



Control

Caching & Delivery v1

Chunked Streaming v1

Configuring Caching & Delivery v1

Caching & Delivery delivers content via HTTP and HTTPS for all file formats. Both full (entire file) and progressive (range request) downloads are supported.

When you select the **Caching & Delivery** option in the **Configure** menu, the *Configurations* page is displayed.

Note: Caching & Delivery settings are read-only and will be removed in a future release. Please use Caching & Delivery (v2) instead.

The *Configurations* page displays a list of the Caching & Delivery configurations for the currently-selected *Company* and *Account*.

In the *Caching & Delivery* page header, you will see either a *static content* label or a *websites & apps* label, depending on which feature is activated for the currently-selected Account.

The following information is shown for each configuration:

- **Published Host** - The public URL prefix used in links to your published content (URLs seen by end users)
- **Published Path** - The URL path, if any, to use with the **Published Host**
- **Origin Host** - The private URL prefix used by Edgio to retrieve and cache content from your origin server (not visible to end users)

- **Origin Path**- the URL path, if any, to use with the **Origin Host**
- **Host Header** - The value that Edgio will include in the HTTP Host header when making requests to your origin
- **Protocol** - The level of HTTP protocol security to use when delivering your cached content to end-users

Creating a New Configuration

To create a new configuration...

- choose whether the configuration is for *static content* or *websites & apps*
- for a new Published Host, click the **new** button at the top of the list
- for a Published Host already in the list, click the **new** button under that host

The *Create configuration* screen will be displayed. After you've filled in the configuration fields in each of the sections, click **Activate** (at the bottom of the page) to enable your new configuration.

Content Location

Setting	Information Requested	Purpose	Selecting the Right Option
Published Protocol	The level of HTTP protocol security to use when delivering your cached content to end-users	To ensure your content is delivered with the level of security you require	<ul style="list-style-type: none"> • To always deliver content insecurely, select HTTP • To always deliver content securely (via SSL), select HTTPS • To deliver content using the protocol specified in the incoming HTTP request, select Both HTTP and HTTPS
Published Host	<p>The fully-qualified domain name that will be used in all public links (Published URLs) to your cached content</p> <div style="border: 1px solid green; padding: 5px; margin-top: 10px;"> <p>Note: A URL that includes the Published Hostname is referred to as a Published URL.</p> </div>	To direct your users to the <i>Content Delivery</i> service (instead of your origin)	<p>In the Published Host field, enter the published hostname specified in the <i>Welcome Letter</i> associated with your Limelight Account, or a CNAME if desired.</p> <p>The published hostname provided by Edgio will be in a form similar to:</p> <p>accountname.vo.llnwd.net</p> <p>If you prefer to publish under a different hostname, you can use a DNS CNAME record to alias (point) your desired name to Edgio published hostname.</p> <div style="border: 1px solid green; padding: 5px; margin-top: 10px;"> <p>Notes:</p> <ul style="list-style-type: none"> • IP addresses are not accepted. You must enter a fully-qualified domain name. • If you can't find the Edgio published hostname in your <i>Welcome Letter</i>, please contact Limelight Customer Service </div> <p>If you want to use a directory name "alias" for a particular origin path, you</p>

			can add the alias by entering it in the Published Path field.
Published Path	The "alias" for a particular origin path.		<p>If the path ends with a filename, check the This path ends with a filename checkbox.</p> <p>If you want to publish select few types, check the Only publish files with these extensions checkbox. Then enter file extensions in the field that displays. When done entering all extensions, press the enter key or tab key.</p>
Location of Content Origin	The location of the content you want the <i>Content Delivery</i> service to deliver (the "origin")	The <i>Content Delivery</i> service needs to know where to find your content when users first request it, and also when it needs to be refreshed in the cache	<p>If your content is not stored with Edgio, choose Outside Edgio infrastructure. Otherwise, choose the appropriate Edgio Storage location.</p> <div style="border: 1px solid green; padding: 5px; margin-top: 10px;"> <p>Note: If you are using Edgio storage but your storage option is not shown, your <i>Content Delivery</i> service is not fully configured. If this is the case, please contact Edgio Client Support.</p> </div>

Table 1. Configure - Delivery - Content Location Settings

If you choose **Outside Edgio infrastructure** in **Location of Content Origin**, the following additional fields are displayed:

- Origin Protocol
- Origin Host
- Origin Path
- Origin HTTP Port

If you choose a Edgio storage option in **Location of Content Origin**, the following fields are displayed:

- Origin Path

Setting	Information Requested	Purpose	Selecting the Right Option
Origin Protocol	The HTTP protocol(s) to use when retrieving content from your origin (when the content is not found in cache or has expired in cache)	To ensure your content is retrieved with the level of security you require	<ul style="list-style-type: none"> • To always retrieve content insecurely, select HTTP Always • To always retrieve content securely (via SSL), select HTTPS Always • To retrieve content using the protocol specified in the user's HTTP request, select Match Inbound Protocol
Origin Host	The fully-qualified domain name or IP	The <i>Content Delivery</i> service needs to know	Enter the domain name or IP address of your origin server in the Origin

	address of your origin server	where to get your content when users first request it, and also when it needs to be refreshed in the cache	Hostname field. Please note that if you enter a domain name, it must be fully qualified.
Origin Path			If your content is all in particular path on your origin, or you added a directory name "alias" with the Published Hostname for a particular origin path, you can enter the origin path by clicking the Add Path link
Origin HTTP port number	The HTTP port number to use when communicating with your origin server, using the Origin Host and Origin Path you specified	If you are using a port other than the default (80) for HTTP, the <i>Content Delivery</i> service needs to know which port you've chosen	Leave the default port number for HTTP unless you are using another port number. If so, enter the new port number in the Origin HTTP Port Number field. Note: The default for HTTPS is 443, and this is the value used by Edgio for all HTTP requests to origin (the value is not editable).
Host Header	The value to include in the HTTP Host header when communicating with your origin server	To help prevent end users from requesting content directly from your origin.	If you plan to block requests to your origin based on the value of the Host header, select Published Hostname or enter a value in the Value field If you are hosting more than one origin on a single server, please see the additional information below.

Table 2. Configure - Delivery - More Content Location Settings

Host Header Details

Browsers usually include the origin domain name of the requested URL in the HTTP Host header. You can use this behavior to detect and block such requests on your origin, denying those with a Host header that matches your domain name, and accepting those that match either your **Published Host** or another value you enter in the **Value** field.

If you are hosting more than one origin on a single server and you want to block based on Host headers, don't use **Published Hostname** - enter a value in the **Value** field instead. If you are hosting more than one origin on a single server and you don't want to block based on Host headers, choose **Origin Host**.

Example Settings

Configuration Field	Value	Notes
Protocol	HTTPS	Accept only HTTPS requests for cached content
Published Host	published.host.com	Use a CNAME alias instead of the name provided in the Welcome Letter (need to set up the CNAME separately)
Published Path	/pubimages/	Use the pubimages directory to uniquely identify the content in cache
Origin Protocol	HTTP Always	Always use HTTP to communicate with the origin server
Origin Host	origin.host.com	
Origin Path	/images/	Directory path to the origin content; note that this doesn't need to match the path (if any) for the Published Hostname
Origin HTTP Port	80	Use the default HTTP port (no need to change anything)
Host Header	Published Hostname	This will block most browser requests made directly to origin

Table 3. Configure - Delivery - Content Location - Example Settings

Using the example configuration settings above, if `favicon.ico` is not cached for this configuration, or has expired in cache, a request to `https://published.host.com/pubimages/favicon.ico` will result in an origin request for `http://origin.host.com/images/favicon.ico`, with an HTTP Host header of `published.host.com`.

Caching Rules

Setting	Information Requested	Purpose	Selecting the Right Option
Origin Cache Control & Expiration Header	Whether to override the default method for determining if an object in cache is expired	In some cases you may want to take explicit control over object expiration times (TTL - "Time To Live").	To allow <i>Content Delivery</i> to calculate TTL, select Honor Origin Cache-Control and Expires headers . Otherwise, choose Override Origin Cache-Control header and TTL values . If you want to set TTL to a specific length of time, select one of the times in the Time To Live (TTL) drop-down menu. Otherwise, to allow adaptive TTL calculation, select Custom from the Time To Live (TTL) drop-down menu.
Cache large files on first request	Whether you want any request for an object to force the full object to		Note: This feature is intended for large file

	be cached, even if the request is cancelled.		<div style="border: 1px solid green; padding: 5px;"> <p>downloads, and is not recommended for caching website objects (such as image, CSS, and JavaScript files).</p> </div>
Ignore "No cache" header	Whether <i>Content Delivery</i> should ignore certain Cache-Control headers when determining whether or not to cache an object retrieved from your origin	You may want to cache objects regardless of origin settings that attempt to turn caching off	<p>If you want to ignore the following Cache-Control headers:</p> <ul style="list-style-type: none"> • Cache-control: no-cache • Cache-control: no-store • Cache-control: private • Pragma: no-cache <p>enable this option. Otherwise, leave it disabled.</p>
Specific Query String Caching	Whether to use URL query terms to determine whether or not objects are cached	You may want to increase cache efficiency by ensuring certain objects are not duplicated due to variations in their query terms	<p>Choose the option that caches the minimum number of objects necessary based on query parameters:</p> <ul style="list-style-type: none"> • Strip no query terms from the cache key • Strip all query terms from the cache key • Exclude specific query terms • Keep only specific query terms <div style="border: 1px solid green; padding: 5px;"> <p>Note: For the Exclude specific query terms and Keep only specific query terms options, you must enter a comma separated list of the query terms to be excluded or included</p> </div>
Vary Headers	Which Vary response header fields Content Delivery should use when differentiating versions of an object in cache	<p>Content Delivery stores a separate version of a requested object for each unique set of request header fields specified by the Vary header.</p> <p>If the Vary header specifies request header fields that change frequently, multiple copies of the same object may be stored in cache.</p> <p>To control this behavior,</p>	<ul style="list-style-type: none"> • If you only want to cache a single version of an object regardless of its Vary header fields, choose Ignore all Vary headers • If want cache a new version of an object whenever any of its Vary header fields changes, choose Do not ignore Vary headers • If want cache a new version of an object whenever all but certain specified Vary header fields change, choose Ignore specific vary headers and select the Vary headers fields to ignore

		<p>you can configure <i>Content Delivery</i> to ignore all Vary headers or specific Vary headers when caching and retrieving objects.</p> <p>All of the Vary headers associated with the object are still maintained and passed on to the client in the response.</p>	
Partial Cache	Whether to use Partial Caching to improve cache performance	Partial Caching is a <i>Content Delivery</i> feature that caches commonly-requested portions of content requested using HTTP GET ranges. This optimization can significantly improve performance for large media files.	To enable this setting, check the Partial Cache checkbox, and in the associated field, enter a Regex value that matches the object URLs you want to optimize
N Byte Download	Whether to download the first "n" bytes to improve cache performance	<i>Content Delivery</i> can automatically cache a specified number of bytes from the beginning of cached files. This optimization can improve first-byte response times in some scenarios.	To enable this setting, check the N Byte Download checkbox, and in the associated field, enter a Regex value that matches the object URLs you want to optimize

Table 4. Configure - Delivery - Caching Rules Settings

Use the **Honor Origin Cache-Control and Expires headers** setting unless you have a specific reason to override the way in which object Time To Live (TTL) is calculated.

