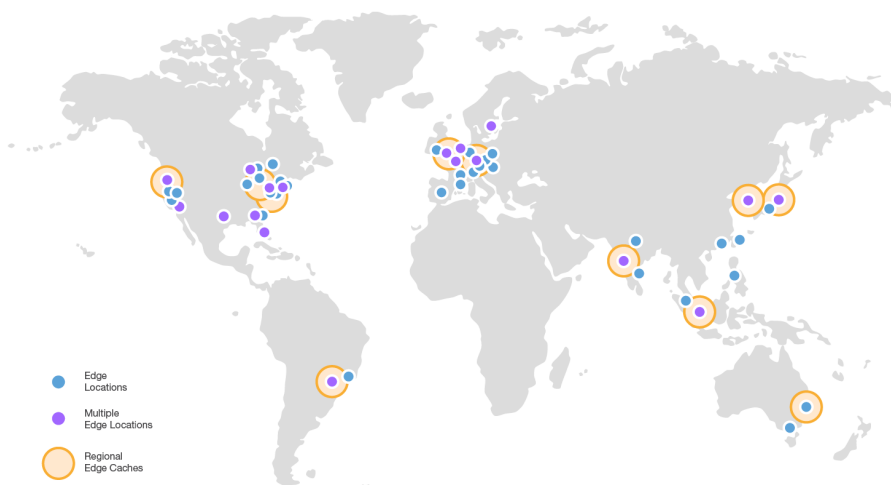


# Amazon CloudFront Edge Infrastructure

## The Amazon CloudFront Global Edge Network

To deliver content to end users with lower latency, Amazon CloudFront uses a global network of **100 Points of Presence (89 Edge Locations and 11 Regional Edge Caches)** in 50 cities across 23 countries. Amazon CloudFront edge locations are located in:



## North America

**Edge Locations:** Ashburn, VA (3); Atlanta, GA (3); Boston, MA; Chicago, IL (2); Dallas/Fort Worth, TX (4); Hayward, CA; Jacksonville, FL; Los Angeles, CA (2); Miami, FL (2); Minneapolis, MN; Montreal, QC; New York, NY (3); Newark, NJ; Palo Alto, CA; Philadelphia, PA; San Jose, CA; Seattle, WA (3); South Bend, IN; St. Louis, MO; Toronto, ON

**Regional Edge Caches:** Virginia; Ohio; Oregon

## Europe

**Edge Locations:** Amsterdam, The Netherlands (2); Berlin, Germany; Dublin, Ireland; Frankfurt, Germany (6); London, England (5); Madrid, Spain; Marseille, France; Milan, Italy; Munich, Germany; Paris, France (3);



re:Invent 2016: Introduction to Amazon Global Network and CloudFront PoPs with James Hamilton

Prague, Czech Republic; Stockholm, Sweden (3); Vienna, Austria;  
Warsaw, Poland; Zurich, Switzerland

**Regional Edge Caches:** Frankfurt, Germany; London, England

## Asia

**Edge Locations:** Chennai, India; Hong Kong, China (3); Kuala Lumpur, Malaysia; Mumbai, India (2); Manila, Philippines; New Delhi, India; Osaka, Japan; Seoul, Korea (3); Singapore (2); Taipei, Taiwan; Tokyo, Japan (5)

**Regional Edge Caches:** Mumbai, India; Singapore; Seoul, South Korea; Tokyo, Japan

## Australia

**Edge Locations:** Melbourne, Australia; Sydney, Australia

**Regional Edge Caches:** Sydney, Australia

## South America

**Edge Locations:** São Paulo, Brazil (2); Rio de Janeiro, Brazil

**Regional Edge Caches:** São Paulo, Brazil

---

# Key Features

## Dynamic and Customized Content

You can use Amazon CloudFront to deliver all of your content, including the dynamic portions of your site that change for each end-user. With CloudFront, you can configure multiple origin servers and multiple cache behaviors based on URL path patterns on your website. You can also configure a minimum expiration period (also known as “time-to-live” or TTL) to as short as 0 seconds, detect user requests based on the device used and the country where the end user is accessing your content from (geo targeting), and specify which query string parameters, cookies, or standard HTTP request headers you want to forward to your custom (non-S3) origin server. In addition, the integration with

## Security Features

You can configure Amazon CloudFront to enforce end-to-end HTTPS connections from your viewer to your origin. The integration between CloudFront and [AWS Certificate Manager](#) allows you to create free custom SSL certificates or bring your own and deploy them in minutes. CloudFront supports advanced protocols and ciphers, and advanced SSL features, such as Session Tickets, OCSP Stapling, and Perfect Forward Secrecy. With CloudFront, you can also securely serve private content by using signed URLs, signed cookies (trusted signers), and use [Origin Access Identity \(OAI\)](#) to restrict access to your Amazon S3 bucket. CloudFront also integrates with [AWS WAF](#), a web application firewall that helps

[Lambda@Edge](#) allows you to customize or personalize content for your end users close to where they're located by writing [AWS Lambda](#) functions deployed to the global CloudFront network and execute these functions in response to CloudFront events.

## Streaming Features

Amazon CloudFront supports multiple protocols for media (audio and video – both on-demand and live) streaming. You can use CloudFront to deliver [on-demand video](#) using the Microsoft Smooth Streaming or the HLS formats without the need to setup or operate any media servers. You can also use CloudFront to deliver live media using Adobe Media Server, Window Media Services, or Wowza Media Server. CloudFront integrates with [AWS Elemental](#) Cloud's video processing and delivery services, including [Amazon Elastic Transcoder](#), a service that allows you to convert your mezzanine (or master) media files stored in [Amazon S3](#) to various formats depending on the devices your viewers will be using to play it.

protect web applications from common web exploits, and [AWS Shield](#), a managed DDoS protection service that safeguards web applications running on AWS. All CloudFront customers benefit from the automatic protections of AWS Shield Standard, at no additional charge. CloudFront is a PCI DSS compliant and [HIPAA eligible service](#) and allows you to log configuration changes to your distributions through [AWS CloudTrail](#) for auditing purposes.

