

# Windows Nginx (Single) SSL 인증서 신규 설치 가이드

본 문서는 주식회사 한국기업보안에서 SSL보안서버인증서 설치를 위해 작성된 문서로  
주식회사 한국기업보안의 동의 없이 무단으로 사용하실 수 없습니다.

[고객센터]

한국기업보안. 유서트 기술팀

02-3442-7230



**한국기업보안**  
Korea Corporation Security

※ (필독)이 문서는 SSL 인증서 설치를 위한 설정이며 관련없는 설정은 부분적으로 생략하였습니다. 서버마다 설정이 상이할 수 있어 인증서 설치 시 해당 문서 참고 부탁드립니다.

## 작업 전 확인사항

### Nginx 경로 확인 방법

키보드 [윈도우 키] + [R] 를 눌러 실행 창을 연 뒤 cmd 를 입력하여 커맨드 라인에 접근합니다.  
아래 명령어를 실행하여 현재 열려있는 서버의 포트 중 웹 서비스에 해당하는 포트를 확인합니다.

```
netstat -ano | findstr LISTEN
```

※ 일반적으로 웹 서비스는 80 포트를 사용합니다.

확인된 항목 가장 오른쪽에 표기된 숫자가 현재 해당 웹 서비스의 PID 입니다.

키보드 [Ctrl] + [Shift] - [Esc] 입력하여 작업 관리자를 실행합니다.

하단 자세히(D) 를 클릭합니다.

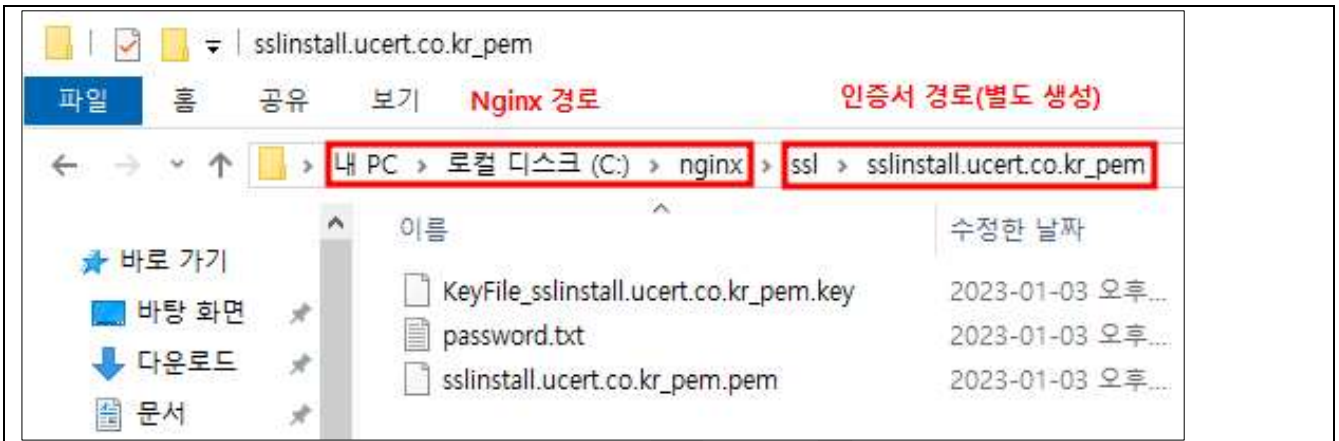
상단의 [세부 정보] 클릭 후 [PID] 항목을 클릭하여 오름차순/내림차순 으로 정렬합니다.

앞서 확인한 웹 서비스 PID 에 해당하는 작업 우클릭 후 [속성]을 클릭합니다.

[일반] - [위치] 항목에 기재된 경로가 해당 서비스의 구동 파일 위치입니다.

1. 발급 받은 인증서를 서버에 업로드 합니다.

※ 어떠한 경로에 인증서를 업로드 하시더라도 동작에는 문제가 없으나,  
관리를 위해 가급적 별도의 폴더를 생성하여, ssl 파일을 업로드 하실 것을 권장 드립니다.  
Nginx 설치 경로에 ssl 폴더를 생성하여 도메인 별로 인증서를 관리하는 것이 일반적입니다.



## 2. Nginx 기본 설정 파일을 수정합니다.(.conf 파일은 메모장으로 열어주시면 됩니다.)

※ 복수의 싱글 인증서 적용 시 포트 및 인증서 경로를 상이하게 적용 합니다.

