SSL인증서 설치 매뉴얼
(Apache)

백업된 인증서 설치

- 본 문서에 안내된 버전 이외의 다른 버전을 사용하시는 경우 안내 내용과 차이가 있을 수 있습니다.
- 본 문서는 기본적인 참고용 자료이며, 구성환경에 따라 안내 내용과 차이가 있을 수 있습니다.
- 본 문서는 서버 담당자를 기준으로 작성 되었습니다.
- 웹 서버 인증서를 설치할 서버 담당자에게 전달하여 주시기 바랍니다.

** 인증서 설치 전 확인사항 **

인증서 설치시 SSL관련 설정은 기존 apache 1.x 에서는 httpd.conf 파일에서 해주었으나
Apache 2.x 에서는 ssl.conf, apache 2.2x 에서는 httpd-ssl.conf 파일에서 설정해 주시면 됩니다.

참고1. Apache의 경우 기본적으로 mod_ssl 모듈이 설치되어 있어야 합니다. 참고

2. Windows 계열의 경우 설치방법이 상이할 수 있으니 참고하시기 바랍니다.

처음 Apache 설치(compile)시 mod-ssl 의 활성화를 위해서 (--enable-ssl)를 추가시켜줘야 합니다.

Mod_SSL 설치 확인($ /usr/local/apache/bin/httpd –l)

```
[root@168 bin]# ./httpd -l
Compiled in modules:
  core.c
  mod_access.c
  mod_auth.c
  mod_include.c
  mod_log_config.c
  mod_env.c
  mod_setenvif.c
  mod_ssl.c
```

1. 인증서 파일 저장

E-Mail 로 전달된 인증서 파일(cert.pem key.pem name-Chain.pem)을 임의의 폴더에
저장합니다.

설정하기 전 기존의 설정파일을 반드시 백업하여 주시길 바랍니다.

2. 설정파일 수정(httpd.conf)

설정파일을 열어서 다음과 같이 내용을 수정하십시오.

LoadModule ssl_module modules/mod_ssl.so --> SSL 모듈 추가 (mod_ssl.c 가 없을 경우)

Include conf/extra/httpd-ssl.conf --> SSL설정파일을 include

** 주석처리가 되어 있다면 주석제거

3. 설정파일 수정(ssl.conf 또는 httpd-ssl.conf)

3-1. 설정파일을 열어서 다음과 같이 VirtualHost 의 내용을 수정하십시오.

- **Apache 1.x 는 httpd.conf**
- **Apache 2.0 은 ssl.conf**
- **Apache 2.2 이상은 httpd-ssl.conf**
- **Apache 2.4 는 httpd-ssl.conf**

**** Tomcat, Weblogic 등의 WAS연동시 해당 Module부분을 추가 설정해주셔야 합니다.**

Listen 443

<VirtualHost _default_:443>
DocumentRoot "/xxx/html"
ServerName www.xxx.co.kr
ServerAdmin admin@xxx.co.kr
SSLEngine on

SSLProtocol all -SSLv2 -SSLv3
SSLCipherSuite HIGH:MEDIUM:!SSLv2:!PSK:!SRP:!ADH:!AECDH

SSLCertificateFile /usr/local/apache/conf/ssl/cert.pem (인증서파일)
SSLCertificateKeyFile /usr/local/apache/conf/ssl/key.pem (키 파일)
SSLCACertificateFile /usr/local/apache/conf/ssl/Name-Chain.pem (체인인증서파일)

➔ 체인인증서 파일명은 첨부해 드리는 파일명으로 수정하여 적용 부탁 드립니다.

3-2. 아파치 재구동

$ ./apachectl startssl(apache 2.2는 ./apachectl start)

```
[root@localhost apache2]# cd bin/
[root@localhost bin]# ./apachectl stop
[root@localhost bin]# ./apachectl start
Apache/2.2.21 mod_ssl/2.2.21 (Pass Phrase Dialog)
Some of your private key files are encrypted for security reasons.
In order to read them you have to provide the pass phrases.

Server www.example.com:443 (RSA)
Enter pass phrase:

OK: Pass Phrase Dialog successful.
[root@localhost bin]#
```

4. 설정파일 수정(다수 인증서 설정)

4-1. 환경설정 (Ex. www.test.com, login.test.com)

Listen 443
Listen 444 ➔ Listen 포트 추가설정

<VirtualHost IP:443>
DocumentRoot "/xxx/1.html"
ServerName www.test.com
ServerAdmin admin@xxx.co.kr
SSLEngine on

