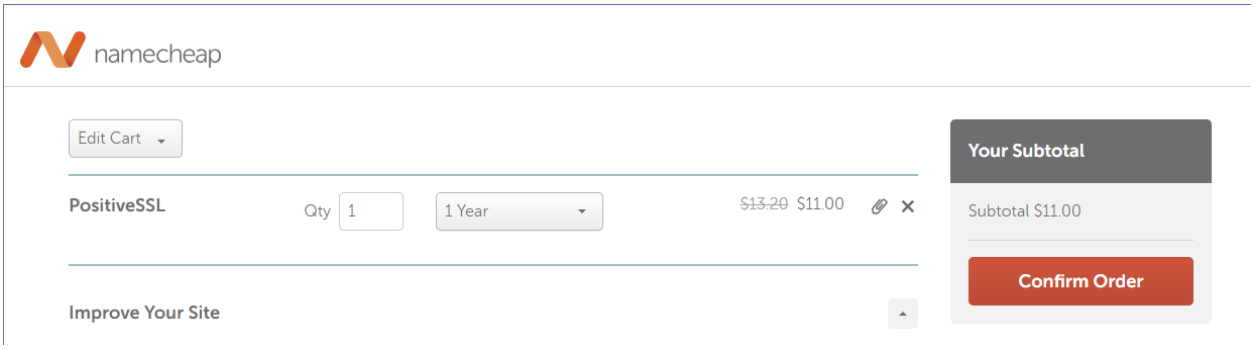
SSL Generation and Updating Process

Step 1:

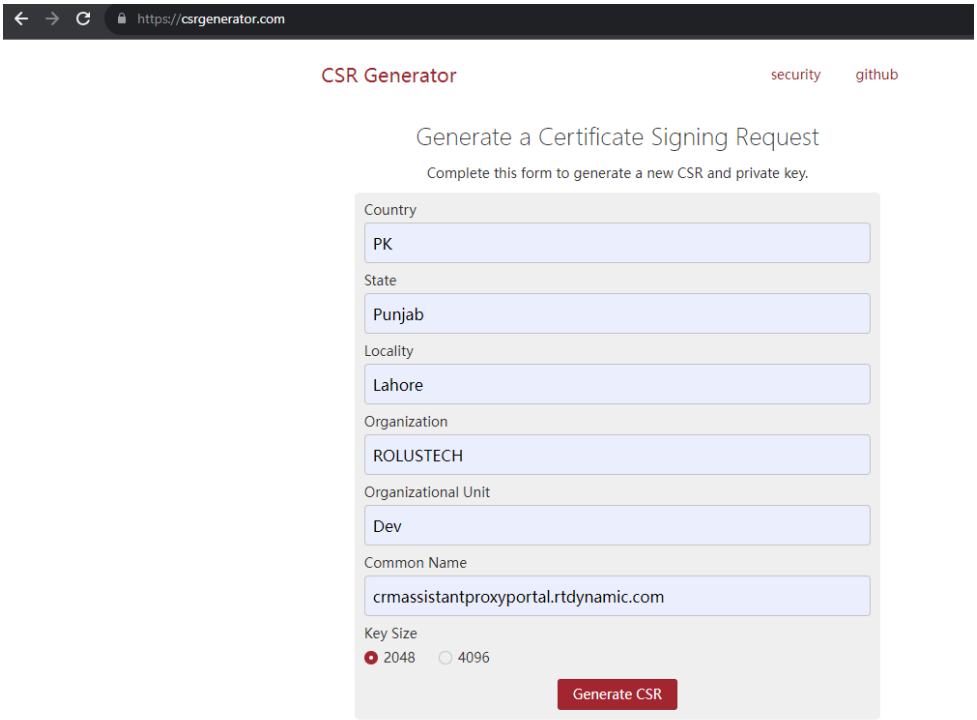
Buy SSL certificate from any SSL provider. I choose name cheap.



