Conversant
Connecting Digital World

CDN Portal

A Technical Guide

Version 2.0
24/11/2023

8 Temasek Boulevard Suntec Tower 3 #20-01 Singapore 038988
Tel: (65) 6226 1138 Fax: (65) 6226 1381 www.conversant.tv|Email: sales@conversant.tv

Contents

1 Overview 3
2 Login 4
3 Website Acceleration (WSA) 5
3.1 Enable Streaming 6
3.2 DNS Configuration 6
3.3 Origin with Multiple Websites on a Single IP Address ..... 错误!未定义书签。
3.4 SSL-Enabled Websites 7
4 FileDownload (LFD) 8
4.1 SimpleName 9
4.2 Domain Name 9
4.3 Testing File Download 11
4.4 Uploading Files using FTP or SFTP 11
5 Policies 12
5.1 Access Control Policies 12
5.2 Cache Control Policies 15
5.3 Redirection Policies 16
6 Analytics 20
6.1 Standard Analytics 20
6.2 Advanced Analytics 24
6.3 Logs 27
7 Copyright and Confidentiality 29

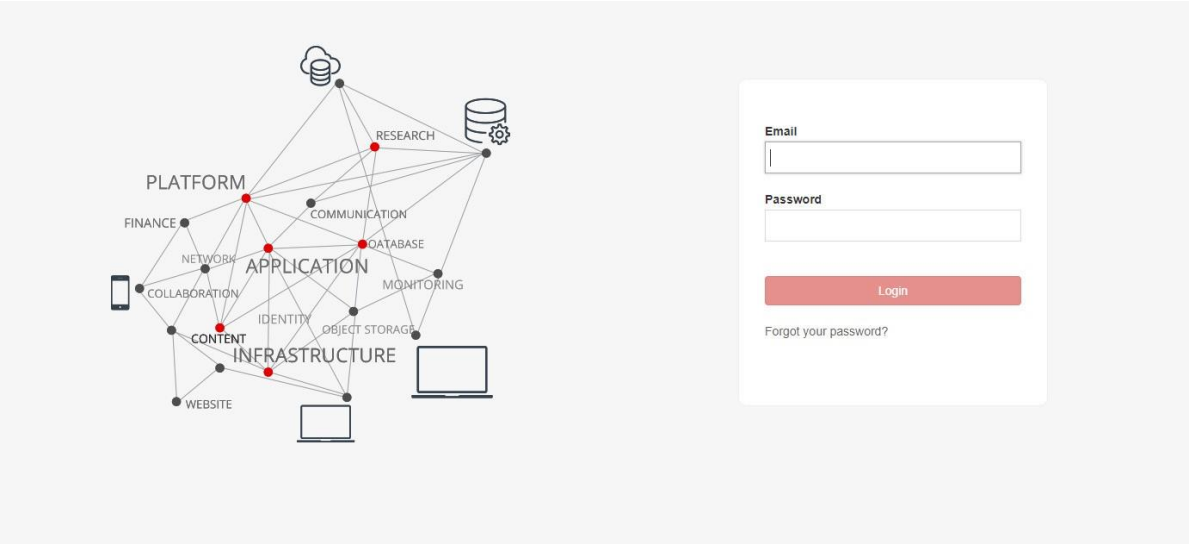
1 Overview

The CDN Portal is accessed for the creation of the respective domains required by customers for Website Acceleration (WSA) and Large File Download (LFD). Users can login via SwiftFederation Portal to add in respective domain name, origin IP for WSA service or upload the files through File Transfer Protocol (FTP) or (SFTP) to their respective LFD Domain.

This guide will provide complete instructions on how to use the modules of Website Acceleration, File Download, Reporting and Policies.

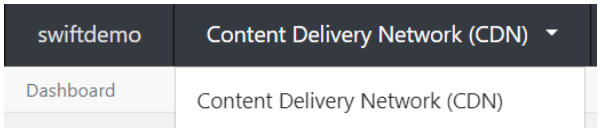
2 Login

Open a web browser and navigate to https://portal.swiftfederation.com/. Enter a valid Username & Password and press the Login button.

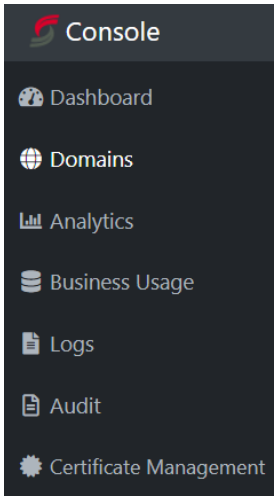


3 Website Acceleration (WSA)

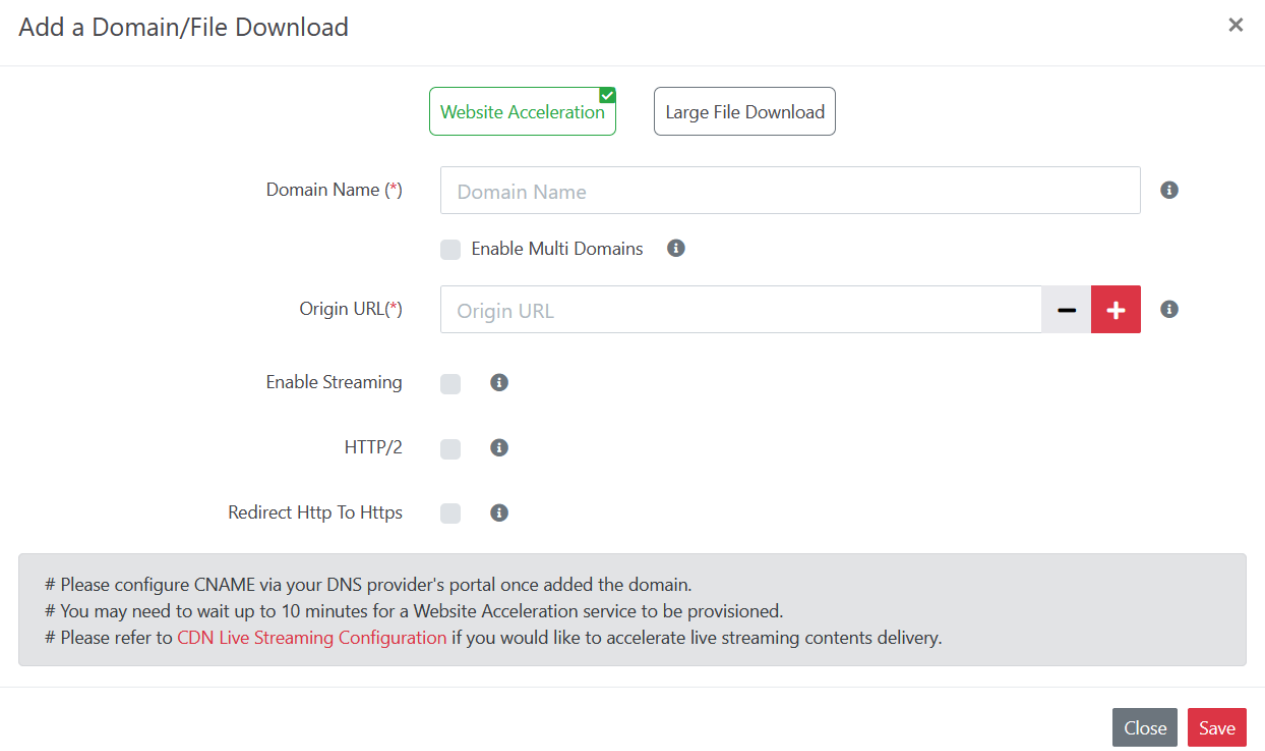
After selecting the customer entity, select CDN in the Products dropdown list.



Select Domains tab on the left hand side.



Enter the public domain name of the website that you wish to be accelerated in the Domain Name box. Enter the domain name or IP address of the Origin server into the Origin URL box.

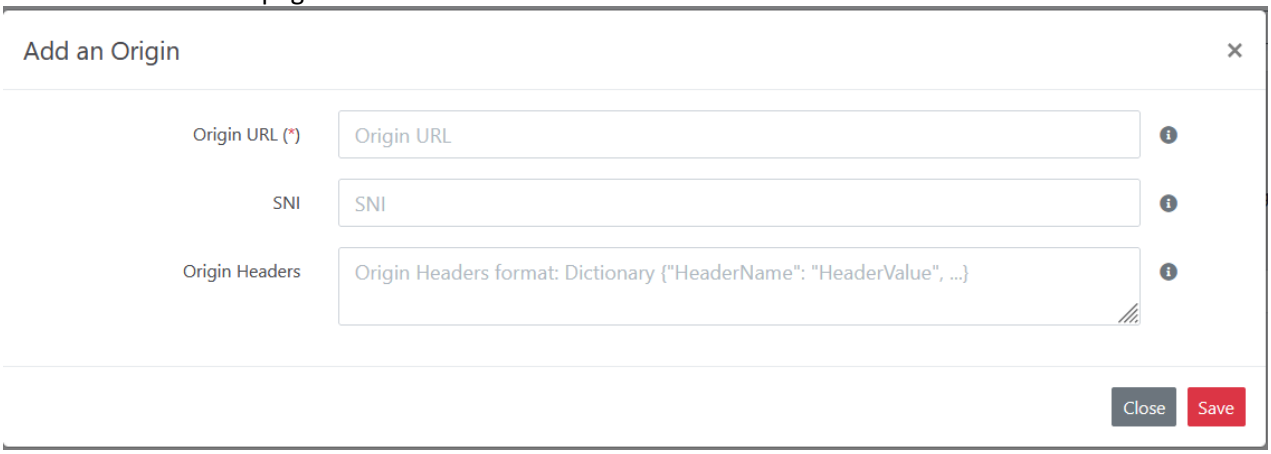


3.1 Enable Multi Domains

When enable Multi Domains option. It allow create some alternative domain names beside the primary domain name. all those domains share cache and configurations. But those domain names should config certificate separately if needed.

3.2 Multi Origins

If there are multi origins server need to be configured, add the “+” button and fill in all the Origin Urls, the origins will be select by failover mode. For more origin headers and SNI settings. Go to the Origins Control section in WSA detail page.

