apply persistent connections automatically.

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

Option	Type	Description
enabled	boolean	Enables the persistent connections behavior.

Option	Type	Description
timeout	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 `v2023-05-30` rule format supports the `persistentConnection` behavior v1.1.
- **Rule format status**: [Deprecated, outdated rule format](#)
- **Access**: [Read-only](#)
- **Allowed in includes**: [Yes](#)

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 `v2023-05-30` rule format supports the `personallyIdentifiableInformation` behavior v1.2.
- **Rule format status**: [Deprecated, outdated rule format](#)
- **Access**: [Read-write](#)
- **Allowed in includes**: [No (temporarily)](#)

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 `v2023-05-30` rule format supports the `phasedRelease` behavior v2.0.
- **Rule format status**: [Deprecated, outdated rule format](#)
- **Access**: [Read-write](#)
- **Allowed in includes**: [No (temporarily)](#)

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.	
isShared Policy	boolean	Whether you want to apply the Cloudlet shared policy to an unlimited number of properties within your account. Learn more about shared policies and how to create them in [Cloudlets Policy Manager](#).	
cloudlet Policy	object	Specifies the Cloudlet policy as an object.	isShared Policy is false
cloudlet Policy.id	number	Identifies the Cloudlet.	
cloudlet Policy.name	string	The Cloudlet's descriptive name.	
cloudlet Shared Policy	string	Identifies the Cloudlet shared policy to use with this behavior. Use the [Cloudlets API](#) to list available shared policies.	isShared Policy is true
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 *random* membership option, it overrides this option's value so that it is effectively `NONE`.	
	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 CookieType 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 CookieType is DURATION
population Refresh	boolean	Enabling this option resets the original duration of the cookie if the browser refreshes before the cookie expires.	population CookieType 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.	

Option	Type	Description	Requires
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 `v2023-05-30` rule format supports the `preconnect` behavior v1.0.
- **Rule format status**: [Deprecated, outdated rule format](#)
- **Access**: [Read-write](#)
- **Allowed in includes**: [Yes](#)

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
preconnectlist	string array	Specifies the set of hostnames to which to preconnect over HTTP2.

predictiveContentDelivery

- **Property Manager name**: [Predictive Content Delivery](#)
- **Behavior version**: The `v2023-05-30` rule format supports the `predictiveContentDelivery` behavior v1.0.
- **Rule format status**: [Deprecated, outdated rule format](#)
- **Access**: [Read-write](#)
- **Allowed in includes**: [Yes](#)

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 [segmentedMedia Optimization](#) behavior, the value for `behavior` is set to `LIVE`.

Option	Type	Description
enabled	boolean	Enables the predictive content delivery behavior.

predictivePrefetching

- **Property Manager name**: Predictive Prefetching
- **Behavior version**: The `v2023-05-30` rule format supports the `predictivePrefetching` behavior v1.1.
- **Rule format status**: Deprecated, outdated rule format
- **Access**: Read-write
- **Allowed in includes**: Yes

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 `v2023-05-30` rule format supports the `prefetch` behavior v1.1.
- **Rule format status**: Deprecated, outdated rule format
- **Access**: Read-write
- **Allowed in includes**: Yes

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 `v2023-05-30` rule format supports the `prefetchable` behavior v1.1.
- **Rule format status**: Deprecated, outdated rule format
- **Access**: Read-write
- **Allowed in includes**: Yes

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 `v2023-05-30` rule format supports the `prefreshCache` behavior v1.2.
- **Rule format status**: Deprecated, outdated rule format
- **Access**: Read-write
- **Allowed in includes**: Yes

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 prefresh 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 prefresh 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` prefreshes the content without unnecessarily increasing load on the origin.

quicBeta

- **Property Manager name**: QUIC Support (Beta)
- **Behavior version**: The `v2023-05-30` rule format supports the `quicBeta` behavior v1.0.
- **Rule format status**: Deprecated, outdated rule format
- **Access**: Read-write
- **Allowed in includes**: No (temporarily)

For a share of responses, includes an `Alt-Svc` header for compatible clients to initiate subsequent sessions using the QUIC protocol.

Option	Type	Description
enabled	boolean	Enables QUIC support.
quicOfferPercentage	number (1-50)	The percentage of responses for which to allow QUIC sessions.

randomSeek

- **Property Manager name**: Random Seek
- **Behavior version**: The `v2023-05-30` rule format supports the `randomSeek` behavior v1.2.
- **Rule format status**: Deprecated, outdated rule format
- **Access**: Read-write
- **Allowed in includes**: Yes

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 `MB` or `GB`.	`mp4` is true

rapid

- **Property Manager name**: Akamai API Gateway
- **Behavior version**: The `v2023-05-30` rule format supports the `rapid` behavior v1.0.
- **Rule format status**: Deprecated, outdated rule format
- **Access**: Read-write
- **Allowed in includes**: No (temporarily)

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
enabled	boolean	Enables API Gateway for the current set of content.

readTimeout

- **Property Manager name**: Read Timeout
- **Behavior version**: The `v2023-05-30` rule format supports the `readTimeout` behavior v1.1.
- **Rule format status**: Deprecated, outdated rule format
- **Access**: Read-write
- **Allowed in includes**: Yes

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

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

realTimeReporting

- **Property Manager name**: Real-time Reporting
- **Behavior version**: The `v2023-05-30` rule format supports the `realTimeReporting` behavior v1.0.
- **Rule format status**: Deprecated, outdated rule format
- **Access**: Read-only
- **Allowed in includes**: Yes

This enables Real-Time Reporting for Akamai Cloud Embed customers. The behavior can only be configured on your behalf by Akamai Professional Services.

Option	Type	Description	Requires
enabled	boolean	Enables reports on delivery of cloud hosted content at near real-time latencies.	
advanced	boolean	Enables advanced options.	
beaconSampling Percentage	number	Specifies the percentage for sampling.	`advanced` is `true`

realUserMonitoring

- **Property Manager name**: Real User Monitoring (RUM)
- **Behavior version**: The `v2023-05-30` rule format supports the `realUserMonitoring` behavior v1.3.
- **Rule format status**: Deprecated, outdated rule format
- **Access**: Read-write
- **Allowed in includes**: No (temporarily)

This behavior is deprecated, but you should not disable or remove it if present.

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
enabled	boolean	When enabled, activates real-use monitoring.

redirect

- **Property Manager name**: [Redirect](#)
- **Behavior version**: The `v2023-05-30` rule format supports the `redirect` behavior v1.5.
- **Rule format status**: [Deprecated, outdated rule format](#)
- **Access**: [Read-write](#)
- **Allowed in includes**: [Yes](#)

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](#)
mobileDefault Choice	enum	Either specify a default response for mobile browsers, or customize your own.	
	`DEFAULT`	Allows all other `responseCode` values.	
	`MOBILE`	Allows only a 302 response code.	
destination Protocol	enum	Choose the protocol for the redirect URL.	
	`SAME_AS_ REQUEST`	Pass through the original protocol.	
	`HTTP`	Use `http`.	
	`HTTPS`	Use `https`.	
destination Hostname	enum	Specify how to change the requested hostname, independently from the pathname.	
	`SAME_AS_ REQUEST`	Preserves the hostname unchanged.	
	`SUBDOMAIN`	Prepends a subdomain from the `destinationHostnameSubdomain` field.	
	`SIBLING`	Replaces the leftmost subdomain with the `destinationHostnameSibling` field.	
	`OTHER`	Specifies a static domain in the `destinationHostnameOther` field.	
destination Hostname Subdomain	string (allows [variables](#))	Specifies a subdomain to prepend to the current hostname. For example, a value of `m` changes `www.example.com` to `m.www.example.com`.	destination Hostname is `SUBDOMAIN`

Option	Type	Description	Requires
destination Hostname Sibling	string (allows variables)	Specifies the subdomain with which to replace to the current hostname's leftmost subdomain. For example, a value of `m` changes `www.example.com` to `m.example. com` .	destination Hostname is `SIBLING`
destination Hostname Other	string (allows variables)	Specifies the full hostname with which to replace the current hostname.	destination Hostname is `OTHER`
destination Path	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 `destinationPathPrefix` field. You also have the option to specify a suffix using `destinationPathSuffix` and `destinationPathSuffixStatus` .	
	`OTHER`	Replaces the current path with the `destinationPathOther` field.	
destination PathPrefix	string (allows variables)	When `destinationPath` is set to `PREFIX_REQUEST` , this prepends the current path. For example, a value of `/prefix/path` changes `/example/index.html` to `/prefix/path/example/index.html` .	destinationPath is `PREFIX_ REQUEST`
destination PathSuffix Status	enum	When `destinationPath` is set to `PREFIX_REQUEST` , this gives you the option of adding a suffix.	destinationPath is `PREFIX_ REQUEST`
	`NO_SUFFIX`	Specify if you want to preserve the end of the path unchanged.	
	`SUFFIX`	The `destinationPathSuffix` provides the value.	
destination PathSuffix	string (allows variables)	When `destinationPath` is set to `PREFIX_REQUEST` and `destinationPathSuffixStatus` is set to `SUFFIX` , this specifies the suffix to append to the path.	destinationPath SuffixStatus is `SUFFIX`
destination PathOther	string (allows variables)	When `destinationPath` is set to `PREFIX_REQUEST` , this replaces the current path.	destinationPath is `OTHER`
queryString	boolean	When set to `APPEND` , passes incoming query string parameters as part of the redirect URL. Otherwise set this to `IGNORE` .	
response Code	enum	Specify the redirect's response code.	
		Supported values: 301 302 303 307	

redirectplus

- **Property Manager name**: Redirect Plus
- **Behavior version**: The `v2023-05-30` rule format supports the `redirectplus` behavior v1.2.
- **Rule format status**: Deprecated, outdated rule format
- **Access**: Read-write
- **Allowed in includes**: Yes

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
enabled	boolean	Enables the redirect feature.
destination	string (allows [variables](#))	Specifies the redirect as a path expression starting with a `/` 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: `/path/to/{{builtin.AK_FILENAME}}` .
response Code	enum	Assigns the status code for the redirect response.
		Supported values:
		301 302 303 307

refererChecking

- **Property Manager name**: [Legacy Referrer Checking](#)
- **Behavior version**: The `v2023-05-30` rule format supports the `refererChecking` behavior v1.1.
- **Rule format status**: [Deprecated, outdated rule format](#)
- **Access**: [Read-write](#)
- **Allowed in includes**: [Yes](#)

Limits allowed requests to a set of domains you specify.

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

removeQueryParameter

- **Property Manager name**: [Remove Outgoing Request Parameters](#)
- **Behavior version**: The `v2023-05-30` rule format supports the `removeQueryParameter` behavior v1.1.
- **Rule format status**: [Deprecated, outdated rule format](#)
- **Access**: [Read-write](#)
- **Allowed in includes**: [Yes](#)

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 `v2023-05-30` rule format supports the `removeVary` behavior v1.1.
- **Rule format status**: [Deprecated, outdated rule format](#)
- **Access**: [Read-write](#)
- **Allowed in includes**: [Yes](#)

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 `v2023-05-30` rule format supports the `report` behavior v1.6.