By default, *Content Delivery* considers an object “stale” (expired from cache) if the number of seconds specified by the associated `Cache-Control: s-maxage` or `Cache-Control: max-age` header has elapsed since initial caching or since the last freshness check, or if neither header is present, if the date and time in the `Expires` header has passed. The order of precedence is `Cache-Control: s-maxage`, `Cache-Control: maxage`, then `Expires`.

If no explicit freshness information is supplied (there are no `Cache-Control: s-maxage`, `Cache-Control: max-age` or `Expires` headers), and a `Last-Modified` header is present, the CDN will by default use the adaptive cache freshness algorithm to calculate remaining TTL, based on 20% of the age of the cached response, subject to a floor of 3 seconds and a ceiling of 3 days.

If you need to override (ignore) the above behavior, you can use the **Override Origin Cache-Control header and TTL values** option to specify a new TTL value using the **Time to live (TTL)** drop-down menu.

You can also control whether generated responses are cached using the **Cache Generated Responses** checkbox (for the **Custom** option) or **Including Generated Responses** (for other values in the drop-down menu).

Notes:

Generated responses are HTTP responses that are generated dynamically (“dynamic content”). These responses often do not include any of the cache control headers needed to determine TTL, and are not cached by default to avoid caching personalized or user-specific responses.

By default, Edgio defines a generated response as one that is missing all of the following headers:

- Expires
- Last-Modified
- Cache-Control: max-age
- Cache-Control: s-max-age

If you choose the **Custom** option for **Time to live (TTL)**, you can change the parameters of the cache freshness algorithm using **Specify custom floor and ceiling cache values**.

If desired, the floor (minimum) can be raised and the ceiling (maximum) can be lowered or raised. If min and max are set equal to each other, the TTL becomes explicit, rather than adaptive.

Arc Light

You can use Arc Light to customize how Content Delivery reacts to HTTP requests and responses. Rules can be triggered when a request or response meets pre-defined conditions, such as a pattern match. Rules are designed based on specific customer needs.

Note: This option is available only for *websites & apps* configurations

Configuration Overview

Use Arc Light to customize how Content Delivery reacts to the following HTTP request and response types:

- Requests
 - Any
 - Origin only
 - Edge only
- Responses
 - Any
 - Origin only
 - Client only

For each of the above request and response types, you can assign one rule. Content Delivery will then execute that rule each time it receives the associated request or response type. The rule will be executed on the Edge Server that receives the request or response.

To enable Arc Light for a specific request or response type, check the checkbox next to the desired type (example: **Rules on Edge Request**). To assign a rule, click one of the rules in the list below the request/response type.

Rules can be triggered when a request or response meets pre-defined conditions, such as a pattern match with:

- The URL, file name, or query term
- The IP address
- The value of a specified HTTP header
- A cookie
- The geographic location of a request (using the IP address)

When a rule is triggered, it can perform a variety of actions, such as:

- Controlling which CORS headers are sent in response to a client request
- Adding a cookie that contains geolocation information
- Adding specific HTTP headers
- Appending special “keys” to cache keys
- Enabling or disabling GZIP compression
- Controlling whether the requested content is cached and setting content TTLs

Rules are designed based on specific customer needs. If you need to use Arc Light or want more information on the types of rules that can be created, please contact your Account Manager or Solutions Engineer.

Configuration Settings

You can configure these settings:

Setting	Information Requested	Purpose	Selecting the Right Option
Which rules do you want to enable?	If you want to create a new rule, the type of HTTP request or response to associate it with	Content Delivery can trigger rules for several types of requests and responses	(see the options below)
Rules on Any Request	Request type	Content Delivery can trigger rules for several types of requests	To trigger a rule on any type of request received by a Edgio Edge Server, check the Rules on Any Request checkbox, and select one of the predefined rules in the list
Rules on Edge Request	Request type	Content Delivery can trigger rules for several types of requests	To trigger a rule on client requests to a Edgio Edge Server, check the Rules on Edge Request checkbox, and select one of the predefined rules in the list
Rules on Origin Request	Request type	Content Delivery can trigger rules for several types of requests	To trigger a rule on Edgio requests to your Origin, check the Rules on Origin Request checkbox, and select one of the predefined rules in the list
Rules on Any Response	Response type	Content Delivery can trigger rules for several types of responses	To trigger a rule on any type of response received by a Edgio Edge Server, check the Rules on Any Response checkbox, and select one of the predefined rules in the list

Rules on Origin Response	Response type	Content Delivery can trigger rules for several types of responses	To trigger a rule on responses received from your Origin, check the Rules on Origin Response checkbox, and select one of the predefined rules in the list
Rules on Client Response	Response type	Content Delivery can trigger rules for several types of responses	To trigger a rule on responses received from the requesting client, check the Rules on Client Response checkbox, and select one of the predefined rules in the list

Media Delivery

Content Delivery supports "seeking" or "scrubbing" (skipping back and forth) within FLV and MP4/H.264 video files. Seeking is controlled via parameters specified in the query terms of the request URL.

Setting	Information Requested	Purpose	Selecting the Right Option
Enable FLV Scrubbing	Whether to allow video client to skip forward and back (seek) within FLV files based on parameters specified in the query terms of the request URL.	Custom clients may want to provide the "seek" capability ("forward" and "back" buttons)	To enable this feature, check the Enable FLV Scrubbing checkbox
Enable MP4/H.264 Scrubbing	Whether to allow video client to skip forward and back (seek) within properly segmented MP4 files based on parameters specified in the query terms of the request URL. When you use this option, any query terms in the URL are ignored. <div style="border: 1px solid green; padding: 5px; margin-top: 10px;"> <p>Note: Query terms are interpreted by EdgePrism, and influence what part of an MP4 file is presented to a user. Other query terms in the URL may be ignored, which may influence the behavior of the origin that delivers the file.</p> </div>	Custom clients may want to provide the "seek" capability ("forward" and "back" buttons)	To enable this feature, check the Enable MP4/H.264 Scrubbing checkbox

Table 5. Configure - Delivery - Media Delivery Settings

Optimization

Setting	Information Requested	Purpose	Selecting the Right Option
Type of Compression	Whether to use Gzip com-	Compressed objects are delivered more quickly,	<ul style="list-style-type: none"> If you want to provide all compressed files from your origin

	pression when delivering XHTML, JavaScript, CSS, and other text files	potentially improving the user experience	<p>server, choose the Gzip Passthrough option</p> <ul style="list-style-type: none"> • If you prefer to have the <i>Content Delivery</i> service compress files when the requesting client can accept them, choose Gzip on-the-fly • If you need to modify Gzip compression defaults, choose Custom, then either Gzip on-the-fly or Gzip Passthrough, and enter your Gzip modification extensions • You can also choose No compression if none of your files should be delivered compressed • For more information on this feature, see Gzip Details
TCP Acceleration	The “profile” to use when accelerating the transfer of IP packets by modifying default TCP parameters	In certain circumstances, you may want to change the TCP Acceleration profile to optimize your delivery performance	<p>When TCP Acceleration is enabled, the XDLL profile is the most efficient in many cases.</p> <div style="border: 1px solid green; padding: 5px; margin-top: 10px;"> <p>Note: TCP Acceleration is an advanced configuration setting, and should only be changed if you’re an expert user.</p> </div>
<p>Enable chunked response to client</p> <div style="border: 1px solid green; padding: 5px; margin-top: 10px;"> <p>Note: for static content configurations only</p> </div>	Whether the <i>Content Delivery</i> service can maintain open TCP connections to your origin server	If there is a cache “miss” and your origin doesn’t provide a <code>Content-Length</code> header, this option allows <i>Content Delivery</i> to serve the requested content more efficiently (in “chunks”)	We recommend you enable this option. Otherwise, new TCP sessions must be established for each new request to origin, and cache miss requests are delivered only when the entire object has been transferred from origin.

Table 6. Configure - Delivery - Optimization Settings

Gzip Details

When **Gzip Passthrough** is enabled, and a client indicates (via HTTP request header) that it prefers to receive compressed content, the *Content Delivery* service will serve a compressed version of the requested object if one is available on the origin server.

Note: *Gzip Passthrough* is available to all customers. If it is not enabled for you, please contact Edgio Support.

If **Gzip On-the-fly** is selected, the *Content Delivery* service creates, caches, and delivers Gzip-compressed content as needed.

Compressible file types include: action, ashx, asmx, asp, aspx, axd, cfm, css, css3, csv, do, doc, docx, htm, html, js, jsf, json, jsp, php, portal, rtf, svg, svgz, tsv, txt, xhtml, xml, site root (/), and extensionless URLs.

Request & Response Headers

Setting	Information Requested	Purpose	Selecting the Right Option
Client Analytics	Whether you want the <i>Content Delivery</i> service to provide geographic user information when requesting content from your origin	You may want to internally capture, analyze and report on user geographic information.	To use this feature, check the Client Analytics checkbox. The geo information is provided to your origin server via two request headers: X-IP-Geo-Country and X-IP-Geo-All. The geo fields provided are continent, country, state, city, dma_id, and asn.
Add client IP address to origin request header <div style="border: 1px solid green; padding: 5px; margin-top: 10px;"> <p>Note: for static content configurations only</p> </div>	Whether you want the <i>Content Delivery</i> service to provide the requesting client's IP address in a custom header when requesting content from your origin	You may want to internally capture, analyze and report on user IP information	To enable this feature, check the Add client IP address to origin request header checkbox, and enter the header name(s) that should contain the client IP address. The default header name is True-Client-IP. Note that the above headers are in addition to X-Forwarded-For, which is always provided to the origin.
POST Requests	Whether you want to accept or ignore POST requests from clients	If you are using a custom client to display content, you may want to allow it to communicate analytics or other information to your origin. Alternatively, you may want to convert POST requests to GET requests, or simply ignore them.	<ul style="list-style-type: none"> To ignore all POST requests, select Disable HTTP POST requests. <i>Content Delivery</i> will respond with an HTTP 413 Request Entity Too Large status code to all POST requests. To accept POST requests and pass them through to your origin, select Enable HTTP POST requests. If a POST request body exceeds 500 MB, <i>Content Delivery</i> will respond with an 413 Request Entity Too Large status code.

