

Copyright 2015 By KICA. All Right Reserved.

Tomcat v5.0+ SSL 설치가이드

Win32, Linux 공통 문서

한국정보인증 KICASSL



당사로부터 JKS형태로 인증서를 받으셨다면 13Page부터 진행하시면 됩니다.

자주 발생하는 문의와 설치 오류 안내
설치 결과 확인 방법은
문서 마지막 장에 설명되어있습니다.

SSL 설치 중 오류 및 SSL 설치 확인 시 참고 부탁드립니다.

- ③ SSL 인증서 설치
- ④ SSL 인증서 설치 확인
- ⑤ SSL 암호화 통신 적용 예제

- SSL 설치 주의사항 및 자주 발생하는 설치 중 오류

③ SSL 인증서 설치

- 발급된 인증서 메일로 수신 (인증서 신청 시 기입한 기술담당자에게 메일로 발송)

- 웹 서버 환경에 따라 아래에 구성으로 전달됨

- (1) SSL 도메인 인증서 (SSL 인증서, 신청한도메인명_cert.pem)

- (2) 코모도 중개 인증서 모음

- 가. **apache, webtob, NginX** – Chain_RootCA_Bundle.crt

- 나. **IIS, Tomcat, Weblogic, Oracle Http Server, iPlanet, IBM HTTP Server, node.js**

- ChainCA1.crt ~ ChainCA2 또는 ChainCA3까지 **[상품마다 차이가 있으며, 압축파일 내 동봉된 ChainCA(숫자).crt 파일 모두 사용]**

- 중개 인증서파일이 하나 이상인 경우, 해당 중개 인증서 전부 검증에 이용합니다

- (3) 코모도 루트 인증서 (RootCA.crt)

**※ 웹서버에 따라 사용하는 중개인증서와 루트인증서는
본 설치가이드에 기입된 파일 형태를 사용해 주시길 바랍니다.**

③ SSL 인증서 설치 [인증서 타입별 주의사항]

- 단일 / 멀티 / 와일드카드 도메인 SSL 인증서에 따른 설치 방법의 차이점

상품 종류	차이점
단일 도메인	한 서버에 복수로 인증서 설치 시 단일 도메인 인증서는 포트 공유 불가능
멀티 도메인	멀티 인증서에 등록된 도메인은 포트 공유가 가능 하므로 <Connector port> ~ </Connector port> 구문을 설치할 도메인 수량에 맞추어 설정해주시면 됩니다. 그 외 다른 내용은 동일합니다.
와일드카드 도메인	와일드카드 인증서는 모든 서브도메인을 사용할 수 있고, 포트 공유가 가능 하므로 <Connector port>~</Connector port> 구문을 도메인에 따라 추가해주시길 바랍니다. 그 외 다른 내용은 동일합니다.

③ SSL 인증서 설치

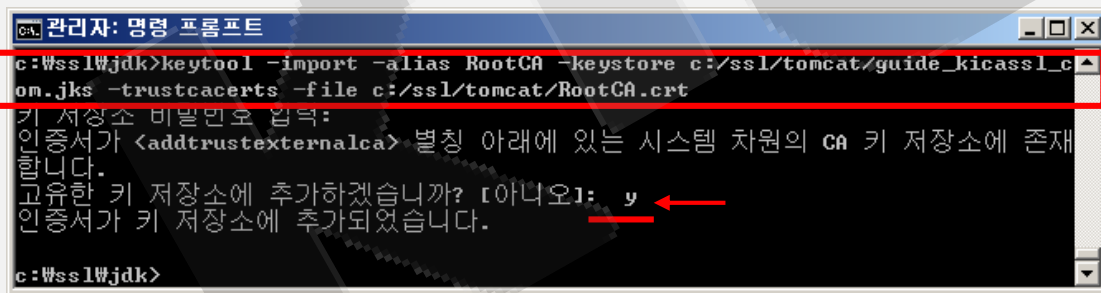
- 1. Keystore에 **루트 인증서 import** [import 권장 순서 : 루트 → 중개(번호 순서 상관없음) → SSL 인증서]

※ 유의사항 : SSL 인증서를 import 전에 모든 중개, 루트가 import 되어야 함. (유효성 검증 오류 발생)

- prompt> `keytool -import -alias [루트인증서 별칭] -keystore [CSR을 생성한 개인키가 있는 JKS 파일명 및 경로] -trustcacerts -file [루트인증서 파일명 및 경로]`

- (1) -import : 인증서를 Keystore에 import
- (2) -alias : import 인증서 별칭
- (3) -keystore : CSR을 생성한 개인키가 있는 Keystore 파일명 및 경로
- (4) -trustcacerts : 파일 종류가 인증서임을 명기
- (5) -file : import할 인증서 파일명 및 경로

