

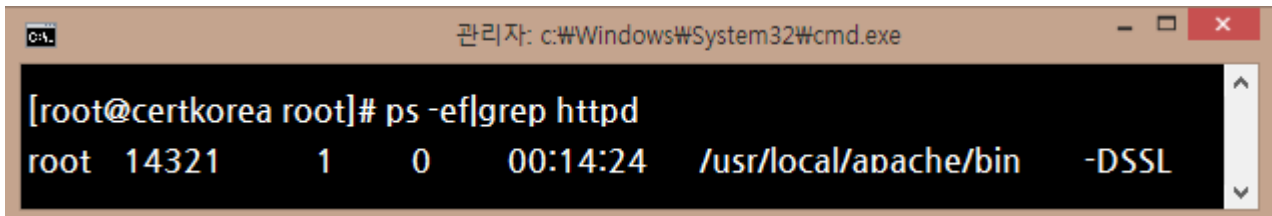
# Apache SSL인증서 설치가이드

써트코리아

(주)파인앤서비스

## 1. 사전준비

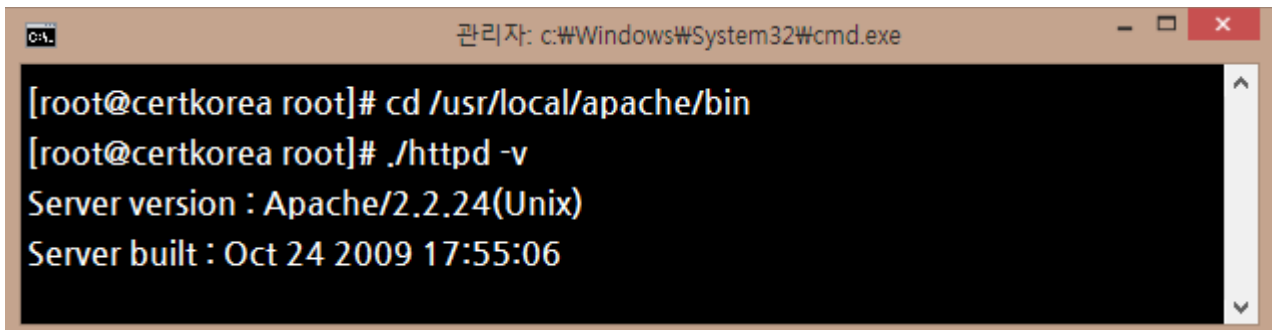
### 1) Apache 프로세스 확인

A terminal window titled '관리자: c:\Windows\System32\cmd.exe' showing the command '[root@certkorea root]# ps -ef|grep httpd'. The output is 'root 14321 1 0 00:14:24 /usr/local/apache/bin -DSSL'.

```
[root@certkorea root]# ps -ef|grep httpd
root 14321 1 0 00:14:24 /usr/local/apache/bin -DSSL
```

※ 프로세스 위치가 /usr/sbin/httpd 로 확인되는 경우, 환경설정파일(.conf)은 /etc/httpd/conf 및 /etc/httpd/conf.d 폴더에 있습니다.

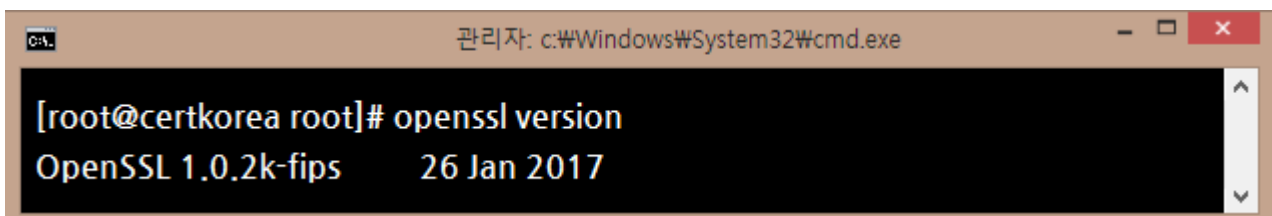
### 2) Apache 버전 확인

A terminal window titled '관리자: c:\Windows\System32\cmd.exe' showing the commands '[root@certkorea root]# cd /usr/local/apache/bin' and '[root@certkorea root]# ./httpd -v'. The output is 'Server version : Apache/2.2.24(Unix)' and 'Server built : Oct 24 2009 17:55:06'.

```
[root@certkorea root]# cd /usr/local/apache/bin
[root@certkorea root]# ./httpd -v
Server version : Apache/2.2.24(Unix)
Server built : Oct 24 2009 17:55:06
```

