Edgecast

Web Services REST API

edgecast

Disclaimer

Care was taken in the creation of this guide. However, Edgecast cannot accept any responsibility for errors or omissions. There are no warranties, expressed or implied, including the warranty of merchantability or fitness for a particular purpose, accompanying this product.

Trademark Information

EDGECAST is a registered trademark of Edgecast Inc.

About This Guide

Web Services REST API

Version 7.40

6/2/2022

Table of Contents

Web Services REST API

Introduction

Our Web Services REST API provides the means through which you can extend your own technologies with the capabilities of our CDN. This allows you to programmatically integrate our CDN with other programs, interfaces, or applications for the purpose of automating the manner through which your media is managed.

Our Web Services consist of a REST-compliant API that operates through HTTPS requests and responses. The HTTPS request and response bodies must be formatted using either JavaScript Object Notation (JSON) or Extensible Markup Language (XML). This type of framework allows you to use your preferred programming language (e.g., C#, C, PHP, Perl, etc.) to perform operations on our CDN through HTTPS requests to a Web Services REST API server.

The security of the communication between your application and a Web Services REST API server is ensured through Secure Sockets Layer (SSL) encryption. The Web Services REST API also protects against unauthorized operations through a user account-specific token.

Change History

A summary of the major changes performed to this document can be viewed from the REST API Help Center at:

- What's New?

Authentication and Authorization

Only authenticated requests to the REST API will be processed. This authentication process serves the following two purposes:

1. Identifies the user making the request.

2. Verifies that the user making the request has sufficient permissions to perform the requested action.

User authentication requires passing a unique value (i.e., token). The type of token that may be used to authenticate your requests varies according to whether the service is hosted on our API gateway.

- **api.edgecast.com:** Requests to api.edgecast.com leverage a REST API token.

  Note: Please contact your CDN administrator to request access to our REST API service. Upon approval, you will be allowed to generate and view tokens.

- **API Gateway (api.vdms.io):** Requests to our API gateway require a token generated from your OAuth 2.0 credentials. By default, this type of token expires after 300 seconds.

  Important: Register your client application via the Identity dashboard (https://manage.vdms.io/) to generate OAuth 2.0 credentials through which you may authorize requests submitted to our API gateway (api.vdms.io).

  Note: Use OAuth 2.0 credentials to authorize requests to Report Builder, RTLD WAF, and most Rules Engine endpoints.

REST API Token

Note: Use OAuth 2.0 credentials to authorize requests to Report Builder, RTLD WAF, and most Rules Engine endpoints. Requests to these endpoints cannot be authorized via a REST API token.

A REST API token is a unique alphanumeric value that identifies the user account through which the requested task will be performed. This ensures that only endpoints that have been authorized for that user account will be successfully completed.

A sample token value is shown below.

```
12345678-1234-1234-1234-1234567890ab
```

A REST API token is required to authenticate a REST API request. Generate and view your unique token(s) from the **Web Services REST API Token** section of the **My Settings** page.

Key information:

- The **Web Services REST API Token** section will not be displayed on that page when the current user account does not have sufficient privileges to use the REST API. Please contact a CDN administrator.

- **Administrator:** A CDN administrator defines each user's level of access to the REST API.

Generating a REST API Token

As a best practice, the REST API token should be updated at regular intervals. The recommended method for updating a REST API token involves the following steps:

1. Navigate to the **My Settings** page.

2. Click **Edit**.

3. Click **Generate New Primary**. When prompted, click **OK** to confirm this action.

4. From your preferred email client, open the verification email and then follow the verification link. The current primary token will be set as a backup token.

   Note: Both primary and backup tokens provide the same level of access to the REST API.

5. Update existing applications to use the new token value.

6. Delete the backup token.

   Tip: It is highly recommended that the backup token only be used to transition your existing applications to the new primary token.

   Note: Tokens that are no longer listed on the **My Settings** page cannot be used to authenticate to a REST API service.

Authenticating Requests

Setting up REST API request authentication requires setting the Authorization request header to your REST API token using the following syntax:

TOK: *Token*

Key information:

- The term "TOK:" and the token value are not case-sensitive.

- An optional space character may separate the term "TOK:" and the token value.

- A request will not be authorized under the following conditions:

    - **Missing/Invalid Token:** Either the Authorization header was not specified or a properly formatted token value (see above) was not defined.

    - **Insufficient Permissions:** Your CDN administrator determines your level of REST API access by granting both HTTP method and user privileges.

- An unauthorized request will generate a 403 Forbidden response. The response body may indicate the reason why the request was deemed unauthorized (e.g., an invalid user was specified).

Examples

Sample Authorization request headers are provided below.

Example #1:

Authorization: TOK:12345678-1234-1234-1234-1234567890ab

Example #2:

Authorization: tok:12345678-1234-1234-1234-1234567890AB

OAuth 2.0

Authorization for our API gateway is managed by a centralized identity management solution called Identity Service (IDS). IDS leverages OAuth 2.0, which complies with the specification defined within RFC 6749, to authorize requests to the API.

Reminder: Use OAuth 2.0 credentials to authorize requests to Report Builder, RTLD WAF, and most Rules Engine endpoints.

Requests to our API gateway are authorized through the following workflow:

1. **Access Token Request:** A client application requests API access from IDS. This request must include authentication information and a scope that defines the type of API requests that will be authorized.

2. **Temporary Access Token:** If IDS is able to authenticate the client application, it will respond with a temporary access token set to the defined scope.

3. **API Request:** The client application must then pass this access token via an Authorization header when submitting a request to our REST API.

4. **API Response:** If the access token authorizes the requested action, then our REST API service will process it.

This workflow is illustrated below.
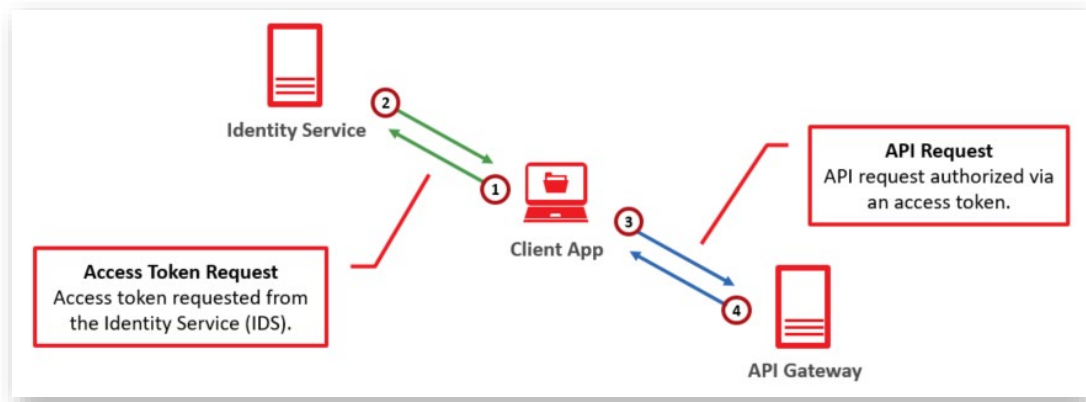
Registering a Client Application (Prerequisite)

Register your client application before interacting with REST API services hosted on our API gateway. Upon successfully registering your client application, the following information will be generated for your client application:

- **Client ID:** A value that uniquely identifies your customer account.

- **Secret:** This value authenticates the client application identified above.

  Important: Do not expose the secret assigned to your account, since it may be used to impersonate your client application. For example, do not define your secret within a client-side script.

Note: Register your client application from the **Security** tab of the Identity dashboard (https://manage.vdms.io/). Refer to the **REST API (OAuth 2.0) Credentials** section below for more information.

Generating Access Tokens

Each request to our REST API service must be authorized via an access token. Access tokens must be requested from IDS.

Important: Access tokens provide temporary authorization (e.g., 5 minutes) to our REST API service. Once an access token expires, it may no longer be used to authorize requests. Attempting to authorize a request with an expired token will result in a 401 Unauthenticated Access response.

Request syntax:

```
POST https://id.vdms.io/connect/token
```

Important: Requests for access tokens requires a Content-Type header set to "application/x-www-form-urlencoded."

Set the request body to:

```
client_id={Client ID}&client_secret={Secret}&grant_type=client_credentials&scope={Scopes}
```

Variable	Description
{Client ID}	Represents your client ID.
{Secret}	Represents the secret assigned to your account.
{Scopes}	Replace this term with one or more scopes. Use the plus symbol (+) to delimit each scope.

Set the scope request body parameter to the desired scope. Common scopes are listed below.

Scope	Description
ec.rules	Authorizes full access to the Rules Engine service.
ec.analytics.rtap.reports.customer	Authorizes full access to the Report Builder service.
ec.rtld	Authorizes full access to the RTLD service.
sec.cps.certificates	Authorizes full access to the Certificate Provisioning System service.

Sample request:

```
POST https://id.vdms.io/connect/token HTTP/1.1

Accept: application/json

Content-Type: application/x-www-form-urlencoded

Host: id.vdms.io

Content-Length: 110

client_id=client123&client_secret=Fad323FSd4GSdce3DFv&grant_type=client_credentials&scope=ec.rules
```

Sample response:

```
HTTP/1.1 200 OK

Cache-Control: no-store, no-cache, max-age=0

Content-Type: application/json; charset=UTF-8

Date: Content-Length: 830

{

        "access_token": "Abc1…0xyZ",

        "expires_in": 300,

        "token_type": "Bearer"

}
```

Authorizing Requests

Requests to our API gateway must be authorized via an access token. Specify an access token within the Authorization request header when submitting a request to our REST API service.

Authorization header syntax:

Bearer *{Access Token}*

Key information:

- The term "Bearer" and the token value are not case-sensitive.

- An unauthorized request will generate a 401 Unauthorized response. The response body may indicate the reason why the request was deemed unauthorized. A request will not be authorized under the following conditions:

  - **Missing/Invalid Token:** Either the Authorization header was not specified or a properly formatted token value (see above) was not defined.

  - **Insufficient Permissions:** The scope associated with the token is insufficient for the requested action.

  - **Expired Token:** A token automatically expires after 300 seconds (i.e., 5 minutes). Once a token has expired, it can no longer authorize requests.

Examples

A sample Authorization request header is provided below.

Authorization: Bearer
Abc1JhbGciOiJSUzI1NiIsImtpZCI6IjI3MjlFRjY4MTYxQjFGGQUQ1MkIzMTU2MjM4QkY2MUYxNz
MwQjY5NzEiLCJ0eXAiOiJKV1QiLCJ4NXQiOiJKeW52YUJZkg2MVNzeFZpT0w5aDhYTUxhWEUif
Q.eyJuYmYiOjE2MDYyMzYxOTQsImV4cCI6MTYwNjIzNjQ5NCwiaXNzIjoiaHR0cHM6Ly9pZC1kZX
YudmRtRtcy5pby9pc1mF1ZCI6WyJodHRwczovL2lkLWRldi52ZG1zLmlvL3Jlc291cmNlcyIsImVjLnJ0bG
QiXSwiY2xpZW50X2lkIjoiZGMxYzUyMTQtOGQyZC00YzM3LTlmYTItYmQ2M2ZhMmJjOGIyIiwia
nRpIjoiOTJjNDc4NjBhMjc2MzI0Zjk4MTFjZDQyZDBmNjgwZTciLCJzY29wZSI6WyJlYy5ydGxkLnNl
dHRpbmdzLmN1c3RvbWVyIl19.XqCA6gmJLJHnbYRALmSKBMn8M2-
KvADtXjRIzxlEWda50s6W8paSVifsiJJneXF5Pta0gSEDwDeljEzQiP7FhD6BP3IkHtYb9eVMdvIktFb
SkYLymI8YM6AYxk6faMFBwYCHn8gWXMV-EKJxPVa4sXGheGxO-
cqz3qUY3c_zAsWfVuf7z2xCkD26VvJNwuIgaCaWDm9Mi0eZl6_DIaF3VBBjFKKpfohPxaM82panj
WdEeoCPEwL_j72YNh-
M55qZSwYRkn60BO2oI6qrPvJ0Y4TiVholgRb8VQ6mZn2TsJIrisMN5ERonltr0xyZ

REST API (OAuth 2.0) Credentials

Note: Our latest APIs authenticate to our system by generating an access token using OAuth 2.0 credentials, while our older APIs use a static REST API token.

Should I generate OAuth credentials for my application?

OAuth credentials are required for the following services:

- Report Builder
- Real-Time Log Delivery
- Rules Engine
- Certificate Provisioning System (CPS)

Generate separate credentials for each unique REST API client that leverages one of the above services.

Note: All other services use a static REST API token.

Overview

Before you may leverage our latest REST API services, you must generate credentials for your REST API client. Manage REST API credentials from manage.vdms.io.

Tenants

A tenant identifies your company or organization. Customers are assigned a single tenant. This tenant contains all of your REST API (OAuth 2.0) client credentials.

REST API (OAuth 2.0) Client Credentials

You may add REST API (OAuth 2.0) credentials for one or more REST API client(s) to your tenant. REST API credentials authorize a client to interact with one or more service(s).

Tip: A security best practice is to generate separate credentials for each unique REST API client.

REST API credentials consist of the following elements:

- **Client ID:** Identifies a REST API client by its system-defined ID. View a client's ID from the **Settings** tab.
- **Secret Key:** A client must pass this private key for identity verification when requesting an access token. View a client's secret key(s) from the **Client Secrets** tab.

> **Tip:** If you suspect that a secret key has been compromised, then you should immediately create a new secret key, update your client to use the new secret key, and then delete the old secret key.

- **Scopes:** Identifies the set of actions that a client is authorized to perform. View a client's scopes from the **APIs** tab.

Scopes

A scope authorizes a REST API client to perform specific actions (e.g., create and retrieve configurations). A scope is defined using the following hierarchy:

```
{Namespace}.{Service}[.{Type}[:{Modifier}]]
```

The above hierarchy allows you to grant broad or narrow permissions to your client. Each element in this hierarchy is described below.

- **Namespace:** Identifies a broad category (i.e., ec). Valid values are:

```
ec | id
```

- **Service:** Identifies a product or a category of products (e.g., analytics, rules, and rtld).

> **Note:** A scope may identify a product or a category of products through multiple services.
> **Example:**
> Both analytics and rtap identify services in the following scope: ec.analytics.rtap).

- **Type:** Optional. Identifies a feature or a type of permission.
  Example:
  In the following scope, deploy identifies a type of permission. In this case, deploy grants permissions to retrieve, submit, and delete deploy requests.

```
ec.rules.deploy
```

- **Modifier:** Optional. Restricts the scope to a subset of permissions. Valid values are:

  - **create:** Restricts the scope to the creation of a resource.

  - **edit:** Restricts the scope to the creation, retrieval, and modification of a resource. It does not authorize the deletion of resources.

  - **delete:** Restricts the scope to the deletion of a resource.

  - **read:** Restricts the scope to the retrieval of a resource.

Example:

The :read modifier in the following scope authorizes the retrieval of deploy requests:

> ec.rules.deploy:read

Key information:

- A security best practice is to only grant the set of scope(s) required for the automation task(s) that the client will perform.

- A broad scope grants all of the scopes underneath it.

    Example:

    The following scope authorizes full access to Rules Engine:

    > ec.rules

    Alternatively, the following scope authorizes the creation, retrieval, modification, and deletion of Rules Engine drafts and policies:

    > ec.rules.policy

- One or more scope(s) must also be defined when requesting an access token. You may only specify a scope that has been explicitly granted or inherited from a broader scope.

Administering REST API Credentials

You can create, modify, and delete REST API credentials.

Tip: The recommended approach for switching to a new secret key is to create a secret key, update your REST API client to use the new secret key, and then delete the old secret key.

To create an account for a REST API client

1. Navigate to the Identity dashboard.

2. Click **Clients** from the side navigation pane.

3. Verify that the **Assigned to Tenant** option is set to your customer account.

4. Click **Create New Client**.

5. In the **Name** option, assign a name that describes this REST API client.

6. In the **Permissions** section, mark each scope that will be assigned to the REST API client.

    Reminder: A security best practice is to only grant the set of scope(s) required for the automation task(s) that the client will perform.

7. Click **Create**.

Note: A **Quick Start** page is shown upon creating an account for your API client. This page contains a sample curl request and response for an access token. It also provides a sample curl request to our REST API service.

To modify a REST API client's account

1. Navigate to the Identity dashboard.

2. Click **Clients** from the side navigation pane.

3. Verify that the **Assigned to Tenant** option is set to your customer account.

4. Click on the desired account.

5. Perform one or more of the following tasks:

   - **Update Name/Description**

     i. Click the **Settings** tab.

     ii. In the **Name** option, modify the account's name.

     iii. In the **Description** option, describe the account's purpose.

     iv. Click **Save**.

   - **Update Access Token Duration**

     i. Click the **Settings** tab.

     ii. In the **JWT Expiration in Seconds** option, determine the number of seconds that an access token will remain valid after being issued.

     iii. Click **Save**.

   - **View Your Client ID**

     i. Click the **Settings** tab.

     ii. Find the **Client ID** option.

   - **Add a Secret Key**

     i. Click the **Client Secrets** tab.

     ii. Click **New Secret Key**.

     iii. In the **Name** option, assign a name to the new secret key.

     iv. Click **Create**.

   - **View or Copy a Secret Key**

     i. Click the **Client Secrets** tab.

     ii. Identify the secret key that you would like to view or copy.

     iii. Click either of the following icons:

       - 👁: Displays the secret key.

       - 🗐: Copies the secret key.

- **Delete a Secret Key**

  Reminder: The recommended approach for switching to a new secret key is to create a secret key, update your REST API client to use the new secret key, and then delete the old secret key.

    i. Click the **Client Secrets** tab.

    ii. Identify the secret key that you would like to delete.

    iii. Verify that it is no longer being used by your REST API client or script.

    iv. Click 🗑 next to the secret key identified in the previous step.

    v. Click **I understand, please delete the client secret** to confirm the deletion of the secret key.

- **Update Scopes**

    i. Click the **APIs** tab.

    ii. Mark each scope that will be granted to the client.

    iii. Clear each scope that will be revoked from the client.

    iv. Click **Save**.

To delete a REST API client's account

Important: Verify that a REST API client is no longer in use prior to deletion. Account deletion cannot be undone.

1. Navigate to the [Identity dashboard](#).

2. Click **Clients** from the side navigation pane.

3. Verify that the **Assigned to Tenant** option is set to your customer account.

4. Click on the desired account.

5. Click the **Settings** tab.

6. Click **Delete Client**.

7. Click **I understand, please delete the client** to confirm the deletion of the REST API client.

Request and Response – Structure and Elements

This section provides an overview of the basic structure and elements of a request/response to our REST API services. It describes:

- HTTP method
- Request URL
- Common request and response headers
- Request body syntax

HTTP Method

HTTP method is a critical component of a request to our REST API service as it determines the type of action being requested.

HTTP Method	Description
DELETE	Deletes the referenced object (e.g., edge CNAME, publishing point, stream key, etc.).
GET	Retrieves information about the referenced object.
POST	Creates a new object.
PUT	Updates the properties associated with an existing object.

Warning: A 405 Method Not Allowed response will be served when the HTTP method submitted with a request to our REST API service is unsupported.

Request URL

The URL for a request to a REST API service follows the basic pattern defined below:

```
https://api.edgecast.com/v2/service/path/resource?parameters
```

Sample request:

```
https://api.edgecast.com/v2/mcc/customers/0001/edge/purge
```

Sample request with parameters:

```
https://api.edgecast.com/v2/reporting/customers/0001/bytestransferred?begindate=2015
-06-01&enddate=2015-07-01
```

Request Headers

Request headers provide information about your request to our Web Services REST API server. This information allows our server to authenticate your request and provides information that allows it to receive and translate the request body.

Important: The use of a Byte Order Mark (BOM) in a request to the REST API is not supported. Keep in mind that some user agents are configured to automatically include a BOM. Please either configure the user agent to exclude the BOM or use a different user agent.

Note: Request header values are case-insensitive.

Request Header	Description
Authorization	This header should identify the Web Services REST API token using the following format: TOK: *Web_Service_REST_API_Token* **Sample value:** TOK:12345678-1234-1234-1234-1234567890ab **Note:** For more information, please refer to the **REST Request Authentication** topic above.
Accept	This header should indicate the format in which the response will be returned. Valid values for JSON and XML are listed below. • **JSON:** Application/JSON • **XML:** Application/XML
Content-Type	This header should indicate the format of the request body. Valid values for JSON and XML are listed below. • **JSON:** Application/JSON • **XML:** Application/XML **Note:** If an endpoint does not have request parameters, then this header can be omitted.
Host	This header, which is set by the user agent, indicates the following host name: api.edgecast.com
Content-Length	This header, which is set by the user agent, indicates the number of bytes contained in the request body.

Request Body

PUT and POST requests typically require request body parameters that describe the action that will take place. These request body parameters are case-sensitive.

Response Headers

Response headers provide information about the response to your request to our Web Services REST API server. A brief description is provided for the response headers that are returned by most endpoints. Standard HTTP response headers are typically returned along with these common response headers.

Response Header	Description
Cache-Control	Indicates that the cache-control for the response body is "private."
Content-Length	Indicates the number of bytes in the response body.
Content-Type	Indicates the format of the response body. This header will report one of the following values: • **JSON:** Application/JSON • **XML:** Application/XML
Date	Identifies the date and time (GMT) at which your request was processed.

Status Codes and Error Messages

Each request for a Web Services REST API endpoint returns a standard HTTP 1.1 status code, as defined in the HTTP 1.1 Status Code Definitions (RFC 2616). The status code included in the response to your request allows you to quickly find out the results for your request. A status code of "200 OK" indicates that the requested endpoint was successfully performed. All other status codes indicate that an error occurred while processing your request.

Error Reporting

The format for error reporting varies by whether the endpoint pertains to the Defend product.

Format (Non-Defend Endpoints)

Error messages for most endpoints are reported in a response element called "Message." A sample error message is displayed below in JSON and XML.

Note: XML schema errors are automatically rejected by the Web Services REST API server. As a result, a generic error message is returned as the response body instead of the "Message" response element.

Sample JSON error message:

```
{"Message":"Access Denied"}
```

Sample XML error message:

```
<Error xmlns="http://www.whitecdn.com/schemas/apiservices/"
xmlns:i="http://www.w3.org/2001/XMLSchema-instance">

        <Message>Access Denied</Message>

</Error>
```

Format - (Defend Endpoints)

The Defend (Origin Protection) endpoints may be requested via the following base URLs:

```
https://api.edgecast.com/v2/mcc/customers/0001/waf

https:// api.edgecast.com /v2/mcc/customers/0001/defend
```

The response body for an error contains the following response elements:

Name	Data Type	Description
errors	Array	Contain an error message.
message	String	Provides a description of the error that occurred.
code	Integer	Indicates a HTTP status code. This status code should only be used for troubleshooting purposes.
success	String	**Note:** This parameter may be included in the error response for a Rate Limiting configuration endpoint. This parameter is set to "false" to indicate that the requested action was unsuccessful.

Note: Certain types of errors (e.g., 405 Method Not Allowed) may return a web page describing the error message (e.g., Method not allowed.) instead of the response described above.

A sample JSON response body is provided below.

```
{
        "errors" : [{

                        "message" : "Invalid date range, beginning date too old: 2014-
        11-08 00:00:00 < 2015-05-04 20:37:53",

                        "code" : 400

            }

        ]

}
```

200 OK Status Code

As previously mentioned, a 200 OK status code indicates that the operation was successfully carried out. This means that the operation was processed by our servers and the proper response was returned. However, the proper response may be an empty response body. For example, updating an object (i.e, PUT request) will typically return an empty response body.

Note: If the request URI for an endpoint requires the identification of a customer, then an invalid account number or custom ID will result in a 400 Bad Request.

Note: GET requests set to an invalid object ID will either return a 200 OK with an empty object or a 400 Bad Request.

Error Messages

A list of common errors and their corresponding HTTP status codes is provided below.

Error Message Type	HTTP Status Code	Description
Inactive/Deleted Customer	400 Bad Request	The customer account number specified in the request URI corresponds to an inactive customer account. The response may contain a Message element that reports "Cannot update or retrieve information of a deleted customer."
Invalid Customer ID Value/Invalid ID Value	400 Bad Request	The customer account number specified in the request URI does not correspond to the customer account associated with the Web Services REST API token specified in the Authorization header.
Invalid Request/Response Type	400 Bad Request	The format specified for the request body does not match the one specified in the Content-Type request header. A generic request error will be returned for this error type.

Error Message Type	HTTP Status Code	Description
Invalid Request URL/Parameter	400 Bad Request	This type of error message occurs when the request URL or a parameter value in the request body contains invalid or improperly formatted data. Below you will find common scenarios for this type of error message. • The request URL is invalid. Make sure that all characters are URL encoded. For example, space characters in a custom ID should be replaced by "%20." • A parameter value does not match the expected format. For example, an e-mail address does not contain an @ symbol. • An invalid value was specified for a parameter. For example, a 2 was specified for a request parameter that can only accept a value of 1 or 3. • A blank value was specified for a required request parameter. • The value specified for a required request parameter is of an invalid data type. For example, a letter is specified for an integer field. A generic message is returned for XML schema errors.
Missing Required Fields	400 Bad Request	This type of error message occurs when a required field for the requested endpoint was not properly specified. Below you will find common scenarios for this type of error message. • An empty value was specified for a required field. • A required request parameter was not included in the request. A generic message is returned for XML schema errors.

Error Message Type	HTTP Status Code	Description
Authentication Failure	403 Forbidden	If a request was not authorized by the Web Services REST API server due to a missing or an invalid token value, then the response will contain a Message element that reports either "Invalid user" or "Access Denied." Please verify the following items: • The Authorization request header was included in your request. • The proper format was used to specify the Web Services REST API token. (i.e., TOK: *Web_Service_REST_API_Token*). • The specified token value matches the primary or backup token assigned to your account. • Keep in mind that the entire value specified for the Authorization header will be used to authenticate a user. Make sure that no characters other than the token header (i.e., TOK:) and the token value have been specified. For example, enclosing the Authorization header value in quotes will generate a 403 Forbidden status code.
Insufficient Access Rights	403 Forbidden	If a request was made by a user with insufficient privileges, then the response will contain a message indicating insufficient access.
Invalid Case	403 Forbidden	This type of error message occurs when a request is formed using improper case.
Invalid Request URI	404 Not Found	This type of error message occurs when the URI is requesting an endpoint that does not exist. Typically, this type of error will return an "Endpoint not found" message. Verify the URI of the offending request. If the URI appears to be correct, make sure that you have not appended a forward slash (/) to the end of the URI.

Error Message Type	HTTP Status Code	Description
Invalid Request	405 Method Not Allowed	This type of error message typically occurs when the specified HTTP method (i.e., GET, PUT, POST, or DELETE) is not allowed for the endpoint specified by the URI. For example, if you are performing a GET function on an endpoint that only accepts a POST.
Server Error	500 Internal Server Error	This type of error message occurs when the Web Services REST API server was unable to handle your request. The response for this type of error will contain a Message element that reports "Operation Error." Sample scenarios under which this status code will be reported are listed below. • The URI is not properly formatted for the requested endpoint. • The Web Services REST API database is not properly responding to the request.

Account Status

A customer's account status determines the type of operations that can be performed on it. There are four different types of customer account statuses, which are active, inactive, suspended, and trial. The type of operations that can be performed for each customer account status is described below.

Customer Account Status	Valid Endpoints
Active	All
Inactive	None
Suspended	Core Reporting Advanced Content Analytics
Trial	All

Note: Your account status is determined by your CDN account manager. If you suspect that your account has been mistakenly been suspended or marked as inactive, please contact your CDN account manager.

Notation Conventions

The following table describes the notation conventions that are used in this guide.

Name	Description
Bold Text	Non-bulleted bold text indicates a reference to a section or chapter heading.
• **Bold text:**	The significance of bulleted bold text depends on the context in which it appears. The most common usages are listed below. • Identifies a term in the request URI. • Identifies a valid value for a request parameter. • Identifies a return value for a response parameter.
Italic Text	Italic text identifies a term that should be replaced with a valid value. Typically, this type of term appears in the request URI.
Parameter	Purple bold font is used to indicate that a request parameter is required. A valid value must be specified for a required request parameter.
Parameter	Gray bold font is used to indicate that a request URI, a request parameter, or a return parameter has been designated as legacy. It is highly recommended to avoid using a legacy URI, request parameter, or return parameter.
`Field`	A sample request or response is indicated by a gray block of text.

CDN Management

Overview

CDN management endpoints allow you to perform basic tasks that affect how users access your content.

Cache Management

An asset can be cached or purged from all of our POPs. These tasks can be performed through the Load Content and the Purge Content endpoints.

Bulk Load Content

Submits a bulk load that defines the content that will be loaded. Loading content caches an asset on our edge servers. This allows that content to be served directly from the edge of our network to your users.

Key information:

- There is a default limit of 50 concurrent load requests at any given time. Exceeding this limit will generate a 400 Bad Request.
  All outstanding load requests count towards this concurrent load request limit. This includes load requests submitted via the MCC, the Load Content endpoint, or the Bulk Load Content endpoint.

  Note: With regards to bulk loads, each specified URL counts as a separate load request. For example, each element defined in the MediaPath array of the Bulk Load Content endpoint counts as a separate load request.

- An asset should only be loaded a single time per unique combination of platform and protocol.

  Note: If a load request is limited to a specific region, then an asset should be loaded a single time per unique combination of platform, protocol, and region.

- A short period of time may elapse before an asset is cached across our entire network. However, a successful request will immediately return an ID in the response. Find out the current status of your load request(s) by passing this ID to:

  - **Loading via Load Content Endpoint:** Get Load Request endpoint

  - **Loading via Bulk Load Content Endpoint:** Get Bulk Load Request endpoint

Request

A request for a bulk load is described below. When submitting this request, you will need to define the following term:

- **AccountNumber:** This term should be replaced by your CDN account number. This number can be found in the upper-right hand corner of the MCC.

HTTP Method	Request URI
PUT	https://api.edgecast.com/v2/mcc/customers/*AccountNumber*/edge/bulkload

Request Headers

This endpoint only takes advantage of the common request headers described in the **Request Headers** section of the **Request and Response Elements** topic.

Request Body

The request parameters for this endpoint are described below.

Name	Description
EdgeNodeRegionIds	An array that defines the set of regions to which the bulk load request will be applied. Set this parameter to the desired region ID(s). Use a comma to delimit multiple regions. **Sample value (JSON):** - EdgeNodeRegionIds: [3,4], Omitting this parameter will apply the load request to the entire network (i.e., all regions). A list of platform-specific regions and their corresponding system-defined IDs can be retrieved through the Get Load/Purge Regions method. **Important:** Although the response for the Get Load/Purge Regions method includes the POPs (i.e., edge nodes) associated with each region and their system-defined IDs, the EdgeNodeRegionIds request parameter only accepts the system-defined IDs for load/purge regions.

Name	Description
MediaPath	Required. An array of string values that identifies each CDN or edge CNAME URL that will be loaded to our edge servers. Make sure to include the appropriate protocol (e.g., http://).
MediaType	Required. An integer set to the system-defined ID of the delivery platform to which assets will be loaded. Valid values are: • **3:** HTTP Large • **8:** HTTP Small • **14:** Application Delivery Network (ADN)

Response

The response to the above request includes an HTTP status code, response headers, and a response body.

Status Code

A status code indicates whether the request was successfully performed. A list of common status codes is provided in the **Status Codes and Error Messages** topic.

Response Headers

The response for this endpoint only returns standard HTTP response headers including those described in the **Response Headers** section of the **Request and Response Elements** topic.

Response Body

The response body for a successful request contains the following response element:

Name	Description
Id	A string that reports the unique ID assigned to the bulk load request.

Errors

The response body for an unsuccessful request may contain an error element that provides additional information. For a list of common error messages, please refer to the **Status Codes and Error Messages** topic.

Sample Request and Response

A sample JSON request is provided below.

```
PUT https://api.edgecast.com/v2/mcc/customers/0001/edge/bulkload HTTP/1.1

Authorization: TOK:12345678-1234-1234-1234-1234567890ab

Accept: application/json
```

```
Content-Type: application/json

Host: api.edgecast.com

Content-Length: 155

{

        "MediaPath": ["http:\/\/wpc.0001.edgecastcdn.net\/000001\/WebPage.htm",
        "http:\/\/wpc.0001.edgecastcdn.net\/000001\/marketing\/*"],

        "MediaType": 3

}
```

A sample JSON response is provided below.

```
HTTP/1.1 200 OK

Cache-Control: private

Content-Length: 33

Content-Type: application/json; charset=utf-8

Date: Thu, 14 Apr 2016 12:00:00 GMT

{

        "Id": " 170fe3a9d4c54d012f680f2a"

}
```

Bulk Purge Content

Submits a bulk purge that defines the content that will be purged. Purging content invalidates the cached version of an asset from our edge servers. By default, the CDN will forward the next request for that content to the origin server.

Key information:

- There is a default limit of 50 concurrent purge requests at any given time. Exceeding this limit will generate a 400 Bad Request.
  All outstanding purge requests count towards this concurrent purge request limit. This includes purge requests submitted via the MCC, the Purge Content endpoint, or the Bulk Purge Content endpoint.

  Note: With regards to bulk purges, each specified URL counts as a separate purge request. For example, each element defined in the MediaPath array of the Bulk Purge Content endpoint counts as a separate purge request.

- An asset only needs to be purged a single time per platform. The asset will be purged for all CDN and edge CNAME URLs that point to the purge location, regardless of the protocol (i.e., http or https) used to reach it.

  Note: If the purge request is limited to a specific region, then an asset should be purged a single time per unique combination of platform and region.

- A short period of time may elapse before an asset is completely purged from our entire network. However, a successful request will immediately return an ID in the response. Find out the current status of your purge request(s) by passing this ID to:
  - **Purging via Purge Content Endpoint:** Get Purge Request endpoint
  - **Purging via Bulk Purge Content Endpoint:** Get Bulk Purge Request endpoint

Request

A request for a bulk purge is described below. When submitting this request, you will need to define the following term:

- **AccountNumber:** This term should be replaced by your CDN account number. This number can be found in the upper-right hand corner of the MCC.

HTTP Method	Request URI
PUT	https://api.edgecast.com/v2/mcc/customers/*AccountNumber*/edge/bulkpurge

Request Headers

This endpoint only takes advantage of the common request headers described in the **Request Headers** section of the **Request and Response Elements** topic.

Request Body

The request parameters for this endpoint are described below.

Name	Description
EdgeNodeRegionIds	An array that defines the set of regions to which the bulk purge request will be applied. Set this parameter to the desired region ID(s). Use a comma to delimit multiple regions. **Sample value (JSON):** - EdgeNodeRegionIds: [3,4], Omitting this parameter will apply the purge request to the entire network (i.e., all regions). A list of platform-specific regions and their corresponding system-defined IDs can be retrieved through the Get Load/Purge Regions method. **Important:** Although the response for the Get Load/Purge Regions method includes the POPs (i.e., edge nodes) associated with each region and their system-defined IDs, the EdgeNodeRegionIds request parameter only accepts the system-defined IDs for load/purge regions.

Name	Description
MediaPath	Required. An array of string values that identifies each CDN or edge CNAME URL that will be purged from our edge servers. Make sure to include the appropriate protocol (e.g., http://).
MediaType	Required. An integer set to the system-defined ID of the delivery platform from which assets will be purged. Valid values are: • **3:** HTTP Large • **8:** HTTP Small • **14:** Application Delivery Network (ADN)

Response

The response to the above request includes an HTTP status code, response headers, and a response body.

Status Code

A status code indicates whether the request was successfully performed. A list of common status codes is provided in the **Status Codes and Error Messages** topic.

Response Headers

The response for this endpoint only returns standard HTTP response headers including those described in the **Response Headers** section of the **Request and Response Elements** topic.

Response Body

The response body for a successful request contains the following response element:

Name	Description
Id	A string that reports the unique ID assigned to the bulk purge request.

Errors

The response body for an unsuccessful request may contain an error element that provides additional information. For a list of common error messages, please refer to the **Status Codes and Error Messages** topic.

Sample Request and Response

A sample JSON request is provided below.

```
PUT https://api.edgecast.com/v2/mcc/customers/0001/edge/bulkpurge HTTP/1.1

Authorization: TOK:12345678-1234-1234-1234-1234567890ab

Accept: application/json
```

```
Content-Type: application/json

Host: api.edgecast.com

Content-Length: 155

{

        "MediaPath": ["http:\/\/wpc.0001.edgecastcdn.net\/000001\/WebPage.htm",
        "http:\/\/wpc.0001.edgecastcdn.net\/000001\/marketing\/*"],

        "MediaType": 3

}
```

A sample JSON response is provided below.

```
HTTP/1.1 200 OK

Cache-Control: private

Content-Length: 33

Content-Type: application/json; charset=utf-8

Date: Thu, 14 Apr 2016 12:00:00 GMT

{

        "Id": " 170fe3a9d4c54d012f680f2a"

}
```

Get Bulk Load Request

Retrieves information, including status, about a bulk load request.

Request

A request to retrieve a bulk load request is described below. When submitting this request, you will need to define the following terms:

- **AccountNumber:** This term should be replaced by your CDN account number. This number can be found in the upper-right hand corner of the MCC.

- **BulkLoadID:** Replace this term with an integer that identifies a bulk load request by its ID. This ID is returned by the Bulk Load Content endpoint.

HTTP Method	Request URI
GET	https://api.edgecast.com/v2/mcc/customers/*AccountNumber*/edge/bulkload/*BulkLoadID*

Request Headers
This endpoint only takes advantage of the common request headers described in the **Request Headers** section of the **Request and Response Elements** topic.

Request Body

Request body parameters are not required by this endpoint.

Response

The response to the above request includes an HTTP status code, response headers, and a response body.

Status Code

A status code indicates whether the request was successfully performed. A list of common status codes is provided in the **Status Codes and Error Messages** topic.

Response Headers

The response for this endpoint only returns standard HTTP response headers including those described in the **Response Headers** section of the **Request and Response Elements** topic.

Response Body

The response body for a successful request contains the following response elements:

Name	Description
Status_Details	An object that provides information about the bulk load request.
Count	An integer that indicates the number of load requests defined in the bulk load request. Each element defined in the MediaPath array of the Bulk Load Content endpoint counts as a separate load request.
Status	A string that indicates the status for the load requests defined in the bulk load request. Valid values are: ▪ **in-progress:** Indicates that one or more load requests have not been completed. ▪ **done:** Indicates that all load requests have been completed.
Created_at	A string that indicates the date and time at which the bulk load request was submitted. **Format:** *MM\/DD\/YYYY hh:mm:ss* AM|PM

Name	Description
Completed_at	A string that indicates the date and time at which all load requests defined in the bulk load request were completed. **Format:** *MM\/DD\/YYYY hh:mm:ss* AM|PM **Note:** A null value is returned when the bulk load request is still being processed.
Batch_id	A string that identifies a bulk load request by its unique ID.
Progress	A string that identifies the percentage of load requests that have been completed.
Completed	An integer that indicates the number of load requests that have been completed.

Errors

The response body for an unsuccessful request may contain an error element that provides additional information. For a list of common error messages, please refer to the **Status Codes and Error Messages** topic.

Sample Request and Response

A sample JSON request is provided below.

```
GET
https://api.edgecast.com/v2/mcc/customers/0001/edge/bulkload/522e0c33e5671c06c14235e
8 HTTP/1.1

Authorization: TOK:12345678-1234-1234-1234-1234567890ab

Accept: application/json

Host: api.edgecast.com
```

A sample JSON response is provided below.

```
HTTP/1.1 200 OK
Cache-Control: private
Content-Type: application/json; charset=utf-8
Date: Thu, 14 Apr 2016 12:00:00 GMT
Content-Length: 227


{
        "Status_Details": {
                "Count": 50,
                "Status": "in-progress",
                "Created_at": "10\/20\/2017 8:33:25 PM",
                "Completed_at": null,
                "Batch_id": "522e0c33e5671c06c14235e8",
                "Progress": "0.0",
                "Completed": 0
        }
}
```

Get Bulk Purge Request

Retrieves information, including status, about a bulk purge request.

Request

A request to retrieve a bulk purge request is described below. When submitting this request, you will need to define the following terms:

- **AccountNumber:** This term should be replaced by your CDN account number. This number can be found in the upper-right hand corner of the MCC.

- **BulkPurgeID:** Replace this term with an integer that identifies a bulk purge request by its ID. This ID is returned by the Bulk Purge Content endpoint.

HTTP Method	Request URI
GET	https://api.edgecast.com/v2/mcc/customers/*AccountNumber*/edge/bulkpurge /*BulkPurgeD*

Request Headers

This endpoint only takes advantage of the common request headers described in the **Request Headers** section of the **Request and Response Elements** topic.

Request Body

Request body parameters are not required by this endpoint.

Response

The response to the above request includes an HTTP status code, response headers, and a response body.

Status Code

A status code indicates whether the request was successfully performed. A list of common status codes is provided in the **Status Codes and Error Messages** topic.

Response Headers

The response for this endpoint only returns standard HTTP response headers including those described in the **Response Headers** section of the **Request and Response Elements** topic.

Response Body

The response body for a successful request contains the following response elements:

Name	Description
Status_Details	An object that provides information about the bulk purge request.
Count	An integer that indicates the number of purge requests defined in the bulk purge request. Each element defined in the MediaPath array of the Bulk Purge Content endpoint counts as a separate purge request.
Status	A string that indicates the status for the purge requests defined in the bulk purge request. Valid values are: ■ **in-progress:** Indicates that one or more purge requests have not been completed. ■ **done:** Indicates that all purge requests have been completed.
Created_at	A string that indicates the date and time at which the bulk purge request was submitted. **Format:** *MM\/DD\/YYYY hh:mm:ss* AM|PM
Completed_at	A string that indicates the date and time at which all purge requests defined in the bulk purge request were completed. **Format:** *MM\/DD\/YYYY hh:mm:ss* AM|PM **Note:** A null value is returned when the bulk purge request is still being processed.
Batch_id	A string that identifies a bulk purge request by its unique ID.
Progress	A string that identifies the percentage of purge requests that have been completed.
Completed	An integer that indicates the number of purge requests that have been completed.

Errors

The response body for an unsuccessful request may contain an error element that provides additional information. For a list of common error messages, please refer to the **Status Codes and Error Messages** topic.

Sample Request and Response

A sample JSON request is provided below.

```
GET
https://api.edgecast.com/v2/mcc/customers/0001/edge/bulkpurge/59ea2a63f4992206a8bfae
28 HTTP/1.1

Authorization: TOK:12345678-1234-1234-1234-1234567890ab

Accept: application/json

Host: api.edgecast.com
```

A sample JSON response is provided below.

```
HTTP/1.1 200 OK

Cache-Control: private

Content-Type: application/json; charset=utf-8

Date: Thu, 14 Apr 2016 12:00:00 GMT

Content-Length: 234


{

        "Status_Details": {

                "Count": 30,

                "Status": "in-progress",

                "Created_at": "10\/20\/2017 4:54:59 PM",

                "Completed_at": null,

                "Batch_id": " 59ea2a63f4992206a8bfae28",

                "Progress": "0.0",

                "Completed": 0

        }

}
```

Get Load/Purge Regions

This method retrieves a list of platform-specific load/purge regions. Load/purge regions may be used to selectively apply a load or purge request to specific region(s).

The set of available regions varies by platform. This method will respond with all regions that apply to at least one of the platforms defined in the request.

Request

A request to retrieve a list of load/purge regions is described below. When submitting this request, you will need to define the following term:

- **PlatformIDs:** Replace this variable with the ID of each platform for which regions will be returned. Use a comma to delimit multiple platforms.If multiple platforms are specified, then the response will include all regions that apply to at least one specified platform. Valid values are:

    - **3:** HTTP Large

    - **8:** HTTP Small

    - **14:** Application Delivery Network (ADN)

HTTP Method	Request URI
GET	https://api.edgecast.com/v2/mcc/lpqregions?mediaTypes=*PlatformIDs*

Request Headers
This endpoint only takes advantage of the common request headers described in the **Request Headers** section of the **Request and Response Elements** topic.

Request Body
Request body parameters are not required by this endpoint.

Response

The response to the above request includes an HTTP status code, response headers, and a response body.

Status Code
A status code indicates whether the request was successfully performed. A list of common status codes is provided in the **Status Codes and Error Messages** topic.

Response Headers
The response for this endpoint only returns standard HTTP response headers including those described in the **Response Headers** section of the **Request and Response Elements** topic.

Response Body

The response body for a successful request contains the following response elements:

Name	Description
EdgeNodes	Lists each POP in the current region.
Code	A string that identifies by a POP by its three-letter abbreviation.
Id	An integer that identifies a POP by its system-defined ID.
Id	An integer that identifies a region by its system-defined ID.
Name	A string that identifies a region by its name.

Errors

The response body for an unsuccessful request may contain an error element that provides additional information. For a list of common error messages, please refer to the **Status Codes and Error Messages** topic.

Sample Request and Response

A sample JSON request is provided below.

```
GET https://api.edgecast.com/v2/mcc/lpqregions?mediaTypes=3 HTTP/1.1

Authorization: TOK:12345678-1234-1234-1234-1234567890ab

Accept: application/json

Host: api.edgecast.com
```

A sample JSON response is provided below.

```
HTTP/1.1 200 OK

Cache-Control: private

Content-Type: application/json; charset=utf-8

Date: Thu, 14 Apr 2016 12:00:00 GMT

Content-Length: 4091

[{
```

```
            "EdgeNodes" : [{
                        "Code" : "DCA",
                        "Id" : 2
                }, {
                        "Code" : "LAX",
                        "Id" : 3
                ...
                }, {
                        "Code" : "BOS",
                        "Id" : 202
                }
            ],
            "Id" : 1,
            "Name" : "North America"
            }, {
            ...
            }, {
            "EdgeNodes" : [{
                        "Code" : "GRU",
                        "Id" : 67
                }, {
                        "Code" : "CGH",
                        "Id" : 151
                }
            ],
            "Id" : 7,
            "Name" : "South America"
     }
]
```

Get Load Request

Retrieves information about a load request.

Request

A request to retrieve a load request is described below. When submitting this request, you will need to define the following terms:

- **AccountNumber:** This term should be replaced by your CDN account number. This number can be found in the upper-right hand corner of the MCC.

- **LoadID:** Replace this term with an integer that identifies a load request by its ID. This ID is returned by the Load Content endpoint.

HTTP Method	Request URI
GET	https://api.edgecast.com/v2/mcc/customers/*AccountNumber*/edge/load/*LoadID*

Request Headers

This endpoint only takes advantage of the common request headers described in the **Request Headers** section of the **Request and Response Elements** topic.

Request Body

Request body parameters are not required by this endpoint.

Response

The response to the above request includes an HTTP status code, response headers, and a response body.

Status Code

A status code indicates whether the request was successfully performed. A list of common status codes is provided in the **Status Codes and Error Messages** topic.

Response Headers

The response for this endpoint only returns standard HTTP response headers including those described in the **Response Headers** section of the **Request and Response Elements** topic.

Response Body

The response body for a successful request contains the following response elements:

Name	Description
AccountNumber	A string that indicates the CDN account number associated with the load request.
CompleteDate	A string that indicates the date and time on which the load request was completed. **Format:** *YYYY-MM-DD hh*:*mm*
Id	A string that identifies a load request by its unique ID.
InDate	A string that indicates the date and time on which the load request was submitted. **Format:** *YYYY-MM-DD hh*:*mm*
MediaPath	A string that indicates the CDN or edge CNAME URL for which a load request was submitted.
MediaTypeId	An integer that indicates the service associated with the load request. Valid values are: • **3:** HTTP Large • **8:** HTTP Small • **14:** Application Delivery Network (ADN)
Regions	Lists all regions to which the load request was applied.
Id	An integer that identifies a region by its system-defined ID.
Name	A string that identifies a region by its name.

Errors

The response body for an unsuccessful request may contain an error element that provides additional information. For a list of common error messages, please refer to the **Status Codes and Error Messages** topic.

Sample Request and Response

A sample JSON request is provided below.

```
GET
https://api.edgecast.com/v2/mcc/customers/0001/edge/load/522e0c33e5671c06c14224d7
HTTP/1.1

Authorization: TOK:12345678-1234-1234-1234-1234567890ab

Accept: application/json

Host: api.edgecast.com
```

A sample JSON response is provided below.

```
HTTP/1.1 200 OK

Cache-Control: private

Content-Type: application/json; charset=utf-8

Date: Thu, 14 Apr 2016 12:00:00 GMT

Content-Length: 234


{

        "AccountNumber" : "0001",

        "CompleteDate" : null,

        "Id" : "522e0c33e5671c06c14224d7",

        "InDate" : "2016-04-14 19:08",

        "MediaPath" : "http:\/\/wpc.0001.edgecastcdn.net\/000001\/WebPage.htm",

        "MediaTypeId" : 3,

        "Regions" : []
}
```

Get Purge Request

Retrieves information about a purge request.

Request

A request to retrieve a purge request is described below. When submitting this request, you will need to define the following terms:

- **AccountNumber:** This term should be replaced by your CDN account number. This number can be found in the upper-right hand corner of the MCC.

- **PurgeID:** Replace this term with an integer that identifies a purge request by its ID. This ID is returned by the Purge Content endpoint.

HTTP Method	Request URI
GET	https://api.edgecast.com/v2/mcc/customers/*AccountNumber*/edge/purge/*PurgeID*

Request Headers

This endpoint only takes advantage of the common request headers described in the **Request Headers** section of the **Request and Response Elements** topic.

Request Body

Request body parameters are not required by this endpoint.

Response

The response to the above request includes an HTTP status code, response headers, and a response body.

Status Code

A status code indicates whether the request was successfully performed. A list of common status codes is provided in the **Status Codes and Error Messages** topic.

Response Headers

The response for this endpoint only returns standard HTTP response headers including those described in the **Response Headers** section of the **Request and Response Elements** topic.

Response Body

The response body for a successful request contains the following response elements:

Name	Description
AccountNumber	A string that indicates the CDN account number associated with the purge request.

Name	Description
CompleteDate	A string that indicates the date and time on which the purge request was completed. **Format:** *YYYY-MM-DD hh*:*mm*
Id	A string that identifies a purge request by its unique ID.
InDate	A string that indicates the date and time on which the purge request was submitted. **Format:** *YYYY-MM-DD hh*:*mm*
MediaPath	A string that indicates the CDN or edge CNAME URL for which a purge request was submitted.
MediaTypeId	An integer that indicates the service associated with the purge request. Valid values are: • **3:** HTTP Large • **8:** HTTP Small • **14:** Application Delivery Network (ADN)
Regions	Lists all regions to which the purge request was applied.
Id	An integer that identifies a region by its system-defined ID.
Name	A string that identifies a region by its name.

Errors

The response body for an unsuccessful request may contain an error element that provides additional information. For a list of common error messages, please refer to the **Status Codes and Error Messages** topic.

Sample Request and Response

A sample JSON request is provided below.

```
GET
https://api.edgecast.com/v2/mcc/customers/0001/edge/purge/522e0c33e5671c06c14224d7
HTTP/1.1

Authorization: TOK:12345678-1234-1234-1234-1234567890ab

Accept: application/json

Host: api.edgecast.com
```

A sample JSON response is provided below.

```
HTTP/1.1 200 OK
Cache-Control: private
Content-Type: application/json; charset=utf-8
Date: Thu, 14 Apr 2016 12:00:00 GMT
Content-Length: 234


{
        "AccountNumber" : "0001",
        "CompleteDate" : null,
        "Id" : "522e0c33e5671c06c14224d7",
        "InDate" : "2015-05-08 19:08",
        "MediaPath" : "http:\/\/wpc.0001.edgecastcdn.net\/000001\/folder1\/*",
        "MediaTypeId" : 3,
        "Regions" : []
}
```

Load Content

Loads (i.e., cache) an asset on our edge servers.

Key information:

- There is a default limit of 50 concurrent load requests at any given time. Exceeding this limit will generate a 400 Bad Request.
  All outstanding load requests count towards this concurrent load request limit. This includes load requests submitted via the MCC, the Load Content endpoint, or the Bulk Load Content endpoint.

  > **Note:** With regards to bulk loads, each specified URL counts as a separate load request. For example, each element defined in the MediaPath array of the Bulk Load Content endpoint counts as a separate load request.

- An asset should only be loaded a single time per unique combination of platform and protocol.

  > **Note:** If a load request is limited to a specific region, then an asset should be loaded a single time per unique combination of platform, protocol, and region.

- A short period of time may elapse before an asset is cached across our entire network. However, a successful request will immediately return an ID in the response. Find out the current status of your load request(s) by passing this ID to:

  - **Loading via Load Content Endpoint:** Get Load Request endpoint

  - **Loading via Bulk Load Content Endpoint:** Get Bulk Load Request endpoint

Request

A request to load an asset is described below. When submitting this request, you will need to define the following term:

- **AccountNumber:** This term should be replaced by your CDN account number. This number can be found in the upper-right hand corner of the MCC.

HTTP Method	Request URI
PUT	https://api.edgecast.com/v2/mcc/customers/*AccountNumber*/edge/load

Request Headers
This endpoint only takes advantage of the common request headers described in the **Request Headers** section of the **Request and Response Elements** topic.

Request Body
The required request parameters for this endpoint are described below.

Name	Description
EdgeNodeRegionIds	An array that defines the set of regions to which the load request will be applied. Set this parameter to the desired region ID(s). Use a comma to delimit multiple regions. **Sample value (JSON):** • EdgeNodeRegionIds: [3,4], Omitting this parameter will apply the load request to the entire network (i.e., all regions). A list of platform-specific regions and their corresponding system-defined IDs can be retrieved through the Get Load/Purge Regions method. **Important:** Although the response for the Get Load/Purge Regions method includes the POPs (i.e., edge nodes) associated with each region and their system-defined IDs, the EdgeNodeRegionIds request parameter only accepts the system-defined IDs for load/purge regions.
MediaPath	Required. A string that indicates the CDN or edge CNAME URL for the asset that will be loaded to our edge servers. Make sure to include the proper protocol (e.g., http:// or rtmp://).
MediaType	Required. An integer that indicates the service for which an asset will be loaded. It should be replaced with the ID associated with the desired service. Valid values are: • **3:** HTTP Large • **8:** HTTP Small • **14:** Application Delivery Network (ADN)

Response

The response to the above request includes an HTTP status code, response headers, and a response body.

Status Code

A status code indicates whether the request was successfully performed. A list of common status codes is provided in the **Status Codes and Error Messages** topic.

Response Headers

The response for this endpoint only returns standard HTTP response headers including those described in the **Response Headers** section of the **Request and Response Elements** topic.

Response Body

The response body for a successful request contains the following response element:

Name	Description
Id	A string that reports the unique number assigned to the load request.

Errors

The response body for an unsuccessful request may contain an error element that provides additional information. For a list of common error messages, please refer to the **Status Codes and Error Messages** topic.

Sample Request and Response

JSON

A sample JSON request is provided below.

```
PUT https://api.edgecast.com/v2/mcc/customers/0001/edge/load HTTP/1.1

Authorization: TOK:12345678-1234-1234-1234-1234567890ab

Accept: application/json

Content-Type: application/json

Host: api.edgecast.com

Content-Length: 92


{

        "MediaPath":"http:\/\/wpc.0001.edgecastcdn.net\/000001\/WebPage.htm",

        "MediaType":3

}
```

A sample JSON response is provided below.

```
HTTP/1.1 200 OK

Cache-Control: private

Content-Length: 33

Content-Type: application/json; charset=utf-8

Date: Thu, 14 Apr 2016 12:00:00 GMT

{

        "Id" : "170fe3a9d4c54d012f680e3c"

}
```

Purge Content

Purges (i.e., delete) the cached version of an asset from our edge servers.

Key information:

- There is a default limit of 50 concurrent purge requests at any given time. Exceeding this limit will generate a 400 Bad Request.
  All outstanding purge requests count towards this concurrent purge request limit. This includes purge requests submitted via the MCC, the Purge Content endpoint, or the Bulk Purge Content endpoint.

  > **Note:** With regards to bulk purges, each specified URL counts as a separate purge request. For example, each element defined in the MediaPath array of the Bulk Purge Content endpoint counts as a separate purge request.

- An asset only needs to be purged a single time per platform. The asset will be purged for all CDN and edge CNAME URLs that point to the purge location, regardless of the protocol (i.e., http or https) used to reach it.

  > **Note:** If the purge request is limited to a specific region, then an asset should be purged a single time per unique combination of platform and region.

- A short period of time may elapse before an asset is cached across our entire network. However, a successful request will immediately return an ID in the response. Find out the current status of your purge request(s) by passing this ID to:

    - **Purging via Purge Content Endpoint:** Get Purge Request endpoint
    - **Purging via Bulk Purge Content Endpoint:** Get Bulk Purge Request endpoint

Request

A request to purge an asset is described below. When submitting this request, you will need to define the following term:

- **AccountNumber:** This term should be replaced by your CDN account number. This number can be found in the upper-right hand corner of the MCC.

HTTP Method	Request URI
PUT	https://api.edgecast.com/v2/mcc/customers/*AccountNumber*/edge/purge

Request Headers

This endpoint only takes advantage of the common request headers described in the **Request Headers** section of the **Request and Response Elements** topic.

Request Body

The required request parameters for this endpoint are described below.

Name	Description
EdgeNodeRegionIds	An array that defines the set of regions to which the purge request will be applied. Set this parameter to the desired region ID(s). Use a comma to delimit multiple regions. **Sample value (JSON):** • EdgeNodeRegionIds: [3,4], Omitting this parameter will apply the purge request to the entire network (i.e., all regions). A list of platform-specific regions and their corresponding system-defined IDs can be retrieved through the Get Load/Purge Regions method. **Important:** Although the response for the Get Load/Purge Regions method includes the POPs (i.e., edge nodes) associated with each region and their system-defined IDs, the EdgeNodeRegionIds request parameter only accepts the system-defined IDs for load/purge regions.
MediaPath	Required. A string that indicates the CDN or edge CNAME URL for the asset or the location that will be purged from our edge servers. Make sure to include the proper protocol (i.e., http:// or rtmp://). For information on how to set the scope of the purge action, please refer to the **Purge Syntax** section in **Appendix A**. **Note:** For the purpose of this endpoint, the http:// and https:// protocols are interchangeable.
MediaType	Required. An integer that indicates the service for which an asset will be purged. It should be replaced with the ID associated with the desired service. Valid values are: • **3:** HTTP Large • **8:** HTTP Small • **14:** Application Delivery Network (ADN)

Response

The response to the above request includes an HTTP status code, response headers, and a response body.

Status Code

A status code indicates whether the request was successfully performed. A list of common status codes is provided in the **Status Codes and Error Messages** topic.

Response Headers

The response for this endpoint only returns standard HTTP response headers including those described in the **Response Headers** section of the **Request and Response Elements** topic.

Response Body

The response body for a successful request contains the following response element:

Name	Description
Id	A string that reports the unique number assigned to the purge request.

Errors

The response body for an unsuccessful request may contain an error element that provides additional information. For a list of common error messages, please refer to the **Status Codes and Error Messages** topic.

Sample Request and Response

A sample JSON request is provided below.

```
PUT https://api.edgecast.com/v2/mcc/customers/0001/edge/purge HTTP/1.1

Authorization: TOK:12345678-1234-1234-1234-1234567890ab

Accept: application/json

Content-Type: application/json

Host: api.edgecast.com

Content-Length: 92


{

        "MediaPath":"http:\/\/wpc.0001.edgecastcdn.net\/000001\/WebPage.htm",

        "MediaType":3

}
```

A sample JSON response is provided below.

```
HTTP/1.1 200 OK

Cache-Control: private

Content-Type: application/json; charset=utf-8

Date: Thu, 14 Apr 2016 12:00:00 GMT

Content-Length: 39

{

        "Id" : "522e0c33e5671c06c14224d7"

}
```

Cache Settings

The endpoints covered in this section allow you to administer query string cache settings. They allow you to update and find out the query string cache and log settings across all HTTP platforms.

Get All Compression Settings

Provides compression setting information for all HTTP platforms. This means that it allows you to find out the current status of the **Compression** option and the file types that will be compressed.

Request

A request to find out compression setting information is described below. When submitting this request, you will need to define the following term:

- **AccountNumber:** This term should be replaced by your CDN account number. This number can be found in the upper-right hand corner of the MCC.

HTTP Method	Request URI
GET	https://api.edgecast.com/v2/mcc/customers/*AccountNumber*/compression

Request Headers
This endpoint only takes advantage of the common request headers described in the **Request Headers** section of the **Request and Response Elements** topic.

Request Body
Request body parameters are not required by this endpoint.

Response

The response to the above request includes an HTTP status code, response headers, and a response body.

Status Code
A status code indicates whether the request was successfully performed. A list of common status codes is provided in the **Status Codes and Error Messages** topic.

Response Headers
The response for this endpoint only returns standard HTTP response headers including those described in the **Response Headers** section of the **Request and Response Elements** topic.

Response Body

The response body for a successful request contains the following response elements for each set of platform-specific compression setting returned by this endpoint:

Name	Description
MediaTypeId	An integer that indicates the platform for which compression setting information will be reported. Valid values for this response element are: • **3:** HTTP Large • **8:** HTTP Small • **14:** Application Delivery Network (ADN)
Status	An integer that indicates whether compression has been enabled. Valid values for this response element are: • **0:** Indicates that compression has been disabled on the specified platform. • **1:** Indicates that compression has been enabled on the specified platform.
ContentTypes	If the **Compression** setting has been enabled, then this response element will contain the set of content types on which compression will be applied.
a:string	A string that indicates a content type on which compression will be applied.

Errors

The response body for an unsuccessful request may contain an error element that provides additional information. For a list of common error messages, please refer to the **Status Codes and Error Messages** topic.

Sample Request and Response

A sample JSON request is provided below.

```
GET https://api.edgecast.com/v2/mcc/customers/0001/compression HTTP/1.1

Authorization: TOK:12345678-1234-1234-1234-1234567890ab

Accept: application/json

Host: api.edgecast.com
```

A sample JSON response is provided below.

```
HTTP/1.1 200 OK
Cache-Control: private
Content-Type: application/json; charset=utf-8
Date: Thu, 14 Apr 2016 12:00:00 GMT
Content-Length: 231


[{
            "MediaTypeId" : 3,
            "Status" : 1,
            "ContentTypes" : ["text\/plain", "text\/html", "text\/css",
        "application\/x-javascript", "text\/javascript"]
        }, {
            "MediaTypeId" : 8,
            "Status" : 0,
            "ContentTypes" : [""]
        }
]
```

Get All Query String Caching Settings

Returns the value assigned to the **Query-String Caching** option for all HTTP platforms.

Request

A request to find out query string caching setting information is described below. When submitting this request, you will need to define the following term:

- **AccountNumber:** This term should be replaced by your CDN account number. This number can be found in the upper-right hand corner of the MCC.

HTTP Method	Request URI
GET	https://api.edgecast.com/v2/mcc/customers/*AccountNumber*/querystringcaching

Request Headers

This endpoint only takes advantage of the common request headers described in the **Request Headers** section of the **Request and Response Elements** topic.

Request Body

Request body parameters are not required by this endpoint.

Response

The response to the above request includes an HTTP status code, response headers, and a response body.

Status Code

A status code indicates whether the request was successfully performed. A list of common status codes is provided in the **Status Codes and Error Messages** topic.

Response Headers

The response for this endpoint only returns standard HTTP response headers including those described in the **Response Headers** section of the **Request and Response Elements** topic.

Response Body

The response body for a successful request contains the following response elements for each setting returned by this endpoint:

Name	Description
MediaTypeId	An integer that indicates the platform for which query string caching information is being reported. Valid values for this response element are: • **3:** HTTP Large • **8:** HTTP Small • **14:** Application Delivery Network (ADN)
QueryStringCaching	A string that indicates the value associated with the query string caching setting on the specified platform. Valid values for this response element are: • **standard-cache:** This mode ignores query strings in the URL when caching assets. • **no-cache:** This mode prevents requests containing query strings from being cached. • **unique-cache:** This mode caches an asset for each request made with a unique URL.

Errors

The response body for an unsuccessful request may contain an error element that provides additional information. For a list of common error messages, please refer to the **Status Codes and Error Messages** topic.

Sample Request and Response

A sample JSON request is provided below.

```
GET https://api.edgecast.com/v2/mcc/customers/0001/querystringcaching HTTP/1.1
Authorization: TOK:12345678-1234-1234-1234-1234567890ab
Accept: application/json
Host: api.edgecast.com
```

A sample JSON response is provided below.

```
HTTP/1.1 200 OK
Cache-Control: private
Content-Type: application/json; charset=utf-8
Date: Thu, 14 Apr 2016 12:00:00 GMT
Content-Length: 85


[{
            "MediaTypeId" : 3,
            "QueryStringCaching" : "unique-cache"
      }, {
            "MediaTypeId" : 8,
            "QueryStringCaching" : "unique-cache"
      }
]
```

Get All Query String Logging Settings

Returns the value assigned to the **Query-String Logging** option for all HTTP platforms.

Request

A request to find out query string logging information is described below. When submitting this request, you will need to define the following term:

- **AccountNumber:** This term should be replaced by your CDN account number. This number can be found in the upper-right hand corner of the MCC.

HTTP Method	Request URI
GET	https://api.edgecast.com/v2/mcc/customers/*AccountNumber*/ querystringlogging

Request Headers

This endpoint only takes advantage of the common request headers described in the **Request Headers** section of the **Request and Response Elements** topic.

Request Body

Request body parameters are not required by this endpoint.

Response

The response to the above request includes an HTTP status code, response headers, and a response body.

Status Code

A status code indicates whether the request was successfully performed. A list of common status codes is provided in the **Status Codes and Error Messages** topic.

Response Headers

The response for this endpoint only returns standard HTTP response headers including those described in the **Response Headers** section of the **Request and Response Elements** topic.

Response Body

The response body for a successful request contains the following response elements for each query string logging setting returned by this endpoint:

Name	Description
MediaTypeId	An integer that indicates the platform for which query string logging information was reported. Valid values for this response element are: • **3:** HTTP Large • **8:** HTTP Small • **14:** Application Delivery Network (ADN)
QueryStringLogging	A string that indicates the value associated with the query string logging setting on the specified platform. Valid values for this response element are: • **no-log:** This mode excludes a URL's query string when recording CDN activity in a raw log file. • **log:** This mode includes a URL's query string when recording CDN activity in a raw log file.

Errors

The response body for an unsuccessful request may contain an error element that provides additional information. For a list of common error messages, please refer to the **Status Codes and Error Messages** topic.

Sample Request and Response

A sample JSON request is provided below.

```
GET https://api.edgecast.com/v2/mcc/customers/0001/querystringlogging HTTP/1.1
Authorization: TOK:12345678-1234-1234-1234-1234567890ab
Accept: application/json
Host: api.edgecast.com
```

A sample JSON response is provided below.

```
HTTP/1.1 200 OK
Cache-Control: private
Content-Type: application/json; charset=utf-8
Date: Thu, 14 Apr 2016 12:00:00 GMT
Content-Length: 85
```

```
[{
            "MediaTypeId" : 3,

            "QueryStringLogging" : "log"

    }, {

            "MediaTypeId" : 8,

            "QueryStringLogging" : "log"

    }
]
```

Get Compression Setting

Provides compression setting information for the specified HTTP platform. This means that it allows you to find out the current status of the **Compression** option and the file types that will be compressed.

Request

A request to find out compression setting information is described below. When submitting this request, you will need to define the following terms:

- **AccountNumber:** This term should be replaced by your CDN account number. This number can be found in the upper-right hand corner of the MCC.

- **MediaTypeID:** This term should be replaced by the ID associated with the desired platform. Valid values for this parameter are listed below.

  - **3:** HTTP Large

  - **8:** HTTP Small

  - **14:** Application Delivery Network (ADN)

HTTP Method	Request URI
GET	https://api.edgecast.com/v2/mcc/customers/*AccountNumber*/compression? mediatypeid=*MediaTypeID*

Request Headers
This endpoint only takes advantage of the common request headers described in the **Request Headers** section of the **Request and Response Elements** topic.

Request Body
Request body parameters are not required by this endpoint.

Response

The response to the above request includes an HTTP status code, response headers, and a response body.

Status Code

A status code indicates whether the request was successfully performed. A list of common status codes is provided in the **Status Codes and Error Messages** topic.

Response Headers

The response for this endpoint only returns standard HTTP response headers including those described in the **Response Headers** section of the **Request and Response Elements** topic.

Response Body

The response body for a successful request contains the following response elements:

Name	Description
MediaTypeId	An integer that indicates the platform for which compression setting information will be reported. Valid values for this response element are: • **3:** HTTP Large • **8:** HTTP Small • **14:** Application Delivery Network (ADN)
Status	An integer that indicates whether compression has been enabled. Valid values for this response element are: • **0:** Indicates that compression has been disabled on the specified platform. • **1:** Indicates that compression has been enabled on the specified platform.
ContentTypes	If the **Compression** setting has been enabled, then this response element will contain the set of content types on which compression will be applied.
a:string	A string that indicates a content type on which compression will be applied.

Errors

The response body for an unsuccessful request may contain an error element that provides additional information. For a list of common error messages, please refer to the **Status Codes and Error Messages** topic.

Sample Request and Response

A sample JSON request is provided below.

```
GET https://api.edgecast.com/v2/mcc/customers/0001/compression?mediatypeid=3
HTTP/1.1

Authorization: TOK:12345678-1234-1234-1234-1234567890ab

Accept: application/json

Host: api.edgecast.com
```

A sample JSON response is provided below.

```
HTTP/1.1 200 OK

Cache-Control: private

Content-Type: application/json; charset=utf-8

Date: Thu, 14 Apr 2016 12:00:00 GMT

Content-Length: 149


{

        "MediaTypeId" : 3,

        "Status" : 1,

        "ContentTypes" : ["text\/plain", "text\/html", "text\/css", "application\/x-
        javascript", "text\/javascript"]

}
```

Get Query String Caching Setting

Returns the value assigned to the **Query-String Caching** option for the specified HTTP platform.

Request

A request to find out query string caching setting information is described below. When submitting this request, you will need to define the following terms:

- **AccountNumber:** This term should be replaced by your CDN account number. This number can be found in the upper-right hand corner of the MCC.

- **MediaTypeID:** This term should be replaced by the ID associated with the desired platform. Valid values for this parameter are listed below.

  - **3:** HTTP Large

  - **8:** HTTP Small

  - **14:** Application Delivery Network (ADN)

HTTP Method	Request URI
GET	https://api.edgecast.com/v2/mcc/customers/*AccountNumber*/querystringcaching?mediatypeid=*MediaTypeID*

Request Headers

This endpoint only takes advantage of the common request headers described in the **Request Headers** section of the **Request and Response Elements** topic.

Request Body

Request body parameters are not required by this endpoint.

Response

The response to the above request includes an HTTP status code, response headers, and a response body.

Status Code

A status code indicates whether the request was successfully performed. A list of common status codes is provided in the **Status Codes and Error Messages** topic.

Response Headers

The response for this endpoint only returns standard HTTP response headers including those described in the **Response Headers** section of the **Request and Response Elements** topic.

Response Body

The response body for a successful request contains the following response elements:

Name	Description
MediaTypeId	An integer that indicates the platform for which query string caching information was reported. Valid values for this response element are: • **3:** HTTP Large • **8:** HTTP Small • **14:** Application Delivery Network (ADN)

Name	Description
QueryStringCaching	A string that indicates the value associated with the query string caching setting on the specified platform. Valid values for this response element are: • **standard-cache:** This mode will ignore query strings in the URL when caching assets. • **no-cache:** This mode prevents requests containing query strings from being cached. • **unique-cache:** This mode will cache an asset for each request made with a unique URL.

Errors

The response body for an unsuccessful request may contain an error element that provides additional information. For a list of common error messages, please refer to the **Status Codes and Error Messages** topic.

Sample Request and Response

A sample JSON request is provided below.

```
GET https://api.edgecast.com/v2/mcc/customers/0001/querystringcaching?mediatypeid=3
HTTP/1.1

Authorization: TOK:12345678-1234-1234-1234-1234567890ab

Accept: application/json

Host: api.edgecast.com
```

A sample JSON response is provided below.

```
HTTP/1.1 200 OK

Cache-Control: private

Content-Type: application/json; charset=utf-8

Date: Thu, 14 Apr 2016 12:00:00 GMT

Content-Length: 85

{
        "MediaTypeId" : 3,
        "QueryStringCaching" : "unique-cache"
}
```

Get Query String Logging Setting

Returns the value assigned to the **Query-String Logging** option for the specified HTTP platform.

Request

A request to find out query string logging information is described below. When submitting this request, you will need to define the following terms:

- **AccountNumber:** This term should be replaced by your CDN account number. This number can be found in the upper-right hand corner of the MCC.

- **MediaTypeID:** This term should be replaced by the ID associated with the desired platform. Valid values for this parameter are listed below.

  - **3:** HTTP Large

  - **8:** HTTP Small

  - **14:** Application Delivery Network (ADN)

HTTP Method	Request URI
GET	https://api.edgecast.com/v2/mcc/customers/*AccountNumber*/querystringlogging?mediatypeid=*MediaTypeID*

Request Headers

This endpoint only takes advantage of the common request headers described in the **Request Headers** section of the **Request and Response Elements** topic.

Request Body

Request body parameters are not required by this endpoint.

Response

The response to the above request includes an HTTP status code, response headers, and a response body.

Status Code

A status code indicates whether the request was successfully performed. A list of common status codes is provided in the **Status Codes and Error Messages** topic.

Response Headers

The response for this endpoint only returns standard HTTP response headers including those described in the **Response Headers** section of the **Request and Response Elements** topic.

Response Body

The response body for a successful request contains the following response elements:

Name	Description
MediaTypeId	An integer that indicates the platform for which query string logging information was reported. Valid values for this response element are: • **3:** HTTP Large • **8:** HTTP Small • **14:** Application Delivery Network (ADN)
QueryStringCaching	A string that indicates the value associated with the query string caching setting on the specified platform. Valid values for this response element are: • **no-log:** This mode excludes a URL's query string when recording CDN activity in a raw log file. • **log:** This mode includes a URL's query string when recording CDN activity in a raw log file.

Errors

The response body for an unsuccessful request may contain an error element that provides additional information. For a list of common error messages, please refer to the **Status Codes and Error Messages** topic.

Sample Request and Response

JSON

A sample JSON request is provided below.

```
GET https://api.edgecast.com/v2/mcc/customers/0001/querystringlogging?mediatypeid=3
HTTP/1.1

Authorization: TOK:12345678-1234-1234-1234-1234567890ab

Accept: application/json

Host: api.edgecast.com
```

A sample JSON response is provided below.

```
HTTP/1.1 200 OK

Cache-Control: private

Content-Type: application/json; charset=utf-8

Date: Thu, 14 Apr 2016 12:00:00 GMT

Content-Length: 85
```

```
{
        "MediaTypeId" : 3,
        "QueryStringLogging" : "log"
}
```

Update Compression Settings

Updates compression setting information for the specified HTTP platform. This means that it allows you to set the current status of the **Compression** option and the file types that will be compressed.

Request

A request to set compression setting information is described below. When submitting this request, you will need to define the following term:

- **AccountNumber:** This term should be replaced by your CDN account number. This number can be found in the upper-right hand corner of the MCC.

HTTP Method	Request URI
PUT	https://api.edgecast.com/v2/mcc/customers/*AccountNumber*/compression

Request Headers

This endpoint only takes advantage of the common request headers described in the **Request Headers** section of the **Request and Response Elements** topic.

Request Body

Required and optional parameters are described below.

Name	Description
ContentTypes	Required. This response element can contain the set of content types on which compression will be applied.
string	A string that indicates a specific content type (e.g., text/plain) on which compression will be applied.
	Note: If you plan on using XML, then you will need to include the following XML namespace when specifying each content type: http://schemas.microsoft.com/2003/10/Serialization/Arrays (e.g., <string xmlns=" http://schemas.microsoft.com/2003/10/Serialization/Arrays ">).

Name	Description
MediaTypeId	Required. An integer that determines the platform for which compression setting information will be reported. Valid values are: • **3:** HTTP Large • **8:** HTTP Small • **14:** Application Delivery Network (ADN)
Status	An integer that determines whether compression will be enabled on the platform defined in the MediaTypeID response body parameter. Valid values are: • **0:** Disable • **1:** Enable

Response

The response to the above request includes an HTTP status code, response headers, and a response body.

Status Code

A status code indicates whether the request was successfully performed. A list of common status codes is provided in the **Status Codes and Error Messages** topic.

Response Headers

The response for this endpoint only returns standard HTTP response headers including those described in the **Response Headers** section of the **Request and Response Elements** topic.

Response Body

The response body for a successful request does not contain a response element.

Errors

The response body for an unsuccessful request may contain an error element that provides additional information. For a list of common error messages, please refer to the **Status Codes and Error Messages** topic.

Sample Request and Response

A sample JSON request is provided below.

```
PUT https://api.edgecast.com/v2/mcc/customers/0001/compression HTTP/1.1

Authorization: TOK:12345678-1234-1234-1234-1234567890ab

Accept: application/json

Content-Type: application/json

Host: api.edgecast.com

Content-Length: 149

{

        "ContentTypes" : ["text\/plain", "text\/html", "text\/css", "application\/x-
        javascript", "text\/javascript"],

        "MediaTypeId" : 3,

        "Status" : 1

}
```

A sample JSON response is provided below.

```
HTTP/1.1 200 OK

Cache-Control: private

Content-Type: application/json; charset=utf-8

Date: Thu, 14 Apr 2016 12:00:00 GMT
```

Update Query String Caching Setting

Sets the **Query-String Caching** option for the specified HTTP platform.

Request

A request to set the query string caching setting is described below. When submitting this request, you will need to define the following term:

- **AccountNumber:** This term should be replaced by your CDN account number. This number can be found in the upper-right hand corner of the MCC.

HTTP Method	Request URI
PUT	https://api.edgecast.com/v2/mcc/customers/*AccountNumber*/ querystringcaching

Request Headers

This endpoint only takes advantage of the common request headers described in the **Request Headers** section of the **Request and Response Elements** topic.

Request Body

The required request parameters for this endpoint are described below.

Name	Description
MediaTypeId	Required. An integer that determines the platform on which the query string caching setting will be set. Valid values for this request parameter are: • **3:** HTTP Large • **8:** HTTP Small • **14:** Application Delivery Network (ADN)
QueryStringCaching	Required. A case-sensitive string that determines the value that will be assigned to the query string caching setting on the specified platform. Valid values for this response element are: • **standard-cache:** This mode ignores query strings in the URL when caching assets. • **no-cache:** This mode prevents requests containing query strings from being cached. • **unique-cache:** This mode caches an asset for each request made with a unique URL.

Response

The response to the above request includes an HTTP status code, response headers, and a response body.

Status Code

A status code indicates whether the request was successfully performed. A list of common status codes is provided in the **Status Codes and Error Messages** topic.

Response Headers

The response for this endpoint only returns standard HTTP response headers including those described in the **Response Headers** section of the **Request and Response Elements** topic.

Response Body

The response body for a successful request does not contain a response element.

Errors

The response body for an unsuccessful request may contain an error element that provides additional information. For a list of common error messages, please refer to the **Status Codes and Error Messages** topic.

Sample Request and Response

A sample JSON request is provided below.

```
PUT https://api.edgecast.com/v2/mcc/customers/0001/querystringcaching HTTP/1.1

Authorization: TOK:12345678-1234-1234-1234-1234567890ab

Accept: application/json

Content-Type: application/json

Host: api.edgecast.com

Content-Length: 47

{

        "MediaTypeId" : 8,

        "QueryStringCaching" : "no-cache"

}
```

A sample JSON response is provided below.

```
HTTP/1.1 200 OK

Cache-Control: private

Content-Type: application/json; charset=utf-8

Date: Thu, 14 Apr 2016 12:00:00 GMT
```

Update Query String Logging Status

Sets the **Query-String Logging** option for the specified HTTP platform.

Request

A request to set the query string logging setting is described below. When submitting this request, you will need to define the following term:

- **AccountNumber:** This term should be replaced by your CDN account number. This number can be found in the upper-right hand corner of the MCC.

HTTP Method	Request URI
PUT	https://api.edgecast.com/v2/mcc/customers/*AccountNumber*/querystringlogging

Request Headers

This endpoint only takes advantage of the common request headers described in the **Request Headers** section of the **Request and Response Elements** topic.

Request Body

The required request parameters for this endpoint are described below.

Name	Description
MediaTypeId	Required. An integer that determines the platform on which the query string logging setting will be set. Valid values for this request parameter are: • **3:** HTTP Large • **8:** HTTP Small • **14:** Application Delivery Network (ADN)
QueryStringLogging	Required. A case-sensitive string that determines the value that will be assigned to the query string logging setting on the specified platform. Valid values for this response element are: • **no-log:** This mode excludes a URL's query string when recording CDN activity in a raw log file. • **log:** This mode includes a URL's query string when recording CDN activity in a raw log file.

Response

The response to the above request includes an HTTP status code, response headers, and a response body.

Status Code

A status code indicates whether the request was successfully performed. A list of common status codes is provided in the **Status Codes and Error Messages** topic.

Response Headers

The response for this endpoint only returns standard HTTP response headers including those described in the **Response Headers** section of the **Request and Response Elements** topic.

Response Body

The response body for a successful request does not contain a response element.

Errors

The response body for an unsuccessful request may contain an error element that provides additional information. For a list of common error messages, please refer to the **Status Codes and Error Messages** topic.

Sample Request and Response

A sample JSON request is provided below.

```
PUT https://api.edgecast.com/v2/mcc/customers/0001/querystringlogging HTTP/1.1

Authorization: TOK:12345678-1234-1234-1234-1234567890ab

Accept: application/json

Content-Type: application/json

Host: api.edgecast.com

Content-Length: 52


{

        "MediaTypeId" : 8,

        "QueryStringLogging" : "log"

}
```

A sample JSON response is provided below.

```
HTTP/1.1 200 OK

Cache-Control: private

Content-Type: application/json; charset=utf-8

Date: Thu, 14 Apr 2016 12:00:00 GMT
```

Customer Origin

The endpoints covered in this section allow you to add, retrieve, update, and delete customer origins. The creation and modification of a customer origin is handled by platform-specific endpoints, while the deletion of a customer origin can be performed by a single endpoint.

Add Customer Origin (ADN)

Adds a customer origin to the ADN platform.

Request

A request to create a customer origin is described below. When submitting this request, you will need to define the following term:

- **xxxx:** Replace this term with your CDN account number.

HTTP Method	Request URI
POST	https://api.edgecast.com/v2/mcc/customers/*xxxx*/origins/adn

Request Headers

This endpoint only takes advantage of the common request headers described in the **Request Headers** section of the **Request and Response Elements** topic.

Request Body

The required request parameters for this endpoint are described below.

Note: The indented parameters indicate that they are a property of the request parameter directly above it. When submitting a request, you will need to use the proper syntax to indicate this relationship. Please refer to the parent request parameter for more information.

Note: Hostnames are associated with a customer origin configuration according to the request type (i.e., HTTP or HTTPS) that they will handle. Although you may choose to define a set of hostnames for each request type, you are only required to specify a single hostname and load balancing method for either request type. If you choose to define one or more hostnames, then you will also need to define the load balancing method for that request type.

Name	Description
DirectoryName	Required. An alphanumeric string that identifies your customer origin configuration. It is appended to the end of the base CDN URL that points to your customer origin server (e.g., http://adn.0001.edgecastcdn.net/800001/***CustomerOrigin***).
FollowRedirects	A Boolean that determines whether our edge servers will respect a URL redirect when validating the set of optimal ADN gateway servers for your customer origin configuration. **Default value:** False

Name	Description
HostHeader	Required. A string that identifies the IP address/hostname and port associated with a request. A host header is especially useful when there are multiple virtual domains hosted on a single physical server or load-balanced set of servers. **Note:** A protocol should not be specified when setting this parameter.
HttpHostnames	Required. This response element is only used to indicate that you plan on specifying one or more hostnames for handling HTTP requests. Keep in mind the following formatting information: • **XML:** Each hostname must be contained within a <Hostname> tag. • **JSON:** The desired set of hostnames must be contained within a set of square brackets. Additionally, each hostname (i.e., Name request parameter) must be contained with a set of curly braces.
Name	Required. A string that determines the hostname/IP address of the origin server that will be associated with the customer origin configuration being created. Use one of the following formats to identify an origin server: • *protocol*://*hostname*:*port* (e.g., http://www.mydomain.com:80) • *protocol*://*IPv4Address*:*port* (e.g., http://10.10.10.255:80) • *protocol*://[*IPv6Address*]:*port* (e.g., http://[1:2:3:4:5:6:7:8]:80)

Name	Description
HttpLoadBalancing	Required. A string that determines how HTTP requests will be load balanced for the specified hostnames. Our servers will use DNS to resolve the specified hostnames into an ordered list of IP addresses. If you have only specified a single web server for this origin server configuration, then either of the following load balancing methods will serve requests through that web server. Valid values for this request parameter are described below. • **PF:** This value indicates that "Primary and Failover" mode will be used to load balance requests for this customer origin. In this mode, the specified hostnames form an ordered failover list. All requests will first be sent to the first hostname in the list. If that server is unavailable (i.e., TCP connection is refused or a timeout occurs), then the request will be sent to the next hostname. • **RR:** This value indicates that "Round Robin" mode will be used to load balance requests for this customer origin. In this mode, our servers will send a balanced numbers of requests to each hostname. **Note:** The load balancing mode specified for your customer origin configuration is independent from any load balancing configuration that may exist at the origin server.
HttpsHostnames	Required. This response element is only used to indicate that you plan on specifying one or more hostnames for handling HTTPS requests. Keep in mind the following formatting information: • **XML:** Each hostname must be contained within a <Hostname> tag. • **JSON:** The desired set of hostnames must be contained within a set of square brackets. Additionally, each hostname (i.e., Name request parameter) must be contained with a set of curly braces. **Important:** This request parameter is only available for customers that have purchased an SSL certificate or the HTTPS feature.