## Reporting and Analytics

Amazon CloudFront offers a variety of solutions for your reporting needs, whether it's receiving detailed cache statistics reports, monitoring your CloudFront usage in near real-time with [Amazon CloudWatch](#), tracking your most popular objects, setting alarms on operational metrics, or learning more about your end users and which domains referred them to your website. You can also choose to receive information about traffic delivered by your CloudFront distribution by enabling CloudFront access logs for no additional cost. [Learn more about CloudFront Reporting and Analytics.](#)

[Explore the Amazon CloudFront Developer Guide for more details >>](#)

---

# Amazon CloudFront FAQs

---

## General

### Q. What is Amazon CloudFront?

Amazon CloudFront is a web service that gives businesses and web application developers an easy and cost effective way to distribute content with low latency and high data transfer speeds. Like other AWS services, Amazon CloudFront is a self-service, pay-per-use offering, requiring no long term commitments or minimum fees. With CloudFront, your files are delivered to end-users using a global network of edge locations.

## Q. What can I do with Amazon CloudFront?

Amazon CloudFront provides a simple API that lets you:

Distribute content with low latency and high data transfer rates by serving requests using a network of edge locations around the world.

Get started without negotiating contracts and minimum commitments.

## Q. How do I get started with Amazon CloudFront?

Click the “Create Free Account” button on the Amazon CloudFront detail page. If you choose to use another AWS service as the origin for the files served through Amazon CloudFront, you must [sign up](#) for that service before creating CloudFront distributions.

## Q. How do I use Amazon CloudFront?

To use Amazon CloudFront, you:

- For static files, store the definitive versions of your files in one or more origin servers. These could be Amazon S3 buckets. For your dynamically generated content that is personalized or customized, you can use Amazon EC2 – or any other web server – as the origin server. These origin servers will store or generate your content that will be distributed through Amazon CloudFront.
- Register your origin servers with Amazon CloudFront through a simple API call. This call will return a CloudFront.net domain name that you can use to distribute content from your origin servers via the Amazon CloudFront service. For instance, you can register the Amazon S3 bucket “bucketname.s3.amazonaws.com” as the origin for all your static content and an Amazon EC2 instance “dynamic.myoriginserver.com” for all your dynamic content. Then, using the API or the AWS Management Console, you can create an Amazon CloudFront distribution that might return “abc123.cloudfront.net” as the distribution domain name.
- Include the cloudfront.net domain name, or a CNAME alias that you create, in your web application, media player, or website. Each request made using the cloudfront.net domain name (or the CNAME you set-up) is routed to the edge location best suited to deliver the content with the highest performance. The edge location will attempt to serve the request with a local copy of the file. If a local copy is not available, Amazon CloudFront will get a copy from the origin. This copy is then available at that edge location for future requests.

## Q. How does Amazon CloudFront provide higher performance?

Amazon CloudFront employs a global network of edge locations and regional edge caches that cache copies of your content close to your viewers. Amazon CloudFront ensures that end-user requests are served by the closest edge location. As a result, viewer requests travel a short distance, improving performance for your viewers. For files not cached at the edge locations and the regional edge caches, Amazon CloudFront keeps persistent connections with your origin servers so that those files can be fetched from the origin servers as quickly as possible. Finally, Amazon CloudFront uses additional optimizations – e.g. wider TCP initial congestion window – to provide higher performance while delivering your content to viewers.

## Q. How does Amazon CloudFront lower my costs to distribute content over the Internet?

Like other AWS services, Amazon CloudFront has no minimum commitments and charges you only for what you use. Compared to self-hosting, Amazon CloudFront spares you from the expense and complexity of

operating a network of cache servers in multiple sites across the internet and eliminates the need to over-provision capacity in order to serve potential spikes in traffic. Amazon CloudFront also uses techniques such as collapsing simultaneous viewer requests at an edge location for the same file into a single request to your origin server. This reduces the load on your origin servers reducing the need to scale your origin infrastructure, which can bring you further cost savings.

Additionally, if you are using an AWS origin (e.g., Amazon S3, Amazon EC2, etc.), effective December 1, 2014, **we are no longer charging for AWS data transfer out to Amazon CloudFront**. This applies to data transfer from all AWS regions to all global CloudFront edge locations.

#### **Q. How does Amazon CloudFront speed up my entire website?**

Amazon CloudFront uses standard cache control headers you set on your files to identify static and dynamic content. Delivering all your content using a single Amazon CloudFront distribution helps you make sure that performance optimizations are applied to your entire website or web application. When using AWS origins, you benefit from improved performance, reliability, and ease of use as a result of AWS's ability to track and adjust origin routes, monitor system health, respond quickly when any issues occur, and the integration of Amazon CloudFront with other AWS services. You also benefit from using different origins for different types of content on a single site – e.g. Amazon S3 for static objects, Amazon EC2 for dynamic content, and custom origins for third-party content – paying only for what you use.

#### **Q. How is Amazon CloudFront different from Amazon S3?**

Amazon CloudFront is a good choice for distribution of frequently accessed static content that benefits from edge delivery—like popular website images, videos, media files or software downloads.

#### **Q. How is Amazon CloudFront different from traditional content delivery solutions?**

Amazon CloudFront lets you quickly obtain the benefits of high performance content delivery without negotiated contracts or high prices. Amazon CloudFront gives all developers access to inexpensive, pay-as-you-go pricing – with a self-service model. Developers also benefit from tight integration with other Amazon Web Services. The solution is simple to use with Amazon S3, Amazon EC2, and Elastic Load Balancing as origin servers, giving developers a powerful combination of durable storage and high performance delivery. Amazon CloudFront also integrates with Amazon Route 53 and AWS CloudFormation for further performance benefits and ease of configuration.

