# System Security

## Overview

- [\*\*Lets Encrypt

Let's Encrypt is a free SSL certificate provider. Certbot is the official client to apply Let's Encrypt SSL certificates to your webserver. This will allow you to have `https://` (encrypted and authenticated) access to your websites.

### Requirements

To use Certbot you need:

- A working Apache, Nginx or Lighttpd webserver

- A URL/domain (e.g.: `mysite.org`). No-IP can be used for a URL/domain that points to your device.

- Ports 80 and 443 (TCP) need to be forwarded to your device. This is typically set within your router.

???+ important "Keep port 80 open for Certbot renewal"

Even when you use only HTTPS on port 443, Let's Encrypt requires port 80 to stay opened for certificate renewals (in your router's forwarding functionality).

![DietPi-LetsEncrypt interface screenshot](../assets/images/dietpi-software-security-certbot.png){: width="400" height="183" loading="lazy"}

### Create and apply your cert

Once Certbot has been installed from `dietpi-software`, run `dietpi-letsencrypt` to configure, create and apply your SSL certificate:

```sh

dietpi-letsencrypt

```

Simply enter the details and settings you require, then select `Apply`.

Let's Encrypt is that simple!

\*\*\*

Website: <https://letsencrypt.org>

## Fail2Ban

Fail2Ban protects your system from brute-force attacks by banning the source IP address.

We have enabled detection for SSH servers (OpenSSH and Dropbear), however, Fail2Ban also supports additional software.

![Fail2Ban logo](../assets/images/dietpi-software-security-fail2ban1.jpg){: width="200" height="157" loading="lazy"}

![Fail2Ban example console logs output](../assets/images/dietpi-software-security-fail2ban2.jpg){: width="550" height="360" loading="lazy"}

Source: [`Lostcontrol` of Fail2ban wiki](https://fail2ban.org/wiki/index.php/File:Fail2ban-screenshot.jpg), [GPL](https://commons.wikimedia.org/w/index.php?curid=19776087)

An IP address is by default ban triggered after 3 failed SSH login attempts. Fail2Ban will ban the source IP address for 10 minutes.

=== "Check status of block activity"

The status can be checked with these commands:

```sh

fail2ban-client status sshd

fail2ban-client status dropbear

```

=== "Enable support for additional programs"

Fail2Ban supports brute-force protection for other software (e.g. Apache, ProFTPD etc).

You can enable/disable these features by modifying the \*/etc/fail2ban/jail.conf\* file, and setting `enable = true` under the \*[software]\* name.

\*\*\*

Website: <https://fail2ban.org/wiki/index.php/Main\_Page>

[Return to the \*\*Optimised Software list\*\*](../../software/)