

Tomcat6(단일도메인& 멀티도메인) 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

02-512-9375



1. Server.xml 파일을 확인하여 SSL 인증서 설정합니다.

```
root@ucert ssl]# vi /usr/local/tomcat/conf/server.xml
<!--
<Connector port="8443" protocol="HTTP/1.1" SSLEnabled="true" maxThreads="150"
scheme="https" secure="true"
※포트번호 같은 경우 443으로 설정되어 있어야 기본 https 접속이 가능하다.
keystoreFile="/usr/local/ssl/www.ucert.co.kr.jks" //인증서 파일 위치 및 파일
keystorePass="*****" //인증서 비밀번호
clientAuth="false" sslProtocol="TLS" />
-->
// 주석을 제거하도록 한다. // <!-- : 시작 / --> : 끝
```

2. 발급 받으신 인증서를 해당 SSL 폴더에 업로드 또는 저장합니다.

```
[root@localhost /ssl]$ ll
-rw-r--r--. 1 root root 1931 Jan 1 11:48 www.ucert.co.kr.jks
-rw-r--r--. 1 root root 1744 Jan 1 11:49 password
```

3. Tomcat을 재실행 주도록 합니다.

```
root@localhost /bin]# ./shutdown.sh
root@localhost /bin]# ./startup.sh
```

4. 포트 확인 : 설정하신 SSL 포트가 Listen 상태 인지 확인합니다.

```
[root@localhost ~]# netstat -na | grep java
tcp        0 0 :::80          :::* LISTEN
tcp        0 0 :::8443        :::* LISTEN
```

웹브라우저 주소창에 "https://도메인:SSL포트" 를 입력하여 접속이 되는지 확인합니다.
SSL기본포트인 443포트로 설정하셨다면 https://도메인 으로 접속 해 주셔도 됩니다.

5. 서버 내에서 인증서 갱신을 확인하도록 합니다.

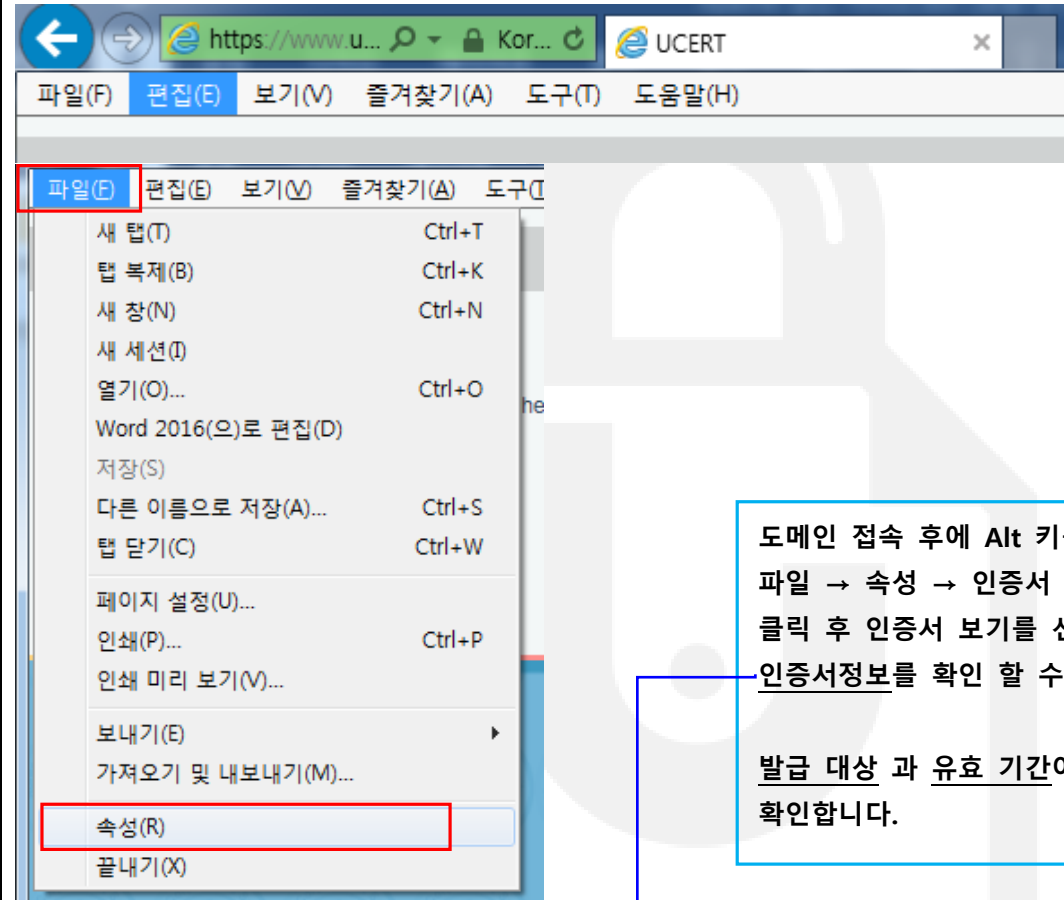
```
[root@localhost ~]# echo "" | openssl s_client -connect localhost:8443 | openssl x509 -noout -dates
위의 명령어를 입력하여 인증서 갱신 날짜를 확인하도록 합니다.

notBefore=Jan 1 00:24:14 2016 GMT      #인증서 시작일
notAfter=Dec 31 :38:20 2017 GMT      #인증서 만료일
```