#### **Q. What types of content does Amazon CloudFront support?**

Amazon CloudFront supports all files that can be served over HTTP. This includes dynamic web pages, such as HTML or PHP pages, any popular static files that are a part of your web application, such as website images, audio, video, media files or software downloads. For on-demand media files, you can also choose to stream your content using RTMP delivery. Amazon CloudFront also supports delivery of live media over HTTP.

#### **Q. Does Amazon CloudFront support delivery of dynamic content?**

Amazon CloudFront supports all files that can be served over HTTP. This includes dynamic web pages, such as HTML or PHP pages, any popular static files that are a part of your web application, such as website images, audio streams, video streams, media files or software downloads. For on-demand media files, you can also choose to stream your content using RTMP delivery. Amazon CloudFront also supports delivery of live media over HTTP.

#### **Q. Does Amazon CloudFront work with non-AWS origin servers?**

Yes. Amazon CloudFront works with any origin server that holds the original, definitive versions of your content, both static and dynamic. There is no additional charge to use a custom origin.

**Q: Does Amazon CloudFront offer a Service Level Agreement (SLA)?**

Yes. The Amazon CloudFront SLA provides for a service credit if a customer's monthly uptime percentage is below our service commitment in any billing cycle. More information can be found [here](#).

**Q: Can I use the AWS Management Console with Amazon CloudFront?**

Yes. You can use the AWS Management Console to configure and manage Amazon CloudFront through a simple, point-and-click web interface. The AWS Management Console supports most of Amazon CloudFront's features, letting you get Amazon CloudFront's low latency delivery without writing any code or installing any software. Access to the AWS Management Console is provided free of charge at <https://console.aws.amazon.com>.

**Q: What tools and libraries work with Amazon CloudFront?**

There are a variety of tools for managing your Amazon CloudFront distribution and libraries for various programming languages available in our [resource center](#).

**Q. Can I point my zone apex (example.com versus www.example.com) at my Amazon CloudFront distribution?**

Yes. By using Amazon Route 53, AWS's authoritative DNS service, you can configure an 'Alias' record that lets you map the apex or root (example.com) of your DNS name to your Amazon CloudFront distribution. Amazon Route 53 will then respond to each request for an Alias record with the right IP address(es) for your CloudFront distribution. Route 53 doesn't charge for queries to Alias records that are mapped to a CloudFront distribution. These queries are listed as "Intra-AWS-DNS-Queries" on the Amazon Route 53 usage report.

## Edge Locations

**Q. What is CloudFront Regional Edge Cache?**

A default CloudFront feature that brings more of your content close to your viewers, even when the content is not popular to stay at a particular edge location. This helps improve performance for your viewers while lowering the operational burden and cost of scaling your origin resources.

**Q. How does regional edge cache work?**

Amazon CloudFront has added several regional edge cache locations globally, at close proximity to your viewers. These locations sit in between your origin webserver and the global edge locations that serve traffic directly to your viewers. As the popularity of your objects reduce, individual edge locations may evict those objects to make room for more popular content. Regional Edge Caches have larger cache width than any individual edge location, so objects remain in cache longer at these regional edge caches. This helps keep more of your content closer to your viewers, reducing the need for CloudFront to go back to your origin webserver and improving overall performance for viewers. For instance, our edge locations in Europe now go to the regional edge cache in Frankfurt to fetch an object before going back to your origin webserver. Regional Edge Cache locations are currently utilized only for requests that need to go back to a custom origin; i.e. requests to S3 origins will skip regional edge cache locations.

**Q. Is regional edge cache feature enabled by default?**

Yes. You do not need to make any changes to your CloudFront distributions; this feature is enabled by default for all new and existing CloudFront distributions. There are no additional charges to use this feature.

#### **Q. Where are the edge network locations used by Amazon CloudFront located?**

Amazon CloudFront uses a global network of edge locations and regional edge caches for content delivery. You can see a full list of Amazon CloudFront locations [here](#).

#### **Q. Can I choose to serve content (or not serve content) to specified countries?**

Yes, the Geo Restriction feature lets you specify a list of countries in which your users can access your content. Alternatively, you can specify the countries in which your users cannot access your content. In both cases, CloudFront responds to a request from a viewer in a restricted country with an HTTP status code 403 (Forbidden).

#### **Q. How accurate is your GeoIP database?**

The accuracy of the IP Address to country lookup database varies by region. Based on recent tests, our overall accuracy for the IP address to country mapping is 99.8%.

#### **Q. Can I serve a custom error message to my end users?**

Yes, you can create custom error messages (for example, an HTML file or a .jpg graphic) with your own branding and content for a variety of HTTP 4xx and 5xx error responses. Then you can configure Amazon CloudFront to return your custom error messages to the viewer when your origin returns one of the specified errors to CloudFront.

#### **Q. How long will Amazon CloudFront keep my files at the edge locations?**

By default, if no cache control header is set, each edge location checks for an updated version of your file whenever it receives a request more than 24 hours after the previous time it checked the origin for changes to that file. This is called the “expiration period.” You can set this expiration period as short as 0 seconds, or as long as you’d like, by setting the cache control headers on your files in your origin. Amazon CloudFront uses these cache control headers to determine how frequently it needs to check the origin for an updated version of that file. For expiration period set to 0 seconds, Amazon CloudFront will revalidate every request with the origin server. If your files don’t change very often, it is best practice to set a long expiration period and implement a versioning system to manage updates to your files.

