SSL인증서 설치 매뉴얼
(Oracle 12c)

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.

1. 인증서 저장(ewallet.p12 cwallet.p12)

E-mail로 수신된 인증서 파일을 해당 서버의 임의의 폴더에 저장

ewallet.p12 → 인증서 파일 cwallet.sso → 자동 로그인 파일

2. 설정파일 수정(httpd.conf)

인증서를 설치할 알맞은 인스턴스 경로의 설정파일 확인

(ex : C:\Oracle\Middleware\Oracle_Home\user_projects\domains\base_domain\config\fmwconfig\components\OHS\instances\ohs1)

설정 파일 내용 중 다음 설정 구문 확인 (주석되어 있을 경우 주석해제)

LoadModule ossl_module "${PRODUCT_HOME}/modules/mod_ossl.so"

Include "ssl.conf"

3. 설정파일 수정(ssl.conf)

설정 파일 내용 중 다음 설정 구문 확인

Listen 443 : SSL 적용 포트 지정

SSLProtocol nzos_Version_1_0 nzos_Version_1_1 nzos_Version_1_2

: 적용할 SSL/TLS Protocol 버전 지정 (예제 설정은 TLS 1.0~TLS1.2 까지 입니다.)

SSLCipherSuite SSL_RSA_WITH_RC4_128_MD5,SSL_RSA_WITH_RC4_128_SHA,...

: 적용할 암호화 알고리즘 지정 (설정 가능한 범위 안내 링크를 참고 부탁 드립니다.)

(http://docs.oracle.com/middleware/1212/webtier/HSADM/directives.htm#HSADM1016)

SSLWallet "${ORACLE_INSTANCE}/config/fmwconfig/components/${COMPONENT_TYPE}/instances/${COMPONENT_NAME}/keystores/default"

: 해당 인스턴스에 설정할 인증서 파일 위치 지정

4. 인증서 파일 저장

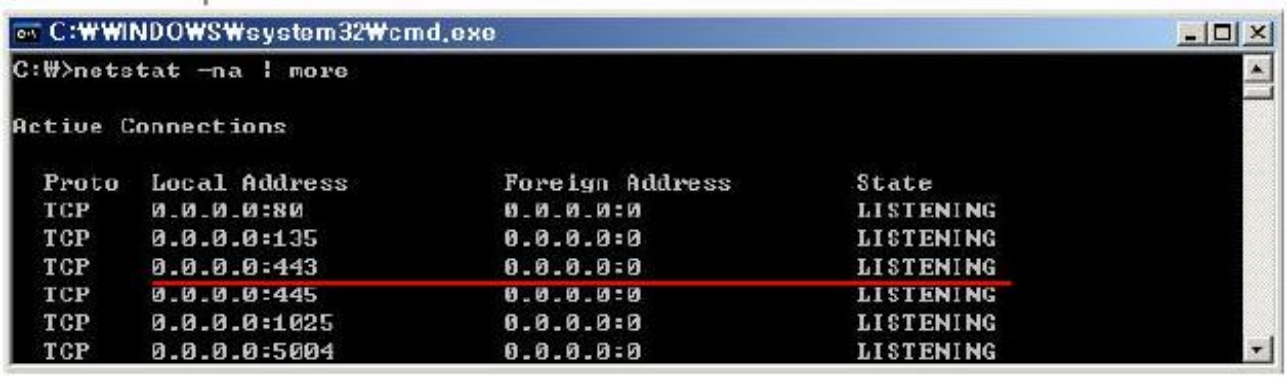
ssl.conf 에서 확인된 인증서 파일 경로에 ewallet.p12, cwallet.sso 파일 이동

예제 경로 : ${ORACLE_INSTANCE}/config/fmwconfig/components/${COMPONENT_TYPE}/instances/${COMPONENT_NAME}/keystores/default"

