

Windows Lighttpd (Single & Multi) 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.

인증기관 Root & Chain 인증서 구분

※ 발급 받은 인증서를 아래표를 참고하여 해당 되는 인증서에 대하여 Root 및 Chain 인증서를 구분.

[GlobalSign] 인증기관

설정구분	인증서 형식
SSLCertificateChainFile	GLOBALSIGN_RSA_DV_SSL_CA_2023.crt [DV] GLOBALSIGN_RSA_OV_SSL_CA_2023.crt [OV] GLOBALSIGN_EXTENDED_VALIDATION_CA_SHA256_G3.crt [EV] ALPHASSL_CA_SHA256_G2.crt (Domain)_ChainBundle.crt
SSLCACertificateFile	GLOBALSIGN_ROOT_CA.crt

[Comodo] - 인증기관

설정구분	인증서 형식
SSLCertificateChainFile	(Domain)_ChainBundle.crt
SSLCACertificateFile	AAA_CERTIFICATE_SERVICES.crt

[Digicert] - 인증기관

설정구분	인증서 형식
SSLCertificateChainFile	THAWTE_RSA_CA_2018.crt
SSLCACertificateFile	DIGICERT_GLOBAL_ROOT_CA.crt



작업 전 확인사항

Lighttpd 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. 발급받은 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.
- 아파치 설치 경로에 ssl 폴더를 생성하여 도메인 별로 인증서를 관리하는 것이 일반적입니다.



2. 인증서 파일을 하나의 pem 파일로 통합합니다.

- ※ Apache(cert) 인증서는 key, cert, chain, root 의 순서로 하나의 pem 파일로 통합합니다.
- ※ Nginx(pem) 인증서는 key, cert 의 순서로 하나의 pem 파일로 통합합니다.
- ※ 인증서 통합은, 빈 파일 생성 후 인증서 파일을 메모장으로 열어, 연이어 복사/붙여넣기 하시면 됩니다.

최종적으로 통합된 인증서 파일의 내용 예시는 아래와 같습니다.

- ※ 인증서 HASH 값은 내용이 길어 생략하였습니다.
- ※ BEGIN CERTIFICATE 와 END CERTIFICATE 는 반드시 쌍으로 이루어져야 합니다.
- ※ CERTIFICATE 구문의 총 갯수는 인증서 종류에 따라 예시와는 차이가 있을 수 있습니다.



3. Lighttpd 설정 파일을 수정합니다.(.conf 파일은 메모장으로 열어 주시면 됩니다.)

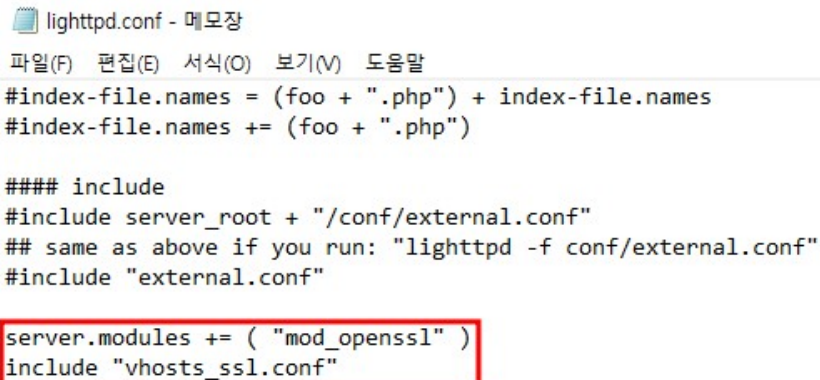
※ 복수의 싱글 인증서 적용 시 포트 및 인증서 경로를 상이하게 적용합니다.