Step 2:

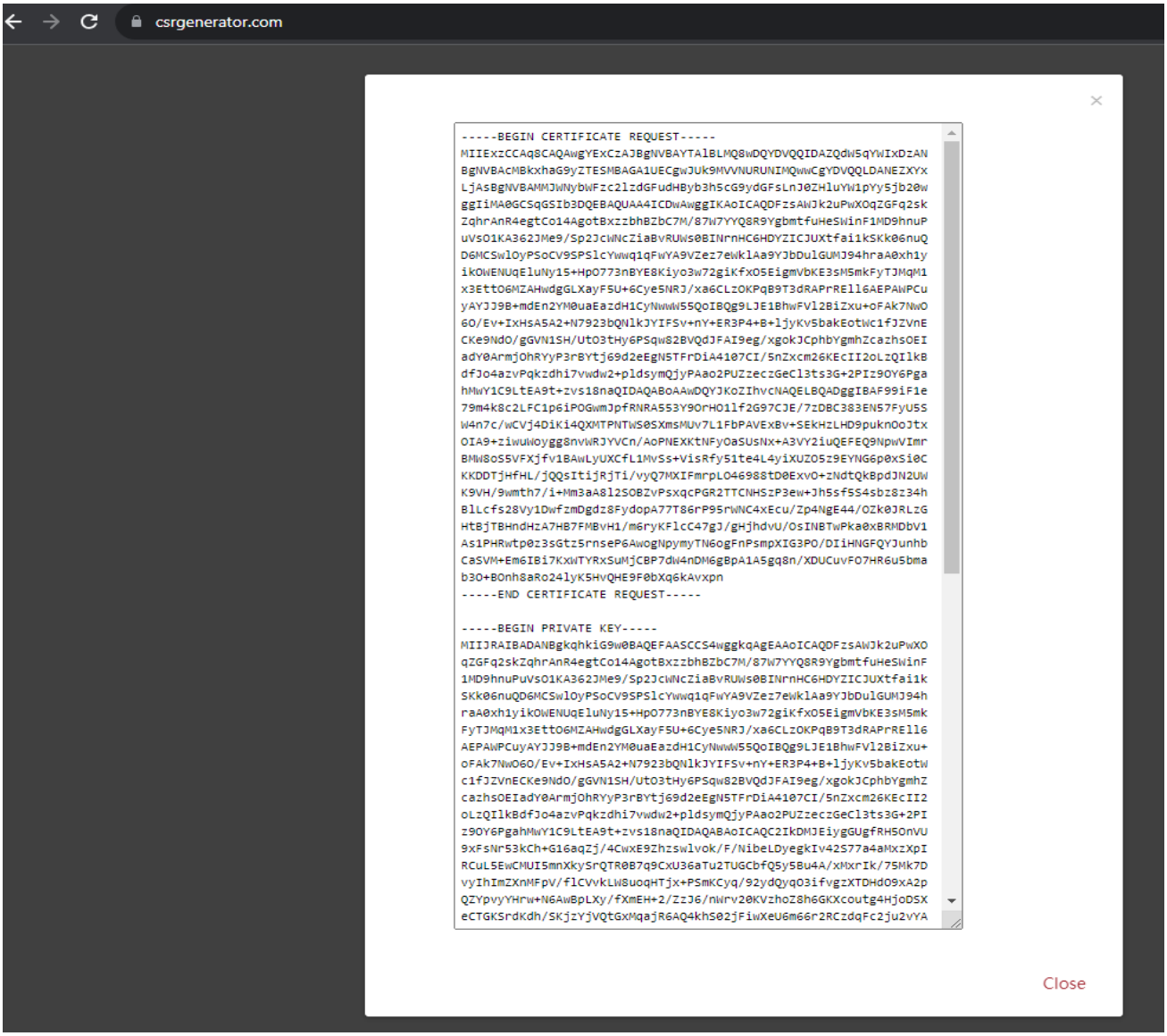
Create CSR , for that go to https://csrgenerator.com/ and enter details.