#### **Q. How do I remove an item from Amazon CloudFront edge locations?**

There are multiple options for removing a file from the edge locations. You can simply delete the file from your origin and as content in the edge locations reaches the expiration period defined in each object’s HTTP header, it will be removed. In the event that offensive or potentially harmful material needs to be removed before the specified expiration time, you can use the Invalidation API to remove the object from all Amazon CloudFront edge locations. You can see the charge for making invalidation requests [here](#).

#### **Q. Is there a limit to the number of invalidation requests I can make?**

If you're invalidating objects individually, you can have invalidation requests for up to 3,000 objects per distribution in progress at one time. This can be one invalidation request for up to 3,000 objects, up to 3,000 requests for one object each, or any other combination that doesn't exceed 3,000 objects.

If you're using the \* wildcard, you can have requests for up to 15 invalidation paths in progress at one time. You can also have invalidation requests for up to 3,000 individual objects per distribution in progress at the same time; the limit on wildcard invalidation requests is independent of the limit on invalidating objects



individually. If you exceed this limit, further invalidation requests will receive an error response until one of the earlier request completes.

You should use invalidation only in unexpected circumstances; if you know beforehand that your files will need to be removed from cache frequently, it is recommended that you either implement a versioning system for your files and/or set a short expiration period.

## Compliance

### Q. Is Amazon CloudFront PCI compliant?

Yes, Amazon CloudFront is included in the set of services that are compliant with the Payment Card Industry Data Security Standard (PCI DSS) Merchant Level 1, the highest level of compliance for service providers. Please see our [developer's guide](#) for more information.

### Q. Is Amazon CloudFront HIPAA eligible?

Yes, AWS has expanded its HIPAA compliance program to include Amazon CloudFront as a HIPAA eligible service. If you have an executed Business Associate Agreement (BAA) with AWS, you can use Amazon CloudFront to accelerate the delivery of protected health information (PHI). For more information, see [HIPAA Compliance](#) and our [developer's guide](#).

## HTTP and HTTP/2

### Q. What types of HTTP requests are supported by Amazon CloudFront?

Amazon CloudFront currently supports GET, HEAD, POST, PUT, PATCH, DELETE and OPTIONS requests.

### Q. Does Amazon CloudFront cache POST responses?

Amazon CloudFront does not cache the responses to POST, PUT, DELETE, and PATCH requests – these requests are proxied back to the origin server. You may enable [caching](#) for the responses to OPTIONS requests.

### Q. How do I use HTTP/2?

If you have an existing Amazon CloudFront distribution, you can turn on HTTP/2 using the API or the Management Console. In the Console, go to the "Distribution Configuration" page and navigate to the section "Supported HTTP Versions." There, you can select "HTTP/2, HTTP/1.1, or HTTP/1.0". HTTP/2 is automatically enabled for all new CloudFront distributions.

### Q. What if my origin does not support HTTP/2?

Amazon CloudFront currently supports HTTP/2 for delivering content to your viewers' clients and browsers. For communication between the edge location and your origin servers, Amazon CloudFront will continue to use HTTP/1.1.

### Q. Does Amazon CloudFront support HTTP/2 without TLS?

Not currently. However, most of the modern browsers support HTTP/2 only over an encrypted connection. You can learn more about using SSL with Amazon CloudFront [here](#).



# Security

## Q. Can I configure my CloudFront distribution to deliver content over HTTPS using my own domain name?

By default, you can deliver your content to viewers over HTTPS by using your CloudFront distribution domain name in your URLs, for example, <https://dxxxxx.cloudfront.net/image.jpg>. If you want to deliver your content over HTTPS using your own domain name and your own SSL certificate, you can use one of our Custom SSL certificate support features. [Learn more.](#)

## Q. What is the difference between SNI Custom SSL and Dedicated IP Custom SSL of Amazon CloudFront?

**Dedicated IP Custom SSL** allocates dedicated IP addresses to serve your SSL content at each CloudFront edge location. Because there is a one to one mapping between IP addresses and SSL certificates, Dedicated IP Custom SSL works with browsers and other clients that do not support SNI. Due to the current IP address costs, Dedicated IP Custom SSL is \$600/month prorated by the hour.

**SNI Custom SSL** relies on the SNI extension of the Transport Layer Security protocol, which allows multiple domains to serve SSL traffic over the same IP address by including the hostname viewers are trying to connect to. As with Dedicated IP Custom SSL, CloudFront delivers content from each Amazon CloudFront edge location and with the same security as the Dedicated IP Custom SSL feature. SNI Custom SSL works with most modern browsers, including Chrome version 6 and later (running on Windows XP and later or OS X 10.5.7 and later), Safari version 3 and later (running on Windows Vista and later or Mac OS X 10.5.6. and later), Firefox 2.0 and later, and Internet Explorer 7 and later (running on Windows Vista and later). Older browsers that do not support SNI cannot establish a connection with CloudFront to load the HTTPS version of your content. SNI Custom SSL is available at no additional cost beyond standard CloudFront data transfer and request fees.

## Q. What is Server Name Indication?

Server Name Indication (SNI) is an extension of the Transport Layer Security (TLS) protocol. This mechanism identifies the domain (server name) of the associated SSL request so the proper certificate can be used in the SSL handshake. This allows a single IP address to be used across multiple servers. SNI requires browser support to add the server name, and while most modern browsers support it, there are a few legacy browsers that do not. For more details see the SNI section of the [CloudFront Developer Guide](#) or the [SNI Wikipedia article](#).

## Q. Does CloudFront Integrate with AWS Certificate Manager?

Yes, you can now provision SSL/TLS certificates and associate them with CloudFront distributions within minutes. Simply provision a certificate using the new AWS Certificate Manager (ACM) and deploy it to your CloudFront distribution with a couple of clicks, and let ACM manage certificate renewals for you. ACM allows you to provision, deploy, and manage the certificate with no additional charges.

