Apache v2.2+ SSL 설치가이드

Windows, Linux 공통 문서

한국정보인증 KICASSL

자주 발생하는 문의 및 설치 오류 / 설치 결과 확인 방법

자주 발생하는 문의와 설치 오류 안내
설치 결과 확인 방법은

문서 마지막 장에 설명되어있습니다.

SSL 설치 중 오류 및 **SSL 설치 확인** 시 **참고 부탁 드립니다.**

목차

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]

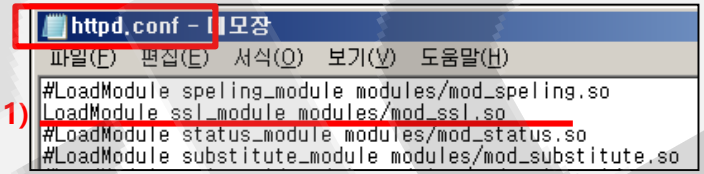
- 단일 / 멀티 / 와일드카드 도메인 SSL 인증서에 따른 설치 방법의 차이점

상품 종류	차이점
단일 도메인	**한 서버에 복수로 인증서 설치 시** 단일 도메인 인증서는 **포트 공유 불가능**하지만, **Apache 2.2.12 버전 이상**부터는 SNI 기능을 이용하여 **포트 공유 가능**합니다.
멀티 도메인	멀티 인증서에 등록된 도메인은 **포트 공유가 가능**하므로 **NameVirtualHost** 설정을 추가하시고, **<Virtual Host> ~ </Virtual Host> 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 **NameVirtualHost** 설정을 추가하시고, **<Virtual Host>~</Virtual Host> 구문을 도메인에 따라 추가해주시길 바랍니다.** 그 외 다른 내용은 동일합니다.

③ SSL 인증서 설치

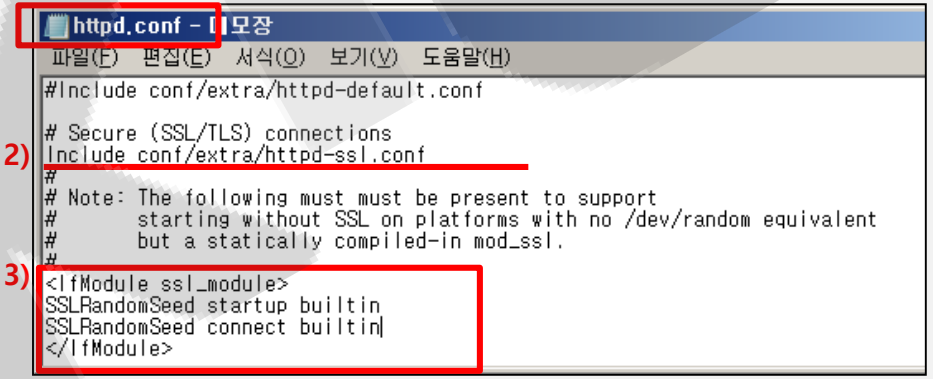
- **Apache Config 파일(httpd.conf) 수정**
  - **httpd.conf** : 일반적으로 "apache 홈/conf "하위에 위치
    (1) LoadModule - mod_ssl.so 주석 제거 확인
    (2) Include - httpd-ssl.conf 주석 제거 확인
    (3) <IfModule ssl_module> ~ </IfModule> 주석 제거 확인

1)



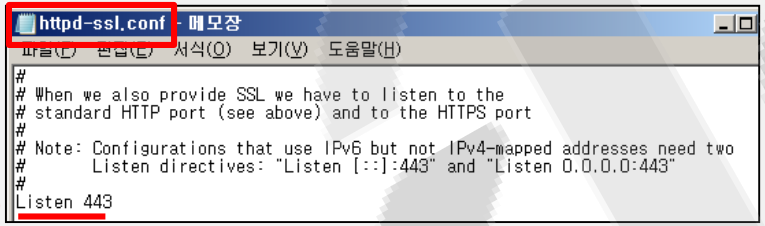
2)

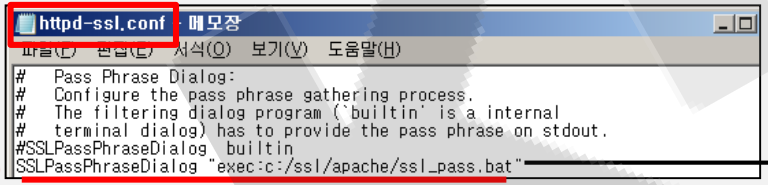
3)



③ SSL 인증서 설치

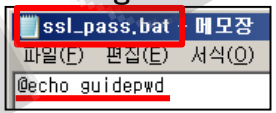
- **Apache Config 파일(httpd-ssl.conf) 수정**
  - **httpd-ssl.conf** : 일반적으로 "apache 홈/conf/extra "하위에 위치 (**앞장**에서 include한 ssl.conf파일)
    (1) Listen 포트 : SSL 사용 포트 설정 (default 포트는 443입니다)
    - 다른 포트로 변경하셔도 되며, 지정하신 포트가 방화벽 등에 차단 포트 인지 확인해주시길 바랍니다
    (2) @echo 비밀번호 : **Windows의 경우** 반드시 SSL 인증서 개인키 비밀번호 자동 로드 포함 (ssl_pass.bat), **Linux의 경우 (ssl_pass.sh)**