			<ul style="list-style-type: none"> To accept POST requests but treat them as GET requests, select Enable HTTP POST requests, and check the Discard request body on POST request checkbox. POST bodies will be discarded.
Add custom request header	Whether you want to include custom headers and values whenever <i>Content Delivery</i> makes a request to your origin	If you want to tag all requests from <i>Content Delivery</i> for later analysis	To add a custom origin request header, click the Add custom request header link, and enter a unique header name and value
Add Edgio server IP address when responding to client	Whether to provide clients with the IP address of the <i>Content DeliveryEdge</i> Server responding to their requests	<p>If you are using a custom client to display content, and you are also capturing performance-related data via the client, you may want to include the <i>Content DeliveryEdge</i> Server IP address for later analysis and reporting.</p> <p>The IP address will be provided in the X-IP-Address response header.</p>	To enable this feature, check the Add Edgio server IP address when responding to client checkbox
Add custom response header	Whether you want to include custom headers and values whenever <i>Content Delivery</i> responds to a client request	If you are using a custom client to display content, you may want to provide it with information that uniquely identifies the <i>Content Delivery</i> service, Limelight Account, etc.	To add a custom client response header, enter a unique header name and value and. Click the "+" button to add additional headers.
Enable Custom Debug Headers	Whether you want to enable Custom Debug Headers	By making an HTTP content request with special "Custom Debug Headers," including a shared secret specific to your service, you can retrieve cache-related information about individual content objects and prevent others from accessing the information.	<p>In the Debug Headers field, enter one or more "tags" to include in the Custom Debug Headers. Then in the Secret Key To Request Debug Information field, enter the secret key (shared secret) provided by Edgio when the Custom Debug Headers feature was enabled.</p> <p>For more information, see Secure Cache Diagnostics.</p>

Table 7. Configure - Delivery - Request & Response Headers Settings

Secure Cache Diagnostics

When troubleshooting caching issues, customers can now directly access diagnostic information about cached content.

Content Delivery customers with *Configuration Self Service* can now request cache-related information about individual content objects, without the risk of this information being accessible by others.

To enable this feature, check the *Enable Custom Debug Headers* checkbox in the *Request and Response Headers* section of *Content Delivery Configuration Self Service*, and provide a comma-separated list of object properties that should be returned in the response, along with a Secret Key to authenticate the request.

Diagnostic response headers can include the following information:

- Whether or not a response is cacheable
- How the cache responded to a request (hit, miss, etc.)
- The number of seconds before the cached response will be considered stale (TTL)
- The total number of seconds representing the freshness lifetime of the response (age + TTL) and how the value was determined (headers, overrides, adaptive TTL, etc .)

When the feature is activated, you will be provided with a unique shared secret.

The properties that can be requested, and their associated response headers and values, are:

Request Key	Response Header	Return Values
is-cacheable	X-LLNW-Dbg-Is-Cacheable	Yes No Negative
cache-hit-type	X-LLNW-Dbg-Cache-Hit-Type	HIT MISS REFRESH_HIT REF_FAIL_HIT REFRESH_MISS CLIENT_REFRESH_MISS IMS_HIT NEGATIVE_HIT DENIED OFFLINE_HIT REDIRECT
ttl	X-LLNW-Dbg-TTL	n{...} seconds an integer followed by a space and the string "seconds"
fresh-life-total	X-LLNW-Dbg-Fresh-Life-Total	n{...} seconds an integer followed by a space and the string "seconds"

If the secret is invalid, the X-LLNW-Dbg-Hdrs header will be ignored and the request will be processed without it.

Request & response example:

Request	Response
GET http://www.customer.com/object.txt HTTP/1.1...X-LLNW-Dbg-Hdrs: is-cacheable,cache-hit-typeX-LLNW-Dbg-Secret: sharedsecret	HTTP/1.1 200 OK...X-LLNW-Dbg-Is-Cacheable: Yes...X-LLNW-Dbg-Cache-Hit-Type: HIT

Failover

Normally, when the CDN receives an HTTP 404 (Not Found), 503 (Service Unavailable) or 504 (Gateway Timeout) response from your origin, the error is passed back to the requesting client. You can modify this configuration option as follows:

- For 404 errors:
 - Serve "stale" content from the CDN Cache, or
 - Request content from a "backup host" (with or without a path), or
 - Redirect to a custom "Not Found" URL.
- For 503 and 504 errors:
 - Request content from a "backup host", or
 - Redirect to a custom "Service Unavailable URL"

Notes:

- Failover URLs must match their own configuration within the CDN
- For 404 error redirects, the original request is reissued to the fallback URL with any modifications still in place
- 503 or 504 errors may have been generated by the origin, but could also be generated by CDN if a connection can't be made to your origin

Setting	Information Requested	Purpose	Selecting the Right Option
Serve stale content instead of 404 error	If the requested content is cached but stale (expired), and there is an HTTP 404 status when requesting a fresh version from your origin, whether you want to pass the 404 status back to the client, or serve the stale content instead	If an object has expired in cache, and your origin server returns a 404 (Page Not Found) error when <i>Content Delivery</i> attempts to get a fresh copy of the object, you may want to serve the expired object instead of allowing the client to handle the 404 message.	If it's not acceptable for the client to handle the 404 message, and you are OK with serving stale content instead, check the Serve stale content instead of 404 error checkbox. Note that if there is no cached object, a 404 message will still be returned to the browser.
Request content from backup host on 404 error	If there is an HTTP 404 status when requesting fresh content from your origin, whether to try a backup origin (hostname only) before handling the 404 status	If your primary origin returns a 404 status, and you have a backup origin, you may want <i>Content Delivery</i> to try the backup before handling the error	To try a backup origin if the primary origin responds with a 404 status, enter the fully-qualified hostname of the backup origin.

			<p>Note: Specific ports are not supported.</p>
<p>Use custom "Not Found" page</p>	<p>Whether you want to pass HTTP 404 status messages back to the client, or serve a custom error page instead</p>	<p>If an object has expired in cache, and your origin server returns a 404 error to <i>Content Delivery</i>, you may want to serve a custom error page instead of allowing the client to handle the 404 message.</p>	<p>If you want to take control over the content displayed by clients when there is a 404 from origin, enter the fully-qualified URL of the content to serve.</p>
<p>Request content from backup origin URL on 404 error</p>	<p>If there is an HTTP 404 status when requesting fresh content from your origin, whether to try a backup URL path before handling the 404 status</p>	<p>status, and you have a backup origin, you may want <i>Content Delivery</i> to try the backup before handling the error</p>	<p>To try a backup URL path if the primary origin responds with a 404 status, enter the fully-qualified path on the backup origin.</p> <p>Notes:</p> <ul style="list-style-type: none"> You can specify either the HTTP or HTTPS protocol, and a port number if desired. This option is required when using the Intelligent Ingest feature of Origin Storage
<p>Request content from backup host on 5xx error</p>	<p>If there is an HTTP 5xx status when requesting fresh content from your origin, whether to try a backup origin before handling the 5xx status</p>	<p>If your primary origin returns a 5xx status, and you have a backup origin, you may want <i>Content Delivery</i> to try the backup before handling the error</p>	<p>To try a backup origin if the primary origin responds with a 5xx status, enter the fully-qualified hostname of the backup origin.</p> <p>Note: Specific ports are not supported.</p>

<p>Use custom "Service Unavailable" page</p>	<p>Whether you want to pass HTTP 503 and 504 status messages back to the client, or serve a custom error page instead</p>	<p>If an object has expired in cache, and your origin server returns a 503 <i>Service Unavailable</i> or 504 <i>Gateway Timeout</i> error to <i>Content Delivery</i>, you may want to serve a custom error page instead of allowing the client to handle the error message.</p>	<p>If you want to take control over the content displayed by clients when there is a 503 or 504 error from origin, enter the fully-qualified URL of the content to serve.</p>
---	---	---	---

Table 8. Configure - Delivery - Failover Settings

Content Security

IP Access Control

Setting	Information Requested	Purpose	Selecting the Right Option
<p>Enable IP Access Control</p>	<p>Whether you want to "allow list" or "deny list" requests based on IP address lists and IP-based geographic locations</p>	<p>IP Access Control allows you to exclude specific geographies or limit access to known entities</p>	<p>Assign access lists to the Caching & Delivery configuration using the following drop-down menus:</p> <ul style="list-style-type: none"> • By IP address list: Select one or more existing lists, then choose either Deny or Allow to indicate the type of restriction. Click Add to add the lists to the Access control list for this configuration section. • By geolocation: Select one or more geographic areas (continents or countries), then choose either Deny or Allow to indicate the type of restriction. Click Add to add the lists to the "Access control list for this configuration" section. <p>Access control list for this configuration Section</p> <p>You can select a default security setting for the configuration - either Default Allow or Default Deny. You can then add one or more IP address lists and geographic locations that modify the default setting. IP address lists and geolocations can be "mixed and matched" in any order desired.</p> <p>To move an item in the list, move the mouse pointer over the item and use the vertical ellipses to drag and drop the item to another location in the list.</p> <p>If you have the correct permissions, click Manage IP Lists to display a dialog that allows you to create new IP access lists. You can also view, edit, and delete existing IP address lists.</p> <p>To view list details, click the + icon to the left of a list.</p> <ul style="list-style-type: none"> • The text "Used by configs in accounts" shows which Accounts have configurations that use the list. • The text "Limited to accounts" shows any accounts to which your <i>Company Admin</i> has limited the list. <p>To create a new list, click the new list button at the top of the dialog, then:</p> <ol style="list-style-type: none"> 1. Provide a name for the list. 2. Provide a single IP address or range of IP addresses. You can also create and upload CSV files of IP addresses. Click the link to see a sample CSV file. 3. Optionally limit the list to accounts. 4. Click the Save button. The new list is now available in the By IP address list: drop-down menu at the top of the section.

Setting	Information Requested	Purpose	Selecting the Right Option
			<p>To deny access to end users attempting to access your content using an anonymous VPN from an unauthorized geolocation, select the Deny 'Anonymized with VPN' access option.</p> <div style="border: 1px solid black; padding: 5px; background-color: #e6f2e6;"> <p>Notes:</p> <ul style="list-style-type: none"> IP address lists and geographic locations are processed in the order they are specified (top to bottom). Once a match is found, subsequent lists and locations are ignored Users with the <i>Company Admin</i> role can manage lists for all accounts. Users with the <i>User</i> role who have been granted the <i>Manage Delivery Configurations</i> permission can apply all lists in the Accounts for which they have been granted management permission. Changes made to IP address lists are applied immediately and affect all Account configurations which use them (even legacy configurations that can't be edited in Control). IP address lists cannot be deleted if they are in use. </div>

Table 9. Configure - Delivery - Content Security Settings

Content Delivery makes it easy to implement and manage IP-based access control using both IP addresses and geographic locations.

Content Delivery Configuration Self Service provides access control using IP addresses and geographic locations ("geo-fencing"). When configuring an Account, you can associate lists of IP addresses and groups of geographic locations with the Account and specify whether to allow or deny each. When managing IP address lists, you can also view whether they are currently in use and which Accounts they are associated with (or limited to).

MediaVault

Setting	Information Requested	Purpose	Selecting the Right Option
Enable MediaVault content protection	Whether you want to use <i>MediaVault</i> to provide additional content security. <i>MediaVault</i> provides high-performance URL authentication.	<i>MediaVault</i> can help you prevent "deep linking" and other unauthorized viewing behavior	<p>To enable this feature, check the Enable <i>MediaVault</i> content protection checkbox, and provide a primary and secondary "shared secret" (both used to prevent URL tampering).</p> <p>You can also change the HTTP Error Code returned by <i>MediaVault</i> from the default 400 code by entering a new value in the Deny Status Code field.</p> <p>For more information, see MediaVault Details.</p>

MediaVault is a high-performance URL authentication service. *MediaVault*'s main purpose is to help you secure your content from unauthorized viewing.

