



v2025-05-30 Property Manager Deprecated Rule Formats

September 15, 2025

Contents

Welcome

[Welcome](#)

PAPI conventions

[Advanced and locked features](#)

[API versioning](#)

v2025-05-30 behaviors

[v2025-05-30 behaviors](#)

[adScalerCircuitBreaker](#)

[adaptiveAcceleration](#)

[advanced](#)

[aggregatedReporting](#)

[akamaizer](#)

[akamaizerTag](#)

[allHttpInCacheHierarchy](#)

[allowCloudletsOrigins](#)

[allowDelete](#)

[allowHTTPSCacheKeySharing](#)

[allowHTTPSDowngrade](#)

[allowOptions](#)

[allowPatch](#)

[allowPost](#)

[allowPut](#)

[allowTransferEncoding](#)

[altSvcHeader](#)

[apiPrioritization](#)

[applicationLoadBalancer](#)

[audienceSegmentation](#)

[autoDomainValidation](#)

[baseDirectory](#)

[bossBeaconing](#)

[breadcrumbs](#)

[breakConnection](#)

[brotli](#)

[cacheError](#)

[cacheId](#)

[cacheKeyIgnoreCase](#)

[cacheKeyQueryParams](#)

[cacheKeyRewrite](#)

[cachePost](#)

[cacheRedirect](#)

[cacheTag](#)

[cacheTagVisible](#)

cached
centralAuthorization
chaseRedirects
clientCertificateAuth
clientCharacteristics
cloudInterconnects
cloudWrapper
cloudWrapperAdvanced
commonMediaClientData
constructResponse
contentCharacteristics
contentCharacteristicsAMD
contentCharacteristicsDD
contentCharacteristicsWsdLive
contentTargetingProtection
corsSupport
cpCode
customBehavior
datastream
dcp
dcpAuthHMACTransformation
dcpAuthRegexTransformation
dcpAuthSubstringTransformation
dcpAuthVariableExtractor
dcpDefaultAuthzGroups
dcpDevRelations
deliveryReceipt
denyAccess
denyDirectFailoverAccess
deviceCharacteristicCached
deviceCharacteristicHeader
dnsAsyncRefresh
dnsPrefresh
downgradeProtocol
downloadCompleteMarker
downloadNotification
downstreamCache
dynamicThroughputOptimization
dynamicThroughputOptimizationOverride
earlyData
earlyDataAdvanced
earlyHints
ecmsBulkUpload
ecmsDatabase
ecmsDataset
ecmsObjectKey
edgeConnect
edgeLoadBalancingAdvanced
edgeLoadBalancingDataCenter
edgeLoadBalancingOrigin
edgeOriginAuthorization

edgeRedirector
edgeScape
edgeSideIncludes
inputValidation
edgeWorker
enforceMtlsSettings
enhancedAkamaiProtocol
enhancedDebug
enhancedProxyDetection
epdForwardHeaderEnrichment
failAction
failoverBotManagerFeatureCompatibility
fastInvalidate
fips
firstPartyMarketing
firstPartyMarketingPlus
forwardRewrite
g2oheader
globalRequestNumber
graphqlCaching
gzipResponse
hdDataAdvanced
healthDetection
hsafEipBinding
http2
http3
httpStrictTransportSecurity
httpToHttpsUpgrade
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
mtlsOriginKeystore
origin
originCharacteristics
originCharacteristicsWsd
originFailureRecoveryMethod
originFailureRecoveryPolicy
originIpAcl
permissionsPolicy
persistentClientConnection
persistentConnection
personallyIdentifiableInformation
phasedRelease
ppcOrigin
preconnect
predictiveContentDelivery
predictivePrefetching
prefetch
shutr
prefetchable
prefreshCache
quicBeta
randomSeek
rapid
readTimeout
realUserMonitoring
redirect
redirectplus
referrerChecking
removeQueryParameter
removeVary
report
requestClientHints
requestControl
requestTypeMarker
resourceOptimizer
resourceOptimizerExtendedCompatibility
responseCode
responseCookie
restrictObjectCaching
returnCacheStatus
rewriteUrl
rumCustom
saasDefinitions
salesForceCommerceCloudClient
salesForceCommerceCloudProvider
salesForceCommerceCloudProviderHostHeader
savePostDcaProcessing
scheduleInvalidation

scriptManagement
segmentedContentProtection
segmentedMediaOptimization
segmentedMediaStreamingPrefetch
setVariable
simulateErrorCode
siteShield
standardTLSMigration
standardTLSMigrationOverride
strictHeaderParsing
sureRoute
tcpOptimization
teaLeaf
tieredDistribution
tieredDistributionAdvanced
tieredDistributionCustomization
timeout
uidConfiguration
validateEntityTag
verifyJsonWebToken
verifyJsonWebTokenForDcp
verifyTokenAuthorization
visitorPrioritization
watermarking
webApplicationFirewall
webSockets
webdav

v2025-05-30 criteria

v2025-05-30 criteria
advancedImMatch
bucket
cacheability
chinaCdnRegion
clientCertificate
clientIp
clientIpVersion
cloudletsOrigin
contentDeliveryNetwork
contentType
debugMode
deviceCharacteristic
edgeWorkersFailure
fileExtension
filename
hostname
matchAdvanced
matchCpCode
matchResponseCode
matchVariable


metadataStage
originTimeout
path
queryStringParameter
random
recoveryConfig
regularExpression
requestCookie
requestHeader
requestMethod
requestProtocol
requestType
responseHeader
serverLocation
time
tokenAuthorization
userAgent
userLocation
userNetwork
variableError

Notice

Notice

Welcome

Welcome

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

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

This guide provides details for all behaviors and criteria the Property Manager API supports in the v2025-05-30 **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.

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.

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.

v2025-05-30 behaviors

v2025-05-30 behaviors

This section provides details for all behaviors the Property Manager API supports for the `v2025-05-30` rule format version. The set available to you depends on the product and modules assigned to the property or the include. You can get it by running either [List available behaviors for a property](#) or [List available behaviors for an include](#).

This `v2025-05-30` rule format is an older deprecated snapshot set of PAPI features. To take advantage of fresh improvements and new features that get released on a regular basis, you should consider using the `latest` rule format. See [Dynamic rule updates](#) 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 `v2025-05-30` 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
<code>responseDelayBased</code>	boolean	Triggers a fallback action based on the delayed response from the technology partner's server.	
<code>responseDelayThreshold</code>	enum	Specifies the maximum response delay that, if exceeded, triggers the fallback action.	<code>responseDelayBased</code> is true
		Supported values: 500ms	
<code>responseCodeBased</code>	boolean	Triggers a fallback action based on the response code from the technology partner's server.	
<code>responseCodes</code>	string	Specifies the codes in the partner's response that trigger the fallback action, either 408 , 500 , 502 , 504 , SAME_AS_RECEIVED , or SPECIFY_YOUR_OWN for a custom code.	<code>responseCodeBased</code> is true
<code>fallbackActionResponseCodeBased</code>	enum	Specifies the fallback action.	<code>responseDelayBased</code> is true OR <code>responseCodeBased</code> is true
	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.	
<code>returnErrorResponseCodeBased</code>	enum	Specifies the error to include in the response to the client.	<code>fallbackActionResponseCodeBased</code> 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.	
<code>specifyYourOwnResponseCodeBased</code>	string	Defines a custom error response.	<code>returnErrorResponseCodeBased</code> is SPECIFY_YOUR_OWN

adaptiveAcceleration

- **Property Manager name:** [Adaptive Acceleration](#)
- **Behavior version:** The `v2025-05-30` rule format supports the `adaptiveAcceleration` behavior v2.3.
- **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.

Note that the [edgeSideIncludes](#) and [akamaizer](#) behaviors are not compatible with the `enableRo` and `enableBrotliCompression` options in the [adaptiveAcceleration](#) behavior for `Ion` products.

Option	Type	Description	Requires
<code>source</code>	string	The source Adaptive Acceleration uses to gather the real user monitoring timing data, either <code>MPULSE</code> or <code>REAL_USER_MONITORING</code> .	
<code>enablePush</code>	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.	
<code>enablePreconnect</code>	boolean	Allows browsers to anticipate what connections your site needs, and establishes those connections ahead of time. See Automatic Preconnect for more information.	
<code>preloadEnable</code>	boolean	Allows browsers to preload necessary fonts before they fetch and process other resources. See Automatic Font Preload for more information.	
<code>abLogic</code>	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, <code>DISABLED</code> by default. See Add A/B testing to A2 for details.	
	<code>DISABLED</code>	Disables the use of Adaptive Acceleration in the A/B testing environment. This is the default value.	
	<code>CLOUDLETS</code>	Applies A/B testing using Cloudlets.	
	<code>MANUAL</code>	Applies A/B testing by redirecting a request to one of two origin servers, based on the cookie included with the request.	
<code>cookieName</code>	string	This specifies the name of the cookie file used for redirecting the requests in the A/B testing environment.	<code>abLogic</code> is <code>MANUAL</code>
<code>enableRo</code>	boolean	Enables the Resource Optimizer, which automates the compression and delivery of your <code>.css</code> , <code>.js</code> , and <code>.svg</code> 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.	

Option	Type	Description	Requires
<code>enableBrotliCompression</code>	boolean	Applies Brotli compression, converting your origin content to cache on edge servers.	
<code>enableForNoncacheable</code>	boolean	Applies Brotli compression to non-cacheable content.	<code>enableBrotliCompression</code> is <code>true</code>

advanced

- **Property Manager name:** [Advanced](#)
- **Behavior version:** The `v2025-05-30` 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
<code>description</code>	string	Human-readable description of what the XML block does.
<code>xml</code>	string	Akamai XML metadata.

aggregatedReporting

- **Property Manager name:** [Aggregated Reporting](#)
- **Behavior version:** The `v2025-05-30` 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](#) ⁶ reports.

Option	Type	Description	Requires
<code>enabled</code>	boolean	Enables aggregated reporting.	
<code>reportName</code>	string	The unique name of the aggregated report within the property. If you reconfigure any attributes or variables in the aggregated reporting behavior, update this field to a unique value to enable logging data in a new instance of the report.	
<code>attributesCount</code>	number (1-4)	The number of attributes to include in the report, ranging from 1 to 4.	
<code>attribute1</code>	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.	
<code>attribute2</code>	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.	<code>attributesCount</code> \geq 2
<code>attribute3</code>	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.	<code>attributesCount</code> \geq 3
<code>attribute4</code>	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.	<code>attributesCount</code> is 4

akamaizer

- **Property Manager name:** [Akamaizer](#)
- **Behavior version:** The `v2025-05-30` 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 `akamaizerTag` behavior.

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

akamaizerTag

- **Property Manager name:** [Akamaize Tag](#)
- **Behavior version:** The `v2025-05-30` 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
<code>matchHostname</code>	string	Specifies the hostname to match on as a Perl-compatible regular expression.	
<code>replacement</code> <code>Hostname</code>	string	Specifies the replacement hostname for the tag to use.	
<code>scope</code>	enum	Specifies the part of HTML content the <code>tagsAttribute</code> refers to.	
	<code>ATTRIBUTE</code>	When <code>tagsAttribute</code> refers to a tag/attribute pair, the match only applies to the attribute.	
	<code>URL_</code> <code>ATTRIBUTE</code>	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.	
	<code>BLOCK</code>	Substitutes within the tag's contents, but not within any nested tags.	
	<code>PAGE</code>	Ignores the <code>tagsAttribute</code> field and performs the substitution on the entire page.	
<code>tagsAttribute</code>	enum	Specifies the tag or tag/attribute combination to operate on.	<code>scope</code> is not <code>PAGE</code>
		Supported values: <code>A</code> <code>AREA</code> <code>AREA_HREF</code> <code>A_HREF</code> <code>BASE</code> <code>BASE_HREF</code>	

Option	Type	Description	Requires
		FORM FORM_ACTION IFRAME IFRAME_SRC IMG IMG_SRC LINK LINK_HREF SCRIPT SCRIPT_SRC TABLE TABLE_BACKGROUND TD TD_BACKGROUND	
<code>replaceAll</code>	boolean	Replaces all matches when enabled, otherwise replaces only the first match.	
<code>includeTagsAttribute</code>	boolean	Whether to include the <code>tagsAttribute</code> value.	

allHttpInCacheHierarchy

- **Property Manager name:** [Allow All Methods on Parent Servers](#)
- **Behavior version:** The `v2025-05-30` 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
<code>enabled</code>	boolean	Enables all HTTP requests for parent servers in the cache hierarchy.

allowCloudletsOrigins

- **Property Manager name:** [Allow Conditional Origins](#)
- **Behavior version:** The `v2025-05-30` 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
<code>enabled</code>	boolean	Allows you to assign custom origin definitions referenced in sub-rules by <code>cloudletsOrigin</code> labels. If disabled, all sub-rules are ignored.
<code>honorBaseDirectory</code>	boolean	Prefixes any Cloudlet-generated origin path with a path defined by an Origin Base Path behavior. If no path is defined, it has no effect. If another Cloudlet policy already prepends the same Origin Base Path, the path is not duplicated.
<code>purgeOriginQueryParameter</code>	string	When purging content from a Cloudlets Origin, this specifies a query parameter name whose value is the specific named origin to purge. Note that this only applies to content purge requests, for example when using the Content Control Utility API .

allowDelete

- **Property Manager name:** [Allow DELETE](#)
- **Behavior version:** The `v2025-05-30` 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
<code>enabled</code>	boolean	Allows DELETE requests. Content does <i>not</i> cache.
<code>allowBody</code>	boolean	Allows data in the body of the DELETE request.

allowHTTPSCacheKeySharing

- **Property Manager name:** [HTTPS Cache Key Sharing](#)
- **Behavior version:** The `v2025-05-30` 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
<code>enabled</code>	boolean	Enables HTTPS cache key sharing.

allowHTTPSDowngrade

- **Property Manager name:** [Protocol Downgrade \(HTTPS Downgrade to Origin\)](#)
- **Behavior version:** The `v2025-05-30` 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
<code>enabled</code>	boolean	Downgrades to HTTP protocol for the origin server.

allowOptions

- **Property Manager name:** [Allow OPTIONS](#)
- **Behavior version:** The `v2025-05-30` 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 [constructResponse](#) behavior to send responses directly from the Akamai network. See also the [allowDelete](#), [allowPatch](#), [allowPost](#), and [allowPut](#) behaviors.

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

allowPatch

- **Property Manager name:** [Allow PATCH](#)
- **Behavior version:** The `v2025-05-30` 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
<code>enabled</code>	boolean	Allows PATCH requests. Content does <i>not</i> cache.

allowPost

- **Property Manager name:** [Allow POST](#)
- **Behavior version:** The `v2025-05-30` 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
<code>enabled</code>	boolean	Allows POST requests.
<code>allowWithoutContentLength</code>	boolean	By default, POST requests also require a <code>Content-Length</code> header, or they result in a 411 error. With this option enabled with no specified <code>Content-Length</code> , the edge server relies on a <code>Transfer-Encoding</code> header to chunk the data. If neither header is present, it assumes the request has no body, and it adds a header with a <code>0</code> value to the forward request.

allowPut

- **Property Manager name:** [Allow PUT](#)
- **Behavior version:** The `v2025-05-30` 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
<code>enabled</code>	boolean	Allows PUT requests. Content does <i>not</i> cache.

allowTransferEncoding

- **Property Manager name:** [Chunked Transfer Encoding](#)
- **Behavior version:** The `v2025-05-30` 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
<code>enabled</code>	boolean	Allows Chunked Transfer Encoding requests.

altSvcHeader

- **Property Manager name:** [Alt-Svc Header](#)
- **Behavior version:** The `v2025-05-30` 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
<code>maxAge</code>	number	Specifies the <code>max-age</code> value in seconds for the <code>Alt-Svc</code> header. The default <code>max-age</code> for an <code>Alt-Svc</code> header is 93600 seconds (26 hours).

apiPrioritization

- **Property Manager name:** [API Prioritization Cloudlet](#)
- **Behavior version:** The `v2025-05-30` 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
<code>enabled</code>	boolean	Activates the API Prioritization feature.	
<code>isSharedPolicy</code>	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 .	
<code>cloudletPolicy</code>	object	Identifies the Cloudlet policy.	<code>isSharedPolicy</code> is <code>false</code>
<code>cloudletPolicy.id</code>	number	Identifies the Cloudlet.	
<code>cloudletPolicy.name</code>	string	The Cloudlet's descriptive name.	
<code>cloudletSharedPolicy</code>	number	Identifies the Cloudlet shared policy to use with this behavior. Use the Cloudlets API to list available shared policies.	<code>isSharedPolicy</code> is <code>true</code>
<code>label</code>	string	A label to distinguish this API Prioritization policy from any others in the same property.	
<code>useThrottledCpCode</code>	boolean	Specifies whether to apply an alternative CP code for requests served the alternate response.	

Option	Type	Description	Requires
<code>throttledCpCode</code>	object	Specifies the CP code as an object. You only need to provide the initial <code>id</code> , stripping any <code>cp_</code> prefix to pass the integer to the rule tree. Additional CP code details may reflect back in subsequent read-only data.	<code>useThrottledCpCode</code> is <code>true</code>
<code>throttledCpCode.cpCodeLimits</code>	array	Read-only. Describes the current usage limit for the CP code.	
<code>throttledCpCode.createdDate</code>	integer	Read-only. UNIX epoch timestamp reflecting when the CP code was originally created.	
<code>throttledCpCode.description</code>	string	Read-only. Additional description for the CP code.	
<code>throttledCpCode.id</code>	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 <code>cpcodeId</code> value from the List CP codes operation.	
<code>throttledCpCode.name</code>	string	Read-only. The name of the CP code you specify as the <code>cpcodeName</code> 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.	
<code>throttledCpCode.products</code>	array	Read-only. The set of products the CP code is assigned to. This reflects <code>productId</code> values you specify when creating a new CP code in PAPI.	
<code>useThrottledStatusCode</code>	boolean	Allows you to assign a specific HTTP response code to a throttled request.	
<code>throttledStatusCode</code>	number	Specifies the HTTP response code for requests that receive the alternate response.	<code>useThrottledStatusCode</code> is <code>true</code>
<code>netStorage</code>	object	Specify the NetStorage domain that contains the alternate response.	
<code>netStorage.cpCode</code>	integer	Identifies a CP code assigned to this storage group.	
<code>netStorage.downloadDomainName</code>	string	Domain name from which content can be downloaded.	
<code>netStorage.g2oToken</code>	string	Signature Header Authentication key.	
<code>netStorage.id</code>	integer	Unique identifier for the storage group.	
<code>netStorage.name</code>	string	Name of the storage group.	
<code>netStoragePath</code>	string	Specify the full NetStorage path for the alternate response, including trailing file name.	
<code>alternateResponseCacheTtl</code>	number (5-30)	Specifies the alternate response's time to live in the cache, <code>5</code> minutes by default.	

applicationLoadBalancer

- **Property Manager name:** [Application Load Balancer Cloudlet](#)

- **Behavior version:** The `v2025-05-30` 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
<code>enabled</code>	boolean	Activates the Application Load Balancer Cloudlet.	
<code>cloudletPolicy</code>	object	Identifies the Cloudlet policy.	
<code>cloudletPolicy.id</code>	number	Identifies the Cloudlet.	
<code>cloudletPolicy.name</code>	string	The Cloudlet's descriptive name.	
<code>label</code>	string	A label to distinguish this Application Load Balancer policy from any others within the same property.	
<code>stickinessCookieType</code>	enum	Determines how a cookie persistently associates the client with a load-balanced origin.	
	<code>NONE</code>	Dynamically reassigns different load-balanced origins for each request.	
	<code>NEVER</code>	Preserves the cookie indefinitely.	
	<code>ON_BROWSER_CLOSE</code>	Limit the cookie duration to browser sessions.	
	<code>FIXED_DATE</code>	Specify a specific time for when the cookie expires.	
	<code>DURATION</code>	Specify a delay for when the cookie expires.	
	<code>ORIGIN_SESSION</code>	Limit the cookie duration to when the <code>ORIGIN_SESSION</code> terminates. (After the cookie expires, the cookie type re-evaluates.)	
<code>stickinessExpirationDate</code>	string (epoch timestamp)	Specifies when the cookie expires.	<code>stickinessCookieType</code> is <code>FIXED_DATE</code>
<code>stickinessDuration</code>	string (duration)	Sets how long it is before the cookie expires.	<code>stickinessCookieType</code> is <code>DURATION</code>
<code>stickinessRefresh</code>	boolean	Extends the duration of the cookie with each new request. When enabled, the <code>DURATION</code> thus specifies the latency between requests that would cause the cookie to expire.	<code>stickinessCookieType</code> is <code>DURATION</code>
<code>originCookieName</code>	string	Specifies the name for your session cookie.	<code>stickinessCookieType</code> is <code>ORIGIN_SESSION</code>
<code>specifyStickinessCookieDomain</code>	boolean	Specifies whether to use a cookie domain with the stickiness cookie, to tell the browser to which domain to send the cookie.	<code>stickinessCookieType</code> is either: <code>ON_BROWSER_CLOSE</code> , <code>FIXED_DATE</code> , <code>DURATION</code> , <code>NEVER</code> , <code>ORIGIN_SESSION</code>
<code>stickinessCookieDomain</code>	string	Specifies the domain to track the stickiness cookie.	<code>specifyStickinessCookieDomain</code> is <code>true</code>
<code>stickinessCookieAutomaticSalt</code>	boolean	Sets whether to assign a <code>salt</code> 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.	<code>stickinessCookieType</code> is either: <code>ON_BROWSER_CLOSE</code> , <code>FIXED_DATE</code> , <code>DURATION</code> , <code>NEVER</code> , <code>ORIGIN_SESSION</code>

Option	Type	Description	Requires
<code>stickinessCookieSalt</code>	string	Specifies the stickiness cookie's salt value. Use this option to share the cookie across many properties.	<code>stickinessCookieAutomaticSalt</code> is <code>false</code>
<code>stickinessCookieSetHttpOnlyFlag</code>	boolean	Ensures the cookie is transmitted only over HTTP.	<code>stickinessCookieType</code> is either: <code>ON_BROWSER_CLOSE</code> , <code>FIXED_DATE</code> , <code>DURATION</code> , <code>NEVER</code> , <code>ORIGIN_SESSION</code>
<code>allDownNetStorage</code>	object	Specifies a NetStorage account for a static maintenance page as a fallback when no origins are available.	
<code>allDownNetStorage.cpCode</code>	integer	Identifies a CP code assigned to this storage group.	
<code>allDownNetStorage.downloadDomainName</code>	string	Domain name from which content can be downloaded.	
<code>allDownNetStorage.g2oToken</code>	string	Signature Header Authentication key.	
<code>allDownNetStorage.id</code>	integer	Unique identifier for the storage group.	
<code>allDownNetStorage.name</code>	string	Name of the storage group.	
<code>allDownNetStorage.File</code>	string	Specifies the fallback maintenance page's filename, expressed as a full path from the root of the Net Storage server.	
<code>allDownStatusCode</code>	string	Specifies the HTTP response code when all load-balancing origins are unavailable.	
<code>failoverStatusCodes</code>	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.	
<code>failoverMode</code>	enum	Determines what to do if an origin fails.	
	<code>AUTOMATIC</code>	Automatically determines which origin in the policy to try next.	
	<code>MANUAL</code>	You define a sequence of failover origins. (If failover runs out of origins, requests are sent to NetStorage.)	
	<code>DISABLED</code>	Turns off failover, but maintains origin stickiness even when the origin goes down.	
<code>failoverOriginMap</code>	object array	Specifies a fixed set of failover mapping rules.	<code>failoverMode</code> is <code>MANUAL</code>
<code>failoverOriginMap[].fromOriginId</code>	string	Specifies the origin whose failure triggers the mapping rule.	
<code>failoverOriginMap[].toOriginIds</code>	string array	Requests stuck to the <code>fromOriginId</code> origin retry for each alternate origin <code>toOriginIds</code> , until one succeeds.	
<code>failoverAttemptsThreshold</code>	number	Sets the number of failed requests that would trigger the failover process.	<code>failoverMode</code> is either: <code>MANUAL</code> , <code>AUTOMATIC</code>
<code>allowCachePrefresh</code>	boolean	Allows the cache to prefetch. Only appropriate if all origins serve the same content for the same URL.	

audienceSegmentation

- **Property Manager name:** [Audience Segmentation Cloudlet](#)
- **Behavior version:** The `v2025-05-30` 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
<code>enabled</code>	boolean	Enables the Audience Segmentation cloudlet feature.	
<code>isSharedPolicy</code>	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 .	
<code>cloudletPolicy</code>	object	Identifies the Cloudlet policy.	<code>isSharedPolicy</code> is <code>false</code>
<code>cloudletPolicy.id</code>	number	Identifies the Cloudlet.	
<code>cloudletPolicy.name</code>	string	The Cloudlet's descriptive name.	
<code>cloudletSharedPolicy</code>	number	This identifies the Cloudlet shared policy to use with this behavior. You can list available shared policies with the Cloudlets API .	<code>isSharedPolicy</code> is <code>true</code>
<code>label</code>	string	Specifies a suffix to append to the cookie name. This helps distinguish this audience segmentation policy from any others within the same property.	
<code>segmentTrackingMethod</code>	enum	Specifies the method to pass segment information to the origin. The Cloudlet passes the rule applied to a given request location.	
		Supported values: <code>IN_COOKIE_HEADER</code> <code>IN_CUSTOM_HEADER</code> <code>IN_QUERY_PARAM</code> <code>NONE</code>	
<code>segmentTrackingQueryParam</code>	string	This query parameter specifies the name of the segmentation rule.	<code>segmentTrackingMethod</code> is <code>IN_QUERY_PARAM</code>
<code>segmentTrackingCookieName</code>	string	This cookie name specifies the name of the segmentation rule.	<code>segmentTrackingMethod</code> is <code>IN_COOKIE_HEADER</code>
<code>segmentTrackingCustomHeader</code>	string	This custom HTTP header specifies the name of the segmentation rule.	<code>segmentTrackingMethod</code> is <code>IN_CUSTOM_HEADER</code>

Option	Type	Description	Requires
<code>populationCookieType</code>	enum	Specifies when the segmentation cookie expires.	
	<code>NEVER</code>	Never expire.	
	<code>ON_BROWSER_CLOSE</code>	Expire at end of browser session.	
	<code>DURATION</code>	Specify a delay.	
<code>populationDuration</code>	string (duration)	Specifies the lifetime of the segmentation cookie.	<code>populationCookieType</code> is <code>DURATION</code>
<code>populationRefresh</code>	boolean	If disabled, sets the expiration time only if the cookie is not yet present in the request.	<code>populationCookieType</code> is <code>DURATION</code>
<code>specifyPopulationCookieDomain</code>	boolean	Whether to specify a cookie domain with the population cookie. It tells the browser to which domain to send the cookie.	
<code>populationCookieDomain</code>	string	Specifies the domain to track the population cookie.	<code>specifyPopulationCookieDomain</code> is <code>true</code>
<code>populationCookieAutomaticSalt</code>	boolean	Whether to assign a <i>salt</i> value automatically to the cookie to prevent manipulation by the user. You should not enable if sharing the population cookie across more than one property.	
<code>populationCookieSalt</code>	string	Specifies the cookie's salt value. Use this option to share the cookie across many properties.	<code>populationCookieAutomaticSalt</code> is <code>false</code>
<code>populationCookieIncludeRuleName</code>	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 `v2025-05-30` 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 `v2025-05-30` 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
<code>value</code>	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 <code>/parent/child/</code> .

bossBeaconing

- **Property Manager name:** [Diagnostic data beacons \(Ex. BOSS\)](#)
- **Behavior version:** The `v2025-05-30` 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
<code>enabled</code>	boolean	Enable diagnostic data beacons.
<code>cpcodes</code>	string	The space-separated list of CP codes that trigger the beacons. You need to specify the same set of CP codes within BOSS.
<code>requestType</code>	enum	Specify when to trigger a beacon.
	<code>EDGE</code>	For edge requests only.
	<code>EDGE_MIDGRESS</code>	Both end and midgress requests.
<code>forwardType</code>	enum	Specify when to trigger a beacon.
	<code>MIDGRESS</code>	For internal midgress forwards only.
	<code>ORIGIN</code>	For origin forwards only.
	<code>MIDGRESS_ORIGIN</code>	Both.
<code>sampling Frequency</code>	enum	Specifies a sampling frequency or disables beacons.
	<code>SAMPLING_ FREQ_0_0</code>	Disables beacons altogether.
	<code>SAMPLING_ FREQ_0_1</code>	Specifies a sampling frequency.
<code>conditional Sampling Frequency</code>	enum	Specifies a conditional sampling frequency or disables beacons.
	<code>CONDITIONAL_ SAMPLING_FREQ_0_0</code>	Disables beacons altogether.
	<code>CONDITIONAL_ SAMPLING_FREQ_0_1</code>	Specifies a sampling frequency.
	<code>CONDITIONAL_ SAMPLING_FREQ_0_2</code>	Specifies a sampling frequency.
	<code>CONDITIONAL_ SAMPLING_FREQ_0_3</code>	Specifies a sampling frequency.
<code>conditional HTTPStatus</code>	string array	Specifies the set of response status codes or ranges that trigger the beacon.
		Supported values: <div> <div>0xx</div> <div>304</div> <div>401</div> <div>404</div> <div>4xx</div> <div>503</div> <div>6xx</div> </div> <div> <div>302</div> <div>3xx</div> <div>403</div> <div>408</div> <div>500</div> <div>5xx</div> </div>
<code>conditionalError Pattern</code>	string	A space-separated set of error patterns that trigger beacons to conditional feeds. Each pattern can include wildcards, where <code>?</code> matches a single character and <code>*</code> matches zero or more characters. For example, <code>*CONNECT* *DENIED*</code> matches two different words as substrings.

breadcrumbs

- **Property Manager name:** [Breadcrumbs](#)
- **Behavior version:** The `v2025-05-30` 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
<code>enabled</code>	boolean	Enables the Breadcrumbs feature.
<code>optMode</code>	boolean	Specifies whether to include Breadcrumbs data in the response header. To bypass the current <code>optMode</code> , append the opposite <code>ak-bc</code> query string to each request from your player.
<code>logging Enabled</code>	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 `v2025-05-30` 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
<code>enabled</code>	boolean	Enables the break connection behavior.

broccoli

- **Property Manager name:** [Brotli Support](#)
- **Behavior version:** The `v2025-05-30` rule format supports the `broccoli` 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.

Note: If you're using Ion and want Akamai to compress your content on edge servers, use these behaviors instead:

- [adaptiveAcceleration](#) . Ion properties include this by default. It offers several forms of compression, including Brotli. See the [Ion guide](#) for more details.
- [adaptiveImageCompression](#) . This is a separate module you can add to your contract.

Note that the [edgeSideIncludes](#) and [akamaiizer](#) behaviors are not compatible with the `enableRo` and `enableBrotli` options in the [adaptiveAcceleration](#) behavior for Ion products.

Option	Type	Description
<code>enabled</code>	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 `v2025-05-30` rule format supports the `cacheError` behavior v1.1.
- **Rule format status:** [Deprecated, outdated rule format](#)
- **Access:** [Read/Write](#)
- **Allowed in includes:** [Yes](#)

With the `caching` behavior also enabled, this caches the origin's error responses to decrease server load. It 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.

Note that the `cacheError` behavior works only with the `caching` behavior enabled.

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

cacheld

- **Property Manager name:** [Cache ID Modification](#)
- **Behavior version:** The `v2025-05-30` 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
<code>rule</code>	<code>enum</code>	Specifies how to modify the cache ID.	
	<code>INCLUDE_QUERY_PARAMS</code>	Includes the specified set of query parameters when forming a cache ID.	
	<code>INCLUDE_COOKIES</code>	Includes specified cookies in the cache ID.	
	<code>INCLUDE_HEADERS</code>	Includes specified HTTP headers in the cache ID.	
	<code>EXCLUDE_QUERY_PARAMS</code>	Excludes the specified set of query parameters when forming a cache ID.	
	<code>INCLUDE_ALL_QUERY_PARAMS</code>	Includes all query parameters when forming a cache ID.	
	<code>INCLUDE_VARIABLE</code>	Includes a specific user variable in the cache ID.	
	<code>INCLUDE_URL</code>	Includes the full URL, the same as the default without the <code>cacheid</code> behavior.	
<code>include Value</code>	<code>boolean</code>	Includes the value of the specified elements in the cache ID. Otherwise only their names are included.	<code>rule is either: INCLUDE_COOKIES , INCLUDE_QUERY_PARAMS , INCLUDE_HEADERS</code>
<code>optional</code>	<code>boolean</code>	Requires the behavior's specified elements to be present for content to cache. When disabled, requests that lack the specified elements are still cached.	<code>rule is either: INCLUDE_COOKIES , INCLUDE_QUERY_PARAMS , INCLUDE_HEADERS , EXCLUDE_QUERY_PARAMS</code>
<code>elements</code>	<code>string array</code>	Specifies the names of the query parameters, cookies, or headers to include or exclude from the cache ID.	<code>rule is either: INCLUDE_COOKIES , INCLUDE_QUERY_PARAMS , INCLUDE_HEADERS , EXCLUDE_QUERY_PARAMS</code>
<code>variable Name</code>	<code>string (variable name)</code>	Specifies the name of the variable you want to include in the cache key.	<code>rule is INCLUDE_VARIABLE</code>

cacheKeyIgnoreCase

- **Property Manager name:** [Ignore Case In Cache Key](#)
- **Behavior version:** The `v2025-05-30` 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
<code>enabled</code>	boolean	Ignores case when forming cache keys.

cacheKeyQueryParams

- **Property Manager name:** [Cache Key Query Parameters](#)
- **Behavior version:** The `v2025-05-30` 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
<code>behavior</code>	enum	Configures how sets of query string parameters translate to cache keys. Be careful not to ignore any parameters that result in substantially different content, as it is <i>not</i> reflected in the cached object.	
	<code>INCLUDE_ALL_PRESERVE_ORDER</code>	Forms a separate key for the entire set of query parameters, but sensitive to the order in which they appear. (For example, <code>?q=akamai&state=ma</code> and <code>?state=ma&q=akamai</code> cache separately.)	
	<code>INCLUDE_ALL_ALPHABETIZE_ORDER</code>	Forms keys for the entire set of parameters, but the order doesn't matter. The examples above both use the same cache key.	
	<code>IGNORE_ALL</code>	Causes query string parameters to be ignored when forming cache keys.	

Option	Type	Description	Requires
	INCLUDE	Include the sequence of values in the <code>parameters</code> field.	
	IGNORE	Include all but the sequence of values in the <code>parameters</code> field.	
<code>parameters</code>	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.	<code>behavior</code> is either: <code>INCLUDE</code> , <code>IGNORE</code>
<code>exactMatch</code>	boolean	When enabled, <code>parameters</code> needs to match exactly. Keep disabled to match string prefixes.	<code>behavior</code> is either: <code>INCLUDE</code> , <code>IGNORE</code>

cacheKeyRewrite

- **Property Manager name:** [Cache Key Path Rewrite \(Beta\)](#)
- **Behavior version:** The `v2025-05-30` 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
<code>purgeKey</code>	string	Specifies the new cache key path as an alphanumeric value.

cachePost

- **Property Manager name:** [Cache POST Responses](#)
- **Behavior version:** The `v2025-05-30` 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
<code>enabled</code>	boolean	Enables caching of POST responses.
<code>useBody</code>	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 <code>Content-Type</code> is <code>application/x-www-form-urlencoded</code> . (Use this in conjunction with <code>cacheId</code> to define relevant query parameters.)

cacheRedirect

- **Property Manager name:** [Cache HTTP Temporary Redirects](#)
- **Behavior version:** The `v2025-05-30` 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
<code>enabled</code>	boolean	Enables the redirect caching behavior.

cacheTag

- **Property Manager name:** [Cache Tag](#)
- **Behavior version:** The `v2025-05-30` 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 `dynamicThroughputOptimization` behavior. Don't include both behaviors in a rule for the same request.

Option	Type	Description
<code>tag</code>	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: <code>[!#\$%'+./^_` ~-]</code>

cacheTagVisible

- **Property Manager name:** [Cache Tag Visibility](#)
- **Behavior version:** The `v2025-05-30` 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
<code>behavior</code>	enum	Specifies when to include the <code>Edge-Cache-Tag</code> in responses.
	<code>NEVER</code>	Strip out the <code>Edge-Cache-Tag</code> header, edge servers' default response.
	<code>PRAGMA_HEADER</code>	Edge servers respond with the <code>Edge-Cache-Tag</code> header only when you pass in a <code>Pragma: akamai-x-get-cache-tags</code> header as part of the request.
	<code>ALWAYS</code>	Include the <code>Edge-Cache-Tag</code> header in all responses.

caching

- **Property Manager name:** [Caching](#)
- **Behavior version:** The `v2025-05-30` 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
<code>behavior</code>	enum	Specify the caching option.	
	<code>MAX_AGE</code>	Honor the origin's <code>MAX_AGE</code> header.	
	<code>NO_STORE</code>	Clears the cache and serves from the origin.	
	<code>BYPASS_CACHE</code>	Retains the cache but serves from the origin.	
	<code>CACHE_CONTROL_AND_EXPIRES</code>	Honor the origin's <code>CACHE_CONTROL</code> or <code>EXPIRES</code> header, whichever comes last. This adds support for the <code>s-maxage</code> response directive specified in RFC 7234 . Use this alternative value to instruct a downstream CDN how long to cache content.	

