TOMCAT(JKS) 보안서버인증서 설치 가이드

보안서버인증서 구성파일 안내

Private.key	**개인키** (예스닉에 CSR 생성을 요청하신 경우에만 제공됩니다.)
도메인명_crt.pem	**보안서버인증서** (CRT 파일)
ChainCA.crt	**체인인증서 번들** (ChinCA1+ChainCA2)
RootCA.crt	**루트인증서**
CSR.pem	**CSR** (인증서 신청 시 사용된 CSR 값)

예스닉 보안서버인증서는 기본적으로 PEM 형식으로 제공되고 있으며,
Tomcat 서버에 인증서를 설치하는 경우 JKS 형식의 인증서 번들파일이 필요합니다.
(APR Connector를 사용하시면 기본 제공된 PEM 형식의 인증서를 사용하기에 JKS 변환이 필요 없습니다.)

PEM 형식의 인증서를 JKS 형식의 인증서로 변환하기 위해서는, 먼저 PFX 형식으로 변환합니다. (openssl 필요)

```
cat 도메인명_crt.pem ChainCA.crt RootCA.crt > 도메인명_bundle.pem

openssl pkcs12 -export -name 도메인명 -in 도메인명_bundle.pem -inkey Private.key -out 도메인명.pfx
```

위에서 변환한 PFX 파일을 Tomcat이 설치된 서버에 업로드 하고, keytool 명령어로 JKS 형식으로 변환합니다.

```
keytool -importkeystore -srckeystore 도메인명.pfx -srcstoretype pkcs12 -destkeystore 도메인명.jks -deststoretype jks
```

Keystore에서 개인키(.jks, .keystore 등)와 CSR을 생성하여 신청하셨다면,
아래 명령어를 참고하여 **루트>체인1>체인2>보안서버인증서** 순서로 등록합니다.
(ChainCA.crt 파일 내용에 BEGIN ~ END 구문을 참고하여 ChainCA1.crt 와 ChainCA2.crt 로 분할합니다.)

```
keytool -import -trustcacerts -alias root -file RootCA.crt -keystore 개인키이름
keytool -import -trustcacerts -alias chain1 -file ChainCA1.crt -keystore 개인키이름
keytool -import -trustcacerts -alias chain2 -file ChainCA2.crt -keystore 개인키이름
keytool -import -trustcacerts -alias crt -file 도메인명_crt.pem -keystore 개인키이름
```

위 과정을 직접 진행하기 어려운 경우, 1:1 친절상담이나 메일로 JKS 형식의 인증서 번들파일 제공을 요청하세요.
(직접 CSR을 생성하신 경우엔 인증서 비밀번호와 함께 개인키 또는 키스토어 파일을 첨부하여 요청해 주세요.)

JKS 형식의 인증서 번들파일을 Tomcat 서버 내 임의의 인증서 폴더에 업로드 하고,
아래 내용을 참고하여 설정 파일을 수정합니다. (APR Connector를 사용하면 PEM 형식의 인증서 업로드 필요)

1. 서버 설정파일 수정 (일반적으로 Tomcat 홈/conf/**server.xml**)

   아래 구문을 찾아 인증서 설치포트, 파일 및 비밀번호 등 내용을 수정합니다.

   (1) Tomcat 6.x 이하 버전

```
<Connector
port="443" protocol="HTTP/1.1" SSLEnabled="true" maxThreds="150" scheme="https" secure="true"
keystoreFile="(인증서 파일 업로드 경로)/(업로드한 JKS 파일명)" keystorePass="(인증서 비밀번호)"
sslEnabledProtocols="TLS"
/>
```

   (2) Tomcat 7.x 이상 버전

```
<Connector
port="443" protocol="HTTP/1.1" SSLEnabled="true" maxThreds="150" scheme="https" secure="true"
keystoreFile="(인증서 파일 업로드 경로)/(업로드한 JKS 파일명)" keystorePass="(인증서 비밀번호)"
sslProtocol="TLSv1.2"
/>
```

   (3) Tomcat + APR 사용

```
<Connector
port="8443" protocol="org.apache.coyote.http11.Http11AprProtocol" SSLEnabled="true"
maxThreds="150" scheme="https" secure="true" SSLProtocol="TLSv1.2"
SSLPassword="(인증서 비밀번호)"
SSLCertificateKeyFile="(인증서 파일 업로드 경로)/Private.key"
SSLCertificateFile="(인증서 파일 업로드 경로)/도메인명_crt.pem"
SSLCertificateChainFile="(인증서 파일 업로드 경로)/ChainCA.crt"
SSLCACertificateFile="(인증서 파일 업로드 경로)/RootCA.crt"
/>
```

2. 수정을 완료하면 Tomcat 웹서버를 재시작하여 적용되었는지 확인합니다.

적용 과정에 오류가 있는 경우 오류내용, 로그, 스크린샷 등을 첨부하여 **1:1 친절상담**이나 **메일**로 문의해 주세요.