Edgecast

Quick Start Guide

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

About This Guide

Quick Start Guide
Version 3.50
11/22/2021

Table of Contents

Getting Started

Overview

This guide is designed to provide the information you need to quickly configure a basic content delivery network (CDN) setup. It provides quick start information for each of the following tasks:

- Delivering Content Using the HTTP Protocol
- Uploading Data to CDN Storage
- Delivering Dynamic Content Using the HTTP Protocol (ADN Platform)
- Securing Site Traffic Via Web Application Firewall

Tip: If you have additional questions or if the desired topic was not covered in this guide, then please refer to the documentation provided from the MCC's **Dashboard** page.

Note: If a platform is not available from your account, then it may not have been activated on your account. Please contact your CDN account manager to add additional services to your account.

Learn About Our CDN Offerings

Our CDN provides you with the capability to deliver content to your clients using several different delivery mechanisms. Additionally, we provide reporting capabilities that allow you to monitor and analyze data delivery patterns and usage.

Before you can start taking advantage of the speed and reliability provided by our CDN, you will need to choose how to deliver your data to your clients. Our CDN allows you to deliver content over the HTTP/HTTPS protocol and to stream video in a variety of formats and protocols. This functionality is provided through our platforms. A platform is a term that encompasses the infrastructure of dedicated servers and devices that have been distributed across our worldwide network of points-of-presence (POPs) for the purpose of efficiently securing and delivering content from an origin point to your customers. Our CDN provides several specialized platforms for data delivery. These platforms are described below.

Platform	Supported Protocol(s)	Description
HTTP Large	HTTP HTTPS	This platform has been optimized to cache static content, which allows it to quickly deliver them to your customers.
Application Delivery Network (ADN)	HTTP HTTPS	This platform specializes in providing whole site acceleration for dynamic websites. The content generated by these types of sites is typically driven by either a database or user interaction. As a result, these types of sites generate unique content that cannot effectively leverage our caching technology. ADN is able to accelerate these types of sites by optimizing the communication between your origin server and your users.

Media Control Center (MCC)

The Media Control Center (MCC) is a browser-based application that provides a central location from which you can view and modify your CDN configuration. Additionally, you may generate reports that provide detailed information on how our CDN is delivering data to your clients. This allows you to analyze data delivery performance, in order to optimize how our CDN caches your organization's assets. The final aspect of MCC configuration allows you to determine who will have access to these features and settings. The MCC is accessible through the following URL:

- https://my.edgecast.com

Before you can gain access to the MCC, you will need to provide authentication. This authentication consists of the e-mail address for an MCC user account and a password.

Tip: If you cannot remember your password, click on the "Forgot Your Password" link. A link that allows you to reset your password will be sent to your e-mail account.

Basic Terminology

Before you start setting up your CDN configuration, you should become familiar with the following common terms:

Term	Definition
CDN URL	This is the general term for any URL that directly references our CDN domain. Typically, this URL is used to request assets via our CDN. **Sample URL for the HTTP Large Platform:** http://wpc.0001.edgecastcdn.net/800001/Folder/Asset.htm
Edge CNAME URL	This type of URL takes advantage of a CNAME record to provide a friendlier alternative to a CDN URL. **Sample URL:** http://images.mydomain.com/Folder/Asset.htm
Edge Server	An edge server is a server that is located within a POP. This type of server is responsible for handling requests and caching assets.
Origin Server	An origin server is the server on which your content resides. The two types of origin servers are described below. • **Customer origin server:** Our CDN can serve data from a server outside of our network after a customer origin server configuration has been created. This type of server is best suited for customers who do not wish to move their data to a CDN origin server. If you plan on using a customer origin server, make sure to create a customer origin configuration on each platform from which data will be delivered. • **CDN origin server:** Our CDN offers a storage service. The server on which your assets are stored is called a CDN origin server. This type of configuration ensures that your servers are not overloaded by client requests. Additionally, since a CDN origin server is located within our network, data can be served more efficiently and reliably to your clients. However, before you can serve content from a CDN origin server, you will need to copy your data onto it using FTP.
Point-of-Presence (POP)	A POP is one of many worldwide locations on our network through which clients can request and receive assets.

HTTP Data Delivery

Introduction

Basic information on how our CDN handles HTTP requests is provided below.

1. Client requests an asset using a CDN URL or an edge CNAME URL.
2. An edge server interprets the request and determines whether the asset is served from cache (i.e., edge server) or an origin server.

An origin server plays an important role within a CDN environment. Before you can serve data to your customers, you will need to figure out whether you would like to serve data from an external server (customer origin server) or from a storage server on our network (CDN origin server).