MediaVault maximizes authentication performance by using tokens to avoid three-way handshakes (common to other methods of authentication) that can lead to severe connection time latency.

Please note that *MediaVault* is *not* a replacement for DRM and should not be associated with user authentication.

MediaVault works like this:

- You enter a shared secret during the configuration process
- You then generate a token (MD5 hash) for each published URL, based on the shared secret, and append it to the URL in a query term or provide it in a cookie. You can generate the token manually by navigating to the *Configure > MediaVault* in the navigation pane, or by creating server-side code on your origin.
- When a request is received, *MediaVault* uses the same hash algorithm to create its own token, which should be identical to the one you appended.
- If the tokens match, *MediaVault* then looks for additional *MediaVault*-specific query terms (such as end date/time and IP address/mask) to determine whether the request is valid. If the tokens don't match, the URL was tampered with and the request is rejected.

For more information, see the *MediaVault User Guide* by navigating to Help Center > Documentation > Delivery > Guides > *MediaVault* in the navigation pane.

Advanced

You can use the **Additional Options** step to view any advanced *Content Delivery* configuration changes Edgio makes to your configuration.

If one or more such configurations is changed from its default value by Edgio, the **Additional Options** tab becomes visible, and the advanced configurations and their settings are displayed:

Setting	Information Requested	Purpose	Selecting the Right Option
(various)	(none) This is a read-only display of advanced <i>Content Delivery</i> configuration changes Edgio has made to your configuration	The information in the Additional Options step can help you better understand your configuration.	If you have questions about any settings in Additional Options, please contact your Account Manager or Edgio support.

Table 10. *Configure - Delivery - Advanced Settings (Read Only)*

The advanced configuration options which can be configured for you by Edgio (and become visible in the *Additional Options* step) include:

Option Name	Description
Assume cacheable pending origin response	If an origin request is pending for an object, continue serving the object from cache
Cache entire object if range request less than offset	Cache the entire object for Range requests ending before the specified Byte offset
Cache hit/miss response trigger	Returns HIT or MISS in the X-CDN-Cache response header when the specified request header (trigger) is present
Cache only "popular" objects	Cache only objects that are "popular" based on the specified "points" (the approximate frequency an object is requested, in seconds)
Convert URL ranges to Range requests	Convert URLs ending in <i>/range/x-y</i> or <i>/range/x-</i> to origin GET range requests

Deny requests with specified Referer header(s)	Deny requests with the specified Referer header(s)
Disable object caching	Do not cache objects
Disable persistent origin connections	Disable persistent origin connections (“enabled” is the default global configuration)
Do not add max-age on all requests to origin	Don’t add Cache-Control: max-age=259200 header on origin requests (but do include any existing Cache-Control headers)
Enable Partial Caching by Regex	Enable Partial Caching for object URLs that match the specified Regex
Gzip compression level	Set the Gzip compression level (0 to 9). The default (and recommended) level is 1.
Ignore bad status codes from origin	Ignore bad status codes from origin (40x and 5xx). If FALSE, other rewrite options may redirect the client to specific URLs based on the status code.
Lowest allowed rate-limiting bitrate	Set the lowest bitrate allowed when rate limiting, in KBytes/second
Make cached URLs case-insensitive	Make the URLs of cached objects case-insensitive by converting all characters to lowercase in the Cache Key. When using this feature, all Purge requests must not contain any uppercase characters.
Max duration client can be idle while receiving response	After this time passes, the client is disconnected and the request is aborted. The default is 30 minutes.
Maximum object TTL	Set the maximum TTL value for all cached objects, in seconds, but honor Cache-Control headers if present
Minimum object TTL	Set the minimum TTL value for all cached objects, in seconds, but honor Cache-Control headers if present
Object TTL for “negative” origin response	Set the object TTL, in seconds, when there is a negative origin response (status codes other than 200, 203, 300, 301 and 401 and/or Cache-Control or Pragma headers with certain values). This rewrite overrides other origin cache control headers.
Origin connect timeout duration	Set the timeout, in seconds, for initiating origin connections (how long to wait when trying to establish a connection)
Origin reply timeout duration	Set the timeout, in seconds, for origin replies (how long to wait for a reply from origin)
Persistent client connection duration	Set the duration, in seconds, of persistent client connections
Persistent origin connection duration	Set the duration, in seconds, of persistent origin connections
Redirect clients to source URL	Redirect clients to the source URL with the specified status code
Refresh-check cached content on every request	Check for fresh origin objects (newer versions of objects) on every request. Most commonly used in conjunction with <i>Ignore bad status codes from origin</i> to enable the origin to allow or deny every request by inspecting all request parameters, including Cookies.
Remove specified response header(s)	Remove origin response headers that match the specified value
Retry failed <i>MediaVault</i> HTTPS hash	If an HTTPS <i>MediaVault</i> hash check fails, retry the same hash-check URL using HTTP

checks	
Store <i>MediaVault</i> hash in cookie	Keep the <i>MediaVault</i> hash secret in a browser cookie (rather than in a URL parameter)
Treat empty responses with 200 status as 404 status	Treat "empty" origin responses (no content body) with 200 status codes as if they are 404 status codes
Do not apply <i>MediaVault</i> on URLs matching the regex	Configure <i>MediaVault</i> to ignore URLs matched by the displayed regular expression

Table 11. *Configure - Delivery - Wizard - Additional Options Available*

Logging


Setting	Information Requested	Purpose	Selecting the Right Option
Log cookies	Whether you want <i>Content Delivery</i> to stop saving cookie information in your log files	If you process log files and don't need the information in the Cookie header, you may want to remove it to simplify processing and/or reduce log file size.	If you know you need Cookie header information in your log files, check the Log cookies checkbox. Otherwise, leave it unchecked. When this setting is enabled, <i>Content Delivery</i> logs all Cookie header information, up to a maximum of 8 KB for the entire header (regardless of the number of cookies in the header).
Log request header	Whether you want <i>Content Delivery</i> to start saving specific Request Headers in your log files	If you process log files and need access to information in the Request Headers, you may want to enable this option	If you know you need Request Header information in your log files, check the Log Request Header checkbox and enter the names of the specific headers to log. Otherwise, leave it unchecked.

Table 12. *Configure - Delivery - Logging Settings*

Notes

You can use the **Notes** field to additional information for others (why the configuration changes were made, etc.). Users can refer to the notes later when browsing historical configuration changes

Previewing a Configuration

 To preview the settings associated with a configuration, click the "eye" icon at the bottom right of the configuration row. For information on the individual settings displayed, please see the setting descriptions in [Creating a New Configuration](#).

Editing a Configuration



To edit a configuration, click the "pencil" icon at the bottom right of the configuration row. For information on the individual settings displayed, please see the setting descriptions in [Creating a New Configuration](#).

Note: For some configurations created for you by Edgio, only the preview ("eye") icon will be visible. If this is the case, and you need to make changes, please contact your Account Manager or Solutions Engineer. Edgio can continue to manage the configuration, or it can be made available for you to edit in the *Control*.

Cloning a Configuration



To clone (make a copy of) a configuration, click the "copy" icon at the bottom right of the configuration row. When you have finished making changes to the settings, click **Activate** to enable the new configuration.

Note: For some configurations created for you by Edgio, only the preview ("eye") icon will be visible. If this is the case, and you need to make changes, please contact your Account Manager or Solutions Engineer. Edgio can continue to manage the configuration, or it can be made available for you to edit in the *Control*.

Deleting a Configuration



To delete a configuration, click the "trash" icon at the bottom right of the configuration row.

Note: For some configurations created for you by Edgio, only the preview ("eye") icon will be visible. If this is the case, and you need to make changes, please contact your Account Manager or Solutions Engineer. Edgio can continue to manage the configuration, or it can be made available for you to edit in the *Control*.

Reverting to a Previous Configuration



Each time you update a configuration, a new version is assigned.

To revert to a previous configuration:

1. Click the "undo" icon at the bottom right of the configuration row.
A list of previous versions display in a dialog.
2. Select the version to which you want to revert

Note: Although you intend to revert to a previous version, the reverted version will become the current version, which will have a new version number. The new version number is displayed at the bottom of the dialog.

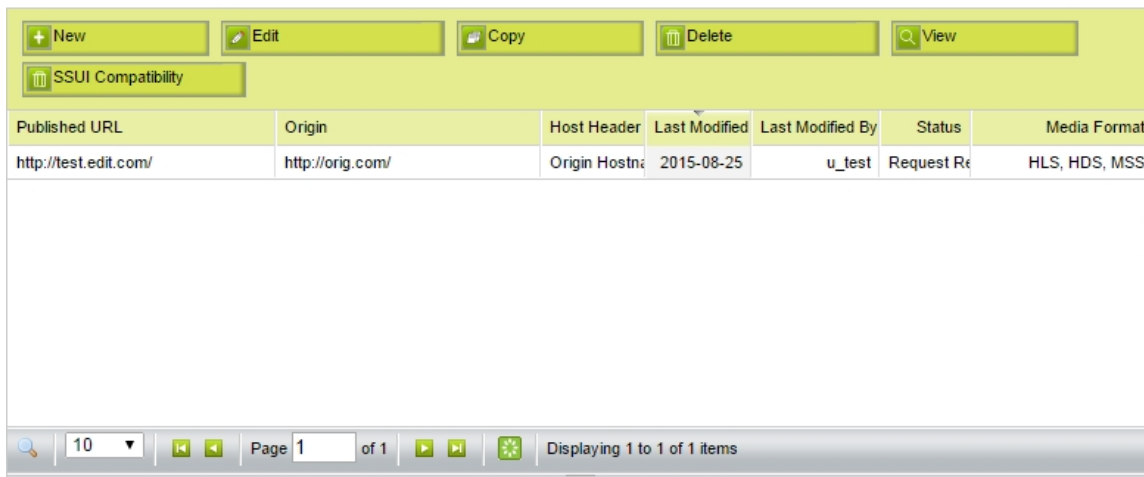
3. Click the **Activate** button.

Configuring Chunked Streaming v1

Chunked Streaming delivers chunked video content via HTTP and HTTPS in four different formats: HDS, HLS, MSS and MPEG-DASH. To use *Chunked Streaming*, you first need to chunk your content and generate the associated manifest files (*Chunked Streaming* does not perform these operations). You can host your content on your own origin servers or with *Origin Storage*.

Note: Chunked Streaming settings are read-only and will be removed in a future release. Please use Chunked Streaming (v2) instead.

When you select the **Chunked Streaming** option in the **Configure** menu, you'll see the *Configurations* page, with a list of your configurations.



