

# Apache Source (Single) SSL 인증서 갱신 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



www.ucs-cert.kr  
**한국기업보안**  
Korea Corporation Security

※ 이 문서는 SSL 인증서 설치를 위한 설정이며 생략된 설정이 존재합니다. 서버마다 설정이 상이할 수 있어 인증서 설치 시 해당 문서 참고 부탁드립니다.

- 작업 전 참고사항.

#### 1. Apache package 및 source 구분

> 아파치 경로확인 명령어: `ps -ef | grep httpd`

-package: `/usr/sbin/httpd` [apache이름은 상이할 수 있음] -> `/etc/httpd` 경로에 설정 존재

-source: `/usr/local/apache` [경로 및 apache이름은 상이할 수 있음]-> 확인 경로에 설정 존재

#### 2. 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_2018.crt [DV]
	GLOBALSIGN_RSA_OV_SSL_CA_2018.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

www.ucert.co.kr



본 문서는 주식회사 한국기업보안에서 SSL보안서버인증서 설치를 위해 작성된 문서로

주식회사 한국기업보안의 동의 없이 무단으로 사용하실 수 없습니다

Copyright 2018-2023. Korea Corporation Security Co., Ltd All pictures cannot be copied without permission.

1. 발급 받으신 인증서를 해당 서버 폴더에 업로드합니다.

2. 기존 인증서의 시작일과 만료일을 확인토록 합니다.

```
[root@localhost Apache]# netstat -nlp | grep httpd
```

```
tcp        0      0 :::80          :::*           LISTEN      118721/httpd
```

```
tcp        0      0 :::443         :::*           LISTEN      118721/httpd
```

\* 설명 : 기존 SSL 사용중인 포트 확인.(포트번호는 443이 아닐 수도 있음)

```
[root@localhost Apache]# echo "" | openssl s_client -connect localhost:443 | openssl x509 -noout -dates
```

\* 설명 : 기존 인증서 시작일 및 만료일 확인.

```
notBefore=Jan 30 11:16:09 2017 GMT  인증서 시작일
```

```
notAfter=Jan 31 10:58:54 2018 GMT  인증서 만료일
```

\* 명령어 : echo "" | openssl s\_client -connect [도메인 or IP]:[포트번호] | openssl x509 -noout -dates

3. httpd.conf 파일을 열어 ssl 설정을 확인합니다.(필요한 문구만을 출력하여 나타내었습니다. 기존 설정 내용과 상이할 수 있는 점 유의 바랍니다.)

```
[root@localhost Apache]# vi conf/httpd.conf
```

```
-----중략-----
```

```
Include conf/extra/httpd-ssl.conf
```

\* 설명 : SSL 설정 파일 위치 확인.

```
-----중략-----
```



본 문서는 주식회사 한국기업보안에서 SSL보안서버인증서 설치를 위해 작성된 문서로

주식회사 한국기업보안의 동의 없이 무단으로 사용하실 수 없습니다

Copyright 2018-2023. Korea Corporation Security Co., Ltd All pictures cannot be copied without permission.

#### 4. 해당 위치에서 SSL 설정 파일 확인합니다.

```
[root@localhost Apache]# vi conf/extra/httpd-ssl.conf
```

##### **Listen 443**

\* 설명 : 사용할 SSL 포트번호를 적용 합니다.

-----중략-----

##### **<VirtualHost \*:443>**

**DocumentRoot "/usr/local/Apache/www"**

\* 설명 :도메인 홈 디렉토리를 설정 합니다.

**ServerName www.ucert.co.kr:443**

\* 설명 : 설치가 필요한 도메인 이름과 포트를 기재 합니다.

**ServerAdmin you@example.com**

**ErrorLog "/usr/local/Apache/logs/error\_log"**

**TransferLog "/usr/local/Apache/logs/access\_log"**

##### **SSLEngine on**

\* 설명 : SSL 엔진 사용을 활성화 합니다.

**SSLCertificateFile "/usr/local/Apache/conf/ssl/File\_www.ucert.co.kr.crt"**

\* 설명 : 인증서 경로 설정 및 파일 명을 설정 합니다.

**SSLCertificateKeyFile "/usr/local/Apache/conf/ssl/KeyFile\_www.ucert.co.kr.key"**

\* 설명 : 개인키 경로 설정 및 파일 명을 설정 합니다.

**SSLCertificateChainFile "/usr/local/Apache/conf/ssl/ChainFile\_ChainBundle.crt"**

\* 설명 : Chain 인증서 경로 설정 및 파일 명을 설정 합니다.

**SSLCACertificateFile "/usr/local/Apache/conf/ssl/CA\_GLOBALSIGN\_ROOT\_CA.crt"**

\* 설명 : Root 인증서 경로 설정 및 파일 명을 설정 합니다.

-----중략-----

**</VirtualHost>**



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

Copyright 2018-2023. Korea Corporation Security Co., Ltd All pictures cannot be copied without permission.