SSLProtocol all -SSLv2 -SSLv3
SSLCipherSuite HIGH:MEDIUM:!SSLv2:!PSK:!SRP:!ADH:!AECDH

SSLCertificateFile /usr/local/apache/conf/ssl1/cert.pem (인증서파일)
SSLCertificateKeyFile /usr/local/apache/conf/ssl1/key.pem (키 파일)
SSLCACertificateFile /usr/local/apache/conf/ssl1/Name-Chain.pem (체인인증서파일)

<VirtualHost IP:444>
DocumentRoot "/xxx/2.html"
ServerName login.test.com
ServerAdmin admin@xxx.co.kr
SSLEngine on

SSLProtocol all -SSLv2 -SSLv3
SSLCipherSuite HIGH:MEDIUM:!SSLv2:!PSK:!SRP:!ADH:!AECDH

SSLCertificateFile /usr/local/apache/conf/ssl2/cert.pem (인증서파일)
SSLCertificateKeyFile /usr/local/apache/conf/ssl2/key.pem (키 파일)
SSLCACertificateFile /usr/local/apache/conf/ssl2/Name-Chain.pem (체인인증서파일)

4-2. 아파치 재구동

$ ./apachectl startssl(apache 2.2는 ./apachectl start)

**** 각 도메인 별로 발급된 싱글 도메인 인증서는 단일 IP환경에서 같은 포트를 사용할 수 없습니다.**
(멀티인증서, Wildcard인증서는 동일한 포트로 설정 가능합니다.)

5. 인증서 Port LISTEN 확인

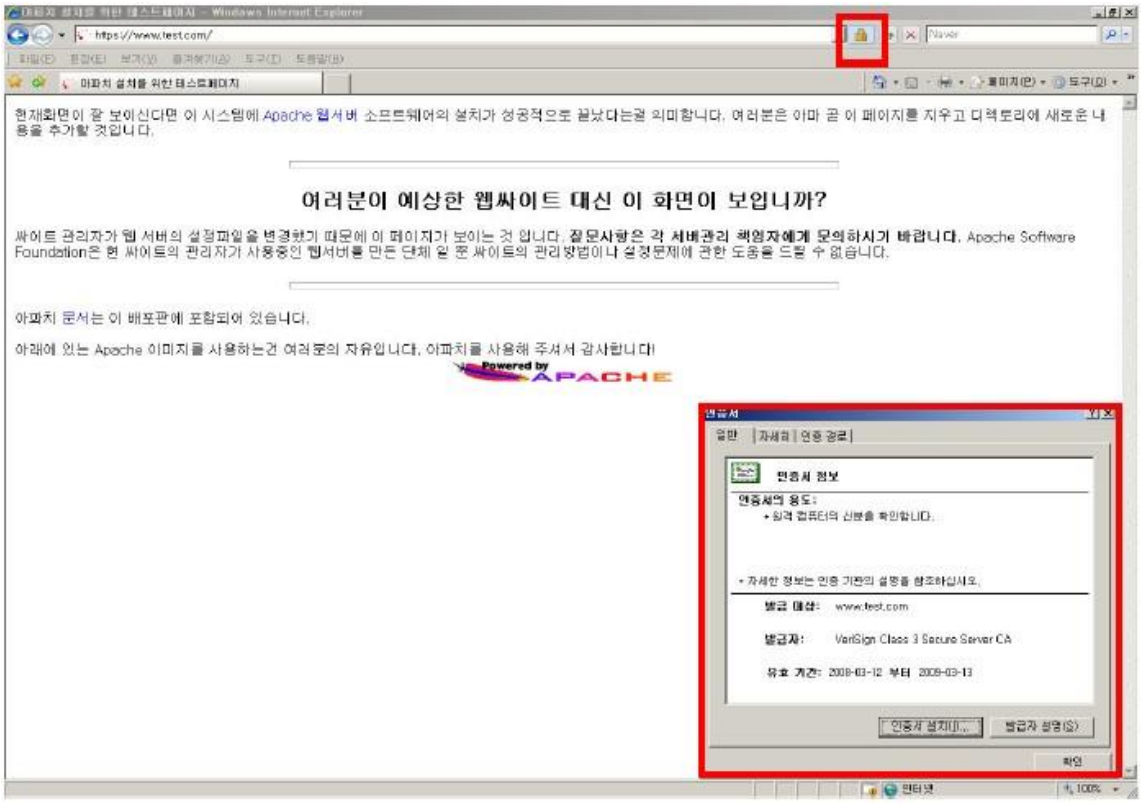
```
[root@168 bin]# netstat -na | grep 443
tcp        0      0 :::443                      :::*                        LISTEN

unix  3      [ ]         STREAM     CONNECTED     543443 /tmp/orbit-root/linc-ca4-0-67
4efd6510ec
[root@168 bin]# netstat -na | grep 444
tcp        0      0 :::444                      :::*                        LISTEN
```