1)


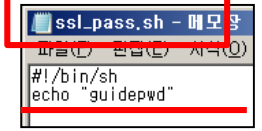
2)


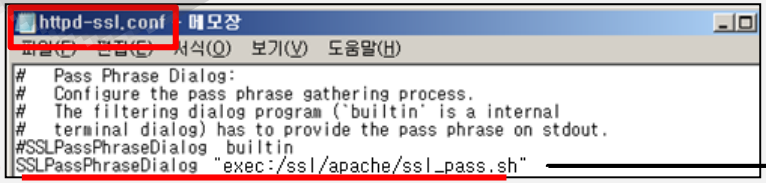
Windows 일 시

Windows : 비밀번호 로드 파일 내용



Linux : sh파일로 제작



2)


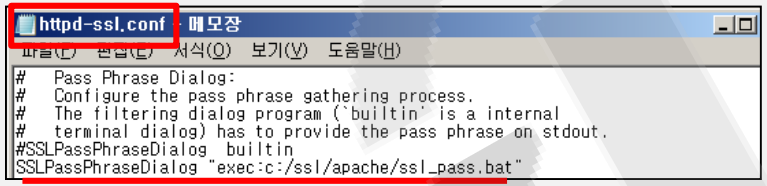
Linux 일 시

해당 .sh파일은 chmod 700 으로 파일권한 변경을 해야 합니다.

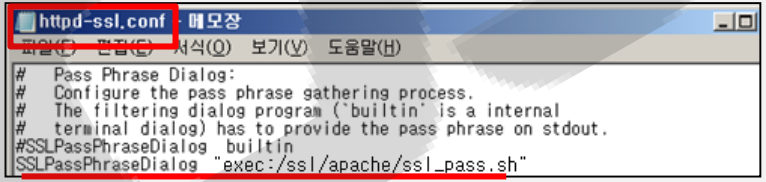
다음 장 샘플 화면 계속 참고바랍니다.

③ SSL 인증서 설치

- **주의사항** - Apache Config 파일(httpd-ssl.conf) 수정
  - Apache Windows 버전의 경우 **꼭 SSLPassPhraseDialog를 설정해야합니다.**
    만일, Builtin으로 되어있을 경우 오류 발생, 꼭 주석처리 필요 - 기동시 오류 발생
  - Apache는 Linux계열만 기동 시 비밀번호를 입력할 수 있음



Windows>일 시 반드시 SSLPassPhraseDialog는 주석처리



Linux>일 시 SSLPassPhraseDialog builtin : 비밀번호 수동입력
SSLPassPhraseDialog "exec~~" : 비밀번호 자동입력

③ SSL 인증서 설치

- **Apache Config 파일(httpd-ssl.conf) 수정**
  - **httpd-ssl.conf** : 일반적으로 "apache 홈/conf/extra "하위에 위치 (**앞장**에서 include한 ssl.conf파일)
    (3) Virtual Host 설정
    - Virtual Host, SSLEngine on, SSLProtocol, SSLCertificateFile, SSLCertificateKeyFile, SSLCertificateChainFile

※ httpd-ssl.conf Virtual Host 설정 내용 (단일 도메인 인증서, 멀티/와일드카드 인증서는 설정하는 도메인의 VirtualHost를 추가)

```
NameVirtualHost *:443   # IP기반일 시 제거

 <VirtualHost *:[SSL 적용 포트 (ex : 443)]>
   DocumentRoot [http 설정과 동일한 디렉토리]
   ServerName [해당 서버의 도메인 (ex : guide.kicassl.com)]
   ServerAdmin [서버 관리자 정보 (ex : webmaster @ kicassl.com)]
   ErrorLog [에러로그를 저장할 경로]/ssl_error_log
   TransferLog [에러로그를 저장할 경로]/ssl_access_log
   ......
   SSLEngine On
   #설명 : 발급받은 인증서 경로와 파일명을 지정합니다.
   SSLCertificateFile "경로/인증서파일" [ex : 도메인명_cert.pem]
   ......
   SSLCertificateKeyFile "경로/개인키파일" [ex : 도메인명_key.pem]
   ......
   SSLCertificateChainFile "경로/Chain_RootCA_Bundle.crt"
   ......
</VirtualHost>
```

