

Apache

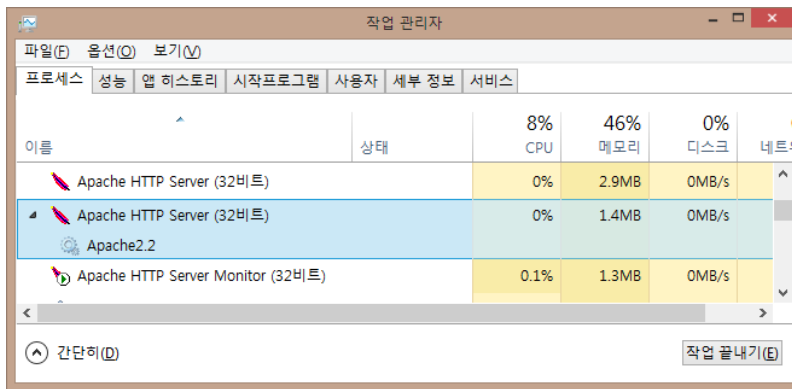
SSL 인증서 설치 매뉴얼

- Windows Apache용 -

I. 사전 준비

1. 프로세스 및 Apache 버전 확인

✓ Apache 프로세스 확인



이름	상태	8% CPU	46% 메모리	0% 디스크	네트워크
Apache HTTP Server (32비트)		0%	2.9MB	0MB/s	
Apache HTTP Server (32비트)		0%	1.4MB	0MB/s	
Apache2.2					
Apache HTTP Server Monitor (32비트)		0.1%	1.3MB	0MB/s	

◎ 작업관리자에서 Apache HTTP Server 혹은 httpd.exe 프로세스가 작동중인지 확인합니다.

✓ Apache 버전 확인

```
C:\Program Files (x86)\Apache2.2\bin>httpd.exe -v
```

```
Server version : Apache/2.2.25 (Win32)
```

```
Server built : Jul 10 2013 01:52:12
```

```
C:\Program Files (x86)\Apache2.2\bin>
```

I. 사전 준비

2. mod_ssl 확인 및 설치

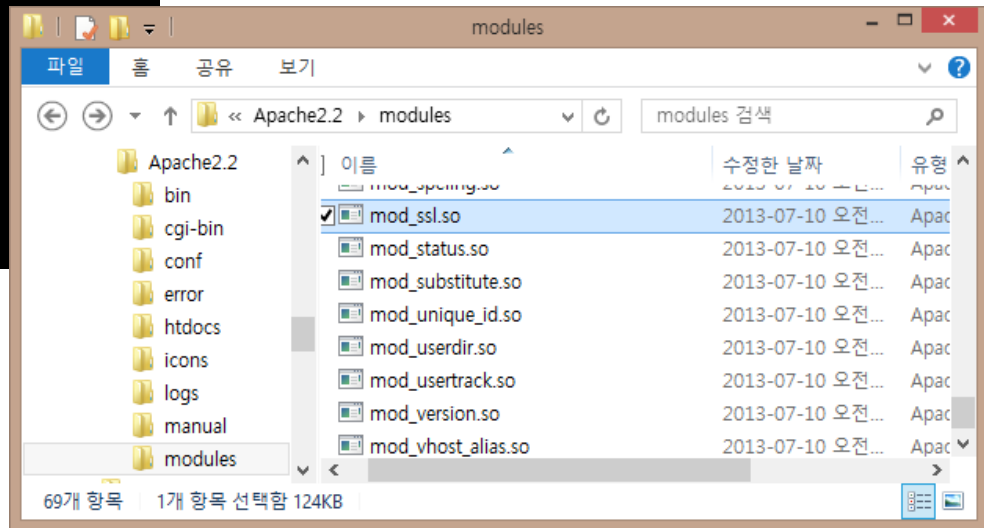
✓ mod_ssl 확인

◎ . bin 폴더에 mod_so.c 파일이 있는지 확인한 후 modules 폴더에 mod_ssl.so 파일이 있는지 확인합니다.

```
C:\Program Files (x86)\Apache2\bin>httpd.exe -l
```

Compiled in modules:

```
core.c
mod_win32.c
mpm_winnt.c
http_core.c
mod_so.c
```



- ✓ mod_ssl.so 파일이 없는 경우, apache가 no_ssl 버전으로 설치된 것입니다.
SSL 포함한 Apache로 다시 설치하셔야 합니다.
Ex)httpd-2.2.25-win32-openssl-0.9.8y.msi

I. 사전 준비

3. openssl 버전 확인

```
C:\Program Files (x86)\Apache2.2\bin>openssl version  
OpenSSL 0.9.8y 5 Feb 2013  
C:\Program Files (x86)\Apache2.2\bin>
```

4. 인증서 파일 확인 및 저장

- ✓ 써트코리아를 통해 발급받은 인증서 파일을 확인합니다.
- ✓ Apache용 인증서는 다음과 같은 파일로 구성되어 있습니다.
 - ◎ www.domain.com.crt : 인증서 파일(공개키)
 - ◎ www.domain.com.key : 개인키 파일(비밀키)
 - ◎ chainca.crt : 루트/중개인증서 파일(인증서 종류에 따라 다릅니다.)

