

Server Certificates

CoAPs

Devices can use secure CoAPs connections to the backend. To use CoAPs a Certificate signed by Lobaró is required.

The setup consists of the following steps:

1. Create a Certificate Signing Request (CSR)
2. Request a Certificate from Lobaró
3. Install the signed Certificate in the Platform

Create a Certificate Signing Request (CSR)

Create Private Key

The key must be created at the Platform server and should never leave the system.

```
openssl ecparam -name prime256v1 -genkey -noout -out platform.key
```



Do not send the resulting private key file `platform.key` to anyone.

Create CSR

Update "-subj" parameter in the command below according to your server and organisation.

- C is Country Name: e.g. C=DE
- ST is State or Province Name (full name): e.g. ST=Hamburg
- O is Organization Name (eg, company): e.g. O=Lobaró GmbH
- CN is Common Name (e.g. server FQDN or YOUR name): e.g. CN=up.lobaró.com
 - The CN **must** match your domain that is configured in the devices. It can also be an IP address.

```
openssl req -new -key platform.key -sha256 -subj "/C=DE/ST=Hamburg/O=Lobaró GmbH/CN=up.lobaró.com" -out "platform.csr"
```

Verify your request with:

```
openssl req -text -noout -in platform.csr
```

Request Certificate from Lobaró

Send the generated CSR file (**platform.csr**) to support@lobaró.de to receive a valid certificate for your Server.

Install the signed Certificate in the Platform

Add or update the following keys in the Platform configuration file:

```
server:
  dtlsConfig:
    dtlsCertDir: "./config" # This way the configuration directory is used to lookup the key and cert.
    dtlsCertName: "platform" # Used to lookup "platform.crt" and "platform.key"
  featureToggle:
    dtlsSecureCoapServiceEnabled: true # removed in > v1.59.1
```



We recommend to **do no backup of the `platform.key`** file. If it's lost, we can issue new certificates.

If you need to backup the key file make sure the backup is encrypted in a secure way.

In case you choose another location than "`./config`" the `docker-compose.yml` must be updated to mount the `dtlsCertDir`:

```
services:
  lobar-backend:
    volumes:
      - </host/path/to/cert-dir>:<dtlsCertDir>
```

To apply the Configuration restart the Platform:

```
docker restart platform_lobar-backend_1
```



In case the commands fails with e.g.

Error response from daemon: No such container: `platform_lobar-backend_1`

Execute

```
docker ps | grep lobar
```

You should find the container that is running the platform. The restart command can be issued with the `CONTAINER ID` or `NAME`