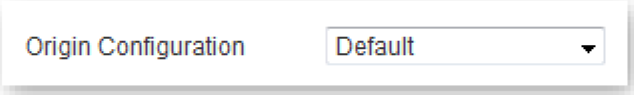
Note: If you would like to take advantage of our CDN storage service, then you should refer to the **CDN Storage** chapter for more information.

How to Set Up an External Server

Before content can be delivered from your own server (i.e., customer origin server), you will need to configure our CDN to recognize it. Once you have configured our CDN appropriately, a CDN URL, which is a URL that uses a CDN domain and content access point (e.g., /800001/MyOrigin), will be assigned to the root folder of your customer origin server. If you would like to use a more user-friendly URL, then you will also need to configure an edge CNAME and add a CNAME on a DNS server that points the domain assigned to your edge CNAME to the root folder of your customer origin server. Both procedures are described below.

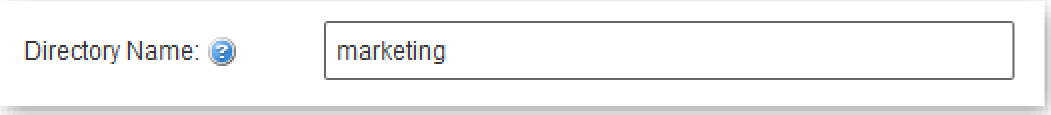
To configure our CDN to recognize an external server

1. Navigate to the Customer Origin page in the MCC.
2. Leave the **Origin Configuration** option set to "Default."



Origin Configuration: Default

3. In the **Directory Name** option, type an alphanumeric word or phrase that will be used to identify an external server. This name will be included in the CDN URL used to access your content.

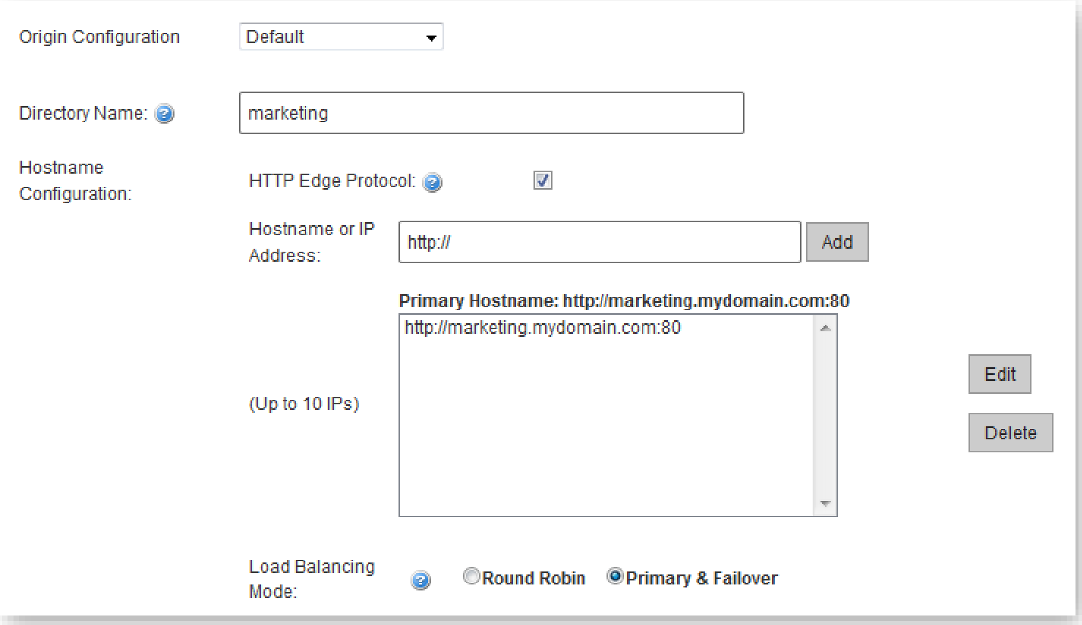


Directory Name: marketing

The following sample URL is based on a sample account number (i.e., 0001) and the name (i.e., images) specified in the above figure.

- **Sample CDN URL (HTTP Large):** http://wpc.0001.edgecastcdn.net/800001/marketing

4. To serve content using the HTTP protocol, make sure that the **HTTP Edge Protocol** option is marked. In the **Hostname or IP Address** option, you should type the domain or IP address of the server where your data resides. You should then append a colon and the port through which communication will take place (e.g., http://marketing.mydomain.com:80). Click **Add** which appears directly to the right of the **Hostname or IP Address** option.