※ ./httpd -v 명령어로 확인되지 않는 경우, ./apachectl -v 로 확인하시면 됩니다.

### 3) openssl 버전 확인

A terminal window titled '관리자: c:\Windows\System32\cmd.exe' showing the command '[root@certkorea root]# openssl version'. The output is 'OpenSSL 1.0.2k-fips 26 Jan 2017'.

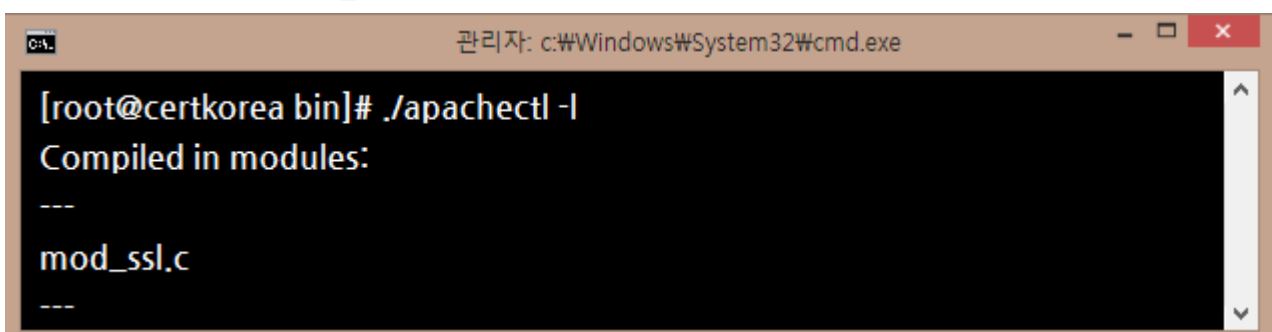
```
[root@certkorea root]# openssl version
OpenSSL 1.0.2k-fips 26 Jan 2017
```

※ openssl 1.0.1 버전 이상 사용을 권장합니다. (TLS1.2 지원 버전)

※ TLS1.3은 openssl 1.1.1 이상에서 지원됩니다.