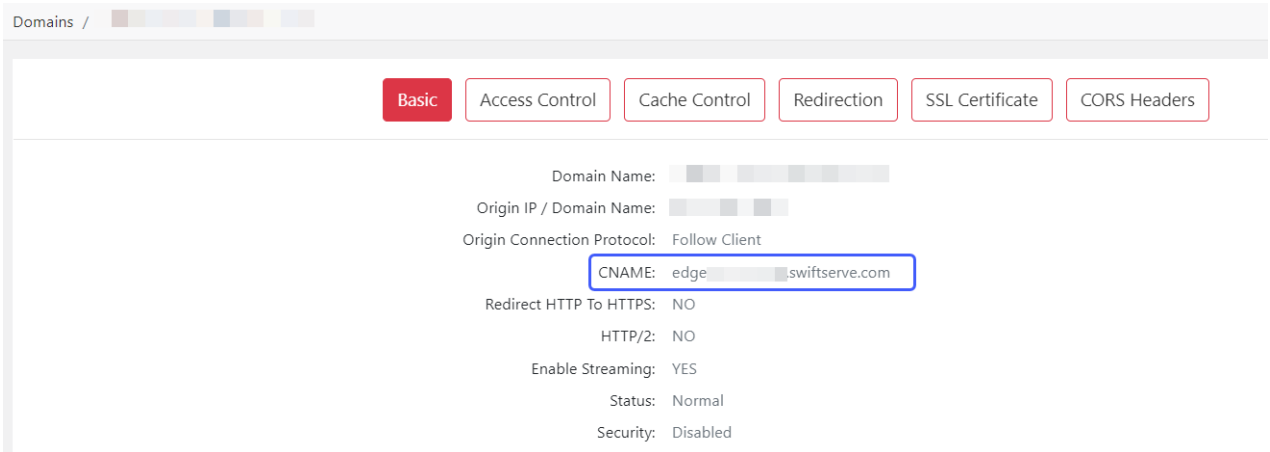


3.3 Enable Streaming

Only enable this option if WSA service is to be use for live video streaming. This option allows sharing of single request from origin server to multiple concurrent client requests for same object. Therefore, significantly reduces the load on origin server while serving large number of clients. Other content such as VOD, web objects or images does not benefit from this option as concurrency of same object request is not high.

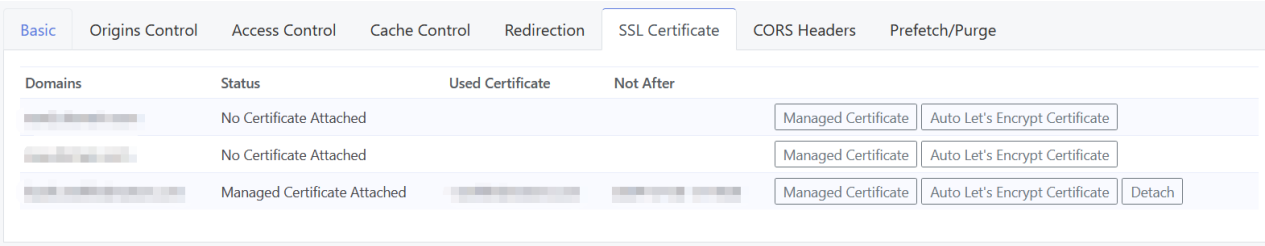
3.4 DNS Configuration

It is also necessary to configure your Domain Name Service (DNS) to point the website domain name to CDN delivery edge. In most cases, this is done by editing www host as CNAME record of CDN delivery domain, which is shown in WSA domain basic information.

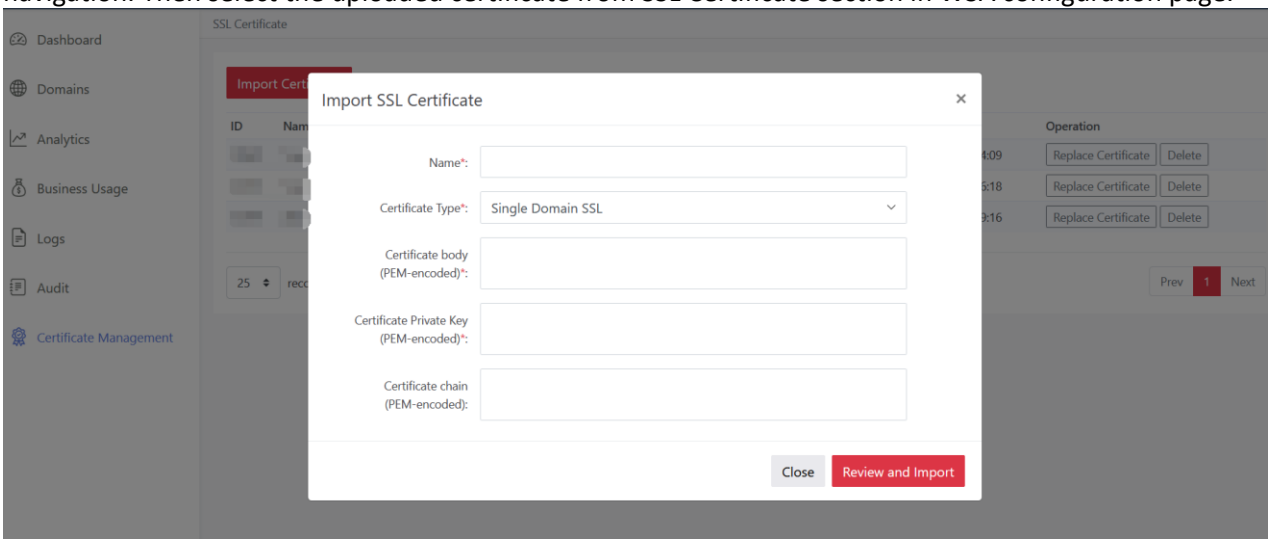


3.5 SSL-Enabled Websites

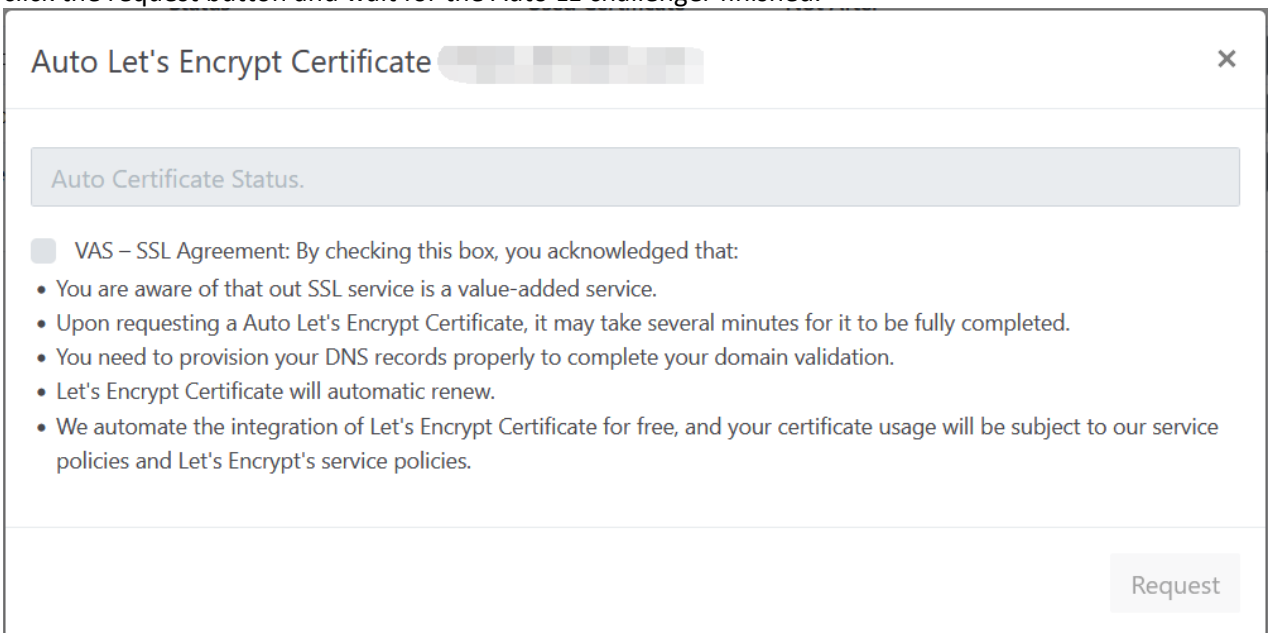
The acceleration of HTTPS (SSL-enabled) websites requires uploading and configuration of managed SSL certificate and key for the WSA domain. Alternatively, customer may request Auto Let's Encrypt Certificate for free. Customer does not need to upload SSL certificate and key for this case.



For managed SSL certificate and key. Customer can upload from the certificate management in the left navigation. Then select the uploaded certificate from SSL Certificate section in WSA configuration page.

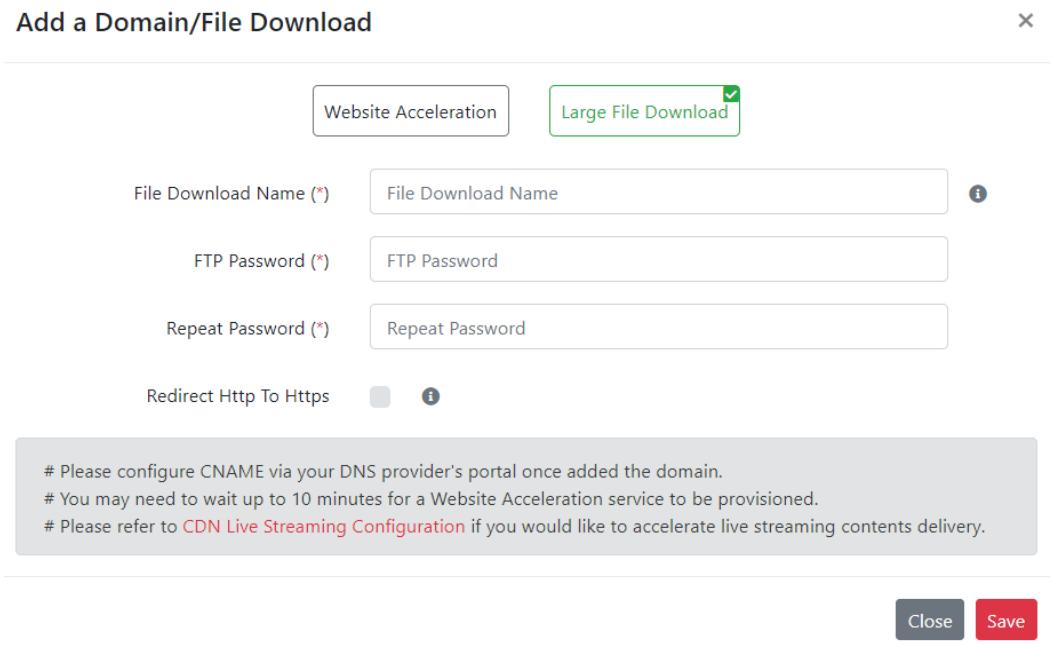


If customer want to use free Auto Let's Encrypt Certificate, first need to make the DNS Configuration then click the request button and wait for the Auto LE challenger finished.



4 FileDownload (LFD)

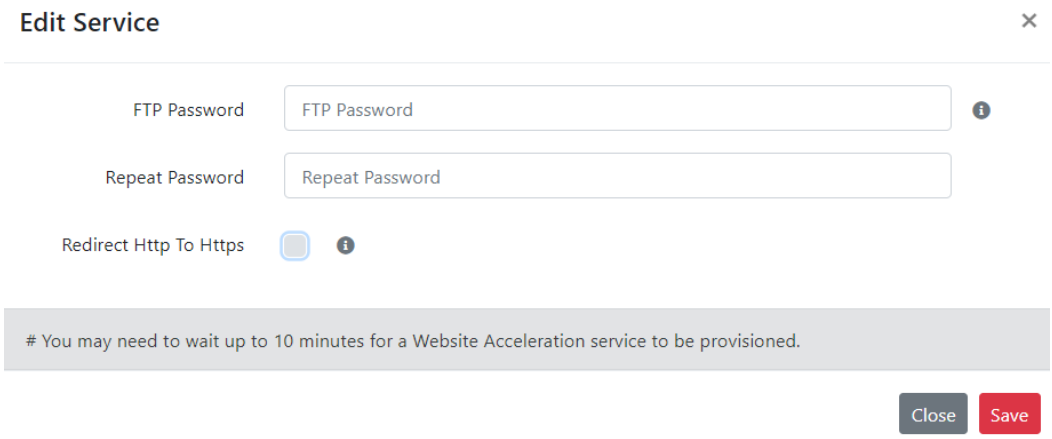
To create a new LFD service, enter the name of the service into File Download Name box.