설정 파일 경로 : <Lighttpd 경로>/conf/lighttpd.conf

1. 파일 최하단에 SSL 모듈 활성화 및 설정파일 분리 구문 추가

server.modules += ("mod_openssl")

include "vhosts_ssl.conf"



```
lighttpd.conf - 메모장
파일(F) 편집(E) 서식(O) 보기(V) 도움말
#index-file.names = (foo + ".php") + index-file.names
#index-file.names += (foo + ".php")

#### include
#include server_root + "/conf/external.conf"
## same as above if you run: "lighttpd -f conf/external.conf"
#include "external.conf"

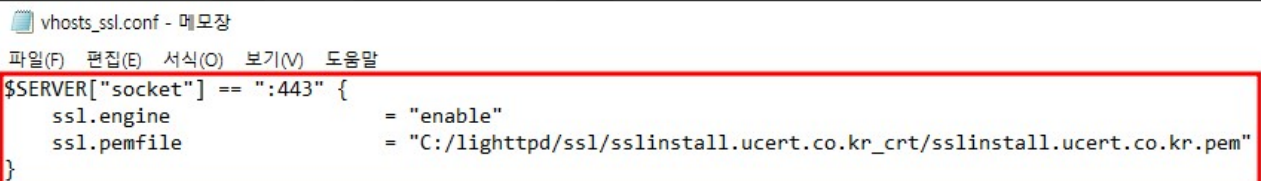
server.modules += ( "mod_openssl" )
include "vhosts_ssl.conf"
```

※ include "vhosts_ssl.conf"

위 구문은 선택사항입니다. 기본 설정파일에 직접 인증서를 선언해도 동작에 지장이 없으나, 이후 관리 상의 편의를 위해 SSL 인증서 설정파일을 따로 분리하는 구문입니다.

2. 경로 상에 vhosts_ssl.conf 파일 생성 후 SSL 구문 추가

```
$SERVER["socket"] == ":443" {
    ssl.engine          = "enable"
    ssl.pemfile         = "인증서파일"
}
```



```
vhosts_ssl.conf - 메모장
파일(F) 편집(E) 서식(O) 보기(V) 도움말
$SERVER["socket"] == ":443" {
    ssl.engine          = "enable"
    ssl.pemfile         = "C:/lighttpd/ssl/sslinstall.ucert.co.kr_crt/sslinstall.ucert.co.kr.pem"
}
```

4. Lighttpd 서비스를 재기동합니다.

실행 파일 경로 : <Lighttpd 경로>/lighttpd.exe

lighttpd.exe -tt -f conf/lighttpd.conf -> 설정파일 구문 검사

4-1. 설정파일 구문 검사(설정파일 내 문법 오류가 없다면 아무것도 출력되지 않습니다.)