Option		Type	Description	Requires
		CACHE_ CONTROL	Honor the origin's <code>CACHE_CONTROL</code> header. This adds support for the <code>s-maxage</code> response directive specified in RFC 7234 . Use this alternative value to instruct a downstream CDN how long to cache content.	
		EXPIRES	Honor the origin's <code>EXPIRES</code> 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 <code>no-cache</code> header, which forces content to revalidate.	behavior is MAX_AGE
defaultTtl		string (duration)	Set the <code>MAX_AGE</code> header for the cached content.	behavior is either: CACHE_CONTROL_AND_ EXPIRES , CACHE_CONTROL , EXPIRES
enhancedRfc Support		boolean	This enables honoring particular <code>Cache-Control</code> header directives from the origin. Supports all official RFC 7234 directives except for <code>no-transform</code> .	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 <code>no-store</code> directive.	enhancedRfcSupport is true
honor Private		boolean	Instructs edge servers not to cache the response when the origin response includes the <code>private</code> directive.	behavior is either: CACHE_CONTROL , CACHE_ CONTROL_AND_EXPIRES
honorNo Cache		boolean	With the <code>no-cache</code> directive present in the response, this instructs edge servers to validate or refetch the response for each request. Effectively, set the time to live <code>ttl</code> to zero seconds.	enhancedRfcSupport is true
honorMaxAge		boolean	This instructs edge servers to cache the object for a length of time set by the <code>max-age</code> directive in the response. When present in the origin response, this directive takes precedence over the <code>max-age</code> directive and the <code>defaultTtl</code> setting.	enhancedRfcSupport is true
honor SMaxage		boolean	Instructs edge servers to cache the object for a length of time set by the <code>s-maxage</code> directive in the response. When present in the origin response, this directive takes precedence over the <code>max-age</code> directive and the <code>defaultTtl</code> setting.	enhancedRfcSupport is true
honorMust 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
honorProxy Revalidate		boolean	With the <code>proxy-revalidate</code> 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 `v2025-05-30` 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
<code>enabled</code>	boolean	Enables the centralized authorization behavior.

chaseRedirects

- **Property Manager name:** [Chase Redirects](#)
- **Behavior version:** The `v2025-05-30` 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
<code>enabled</code>	boolean	Allows edge servers to chase redirects.
<code>limit</code>	string	Specifies, as a string, the maximum number of redirects to follow.
<code>serve404</code>	boolean	Once the redirect <code>limit</code> is reached, enabling this option serves an HTTP <code>404</code> (Not Found) error instead of the last redirect.

clientCertificateAuth

- **Property Manager name:** [Client Certificate Authentication](#)
- **Behavior version:** The `v2025-05-30` rule format supports the `clientCertificateAuth` behavior v1.0.
- **Rule format status:** [Deprecated, outdated rule format](#)
- **Access:** [Read/Write](#)
- **Allowed in includes:** [Yes](#)

Sends a `Client-To-Edge` header to your origin server with details from the mutual TLS certificate sent from the requesting client to the edge network. This establishes transitive trust between the client and your origin server.

Option	Type	Description
<code>enable</code>	boolean	Constructs the <code>Client-To-Edge</code> authentication header using information from the client to edge mTLS handshake and forwards it to your origin. You can configure your origin to acknowledge the header to enable transitive trust. Some form of the client x.509 certificate needs to be included in the header. You can include the full certificate or specific attributes.
<code>enableCompleteClientCertificate</code>	boolean	Whether to include the complete client certificate in the header, in its binary (DER) format. DER-formatted certificates leave out the <code>BEGIN CERTIFICATE/END CERTIFICATE</code> statements and most often use the <code>.der</code> extension. Alternatively, you can specify individual <code>clientCertificateAttributes</code> you want included in the request.
<code>clientCertificateAttributes</code>	string array	Specify client certificate attributes to include in the <code>Client-To-Edge</code> authentication header that's sent to your origin server.
	<code>SUBJECT</code>	The distinguished name of the client certificate's public key, in the <code>Client-To-Edge</code> authentication header.
	<code>COMMON_NAME</code>	The common name (CN) that's been set in the client certificate, in the <code>Client-To-Edge</code> authentication header.
	<code>SHA256_FINGERPRINT</code>	An SHA-256 encrypted fingerprint of the client certificate, in the <code>Client-To-Edge</code> authentication header.
	<code>ISSUER</code>	The distinguished name of the entity that issued the certificate, in the <code>Client-To-Edge</code> authentication header.
<code>enableClientCertificateValidationStatus</code>	boolean	Whether to include the current validation status of the client certificate in the <code>Client-To-Edge</code> authentication header. This verifies the validation status of the certificate, regardless of the certificate attributes you're including in the header.

clientCharacteristics

- **Property Manager name:** [Client Characteristics](#)
- **Behavior version:** The `v2025-05-30` 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
<code>country</code>	enum	Specifies the client request's geographic region.
	<code>GLOBAL</code>	Global.
	<code>GLOBAL_US_CENTRIC</code>	Regional.
	<code>GLOBAL_EU_CENTRIC</code>	Regional.
	<code>GLOBAL_ASIA_CENTRIC</code>	Regional.
	<code>EUROPE</code>	Europe.
	<code>NORTH_AMERICA</code>	North America.
	<code>SOUTH_AMERICA</code>	South America.
	<code>NORDICS</code>	Northern Europe.
	<code>ASIA_PACIFIC</code>	Asia and Pacific Islands.
	<code>AUSTRALIA</code>	Australia.
	<code>GERMANY</code>	Germany.
	<code>INDIA</code>	India.
	<code>ITALY</code>	Italy.
	<code>JAPAN</code>	Japan.
	<code>TAIWAN</code>	Taiwan.
	<code>UNITED_KINGDOM</code>	United Kingdom.
	<code>OTHER</code>	A fallback value.
	<code>UNKNOWN</code>	Defer any optimizations.

cloudInterconnects

- **Property Manager name:** [Cloud Interconnects for Google Cloud \(GCP\)](#).
- **Behavior version:** The `v2025-05-30` 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
<code>enabled</code>	boolean	Channels the traffic to maximize the egress discount at the origin.
<code>cloudLocations</code>	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.
	<code>AS</code>	Asia.
	<code>EU</code>	Europe.
	<code>NA</code>	North America.

cloudWrapper

- **Property Manager name:** [Cloud Wrapper](#)
- **Behavior version:** The `v2025-05-30` 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
<code>enabled</code>	boolean	Enables Cloud Wrapper behavior.
<code>location</code>	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 `v2025-05-30` 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
<code>enabled</code>	boolean	Enables failover for Cloud Wrapper.	
<code>failoverMap</code>	string	Specifies the failover map to handle Cloud Wrapper failures. Contact your account representative for more information.	
<code>custom</code> <code>FailoverMap</code>	string (allows variables)	Specifies the custom failover map to handle Cloud Wrapper failures. Contact your account representative for more information.	<code>failoverMap</code> is Custom

commonMediaClientData

- **Property Manager name:** [Common Media Client Data support](#)
- **Behavior version:** The `v2025-05-30` 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
<code>enableCMCDSegmentPrefetch</code>	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 `v2025-05-30` 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. For example, you might want to send a customized response if the URL doesn't point to an object on the origin server, or if the end user is not authorized to view the requested content. You can use it with all request methods you allow for your property, including POST. For more details, see the [allowOptions](#), [allowPatch](#), [allowPost](#), [allowPut](#), and [allowDelete](#) behaviors.

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												
<code>enabled</code>	boolean	Serves the custom response.												
<code>body</code>	string (allows variables)	HTML response of up to 2000 characters to send to the end-user client.												
<code>responseCode</code>	enum	The HTTP response code to send to the end-user client.												
		Supported values: <table><tr><td>200</td><td>403</td><td>405</td><td>500</td><td>502</td><td>504</td></tr><tr><td>401</td><td>404</td><td>417</td><td>501</td><td>503</td><td></td></tr></table>	200	403	405	500	502	504	401	404	417	501	503	
200	403	405	500	502	504									
401	404	417	501	503										

Option	Type	Description
<code>forceEviction</code>	boolean	For GET requests from clients, this forces edge servers to evict the underlying object from cache. Defaults to <code>false</code> .
<code>ignorePurge</code>	boolean	Whether to ignore the custom response when purging.

contentCharacteristics

- **Property Manager name:** [Content Characteristics](#)
- **Behavior version:** The `v2025-05-30` 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
<code>objectSize</code>	enum	Optimize based on the size of the object retrieved from the origin.
	<code>LESS_THAN_1MB</code>	Less than 1Mb.
	<code>ONE_MB_TO_TEN_MB</code>	1-10 Mb.
	<code>TEN_MB_TO_100_MB</code>	10-100 Mb.
	<code>OTHER</code>	A fallback value.
	<code>UNKNOWN</code>	Defer this optimization.
<code>popularityDistribution</code>	enum	Optimize based on the content's expected popularity.
	<code>LONG_TAIL</code>	A low volume of requests over a long period.
	<code>ALL_POPULAR</code>	A high volume of requests over a short period.
	<code>OTHER</code>	A fallback value.
	<code>UNKNOWN</code>	Defer this optimization.
<code>catalogSize</code>	enum	Optimize based on the total size of the content library delivered.
	<code>SMALL</code>	Under 100GB.

Option	Type	Description
	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 v2025-05-30 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.	

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

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

Option	Type	Description	Requires
	ONE_MB_TO_TEN_MB	1-10Mb.	
	TEN_MB_TO_100_MB	10-100Mb.	
	GREATER_THAN_100MB	More than 100Mb.	
	UNKNOWN	Defer this optimization.	
	OTHER	Sizes that straddle these ranges.	
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.	
segmentDurationSmooth Custom	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 `v2025-05-30` 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
<code>objectSize</code>	enum	Optimize based on the size of the object retrieved from the origin.
	<code>LESS_THAN_1MB</code>	Less than 1Mb.
	<code>ONE_MB_TO_TEN_MB</code>	1-10Mb.
	<code>TEN_MB_TO_100_MB</code>	10-100Mb.
	<code>GREATER_THAN_100MB</code>	More than 100Mb.
	<code>OTHER</code>	A fallback value.
	<code>UNKNOWN</code>	Defer this optimization.
<code>popularityDistribution</code>	enum	Optimize based on the content's expected popularity.
	<code>LONG_TAIL</code>	A low volume of requests over a long period.
	<code>ALL_POPULAR</code>	A high volume of requests over a short period.
	<code>OTHER</code>	A fallback value.
	<code>UNKNOWN</code>	Defer this optimization.
<code>catalogSize</code>	enum	Optimize based on the total size of the content library delivered.
	<code>SMALL</code>	Less than 100Gb.
	<code>MEDIUM</code>	100Gb-1Tb.
	<code>LARGE</code>	1-100Tb.
	<code>EXTRA_LARGE</code>	More than 100Tb.
	<code>OTHER</code>	A fallback value.
	<code>UNKNOWN</code>	Defer this optimization.
<code>contentType</code>	enum	Optimize based on the type of content.
	<code>VIDEO</code>	Video.
	<code>SOFTWARE</code>	Software.
	<code>SOFTWARE_PATCH</code>	Software patch.
	<code>GAME</code>	Game.
	<code>GAME_PATCH</code>	Game patch.
	<code>OTHER_DOWNLOADS</code>	Other downloads that don't fall into these categories.

Option	Type	Description
	UNKNOWN	Defer this optimization.
optimizeOption	boolean	Optimizes the delivery throughput and download times for large files.

contentCharacteristicsWsdLive

- **Property Manager name:** [Content Characteristics - Streaming Video Live](#)
- **Behavior version:** The v2025-05-30 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.	

Option	Type	Description	Requires
popularity Distribution	enum	Optimize based on the content's expected popularity.	
	LONG_TAIL	A low volume of requests over a long period.	
	ALL_POPULAR	A high volume of requests over a short period.	
	UNKNOWN	Defer this optimization.	
hls	boolean	Enable delivery of HLS media.	
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

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

contentTargetingProtection

- **Property Manager name:** [Content Targeting - Protection](#)
- **Behavior version:** The `v2025-05-30` 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
<code>enabled</code>	boolean	Enables the Content Targeting feature.	
<code>enableGeoProtection</code>	boolean	When enabled, verifies IP addresses are unique to specific geographic regions.	
<code>geoProtectionMode</code>	enum	Specifies how to handle requests.	<code>enableGeoProtection</code> is <code>true</code>
	<code>ALLOW</code>	Allow requests.	
	<code>DENY</code>	Deny requests.	
<code>countries</code>	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.	<code>enableGeoProtection</code> is <code>true</code>
<code>regions</code>	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.	<code>enableGeoProtection</code> is <code>true</code>
<code>dmcs</code>	string array	Specifies the set of Designated Market Area codes from which to allow or deny traffic. See EdgeScape Data Codes [®] for a list.	<code>enableGeoProtection</code> is <code>true</code>
<code>overrideIPAddresses</code>	string array	Specify a set of IP addresses or CIDR blocks that exceptions to the set of included or excluded areas.	<code>enableGeoProtection</code> is <code>true</code>
<code>enableGeoRedirectOnDeny</code>	boolean	When enabled, redirects denied requests rather than responding with an error code.	<code>enableGeoProtection</code> is <code>true</code>
<code>geoRedirectUrl</code>	string	This specifies the full URL to the redirect page for denied requests.	<code>enableGeoRedirectOnDeny</code> is <code>true</code>
<code>enableIPProtection</code>	boolean	Allows you to control access to your content from specific sets of IP addresses and CIDR blocks.	
<code>ipProtectionMode</code>	enum	Specifies how to handle requests.	<code>enableIPProtection</code> is <code>true</code>
	<code>ALLOW</code>	Allow requests.	
	<code>DENY</code>	Deny requests.	
<code>ipAddresses</code>	string array	Specify a set of IP addresses or CIDR blocks to allow or deny.	<code>enableIPProtection</code> is <code>true</code>
<code>enableIPRedirectOnDeny</code>	boolean	When enabled, redirects denied requests rather than responding with an error code.	<code>enableIPProtection</code> is <code>true</code>
<code>ipRedirectUrl</code>	string	This specifies the full URL to the redirect page for denied requests.	<code>enableIPRedirectOnDeny</code> is <code>true</code>
<code>enableReferrerProtection</code>	boolean	Allows you allow traffic from certain referring websites, and disallow traffic from unauthorized sites that hijack those links.	

Option	Type	Description	Requires
<code>referrerProtectionMode</code>	enum	Specify the action to take.	<code>enableReferrerProtection</code> is <code>true</code>
	<code>ALLOW</code>	Allow requests.	
	<code>DENY</code>	Deny requests.	
<code>referrerDomains</code>	string array	Specifies the set of domains from which to allow or deny traffic.	<code>enableReferrerProtection</code> is <code>true</code>
<code>enableReferrerRedirectOnDeny</code>	boolean	When enabled, redirects denied requests rather than responding with an error code.	<code>enableReferrerProtection</code> is <code>true</code>
<code>referrerRedirectUrl</code>	string	This specifies the full URL to the redirect page for denied requests.	<code>enableReferrerRedirectOnDeny</code> is <code>true</code>

corsSupport

- **Property Manager name:** [CORS Protocol Support](#)
- **Behavior version:** The `v2025-05-30` 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
<code>enabled</code>	boolean	Enables CORS feature.	
<code>allowOrigins</code>	enum	In responses to preflight requests, sets which origin hostnames to accept requests from.	
	<code>ANY</code>	Accept from any origin hostname.	
	<code>SPECIFIED</code>	Accept from a set of origin hostnames.	
<code>origins</code>	string array	Defines the origin hostnames to accept requests from. The hostnames that you enter need to start with <code>http</code> or <code>https</code> . For detailed hostname syntax requirements, refer to RFC-952 and RFC-1123 specifications.	<code>allowOrigins</code> is <code>SPECIFIED</code>
<code>allowCredentials</code>	boolean	Accepts requests made using credentials, like cookies or TLS client certificates.	

Option	Type	Description	Requires
<code>allowHeaders</code>	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.	
<code>headers</code>	string array	Defines the supported request headers.	<code>allowHeaders</code> is SPECIFIED
<code>methods</code>	string array	Specifies any combination of the following methods that are allowed when accessing the resource from an external domain: <code>DELETE</code> , <code>GET</code> , <code>PATCH</code> , <code>POST</code> , <code>HEAD</code> , and <code>PUT</code> .	
<code>exposeHeaders</code>	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: <code>Cache-Control</code> , <code>Content-Language</code> , <code>Content-Type</code> , <code>Expires</code> , <code>Last-Modified</code> , and <code>Pragma</code> . You can add other header names to make them accessible to clients.	
<code>preflightMaxAge</code>	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 `v2025-05-30` 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
<code>value</code>	object	Specifies the CP code as an object. You only need to provide the initial <code>id</code> , stripping any <code>cpc_</code> <code>prefix</code> to pass the integer to the rule tree. Additional CP code details may reflect back in subsequent read-only data.
<code>value.cpCodeLimits</code>	array	Read-only. Describes the current usage limit for the CP code.

Option	Type	Description
<code>value.createdDate</code>	integer	Read-only. UNIX epoch timestamp reflecting when the CP code was originally created.
<code>value.description</code>	string	Read-only. Additional description for the CP code.
<code>value.id</code>	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 <code>cpcodeId</code> value from the List CP codes operation.
<code>value.name</code>	string	Read-only. The name of the CP code you specify as the <code>cpcodeName</code> 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.
<code>value.products</code>	array	Read-only. The set of products the CP code is assigned to. This reflects <code>productId</code> values you specify when creating a new CP code in PAPI.

customBehavior

- **Property Manager name:** [Custom Behavior](#)
- **Behavior version:** The `v2025-05-30` 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
<code>behaviorId</code>	string	The unique identifier for the predefined custom behavior you want to insert into the current rule.

datastream

- **Property Manager name:** [DataStream](#)

- **Behavior version:** The `v2025-05-30` 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
<code>streamType</code>	enum	Specify the DataStream type.	
	<code>BEACON</code>	Low latency streaming of raw or aggregated data for push delivery or through the pull API.	
	<code>LOG</code>	Scalable, low latency streaming of raw data for push delivery.	
	<code>BEACON_</code> <code>AND_LOG</code>	Specify both.	
<code>enabled</code>	boolean	Enables DataStream reporting.	
<code>datastream</code> <code>Ids</code>	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.	
<code>logEnabled</code>	boolean	Enables log collection for the property by associating it with DataStream configurations.	<code>streamType</code> is either: <code>LOG</code> , <code>BEACON_AND_LOG</code>
<code>logStream</code> <code>Name</code>	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.	<code>logEnabled</code> is <code>true</code>
<code>sampling</code> <code>Percentage</code>	number	Specifies the percentage of log data you want to collect for this property.	<code>logEnabled</code> is <code>true</code>
<code>collect</code> <code>Midgress</code> <code>Traffic</code>	boolean	If enabled, gathers midgress traffic data within the Akamai platform, such as between two edge servers, for all streams configured.	<code>logEnabled</code> is <code>true</code>

dcp

- **Property Manager name:** [IoT Edge Connect](#)
- **Behavior version:** The `v2025-05-30` 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
<code>enabled</code>	boolean	Enables IoT Edge Connect.
<code>namespaceId</code>	string	Specifies the globally reserved name for a specific configuration. It includes authorization rules over publishing and subscribing to logical categories known as <i>topics</i> . This provides a root path for all topics defined within a namespace configuration. You can use the IoT Edge Connect API to configure access control lists for your namespace configuration.
<code>tlsenabled</code>	boolean	When enabled, you can publish and receive messages over a secured MQTT connection on port 8883.
<code>wsenabled</code>	boolean	When enabled, you can publish and receive messages through a secured MQTT connection over WebSockets on port 443.
<code>gwenabled</code>	boolean	When enabled, you can publish and receive messages over a secured HTTP connection on port 443.
<code>anonymous</code>	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 `v2025-05-30` 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 [dcpAuthSubstringTransformation](#) 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 v2025-05-30 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 <code>^(.{0,10})</code> omits the first character, but then captures up to 10 characters after that. If the regular expression does not capture a substring, authentication may fail.

dcpAuthSubstringTransformation

- **Property Manager name:** [Variable Substring Transformation](#)
- **Behavior version:** The `v2025-05-30` 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
<code>substring</code> 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.
<code>substring</code> End	string	The zero-based index offset of the last character to extract, where <code>-1</code> 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 `v2025-05-30` 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: [dcpAuthHMACTransformation](#) , [dcpAuthRegexTransformation](#) , Or [dcpAuthSubstringTransformation](#) .

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

dcpDefaultAuthzGroups

- **Property Manager name:** [Default Authorization Groups](#)
- **Behavior version:** The `v2025-05-30` 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
<code>groupNames</code>	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 `v2025-05-30` 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
<code>enabled</code>	boolean	Enables the default JWT server and sets the authentication endpoint to a default path.	
<code>customValues</code>	boolean	Allows you to specify custom JWT server connection values.	
<code>hostname</code>	string	Specifies the JWT server's hostname.	<code>customValues</code> is <code>true</code>
<code>path</code>	string	Specifies the path to your JWT server's authentication endpoint. This lets you generate JWTs to sign your requests.	<code>customValues</code> is <code>true</code>

deliveryReceipt

- **Property Manager name:** [Cloud Monitor Data Delivery](#).
- **Behavior version:** The `v2025-05-30` 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 `v2025-05-30` 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
<code>reason</code>	string	Text message that keys why access is denied. Any subsequent <code>denyAccess</code> behaviors within the rule tree may refer to the same <code>reason</code> key to override the current behavior.

Option	Type	Description
enabled	boolean	Denies access when enabled.

denyDirectFailoverAccess

- **Property Manager name:** [Security Failover Protection](#)
- **Behavior version:** The v2025-05-30 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 v2025-05-30 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
<code>elements</code>	string array	Specifies a set of information about the device with which to generate a separate cache key.
		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 XHTMLP_PREFERRED_MIME_TYPE XHTML_FILE_UPLOAD XHTML_PREFERRED_CHARSET XHTML_SUPPORTS_IFRAME XHTML_SUPPORTS_TABLE_FOR_LAYOUT XHTML_SUPPORT_LEVEL XHTML_TABLE_SUPPORT

deviceCharacteristicHeader

- **Property Manager name:** [Device Characterization - Forward in Header](#)
- **Behavior version:** The `v2025-05-30` 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
<code>elements</code>	string array	Specifies the set of information about the requesting device to send to the origin server.
		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 XHTLMMP_PREFERRED_MIME_TYPE XHTML_FILE_UPLOAD XHTML_PREFERRED_CHARSET XHTML_SUPPORTS_IFRAME XHTML_SUPPORTS_TABLE_FOR_LAYOUT XHTML_SUPPORT_LEVEL XHTML_TABLE_SUPPORT

dnsAsyncRefresh

- **Property Manager name:** [DNS Asynchronous Refresh](#)
- **Behavior version:** The `v2025-05-30` 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
<code>enabled</code>	boolean	Allows edge servers to refresh an expired DNS record after serving content.
<code>timeout</code>	string (duration)	Set the maximum allowed time an expired DNS record may be active.

dnsPrefresh

- **Property Manager name:** [DNS Prefresh](#)
- **Behavior version:** The `v2025-05-30` 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
<code>enabled</code>	boolean	Allows edge servers to refresh DNS records before they expire.
<code>delay</code>	string (duration)	Specifies the amount of time following a DNS record's expiration to asynchronously prefetch it.
<code>timeout</code>	string (duration)	Specifies the amount of time to prefetch a DNS entry if there have been no requests to the domain name.

downgradeProtocol

- **Property Manager name:** [Protocol Downgrade](#)
- **Behavior version:** The `v2025-05-30` 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 `v2025-05-30` 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 `v2025-05-30` 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 `v2025-05-30` 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
<code>behavior</code>	enum	Specify the caching instructions the edge server sends to the end user's client.	
	<code>ALLOW</code>	The value of <code>allowBehavior</code> chooses the caching method and headers to send to the client.	
	<code>MUST_REVALIDATE</code>	This equates to a <code>Cache-Control: no-cache</code> header, which allows caching but forces the client browser to send an <code>if-modified-since</code> request each time it requests the object.	
	<code>BUST</code>	Sends cache-busting headers downstream.	
	<code>TUNNEL_ORIGIN</code>	This passes <code>Cache-Control</code> and <code>Expires</code> headers from the origin to the downstream client.	
	<code>NONE</code>	Don't send any caching headers. Allow client browsers to cache content according to their own default settings.	
<code>allowBehavior</code>	enum	Specify how the edge server calculates the downstream cache by setting the value of the <code>Expires</code> header.	<code>behavior</code> is <code>ALLOW</code>
	<code>LESSER</code>	Sends the lesser value of what the origin specifies and the edge cache's remaining duration. This is the default behavior.	

Option	Type	Description	Requires
	GREATER	Sends the greater value of what the origin specifies and the edge cache's remaining duration.	
	REMAINING_LIFETIME	Sends the value of the edge cache's remaining duration, without comparing it to the origin's headers.	
	FROM_MAX_AGE	Sends the <code>cache:max-age</code> value applied to the object, without evaluating the cache's duration.	
	FROM_VALUE	Sends the value of the edge cache's duration.	
	PASS_ORIGIN	Sends the value of the origin's header, without evaluating the edge cache's duration.	
<code>ttl</code>	string (duration)	Sets the duration of the cache. Setting the value to <code>0</code> equates to a <code>no-cache</code> header that forces revalidation.	<code>allowBehavior</code> is <code>FROM_VALUE</code>
<code>sendHeaders</code>	enum	Specifies the HTTP headers to include in the response to the client.	<code>behavior</code> is <code>ALLOW</code>
	CACHE_CONTROL_AND_EXPIRES	Sends both <code>Cache-Control</code> and <code>Expires</code> header.	
	CACHE_CONTROL	Sends only the origin's <code>Cache-Control</code> header.	
	EXPIRES	Sends only the origin's <code>Expires</code> header.	
	PASS_ORIGIN	Sends the same set of <code>Cache-Control</code> and <code>Expires</code> headers received from the origin.	
<code>sendPrivate</code>	boolean	Adds a <code>Cache-Control: private</code> header to prevent objects from being cached in a shared caching proxy.	<code>behavior</code> is either: <code>ALLOW</code> , <code>MUST_REVALIDATE</code> AND <code>sendHeaders</code> is not <code>EXPIRES</code>

dynamicThroughputOptimization

- **Property Manager name:** [Quick Retry](#)
- **Behavior version:** The `v2025-05-30` rule format supports the `dynamicThroughputOptimization` 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
<code>enabled</code>	boolean	Enables the quick retry feature.

dynamicThroughputOptimizationOverride

- **Property Manager name:** [Quick Retry Override](#)
- **Behavior version:** The `v2025-05-30` rule format supports the `dynamicThroughputOptimizationOverride` 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 [dynamicThroughputOptimization](#) 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
<code>throughput</code>	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.

earlyData

- **Property Manager name:** [Early Data \(0-RTT\)](#)
- **Behavior version:** The `v2025-05-30` rule format supports the `earlyData` behavior v1.0.
- **Rule format status:** [Deprecated, outdated rule format](#)

- **Access:** [Read/Write](#)
- **Allowed in includes:** [No \(temporarily\)](#)

Use this behavior to enable sending early data during the TLS 1.3 handshake between requests from your client and Akamai edge servers. This is available for QUIC connections and Transmission Control Protocol (TCP).

To use Early Data, your certificate needs to support transport layer security (TLS) version 1.3. This ensures your origin server understands the `Early-Data` header and correctly generates the 425 (Too Early) status code.

Option	Type	Description
<code>enabled</code>	boolean	Enables sending early data, which further reduces latency in TLS 1.3 connections.

earlyDataAdvanced

- **Property Manager name:** [Early_Data \(0-RTT\) Advanced](#)
- **Behavior version:** The `v2025-05-30` rule format supports the `earlyDataAdvanced` behavior v1.1.
- **Rule format status:** [Deprecated, outdated rule format](#)
- **Access:** [Read/Write](#)
- **Allowed in includes:** [No \(temporarily\)](#)

Use this behavior to allow query string parameters in early data, also known as 0-RTT data.

Note that the base `earlyData` behavior needs to be present in the property in order to use the `earlyDataAdvanced` behavior.

Option	Type	Description
<code>allowQueryStringParams</code>	boolean	Allows support for URLs with query string parameters. When disabled, URLs that contain query strings aren't eligible for early data processing, and are rejected with a 425 Too Early status code.
<code>supportedHttpMethods</code>	string array	Sets the HTTP methods to use Early Data for, with allowed values: <code>GET</code> , <code>PUT</code> , <code>POST</code> , <code>DELETE</code> , <code>HEAD</code> , and <code>OPTIONS</code> . The default is only <code>GET</code> .
	<code>GET</code>	Allows support for the GET method.
	<code>HEAD</code>	Allows support for the HEAD method.
	<code>OPTIONS</code>	Allows support for the OPTIONS method.
	<code>POST</code>	Allows support for the POST method.
	<code>PUT</code>	Allows support for the PUT method.
	<code>DELETE</code>	Allows support for the DELETE method.

earlyHints

- **Property Manager name:** [Early Hints](#)
- **Behavior version:** The `v2025-05-30` rule format supports the `earlyHints` behavior v1.0.
- **Rule format status:** [Deprecated, outdated rule format](#)
- **Access:** [Read/Write](#)
- **Allowed in includes:** [Yes](#)

Use Early Hints to send an HTTP 103 status code with preliminary HTTP headers at the client request stage, so that a browser can preload critical website resources or preconnect to a specific domain while waiting for the final response.

The 103 response occurs only when the `Sec-Fetch-Mode` request header’s value is `navigate` . Since this is a default setting that’s already a part of the behavior’s logic, you don’t need to set any additional match criteria. However, if you add this behavior to a rule where a `[requestHeader](#)` criteria matches a `Sec-Fetch-Mode` value other than `navigate``, you get a validation error.

See the [Property Manager guide](#) for more caveats, examples, and implementations using EdgeWorkers.

Option	Type	Description
<code>enabled</code>	boolean	Enable the behavior so that browsers can use that waiting time to preload the resource URLs you specify or preconnect to static or image domains.
<code>resource Url</code>	string (allows variables)	Enter the URL to a resource you want clients to receive as an early hint. Edge servers include each resource URL you provide in an instance of the <code>Link</code> header that’s sent back to the client in the HTTP 103 response. You only need to specify the value of the header, as edge servers automatically add the <code>Link</code> header name to the response. Use commas to separate multiple entries. This field supports variables and string concatenation. The URL must be enclosed between <code><</code> and <code>></code> as shown in the example below. Example: <code><https://cdn.example.com/assets/main1.css>;rel=preload;as=style, <https://cdn.example.com/assets/main2.css>;rel=preload;as=style</code>

ecmsBulkUpload

- **Property Manager name:** [Message Store bulk upload](#)
- **Behavior version:** The `v2025-05-30` 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
<code>enabled</code>	boolean	Enables sending a compressed archive file with objects. Sends the archive file to the default path of the target data set: <code><hostname>/bulk/<database_name>/<dataset_name></code> .

ecmsDatabase

- **Property Manager name:** [Message Store database selection](#)
- **Behavior version:** The `v2025-05-30` 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
<code>database</code>	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: <code><hostname>/datastore/<data_set_name>/<object_key></code> .	
<code>extract Location</code>	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.	

Option	Type	Description	Requires
	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 <code>X-KV-Database</code> .	extract Location is CLIENT_ REQUEST_HEADER
query Parameter Name	string	Specifies the query string parameter that passed the database name. By default, it points to <code>database</code> .	extract Location is QUERY_STRING
regex Pattern	string	Specifies the regular expression that matches the database name in the URL.	extract Location is REGEX

ecmsDataset

- **Property Manager name:** [Message Store data set selection](#)
- **Behavior version:** The `v2025-05-30` 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: <code><hostname>/datastore/<database_name>/<object_key></code> .	
extract Location	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.	

Option	Type	Description	Requires
	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 <code>x-KV-Dataset</code> .	extract Location is CLIENT_ REQUEST_HEADER
query Parameter Name	string	Specifies the query string parameter that passed the data set name. By default, it points to <code>dataset</code> .	extract Location is QUERY_STRING
regex Pattern	string	Specifies the regular expression that matches the data set name in the URL.	extract Location is REGEX

ecmsObjectKey

- **Property Manager name:** [Message Store object key selection](#)
- **Behavior version:** The `v2025-05-30` 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: <code><hostname>/bulk/<database_name>/<dataset_name></code> .

edgeConnect

- **Property Manager name:** [Cloud Monitor Instrumentation](#)
- **Behavior version:** The `v2025-05-30` 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
<code>enabled</code>	boolean	Enables Cloud Monitor's log-publishing behavior.	
<code>apiConnector</code>	enum	Describes the API connector type.	
		Supported values: BMC_APM SIEM_JSON DEFAULT	
<code>apiDataElements</code>	string array	Specifies the data set to log.	
		Supported values: APM GEO HTTP NETWORK_PERFORMANCE NETWORK_V1 REQUEST_HEADER RESPONSE_HEADER SEC_APP_V2 SEC_RATE_DENY_V2 SEC_RATE_WARN_V2	
<code>destinationHostname</code>	string	Specifies the target hostname accepting push API requests.	
<code>destinationPath</code>	string	Specifies the push API's endpoint.	
<code>overrideAggregateSettings</code>	boolean	When enabled, overrides default log settings.	
<code>aggregateTime</code>	string (duration)	Specifies how often logs are generated.	<code>overrideAggregateSettings</code> is <code>true</code>
<code>aggregateLines</code>	string	Specifies the maximum number of lines to include in each log.	<code>overrideAggregateSettings</code> is <code>true</code>
<code>aggregateSize</code>	string	Specifies the log's maximum size.	<code>overrideAggregateSettings</code> is <code>true</code>

edgeLoadBalancingAdvanced

- **Property Manager name:** [Edge Load Balancing: Advanced Metadata](#)
- **Behavior version:** The `v2025-05-30` 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
<code>description</code>	string	A description of what the <code>xml</code> block does.
<code>xml</code>	string	A block of Akamai XML metadata.

edgeLoadBalancingDataCenter

- **Property Manager name:** [Edge Load Balancing: Data Center](#)
- **Behavior version:** The `v2025-05-30` 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
<code>originId</code>	string	Corresponds to the <code>id</code> specified by the edgeLoadBalancingOrigin behavior associated with this data center.	
<code>description</code>	string	Provides a description for the ELB data center, for your own reference.	
<code>hostname</code>	string	Specifies the data center's hostname.	
<code>cookieName</code>	string	If using session persistence, this specifies the value of the cookie named in the corresponding edgeLoadBalancingOrigin behavior's <code>cookie_name</code> option.	
<code>enableFailover</code>	boolean	Allows you to specify failover rules.	
<code>ip</code>	string	Specifies this data center's IP address.	<code>enableFailover</code> is <code>true</code>
<code>failoverRules</code>	object array	Provides up to four failover rules to apply in the specified order.	<code>enableFailover</code> is <code>true</code>
<code>failoverRules[].failoverHostname</code>	string	The hostname of the data center to fail over to.	
<code>failoverRules[].modifyRequest</code>	boolean	Allows you to modify the request's hostname or path.	
<code>failoverRules[].overrideHostname</code>	boolean	Overrides the request's hostname with the <code>failover_hostname</code> .	<code>modifyRequest</code> is <code>true</code>
<code>failoverRules[].contextRoot</code>	string	Specifies the path to use in the forwarding request, typically the root (/) when failing over to a different data center, or a full path such as <code>/static/error.html</code> when failing over to an error page.	<code>modifyRequest</code> is <code>true</code>
<code>failoverRules[].absolutePath</code>	boolean	When enabled, interprets the path specified by <code>context_root</code> as an absolute server path, for example to reference a site-down page. Otherwise when disabled, the path is appended to the request.	<code>modifyRequest</code> is <code>true</code>

edgeLoadBalancingOrigin

- **Property Manager name:** [Edge Load Balancing: Origin Definition](#)
- **Behavior version:** The `v2025-05-30` 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
<code>id</code>	string	Specifies a unique descriptive string for this ELB origin. The value needs to match the <code>origin_id</code> specified by the edgeLoadBalancingDataCenter behavior associated with this origin.	
<code>description</code>	string	Provides a description for the ELB origin, for your own reference.	
<code>hostname</code>	string	Specifies the hostname associated with the ELB rule.	
<code>enableSessionPersistence</code>	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.	
<code>cookieName</code>	string	This specifies the name of the cookie that marks users' persistent sessions. The accompanying edgeLoadBalancingDataCenter behavior's <code>description</code> option specifies the cookie's value.	<code>enableSessionPersistence</code> is <code>true</code>

edgeOriginAuthorization

- **Property Manager name:** [Edge Server Identification](#)
- **Behavior version:** The `v2025-05-30` 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
<code>enabled</code>	boolean	Enables the cookie-authorization behavior.