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

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

Option	Type	Description	Requires
logHost	boolean	Log the `Host` header.	
logReferer	boolean	Log the `Referer` header.	
logUser Agent	boolean	Log the `User-Agent` header.	
logAccept Language	boolean	Log the `Accept-Language` header.	
log Cookies	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.	`log Cookies` is `SOME`
logCustom LogField	boolean	Whether to append additional custom data to each log line.	
customLog Field	string (allows [variables](#))	Specifies an additional data field to append to each log line, maximum 1000 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.	`logCustom LogField` is `true`
logEdgeIP	boolean	Whether to log the IP address of the Akamai edge server that served the response to the client.	
log XForwarded For	boolean	Log any `X-Forwarded-For` request header.	

requestControl

- **Property Manager name**: [Request Control Cloudlet](#)
- **Behavior version**: The `v2023-05-30` rule format supports the `requestControl` behavior v4.0.
- **Rule format status**: [Deprecated, outdated rule format](#)
- **Access**: [Read-write](#)
- **Allowed in includes**: [No (temporarily)](#)

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.	
isSharedPolicy	boolean	Whether you want to apply the Cloudlet shared policy to an unlimited number of properties within your account. Learn more about shared policies and how to create them in Cloudlets Policy Manager.	
cloudletPolicy	object	Identifies the Cloudlet policy.	isSharedPolicy is false
cloudletPolicy.id	number	Identifies the Cloudlet.	
cloudletPolicy.name	string	The Cloudlet's descriptive name.	
cloudletSharedPolicy	string	Identifies the Cloudlet shared policy to use with this behavior. Use the Cloudlets API to list available shared policies.	isSharedPolicy is true
enableBranded403	boolean	If enabled, serves a branded 403 page for this Cloudlet instance.	
branded403StatusCode	enum	Specifies the response status code for the branded deny action.	enableBranded403 is true
		Supported values: 200 302 403 503	
netStorage	object	Specifies the NetStorage domain that contains the branded 403 page.	enableBranded403 is true AND branded403StatusCode is not 302
netStorage.cpCode	integer	Identifies a CP code assigned to this storage group.	
netStorage.downloadDomainName	string	Domain name from which content can be downloaded.	
netStorage.g2oToken	string	Signature Header Authentication key.	
netStorage.id	integer	Unique identifier for the storage group.	
netStorage.name	string	Name of the storage group.	
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 branded403StatusCode is not 302
branded403Url	string	Specifies the redirect URL for the branded deny action.	enableBranded403 is true AND branded403StatusCode is 302
brandedDenyCacheTtl	number (5-30)	Specifies the branded response page's time to live in the cache, 5 minutes by default.	enableBranded403 is true AND branded403StatusCode is not 302

requestTypeMarker

- **Property Manager name**: Request Type Marker
- **Behavior version**: The `v2023-05-30` rule format supports the `requestTypeMarker` behavior v1.0.
- **Rule format status**: Deprecated, outdated rule format
- **Access**: Read-write
- **Allowed in includes**: Yes

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 `v2023-05-30` rule format supports the `resourceOptimizer` behavior v1.1.
- **Rule format status**: Deprecated, outdated rule format
- **Access**: Read-write
- **Allowed in includes**: Yes

This behavior is deprecated, but you should not disable or remove it if present.

Use this along with `adaptiveAcceleration` to compress and cache resources such as JavaScript, CSS, and font files.

Option	Type	Description
enabled	boolean	Enables the Resource Optimizer feature.

resourceOptimizerExtendedCompatibility

- **Property Manager name**: [Resource Optimizer Extended Compatibility](#)
- **Behavior version**: The `v2023-05-30` rule format supports the `resourceOptimizerExtendedCompatibility` behavior v1.1.
- **Rule format status**: [Deprecated, outdated rule format](#)
- **Access**: [Read-write](#)
- **Allowed in includes**: [Yes](#)

This enhances the standard version of the `resourceOptimizer` behavior to support the compression of additional file formats and address some compatibility issues.

Option	Type	Description
enabled	boolean	Enables the Resource Optimizer feature.
enableAllFeatures	boolean	Enables [additional support](#) and error handling.

responseCode

- **Property Manager name**: [Set Response Code](#)
- **Behavior version**: The `v2023-05-30` rule format supports the `responseCode` behavior v1.1.
- **Rule format status**: [Deprecated, outdated rule format](#)
- **Access**: [Read-write](#)
- **Allowed in includes**: [Yes](#)

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](#)
statusCode	enum	The HTTP status code to replace the existing one.	
		Supported values: 100 102 122 201 203 205 207 300 302 304 306 308 401 403 405 407 409 101 103 200 202 204 206 226 301 303 305 307 400 402 404 406 408 410	
override206	boolean	Allows any specified `200` success code to override a `206` partial-content code, in which case the response's content length matches the requested range length.	status Code is 200

responseCookie

- **Property Manager name**: Set Response Cookie
- **Behavior version**: The `v2023-05-30` rule format supports the `responseCookie` behavior v1.3.
- **Rule format status**: Deprecated, outdated rule format
- **Access**: Read-write
- **Allowed in includes**: Yes

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

Option	Type	Description	Requires
cookie Name	string (allows variables)	Specifies the name of the cookie, which serves as a key to determine if the cookie is set.	
enabled	boolean	Allows you to set a response cookie.	
type	enum	What type of value to assign.	
	FIXED	Assign a `FIXED` value based on the `value` field.	
	UNIQUE	Assign a unique value.	
value	string (allows variables)	If the cookie `type` is `FIXED`, this specifies the cookie value.	type is FIXED
format	enum	When the `type` of cookie is set to `UNIQUE`, this sets the date format.	type is UNIQUE
	AKAMAI	Akamai format, which adds milliseconds to the date stamp.	
	APACHE	Apache format.	
default Domain	boolean	When enabled, uses the default domain value, otherwise the set specified in the `domain` field.	
default Path	boolean	When enabled, uses the default path value, otherwise the set specified in the `path` field.	
domain	string (allows variables)	If the `defaultDomain` is disabled, this sets the domain for which the cookie is valid. For example, `example.com` makes the cookie valid for that hostname and all subdomains.	default Domain is false
path	string (allows variables)	If the `defaultPath` 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 `expirationDate` field value.	
	DURATION	Requires a corresponding `duration` field value.	
	NEVER	Let the cookie persist indefinitely.	
expiration Date	string (epoch timestamp)	If `expires` is set to `FIXED_DATE`, this sets when the cookie expires as a UTC date and time.	expires is FIXED_ DATE

Option	Type	Description	Requires
duration	string (duration)	If `expires` is set to `DURATION`, this sets the cookie's lifetime.	`expires` is `DURATION`
sameSite	enum	This option controls the `SameSite` cookie attribute that reduces the risk of cross-site request forgery attacks.	
	DEFAULT	Send the `SameSite` cookie attribute.	
	NONE	Send the cookie in all contexts if the `secure` option is enabled.	
	LAX	Send the cookie also when the user navigates to a URL from an external site.	
	STRICT	Send the cookie only to the same site that originated it.	
secure	boolean	When enabled, sets the cookie's `Secure` flag to transmit it with `HTTPS`.	
httpOnly	boolean	When enabled, includes the `HttpOnly` attribute in the `Set-Cookie` response header to mitigate the risk of client-side scripts accessing the protected cookie, if the browser supports it.	

restrictObjectCaching

- **Property Manager name**: Object Caching
- **Behavior version**: The `v2023-05-30` rule format supports the `restrictObjectCaching` behavior v1.2.
- **Rule format status**: Deprecated, outdated rule format
- **Access**: Read-write
- **Allowed in includes**: Yes

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.

returnCacheStatus

- **Property Manager name**: Return Cache Status
- **Behavior version**: The `v2023-05-30` rule format supports the `returnCacheStatus` behavior v1.0.
- **Rule format status**: Deprecated, outdated rule format
- **Access**: Read-write

- **Allowed in includes**: Yes

Generates a response header with information about cache status. Among other things, this can tell you whether the response came from the Akamai cache, or from the origin. Status values report with either of these forms of syntax, depending for example on whether you're deploying traffic using sureRoute or tieredDistribution :

```
{status} from child
{status} from child, {status} from parent
```

The status value can be any of the following:

- Hit - the object was retrieved from Akamai's cache.
- Miss - the object was not found in the Akamai cache.
- RefreshHit - the object was found in Akamai's cache, but was stale, so an If-Modified-Since request was made to the customer origin, with 304 as the response code, indicating unmodified content.
- HitStale - the object was found in Akamai's cache and was stale, but a more recent object was not available from the customer origin, so the cache served the stale object to the client.
- Constructed - the constructResponse behavior directly specified the response to the client.
- Redirect - the Akamai edge configuration specified a redirect, typically by executing the redirect , redirectplus , or edgeRedirector behaviors.
- Error - an error occurred, typically when authorization is denied or the request is rejected by WAF.

Option	Type	Description
responseHeaderName	string	Specifies the name of the HTTP header in which to report the cache status value.

rewriteUrl

- **Property Manager name**: Modify Outgoing Request Path
- **Behavior version**: The v2023-05-30 rule format supports the rewriteUrl behavior v1.3.
- **Rule format status**: Deprecated, outdated rule format
- **Access**: Read-write
- **Allowed in includes**: Yes

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* that start and end with a / character.

This behavior's rewrite operations can't override any the baseDirectory behavior specifies.

Option	Type	Description	Requires
behavior	enum	The action to perform on the path.	

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

rumCustom

- **Property Manager name**: [RUM SampleRate](#)
- **Behavior version**: The `v2023-05-30` rule format supports the `rumCustom` behavior v1.0.
- **Rule format status**: [Deprecated, outdated rule format](#)
- **Access**: [Read-only](#)
- **Allowed in includes**: [No (temporarily)](#)

This behavior is deprecated, but you should not disable or remove it if present.

With realUserMonitoring enabled, this configures the sample of data to include in your RUM report. The realUser Monitoring behavior is deprecated as well.