Name	Description
Name	Required. A string that determines the hostname/IP address of the origin server that will be associated with the customer origin configuration being created. Use one of the following formats to identify an origin server: • *protocol*://*hostname*:*port* (e.g., http://www.mydomain.com:80) • *protocol*://*IPv4Address*:*port* (e.g., http://10.10.10.255:80) • *protocol*://[*IPv6Address*]:*port* (e.g., http://[1:2:3:4:5:6:7:8]:80) **Note:** If you specify HTTP hostnames to serve HTTPS requests, then you will sacrifice end-to-end data encryption.
HttpsLoadBalancing	Required. A string that determines how HTTPS requests will be load balanced for the specified hostnames. Our servers will use DNS to resolve the specified hostnames into an ordered list of IP addresses. If you have only specified a single web server for this origin server configuration, then either of the following load balancing methods will serve requests through that web server. Valid values for this request parameter are described below. • **PF:** This value indicates that "Primary and Failover" mode will be used to load balance requests for this customer origin. In this mode, the specified hostnames form an ordered failover list. All requests will first be sent to the first hostname in the list. If that server is unavailable (i.e., TCP connection is refused or a timeout occurs), then the request will be sent to the next hostname. • **RR:** This value indicates that "Round Robin" mode will be used to load balance requests for this customer origin. In this mode, our servers will send a balanced numbers of requests to each hostname. **Note:** The load balancing mode specified for your customer origin configuration is independent from any load balancing configuration that may exist at the origin server.

Name	Description
NetworkConfiguration	An integer that determines how hostnames associated with this customer origin configuration will be resolved to an IP address. Valid values are: • **1:** Default. Indicates that the IP preference for this customer origin will be system-defined. Currently, this configuration causes hostnames to be resolved to IPv4 only. • **2:** IPv6 Preferred over IPv4. Indicates that although hostnames for this customer origin can be resolved to either IP version, a preference will be given to IPv6. • **3:** IPv4 Preferred over IPv6. Indicates that although hostnames for this customer origin can be resolved to either IP version, a preference will be given to IPv4. • **4:** IPv4 Only. Indicates that hostnames for this customer origin can only be resolved to IPv4. • **5:** IPv6 Only. Indicates that hostnames for this customer origin can only be resolved to IPv6.
ValidationURL	Required. A string that defines the URL to a sample asset stored on your servers. A set of optimal ADN gateway servers for your customer origin server is determined through the delivery of this sample asset. **Note:** Make sure that the domain in the specified URL matches the one defined in the HostHeader request parameter.

Response

The response to the above request includes an HTTP status code, response headers, and a response body.

Status Code

A status code indicates whether the request was successfully performed. A list of common status codes is provided in the **Status Codes and Error Messages** topic.

Response Headers

The response for this endpoint only returns standard HTTP response headers including those described in the **Response Headers** section of the **Request and Response Elements** topic.

Response Body

The response body for a successful request contains the following response element:

Name	Description
CustomerOriginId	An integer that indicates the unique ID assigned to this customer origin configuration.

Errors

The response body for an unsuccessful request may contain an error element that provides additional information. For a list of common error messages, please refer to the **Status Codes and Error Messages** topic.

Sample Request and Response

A sample JSON request is provided below.

```
POST https://api.edgecast.com/v2/mcc/customers/0001/origins/adn HTTP/1.1

Authorization: TOK:12345678-1234-1234-1234-1234567890ab

Accept: application/json

Content-Type: application/json

Host: api.edgecast.com

Content-Length: 419


{
        "DirectoryName" : "MyWebServer",

        "HostHeader" : "webapp.mydomain.com:80",

        "HttpHostnames" :

        [{

                    "Name" : "http:\/\/webapp1.mydomain.com:80"

                }, {

                    "Name" : "http:\/\/webapp2.mydomain.com:80"

                }

        ],

        "HttpLoadBalancing" : "RR",

        "HttpsHostnames" :

        [{

                    "Name" : "https:\/\/webapp.mydomain.com:443"

                }

        ],

        "HttpsLoadBalancing" : "PF",

        "ValidationURL":"http:\/\/webapp.mydomain.com:80\/images\/PerformanceTestObje
        ct_5k.gif"

}
```

A sample JSON response is provided below.

```
HTTP/1.1 200 OK

Cache-Control: private

Content-Length: 25

Content-Type: application/json; charset=utf-8

Date: Mon, 10 Jan 2011 12:00:00 GMT


{

       "CustomerOriginId" : 123456

}
```

Add Customer Origin (HTTP Large)

Adds a customer origin to the HTTP Large platform.

Request

A request to create a customer origin configuration is described below.

- **xxxx:** Replace this term with your CDN account number.

HTTP Method	Request URI
POST	https://api.edgecast.com/v2/mcc/customers/*xxxx*/origins/httplarge

Request Headers

This endpoint only takes advantage of the common request headers described in the **Request Headers** section of the **Request and Response Elements** topic.

Request Body

Optional and required request parameters for this endpoint are described below.

Note: The indented parameters indicate that they are a property of the request parameter directly above it. When submitting a request, you will need to use the proper syntax to indicate this relationship. Please refer to the parent request parameter for more information.

Note: Hostnames are associated with a customer origin configuration according to the request type (i.e., HTTP or HTTPS) that they will handle. Although you may choose to define a set of hostnames for each request type, you are only required to specify a single hostname and load balancing method for either request type. If you choose to define one or more hostnames, then you will also need to define the load balancing method for that request type.

Name	Description
DirectoryName	Required. An alphanumeric string that identifies your customer origin configuration. It is appended to the end of the base CDN URL that points to your customer origin server (e.g., http://wpc.0001.edgecastcdn.net/800001/***CustomerOrigin***).
HostHeader	Required. A string that identifies the IP address/hostname and port that will be reported in the Host header field for requests to this customer origin. A host header is especially useful when there are multiple virtual domains hosted on a single physical server or load-balanced set of servers.
	Note: A protocol should not be specified when setting this parameter.
HttpHostnames	Required. This response element is only used to indicate that you plan on specifying one or more hostnames/IP addresses. Keep in mind the following formatting information:
	• **XML:** Each hostname/IP address must be contained within a <Hostname> tag.
	• **JSON:** The desired set of hostnames/IP addresses must be contained within a set of square brackets. Additionally, each one (i.e., Name request parameter) must be contained with a set of curly braces.
Name	Required. A string that determines the hostname/IP address of the origin server that will be associated with the customer origin configuration being created.
	Use one of the following formats to identify an origin server:
	• *protocol*://*hostname*:*port* (e.g., http://www.mydomain.com:80)
	• *protocol*://*IPv4Address*:*port* (e.g., http://10.10.10.255:80)
	• *protocol*://[*IPv6Address*]:*port* (e.g., http://[1:2:3:4:5:6:7:8]:80)
HttpLoadBalancing	Required. A string that determines how HTTP requests will be load balanced for the specified hostnames. Our servers will use DNS to resolve the specified hostnames into an ordered list of IP addresses. If you have only specified a single web server for this origin server configuration, then either of the following load balancing methods will serve requests through that web server.
	Valid values for this request parameter are described below.
	• **PF:** This value indicates that "Primary and Failover" mode will be used to load balance requests for this customer origin. In this mode, the specified hostnames form an ordered failover

Name	Description
	list. All requests will first be sent to the first hostname in the list. If that server is unavailable (i.e., TCP connection is refused or a timeout occurs), then the request will be sent to the next hostname. • **RR:** This value indicates that "Round Robin" mode will be used to load balance requests for this customer origin. In this mode, our servers will send a balanced numbers of requests to each hostname. **Note:** The load balancing mode specified for your customer origin configuration is independent from any load balancing configuration that may exist at the origin server.
HttpsHostnames	Required. This response element is only used to indicate that you plan on specifying one or more hostnames/IP addresses for handling HTTPS requests. Keep in mind the following formatting information: • **XML:** Each hostname/IP address must be contained within a \<Hostname> tag. • **JSON:** The desired set of hostnames/IP addresses must be contained within a set of square brackets. Additionally, each one (i.e., Name request parameter) must be contained with a set of curly braces. **Important:** This request parameter is only available for customers that have purchased an SSL certificate or the HTTPS feature.
Name	Required. A string that determines the hostname/IP address of the origin server that will be associated with the customer origin configuration being created. Use one of the following formats to identify an origin server: • *protocol*://*hostname*:*port* (e.g., http://www.mydomain.com:80) • *protocol*://*IPv4Address*:*port* (e.g., http://10.10.10.255:80) • *protocol*://[*IPv6Address*]:*port* (e.g., http://[1:2:3:4:5:6:7:8]:80) **Note:** If you specify HTTP hostnames to serve HTTPS requests, then you will sacrifice end-to-end data encryption.
HttpsLoadBalancing	Required. A string that determines how HTTPS requests will be load balanced for the specified hostnames. Our servers will use DNS to resolve the specified hostnames into an ordered list of IP addresses. If you have only specified a single web server for this origin server

Name	Description
	configuration, then either of the following load balancing methods will serve requests through that web server. Valid values for this request parameter are described below. • **PF:** This value indicates that "Primary and Failover" mode will be used to load balance requests for this customer origin. In this mode, the specified hostnames form an ordered failover list. All requests will first be sent to the first hostname in the list. If that server is unavailable (i.e., TCP connection is refused or a timeout occurs), then the request will be sent to the next hostname. • **RR:** This value indicates that "Round Robin" mode will be used to load balance requests for this customer origin. In this mode, our servers will send a balanced numbers of requests to each hostname. **Note:** The load balancing mode specified for your customer origin configuration is independent from any load balancing configuration that may exist at the origin server.
ShieldPOPs	The Origin Shield feature, which must be purchased separately, can be used to reduce the number of requests that must be handled by your customer origin server. If you choose to protect your customer origin with this feature, then you will need to specify each point-of-presence (POP) location where Origin Shield servers will be used to provide an intermediate cache layer between our edge servers and your customer origin. Specify each desired Origin Shield location as an object containing the following key-value pair: 'POPCode': "{*Origin Shield Location*}" **Tip:** If you would like to configure the Origin Shield feature to produce an optimal reduction in requests to your customer origin server, then you should only specify a single location. The specified location should be the POP closest to your customer origin server. **Tip:** Turn off Origin Shield by specifying an empty array. **Note:** Do not specify more than 4 Origin Shield locations.

Name	Description
POPCode	A string that indicates a three or four-letter abbreviation for the desired Origin Shield location. For more information, please refer to the **Appendix E: Origin Shield Locations and Settings** section.
	Important: Specify each desired location using uppercase letters.
	Tip: A list of locations can be retrieved through the Get Origin Shield POPs - HTTP Large endpoint.
networkConfiguration	An integer that determines how hostnames associated with this customer origin configuration will be resolved to an IP address. Valid values are:

- **1:** Default. Indicates that the IP preference for this customer origin will be system-defined. Currently, this configuration causes hostnames to be resolved to IPv4 only.

- **2:** IPv6 Preferred over IPv4. Indicates that although hostnames for this customer origin can be resolved to either IP version, a preference will be given to IPv6.

- **3:** IPv4 Preferred over IPv6. Indicates that although hostnames for this customer origin can be resolved to either IP version, a preference will be given to IPv4.

- **4:** IPv4 Only. Indicates that hostnames for this customer origin can only be resolved to IPv4.

- **5:** IPv6 Only. Indicates that hostnames for this customer origin can only be resolved to IPv6.

Response

The response to the above request includes an HTTP status code, response headers, and a response body.

Status Code
A status code indicates whether the request was successfully performed. A list of common status codes is provided in the **Status Codes and Error Messages** topic.

Response Headers
The response for this endpoint only returns standard HTTP response headers including those described in the **Response Headers** section of the **Request and Response Elements** topic.

Response Body
The response body for a successful request contains the following response element:

Name	Description
CustomerOriginId	An integer that indicates the unique ID assigned to this customer origin configuration.

Errors

The response body for an unsuccessful request may contain an error element that provides additional information. For a list of common error messages, please refer to the **Status Codes and Error Messages** topic.

Sample Request and Response

A sample JSON request is provided below.

```
POST https://api.edgecast.com/v2/mcc/customers/0001/origins/httplarge HTTP/1.1
Authorization: TOK:12345678-1234-1234-1234-1234567890ab
Accept: application/json
Content-Type: application/json
Host: api.edgecast.com
Content-Length: 413


{
        "DirectoryName" : "MyCustomerOrigin",
        "HostHeader" : "images.mydomain.com:80",
        "HttpHostnames" :
        [{
                    "Name" : "http:\/\/images1.mydomain.com:80"
             }, {
                    "Name" : "http:\/\/images2.mydomain.com:80"
             }
        ],
        "HttpLoadBalancing" : "RR",
        "HttpsHostnames" :
        [{
                    "Name" : "https:\/\/images.mydomain.com:443"
             }
        ],
        "HttpsLoadBalancing" : "PF",
        "ShieldPOPs" :
        [{
                    "POPCode" : "LAA"
```

```
            }
        ]
}
```

A sample JSON response is provided below.

```
HTTP/1.1 200 OK

Cache-Control: private

Content-Length: 25

Content-Type: application/json; charset=utf-8

Date: Mon, 10 Jan 2011 12:00:00 GMT


{

        "CustomerOriginId" : 1234

}
```

Add Customer Origin (HTTP Small)

Adds a customer origin to the HTTP Large platform.

Request

A request to create a customer origin is described below. When submitting this request, you will need to define the following terms:

- **xxxx:** Replace this term with your CDN account number.

HTTP Method	Request URI
POST	https://api.edgecast.com/v2/mcc/customers/*xxxx*/origins/httpsmall

Request Headers

This endpoint only takes advantage of the common request headers described in the **Request Headers** section of the **Request and Response Elements** topic.

Request Body

Optional and required request parameters for this endpoint are described below.

Note: The indented parameters indicate that they are a property of the request parameter directly above it. When submitting a request, you will need to use the proper syntax to indicate this relationship. Please refer to the parent request parameter for more information.

Note: Hostnames are associated with a customer origin configuration according to the request type (i.e., HTTP or HTTPS) that they will handle. Although you may choose to define a set of hostnames for each request type, you are only required to specify a single hostname and load

balancing method for either request type. If you choose to define one or more hostnames, then you will also need to define the load balancing method for that request type.

Name	Description
DirectoryName	Required. An alphanumeric string that identifies your customer origin configuration. It is appended to the end of the base CDN URL that points to your customer origin server (e.g., http://wac.0001.edgecastcdn.net/800001/*CustomerOrigin*).
HostHeader	Required. A string that identifies the IP address/hostname and port associated with a request. A host header is especially useful when there are multiple virtual domains hosted on a single physical server or load-balanced set of servers. **Note:** A protocol should not be specified when setting this parameter.
HttpHostnames	Required. This response element is only used to indicate that you plan on specifying one or more hostnames for handling HTTP requests. Keep in mind the following formatting information: • **XML:** Each hostname must be contained within a <Hostname> tag. • **JSON:** The desired set of hostnames must be contained within a set of square brackets. Additionally, each hostname (i.e., Name request parameter) must be contained with a set of curly braces.
Name	Required. A string that determines the hostname/IP address of the origin server that will be associated with the customer origin configuration being created. Use one of the following formats to identify an origin server: • *protocol*://*hostname*:*port* (e.g., http://www.mydomain.com:80) • *protocol*://*IPv4Address*:*port* (e.g., http://10.10.10.255:80) • *protocol*://[*IPv6Address*]:*port* (e.g., http://[1:2:3:4:5:6:7:8]:80)

Name	Description
HttpLoadBalancing	Required. A string that determines how HTTP requests will be load balanced for the specified hostnames. Our servers will use DNS to resolve the specified hostnames into an ordered list of IP addresses. If you have only specified a single web server for this origin server configuration, then either of the following load balancing methods will serve requests through that web server. Valid values for this request parameter are described below. • **PF:** This value indicates that "Primary and Failover" mode will be used to load balance requests for this customer origin. In this mode, the specified hostnames form an ordered failover list. All requests will first be sent to the first hostname in the list. If that server is unavailable (i.e., TCP connection is refused or a timeout occurs), then the request will be sent to the next hostname. • **RR:** This value indicates that "Round Robin" mode will be used to load balance requests for this customer origin. In this mode, our servers will send a balanced numbers of requests to each hostname. **Note:** The load balancing mode specified for your customer origin configuration is independent from any load balancing configuration that may exist at the origin server.
HttpsHostnames	Required. This response element is only used to indicate that you plan on specifying one or more hostnames for handling HTTPS requests. Keep in mind the following formatting information: • **XML:** Each hostname must be contained within a <Hostname> tag. • **JSON:** The desired set of hostnames must be contained within a set of square brackets. Additionally, each hostname (i.e., Name request parameter) must be contained with a set of curly braces. **Important:** This request parameter is only available for customers that have purchased an SSL certificate or the HTTPS feature.

Name	Description
Name	Required. A string that determines the hostname/IP address of the origin server that will be associated with the customer origin configuration being created.
	Use one of the following formats to identify an origin server:
	• *protocol*://*hostname*:*port* (e.g., http://www.mydomain.com:80)
	• *protocol*://*IPv4Address*:*port* (e.g., http://10.10.10.255:80)
	• *protocol*://[*IPv6Address*]:*port* (e.g., http://[1:2:3:4:5:6:7:8]:80)
	Note: If you specify HTTP hostnames to serve HTTPS requests, then you will sacrifice end-to-end data encryption.
HttpsLoadBalancing	Required. A string that determines how HTTPS requests will be load balanced for the specified hostnames. Our servers will use DNS to resolve the specified hostnames into an ordered list of IP addresses. If you have only specified a single web server for this origin server configuration, then either of the following load balancing methods will serve requests through that web server.
	Valid values for this request parameter are described below.
	• **PF:** This value indicates that "Primary and Failover" mode will be used to load balance requests for this customer origin. In this mode, the specified hostnames form an ordered failover list. All requests will first be sent to the first hostname in the list. If that server is unavailable (i.e., TCP connection is refused or a timeout occurs), then the request will be sent to the next hostname.
	• **RR:** This value indicates that "Round Robin" mode will be used to load balance requests for this customer origin. In this mode, our servers will send a balanced numbers of requests to each hostname.
	Note: The load balancing mode specified for your customer origin configuration is independent from any load balancing configuration that may exist at the origin server.

Name	Description
ShieldPOPs	The Origin Shield feature, which must be purchased separately, can be used to reduce the number of requests that must be handled by your customer origin server. If you choose to protect your customer origin with this feature, then you will need to specify each point-of-presence (POP) location where Origin Shield servers will be used to provide an intermediate cache layer between our edge servers and your customer origin.
	Specify each desired Origin Shield location as an object containing the following key-value pair:
	'POPCode': "{*Origin Shield Location*}"
	Tip: If you would like to configure the Origin Shield feature to produce an optimal reduction in requests to your customer origin server, then you should only specify a single location. The specified location should be the POP closest to your customer origin server.
	Tip: Turn off Origin Shield by specifying an empty array.
	Note: Do not specify more than 4 Origin Shield locations.
POPCode	A string that indicates a three or four-letter abbreviation for the desired Origin Shield location. For more information, please refer to the **Appendix E: Origin Shield Locations and Settings** section.
	Important: Specify each desired location using uppercase letters.
	Tip: A list of locations can be retrieved through the Get Origin Shield POPs - HTTP Small endpoint.

Name	Description
networkConfiguration	An integer that determines how hostnames associated with this customer origin configuration will be resolved to an IP address. Valid values are: • **1:** Default. Indicates that the IP preference for this customer origin will be system-defined. Currently, this configuration causes hostnames to be resolved to IPv4 only. • **2:** IPv6 Preferred over IPv4. Indicates that although hostnames for this customer origin can be resolved to either IP version, a preference will be given to IPv6. • **3:** IPv4 Preferred over IPv6. Indicates that although hostnames for this customer origin can be resolved to either IP version, a preference will be given to IPv4. • **4:** IPv4 Only. Indicates that hostnames for this customer origin can only be resolved to IPv4. • **5:** IPv6 Only. Indicates that hostnames for this customer origin can only be resolved to IPv6.

Response

The response to the above request includes an HTTP status code, response headers, and a response body.

Status Code

A status code indicates whether the request was successfully performed. A list of common status codes is provided in the **Status Codes and Error Messages** topic.

Response Headers

The response for this endpoint only returns standard HTTP response headers including those described in the **Response Headers** section of the **Request and Response Elements** topic.

Response Body

The response body for a successful request contains the following response element:

Name	Description
CustomerOriginId	An integer that indicates the unique ID assigned to this customer origin configuration.

Errors

The response body for an unsuccessful request may contain an error element that provides additional information. For a list of common error messages, please refer to the **Status Codes and Error Messages** topic.

Sample Request and Response

A sample JSON request is provided below.

```
POST https://api.edgecast.com/v2/mcc/customers/0001/origins/httpsmall HTTP/1.1
Authorization: TOK:12345678-1234-1234-1234-1234567890ab
Accept: application/json
Content-Type: application/json
Host: api.edgecast.com
Content-Length: 385


{
        "DirectoryName" : "MyCustomerOrigin",
        "HostHeader" : "images.mydomain.com:80",
        "HttpHostnames" :
        [{
                        "Name" : "http:\/\/images1.mydomain.com:80"
                }, {
                        "Name" : "http:\/\/images2.mydomain.com:80"
                }
        ],
        "HttpLoadBalancing" : "RR",
        "HttpsHostnames" :
        [{
                        "Name" : "https:\/\/images.mydomain.com:443"
                }
        ],
        "HttpsLoadBalancing" : "PF",
        "ShieldPOPs" :
        [{
                        "POPCode" : "OXR"
                }
        ]
}
```

A sample JSON response is provided below.

```
HTTP/1.1 200 OK

Cache-Control: private

Content-Length: 25

Content-Type: application/json; charset=utf-8

Date: Mon, 10 Jan 2011 12:00:00 GMT


{

        "CustomerOriginId" : 1234

}
```

Delete Customer Origin

Deletes a customer origin.

Important: The deletion of a customer origin takes place immediately. Additionally, once a customer origin has been deleted, it cannot be recovered.

Request

A request to delete a customer origin is described below. When submitting this request, you will need to define the following terms:

- **xxxx:** Replace this term with your CDN account number.

- **CustomerOriginID:** Replace this term with the ID of the customer origin configuration that should be deleted.

HTTP Method	Request URI
DELETE	https://api.edgecast.com/v2/mcc/customers/*xxxx*/origins/*CustomerOriginID*

Request Headers
This endpoint only takes advantage of the common request headers described in the **Request Headers** section of the **Request and Response Elements** topic.

Request Body
Request body parameters are not required by this endpoint.

Response

The response to the above request includes an HTTP status code, response headers, and a response body.

Status Code

A status code indicates whether the request was successfully performed. A list of common status codes is provided in the **Status Codes and Error Messages** topic.

Response Headers

The response for this endpoint only returns standard HTTP response headers including those described in the **Response Headers** section of the **Request and Response Elements** topic.

Response Body

The response body for a successful request does not contain a response element.

Errors

The response body for an unsuccessful request may contain an error element that provides additional information. For a list of common error messages, please refer to the **Status Codes and Error Messages** topic.

Sample Request and Response

The request format is identical for both JSON and XML. A sample request is provided below.

```
DELETE https://api.edgecast.com/v2/mcc/customers/0001/origins/10 HTTP/1.1
Authorization: TOK:12345678-1234-1234-1234-1234567890ab
Host: api.edgecast.com
```

The response is identical for both JSON and XML. A sample response is provided below.

```
HTTP/1.1 200 OK
Cache-Control: private
Date: Mon, 10 Jan 2011 12:00:00 GMT
```

Get All Customer Origins (ADN)

Retrieves all customer origins for the ADN platform.

Request

A request to retrieve a list of the customer origins (ADN) associated with a customer's account is described below. When submitting this request, you will need to define the following term:

- **xxxx:** Replace this term with your CDN account number.

HTTP Method	Request URI
GET	https://api.edgecast.com/v2/mcc/customers/*xxxx*/origins/adn

Request Headers

This endpoint only takes advantage of the common request headers described in the **Request Headers** section of the **Request and Response Elements** topic.

Request Body

Request body parameters are not required by this endpoint.

Response

The response to the above request includes an HTTP status code, response headers, and a response body.

Status Code

A status code indicates whether the request was successfully performed. A list of common status codes is provided in the **Status Codes and Error Messages** topic.

Response Headers

The response for this endpoint only returns standard HTTP response headers including those described in the **Response Headers** section of the **Request and Response Elements** topic.

Response Body

The response body for a successful request contains the following response elements for each customer origin returned by this endpoint:

Name	Description
FollowRedirects	A Boolean that indicates whether our edge servers will respect a URL redirect when validating the set of optimal ADN gateway servers for your customer origin configuration.

Name	Description
NetworkConfiguration	An integer that indicates how hostnames associated with a customer origin configuration will be resolved to an IP address. Valid values are: • **1:** Default. Indicates that the IP preference for this customer origin will be system-defined. Currently, this configuration causes hostnames to be resolved to IPv4 only. • **2:** IPv6 Preferred over IPv4. Indicates that although hostnames for this customer origin can be resolved to either IP version, a preference will be given to IPv6. • **3:** IPv4 Preferred over IPv6. Indicates that although hostnames for this customer origin can be resolved to either IP version, a preference will be given to IPv4. • **4:** IPv4 Only. Indicates that hostnames for this customer origin can only be resolved to IPv4. • **5:** IPv6 Only. Indicates that hostnames for this customer origin can only be resolved to IPv6.
ValidationURL	A string that indicates the URL to a sample asset. A set of optimal ADN gateway servers for your customer origin server is determined through the delivery of this sample asset.
DirectoryName	An alphanumeric string that identifies your customer origin configuration. This name is appended to the end of the base CDN URL that points to your customer origin server (e.g., http://adn.0001.edgecastcdn.net/800001/*CustomerOrigin*).
HostHeader	A string that identifies the IP address/hostname and port associated with a request.
HttpFullUrl	A string that indicates the CDN URL for HTTP requests to this customer origin server.
HttpHostnames	This response element contains the hostnames that will handle HTTP requests.
IsPrimary	This response element indicates whether the current hostname is the primary one for HTTP requests. Valid values for this response element are described below. • **0:** Indicates that the current hostname is not the primary one. This value will always be reported for the Round-Robin load balancing mode. • **1:** Indicates that the current hostname is the primary one.
Name	This string reports the URL for the current hostname. This URL consists of the protocol, hostname, and the port.

Name	Description
Ordinal	This integer indicates the position in the ordered list for the current hostname. This position is primarily used by "Primary and Failover" load balancing mode to determine which hostname will take over when a hostname higher on the list is unreachable.
HttpLoadBalancing	A string that indicates how HTTP requests will be load balanced for the specified hostnames. Valid values for this response element are described below. • **PF:** This value indicates that "Primary and Failover" mode will be used to load balance requests for this customer origin. In this mode, the specified hostnames form an ordered failover list. All requests will first be sent to the first hostname in the list. If that server is unavailable (i.e., TCP connection is refused or a timeout occurs), then the request will be sent to the next hostname. • **RR:** This value indicates that "Round Robin" mode will be used to load balance requests for this customer origin. In this mode, our servers will send a balanced numbers of requests to each hostname. **Note:** The load balancing mode indicated for your customer origin configuration is independent from any load balancing configuration that may exist at the origin server.
HttpsFullUrl	A string that indicates the CDN URL for HTTPS requests to this customer origin server.
HttpsHostnames	This response element contains the hostnames that will handle HTTPS requests.
IsPrimary	This response element indicates whether the current hostname is the primary one for HTTPS requests. Valid values for this response element are described below. • **0:** Indicates that the current hostname is not the primary one. This value will always be reported for the Round-Robin load balancing mode. • **1:** Indicates that the current hostname is the primary one.
Name	This string reports the URL for the current hostname. This URL consists of the protocol, hostname, and the port.
Ordinal	This integer indicates the position in the ordered list for the current hostname. This position is primarily used by "Primary and Failover" load balancing mode to determine which hostname will take over when a hostname higher on the list is unreachable.

Name	Description
HttpsLoadBalancing	A string that indicates how HTTPS requests will be load balanced for the specified hostnames. Valid values for this response element are described below. **PF:** This value indicates that "Primary and Failover" mode will be used to load balance requests for this customer origin. In this mode, the specified hostnames form an ordered failover list. All requests will first be sent to the first hostname in the list. If that server is unavailable (i.e., TCP connection is refused or a timeout occurs), then the request will be sent to the next hostname. **RR:** This value indicates that "Round Robin" mode will be used to load balance requests for this customer origin. In this mode, our servers will send a balanced numbers of requests to each hostname. **Note:** The load balancing mode indicated for your customer origin configuration is independent from any load balancing configuration that may exist at the origin server.
Id	An integer that indicates the unique ID assigned to this customer origin configuration.
MediaTypeId	An integer that identifies the platform on which the customer origin configuration resides. This response element will always report "14," which is the value assigned to the ADN platform.

Errors

The response body for an unsuccessful request may contain an error element that provides additional information. For a list of common error messages, please refer to the **Status Codes and Error Messages** topic.

Sample Request and Response

A sample JSON request is provided below.

```
GET https://api.edgecast.com/v2/mcc/customers/0001/origins/adn HTTP/1.1

Authorization: TOK:12345678-1234-1234-1234-1234567890ab

Accept: application/json

Host: api.edgecast.com
```

A sample JSON response is provided below.

```
HTTP/1.1 200 OK
Cache-Control: private
Content-Length: 1100
Content-Type: application/json; charset=utf-8
Date: Mon, 10 Jan 2011 12:00:00 GMT


[{
            "FollowRedirects" : true,
            "NetworkConfiguration" : 1,
            "ValidationURL" :
      "http:\/\/socialmedia.mydomain.com\/images\/PerformanceTestObject_5k.gif",
            "DirectoryName" : "socialmedia",
            "HostHeader" : "socialmedia.mydomain.com",
            "HttpFullUrl" :
      "http:\/\/adn.0001.edgecastcdn.net\/800001\/socialmedia",
            "HttpHostnames" : [{
                        "IsPrimary" : 1,
                        "Name" : "http:\/\/socialmedia.mydomain.com:80",
                        "Ordinal" : 0
                }
            ],
            "HttpLoadBalancing" : "PF",
            "HttpsFullUrl" : "",
            "HttpsHostnames" : [],
            "HttpsLoadBalancing" : "",
            "Id" : 44764,
            "MediaTypeId" : 14
      }, {
            "FollowRedirects" : true,
            "NetworkConfiguration" : 1,
            "ValidationURL" : "http:\/\/banking.mydomain.com\/asset.txt",
            "DirectoryName" : "banking",
            "HostHeader" : "banking.mydomain.com",
            "HttpFullUrl" : "http:\/\/adn.0001.edgecastcdn.net\/800001\/banking",
            "HttpHostnames" : [{
                        "IsPrimary" : 1,
                        "Name" : "http:\/\/banking.mydomain.com:80",
                        "Ordinal" : 0
```

```
                }
        ],
        "HttpLoadBalancing" : "PF",
        "HttpsFullUrl" : "",
        "HttpsHostnames" : [],
        "HttpsLoadBalancing" : "",
        "Id" : 114197,
        "MediaTypeId" : 14
    }
]
```

Get All Customer Origins (HTTP Large)

Retrieves all customer origin configurations for the HTTP Large platform.

Request

A request to retrieve a list of customer origins (HTTP Large) is described below. When submitting this request, you will need to define the following term:

- **xxxx:** Replace this term with your CDN account number.

HTTP Method	Request URI
GET	https://api.edgecast.com/v2/mcc/customers/*xxxx*/origins/httplarge

Request Headers
This endpoint only takes advantage of the common request headers described in the **Request Headers** section of the **Request and Response Elements** topic.

Request Body
Request body parameters are not required by this endpoint.

Response

The response to the above request includes an HTTP status code, response headers, and a response body.

Status Code
A status code indicates whether the request was successfully performed. A list of common status codes is provided in the **Status Codes and Error Messages** topic.

Response Headers
The response for this endpoint only returns standard HTTP response headers including those described in the **Response Headers** section of the **Request and Response Elements** topic.

Response Body

The response body for a successful request contains the following response elements for each customer origin returned by this endpoint:

Name	Description
DirectoryName	A string that indicates the unique identification for your customer origin configuration. This name is appended to the end of the base CDN URL that points to your customer origin server (e.g., http://wpc.0001.edgecastcdn.net/800001/*CustomerOrigin*).
HostHeader	A string that identifies the IP address/hostname and port associated with a request.
HttpFullUrl	A string that indicates the CDN URL for HTTP requests to this customer origin server.
HttpHostnames	This response element contains the hostnames that will handle HTTP requests.
IsPrimary	This response element indicates whether the current hostname is the primary one. Valid values for this response element are described below. • **0:** Indicates that the current hostname is not the primary one. This value will always be reported for the Round-Robin load balancing mode. • **1:** Indicates that the current hostname is the primary one.
Name	This string reports the URL for the current hostname. This URL consists of the protocol, hostname, and the port.
Ordinal	This integer indicates the position in the ordered list for the current hostname. This position is primarily used by Primary Failover load balancing mode to determine which hostname will take over when a hostname higher on the list is unreachable.
HttpLoadBalancing	A string that indicates how HTTP requests will be load balanced for the specified hostnames. Valid values for this response element are described below. • **PF:** This value indicates that "Primary and Failover" mode will be used to load balance requests for this customer origin. In this mode, the specified hostnames form an ordered failover list. All requests will first be sent to the first hostname in the list. If that server is unavailable (i.e., TCP connection is refused or a timeout occurs), then the request will be sent to the next hostname. • **RR:** This value indicates that "Round Robin" mode will be used to load balance requests for this customer origin. In this mode, our servers will send a balanced numbers of requests to each hostname.

Name	Description
	Note: The load balancing mode indicated for your customer origin configuration is independent from any load balancing configuration that may exist at the origin server.
HttpsFullUrl	A string that indicates the CDN URL for HTTPS requests to this customer origin server.
HttpsHostnames	This response element contains the hostnames that will handle HTTPS requests.
IsPrimary	This response element indicates whether the current hostname is the primary one. Valid values for this response element are described below. • **0:** Indicates that the current hostname is not the primary one. This value will always be reported for the Round-Robin load balancing mode. • **1:** Indicates that the current hostname is the primary one.
Name	This string reports the URL for the current hostname. This URL consists of the protocol, hostname, and the port.
Ordinal	This integer indicates the position in the ordered list for the current hostname. This position is primarily used by Primary Failover load balancing mode to determine which hostname will take over when a hostname higher on the list is unreachable.
HttpsLoadBalancing	A string that indicates how HTTPS requests will be load balanced for the specified hostnames. Valid values for this response element are described below. • **PF:** This value indicates that "Primary and Failover" mode will be used to load balance requests for this customer origin. In this mode, the specified hostnames form an ordered failover list. All requests will first be sent to the first hostname in the list. If that server is unavailable (i.e., TCP connection is refused or a timeout occurs), then the request will be sent to the next hostname. • **RR:** This value indicates that "Round Robin" mode will be used to load balance requests for this customer origin. In this mode, our servers will send a balanced numbers of requests to each hostname. **Note:** The load balancing mode indicated for your customer origin configuration is independent from any load balancing configuration that may exist at the origin server.

Name	Description
Id	An integer that indicates the unique ID assigned to this customer origin configuration.
MediaTypeId	An integer that identifies the platform on which the customer origin configuration resides. This response element will always report "3," which is the value assigned to the HTTP Large platform.
ShieldPOPs	If the Origin Shield feature has been enabled on this customer origin configuration, then this response parameter will contain an object for each Origin Shield location that will act as an intermediate cache layer between our edge servers and your customer origin server.
Name	For each location returned by this endpoint, this response element will return a null value.
POPCode	This response element contains a three or four-letter abbreviation that indicates a POP location for which the Origin Shield feature has been activated. For more information, please refer to the **Appendix E: Origin Shield Locations and Settings** section.
Region	For each location returned by this endpoint, this response element will return a null value.

Name	Description
UseOriginShield	An integer that indicates whether Origin Shield has been activated on the customer origin. Valid values for this response element are described below. • **0:** Disabled. • **1:** Enabled. The customer origin configuration is protected by the Origin Shield feature.
networkConfiguration	An integer that indicates how hostnames associated with a customer origin configuration will be resolved to an IP address. Valid values are: • **1:** Default. Indicates that the IP preference for this customer origin will be system-defined. Currently, this configuration causes hostnames to be resolved to IPv4 only. • **2:** IPv6 Preferred over IPv4. Indicates that although hostnames for this customer origin can be resolved to either IP version, a preference will be given to IPv6. • **3:** IPv4 Preferred over IPv6. Indicates that although hostnames for this customer origin can be resolved to either IP version, a preference will be given to IPv4. • **4:** IPv4 Only. Indicates that hostnames for this customer origin can only be resolved to IPv4. • **5:** IPv6 Only. Indicates that hostnames for this customer origin can only be resolved to IPv6.

Errors

The response body for an unsuccessful request may contain an error element that provides additional information. For a list of common error messages, please refer to the **Status Codes and Error Messages** topic.

Sample Request and Response

A sample JSON request is provided below.

```
GET https://api.edgecast.com/v2/mcc/customers/0001/origins/httplarge HTTP/1.1

Authorization: TOK:12345678-1234-1234-1234-1234567890ab

Accept: application/json

Host: api.edgecast.com
```

A sample JSON response is provided below.

```
HTTP/1.1 200 OK
Cache-Control: private
Content-Length: 921
Content-Type: application/json; charset=utf-8
Date: Mon, 10 Jan 2011 12:00:00 GMT


[{
        "DirectoryName" : "MyCustomerOrigin",
        "HostHeader" : "images.mydomain.com:80",
        "HttpFullUrl" :
    "http:\/\/wpc.0001.edgecastcdn.net\/800001\/MyCustomerOrigin",
        "HttpHostnames" :
        [{
                    "IsPrimary" : 0,
                    "Name" : "http:\/\/images1.mydomain.com:80",
                    "Ordinal" : 0
            }, {
                    "IsPrimary" : 0,
                    "Name" : "http:\/\/images2.mydomain.com:80",
                    "Ordinal" : 1
            }
        ],
        "HttpLoadBalancing" : "RR",
        "HttpsFullUrl" : null,
        "HttpsHostnames" : [],
        "HttpsLoadBalancing" : null,
        "Id" : 1235,
        "MediaTypeId" : 3,
        "ShieldPOPs" : [],
        "UseOriginShield" : 0,
        "networkConfiguration" : 1
    }, {
        "DirectoryName" : "documents",
        "HostHeader" : "documents.mydomain.com:80",
        "HttpFullUrl" : "http:\/\/wpc.0001.edgecastcdn.net\/800001\/documents",
        "HttpHostnames" :
        [{
```

```
                "IsPrimary" : 0,
                "Name" : "http:\/\/documents1.mydomain.com:80",
                "Ordinal" : 0
        }, {
                "IsPrimary" : 0,
                "Name" : "http:\/\/documents2.mydomain.com:80",
                "Ordinal" : 1
        }
    ],
    "HttpLoadBalancing" : "RR",
    "HttpsFullUrl" : null,
    "HttpsHostnames" : [],
    "HttpsLoadBalancing" : null,
    "Id" : 1235,
    "MediaTypeId" : 3,
    "ShieldPOPs" : [],
    "UseOriginShield" : 0,
    "networkConfiguration" : 1
    }
]
```

Get All Customer Origins (HTTP Small)

Retrieves all customer origin configurations associated with the HTTP Small platform.

Request

A request to retrieve a list of customer origins is described below. When submitting this request, you will need to define the following term:

- **xxxx:** Replace this term with your CDN account number.

HTTP Method	Request URI
GET	https://api.edgecast.com/v2/mcc/customers/*xxxx*/origins/httpsmall

Request Headers
This endpoint only takes advantage of the common request headers described in the **Request Headers** section of the **Request and Response Elements** topic.

Request Body
Request body parameters are not required by this endpoint.

Response

The response to the above request includes an HTTP status code, response headers, and a response body.

Status Code

A status code indicates whether the request was successfully performed. A list of common status codes is provided in the **Status Codes and Error Messages** topic.

Response Headers

The response for this endpoint only returns standard HTTP response headers including those described in the **Response Headers** section of the **Request and Response Elements** topic.

Response Body

The response body for a successful request contains the following response elements for each customer origin returned by this endpoint:

Name	Description
DirectoryName	An alphanumeric string that identies your customer origin configuration. This name is appended to the end of the base CDN URL that points to your customer origin server (e.g., http://wac.0001.edgecastcdn.net/800001/*CustomerOrigin*).
HostHeader	A string that identifies the IP address/hostname and port associated with a request.
HttpFullUrl	A string that indicates the CDN URL for HTTP requests to this customer origin server.
HttpHostnames	This response element contains the hostnames that will handle HTTP requests.
IsPrimary	This response element indicates whether the current hostname is the primary one. Valid values for this response element are described below. • **0:** Indicates that the current hostname is not the primary one. This value will always be reported for the Round-Robin load balancing mode. • **1:** Indicates that the current hostname is the primary one.
Name	This string reports the URL for the current hostname. This URL consists of the protocol, hostname, and the port.
Ordinal	This integer indicates the position in the ordered list for the current hostname. This position is primarily used by Primary Failover load balancing mode to determine which hostname will take over when a hostname higher on the list is unreachable.

Name	Description
HttpLoadBalancing	A string that indicates how HTTP requests will be load balanced for the specified hostnames. Valid values for this response element are described below. • **PF:** This value indicates that "Primary and Failover" mode will be used to load balance requests for this customer origin. In this mode, the specified hostnames form an ordered failover list. All requests will first be sent to the first hostname in the list. If that server is unavailable (i.e., TCP connection is refused or a timeout occurs), then the request will be sent to the next hostname. • **RR:** This value indicates that "Round Robin" mode will be used to load balance requests for this customer origin. In this mode, our servers will send a balanced numbers of requests to each hostname. **Note:** The load balancing mode indicated for your customer origin configuration is independent from any load balancing configuration that may exist at the origin server.
HttpsFullUrl	A string that indicates the CDN URL for HTTPS requests to this customer origin server.
HttpsHostnames	This response element contains the hostnames that will handle HTTPS requests.
IsPrimary	This response element indicates whether the current hostname is the primary one. Valid values for this response element are described below. • **0:** Indicates that the current hostname is not the primary one. This value will always be reported for the Round-Robin load balancing mode. • **1:** Indicates that the current hostname is the primary one.
Name	This string reports the URL for the current hostname. This URL consists of the protocol, hostname, and the port.
Ordinal	This integer indicates the position in the ordered list for the current hostname. This position is primarily used by Primary Failover load balancing mode to determine which hostname will take over when a hostname higher on the list is unreachable.

Name	Description
HttpsLoadBalancing	A string that indicates how HTTPS requests will be load balanced for the specified hostnames. Valid values for this response element are described below. • **PF:** This value indicates that "Primary and Failover" mode will be used to load balance requests for this customer origin. In this mode, the specified hostnames form an ordered failover list. All requests will first be sent to the first hostname in the list. If that server is unavailable (i.e., TCP connection is refused or a timeout occurs), then the request will be sent to the next hostname. • **RR:** This value indicates that "Round Robin" mode will be used to load balance requests for this customer origin. In this mode, our servers will send a balanced numbers of requests to each hostname. **Note:** The load balancing mode indicated for your customer origin configuration is independent from any load balancing configuration that may exist at the origin server.
Id	An integer that indicates the unique ID assigned to this customer origin configuration.
MediaTypeId	An integer that identifies the platform on which the customer origin configuration resides. This response element will always report "8," which is the value assigned to the HTTP Small platform.
ShieldPOPs	If the Origin Shield feature has been enabled on this customer origin configuration, then this response parameter will contain an object for each Origin Shield location that will act as an intermediate cache layer between our edge servers and your customer origin server.
Name	For each Origin Shield location returned by this endpoint, this response element will return a null value.
POPCode	This response element contains a three or four-letter abbreviation that indicates a POP location for which the Origin Shield feature has been activated. For more information, please refer to the **Appendix E: Origin Shield Locations and Settings** section.
Region	For each Origin Shield location returned by this endpoint, this response element will return a null value.

Name	Description
UseOriginShield	An integer that indicates whether Origin Shield has been activated on the customer origin. Valid values for this response element are described below. • **0:** The customer origin configuration is not protected by Origin Shield. • **1:** The customer origin configuration is protected by Origin Shield.
networkConfiguration	An integer that indicates how hostnames associated with a customer origin configuration will be resolved to an IP address. Valid values are: • **1:** Default. Indicates that the IP preference for this customer origin will be system-defined. Currently, this configuration causes hostnames to be resolved to IPv4 only. • **2:** IPv6 Preferred over IPv4. Indicates that although hostnames for this customer origin can be resolved to either IP version, a preference will be given to IPv6. • **3:** IPv4 Preferred over IPv6. Indicates that although hostnames for this customer origin can be resolved to either IP version, a preference will be given to IPv4. • **4:** IPv4 Only. Indicates that hostnames for this customer origin can only be resolved to IPv4. • **5:** IPv6 Only. Indicates that hostnames for this customer origin can only be resolved to IPv6.

Errors

The response body for an unsuccessful request may contain an error element that provides additional information. For a list of common error messages, please refer to the **Status Codes and Error Messages** topic.

Sample Request and Response

A sample JSON request is provided below.

```
GET https://api.edgecast.com/v2/mcc/customers/0001/origins/httpsmall HTTP/1.1

Authorization: TOK:12345678-1234-1234-1234-1234567890ab

Accept: application/json

Host: api.edgecast.com
```

A sample JSON response is provided below.

```
HTTP/1.1 200 OK
Cache-Control: private
Content-Length: 921
Content-Type: application/json; charset=utf-8
Date: Mon, 10 Jan 2011 12:00:00 GMT


[{
        "DirectoryName" : "MyCustomerOrigin",
        "HostHeader" : "images.mydomain.com:80",
        "HttpFullUrl" :
      "http:\/\/wac.0001.edgecastcdn.net\/800001\/MyCustomerOrigin",
        "HttpHostnames" :
      [{
                    "IsPrimary" : 0,
                    "Name" : "http:\/\/images1.mydomain.com:80",
                    "Ordinal" : 0
            }, {
                    "IsPrimary" : 0,
                    "Name" : "http:\/\/images2.mydomain.com:80",
                    "Ordinal" : 1
            }
      ],
        "HttpLoadBalancing" : "RR",
        "HttpsFullUrl" : null,
        "HttpsHostnames" : [],
        "HttpsLoadBalancing" : null,
        "Id" : 1235,
        "MediaTypeId" : 8,
        "ShieldPOPs" : [],
        "UseOriginShield" : 0,
        "networkConfiguration" : 1
      }, {
        "DirectoryName" : "documents",
        "HostHeader" : "documents.mydomain.com:80",
        "HttpFullUrl" : "http:\/\/wac.0001.edgecastcdn.net\/800001\/documents",
        "HttpHostnames" :
            [{
```

```
                "IsPrimary" : 0,
                "Name" : "http:\/\/documents1.mydomain.com:80",
                "Ordinal" : 0
        }, {
                "IsPrimary" : 0,
                "Name" : "http:\/\/documents2.mydomain.com:80",
                "Ordinal" : 1
        }
    ],
       "HttpLoadBalancing" : "RR",
       "HttpsFullUrl" : null,
       "HttpsHostnames" : [],
       "HttpsLoadBalancing" : null,
       "Id" : 1235,
       "MediaTypeId" : 8,
       "ShieldPOPs" : [],
       "UseOriginShield" : 0,
       "networkConfiguration" : 1
    }
]
```

Get CDN IP Blocks

Retrieve a list of IPv4 and IPv6 blocks used by our CDN service.

Tip: Ensure that our CDN may communicate with your web servers by whitelisting these IP blocks on your firewall.

Request

A request to retrieve a listing of IP blocks is described below.

HTTP Method	Request URI
GET	https://api.edgecast.com/v2/mcc/customers/superblocks

Request Headers
This endpoint only takes advantage of the common request headers described in the **Request Headers** section of the **Request and Response Elements** topic.

Request Body
Request body parameters are not required by this endpoint.

Response

The response to the above request includes an HTTP status code, response headers, and a response body.

Status Code

A status code indicates whether the request was successfully performed. A list of common status codes is provided in the **Status Codes and Error Messages** topic.

Response Headers

The response for this endpoint only returns standard HTTP response headers including those described in the **Response Headers** section of the **Request and Response Elements** topic.

Response Body

The response body for a successful request contains the following response elements:

Name	Description
SuperBlockIPv4	An array containing string values that identify the IPv4 blocks used by our CDN service.
SuperBlockIPv6	An array containing string values that identify the IPv6 blocks used by our CDN service.

Errors

The response body for an unsuccessful request may contain an error element that provides additional information. For a list of common error messages, please refer to the **Status Codes and Error Messages** topic.

Sample Request and Response

A sample JSON request is provided below.

```
GET https://api.edgecast.com/v2/mcc/customers/superblocks HTTP/1.1

Authorization: TOK:12345678-1234-1234-1234-1234567890ab

Accept: application/json

Host: api.edgecast.com
```

A sample JSON response is provided below.

```
HTTP/1.1 200 OK

Cache-Control: private

Content-Length: 1255

Content-Type: application/json; charset=utf-8

Date: Mon, 10 Jan 2011 12:00:00 GMT
```

```
{
        "SuperBlockIPv4": ["5.104.64.0\/21", "46.22.64.0\/20", "61.49.62.128\/25",
        "61.221.181.64\/26", "68.232.32.0\/20", "72.21.80.0\/20",
        "88.194.45.128\/26", "93.184.208.0\/20", "101.226.203.0\/24",
        "108.161.240.0\/20", "110.232.176.0\/22", "117.18.232.0\/21",
        "117.103.183.0\/24", "120.132.137.0\/25", "121.156.59.224\/27",
        "121.189.46.0\/23", "152.195.0.0\/16", "180.240.184.0\/24", "192.16.0.0\/18",
        "192.30.0.0\/19", "192.229.128.0\/17", "194.255.210.64\/26",
        "198.7.16.0\/20", "203.74.4.64\/26", "213.64.234.0\/26", "213.65.58.0\/24",
        "68.140.206.0\/23", "68.130.0.0\/17", "152.190.247.0\/24",
        "65.222.137.0\/26", "65.222.145.128\/26", "65.198.79.64\/26",
        "65.199.146.192\/26", "65.200.151.160\/27", "65.200.157.192\/27",
        "68.130.128.0\/24", "68.130.136.0\/21", "65.200.46.128\/26",
        "213.175.80.0\/24"],

        "SuperBlockIPv6": ["2001:2011:c002:0000:0000:0000:0000:0000\/48",
        "2001:2040:c006:0000:0000:0000:0000:0000\/48",
        "2001:2060:bffb:0000:0000:0000:0000:0000\/48",
        "2001:b032:c101:0000:0000:0000:0000:0000\/48",
        "2405:8f00:edca:0000:0000:0000:0000:0000\/48",
        "2405:8f00:edcb:0000:0000:0000:0000:0000\/48",
        "2606:2800:0000:0000:0000:0000:0000:0000\/32",
        "2600:40ff:fffb:0000:0000:0000:0000:0000\/56",
        "2a02:16d8:0103:0000:0000:0000:0000:0000\/48"]

}
```

Get Customer Origin (ADN)

Retrieves the properties of a customer origin configuration.

Request

A request to retrieve customer origin information is described below. When submitting this request, you will need to define the following terms:

- **xxxx:** Replace this term with your CDN account number.

- **CustomerOriginID:** This term identifies the customer origin configuration whose information will be returned. It should be replaced by the ID associated with the desired customer origin configuration. The ID associated with each customer origin configuration is returned by the Get All Customer Origins (ADN) endpoint.

HTTP Method	Request URI
GET	https://api.edgecast.com/v2/mcc/customers/*xxxx*/origins/adn/*CustomerOriginID*

Request Headers
This endpoint only takes advantage of the common request headers described in the **Request Headers** section of the **Request and Response Elements** topic.

Request Body

Request body parameters are not required by this endpoint.

Response

The response to the above request includes an HTTP status code, response headers, and a response body.

Status Code

A status code indicates whether the request was successfully performed. A list of common status codes is provided in the **Status Codes and Error Messages** topic.

Response Headers

The response for this endpoint only returns standard HTTP response headers including those described in the **Response Headers** section of the **Request and Response Elements** topic.

Response Body

The response body for a successful request contains the following response elements:

Name	Description
FollowRedirects	A Boolean that indicates whether our edge servers will respect a URL redirect when validating the set of optimal ADN gateway servers for your customer origin configuration.
NetworkConfiguration	An integer that indicates how hostnames associated with a customer origin configuration will be resolved to an IP address. Valid values are: • **1:** Default. Indicates that the IP preference for this customer origin will be system-defined. Currently, this configuration causes hostnames to be resolved to IPv4 only. • **2:** IPv6 Preferred over IPv4. Indicates that although hostnames for this customer origin can be resolved to either IP version, a preference will be given to IPv6. • **3:** IPv4 Preferred over IPv6. Indicates that although hostnames for this customer origin can be resolved to either IP version, a preference will be given to IPv4. • **4:** IPv4 Only. Indicates that hostnames for this customer origin can only be resolved to IPv4. • **5:** IPv6 Only. Indicates that hostnames for this customer origin can only be resolved to IPv6.
ValidationURL	A string that indicates the URL to a sample asset. A set of optimal ADN gateway servers for your customer origin server is determined through the delivery of this sample asset.

Name	Description
DirectoryName	An alphanumeric string that identifies your customer origin configuration. This name is appended to the end of the base CDN URL that points to your customer origin server (e.g., http://adn.0001.edgecastcdn.net/800001/*CustomerOrigin*).
HostHeader	A string that identifies the IP address/hostname and port associated with a request.
HttpFullUrl	A string that indicates the CDN URL for HTTP requests to this customer origin server.
HttpHostnames	This response element contains the hostnames that will handle HTTP requests.
IsPrimary	This response element indicates whether the current hostname is the primary one for HTTP requests. Valid values for this response element are described below. • **0:** Indicates that the current hostname is not the primary one. This value will always be reported for the Round-Robin load balancing mode. • **1:** Indicates that the current hostname is the primary one.
Name	This string reports the URL for the current hostname. This URL consists of the protocol, hostname, and the port.
Ordinal	This integer indicates the position in the ordered list for the current hostname. This position is primarily used by "Primary and Failover" load balancing mode to determine which hostname will take over when a hostname higher on the list is unreachable.
HttpLoadBalancing	A string that indicates how HTTP requests will be load balanced for the specified hostnames. Valid values for this response element are described below. • **PF:** This value indicates that "Primary and Failover" mode will be used to load balance requests for this customer origin. In this mode, the specified hostnames form an ordered failover list. All requests will first be sent to the first hostname in the list. If that server is unavailable (i.e., TCP connection is refused or a timeout occurs), then the request will be sent to the next hostname. • **RR:** This value indicates that "Round Robin" mode will be used to load balance requests for this customer origin. In this mode, our servers will send a balanced numbers of requests to each hostname. **Note:** The load balancing mode indicated for your customer origin configuration is independent from any load balancing configuration that may exist at the origin server.

Name	Description
HttpsFullUrl	A string that indicates the CDN URL for HTTPS requests to this customer origin server.
HttpsHostnames	This response element contains the hostnames that will handle HTTPS requests.
IsPrimary	This response element indicates whether the current hostname is the primary one for HTTPS requests. Valid values for this response element are described below. • **0:** Indicates that the current hostname is not the primary one. This value will always be reported for the Round-Robin load balancing mode. • **1:** Indicates that the current hostname is the primary one.
Name	This string reports the URL for the current hostname. This URL consists of the protocol, hostname, and the port.
Ordinal	This integer indicates the position in the ordered list for the current hostname. This position is primarily used by "Primary and Failover" load balancing mode to determine which hostname will take over when a hostname higher on the list is unreachable.
HttpsLoadBalancing	A string that indicates how HTTPS requests will be load balanced for the specified hostnames. Valid values for this response element are described below. • **PF:** This value indicates that "Primary and Failover" mode will be used to load balance requests for this customer origin. In this mode, the specified hostnames form an ordered failover list. All requests will first be sent to the first hostname in the list. If that server is unavailable (i.e., TCP connection is refused or a timeout occurs), then the request will be sent to the next hostname. • **RR:** This value indicates that "Round Robin" mode will be used to load balance requests for this customer origin. In this mode, our servers will send a balanced numbers of requests to each hostname. **Note:** The load balancing mode indicated for your customer origin configuration is independent from any load balancing configuration that may exist at the origin server.
Id	An integer that indicates the unique ID assigned to this customer origin configuration.
MediaTypeId	An integer that identifies the platform on which the customer origin configuration resides. This response element will always report "14," which is the value assigned to the ADN platform.

Errors

The response body for an unsuccessful request may contain an error element that provides additional information. For a list of common error messages, please refer to the **Status Codes and Error Messages** topic.

Sample Request and Response

A sample JSON request is provided below.

```
GET https://api.edgecast.com/v2/mcc/customers/0001/origins/adn/123456 HTTP/1.1
Authorization: TOK:12345678-1234-1234-1234-1234567890ab
Accept: application/json
Host: api.edgecast.com
```

A sample JSON response is provided below.

```
HTTP/1.1 200 OK
Cache-Control: private
Content-Length: 507
Content-Type: application/json; charset=utf-8
Date: Mon, 10 Jan 2011 12:00:00 GMT


{
        "FollowRedirects" : true,
        "NetworkConfiguration" : 1,
        "ValidationURL" : "http:\/\/banking.mydomain.com\/asset.txt",
        "DirectoryName" : "banking",
        "HostHeader" : "banking.mydomain.com",
        "HttpFullUrl" : "http:\/\/adn.0001.edgecastcdn.net\/800001\/banking",
        "HttpHostnames" : [{
                    "IsPrimary" : 1,
                    "Name" : "http:\/\/banking.mydomain.com:80",
                    "Ordinal" : 0
            }
        ],
        "HttpLoadBalancing" : "PF",
        "HttpsFullUrl" : "",
        "HttpsHostnames" : [],
        "HttpsLoadBalancing" : "",
        "Id" : 123456,
        "MediaTypeId" : 14
```

```
}
```

Get Customer Origin (HTTP Large)

Retrieves the properties of a customer origin configuration.

Request

A request to retrieve customer origin information is described below. When submitting this request, you will need to define the following terms:

- **xxxx:** Replace this term with your CDN account number.

- **CustomerOriginID:** This term identifies the customer origin configuration whose information will be returned. It should be replaced by the ID associated with the desired customer origin configuration. The ID associated with each customer origin configuration is returned by the Get All Customer Origins (HTTP Large) endpoint.

HTTP Method	Request URI
GET	https://api.edgecast.com/v2/mcc/customers/*xxxx*/origins/httplarge/*CustomerOriginID*

Request Headers
This endpoint only takes advantage of the common request headers described in the **Request Headers** section of the **Request and Response Elements** topic.

Request Body
Request body parameters are not required by this endpoint.

Response

The response to the above request includes an HTTP status code, response headers, and a response body.

Status Code
A status code indicates whether the request was successfully performed. A list of common status codes is provided in the **Status Codes and Error Messages** topic.

Response Headers
The response for this endpoint only returns standard HTTP response headers including those described in the **Response Headers** section of the **Request and Response Elements** topic.

Response Body
The response body for a successful request contains the following response elements:

Name	Description
DirectoryName	A string that identifies your customer origin configuration. This name is appended to the end of the base CDN URL that points to your customer origin server (e.g., http://wpc.0001.edgecastcdn.net/800001/***CustomerOrigin***).
HostHeader	A string that identifies the IP address/hostname and port associated with a request.
HttpFullUrl	A string that indicates the CDN URL for HTTP requests to this customer origin server.
HttpHostnames	This response element contains the hostnames that will handle HTTP requests.
IsPrimary	This response element indicates whether the current hostname is the primary one. Valid values for this response element are described below. • **0:** Indicates that the current hostname is not the primary one. This value will always be reported for the Round-Robin load balancing mode. • **1:** Indicates that the current hostname is the primary one.
Name	This string reports the URL for the current hostname. This URL consists of the protocol, hostname, and the port.
Ordinal	This integer indicates the position in the ordered list for the current hostname. This position is primarily used by Primary Failover load balancing mode to determine which hostname will take over when a hostname higher on the list is unreachable.
HttpLoadBalancing	A string that indicates how HTTP requests will be load balanced for the specified hostnames. Valid values for this response element are described below. • **PF:** This value indicates that "Primary and Failover" mode will be used to load balance requests for this customer origin. In this mode, the specified hostnames form an ordered failover list. All requests will first be sent to the first hostname in the list. If that server is unavailable (i.e., TCP connection is refused or a timeout occurs), then the request will be sent to the next hostname. • **RR:** This value indicates that "Round Robin" mode will be used to load balance requests for this customer origin. In this mode, our servers will send a balanced numbers of requests to each hostname. **Note:** The load balancing mode indicated for your customer origin configuration is independent from any load balancing configuration that may exist at the origin server.

Name	Description
HttpsFullUrl	A string that indicates the CDN URL for HTTPS requests to this customer origin server.
HttpsHostnames	This response element contains the hostnames that will handle HTTPS requests.
IsPrimary	This response element indicates whether the current hostname is the primary one. Valid values for this response element are described below. • **0:** Indicates that the current hostname is not the primary one. This value will always be reported for the Round-Robin load balancing mode. • **1:** Indicates that the current hostname is the primary one.
Name	This string reports the URL for the current hostname. This URL consists of the protocol, hostname, and the port.
Ordinal	This integer indicates the position in the ordered list for the current hostname. This position is primarily used by Primary Failover load balancing mode to determine which hostname will take over when a hostname higher on the list is unreachable.
HttpsLoadBalancing	A string that indicates how HTTPS requests will be load balanced for the specified hostnames. Valid values for this response element are described below. • **PF:** This value indicates that "Primary and Failover" mode will be used to load balance requests for this customer origin. In this mode, the specified hostnames form an ordered failover list. All requests will first be sent to the first hostname in the list. If that server is unavailable (i.e., TCP connection is refused or a timeout occurs), then the request will be sent to the next hostname. • **RR:** This value indicates that "Round Robin" mode will be used to load balance requests for this customer origin. In this mode, our servers will send a balanced numbers of requests to each hostname. **Note:** The load balancing mode indicated for your customer origin configuration is independent from any load balancing configuration that may exist at the origin server.
Id	An integer that indicates the unique ID assigned to this customer origin configuration.
MediaTypeId	An integer that identifies the platform on which the customer origin configuration resides. This response element will always report "3," which is the value assigned to the HTTP Large platform.

Name	Description
ShieldPOPs	If the Origin Shield feature has been enabled on this customer origin configuration, then this response parameter will contain an object for each Origin Shield location that will act as an intermediate cache layer between our edge servers and your customer origin server.
Name	For each Origin Shield location returned by this endpoint, this response element will return a null value.
POPCode	This response element contains a three or four-letter abbreviation that indicates a POP location for which the Origin Shield feature has been activated. For more information, please refer to the **Appendix E: Origin Shield Locations and Settings** section.
Region	For each Origin Shield location returned by this endpoint, this response element will return a null value.
UseOriginShield	An integer that indicates whether Origin Shield has been activated on the customer origin. Valid values for this response element are described below. • **0:** The customer origin configuration is not protected by Origin Shield. • **1:** The customer origin configuration is protected by Origin Shield.
networkConfiguration	An integer that indicates how hostnames associated with a customer origin configuration will be resolved to an IP address. Valid values are: • **1:** Default. Indicates that the IP preference for this customer origin will be system-defined. Currently, this configuration causes hostnames to be resolved to IPv4 only. • **2:** IPv6 Preferred over IPv4. Indicates that although hostnames for this customer origin can be resolved to either IP version, a preference will be given to IPv6. • **3:** IPv4 Preferred over IPv6. Indicates that although hostnames for this customer origin can be resolved to either IP version, a preference will be given to IPv4. • **4:** IPv4 Only. Indicates that hostnames for this customer origin can only be resolved to IPv4. • **5:** IPv6 Only. Indicates that hostnames for this customer origin can only be resolved to IPv6.

Errors

The response body for an unsuccessful request may contain an error element that provides additional information. For a list of common error messages, please refer to the **Status Codes and Error Messages** topic.

Sample Request and Response

A sample JSON request is provided below.

```
GET https://api.edgecast.com/v2/mcc/customers/0001/origins/httplarge/12 HTTP/1.1

Authorization: TOK:12345678-1234-1234-1234-1234567890ab

Accept: application/json

Host: api.edgecast.com
```

A sample JSON response is provided below.

```
HTTP/1.1 200 OK

Cache-Control: private

Content-Length: 453

Content-Type: application/json; charset=utf-8

Date: Mon, 10 Jan 2011 12:00:00 GMT

{

        "DirectoryName" : "MyCustomerOrigin",

        "HostHeader" : "images.mydomain.com:80",

        "HttpFullUrl" :
        "http:\/\/wpc.0001.edgecastcdn.net\/800001\/MyCustomerOrigin",

        "HttpHostnames" :

        [{

                    "IsPrimary" : 0,

                    "Name" : "http:\/\/images1.mydomain.com:80",

                    "Ordinal" : 0

            }, {

                    "IsPrimary" : 0,

                    "Name" : "http:\/\/images2.mydomain.com:80",

                    "Ordinal" : 1

            }

        ],

        "HttpLoadBalancing" : "RR",

        "HttpsFullUrl" : null,

        "HttpsHostnames" : [],

        "HttpsLoadBalancing" : null,

        "Id" : 1211,

        "MediaTypeId" : 3,

        "ShieldPOPs" : [],

        "UseOriginShield" : 0,
```

```
        "networkConfiguration" : 1
}
```

Get Customer Origin (HTTP Small)

Retrieves the properties of a customer origin configuration.

Request

A request to retrieve customer origin information is described below. When submitting this request, you will need to define the following terms:

- **xxxx:** Replace this term with your CDN account number.

- **CustomerOriginID:** This term identifies the customer origin configuration whose information will be returned. It should be replaced by the ID associated with the desired customer origin configuration. The ID associated with each customer origin configuration is returned by the Get All Customer Origins (HTTP Small) endpoint.

HTTP Method	Request URI
GET	https://api.edgecast.com/v2/mcc/customers/*xxxx*/origins/httpsmall/*CustomerOriginID*

Request Headers

This endpoint only takes advantage of the common request headers described in the **Request Headers** section of the **Request and Response Elements** topic.

Request Body

Request body parameters are not required by this endpoint.

Response

The response to the above request includes an HTTP status code, response headers, and a response body.

Status Code

A status code indicates whether the request was successfully performed. A list of common status codes is provided in the **Status Codes and Error Messages** topic.

Response Headers

The response for this endpoint only returns standard HTTP response headers including those described in the **Response Headers** section of the **Request and Response Elements** topic.

Response Body

The response body for a successful request contains the following response elements:

Name	Description
DirectoryName	An alphanumeric string that identifies your customer origin configuration. This name is appended to the end of the base CDN URL that points to your customer origin server (e.g., http://wac.0001.edgecastcdn.net/800001/*CustomerOrigin*).
HostHeader	A string that identifies the IP address/hostname and port associated with a request.
HttpFullUrl	A string that indicates the CDN URL for HTTP requests to this customer origin server.
HttpHostnames	This response element contains the hostnames that will handle HTTP requests.
IsPrimary	This response element indicates whether the current hostname is the primary one. Valid values for this response element are described below. • **0:** Indicates that the current hostname is not the primary one. This value will always be reported for the Round-Robin load balancing mode. • **1:** Indicates that the current hostname is the primary one.
Name	This string reports the URL for the current hostname. This URL consists of the protocol, hostname, and the port.
Ordinal	This integer indicates the position in the ordered list for the current hostname. This position is primarily used by Primary Failover load balancing mode to determine which hostname will take over when a hostname higher on the list is unreachable.
HttpLoadBalancing	A string that indicates how HTTP requests will be load balanced for the specified hostnames. Valid values for this response element are described below. • **PF:** This value indicates that "Primary and Failover" mode will be used to load balance requests for this customer origin. In this mode, the specified hostnames form an ordered failover list. All requests will first be sent to the first hostname in the list. If that server is unavailable (i.e., TCP connection is refused or a timeout occurs), then the request will be sent to the next hostname. • **RR:** This value indicates that "Round Robin" mode will be used to load balance requests for this customer origin. In this mode, our servers will send a balanced numbers of requests to each hostname. **Note:** The load balancing mode indicated for your customer origin configuration is independent from any load balancing configuration that may exist at the origin server.

Name	Description
HttpsFullUrl	A string that indicates the CDN URL for HTTPS requests to this customer origin server.
HttpsHostnames	This response element contains the hostnames that will handle HTTPS requests.
IsPrimary	This response element indicates whether the current hostname is the primary one. Valid values for this response element are described below. • **0:** Indicates that the current hostname is not the primary one. This value will always be reported for the Round-Robin load balancing mode. • **1:** Indicates that the current hostname is the primary one.
Name	This string reports the URL for the current hostname. This URL consists of the protocol, hostname, and the port.
Ordinal	This integer indicates the position in the ordered list for the current hostname. This position is primarily used by Primary Failover load balancing mode to determine which hostname will take over when a hostname higher on the list is unreachable.
HttpsLoadBalancing	A string that indicates how HTTPS requests will be load balanced for the specified hostnames. Valid values for this response element are described below. • **PF:** This value indicates that "Primary and Failover" mode will be used to load balance requests for this customer origin. In this mode, the specified hostnames form an ordered failover list. All requests will first be sent to the first hostname in the list. If that server is unavailable (i.e., TCP connection is refused or a timeout occurs), then the request will be sent to the next hostname. • **RR:** This value indicates that "Round Robin" mode will be used to load balance requests for this customer origin. In this mode, our servers will send a balanced numbers of requests to each hostname. **Note:** The load balancing mode indicated for your customer origin configuration is independent from any load balancing configuration that may exist at the origin server.
Id	An integer that indicates the unique ID assigned to this customer origin configuration.
MediaTypeId	An integer that identifies the platform on which the customer origin configuration resides. This response element will always report "8," which is the value assigned to the HTTP Small platform.

Name	Description
ShieldPOPs	If the Origin Shield feature has been enabled on this customer origin configuration, then this response parameter will contain an object for each Origin Shield location that will act as an intermediate cache layer between our edge servers and your customer origin server.
Name	For each Origin Shield location returned by this endpoint, this response element will return a null value.
POPCode	This response element contains a three or four-letter abbreviation that indicates a POP location for which the Origin Shield feature has been activated. For more information, please refer to the **Appendix E: Origin Shield Locations and Settings** section.
Region	For each Origin Shield location returned by this endpoint, this response element will return a null value.
UseOriginShield	An integer that indicates whether Origin Shield has been activated on the customer origin. Valid values for this response element are described below. • **0:** This customer origin configuration is not protected by Origin Shield. • **1:** This customer origin configuration is protected by Origin Shield.
networkConfiguration	An integer that indicates how hostnames associated with a customer origin configuration will be resolved to an IP address. Valid values are: • **1:** Default. Indicates that the IP preference for this customer origin will be system-defined. Currently, this configuration causes hostnames to be resolved to IPv4 only. • **2:** IPv6 Preferred over IPv4. Indicates that although hostnames for this customer origin can be resolved to either IP version, a preference will be given to IPv6. • **3:** IPv4 Preferred over IPv6. Indicates that although hostnames for this customer origin can be resolved to either IP version, a preference will be given to IPv4. • **4:** IPv4 Only. Indicates that hostnames for this customer origin can only be resolved to IPv4. • **5:** IPv6 Only. Indicates that hostnames for this customer origin can only be resolved to IPv6.

Errors

The response body for an unsuccessful request may contain an error element that provides additional information. For a list of common error messages, please refer to the **Status Codes and Error Messages** topic.

Sample Request and Response

A sample JSON request is provided below.

```
GET https://api.edgecast.com/v2/mcc/customers/0001/origins/httpsmall/12 HTTP/1.1
Authorization: TOK:12345678-1234-1234-1234-1234567890ab
Accept: application/json
Host: api.edgecast.com
```

A sample JSON response is provided below.

```
HTTP/1.1 200 OK
Cache-Control: private
Content-Length: 453
Content-Type: application/json; charset=utf-8
Date: Mon, 10 Jan 2011 12:00:00 GMT

{
        "DirectoryName" : "MyCustomerOrigin",
        "HostHeader" : "images.mydomain.com:80",
        "HttpFullUrl" :
        "http:\/\/wac.0001.edgecastcdn.net\/800001\/MyCustomerOrigin",
        "HttpHostnames" :
        [{
                    "IsPrimary" : 0,
                    "Name" : "http:\/\/images1.mydomain.com:80",
                    "Ordinal" : 0
            }, {
                    "IsPrimary" : 0,
                    "Name" : "http:\/\/images2.mydomain.com:80",
                    "Ordinal" : 1
            }
        ],
        "HttpLoadBalancing" : "RR",
        "HttpsFullUrl" : null,
        "HttpsHostnames" : [],
        "HttpsLoadBalancing" : null,
        "Id" : 1211,
        "MediaTypeId" : 8,
        "ShieldPOPs" : [],
        "UseOriginShield" : 0,
```

```
        "networkConfiguration" : 1
}
```

Get Customer Origin Status

Retrieves the propagation status for a customer origin configuration.

Note: This endpoint may not be used to retrieve propagation status for customer origin configurations that were last updated more than 7 days ago.

Request

A request to retrieve status information is described below. When submitting this request, you will need to define the following terms:

- **xxxx:** Replace this term with the desired customer account number.

- **CustomerOriginID:** Replace this term with the system-defined ID for the desired customer origin configuration.

  Use a platform-specific **Get All Customer Origins** endpoint to retrieve the system-defined ID for the desired customer origin.

  Sample request for the HTTP Large platform:

  > https://api.edgecast.com/v2/mcc/customers/0001/origins/httplarge

  Note: Please refer to the REST API Help Center for more detailed information on this endpoint.

HTTP Method	Request URI
GET	https://api.edgecast.com/v2/mcc/customers/*xxxx*/origins/*CustomerOriginID*/status

Request Headers
This endpoint only takes advantage of the common request headers described in the **Request Headers** section of the **Request and Response Elements** topic.

Request Body
Request body parameters are not required by this endpoint.

Response

The response to the above request includes an HTTP status code, response headers, and a response body.

Status Code

A status code indicates whether the request was successfully performed. A list of common status codes is provided in the **Status Codes and Error Messages** topic.

Response Headers

The response for this endpoint only returns standard HTTP response headers including those described in the **Response Headers** section of the **Request and Response Elements** topic.

Response Body

The response body for a successful request varies according to the following factors:

- **New / Update:** The following response will be provided immediately after a customer origin configuration is created or updated:

  ```
  {"Status":"New","Percent_propagated":0}
  ```

- **Existing Configurations:** If the customer origin configuration is older than 7 days, then this endpoint will return a 400 Bad Request with the following response body:

  ```
  {"Message":"Action Queue Id missing"}
  ```

- **Deployment:** Once the deployment of the new/updated customer origin configuration begins, the response body will contain the following response elements:

Name	Data Type	Description
Status	String	Indicates the customer origin's current propagation status. Valid values are: • **New:** Indicates that the configuration has been created, but the propagation process has not started. **Note:** A new configuration may stay in this state for a few minutes while it undergoes a validation/verification process. • **propagating:** Indicates that the configuration is in the process of being propagated. • **propagated:** Indicates that the configuration has been propagated across the entire network.
Percent_propagated	Decimal	Indicates the average configuration propagation percentage across all POPs.

Name	Data Type	Description
Pops	Array	Contains a list of POPs and their current configuration propagation percentage.
name	String	Identifies a POP by region and name. **Syntax (Single POP per Location):** *Region* : *POPName* **Syntax (Multiple POPs per Location):** If a location contains multiple POPs, then a three-letter abbreviation will identify each POP: *Region* : *POPName* (*POP*)
percentage_propagated	Decimal	Indicates the percentage of servers within a POP to which the configuration has been propagated.

Errors

The response body for an unsuccessful request may contain an error element that provides additional information. For a list of common error messages, please refer to the **Status Codes and Error Messages** topic.

Sample Request and Response

A sample JSON request is provided below.

```
GET https://api.edgecast.com/v2/mcc/customers/0001/origins/123456/status HTTP/1.1
Authorization: TOK:12345678-1234-1234-1234-1234567890ab
Accept: application/json
Host: api.edgecast.com
```

A sample JSON response is provided below.

```
HTTP/1.1 200 OK
Cache-Control: private
Content-Type: application/json; charset=utf-8
Date: Thu, 14 Apr 2016 12:00:00 GMT
Content-Length: 7718

{
        "Status": "propagating",
        "Percent_propagated": 8.759656026818249,
        "Pops": [{
                    "name": "South America : Valparaiso, Chile",
```

```
                "percentage_propagated": 15.789473684210526
        }, {

                ...
                "name": "South America : Lima, Peru",
                "percentage_propagated": 14.285714285714285
        }, {
                "name": "North America : San Jose",
                "percentage_propagated": 14.000000000000002
        }, {
                "name": "Europe : London (LHR2)",
                "percentage_propagated": 15.894039735099339
        }, {
                "name": "Australia : Auckland",
                "percentage_propagated": 23.076923076923077
        }
    ]
}
```

Get Origin Shield POPs (HTTP Large)

This endpoint returns a list of the available Origin Shield locations for the HTTP Large platform. This list consists of the name, POP code, and region for each POP that can provide Origin Shield protection to a customer origin server. These abbreviations can then be used to set or to interpret Origin Shield settings for a customer origin.

Note: This endpoint does not return data for bypass region settings. For information on bypass region settings, please refer to **Appendix E: Origin Shield Locations and Settings**.

Request

A request to find out the available Origin Shield locations (HTTP Large) is described below. When submitting this request, you will need to define the following term:

- **xxxx:** Replace this term with your CDN account number.

HTTP Method	Request URI
GET	https://api.edgecast.com/v2/mcc/customers/*xxxx*/origins/httplarge/shieldpops

Request Headers

This endpoint only takes advantage of the common request headers described in the **Request Headers** section of the **Request and Response Elements** topic.

Request Body

Request body parameters are not required by this endpoint.

Response

The response to the above request includes an HTTP status code, response headers, and a response body.

Status Code

A status code indicates whether the request was successfully performed. A list of common status codes is provided in the **Status Codes and Error Messages** topic.

Response Headers

The response for this endpoint only returns standard HTTP response headers including those described in the **Response Headers** section of the **Request and Response Elements** topic.

Response Body

The response body for a successful request contains the following response elements for each Origin Shield POP returned by this endpoint:

Name	Description
Name	A string that indicates the name of the POP location where Origin Shield servers reside.
POPCode	A string that indicates the three-letter abbreviation corresponding to the POP location identified by the Name request parameter.
Region	A string that indicates the region corresponding to the POP location identified by the Name request parameter.
	Tip: The region associated with a POP is relevant when configuring an origin server to bypass Origin Shield protection on certain regions.

Errors

The response body for an unsuccessful request may contain an error element that provides additional information. For a list of common error messages, please refer to the **Status Codes and Error Messages** topic.

Sample Request and Response

A sample JSON request is provided below.

```
GET https://api.edgecast.com/v2/mcc/customers/0001/origins/httplarge/shieldpops
HTTP/1.1

Authorization: TOK:12345678-1234-1234-1234-1234567890ab

Accept: application/json

Host: api.edgecast.com
```

A sample JSON response is provided below.

```
HTTP/1.1 200 OK
Cache-Control: private
Content-Length: 1428
Content-Type: application/json; charset=utf-8
Date: Mon, 10 Jan 2011 12:00:00 GMT


[{
            "Name" : "Ashburn",
            "POPCode" : "DCA",
            "Region" : "US East"
    }, {
            ...
    }, {
            "Name" : "San Jose",
            "POPCode" : "SJC",
            "Region" : "US West"
    }, {
            "Name" : "Osaka",
            "POPCode" : "KIX",
            "Region" : "Asia"
    }
]
```

Get Origin Shield POPs (HTTP Small)

This endpoint returns a list of the available Origin Shield locations for the HTTP Small platform. This list consists of the name, POP code, and region for each POP that can provide Origin Shield protection to a customer origin server. These abbreviations can then be used to set or to interpret Origin Shield settings for a customer origin.

Note: This endpoint does not return data for bypass region settings. For information on bypass region settings, please refer to **Appendix E: Origin Shield Locations and Settings**.

Request

A request to find out the available Origin Shield locations (HTTP Small) is described below. When submitting this request, you will need to define the following term:

- **xxxx:** Replace this term with your CDN account number.

HTTP Method	Request URI
GET	https://api.edgecast.com/v2/mcc/customers/*xxxx*/origins/httpsmall/shieldpops

Request Headers

This endpoint only takes advantage of the common request headers described in the **Request Headers** section of the **Request and Response Elements** topic.

Request Body

Request body parameters are not required by this endpoint.

Response

The response to the above request includes an HTTP status code, response headers, and a response body.

Status Code

A status code indicates whether the request was successfully performed. A list of common status codes is provided in the **Status Codes and Error Messages** topic.

Response Headers

The response for this endpoint only returns standard HTTP response headers including those described in the **Response Headers** section of the **Request and Response Elements** topic.

Response Body

The response body for a successful request contains the following response elements for each Origin Shield POP returned by this endpoint:

Name	Description
Name	A string that indicates the name of the POP location where Origin Shield servers reside.
POPCode	A string that indicates the three-letter abbreviation corresponding to the POP location identified by the Name request parameter.
Region	A string that indicates the region corresponding to the POP location identified by the Name request parameter.
	Tip: The region associated with a POP is relevant when configuring an origin server to bypass Origin Shield protection on certain regions.

Errors

The response body for an unsuccessful request may contain an error element that provides additional information. For a list of common error messages, please refer to the **Status Codes and Error Messages** topic.

Sample Request and Response

A sample JSON request is provided below.

```
GET https://api.edgecast.com/v2/mcc/customers/0001/origins/httpsmall/shieldpops
HTTP/1.1

Authorization: TOK:12345678-1234-1234-1234-1234567890ab

Accept: application/json

Host: api.edgecast.com
```

A sample JSON response is provided below.

```
HTTP/1.1 200 OK

Cache-Control: private

Content-Length: 1428

Content-Type: application/json; charset=utf-8

Date: Mon, 10 Jan 2011 12:00:00 GMT


[{

        "Name" : "Ashburn",

        "POPCode" : "DCA",

        "Region" : "US East"

    }, {

        ...

    }, {

        "Name" : "San Jose",
```

```
            "POPCode" : "SJC",

            "Region" : "US West"

    }, {

            "Name" : "Osaka",

            "POPCode" : "KIX",

            "Region" : "Asia"

    }

 ]
```

Reselect ADN Gateways

Reselects the set of ADN gateways that will be associated with a customer origin.

Request

A request to reselect ADN gateways is described below. When submitting this request, you will need to define the following terms:

- **xxxx:** Replace this term with your CDN account number.

- **CustomerOriginID:** This term determines the customer origin that will be updated. It should be replaced by the ID of the customer origin that you would like to update.

HTTP Method	Request URI
PUT	https://api.edgecast.com/v2/mcc/customers/*xxxx*/origins/adn/*CustomerOriginID*/reselect

Request Headers
This endpoint only takes advantage of the common request headers described in the **Request Headers** section of the **Request and Response Elements** topic.

Request Body
Request body parameters are not required by this endpoint.

Response

The response to the above request includes an HTTP status code, response headers, and a response body.

Status Code
A status code indicates whether the request was successfully performed. A list of common status codes is provided in the **Status Codes and Error Messages** topic.

Response Headers

The response for this endpoint only returns standard HTTP response headers including those described in the **Response Headers** section of the **Request and Response Elements** topic.

Response Body

The response body for a successful request does not contain a response element.

Errors

The response body for an unsuccessful request may contain an error element that provides additional information. For a list of common error messages, please refer to the **Status Codes and Error Messages** topic.

Sample Request and Response

The request format is identical for both JSON and XML. A sample request is provided below.

```
PUT https://api.edgecast.com/v2/mcc/customers/0001/origins/adn/123456/reselect
HTTP/1.1

Authorization: TOK:12345678-1234-1234-1234-1234567890ab

Host: api.edgecast.com
```

The response is identical for both JSON and XML. A sample response is provided below.

```
HTTP/1.1 200 OK

Cache-Control: private

Date: Mon, 10 Jan 2011 12:00:00 GMT
```

Update Customer Origin (ADN)

Sets the properties for a customer origin on the ADN platform.

Important: Updating a customer origin will overwrite the entire customer origin configuration. This will occur regardless of whether a request parameter has been excluded from the request.

Note: This endpoint cannot be used to update the directory assigned to a customer origin configuration that has been associated with an edge CNAME.

Request

A request to update the properties of a customer origin configuration is described below. When submitting this request, you will need to define the following terms:

- **xxxx:** Replace this term with your CDN account number.

- **CustomerOriginID:** This term determines the customer origin that will be updated. It should be replaced by the ID of the customer origin that you would like to update.

HTTP Method	Request URI
PUT	https://api.edgecast.com/v2/mcc/customers/*xxxx*/origins/adn/*CustomerOriginID*

Request Headers

This endpoint only takes advantage of the common request headers described in the **Request Headers** section of the **Request and Response Elements** topic.

Request Body

The request parameters for this endpoint are described below.

Note: The indented parameters indicate that they are a property of the request parameter directly above it. When submitting a request, you will need to use the proper syntax to indicate this relationship. Please refer to the parent request parameter for more information.

Note: Hostnames are associated with a customer origin configuration according to the request type (i.e., HTTP or HTTPS) that they will handle. Although you may choose to define a set of hostnames for each request type, you are only required to specify a single hostname and load balancing method for either request type. If you choose to define one or more hostnames, then you will also need to define the load balancing method for that request type.

Name	Description
DirectoryName	Required. An alphanumeric string that identifies your customer origin configuration. It is appended to the end of the base CDN URL that points to your customer origin server (e.g., http://adn.0001.edgecastcdn.net/800001/***CustomerOrigin***).
	Important: This setting is read-only for a customer origin configuration that has been associated with at least one edge CNAME configuration. For this type of scenario, make sure that this response element is set to the directory name currently assigned to the customer origin configuration.
FollowRedirects	A Boolean that determines whether our edge servers will respect a URL redirect when validating the set of optimal ADN gateway servers for your customer origin configuration. **Default value:** False
HostHeader	Required. A string that identifies the IP address/hostname and port associated with a request. A host header is especially useful when there are multiple virtual domains hosted on a single physical server or load-balanced set of servers.
	Note: A protocol should not be specified when setting this parameter.