Origin Configuration: Default

Directory Name: marketing

Hostname Configuration:

HTTP Edge Protocol: ☑

Hostname or IP Address: http://

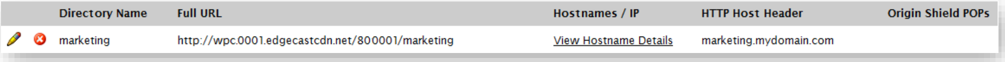
Primary Hostname: http://marketing.mydomain.com:80

http://marketing.mydomain.com:80

(Up to 10 IPs)

Load Balancing Mode: ○ Round Robin ● Primary & Failover

5. Click **Add** (shown in the bottom right-hand corner above) to save your customer origin configuration. The CDN URL that you should use to access content on that customer origin server will be listed under the **Full URL** column, which can be viewed at the top of the **Customer Origin** page. This CDN URL (e.g., http://wpc.0001.edgecastcdn.net/800001/marketing) points to the root folder of your customer origin server. To provide a link to your content, simply append the relative path to the desired asset to this URL (e.g., http://wpc.0001.edgecastcdn.net/800001/marketing**/collateral/ad01.pdf**).



		Directory Name	Full URL	Hostnames / IP	HTTP Host Header	Origin Shield POPs
✎	⊗	marketing	http://wpc.0001.edgecastcdn.net/800001/marketing	View Hostname Details	marketing.mydomain.com	

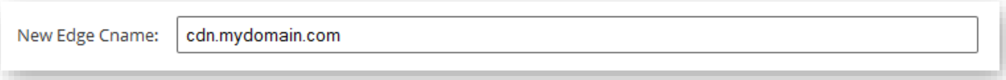
6. Make sure that the IP addresses listed at the bottom of the page are allowed access to your server.

Important: It may take up to an hour before you will be able to access content on your customer origin server through our CDN.

To create a user-friendly URL to an external server

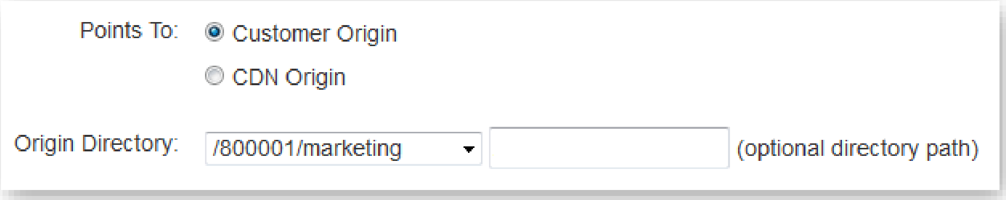
Note: This optional procedure should only be performed if you would like to provide a user-friendly URL for your users.

1. Navigate to the Edge CNAMEs page, which can be found in the MCC.
2. In the **New Edge Cname** option, type the name of the domain that will be used to reference the customer origin configuration created above. The CNAME should be specified in lower-case letters and should not include a protocol (i.e., http://).



New Edge Cname: cdn.mydomain.com

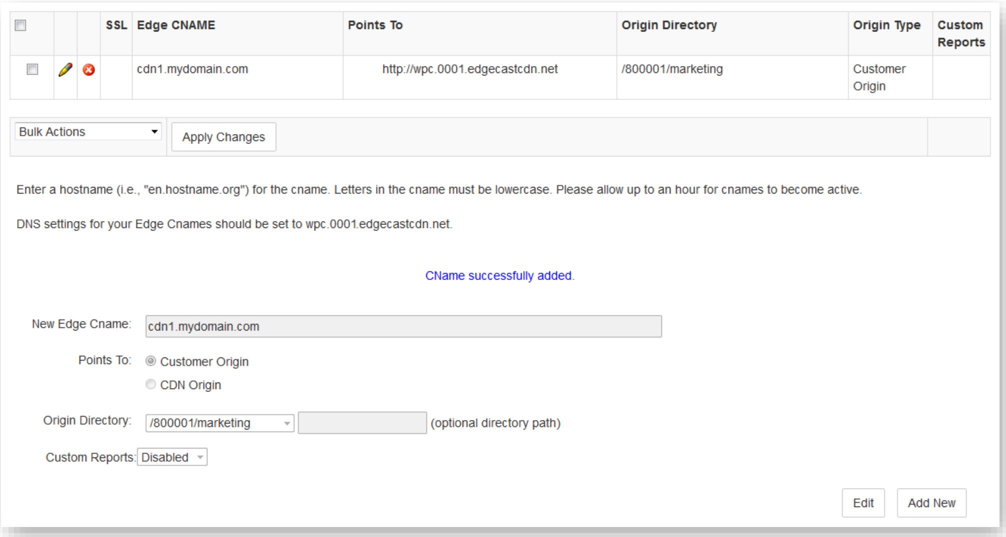
3. In the **Points to** option, select "Customer Origin."
4. In the **Origin Directory** option, select the recently created customer origin configuration.