Published URL	Origin	Host Header	Last Modified	Last Modified By	Status	Media Format
http://test.edit.com/	http://orig.com/	Origin Hostname	2015-08-25	u_test	Request Rejected	HLS, HDS, MSS

Figure 1. Configurations Page

The *Chunked Streaming Configurations* list provides the following information for each configuration:

- **Published URL** (Published Hostname) - The public URL prefix used in links to your published content (URLs seen by end users)
- **Origin** (Origin Hostname) - The private URL prefix used by Edgio to retrieve and cache content from your origin server (not visible to end users)
- **Host Header Value** - the value that Edgio will include in the HTTP Host header when making requests to your origin
- **Last Modified** - The date the configuration was last changed
- **Last Modified By** - The portal ID of the user who last changed the configuration
- **Status** - The processing status of the configuration:
 - **Pending** - The configuration has been submitted, but provisioning has not yet started
 - **In Progress** - The provisioning process has started
 - **Propagating** - The new provisioning configuration is available to all servers that need it, but is not fully deployed
 - **Complete** - The configuration was successfully deployed
 - **Failed** - The configuration was not successfully deployed - please contact Edgio Support for assistance
 - **Unknown** - The status of the configuration could not be determined - please contact Edgio Support for assistance
- **Media Format** - The media formats which the content is delivered in

Creating a New Configuration

To create a new configuration:

- In the *Chunked Streaming Configurations* list, select **New** from the buttons at the top of the list, and the first step of the configuration wizard will be displayed
- Complete each step as necessary, then click **Submit**

Wizard Step: Content Location

In order to fill the cache, the service needs to know where to get your content. In this step, you specify whether you are using CDN Storage or hosting your content outside of the Edgio infrastructure.

Figure 2. Content Location Step

Setting	Information Requested	Why It's Needed	Selecting the Right Option
Content Location	The location of the content you want the <i>Chunked Streaming</i> service to deliver (the "origin")	The <i>Chunked Streaming</i> service needs to know where to find your content when users first request it, and also when it needs to be refreshed in the cache	If your content is in <i>Origin Storage</i> or <i>Edgio Discrete Storage</i> , choose CDN Storage . Otherwise, choose Outside Edgio infrastructure .

Table 1. Content Location Settings

Note: If the **CDN Storage** option is unavailable, and you are already using CDN Storage, your service is not fully configured. If this is the case, please contact Edgio support.

Wizard Step: Basic Configuration

If you chose **CDN Storage** as your Content Location in Step 1, you'll see the following in the *Basic Configuration* step. Note that **Origin Hostname** is a drop-down menu that lists the available types of CDN Storage:

Basic Configuration

Protocol: HTTP | Published Hostname: www.one.example.com | Add Path

Origin Hostname: Limelight Cloud Storage | Add Path

Origin HTTP port number: 80

Host Header Value: Published Hostname, Origin Hostname, Other: www.one.example.com

Buttons: Done, Cancel, Back, Next

Figure 3. Basic Configuration Step - CDN Storage

If you chose **Outside Edge Server infrastructure** as your Content Location in the *Content Location* step, you'll see a slightly different view. Note that **Origin Hostname** becomes an editable field, and you can also select an **Origin Protocol**:

Basic Configuration

Protocol: HTTP | Published Hostname: www.one.example.com | Add Path

Origin Hostname: Limelight Discrete Storage | Add Path

Origin HTTP port number: [Empty]

Host Header Value: Published Hostname, Origin Hostname, Other: www.one.example.com

Closest POP to the Origin: None

Figure 4. Basic Configuration Step - Outside Edgio Infrastructure

Protocol

The **Protocol** drop-down menu controls the level of security used when delivering content to your users.

Setting	Information Requested	Why It's Needed	Selecting the Right Option
Protocol	The HTTP protocol(s) to use to when delivering your cached content to end users	To ensure your content is delivered with the level of security you require	<ul style="list-style-type: none"> To always deliver content insecurely, select HTTP To always deliver content securely (via SSL), select HTTPS To deliver content using the protocol specified in the incoming HTTP request, select Both HTTP and

Table 2. Protocol Settings

Published Hostname

The **Published Hostname** is the domain name used in all public links (Published URLs) to your cached content.

Setting	Information Requested	Why It's Needed	Selecting the Right Option
Published Hostname	The fully-qualified domain name that will be used in all links to your cached content	To direct your users to the service (instead of your origin)	Enter the published hostname specified in your Welcome Letter, or a CNAME if desired, in the Published Hostname field . . . Please note that IP addresses are not accepted. You must enter a fully-qualified domain name. If you want to use a directory name "alias" for a particular origin path, you can add the alias by clicking the Add Path link.

Table 3. Published Hostname Settings

Edgio will provide you with the correct **Published Hostname** in the *Welcome Letter* associated with your Limelight Account. By default, the **Published Hostname** will be in the form similar to:
accountname.vo.llnwd.net

If you prefer to publish a different hostname name, you can use a DNS CNAME record to alias (point) your desired name to the one provided by Edgio.

Origin Protocol

The **Origin Protocol** drop-down menu controls how content is requested from your origin (when the content is not found in cache or has expired in cache).

Setting	Information Requested	Why It's Needed	Selecting the Right Option
Origin Protocol	The HTTP protocol(s) to use when retrieving content from your origin	To ensure your content is retrieved with the level of security you require	<ul style="list-style-type: none"> To always retrieve content insecurely, select HTTP Always To always retrieve content securely (via SSL), select HTTPS Always To retrieve content using the protocol specified in the user's HTTP request, select Match Inbound Protocol

Table 4. Origin Protocol Settings

Origin Hostname

Note: this option appears only when you select **Outside Edgio Infrastructure** as your content location.

Setting	Information Requested	Why It's Needed	Selecting the Right Option
Origin Hostname	The fully-qualified domain name or IP address of your origin server	The <i>Chunked Streaming</i> service needs to know where to get your content when users first request it, and also when it needs to be refreshed in the cache	Enter the domain name or IP address of your origin server in the Origin Hostname field. Please note that if you enter a domain name, it must be fully qualified. If your content is all in particular path on your origin, or you added a directory name "alias" with the Published Hostname for a particular origin path, you can enter the origin path by clicking the Add Path link.

Table 5. Origin Hostname Settings

Origin HTTP port number

Origin HTTP Port Number is the web server port Edgio will use in association with your Origin Hostname. The default for HTTP is port 80, and this value is pre-filled in the **Origin HTTP Port Number** field. The default for HTTPS is 443, and this is the value used by Edgio for all HTTP requests to origin (the value is not editable).

Setting	Information Requested	Why It's Needed	Selecting the Right Option
Origin HTTP port number	The HTTP port number to use when communicating with your origin server	If you are using a port other than the default (80) for HTTP, the <i>Chunked Streaming</i> service needs to know which port you've chosen	Leave the default port number for HTTP unless you are using another port number. If so, enter the new port number in the Origin HTTP Port Number field.

Table 6. Origin HTTP Port Number Settings

Host Header Value

Host Header Value specifies the value that the service will include in the HTTP `Host` header when making requests to your origin.

Setting	Information Requested	Why It's Needed	Selecting the Right Option
Host Header Value	The value to include in the HTTP <code>Host</code> header when communicating with your origin server	To help prevent end users from requesting content directly from your origin.	If you plan to block requests to your origin based on the value of the <code>Host</code> header, select Published Hostname or enter a value in the Other field. If you chose Edgio Storage as your content location, the Host Header Value defaults to the Origin Hostname . Note: If you are hosting more than

one origin on a single server, please see the additional information below.

Table 7. Host Header Settings

Closest POP to Origin

Setting	Information Requested	Why It's Needed	Selecting the Right Option
Closest POP to the Origin	Whether the <i>Chunked Streaming</i> service should always request origin content using a specified group of Edgio POPs	In some cases, performance can be improved by specifying POPs	<p>This option is available only when configured by Edgio. Please consult Edgio Support if you are not sure which POP to choose.</p> <p>If you chose Edgio Storage as your content location, Closest POP to the Origin is preselected for best performance.</p>

Table 8. Closest POP to Origin Settings

Browsers usually include the origin domain name of the requested URL in the HTTP Host header. You can use this behavior to detect and block such requests on your origin, denying those with a Host header that matches your domain name, and accepting those that match either your **Published Hostname** or another value you enter in the **Other** field.

If you are hosting more than one origin on a single server and you want to block based on Host headers, don't use **Published Hostname** - enter a value in the **Other** field instead. If you are hosting more than one origin on a single server and you don't want to block based on Host headers, choose **Origin Hostname**.

Example Settings

Configuration Field	Value	Notes
Protocol	HTTPS	Accept only HTTPS requests for cached content
Published Hostname	published.host.com	Use a CNAME alias instead of the name provided in the Welcome Letter (need to set up the CNAME separately)
Add Path	/pubimages/	Use the pubimages directory to uniquely identify the content in cache
Origin Protocol	HTTP Always	Always use HTTP to communicate with the origin server
Origin Hostname	origin.host.com	
Add Path	/images/	Directory path to the origin content; note that this doesn't need to match the path (if any) for the Published Hostname
Origin HTTP port number	80	Use the default HTTP port (no need to change anything)

Host Header Value	Published Hostname	This will block most browser requests made directly to origin
--------------------------	--------------------	---

Table 9. Example Settings

Using the example configuration settings above, if `favicon.ico` is not cached for this configuration, or has expired in cache, a request to `https://published.host.com/pubimages/favicon.ico` will result in an origin request for `http://origin.host.com/images/favicon.ico`, with an HTTP Host header of `published.host.com`.

Object	Incoming Request	Origin Request
<code>favicon.ico</code>	<code>https://published.host.com/pubimages/favicon.ico</code>	<code>http://origin.host.com/images/favicon.ico</code> Host: <code>published.host.com</code>

Table 10. Example Response

Wizard Step: Basic Cache

Basic Cache Rules

Honor Origin Cache-Control and Expires headers ⓘ
 Override Origin Cache-Control header and TTL values ⓘ

Figure 5. Basic Cache Step - Honor Origin Settings

Basic Cache Rules

Honor Origin Cache-Control and Expires headers ⓘ
 Override Origin Cache-Control header and TTL values ⓘ

Time to live (TTL)

Cache Generated Responses

Specify custom floor and ceiling cache values ⓘ

Min: Max:

Figure 6. Basic Cache Step - Override Origin Settings

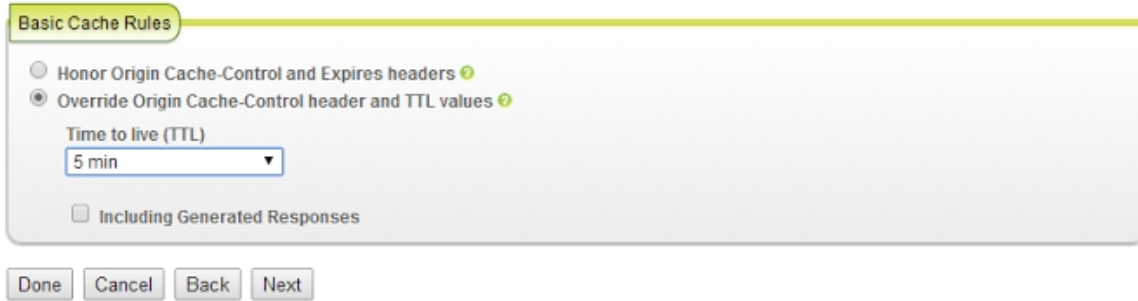


Figure 7. Basic Cache Step - Override Origin Settings - Custom TTL

Setting	Information Requested	Why It's Needed	Selecting the Right Option
Basic Cache Rules	Whether to override the default method for determining if an object in cache is expired	In some cases you may want to take explicit control over object expiration times (TTL - "Time To Live").	<p>To allow Chunked Streaming to calculate TTL, select Honor Origin Cache-Control and Expires headers . Otherwise, choose Override Origin Cache-Control header and TTL values . If you want to set TTL to a specific length of time, select one of the times in the Time To Live (TTL) drop-down menu. Otherwise, to allow adaptive TTL calculation, select Custom from the Time To Live (TTL) drop-down menu.</p> <div style="border: 1px solid green; padding: 5px; background-color: #e6f2e6;"> <p>Note: TTL values set in this step are applied to all content under the Published URL, except for chunks and manifest files - TTLs for these are set individually in the Media Delivery step. In particular, TTL values set in this step apply to Cross Domain (<code>crossdomain.xml</code>) and Client Access Policy (<code>clientaccesspolicy.xml</code>) files, which should be in the root directory of the Published URL.</p> </div>

Table 11. Basic Cache Settings

Use the **Honor Origin Cache-Control and Expires headers** setting unless you have a specific reason to override the way in which object Time To Live (TTL) is calculated.

