Security

- *.SO.local Self Signed SSL Certificate

*.SO.local Self Signed SSL Certificate

Expires : 06 2036

so.local.wildcard.self-signed.2026-2036.crt (http://www.so.local/ssl/so.local.wildcard.self-signed.2026-2036.crt)

so.local.wildcard.self-signed.2026-2036.key (http://www.so.local/ssl/so.local.wildcard.self-signed.2026-2036.key)

Import the certificate on end user devices

manually import the `server.crt` file into the trusted root store of every device accessing the site:

- **Windows:** Double-click `server.crt` -> Click **Install Certificate** -> Choose **Local Machine** -> Choose **Place all certificates in the following store** -> Browse and select **Trusted Root Certification Authorities**.
- **macOS:** Double-click `server.crt` to open Keychain Access. Drag it into the **System** keychain. Double-click the imported certificate, expand the **Trust** section, and change "When using this certificate" to **Always Trust**.
- **Linux (Ubuntu/Debian):** Copy the file to `/usr/local/share/ca-certificates/server.crt` and run `sudo update-ca-certificates`.
- **iOS / Android:** You must email/airdrop the `.crt` file to the device, install it via settings, and (on iOS) specifically go to *Settings -> General -> About -> Certificate Trust Settings* to enable full trust for it.

Locations currently used

Nginx Proxy Manager on Ubuntu Server

How to create another one,

sudo apt-get install openssl

nano ssl.conf

```
[req]
default_bits       = 2048
default_keyfile    = server.key
```

```
distinguished_name = req_distinguished_name
req_extensions     = v3_req
x509_extensions    = v3_req
prompt             = no

[req_distinguished_name]
C            = UK
ST           = Nottinghamshire
L            = Mansfield
O            = Sherwood Observatory
OU           = IT
CN           = *.so.local

[v3_req]
keyUsage = critical, digitalSignature, keyEncipherment
extendedKeyUsage = serverAuth
subjectAltName = @alt_names

[alt_names]
DNS.1 = so.local
DNS.2 = *.so.local
```

openssl req -x509 -nodes -days 3650 -newkey rsa:2048 -keyout server.key -out server.crt -config ssl.conf