Points To: ● Customer Origin
○ CDN Origin

Origin Directory: /800001/marketing ▾ (optional directory path)

5. Click **Add**. An edge CNAME that points to your recently created customer origin configuration should appear at the top of the **Edge CNAMEs** page.



□			SSL	Edge CNAME	Points To	Origin Directory	Origin Type	Custom Reports
□	✎	✖		cdn1.mydomain.com	http://wpc.0001.edgecastcdn.net	/800001/marketing	Customer Origin	

Enter a hostname (i.e., "en.hostname.org") for the cname. Letters in the cname must be lowercase. Please allow up to an hour for cnames to become active.

DNS settings for your Edge Cnames should be set to wpc.0001.edgecastcdn.net.

CName successfully added.

New Edge Cname: cdn1.mydomain.com

Points To: ● Customer Origin ○ CDN Origin

Origin Directory: /800001/marketing (optional directory path)

Custom Reports: Disabled

6. Modify/register a CNAME record through your DNS service provider. This CNAME record should point the hostname specified in step 2 (e.g., images.domain.org) to the CDN hostname (e.g., wpc.0001.edgecastcdn.net). Requests to an edge CNAME URL will not resolve to our CDN service until this CNAME record exists.

Important: It may take up to an hour after creating an edge CNAME configuration before you will be able to access your content using an edge CNAME URL.

How to Access HTTP Content

Your content can be accessed by appending a relative path to a CDN or an edge CNAME URL. If you do not know which CDN or edge CNAME URL to use, then you will need to know the following information:

- Platform
- Origin Server Type
- Relative Path

The importance for each of these items is discussed below.

Note: If you haven't already created a customer origin configuration or uploaded your content to a CDN origin server, then please do so before continuing. For information on how to use our CDN storage service, please refer to the **CDN Storage** chapter.

Platform

Deliver content over the HTTP protocol using the HTTP Large platform.

Origin Server Type

The next step is to figure out whether you plan on using a CDN origin server or a customer origin server. Once you know which type of origin server will be used to serve your content, please find the base CDN or edge CNAME URL corresponding to it from the **HTTP Large** page.

Heading	**Description**
URLs for EdgeCast Origin	This section provides the URLs that can be used to access content on a CDN origin server. **Example:** http://wpc.*xxxx*.edgecastcdn.net/00*xxxx*/
URLs for your Origin	This section provides the URLs that can be used to access content on each customer origin server that has been configured for the current platform.
SSL URL	This section lists the URLs that can be used to access content over the HTTPS protocol. The following requirements must be met before an HTTPS URL will be listed in this section: • A CDN account manager must enable the SSL Traffic feature on the desired platform. • A TLS certificate must be installed on our network. • You must create an edge CNAME corresponding to the domain associated with the SSL certificate. Learn more.

Relative Path

The final piece of information that you will need to build a CDN URL or an edge CNAME URL is the relative path to the desired asset. Typically, the starting point for this relative path is the root folder of the desired server. This relative path needs to be appended to the base URL discovered above in the **Origin Server Type** section.

Note: If you plan on using an edge CNAME URL, then the starting point is determined by whether you have specified an optional directory path. If you did not specify one, then the starting point is the root folder. Otherwise, the starting point for this relative path is the folder specified by that option.

Sample URLs are provided below.

- **HTTP Large (CDN URL):**
  http://wpc.*xxxx*.edgecastcdn.net/00*xxxx*/Videos/Presentation01.ppt
- **Edge CNAME URL:**
  http://videos.mydomain.com/Presentation01.ppt

CDN Storage

Uploading Data to CDN Storage

Our CDN offers a storage service from which your content may be delivered. Content delivery from CDN storage requires that you copy the desired data to it via a SFTP client or rsync.

Setting up a SFTP client requires the following information:

- Rysnc hostname. View this hostname on the RSYNC page.
- Your MCC user name (i.e., e-mail address) and password.

Note: Access to the **RSYNC** page is required for SFTP access to the CDN origin server.

Application Delivery Network (ADN)

Introduction

The primary purpose of the Application Delivery Network (ADN) platform is to accelerate web site performance for dynamic content. Dynamic content usually deals with database or user-driven interactions. Caching this type of unique content will not generate substantial performance gains. As a result, this platform relies on improving web site performance through a variety of protocol and communication optimizations.

Basic information on how our CDN typically handles HTTP requests over the ADN platform is provided below.

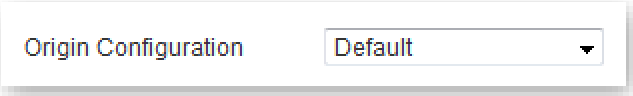
1. A client requests an asset using a CDN URL or an edge CNAME URL.
2. An edge server interprets the request and forwards it to the ADN Gateway server that can best deliver the request to the customer origin server.
3. The customer origin server returns the requested content to the ADN Gateway server.
4. The ADN Gateway server delivers the request to the client via an edge server.

