There are several types of SSL certificates that can be used to protect your Hudu instance. In this tutorial, we will use a Domain Verification ("DV") certificate from Comodo SSL Store: https://comodosslstore.com . Other certificate authorities other than DV exist and the process for purchasing and installing the certificates for Hudu are very similar.

1. Purchase your DV certificate from the authority of your choice. During the process it will ask you to paste your csr. Typically, the authority will ask you what your webserver is. Hudu uses NGINX, which is not listed at Comodo, and you will have to answer OTHER.

2. Generate your CSR on the Hudu host, as follows:

    a. Login to your Hudu host. Go into the /var/www/hudu2/config/keys folder. Depending on how you installed, you may need to create the keys folder.

    b. Run ***openssl req -new -newkey rsa:2048 -nodes -keyout server.key -out server.csr***
    Note: Replace "server" with the domain name you intend to secure.

    c. Enter the following CSR details when prompted:

        1. Common Name: The FQDN (fully-qualified domain name) you want to secure with the certificate s0uch as **www.google.com**, secure.website.org, *.domain.net, etc.

        2. Organization: The full legal name of your organization including the corporate identifier.

        3. Organization Unit (OU): Your department such as 'Information Technology' or 'Website Security.'

        4. City or Locality: The locality or city where your organization is legally incorporated. Do not abbreviate.

        5. State or Province: The state or province where your organization is legally incorporated. Do not abbreviate.

        6. Country: The official two-letter country code (i.e. US, CH) where your organization is legally incorporated.

3. This will create a yourdomain.csr in your keys folder. You will want to "more" this file and take a copy including the beginning and ending parts of the CSR.

4. Paste into the authority website asking for the CSR.

5. This process will also generate your private key, which will have an extension of .KEY

6. Comodo will email you your certificate (others may want you to download them).

    i) This will include your intermediate Key and your public key. The intermediate certificate will be the one for NGINX.
    ii) Copy the Certificate Files into the /var/www/hudu2/config/keys folder
    Note: For better security, make them readable by root only.

iii) You need to link the two certificates (or "Concatenate" them) into a single file by entering the command below:
cat your_domain_name.crt Intermediate.crt >> bundle.crt

iv) You will need to validate your keys by responding to an email. Check that you have access to the email on the domain. Typically this may be webmaster@yourdomain.com or admin@yourdomain.com. Click the validation link or copy and paste the code given.

v) Your authority should show validated before your certificate will work.

7. Edit your default file in /var/www/hudu2/config/nginx/sites-conf/

   i) Change the private key to your private key name (i.e., hudu.yourdomain.com.key)

8. Restart Hudu docker by changing into the hudu2 folder (cd ~/hudu2) and run sudo docker-compose down && docker-compose up -d

9. Your SSL certificate will now be active.