6. 웹페이지에서 인증서 설치 확인

- https://URL 로 확인

- 443포트를 제외한 다른 포트로 설정하였을 경우 https://URL:포트 로 확인



7. 인증서 관리

인증서 파일을 분실하거나 비밀번호를 잊어버릴 경우 인증서 파일을 재발급 받아야 합니다.

재발급 시 재품에 따라 재발급되는 시간이 3일이상 걸릴 수도 있으니 인증서 파일과 관련된 정보를 관리하시길 바랍니다.

*** SSL인증서 적용 방법 ***

기본적으로 SSL 적용 방법은 소스코드에서 액션을 취하는 Page(링크 걸린 페이지주소)를 http://에서 https:// 로 바꿔주어야 합니다. (https://로 통신시에만 SSL 암호화적용)

이와 같이 적용시 절대경로로 https://를 호출해 와야 하며, 이하 소스상에 있는 파일들은 절대경로(or 상대경로)로 주셔도 상관없습니다.
(로그인, 회원가입, 아이디 찾기, 회원정보수정 등등 개인정보가 들어가는 Page에 적용)

Ex)

*** SSL인증서 적용 방법 ***

1. 보안 Page에 SSL 적용하기(부분적용 예시)

- 전체 Page 적용방법의 경우, 약간의 속도저하 또는 https://로의 소스변경의 불편함이 있으므로 개인정보가 들어가는 Page(ex. 로그인, 회원가입)에서만 적용시키시길 권장해 드립니다.

- 로그인 Page 구성 파일에 아래와 같이 수정(예시1)

<ex. 로그인 Action 클릭시>


```
.....(생략).....
<h2 class="hidden_phrase">로그인</h2>
<form name="login" id="login" method="post" action="https://logins.crosscert.com
/login/login.cgi">
<input type="hidden" name="url" value="http://www.crosscert.com/?t_top=login" />
<input type="hidden" name="pw" value="" />
<fieldset>
.....(생략).....
```

이와 같이 개인정보 입력 Page(ex. 로그인, 회원가입등)에서 Action시 https:// 가 호출되게 수정하면 사용자의 ID, PW 등이 보안통신 적용 됩니다.

로그인이 완료된 후, 메인 Page로 돌아올 때는 http://로 적용해 주셔도 됩니다.
(개인정보 필요한 Page만 적용)

참고1. 로그인 입력 Page에서부터 https://로 적용해주셔도 상관없습니다.(자물쇠 표시 확인가능)

참고2. '경고창' 발생시 '보안경고메시지 해결 방법 매뉴얼'을 참조해 주시기 바랍니다.

*** SSL인증서 적용 방법 ***

2. 전체 Page에 SSL 적용하기(전체적용 예시)

- index.html 파일에 아래와 같이 수정(예시1)

```
<head>
<script>
var url_1 = window.location;
var url_2 = "http://(도메인)/";
if (url_1 == url_2) window.location = "https://(도메인)/";;
</script>
</head>
```

- index.html 파일에 아래와 같이 수정(예시2)

```
<meta http-equiv="refresh" content="0;url=https://(도메인)">
```

위와 같이 전체 Page에 적용 시 https:// 로 바로 리다이렉션 되며, 이후 Page가 상대경로로 되있을 경우 계속해서 https:// 보안통신이 적용됩니다.

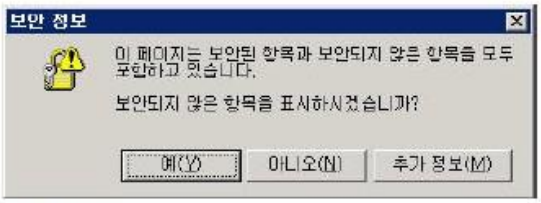
참고1. 전체 Page를 https:// 로 적용 시 약간(약 5%정도)의 속도저하가 있을 수 있습니다.

참고2. "보안된 항목과 보안되지 않는 항목을 ..." 의 경고창이 뜰 수 있습니다.

