Free SSL Certificate powered by Let's Encrypt on your CentOS server

Let's Encrypt is a non-profit certificate authority run by Internet Security Research Group that provides X.509 certificates for Transport Layer Security encryption at no charge.

Install required compontents for Let's Encrypt

```
# Step 1: Installing dependent modules
sudo yum install -y epel-release mod_ssl


# Step 2: Downloading the Let’s Encrypt client
sudo yum install -y python-certbot-apache
```

Create SSL certificate

```
sudo certbot --apache -d kurapa.com
```

If everything goes fine, you will see the message like below:

```
$ sudo certbot --apache -d kurapa.com
Saving debug log to /var/log/letsencrypt/letsencrypt.log
Plugins selected: Authenticator apache, Installer apache
Starting new HTTPS connection (1): acme-v02.api.letsencrypt.org
Requesting a certificate for kurapa.com
Performing the following challenges:
http-01 challenge for kurapa.com
Waiting for verification...
Cleaning up challenges
Deploying Certificate to VirtualHost /etc/httpd/conf.d/vhosts.conf
Redirecting vhost in /etc/httpd/conf.d/vhosts.conf to ssl vhost in /etc/httpd/conf.d/vhosts.conf

- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
Congratulations! You have successfully enabled https://kurapa.com
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -

IMPORTANT NOTES:
 - Congratulations! Your certificate and chain have been saved at:
   /etc/letsencrypt/live/kurapa.com/fullchain.pem
   Your key file has been saved at:
   /etc/letsencrypt/live/kurapa.com/privkey.pem
   Your certificate will expire on 2022-01-19. To obtain a new or
   tweaked version of this certificate in the future, simply run
   certbot again with the "certonly" option. To non-interactively
   renew *all* of your certificates, run "certbot renew"
 - 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

$
```

Wild Card SSL?

Following shell script (wild_certbot.sh) will enable you to create wild card domain

wild_certbot.sh

```
#!/bin/bash
certbot certonly --manual \
  --preferred-challenges=dns \
  --email $1 \
  --server https://acme-v02.api.letsencrypt.org/directory \
  --agree-tos \
  --manual-public-ip-logging-ok \
  -d "$2,*.$2"
```

You can do it as following:

```
$ wild_certbot.sh kurapa@kurapa.com kurapa.com
```

Then you will see like below:

```
Use of --manual-public-ip-logging-ok is deprecated.
Saving debug log to /var/log/letsencrypt/letsencrypt.log
Plugins selected: Authenticator manual, Installer None
Starting new HTTPS connection (1): acme-v02.api.letsencrypt.org
Requesting a certificate for *.kurapa.com
Performing the following challenges:
dns-01 challenge for kurapa.com

- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
Please deploy a DNS TXT record under the name
_acme-challenge.kurapa.com with the following value:

W8GGMfEG4ck-dOF9dyHG8gNCc1uR_Ql_KjEi1jltuLQ

Before continuing, verify the record is deployed.
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
Press Enter to Continue
Waiting for verification...
Resetting dropped connection: acme-v02.api.letsencrypt.org
Cleaning up challenges
Use of --manual-public-ip-logging-ok is deprecated.

IMPORTANT NOTES:
 - Congratulations! Your certificate and chain have been saved at:
   /etc/letsencrypt/live/kurapa.com-0001/fullchain.pem
   Your key file has been saved at:
   /etc/letsencrypt/live/kurapa.com-0001/privkey.pem
   Your certificate will expire on 2022-01-20. To obtain a new or
   tweaked version of this certificate in the future, simply run
   certbot again. To non-interactively renew *all* of your
   certificates, run "certbot renew"
 - 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
```

Note that you should update a DNS TXT record based on the guide above, as a step, before verfication.

How to update SSL?

As long as you have certificates based on Let's Encrypt, you can simply update it as:

```
sudo certbot renew
```

If it doesn't require updating the SSL, it will show like:

```
Saving debug log to /var/log/letsencrypt/letsencrypt.log
Plugins selected: Authenticator apache, Installer apache
Starting new HTTPS connection (1): acme-v02.api.letsencrypt.org
Cert not yet due for renewal
Keeping the existing certificate
```