

# Tomcat8(단일도메인& 멀티도메인) SSL 인증서 갱신 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



※Tomcat 8의 경우 2가지 버전에 따라 설정 방법이 다릅니다. 아래의 버전 별로 적용 부탁드립니다.

## 아파치 톰캣 8.0.x 이상 버전일 경우

1. Server.xml 파일을 확인하여 SSL 인증서 확인.

```
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]$ cp www.ucert.co.kr.jks ssl_old_20160101
[root@localhost /ssl]$ cp password ssl_old_20160101
```

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.

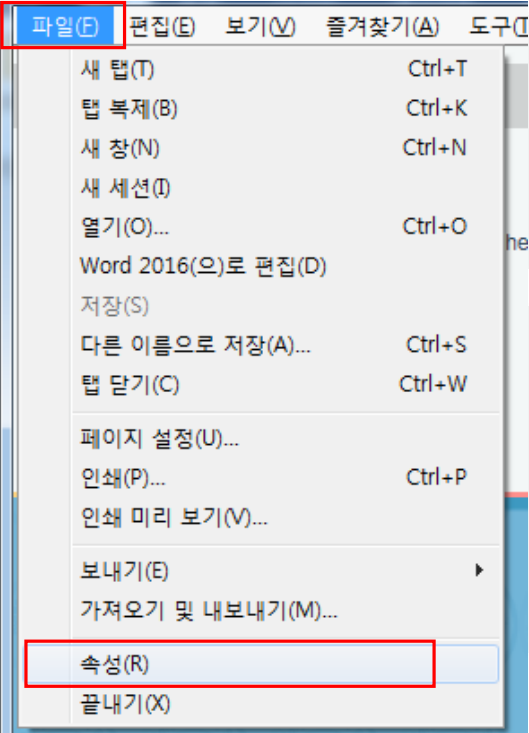
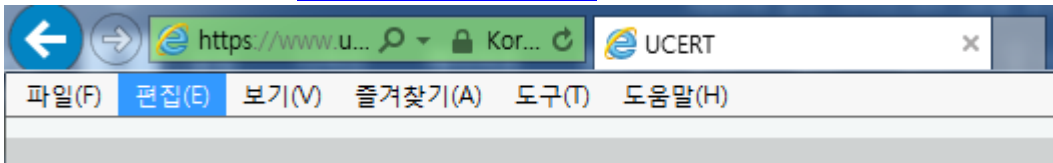
```
[root@localhost ~]# echo "" | openssl s_client -connect localhost:8443 | openssl x509 -noout -dates
위의 명령어를 입력하여 인증서 갱신 날짜를 확인하도록 합니다.

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

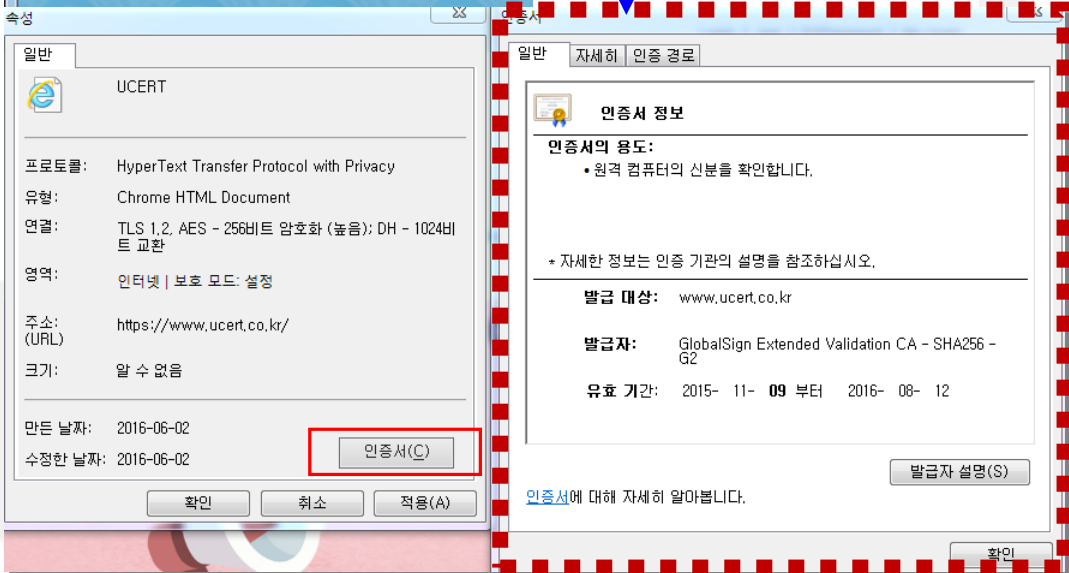
6. 웹페이지에서의 인증서 확인 방법



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](http://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.

## 아파치 톰캣 8.5.x 이상 버전일 경우

8.5x 이상의 경우 아래의 주의 사항을 살펴보자.

- 1) 이 버전의 경우 위 8.0.x의 버전과 동일한 방법으로 진행을 해도 무방하다.
- 2) 톰캣 재시작 이후 약 1분 정도 사이트 접속이 되지 않는다. 이 경우 프로세스는 가동중이지만 웹에서의 접속은 잠시 불가하다.
- 3) 8.5x 이상의 경우 1)으로 인해 SSL 설정 방법이 2가지가 된다.

1. Server.xml 파일을 확인하여 SSL 인증서 확인.

```
root@ucert ssl]# vi /usr/local/tomcat/conf/server.xml
<!--
<Connector port="8443" protocol="org.apache.coyote.http11.Http11NioProtocol"
    ※포트번호는 원하는 포트로 진행한다. 디폴트로 443 포트를 사용한다.
    maxThreads="150" SSLEnabled="true">
    <SSLHostConfig>
        <Certificate certificateKeystoreFile="/usr/local/ssl/www.ucert.co.kr.jks"
            certificateKeystorePassword="*****"
            ※인증서 경로 및 패스워드 확인.
            type="RSA" />
    </SSLHostConfig>
</Connector>
-->
// 주석을 제거하도록 한다. // <!-- : 시작 / --> : 끝
```

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

```
[root@localhost /ssl]$ cp www.ucert.co.kr.jks ssl_old_20160101
[root@localhost /ssl]$ cp password ssl_old_20160101
```

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
```

# UCERT

[www.ucert.co.kr](http://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.

## 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.

속성

일반

UCERT

프로토콜: HyperText Transfer Protocol with Privacy  
유형: Chrome HTML Document  
연결: TLS 1.2, AES - 256비트 암호화 (높음); DH - 1024비트 교환  
영역: 인터넷 | 보호 모드: 설정  
주소 (URL): <https://www.ucert.co.kr/>  
크기: 알 수 없음

만든 날짜: 2016-06-02  
수정한 날짜: 2016-06-02

인증서(C)

확인 취소 적용(A)

인증서 정보

인증서의 용도:

- 원격 컴퓨터의 신분을 확인합니다.
- 자세한 정보는 인증 기관의 설명을 참조하십시오.

발급 대상: [www.ucert.co.kr](http://www.ucert.co.kr)

발급자: GlobalSign Extended Validation CA - SHA256 - G2

유효 기간: 2015- 11- 09 부터 2016- 08- 12

발급자 설명(S)

인증서에 대해 자세히 알아보십시오.

확인

[www.ucert.co.kr](http://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.