Name	Description
HttpHostnames	Required. This response element is only used to indicate that you plan on specifying one or more hostnames for handling HTTP requests. Keep in mind the following formatting information: • **XML:** Each hostname must be contained within a `<Hostname>` tag. • **JSON:** The desired set of hostnames must be contained within a set of square brackets. Additionally, each hostname (i.e., Name request parameter) must be contained with a set of curly braces.
Name	Required. A string that determines the hostname/IP address of the origin server that will be associated with the customer origin configuration being created. Use one of the following formats to identify an origin server: • *protocol*://*hostname*:*port* (e.g., http://www.mydomain.com:80) • *protocol*://*IPv4Address*:*port* (e.g., http://10.10.10.255:80) • *protocol*://[*IPv6Address*]:*port* (e.g., http://[1:2:3:4:5:6:7:8]:80)
HttpLoadBalancing	Required. A string that determines how HTTP requests will be load balanced for the specified hostnames. Our servers will use DNS to resolve the specified hostnames into an ordered list of IP addresses. If you have only specified a single web server for this origin server configuration, then either of the following load balancing methods will serve requests through that web server. Valid values for this request parameter are described below. • **PF:** This value indicates that "Primary and Failover" mode will be used to load balance requests for this customer origin. In this mode, the specified hostnames form an ordered failover list. All requests will first be sent to the first hostname in the list. If that server is unavailable (i.e., TCP connection is refused or a timeout occurs), then the request will be sent to the next hostname. • **RR:** This value indicates that "Round Robin" mode will be used to load balance requests for this customer origin. In this mode, our servers will send a balanced numbers of requests to each hostname. **Note:** The load balancing mode specified for your customer origin configuration is independent from any load balancing configuration that may exist at the origin server.

Name	Description
HttpsHostnames	Required. This response element is only used to indicate that you plan on specifying one or more hostnames for handling HTTPS requests. Keep in mind the following formatting information: • **XML:** Each hostname must be contained within a \<Hostname> tag. • **JSON:** The desired set of hostnames must be contained within a set of square brackets. Additionally, each hostname (i.e., Name request parameter) must be contained with a set of curly braces. **Important:** This request parameter is only available for customers that have purchased an SSL certificate or the HTTPS feature.
Name	Required. A string that determines the hostname/IP address of the origin server that will be associated with the customer origin configuration being created. Use one of the following formats to identify an origin server: • *protocol*://*hostname*:*port* (e.g., http://www.mydomain.com:80) • *protocol*://*IPv4Address*:*port* (e.g., http://10.10.10.255:80) • *protocol*://[*IPv6Address*]:*port* (e.g., http://[1:2:3:4:5:6:7:8]:80) **Note:** If you specify HTTP hostnames to serve HTTPS requests, then you will sacrifice end-to-end data encryption.
HttpsLoadBalancing	Required. A string that determines how HTTPS requests will be load balanced for the specified hostnames. Our servers will use DNS to resolve the specified hostnames into an ordered list of IP addresses. If you have only specified a single web server for this origin server configuration, then either of the following load balancing methods will serve requests through that web server. Valid values for this request parameter are described below. • **PF:** This value indicates that "Primary and Failover" mode will be used to load balance requests for this customer origin. In this mode, the specified hostnames form an ordered failover list. All requests will first be sent to the first hostname in the list. If that server is unavailable (i.e., TCP connection is refused or a timeout occurs), then the request will be sent to the next hostname. • **RR:** This value indicates that "Round Robin" mode will be used to load balance requests for this customer origin. In this

Name	Description
	mode, our servers will send a balanced numbers of requests to each hostname.
	Note: The load balancing mode specified for your customer origin configuration is independent from any load balancing configuration that may exist at the origin server.
NetworkConfiguration	An integer that determines how hostnames associated with this customer origin configuration will be resolved to an IP address. Valid values are: • **1:** Default. Indicates that the IP preference for this customer origin will be system-defined. Currently, this configuration causes hostnames to be resolved to IPv4 only. • **2:** IPv6 Preferred over IPv4. Indicates that although hostnames for this customer origin can be resolved to either IP version, a preference will be given to IPv6. • **3:** IPv4 Preferred over IPv6. Indicates that although hostnames for this customer origin can be resolved to either IP version, a preference will be given to IPv4. • **4:** IPv4 Only. Indicates that hostnames for this customer origin can only be resolved to IPv4. • **5:** IPv6 Only. Indicates that hostnames for this customer origin can only be resolved to IPv6.
ValidationURL	Required. A string that defines the URL to a sample asset stored on your servers. A set of optimal ADN gateway servers for your customer origin server is determined through the delivery of this sample asset.
	Note: Make sure that the domain in the specified URL matches the one defined in the HostHeader request parameter.

Response

The response to the above request includes an HTTP status code, response headers, and a response body.

Status Code

A status code indicates whether the request was successfully performed. A list of common status codes is provided in the **Status Codes and Error Messages** topic.

Response Headers

The response for this endpoint only returns standard HTTP response headers including those described in the **Response Headers** section of the **Request and Response Elements** topic.

Response Body

The response body for a successful request does not contain a response element.

Errors

The response body for an unsuccessful request may contain an error element that provides additional information. For a list of common error messages, please refer to the **Status Codes and Error Messages** topic.

Sample Request and Response

A sample JSON request is provided below.

```
PUT https://api.edgecast.com/v2/mcc/customers/0001/origins/adn/123456 HTTP/1.1

Authorization: TOK:12345678-1234-1234-1234-1234567890ab

Accept: application/json

Content-Type: application/json

Host: api.edgecast.com

Content-Length: 417


{

        "DirectoryName" : "MyWebServer",

        "HostHeader" : "webapp.mydomain.com:80",

        "HttpHostnames" :

        [{

                    "Name" : "http:\/\/webapp1.mydomain.com:80"

              }, {

                    "Name" : "http:\/\/webapp2.mydomain.com:80"

              }

        ],

        "HttpLoadBalancing" : "RR",

        "HttpsHostnames" :

        [{

                    "Name" : "https:\/\/webapp.mydomain.com:443"

              }

        ],

        "HttpsLoadBalancing" : "PF",

        "ValidationURL":"http:\/\/webapp.mydomain.com:443\/images\/PerformanceTestObj
        ect_5k.gif"

}
```

A sample JSON response is provided below.

```
HTTP/1.1 200 OK
Cache-Control: private
Content-Length: 0
Content-Type: application/json; charset=utf-8
Date: Mon, 10 Jan 2011 12:00:00 GMT
```

Update Customer Origin (HTTP Large)

Sets the properties for a customer origin on the HTTP Large platform.

Important: Updating a customer origin will overwrite the entire customer origin configuration. This will occur regardless of whether a request parameter has been excluded from the request.

Note: This endpoint cannot be used to update the directory assigned to a customer origin configuration that has been associated with an edge CNAME.

Request

A request to update a customer origin configuration is described below. When submitting this request, you will need to define the following terms:

- **xxxx:** Replace this term with your CDN account number.

- **CustomerOriginID:** This term determines the customer origin that will be updated. It should be replaced by the ID of the customer origin that you would like to update.

HTTP Method	Request URI
PUT	https://api.edgecast.com/v2/mcc/customers/*xxxx*/origins/httplarge/*CustomerOriginID*

Request Headers

This endpoint only takes advantage of the common request headers described in the **Request Headers** section of the **Request and Response Elements** topic.

Request Body

The request parameters for this endpoint are described below.

Note: Indented parameters indicate that they are a property of the request parameter directly above it. When submitting a request, you will need to use the proper syntax to indicate this relationship. Please refer to the parent request parameter for more information.

Note: Hostnames are associated with a customer origin configuration according to the request type (i.e., HTTP or HTTPS) that they will handle. Although you may choose to define a set of hostnames for each request type, you are only required to specify a single hostname and load

balancing method for either request type. If you choose to define one or more hostnames, then you will also need to define the load balancing method for that request type.

Name	Description
DirectoryName	Required. An alphanumeric string that identifies your customer origin configuration. It is appended to the end of the base CDN URL that points to your customer origin server (e.g., http://wpc.0001.edgecastcdn.net/800001/*CustomerOrigin*).
	Important: This setting is read-only for a customer origin configuration that has been associated with at least one edge CNAME configuration. For this type of scenario, make sure that this response element is set to the directory name currently assigned to the customer origin configuration.
HostHeader	Required. A string that identifies the IP address/hostname and port associated with a request. A host header is especially useful when there are multiple virtual domains hosted on a single physical server or load-balanced set of servers.
	Note: A protocol should not be specified when setting this parameter.
HttpHostnames	Required. This response element is only used to indicate that you plan on specifying one or more hostnames for handling HTTP requests. Keep in mind the following formatting information: • **XML:** Each hostname must be contained within a <Hostname> tag. • **JSON:** The desired set of hostnames must be contained within a set of square brackets. Additionally, each hostname (i.e., Name request parameter) must be contained with a set of curly braces.
Name	Required. A string that determines the hostname/IP address of the origin server that will be associated with the customer origin configuration being updated. Use one of the following formats to identify an origin server: • *protocol*://*hostname*:*port* (e.g., http://www.mydomain.com:80) • *protocol*://*IPv4Address*:*port* (e.g., http://10.10.10.255:80) • *protocol*://[*IPv6Address*]:*port* (e.g., http://[1:2:3:4:5:6:7:8]:80)
HttpLoadBalancing	Required. A string that determines how HTTP requests will be load balanced for the specified hostnames. Our servers will use DNS to resolve the specified hostnames into an ordered list of IP addresses.

Name	Description
	If you have only specified a single web server for this origin server configuration, then either of the following load balancing methods will serve requests through that web server.
	Valid values for this request parameter are described below.
	PF: This value indicates that "Primary and Failover" mode will be used to load balance requests for this customer origin. In this mode, the specified hostnames form an ordered failover list. All requests will first be sent to the first hostname in the list. If that server is unavailable (i.e., TCP connection is refused or a timeout occurs), then the request will be sent to the next hostname. **RR:** This value indicates that "Round Robin" mode will be used to load balance requests for this customer origin. In this mode, our servers will send a balanced numbers of requests to each hostname.
	Note: The load balancing mode specified for your customer origin configuration is independent from any load balancing configuration that may exist at the origin server.
HttpsHostnames	Required. This response element is only used to indicate that you plan on specifying one or more hostnames for handling HTTPS requests. Keep in mind the following formatting information:
	XML: Each hostname must be contained within a <Hostname> tag. **JSON:** The desired set of hostnames must be contained within a set of square brackets. Additionally, each hostname (i.e., Name request parameter) must be contained with a set of curly braces.
	Important: This request parameter is only available for customers that have purchased an SSL certificate or the HTTPS feature.

Name	Description
Name	Required. A string that determines the hostname/IP address of the origin server that will be associated with the customer origin configuration being updated.
	Use one of the following formats to identify an origin server:
	- *protocol*://*hostname*:*port* (e.g., http://www.mydomain.com:80)
	- *protocol*://*IPv4Address*:*port* (e.g., http://10.10.10.255:80)
	- *protocol*://[*IPv6Address*]:*port* (e.g., http://[1:2:3:4:5:6:7:8]:80)
	Note: If you specify HTTP hostnames to serve HTTPS requests, then you will sacrifice end-to-end data encryption.
HttpsLoadBalancing	Required. A string that determines how HTTPS requests will be load balanced for the specified hostnames. Our servers will use DNS to resolve the specified hostnames into an ordered list of IP addresses. If you have only specified a single web server for this origin server configuration, then either of the following load balancing methods will serve requests through that web server.
	Valid values for this request parameter are described below.
	- **PF:** This value indicates that "Primary and Failover" mode will be used to load balance requests for this customer origin. In this mode, the specified hostnames form an ordered failover list. All requests will first be sent to the first hostname in the list. If that server is unavailable (i.e., TCP connection is refused or a timeout occurs), then the request will be sent to the next hostname.
	- **RR:** This value indicates that "Round Robin" mode will be used to load balance requests for this customer origin. In this mode, our servers will send a balanced numbers of requests to each hostname.
	Note: The load balancing mode specified for your customer origin configuration is independent from any load balancing configuration that may exist at the origin server.

Name	Description
ShieldPOPs	The Origin Shield feature, which must be purchased separately, can be used to reduce the number of requests that must be handled by your customer origin server. If you choose to protect your customer origin with this feature, then you will need to specify each point-of-presence (POP) location where Origin Shield servers will be used to provide an intermediate cache layer between our edge servers and your customer origin. Specify each desired Origin Shield location as an object containing the following key-value pair: 'POPCode': "{*Origin Shield Location*}" **Tip:** If you would like to configure the Origin Shield feature to produce an optimal reduction in requests to your customer origin server, then you should only specify a single location. The specified location should be the POP closest to your customer origin server. **Tip:** Turn off Origin Shield by specifying an empty array. **Note:** Do not specify more than 4 Origin Shield locations.
POPCode	A string that indicates a three or four-letter abbreviation for the desired Origin Shield location. For more information, please refer to the **Appendix E: Origin Shield Locations and Settings** section. **Important:** Specify each desired location using uppercase letters. **Tip:** A list of locations can be retrieved through the Get Origin Shield POPs - HTTP Large endpoint.

Name	Description
networkConfiguration	An integer that determines how hostnames associated with this customer origin configuration will be resolved to an IP address. Valid values are: • **1:** Default. Indicates that the IP preference for this customer origin will be system-defined. Currently, this configuration causes hostnames to be resolved to IPv4 only. • **2:** IPv6 Preferred over IPv4. Indicates that although hostnames for this customer origin can be resolved to either IP version, a preference will be given to IPv6. • **3:** IPv4 Preferred over IPv6. Indicates that although hostnames for this customer origin can be resolved to either IP version, a preference will be given to IPv4. • **4:** IPv4 Only. Indicates that hostnames for this customer origin can only be resolved to IPv4. • **5:** IPv6 Only. Indicates that hostnames for this customer origin can only be resolved to IPv6.

Response

The response to the above request includes an HTTP status code, response headers, and a response body.

Status Code

A status code indicates whether the request was successfully performed. A list of common status codes is provided in the **Status Codes and Error Messages** topic.

Response Headers

The response for this endpoint only returns standard HTTP response headers including those described in the **Response Headers** section of the **Request and Response Elements** topic.

Response Body

The response body for a successful request does not contain a response element.

Errors

The response body for an unsuccessful request may contain an error element that provides additional information. For a list of common error messages, please refer to the **Status Codes and Error Messages** topic.

Sample Request and Response

A sample JSON request is provided below.

```
PUT https://api.edgecast.com/v2/mcc/customers/0001/origins/httplarge/1234 HTTP/1.1
```

```
Authorization: TOK:12345678-1234-1234-1234-1234567890ab
Accept: application/json
Content-Type: application/json
Host: api.edgecast.com
Content-Length: 434


{
        "DirectoryName" : "MyCustomerOrigin",
        "HostHeader" : "images.mydomain.com:80",
        "HttpHostnames" :
        [{
                    "Name" : "http:\/\/images1.mydomain.com:80"
            }, {
                    "Name" : "http:\/\/images2.mydomain.com:80"
            }
        ],
        "HttpLoadBalancing" : "RR",
        "HttpsHostnames" :
        [{
                    "Name" : "https:\/\/images.mydomain.com:443"
            }
        ],
        "HttpsLoadBalancing" : "PF",
        "ShieldPOPs" :
        [{
                    "POPCode" : "LAA"
            }
        ]
}
```

A sample JSON response is provided below.

```
HTTP/1.1 200 OK
Cache-Control: private
Content-Type: application/json; charset=utf-8
Date: Mon, 10 Jan 2011 12:00:00 GMT
```

Update Customer Origin (HTTP Small)

Sets the properties for a customer origin on the HTTP Small platform.

Important: Updating a customer origin will overwrite the entire customer origin configuration. This will occur regardless of whether a request parameter has been excluded from the request.

Note: This endpoint cannot be used to update the directory assigned to a customer origin configuration that has been associated with an edge CNAME.

Request

A request to update the properties of a customer origin configuration is described below. When submitting this request, you will need to define the following terms:

- **xxxx:** Replace this term with your CDN account number.

- **CustomerOriginID:** This term determines the customer origin that will be updated. It should be replaced by the ID of the customer origin that you would like to update.

HTTP Method	Request URI
PUT	https://api.edgecast.com/v2/mcc/customers/*xxxx*/origins/httpsmall/ *CustomerOriginID*

Request Headers

This endpoint only takes advantage of the common request headers described in the **Request Headers** section of the **Request and Response Elements** topic.

Request Body

The request parameters for this endpoint are described below.

Note: The indented parameters indicate that they are a property of the request parameter directly above it. When submitting a request, you will need to use the proper syntax to indicate this relationship. Please refer to the parent request parameter for more information.

Note: Hostnames are associated with a customer origin configuration according to the request type (i.e., HTTP or HTTPS) that they will handle. Although you may choose to define a set of hostnames for each request type, you are only required to specify a single hostname and load balancing method for either request type. If you choose to define one or more hostnames, then you will also need to define the load balancing method for that request type.

Name	Description
DirectoryName	Required. An alphanumeric string that identifies your customer origin configuration. This name is appended to the end of the base CDN URL that points to your customer origin server (e.g., http://wac.0001.edgecastcdn.net/800001/*CustomerOrigin*).
	Important: This setting is read-only for a customer origin configuration that has been associated with at least one edge CNAME configuration. For this type of scenario, make sure that this response element is set to the directory name currently assigned to the customer origin configuration.
HostHeader	Required. A string that identifies the IP address/hostname and port associated with a request. A host header is especially useful when there are multiple virtual domains hosted on a single physical server or load-balanced set of servers.
	Note: A protocol should not be specified when setting this parameter.
HttpHostnames	Required. This response element is only used to indicate that you plan on specifying one or more hostnames for handling HTTP requests. Keep in mind the following formatting information: • **XML:** Each hostname must be contained within a <Hostname> tag. • **JSON:** The desired set of hostnames must be contained within a set of square brackets. Additionally, each hostname (i.e., Name request parameter) must be contained with a set of curly braces.
Name	Required. A string that determines the hostname/IP address of the origin server that will be associated with the customer origin configuration being updated. Use one of the following formats to identify an origin server: • *protocol*://*hostname*:*port* (e.g., http://www.mydomain.com:80) • *protocol*://*IPv4Address*:*port* (e.g., http://10.10.10.255:80) • *protocol*://[*IPv6Address*]:*port* (e.g., http://[1:2:3:4:5:6:7:8]:80)

Name	Description
HttpLoadBalancing	Required. A string that determines how HTTP requests will be load balanced for the specified hostnames. Our servers will use DNS to resolve the specified hostnames into an ordered list of IP addresses. If you have only specified a single web server for this origin server configuration, then either of the following load balancing methods will serve requests through that web server. Valid values for this request parameter are described below. • **PF:** This value indicates that "Primary and Failover" mode will be used to load balance requests for this customer origin. In this mode, the specified hostnames form an ordered failover list. All requests will first be sent to the first hostname in the list. If that server is unavailable (i.e., TCP connection is refused or a timeout occurs), then the request will be sent to the next hostname. • **RR:** This value indicates that "Round Robin" mode will be used to load balance requests for this customer origin. In this mode, our servers will send a balanced numbers of requests to each hostname. **Note:** The load balancing mode specified for your customer origin configuration is independent from any load balancing configuration that may exist at the origin server.
HttpsHostnames	Required. This response element is only used to indicate that you plan on specifying one or more hostnames for handling HTTPS requests. Keep in mind the following formatting information: • **XML:** Each hostname must be contained within a <Hostname> tag. • **JSON:** The desired set of hostnames must be contained within a set of square brackets. Additionally, each hostname (i.e., Name request parameter) must be contained with a set of curly braces. **Important:** This request parameter is only available for customers that have purchased an SSL certificate or the HTTPS feature.

Name	Description
Name	Required. A string that determines the hostname/IP address of the origin server that will be associated with the customer origin configuration being updated. Use one of the following formats to identify an origin server: • *protocol*://*hostname*:*port* (e.g., http://www.mydomain.com:80) • *protocol*://*IPv4Address*:*port* (e.g., http://10.10.10.255:80) • *protocol*://[*IPv6Address*]:*port* (e.g., http://[1:2:3:4:5:6:7:8]:80) **Note:** If you specify HTTP hostnames to serve HTTPS requests, then you will sacrifice end-to-end data encryption.
HttpsLoadBalancing	Required. A string that determines how HTTPS requests will be load balanced for the specified hostnames. Our servers will use DNS to resolve the specified hostnames into an ordered list of IP addresses. If you have only specified a single web server for this origin server configuration, then either of the following load balancing methods will serve requests through that web server. Valid values for this request parameter are described below. • **PF:** This value indicates that "Primary and Failover" mode will be used to load balance requests for this customer origin. In this mode, the specified hostnames form an ordered failover list. All requests will first be sent to the first hostname in the list. If that server is unavailable (i.e., TCP connection is refused or a timeout occurs), then the request will be sent to the next hostname. • **RR:** This value indicates that "Round Robin" mode will be used to load balance requests for this customer origin. In this mode, our servers will send a balanced numbers of requests to each hostname. **Note:** The load balancing mode specified for your customer origin configuration is independent from any load balancing configuration that may exist at the origin server.

Name	Description
ShieldPOPs	The Origin Shield feature, which must be purchased separately, can be used to reduce the number of requests that must be handled by your customer origin server. If you choose to protect your customer origin with this feature, then you will need to specify each point-of-presence (POP) location where Origin Shield servers will be used to provide an intermediate cache layer between our edge servers and your customer origin. Specify each desired Origin Shield location as an object containing the following key-value pair: 'POPCode': "{*Origin Shield Location*}" **Tip:** If you would like to configure the Origin Shield feature to produce an optimal reduction in requests to your customer origin server, then you should only specify a single location. The specified location should be the POP closest to your customer origin server. **Tip:** Turn off Origin Shield by specifying an empty array. **Note:** Do not specify more than 4 Origin Shield locations.
POPCode	A string that indicates a three or four-letter abbreviation for the desired Origin Shield location. For more information, please refer to the **Appendix E: Origin Shield Locations and Settings** section. **Important:** Specify each desired location using uppercase letters. **Tip:** A list of locations can be retrieved through the Get Origin Shield POPs - HTTP Small endpoint.

Name	Description
networkConfiguration	An integer that determines how hostnames associated with this customer origin configuration will be resolved to an IP address. Valid values are: • **1:** Default. Indicates that the IP preference for this customer origin will be system-defined. Currently, this configuration causes hostnames to be resolved to IPv4 only. • **2:** IPv6 Preferred over IPv4. Indicates that although hostnames for this customer origin can be resolved to either IP version, a preference will be given to IPv6. • **3:** IPv4 Preferred over IPv6. Indicates that although hostnames for this customer origin can be resolved to either IP version, a preference will be given to IPv4. • **4:** IPv4 Only. Indicates that hostnames for this customer origin can only be resolved to IPv4. • **5:** IPv6 Only. Indicates that hostnames for this customer origin can only be resolved to IPv6.

Response

The response to the above request includes an HTTP status code, response headers, and a response body.

Status Code

A status code indicates whether the request was successfully performed. A list of common status codes is provided in the **Status Codes and Error Messages** topic.

Response Headers

The response for this endpoint only returns standard HTTP response headers including those described in the **Response Headers** section of the **Request and Response Elements** topic.

Response Body

The response body for a successful request does not contain a response element.

Errors

The response body for an unsuccessful request may contain an error element that provides additional information. For a list of common error messages, please refer to the **Status Codes and Error Messages** topic.

Sample Request and Response

A sample JSON request is provided below.

```
PUT https://api.edgecast.com/v2/mcc/customers/0001/origins/httpsmall/1234 HTTP/1.1
Authorization: TOK:12345678-1234-1234-1234-1234567890ab
Accept: application/json
Content-Type: application/json
Host: api.edgecast.com
Content-Length: 385


{
        "DirectoryName" : "MyCustomerOrigin",
        "HostHeader" : "images.mydomain.com:80",
        "HttpHostnames" :
        [{
                        "Name" : "http:\/\/images1.mydomain.com:80"
                }, {
                        "Name" : "http:\/\/images2.mydomain.com:80"
                }
        ],
        "HttpLoadBalancing" : "RR",
        "HttpsHostnames" :
        [{
                        "Name" : "https:\/\/images.mydomain.com:443"
                }
        ],
        "HttpsLoadBalancing" : "PF",
        "ShieldPOPs" :
        [{
                        "POPCode" : "OXR"
                }
        ]
}
```

A sample JSON response is provided below.

```
HTTP/1.1 200 OK
Cache-Control: private
Content-Length: 25
Content-Type: application/json; charset=utf-8
Date: Mon, 10 Jan 2011 12:00:00 GMT
```

Edge CNAMEs

The endpoints covered in this section allow you to add, retrieve, update, and delete edge CNAMEs.

Add Edge CNAME

Creates an edge CNAME.

Note: Although Creates an edge CNAME, it will not add a CNAME record on a DNS server. This step must be performed before content can be requested through the new edge CNAME.

Request

A request to create an edge CNAME is described below. When submitting this request, you will need to define the following term:

- **xxxx:** Replace this term with your CDN account number.

HTTP Method	Request URI
POST	https://api.edgecast.com/v2/mcc/customers/*xxxx*/cnames

Request Headers

This endpoint only takes advantage of the common request headers described in the **Request Headers** section of the **Request and Response Elements** topic.

Request Body

Optional and required request parameters for this endpoint are described below.

Name	Description
DirPath	Required. A string that identifies a location on the origin server. This string should specify the relative path from the root folder of the origin server to the desired location.
	Tip: Set this parameter to blank to point the edge CNAME to the root folder of the origin server.
EnableCustomReports	An integer that determines whether hits and data transferred statistics will be tracked for this edge CNAME. Logged data can be viewed through the Custom Reports module.
	Valid values for this parameter are:
	- **0:** Disabled (Default Value).
	- **1:** Enabled. CDN activity on this edge CNAME will be logged.

Name	Description
MediaTypeId	Required. An integer that identifies the platform on which the edge CNAME will be created. Valid values for this parameter are: • **3:** HTTP Large (Includes SSL Traffic) • **8:** HTTP Small (Includes SSL Traffic) • **14:** Application Delivery Network (ADN) – (Includes SSL Traffic)
Name	Required. A string that sets the name that will be assigned to the edge CNAME. It should only contain lower-case alphanumeric characters, dashes, and periods. The name specified for this parameter should also be defined as a CNAME record on a DNS server. The CNAME record defined on the DNS server should point to the CDN hostname (e.g., wpc.0001.edgecastcdn.net) for the platform identified by the MediaTypeId request parameter.
OriginId	Required. An integer that identifies whether an edge CNAME will be created for a CDN origin server or a customer origin server. Valid values for this parameter are listed below. • **-1:** Indicates that you would like to create an edge CNAME for our CDN storage service. This type of edge CNAME points to the root folder of a CDN origin server (e.g., /000001). • *CustomerOriginID*: Specifying an ID for an existing customer origin configuration indicates that you would like to create an edge CNAME for that customer origin. This type of edge CNAME points to the root folder of that customer origin server (e.g., /800001/*CustomerOrigin*). **Tip:** Retrieve a list of customer origin IDs through the Get All Customer Origins Creates that corresponds to the desired platform.

Response

The response to the above request includes an HTTP status code, response headers, and a response body.

Status Code

A status code indicates whether the request was successfully performed. A list of common status codes is provided in the **Status Codes and Error Messages** topic.

Response Headers

The response for this endpoint only returns standard HTTP response headers including those described in the **Response Headers** section of the **Request and Response Elements** topic.

Response Body

The response body for a successful request contains the following response element:

Name	Description
CNameId	An integer that indicates the ID assigned to the new edge CNAME.

Errors

The response body for an unsuccessful request may contain an error element that provides additional information. For a list of common error messages, please refer to the **Status Codes and Error Messages** topic.

Sample Request and Response

A sample JSON request is provided below.

```
POST https://api.edgecast.com/v2/mcc/customers/0001/cnames HTTP/1.1

Authorization: TOK:12345678-1234-1234-1234-1234567890ab

Accept: application/json

Content-Type: application/json

Host: api.edgecast.com

Content-Length: 99


{

        "DirPath" : "",

        "MediaTypeId" : 3,

        "Name" : "images.mydomain.com",

        "OriginId" : -1

}
```

A sample JSON response is provided below.

```
HTTP/1.1 200 OK

Cache-Control: private

Content-Length: 19

Content-Type: application/json; charset=utf-8

Date: Mon, 10 Jan 2011 12:00:00 GMT


{

        "CNameId" : 5

}
```

Delete Edge CNAME

Deletes an edge CNAME from a customer's account.

Important: Upon deleting an edge CNAME, it is strongly recommended to either point the corresponding CNAME record away from our CDN service or remove that record from the DNS zone. This best practice is designed to reduce your risk exposure.

Request

A request to delete an edge CNAME is described below. When submitting this request, you will need to define the following terms:

- **xxxx:** Replace this term with your CDN account number.

- **EdgeCNAMEID:** This term identifies an edge CNAME by its ID.

HTTP Method	Request URI
DELETE	https://api.edgecast.com/v2/mcc/customers/*xxxx*/cnames/*EdgeCNAMEID*

Request Headers

This endpoint only takes advantage of the common request headers described in the **Request Headers** section of the **Request and Response Elements** topic.

Request Body

Request body parameters are not required by this endpoint.

Response

The response to the above request includes an HTTP status code, response headers, and a response body.

Status Code

A status code indicates whether the request was successfully performed. A list of common status codes is provided in the **Status Codes and Error Messages** topic.

Response Headers

The response for this endpoint only returns standard HTTP response headers including those described in the **Response Headers** section of the **Request and Response Elements** topic.

Response Body

The response body for a successful request does not contain a response element.

Errors

The response body for an unsuccessful request may contain an error element that provides additional information. For a list of common error messages, please refer to the **Status Codes and Error Messages** topic.

Sample Request and Response

The request format is identical for both JSON and XML. A sample request is provided below.

```
DELETE https://api.edgecast.com/v2/mcc/customers/0001/cnames/123456 HTTP/1.1

Authorization: TOK:12345678-1234-1234-1234-1234567890ab

Host: api.edgecast.com
```

The response is identical for both JSON and XML. A sample response is provided below.

```
HTTP/1.1 200 OK

Cache-Control: private

Date: Mon, 10 Jan 2011 12:00:00 GMT
```

Get All Edge CNAMEs (ADN)

Retrieves all edge CNAMEs for the ADN platform.

Request

A request to retrieve a list of the edge CNAMEs (ADN) associated with a customer's account is described below. When submitting this request, you will need to define the following term:

- **xxxx:** Replace this term with your CDN account number.

HTTP Method	Request URI
GET	https://api.edgecast.com/v2/mcc/customers/*xxxx*/cnames/adn

Request Headers
This endpoint only takes advantage of the common request headers described in the **Request Headers** section of the **Request and Response Elements** topic.

Request Body
Request body parameters are not required by this endpoint.

Response

The response to the above request includes an HTTP status code, response headers, and a response body.

Status Code
A status code indicates whether the request was successfully performed. A list of common status codes is provided in the **Status Codes and Error Messages** topic.

Response Headers
The response for this endpoint only returns standard HTTP response headers including those described in the **Response Headers** section of the **Request and Response Elements** topic.

Response Body

The response body for a successful request contains the following response elements for each edge CNAME returned by this endpoint:

Name	Description
DirPath	A string that indicates the relative location on the origin server to which the edge CNAME is pointed. If this response element is set to blank, then the edge CNAME points to the root folder of the origin server.
EnableCustomReports	An integer that indicates whether hits and data transferred statistics are being tracked for this edge CNAME. Logged data can be viewed through the Custom Reports module. Valid values for this parameter are: • **0:** Disabled (Default Value). • **1:** Enabled. CDN activity on this edge CNAME is being logged.
Id	An integer that indicates the ID for the edge CNAME.
MediaTypeId	An integer that indicates the platform on which the edge CNAME configuration resides. This response element will always report "14," which is the value assigned to the ADN platform.
Name	A string that indicates the name assigned to the edge CNAME.
OriginId	An integer that indicates the origin server associated with the edge CNAME. Valid return values are: • **-1:** Indicates that the edge CNAME points to a CDN origin server. • *CustomerOriginID*: Identifies the customer origin server associated with an edge CNAME by its ID.

Name	Description
OriginString	A string that indicates the origin identifier, the account number, and the relative path associated with the edge CNAME. This information is returned using the following format: */yyxxxx/Path*. • **yy:** Indicates the origin identifier (e.g., 00, 80, 20, etc.) associated with the edge CNAME. • **xxxx:** Indicates the CDN customer account number associated with the edge CNAME. • **Path:** Indicates the relative path to the location on the origin server to which the edge CNAME is pointed. This relative path is also returned by the DirPath response element. ▪ **Customer Origin:** If an edge CNAME points to a customer origin server, then this relative path will always start with the name of the customer origin configuration (e.g., /800001/myorigin).

Errors

The response body for an unsuccessful request may contain an error element that provides additional information. For a list of common error messages, please refer to the **Status Codes and Error Messages** topic.

Sample Request and Response

A sample JSON request is provided below.

```
GET https://api.edgecast.com/v2/mcc/customers/0001/cnames/adn HTTP/1.1

Authorization: TOK:12345678-1234-1234-1234-1234567890ab

Accept: application/json

Host: api.edgecast.com
```

A sample JSON response is provided below.

```
HTTP/1.1 200 OK

Cache-Control: private

Content-Length: 416

Content-Type: application/json; charset=utf-8

Date: Mon, 10 Jan 2011 12:00:00 GMT
```

```
[{
            "DirPath" : "\/application",

            "EnableCustomReports" : 0,

            "Id" : 139019,

            "MediaTypeId" : 14,

            "Name" : "cdnbanking.mydomain.com",

            "OriginId" : 114197,

            "OriginString" : "\/800001\/banking "

    }, {

            "DirPath" : "",

            "EnableCustomReports" : 0,

            "Id" : 143659,

            "MediaTypeId" : 14,

            "Name" : "cdn.socialmedia.com",

            "OriginId" : -1,

            "OriginString" : "\/000001"

    }
]
```

Get All Edge CNAMEs (HTTP Large)

Retrieves all edge CNAMEs for the HTTP Large platform.

Request

A request to retrieve a list of the edge CNAMEs (HTTP Large) associated with a customer's account is described below. When submitting this request, you will need to define the following terms:

- **xxxx:** Replace this term with your CDN account number.

HTTP Method	Request URI
GET	https://api.edgecast.com/v2/mcc/customers/*xxxx*/cnames/httplarge

Request Headers

This endpoint only takes advantage of the common request headers described in the **Request Headers** section of the **Request and Response Elements** topic.

Request Body

Request body parameters are not required by this endpoint.

Response

The response to the above request includes an HTTP status code, response headers, and a response body.

Status Code

A status code indicates whether the request was successfully performed. A list of common status codes is provided in the **Status Codes and Error Messages** topic.

Response Headers

The response for this endpoint only returns standard HTTP response headers including those described in the **Response Headers** section of the **Request and Response Elements** topic.

Response Body

The response body for a successful request contains the following response elements for each edge CNAME returned by this endpoint:

Name	Description
DirPath	A string that indicates the relative location on the origin server to which the edge CNAME is pointed. If this response element is set to blank, then the edge CNAME points to the root folder of the origin server.
EnableCustomReports	An integer that indicates whether hits and data transferred statistics are being tracked for this edge CNAME. Logged data can be viewed through the Custom Reports module. Valid values for this parameter are: • **0:** Disabled (Default Value). • **1:** Enabled. CDN activity on this edge CNAME is being logged.
Id	An integer that indicates the ID for the edge CNAME.
MediaTypeId	An integer that indicates the platform on which the edge CNAME configuration resides. This response element will always report "3," which is the value assigned to the HTTP Large platform.
Name	A string that indicates the name assigned to the edge CNAME.
OriginId	An integer that indicates the origin server associated with the edge CNAME. Valid return values are: • **-1:** Indicates that the edge CNAME points to a CDN origin server. • *CustomerOriginID*: Identifies the customer origin server associated with an edge CNAME by its ID.

Name	Description
OriginString	A string that indicates the origin identifier, the account number, and the relative path associated with the edge CNAME. This information is returned using the following format: */yyxxxx/Path*. • **yy:** Indicates the origin identifier (e.g., 00, 80, 20, etc.) associated with the edge CNAME. • **xxxx:** Indicates the CDN customer account number associated with the edge CNAME. • **Path:** Indicates the relative path to the location on the origin server to which the edge CNAME is pointed. This relative path is also returned by the DirPath response element. ▪ **Customer Origin:** If an edge CNAME points to a customer origin server, then this relative path will always start with the name of the customer origin configuration (e.g., /800001/myorigin).

Errors

The response body for an unsuccessful request may contain an error element that provides additional information. For a list of common error messages, please refer to the **Status Codes and Error Messages** topic.

Sample Request and Response

A sample JSON request is provided below.

```
GET https://api.edgecast.com/v2/mcc/customers/0001/cnames/httplarge HTTP/1.1
Authorization: TOK:12345678-1234-1234-1234-1234567890ab
Accept: application/json
Host: api.edgecast.com
```

A sample JSON response is provided below.

```
HTTP/1.1 200 OK
Cache-Control: private
Content-Length: 386
Content-Type: application/json; charset=utf-8
Date: Mon, 10 Jan 2011 12:00:00 GMT


[{
            "DirPath" : "",
            "EnableCustomReports" : 0,
```

```
        "Id" : 10101,

        "MediaTypeId" : 3,

        "Name" : "www.domain.com",

        "OriginId" : -1,

        "OriginString" : "\/000001"

}, {

        "DirPath" : "\/2011\/images",

        "EnableCustomReports" : 0,

        "Id" : 55330,

        "MediaTypeId" : 3,

        "Name" : "images.domain.com",

        "OriginId" : 12345,

        "OriginString" : "\/800001\/101.10.10.10\/2011\/images"

}

]
```

Get All Edge CNAMEs (HTTP Small)

Retrieves all edge CNAMEs for the HTTP Small platform associated with a particular customer.

Request

A request to retrieve a list of the edge CNAMEs (HTTP Small) associated with a customer's account is described below. When submitting this request, you will need to define the following term:

- **xxxx:** Replace this term with your CDN account number.

HTTP Method	Request URI
GET	https://api.edgecast.com/v2/mcc/customers/*xxxx*/cnames/httpsmall

Request Headers
This endpoint only takes advantage of the common request headers described in the **Request Headers** section of the **Request and Response Elements** topic.

Request Body
Request body parameters are not required by this endpoint.

Response

The response to the above request includes an HTTP status code, response headers, and a response body.

Status Code

A status code indicates whether the request was successfully performed. A list of common status codes is provided in the **Status Codes and Error Messages** topic.

Response Headers

The response for this endpoint only returns standard HTTP response headers including those described in the **Response Headers** section of the **Request and Response Elements** topic.

Response Body

The response body for a successful request contains the following response elements for each edge CNAME returned by this endpoint:

Name	Description
DirPath	A string that indicates the relative location on the origin server to which the edge CNAME is pointed. If this response element is set to blank, then the edge CNAME points to the root folder of the origin server.
EnableCustomReports	An integer that indicates whether hits and data transferred statistics are being tracked for this edge CNAME. Logged data can be viewed through the Custom Reports module. Valid values for this parameter are: • **0:** Disabled (Default Value). • **1:** Enabled. CDN activity on this edge CNAME is being logged.
Id	An integer that indicates the ID for the edge CNAME.
MediaTypeId	An integer that indicates the platform on which the edge CNAME configuration resides. This response element will always report "8," which is the value assigned to the HTTP Small platform.
Name	A string that indicates the name assigned to the edge CNAME.
OriginId	An integer that indicates the origin server associated with the edge CNAME. Valid return values are: • **-1:** Indicates that the edge CNAME points to a CDN origin server. • *CustomerOriginID*: Identifies the customer origin server associated with an edge CNAME by its ID.

Name	Description
OriginString	A string that indicates the origin identifier, the account number, and the relative path associated with the edge CNAME. This information is returned using the following format: */yyxxxx/Path*. • **yy:** Indicates the origin identifier (e.g., 00, 80, 20, etc.) associated with the edge CNAME. • **xxxx:** Indicates the CDN customer account number associated with the edge CNAME. • **Path:** Indicates the relative path to the location on the origin server to which the edge CNAME is pointed. This relative path is also returned by the DirPath response element. ▪ **Customer Origin:** If an edge CNAME points to a customer origin server, then this relative path will always start with the name of the customer origin configuration (e.g., /800001/myorigin).

Errors

The response body for an unsuccessful request may contain an error element that provides additional information. For a list of common error messages, please refer to the **Status Codes and Error Messages** topic.

Sample Request and Response

A sample JSON request is provided below.

```
GET https://api.edgecast.com/v2/mcc/customers/0001/cnames/httpsmall HTTP/1.1

Authorization: TOK:12345678-1234-1234-1234-1234567890ab

Accept: application/json

Host: api.edgecast.com
```

A sample JSON response is provided below.

```
HTTP/1.1 200 OK

Cache-Control: private

Content-Length: 386

Content-Type: application/json; charset=utf-8

Date: Mon, 10 Jan 2011 12:00:00 GMT


[{

            "DirPath" : "",

            "EnableCustomReports" : 0,

            "Id" : 20101,
```

```
            "MediaTypeId" : 8,
            "Name" : "www.domain.com",
            "OriginId" : -1,
            "OriginString" : "\/000001"
    }, {
            "DirPath" : "\/2011\/images",
            "EnableCustomReports" : 0,
            "Id" : 25330,
            "MediaTypeId" : 8,
            "Name" : "images.domain.com",
            "OriginId" : 12300,
            "OriginString" : "\/800001\/101.10.10.10\/2011\/images"
    }
]
```

Get Edge CNAME

Returns the properties of an edge CNAME.

Note: If you would like to retrieve a list of edge CNAMEs by platform for a particular customer's account, please refer to the section corresponding to the desired platform.

Request

A request to view the properties associated with an edge CNAME is described below. When submitting this request, you will need to define the following terms:

- **xxxx:** Replace this term with your CDN account number.

- **EdgeCNAMEID:** This term should be replaced by the ID assigned to the edge CNAME whose properties you would like to view. The ID associated with each edge CNAME is returned by the platform-specific Returns called "Get All Edge CNAMEs."

HTTP Method	Request URI
GET	https://api.edgecast.com/v2/mcc/customers/*xxxx*/cnames/*EdgeCNAMEID*

Request Headers

This endpoint only takes advantage of the common request headers described in the **Request Headers** section of the **Request and Response Elements** topic.

Request Body

Request body parameters are not required by this endpoint.

Response

The response to the above request includes an HTTP status code, response headers, and a response body.

Status Code

A status code indicates whether the request was successfully performed. A list of common status codes is provided in the **Status Codes and Error Messages** topic.

Response Headers

The response for this endpoint only returns standard HTTP response headers including those described in the **Response Headers** section of the **Request and Response Elements** topic.

Response Body

The response body for a successful request contains the following response elements:

Name	Description
DirPath	A string that indicates a location on the origin server. This string should specify the relative path from the root folder to the desired location. A blank value indicates that the edge CNAME points to the root folder of the origin server.
EnableCustomReports	An integer that indicates whether hits and data transferred statistics are being tracked for this edge CNAME. Logged data can be viewed through the Custom Reports module. Valid values for this parameter are: • **0:** Disabled (Default Value). • **1:** Enabled. CDN activity on this edge CNAME is being logged.
Id	An integer that indicates the ID assigned to the edge CNAME.
MediaTypeId	An integer that indicates the platform associated with the edge CNAME. A platform is identified by its ID. Valid return values are: • **3:** HTTP Large • **8:** HTTP Small • **14:** ADN
Name	A string that indicates the name assigned to the edge CNAME.

Name	Description
OriginId	An integer that indicates the origin server associated with the edge CNAME. Valid return values are: • **-1:** Indicates that the edge CNAME points to a CDN origin server. • *CustomerOriginID*: Identifies the customer origin server associated with an edge CNAME by its ID.
OriginString	A string that indicates the origin identifier, the account number, and the relative path associated with the edge CNAME. This information is returned using the following format: */yyxxxx/Path*. • **yy:** Indicates the origin identifier (e.g., 00, 80, 20, etc.) associated with the edge CNAME. • **xxxx:** Indicates the CDN customer account number associated with the edge CNAME. • **Path:** Indicates the relative path to the location on the origin server to which the edge CNAME is pointed. This relative path is also returned by the DirPath response element. ▪ **Customer Origin:** If an edge CNAME points to a customer origin server, then this relative path will always start with the name of the customer origin configuration (e.g., /800001/myorigin).

Errors

The response body for an unsuccessful request may contain an error element that provides additional information. For a list of common error messages, please refer to the **Status Codes and Error Messages** topic.

Sample Request and Response

A sample JSON request is provided below.

```
GET https://api.edgecast.com/v2/mcc/customers/0001/cnames/123456 HTTP/1.1

Authorization: TOK:12345678-1234-1234-1234-1234567890ab

Accept: application/json

Host: api.edgecast.com
```

A sample JSON response is provided below.

```
HTTP/1.1 200 OK

Cache-Control: private

Content-Length: 192

Content-Type: application/json; charset=utf-8

Date: Mon, 10 Jan 2011 12:00:00 GMT

{

        "DirPath" : "\/RelativePath",

        "EnableCustomReports" : 0,

        "Id" : 123456,

        "MediaTypeId" : 3,

        "Name" : "images.mydomain.com",

        "OriginId" : -1,

        "OriginString" : "\/000001\/RelativePath"

}
```

Get Edge CNAME Status

Retrieves the propagation status for an edge CNAME configuration.

Note: This endpoint may not be used to retrieve propagation status for edge CNAME configurations that were last updated more than 7 days ago.

Request

A request to retrieve status information is described below. When submitting this request, you will need to define the following terms:

- **xxxx:** Replace this term with the desired customer account number.

- **EdgeCNAMEID:** Replace this term with the system-defined ID for the desired edge CNAME configuration.

  Use a platform-specific Get All Edge CNAMEs endpoint to retrieve the system-defined ID for the desired customer origin.

  Sample request for the HTTP Large platform:

  https://api.edgecast.com/v2/mcc/customers/0001/cnames/httplarge

Note: Please refer to the REST API Help Center for more detailed information on this endpoint.

HTTP Method	Request URI
GET	https://api.edgecast.com/v2/mcc/customers/*xxxx*/cnames/*EdgeCNAMEID*/status

Request Headers

This endpoint only takes advantage of the common request headers described in the **Request Headers** section of the **Request and Response Elements** topic.

Request Body

Request body parameters are not required by this endpoint.

Response

The response to the above request includes an HTTP status code, response headers, and a response body.

Status Code

A status code indicates whether the request was successfully performed. A list of common status codes is provided in the **Status Codes and Error Messages** topic.

Response Headers

The response for this endpoint only returns standard HTTP response headers including those described in the **Response Headers** section of the **Request and Response Elements** topic.

Response Body

The response body for a successful request varies according to the following factors:

- **New / Update:** The following response will be provided immediately after an edge CNAME configuration is created or updated:

  ```
  {"Status":"New","Percent_propagated":0}
  ```

- **Existing Configurations:** If the edge CNAME configuration is older than 7 days, then this endpoint will return a 400 Bad Request with the following response body:

  ```
  {"Message":"Action Queue Id missing"}
  ```

- **Deployment:** Once the deployment of the new/updated edge CNAME configuration begins, the response body will contain the following response elements:

Name	Data Type	Description
Status	String	Indicates the edge CNAME's current propagation status. Valid values are: • **New:** Indicates that the configuration has been created, but the propagation process has not started. > **Note:** A new configuration may stay in this state for a few minutes while it undergoes a validation/verification process. • **propagating:** Indicates that the configuration is in the process of being propagated. • **propagated:** Indicates that the configuration has been propagated across the entire network.
Percent_propagated	Decimal	Indicates the average configuration propagation percentage across all POPs.
Pops	Array	Contains a list of POPs and their current configuration propagation percentage.
name	String	Identifies a POP by region and name. **Syntax (Single POP per Location):** *Region* : *POPName* **Syntax (Multiple POPs per Location):** If a location contains multiple POPs, then a three-letter abbreviation will identify each POP: *Region* : *POPName* (*POP*)
percentage_propagated	Decimal	Indicates the percentage of servers within a POP to which the configuration has been propagated.

Errors

The response body for an unsuccessful request may contain an error element that provides additional information. For a list of common error messages, please refer to the **Status Codes and Error Messages** topic.

Sample Request and Response

A sample JSON request is provided below.

```
GET https://api.edgecast.com/v2/mcc/customers/0001/cnames/123456/status HTTP/1.1

Authorization: TOK:12345678-1234-1234-1234-1234567890ab

Accept: application/json

Host: api.edgecast.com
```

A sample JSON response is provided below.

```
HTTP/1.1 200 OK

Cache-Control: private

Content-Type: application/json; charset=utf-8

Date: Thu, 14 Apr 2016 12:00:00 GMT

Content-Length: 7051

{

        "Status": "propagated",

        "Percent_propagated": 100,

        "Pops": [{

                        "name": "South America : Valparaiso, Chile",

                        "percentage_propagated": 100

                }, {

                        ...

                        "name": "Europe : London",

                        "percentage_propagated": 91.20879120879121

                }, {

                        "name": "North America : Atlanta",

                        "percentage_propagated": 100

                }, {

                        "name": "North America : Miami",

                        "percentage_propagated": 100

                }, {

                        "name": "Europe : London",

                        "percentage_propagated": 100

                }

        ]
}
```

Update Edge CNAME

Updates the properties of an edge CNAME configuration.

Note: Although this endpoint allows you to modify the hostname associated with an edge CNAME configuration, it will not update the corresponding CNAME record on a DNS server. Make sure to do so upon updating an edge CNAME's hostname.

Request

A request to update the properties associated with an edge CNAME configuration is described below. When submitting this request, you will need to define the following terms:

- **xxxx:** Replace this term with your CDN account number.

- **EdgeCNAMEID:** This term should be replaced by the ID corresponding to the edge CNAME configuration whose properties you would like to update. The ID associated with each edge CNAME is returned by the platform-specific endpoint called "Get All Edge CNAMEs."

HTTP Method	Request URI
PUT	https://api.edgecast.com/v2/mcc/customers/*xxxx*/cnames/*EdgeCNAMEID*

Request Headers

This endpoint only takes advantage of the common request headers described in the **Request Headers** section of the **Request and Response Elements** topic.

Request Body

The request parameters for this endpoint are described below.

Note: Omitting or setting an optional parameter to null will prevent it from being assigned a value.

Name	Description
DirPath	A string that defines a location on the origin server to which the edge CNAME configuration will be pointed. This string should specify the relative path from the origin server's root folder to the desired folder. **Tip:** Set this parameter to blank to point the edge CNAME to the root folder of the origin server.

Name	Description
EnableCustomReports	An integer that determines whether hits and data transferred statistics will be tracked for this edge CNAME. Logged data can be viewed through the Custom Reports module.
	Valid values for this parameter are:
	• **0:** Disabled (Default Value).
	• **1:** Enabled. CDN activity on this edge CNAME will be logged.
Name	A string that indicates the name associated with the edge CNAME. It should only contain lower-case alphanumeric characters, dashes, and periods.
OriginId	An integer that determines whether the edge CNAME will point to a CDN origin server or a customer origin server. Valid values for this parameter are listed below.
	• **-1:** Indicates that you would like to point the edge CNAME to the root folder of a CDN origin server (/00*xxxx*).
	• *CustomerOriginID*: Specifying an ID for an existing customer origin configuration indicates that you would like to point an edge CNAME to that customer origin. This type of edge CNAME points to the root folder of that customer origin server (/80*xxxx*/*CustomerOrigin*).
	Tip: Retrieve a list of customer origin IDs through the various Get All Customer Origins endpoints.

Response

The response to the above request includes an HTTP status code, response headers, and a response body.

Status Code

A status code indicates whether the request was successfully performed. A list of common status codes is provided in the **Status Codes and Error Messages** topic.

Response Headers

The response for this endpoint only returns standard HTTP response headers including those described in the **Response Headers** section of the **Request and Response Elements** topic.

Response Body

The response body for a successful request does not contain a response element.

Errors

The response body for an unsuccessful request may contain an error element that provides additional information. For a list of common error messages, please refer to the **Status Codes and Error Messages** topic.

Sample Request and Response

A sample JSON request is provided below.

```
PUT https://api.edgecast.com/v2/mcc/customers/0001/cnames/123456 HTTP/1.1
Authorization: TOK:12345678-1234-1234-1234-1234567890ab
Accept: application/json
Host: api.edgecast.com
Content-Length: 133


{
        "DirPath" : "\/RelativePath",
        "EnableCustomReports" : 0,
        "Name" : "images.mydomain.com",
        "OriginId" : -1
}
```

A sample JSON response is provided below.

```
HTTP/1.1 200 OK
Cache-Control: private
Content-Length: 0
Content-Type: application/json; charset=utf-8
Date: Mon, 10 Jan 2011 12:00:00 GMT
```

Dynamic Cloud Packaging

Automate the administration of Dynamic Cloud Packaging configurations, such as:

- Instances

- Encrypted HLS directories

- Live authentication keys

Add Encrypted HLS Directory

Adds an encrypted HLS directory configuration that is only applicable for on-demand streaming via Dynamic Cloud Packaging.

Note: The workflow for updating an encrypted HLS directory configuration is to delete the old configuration and then create a new one through this endpoint.

Request

A request to create an encrypted HLS directory is described below. When submitting this request, you will need to define the following term:

- **xxxx:** Replace this term with your CDN account number.

HTTP Method	Request URI
POST	https://api.edgecast.com/v2/mcc/customers/*xxxx*/httpstreaming/dcp/vod/ehlsdirectory

Request Headers
This endpoint only takes advantage of the common request headers described in the **Request Headers** section of the **Request and Response Elements** topic.

Request Body
The required request parameters for this endpoint are described below.

Name	Data Type	Description
OriginType	Object	Contains an integer value that identifies the type of origin server to which this configuration will be applied.
ID	Integer	Identifies a type of origin server. Valid values are: - **1:** CDN Origin - **2:** Customer Origin

Name	Data Type	Description
Path	String	Identifies a directory by its relative path. Encrypted HLS will be applied to on-demand content streamed from this directory.

Response

The response to the above request includes an HTTP status code, response headers, and a response body.

Status Code

A status code indicates whether the request was successfully performed. A list of common status codes is provided in the **Status Codes and Error Messages** topic.

Response Headers

The response for this endpoint only returns standard HTTP response headers including those described in the **Response Headers** section of the **Request and Response Elements** topic.

Response Body

The response body for a successful request contains the following response element:

Name	Data Type	Description
Id	Integer	Identifies the newly created encrypted HLS directory configuration by its system-defined ID.

Errors

The response body for an unsuccessful request may contain an error element that provides additional information. For a list of common error messages, please refer to the **Status Codes and Error Messages** topic.

Sample Request and Response

A sample JSON request is provided below.

```
POST
https://api.edgecast.com/v2/mcc/customers/0001/httpstreaming/dcp/vod/ehlsdirectory
HTTP/1.1

Authorization: TOK:12345678-1234-1234-1234-1234567890ab

Accept: application/json

Content-Type: application/json

Host: api.edgecast.com

Content-Length: 68
```

```
[{
          "OriginType": {
                    "Id": 2
          },
          "Path": "\/videos"
     }
]
```

A sample JSON response is provided below.

```
HTTP/1.1 200 OK

Cache-Control: private

Content-Length: 23

Content-Type: application/json; charset=utf-8

Date: Mon, 10 Jan 2011 12:00:00 GMT


[{
          "Id": 6687
     }
]
```

Add Instance

Creates an instance.

Request

A request to create an instance is described below. When submitting this request, you will need to define the following term:

- **xxxx:** Replace this term with your CDN account number.

HTTP Method	Request URI
POST	https://api.edgecast.com/v2/mcc/customers/*xxxx*/httpstreaming/dcp/live

Request Headers
This endpoint only takes advantage of the common request headers described in the **Request Headers** section of the **Request and Response Elements** topic.

Request Body
Optional and required request parameters for this endpoint are described below.

Name	Data Type	Description
EncryptedKeyRotation	Integer	**Note:** The Encrypted Key Rotation feature requires activation on your account. Please contact your CDN account manager to activate it.
		Note: A prerequisite for this capability is the enablement of the Encrypted HLS feature on this instance through the Encrypted parameter.
		Determines whether the encryption key generated for a live event will be rotated at regular intervals.
		Valid states:
		• **Missing/Null:** Omit this parameter or set it to a null value to disable encrypted key rotation.
		• **Seconds:** Set this parameter to the desired time interval. This time interval must be:
		▪ Greater than or equal to 10 seconds and less than or equal to 1440 seconds.
		▪ Specified in multiples of 5 (e.g., 10, 15, 20, etc.) seconds.
		Important: The Server-Side Archiving feature is incompatible with this feature. Do not enable both features within a single instance.
		Note: Encryption key rotation may only take place at the start of a new segment. Therefore, the live event's segment size factors into when the encryption key will be rotated.
		Default Value: null
SsaEnabled	Boolean	**Note:** SSA requires activation on your account. Please contact your CDN account manager to activate it.
		Determines whether Server-Side Archiving (SSA) will be enabled for all live streams generated from this instance.
		Important: The Server-Side Archiving feature is incompatible with the Encrypted HLS feature. Do not enable both features within a single instance.
		Default Value: False

Name	Data Type	Description
Encrypted	Boolean	Determines whether the live streams generated for this instance will be secured with encrypted HLS. Valid values are: • **True:** Enabled • **False:** Disabled (default) **Important:** The Server-Side Archiving feature is incompatible with the Encrypted HLS feature. Do not enable both features within a single instance.
InstanceName	String	Assigns a name to the instance. **Note:** This name will be incorporated into the publishing point and playback URL. Therefore, it should be URL-compatible.
DvrDuration	Integer	Determines the length, in minutes, of the DVR window. The length of this DVR window may be set from 5 to 180 minutes (i.e., 3 hours). **Default Value:** 1 minute
SegmentSize	Integer	Determines the size, in seconds, of the segments that will be generated for this instance. Segment size may be set from 1 to 20 seconds.

Response

The response to the above request includes an HTTP status code, response headers, and a response body.

Status Code

A status code indicates whether the request was successfully performed. A list of common status codes is provided in the **Status Codes and Error Messages** topic.

Response Headers

The response for this endpoint only returns standard HTTP response headers including those described in the **Response Headers** section of the **Request and Response Elements** topic.

Response Body

The response body for a successful request contains the following response element:

Name	Data Type	Description
DvrDuration	Integer	Indicates the length, in minutes, of the DVR window. The length of this DVR window may be set from 5 to 180 minutes (i.e., 3 hours). **Note:** If a DVR window was not specified in the request, then this parameter will report a default duration of 1 minute.
Encrypted	Boolean	Indicates whether the live streams generated for this instance will be secured with encrypted HLS.
EncryptedKeyRotation	Integer	Indicates the interval, in seconds, at which the encryption key generated for the live event will be rotated. **Note:** Encryption key rotation may only take place at the start of a new segment. Therefore, the live event's segment size factors into when the encryption key will be rotated.
HlsPlaybackUrl	String	Indicates the instance's HLS playback URL. Syntax: http:\/\/wpc.*xxxx*.edgecastcdn.net\/24*xxxx*\/*InstanceName*\/<streamName>.m3u8
Id	Integer	Indicates the unique system-defined ID assigned to the instance.
InstanceName	String	Identifies the instance by its name.
MpegDashPlaybackUrl	String	Indicates the instance's MPEG-DASH playback URL. Syntax: http:\/\/wpc.*xxxx*.edgecastcdn.net\/24*xxxx*\/*InstanceName*\/<streamName>.mpd
PublishUrl	String	Indicates the publishing point's relative path followed by syntax information on how to authorize a stream. Syntax: \/20*xxxx*\/*InstanceName*\/<streamName>?<Live Authentication Key>
SegmentSize	Integer	Indicates the size, in seconds, of the segments that will be generated for this instance.
SsaEnabled	Boolean	Indicates whether Server-Side Archiving (SSA) has been enabled on this instance. **Note:** SSA requires activation on your account. Please contact your CDN account manager to activate it.

The response body for an unsuccessful request may contain an error element that provides additional information. For a list of common error messages, please refer to the **Status Codes and Error Messages** topic.

Sample Request and Response

A sample JSON request is provided below.

```
POST https://api.edgecast.com/v2/mcc/customers/0001/httpstreaming/dcp/live HTTP/1.1

Authorization: TOK:12345678-1234-1234-1234-1234567890ab

Accept: application/json

Content-Type: application/json

Host: api.edgecast.com

Content-Length: 61


{

        "InstanceName": "mythirdinstance",

        "SegmentSize": 10

}
```

A sample JSON response is provided below.

```
HTTP/1.1 200 OK

Cache-Control: private

Content-Length: 431

Content-Type: application/json; charset=utf-8

Date: Mon, 10 Jan 2011 12:00:00 GMT


{

        "DvrDuration": null,

        "Encrypted": false,

        "EncryptedKeyRotation": null,

        "HlsPlaybackUrl":
        "http:\/\/wpc.0001.edgecastcdn.net\/240001\/myinstance\/<streamName>.m3u8",

        "Id": 1317,

        "InstanceName": "myinstance",

        "MpegDashPlaybackUrl":
        "http:\/\/wpc.0001.edgecastcdn.net\/240001\/myinstance\/<streamName>.mpd",

        "PublishUrl": "\/200001\/myinstance\/<streamName>?<Live Authentication Key>",

        "SegmentSize": 10,

        "SsaEnabled": false
```

```
}
```

Add Stream Key

Adds a stream key that provides authorization for the Dynamic Cloud Packaging streaming service.

Request

A request to create a stream key is described below. When submitting this request, you will need to define the following term:

- **xxxx:** Replace this term with your CDN account number.

HTTP Method	Request URI
POST	https://api.edgecast.com/v2/mcc/customers/*xxxx*/httpstreaming/dcp/streamkeys

Request Headers

This endpoint only takes advantage of the common request headers described in the **Request Headers** section of the **Request and Response Elements** topic.

Request Body

The required request parameters for this endpoint are described below.

Name	Data Type	Description
DirPath	String	Identifies a stream by its relative path. The starting point for this relative path is indicated in blue font below. rtmp://fso.oxr.0001.edgecastcdn.net/200001/myinstance/mystream **Note:** The stream identified by this parameter will be authorized by the value defined in the Key parameter. This stream path must consist of: • Alphanumeric characters • A single forward slash that delimits the instance name from the stream name. Optionally, an asterisk (*), which represents one or more characters, may be appended to the stream name. **Tip:** Do not specify a pattern after an asterisk as it will be ignored.

Name	Data Type	Description
Key	String	Identifies the live authentication key that may be used to authenticate streams published to the path specified by this stream key configuration. This key must be 256 alphanumeric characters or less.

Response

The response to the above request includes an HTTP status code, response headers, and a response body.

Status Code

A status code indicates whether the request was successfully performed. A list of common status codes is provided in the **Status Codes and Error Messages** topic.

Response Headers

The response for this endpoint only returns standard HTTP response headers including those described in the **Response Headers** section of the **Request and Response Elements** topic.

Response Body

The response body for a successful request contains the following response elements:

Name	Data Type	Description
DirPath	String	Indicates the stream path assigned to the new stream key.
Id	Integer	Indicates the unique system-defined ID assigned to the newly created stream key.
Key	String	Indicates the live authentication key assigned to the new stream key.

Errors

The response body for an unsuccessful request may contain an error element that provides additional information. For a list of common error messages, please refer to the **Status Codes and Error Messages** topic.

Sample Request and Response

A sample JSON request is provided below.

```
POST https://api.edgecast.com/v2/mcc/customers/0001/httpstreaming/dcp/streamkeys
HTTP/1.1

Authorization: TOK:12345678-1234-1234-1234-1234567890ab

Accept: application/json

Content-Type: application/json

Host: api.edgecast.com

Content-Length: 69

{

        "DirPath" : "myinstance\/livevideos",

        "Key" : "abcdef123456"

}
```

A sample JSON response is provided below.

```
HTTP/1.1 200 OK

Cache-Control: private

Content-Length: 69

Content-Type: application/json; charset=utf-8

Date: Mon, 10 Jan 2011 12:00:00 GMT


{

        "DirPath": "myinstance\/livevideos",

        "Id": 193950,

        "Key": "abcdef123456"

}
```

Delete Encrypted HLS Directory

Deletes an encrypted HLS directory configuration.

Important: The deletion of an encrypted HLS directory configuration takes place immediately. Additionally, once it has been deleted, it cannot be recovered.

Request

A request to delete an encrypted HLS directory is described below. When submitting this request, you will need to define the following terms:

- **xxxx:** Replace this term with your CDN account number.

- **EHLSDirectoryID:** Replace this variable with the system-defined ID of the encrypted HLS directory configuration that will be deleted.

    Tip: Use the Get Encrypted HLS Directories endpoint to retrieve a list of encrypted HLS directory configurations and their system-defined IDs.

HTTP Method	Request URI
DELETE	https://api.edgecast.com/v2/mcc/customers/*xxxx*/httpstreaming/dcp/vod/ ehlsdirectory/*EHLSDirectoryID*

Request Headers

This endpoint only takes advantage of the common request headers described in the **Request Headers** section of the **Request and Response Elements** topic.

Request Body

Request body parameters are not required by this endpoint.

Response

The response to the above request includes an HTTP status code, response headers, and a response body.

Status Code

A status code indicates whether the request was successfully performed. A list of common status codes is provided in the **Status Codes and Error Messages** topic.

Response Headers

The response for this endpoint only returns standard HTTP response headers including those described in the **Response Headers** section of the **Request and Response Elements** topic.

Response Body

The response body for a successful request does not contain a response element.

The response body for an unsuccessful request may contain an error element that provides additional information. For a list of common error messages, please refer to the **Status Codes and Error Messages** topic.

Sample Request and Response

A sample request is provided below.

```
DELETE
https://api.edgecast.com/v2/mcc/customers/0001/httpstreaming/dcp/vod/ehlsdirectory/1
010 HTTP/1.1

Authorization: TOK:12345678-1234-1234-1234-1234567890ab

Host: api.edgecast.com
```

A sample response is provided below.

```
HTTP/1.1 200 OK

Cache-Control: private

Date: Mon, 10 Jan 2011 12:00:00 GMT
```

Delete Instance

Deletes an instance.

Important: The deletion of an instance takes place immediately. Additionally, once an instance has been deleted, it cannot be recovered.

Request

A request to delete an instance is described below. When submitting this request, you will need to define the following terms:

- **xxxx:** Replace this term with your CDN account number.

- **InstanceID:** Replace this variable with the system-defined ID of the desired instance.

    Tip: Retrieve a list of instances and their system-defined IDs through the Get All Instances endpoint.

HTTP Method	Request URI
DELETE	https://api.edgecast.com/v2/mcc/customers/*xxxx*/httpstreaming/dcp/live/*InstanceID*

Request Headers

This endpoint only takes advantage of the common request headers described in the **Request Headers** section of the **Request and Response Elements** topic.

Request Body

Request body parameters are not required by this endpoint.

Response

The response to the above request includes an HTTP status code, response headers, and a response body.

Status Code

A status code indicates whether the request was successfully performed. A list of common status codes is provided in the **Status Codes and Error Messages** topic.

Response Headers

The response for this endpoint only returns standard HTTP response headers including those described in the **Response Headers** section of the **Request and Response Elements** topic.

Response Body

The response body for a successful request does not contain a response element.

Errors

The response body for an unsuccessful request may contain an error element that provides additional information. For a list of common error messages, please refer to the **Status Codes and Error Messages** topic.

Sample Request and Response

A sample request is provided below.

```
DELETE https://api.edgecast.com/v2/mcc/customers/0001/httpstreaming/dcp/live/775
HTTP/1.1

Authorization: TOK:12345678-1234-1234-1234-1234567890ab

Host: api.edgecast.com
```

A sample response is provided below.

```
HTTP/1.1 200 OK

Cache-Control: private

Date: Mon, 10 Jan 2011 12:00:00 GMT
```

Delete Stream Key

Deletes a stream key that authorizes a live stream on the Dynamic Cloud Packaging streaming service.

Request

A request to delete a stream key is described below. When submitting this request, you will need to define the following terms:

- **xxxx:** Replace this term with your CDN account number.

- **KeyID:** Replace this variable with the unique ID assigned to the stream key that will be deleted.

    Tip: Use the Get Stream Keys endpoint to retrieve a listing of stream keys and their IDs. Replace this variable with the system-defined ID of the desired instance.

HTTP Method	Request URI
DELETE	https://api.edgecast.com/v2/mcc/customers/*xxxx*/httpstreaming/dcp/streamkeys/*KeyID*

Request Headers

This endpoint only takes advantage of the common request headers described in the **Request Headers** section of the **Request and Response Elements** topic.

Request Body

Request body parameters are not required by this endpoint.

Response

The response to the above request includes an HTTP status code, response headers, and a response body.

Status Code

A status code indicates whether the request was successfully performed. A list of common status codes is provided in the **Status Codes and Error Messages** topic.

Response Headers

The response for this endpoint only returns standard HTTP response headers including those described in the **Response Headers** section of the **Request and Response Elements** topic.

Response Body

The response body for a successful request does not contain a response element.

The response body for an unsuccessful request may contain an error element that provides additional information. For a list of common error messages, please refer to the **Status Codes and Error Messages** topic.

Sample Request and Response

A sample request is provided below.

```
DELETE
https://api.edgecast.com/v2/mcc/customers/0001/httpstreaming/dcp/streamkeys/193950
HTTP/1.1

Authorization: TOK:12345678-1234-1234-1234-1234567890ab

Host: api.edgecast.com
```

A sample response is provided below.

```
HTTP/1.1 200 OK

Cache-Control: private

Date: Mon, 10 Jan 2011 12:00:00 GMT
```

Get All Instances

Retrieves a listing of all instances and their configuration.

Request

A request to retrieve instances is described below. When submitting this request, you will need to define the following variable:

- **AccountNumber:** Replace this variable with your CDN account number. This number can be found in the upper-right hand corner of the MCC.

HTTP Method	Request URI
GET	https://api.edgecast.com/v2/mcc/customers/*AccountNumber*/httpstreaming/dcp/live

Request Headers

The response for this endpoint only includes standard HTTP request headers including those described in the **Request Headers** section of the **Request and Response Elements** topic.

Request Body

Request body parameters are not required by this endpoint.

Response

The response to the above request includes an HTTP status code, response headers, and a response body.

Status Code

A status code indicates whether the request was successfully performed. A list of common status codes is provided in the **Status Codes and Error Messages** topic.

Response Headers

The response for this endpoint only returns standard HTTP response headers including those described in the **Response Headers** section of the **Request and Response Elements** topic.

Response Body

The response body for a successful request contains the following response elements:

Name	Data Type	Description
DvrDuration	Integer	Determines the length, in minutes, of the DVR window. The length of this DVR window may be set from 5 to 180 minutes (i.e., 3 hours). **Note:** If a DVR window was not specified during instance creation/modification, then this parameter will report a default duration of 1 minute.
Encrypted	Boolean	Indicates whether the live streams generated for this instance will be secured with encrypted HLS.
EncryptedKeyRotation	Integer	Indicates the interval, in seconds, at which the encryption key generated for the live event will be rotated. **Note:** Encryption key rotation may only take place at the start of a new segment. Therefore, the live event's segment size factors into when the encryption key will be rotated. **Note:** A null value indicates that encrypted key rotation has been disabled.
HlsPlaybackUrl	String	Indicates the instance's HLS playback URL. Syntax: http:\/\/wpc.*xxxx*.edgecastcdn.net\/24*xxxx*\/*InstanceName*\/<streamName>.m3u8
Id	Integer	Indicates the unique system-defined ID assigned to the instance.
InstanceName	String	Identifies the instance by its name.
MpegDashPlaybackUrl	String	Indicates the instance's MPEG-DASH playback URL. Syntax: http:\/\/wpc.*xxxx*.edgecastcdn.net\/24*xxxx*\/*InstanceName*\/<streamName>.mpd
PublishUrl	String	Indicates the publishing point's relative path followed by syntax information on how to authorize a stream. Syntax: \/20*xxxx*\/*InstanceName*\/<streamName>?<Live Authentication Key>
SegmentSize	Integer	Indicates the size, in seconds, of the segments that will be generated for this instance.

Name	Data Type	Description
SsaEnabled	Boolean	Indicates whether Server-Side Archiving (SSA) has been enabled on this instance.
		Note: SSA requires activation on your account. Please contact your CDN account manager to activate it.

Errors

The response body for an unsuccessful request may contain an error element that provides additional information. For a list of common error messages, please refer to the **Status Codes and Error Messages** topic.

Sample Request and Response

A sample JSON request is provided below.

```
GET https://api.edgecast.com/v2/mcc/customers/0001/httpstreaming/dcp/live HTTP/1.1

Authorization: TOK:12345678-1234-1234-1234-1234567890ab

Accept: application/json

Host: api.edgecast.com
```

A sample JSON response is provided below.

```
HTTP/1.1 200 OK

Cache-Control: private

Content-Type: application/json; charset=utf-8

Date: Thu, 14 Apr 2016 12:00:00 GMT

Content-Length: 944

[{

        "DvrDuration": null,

        "Encrypted": false,

        "EncryptedKeyRotation": null,

        "HlsPlaybackUrl":
"http:\/\/wpc.0001.edgecastcdn.net\/240001\/myfirstinstance\/<streamName>.m3u
8",

        "Id": 752,

        "InstanceName": "myfirstinstance",

        "MpegDashPlaybackUrl":
"http:\/\/wpc.0001.edgecastcdn.net\/240001\/myfirstinstance\/<streamName>.mpd
",

        "PublishUrl": "\/200001\/myfirstinstance\/<streamName>?<Live
Authentication Key>",

        "SegmentSize": 10,
```

```
            "SsaEnabled": false
    }, {

            "DvrDuration": 20,

            "Encrypted": true,

            "EncryptedKeyRotation": null,

            "HlsPlaybackUrl":
    "http:\/\/wpc.0001.edgecastcdn.net\/240001\/mysecondinstance\/<streamName>.m3
    u8",

            "Id": 753,

            "InstanceName": "mysecondinstance",

            "MpegDashPlaybackUrl":
    "http:\/\/wpc.0001.edgecastcdn.net\/240001\/mysecondinstance\/<streamName>.mp
    d",

            "PublishUrl": "\/200001\/mysecondinstance\/<streamName>?<Live
    Authentication Key>",

            "SegmentSize": 10,

            "SsaEnabled": false

    }
]
```

Get Encrypted HLS Directories

Retrieves a list of all encrypted HLS directories. This list may be filtered by ID or by origin type.

Request

A request to retrieve encrypted HLS directories is described below. When submitting this request, you may need to define the following variables:

- **AccountNumber:** Replace this variable with your CDN account number. This number can be found in the upper-right hand corner of the MCC.

- **EHLSDirectoryID:** Replace this variable with the system-defined ID for the desired encrypted HLS directory. The response will be filtered to only return data for the specified encrypted HLS directory.

  Note: The id query string parameter should only be specified if you would like to filter the response to a specific encrypted HLS directory. Return all encrypted HLS directories by excluding query string parameters from the request.

- **OriginTypeID:** Replace this variable with one of the following values:

  - **1:** Filters the response to only include encrypted HLS directories that have been defined for CDN storage.

- **2:** Filters the response to only include encrypted HLS directories that have been defined for customer origin configurations.

> **Note:** The originid query string parameter should only be specified if you would like to filter the response by origin type. Return all encrypted HLS directories by excluding query string parameters from the request.

HTTP Method	Request URI
GET	Retrieve All Encrypted HLS Directories: https://api.edgecast.com/v2/mcc/customers/*AccountNumber*/httpstreaming/dcp/vod/ehlsdirectory Retrieve a Filtered List of Encrypted HLS Directories: https://api.edgecast.com/v2/mcc/customers/*AccountNumber*/httpstreaming/dcp/vod/ehlsdirectory?id=*EHLSDirectoryID*&originid=*OriginTypeID*

Request Headers

The response for this endpoint only includes standard HTTP request headers including those described in the **Request Headers** section of the **Request and Response Elements** topic.

Request Body

Request body parameters are not required by this endpoint.

Response

The response to the above request includes an HTTP status code, response headers, and a response body.

Status Code

A status code indicates whether the request was successfully performed. A list of common status codes is provided in the **Status Codes and Error Messages** topic.

Response Headers

The response for this endpoint only returns standard HTTP response headers including those described in the **Response Headers** section of the **Request and Response Elements** topic.

Response Body

The response body for a successful request contains the following response parameters for each encrypted HLS directory returned by this endpoint:

Name	Data Type	Description
CustomerId	Integer	**Important:** Please ignore this parameter. It is slated to be removed from the response.

Name	Data Type	Description
Id	Integer	Identifies an encrypted HLS directory configuration by its system-defined ID.
OriginName	String	Identifies the type of origin server to which encryption will be applied. Valid values are: • **CDN:** Represents CDN storage. • **Customer:** Represents customer origin configurations.
OriginTypeId	Integer	Identifies the type of origin server to which encryption will be applied. Valid values are: • **1:** Represents CDN storage. • **2:** Represents customer origin configurations.
Path	String	Identifies the directory to which encryption will be applied for on-demand playback via Dynamic Cloud Packaging. **Note:** Encryption will only be applied to playback requests for content stored in this directory and that are directed at the type of origin server identified by the OriginTypeID element.

Errors

The response body for an unsuccessful request may contain an error element that provides additional information. For a list of common error messages, please refer to the **Status Codes and Error Messages** topic.

Sample Request and Response

A sample JSON request is provided below.

```
GET
https://api.edgecast.com/v2/mcc/customers/0001/httpstreaming/dcp/vod/ehlsdirectory
HTTP/1.1

Authorization: TOK:12345678-1234-1234-1234-1234567890ab

Accept: application/json

Host: api.edgecast.com
```

A sample JSON response is provided below.

```
HTTP/1.1 200 OK
Cache-Control: private
Content-Type: application/json; charset=utf-8
Date: Thu, 14 Apr 2016 12:00:00 GMT
Content-Length: 105

[{
            "Id": 6375,
            "OriginName": "CDN",
            "OriginTypeId": 1,
            "Path": "\/videos"
    }
]
```

Get Global Key

Retrieves the global key that provides authorization for the Dynamic Cloud Packaging streaming service.

Request

A request to retrieve the global key is described below. When submitting this request, you will need to define the following variable:

- **AccountNumber:** Replace this variable with your CDN account number. This number can be found in the upper-right hand corner of the MCC.

HTTP Method	Request URI
GET	https://api.edgecast.com/v2/mcc/customers/*AccountNumber*/httpstreaming/dcp/globalkey

Request Headers
The response for this endpoint only includes standard HTTP request headers including those described in the **Request Headers** section of the **Request and Response Elements** topic.

Request Body
Request body parameters are not required by this endpoint.

Response

The response to the above request includes an HTTP status code, response headers, and a response body.

Status Code

A status code indicates whether the request was successfully performed. A list of common status codes is provided in the **Status Codes and Error Messages** topic.

Response Headers

The response for this endpoint only returns standard HTTP response headers including those described in the **Response Headers** section of the **Request and Response Elements** topic.

Response Body

The response body for a successful request contains the following response element:

Name	Data Type	Description
Key	String	Reports the value assigned to Dynamic Cloud Packaging's global live authentication key.

Errors

The response body for an unsuccessful request may contain an error element that provides additional information. For a list of common error messages, please refer to the **Status Codes and Error Messages** topic.

Sample Request and Response

A sample JSON request is provided below.

```
GET https://api.edgecast.com/v2/mcc/customers/0001/httpstreaming/dcp/globalkey
HTTP/1.1

Authorization: TOK:12345678-1234-1234-1234-1234567890ab

Accept: application/json

Host: api.edgecast.com
```

A sample JSON response is provided below.

```
HTTP/1.1 200 OK

Cache-Control: private

Content-Type: application/json; charset=utf-8

Date: Thu, 14 Apr 2016 12:00:00 GMT

Content-Length: 34

{
        "Key": "123457890abcdefghi"
}
```

Get Stream Keys

Retrieves stream keys that provide authorization for the Dynamic Cloud Packaging streaming service. The response may be filtered to only return a single stream key.

Request

A request to retrieve stream keys is described below. When submitting this request, you may need to define the following variables:

- **AccountNumber:** Replace this variable with your CDN account number. This number can be found in the upper-right hand corner of the MCC.

- **StreamID:** Replace this variable with the system-defined ID associated with the desired stream key.

    Note: The id query string parameter should only be specified to filter the response to return a single stream key.

HTTP Method	Request URI
GET	Retrieve all stream keys: https://api.edgecast.com/v2/mcc/customers/*AccountNumber*/httpstreaming/dcp/streamkeys Retrieve a specific stream key: https://api.edgecast.com/v2/mcc/customers/*AccountNumber*/httpstreaming/dcp/streamkeys?id=*StreamID*

Request Headers
The response for this endpoint only includes standard HTTP request headers including those described in the **Request Headers** section of the **Request and Response Elements** topic.

Request Body
Request body parameters are not required by this endpoint.

Response

The response to the above request includes an HTTP status code, response headers, and a response body.

Status Code
A status code indicates whether the request was successfully performed. A list of common status codes is provided in the **Status Codes and Error Messages** topic.

Response Headers
The response for this endpoint only returns standard HTTP response headers including those described in the **Response Headers** section of the **Request and Response Elements** topic.

Response Body

The response body for a successful request contains the following response parameters for each stream key returned by this endpoint:

Name	Data Type	Description
DirPath	String	Identifies a stream by its relative path. The starting point for this relative path is indicated in blue font below. rtmp://fso.oxr.0001.edgecastcdn.net/200001/myinstance/mystream **Note:** The stream identified by this parameter will be authorized by the value defined in the Key parameter.
Id	Integer	Reports the unique identifier assigned to a stream key configuration.
Key	String	Identifies the live authentication key that may be used to authenticate streams published to the relative path associated with this stream key configuration.

Errors

The response body for an unsuccessful request may contain an error element that provides additional information. For a list of common error messages, please refer to the **Status Codes and Error Messages** topic.

Sample Request and Response

A sample JSON request is provided below.

```
GET https://api.edgecast.com/v2/mcc/customers/0001/httpstreaming/dcp/streamkeys
HTTP/1.1

Authorization: TOK:12345678-1234-1234-1234-1234567890ab

Accept: application/json

Host: api.edgecast.com
```

A sample JSON response is provided below.

```
HTTP/1.1 200 OK
Cache-Control: private
Content-Type: application/json; charset=utf-8
Date: Thu, 14 Apr 2016 12:00:00 GMT
Content-Length: 294

[{
            "DirPath": "myinstance\/mystream",
            "Id": 192836,
            "Key": "123457890abcdefghi"
    }, {
            "DirPath": "myinstance\/salesconference",
            "Id": 192837,
            "Key": "223457890abcdefghi"
    }, {
            "DirPath": "myinstance\/marketingevent",
            "Id": 192873,
            "Key": "323457890abcdefghi"
    }
]
```

Update Global Key

Updates the value assigned to the global key that provides authorization for the Dynamic Cloud Packaging streaming service.

Request

A request to update the global key is described below. When submitting this request, you will need to define the following variable:

- **AccountNumber:** Replace this variable with your CDN account number. This number can be found in the upper-right hand corner of the MCC.

HTTP Method	Request URI
PUT	https://api.edgecast.com/v2/mcc/customers/*AccountNumber*/httpstreaming /dcp/globalkey

Request Headers

The response for this endpoint only includes standard HTTP request headers including those described in the **Request Headers** section of the **Request and Response Elements** topic.

Request Body

The request parameters for this endpoint are described below.

Name	Data Type	Description
Key	String	Identifies the global live authentication key that may be used to authenticate any stream that is published to a location that has not been secured by a stream key. This key must be 256 alphanumeric characters or less.

Response

The response to the above request includes an HTTP status code, response headers, and a response body.

Status Code

A status code indicates whether the request was successfully performed. A list of common status codes is provided in the **Status Codes and Error Messages** topic.

Response Headers

The response for this endpoint only returns standard HTTP response headers including those described in the **Response Headers** section of the **Request and Response Elements** topic.

Response Body

The response body for a successful request does not contain a response parameter.

The response body for an unsuccessful request may contain an error element that provides additional information. For a list of common error messages, please refer to the **Status Codes and Error Messages** topic.

Sample Request and Response

A sample JSON request is provided below.

```
PUT https://api.edgecast.com/v2/mcc/customers/0001/httpstreaming/dcp/globalkey

HTTP/1.1

Authorization: TOK:12345678-1234-1234-1234-1234567890ab

Accept: application/json

Host: api.edgecast.com

Content-Length: 25


{

        "Key" : "abcdef123456"

}
```

A sample JSON response is provided below.

```
HTTP/1.1 200 OK

Cache-Control: private

Content-Type: application/xml; charset=utf-8

Date: Thu, 14 Apr 2016 12:00:00 GMT
```

Update Instance

Updates an instance's configuration.

Note: An instance's name cannot be modified.

Request

A request to update an instance is described below. When submitting this request, you will need to define the following variables:

- **AccountNumber:** Replace this variable with your CDN account number. This number can be found in the upper-right hand corner of the MCC.

- **InstanceID:** Replace this variable with the system-defined ID of the desired instance.

  Note: Retrieve a list of instances and their system-defined IDs through the Get All Instances endpoint.

HTTP Method	Request URI
PUT	https://api.edgecast.com/v2/mcc/customers/*AccountNumber*/httpstreaming/dcp/live/*InstanceID*

Request Headers

The response for this endpoint only includes standard HTTP request headers including those described in the **Request Headers** section of the **Request and Response Elements** topic.

Request Body

Optional and required request parameters for this endpoint are described below.