Option	Type	Description
rumSample Rate	number (0-100)	Specifies the percentage of web traffic to include in your RUM report.
rumGroup Name	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 v2023-05-30 rule format supports the saasDefinitions behavior v3.1.
- **Rule format status**: Deprecated, outdated rule format
- **Access**: Read-write
- **Allowed in includes**: No (temporarily)

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
customer Action	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.	
customer CnameEnabled	boolean	Enabling this allows you to identify customers using a *CNAME chain* rather than a single hostname.	customerAction is HOSTNAME
customer CnameLevel	number	Specifies the number of CNAMEs to use in the chain.	customerCnameEnabled is true
customer Cookie	string	This specifies the name of the cookie that identifies the customer.	customerAction is COOKIE
customer QueryString	string	This names the query parameter that identifies the customer.	customerAction is QUERY_STRING

Option	Type	Description	Requires
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 CnameEnabled	boolean	Enabling this allows you to identify applications using a *CNAME chain* rather than a single hostname.	`applicationAction` is `HOSTNAME`
application CnameLevel	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 QueryString	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`
usersAction	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.	
usersCname Enabled	boolean	Enabling this allows you to identify users using a *CNAME chain* rather than a single hostname.	`usersAction` is `HOSTNAME`
usersCname Level	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`
usersQuery String	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 `v2023-05-30` rule format supports the `salesForceCommerceCloudClient` behavior v1.2.
- **Rule format status**: [Deprecated, outdated rule format](#)
- **Access**: [Read-write](#)
- **Allowed in includes**: [No (temporarily)](#)

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 *instance-realm-customer*, where *instance* is either `production` or `development` , *realm* is your Salesforce Commerce Cloud service `$REALM` value, and *customer* 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.	
sf3cOriginHostHeader	string (allows [variables](#))	This specifies the hostname or IP address of the custom Salesforce host header.	originHostHeader is CUSTOMER
allowOverrideOriginCacheKey	boolean	When enabled, overrides the forwarding origin's cache key.	

salesForceCommerceCloudProvider

- **Property Manager name**: [Akamai Provider for Salesforce Commerce Cloud](#)
- **Behavior version**: The `v2023-05-30` rule format supports the `salesForceCommerceCloudProvider` behavior v1.0.
- **Rule format status**: [Deprecated, outdated rule format](#)
- **Access**: [Read-write](#)
- **Allowed in includes**: [No (temporarily)](#)

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

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

salesForceCommerceCloudProviderHostHeader

- **Property Manager name**: [Akamai Provider for Salesforce Commerce Cloud Host Header Control](#)
- **Behavior version**: The `v2023-05-30` rule format supports the `salesForceCommerceCloudProviderHostHeader` behavior v1.0.
- **Rule format status**: [Deprecated, outdated rule format](#)
- **Access**: [Read-write](#)
- **Allowed in includes**: [No (temporarily)](#)

Manages host header values sent to the Salesforce Commerce Cloud platform.

Option	Type	Description
hostHeaderSource	enum	Specify where the host header derives from.
	PROPERTY	From this property.
	CUSTOMER	From the customer's property.

savePostDcaProcessing

- **Property Manager name**: [Save POST DCA processing result](#)
- **Behavior version**: The `v2023-05-30` rule format supports the `savePostDcaProcessing` behavior v1.1.
- **Rule format status**: [Deprecated, outdated rule format](#)

- **Access**: [Read-only](#)
- **Allowed in includes**: [Yes](#)

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 `v2023-05-30` rule format supports the `scheduleInvalidation` behavior v1.2.
- **Rule format status**: [Deprecated, outdated rule format](#)
- **Access**: [Read-write](#)
- **Allowed in includes**: [Yes](#)

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 `start` time based on the `repeatInterval` time.	
repeat Interval	string (duration)	Specifies how often to invalidate content from the `start` time, expressed in seconds. For example, an expiration set to midnight and an interval of `86400` seconds invalidates content once a day. Repeating intervals of less than 5 minutes are not allowed for [NetStorage](#) origins.	`repeat` is true
refresh Method	enum	Specifies how to invalidate the content.	
	INVALIDATE	Sends an `If-Modified-Since` 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.	

shutr

- **Property Manager name**: [SHUTR](#)
- **Behavior version**: The `v2023-01-05` rule format supports the `shutr` behavior v1.1.
- **Rule format status**: [Deprecated, outdated rule format](#)
- **Access**: [Read-write](#)
- **Allowed in includes**: [Yes](#)

This behavior is deprecated, but you should not disable or remove it if present.

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.

scriptManagement

- **Property Manager name**: [Script Management](#)
- **Behavior version**: The `v2023-05-30` rule format supports the `scriptManagement` behavior v1.4.
- **Rule format status**: [Deprecated, outdated rule format](#)
- **Access**: [Read-write](#)
- **Allowed in includes**: [No (temporarily)](#)

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

Option	Type	Description	[Requires](#)
enabled	boolean	Enables the Script Management feature.	
serviceworker	enum	Script Management uses a JavaScript service worker called `akam-sw.js`. It applies a policy that helps you manage scripts.	
	YES_ SERVICE_ WORKER	Review insights about script usage, and create a policy to list scripts you want to defer or block. This also installs the `akam-sw.js` service worker for you.	
	NO_ SERVICE_ WORKER	Review insights about script usage. The `akam-sw.js` service worker isn't installed.	
timestamp	number	A read-only epoch timestamp that represents the last time a Script Management policy was synchronized with its Ion property.	`enabled` is never visible

segmentedContentProtection

- **Property Manager name**: Segmented Media Protection
- **Behavior version**: The `v2023-05-30` rule format supports the `segmentedContentProtection` behavior v2.0.
- **Rule format status**: Deprecated, outdated rule format
- **Access**: Read-write
- **Allowed in includes**: Yes

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.	use Advanced 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.	use Advanced is `true`
headerFor Salt	string array	This allows you to include additional salt properties specific to each end user to strengthen the relationship between the session token and playback session. This specifies the set of request headers whose values generate the salt value, typically `User-Agent`, `X-Playback-Session-Id`, and `Origin`. Any specified header needs to appear in the player's request.	use Advanced is `true`
sessionId	boolean	Enabling this option carries the `session_id` value from the access token over to the session token, for use in tracking and counting unique playback sessions.	use Advanced is `true`
data Payload	boolean	Enabling this option carries the `data/payload` field from the access token over to the session token, allowing access to opaque data for log analysis for a URL protected by a session token.	use Advanced is `true`
ip	boolean	Enabling this restricts content access to a specific IP address, only appropriate if it does not change during the playback session.	use Advanced is `true`
acl	boolean	Enabling this option carries the `ACL` field from the access token over to the session token, to limit the requesting client's access to the specific URL or path set in the `ACL` field. Playback may fail if the base path of the master playlist (and variant playlist, plus segments) varies from that of the `ACL` field.	use Advanced is `true`
enable TokenIn URI	boolean	When enabled, passes tokens in HLS variant manifest URLs and HLS segment URLs, as an alternative to cookies.	
hlsMaster Manifest Files	string array	Specifies the set of filenames that form HLS master manifest URLs. You can use `*` wildcard character that matches zero or more characters. Make sure to specify master manifest filenames uniquely, to distinguish them from variant manifest files.	enable TokenIn URI is `true`
token Revocation Enabled	boolean	Enable this to deny requests from playback URLs that contain a `TokenAuth` token that uses specific token identifiers.	

Option	Type	Description	Requires
revoked ListId	string	Identifies the `TokenAuth` tokens to block from accessing your content.	token Revocation Enabled is true
hlsMedia Encryption	boolean	Enables HLS Segment Encryption.	
dash Media Encryption	boolean	Whether to enable DASH Media Encryption.	

segmentedMediaOptimization

- **Property Manager name**: [Segmented Media Delivery Mode](#)
- **Behavior version**: The `v2023-05-30` rule format supports the `segmentedMediaOptimization` behavior v1.3.
- **Rule format status**: [Deprecated, outdated rule format](#)
- **Access**: [Read-write](#)
- **Allowed in includes**: [Yes](#)

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.	
enableUll Streaming	boolean	Enables ultra low latency (ULL) streaming. ULL reduces latency and decreases overall transfer time of live streams.	behavior is 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.	
startTime	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

Option	Type	Description	Requires
dvrType	enum	The type of DVR.	showAdvanced is true
	CONFIGURABLE	A configurable DVR.	
	UNKNOWN	An unknown DVR.	
dvrWindow	string (duration)	Set the duration for your media, or `0m` if a DVR is not required.	showAdvanced is true AND dvrType is CONFIGURABLE

segmentedMediaStreamingPrefetch

- **Property Manager name**: Segmented Media Streaming - Prefetch
- **Behavior version**: The `v2023-05-30` rule format supports the `segmentedMediaStreamingPrefetch` behavior v1.0.
- **Rule format status**: Deprecated, outdated rule format
- **Access**: Read-write
- **Allowed in includes**: Yes

Prefetches HLS and DASH media stream manifest and segment files, accelerating delivery to end users. For prefetching to work, your origin media's response needs to specify `CDN-Origin-Assist-Prefetch-Path` headers with each URL to prefetch, expressed as either a relative or absolute path.

Option	Type	Description
enabled	boolean	Enables media stream prefetching.

setVariable

- **Property Manager name**: Set Variable
- **Behavior version**: The `v2023-05-30` rule format supports the `setVariable` behavior v1.6.
- **Rule format status**: Deprecated, outdated rule format
- **Access**: Read-write
- **Allowed in includes**: Yes

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 `VAR`, its name is preprended with `PMUSER_` and accessible in a `user` namespace, so that you invoke it in subsequent text fields within the rule tree as `{{user.PMUSER_VAR}}`. In deployed [XML metadata](#), it appears as `%(PMUSER_VAR)`.	
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 `new_filename.{{builtin.AK_EXTENSION}}` to embed a system variable.	valueSource is EXPRESSION
extract Location	enum	This specifies from where to get the value.	valueSource is EXTRACT
	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.	
	DEVICE_PROFILE	For client device attributes.	
	RESPONSE_ HEADER	A response header.	
	SET_COOKIE	Cookie.	
certificate FieldName	enum	Specifies the certificate's content.	extractLocation is CLIENT_CERTIFICATE
	VERSION	The certificate's X509 version number.	
	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 *distinguished name* field for the certificate's issuer.	
	SUBJECT_DN	The *distinguished name* 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.	

Option	Type	Description	Requires
	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 (allows [variables](#))	Specifies the case-insensitive name of the HTTP header to extract.	extractLocation is CLIENT_REQUEST_HEADER
response HeaderName	string (allows [variables](#))	Specifies the case-insensitive name of the HTTP header to extract.	extractLocation is RESPONSE_HEADER
setCookie Name	string (allows [variables](#))	Specifies the name of the origin's `Set-Cookie` response header.	extractLocation is SET_ COOKIE
cookieName	string (allows [variables](#))	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.	
	LAT	Latitude.	
	LONG	Longitude.	
	TIMEZONE	Time zone.	
	ZIP	Zip code.	
	CONTINENT	Two-letter continent code.	
	NETWORK	Network name.	
	NETWORK_TYPE	Network type.	

Option	Type	Description	Requires
	ASNUM	Autonomous System Number.	
	THROUGHPUT	Tiered throughput level.	
	BW	Tiered bandwidth level.	
path Component Offset	string (allows variables)	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 (allows variables)	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	Specifies the lower bound of the random number.	generator is `RAND`
maxRandom Number	string	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.	
	BASE_32_DECODE	String encoding.	
	BASE_32_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.	
	EPOCH_TO_STRING	Time format.	
	EXTRACT_PARAM	String format.	
	HASH	Integer data digest.	
	JSON_EXTRACT	JSONPath extraction from a variable.	
	HEX_TO_DECIMAL	Numeric conversion.	
	HEX_DECODE	String conversion.	
	HEX_ENCODE	String conversion.	