[루트인증서 import]



```

CA 관리자: 명령 프롬프트
c:\ssl\jdk>keytool -import -alias RootCA -keystore c:/ssl/tomcat/guide_kicassl_c
on.jks -trustcacerts -file c:/ssl/tomcat/RootCA.crt
키 저장소 비밀번호 입력:
인증서가 <addtrustexternalca> 별칭 아래에 있는 시스템 차원의 CA 키 저장소에 존재
합니다.
고유한 키 저장소에 추가하겠습니까? [아니오]: y
인증서가 키 저장소에 추가되었습니다.
c:\ssl\jdk>
    
```

③ SSL 인증서 설치

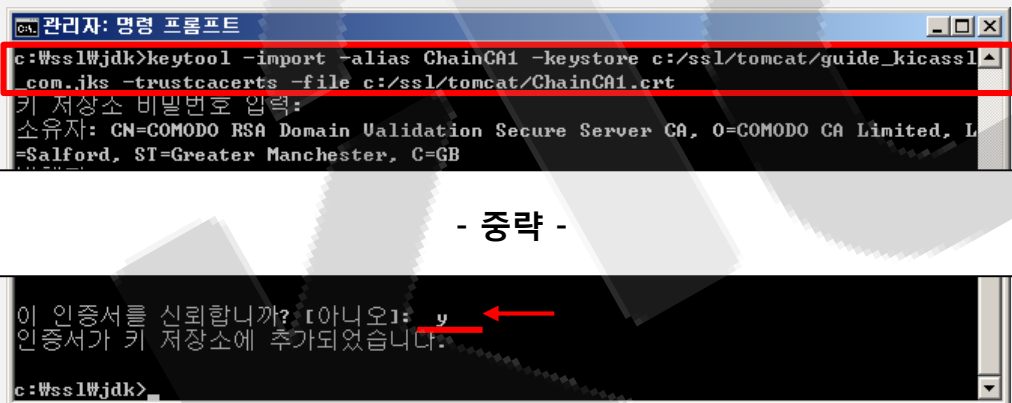
- 2. Keystore에 **중개 인증서 import** [import 권장 순서 : 루트 → 중개(번호 순서 상관없음) → SSL 인증서]

※ 유의사항 : SSL 인증서를 import 전에 모든 중개, 루트가 import 되어야 함. (유효성 검증 오류 발생)

- prompt> `keytool -import -alias [중개인증서n 별칭] -keystore [CSR을 생성한 개인키가 있는 JKS 파일명 및 경로] -trustcacerts -file [중개인증서n 파일명 및 경로]`

▶ Root 인증서 import와 동일하여 ChainCA1.crt, ChainCA2.crt로 "-file", "-alias"의 내용을 변경하여 import 합니다.

[ChainCA1 import]



다음 장 샘플 화면 계속 참고바랍니다.

③ SSL 인증서 설치

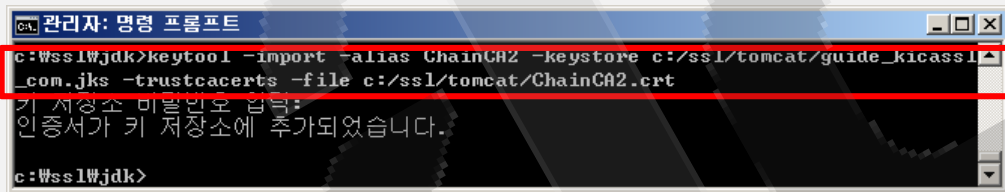
- 2. Keystore에 **중개 인증서 import** [import 권장 순서 : 루트 → 중개(번호 순서 상관없음) → SSL 인증서]

※ 유의사항 : SSL 인증서를 import 전에 모든 중개, 루트가 import 되어야 함. (유효성 검증 오류 발생)

- prompt> `keytool -import -alias [중개인증서n 별칭] -keystore [CSR을 생성한 개인키가 있는 JKS 파일명 및 경로] -trustcacerts -file [중개인증서n 파일명 및 경로]`

▶ Root 인증서 import와 동일하여 ChainCA1.crt, ChainCA2.crt로 "-file", "-alias"의 내용을 변경하여 import 합니다.

[ChainCA2/숫자 반복 import] 전송한 파일들 중에 ChainCA3까지 존재한다면 ChainCA3까지 해주셔야 합니다.



```
관리자: 명령 프롬프트
c:\WsslWjdk>keytool -import -alias ChainCA2 -keystore c:/ssl/tomcat/guide_kicassl_com.jks -trustcacerts -file c:/ssl/tomcat/ChainCA2.crt
키 저장소 미발견 오류:
인증서가 키 저장소에 추가되었습니다.
c:\WsslWjdk>
```

다음 장 샘플 화면 계속 참고바랍니다.