Note that CloudFront still supports using certificates that you obtained from a third-party certificate authority and uploaded to the IAM certificate store.

## Q. Does Amazon CloudFront support access controls for paid or private content?

Yes, Amazon CloudFront has an optional private content feature. When this option is enabled, Amazon CloudFront will only deliver files when you say it is okay to do so by securely signing your requests. Learn more about this feature by reading the [CloudFront Developer Guide](#).

## Q. How can I safeguard my web applications delivered via CloudFront from DDoS attacks?

As an AWS customer, you get **AWS Shield Standard** at no additional cost. AWS Shield is a managed service that provides protection against DDoS attacks for web applications running on AWS. AWS Shield Standard provides protection for all AWS customers against common and most frequently occurring Infrastructure (layer 3 and 4) attacks like SYN/UDP Floods, Reflection attacks, and others to support high availability of your applications on AWS.

**AWS Shield Advanced** is an optional paid service available to AWS Business Support and AWS Enterprise Support customers. AWS Shield Advanced provides additional protections against larger and more sophisticated attacks for your applications running on Elastic Load Balancing (ELB), Amazon CloudFront and Route 53.

#### Q. How can I protect my web applications delivered via CloudFront?

You can integrate your CloudFront distribution with **AWS WAF**, a web application firewall that helps protect web applications from attacks by allowing you to configure rules based on IP addresses, HTTP headers, and custom URI strings. Using these rules, AWS WAF can block, allow, or monitor (count) web requests for your web application. Please see [AWS WAF Developer Guide](#) for more information.

## Caching

#### Q. Can I add or modify request headers forwarded to the origin?

Yes, you can configure Amazon CloudFront to add custom headers, or override the value of existing headers, to requests forwarded to your origin. You can use these headers to help validate that requests made to your origin were sent from CloudFront; you can even configure your origin to only allow requests that contain the custom header values you specify. Additionally, if you use multiple CloudFront distributions with the same origin, you can use custom headers to distinguish origin request made by each different distribution. Finally, custom headers can be used to help determine the right CORS headers returned for your requests. You can configure custom headers via the CloudFront API and the AWS Management Console. There are no additional charges for this feature. For more details on how to set your custom headers, you can read more [here](#).

#### Q. How does Amazon CloudFront handle HTTP cookies?

Amazon CloudFront supports delivery of dynamic content that is customized or personalized using HTTP cookies. To use this feature, you specify whether you want Amazon CloudFront to forward some or all of your cookies to your custom origin server. Amazon CloudFront then considers the forwarded cookie values when identifying a unique object in its cache. This way, your end users get both the benefit of content that is personalized just for them with a cookie and the performance benefits of Amazon CloudFront. You can also optionally choose to log the cookie values in Amazon CloudFront access logs.

#### Q. How does Amazon CloudFront handle query string parameters in the URL?

A query string may be optionally configured to be part of the cache key for identifying objects in the Amazon CloudFront cache. This helps you build dynamic web pages (e.g. search results) that may be cached at the edge for some amount of time.

#### Q. Can I specify which query parameters to use in the cache key?

Yes, query string whitelisting feature allows you to easily configure Amazon CloudFront to only use certain parameters in the cache key, while still forwarding all the parameters to the origin.

#### Q. Is there a limit to the number of query parameters that can be whitelisted?

Yes, you can configure Amazon CloudFront to whitelist up to 10 query parameters.

#### **Q. What parameter types are supported?**

Amazon CloudFront supports URI query parameters as defined in section 3.4 of RFC3986. Specifically, it supports query parameters embedded in an HTTP GET string after the '?' character, and delimited by the '&' character.

#### **Q. Does CloudFront support gzip compression?**

Yes, CloudFront will automatically compress your text or binary data. To use the feature, simply specify within your cache behavior settings that you would like CloudFront to compress objects automatically and ensure that your client adds Accept-Encoding: gzip in the request header (most modern web browser do this by default)..For more information on this feature, please refer to [our developer guide](#).

## Streaming

#### **Q. What is streaming? Why would I want to stream my content?**

Generally, streaming refers to delivering audio and video to end users on the internet without having to download the media file prior to playback. The protocols used for streaming include proprietary ones such as Adobe's Real Time Messaging Protocol (RTMP) and those that use HTTP for delivery such as Apple's HTTP Live Streaming (HLS), Adobe's HTTP Dynamic Streaming (HDS) and Microsoft's Smooth Streaming. These protocols are different than the delivery of web pages and other content because streaming protocols deliver content in real time – the viewers watch the bytes as they are delivered. Streaming content has several potential benefits for you and your end-users:

- Streaming can give viewers more control over their viewing experience. For instance, it is easier for a viewer to seek forward in a video using streaming than using traditional download delivery.
- Streaming can give you more control over your content, as no file remains on the viewer's computer when they finish watching a video.
- Streaming can help you reduce your costs, as it only delivers portions of a media file that the viewers actually watch. In contrast, with traditional downloads, frequently the whole media file will be downloaded by the viewers, even if they only watch a portion of the file.

#### **Q. Does Amazon CloudFront support on-demand streaming protocols?**

Yes, Amazon CloudFront provides you with multiple options to deliver on-demand content. If you have media files that have been converted to either HLS format or Microsoft Smooth Streaming format prior to storing in Amazon S3 (or a custom origin), you can use an Amazon CloudFront web distribution to stream in that format without having to run any media servers. In addition you can also run a third party streaming server (e.g. Wowza Media Server available on AWS Marketplace) on Amazon EC2 which can convert a media file to the required HTTP streaming format. This server can then be designated as the origin for an Amazon CloudFront web distribution. Another option, if you want to stream using RTMP, is to store your media files on Amazon S3 and use it as the origin for an Amazon CloudFront RTMP distribution.