The name for a Large File Download service can be in one of two forms:

- a short text-based name; or
- a fully-qualified domain name

The name used will also become the (S)FTP upload username. Enter and confirm the FTP password. You may change this later by clicking on Edit button in the Domains tab.



4.1 Simple Name

When a short text-based name is entered, the content will be delivered with an URL based on the assigned CDN edge domain.

Delivery URL can be referenced by visiting the file browser and clicking on the name of a file residing below pub folder.

For example, a file download service with the name *mylfdproperty* shall correspond to a delivery URL of the form:

http://[CDN edge domain]/[customer-name]/mylfdproperty/filename

- customer-name is the name of the customer
- filename is the name of the file being served

4.2 Domain Name

If a fully-qualified domain is entered then the content will be delivered via that domain instead of assigned CDN edge domain. This delivery URL can also be referenced by visiting the file browser and clicking on the name of a file.

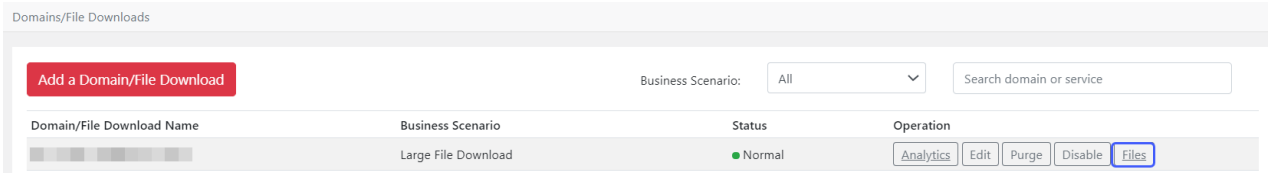
For example a file download service with the name www.myfdproperty.com would use a delivery URL of the form:

http://www.mylfdproperty.com/filename

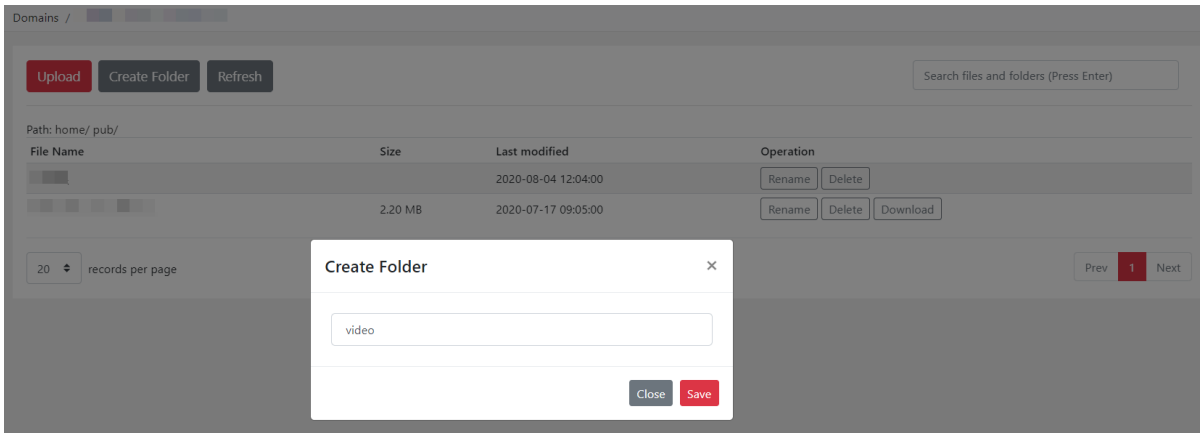
- Filename is the name of the file being served

You may obtain the LFD URL by:

Select the Product: CDN and go under the Domains tab. Select the Large File Download domain and select the 'File' button.

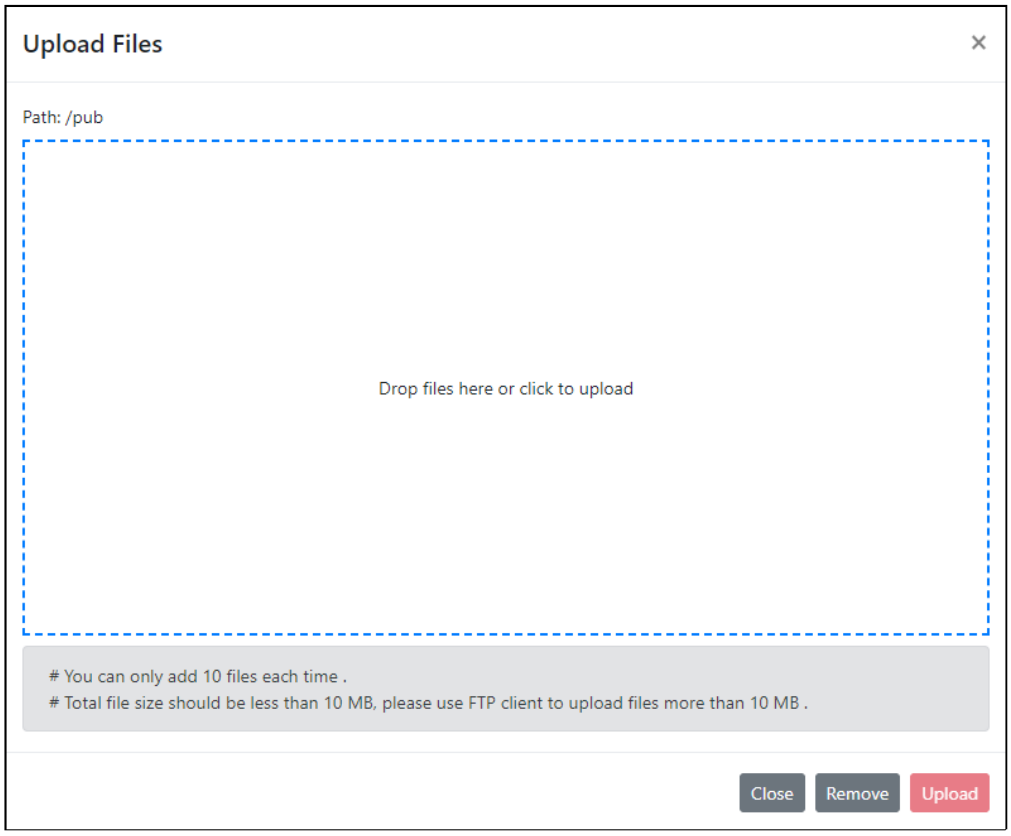


Create the Folders accordingly by selecting the Create Folder button. You may put files in any directory and arrange them as you wish, however only files in the pub directory or a sub-directory thereof will be accessible to end-users.

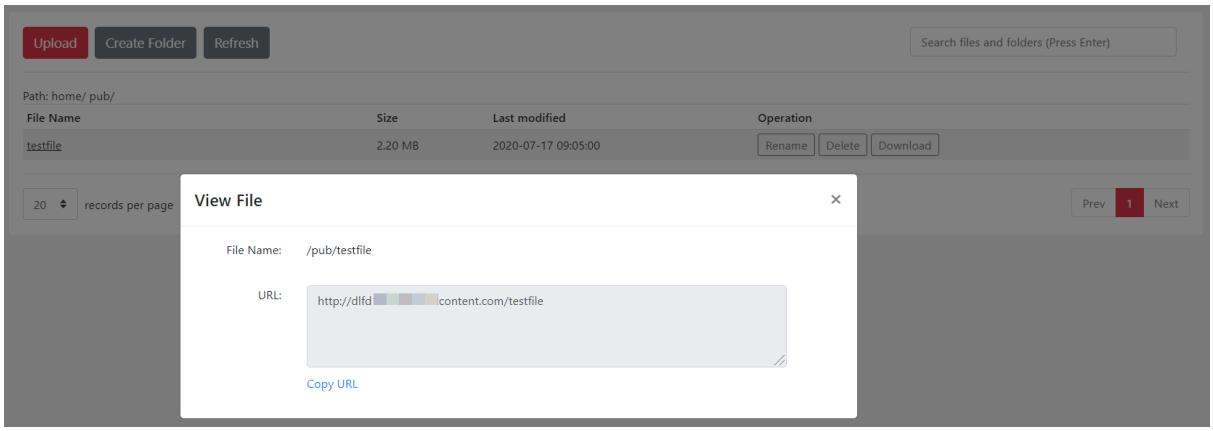


Enter the respective folders and select Upload button to bulk upload files into the respective folder.

Note:
The maximum files that can be uploaded each time are 10 files.
If the total file size is more than 10 MB, advisable to use FTP client utility for the transfer/upload instead.

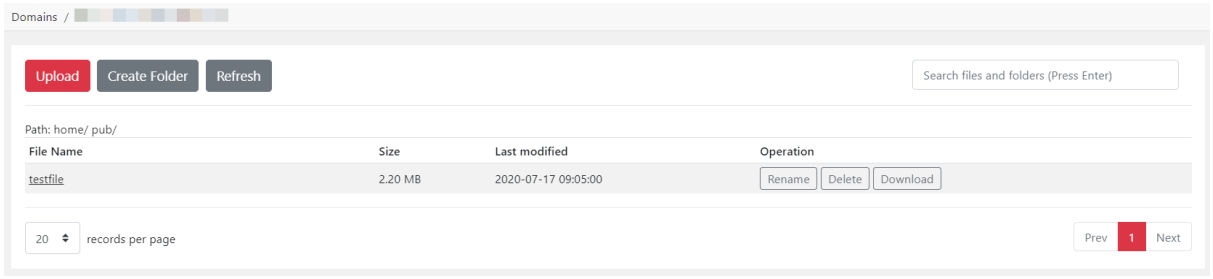


To get the respective file URL, click on the file name and select Copy URL to embed URL to your respective website or share accordingly.



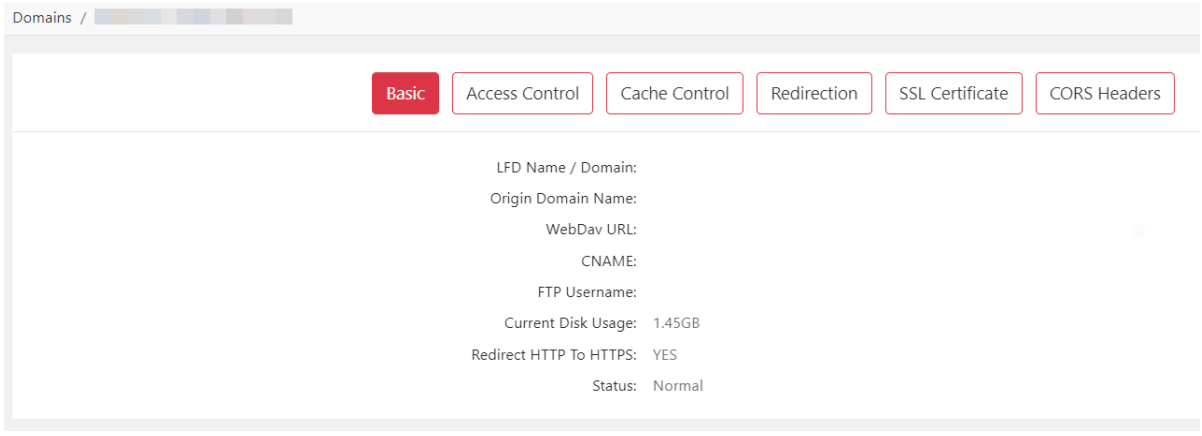
4.3 Testing File Download

You can test the download of files by selecting the folder. There is a download button for each file. Simply click on the download button to download the respective files.