③ SSL 인증서 설치

- **Apache Config 파일(httpd-ssl.conf) 수정**

√ 멀티/와일드카드 인증서 / 싱글 인증서 여러 개를 동일 포트에 설정 Tip

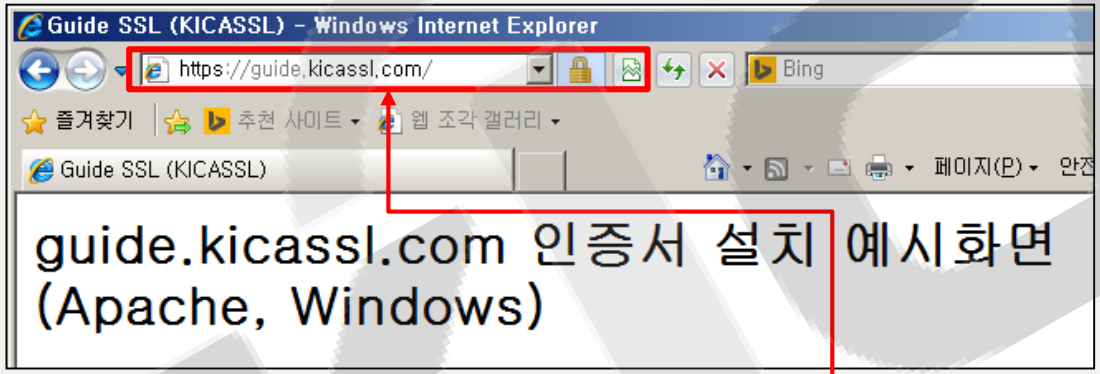
- **나머지 도메인에 대한 Virtual Host 설정은,** 기존 완성한 하나의 <VirtualHost> 블록을 복사한 후 **DocumentRoot, ServerName, ServerAdmin, ErrorLog, TransferLog 항목**만 적절하게 수정하여 주시면 됩니다.
- 동일 포트로 설정하는 경우, Virtualhost 바깥쪽에 **NameVirtualHost 옵션**을 추가하여야 합니다.
  (예 : NameVirtualHost *:443)

```
NameVirtualHost *:443

<VirtualHost *:443>
    DocumentRoot "C:₩Program Files₩Apache24₩test"
    ServerName *.kicassl.com
    ServerAlias test.kicassl.com
    SSLEngine on
    ...
    [설정 내용]
    ...
</VirtualHost>
<VirtualHost *:443>
    DocumentRoot "C:₩Program Files₩Apache24₩testsite2"
    ServerName *.kicassl.com
    ServerAlias testsite2.kicassl.com
    SSLEngine on
    ...
    [설정 내용]
    ...
</VirtualHost>
```

④ SSL 인증서 설치 확인

- **SSL 관련 설정 완료 후 Apache 웹서버 재기동**
  - **만일, 재기동시 오류가 발생하신다면 SSL 오류 로그 또는 오류 로그 확인 부탁 드리겠습니다.**
  - "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 작업**이 반드시 필요합니다.

- **전체 페이지를** 암호화하면 **암호화 적용이 필요 없는 부분까지 암호화하여 부분 암호화 보다 서버에 부하를 줄 수 있습니다.**
- **부분 페이지(로그인 및 회원가입 등)만 암호화하면 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"><img src="http://www.kicassl.com/images/logo.gif">
```

↓

```
<a href="https://www.kicassl.com/" target="_blank"><img src="https://www.kicassl.com/images/logo.gif">
또는 <img src="/images/logo.gif (상대 경로)">
```

※ 만일, SSL을 적용한 포트가 **default포트인 443 포트**일 경우, 위와 같이 **"https://"**만 변경하지만 **443 이외의 포트를 적용한 경우 아래와 같이 포트 번호를 반드시 명시해 주셔야 합니다.**

```
<a href="https://www.kicassl.com:444/" target="_blank"><img src="https://www.kicassl.com:444"/images/logo.gif">
또는 <img src="/images/logo.gif (상대 경로)">
```

SSL 설치 주의사항 및 자주 발생하는 설치 중 오류

- **"인증서와 개인키가 keypair(키 쌍)이 안 맞으면 인증서가 정상 로드 되지 않음."**
  - **발급 신청 시 기입한 CSR을 생성한 개인키만 발급된 인증서와 사용할 수 있음**
    - 개인키를 여러 번 생성하였으면, 최종 신청 시 기입한 CSR을 생성한 개인키만 사용할 수 있습니다.

- **"개인키가 발급한 SSL 인증서와 매칭 오류 시 표시 메세지/로그"**
  - **"키와 인증서가 매칭 되지 않습니다"** 등과 같은 **매칭 오류 메세지가 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 메세지가 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 메세지가 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 SSL인증서는 동일한 포트 공유가 가능한 SSL 인증서 입니다.**
    - 멀티도메인 인증서 설치 후 인증서에 **도메인을 추가 신청 시 인증서는 재설치 해야 합니다.**

SSL 설치 주의사항 및 자주 발생하는 설치 중 오류

- **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 포트로 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://아이피:포트로 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)

SSL 설치 주의사항 및 자주 발생하는 설치 중 오류

- **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㈜ SSL (Korea Information Certificate Authority, Inc.)

E-mail. Webmaster_@_kicassl.com