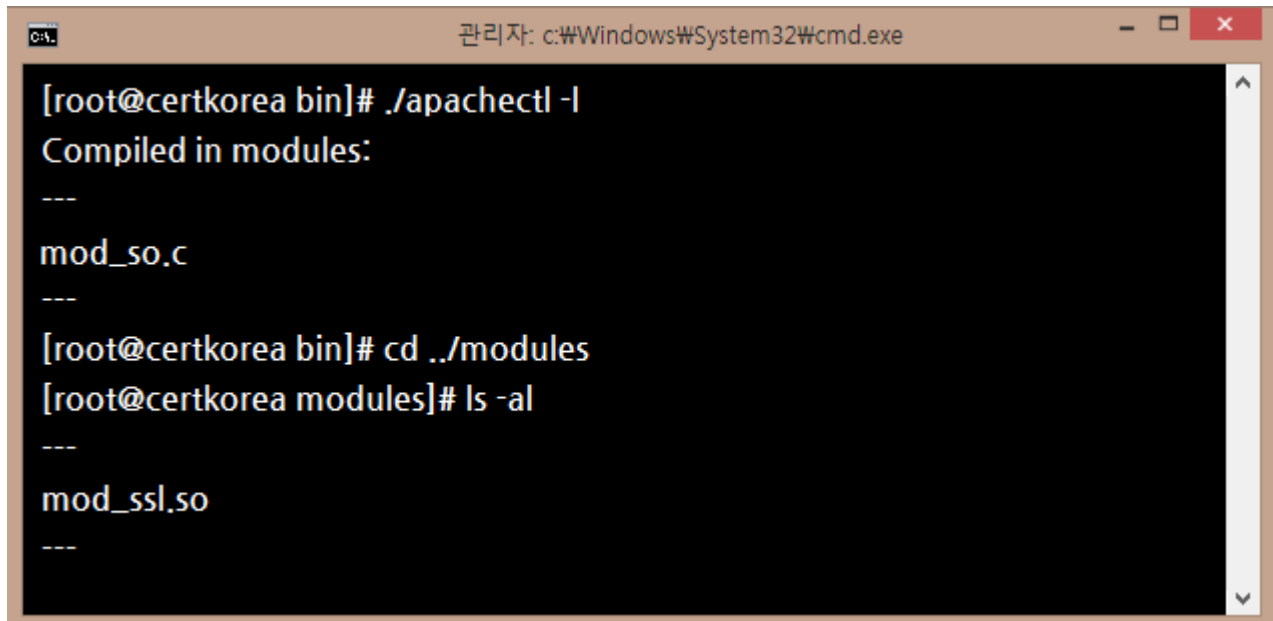
### 4) mod\_ssl 확인

- 정적모듈로 설치된 mod\_ssl 확인

A terminal window titled '관리자: c:\Windows\System32\cmd.exe' showing the command '[root@certkorea bin]# ./apachectl -l'. The output is 'Compiled in modules:' followed by 'mod\_ssl.c' on a separate line.

```
[root@certkorea bin]# ./apachectl -l
Compiled in modules:
---
mod_ssl.c
---
```

- 동적모듈로 설치된 mod\_ssl 확인



```
C:\Windows\System32\cmd.exe
[root@certkorea bin]# ./apachectl -l
Compiled in modules:
---
mod_so.c
---
[root@certkorea bin]# cd ../modules
[root@certkorea modules]# ls -al
---
mod_ssl.so
---
```

※ 정적모듈 or 동적모듈 중 하나로만 확인되면 됩니다.

※ 동적모듈의 경우, mod\_so.c 및 mod\_ssl.so 둘 다 확인된 경우에만 SSL 적용 가능합니다.

## 2. 인증서 설치

※ 갱신 설치의 경우, 기존 인증서 파일 백업 후 갱신된 인증서 파일 저장, Apache 서비스 재시작 하시면 됩니다.

- 1) httpd.conf 파일에서 mod\_ssl 모듈을 Load

### #동적모듈

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

※ httpd.conf 파일에서 해당 부분을 주석해제 하거나, 추가합니다.

※ mod\_ssl이 정적모듈로 설치된 경우, 이 부분은 생략 됩니다.

- 2) httpd.conf 파일에서 httpd-ssl.conf 파일을 Include

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

OR

```
<IfModule mod_ssl.c>
Include          extra/httpd-ssl.conf
</IfModule>
```

※ httpd.conf 파일에서 해당 부분을 주석해제 하거나, 추가합니다.

3) httpd-ssl.conf 파일에서 SSL포트 Listen 및 VirtualHost 설정

```
Listen 443
```

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

```
DocumentRoot "/usr/local/htdocs" ← Document Root 동기화
```

```
ServerName www.certkorea.co.kr:443 ← ServerName 동기화
```

```
.....
```

```
#SSL 환경설정
```

```
SSLEngine on
```

```
SSLProtocol -All +TLSv1.2 +TLSv1.3
```

```
SSLCipherSuite ECDHE-RSA-AES128-GCM-SHA256:ECDHE-RSA-AES256-GCM-SHA384:ECDHE-RSA-CHACHA20-POLY1305:DHE-RSA-AES128-GCM-SHA256:DHE-RSA-AES256-GCM-SHA384
```

```
#인증서(cert), 개인키(key), 체인(chainca) 설정
```

```
SSLCertificateFile /usr/local/apache/conf/ssl/www.certkorea.co.kr.crt
```

```
SSLCertificateKeyFile /usr/local/apache/conf/ssl/www.certkorea.co.kr.key
```

```
SSLCACertificateFile /usr/local/apache/conf/ssl/chainca.crt
```

```
.....
```

```
</VirtualHost>
```

※ JkMount(mod\_jk.so)를 이용해서 Tomcat과 연동되는 경우, 80포트의 JkMount 설정을 SSL 관련 VirtualHost에 동일하게 복사해야 합니다.

