

How to setup custom hostname and SSL certificate for your API domain in 5 minutes

Code		Author	BrainCert
Created Date	2017-08-01 12:27:37	Last Update	2017-08-12 12:30:03
Rating	☆☆☆☆☆	Votes	21

You can easily CNAME your domain to the API endpoint `api.braincert.com` in order to receive the performance and security benefits of BrainCert. After you have added the CNAME entry in your DNS server, click the '**Request SSL Certificate**' button in the [API dashboard](#) and BrainCert will attempt to issue an SSL certificate for the custom hostname without any other validation or private key requirements. It's that simple!

HTML5 Virtual Classroom relies on SSL (HTTPS) to function and it will not work with external domains. BrainCert recommends using our native enterprise SSL feature for this service.

Browser < – SSL – > BrainCert Enterprise SSL proxy < – SSL – >
`api.braincert.com`

Follow the instructions below and we promise it will only take less than 5 minutes. :)

- [Step 1 - Create CNAME record in your DNS server](#)
- [Step 2 - Map your custom hostname](#)
- [Step 3 - Generate SSL Certificate](#)
- [Step 4 - Turn off CloudFlare orange cloud](#)
- Step 5 - Testing your SSL hostname
 - [Check CNAME mapping](#)
 - [Check SSL Certificate](#)

Step 1 - Create CNAME record in your DNS server

Log in to your domain registrar's site and locate the Zone File Settings, DNS Manager, or similar area of your control panel. Here you will create a CNAME record that points your domain to **api.braincert.com**. You'll generally see three fields

Alias - For example, **www** or **live**

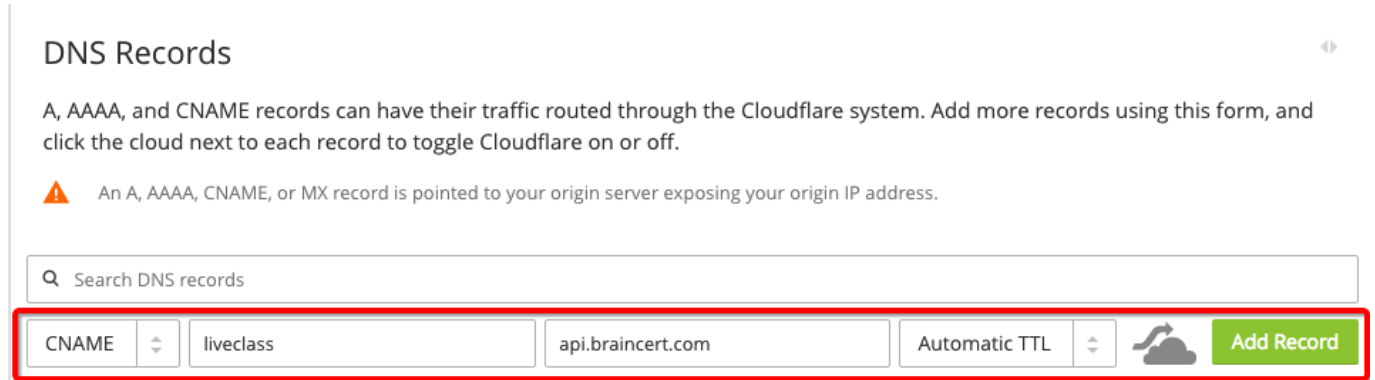
(indicating that the `www.yourdomain.com` or `liveclass.yourdomain.com` record should point to `api.braincert.com`)

Record Type - Should be CNAME

(indicating that you would like to point to BrainCert by using its name)

Points To - Should be `api.braincert.com`

In this example, we are using CloudFlare as DNS server. Select CNAME as the entry, and alias as "liveclass" that points to our API endpoint `api.braincert.com`. If you are using CloudFlare, remember to turn off orange cloud for this entry to grey cloud. You can create similar CNAME entry with any registrar where your domain is registered such as Namecheap, Godaddy, 1and1, and so on.