Name	Data Type	Description
EncryptedKeyRotation	Integer	**Note:** The Encrypted Key Rotation feature requires activation on your account. Please contact your CDN account manager to activate it. **Note:** A prerequisite for this capability is the enablement of the Encrypted HLS feature on this instance through the Encrypted parameter. Determines whether the encryption key generated for a live event will be rotated at regular intervals. Valid states: • **Missing/Null:** Omit this parameter or set it to a null value to disable encrypted key rotation. • **Seconds:** Set this parameter to the desired time interval. This time interval must be: 　▪ Greater than or equal to 10 seconds and less than or equal to 1440 seconds. 　▪ Specified in multiples of 5 (e.g., 10, 15, 20, etc.) seconds. **Important:** The Server-Side Archiving feature is incompatible with this feature. Do not enable both features within a single instance. **Note:** Encryption key rotation may only take place at the start of a new segment. Therefore, the live event's segment size factors into when the encryption key will be rotated. **Default Value:** null

Name	Data Type	Description
SsaEnabled	Boolean	**Note:** SSA requires activation on your account. Please contact your CDN account manager to activate it.
		Determines whether Server-Side Archiving (SSA) will be enabled for all live streams generated from this instance.
		Important: The Server-Side Archiving feature is incompatible with the Encrypted HLS feature. Do not enable both features within a single instance.
		Default Value: False
Encrypted	Boolean	Determines whether the live streams generated for this instance will be secured with encrypted HLS.
		Valid values are:
		• **True:** Enabled
		• **False:** Disabled (default)
		Important: The Server-Side Archiving feature is incompatible with the Encrypted HLS feature. Do not enable both features within a single instance.
		Default Value: False
DvrDuration	Integer	Determines the length, in minutes, of the DVR window. The length of this DVR window may be set from 5 to 180 minutes (i.e., 3 hours).
		Important: If a DVR window is not defined during instance creation, then the instance will be assigned a default DVR window of 1 minute. If you would like to retain this default DVR window duration, then you should omit the DvrDuration parameter when requesting this endpoint.
		Default Value: 1 minute
SegmentSize	Integer	Determines the size, in seconds, of the segments that will be generated for this instance. Segment size may be set from 1 to 20 seconds.

Response

The response to the above request includes an HTTP status code, response headers, and a response body.

Status Code

A status code indicates whether the request was successfully performed. A list of common status codes is provided in the **Status Codes and Error Messages** topic.

Response Headers

The response for this endpoint only returns standard HTTP response headers including those described in the **Response Headers** section of the **Request and Response Elements** topic.

Response Body

The response body for a successful request contains the following response elements:

Name	Data Type	Description
DvrDuration	Integer	Indicates the length, in minutes, of the DVR window. The length of this DVR window may be set from 5 to 180 minutes (i.e., 3 hours). **Note:** If a DVR window was not specified in the request, then this parameter will report a default duration of 1 minute.
Encrypted	Boolean	Indicates whether the live streams generated for this instance will be secured with encrypted HLS.
EncryptedKeyRotation	Integer	Indicates the interval, in seconds, at which the encryption key generated for the live event will be rotated. **Note:** Encryption key rotation may only take place at the start of a new segment. Therefore, the live event's segment size factors into when the encryption key will be rotated. **Note:** A null value indicates that encrypted key rotation has been disabled.
HlsPlaybackUrl	String	Indicates the instance's HLS playback URL. Syntax: http:\/\/wpc.*xxxx*.edgecastcdn.net\/24*xxxx*\/*InstanceName*\/<streamName>.m3u8
Id	Integer	Indicates the unique system-defined ID assigned to the instance.
InstanceName	String	Identifies the instance by its name.
MpegDashPlaybackUrl	String	Indicates the instance's MPEG-DASH playback URL. Syntax: http:\/\/wpc.*xxxx*.edgecastcdn.net\/24*xxxx*\/*InstanceName*\/<streamName>.mpd

Name	Data Type	Description
PublishUrl	String	Indicates the publishing point's relative path followed by syntax information on how to authorize a stream. Syntax: \/20*xxxx*\/*InstanceName*\/<streamName>?<Live Authentication Key>
SegmentSize	Integer	Indicates the size, in seconds, of the segments that will be generated for this instance.
SsaEnabled	Boolean	Indicates whether Server-Side Archiving (SSA) has been enabled on this instance. **Note:** SSA requires activation on your account. Please contact your CDN account manager to activate it.

Errors

The response body for an unsuccessful request may contain an error element that provides additional information. For a list of common error messages, please refer to the **Status Codes and Error Messages** topic.

Sample Request and Response

A sample JSON request is provided below.

```
PUT https://api.edgecast.com/v2/mcc/customers/0001/httpstreaming/dcp/live/750
HTTP/1.1

Authorization: TOK:12345678-1234-1234-1234-1234567890ab

Accept: application/json

Host: api.edgecast.com

Content-Length: 45


{

        "DvrDuration": 15,

        "SegmentSize": 10

}
```

A sample JSON response is provided below.

```
HTTP/1.1 200 OK

Cache-Control: private

Content-Type: application/xml; charset=utf-8

Date: Thu, 14 Apr 2016 12:00:00 GMT

Content-Length: 431

{

        "DvrDuration": 25,

        "Encrypted": false,

        "EncryptedKeyRotation": null,

        "HlsPlaybackUrl":
        "http:\/\/wpc.0001.edgecastcdn.net\/240001\/myinstance\/<streamName>.m3u8",

        "Id": 750,

        "InstanceName": "myinstance",

        "MpegDashPlaybackUrl":
        "http:\/\/wpc.0001.edgecastcdn.net\/240001\/myinstance\/<streamName>.mpd",

        "PublishUrl": "\/200001\/myinstance\/<streamName>?<Live Authentication Key>",

        "SegmentSize": 10,

        "SsaEnabled": false

}
```

Update Stream Key

Updates the properties of an existing stream key that provides authorization for the Dynamic Cloud Packaging streaming service.

Request

A request to update a stream key is described below. When submitting this request, you will need to define the following variables:

- **AccountNumber:** Replace this variable with your CDN account number. This number can be found in the upper-right hand corner of the MCC.

- **KeyID:** Replace this variable with the system-defined ID assigned to the stream key that you would like to update.

  Note: Use the Get Stream Keys endpoint to retrieve a listing of stream keys and their IDs.

HTTP Method	Request URI
PUT	https://api.edgecast.com/v2/mcc/customers/*AccountNumber*/httpstreaming/dcp/streamkeys/*KeyID*

Request Headers

The response for this endpoint only includes standard HTTP request headers including those described in the **Request Headers** section of the **Request and Response Elements** topic.

Request Body

The request parameters for this endpoint are described below.

Name	Data Type	Description
DirPath	String	Identifies a stream by its relative path. The starting point for this relative path is indicated in blue font below.
		rtmp://fso.oxr.0001.edgecastcdn.net/200001/myinstance/mystream
		Note: The stream identified by this parameter will be authorized by the value defined in the Key parameter.
		This stream path must consist of:
		• Alphanumeric characters
		• A single forward slash that delimits the instance name from the stream name.
		Optionally, an asterisk (*), which represents one or more characters, may be appended to the stream name.
		Note: Do not specify a pattern after an asterisk as it will be ignored.
Key	String	Identifies the live authentication key that may be used to authenticate streams published to the path specified by this stream key configuration. This key must be 256 alphanumeric characters or less.

Response

The response to the above request includes an HTTP status code, response headers, and a response body.

Status Code

A status code indicates whether the request was successfully performed. A list of common status codes is provided in the **Status Codes and Error Messages** topic.

Response Headers

The response for this endpoint only returns standard HTTP response headers including those described in the **Response Headers** section of the **Request and Response Elements** topic.

Response Body

The response body for a successful request does not contain a response parameter.

Errors

The response body for an unsuccessful request may contain an error element that provides additional information. For a list of common error messages, please refer to the **Status Codes and Error Messages** topic.

Sample Request and Response

A sample JSON request is provided below.

```
PUT
https://api.edgecast.com/v2/mcc/customers/0001/httpstreaming/dcp/streamkeys/193950

HTTP/1.1

Authorization: TOK:12345678-1234-1234-1234-1234567890ab

Accept: application/json

Host: api.edgecast.com

Content-Length: 45


{

        "DirPath" : "myinstance\/secure",

        "Key" : "123456",

}
```

A sample JSON response is provided below.

```
HTTP/1.1 200 OK

Cache-Control: private

Content-Type: application/xml; charset=utf-8

Date: Thu, 14 Apr 2016 12:00:00 GMT
```

Log Settings

The endpoints covered in this section allow you to find out and update your log storage and format configuration.

Get Log Format Settings

Provides information describing your current log format configuration for all HTTP platforms. The settings returned by this endpoint are:

- Base log file format

- Date/time format

- Custom field

- URL format (i.e., content access point inclusion)

Request

A request to retrieve your current log format configuration is described below. When submitting this request, you will need to define the following term:

- **AccountNumber:** This term should be replaced by your CDN account number. This number can be found in the upper-right hand corner of the MCC.

HTTP Method	Request URI
GET	https://api.edgecast.com/v2/mcc/customers/*AccountNumber*/logformat

Request Headers
This endpoint only takes advantage of the common request headers described in the **Request Headers** section of the **Request and Response Elements** topic.

Request Body
Request body parameters are not required by this endpoint.

Response

The response to the above request includes an HTTP status code, response headers, and a response body.

Status Code
A status code indicates whether the request was successfully performed. A list of common status codes is provided in the **Status Codes and Error Messages** topic.

Response Headers

The response for this endpoint only returns standard HTTP response headers including those described in the **Response Headers** section of the **Request and Response Elements** topic.

Response Body

The response body for a successful request contains the following response elements:

Name	Description
AN	A string that indicates the customer account number whose configuration will be returned. This customer account number will always match the one specified in the request URI.
BaseFormat	An integer that indicates the current base log file format. Valid values for this response element are: • **1:** Indicates that log data will be stored using a default log file format. This format is similar to an extended W3C log file format. • **2:** Indicates that log data will be stored using the combined log file format. This format is the default log file format used by Apache web servers.
CustomFieldHeader	A string that indicates the name of the custom log field header. This response element will always be blank when the **Add the custom file to the log file** option is cleared or the ShowCustomField response element is set to 0.
DateTimeFormat	An integer that indicates the format that will be used to report the date/time field. Valid values for this response element are: • **0:** Indicates that the date/time field will be reported using Unix time (a.k.a. POSIX time or Unix epoch). • **1:** Indicates that the date/time field will be reported using a custom format. The format that will be used depends on the base log file format. An example of how the date/time field will be formatted is provided for each type of log file format. ▪ **Default format:** 2012-12-10 11:00:00 ▪ **Combined format:** 10/Dec/2012:11:00:00 +0000

Name	Description
RemoveContentAccessPoint	An integer that indicates whether the content access point will be included in the URL reported by the cs-uri-stem field. Valid values for this response element are: • **0:** Indicates that the content access point will be included in the URL reported by the cs-uri-stem field. • **1:** Indicates that the content access point will be excluded from the URL reported by the cs-uri-stem field.
ShowCustomField	An integer that indicates whether a custom log field will be included in the raw log file. The name for this custom log field is defined by the CustomFieldHeader response element. Valid values for this response element are: • **0:** Indicates that a custom log field will be excluded from your raw log files. • **1:** Indicates that a custom log field will be included in your raw log files.

Errors

The response body for an unsuccessful request may contain an error element that provides additional information. For a list of common error messages, please refer to the **Status Codes and Error Messages** topic.

Sample Request and Response

A sample JSON request is provided below.

```
GET https://api.edgecast.com/v2/mcc/customers/0001/logformat HTTP/1.1

Authorization: TOK:12345678-1234-1234-1234-1234567890ab

Accept: application/json

Host: api.edgecast.com
```

A sample JSON response is provided below.

```
HTTP/1.1 200 OK

Cache-Control: private

Content-Type: application/json; charset=utf-8

Date: Thu, 14 Apr 2016 12:00:00 GMT

Content-Length: 158
```

```
{
        "AN" : "0001",
        "BaseFormat" : 1,
        "CustomFieldHeader" : "x-ec_custom-1",
        "DateTimeFormat" : 0,
        "RemoveContentAccessPoint" : 0,
        "ShowCustomField" : 1
}
```

Get Log Storage Settings

Provides information describing your current log storage configuration for all platforms. The settings returned by this endpoint are:

- Log storage overall status
- Log storage status by platform
- Log retention period

Request

A request to retrieve your current log storage configuration is described below. When submitting this request, you will need to define the following term:

- **AccountNumber:** This term should be replaced by your CDN account number. This number can be found in the upper-right hand corner of the MCC.

HTTP Method	Request URI
GET	https://api.edgecast.com/v2/mcc/customers/*AccountNumber*/logstorage

Request Headers

This endpoint only takes advantage of the common request headers described in the **Request Headers** section of the **Request and Response Elements** topic.

Request Body

Request body parameters are not required by this endpoint.

Response

The response to the above request includes an HTTP status code, response headers, and a response body.

Status Code

A status code indicates whether the request was successfully performed. A list of common status codes is provided in the **Status Codes and Error Messages** topic.

Response Headers

The response for this endpoint only returns standard HTTP response headers including those described in the **Response Headers** section of the **Request and Response Elements** topic.

Response Body

The response body for a successful request contains the following response elements:

Name	Description
AN	A string that indicates the customer account number whose configuration will be returned. This customer account number will always match the one specified in the request URI.
DaysToKeep	An integer that indicates the length of time that the log file will be kept in CDN storage. Valid values for this response element are: • **-1:** Indicates that log files will be kept in CDN storage until they are manually deleted. • **0:** Indicates that log storage has been disabled. • **1**, **5**, **10**, **15**, **30**, **45**, or **60:** Indicates that log files will be kept in CDN storage for the specified number of days. Log files that exceed this retention schedule will be deleted.
IsEnabled	Indicates whether log storage archival is enabled. Valid values for this response element are: • **0:** Indicates that log files will not be archived to CDN storage. • **1:** Indicates that log files can be archived to CDN storage. Whether log files will be archived is determined on a per platform basis as defined by the MediaTypeStatus response element.
MediaTypeStatuses	Lists the log file archival configuration for each platform.
IsEnabled	An integer that indicates whether log files will be archived for a particular platform. Valid values for this response element are: • **0:** Indicates that log files will not be archived to CDN storage for the platform indicated by the corresponding MediaTypeId response element. • **1:** Indicates that log file archival is allowed for the platform indicated by the corresponding MediaTypeId response element. The main IsEnabled response element (see above) determines whether log files will actually be archived.
MediaTypeId	An integer that identifies the platform whose log file archival status was reported by the IsEnabled response element. Valid values for this response element are: • **3:** HTTP Large • **8:** HTTP Small • **14:** Application Delivery Network (ADN)

Errors

The response body for an unsuccessful request may contain an error element that provides additional information. For a list of common error messages, please refer to the **Status Codes and Error Messages** topic.

Sample Request and Response

A sample JSON request is provided below.

```
GET https://api.edgecast.com/v2/mcc/customers/0001/logstorage HTTP/1.1
Authorization: TOK:12345678-1234-1234-1234-1234567890ab
Accept: application/json
Host: api.edgecast.com
```

A sample JSON response is provided below.

```
HTTP/1.1 200 OK
Cache-Control: private
Content-Type: application/json; charset=utf-8
Date: Thu, 14 Apr 2016 12:00:00 GMT
Content-Length: 277
{
        "AN" : "0001",
        "DaysToKeep" : -1,
        "IsEnabled" : 1,
        "MediaTypeStatuses" : [{
                        "IsEnabled" : 1,
                        "MediaTypeId" : 3
                }, {
                        "IsEnabled" : 1,
                        "MediaTypeId" : 8
                }, {
                        "IsEnabled" : 1,
                        "MediaTypeId" : 1
                }, {
                        "IsEnabled" : 0,
                        "MediaTypeId" : 14
                }
        ]
}
```

Update Log Format Settings

Defines the log format for all HTTP platforms. The settings defined by this endpoint are:

- Base log file format

- Date/time format

- Custom field

- URL format (i.e., content access point inclusion)

Request

A request to define your log format configuration is described below. When submitting this request, you will need to define the following term:

- **AccountNumber:** This term should be replaced by your CDN account number. This number can be found in the upper-right hand corner of the MCC.

HTTP Method	Request URI
PUT	https://api.edgecast.com/v2/mcc/customers/*AccountNumber*/logformat

Request Headers

This endpoint only takes advantage of the common request headers described in the **Request Headers** section of the **Request and Response Elements** topic.

Request Body

Optional parameters are described below.

Name	Description
BaseFormat	An integer that determines the base log file format. Valid values for this parameter are: - **1:** Determines that log data will be stored using a default log file format. This format is similar to an extended W3C log file format. - **2:** Determines that log data will be stored using the combined log file format. This format is the default log file format used by Apache web servers.

Name	Description
CustomFieldHeader	A string that determines the name of the custom log field header. The ShowCustomField parameter affects the behavior of this parameter. Possible ShowCustomField values are listed below. • **0:** This parameter will be set to an empty string, regardless of whether a value has been defined for it. • **1:** A value must be specified for this parameter.
DateTimeFormat	An integer that determines the format that will be used to report the date/time field. Valid values for this parameter are: • **0:** Determines that the date/time field will be reported using Unix time (a.k.a. POSIX time or Unix epoch). • **1:** Determines that the date/time field will be reported using a custom format. The format that will be used depends on the base log file format. An example of how the date/time field will be formatted is provided for each type of log file format. ▪ **Default format:** 2012-12-10 11:00:00 ▪ **Combined format:** 10/Dec/2012:11:00:00 +0000
RemoveContentAccessPoint	An integer that determines whether the content access point will be included in the URL reported by the cs-uri-stem field. Valid values for this parameter are: • **0:** Determines that the content access point will be included in the URL reported by the cs-uri-stem field. • **1:** Determines that the content access point will be excluded from the URL reported by the cs-uri-stem field.
ShowCustomField	An integer that determines whether a custom log field will be included in the raw log file. The name for this custom log field is defined by the CustomFieldHeader response element. Valid values for this parameter are: • **0:** Determines that the custom log field will be excluded from raw log files and the CustomFieldHeader parameter will be set to blank. • **1:** Determines that the custom log field will be included in raw log files. This type of configuration requires that a value be specified for the CustomFieldHeader parameter.

Response

The response to the above request includes an HTTP status code, response headers, and a response body.

Status Code

A status code indicates whether the request was successfully performed. A list of common status codes is provided in the **Status Codes and Error Messages** topic.

Response Headers

The response for this endpoint only returns standard HTTP response headers including those described in the **Response Headers** section of the **Request and Response Elements** topic.

Response Body

The response body for a successful request does not contain a response element.

Errors

The response body for an unsuccessful request may contain an error element that provides additional information. For a list of common error messages, please refer to the **Status Codes and Error Messages** topic.

Sample Request and Response

A sample JSON request is provided below.

```
PUT https://api.edgecast.com/v2/mcc/customers/0001/logformat HTTP/1.1

Authorization: TOK:12345678-1234-1234-1234-1234567890ab

Accept: application/json

Content-Type: application/json

Host: api.edgecast.com

Content-Length: 142


{

        "BaseFormat" : 1,

        "CustomFieldHeader" : "x-ec_custom-1",

        "DateTimeFormat" : 0,

        "RemoveContentAccessPoint" : 0,

        "ShowCustomField" : 1

}
```

A sample JSON response is provided below.

```
HTTP/1.1 200 OK

Cache-Control: private

Content-Type: application/json; charset=utf-8

Date: Thu, 14 Apr 2016 12:00:00 GMT
```

Update Log Storage Settings

Defines your log storage configuration for each available platform. The settings defined by this endpoint are:

- Log storage overall status

- Log storage status by platform

- Log retention period

Note: This endpoint can only be performed if the logging capability has been activated on the desired platform. Attempting to configure log storage settings on a platform for which it has not been activated will generate a 400 Bad Request. Please contact your CDN account manager to activate logging.

Request

A request to set your log storage configuration is described below. When submitting this request, you will need to define the following term:

- **AccountNumber:** This term should be replaced by your CDN account number. This number can be found in the upper-right hand corner of the MCC.

HTTP Method	Request URI
PUT	https://api.edgecast.com/v2/mcc/customers/*AccountNumber*/logstorage

Request Headers

This endpoint only takes advantage of the common request headers described in the **Request Headers** section of the **Request and Response Elements** topic.

Request Body

Optional parameters are described below.

Name	Description
DaysToKeep	An integer that determines the length of time that the log file will be kept in CDN storage. Valid values for this parameter are -1, 1, 5, 10, 15, 30, 45, or 60. • **-1:** Determines that log files will be kept in CDN storage until they are manually deleted. • **#:** Determines that log files will be kept in CDN storage for the specified number of days (i.e., 1, 5, 10, 15, 30, 45, or 60). Once a log file has been stored for the specified number of days, it will be deleted.
IsEnabled	Determines whether log storage archival is enabled. Valid values for this parameter are: • **0:** Determines that log files will not be archived to CDN storage. It will also set the DaysToKeep parameter to "0," regardless of the value assigned to it in the request body. • **1:** Determines that log files can be archived to CDN storage. Whether log files will be archived is determined on a per platform basis as defined by the MediaTypeStatus parameter.
MediaTypeStatuses	Defines the log file archival configuration for each platform. **Note:** Although the following platform-specific parameters (i.e., IsEnabled and MediaTypeId) are optional, they must be specified as a pair. An error will be returned when one parameter is specified without the other.
IsEnabled	An integer that determines whether log files will be archived for a particular platform. Valid values for this parameter are: • **0:** Log files for the platform indicated in the corresponding MediaTypeId parameter will not be archived. This is the default value for each specified MediaTypeId parameter. • **1:** Log files for the platform indicated in the corresponding MediaTypeId parameter can be archived. The main IsEnabled parameter (see above) determines whether log files will actually be archived.
MediaTypeId	An integer that identifies the platform for which log file archival will be enabled or disabled. Valid values for this parameter are: • **3:** HTTP Large • **8:** HTTP Small • **14:** Application Delivery Network (ADN)

Response

The response to the above request includes an HTTP status code, response headers, and a response body.

Status Code

A status code indicates whether the request was successfully performed. A list of common status codes is provided in the **Status Codes and Error Messages** topic.

Response Headers

The response for this endpoint only returns standard HTTP response headers including those described in the **Response Headers** section of the **Request and Response Elements** topic.

Response Body

The response body for a successful request does not contain a response element.

Errors

The response body for an unsuccessful request may contain an error element that provides additional information. For a list of common error messages, please refer to the **Status Codes and Error Messages** topic.

Sample Request and Response

A sample JSON request is provided below.

```
PUT https://api.edgecast.com/v2/mcc/customers/0001/logstorage HTTP/1.1
Authorization: TOK:12345678-1234-1234-1234-1234567890ab
Accept: application/json
Content-Type: application/json
Host: api.edgecast.com
Content-Length: 212


{
        "DaysToKeep" : -1,
        "IsEnabled" : 1,
        "MediaTypeStatuses" : [{
                    "IsEnabled" : 1,
                    "MediaTypeId" : 3
            }, {
                    "IsEnabled" : 1,
                    "MediaTypeId" : 8
            }, {
                    "IsEnabled" : 1,
```

```
                    "MediaTypeId" : 2
            }
        ]
}
```

A sample JSON response is provided below.

```
HTTP/1.1 200 OK
Cache-Control: private
Content-Type: application/json; charset=utf-8
Date: Thu, 14 Apr 2016 12:00:00 GMT
```

Route (DNS)

The endpoints covered in this section only apply to the Route (DNS) platform. Use these endpoints to add, update, retrieve, copy, and delete zones.

Add Primary Zone

Creates a primary zone. A new zone can contain any of the following items:

- Records

- Load balancing groups

- Failover groups

- Health check configurations

Request

A request to create a zone is described below.

HTTP Method	Request URI
POST	https://api.edgecast.com/v2/mcc/customers/*xxxx*/dns/routezone

Define the following terms when submitting the above request:

- **xxxx:** Replace this term with your CDN account number.

Request Headers

This endpoint only takes advantage of common request headers.

Note: This endpoint only supports JSON.

Request Body

The required request parameters for this endpoint are described below.

Name	Description
Comment	A string that assigns a comment to the zone.
DomainName	A string that defines a zone's name.
FailoverGroups	Define the zone's failover groups within this request parameter.
Group	Define a specific failover group within this request parameter.
[A|AAAA|CNAME]	The name of this request parameter should be set to the record type (i.e., A, AAAA, or CNAME) that will be associated with the group. **Key information:** • A failover group must contain exactly two records of the same type. • The supported configurations for a failover group are: ▪ A records only ▪ AAAA records only ▪ A and AAAA records ▪ CNAME records only
HealthCheck	Define a record's health check configuration within this request parameter.
CheckInterval	An integer that defines the number of seconds between health checks.
CheckTypeId	An integer that defines the type of health check by its system-defined ID. Use the Get Available Health Check Types endpoint to retrieve a list of health check types and their IDs.
ContentVerification	A string that defines the text that will be used to verify the success of the health check.
EmailNotificationAddress	A string that defines the e-mail address to which health check notifications will be sent.
FailedCheckThreshold	An integer that defines the number of consecutive times that the same result must be returned before a health check agent will indicate a change in status.

Name	Description
HTTPMethodId	An integer that defines an HTTP method by its system-defined ID. An HTTP method is only used by HTTP/HTTPs health checks.
	Use the Get Available HTTP Methods (Health Checks) endpoint to retrieve a list of HTTP methods and their IDs.
IPAddress	A string that defines the IP address (IPv4 or IPv6) to which TCP health checks will be directed.
IPVersion	An integer that defines an IP version by its system-defined ID. This IP version is only used by HTTP/HTTPs health checks.
	Use the Get Available IP Versions (Health Checks) endpoint to retrieve a list of IP versions and their IDs.
PortNumber	An integer that defines the port to which TCP health checks will be directed.
ReintegrationMethodId	An integer that defines the method through which an unhealthy server/domain will be integrated back into a group.
	Use the Get Available Health Check Reintegration Methods endpoint to retrieve a list of reintegration methods and their IDs.
Uri	A string that defines the URI to which HTTP/HTTPs health checks will be directed.
IsPrimary	A Boolean that defines whether the current record is the primary server/domain to which traffic will be directed.
Record	Define a record's properties within this request parameter.
Name	A string that defines the record's name.
Rdata	A string that defines the record's value.
TTL	An integer that defines the record's TTL.
GroupTypeId	An integer that should be set to "3."
Name	A string that defines the name of the failover group.
LoadBalancingGroups	Define the zone's load balancing groups within this request parameter.

Name	Description
Group	Define a specific load balancing group within this request parameter.
[A|AAAA|CNAME]	The name of this request parameter should be set to the record type (i.e., A, AAAA, or CNAME) that will be associated with the group. **Key information:** • A load balancing group must contain at least two records of the same type. • The supported configurations for a load balancing group are: ▪ A records only ▪ AAAA records only ▪ A and AAAA records ▪ CNAME records only
HealthCheck	Define a record's health check configuration within this request parameter.
CheckInterval	An integer that defines the number of seconds between health checks.
CheckTypeId	An integer that defines the type of health check by its system-defined ID. Use the Get Available Health Check Types endpoint to retrieve a list of health check types and their IDs.
ContentVerification	A string that defines the text that will be used to verify the success of the health check.
EmailNotificationAddress	A string that defines the e-mail address to which health check notifications will be sent.
FailedCheckThreshold	An integer that defines the number of consecutive times that the same result must be returned before a health check agent will indicate a change in status.
HTTPMethodId	An integer that defines an HTTP method by its system-defined ID. An HTTP method is only used by HTTP/HTTPs health checks. Use the Get Available HTTP Methods (Health Checks) endpoint to retrieve a list of HTTP methods and their IDs.

Name	Description
IPAddress	A string that defines the IP address (IPv4 or IPv6) to which TCP health checks will be directed.
IPVersion	An integer that defines an IP version by its system-defined ID. This IP version is only used by HTTP/HTTPs health checks. Use the Get Available IP Versions (Health Checks) endpoint to retrieve a list of IP versions and their IDs.
PortNumber	An integer that defines the port to which TCP health checks will be directed.
ReintegrationMethodId	An integer that defines the method through which an unhealthy server/domain will be integrated back into a group. Use the Get Available Health Check Reintegration Methods endpoint to retrieve a list of reintegration methods and their IDs.
Uri	A string that defines the URI to which HTTP/HTTPs health checks will be directed.
Record	Define a record's properties within this request parameter.
Name	A string that defines the record's name.
Rdata	A string that defines the record's value.
TTL	An integer that defines the record's TTL.
Weight	An integer that defines the load balancing weight assigned to the record.
GroupTypeId	An integer that should be set to "3."
Name	A string that defines the name of the load balancing group.
Records	Define the set of records that will be associated with the zone. This section should only describe records that do not belong to a load balancing or failover group.

Name	Description
RecordType	Each type of record is defined in its own section. Create a section for each desired record type. The available record types are: • A • AAAA • CAA • CNAME • MX • NS • PTR • SPF • SRV • TXT
Name	A string that defines a record's name.
Rdata	A string that defines a record's value.
TTL	An integer that defines a record's TTL.
Status	An integer that defines a zone's status by its system-defined ID. Use the Get Available Zone Statuses endpoint to retrieve a list of statuses and their IDs.
ZoneType	An integer that indicates that a primary zone will be created. Set this request element to "1."

Response

The response to the above request includes an HTTP status code, response headers, and a response body.

Status Code

A status code indicates whether the request was successfully performed.

Response Headers

The response for this endpoint only includes standard HTTP response headers. View common response headers.

Response Body

The response body for a successful request returns the properties of the newly created zone.

Name	Description
Comment	A string that indicates the comment associated with the new zone.
DomainName	A string that indicates the new zone's name.
FailoverGroups	This response element contains the set of failover groups associated with the new zone.
Group	This response element contains a failover group.
[A|AAAA|CNAME]	Each group contains a section for each record type. Records are returned in the following order. • A • AAAA • CNAME This response element contains the following information about a record: • Health check configuration • Properties • Primary status **Note:** If the group does not contain a particular type of record, then that section will remain blank.
HealthCheck	This response element describes the health check configuration associated with a record in the group. **Note:** A null value is returned if a health check configuration has not been defined.
CheckInterval	An integer that indicates the number of seconds between health checks.
CheckTypeId	An integer that identifies a type of health check by its system-defined ID. Use the Get Available Health Check Types endpoint to retrieve a list of health check types and their IDs.
ContentVerification	A string that indicates the text that will be used to verify the success of the health check.

Name	Description
EmailNotificationAddress	A string that indicates the e-mail address to which health check notifications will be sent.
FailedCheckThreshold	An integer that indicates the number of consecutive times that the same result must be returned before a health check agent will indicate a change in status.
HTTPMethodId	An integer that identifies an HTTP method by its system-defined ID. An HTTP method is only used by HTTP/HTTPs health checks. Use the Get Available HTTP Methods (Health Checks) endpoint to retrieve a list of HTTP methods and their IDs.
IPAddress	A string that indicates the IP address (IPv4 or IPv6) to which TCP health checks will be directed.
IPVersion	An integer that identifies an IP version by its system-defined ID. This IP version is only used by HTTP/HTTPs health checks. Use the Get Available IP Versions (Health Checks) endpoint to retrieve a list of IP versions and their IDs.
PortNumber	An integer that indicates the port to which TCP health checks will be directed.
ReintegrationMethodId	An integer that indicates the method through which an unhealthy server/domain will be integrated back into a group. Use the Get Available Health Check Reintegration Methods endpoint to retrieve a list of reintegration methods and their IDs.
Status	An integer that indicates the server/domain's health check status by its system-defined ID.
StatusName	A string that indicates the server/domain's health check status.
Uri	A string that indicates the URI to which HTTP/HTTPs health checks will be directed.
IsPrimary	A Boolean that indicates whether the current record is the primary server/domain to which traffic will be directed.
Record	This response element contains the record's properties.

Name	Description
Name	A string that indicates the record's name.
Rdata	A string that indicates the record's value.
TTL	An integer that indicates the record's TTL.
GroupTypeId	An integer that indicates the type of failover group by its system-defined ID. This response element will always report "3" which corresponds to zones.
Name	A string that indicates the name of the failover group.
LoadBalancingGroups	This response element contains the set of load balancing groups associated with the zone.
Group	This request element contains a load balancing group.
[A|AAAA|CNAME]	Each group contains a section for each record type. Records are returned in the following order. • A • AAAA • CNAME This response element contains the following information about a record: • Health check configuration • Properties • Primary status **Note:** If the group does not contain a particular type of record, then that section will remain blank.
HealthCheck	This response element describes the health check configuration associated with a record in the group. **Note:** A null value is returned if a health check configuration has not been defined.
CheckInterval	An integer that indicates the number of seconds between health checks.

Name	Description
CheckTypeId	An integer that indicates the type of health check by its system-defined ID.
	Use the Get Available Health Check Types endpoint to retrieve a list of health check types and their IDs.
ContentVerification	A string that indicates the text that will be used to verify the success of the health check.
EmailNotificationAddress	A string that identifies the e-mail address to which health check notifications will be sent.
FailedCheckThreshold	An integer that indicates the number of consecutive times that the same result must be returned before a health check agent will indicate a change in status.
HTTPMethodId	An integer that identifies an HTTP method by its system-defined ID. An HTTP method is only used by HTTP/HTTPs health checks.
	Use the Get Available HTTP Methods (Health Checks) endpoint to retrieve a list of HTTP methods and their IDs.
IPAddress	A string that indicates the IP address (IPv4 or IPv6) to which TCP health checks will be directed.
IPVersion	An integer that identifies an IP version by its system-defined ID. This IP version is only used by HTTP/HTTPs health checks.
	Use the Get Available IP Versions (Health Checks) endpoint to retrieve a list of IP versions and their IDs.
PortNumber	An integer that indicates the port to which TCP health checks will be directed.
ReintegrationMethodId	An integer that indicates the method through which an unhealthy server/domain will be integrated back into a group.
	Use the Get Available Health Check Reintegration Methods endpoint to retrieve a list of reintegration methods and their IDs.
Status	An integer that indicates the server/domain's health check status by its system-defined ID.
StatusName	A string that indicates the server/domain's health check status.

Name	Description
Uri	A string that indicates the URI to which HTTP/HTTPs health checks will be directed.
Record	This response element contains the record's properties.
Name	A string that indicates the record's name.
Rdata	A string that indicates the record's value.
TTL	An integer that indicates the record's TTL.
Weight	An integer that indicates the load balancing weight assigned to the record.
GroupTypeId	An integer that indicates the type of load balancing group by its system-defined ID. This response element will always report "3" which corresponds to zones.
Name	A string that indicates the name of the load balancing group.
Records	This response element describes the records associated with the new zone. This section only describes records that do not belong to a load balancing or failover group. **Note:** A null value is returned when the zone does not contain additional records.
RecordType	Each type of record is listed in its own section. Records are returned in the following order. • A • AAAA • CAA • CNAME • MX • NS • PTR • SPF • SRV • TXT This response element contains all of a zone's records for a given type.

Name	Description
Name	A string that indicates a record's name.
Rdata	A string that indicates a record's value.
TTL	An integer that indicates a record's TTL.
Status	An integer that indicates the new zone's status by its system-defined ID. Use the Get Available Zone Statuses endpoint to retrieve a list of statuses and their IDs.
Version	An integer that indicates the new zone's version. This version is incremented whenever a change is applied to the zone.
ZoneId	An integer that identifies the new zone by its system-defined ID.
ZoneType	An integer that indicates that a primary zone has been created. This response element will always be set to "1."

Errors

The response body for an unsuccessful request may contain an error element that provides additional information. View common error messages.

Sample Request and Response (JSON)

A sample JSON request is shown below.

```
POST https://api.edgecast.com/v2/mcc/customers/0001/dns/routezone HTTP/1.1

Authorization: TOK:12345678-1234-1234-1234-1234567890ab

Accept: application/json

Content-Type: application/json

Host: api.edgecast.com

Content-Length: 1718


{

        "Comment" : "",

        "DomainName" : "myzone.com.",

        "FailoverGroups" : [{

                    "Group" : {

                            "A" : [],

                            "AAAA" : [],

                            "CNAME" : [{
```

```
                                        "HealthCheck" : null,
                                        "IsPrimary" : false,
                                        "Record" : {
                                                "Name" : "web",
                                                "Rdata" : "web01.myzone.com.",
                                                "TTL" : 300
                                        }
                                }, {
                                        "HealthCheck" : null,
                                        "IsPrimary" : true,
                                        "Record" : {
                                                "Name" : "web",
                                                "Rdata" : "web02.myzone.com.",
                                                "TTL" : 300
                                        }
                                }
                        ]
                },
                "GroupTypeId" : 3,
                "Name" : "web"
        }
],
"LoadBalancingGroups" : [{
                "Group" : {
                        "A" : [],
                        "AAAA" : [],
                        "CNAME" : [{
                                        "HealthCheck" : null,
                                        "Record" : {
                                                "Name" : "mycdn",
                                                "Rdata" : "www.myzone.com.",
                                                "TTL" : 300
                                        },
                                        "Weight" : 50
                                }, {
                                        "HealthCheck" : null,
                                        "Record" : {
                                                "Name" : "mycdn",
```

```
                                    "Rdata" : "www2.myzone.com.",
                                    "TTL" : 300
                                },
                                "Weight" : 50
                            }
                        ]
                },
                "GroupTypeId" : 3,
                "Name" : "mycdn"
            }
    ],
    "Records" : {
            "A" : [{
                        "Name" : "www",
                        "Rdata" : "10.55.66.22",
                        "TTL" : 3600
                }, {
                        "Name" : "www",
                        "Rdata" : "55.66.88.11",
                        "TTL" : 3600
                }, {
                        "Name" : "www",
                        "Rdata" : "66.77.99.22",
                        "TTL" : 3600
                }, {
                        "Name" : "www",
                        "Rdata" : "11.66.77.33",
                        "TTL" : 3600
                }
            ],
            "AAAA" : [{
                        "Name" : "www",
                        "Rdata" : "1:1:1:2:3:4:5:6",
                        "TTL" : 3600
                }, {
                        "Name" : "www",
                        "Rdata" : "::2",
                        "TTL" : 3600
```

```
                    }
            ],
            "CNAME" : [],
            "MX" : [],
            "NS" : [],
            "SPF" : [],
            "SRV" : [],
            "TXT" : []
        },
        "Status" : 2,
        "ZoneType" : 1
}
```

A sample JSON response is shown below.

```
HTTP/1.1 200 OK
Cache-Control: private
Content-Type: application/json; charset=utf-8
Date: Thu, 14 Apr 2016 12:00:00 GMT
Content-Length: 1380


{
        "Comment" : "",
        "DomainName" : "myzone.com.",
        "FailoverGroups" : [{
                    "Group" : {
                            "A" : [],
                            "AAAA" : [],
                            "CNAME" : [{
                                        "HealthCheck" : null,
                                        "IsPrimary" : false,
                                        "Record" : {
                                                "Name" : "web",
                                                "Rdata" : "web01.myzone.com.",
                                                "TTL" : 300
                                        }
                                }, {
                                        "HealthCheck" : null,
                                        "IsPrimary" : true,
                                        "Record" : {
```

```json
                                                "Name" : "web",
                                                "Rdata" : "web02.myzone.com.",
                                                "TTL" : 300
                                        }
                                }
                        ]
                },
                "GroupTypeId" : 3,
                "Name" : "web"
        }
    ],
    "LoadBalancingGroups" : [{
                "Group" : {
                        "A" : [],
                        "AAAA" : [],
                        "CNAME" : [{
                                        "HealthCheck" : null,
                                        "Record" : {
                                                "Name" : "mycdn",
                                                "Rdata" : "www.myzone.com.",
                                                "TTL" : 300
                                        },
                                        "Weight" : 50
                                }, {
                                        "HealthCheck" : null,
                                        "Record" : {
                                                "Name" : "mycdn",
                                                "Rdata" : "www2.myzone.com.",
                                                "TTL" : 300
                                        },
                                        "Weight" : 50
                                }
                        ]
                },
                "GroupTypeId" : 3,
                "Name" : "mycdn"
        }
    ],
```

```
        "Records" : {
                "A" : [{
                                "Name" : "www",
                                "Rdata" : "10.55.66.22",
                                "TTL" : 3600
                        }, {
                        ...
                        }, {
                                "Name" : "www",
                                "Rdata" : "11.66.77.33",
                                "TTL" : 3600
                        }
                ],
                "AAAA" : [{
                                "Name" : "www",
                                "Rdata" : "1:1:1:2:3:4:5:6",
                                "TTL" : 3600
                        }, {
                                "Name" : "www",
                                "Rdata" : "::2",
                                "TTL" : 3600
                        }
                ],
                "CNAME" : [],
                "MX" : [],
                "NS" : [],
                "SPF" : [],
                "SRV" : [],
                "TXT" : []
        },
        "Status" : 2,
        "Version" : 1234567890,
        "ZoneId" : 1234,
        "ZoneType" : 1
}
```

Copy Primary Zone

Creates a copy of a primary zone. The only difference between the original zone and its copy is the name assigned to it.

Request

A request to copy a zone is described below.

HTTP Method	Request URI
POST	https://api.edgecast.com/v2/mcc/customers/*xxxx*/dns/routezone/copy

Define the following terms when submitting the above request:

- **xxxx:** Replace this term with your CDN account number.

Request Headers

This endpoint only takes advantage of common request headers.

Note: This endpoint only supports JSON.

Request Body

The required request parameters for this endpoint are described below.

Name	Description
FromDomainName	A string that identifies the zone that will be copied by its name.
ToDomainName	A string that defines the name that will be assigned to the new zone.

Response

The response to the above request includes an HTTP status code, response headers, and a response body.

Status Code

A status code indicates whether the request was successfully performed.

Response Headers

The response for this endpoint only includes standard HTTP response headers. View common response headers.

Response Body

The response body for a successful request returns the properties of the newly created zone.

Name	Description
Comment	A string that indicates the comment associated with the new zone.
DomainName	A string that indicates the new zone's name.
FailoverGroups	This response element contains the set of failover groups associated with the new zone.
Group	This response element contains a failover group.
[A|AAAA|CNAME]	Each group contains a section for each record type. Records are returned in the following order. • A • AAAA • CNAME This response element contains the following information about a record: • Health check configuration • Properties • Primary status **Note:** If the group does not contain a particular type of record, then that section will remain blank.
HealthCheck	This response element describes the health check configuration associated with a record in the group. **Note:** A null value is returned if a health check configuration has not been defined.
CheckInterval	An integer that indicates the number of seconds between health checks.
CheckTypeId	An integer that identifies a type of health check by its system-defined ID. Use the Get Available Health Check Types endpoint to retrieve a list of health check types and their IDs.
ContentVerification	A string that indicates the text that will be used to verify the success of the health check.

Name	Description
EmailNotificationAddress	A string that indicates the e-mail address to which health check notifications will be sent.
FailedCheckThreshold	An integer that indicates the number of consecutive times that the same result must be returned before a health check agent will indicate a change in status.
HTTPMethodId	An integer that identifies an HTTP method by its system-defined ID. An HTTP method is only used by HTTP/HTTPs health checks. Use the Get Available HTTP Methods (Health Checks) endpoint to retrieve a list of HTTP methods and their IDs.
IPAddress	A string that indicates the IP address (IPv4 or IPv6) to which TCP health checks will be directed.
IPVersion	An integer that identifies an IP version by its system-defined ID. This IP version is only used by HTTP/HTTPs health checks. Use the Get Available IP Versions (Health Checks) endpoint to retrieve a list of IP versions and their IDs.
PortNumber	An integer that indicates the port to which TCP health checks will be directed.
ReintegrationMethodId	An integer that indicates the method through which an unhealthy server/domain will be integrated back into a group. Use the Get Available Health Check Reintegration Methods endpoint to retrieve a list of reintegration methods and their IDs.
Status	An integer that indicates the server/domain's health check status by its system-defined ID.
StatusName	A string that indicates the server/domain's health check status.
Uri	A string that indicates the URI to which HTTP/HTTPs health checks will be directed.
IsPrimary	A Boolean that indicates whether the current record is the primary server/domain to which traffic will be directed.
Record	This response element contains the record's properties.

Name	Description
Name	A string that indicates the record's name.
Rdata	A string that indicates the record's value.
TTL	An integer that indicates the record's TTL.
GroupTypeId	An integer that indicates the type of failover group by its system-defined ID. This response element will always report "3" which corresponds to zones.
Name	A string that indicates the name of the failover group.
LoadBalancingGroups	This response element contains the set of load balancing groups associated with the zone.
Group	This request element contains a load balancing group.
[A|AAAA|CNAME]	Each group contains a section for each record type. Records are returned in the following order. • A • AAAA • CNAME This response element contains the following information about a record: • Health check configuration • Properties • Primary status **Note:** If the group does not contain a particular type of record, then that section will remain blank.
HealthCheck	This response element describes the health check configuration associated with a record in the group. **Note:** A null value is returned if a health check configuration has not been defined.
CheckInterval	An integer that indicates the number of seconds between health checks.

Name	Description
CheckTypeId	An integer that indicates the type of health check by its system-defined ID. Use the Get Available Health Check Types endpoint to retrieve a list of health check types and their IDs.
ContentVerification	A string that indicates the text that will be used to verify the success of the health check.
EmailNotificationAddress	A string that identifies the e-mail address to which health check notifications will be sent.
FailedCheckThreshold	An integer that indicates the number of consecutive times that the same result must be returned before a health check agent will indicate a change in status.
HTTPMethodId	An integer that identifies an HTTP method by its system-defined ID. An HTTP method is only used by HTTP/HTTPs health checks. Use the Get Available HTTP Methods (Health Checks) endpoint to retrieve a list of HTTP methods and their IDs.
IPAddress	A string that indicates the IP address (IPv4 or IPv6) to which TCP health checks will be directed.
IPVersion	An integer that identifies an IP version by its system-defined ID. This IP version is only used by HTTP/HTTPs health checks. Use the Get Available IP Versions (Health Checks) endpoint to retrieve a list of IP versions and their IDs.
PortNumber	An integer that indicates the port to which TCP health checks will be directed.
ReintegrationMethodId	An integer that indicates the method through which an unhealthy server/domain will be integrated back into a group. Use the Get Available Health Check Reintegration Methods endpoint to retrieve a list of reintegration methods and their IDs.
Status	An integer that indicates the server/domain's health check status by its system-defined ID.
StatusName	A string that indicates the server/domain's health check status.

Name	Description
Uri	A string that indicates the URI to which HTTP/HTTPs health checks will be directed.
Record	This response element contains the record's properties.
Name	A string that indicates the record's name.
Rdata	A string that indicates the record's value.
TTL	An integer that indicates the record's TTL.
Weight	An integer that indicates the load balancing weight assigned to the record.
GroupTypeId	An integer that indicates the type of load balancing group by its system-defined ID. This response element will always report "3" which corresponds to zones.
Name	A string that indicates the name of the load balancing group.
Records	This response element describes the records associated with the new zone. This section only describes records that do not belong to a load balancing or failover group. **Note:** A null value is returned when the zone does not contain additional records.
RecordType	Each type of record is listed in its own section. Records are returned in the following order. • A • AAAA • CAA • CNAME • MX • NS • PTR • SPF • SRV • TXT This response element contains all of a zone's records for a given type.

Name	Description
Name	A string that indicates a record's name.
Rdata	A string that indicates a record's value.
TTL	An integer that indicates a record's TTL.
Status	An integer that indicates the new zone's status by its system-defined ID. Use the Get Available Zone Statuses endpoint to retrieve a list of statuses and their IDs.
Version	An integer that indicates the new zone's version. This version is incremented whenever a change is applied to the zone.
ZoneId	An integer that identifies the new zone by its system-defined ID.
ZoneType	An integer that indicates that a primary zone has been created. This response element will always be set to "1."

Errors

The response body for an unsuccessful request may contain an error element that provides additional information. View common error messages.

Sample Request and Response (JSON)

A sample JSON request is shown below.

```
POST https://api.edgecast.com/v2/mcc/customers/0001/dns/routezone/copy HTTP/1.1

Authorization: TOK:12345678-1234-1234-1234-1234567890ab

Accept: application/json

Content-Type: application/json

Host: api.edgecast.com

Content-Length: 72


{

        "FromDomainName":"myzone.com",

        "ToDomainName":"copyofmyzone.com"

}
```

A sample JSON response is shown below.

```
HTTP/1.1 200 OK

Cache-Control: private
```

```
Content-Type: application/json; charset=utf-8
Date: Thu, 14 Apr 2016 12:00:00 GMT
Content-Length: 1380


{
        "Comment" : "",
        "DomainName" : "copyofmyzone.com.",
        "FailoverGroups" : [{
                    "Group" : {
                            "A" : [],
                            "AAAA" : [],
                            "CNAME" : [{
                                            "HealthCheck" : null,
                                            "IsPrimary" : false,
                                            "Record" : {
                                                    "Name" : "web",
                                                    "Rdata" : "web01.myzone.com.",
                                                    "TTL" : 300
                                            }
                                    }, {
                                            "HealthCheck" : null,
                                            "IsPrimary" : true,
                                            "Record" : {
                                                    "Name" : "web",
                                                    "Rdata" : "web02.myzone.com.",
                                                    "TTL" : 300
                                            }
                                    }
                            ]
                    },
                    "GroupTypeId" : 3,
                    "Name" : "web"
            }
        ],
        "LoadBalancingGroups" : [{
                    "Group" : {
                            "A" : [],
                            "AAAA" : [],
```

```
                                "CNAME" : [{
                                        "HealthCheck" : null,
                                        "Record" : {
                                                "Name" : "mycdn",
                                                "Rdata" : "www.myzone.com.",
                                                "TTL" : 300
                                        },
                                        "Weight" : 50
                                }, {
                                        "HealthCheck" : null,
                                        "Record" : {
                                                "Name" : "mycdn",
                                                "Rdata" : "www2.myzone.com.",
                                                "TTL" : 300
                                        },
                                        "Weight" : 50
                                }
                        ]
                },
                "GroupTypeId" : 3,
                "Name" : "mycdn"
        }
],
"Records" : {
        "A" : [{
                        "Name" : "www",
                        "Rdata" : "10.55.66.22",
                        "TTL" : 3600
                }, {
                        "Name" : "www",
                        "Rdata" : "55.66.88.11",
                        "TTL" : 3600
                }, {
                        "Name" : "www",
                        "Rdata" : "66.77.99.22",
                        "TTL" : 3600
                }, {
                        "Name" : "www",
```

```
                        "Rdata" : "11.66.77.33",

                        "TTL" : 3600

                }
        ],
        "AAAA" : [{

                        "Name" : "www",

                        "Rdata" : "1:1:1:2:3:4:5:6",

                        "TTL" : 3600

                }, {

                        "Name" : "www",

                        "Rdata" : "::2",

                        "TTL" : 3600

                }
        ],
        "CNAME" : [],
        "MX" : [],
        "NS" : [],
        "SPF" : [],
        "SRV" : [],
        "TXT" : []
    },
    "Status" : 2,
    "Version" : 1234567890,
    "ZoneId" : 1234,
    "ZoneType" : 1
}
```

Delete Primary Zone

Deletes a primary zone.

Warning: The deletion of a primary zone takes place immediately and cannot be undone.

Note: This endpoint may not be used to delete a secondary zone.

Request

A request to delete a primary zone is described below.

HTTP Method	Request URI
DELETE	https://api.edgecast.com/v2/mcc/customers/*xxxx*/dns/routezone/*ZoneID*

Define the following terms when submitting the above request:

- **xxxx:** Replace this term with your CDN account number.

- **ZoneID:** Replace this term with the system-defined ID of the desired zone. Use the Get All Zones endpoint to retrieve a list of zones and their system-defined IDs.

Request Headers

This endpoint only takes advantage of common request headers.

Note: This endpoint only supports JSON.

Request Body

Request body parameters are not required by this endpoint.

Response

The response to the above request includes an HTTP status code, response headers, and a response body.

Status Code

A status code indicates whether the request was successfully performed.

Response Headers

The response for this endpoint only includes standard HTTP response headers. View common response headers.

Response Body

The response body for a successful request does not contain a response element.

Errors

The response body for an unsuccessful request may contain an error element that provides additional information. View common error messages.

Sample Request and Response (JSON)

A sample JSON request is shown below.

```
DELETE https://api.edgecast.com/v2/mcc/customers/0001/dns/routezone/1234 HTTP/1.1
Authorization: TOK:12345678-1234-1234-1234-1234567890ab
Host: api.edgecast.com
```

A sample JSON response is shown below.

```
HTTP/1.1 200 OK
Cache-Control: private
Date: Thu, 14 Apr 2016 12:00:00 GMT
```

Get All Zones

This endpoint returns a list of primary zones. This list may be filtered by zone status.

Request

A request to retrieve zones is described below.

HTTP Method	Request URI
GET	https://api.edgecast.com/v2/mcc/customers/*xxxx*/dns/routezones?status=*StatusID*

Define the following terms when submitting the above request:

- **xxxx:** Replace this term with your CDN account number.

- **StatusID:** Replace this term with the ID for the desired zone status. The response will be filtered by the specified status. If the response should not be filtered by status, then the status query string parameter should not be included in the request URI.

Request Headers

This endpoint only takes advantage of common request headers.

Note: This endpoint only supports JSON.

Request Body

Request body parameters are not required by this endpoint.

Response

The response to the above request includes an HTTP status code, response headers, and a response body.

Status Code

A status code indicates whether the request was successfully performed.

Response Headers

The response for this endpoint only includes standard HTTP response headers. View common response headers.

Response Body

The response body for a successful request contains the following response elements for each zone returned by this endpoint:

Name	Description
DomainName	A string that identifies a zone by its name.
Status	An integer that indicates a zone's status by its system-defined ID. Use the Get Available Zone Statuses endpoint to retrieve a list of zone statuses.
Version	An integer that indicates a zone's version. This version number is incremented whenever a change is applied to a zone.
ZoneId	An integer that identifies a zone by its system-defined ID.
ZoneType	An integer that indicates the type of zone being described. Use the Get Available Zone Types endpoint to retrieve a list of zone types.

Errors

The response body for an unsuccessful request may contain an error element that provides additional information. View common error messages.

Sample Request and Response (JSON)

A sample JSON request is shown below.

```
GET https://api.edgecast.com/v2/mcc/customers/0001/dns/routezones HTTP/1.1

Authorization: TOK:12345678-1234-1234-1234-1234567890ab

Accept: application/json

Host: api.edgecast.com
```

A sample JSON response is shown below.

```
HTTP/1.1 200 OK

Cache-Control: private

Content-Type: application/json; charset=utf-8

Date: Thu, 14 Apr 2016 12:00:00 GMT

Content-Length: 248
```

```
[{
            "DomainName" : "myzone.com.",
            "Status" : 2,
            "Version" : 1390352161,
            "ZoneId" : 1234,
            "ZoneType" : 1
     }, {
            "DomainName" : "mydomain.com.",
            "Status" : 2,
            "Version" : 1390352161,
            "ZoneId" : 1235,
            "ZoneType" : 1
     }
]
```

Get Available Health Check Reintegration Methods

Returns a list of methods through which a server/domain can be reintegrated into a load balancing or failover group.

Request

A request to retrieve reintegration methods is described below.

HTTP Method	Request URI
GET	https://api.edgecast.com/v2/mcc/dns/routereintegrationmethodtypes

Request Headers
This endpoint only takes advantage of common request headers.

Note: This endpoint only supports JSON.

Request Body
Request body parameters are not required by this endpoint.

Response

The response to the above request includes an HTTP status code, response headers, and a response body.

Status Code
A status code indicates whether the request was successfully performed.

Response Headers

The response for this endpoint only includes standard HTTP response headers. View common response headers.

Response Body

The response body for a successful request contains the following response elements for each reintegration method returned by this endpoint:

Name	Description
Id	An integer that indicates the system-defined ID assigned to the reintegration method.
Name	A string that indicates the name of a reintegration method.

Errors

The response body for an unsuccessful request may contain an error element that provides additional information. View common error messages.

Sample Request and Response (JSON)

A sample JSON request is shown below.

```
GET https://api.edgecast.com/v2/mcc/dns/routereintegrationmethodtypes HTTP/1.1
Authorization: TOK:12345678-1234-1234-1234-1234567890ab
Accept: application/json
Host: api.edgecast.com
```

A sample JSON response is shown below.

```
HTTP/1.1 200 OK
Cache-Control: private
Content-Type: application/json; charset=utf-8
Date: Thu, 14 Apr 2016 12:00:00 GMT
Content-Length: 87

[{
            "Id" : 1,
            "Name" : "Automatic"
      }, {
            "Id" : 2,
            "Name" : "Manual"
      }
]
```

Get Available Health Check Types

Returns a list of the supported methods that may be used to probe a server/domain's health status.

Request

A request to retrieve supported health check types is described below.

HTTP Method	Request URI
GET	https://api.edgecast.com/v2/mcc/dns/routehealthchecktypes

Request Headers

This endpoint only takes advantage of common request headers.

Note: This endpoint only supports JSON.

Request Body

Request body parameters are not required by this endpoint.

Response

The response to the above request includes an HTTP status code, response headers, and a response body.

Status Code

A status code indicates whether the request was successfully performed.

Response Headers

The response for this endpoint only includes standard HTTP response headers. View common response headers.

Response Body

The response body for a successful request contains the following response elements for each health check type returned by this endpoint:

Name	Description
Id	An integer that indicates the system-defined ID assigned to the health check type.
Name	A string that indicates the name of the health check type supported by our DNS Health Checks module.

Errors

The response body for an unsuccessful request may contain an error element that provides additional information. View common error messages.

Sample Request and Response (JSON)

A sample JSON request is shown below.

```
GET https://api.edgecast.com/v2/mcc/dns/routehealthchecktypes HTTP/1.1

Authorization: TOK:12345678-1234-1234-1234-1234567890ab

Accept: application/json

Host: api.edgecast.com
```

A sample JSON response is shown below.

```
HTTP/1.1 200 OK

Cache-Control: private

Content-Type: application/json; charset=utf-8

Date: Thu, 14 Apr 2016 12:00:00 GMT

Content-Length: 166

[{

            "Id" : 1,

            "Name" : "HTTP"

      }, {

            "Id" : 2,

            "Name" : "HTTPs"

      }, {

            "Id" : 3,

            "Name" : "TCP Open"

      }, {

            "Id" : 4,

            "Name" : "TCP SSL"

      }

]
```

Get Available HTTP Methods (Health Checks)

Returns a list of the HTTP methods supported by the DNS Health Checks module.

Request

A request to retrieve a list of HTTP methods is described below.

HTTP Method	Request URI
GET	https://api.edgecast.com/v2/mcc/dns/routehttpmethodtypes

Request Headers

This endpoint only takes advantage of common request headers.

Note: This endpoint only supports JSON.

Request Body

Request body parameters are not required by this endpoint.

Response

The response to the above request includes an HTTP status code, response headers, and a response body.

Status Code

A status code indicates whether the request was successfully performed.

Response Headers

The response for this endpoint only includes standard HTTP response headers. View common response headers.

Response Body

The response body for a successful request contains the following response elements for each HTTP method returned by this endpoint:

Name	Description
Id	An integer that indicates the system-defined ID assigned to an HTTP method.
Name	A string that indicates the name of a supported HTTP method.

Errors

The response body for an unsuccessful request may contain an error element that provides additional information. View common error messages.

Sample Request and Response (JSON)

A sample JSON request is shown below.

```
GET https://api.edgecast.com/v2/mcc/dns/routehttpmethodtypes HTTP/1.1

Authorization: TOK:12345678-1234-1234-1234-1234567890ab

Accept: application/json

Host: api.edgecast.com
```

A sample JSON response is shown below.

```
HTTP/1.1 200 OK

Cache-Control: private

Content-Type: application/json; charset=utf-8

Date: Thu, 14 Apr 2016 12:00:00 GMT

Content-Length: 79

[{

            "Id" : 1,

            "Name" : "GET"

    }, {

            "Id" : 2,

            "Name" : "POST"

    }

]
```

Get Available IP Versions (Health Checks)

Returns the available set of IP versions supported by our DNS Health Checks module.

Request

A request to find out the supported set of IP versions is described below.

HTTP Method	Request URI
GET	https://api.edgecast.com/v2/mcc/dns/routehealthcheckipversion

Request Headers

This endpoint only takes advantage of common request headers.

Note: This endpoint only supports JSON.

Request Body

Request body parameters are not required by this endpoint.

Response

The response to the above request includes an HTTP status code, response headers, and a response body.

Status Code

A status code indicates whether the request was successfully performed.

Response Headers

The response for this endpoint only includes standard HTTP response headers. View common response headers.

Response Body

The response body for a successful request contains the following response elements for each IP version returned by this endpoint:

Name	Description
Id	An integer that indicates the system-defined ID assigned to the IP version.
Name	A string that indicates the name of the IP version supported by our DNS Health Checks module.

Errors

The response body for an unsuccessful request may contain an error element that provides additional information. View common error messages.

Sample Request and Response (JSON)

A sample JSON request is shown below.

```
GET https://api.edgecast.com/v2/mcc/dns/routehealthcheckipversion HTTP/1.1

Authorization: TOK:12345678-1234-1234-1234-1234567890ab

Accept: application/json

Host: api.edgecast.com
```

A sample JSON response is shown below.

```
HTTP/1.1 200 OK

Cache-Control: private

Content-Type: application/json; charset=utf-8

Date: Thu, 14 Apr 2016 12:00:00 GMT

Content-Length: 80
```

```
[{
            "Id" : 1,

            "Name" : "IPv4"

      }, {

            "Id" : 2,

            "Name" : "IPv6"

      }
]
```

Get Available Load Balancing and Failover Group Types

Returns a list of the available types of load balancing and failover groups.

Request

A request to the available set of group types is described below.

HTTP Method	Request URI
GET	https://api.edgecast.com/v2/mcc/dns/routegrouptypes

Request Headers

This endpoint only takes advantage of common request headers.

Note: This endpoint only supports JSON.

Request Body

Request body parameters are not required by this endpoint.

Response

The response to the above request includes an HTTP status code, response headers, and a response body.

Status Code

A status code indicates whether the request was successfully performed.

Response Headers

The response for this endpoint only includes standard HTTP response headers. View common response headers.

Response Body

The response body for a successful request contains the following response elements for each group type returned by this endpoint:

Name	Description
Id	An integer that indicates the system-defined ID assigned to the group type.
Name	A string that indicates the load balancing/failover group type.

Errors

The response body for an unsuccessful request may contain an error element that provides additional information. View common error messages.

Sample Request and Response (JSON)

A sample JSON request is shown below.

```
GET https://api.edgecast.com/v2/mcc/dns/routegrouptypes HTTP/1.1

Authorization: TOK:12345678-1234-1234-1234-1234567890ab

Accept: application/json

Host: api.edgecast.com
```

A sample JSON response is shown below.

```
HTTP/1.1 200 OK

Cache-Control: private

Content-Type: application/json; charset=utf-8

Date: Thu, 14 Apr 2016 12:00:00 GMT

Content-Length: 125

[{

        "Id" : 1,

        "Name" : "CNAME"

    }, {

        "Id" : 2,

        "Name" : "Subdomain"

    }, {

        "Id" : 3,

        "Name" : "Zone"

    }

]
```

Get Available Record Types

Returns a list of the available types of records and their system-defined IDs.

Request

A request to retrieve record types is described below.

HTTP Method	Request URI
GET	https://api.edgecast.com/v2/mcc/dns/routezonerecordtypes

Request Headers

This endpoint only takes advantage of common request headers.

Note: This endpoint only supports JSON.

Request Body

Request body parameters are not required by this endpoint.

Response

The response to the above request includes an HTTP status code, response headers, and a response body.

Status Code

A status code indicates whether the request was successfully performed.

Response Headers

The response for this endpoint only includes standard HTTP response headers. View common response headers.

Response Body

The response body for a successful request contains the following response elements for each record type returned by this endpoint:

Name	Description
Id	An integer that indicates the system-defined ID assigned to the record type.
Name	A string that indicates the name of the record type.

Errors

The response body for an unsuccessful request may contain an error element that provides additional information. View common error messages.

Sample Request and Response (JSON)

A sample JSON request is shown below.

```
GET https://api.edgecast.com/v2/mcc/dns/routezonerecordtypes HTTP/1.1
Authorization: TOK:12345678-1234-1234-1234-1234567890ab
Accept: application/json
Host: api.edgecast.com
```

A sample JSON response is shown below.

```
HTTP/1.1 200 OK
Cache-Control: private
Content-Type: application/json; charset=utf-8
Date: Thu, 14 Apr 2016 12:00:00 GMT
Content-Length: 306

[{
            "Id" : 1,
            "Name" : "A"
     }, {
            "Id" : 2,
            "Name" : "AAAA"
     }, {
            "Id" : 3,
            "Name" : "CNAME"
     }, {
            "Id" : 4,
            "Name" : "MX"
     }, {
            "Id" : 5,
            "Name" : "NS"
     }, {
            "Id" : 8,
            "Name" : "SPF"
     }, {
            "Id" : 9,
            "Name" : "SRV"
     }, {
            "Id" : 10,
            "Name" : "TXT"
     }
]
```

Get Available Zone Statuses

Returns a list of possible zone statuses.

Request

A request to retrieve a list of zone statuses is described below.

HTTP Method	Request URI
GET	https://api.edgecast.com/v2/mcc/dns/routezonestatus

Request Headers

This endpoint only takes advantage of common request headers.

Note: This endpoint only supports JSON.

Request Body

Request body parameters are not required by this endpoint.

Response

The response to the above request includes an HTTP status code, response headers, and a response body.

Status Code

A status code indicates whether the request was successfully performed.

Response Headers

The response for this endpoint only includes standard HTTP response headers. View common response headers.

Response Body

The response body for a successful request contains the following response elements for each zone status returned by this endpoint:

Name	Description
Id	An integer that indicates the system-defined ID assigned to a zone status.
Name	A string that indicates the name of a zone status.

Errors

The response body for an unsuccessful request may contain an error element that provides additional information. View common error messages.

Sample Request and Response (JSON)

A sample JSON request is shown below.

```
GET https://api.edgecast.com/v2/mcc/dns/routezonestatus HTTP/1.1

Authorization: TOK:12345678-1234-1234-1234-1234567890ab

Accept: application/json

Host: api.edgecast.com
```

A sample JSON response is shown below.

```
HTTP/1.1 200 OK

Cache-Control: private

Content-Type: application/json; charset=utf-8

Date: Thu, 14 Apr 2016 12:00:00 GMT

Content-Length: 86

[{

            "Id" : 1,

            "Name" : "Active"

    }, {

            "Id" : 2,

            "Name" : "Inactive"

    }

]
```

Get Available Zone Types

Returns a list of the available types of zones.

Request

A request to retrieve zone types is described below.

HTTP Method	Request URI
GET	https://api.edgecast.com/v2/mcc/dns/routezonetypes

Request Headers
This endpoint only takes advantage of common request headers.

Note: This endpoint only supports JSON.

Request Body
Request body parameters are not required by this endpoint.

Response

The response to the above request includes an HTTP status code, response headers, and a response body.

Status Code

A status code indicates whether the request was successfully performed.

Response Headers

The response for this endpoint only includes standard HTTP response headers. View common response headers.

Response Body

The response body for a successful request contains the following response elements for each zone type returned by this endpoint:

Name	Description
Id	An integer that indicates the system-defined ID assigned to the zone type.
Name	A string that indicates the name of the zone type.

Errors

The response body for an unsuccessful request may contain an error element that provides additional information. View common error messages.

Sample Request and Response (JSON)

A sample JSON request is shown below.

```
GET https://api.edgecast.com/v2/mcc/dns/routezonetypes HTTP/1.1
Authorization: TOK:12345678-1234-1234-1234-1234567890ab
Accept: application/json
Host: api.edgecast.com
```

A sample JSON response is shown below.

```
HTTP/1.1 200 OK
Cache-Control: private
Content-Type: application/json; charset=utf-8
Date: Thu, 14 Apr 2016 12:00:00 GMT
Content-Length: 88
```

```
[{
            "Id" : 1,
            "Name" : "Primary"
    }, {
            "Id" : 2,
            "Name" : "Secondary"
    }
]
```

Get Zone

Retrieves a zone's properties and describes all of its records.

Request

A request to retrieve a zone is described below.

HTTP Method	Request URI
GET	https://api.edgecast.com/v2/mcc/customers/*xxxx*/dns/routezone ?id=*ZoneID*&name=*ZoneName*&timestamp=*DateTime*

Define the following terms when submitting the above request:

- **xxxx:** Replace this term with your CDN account number.

- **ZoneID:** Replace this term with the ID of the desired zone.

- **ZoneName:** Replace this term with the name of the desired zone.

- **DateTime:** Optional. Retrieve the version of a zone at a given point in time. Replace this term with the desired date/time. The format for this term is: *YYYY-MM-DD*T*hh:mm:ss*.

Note: Either the id or the name query string parameter must be specified.

Note: Time (i.e., T*hh:mm:ss*) is optional. If time is not specified, then a default time (i.e., 00:00:00) will be used.

Request Headers
This endpoint only takes advantage of common request headers.

Note: This endpoint only supports JSON.

Request Body
Request body parameters are not required by this endpoint.

Response

The response to the above request includes an HTTP status code, response headers, and a response body.

Status Code

A status code indicates whether the request was successfully performed.

Response Headers

The response for this endpoint only includes standard HTTP response headers. View common response headers.

Response Body

The response body for a successful request contains the following response elements for the zone returned by this endpoint:

Name	Description
Comment	A string that indicates the comment associated with a zone.
DomainName	A string that indicates a zone's name.
FailoverGroups	This response element contains the set of failover groups associated with a zone.
Group	This response element contains a failover group.
[A|AAAA|CNAME]	Each group contains a section for each record type. Records are returned in the following order. • A • AAAA • CNAME This response element contains the following information about a record: • Health check configuration • Properties • Primary status **Note:** If the group does not contain a particular type of record, then that section will remain blank.

Name	Description
HealthCheck	This response element describes the health check configuration associated with a record in the group.
	Note: A null value is returned if a health check configuration has not been defined.
CheckInterval	An integer that indicates the number of seconds between health checks.
CheckTypeId	An integer that identifies a type of health check by its system-defined ID.
	Use the Get Available Health Check Types endpoint to retrieve a list of health check types and their IDs.
ContentVerification	A string that indicates the text that will be used to verify the success of the health check.
EmailNotificationAddress	A string that indicates the e-mail address to which health check notifications will be sent.
FailedCheckThreshold	An integer that indicates the number of consecutive times that the same result must be returned before a health check agent will indicate a change in status.
HTTPMethodId	An integer that identifies an HTTP method by its system-defined ID. An HTTP method is only used by HTTP/HTTPs health checks.
	Use the Get Available HTTP Methods (Health Checks) endpoint to retrieve a list of HTTP methods and their IDs.
IPAddress	A string that indicates the IP address (IPv4 or IPv6) to which TCP health checks will be directed.
IPVersion	An integer that identifies an IP version by its system-defined ID. This IP version is only used by HTTP/HTTPs health checks.
	Use the Get Available IP Versions (Health Checks) endpoint to retrieve a list of IP versions and their IDs.
PortNumber	An integer that indicates the port to which TCP health checks will be directed.

Name	Description
ReintegrationMethodId	An integer that indicates the method through which an unhealthy server/domain will be integrated back into a group. Use the Get Available Health Check Reintegration Methods endpoint to retrieve a list of reintegration methods and their IDs.
Status	An integer that indicates the server/domain's health check status by its system-defined ID.
StatusName	A string that indicates the server/domain's health check status.
Uri	A string that indicates the URI to which HTTP/HTTPs health checks will be directed.
IsPrimary	A Boolean that indicates whether the current record is the primary server/domain to which traffic will be directed.
Record	This response element contains the record's properties.
Name	A string that indicates the record's name.
Rdata	A string that indicates the record's value.
TTL	An integer that indicates the record's TTL.
GroupTypeId	An integer that indicates the type of failover group by its system-defined ID. This response element will always report "3" which corresponds to zones.
Name	A string that indicates the name of the failover group.
LoadBalancingGroups	This response element contains the set of load balancing groups associated with the zone.
Group	This request element contains a load balancing group.

Name	Description
[A|AAAA|CNAME]	Each group contains a section for each record type. Records are returned in the following order. • A • AAAA • CNAME This response element contains the following information about a record: • Health check configuration • Properties • Primary status **Note:** If the group does not contain a particular type of record, then that section will remain blank.
HealthCheck	This response element describes the health check configuration associated with a record in the group. **Note:** A null value is returned if a health check configuration has not been defined.
CheckInterval	An integer that indicates the number of seconds between health checks.
CheckTypeId	An integer that indicates the type of health check by its system-defined ID. Use the Get Available Health Check Types endpoint to retrieve a list of health check types and their IDs.
ContentVerification	A string that indicates the text that will be used to verify the success of the health check.
EmailNotificationAddress	A string that identifies the e-mail address to which health check notifications will be sent.
FailedCheckThreshold	An integer that indicates the number of consecutive times that the same result must be returned before a health check agent will indicate a change in status.

Name	Description
HTTPMethodId	An integer that identifies an HTTP method by its system-defined ID. An HTTP method is only used by HTTP/HTTPs health checks. Use the Get Available HTTP Methods (Health Checks) endpoint to retrieve a list of HTTP methods and their IDs.
IPAddress	A string that indicates the IP address (IPv4 or IPv6) to which TCP health checks will be directed.
IPVersion	An integer that identifies an IP version by its system-defined ID. This IP version is only used by HTTP/HTTPs health checks. Use the Get Available IP Versions (Health Checks) endpoint to retrieve a list of IP versions and their IDs.
PortNumber	An integer that indicates the port to which TCP health checks will be directed.
ReintegrationMethodId	An integer that indicates the method through which an unhealthy server/domain will be integrated back into a group. Use the Get Available Health Check Reintegration Methods endpoint to retrieve a list of reintegration methods and their IDs.
Status	An integer that indicates the server/domain's health check status by its system-defined ID.
StatusName	A string that indicates the server/domain's health check status.
Uri	A string that indicates the URI to which HTTP/HTTPs health checks will be directed.
Record	This response element contains the record's properties.
Name	A string that indicates the record's name.
Rdata	A string that indicates the record's value.
TTL	An integer that indicates the record's TTL.
Weight	An integer that indicates the load balancing weight assigned to the record.

Name	Description
GroupTypeId	An integer that indicates the type of load balancing group by its system-defined ID. This response element will always report "3" which corresponds to zones.
Name	A string that indicates the name of the load balancing group.
Records	This response element describes the records associated with a zone. This section only describes records that do not belong to a load balancing or failover group. **Note:** A null value is returned when the zone does not contain additional records.
RecordType	Each type of record is listed in its own section. Records are returned in the following order. • A • AAAA • CAA • CNAME • MX • NS • PTR • SPF • SRV • TXT This response element contains all of a zone's records for a given type.
Name	A string that indicates a record's name.
Rdata	A string that indicates a record's value.
TTL	An integer that indicates a record's TTL.
Status	An integer that indicates a zone's status by its system-defined ID. Use the Get Available Zone Statuses endpoint to retrieve a list of statuses and their IDs.

Name	Description
Version	An integer that indicates a zone's version. This version is incremented whenever a change is applied to the zone.
ZoneId	An integer that identifies a zone by its system-defined ID.
ZoneType	An integer that indicates a zone's type by its system-defined ID. Use the Get Available Zone Types endpoint to retrieve a list of zone types and their IDs.

Errors

The response body for an unsuccessful request may contain an error element that provides additional information. View common error messages.

Sample Request and Response (JSON)

A sample JSON request is shown below.

```
GET https://api.edgecast.com/v2/mcc/customers/0001/dns/routezone?id=1234 HTTP/1.1
Authorization: TOK:12345678-1234-1234-1234-1234567890ab
Accept: application/json
Host: api.edgecast.com
```

A sample JSON response is shown below.

```
HTTP/1.1 200 OK
Cache-Control: private
Content-Type: application/json; charset=utf-8
Date: Thu, 14 Apr 2016 12:00:00 GMT
Content-Length: 1668


{
        "Comment" : "",
        "DomainName" : "myzone.com.",
        "FailoverGroups" : [{
                    "Group" : {
                            "A" : [],
                            "AAAA" : [],
                            "CNAME" : [{
                                        "HealthCheck" : null,
                                        "IsPrimary" : false,
```

```
                                "Record" : {
                                        "Name" : "web",
                                        "Rdata" : "web01.myzone.com.",
                                        "TTL" : 300
                                }
                        }, {
                                "HealthCheck" : null,
                                "IsPrimary" : true,
                                "Record" : {
                                        "Name" : "web",
                                        "Rdata" : "web02.myzone.com.",
                                        "TTL" : 300
                                }
                        }
                ]
        },
        "GroupTypeId" : 3,
        "Name" : "web"
    }
],
"LoadBalancingGroups" : [{
            "Group" : {
                "A" : [],
                "AAAA" : [],
                "CNAME" : [{
                            "HealthCheck" : null,
                            "Record" : {
                                    "Name" : "mycdn",
                                    "Rdata" : "www.myzone.com.",
                                    "TTL" : 300
                            },
                            "Weight" : 50
                        }, {
                            "HealthCheck" : null,
                            "Record" : {
                                    "Name" : "mycdn",
                                    "Rdata" : "www2.myzone.com.",
                                    "TTL" : 300
```

```
                                               },
                                               "Weight" : 50
                                       }
                               ]
                       },
                       "GroupTypeId" : 3,
                       "Name" : "mycdn"
               }
       ],
       "Records" : {
               "A" : [{
                               "Name" : "www",
                               "Rdata" : "10.55.66.22",
                               "TTL" : 3600
                       }, {
                               "Name" : "www",
                               "Rdata" : "55.66.88.11",
                               "TTL" : 3600
                       }, {
                               "Name" : "www",
                               "Rdata" : "66.77.99.22",
                               "TTL" : 3600
                       }, {
                               "Name" : "www",
                               "Rdata" : "11.66.77.33",
                               "TTL" : 3600
                       }
               ],
               "AAAA" : [{
                               "Name" : "www",
                               "Rdata" : "1:1:1:2:3:4:5:6",
                               "TTL" : 3600
                       }, {
                               "Name" : "www",
                               "Rdata" : "::2",
                               "TTL" : 3600
                       }
               ],
```

```
            "CNAME" : [],
            "MX" : [],
            "NS" : [],
            "SPF" : [],
            "SRV" : [],
            "TXT" : []
        },
        "Status" : 2,
        "Version" : 1234567890,
        "ZoneId" : 1234,
        "ZoneType" : 1
}
```

Update Primary Zone

Updates an entire primary zone by overwriting the previous version with the submitted zone data. All missing zone properties, records, groups, and health checks are treated as deletions.

The recommended method to update a zone is described below.

1. Use the Get Zone endpoint to retrieve the entire zone.

2. The response of the above endpoint should be modified as needed. For example, insert or remove the desired records or load balancing/failover configurations.

3. Set the request body of this endpoint to the zone data updated in step 2.

Request

A request to update a zone is described below.

HTTP Method	Request URI
PUT	https://api.edgecast.com/v2/mcc/customers/*xxxx*/dns/routezone

Define the following terms when submitting the above request:

- **xxxx:** Replace this term with your CDN account number.

Request Headers

This endpoint only takes advantage of common request headers.

Note: This endpoint only supports JSON.

Request Body

The required request parameters for this endpoint are described below.

Name	Description
Comment	A string that assigns a comment to the zone.
DomainName	A string that should be set to the current name assigned to the zone. **Note:** The name assigned to a zone cannot be modified.
FailoverGroups	Define the zone's failover groups within this request parameter.
Group	Define a specific failover group within this request parameter.

[A|AAAA|CNAME]	The name of this request parameter should be set to the record type (i.e., A, AAAA, or CNAME) that will be associated with the group.
	
	Key information:
	
	• A failover group must contain exactly two records of the same type.
	
	• The supported configurations for a failover group are:
	
	  ▪ A records only
	
	  ▪ AAAA records only
	
	  ▪ A and AAAA records
	
	  ▪ CNAME records only

HealthCheck	Define a record's health check configuration within this request parameter.
CheckInterval	An integer that defines the number of seconds between health checks.
CheckTypeId	An integer that defines the type of health check by its system-defined ID. Use the Get Available Health Check Types endpoint to retrieve a list of health check types and their IDs.

Name	Description
ContentVerification	A string that defines the text that will be used to verify the success of the health check.
EmailNotificationAddress	A string that defines the e-mail address to which health check notifications will be sent.
FailedCheckThreshold	An integer that defines the number of consecutive times that the same result must be returned before a health check agent will indicate a change in status.
HTTPMethodId	An integer that defines an HTTP method by its system-defined ID. An HTTP method is only used by HTTP/HTTPs health checks. Use the Get Available HTTP Methods (Health Checks) endpoint to retrieve a list of HTTP methods and their IDs.
IPAddress	A string that defines the IP address (IPv4 or IPv6) to which TCP health checks will be directed.
IPVersion	An integer that defines an IP version by its system-defined ID. This IP version is only used by HTTP/HTTPs health checks. Use the Get Available IP Versions (Health Checks) endpoint to retrieve a list of IP versions and their IDs.
PortNumber	An integer that defines the port to which TCP health checks will be directed.
ReintegrationMethodId	An integer that defines the method through which an unhealthy server/domain will be integrated back into a group. Use the Get Available Health Check Reintegration Methods endpoint to retrieve a list of reintegration methods and their IDs.
Uri	A string that defines the URI to which HTTP/HTTPs health checks will be directed.
IsPrimary	A Boolean that defines whether the current record is the primary server/domain to which traffic will be directed.
Record	Define a record's properties within this request parameter.
Name	A string that defines the record's name.
Rdata	A string that defines the record's value.

Name	Description
TTL	An integer that defines the record's TTL.
GroupTypeId	An integer that should be set to "3."
Name	A string that defines the name of the failover group.
LoadBalancingGroups	Define the zone's load balancing groups within this request parameter.
Group	Define a specific load balancing group within this request parameter.
[A|AAAA|CNAME]	The name of this request parameter should be set to the record type (i.e., A, AAAA, or CNAME) that will be associated with the group. **Key information:** • A load balancing group must contain at least two records of the same type. • The supported configurations for a load balancing group are: ▪ A records only ▪ AAAA records only ▪ A and AAAA records ▪ CNAME records only
HealthCheck	Define a record's health check configuration within this request parameter.
CheckInterval	An integer that defines the number of seconds between health checks.
CheckTypeId	An integer that defines the type of health check by its system-defined ID. Use the Get Available Health Check Types endpoint to retrieve a list of health check types and their IDs.
ContentVerification	A string that defines the text that will be used to verify the success of the health check.
EmailNotificationAddress	A string that defines the e-mail address to which health check notifications will be sent.
FailedCheckThreshold	An integer that defines the number of consecutive times that the same result must be returned before a health check agent will indicate a change in status.

Name				Description
	HTTPMethodId			An integer that defines an HTTP method by its system-defined ID. An HTTP method is only used by HTTP/HTTPs health checks.
				Use the Get Available HTTP Methods (Health Checks) endpoint to retrieve a list of HTTP methods and their IDs.
	IPAddress			A string that defines the IP address (IPv4 or IPv6) to which TCP health checks will be directed.
	IPVersion			An integer that defines an IP version by its system-defined ID. This IP version is only used by HTTP/HTTPs health checks.
				Use the Get Available IP Versions (Health Checks) endpoint to retrieve a list of IP versions and their IDs.
	PortNumber			An integer that defines the port to which TCP health checks will be directed.
	ReintegrationMethodId			An integer that defines the method through which an unhealthy server/domain will be integrated back into a group.
				Use the Get Available Health Check Reintegration Methods endpoint to retrieve a list of reintegration methods and their IDs.
	Uri			A string that defines the URI to which HTTP/HTTPs health checks will be directed.
	Record			Define a record's properties within this request parameter.
		Name		A string that defines the record's name.
		Rdata		A string that defines the record's value.
		TTL		An integer that defines the record's TTL.
		Weight		An integer that defines the load balancing weight assigned to the record.
	GroupTypeId			An integer that should be set to "3."
	Name			A string that defines the name of the load balancing group.
Records				Define the set of records that will be associated with the zone. This section should only describe records that do not belong to a load balancing or failover group.

Name	Description
RecordType	Each type of record is defined in its own section. Create a section for each desired record type. The available record types are: • A • AAAA • CAA • CNAME • MX • NS • PTR • SPF • SRV • TXT
Name	A string that defines a record's name.
Rdata	A string that defines a record's value.
TTL	An integer that defines a record's TTL.
Status	An integer that defines a zone's status by its system-defined ID. Use the Get Available Zone Statuses endpoint to retrieve a list of statuses and their IDs.
Version	An integer that indicates the current version of the zone being updated. **Note:** The specified version number must match the one registered on our system. This prevents a newer version of the zone being overwritten by an older version.
ZoneId	An integer that identifies the zone that will be updated by its system-defined ID.
ZoneType	An integer that indicates that a primary zone will be created. Set this request element to "1."

Response

The response to the above request includes an HTTP status code, response headers, and a response body.

Status Code

A status code indicates whether the request was successfully performed.

Response Headers

The response for this endpoint only includes standard HTTP response headers. View common response headers.

Response Body

The response body for a successful request returns the properties of the updated zone.

Name	Description
Comment	A string that indicates the comment associated with the updated zone.
DomainName	A string that indicates the updated zone's name.
FailoverGroups	This response element contains the set of failover groups associated with the updated zone.
Group	This response element contains a failover group.
[A|AAAA|CNAME]	Each group contains a section for each record type. Records are returned in the following order. • A • AAAA • CNAME This response element contains the following information about a record: • Health check configuration • Properties • Primary status **Note:** If the group does not contain a particular type of record, then that section will remain blank.
HealthCheck	This response element describes the health check configuration associated with a record in the group. **Note:** A null value is returned if a health check configuration has not been defined.
CheckInterval	An integer that indicates the number of seconds between health checks.

Name	Description
CheckTypeId	An integer that identifies a type of health check by its system-defined ID. Use the Get Available Health Check Types endpoint to retrieve a list of health check types and their IDs.
ContentVerification	A string that indicates the text that will be used to verify the success of the health check.
EmailNotificationAddress	A string that indicates the e-mail address to which health check notifications will be sent.
FailedCheckThreshold	An integer that indicates the number of consecutive times that the same result must be returned before a health check agent will indicate a change in status.
HTTPMethodId	An integer that identifies an HTTP method by its system-defined ID. An HTTP method is only used by HTTP/HTTPs health checks. Use the Get Available HTTP Methods (Health Checks) endpoint to retrieve a list of HTTP methods and their IDs.
IPAddress	A string that indicates the IP address (IPv4 or IPv6) to which TCP health checks will be directed.
IPVersion	An integer that identifies an IP version by its system-defined ID. This IP version is only used by HTTP/HTTPs health checks. Use the Get Available IP Versions (Health Checks) endpoint to retrieve a list of IP versions and their IDs.
PortNumber	An integer that indicates the port to which TCP health checks will be directed.
ReintegrationMethodId	An integer that indicates the method through which an unhealthy server/domain will be integrated back into a group. Use the Get Available Health Check Reintegration Methods endpoint to retrieve a list of reintegration methods and their IDs.
Status	An integer that indicates the server/domain's health check status by its system-defined ID.
StatusName	A string that indicates the server/domain's health check status.