5. OHS 재구동

6. 인증서 Port LISTEN 확인

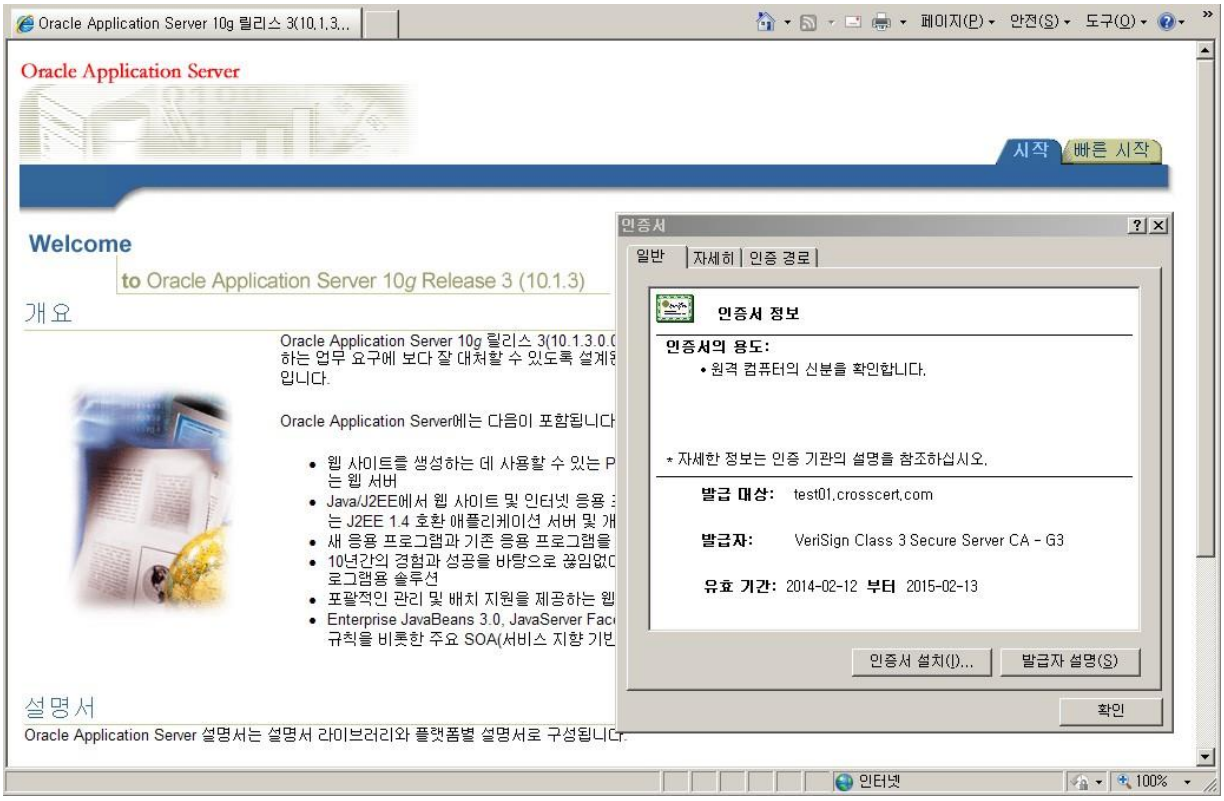
$ netstat –na | more



7. 웹 페이지에서 인증서 설치 확인

- https://URL 로 확인

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



** 브라우저의 주소창 옆이나 하단의 자물쇠 모양을 클릭하시면 인증서를 확인하실 수 있습니다.

8. 인증서 관리

인증서 파일을 분실하거나 비밀번호를 잊어버릴 경우 인증서 파일을 재발급 받아야 합니다. 재발급 시 제품에 따라 재발급되는 시간이 짧게는 1시간부터 길게는 2일이상 소요될 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.

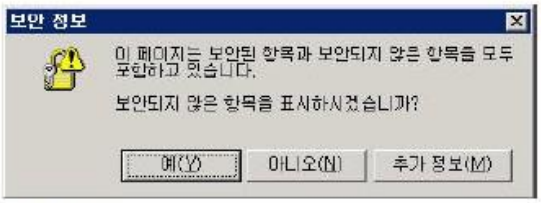
참고1. 전체 Page를 https:// 로 적용 시 약간(약 5%정도)의 속도저하가 있을 수 있습니다.