Option	Type	Description	Requires
	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.	
	COMPRESS_WHITESPACE	Convert whitespace characters to spaces, then compress multiple space characters into only one.	
	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.	
	BASE_64_URL_DECODE	The same as `BASE_64_DECODE`, except before decoding replaces `+` with `-` and `/` with `_`. If due to the encoding there are not enough characters for the algorithm, this adds `=` characters at the end of the string. See [Output padding](#) for more information.	
	BASE_64_URL_ENCODE	The same as `BASE_64_ENCODE`, except after encoding this removes trailing `=` characters, replacing `+` with `-` and `/` with `_`.	
	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`, `JSON_EXTRACT`
algorithm	enum	Specifies the algorithm to apply.	`transform` is either: `ENCRYPT`, `DECRYPT`
	ALG_3DES	Triple DES.	

Option	Type	Description	Requires
	`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.	
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`

Option	Type	Description	Requires
global Substitution	boolean	Replaces all matches in the string, not just the first.	transform is SUBSTITUTE
startIndex	string	Specifies the zero-based character offset at the start of the substring. Negative indexes specify the offset from the end of the string. Consider this example for a string of abcdefghij : startIndex = 0, endIndex = 1, result = a startIndex = 0, endIndex = 2, Result = ab startIndex = 1, endIndex = 1, Result = <null> startIndex = 1, endIndex = 2, Result = b startIndex = 3, endIndex = -1, Result = defghij startIndex = -2, endIndex = -1, Result = j	transform is SUBSTRING
endIndex	string	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. Consider this example for a string of abcdefghij : startIndex = 0, endIndex = 1, result = a startIndex = 0, endIndex = 2, Result = ab startIndex = 1, endIndex = 1, Result = <null> startIndex = 1, endIndex = 2, Result = b startIndex = 3, endIndex = -1, Result = defghij startIndex = -2, endIndex = -1, Result = j	transform is SUBSTRING
exceptChars	string	Specifies characters *not* 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
device Profile	enum	Specifies the client device attribute. Possible values specify information about the client device, including device type, size and browser. For details on fields, see Device Characterization.	extractLocation is DEVICE_PROFILE
	IS_MOBILE	Basic device attributes, boolean.	
	IS_TABLET	Basic device attributes, boolean.	
	IS_WIRELESS_ DEVICE	Basic device attributes, boolean.	
	PHYSICAL_SCREEN_ HEIGHT	Device screen size in millimeters.	
	PHYSICAL_SCREEN_ WIDTH	Device screen size in millimeters.	
	RESOLUTION_ HEIGHT	Device screen size in pixels.	
	RESOLUTION_ WIDTH	Device screen size in pixels.	
	VIEWPORT_WIDTH	Device viewport size in millimeters.	
	BRAND_NAME	Basic device attributes, string values.	
	DEVICE_OS	Basic device attributes, string values.	
	DEVICE_OS_ VERSION	Basic device attributes, string values.	
	DUAL_ ORIENTATION	Whether the display adapts to portrait/landscape orientation.	
	MAX_IMAGE_ HEIGHT	Maximum image size that can be displayed, in pixels.	
	MAX_IMAGE_ WIDTH	Maximum image size that can be displayed, in pixels.	
	MOBILE_BROWSER	Basic device attributes, string values.	

Option	Type	Description	Requires
	`MOBILE_BROWSER_VERSION`	Basic device attributes, string values.	
	`PDF_SUPPORT`	Device support capabilities, boolean.	
	`COOKIE_SUPPORT`	Device support capabilities, boolean.	

simulateErrorCode

- **Property Manager name**: Simulate Error Response Code
- **Behavior version**: The `v2023-05-30` rule format supports the `simulateErrorCode` behavior v1.1.
- **Rule format status**: Deprecated, outdated rule format
- **Access**: Read-write
- **Allowed in includes**: Yes

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

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

siteShield

- **Property Manager name**: SiteShield
- **Behavior version**: The `v2023-05-30` rule format supports the `siteShield` behavior v1.3.
- **Rule format status**: Deprecated, outdated rule format
- **Access**: Read-write

- **Allowed in includes**: [No (temporarily)](#)

This behavior implements the [Site Shield](#) feature, which helps prevent non-Akamai machines from contacting your origin. You get an email with 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
ssmap	object	Identifies the hostname for the Site Shield map. See [Create a Site Shield map](#) for more details. Form an object with a `value` key that references the hostname, for example: `"ssmap":{"value":"ss.akamai.net"}`.

standardTLSMigration

- **Property Manager name**: [Standard TLS Migration](#)
- **Behavior version**: The `v2023-05-30` rule format supports the `standardTLSMigration` behavior v1.0.
- **Rule format status**: [Deprecated, outdated rule format](#)
- **Access**: [Read-write](#)
- **Allowed in includes**: [No (temporarily)](#)

This behavior is deprecated, but you should not disable or remove it if present.

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](#)
enabled	boolean	Allows migration to Standard TLS.	
migrationFrom	enum	What kind of traffic you're migrating from.	
	SHARED_CERT	A shared certificate.	
	NON_SECURE	Non-secure traffic.	
	ENHANCED_SECURE	Enhanced Secure TLS.	
allow HTTPSUpgrade	boolean	Allows temporary upgrade of HTTP traffic to HTTPS.	migrationFrom is NON_SECURE
allow HTTPSDowngrade	boolean	Allow temporary downgrade of HTTPS traffic to HTTP. This removes various `Origin`, `Referer`, `Cookie`, `Cookie2`, `sec-*` and `proxy-*` headers from the request to origin.	migrationFrom is NON_SECURE
migrationStart Time	string (epoch timestamp)	Specifies when to start migrating the cache.	allow HTTPSUpgrade is true OR allow HTTPSDowngrade is true

Option	Type	Description	Requires
migration Duration	number	Specifies the number of days to migrate the cache.	allow HTTPSUpgrade is true OR allow HTTPSDowngrade is true
cacheSharing StartTime	string (epoch timestamp)	Specifies when to start cache sharing.	migrationFrom is ENHANCED_ SECURE
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.	

standardTLSMigrationOverride

- **Property Manager name**: Standard TLS Migration Override
- **Behavior version**: The `v2023-05-30` rule format supports the `standardTLSMigrationOverride` behavior v1.0.
- **Rule format status**: Deprecated, outdated rule format
- **Access**: Read-only
- **Allowed in includes**: No (temporarily)

This behavior is deprecated, but you should not disable or remove it if present.

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.

strictHeaderParsing

- **Property Manager name**: [Strict Header Parsing](#)
- **Behavior version**: The `v2023-05-30` rule format supports the `strictHeaderParsing` behavior v1.1.
- **Rule format status**: [Deprecated, outdated rule format](#)
- **Access**: [Read-write](#)
- **Allowed in includes**: [Yes](#)

This behavior specifies how the edge servers should handle requests containing improperly formatted or invalid headers that don't comply with [RFC 9110](#)⧉.

Some clients may send invalid or incorrectly-formatted, non-RFC-compliant request headers. If such requests reach the origin server, this vulnerability can be exploited by a "bad actor", for example to poison your cache and cause invalid content to be returned to your end users. Use Strict Header Parsing to tell the edge servers what requests to reject, independently of the Akamai platform's default behavior. Therefore, you may either get the protection earlier than the global customer base or defer changes to a later time, though not recommended. Note that the two modes are independent – each of them concerns different issues with the request headers. For both options, a warning is written to the edge server logs whether the option is enabled or disabled.

As Akamai strives to be fully RFC-compliant, you should enable both options as best practice.

Enabling both options ensures that Akamai edge servers reject requests with invalid headers and don't forward them to your origin. In such cases, the end user receives a 400 Bad Request HTTP response code.

Option	Type	Description
valid Mode	boolean	Rejects requests made with non-RFC-compliant headers that contain invalid characters in the header name or value or which contain invalidly-folded header lines. When disabled, the edge servers allow such requests, passing the invalid headers to the origin server unchanged.
strict Mode	boolean	Rejects requests made with non-RFC-compliant, improperly formatted headers, where the header line starts with a colon, misses a colon or doesn't end with CR LF. When disabled, the edge servers allow such requests, but correct the violation by removing or rewriting the header line before passing the headers to the origin server.

subCustomer

- **Property Manager name**: [Subcustomer Enablement](#)

- **Behavior version**: The `v2023-05-30` rule format supports the `subCustomer` behavior v1.6.
- **Rule format status**: Deprecated, outdated rule format
- **Access**: Read-write
- **Allowed in includes**: No (temporarily)

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.	
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 `suffix.example.com`, then to purge `subcustomer.com/some/path`, specify `subcustomer.com.suffix.example.com/some/path` as the purge request's URL.	`origin` is true
caching	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.	
web Application Firewall	boolean	Web application firewall (WAF) filters, monitors, and blocks certain HTTP traffic. Use Akamai Cloud Embed to add a specific behavior to a subcustomer policy and configure how WAF protection is applied.	

sureRoute

- **Property Manager name**: [SureRoute](#)
- **Behavior version**: The `v2023-05-30` rule format supports the `sureRoute` behavior v1.5.
- **Rule format status**: [Deprecated, outdated rule format](#)
- **Access**: [Read-write](#)
- **Allowed in includes**: [No (temporarily)](#)

The [SureRoute](#) feature continually tests different routes between origin and edge servers to identify the optimal path. By default, it conducts *races* 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
enabled	boolean	Enables the SureRoute behavior, to optimize delivery of non-cached content.	
type	enum	Specifies the set of edge servers used to test routes.	
	PERFORMANCE	Use the default set of edge servers.	
	CUSTOM_MAP	A custom map that you need to get from Akamai Professional Services.	
custom Map	string	If `type` is `CUSTOM_MAP`, this specifies the map string provided to you by Akamai Professional Services, or included as part of the [Site Shield](#) product.	`type` is `CUSTOM_MAP`
test Object Url	string	Specifies the path and filename for your origin's test object to use in races to test routes. 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 `200` HTTP response and does not require authentication. The file should be an average-sized static HTML file (`Content-Type: text/html`) that is no smaller than 8KB, with no back-end processing. 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.	
toHost Status	enum	Specifies which hostname to use.	
	INCOMING_HH	Use the incoming `Host` header when requesting the SureRoute test object.	
	OTHER	Use `toHost` to specify a custom `Host` header.	
toHost	string	If `toHostStatus` is `OTHER`, this specifies the custom `Host` header to use when requesting the SureRoute test object.	`toHost Status` is `OTHER`
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.	