※ TLS1.3은 openssl 1.1.1 이상에서 지원됩니다.

openssl 1.0.1 및 1.0.2를 사용하는 경우, SSLProtocol 설정은 아래와 같이 사용하셔야 합니다.

**SSLProtocol -All +TLSv1.2**

※ Wildcard / SAN(멀티도메인) 인증서 설정 시, 각 도메인 별로 SSL VirtualHost를 설정하고, SSL 관련 설정(SSLEngine / SSLProtocol / SSLCipherSuite / SSLCertificateFile / SSLCertificateKeyFile / SSLCACertificateFile)을 동일하게 설정하시면 됩니다.

※ 갱신 설치 시, 기존 파일을 백업한 후 갱신된 인증서파일로 업로드 및 Apache 서비스 재시작 하시면 됩니다.

4) Syntax에 오류가 없는지 확인합니다.

```
관리자: c:\Windows\System32\cmd.exe

[root@certkorea bin]# ./apachectl configtest
Syntax OK
```

5) Apache 서비스를 재시작 합니다.

```
관리자: c:\Windows\System32\cmd.exe

[root@certkorea bin]# ./httpd stop
/usr/local/apache/apachectl stop : httpd stopped
[root@certkorea bin] # ./httpd start
```

- ※ ./httpd restart
- ./apachectl restart
- ./apachectl graceful
- 등 해당 서버의 서비스 재시작 방식으로 재시작 하시면 됩니다.

## 3. 설치 확인

1) 서비스 구동 확인

- 아래의 명령어로 서비스가 정상 구동되었는지 확인 합니다.

```
관리자: c:\Windows\System32\cmd.exe

[root@certkorea root]# ps -ef|grep httpd
root 14321      1    0   00:14:24   /usr/local/apache/bin   -DSSL
```

2) SSL 포트 확인

- 아래의 명령어로 SSL포트가 LISTEN 되는지 확인 합니다.

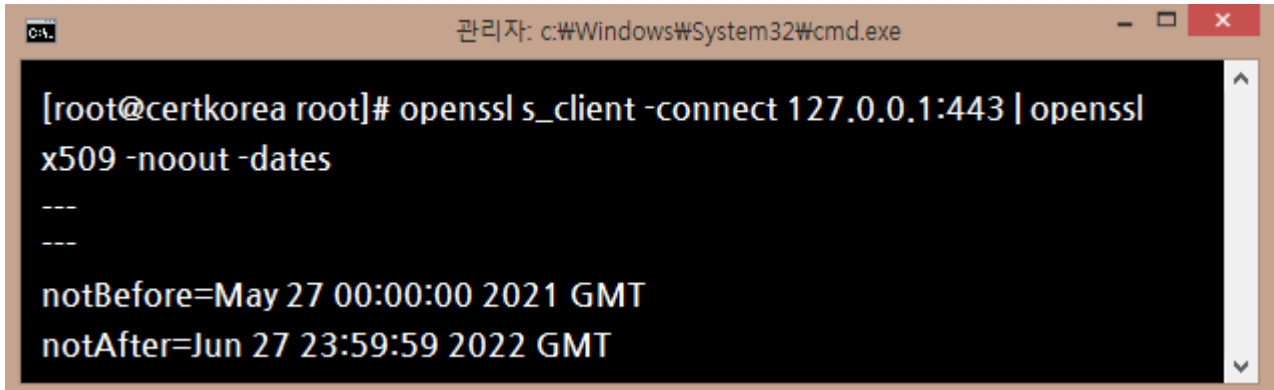
```
관리자: c:\Windows\System32\cmd.exe

[root@certkorea bin]# netstat -nap|grep httpd
tcp    0      0 0.0.0.0:80 0.0.0.0:*   LISTEN  14321/httpd
tcp    0      0 0.0.0.0:443 0.0.0.0:*   LISTEN  14321/httpd
```