In my case I have to set SSL on this domain. https://crmassistantproxyportal.rtdynamic.com



After entering this detail, Click and **Generate CSR**.

This generate CSR key and private key,



Now copy and save it to notepad.

Copy Private Key and place it in separate file, after that save it. Save the File with extension of **.key**. File name can be domain name (which is the site name you want SSL for).

CSR code start from **BEGIN CERTIFICATE REQUEST** and ends on **END CERTIFICATE REQUEST**

This is used in **Step 3**

Step 3:

In the dashboard choose SSL certificate, find new SSL certificate and click **Active**

Enter the CSR code and Domain name to proceed.

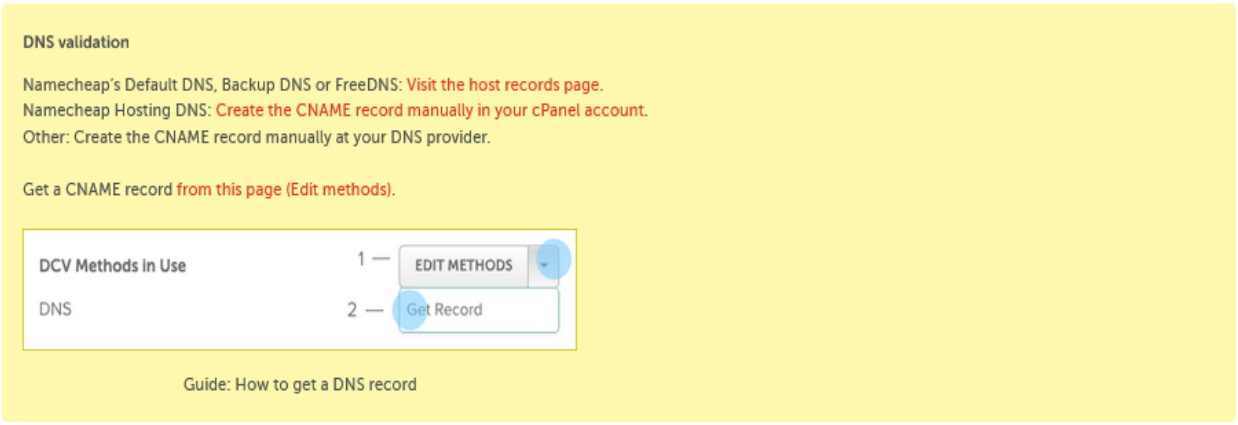
Step 4:

It will ask to choose Validation method.