By default, *Chunked Streaming* considers an object “stale” (expired from cache) if the number of seconds specified by the associated `Cache-Control: s-maxage` or `Cache-Control: max-age` header has elapsed since initial caching or since the last freshness check, or if neither header is present, if the date and time in the Expires header has passed. The order of precedence is `Cache-Control: s-maxage` , `Cache-Control: maxage` , then Expires.

If no explicit freshness information is supplied (there are no `Cache-Control: s-maxage` , `Cache-Control: max-age` or Expires headers), and a Last-Modified header is present, the CDN will by default use the adaptive cache freshness algorithm to calculate remaining TTL, based on 20% of the age of the cached response, subject to a floor of 3 seconds and a ceiling of 3 days.

If you need to override (ignore) the above behavior, you can use the **Override Origin Cache-Control header and TTL values** option to specify a new TTL value using the **Time to live (TTL)** drop-down menu.

You can also control whether generated responses are cached using the **Cache Generated Responses** checkbox (for the **Custom** option) or **Including Generated Responses** (for other values in the drop-down menu).

Note:

Generated responses are HTTP responses that are generated dynamically (“dynamic content”). These responses often do not include any of the cache control headers needed to determine TTL, and are not cached by default to avoid caching personalized or user-specific responses.

By default, Edgio defines a generated response as one that is missing all of the following headers:

- Expires
- Last-Modified
- Cache-Control: max-age
- Cache-Control: s-max-age

If you choose the **Custom** option for **Time to live (TTL)**, you can change the parameters of the cache freshness algorithm using **Specify custom floor and ceiling cache values**.

If desired, the floor (minimum) can be raised and the ceiling (maximum) can be lowered or raised. If min and max are set equal to each other, the TTL becomes explicit, rather than adaptive.

Wizard Step: Media Delivery

Step 1
Content Location

Step 2
Basic Configuration

Step 3
Basic Cache

Step 4
Media Delivery

Step 5
Advanced Cache

Step 6
Logging

Step 7
Failover

Step 8
Additional Options

Step 9
Review

[Revision History](#)

Media Delivery

Delivery Mode

Live OnDemand

HDS

HDS Live

Chunks TTL

Manifest TTL

HLS

HLS Live

Chunks TTL

Manifest TTL

MSS

MSS Live

Chunks TTL

Min

Max

Manifest TTL

MPEG-DASH

click to select

Chunks TTL

Manifest TTL

HDS manifest and chunks file extensions

HLS manifest and chunks file extensions

MSS manifest and chunks file extensions

MPEG-DASH manifest and chunks file extensions

Done
Cancel
Back
Next

Figure 8. Media Delivery Step

Setting	Information Requested	Why It's Needed	Selecting the Right Option
Delivery Mode	Whether your configuration is for live video streams, or for video files available at any time (on demand)	To properly configure manifest file cacheability	Choose Live if you are delivering live streams, or On Demand for files that can be accessed at any time.
HDS / HLS / MSS / MPEG-DASH	The video formats to use when delivering your content	To properly configure optimizations for each format	Select each format (HDS , HLS , MSS or MPEG-DASH) that you want to deliver, based on the requirements of your video client.
Chunks TTL	The amount of time each chunk will be cached	In some cases you may want to take explicit control over object expiration times (TTL - "Time To	If the TTL provided by your origin is correct, use the default Honor Origin TTL setting. Otherwise, choose a specific TTL value (2 minutes to 60 days), or select Custom to set both the minimum and maximum TTL.

		Live”)																	
Manifest TTL	The amount of time the manifest will be cached	In some cases you may want to take explicit control over object expiration times (TTL - “Time To Live”)		If the TTL provided by your origin is correct, use the default Honor Origin TTL setting. Otherwise, choose a specific TTL value (2 minutes to 60 days), or select Custom to set both the minimum and maximum TTL.															
manifest and chunks file extensions	The file extensions you used for manifest files and content chunk files, for each media type you selected	The <i>Chunked Streaming</i> service needs this information to function properly		Please use the file naming rules below for manifest and chunk files. These formats must be followed for the <i>Chunked Streaming</i> service to work properly:															
				<table border="1"> <thead> <tr> <th></th> <th>Chunks</th> <th>Manifest</th> </tr> </thead> <tbody> <tr> <td>HDS</td> <td>use Seg/Frag annotation in the file names</td> <td>use one of the following file extensions: bootstrap, drmmeta, f4m, f4x</td> </tr> <tr> <td>HLS</td> <td>use one of the following file extensions: aac, mp3, ts</td> <td>use one of the following file extensions: m3u, m3u8</td> </tr> <tr> <td>MSS</td> <td>include the keyword QualityLevels in the URL</td> <td>include either Manifest or manifest as a keyword in the URL</td> </tr> <tr> <td>MPEG-DASH</td> <td>use the dash file extension</td> <td>use the mpd file extension</td> </tr> </tbody> </table>		Chunks	Manifest	HDS	use Seg/Frag annotation in the file names	use one of the following file extensions: bootstrap, drmmeta, f4m, f4x	HLS	use one of the following file extensions: aac, mp3, ts	use one of the following file extensions: m3u, m3u8	MSS	include the keyword QualityLevels in the URL	include either Manifest or manifest as a keyword in the URL	MPEG-DASH	use the dash file extension	use the mpd file extension
	Chunks	Manifest																	
HDS	use Seg/Frag annotation in the file names	use one of the following file extensions: bootstrap, drmmeta, f4m, f4x																	
HLS	use one of the following file extensions: aac, mp3, ts	use one of the following file extensions: m3u, m3u8																	
MSS	include the keyword QualityLevels in the URL	include either Manifest or manifest as a keyword in the URL																	
MPEG-DASH	use the dash file extension	use the mpd file extension																	

Table 12. Media Delivery Settings

Wizard Step: Advanced Cache

Advanced Cache

Advanced Cache

Ignore objects with Vary headers ?
 Ignore all Vary headers when caching ?
 Ignore specific Vary headers ?

Specific Query String Caching: ?

Strip no query terms from the cache key
 Strip all query terms from the cache key
 Exclude specific query terms
 Keep only specific query terms

Partial Cache ?
 N Byte Download ?

Figure 9. Advanced Cache Step - Advanced Cache Controls

Setting	Information Requested	Why It's Needed	Selecting the Right Option
Vary Headers	Which Vary response header fields <i>Chunked Streaming</i> should use when differentiating versions of an object in cache	<p><i>Chunked Streaming</i> stores a separate version of a requested object for each unique set of request header fields specified by the Vary header.</p> <p>If the Vary header specifies request header fields that change frequently, multiple copies of the same object may be stored in cache.</p> <p>To control this behavior, you can configure <i>Chunked Streaming</i> to ignore all Vary headers or specific Vary headers when caching and retrieving objects.</p> <p>All of the Vary headers associated with the object are still maintained and passed on to the client in the response.</p>	<ul style="list-style-type: none"> If you only want to cache a single version of an object regardless of its Vary header fields, choose ignore objects with Vary headers If you want to cache a new version of an object whenever any of its Vary header fields changes, choose ignore all Vary headers when caching If you want to cache a new version of an object whenever all but certain specified Vary header fields change, choose ignore specific vary headers and select the Vary headers fields to ignore

Table 13. Advanced Cache Settings

Optimization

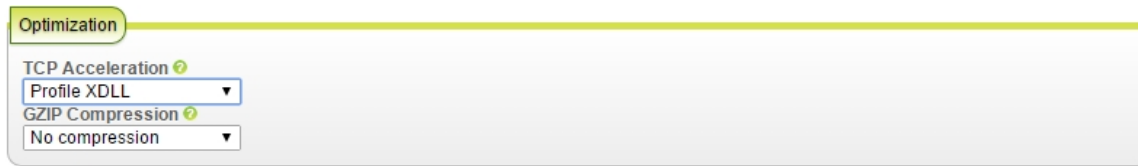


Figure 10. Advanced Cache Step - Optimization Controls

Setting	Information Requested	Why It's Needed	Selecting the Right Option
TCP Acceleration	The “profile” to use when accelerating the transfer of IP packets by modifying default TCP parameters	In certain circumstances, you may want to change the TCP Acceleration profile to optimize your delivery performance	<p>When TCP Acceleration is enabled, the XDLL profile is the most efficient in many cases.</p> <div style="border: 1px solid green; padding: 5px; background-color: #e6f2e6;"> <p>Note: TCP Acceleration is an advanced configuration setting, and should only be changed if you're an expert user.</p> </div>
Gzip Compression	Whether to use Gzip compression when delivering XHTML, JavaScript, CSS, and other text files	Compressed objects are delivered more quickly, potentially improving the user experience	<ul style="list-style-type: none"> • If you want to provide all compressed files from your origin server, choose the Gzip Passthrough option. • If you prefer to have the <i>Chunked Streaming</i> service compress files when the requesting client can accept them, choose Gzip on-the-fly. • If you need to modify Gzip compression defaults, choose Custom, then either Gzip on-the-fly or Gzip Passthrough, and enter your Gzip modification extensions • You can also choose No compression if none of your files should be delivered compressed. <p>For more information on this feature, see Gzip Details.</p> <div style="border: 1px solid green; padding: 5px; background-color: #e6f2e6;"> <p>Note: Compression cannot be applied to chunks.</p> </div>

Table 14. Optimization Settings

Gzip Details

When **Gzip Passthrough** is enabled, and a client indicates (via HTTP request header) that it prefers to receive compressed content, the *Chunked Streaming* service will serve a compressed version of the requested object if one is available on the origin server.