③ SSL 인증서 설치

- 3. Keystore에 **SSL 인증서 import** [import 권장 순서 : 루트 → 중개(번호 순서 상관없음) → SSL 인증서]

※ 유의사항 : SSL 인증서를 import 전에 모든 중개, 루트가 import 되어야 함. (유효성 검증 오류 발생)

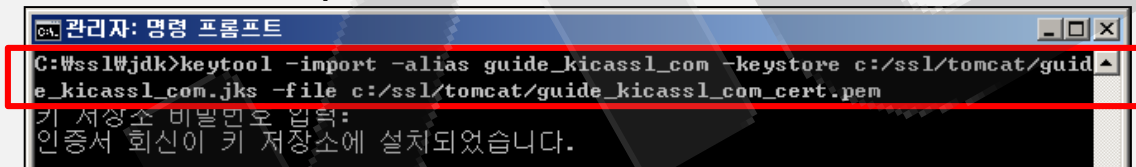
- prompt> `keytool -import -alias [생성한 개인키 별칭] -keystore [CSR을 생성한 개인키가 있는 JKS 파일명 및 경로] -file [SSL인증서 파일명 및 경로]`

※ 여기서 입력하는 "alias"는 본 문서 "①"에서 키스토어 생성 시 입력한 "개인키 별칭(예: guide_kicassl_com)"과 꼭 동일하여야 합니다.

만일, 개인키 별칭과 다르면 아래와 같은 메세지 표시가 안되며

또한 유효성 검증이 되지 않아 신뢰되지 않는 사이트로 표시됩니다.

[SSL 인증서 정상 import]



```
관리자: 명령 프롬프트
C:\WsslWjdk>keytool -import -alias guide_kicassl_com -keystore c:/ssl/tomcat/guide_kicassl_com.jks -file c:/ssl/tomcat/guide_kicassl_com_cert.pem
키 저장소 비밀번호 입력:
인증서 회신이 키 저장소에 설치되었습니다.
```

다음 장 샘플 화면 계속 참고바랍니다.

③ SSL 인증서 설치

- 3. Keystore에 **SSL 인증서 import** [import 권장 순서 : 루트 → 중개(번호 순서 상관없음) → SSL 인증서]
 ※ 유의사항 : SSL 인증서를 import 전에 모든 중개, 루트가 import 되어야 함. (유효성 검증 오류 발생)
 - prompt> `keytool -import -alias [생성한 개인키 별칭] -keystore [CSR을 생성한 개인키가 있는 JKS 파일명 및 경로] -file [SSL인증서 파일명 및 경로]`

※ 여기서 입력하는 "alias"는 본 문서 "①"에서 키스토어 생성 시 입력한 "개인키 별칭(예: guide_kicassl_com)"과 꼭 동일하여야 합니다.
 만일, 개인키 별칭과 다르면 아래와 같은 메세지 표시가 안되며
 또한 유효성 검증이 되지 않아 신뢰되지 않는 사이트로 표시됩니다.

[중개 또는 루트 인증서가 import 되지 않았을 때 발생하는 오류 화면]

```
관리자: 명령 프롬프트
C:\ssl\jdk>keytool -import -alias guide_kicassl_com -keystore c:/ssl/tomcat/guide_kicassl_com.jks -file c:/ssl/tomcat/guide_kicassl_com_cert.pem
키 저장소 비밀번호 입력:
keytool 오류: java.lang.Exception: 회신의 체인 설정을 실패했습니다.
```

[발급된 인증서와 개인키가 일치하지 않을 때 발생하는 오류 화면 (인증서 재발급 필요)]

```
관리자: 명령 프롬프트
C:\ssl\jdk>keytool -import -alias guide_kicassl_com -keystore c:/ssl/tomcat/guide_kicassl_com.jks -file c:/ssl/tomcat/guide_kicassl_com_cert.pem
키 저장소 비밀번호 입력:
keytool 오류: java.lang.Exception: 회신과 키 저장소의 공용 키가 일치하지 않습니다.
```

