

Windows Apache (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.

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

1. 아파치 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.

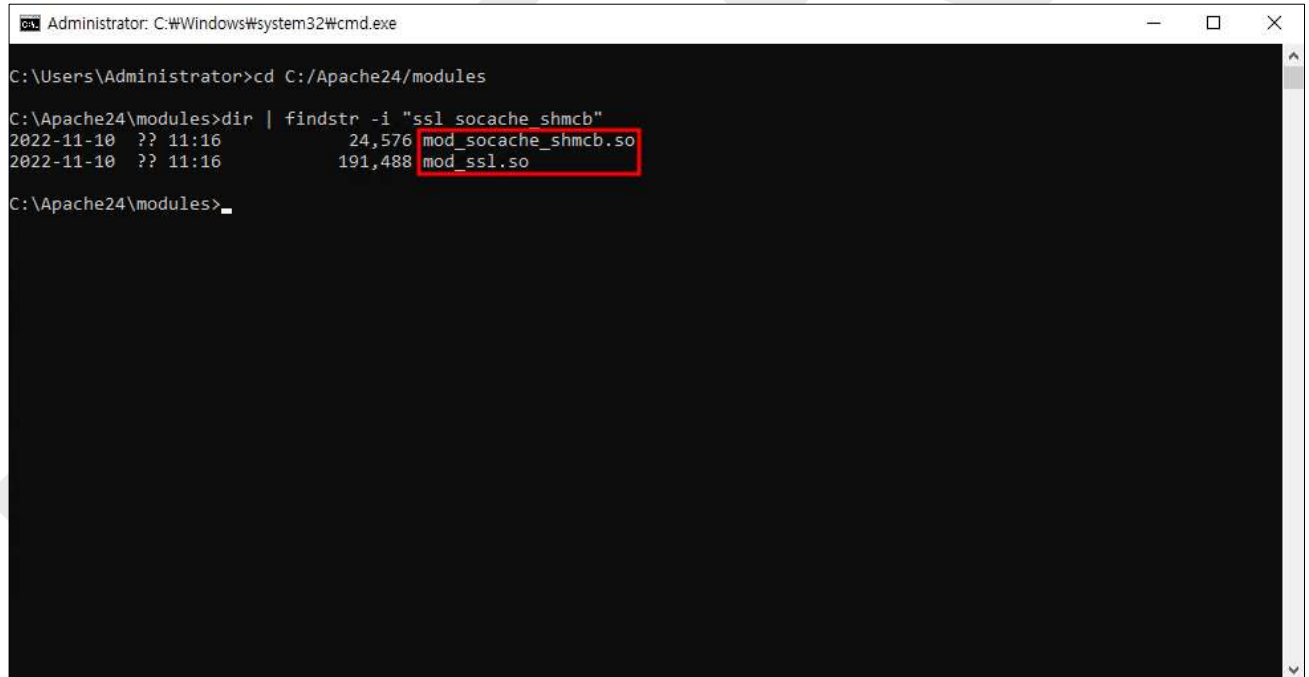
앞서 확인한 웹 서비스 PID 에 해당하는 작업 우클릭 후 [속성]을 클릭합니다.

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

2. SSL 관련 기본 모듈 설치 여부 확인 방법

명령어 : cd <아파치 경로>/modules

명령어 : dir | findstr -i "ssl socache_shmcb"

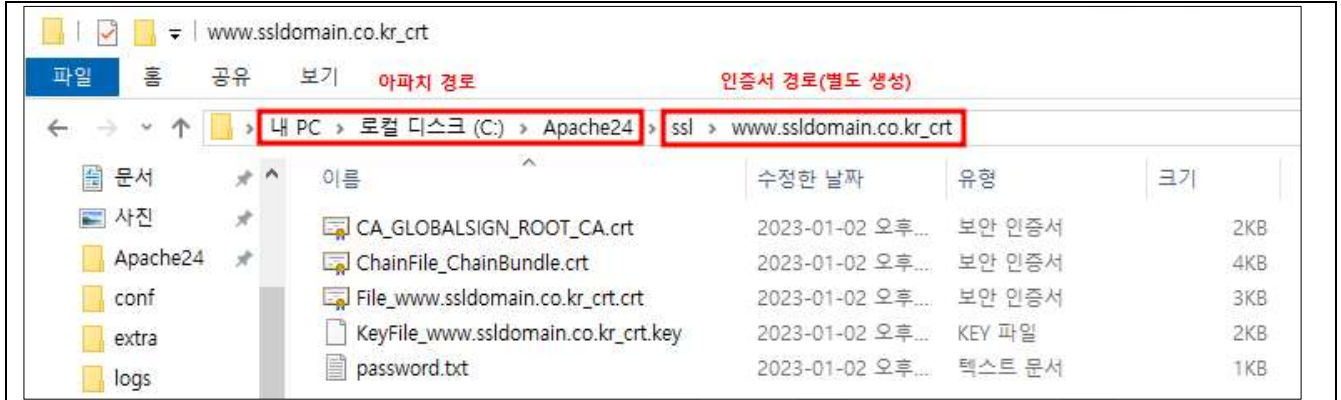


```
Administrator: C:\Windows\system32\cmd.exe
C:\Users\Administrator>cd C:/Apache24/modules
C:\Apache24\modules>dir | findstr -i "ssl socache shmcb"
2022-11-10 ?? 11:16          24,576 mod_socache_shmcb.so
2022-11-10 ?? 11:16       191,488 mod_ssl.so
C:\Apache24\modules>
```