Note: *Gzip Passthrough* is available to all customers. If it is not enabled for you, please contact EdgioSupport.

If **Gzip On-the-fly** is selected, the *Chunked Streaming* service creates, caches, and delivers Gzip-compressed content as needed.

Compressible file types include: action, ashx, asmx, asp, aspx, axd, cfm, css, css3, csv, do, doc, docx, htm, html, js, jsf, json, jsp, php, portal, rtf, svg, svgz, tsv, txt, xhtml, xml, site root (/), and extensionless URLs.

Request and Response Headers

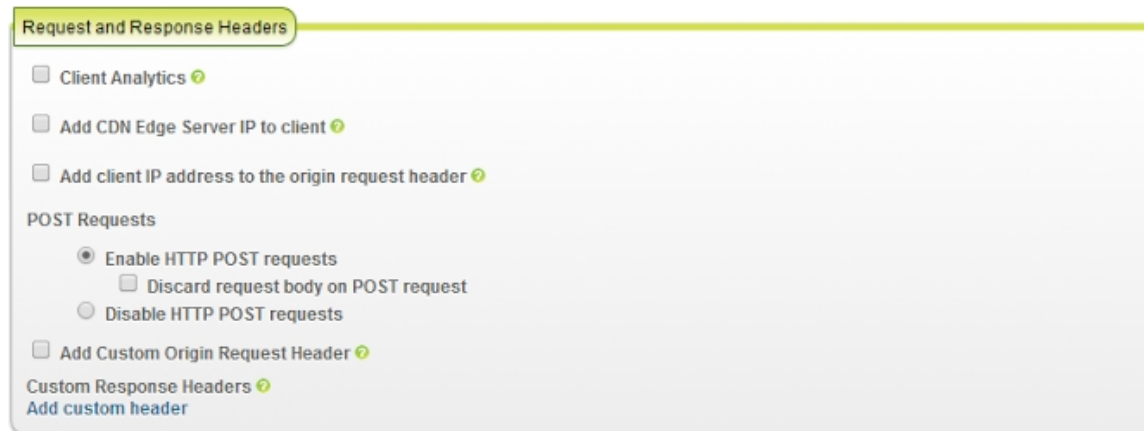


Figure 11. Advanced Cache Step - Header Controls

Setting	Information Requested	Why It's Needed	Selecting the Right Option
Client Analytics	Whether you want the <i>Chunked Streaming</i> service to provide geographic user information when requesting content from your origin	You may want to internally capture, analyze and report on user geographic information.	To use this feature, check the Client Analytics checkbox. The geo information is provided to your origin server via two request headers: X-IP-Geo-Country and X-IP-Geo-All. The geo fields provided are continent, country, state, city, dma_id and asn.
Add CDN Edge Server IP to client	Whether to provide clients with the IP address of the	If you are using a custom client to display content, and you are also capturing performance-related	To enable this feature, check the Add CDN Edge Server IP to client checkbox

	<i>Chunked Streaming</i> Edge Server responding to their requests	data via the client, you may want to include the <i>Chunked Streaming</i> Edge Server IP address for later analysis and reporting. The IP address will be provided in the X-IP-Address response header.	
Add client IP address to the origin request header	Whether you want the <i>Chunked Streaming</i> service to provide the requesting client's IP address in a custom header when requesting content from your origin	You may want to internally capture, analyze and report on user IP information	To enable this feature, check the Add CDN Edge Server IP to client checkbox, and enter the header name(s) that should contain the client IP address. The default header name is True-Client-IP . Note that the above headers are in addition to X-Forwarded-For , which is always provided to the origin.
POST Requests	Whether you want to accept or ignore POST requests from clients	If you are using a custom client to display content, you may want to allow it to communicate analytics or other information to your origin. Alternatively, you may want to convert POST requests to GET requests, or simply ignore them.	<ul style="list-style-type: none"> To ignore all POST requests, select Disable HTTP POST requests . <i>Chunked Streaming</i> will respond with an HTTP 413 "Request Entity Too Large" status code to all POST requests. To accept POST requests and pass them through to your origin, select Enable HTTP POST requests . If a POST request body exceeds 500 MB, <i>Chunked Streaming</i> will respond with an HTTP 413 "Request Entity Too Large" status code. To accept POST requests but treat them as GET requests, select Enable HTTP POST requests, and check the Discard request body on POST request checkbox. POST bodies will be discarded.
Custom Request Headers	Whether you want to include custom headers and values whenever <i>Chunked Streaming</i> makes a request to your origin	If you want to tag all requests from <i>Chunked Streaming</i> for later analysis	To add a custom origin request header, click the Add custom header link, and enter a unique header name and value

Custom Response Headers	Whether you want to include custom headers and values whenever <i>Chunked Streaming</i> responds to a client request	If you are using a custom client to display content, you may want to provide it with information that uniquely identifies the <i>Chunked Streaming</i> service, Limelight Account, etc.	To add a custom client response header, click the Add custom header link, and enter a unique header name and value
--------------------------------	--	---	---

Table 15. Header Settings

Progressive Video Download

Note : Progressive Video settings are displayed only when necessary for compatibility with legacy configurations.

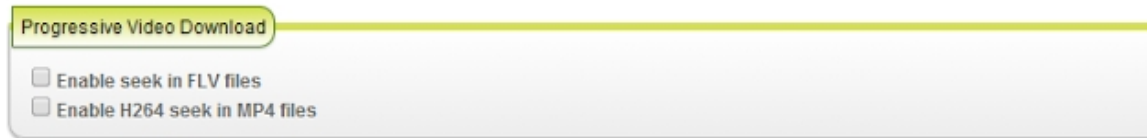


Figure 12. Advanced Cache Step - Progressive Video Download Controls

Setting	Information Requested	Why It's Needed	Selecting the Right Option
Enable seek in FLV files	Whether to allow video client to skip forward and back (seek) within FLV files based on parameters specified in the query terms of the request URL.	Custom clients may want to provide the “seek” capability (“forward” and “back” buttons)	To enable this feature, check the Enable seek in FLV files checkbox
Enable H264 seek in MP4 files	Whether to allow video client to skip forward and back (seek) within MP4 files based on parameters specified in the query terms of the request URL.	Custom clients may want to provide the “seek” capability (“forward” and “back” buttons)	To enable this feature, check the Enable H264 seek in MP4 files checkbox

Table 16. Progressive Video Download Settings

Content Security

Figure 13. Advanced Cache Step - Content Security Controls

Setting	Information Requested	Why It's Needed	Selecting the Right Option
Enable IP Blocking	Whether you want to allow or deny access to your content by geographic region or named IP list	You may need to limit the audience for your content to certain regions to meet licensing restrictions, or exclude certain regions that are outside your target audience.	<p>Once you have determined which geographies you want to manage, begin typing the name of a continent or country in the desired field (Allow access or Deny access). As you type, a pop-up list will display available choices that match your entry.</p> <p>If named IP lists have been created for your Account, you can also enter those names in the fields.</p> <p>If you need to provide the video client with an error code when access is blocked, enter an integer code in the Deny Status Code field.</p>
Enable MediaVault content protection	Whether you want to use to provide additional content security. provides high-performance cookie-based URL authentication.	<i>MediaVault</i> can help you prevent “deep linking” and other unauthorized viewing behavior	<p>To enable this feature, check the Enable MediaVault content protection checkbox, and provide a primary and secondary “shared secret” (both used to prevent URL tampering).</p> <p>If you need to provide different shared secrets for each media format, uncheck the Same hash secrets for all formats checkbox. Separate fields will then be</p>

			displayed for each media format. For more information, see Details
--	--	--	---

Table 17. Content Security Settings

MediaVault Details

MediaVault is a high-performance URL authentication service. MediaVault's main purpose is to help you secure your content from unauthorized viewing.

MediaVault maximizes authentication performance by using tokens to avoid three-way handshakes (common to other methods of authentication) that can lead to severe connection time latency.

Please note that MediaVault is *not* a replacement for DRM and should not be associated with user authentication.

MediaVault works like this:

- You enter a shared secret during the configuration process
- You then generate a token (MD5 hash) for each published URL, based on the shared secret, and append it to the URL in a query term or provide it in a cookie. You can generate the token manually by navigating to the *Configure > MediaVault* in the navigation pane, or by creating server-side code on your origin.
- When a request is received, MediaVault uses the same hash algorithm to create it's own token, which should be identical to the one you appended.
- If the tokens match, MediaVault then looks for additional MediaVault-specific query terms (such as end date/time and IP address/mask) to determine whether the request is valid. If the tokens don't match, the URL was tampered with and the request is rejected.

For more information, see the MediaVault User Guide by navigating to Help Center > Documentation > Delivery > Guides > MediaVault in the navigation pane.

Wizard Step: Logging



Figure 14. Logging Step Controls

Setting	Information Requested	Why It's Needed	Selecting the Right Option
Do not log cookies in log file	Whether you want <i>Chunked Streaming</i> to <i>stop</i> saving cookie information in your log files	If you process log files and don't need the information in the Cookie header, you may want to remove it to simplify processing and/or reduce log file size.	If you know you <i>don't need</i> Cookie header information in your log files, check the Do not log cookies in log file checkbox. Otherwise, leave it unchecked.
Log Request	Whether you want <i>Chunked Streaming</i>	If you process log files and need access to information in the	If you know you <i>do need</i> Request Header information in your log files, check the Log

Header	to <i>start</i> saving specific Request Headers in your log files	Request Headers, you may want to enable this option	Request Header checkbox and enter the names of the specific headers to log. Otherwise, leave it unchecked.
---------------	---	---	---

Table 18. Logging Settings

Chunked Streaming normally logs all Cookie header information, up to a maximum of 8 KB for the entire header (regardless of the number of cookies in the header).

Wizard Step: Failover

The screenshot shows a wizard interface for failover settings. It is divided into two main sections: "404 Handling" and "Origin Server Error (5xx)".

- 404 Handling:**
 - Serve stale content** (with a help icon)
 - Request content from an alternate hostname** (with a help icon). Below this is a text input field for "Hostname:" containing "www.one.example.com".
 - Object not available URL** (with a help icon). Below this is a text input field for "URL:" containing "http://test.example.com/test.html".
- Origin Server Error (5xx):**
 - Request content from an alternate hostname** (with a help icon). Below this is a text input field for "Hostname:" containing "www.one.example.com".
 - Service not available URL** (with a help icon). Below this is a text input field for "URL:" containing "http://test.example.com/test.html".

At the bottom of the wizard, there are four buttons: "Done", "Cancel", "Back", and "Next".

Figure 15. Failover Step Controls

Normally, when the CDN receives a 404 response from the origin, it is passed back to the requesting client. With the **Serve stale content** option, if there is cached content for a given request and the origin returns a 404, the Edge Server returns the stale content instead of issuing a 404 to the client.

Object not available URL specifies a URL to be used for content retrieval instead of sending a 404 response code to the client. The original request is reissued to the fallback URL with any modifications still in place. The option is used to provide a custom "not found" message or to provide instructions to retry the request. Any URL used for this option must match its own configuration within the CDN.