Option	Type	Description	Requires
enable Custom Key	boolean	When disabled, caches race results under the race destination's hostname. If enabled, use `customStatKey` 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

tcpOptimization

- **Property Manager name**: TCP Optimizations
- **Behavior version**: The `v2023-05-30` rule format supports the `tcpOptimization` behavior v1.1.
- **Rule format status**: Deprecated, outdated rule format
- **Access**: Read-write
- **Allowed in includes**: Yes

This behavior is deprecated, but you should not disable or remove it if present.

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.

teaLeaf

- **Property Manager name**: IBM Tealeaf Connector
- **Behavior version**: The `v2023-05-30` rule format supports the `teaLeaf` behavior v1.0.
- **Rule format status**: Deprecated, outdated rule format
- **Access**: Read-write
- **Allowed in includes**: No (temporarily)

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

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

tieredDistribution

- **Property Manager name**: Tiered Distribution
- **Behavior version**: The v2023-05-30 rule format supports the tieredDistribution behavior v1.3.
- **Rule format status**: Deprecated, outdated rule format
- **Access**: Read-write
- **Allowed in includes**: No (temporarily)

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.	
	CHAUS	Australia.	
	CH	A global map.	

tieredDistributionAdvanced

- **Property Manager name**: [Tiered Distribution (Advanced)](#)
- **Behavior version**: The `v2023-05-30` rule format supports the `tieredDistributionAdvanced` behavior v1.0.
- **Rule format status**: [Deprecated, outdated rule format](#)
- **Access**: [Read-only](#)
- **Allowed in includes**: [Yes](#)

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 `tieredDistribution` .

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

tieredDistributionCustomization

- **Property Manager name**: [Tiered Distribution Customization](#)
- **Behavior version**: The `v2023-05-30` rule format supports the `tieredDistributionCustomization` behavior v1.1.
- **Rule format status**: [Deprecated, outdated rule format](#)
- **Access**: [Read-only](#)
- **Allowed in includes**: [Yes](#)

With Tiered Distribution, Akamai edge servers retrieve cached content from other Akamai servers, rather than directly from the origin. This behavior sets custom Tiered Distribution maps (TD0) and migrates TD1 maps configured with [advanced features](#) to Cloud Wrapper. You need to enable `cloudWrapper` within the same rule.

Option	Type	Description	[Requires](#)
`custom Map Enabled`	boolean	Enables custom maps.	

Option	Type	Description	Requires
custom Map Name	string (allows variables)	Specifies the custom map name.	custom Map Enabled is true
serial Start	string	Specifies a numeric serial start value.	custom Map Enabled is true
serial End	string	Specifies a numeric serial end value. Akamai uses serial numbers to group machines and share objects in their cache with other machines in the same region.	custom Map Enabled is true
hash Algorithm	enum	Specifies the hash algorithm.	custom Map Enabled is true
	GCC	A GCC hash.	
	JENKINS	A Jenkins hash.	
map Migration Enabled	boolean	Enables migration of the custom map to Cloud Wrapper.	
migration WithinCw Maps Enabled	boolean	Enables migration within Cloud Wrapper maps.	map Migration Enabled is true
location	string	Location from which Cloud Wrapper migration is performed. User should choose the existing Cloud Wrapper location. The new Cloud Wrapper location (to which migration has to happen) is expected to be updated as part of the main "Cloud Wrapper" behavior.	migration WithinCw Maps Enabled is true
migration StartDate	string (epoch timestamp)	Specifies when to start migrating the map.	map Migration Enabled is true
migration EndDate	string (epoch timestamp)	Specifies when the map migration should end.	map Migration Enabled is true

timeout

- **Property Manager name**: Connect Timeout
- **Behavior version**: The `v2023-05-30` rule format supports the `timeout` behavior v1.1.
- **Rule format status**: Deprecated, outdated rule format
- **Access**: Read-write

- **Allowed in includes**: [Yes](#)

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 `v2023-05-30` rule format supports the `uidConfiguration` behavior v1.0.
- **Rule format status**: [Deprecated, outdated rule format](#)
- **Access**: [Read-write](#)
- **Allowed in includes**: [No (temporarily)](#)

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.	
	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](#).	
headerName	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 `v2023-05-30` rule format supports the `validateEntityTag` behavior v1.2.
- **Rule format status**: [Deprecated, outdated rule format](#)
- **Access**: [Read-write](#)
- **Allowed in includes**: [Yes](#)

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.

Note that Akamai only supports strong `ETag` values. Weak `ETag` values are ignored and a full response is always returned. For more details, see the [RFC Standard](#) ⧉.

Option	Type	Description
enabled	boolean	Enables the ETag validation behavior.

verifyJsonWebToken

- **Property Manager name**: [JWT verification](#)
- **Behavior version**: The `v2023-05-30` rule format supports the `verifyJsonWebToken` behavior v1.1.
- **Rule format status**: [Deprecated, outdated rule format](#)
- **Access**: [Read-write](#)
- **Allowed in includes**: [Yes](#)

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

Option	Type	Description	[Requires](#)
extract Location	enum	Specify from where to extract the JWT value.	
	CLIENT_ REQUEST_ HEADER	The value is in a client request header.	
	QUERY_ STRING	The value is in the request's query string.	
header Name	string	This specifies the name of the header from which to extract the JWT value.	extractLocation is CLIENT_ REQUEST_HEADER
query Parameter Name	string	This specifies the name of the query parameter from which to extract the JWT value.	extractLocation is QUERY_ STRING

Option	Type	Description	Requires
jwt	string	An identifier for the JWT keys collection.	
enable RS256	boolean	Verifies JWTs signed with the RS256 algorithm. This signature helps ensure that the token hasn't been tampered with.	
enable ES256	boolean	Verifies JWTs signed with the ES256 algorithm. This signature helps ensure that the token hasn't been tampered with.	

verifyJsonWebTokenForDcp

- **Property Manager name**: JWT
- **Behavior version**: The `v2023-05-30` rule format supports the `verifyJsonWebTokenForDcp` behavior v1.0.
- **Rule format status**: Deprecated, outdated rule format
- **Access**: Read-write
- **Allowed in includes**: Yes

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.	

Option	Type	Description	Requires
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`
headerName	string	This specifies the name of the header to extract the JWT value from.	`customHeader` is `true`
query Parameter Name	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.	
extractClient Id	boolean	Allows you to extract the client ID claim name stored in JWT.	
clientId	string	This specifies the claim name.	`extractClientId` is `true`
extract Authorizations	boolean	Allows you to extract the authorization groups stored in the JWT.	
authorizations	string	This specifies the authorization group name.	`extractAuthorizations` is `true`
extractUser Name	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 `v2023-05-30` rule format supports the `verifyTokenAuthorization` behavior v1.4.
- **Rule format status**: Deprecated, outdated rule format
- **Access**: Read-write
- **Allowed in includes**: Yes

Verifies Auth 2.0 tokens.

Option	Type	Description	Requires
use Advanced	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: COOKIE QUERY_STRING CLIENT_REQUEST_HEADER	

Option	Type	Description	Requires
locationId	string	When `location` is `CLIENT_REQUEST_HEADER`, specifies the name of the incoming request's header where to find the token.	
algorithm	enum	Specifies the algorithm that generates the token. It needs to match the method chosen in the token generation code.	`useAdvanced` is `true`
		Supported values: MD5 SHA1 SHA256	
escapeHmac Inputs	boolean	URL-escapes HMAC inputs passed in as query parameters.	`useAdvanced` is `true`
ignoreQuery String	boolean	Enabling this removes the query string from the URL used to form an encryption key.	`useAdvanced` 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.	`useAdvanced` 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.	`useAdvanced` 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 `v2023-05-30` rule format supports the `visitorPrioritization` behavior v3.6.
- **Rule format status**: Deprecated, outdated rule format
- **Access**: Read-write
- **Allowed in includes**: No (temporarily)

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 *salt* 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
allowedUser 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 to all allowed users.	allowedUser CookieEnabled is true AND allowed UserCookie Advanced is true AND allowed UserCookie AutomaticSalt is false

Option	Type	Description	Requires
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`
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`
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`

Option	Type	Description	Requires
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`
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 CP code for requests sent to the waiting room. You only need to provide the initial `id`, stripping any `cpc_` `prefix` to pass the integer to the rule tree. Additional CP code details may reflect back in subsequent read-only data.	waitingRoom UseCpCode is `true`
waitingRoomCp Code.cpCode Limits	array	**Read-only**. Describes the current usage limit for the CP code.	
waitingRoomCp Code.created Date	integer	**Read-only**. UNIX epoch timestamp reflecting when the CP code was originally created.	
waitingRoomCp Code.description	string	**Read-only**. Additional description for the CP code.	
waitingRoomCp Code.id	integer	Unique identifier for each CP code. Initially, you get this value when creating a new CP code in PAPI. You can also assign a `cpcodeId` value from the List CP codes operation.	

Option	Type	Description	Requires
waitingRoomCp Code.name	string	**Read-only**. The name of the CP code you specify as the `cpcodeName` when [creating a new CP code](#) in PAPI. You can modify this value with the [PUT operation](#) in the CP codes and Reporting Groups API.	
waitingRoomCp Code.products	array	**Read-only**. The set of products the CP code is assigned to. This reflects `product Id` values you specify when [creating a new CP code](#) in PAPI.	
waitingRoomNet Storage	object	Specifies the NetStorage domain for the waiting room page.	
waitingRoomNet Storage.cpCode	integer	Identifies a CP code assigned to this storage group.	
waitingRoomNet Storage.download DomainName	string	Domain name from which content can be downloaded.	
waitingRoomNet Storage.g2o Token	string	Signature Header Authentication key.	
waitingRoomNet Storage.id	integer	Unique identifier for the storage group.	
waitingRoomNet Storage.name	string	Name of the storage group.	
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.	

watermarking

- **Property Manager name**: [Watermarking](#)
- **Behavior version**: The `v2023-05-30` rule format supports the `watermarking` behavior v1.1.
- **Rule format status**: [Deprecated, outdated rule format](#)
- **Access**: [Read-write](#)
- **Allowed in includes**: [Yes](#)

Adds watermarking for each valid user's content. Content segments are delivered from different sources using a pattern unique to each user, based on a watermarking token included in each request. If your content is pirated or redistributed, you can forensically analyze the segments to extract the pattern, and identify the user who leaked the content.

Option	Type	Description	Requires
enable	boolean	Enables the watermarking behavior.	
signature Verification Enable	boolean	When enabled, you can verify the signature in your watermarking token.	

