

Let's Encrypt `SSL`

- [Let's Encrypt \(Apache2\)](#)

Let's Encrypt (Apache2)

📄 :

OS: Debian GNU/Linux 12 (bookworm) x86_64
Host: PRO ADL-U Cubi 5 (MS-B0A8) 1.0
Kernel: 6.8.4-3-pve
Uptime: 5 hours, 52 mins
Packages: 556 (dpkg)
Shell: bash 5.2.15
Terminal: /dev/pts/3
CPU: 12th Gen Intel i7-1255U (4) @ 4.700GHz
Memory: 241MiB / 4096MiB
Apache2

1. 📄DNS📄DNS📄📄📄📄📄📄📄📄

```
apt-get update  
apt-get install certbot python3-certbot-apache -y
```

2. 📄Certbot📄

```
certbot -h
```

certbot [SUBCOMMAND] [options] [-d DOMAIN] [-d DOMAIN] ...

Certbot can obtain and install HTTPS/TLS/SSL certificates. By default, it will attempt to use a webserver both for obtaining and installing the certificate. The most common SUBCOMMANDS and flags are:

obtain, install, and renew certificates:

(default) run	Obtain & install a certificate in your current webserver
certonly	Obtain or renew a certificate, but do not install it
renew	Renew all previously obtained certificates that are near expiry
enhance	Add security enhancements to your existing configuration
-d DOMAINS	Comma-separated list of domains to obtain a certificate for

--apache Use the Apache plugin for authentication & installation
--standalone Run a standalone webserver for authentication
(the certbot nginx plugin is not installed)
--webroot Place files in a server's webroot folder for authentication
--manual Obtain certificates interactively, or using shell script
hooks

-n Run non-interactively
--test-cert Obtain a test certificate from a staging server
--dry-run Test "renew" or "certonly" without saving any certificates
to disk

manage certificates:

certificates Display information about certificates you have from Certbot
revoke Revoke a certificate (supply --cert-name or --cert-path)
delete Delete a certificate (supply --cert-name)

manage your account:

register Create an ACME account
unregister Deactivate an ACME account
update_account Update an ACME account
show_account Display account details
--agree-tos Agree to the ACME server's Subscriber Agreement
-m EMAIL Email address for important account notifications

More detailed help:

-h, --help [TOPIC] print this message, or detailed help on a topic;
the available TOPICS are:

all, automation, commands, paths, security, testing, or any of the
subcommands or plugins (certonly, renew, install, register, nginx,
apache, standalone, webroot, etc.)

-h all print a detailed help page including all topics
--version print the version number

3. `certbot`

```
certbot certonly --apache -w /var/www/xxxxxx/ -d xx.aa.bb.cc --email xxx@aa.bb.cc
```

4. `certbot`

```
ls -la /etc/letsencrypt/live/xx.aa.bb.cc
```

```
lrwxrwxrwx 1 root root 43 Jun 7 22:53 cert.pem -> ../../archive/xx.aa.bb.cc/cert1.pem
lrwxrwxrwx 1 root root 44 Jun 7 22:53 chain.pem -> ../../archive/xx.aa.bb.cc/chain1.pem
lrwxrwxrwx 1 root root 48 Jun 7 22:53 fullchain.pem -> ../../archive/xx.aa.bb.cc/fullchain1.pem
lrwxrwxrwx 1 root root 46 Jun 7 22:53 privkey.pem -> ../../archive/xx.aa.bb.cc/privkey1.pem
```

5. Apache2 conf

```
vim /etc/apache2/sites-available/xxxxxx.conf
```

```
<VirtualHost *:443>
    SSLEngine on
    ServerAdmin webmaster@localhost
    DocumentRoot /var/www/xxxxxx
    SSLCertificateFile /etc/letsencrypt/live/xx.aa.bb.cc/cert.pem
    SSLCertificateKeyFile /etc/letsencrypt/live/xx.aa.bb.cc/privkey.pem
    SSLCertificateChainFile /etc/letsencrypt/live/xx.aa.bb.cc/chain.pem
</VirtualHost>
```

Restart Apache Service

```
systemctl restart apache2
```

6. SSL



resolves to



Server Type: Apache



The certificate should be trusted by all major web browsers (all the correct intermediate certificates are installed).



The certificate will expire in 89 days.



The hostname

is correctly listed in the certificate.



Common name:
SANs:
Valid from June 7, 2024 to September 5, 2024
Serial Number:
Signature Algorithm:
Issuer: E6



Common name: E6
Organization: Let's Encrypt
Location: US
Valid from March 12, 2024 to March 12, 2027
Serial Number: b0573e9173972770dbb487cb3a452b38
Signature Algorithm: sha256WithRSAEncryption
Issuer: ISRG Root X1

7. `certbot.timer` Certificates renew

```
systemctl status certbot.timer
```

* certbot.timer - Run certbot twice daily

Loaded: loaded (/lib/systemd/system/certbot.timer; **enabled**; preset: **enabled**)

Active: **active** (waiting) since Fri 2024-06-07 17:37:05 CST; 6h ago

Trigger: Sat 2024-06-08 08:04:10 CST; 8h left

Triggers: * certbot.service

Jun 07 17:37:05 systemd[1]: Started certbot.timer - Run certbot twice daily.

```
certbot renew --dry-run
```

Saving debug log to /var/log/letsencrypt/letsencrypt.log

Processing /etc/letsencrypt/renewal/xx.aa.bb.cc.conf

Simulating renewal of an existing certificate for xx.aa.bb.cc

Congratulations, all simulated renewals succeeded:

/etc/letsencrypt/live/mdfk.goddamn.idv.tw/fullchain.pem (**success**)