

Apache Package (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.

- 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



1. 발급 받으신 인증서를 해당 서버에 업로드 합니다.

2. `[$httpd_Home]/modules` 디렉토리를 확인하여 ssl 모듈을 확인 합니다.

```
[root@localhost httpd]# ls modules
```

<code>mod_authn_anon.so</code>	<code>mod_authz_owner.so</code>	<code>mod_deflate.so</code>	<code>mod_session.so</code>
<code>mod_authn_dbd.so</code>	<code>mod_authz_user.so</code>	<code>mod_dir.so</code>	<code>mod_speling.so</code>
<code>mod_authn_dbm.so</code>	<code>mod_autoindex.so</code>	<code>mod_disk_cache.so</code>	<code>mod_ssl.so</code>
<code>mod_authn_default.so</code>	<code>mod_cache.so</code>	<code>mod_dnssd.so</code>	<code>mod_status.so</code>

3. `ssl.conf` 파일 수정 합니다. 모듈 및 설정 파일을 주석 제거하여 활성화 시킵니다.
(필요한 문구만을 출력 하였습니다.)

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

```
LoadModule ssl_module modules/mod_ssl.so
```

* 설명 : ssl 모듈 불러오는 설정입니다.

```
Listen 443
```

* 설명 : 사용할 SSL 포트번호를 적용 합니다. 멀티 인증서의 경우 동일한 포트 사용이 가능하며 싱글 인증서 및 동일한 서버의 다른 프로세스에서 사용중인 포트에 중복 적용은 불가합니다.

-----중략-----

```
SSLHonorCipherOrder on
```

* 설명 : 서버가 호환할 수 있는 가장 높은 보안 연결 설정을 시도하도록 하는 설정
이 옵션을 'on' 으로 할 경우, 네트워크 환경에 따라 SSL속도가 느려질 수 있어 해당 경우, 'off'로 변경하
시기 바랍니다.

```
NameVirtualHost *:443
```

```
<VirtualHost *:443>
```

* 설명 : `www.ucert.co.kr` SSL 설정을 합니다.

```
DocumentRoot "/var/www/html"
```

* 설명 :도메인 홈 디렉토리를 설정 합니다.

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

* 설명 : 설치가 필요한 도메인 이름과 포트를 기재 합니다.

```
ErrorLog logs/ssl_error_log
```

```
TransferLog logs/ssl_access_log
```

```
LogLevel warn
```



SSLEngine on

* 설명 : SSL을 사용합니다.

SSLProtocol all -SSLv2 -SSLv3

* 설명 : SSL 프로토콜 설정을 합니다.

SSLCipherSuite DEFAULT:!EXP:!SSLv2:!DES:!IDEA:!SEED:+3DES

SSLCertificateFile /etc/httpd/conf.d/ssl/File_www.ucert.co.kr.crt

* 설명 : 인증서 경로 설정 및 파일 명

SSLCertificateKeyFile /etc/httpd/conf.d/ssl/KeyFile_www.ucert.co.kr.key

* 설명 : 개인키 경로 설정 및 파일 명

SSLCertificateChainFile /etc/httpd/conf.d/ssl/ChainFile_ChainBundle.crt

* 설명 : Chain 인증서 경로 설정 및 파일 명

SSLCACertificateFile /etc/httpd/conf.d/ssl/CA_GLOBALSIGN_ROOT_CA.crt

* 설명 : Root 인증서 경로 설정 및 파일 명

-----중략-----

</VirtualHost>

<VirtualHost *:443>

* 설명 : dev.ucert.co.kr SSL 설정을 합니다.

DocumentRoot "/var/dev/html"

* 설명 : dev 홈 디렉토리 설정을 합니다.

ServerName dev.ucert.co.kr:443

* 설명 : www가 아닌 dev 도메인 이름을 기입 합니다.

ErrorLog logs/ssl_error_log

TransferLog logs/ssl_access_log

LogLevel warn

SSLEngine on

* 설명 : SSL을 사용 합니다.

SSLProtocol all -SSLv2 -SSLv3

* 설명: SSL 프로토콜 설정을 합니다.

SSLCipherSuite DEFAULT:!EXP:!SSLv2:!DES:!IDEA:!SEED:+3DES



```
SSLCertificateFile /etc/httpd/conf.d/ssl/File_www.ucert.co.kr.crt
SSLCertificateKeyFile /etc/httpd/conf.d/ssl/KeyFile_www.ucert.co.kr.key
SSLCertificateChainFile /etc/httpd/conf.d/ssl/ChainFile_ChainBundle.crt
SSLCACertificateFile /etc/httpd/conf.d/ssl/CA_GLOBALSIGN_ROOT_CA.crt
```

* 설명 : 인증서 위치는 www.ucert.co.kr 도메인과 동일한 위치로 지정 합니다.

-----중략-----

</VirtualHost>

4. 아파치 프로세스 재시작을 진행 합니다.

```
[root@localhost httpd]# /usr/sbin/apachectl -t
```

Syntax OK

* 설명 : 설정 문법에 오류가 없는 지 확인 합니다.

```
[root@localhost httpd]# /usr/sbin/apachectl -v
```

* 설명 : 아파치 버전을 확인 합니다.

※ 비밀번호가 설정 된 인증서라면 재시작 시 비밀번호 입력을 합니다.