How to Set Up an External Server

In order to deliver content from your server (i.e., customer origin server), our CDN must be configured to recognize it. After which, a CDN URL, which is a URL that uses a CDN domain and content access point (e.g., /800001/MyOrigin), will be assigned to the root folder of your customer origin server. If you would like to use a more user-friendly URL, then you will also need to configure an edge CNAME and add a CNAME on a DNS server that points the domain assigned to your edge CNAME to the root folder of your customer origin server. Both procedures are described below.

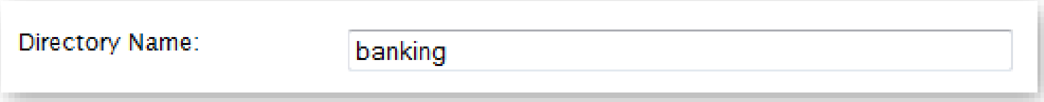
To configure our CDN to recognize an external server

1. Navigate to the Customer Origin page in the MCC.
2. Leave the **Origin Configuration** option set to "Default."



Origin Configuration: Default

3. In the **Directory Name** option, type an alphanumeric word or phrase that will be used to identify an external server. This name will be included in the CDN URL used to access your content.

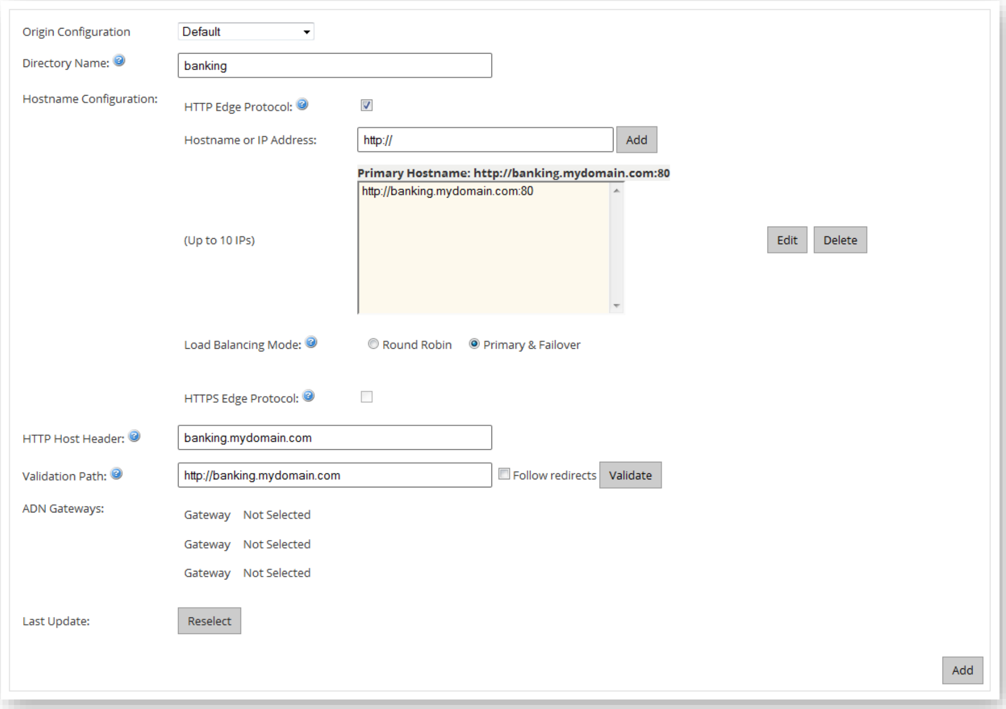


Directory Name: banking

The following sample URL is based on a sample account number (i.e., 0001) and the name (i.e., banking) specified in the above figure.

http://adn.0001.edgecastcdn.net/800001/banking

4. To serve content using the HTTP protocol, make sure that the **HTTP Edge Protocol** option is marked. In the **Hostname or IP Address** option, you should type the domain or IP address of the desired server. You should then append a colon and the port through which communication will take place (e.g., http://banking.mydomain.com:80). Click **Add** which appears directly to the right of the **Hostname or IP Address** option.