Name	Description
Uri	A string that indicates the URI to which HTTP/HTTPs health checks will be directed.
IsPrimary	A Boolean that indicates whether the current record is the primary server/domain to which traffic will be directed.
Record	This response element contains the record's properties.
Name	A string that indicates the record's name.
Rdata	A string that indicates the record's value.
TTL	An integer that indicates the record's TTL.
GroupTypeId	An integer that indicates the type of failover group by its system-defined ID. This response element will always report "3" which corresponds to zones.
Name	A string that indicates the name of the failover group.
LoadBalancingGroups	This response element contains the set of load balancing groups associated with the zone.
Group	This request element contains a load balancing group.
[A|AAAA|CNAME]	Each group contains a section for each record type. Records are returned in the following order. • A • AAAA • CNAME This response element contains the following information about a record: • Health check configuration • Properties • Primary status **Note:** If the group does not contain a particular type of record, then that section will remain blank.

Name	Description
HealthCheck	This response element describes the health check configuration associated with a record in the group.
	Note: A null value is returned if a health check configuration has not been defined.
CheckInterval	An integer that indicates the number of seconds between health checks.
CheckTypeId	An integer that indicates the type of health check by its system-defined ID.
	Use the Get Available Health Check Types endpoint to retrieve a list of health check types and their IDs.
ContentVerification	A string that indicates the text that will be used to verify the success of the health check.
EmailNotificationAddress	A string that identifies the e-mail address to which health check notifications will be sent.
FailedCheckThreshold	An integer that indicates the number of consecutive times that the same result must be returned before a health check agent will indicate a change in status.
HTTPMethodId	An integer that identifies an HTTP method by its system-defined ID. An HTTP method is only used by HTTP/HTTPs health checks.
	Use the Get Available HTTP Methods (Health Checks) endpoint to retrieve a list of HTTP methods and their IDs.
IPAddress	A string that indicates the IP address (IPv4 or IPv6) to which TCP health checks will be directed.
IPVersion	An integer that identifies an IP version by its system-defined ID. This IP version is only used by HTTP/HTTPs health checks.
	Use the Get Available IP Versions (Health Checks) endpoint to retrieve a list of IP versions and their IDs.
PortNumber	An integer that indicates the port to which TCP health checks will be directed.

Name	Description
ReintegrationMethodId	An integer that indicates the method through which an unhealthy server/domain will be integrated back into a group.
	Use the Get Available Health Check Reintegration Methods endpoint to retrieve a list of reintegration methods and their IDs.
Status	An integer that indicates the server/domain's health check status by its system-defined ID.
StatusName	A string that indicates the server/domain's health check status.
Uri	A string that indicates the URI to which HTTP/HTTPs health checks will be directed.
Record	This response element contains the record's properties.
Name	A string that indicates the record's name.
Rdata	A string that indicates the record's value.
TTL	An integer that indicates the record's TTL.
Weight	An integer that indicates the load balancing weight assigned to the record.
GroupTypeId	An integer that indicates the type of load balancing group by its system-defined ID. This response element will always report "3" which corresponds to zones.
Name	A string that indicates the name of the load balancing group.
Records	This response element describes the records associated with the updated zone. This section only describes records that do not belong to a load balancing or failover group.
	Note: A null value is returned when the zone does not contain additional records.

Name	Description
RecordType	Each type of record is listed in its own section. Records are returned in the following order. • A • AAAA • CAA • CNAME • MX • NS • PTR • SPF • SRV • TXT This response element contains all of a zone's records for a given type.
Name	A string that indicates a record's name.
Rdata	A string that indicates a record's value.
TTL	An integer that indicates a record's TTL.
Status	An integer that indicates the updated zone's status by its system-defined ID. Use the Get Available Zone Statuses endpoint to retrieve a list of statuses and their IDs.
Version	An integer that indicates the updated zone's version. This version is incremented whenever a change is applied to the zone.
ZoneId	An integer that identifies the updated zone by its system-defined ID.
ZoneType	An integer that indicates that a primary zone has been updated. This response element will always be set to "1."

Errors

The response body for an unsuccessful request may contain an error element that provides additional information. View common error messages.

Sample Request and Response (JSON)

A sample JSON request is shown below.

```
PUT https://api.edgecast.com/v2/mcc/customers/0001/dns/routezone HTTP/1.1
Authorization: TOK:12345678-1234-1234-1234-1234567890ab
Accept: application/json
Content-Type: application/json
Host: api.edgecast.com
Content-Length: 1718


{
        "Comment" : "",
        "DomainName" : "myzone.com.",
        "FailoverGroups" : [{
                    "Group" : {
                            "A" : [],
                            "AAAA" : [],
                            "CNAME" : [{
                                            "HealthCheck" : null,
                                            "IsPrimary" : false,
                                            "Record" : {
                                                    "Name" : "web",
                                                    "Rdata" : "web01.myzone.com.",
                                                    "TTL" : 300
                                            }
                                    }, {
                                            "HealthCheck" : null,
                                            "IsPrimary" : true,
                                            "Record" : {
                                                    "Name" : "web",
                                                    "Rdata" : "web02.myzone.com.",
                                                    "TTL" : 300
                                            }
                                    }
                            ]
                    },
                    "GroupTypeId" : 3,
                    "Name" : "web"
            }
        ],
        "LoadBalancingGroups" : [{
```

```
                    "Group" : {
                            "A" : [],
                            "AAAA" : [],
                            "CNAME" : [{
                                            "HealthCheck" : null,
                                            "Record" : {
                                                    "Name" : "mycdn",
                                                    "Rdata" : "www.myzone.com.",
                                                    "TTL" : 300
                                            },
                                            "Weight" : 50
                                    }, {
                                            "HealthCheck" : null,
                                            "Record" : {
                                                    "Name" : "mycdn",
                                                    "Rdata" : "www2.myzone.com.",
                                                    "TTL" : 300
                                            },
                                            "Weight" : 50
                                    }
                            ]
                    },
                    "GroupTypeId" : 3,
                    "Name" : "mycdn"
            }
    ],
    "Records" : {
            "A" : [{
                            "Name" : "www",
                            "Rdata" : "10.55.66.22",
                            "TTL" : 3600
                    }, {
                            "Name" : "www",
                            "Rdata" : "55.66.88.11",
                            "TTL" : 3600
                    }, {
                            "Name" : "www",
                            "Rdata" : "66.77.99.22",
```

```
                                "TTL" : 3600
                }, {
                                "Name" : "www",
                                "Rdata" : "11.66.77.33",
                                "TTL" : 3600
                }
        ],
        "AAAA" : [{
                                "Name" : "www",
                                "Rdata" : "1:1:1:2:3:4:5:6",
                                "TTL" : 3600
                }, {
                                "Name" : "www",
                                "Rdata" : "::2",
                                "TTL" : 3600
                }
        ],
        "CNAME" : [],
        "MX" : [],
        "NS" : [],
        "SPF" : [],
        "SRV" : [],
        "TXT" : []
    },
    "Status" : 2,
    "Version" : 1234567890,
    "ZoneId" : 1234,
    "ZoneType" : 1
}
```

A sample JSON response is shown below.

```
HTTP/1.1 200 OK
Cache-Control: private
Content-Type: application/json; charset=utf-8
Date: Thu, 14 Apr 2016 12:00:00 GMT
Content-Length: 1380


{
    "Comment" : "",
```

```
        "DomainName" : "myzone.com.",
        "FailoverGroups" : [{
                    "Group" : {
                        "A" : [],
                        "AAAA" : [],
                        "CNAME" : [{
                                    "HealthCheck" : null,
                                    "IsPrimary" : false,
                                    "Record" : {
                                        "Name" : "web",
                                        "Rdata" : "web01.myzone.com.",
                                        "TTL" : 300
                                    }
                            }, {
                                    "HealthCheck" : null,
                                    "IsPrimary" : true,
                                    "Record" : {
                                        "Name" : "web",
                                        "Rdata" : "web02.myzone.com.",
                                        "TTL" : 300
                                    }
                            }
                        ]
                    },
                    "GroupTypeId" : 3,
                    "Name" : "web"
            }
        ],
        "LoadBalancingGroups" : [{
                    "Group" : {
                        "A" : [],
                        "AAAA" : [],
                        "CNAME" : [{
                                    "HealthCheck" : null,
                                    "Record" : {
                                        "Name" : "mycdn",
                                        "Rdata" : "www.myzone.com.",
                                        "TTL" : 300
```

```
                                                },
                                                "Weight" : 50
                                        }, {
                                                "HealthCheck" : null,
                                                "Record" : {
                                                        "Name" : "mycdn",
                                                        "Rdata" : "www2.myzone.com.",
                                                        "TTL" : 300
                                                },
                                                "Weight" : 50
                                        }
                                ]
                        },
                        "GroupTypeId" : 3,
                        "Name" : "mycdn"
                }
        ],
        "Records" : {
                "A" : [{
                                "Name" : "www",
                                "Rdata" : "10.55.66.22",
                                "TTL" : 3600
                        }, {
                                "Name" : "www",
                                "Rdata" : "55.66.88.11",
                                "TTL" : 3600
                        }, {
                                "Name" : "www",
                                "Rdata" : "66.77.99.22",
                                "TTL" : 3600
                        }, {
                                "Name" : "www",
                                "Rdata" : "11.66.77.33",
                                "TTL" : 3600
                        }
                ],
                "AAAA" : [{
                                "Name" : "www",
```

```
                              "Rdata" : "1:1:1:2:3:4:5:6",
                              "TTL" : 3600
                   }, {
                              "Name" : "www",
                              "Rdata" : "::2",
                              "TTL" : 3600
                   }
          ],
          "CNAME" : [],
          "MX" : [],
          "NS" : [],
          "SPF" : [],
          "SRV" : [],
          "TXT" : []
     },
     "Status" : 2,
     "Version" : 1234567890,
     "ZoneId" : 1234,
     "ZoneType" : 1
}
```

Token-Based Authentication

This section covers how you can perform basic Token-Based Authentication administrative tasks, such as defining authentication directories and updating the primary key that will be used to encrypt/decrypt token data. It also allows you to encrypt Token-Based Authentication parameters as a token value. It is important to note that all of these configuration tasks are platform-specific. Updating the Token-Based Authentication configuration on a particular platform will not affect how Token-Based Authentication works on any other platform.

Add Authentication Directory (Legacy)

Important: This endpoint has been deprecated. Please use the Add Token-Based Authentication Directory endpoint instead.

This legacy endpoint is used to add a platform-specific authentication directory. The proper syntax for requesting this legacy endpoint is provided below.

HTTP Method	Request URI
POST	**https://api.edgecast.com/v2/mcc/customers/*AccountNumber*/token/directory**

Note: For additional information about this legacy endpoint, please refer to the REST API Help Center.

Add Token-Based Authentication Directory

Adds a platform-specific directory that will require authentication. Keep in mind that Token-Based Authentication is applied recursively to each authentication directory.

Note: It may take up to an hour for this change to take effect.

Request

A request to add an authentication directory is described below. When submitting this request, you will need to define the following term:

- **AccountNumber:** This term should be replaced by your CDN account number. This number can be found in the upper-right hand corner of the MCC.

HTTP Method	Request URI
POST	https://api.edgecast.com/v2/mcc/customers/*AccountNumber*/token/directories

Request Headers

This endpoint only takes advantage of the common request headers described in the **Request Headers** section of the **Request and Response Elements** topic.

Request Body

The required request parameters for this endpoint are described below.

Name	Description
Directory	Required. A string that indicates the relative path to the authentication directory. The starting point for this relative path varies according to origin server type.
	• **CDN Origin Server:** The root folder for your CDN storage account can be specified using a forward slash (i.e., /). If you would like to specify a different folder, simply append the relative path to that folder (e.g., /Presentations/2011).
	• **Customer Origin Server:** The root folder for your customer origin server can be specified by typing a forward slash, the name of your customer origin server, and then another forward slash (e.g., /MyCustomerOrigin/). If you would like to specify a different folder, simply append the relative path to that folder (e.g., /MyCustomerOrigin/Presentations/2011).
	Reminder: This configuration will only secure the specified location for the platform specified by the MediaType parameter. Please make sure to set up Token-Based Authentication on other platforms to ensure that the content in question requires authentication.
MediaTypeId	Required. An integer that indicates the service on which a new authentication directory will be defined. It should be replaced with the ID associated with the desired service. Valid values are:
	• **3:** HTTP Large
	• **8:** HTTP Small
	• **14:** Application Delivery Network (ADN)

Response

The response to the above request includes an HTTP status code, response headers, and a response body.

Status Code

A status code indicates whether the request was successfully performed. A list of common status codes is provided in the **Status Codes and Error Messages** topic.

Response Headers

The response for this endpoint only returns standard HTTP response headers including those described in the **Response Headers** section of the **Request and Response Elements** topic.

Response Body

The response body for a successful request contains the following response element:

Name	Description
Id	An integer that indicates the unique ID assigned to the new authentication directory.

Errors

The response body for an unsuccessful request may contain an error element that provides additional information. For a list of common error messages, please refer to the **Status Codes and Error Messages** topic.

Sample Request and Response

A sample JSON request is provided below.

```
POST https://api.edgecast.com/v2/mcc/customers/0001/token/directories HTTP/1.1

Authorization: TOK:12345678-1234-1234-1234-1234567890ab

Accept: application/json

Content-Type: application/json

Host: api.edgecast.com

Content-Length: 71


{

        "Directory":"\/MyCustomerOrigin\/Presentations",

        "MediaTypeId":3

}
```

A sample JSON response is provided below.

```
HTTP/1.1 200 OK

Cache-Control: private

Content-Type: application/xml; charset=utf-8

Date: Thu, 14 Apr 2016 12:00:00 GMT

Content-Length: 14


{

        "Id":123

}
```

Delete Token-Based Authentication Directory

Deletes an authentication directory.

Note: It may take up to an hour for this change to take effect.

Request

A request to delete an authentication directory is described below. When submitting this request, you will need to define the following terms:

- **AccountNumber:** This term should be replaced by your CDN account number. This number can be found in the upper-right hand corner of the MCC.

- **TBADirectoryID:** This term should be replaced by the unique system-defined ID associated with the desired authentication directory. This ID can be returned through the Get All Token-Based Authentication Directories endpoint.

HTTP Method	Request URI
DELETE	https://api.edgecast.com/v2/mcc/customers/*AccountNumber*/token/directories/*TBADirectoryID*

Request Headers

This endpoint only takes advantage of the common request headers described in the **Request Headers** section of the **Request and Response Elements** topic.

Request Body

Request body parameters are not required by this endpoint.

Response

The response to the above request includes an HTTP status code, response headers, and a response body.

Status Code

A status code indicates whether the request was successfully performed. A list of common status codes is provided in the **Status Codes and Error Messages** topic.

Response Headers

The response for this endpoint only returns standard HTTP response headers including those described in the **Response Headers** section of the **Request and Response Elements** topic.

Response Body

The response body for a successful request does not contain a response element.

The response body for an unsuccessful request may contain an error element that provides additional information. For a list of common error messages, please refer to the **Status Codes and Error Messages** topic.

Sample Request and Response

The request format is identical for both JSON and XML. A sample request is shown below.

```
DELETE https://api.edgecast.com/v2/mcc/customers/0001/token/directories/123 HTTP/1.1
Authorization: TOK:12345678-1234-1234-1234-1234567890ab
Host: api.edgecast.com
```

The response is identical for both JSON and XML. A sample response is shown below.

```
HTTP/1.1 200 OK
Cache-Control: private
Date: Thu, 14 Apr 2016 12:00:00 GMT
```

Encrypt Token Data

Important: You should upgrade to Token-Based Authentication 3.0. Learn more (CDN Help Center).

Tip: Set the TokenVersion request body parameter to "V3" to generate tokens using encryption version 3.0.

Encrypts data for use with Token-Based Authentication. This encryption process does not alter the configuration of your customer account. It is only provided for your convenience. Leverage this method to generate token values that may be used when linking to content that requires authentication.

Request

A request to encrypt data as a token value is described below.

HTTP Method	Request URI
PUT	https://api.edgecast.com/v2/mcc/token/encrypt

Request Headers

This endpoint only takes advantage of the common request headers described in the **Request Headers** section of the **Request and Response Elements** topic.

Request Body

The required request parameters for this endpoint are described below.

Name	Description
Key	Required. A string that indicates the primary Token-Based Authentication key associated with the specified platform.
TokenParameter	Required. A string that identifies the criteria that a user agent must meet before an asset will be served to that client. The format for each criterion is the token parameter, an equal sign, and the value that the client must meet. If you would like to specify multiple requirements, then each token parameter/value pair must be delimited using an ampersand (e.g., ec_expire=1356955200&ec_country_deny=CA&ec_country_allow=US,MX) .
	Tip: You can generate this syntax through the encrypt tool that is provided from the **Token-Based Authentication** page in the MCC.
	Tip: An ampersand (&) is a reserved character in XML. Therefore, you must specify each ampersand using its entity reference (i.e., &).
TokenVersion	A string that identifies the encryption version that will be used to generate the token. Valid values are: • **V3:** Generates a token using encryption version 3.0. This is the recommended value. • **V2:** Generates a token using encryption version 2.0. **Default Behavior:** The token will be encrypted using the specified key's minimum encryption version. If the specified key doesn't exist, then the token will be encrypted using version 2.0.

Response

The response to the above request includes an HTTP status code, response headers, and a response body.

Status Code

A status code indicates whether the request was successfully performed. A list of common status codes is provided in the **Status Codes and Error Messages** topic.

Response Headers

The response for this endpoint only returns standard HTTP response headers including those described in the **Response Headers** section of the **Request and Response Elements** topic.

Response Body

The response body for a successful request contains the following response element:

Name	Description
Token	A string that indicates the encrypted token value generated from the criteria specified in the TokenParameter request parameter. This token value can be specified as a query string parameter in a request URL to gain access to content secured by Token-Based Authentication.

Errors

The response body for an unsuccessful request may contain an error element that provides additional information. For a list of common error messages, please refer to the **Status Codes and Error Messages** topic.

Sample Request and Response

A sample JSON request is provided below.

```
PUT https://api.edgecast.com/v2/mcc/token/encrypt HTTP/1.1

Authorization: TOK:12345678-1234-1234-1234-1234567890ab

Accept: application/json

Content-Type: application/json

Host: api.edgecast.com

Content-Length: 107


{

    "Key" : "MyPrimaryKeyTBA",

    "TokenParameter" :
    "ec_expire=1356955200&ec_country_deny=CA&ec_country_allow=US,MX",

    "TokenVersion" : "V3"

}
```

A sample JSON response is provided below.

```
HTTP/1.1 200 OK

Cache-Control: private

Content-Length: 174

Content-Type: application/xml; charset=utf-8

Date: Thu, 14 Apr 2016 12:00:00 GMT

{

    "Token" :
    "c17fe661298545b8c6c39808e4c6c32a87a215a1d3bfdb2ebd2ec06c9ce42538767ce212e8aa
    17689f1511033fdd302f98a487abc821bf3726b845afeded843c79b82686f46d61da6a296e3b"

}
```

Get All Token-Based Authentication Directories

This method retrieves a platform-specific list of authentication directories.

Request

A request to retrieve a list of authentication directories is described below. When submitting this request, you will need to define the following terms:

- **AccountNumber:** This term should be replaced by your CDN account number. This number can be found in the upper-right hand corner of the MCC.

- **MediaTypeID:** This term should be replaced by the ID associated with the desired platform. Valid values for this parameter are listed below.

  - **3:** HTTP Large
  - **8:** HTTP Small
  - **14:** Application Delivery Network (ADN)

HTTP Method	Request URI
GET	https://api.edgecast.com/v2/mcc/customers/*AccountNumber*/token/directories?mediatypeid=*MediaTypeID*

Request Headers

This endpoint only takes advantage of the common request headers described in the **Request Headers** section of the **Request and Response Elements** topic.

Request Body

Request body parameters are not required by this endpoint.

Response

The response to the above request includes an HTTP status code, response headers, and a response body.

Status Code

A status code indicates whether the request was successfully performed. A list of common status codes is provided in the **Status Codes and Error Messages** topic.

Response Headers

The response for this endpoint only returns standard HTTP response headers including those described in the **Response Headers** section of the **Request and Response Elements** topic.

Response Body

The response body for a successful request contains the following response elements for each directory returned by this endpoint:

Name	Description
Id	An integer that indicates the unique ID assigned to an authentication directory.
Directory	A string that indicates the relative path to an authentication directory.
MediaTypeId	An integer that indicates an authentication directory's platform. Valid values for this response element are: • **3:** HTTP Large • **8:** HTTP Small • **14:** Application Delivery Network (ADN)

Errors

The response body for an unsuccessful request may contain an error element that provides additional information. For a list of common error messages, please refer to the **Status Codes and Error Messages** topic.

Sample Request and Response

A sample JSON request is provided below.

```
GET https://api.edgecast.com/v2/mcc/customers/0001/token/directories?mediatypeid=3
HTTP/1.1

Authorization: TOK:12345678-1234-1234-1234-1234567890ab

Accept: application/json

Host: api.edgecast.com
```

A sample JSON response is provided below.

```
HTTP/1.1 200 OK

Cache-Control: private

Content-Type: application/xml; charset=utf-8

Date: Thu, 14 Apr 2016 12:00:00 GMT

Content-Length: 184


[{

            "Id" : 123,

            "Directory" : "\/MyCustomerOrigin\/Presentations",

            "MediaTypeId" : 3

      }, {

            "Id" : 124,

            "Directory" : "\/MyCustomerOrigin\/Documents",

            "MediaTypeId" : 3
```

```
        }
    ]
```

Get Token-Based Authentication Directory

Retrieves information about an authentication directory.

Request

A request to retrieve an authentication directory is described below. When submitting this request, you will need to define the following terms:

- **AccountNumber:** This term should be replaced by your CDN account number. This number can be found in the upper-right hand corner of the MCC.

- **TBADirectoryID:** This term should be replaced by the unique system-defined ID associated with the desired authentication directory. This ID can be returned through the Get All Token-Based Authentication Directories endpoint.

HTTP Method	Request URI
GET	https://api.edgecast.com/v2/mcc/customers/*AccountNumber*/token/directories/*TBADirectoryID*

Request Headers

This endpoint only takes advantage of the common request headers described in the **Request Headers** section of the **Request and Response Elements** topic.

Request Body

Request body parameters are not required by this endpoint.

Response

The response to the above request includes an HTTP status code, response headers, and a response body.

Status Code

A status code indicates whether the request was successfully performed. A list of common status codes is provided in the **Status Codes and Error Messages** topic.

Response Headers

The response for this endpoint only returns standard HTTP response headers including those described in the **Response Headers** section of the **Request and Response Elements** topic.

Response Body

The response body for a successful request contains the following response elements:

Name	Description
Id	An integer that indicates the unique ID assigned to an authentication directory.
Directory	A string that indicates the relative path to an authentication directory.
MediaTypeId	An integer that indicates an authentication directory's platform. Valid values for this response element are: • **3:** HTTP Large • **8:** HTTP Small • **14:** Application Delivery Network (ADN)

Errors

The response body for an unsuccessful request may contain an error element that provides additional information. For a list of common error messages, please refer to the **Status Codes and Error Messages** topic.

Sample Request and Response

A sample JSON request is provided below.

```
GET https://api.edgecast.com/v2/mcc/customers/0001/token/directories/123 HTTP/1.1
Authorization: TOK:12345678-1234-1234-1234-1234567890ab
Accept: application/json
Host: api.edgecast.com
```

A sample JSON response is provided below.

```
HTTP/1.1 200 OK
Cache-Control: private
Content-Type: application/xml; charset=utf-8
Date: Thu, 14 Apr 2016 12:00:00 GMT
Content-Length: 88

{
      "Id" : 123,
      "Directory" : "\/MyCustomerOrigin\/Presentations",
      "MediaTypeId" : 3
}
```

Update Primary Key

Important: You should upgrade to Token-Based Authentication 3.0. Learn more (CDN Help Center).

Tip: Set the MinVersion request body parameter to "V3" to only allow the new key to encrypt/decrypt tokens using version 3.0.

Updates the primary Token-Based Authentication key associated with the specified platform. This key is used by our servers to encrypt and decrypt a token value.

Important: The update of a primary key may take up to an hour to take effect. However, a response will be returned immediately.

Warning: This endpoint should be used with care. The safest method for updating your primary key is to do so through the **Token-Based Authentication** page in the MCC. Continuous access to your content cannot be guaranteed when a backup key is not used. For more information, please refer to the **Token-Based Authentication Administration Guide**.

Request

A request to update a primary key is described below. When submitting this request, you will need to define the following term:

- **AccountNumber:** This term should be replaced by your CDN account number. This number can be found in the upper-right hand corner of the MCC.

HTTP Method	Request URI
PUT	https://api.edgecast.com/v2/mcc/customers/*AccountNumber*/token/key

Request Headers
This endpoint only takes advantage of the common request headers described in the **Request Headers** section of the **Request and Response Elements** topic.

Request Body
The required request parameters for this endpoint are described below.

Name	Description
Key	Required. A string that updates the value assigned to the primary Token-Based Authentication key associated with the specified platform. Only alphanumeric characters are supported by this string value.

Name	Description
MediaType	Required. An integer that indicates the service whose primary key will be updated. It should be replaced with the ID associated with the desired service. Valid values are: • **3:** HTTP Large • **8:** HTTP Small • **14:** Application Delivery Network (ADN)
MinVersion	A string that indicates the minimum encryption version that will be assigned to the new primary encryption key. Valid values are: • **V3:** Indicates that the new primary key may only be used to encrypt/decrypt tokens generated using version 3.0. This is the recommended value. • **V2:** Indicates that the new primary key may be used to encrypt/decrypt tokens generated using version 2.0 or 3.0. **Default Behavior:** The new key will be assigned the same minimum encryption version as the previous primary key. If a minimum encryption version was not manually defined for the previous primary key, then the new primary key will be assigned to V2.

Response

The response to the above request includes an HTTP status code, response headers, and a response body.

Status Code

A status code indicates whether the request was successfully performed. A list of common status codes is provided in the **Status Codes and Error Messages** topic.

Response Headers

The response for this endpoint only returns standard HTTP response headers including those described in the **Response Headers** section of the **Request and Response Elements** topic.

Response Body

The response body for a successful request does not contain a response element.

Errors

The response body for an unsuccessful request may contain an error element that provides additional information. For a list of common error messages, please refer to the **Status Codes and Error Messages** topic.

Sample Request and Response

A sample JSON request is provided below.

```
PUT https://api.edgecast.com/v2/mcc/customers/0001/token/key HTTP/1.1

Authorization: TOK:12345678-1234-1234-1234-1234567890ab

Accept: application/json

Content-Type: application/json

Host: api.edgecast.com

Content-Length: 41


{

        "Key":"MyPrimaryKeyTBA",

        "MediaType":3,

        "MinVersion" : "V3"

}
```

A sample JSON response is provided below.

```
HTTP/1.1 200 OK

Cache-Control: private

Content-Type: application/xml; charset=utf-8

Date: Thu, 14 Apr 2016 12:00:00 GMT
```

Update Token-Based Authentication Directory

Updates an authentication directory.

Request

A request to update an authentication directory is described below. When submitting this request, you will need to define the following terms:

- **AccountNumber:** This term should be replaced by your CDN account number. This number can be found in the upper-right hand corner of the MCC.

- **TBADirectoryID:** This term should be replaced by the unique system-defined ID associated with the desired authentication directory. This ID can be returned through the Get All Token-Based Authentication Directories endpoint.

HTTP Method	Request URI
PUT	https://api.edgecast.com/v2/mcc/customers/*AccountNumber*/token /directories/*TBADirectoryID*

Request Headers

This endpoint only takes advantage of the common request headers described in the **Request Headers** section of the **Request and Response Elements** topic.

Request Body

A required request parameter for this endpoint is described below.

Name	Description
Directory	A string that determines the relative path to an authentication directory.

Response

The response to the above request includes an HTTP status code, response headers, and a response body.

Status Code

A status code indicates whether the request was successfully performed. A list of common status codes is provided in the **Status Codes and Error Messages** topic.

Response Headers

The response for this endpoint only returns standard HTTP response headers including those described in the **Response Headers** section of the **Request and Response Elements** topic.

Response Body

The response body for a successful request does not contain a response element.

The response body for an unsuccessful request may contain an error element that provides additional information. For a list of common error messages, please refer to the **Status Codes and Error Messages** topic.

Sample Request and Response

A sample JSON request is provided below.

```
PUT https://api.edgecast.com/v2/mcc/customers/0001/token/directories/123 HTTP/1.1

Authorization: TOK:12345678-1234-1234-1234-1234567890ab

Accept: application/json

Host: api.edgecast.com

Content-Length: 55


{

        "Directory" : "\/MyCustomerOrigin\/Presentations"

}
```

A sample JSON response is provided below.

```
HTTP/1.1 200 OK

Cache-Control: private

Content-Type: application/xml; charset=utf-8

Date: Thu, 14 Apr 2016 12:00:00 GMT
```

Web Application Firewall (WAF) – Threat Event Log

The methods described in this section are designed to retrieve WAF event log information.

Get Available Event Log Fields

This method provides a list of the available event log fields and their definitions.

Note: This method only supports JSON.

Request

A request to retrieve event log fields is described below. When submitting this request, you will need to define the following terms:

- **AccountNumber:** This term should be replaced by your CDN account number. This number can be found in the upper-right hand corner of the MCC.

HTTP Method	Request URI
GET	https://api.edgecast.com/v2/mcc/customers/*AccountNumber*/waf/eventlogs/fields

Request Headers

This endpoint only takes advantage of the common request headers described in the **Request Headers** section of the **Request and Response Elements** topic.

Request Body

Request body parameters are not required by this endpoint.

Response

The response to the above request includes an HTTP status code, response headers, and a response body.

Status Code

A status code indicates whether the request was successfully performed. A list of common status codes is provided in the **Status Codes and Error Messages** topic.

Response Headers

The response for this endpoint only returns standard HTTP response headers including those described in the **Response Headers** section of the **Request and Response Elements** topic.

Response Body

The response body for a successful request contains the following response elements:

Name	Data Type	Description
fields		This response element contains the set of available fields.
name	String	Indicates the name of a field.
data_type	String	Indicates the field's data type (e.g., string or number).
description	String	Describes the field's purpose.

Errors

The response body for an unsuccessful request may contain an error element that provides additional information. For a list of common error messages, please refer to the **Status Codes and Error Messages** topic.

Sample Request and Response

A sample JSON request is provided below.

```
GET https://api.edgecast.com/v2/mcc/customers/0001/waf/eventlogs/fields HTTP/1.1
```

```
Authorization: TOK:12345678-1234-1234-1234-1234567890ab

Accept: application/json

Host: api.edgecast.com
```

A sample JSON response is provided below.

```
HTTP/1.1 200 OK

Cache-Control: private

Content-Type: application/json; charset=utf-8

Date: Thu, 14 Apr 2016 12:00:00 GMT

Content-Length: 2475

{

    "fields" : [{

                "name" : "Timestamp",

                "data_type" : "date",

                "description" : "timestamp of log entry as UTC timestamp"

        }, {

                ...

                "name" : "id",

                "data_type" : "string",

                "description" : "ID of WAF event"

        }

    ]

}
```

Get Event Count

This method returns the total number of events that occurred during the specified time period.

Note: This method only supports JSON.

Request

A request to find out the total number of events for a specified time period is described below. When submitting this request, you will need to define the following terms:

- **AccountNumber:** This term should be replaced by your CDN account number. This number can be found in the upper-right hand corner of the MCC.

- **StartDateTime:** Required. Replace this variable with the start date/time for the report. Only activity that took place after the specified date/time will be included in the report. **Format:** *YYYY-MM-DD*T*hh*:*mm*:*ss*

- **EndDateTime:** Required. Replace this variable with the end date/time for the report. Activity that took place after the specified date/time will not be included in the report. **Format:** *YYYY-MM-DD*T*hh*:*mm*:*ss*

Note: Time (i.e., T*hh*:*mm*:*ss*) is optional. If time is not specified, then a default time (i.e., 00:00:00) will be used.

Note: For more information on date/time format, please refer to **Appendix B: Report Date/Time Format**.

HTTP Method	Request URI
GET	https://api.edgecast.com/v2/mcc/customers/*AccountNumber*/waf/eventlogs /count?start_time=*StartDateTime*&end_time=*EndDateTime*

Request Headers

This endpoint only takes advantage of the common request headers described in the **Request Headers** section of the **Request and Response Elements** topic.

Request Body

Request body parameters are not required by this endpoint.

Response

The response to the above request includes an HTTP status code, response headers, and a response body.

Status Code

A status code indicates whether the request was successfully performed. A list of common status codes is provided in the **Status Codes and Error Messages** topic.

Response Headers

The response for this endpoint only returns standard HTTP response headers including those described in the **Response Headers** section of the **Request and Response Elements** topic.

Response Body

The response body for a successful request contains the following response elements:

Name	Data Type	Description
Count	Integer	Indicates the total number of events that occurred during the specified time period.

Errors

The response body for an unsuccessful request may contain an error element that provides additional information. For a list of common error messages, please refer to the **Status Codes and Error Messages** topic.

Sample Request and Response

A sample JSON request is provided below.

```
GET
https://api.edgecast.com/v2/mcc/customers/0001/waf/eventlogs/count?start_time=2014-
10-20&end_time=2014-10-31 HTTP/1.1

Authorization: TOK:12345678-1234-1234-1234-1234567890ab

Accept: application/json

Host: api.edgecast.com
```

A sample JSON response is provided below.

```
HTTP/1.1 200 OK

Cache-Control: private

Content-Type: application/json; charset=utf-8

Date: Thu, 14 Apr 2016 12:00:00 GMT

Content-Length: 24


{

        "count" : 3335091

}
```

Get Event Log Entries

This method returns paginated event log data. This data can be filtered by:

- Time Period

- Field values

Note: A request for event log entries may return information on thousands of requests. Due to the amount of time that it would take to transmit this data, the response for this method has been split up into pages. Retrieve all events that match the specified criteria by requesting each page. Use the page_of response element in your script to cycle through each page.

Note: This method only supports JSON.

Request

A request to retrieve event log data is described below. When submitting this request, you will need to define the following terms:

- **AccountNumber:** This term should be replaced by your CDN account number. This number can be found in the upper-right hand corner of the MCC.

- **StartDateTime:** Replace this variable with the start date/time for the report. Only activity that took place after the specified date/time will be included in the report. **Format:** *YYYY-MM-DD*T*hh*:*mm*:*ss*

  Important: A valid request must either include or exclude both date/time parameters (i.e., start_time and end_time).

  Note: Omitting both date/time parameters (i.e., start_time and end_time) will return data for 24 hours prior to the time when the request was submitted.

- **EndDateTime:** Replace this variable with the end date/time for the report. Activity that took place after the specified date/time will not be included in the report. **Format:** *YYYY-MM-DD*T*hh*:*mm*:*ss*

- **Filters:** Replace this variable with the desired filter(s).

  - Specify one or more filters using URL-encoded JSON.

  - Only events that satisfy all specified filters may be returned by this method.

  - Specify a field name and a value for each desired filter.

  - Field names and values are case-sensitive.

  - Use a comma to delimit each filter.

  - Set up a filter that can be satisfied by multiple values by comma-delimiting each value within brackets.

  - A "starts with" match may be defined by appending an asterisk (i.e., *) to the desired value. Any other usage of an asterisk wildcard is unsupported.

- **PageNumber:** Replace this variable with the page number that will be returned. This method will only include log events corresponding to that page in the response.

  Note: Omitting the page query string parameter in the request will return the first page.

- **ItemsPerPage:** Replace this variable with the number of log events that may be included on each page. The number of items per page determines the number of pages that may be returned.

  Note: Omitting the page_size query string parameter in the request will return a maximum of 100 log events per page.

  Note: The maximum value for this variable is 1000.

Note: Time (i.e., T*hh*:*mm*:*ss*) is optional. If time is not specified, then a default time (i.e., 00:00:00) will be used.

Note: For more information on date/time format, please refer to **Appendix B: Report Date/Time Format**.

HTTP Method	Request URI
GET	https://api.edgecast.com/v2/mcc/customers/*AccountNumber*/waf/eventlogs ?start_time=*StartDateTime*&end_time=*EndDateTime*&filters=*Filters*&page= *PageNumber*&page_size=*ItemsPerPage*

Request Headers

This endpoint only takes advantage of the common request headers described in the **Request Headers** section of the **Request and Response Elements** topic.

Request Body

Request body parameters are not required by this endpoint.

Response

The response to the above request includes an HTTP status code, response headers, and a response body.

Status Code

A status code indicates whether the request was successfully performed. A list of common status codes is provided in the **Status Codes and Error Messages** topic.

Response Headers

The response for this endpoint only returns standard HTTP response headers including those described in the **Response Headers** section of the **Request and Response Elements** topic.

Response Body

The response body for a successful request reports:

- **Basic Event Information:** Each element in the events array describes the request and the client that committed the violation(s).

- **Sub Events:** Specific information about each rule violation will be reported under the Sub Events parameter.

Note: This endpoint only returns event fields (e.g., Epoch Time or Matched On) that contain data. Therefore, the set of event fields returned by this endpoint may vary by event.

Name	Data Type	Description
events	Array	Contains a list of fields for each event reported on this page. **Note:** Only fields that contain data for the event being reported will be included in the response. This means that the set of fields reported for each event may vary.
page	Integer	Indicates the number of the page that was returned.
page_of	Integer	Indicates the total number of pages required to return the event log data that matches the criteria defined in the request. The total number of pages is determined as indicated below. (# of Eligible Log Events) / (ItemsPerPage) The result of the above formula is rounded up to the nearest whole integer.
time_from	Number (floating-point)	Indicates the report's start date/time, in seconds, using Unix time. **Syntax:** *Seconds*.0
time_to	Number (floating-point)	Indicates the report's end date/time, in seconds, using Unix time. **Syntax:** *Seconds*.0

events Array

The events array contains an object for each event reported on this page. The members of this object are described below.

Name	Data Type	Description
Acl ID	String	Reserved for future use.
Acl Name	String	Reserved for future use.

Name	Data Type	Description
Action Type	String	Indicates the action that was triggered as a result of the violation. Valid values are: • **ALERT:** This term has been deprecated in favor of NOP. • **BLOCK_REQUEST:** Indicates that the request that violated a rule was blocked. • **BLOCK:** This term has been deprecated in favor of BLOCK_REQUEST. • **NOP:** Indicates that an alert was generated in response to the rule violation. • **REDIRECT_302:** Indicates that the request that violated a rule was redirected to the URL associated with the instance defined by the **Instance Name** parameter. • **CUSTOM_RESPONSE:** Indicates that a custom response was returned to the client that submitted a request that violated a rule.
Bots ID	String	Reserved for future use.
Bots Name	String	Reserved for future use.
City Name	String	Identifies the city from which the request originated.
Client IP	String	Identifies the IP address of the client from which the violation originated.
Country Code	String	Identifies the country from which the request originated by its country code.
Country Name	String	Identifies the country from which the request originated.
Epoch Time	Number (floating-point)	Indicates the Unix time, in seconds, at which the violation took place. **Syntax:** *Seconds.Microseconds*

Name	Data Type	Description
Event ID	String	Indicates the unique ID assigned to the event. **Tip:** Pass this ID to the Get Event Log Entry endpoint to retrieve this event log entry.
Host	String	Indicates the hostname that was requested.
id	String	Indicates the hash value for the event's ID.
Instance Name	String	Indicates the name of the instance that activated the profile containing the rule that the requested violated.
Matched Data	String	**Signature Detection Mode Only** Deprecated. Indicates the client-side data that triggered the violation. For example, this parameter may report a client's IP address or a portion of the URL that violated the request.
Matched On	String	**Signature Detection Mode Only** Deprecated. Indicates the variable that identifies where the violation was found.
Matched Value	String	Deprecated. Indicates the value of the variable defined in the Matched On parameter.
Profile Name	String	Indicates the name of the profile that triggered the violation.
Profile Type	String	Indicates whether the request was screened as a result of an instance's production or audit profile. Valid values are: • PRODUCTION • AUDIT
Referer	String	Indicates the request's referrer as defined by the Referer request header.
Rule ID	Integer	**Note:** This parameter has been deprecated. **Note:** The ID for each rule that was violated is reported under the Sub Events parameter.

Name	Data Type	Description
Rule Message	String	Provides the following basic information about the anomaly score violation(s). Inbound Anomaly Score Exceeded (Total Score: *#*, SQLi=*#*, XSS=*#*): Last Matched Message: *RuleID-RuleMessage*
Rule Policy	String	Indicates the name of the policy that was violated.
Rule Severity	Integer	**Signature Detection Mode Only** Deprecated. Indicates the severity of the violation. This value may range from -1 to 6 where 6 represents the lowest severity level.
Rule Tags	Array	Indicates the tags associated with the rule that the request violated. These tags may be used to determine whether a rule, access control, or global setting was violated.
Rules Config ID	String	Reserved for future use.
Rules Config Name	String	Reserved for future use.
Scope ID	String	Reserved for future use.
Scope Name	String	Reserved for future use.
Sub Event Count	Integer	Indicates the total number of sub events.
Sub Events	Array	Contains a list of fields that describe each sub event associated with the current event. A sub event is reported for each rule violation incurred by a request.
Timestamp	String	Indicates the date and time (GMT) at which the violation took place. **Format:** *YYYY-MM-DD*T*hh*:*mm*:*ss.fffffff*Z
URL	String	Indicates the URL that was requested.
User Agent	String	Indicates the user agent that submitted the request that triggered the rule violation.

Sub Events Array

The Sub Events array contains an object that describe each sub event associated with the current event. A sub event is reported for each rule violation incurred by a request.

Name	Data Type	Description
Matched Data	String	Deprecated. Indicates the client-side data that triggered the violation. For example, this parameter may report a client's IP address or a portion of the URL that violated the request.
Matched On	String	Indicates the variable that identifies where the violation was found.
Matched Value	String	Indicates the value of the variable defined in the Matched On parameter.
Rule ID	Integer	Indicates the ID for the rule that the request violated.
Rule Message	String	Provides a description of the rule that the request violated.
Rule Severity	Integer	Indicates the severity of the violation. This value may range from -1 to 6 where 6 represents the lowest severity level.
Total Anomaly Score	Integer	Indicates the total anomaly score for the current rule violation. This score is calculated by summing the anomaly score of the current rule violation with all rule violations reported above this sub event.

Errors

The response body for an unsuccessful request may contain an error element that provides additional information. For a list of common error messages, please refer to the **Status Codes and Error Messages** topic.

Sample Request and Response

A sample JSON request is provided below.

```
GET https://api.edgecast.com/v2/mcc/customers/0001/waf/ eventlogs?start_time=2016-09-
01&end_time=2016-09-12&page_size=2 HTTP/1.1

Authorization: TOK:12345678-1234-1234-1234-1234567890ab

Accept: application/json

Host: api.edgecast.com
```

A sample JSON response is provided below.

```
HTTP/1.1 200 OK

Cache-Control: private

Content-Type: application/json; charset=utf-8

Date: Thu, 14 Apr 2016 12:00:00 GMT

Content-Length: 2676

{
        "page_of" : 100,
        "time_to" : 1473638400.0,
        "time_from" : 1472688000.0,
        "events" : [{
                    "Epoch Time" : 1473207640.345809,
                    "Profile Type" : "PRODUCTION",
                    "Client IP" : "192.12.22.25",
                    "Rule Message" : "Inbound Anomaly Score Exceeded (Total Score:
        5, SQLi=3, XSS=0): Last Matched Message: 981255-Detects MSSQL code execution
        and information gathering attempts",
                    "Sub Event Count" : 1,
                    "Timestamp" : "2016-09-07T00:20:40.345809Z",
                    "URL" : "http://www.mydomain.com/mywebpage.html",
                    "Country Code" : "US",
                    "Rule Policy" : "Inbound blocking",
                    "Action Type" : "CUSTOM_RESPONSE",
                    "Host" : "www.mydomain.com",
                    "Instance Name" : "My Instance",
                    "Profile Name" : "My Profile",
                    "Rule Tags" : "OWASP_CRS/ANOMALY/EXCEEDED",
                    "Sub Events" : [{
                                "Matched On" : "ARGS:a",
                                "Rule Message" : "Detects MSSQL code execution
        and information gathering attempts",
```

```
                                "Matched Data" : "'select *",

                                "Total Anomaly Score" : 5,

                                "Rule ID" : 981255,

                                "Rule Severity" : 2,

                                "Matched Value" : "'select * from site'"

                    }

              ],

              "User Agent" : "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_11_6)
    AppleWebKit/537.36 (KHTML, like Gecko) Chrome/52.0.2743.116 Safari/537.36",

              "id" :
    "udidK2wtEHpw4OQkoQKa3JI06QAeUKXwYqM_dgbsuvYwygOWO_uTVGQPxR5ELPpJ19wTpnflk7yn
    rIJzAMH2tA=="

        }, {

              "Epoch Time" : 1473207637.5252609,

              "Profile Type" : "PRODUCTION",

              "Client IP" : "192.144.23.52",

              "Rule Message" : "Inbound Anomaly Score Exceeded (Total Score:
    5, SQLi=3, XSS=0): Last Matched Message: 981255-Detects MSSQL code execution
    and information gathering attempts",

              "Sub Event Count" : 1,

              "Timestamp" : "2016-09-07T00:20:37.525261Z",

              "URL" : "http://www.mydomain.com/mywebpage.html",

              "Country Code" : "US",

              "Rule Policy" : "Inbound blocking",

              "Action Type" : "CUSTOM_RESPONSE",

              "Host" : "www.mydomain.com",

              "Instance Name" : "My Instance",

              "Profile Name" : "My Profile",

              "Rule Tags" : "OWASP_CRS/ANOMALY/EXCEEDED",

              "Sub Events" : [{

                                "Matched On" : "ARGS:a",

                                "Rule Message" : "Detects MSSQL code execution
    and information gathering attempts",

                                "Matched Data" : "'select *",

                                "Total Anomaly Score" : 5,

                                "Rule ID" : 981255,

                                "Rule Severity" : 2,

                                "Matched Value" : "'select * from site'"

                    }

              ],
```

```
                    "User Agent" : "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_11_6)
        AppleWebKit/537.36 (KHTML, like Gecko) Chrome/52.0.2743.116 Safari/537.36",

                    "id" :
        "kYSbc5AqNC7kD9k38me0Mu9f_hEuHkQhTJqzK0IKP1Oxux2sUgh5GQEPL004Wcan7RSqjGT4nv_b
        RvfeZSGwkQ== ",

                    "Event ID": "549737276120186591170055509529321564774"

            }
        ],
        "page" : 1
}
```

Get Event Log Entry

This method retrieves a specific event log entry.

Note: This method only supports JSON.

Request

A request to retrieve an event log entry is described below. When submitting this request, you will need to define the following terms:

- **AccountNumber:** This term should be replaced by your CDN account number. This number can be found in the upper-right hand corner of the MCC.

- **EventID:** Replace this variable with either of the following values:

  - **Request ID:** Represents the ID returned by the EVENT_ID variable. This variable may be used within a custom response to uniquely identify malicious requests.

  - **Event Log Entry ID:** Represents the ID of the desired event log entry.

    Tip: Use the Get Event Log Entries endpoint to retrieve a list of event log entries and their system-assigned IDs.

HTTP Method	Request URI
GET	https://api.edgecast.com/v2/mcc/customers/*AccountNumber*/waf/eventlogs/*EventID*

Request Headers

This endpoint only takes advantage of the common request headers described in the **Request Headers** section of the **Request and Response Elements** topic.

Request Body

Request body parameters are not required by this endpoint.

Response

The response to the above request includes an HTTP status code, response headers, and a response body.

Status Code

A status code indicates whether the request was successfully performed. A list of common status codes is provided in the **Status Codes and Error Messages** topic.

Response Headers

The response for this endpoint only returns standard HTTP response headers including those described in the **Response Headers** section of the **Request and Response Elements** topic.

Response Body

The response body for a successful request reports:

- **Basic Event Information:** Each element in the events array describes the request and the client that committed the violation(s).

- **Sub Events:** Specific information about each rule violation will be reported under the Sub Events parameter.

Note: This endpoint only returns event fields (e.g., Epoch Time or Matched On) that contain data. Therefore, the set of event fields returned by this endpoint may vary by event.

event Object

The event object contains a list of fields for the event returned by this endpoint.

Name	Data Type	Description
Acl ID	String	Reserved for future use.
Acl Name	String	Reserved for future use.

Name	Data Type	Description
Action Type	String	Indicates the action that was triggered as a result of the violation. Valid values are: • **ALERT:** This term has been deprecated in favor of NOP. • **BLOCK_REQUEST:** Indicates that the request that violated a rule was blocked. • **BLOCK:** This term has been deprecated in favor of BLOCK_REQUEST. • **NOP:** Indicates that an alert was generated in response to the rule violation. • **REDIRECT_302:** Indicates that the request that violated a rule was redirected to the URL associated with the instance defined by the **Instance Name** parameter. • **CUSTOM_RESPONSE:** Indicates that a custom response was returned to the client that submitted a request that violated a rule.
Bots ID	String	Reserved for future use.
Bots Name	String	Reserved for future use.
City Name	String	Identifies the city from which the request originated.
Client IP	String	Identifies the IP address of the client from which the violation originated.
Country Code	String	Identifies the country from which the request originated by its country code.
Country Name	String	Identifies the country from which the request originated.
Epoch Time	Number (floating-point)	Indicates the Unix time, in seconds, at which the violation took place. **Syntax:** *Seconds.Microseconds*
Event ID	String	Indicates the unique ID assigned to the event. **Tip:** Pass this ID to the Get Event Log Entry endpoint to retrieve this event log entry.

Name	Data Type	Description
Host	String	Indicates the hostname that was requested.
id	String	Indicates the hash value for the event's ID.
Instance Name	String	Indicates the name of the instance that activated the profile containing the rule that the requested violated.
Matched Data	String	**Signature Detection Mode Only** Deprecated. Indicates the client-side data that triggered the violation. For example, this parameter may report a client's IP address or a portion of the URL that violated the request.
Matched On	String	**Signature Detection Mode Only** Deprecated. Indicates the variable that identifies where the violation was found.
Matched Value	String	Deprecated. Indicates the value of the variable defined in the Matched On parameter.
Profile Name	String	Indicates the name of the profile that triggered the violation.
Profile Type	String	Indicates whether the request was screened as a result of an instance's production or audit profile. Valid values are: • PRODUCTION • AUDIT
Referer	String	Indicates the request's referrer as defined by the Referer request header.
Rule ID	Integer	**Note:** This parameter has been deprecated. **Note:** The ID for each rule that was violated is reported under the Sub Events parameter.
Rule Message	String	Provides the following basic information about the anomaly score violation(s). Inbound Anomaly Score Exceeded (Total Score: #, SQLi=#, XSS=#): Last Matched Message: *RuleID-RuleMessage*
Rule Policy	String	Indicates the name of the policy that was violated.

Name	Data Type	Description
Rule Severity	Integer	**Signature Detection Mode Only** Deprecated. Indicates the severity of the violation. This value may range from -1 to 6 where 6 represents the lowest severity level.
Rule Tags	Array	Indicates the tags associated with the rule that the request violated. These tags may be used to determine whether a rule, access control, or global setting was violated.
Rules Config ID	String	Reserved for future use.
Rules Config Name	String	Reserved for future use.
Scope ID	String	Reserved for future use.
Scope Name	String	Reserved for future use.
Sub Event Count	Integer	Indicates the total number of sub events.
Sub Events	Array	Contains a list of fields that describe each sub event associated with the current event. A sub event is reported for each rule violation incurred by a request.
Timestamp	String	Indicates the date and time (GMT) at which the violation took place. **Format:** *YYYY-MM-DDThh:mm:ss.ffffffZ*
URL	String	Indicates the URL that was requested.
User Agent	String	Indicates the user agent that submitted the request that triggered the rule violation.

Sub Events Array

The Sub Events array contains an object that describe each sub event associated with the current event. A sub event is reported for each rule violation incurred by a request.

Name	Data Type	Description
Matched Data	String	Deprecated. Indicates the client-side data that triggered the violation. For example, this parameter may report a client's IP address or a portion of the URL that violated the request.
Matched On	String	Indicates the variable that identifies where the violation was found.
Matched Value	String	Indicates the value of the variable defined in the Matched On parameter.

Name	Data Type	Description
Rule ID	Integer	Indicates the ID for the rule that the request violated.
Rule Message	String	Provides a description of the rule that the request violated.
Rule Severity	Integer	Indicates the severity of the violation. This value may range from -1 to 6 where 6 represents the lowest severity level.
Total Anomaly Score	Integer	Indicates the total anomaly score for the current rule violation. This score is calculated by summing the anomaly score of the current rule violation with all rule violations reported above this sub event.

Errors

The response body for an unsuccessful request may contain an error element that provides additional information. For a list of common error messages, please refer to the **Status Codes and Error Messages** topic.

Sample Request and Response

A sample JSON request is provided below.

```
GET
https://api.edgecast.com/v2/mcc/customers/0001/waf/eventlogs/ZG5cuvyo_poJuwGPzlcRJMc
w5qkW6DWLWtIrXFuYC1uQ6YJEN4mw1-imyLMl08TNYci2e5OaonfD7rw== HTTP/1.1

Authorization: TOK:12345678-1234-1234-1234-1234567890ab

Accept: application/json

Host: api.edgecast.com
```

A sample JSON response is provided below.

```
HTTP/1.1 200 OK

Cache-Control: private

Content-Type: application/json; charset=utf-8

Date: Thu, 14 Apr 2016 12:00:00 GMT

Content-Length: 1240

{
        "event" : {
                "Epoch Time" : 1473207640.345809,
                "Profile Type" : "PRODUCTION",
                "Sub Event Count" : 1,
```

```
        "Client IP" : "192.12.22.25",

        "Rule Tags" : [

                "OWASP_CRS/ANOMALY/EXCEEDED"

        ],

        "Timestamp" : "2016-09-07T00:20:40.345809Z",

        "Rule Message" : "Inbound Anomaly Score Exceeded (Total Score: 5,
SQLi=3, XSS=0): Last Matched Message: 981255-Detects MSSQL code execution and
information gathering attempts",

        "URL" : "http://www.mydomain.com/mywebpage.html",

        "Country Code" : "US",

        "Action Type" : "CUSTOM_RESPONSE",

        "Host" : "www.mydomain.com",

        "Instance Name" : "My Instance",

        "Profile Name" : "My Profile",

        "Sub Events" : [{

                    "Matched On" : "ARGS:a",

                    "Rule Message" : "Detects MSSQL code execution and
information gathering attempts",

                    "Matched Data" : "'select *",

                    "Total Anomaly Score" : 5,

                    "Rule ID" : 981255,

                    "Rule Severity" : 2,

                    "Matched Value" : "'select * from site'"

            }

        ],

        "User Agent" : "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_11_6)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/52.0.2743.116 Safari/537.36",

        "id" :
"veidK2wtEHpw4OQkoQKa3JI06QAeUKXwYqM_dgbsuvYwygOWO_uTVGQPxR5ELPpJ19wTpnflk7yn
rIJzAMH2tA=="

    }
}
```

Get Top Event Log Entries

This method identifies up to the top 10 events for a particular event log field. It returns a list of these events stored in descending order of frequency.

Note: This method only supports JSON.

Request

A request to retrieve a list of the most frequent events is described below. When submitting this request, you will need to define the following terms:

- **AccountNumber:** This term should be replaced by your CDN account number. This number can be found in the upper-right hand corner of the MCC.

- **Field:** Required. Replace this variable with the name of the desired field. Use the Get Available Event Log Fields (WAF) method to retrieve a list of the available fields.

- **StartDateTime:** Required. Replace this variable with the start date/time for the report. Only activity that took place after the specified date/time will be included in the report. **Format:** *YYYY-MM-DD*T*hh*:*mm*:*ss*

- **EndDateTime:** Required. Replace this variable with the end date/time for the report. Activity that took place after the specified date/time will not be included in the report. **Format:** *YYYY-MM-DD*T*hh*:*mm*:*ss*

- **ItemsPerPage:** Replace this variable with the number of log events that may be included on each page.

  Note: Omitting the page_size query string parameter in the request will return a maximum of 10 log events per page.

  Note: The maximum value for this variable is 100.

Note: Time (i.e., T*hh*:*mm*:*ss*) is optional. If time is not specified, then a default time (i.e., 00:00:00) will be used.

Note: For more information on date/time format, please refer to **Appendix B: Report Date/Time Format**.

HTTP Method	Request URI
GET	https://api.edgecast.com/v2/mcc/customers/*AccountNumber*/waf /eventlogs/top?field=*Field*&start_time=*StartDateTime*&end_time= *EndDateTime*&page_size=*ItemsPerPage*

Request Headers

This endpoint only takes advantage of the common request headers described in the **Request Headers** section of the **Request and Response Elements** topic.

Request Body

Request body parameters are not required by this endpoint.

Response

The response to the above request includes an HTTP status code, response headers, and a response body.

Status Code

A status code indicates whether the request was successfully performed. A list of common status codes is provided in the **Status Codes and Error Messages** topic.

Response Headers

The response for this endpoint only returns standard HTTP response headers including those described in the **Response Headers** section of the **Request and Response Elements** topic.

Response Body

The response body for a successful request contains the following response elements:

Name	Data Type	Description
total	Integer	Indicates the total number of events that occurred during the specified time period.
signature	Array	Deprecated. This response element contains a list of the most frequent events for the field specified in the request. **Key information:** • The upper limit for the number of log events included in this list is determined by the page_size query string parameter. • This list is sorted in descending order of frequency.
count	Integer	Deprecated. Indicates the total number of events that were: • Assigned the value defined in the *term* response element. • Occurred during the time period defined in the request. • Triggered by a profile whose threat detection method is signature mode.
term	String	Deprecated. Indicates a unique value for the field defined in the request (i.e., ?field=*Field*)
time_to	Number (floating-point)	Indicates the report's end date/time, in seconds, using Unix time. **Syntax:** *Seconds*.0

Name	Data Type	Description
time_from	Number (floating-point)	Indicates the report's start date/time, in seconds, using Unix time. **Syntax:** *Seconds*.0
anomaly	Array	This response element contains a list of the most frequent events for the field specified in the request. **Key information:** • The upper limit for the number of log events included in this list is determined by the page_size query string parameter. • This list is sorted in descending order of frequency.
count	Integer	Indicates the total number of events that were: • Assigned the value defined in the *term* response element. • Occurred during the time period defined in the request.
term	String	Indicates a unique value for the field defined in the request (i.e., ?field=*Field*)
results	Array	This response element contains a list of the most frequent events for the field specified in the request. **Key information:** • The upper limit for the number of log events included in this list is determined by the page_size query string parameter. • This list is sorted in descending order of frequency.
count	Integer	Indicates the total number of events that were: • Assigned the value defined in the *term* response element. • Occurred during the time period defined in the request.
term	String	Indicates a unique value for the field defined in the request (i.e., ?field=*Field*)

Errors

The response body for an unsuccessful request may contain an error element that provides additional information. For a list of common error messages, please refer to the **Status Codes and Error Messages** topic.

Sample Request and Response

A sample JSON request is provided below.

```
GET
https://api.edgecast.com/v2/mcc/customers/0001/waf/eventlogs/top?field=Host&start_ti
me=2014-10-20&end_time=2014-10-21 HTTP/1.1

Authorization: TOK:12345678-1234-1234-1234-1234567890ab

Accept: application/json

Host: api.edgecast.com
```

A sample JSON response is provided below.

```
HTTP/1.1 200 OK

Cache-Control: private

Content-Type: application/json; charset=utf-8

Date: Thu, 14 Apr 2016 12:00:00 GMT

Content-Length: 382


{
        "total" : 15112,
        "signature" : [{
                    "count" : 15111,
                    "term" : "www.mydomain.com"
              }, {
                    "count" : 1,
                    "term" : "www.mydomain.com:443"
              }
        ],
        "time_to" : 1414022400.0,
        "time_from" : 1413936000.0,
        "anomaly" : [],
        "results" : [{
                    "count" : 15111,
                    "term" : "www.mydomain.com"
              }, {
                    "count" : 1,
                    "term" : "www.mydomain.com:443"
              }
        ]
}
```

Rate Limiting Event Logs

The endpoints described in this section are designed to retrieve event log information on rate limited requests. A brief description for each available endpoint is provided below.

Name	Description
Get Available Event Log Fields (Rate Limiting)	Retrieves a list of the available event log fields.
Get Event Log Entries (Rate Limiting)	Retrieves event log information for a set of rate limited requests.
Get Event Log Entry (Rate Limiting)	Retrieves event log information for a specific rate limited request.
Get Event Log Entry Count (Rate Limiting)	Indicates the total number of rate limited requests that meet the specified criteria.
Get Top Event Log Entries (Rate Limiting)	Indicates the type of records that are most frequently rate limited.

Get Available Event Log Fields (Rate Limiting)

This endpoint retrieves a list of the available event log fields.

Note: This endpoint only supports JSON.

Request

A request to retrieve a listing of fields is described below. When submitting this request, you will need to define the following variable:

- **AccountNumber:** Replace this variable with your CDN account number. This number can be found in the upper-right hand corner of the MCC.

HTTP Method	Request URI
GET	https://api.edgecast.com/v2/mcc/customers/*AccountNumber*/defend/rate_limiting/eventlogs/fields

Request Headers
The response for this endpoint only includes standard HTTP request headers including those described in the **Request Headers** section of the **Request and Response Elements** topic.

Request Body
Request body parameters are not required by this endpoint.

Response

The response to the above request includes an HTTP status code, response headers, and a response body.

Status Code
A status code indicates whether the request was successfully performed. A list of common status codes is provided in the **Status Codes and Error Messages** topic.

Response Headers
The response for this endpoint only returns standard HTTP response headers including those described in the **Response Headers** section of the **Request and Response Elements** topic.

Response Body

The response body for a successful request contains the following response elements:

Name	Data Type	Description
fields	Array	This response element contains the set of available event log fields.
name	String	Identifies an event log field by its name.

data_type	String	Indicates the event log field's data type.
		
		Valid values are:
		
		• **date:** Indicates that the event log field reports date/time in UTC.
		
		    ▪ **Format:** *YYYY-MM-DD*T*hh*:*mm*:*ss*.*ffffff*Z
		
		    ▪ **Example:** 2015-06-30T20:42:09.330793Z
		    The above value represents June 30th, 2015 at 8:42 p.m. UTC.
		
		    Note: For more information on date/time format, please refer to **Appendix B: Report Date/Time Format**.
		
		• **epoch:** Indicates that the event log field reports a date in Unix time (UTC).
		
		    • **Example:** 1435696928.9078219
		    The above value represents June 30th, 2015 at 8:42 p.m. UTC.
		
		• **ip:** Indicates that the event log field reports an IP address (IPv4) in dot-decimal notation.
		
		    ▪ **Example:** 101.100.20.200
		
		• **string:** Indicates that the event log field reports data as a string value.

description	String	Provides a brief description of the event log field's purpose.

Errors

The response body for an unsuccessful request may contain an error element that provides additional information. For a list of common error messages, please refer to the **Status Codes and Error Messages** topic.

Sample Request and Response

A sample JSON request is provided below.

```
GET
https://api.edgecast.com/v2/mcc/customers/0001/defend/rate_limiting/eventlogs/fields
HTTP/1.1

Authorization: TOK:12345678-1234-1234-1234-1234567890ab

Accept: application/json

Host: api.edgecast.com
```

A sample JSON response is provided below.

```
HTTP/1.1 200 OK

Cache-Control: private

Content-Type: application/json; charset=utf-8

Date: Thu, 14 Apr 2016 12:00:00 GMT

Content-Length: 2196

    {
    "fields" : [{
                "name" : "id",
                "data_type" : "string",
                "description" : "ID of event"
        }, {
                ...
        }, {
                "name" : "Country Code",
                "data_type" : "string",
                "description" : "Two letter country code"
        }
    ]
}
```

Get Event Log Entries (Rate Limiting)

This endpoint returns paginated event log data. This data can be filtered by:

- Time Period

- Field values

Note: A request for event log entries may return information on thousands of requests. Due to the amount of time that it would take to transmit this data, the response for this endpoint has been split up into pages. Retrieve all events that match the specified criteria by requesting each page. Use the page_of response element in your script to cycle through each page.

Note: This endpoint only supports JSON.

Request

A request to retrieve event log data is described below. When submitting this request, you will need to define the following variables:

- **AccountNumber:** Replace this variable with your CDN account number. This number can be found in the upper-right hand corner of the MCC.

- **StartDateTime:** Replace this variable with the start date/time for the report. Only activity that took place after the specified date/time will be included in the report. **Format:** *YYYY-MM-DD*T*hh*:*mm*:*ss*

    Important: A valid request must either include or exclude both date/time parameters (i.e., start_time and end_time).

    Note: Omitting both date/time parameters (i.e., start_time and end_time) will return data for 24 hours prior to the time when the request was submitted.

- **EndDateTime:** Replace this variable with the end date/time for the report. Activity that took place after the specified date/time will not be included in the report. **Format:** *YYYY-MM-DD*T*hh*:*mm*:*ss*

- **ItemsPerPage:** Replace this variable with the number of events that may be included on each page. The number of items per page determines the number of pages that may be returned.

    - The maximum value for this variable is 1000.

    - Omitting the per_page query string parameter in the request will return a maximum of 10 entries per page.

- **PageNumber:** Replace this variable with the page number that will be returned. This endpoint will only include events corresponding to that page in the response.

    - Omitting the page query string parameter will generate a response for the first page (i.e., page=1).

- **Filters:** Replace this variable with the desired filter(s).

    - Specify one or more filters using URL-encoded JSON.

    - Only events that satisfy all specified filters may be returned by this endpoint.

    - Specify a field name and a value for each desired filter. Use the Get Available Event Log Fields (Rate Limiting) endpoint to retrieve a list of fields.

    - Field names and values are case-sensitive.

    - Use a comma to delimit each filter.

    - Set up a filter that can be satisfied by multiple values by comma-delimiting each value within brackets.

    - A "starts with" match may be defined by appending an asterisk (i.e., *) to the desired value. Any other usage of an asterisk wildcard is unsupported.

Note: Omitting a start date/time will return the events that took place within the last 24 hours.

Note: Time (i.e., T*hh*:*mm*:*ss*) is optional when defining a start and end date/time. If time is not specified, then a default time (i.e., 00:00:00) will be used. For more information on date/time format, please refer to **Appendix B: Report Date/Time Format**.

HTTP Method	Request URI
GET	https://api.edgecast.com/v2/mcc/customers/*AccountNumber*/defend/ rate_limiting/eventlogs?start_time=*StartDateTime*&end_time= *EndDateTime*&per_page=*ItemsPerPage*&page=*PageNumber*&filters= *Filters*

Request Headers

The response for this endpoint only includes standard HTTP request headers including those described in the **Request Headers** section of the **Request and Response Elements** topic.

Request Body

Request body parameters are not required by this endpoint.

Response

The response to the above request includes an HTTP status code, response headers, and a response body.

Status Code

A status code indicates whether the request was successfully performed. A list of common status codes is provided in the **Status Codes and Error Messages** topic.

Response Headers

The response for this endpoint only returns standard HTTP response headers including those described in the **Response Headers** section of the **Request and Response Elements** topic.

Response Body

The response body for a successful request contains the following response elements:

Name	Data Type	Description
page_of	Integer	Indicates the total number of pages in the report.
		Reminder: This value is determined by the total number of eligible event log entries divided by the maximum number of entries per page. Both of these factors are defined in the request URL.
time_to	Number (floating-point)	Indicates the report's end date/time, in seconds, using Unix time.
		Syntax: *Seconds*.0
time_from	Number (floating-point)	Indicates the report's start date/time, in seconds, using Unix time.
		Syntax: *Seconds*.0
events	Array	This response element contains a list of fields for each event reported on this page.
		Note: The current page is indicated by the page response element.
Status	String	Identifies by name the HTTP status code for the response to a rate limited request.
		Format: HTTP_STATUS_*Name*
		Example: HTTP_STATUS_FOUND
		In the above sample value, the HTTP status code describing the response for a rate limited request was a 302 Found.
Epoch Time	Number (floating-point)	Indicates the Unix time, in seconds, at which the request was processed.
		Syntax: *Seconds*.*Microseconds*

Name	Data Type	Description
Rate Limiting Enforcement Type	String	Indicates the type of action that was applied to the rate limited request.
Client IP	String	Indicates the IP address of the client that submitted the rate limited request.
URL	String	Indicates the URL that was requested.
Timestamp	String	Indicates the date and time (UTC/GMT) at which the request was processed. **Format:** *YYYY-MM-DD*T*hh*:*mm*:*ss.ffffff*Z **Note:** For more information on date/time format, please refer to **Appendix B: Report Date/Time Format**.
Rate Limiting Enforcement Rule ID	String	This field is reserved for future use.
@fields.COMMON_Header	Object	This field is reserved for future use.
Country Code	String	Identifies the country from which the request originated by its ISO 3166 country code. A list of country codes is available from the CDN Help Center: • [Country Codes (ISO 3166)](#)
Rate Limiting Enforcement Tuple ID	String	Indicates the action that was applied to the rate limited request by its system-defined ID.
Host	String	Identifies the host to which the request was directed. This value is derived from the request's Host header.
Referer	String	Identifies the request's referrer. This value is derived from the request's Referer header.
Rate Limiting Enforcement Start Epoch	Integer	Indicates when the rate limiting action was applied to the request. The date and time is reported in Unix time (a.k.a. POSIX time or Unix epoch). **Important:** Time is reported in milliseconds instead of seconds. Please convert this value from milliseconds to seconds prior to leveraging it with Unix time functions.

Name	Data Type	Description
Request Method	String	Indicates the request's HTTP method. **Format:** HTTP_METHOD_*Name* **Example:** HTTP_METHOD_GET
Rate Limiting Enforcement Percentage	Number (floating-point)	Indicates the percentage of eligible requests that were rate limited when the event took place.
Rate Limiting Enforcement Duration	Integer	Indicates the minimum length of time, in seconds, that eligible requests were rate limited when the event took place.
User Agent	String	Indicates the user agent that submitted the request. This value is derived from the request's User-Agent header.
id	String	Identifies the event log entry that describes the current rate limited request by its system-defined ID.
page	Integer	Indicates the page number for the page that was returned by this endpoint. **Note:** This response element should match the "page" query string parameter defined in the request URL. If that parameter was omitted, then this response element will be set to 1.

Errors

The response body for an unsuccessful request may contain an error element that provides additional information. For a list of common error messages, please refer to the **Status Codes and Error Messages** topic.

Sample Request and Response

A sample JSON request is provided below.

```
GET
https://api.edgecast.com/v2/mcc/customers/0001/defend/rate_limiting/eventlogs?start_
time=2015-06-30T20:00:00&end_time=2015-06-30T21:00:00&page=1 HTTP/1.1

Authorization: TOK:12345678-1234-1234-1234-1234567890ab

Accept: application/json

Host: api.edgecast.com
```

A sample JSON response is provided below.

```
HTTP/1.1 200 OK
Cache-Control: private
Content-Type: application/json; charset=utf-8
Date: Thu, 14 Apr 2016 12:00:00 GMT
Content-Length: 9091

{
        "page_of" : 1,
        "time_to" : 1473638400.0,
        "time_from" : 1472688000.0,
        "events" : [{
                    "Status" : "HTTP_STATUS_SERVICE_NOT_AVAILABLE",
                    "Epoch Time" : 1473470411.2213371,
                    "Host" : "cdn.mydomain.com",
                    "Client IP" : "192.12.16.24",
                    "URL" : "http://cdn.mydomain.com/000001/mywebpage.html",
                    "Timestamp" : "2016-09-10T01:20:11.221337Z",
                    "Rate Limiting Enforcement Rule ID" : "XXXNAXXX@ddos.RULE_ID",
                    "@fields.COMMON_HEADER" : {},
                    "Country Code" : "US",
                    "Rate Limiting Enforcement Tuple ID" : "2c85167d-865d-4701-
        9a9a-11410327f8610001",
                    "Rate Limiting Enforcement Type" : "DROP_REQUEST",
                    "Referer" : "XXXNAXXX@fields.REFERER",
                    "Rate Limiting Enforcement Start Epoch" : 1473470411000,
                    "Request Method" : "HTTP_METHOD_GET",
                    "Rate Limiting Enforcement Percentage" : 96.97,
                    "Rate Limiting Enforcement Duration" : 280,
                    "User Agent" : "Server Load Tester",
                    "id" : "z-dgB40S7zgoqT8Nh_-
        zTyhxxLprMULRXpQLDCOwjOC_D1RvHs9qFCL4i88CPJ7SW6ssFBGPsmQ9GqiO_A_LMw=="
            }, {
                    ...
            }, {
                    "Status" : "HTTP_STATUS_SERVICE_NOT_AVAILABLE",
                    "Epoch Time" : 1473470402.730159,
                    "Host" : "cdn.mydomain.com",
                    "Client IP" : "192.12.16.24",
```

```
                    "URL" : "http://cdn.mydomain.com/000001/mywebpage.html",

                    "Timestamp" : "2016-09-10T01:20:02.730159Z",

                    "Rate Limiting Enforcement Rule ID" : "XXXNAXXX@ddos.RULE_ID",

                    "@fields.COMMON_HEADER" : {},

                    "Country Code" : "US",

                    "Rate Limiting Enforcement Tuple ID" : "2c85167d-865d-4701-
        9a9a-11410327f8610001",

                    "Rate Limiting Enforcement Type" : "DROP_REQUEST",

                    "Referer" : "XXXNAXXX@fields.REFERER",

                    "Rate Limiting Enforcement Start Epoch" : 1473470402000,

                    "Request Method" : "HTTP_METHOD_GET",

                    "Rate Limiting Enforcement Percentage" : 96.97,

                    "Rate Limiting Enforcement Duration" : 280,

                    "User Agent" : "Server Load Tester",

                    "id" : "F39U9yCoV6CaXBELa-2cjS5QDcjjPPQmH-
        mVRP5aUIXAhznwjC3I8kMDjcPEgmxKzMIrkJqYZ0KduFKWMqp-3Q=="

            }
        ],
        "page" : 1
}
```

Get Event Log Entry (Rate Limiting)

This endpoint retrieves a specific event log entry by its system-defined ID.

Note: This endpoint only supports JSON.

Request

A request to retrieve an event log entry is described below. When submitting this request, you will need to define the following variables:

- **AccountNumber:** Replace this variable with your CDN account number. This number can be found in the upper-right hand corner of the MCC.

- **EventID:** Replace this variable with the encoded ID of the desired event log entry. Use the Get Event Log Entries (Rate Limiting) endpoint to retrieve a list of event log entries and an encoded version of their system-assigned IDs.

HTTP Method	Request URI
GET	https://api.edgecast.com/v2/mcc/customers/*AccountNumber*/defend/ rate_limiting/eventlogs/recordid=*EventID*

Request Headers

The response for this endpoint only includes standard HTTP request headers including those described in the **Request Headers** section of the **Request and Response Elements** topic.

Request Body

Request body parameters are not required by this endpoint.

Response

The response to the above request includes an HTTP status code, response headers, and a response body.

Status Code

A status code indicates whether the request was successfully performed. A list of common status codes is provided in the **Status Codes and Error Messages** topic.

Response Headers

The response for this endpoint only returns standard HTTP response headers including those described in the **Response Headers** section of the **Request and Response Elements** topic.

Response Body

The response body for a successful request contains the following response elements:

Name	Data Type	Description
event	Array	This response element contains a list of fields for the requested event.
Status	String	Identifies by name the HTTP status code for the response to a rate limited request. **Format:** HTTP_STATUS_*Name* **Example:** HTTP_STATUS_FOUND In the above sample value, the HTTP status code describing the response for a rate limited request was a 302 Found.
Epoch Time	Number (floating-point)	Indicates the Unix time, in seconds, at which the request was processed. **Syntax:** *Seconds.Microseconds*
Rate Limiting Enforcement Rule ID	String	Indicates the action that was applied to the rate limited request by its system-defined ID.
Client IP	String	Indicates the IP address of the client that submitted the rate limited request.
URL	String	Indicates the URL that was requested.
Timestamp	String	Indicates the date and time (UTC/GMT) at which the request was processed. **Format:** *YYYY-MM-DDThh:mm:ss.ffffffZ* **Note:** For more information on date/time format, please refer to **Appendix B: Report Date/Time Format**.
Rate Limiting Enforcement Duration	Integer	Indicates the minimum length of time, in seconds, that eligible requests were rate limited when the event took place.
Country Code	String	Identifies the country from which the request originated by its ISO 3166 country code. A list of country codes is available from the CDN Help Center: Country Codes (ISO 3166)
@fields.COMMON_Header	Object	This field is reserved for future use.

Name	Data Type	Description
Host	String	Identifies the host to which the request was directed. This value is derived from the request's Host header.
Rate Limiting Enforcement Type	String	Indicates the type of action that was applied to the rate limited request.
Rate Limiting Enforcement Start Epoch	Integer	Indicates when the rate limiting action was applied to the request. The date and time is reported in Unix time (a.k.a. POSIX time or Unix epoch). **Important:** Time is reported in milliseconds instead of seconds. Please convert this value from milliseconds to seconds prior to leveraging it with Unix time functions.
Request Method	String	Indicates the request's HTTP method. **Format:** HTTP_METHOD_*Name* **Example:** HTTP_METHOD_GET
Rate Limiting Enforcement Percentage	Number (floating-point)	Indicates the percentage of eligible requests that were rate limited when the event took place.
Referer	String	Identifies the request's referrer. This value is derived from the request's Referer header.
User Agent	String	Indicates the user agent that submitted the request. This value is derived from the request's User-Agent header.
id	String	Identifies the event log entry that describes the current rate limited request by its system-defined ID.

Errors

The response body for an unsuccessful request may contain an error element that provides additional information. For a list of common error messages, please refer to the **Status Codes and Error Messages** topic.

Sample Request and Response

A sample JSON request is provided below.

```
GET
https://api.edgecast.com/v2/mcc/customers/0001/defend/rate_limiting/eventlogs/record
id= z-dgB40S7zgoqT8Nh_-
zTyhxxLprMULRXpQLDCOwjOC_D1RvHs9qFCL4i88CPJ7SW6ssFBGPsmQ9GqiO_A_LMw== HTTP/1.1

Authorization: TOK:12345678-1234-1234-1234-1234567890ab

Accept: application/json

Host: api.edgecast.com
```

A sample JSON response is provided below.

```
HTTP/1.1 200 OK

Cache-Control: private

Content-Type: application/json; charset=utf-8

Date: Thu, 14 Apr 2016 12:00:00 GMT

Content-Length: 932

{
        "event" : {
                "Status" : "HTTP_STATUS_SERVICE_NOT_AVAILABLE",
                "Epoch Time" : 1473470411.2213371,
                "Rate Limiting Enforcement Rule ID" : "XXXNAXXX@ddos.RULE_ID",
                "Client IP" : "192.12.16.24",
                "URL" : "http://cdn.mydomain.com/000001/mywebpage.html",
                "Timestamp" : "2016-09-10T01:20:11.221337Z",
                "Rate Limiting Enforcement Duration" : 280,
                "Country Code" : "US",
                "@fields.COMMON_HEADER" : {},
                "Rate Limiting Enforcement Tuple ID" : "2c85167d-865d-4701-9a9a-
        11410327f86114631",
                "Rate Limiting Enforcement Type" : "DROP_REQUEST",
                "Referer" : "XXXNAXXX@fields.REFERER",
                "Rate Limiting Enforcement Start Epoch" : 1473470411000,
                "Request Method" : "HTTP_METHOD_GET",
                "Rate Limiting Enforcement Percentage" : 96.97,
                "Host" : "cdn.mydomain.com",
                "User Agent" : "Server Load Tester",
                "id" : "z-dgB40S7zgoqT8Nh_-
        zTyhxxLprMULRXpQLDCOwjOC_D1RvHs9qFCL4i88CPJ7SW6ssFBGPsmQ9GqiO_A_LMw=="
        }
}
```

Get Event Log Entry Count (Rate Limiting)

This endpoint indicates the total number of event log entries that occurred within a specified time period.

Note: This endpoint only supports JSON.

Request

A request to retrieve a sum of event log entries is described below. When submitting this request, you will need to define the following variables:

- **AccountNumber:** Replace this variable with your CDN account number. This number can be found in the upper-right hand corner of the MCC.

- **StartDateTime:** Required. Replace this variable with the start date/time for the report. Only activity that took place after the specified date/time will be included in the report. **Format:** *YYYY-MM-DDThh:mm:ss*

- **EndDateTime:** Required. Replace this variable with the end date/time for the report. Activity that took place after the specified date/time will not be included in the report. **Format:** *YYYY-MM-DDThh:mm:ss*

Note: Time (i.e., T*hh*:*mm*:*ss*) is optional when defining a start and end date/time. If time is not specified, then a default time (i.e., 00:00:00) will be used. For more information on date/time format, please refer to **Appendix B: Report Date/Time Format**.

HTTP Method	Request URI
GET	https://api.edgecast.com/v2/mcc/customers/*AccountNumber*/defend/ rate_limiting/eventlogs/count? start_time=*StartDateTime*&end_time= *EndDateTime*

Request Headers
The response for this endpoint only includes standard HTTP request headers including those described in the **Request Headers** section of the **Request and Response Elements** topic.

Request Body
Request body parameters are not required by this endpoint.

Response

The response to the above request includes an HTTP status code, response headers, and a response body.

Status Code
A status code indicates whether the request was successfully performed. A list of common status codes is provided in the **Status Codes and Error Messages** topic.

Response Headers

The response for this endpoint only returns standard HTTP response headers including those described in the **Response Headers** section of the **Request and Response Elements** topic.

Response Body

The response body for a successful request contains the following response element:

Name	Data Type	Description
count	Integer	Indicates the number of event log entries that took place during the given time period.

Errors

The response body for an unsuccessful request may contain an error element that provides additional information. For a list of common error messages, please refer to the **Status Codes and Error Messages** topic.

Sample Request and Response

A sample JSON request is provided below.

```
GET
https://api.edgecast.com/v2/mcc/customers/0001/defend/rate_limiting/eventlogs/count?
start_time=2015-06-30&end_time=2015-07-01 HTTP/1.1

Authorization: TOK:12345678-1234-1234-1234-1234567890ab

Accept: application/json

Host: api.edgecast.com
```

A sample JSON response is provided below.

```
HTTP/1.1 200 OK

Cache-Control: private

Content-Type: application/json; charset=utf-8

Date: Thu, 14 Apr 2016 12:00:00 GMT

Content-Length: 22

{
        "count" : 43061
}
```

Get Top Event Log Entries (Rate Limiting)

This endpoint provides the top events over a given time period.

Note: This endpoint only supports JSON.

Request

A request to retrieve the top occurring event log entries is described below. When submitting this request, you will need to define the following variables:

- **AccountNumber:** Required. Replace this variable with your CDN account number. This number can be found in the upper-right hand corner of the MCC.

- **Field:** Required. Replace this variable with the name of the desired field. Use the Get Event Log Fields (Rate Limiting) endpoint to retrieve a list of the available fields.

- **StartDateTime:** Required. Replace this variable with the start date/time for the report. Only activity that took place after the specified date/time will be included in the report. **Format:** *YYYY-MM-DD*T*hh*:*mm*:*ss*

- **EndDateTime:** Required. Replace this variable with the end date/time for the report. Activity that took place after the specified date/time will not be included in the report. **Format:** *YYYY-MM-DD*T*hh*:*mm*:*ss*

- **ItemsPerPage:** Replace this variable with the number of log events that may be included on each page.

    Note: Omitting the page_size query string parameter in the request will return a maximum of 10 log events per page.

    Note: The maximum value for this variable is 100.

Note: Time (i.e., T*hh*:*mm*:*ss*) is optional when defining a start and end date/time. If time is not specified, then a default time (i.e., 00:00:00) will be used. For more information on date/time format, please refer to **Appendix B: Report Date/Time Format**.

HTTP Method	Request URI
GET	https://api.edgecast.com/v2/mcc/customers/*AccountNumber*/defend/rate_limiting/eventlogs/top?field=*Field*&start_time=*StartDateTime*&end_time=*EndDateTime*&page_size=*ItemsPerPage*

Request Headers

The response for this endpoint only includes standard HTTP request headers including those described in the **Request Headers** section of the **Request and Response Elements** topic.

Request Body

Request body parameters are not required by this endpoint.

Response

The response to the above request includes an HTTP status code, response headers, and a response body.

Status Code

A status code indicates whether the request was successfully performed. A list of common status codes is provided in the **Status Codes and Error Messages** topic.

Response Headers

The response for this endpoint only returns standard HTTP response headers including those described in the **Response Headers** section of the **Request and Response Elements** topic.

Response Body

The response body for a successful request contains the following response elements for each available action type:

Name	Data Type	Description
time_to	Number (floating-point)	Indicates the report's end date/time, in seconds, using Unix time. **Syntax:** *Seconds*.0
total	Integer	Indicates the total number of requests that occurred during the requested date range that satisfied at least one of the specified filters.
time_from	Number (floating-point)	Indicates the report's start date/time, in seconds, using Unix time. **Syntax:** *Seconds*.0
results	Array	Contains the results for the requested report.
count	Integer	Indicates the total number of requests that occurred during the requested date range that satisfy both of the following: • The criteria defined in the filters query string parameter. • The value defined in the term response element.
term	String	Indicates a unique value for the field defined in the request (i.e., ?field=Field)

Errors

The response body for an unsuccessful request may contain an error element that provides additional information. For a list of common error messages, please refer to the **Status Codes and Error Messages** topic.