### 3) openssl 명령어로 확인

- 아래의 명령어를 이용해서 서버에서 인증서 적용 여부를 확인합니다.

openssl s\_client -connect 127.0.0.1:443 | openssl x509 -noout -dates

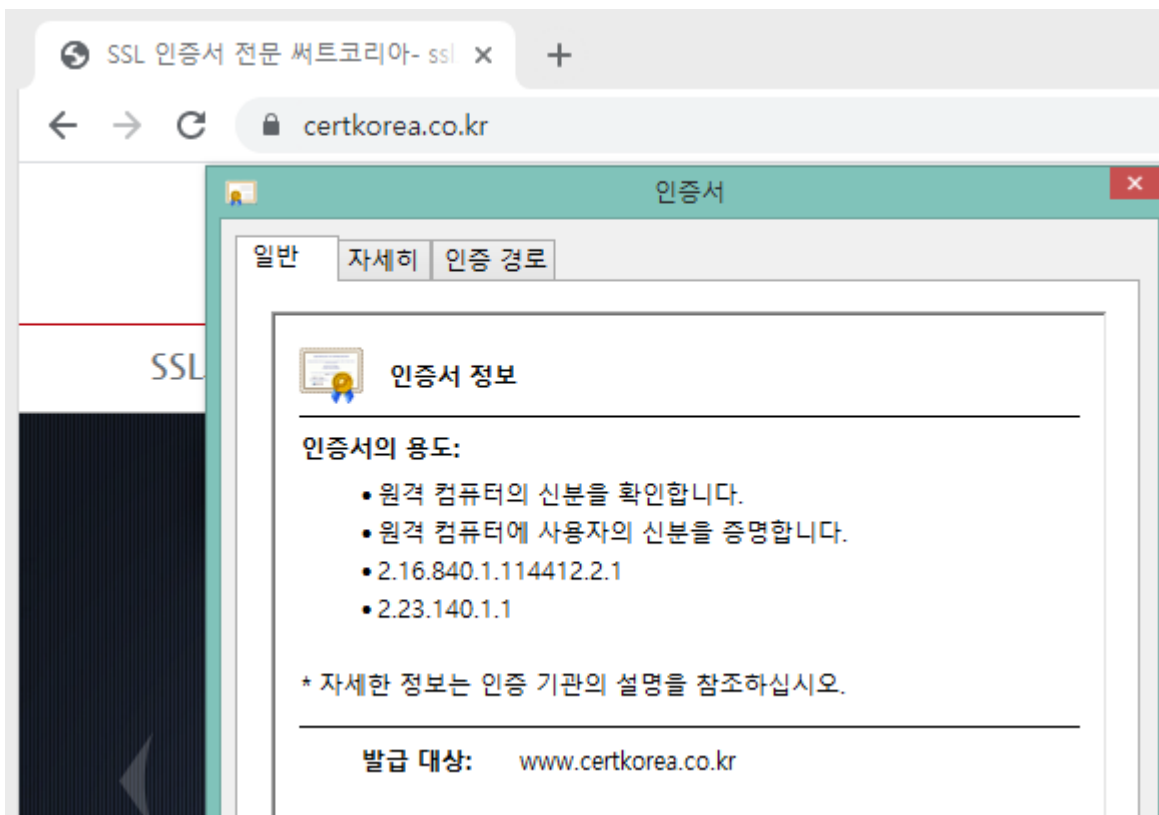


※ 127.0.0.1 대신에 localhost 나 도메인을 입력하셔도 됩니다.

※ 443 외에 다른 포트로 설정하신 경우, 해당 포트번호로 확인하시기 바랍니다.

### 4) 브라우저 확인

- 서버 브라우저 및 외부망 브라우저에서 https://도메인:SSL포트 로 접속, 인증서 정보를 확인합니다.



※ 설치관련 문의사항이나 오류가 있는 경우, 02-3444-2750 내선3번(기술문의) 로 연락 부탁드립니다.