

# zeroSSL로 https적용하기

태그

## 공식 안내 사이트

### Install SSL Certificate on NGINX - ZeroSSL Help Center

This tutorial explains the steps required to install a new SSL certificate on an NGINX web server as well as an HTTPS redirect to enable secure website access.

<https://zerossl.com/help/installation/nginx/>

1. ZeroSSL 사이트 회원가입
2. 도메인 입력

## New Certificate

Cancel

### SSL Certificate Setup

You're on your way to issuing a brand-new SSL certificate for one or multiple domains. Before you can install your new certificate, please complete the steps below.

Domains

☐ I need a wildcard certificate PRO

Please enter at least one domain to secure. For single-domain certificates the WWW-version of your domain will always be included at no extra charge.

Enter Domains

p.ssafy.io

✓ .p.ssafy.io

+ Add Domain PRO

Next Step →

3. 90일 선택

Validity

You can now choose between generating 90-day or one-year certificate validity. To keep manual work at a minimum, we recommend 1-year certificates.

☒ 90-Day Certificate

☐ 1-Year Certificate PRO

Next Step →

#### 4. next step

▼ CSR & Contact

Before validation, we will auto-generate contact information and a CSR for your certificate.  
To enter your information manually or paste an existing CSR, please uncheck the box below.

☒ Auto-Generate CSR ?

Next Step →

#### 5. free 요금제 선택

▼ Finalize Your Order

Based on your selection of a 90-Day SSL Certificate you are fine staying on the Free Plan.  
To create and validate your SSL Certificate, please click "Next Step" below.

✓

Free

\$0 / month

Selected

3 90-Day Certificates

✕ 1-Year Certificates

✕ Multi-Domain Certs

✕ 90-Day Wildcards

✕ 1-Year Wildcards

✕ REST API Access

✕ Technical Support

🏠

Basic

\$10 / month  
or \$8 if billed yearly

Select

∞ 90-Day Certificates

3 1-Year Certificates

✓ Multi-Domain Certs

✕ 90-Day Wildcards

✕ 1-Year Wildcards

✓ REST API Access

✓ Technical Support

★

Premium

\$50 / month  
or \$40 if billed yearly

Select

∞ 90-Day Certificates

10 1-Year Certificates

✓ Multi-Domain Certs

∞ 90-Day Wildcards

1 1-Year Wildcards

✓ REST API Access

✓ Technical Support

⚡

Business

\$100 / month  
or \$80 if billed yearly

Select

∞ 90-Day Certificates

25 1-Year Certificates

✓ Multi-Domain Certs

∞ 90-Day Wildcards

3 1-Year Wildcards

✓ REST API Access

✓ Technical Support

←

→

Next Step →

#### 6. http file upload 선택

zeroSSL로 https적용하기

2

**HTTP File Upload**

✔ Follow the steps below

To verify your domain using **HTTP File Upload**, please follow the steps below:

- 1 Download your Auth File using the following link: [Download Auth File](#)
- 2 Upload the Auth File to your HTTP server under: `/.well-known/pki-validation/`
- 3 Make sure your file is available under the following link: <http://.p.ssafy.io/.well-known/pki-validation/4D4AC643F710E470365BB9C05282A69E.txt>
- 4 Click "Next Step" to continue.

Next Step →

## 7. Download auth File

## 8. ec2 nginx 기본 default 설정 파일로 인증



설정 파일에서 root를 바꿔서 진행하면, Auth File을 인식하지 못하는 에러가 남.

## 9. root 폴더로 이동

```
cd /var/www/html
```

## 10. 폴더 생성

```
mkdir .well-known
cd .well-known
mkdir pki-validation
```

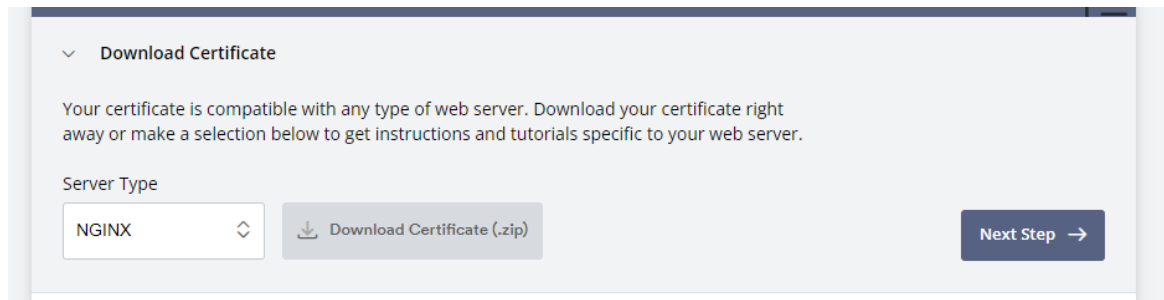
## 11. txt 파일 생성 후 내용 입력

```
vi [파일명].txt

# 파일 내용 입력
# 파일 내용 저장
# ESC -> :wq
```

## 12. next step

## 13. 인증서 파일 다운로드



#### 14. 인증서 파일 ec2 업로드

```
cd /etc/[인증서 넣을 폴더]

# 방법 1. 메모장 & vi 활용해서 복사/붙여넣기
# 방법 2. mobaXterm 을 활용한 복사/붙여넣기
```

#### 15. nginx default conf 수정

```
# 주석 부분 내용 추가
server {

    listen    443;

<--- 내용 추가할 부분 시작--->
    ssl      on;
    ssl_certificate    /etc/ssl/certificate.crt;
    ssl_certificate_key    /etc/ssl/private.key;
<--- 내용 추가할 부분 끝--->

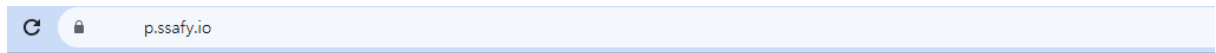
    server_name your.domain.com;
    access_log /var/log/nginx/nginx.vhost.access.log;
    error_log /var/log/nginx/nginx.vhost.error.log;
    location / {
        root    /home/www/public_html/your.domain.com/public/;
        index  index.html;
    }
}
```

#### 16. nginx 재시작

```
sudo systemctl restart nginx
```

17. zerossI 사이트에서 **Check Installation** 클릭

18. 자물쇠 표시가 나온다면 끝!



## Welcome to nginx!

If you see this page, the nginx web server is successfully working. Further configuration is required.