Sample Request and Response

A sample JSON request is provided below.

```
GET
https://api.edgecast.com/v2/mcc/customers/0001/defend/rate_limiting/eventlogs/top?fi
eld=Referrer&start_time=2015-10-28&end_time=2015-11-05 HTTP/1.1

Authorization: TOK:12345678-1234-1234-1234-1234567890ab

Accept: application/json

Host: api.edgecast.com
```

A sample JSON response is provided below.

```
HTTP/1.1 200 OK

Cache-Control: private

Content-Type: application/json; charset=utf-8

Date: Thu, 14 Apr 2016 12:00:00 GMT

Content-Length: 262


{
        "time_to" : 1446681600.0,

        "total" : 13100,

        "time_from" : 1445990400.0,

        "results" : [{

                    "count" : 8700,

                    "term" : "www.exampledomain1.com"

            }, {

                    "count" : 4400,

                    "term" : "www.exampledomain2.com"

            }

        ]
}
```

Rules Engine (Version 4)

This section contains the Get Deploy Request Status endpoint that returns the propagation status for a deploy request to the production environment.

Get Deploy Request Status (Rules Engine v4)

Retrieves the propagation status for a deploy request to the production environment.

Important: This endpoint does not support the retrieval of propagation status for deploy requests submitted to the staging environment.

Request

A request to retrieve status information is described below. When submitting this request, you will need to define the following terms:

- **xxxx:** Replace this term with the desired customer account number.

- **DeployRequestID:** Replace this term with the system-defined ID for the desired deploy request.

  Find out a deploy request's ID by performing the following steps:

  1. Open the customer's MCC.

  2. Navigate to the **Rules Engine** page for the desired platform.

  3. Find the **Production** section and then click either the policy name or the "View deploy request link."

  4. Look up the desired deploy request's ID in the breadcrumb navigation.

HTTP Method	Request URI
GET	https://api.edgecast.com/v2/mcc/customers/*xxxx*/rulesv4/*DeployRequestID*/status

Request Headers

This endpoint only takes advantage of the common request headers described in the **Request Headers** section of the **Request and Response Elements** topic.

Request Body

Request body parameters are not required by this endpoint.

Response

The response to the above request includes an HTTP status code, response headers, and a response body.

Status Code

A status code indicates whether the request was successfully performed. A list of common status codes is provided in the **Status Codes and Error Messages** topic.

Response Headers

The response for this endpoint only returns standard HTTP response headers including those described in the **Response Headers** section of the **Request and Response Elements** topic.

Response Body

The response body for a successful request contains the following response elements:

Name	Data Type	Description
Status	String	Indicates the deploy request's current propagation status. Valid values are: • **New:** Indicates that the configuration has been created, but the propagation process has not started. **Note:** A new configuration may stay in this state for a few minutes while it undergoes a validation/verification process. • **propagating:** Indicates that the configuration is in the process of being propagated. • **propagated:** Indicates that the configuration has been propagated across the entire network.
Percent_propagated	Decimal	Indicates the average configuration propagation percentage across all POPs.
Pops	Array	Contains a list of POPs and their current configuration propagation percentage.

Name	Data Type	Description
name	String	Identifies a POP by region and name. **Syntax (Single POP per Location):** *Region* : *POPName* **Syntax (Multiple POPs per Location):** If a location contains multiple POPs, then a three-letter abbreviation will identify each POP: *Region* : *POPName* (*POP*)
percentage_propagated	Decimal	Indicates the percentage of servers within a POP to which the configuration has been propagated.

Errors

The response body for an unsuccessful request may contain an error element that provides additional information. For a list of common error messages, please refer to the **Status Codes and Error Messages** topic.

Staging Environment Deploy Requests

Requesting propagation status for a deploy request submitted to the Staging environment will return a 500 Internal Server Error with the following response body:

```
{

        "Message": "Operation Error. Contact Administrator"

}
```

Sample Request and Response

A sample JSON request is provided below.

```
GET https://api.edgecast.com/v2/mcc/customers/0001/rulesv4/123456/status HTTP/1.1

Authorization: TOK:12345678-1234-1234-1234-1234567890ab

Accept: application/json

Host: api.edgecast.com
```

A sample JSON response is provided below.

```
HTTP/1.1 200 OK
Cache-Control: private
Content-Type: application/json; charset=utf-8
Date: Thu, 14 Apr 2016 12:00:00 GMT
Content-Length: 7255

{
        "Status": "propagating",
        "Percent_propagated": 2.666083916083916,
        "Pops": [{
                        "name": "South America : Valparaiso, Chile",
                        "percentage_propagated": 5.263157894736842
                }, {
                        ...
                        "name": "South America : Lima, Peru",
                        "percentage_propagated": 10.0
                }, {
                        "name": "North America : San Jose",
                        "percentage_propagated": 4.0
                }, {
                        "name": "Australia : Auckland",
                        "percentage_propagated": 3.7037037037037033
                }
        ]
}
```

Edge Nodes

This section describes an endpoint through which a descriptive list of edge nodes can be generated.

Get All Edge Nodes

This endpoint retrieves a comprehensive list of edge nodes (i.e., POPs). This list includes metadata describing each edge node, such as its location and IP blocks.
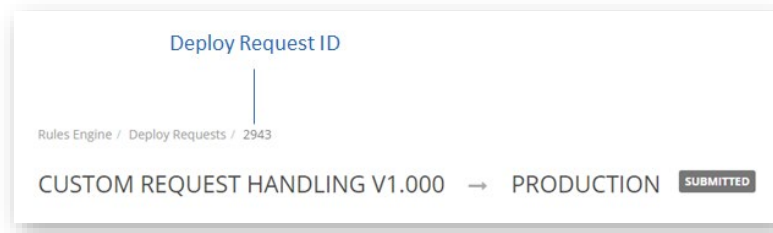
Request

A request to retrieve a list of edge nodes is described below. When submitting this request, you will need to define the following term:

- **xxxx:** This term should be replaced by the account number associated with the desired customer account.

HTTP Method	Request URI
GET	https://api.edgecast.com/v2/mcc/customers/*xxxx*/edgenodes

Request Headers

This endpoint only takes advantage of the common request headers described in the **Request Headers** section of the **Request and Response Elements** topic.

Request Body

Request body parameters are not required by this endpoint.

Response

The response to the above request includes an HTTP status code, response headers, and a response body.

Status Code

A status code indicates whether the request was successfully performed. A list of common status codes is provided in the **Status Codes and Error Messages** topic.

Response Headers

The response for this endpoint only returns standard HTTP response headers including those described in the **Response Headers** section of the **Request and Response Elements** topic.

Response Body

The response body for a successful request contains the following response elements for each edge node returned by this endpoint.

Name	Description
Code	A string that identifies an edge node by its three letter abbreviation.
Continent	A string that indicates the continent on which the edge node is located.
City	A string that indicates the city where the edge node is located.
V4	Lists each public IP block (IPv4) associated with an edge node.
IPAddressRange	This tag represents a single IP block (IPv4) associated with an edge node.
StartIp	A string that indicates the start IP address of the IP block (IPv4) associated with an edge node.
EndIp	A string that indicates the end IP address of the IP block (IPv4) associated with an edge node.
SubnetMask	A string that indicates the edge node's IPv4 subnet mask. A routing prefix is used to identify a subnet mask.
V6	Lists each public IP block (IPv6) associated with an edge node.
IPAddressRange	This tag represents a single IP block (IPv6) associated with an edge node.
StartIp	A string that indicates the start IP address of the IP block (IPv6) associated with an edge node.
EndIp	A string that indicates the end IP address of the IP block (IPv6) associated with an edge node.
SubnetMask	A string that indicates the edge node's IPv6 subnet mask. A routing prefix is used to identify a subnet mask.

Errors

The response body for an unsuccessful request may contain an error element that provides additional information. For a list of common error messages, please refer to the **Status Codes and Error Messages** topic.

Sample Request and Response

A sample JSON request is shown below.

```
GET https://api.edgecast.com/v2/mcc/customers/0001/edgenodes HTTP/1.1
Authorization: TOK:12345678-1234-1234-1234-1234567890ab
Accept: application/json
Host: api.edgecast.com
```

A sample JSON response is shown below.

```
HTTP/1.1 200 OK
Cache-Control: private
Content-Type: application/json; charset=utf-8
Date: Thu, 14 Apr 2016 12:00:00 GMT
Content-Length: 1130

[{
            "Code" : "OXR",
            "Continent" : "North America",
            "City" : "Los Angeles",
            "V4" : [{
                        "StartIp" : "46.22.69.0",
                        "EndIp" : "46.22.69.255",
                        "SubnetMask" : "24"
                }, {
                        "StartIp" : "68.232.40.0",
                        "EndIp" : "68.232.40.255",
                        "SubnetMask" : "24"
                }, {
                        "StartIp" : "72.21.84.0",
                        "EndIp" : "72.21.84.255",
                        "SubnetMask" : "24"
                }, {
                        "StartIp" : "72.21.94.0",
                        "EndIp" : "72.21.94.255",
                        "SubnetMask" : "24"
                }, {
                        "StartIp" : "93.184.218.0",
                        "EndIp" : "93.184.218.255",
                        "SubnetMask" : "24"
```

```
                }
            ],
            "V6" : [{
                        "StartIp" : "2606:2800:4000:0000:0000:0000:0000:0000",
                        "EndIp" : "2606:2800:4000:ffff:ffff:ffff:ffff:ffff",
                        "SubnetMask" : "48"
                }
            ]
            , {
            "Code" : "CPM",
            "Continent" : "North America",
            "City" : "Los Angeles",
            "V4" : [{
                        "StartIp" : "108.161.248.0",
                        "EndIp" : "108.161.249.254",
                        "SubnetMask" : "23"
                }
            ],
            "V6" : [{
                        "StartIp" : "2606:2800:4004:0000:0000:0000:0000:0000",
                        "EndIp" : "2606:2800:4005:ffff:ffff:ffff:ffff:ffff",
                        "SubnetMask" : "47"
                }
            ]
        }
    ]
]
```

Reporting

Overview

Reporting endpoints allow you to generate reports based on CDN activity for your account.

Billing

This section describes billing-related endpoints.

Get Billing Regions

Retrieves a list of billing regions. A billing region must be specified when retrieving billing statistics for a particular month through the Get Traffic Usage endpoint.

Request

A request to retrieve a list of billing regions is described below.

HTTP Method	Request URI
GET	https://api.edgecast.com/v2/reporting/billing/regions

Request Headers
This endpoint only takes advantage of the common request headers described in the **Request Headers** section of the **Request and Response Elements** topic.

Request Body
Request body parameters are not required by this endpoint.

Response

The response to the above request includes an HTTP status code, response headers, and a response body.

Status Code
A status code indicates whether the request was successfully performed. A list of common status codes is provided in the **Status Codes and Error Messages** topic.

Response Headers
The response for this endpoint only returns standard HTTP response headers including those described in the **Response Headers** section of the **Request and Response Elements** topic.

Response Body

The response body for a successful request contains the following response elements for each billing region returned by this endpoint:

Name	Description
Code	A string that identifies the abbreviation associated with the billing region.
Description	A string that provides a description for the billing region.
Id	An integer that defines the ID associated with the billing region.
Name	A string that provides the name of the billing region.
Status	An integer that provides status information for the billing region. Return values for this parameter are: • **0:** Indicates that the billing region is inactive. • **1:** indicates that the billing region is active.
EdgeNodes	This response element contains a listing of POPs associated with the current billing region.
EdgeNodeId	An integer that identifies an edge node (POP) by its system-defined ID.
Code	A string that identifies an edge node by its three letter abbreviation.
Continent	A string that indicates the continent on which the edge node is located.
City	A string that indicates the city where the edge node is located.

Errors

The response body for an unsuccessful request may contain an error element that provides additional information. For a list of common error messages, please refer to the **Status Codes and Error Messages** topic.

Sample Request and Response

A sample JSON request is provided below.

```
GET https://api.edgecast.com/v2/reporting/billing/regions HTTP/1.1

Authorization: TOK:12345678-1234-1234-1234-1234567890ab

Accept: application/json

Host: api.edgecast.com
```

A sample JSON response is provided below.

```
HTTP/1.1 200 OK
Cache-Control: private
Content-Type: application/json; charset=utf-8
Date: Thu, 14 Apr 2016 12:00:00 GMT
Content-Length: 20889

[{
            "Code" : "GL",
            "Description" : "Global",
            "Id" : -1,
            "Name" : "Global",
            "Status" : 1,
            "EdgeNodes" : [{
                        "EdgeNodeId" : 2142,
                        "Code" : "AMS",
                        "Continent" : "Europe",
                        "City" : "Amsterdam"
                }, {
                        ...
                }, {
                        "EdgeNodeId" : 3018,
                        "Code" : "VEN",
                        "Continent" : "Europe",
                        "City" : "Venlo"
                }
            ]
    }, {
            "Code" : "NE",
            "Description" : "North America & Europe",
            "Id" : 0,
            "Name" : "North America & Europe",
            "Status" : 1,
            "EdgeNodes" : [{
                        "EdgeNodeId" : 2920,
                        "Code" : "AMS",
                        "Continent" : "Europe",
                        "City" : "Amsterdam"
                }, {
```

```
                        ...
            }, {
                        "EdgeNodeId" : 2988,
                        "Code" : "BOS",
                        "Continent" : "North America",
                        "City" : "Boston"
            }
        ]
}, {
        "Code" : "AP",
        "Description" : "Asia & South America",
        "Id" : 1,
        "Name" : "Asia & South America",
        "Status" : 1,
        "EdgeNodes" : [{
                        "EdgeNodeId" : 2993,
                        "Code" : "AUA",
                        "Continent" : "Australia",
                        "City" : "Australia"
            }, {
                        ...
            }, {
                        "EdgeNodeId" : 3016,
                        "Code" : "MEB",
                        "Continent" : "Australia",
                        "City" : "Melbourne"
            }
        ]
}, {
        "Code" : "GEO:IN",
        "Description" : "",
        "Id" : 2,
        "Name" : "India",
        "Status" : 1,
        "EdgeNodes" : [{
                        "EdgeNodeId" : 634,
                        "Code" : "INA",
                        "Continent" : "Asia",
```

```
                            "City" : "Mumbai"
                }, {
                            "EdgeNodeId" : 635,
                            "Code" : "INB",
                            "Continent" : "Asia",
                            "City" : "Bangalore"
                }
        ]
}, {
        "Code" : "GEO:CN",
        "Description" : "",
        "Id" : 3,
        "Name" : "China",
        "Status" : 1,
        "EdgeNodes" : [{
                            "EdgeNodeId" : 636,
                            "Code" : "CNA",
                            "Continent" : "Asia",
                            "City" : "China - A"
                }, {
                            "EdgeNodeId" : 637,
                            "Code" : "CNB",
                            "Continent" : "Asia",
                            "City" : "China - B"
                }
        ]
}, {
        "Code" : "NET:ID",
        "Description" : "Indonesia",
        "Id" : 4,
        "Name" : "Indonesia",
        "Status" : 1,
        "EdgeNodes" : [{
                            "EdgeNodeId" : 1005,
                            "Code" : "BTH",
                            "Continent" : "Asia",
                            "City" : "Batam"
                }, {
```

```
                            "EdgeNodeId" : 1006,
                            "Code" : "CGK",
                            "Continent" : "Asia",
                            "City" : "Jakarta"
                    }
            ]
    }, {
            "Code" : "NET:NO",
            "Description" : "Nordics",
            "Id" : 5,
            "Name" : "Nordics",
            "Status" : 1,
            "EdgeNodes" : [{
                            "EdgeNodeId" : 2704,
                            "Code" : "CPH",
                            "Continent" : "Europe",
                            "City" : "Copenhagen"
                    }, {
                            "EdgeNodeId" : 2705,
                            "Code" : "HEL",
                            "Continent" : "Europe",
                            "City" : "Helsinki"
                    }, {
                            "EdgeNodeId" : 2706,
                            "Code" : "STO",
                            "Continent" : "Europe",
                            "City" : "Stockholm"
                    }
            ]
    }, {
            "Code" : "NET:TW",
            "Description" : "Taiwan",
            "Id" : 6,
            "Name" : "Taiwan",
            "Status" : 1,
            "EdgeNodes" : [{
                            "EdgeNodeId" : 2703,
                            "Code" : "KHH",
```

```
                                "Continent" : "Asia",

                                "City" : "Kaohsiung"

                }

        ]

}, {

        "Code" : "GEO:LA",

        "Description" : "Latin America",

        "Id" : 7,

        "Name" : "Latin America",

        "Status" : 1,

        "EdgeNodes" : [{

                        "EdgeNodeId" : 1825,

                        "Code" : "CGH",

                        "Continent" : "South America",

                        "City" : "Sao Paulo"

                }

        ]

}, {

        "Code" : "NET:KR",

        "Description" : "Korea",

        "Id" : 8,

        "Name" : "Korea",

        "Status" : 1,

        "EdgeNodes" : [{

                        "EdgeNodeId" : 2702,

                        "Code" : "ICN",

                        "Continent" : "Asia",

                        "City" : "Seoul"

                }

        ]

}

]
```

Get Billing Usage Data

Returns billing usage data for the specified month. This data may be filtered by one of the following criteria:

- Billing Region
- Country
- POP(s)

Request

A request to retrieve billing usage data is described below. When submitting this request, you will need to define the following terms:

- **AccountNumber:** This term should be replaced by your CDN account number.
- **Platform:** This term should be replaced by the ID associated with the desired platform. Valid values for this parameter are listed below.
  - **3:** HTTP Large
  - **7:** HTTP Large (SSL Traffic Only)
  - **8:** HTTP Small
  - **9:** HTTP Small (SSL Traffic Only)
  - **14:** Application Delivery Network (ADN)
  - **15:** Application Delivery Network (ADN) – (SSL Traffic Only)
- **BillingMonth:** Replace this variable with the 1st of the month for which billing information will be returned.
  Syntax: *YYYY-MM*-01
- **RegionID:** Replace this variable with the ID of the billing region for which billing information will be returned.

  Tip: Use the Get Billing Regions endpoint to retrieve a listing of billing regions and IDs.

  Note: The region, country, and pops query string parameters are optional and mutually exclusive. A request to this endpoint may include up to one of these filters. The region query string parameter (e.g., &region=0) should only be defined when billing data should be restricted to the specified billing region.

- **CountryCode:** Replace this variable with the ISO 3166 code corresponding to the country for which billing information will be returned.

  Tip: A list of country codes is available from the [Country Codes (ISO 3166) article](#) in the CDN Help Center.

- **POPs:** Optional. Limit report data to one or more POPs by replacing this variable with a comma-delimited list of the desired POPs.

> **Tip:** Use the Get All Edge Nodes endpoint to retrieve a list of POPs and their codes.

> **Note:** The region, country, and pops query string parameters are optional and mutually exclusive. A request to this endpoint may include up to one of these filters. The pops query string parameter (e.g., oxr,dca,mia) should only be defined when billing data should be restricted to the specified POP(s).

HTTP Method	Request URI
GET	https://api.edgecast.com/v2/reporting/customers/*AccountNumber*/media /*Platform*/units/0/billingtraffic?begindate=*BillingMonth*&region=*RegionID* &country=*CountryCode*&pops=*POPs*

Request Headers

This endpoint only takes advantage of the common request headers described in the **Request Headers** section of the **Request and Response Elements** topic.

Request Body

Request body parameters are not required by this endpoint.

Response

The response to the above request includes an HTTP status code, response headers, and a response body.

Status Code

A status code indicates whether the request was successfully performed. A list of common status codes is provided in the **Status Codes and Error Messages** topic.

Response Headers

The response for this endpoint only returns standard HTTP response headers including those described in the **Response Headers** section of the **Request and Response Elements** topic.

Response Body

The response body for a successful request contains the following response elements for each billing region returned by this endpoint:

Name	Data Type	Description
AccountNumber	String	Indicates the CDN account number associated with the requested billing data.

Name	Data Type	Description
MediaTypeId	Integer	Indicates the service associated with the requested billing data. Valid values are: • **3:** HTTP Large • **7:** HTTP Large (SSL Traffic Only) • **8:** HTTP Small • **9:** HTTP Small (SSL Traffic Only) • **14:** Application Delivery Network (ADN) • **15:** Application Delivery Network (ADN) – (SSL Traffic Only)
Country	String	Indicates the code for the country for which billing data was provided. This code will always match the value defined in the request's country query string parameter. **Note:** This response parameter is only returned when the country query string parameter is defined in the request.
RegionId	Integer	Indicates the ID of the region for which billing data was provided. This ID will always match the value defined in the request's region query string parameter. **Note:** This response parameter is only returned when the region query string parameter is defined in the request.
Pops	String	Indicates the set of POPs for which billing data was provided. Valid values are: • **all:** Indicates that the provided billing data was derived from all POPs. • **POP Listing:** If billing data is being filtered by region, country, or POP(s), then this parameter will be set to a comma-delimited list of POPs for which billing data was provided.
UsageUnits	Integer	This parameter should always return 0.
Data	Array Object Values	Contains a data object that describes billing data.

Name	Data Type	Description
Bandwidth	Number Floating Point	Indicates bandwidth usage, in Mbps, for the requested billing month. **Note:** The reported usage information reflects any filters (e.g., region, country, or POPs) that may have been defined in the request.
DataTransferred	Number Floating Point	Indicates the total amount of data transferred, in GBs, for the requested billing month. **Note:** The reported usage information reflects any filters (e.g., region, country, or POPs) that may have been defined in the request.
StartDate	String	Indicates the month for which billing information was reported. **Syntax:** *YYYY-MM*-01

Errors

The response body for an unsuccessful request may contain an error element that provides additional information. For a list of common error messages, please refer to the **Status Codes and Error Messages** topic.

Sample Request and Response

A sample JSON request is provided below.

```
GET
https://api.edgecast.com/v2/reporting/customers/0001/media/14/units/0/billingtraffic
?begindate=2018-01-01 HTTP/1.1

Authorization: TOK:12345678-1234-1234-1234-1234567890ab

Accept: application/json

Host: api.edgecast.com
```

A sample JSON response is provided below.

```
HTTP/1.1 200 OK

Cache-Control: private

Content-Type: application/json; charset=utf-8

Date: Thu, 14 Apr 2016 12:00:00 GMT

Content-Length: 248

[{

            "AccountNumber": "0001",

            "MediaTypeId": 14,

            "Pops": "all",

            "UsageUnits": 0,

            "Data": [{

                        "Bandwidth": 1484302.2916001333,

                        "DataTransferred": 191320916.11106589,

                        "StartDate": "01\/1\/2018 12:00:00 AM"

                }

            ]

        }

]
```

Customer Accounts

This section describes the endpoints that can be used to retrieve the name and the CDN account number associated with a customer account.

Get Customer Account Number

Retrieves a customer's CDN account number based on a custom ID.

Request

A request to retrieve a customer's account number is described below. When submitting this request, you will need to define the following term:

- **CustomID:** This term should be replaced by the custom ID associated with the desired customer account.

HTTP Method	Request URI
GET	https://api.edgecast.com/v2/reporting/customers/accountnumber?customercustomid=*CustomID*

Request Headers
This endpoint only takes advantage of the common request headers described in the **Request Headers** section of the **Request and Response Elements** topic.

Request Body
Request body parameters are not required by this endpoint.

Response

The response to the above request includes an HTTP status code, response headers, and a response body.

Status Code
A status code indicates whether the request was successfully performed. A list of common status codes is provided in the **Status Codes and Error Messages** topic.

Response Headers
The response for this endpoint only returns standard HTTP response headers including those described in the **Response Headers** section of the **Request and Response Elements** topic.

Response Body
The response body for a successful request contains the following response element:

Name	Description
AccountNumber	A string that identifies the customer account number associated with the specified custom ID.

Errors

The response body for an unsuccessful request may contain an error element that provides additional information. For a list of common error messages, please refer to the **Status Codes and Error Messages** topic.

Sample Request and Response

A sample JSON request is provided below.

```
GET
https://api.edgecast.com/v2/reporting/customers/accountnumber?customercustomid=CID01
HTTP/1.1

Authorization: TOK:12345678-1234-1234-1234-1234567890ab

Accept: application/json

Host: api.edgecast.com
```

A sample JSON response is provided below.

```
HTTP/1.1 200 OK

Cache-Control: private

Content-Type: application/json; charset=utf-8

Date: Thu, 14 Apr 2016 12:00:00 GMT

Content-Length: 245


{

        "AccountNumber" : "0001"

}
```

Get Customer Name

Retrieves a customer's name by its CDN account number.

Request

A request to retrieve a customer's name is described below. When submitting this request, you will need to define the following term:

- **xxxx:** This term should be replaced by the account number associated with the desired customer account.

HTTP Method	Request URI
GET	https://api.edgecast.com/v2/reporting/customers/*xxxx*/customername

Request Headers

This endpoint only takes advantage of the common request headers described in the **Request Headers** section of the **Request and Response Elements** topic.

Request Body

Request body parameters are not required by this endpoint.

Response

The response to the above request includes an HTTP status code, response headers, and a response body.

Status Code

A status code indicates whether the request was successfully performed. A list of common status codes is provided in the **Status Codes and Error Messages** topic.

Response Headers

The response for this endpoint only returns standard HTTP response headers including those described in the **Response Headers** section of the **Request and Response Elements** topic.

Response Body

The response body for a successful request contains the following response element:

Name	Description
AccountName	A string that identifies the name associated with the specified customer account number.

Errors

The response body for an unsuccessful request may contain an error element that provides additional information. For a list of common error messages, please refer to the **Status Codes and Error Messages** topic.

Sample Request and Response

A sample JSON request is provided below.

```
GET https://api.edgecast.com/v2/reporting/customers/0001/customername HTTP/1.1

Authorization: TOK:12345678-1234-1234-1234-1234567890ab

Accept: application/json

Host: api.edgecast.com
```

A sample JSON response is provided below.

```
HTTP/1.1 200 OK

Cache-Control: private

Content-Type: application/json; charset=utf-8

Date: Thu, 14 Apr 2016 12:00:00 GMT

Content-Length: 34


{

        "AccountName" : "My Company"

}
```

Core Reporting

This section describes the Core Reporting endpoints that can be used to retrieve data about activity on your CDN account.

Note: Core Reporting endpoints can only generate reports for CDN activity within the last 18 months.

Get All Data Transferred

This platform-independent endpoint retrieves the total amount of data transferred (bytes) for your CDN account over a specific time period.

Note: This endpoint does not include data for transactions that did not complete during the requested time period, even if the transaction started before or during the time period covered by the report.

Request

A request to retrieve data transferred is described below. When submitting this request, you will need to define the following terms:

- **AccountNumber:** This term should be replaced by your CDN account number.

- **StartDateTime:** This term should be replaced by the start date/time for the report. Only activity that took place after the specified date/time will be included in the report. The format for this term is: *YYYY-MM-DD*T*hh*:*mm*:*ss*.

- **EndDateTime:** This term should be replaced by the end date/time for the report. Activity that took place after the specified date/time will not be included in the report. The format for this term is: *YYYY-MM-DD*T*hh*:*mm*:*ss*.

- **POPs:** Optional. You can choose to limit report data to one or more POPs.

    - **All POPs:** If you would like to generate report data for all POPs, then you should not include "&pops=*POPs* " parameter in the request.

    - **POP-Specific Report:** Replace the term *POPs* with a comma-delimited list of the desired POPs (e.g., oxr,dca,mia). Each POP's code is reported by the Code response element in the Get All Edge Nodes endpoint.

- **RegionID:** Optional. You can choose to limit report data by region. Use the Get Billing Regions endpoint to retrieve a listing of regions and their IDs. If the regionid parameter is not specified, then report data for all regions will be returned.

Important: Returns data in 5 minute intervals (e.g., 00:00:00, 00:05:00, 00:10:00, etc.). Specifying a time that falls in between a 5 minute interval (e.g., 00:02:59) will include all data associated with that 5 minute interval (e.g., 00:00:00 – 00:04:59).

Important: The pops and regionid parameters are mutually exclusive. Specifying both parameters will result in an error.

Note: The time portion (i.e., *hh*:*mm*:*ss*) of the StartDateTime and EndDateTime request parameters is optional. If a specific time is not specified, then a default time (i.e., 00:00:00) will be used.

Note: For more information on date/time format, please refer to **Appendix B: Report Date/Time Format**.

HTTP Method	Request URI
GET	https://api.edgecast.com/v2/reporting/customers/*AccountNumber/*bytestransferred ?begindate=*StartDateTime*&enddate=*EndDateTime*&pops=*POPs*&regionid=*RegionID*

Request Headers

This endpoint only takes advantage of the common request headers described in the **Request Headers** section of the **Request and Response Elements** topic.

Request Body

Request body parameters are not required by this endpoint.

Response

The response to the above request includes an HTTP status code, response headers, and a response body.

Status Code

A status code indicates whether the request was successfully performed. A list of common status codes is provided in the **Status Codes and Error Messages** topic.

Response Headers

The response for this endpoint only returns standard HTTP response headers including those described in the **Response Headers** section of the **Request and Response Elements** topic.

Response Body

The response body for a successful request contains the following response element:

Name	Description
Bytes	An integer that indicates the number of bytes transferred over the given time period. This statistic includes CDN activity for all platforms.
	Note: Keep in mind that the pops request element determines whether Returns the amount of data transferred for the entire CDN network or if it will be limited to specific POP locations.

The response body for an unsuccessful request may contain an error element that provides additional information. For a list of common error messages, please refer to the **Status Codes and Error Messages** topic.

Sample Request and Response

A sample JSON request is provided below.

```
GET
https://api.edgecast.com/v2/reporting/customers/0001/bytestransferred?begindate=2012
-11-01&enddate=2012-12-01 HTTP/1.1

Authorization: TOK:12345678-1234-1234-1234-1234567890ab

Accept: application/json

Host: api.edgecast.com
```

A sample JSON response is provided below.

```
HTTP/1.1 200 OK

Cache-Control: private

Content-Type: application/json; charset=utf-8

Date: Thu, 14 Apr 2016 12:00:00 GMT

Content-Length: 43


{

        "Bytes" : 2577643208458154598455511324

}
```

Get Cache Status Activity

Retrieves the total amount of hits over a given time period for each cache status on a specified platform.

Request

A request to retrieve cache status statistics is described below. When submitting this request, you will need to define the following terms:

- **AccountNumber:** This term should be replaced by your CDN account number.

- **Platform:** This term should be replaced by an integer that indicates the platform for which a report will be generated. Valid values for this term are:

    - **3:** HTTP Large

    - **8:** HTTP Small

    - **14:** Application Delivery Network (ADN)

- **StartDateTime:** This term should be replaced by the start date/time for the report. Only activity that took place after the specified date/time will be included in the report. The format for this term is: *YYYY-MM-DD*T*hh*:*mm*:*ss*.

- **EndDateTime:** This term should be replaced by the end date/time for the report. Activity that took place after the specified date/time will not be included in the report. The format for this term is: *YYYY-MM-DD*T*hh*:*mm*:*ss*.

Important: Returns data in 1 hour intervals (e.g., 00:00:00, 01:00:00, 02:00:00, etc.). Specifying a time that falls in between a 1 hour interval (e.g., 00:50:05) will include all data associated with that hour (e.g., 00:00:00 – 00:59:59).

Note: The time portion (i.e., *hh*:*mm*:*ss*) of the StartDateTime and EndDateTime request parameters is optional. If a specific time is not specified, then a default time (i.e., 00:00:00) will be used.

Note: For more information on date/time format, please refer to **Appendix B: Report Date/Time Format**.

HTTP Method	Request URI
GET	https://api.edgecast.com/v2/reporting/customers/*AccountNumber*/media/*Platform*/cachestats?begindate=*StartDateTime*&enddate=*EndDateTime*

Request Headers

This endpoint only takes advantage of the common request headers described in the **Request Headers** section of the **Request and Response Elements** topic.

Request Body

Request body parameters are not required by this endpoint.

Response

The response to the above request includes an HTTP status code, response headers, and a response body.

Status Code

A status code indicates whether the request was successfully performed. A list of common status codes is provided in the **Status Codes and Error Messages** topic.

Response Headers

The response for this endpoint only returns standard HTTP response headers including those described in the **Response Headers** section of the **Request and Response Elements** topic.

Response Body

The response body for a successful request contains the following response elements for each cache status returned by this endpoint:

Name	Description
Hits	An integer that indicates the total number of hits for the cache status identified by the Name return parameter.
Name	A string that identifies a cache status by its name. Valid return values are defined below.

A list of valid cache statuses are defined below.

Cache Status	Description
CONFIG_NOCACHE	This status is reported when an asset's Cache-Control and Expires headers indicate that it should not be cached on a POP or by the HTTP client. As a result, the asset was served from the origin server.
NONE	This status indicates that a cache content freshness check was not performed. This check is skipped when Token-Based Authentication denies a request or when an HTTP request method is used that bypasses cache (e.g., PUT, DELETE, etc).
TCP_CLIENT_REFRESH_MISS	This status is reported when an HTTP client (e.g., browser) forces an edge server to retrieve a new version of a stale asset from the origin server. By default, our servers prevent an HTTP client from forcing our edge servers to retrieve a new version of the asset from the origin server. However, this behavior can be overridden through the use of HTTP Rules Engine.
TCP_EXPIRED_HIT	This status is reported when a request that targeted an asset with an expired time to live (TTL), such as when the asset's max-age has expired, was served directly from the POP to the client. An expired request typically results in a revalidation request to the origin server. In order for a TCP_EXPIRED_HIT to occur, the origin server must indicate that a newer version of the asset does not exist. This type of situation will typically update that asset's Cache-Control and Expires headers.
TCP_EXPIRED_MISS	This status is reported when a newer version of an expired cached asset is served from the POP to the client. If the TTL for a cached asset has expired (e.g., expired max-age), then a check will be performed on the origin server for a newer version of that asset. If an updated version is found, then it will be served to the client instead of the cached version. If the origin server or HTTP Rules Engine does not specifically prevent that asset from being cached, then it will be cached on the POP closest to the client that requested it.
TCP_HIT	This status is reported when a request is served directly from the POP to the client. An asset is immediately served from a POP when it is cached on the POP closest to the client and it has a valid TTL. TTL is determined by the Cache-Control: s-maxage, Cache-Control: max-age, and Expires headers.

Cache Status	Description
TCP_MISS	This status indicates that a cached version of the requested asset was not found on the POP closest to the client. The asset will be requested from either an origin server or an origin shield server and then served to the client. If the origin server or HTTP Rules Engine does not specifically prevent that asset from being cached, then it will be cached on the POP closest to the client that requested it.
UNCACHEABLE	This status is reported when a request results in an error (e.g., 403 Forbidden, 404 Not Found, etc.).

Errors

The response body for an unsuccessful request may contain an error element that provides additional information. For a list of common error messages, please refer to the **Status Codes and Error Messages** topic.

Sample Request and Response

A sample JSON request is provided below.

```
GET
https://api.edgecast.com/v2/reporting/customers/0001/media/3/cachestats?begindate=20
11-06-01&enddate=2011-07-01 HTTP/1.1

Authorization: TOK:12345678-1234-1234-1234-1234567890ab

Accept: application/json

Host: api.edgecast.com
```

A sample JSON response is provided below.

```
HTTP/1.1 200 OK

Cache-Control: private

Content-Type: application/json; charset=utf-8

Date: Thu, 14 Apr 2016 12:00:00 GMT

Content-Length: 142


[{

        "Hits" : 87619673,

        "Name" : "TCP_HIT"

    }, {

        "Hits" : 22725,

        "Name" : "TCP_MISS"

    }, {

        "Hits" : 8750,
```

```
            "Name" : "CONFIG_NOCACHE"
    }, {

            "Hits" : 2388,

            "Name" : "UNCACHEABLE"

    }
]
```

Get CNAME Hits (Deprecated)

Important: This endpoint has been deprecated and support for it will slowly be phased out. Data collection for this endpoint stopped as of 11/1/2012. However, for the purpose of viewing historical data, this endpoint will remain available for a reasonable time period.

Retrieves the total amount of hits and data transferred over a given time period for each CNAME on a specified platform. For the purpose of this endpoint, a CNAME consists of all edge CNAMEs and the system-defined hostname (e.g., wpc.0001.edgecastcdn.net) assigned to your customer account.

Note: A customer's system-defined hostname is a CNAME to a server on our network.

Note: This endpoint does not include hits/data for transactions that did not complete during the requested time period, even if the transaction started before or during the time period covered by the report.

Request

A request to retrieve CNAME statistics is described below. When submitting this request, you will need to define the following terms:

- **AccountNumber:** This term should be replaced by your CDN account number.

- **Platform:** This term should be replaced by an integer that indicates the platform for which a report will be generated. Valid values for this term are:

    - **3:** HTTP Large

    - **8:** HTTP Small

- **StartDateTime:** This term should be replaced by the start date/time for the report. Only activity that took place after the specified date/time will be included in the report. The format for this term is: *YYYY-MM-DD*T*hh*:*mm*:*ss*.

- **EndDateTime:** This term should be replaced by the end date/time for the report. Activity that took place after the specified date/time will not be included in the report. The format for this term is: *YYYY-MM-DD*T*hh*:*mm*:*ss*.

Important: This endpoint cannot request report data that occurs on or after 11/1/2012 00:00:00.

Important: Returns data in 1 hour intervals (e.g., 00:00:00, 01:00:00, 02:00:00, etc.). Specifying a time that falls in between a 1 hour interval (e.g., 00:50:05) will include all data associated with that hour (e.g., 00:00:00 – 00:59:59).

Note: The time portion (i.e., *hh:mm:ss*) of the StartDateTime and EndDateTime request parameters is optional. If a specific time is not specified, then a default time (i.e., 00:00:00) will be used.

Note: For more information on date/time format, please refer to **Appendix B: Report Date/Time Format**.

HTTP Method	Request URI
GET	https://api.edgecast.com/v2/reporting/customers/*AccountNumber/*media /*Platform*/cnames?begindate=*StartDateTime*&enddate=*EndDateTime*

Request Headers

This endpoint only takes advantage of the common request headers described in the **Request Headers** section of the **Request and Response Elements** topic.

Request Body

Request body parameters are not required by this endpoint.

Response

The response to the above request includes an HTTP status code, response headers, and a response body.

Status Code

A status code indicates whether the request was successfully performed. A list of common status codes is provided in the **Status Codes and Error Messages** topic.

Response Headers

The response for this endpoint only returns standard HTTP response headers including those described in the **Response Headers** section of the **Request and Response Elements** topic.

Response Body

The response body for a successful request contains the following response elements for each CNAME returned by this endpoint:

Name	Description
Bytes	An integer that indicates the total number of data transferred (bytes) for a particular CNAME.

Name	Description
Hits	An integer that indicates the total number of hits for a particular CNAME.
Name	A string that identifies a CNAME.

Errors

The response body for an unsuccessful request may contain an error element that provides additional information. For a list of common error messages, please refer to the **Status Codes and Error Messages** topic.

Sample Request and Response

A sample JSON request is provided below.

```
GET
https://api.edgecast.com/v2/reporting/customers/0001/media/3/cnames?begindate=2011-
06-01&enddate=2011-07-01 HTTP/1.1

Authorization: TOK:12345678-1234-1234-1234-1234567890ab

Accept: application/json

Host: api.edgecast.com
```

A sample JSON response is provided below.

```
HTTP/1.1 200 OK

Cache-Control: private

Content-Type: application/json; charset=utf-8

Date: Thu, 14 Apr 2016 12:00:00 GMT

Content-Length: 216


[{
            "Bytes" : 26182770916,
            "Hits" : 228445,
            "Name" : "wpc.0001.edgecastcdn.net"
      }, {
            "Bytes" : 6958089484,
            "Hits" : 16646983,
            "Name" : "gp1.wpc.edgecastcdn.net"
      }, {
            "Bytes" : 36890,
            "Hits" : 97,
            "Name" : "images.hostname.org"
      }
]
```

Get Current Storage Usage

Returns the current amount of storage space being used on a CDN origin server.

Request

A request to retrieve current storage space usage is described below. When submitting this request, you will need to define the following term:

- **AccountNumber:** This term should be replaced by your CDN account number.

HTTP Method	Request URI
GET	https://api.edgecast.com/v2/reporting/customers/*AccountNumber*/lateststorageusage

Request Headers

This endpoint only takes advantage of the common request headers described in the **Request Headers** section of the **Request and Response Elements** topic.

Request Body

Request body parameters are not required by this endpoint.

Response

The response to the above request includes an HTTP status code, response headers, and a response body.

Status Code

A status code indicates whether the request was successfully performed. A list of common status codes is provided in the **Status Codes and Error Messages** topic.

Response Headers

The response for this endpoint only returns standard HTTP response headers including those described in the **Response Headers** section of the **Request and Response Elements** topic.

Response Body

The response body for a successful request contains the following response element:

Name	Description
UsageResult	A number (floating-point) that indicates the current amount of disk space usage (GB) on a CDN origin server.

Errors

The response body for an unsuccessful request may contain an error element that provides additional information. For a list of common error messages, please refer to the **Status Codes and Error Messages** topic.

Sample Request and Response

A sample JSON request is provided below.

```
GET https://api.edgecast.com/v2/reporting/customers/0001/lateststorageusage HTTP/1.1
Authorization: TOK:12345678-1234-1234-1234-1234567890ab
Accept: application/json
Host: api.edgecast.com
```

A sample JSON response is provided below.

```
HTTP/1.1 200 OK
Cache-Control: private
Content-Type: application/json; charset=utf-8
Date: Thu, 14 Apr 2016 12:00:00 GMT
Content-Length: 20


{
        "UsageResult" : 85.5
}
```

Get Data Transferred by Platform

Retrieves the total amount of data transferred over the specified platform in a given time period.

Request

A request to retrieve data transferred information by platform is described below. When submitting this request, you will need to define the following terms:

- **AccountNumber:** This term should be replaced by your CDN account number.

- **Platform:** This term should be replaced by an integer that indicates the platform for which a report will be generated. Valid values for this term are:

    - **2:** Flash Media Streaming

    - **3:** HTTP Large

    - **7:** HTTP Large (SSL Traffic Only)

    - **8:** HTTP Small

    - **9:** HTTP Small (SSL Traffic Only)

    - **14:** Application Delivery Network (ADN)

    - **15:** Application Delivery Network (ADN) – (SSL Traffic Only)

- **StartDateTime:** This term should be replaced by the start date/time for the report. Only activity that took place after the specified date/time will be included in the report. The format for this term is: *YYYY-MM-DD*T*hh*:*mm*:*ss*.

- **EndDateTime:** This term should be replaced by the end date/time for the report. Activity that took place after the specified date/time will not be included in the report. The format for this term is: *YYYY-MM-DD*T*hh*:*mm*:*ss*.

- **POPs:** Optional. You can choose to filter report data to one or more POPs as indicated below.

    - **All POPs:** If you would like to generate report data for all POPs, then you should not include "&pops=*POPs* " parameter in the request.

    - **POP-Specific Report:** Replace the term *POPs* with a comma-delimited list of the desired POPs (e.g., oxr,dca,mia). Each POP's code is reported by the Code response element in the Get All Edge Nodes endpoint.

Important: Returns data in 5 minute intervals (e.g., 00:00:00, 00:05:00, 00:10:00, etc.). Specifying a time that falls in between a 5 minute interval (e.g., 00:02:59) will include all data associated with that 5 minute interval (e.g., 00:00:00 – 00:04:59).

Note: The time portion (i.e., *hh:mm:ss*) of the StartDateTime and EndDateTime request parameters is optional. If a specific time is not specified, then a default time (i.e., 00:00:00) will be used.

Note: For more information on date/time format, please refer to **Appendix B: Report Date/Time Format**.

HTTP Method	Request URI
GET	https://api.edgecast.com/v2/reporting/customers/*AccountNumber*/media/*Platform* /bytestransferred?begindate=*StartDateTime*&enddate=*EndDateTime*&pops=*POPs*

Request Headers

This endpoint only takes advantage of the common request headers described in the **Request Headers** section of the **Request and Response Elements** topic.

Request Body

Request body parameters are not required by this endpoint.

Response

The response to the above request includes an HTTP status code, response headers, and a response body.

Status Code

A status code indicates whether the request was successfully performed. A list of common status codes is provided in the **Status Codes and Error Messages** topic.

Response Headers

The response for this endpoint only returns standard HTTP response headers including those described in the **Response Headers** section of the **Request and Response Elements** topic.

Response Body

The response body for a successful request contains the following response element:

Name	Description
Bytes	An integer that indicates the total number of bytes that were transferred on the specified platform over a given time period.
	Note: Keep in mind that the pops request parameter determines whether Returns the amount of data transferred for the entire CDN network or if it will be limited to specific POP locations.

Errors

The response body for an unsuccessful request may contain an error element that provides additional information. For a list of common error messages, please refer to the **Status Codes and Error Messages** topic.

Sample Request and Response

A sample JSON request is provided below.

```
GET
https://api.edgecast.com/v2/reporting/customers/0001/media/3/bytestransferred?begind
ate=2012-11-01&enddate=2012-12-01 HTTP/1.1

Authorization: TOK:12345678-1234-1234-1234-1234567890ab

Accept: application/json

Host: api.edgecast.com
```

A sample JSON response is provided below.

```
HTTP/1.1 200 OK

Cache-Control: private

Content-Type: application/json; charset=utf-8

Date: Thu, 14 Apr 2016 12:00:00 GMT

Content-Length: 21


{

        "Bytes" : 64457041333

}
```

Get Data Transferred by Platform & Interval

Retrieves the amount of data transferred (bytes) for your CDN account. The data returned by this report can be filtered to only include CDN traffic that meets the following criteria:

- Date range

- Platform

- POP locations

- Region

Additionally, you can define the time interval that will be used to report the amount of data transferred.

Note: This endpoint does not include data for transactions that did not complete during the requested time period, even if the transaction started before or during the time period covered by the report.

Request

A request to retrieve data transferred information by time interval is described below. When submitting this request, you will need to define the following terms:

- **AccountNumber:** This term should be replaced by your CDN account number.

- **StartDateTime:** This term should be replaced by the start date/time for the report. Only activity that completed after the specified date/time will be included in the report. The format for this term is: *YYYY-MM-DD*T*hh*:*mm*:*ss*.

- **EndDateTime:** This term should be replaced by the end date/time for the report. Activity that completed after the specified date/time will be excluded from the report. The format for this term is: *YYYY-MM-DD*T*hh*:*mm*:*ss*.

- **Platform:** Optional. This term should be replaced by an integer that indicates the platform for which a report will be generated. If the mediatypeid parameter is not specified, then report data for all platforms will be returned. Valid values for this term are:

    - **2:** Flash Media Streaming

    - **3:** HTTP Large

    - **7:** HTTP Large (SSL Traffic Only)

    - **8:** HTTP Small

    - **9:** HTTP Small (SSL Traffic Only)

    - **14:** Application Delivery Network (ADN)

    - **15:** Application Delivery Network (ADN) – (SSL Traffic Only)

- **Interval:** Optional. This term should be replaced by an integer that indicates the time interval that will be used to return report data. If the intervalid parameter is not specified, then report data will be returned in five minute intervals. Valid values for this term are:
    - **1:** 5 minute intervals (e.g., 00:00:00, 00:05:00, 00:10:00, etc.)
    - **2:** Hourly intervals (e.g., 00:00:00, 01:00:00, 02:00:00, etc.)
    - **3:** Daily intervals (e.g., 2012-11-01T00:00:00, 2012-11-02T00:00:00, 2012-11-03T00:00:00, etc.)
- **POPs:** Optional. You can choose to limit report data to one or more POPs.
    - **All POPs:** If you would like to generate report data for all POPs, then you should not include "&pops=*POPs* " parameter in the request.
    - **POP-Specific Report:** Replace the term *POPs* with a comma-delimited list of the desired POPs (e.g., oxr,dca,mia). Each POP's code is reported by the Code response element in the Get All Edge Nodes endpoint.
- **RegionID:** Optional. You can choose to limit report data by region. Use the Get Billing Regions endpoint to retrieve a listing of regions and their IDs. If the regionid parameter is not specified, then report data for all regions will be returned.

Important: Specifying a time that falls in between the time interval specified for this endpoint (e.g., 00:04:59) will retrieve all data associated with that time interval (e.g., 00:00:00 – 00:04:59).

Important: The pops and regionid parameters are mutually exclusive. Specifying both parameters will result in an error.

Note: The specified time interval cannot exceed 45 days.

Note: The time portion (i.e., *hh:mm:ss*) of the StartDateTime and EndDateTime request parameters is optional. If a specific time is not specified, then a default time (i.e., 00:00:00) will be used.

Note: For more information on date/time format, please refer to **Appendix B: Report Date/Time Format**.

HTTP Method	Request URI
GET	https://api.edgecast.com/v2/reporting/customers/*AccountNumber/*bytestransferred/interval?begindate=*StartDateTime*&enddate=*EndDateTime*&mediatypeid=*Platform*&intervalid=*Interval*&pops=*POPs*&regionid=*RegionID*

Request Headers

This endpoint only takes advantage of the common request headers described in the **Request Headers** section of the **Request and Response Elements** topic.

Request Body

Request body parameters are not required by this endpoint.

Response

The response to the above request includes an HTTP status code, response headers, and a response body.

Status Code

A status code indicates whether the request was successfully performed. A list of common status codes is provided in the **Status Codes and Error Messages** topic.

Response Headers

The response for this endpoint only returns standard HTTP response headers including those described in the **Response Headers** section of the **Request and Response Elements** topic.

Response Body

The response body for a successful request contains the following response elements.

Name	Description
AN	A string that identifies a customer by its system-defined account number.
MediaTypeId	An integer that identifies the platform for which statistics are being reported. Valid values for this parameter are: • **2:** Flash Media Streaming • **3:** HTTP Large • **7:** HTTP Large (SSL Traffic Only) • **8:** HTTP Small • **9:** HTTP Small (SSL Traffic Only) • **14:** Application Delivery Network (ADN) • **15:** Application Delivery Network (ADN) – (SSL Traffic Only)

Name	Description
Data	This response element contains a set of time slices that report the amount of data transferred over the specified platform and time period. The number and frequency of time slices is determined by the intervalid request parameter.
	Note: If a platform is not specified in the request URI, then an instance of this response element will be returned for each platform. This will occur regardless of whether CDN activity took place for that platform.
DataTransferred	Encapsulates the report data returned for a specific platform and time interval.
	Note: In JSON, this response element is indicated as "{ … }."
	Note: This response element is repeated until the entire time period indicated in the request URI has been covered.
DateTimeSlice	A string that identifies a time slice by its start date and time. This response element indicates this start date and time using the following format: *YYYY-MM-DD hh:mm*.
Bytes	An integer that indicates the number of bytes that were transferred during a specific time slice for the specified platform. This value only includes traffic that met the criteria specified in the GET request.

Errors

The response body for an unsuccessful request may contain an error element that provides additional information. For a list of common error messages, please refer to the **Status Codes and Error Messages** topic.

Sample Request and Response

A sample JSON request is provided below.

```
GET
https://api.edgecast.com/v2/reporting/customers/0001/bytestransferred/interval?begin
date=2012-10-01&enddate=2012-10-01T05:00:00&mediatypeid=3&intervalid=2 HTTP/1.1

Authorization: TOK:12345678-1234-1234-1234-1234567890ab

Accept: application/json

Host: api.edgecast.com
```

A sample JSON response is provided below.

```
HTTP/1.1 200 OK
Cache-Control: private
Content-Type: application/json; charset=utf-8
Date: Thu, 14 Apr 2016 12:00:00 GMT
Content-Length: 512

[{
             "AN" : "0001",
             "MediaTypeId" : 3,
             "Data" : [{
                          "DateTimeSlice" : "2012-10-01 00:00",
                          "Bytes" : 516514354
                    }, {
                          "DateTimeSlice" : "2012-10-01 01:00",
                          "Bytes" : 465465452
                    }, {
                          "DateTimeSlice" : "2012-10-01 02:00",
                          "Bytes" : 688465452
                    }, {
                          "DateTimeSlice" : "2012-10-01 03:00",
                          "Bytes" : 789456321
                    }, {
                          "DateTimeSlice" : "2012-10-01 04:00",
                          "Bytes" : 623845975
                    }, {
                          "DateTimeSlice" : "2012-10-01 05:00",
                          "Bytes" : 689746521
                    }
               ]
          }
]
```

Get Hits by Status Code & Platform

Retrieves the hit statistics for each status code returned for content delivered over our CDN. The data returned by this report can be filtered to only include CDN traffic that meets the following criteria:

- Platform

- Date range

Request

A request to retrieve hit statistics is described below. When submitting this request, you will need to define the following terms:

- **AccountNumber:** This term should be replaced by your CDN account number.

- **Platform:** This term should be replaced by an integer that indicates the platform for which a report will be generated. Valid values for this term are:

  - **0:** All Platforms

  - **2:** Flash Media Streaming

  - **3:** HTTP Large

  - **8:** HTTP Small

  - **14:** Application Delivery Network (ADN)

- **StartDateTime:** This term should be replaced by the start date/time for the report. Only activity that completed after the specified date/time will be included in the report. The format for this term is: *YYYY-MM-DD*T*hh*:*mm*:*ss*.

- **EndDateTime:** This term should be replaced by the end date/time for the report. Activity that completed after the specified date/time will be excluded from the report. The format for this term is: *YYYY-MM-DD*T*hh*:*mm*:*ss*.

Important: Specifying a time that falls in between a one hour time interval (e.g., 00:00:01) will retrieve all data associated with that time interval (e.g., 00:00:00 – 00:59:59).

Note: The time portion (i.e., *hh*:*mm*:*ss*) of the StartDateTime and EndDateTime request parameters is optional. If a specific time is not specified, then a default time (i.e., 00:00:00) will be used.

Note: For more information on date/time format, please refer to **Appendix B: Report Date/Time Format**.

HTTP Method	Request URI
GET	https://api.edgecast.com/v2/reporting/customers/*AccountNumber*/media/*Platform*/hits?begindate=*StartDateTime*&enddate=*EndDateTime*

Request Headers

This endpoint only takes advantage of the common request headers described in the **Request Headers** section of the **Request and Response Elements** topic.

Request Body

Request body parameters are not required by this endpoint.

Response

The response to the above request includes an HTTP status code, response headers, and a response body.

Status Code

A status code indicates whether the request was successfully performed. A list of common status codes is provided in the **Status Codes and Error Messages** topic.

Response Headers

The response for this endpoint only returns standard HTTP response headers including those described in the **Response Headers** section of the **Request and Response Elements** topic.

Response Body

The response body for a successful request contains the following response elements for each status code.

Name	Description
Description	A string that identifies a status code by its description (e.g., OK, Forbidden, Not Found, etc.)
HitPercentage	A number (floating-point) that indicates the percentage of requests that resulted in the specified status code over the given time period & platform.
Hits	An integer that indicates the number of requests that resulted in the specified status code over the given time period & platform.
StatusCode	An integer that identifies a status code (200, 403, 404, etc.).

Errors

The response body for an unsuccessful request may contain an error element that provides additional information. For a list of common error messages, please refer to the **Status Codes and Error Messages** topic.

Sample Request and Response

A sample JSON request is provided below.

```
GET
https://api.edgecast.com/v2/reporting/customers/0001/media/3/hits?begindate=2013-06-
01&enddate=2013-07-01 HTTP/1.1

Authorization: TOK:12345678-1234-1234-1234-1234567890ab

Accept: application/json

Host: api.edgecast.com
```

A sample JSON response is provided below.

```
HTTP/1.1 200 OK

Cache-Control: private

Content-Type: application/json; charset=utf-8

Date: Thu, 14 Apr 2016 12:00:00 GMT

Content-Length: 487


[{

          "Description" : "",

          "HitPercentage" : 57.96,

          "Hits" : 638045,

          "StatusCode" : 200

     }, {

          ...

     }, {

          "Description" : "",

          "HitPercentage" : 0,

          "Hits" : 2,

          "StatusCode" : 405

     }
]
```

Get Maximum Storage Usage

Returns the maximum amount of storage space used on a CDN origin server during the given time period.

Request

A request to retrieve maximum storage space usage is described below. When submitting this request, you will need to define the following terms:

- **AccountNumber:** This term should be replaced by your CDN account number.

- **StartDateTime:** This term should be replaced by the start date/time for the report. Only activity that took place after the specified date/time will be included in the report. The format for this term is: *YYYY-MM-DD*T*hh*:*mm*:*ss*.

- **EndDateTime:** This term should be replaced by the end date/time for the report. Activity that took place after the specified date/time will not be included in the report. The format for this term is: *YYYY-MM-DD*T*hh*:*mm*:*ss*.

Note: Keep in mind that time is optional. If time is not specified, then a default time (i.e., 00:00:00) will be used.

Note: For more information on date/time format, please refer to **Appendix B: Report Date/Time Format**.

HTTP Method	Request URI
GET	https://api.edgecast.com/v2/reporting/customers/*AccountNumber/*maxstorageusage?begindate=*StartDateTime*&enddate=*EndDateTime*

Request Headers

This endpoint only takes advantage of the common request headers described in the **Request Headers** section of the **Request and Response Elements** topic.

Request Body

Request body parameters are not required by this endpoint.

Response

The response to the above request includes an HTTP status code, response headers, and a response body.

Status Code

A status code indicates whether the request was successfully performed. A list of common status codes is provided in the **Status Codes and Error Messages** topic.

Response Headers

The response for this endpoint only returns standard HTTP response headers including those described in the **Response Headers** section of the **Request and Response Elements** topic.

Response Body

The response body for a successful request contains the following response element:

Name	Description
UsageResult	A number (floating-point) that indicates the highest level of disk space usage (GB) over the given time period.

Errors

The response body for an unsuccessful request may contain an error element that provides additional information. For a list of common error messages, please refer to the **Status Codes and Error Messages** topic.

Sample Request and Response

A sample JSON request is provided below.

```
GET
https://api.edgecast.com/v2/reporting/customers/0001/maxstorageusage?begindate=2011-
06-01&enddate=2011-07-01 HTTP/1.1

Authorization: TOK:12345678-1234-1234-1234-1234567890ab

Accept: application/json

Host: api.edgecast.com
```

A sample JSON response is provided below.

```
HTTP/1.1 200 OK

Cache-Control: private

Content-Type: application/json; charset=utf-8

Date: Thu, 14 Apr 2016 12:00:00 GMT

Content-Length: 20


{

        "UsageResult" : 85.5

}
```

Get Route Summary Query

Retrieves the total number of DNS queries over a given time period for either of the following:

- All primary and secondary zones

- A specific primary or secondary zone

Request

A request to retrieve DNS query summary information is described below. When submitting this request, you will need to define the following terms:

- **AccountNumber:** This term should be replaced by your CDN account number.

- **ZoneID:** Replace this variable with either of the following values:

    - **0:** Retrieves DNS queries for all zones.

    - **ID:** Replace this variable with the system-defined ID of the desired primary or secondary zone. Retrieve a list of all primary and secondary zones and their system-defined IDs through the Get All Zones endpoint.

- **ZoneName:** Replace this variable with the name of the desired zone.

- **StartDateTime:** Replace this variable with the start date/time for the report. Only activity that took place after the specified date/time will be included in the report. **Format:** *YYYY-MM-DD*T*hh*:*mm*:*ss*

- **EndDateTime:** Replace this variable with the end date/time for the report. Activity that took place after the specified date/time will not be included in the report. **Format:** *YYYY-MM-DD*T*hh*:*mm*:*ss*

Note: Time (i.e., T*hh*:*mm*:*ss*) is optional. If time is not specified, then a default time (i.e., 00:00:00) will be used.

HTTP Method	Request URI
GET	https://api.edgecast.com/v2/reporting/customers/*AccountNumber*/routesummary?zoneid=*ZoneID*&zonename=*ZoneName*&begindate=*StartDateTime*&enddate=*EndDateTime*

Tip: Omit the zoneid and zonename query string parameters to retrieve statistics for all primary and secondary zones.

Request Headers

This endpoint only takes advantage of the common request headers described in the **Request Headers** section of the **Request and Response Elements** topic.

Request Body

Request body parameters are not required by this endpoint.

Response

The response to the above request includes an HTTP status code, response headers, and a response body.

Status Code

A status code indicates whether the request was successfully performed. A list of common status codes is provided in the **Status Codes and Error Messages** topic.

Response Headers

The response for this endpoint only returns standard HTTP response headers including those described in the **Response Headers** section of the **Request and Response Elements** topic.

Response Body

The response body for a successful request contains the following response elements:

Name	Data Type	Description
Zone	String	Identifies a primary or secondary zone by its name.
Id	Integer	Identifies a primary or secondary zone by its system-defined ID.
QueryCount	String	Indicates the number of DNS queries that were received for the zone identified by the Zone response element.

Errors

The response body for an unsuccessful request may contain an error element that provides additional information. For a list of common error messages, please refer to the **Status Codes and Error Messages** topic.

Sample Request and Response

A sample JSON request is provided below.

```
GET
https://api.edgecast.com/v2/reporting/customers/0001/routesummary?begindate=2016-03-15&enddate=2016-03-17 HTTP/1.1

Authorization: TOK:12345678-1234-1234-1234-1234567890ab

Accept: application/json

Host: api.edgecast.com
```

A sample JSON response is provided below.

```
HTTP/1.1 200 OK
Cache-Control: private
Content-Type: application/json; charset=utf-8
Date: Thu, 14 Apr 2016 12:00:00 GMT
Content-Length: 161


[{
            "Zone" : "mydomain.net.",
            "Id" : 4528,
            "QueryCount" : "1234"
      }, {
            "Zone" : "myexample.com.",
            "Id" : 4566,
            "QueryCount" : "1235"
      }
]
```

Get Traffic Usage

Provides traffic usage statistics corresponding to the combination of a particular platform and billing region. The type of billing information returned by this endpoint, which can either be Data Transferred or Bandwidth Usage, is determined by the Units request parameter. Please choose the billing method that corresponds to the one specified in your contract.

Note: For the purposes of billing, report data is closed on the 3rd of the month. This means that report data for the current month is incomplete until after the third of the next month.

Bandwidth Usage

Bandwidth usage information for the specified platform and billing region over the specified month can be viewed by setting the Units request parameter to 1. This setting will cause this endpoint to report the amount of data (Megabits) transferred per second during peak usage. This information is useful for viewing whether 95% usage of the bandwidth specified in your contract has been exceeded.

Data Transferred

The total amount of data transferred (GB) for the specified platform and billing region over the specified month can be viewed by setting the Units request parameter to 2.

Request

A request to retrieve billing statistics is described below. When submitting this request, you will need to define the following terms:

- **AccountNumber:** This term should be replaced by your CDN account number.

- **Platform:** This term should be replaced by an integer that indicates the platform for which a report will be generated. Valid values for this term are:

    - **2:** Flash Media Streaming

    - **3:** HTTP Large

    - **7:** HTTP Large (SSL Traffic Only)

    - **8:** HTTP Small

    - **9:** HTTP Small (SSL Traffic Only)

    - **14:** Application Delivery Network (ADN)

    - **15:** Application Delivery Network (ADN) – (SSL Traffic Only)

- **Region:** This term should be replaced by an integer that indicates the billing region for which a report will be generated. Valid values for this term are defined by the Id return value of the Get Billing Regions endpoint.

- **Units:** This term should be replaced by an integer that determines whether the UsageResult response element will return bandwidth usage or data transferred statistics. Valid values for this term are:

    - **1:** Megabits per second (Mbps) – Bandwidth Usage

    - **2:** Gigabytes (GB) – Data Transferred

- **BillingMonth:** This term indicates the month for which billing information will be returned. When specifying this option, you must specify the 1st of the desired month (e.g., 2011-06-01). The format for this term is: *YYYY-MM-DD*.

Important: If you specify a date other than the 1st of the month, then the return value will not reflect the usage information for that month.

HTTP Method	Request URI
GET	https://api.edgecast.com/v2/reporting/customers/*AccountNumber*/media/*Platform*/region/*Region*/units/*Units*/trafficusage?begindate=*BillingMonth*

Request Headers

This endpoint only takes advantage of the common request headers described in the **Request Headers** section of the **Request and Response Elements** topic.

Request Body

Request body parameters are not required by this endpoint.

Response

The response to the above request includes an HTTP status code, response headers, and a response body.

Status Code

A status code indicates whether the request was successfully performed. A list of common status codes is provided in the **Status Codes and Error Messages** topic.

Response Headers

The response for this endpoint only returns standard HTTP response headers including those described in the **Response Headers** section of the **Request and Response Elements** topic.

Response Body

The response body for a successful request contains the following response element:

Name	Description
UsageResult	A number (floating-point) that indicates the total amount of bandwidth usage or data transferred for the specified billing region, platform, and month. The units for this return parameter are determined by the Units request parameter.

Errors

The response body for an unsuccessful request may contain an error element that provides additional information. For a list of common error messages, please refer to the **Status Codes and Error Messages** topic.

Sample Request and Response

A sample JSON request is provided below.

```
GET
https://api.edgecast.com/v2/reporting/customers/0001/media/3/region/0/units/1/traffi
cusage?begindate=2011-06-01 HTTP/1.1

Authorization: TOK:12345678-1234-1234-1234-1234567890ab

Accept: application/json

Host: api.edgecast.com
```

A sample JSON response is provided below.

```
HTTP/1.1 200 OK

Cache-Control: private

Content-Type: application/json; charset=utf-8

Date: Thu, 14 Apr 2016 12:00:00 GMT

Content-Length: 21


{

        "UsageResult" : 85.5

}
```

Custom Reports

The following endpoints support the Custom Report module to retrieve CDN activity statistics by edge CNAME:

Name	Description
Get Edge CNAME Report - Data Transferred or Hits	Retrieves total data transferred or total hits statistics for all custom report codes.
Get Data Transferred and Hits by Custom Report Codes	Retrieves CDN activity statistics for each custom report code.
Get Group Codes	Retrieves a list of the available group codes.
Get Metric Codes	Retrieves a list of the available metric codes.
Get Report Codes	Retrieves a list of custom report codes.

Note: These endpoints may only generate reports for CDN activity within the last 18 months.

Get Edge CNAME Report - Data Transferred or Hits

This endpoint retrieves total data transferred or total hits statistics for each edge CNAME for which custom reports has been activated. Additionally, these statistics will be broken down by either cache status code or HTTP status code.

Request

A request to retrieve a custom report is described below. When submitting this request, you will need to define the following terms:

- **AccountNumber:** This term should be replaced by your CDN account number.

- **Platform:** This term should be replaced by the ID associated with the desired platform. Valid values for this parameter are listed below.

    - **2:** Flash Media Streaming

    - **3:** HTTP Large

    - **8:** HTTP Small

    - **14:** Application Delivery Network (ADN)

- **StartDate:** This term should be replaced by the start date for the report. Only activity that took place after the specified date will be included in the report. The format for this term is: *YYYY-MM-DD*.

- **EndDate:** This term should be replaced by the end date for the report. Activity that took place after the specified date will not be included in the report. The format for this term is: *YYYY-MM-DD*.

- **MetricCode:** Replace this variable with the metric code that identifies the type of report to generate. By default, a "hits" report will be generated. Use the Get Metric Codes endpoint to retrieve a list of metric codes.

- **GroupCode:** Replace this variable with the group code that identifies the type of statistics that will be included in the report. By default, report statistics will be broken down by HTTP status codes. Use the Get Group Codes endpoint to retrieve a list of group codes.

Note: For more information on date/time format, please refer to **Appendix B: Report Date/Time Format**.

HTTP Method	Request URI
GET	https://api.edgecast.com/v2/reporting/customers/*AccountNumber*/media/*Platform*/customreport?begindate=*StartDate*&enddate=*EndDate*&metriccode=*MetricCode*&groupcode=*GroupCode*

Request Headers

This endpoint only takes advantage of the common request headers described in the **Request Headers** section of the **Request and Response Elements** topic.

Request Body

Request body parameters are not required by this endpoint.

Response

The response to the above request includes an HTTP status code, response headers, and a response body.

Status Code

A status code indicates whether the request was successfully performed. A list of common status codes is provided in the **Status Codes and Error Messages** topic.

Response Headers

The response for this endpoint only returns standard HTTP response headers including those described in the **Response Headers** section of the **Request and Response Elements** topic.

Response Body

The response body for a successful request contains the following response elements:

Name	Description
MetricCode	A string that identifies the type of report that was generated by its metric code.
Description	A string that describes the type of report that was generated.
Data	An array that describes the report.
GroupCode	A string that identifies the type of statistics included in the report by its metric code.
Description	A string that describes the type of statistics included in the report.
Data	An array that contains report data.
Description	A string that describes the report code (e.g., edge CNAME) for which report data is reported.
TotalCount	A string that indicates either of the following: • Total Hits • Total Data Transferred in Megabytes The value reported in this response element is determined by the metric code reported by the MetricCode response element.

Name	Description
Data	An array that contains statistics broken down by the category defined in the GroupCode response element.
KeyCode	A string that identifies the type of statistic being reported by its code.
Description	A string that describes the type of statistic being reported. **Note:** Please refer to the **Custom Reports Fields** section of the **EC360 Analytics Suite User Guide** for a description for each field.
Count	A string that indicates either of the following for the type of statistic defined by the KeyCode response element: • Hits • Data Transferred in Megabytes The value reported in this response element is determined by the metric code reported by the MetricCode response element.

Errors

The response body for an unsuccessful request may contain an error element that provides additional information. For a list of common error messages, please refer to the **Status Codes and Error Messages** topic.

Sample Request and Response

A sample JSON request is provided below.

```
GET
https://api.edgecast.com/v2/reporting/customers/0001/media/3/customreport?begindate=
2015-07-01&enddate=2015-07-29 HTTP/1.1

Authorization: TOK:12345678-1234-1234-1234-1234567890ab

Accept: application/json

Host: api.edgecast.com
```

A sample JSON response is provided below.

```
HTTP/1.1 200 OK

Cache-Control: private

Content-Type: application/json; charset=utf-8

Date: Thu, 14 Apr 2016 12:00:00 GMT

Content-Length: 1808

[{

            "MetricCode" : "Hits",
```

```
            "Description" : "Hits",
            "Data" : [{
                        "GroupCode" : "HTTP_STATUS",
                        "Description" : "HTTP Response Codes",
                        "Data" : [{
                                    "Description" : "cdn.mydomain.com",
                                    "TotalCount" : "9656108598",
                                    "Data" : [{
                                                "KeyCode" :
"HTTP_STATUS_2xx",

                                                "Description" : "2xx",
                                                "Count" : "1013588860"
                                        }, {
                                                "KeyCode" :
"HTTP_STATUS_3xx",

                                                "Description" : "3xx",
                                                "Count" : "32752"
                                        }, {
                                                "KeyCode" :
"HTTP_STATUS_4xx",

                                                "Description" : "4xx",
                                                "Count" : "23711"
                                        }, {
                                                "KeyCode" :
"HTTP_STATUS_5xx",

                                                "Description" : "5xx",
                                                "Count" : "541"
                                        }, {
                                                "KeyCode" :
"HTTP_STATUS_OTHER",

                                                "Description" : "Other",
                                                "Count" : "0"
                                        }, {
                                                "KeyCode" : "000",
                                                "Description" :
"Unassigned",

                                                "Count" : "8642462734"
                                    }
                                ]
                        }, {
```

```
                                                   "Description" : "stream.mydomain.com",
                                                   "TotalCount" : "13954422087.14",
                                                   "Data" : [{
                                                           "KeyCode" : "LOG_TCP_HIT",
                                                           "Description" : "Cache
        Hits",
                                                           "Count" : "740617948.87"
                                           }, {
                                                           "KeyCode" :
        "LOG_TCP_MISS",
                                                           "Description" : "Misses",
                                                           "Count" : "18364385.29"
                                           }, {
                                                           "KeyCode" :
        "LOG_CONFIG_NOCACHE",
                                                           "Description" : "No
        Cache",
                                                           "Count" : "0"
                                           }, {
                                                           "KeyCode" :
        "LOG_UNCACHEABLE",
                                                           "Description" :
        "Uncacheable",
                                                           "Count" : "0"
                                           }, {
                                                           "KeyCode" : "LOG_OTHER",
                                                           "Description" : "Other",
                                                           "Count" : "492443420.55"
                                           }, {
                                                           "KeyCode" : "000",
                                                           "Description" :
        "Unassigned",
                                                           "Count" : "12702996332.43"
                                           }
                                   ]
                           }
                   ]
           }
   ]
```

Get Data Transferred & Hits by Custom Report Codes

Retrieves the number of hits and the total amount of data transferred for each custom report code.

Note: A unique custom report code is associated with each edge CNAME for which the custom report capability has been enabled.

Request

A request to retrieve CDN activity for each custom report code is described below. When submitting this request, you will need to define the following terms:

- **AccountNumber:** This term should be replaced by your CDN account number.

- **Platform:** This term should be replaced by the ID associated with the desired platform. Valid values for this parameter are listed below.

  - **2:** Flash Media Streaming

  - **3:** HTTP Large

  - **8:** HTTP Small

  - **14:** Application Delivery Network (ADN)

- **StartDateTime:** This term should be replaced by the start date for the report. Only activity that took place after the specified date will be included in the report. The format for this term is: *YYYY-MM-DD*T*hh*:*mm*:*ss*.

- **EndDateTime:** This term should be replaced by the end date for the report. Activity that took place after the specified date will not be included in the report. The format for this term is: *YYYY-MM-DD*T*hh*:*mm*:*ss*.

Important: Returns data in 1 hour intervals (e.g., 00:00:00, 01:00:00, 02:00:00, etc.). Specifying a time that falls in between a 1 hour interval (e.g., 00:50:05) will include all data associated with that hour (e.g., 00:00:00 – 00:59:59).

Note: The time portion (i.e., *hh*:*mm*:*ss*) of the StartDateTime and EndDateTime request parameters is optional. If a specific time is not specified, then a default time (i.e., 00:00:00) will be used.

Note: For more information on date/time format, please refer to **Appendix B: Report Date/Time Format**.

HTTP Method	Request URI
GET	https://api.edgecast.com/v2/reporting/customers/*AccountNumber*/media/*Platform*/cnamereportcodes?begindate=*StartDateTime*&enddate=*EndDateTime*

Request Headers

This endpoint only takes advantage of the common request headers described in the **Request Headers** section of the **Request and Response Elements** topic.

Request Body

Request body parameters are not required by this endpoint.

Response

The response to the above request includes an HTTP status code, response headers, and a response body.

Status Code

A status code indicates whether the request was successfully performed. A list of common status codes is provided in the **Status Codes and Error Messages** topic.

Response Headers

The response for this endpoint only returns standard HTTP response headers including those described in the **Response Headers** section of the **Request and Response Elements** topic.

Response Body

The response body for a successful request contains the following response elements for each report code returned by this endpoint:

Name	Description
Bytes	An integer that indicates the total amount of data transferred (in bytes) for the specified report code.
	Keep in mind that this data is filtered by time period and platform.
Description	A string that provides a description for a report code. The provided information varies according to report code type.
	For example, if an edge CNAME has been associated with a report code, then this response element will report the name of that edge CNAME.
Hits	An integer that indicates the total number of hits that occurred for the specified report code.
	Keep in mind that this data is filtered by time period and platform.
ReportCode	An integer that identifies a report code by its system-defined ID.

Errors

The response body for an unsuccessful request may contain an error element that provides additional information. For a list of common error messages, please refer to the **Status Codes and Error Messages** topic.

Sample Request and Response

A sample JSON request is provided below.

```
GET
https://api.edgecast.com/v2/reporting/customers/0001/media/3/cnamereportcodes?begind
ate=2012-11-01&enddate=2012-11-15 HTTP/1.1

Authorization: TOK:12345678-1234-1234-1234-1234567890ab

Accept: application/json

Host: api.edgecast.com
```

A sample JSON response is provided below.

```
HTTP/1.1 200 OK

Cache-Control: private

Content-Type: application/json; charset=utf-8

Date: Thu, 14 Apr 2016 12:00:00 GMT

Content-Length: 248

[{

            "Bytes" : 55515129610593,

            "Description" : "www.edgecname1.com",

            "Hits" : 21873348,

            "ReportCode" : 10042

      }, {

            "Bytes" : 45792193956438,

            "Description" : "www.edgecname2.com",

            "Hits" : 34243537,

            "ReportCode" : 10044

      }
]
```

Get Group Codes

This endpoint retrieves a list of the available group codes. Group codes define the type of statistics that will be returned by the Get Edge CNAME Report - Data Transferred or Hits endpoint.

Request

A request to retrieve group codes is described below.

HTTP Method	Request URI
GET	https://api.edgecast.com/v2/reporting/customreport/groupcodetypes

Request Headers

This endpoint only takes advantage of the common request headers described in the **Request Headers** section of the **Request and Response Elements** topic.

Request Body

Request body parameters are not required by this endpoint.

Response

The response to the above request includes an HTTP status code, response headers, and a response body.

Status Code

A status code indicates whether the request was successfully performed. A list of common status codes is provided in the **Status Codes and Error Messages** topic.

Response Headers

The response for this endpoint only returns standard HTTP response headers including those described in the **Response Headers** section of the **Request and Response Elements** topic.

Response Body

The response body for a successful request contains the following response elements for each group code returned by this endpoint.

Name	Description
GroupCode	A string that identifies a type of statistic by its group code. Use this code when generating a report via the Get Edge CNAME Report - Data Transferred or Hits endpoint.
Description	A string that provides a description for the current group code.

The response body for an unsuccessful request may contain an error element that provides additional information. For a list of common error messages, please refer to the **Status Codes and Error Messages** topic.

Sample Request and Response

A sample JSON request is provided below.

```
GET https://api.edgecast.com/v2/reporting/customreport/groupcodetypes HTTP/1.1

Authorization: TOK:12345678-1234-1234-1234-1234567890ab

Accept: application/json

Host: api.edgecast.com
```

A sample JSON response is provided below.

```
HTTP/1.1 200 OK

Cache-Control: private

Content-Type: application/json; charset=utf-8

Date: Thu, 14 Apr 2016 12:00:00 GMT

Content-Length: 151


[{

            "GroupCode" : "HTTP_STATUS",

            "Description" : "HTTP Response Codes"

     }, {

            "GroupCode" : "LOG_TCP",

            "Description" : "Cache Status"

     }
]
```

Get Metric Codes

This endpoint retrieves a list of the available metric codes. Metric codes define the type of report that will be returned by the Get Edge CNAME Report - Data Transferred or Hits endpoint.

Request

A request to retrieve metric codes is described below.

HTTP Method	Request URI
GET	https://api.edgecast.com/v2/reporting/customreport/metriccodetypes

Request Headers

This endpoint only takes advantage of the common request headers described in the **Request Headers** section of the **Request and Response Elements** topic.

Request Body

Request body parameters are not required by this endpoint.

Response

The response to the above request includes an HTTP status code, response headers, and a response body.

Status Code

A status code indicates whether the request was successfully performed. A list of common status codes is provided in the **Status Codes and Error Messages** topic.

Response Headers

The response for this endpoint only returns standard HTTP response headers including those described in the **Response Headers** section of the **Request and Response Elements** topic.

Response Body

The response body for a successful request contains the following response elements for each metric code returned by this endpoint.

Name	Description
MetricCode	A string that identifies a type of report by its metric code. Use this code when generating a report via the Get Edge CNAME Report - Data Transferred or Hits endpoint.
Description	A string that provides a description for the current metric code.

The response body for an unsuccessful request may contain an error element that provides additional information. For a list of common error messages, please refer to the **Status Codes and Error Messages** topic.

Sample Request and Response

A sample JSON request is provided below.

```
GET https://api.edgecast.com/v2/reporting/customreport/metriccodetypes HTTP/1.1
Authorization: TOK:12345678-1234-1234-1234-1234567890ab
Accept: application/json
Host: api.edgecast.com
```

A sample JSON response is provided below.

```
HTTP/1.1 200 OK
Cache-Control: private
Content-Type: application/json; charset=utf-8
Date: Thu, 14 Apr 2016 12:00:00 GMT
Content-Length: 130

[{
            "MetricCode" : "Hits",
            "Description" : "Hits"
      }, {
            "MetricCode" : "DT",
            "Description" : "Data Transferred"
      }
]
```

Get Report Codes

Retrieves a listing of report codes. This list can be filtered by platform.

Request

Two variations of this request are provided below. The first request retrieves a listing of all report codes, while the second request only retrieves report codes associated with the specified platform. When submitting this request, you will need to define the following terms:

- **AccountNumber:** This term should be replaced by your customer's CDN account number.

- **Platform:** Optional. This term should be replaced by an integer that indicates the platform for which a report will be generated. If the mediatypeid parameter is not specified, then report data for all platforms will be returned. Valid values for this term are:

  - **2:** Flash Media Streaming

  - **3:** HTTP Large

  - **7:** HTTP Large (SSL Traffic Only)

  - **8:** HTTP Small

  - **9:** HTTP Small (SSL Traffic Only)

  - **14:** Application Delivery Network (ADN)

  - **15:** Application Delivery Network (ADN) – (SSL Traffic Only)

HTTP Method	Request URI
GET	https://api.edgecast.com/v2/reporting/customers/*AccountNumber*/reportcodes
GET	https://api.edgecast.com/v2/reporting/customers/*AccountNumber*/reportcodes?mediatypeid=*Platform*

Request Headers

This endpoint only takes advantage of the common request headers described in the **Request Headers** section of the **Request and Response Elements** topic.

Request Body

Request body parameters are not required by this endpoint.

Response

The response to the above request includes an HTTP status code, response headers, and a response body.

Status Code

A status code indicates whether the request was successfully performed. A list of common status codes is provided in the **Status Codes and Error Messages** topic.

Response Headers

The response for this endpoint only returns standard HTTP response headers including those described in the **Response Headers** section of the **Request and Response Elements** topic.

Response Body

The response body for a successful request contains the following response elements for each report code returned by this endpoint.

Name	Description
Description	A string that describes a report code.
	Note: If the report code is for an edge CNAME, then this response element will identify the corresponding domain.
MediaTypeid	An integer that identifies the platform corresponding to that report code. Valid values are:
	• **2:** Flash Media Streaming
	• **3:** HTTP Large
	• **7:** HTTP Large (SSL Traffic Only)
	• **8:** HTTP Small
	• **9:** HTTP Small (SSL Traffic Only)
	• **14:** Application Delivery Network (ADN)
	• **15:** Application Delivery Network (ADN) – (SSL Traffic Only)
ReportCode	An integer that identifies a report code.

Errors

The response body for an unsuccessful request may contain an error element that provides additional information. For a list of common error messages, please refer to the **Status Codes and Error Messages** topic.

Sample Request and Response

A sample JSON request is provided below.

```
GET https://api.edgecast.com/v2/reporting/customers/0001/reportcodes HTTP/1.1

Authorization: TOK:12345678-1234-1234-1234-1234567890ab

Accept: application/json

Host: api.edgecast.com
```

A sample JSON response is provided below.

```
HTTP/1.1 200 OK

Cache-Control: private

Content-Type: application/json; charset=utf-8

Date: Thu, 14 Apr 2016 12:00:00 GMT

Content-Length: 195


[{

            "Description" : "secure.mydomain.com",

            "MediaTypeid" : 3,

            "ReportCode" : 10000

    }, {

            "Description" : "marketing.mydomain.com",

            "MediaTypeid" : 3,

            "ReportCode" : 10001

    }
]
```

Real-Time Statistics Module

Note: Most endpoints for the Real-Time Statistics module can be found in the realtimestats service.

The reporting service contains the Get Current Edge CNAME Statistics endpoint that reports the most recent statistics on a per edge CNAME basis.

Get Current Edge CNAME Statistics

Reports summarized and POP-specific real-time statistics for:

- All traffic delivered over a specific platform.

- Platform-specific traffic for each edge CNAME that meets the following requirements:

    - The edge CNAME's **Custom Reports** option is set to "Enabled."

    - Traffic is being served through the edge CNAME.

Note: The response for this endpoint may be filtered to only return statistics for a single edge CNAME.

Should I use Get Current Edge CNAME Statistics or Get Current Edge CNAME Statistics II?

The main difference in functionality between these two endpoints is that the Get Current Edge CNAME Statistics II endpoint returns the timestamp at which real-time statistics were retrieved.

Note: Another difference between these two endpoints is the manner in which the response is organized. However, this difference does not affect the provided feature set.

Request

A request to retrieve real-time statistics broken down by edge CNAME is described below. When submitting this request, you will need to define the following terms:

- **AccountNumber:** This term should be replaced by your CDN account number.

- **Platform:** This term should be replaced by the ID associated with the desired platform. Valid values for this parameter are listed below.

    - **cache:** HTTP Large

    - **wac:** HTTP Small

    - **adn:** Application Delivery Network

- **EdgeCNAME:** Replace this variable with the desired edge CNAME.

    Note: Including the cname query string parameter when requesting this endpoint will filter the response to only display statistics for the specified edge CNAME.

HTTP Method	Request URI
GET	https://api.edgecast.com/v2/reporting/customers/*AccountNumber*/rts /*Platform*?cname=*EdgeCNAME*

Request Headers

This endpoint only takes advantage of the common request headers described in the **Request Headers** section of the **Request and Response Elements** topic.

Request Body

Request body parameters are not required by this endpoint.

Response

The response to the above request includes an HTTP status code, response headers, and a response body.

Status Code

A status code indicates whether the request was successfully performed. A list of common status codes is provided in the **Status Codes and Error Messages** topic.

Response Headers

The response for this endpoint only returns standard HTTP response headers including those described in the **Response Headers** section of the **Request and Response Elements** topic.

Response Body

The response body for a successful request contains response elements that report statistics for:

- All POPs (i.e., total).

- Each POP location.

Note: POP locations that are not serving traffic for the relevant edge CNAMEs will be omitted from the response.

Name	Data Type	Description
POPCode	String	Indicates the scope for the statistics reported by the RTStats response element. Valid values are: • **Blank:** A blank value indicates that the reported real-time statistics are for the entire network. • **POP:** If this response element is set to a three-letter POP code, then real-time statistics are only being reported for that POP location.