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

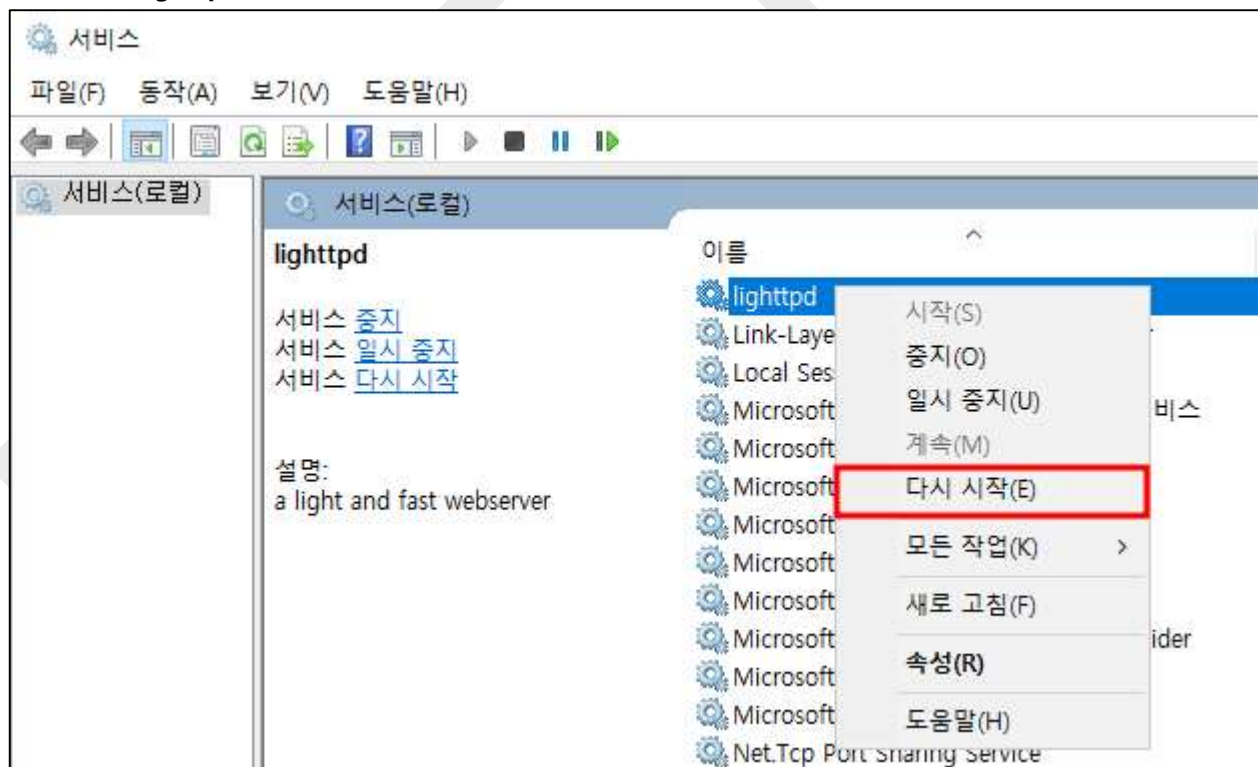
C:\Users\Administrator>cd C:/Lighttpd

C:\lighttpd>lighttpd.exe -tt -f conf/lighttpd.conf

C:\lighttpd>_
```

4-2. Lighttpd 재기동

키보드 윈도우 키 + [R] 을 눌러 실행 창을 연 뒤 services.msc 를 입력하여 서비스 창에 접근합니다.
실행 중인 lighttpd 를 찾은 후 우클릭하여 [다시 시작]을 진행합니다.



5. Lighttpd 기동 여부를 확인합니다.

5-1. Lighttpd 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
```

웹 서버가 HTTP(80/TCP), HTTPS(443/TCP) 포트를 열어두고 통신을 기다리는 상태입니다.

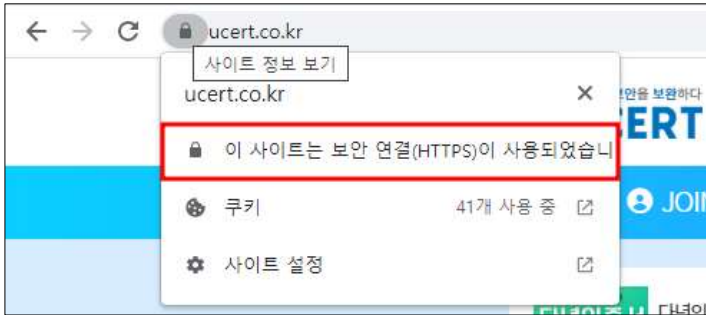
별도의 포트를 설정한 경우, 해당 포트가 LISTENING 상태인 지 여부를 확인해 주시면 됩니다.

6. 웹페이지에서 인증서를 확인합니다.

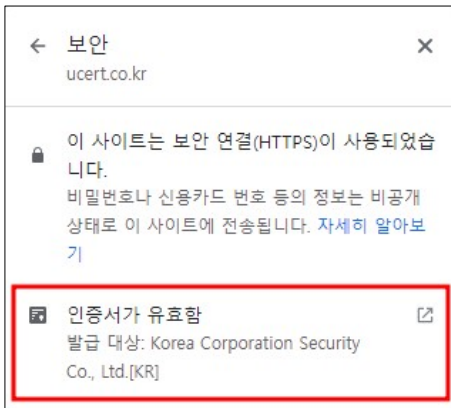
Chrome 확인 방법 <https://www.ucert.co.kr> 접속 예

6-1. [https](https://www.ucert.co.kr) 주소로 접속된 사이트 브라우저 상단 URL 좌측 자물쇠

6-2. 이 사이트는 보안 연결(HTTPS)이 사용되었습니다. 클릭



6-3. 인증서가 유효함 클릭



6-4. 인증서 뷰어 페이지에서 인증서 확인