Origin Configuration: Default

Directory Name: banking

Hostname Configuration:

HTTP Edge Protocol: ☑

Hostname or IP Address: http://

Primary Hostname: http://banking.mydomain.com:80

(Up to 10 IPs) http://banking.mydomain.com:80

Load Balancing Mode: ○ Round Robin ● Primary & Failover

HTTPS Edge Protocol: □

HTTP Host Header: banking.mydomain.com

Validation Path: http://banking.mydomain.com □ Follow redirects

ADN Gateways:

Gateway Not Selected

Gateway Not Selected

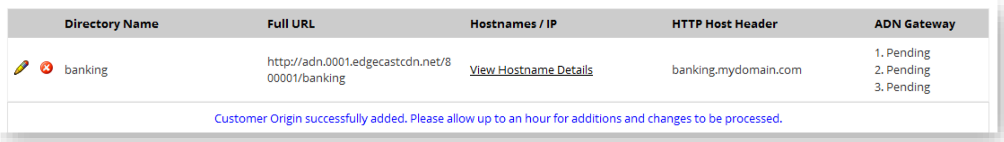
Gateway Not Selected

Last Update:

5. Upload a 5 KB asset to your server.

6. In the **Validation Path** option, type a URL that points to the asset uploaded in the previous step. Make sure that the domain specified in this URL matches the value defined in the **HTTP Host Header** option. Click **Validate**. If the result returns "200 OK" for all domains/IP addresses, then proceed to the next step.

7. Click **Add** (shown in the bottom right-hand corner in the above illustration) to save your customer origin configuration.



	Directory Name	Full URL	Hostnames / IP	HTTP Host Header	ADN Gateway
	banking	http://adn.0001.edgecastcdn.net/800001/banking	View Hostname Details	banking.mydomain.com	1. Pending 2. Pending 3. Pending

Customer Origin successfully added. Please allow up to an hour for additions and changes to be processed.

The CDN URL that you should use to access content on that customer origin server will be listed under the **Full URL** column (as shown above). This CDN URL (e.g., http://adn.0001.edgecastcdn.net/800001/banking) points to the root folder of your customer origin server. To provide a link to your content, simply append the relative path to the desired asset to this URL (e.g., http://adn.0001.edgecastcdn.net/800001/banking**/web/main.aspx**).

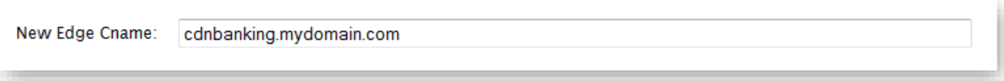
8. Make sure that the IP addresses listed at the bottom of the page are allowed access to your server.

Important: It may take up to an hour before you will be able to access content on your customer origin server through our CDN.

To create a user-friendly URL to an external server

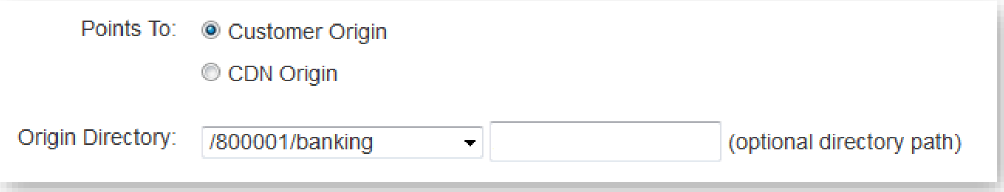
Note: This optional procedure should only be performed if you would like to provide a user-friendly URL for your users.

1. Navigate to the Edge CNAMEs page.
2. In the **New Edge Cname** option, type the name of the domain that will be used to reference the customer origin configuration created above. The CNAME should be specified in lower-case letters and should not include a protocol (i.e., http://).



New Edge Cname: cdnbanking.mydomain.com

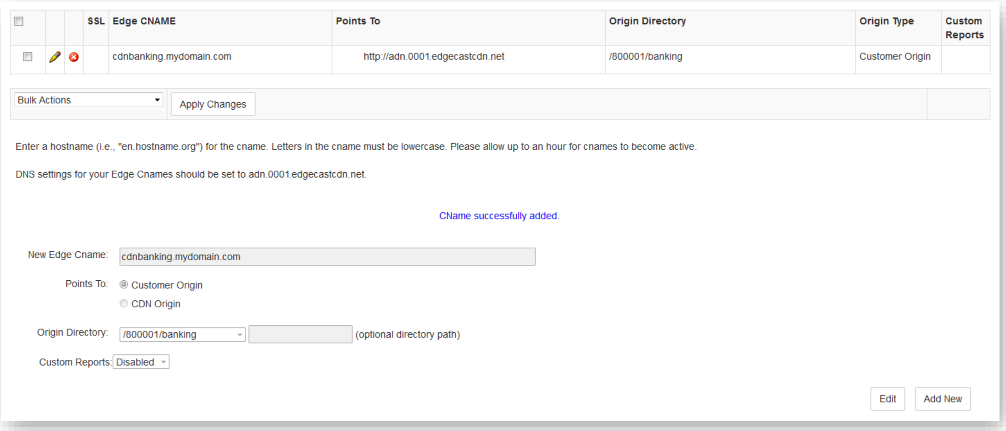
3. In the **Points to** option, select "Customer Origin."
4. In the **Origin Directory** option, select the recently created customer origin configuration.