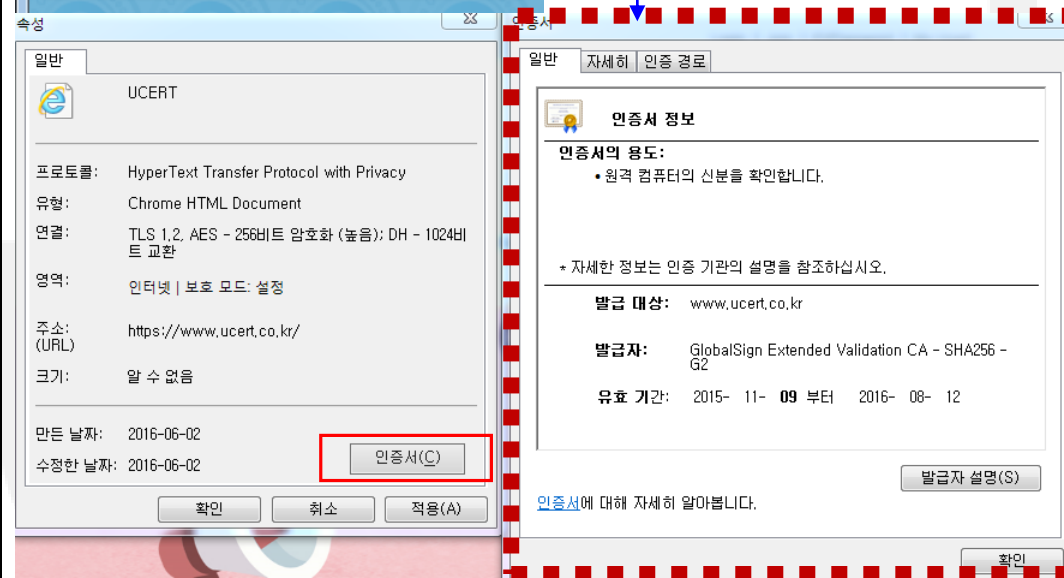
6. 웹페이지에서의 인증서 확인 방법

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.



www.ucert.co.kr



본 문서는 주식회사 한국기업보안에서 SSL보안서버인증서 설치를 위해 작성된 문서로
주식회사 한국기업보안의 동의 없이 무단으로 사용하실 수 없습니다

Copyright 2018. Korea Corporation Security Co., Ltd All pictures cannot be copied without permission.