위처럼 ssl, socache_shmcb 모듈이 조회된다면, ssl 사용을 위한 모듈은 설치가 되어있는 상태입니다.

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

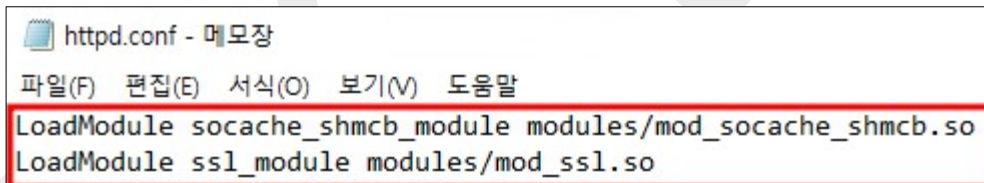


2. 아파치 기본 설정 파일을 수정합니다.(.conf 파일은 메모장으로 열어주시면 됩니다.)

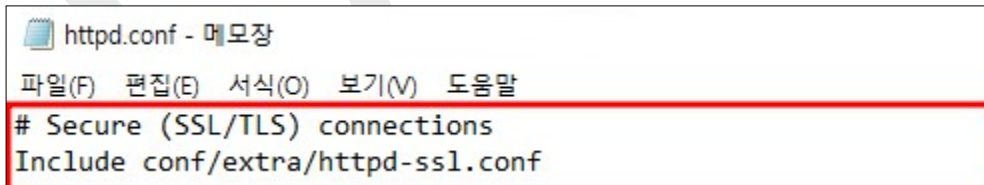
※ 복수의 싱글 인증서 적용 시 포트 및 인증서 경로를 상이하게 적용 합니다.

설정 파일 경로 : <아파치 경로>/conf/httpd.conf

1. ssl, socache_shmcb 모듈 활성화 구문 주석(#) 해제



2. SSL VirtualHost 설정파일 인식 구문 주석(#) 해제



3. 아파치 기본 https 설정 파일을 수정합니다.

설정 파일 경로 : <아파치 경로>/conf/extra/httpd-ssl.conf

<VirtualHost _default_:443> 구문 하단 내용을 수정하며, 수정할 구문은 아래와 같습니다.

DocumentRoot -> ServerName 에 명시한 도메인으로 접속 시 연결될 서버의 폴더를 지정

ServerName -> DocumentRoot 로 연결될 도메인 주소 1개를 지정

ServerAlias -> ServerName 외 DocumentRoot 로 연결될 도메인 주소를 추가 지정

ServerAdmin -> 에러 발생 시 사이트에 명시할 관리자 메일 주소 지정(선택사항)

SSLCertificateFile -> HTTPS 접속에 사용될 SSL 인증서 파일 지정

SSLCertificateKeyFile -> HTTPS 접속에 사용될 개인 키 파일 지정

SSLCertificateChainFile -> HTTPS 접속에 사용될 SSL 인증서 체인 파일 지정

SSLCACertificateFile -> HTTPS 접속에 사용될 ROOT 인증서 파일 지정

3-1. DocumentRoot, ServerName, ServerAlias, ServerAdmin 예시

```
DocumentRoot "${SRVROOT}/htdocs"
```

```
ServerName ssldomain.co.kr
```

```
ServerAlias www.ssldomain.co.kr
```

```
ServerAdmin admin@example.com
```

3-2. SSLCertificateFile 예시

```
SSLCertificateFile "ssl/www.ssldomain.co.kr_crt/File_www.ssldomain.co.kr_crt.crt"
```

3-3 SSLCertificateKeyFile 예시

```
SSLCertificateKeyFile "ssl/www.ssldomain.co.kr_crt/KeyFile_www.ssldomain.co.kr_crt.key"
```

3-4 SSLCertificateChainFile 예시

```
SSLCertificateChainFile "ssl/www.ssldomain.co.kr_crt/ChainFile_ChainBundle.crt"
```

3-5 SSLCACertificateFile 예시

```
SSLCACertificateFile "ssl/www.ssldomain.co.kr_crt/CA_GLOBALSIGN_ROOT_CA.crt"
```

4. 아파치 서비스를 재기동합니다.