The screenshot shows the Cloudflare DNS Records management interface. At the top, it says "DNS Records" and provides instructions: "A, AAAA, and CNAME records can have their traffic routed through the Cloudflare system. Add more records using this form, and click the cloud next to each record to toggle Cloudflare on or off." Below this is a warning icon and text: "An A, AAAA, CNAME, or MX record is pointed to your origin server exposing your origin IP address." A search bar is present with the text "Search DNS records". The main form is highlighted with a red border and contains the following fields: a dropdown menu set to "CNAME", a text input field containing "liveclass", another text input field containing "api.braincert.com", a dropdown menu set to "Automatic TTL", a cloud icon, and a green "Add Record" button.

Note: Depending on your provider you may already have a CNAME set up with your domain Alias. If so, you will need to edit this existing CNAME so that 'Points To' is `api.braincert.com`

Step 2 - Map your custom hostname

To map an external domain, go to Virtual Classroom API [dashboard](#) and click on the "Hostname and SSL Certificate" tab on the left.



Type your custom hostname that you would like to use and click button "set custom hostname". You don't need to type `http://` or `https://` as part of the hostname at this time. In this example, we have used `liveclass.eduweaver.com` as custom hostname.



Make sure you click "Set custom hostname" to save your changes.

Step 3 - Generate SSL Certificate

After completing step 2, now it is time to generate your free enterprise SSL certificate. Until today, your best bet with other platforms was to CNAME your hostname to their infrastructure, having you generate a private key and CSR, send the latter to a CA for signing, and then securely provide them with the key material (and again upon renewal). Or maybe you have engineering resources to spend and can build and maintain a solution to generate and securely store private keys, acquire and renew certificates, and push them to a CDN so TLS can be terminated in a performant manner (i.e., as close to your customers' users as possible). Whichever route you choose, the technical complexity

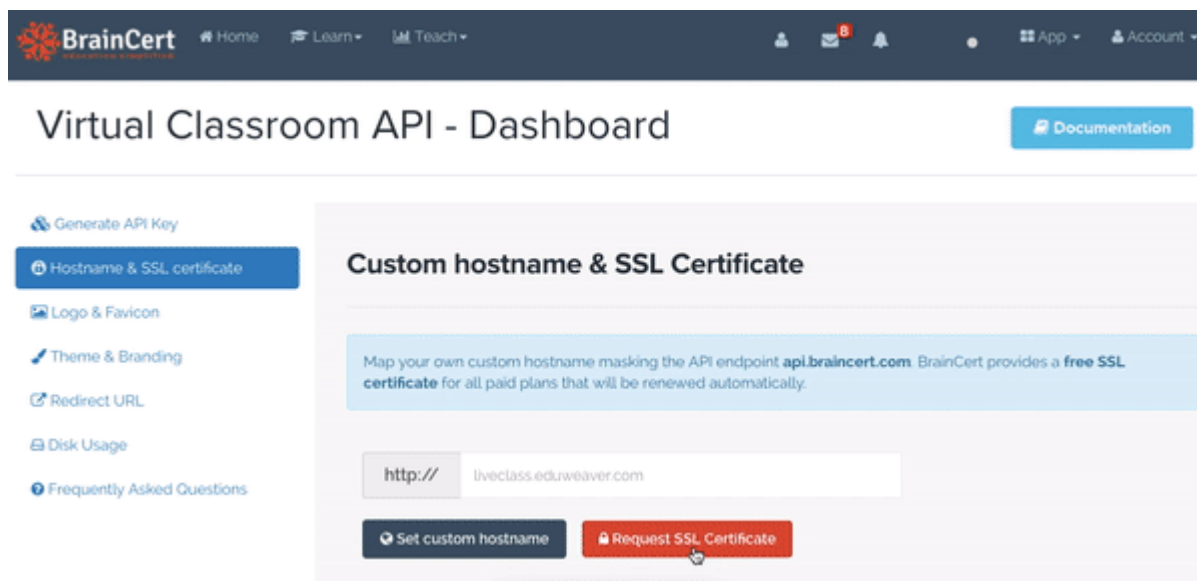
and burden of maintenance is high—either for your customers or your engineering and support teams.