5. 인증서 갱신 시

- ✓ 기존 인증서 파일 백업 > 갱신된 인증서 업데이트 > Apache 서비스 재시작만 처리하시면 됩니다.

II. 인증서 설치

1. httpd.conf

✓ mod_ssl 모듈을 Load

```
#  
# Dynamic Shared Object (DSO) Support  
#  
# To be able to use the functionality of a module which was built as a DSO you  
# have to place corresponding 'LoadModule' lines at this location so the  
# directives contained in it are actually available _before_ they are used.  
# Statically compiled modules (those listed by 'httpd -l') do not need  
# to be loaded here.  
#  
.....  
LoadModule ssl_module modules/mod_ssl.so  
.....  
#mod_ssl.so 관련 주석 해제
```

✓ httpd-ssl.conf 파일을 Include

```
# Various default settings  
#Include conf/extra/httpd-default.conf  
  
# Secure (SSL/TLS) connections  
Include conf/extra/httpd-ssl.conf  
#주석 해제
```

II. 인증서 설치

2. httpd-ssl.conf

✓ 443 포트를 Listen

```
Listen 443
```

✓ SSL 관련 VirtualHost 설정

```
<VirtualHost *:443>
DocumentRoot "C:\Program Files (x86)\Apache2.2\wwwroot"
ServerName www.certkorea.co.kr:443
.....
SSLEngine on
SSLProtocol All -SSLv2 -SSLv3
SSLCipherSuite ECDHE-RSA-AES128-SHA256:AES128-GCM-
SHA256:!RC4:HIGH:!MD5:!aNULL:!EDH
#인증서 파일의 위치를 지정합니다.
SSLCertificateFile "C:\Program Files (x86)\Apache2.2\conf\ssl\www.certkorea.co.kr.crt"
#개인키 파일의 위치를 지정합니다.
SSLCertificateKeyFile "C:\Program Files (x86)\Apache2.2\conf\ssl\www.certkorea.co.kr.key"
#루트/중개인증서 파일의 위치를 지정합니다.
SSLCACertificateFile "C:\Program Files (x86)\Apache2.2\conf\ssl\chainca.crt"
.....
</VirtualHost>
```

II. 인증서 설치

2. httpd-ssl.conf

◎ JkMount(mod_jk.so)를 이용해서 Tomcat과 연동 설정한 경우, SSL 관련 VirtualHost에도 동일하게 설정해주셔야 합니다.

◎ Wildcard / MDC(Multi-Domain) 인증서

-> Wildcard / MDC 인증서의 경우, ssl.conf 파일에 각 도메인의 VirtualHost 설정을 하고, 인증서 파일, 개인키 파일, 루트/중개인증서 파일, SSL 포트등 SSL관련 설정을 동일하게 처리하시면 됩니다.

3. 갱신설치

✓ 갱신 설치의 경우, 갱신 발급된 인증서 파일, 개인키 파일, 루트/중개인증서 파일로 교체하신 후, Apache 서비스만 재시작 하시면 됩니다.

II. 인증서 설치

4. 서비스 재시작

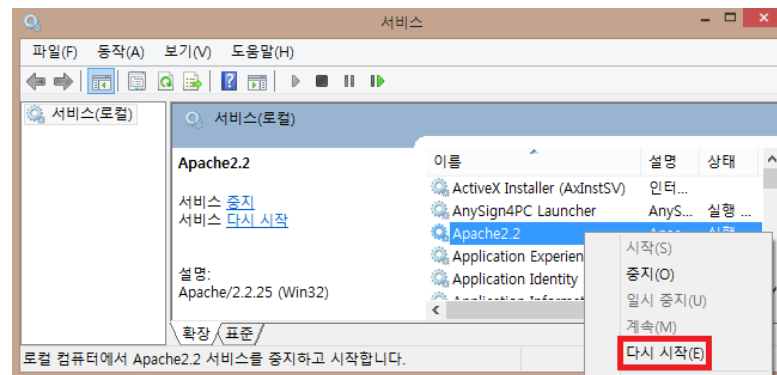
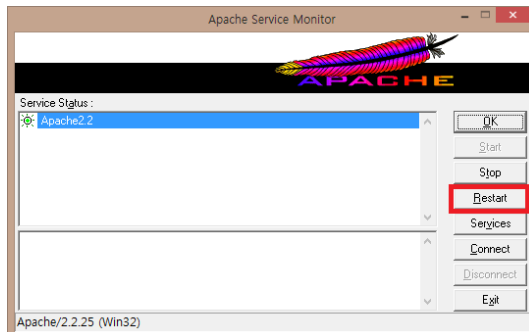
✓ 구문 오류 체크

```
C:\Program Files (x86)\Apache2.2\bin>httpd.exe -t  
Syntax OK
```