Option	Type	Description	Requires
verification KeyId1	string	Specifies a unique identifier for the first public key.	signature Verification Enable is true
verification PublicKey1	string	Specifies the first public key in its entirety.	signature Verification Enable is true
verification KeyId2	string	Specifies a unique identifier for the optional second public key.	signature Verification Enable is true
verification PublicKey2	string	Specifies the optional second public key in its entirety. Specify a second key to enable rotation.	signature Verification Enable is true
pattern Decryption Enable	boolean	If patterns in your watermarking tokens have been encrypted, enabling this allows you to provide values to decrypt them.	
decryption Password Id1	string	Specifies a label that corresponds to the primary password.	pattern Decryption Enable is true
decryption Password1	string	Provides the primary password used to encrypt patterns in your watermarking tokens.	pattern Decryption Enable is true
decryption Password Id2	string	Specifies a label for the secondary password, used in rotation scenarios to identify which password to use for decryption.	pattern Decryption Enable is true
decryption Password2	string	Provides the secondary password you can use to rotate passwords.	pattern Decryption Enable is true
useOriginal AsA	boolean	When you work with your watermarking vendor, you can apply several preprocessing methods to your content. See the [AMD help](#) for more information. With the standard *filename-prefix AB naming* preprocessing method, the watermarking vendor creates two variants of the original segment content and labels them as an `A` and `B` segment in the filename. If you selected the *unlabeled A variant* preprocessing method, enabling this option tells your configuration to use the original filename segment content as your `A` variant.	
abVariant Location	enum	When you work with your watermarking vendor, you can apply several preprocessing methods to your content. See the [AMD help](#) for more information. Use this option to specify the location of the `A` and `B` variant segments.	
	FILENAME_ PREFIX	Set for the standard, *filename-prefix AB naming* preprocessing method, where the variant letter is included in the filename.	
	PARENT_ DIRECTORY_ PREFIX	Set for the *directory-prefix AB naming* preprocessing method, where variants are located in a subdirectory named after the variants, such as `/B/segment1.ts`.	

webApplicationFirewall

- **Property Manager name**: [Web Application Firewall (WAF)](#)
- **Behavior version**: The `v2023-05-30` rule format supports the `webApplicationFirewall` behavior v1.1.
- **Rule format status**: [Deprecated, outdated rule format](#)
- **Access**: [Read-write](#)
- **Allowed in includes**: [No (temporarily)](#)

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 `v2023-05-30` rule format supports the `webSockets` behavior v1.1.
- **Rule format status**: [Deprecated, outdated rule format](#)
- **Access**: [Read-write](#)
- **Allowed in includes**: [Yes](#)

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

Option	Type	Description
enabled	boolean	Enables WebSocket traffic.

webdav

- **Property Manager name**: [WebDAV](#)
- **Behavior version**: The `v2023-05-30` rule format supports the `webdav` behavior v1.1.

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

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.

v2023-05-30 criteria

v2023-05-30 criteria

This section provides details for all criteria the Property Manager API supports for the `v2023-05-30` 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 `v2023-05-30` 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 `v2023-05-30` rule format supports the `advancedImMatch` criteria v1.2.
- **Rule format status**: [Deprecated, outdated rule format](#)
- **Access**: [Read-write](#)
- **Allowed in includes**: [Yes](#)

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

Option	Type	Description
matchOperator	enum	Specifies the match's logic.
	IS	Matches the selected requests.
	IS_NOT	Does not match the selected requests.
matchOn	enum	Specifies the match's scope.
	ANY_IM	Whether to match any requests that also include generated derivatives.
	PRISTINE	Whether to match only pristine requests on original images or videos from Image and Video Manager.

bucket

- **Property Manager name**: Percentage of Clients
- **Criteria version**: The v2023-05-30 rule format supports the bucket criteria v1.1.
- **Rule format status**: Deprecated, outdated rule format
- **Access**: Read-write
- **Allowed in includes**: Yes

This matches a specified percentage of requests when used with the accompanying behavior. Contact Akamai Professional Services for help configuring it.

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

cacheability

- **Property Manager name**: Response Cacheability
- **Criteria version**: The v2023-05-30 rule format supports the cacheability criteria v1.1.
- **Rule format status**: Deprecated, outdated rule format
- **Access**: Read-write
- **Allowed in includes**: Yes

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
matchOperator	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.

chinaCdnRegion

- **Property Manager name**: ChinaCDN Region
- **Criteria version**: The `v2023-05-30` rule format supports the `chinaCdnRegion` criteria v1.0.
- **Rule format status**: Deprecated, outdated rule format
- **Access**: Read-write
- **Allowed in includes**: Yes

Identifies traffic deployed over Akamai's regional ChinaCDN infrastructure.

Option	Type	Description
matchOperator	enum	Specify whether the request `IS` or `IS_NOT` deployed over ChinaCDN.
	IS	The request is deployed over ChinaCDN.
	IS_NOT	The request is not deployed over ChinaCDN.

clientCertificate

- **Property Manager name**: Client certificate
- **Criteria version**: The `v2023-05-30` rule format supports the `clientCertificate` criteria v1.1.
- **Rule format status**: Deprecated, outdated rule format
- **Access**: Read-write
- **Allowed in includes**: Yes

Matches whether you have configured a client certificate to authenticate requests to edge servers.

Option	Type	Description	Requires
isCertificate Present	boolean	Executes rule behaviors only if a client certificate authenticates requests.	
isCertificate Valid	enum	Matches whether the certificate is `VALID` or `INVALID`. You can also `IGNORE` the certificate's validity.	isCertificatePresent is true
	VALID	Match when the certificate is valid.	
	INVALID	Match when the certificate is invalid.	
	IGNORE	Ignores the certificate's is valid.	

clientIp

- **Property Manager name**: Client IP
- **Criteria version**: The `v2023-05-30` rule format supports the `clientIp` criteria v1.1.
- **Rule format status**: Deprecated, outdated rule format
- **Access**: Read-write
- **Allowed in includes**: Yes

Matches the IP number of the requesting client. To use this condition to match end-user IP addresses, apply it together with the `requestType` matching on the `CLIENT_REQ` value.

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 `v2023-05-30` rule format supports the `clientIpVersion` criteria v1.1.
- **Rule format status**: [Deprecated, outdated rule format](#)
- **Access**: [Read-write](#)
- **Allowed in includes**: [Yes](#)

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 `v2023-05-30` rule format supports the `cloudletsOrigin` criteria v1.2.
- **Rule format status**: [Deprecated, outdated rule format](#)
- **Access**: [Read-write](#)
- **Allowed in includes**: [Yes](#)

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 `v2023-05-30` rule format supports the `contentDeliveryNetwork` criteria v1.3.
- **Rule format status**: Deprecated, outdated rule format
- **Access**: Read-write
- **Allowed in includes**: Yes

Specifies the type of Akamai network handling the request.

Option	Type	Description
matchOperator	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 `v2023-05-30` rule format supports the `contentType` criteria v1.1.
- **Rule format status**: Deprecated, outdated rule format
- **Access**: Read-write
- **Allowed in includes**: Yes

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

Warning. The Content Type match was updated in April 2023 and the change affects configurations that implement it together with the `gzipResponse` behavior. With the new change, if the origin server sends out the content in an uncompressed format, the Akamai edge servers cache it and deliver it to the requesting client in the compressed .gzip format. Clients using the Content-Length response header to determine the file size will now see the compressed size of the object returned from Akamai, rather than the uncompressed size of the object returned from the origin. If you updated your property configuration after April 3rd 2023, your `contentType` match is affected by this change.

Option	Type	Description
matchOperator	enum	Matches any `Content-Type` among specified `values` when set to `IS_ONE_OF`, otherwise `IS_NOT_ONE_OF` reverses the match.
	IS_ONE_OF	Matches any `Content-Type` among the specified `values`.

Option	Type	Description
	IS_NOT_ ONE_OF	Matches none of the specified `values` .
values	string array	`Content-Type` response header value, for example `text/html` .
match Wildcard	boolean	Allows wildcards in the `value` field, where `?` matches a single character and `*` matches zero or more characters. Specifying `text/*` matches both `text/html` and `text/css` .
matchCase Sensitive	boolean	Sets a case-sensitive match for all `values` .

deviceCharacteristic

- **Property Manager name**: Device Characteristics
- **Criteria version**: The `v2023-05-30` rule format supports the `deviceCharacteristic` criteria v1.3.
- **Rule format status**: Deprecated, outdated rule format
- **Access**: Read-write
- **Allowed in includes**: [Yes](Yes)

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
characteristic	enum	Aspect of the device or browser to match.	
	BRAND_ NAME	String value such as `Samsung` or `Apple` .	
	MODEL_ NAME	String value such as `SCH-I110` .	
	MARKETING_ NAME	String value such as `Samsung Illusion` .	
	IS_ WIRELESS_ DEVICE	Boolean value.	
	IS_TABLET	Boolean value, subset of `IS_MOBILE` .	
	DEVICE_OS	String value.	
	DEVICE_OS_ VERSION	Version string value.	
	MOBILE_ BROWSER	String value.	
	MOBILE_ BROWSER_ VERSION	Version string value.	

Option	Type	Description	Requires
	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.	
stringMatchOperator	enum	When the `characteristic` expects a string value, set this to `MATCHES_ONE_OF` to match against the `stringValue` set, otherwise set to `DOES_NOT_MATCH_ONE_OF` to exclude that set of values.	`characteristic` is either: `BRAND_NAME`, `MODEL_NAME`, `MARKETING_NAME`, `DEVICE_OS`, `MOBILE_BROWSER`, `PREFERRED_MARKUP`, `HTML_PREFERRED_DTD`, `XHTML_PREFERRED_CHARSET`, `VIEWPORT_WIDTH`, `XHTMLMP_PREFERRED_MIME_TYPE`, `AJAX_PREFERRED_GEOLOC_API`, `XHTML_FILE_UPLOAD`, `XHTML_SUPPORTS_IFRAME`, `FLASH_LITE_VERSION`
	MATCHES_ONE_OF	The value is included as a `stringValue`.	
	DOES_NOT_MATCH_ONE_OF	The value is not included as a `stringValue`.	
numericMatchOperator	enum	When the `characteristic` expects a numeric value, compares the specified `numericValue` against the matched client.	`characteristic` is either: `RESOLUTION_WIDTH`, `RESOLUTION_HEIGHT`, `PHYSICAL_SCREEN_HEIGHT`, `PHYSICAL_SCREEN_WIDTH`, `XHTML_SUPPORT_LEVEL`, `MAX_IMAGE_WIDTH`, `MAX_IMAGE_HEIGHT`, `VIEWPORT_INITIAL_SCALE`
	IS	Values are equal.	
	IS_NOT	Values are not equal.	
	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.	

Option	Type	Description	Requires
versionMatch Operator	enum	When the `characteristic` expects a version string value, compares the specified `version Value` 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_ SUPPRT`, `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 `string Value` field.	`stringMatchOperator` is either: `MATCHES_ONE_OF`, `DOES_NOT_ MATCH_ONE_OF`
match Wildcard	boolean	Allows wildcards in the `stringValue` field, where `?` matches a single character and `*` matches zero or more characters.	`stringMatchOperator` is either: `MATCHES_ONE_OF`, `DOES_NOT_ MATCH_ONE_OF`

edgeWorkersFailure

- **Property Manager name**: EdgeWorkers Execution Status
- **Criteria version**: The `v2023-05-30` rule format supports the `edgeWorkersFailure` criteria v1.2.
- **Rule format status**: Deprecated, outdated rule format
- **Access**: Read-write

- **Allowed in includes**: <u>Yes</u>

Checks the EdgeWorkers execution status and detects whether a customer's JavaScript failed on edge servers.