#### **Q. Does Amazon CloudFront support live streaming to multiple platforms?**

Yes. Amazon CloudFront provides you three options to easily and cost-effectively deliver live events over HTTP to multiple platforms:

**Live Streaming using Wowza Media Server 3.6:** Using Amazon CloudFront with Wowza Media Server combines the benefits of Wowza Media Server with the reliability, scalability, low latency and cost-efficiency of Amazon CloudFront to stream live events to multiple streaming formats, including Apple HTTP Live Streaming (HLS), Adobe HTTP Dynamic Streaming (HDS) and Microsoft Smooth Streaming. We've made this simple for you by creating an AWS CloudFormation template that handles all of the provisioning and sequencing for all the AWS resources you need for this live streaming stack. Amazon CloudFront provides you the scale and flexible pay-as-you-go pricing model, while the use of HTTP protocols for streaming your live event offers your viewers easy access to your live content. Using Amazon CloudFront for live streaming also gives you full control of your Wowza origin server so you can configure it to best work with the specific nature of your event. In addition, you can choose the Amazon EC2 instance type and AWS region that best meet the needs of your live event. A detailed tutorial for setting-up live HTTP streaming using Amazon CloudFront is available [here](#).

**Live Streaming using Adobe Media Server 5.0:** Amazon CloudFront can be used with Amazon EC2 running Adobe Media Server (AMS 5.0) for live HTTP streaming to both Flash Player and Apple iOS devices. Amazon EC2 (running AMS 5.0) must be configured as the origin for a CloudFront web distribution. Similar to our other live streaming solutions we have setup an AWS CloudFormation template to make it easy for you to setup your pay-as-you-go streaming stack while providing you with full control of the AMS server running in the Amazon EC2 instances provisioned. A detailed tutorial (which also points to the AWS CloudFormation templates) for setting-up live HTTP streaming using CloudFront and AMS 5.0 is available [here](#).

**Live Streaming using Windows Media Services:** You can also use Amazon CloudFront and Amazon EC2 running Windows Media Services for live streaming. With this solution, you can deliver live media over HTTP to both Microsoft Silverlight clients and Apple iOS devices. We've made it simple to get started by creating a [tutorial](#) and an AWS CloudFormation template to automate the provisioning of AWS resources for your live streaming stack. You only pay for the AWS resources you consume, and have full control over the origin server (Amazon EC2 instance running Windows Media Services) so you can configure additional IIS Live Smooth Streaming functionality.

## Limits

**Q. Can I use Amazon CloudFront if I expect usage peaks higher than 10 Gbps or 15,000 RPS?**

Yes. Complete our request for higher limits [here](#), and we will add more capacity to your account within two business days.

**Q: Is there a limit to the number of distributions my Amazon CloudFront account may deliver?**

For the current limit on the number of distributions that you can create for each AWS account, see [Amazon CloudFront Limits](#) in the Amazon Web Services General Reference. To request a higher limit, please go to the [CloudFront Limit Increase Form](#).

**Q: What is the maximum size of a file that can be delivered through Amazon CloudFront?**

The maximum size of a single file that can be delivered through Amazon CloudFront is 20 GB. This limit applies to all Amazon CloudFront distributions.

## Logging and Reporting

### **Q: Can I get access to request logs for content delivered through Amazon CloudFront?**

Yes. When you create or modify a CloudFront distribution, you can enable access logging. When enabled, this feature will automatically write detailed log information in a W3C extended format into an Amazon S3 bucket that you specify. Access logs contain detailed information about each request for your content, including the object requested, the date and time of the request, the edge location serving the request, the client IP address, the referrer, the user agent, the cookie header, and the result type (for example, cache hit/miss/error).

### **Q: Does Amazon CloudFront offer ready-to-use reports so I can learn more about my usage, viewers, and content being served?**

Yes. Whether it's receiving detailed cache statistics reports, monitoring your CloudFront usage, seeing where your customers are viewing your content from, or setting near real-time alarms on operational metrics, Amazon CloudFront offers a variety of solutions for your reporting needs. You can access all our reporting options by visiting the Amazon CloudFront Reporting & Analytics dashboard in the AWS Management Console. You can also learn more about our various reporting options by viewing Amazon CloudFront's [Reports & Analytics page](#).

### **Q: Can I tag my distributions?**

Yes. Amazon CloudFront supports cost allocation tagging. Tags make it easier for you to allocate costs and optimize spending by categorizing and grouping AWS resources. For example, you can use tags to group resources by administrator, application name, cost center, or a specific project. To learn more about cost allocation tagging, see [Using Cost Allocation Tags](#). If you are ready to add tags to your CloudFront distributions, see [Amazon CloudFront Add Tags page](#).

### **Q: Can I get a history of all Amazon CloudFront API calls made on my account for security, operational or compliance auditing?**

Yes. To receive a history of all Amazon CloudFront API calls made on your account, you simply turn on AWS CloudTrail in the [CloudTrail's AWS Management Console](#). For more information, visit [AWS CloudTrail home page](#).

### **Q: Do you have options for monitoring and alarming metrics in real time?**

You can monitor, alarm and receive notifications on the operational performance of your Amazon CloudFront distributions within just a few minutes of the viewer request using Amazon CloudWatch. CloudFront automatically publishes six operational metrics, each at 1-minute granularity, into Amazon CloudWatch. You can then use CloudWatch to set alarms on any abnormal patterns in your CloudFront traffic. To learn how to get started monitoring CloudFront activity and setting alarms via CloudWatch, please view our walkthrough in the [Amazon CloudFront Developer Guide](#) or simply navigate to the [Amazon CloudFront Management Console](#) and select Monitoring & Alarming in the navigation pane.