4.4 Uploading Files using FTP or SFTP

The server to connect to is displayed on the Basic tab and standard ports are 21 for FTP and 22 for SFTP. For instance, if you are using Microsoft Windows, simply download FTP software (e.g. WinSCP). Key in the Hostname, Port number, User name, Password and select Login button. The required information can be referenced when you clicked on the LFD Domain.



5 Policies

Policies enable administrators to provide rules to govern access to their content. Administrators can apply rules to all content requests or specific content requests (described by URL pattern) that restricts access based on GeoIP, ranges of IP addresses or token authentication. Policies can also apply specific cache control settings to dictate caching behavior at CDN edge.

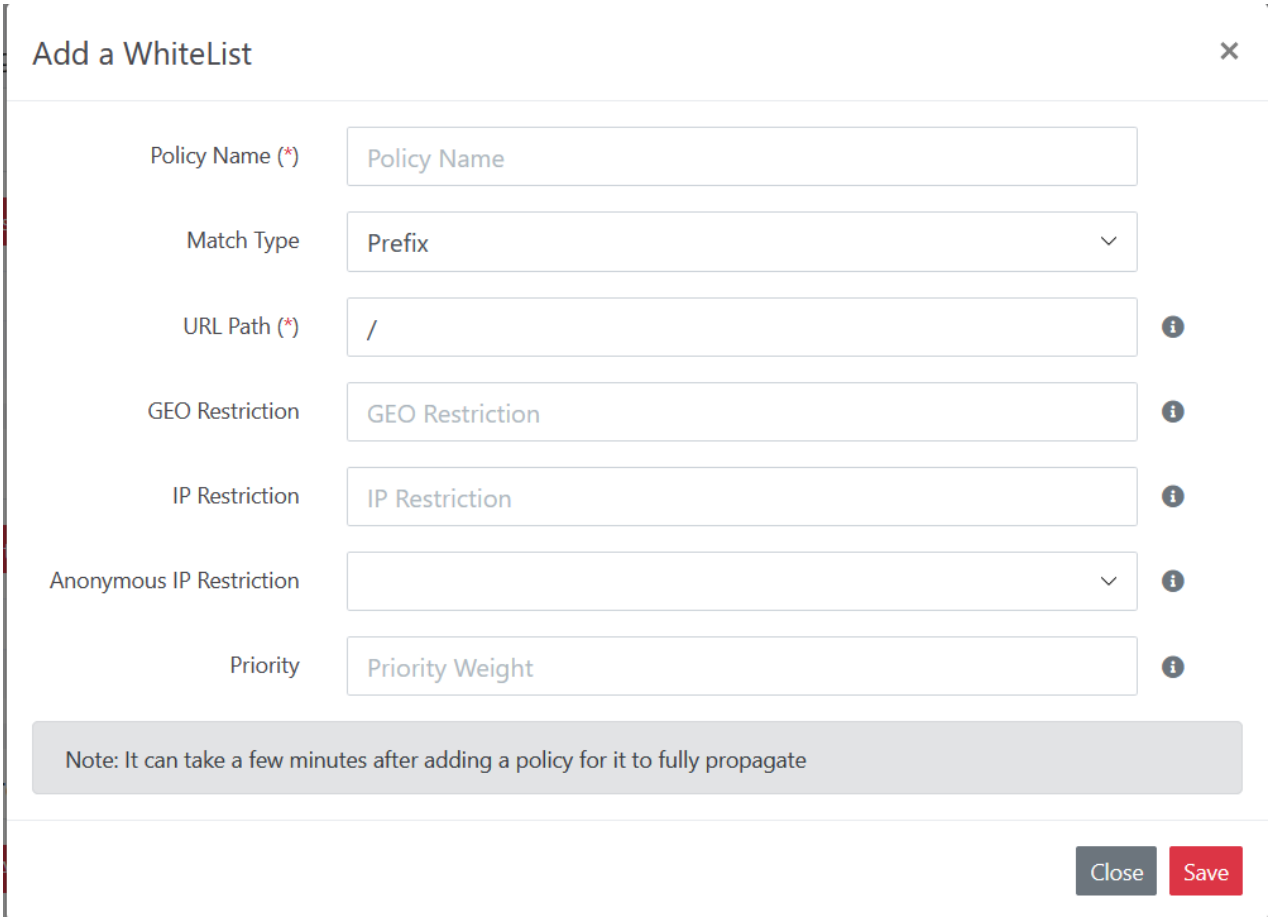
Policies are created and apply per configured service.

5.1 Access Control Policies

It is possible to restrict access to some or all content for all types of service with the following criteria:

- GeoIP Restriction: CDN restricts access base on the country that the end-user is requesting from.
- IP Restriction: An IP range can be manually specified.

The above 2 restrictions can be done through adding a Whitelist or Blacklist policy.
End-user requests that match the Whitelist policy will be allowed to download the content.

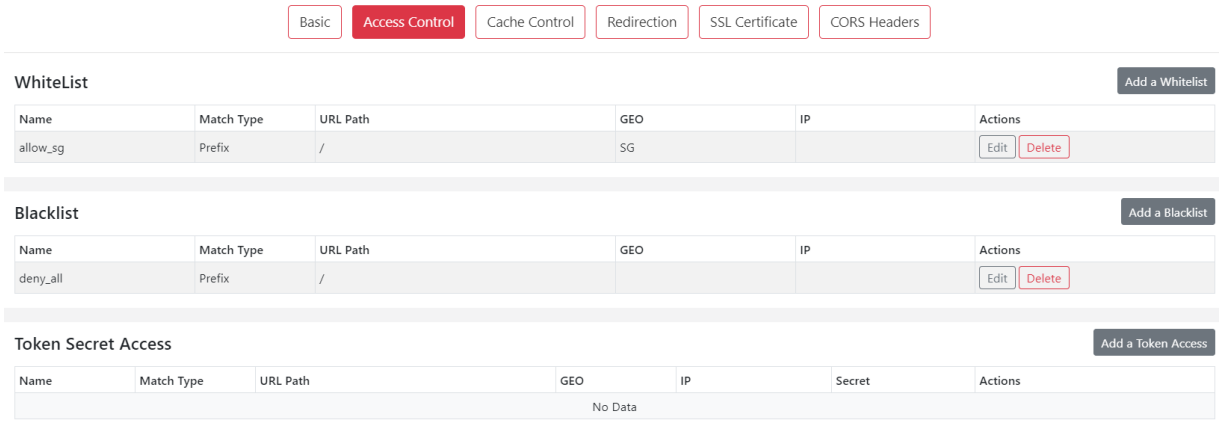


End-user requests that match the Blacklist policy will be denied from downloading the content.

CDN allows all access by default. To restrict content access, create one or more access control policies. These can be either:

- configure Blacklist policy to deny access in certain cases; or
- a deny all Blacklist policy with one or more Whitelist policies to selectively permit access.

For instance, below policies will deny all access except for end users accessing from country SG.



Policies should be given a name and can apply to all or part of the content based on the URL Path, match by prefix or regular expression. Policies should typically contain a geographic restriction or an IP restriction.

A geographic restriction is selected by specifying the ISO3166 country code, for example SG for Singapore. An IP restriction is selected by specifying an IP range in IP/CIDR or IP/mask format.

A full list of country codes can be found here: https://www.iso.org/obp/ui/#search

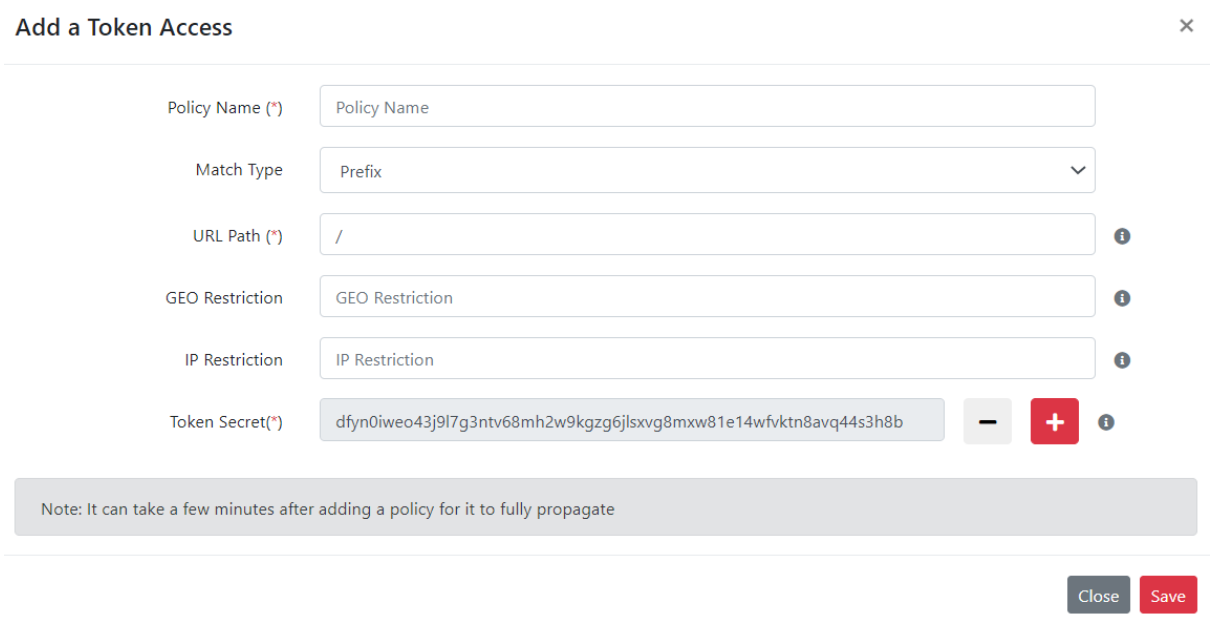
Although it is possible to specify both, the IP range will take precedence if this is done.

If there are multiple policies, a best match approach is used. The policy with the longest matching prefix is preferred. If several have equal lengths then the one with the smallest subnet will be chosen. Any IP range match will take precedence over a geographical policy.

If it is not possible to test the policy directly from the intended location(s), then add an additional policy under Access Control (for example to affect your IP address) to test and remove it afterwards. Please note that it may take up to ten minutes for any policy changes to propagate to all delivery nodes.

Token Access

Token requests which match the Token Access policy will require that the request also contains a valid cryptographic token for this content before content will be delivered.