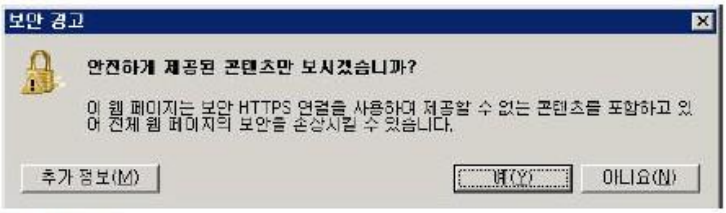
- 이 경우는 메인 Page에 http:// 와 https:// 가 공존하기 때문에 모두 https:// 로 소스변경
- 자바스크립트, 플래쉬 등의 데이터도 모두 https:// 로 변경

*** 보안경고 메시지 해결 방법 ***

1. 보안 정보(경고)창



(IE 6버전)



(IE 7,8버전)

원인 : 인터넷 익스플로러에서 https://URL 접속 시 메인 페이지 및 해당 페이지 소스상에서 http:// 호출되는 데이터 즉, **보안 되지 않은 항목(http://)**때문에 인터넷 익스플로러가 사용자에게 보여주는 메시지입니다.

해결 방법

해당페이지에 http://로 되있는 소스를 모두 **https://로 변경.**

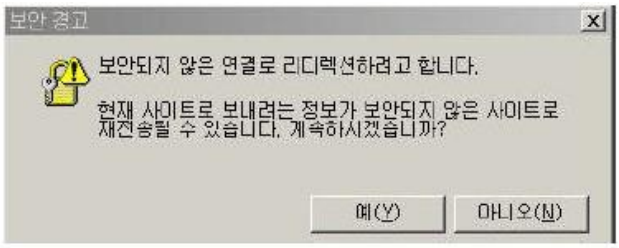
또한 플래쉬가 있는 경우 소스상에서 http://download.macromedia.com/~~/*.cab

→ https:// 변경.

다른 서버에서 http://절대경로 호출되는 이미지, 헤더파일등등이 있는 경우

→ 해당되는 파일을 웹 서버 홈디렉토리에 하위에 경로를 통해서 호출 또는 다른 서버쪽에도 인증서 설치 후 https://절대경로 로 호출

2. 보안 정보(리디렉션)창



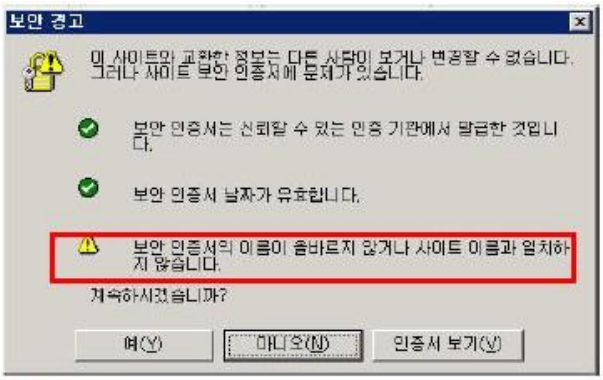
원인 : 예를 들어, https://URL/login.jsp로 접속 시 로그인 처리 프로세스 과정 혹은 소스상에서 직접적으로 **http://리턴URL** 주소를 넘겨줄 때 나타나는 **경고메시지** 입니다.

해결방법

http://리턴URL를 meta 태그 혹은 JavaScript를 통해서 Return url를 설정 해주시면 됩니다.

*** 보안경고 메시지 해결 방법 ***

3. 인증서 발급주소와 실제 접속 site 주소가 상이한 경우

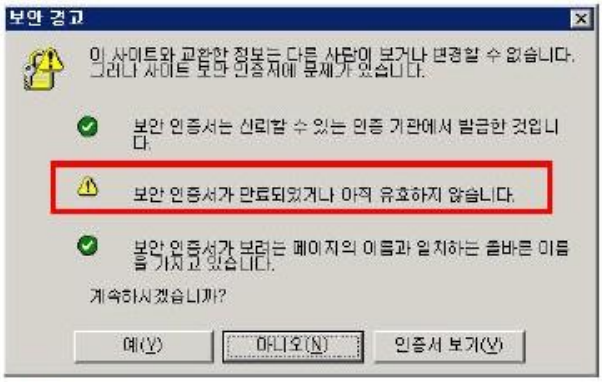


(IE 6버전)