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

edgeRedirector

- **Property Manager name:** [Edge Redirector Cloudlet](#)
- **Behavior version:** The `v2025-05-30` 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
<code>enabled</code>	boolean	Enables the Edge Redirector Cloudlet.	
<code>isSharedPolicy</code>	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 .	
<code>cloudletPolicy</code>	object	Specifies the Cloudlet policy as an object.	<code>isSharedPolicy</code> is <code>false</code>
<code>cloudletPolicy.id</code>	number	Identifies the Cloudlet.	
<code>cloudletPolicy.name</code>	string	The Cloudlet's descriptive name.	
<code>cloudletSharedPolicy</code>	number	Identifies the Cloudlet shared policy to use with this behavior. Use the Cloudlets API to list available shared policies.	<code>isSharedPolicy</code> is <code>true</code>

edgeScape

- **Property Manager name:** [Content Targeting \(EdgeScape\)](#)
- **Behavior version:** The `v2025-05-30` 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
<code>enabled</code>	boolean	When enabled, sends the <code>X-Akamai-Edgescape</code> request header to the origin.

edgeSideIncludes

- **Property Manager name:** [ESI \(Edge Side Includes\)](#)
- **Behavior version:** The `v2025-05-30` 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
<code>enabled</code>	boolean	Enables ESI processing.	
<code>enableViaHttp</code>	boolean	Enable ESI only for content featuring the <code>Edge-control: dca=esi</code> HTTP response header.	

Option	Type	Description	Requires
<code>passSetCookie</code>	boolean	Allows edge servers to pass your origin server's cookies to the ESI processor.	<code>enableViaHttp</code> is <code>true</code>
<code>passClientIp</code>	boolean	Allows edge servers to pass the client IP header to the ESI processor.	<code>enableViaHttp</code> is <code>true</code>
<code>i18nStatus</code>	boolean	Provides internationalization support for ESI.	<code>enableViaHttp</code> is <code>true</code>
<code>i18nCharset</code>	string array	Specifies the character sets to use when transcoding the ESI language, <code>UTF-8</code> and <code>ISO-8859-1</code> for example.	<code>i18nStatus</code> is <code>true</code>
<code>detectInjection</code>	boolean	Denies attempts to inject ESI code.	

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
<code>enabled</code>	boolean	Applies the Input Validation Cloudlet behavior.	
<code>cloudletPolicy</code>	object	Identifies the Cloudlet policy.	
<code>cloudletPolicy.id</code>	number	Identifies the Cloudlet.	
<code>cloudletPolicy.name</code>	string	The Cloudlet's descriptive name.	

Option	Type	Description	Requires
<code>label</code>	string	Distinguishes this Input Validation policy from any others within the same property.	
<code>userIdentificationByCookie</code>	boolean	When enabled, identifies users by the value of a cookie.	
<code>userIdentificationByKeyCookie</code>	string	This specifies the cookie name whose value needs to remain constant across requests to identify a user.	<code>userIdentificationByCookie</code> is <code>true</code>
<code>userIdentificationByIp</code>	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.	
<code>userIdentificationByHeaders</code>	boolean	When enabled, identifies users by specific HTTP headers on GET or POST requests.	
<code>userIdentificationKeyHeaders</code>	string array	This specifies the HTTP headers whose combined set of values identify each end user.	<code>userIdentificationByHeaders</code> is <code>true</code>
<code>userIdentificationByParams</code>	boolean	When enabled, identifies users by specific query parameters on GET or POST requests.	
<code>userIdentificationKeyParams</code>	string array	This specifies the query parameters whose combined set of values identify each end user.	<code>userIdentificationByParams</code> is <code>true</code>
<code>allowLargePostBody</code>	boolean	Fails POST request bodies that exceed 16 KB when enabled, otherwise allows them to pass with no validation for policy compliance.	
<code>resetOnValid</code>	boolean	Upon receiving a valid request, enabling this resets the <code>penaltyThreshold</code> counter to zero. Otherwise, even those series of invalid requests that are interrupted by valid requests may trigger the <code>penaltyAction</code> .	
<code>validateOnOriginWith</code>	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.	
	<code>DISABLED</code>	Specify if no additional validation is necessary.	
	<code>RESPONSE_CODE</code>	Use a response code.	
	<code>RESPONSE_CODE_AND_HEADER</code>	Use a response code and header.	
<code>validateOnOriginHeaderName</code>	string	If <code>validateOnOriginWith</code> is set to <code>RESPONSE_CODE_AND_HEADER</code> , this specifies the header name for a request that the origin identifies as invalid.	<code>validateOnOriginWith</code> is <code>RESPONSE_CODE_AND_HEADER</code>
<code>validateOnOriginHeaderValue</code>	string	If <code>validateOnOriginWith</code> is set to <code>RESPONSE_CODE_AND_HEADER</code> , this specifies an invalid request's header value that corresponds to the <code>validateOnOriginHeaderName</code> .	<code>validateOnOriginWith</code> is <code>RESPONSE_CODE_AND_HEADER</code>
<code>validateOnOriginResponseCode</code>	number	Unless <code>validateOnOriginWith</code> is <code>DISABLED</code> , this identifies the integer response code for requests the origin identifies as invalid.	<code>validateOnOriginWith</code> is either: <code>RESPONSE_CODE</code> , <code>RESPONSE_CODE_AND_HEADER</code>
<code>failure302Uri</code>	string	Specifies the redirect link for invalid requests that have not yet triggered a penalty.	
<code>penaltyThreshold</code>	number	Specifies the number of invalid requests permitted before executing the <code>penaltyAction</code> .	
<code>penaltyAction</code>	enum	Once the <code>penaltyThreshold</code> of invalid requests is met, this specifies the response.	

Option	Type	Description	Requires
	REDIRECT_302	A 302 redirect response.	
	BLANK_403	A 403 response with no body content.	
	BRANDED_403	A custom 403 response.	
penalty302Uri	string	Specifies the redirect link for end users who trigger the penalty.	penaltyAction is REDIRECT_302
penaltyNetStorage	object	Specifies the NetStorage account that serves out the penalty's static 403 response content. Details appear in an object featuring a downloadDomainName string member that identifies the NetStorage hostname, and an integer cpCode to track the traffic.	penaltyAction is BRANDED_403
penaltyNetStorage.cpCodeList	array	A set of CP codes that apply to this storage group.	
penaltyNetStorage.downloadDomainName	string	Domain name from which content can be downloaded.	
penaltyNetStorage.id	number	Unique identifier for the storage group.	
penaltyNetStorage.name	string	Name of the storage group.	
penaltyNetStorage.uploadDomainName	string	Domain name used to upload content.	
penalty403NetStoragePath	string	Specifies the full path to the static 403 response content relative to the downloadDomainName in the penaltyNetStorage object.	penaltyAction is BRANDED_403
penaltyBrandedDenyCacheTtl	number (5-30)	Specifies the penalty response's time to live in the cache, 5 minutes by default.	penaltyAction is BRANDED_403

edgeWorker

- **Property Manager name:** [EdgeWorkers](#)
- **Behavior version:** The v2025-05-30 rule format supports the edgeWorker behavior v1.9.
- **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
<code>enabled</code>	boolean	When enabled, applies specified EdgeWorker functionality to this rule's web traffic.
<code>edgeWorkerId</code>	string	Identifies the EdgeWorker application to apply to this rule's web traffic. You can use the EdgeWorkers API to get this value.
<code>mPulse</code>	boolean	Enables mPulse reports that include data about EdgeWorkers errors generated due to JavaScript errors. For more details, see Integrate mPulse reports with EdgeWorkers .

enforceMtlsSettings

- **Property Manager name:** [Enforce mTLS settings](#)
- **Behavior version:** The `v2025-05-30` rule format supports the `enforceMtlsSettings` behavior v1.0.
- **Rule format status:** [Deprecated, outdated rule format](#)
- **Access:** [Read/Write](#)
- **Allowed in includes:** [Yes](#)

This behavior repeats mTLS validation checks between a requesting client and the edge network. If the checks fail, you can deny the request or apply custom error handling. To use this behavior, you need to add either the `hostname` or `clientCertificate` criteria to the same rule.

Option	Type	Description	Requires
<code>enableAuthSet</code>	boolean	Whether to require a specific mutual transport layer security (mTLS) certificate authority (CA) set in a request from a client to the edge network.	
<code>certificateAuthoritySet</code>	string	Specify the client certificate authority (CA) sets you want to support in client requests. Run the List CA Sets operation in the mTLS Edge TrustStore API to get the <code>setId</code> value and pass it in this option as a string. If a request includes a set not defined here, it will be denied. The preset list items you can select are contingent on the CA sets you've created using the mTLS Edge Truststore, and then associated with a certificate in the Certificate Provisioning System .	<code>enableAuthSet is true</code>
<code>enableOcspStatus</code>	boolean	Whether the mutual transport layer security requests from a client should use the online certificate support protocol (OCSP). OCSP can determine the x.509 certificate revocation status during the TLS handshake.	
<code>enableDenyRequest</code>	boolean	This denies a request from a client that doesn't match what you've set for the options in this behavior. When disabled, non-matching requests are allowed, but you can incorporate a custom handling operation, such as reviewing generated log entries to see the discrepancies, enable the <code>Client-To-Edge</code> authentication header, or issue a custom message. This behavior only checks the Certificate Provisioning System settings. It doesn't check the current client certificate and doesn't deny invalid certs.	<code>enableAuthSet is true</code> OR <code>enableOcspStatus is true</code>

enhancedAkamaiProtocol

- **Property Manager name:** [Enhanced Akamai Protocol](#)
- **Behavior version:** The `v2025-05-30` 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.

enhancedDebug

- **Property Manager name:** [Enhanced Debug](#)
- **Behavior version:** The `v2025-05-30` rule format supports the `enhancedDebug` behavior v1.0.
- **Rule format status:** [Deprecated, outdated rule format](#)
- **Access:** [Read/Write](#)
- **Allowed in includes:** [Yes](#)

This behavior, available by default for all products, provides support for enhanced debugging on edge servers. It includes all the functionality provided by the existing `Pragma` header debugging, but is more secure and provides additional information. All requests that use this behavior pass an auth token that you generate using a secret debug key in the `Akamai-Debug` request header.

Option	Type	Description	Requires
<code>enableDebug</code>	boolean	Enables enhanced debugging using the <code>Akamai-Debug</code> request header.	
<code>debugKey</code>	object array	Specifies the debug key to use for all requests processed by this property. The debug key value needs to be a 64-byte hex string. You can generate the key in one property and then reuse it in other configurations.	<code>enableDebug</code> is <code>true</code>
<code>disablePragma</code>	boolean	Whether you want to disable the standard debugging that uses the <code>Pragma</code> request header.	<code>enableDebug</code> is <code>true</code>
<code>generateGrn</code>	boolean	Whether you want to return the Global Request Number (GRN) in the <code>Akamai-GRN</code> response header for all requests, even if the <code>Akamai-Debug</code> request header is not passed. The <code>Akamai-GRN</code> header is useful for log extraction.	<code>enableDebug</code> is <code>true</code>

enhancedProxyDetection

- **Property Manager name:** [Enhanced Proxy Detection with GeoGuard](#)
- **Behavior version:** The `v2025-05-30` rule format supports the `enhancedProxyDetection` behavior v1.3.
- **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
<code>enabled</code>	boolean	Applies GeoGuard proxy detection.	
<code>forwardHeaderEnrichment</code>	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 or three-letter designation. See the epdForwardHeaderEnrichment behavior for details.	
<code>enableConfigurationMode</code>	enum	Specifies how to field the proxy request.	
	<code>BEST_PRACTICE</code>	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.	

Option	Type	Description	Requires
	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.	
bestPracticeAction	enum	Specifies how to field the proxy request.	enableConfiguration Mode is BEST_PRACTICE
	ALLOW	Allow the request.	
	DENY	Deny the request.	
	REDIRECT	Respond with a redirect.	
bestPracticeRedirecturl	string (allows variables)	This specifies the URL to which to redirect requests.	bestPracticeAction is REDIRECT
detectAnonymousVpn	boolean	This detects requests from anonymous VPNs.	enableConfiguration Mode is ADVANCED
detectAnonymousVpnAction	enum	Specifies how to field anonymous VPN requests.	detectAnonymousVpn is true
	ALLOW	Allow the request.	
	DENY	Deny the request.	
	REDIRECT	Respond with a redirect.	
detectAnonymousVpnRedirecturl	string (allows variables)	This specifies the URL to which to redirect anonymous VPN requests.	detectAnonymousVpnAction is REDIRECT
detectPublicProxy	boolean	This detects requests from public proxies.	enableConfiguration Mode is ADVANCED
detectPublicProxyAction	enum	Specifies how to field public proxy requests.	detectPublicProxy is true
	ALLOW	Allow the request.	
	DENY	Deny the request.	
	REDIRECT	Respond with a redirect.	
detectPublicProxyRedirecturl	string (allows variables)	This specifies the URL to which to redirect public proxy requests.	detectPublicProxyAction is REDIRECT
detectTorExitNode	boolean	This detects requests from Tor exit nodes.	enableConfiguration Mode is ADVANCED
detectTorExitNodeAction	enum	This specifies whether to DENY , ALLOW , or REDIRECT requests from Tor exit nodes.	detectTorExitNode is true
	ALLOW	Allow the request.	
	DENY	Deny the request.	
	REDIRECT	Respond with a redirect.	
detectTorExitNodeRedirecturl	string (allows variables)	This specifies the URL to which to redirect requests from Tor exit nodes.	detectTorExitNodeAction is REDIRECT
detectSmartDNSProxy	boolean	This detects requests from smart DNS proxies.	enableConfiguration Mode is ADVANCED
detectSmartDNSProxyAction	enum	Specifies whether to DENY , ALLOW , or REDIRECT smart DNS proxy requests.	detectSmartDNSProxy is true

Option	Type	Description	Requires
	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 DNSProxyAction is REDIRECT
detectHosting Provider	boolean	This detects requests from a hosting provider.	enableConfiguration Mode is ADVANCED
detectHosting ProviderAction	enum	This specifies whether to DENY , ALLOW , or REDIRECT requests from hosting providers.	detectHosting Provider is true
	ALLOW	Allow the request.	
	DENY	Deny the request.	
	REDIRECT	Respond with a redirect.	
detectHosting Provider Redirecturl	string (allows variables)	This specifies the absolute URL to which to redirect requests from hosting providers.	detectHosting ProviderAction is REDIRECT
detectVpnData Center	boolean	This detects requests from VPN data centers.	enableConfiguration Mode is ADVANCED
detectVpnData CenterAction	enum	This specifies whether to DENY , ALLOW , or REDIRECT requests from VPN data centers.	detectVpnData Center is true
	ALLOW	Allow the request.	
	DENY	Deny the request.	
	REDIRECT	Respond with a redirect.	
detectVpnData Center Redirecturl	string (allows variables)	This specifies the URL to which to redirect requests from VPN data centers.	detectVpnData CenterAction is REDIRECT
detectRelayProxy	boolean	This detects requests from a relay proxy.	enableConfiguration Mode is ADVANCED
detectRelayProxy Action	enum	This specifies whether to DENY , ALLOW , or REDIRECT requests from a relay proxy.	detectRelayProxy is true
	ALLOW	Allow the request.	
	DENY	Deny the request.	
	REDIRECT	Respond with a redirect.	
detectRelayProxy Redirecturl	string (allows variables)	This specifies the URL to which to redirect requests from a relay proxy.	detectRelayProxy Action is REDIRECT
detectProxyOver Vpn	boolean	This detects requests from a proxy over VPN.	enableConfiguration Mode is ADVANCED
detectProxyOver VpnAction	enum	This specifies whether to DENY , ALLOW , or REDIRECT requests from a proxy over VPN.	detectProxyOver Vpn is true
	ALLOW	Allow the request.	
	DENY	Deny the request.	
	REDIRECT	Respond with a redirect.	

Option	Type	Description	Requires
<code>detectProxyOverVpnRedirecturl</code>	string (allows variables)	This specifies the redirect URL for requests from a proxy over VPN.	<code>detectProxyOverVpn</code> Action is REDIRECT
<code>detectResidentialProxy</code>	boolean	This detects requests from a residential proxy. See Enhanced Proxy Detection with GeoGuard and learn more about this GeoGuard category before enabling it.	<code>enableConfiguration</code> Mode is ADVANCED
<code>detectResidentialProxyAction</code>	enum	This specifies whether to DENY , ALLOW , or REDIRECT requests from residential proxies.	<code>detectResidentialProxy</code> is true
	ALLOW	Allow the request.	
	DENY	Deny the request.	
	REDIRECT	Respond with a redirect.	
<code>detectResidentialProxyRedirecturl</code>	string (allows variables)	This specifies the URL to which to redirect requests.	<code>detectResidentialProxyAction</code> is REDIRECT

epdForwardHeaderEnrichment

- **Property Manager name:** [Enhanced Proxy Detection with GeoGuard - Forward Header Enrichment](#)
- **Behavior version:** The `v2025-05-30` 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
<code>enabled</code>	boolean	<p>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 codes that indicate the IP address type detected by edge servers:</p> <ul style="list-style-type: none"> • <code>av</code> for <code>is_anonymous_vpn</code> • <code>hp</code> for <code>is_hosting_provider</code> • <code>pp</code> for <code>is_public_proxy</code> • <code>dp</code> for <code>is_smart_dns_proxy</code> • <code>tn</code> for <code>is_tor_exit_node</code>

Option	Type	Description
		<ul style="list-style-type: none"> <code>vc</code> for <code>is_vpn_datacentre</code> <code>rp</code> for <code>is_residential_proxy</code> <code>rlp</code> for <code>is_relay_proxy</code> <code>pv</code> for <code>is_proxy_over_vpn</code>

failAction

- **Property Manager name:** [Site Failover](#)
- **Behavior version:** The `v2025-05-30` 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
<code>enabled</code>	boolean	When enabled in case of a failure to contact the origin, the current behavior applies.	
<code>actionType</code>	enum	Specifies the basic action to take when there is a failure to contact the origin.	
	<code>SERVE_STALE</code>	Serves content that is already in the cache.	
	<code>REDIRECT</code>	Specifies a redirect action. (Use with these options: <code>redirectHostnameType</code> , <code>redirectHostname</code> , <code>redirectCustomPath</code> , <code>redirectPath</code> , <code>redirectMethod</code> , <code>modifyProtocol</code> , and <code>protocol</code> .)	
	<code>RECREATED_CO</code>	Serves alternate content from your network. (Use with these options: <code>contentHostname</code> , <code>contentCustomPath</code> , and <code>contentPath</code> .)	
	<code>RECREATED_CEX</code>	Serves alternate content from an external network. (Use with these options: <code>cexHostname</code> , <code>cexCustomPath</code> , and <code>cexPath</code> .)	
	<code>RECREATED_NS</code>	Serves NetStorage content. (Use with these options: <code>netStorageHostname</code> , <code>netStoragePath</code> , and <code>cpCode</code> .)	
	<code>DYNAMIC</code>	Allows you to serve dynamic SaaS content if SaaS acceleration is available on your contract. (Use with these options: <code>dynamic</code>	

Option	Type	Description	Requires
		Method , dynamicCustomPath , saasType , saasSuffix , saasRegex , and saasReplace .)	
saasType	enum	Identifies the component of the request that identifies the SaaS dynamic fail action.	actionType is DYNAMIC
		Supported values: COOKIE HOSTNAME PATH QUERY_STRING	
saasCnameEnabled	boolean	Specifies whether to use a CNAME chain to determine the hostname for the SaaS dynamic failaction.	saasType is HOSTNAME
saasCnameLevel	number	Specifies the number of elements in the CNAME chain backwards from the edge hostname that determines the hostname for the SaaS dynamic failaction.	saasCnameEnabled is true
saasCookie	string (allows variables)	Specifies the name of the cookie that identifies this SaaS dynamic failaction.	saasType is COOKIE
saasQueryString	string (allows variables)	Specifies the name of the query parameter that identifies this SaaS dynamic failaction.	saasType is QUERY_STRING
saasRegex	string	Specifies the substitution pattern (a Perl-compatible regular expression) that defines the SaaS dynamic failaction.	actionType is DYNAMIC
saasReplace	string (allows variables)	Specifies the replacement pattern that defines the SaaS dynamic failaction.	actionType is DYNAMIC
saasSuffix	string (allows variables)	Specifies the static portion of the SaaS dynamic failaction.	actionType is DYNAMIC
dynamicMethod	enum	Specifies the redirect method.	actionType is DYNAMIC
	SERVE_301	A 301 redirect response.	
	SERVE_302	A 302 redirect response.	
	SERVE_ALTERNATE	Serve an alternate response.	
dynamicCustomPath	boolean	Allows you to modify the original requested path.	actionType is DYNAMIC
dynamicPath	string (allows variables)	Specifies the new path.	dynamicCustomPath is true
redirectHostnameType	enum	Whether to preserve or customize the hostname.	actionType is REDIRECT
	ORIGINAL	Preserve the original hostname in the redirect.	
	ALTERNATE	Specify a redirectHostname .	
redirectHostname	string (allows variables)	When the actionType is REDIRECT and the redirectHostname Type is ALTERNATE , this specifies the hostname for the redirect.	redirectHostname Type is ALTERNATE
redirectCustomPath	boolean	Uses the redirectPath to customize a new path.	actionType is REDIRECT
redirectPath	string (allows variables)	Specifies a new path.	redirectCustomPath is true
redirectMethod	enum	Specifies the HTTP response code.	actionType is REDIRECT
		Supported values:	

Option	Type	Description	Requires
		301 302	
<code>contentHostname</code>	string (allows variables)	Specifies the static hostname for the alternate redirect.	<code>actionType</code> is <code>RECREATED_CO</code>
<code>contentCustomPath</code>	boolean	Specifies a custom redirect path.	<code>actionType</code> is <code>RECREATED_CO</code>
<code>contentPath</code>	string (allows variables)	Specifies a custom redirect path.	<code>contentCustomPath</code> is <code>true</code>
<code>netStorageHostname</code>	object	When the <code>actionType</code> is <code>RECREATED_NS</code> , specifies the Net Storage origin to serve the alternate content. Contact Akamai Professional Services for your NetStorage origin's <code>id</code> .	<code>actionType</code> is <code>RECREATED_NS</code>
<code>netStorageHostname.cpCode</code>	integer	Identifies a CP code assigned to this storage group.	
<code>netStorageHostname.downloadDomainName</code>	string	Domain name from which content can be downloaded.	
<code>netStorageHostname.g2oToken</code>	string	Signature Header Authentication key.	
<code>netStorageHostname.id</code>	integer	Unique identifier for the storage group.	
<code>netStorageHostname.name</code>	string	Name of the storage group.	
<code>netStoragePath</code>	string (allows variables)	When the <code>actionType</code> is <code>RECREATED_NS</code> , specifies the path for the NetStorage request.	<code>actionType</code> is <code>RECREATED_NS</code>
<code>cexHostname</code>	string (allows variables)	Specifies a hostname.	<code>actionType</code> is <code>RECREATED_CEX</code>
<code>cexCustomPath</code>	boolean	Specifies a custom path.	<code>actionType</code> is <code>RECREATED_CEX</code>
<code>cexPath</code>	string (allows variables)	Specifies a custom path.	<code>cexCustomPath</code> is <code>true</code>
<code>cpCode</code>	object	Specifies a CP code for which to log errors for the NetStorage location. You only need to provide the initial <code>id</code> , stripping any <code>cpCode.prefix</code> to pass the integer to the rule tree. Additional CP code details may reflect back in subsequent read-only data.	<code>actionType</code> is <code>RECREATED_NS</code>
<code>cpCode.cpCodeLimits</code>	array	Read-only. Describes the current usage limit for the CP code.	
<code>cpCode.createdDate</code>	integer	Read-only. UNIX epoch timestamp reflecting when the CP code was originally created.	
<code>cpCode.description</code>	string	Read-only. Additional description for the CP code.	
<code>cpCode.id</code>	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 <code>cpcodeId</code> value from the List CP codes operation.	
<code>cpCode.name</code>	string	Read-only. The name of the CP code you specify as the <code>cpcodeName</code> 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.	
<code>cpCode.products</code>	array	Read-only. The set of products the CP code is assigned to. This reflects <code>productId</code> values you specify when creating a new CP code in PAPI.	

Option	Type	Description	Requires																																																												
<code>statusCode</code>	enum	Assigns a new HTTP status code to the failure response.	<code>actionType</code> is <code>RECREATED_NS</code>																																																												
		Supported values: <table><tr><td>100</td><td>205</td><td>406</td><td>416</td><td>444</td><td>506</td></tr><tr><td>101</td><td>206</td><td>407</td><td>417</td><td>449</td><td>507</td></tr><tr><td>102</td><td>207</td><td>408</td><td>422</td><td>450</td><td>509</td></tr><tr><td>103</td><td>226</td><td>409</td><td>423</td><td>499</td><td>510</td></tr><tr><td>122</td><td>400</td><td>410</td><td>424</td><td>500</td><td>511</td></tr><tr><td>200</td><td>401</td><td>411</td><td>425</td><td>501</td><td>598</td></tr><tr><td>201</td><td>402</td><td>412</td><td>426</td><td>502</td><td>599</td></tr><tr><td>202</td><td>403</td><td>413</td><td>428</td><td>503</td><td></td></tr><tr><td>203</td><td>404</td><td>414</td><td>429</td><td>504</td><td></td></tr><tr><td>204</td><td>405</td><td>415</td><td>431</td><td>505</td><td></td></tr></table>	100	205	406	416	444	506	101	206	407	417	449	507	102	207	408	422	450	509	103	226	409	423	499	510	122	400	410	424	500	511	200	401	411	425	501	598	201	402	412	426	502	599	202	403	413	428	503		203	404	414	429	504		204	405	415	431	505		
100	205	406	416	444	506																																																										
101	206	407	417	449	507																																																										
102	207	408	422	450	509																																																										
103	226	409	423	499	510																																																										
122	400	410	424	500	511																																																										
200	401	411	425	501	598																																																										
201	402	412	426	502	599																																																										
202	403	413	428	503																																																											
203	404	414	429	504																																																											
204	405	415	431	505																																																											
<code>preserveQueryString</code>	boolean	When using either <code>contentCustomPath</code> , <code>cexCustomPath</code> , <code>dynamicCustomPath</code> , or <code>redirectCustomPath</code> to specify a custom path, enabling this passes in the original request's query string as part of the path.	<code>contentCustomPath</code> is <code>true</code> OR <code>cexCustomPath</code> is <code>true</code> OR <code>redirectCustomPath</code> is <code>true</code> OR <code>dynamicCustomPath</code> is <code>true</code>																																																												
<code>modifyProtocol</code>	boolean	Modifies the redirect's protocol using the value of the <code>protocol</code> field.	<code>actionType</code> is <code>REDIRECT</code> OR <code>dynamicMethod</code> is either: <code>SERVE_301</code> , <code>SERVE_302</code>																																																												
<code>protocol</code>	enum	When the <code>actionType</code> is <code>REDIRECT</code> and <code>modifyProtocol</code> is enabled, this specifies the redirect's protocol.	<code>modifyProtocol</code> is <code>true</code>																																																												
		Supported values: <table><tr><td>HTTP</td></tr><tr><td>HTTPS</td></tr></table>	HTTP	HTTPS																																																											
HTTP																																																															
HTTPS																																																															

failoverBotManagerFeatureCompatibility

- **Property Manager name:** Security Failover Feature Compatibility
- **Behavior version:** The `v2025-05-30` 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
<code>compatibility</code>	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 `v2025-05-30` 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
<code>enabled</code>	boolean	When enabled, forces a validation test for all edge content to which the behavior applies.

fips

- **Property Manager name:** [FIPS mode - origin](#)
- **Behavior version:** The `v2025-05-30` rule format supports the `fips` behavior v1.0.
- **Rule format status:** [Deprecated, outdated rule format](#)

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

Ensures [Federal Information Process Standards \(FIPS\) 140-2](#) compliance for a connection to an origin server. For this behavior to work properly, verify that your origin's secure certificate supports Enhanced TLS and is FIPS-compliant.

Note that you can't use `fips` if `downgradeProtocol` or `allowHTTPSDowngrade` behaviors are enabled in the same property.

Option	Type	Description
<code>enable</code>	boolean	When enabled, supports the use of FIPS-validated ciphers in the connection between this delivery configuration and your origin server.

firstPartyMarketing

- **Property Manager name:** Cloud Marketing Cloudlet (Beta)
- **Behavior version:** The `v2025-05-30` 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
<code>enabled</code>	boolean	Enables the Cloud Marketing Cloudlet.	
<code>javascriptInsertionRule</code>	enum	Select how to insert the MediaMath JavaScript reference script.	
	<code>NEVER</code>	Specify this if inserting the script at the origin.	
	<code>POLICY</code>	Allow the Cloudlet policy to determine when to insert it.	
	<code>ALWAYS</code>	Insert it for all edge requests.	
<code>cloudletPolicy</code>	object	Identifies the Cloudlet policy.	<code>javascriptInsertionRule</code> is <code>POLICY</code>

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

firstPartyMarketingPlus

- **Property Manager name:** Cloud Marketing Plus Cloudlet (Beta)
- **Behavior version:** The `v2025-05-30` 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
<code>enabled</code>	boolean	Enables the Cloud Marketing Plus Cloudlet.	
<code>javascriptInsertionRule</code>	enum	Select how to insert the MediaMath JavaScript reference script.	
	<code>NEVER</code>	Specify this if inserting the script at the origin.	
	<code>POLICY</code>	Allow the Cloudlet policy to determine when to insert it.	
	<code>ALWAYS</code>	Insert it for all edge requests.	
<code>cloudletPolicy</code>	object	Identifies the Cloudlet policy.	<code>javascriptInsertionRule</code> is <code>POLICY</code>
<code>cloudletPolicy.id</code>	number	Identifies the Cloudlet.	
<code>cloudletPolicy.name</code>	string	The Cloudlet's descriptive name.	

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

forwardRewrite

- **Property Manager name:** [Forward Rewrite Cloudlet](#)
- **Behavior version:** The `v2025-05-30` 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
<code>enabled</code>	boolean	Enables the Forward Rewrite Cloudlet behavior.	
<code>isSharedPolicy</code>	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 .	
<code>cloudletPolicy</code>	object	Identifies the Cloudlet policy.	<code>isSharedPolicy</code> is <code>false</code>
<code>cloudletPolicy.id</code>	number	Identifies the Cloudlet.	
<code>cloudletPolicy.name</code>	string	The Cloudlet's descriptive name.	
<code>cloudletSharedPolicy</code>	number	This identifies the Cloudlet shared policy to use with this behavior. You can list available shared policies with the Cloudlets API .	<code>isSharedPolicy</code> is <code>true</code>

g2oheader

- **Property Manager name:** [Signature Header Authentication](#)
- **Behavior version:** The `v2025-05-30` 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
<code>enabled</code>	boolean	Enables the g2o verification behavior.	
<code>dataHeader</code>	string	Specifies the name of the header that contains the request data that needs to be encrypted.	
<code>signedHeader</code>	string	Specifies the name of the header containing encrypted request data.	
<code>encodingVersion</code>	enum	Specifies the version of the encryption algorithm as an integer from <code>1</code> through <code>5</code> .	
		Supported values: <code>1 3 5</code> <code>2 4</code>	
<code>useCustomSignString</code>	boolean	When disabled, the encrypted string is based on the forwarded URL. If enabled, you can use <code>customSignString</code> to customize the set of data to encrypt.	
<code>customSignString</code>	string array	Specifies the set of data to be encrypted as a combination of concatenated strings.	<code>useCustomSignString</code> is <code>true</code>
	<code>AK_METHOD</code>	Incoming request method.	
	<code>AK_SCHEME</code>	Incoming request scheme (HTTP or HTTPS).	
	<code>AK_HOSTHEADER</code>	Incoming request hostname.	
	<code>AK_DOMAIN</code>	Incoming request domain.	
	<code>AK_URL</code>	Incoming request URL.	
	<code>AK_PATH</code>	Incoming request path.	
	<code>AK_QUERY</code>	Incoming request query string.	
	<code>AK_FILENAME</code>	Incoming request filename.	
	<code>AK_EXTENSION</code>	Incoming request filename extension.	