BrainCert's free enterprise SSL certificate was built with these difficulties in mind, and solves this with the simplicity that you would expect. With our highly-secure SSL certificate, all you have to do is to CNAME your domain to the API endpoint in order to receive the performance and security benefits of BrainCert. Furthermore, there is no need to send us your SSL certificate key or CSR.

Click on the button "Request SSL Certificate" to get started.



You will see a popup with clear instructions guiding you with this SSL certificate process.



Once done, click on the "Finish" green button in the popup to finish the SSL setup process. Once the CNAME is in place and BrainCert takes care of the rest. We'll provision the hostname at our edge for forwarding on to your specified origin, acquire SSL certificates to enable HTTPS and HTTP/2, and sit in front of any DDoS or L7 attacks that may target your custom hostname. All the benefits of BrainCert's enterprise network, including CDN and content optimization, are extended to your custom hostname without you having to do anything other than adding a simple DNS record.

Additionally, because this SSL solution is built on BrainCert's industry leading SSL/TLS implementation, your customers visiting your custom virtual classroom hostname (external domain) will benefit from all of the work we've done to make HTTPS fast, secure, and reliable such as deploying OCSP stapling, implementing TLS 1.3 (and 0-RTT), and optimizing TLS over TCP. Most importantly, by terminating these TLS connections as physically close to your customers as possible (as opposed to directly on your origin), your customers will benefit from the most interconnected network on the internet.

Click on the "Hostname and SSL Certificate" tab on the left navigation. You will now see that your domain field is greyed out and cannot be edited. This is because SSL certificate is now active for this hostname. You will also see the info icon on the right side of the hostname field which also confirms that SSL certificate is now active.



When you click on the info icon or "Request SSL Certificate" button again, you will see a popup with

the success message.



To change hostname, click on the delete icon to start all over again.



Click on the "I agree" green button to confirm deletion of your SSL certificate.



Step 4 - Turn off CloudFlare orange cloud

If you currently using CloudFlare for SSL proxying, we recommend you to turn off the orange cloud to grey cloud to receive the performance and security benefits of BrainCert. Please note that this is required only for the CNAME record that is pointing to `api.braincert.com`. You may continue to use CloudFlare for all your other records if needed.



Orange clouded connections will not be allowed after August 27, 2017.

Step 5 - Testing your SSL hostname

Congratulations! Now that you have completed all the steps, it is now time to verify the CNAME mapping and SSL certificate.

Check CNAME mapping

You can use dig tool in your command prompt to check the CNAME mapping. You should see your hostname with correct CNAME mapping to `api.braincert.com`.

```
$ dig liveclass.eduweaver.com
; <<>> DiG 9.8.3-P1 <<>> liveclass.eduweaver.com
;; global options: +cmd
;; Got answer:
;; ->HEADER<<- opcode: QUERY, status: NOERROR, id: 38036
;; flags: qr rd ra; QUERY: 1, ANSWER: 6, AUTHORITY: 0, ADDITIONAL: 0
;; QUESTION SECTION:
;liveclass.eduweaver.com. IN A
;; ANSWER SECTION:
liveclass.eduweaver.com. 300 IN CNAME api.braincert.com.
api.braincert.com. 300 IN A 104.17.196.79
```

```
api.braincert.com. 300 IN A 104.17.195.79
api.braincert.com. 300 IN A 104.17.194.79
api.braincert.com. 300 IN A 104.17.193.79
api.braincert.com. 300 IN A 104.17.192.79
;; Query time: 35 msec
;; SERVER: 192.168.1.1#53(192.168.1.1)
;; WHEN: Tue Aug  1 12:23:41 2017
;; MSG SIZE rcvd: 149
```

Check SSL Certificate

Open your browser and go to your custom hostname in the format <https://liveclass.eduweaver.com/v2>. Change liveclass.eduweaver.com to your own hostname. You will see a green lock icon that confirms a secure SSL connection.



If you see a browser error similar to the message below, it means that your SSL certificate is not setup correctly. The connection is not secure and virtual classroom will not work.