Service not available URL specifies a URL to return instead of sending a 503 (Service Unavailable) or 504 (Gateway Timeout) response. The 503 or 504 may have been generated by the origin, but could also be internally generated by CDN should a connection failure to origin occur. Any URL used for this option must match its own configuration within the CDN.

Setting	Information Requested	Why It's Needed	Selecting the Right Option
Serve Stale Content	If the requested content is cached but stale (expired), and there is an HTTP 404 status when requesting a fresh version from your origin, whether you want to pass the 404 status back to the client, or serve the stale content instead	If an object has expired in cache, and your origin server returns a 404 (Page Not Found) error when <i>Chunked Streaming</i> attempts to get a fresh copy of the object, you may want to serve the expired object instead of allowing the client to handle the 404 message.	If it's not acceptable for the client to handle the 404 message, and you are OK with serving stale content instead, check the Serve Stale Content checkbox. Note that if there is no cached object, a 404 message will still be returned to the browser.
Request content from an alternate hostname	If there is an HTTP 404 status when requesting fresh content from your origin, whether to try a backup origin before handling the 404 status	If your primary origin returns a 404 status, and you have a backup origin, you may want <i>Chunked Streaming</i> to try the backup before handling the error	To try a backup origin if the primary origin responds with a 404 status, enable Request content from an alternate hostname and enter the fully-qualified hostname of the backup origin. Note that specific ports are not supported.
Object not available URL	Whether you want to pass HTTP 404 status messages back to the client, or serve a custom error page instead	If an object has expired in cache, and your origin server returns a 404 error to <i>Chunked Streaming</i> , you may want to serve a custom error page instead of allowing the client to handle the 404 message.	If you want to take control over the content displayed by clients when there is a 404 from origin, check the Object not available URL checkbox, and enter the fully-qualified URL of the content to serve.
Request content from an alternate hostname	If there is an HTTP 5xx status when requesting fresh content from your origin, whether to try a backup origin before handling the 5xx status	If your primary origin returns a 5xx status, and you have a backup origin, you may want <i>Chunked Streaming</i> to try the backup before handling the error	To try a backup origin if the primary origin responds with a 5xx status, enable Request content from an alternate hostname and enter the fully-qualified hostname of the backup origin. Note that specific ports are not supported.
Service not available URL	Whether you want to pass HTTP 503 and 504 status messages back to the client, or serve a custom error page instead	If an object has expired in cache, and your origin server returns a 503 (Service Unavailable) or 504 (Gateway Timeout) error to <i>Chunked Streaming</i> , you may want to serve a custom error page instead of allowing the client to handle the 5xx message.	If you want to take control over the content displayed by clients when there is a 503 or 504 error from origin, check the Service not available URL checkbox, and enter the fully-qualified URL of the content to serve.

Table 19. Failover Settings

Wizard Step: Additional Options



Figure 16. Additional Options Step (Read Only)

You can use the **Additional Options** step to view any advanced configuration changes Edgio makes to your configuration.

If one or more such configurations is changed from its default value by Edgio, the **Additional Options** tab becomes visible, and the advanced configurations and their settings are displayed:

Setting	Information Requested	Why It's Needed	Selecting the Right Option
(various)	(none) This is a read-only display of advanced <i>Chunked Streaming</i> configuration changes Edgio has made to your configuration	The information in the Additional Options step can help you better understand your configuration.	If you have questions about any settings in Additional Options, please contact your Account Manager or Edgio support.

Table 20. Additional Options Settings (Read Only)

The advanced configuration options which can be configured for you by Edgio (and become visible in the *Additional Options* step) include:

Option Name	Description
Assume cacheable pending origin response	If an origin request is pending for an object, continue serving the object from cache
Cache entire object if range request less than offset	Cache the entire object for Range requests ending before the specified Byte offset
Cache hit/miss response trigger	Returns HIT or MISS in the X-CDN-Cache response header when the specified request header (trigger) is present
Cache only "popular" objects	Cache only objects that are "popular" based on the specified "points" (the approximate frequency an object is requested, in seconds)
Convert URL ranges to Range requests	Convert URLs ending in /range/x-y or /range/x- to origin GET range requests

Deny requests with specified Referrer header(s)	Deny requests with the specified Referrer header(s)
Disable object caching	Do not cache objects
Disable persistent origin connections	Disable persistent origin connections (“enabled” is the default global configuration)
Do not add max-age on all requests to origin	Don’t add Cache-Control: max-age=259200 header on origin requests (but do include any existing Cache-Control headers)
Enable partial caching by regex	Enable partial caching for object URLs that match the specified regex
Gzip compression level	Set the Gzip compression level (0 to 9). The default (and recommended) level is 1.
Ignore bad status codes from origin	Ignore bad status codes from origin (40x and 5xx). If FALSE, other rewrite options may redirect the client to specific URLs based on the status code.
Lowest allowed rate-limiting bitrate	Set the lowest bitrate allowed when rate limiting, in KBytes/second
Make cached URLs case-insensitive	Make the URLs of cached objects case-insensitive by converting all characters to lowercase in the Cache Key. When using this feature, all Purge requests must not contain any uppercase characters.
Max duration client can be idle while receiving response	After this time passes, the client is disconnected and the request is aborted. The default is 30 minutes.
Maximum object TTL	Set the maximum TTL value for all cached objects, in seconds, but honor Cache-Control headers if present
Minimum object TTL	Set the minimum TTL value for all cached objects, in seconds, but honor Cache-Control headers if present
Object TTL for “negative” origin response	Set the object TTL, in seconds, when there is a negative origin response (status codes other than 200, 203, 300, 301 and 401 and/or Cache-Control or Pragma headers with certain values). This rewrite overrides other origin cache control headers.
Origin connect timeout duration	Set the timeout, in seconds, for initiating origin connections (how long to wait when trying to establish a connection)
Origin reply timeout duration	Set the timeout, in seconds, for origin replies (how long to wait for a reply from origin)
Persistent client connection duration	Set the duration, in seconds, of persistent client connections
Persistent origin connection duration	Set the duration, in seconds, of persistent origin connections
Redirect clients to source URL	Redirect clients to the source URL with the specified status code
Refresh-check cached content on every request	Check for fresh origin objects (newer versions of objects) on every request. Most commonly used in conjunction with <i>Ignore bad status codes from origin</i> to enable the origin to allow or deny every request by inspecting all request parameters, including Cookies.
Remove specified response header(s)	Remove origin response headers that match the specified value
Retry failed <i>MediaVault</i> HTTPS hash	If an HTTPS <i>MediaVault</i> hash check fails, retry the same hash-check URL using HTTP

checks	
Store <i>MediaVault</i> hash in cookie	Keep the <i>MediaVault</i> hash secret in a browser cookie (rather than in a URL parameter)
Treat empty responses with 200 status as 404 status	Treat “empty” origin responses (no content body) with 200 status codes as if they are 404 status codes

Table 21. Additional Options Available

Wizard Step: Review

The Review step is the final step in the configuration process, and gives you an opportunity to confirm you’ve made the changes you intended before submitting your configuration.

Setting	Information Requested	Why It’s Needed	Selecting the Right Option
(all changes from previous steps)	Review and approve the changes you made in previous steps	To confirm you’ve changed the settings you expected	Click Submit to save your settings in a new configuration. Click Back to make changes to previous steps, or Cancel to discard all of your unsaved settings.
Notes	Optional notes that you can refer to later when browsing historical configuration changes	You may find it helpful to include additional information for others (why the configuration changes were made, etc.)	If you want to save notes with your configuration, just enter them in the Notes field
Revision History	Optional. Limited availability.	You can review all of your previous configuration changes, and “roll back” to any previous state if desired	This feature is accessible via the “Revision History” link in any wizard step

Table 22. Review Fields

Revision History Details

If you select the “Revision History” link in any wizard step, you can now review all of your previous configuration changes, and roll back to any previous state.

The configuration version number, creation date/time, submitting user, and any notes entered in the Review step are displayed for each historical change

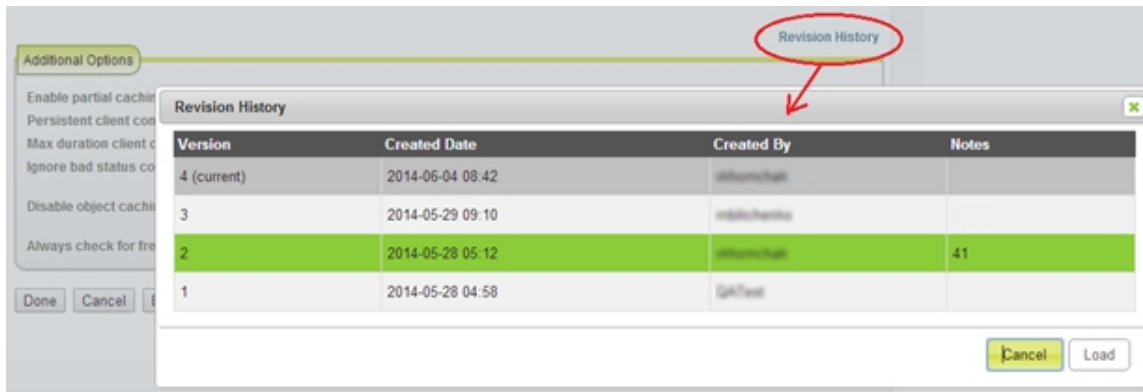


Figure 17. Revision History link and pop-up dialog with historical configuration versions

Selecting a version loads its settings into the configuration wizard and displays an alert above the wizard tabs to make it clear that a historical configuration is loaded.

As with any configuration changes, clicking **Submit** in the *Review* step will save the configuration, and clicking **Cancel** will discard the changes.

Editing a Chunked Streaming Configuration

To **Edit** a configuration:

- In the main menu, select **Configure**, select **Chunked Streaming**, choose a configuration to edit from the *Chunked Streaming Configurations* list, and then click **Edit**. The first step of the configuration wizard will appear.
- Configure each step as necessary then click **Submit**. For more information on the contents of each step, see [Creating a New Configuration](#).

Copying a Chunked Streaming Configuration

To **Copy** a configuration:

- In the main menu, select **Configure**, select **Chunked Streaming**, choose a configuration from the *Chunked Streaming Configurations* list, and then click **Copy**. The first step of the configuration wizard will appear.
- Configure each step as necessary then click **Submit**. For more information on the contents of each step, see [Creating a New Configuration](#).

Note: All configuration options are copied, including those visible only in the *Additional Options* step. In the simplest case, you may only need to change the **Published Hostname** field in the *Basic Configuration* step.

Deleting a Chunked Streaming Configuration

To **Delete** a configuration:

- In the main menu, select **Configure**, select **Chunked Streaming**, choose a configuration from the *Chunked Streaming Configurations* list, and then click **Delete**. The *Please confirm the delete request* dialog appears.
- Type DELETE in the space provided to permanently delete the selected record and the configuration is deleted.

Viewing a Chunked Streaming Configuration

To **View** a configuration:

- In the main menu, select **Configure**, select **Chunked Streaming**, choose a configuration from the *Chunked Streaming Configurations* list, and then click **View**.