Option	Type	Description	Requires
	AK_CLIENT_ REAL_IP	Incoming client IP.	
secretKey	object array	Specifies the shared secret key.	
nonce	string	Specifies the cryptographic <i>nonce</i> string.	

globalRequestNumber

- **Property Manager name:** [Global Request Number](#)
- **Behavior version:** The `v2025-05-30` 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 <code>outputOption</code> set to specify any set of headers, this specifies the name of the header to report the GRN value.	<code>outputOption</code> is either: <code>RESPONSE_HEADER</code> , <code>REQUEST_HEADER</code> , <code>BOTH_HEADERS</code>
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.	<code>outputOption</code> is <code>ASSIGN_VARIABLE</code>

graphqlCaching

- **Property Manager name:** [GraphQL Caching](#)
- **Behavior version:** The `v2025-05-30` 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
<code>enabled</code>	boolean	Enables GraphQL caching.
<code>cacheResponsesWithErrors</code>	boolean	When enabled, caches responses that include an <code>error</code> 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.
<code>postRequestProcessingErrorHandling</code>	enum	Specify what happens if GraphQL query processing fails on POST requests.
	<code>APPLY_CACHING_BEHAVIOR</code>	If your GraphQL server does not allow mutations and subscriptions, this offloads requests.
	<code>NO_STORE</code>	Pass requests to the origin.
<code>operationsUrlQueryParameterName</code>	string	Specifies the name of a query parameter that identifies requests as GraphQL queries.
<code>operationsJsonBodyParameterName</code>	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 `v2025-05-30` 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
<code>behavior</code>	enum	Specify when to compress responses.
	<code>ORIGIN_RESPONSE</code>	Compress for clients that send an <code>Accept-Encoding: gzip</code> header.
	<code>ALWAYS</code>	Always compress.
	<code>NEVER</code>	Never compress.

hdDataAdvanced

- **Property Manager name:** [HD Data Override: Advanced Metadata](#)
- **Behavior version:** The `v2025-05-30` 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
<code>description</code>	string	Human-readable description of what the XML block does.
<code>xml</code>	string	A block of Akamai XML metadata.

healthDetection

- **Property Manager name:** [Origin Health Detection](#)
- **Behavior version:** The `v2025-05-30` 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
<code>retryCount</code>	number	The number of consecutive connection failures that mark an IP address as faulty.
<code>retryInterval</code>	string (duration)	Specifies the amount of time the edge server will wait before trying to reconnect to an IP address it has already identified as faulty.
<code>maximumReconnects</code>	number	Specifies the maximum number of times the edge server will contact your origin server. If your origin is associated with several IP addresses, <code>maximumReconnects</code> effectively overrides the value of <code>retryCount</code> .

hsafEipBinding

- **Property Manager name:** [HSAF for Edge IP Binding](#)
- **Behavior version:** The `v2025-05-30` 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
<code>enabled</code>	boolean	Enables HSAF for Edge IP Binding customers with a large footprint.	
<code>customExtractedSerial</code>	boolean	Whether to pull the serial number from the variable value set in the <code>advanced</code> behavior. Work with your Akamai Services team to add the <code>advanced</code> behavior earlier in your property to extract and apply the <code>AKA_PM_EIP_HSAF_SERIAL</code> variable.	
<code>hashMinValue</code>	number	Specifies the minimum value for the HSAF hash range, from 2 through 2045. This needs to be lower than <code>hashMaxValue</code> .	<code>customExtractedSerial</code> is <code>false</code>
<code>hashMaxValue</code>	number	Specifies the maximum value for the hash range, from 3 through 2046. This needs to be higher than <code>hashMinValue</code> .	<code>customExtractedSerial</code> is <code>false</code>
<code>tier</code>	enum	Specifies where the behavior is applied.	
	<code>EDGE</code>	Applies Hash Serial and Forward only at edge regions.	
	<code>PARENT</code>	Applies Hash Serial and Forward using tiers. For more details, see the Edge IP Binding documentation .	
	<code>BOTH</code>	Applies Hash Serial and Forward in both environments.	

http2

- **Property Manager name:** [HTTP/2](#)
- **Behavior version:** The `v2025-05-30` 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 `v2025-05-30` 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
<code>enable</code>	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 `v2025-05-30` 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
<code>enable</code>	boolean	Applies HSTS to this set of requests.	
<code>maxAge</code>	enum	Specifies the duration for which to apply HSTS for new browser connections.	
	<code>ZERO_MINS</code>	This effectively disables HSTS, without affecting any existing browser connections.	
	<code>TEN_MINS</code>	10 minutes.	
	<code>ONE_DAY</code>	1 day.	
	<code>ONE_MONTH</code>	1 month.	
	<code>THREE_MONTHS</code>	3 months.	
	<code>SIX_MONTHS</code>	6 months.	
	<code>ONE_YEAR</code>	1 year.	
	<code>TWO_YEARS</code>	2 years. It's a recommended setting.	
<code>includeSubDomains</code>	boolean	When enabled, applies HSTS to all subdomains.	<code>maxAge</code> is not <code>ZERO_MINS</code>
<code>preload</code>	boolean	When enabled, adds this domain to the browser's preload list. You still need to declare the domain at https://hstspreload.org .	<code>maxAge</code> is not <code>ZERO_MINS</code>
<code>redirect</code>	boolean	When enabled, redirects all HTTP requests to HTTPS.	<code>maxAge</code> is not <code>ZERO_MINS</code>
<code>redirectStatus Code</code>	enum	Specifies a response code.	<code>maxAge</code> is not <code>ZERO_MINS</code> AND <code>redirect</code> is <code>true</code>
		Supported values: <div>301</div> <div>302</div>	

httpToHttpsUpgrade

- **Property Manager name:** [HTTP to HTTPS Upgrade](#)
- **Behavior version:** The `v2025-05-30` 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.

imOverride

- **Property Manager name:** [Image and Video Manager: Set Parameter](#)
- **Behavior version:** The `v2025-05-30` 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
<code>override</code>	enum	Selects the type of query parameter you want to set.	
	<code>POLICY</code>	For the name of the Image and Video Manager policy you want to apply.	
	<code>POLICY_VARIABLE</code>	Specify that you want to set an Image and Video Manager policy variable from a rule tree variable defined in the property.	
	<code>WIDTH</code>	A predefined width to constrain the image to.	
	<code>FORMAT</code>	For browser types.	
	<code>DPR</code>	For pixel density.	
	<code>EXCLUDE_QUERY</code>	Excludes the specified query parameters from the cache key.	
<code>typesel</code>	enum	Specifies how to set a query parameter.	<code>override</code> is not <code>POLICY_VARIABLE</code> AND <code>override</code> is not <code>EXCLUDE_QUERY</code>
	<code>VALUE</code>	Assign a specific value.	
	<code>VARIABLE</code>	Assign a Property Manager rule tree <code>VARIABLE</code> .	
<code>formatvar</code>	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 <code>format</code> option below.	<code>override</code> is <code>FORMAT</code> AND <code>typesel</code> is <code>VARIABLE</code>

Option	Type	Description	Requires
<code>format</code>	enum	Specifies the type of the browser, or the encodings passed in the <code>Accept</code> header, that you want to optimize images for.	<code>override is FORMAT</code> <code>AND typeset is VALUE</code>
	<code>CHROME</code>	Google Chrome.	
	<code>IE</code>	Internet Explorer.	
	<code>SAFARI</code>	Apple Safari.	
	<code>GENERIC</code>	Generic.	
	<code>AVIF_WEBP_JPEG_PNG_GIF</code>	Best of AVIF, WebP, JPEG, PNG, and GIF.	
	<code>JP2_WEBP_JPEG_PNG_GIF</code>	Best of JP2, WebP, JPEG, PNG, and GIF.	
	<code>WEBP_JPEG_PNG_GIF</code>	Best of WebP, JPEG, PNG, and GIF.	
	<code>JPEG_PNG_GIF</code>	Best of JPEG, PNG, GIF.	
<code>dprvar</code>	string (variable name)	This selects the variable with the desired pixel density. The variable specifies the same type of data as the <code>dpr</code> option below.	<code>override is DPR</code> <code>AND typeset is VARIABLE</code>
<code>dpr</code>	number	Directly specifies the pixel density. The numeric value is a scaling factor of 1, representing normal density.	<code>override is DPR</code> <code>AND typeset is VALUE</code>
<code>widthvar</code>	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.	<code>override is WIDTH</code> <code>AND typeset is VARIABLE</code>
<code>width</code>	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.	<code>override is WIDTH</code> <code>AND typeset is VALUE</code>
<code>policyvar</code>	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.	<code>override is POLICY</code> <code>AND typeset is VARIABLE</code>
<code>policy</code>	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.	<code>override is POLICY</code> <code>AND typeset is VALUE</code>
<code>policyvarName</code>	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.	<code>override is POLICY_VARIABLE</code>
<code>policyvarIMvar</code>	string (variable name)	This selects one of the property's rule tree variables to assign to the <code>policyvarName</code> variable within Image and Video Manager.	<code>override is POLICY_VARIABLE</code>
<code>excludeAllQueryParameters</code>	boolean	Whether to exclude all query parameters from the Image and Video Manager cache key.	<code>override is EXCLUDE_QUERY</code>
<code>excludedQueryParameters</code>	string array	Specifies individual query parameters to exclude from the Image and Video Manager cache key.	<code>override is EXCLUDE_QUERY</code> <code>AND excludeAllQueryParameters is false</code>

imageManager

- **Property Manager name:** [Image and Video Manager \(Images\)](#)
- **Behavior version:** The `v2025-05-30` rule format supports the `imageManager` behavior v2.1.
- **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 [advanced ImMatch](#) to ensure the behavior applies to the requests from the Image and Video Manager backend.

This behavior is incompatible with the [clientIp](#) criteria.

Option	Type	Description	Requires
<code>enabled</code>	boolean	Enable image management capabilities and generate a corresponding API token.	
<code>resize</code>	boolean	Specify whether to scale down images to the maximum screen resolution, as determined by the rendering device's user agent. Note that enabling this may affect screen layout in unexpected ways.	
<code>applyBestFileType</code>	boolean	Specify whether to convert images to the best file type for the requesting device, based on its user agent and the initial image file. This produces the smallest file size possible that retains image quality.	
<code>superCacheRegion</code>	enum	Specifies a location for your site's heaviest traffic, for use in caching derivatives on edge servers.	<code>useExisting PolicySet</code> is not <code>true</code>
	<code>US</code>	United States.	
	<code>ASIA</code>	Asia.	
	<code>AUSTRALIA</code>	Australia.	
	<code>EMEA</code>	Europe, Middle East, and Africa.	
	<code>JAPAN</code>	Japan.	
	<code>CHINA</code>	China.	
<code>cloudWrapperEnabled</code>	boolean	Enables Cache+ to improve cache retention and performance. When enabled, Image and Video Manager stores derivatives in Cloud Wrapper.	
<code>cloudWrapperRollout Start</code>	boolean	Allows Cloud Wrapper to fetch from that cache for 30 days when a cache miss occurs before sending the request to the origin. Note that if using Image and Video Manager, the objects may already be in cache.	<code>cloudWrapper Enabled</code> is <code>true</code>
<code>cloudWrapperUrlPath</code>	string array	With <code>cloudWrapperEnabled</code> set to <code>true</code> , specifies paths for which Image and Video Manager will store derivatives in Cloud Wrapper. You can use wildcards for each specified path, where <code>?</code> matches a single character and <code>*</code> matches zero or more characters. Leaving this field empty means	<code>cloudWrapper Enabled</code> is <code>true</code>

Option	Type	Description	Requires
		all Image and Video Manager derivative traffic will be stored in Cloud Wrapper.	
<code>cpCodeOriginal</code>	object	Assigns a CP code to track traffic and billing for original images that the Image and Video Manager has not modified. You only need to provide the initial <code>id</code> , stripping any <code>cpc_</code> prefix to pass the integer to the rule tree. Additional CP code details may reflect back in subsequent read-only data.	
<code>cpCodeOriginal.cpCodeLimits</code>	array	Read-only. Describes the current usage limit for the CP code.	
<code>cpCodeOriginal.createdDate</code>	integer	Read-only. UNIX epoch timestamp reflecting when the CP code was originally created.	
<code>cpCodeOriginal.description</code>	string	Read-only. Additional description for the CP code.	
<code>cpCodeOriginal.id</code>	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 <code>cpcodeId</code> value from the List CP codes operation.	
<code>cpCodeOriginal.name</code>	string	Read-only. The name of the CP code you specify as the <code>cpcodeName</code> 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.	
<code>cpCodeOriginal.products</code>	array	Read-only. The set of products the CP code is assigned to. This reflects <code>productId</code> values you specify when creating a new CP code in PAPI.	
<code>cpCodeTransformed</code>	object	Assigns a separate CP code to track traffic and billing for derived images. You only need to provide the initial <code>id</code> , stripping any <code>cpc_</code> prefix to pass the integer to the rule tree. Additional CP code details may reflect back in subsequent read-only data.	
<code>cpCodeTransformed.cpCodeLimits</code>	array	Read-only. Describes the current usage limit for the CP code.	
<code>cpCodeTransformed.createdDate</code>	integer	Read-only. UNIX epoch timestamp reflecting when the CP code was originally created.	
<code>cpCodeTransformed.description</code>	string	Read-only. Additional description for the CP code.	
<code>cpCodeTransformed.id</code>	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 <code>cpcodeId</code> value from the List CP codes operation.	
<code>cpCodeTransformed.name</code>	string	Read-only. The name of the CP code you specify as the <code>cpcodeName</code> 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.	
<code>cpCodeTransformed.products</code>	array	Read-only. The set of products the CP code is assigned to. This reflects <code>productId</code> values you specify when creating a new CP code in PAPI.	
<code>useExistingPolicySet</code>	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.	
<code>policySet</code>	object	Identifies the existing policy set configured with Image and Video Manager API .	<code>useExistingPolicySet</code> is <code>true</code>
<code>advanced</code>	boolean	Generates a custom Image and Video Manager API token to apply a corresponding policy to this set of images. The token consists of a descriptive label (the <code>policyToken</code>) concatenated with a property-specific identifier that's generated when you save the property. The API registers the token when you activate the property.	<code>useExistingPolicySet</code> is <code>false</code>

Option	Type	Description	Requires
<code>policyToken</code>	string	Assign a prefix label to help match the policy token to this set of images, limited to 32 alphanumeric or underscore characters. If you don't specify a label, <i>default</i> becomes the prefix.	advanced is true
<code>policyTokenDefault</code>	string	Specify the default policy identifier, which is registered with the Image and Video Manager API once you activate this property. The advanced option needs to be inactive.	advanced is false

imageManagerVideo

- **Property Manager name:** [Image and Video Manager \(Videos\)](#)
- **Behavior version:** The `v2025-05-30` 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
<code>enabled</code>	boolean	Applies Image and Video Manager's video optimization to the current content.	
<code>resize</code>	boolean	When enabled, scales down video for smaller mobile screens, based on the device's <code>User-Agent</code> header.	
<code>applyBestFileType</code>	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.	
<code>superCacheRegion</code>	enum	To optimize caching, assign a region close to your site's heaviest traffic.	<code>useExistingPolicySet</code> is not true
	US	United States.	
	ASIA	Asia.	
	AUSTRALIA	Australia.	
	EMEA	Europe, Middle East, and Africa.	
	JAPAN	Japan.	
	CHINA	China.	

Option	Type	Description	Requires
<code>cpCodeOriginal</code>	object	Specifies the CP code for which to track Image and Video Manager video traffic. Use this along with <code>cpCodeTransformed</code> to track traffic to derivative video content. You only need to provide the initial <code>id</code> , stripping any <code>cpc_</code> prefix to pass the integer to the rule tree. Additional CP code details may reflect back in subsequent read-only data.	
<code>cpCodeOriginal.cpCodeLimits</code>	array	Read-only. Describes the current usage limit for the CP code.	
<code>cpCodeOriginal.createdDate</code>	integer	Read-only. UNIX epoch timestamp reflecting when the CP code was originally created.	
<code>cpCodeOriginal.description</code>	string	Read-only. Additional description for the CP code.	
<code>cpCodeOriginal.id</code>	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 <code>cpcodeId</code> value from the List CP codes operation.	
<code>cpCodeOriginal.name</code>	string	Read-only. The name of the CP code you specify as the <code>cpcodeName</code> 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.	
<code>cpCodeOriginal.products</code>	array	Read-only. The set of products the CP code is assigned to. This reflects <code>productId</code> values you specify when creating a new CP code in PAPI.	
<code>cpCodeTransformed</code>	object	Specifies the CP code to identify derivative transformed video content. You only need to provide the initial <code>id</code> , stripping any <code>cpc_</code> prefix to pass the integer to the rule tree. Additional CP code details may reflect back in subsequent read-only data.	
<code>cpCodeTransformed.cpCodeLimits</code>	array	Read-only. Describes the current usage limit for the CP code.	
<code>cpCodeTransformed.createdDate</code>	integer	Read-only. UNIX epoch timestamp reflecting when the CP code was originally created.	
<code>cpCodeTransformed.description</code>	string	Read-only. Additional description for the CP code.	
<code>cpCodeTransformed.id</code>	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 <code>cpcodeId</code> value from the List CP codes operation.	
<code>cpCodeTransformed.name</code>	string	Read-only. The name of the CP code you specify as the <code>cpcodeName</code> 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.	
<code>cpCodeTransformed.products</code>	array	Read-only. The set of products the CP code is assigned to. This reflects <code>productId</code> values you specify when creating a new CP code in PAPI.	
<code>useExistingPolicySet</code>	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.	
<code>policySet</code>	object	Identifies the existing policy set configured with Image and Video Manager API .	<code>useExistingPolicySet</code> is <code>true</code>
<code>advanced</code>	boolean	When disabled, applies a single standard policy based on your property name. Allows you to reference a rule-specific <code>policyToken</code> for videos with different match criteria.	<code>useExistingPolicySet</code> is <code>false</code>
<code>policyToken</code>	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	<code>advanced</code> is <code>true</code>

Option	Type	Description	Requires
		include up to 64 alphanumeric, dash, or underscore characters.	
<code>policyTokenDefault</code>	string	Specifies the default policy identifier, which is registered with the Image and Video Manager API once you activate this property.	<code>advanced</code> is <code>false</code>

include

- **Property Manager name:** [Include](#)
- **Behavior version:** The `v2025-05-30` 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
<code>id</code>	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 <code>inc_</code> ID prefix.

instant

- **Property Manager name:** [Akamai Instant \(Prefetching\)](#)
- **Behavior version:** The `v2025-05-30` 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>`, ``, `<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
<code>prefetch</code> <code>Cacheable</code>	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 tiered Distribution behavior enabled.	
<code>prefetchNoStore</code>	boolean	Allows otherwise non-cacheable <code>no-store</code> content to prefetch if the URL path ends with <code>/</code> to indicate a request for a default file, or if the extension matches the value of the <code>prefetchNoStoreExtensions</code> option. Only applies to content with the sure Route behavior enabled.	
<code>prefetchNoStoreExtensions</code>	string array	Specifies a set of file extensions for which the <code>prefetchNoStore</code> option is allowed.	<code>prefetchNoStore</code> is <code>true</code>
<code>prefetchHtml</code>	boolean	Allows edge servers to prefetch additional HTML pages while pages that link to them are being delivered. This only applies to links from <code><a></code> or <code><link></code> tags with the appropriate link relation attribute.	<code>prefetchCacheable</code> is <code>true</code> OR <code>prefetchNoStore</code> is <code>true</code>
<code>customLinkRelations</code>	string array	Specify link relation values that activate the prefetching behavior. For example, specifying <code>fetch</code> allows you to use shorter <code>rel="fetch"</code> markup.	<code>prefetchHtml</code> is <code>true</code>

instantConfig

- **Property Manager name:** [InstantConfig](#)
- **Behavior version:** The `v2025-05-30` 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
<code>enabled</code>	boolean	Enables the InstantConfig behavior.

largeFileOptimization

- **Property Manager name:** [Large File Optimization](#)
- **Behavior version:** The `v2025-05-30` 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
<code>enabled</code>	boolean	Enables the file optimization behavior.	
<code>enablePartialObjectCaching</code>	enum	Specifies whether to cache partial objects.	
	<code>PARTIAL_OBJECT_CACHING</code>	Allows <i>partial-object caching</i> , 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.	
	<code>NON_PARTIAL_OBJECT_CACHING</code>	Caches entire objects. The size of the object to be cached can't be greater than 1800 MB.	
<code>minimumSize</code>	string	Optimization only applies to files larger than this, expressed as a number suffixed with a unit string such as <code>MB</code> or <code>GB</code> .	<code>enablePartialObjectCaching</code> is <code>PARTIAL_OBJECT_CACHING</code>
<code>maximumSize</code>	string	Optimization does not apply to files larger than this, expressed as a number suffixed with a unit string such as <code>MB</code> or <code>GB</code> . 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.	<code>enablePartialObjectCaching</code> is <code>PARTIAL_OBJECT_CACHING</code>

Option	Type	Description	Requires
<code>useVersioning</code>	boolean	When <code>enablePartialObjectCaching</code> is set to <code>PARTIAL_OBJECT_CACHING</code> , 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.	<code>enablePartialObjectCaching</code> is <code>PARTIAL_OBJECT_CACHING</code>

largeFileOptimizationAdvanced

- **Property Manager name:** [Large File Optimization \(Advanced\)](#)
- **Behavior version:** The `v2025-05-30` 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
<code>enabled</code>	boolean	Enables the file optimization behavior.
<code>objectSize</code>	string	Specifies the size of the file at which point to apply partial object (POC) caching. Append a numeric value with a <code>MB</code> or <code>GB</code> suffix.
<code>fragmentSize</code>	enum	Specifies the size of each fragment used for partial object caching.
		Supported values: <div> <div>FOUR_MB</div> <div>ONE_MB</div> <div>HALF_MB</div> <div>TWO_MB</div> </div>
<code>prefetchDuringRequest</code>	number	The number of POC fragments to prefetch during the request.
<code>prefetchAfterRequest</code>	number	The number of POC fragments to prefetch after the request.

limitBitRate

- **Property Manager name:** [Bit Rate Limiting](#)
- **Behavior version:** The `v2025-05-30` 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
<code>enabled</code>	boolean	When enabled, activates the bit rate limiting behavior.
<code>bitrateTable</code>	object array	Specifies a download rate that corresponds to a <code>thresholdTable</code> entry. The bit rate appears as a two-member object consisting of a numeric <code>bitrateValue</code> and a <code>bitrateUnit</code> string, with allowed values of <code>Kbps</code> , <code>Mbps</code> , and <code>Gbps</code> .
<code>bitrateTable[].bitrateValue</code>	number	The numeric indicator of the download rate.
<code>bitrateTable[].bitrateUnit</code>	enum	The unit of measurement, either <code>KBPS</code> , <code>MBPS</code> , or <code>GBPS</code> .
		Supported values: <code>GBPS</code> <code>MBPS</code> <code>KBPS</code>
<code>thresholdTable</code>	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 <code>bitrateTable</code> entry. The threshold appears as a two-member object consisting of a numeric <code>thresholdValue</code> and <code>thresholdUnit</code> string, with allowed values of <code>SECONDS</code> or <code>BYTES</code> .
<code>thresholdTable[].thresholdValue</code>	number	The numeric indicator of the minimum file size or elapsed download time.
<code>thresholdTable[].thresholdUnit</code>	enum	The unit of measurement, either <code>SECONDS</code> of the elapsed download time, or <code>BYTES</code> of the file size.
		Supported values: <code>BYTES</code> <code>SECONDS</code>

logCustom

- **Property Manager name:** [Log_Custom_Details](#)
- **Behavior version:** The `v2025-05-30` 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
<code>logCustomLogField</code>	boolean	Whether to append additional custom data to each log line.	
<code>customLogField</code>	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, <code>round-trip: {{builtin.AK_CLIENT_TURNAROUND_TIME}}ms</code> 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 <code>customLogField</code> settings in the report behavior.	<code>logCustomLogField</code> is <code>true</code>

mPulse

- **Property Manager name:** [mPulse](#)
- **Behavior version:** The `v2025-05-30` 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
<code>enabled</code>	boolean	Applies performance monitoring to this behavior's set of content.
<code>requirePci</code>	boolean	Suppresses gathering metrics for potentially sensitive end-user interactions. Enabling this omits data from some older browsers.
<code>loaderVersion</code>	enum	Specifies the version of the Boomerang JavaScript loader snippet. See mPulse Loader Snippets for more information.
	<code>V10</code>	Use version 10.
	<code>V12</code>	Use version 12.
	<code>LATEST</code>	Automatically update to the latest available production version.
	<code>BETA</code>	Use the latest version, including beta releases.
<code>apiKey</code>	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 .
<code>bufferSize</code>	string	Allows you to override the browser's default (150) maximum number of reported performance timeline entries.
<code>configOverride</code>	string	A JSON string representing a configuration object passed to the JavaScript library under which mPulse runs. It corresponds at run-time to the <code>window.BOOMR_config</code> object. For example, this turns on monitoring of Single Page App frameworks: <code>"{\\"history\\": {\\"enabled\\": true, \\"auto\\": true}}"</code> . See Configuration Overrides for more information.

manifestPersonalization

- **Property Manager name:** [Manifest Personalization](#)
- **Behavior version:** The `v2025-05-30` 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
<code>enabled</code>	boolean	Enables the Manifest Personalization feature.	
<code>hlsEnabled</code>	boolean	Allows you to customize the HLS master manifest that's sent to the requesting client.	
<code>hlsMode</code>	enum	Applies with <code>hlsEnabled</code> on.	<code>hlsEnabled</code> is <code>true</code>

Option	Type	Description	Requires
	BEST_PRACTICE	Specify the default best practice mode.	
	CUSTOM	Specify a custom manifest.	
hlsPreferredBitrate	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
hlsFilterInBitrates	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
hlsFilterInBitrateRanges	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
hlsQueryParamEnabled	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
hlsQueryParamSecretKey	object array	Specifies a primary key as a token to accompany the request.	hlsQueryParamEnabled is true
hlsQueryParamTransitionKey	object array	Specifies a transition key as a token to accompany the request.	hlsQueryParamEnabled is true
hlsShowAdvanced	boolean	Allows you to configure advanced settings.	hlsEnabled is true
hlsEnableDebugHeaders	boolean	Includes additional Akamai-Manifest-Personalization and Akamai-Manifest-Personalization-Config-Source debugging headers.	hlsShowAdvanced is true

manifestRerouting

- **Property Manager name:** [Manifest Rerouting](#)
- **Behavior version:** The v2025-05-30 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
<code>partner</code>	enum	Set this value to <code>adobe_primetime</code> , which is an external technology partner that provides value added offerings, like advertisement integration, to the requested media objects.
	<code>adobe_primetime</code>	This is currently the only supported value.
<code>username</code>	string	The user name for your Adobe Primetime account.

manualServerPush

- **Property Manager name:** [Manual Server Push](#)
- **Behavior version:** The `v2025-05-30` 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
<code>serverpushlist</code>	string array	Specifies the set of objects to load into the client browser's cache over HTTP2. Each value in the array represents a hostname and full path to the object, such as <code>www.example.com/js/site.js</code> .

mediaAcceleration

- **Property Manager name:** [Media Acceleration](#)
- **Behavior version:** The `v2025-05-30` 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
<code>enabled</code>	boolean	Enables Media Acceleration.

mediaAccelerationQuicOptout

- **Property Manager name:** [Media Acceleration \(QUIC Protocol\) Opt-Out](#)
 - **Behavior version:** The `v2025-05-30` rule format supports the `mediaAccelerationQuicOptout` behavior v1.0.
 - **Rule format status:** [Deprecated, outdated rule format](#)
 - **Access:** [Read/Write](#)
 - **Allowed in includes:** [No \(temporarily\).](#)
-

This behavior is deprecated.

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 `v2025-05-30` 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
<code>enabled</code>	boolean	Enables client-side download analytics.
<code>beaconId</code>	string	Specifies the ID of data source's beacon.
<code>useHybridHttpUdp</code>	boolean	Enables the hybrid HTTP/UDP protocol.

mediaFileRetrievalOptimization

- **Property Manager name:** [Media File Retrieval Optimization](#)
- **Behavior version:** The `v2025-05-30` 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
<code>enabled</code>	boolean	Enables the partial-object caching behavior.

mediaOriginFailover

- **Property Manager name:** [Media Origin Failover](#)
- **Behavior version:** The `v2025-05-30` rule format supports the `mediaOriginFailover` behavior v1.1.
- **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
<code>detectOriginUnresponsive</code>	boolean	Allows you to configure what happens when the origin is unresponsive.	
<code>originUnresponsiveDetectionLevel</code>	enum	Specify the level of response to slow origin connections.	<code>detectOriginUnresponsive is true</code>
	<code>AGGRESSIVE</code>	Aggressive response.	
	<code>CONSERVATIVE</code>	Conservative response.	
	<code>MODERATE</code>	Moderate response.	
<code>originUnresponsiveBlocklistOriginIp</code>	boolean	Enabling this blocklists the origin's IP address.	<code>detectOriginUnresponsive is true</code>
<code>originUnresponsiveBlocklistWindow</code>	enum	This sets the delay before blocklisting an IP address.	<code>originUnresponsiveBlocklistOriginIp is true</code>
	<code>TEN_S</code>	10 seconds.	
	<code>THIRTY_S</code>	30 seconds.	
<code>originUnresponsiveRecovery</code>	enum	This sets the recovery option.	<code>detectOriginUnresponsive is true</code>
	<code>RETRY_X_TIMES</code>	Retry.	
	<code>SWITCH_TO_BACKUP_ORIGIN</code>	Switch to a backup origin.	
	<code>REDIRECT_TO_DIFFERENT_ORIGIN_LOCATION</code>	Redirect to a different origin.	
<code>originUnresponsiveRetryLimit</code>	enum	Sets how many times to retry.	<code>originUnresponsiveRecovery is RETRY_X_TIMES</code>
		Supported values: <code>ONE</code> <code>TWO</code> <code>THREE</code>	
<code>originUnresponsiveBackupHost</code>	string	This specifies the origin hostname.	<code>originUnresponsiveRecovery is SWITCH_TO_BACKUP_ORIGIN</code>
<code>originUnresponsiveAlternateHost</code>	string	This specifies the redirect's destination hostname.	<code>originUnresponsiveRecovery is REDIRECT_TO_DIFFERENT_ORIGIN_LOCATION</code>
<code>originUnresponsiveModifyRequestPath</code>	boolean	Modifies the request path.	<code>originUnresponsiveRecovery is SWITCH_TO_BACKUP_ORIGIN</code> OR <code>originUnresponsiveRecovery is REDIRECT_TO_DIFFERENT_ORIGIN_LOCATION</code>
<code>originUnresponsiveModifiedPath</code>	string	This specifies the path to form the new URL.	<code>originUnresponsiveModifyRequestPath is true</code>
<code>originUnresponsiveIncludeQueryString</code>	boolean	Enabling this includes the original set of query parameters.	<code>originUnresponsiveModifyRequestPath is true</code>
<code>originUnresponsiveRedirectMethod</code>	enum	Specifies the redirect response code.	<code>originUnresponsiveRecovery is REDIRECT_TO_DIFFERENT_ORIGIN_</code>

Option	Type	Description	Requires
			LOCATION
		Supported values: 301 302	
originUnresponsiveChangeProtocol	boolean	This allows you to change the request protocol.	originUnresponsiveRecovery is SWITCH_TO_BACKUP_ORIGIN OR originUnresponsiveRecovery is REDIRECT_TO_DIFFERENT_ORIGIN_LOCATION
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
originUnavailableBlocklistOriginIp	boolean	Enabling this blocklists the origin's IP address.	detectOriginUnavailable is true
originUnavailableBlocklistWindow	enum	This sets the delay before blocklisting an IP address.	originUnavailableBlocklistOriginIp 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 TWO 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

Option	Type	Description	Requires
			OR <code>originUnavailableRecovery</code> is <code>REDIRECT_TO_DIFFERENT_ORIGIN_LOCATION</code>
<code>originUnavailableModifiedPath</code>	string	This specifies the path to form the new URL.	<code>originUnavailableModifyRequestPath</code> is <code>true</code>
<code>originUnavailableIncludeQueryString</code>	boolean	Enabling this includes the original set of query parameters.	<code>originUnavailableModifyRequestPath</code> is <code>true</code>
<code>originUnavailableRedirectMethod</code>	enum	Specifies either a redirect response code.	<code>originUnavailableRecovery</code> is <code>REDIRECT_TO_DIFFERENT_ORIGIN_LOCATION</code>
		Supported values: 301 302	
<code>originUnavailableChangeProtocol</code>	boolean	Modifies the request protocol.	<code>originUnavailableRecovery</code> is <code>SWITCH_TO_BACKUP_ORIGIN</code> OR <code>originUnavailableRecovery</code> is <code>REDIRECT_TO_DIFFERENT_ORIGIN_LOCATION</code>
<code>originUnavailableProtocol</code>	enum	Specifies either the <code>HTTP</code> or <code>HTTPS</code> protocol.	<code>originUnavailableChangeProtocol</code> is <code>true</code>
		Supported values: <code>HTTP</code> <code>HTTPS</code>	
<code>detectObjectUnavailable</code>	boolean	Allows you to configure failover settings when the origin has content errors.	
<code>objectUnavailableDetectionLevel</code>	enum	Specify <code>RESPONSE_CODES</code> , the only available option.	<code>detectObjectUnavailable</code> is <code>true</code>
	<code>RESPONSE_CODES</code>	This is the only value currently available.	
<code>objectUnavailableResponseCodes</code>	string array	Specifies the set of response codes identifying when there are content errors.	<code>detectObjectUnavailable</code> is <code>true</code>
<code>objectUnavailableBlocklistOriginIp</code>	boolean	Enabling this blocklists the origin's IP address.	<code>detectObjectUnavailable</code> is <code>true</code>
<code>objectUnavailableBlocklistWindow</code>	enum	This sets the delay before blocklisting an IP address.	<code>objectUnavailableBlocklistOriginIp</code> is <code>true</code>
	<code>TEN_S</code>	10 seconds.	
	<code>THIRTY_S</code>	30 seconds.	
<code>objectUnavailableRecovery</code>	enum	This sets the recovery option.	<code>detectObjectUnavailable</code> is <code>true</code>
	<code>RETRY_X_TIMES</code>	Retry.	
	<code>SWITCH_TO_BACKUP_ORIGIN</code>	Switch to a backup origin.	
	<code>REDIRECT_TO_DIFFERENT_ORIGIN_LOCATION</code>	Redirect to a different origin.	
<code>objectUnavailableRetryLimit</code>	enum	Sets how many times to retry.	<code>objectUnavailableRecovery</code> is <code>RETRY_X_TIMES</code>
		Supported values:	

Option	Type	Description	Requires
		ONE TWO THREE	
<code>objectUnavailableBackupHost</code>	string	This specifies the origin hostname.	<code>objectUnavailableRecovery</code> is <code>SWITCH_TO_BACKUP_ORIGIN</code>
<code>objectUnavailableAlternateHost</code>	string	This specifies the redirect's destination hostname.	<code>objectUnavailableRecovery</code> is <code>REDIRECT_TO_DIFFERENT_ORIGIN_LOCATION</code>
<code>objectUnavailableModifyRequestPath</code>	boolean	Enabling this allows you to modify the request path.	<code>objectUnavailableRecovery</code> is <code>SWITCH_TO_BACKUP_ORIGIN</code> OR <code>objectUnavailableRecovery</code> is <code>REDIRECT_TO_DIFFERENT_ORIGIN_LOCATION</code>
<code>objectUnavailableModifiedPath</code>	string	This specifies the path to form the new URL.	<code>objectUnavailableModifyRequestPath</code> is <code>true</code>
<code>objectUnavailableIncludeQueryString</code>	boolean	Enabling this includes the original set of query parameters.	<code>objectUnavailableModifyRequestPath</code> is <code>true</code>
<code>objectUnavailableRedirectMethod</code>	enum	Specifies a redirect response code.	<code>objectUnavailableRecovery</code> is <code>REDIRECT_TO_DIFFERENT_ORIGIN_LOCATION</code>
		Supported values: 301 302	
<code>objectUnavailableChangeProtocol</code>	boolean	Changes the request protocol.	<code>objectUnavailableRecovery</code> is <code>SWITCH_TO_BACKUP_ORIGIN</code> OR <code>objectUnavailableRecovery</code> is <code>REDIRECT_TO_DIFFERENT_ORIGIN_LOCATION</code>
<code>objectUnavailableProtocol</code>	enum	Specifies either the <code>HTTP</code> or <code>HTTPS</code> protocol.	<code>objectUnavailableChangeProtocol</code> is <code>true</code>
		Supported values: <code>HTTP</code> <code>HTTPS</code>	
<code>clientResponseCode</code>	string	Specifies the response code served to the client.	
<code>cacheErrorResponse</code>	boolean	When enabled, caches the error response.	
<code>cacheWindow</code>	enum	This sets error response's TTL.	<code>cacheErrorResponse</code> is <code>true</code>
	<code>ONE_S</code>	1 second.	
	<code>TEN_S</code>	10 seconds.	
	<code>THIRTY_S</code>	30 seconds.	

metadataCaching

- **Property Manager name:** [Metadata Caching](#)
- **Behavior version:** The `v2025-05-30` 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
<code>enabled</code>	boolean	Enables metadata caching.

mobileSdkPerformance

- **Property Manager name:** [Mobile App Performance SDK](#)
- **Behavior version:** The `v2025-05-30` 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
<code>enabled</code>	boolean	Enables the Mobile App Performance SDK.
<code>secondaryMultipathToOrigin</code>	boolean	When enabled, sends secondary multi-path requests to the origin server.

modifyIncomingRequestHeader

- **Property Manager name:** [Modify Incoming Request Header](#)
- **Behavior version:** The `v2025-05-30` 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
<code>action</code>	enum	Either <code>ADD</code> , <code>DELETE</code> , <code>MODIFY</code> , or <code>PASS</code> incoming HTTP request headers.	
	<code>ADD</code>	Add the header.	
	<code>DELETE</code>	Delete the header.	
	<code>MODIFY</code>	Modify the header.	
	<code>PASS</code>	Pass through the header.	
<code>standardAddHeaderName</code>	enum	If the value of <code>action</code> is <code>ADD</code> , this specifies the name of the field to add.	<code>action</code> is <code>ADD</code>
	<code>ACCEPT_ENCODING</code>	Add an <code>Accept-Encoding</code> header.	
	<code>ACCEPT_LANGUAGE</code>	Add an <code>Accept-Language</code> header.	
	<code>OTHER</code>	Specify another header to add.	
<code>standardDeleteHeaderName</code>	enum	If the value of <code>action</code> is <code>DELETE</code> , this specifies the name of the field to remove.	<code>action</code> is <code>DELETE</code>
	<code>IF_MODIFIED_SINCE</code>	The <code>If-Modified-Since</code> header.	
	<code>VIA</code>	The <code>Via</code> header.	
	<code>OTHER</code>	Specify another header to remove.	
<code>standardModifyHeaderName</code>	enum	If the value of <code>action</code> is <code>MODIFY</code> , this specifies the name of the field to modify.	<code>action</code> is <code>MODIFY</code>
	<code>ACCEPT_ENCODING</code>	Add an <code>Accept-Encoding</code> header.	
	<code>ACCEPT_LANGUAGE</code>	Add an <code>Accept-Language</code> header.	
	<code>OTHER</code>	Specify another header to add.	