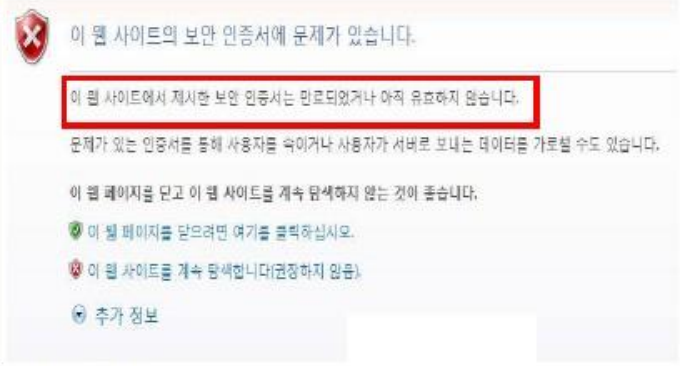
(IE 7,8버전)

www.crosscert.com 으로 인증서를 발급 받아 설치한 후 실제 적용은 login.crosscert.com으로 걸어두는 경우와 같이 인증서를 발급 받은 주소와 실제로 접속한 주소가 다른 경우에 위와 같은 경고 창이 나오게 됩니다.

4. 인증서가 유효하지 않은 경우



(IE 6버전)



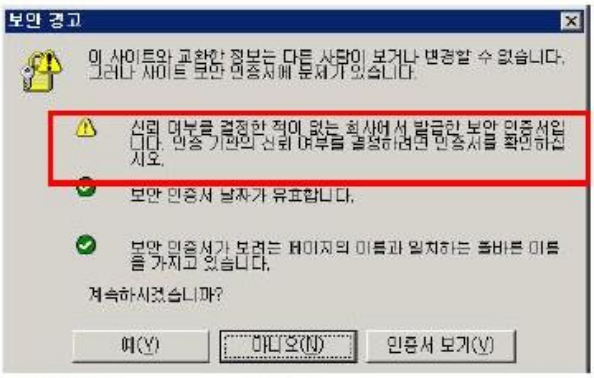
(IE 7,8버전)

인증서는 유효기간을 가지고 있는데, 이 기간이 지난 인증서를 계속 설치해 두는 경우에 나오는 경고 창 입니다. 인증서를 새로 발급 받아서 유효기간을 갱신하셔야 합니다.

참고1. 해당 PC의 현재시간이 정상적으로 보이는지 확인해 주시기 바랍니다.
참고2. '인증서 보기' – '인증 경로' 에서 중간부분 X 표시가 되어있다면 '체인인증서' 를 설정해주시기 바랍니다.

*** 보안경고 메시지 해결 방법 ***

3. 인증서 발급주소와 실제 접속 site 주소가 상이한 경우



(IE 6버전)

(IE 7,8버전)

이 경우는 웹 서버 인증서를 발급한 인증기관을 웹 브라우저가 인식하지 못하는 경우로써, 브라우저에는 기본적으로 신뢰할 수 있는 인증기관 리스트가 내장되어 있는데 그 리스트에 없는, 즉, 신뢰할 수 없는 인증기관에서 발급된 인증서를 설치한 경우에 발생하는 경고 창입니다.

웹 서버에서 자체적으로 만든 인증서를 설치한 경우 또는 Trial 인증서를 설치할 경우와 체인인증서가 설치되어 있지 않은경우에 가장 많이 생깁니다.

*** 인증서 설치 후 오류발생 시 확인사항 ***

1. 웹 방화벽 또는 장비에 인증서 설치 여부 확인

   - 기존에 설치된 인증서가 만료되어 새로운 인증서로 갱신하였으나 웹 서버나 로컬에서는 인증서가 교체된 것으로 확인되지만, 외부에서 접속하였을 때 기존의 인증서로 보이는 경우 확인 필요

2. 웹 방화벽 또는 장비에 설정포트 오픈 여부 확인

   - 서버에서 443포트가 Listen되고 외부에서 https://url로 접속 시 통신이 되지 않을 경우 웹 방화벽이나 장비의 설정포트 오픈 여부를 확인

3. load balancing일 경우 해당 모든 서버에 인증서 설치 여부 확인

4. 사용자들의 시스템 날짜를 체크

   - 대다수의 사용자들은 정상적으로 접속이 되나 일부 사용자에게서 보안경고가 발생할 경우 확인 필요

한국전자인증 기술지원팀 Tel : 02-1588-1314(3) / Fax : 02-2055-3732
e-Mail : vcs@crosscert.com