## Lambda@Edge

### **Q: What is Lambda@Edge?**

Lambda@Edge allows you to run code at global AWS edge locations without provisioning or managing servers, responding to end users at the lowest network latency. You just upload your Node.js code to AWS Lambda and configure your function to be triggered in response to Amazon CloudFront requests (i.e., when a viewer request lands, when a request is forwarded to or received back from the origin, and right before responding back to the end user). The code is then ready to execute at every AWS edge location when a

request for content is received, and scales with the volume of requests across CloudFront edge locations. Learn more in our [documentation](#).

### Q. How do I customize content with Lambda@Edge?

Once you have identified a content delivery decision you would like to make at the CloudFront edge, identify which cache behaviors, and what point in the request flow the logic applies to (i.e., when a viewer request lands, when a request is forwarded to or received back from the origin, or right before responding back to the end viewer). Next, write a Node.js Lambda function using the Lambda console or API, and associate it with the selected CloudFront trigger event for your distribution. Once saved, the next time an applicable request is made to your distribution, the function is propagated to the CloudFront edge, and will scale and execute as needed. Learn more in our [documentation](#).

### What events can be triggered with Amazon CloudFront?

Your functions will automatically trigger in response to the following Amazon CloudFront events:

- **Viewer Request** - This event occurs when an end user or a device on the Internet makes an HTTP(S) request to CloudFront, and the request arrives at the edge location closest to that user.
- **Viewer Response** - This event occurs when the CloudFront server at the edge is ready to respond to the end user or the device that made the request.
- **Origin Request** - This event occurs when the CloudFront edge server does not already have the requested object in its cache, and the viewer request is ready to be sent to your backend origin webserver (e.g. Amazon EC2, or Application Load Balancer, or Amazon S3).
- **Origin Response** - This event occurs when the CloudFront server at the edge receives a response from your backend origin webserver.

## IPv6

### Q. What is IPv6?

Every server and device connected to the Internet must have a numeric Internet Protocol (IP) address. As the Internet and the number of people using it grows exponentially, so does the need for IP addresses. IPv6 is a new version of the Internet Protocol that uses a larger address space than its predecessor IPv4. Under IPv4, every IP address is 32 bits long, which allows 4.3 billion unique addresses. An example IPv4 address is 192.0.2.1. In comparison, IPv6 addresses are 128 bits, which allow for approximately three hundred and forty trillion, trillion unique IP addresses. An example IPv6 address is: 2001:0db8:85a3:0:0:8a2e:0370:7334

### Q. What can I do with IPv6?

Using IPv6 support for Amazon CloudFront, your applications can connect to Amazon CloudFront edge locations without needing any IPv6 to IPv4 translation software or systems. You can meet the requirements for IPv6 adoption set by governments - including the [U.S. Federal government](#) - and benefit from IPv6 extensibility, simplicity in network management, and additional built-in support for security.

### Q. Should I expect a change in Amazon CloudFront performance when using IPv6?

No, you will see the same performance when using either IPv4 or IPv6 with Amazon CloudFront.

### Q: Are there any Amazon CloudFront features that will not work with IPv6?



All existing features of Amazon CloudFront will continue to work on IPv6, though there are two changes you may need for internal IPv6 address processing before you turn on IPv6 for your distributions.

1. If you have turned on the [Amazon CloudFront Access Logs](#) feature, you will start seeing your viewer's IPv6 address in the "c-ip" field and may need to verify that your log processing systems continue to work for IPv6.
2. When you enable IPv6 for your Amazon CloudFront distribution, you will get IPv6 addresses in the '[X-Forwarded-For](#)' header that is sent to your origins. If your origin systems are only able to process IPv4 addresses, you may need to verify that your origin systems continue to work for IPv6.

Additionally, if you use IP whitelists for Trusted Signers, you should use an IPv4-only distribution for your Trusted Signer URLs with IP whitelists and an IPv4 / IPv6 distribution for all other content. This model sidesteps an issue that would arise if the signing request arrived over an IPv4 address and was signed as such, only to have the request for the content arrive via a different IPv6 address that is not on the whitelist.

To learn more about IPv6 support in Amazon CloudFront, see "[IPv6 support on Amazon CloudFront](#)" in the Amazon CloudFront Developer Guide.

**Q: Does that mean if I want to use IPv6 at all I cannot use Trusted Signer URLs with IP whitelist?**

No. If you want to use IPv6 and Trusted Signer URLs with IP whitelist you should use two separate distributions. You should dedicate a distribution exclusively to your Trusted Signer URLs with IP whitelist and disable IPv6 for that distribution. You would then use another distribution for all other content, which will work with both IPv4 and IPv6.

**Q. If I enable IPv6, will the IPv6 address appear in the Access Log?**

Yes, your viewer's IPv6 addresses will now be shown in the "c-ip" field of the access logs, if you have the Amazon CloudFront Access Logs feature enabled. You may need to verify that your log processing systems continue to work for IPv6 addresses before you turn on IPv6 for your distributions. Please contact Developer Support if you have any issues with IPv6 traffic impacting your tool or software's ability to handle IPv6 addresses in access logs. For more details, please refer to the [Amazon CloudFront Access Logs](#) documentation.

**Q: Can I disable IPv6 for all my new distributions?**

Yes, for both new and existing distributions, you can use the Amazon CloudFront console or API to enable / disable IPv6 per distribution.

**Q: Are there any reasons why I would want to disable IPv6?**

In discussions with customers, the only common case we heard about was internal IP address processing. When you enable IPv6 for your Amazon CloudFront distribution, in addition to getting an IPv6 address in your detailed access logs, you will get IPv6 addresses in the '[X-Forwarded-For](#)' header that is sent to your origins. If your origin systems are only able to process IPv4 addresses, you may need to verify that your origin systems continue to work for IPv6 addresses before you turn on IPv6 for your distributions.