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

modifyIncomingResponseHeader

- **Property Manager name:** [Modify Incoming Response Header](#)
- **Behavior version:** The `v2025-05-30` 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
<code>action</code>	enum	Either <code>ADD</code> , <code>DELETE</code> , <code>MODIFY</code> , or <code>PASS</code> incoming HTTP response headers.	
	<code>ADD</code>	Add the header.	
	<code>DELETE</code>	Delete the header.	
	<code>MODIFY</code>	Modify the header.	
	<code>PASS</code>	Pass through the header.	
<code>standardAddHeaderName</code>	enum	If the value of <code>action</code> is <code>ADD</code> , this specifies the name of the field to add.	<code>action</code> is <code>ADD</code>
	<code>CACHE_CONTROL</code>	The <code>Cache-Control</code> header.	
	<code>CONTENT_TYPE</code>	The <code>Content-Type</code> header.	
	<code>EDGE_CONTROL</code>	The <code>Edge-Control</code> header.	
	<code>EXPIRES</code>	The <code>Expires</code> header.	
	<code>LAST_MODIFIED</code>	The <code>Last-Modified</code> header.	
	<code>OTHER</code>	Specify another header to add.	
<code>standardDeleteHeaderName</code>	enum	If the value of <code>action</code> is <code>DELETE</code> , this specifies the name of the field to remove.	<code>action</code> is <code>DELETE</code>
	<code>CACHE_CONTROL</code>	The <code>Cache-Control</code> header.	
	<code>CONTENT_TYPE</code>	The <code>Content-Type</code> header.	
	<code>VARY</code>	The <code>Vary</code> header.	
	<code>OTHER</code>	Specify another header to remove.	
<code>standardModifyHeaderName</code>	enum	If the value of <code>action</code> is <code>MODIFY</code> , this specifies the name of the field to modify.	<code>action</code> is <code>MODIFY</code>
	<code>CACHE_CONTROL</code>	The <code>Cache-Control</code> header.	
	<code>CONTENT_TYPE</code>	The <code>Content-Type</code> header.	
	<code>EDGE_CONTROL</code>	The <code>Edge-Control</code> header.	
	<code>OTHER</code>	Specify another header to modify.	
<code>standardPassHeaderName</code>	enum	If the value of <code>action</code> is <code>PASS</code> , this specifies the name of the field to pass through.	<code>action</code> is <code>PASS</code>
	<code>CACHE_CONTROL</code>	Pass through the <code>Cache-Control</code> header.	
	<code>EXPIRES</code>	Pass through the <code>Expires</code> header.	
	<code>PRAGMA</code>	Pass through the <code>Pragma</code> header.	
	<code>OTHER</code>	Specify another header to pass.	
<code>customHeaderName</code>	string (allows variables)	Specifies a custom field name that applies when the relevant <i>standard</i> header name is set to <code>OTHER</code> .	<code>standardAddHeaderName</code> is <code>OTHER</code> OR <code>standardDeleteHeaderName</code> is <code>OTHER</code> OR <code>standardModifyHeaderName</code> is <code>OTHER</code> OR <code>standardPassHeaderName</code> is <code>OTHER</code>

Option	Type	Description	Requires
<code>headerValue</code>	string (allows variables)	Specifies the header's new value.	<code>action</code> is <code>ADD</code>
<code>newHeaderValue</code>	string (allows variables)	Specifies an HTTP header replacement value.	<code>action</code> is <code>MODIFY</code>
<code>avoidDuplicate Headers</code>	boolean	When enabled with the <code>action</code> set to <code>MODIFY</code> , prevents creation of more than one instance of a header.	<code>action</code> is <code>MODIFY</code>

modifyOutgoingRequestHeader

- **Property Manager name:** [Modify Outgoing Request Header](#)
- **Behavior version:** The `v2025-05-30` 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
<code>action</code>	enum	Either <code>ADD</code> or <code>DELETE</code> outgoing HTTP request headers, <code>MODIFY</code> their fixed values, or specify a <code>REGEX</code> pattern to transform them.	
	<code>ADD</code>	Add the header.	
	<code>DELETE</code>	Delete the header.	
	<code>MODIFY</code>	Modify the header.	
	<code>REGEX</code>	Specify another header to modify.	
<code>standardAdd HeaderName</code>	enum	If the value of <code>action</code> is <code>ADD</code> , this specifies the name of the field to add.	<code>action</code> is <code>ADD</code>
	<code>USER_AGENT</code>	The <code>User-Agent</code> header.	
	<code>OTHER</code>	Specify another header to add.	

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

modifyOutgoingResponseHeader

- **Property Manager name:** [Modify Outgoing Response Header](#)
- **Behavior version:** The `v2025-05-30` 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
<code>action</code>	enum	Either <code>ADD</code> or <code>DELETE</code> outgoing HTTP response headers, <code>MODIFY</code> their fixed values, or specify a <code>REGEX</code> pattern to transform them.	
	<code>ADD</code>	Add the header.	
	<code>DELETE</code>	Delete the header.	
	<code>MODIFY</code>	Modify the header.	
	<code>REGEX</code>	Specify another header to modify.	
<code>standardAddHeaderName</code>	enum	If the value of <code>action</code> is <code>ADD</code> , this specifies the name of the field to add.	<code>action</code> is <code>ADD</code>
	<code>CACHE_CONTROL</code>	The <code>Cache-Control</code> header.	
	<code>CONTENT_DISPOSITION</code>	The <code>Content-Disposition</code> header.	
	<code>CONTENT_TYPE</code>	The <code>Content-Type</code> header.	
	<code>EDGE_CONTROL</code>	The <code>Edge-Control</code> header.	
	<code>P3P</code>	Specify another header to add.	
	<code>PRAGMA</code>	The <code>Pragma</code> header.	
	<code>ACCESS_CONTROL_ALLOW_ORIGIN</code>	The <code>Access-Control-Allow-Origin</code> header.	
	<code>ACCESS_CONTROL_ALLOW_METHODS</code>	The <code>Access-Control-Allow-Methods</code> header.	
	<code>ACCESS_CONTROL_ALLOW_HEADERS</code>	The <code>Access-Control-Allow-Headers</code> header.	
	<code>ACCESS_CONTROL_EXPOSE_HEADERS</code>	The <code>Access-Control-Expose-Headers</code> header.	
	<code>ACCESS_CONTROL_ALLOW_CREDENTIALS</code>	The <code>Access-Control-Allow-Credentials</code> header.	
	<code>ACCESS_CONTROL_MAX_AGE</code>	The <code>Access-Control-Max-Age</code> header.	
	<code>OTHER</code>	Specify another header to add.	
<code>standardDeleteHeaderName</code>	enum	If the value of <code>action</code> is <code>DELETE</code> , this specifies the name of the field to remove.	<code>action</code> is <code>DELETE</code>
	<code>CACHE_CONTROL</code>	The <code>Cache-Control</code> header.	

Option		Type	Description	Requires
		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 ModifyHeader Name	enum		If the value of <code>action</code> is <code>MODIFY</code> or <code>REGEX</code> , this specifies the name of the field to modify.	<code>action</code> is <code>MODIFY</code> OR <code>action</code> is <code>REGEX</code>
		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.	
customHeader Name	string (allows variables)		Specifies a custom field name that applies when the relevant <i>standard</i> header name is set to <code>OTHER</code> .	<code>standardAddHeader Name</code> is <code>OTHER</code>

Option	Type	Description	Requires
			OR standard DeleteHeaderName is OTHER OR standard ModifyHeaderName is OTHER
headerValue	string (allows variables)	Specifies the existing value of the header to match.	action is ADD
newHeader Value	string (allows variables)	Specifies the new HTTP header replacement value.	action is MODIFY
regexHeader Match	string	Specifies a Perl-compatible regular expression to match within the header value.	action is REGEX
regexHeader Replace	string (allows variables)	Specifies text that replaces the <code>regexHeaderMatch</code> pattern within the header value.	action is REGEX
match Multiple	boolean	When enabled with the <code>action</code> set to <code>REGEX</code> , replaces all occurrences of the matched regular expression, otherwise only the first match if disabled.	action is REGEX
avoid Duplicate Headers	boolean	When enabled with the <code>action</code> set to <code>MODIFY</code> , prevents creation of more than one instance of a header. The last header clobbers others with the same name. This option affects the entire set of outgoing headers, and is not confined to the subset of regular expression matches.	action is MODIFY

modifyViaHeader

- **Property Manager name:** [Modify Via Header](#)
- **Behavior version:** The `v2025-05-30` 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 <code>Via</code> 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 <code>via</code> header.	<code>modificationOption</code> is <code>RENAME_ HEADER</code>

mtlsOriginKeystore

- **Property Manager name:** [mTLS Edge Server to Origin](#)
- **Behavior version:** The `v2025-05-30` rule format supports the `mtlsOriginKeystore` behavior v1.0.
- **Rule format status:** [Deprecated, outdated rule format](#)
- **Access:** [Read/Write](#)
- **Allowed in includes:** [Yes](#)

Establish a Mutual TLS (mTLS) connection between the edge server and the origin to authenticate requests. This ensures that the requests to your origin server come directly from the Akamai network. In the mTLS protocol, the origin asks the edge server to present its identity certificate. For this negotiation to work, either the origin needs to be configured for mTLS sessions, or the edge server is allowed to proceed without the edge certificate, effectively performing a standard (non-mutual) TLS connection to the origin.

Option	Type	Description
<code>enable</code>	boolean	Allows a specific mutual transport layer (mTLS) client certificate in a request from the edge server to the origin.
<code>client Certificate VersionGuid</code>	string	Specifies the client certificate to authenticate your origin with the edge server. You need to create client certificates using the Mutual TLS Origin Keystore API or application.
<code>authClient Cert</code>	boolean	When enabled, the edge server requires a prompt from the origin for the client certificate's identity. If the edge server gets the request, it proceeds with the mTLS session and connects to the origin. If the edge server doesn't get the request, the connection to the origin stops and a client error is reported. When disabled, the edge server proceeds without a request for the client certificate, making a standard TLS connection to the origin. Disabled by default.

origin

- **Property Manager name:** [Origin Server](#)
- **Behavior version:** The `v2025-05-30` rule format supports the `origin` behavior v1.25.
- **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
<code>originType</code>	enum	Choose where your content is retrieved from.	
	<code>CUSTOMER</code>	From your own server.	
	<code>NET_STORAGE</code>	From your NetStorage account. This option is most appropriate for static content.	
	<code>MEDIA_SERVICE_LIVE</code>	From a Media Services Live origin.	
	<code>EDGE_LOAD_BALANCING_ORIGIN_GROUP</code>	From any available Edge Load Balancing origin.	
	<code>SAAS_DYNAMIC_ORIGIN</code>	From a SaaS dynamic origin if SaaS acceleration is available on your contract.	
<code>netStorage</code>	object	Specifies the details of the NetStorage server.	<code>originType</code> is <code>NET_STORAGE</code>
<code>netStorage.cpCode</code>	integer	Identifies a CP code assigned to this storage group.	
<code>netStorage.downloadDomainName</code>	string	Domain name from which content can be downloaded.	
<code>netStorage.g2oToken</code>	string	Signature Header Authentication key.	
<code>netStorage.id</code>	integer	Unique identifier for the storage group.	
<code>netStorage.name</code>	string	Name of the storage group.	
<code>originId</code>	string	Identifies the Edge Load Balancing origin. This needs to correspond to an edgeLoadBalancingOrigin behavior's <code>id</code> attribute within the same property.	<code>originType</code> is <code>EDGE_LOAD_BALANCING_ORIGIN_GROUP</code>
<code>hostname</code>	string (allows variables)	Specifies the hostname or IPv4 address of your origin server, from which edge servers can retrieve your content.	<code>originType</code> is <code>CUSTOMER</code>

Option	Type	Description	Requires
<code>secondHostnameEnabled</code>	boolean	Available only for certain products. This specifies whether you want to use an additional origin server address.	
<code>secondHostname</code>	string (allows variables)	Specifies the origin server's hostname, IPv4 address, or IPv6 address. Edge servers retrieve your content from this origin server.	<code>secondHostnameEnabled</code> is <code>true</code>
<code>mslorigin</code>	string	This specifies the media's origin server.	<code>originType</code> is <code>MEDIA_SERVICE_LIVE</code>
<code>saasType</code>	enum	Specifies the part of the request that identifies this SaaS dynamic origin.	<code>originType</code> is <code>SAAS_DYNAMIC_ORIGIN</code>
		Supported values: COOKIE HOSTNAME PATH QUERY_STRING	
<code>saasCnameEnabled</code>	boolean	Enabling this allows you to use a <i>CNAME chain</i> to determine the hostname for this SaaS dynamic origin.	<code>saasType</code> is <code>HOSTNAME</code>
<code>saasCnameLevel</code>	number	Specifies the desired number of hostnames to use in the <i>CNAME chain</i> , starting backwards from the edge server.	<code>saasCnameEnabled</code> is <code>true</code>
<code>saasCookie</code>	string	Specifies the name of the cookie that identifies this SaaS dynamic origin.	<code>saasType</code> is <code>COOKIE</code>
<code>saasQueryString</code>	string	Specifies the name of the query parameter that identifies this SaaS dynamic origin.	<code>saasType</code> is <code>QUERY_STRING</code>
<code>saasRegex</code>	string	Specifies the Perl-compatible regular expression match that identifies this SaaS dynamic origin.	<code>originType</code> is <code>SAAS_DYNAMIC_ORIGIN</code>
<code>saasReplace</code>	string	Specifies replacement text for what <code>saasRegex</code> matches.	<code>originType</code> is <code>SAAS_DYNAMIC_ORIGIN</code>
<code>saasSuffix</code>	string	Specifies the static part of the SaaS dynamic origin.	<code>originType</code> is <code>SAAS_DYNAMIC_ORIGIN</code>
<code>forwardHostHeader</code>	enum	When the <code>originType</code> is set to either <code>CUSTOMER</code> or <code>SAAS_DYNAMIC_ORIGIN</code> , this specifies which <code>Host</code> header to pass to the origin.	<code>originType</code> is either: <code>CUSTOMER</code> , <code>SAAS_DYNAMIC_ORIGIN</code>
	<code>REQUEST_HOST_HEADER</code>	Passes the original request's header.	
	<code>ORIGIN_HOSTNAME</code>	Passes the current origin's <code>HOSTNAME</code> .	
	<code>CUSTOM</code>	Passes the value of <code>customForwardHostHeader</code> . Use this option if you want requests handled by different properties to converge on the same cached object.	
<code>customForwardHostHeader</code>	string (allows variables)	This specifies the name of the custom host header the edge server should pass to the origin.	<code>forwardHostHeader</code> is <code>CUSTOM</code>
<code>cacheKeyHostname</code>	enum	Specifies the hostname to use when forming a cache key.	<code>originType</code> is either: <code>CUSTOMER</code> , <code>SAAS_DYNAMIC_ORIGIN</code>
	<code>REQUEST_HOST_HEADER</code>	Specify when using a virtual server.	
	<code>ORIGIN_HOSTNAME</code>	Specify if your origin server's responses do not depend on the hostname.	
<code>ipVersion</code>	enum	Specifies which IP version to use when getting content from the origin.	<code>originType</code> is either: <code>CUSTOMER</code> , <code>EDGE_LOAD</code>

Option	Type	Description	Requires
		When using IPv6-Only or Dual Stack and the Origin IP Access Control List feature, add the <code>originIpAcl</code> behavior to the same rule or a parent rule.	BALANCING_ORIGIN_GROUP
	IPV4	Use IPV4.	
	DUALSTACK	Use both versions.	
	IPV6	Use IPV6.	
<code>useUniqueCacheKey</code>	boolean	With a shared <code>hostname</code> such as provided by Amazon AWS, sets a unique cache key for your content.	
<code>compress</code>	boolean	Enables <i>gzip</i> compression for non-NetStorage origins.	<code>originType</code> is either: CUSTOMER , EDGE_LOAD_ BALANCING_ORIGIN_GROUP , SAAS_DYNAMIC_ORIGIN
<code>enableTrueClientIp</code>	boolean	When enabled on non-NetStorage origins, allows you to send a custom header (the <code>trueClientIpHeader</code>) identifying the IP address of the immediate client connecting to the edge server. This may provide more useful information than the standard <code>X-Forward-For</code> header, which proxies may modify.	<code>originType</code> is either: CUSTOMER , EDGE_LOAD_ BALANCING_ORIGIN_GROUP , SAAS_DYNAMIC_ORIGIN
<code>trueClientIpHeader</code>	string	This specifies the name of the field that identifies the end client's IP address, for example <code>True-Client-IP</code> .	<code>enableTrueClientIp</code> is <code>true</code>
<code>trueClientIpClientSetting</code>	boolean	If a client sets the <code>True-Client-IP</code> header, the edge server allows it and passes the value to the origin. Otherwise the edge server removes it and sets the value itself.	<code>enableTrueClientIp</code> is <code>true</code>
<code>verificationMode</code>	enum	For non-NetStorage origins, maximize security by controlling which certificates edge servers should trust.	<code>originType</code> 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 <i>Secure Delivery - Customer Cert</i> 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.	
<code>originSni</code>	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. If you want to use TLS version 1.3 in your existing properties, enable this option. New properties have this enabled by default.	<code>originType</code> is either: CUSTOMER , EDGE_LOAD_ BALANCING_ORIGIN_GROUP , SAAS_DYNAMIC_ORIGIN AND <code>verificationMode</code> is either: PLATFORM_SETTINGS , CUSTOM , THIRD_PARTY
<code>customValidCnValues</code>	string array	Specifies values to look for in the origin certificate's <code>Subject Alternate Name</code> or <code>Common Name</code> fields. Specify <code>{{Origin Hostname}}</code> and <code>{{Forward Host Header}}</code> 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.)	<code>verificationMode</code> is <code>CUSTOM</code>
<code>originCertsToHonor</code>	enum	Specifies which certificate to trust.	<code>verificationMode</code> is <code>CUSTOM</code>

Option	Type	Description	Requires
	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.	
customCertificate Authorities	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
custom Certificates	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
minTlsVersion	enum	Specifies the minimum TLS version to use for connections to your origin server.	originType is either: CUSTOMER , MEDIA_ SERVICE_LIVE
	DYNAMIC	Supports all currently public versions of TLS.	
	TLSV1_1	Supports TLS version 1.1.	
	TLSV1_2	Supports TLS version 1.2.	
	TLSV1_3	Supports TLS version 1.3. This behavior supports TLS 1.3 by default.	
maxTlsVersion	enum	Specifies the maximum TLS version to use for connections to your origin server. As best practice, use DYNAMIC to automatically apply the latest supported version.	originType is either: CUSTOMER , MEDIA_ SERVICE_LIVE
	DYNAMIC	Automatically applies the latest supported version.	
	TLSV1_1	Supports TLS version 1.1.	
	TLSV1_2	Supports TLS version 1.2.	
	TLSV1_3	Supports TLS version 1.3. This behavior supports TLS 1.3 by default.	
http2Enabled	boolean	Limited Availability. When enabled, the edge server sends multiple HTTP requests over a single HTTP/2 connection to the origin.	originType is either: CUSTOMER

originCharacteristics

- **Property Manager name:** [Origin Characteristics](#)
- **Behavior version:** The `v2025-05-30` rule format supports the `originCharacteristics` behavior v1.9.
- **Rule format status:** [Deprecated, outdated rule format](#)
- **Access:** [Read/Write](#)
- **Allowed in includes:** [Yes](#)

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
<code>authenticationMethod</code>	enum	Specifies the authentication method.	
	<code>AUTOMATIC</code>	Use default authentication.	
	<code>SIGNATURE_HEADER_AUTHENTICATION</code>	Available with the Adaptive Media Delivery, Object Delivery, Download Delivery, API Acceleration, Dynamic Site Acceleration, and Ion products.	
	<code>MSL_AUTHENTICATION</code>	Available with the Adaptive Media Delivery product.	
	<code>AWS</code>	Amazon Web Services. If you're using this authentication method, any chaseRedirects behavior you specify gets automatically disabled.	
	<code>GCS_HMAC_AUTHENTICATION</code>	Google Cloud Platform. If you're using this authentication method, any chaseRedirects behavior you specify gets automatically disabled.	
<code>encodingVersion</code>	enum	Specifies the version of the encryption algorithm, an integer from <code>1</code> to <code>5</code> .	<code>authenticationMethod</code> is <code>SIGNATURE_HEADER_AUTHENTICATION</code>
<code>useCustomSignString</code>	boolean	Specifies whether to customize your signed string.	<code>authenticationMethod</code> is <code>SIGNATURE_HEADER_AUTHENTICATION</code>
<code>customSignString</code>	string array	Specifies the data to be encrypted as a series of enumerated variable names. See Built-in system variables for guidance on each.	<code>authenticationMethod</code> is <code>SIGNATURE_HEADER_AUTHENTICATION</code> AND <code>useCustomSignString</code> is <code>true</code>
		Supported values: <code>AK_CLIENT_REAL_IP</code> <code>AK_DOMAIN</code> <code>AK_EXTENSION</code> <code>AK_FILENAME</code>	

Option	Type	Description	Requires
		AK_HOSTHEADER AK_METHOD AK_PATH AK_QUERY AK_SCHEME AK_URL	
secretKey	object array	Specifies the shared secret key.	authenticationMethod is SIGNATURE_HEADER_AUTHENTICATION
nonce	string	Specifies the nonce.	authenticationMethod is SIGNATURE_HEADER_AUTHENTICATION
mslkey	string	Specifies the access key provided by the hosting service.	authenticationMethod is MSL_AUTHENTICATION
mslname	string	Specifies the origin name provided by the hosting service.	authenticationMethod is MSL_AUTHENTICATION
accessKey EncryptedStorage	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.	authenticationMethod 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.	authenticationMethod is GCS_HMAC_AUTHENTICATION AND accessKeyEncryptedStorage is true
gcsHmacKeyAccess Id	string	Specifies the active access ID linked to your Google account.	authenticationMethod is GCS_HMAC_AUTHENTICATION AND accessKeyEncryptedStorage 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.	authenticationMethod is GCS_HMAC_AUTHENTICATION AND accessKeyEncryptedStorage is not true
awsAccessKey VersionGuid	string	Identifies the unique awsAccessKeyVersionGuid access key created in Cloud Access Manager to sign your requests to AWS S3.	authenticationMethod is AWS AND accessKeyEncryptedStorage is true
awsAccessKeyId	string	Specifies active access key ID linked to your AWS account.	authenticationMethod is AWS AND accessKeyEncryptedStorage is not true
awsSecretAccess Key	string	Specifies the secret linked to the access key identifier that you want to use to sign requests to AWS.	authenticationMethod is AWS AND accessKeyEncryptedStorage is not true
awsRegion	string	This specifies the AWS region code of the location where your bucket resides.	authenticationMethod is AWS

Option	Type	Description	Requires
<code>awsHost</code>	string	This specifies the AWS hostname, without <code>http://</code> or <code>https://</code> prefixes. If you leave this option empty, it inherits the hostname from the <code>origin</code> behavior.	<code>authenticationMethod</code> is <code>AWS</code>
<code>awsService</code>	string	This specifies the subdomain of your AWS service. It precedes <code>amazonaws.com</code> or the region code in the AWS hostname. For example, <code>s3.amazonaws.com</code> .	<code>authenticationMethod</code> is <code>AWS</code>
<code>sortQueryParams</code>	boolean	Sorts the query string parameters alphabetically by key name.	<code>authenticationMethod</code> is either: <code>AWS</code> , <code>GCS_HMAC_AUTHENTICATION</code>
<code>encodeQueryParams</code>	boolean	Encodes the query string parameters.	<code>authenticationMethod</code> is either: <code>AWS</code> , <code>GCS_HMAC_AUTHENTICATION</code>
<code>encodeEquals</code>	boolean	Encodes any equal (=) characters in a query parameter's value.	<code>encodeQueryParams</code> is <code>true</code>
<code>country</code>	enum	Specifies the origin's geographic region.	
	<code>EUROPE</code>	Europe.	
	<code>NORTH_AMERICA</code>	North America.	
	<code>LATIN_AMERICA</code>	Latin America.	
	<code>SOUTH_AMERICA</code>	South America.	
	<code>NORDICS</code>	Northern Europe.	
	<code>ASIA_PACIFIC</code>	Asia and Pacific Islands.	
	<code>OTHER_AMERICAS</code>	Other Americas.	
	<code>OTHER_APJ</code>	Asia, Pacific, Japan.	
	<code>OTHER_EMEA</code>	Europe, Middle East, Africa.	
	<code>AUSTRALIA</code>	Australia.	
	<code>GERMANY</code>	Germany.	
	<code>INDIA</code>	India.	
	<code>ITALY</code>	Italy.	
	<code>JAPAN</code>	Japan.	
	<code>MEXICO</code>	Mexico.	
	<code>TAIWAN</code>	Taiwan.	
	<code>UNITED_KINGDOM</code>	United Kingdom.	
	<code>US_EAST</code>	Eastern United States.	
	<code>US_CENTRAL</code>	Central United States.	
	<code>US_WEST</code>	Western United States.	
	<code>GLOBAL_MULTI_GEO</code>	Global.	
	<code>OTHER</code>	A fallback value.	
	<code>UNKNOWN</code>	Defer this optimization.	
	<code>ADC</code>	Akamai Direct Connection, available to Adaptive Media Delivery customers.	

Option	Type	Description	Requires
<code>directConnect</code> <code>Geo</code>	string	Provides a region used by Akamai Direct Connection.	<code>country</code> is <code>ADC</code>

originCharacteristicsWsd

- **Property Manager name:** [Origin Characteristics](#)
- **Behavior version:** The `v2025-05-30` 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
<code>origintype</code>	enum	Specifies an origin type.
	<code>AZURE</code>	An Azure origin type.
	<code>UNKNOWN</code>	An unknown origin type.

originFailureRecoveryMethod

- **Property Manager name:** [Origin Failure Recovery Method](#)
- **Behavior version:** The `v2025-05-30` 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
<code>recoveryMethod</code>	enum	Specifies the recovery method.	
	<code>RETRY_ALTERNATE_ORIGIN</code>	Retry with the alternate origin.	
	<code>RESPOND_CUSTOM_STATUS</code>	Customize the response.	
<code>customStatusCode</code>	string	Specifies the custom status code to be sent to the client.	<code>recoveryMethod</code> is <code>RESPOND_CUSTOM_STATUS</code>

originFailureRecoveryPolicy

- **Property Manager name:** [Origin Failure Recovery Policy](#)
- **Behavior version:** The `v2025-05-30` 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
<code>enabled</code>	boolean	Activates and configures a recovery policy.	
<code>enableIPAvoidance</code>	boolean	Temporarily blocks an origin IP address that experienced a certain number of failures. When an IP address is blocked, the <code>configName</code> established for <code>originResponsivenessRecoveryConfigName</code> is applied.	
<code>ipAvoidanceErrorThreshold</code>	number	Defines the number of failures that need to occur to an origin address before it's blocked.	<code>enableIPAvoidance</code> is <code>true</code>
<code>ipAvoidanceRetryInterval</code>	number	Defines the number of seconds after which the IP address is removed from the blocklist.	<code>enableIPAvoidance</code> is <code>true</code>

Option	Type	Description	Requires
<code>binaryEquivalentContent</code>	boolean	Synchronizes content between the primary and backup origins, byte for byte.	
<code>monitorOriginResponsiveness</code>	boolean	Enables continuous monitoring of connectivity to the origin. If necessary, applies retry or recovery actions.	
<code>originResponsivenessTimeout</code>	enum	The timeout threshold that triggers a retry or recovery action.	<code>monitorOriginResponsiveness</code> is <code>true</code>
	AGGRESSIVE	A 2 second threshold.	
	MODERATE	3 seconds.	
	CONSERVATIVE	4 seconds.	
	USER_SPECIFIED	Specify your own timeout.	
<code>originResponsivenessCustomTimeout</code>	number	Specify a custom timeout, from 1 to 10 seconds.	<code>originResponsivenessTimeout</code> is <code>USER_SPECIFIED</code>
<code>originResponsivenessEnableRetry</code>	boolean	If a specific failure condition applies, attempts a retry on the same origin before executing the recovery method.	<code>monitorOriginResponsiveness</code> is <code>true</code>
<code>originResponsivenessEnableRecovery</code>	boolean	Enables a recovery action for a specific failure condition.	<code>monitorOriginResponsiveness</code> is <code>true</code>
<code>originResponsivenessRecoveryConfigName</code>	string	Specifies a recovery configuration using the <code>configName</code> you defined in the recoveryConfig match criteria. Specify 3 to 20 alphanumeric characters or dashes. Ensure that you use the recoveryConfig match criteria to apply this option.	<code>originResponsivenessEnableRecovery</code> is <code>true</code>
<code>monitorStatusCodes1</code>	boolean	Enables continuous monitoring for the specific origin status codes that trigger retry or recovery actions.	
<code>monitorResponseCodes1</code>	string array	Defines the origin response codes that trigger a subsequent retry or recovery action. Specify a single code entry (<code>501</code>) or a range (<code>501:504</code>). If you configure other <code>monitorStatusCodes*</code> and <code>monitorResponseCodes*</code> options, you can't use the same codes here.	<code>monitorStatusCodes1</code> is <code>true</code>
<code>monitorStatusCodes1EnableRetry</code>	boolean	When the defined response codes apply, attempts a retry on the same origin before executing the recovery method.	<code>monitorStatusCodes1</code> is <code>true</code>
<code>monitorStatusCodes1EnableRecovery</code>	boolean	Enables the recovery action for the response codes you define.	<code>monitorStatusCodes1</code> is <code>true</code>
<code>monitorStatusCodes1RecoveryConfigName</code>	string	Specifies a recovery configuration using the <code>configName</code> you defined in the recoveryConfig match criteria. Specify 3 to 20 alphanumeric characters or dashes. Ensure that you use the recoveryConfig match criteria to apply this option.	<code>monitorStatusCodes1EnableRecovery</code> is <code>true</code>
<code>monitorStatusCodes2</code>	boolean	Enables continuous monitoring for the specific origin status codes that trigger retry or recovery actions.	
<code>monitorResponseCodes2</code>	string array	Defines the origin response codes that trigger a subsequent retry or recovery action. Specify a single code entry (<code>501</code>) or a range (<code>501:504</code>). If you configure other <code>monitorStatusCodes*</code> and <code>monitorResponseCodes*</code> options, you can't use the same codes here.	<code>monitorStatusCodes2</code> is <code>true</code>

Option	Type	Description	Requires
<code>monitorStatusCodes2EnableRetry</code>	boolean	When the defined response codes apply, attempts a retry on the same origin before executing the recovery method.	<code>monitorStatusCodes2</code> is <code>true</code>
<code>monitorStatusCodes2EnableRecovery</code>	boolean	Enables the recovery action for the response codes you define.	<code>monitorStatusCodes2</code> is <code>true</code>
<code>monitorStatusCodes2RecoveryConfigName</code>	string	Specifies a recovery configuration using the <code>configName</code> you defined in the recoveryConfig match criteria. Specify 3 to 20 alphanumeric characters or dashes. Ensure that you use the recoveryConfig match criteria to apply this option.	<code>monitorStatusCodes2EnableRecovery</code> is <code>true</code>
<code>monitorStatusCodes3</code>	boolean	Enables continuous monitoring for the specific origin status codes that trigger retry or recovery actions.	
<code>monitorResponseCodes3</code>	string array	Defines the origin response codes that trigger a subsequent retry or recovery action. Specify a single code entry (<code>501</code>) or a range (<code>501:504</code>). If you configure other <code>monitorStatusCodes*</code> and <code>monitorResponseCodes*</code> options, you can't use the same codes here..	<code>monitorStatusCodes3</code> is <code>true</code>
<code>monitorStatusCodes3EnableRetry</code>	boolean	When the defined response codes apply, attempts a retry on the same origin before executing the recovery method.	<code>monitorStatusCodes3</code> is <code>true</code>
<code>monitorStatusCodes3EnableRecovery</code>	boolean	Enables the recovery action for the response codes you define.	<code>monitorStatusCodes3</code> is <code>true</code>
<code>monitorStatusCodes3RecoveryConfigName</code>	string	Specifies a recovery configuration using the <code>configName</code> you defined in the recoveryConfig match criteria. Specify 3 to 20 alphanumeric characters or dashes. Ensure that you use the recoveryConfig match criteria to apply this option.	<code>monitorStatusCodes3EnableRecovery</code> is <code>true</code>

originIpAcl

- **Property Manager name:** [Origin IP Access Control List](#)
- **Behavior version:** The `v2025-05-30` 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
<code>enable</code>	boolean	Enables the Origin IP Access Control List behavior.

permissionsPolicy

- **Property Manager name:** [Permissions-Policy](#)
- **Behavior version:** The `v2025-05-30` rule format supports the `permissionsPolicy` behavior v1.0.
- **Rule format status:** [Deprecated, outdated rule format](#)
- **Access:** [Read/Write](#)
- **Allowed in includes:** [Yes](#)

Manages whether your page and its embedded iframes can access various browser features that affect end-user privacy, security, and performance.

Use this together with [requestClientHints](#) .

Option	Type	Description																								
<code>permissionsPolicyDirective</code>	string array	<p>Each directive represents a browser feature. Specify the ones you want enabled in a client browser that accesses your content. You can add custom entries or provide pre-set values from the list. For more details on each value, see the guide section for this behavior.</p> <table><tr><td><code>battery</code></td><td><code>ch-ua-full-version-list</code></td><td><code>ch-width</code></td><td><code>geolocation</code></td></tr><tr><td><code>camera</code></td><td><code>ch-ua-mobile</code></td><td><code>device-memory</code></td><td><code>microphone</code></td></tr><tr><td><code>ch-ua</code></td><td><code>ch-ua-model</code></td><td><code>display-capture</code></td><td><code>rtt</code></td></tr><tr><td><code>ch-ua-arch</code></td><td><code>ch-ua-platform</code></td><td><code>downlink</code></td><td></td></tr><tr><td><code>ch-ua-bitness</code></td><td><code>ch-ua-platform-version</code></td><td><code>ect</code></td><td></td></tr><tr><td><code>ch-dpr</code></td><td><code>ch-viewport-width</code></td><td><code>fullscreen</code></td><td></td></tr></table>	<code>battery</code>	<code>ch-ua-full-version-list</code>	<code>ch-width</code>	<code>geolocation</code>	<code>camera</code>	<code>ch-ua-mobile</code>	<code>device-memory</code>	<code>microphone</code>	<code>ch-ua</code>	<code>ch-ua-model</code>	<code>display-capture</code>	<code>rtt</code>	<code>ch-ua-arch</code>	<code>ch-ua-platform</code>	<code>downlink</code>		<code>ch-ua-bitness</code>	<code>ch-ua-platform-version</code>	<code>ect</code>		<code>ch-dpr</code>	<code>ch-viewport-width</code>	<code>fullscreen</code>	
<code>battery</code>	<code>ch-ua-full-version-list</code>	<code>ch-width</code>	<code>geolocation</code>																							
<code>camera</code>	<code>ch-ua-mobile</code>	<code>device-memory</code>	<code>microphone</code>																							
<code>ch-ua</code>	<code>ch-ua-model</code>	<code>display-capture</code>	<code>rtt</code>																							
<code>ch-ua-arch</code>	<code>ch-ua-platform</code>	<code>downlink</code>																								
<code>ch-ua-bitness</code>	<code>ch-ua-platform-version</code>	<code>ect</code>																								
<code>ch-dpr</code>	<code>ch-viewport-width</code>	<code>fullscreen</code>																								
<code>allowList</code>	string	<p>The features you've set in <code>permissionsPolicyDirective</code> are enabled for domains you specify here. They'll remain disabled for all other domains. Separate multiple domains with a single space. To block the specified directives from all domains, set this to <code>none</code> . This generates an empty value in the <code>Permissions-Policy</code> header.</p>																								

persistentClientConnection

- **Property Manager name:** [Persistent Connections: Client to Edge](#)
- **Behavior version:** The `v2025-05-30` 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
<code>enabled</code>	boolean	Enables the persistent connections behavior.
<code>timeout</code>	string (duration)	Specifies the timeout period after which edge server closes the persistent connection with the client, 500 seconds by default.

persistentConnection

- **Property Manager name:** [Persistent Connections: Edge to Origin](#)
- **Behavior version:** The `v2025-05-30` 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
<code>enabled</code>	boolean	Enables persistent connections.
<code>timeout</code>	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 `v2025-05-30` 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
<code>enabled</code>	boolean	When enabled, marks content as personally identifiable information (PII).

phasedRelease

- **Property Manager name:** [Phased Release Cloudlet](#)
- **Behavior version:** The `v2025-05-30` 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
<code>enabled</code>	boolean	Enables the Phased Release Cloudlet.	
<code>isSharedPolicy</code>	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 .	
<code>cloudletPolicy</code>	object	Specifies the Cloudlet policy as an object.	<code>isSharedPolicy</code> is <code>false</code>
<code>cloudletPolicy.id</code>	number	Identifies the Cloudlet.	
<code>cloudletPolicy.name</code>	string	The Cloudlet's descriptive name.	
<code>cloudletSharedPolicy</code>	number	Identifies the Cloudlet shared policy to use with this behavior. Use the Cloudlets API to list available shared policies.	<code>isSharedPolicy</code> is <code>true</code>
<code>label</code>	string	A label to distinguish this Phased Release policy from any others within the same property.	
<code>populationCookieType</code>	enum	Select when to assign a cookie to the population of users the Cloudlet defines. If you select the Cloudlet's <i>random</i> membership option, it overrides this option's value so that it is effectively <code>NONE</code> .	
	<code>NONE</code>	Do not expire the cookie.	
	<code>NEVER</code>	Never assign a cookie.	
	<code>ON_BROWSER_CLOSE</code>	Once the browser session ends.	
	<code>FIXED_DATE</code>	Specify a time when the cookie expires.	
	<code>DURATION</code>	Specify a delay before the cookie expires.	
<code>populationExpirationDate</code>	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.	<code>populationCookieType</code> is <code>FIXED_DATE</code>
<code>populationDuration</code>	string (duration)	Sets the lifetime of the cookie from the initial request. Subsequent requests re-evaluate based on current membership settings.	<code>populationCookieType</code> is <code>DURATION</code>
<code>populationRefresh</code>	boolean	Enabling this option resets the original duration of the cookie if the browser refreshes before the cookie expires.	<code>populationCookieType</code> is <code>DURATION</code>
<code>failoverEnabled</code>	boolean	Allows failure responses at the origin defined by the Cloudlet to fail over to the prevailing origin defined by the property.	
<code>failoverResponseCode</code>	string array	Defines the set of failure codes that initiate the failover response.	<code>failoverEnabled</code> is <code>true</code>
<code>failoverDuration</code>	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 <code>0</code> to immediately request the alternate origin upon failure.	<code>failoverEnabled</code> is <code>true</code>

pqcOrigin

- **Property Manager name:** [Post Quantum Cryptography to Origin](#)
- **Behavior version:** The `v2025-05-30` rule format supports the `pqcOrigin` behavior v1.0.
- **Rule format status:** [Deprecated, outdated rule format](#)
- **Access:** [Read/Write](#)
- **Allowed in includes:** [Yes](#)

Note that this behavior is in Limited Availability. To enable it, contact your Akamai account team.