The secret key to generate the encoded string can be viewed at the bottom of the Access Control tab by clicking the Show button. This is only visible when the portal is accessed via HTTPS and must be kept secret at all times for token policy to be effective.

Once a token policy is created, you will need to use the secret key to generate an encoded string to add to URLs for end user consumption as follows:

Tokens are time limited with two parameters:

- stime Start time (not valid before this time)
- etime End time (not valid after this time)

The formats of these are:
yyyymmddHHMMSS, e.g. 20120424115300 in UTC (date –u +%Y%m%d%H%M%S).

They may be optionally restricted to an IP address by adding *&ip=1.2.3.4* as an additional parameter.

For example, this basic URL:
http://www.example.com/path/to/resource?clientId=12345&product=A123&other=xyz

Remove protocol and hostname from the hash input leaving:
/path/to/resource?clientId=12345&product=A123&other=xyz

Add the time validity fields (these are required, not optional):
/path/to/resource?clientId=12345&product=A123&other=xyz&stime=20081201060100&etime=20081201183000

Calculate the encoded string as 0 concatenated with the first 20 characters of an HMACSHA1 hash using the result of step 2 and the secret key.

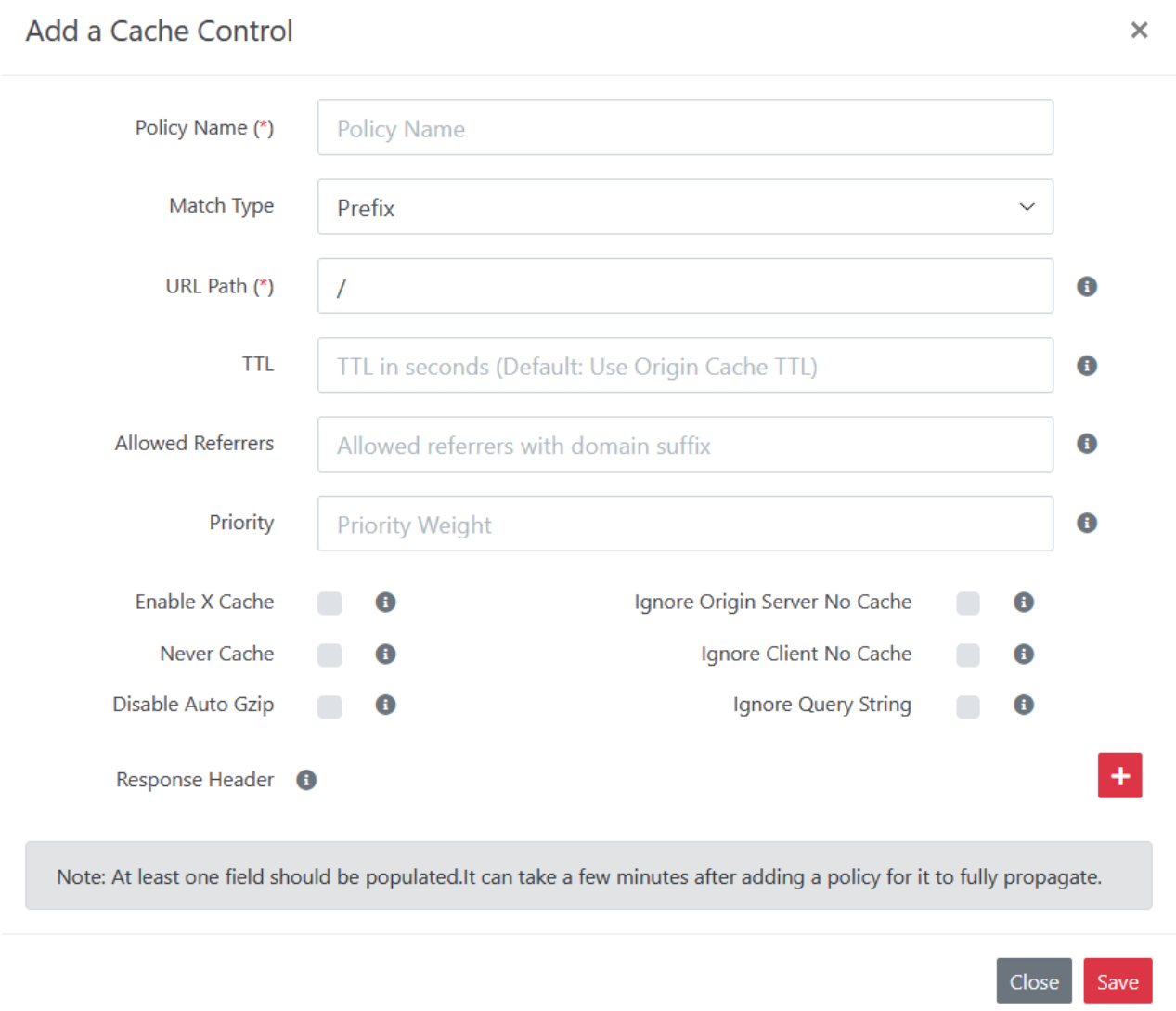
Build new URL:
http://www.example.com/path/to/resource?clientId=12345&product=A123&other=xyz&stime=20081201060100&etime=20081201100100&encoded=0<first20chars-of-hash>

Sample code for the encoded string (hash) calculation in a number of different programming languages is

available separately from your vendor or by contacting Conversant support team.

An end-user who attempts to access a prohibited content will receive a ”Forbidden” message (http response code 403) from their browser.

5.2 Cache Control Policies



- Time to Live (TTL)
  Specify the time in seconds to cache data returned for the request. Note: Applicable to File Download and Website Acceleration services.

Set these options to ignore cache headers or query strings:

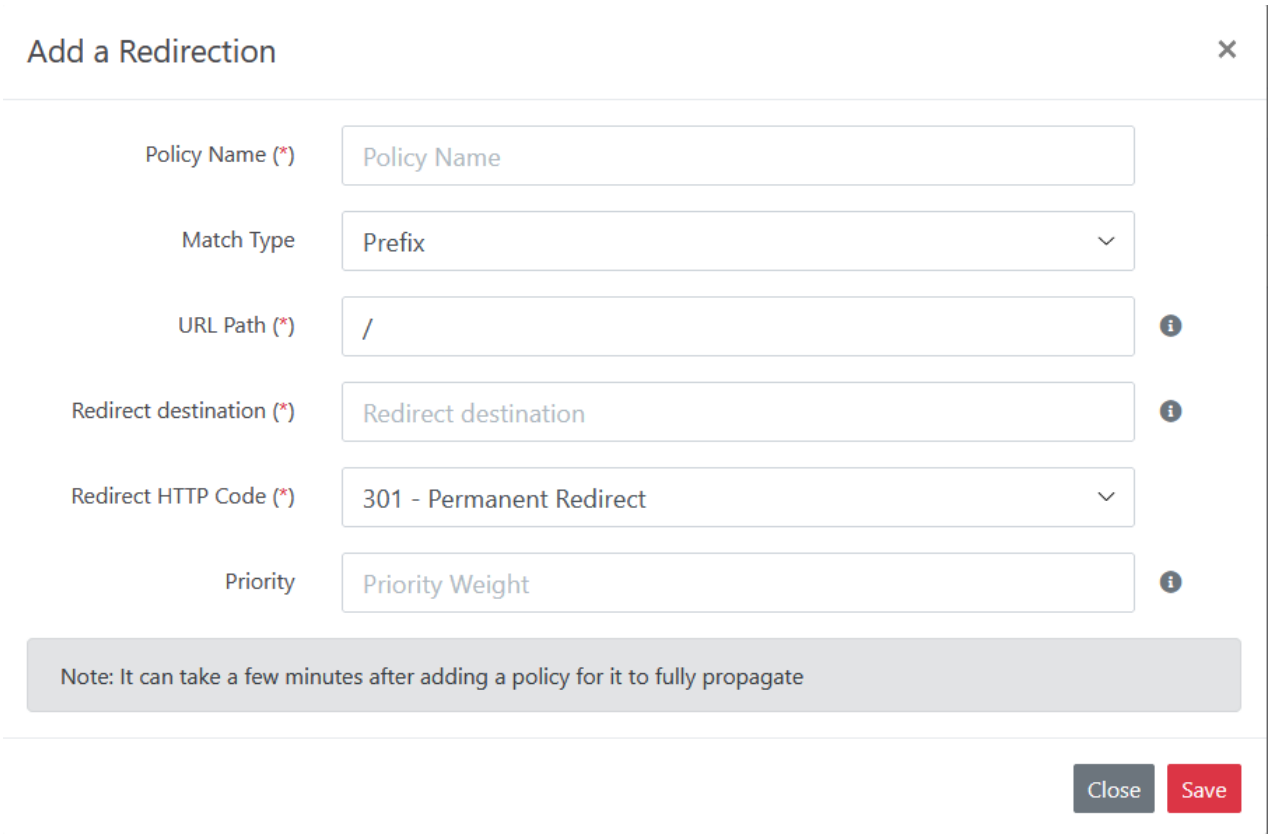
- Ignore Origin Server No Cache - Enable this option to ignore no cache header from origin server. e.g.
  Cache-Control: no-cache
  Cache-Control: no-store
- Ignore Client No Cache - Enable this option to ignore no-cache header from client.
- Ignore Query String - Enable this option to ignore any URL query string when indexing a cache object.

All the above options will improve cache hit rate at CDN edge, especially Ignore Query String option but use on this option depends on customer's web application logic. i.e. CDN edge will serve the same *photo.jpg* cached object for all the 3 different client requests listed below when Ignore Query String option is enabled.

http://www.example.com/path/to/photo.jpg
http://www.example.com/path/to/photo.jpg?clientId=12345&product=A123
http://www.example.com/path/to/photo.jpg?clientId=67890&product=A456

5.3 Redirection Policies

Add this policy to redirect matching URL to another destination URL. The redirection response code can be either a 301 Permanent Redirect or 302 Temporary Redirect.



There are two match types for CDN to determine the URL that a policy should be applied to:

- Prefix
  The Prefix match type will apply a policy where the URL begins with the path specified in the URL Path field. For example, a URL path of /images would apply the policy to all files in the folder /images. Alternatively, you can setup a policy on a particular file by explicitly entering the file path as the prefix, i.e. the URL /files/mydownload.zip would apply the policy to the single file mydownload.zip under files folder.

- Regex (Regular Expression)
  Regular Expressions (Regex) matching allows for some very flexible policies by providing the ability to define patterns in the file path. For example, a regex /video/.+\.mp4 would match all files in the /video folder with the extension .mp4. CDN parses the URL of the request to determine if a policy rule should be applied. Care should be taken when using regex matching for

URL paths; regular expressions are powerful, but also require caution to ensure that there are no unintended consequences of their use.

There are many dialects of Regular Expressions that all look similar but have important differences. CDN policy uses the Perl syntax. For more information on regex, this website provides a useful introduction: http://www.regular-expressions.info/quickstart.html

Brief explanation on Regex

- Special Characters
  Regular Expressions are a combination of text and patterns. The patterns are defined using a special set of characters:
  . [{ } ( ) \ * + ? | ^ $

  If you need to use any of the special pattern defining characters within the text parts of the expression, they must be prefixed with \ (backslash). The backslash indicates that the character is part of the match, rather than a special pattern character.