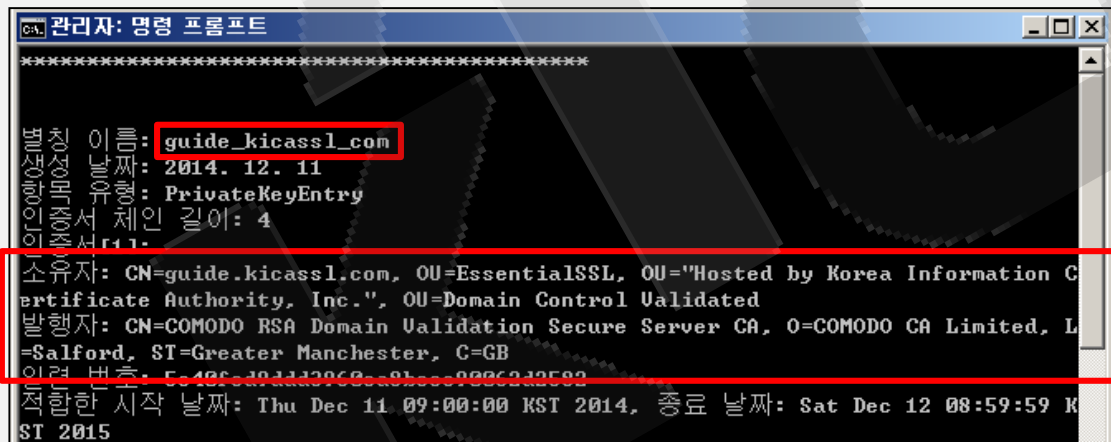
③ SSL 인증서 설치

• 4. Keystore의 import 상태 확인

- prompt> `keytool -list -keystore [확인할 JKS 파일명 및 경로] -v`

- (1) -list : Keystore에 import된 인증서 보기 옵션
- (2) -keystore : 확인할 Keystore 파일명 및 경로
- (3) -v : 인증서 정보 상세히 보기 옵션

※ 정상적으로 SSL 인증서가 import되어 Tomcat에 적용 사용가능한 JKS 상태 예제 [소유자와 발행자 정보가 같지 않아야 함]



```
관리자: 명령 프롬프트
*****
이름: guide_kicassl.com
날짜: 2014. 12. 11
유형: PrivateKeyEntry
서 체인 길이: 4
소유자: CN=guide.kicassl.com, OU=EssentialSSL, OU="Hosted by Korea Information Certificate Authority, Inc.", OU=Domain Control Validated
발행자: CN=COMODO RSA Domain Validation Secure Server CA, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB
적합한 시작 날짜: Thu Dec 11 09:00:00 KST 2014, 종료 날짜: Sat Dec 12 08:59:59 KST 2015
```

다음 장 샘플 화면 계속 참고바랍니다.

③ SSL 인증서 설치

• 4. Keystore의 import 상태 확인

- prompt> `keytool -list -keystore [확인할 JKS 파일명 및 경로] -v`

- (1) -list : Keystore에 import된 인증서 보기 옵션
- (2) -keystore : 확인할 Keystore 파일명 및 경로
- (3) -v : 인증서 정보 상세히 보기 옵션

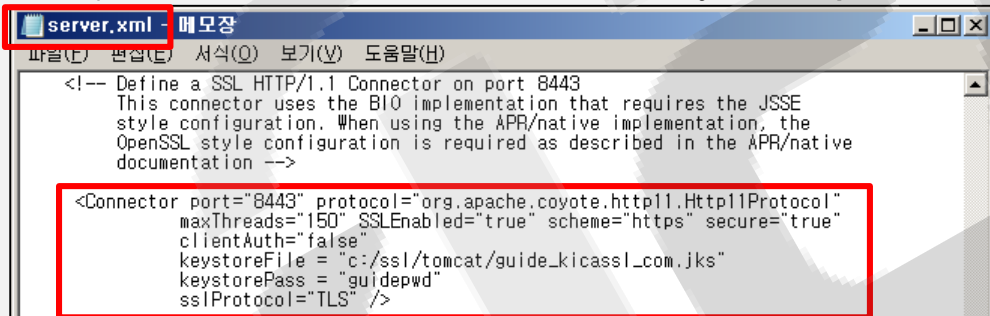
※ 정상적으로 SSL 인증서가 import되지 않은 JKS 상태 예제 [소유자와 발행자 정보가 같으므로 오류]

```

C:\> 관리자: 명령 프롬프트
*****
변환 이름: guide_kicassl.com
날짜: 2014. 12. 11
유형: PrivateKeyEntry
인증서 체인 길이: 1
인증서[1]:
소유자: CN=guide.kicassl.com, OU=SSL Team, O="Korea Information Certificate Authority, Inc", L=Sunnam-Si Bundang-Gu, ST=Gyeonggi-Do, C=KR
발행자: CN=guide.kicassl.com, OU=SSL Team, O="Korea Information Certificate Authority, Inc", L=Sunnam-Si Bundang-Gu, ST=Gyeonggi-Do, C=KR
일련 번호: 164083b5
적합한 시작 날짜: Wed Nov 26 18:34:00 KST 2014, 종료 날짜: Tue Feb 24 18:34:00 KST 2015
    
```

③ SSL 인증서 설치 [Tomcat v6.x, v7.x+ 공통, Keystore 사용]

- **server.xml** : 일반적으로 “Tomcat 홈/conf”하위에 위치
 - SSL 인증서 사용 설정 및 경로 설정
 - “Connect on port 8443” 구문 검색 후 아래와 같이 주석제거, **keystore**, **Https Port 정보 입력**



※ **server.xml** 설정 내용 (Tomcat 웹서버의 경우 인증서를 1개만 설치하여 사용하실 수 있습니다.)