Use this behavior to enable Post Quantum Cryptography (PQC) key exchanges.

This behavior is compatible only with Media Service Live and custom origins. To use Post Quantum Cryptography to Origin (PQC), your Origin TLS version needs transport layer security (TLS) version 1.3 and support for PQC ([X25519MLKEM768 key exchange](#)). It applies only to Enhanced TLS hostnames. Standard TLS hostnames in your property won't be affected by this change.

Option	Type	Description
<code>enabled</code>	boolean	Enables Post Quantum Cryptography (PQC) key exchanges.

preconnect

- **Property Manager name:** [Manual Preconnect](#)
- **Behavior version:** The `v2025-05-30` 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
<code>preconnectlist</code>	string array	Specifies the set of hostnames to which to preconnect over HTTP2.

predictiveContentDelivery

- **Property Manager name:** [Predictive Content Delivery](#)
- **Behavior version:** The `v2025-05-30` 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
<code>enabled</code>	boolean	Enables the predictive content delivery behavior.

predictivePrefetching

- **Property Manager name:** [Predictive Prefetching](#)
- **Behavior version:** The `v2025-05-30` 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.

Note that `predictivePrefetching` is disabled in [Ion](#) and [Dynamic Site Accelerator](#) by default. To enable the behavior, you need to activate it in your property.

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

prefetch

- **Property Manager name:** [Prefetch Objects](#)
- **Behavior version:** The `v2025-05-30` 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.

Note that `prefetch` is disabled in [Ion](#) and [Dynamic Site Accelerator](#) by default. To enable the behavior, you need to activate it in your property.

Option	Type	Description
<code>enabled</code>	boolean	Applies prefetching behavior when enabled.

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.

prefetchable

- **Property Manager name:** [Prefetchable Objects](#)
- **Behavior version:** The `v2025-05-30` 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
<code>enabled</code>	boolean	Allows matching content to prefetch when referenced on a requested parent page.

prefreshCache

- **Property Manager name:** [Cache Prefreshing](#)
- **Behavior version:** The `v2025-05-30` 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
<code>enabled</code>	boolean	Enables the cache prefreshing behavior.
<code>prefreshval</code>	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 <code>95</code> prefreshes the content without unnecessarily increasing load on the origin.

quicBeta

- **Property Manager name:** [QUIC Support \(Beta\)](#)
- **Behavior version:** The `v2025-05-30` rule format supports the `quicBeta` behavior v1.0.
- **Rule format status:** [Deprecated, outdated rule format](#)
- **Access:** [Read/Write](#)
- **Allowed in includes:** [No \(temporarily\)](#).

This behavior is deprecated.

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

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

randomSeek

- **Property Manager name:** [Random Seek](#)
- **Behavior version:** The `v2025-05-30` 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
<code>flv</code>	boolean	Enables random seek optimization in FLV files.	
<code>mp4</code>	boolean	Enables random seek optimization in MP4 files.	
<code>maximum Size</code>	string	Sets the maximum size of the MP4 file to optimize, expressed as a number suffixed with a unit string such as <code>MB</code> or <code>GB</code> .	<code>mp4</code> is <code>true</code>

rapid

- **Property Manager name:** [Akamai API Gateway](#)
- **Behavior version:** The `v2025-05-30` 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
<code>enabled</code>	boolean	Enables API Gateway for the current set of content.

readTimeout

- **Property Manager name:** [Read Timeout](#)
- **Behavior version:** The `v2025-05-30` rule format supports the `readTimeout` behavior v1.2.
- **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.

Option	Type	Description
<code>value</code>	string (duration)	The amount of time an edge server should wait for each read statement to return a response from the forward server after a connection has already been established. Larger objects may need many reads, and this timeout applies to each read separately. Any failure to complete a read within this time limit aborts the request and sends a 504 Gateway Timeout error to the client.
<code>firstByte Timeout</code>	string (duration)	The amount of time an edge server should wait for the first byte of the response to be returned from the forward server after a connection has already been established. Instead of continually waiting for the content, edge servers send a 504 Gateway Timeout error to the client. If your origin server is handling high loads and might respond slowly, specify a short timeout. Defaults to 20 seconds. The value for First Byte Timeout can't be 0 and it can't exceed 10 minutes (600 seconds).

realUserMonitoring

- **Property Manager name:** [Real User Monitoring \(RUM\)](#)
- **Behavior version:** The `v2025-05-30` 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
<code>enabled</code>	boolean	When enabled, activates real-use monitoring.

redirect

- **Property Manager name:** [Redirect](#)
- **Behavior version:** The `v2025-05-30` 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
<code>mobileDefaultChoice</code>	enum	Either specify a default response for mobile browsers, or customize your own.	
	<code>DEFAULT</code>	Allows all other <code>responseCode</code> values.	
	<code>MOBILE</code>	Allows only a 302 response code.	

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

Option	Type	Description	Requires
		<div> <div>301</div> <div>303</div> <div>302</div> <div>307</div> </div>	

redirectplus

- **Property Manager name:** [Redirect Plus](#)
- **Behavior version:** The `v2025-05-30` 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
<code>enabled</code>	boolean	Enables the redirect feature.
<code>destination</code>	string (allows variables)	Specifies the redirect as a path expression starting with a <code>/</code> character relative to the current root, or as a fully qualified URL. Optionally inject variables, as in this example that refers to the original request's filename: <code>/path/to/{{builtin.AK_FILENAME}}</code> .
<code>response Code</code>	enum	Assigns the status code for the redirect response.
		Supported values: <div> <div>301</div> <div>303</div> <div>302</div> <div>307</div> </div>

referrerChecking

- **Property Manager name:** [Legacy Referrer Checking](#)
- **Behavior version:** The `v2025-05-30` rule format supports the `referrerChecking` 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
<code>enabled</code>	boolean	Enables the referer-checking behavior.
<code>strict</code>	boolean	When enabled, excludes requests whose <code>Referer</code> header include a relative path, or that are missing a <code>Referer</code> . When disabled, only excludes requests whose <code>Referer</code> hostname is not part of the <code>domains</code> set.
<code>domains</code>	string array	Specifies the set of allowed domains. With <code>allowChildren</code> disabled, prefixing values with <code>*</code> specifies domains for which subdomains are allowed.
<code>allowChildren</code>	boolean	Allows all subdomains for the <code>domains</code> set, just like adding a <code>*</code> prefix to each.

removeQueryParam

- **Property Manager name:** [Remove Outgoing Request Parameters](#)
- **Behavior version:** The `v2025-05-30` rule format supports the `removeQueryParam` 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
<code>parameters</code>	string array	Specifies parameters to remove from the request.

removeVary

- **Property Manager name:** [Remove Vary Header](#)
- **Behavior version:** The `v2025-05-30` 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
<code>enabled</code>	boolean	When enabled, removes the <code>Vary</code> header to ensure objects can be cached.

report

- **Property Manager name:** [Log Request Details](#)
- **Behavior version:** The `v2025-05-30` 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
<code>logHost</code>	boolean	Log the <code>Host</code> header.	
<code>logReferer</code>	boolean	Log the <code>Referer</code> header.	
<code>logUserAgent</code>	boolean	Log the <code>User-Agent</code> header.	
<code>logAcceptLanguage</code>	boolean	Log the <code>Accept-Language</code> header.	

Option	Type	Description	Requires
<code>logCookies</code>	enum	Specifies the set of cookies to log.	
	<code>OFF</code>	Do not log cookies.	
	<code>ALL</code>	Log all cookies.	
	<code>SOME</code>	A specific set of <code>cookies</code> .	
<code>cookies</code>	string array	This specifies the set of cookies names whose values you want to log.	<code>logCookies</code> is <code>SOME</code>
<code>logCustomLogField</code>	boolean	Whether to append additional custom data to each log line.	
<code>customLogField</code>	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, <code>round-trip: {{builtin.AK_CLIENT_TURNAROUND_TIME}}ms</code> logs the total time to complete the response. See Support for variables for more information. If you enable the <code>logCustom</code> behavior, it overrides the <code>customLogField</code> option.	<code>logCustomLogField</code> is <code>true</code>
<code>logEdgeIP</code>	boolean	Whether to log the IP address of the Akamai edge server that served the response to the client.	
<code>logXForwardedFor</code>	boolean	Log any <code>X-Forwarded-For</code> request header.	

requestClientHints

- **Property Manager name:** [Request Client Hints](#)
- **Behavior version:** The `v2025-05-30` rule format supports the `requestClientHints` behavior v1.0.
- **Rule format status:** [Deprecated, outdated rule format](#)
- **Access:** [Read/Write](#)
- **Allowed in includes:** [Yes](#)

Client hints are HTTP request header fields that determine which resources the browser should include in the response. This behavior configures and prioritizes the client hints you want to send to request specific client and device information.

Use `requestClientHints` together with the [permissionsPolicy](#) behavior.

Option	Type	Description
<code>acceptCh</code>	string array	The client hint data objects you want to receive from the browser. You can add custom entries or provide pre-set values from the list. For more details on each value, see the guide section for this behavior. If you've configured your origin server to pass along data objects, they merge with the ones you set in this array, before the list is sent to the client.

Option	Type	Description
		<div> Device-Memory Sec-CH-DPR Sec-CH-UA-Full-Version-Li Sec-CH-UA-Platform-Version Downlink Sec-CH-UA Sec-CH-UA-Mobile Sec-CH-Viewport-Width ECT Sec-CH-UA-Arch Sec-CH-UA-Model Sec-CH-Width RTT Sec-CH-UA-Bitness Sec-CH-UA-Platform </div>
accept CriticalCh	string array	<p>The critical client hint data objects you want to receive from the browser. The original request from the browser needs to include these objects. Otherwise, a new response header is sent back to the client, asking for all of these client hint data objects. You can add custom entries or provide pre-set values from the list. For more details on each value, see the guide section for this behavior.</p> <div> Device-Memory Sec-CH-DPR Sec-CH-UA-Full-Version-Li Sec-CH-UA-Platform-Version Downlink Sec-CH-UA Sec-CH-UA-Mobile Sec-CH-Viewport-Width ECT Sec-CH-UA-Arch Sec-CH-UA-Model Sec-CH-Width RTT Sec-CH-UA-Bitness Sec-CH-UA-Platform </div>
reset	boolean	<p>This sends an empty instance of the <code>Accept-CH</code> response header to clear other <code>Accept-CH</code> values currently stored in the client browser. This empty header doesn't get merged with other objects sent from your origin server.</p> <p>To enable this option, make sure you leave <code>acceptCh</code> and <code>acceptCriticalCh</code> empty.</p>

requestControl

- **Property Manager name:** [Request Control Cloudlet](#)
- **Behavior version:** The `v2025-05-30` 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.	<code>isSharedPolicy</code> is <code>false</code>

Option	Type	Description	Requires
<code>cloudletPolicy.id</code>	number	Identifies the Cloudlet.	
<code>cloudletPolicy.name</code>	string	The Cloudlet's descriptive name.	
<code>cloudletSharedPolicy</code>	number	Identifies the Cloudlet shared policy to use with this behavior. Use the Cloudlets API to list available shared policies.	<code>isSharedPolicy</code> is <code>true</code>
<code>enableBranded403</code>	boolean	If enabled, serves a branded 403 page for this Cloudlet instance.	
<code>branded403StatusCode</code>	enum	Specifies the response status code for the branded deny action.	<code>enableBranded403</code> is <code>true</code>
		Supported values: <div> <div>200</div> <div>403</div> <div>302</div> <div>503</div> </div>	
<code>netStorage</code>	object	Specifies the NetStorage domain that contains the branded 403 page.	<code>enableBranded403</code> is <code>true</code> AND <code>branded403StatusCode</code> is not <code>302</code>
<code>netStorage.cpCode</code>	integer	Identifies a CP code assigned to this storage group.	
<code>netStorage.downloadDomainName</code>	string	Domain name from which content can be downloaded.	
<code>netStorage.g2oToken</code>	string	Signature Header Authentication key.	
<code>netStorage.id</code>	integer	Unique identifier for the storage group.	
<code>netStorage.name</code>	string	Name of the storage group.	
<code>branded403File</code>	string	Specifies the full path of the branded 403 page, including the filename, but excluding the NetStorage CP code path component.	<code>enableBranded403</code> is <code>true</code> AND <code>branded403StatusCode</code> is not <code>302</code>
<code>branded403Url</code>	string	Specifies the redirect URL for the branded deny action.	<code>enableBranded403</code> is <code>true</code> AND <code>branded403StatusCode</code> is <code>302</code>
<code>brandedDenyCacheTtl</code>	number (5-30)	Specifies the branded response page's time to live in the cache, 5 minutes by default.	<code>enableBranded403</code> is <code>true</code> AND <code>branded403StatusCode</code> is not <code>302</code>

requestTypeMarker

- **Property Manager name:** [Request Type Marker](#)
- **Behavior version:** The `v2025-05-30` 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 `v2025-05-30` 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.

The [brotli](#) compression behavior replaces the Resource Optimizer feature. Learn more about [using Brotli Compression](#).

Option	Type	Description
enabled	boolean	Enables the Resource Optimizer feature.

resourceOptimizerExtendedCompatibility

- **Property Manager name:** [Resource Optimizer Extended Compatibility](#)

- **Behavior version:** The `v2025-05-30` 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.

The `brrotli` compression behavior replaces the Resource Optimizer feature. Learn more about [using Brotli Compression](#).

Option	Type	Description
<code>enabled</code>	boolean	Enables the Resource Optimizer feature.
<code>enableAllFeatures</code>	boolean	Enables additional support and error handling.

responseCode

- **Property Manager name:** [Set Response Code](#)
- **Behavior version:** The `v2025-05-30` 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.																																																																									
		<div>Supported values:<table><tr><td>100</td><td>203</td><td>302</td><td>401</td><td>409</td><td>417</td><td>431</td><td>503</td><td>598</td></tr><tr><td>101</td><td>204</td><td>303</td><td>402</td><td>410</td><td>422</td><td>444</td><td>504</td><td>599</td></tr><tr><td>102</td><td>205</td><td>304</td><td>403</td><td>411</td><td>423</td><td>449</td><td>505</td><td></td></tr><tr><td>103</td><td>206</td><td>305</td><td>404</td><td>412</td><td>424</td><td>450</td><td>506</td><td></td></tr><tr><td>122</td><td>207</td><td>306</td><td>405</td><td>413</td><td>425</td><td>499</td><td>507</td><td></td></tr><tr><td>200</td><td>226</td><td>307</td><td>406</td><td>414</td><td>426</td><td>500</td><td>509</td><td></td></tr><tr><td>201</td><td>300</td><td>308</td><td>407</td><td>415</td><td>428</td><td>501</td><td>510</td><td></td></tr><tr><td>202</td><td>301</td><td>400</td><td>408</td><td>416</td><td>429</td><td>502</td><td>511</td><td></td></tr></table></div>	100	203	302	401	409	417	431	503	598	101	204	303	402	410	422	444	504	599	102	205	304	403	411	423	449	505		103	206	305	404	412	424	450	506		122	207	306	405	413	425	499	507		200	226	307	406	414	426	500	509		201	300	308	407	415	428	501	510		202	301	400	408	416	429	502	511		
100	203	302	401	409	417	431	503	598																																																																			
101	204	303	402	410	422	444	504	599																																																																			
102	205	304	403	411	423	449	505																																																																				
103	206	305	404	412	424	450	506																																																																				
122	207	306	405	413	425	499	507																																																																				
200	226	307	406	414	426	500	509																																																																				
201	300	308	407	415	428	501	510																																																																				
202	301	400	408	416	429	502	511																																																																				

Option	Type	Description	Requires
<code>override206</code>	boolean	Allows any specified <code>200</code> success code to override a <code>206</code> partial-content code, in which case the response's content length matches the requested range length.	<code>statusCode</code> is <code>200</code>

responseCookie

- **Property Manager name:** [Set Response Cookie](#)
- **Behavior version:** The `v2025-05-30` 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
<code>cookieName</code>	string (allows variables)	Specifies the name of the cookie, which serves as a key to determine if the cookie is set.	
<code>enabled</code>	boolean	Allows you to set a response cookie.	
<code>type</code>	enum	What type of value to assign.	
	<code>FIXED</code>	Assign a <code>FIXED</code> value based on the <code>value</code> field.	
	<code>UNIQUE</code>	Assign a unique value.	
<code>value</code>	string (allows variables)	If the cookie <code>type</code> is <code>FIXED</code> , this specifies the cookie value.	<code>type</code> is <code>FIXED</code>
<code>format</code>	enum	When the <code>type</code> of cookie is set to <code>UNIQUE</code> , this sets the date format.	<code>type</code> is <code>UNIQUE</code>
	<code>AKAMAI</code>	Akamai format, which adds milliseconds to the date stamp.	
	<code>APACHE</code>	Apache format.	
<code>defaultDomain</code>	boolean	When enabled, uses the default domain value, otherwise the set specified in the <code>domain</code> field.	
<code>defaultPath</code>	boolean	When enabled, uses the default path value, otherwise the set specified in the <code>path</code> field.	
<code>domain</code>	string (allows variables)	If the <code>defaultDomain</code> is disabled, this sets the domain for which the cookie is valid. For example, <code>example.com</code> makes the cookie valid for that hostname and all subdomains.	<code>defaultDomain</code> is <code>false</code>
<code>path</code>	string (allows variables)	If the <code>defaultPath</code> is disabled, sets the path component for which the cookie is valid.	<code>defaultPath</code> is <code>false</code>

Option	Type	Description	Requires
<code>expires</code>	enum	Sets various ways to specify when the cookie expires.	
	<code>ON_BROWSER_CLOSE</code>	Limit the cookie to the duration of the session.	
	<code>FIXED_DATE</code>	Requires a corresponding <code>expirationDate</code> field value.	
	<code>DURATION</code>	Requires a corresponding <code>duration</code> field value.	
	<code>NEVER</code>	Let the cookie persist indefinitely.	
<code>expirationDate</code>	string (epoch timestamp)	If <code>expires</code> is set to <code>FIXED_DATE</code> , this sets when the cookie expires as a UTC date and time.	<code>expires</code> is <code>FIXED_DATE</code>
<code>duration</code>	string (duration)	If <code>expires</code> is set to <code>DURATION</code> , this sets the cookie's lifetime.	<code>expires</code> is <code>DURATION</code>
<code>sameSite</code>	enum	This option controls the <code>SameSite</code> cookie attribute that reduces the risk of cross-site request forgery attacks.	
	<code>DEFAULT</code>	Send the <code>SameSite</code> cookie attribute.	
	<code>NONE</code>	Send the cookie in all contexts if the <code>secure</code> option is enabled.	
	<code>LAX</code>	Send the cookie also when the user navigates to a URL from an external site.	
	<code>STRICT</code>	Send the cookie only to the same site that originated it.	
<code>secure</code>	boolean	When enabled, sets the cookie's <code>Secure</code> flag to transmit it with <code>HTTPS</code> .	
<code>httpOnly</code>	boolean	When enabled, includes the <code>HttpOnly</code> attribute in the <code>Set-Cookie</code> 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 `v2025-05-30` 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 `v2025-05-30` 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
<code>responseHeaderName</code>	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 `v2025-05-30` 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
<code>behavior</code>	enum	The action to perform on the path.	
	<code>REPLACE</code>	Specify the <code>match</code> and <code>targetPath</code> . For example, a <code>match</code> of <code>/path1/</code> and a <code>targetPath</code> of <code>/path1/path2/</code> changes <code>/path1/page.html</code> to <code>/path1/path2/page.html</code> .	
	<code>REMOVE</code>	Specify the <code>match</code> . For example, a <code>match</code> of <code>/path2/</code> changes <code>/path1/path2/page.html</code> to <code>/path1/page.html</code> .	
	<code>REWRITE</code>	Specify the <code>targetUrl</code> . For example, you can direct traffic to <code>/error/restricted.html</code> .	
	<code>PREPEND</code>	Specify the <code>targetPathPrepend</code> . For example, if set to <code>/prefix/</code> , <code>/path1/page.html</code> changes to <code>/prefix/path1/page.html</code> .	
	<code>REGEX_REPLACE</code>	Specify the <code>matchRegex</code> and <code>targetRegex</code> . For example, specifying <code>logo\\. (png gif jpe?g)</code> and <code>brand\\\$1</code> changes <code>logo.png</code> to <code>brand.png</code> .	
<code>match</code>	string	When <code>behavior</code> is <code>REMOVE</code> or <code>REPLACE</code> , specifies the part of the incoming path you'd like to remove or modify.	<code>behavior</code> is either: <code>REMOVE</code> , <code>REPLACE</code>
<code>matchRegex</code>	string	When <code>behavior</code> is set to <code>REGEX_REPLACE</code> , specifies the Perl-compatible regular expression to replace with <code>targetRegex</code> .	<code>behavior</code> is <code>REGEX_REPLACE</code>
<code>targetRegex</code>	string (allows variables)	When <code>behavior</code> is set to <code>REGEX_REPLACE</code> , this replaces whatever the <code>matchRegex</code> field matches, along with any captured sequences from <code>\\\$1</code> through <code>\\\$9</code> .	<code>behavior</code> is <code>REGEX_REPLACE</code>
<code>targetPath</code>	string (allows variables)	When <code>behavior</code> is set to <code>REPLACE</code> , this path replaces whatever the <code>match</code> field matches in the incoming request's path.	<code>behavior</code> is <code>REPLACE</code>
<code>targetPathPrepend</code>	string (allows variables)	When <code>behavior</code> is set to <code>PREPEND</code> , specifies a path to prepend to the incoming request's URL.	<code>behavior</code> is <code>PREPEND</code>
<code>targetUrl</code>	string (allows variables)	When <code>behavior</code> is set to <code>REWRITE</code> , specifies the full path to request from the origin.	<code>behavior</code> is <code>REWRITE</code>
<code>matchMultiple</code>	boolean	When enabled, replaces all potential matches rather than only the first.	<code>behavior</code> is either: <code>REMOVE</code> , <code>REPLACE</code> , <code>REGEX_REPLACE</code>

Option	Type	Description	Requires
<code>keepQueryString</code>	boolean	When enabled, retains the original path's query parameters.	<code>behavior</code> is not <code>REWRITE</code>

rumCustom

- **Property Manager name:** [RUM SampleRate](#)
- **Behavior version:** The `v2025-05-30` 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 `realUserMonitoring` behavior is deprecated as well.

Option	Type	Description
<code>rumSampleRate</code>	number (0-100)	Specifies the percentage of web traffic to include in your RUM report.
<code>rumGroupName</code>	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 `v2025-05-30` 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
<code>customerAction</code>	enum	Specifies the request component that identifies a SaaS customer.	
	<code>DISABLED</code>	This effectively ignores customers.	
	<code>HOSTNAME</code>	In a hostname.	
	<code>PATH</code>	In the URL path.	
	<code>QUERY_STRING</code>	In a query parameter.	
	<code>COOKIE</code>	In a cookie.	
<code>customerCnameEnabled</code>	boolean	Enabling this allows you to identify customers using a <i>CNAME chain</i> rather than a single hostname.	<code>customerAction</code> is <code>HOSTNAME</code>
<code>customerCnameLevel</code>	number	Specifies the number of CNAMEs to use in the chain.	<code>customerCnameEnabled</code> is <code>true</code>
<code>customerCookie</code>	string	This specifies the name of the cookie that identifies the customer.	<code>customerAction</code> is <code>COOKIE</code>
<code>customerQueryString</code>	string	This names the query parameter that identifies the customer.	<code>customerAction</code> is <code>QUERY_STRING</code>
<code>customerRegex</code>	string	Specifies a Perl-compatible regular expression with which to substitute the request's customer ID.	<code>customerAction</code> is either: <code>HOSTNAME</code> , <code>PATH</code> , <code>COOKIE</code> , <code>QUERY_STRING</code>
<code>customerReplace</code>	string	Specifies a string to replace the request's customer ID matched by <code>customerRegex</code> .	<code>customerAction</code> is either: <code>HOSTNAME</code> , <code>PATH</code> , <code>COOKIE</code> , <code>QUERY_STRING</code>
<code>applicationAction</code>	enum	Specifies the request component that identifies a SaaS application.	
	<code>DISABLED</code>	This effectively ignores applications.	
	<code>HOSTNAME</code>	In the hostname.	
	<code>PATH</code>	In the URL path.	
	<code>QUERY_STRING</code>	In a query parameter.	
	<code>COOKIE</code>	In a cookie.	
<code>applicationCnameEnabled</code>	boolean	Enabling this allows you to identify applications using a <i>CNAME chain</i> rather than a single hostname.	<code>applicationAction</code> is <code>HOSTNAME</code>
<code>applicationCnameLevel</code>	number	Specifies the number of CNAMEs to use in the chain.	<code>applicationCnameEnabled</code> is <code>true</code>
<code>applicationCookie</code>	string	This specifies the name of the cookie that identifies the application.	<code>applicationAction</code> is <code>COOKIE</code>

Option	Type	Description	Requires
<code>applicationQueryString</code>	string	This names the query parameter that identifies the application.	<code>applicationAction</code> is <code>QUERY_STRING</code>
<code>applicationRegex</code>	string	Specifies a Perl-compatible regular expression with which to substitute the request's application ID.	<code>applicationAction</code> is either: <code>HOSTNAME</code> , <code>PATH</code> , <code>COOKIE</code> , <code>QUERY_STRING</code>
<code>applicationReplace</code>	string	Specifies a string to replace the request's application ID matched by <code>applicationRegex</code> .	<code>applicationAction</code> is either: <code>HOSTNAME</code> , <code>PATH</code> , <code>COOKIE</code> , <code>QUERY_STRING</code>
<code>usersAction</code>	enum	Specifies the request component that identifies a SaaS user.	
	<code>DISABLED</code>	This effectively ignores users.	
	<code>HOSTNAME</code>	In a hostname.	
	<code>PATH</code>	In the URL path.	
	<code>QUERY_STRING</code>	In a query parameter.	
	<code>COOKIE</code>	In a cookie.	
<code>usersCnameEnabled</code>	boolean	Enabling this allows you to identify users using a <i>CNAME chain</i> rather than a single hostname.	<code>usersAction</code> is <code>HOSTNAME</code>
<code>usersCnameLevel</code>	number	Specifies the number of CNAMEs to use in the chain.	<code>usersCnameEnabled</code> is <code>true</code>
<code>usersCookie</code>	string	This specifies the name of the cookie that identifies the user.	<code>usersAction</code> is <code>COOKIE</code>
<code>usersQueryString</code>	string	This names the query parameter that identifies the user.	<code>usersAction</code> is <code>QUERY_STRING</code>
<code>usersRegex</code>	string	Specifies a Perl-compatible regular expression with which to substitute the request's user ID.	<code>usersAction</code> is either: <code>HOSTNAME</code> , <code>PATH</code> , <code>COOKIE</code> , <code>QUERY_STRING</code>
<code>usersReplace</code>	string	Specifies a string to replace the request's user ID matched by <code>usersRegex</code> .	<code>usersAction</code> is either: <code>HOSTNAME</code> , <code>PATH</code> , <code>COOKIE</code> , <code>QUERY_STRING</code>

salesForceCommerceCloudClient

- **Property Manager name:** [Akamai Connector for Salesforce Commerce Cloud](#)
- **Behavior version:** The `v2025-05-30` 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
<code>enabled</code>	boolean	Enables the Akamai Connector for Salesforce Commerce Cloud.	
<code>connectorId</code>	string (allows variables)	An ID value that helps distinguish different types of traffic sent from Akamai to the Salesforce Commerce Cloud. Form the value as <i>instance-realm-customer</i> , where <i>instance</i> is either <code>production</code> or <code>development</code> , <i>realm</i> is your Salesforce Commerce Cloud service <code>\$REALM</code> value, and <i>customer</i> is the name for your organization in Salesforce Commerce Cloud. You can use alphanumeric characters, underscores, or dot characters within dash-delimited segment values.	
<code>originType</code>	enum	Specifies where the origin is.	
	<code>DEFAULT</code>	Use a default Salesforce origin.	
	<code>CUSTOMER</code>	Customize the origin.	
<code>sf3cOriginHost</code>	string (allows variables)	This specifies the hostname or IP address of the custom Salesforce origin.	<code>originType</code> is <code>CUSTOMER</code>
<code>originHostHeader</code>	enum	Specifies where the <code>Host</code> header is defined.	
	<code>DEFAULT</code>	Use the default Salesforce header.	
	<code>CUSTOMER</code>	Customize the header.	
<code>sf3cOriginHostHeader</code>	string (allows variables)	This specifies the hostname or IP address of the custom Salesforce host header.	<code>originHostHeader</code> is <code>CUSTOMER</code>
<code>allowOverrideOriginCacheKey</code>	boolean	When enabled, overrides the forwarding origin's cache key.	

salesForceCommerceCloudProvider

- **Property Manager name:** [Akamai Provider for Salesforce Commerce Cloud](#)
- **Behavior version:** The `v2025-05-30` 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 v2025-05-30 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 v2025-05-30 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
<code>enabled</code>	boolean	Enables processing of POST requests.

scheduleInvalidation

- **Property Manager name:** [Scheduled Invalidation](#)
- **Behavior version:** The `v2025-05-30` 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.

Note that this behavior is no longer compatible with the [metadataStage](#) criteria.

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

scriptManagement

- **Property Manager name:** [Script Management](#)
- **Behavior version:** The `v2025-05-30` 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. See [Script Management API](#) for more information.

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

segmentedContentProtection

- **Property Manager name:** [Segmented Media Protection](#)
- **Behavior version:** The `v2025-05-30` rule format supports the `segmentedContentProtection` behavior v2.1.
- **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
<code>enabled</code>	boolean	Enables the segmented content protection behavior.	
<code>key</code>	object array	Specifies the encryption key to use as a shared secret to validate tokens.	
<code>useAdvanced</code>	boolean	Allows you to specify advanced <code>transitionKey</code> and <code>salt</code> options.	
<code>transitionKey</code>	object array	An alternate encryption key to match along with the <code>key</code> field, allowing you to rotate keys with no down time.	<code>useAdvanced</code> is <code>true</code>
<code>salt</code>	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.	<code>useAdvanced</code> is <code>true</code>
<code>headerForSalt</code>	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 <code>User-Agent</code> , <code>X-Playback-Session-Id</code> , and <code>Origin</code> . Any specified header needs to appear in the player's request.	<code>useAdvanced</code> is <code>true</code>
<code>sessionId</code>	boolean	Enabling this option carries the <code>session_id</code> value from the access token over to the session token, for use in tracking and counting unique playback sessions.	<code>useAdvanced</code> is <code>true</code>
<code>dataPayload</code>	boolean	Enabling this option carries the <code>data/payload</code> 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.	<code>useAdvanced</code> is <code>true</code>
<code>ip</code>	boolean	Enabling this restricts content access to a specific IP address, only appropriate if it does not change during the playback session.	<code>useAdvanced</code> is <code>true</code>
<code>acl</code>	boolean	Enabling this option carries the <code>ACL</code> 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 <code>ACL</code> field. Playback may fail if the base path of the master playlist (and variant playlist, plus segments) varies from that of the <code>ACL</code> field.	<code>useAdvanced</code> is <code>true</code>
<code>enableTokenInURI</code>	boolean	When enabled, passes tokens in HLS variant manifest URLs and HLS segment URLs, as an alternative to cookies.	
<code>hlsMasterManifestFiles</code>	string array	Specifies the set of filenames that form HLS master manifest URLs. You can use <code>*</code> wildcard character that matches zero or more characters. Make sure to specify master manifest filenames uniquely, to distinguish them from variant manifest files.	<code>enableTokenInURI</code> is <code>true</code>
<code>enableTokenInQueryString</code>	boolean	When enabled, in the DASH media encryption variant, passes tokens in query strings, as an alternative to cookies.	
<code>tokenRevocationEnabled</code>	boolean	Enable this to deny requests from playback URLs that contain a <code>TokenAuth</code> token that uses specific token identifiers.	
<code>revokedListId</code>	string	Identifies the <code>TokenAuth</code> tokens to block from accessing your content.	<code>tokenRevocationEnabled</code> is <code>true</code>
<code>hlsMediaEncryption</code>	boolean	Enables HLS Segment Encryption.	
<code>dashMediaEncryption</code>	boolean	Whether to enable DASH Media Encryption.	

segmentedMediaOptimization

- **Property Manager name:** [Segmented Media Delivery Mode](#)
- **Behavior version:** The `v2025-05-30` 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
<code>behavior</code>	enum	Sets the type of media content to optimize.	
	<code>ON_DEMAND</code>	Media is available on demand. This is the only option allowed for NetStorage origins.	
	<code>LIVE</code>	Media is streaming live.	
<code>enableUllStreaming</code>	boolean	Enables ultra low latency (ULL) streaming. ULL reduces latency and decreases overall transfer time of live streams.	<code>behavior is LIVE</code>
<code>showAdvanced</code>	boolean	Allows you to configure advanced media options.	<code>behavior is LIVE</code>
<code>liveType</code>	enum	The type of live media.	<code>showAdvanced is true</code>
	<code>CONTINUOUS</code>	Not confined to a range of time.	
	<code>EVENT</code>	An event for a range of time.	
<code>startTime</code>	string (epoch timestamp)	This specifies when the live media event begins.	<code>showAdvanced is true</code> <code>AND liveType is</code> <code>EVENT</code>
<code>endTime</code>	string (epoch timestamp)	This specifies when the live media event ends.	<code>showAdvanced is true</code> <code>AND liveType is</code> <code>EVENT</code>
<code>dvrType</code>	enum	The type of DVR.	<code>showAdvanced is true</code>
	<code>CONFIGURABLE</code>	A configurable DVR.	
	<code>UNKNOWN</code>	An unknown DVR.	
<code>dvrWindow</code>	string (duration)	Set the duration for your media, or <code>0m</code> if a DVR is not required.	<code>showAdvanced is true</code> <code>AND dvrType is</code> <code>CONFIGURABLE</code>

segmentedMediaStreamingPrefetch

- **Property Manager name:** [Segmented Media Streaming - Prefetch](#)
- **Behavior version:** The `v2025-05-30` 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
<code>enabled</code>	boolean	Enables media stream prefetching.

setVariable

- **Property Manager name:** [Set Variable](#)
- **Behavior version:** The `v2025-05-30` rule format supports the `setVariable` behavior v1.7.
- **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
<code>variableName</code>	string (variable name)	Specifies the predeclared root name of the variable to modify. When you declare a variable name such as <code>VAR</code> , its name is prepended with <code>PMUSER_</code> and accessible in a <code>user</code> namespace, so that you invoke it in subsequent text fields within the rule tree as <code>{{user.PMUSER_VAR}}</code> . In deployed XML metadata , it appears as <code>% (PMUSER_VAR)</code> .	
<code>valueSource</code>	enum	Determines how you want to set the value.	
	<code>EXPRESSION</code>	Specify your own string expression.	
	<code>EXTRACT</code>	Extract it from another value.	
	<code>GENERATE</code>	Generate the value.	
<code>variableValue</code>	string (allows variables)	This directly specifies the value to assign to the variable. The expression may include a mix of static text and other variables, such as <code>new_filename.{{builtin.AK_EXTENSION}}</code> to embed a system variable.	<code>valueSource</code> is <code>EXPRESSION</code>
<code>extractLocation</code>	enum	This specifies from where to get the value.	<code>valueSource</code> is <code>EXTRACT</code>
	<code>CLIENT_CERTIFICATE</code>	Client certificate.	
	<code>CLIENT_REQUEST_HEADER</code>	Client request header.	
	<code>COOKIE</code>	Cookie.	
	<code>EDGESCAPE</code>	For location or network data.	
	<code>PATH_COMPONENT_OFFSET</code>	Substring within the URL path.	
	<code>QUERY_STRING</code>	A query parameter.	
	<code>DEVICE_PROFILE</code>	For client device attributes.	
	<code>RESPONSE_HEADER</code>	A response header.	
	<code>SET_COOKIE</code>	Cookie.	
<code>certificateFieldName</code>	enum	Specifies the certificate's content.	<code>extractLocation</code> is <code>CLIENT_CERTIFICATE</code>
	<code>VERSION</code>	The certificate's X509 version number.	
	<code>SERIAL</code>	The serial number, expressed in hex.	
	<code>FINGERPRINT_MD5</code>	The hex-encoded MD5 fingerprint.	
	<code>FINGERPRINT_SHA1</code>	The hex-encoded SHA1 fingerprint.	
	<code>FINGERPRINT_DYN</code>	The hex-encoded fingerprint generated based on the <code>SIGNATURE_ALGORITHM</code> .	
	<code>ISSUER_DN</code>	The <i>distinguished name</i> field for the certificate's issuer.	
	<code>SUBJECT_DN</code>	The <i>distinguished name</i> field for the user.	
	<code>NOT_BEFORE</code>	The start of the time range, expressed in <code>YYYY/MM/DD HH:MI:SS ZONE</code> format, where the zone is optional.	
	<code>NOT_AFTER</code>	The end of the time range, expressed in <code>YYYY/MM/DD HH:MI:SS ZONE</code> format, where the zone is optional.	