  For example, a regex policy of /animated$files would not match the actual path /animated$ files unless written with a backslash: /animated\$files.

- Wildcards
  The simplest form of regex is to use a wildcard. In regex syntax, the full stop (or period) (.) matches any single character. We can extend this by adding a multiplier (*, + or ?).

  .* matches zero or more characters
  .+ matches one or more
  .? matches zero or one

  You can also apply multipliers to text and ranges.

- Ranges
  You can create a pattern that matches a range of text by putting it inside square brackets: []. This can be a set of characters or a range of characters. For example:

  [123456789] is the same as [1-9].
  [a-zA-Z0-9] matches any single lowercase or uppercase letter or digit.

  And you can combine them with multipliers: [a-z]+ matches one or more lowercase letter

- Alternates
  Alternate options can be specified which means that, for example, you can create a pattern that matches three file extensions explicitly. The alternates are listed as (<pattern1>|<pattern2>| <pattern3>).

  The patterns in the alternates can be plain text or regular expressions.

- Anchoring
  As with prefix policies, the regex must match the leading / on a path - so a simple pattern of filename.txt will not match anything.

  The regex must match all the way to the end of the path - so /file will match http://host/file but not http://host/file.txt.
  Some Common Examples

  /files/august matches just the path /files/august - this is the not the same as using a prefix as it will only match this particular path and not any paths beneath it.

  /files/.+/index.html matches all the index.html files under the 'files' root folder, regardless of

which subdirectory they may be in.

/files/august/.+\.(mp4|ogg|swf) matches all files in the /files/august directory that have the extensions .mp4, .ogg or .swf. Note the \ in front of the '.' to ensure it acts as text rather than as part of a pattern.

- Multiple Matches
  What happens if more than one policy matches the URL? The policies are compared and the most specific policy is used.

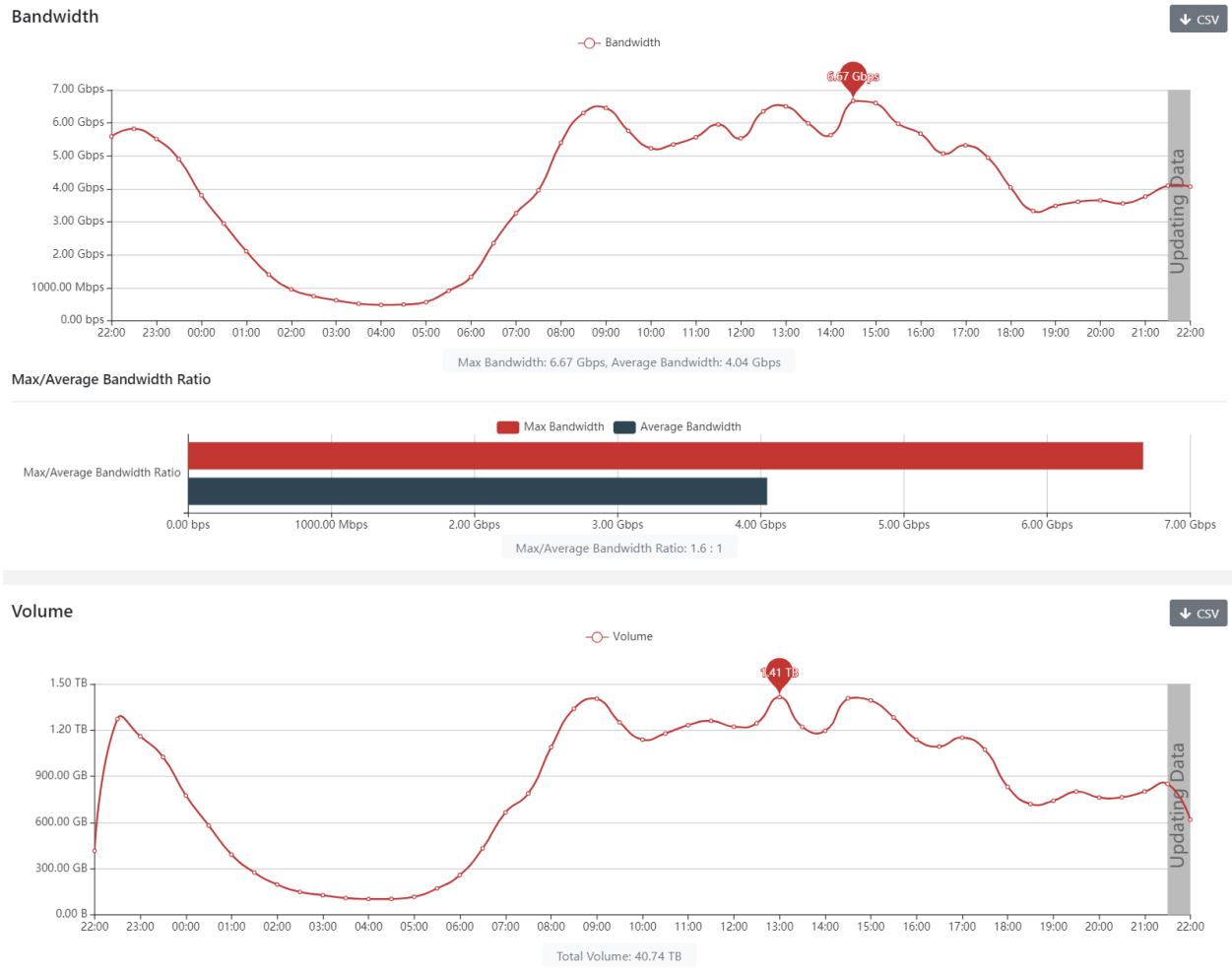
  First, the prefixes and regexes are compared to find the most specific. If they are equivalent, the IP subnet and location are examined.
  When comparing two prefixes, the longest prefix is regarded as the most specific.
  When comparing two regexes, the length of text at the beginning of the expression is inspected before any pattern. The most specific regex is the one with the longest initial text.
  When comparing a regex and a prefix, the length of initial text from the regex is compared with the length of the prefix, and whichever is longer is taken as the most specific.

6 Analytics

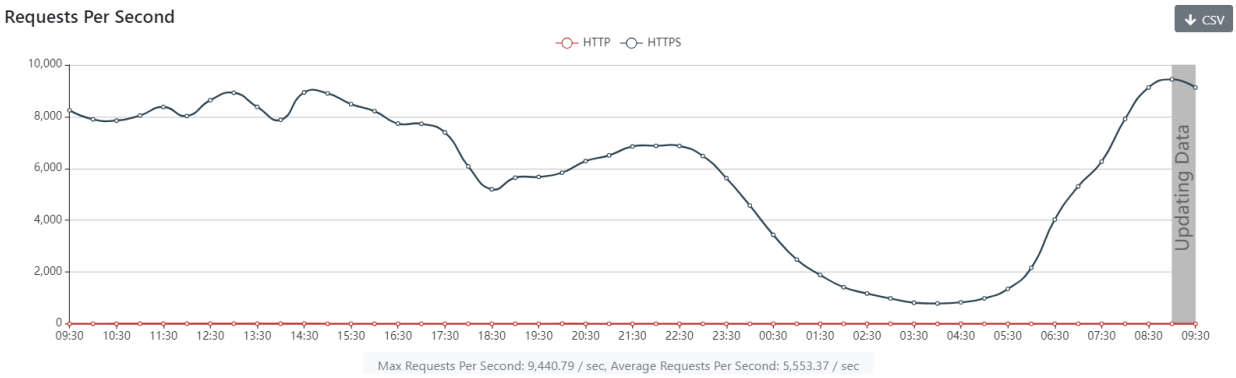
Analytics provides valuable business insights on CDN services viewable from SwiftFederation portal. Analytics are classified into standard and advance. Standard analytics are generally CDN traffic usage, performance and user distribution type of reporting. Advanced analytics are statistics related to customer's content type and end users information which is optionally enabled upon request. Analytics are presented on per service or on aggregated service, view over periods of hours, days, months or in custom range. Reporting data of different customers are further aggregated under a partner entity, which may has multiple customer entities.

6.1 Standard Analytics

a) Aggregated bandwidth and data volume utilization graph of customer CDN services with average and peak values.

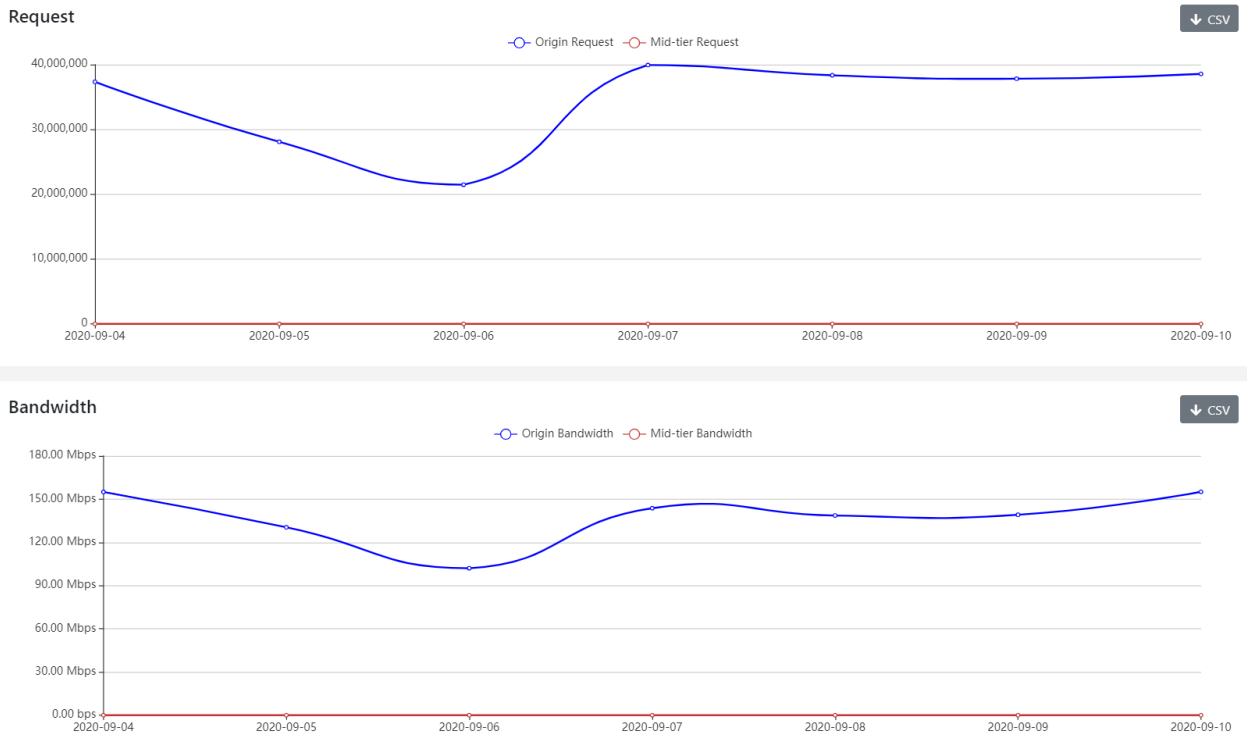


b) Aggregated request per second graph with HTTP and secure HTTPS segregation.