실행 파일 경로 : <아파치 경로>/bin/httpd.exe

httpd.exe -t -> 설정파일 구문 검사

httpd.exe -k stop -> 아파치 중지

httpd.exe -k start -> 아파치 시작

또는

httpd.exe -k restart -> 아파치 재기동

4-1. 설정파일 구문 검사(설정파일 내 문법 오류가 없다면 Syntax OK 가 출력됩니다.)

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

C:\Users\Administrator>cd C:/Apache24/bin

C:\Apache24\bin>httpd.exe -t
Syntax OK

C:\Apache24\bin>_
```

4-2. 아파치 재기동

Key 파일에 패스워드가 설정되어 있다면, 아파치 시작 과정 중 패스워드가 요구되며, 재기동의 경우 패스워드 요구 절차가 생략되며 아파치가 중지되므로, 가급적 중지 후 시작을 권장 드립니다.

방법 1 - 아파치 중지 후 시작

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

C:\Apache24\bin>httpd.exe -k stop
The 'Apache2.4' service is stopping.
The 'Apache2.4' service has stopped.

C:\Apache24\bin>_

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

C:\Apache24\bin>httpd.exe -k start

C:\Apache24\bin>_
```

방법 2 - 아파치 재기동

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

C:\Apache24\bin>httpd.exe -k restart

C:\Apache24\bin>_
```


5. 아파치 기동 여부 및 인증서 설치 상태를 확인 합니다.

5-1. 아파치 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
```

아파치와 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.

5-2. 인증서 설치 상태 확인

실행 파일 경로 : <아파치 경로>/bin/openssl.exe

명령어 : `echo "" | openssl.exe s_client -connect localhost:443 | openssl.exe x509 -dates | findstr not`

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

C:\Users\Administrator>cd C:/Apache24/bin

C:\Apache24\bin>echo "" | openssl.exe s_client -connect localhost:443 | openssl.exe x509 -dates | findstr not
Can't use SSL_get_servername
depth=2 OU = GlobalSign Root CA - R3, O = GlobalSign, CN = GlobalSign
verify error:num=20:unable to get local issuer certificate
verify return:1
depth=1 C = BE, O = GlobalSign nv-sa, CN = GlobalSign Extended Validation CA - SHA256 - G3
verify return:1
depth=0 businessCategory = Private Organization, serialNumber = 110111-3999666, jurisdictionC = KR, C = KR, ST
L = Seocho-gu, street = "53, Gangnam-daero 99-gil", O = "Korea Corporation Security Co., Ltd.", CN =
.kr
verify return:1
notBefore=Aug 9 07:46:02 2022 GMT 인증서 시작일
notAfter=Sep 10 07:46:01 2023 GMT 인증서 만료일

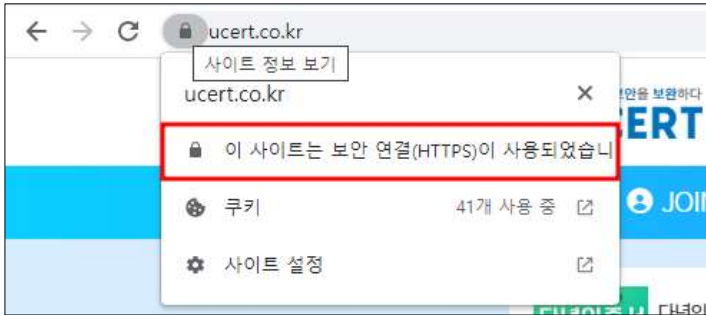
C:\Apache24\bin>
```

6. 웹페이지에서 인증서를 확인 합니다.

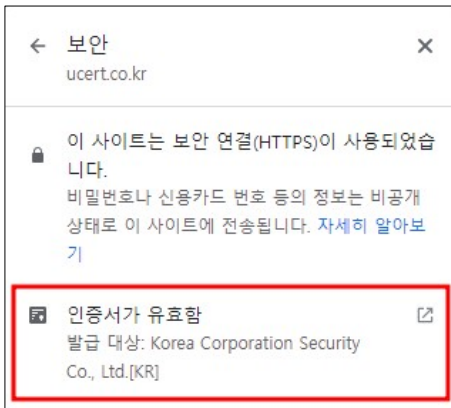
Chrome 확인 방법 <https://www.ucert.co.kr> 접속 예

6-1. https 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

