

Certification HTTPS

Installez certbot sur ubuntu 20 : <https://certbot.eff.org/instructions?ws=other&os=ubuntu>

```
root@ubuntu-js:~# certbot
Saving debug log to /var/log/letsencrypt/letsencrypt.log
Enter email address (used for urgent renewal and security notices)
(Enter 'c' to cancel): si@valoxy.fr

-----
Please read the Terms of Service at
https://letsencrypt.org/documents/LE-SA-v1.3-September-21-2022.pdf. You must
agree in order to register with the ACME server. Do you agree?
-----
(Y)es/(N)o: y

-----
Would you be willing, once your first certificate is successfully issued, to
share your email address with the Electronic Frontier Foundation, a founding
partner of the Let's Encrypt project and the non-profit organization that
develops Certbot? We'd like to send you email about our work encrypting the web,
EFF news, campaigns, and ways to support digital freedom.
-----
(Y)es/(N)o: n
Account registered.
Please enter the domain name(s) you would like on your certificate (comma and/or
space separated) (Enter 'c' to cancel): valostart.fr
Requesting a certificate for valostart.fr

Successfully received certificate.
Certificate is saved at: /etc/letsencrypt/live/valostart.fr/fullchain.pem
Key is saved at: /etc/letsencrypt/live/valostart.fr/privkey.pem
This certificate expires on 2023-09-10.
These files will be updated when the certificate renews.
Certbot has set up a scheduled task to automatically renew this certificate in t
he background.

Deploying certificate
Successfully deployed certificate for valostart.fr to /etc/apache2/sites-availab
le/000-default-le-ssl.conf
Congratulations! You have successfully enabled HTTPS on https://valostart.fr

-----
If you like Certbot, please consider supporting our work by:
* Donating to ISRG / Let's Encrypt: https://letsencrypt.org/donate
* Donating to EFF: https://eff.org/donate-le
-----
```

Copié/Collé le code dans le fichier racine (app.js ou index.js) (yourdomain.com dans le code à échangé)

```
// Dependencies

const fs = require('fs');
const http = require('http');
const https = require('https');
const express = require('express');

const app = express();

// Certificate

const privateKey = fs.readFileSync('/etc/letsencrypt/live/yourdomain.com/privkey.pem', 'utf8');
const certificate = fs.readFileSync('/etc/letsencrypt/live/yourdomain.com/cert.pem', 'utf8');
const ca = fs.readFileSync('/etc/letsencrypt/live/yourdomain.com/fullchain.pem', 'utf8');

const credentials = {
  key: privateKey,
  cert: certificate,
  ca: ca
};

// Starting both http & https servers

const httpServer = http.createServer(app);
const httpsServer = https.createServer(credentials, app);

httpServer.listen(80, () => {
  console.log('HTTP Server running on port 80');
});

httpsServer.listen(443, () => {
  console.log('HTTPS Server running on port 443');
});

//force user à https
app.enable('trust proxy')
app.use(function(request, response, next) {

  if (process.env.NODE_ENV !== 'development' && !request.secure) {
    return response.redirect("https://" + request.headers.host + request.url);
  }

  next();
})
```

Vérifiez votre site :

 <https://oliv.valoit.fr/index>