**HTTP TO HTTPS REDIRECTION FOR WISECOW SCRIPT**

 Here I have used self signed certificates where http to https redirection will happen in my host device

In this documentation I have included the steps to create certificates,nginx configuration and other required configurations

**SELF-SIGNED CERTIFICATE**

**Generate Root CA Private Key (Encrypted)**

openssl genrsa -out wisecow-RootCA.key 4096

openssl req -x509 -new -key wisecow-RootCA.key -sha256 -days 3650 -out nabla-RootCA.crt -subj "/C=US/ST=California/L=San Francisco/O=Nabla/CN=Nabla Root CA"

**This creates nabla-RootCA.crt — your self-signed Root CA certificate.**

**Generate Private Key for GitLab Domain**

openssl genrsa -out wisecow-test.com.key 2048

**This is the key Wisecow will use for SSL.**

**Create Certificate Signing Request (CSR)**

openssl req -new -key wisecow-test.key -out wisecow-test.com.csr -subj "/C=IN/ST=Maharashtra/L=Pune/O=Nabla/CN=wisecow-test.com"

**This generates a CSR, which we will sign next.**

**Create a file called wisecow-test.ext with the following content:**

authorityKeyIdentifier=keyid,issuer  
basicConstraints=CA:FALSE  
keyUsage = digitalSignature, nonRepudiation, keyEncipherment, dataEncipherment  
subjectAltName = @alt\_names

[alt\_names]  
DNS.1 = wisecow-test.com  
DNS.2 = [www.wisecow-test.com](http://www.nabla-gitlab.com)

**You can add more DNS entries or IPs under [alt\_names] if needed.**

**Sign the GitLab Certificate with Your Root CA**

openssl x509 -req \  
 -in wisecow-test.com.csr \  
 -CA wisecow-RootCA.crt \  
 -CAkey wisecow-RootCA.key \  
 -CAcreateserial \  
 -out wisecow-test.com.crt \  
 -days 825 \  
 -sha256 \  
 -extfile wisecow-test.ext

**This creates the signed certificate wisecow-test.com.crt for use in GitLab.**

**After completing all the above steps, we will have generated following files**

wisecow-RootCA.key wisecow-test.com.crt wisecow-test.com.key

wisecow-RootCA.crt wisecow-RootCA.srl wisecow-test.com.csr

**Some of them are needed in the next configurations**

**NGINX CONFIGURATION**

**Open the path /etc/nginx/conf.d/ and make a file name wisecow-test.com.conf and inside it put the following configuration**

server {

listen 80;

server\_name wisecow-test.com;

return 301 https://wisecow-test.com;

}

server {

listen 443 ssl;

server\_name wisecow-test.com;

ssl\_certificate /etc/ssl/wisecow-test.com.crt;

ssl\_certificate\_key /etc/ssl/wisecow-test.com.key;

location / {

proxy\_pass http://localhost:9100;

proxy\_set\_header Host $host;

proxy\_set\_header X-Real-IP $remote\_addr;

proxy\_set\_header X-Forwarded-For $proxy\_add\_x\_forwarded\_for;

proxy\_set\_header X-Forwarded-Proto $scheme;

proxy\_connect\_timeout 60s;

proxy\_send\_timeout 60s;

proxy\_read\_timeout 60s;

send\_timeout 60s;

proxy\_buffers 4 256k;

proxy\_buffer\_size 128k;

proxy\_busy\_buffers\_size 256k;

**Make sure wisecow-test.com.crt and wisecow-test.comkey are present in the /etc/ssl/ folder**

**After saving the file run the following commands**

sudo nginx -it

sudo nginx -s reload

**It will test for errors in configuration and the reload the nginx with new configuration**

**Now add the wisecow-RootCA.crt** **in the /usr/local/share/ca-certificates/ folder**

**Now run the command**

sudo update-ca-certificates

**After this add the wisecow-RootCA.crt in the certificate section of your web browser**

**I am using wsl so I also update host file of windows and added the following line**

127.0.0.1 wisecow-test.com

**After this configuration the output should be like this**

**Double tap the below shown recording for result**

A screenshot of a computer

AI-generated content may be incorrect.

****