Points To: ● Customer Origin ○ CDN Origin

Origin Directory: /800001/banking (optional directory path)

5. Click **Add**. An edge CNAME that points to your recently created customer origin configuration should appear at the top of the **Edge CNAMEs** page.



□			SSL	Edge CNAME	Points To	Origin Directory	Origin Type	Custom Reports
□				cdnbanking.mydomain.com	http://adn.0001.edgecastcdn.net	/800001/banking	Customer Origin	

Enter a hostname (i.e., "en.hostname.org") for the cname. Letters in the cname must be lowercase. Please allow up to an hour for cnames to become active.

DNS settings for your Edge Cnames should be set to adn.0001.edgecastcdn.net.

CName successfully added.

New Edge Cname: cdnbanking.mydomain.com

Points To: ● Customer Origin ○ CDN Origin

Origin Directory: /800001/banking (optional directory path)

Custom Reports: Disabled

6. Register a CNAME record on a DNS server. This CNAME should point the domain (e.g., cdnbanking.mydomain.com), which was specified in step 2, to the CDN domain (e.g., adn.0001.edgecastcdn.net). You will not be able to use this edge CNAME URL until this step is completed.

Important: It may take up to an hour after creating an edge CNAME configuration before you will be able to access your content using an edge CNAME URL.

How to Access Content via ADN

Your content can be accelerated via ADN by linking to it using a CDN or an edge CNAME URL listed on the Application Delivery Network page. This will require that you append a relative path to the CDN or edge CNAME URL. Typically, the starting point for this relative path is the root folder of the desired server.

Sample URLs are provided below.

- **CDN URL:** http://adn.*xxxx*.edgecastcdn.net/00*xxxx*/web/main.aspx
- **Edge CNAME URL:** http://cdnbanking.mydomain.com/web/main.aspx

Both of the above sample URLs point to an asset called "index.html," which can be found in the "web" folder. The "web" folder is a subfolder off the root folder of the customer origin server.

Tip: In order to improve a web site's performance, you should update the links referenced in src attributes. If you would also like to speed up linked content, then you should update the links referenced in href attributes as well.

Web Application Firewall

Introduction

Our Web Application Firewall (WAF) offering is designed to secure site traffic against malicious and unwanted traffic. The core methods through which it secures site traffic are listed below.

- Leverages our distributed worldwide network to provide protection against large-scale distributed denial of service (DDoS) attacks.
- Screens traffic for the purpose of identifying application layer attacks.
- Filters traffic by defining access controls and predefined security screening rules.
- Restricts the rate at which requests may flow to your application.

Setup Overview

Setting up WAF consists of:

1. Creating rules that define a security policy.
    - **Access Rules:** Use an access rule to identify traffic that should be allowed, denied, or screened through whitelists, accesslists, and blacklists.
    - **Rate Rules:** Use a rate rule to restrict the flow of traffic to your application.
    - **Bot Rules:** Use a bot rule to block traffic generated by basic bots.
    - **Custom Rules:** Use a custom rule to define custom criteria for identifying threats.
    - **Managed Rules:** Use a managed rule to leverage predefined rules to detect application layer attacks.
2. Creating a Security Application Manager configuration that identifies the security policy that will be applied to your application.
3. Monitoring threats to site traffic through the WAF dashboard.

A walkthrough is provided for each of the above steps.

Step 1: Create Rules

Step-by-step instructions on how to create an access rule, rate rule, and managed rule are provided below.

Tip: Create a custom rule to identify threats using custom criteria that takes into account your site's traffic profile to avoid false positives.

Create an Access Rule

Create an access rule that identifies traffic that should be allowed, denied, or screened through whitelists, accesslists, and blacklists.

1. Navigate to the **Access Rules** page. From the main menu, navigate to **More** | **WAF** | **WAF *Tier*** | **Security Rule Manager** | **Access Rules**.
2. Click **Add Access Rule**.
3. In the **Name** option, type "My Access Rule".
4. From the **Add an Access Control** option, select **IP**.
5. Click **Add Blacklist**.
6. Specify an IP address from which suspicious traffic originates.
7. Click **Save**.

Create a Rate Rule

Use a rate rule to restrict the flow of traffic to your application.