Option	Type	Description	Requires
	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.	
headerName	string (allows variables)	Specifies the case-insensitive name of the HTTP header to extract.	extractLocation is CLIENT_REQUEST_HEADER
responseHeaderName	string (allows variables)	Specifies the case-insensitive name of the HTTP header to extract.	extractLocation is RESPONSE_HEADER
setCookieName	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-Edgescap header's field name. Possible values specify basic geolocation, various geographic standards, and information about the client's network. For details on Edge Scape header fields, see the EdgeScape User Guide ⁶ .	extractLocation is EDGESCAP
	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.	

Option	Type	Description	Requires
	NETWORK_TYPE	Network type.	
	ASNUM	Autonomous System Number.	
	THROUGHPUT	Tiered throughput level.	
	BW	Tiered bandwidth level.	
pathComponent 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
queryParameter 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.	
numberOfBytes	number (1-16)	Specifies the number of random hex bytes to generate.	generator is HEXRAND
minRandom Number	number	Specifies the lower bound of the random number.	generator is RAND
maxRandom Number	number	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.	

Option	Type	Description	Requires
	HEX_DECODE	String conversion.	
	HEX_ENCODE	String conversion.	
	HMAC	Data digest.	
	LOWER	String function.	
	MD5	Data digest.	
	MINUS	Arithmetic function, reverse sign.	
	MODULO	Arithmetic function, get remainder.	
	MULTIPLY	Arithmetic function.	
	NORMALIZE_PATH_WIN	Convert Windows paths to Unix format and remove relative path syntax.	
	REMOVE_WHITESPACE	String conversion.	
	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 <code>BASE_64_DECODE</code> , except before decoding replaces <code>+</code> with <code>-</code> and <code>/</code> with <code>_</code> . If due to the encoding there are not enough characters for the algorithm, this adds <code>=</code> characters at the end of the string. See Output padding for more information.	
	BASE_64_URL_ENCODE	The same as <code>BASE_64_ENCODE</code> , except after encoding this removes trailing <code>=</code> characters, replacing <code>+</code> with <code>-</code> and <code>/</code> with <code>_</code> .	
	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 <code>transform</code> function is set to various arithmetic functions (<code>ADD</code> , <code>SUBTRACT</code> , <code>MULTIPLY</code> ,	<code>transform</code> is either: <code>ADD</code> , <code>BITWISE_AND</code> , <code>BITWISE_OR</code> , <code>BITWISE_XOR</code> ,

Option	Type	Description	Requires
		DIVIDE , or MODULO) or bitwise functions (BITWISE_AND , BITWISE_OR , 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.	
	ALG_AES128	Advanced Encryption Standard, 128 bits.	
	ALG_AES256	Advanced Encryption Standard, 256 bits.	
encryptionKey	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
encryptionMode	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
prependBytes	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
hmacAlgorithm	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

Option	Type	Description	Requires
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
caseSensitive	boolean	Enabling this makes all matches case sensitive.	transform is either: EXTRACT_PARAM, SUBSTITUTE
global Substitution	boolean	Replaces all matches in the string, not just the first.	transform is SUBSTITUTE
startIndex	number	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 <code>abcdefghij</code> : <pre> 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 </pre>	transform is SUBSTRING
endIndex	number	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 <code>abcdefghij</code> : <pre> 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 </pre>	transform is SUBSTRING
exceptChars	string	Specifies characters <i>not</i> to encode, possibly overriding the default set.	transform is URL_ENCODE
forceChars	string	Specifies characters to encode, possibly overriding the default set.	transform is URL_ENCODE
deviceProfile	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.	

Option	Type	Description	Requires
	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.	
	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 `v2025-05-30` 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
<code>error</code> Type	enum	Specifies the type of error.	
		Supported values: <code>ERR_CONNECT_FAIL</code>	

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

siteShield

- **Property Manager name:** [SiteShield](#)
- **Behavior version:** The `v2025-05-30` 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 <code>value</code> key that references the hostname, for example: <code>"ssmap": {"value": "ss.akamai.net"}</code> .

standardTLSMigration

- **Property Manager name:** [Standard TLS Migration](#)

- **Behavior version:** The `v2025-05-30` 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
<code>enabled</code>	boolean	Allows migration to Standard TLS.	
<code>migrationFrom</code>	enum	What kind of traffic you're migrating from.	
	<code>SHARED_CERT</code>	A shared certificate.	
	<code>NON_SECURE</code>	Non-secure traffic.	
	<code>ENHANCED_SECURE</code>	Enhanced Secure TLS.	
<code>allowHTTPSUpgrade</code>	boolean	Allows temporary upgrade of HTTP traffic to HTTPS.	<code>migrationFrom</code> is <code>NON_SECURE</code>
<code>allowHTTPSDowngrade</code>	boolean	Allow temporary downgrade of HTTPS traffic to HTTP. This removes various <code>Origin</code> , <code>Referer</code> , <code>Cookie</code> , <code>Cookie2</code> , <code>sec-*</code> and <code>proxy-*</code> headers from the request to origin.	<code>migrationFrom</code> is <code>NON_SECURE</code>
<code>migrationStartTime</code>	string (epoch timestamp)	Specifies when to start migrating the cache.	<code>allowHTTPSUpgrade</code> is <code>true</code> OR <code>allowHTTPSDowngrade</code> is <code>true</code>
<code>migrationDuration</code>	number	Specifies the number of days to migrate the cache.	<code>allowHTTPSUpgrade</code> is <code>true</code> OR <code>allowHTTPSDowngrade</code> is <code>true</code>
<code>cacheSharingStartTime</code>	string (epoch timestamp)	Specifies when to start cache sharing.	<code>migrationFrom</code> is <code>ENHANCED_SECURE</code>
<code>cacheSharingDuration</code>	number	Specifies the number cache sharing days.	<code>migrationFrom</code> is <code>ENHANCED_SECURE</code>
<code>isCertificateSNIOOnly</code>	boolean	Sets whether your new certificate is SNI-only.	<code>migrationFrom</code> is <code>ENHANCED_SECURE</code>
<code>isTieredDistributionUsed</code>	boolean	Allows you to align traffic to various tieredDistribution areas.	<code>migrationFrom</code> is <code>NON_SECURE</code>
<code>tdLocation</code>	enum	Specifies the tieredDistribution location.	<code>isTieredDistributionUsed</code> is <code>true</code>
	<code>GLOBAL</code>	Global.	
	<code>APAC</code>	Asia and Pacific.	
	<code>EUROPE</code>	Europe.	
	<code>US_EAST</code>	Eastern United States.	

Option	Type	Description	Requires
	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 v2025-05-30 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 v2025-05-30 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
<code>valid Mode</code>	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.
<code>strict Mode</code>	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.

sureRoute

- **Property Manager name:** [SureRoute](#)
- **Behavior version:** The `v2025-05-30` 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 *rac*es to identify alternative paths to use in case of a transmission failure. These races increase origin traffic slightly.

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

Option	Type	Description	Requires
<code>enabled</code>	boolean	Enables the SureRoute behavior, to optimize delivery of non-cached content.	

Option	Type	Description	Requires
<code>type</code>	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.	
<code>customMap</code>	string	If <code>type</code> is <code>CUSTOM_MAP</code> , this specifies the map string provided to you by Akamai Professional Services, or included as part of the Site Shield product.	<code>type</code> is <code>CUSTOM_MAP</code>
<code>testObjectUrl</code>	string	<p>Specifies the path and filename for your origin's test object to use in races to test routes.</p> <p>Akamai provides sample test objects for the Dynamic Site Accelerator and Web Application Accelerator products. If you want to use your own test object, it needs to be on the same origin server as the traffic being served through SureRoute. Make sure it returns a 200 HTTP response and does not require authentication. The file should be an average-sized static HTML file (<code>Content-Type: text/html</code>) that is no smaller than 8KB, with no back-end processing.</p> <p>If you have more than one origin server deployed behind a load balancer, you can configure it to serve the test object directly on behalf of the origin, or route requests to the same origin server to avoid deploying the test object on each origin server.</p>	
<code>toHostStatus</code>	enum	Specifies which hostname to use.	
	INCOMING_HH	Use the incoming <code>Host</code> header when requesting the SureRoute test object.	
	OTHER	Use <code>toHost</code> to specify a custom <code>Host</code> header.	
<code>toHost</code>	string	If <code>toHostStatus</code> is <code>OTHER</code> , this specifies the custom <code>Host</code> header to use when requesting the SureRoute test object.	<code>toHostStatus</code> is <code>OTHER</code>
<code>raceStatTtl</code>	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.	
<code>forceSslForward</code>	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.	
<code>enableCustomKey</code>	boolean	When disabled, caches race results under the race destination's hostname. If enabled, use <code>customStatKey</code> to specify a custom hostname.	
<code>customStatKey</code>	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.	<code>enableCustomKey</code> is <code>true</code>

tcpOptimization

- **Property Manager name:** [TCP Optimizations](#)
- **Behavior version:** The `v2025-05-30` 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 `v2025-05-30` rule format supports the `teaLeaf` behavior v1.0.
- **Rule format status:** [Deprecated, outdated rule format](#)
- **Access:** [Read/Write](#)
- **Allowed in includes:** [No \(temporarily\)](#).

Note that this behavior is decommissioned.

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

tieredDistribution

- **Property Manager name:** [Tiered Distribution](#)
- **Behavior version:** The `v2025-05-30` 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
<code>enabled</code>	boolean	When enabled, activates tiered distribution.	
<code>tieredDistributionMap</code>	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.	<code>is_secure</code> is <code>false</code> in top-level rule
	<code>CH2</code>	A global map.	
	<code>CHAPAC</code>	China and the Asian Pacific area.	
	<code>CHEU2</code>	Europe.	
	<code>CHEUS2</code>	Eastern United States.	
	<code>CHCUS2</code>	Central United States.	
	<code>CHWUS2</code>	Western United States.	
	<code>CHAUS</code>	Australia.	
	<code>CH</code>	A global map.	

tieredDistributionAdvanced

- **Property Manager name:** [Tiered Distribution \(Advanced\)](#)
- **Behavior version:** The `v2025-05-30` 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
<code>enabled</code>	boolean	When enabled, activates tiered distribution.
<code>tieredDistributionMap</code>	string	Optionally map the tiered parent server's location close to your origin: <code>CHEU2</code> for Europe; <code>CHAUS</code> for Australia; <code>CHAPAC</code> for China and the Asian Pacific area; <code>CHWUS2</code> , <code>CHCUS2</code> , and <code>CHEUS2</code> for different parts of the United States. Choose <code>CH</code> or <code>CH2</code> 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 `v2025-05-30` 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
<code>customMapEnabled</code>	boolean	Enables custom maps.	
<code>customMapName</code>	string (allows variables)	Specifies the custom map name.	<code>customMapEnabled</code> is <code>true</code>
<code>serialStart</code>	string	Specifies a numeric serial start value.	<code>customMapEnabled</code> is <code>true</code>

Option	Type	Description	Requires
<code>serialEnd</code>	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.	<code>customMap</code> Enabled is <code>true</code>
<code>hashAlgorithm</code>	enum	Specifies the hash algorithm.	<code>customMap</code> Enabled is <code>true</code>
	<code>GCC</code>	A GCC hash.	
	<code>JENKINS</code>	A Jenkins hash.	
<code>mapMigration</code> Enabled	boolean	Enables migration of the custom map to Cloud Wrapper.	
<code>migration</code> <code>WithinCwMaps</code> Enabled	boolean	Enables migration within Cloud Wrapper maps.	<code>mapMigration</code> Enabled is <code>true</code>
<code>location</code>	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.	<code>migrationWithin</code> <code>CwMapsEnabled</code> is <code>true</code>
<code>migration</code> <code>StartDate</code>	string (epoch timestamp)	Specifies when to start migrating the map.	<code>mapMigration</code> Enabled is <code>true</code>
<code>migrationEnd</code> <code>Date</code>	string (epoch timestamp)	Specifies when the map migration should end.	<code>mapMigration</code> Enabled is <code>true</code>

timeout

- **Property Manager name:** [Connect Timeout](#)
- **Behavior version:** The `v2025-05-30` 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
<code>value</code>	string (duration)	Specifies the timeout, for example <code>10s</code> .

uidConfiguration

- **Property Manager name:** [UID Configuration](#)
- **Behavior version:** The v2025-05-30 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.	
extractLocation	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
queryParameterName	string	This specifies the name of the query parameter from which to extract the UID value.	extractLocation is QUERY_STRING
variableName	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 v2025-05-30 rule format supports the validateEntityTag behavior v1.3.

- **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.

You can specify whether this behavior should support only strong `ETag` values, ignoring weak `ETag` and always returning a full response, or weak values should also be accepted. For more details, see the [RFC Standard](#).

Option	Type	Description
<code>enabled</code>	boolean	Enables the ETag validation behavior.
<code>nonStrictEnabled</code>	boolean	Whether you want to allow strong <code>ETag</code> values that are not surrounded by double quotes. Technically these are malformed and non-standard, but are commonly used.
<code>weakEnabled</code>	boolean	Whether you want to allow weak <code>ETag</code> values that start with <code>W/</code> .

verifyJsonWebToken

- **Property Manager name:** [JWT verification](#)
- **Behavior version:** The `v2025-05-30` 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
<code>extractLocation</code>	enum	Specify from where to extract the JWT value.	
	<code>CLIENT_REQUEST_HEADER</code>	The value is in a client request header.	
	<code>QUERY_STRING</code>	The value is in the request's query string.	
<code>headerName</code>	string	This specifies the name of the header from which to extract the JWT value.	<code>extractLocation</code> is <code>CLIENT_REQUEST_HEADER</code>
<code>queryParameterName</code>	string	This specifies the name of the query parameter from which to extract the JWT value.	<code>extractLocation</code> is <code>QUERY_STRING</code>

Option	Type	Description	Requires
<code>jwt</code>	string	An identifier for the JWT keys collection.	
<code>enableRS256</code>	boolean	Verifies JWTs signed with the RS256 algorithm. This signature helps ensure that the token hasn't been tampered with.	
<code>enableES256</code>	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 `v2025-05-30` 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
<code>extractLocation</code>	enum	Specifies where to get the JWT value from.	
	<code>CLIENT_REQUEST_HEADER</code>	From the client request header.	
	<code>QUERY_STRING</code>	From the query string.	
	<code>CLIENT_REQUEST_HEADER_AND_QUERY_STRING</code>	From both.	
<code>primaryLocation</code>	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.	<code>extractLocation</code> is <code>CLIENT_REQUEST_HEADER_AND_QUERY_STRING</code>
	<code>CLIENT_REQUEST_HEADER</code>	Get the JWT value from the request header.	
	<code>QUERY_STRING</code>	Get the JWT value from the query string.	

Option	Type	Description	Requires
<code>customHeader</code>	boolean	The JWT value comes from the <code>X-Akamai-DCP-Token</code> header by default. Enabling this option allows you to extract it from another header name that you specify.	<code>extractLocation</code> is either: <code>CLIENT_REQUEST_HEADER</code> , <code>CLIENT_REQUEST_HEADER_AND_QUERY_STRING</code>
<code>headerName</code>	string	This specifies the name of the header to extract the JWT value from.	<code>customHeader</code> is <code>true</code>
<code>queryParameterName</code>	string	Specifies the name of the query parameter from which to extract the JWT value.	<code>extractLocation</code> is either: <code>QUERY_STRING</code> , <code>CLIENT_REQUEST_HEADER_AND_QUERY_STRING</code>
<code>jwt</code>	string	An identifier for the JWT keys collection.	
<code>extractClientId</code>	boolean	Allows you to extract the client ID claim name stored in JWT.	
<code>clientId</code>	string	This specifies the claim name.	<code>extractClientId</code> is <code>true</code>
<code>extractAuthorizations</code>	boolean	Allows you to extract the authorization groups stored in the JWT.	
<code>authorizations</code>	string	This specifies the authorization group name.	<code>extractAuthorizations</code> is <code>true</code>
<code>extractUserName</code>	boolean	Allows you to extract the user name stored in the JWT.	
<code>userName</code>	string	This specifies the user name.	<code>extractUserName</code> is <code>true</code>
<code>enableRS256</code>	boolean	Verifies JWTs signed with the RS256 algorithm. This signature helps to ensure that the token hasn't been tampered with.	
<code>enableES256</code>	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 `v2025-05-30` 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
<code>useAdvanced</code>	boolean	If enabled, allows you to specify advanced options such as <code>algorithm</code> , <code>escapeHmacInputs</code> , <code>ignoreQueryString</code> , <code>transitionKey</code> , and <code>salt</code> .	
<code>location</code>	enum	Specifies where to find the token in the incoming request.	
		Supported values: <code>CLIENT_REQUEST_HEADER</code> <code>COOKIE</code> <code>QUERY_STRING</code>	
<code>locationId</code>	string	When <code>location</code> is <code>CLIENT_REQUEST_HEADER</code> , specifies the name of the incoming request's header where to find the token.	
<code>algorithm</code>	enum	Specifies the algorithm that generates the token. It needs to match the method chosen in the token generation code.	<code>useAdvanced</code> is <code>true</code>
		Supported values: <code>MD5</code> <code>SHA256</code> <code>SHA1</code>	
<code>escapeHmacInputs</code>	boolean	URL-escapes HMAC inputs passed in as query parameters.	<code>useAdvanced</code> is <code>true</code>
<code>ignoreQueryString</code>	boolean	Enabling this removes the query string from the URL used to form an encryption key.	<code>useAdvanced</code> is <code>true</code>
<code>key</code>	object array	The shared secret used to validate tokens, which needs to match the key used in the token generation code.	
<code>transitionKey</code>	object array	Specifies a transition key as a hex value.	<code>useAdvanced</code> is <code>true</code>
<code>salt</code>	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.	<code>useAdvanced</code> is <code>true</code>
<code>failureResponse</code>	boolean	When enabled, sends an HTTP error when an authentication test fails.	

visitorPrioritization

- **Property Manager name:** [Visitor Prioritization Cloudlet](#)
- **Behavior version:** The `v2025-05-30` 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](#)⁶. 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
<code>enabled</code>	boolean	Enables the Visitor Prioritization behavior.	
<code>cloudletPolicy</code>	object	Identifies the Cloudlet policy.	
<code>cloudletPolicy.id</code>	number	Identifies the Cloudlet.	
<code>cloudletPolicy.name</code>	string	The Cloudlet's descriptive name.	
<code>userIdentificationByCookie</code>	boolean	When enabled, identifies users by the value of a cookie.	
<code>userIdentificationKeyCookie</code>	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.	<code>userIdentificationByCookie</code> is <code>true</code>
<code>userIdentificationByHeaders</code>	boolean	When enabled, identifies users by the values of GET or POST request headers.	
<code>userIdentificationKeyHeaders</code>	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.	<code>userIdentificationByHeaders</code> is <code>true</code>
<code>userIdentificationByIp</code>	boolean	Allows IP addresses to identify users.	
<code>userIdentificationByParams</code>	boolean	When enabled, identifies users by the values of GET or POST request parameters.	
<code>userIdentificationKeyParams</code>	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.	<code>userIdentificationByParams</code> is <code>true</code>
<code>allowedUserCookieEnabled</code>	boolean	Sets a cookie for users who have been allowed through to the site.	
<code>allowedUserCookieLabel</code>	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.	<code>allowedUserCookieEnabled</code> is <code>true</code>
<code>allowedUserCookieDuration</code>	number (0-600)	Sets the number of seconds for the allowed user's session once allowed through to the site.	<code>allowedUserCookieEnabled</code> is <code>true</code>
<code>allowedUserCookieRefresh</code>	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.	<code>allowedUserCookieEnabled</code> is <code>true</code>
<code>allowedUserCookieAdvanced</code>	boolean	Sets advanced configuration options for the allowed user's cookie.	<code>allowedUserCookieEnabled</code> is <code>true</code>
<code>allowedUserCookieAutomaticSalt</code>	boolean	Sets an automatic <i>salt</i> value to verify the integrity of the cookie for an allowed user. Disable this if you want to share the cookie across properties.	<code>allowedUserCookieEnabled</code> is <code>true</code> AND <code>allowedUserCookieAdvanced</code> is <code>true</code>
<code>allowedUserCookieSalt</code>	string	Specifies a fixed <i>salt</i> value, which is incorporated into the cookie's value to prevent users from manipulating it. You can use the same salt string across different behaviors or properties to apply a single cookie to all allowed users.	<code>allowedUserCookieEnabled</code> is <code>true</code> AND <code>allowedUserCookieAdvanced</code> is <code>true</code> AND <code>allowedUser</code>

Option	Type	Description	Requires
			CookieAutomaticSalt is false
allowedUserCookieDomainType	enum	Specify with allowedUserCookieAdvanced enabled.	allowedUserCookieEnabled is true AND allowedUserCookieAdvanced is true
	DYNAMIC	Use the dynamic incoming host header.	
	CUSTOMER	Use a customer-defined cookie domain.	
allowedUserCookieDomain	string	Specifies a domain for an allowed user cookie.	allowedUserCookieEnabled is true AND allowedUserCookieAdvanced is true AND allowedUserCookieDomainType is CUSTOMER
allowedUserCookieHttpOnly	boolean	Applies the HttpOnly flag to the allowed user's cookie to ensure it's accessed over HTTP and not manipulated by the client.	allowedUserCookieEnabled is true AND allowedUserCookieAdvanced is true
waitingRoomCookieEnabled	boolean	Enables a cookie to track a waiting room assignment.	
waitingRoomCookieShareLabel	boolean	Enabling this option shares the same allowedUserCookieLabel string. If disabled, specify a different waitingRoomCookieLabel.	waitingRoomCookieEnabled is true AND allowedUserCookieEnabled is true
waitingRoomCookieLabel	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.	waitingRoomCookieEnabled is true
waitingRoomCookieDuration	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.	waitingRoomCookieEnabled is true
waitingRoomCookieAdvanced	boolean	When enabled along with waitingRoomCookieEnabled, sets advanced configuration options for the waiting room cookie.	waitingRoomCookieEnabled is true
waitingRoomCookieAutomaticSalt	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.	waitingRoomCookieEnabled is true AND waitingRoomCookieAdvanced is true
waitingRoomCookieSalt	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.	waitingRoomCookieEnabled is true AND waitingRoomCookieAdvanced is true AND waitingRoomCookieAutomaticSalt is false

Option	Type	Description	Requires
<code>waitingRoomCookieDomainType</code>	enum	Specify with <code>waitingRoomCookieAdvanced</code> enabled, selects whether to use the <code>DYNAMIC</code> incoming host header, or a <code>CUSTOMER</code> -defined cookie domain.	<code>waitingRoomCookieEnabled</code> is <code>true</code> AND <code>waitingRoomCookieAdvanced</code> is <code>true</code>
	<code>DYNAMIC</code>	Use the dynamic incoming host header.	
	<code>CUSTOMER</code>	Use a customer-defined cookie domain.	
<code>waitingRoomCookieDomain</code>	string	Specifies a domain for the waiting room cookie.	<code>waitingRoomCookieEnabled</code> is <code>true</code> AND <code>waitingRoomCookieAdvanced</code> is <code>true</code> AND <code>waitingRoomCookieDomainType</code> is <code>CUSTOMER</code>
<code>waitingRoomCookieHttpOnly</code>	boolean	Applies the <code>HttpOnly</code> flag to the waiting room cookie to ensure it's accessed over HTTP and not manipulated by the client.	<code>waitingRoomCookieEnabled</code> is <code>true</code> AND <code>waitingRoomCookieAdvanced</code> is <code>true</code>
<code>waitingRoomStatusCode</code>	number	Specifies the response code for requests sent to the waiting room.	
<code>waitingRoomUseCpCode</code>	boolean	Allows you to assign a different CP code that tracks any requests that are sent to the waiting room.	
<code>waitingRoomCpCode</code>	object	Specifies a CP code for requests sent to the waiting room. You only need to provide the initial <code>id</code> , stripping any <code>cpc_</code> prefix to pass the integer to the rule tree. Additional CP code details may reflect back in subsequent read-only data.	<code>waitingRoomUseCpCode</code> is <code>true</code>
<code>waitingRoomCpCode.cpCodeLimits</code>	array	Read-only. Describes the current usage limit for the CP code.	
<code>waitingRoomCpCode.createdDate</code>	integer	Read-only. UNIX epoch timestamp reflecting when the CP code was originally created.	
<code>waitingRoomCpCode.description</code>	string	Read-only. Additional description for the CP code.	
<code>waitingRoomCpCode.id</code>	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 <code>cpcodeId</code> value from the List CP codes operation.	
<code>waitingRoomCpCode.name</code>	string	Read-only. The name of the CP code you specify as the <code>cpcodeName</code> 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.	
<code>waitingRoomCpCode.products</code>	array	Read-only. The set of products the CP code is assigned to. This reflects <code>productId</code> values you specify when creating a new CP code in PAPI.	
<code>waitingRoomNetStorage</code>	object	Specifies the NetStorage domain for the waiting room page.	
<code>waitingRoomNetStorage.cpCode</code>	integer	Identifies a CP code assigned to this storage group.	
<code>waitingRoomNetStorage.downloadDomain</code>	string	Domain name from which content can be downloaded.	

Option	Type	Description	Requires
Name			
<code>waitingRoomNetStorage.g2oToken</code>	string	Signature Header Authentication key.	
<code>waitingRoomNetStorage.id</code>	integer	Unique identifier for the storage group.	
<code>waitingRoomNetStorage.name</code>	string	Name of the storage group.	
<code>waitingRoomDirectory</code>	string (allows variables)	Specifies the NetStorage directory that contains the static waiting room page, with no trailing slash character.	
<code>waitingRoomCacheTtl</code>	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 `v2025-05-30` 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
<code>enable</code>	boolean	Enables the watermarking behavior.	
<code>signatureVerificationEnable</code>	boolean	When enabled, you can verify the signature in your watermarking token.	
<code>verificationKeyId</code>	string	Specifies a unique identifier for the first public key.	<code>signatureVerificationEnable</code> is <code>true</code>
<code>verificationPublicKey1</code>	string	Specifies the first public key in its entirety.	<code>signatureVerificationEnable</code> is <code>true</code>

Option	Type	Description	Requires
<code>verificationKeyId2</code>	string	Specifies a unique identifier for the optional second public key.	<code>signatureVerificationEnable</code> is true
<code>verificationPublicKey2</code>	string	Specifies the optional second public key in its entirety. Specify a second key to enable rotation.	<code>signatureVerificationEnable</code> is true
<code>patternDecryptionEnable</code>	boolean	If patterns in your watermarking tokens have been encrypted, enabling this allows you to provide values to decrypt them.	
<code>decryptionPasswordId1</code>	string	Specifies a label that corresponds to the primary password.	<code>patternDecryptionEnable</code> is true
<code>decryptionPassword1</code>	string	Provides the primary password used to encrypt patterns in your watermarking tokens.	<code>patternDecryptionEnable</code> is true
<code>decryptionPasswordId2</code>	string	Specifies a label for the secondary password, used in rotation scenarios to identify which password to use for decryption.	<code>patternDecryptionEnable</code> is true
<code>decryptionPassword2</code>	string	Provides the secondary password you can use to rotate passwords.	<code>patternDecryptionEnable</code> is true
<code>useOriginalAsA</code>	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 <i>filename-prefix AB naming</i> preprocessing method, the watermarking vendor creates two variants of the original segment content and labels them as an <code>A</code> and <code>B</code> segment in the filename. If you selected the <i>unlabeled A variant</i> preprocessing method, enabling this option tells your configuration to use the original filename segment content as your <code>A</code> variant.	
<code>abVariantLocation</code>	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 <code>A</code> and <code>B</code> variant segments.	
	<code>FILENAME_PREFIX</code>	Set for the standard, <i>filename-prefix AB naming</i> preprocessing method, where the variant letter is included in the filename.	
	<code>PARENT_DIRECTORY_PREFIX</code>	Set for the <i>directory-prefix AB naming</i> preprocessing method, where variants are located in a subdirectory named after the variants, such as <code>/B/segment1.ts</code> .	

webApplicationFirewall

- **Property Manager name:** [Web Application Firewall \(WAF\)](#)
- **Behavior version:** The `v2025-05-30` 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
<code>firewallConfiguration</code>	object	An object featuring details about your firewall configuration.

webSockets

- **Property Manager name:** [WebSockets](#)
- **Behavior version:** The `v2025-05-30` 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
<code>enabled</code>	boolean	Enables WebSocket traffic.

webdav

- **Property Manager name:** [WebDAV](#)
- **Behavior version:** The `v2025-05-30` 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
<code>enabled</code>	boolean	Enables the WebDAV behavior.

v2025-05-30 criteria

v2025-05-30 criteria

This section provides details for all criteria the Property Manager API supports for the `v2025-05-30` rule format version. The set available to you depends on the product and modules assigned to the property or the include. You can get it by running either [List available criteria for a property](#) or [List available criteria for an include](#).

This `v2025-05-30` rule format is an older deprecated snapshot set of PAPI features. To take advantage of fresh improvements and new features that get released on a regular basis, you should consider using the `latest` rule format. See [Dynamic rule updates](#) 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 `v2025-05-30` 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
<code>matchOperator</code>	enum	Specifies the match's logic.
	<code>IS</code>	Matches the selected requests.
	<code>IS_NOT</code>	Does not match the selected requests.
<code>matchOn</code>	enum	Specifies the match's scope.
	<code>ANY_IM</code>	Whether to match any requests that also include generated derivatives.
	<code>PRISTINE</code>	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 `v2025-05-30` 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
<code>percentage</code>	number (0-100)	Specifies the percentage of requests to match.

cacheability

- **Property Manager name:** [Response Cacheability](#)
- **Criteria version:** The `v2025-05-30` 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' `cacheing` instructions, in which case this criteria does not apply.

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

chinaCdnRegion

- **Property Manager name:** [ChinaCDN Region](#)
- **Criteria version:** The `v2025-05-30` 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
<code>matchOperator</code>	enum	Specify whether the request <code>IS</code> or <code>IS_NOT</code> deployed over ChinaCDN.
	<code>IS</code>	The request is deployed over ChinaCDN.
	<code>IS_NOT</code>	The request is not deployed over ChinaCDN.

clientCertificate

- **Property Manager name:** [Client certificate](#)
- **Criteria version:** The `v2025-05-30` rule format supports the `clientCertificate` criteria v1.2.
- **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
<code>isCertificatePresent</code>	boolean	Executes rule behaviors only if a client certificate authenticates requests.	
<code>isCertificateValid</code>	enum	Matches whether the certificate is <code>VALID</code> or <code>INVALID</code> . You can also <code>IGNORE</code> the certificate's validity.	<code>isCertificatePresent</code> is <code>true</code>
	<code>VALID</code>	Match when the certificate is valid.	
	<code>INVALID</code>	Match when the certificate is invalid.	
	<code>IGNORE</code>	Ignores the certificate's is valid.	
<code>enforceMtls</code>	boolean	Specifies custom handling of requests if any of the checks in the enforceMtlsSettings behavior fail. Enable this and use with behaviors such as logCustom so that they execute if the check fails. You need to add the enforceMtlsSettings behavior to a parent rule, with its own unique match condition and <code>enableDenyRequest</code> option disabled.	

clientIp

- **Property Manager name:** [Client IP](#)
- **Criteria version:** The `v2025-05-30` 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
<code>match</code> <code>Operator</code>	enum	Matches the contents of <code>values</code> if set to <code>IS_ONE_OF</code> , otherwise <code>IS_NOT_ONE_OF</code> reverses the match.
	<code>IS_ONE_OF</code>	Matches any of the specified <code>values</code> .
	<code>IS_NOT_ONE_OF</code>	Does not match any of the specified <code>values</code> .
<code>values</code>	string array	IP or CIDR block, for example: <code>71.92.0.0/14</code> .
<code>useHeaders</code>	boolean	When connecting via a proxy server as determined by the <code>X-Forwarded-For</code> 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 `v2025-05-30` 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
<code>value</code>	enum	The IP version of the client request, either <code>IPV4</code> or <code>IPV6</code> .
	<code>IPV4</code>	Matches the IPv4 protocol.
	<code>IPV6</code>	Matches the IPv6 protocol.
<code>useXForwardedFor</code> <code>For</code>	boolean	When connecting via a proxy server as determined by the <code>X-Forwarded-For</code> 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 `v2025-05-30` 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
<code>originId</code>	string	The Cloudlets Origins identifier, limited to alphanumeric and underscore characters.

contentDeliveryNetwork

- **Property Manager name:** [CDN Network](#)
- **Criteria version:** The `v2025-05-30` 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
<code>matchOperator</code>	enum	Matches the specified <code>network</code> if set to <code>IS</code> , otherwise <code>IS_NOT</code> reverses the match.
	<code>IS</code>	Matches the specified <code>network</code> .

Option	Type	Description
	IS_NOT	Does not match the specified <code>network</code> .
<code>network</code>	enum	Match the network.
	STAGING	Match the staging network.
	PRODUCTION	Match the production network.

contentType

- **Property Manager name:** [Content Type](#)
- **Criteria version:** The `v2025-05-30` 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
<code>matchOperator</code>	enum	Matches any <code>Content-Type</code> among specified <code>values</code> when set to <code>IS_ONE_OF</code> , otherwise <code>IS_NOT_ONE_OF</code> reverses the match.
	<code>IS_ONE_OF</code>	Matches any <code>Content-Type</code> among the specified <code>values</code> .
	<code>IS_NOT_ONE_OF</code>	Matches none of the specified <code>values</code> .
<code>values</code>	string array	<code>Content-Type</code> response header value, for example <code>text/html</code> .
<code>matchWildcard</code>	boolean	Allows wildcards in the <code>value</code> field, where <code>?</code> matches a single character and <code>*</code> matches zero or more characters. Specifying <code>text/*</code> matches both <code>text/html</code> and <code>text/css</code> .
<code>matchCase Sensitive</code>	boolean	Sets a case-sensitive match for all <code>values</code> .

debugMode

- **Property Manager name:** [Debug_Mode](#)
- **Criteria version:** The `v2025-05-30` rule format supports the `debugMode` criteria v1.0.
- **Rule format status:** [Deprecated, outdated rule format](#)
- **Access:** [Read-only](#)
- **Allowed in includes:** [Yes](#)

The match applies when the request is debugged using the `enhancedDebug` behavior.

Option	Type	Description
<code>debugMode</code>	boolean	Whether the request is being debugged using Enhanced Debug.

deviceCharacteristic

- **Property Manager name:** [Device Characteristics](#)
- **Criteria version:** The `v2025-05-30` rule format supports the `deviceCharacteristic` criteria v1.3.
- **Rule format status:** [Deprecated, outdated rule format](#)
- **Access:** [Read/Write](#)
- **Allowed in includes:** [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
<code>characteristic</code>	enum	Aspect of the device or browser to match.	
	<code>BRAND_NAME</code>	String value such as <code>Samsung</code> or <code>Apple</code> .	
	<code>MODEL_NAME</code>	String value such as <code>SCH-I110</code> .	