Option	Type	Description
execStatus	enum	Specify execution status.
	`FAILURE`	Execution failed.
	`SUCCESS`	Execution succeeded.

fileExtension

- **Property Manager name**: <u>File Extension</u>
- **Criteria version**: The `v2023-05-30` rule format supports the `fileExtension` criteria v1.1.
- **Rule format status**: <u>Deprecated, outdated rule format</u>
- **Access**: <u>Read-write</u>
- **Allowed in includes**: <u>Yes</u>

Matches the requested filename's extension, if present.

Option	Type	Description
matchOperator	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`.
matchCaseSensitive	boolean	Sets a case-sensitive match.

filename

- **Property Manager name**: <u>Filename</u>
- **Criteria version**: The `v2023-05-30` rule format supports the `filename` criteria v1.1.

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

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.	
values	string array	Matches the filename component of the request URL. Allows wildcards, where `?` matches a single character and `*` matches zero or more characters. 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 `values` field.	`matchOperator` is either: `IS_ONE_OF` , `IS_NOT_ONE_OF`

hostname

- **Property Manager name**: [Hostname](#)
- **Criteria version**: The `v2023-05-30` rule format supports the `hostname` criteria v1.1.
- **Rule format status**: [Deprecated, outdated rule format](#)
- **Access**: [Read-write](#)
- **Allowed in includes**: [Yes](#)

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` .

Option	Type	Description
	IS_NOT_ONE_OF	Does not matche the contents of `values`.
values	string array	A list of hostnames. Allows wildcards, where `?` matches a single character and `*` matches zero or more characters. Specifying `*.example.com` matches both `m.example.com` and `www.example.com`.

matchAdvanced

- **Property Manager name**: [Advanced Match](#)
- **Criteria version**: The `v2023-05-30` rule format supports the `matchAdvanced` criteria v1.1.
- **Rule format status**: [Deprecated, outdated rule format](#)
- **Access**: [Read-only](#)
- **Allowed in includes**: [Yes](#)

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.
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 `v2023-05-30` rule format supports the `matchCpCode` criteria v1.1.
- **Rule format status**: [Deprecated, outdated rule format](#)
- **Access**: [Read-write](#)
- **Allowed in includes**: [Yes](#)

Match the assigned content provider code.

Option	Type	Description
value	object	Specifies the CP code as an object. You only need to provide the initial `id` to match the CP code, stripping any `cpc_` `prefix` to pass the integer to the rule tree. Additional CP code details may reflect back in subsequent read-only data.
value.cpCode Limits	array	**Read-only**. Describes the current usage limit for the CP code.
value.created Date	integer	**Read-only**. UNIX epoch timestamp reflecting when the CP code was originally created.
value.description	string	**Read-only**. Additional description for the CP code.
value.id	integer	Unique identifier for each CP code. Initially, you get this value when [creating a new CP code](#) in PAPI. You can also assign a `cpcodeId` value from the [List CP codes](#) operation.
value.name	string	**Read-only**. The name of the CP code you specify as the `cpcodeName` when [creating a new CP code](#) in PAPI. You can modify this value with the [PUT operation](#) in the CP codes and Reporting Groups API.
value.products	array	**Read-only**. The set of products the CP code is assigned to. This reflects `productId` values you specify when [creating a new CP code](#) in PAPI.

matchResponseCode

- **Property Manager name**: [Response Status Code](#)
- **Criteria version**: The `v2023-05-30` rule format supports the `matchResponseCode` criteria v1.2.
- **Rule format status**: [Deprecated, outdated rule format](#)
- **Access**: [Read-write](#)
- **Allowed in includes**: [Yes](#)

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

matchVariable

- **Property Manager name**: Variable
- **Criteria version**: The `v2023-05-30` rule format supports the `matchVariable` criteria v1.2.
- **Rule format status**: Deprecated, outdated rule format
- **Access**: Read-write
- **Allowed in includes**: Yes

Matches a built-in variable, or a custom variable pre-declared within the rule tree by the `setVariable` 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 `variableExpression` string.	
	IS_NOT	Does not match the `variableExpression` string.	
	IS_ONE_OF	Matches any of an array of string `variableValues` .	
	IS_NOT_ONE_OF	Does not match any of an array of string `variable Values` .	
	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 `lowerBound` and `upperBound` values.	
	IS_NOT_BETWEEN	Is outside the numeric `lowerBound` and `upperBound` range.	
	IS_GREATER_THAN	Is greater than the `variableExpression` 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 `variableExpression` string-formatted number.	
variable Values	string array	Specifies an array of matching strings.	`matchOperator` is either: `IS_ONE_OF` , `IS_NOT_ONE_OF`

Option	Type	Description	Requires
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 allows wildcards, where `?` matches a single character and `*` matches zero or more characters.	`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 `v2023-05-30` rule format supports the `metadataStage` criteria v1.0.
- **Rule format status**: [Deprecated, outdated rule format](#)
- **Access**: [Read-write](#)
- **Allowed in includes**: [Yes](#)

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.
	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.

Option	Type	Description
	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 `forward-request` 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 `client-request` stage.

originTimeout

- **Property Manager name**: [Origin Timeout](#)
- **Criteria version**: The `v2023-05-30` rule format supports the `originTimeout` criteria v1.1.
- **Rule format status**: [Deprecated, outdated rule format](#)
- **Access**: [Read-write](#)
- **Allowed in includes**: [Yes](#)

Matches when the origin responds with a timeout error.

Option	Type	Description
matchOperator	enum	Specifies a single required `ORIGIN_TIMED_OUT` value.
	ORIGIN_TIMED_OUT	This is currently the only supported value.

path

- **Property Manager name**: [Path](#)
- **Criteria version**: The `v2023-05-30` rule format supports the `path` criteria v1.2.
- **Rule format status**: [Deprecated, outdated rule format](#)
- **Access**: [Read-write](#)

- **Allowed in includes**: Yes

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` . This field allows wildcards, where `?` matches a single character and `*` matches zero or more characters. For example, `/blog/*/2014` matches paths with two fixed segments and other varying segments between them.
match Case Sensitive	boolean	Sets a case-sensitive match.
normalize	boolean	Transforms URLs before comparing them with the provided value. URLs are decoded, and any directory syntax such as `../..` or `//` is stripped as a security measure. This protects URL paths from being accessed by unauthorized users.

queryStringParameter

- **Property Manager name**: Query String Parameter
- **Criteria version**: The `v2023-05-30` rule format supports the `queryStringParameter` criteria v1.1.
- **Rule format status**: Deprecated, outdated rule format
- **Access**: Read-write
- **Allowed in includes**: Yes

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.	

Option	Type	Description	Requires
	EXISTS	Whether the query field's `parameterName` is present in the requesting URL.	
	DOES_ NOT_ EXIST	Whether the query field's `parameterName` is absent from the requesting URL.	
	IS_LESS_ THAN	Matches a range when the `value` is numeric.	
	IS_MORE_ THAN	Matches a range when the `value` is numeric.	
	IS_ BETWEEN	Is between the numeric `lowerBound` and `upperBound` values.	
values	string array	The value of the query field, for example, `string` in `?q=string` .	`matchOperator` is either: `IS_ ONE_OF` , `IS_NOT_ONE_OF`
lowerBound	number	Specifies the match's minimum value.	`matchOperator` is either: `IS_ MORE_THAN` , `IS_BETWEEN`
upperBound	number	When the `value` is numeric, this field specifies the match's maximum value.	`matchOperator` is either: `IS_ LESS_THAN` , `IS_BETWEEN`
match Wildcard Name	boolean	Allows wildcards in the `parameterName` field, where `?` matches a single character and `*` matches zero or more characters.	
matchCase Sensitive Name	boolean	Sets a case-sensitive match for the `parameterName` field.	
match WildcardValue	boolean	Allows wildcards in the `value` field, where `?` matches a single character and `*` matches zero or more characters.	`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`
escapeValue	boolean	Matches when the `value` is URL-escaped.	`matchOperator` is either: `IS_ ONE_OF` , `IS_NOT_ONE_OF`

random

- **Property Manager name**: Sample Percentage
- **Criteria version**: The `v2023-05-30` rule format supports the `random` criteria v1.0.
- **Rule format status**: Deprecated, outdated rule format
- **Access**: Read-write
- **Allowed in includes**: Yes

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

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

recoveryConfig

- **Property Manager name**: Recovery Configuration Name
- **Criteria version**: The `v2023-05-30` rule format supports the `recoveryConfig` criteria v1.0.
- **Rule format status**: Deprecated, outdated rule format
- **Access**: Read-write
- **Allowed in includes**: Yes

Matches on specified origin recovery scenarios. The `originFailureRecoveryPolicy` behavior defines the scenarios that trigger the recovery or retry methods you set in the `originFailureRecoveryMethod` rule. If the origin fails, the system checks the name of the recovery method applied to your policy. It then either redirects the requesting client to a backup origin or returns predefined HTTP response codes.

Option	Type	Description
config Name	string	A unique identifier used for origin failure recovery configurations. This is the recovery method configuration name you apply when setting origin failure recovery methods and scenarios in `originFailureRecoveryMethod` and `originFailureRecovery Policy` behaviors. The value can contain alphanumeric characters and dashes.

regularExpression

- **Property Manager name**: Regex
- **Criteria version**: The `v2023-05-30` rule format supports the `regularExpression` criteria v1.0.
- **Rule format status**: Deprecated, outdated rule format
- **Access**: Read-write
- **Allowed in includes**: Yes

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

Option	Type	Description
matchString	string (allows variables)	The string to match, typically the contents of a dynamic variable.

Option	Type	Description
regex	string	The regular expression (PCRE) to match against the string.
caseSensitive	boolean	Sets a case-sensitive regular expression match.

requestCookie

- **Property Manager name**: [Request Cookie](#)
- **Criteria version**: The `v2023-05-30` rule format supports the `requestCookie` criteria v1.1.
- **Rule format status**: [Deprecated, outdated rule format](#)
- **Access**: [Read-write](#)
- **Allowed in includes**: [Yes](#)

Match the cookie name or value passed with the request.