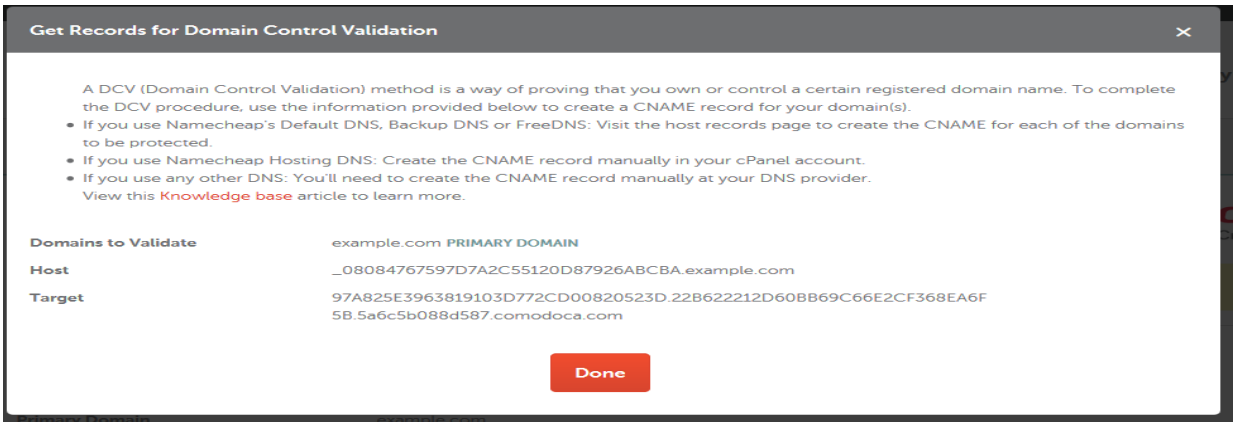
Add CNAME record

This validation method involves adding a CNAME record to the DNS settings of your domain.

After you complete SSL activation, you'll find instructions on completing this DCV method as well as the values you will need for the CNAME record in the SSL Details page of your account:



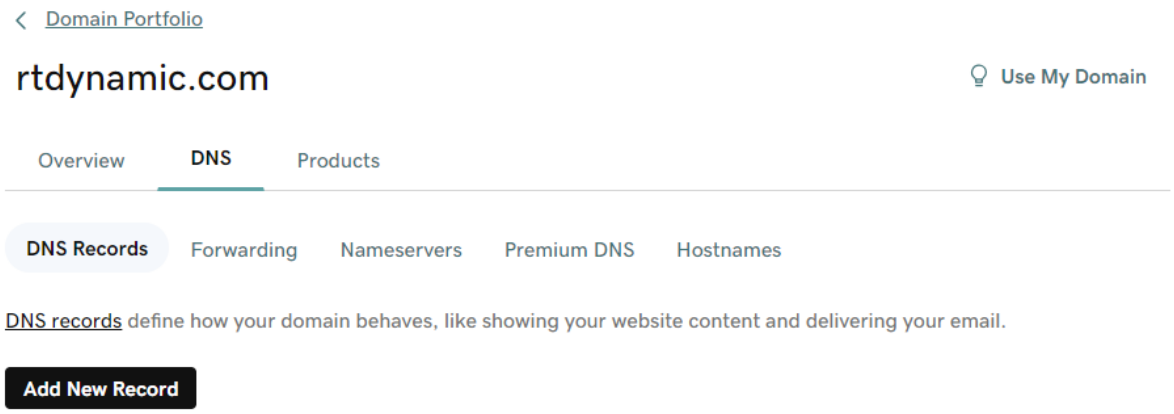
Click on Get Record to see the CNAME record values.



Step 5:

Go to site where you have site hosted to set CNAME record, for my scenario I have it hosted on **godaddy.com**

Go to Domain => DNS =>

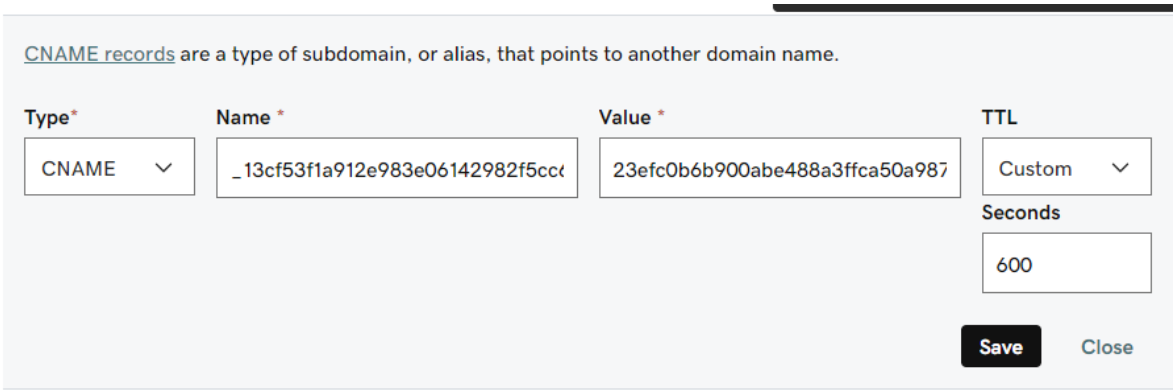


Click on **Add New Record:**

Enter **Name** and **Value** which is given in get record Image. (shown Above)