비밀번호가 제거 된 인증서 사용 시 비밀번호 입력이 불필요합니다.

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

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

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

* 설명 : 아파치 재시작을 진행 합니다.

※ 재기동 명령어는 서버마다 상이하여 명령어 확인 후 진행이 필요합니다.

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

* 설명 : 아파치 데몬 확인을 진행 합니다.

root	117031	1	0 Feb20	00:00:03	/usr/sbin/httpd
daemon	117032	117031	0 Feb20	00:00:00	/usr/sbin/httpd
daemon	117033	117031	0 Feb20	00:00:00	/usr/sbin/httpd
daemon	117034	117031	0 Feb20	00:00:00	/usr/sbin/httpd
daemon	117121	117031	0 Feb20	00:00:00	/usr/sbin/httpd
root	118682	117620	0 01:22 pts/1	00:00:00	grep httpd



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

* 설명 : 적용한 SSL 포트의 Listen 여부를 확인 합니다.

```
tcp        0      0 0 :::80          :::*   LISTEN    118721/httpd
tcp        0      0 0 :::443         :::*   LISTEN    118721/httpd
```

5. 인증서 설치를 확인 합니다.

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

* 설명 : 위의 명령어를 입력하여 인증서 갱신 날짜를 확인 합니다.

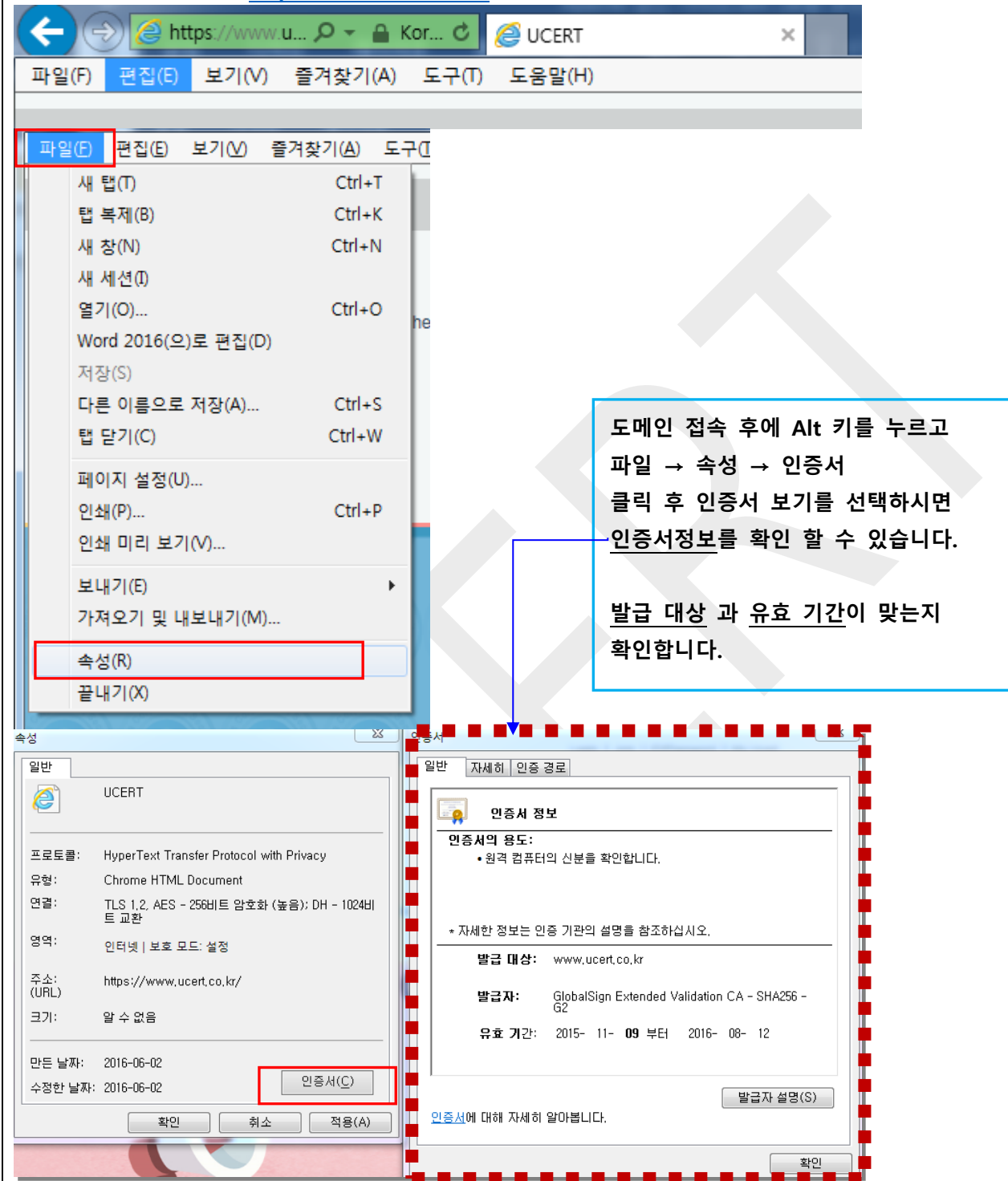
```
notBefore=Jan 1 00:24:14 2018 GMT #인증서 시작일
```

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

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

6. 웹페이지에서 인증서를 확인 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