Option	Type	Description	Requires
	MARKETING_NAME	String value such as <code>Samsung Illusion</code> .	
	IS_WIRELESS_DEVICE	Boolean value.	
	IS_TABLET	Boolean value, subset of <code>IS_MOBILE</code> .	
	DEVICE_OS	String value.	
	DEVICE_OS_VERSION	Version string value.	
	MOBILE_BROWSER	String value.	
	MOBILE_BROWSER_VERSION	Version string value.	
	RESOLUTION_WIDTH	Number of pixels wide.	
	RESOLUTION_HEIGHT	Number of pixels high.	
	PHYSICAL_SCREEN_HEIGHT	Number of millimeters high.	
	PHYSICAL_SCREEN_WIDTH	Number of millimeters wide.	
	COOKIE_SUPPORT	Boolean value.	
	AJAX_SUPPORT_JAVASCRIPT	Boolean value.	
	FULL_FLASH_SUPPORT	Boolean value.	
	ACCEPT_THIRD_PARTY_COOKIE	Boolean value.	
	XHTML_SUPPORT_LEVEL	Numeric value.	
	IS_MOBILE	Boolean value.	
<code>stringMatch</code> Operator	enum	When the <code>characteristic</code> expects a string value, set this to <code>MATCHES_ONE_OF</code> to match against the <code>stringValue</code> set, otherwise set to <code>DOES_NOT_MATCH_ONE_OF</code> to exclude that set of values.	<code>characteristic</code> is either: <code>BRAND_NAME</code> , <code>MODEL_NAME</code> , <code>MARKETING_NAME</code> , <code>DEVICE_OS</code> , <code>MOBILE_BROWSER</code> , <code>PREFERRED_MARKUP</code> , <code>HTML_PREFERRED_DTD</code> , <code>XHTML_PREFERRED_CHARSET</code> , <code>VIEWPORT_WIDTH</code> , <code>XHTMLMP_PREFERRED_MIME_TYPE</code> , <code>AJAX_PREFERRED_GEOLOC_API</code> , <code>XHTML_FILE_UPLOAD</code> , <code>XHTML_SUPPORTS_IFRAME</code> , <code>FLASH_LITE_VERSION</code>
	MATCHES_ONE_OF	The value is included as a <code>stringValue</code> .	

Option	Type	Description	Requires
	DOES_NOT_MATCH_ONE_OF	The value is not included as a <code>string</code> Value .	
<code>numericMatch</code> Operator	enum	When the <code>characteristic</code> expects a numeric value, compares the specified <code>numericValue</code> against the matched client.	<code>characteristic</code> is either: <code>RESOLUTION_WIDTH</code> , <code>RESOLUTION_HEIGHT</code> , <code>PHYSICAL_SCREEN_HEIGHT</code> , <code>PHYSICAL_SCREEN_WIDTH</code> , <code>XHTML_SUPPORT_LEVEL</code> , <code>MAX_IMAGE_WIDTH</code> , <code>MAX_IMAGE_HEIGHT</code> , <code>VIEWPORT_INITIAL_SCALE</code>
	IS	Values are equal.	
	IS_NOT	Values are not equal.	
	IS_LESS_THAN	The <code>numericValue</code> is less than the matched client.	
	IS_LESS_THAN_OR_EQUAL	The <code>numericValue</code> is less than or equal to the matched client.	
	IS_MORE_THAN	The <code>numericValue</code> is more than the matched client.	
	IS_MORE_THAN_OR_EQUAL	The <code>numericValue</code> is more than or equal to the matched client.	
<code>versionMatch</code> Operator	enum	When the <code>characteristic</code> expects a version string value, compares the specified <code>versionValue</code> against the matched client, using the following operators: <code>IS</code> , <code>IS_MORE_THAN_OR_EQUAL</code> , <code>IS_MORE_THAN</code> , <code>IS_LESS_THAN_OR_EQUAL</code> , <code>IS_LESS_THAN</code> , <code>IS_NOT</code> .	<code>characteristic</code> is either: <code>DEVICE_OS_VERSION</code> , <code>MOBILE_BROWSER_VERSION</code>
	IS	The <code>versionValue</code> equals the matched client.	
	IS_NOT	The <code>versionValue</code> does not equal the matched client.	
	IS_LESS_THAN	The <code>versionValue</code> is less than the matched client.	
	IS_LESS_THAN_OR_EQUAL	The <code>versionValue</code> is less than or equal to the matched client.	
	IS_MORE_THAN	The <code>versionValue</code> is more than the matched client.	
	IS_MORE_THAN_OR_EQUAL	The <code>versionValue</code> is more than or equal to the matched client.	
<code>booleanValue</code>	boolean	When the <code>characteristic</code> expects a boolean value, this specifies the value.	<code>characteristic</code> is either: <code>IS_WIRELESS_DEVICE</code> , <code>IS_TABLET</code> , <code>COOKIE_SUPPORT</code> , <code>AJAX_SUPPORT</code> , <code>JAVASCRIPT</code> , <code>FULL_FLASH_SUPPRT</code> , <code>DUAL_ORIENTATION</code> , <code>ACCEPT_THIRD_PARTY_COOKIE</code> , <code>GIF_ANIMATED</code> , <code>JPG</code> , <code>PNG</code> , <code>XHTML_SUPPORTS_TABLE_FOR_LAYOUT</code> , <code>XHTML_TABLE_SUPPORT</code> , <code>PDF_SUPPORT</code> , <code>IS_MOBILE</code>
<code>stringValue</code>	string array	When the <code>characteristic</code> expects a string, this specifies the set of values.	<code>stringMatchOperator</code> is either: <code>MATCHES_ONE_OF</code> , <code>DOES_NOT_MATCH_ONE_OF</code>

Option	Type	Description	Requires
<code>numericValue</code>	number	When the <code>characteristic</code> expects a numeric value, this specifies the number.	<code>numericMatchOperator</code> is either: <code>IS</code> , <code>IS_NOT</code> , <code>IS_LESS_THAN</code> , <code>IS_LESS_THAN_OR_EQUAL</code> , <code>IS_MORE_THAN</code> , <code>IS_MORE_THAN_OR_EQUAL</code>
<code>versionValue</code>	string	When the <code>characteristic</code> expects a version number, this specifies it as a string.	<code>versionMatchOperator</code> is either: <code>IS</code> , <code>IS_NOT</code> , <code>IS_LESS_THAN</code> , <code>IS_LESS_THAN_OR_EQUAL</code> , <code>IS_MORE_THAN</code> , <code>IS_MORE_THAN_OR_EQUAL</code>
<code>matchCaseSensitive</code>	boolean	Sets a case-sensitive match for the <code>stringValue</code> field.	<code>stringMatchOperator</code> is either: <code>MATCHES_ONE_OF</code> , <code>DOES_NOT_MATCH_ONE_OF</code>
<code>matchWildcard</code>	boolean	Allows wildcards in the <code>stringValue</code> field, where <code>?</code> matches a single character and <code>*</code> matches zero or more characters.	<code>stringMatchOperator</code> is either: <code>MATCHES_ONE_OF</code> , <code>DOES_NOT_MATCH_ONE_OF</code>

edgeWorkersFailure

- **Property Manager name:** [EdgeWorkers Execution Status](#)
- **Criteria version:** The `v2025-05-30` rule format supports the `edgeWorkersFailure` criteria v1.2.
- **Rule format status:** [Deprecated, outdated rule format](#)
- **Access:** [Read/Write](#)
- **Allowed in includes:** [Yes](#)

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

Option	Type	Description
<code>execStatus</code>	enum	Specify execution status.
	<code>FAILURE</code>	Execution failed.
	<code>SUCCESS</code>	Execution succeeded.

fileExtension

- **Property Manager name:** [File Extension](#)
- **Criteria version:** The `v2025-05-30` rule format supports the `fileExtension` criteria v1.1.
- **Rule format status:** [Deprecated, outdated rule format](#)
- **Access:** [Read/Write](#)
- **Allowed in includes:** [Yes](#)

Matches the requested filename's extension, if present.

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

filename

- **Property Manager name:** [Filename](#)
- **Criteria version:** The `v2025-05-30` 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
<code>match Operator</code>	enum	If set to <code>IS_ONE_OF</code> or <code>IS_NOT_ONE_OF</code> , matches whether the filename matches one of the <code>values</code> . If set to <code>IS_EMPTY</code> or <code>IS_NOT_EMPTY</code> , matches whether the specified filename is part of the path.	
	<code>IS_ONE_OF</code>	The filename matches one of the <code>values</code> .	

Option	Type	Description	Requires
	IS_NOT_ONE_OF	The filename does not match one of the <code>values</code> .	
	IS_EMPTY	The filename is not part of the path.	
	IS_NOT_EMPTY	The filename is part of the path.	
<code>values</code>	string array	Matches the filename component of the request URL. Allows wildcards, where <code>?</code> matches a single character and <code>*</code> matches zero or more characters. For example, specify <code>filename.*</code> to accept any extension.	<code>matchOperator</code> is either: <code>IS_ONE_OF</code> , <code>IS_NOT_ONE_OF</code>
<code>matchCase Sensitive</code>	boolean	Sets a case-sensitive match for the <code>values</code> field.	<code>matchOperator</code> is either: <code>IS_ONE_OF</code> , <code>IS_NOT_ONE_OF</code>

hostname

- **Property Manager name:** [Hostname](#)
- **Criteria version:** The `v2025-05-30` 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
<code>match Operator</code>	enum	Matches the contents of <code>values</code> when set to <code>IS_ONE_OF</code> , otherwise <code>IS_NOT_ONE_OF</code> reverses the match.
	IS_ONE_OF	Matches the contents of <code>values</code> .
	IS_NOT_ONE_OF	Does not matche the contents of <code>values</code> .
<code>values</code>	string array	A list of hostnames. Allows wildcards, where <code>?</code> matches a single character and <code>*</code> matches zero or more characters. Specifying <code>*.example.com</code> matches both <code>m.example.com</code> and <code>www.example.com</code> .

matchAdvanced

- **Property Manager name:** [Advanced Match](#)
- **Criteria version:** The `v2025-05-30` 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
<code>description</code>	string	A human-readable description of what the XML block does.
<code>openXml</code>	string	An XML string that opens the relevant block.
<code>closeXml</code>	string	An XML string that closes the relevant block.

matchCpCode

- **Property Manager name:** [Content Provider Code](#)
- **Criteria version:** The `v2025-05-30` 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
<code>value</code>	object	Specifies the CP code as an object. You only need to provide the initial <code>id</code> to match the CP code, stripping any <code>cp_code_prefix</code> to pass the integer to the rule tree. Additional CP code details may reflect back in subsequent read-only data.

Option	Type	Description
<code>value.cpCodeLimits</code>	array	Read-only. Describes the current usage limit for the CP code.
<code>value.createdDate</code>	integer	Read-only. UNIX epoch timestamp reflecting when the CP code was originally created.
<code>value.description</code>	string	Read-only. Additional description for the CP code.
<code>value.id</code>	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 <code>cpcodeId</code> value from the List CP codes operation.
<code>value.name</code>	string	Read-only. The name of the CP code you specify as the <code>cpcodeName</code> 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.
<code>value.products</code>	array	Read-only. The set of products the CP code is assigned to. This reflects <code>productId</code> values you specify when creating a new CP code in PAPI.

matchResponseCode

- **Property Manager name:** [Response Status Code](#)
- **Criteria version:** The `v2025-05-30` 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
<code>matchOperator</code>	enum	Matches numeric range or a specified set of <code>values</code> .	
	<code>IS_ONE_OF</code>	Matches the contents of <code>values</code> .	
	<code>IS_NOT_ONE_OF</code>	Does not match the contents of <code>values</code> .	
	<code>IS_BETWEEN</code>	Matches the numeric range between <code>lowerBound</code> and <code>upperBound</code> .	
	<code>IS_NOT_BETWEEN</code>	Does not match the numeric range between <code>lowerBound</code> and <code>upperBound</code> .	
<code>values</code>	string array	A set of response codes to match, for example <code>["404","500"]</code> .	<code>matchOperator</code> is either: <code>IS_ONE_OF</code> , <code>IS_NOT_ONE_OF</code>
<code>lowerBound</code>	number	Specifies the start of a range of responses. For example, <code>400</code> to match anything from <code>400</code> to <code>500</code> .	<code>matchOperator</code> is either: <code>IS_BETWEEN</code> , <code>IS_NOT_BETWEEN</code>

Option	Type	Description	Requires
upperBound	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 v2025-05-30 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 variable Values .	
	IS_NOT_ONE_OF	Does not match any of an array of string variableValues .	
	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 upper Bound values.	
	IS_NOT_BETWEEN	Is outside the numeric lowerBound and upper Bound range.	
	IS_GREATER_THAN	Is greater than the variableExpression string-formatted number.	

Option	Type	Description	Requires
	IS_GREATER_THAN_OR_EQUAL_TO	Is greater than or equal to the <code>variableExpression</code> string-formatted number.	
	IS_LESS_THAN	Is less than the <code>variableExpression</code> string-formatted number.	
	IS_LESS_THAN_OR_EQUAL_TO	Is less than or equal to the <code>variableExpression</code> string-formatted number.	
<code>variableValues</code>	string array	Specifies an array of matching strings.	<code>matchOperator</code> is either: <code>IS_ONE_OF</code> , <code>IS_NOT_ONE_OF</code>
<code>variableExpression</code>	string (allows variables)	Specifies a single matching string.	<code>matchOperator</code> is either: <code>IS</code> , <code>IS_NOT</code> , <code>IS_GREATER_THAN</code> , <code>IS_GREATER_THAN_OR_EQUAL_TO</code> , <code>IS_LESS_THAN</code> , <code>IS_LESS_THAN_OR_EQUAL_TO</code>
<code>lowerBound</code>	string	Specifies the range's numeric minimum value.	<code>matchOperator</code> is either: <code>IS_BETWEEN</code> , <code>IS_NOT_BETWEEN</code>
<code>upperBound</code>	string	Specifies the range's numeric maximum value.	<code>matchOperator</code> is either: <code>IS_BETWEEN</code> , <code>IS_NOT_BETWEEN</code>
<code>matchWildcard</code>	boolean	When matching string expressions, enabling this allows wildcards, where <code>?</code> matches a single character and <code>*</code> matches zero or more characters.	<code>matchOperator</code> is either: <code>IS</code> , <code>IS_NOT</code> , <code>IS_ONE_OF</code> , <code>IS_NOT_ONE_OF</code>
<code>matchCaseSensitive</code>	boolean	When matching string expressions, enabling this performs a case-sensitive match.	<code>matchOperator</code> is either: <code>IS</code> , <code>IS_NOT</code> , <code>IS_ONE_OF</code> , <code>IS_NOT_ONE_OF</code>

metadataStage

- **Property Manager name:** [Metadata Stage](#)
- **Criteria version:** The `v2025-05-30` 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
<code>match</code> Operator	enum	Compares the current rule with the specified metadata stage.
	<code>IS</code>	The current rule is at the specified metadata stage.
	<code>IS_NOT</code>	The current rule is not at the specified metadata stage.
<code>value</code>	enum	Specifies the metadata stage.
	<code>cache-hit</code>	Content is cacheable and is already cached, but not yet tested for freshness.
	<code>client-done</code>	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.
	<code>client-request</code>	When the Akamai server receives the request. Most processing happens in this stage, including determining the object's cacheability and cache key.
	<code>client-request-body</code>	Runs when the Akamai server inspects the contents of a request POST body, typically as a security check.
	<code>client-response</code>	Occurs after the full response has been returned from the forward server or retrieved from Akamai's cache, prior to constructing a response.
	<code>content-policy</code>	This stage determines whether any Cloudlets or security products are associated with the request. It gets ignored in requests for other products.
	<code>forward-request</code>	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.
	<code>forward-response</code>	After the forward server responds and all response headers have been read. Doesn't run for the content retrieved from Akamai's cache.
	<code>forward-start</code>	Immediately before the <code>forward-request</code> stage, while the Akamai server selects a forward server or persistent connection. Doesn't run for the content retrieved from Akamai's cache.
	<code>ipa-response</code>	Runs when a response is received from an intermediate processing agent (IPA) server, called at the end of the <code>client-request</code> stage.

originTimeout

- **Property Manager name:** [Origin Timeout](#)
- **Criteria version:** The `v2025-05-30` 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
<code>matchOperator</code>	enum	Specifies a single required <code>ORIGIN_TIMED_OUT</code> value.
	<code>ORIGIN_TIMED_OUT</code>	This is currently the only supported value.

path

- **Property Manager name:** [Path](#)
- **Criteria version:** The `v2025-05-30` 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
<code>matchOperator</code>	enum	Matches the contents of the <code>values</code> array.
	<code>MATCHES_ONE_OF</code>	Matches any of the <code>values</code> array.
	<code>DOES_NOT_MATCH_ONE_OF</code>	Matches none of the <code>values</code> array.
<code>values</code>	string array	Matches the URL path, excluding leading hostname and trailing query parameters. The path is relative to the server root, for example <code>/blog</code> . This field allows wildcards, where <code>?</code> matches a single character and <code>*</code> matches zero or more characters. For example, <code>/blog/*/2014</code> matches paths with two fixed segments and other varying segments between them.
<code>matchCaseSensitive</code>	boolean	Sets a case-sensitive match.
<code>normalize</code>	boolean	Transforms URLs before comparing them with the provided value. URLs are decoded, and any directory syntax such as <code>../..</code> or <code>//</code> 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 `v2025-05-30` 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
<code>parameterName</code>	string	The name of the query field, for example, <code>q</code> in <code>?q=string</code> .	
<code>matchOperator</code>	enum	Narrows the match criteria.	
	<code>IS_ONE_OF</code>	Tests whether the field's <code>value</code> string matches.	
	<code>IS_NOT_ONE_OF</code>	Tests whether the field's <code>value</code> string does not match.	
	<code>EXISTS</code>	Whether the query field's <code>parameterName</code> is present in the requesting URL.	
	<code>DOES_NOT_EXIST</code>	Whether the query field's <code>parameterName</code> is absent from the requesting URL.	
	<code>IS_LESS_THAN</code>	Matches a range when the <code>value</code> is numeric.	
	<code>IS_MORE_THAN</code>	Matches a range when the <code>value</code> is numeric.	
	<code>IS_BETWEEN</code>	Is between the numeric <code>lowerBound</code> and <code>upperBound</code> values.	
<code>values</code>	string array	The value of the query field, for example, <code>string</code> in <code>?q=string</code> .	<code>matchOperator</code> is either: <code>IS_ONE_OF</code> , <code>IS_NOT_ONE_OF</code>
<code>lowerBound</code>	number	Specifies the match's minimum value.	<code>matchOperator</code> is either: <code>IS_MORE_THAN</code> , <code>IS_BETWEEN</code>
<code>upperBound</code>	number	When the <code>value</code> is numeric, this field specifies the match's maximum value.	<code>matchOperator</code> is either: <code>IS_LESS_THAN</code> , <code>IS_BETWEEN</code>
<code>matchWildcardName</code>	boolean	Allows wildcards in the <code>parameterName</code> field, where <code>?</code> matches a single character and <code>*</code> matches zero or more characters.	
<code>matchCaseSensitiveName</code>	boolean	Sets a case-sensitive match for the <code>parameterName</code> field.	
<code>matchWildcardValue</code>	boolean	Allows wildcards in the <code>value</code> field, where <code>?</code> matches a single character and <code>*</code> matches zero or more characters.	<code>matchOperator</code> is either: <code>IS_ONE_OF</code> , <code>IS_NOT_ONE_OF</code>
<code>matchCaseSensitiveValue</code>	boolean	Sets a case-sensitive match for the <code>value</code> field.	<code>matchOperator</code> is either: <code>IS_ONE_OF</code> , <code>IS_NOT_ONE_OF</code>

Option	Type	Description	Requires
<code>escapeValue</code>	boolean	Matches when the <code>value</code> is URL-escaped.	<code>matchOperator</code> is either: <code>IS_ONE_OF</code> , <code>IS_NOT_ONE_OF</code>

random

- **Property Manager name:** [Sample Percentage](#)
- **Criteria version:** The `v2025-05-30` 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
<code>bucket</code>	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 `v2025-05-30` 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
<code>configName</code>	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 originFailureRecoveryPolicy behaviors. The value can contain alphanumeric characters and dashes.

regularExpression

- **Property Manager name:** [Regex](#)
- **Criteria version:** The `v2025-05-30` 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
<code>matchString</code>	string (allows variables)	The string to match, typically the contents of a dynamic variable.
<code>regex</code>	string	The regular expression (PCRE) to match against the string.
<code>caseSensitive</code>	boolean	Sets a case-sensitive regular expression match.

requestCookie

- **Property Manager name:** [Request Cookie](#)
- **Criteria version:** The `v2025-05-30` 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
<code>cookieName</code>	string (allows variables)	The name of the cookie, which can be a variable. For example, <code>visitor in visitor:anon</code> .	
<code>matchOperator</code>	enum	Narrows the match criteria.	
	<code>IS</code>	If the field's <code>value</code> string matches.	
	<code>IS_NOT</code>	If the field's <code>value</code> string does not match.	
	<code>EXISTS</code>	Matches if the <code>cookieName</code> cookie exists.	
	<code>DOES_NOT_EXIST</code>	Matches if the <code>cookieName</code> cookie does not exist.	
	<code>IS_BETWEEN</code>	Is between the numeric <code>lowerBound</code> and <code>upperBound</code> values.	
<code>value</code>	string (allows variables)	The cookie's value, which can be a variable. For example, <code>anon</code> in <code>visitor:anon</code> .	<code>matchOperator</code> is either: <code>IS</code> , <code>IS_NOT</code>
<code>lowerBound</code>	number	When the <code>value</code> is numeric, this field specifies the match's minimum value.	<code>matchOperator</code> is <code>IS_BETWEEN</code>
<code>upperBound</code>	number	When the <code>value</code> is numeric, this field specifies the match's maximum value.	<code>matchOperator</code> is <code>IS_BETWEEN</code>
<code>matchWildcardName</code>	boolean	Allows wildcards in the <code>cookieName</code> field, where <code>?</code> matches a single character and <code>*</code> matches zero or more characters.	
<code>matchCaseSensitiveName</code>	boolean	Sets a case-sensitive match for the <code>cookieName</code> field.	
<code>matchWildcardValue</code>	boolean	Allows wildcards in the <code>value</code> field, where <code>?</code> matches a single character and <code>*</code> matches zero or more characters.	<code>matchOperator</code> is either: <code>IS</code> , <code>IS_NOT</code>
<code>matchCaseSensitiveValue</code>	boolean	Sets a case-sensitive match for the <code>value</code> field.	<code>matchOperator</code> is either: <code>IS</code> , <code>IS_NOT</code>

requestHeader

- **Property Manager name:** [Request Header](#)
- **Criteria version:** The `v2025-05-30` 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
<code>headerName</code>	string	The name of the request header, for example <code>Accept-Language</code> .	
<code>matchOperator</code>	enum	Narrows the match criteria.	
	<code>IS_ONE_OF</code>	Tests whether the field's <code>value</code> string matches.	
	<code>IS_NOT_ONE_OF</code>	Tests whether the field's <code>value</code> string does not match.	
	<code>EXISTS</code>	Tests if the <code>headerName</code> field exists.	
	<code>DOES_NOT_EXIST</code>	Tests if the <code>headerName</code> field is absent.	
<code>values</code>	string array	The request header's value, for example <code>en-US</code> when the header <code>headerName</code> is <code>Accept-Language</code> .	<code>matchOperator</code> is either: <code>IS_ONE_OF</code> , <code>IS_NOT_ONE_OF</code>
<code>matchWildcardName</code>	boolean	Allows wildcards in the <code>headerName</code> field, where <code>?</code> matches a single character and <code>*</code> matches zero or more characters.	
<code>matchWildcardValue</code>	boolean	Allows wildcards in the <code>value</code> field, where <code>?</code> matches a single character and <code>*</code> matches zero or more characters.	<code>matchOperator</code> is either: <code>IS_ONE_OF</code> , <code>IS_NOT_ONE_OF</code>
<code>matchCaseSensitiveValue</code>	boolean	Sets a case-sensitive match for the <code>value</code> field.	<code>matchOperator</code> is either: <code>IS_ONE_OF</code> , <code>IS_NOT_ONE_OF</code>

requestMethod

- **Property Manager name:** [Request Method](#)
- **Criteria version:** The `v2025-05-30` 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
<code>matchOperator</code>	enum	Matches the <code>value</code> when set to <code>IS</code> , otherwise <code>IS_NOT</code> reverses the match.
	<code>IS</code>	Matches the <code>value</code> .
	<code>IS_NOT</code>	Does not match the <code>value</code> .

Option	Type	Description
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 v2025-05-30 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 v2025-05-30 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 .

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

responseHeader

- **Property Manager name:** [Response Header](#)
- **Criteria version:** The `v2025-05-30` 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
<code>headerName</code>	string	The name of the response header, for example <code>Content-Type</code> .	
<code>matchOperator</code>	enum	Narrows the match according to various criteria.	
	<code>IS_ONE_OF</code>	The field's <code>value</code> string matches.	
	<code>IS_NOT_ONE_OF</code>	The field's <code>value</code> string does not match.	
	<code>EXISTS</code>	The HTTP field <code>headerName</code> is present.	
	<code>DOES_NOT_EXIST</code>	The HTTP field <code>headerName</code> is absent.	
	<code>IS_LESS_THAN</code>	Matches ranges when the <code>value</code> is numeric.	
	<code>IS_MORE_THAN</code>	Matches ranges when the <code>value</code> is numeric.	
	<code>IS_BETWEEN</code>	Is between the numeric <code>lowerBound</code> and <code>upperBound</code> values.	

Option	Type	Description	Requires
values	string array	The response header's value, for example <code>application/x-www-form-urlencoded</code> when the header <code>headerName</code> is <code>Content-Type</code> .	<code>matchOperator</code> is either: <code>IS_ONE_OF</code> , <code>IS_NOT_ONE_OF</code>
lowerBound	number	When the <code>value</code> is numeric, this field specifies the match's minimum value.	<code>matchOperator</code> is either: <code>IS_MORE_THAN</code> , <code>IS_BETWEEN</code>
upperBound	number	When the <code>value</code> is numeric, this field specifies the match's maximum value.	<code>matchOperator</code> is either: <code>IS_LESS_THAN</code> , <code>IS_BETWEEN</code>
matchWildcardName	boolean	Allows wildcards in the <code>headerName</code> field, where <code>?</code> matches a single character and <code>*</code> matches zero or more characters.	
matchWildcardValue	boolean	Allows wildcards in the <code>value</code> field, where <code>?</code> matches a single character and <code>*</code> matches zero or more characters.	<code>matchOperator</code> is either: <code>IS_ONE_OF</code> , <code>IS_NOT_ONE_OF</code>
matchCaseSensitiveValue	boolean	When enabled, the match is case-sensitive for the <code>value</code> field.	<code>matchOperator</code> is either: <code>IS_ONE_OF</code> , <code>IS_NOT_ONE_OF</code>

serverLocation

- **Property Manager name:** [Akamai Server Location](#)
- **Criteria version:** The `v2025-05-30` 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
locationType	enum	Indicates the geographic scope.	
	COUNTRY	Country.	
	CONTINENT	Continent.	
	REGION	States or provinces within a country.	
matchOperator	enum	Matches the specified set of values when set to <code>IS_ONE_OF</code> , otherwise <code>IS_NOT_ONE_OF</code> reverses the match.	
	IS_ONE_OF	Matches any of the specified <code>values</code> .	
	IS_NOT_ONE_OF	Does not match any of the specified <code>values</code> .	
countries	string array	ISO 3166-1 country codes, such as <code>US</code> or <code>CN</code> .	<code>locationType</code> is <code>COUNTRY</code>

Option	Type	Description	Requires
<code>continents</code>	string array	Continent codes.	<code>locationType</code> is <code>CONTINENT</code>
	<code>AF</code>	Africa.	
	<code>AS</code>	Asia.	
	<code>EU</code>	Europe.	
	<code>NA</code>	North America.	
	<code>OC</code>	Oceania.	
	<code>OT</code>	Antarctica.	
	<code>SA</code>	South America.	
<code>regions</code>	string array	ISO 3166 country and region codes, for example <code>US:MA</code> for Massachusetts or <code>JP:13</code> for Tokyo.	<code>locationType</code> is <code>REGION</code>

time

- **Property Manager name:** [Time Interval](#)
- **Criteria version:** The `v2025-05-30` 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
<code>matchOperator</code>	enum	Specifies how to define the range of time.	
	<code>BEGINNING</code>	The duration is indefinite, using the value of <code>beginDate</code> .	
	<code>BETWEEN</code>	Sets a single range between two dates, using the values of <code>beginDate</code> and <code>endDate</code> .	
	<code>LASTING</code>	Sets a single range, but based on duration relative to the starting time. It relies on the values of <code>lastingDate</code> and <code>lastingDuration</code> .	
	<code>REPEATING</code>	Allows a <code>LASTING</code> -style range to repeat at regular intervals. It relies on the values of <code>repeatBeginDate</code> , <code>repeatDuration</code> , and <code>repeatInterval</code> .	
<code>repeatInterval</code>	string (duration)	Sets the time between each repeating time period's starting points.	<code>matchOperator</code> is <code>REPEATING</code>

Option	Type	Description	Requires
<code>repeatDuration</code>	string (duration)	Sets the duration of each repeating time period.	<code>matchOperator</code> is <code>REPEATING</code>
<code>lastingDuration</code>	string (duration)	Specifies the end of a time period as a duration relative to the <code>lastingDate</code> .	<code>matchOperator</code> is <code>LASTING</code>
<code>lastingDate</code>	string (timestamp)	Sets the start of a fixed time period.	<code>matchOperator</code> is <code>LASTING</code>
<code>repeatBeginDate</code>	string (timestamp)	Sets the start of the initial time period.	<code>matchOperator</code> is <code>REPEATING</code>
<code>applyDaylightSavingsTime</code>	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.	<code>matchOperator</code> is <code>REPEATING</code>
<code>beginDate</code>	string (timestamp)	Sets the start of a time period.	<code>matchOperator</code> is <code>BEGINNING</code> OR <code>matchOperator</code> is <code>BETWEEN</code>
<code>endDate</code>	string (timestamp)	Sets the end of a fixed time period.	<code>matchOperator</code> is <code>BETWEEN</code>

tokenAuthorization

- **Property Manager name:** [Token Verification Result](#)
- **Criteria version:** The `v2025-05-30` 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
<code>matchOperator</code>	enum	Error match scope.	
	<code>IS_SUCCESS</code>	No errors occurred.	
	<code>IS_CUSTOM_FAILURE</code>	Match any error in <code>statusList</code> .	
	<code>IS_ANY_FAILURE</code>	Any error occurred.	

userAgent

- **Property Manager name:** [User Agent](#)
- **Criteria version:** The `v2025-05-30` 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
<code>match</code> Operator	enum	Matches the specified set of <code>values</code> when set to <code>IS_ONE_OF</code> , otherwise <code>IS_NOT_ONE_OF</code> reverses the match.
	<code>IS_ONE_OF</code>	Matches any of the specified <code>values</code> .
	<code>IS_NOT_ONE_OF</code>	Does not match any of the specified <code>values</code> .
<code>values</code>	string array	The <code>User-Agent</code> header's value. For example, <code>Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)</code> .
<code>match</code> Wildcard	boolean	Allows wildcards in the <code>value</code> field, where <code>?</code> matches a single character and <code>*</code> matches zero or more characters. For example, <code>*Android*</code> , <code>*iPhone5*</code> , <code>*Firefox*</code> , or <code>*Chrome*</code> allow substring matches.
<code>matchCase</code> Sensitive	boolean	Sets a case-sensitive match for the <code>value</code> field.

userLocation

- **Property Manager name:** [User Location Data](#)
- **Criteria version:** The `v2025-05-30` 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.	
matchOperator	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 .	
countryValues	string array	ISO 3166-1 country codes, such as US or CN .	field is COUNTRY
continentValues	string array	Continent codes.	field is CONTINENT
	AF	Africa.	
	AS	Asia.	
	EU	Europe.	
	NA	North America.	
	OC	Oceania.	
	OT	Antarctica.	
	SA	South America.	
regionValues	string array	ISO 3166 country and region codes, for example US:MA for Massachusetts or JP:13 for Tokyo.	field is REGION
checkIps	enum	Specifies which IP addresses determine the user's location.	
	BOTH	Behaves like HEADERS , but also considers the connecting client's IP address.	
	CONNECTING	Considers the connecting client's IP address.	
	HEADERS	Considers IP addresses specified in the X-Forwarded-For header, succeeding if any of them match.	
useOnlyFirstXForwardedForIp	boolean	When connecting via a proxy server as determined by the X-Forwarded-For header, enabling this option matches the end client specified in the header. Disabling it matches the connecting client's IP address.	checkIps is either: BOTH , HEADERS

userNetwork

- **Property Manager name:** [User Network Data](#)
- **Criteria version:** The `v2025-05-30` 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
<code>field</code>	enum	The type of information to match.	
	<code>NETWORK</code>	A specific network.	
	<code>NETWORK_</code> <code>TYPE</code>	A more general <code>NETWORK_TYPE</code> .	
	<code>BANDWIDTH</code>	Bandwidth.	
<code>matchOperator</code>	enum	Matches the specified set of values when set to <code>IS_ONE_OF</code> , otherwise <code>IS_</code> <code>NOT_ONE_OF</code> reverses the match.	
	<code>IS_ONE_OF</code>	Matches any of the specified <code>values</code> .	
	<code>IS_NOT_ONE_</code> <code>OF</code>	Does not match any of the specified <code>values</code> .	
<code>networkValues</code>	string array	Any set of specific networks.	<code>field</code> is <code>NETWORK</code>
		Supported values: @NIFTY AIRTEL ALPHA_INTERNET ALTITUDE_TELECOM AOL ARNET ASAHI ATT AWS BELLALIAN BELL_CANADA BIGLOBE BITMAILER BOUYGUES BRIGHT_HOUSE BSKYB BT CABLEONE CABLEVISION CERNET CHARTER CHINANET CHINA_MOBILE CHINA_UNICOM CLEARWIRE COGECO COLOCROSSING COLT COMCAST COMPLETEL COMPUSERVE COVAD DION DIRECTV DREAMNET DTAG DTI	

Option	Type	Description	Requires
		EARTHLINK EASYNET EITC ETISALAT EUROCIBER FASTWEB FIBERTEL FRANCE_TELECOM FREE FREECOM FRONTIER GOOGLECLOUD H3G HINET IBM IDECNET IIJ4U INFOSPHERE JANET JAZZTELL JUSTNET LIVEDOOR MCI MEDIACOM MEDIA_ONE MICROSOFT MIL NERIM NEWNET NUMERICABLE OCN ODN ONO PANASONIC_HI_HO PLALA PLUSNET PRODIGY QWEST RCN REDIRIS RENATER RESERVED RETEVISION ROAD_RUNNER ROGERS SASKTEL SEEDNET SEIKYO_INTERNET SFR SHAW SOFTLAYER SO_NET SPRINT SUDDENLINK TALKTALK TEKSAVY TELEFONICA TELSTRA TERRA_MEXICO TI TIKITIKI TIME_WARNER TISCALI TURK_TELEKOM T_MOBILE UNI2 UNINET UPC USEMB UUNET VERIZON VIRGIN_MEDIA VODAFONE WAKWAK WIND WINDSTREAM ZERO	

Option	Type	Description	Requires
<code>bandwidth</code> Values	string array	Bandwidth range in bits per second, either <code>1</code> , <code>57</code> , <code>257</code> , <code>1000</code> , <code>2000</code> , or <code>5000</code> .	<code>field</code> is <code>BANDWIDTH</code>
<code>checkIps</code>	enum	Specifies which IP addresses determine the user's network.	
	<code>BOTH</code>	Behaves like <code>HEADERS</code> , but also considers the connecting client's IP address.	
	<code>CONNECTING</code>	Considers the connecting client's IP address.	
	<code>HEADERS</code>	Considers IP addresses specified in the <code>X-Forwarded-For</code> header, succeeding if any of them match.	
<code>useOnlyFirstXForwardedForIp</code>	boolean	When connecting via a proxy server as determined by the <code>X-Forwarded-For</code> header, enabling this option matches the end client specified in the header. Disabling it matches the connecting client's IP address.	<code>checkIps</code> is either: <code>BOTH</code> , <code>HEADERS</code>

variableError

- **Property Manager name:** [Variable Error](#)
- **Criteria version:** The `v2025-05-30` 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
<code>result</code>	boolean	Matches errors for the specified set of <code>variableNames</code> , otherwise matches errors from variables outside that set.
<code>variableNames</code>	string array	The name of the variable whose error triggers the match, or a space- or comma-delimited list of more than one variable name. Note that if you define a variable named <code>VAR</code> , the name in this field needs to appear with its added prefix as <code>PMUSER_VAR</code> . When such a variable is inserted into other fields, it appears with an additional namespace as <code>{{user.PMUSER_VAR}}</code> . See the setVariable behavior for details on variable names.

Notice

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

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

© 2025 Akamai Technologies, Inc. All Rights Reserved. No part of this publication may be reproduced, transmitted, transcribed, stored in a retrieval system or translated into any language in any form by any means without the written permission of Akamai Technologies, Inc. While precaution has been taken in the preparation of this document, Akamai Technologies, Inc. assumes no responsibility for errors, omissions, or for damages resulting from the use of the information herein. The information in this document is subject to change without notice. Without limitation of the foregoing, if this document discusses a product or feature in beta or limited availability, such information is provided with no representation or guarantee as to the matters discussed, as such products/features may have bugs or other issues.

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

Published September 15, 2025