CERT KOREA

FINE& SERVICE

Tomcat
SSL인증서 설치가이드

써트코리아

(주)파인앤서비스

1. 인증서 설치

※ 갱신 설치의 경우, 기존 인증서 파일 백업 후 갱신된 인증서 파일 저장, Tomcat 서비스 재시작만 처리 하시면 됩니다.

1) server.xml 파일에서 SSL VirtualHost 설정

※ 아래 예시의 노란색 주석부분을 참고해서 설정합니다. 그 외의 항목은 기존 설정을 그대로 사용하면 됩니다.

※ Tomcat 버전 및 설치 환경에 따라 설정을 선택해서 적용하시기 바랍니다.

◎ Tomcat 6-7

```
<Connector port="443" protocol="HTTP/1.1" SSLEnabled="true"
       maxThreads="150" scheme="https" secure="true" clientAuth="false"
       keystoreFile="/usr/local/tomcat/ssl/domain.jks"
       keystorePass="password" sslProtocol="TLS" />
```

◎ Tomcat 8

```
<Connector port="443" protocol="HTTP/1.1" SSLEnabled="true"
       maxThreads="150" scheme="https" secure="true" clientAuth="false"
       keystoreFile="/usr/local/tomcat/ssl/domain.jks"
       keystorePass="password" sslProtocol="TLS"
       ciphers="TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384,
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256. TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384,
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256, TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA,
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA" />
```

◎ Tomcat 8.5 이상

```
<Connector port="443" protocol="org.apache.coyote.http11.Http11NioProtocol"
       maxThreads="150" SSLEnabled="true" >
       <SSLHostConfig hostName="domain.com">
          <Certificate certificateKeystoreFile="/usr/local/tomcat/ssl/domain.jks"
                certificateKeystorePassword="password" type="RSA"
                ciphers="TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384,
                TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256,
                TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384,
                TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256,
                TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA,
                TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA" />
       </SSLHostConfig>
</Connector>
```

※ Tomcat 9 일부 버전에서 위의 설정으로 정상 반영되지 않을 수 있습니다.
위의 설정으로 적용되지 않을 경우, Tomcat8 설정을 적용하시면 됩니다.

◎ Tomcat - PFX(P12)

```
<Connector port="443" protocol="org.apache.coyote.http11.Http11NioProtocol" SSLEnabled="true"
        maxThreads="150" scheme="https" secure="true" clientAuth="false"
        keystoreFile="/usr/local/tomcat/ssl/domain.pfx" keystoretype="pkcs12"
        keystorePass="password" sslProtocol="TLS"
        ciphers="TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384,
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256, TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384,
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256, TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA,
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA" />
```

※ PFX/P12 파일은 같은 형식의 파일입니다.

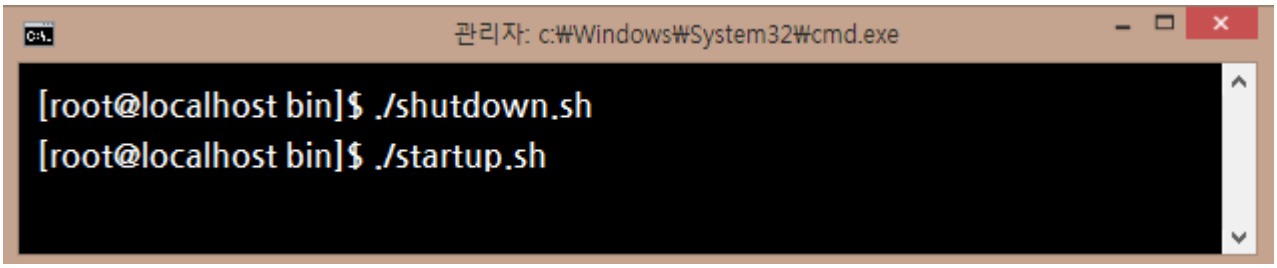
◎ Tomcat 8 이하 - APR

```
<Connector port="443" protocol="org.apache.coyote.http11.Http11AprProtocol" SSLEnabled="true"
        maxThreads="150" scheme="https" secure="true" clientAuth="false"
        SSLCertificateFile="/usr/local/tomcat/ssl/domain.crt"
        SSLCertificateKeyFile="/usr/local/tomcat/ssl/domain.key"
        SSLCertificateChainFile="/usr/local/tomcat/ssl/chainca.crt"
        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"
        SSLHonorCipherOrder="on"/>
```

◎ Tomcat 8.5 이상 - APR

```
<Connector port="443" protocol="org.apache.coyote.http11.Http11AprProtocol"
        maxThreads="150" SSLEnabled="true" >
        <SSLHostConfig hostName="domain.com">
            <Certificate certificateFile="/usr/local/tomcat/ssl/domain.crt"
                    certificateKeyFile="/usr/local/tomcat/ssl/domain.key"
                    certificateChainFile="/usr/local/tomcat/ssl/chainca.crt" type="RSA"
                    ciphers="TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384,
                    TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256,
                    TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384,
                    TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256,
                    TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA,
                    TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA" />
        </SSLHostConfig>
        </Connector>
```