443으로 변경하여 설정합니다. 만일 443이 아닐 경우 해당 도메인 https접속 시 포트번호까지 입력해 주셔야 합니다.

```
<Connector port="443[사용할 포트번호]" protocol="org.apache.coyote.http11.Http11Protocol"
    maxThreads="150" SSLEnabled="true" scheme="https" secure="true"
    clientAuth="false"
    keystoreFile="C:\ssl\ssl\tomcat\guide_kicassl_com.jks [앞 장에서 생성한 키스토어 파일]"
    keystorePass = "guidepwd [키스토어 비밀번호]"
    sslProtocol="TLS" />
```

③ SSL 인증서 설치 [Tomcat v6.x+ v7.x+ 공통, Keystore 사용]

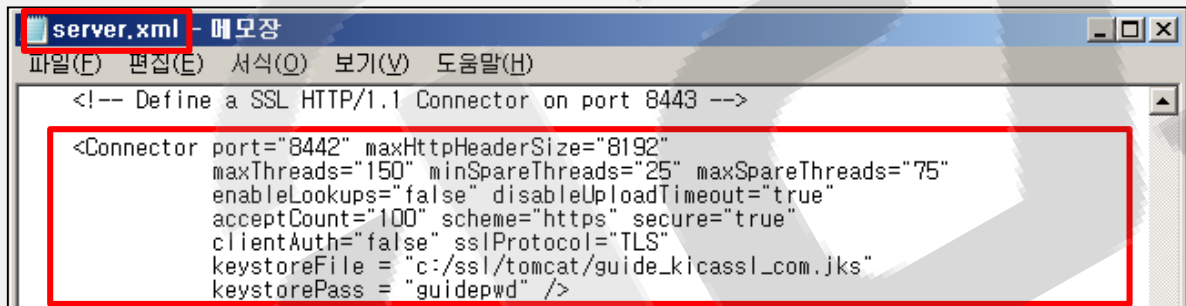
- server.xml : 일반적으로 "Tomcat 홈/conf"하위에 위치
 - 앞 장 설정 변경 후 데몬 기동 또는 https포트가 정상 실행이 안될 시 아래와 같이 Protocol 변경

※ 변경한 server.xml 설정 내용 (Tomcat 웹서버의 경우 인증서를 1개만 설치하여 사용하실 수 있습니다.)
443으로 변경하여 설정합니다. 만일 443이 아닐 경우 해당 도메인 https접속 시 포트번호까지 입력해주셔야 합니다.

```
<Connector port="443[사용할 포트번호]" protocol="HTTP/1.1"
    maxThreads="150" SSLEnabled="true" scheme="https" secure="true"
    clientAuth="false"
    keystoreFile="C:\ssl\ssl\tomcat\guide_kicassl_com.jks [앞 장에서 생성한 키스토어 파일]"
    keystorePass = "guidepwd [키스토어 비밀번호]"
    sslProtocol="TLS" />
```

③ SSL 인증서 설치 [Tomcat v5.x Keystore 사용]

- server.xml : 일반적으로 "Tomcat 홈/conf"하위에 위치
 - SSL 인증서 사용 설정 및 경로 설정
 - "Connect on port 8443" 구문 검색 후 아래와 같이 주석제거, keystore, Https Port 정보 입력



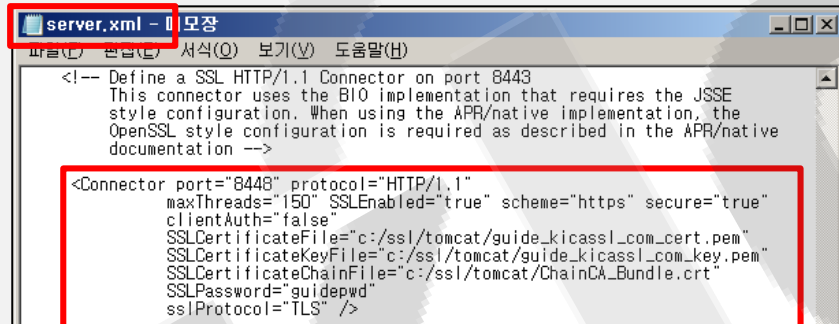
※ server.xml 설정 내용 (Tomcat 웹서버의 경우 인증서를 1개만 설치하여 사용하실 수 있습니다.)