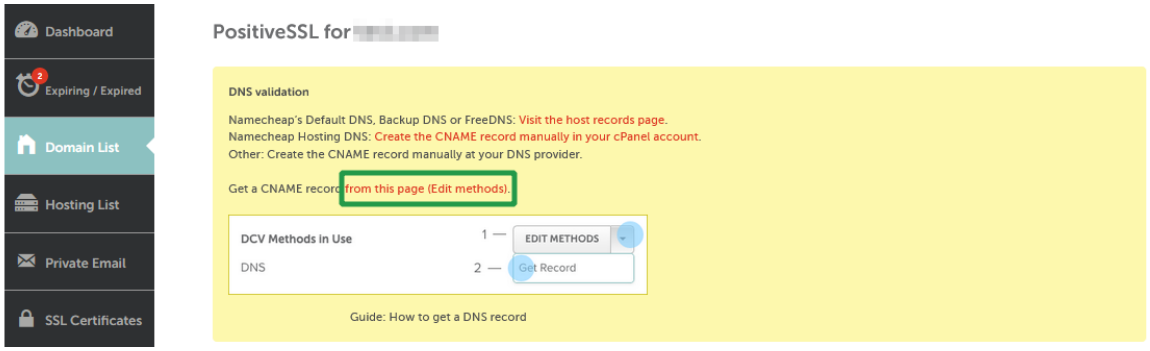
After that save it.

Please refer to picture shown below.

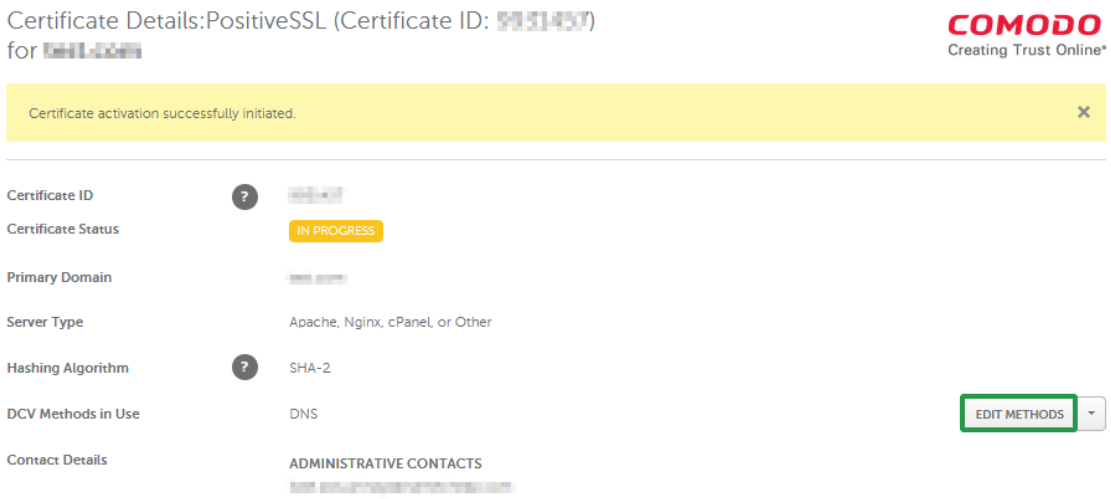


Step 6:

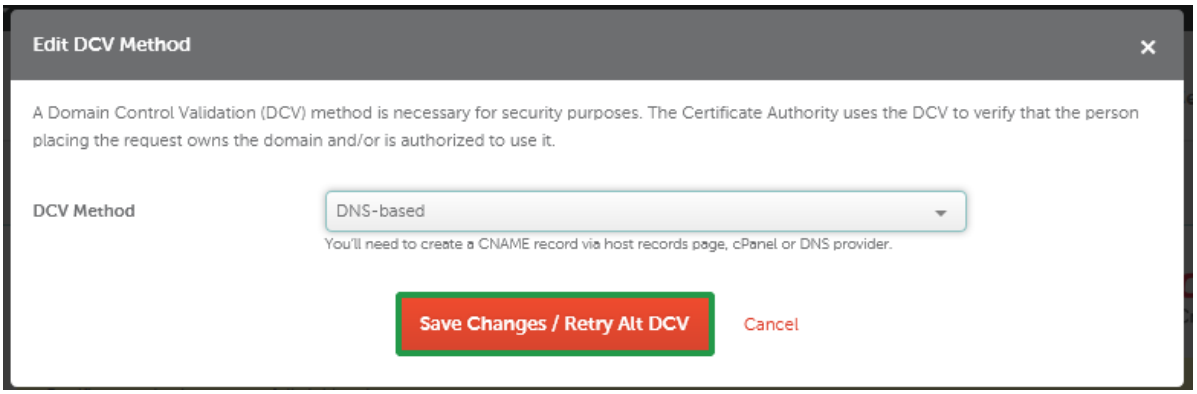
Once the correct values are set up, head to the SSL details page again, click the link beside "Get a CNAME record".



On the new page, click the 'EDIT METHODS' button.



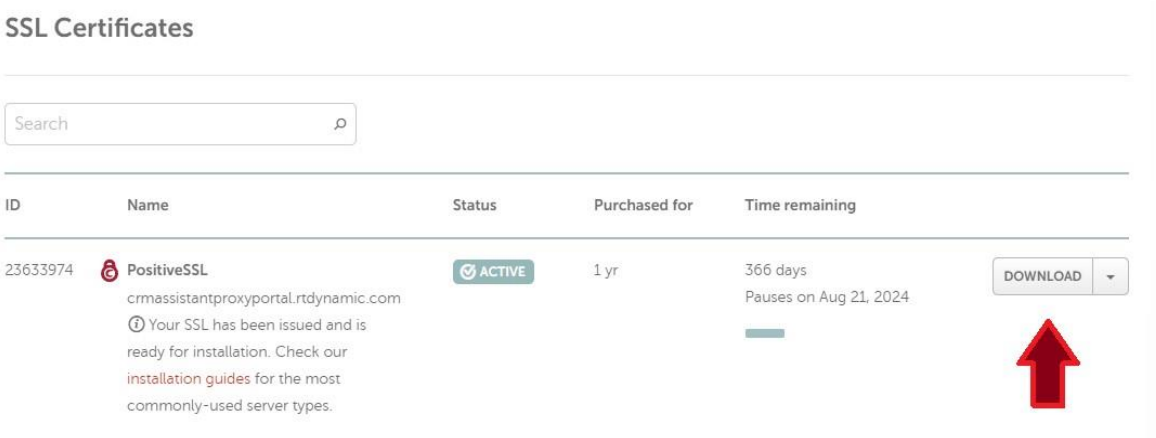
In the pop-up window, please click Save Changes/Retry Alt DCV to speed up the process of domain control validation.



After this SSL will be enabled.

Step 7:

Download the SSL certificate as shown in figure.



Step 8:

Extract the downloaded file and copy the **.key** file from Step 2 and place it in current folder.

Follow the given step for SSL update.

- Login into the respective instance/server
- Check the path where the current SSL files are placed (Mostly are available here as per our pattern --> /etc/apache2/ssl)

- Move the currently available three files to some other directory for a backup purpose (Move to /opt/create-new-dir)
- Upload the file into same directory (/etc/apache2/ssl)
- Also update the SSL certificate name and path in https virtual host (in my case its /etc/apache2/sites-available/default-ssl.conf)
- Restart the web service and verify

It should be all set now.