5. 설정되어 있는 기존 인증서 경로에 신규 인증서 업로드합니다.

```
[root@localhost Apache]# ls -al /usr/local/Apache/conf/ssl/
-rw-r--r--. 1 root root 1931 Feb 22 00:00 ChainFile_ChainBundle.crt
-rw-r--r--. 1 root root 1744 Feb 22 00:00 File_www.ucert.co.kr.crt
-rw-r--r--. 1 root root 1931 Feb 22 00:00 KeyFile_www.ucert.co.kr.key
-rw-r--r--. 1 root root 1931 Feb 22 00:00 CA_GLOBALSIGN_ROOT_CA.crt
-rw-r--r--. 1 root root 1744 Feb 22 00:00 password.txt
```

\* 설명 : 해당 위치에 인증서가 있는 지 확인합니다.

```
[root@localhost Apache]# mkdir /usr/local/Apache/conf/ssl/20180223
```

```
[root@localhost Apache]# cp /conf/ssl/* /conf/ssl/20180223
```

```
[root@localhost Apache]# ls -al /usr/local/Apache/conf/20180223
```

```
-rw-r--r--. 1 root root 1931 Feb 22 00:00 ChainFile_ChainBundle.crt
-rw-r--r--. 1 root root 1744 Feb 22 00:00 File_www.ucert.co.kr.crt
-rw-r--r--. 1 root root 1931 Feb 22 00:00 KeyFile_www.ucert.co.kr.key
-rw-r--r--. 1 root root 1931 Feb 22 00:00 CA_GLOBALSIGN_ROOT_CA.crt
```

\* 설명 : ssl 디렉토리의 인증서를 20180223 디렉토리에 백업을 진행하고 백업을 확인합니다.

```
[root@localhost Apache]# cp /conf/ssl_new/* /usr/local/Apache/conf/ssl
```

\* 설명 : 신규 업데이트한 인증서 파일을 기존 인증서 폴더에 저장한다.

※ 인증서파일의 파일명은 예시이므로 사용자 설정에 따라 인증서 파일명이 달라질 수 있습니다.

6. 아파치 프로세스 재시작을 진행 합니다.

```
[root@localhost Apache]# /usr/local/Apache/bin/apachectl -t
```

Syntax OK

\* 설명 : 설정 문법에 오류가 없는 지 확인 합니다.

※ 비밀번호가 설정 된 인증서라면 재시작 시 비밀번호 입력을 합니다.

비밀번호가 제거 된 인증서 사용 시 비밀번호 입력이 불필요합니다.

```
[root@localhost Apache]# bin/apachectl stop
```

```
[root@localhost Apache]# bin/apachectl start
```

```
[root@localhost Apache]# bin/apachectl restart
```

\* 설명 : 아파치 재시작을 진행 합니다.

※ 재기동 명령어는 서버마다 상이하여 명령어 확인 후 진행이 필요합니다.



```
[root@localhost Apache]# ps -ef | grep httpd
```

\* 설명 : 아파치 데몬 확인을 진행 합니다.

```
root      4468      1  0  09:14 ?        00:00:00 /usr/local/Apache/bin/httpd -k start
daemon    4469    4468  0  09:14 ?        00:00:00 /usr/local/Apache/bin/httpd -k start
daemon    4470    4468  0  09:14 ?        00:00:00 /usr/local/Apache/bin/httpd -k start
daemon    4471    4468  0  09:14 ?        00:00:00 /usr/local/Apache/bin/httpd -k start
root      4558    4442  0  09:14 pts/3    00:00:00 grep httpd
```

```
[root@localhost Apache]# netstat -nlp | grep httpd
```

```
tcp        0      0 :::80          :::*   LISTEN    4468/httpd
tcp        0      0 :::443         :::*   LISTEN    4468/httpd
```

#### 7. 인증서 설치를 확인하도록 합니다.

```
[root@localhost ~]# echo "" | openssl s_client -connect localhost:443 | openssl x509 -noout -dates
```

\* 설명 : 위의 명령어를 입력하여 인증서 갱신 날짜를 확인하도록 합니다.

```
notBefore=Jan 1 00:24:14 2018 GMT #인증서 시작일
```

```
notAfter=Dec 31 :38:20 2019 GMT #인증서 만료일
```

\* 명령어 형식 : echo "" | openssl s\_client -connect [도메인 or IP]:[포트번호] | openssl x509 -noout -dates

#### ※ 주의사항 ※

서버상에서 인증서 확인 시 교체된 것으로 확인되거나 사이트에서 기존 인증서로 확인될 경우 서버 앞 단의 장비 확인 및 인증서 교체 작업이 필요합니다.



본 문서는 주식회사 한국기업보안에서 SSL보안서버인증서 설치를 위해 작성된 문서로

주식회사 한국기업보안의 동의 없이 무단으로 사용하실 수 없습니다

Copyright 2018-2023. Korea Corporation Security Co., Ltd All pictures cannot be copied without permission.

## 8. 웹페이지에서의 인증서 확인을 하도록 합니다.

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

도메인 접속 후에 Alt 키를 누르고  
파일 → 속성 → 인증서  
클릭 후 인증서 보기를 선택하시면  
인증서정보를 확인 할 수 있습니다.

발급 대상 과 유효 기간이 맞는지  
확인합니다.

인증서 정보

인증서의 용도:

- 원격 컴퓨터의 신분을 확인합니다.

\* 자세한 정보는 인증 기관의 설명을 참조하십시오.

발급 대상: www.ucert.co.kr

발급자: GlobalSign Extended Validation CA - SHA256 - G2

유효 기간: 2015- 11- 09 부터 2016- 08- 12

발급자 설명(S)

인증서에 대해 자세히 알아보십시오.

확인