443으로 변경하여 설정합니다. 만일 443이 아닐 경우 해당 도메인 https접속 시 포트번호까지 입력해주셔야 합니다.

```
<Connector port="443[사용할 포트번호]" maxHttpHeaderSize="8192"
  maxThreads="150" minSpareThreads="25" maxSpareThreads="75"
  enableLookups="false" disableUploadTimeout="true"
  acceptCount="100" scheme="https" secure="true"
  clientAuth="false" sslProtocol="TLS"
  keystoreFile="C:\ssl\ssl\tomcat\guide_kicassl_com.jks [앞 장에서 생성한 키스토어 파일]"
  keystorePass = "guidepwd [키스토어 비밀번호]" />
```

③ SSL 인증서 설치 [Tomcat v5.5+ APR(Apache Portable Runtime Native) 사용]

- **server.xml** : 일반적으로 “Tomcat 홈/conf”하위에 위치
 - SSL 인증서 사용 설정 및 경로 설정
 - **APR 모드로 사용 시 해당 Tomcat에 APR모드를 먼저 설정하여야 함(서버관리자 문의)**
 - APR 모드란 Apache 서버처럼 JKS(Keystore)대신 인증서 파일을 사용하는 방법입니다. (CSR생성 및 발급은 Apache 매뉴얼 참고)



※ **server.xml** 설정 내용 (Tomcat 웹서버의 경우 인증서를 1개만 설치하여 사용할 수 있습니다.)

443으로 변경하여 설정합니다. 만일 443이 아닐 경우 해당 도메인 https접속 시 포트번호까지 입력해주셔야 합니다.

```
<Connector port="443[사용할 포트번호]" protocol="HTTP/1.1"
maxThreads="150" SSLEnabled="true" scheme="https" secure="true"
clientAuth="false"
SSLCertificateFile="C:\ssl\ssl\tomcat\guide_kicassl_com_cert.pem [메일로 수신받은 인증서 ".pem"파일]"
SSLCertificateKeyFile="[CSR생성시 기입한 개인키파일]"
SSLCertificateChainFile="C:\ssl\ssl\tomcat\Chain_RootCA_Bundle.crt [메일로 수신받은 인증서 ".crt"파일]"
SSLPassword="guidepwd [키스토어 비밀번호]"
sslProtocol="TLS" />
```


③ SSL 인증서 설치

- “hosts” 파일에 ServerName과 IP 매핑 설정

※ ServerName 항목이 유효하기 위해서는 서버의 “hosts”파일의 내용에 SSL인증서를 적용할 도메인들에 대한 IP매핑 설정이 필요합니다.

- “hosts” 파일 경로

(가) Windows OS : [윈도우 설치 홈디렉토리]/system32/drivers/etc 내부 존재

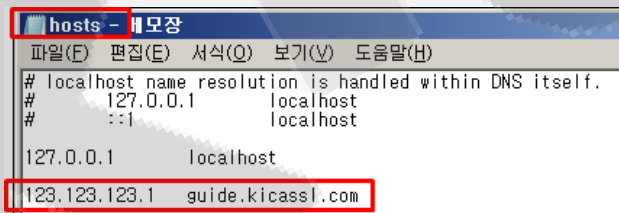
(나) Linux OS : /etc 내부 존재

- “hosts” 설정 추가 예제

“guide.kicassl.com” 에 대한 ip주소가 “123.123.123.1”이라면 hosts 파일에 “123.123.123.1 guide.kicassl.com” 을 추가합니다.

(사용하실 정보에 맞추어 입력해주시길 바랍니다.)

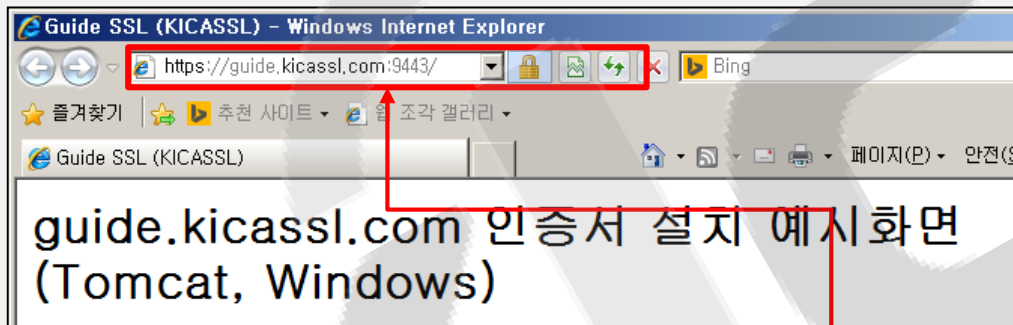
- hosts 설정 예제 화면



```
hosts - 모창
파일(F) 편집(E) 서식(Q) 보기(V) 도움말(H)
# localhost name resolution is handled within DNS itself.
#       127.0.0.1       localhost
#       ::1            localhost
127.0.0.1       localhost
123.123.123.1  guide.kicassl.com
```