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

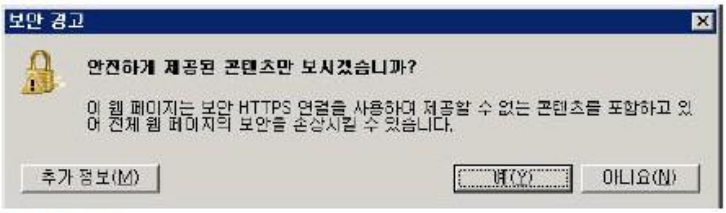
- 이 경우는 메인 Page에 http:// 와 https:// 가 공존하기 때문에 모두 https:// 로 소스변경
- 자바스크립트, 플래쉬 등의 데이터도 모두 https:// 로 변경

*** 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.**

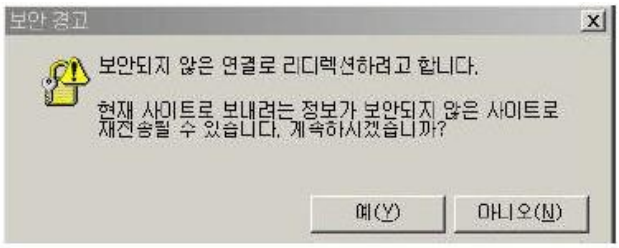
또한 플래쉬가 있는 경우 소스상에서 http://download.macromedia.com/~~/*.cab

→ 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



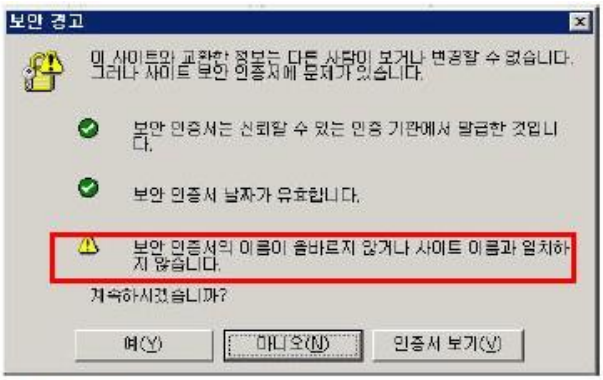
원인 : 예를 들어, https://URL/login.jsp로 접속 시 로그인 처리 프로세스 과정 혹은 소스상에서 직접적으로 **http://리턴URL 주소를 넘겨줄 때 나타나는 경고메시지** 입니다.

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

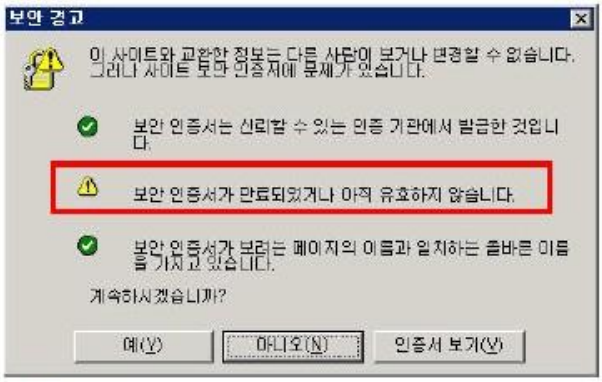


(IE 6버전)

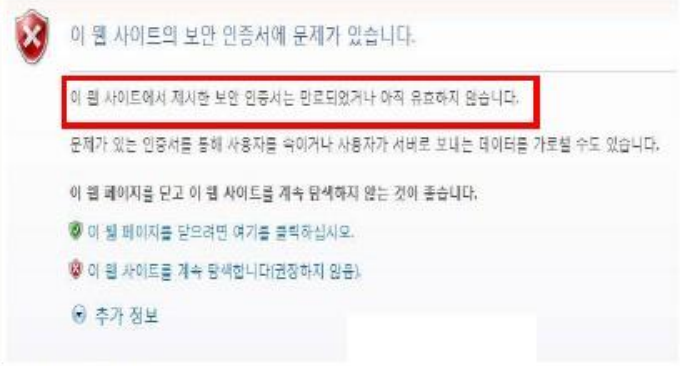
(IE 7,8버전)

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)



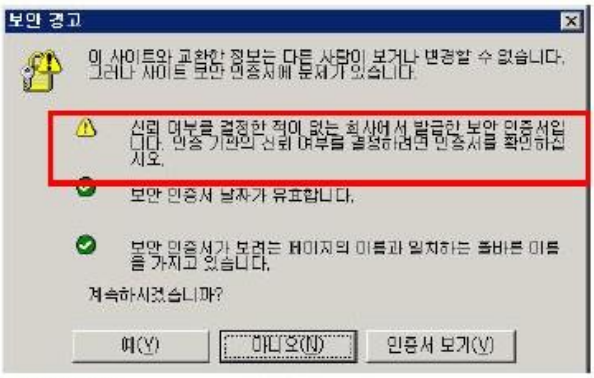
(IE 7,8버전)

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