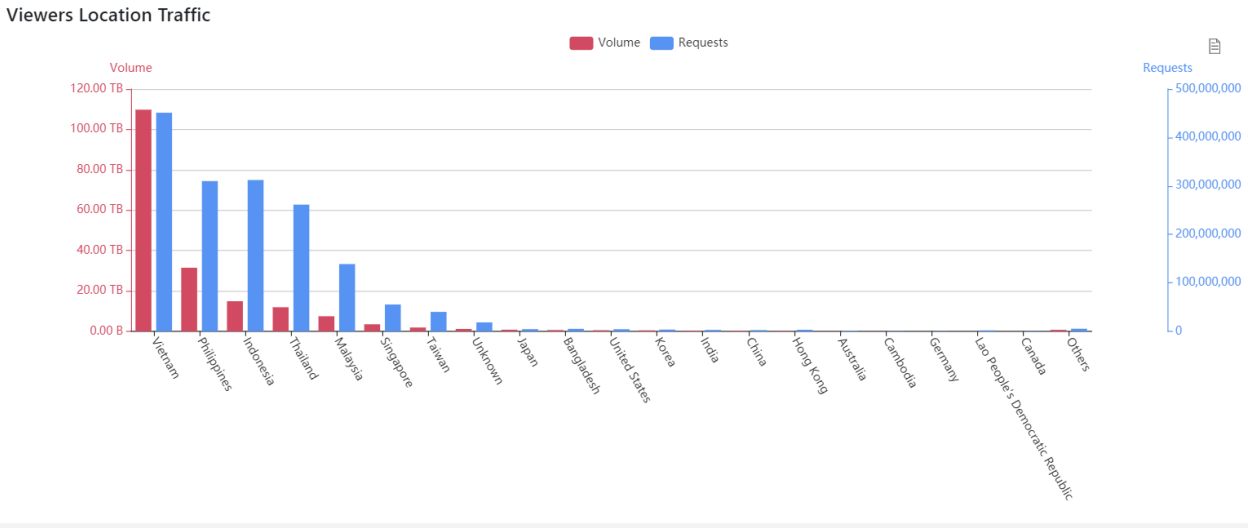


c) Cache hit rate performance graphs in terms of request or byte. Byte hit rate is formulated base on percentage of bytes served from cache over total bytes served to end users including bytes from origin server. Higher hit rate means better performance with more content served from cache directly.

d) Origin request and bandwidth performance graphs show the load on customer origin servers. Minimizing the load on origin servers improve client download performance by serving more from cache. Mid-tier Request/Bandwidth graph will be shown when mid-tier caching on a service is enabled.



e) Viewers location shows the level of demand for customer content in each country.

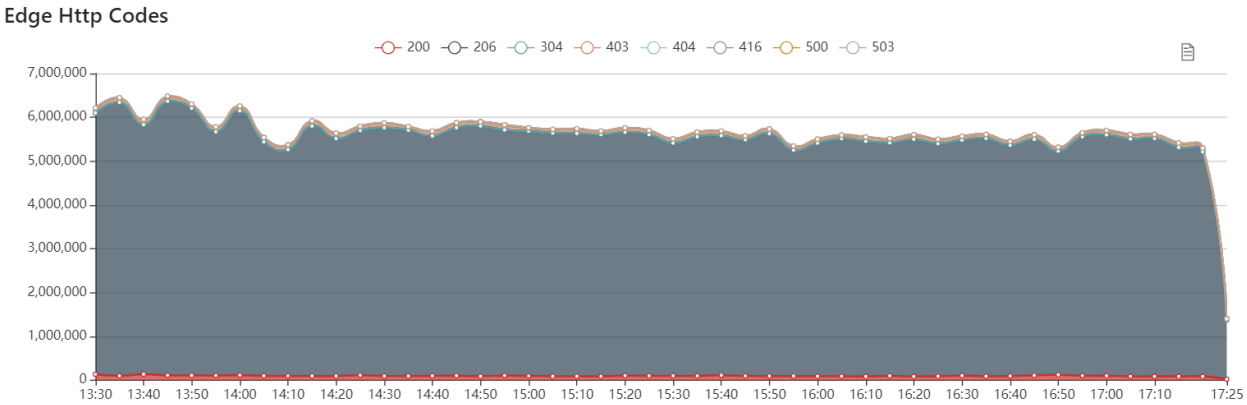


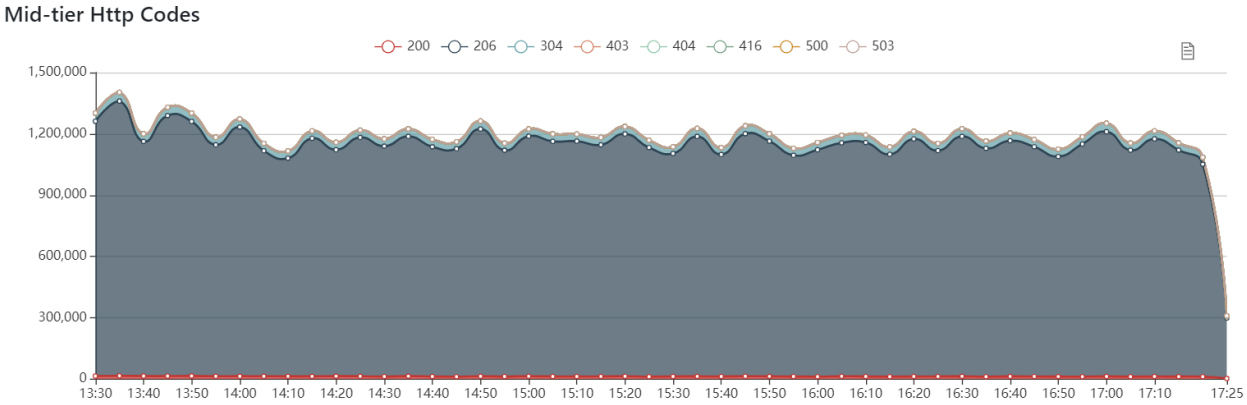
Viewers Location Traffic Details

Search location

Location	Volume	Number of Requests	Volume of Conversant Infra
Vietnam	109.77 TB (58.78%)	451,072,545 (27.77%)	0 Byte
Philippines	31.49 TB (16.86%)	310,038,371 (19.09%)	0 Byte
Indonesia	14.91 TB (7.98%)	312,177,352 (19.22%)	0 Byte
Thailand	11.92 TB (6.38%)	261,428,117 (16.10%)	0 Byte
Malaysia	7.46 TB (4.00%)	138,755,518 (8.54%)	0 Byte
Singapore	3.48 TB (1.86%)	55,316,966 (3.41%)	0 Byte
Taiwan	1.89 TB (1.01%)	40,060,889 (2.47%)	0 Byte

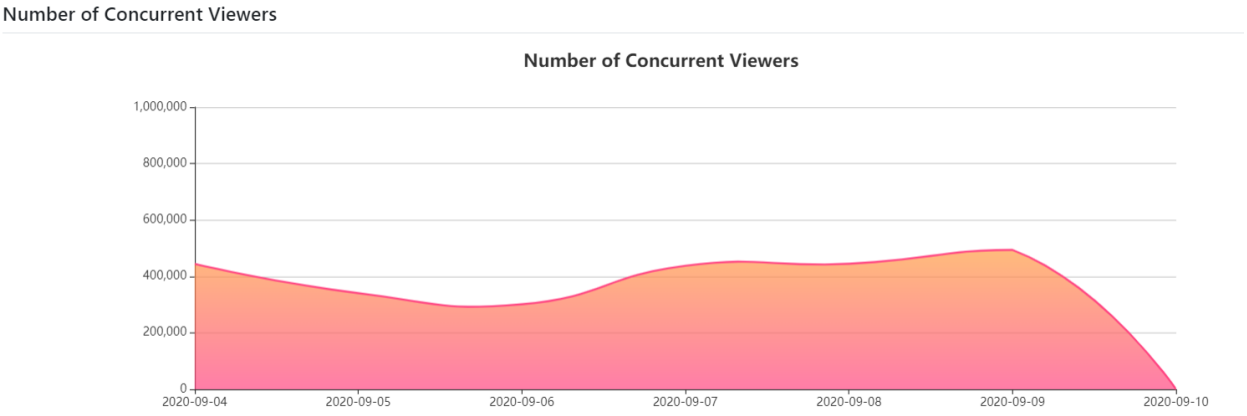
f) HTTP response codes graph provides immediate review on customer content delivery status, where optimally most requests should have 2xx codes response. A high level of error code should prompt an investigation for underlying technical issues. Mid-tier HTTP Codes graph will be shown when mid-tier caching on a service is enabled.





6.2 Advanced Analytics

a) Concurrent viewers is more relevant to video streaming, the graph implies the popularity of customer content.



b) User agent statistics provides insight on end user devices that is valuable for customer's business and marketing decisions.

Browsers | Operating Systems | Devices

Browsers

CSV

Browsers	Version	Requests
Chrome	Chrome 85.0.4183.101	549,266,345 (15.61%)
Chrome	Chrome 85.0.4183.102	438,606,381 (12.46%)
Coc Coc Browser	Coc Coc Browser 89.0.124	282,857,904 (8.04%)
Chrome	Chrome 85.0.4183.121	216,031,942 (6.14%)
Safari	Safari 13.1.2	173,599,518 (4.93%)
AppleCoreMedia	AppleCoreMedia 1.0.0.17H35	124,340,323 (3.53%)
Chrome Webview	Chrome Webview 57.0.2987.108	103,755,500 (2.95%)
Chrome	Chrome 85.0.4183.120	86,049,401 (2.44%)
SamsungBrowser	SamsungBrowser 12.1	84,764,167 (2.41%)
Chrome	Chrome 85.0.4183.109	65,758,025 (1.87%)
UIWebView	UIWebView 605.1.15	58,660,304 (1.67%)
Safari	Safari 12.1.2	55,118,945 (1.57%)

Browsers | Operating Systems | Devices

Operating Systems

CSV

Operating Systems	Requests
Android	1,305,604,316(37.1%)
Windows NT	1,175,683,085(33.41%)
iOS	973,818,282(27.67%)
Mac OS X	37,216,329(1.06%)
-	6,692,300(0.19%)
Linux	6,204,870(0.18%)
Tizen	4,902,444(0.14%)
Google	2,708,475(0.08%)
Windows Phone	2,394,923(0.07%)
BlackBerry	1,624,142(0.05%)
Ubuntu	876,161(0.02%)