④ SSL 인증서 설치 확인

- SSL 관련 설정 완료 후 Tomcat 웹서버 재기동
 - 만일, 재기동시 오류가 발생하신다면 SSL 오류 로그 또는 오류 로그 확인 부탁드립니다.
 - "https://신청한 도메인:포트" 으로 접속하여 자물쇠 표시 및 https 통신 확인



443포트는 기본포트이기 때문에 포트번호 생략 가능.
만일, 다른 포트를 사용시 포트번호를 꼭 입력해야 합니다.

만일, 접속이 안될 시 본 가이드 마지막 부분의 "SSL 설치 주의사항 및 자주 발생하는 설치 중 오류"를 확인해주시길 바랍니다.

⑤ SSL 암호화 통신 적용 예제

※ SSL인증서를 웹 서버에 설치한 후 **SSL암호화 통신(https 프로토콜)**이 가능하도록 웹 페이지에 적용하는 작업이 반드시 필요합니다.

- **전체 페이지**를 암호화하면 암호화 적용이 필요 없는 부분까지 암호화하여 부분 암호화 보다 서버에 부하를 줄 수 있습니다.
- **부분 페이지(로그인 및 회원가입 등)만 암호화**하면 전체 페이지 적용에 비해 서버 부하가 증가하는 것을 줄일 수 있습니다.

▶ SSL 암호화 통신을 위한 기본적인 변경 사항

(1) 웹페이지 소스 내부에 "http://" 호출 경로 및 링크 수정

SSL인증서의 적용은 아래와 같이 "http://"로 호출하는 부분을 "https://"로 변경하시길 바랍니다.

```
<a href="http://www.kicassl.com/" target="_blank">
```



```
<a href="https://www.kicassl.com/" target="_blank">  
또는 
```

※ 만일, SSL을 적용한 포트가 **default 포트인 443** 포트일 경우, 위와 같이 "https://"만 변경하지만 **443 이외의** **포트를 적용한 경우** 아래와 같이 **포트 번호**를 반드시 명시해 주셔야 합니다.

```
<a href="https://www.kicassl.com:444/" target="_blank">  
또는 
```

- “인증서와 개인키가 **keypair**(키 쌍)이 안 맞으면 인증서가 정상 로드 되지 않음.”
 - 발급 신청 시 기입한 **CSR**을 생성한 **개인키**만 발급된 인증서와 사용할 수 있음
 - 개인키를 여러 번 생성하였으면, 최종 신청 시 기입한 CSR을 생성한 개인키만 사용할 수 있습니다.
- “개인키가 발급한 **SSL 인증서**와 매칭 오류 시 **표시 메시지/로그**”
 - “키와 인증서가 매칭 되지 않습니다” 등과 같은 **매칭 오류 메시지가 로그/표시됨. (키워드 : matching)**
 - > CSR 생성 시 사용한 개인키 파일로 다시 설정하시거나, 현재 소유한 개인키 파일과 맞는 인증서로 재발급 하셔야 합니다.
 - “중개(체인)을 검증을 실패 하였습니다” 등과 같은 **체인 오류 메시지가 로그/표시됨. (키워드 : chain)**
 - > 중개 인증서 관련 설정 내용에 확인이 필요합니다.
 - 1) Keystore 등 import가 필요한 웹 서버는 중개인증서를 import 여부 확인
 - 2) 중개인증서 경로를 별도로 설정하는 웹 서버는 중개인증서 경로 및 파일 위치 확인
 - “개인키의 비밀번호가 맞지 않습니다.” 등과 같은 **비밀번호 오류 메시지가 로그/표시됨. (키워드 : private key, password, passphrase)**
 - > 입력하신 개인키 암호가 다르므로, 재발급이 필요합니다. (파일 오류 및 비밀번호 오류 사유)
- “**1개의 서버에서 여러 도메인(인증서) 사용시 주의사항**”
 - https(SSL)을 사용하는 포트는 설치한 인증서 수량과 같아야 합니다.
 - 2개의 인증서를 설치 시 2개의 각각 다른 포트가 필요함
 - **와일드카드 SSL인증서 (*.kicassl.com), 멀티도메인 SSL인증서**는 동일한 포트 공유가 가능한 SSL 인증서 입니다.
 - **멀티도메인 인증서 설치 후 인증서**에 도메인을 추가 신청 시 인증서는 재설치 해야 합니다.