Name	Data Type	Description
RTStats	Array	This response element contains real-time statistics for each qualifying edge CNAME. The scope for these statistics is determined by the POPCode response element.
CName	String	Determines the scope for which real-time statistics will be reported. Valid values are: • *EdgeCNAME:* This term identifies an edge CNAME by its name. Indicates that the current object reports real-time statistics for this edge CNAME. • **Total:** Indicates the current object reports real-time statistics for all traffic being delivered over the specified platform. **Note:** Total traffic will not be reported when requesting real-time statistics for a specific edge CNAME using the **cname** query string parameter.
BW	Number (floating-point)	Indicates bandwidth, in bytes per second, for the scope defined in the CName response parameter.
CONN	Number (floating-point)	Indicates the number of new connections per second for the scope defined in the CName response parameter.
HITS	Number (floating-point)	Indicates the number of hits per second for the scope defined in the CName response parameter.
cache.cfg-nocache	Number (floating-point)	Indicates the number of requests per second that resulted in a CONFIG_NOCACHE for the scope defined in the CName response parameter.
cache.cli-refresh-miss	Number (floating-point)	Indicates the number of requests per second that resulted in a TCP_CLIENT_REFRESH_MISS for the scope defined in the CName response parameter.
cache.hit	Number (floating-point)	Indicates the number of requests per second that resulted in a TCP_HIT for the scope defined in the CName response parameter.

Name	Data Type	Description
cache.miss	Number (floating-point)	Indicates the number of requests per second that resulted in a TCP_MISS for the scope defined in the CName response parameter.
cache.none	Number (floating-point)	Indicates the number of requests per second that resulted in a NONE for the scope defined in the CName response parameter.
cache.not-cacheable	Number (floating-point)	Indicates the number of requests per second that resulted in an UNCACHEABLE for the scope defined in the CName response parameter.
cache.xphit	Number (floating-point)	Indicates the number of requests per second that resulted in a TCP_EXPIRED_HIT for the scope defined in the CName response parameter.
cache.xpmiss	Number (floating-point)	Indicates the number of requests per second that resulted in a TCP_EXPIRED_MISS for the scope defined in the CName response parameter.
http.2xx	Number (floating-point)	Indicates the number of requests per second that resulted in a 2xx status code (e.g., 200, 201, 202, etc.) for the scope defined in the CName response parameter.
http.304	Number (floating-point)	Indicates the number of requests per second that resulted in a 304 Not Modified status code for the scope defined in the CName response parameter.
http.3xx	Number (floating-point)	Indicates the number of requests per second that resulted in a 3xx status code (e.g., 300, 301, 302, etc.) for the scope defined in the CName response parameter.
http.403	Number (floating-point)	Indicates the number of requests per second that resulted in a 403 Forbidden status code for the scope defined in the CName response parameter.
http.404	Number (floating-point)	Indicates the number of requests per second that resulted in a 404 Not Found status code for the scope defined in the CName response parameter.
http.4xx	Number (floating-point)	Indicates the number of requests per second that resulted in a 4xx status code (e.g., 400, 401, 402, 405, etc.) for the scope defined in the CName response parameter.

Name	Data Type	Description
http.5xx	Number (floating-point)	Indicates the number of requests per second that resulted in a 5xx status code (e.g., 500, 501, 502, etc.) for the scope defined in the CName response parameter.
http.other	Number (floating-point)	Indicates the number of requests per second that resulted in a status code that is not listed above for the scope defined in the CName response parameter.

Errors

The response body for an unsuccessful request may contain an error element that provides additional information. For a list of common error messages, please refer to the **Status Codes and Error Messages** topic.

Sample Request and Response

A sample JSON request is provided below.

```
GET
https://api.edgecast.com/v2/reporting/customers/0001/rts/cache?cname=cdn.mydomain.com HTTP/1.1

Authorization: TOK:12345678-1234-1234-1234-1234567890ab

Accept: application/json

Host: api.edgecast.com
```

A sample JSON response is provided below.

```
HTTP/1.1 200 OK

Cache-Control: private

Content-Type: application/json; charset=utf-8

Date: Thu, 14 Apr 2016 12:00:00 GMT

Content-Length: 20123
```

```
[{
            "POPCode" : "",
            "RTStats" : [{
                            "CName" : "cdn.mydomain.com",
                            "BW" : 12879605976.397789,
                            "CONN" : 90804.333916,
                            ...
                            "http.4xx" : 4.366612,
                            "http.5xx" : 5.549692
                    }
            ]
    }, {
            ...
    }, {
    "POPCode" : "waw",
            "RTStats" : [{
                            "CName" : "cdn.mydomain.com",
                            "BW" : 24186522.053812,
                            "CONN" : 125.717036,
                            "HITS" : 95.450761,
                            "cache.hit" : 77.283582,
                            "cache.miss" : 12.317016,
                            "cache.xphit" : 0.533319,
                            "http.2xx" : 95.334094,
                            "http.304" : 0.116667
                    }
            ]
    }
]
```

Get Current Edge CNAME Statistics II

Reports summarized and POP-specific real-time statistics for:

- All traffic delivered over a specific platform.

- Platform-specific traffic for each edge CNAME that meets the following requirements:

    - The edge CNAME's **Custom Reports** option is set to "Enabled."

    - Traffic is being served through the edge CNAME.

Note: The response for this endpoint may be filtered to only return statistics for a single edge CNAME.

Should I use Get Current Edge CNAME Statistics or Get Current Edge CNAME Statistics II?
The main difference in functionality between these two endpoints is that the Get Current Edge CNAME Statistics II endpoint returns the timestamp at which real-time statistics were retrieved.

Note: Another difference between these two endpoints is the manner in which the response is organized. However, this difference does not affect the provided feature set.

Request

A request to retrieve real-time statistics broken down by edge CNAME is described below. When submitting this request, you will need to define the following terms:

- **AccountNumber:** This term should be replaced by your CDN account number.

- **Platform:** This term should be replaced by the ID associated with the desired platform. Valid values for this parameter are listed below.

    - **cache:** HTTP Large

    - **wac:** HTTP Small

    - **adn:** Application Delivery Network

- **EdgeCNAME:** Replace this variable with the desired edge CNAME.

    Note: Including the cname query string parameter when requesting this endpoint will filter the response to only display statistics for the specified edge CNAME.

HTTP Method	Request URI
GET	https://api.edgecast.com/v2/reporting/customers/*AccountNumber* /realtimestats/*Platform*?cname=*EdgeCNAME*

Request Headers
This endpoint only takes advantage of the common request headers described in the **Request Headers** section of the **Request and Response Elements** topic.

Request Body

Request body parameters are not required by this endpoint.

Response

The response to the above request includes an HTTP status code, response headers, and a response body.

Status Code

A status code indicates whether the request was successfully performed. A list of common status codes is provided in the **Status Codes and Error Messages** topic.

Response Headers

The response for this endpoint only returns standard HTTP response headers including those described in the **Response Headers** section of the **Request and Response Elements** topic.

Response Body

The response body for a successful request contains response elements that report statistics for:

- All POPs (i.e., total).

- Each POP location.

Note: POP locations that are not serving traffic for the relevant edge CNAMEs will be omitted from the response.

Name	Data Type	Description
Timestamp	String	Identifies the date and time for which real-time statistics was reported. **Format:** *MM\/DD\/YYYY hh*:*mm*:*ss* **Note:** Time is indicated using 24-hour clock notation in UTC/GMT.
POPs	Array	Contains real-time statistics for each eligible edge CNAME.

Name	Data Type	Description
POPCode	String	Indicates the scope for the statistics reported by the RTStats response element. Valid values are: • **Blank:** A blank value indicates that the reported real-time statistics are for the entire network. • **POP:** If this response element is set to a three-letter POP code, then real-time statistics are only being reported for that POP location.
RTStats	Array	This response element contains real-time statistics for each qualifying edge CNAME. The scope for these statistics is determined by the POPCode response element.
CName	String	Determines the scope for which real-time statistics will be reported. Valid values are: • *EdgeCNAME*: This term identifies an edge CNAME by its name. Indicates that the current object reports real-time statistics for this edge CNAME. • **Total:** Indicates the current object reports real-time statistics for all traffic being delivered over the specified platform. **Note:** Total traffic will not be reported when requesting real-time statistics for a specific edge CNAME using the **cname** query string parameter.
BW	Number (floating-point)	Indicates bandwidth, in bytes per second, for the scope defined in the CName response parameter.
CONN	Number (floating-point)	Indicates the number of new connections per second for the scope defined in the CName response parameter.
HITS	Number (floating-point)	Indicates the number of hits per second for the scope defined in the CName response parameter.

Name	Data Type	Description
cache.cfg-nocache	Number (floating-point)	Indicates the number of requests per second that resulted in a CONFIG_NOCACHE for the scope defined in the CName response parameter.
cache.cli-refresh-miss	Number (floating-point)	Indicates the number of requests per second that resulted in a TCP_CLIENT_REFRESH_MISS for the scope defined in the CName response parameter.
cache.hit	Number (floating-point)	Indicates the number of requests per second that resulted in a TCP_HIT for the scope defined in the CName response parameter.
cache.miss	Number (floating-point)	Indicates the number of requests per second that resulted in a TCP_MISS for the scope defined in the CName response parameter.
cache.none	Number (floating-point)	Indicates the number of requests per second that resulted in a NONE for the scope defined in the CName response parameter.
cache.not-cacheable	Number (floating-point)	Indicates the number of requests per second that resulted in a UNCACHEABLE for the scope defined in the CName response parameter.
cache.xphit	Number (floating-point)	Indicates the number of requests per second that resulted in a TCP_EXPIRED_HIT for the scope defined in the CName response parameter.
cache.xpmiss	Number (floating-point)	Indicates the number of requests per second that resulted in a TCP_EXPIRED_MISS for the scope defined in the CName response parameter.
http.2xx	Number (floating-point)	Indicates the number of requests per second that resulted in a 2xx status code (e.g., 200, 201, 202, etc.) for the scope defined in the CName response parameter.
http.304	Number (floating-point)	Indicates the number of requests per second that resulted in a 304 Not Modified status code for the scope defined in the CName response parameter.
http.3xx	Number (floating-point)	Indicates the number of requests per second that resulted in a 3xx status code (e.g., 300, 301, 302, etc.) for the scope defined in the CName response parameter.

Name	Data Type	Description
http.403	Number (floating-point)	Indicates the number of requests per second that resulted in a 403 Forbidden status code for the scope defined in the CName response parameter.
http.404	Number (floating-point)	Indicates the number of requests per second that resulted in a 404 Not Found status code for the scope defined in the CName response parameter.
http.4xx	Number (floating-point)	Indicates the number of requests per second that resulted in a 4xx status code (e.g., 400, 401, 402, 405, etc.) for the scope defined in the CName response parameter.
http.5xx	Number (floating-point)	Indicates the number of requests per second that resulted in a 5xx status code (e.g., 500, 501, 502, etc.) for the scope defined in the CName response parameter.
http.other	Number (floating-point)	Indicates the number of requests per second that resulted in a status code that is not listed above for the scope defined in the CName response parameter.

Errors

The response body for an unsuccessful request may contain an error element that provides additional information. For a list of common error messages, please refer to the **Status Codes and Error Messages** topic.

Sample Request and Response

A sample JSON request is provided below.

```
GET
https://api.edgecast.com/v2/reporting/customers/0001/realtimestats/cache?cdn.mydomain.com HTTP/1.1

Authorization: TOK:12345678-1234-1234-1234-1234567890ab

Accept: application/json

Host: api.edgecast.com
```

A sample JSON response is provided below.

```
HTTP/1.1 200 OK

Cache-Control: private

Content-Type: application/json; charset=utf-8

Date: Thu, 14 Apr 2016 12:00:00 GMT

Content-Length: 19180
```

```json
{
        "Timestamp" : "06\/30\/2016 17:43:02",
        "POPs" : [{
                        "POPCode" : "",
                        "RTStats" : [{
                                        "CName" : "cdn.mydomain.com",
                                        "BW" : 731309317.738477,
                                        "CONN" : 1077.077293,
                                        "HITS" : 792.478335,
                                        "cache.hit" : 737.097289,
                                        ...
                                        "http.5xx" : 0.017777
                                }
                        ]
                }, {
                        ...
                }, {
                        "POPCode" : "waw",
                        "RTStats" : [{
                                        "CName" : "cdn.mydomain.com",
                                        "BW" : 1444547.183443,
                                        "CONN" : 3.183333,
                                        "HITS" : 2.017777,
                                        "cache.hit" : 1.533333,
                                        "cache.miss" : 0.233333,
                                        "cache.xphit" : 0.017777,
                                        "http.2xx" : 1.477777,
                                        "http.304" : 0.55
                                }
                        ]
                }
        ]
}
```

Get Real-Time Statistics by Country and Edge CNAME

Reports the following real-time statistics for traffic delivered over the specified platform:

- Total real-time statistics

- Total real-time statistics for each edge CNAME

- Total real-time statistics for each country

- Country-specific real-time statistics broken down by edge CNAME

Note: As indicated above, real-time statistics may be reported on a per edge CNAME basis. This type of data is only reported for edge CNAME configurations where the **Custom Reports** option has been enabled.

Request

A request to retrieve real-time statistics is described below. When submitting this request, you will need to define the following terms:

- **AccountNumber:** This term should be replaced by your CDN account number.

- **Platform:** This term should be replaced by the ID associated with the desired platform. Valid values for this parameter are listed below.

  - **cache:** HTTP Large

  - **wac:** HTTP Small

  - **adn:** Application Delivery Network

- **EdgeCNAME:** Replace this variable with the case-sensitive name of the desired edge CNAME.

- **CountryCode:** Replace this variable with the ISO 3166 code corresponding to the country for which real-time statistics will be returned.

  Tip: A list of country codes is available from the Country Codes (ISO 3166) article in the CDN Help Center.

HTTP Method	Request URI
GET	https://api.edgecast.com/v2/reporting/customers/*AccountNumber*/country realtimestats/*Platform*?cname=*EdgeCNAME*&country=*CountryCode*

Request Headers

This endpoint only takes advantage of the common request headers described in the **Request Headers** section of the **Request and Response Elements** topic.

Request Body

Request body parameters are not required by this endpoint.

Response

The response to the above request includes an HTTP status code, response headers, and a response body.

Status Code

A status code indicates whether the request was successfully performed. A list of common status codes is provided in the **Status Codes and Error Messages** topic.

Response Headers

The response for this endpoint only returns standard HTTP response headers including those described in the **Response Headers** section of the **Request and Response Elements** topic.

Response Body

The response body for a successful request that does not filter data contains response parameters that report statistics for:

- Total real-time statistics
- Total real-time statistics for each edge CNAME
- Total real-time statistics for each country
- Country-specific real-time statistics broken down by edge CNAME

Note: Countries or edge CNAMEs through which traffic is not being served will be omitted from the response.

Name	Data Type	Description
Timestamp	String	Identifies the date and time for which real-time statistics was reported. **Format:** *MM\/DD\/YYYY hh:mm:ss* **Note:** Time is indicated using 24-hour clock notation in UTC/GMT. **Note:** For more information on date/time format, please refer to **Appendix B: Report Date/Time Format**.
Countries	Array	Contains real-time statistics for each country through which traffic was served.

Name	Data Type	Description
CountryCode	String	Indicates the scope for the RTStats array. Valid values are: • **Blank:** A blank value indicates that the reported real-time statistics are for the entire network. • **POP:** If this response parameter is set to a two-letter country code, then real-time statistics are only being reported for that country location.
Country	String	Indicates the scope for the RTStats array. Valid values are: • **Blank:** A blank value indicates that the reported real-time statistics are for the entire network. • **POP:** If this response parameter is set to the name of a country, then real-time statistics are only being reported for that location.
RTStats	Array	This response parameter contains summarized and country-specific real-time statistics for each qualifying edge CNAME. The scope for these statistics is determined by the Country response parameter.
ReportCode	String	Determines the scope for which real-time statistics will be reported. Valid values are: • **ReportCode:** This term identifies an edge CNAME by its report code. Indicates that the current object reports real-time statistics for this edge CNAME. • **Total:** Indicates the current object reports real-time statistics for all traffic being delivered over the specified platform. **Note:** Total traffic will not be reported when requesting real-time statistics for a specific edge CNAME using the cname query string parameter.

Name	Data Type	Description
CName	String	Determines the scope for which real-time statistics will be reported. Valid values are: • **EdgeCNAME:** This term identifies an edge CNAME by its name. Indicates that the current object reports real-time statistics for this edge CNAME. • **Total:** Indicates the current object reports real-time statistics for all traffic being delivered over the specified platform. **Note:** Total traffic will not be reported when requesting real-time statistics for a specific edge CNAME using the cname query string parameter.
BW	Number floating-point	Indicates bandwidth, in bytes per second, for the scope defined by the Country and CName response parameters.
CONN	Number floating-point	Indicates the number of new connections per second for the scope defined by the Country and CName response parameters.
HITS	Number floating-point	Indicates the number of hits per second for the scope defined by the Country and CName response parameters.
CacheStats	Array	This response parameter contains real-time statistics for cache status codes.

Name	Data Type	Description
Key	String	Identifies a cache status code for which real-time statistics will be reported. Valid values are: • cache.cfg-nocache • cache.cli-refresh-miss • cache.hit • cache.miss • cache.none • cache.not-cacheable • cache.xphit • cache.xpmiss [Learn more about cache status codes.](#)
Value	Number floating-point	Indicates the number of requests per second that resulted in the cache status code identified by the Key response parameter for the scope defined by the Country and CName response parameters.
HttpStatuses	Array	This response parameter contains real-time statistics for HTTP status codes.
Key	String	Identifies a HTTP status code for which real-time statistics will be reported. Valid values are: • **http.2xx:** 2xx status code (e.g., 200, 201, 202, etc.) • **http.304:** 304 Not Modified status code • **http.3xx:** 3xx status code (e.g., 300, 301, 302, etc.) • **http.403:** 403 Forbidden status code • **http.404:** 404 Not Found status code • **http.4xx:** 4xx status code (e.g., 400, 401, 402, 405, etc.) • **http.5xx:** 5xx status code (e.g., 500, 501, 502, etc.) • **http.other:** Identifies a status code that is not listed above.

Name	Data Type	Description
Value	Number floating-point	Indicates the number of requests per second that resulted in the HTTP status code identified by the Key response parameter for the scope defined by the Country and CName response parameters.

Errors

The response body for an unsuccessful request may contain an error element that provides additional information. For a list of common error messages, please refer to the **Status Codes and Error Messages** topic.

Sample Request and Response

A sample JSON request is provided below.

```
GET
https://api.edgecast.com/v2/reporting/customers/0001/countryrealtimestats/and?cname=
cdn.example.com&country=us om HTTP/1.1

Authorization: TOK:12345678-1234-1234-1234-1234567890ab

Accept: application/json

Host: api.edgecast.com
```

A sample JSON response is provided below.

```
HTTP/1.1 200 OK

Cache-Control: private

Content-Type: application/json; charset=utf-8

Date: Thu, 14 Apr 2016 12:00:00 GMT

Content-Length: 942

{
        "Timestamp": "01\/18\/2018 22:00:29",

        "Countries": [{

                    "CountryCode": "US",

                    "Country": "United States",

                    "RTStats": [{

                                "ReportCode": "10012",

                                "CName": "cdn.example.com",

                                "BW": 57137424356.900772,

                                "CONN": 6256.201794999999,

                                "HITS": 103441.41254399999,

                                "CacheStats": [{

                                            "Key": "cache.hit",
```

```
                                        "Value": 103055.56026999999
                                }, {
                                        "Key": "cache.miss",
                                        "Value": 4.2333339999999993
                                }, {
                                        "Key": "cache.none",
                                        "Value": 329.719241
                                }, {
                                        "Key": "cache.xphit",
                                        "Value": 0.650001
                                }, {
                                        "Key": "cache.xpmiss",
                                        "Value": 0.016667
                                }
                        ],
                        "HttpStatuses": [{
                                        "Key": "http.2xx",
                                        "Value": 103306.54617099995
                                }, {
                                        "Key": "http.403",
                                        "Value": 134.166676
                                }, {
                                        "Key": "http.304",
                                        "Value": 0.7
                                }
                        ]
                }
        ]
    }
  ]
}
```

Advanced Content Analytics

This section describes the endpoints that leverage the Advanced Content Analytics module to retrieve data about activity on your CDN account. The Advanced Content Analytics module must be purchased separately. These endpoints will only be available on accounts on which this feature has been enabled.

Note: Advanced Content Analytics endpoints can only generate reports for CDN activity within the last 90 days.

Get Asset Activity

Retrieves statistics for the top 250 requested assets over a specific time period.

Request

A request to retrieve statistics for the top 250 requested assets is described below. When submitting this request, you will need to define the following terms:

- **AccountNumber:** This term should be replaced by your CDN account number.

- **Platform:** This term should be replaced by the ID associated with the desired platform. Valid values for this parameter are listed below.

    - **2:** Flash Media Streaming

    - **3:** HTTP Large

    - **14:** Application Delivery Network (ADN)

- **StartDateTime:** This term should be replaced by the start date for the report. Only activity that took place after the specified date will be included in the report. The format for this term is: *YYYY-MM-DD*T*hh*:*mm*:*ss*.

- **EndDateTime:** This term should be replaced by the end date for the report. Activity that took place after the specified date will not be included in the report. The format for this term is: *YYYY-MM-DD*T*hh*:*mm*:*ss*.

Important: Returns data in 1 day intervals. This means that this report will return data for the specified time period including the specified start and end date. This will occur regardless of whether a time value was specified. This means that time is optional and irrelevant for this endpoint.

Note: For more information on date/time format, please refer to **Appendix B: Report Date/Time Format**.

HTTP Method	Request URI
GET	https://api.edgecast.com/v2/reporting/customers/*AccountNumber*/media /*Platform*/filestats?begindate=*StartDateTime*&enddate=*EndDateTime*

Request Headers

This endpoint only takes advantage of the common request headers described in the **Request Headers** section of the **Request and Response Elements** topic.

Request Body

Request body parameters are not required by this endpoint.

Response

The response to the above request includes an HTTP status code, response headers, and a response body.

Status Code

A status code indicates whether the request was successfully performed. A list of common status codes is provided in the **Status Codes and Error Messages** topic.

Response Headers

The response for this endpoint only returns standard HTTP response headers including those described in the **Response Headers** section of the **Request and Response Elements** topic.

Response Body

The response body for a successful request contains the following response elements for each asset returned by this endpoint:

Name	Description
DataTransferred	An integer that indicates the total amount of data transferred (in bytes) for the specified asset over the specified time period.
DataTransferredPercentage	A number (floating-point) value that indicates the data transferred percentage for the specified asset. Keep in mind that this percentage is calculated from the total amount of data transferred for all assets included in this report over the specified time period.
Duration	A number (floating-point) value that indicates the average amount of time, in seconds, that it took our CDN to serve an asset to a client.
Hits	An integer that indicates the total number of hits for the specified asset over the specified time period.

Name	Description
HitsPercent	A number (floating-point) value that indicates the hits percentage for the specified asset. Keep in mind that this percentage is calculated from the total hits for all assets included in this report over the specified time period.
Path	A string that identifies the relative path to the asset for which statistical information is returned. This path starts directly after the hostname.

Errors

The response body for an unsuccessful request may contain an error element that provides additional information. For a list of common error messages, please refer to the **Status Codes and Error Messages** topic.

Sample Request and Response

A sample JSON request is provided below.

```
GET
https://api.edgecast.com/v2/reporting/customers/0001/media/3/filestats?begindate=2011-06-01&enddate=2011-06-02 HTTP/1.1

Authorization: TOK:12345678-1234-1234-1234-1234567890ab

Accept: application/json

Host: api.edgecast.com
```

A sample JSON response is provided below.

```
HTTP/1.1 200 OK

Cache-Control: private

Content-Type: application/json; charset=utf-8

Date: Thu, 14 Apr 2016 12:00:00 GMT

Content-Length: 654

[{

        "DataTransferred" : 29731911100,

        "DataTransferredPercentage" : 43.7475,

        "Duration": 0.5021,

        "Hits" : 70286037,

        "HitsPercent" : 81.1283,

        "Path" : "\/000001\/2011\/main.html"

    }, {

        "DataTransferred" : 7161857970,

        "DataTransferredPercentage" : 10.5428,
```

```
                "Duration": 0.5224,
                "Hits" : 15966987,
                "HitsPercent" : 18.43,
                "Path" : "\/000001\/2011\/Demo01.ppt"
        }, {

                "DataTransferred" : 1954210120,
                "DataTransferredPercentage" : 2.8679,
                "Duration": 0.5226,
                "Hits" : 176268,
                "HitsPercent" : 0.2035,
                "Path" : "\/000001\/2011\/Revenue.xls"
        }, {

                "DataTransferred" : 0,
                "DataTransferredPercentage" : 0,
                "Duration": 0.5053,
                "Hits" : 1,
                "HitsPercent" : 0,
                "Path" : "\/000001\/2011\/icon.gif"
        }
]
```

Get Directory Activity

Retrieves statistics for the top 250 requested directories over a specific time period.

Request

A request to retrieve directory statistics is described below. When submitting this request, you will need to define the following terms:

- **AccountNumber:** This term should be replaced by your CDN account number.

- **Platform:** This term should be replaced by the ID associated with the desired platform. Valid values for this parameter are listed below.

    - **2:** Flash Media Streaming

    - **3:** HTTP Large

    - **14:** Application Delivery Network (ADN)

- **StartDateTime:** This term should be replaced by the start date for the report. Only activity that took place after the specified date will be included in the report. The format for this term is: *YYYY-MM-DD*T*hh:mm:ss*.

- **EndDateTime:** This term should be replaced by the end date for the report. Activity that took place after the specified date will not be included in the report. The format for this term is: *YYYY-MM-DD*T*hh:mm:ss*.

Important: Returns data in 1 day intervals. This means that this report will return data for the specified time period including the specified start and end date. This will occur regardless of whether a time value was specified. This means that time is optional and irrelevant for this endpoint.

Note: For more information on date/time format, please refer to **Appendix B: Report Date/Time Format**.

HTTP Method	Request URI
GET	https://api.edgecast.com/v2/reporting/customers/*AccountNumber*/media/*Platform*/directorystats?begindate=*StartDateTime*&enddate=*EndDateTime*

Request Headers

This endpoint only takes advantage of the common request headers described in the **Request Headers** section of the **Request and Response Elements** topic.

Request Body

Request body parameters are not required by this endpoint.

Response

The response to the above request includes an HTTP status code, response headers, and a response body.

Status Code

A status code indicates whether the request was successfully performed. A list of common status codes is provided in the **Status Codes and Error Messages** topic.

Response Headers

The response for this endpoint only returns standard HTTP response headers including those described in the **Response Headers** section of the **Request and Response Elements** topic.

Response Body

The response body for a successful request contains the following response elements for each directory returned by this endpoint:

Name	Description
DataTransferred	An integer that indicates the total amount of data transferred (in bytes) for the specified directory over the specified time period.
DataTransferredPercent	A number (floating-point) value that indicates the data transferred percentage for the specified directory. Keep in mind that this percentage is calculated from the total amount of data transferred for all directories included in this report over the specified period of time.
Duration	A number (floating-point) value that indicates the average amount of time, in seconds, that it took our CDN to serve an asset to a client.
FullDirectoryPath	A string that identifies the relative path to the directory for which statistical information is returned. This path starts directly after the hostname.
Hits	An integer that indicates the total number of hits for the specified directory over the specified time period.
HitsPercent	A number (floating-point) value that indicates the hits percentage for the specified directory. Keep in mind that this percentage is calculated from the total hits for all directories included in this report over the specified time period.

Errors

The response body for an unsuccessful request may contain an error element that provides additional information. For a list of common error messages, please refer to the **Status Codes and Error Messages** topic.

Sample Request and Response

A sample JSON request is provided below.

```
GET
https://api.edgecast.com/v2/reporting/customers/0001/media/3/directorystats?begindat
e=2011-06-01&enddate=2011-06-02 HTTP/1.1

Authorization: TOK:12345678-1234-1234-1234-1234567890ab

Accept: application/json

Host: api.edgecast.com
```

A sample JSON response is provided below.

```
HTTP/1.1 200 OK

Cache-Control: private

Content-Type: application/json; charset=utf-8

Date: Thu, 14 Apr 2016 12:00:00 GMT

Content-Length: 534


[{

            "DataTransferred" : 66872640800,

            "DataTransferredPercent" : 98.381,

            "Duration" : 0.5012,

            "FullDirectoryPath" : "\/000001\/HTML\/",

            "Hits" : 86471638,

            "HitsPercent" : 99.8107

      }, {

            "DataTransferred" : 955630223,

            "DataTransferredPercent" : 1.4,

            "Duration" : 0.5232,

            "FullDirectoryPath" : "\/000001\/HTML\/Resources\/",

            "Hits" : 83859,

            "HitsPercent" : 0.0968

      }, {

            "DataTransferred" : 21474837,

            "DataTransferredPercent" : 0.032,

            "Duration" : 0.5235,

            "FullDirectoryPath" : "\/000001\/HTML\/",

            "Hits" : 53059,

            "HitsPercent" : 0.0612

      }
```

```
]
```

Get Download Activity

Retrieves download statistics for the top 250 downloaded assets over a specific time period.

Please keep in mind the following information when generating this report:

- This report only provides information for assets larger than 50 KB.

- Reports generated for accounts on which compression has been enabled may be inaccurate, since the logged file size may be larger than the total bytes transferred.

- This report may not accurately represent streaming video downloads, since users may seek to different parts of the video.

Request

A request to retrieve download statistics is described below. When submitting this request, you will need to define the following terms:

- **AccountNumber:** This term should be replaced by your CDN account number.

- **Platform:** This term should be replaced by the ID associated with the desired platform. Valid values for this parameter are listed below.

   - **2:** Flash Media Streaming

   - **3:** HTTP Large

   - **14:** Application Delivery Network (ADN)

- **StartDateTime:** This term should be replaced by the start date for the report. Only activity that took place after the specified date will be included in the report. The format for this term is: *YYYY-MM-DD*T*hh*:*mm*:*ss*.

- **EndDateTime:** This term should be replaced by the end date for the report. Activity that took place after the specified date will not be included in the report. The format for this term is: *YYYY-MM-DD*T*hh*:*mm*:*ss*.

Important: Returns data in 1 day intervals. This means that this report will return data for the specified time period including the specified start and end date. This will occur regardless of whether a time value was specified. This means that time is optional and irrelevant for this endpoint.

Note: For more information on date/time format, please refer to **Appendix B: Report Date/Time Format**.

HTTP Method	Request URI
GET	https://api.edgecast.com/v2/reporting/customers/*AccountNumber/*media/*Platform*/completedownloads?begindate=*StartDateTime*&enddate=*EndDateTime*

Request Headers

This endpoint only takes advantage of the common request headers described in the **Request Headers** section of the **Request and Response Elements** topic.

Request Body

Request body parameters are not required by this endpoint.

Response

The response to the above request includes an HTTP status code, response headers, and a response body.

Status Code

A status code indicates whether the request was successfully performed. A list of common status codes is provided in the **Status Codes and Error Messages** topic.

Response Headers

The response for this endpoint only returns standard HTTP response headers including those described in the **Response Headers** section of the **Request and Response Elements** topic.

Response Body

The response body for a successful request contains the following response elements for each asset returned by this endpoint:

Name	Description
CompleteDownloadPercent	A number (floating-point) that indicates the percentage that the entire asset was downloaded. A decimal value is not reported for whole numbers (e.g., 100).
CompleteDownloads	An integer that indicates the total number of times that the entire asset was downloaded.
DownloadAttempts	An integer that indicates the total number of attempts to download the specified asset.
File	A string that indicates the relative path to an asset. This path starts directly after the hostname.

Errors

The response body for an unsuccessful request may contain an error element that provides additional information. For a list of common error messages, please refer to the **Status Codes and Error Messages** topic.

Sample Request and Response

A sample JSON request is provided below.

```
GET
https://api.edgecast.com/v2/reporting/customers/0001/media/3/completedownloads?begin
date=2011-06-01&enddate=2011-06-02 HTTP/1.1

Authorization: TOK:12345678-1234-1234-1234-1234567890ab

Accept: application/json

Host: api.edgecast.com
```

A sample JSON response is provided below.

```
HTTP/1.1 200 OK

Cache-Control: private

Content-Type: application/json; charset=utf-8

Date: Thu, 14 Apr 2016 12:00:00 GMT

Content-Length: 534


[{

            "CompleteDownloadPercent" : 81.33,

            "CompleteDownloads" : 4952436300,

            "DownloadAttempts" : 4952436298,

            "File" : "\/000001\/2011\/Main.html"

      }, {

            "CompleteDownloadPercent" : 18.33,

            "CompleteDownloads" : 1116424040,

            "DownloadAttempts" : 1116424040,

            "File" : "\/000001\/Resources\/Video01.flv"

      }, {

            "CompleteDownloadPercent" : 0.16,

            "CompleteDownloads" : 9525486,

            "DownloadAttempts" : 9525474,

            "File" : "\/000001\/Resources\/Border.gif"

      }
]
```

Real-Time Log Delivery (RTLD)

Real-Time Log Delivery (RTLD) delivers log data in near real-time to a variety of destinations. It consists of two independent modules, which are:

- **Real-Time Log Delivery CDN (RTLD CDN):** Delivers log data that describes requests submitted to our CDN service.

  Note: This feature must be purchased separately. For more information, please contact your CDN account manager.

- **Real-Time Log Delivery WAF (RTLD WAF):** Delivers log data that describes requests identified by Web Application Firewall (WAF) or WAF Essential as threats.

Note: Profile configurations for the above modules are administered independently. For example, you may not retrieve or administer a RTLD WAF profile when requesting a RTLD CDN endpoint.

RTLD CDN

Use these endpoints to automate the administration of RTLD CDN.

Add RTLD CDN Profile

Creates a RTLD CDN profile.

Request

A request to create a RTLD CDN profile is described below. When submitting this request, you will need to define the following term:

- **AccountNumber:** This term should be replaced by your CDN account number. This number can be found in the upper-right hand corner of the MCC.

HTTP Method	Request URI
POST	https://api.edgecast.com/v2/mcc/customers/*AccountNumber*/rtld/settings

Request Headers
This endpoint only takes advantage of the common request headers described in the **Request Headers** section of the **Request and Response Elements** topic.

Request Body
Pass the following request body parameters:

Name	Data Type	Description
profile_name	String	Assigns a unique name to the log delivery profile. The maximum length for this property is 36 characters.
description	String	Determines the log delivery profile's description. The maximum length for this property is 100 characters.
log_format	String	Determines the format for log data. Valid values are: json | json_array | json_lines | csv **Note:** This property may only be defined when delivery_method is set to http_post, aws_s3, azure_blob_storage, or gcs.
enabled	Boolean	Determines whether log data will be delivered to the destination defined by the delivery_method parameter. Valid values are: true | false
custom_cookies	Array of string values	Defines each cookie that will be logged for each request.
custom_request_headers	Array of string values	Defines each request header that will be logged for each request.
custom_response_headers	Array of string values	Defines each response header that will be logged for each request.
delivery_method	String	Required. Determines the destination (e.g., aws_s3 or azure_blob_storage) to which log data will be delivered. **Tip:** Use the Get Log Delivery Methods endpoint to retrieve the set of valid values for this parameter. **Note:** You should only configure the delivery method defined by this parameter. For example, if you set this parameter to http_post, you should define the http_post object and then either omit or set the objects for other delivery methods (e.g., aws_s3 or azure_blob_storage) to null.

Name	Data Type	Description
fields	Array	Required. Specify a string value for each log field that will be delivered.
		Tip: Use the Get Log Fields (RTLD CDN) endpoint to retrieve the set of valid values for this parameter.
downsampling_rate	Decimal	Determines the rate at which log data will be downsampled. Omit or set this parameter to null to disable log data downsampling.
		Tip: Use the Get Log Downsampling Rates endpoint to retrieve the set of valid values for this parameter.
platforms	Array	Required. Specify a string value for each platform for which this RTLD CDN profile will be applied.
		http_large | http_small | adn
filters	Object	Contains your log data filtering profile.
status_codes	Array	Specify a string value for each HTTP status code for which log data will be delivered. Omit this parameter or define an empty array if log data should not be filtered by HTTP status codes.
		Tip: Use the Get HTTP Status Codes endpoint to retrieve the set of valid values for this parameter.
		Example:
		"status_codes": ["2xx", "3xx"],

Name	Data Type	Description
cnames	Array	Specify a string value for each edge CNAME for which log data will be delivered. Omit this parameter or define an empty array if log data should not be filtered by edge CNAMEs.
		Tip: Retrieve edge CNAMEs via the Name response parameter from the Get All Edge CNAMEs - ADN, Get All Edge CNAMEs - HTTP Large, and/or Get All Edge CNAMEs - HTTP Small endpoints.
		Example: "cnames": ["cdn1.example.com", "cdn2.example.com"],
cnames_condition	String	Determines how log data will be filtered by edge CNAME(s). Valid values are: • **in:** Filters log data to only include requests that point to the edge CNAMEs defined within the cnames property. • **not_in:** Filters log data to exclude requests that point to the edge CNAMEs defined within the cnames property.
user_agent_regexp	String	Defines a RE2-compatible regular expression pattern that identifies the set of user agents by which log data will be filtered.
http_post	Object	**Note:** Required when delivery_method is set to http_post. Contains the configuration for the HTTP POST log delivery method.

Name	Data Type	Description
authentication_type	String	**Note:** Required when delivery_method is set to http_post.
		Determines how log delivery requests will be authenticated to your web servers.
		Tip: Use the Get HTTP POST Authentication Methods endpoint to retrieve the set of valid values for this parameter.
destination_endpoint	String	**Note:** Required when delivery_method is set to http_post.
		Defines the absolute URL to which log data will be delivered.
		Sample value:
		https://logs.example.com/cdn/
token	String	**Note:** Required when authentication_type is set to custom_authentication.
		Defines the token value that will be passed via the Authorization request header whenever log data is delivered to your web servers.
username	String	**Note:** Required when authentication_type is set to http_basic.
		Defines the user name through which requests to your web server will be authenticated.
password	String	**Note:** Required when authentication_type is set to http_basic.
		Defines the password through which requests to your web server will be authenticated.
		Note: Base-64 encoding will applied to the specified credentials. After which, the encoded value will be passed via the Authorization header.

Name	Data Type	Description
aws_s3	Object	**Note:** Required when delivery_method is set to aws_s3. Contains the configuration for the AWS S3 log delivery method.
bucket	String	**Note:** Required when delivery_method is set to aws_s3. Determines the AWS S3 bucket to which log data will be delivered.
prefix	String	Defines the prefix that identifies a virtual log file storage location and/or a prefix that will be added to each object added to your bucket.
region	String	**Note:** Required when delivery_method is set to aws_s3. Identifies the region assigned to the AWS S3 bucket defined by the bucket parameter. **Tip:** Use the Get AWS Regions endpoint to retrieve the set of valid values for this parameter.
splunk_enterprise	Object	**Note:** Required when delivery_method is set to splunk_enterprise. Contains the configuration for the Splunk Enterprise log delivery method.
url	String	**Note:** Required when delivery_method is set to splunk_enterprise. Defines a URL that points to your Splunk Enterprise's HTTP Event Collector configuration. **Default URL syntax:** https://{Splunk-Enterprise-Hostname}:{port}/services/collector/raw

Name	Data Type	Description
token	String	**Note:** Required when delivery_method is set to splunk_enterprise.
		Defines the token corresponding to the HTTP Event Collector configuration associated with the URL defined by the url parameter.
sumo_logic	Object	**Note:** Required when delivery_method is set to sumo_logic.
		Contains the configuration for the Sumo Logic log delivery method.
url	String	**Note:** Required when delivery_method is set to sumo_logic.
		Defines a URL that points to the HTTP source defined within Sumo Logic.
azure_blob_storage	Object	**Note:** Required when delivery_method is set to azure_blob_storage.
		Contains the configuration for the Azure Blob Storage log delivery method.
url	String	**Note:** Required when delivery_method is set to azure_blob_storage.
		Defines a URL that points to the Blob container to which log data will be posted.
prefix	String	Defines a virtual log file storage location and/or a prefix that will be added to each log file added to your container.
access_type	String	**Note:** Required when delivery_method is set to azure_blob_storage.
		Determines whether log data uploads will be authorized via a SAS token or an access key
		Tip: Use the Get Access Types (Azure Blob Storage) endpoint to retrieve the set of valid values for this parameter.

Name	Data Type	Description
access_key	String	**Note:** Required when access_type is set to access_key. Defines the access key through which log data uploads will be authorized.
token	String	**Note:** Required when access_type is set to sas_token. Defines the SAS token through which log data uploads will be authorized.
datadog	Object	**Note:** Required when delivery_method is set to datadog. Contains the profile for the Datadog log delivery method.
site	String	**Note:** Required when delivery_method is set to datadog. Defines the Datadog site to which log data will be delivered. Valid values are: US | EU
api_key	String	**Note:** Required when delivery_method is set to datadog. Defines the API key through which log data uploads will be authorized.
service_attribute_value	String	**Note:** Required when delivery_method is set to datadog. Defines a value through which uploaded log data will be identified within the Datadog environment.
gcs	Object	**Note:** Required when delivery_method is set to gcs. Contains the configuration for the Google Cloud Storage log delivery method.

Name	Data Type	Description
bucket	String	**Note:** Required when delivery_method is set to gcs. Determines the Google Cloud Storage bucket to which log data will be delivered.
prefix	String	Defines the prefix that identifies a virtual log file storage location and/or a prefix that will be added to each object added to your bucket.
new_relic	Object	**Note:** Required when delivery_method is set to new_relic. Contains the configuration for the New Relic log delivery method.
account_id	String	**Note:** Required when delivery_method is set to new_relic. Identifies the system-defined ID for the New Relic account to which log data will be uploaded.
event_type	String	**Note:** Required when delivery_method is set to new_relic. Defines the label that identifies log data delivered to New Relic as a result of this profile. Specify a label that solely consists of alphanumeric characters, underscores, and colons.
insert_key	String	**Note:** Required when delivery_method is set to new_relic. Defines the Inserts insight API key through which log data uploads will be authorized.

Response

The response to the above request includes an HTTP status code, response headers, and a response body.

Status Code

A status code indicates whether the request was successfully performed. A list of common status codes is provided in the **Status Codes and Error Messages** topic.

Response Headers

The response for this endpoint only returns standard HTTP response headers including those described in the **Response Headers** section of the **Request and Response Elements** topic.

Response Body

The response body for a successful request contains the following response element:

Name	Data Type	Description
@id	String	Indicates the relative path to the requested endpoint.
@type	String	Returns RtldSetting.
id	Integer	Indicates the system-defined ID for your RTLD CDN profile.
profile_name	String	Indicates the log delivery profile's name.
description	String	Indicates the log delivery profile's description.
log_format	String	Indicates the format for log data. **Note:** A null value indicates that a default log format will be used.
account_number	String	Indicates your customer account number.
enabled	Boolean	Indicates whether the RTLD CDN profile is enabled. Valid values are: true | false
custom_cookies	Array of string values	Indicates each cookie that will be logged for each request.
custom_request_headers	Array of string values	Indicates each request header that will be logged for each request.
custom_response_headers	Array of string values	Indicates each response header that will be logged for each request.
delivery_method	String	Indicates the destination to which log data will be delivered.
fields	Array	Indicates the set of log fields that will be delivered.
downsampling_rate	Decimal	Indicates the rate at which log data will be downsampled. A null value indicates that log data will not be downsampled.

Name	Data Type	Description
platforms	Array	Indicates the set of platforms to which this RTLD CDN profile will be applied.
filters	Object	Contains your log data filtering configuration.
status_codes	Array	Indicates the set of HTTP status codes by which log data will be filtered. A null value indicates that log data will not be filtered by HTTP status codes.
cnames	Array	Indicates the set of edge CNAMEs by which log data will be filtered. A null value indicates that log data will not be filtered by edge CNAMEs.
cnames_condition	String	Indicates how log data will be filtered by edge CNAME(s). Valid values are: **in:** Filters log data to only include requests that point to the edge CNAMEs defined within the cnames property. **not_in:** Filters log data to exclude requests that point to the edge CNAMEs defined within the cnames property.
user_agent_regexp	String	Indicates the set of user agents by which log data will be filtered through a RE2-compatible regular expression pattern.
http_post	Object	Contains the configuration for the HTTP POST log delivery method.
authentication_type	String	Indicates how log delivery requests will be authenticated to your web servers.
destination_endpoint	String	Indicates the absolute URL to which log data will be delivered.
token	String	Indicates the token value that will be passed via the Authorization request header whenever log data is delivered to your web servers.
username	String	Indicates the user name through which requests to your web server will be authenticated.
password	String	Indicates the encrypted value of the password through which requests to your web server will be authenticated.
masked_password	String	Indicates a masked value that represents the password defined within the password element.
masked_token	String	Indicates a masked value that represents the token defined within the token element.
aws_s3	Object	Contains the configuration for the AWS S3 log delivery method.
bucket	String	Indicates the AWS S3 bucket to which log data will be delivered.

Name	Data Type	Description
prefix	String	Indicates the prefix that identifies a virtual log file storage location and/or a prefix that will be added to each object added to your bucket.
region	String	Indicates the region assigned to the AWS S3 bucket defined by the bucket parameter.
splunk_enterprise	Object	Contains the configuration for the Splunk Enterprise log delivery method.
url	String	Indicates a URL that points to your Splunk Enterprise's HTTP Event Collector configuration.
token	String	Indicates the token corresponding to the HTTP Event Collector configuration associated with the URL defined by the url parameter.
sumo_logic	Object	Contains the configuration for the Sumo Logic log delivery method.
url	String	Indicates a URL that points to the HTTP source defined within Sumo Logic.
masked_url	String	Indicates a masked value that represents the URL defined within the url element.
azure_blob_storage	Object	Contains the configuration for the Azure Blob Storage log delivery method.
url	String	Indicates a URL that points to the Blob container to which log data will be posted.
prefix	String	Indicates a virtual log file storage location and/or a prefix that will be added to each log file added to your container.
access_type	String	Indicates whether log data uploads will be authorized via a SAS token or an access key.
access_key	String	Indicates the access key through which log data uploads will be authorized.
token	String	Indicates the SAS token through which log data uploads will be authorized.
masked_access_key	String	Indicates a masked value that represents the access key defined within the access_key element.
masked_token	String	Indicates a masked value that represents the SAS token defined within the token element.
datadog	Object	Contains the profile for the Datadog log delivery method.
site	String	Indicates the Datadog site to which log data will be delivered. Valid values are: US | EU
api_key	String	Indicates the API key through which log data uploads will be authorized.
service_attribute_value	String	Indicates a value through which uploaded log data will be identified within the Datadog environment.

Name	Data Type	Description
masked_api_key	String	Indicates a masked value that represents the API key defined within the api_key element.
gcs	Object	Contains the configuration for the Google Cloud Storage log delivery method.
bucket	String	Indicates the Google Cloud Storage bucket to which log data will be delivered.
prefix	String	Indicates the prefix that identifies a virtual log file storage location and/or a prefix that will be added to each object added to your bucket.
new_relic	Object	Contains the configuration for the New Relic log delivery method.
account_id	String	Indicates the system-defined ID for the New Relic account to which log data will be uploaded.
event_type	String	Indicates the label that identifies log data delivered to New Relic as a result of this profile.
insert_key	String	Indicates the Inserts insight API key through which log data uploads will be authorized.
masked_insert_key	String	Indicates a masked value that represents the Inserts insight API key defined within the insert_key element.

Errors

The response body for an unsuccessful request may contain an error element that provides additional information. For a list of common error messages, please refer to the **Status Codes and Error Messages** topic.

Sample Request and Response

A sample JSON request is provided below.

```
POST https://api.edgecast.com/v2/mcc/customers/0001/rtld/settings HTTP/1.1

Authorization: TOK:12345678-1234-1234-1234-1234567890ab

Accept: application/json

Content-Type: application/json

Host: api.edgecast.com

Content-Length: 513
```

```
{
        "delivery_method": "http_post",

        "fields": ["user_agent", "rewritten_path", "path", "timestamp", "client_ip",
        "client_ip_version", "status_code", "status", "cache_status", "bytes_out",
        "write_time", "file_size", "server_ip", "server_port", "method", "host",
        "query", "auth_user", "read_time"],

        "platforms": [

                "adn"

        ],

        "http_post": {

                "destination_endpoint": "https://logs.example.com/cdn/",

                "authentication_type": "none",

                "token": null,

                "username": null,

                "password": null

        }

}
```

A sample JSON response is provided below.

```
HTTP/1.1 200 OK
Cache-Control: private
Content-Type: application/xml; charset=utf-8
Date: Thu, 14 Apr 2016 12:00:00 GMT
Content-Length: 900


{
        "@id": "/v2/mcc/customers/0001/rtld/settings",

        "@type": "RtldSetting",

        "id": 20,

        "account_number": "0001",

        "delivery_method": "http_post",

        "enabled": false,

        "downsampling_rate": null,

        "fields": ["user_agent", "rewritten_path", "path", "timestamp", "client_ip",
        "client_ip_version", "status_code", "status", "cache_status", "bytes_out",
        "write_time", "file_size", "server_ip", "server_port", "method", "host",
        "query", "auth_user", "read_time"],

        "platforms": [

                "adn"

        ],
```

```
        "filters": {
                "status_codes": null,
                "cnames": null
        },
        "aws_s3": null,
        "http_post": {
                "destination_endpoint": "https://logs.example.com/cdn/",
                "authentication_type": "none",
                "token": null,
                "username": null,
                "password": null
        },
        "sumo_logic": null,
        "splunk_enterprise": null,
        "azure_blob_storage": null
}
```

Delete RTLD CDN Profile

Deletes a RTLD CDN profile.

Request

A request to delete a RTLD CDN profile is described below. When submitting this request, you will need to define the following variable:

- **AccountNumber:** Replace this variable with your CDN account number. This number can be found in the upper-right hand corner of the MCC.

- **SettingsID:** Replace this variable with the system-defined ID assigned to your RTLD CDN profile.

Tip: Reference the items[0].id parameter from the Get All RTLD CDN Profiles endpoint to find out the ID assigned to your RTLD CDN profile.

HTTP Method	Request URI
DELETE	https://api.edgecast.com/v2/mcc/customers/*AccountNumber*/rtld/settings/*SettingsID*

Request Headers

The response for this endpoint only includes standard HTTP request headers including those described in the **Request Headers** section of the **Request and Response Elements** topic.

Request Body

Request body parameters are not required by this endpoint.

Response

The response to the above request includes an HTTP status code, response headers, and a response body.

Status Code

A status code indicates whether the request was successfully performed. A list of common status codes is provided in the **Status Codes and Error Messages** topic.

Response Headers

The response for this endpoint only returns standard HTTP response headers including those described in the **Response Headers** section of the **Request and Response Elements** topic.

Response Body

The response body for a successful request does not contain a response element.

Errors

The response body for an unsuccessful request may contain an error element that provides additional information. For a list of common error messages, please refer to the **Status Codes and Error Messages** topic.

Sample Request and Response

A sample JSON request is provided below.

DELETE https://api.edgecast.com/v2/mcc/customers/0001/rtld/settings/20 HTTP/1.1

Authorization: TOK:12345678-1234-1234-1234-1234567890ab

Accept: application/json

Host: api.edgecast.com

A sample JSON response is provided below.

HTTP/1.1 204 No Content

Cache-Control: private

Content-Type: application/json; charset=utf-8

Date: Thu, 14 Apr 2016 12:00:00 GMT

Content-Length: 0

Get All RTLD CDN Profiles

Retrieves all of your RTLD CDN profiles.

Request

A request to retrieve your log delivery profiles is described below. When submitting this request, you will need to define the following variable:

- **AccountNumber:** Replace this variable with your CDN account number. This number can be found in the upper-right hand corner of the MCC.

HTTP Method	Request URI
GET	https://api.edgecast.com/v2/mcc/customers/*AccountNumber*/rtld/settings

Request Headers

The response for this endpoint only includes standard HTTP request headers including those described in the **Request Headers** section of the **Request and Response Elements** topic.

Request Body

Request body parameters are not required by this endpoint.

Response

The response to the above request includes an HTTP status code, response headers, and a response body.

Status Code

A status code indicates whether the request was successfully performed. A list of common status codes is provided in the **Status Codes and Error Messages** topic.

Response Headers

The response for this endpoint only returns standard HTTP response headers including those described in the **Response Headers** section of the **Request and Response Elements** topic.

Response Body

The response body for a successful request contains the following response elements:

Name	Data Type	Description
@id	String	Indicates the relative path to the requested endpoint.
@type	String	Returns Collection.
items	Array	Contains your Real-Time Log Delivery profiles.

Name	Data Type	Description
@id	Integer	Indicates the relative path to an endpoint that returns a specific RTLD CDN profile.
@type	String	Returns RtldSetting.
id	Integer	Indicates the system-defined ID for your RTLD CDN profile.
profile_name	String	Indicates the log delivery profile's name.
description	String	Indicates the log delivery profile's description.
log_format	String	Indicates the format for log data. **Note:** A null value indicates that a default log format will be used.
account_number	String	Indicates your customer account number.
enabled	Boolean	Indicates whether the RTLD CDN profile is enabled. Valid values are: true | false
custom_cookies	Array of string values	Indicates each cookie that will be logged for each request.
custom_request_headers	Array of string values	Indicates each request header that will be logged for each request.
custom_response_headers	Array of string values	Indicates each response header that will be logged for each request.
delivery_method	String	Indicates the destination to which log data will be delivered.
fields	Array	Indicates the set of log fields that will be delivered.
downsampling_rate	Decimal	Indicates the rate at which log data will be downsampled. A null value indicates that log data will not be downsampled.
platforms	Array	Indicates the set of platforms to which this RTLD CDN profile will be applied.
filters	Object	Contains your log data filtering configuration.
status_codes	Array	Indicates the set of HTTP status codes by which log data will be filtered. A null value indicates that log data will not be filtered by HTTP status codes.

Name	Data Type	Description
cnames	Array	Indicates the set of edge CNAMEs by which log data will be filtered. A null value indicates that log data will not be filtered by edge CNAMEs.
cnames_condition	String	Indicates how log data will be filtered by edge CNAME(s). Valid values are: • **in:** Filters log data to only include requests that point to the edge CNAMEs defined within the cnames property. • **not_in:** Filters log data to exclude requests that point to the edge CNAMEs defined within the cnames property.
user_agent_regexp	String	Indicates the set of user agents by which log data will be filtered through a RE2-compatible regular expression pattern.
http_post	Object	Contains the configuration for the HTTP POST log delivery method.
authentication_type	String	Indicates how log delivery requests will be authenticated to your web servers.
destination_endpoint	String	Indicates the absolute URL to which log data will be delivered.
token	String	Indicates the token value that will be passed via the Authorization request header whenever log data is delivered to your web servers.
username	String	Indicates the user name through which requests to your web server will be authenticated.
password	String	Indicates the encrypted value of the password through which requests to your web server will be authenticated.
masked_password	String	Indicates a masked value that represents the password defined within the password element.
masked_token	String	Indicates a masked value that represents the token defined within the token element.
aws_s3	Object	Contains the configuration for the AWS S3 log delivery method.

Name	Data Type	Description
bucket	String	Indicates the AWS S3 bucket to which log data will be delivered.
prefix	String	Indicates the prefix that identifies a virtual log file storage location and/or a prefix that will be added to each object added to your bucket.
region	String	Indicates the region assigned to the AWS S3 bucket defined by the bucket parameter.
splunk_enterprise	Object	Contains the configuration for the Splunk Enterprise log delivery method.
url	String	Indicates a URL that points to your Splunk Enterprise's HTTP Event Collector configuration.
token	String	Indicates the token corresponding to the HTTP Event Collector configuration associated with the URL defined by the url parameter.
sumo_logic	Object	Contains the configuration for the Sumo Logic log delivery method.
url	String	Indicates a URL that points to the HTTP source defined within Sumo Logic.
masked_url	String	Indicates a masked value that represents the URL defined within the url element.
azure_blob_storage	Object	Contains the configuration for the Azure Blob Storage log delivery method.
url	String	Indicates a URL that points to the Blob container to which log data will be posted.
prefix	String	Indicates a virtual log file storage location and/or a prefix that will be added to each log file added to your container.
access_type	String	Indicates whether log data uploads will be authorized via a SAS token or an access key.
access_key	String	Indicates the access key through which log data uploads will be authorized.
token	String	Indicates the SAS token through which log data uploads will be authorized.
masked_access_key	String	Indicates a masked value that represents the access key defined within the access_key element.

Name	Data Type	Description
masked_token	String	Indicates a masked value that represents the SAS token defined within the token element.
datadog	Object	Contains the profile for the Datadog log delivery method.
site	String	Indicates the Datadog site to which log data will be delivered. Valid values are: US | EU
api_key	String	Indicates the API key through which log data uploads will be authorized.
service_attribute_value	String	Indicates a value through which uploaded log data will be identified within the Datadog environment.
masked_api_key	String	Indicates a masked value that represents the API key defined within the api_key element.
total_items	Integer	Returns 1. Indicates the total number of RTLD CDN profiles that were included in the response.
gcs	Object	Contains the configuration for the Google Cloud Storage log delivery method.
bucket	String	Indicates the Google Cloud Storage bucket to which log data will be delivered.
prefix	String	Indicates the prefix that identifies a virtual log file storage location and/or a prefix that will be added to each object added to your bucket.
new_relic	Object	Contains the configuration for the New Relic log delivery method.
account_id	String	Indicates the system-defined ID for the New Relic account to which log data will be uploaded.
event_type	String	Indicates the label that identifies log data delivered to New Relic as a result of this profile.
insert_key	String	Indicates the Inserts insight API key through which log data uploads will be authorized.
masked_insert_key	String	Indicates a masked value that represents the Inserts insight API key defined within the insert_key element.

Errors

The response body for an unsuccessful request may contain an error element that provides additional information. For a list of common error messages, please refer to the **Status Codes and Error Messages** topic.

Sample Request and Response

A sample JSON request is provided below.

```
GET https://api.edgecast.com/v2/mcc/customers/0001/rtld/settings HTTP/1.1

Authorization: TOK:12345678-1234-1234-1234-1234567890ab

Accept: application/json

Host: api.edgecast.com
```

A sample JSON response is provided below.

```
HTTP/1.1 200 OK

Cache-Control: private

Content-Type: application/json; charset=utf-8

Date: Thu, 14 Apr 2016 12:00:00 GMT

Content-Length: 1013

{

        "@id": "/v2/mcc/customers/0001/rtld/settings",

        "@type": "Collection",

        "items": [{

                    "@id": "/v2/mcc/customers/0001/rtld/settings/20",

                    "@type": "RtldSetting",

                    ...

                    "http_post": {

                            "destination_endpoint":
        "https://logs.example.com/cdn/",

                            "authentication_type": "none",

                            "token": null,

                            "username": null,

                            "password": null

                },

            }

        ],

        "total_items": 1

}
```

Get RTLD CDN Profile

Retrieves a RTLD CDN profile.

Request

A request to retrieve your RTLD CDN profile is described below. When submitting this request, you will need to define the following variable:

- **AccountNumber:** Replace this variable with your CDN account number. This number can be found in the upper-right hand corner of the MCC.

- **SettingsID:** Replace this variable with the system-defined ID assigned to your RTLD CDN profile.

Tip: Reference the items[0].id parameter from the Get All RTLD CDN Profiles endpoint to find out the ID assigned to your RTLD CDN profile.

HTTP Method	Request URI
GET	https://api.edgecast.com/v2/mcc/customers/*AccountNumber*/rtld/settings/*SettingsID*

Request Headers

The response for this endpoint only includes standard HTTP request headers including those described in the **Request Headers** section of the **Request and Response Elements** topic.

Request Body

Request body parameters are not required by this endpoint.

Response

The response to the above request includes an HTTP status code, response headers, and a response body.

Status Code

A status code indicates whether the request was successfully performed. A list of common status codes is provided in the **Status Codes and Error Messages** topic.

Response Headers

The response for this endpoint only returns standard HTTP response headers including those described in the **Response Headers** section of the **Request and Response Elements** topic.

Response Body

The response body for a successful request contains the following response elements:

Name	Data Type	Description
@id	String	Indicates the relative path to the requested endpoint.
@type	String	Returns RtldSetting.
id	Integer	Indicates the system-defined ID for your RTLD CDN profile.
profile_name	String	Indicates the log delivery profile's name.
description	String	Indicates the log delivery profile's description.
log_format	String	Indicates the format for log data. **Note:** A null value indicates that a default log format will be used.
account_number	String	Indicates your customer account number.
enabled	Boolean	Indicates whether the RTLD CDN profile is enabled. Valid values are: true | false
custom_cookies	Array of string values	Indicates each cookie that will be logged for each request.
custom_request_headers	Array of string values	Indicates each request header that will be logged for each request.
custom_response_headers	Array of string values	Indicates each response header that will be logged for each request.
delivery_method	String	Indicates the destination to which log data will be delivered.
fields	Array	Indicates the set of log fields that will be delivered.
downsampling_rate	Decimal	Indicates the rate at which log data will be downsampled. A null value indicates that log data will not be downsampled.
platforms	Array	Indicates the set of platforms to which this RTLD CDN profile will be applied.
filters	Object	Contains your log data filtering configuration.

Name	Data Type	Description
status_codes	Array	Indicates the set of HTTP status codes by which log data will be filtered. A null value indicates that log data will not be filtered by HTTP status codes.
cnames	Array	Indicates the set of edge CNAMEs by which log data will be filtered. A null value indicates that log data will not be filtered by edge CNAMEs.
cnames_condition	String	Indicates how log data will be filtered by edge CNAME(s). Valid values are: • **in:** Filters log data to only include requests that point to the edge CNAMEs defined within the cnames property. • **not_in:** Filters log data to exclude requests that point to the edge CNAMEs defined within the cnames property.
user_agent_regexp	String	Indicates the set of user agents by which log data will be filtered through a RE2-compatible regular expression pattern.
http_post	Object	Contains the configuration for the HTTP POST log delivery method.
authentication_type	String	Indicates how log delivery requests will be authenticated to your web servers.
destination_endpoint	String	Indicates the absolute URL to which log data will be delivered.
token	String	Indicates the token value that will be passed via the Authorization request header whenever log data is delivered to your web servers.
username	String	Indicates the user name through which requests to your web server will be authenticated.
password	String	Indicates the encrypted value of the password through which requests to your web server will be authenticated.

Name	Data Type	Description
masked_password	String	Indicates a masked value that represents the password defined within the password element.
masked_token	String	Indicates a masked value that represents the token defined within the token element.
aws_s3	Object	Contains the configuration for the AWS S3 log delivery method.
bucket	String	Indicates the AWS S3 bucket to which log data will be delivered.
prefix	String	Indicates the prefix that identifies a virtual log file storage location and/or a prefix that will be added to each object added to your bucket.
region	String	Indicates the region assigned to the AWS S3 bucket defined by the bucket parameter.
splunk_enterprise	Object	Contains the configuration for the Splunk Enterprise log delivery method.
url	String	Indicates a URL that points to your Splunk Enterprise's HTTP Event Collector configuration.
token	String	Indicates the token corresponding to the HTTP Event Collector configuration associated with the URL defined by the url parameter.
sumo_logic	Object	Contains the configuration for the Sumo Logic log delivery method.
url	String	Indicates a URL that points to the HTTP source defined within Sumo Logic.
masked_url	String	Indicates a masked value that represents the URL defined within the url element.
azure_blob_storage	Object	Contains the configuration for the Azure Blob Storage log delivery method.
url	String	Indicates a URL that points to the Blob container to which log data will be posted.

Name	Data Type	Description
prefix	String	Indicates a virtual log file storage location and/or a prefix that will be added to each log file added to your container.
access_type	String	Indicates whether log data uploads will be authorized via a SAS token or an access key.
access_key	String	Indicates the access key through which log data uploads will be authorized.
token	String	Indicates the SAS token through which log data uploads will be authorized.
masked_access_key	String	Indicates a masked value that represents the access key defined within the access_key element.
masked_token	String	Indicates a masked value that represents the SAS token defined within the token element.
datadog	Object	Contains the profile for the Datadog log delivery method.
site	String	Indicates the Datadog site to which log data will be delivered. Valid values are: US | EU
api_key	String	Indicates the API key through which log data uploads will be authorized.
service_attribute_value	String	Indicates a value through which uploaded log data will be identified within the Datadog environment.
masked_api_key	String	Indicates a masked value that represents the API key defined within the api_key element.
gcs	Object	Contains the configuration for the Google Cloud Storage log delivery method.
bucket	String	Indicates the Google Cloud Storage bucket to which log data will be delivered.
prefix	String	Indicates the prefix that identifies a virtual log file storage location and/or a prefix that will be added to each object added to your bucket.
new_relic	Object	Contains the configuration for the New Relic log delivery method.

Name	Data Type	Description
account_id	String	Indicates the system-defined ID for the New Relic account to which log data will be uploaded.
event_type	String	Indicates the label that identifies log data delivered to New Relic as a result of this profile.
insert_key	String	Indicates the Inserts insight API key through which log data uploads will be authorized.
masked_insert_key	String	Indicates a masked value that represents the Inserts insight API key defined within the insert_key element.

Errors

The response body for an unsuccessful request may contain an error element that provides additional information. For a list of common error messages, please refer to the **Status Codes and Error Messages** topic.

Sample Request and Response

A sample JSON request is provided below.

GET https://api.edgecast.com/v2/mcc/customers/0001/rtld/settings/20 HTTP/1.1

Authorization: TOK:12345678-1234-1234-1234-1234567890ab

Accept: application/json

Host: api.edgecast.com

A sample JSON response is provided below.

HTTP/1.1 200 OK

Cache-Control: private

Content-Type: application/json; charset=utf-8

Date: Thu, 14 Apr 2016 12:00:00 GMT

Content-Length: 835

```json
{
        "@id": "/v2/mcc/customers/0001/rtld/settings/20",

        "@type": "RtldSetting",

        ...

        "http_post": {

                "destination_endpoint": "https://logs.example.com/cdn/",

                "authentication_type": "none",

                "token": null,

                "username": null,

                "password": null

        },

        "sumo_logic": null,

        "splunk_enterprise": null,

        "azure_blob_storage": null

}
```

Update RTLD CDN Profile

Updates a RTLD CDN profile.

Request

A request to update a RTLD CDN profile is described below. When submitting this request, you will need to define the following terms:

- **AccountNumber:** This term should be replaced by your CDN account number. This number can be found in the upper-right hand corner of the MCC.

- **SettingsID:** Replace this variable with the system-defined ID assigned to your RTLD CDN profile.

    Tip: Reference the items[0].id parameter from the Get All RTLD CDN Profiles endpoint to find out the ID assigned to your RTLD CDN profile.

HTTP Method	Request URI
PUT	https://api.edgecast.com/v2/mcc/customers/*AccountNumber*/rtld/settings/*SettingsID*

Request Headers

This endpoint only takes advantage of the common request headers described in the **Request Headers** section of the **Request and Response Elements** topic.

Request Body

Pass the following request body parameters:

Name	Data Type	Description
@id	String	Identifies the relative path to the requested endpoint.
@type	String	Set to RtldSetting.
profile_name	String	Assigns a unique name to the log delivery profile. The maximum length for this property is 36 characters.
description	String	Determines the log delivery profile's description. The maximum length for this property is 100 characters.

Name	Data Type	Description
log_format	String	Determines the format for log data. Valid values are: json | json_array | json_lines | csv **Note:** This property may only be defined when delivery_method is set to http_post, aws_s3, azure_blob_storage, or gcs.
enabled	Boolean	Determines whether log data will be delivered to the destination defined by the delivery_method parameter. Valid values are: true | false
custom_cookies	Array of string values	Defines each cookie that will be logged for each request.
custom_request_headers	Array of string values	Defines each request header that will be logged for each request.
custom_response_headers	Array of string values	Defines each response header that will be logged for each request.
delivery_method	String	Required. Determines the destination (e.g., aws_s3 or azure_blob_storage) to which log data will be delivered. **Tip:** Use the Get Log Delivery Methods endpoint to retrieve the set of valid values for this parameter. **Note:** You should only configure the delivery method defined by this parameter. For example, if you set this parameter to http_post, you should define the http_post object and then either omit or set the objects for other delivery methods (e.g., aws_s3 or azure_blob_storage) to null.
fields	Array	Required. Specify a string value for each log field that will be delivered. **Tip:** Use the Get Log Fields (RTLD CDN) endpoint to retrieve the set of valid values for this parameter.

Name	Data Type	Description
downsampling_rate	Decimal	Determines the rate at which log data will be downsampled. Omit or set this parameter to null to disable log data downsampling.
		Tip: Use the Get Log Downsampling Rates endpoint to retrieve the set of valid values for this parameter.
platforms	Array	Required. Specify a string value for each platform for which this RTLD CDN profile will be applied.
		http_large | http_small | adn
filters	Object	Contains your log data filtering configuration.
status_codes	Array	Specify a string value for each HTTP status code for which log data will be delivered. Omit this parameter or define an empty array if log data should not be filtered by HTTP status codes.
		Tip: Use the Get HTTP Status Codes endpoint to retrieve the set of valid values for this parameter.
		Example:
		"status_codes": ["2xx", "3xx"],
cnames	Array	Specify a string value for each edge CNAME for which log data will be delivered. Omit this parameter or define an empty array if log data should not be filtered by edge CNAMEs.
		Tip: Retrieve edge CNAMEs via the Name response parameter from the Get All Edge CNAMEs - ADN, Get All Edge CNAMEs - HTTP Large, and/or Get All Edge CNAMEs - HTTP Small endpoints.
		Example:
		"cnames": ["cdn1.example.com", "cdn2.example.com"],

Name	Data Type	Description
cnames_condition	String	Determines how log data will be filtered by edge CNAME(s). Valid values are: • **in:** Filters log data to only include requests that point to the edge CNAMEs defined within the cnames property. • **not_in:** Filters log data to exclude requests that point to the edge CNAMEs defined within the cnames property.
user_agent_regexp	String	Defines a RE2-compatible regular expression pattern that identifies the set of user agents by which log data will be filtered.
http_post	Object	**Note:** Required when delivery_method is set to http_post. Contains the configuration for the HTTP POST log delivery method.
authentication_type	String	**Note:** Required when delivery_method is set to http_post. Determines how log delivery requests will be authenticated to your web servers. **Tip:** Use the Get HTTP POST Authentication Methods endpoint to retrieve the set of valid values for this parameter.
destination_endpoint	String	**Note:** Required when delivery_method is set to http_post. Defines the absolute URL to which log data will be delivered. **Sample value:** https://logs.example.com/cdn/

Name	Data Type	Description
token	String	**Note:** Required when authentication_type is set to custom_authentication.
		Defines the token value that will be passed via the Authorization request header whenever log data is delivered to your web servers.
username	String	**Note:** Required when authentication_type is set to http_basic.
		Defines the user name through which requests to your web server will be authenticated.
password	String	**Note:** Required when authentication_type is set to http_basic.
		Defines the password through which requests to your web server will be authenticated.
		Note: Base-64 encoding will applied to the specified credentials. After which, the encoded value will be passed via the Authorization header.
aws_s3	Object	**Note:** Required when delivery_method is set to aws_s3.
		Contains the configuration for the AWS S3 log delivery method.
bucket	String	**Note:** Required when delivery_method is set to aws_s3.
		Determines the AWS S3 bucket to which log data will be delivered.
prefix	String	Defines the prefix that identifies a virtual log file storage location and/or a prefix that will be added to each object added to your bucket.

Name	Data Type	Description
region	String	**Note:** Required when delivery_method is set to aws_s3.
		Identifies the region assigned to the AWS S3 bucket defined by the bucket parameter.
		Tip: Use the Get AWS Regions endpoint to retrieve the set of valid values for this parameter.
splunk_enterprise	Object	**Note:** Required when delivery_method is set to splunk_enterprise.
		Contains the configuration for the Splunk Enterprise log delivery method.
url	String	**Note:** Required when delivery_method is set to splunk_enterprise.
		Defines a URL that points to your Splunk Enterprise's HTTP Event Collector configuration.
		Default URL syntax:
		https://{Splunk-Enterprise-Hostname}:{port}/services/collector/raw
token	String	**Note:** Required when delivery_method is set to splunk_enterprise.
		Defines the token corresponding to the HTTP Event Collector configuration associated with the URL defined by the url parameter.
sumo_logic	Object	**Note:** Required when delivery_method is set to sumo_logic.
		Contains the configuration for the Sumo Logic log delivery method.

Name	Data Type	Description
url	String	**Note:** Required when delivery_method is set to sumo_logic.
		Defines a URL that points to the HTTP source defined within Sumo Logic.
azure_blob_storage	Object	**Note:** Required when delivery_method is set to azure_blob_storage.
		Contains the configuration for the Azure Blob Storage log delivery method.
url	String	**Note:** Required when delivery_method is set to azure_blob_storage.
		Defines a URL that points to the Blob container to which log data will be posted.
prefix	String	Defines a virtual log file storage location and/or a prefix that will be added to each log file added to your container.
access_type	String	**Note:** Required when delivery_method is set to azure_blob_storage.
		Determines whether log data uploads will be authorized via a SAS token or an access key
		Tip: Use the Get Access Types (Azure Blob Storage) endpoint to retrieve the set of valid values for this parameter.
access_key	String	**Note:** Required when access_type is set to access_key.
		Defines the access key through which log data uploads will be authorized.
token	String	**Note:** Required when access_type is set to sas_token.
		Defines the SAS token through which log data uploads will be authorized.

Name	Data Type	Description
datadog	Object	**Note:** Required when delivery_method is set to datadog. Contains the profile for the Datadog log delivery method.
site	String	**Note:** Required when delivery_method is set to datadog. Defines the Datadog site to which log data will be delivered. Valid values are: US | EU
api_key	String	**Note:** Required when delivery_method is set to datadog. Defines the API key through which log data uploads will be authorized.
service_attribute_value	String	**Note:** Required when delivery_method is set to datadog. Defines a value through which uploaded log data will be identified within the Datadog environment.
gcs	Object	**Note:** Required when delivery_method is set to gcs. Contains the configuration for the Google Cloud Storage log delivery method.
bucket	String	**Note:** Required when delivery_method is set to gcs. Determines the Google Cloud Storage bucket to which log data will be delivered.
prefix	String	Defines the prefix that identifies a virtual log file storage location and/or a prefix that will be added to each object added to your bucket.

Name	Data Type	Description
new_relic	Object	**Note:** Required when delivery_method is set to new_relic. Contains the configuration for the New Relic log delivery method.
account_id	String	**Note:** Required when delivery_method is set to new_relic. Identifies the system-defined ID for the New Relic account to which log data will be uploaded.
event_type	String	**Note:** Required when delivery_method is set to new_relic. Defines the label that identifies log data delivered to New Relic as a result of this profile. Specify a label that solely consists of alphanumeric characters, underscores, and colons.
insert_key	String	**Note:** Required when delivery_method is set to new_relic. Defines the Inserts insight API key through which log data uploads will be authorized.

Response

The response to the above request includes an HTTP status code, response headers, and a response body.

Status Code

A status code indicates whether the request was successfully performed. A list of common status codes is provided in the **Status Codes and Error Messages** topic.

Response Headers

The response for this endpoint only returns standard HTTP response headers including those described in the **Response Headers** section of the **Request and Response Elements** topic.

Response Body

The response body for a successful request contains the following response elements:

Name	Data Type	Description
@id	String	Indicates the relative path to the requested endpoint.
@type	String	Returns RtldSetting.
id	Integer	Indicates the system-defined ID for your RTLD CDN profile.
account_number	String	Indicates your customer account number.
profile_name	String	Indicates the log delivery profile's name.
description	String	Indicates the log delivery profile's description.
log_format	String	Indicates the format for log data. **Note:** A null value indicates that a default log format will be used.
enabled	Boolean	Indicates whether the RTLD CDN profile is enabled. Valid values are: true | false
custom_cookies	Array of string values	Indicates each cookie that will be logged for each request.
custom_request_headers	Array of string values	Indicates each request header that will be logged for each request.
custom_response_headers	Array of string values	Indicates each response header that will be logged for each request.
delivery_method	String	Indicates the destination to which log data will be delivered.
fields	Array	Indicates the set of log fields that will be delivered.
downsampling_rate	Decimal	Indicates the rate at which log data will be downsampled. A null value indicates that log data will not be downsampled.
platforms	Array	Indicates the set of platforms to which this RTLD CDN profile will be applied.
filters	Object	Contains your log data filtering configuration.
status_codes	Array	Indicates the set of HTTP status codes by which log data will be filtered. A null value indicates that log data will not be filtered by HTTP status codes.

Name	Data Type	Description
cnames	Array	Indicates the set of edge CNAMEs by which log data will be filtered. A null value indicates that log data will not be filtered by edge CNAMEs.
cnames_condition	String	Indicates how log data will be filtered by edge CNAME(s). Valid values are: • **in:** Filters log data to only include requests that point to the edge CNAMEs defined within the cnames property. • **not_in:** Filters log data to exclude requests that point to the edge CNAMEs defined within the cnames property.
user_agent_regexp	String	Indicates the set of user agents by which log data will be filtered through a RE2-compatible regular expression pattern.
http_post	Object	Contains the configuration for the HTTP POST log delivery method.
authentication_type	String	Indicates how log delivery requests will be authenticated to your web servers.
destination_endpoint	String	Indicates the absolute URL to which log data will be delivered.
token	String	Indicates the token value that will be passed via the Authorization request header whenever log data is delivered to your web servers.
username	String	Indicates the user name through which requests to your web server will be authenticated.
password	String	Indicates the encrypted value of the password through which requests to your web server will be authenticated.
masked_password	String	Indicates a masked value that represents the password defined within the password element.
masked_token	String	Indicates a masked value that represents the token defined within the token element.
aws_s3	Object	Contains the configuration for the AWS S3 log delivery method.
bucket	String	Indicates the AWS S3 bucket to which log data will be delivered.
prefix	String	Indicates the prefix that identifies a virtual log file storage location and/or a prefix that will be added to each object added to your bucket.

Name	Data Type	Description
region	String	Indicates the region assigned to the AWS S3 bucket defined by the bucket parameter.
splunk_enterprise	Object	Contains the configuration for the Splunk Enterprise log delivery method.
url	String	Indicates a URL that points to your Splunk Enterprise's HTTP Event Collector configuration.
token	String	Indicates the token corresponding to the HTTP Event Collector configuration associated with the URL defined by the url parameter.
sumo_logic	Object	Contains the configuration for the Sumo Logic log delivery method.
url	String	Indicates a URL that points to the HTTP source defined within Sumo Logic.
masked_url	String	Indicates a masked value that represents the URL defined within the url element.
azure_blob_storage	Object	Contains the configuration for the Azure Blob Storage log delivery method.
url	String	Indicates a URL that points to the Blob container to which log data will be posted.
prefix	String	Indicates a virtual log file storage location and/or a prefix that will be added to each log file added to your container.
access_type	String	Indicates whether log data uploads will be authorized via a SAS token or an access key.
access_key	String	Indicates the access key through which log data uploads will be authorized.
token	String	Indicates the SAS token through which log data uploads will be authorized.
masked_access_key	String	Indicates a masked value that represents the access key defined within the access_key element.
masked_token	String	Indicates a masked value that represents the SAS token defined within the token element.
datadog	Object	Contains the profile for the Datadog log delivery method.
site	String	Indicates the Datadog site to which log data will be delivered. Valid values are: US | EU

Name	Data Type	Description
api_key	String	Indicates the API key through which log data uploads will be authorized.
service_attribute_value	String	Indicates a value through which uploaded log data will be identified within the Datadog environment.
masked_api_key	String	Indicates a masked value that represents the API key defined within the api_key element.
gcs	Object	Contains the configuration for the Google Cloud Storage log delivery method.
bucket	String	Indicates the Google Cloud Storage bucket to which log data will be delivered.
prefix	String	Indicates the prefix that identifies a virtual log file storage location and/or a prefix that will be added to each object added to your bucket.
new_relic	Object	Contains the configuration for the New Relic log delivery method.
account_id	String	Indicates the system-defined ID for the New Relic account to which log data will be uploaded.
event_type	String	Indicates the label that identifies log data delivered to New Relic as a result of this profile.
insert_key	String	Indicates the Inserts insight API key through which log data uploads will be authorized.
masked_insert_key	String	Indicates a masked value that represents the Inserts insight API key defined within the insert_key element.

Errors

The response body for an unsuccessful request may contain an error element that provides additional information. For a list of common error messages, please refer to the **Status Codes and Error Messages** topic.

Sample Request and Response

A sample JSON request is provided below.

```
PUT https://api.edgecast.com/v2/mcc/customers/0001/rtld/settings/20 HTTP/1.1

Authorization: TOK:12345678-1234-1234-1234-1234567890ab

Accept: application/json

Content-Type: application/json

Host: api.edgecast.com

Content-Length: 848

{

        "@id": "/v2/mcc/customers/0001/rtld/settings/20",

        "@type": "RtldSetting",

        "delivery_method": "http_post",

        "enabled": true,

        "downsampling_rate": null,

        "fields": ["user_agent", "rewritten_path", "path", "timestamp", "client_ip",
        "client_ip_version", "status_code", "cache_status", "bytes_out",
        "write_time", "file_size", "server_ip", "server_port", "method", "host",
        "query", "auth_user", "read_time", "bytes_in", "referer"],

        "platforms": ["adn"],

        "filters": {

                "status_codes": null,

                "cnames": null

        },

        "aws_s3": null,

        "http_post": {

                "destination_endpoint": "https://logs.example.com/cdn/",

                "authentication_type": "none",

                "token": null,

                "username": null,

                "password": null

        },

        "sumo_logic": null,

        "splunk_enterprise": null,

        "azure_blob_storage": null

}
```

A sample JSON response is provided below.

```
HTTP/1.1 200 OK
Cache-Control: private
Content-Type: application/xml; charset=utf-8
Date: Thu, 14 Apr 2016 12:00:00 GMT
Content-Length: 1013

{
        "@id": "/v2/mcc/customers/0001/rtld/settings/20",
        "@type": "RtldSetting",
        …
        "platforms": ["adn"],
        "filters": {
                "status_codes": null,
                "cnames": null
        },
        "aws_s3": null,
        "http_post": {
                "destination_endpoint": "https://logs.example.com/cdn/",
                "authentication_type": "none",
                "token": null,
                "username": null,
                "password": null
        }
}
```

RTLD WAF

Use these endpoints, which leverage OAuth 2.0 for authentication, to automate the administration of RTLD WAF.

Add RTLD WAF Profile

Creates a RTLD WAF profile.

Request

Create a RTLD WAF profile via the following request:

HTTP Method	Request URI
POST	https://api.vdms.io/rtld/v1/waf/profiles

Request Headers

This endpoint only takes advantage of common request headers.

Important: Unlike requests to api.edgecast.com, requests to our API gateway (api.vdms.io) require an access token (OAuth).

Request Body

Pass the following request body parameters:

Name	Data Type	Description
aws_s3	Object	**Important:** Required when delivery_method is set to aws_s3. Contains the configuration for the AWS S3 log delivery method.
azure_blob_storage	Object	**Important:** Required when delivery_method is set to azure_blob_storage. Contains the configuration for the Azure Blob Storage log delivery method.
datadog	Object	**Important:** Required when delivery_method is set to datadog. Contains the configuration for the Datadog log delivery method.

Name	Data Type	Description
delivery_method	String	Required. Determines the destination (e.g., aws_s3 or azure_blob_storage) to which log data will be delivered.
		Tip: Use the Get Log Delivery Methods endpoint to retrieve the set of valid values for this parameter.
		Note: You should only configure the delivery method defined by this parameter. For example, if you set this parameter to http_post, you should define the http_post object and then either omit or set the objects for other delivery methods (e.g., aws_s3 or azure_blob_storage) to null.
description	String	Defines the log delivery profile's description. Limit this description to 100 characters.
downsampling_rate	Decimal	Determines the rate at which log data will be downsampled.
		Tip: Use the Get Log Downsampling Rates endpoint to retrieve the set of valid values for this parameter.
		Note: RTLD will not downsample log data when this property is set to a null value.
enabled	Boolean	Determines whether RTLD WAF will use this profile to deliver log data. Valid values are: true | false
fields	Array of string values	Required. Defines the set of log fields that will be delivered.
		Tip: Use the Get Log Fields (RTLD WAF) endpoint to retrieve the set of valid values for this parameter.
filters	Object	Contains your log data filtering configuration.
gcs	Object	**Note:** Required when delivery_method is set to gcs.
		Contains the configuration for the Google Cloud Storage log delivery method.
http_post	Object	**Important:** Required when delivery_method is set to http_post.
		Contains the configuration for the HTTP POST log delivery method.

Name	Data Type	Description
log_format	String	Determines the log data's format. Valid values are:json | json_array | json_lines
		Important: This property may only be defined when delivery_method is set to http_post, aws_s3, or azure_blob_storage. **Note:** RTLD uses a default log format when this property is set to a null value.Learn more.
profile_name	String	Determines the log delivery profile's name. Limit this unique name to 36 characters.
splunk_enterprise	Object	**Important:** Required when delivery_method is set to splunk_enterprise. Contains the configuration for the Splunk Enterprise log delivery method.
sumo_logic	Object	**Important:** Required when delivery_method is set to sumo_logic. Contains the configuration for the Sumo Logic log delivery method.

aws_s3 Object

The aws_s3 object describes the AWS S3 log delivery method using the following properties:

Name	Data Type	Description
bucket	String	**Important:** Required when delivery_method is set to aws_s3. Determines the AWS S3 bucket to which log data will be delivered.
prefix	String	Defines the prefix that identifies a virtual log file storage location and/or a prefix that will be added to each object added to your bucket.

Name	Data Type	Description
region	String	**Important:** Required when delivery_method is set to aws_s3.
		Determines the region assigned to the AWS S3 bucket defined by the bucket parameter.
		Tip: Use the Get AWS Regions endpoint to retrieve the set of valid values for this parameter.

azure_blob_storage Object

The azure_blob_storage object describes the Azure Blob Storage log delivery method using the following properties:

Name	Data Type	Description
access_key	String	**Important:** Required when access_type is set to access_key.
		Determines the access key through which log data uploads will be authorized.
access_type	String	**Important:** Required when delivery_method is set to azure_blob_storage.
		Determines whether log data uploads will be authorized via a SAS token or an access key.
		Note: Use the Get Access Types (Azure Blob Storage) endpoint to retrieve the set of valid values for this parameter.
prefix	String	Defines a virtual log file storage location and/or a prefix that will be added to each log file added to your container.
token	String	**Important:** Required when access_type is set to sas_token.
		Defines the SAS token through which log data uploads will be authorized.

