ARTIGO: 11867
Como instalar SSL certificado em um NGINX server, combinar certificados num arquivo único
Isso é uma cópia de manual nesse link https://www.ssls.com/knowledgebase/how-to-install-an-ssl-certificate-on-a-nginx-server/

Vou clonar aqui só pra garantir de ter mais um... lol

--- atualização ---
na verdade esse comando funciona

```
cat end-user.crt <(echo) intermediate.pem <(echo) root.crt > bundled.crt
```

```
exemplo: cat www.4gym.com.br.crt <(echo) www.4gym.com.br.ca-bundle <(echo) >  bundled-new.crt
```

os comando abaixo aqui deu erro, kkkkrssrrsrs
--- fim atualiza

After the certificate is issued and sent to you by the Certificate Authority, you can proceed with the certificate installation on your Nginx server.

Combine certificates into one file

First of all, you need to concatenate the certificate issued for your domain with intermediate and root certificates into one file. The order of the certificates in the file is important. The certificate for your domain name should go first, intermediate certificates should follow it and the last certificate in the chain should be the root one.

You can combine the files either manually, copying and pasting the correspondent certificates into one single file or you can use the following commands if the certificate files were uploaded to the server:

1) If you received and uploaded the intermediate and root certificates separately, please use this method:

cat your_domain.crt intermediate.crt root.crt >> ssl-bundle.crt

For example, this particular command is applicable for PositiveSSL certificate:

cat example_com.crt COMODORSADomainValidationSecureServerCA.crt COMODORSAAddTrustCA.crt AddTrustExternalCARoot.crt >> ssl-bundle.crt

2) If you received the intermediate certificates in one bundle file or downloaded the certificate files in your account with us, you can use this command:

cat example_com.crt bundle.crt >> ssl-bundle.crt

Place the concatenated file into the directory with SSL certificates on your Nginx server.

Edit your Nginx configuration file

After the certificate is uploaded, you need to modify your Nginx configuration file (by default it is called nginx.conf) and edit or add virtual host for 443 port for your website.

If there is no virtual host for 443 port, you can duplicate the record for port 80 (it should be in the configuration file by default) and change port 80 to port 443. Simply add it below the non-secure module.

In addition you will need to add the special lines in the record:

ssl on;

ssl_certificate should be pointed to the location of the concatenated certificate file;

ssl_certificate_key should be pointed to the location of the private key generated along with the CSR that was used for the certificate activation.

The completed Virtual Host should look something like this:

server {

listen 443;

ssl on;

ssl_certificate /etc/ssl/ssl-bundle.crt;

ssl_certificate_key /etc/ssl/ssl-tutorials.key;

server_name ssl-tutorials.com;

access_log /var/log/nginx/nginx.vhost.access.log;

error_log /var/log/nginx/nginx.vhost.error.log;

location / {

root /var/www/;

index index.html;

}

}

If you want to configure OCSP Stapling on your server, please add the following lines to the virtual host section for the website:

ssl_stapling on;
ssl_stapling_verify on;

Note: OCSP Stapling can be configured on Nginx server starting from 1.3.7+

After the modifications are saved, please restart the Nginx server to apply the changes.