- https 사용 포트를 “443”이 아닌 다른 포트를 지정하면 URL 입력 시 포트까지 입력해야 함.
 - [https://guide.kicassl.com:443] “443”포트는 기본 SSL 포트이므로 생략이 가능함
 - [https://guide.kicassl.com:8443] “8443”포트로 SSL 포트 설정 시 URL에 포트번호 필수 기입
 - 본 문서 있는 포트는 예제로 입력한 포트로 사용하시려는 포트 변경하시면 됩니다.
- https접속 시 SSL 인증서가 웹 서버에 설치한 SSL 인증서가 아닌 다른 SSL 인증서가 로드 되는 오류
 - 설치하신 웹서버로 직접 접속하여 어떤 인증서를 로드 했는지 확인 필요
 - > 웹 서버 IP주소로 https://123.123.123.123:443 으로 접속 후 표시되는 인증서 오류 화면에서 “계속 탐색” 클릭
 - 웹브라우저에 로드된 SSL 인증서 정보를 확인 합니다. 설치된 인증서가 표시된다면
 - L4, 방화벽 또는 웹 서버 앞 단에 장비에도 SSL 인증서 설치가 필요한지 확인이 필요합니다.
- 안드로이드 v5.0(롤리팝)+ 또는 구글 크롬 브라우저에서 https 접속이 안될 시
 - 웹 서버에 SSL Protocol 중 TLSv1.2와 TLSv1.1을 사용 가능하도록 수정하고 해당 웹 서버의 최신 보안패치를 설치 필요
 - > 2014년 말 SSLv3 Protocol 보안 취약성 발견으로 TLSv1.1이상 사용이 권고되어 해당 프로토콜 미지원시 접속이 안될 수 있습니다
- https 접속 시 딜레이가 길거나, 경고 메시지(“인증서 해지 목록을 확인 할 수 없습니다.”) 표시 오류
 - 사용자의 환경이 공용망이 아닌 경우, 외부 CRL 및 OCSP URL로 접속이 제한되어 있다면 브라우저가 SSL 인증서 관련 정보 탐색을 하지 못하여 발생
 - > 방화벽 등 네트워크 장비에서 관련 접속 URL(또는 IP) 및 port 를 open 하여 사용자가 원활히 접속하여 사용 할 수 있도록 작업 필요
 - (CRL, OCSP URL 정보는 인증서마다 다르므로 인증서 파일 상세 정보에서 “자세히”탭 내용 중 “CRL 배포 지점”, 기관 정보 액세스”에 기입된 URL을 확인하시길 바랍니다)

- 해당 도메인 접속 시 “유효하지 않은 인증서” 라는 표시 발생 시
 - 폐쇄망 등 특정 환경의 사용자만 발생할 시
 - > 중개인증서가 웹 서버에 설치의 문제가 있어서 사용자(접속자)에게 중개인증서를 전달해주지 못 할 때 발생할 수 있음
 - 중개인증서 본 가이드의 설치 부분을 확인해 주시길 바랍니다.
 - WIN XP, IE 8이하 등 낮은 버전 환경 또는 윈도우 업데이트를 하지 않은 사용자
 - > 사용자(접속자)의 환경에 루트인증서가 존재하지 않아 발생할 수 있음
 - 윈도우에 내장된 윈도우 업데이트를 통해 윈도우 업데이트를 하거나, 첨부한 RootCA.crt 파일을 직접 사용자PC에 수동 설치해야 합니다.
- 해당 도메인 접속 시 “만료된 인증서” 라는 표시 발생 시
 - 해당 도메인의 접속한 사용자 PC의 시간이 현재 시간인지 확인해주시길 바랍니다.
 - 해당 도메인에 설치된 인증서 정보창을 띄워 해당 인증서의 만료일을 확인해주시기 바랍니다.
 - > 도메인 인증서 갱신을 했는데도 발생한 경우, 방화벽 또는 L4 등 다른 장비에 인증서 설치가 필요한지 확인해주시길 바랍니다.
- 해당 도메인 접속 시 “폐기된 인증서” 라는 표시 발생 시
 - 인증서가 폐기 또는 해지된 경우 KICASSL에 전화 문의 해주시길 바랍니다..
- 추가 질문사항은 한국정보인증 KICASSL 웹사이트의 FAQ를 확인해주시길 바랍니다.
 - www.kicassl.com 링크

감사합니다

신뢰세상
A World of Trust

한국정보인증(주) SSL (Korea Information Certificate Authority, Inc.)

E-mail. webmaster@kicassl.com