1. Navigate to the **Rate Rules** page. From the main menu, navigate to **More** | **WAF** | **WAF *Tier*** | **Security Rule Manager** | **Rate Rules**.
2. Click **Add Rate Rule**.
3. In the **Rule name** option, type "My Rate Limit."
4. In the **Apply rate limit to** option, select **IP address**.
5. In the **Rate limit** section, set the **Number of requests** option to **100** and the **Time period** option to **1 minute**.
6. Click **Save**.

Create a Managed Rule

Create a managed rule that leverages predefined rules to detect application layer attacks.

1. Navigate to the **Managed Rules** page. From the main menu, navigate to **More** | **WAF** | **WAF *Tier*** | **Security Rule Manager** | **Managed Rules**.
2. Click **Add Managed Rule**.
3. In the **Name** option, type "My Managed Rule."
4. Click the **Policies** tab. In the **Ruleset** option, select **ECRS 2020-11-02**.
5. Set the **Threshold** option to **5**.
6. Set the **Paranoia Level** option to **1**.
7. From the **Policies** section, disable policies that do not apply to your application. For example, you may safely disable Adv Drupal, Adv SharePoint, and Adv WordPress if your application does not leverage those platforms.
8. Click **Save**.

Step 2: Create a Security Application Manager Configuration

Step-by-step instructions on how to create a Security Application Manager configuration that identifies the security policy that will be applied to your application are provided below.

1. Navigate to the **Security Application Manager** page. From the main menu, navigate to **More** | **WAF** | **WAF *Tier*** | **Security Application Manager**.
2. Click **Add New**.
3. In the **Name** option, type "My Application."
4. From the **Rules** section, click **Access Rule**.
5. From the **Production Access Rule** option, select **My Access Rule**.
6. From the **Action type** option, select **Alert only**.
7. From the **Rules** section, click **Managed Rule**.
8. From the **Production Managed Rule** option, select **My Rate Limit**.
9. From the **Action type** option, select **Alert only**.
10. From the **Rules** section, click **Rate Rules**.
11. From the **Add Rate Rule** option, select **My Managed Rule**.
12. From the **Action type** option, select **Drop request (429 Too Many Requests)**.
13. Click **Save**.

Step 3: Monitor Threats

The Threats dashboard illustrates threat detection trends and lists recent illegitimate requests. This dashboard is a useful tool for:

- Verifying that a newly activated instance/profile will not impact legitimate traffic.
- Analyzing threats directed to your site.

Note: By default, the dashboard tracks the set of threats detected over the last week.

Data Gathering

After an instance has been activated, time needs to pass to allow WAF to gather sufficient data from which trends may be detected.

Wait a reasonable amount of time (e.g., 24 hours) after setting up a Security Application Manager configuration.

Navigate to the Threats Dashboard

View graphs and detailed alert data from the Threats dashboard.

Navigate to the **Threats Dashboard** page. From the main menu, navigate to **More** | **WAF** | **WAF *Tier*** | **Dashboard**.

Review Trends

The dashboard's graph provides insight into trends at a glance.

Review the graph at the top of the dashboard. Check for an abnormally high number of detected threats.

Analyze Individual Threats

It is useful to view detailed information on detected threats to ensure that WAF is correctly identifying threats.

1. Click the ☰ icon from the upper-right hand side of the window.
2. Click on each alert to view detailed information on it.
    - Pay special attention to the requested URL. Verify that it is an illegitimate request.
    - If an alert was generated for a legitimate request, then review the **Rule Tags**, **Matched On**, and **Matched Value** fields to see why the request was flagged.
        - Check whether the web application may be changed to prevent this type of request from occurring.
        - Our recommendation is that all of the following conditions be met before disabling a rule:
            - Your application cannot be updated to reduce false positives.
            - A rule exception cannot be created to eliminate false positives.
            - A significant number of requests will be impacted by this rule,

        Note: You may safely disable a threat detection policy if it secures a platform (e.g., Drupal, SharePoint, and WordPress) that is not leveraged by your application.

        If you must disable a rule, then note the values for the Rule Tags and Rule ID fields.

            - The Rule Tags field identifies the threat detection policy.
            - Look for the rule ID defined in the Rule ID fields within your managed rule's policy. Disable that rule.

            Tip: You may filter rules by ID when viewing a managed rule's policy.

Further Assistance

Resources

Thank you for allowing us to help you set up a basic configuration of our CDN platforms/services. If you have additional questions or if you are looking for information on the additional features that our CDN provides, please make sure to check with one of the following resources:

- **Help Library:** Learn about our services and features through our:
    - CDN Help Center
    - REST API Help Center
    - Route Help Center
    - Alternatively, download platform/service-specific PDF documents from our CDN Help Center.
- **Live Assistance:** Your CDN account manager is happy to assist with any questions you may have about our platforms/services. If you are unsure of who manages your CDN account, then call us at 1-877-Edge-CDN (1-877-3343-236).