Name	Data Type	Description
url	String	**Important:** Required when delivery_method is set to azure_blob_storage. Definea a URL that points to the Blob container to which log data will be posted.

datadog Object

The datadog object describes the Datadog log delivery method using the following properties:

Name	Data Type	Description
api_key	String	**Important:** Required when delivery_method is set to datadog. Defines the API key through which log data uploads will be authorized.
service_attribute_value	String	**Important:** Required when delivery_method is set to datadog. Defines a value through which uploaded log data will be identified within the Datadog environment.
Site	String	**Important:** Required when delivery_method is set to datadog. Determines the Datadog site to which log data will be delivered. Valid values are: US	EU

filters Object

The filters object describes your log filtering configuration using the following properties:

Name	Data Type	Description
acl_config_name	Array of string values	Defines the set of access rules by which log data will be filtered. Identify each desired access rule by its name. A null value indicates that log data will not be filtered by access rule.
cnames	Array of string values	Defines the set of edge CNAMEs by which log data will be filtered. A null value indicates that log data will not be filtered by edge CNAMEs.

Name	Data Type	Description
cnames_condition	String	Defines how log data will be filtered by edge CNAME(s). Valid values are: • **in:** Filters log data to only include requests that point to the edge CNAMEs defined within the cnames property. • **not_in:** Filters log data to exclude requests that point to the edge CNAMEs defined within the cnames property.
country_code	Array of string values	Defines the set of countries (ISO 3166 country codes) by which log data will be filtered. Identify each desired country by its ISO 3166 country code. A null value indicates that log data will not be filtered by country.
country_code_condition	String	Determines how log data will be filtered by country. Valid values are: • **in:** Filters log data to only include requests that originate from the countries defined within the country_code property. • **not_in:** Filters log data to exclude requests that originate from the countries defined within the country_code property.
rules_config_name	Array of string values	Defines the set of custom rules by which log data will be filtered. Identify each desired custom rule by its name. A null value indicates that log data will not be filtered by custom rule.
scope_config_name	Array of string values	Defines the set of security application manager configurations by which log data will be filtered. Identify each desired security application manager configuration by its name. A null value indicates that log data will not be filtered by security application manager configuration.
user_agent_regexp	String	Reserved for future use.
waf_profile_name	Array of string values	Defines the set of managed rules by which log data will be filtered. Identify each desired managed rule by its name. A null value indicates that log data will not be filtered by managed rule.

gcs Object

The gcs object describes the Google Cloud Storage log delivery method using the following properties:

Name	Data Type	Description
bucket	String	**Note:** Required when delivery_method is set to gcs. Determines the Google Cloud Storage bucket to which log data will be delivered.
prefix	String	Defines the prefix that identifies a virtual log file storage location and/or a prefix that will be added to each object added to your bucket.

http_post Object

The http_post object describes the HTTP POST log delivery method using the following properties:

Name	Data Type	Description
authentication_type	String	**Important:** Required when delivery_method is set to http_post. Determines how log delivery requests will be authenticated to your web servers. **Tip:** Use the Get HTTP POST Authentication Methods endpoint to retrieve the set of valid values for this parameter.
destination_endpoint	String	**Important:** Required when delivery_method is set to http_post. Defines the absolute URL to which log data will be delivered. **Sample value:** https://logs.example.com/cdn/

Name	Data Type	Description
password	String	**Important:** Required when authentication_type is set to http_basic.
		Defines the encrypted value of the password through which requests to your web server will be authenticated.
		Note: Base-64 encoding will applied to the specified credentials. After which, the encoded value will be passed via the Authorization header.
token	String	**Important:** Required when authentication_type is set to custom_authentication.
		Defines the token value that will be passed via the Authorization request header whenever log data is delivered to your web servers.
username	String	**Important:** Required when authentication_type is set to http_basic.
		Determines the user name through which requests to your web server will be authenticated.

splunk_enterprise Object

The splunk_enterprise object describes the Splunk Enterprise log delivery method using the following properties:

Name	Data Type	Description
token	String	**Important:** Required when delivery_method is set to splunk_enterprise.
		Defines the token for the HTTP Event Collector configuration associated with the URL corresponding to the url parameter.

Name	Data Type	Description
url	String	**Important:** Required when delivery_method is set to splunk_enterprise.
		Defines a URL that points to your Splunk Enterprise's HTTP Event Collector configuration.
		Default URL syntax:
		https://*{Splunk-Enterprise-Hostname}*:*{port}*/services/collector/raw

sumo_logic Object

The sumo_logic object describes the Sumo Logic log delivery method using the following properties:

Name	Data Type	Description
url	String	**Important:** Required when delivery_method is set to sumo_logic.
		Defines a URL that points to the HTTP source defined within Sumo Logic.

Response

The response to the above request includes an HTTP status code, response headers, and a response body.

Status Code

A status code indicates whether the request was successfully performed.

Response Headers

The response for this endpoint only includes standard HTTP response headers.

Response Body

The response body for a successful request contains the following response elements:

Name	Data Type	Description
@id	String	Indicates the relative path to an endpoint that returns a RTLD WAF profile.
@type	String	Returns RtldSetting.
account_number	String	Indicates your customer account number.
aws_s3	Object	Contains the configuration for the AWS S3 log delivery method.

Name	Data Type	Description
azure_blob_storage	Object	Contains the configuration for the Azure Blob Storage log delivery method.
created_by	String	Reserved for future use.
created_on	String	Indicates the timestamp at which this profile was created. **Syntax:** YYYY-MM-DDThh:mm:ss.ffffffZ
datadog	Object	Contains the configuration for the Datadog log delivery method.
delivery_method	String	Indicates the destination (e.g., aws_s3 or azure_blob_storage) to which log data will be delivered.
description	String	Indicates the log delivery profile's description.
downsampling_rate	Decimal	Indicates the rate at which log data will be downsampled. **Note:** RTLD will not downsample log data when this property is set to a null value.
enabled	Boolean	Indicates whether RTLD WAF will use this profile to deliver log data.
fields	Array of string values	Indicates the set of log fields that will be delivered.
filters	Object	Contains your log data filtering configuration.
gcs	Object	Contains the configuration for the Google Cloud Storage log delivery method.
http_post	Object	Contains the configuration for the HTTP POST log delivery method.
id	Integer	Indicates the system-defined ID for a RTLD WAF profile.
last_modified_on	String	Indicates the timestamp at which this profile was last modified. **Syntax:** YYYY-MM-DDThh:mm:ss.ffffffZ
log_format	String	Indicates the log data's format. Valid values are:json | json_array | json_lines **Note:** RTLD uses a default log format when this property is set to a null value.Learn more.
profile_name	String	Indicates the log delivery profile's name.

Name	Data Type	Description
splunk_enterprise	Object	Contains the configuration for the Splunk Enterprise log delivery method.
sumo_logic	Object	Contains the configuration for the Sumo Logic log delivery method.

aws_s3 Object

The aws_s3 object describes the AWS S3 log delivery method using the following properties:

Name	Data Type	Description
bucket	String	Indicates the AWS S3 bucket to which log data will be delivered.
prefix	String	Indicates the prefix that identifies a virtual log file storage location and/or a prefix that will be added to each object added to your bucket.
region	String	Indicates the region assigned to the AWS S3 bucket defined by the bucket parameter.

azure_blob_storage Object

The azure_blob_storage object describes the Azure Blob Storage log delivery method using the following properties:

Name	Data Type	Description
access_key	String	Indicates the access key through which log data uploads will be authorized.
access_type	String	Indicates whether log data uploads will be authorized via a SAS token or an access key.
masked_access_key	String	Indicates a masked value that represents the access key defined within the access_key element.
masked_token	String	Indicates a masked value that represents the SAS token defined within the token element.
prefix	String	Indicates a virtual log file storage location and/or a prefix that will be added to each log file added to your container.
token	String	Indicates the SAS token through which log data uploads will be authorized.
url	String	Definea a URL that points to the Blob container to which log data will be posted.

datadog Object

The datadog object describes the Datadog log delivery method using the following properties:

Name	Data Type	Description
api_key	String	Indicates the API key through which log data uploads will be authorized.
masked_api_key	String	Indicates a masked value that represents the API key defined within the api_key element.
service_attribute_value	String	Indicates a value through which uploaded log data will be identified within the Datadog environment.
Site	String	Indicates the Datadog site to which log data will be delivered. Valid values are: US | EU

filters Object

The filters object describes your log filtering configuration using the following properties:

Name	Data Type	Description
acl_config_name	Array of string values	Indicates the set of access rules by which log data will be filtered. A null value indicates that log data will not be filtered by access rule.
cnames	Array of string values	Indicates the set of edge CNAMEs by which log data will be filtered. A null value indicates that log data will not be filtered by edge CNAMEs.
cnames_condition	String	Indicates how log data will be filtered by edge CNAME(s). Valid values are: • **in:** Filters log data to only include requests that point to the edge CNAMEs defined within the cnames property. • **not_in:** Filters log data to exclude requests that point to the edge CNAMEs defined within the cnames property.
country_code	Array of string values	Indicates the set of countries (ISO 3166 country codes) by which log data will be filtered. A null value indicates that log data will not be filtered by country.

Name	Data Type	Description
country_code_condition	String	Indicates how log data will be filtered by country. Valid values are: • **in:** Filters log data to only include requests that originate from the countries defined within the country_code property. • **not_in:** Filters log data to exclude requests that originate from the countries defined within the country_code property.
rules_config_name	Array of string values	Indicates the set of custom rules by which log data will be filtered. A null value indicates that log data will not be filtered by custom rule.
scope_config_name	Array of string values	Indicates the set of security application manager configurations by which log data will be filtered. A null value indicates that log data will not be filtered by security application manager configuration.
user_agent_regexp	String	Reserved for future use.
waf_profile_name	Array of string values	Indicates the set of managed rules by which log data will be filtered. A null value indicates that log data will not be filtered by managed rule.

gcs Object

The gcs object describes the Google Cloud Storage log delivery method using the following properties:

Name	Data Type	Description
bucket	String	Indicates the Google Cloud Storage bucket to which log data will be delivered.
prefix	String	Indicates the prefix that identifies a virtual log file storage location and/or a prefix that will be added to each object added to your bucket.

http_post Object

The http_post object describes the HTTP POST log delivery method using the following properties:

Name	Data Type	Description
authentication_type	String	Indicates how log delivery requests will be authenticated to your web servers.

Name	Data Type	Description
destination_endpoint	String	Indicates the absolute URL to which log data will be delivered. **Sample value:** https://logs.example.com/cdn/
masked_password	String	Indicates a masked value that represents the password defined within the password element.
masked_token	String	Indicates a masked value that represents the token defined within the token element.
password	String	Indicates the encrypted value of the password through which requests to your web server will be authenticated.
token	String	Indicates the token value that will be passed via the Authorization request header whenever log data is delivered to your web servers.
username	String	Indicates the user name through which requests to your web server will be authenticated.

splunk_enterprise Object

The splunk_enterprise object describes the Splunk Enterprise log delivery method using the following properties:

Name	Data Type	Description
masked_token	String	Indicates a masked value that represents the token defined within the token element.
token	String	Indicates the token for the HTTP Event Collector configuration associated with the URL corresponding to the url parameter.
url	String	Indicates a URL that points to your Splunk Enterprise's HTTP Event Collector configuration.

sumo_logic Object

The sumo_logic object describes the Sumo Logic log delivery method using the following properties:

Name	Data Type	Description
masked_url	String	Indicates a masked value that represents the URL defined within the url element.
url	String	Indicates a URL that points to the HTTP source defined within Sumo Logic.

Errors

The response body for an unsuccessful request will contain an error response that provides additional information.

Sample Request and Response (JSON)

A sample JSON request is shown below.

```
POST https://api.vdms.io/rtld/v1/waf/profiles HTTP/1.1

Authorization: Bearer A1bcbGciOiJSUzI1NiIsImtpZCI6Ij13N1VGQ01z...

Accept: application/json

Content-Type: application/json

Host: api.vdms.io

Content-Length: 533

{
        "delivery_method": "http_post",

        "profile_name": "My Profile",

        "fields": ["rule_message", "rule_tags", "client_country_code", "client_country",
"client_city", "sub_events_count", "sub_events", "waf_instance_name", "waf_profile_name",
"action_type", "waf_profile_type", "timestamp", "client_ip", "server_port", "url", "host",
"user_agent", "referer", "account_number", "uuid"],

        "http_post": {

                "destination_endpoint": "https://logs.example.com/waf/",

                "authentication_type": "none",

                "token": null,

                "username": null,

                "password": null

        }

}
```

A sample JSON response is shown below.

```
HTTP/1.1 200 OK

Cache-Control: no-cache

Content-Type: application/json; charset=utf-8

Date: Thu, 14 Apr 2016 12:00:00 GMT

Content-Length: 900
```

```json
{
        "@id": "/rtld/v1/waf/profiles/10012",

        "@type": "RtldSetting",

        "id": 10012,

        "account_number": "0001",

        "delivery_method": "http_post",

        "profile_name": "My Profile",

        "enabled": false,

        "downsampling_rate": null,

        "fields": ["rule_message", "rule_tags", "client_country_code", "client_country",
"client_city", "sub_events_count", "sub_events", "waf_instance_name", "waf_profile_name",
"action_type", "waf_profile_type", "timestamp", "client_ip", "server_port", "url", "host",
"user_agent", "referer", "account_number", "uuid"],

        "aws_s3": null,

        "http_post": {

                "destination_endpoint": "https://logs.example.com/waf/",

                "authentication_type": "none",

                "token": null,

                "username": null,

                "password": null

        },

        "sumo_logic": null,

        "splunk_enterprise": null,

        "azure_blob_storage": null

}
```

Delete RTLD WAF Profile

Deletes a RTLD WAF profile.

Request

Delete a specific RTLD WAF profile via the following request:

HTTP Method	Request URI
DELETE	https://api.vdms.io/rtld/v1/waf/profiles/*ProfileID*

Define the following variable when submitting the above request:

Variable	Description
ProfileID	Replace this variable with the system-defined ID assigned to the desired RTLD WAF profile.
	Tip: Use the Get All RTLD WAF Profiles endpoint to find out the system-defined ID assigned to your RTLD WAF profile.

Request Headers

This endpoint only takes advantage of common request headers.

Important: Unlike requests to api.edgecast.com, requests to our API gateway (api.vdms.io) require an access token (OAuth).

Request Body

Request body parameters are not required by this endpoint.

Response

The response to the above request includes an HTTP status code, response headers, and a response body.

Status Code

A status code indicates whether the request was successfully performed.

Response Headers

The response for this endpoint only includes standard HTTP response headers.

Response Body

The response body for a successful request does not contain a response body.

Errors

The response body for an unsuccessful request will contain an error response that provides additional information.

Sample Request and Response (JSON)

A sample JSON request is shown below.

```
DELETE https://api.vdms.io/rtld/v1/waf/profiles/20 HTTP/1.1

Authorization: Bearer A1bcbGciOiJSUzI1NiIsImtpZCI6Ij13N1VGQ01z...

Accept: application/json

Content-Type: application/json

Host: api.vdms.io
```

A sample JSON response is shown below.

```
HTTP/1.1 204 No Content

Cache-Control: no-cache

Content-Type: application/json; charset=utf-8

Date: Thu, 14 Apr 2016 12:00:00 GMT

Content-Length: 0
```

Get All RTLD WAF Profiles

Retrieves all of your RTLD WAF profiles.

Request

Retrieve all RTLD WAF profiles via the following request:

HTTP Method	Request URI
GET	https://api.vdms.io/rtld/v1/waf/profiles

Request Headers

This endpoint only takes advantage of common request headers.

Important: Unlike requests to api.edgecast.com, requests to our API gateway (api.vdms.io) require an access token (OAuth).

Request Body

Request body parameters are not required by this endpoint.

Response

The response to the above request includes an HTTP status code, response headers, and a response body.

Status Code

A status code indicates whether the request was successfully performed.

Response Headers

The response for this endpoint only includes standard HTTP response headers.

Response Body

The response body for a successful request contains the following response elements:

Name	Data Type	Description
@id	String	Indicates the relative path to the requested endpoint.
@type	String	Returns Collection.
items	Array	Contains your RTLD WAF profiles.
total_items	Integer	Indicates the total number of RTLD WAF profiles that were included in the response.

items Array

The items array describes each RTLD WAF profile using the following properties:

Name	Data Type	Description
@id	String	Indicates the relative path to an endpoint that returns a RTLD WAF profile.
@type	String	Returns RtldSetting.
account_number	String	Indicates your customer account number.
aws_s3	Object	Contains the configuration for the AWS S3 log delivery method.
azure_blob_storage	Object	Contains the configuration for the Azure Blob Storage log delivery method.
created_by	String	Reserved for future use.
created_on	String	Indicates the timestamp at which this profile was created. **Syntax:** YYYY-MM-DDThh:mm:ss.ffffffZ
datadog	Object	Contains the configuration for the Datadog log delivery method.
delivery_method	String	Indicates the destination (e.g., aws_s3 or azure_blob_storage) to which log data will be delivered.
description	String	Indicates the log delivery profile's description.

Name	Data Type	Description
downsampling_rate	Decimal	Indicates the rate at which log data will be downsampled. **Note:** RTLD will not downsample log data when this property is set to a null value.
enabled	Boolean	Indicates whether RTLD WAF will use this profile to deliver log data.
fields	Array of string values	Indicates the set of log fields that will be delivered.
filters	Object	Contains your log data filtering profile.
gcs	Object	Contains the configuration for the Google Cloud Storage log delivery method.
http_post	Object	Contains the configuration for the HTTP POST log delivery method.
id	Integer	Indicates the system-defined ID for a RTLD WAF profile.
last_modified_on	String	Indicates the timestamp at which this profile was last modified. **Syntax:** YYYY-MM-DDThh:mm:ss.ffffffZ
log_format	String	Indicates the log data's format. Valid values are:json | json_array | json_lines **Note:** RTLD uses a default log format when this property is set to a null value.Learn more.
profile_name	String	Indicates the log delivery profile's name.
splunk_enterprise	Object	Contains the configuration for the Splunk Enterprise log delivery method.
sumo_logic	Object	Contains the configuration for the Sumo Logic log delivery method.

aws_s3 Object

The aws_s3 object describes the AWS S3 log delivery method using the following properties:

Name	Data Type	Description
bucket	String	Indicates the AWS S3 bucket to which log data will be delivered.

Name	Data Type	Description
prefix	String	Indicates the prefix that identifies a virtual log file storage location and/or a prefix that will be added to each object added to your bucket.
region	String	Indicates the region assigned to the AWS S3 bucket defined by the bucket parameter.

azure_blob_storage Object

The azure_blob_storage object describes the Azure Blob Storage log delivery method using the following properties:

Name	Data Type	Description
access_key	String	Indicates the access key through which log data uploads will be authorized.
access_type	String	Indicates whether log data uploads will be authorized via a SAS token or an access key.
masked_access_key	String	Indicates a masked value that represents the access key defined within the access_key element.
masked_token	String	Indicates a masked value that represents the SAS token defined within the token element.
prefix	String	Indicates a virtual log file storage location and/or a prefix that will be added to each log file added to your container.
token	String	Indicates the SAS token through which log data uploads will be authorized.
url	String	Defines a URL that points to the Blob container to which log data will be posted.

datadog Object

The datadog object describes the Datadog log delivery method using the following properties:

Name	Data Type	Description
api_key	String	Indicates the API key through which log data uploads will be authorized.
masked_api_key	String	Indicates a masked value that represents the API key defined within the api_key element.
service_attribute_value	String	Indicates a value through which uploaded log data will be identified within the Datadog environment.
Site	String	Indicates the Datadog site to which log data will be delivered. Valid values are: US	EU

filters Object

The filters object describes your log filtering configuration using the following properties:

Name	Data Type	Description
acl_config_name	Array of string values	Indicates the set of access rules by which log data will be filtered. A null value indicates that log data will not be filtered by access rule.
cnames	Array of string values	Indicates the set of edge CNAMEs by which log data will be filtered. A null value indicates that log data will not be filtered by edge CNAMEs.
cnames_condition	String	Indicates how log data will be filtered by edge CNAME(s). Valid values are: **in:** Filters log data to only include requests that point to the edge CNAMEs defined within the cnames property. **not_in:** Filters log data to exclude requests that point to the edge CNAMEs defined within the cnames property.
country_code	Array of string values	Indicates the set of countries (ISO 3166 country codes) by which log data will be filtered. A null value indicates that log data will not be filtered by country.
country_code_condition	String	Indicates how log data will be filtered by country. Valid values are: **in:** Filters log data to only include requests that originate from the countries defined within the country_code property. **not_in:** Filters log data to exclude requests that originate from the countries defined within the country_code property.
rules_config_name	Array of string values	Indicates the set of custom rules by which log data will be filtered. A null value indicates that log data will not be filtered by custom rule.
scope_config_name	Array of string values	Indicates the set of security application manager configurations by which log data will be filtered. A null value indicates that log data will not be filtered by security application manager configuration.
user_agent_regexp	String	Reserved for future use.
waf_profile_name	Array of string values	Indicates the set of managed rules by which log data will be filtered. A null value indicates that log data will not be filtered by managed rule.

gcs Object

The gcs object describes the Google Cloud Storage log delivery method using the following properties:

Name	Data Type	Description
bucket	String	Indicates the Google Cloud Storage bucket to which log data will be delivered.
prefix	String	Indicates the prefix that identifies a virtual log file storage location and/or a prefix that will be added to each object added to your bucket.

http_post Object

The http_post object describes the HTTP POST log delivery method using the following properties:

Name	Data Type	Description
authentication_type	String	Indicates how log delivery requests will be authenticated to your web servers.
destination_endpoint	String	Indicates the absolute URL to which log data will be delivered. **Sample value:** https://logs.example.com/cdn/
masked_password	String	Indicates a masked value that represents the password defined within the password element.
masked_token	String	Indicates a masked value that represents the token defined within the token element.
password	String	Indicates the encrypted value of the password through which requests to your web server will be authenticated.
token	String	Indicates the token value that will be passed via the Authorization request header whenever log data is delivered to your web servers.
username	String	Indicates the user name through which requests to your web server will be authenticated.

splunk_enterprise Object

The splunk_enterprise object describes the Splunk Enterprise log delivery method using the following properties:

Name	Data Type	Description
masked_token	String	Indicates a masked value that represents the token defined within the token element.
token	String	Indicates the token for the HTTP Event Collector configuration associated with the URL corresponding to the url parameter.
url	String	Indicates a URL that points to your Splunk Enterprise's HTTP Event Collector configuration.

sumo_logic Object

The sumo_logic object describes the Sumo Logic log delivery method using the following properties:

Name	Data Type	Description
masked_url	String	Indicates a masked value that represents the URL defined within the url element.
url	String	Indicates a URL that points to the HTTP source defined within Sumo Logic.

Errors

The response body for an unsuccessful request will contain an error response that provides additional information.

Sample Request and Response (JSON)

A sample JSON request is shown below.

```
GET https://api.vdms.io/rtld/v1/waf/profiles HTTP/1.1

Authorization: Bearer A1bcbGciOiJSUzI1NiIsImtpZCI6Ij13N1VGQ01z...

Accept: application/json

Content-Type: application/json

Host: api.vdms.io

Content-Length: 533
```

A sample JSON response is shown below.

```
HTTP/1.1 200 OK
Cache-Control: no-cache
Content-Type: application/json; charset=utf-8
Date: Thu, 14 Apr 2016 12:00:00 GMT
Content-Length: 900

{
        "@id": "/rtld/v1/waf/profiles/10012",
        "@type": "RtldSetting",
        "id": 10012,
        "account_number": "0001",
        "delivery_method": "http_post",
        "profile_name": "My Profile",
        "enabled": false,
        "downsampling_rate": null,
        "fields": ["rule_message", "rule_tags", "client_country_code", "client_country",
"client_city", "sub_events_count", "sub_events", "waf_instance_name", "waf_profile_name",
"action_type", "waf_profile_type", "timestamp", "client_ip", "server_port", "url", "host",
"user_agent", "referer", "account_number", "uuid"],
        "aws_s3": null,
        "http_post": {
                "destination_endpoint": "https://logs.example.com/waf/",
                "authentication_type": "none",
                "token": null,
                "username": null,
                "password": null
        },
        "sumo_logic": null,
        "splunk_enterprise": null,
        "azure_blob_storage": null
}
```

Get RTLD WAF Profile

Retrieves a RTLD WAF profile.

Request

Retrieve a specific RTLD WAF profiles via the following request:

HTTP Method	Request URI
GET	https://api.vdms.io/rtld/v1/waf/profiles/*ProfileID*

Define the following variable when submitting the above request:

Variable	Description
ProfileID	Replace this variable with the system-defined ID assigned to the desired RTLD WAF profile.
	Tip: Use the Get All RTLD WAF Profiles endpoint to find out the system-defined ID assigned to your RTLD WAF profile.

Request Headers

This endpoint only takes advantage of common request headers.

Important: Unlike requests to api.edgecast.com, requests to our API gateway (api.vdms.io) require an access token (OAuth).

Request Body

Request body parameters are not required by this endpoint.

Response

The response to the above request includes an HTTP status code, response headers, and a response body.

Status Code

A status code indicates whether the request was successfully performed.

Response Headers

The response for this endpoint only includes standard HTTP response headers.

Response Body

The response body for a successful request contains the following response elements:

Name	Data Type	Description
@id	String	Indicates the relative path to an endpoint that returns a RTLD WAF profile.

Name	Data Type	Description
@type	String	Returns RtldSetting.
account_number	String	Indicates your customer account number.
aws_s3	Object	Contains the configuration for the AWS S3 log delivery method.
azure_blob_storage	Object	Contains the configuration for the Azure Blob Storage log delivery method.
created_by	String	Reserved for future use.
created_on	String	Indicates the timestamp at which this profile was created. **Syntax:** YYYY-MM-DDThh:mm:ss.ffffffZ
datadog	Object	Contains the configuration for the Datadog log delivery method.
delivery_method	String	Indicates the destination (e.g., aws_s3 or azure_blob_storage) to which log data will be delivered.
description	String	Indicates the log delivery profile's description.
downsampling_rate	Decimal	Indicates the rate at which log data will be downsampled. **Note:** RTLD will not downsample log data when this property is set to a null value.
enabled	Boolean	Indicates whether RTLD WAF will use this profile to deliver log data.
fields	Array of string values	Indicates the set of log fields that will be delivered.
filters	Object	Contains your log data filtering profile.
gcs	Object	Contains the configuration for the Google Cloud Storage log delivery method.
http_post	Object	Contains the configuration for the HTTP POST log delivery method.
id	Integer	Indicates the system-defined ID for a RTLD WAF profile.
last_modified_on	String	Indicates the timestamp at which this profile was last modified. **Syntax:** YYYY-MM-DDThh:mm:ss.ffffffZ

Name	Data Type	Description
log_format	String	Indicates the log data's format. Valid values are:json | json_array | json_lines **Note:** RTLD uses a default log format when this property is set to a null value.Learn more.
profile_name	String	Indicates the log delivery profile's name.
splunk_enterprise	Object	Contains the configuration for the Splunk Enterprise log delivery method.
sumo_logic	Object	Contains the configuration for the Sumo Logic log delivery method.

aws_s3 Object

The aws_s3 object describes the AWS S3 log delivery method using the following properties:

Name	Data Type	Description
bucket	String	Indicates the AWS S3 bucket to which log data will be delivered.
prefix	String	Indicates the prefix that identifies a virtual log file storage location and/or a prefix that will be added to each object added to your bucket.
region	String	Indicates the region assigned to the AWS S3 bucket defined by the bucket parameter.

azure_blob_storage Object

The azure_blob_storage object describes the Azure Blob Storage log delivery method using the following properties:

Name	Data Type	Description
access_key	String	Indicates the access key through which log data uploads will be authorized.
access_type	String	Indicates whether log data uploads will be authorized via a SAS token or an access key.
masked_access_key	String	Indicates a masked value that represents the access key defined within the access_key element.
masked_token	String	Indicates a masked value that represents the SAS token defined within the token element.
prefix	String	Indicates a virtual log file storage location and/or a prefix that will be added to each log file added to your container.

Name	Data Type	Description
token	String	Indicates the SAS token through which log data uploads will be authorized.
url	String	Definea a URL that points to the Blob container to which log data will be posted.

datadog Object

The datadog object describes the Datadog log delivery method using the following properties:

Name	Data Type	Description
api_key	String	Indicates the API key through which log data uploads will be authorized.
masked_api_key	String	Indicates a masked value that represents the API key defined within the api_key element.
service_attribute_value	String	Indicates a value through which uploaded log data will be identified within the Datadog environment.
Site	String	Indicates the Datadog site to which log data will be delivered. Valid values are: US | EU

filters Object

The filters object describes your log filtering configuration using the following properties:

Name	Data Type	Description
acl_config_name	Array of string values	Indicates the set of access rules by which log data will be filtered. A null value indicates that log data will not be filtered by access rule.
cnames	Array of string values	Indicates the set of edge CNAMEs by which log data will be filtered. A null value indicates that log data will not be filtered by edge CNAMEs.
cnames_condition	String	Indicates how log data will be filtered by edge CNAME(s). Valid values are: • **in:** Filters log data to only include requests that point to the edge CNAMEs defined within the cnames property. • **not_in:** Filters log data to exclude requests that point to the edge CNAMEs defined within the cnames property.
country_code	Array of string values	Indicates the set of countries (ISO 3166 country codes) by which log data will be filtered. A null value indicates that log data will not be filtered by country.

Name	Data Type	Description
country_code_condition	String	Indicates how log data will be filtered by country. Valid values are: • **in:** Filters log data to only include requests that originate from the countries defined within the country_code property. • **not_in:** Filters log data to exclude requests that originate from the countries defined within the country_code property.
rules_config_name	Array of string values	Indicates the set of custom rules by which log data will be filtered. A null value indicates that log data will not be filtered by custom rule.
scope_config_name	Array of string values	Indicates the set of security application manager configurations by which log data will be filtered. A null value indicates that log data will not be filtered by security application manager configuration.
user_agent_regexp	String	Reserved for future use.
waf_profile_name	Array of string values	Indicates the set of managed rules by which log data will be filtered. A null value indicates that log data will not be filtered by managed rule.

gcs Object

The gcs object describes the Google Cloud Storage log delivery method using the following properties:

Name	Data Type	Description
bucket	String	Indicates the Google Cloud Storage bucket to which log data will be delivered.
prefix	String	Indicates the prefix that identifies a virtual log file storage location and/or a prefix that will be added to each object added to your bucket.

http_post Object

The http_post object describes the HTTP POST log delivery method using the following properties:

Name	Data Type	Description
authentication_type	String	Indicates how log delivery requests will be authenticated to your web servers.

Name	Data Type	Description
destination_endpoint	String	Indicates the absolute URL to which log data will be delivered. **Sample value:** https://logs.example.com/cdn/
masked_password	String	Indicates a masked value that represents the password defined within the password element.
masked_token	String	Indicates a masked value that represents the token defined within the token element.
password	String	Indicates the encrypted value of the password through which requests to your web server will be authenticated.
token	String	Indicates the token value that will be passed via the Authorization request header whenever log data is delivered to your web servers.
username	String	Indicates the user name through which requests to your web server will be authenticated.

splunk_enterprise Object

The splunk_enterprise object describes the Splunk Enterprise log delivery method using the following properties:

Name	Data Type	Description
masked_token	String	Indicates a masked value that represents the token defined within the token element.
token	String	Indicates the token for the HTTP Event Collector configuration associated with the URL corresponding to the url parameter.
url	String	Indicates a URL that points to your Splunk Enterprise's HTTP Event Collector configuration.

sumo_logic Object

The sumo_logic object describes the Sumo Logic log delivery method using the following properties:

Name	Data Type	Description
masked_url	String	Indicates a masked value that represents the URL defined within the url element.
url	String	Indicates a URL that points to the HTTP source defined within Sumo Logic.

Errors

The response body for an unsuccessful request will contain an error response that provides additional information.

Sample Request and Response (JSON)

A sample JSON request is shown below.

GET https://api.vdms.io/rtld/v1/waf/profiles/10012 HTTP/1.1

Authorization: Bearer A1bcbGciOiJSUzI1NiIsImtpZCI6Ij13N1VGQ01z...

Accept: application/json

Content-Type: application/json

Host: api.vdms.io

Content-Length: 533

A sample JSON response is shown below.

HTTP/1.1 200 OK

Cache-Control: no-cache

Content-Type: application/json; charset=utf-8

Date: Thu, 14 Apr 2016 12:00:00 GMT

Content-Length: 900

{

    "@id": "/rtld/v1/waf/profiles/10012",

    "@type": "RtldSetting",

    "id": 10012,

    "account_number": "0001",

    "delivery_method": "http_post",

    "profile_name": "My Profile",

    "enabled": false,

    "downsampling_rate": null,

    "fields": ["rule_message", "rule_tags", "client_country_code", "client_country", "client_city", "sub_events_count", "sub_events", "waf_instance_name", "waf_profile_name", "action_type", "waf_profile_type", "timestamp", "client_ip", "server_port", "url", "host", "user_agent", "referer", "account_number", "uuid"],

    "aws_s3": null,

    "http_post": {

```
                    "destination_endpoint": "https://logs.example.com/waf/",

                    "authentication_type": "none",

                    "token": null,

                    "username": null,

                    "password": null

              },

              "sumo_logic": null,

              "splunk_enterprise": null,

              "azure_blob_storage": null

        }
```

Update RTLD WAF Profile

Updates a RTLD WAF profile.

Request

Update a specific RTLD WAF profile via the following request:

HTTP Method	Request URI
PUT	https://api.vdms.io/rtld/v1/waf/profiles/*ProfileID*

Define the following variable when submitting the above request:

Variable	Description
ProfileID	Replace this variable with the system-defined ID assigned to the desired RTLD WAF profile.
	Tip: Use the Get All RTLD WAF Profiles endpoint to find out the system-defined ID assigned to your RTLD WAF profile.

Request Headers

This endpoint only takes advantage of common request headers.

Important: Unlike requests to api.edgecast.com, requests to our API gateway (api.vdms.io) require an access token (OAuth).

Request Body

Pass the following request body parameters:

Name	Data Type	Description
aws_s3	Object	**Important:** Required when delivery_method is set to aws_s3. Contains the configuration for the AWS S3 log delivery method.
azure_blob_storage	Object	**Important:** Required when delivery_method is set to azure_blob_storage. Contains the configuration for the Azure Blob Storage log delivery method.
datadog	Object	**Important:** Required when delivery_method is set to datadog. Contains the configuration for the Datadog log delivery method.
delivery_method	String	Required. Determines the destination (e.g., aws_s3 or azure_blob_storage) to which log data will be delivered. **Tip:** Use the Get Log Delivery Methods endpoint to retrieve the set of valid values for this parameter. **Note:** You should only configure the delivery method defined by this parameter. For example, if you set this parameter to http_post, you should define the http_post object and then either omit or set the objects for other delivery methods (e.g., aws_s3 or azure_blob_storage) to null.
description	String	Defines the log delivery profile's description. Limit this description to 100 characters.
downsampling_rate	Decimal	Determines the rate at which log data will be downsampled. **Tip:** Use the Get Log Downsampling Rates endpoint to retrieve the set of valid values for this parameter. **Note:** RTLD will not downsample log data when this property is set to a null value.
enabled	Boolean	Determines whether RTLD WAF will use this profile to deliver log data. Valid values are: true | false

Name	Data Type	Description
fields	Array of string values	Required. Defines the set of log fields that will be delivered. **Tip:** Use the Get Log Fields (RTLD WAF) endpoint to retrieve the set of valid values for this parameter.
filters	Object	Contains your log data filtering configuration.
gcs	Object	**Note:** Required when delivery_method is set to gcs. Contains the configuration for the Google Cloud Storage log delivery method.
http_post	Object	**Important:** Required when delivery_method is set to http_post. Contains the configuration for the HTTP POST log delivery method.
log_format	String	Determines the log data's format. Valid values are:json | json_array | json_lines **Important:** This property may only be defined when delivery_method is set to http_post, aws_s3, or azure_blob_storage. **Note:** RTLD uses a default log format when this property is set to a null value.Learn more.
profile_name	String	Determines the log delivery profile's name. Limit this unique name to 36 characters.
splunk_enterprise	Object	**Important:** Required when delivery_method is set to splunk_enterprise. Contains the configuration for the Splunk Enterprise log delivery method.
sumo_logic	Object	**Important:** Required when delivery_method is set to sumo_logic. Contains the configuration for the Sumo Logic log delivery method.

aws_s3 Object

The aws_s3 object describes the AWS S3 log delivery method using the following properties:

Name	Data Type	Description
bucket	String	**Important:** Required when delivery_method is set to aws_s3.
		Determines the AWS S3 bucket to which log data will be delivered.
prefix	String	Defines the prefix that identifies a virtual log file storage location and/or a prefix that will be added to each object added to your bucket.
region	String	**Important:** Required when delivery_method is set to aws_s3.
		Determines the region assigned to the AWS S3 bucket defined by the bucket parameter.
		Tip: Use the Get AWS Regions endpoint to retrieve the set of valid values for this parameter.

azure_blob_storage Object

The azure_blob_storage object describes the Azure Blob Storage log delivery method using the following properties:

Name	Data Type	Description
access_key	String	**Important:** Required when access_type is set to access_key.
		Determines the access key through which log data uploads will be authorized.
access_type	String	**Important:** Required when delivery_method is set to azure_blob_storage.
		Determines whether log data uploads will be authorized via a SAS token or an access key.
		Note: Use the Get Access Types (Azure Blob Storage) endpoint to retrieve the set of valid values for this parameter.

Name	Data Type	Description
prefix	String	Defines a virtual log file storage location and/or a prefix that will be added to each log file added to your container.
token	String	**Important:** Required when access_type is set to sas_token. Defines the SAS token through which log data uploads will be authorized.
url	String	**Important:** Required when delivery_method is set to azure_blob_storage. Definea a URL that points to the Blob container to which log data will be posted.

datadog Object

The datadog object describes the Datadog log delivery method using the following properties:

Name	Data Type	Description
api_key	String	**Important:** Required when delivery_method is set to datadog. Defines the API key through which log data uploads will be authorized.
service_attribute_value	String	**Important:** Required when delivery_method is set to datadog. Defines a value through which uploaded log data will be identified within the Datadog environment.
Site	String	**Important:** Required when delivery_method is set to datadog. Determines the Datadog site to which log data will be delivered. Valid values are: US	EU

The filters object describes your log filtering configuration using the following properties:

Name	Data Type	Description
acl_config_name	Array of string values	Defines the set of access rules by which log data will be filtered. Identify each desired access rule by its name. A null value indicates that log data will not be filtered by access rule.
cnames	Array of string values	Defines the set of edge CNAMEs by which log data will be filtered. A null value indicates that log data will not be filtered by edge CNAMEs.
cnames_condition	String	Defines how log data will be filtered by edge CNAME(s). Valid values are: • **in:** Filters log data to only include requests that point to the edge CNAMEs defined within the cnames property. • **not_in:** Filters log data to exclude requests that point to the edge CNAMEs defined within the cnames property.
country_code	Array of string values	Defines the set of countries (ISO 3166 country codes) by which log data will be filtered. Identify each desired country by its ISO 3166 country code. A null value indicates that log data will not be filtered by country.
country_code_condition	String	Determines how log data will be filtered by country. Valid values are: • **in:** Filters log data to only include requests that originate from the countries defined within the country_code property. • **not_in:** Filters log data to exclude requests that originate from the countries defined within the country_code property.
rules_config_name	Array of string values	Defines the set of custom rules by which log data will be filtered. Identify each desired custom rule by its name. A null value indicates that log data will not be filtered by custom rule.
scope_config_name	Array of string values	Defines the set of security application manager configurations by which log data will be filtered. Identify each desired security application manager configuration by its name. A null value indicates that log data will not be filtered by security application manager configuration.

Name	Data Type	Description
user_agent_regexp	String	Reserved for future use.
waf_profile_name	Array of string values	Defines the set of managed rules by which log data will be filtered. Identify each desired managed rule by its name. A null value indicates that log data will not be filtered by managed rule.

gcs Object

The gcs object describes the Google Cloud Storage log delivery method using the following properties:

Name	Data Type	Description
bucket	String	**Note:** Required when delivery_method is set to gcs. Determines the Google Cloud Storage bucket to which log data will be delivered.
prefix	String	Defines the prefix that identifies a virtual log file storage location and/or a prefix that will be added to each object added to your bucket.

http_post Object

The http_post object describes the HTTP POST log delivery method using the following properties:

Name	Data Type	Description
authentication_type	String	**Important:** Required when delivery_method is set to http_post. Determines how log delivery requests will be authenticated to your web servers. **Tip:** Use the Get HTTP POST Authentication Methods endpoint to retrieve the set of valid values for this parameter.
destination_endpoint	String	**Important:** Required when delivery_method is set to http_post. Defines the absolute URL to which log data will be delivered. **Sample value:** https://logs.example.com/cdn/

Name	Data Type	Description
password	String	**Important:** Required when authentication_type is set to http_basic.
		Defines the encrypted value of the password through which requests to your web server will be authenticated.
		Note: Base-64 encoding will applied to the specified credentials. After which, the encoded value will be passed via the Authorization header.
token	String	**Important:** Required when authentication_type is set to custom_authentication.
		Defines the token value that will be passed via the Authorization request header whenever log data is delivered to your web servers.
username	String	**Important:** Required when authentication_type is set to http_basic.
		Determines the user name through which requests to your web server will be authenticated.

splunk_enterprise Object

The splunk_enterprise object describes the Splunk Enterprise log delivery method using the following properties:

Name	Data Type	Description
token	String	**Important:** Required when delivery_method is set to splunk_enterprise.
		Defines the token for the HTTP Event Collector configuration associated with the URL corresponding to the url parameter.

Name	Data Type	Description
url	String	**Important:** Required when delivery_method is set to splunk_enterprise. Defines a URL that points to your Splunk Enterprise's HTTP Event Collector configuration. **Default URL syntax:** https://*{Splunk-Enterprise-Hostname}*:*{port}*/services/collector/raw

sumo_logic Object

The sumo_logic object describes the Sumo Logic log delivery method using the following properties:

Name	Data Type	Description
url	String	**Important:** Required when delivery_method is set to sumo_logic. Defines a URL that points to the HTTP source defined within Sumo Logic.

Response

The response to the above request includes an HTTP status code, response headers, and a response body.

Status Code

A status code indicates whether the request was successfully performed.

Response Headers

The response for this endpoint only includes standard HTTP response headers.

Response Body

The response body for a successful request contains the following response elements:

Name	Data Type	Description
@id	String	Indicates the relative path to an endpoint that returns a RTLD WAF profile.
@type	String	Returns RtldSetting.
account_number	String	Indicates your customer account number.
aws_s3	Object	Contains the configuration for the AWS S3 log delivery method.

Name	Data Type	Description
azure_blob_storage	Object	Contains the configuration for the Azure Blob Storage log delivery method.
created_by	String	Reserved for future use.
created_on	String	Indicates the timestamp at which this profile was created. **Syntax:** YYYY-MM-DDThh:mm:ss.ffffffZ
datadog	Object	Contains the configuration for the Datadog log delivery method.
delivery_method	String	Indicates the destination (e.g., aws_s3 or azure_blob_storage) to which log data will be delivered.
description	String	Indicates the log delivery profile's description.
downsampling_rate	Decimal	Indicates the rate at which log data will be downsampled. **Note:** RTLD will not downsample log data when this property is set to a null value.
enabled	Boolean	Indicates whether RTLD WAF will use this profile to deliver log data.
fields	Array of string values	Indicates the set of log fields that will be delivered.
filters	Object	Contains your log data filtering profile.
gcs	Object	Contains the configuration for the Google Cloud Storage log delivery method.
http_post	Object	Contains the configuration for the HTTP POST log delivery method.
id	Integer	Indicates the system-defined ID for a RTLD WAF profile.
last_modified_on	String	Indicates the timestamp at which this profile was last modified. **Syntax:** YYYY-MM-DDThh:mm:ss.ffffffZ
log_format	String	Indicates the log data's format. Valid values are:json | json_array | json_lines **Note:** RTLD uses a default log format when this property is set to a null value.Learn more.
profile_name	String	Indicates the log delivery profile's name.

Name	Data Type	Description
splunk_enterprise	Object	Contains the configuration for the Splunk Enterprise log delivery method.
sumo_logic	Object	Contains the configuration for the Sumo Logic log delivery method.

aws_s3 Object

The aws_s3 object describes the AWS S3 log delivery method using the following properties:

Name	Data Type	Description
bucket	String	Indicates the AWS S3 bucket to which log data will be delivered.
prefix	String	Indicates the prefix that identifies a virtual log file storage location and/or a prefix that will be added to each object added to your bucket.
region	String	Indicates the region assigned to the AWS S3 bucket defined by the bucket parameter.

azure_blob_storage Object

The azure_blob_storage object describes the Azure Blob Storage log delivery method using the following properties:

Name	Data Type	Description
access_key	String	Indicates the access key through which log data uploads will be authorized.
access_type	String	Indicates whether log data uploads will be authorized via a SAS token or an access key.
masked_access_key	String	Indicates a masked value that represents the access key defined within the access_key element.
masked_token	String	Indicates a masked value that represents the SAS token defined within the token element.
prefix	String	Indicates a virtual log file storage location and/or a prefix that will be added to each log file added to your container.
token	String	Indicates the SAS token through which log data uploads will be authorized.
url	String	Definea a URL that points to the Blob container to which log data will be posted.

datadog Object

The datadog object describes the Datadog log delivery method using the following properties:

Name	Data Type	Description
api_key	String	Indicates the API key through which log data uploads will be authorized.
masked_api_key	String	Indicates a masked value that represents the API key defined within the api_key element.
service_attribute_value	String	Indicates a value through which uploaded log data will be identified within the Datadog environment.
Site	String	Indicates the Datadog site to which log data will be delivered. Valid values are: US | EU

filters Object

The filters object describes your log filtering configuration using the following properties:

Name	Data Type	Description
acl_config_name	Array of string values	Indicates the set of access rules by which log data will be filtered. A null value indicates that log data will not be filtered by access rule.
cnames	Array of string values	Indicates the set of edge CNAMEs by which log data will be filtered. A null value indicates that log data will not be filtered by edge CNAMEs.
cnames_condition	String	Indicates how log data will be filtered by edge CNAME(s). Valid values are: • **in:** Filters log data to only include requests that point to the edge CNAMEs defined within the cnames property. • **not_in:** Filters log data to exclude requests that point to the edge CNAMEs defined within the cnames property.
country_code	Array of string values	Indicates the set of countries (ISO 3166 country codes) by which log data will be filtered. A null value indicates that log data will not be filtered by country.

Name	Data Type	Description
country_code_condition	String	Indicates how log data will be filtered by country. Valid values are: • **in:** Filters log data to only include requests that originate from the countries defined within the country_code property. • **not_in:** Filters log data to exclude requests that originate from the countries defined within the country_code property.
rules_config_name	Array of string values	Indicates the set of custom rules by which log data will be filtered. A null value indicates that log data will not be filtered by custom rule.
scope_config_name	Array of string values	Indicates the set of security application manager configurations by which log data will be filtered. A null value indicates that log data will not be filtered by security application manager configuration.
user_agent_regexp	String	Reserved for future use.
waf_profile_name	Array of string values	Indicates the set of managed rules by which log data will be filtered. A null value indicates that log data will not be filtered by managed rule.

gcs Object

The gcs object describes the Google Cloud Storage log delivery method using the following properties:

Name	Data Type	Description
bucket	String	Indicates the Google Cloud Storage bucket to which log data will be delivered.
prefix	String	Indicates the prefix that identifies a virtual log file storage location and/or a prefix that will be added to each object added to your bucket.

http_post Object

The http_post object describes the HTTP POST log delivery method using the following properties:

Name	Data Type	Description
authentication_type	String	Indicates how log delivery requests will be authenticated to your web servers.

Name	Data Type	Description
destination_endpoint	String	Indicates the absolute URL to which log data will be delivered. **Sample value:** https://logs.example.com/cdn/
masked_password	String	Indicates a masked value that represents the password defined within the password element.
masked_token	String	Indicates a masked value that represents the token defined within the token element.
password	String	Indicates the encrypted value of the password through which requests to your web server will be authenticated.
token	String	Indicates the token value that will be passed via the Authorization request header whenever log data is delivered to your web servers.
username	String	Indicates the user name through which requests to your web server will be authenticated.

splunk_enterprise Object

The splunk_enterprise object describes the Splunk Enterprise log delivery method using the following properties:

Name	Data Type	Description
masked_token	String	Indicates a masked value that represents the token defined within the token element.
token	String	Indicates the token for the HTTP Event Collector configuration associated with the URL corresponding to the url parameter.
url	String	Indicates a URL that points to your Splunk Enterprise's HTTP Event Collector configuration.

sumo_logic Object

The sumo_logic object describes the Sumo Logic log delivery method using the following properties:

Name	Data Type	Description
masked_url	String	Indicates a masked value that represents the URL defined within the url element.
url	String	Indicates a URL that points to the HTTP source defined within Sumo Logic.

Errors

The response body for an unsuccessful request will contain an error response that provides additional information.

Sample Request and Response (JSON)

A sample JSON request is shown below.

```
PUT https://api.vdms.io/rtld/v1/waf/profiles/10011 HTTP/1.1

Authorization: Bearer A1bcbGciOiJSUzI1NiIsImtpZCI6Ij13N1VGQ01z...

Accept: application/json

Content-Type: application/json

Host: api.vdms.io

Content-Length: 533

{
        "delivery_method": "http_post",

        "profile_name": "My Profile",

        "fields": ["rule_message", "rule_tags", "client_country_code", "client_country",
"client_city", "sub_events_count", "sub_events", "waf_instance_name", "waf_profile_name",
"action_type", "waf_profile_type", "timestamp", "client_ip", "server_port", "url", "host",
"user_agent", "referer", "account_number", "uuid"],

        "http_post": {

                "destination_endpoint": "https://logs.example.com/waf/",

                "authentication_type": "none",

                "token": null,

                "username": null,

                "password": null

        }

}
```

A sample JSON response is shown below.

```
HTTP/1.1 200 OK

Cache-Control: no-cache

Content-Type: application/json; charset=utf-8

Date: Thu, 14 Apr 2016 12:00:00 GMT

Content-Length: 900
```

```
{
        "@id": "/rtld/v1/waf/profiles/10011",

        "@type": "RtldSetting",

        "id": 10011,

        "account_number": "0001",

        "delivery_method": "http_post",

        "profile_name": "My Profile",

        "enabled": false,

        "downsampling_rate": null,

        "fields": ["rule_message", "rule_tags", "client_country_code", "client_country",
"client_city", "sub_events_count", "sub_events", "waf_instance_name", "waf_profile_name",
"action_type", "waf_profile_type", "timestamp", "client_ip", "server_port", "url", "host",
"user_agent", "referer", "account_number", "uuid"],

        "aws_s3": null,

        "http_post": {

                "destination_endpoint": "https://logs.example.com/waf/",

                "authentication_type": "none",

                "token": null,

                "username": null,

                "password": null

        },

        "sumo_logic": null,

        "splunk_enterprise": null,

        "azure_blob_storage": null

}
```

RTLD (General)

Use these endpoints to look up information related to RTLD settings.

Get AWS Regions

Retrieves a list of AWS regions to which log data may be delivered.

Request

Retrieve AWS regions via the following request:

HTTP Method	Request URI
GET	https://api.edgecast.com/v2/mcc/rtld/aws-regions

Request Headers

The response for this endpoint only includes standard HTTP request headers including those described in the **Request Headers** section of the **Request and Response Elements** topic.

Request Body

Request body parameters are not required by this endpoint.

Response

The response to the above request includes an HTTP status code, response headers, and a response body.

Status Code

A status code indicates whether the request was successfully performed. A list of common status codes is provided in the **Status Codes and Error Messages** topic.

Response Headers

The response for this endpoint only returns standard HTTP response headers including those described in the **Response Headers** section of the **Request and Response Elements** topic.

Response Body

The response body for a successful request contains the following response elements:

Name	Data Type	Description
@id	String	Returns /v2/mcc/rtld/aws-regions.
@type	String	Returns Collection.
items	Array	Contains the AWS regions to which log data may be delivered.
code	String	Identifies an AWS region by its code name. Reference this code name when defining or retrieving a RTLD profile.
name	String	Identifies an AWS region by its name.
total_items	Integer	Indicates the total number of AWS regions that were included in the response.

Errors

The response body for an unsuccessful request may contain an error element that provides additional information. For a list of common error messages, please refer to the **Status Codes and Error Messages** topic.

Sample Request and Response

A sample JSON request is provided below.

```
GET https://api.edgecast.com/v2/mcc/rtld/aws-regions HTTP/1.1

Authorization: TOK:12345678-1234-1234-1234-1234567890ab

Accept: application/json

Host: api.edgecast.com
```

A sample JSON response is provided below.

```
HTTP/1.1 200 OK

Cache-Control: private

Content-Type: application/json; charset=utf-8

Date: Thu, 14 Apr 2016 12:00:00 GMT

Content-Length: 1060
```

```
{
        "@id": "/v2/mcc/rtld/aws-regions",
        "@type": "Collection",
        "items": [{
                        "code": "ap-south-1",
                        "name": "Asia Pacific (Mumbai)"
                }, {
                        ...
                }, {
                        "code": "us-west-2",
                        "name": "US West (Oregon)"
                }
        ],
        "total_items": 14
}
```

Get Access Types (Azure Blob Storage)

Retrieves the available access types for Azure Blob Storage.

Request

Retrieve access types via the following request:

HTTP Method	Request URI
GET	https://api.edgecast.com/v2/mcc/rtld/azure-access-types

Request Headers

The response for this endpoint only includes standard HTTP request headers including those described in the **Request Headers** section of the **Request and Response Elements** topic.

Request Body

Request body parameters are not required by this endpoint.

Response

The response to the above request includes an HTTP status code, response headers, and a response body.

Status Code

A status code indicates whether the request was successfully performed. A list of common status codes is provided in the **Status Codes and Error Messages** topic.

Response Headers

The response for this endpoint only returns standard HTTP response headers including those described in the **Response Headers** section of the **Request and Response Elements** topic.

Response Body

The response body for a successful request contains the following response elements:

Name	Data Type	Description
@id	String	Returns /v2/mcc/rtld/azure-access-types.
@type	String	Returns Collection.
items	Array	Contains the available access types for Azure Blob Storage.
code	String	Identifies an access type by its code name. Reference this code name when defining or retrieving a RTLD profile.
name	String	Identifies an access type by its name.

Name	Data Type	Description
total_items	Integer	Indicates the total number of access types that were included in the response.

Errors

The response body for an unsuccessful request may contain an error element that provides additional information. For a list of common error messages, please refer to the **Status Codes and Error Messages** topic.

Sample Request and Response

A sample JSON request is provided below.

```
GET https://api.edgecast.com/v2/mcc/rtld/azure-access-types HTTP/1.1

Authorization: TOK:12345678-1234-1234-1234-1234567890ab

Accept: application/json

Host: api.edgecast.com
```

A sample JSON response is provided below.

```
HTTP/1.1 200 OK

Cache-Control: private

Content-Type: application/json; charset=utf-8

Date: Thu, 14 Apr 2016 12:00:00 GMT

Content-Length: 224

{
        "@id": "/v2/mcc/rtld/azure-access-types",
        "@type": "Collection",
        "items": [{
                        "code": "sas_token",
                        "name": "SAS Token"
                }, {
                        "code": "access_key",
                        "name": "Access Key"
                }
        ],
        "total_items": 2
}
```

Get HTTP POST Authentication Methods

Retrieves the available authentication methods when delivering log data via HTTP POST.

Request

Retrieve authentication methods via the following request:

HTTP Method	Request URI
GET	https://api.edgecast.com/v2/mcc/rtld/http-authentication-methods

Request Headers

The response for this endpoint only includes standard HTTP request headers including those described in the **Request Headers** section of the **Request and Response Elements** topic.

Request Body

Request body parameters are not required by this endpoint.

Response

The response to the above request includes an HTTP status code, response headers, and a response body.

Status Code

A status code indicates whether the request was successfully performed. A list of common status codes is provided in the **Status Codes and Error Messages** topic.

Response Headers

The response for this endpoint only returns standard HTTP response headers including those described in the **Response Headers** section of the **Request and Response Elements** topic.

Response Body

The response body for a successful request contains the following response elements:

Name	Data Type	Description
@id	String	Returns /v2/mcc/rtld/http-authentication-methods.
@type	String	Returns Collection.
items	Array	Contains the available authentication methods for HTTP POST log delivery.
code	String	Identifies an authentication method by its code name. Reference this code name when defining or retrieving a RTLD profile.

Name	Data Type	Description
name	String	Identifies an authentication method by its name.
total_items	Integer	Indicates the total number of authentication methods that were included in the response.

Errors

The response body for an unsuccessful request may contain an error element that provides additional information. For a list of common error messages, please refer to the **Status Codes and Error Messages** topic.

Sample Request and Response

A sample JSON request is provided below.

```
GET https://api.edgecast.com/v2/mcc/rtld/http-authentication-methods HTTP/1.1

Authorization: TOK:12345678-1234-1234-1234-1234567890ab

Accept: application/json

Host: api.edgecast.com
```

A sample JSON response is provided below.

```
HTTP/1.1 200 OK

Cache-Control: private

Content-Type: application/json; charset=utf-8

Date: Thu, 14 Apr 2016 12:00:00 GMT

Content-Length: 304

{
        "@id": "/v2/mcc/rtld/http-authentication-methods",

        "@type": "Collection",

        "items": [{

                        "code": "custom_authentication",

                        "name": "Custom Authentication"

                }, {

                        "code": "http_basic",

                        "name": "HTTP Basic"

                }, {

                        "code": "none",

                        "name": "None"

                }

        ],
```

```
        "total_items": 3
}
```

Get HTTP Status Codes

Retrieves the available HTTP status codes for filtering log data.

Request

Retrieve HTTP status codes via the following request:

HTTP Method	Request URI
GET	https://api.edgecast.com/v2/mcc/rtld/status-codes

Request Headers

The response for this endpoint only includes standard HTTP request headers including those described in the **Request Headers** section of the **Request and Response Elements** topic.

Request Body

Request body parameters are not required by this endpoint.

Response

The response to the above request includes an HTTP status code, response headers, and a response body.

Status Code

A status code indicates whether the request was successfully performed. A list of common status codes is provided in the **Status Codes and Error Messages** topic.

Response Headers

The response for this endpoint only returns standard HTTP response headers including those described in the **Response Headers** section of the **Request and Response Elements** topic.

Response Body

The response body for a successful request contains the following response elements:

Name	Data Type	Description
@id	String	Returns /v2/mcc/rtld/status-codes.
@type	String	Returns Collection.
items	Array	Contains the available HTTP status codes for filtering log data.

Name	Data Type	Description
code	String	Identifies a HTTP status code by its code name. Reference this code name when defining or retrieving a RTLD profile.
name	String	Identifies a HTTP status code by its name.
total_items	Integer	Indicates the total number of HTTP status codes that were included in the response.

Errors

The response body for an unsuccessful request may contain an error element that provides additional information. For a list of common error messages, please refer to the **Status Codes and Error Messages** topic.

Sample Request and Response

A sample JSON request is provided below.

```
GET https://api.edgecast.com/v2/mcc/rtld/status-codes HTTP/1.1
Authorization: TOK:12345678-1234-1234-1234-1234567890ab
Accept: application/json
Host: api.edgecast.com
```

A sample JSON response is provided below.

```
HTTP/1.1 200 OK
Cache-Control: private
Content-Type: application/json; charset=utf-8
Date: Thu, 14 Apr 2016 12:00:00 GMT
Content-Length: 282

{
        "@id": "/v2/mcc/rtld/status-codes",
        "@type": "Collection",
        "items": [{
                    "code": "2xx",
                    "name": "2XX"
            }, {
                    ...
            }, {
                    "code": "5xx",
                    "name": "5XX"
```

```
          }
      ],
      "total_items": 4
 }
```

Get Log Delivery Methods

Retrieves the available destinations for the delivery of log data.

Request

Retrieve delivery methods via the following request:

HTTP Method	Request URI
GET	https://api.edgecast.com/v2/mcc/rtld/delivery-methods

Request Headers

The response for this endpoint only includes standard HTTP request headers including those described in the **Request Headers** section of the **Request and Response Elements** topic.

Request Body

Request body parameters are not required by this endpoint.

Response

The response to the above request includes an HTTP status code, response headers, and a response body.

Status Code

A status code indicates whether the request was successfully performed. A list of common status codes is provided in the **Status Codes and Error Messages** topic.

Response Headers

The response for this endpoint only returns standard HTTP response headers including those described in the **Response Headers** section of the **Request and Response Elements** topic.

Response Body

The response body for a successful request contains the following response elements:

Name	Data Type	Description
@id	String	Returns /v2/mcc/rtld/delivery-methods.
@type	String	Returns Collection.
items	Array	Contains the available destinations for log delivery.
code	String	Identifies a log delivery destination by its code name. Reference this code name when defining or retrieving a RTLD profile.
name	String	Identifies a log delivery destination by its name.
total_items	Integer	Indicates the total number of log delivery destinations that were included in the response.

Errors

The response body for an unsuccessful request may contain an error element that provides additional information. For a list of common error messages, please refer to the **Status Codes and Error Messages** topic.

Sample Request and Response

A sample JSON request is provided below.

```
GET https://api.edgecast.com/v2/mcc/rtld/delivery-methods HTTP/1.1

Authorization: TOK:12345678-1234-1234-1234-1234567890ab

Accept: application/json

Host: api.edgecast.com
```

A sample JSON response is provided below.

```
HTTP/1.1 200 OK

Cache-Control: private

Content-Type: application/json; charset=utf-8

Date: Thu, 14 Apr 2016 12:00:00 GMT

Content-Length: 421

{

        "@id": "/v2/mcc/rtld/delivery-methods",

        "@type": "Collection",

        "items": [{
```

```
                "code": "aws_s3",

                "name": "AWS S3"

        }, {

                ...

        }, {

                "code": "sumo_logic",

                "name": "Sumo Logic"

        }

    ],

    "total_items": 5

}
```

Get Log Downsampling Rates

Retrieves the available rates for downsampling the set of log data delivered to your destination.

Request

Retrieve downsampling rates via the following request:

HTTP Method	Request URI
GET	https://api.edgecast.com/v2/mcc/rtld/downsampling-rates

Request Headers

The response for this endpoint only includes standard HTTP request headers including those described in the **Request Headers** section of the **Request and Response Elements** topic.

Request Body

Request body parameters are not required by this endpoint.

Response

The response to the above request includes an HTTP status code, response headers, and a response body.

Status Code

A status code indicates whether the request was successfully performed. A list of common status codes is provided in the **Status Codes and Error Messages** topic.

Response Headers

The response for this endpoint only returns standard HTTP response headers including those described in the **Response Headers** section of the **Request and Response Elements** topic.

Response Body

The response body for a successful request contains the following response elements:

Name	Data Type	Description
@id	String	Returns /v2/mcc/rtld/downsampling-rates.
@type	String	Returns Collection.
items	Array	Contains a decimal value for each available downsampling rate.
total_items	Integer	Indicates the total number of downsampling rates that were included in the response.

Errors

The response body for an unsuccessful request may contain an error element that provides additional information. For a list of common error messages, please refer to the **Status Codes and Error Messages** topic.

Sample Request and Response

A sample JSON request is provided below.

```
GET https://api.edgecast.com/v2/mcc/rtld/downsampling-rates HTTP/1.1

Authorization: TOK:12345678-1234-1234-1234-1234567890ab

Accept: application/json

Host: api.edgecast.com
```

A sample JSON response is provided below.

```
HTTP/1.1 200 OK

Cache-Control: private

Content-Type: application/json; charset=utf-8

Date: Thu, 14 Apr 2016 12:00:00 GMT

Content-Length: 152

{

        "@id": "/v2/mcc/rtld/downsampling-rates",

        "@type": "Collection",

        "items": [0.1, 1.0, 25.0, 50.0, 75.0],

        "total_items": 5

}
```

Get Log Fields (RTLD CDN)

Retrieves the available set of log fields for RTLD CDN.

Request

Retrieve RTLD CDN log fields via the following request:

HTTP Method	Request URI
GET	https://api.edgecast.com/v2/mcc/rtld/fields

Request Headers

The response for this endpoint only includes standard HTTP request headers including those described in the **Request Headers** section of the **Request and Response Elements** topic.

Request Body

Request body parameters are not required by this endpoint.

Response

The response to the above request includes an HTTP status code, response headers, and a response body.

Status Code

A status code indicates whether the request was successfully performed. A list of common status codes is provided in the **Status Codes and Error Messages** topic.

Response Headers

The response for this endpoint only returns standard HTTP response headers including those described in the **Response Headers** section of the **Request and Response Elements** topic.

Response Body

The response body for a successful request contains the following response elements:

Name	Data Type	Description
@id	String	Returns /v2/mcc/rtld/fields.
@type	String	Returns Collection.
items	Array	Contains the available log fields.
code	String	Identifies a log field by its code name. Reference this code name when defining or retrieving a RTLD profile.
name	String	Identifies a log field by its name.

Name	Data Type	Description
total_items	Integer	Indicates the total number of log fields that were included in the response.

Errors

The response body for an unsuccessful request may contain an error element that provides additional information. For a list of common error messages, please refer to the **Status Codes and Error Messages** topic.

Sample Request and Response

A sample JSON request is provided below.

```
GET https://api.edgecast.com/v2/mcc/rtld/fields HTTP/1.1
Authorization: TOK:12345678-1234-1234-1234-1234567890ab
Accept: application/json
Host: api.edgecast.com
```

A sample JSON response is provided below.

```
HTTP/1.1 200 OK
Cache-Control: private
Content-Type: application/json; charset=utf-8
Date: Thu, 14 Apr 2016 12:00:00 GMT
Content-Length: 1444

    {
        "@id": "/v2/mcc/rtld/fields",
        "@type": "Collection",
        "items": [{
                "code": "user_agent",
                "name": "User Agent"
            }, {
                ...
            }, {
                "code": "referer",
                "name": "Referrer"
            }
        ],
        "total_items": 22
    }
```

Get Log Fields (RTLD WAF)

Retrieves the available set of log fields for RTLD WAF.

Request

Retrieve a RTLD WAF log fields via the following request:

HTTP Method	Request URI
GET	https://api.vdms.io/rtld/v1/waf/fields

Define the following variable when submitting the above request:

Variable	Description
ProfileID	Replace this variable with the system-defined ID assigned to the desired RTLD WAF profile.
	Tip: Use the Get All RTLD WAF Profiles endpoint to find out the system-defined ID assigned to your RTLD WAF profile.

Request Headers

This endpoint only takes advantage of common request headers.

Important: Unlike requests to api.edgecast.com, requests to our API gateway (api.vdms.io) require an access token (OAuth).

Request Body

Request body parameters are not required by this endpoint.

Response

The response to the above request includes an HTTP status code, response headers, and a response body.

Status Code

A status code indicates whether the request was successfully performed.

Response Headers

The response for this endpoint only includes standard HTTP response headers.

Response Body

The response body for a successful request contains the following response elements:

Name	Data Type	Description
@id	String	Returns /waf/fields.
@type	String	Returns Collection.
items	Array of objects	Contains the available log fields.
total_items	Integer	Indicates the total number of log fields that were included in the response.

items Array

The items array describes each log field using the following properties:

Name	Data Type	Description
category	String	Identifies the log field's category.
code	String	Identifies a log field by its code name. Reference this code name when defining or retrieving a RTLD WAF profile.
name	String	Identifies a log field by its name.

Errors

The response body for an unsuccessful request will contain an error response that provides additional information.

Sample Request and Response (JSON)

A sample JSON request is shown below.

```
GET https://api.vdms.io/rtld/v1/waf/fields HTTP/1.1

Authorization: Bearer A1bcbGciOiJSUzI1NiIsImtpZCI6Ij13N1VGQ01z...

Accept: application/json

Content-Type: application/json

Host: api.vdms.io
```

A sample JSON response is shown below.

```
HTTP/1.1 200 OK
Cache-Control: no-cache
Content-Type: application/json; charset=utf-8
Date: Thu, 14 Apr 2016 12:00:00 GMT
Content-Length: 1931

{
        "@id": "/waf/fields",
        "@type": "Collection",
        "items": [{
                        "category": "Client Geography",
                        "code": "client_country_code",
                        "name": "Country Code"
                }, {
                …
                }, {
                        "category": "Client Geography",
                        "code": "client_country",
                        "name": "Country Name"
                }
        ],
        "total_items": 20
}
```

Real-Time Statistics

Real-Time Statistics Endpoints

Real-Time Statistics endpoints allow you to view statistical information that reflects the current level of CDN activity for your account. This information provides a snapshot of usage information for your CDN account.

Calculating Real-Time Statistics

Each Real-Time Statistics metric is calculated as follows:

1. Each server provides statistical information every minute.

2. Upon requesting a particular metric, the average value on a per second basis is calculated as indicated below.

    a. Sum the last value provided by each server.

    b. Divide the above sum by 60.

Get Current Bandwidth

Returns the current amount of bandwidth usage on a per platform basis.

Request

A request for the current amount of bandwidth usage is described below. When submitting this request, you will need to define the following terms:

- **AccountNumber:** This term should be replaced by your CDN account number. This number can be found in the upper-right hand corner of the MCC.

- **Platform:** This term should be replaced by the ID associated with the desired platform. Valid values for this parameter are listed below.

    - **3:** HTTP Large

    - **8:** HTTP Small

    - **14:** Application Delivery Network (ADN)

HTTP Method	Request URI
GET	https://api.edgecast.com/v2/realtimestats/customers/*AccountNumber*/media/*Platform*/bandwidth

Request Headers

This endpoint only takes advantage of the common request headers described in the **Request Headers** section of the **Request and Response Elements** topic.

Request Body

Request body parameters are not required by this endpoint.

Response

The response to the above request includes an HTTP status code, response headers, and a response body.

Status Code

A status code indicates whether the request was successfully performed. A list of common status codes is provided in the **Status Codes and Error Messages** topic.

Response Headers

The response for this endpoint only returns standard HTTP response headers including those described in the **Response Headers** section of the **Request and Response Elements** topic.

Response Body

The response body for a successful request contains the following response element:

Name	Description
Result	A number (floating-point) value that indicates the current amount of bandwidth usage for your account on the specified platform. This value is reported in bits per second.

Errors

The response body for an unsuccessful request may contain an error element that provides additional information. For a list of common error messages, please refer to the **Status Codes and Error Messages** topic.

Sample Request and Response

A sample JSON request is provided below.

```
GET https://api.edgecast.com/v2/realtimestats/customers/0001/media/3/bandwidth
HTTP/1.1

Authorization: TOK:12345678-1234-1234-1234-1234567890ab

Accept: application/json

Host: api.edgecast.com
```

A sample JSON response is provided below.

```
HTTP/1.1 200 OK

Cache-Control: private

Content-Type: application/json; charset=utf-8

Date: Thu, 14 Apr 2016 12:00:00 GMT

Content-Length: 31


{

        "Result" : 8059050.365432

}
```

Get Current Cache Status Statistics

Provides a breakdown of the cache statuses currently being returned for requests to your CDN account.

Request

A request for cache status statistics is described below. When submitting this request, you will need to define the following terms:

- **AccountNumber:** This term should be replaced by your CDN account number. This number can be found in the upper-right hand corner of the MCC.

- **Platform:** This term should be replaced by the ID associated with the desired platform. Valid values for this parameter are listed below.

    - **3:** HTTP Large

    - **8:** HTTP Small

    - **14:** Application Delivery Network (ADN)

HTTP Method	Request URI
GET	https://api.edgecast.com/v2/realtimestats/customers/*AccountNumber*/media/*Platform*/cachestatus

Request Headers

This endpoint only takes advantage of the common request headers described in the **Request Headers** section of the **Request and Response Elements** topic.

Request Body

Request body parameters are not required by this endpoint.

Response

The response to the above request includes an HTTP status code, response headers, and a response body.

Status Code

A status code indicates whether the request was successfully performed. A list of common status codes is provided in the **Status Codes and Error Messages** topic.

Response Headers

The response for this endpoint only returns standard HTTP response headers including those described in the **Response Headers** section of the **Request and Response Elements** topic.

Response Body

The response body for a successful request contains the following response elements for each cache status returned by this endpoint:

Name	Description
CacheStatus	A string that indicates the name of the cache status for which statistical information will be returned.
Connections	An integer that indicates the total number of requests per second that resulted in the specified cache status.

A brief description is provided below for each cache status.

Cache Status	Description
CONFIG_NOCACHE	This status is reported when an asset's Cache-Control and Expires headers indicate that it should not be cached on a POP or by the HTTP client. As a result, the asset was served from the origin server.
NONE	This status indicates that a cache content freshness check was not performed. This check is skipped when Token-Based Authentication denies a request or when an HTTP request method is used that bypasses cache (e.g., PUT, DELETE, etc).
TCP_CLIENT_REFRESH_MISS	This status is reported when an HTTP client (e.g., browser) forces an edge server to retrieve a new version of a stale asset from the origin server. By default, our servers prevent an HTTP client from forcing our edge servers to retrieve a new version of the asset from the origin server. However, this behavior can be overridden through the use of HTTP Rules Engine.
TCP_EXPIRED_HIT	This status is reported when a request that targeted an asset with an expired time to live (TTL), such as when the asset's max-age has expired, was served directly from the POP to the client. An expired request typically results in a revalidation request to the origin server. In order for a TCP_EXPIRED_HIT to occur, the origin server must indicate that a newer version of the asset does not exist. This type of situation will typically update that asset's Cache-Control and Expires headers.

Cache Status	Description
TCP_EXPIRED_MISS	This status is reported when a newer version of an expired cached asset is served from the POP to the client. If the TTL for a cached asset has expired (e.g., expired max-age), then a check will be performed on the origin server for a newer version of that asset. If an updated version is found, then it will be served to the client instead of the cached version. If the origin server or HTTP Rules Engine does not specifically prevent that asset from being cached, then it will be cached on the POP closest to the client that requested it.
TCP_HIT	This status is reported when a request is served directly from the POP to the client. An asset is immediately served from a POP when it is cached on the POP closest to the client and it has a valid TTL. TTL is determined by the Cache-Control: s-maxage, Cache-Control: max-age, and Expires headers.
TCP_MISS	This status indicates that a cached version of the requested asset was not found on the POP closest to the client. The asset will be requested from either an origin server or an origin shield server and then served to the client. If the origin server or HTTP Rules Engine does not specifically prevent that asset from being cached, then it will be cached on the POP closest to the client that requested it.
UNCACHEABLE	This status is reported when a request results in an error (e.g., 403 Forbidden, 404 Not Found, etc.).

Errors

The response body for an unsuccessful request may contain an error element that provides additional information. For a list of common error messages, please refer to the **Status Codes and Error Messages** topic.

Sample Request and Response

A sample JSON request is provided below.

```
GET https://api.edgecast.com/v2/realtimestats/customers/0001/media/3/cachestatus
HTTP/1.1

Authorization: TOK:12345678-1234-1234-1234-1234567890ab

Accept: application/json

Host: api.edgecast.com
```

A sample JSON response is provided below.

```
HTTP/1.1 200 OK
Cache-Control: private
Content-Type: application/json; charset=utf-8
Date: Thu, 14 Apr 2016 12:00:00 GMT
Content-Length: 492


[{
            "CacheStatus" : "TCP_HIT",
            "Connections" : 3550
    }, {
            "CacheStatus" : "TCP_EXPIRED_HIT",
            "Connections" : 1525
    }, {
            "CacheStatus" : "TCP_MISS",
            "Connections" : 125
    }, {
            "CacheStatus" : "TCP_EXPIRED_MISS",
            "Connections" : 0
    }, {
            "CacheStatus" : "TCP_CLIENT_REFRESH_MISS",
            "Connections" : 0
    }, {
            "CacheStatus" : "NONE",
            "Connections" : 0
    }, {
            "CacheStatus" : "CONFIG_NOCACHE",
            "Connections" : 0
    }, {
            "CacheStatus" : "UNCACHEABLE",
            "Connections" : 0
    }
]
```

Get Current Status Codes Statistics

Provides a breakdown of the HTTP status codes currently being returned for requests to your CDN account.

Request

A request for status codes statistics is described below. When submitting this request, you will need to define the following terms:

- **AccountNumber:** This term should be replaced by your CDN account number. This number can be found in the upper-right hand corner of the MCC.

- **Platform:** This term should be replaced by the ID associated with the desired platform. Valid values for this parameter are listed below.

    - **3:** HTTP Large

    - **8:** HTTP Small

    - **14:** Application Delivery Network (ADN)

HTTP Method	Request URI
GET	https://api.edgecast.com/v2/realtimestats/customers/*AccountNumber*/media/*Platform*/statuscode

Request Headers
This endpoint only takes advantage of the common request headers described in the **Request Headers** section of the **Request and Response Elements** topic.

Request Body
Request body parameters are not required by this endpoint.

Response

The response to the above request includes an HTTP status code, response headers, and a response body.

Status Code
A status code indicates whether the request was successfully performed. A list of common status codes is provided in the **Status Codes and Error Messages** topic.

Response Headers
The response for this endpoint only returns standard HTTP response headers including those described in the **Response Headers** section of the **Request and Response Elements** topic.

Response Body

The response body for a successful request contains the following response elements for each status code returned by this endpoint:

Name	Description
Connections	An integer that indicates the total number of requests per second that resulted in the specified status code.
StatusCode	A string that indicates the type of status code for which statistical information will be returned.

A brief description is provided below for each type of status code.

Name	Description
2xx	A 2xx status code represents any HTTP status code in the 200 range (e.g., 200, 201, 202, etc.). This type of status code indicates that the request was successfully delivered to the client.
304	This status code indicates that the requested asset has not been modified since it was last retrieved by the HTTP client.
3xx	A 3xx status code represents any HTTP status code in the 300 range (e.g., 300, 301, 302, etc.). This type of status code indicates that the request resulted in a redirection.
403	This status code indicates that the request was deemed unauthorized. One possible cause for this status code is when an unauthorized user requests an asset protected by Token-Based Authentication.
404	This status code indicates that the requested asset could not be found.
4xx	A 4xx status code represents any HTTP status code in the 400 range (e.g., 400, 401, 402, 405, etc.). This status code indicates that the requested asset was not delivered to the client.
5xx	A 5xx status code represents any HTTP status code in the 500 range (e.g., 500, 501, 502, etc.).
Other	This category is a catch-all for all status codes not covered by any of the above status codes.

Errors

The response body for an unsuccessful request may contain an error element that provides additional information. For a list of common error messages, please refer to the **Status Codes and Error Messages** topic.

Sample Request and Response

A sample JSON request is provided below.

```
GET https://api.edgecast.com/v2/realtimestats/customers/0001/media/3/statuscode
HTTP/1.1

Authorization: TOK:12345678-1234-1234-1234-1234567890ab

Accept: application/json

Host: api.edgecast.com
```

A sample JSON response is provided below.

```
HTTP/1.1 200 OK

Cache-Control: private

Content-Type: application/json; charset=utf-8

Date: Thu, 14 Apr 2016 12:00:00 GMT

Content-Length: 407


[{

            "Connections" : 5600,

            "StatusCode" : "2xx"

      }, {

            "Connections" : 0,

            "StatusCode" : "304"

      }, {

            "Connections" : 0,

            "StatusCode" : "3xx"

      }, {

            "Connections" : 0,

            "StatusCode" : "403"

      }, {

            "Connections" : 0,

            "StatusCode" : "404"

      }, {

            "Connections" : 0,

            "StatusCode" : "4xx"

      }, {

            "Connections" : 0,

            "StatusCode" : "5xx"

      }, {

            "Connections" : 0,

            "StatusCode" : "other"

      }

]
```

Get Current Total Connections

Returns the total new connections per second on the specified platform. For the purposes of this endpoint, a connection is initiated when a user agent (e.g., web browser) requests content through the CDN. After which, the user agent determines whether future requests within that session will reuse that connection or whether new connections will be established.

How is this statistic calculated?

This statistic is calculated using the following two steps:

1. The average number of new connections per second on each edge server is calculated.

2. This data is collected from all edge servers and then summed.

Request

A request to find out the total number of new connections per second is described below. When submitting this request, you will need to define the following terms:

- **AccountNumber:** This term should be replaced by your CDN account number. This number can be found in the upper-right hand corner of the MCC.

- **Platform:** This term should be replaced by the ID associated with the desired delivery platform. Valid values for this parameter are listed below.

  - **3:** HTTP Large

  - **8:** HTTP Small

  - **14:** Application Delivery Network (ADN)

HTTP Method	Request URI
GET	https://api.edgecast.com/v2/realtimestats/customers/*AccountNumber*/media/*Platform*/connections

Request Headers
This endpoint only takes advantage of the common request headers described in the **Request Headers** section of the **Request and Response Elements** topic.

Request Body
Request body parameters are not required by this endpoint.

Response

The response to the above request includes an HTTP status code, response headers, and a response body.

Status Code

A status code indicates whether the request was successfully performed. A list of common status codes is provided in the **Status Codes and Error Messages** topic.

Response Headers

The response for this endpoint only returns standard HTTP response headers including those described in the **Response Headers** section of the **Request and Response Elements** topic.

Response Body

The response body for a successful request contains the following response element:

Name	Description
Result	A number (floating-point) that indicates the total number of new connections per second on the specified platform.

Errors

The response body for an unsuccessful request may contain an error element that provides additional information. For a list of common error messages, please refer to the **Status Codes and Error Messages** topic.

Sample Request and Response

A sample JSON request is provided below.

```
GET https://api.edgecast.com/v2/realtimestats/customers/0001/media/3/connections
HTTP/1.1

Authorization: TOK:12345678-1234-1234-1234-1234567890ab

Accept: application/json

Host: api.edgecast.com
```

A sample JSON response is provided below.

```
HTTP/1.1 200 OK

Cache-Control: private

Content-Type: application/json; charset=utf-8

Date: Thu, 14 Apr 2016 12:00:00 GMT

Content-Length: 35


{

        "Result" : 21099.000994

}
```

Appendix A

Purge Syntax

Please refer to the CDN Help Center for information on purge syntax.

Appendix B

Report Date/Time Format

Many of the Reporting endpoints require that you specify a time period for the statistical information that will be returned. When specifying a start or end date, you will need to use one of the following formats:

- **Date:** *YYYY-MM-DD*

- **Date/Time:** *YYYY-MM-DD*T*hh*:*mm*:*ss*

The above "Date" format can be used by any Reporting endpoint that requires that you specify a start or end date. The above "Date/Time" format can only be used by reports that specifically indicate that time can be specified.

Note: Time (i.e., T*hh*:*mm*:*ss*) is optional. If time is not specified, then a default time (i.e., 00:00:00) will be used.

The variables used for the date and the date/time formats are described below.

- **YYYY:** Represents a year in the Gregorian calendar using a four digit number (e.g., 2011).

- **MM:** Represents a two digit month between 01 (January) and 12 (December).

- **DD:** Represents a two digit day between 01 and 31.

- **T:** Indicates a delimiter between date and time. This delimiter is only required if you would like to specify a time. Keep in mind that time must be specified using 24-hour clock notation in UTC/GMT.

- **hh:** Represents a two digit hour between 00 (midnight) and 23 (11 p.m.).

- **mm:** Represents the number of minutes into the specified hour. Minutes should be specified using two digits between 00 and 59.

- **ss:** Represents the number of seconds into the specified minute. Seconds should be specified using two digits between 00 and 59.

Relationship between Start/End Time and Data Reported

The time period used to generate a report plays an important role in determining the bulk of the CDN activity data that will be reported. However, there is another factor that determines whether additional CDN activity will be included in the reported value. This factor is that start and end date/times are inclusive. In order to understand what this means, you will need to know that data is reported in chunks of time (e.g., 5 minutes, 1 hour, 1 day, etc.). A report will include all of the chunks that fall within the specified time period and the chunks that correspond to the specified start and end date/time. This will occur regardless of whether the specified start and end date/time falls at the start, middle, or end of a chunk of time.

A few key facts about how time chunks affect or interact with report data:

- The amount of time covered by a chunk varies for each type of report. This time interval can either be 5 minutes, 1 hour, 1 day, or 1 month.

- A report's time chunk should not be confused with the date/time range used to generate the report. Please refer to the documentation provided for the desired endpoint to find out the time chunk that it uses to report data.

- A start or end date/time cannot be specified for monthly reports (e.g., Get Traffic Usage). The data returned for this type of endpoint will always be limited to the specified month (e.g., 08-01-2012 00:00:00 – 08-31-2012 23:59:59 GMT).

It is important to know the following information when generating a report:

- What is the report's start and end date/time?

- What type of time chunk is used to report data?

The above information can be used to identify the exact time period that will be covered by a report. Simply make sure to account for the chunk of time used by the report to figure out the exact time period for which CDN activity will be reported.

The following table illustrates how the exact time period that will be included in a report can be calculated for each type of time chunk. This example assumes that the following date/time range was used to generate the report:

- **Start Date/Time:** 2012-08-01 07:02:00

- **End Date/Time:** 2012-08-02 00:00:00

Time Chunk	Actual Start Date/Time	Actual End Date/Time
5 Minutes	2012-08-01 07:00:00	2012-08-02 00:04:59
1 Hour	2012-08-01 07:00:00	2012-08-02 00:59:59
1 Day	2012-08-01 00:00:00	2012-08-02 23:59:59

Appendix C

Legacy Endpoints

Please refer to the REST API Help Center for information on legacy endpoints.

Appendix D

POP Listing

A list of POPs, their corresponding abbreviation, and the region that they serve is available from the CDN Help Center:

- [POP Listing](#)

Appendix E

Origin Shield Locations and Settings

A list of Origin Shield locations can be retrieved through either the Get Origin Shield POPs (HTTP Large) or the Get Origin Shield POPs (HTTP Small) operation. Both of these operations will return the name, POP code, and the region associated with each Origin Shield location for the specified platform.

The Origin Shield feature allows you to bypass one or more regions when defining multiple POP locations. Bypassing a region indicates that requests for that region will bypass the Origin Shield and go directly to the customer origin server. This type of configuration is the equivalent of turning Origin Shield off for a particular region. The following table provides a listing of bypass region options. This list provides a descriptive name, code, and the region corresponding to each bypass region option.

Name	Code	Region
Bypass Asia	BYAP	Asia
Bypass E Coast US	BYEC	US East
Bypass Europe	BYEU	Europe
Bypass W Coast US	BYWC	US West