설정 파일 경로 : <Nginx 경로>/conf/nginx.conf

### 1. Nginx 기본 경로에 페이지가 존재한다면, 아래와 같이 구문 삽입

```
worker_processes 1;

events {
    worker_connections 1024;
}

http {
    include C:/nginx/conf/custom_config/*.conf;
    include mime.types;
    default_type application/octet-stream;

    sendfile on;

    keepalive_timeout 65;

    server {
        listen 80 default;
        server_name localhost;

        location / {
            root html;
            index index.html index.htm;
        }

        error_page 500 502 503 504 /50x.html;
        location = /50x.html {
            root html;
        }
    }

    server {
        listen 443 ssl;
        server_name sslinstall.ucert.co.kr;
        ssl_certificate C:/nginx/ssl/sslinstall.ucert.co.kr_pem/sslinstall.ucert.co.kr_pem.pem;
        ssl_certificate_key C:/nginx/ssl/sslinstall.ucert.co.kr_pem/KeyFile_sslinstall.ucert.co.kr_pem.key;
    }
}
```

도메인의 https 접속이 Nginx 기본 경로가 아닌 별도의 경로에 연결되어야 한다면,  
listen 및 server\_name 구문 하단에 root 및 location 구문으로 설정 진행합니다.

```
server {
    listen 443 ssl;
    server_name sslinstall.ucert.co.kr;
    root "ucert";
    location / {
        index index.html;
    }
    ssl_certificate C:/nginx/ssl/sslinstall.ucert.co.kr_pem/sslinstall.ucert.co.kr_pem.pem;
    ssl_certificate_key C:/nginx/ssl/sslinstall.ucert.co.kr_pem/KeyFile_sslinstall.ucert.co.kr_pem.key;
}
```

root 구문이 지시하는 경로는, 기본적으로 Nginx 경로 하단의 폴더명입니다.

### 3. Nginx 서비스를 재기동합니다.

실행 파일 경로 : <Nginx 경로>/bin/nginx.exe

nginx.exe -t -> 설정파일 구문 검사

nginx.exe -s stop -> Nginx 중지

start nginx.exe -> Nginx 시작

또는

nginx.exe -s reload -> Nginx 재기동

3-1. 설정파일 구문 검사(설정파일 내 문법 오류가 없다면 syntax is ok, test is successful 문구가 출력됩니다.)

```
Administrator: C:\Windows\system32\cmd.exe

C:\nginx>nginx.exe -t
nginx: the configuration file C:\nginx\conf\nginx.conf syntax is ok
nginx: configuration file C:\nginx\conf\nginx.conf test is successful
C:\nginx>_
```

#### 3-2. Nginx 재기동

방법 1 - Nginx 중지 후 시작

```
Administrator: C:\Windows\system32\cmd.exe

C:\nginx>nginx.exe -s stop
C:\nginx>start nginx.exe
C:\nginx>_
```

방법 2 - Nginx 재기동

```
Administrator: C:\Windows\system32\cmd.exe

C:\nginx>nginx.exe -s reload
C:\nginx>_
```

#### 4. Nginx 기동 여부 및 인증서 설치 상태를 확인 합니다.

##### Nginx 기동 여부 확인

명령어 : netstat -ano | findstr LISTEN

```
Administrator: C:\Windows\system32\cmd.exe

C:\Users\Administrator>netstat -ano | findstr LISTEN
TCP 0.0.0.0:80 0.0.0.0:0 LISTENING 6108
TCP 0.0.0.0:135 0.0.0.0:0 LISTENING 896
TCP 0.0.0.0:443 0.0.0.0:0 LISTENING 6108
TCP 0.0.0.0:445 0.0.0.0:0 LISTENING 4
TCP 0.0.0.0:3389 0.0.0.0:0 LISTENING 480
```

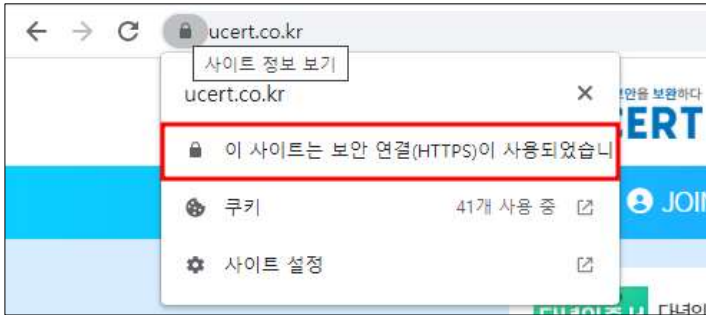
Nginx와 같은 웹 서버가 HTTP(80/TCP), HTTPS(443/TCP) 포트를 열어두고 통신을 기다리는 상태입니다. 별도의 포트를 설정한 경우, 해당 포트가 LISTENING 상태인 지 여부를 확인해 주시면 됩니다.

## 5. 웹페이지에서 인증서를 확인 합니다.

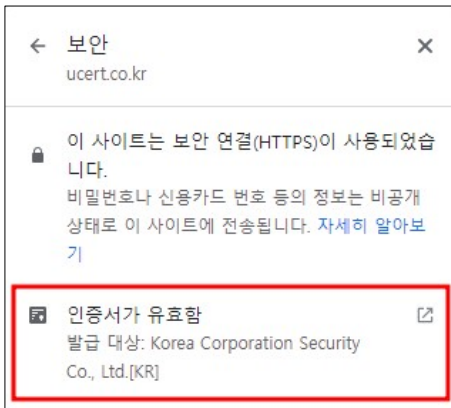
Chrome 확인 방법 <https://www.ucert.co.kr> 접속 예

5-1. https 주소로 접속된 사이트 브라우저 상단 URL 좌측 자물쇠

5-2. 이 사이트는 보안 연결(HTTPS)이 사용되었습니다. 클릭



5-3. 인증서가 유효함 클릭



5-4. 인증서 뷰어 페이지에서 인증서 확인