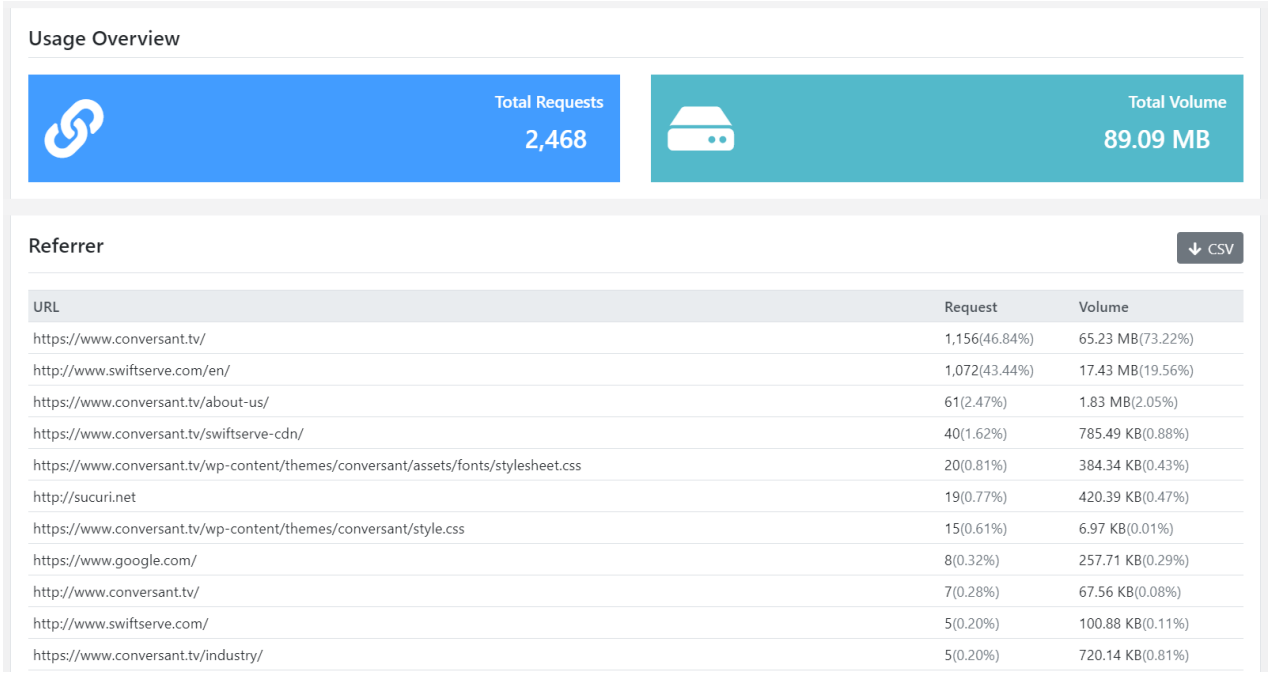
Browsers | Operating Systems | Devices

Devices

CSV

Device	Requests
Desktop	1,175,381,722
Apple iPhone	931,143,635
Android Mobile	128,335,764
Samsung SM-G610F	57,011,243
Apple iPad	42,682,037
Samsung SM-J730G	37,689,714
Apple Macintosh	37,219,247
Samsung SM-A505F	26,890,926
Samsung SM-A750GN	24,627,779
Samsung SM-A515F	19,888,256
Samsung SM-N950F	19,573,044

c) Referrer statistics informs customer on how the end users get to know about their content.



Usage Overview

Total Requests
2,468

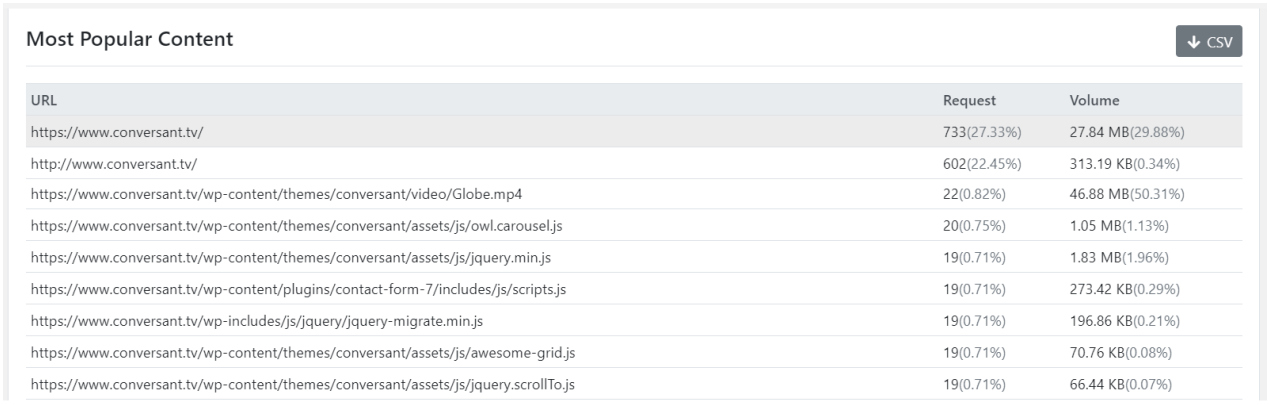
Total Volume
89.09 MB

Referrer

CSV

URL	Request	Volume
https://www.conversant.tv/	1,156(46.84%)	65.23 MB(73.22%)
http://www.swiftserve.com/en/	1,072(43.44%)	17.43 MB(19.56%)
https://www.conversant.tv/about-us/	61(2.47%)	1.83 MB(2.05%)
https://www.conversant.tv/swiftserve-cdn/	40(1.62%)	785.49 KB(0.88%)
https://www.conversant.tv/wp-content/themes/conversant/assets/fonts/stylesheet.css	20(0.81%)	384.34 KB(0.43%)
http://sucuri.net	19(0.77%)	420.39 KB(0.47%)
https://www.conversant.tv/wp-content/themes/conversant/style.css	15(0.61%)	6.97 KB(0.01%)
https://www.google.com/	8(0.32%)	257.71 KB(0.29%)
http://www.conversant.tv/	7(0.28%)	67.56 KB(0.08%)
http://www.swiftserve.com/	5(0.20%)	100.88 KB(0.11%)
https://www.conversant.tv/industry/	5(0.20%)	720.14 KB(0.81%)

d) Most popular content statistics provides a more detailed breakdown on the popularity customer content.

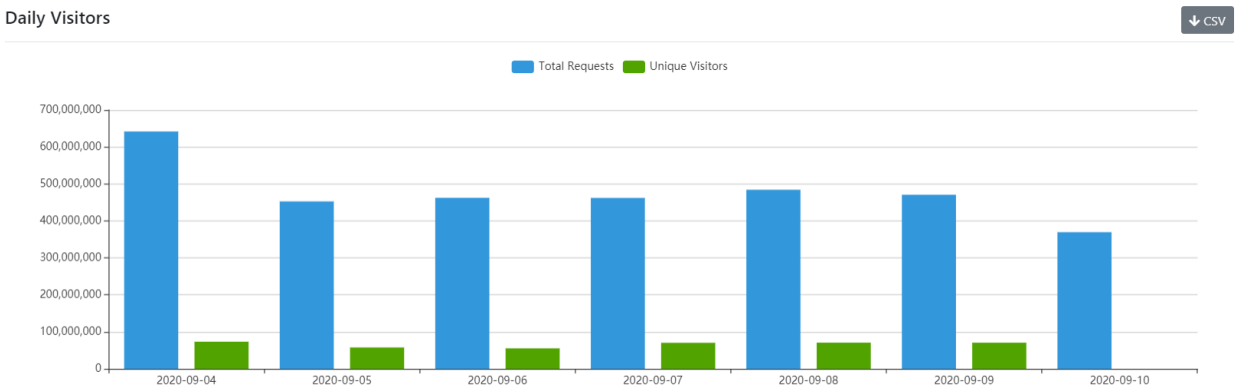


Most Popular Content

CSV

URL	Request	Volume
https://www.conversant.tv/	733(27.33%)	27.84 MB(29.88%)
http://www.conversant.tv/	602(22.45%)	313.19 KB(0.34%)
https://www.conversant.tv/wp-content/themes/conversant/video/Globe.mp4	22(0.82%)	46.88 MB(50.31%)
https://www.conversant.tv/wp-content/themes/conversant/assets/js/owl.carousel.js	20(0.75%)	1.05 MB(1.13%)
https://www.conversant.tv/wp-content/themes/conversant/assets/js/jquery.min.js	19(0.71%)	1.83 MB(1.96%)
https://www.conversant.tv/wp-content/plugins/contact-form-7/includes/js/scripts.js	19(0.71%)	273.42 KB(0.29%)
https://www.conversant.tv/wp-includes/js/jquery/jquery-migrate.min.js	19(0.71%)	196.86 KB(0.21%)
https://www.conversant.tv/wp-content/themes/conversant/assets/js/awesome-grid.js	19(0.71%)	70.76 KB(0.08%)
https://www.conversant.tv/wp-content/themes/conversant/assets/js/jquery.scrollTo.js	19(0.71%)	66.44 KB(0.07%)

e) Daily visitors not only provide daily request number but also unique visitors, which tell how many different users downloaded customer content.



6.3 Logs

The Logs tab allows download of gzip archives containing the service access logs.

Domain Name: select domain Time Range: 2020-09-25 18:00~2020-09-26 18:00 OK

Log File Name	Size	Log Datetime	Actions
20200925100000-15.log.gz	1KB	2020-09-25 18:00:00	Download
20200925100000-5.log.gz	1KB	2020-09-25 18:00:00	Download
20200925100500-6.log.gz	1KB	2020-09-25 18:05:00	Download
20200925101000-2.log.gz	1KB	2020-09-25 18:10:00	Download
20200925101500-10.log.gz	1KB	2020-09-25 18:15:00	Download
20200925101500-15.log.gz	1KB	2020-09-25 18:15:00	Download
20200925101500-17.log.gz	1KB	2020-09-25 18:15:00	Download
20200925101500-7.log.gz	4 KB	2020-09-25 18:15:00	Download
20200925102000-19.log.gz	1KB	2020-09-25 18:20:00	Download
20200925102000-5.log.gz	1KB	2020-09-25 18:20:00	Download

The logs will be kept for 30 days. Log archives will be available 1 hour after log generation.

Please download via API if large amount of log needs to be downloaded.

Each column of access log entry corresponds to the following list of field names.

$remote_addr - - [$time_local] "$request" $status $request_time - $bytes_sent "$http_referer" "$http_user_agent" "-" "$session_id" "$HIT" "$server_addr" $ttfb

- $remote_addr: Client IP address, e.g. 45.32.174.90.
- '-': Represents a blank field.
- $time_local: Request completion time stamp in UTC+08 timezone, e.g. 11/Jan/2017:18:38:57 +0800.
- $request: HTTP Request Method (e.g. GET or POST) and URL .An example will be "GET http://image.example1.com/upload_files/images/360_270/20150410/eb252121-b392-4651-b938- 117991cfb9b5.jpg"
- $status: HTTP Response Code (e.g. 200 or 403).
- $request_time: Request Duration in milliseconds (e.g. 955.123)
- $bytes_sent: Number of bytes sent to the client which includes HTTP content and headers.

- $http_referer: HTTP Referrer string corresponds to the HTTP Referrer header in client request.
- $http_user_agent: HTTP User Agent string corresponds to the HTTP User-Agent header in client request, e.g. “Mozilla/5.0 (Windows NT 5.1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/27.0.1453.116 Safari/537.36".
- $session_id: Unique client session ID.
- $HIT: Cache status to indicate whether the request is a cache hit or cache miss.
- $server_addr: Server address refers to the CDN node IP, which client requests content from.
- $ttfb: Time to First Byte refers to time it took CDN node to send first byte of data to the client.

7 Copyright and Confidentiality