◎ 구문 오류 체크 시 error가 발생하면, 해당 error에 대한 처리를 완료하신 후 Apache 서비스를 재시작 해야합니다. 에러 메시지를 저희 씨트코리아로 보내주시면 처리 방법을 안내해 드리겠습니다.

✓ Apache 재시작

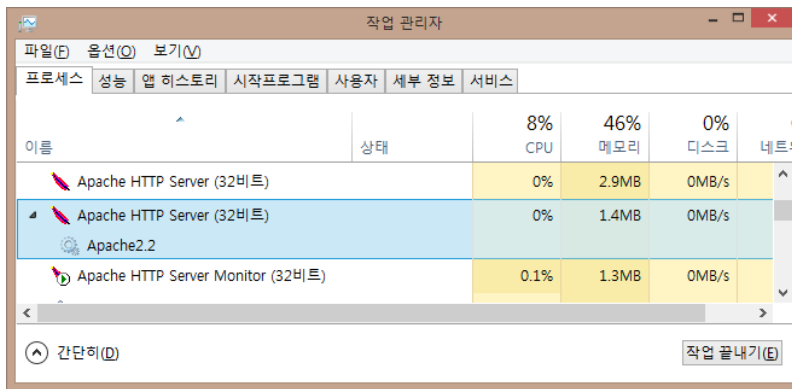
- ◎ Apache Service Monitor에서 Restart 하거나
- ◎ 관리도구 > 서비스 에서 Apache2.2 서비스 다시 시작



III. 확인 및 테스트

1. 서비스 구동 확인

✓ Apache 프로세스가 정상 작동되는지 확인 합니다.



The screenshot shows the Windows Task Manager window with the 'Processes' tab selected. It lists several Apache-related processes. The 'Apache HTTP Server (32비트)' process is highlighted in blue, indicating it is the active process.

이름	상태	8% CPU	46% 메모리	0% 디스크	네트
Apache HTTP Server (32비트)		0%	2.9MB	0MB/s	
Apache HTTP Server (32비트)		0%	1.4MB	0MB/s	
Apache2.2					
Apache HTTP Server Monitor (32비트)		0.1%	1.3MB	0MB/s	

◎ 작업관리자에서 Apache HTTP Server 혹은 httpd.exe 프로세스가 작동중인지 확인합니다.

2. SSL 포트 확인

✓ netstat 명령어로 SSL포트(기본 443)가 LISTEN 중인지 확인합니다.

```
C:\Program Files (x86)\Apache2\bin> netstat -an | findstr 443
```

TCP	0.0.0.0:443	0.0.0.0:0
TCP	[::]:443	[::]:0

III. 확인 및 테스트

3. 방화벽 확인

- ✓ 사용하고 있는 방화벽에서 SSL포트(기본 443)를 80포트와 동일한 조건으로 OPEN 해주시기 바랍니다.

4. 브라우저 테스트

- ✓ https로 사이트에 접속하여 자물쇠 및 인증서를 확인합니다.

Internet Explorer



Chrome



FireFox



◎ 영문회사명 표기 및 그린바는 EV 제품만 표시됩니다.
일반 SSL 인증서는 자물쇠 모양만 표시됩니다.

IV. 문제해결

✓ 서비스 재시작 후 443 포트가 Listen 되지 않는 경우

- ◎ httpd.conf 에서 ssl_module이 Load 되었는지 확인합니다.
- ◎ httpd.conf 에서 httpd-ssl.conf 파일이 Include 되었는지 확인합니다.
- ◎ httpd-ssl.conf 에서 Listen 443이 설정되었는지 확인합니다.

✓ 서비스 재시작 후 http로 확인되는 페이지가 https로 접속 시 “403 Not Found” 오류가 발생하는 경우

- ◎ httpd.conf의 80포트 관련 Directory 설정을 httpd-ssl.conf 파일의 443포트 관련 VirtualHost에 복사해 주시면 됩니다.

✓ Error_log

- ◎ 그 외의 문제가 발생할 경우 logs 폴더의 error_log를 확인하시고 오류구문을 써트코리아(support@certkorea.co.kr)로 보내주시기 바랍니다.

THANK YOU!