Option	Type	Description	Requires
cookieName	string	The name of the cookie, for example, `visitor` in `visitor:anon`.	
matchOperator	enum	Narrows the match criteria.	
	IS	If the field's `value` string matches.	
	IS_NOT	If the field's `value` string does not match.	
	EXISTS	Matches if the `cookieName` cookie exists.	
	DOES_ NOT_ EXIST	Matches if the `cookieName` cookie does not exist.	
	IS_ BETWEEN	Is between the numeric `lowerBound` and `upperBound` values.	
value	string	The cookie's value, for example, `anon` in `visitor:anon`.	`matchOperator` is either: `IS`, `IS_NOT`
lowerBound	number	When the `value` is numeric, this field specifies the match's minimum value.	`matchOperator` is `IS_ BETWEEN`
upperBound	number	When the `value` is numeric, this field specifies the match's maximum value.	`matchOperator` is `IS_ BETWEEN`
matchWildcard Name	boolean	Allows wildcards in the `cookieName` field, where `?` matches a single character and `*` matches zero or more characters.	
matchCase SensitiveName	boolean	Sets a case-sensitive match for the `cookieName` field.	
matchWildcard Value	boolean	Allows wildcards in the `value` field, where `?` matches a single character and `*` matches zero or more characters.	`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 `v2023-05-30` rule format supports the `requestHeader` criteria v1.1.
- **Rule format status**: Deprecated, outdated rule format
- **Access**: Read-write
- **Allowed in includes**: Yes

Match HTTP header names or values.

Option	Type	Description	Requires
headerName	string	The name of the request header, for example `Accept-Language` .	
matchOperator	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`
matchWildcardName	boolean	Allows wildcards in the `headerName` field, where `?` matches a single character and `*` matches zero or more characters.	
matchWildcardValue	boolean	Allows wildcards in the `value` field, where `?` matches a single character and `*` matches zero or more characters.	`matchOperator` is either: `IS_ONE_OF` , `IS_NOT_ONE_OF`
matchCaseSensitiveValue	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 `v2023-05-30` rule format supports the `requestMethod` criteria v1.4.
- **Rule format status**: Deprecated, outdated rule format

- **Access**: [Read-write](#)
- **Allowed in includes**: [Yes](#)

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_MKCALENDAR	WebDAV method.
	DAV_MKCOL	WebDAV method.
	DAV_MOVE	WebDAV method.
	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 `v2023-05-30` rule format supports the `requestProtocol` criteria v1.0.
- **Rule format status**: [Deprecated, outdated rule format](#)
- **Access**: [Read-write](#)
- **Allowed in includes**: [Yes](#)

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 `v2023-05-30` rule format supports the `requestType` criteria v1.1.
- **Rule format status**: [Deprecated, outdated rule format](#)
- **Access**: [Read-write](#)
- **Allowed in includes**: [Yes](#)

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
match Operator	enum	Specifies whether the request `IS` or `IS_NOT` the type of specified `value`.
	IS	The request is the type of specified `value`.
	IS_NOT	The request is not the type of specified `value`.
value	enum	Specifies the type of request, either a standard `CLIENT_REQ`, an `ESI_FRAGMENT`, or an `EW_SUBREQUEST`.
	CLIENT_REQ	A client request.

Option	Type	Description
	ESI_FRAGMENT	An Edge Side Include fragment.
	EW_SUBREQUEST	An EdgeWorkers sub-request.

responseHeader

- **Property Manager name**: [Response Header](#)
- **Criteria version**: The `v2023-05-30` rule format supports the `responseHeader` criteria v1.2.
- **Rule format status**: [Deprecated, outdated rule format](#)
- **Access**: [Read-write](#)
- **Allowed in includes**: [Yes](#)

Match HTTP header names or values.

Option	Type	Description	Requires
headerName	string	The name of the response header, for example `Content-Type`.	
matchOperator	enum	Narrows the match according to various criteria.	
	IS_ONE_OF	The field's `value` string matches.	
	IS_NOT_ONE_OF	The field's `value` string does not match.	
	EXISTS	The HTTP field `headerName` is present.	
	DOES_NOT_EXIST	The HTTP field `headerName` is absent.	
	IS_LESS_THAN	Matches ranges when the `value` is numeric.	
	IS_MORE_THAN	Matches ranges when the `value` is numeric.	
	IS_BETWEEN	Is between the numeric `lowerBound` and `upperBound` values.	
values	string array	The response header's value, for example `application/x-www-form-urlencoded` when the header `headerName` is `Content-Type`.	`matchOperator` is either: `IS_ONE_OF`, `IS_NOT_ONE_OF`
lowerBound	number	When the `value` is numeric, this field specifies the match's minimum value.	`matchOperator` is either: `IS_MORE_THAN`, `IS_BETWEEN`
upperBound	number	When the `value` is numeric, this field specifies the match's maximum value.	`matchOperator` is either: `IS_LESS_THAN`, `IS_BETWEEN`
matchWildcardName	boolean	Allows wildcards in the `headerName` field, where `?` matches a single character and `*` matches zero or more characters.	

Option	Type	Description	Requires
match WildcardValue	boolean	Allows wildcards in the `value` field, where `?` matches a single character and `*` matches zero or more characters.	`matchOperator` is either: `IS_ONE_OF`, `IS_NOT_ONE_OF`
matchCase Sensitive Value	boolean	When enabled, the match is case-sensitive for the `value` field.	`matchOperator` is either: `IS_ONE_OF`, `IS_NOT_ONE_OF`

serverLocation

- **Property Manager name**: [Akamai Server Location](#)
- **Criteria version**: The `v2023-05-30` rule format supports the `serverLocation` criteria v1.0.
- **Rule format status**: [Deprecated, outdated rule format](#)
- **Access**: [Read-write](#)
- **Allowed in includes**: [Yes](#)

The location of the Akamai server handling the request.

Option	Type	Description	Requires
location Type	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`.	
countries	string array	ISO 3166-1 country codes, such as `US` or `CN`.	`locationType` is `COUNTRY`
continents	string array	Continent codes.	`locationType` is `CONTINENT`
	AF	Africa.	
	AS	Asia.	
	EU	Europe.	
	NA	North America.	
	OC	Oceania.	
	OT	Antarctica.	
	SA	South America.	

Option	Type	Description	Requires
regions	string array	ISO 3166 country and region codes, for example `US:MA` for Massachusetts or `JP:13` for Tokyo.	`locationType` is `REGION`

time

- **Property Manager name**: [Time Interval](#)
- **Criteria version**: The `v2023-05-30` rule format supports the `time` criteria v1.1.
- **Rule format status**: [Deprecated, outdated rule format](#)
- **Access**: [Read-write](#)
- **Allowed in includes**: [Yes](#)

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 `beginDate`.	
	`BETWEEN`	Sets a single range between two dates, using the values of `beginDate` and `endDate`.	
	`LASTING`	Sets a single range, but based on duration relative to the starting time. It relies on the values of `lastingDate` and `lastingDuration`.	
	`REPEATING`	Allows a `LASTING`-style range to repeat at regular intervals. It relies on the values of `repeatBeginDate`, `repeatDuration`, and `repeatInterval`.	
repeat Interval	string (duration)	Sets the time between each repeating time period's starting points.	match Operator is `REPEATING`
repeat Duration	string (duration)	Sets the duration of each repeating time period.	match Operator is `REPEATING`
lasting Duration	string (duration)	Specifies the end of a time period as a duration relative to the `lastingDate`.	match Operator is `LASTING`
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`

Option	Type	Description	Requires
begin Date	string (timestamp)	Sets the start of a time period.	`match Operator` is `BEGINNING` OR `match Operator` is `BETWEEN`
endDate	string (timestamp)	Sets the end of a fixed time period.	`match Operator` is `BETWEEN`

tokenAuthorization

- **Property Manager name**: Token Verification Result
- **Criteria version**: The `v2023-05-30` rule format supports the `tokenAuthorization` criteria v1.2.
- **Rule format status**: Deprecated, outdated rule format
- **Access**: Read-write
- **Allowed in includes**: Yes

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 `v2023-05-30` rule format supports the `userAgent` criteria v1.1.
- **Rule format status**: Deprecated, outdated rule format
- **Access**: Read-write
- **Allowed in includes**: Yes

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 wildcards in the `value` field, where `?` matches a single character and `*` matches zero or more characters. For example, `*Android*`, `*iPhone5*`, `*Firefox*`, or `*Chrome*` allow substring matches.
match Case Sensitive	boolean	Sets a case-sensitive match for the `value` field.

userLocation

- **Property Manager name**: User Location Data
- **Criteria version**: The `v2023-05-30` rule format supports the `userLocation` criteria v1.2.
- **Rule format status**: Deprecated, outdated rule format
- **Access**: Read-write
- **Allowed in includes**: Yes

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.	
useOnly First XForwarded ForIp	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 `v2023-05-30` rule format supports the `userNetwork` criteria v1.1.
- **Rule format status**: Deprecated, outdated rule format
- **Access**: Read-write
- **Allowed in includes**: Yes

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.	

Option	Type	Description	Requires
	`IS_ONE_OF`	Matches any of the specified `values`.	
	`IS_NOT_ONE_OF`	Does not match any of the specified `values`.	
network Values	string array	Any set of specific networks.	`field` is `NETWORK`

Supported values:

@NIFTY	COLT	INFOSPHERE	ROGERS
AIRTEL	COMCAST	JANET	SASKTEL
ALPHA_INTERNET	COMPLETEL	JAZZTELL	SEEDNET
ALTITUDE_TELECOM	COMPUSERVE	JUSTNET	SEIKYO_INTERNET
AOL	COVAD	LIVEDOOR	SFR
ARNET	DION	MCI	SHAW
ASAHI	DIRECTV	MEDIACOM	SOFTLAYER
ATT	DREAMNET	MEDIA_ONE	SO_NET
AWS	DTAG	MICROSOFT	SPRINT
BELLALIANT	DTI	MIL	SUDDENLINK
BELL_CANADA	EARTHLINK	NERIM	TALKTALK
BIGLOBE	EASYNET	NEWNET	TEKSAAVY
BITMAILER	EITC	NUMERICABLE	TELEFONICA
BOUYGUES	ETISALAT	OCN	TELSTRA
BRIGHT_HOUSE	EUROCIBER	ODN	TERRA_MEXICO
BSKYB	FASTWEB	ONO	TI
BT	FIBERTEL	PANASONIC_HI_HO	TIKITIKI
CABLEONE	FRANCE_TELECOM	PLALA	TIME_WARNER
CABLEVISION	FREE	PLUSNET	TISCALI
CERNET	FREECOM	PRODIGY	TURK_TELEKOM
CHARTER	FRONTIER	QWEST	T_MOBILE
CHINANET	GOOGLECLOUD	RCN	UNI2
CHINA_MOBILE	H3G	REDIRIS	UNINET
CHINA_UNICOM	HINET	RENATER	UPC
CLEARWIRE	IBM	RESERVED	USEMB
COGECO	IDECNET	RETEVISION	UUNET
COLOCROSSING	IIJ4U	ROAD_RUNNER	VERIZON

Option	Type	Description	Requires
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.	
useOnly First XForwarded ForIp	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 `v2023-05-30` rule format supports the `variableError` criteria v1.1.

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

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 `variableNames`, otherwise matches errors from variables outside that set.
`variable Names`	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 `VAR`, the name in this field needs to appear with its added prefix as `PMUSER_VAR`. When such a variable is inserted into other fields, it appears with an additional namespace as `{{user.PMUSER_VAR}}`. 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 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.

Published November 6, 2023

Akamai.com   Legal & privacy   Cookie settings   Akamai status