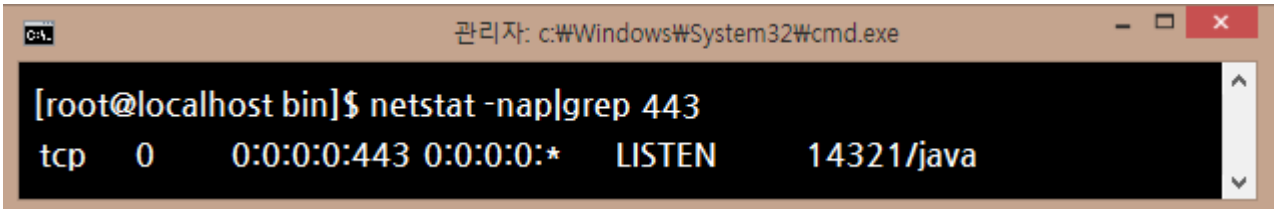
2) Tomcat 서비스 재시작



2. 설치 확인

1) SSL 포트 확인

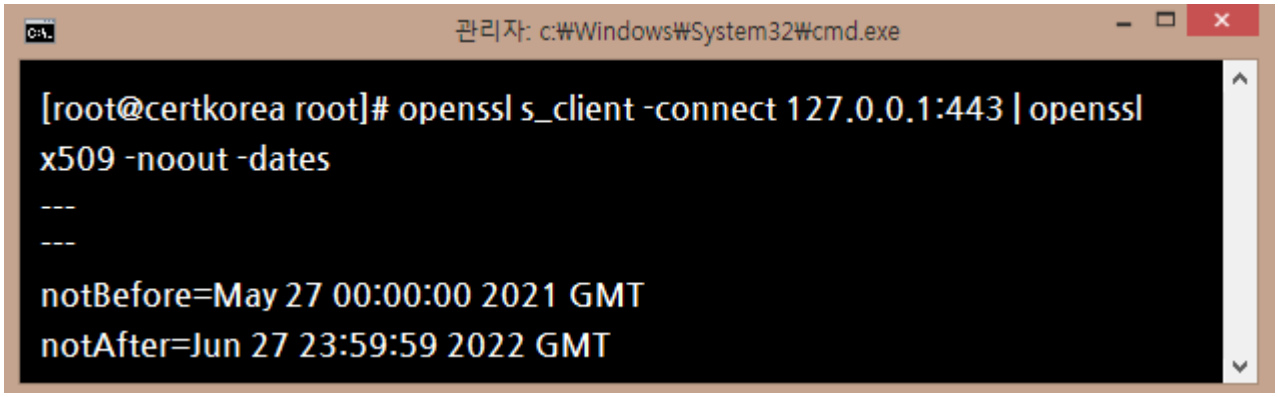
- 아래의 명령어로 SSL포트가 LISTEN 되는지 확인 합니다.



2) openssl 명령어로 확인

- 아래의 명령어를 이용해서 서버에서 인증서 적용 여부를 확인합니다.

openssl s_client -connect 127.0.0.1:443 | openssl x509 -noout -dates

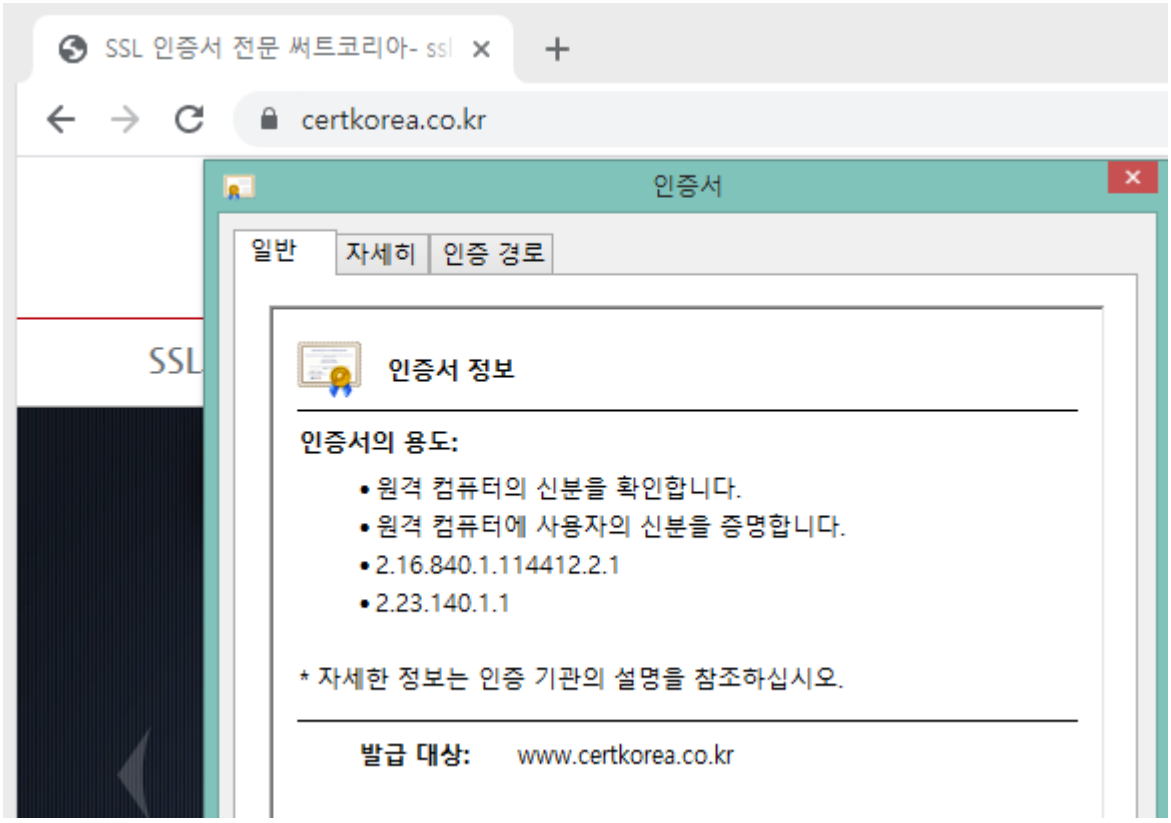


※ 127.0.0.1 대신에 localhost 나 도메인을 입력하셔도 됩니다.

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

3) 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 부탁 드립니다.