**Q: I enabled IPv6 for my distribution but a DNS lookup doesn't return any IPv6 addresses. What is happening?**

Amazon CloudFront has very diverse connectivity around the globe, but there are still certain networks that do not have ubiquitous IPv6 connectivity. While the long term future of the Internet is obviously IPv6, for the foreseeable future every endpoint on the Internet will have IPv4 connectivity. When we find parts of the Internet that have better IPv4 connectivity than IPv6, we will prefer the former.



**Q: If I use Route 53 to handle my DNS needs and I created an alias record pointing to an Amazon CloudFront distribution, do I need to update my alias records to enable IPv6?**

Yes, you can create Route 53 alias records pointing to your Amazon CloudFront distribution to support both IPv4 and IPv6 by using "A" and "AAAA" record type respectively. If you want to enable IPv4 only, you need only one alias record with type "A". For details on alias resource record sets, please refer to the [Amazon Route 53 Developer Guide](#).

## Billing

**Q. How will I be charged for my use of Amazon CloudFront?**

Amazon CloudFront charges are based on actual usage of the service in four areas: Data Transfer Out, HTTP/HTTPS Requests, Invalidation Requests, and Dedicated IP Custom SSL certificates associated with a CloudFront distribution.

With the [AWS Free Usage Tier](#), you can get started with Amazon CloudFront for free. Upon sign-up, new AWS customers receive 50 GB Data Transfer Out and 2,000,000 HTTP and HTTPS Requests for Amazon CloudFront each month for one year.

- **Data Transfer Out to Internet**

You will be charged for the volume of data transferred out of the Amazon CloudFront edge locations, measured in GB. If you are using other Amazon Web Services as the origins of your files, you will be charged separately for use of those services, including for storage, compute hours, GET requests and data transfer out of that service to Amazon CloudFront's edge locations. Usage tiers for data transfer are measured separately for each geographic region. You can see the rates for Amazon CloudFront data transfer to the Internet [here](#).

- **Data Transfer Out to Origin**

You will be charged for the volume of data transferred out, measured in GB, from the Amazon CloudFront edge locations to your origin (both AWS origins and other origin servers). You can see the rates for Amazon CloudFront data transfer to Origin [here](#).

- **HTTP/HTTPS Requests**

You will be charged for number of HTTP/HTTPS requests made to Amazon CloudFront for your content. You can see the rates for HTTP/HTTPS requests [here](#).

- **Invalidation Requests**

You are charged per path in your invalidation request. A path listed in your invalidation request represents the URL (or multiple URLs if the path contains a wildcard character) of the object you want to invalidate from CloudFront cache. You can request up to 1,000 paths each month from Amazon CloudFront at no additional charge. Beyond the first 1,000 paths, you will be charged per path listed in your invalidation requests. You can see the rates for invalidation requests [here](#).

- **Dedicated IP Custom SSL**

You pay \$600 per month for each custom SSL certificate associated with one or more CloudFront distributions using the Dedicated IP version of custom SSL certificate support. This monthly fee is pro-rated by the hour. For example, if you had your custom SSL certificate associated with at least one CloudFront distribution for just 24 hours (i.e. 1 day) in the month of June, your total charge for using the custom SSL certificate feature in June will be  $(1 \text{ day} / 30 \text{ days}) * \$600 = \$20$ . To use Dedicated IP Custom SSL certificate

support, upload a SSL certificate and use the AWS Management Console to associate it with your CloudFront distributions. If you need to associate more than two custom SSL certificates with your CloudFront distribution, please include details about your use case and the number of custom SSL certificates you intend to use in the [CloudFront Limit Increase Form](#).

Usage tiers for data transfer are measured separately for each geographic region. The prices above are exclusive of applicable taxes, fees, or similar governmental charges, if any exist, except as otherwise noted.

**Q: Does your prices include taxes?**

Except as otherwise noted, our prices are exclusive of applicable taxes and duties, including VAT and applicable sales tax. For customers with a Japanese billing address, use of AWS services is subject to Japanese Consumption Tax. [Learn more](#).

**Q: How am I charged for 304 responses?**

A 304 is a response to a conditional GET request and will result in a charge for the HTTP/HTTPS request and the Data Transfer Out to Internet. A 304 response does not contain a message-body; however, the HTTP headers will consume some bandwidth for which you would be charged standard CloudFront data transfer fees. The amount of data transfer depends on the headers associated with your object.

**Q. Can I choose to only serve content from less expensive Amazon CloudFront regions?**

Yes, "Price Classes" provides you an option to lower the prices you pay to deliver content out of Amazon CloudFront. By default, Amazon CloudFront minimizes end user latency by delivering content from its entire global network of edge locations. However, because we charge more where our costs are higher, this means that you pay more to deliver your content with low latency to end-users in some locations. Price Classes let you reduce your delivery prices by excluding Amazon CloudFront's more expensive edge locations from your Amazon CloudFront distribution. In these cases, Amazon CloudFront will deliver your content from edge locations within the locations in the price class you selected and charge you the data transfer and request pricing from the actual location where the content was delivered.

If performance is most important to you, you don't need to do anything; your content will be delivered by our whole network of locations. However, if you wish to use another Price Class, you can configure your distribution through the AWS Management Console or via the Amazon CloudFront API. If you select a price class that does not include all locations, some of your viewers, especially those in geographic locations that are not in your price class, may experience higher latency than if your content were being served from all Amazon CloudFront locations.

Note that Amazon CloudFront may still occasionally serve requests for your content from an edge location in a location that is not included in your price class. When this occurs, you will only be charged the rates for the least expensive location in your price class.

You can see the list of locations making up each price class [here](#).