

- New Chat
- Today
- Test Apache2 with HT
- Yesterday
- Handcrafted Laser-Cut A
- Previous 30 Days
- Python Hello World
- LED Layout in CSV
- New chat
- Barclays and Skipton Lic
- Reword Request for Con
- Discussing Financial Sup
- New chat
- Learn German with TV
- DMX Terminators and Se
- Strip and Return Integer
- Git on RPI4 Setup
- Split and Get Last Part
- New chat
- QLC+ Lighting Control S
- PHP: Calculate Days Bet
- Raspberry Pi Assistance
- SSHFS Remote Mounting
- Change Linux Mint Hostn

- August
- Resetting Default Text S
- Find Laptop GPU: Linux

Refer a friend

NEW

I dont have the unit online yet so before i go doing the proper ssl certificate i want to test apache2 is working with port 443, currently i cannot get past the page saying ""This site can't provide a secure connection""

If I connection over http with http://server.local it shows the apache2 webpage



If you're getting a "This site can't provide a secure connection" error, it indicates that the SSL/TLS handshake is failing. This might be due to a variety of reasons, such as misconfiguration or a problem with the SSL certificate. Since you're still in a testing phase and the server is not yet online, you might want to consider using a self-signed certificate for testing HTTPS connections. Here's a step-by-step guide:

Prerequisites

Ensure Apache2 is installed and running:

```
bash

sudo apt update
sudo apt install apache2
sudo systemctl start apache2
```

Copy code

Generating a Self-Signed SSL Certificate

1. Install `openssl`:

```
bash

sudo apt install openssl
```

Copy code

2. Generate a self-signed certificate:

```
bash

sudo openssl req -x509 -nodes -days 365 -newkey rsa:2048 -keyout
```

Copy code

Follow the prompts to complete the certificate details.

Configuring Apache to Use SSL

1. Enable the SSL module:

```
bash
```

Copy code

Regenerate

Send a message

