**Steps for enabling https connection in NGINX:**

• Install in local machine through OpenSSL from the website below.

<https://slproweb.com/products/Win32OpenSSL.html>

Win64 OpenSSL v3.1.3 Light EXE version

• Set OpenSSL path in environment variable.

• In the command line -

Generate the RSA private key

openssl genrsa -des3 -out selfsign.key 4096

Enter the password for the key (password):

• The next step is to sign the request for our signature.

openssl req -new -key selfsign.key -out selfsign.csr

openssl x509 -req -in selfsign.csr -signkey selfsign.key -out selfsign.crt -days 365

Enter the password for the key (password):

Fill in the details

• Do ls to see myhostname.key and myhostname.csr is created.

• The key file we have is password protected, if we are going to use this in nginx every time the server starts or restarts, we have to enter a password for our key, now we don't want to do that, so we go for remove password

• We will create a copy of myhostname, call this myhostname.key for the password, the password version will have a .pwd extension after ie;

copy selfsign.key selfsign.key.pw

openssl rsa -in selfsign.key.pw -out selfsign.key

which will overwrite the previous one with this list of password versions, but for that we need to enter the password.

Enter the password for the key (password):

• Now we need to sign it with

openssl x509 -req -in selfsign.csr -signkey selfsign.key -out selfsign.crt -days 365

* To check the validity of the certificate

openssl x509 -noout -enddate -in selfsign.crt

• Store the SSL certificates in the nginx configuration directory.

• Go to gitlab->Infovision->JSW ->common-services ->frontend->mdm-mfe->milestone-3

Create an own branch from ms3 to update and test the changes.

Now in own branch click on devops repo and replace/add the crt and key files

And update it.

* Now create a MR to Milestone3 and get reviewed by Lead and merge
* In dev environment redeploy the mdm-mfe after the pipeline got succeded.

To verify check in browser <https://10.0.3.156/mdm/swagger-ui/index.html>

Click on not secure URL -> certificate is not valid ->general

You can find under validity period

A screenshot of a computer

Description automatically generated

**Existing process:**

• Now scp the crt file and the key to the tmp folder on the IVL server

scp myhostname.crt myhostname.key administrator@10.0.3.156:/tmp/

Password:

• Login to IVL dev server 10.0.3.156

cd /usr/share/nginx

cp /tmp/myhostname.crt /etc/nginx/server.crt

cp /tmp/myhostname.key /etc/nginx/server.key

vi /etc/nginx/nginx.conf

**nginx conf file:**

worker\_connections 1024;

}

http {

include mime.types;

default\_type application/octet-stream;

server {

listen 80 default\_server;

server\_name \_;

return 301 https://$host$request\_uri;

}

server{

listen 443 ssl;

server\_name localhost;

ssl\_certificate server.crt;

ssl\_certificate\_key server.key;

ssl\_session\_timeout 5m;

ssl\_protocols TLSv1.2 TLSv1.3;

ssl\_ciphers HIGH:!aNULL:!MD5;

ssl\_prefer\_server\_ciphers on;

location / {

root html/crm-base;

index index.html;

}

location /crm-base {

try\_files $uri $uri/ /index.html;

}

location /aas {

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

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

proxy\_set\_header Host $http\_host;

proxy\_pass http://localhost:8089;

}

location /mdm {

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

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

proxy\_set\_header Host $http\_host;

proxy\_pass http://localhost:8090;

}

location /ums {

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

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

proxy\_set\_header Host $http\_host;

proxy\_pass http://localhost:8091;

}

location /ens {

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

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

proxy\_set\_header Host $http\_host;

proxy\_pass http://localhost:8093;

}

}

}

nginx -s reload

HTTPS has been enabled on our IVL dev server. Try using with links

1. <https://10.0.3.156/aas/swagger-ui/index.html>.
2. <https://10.0.3.156/mdm/swagger-ui/index.html>.
3. <https://10.0.3.156/ums/swagger-ui/index.html>.
4. <https://10.0.3.156/ens/swagger-ui/index.html>.

Note: The Highlighted yellow colour indicates commands.