

Oracle HTTP Server (Single) 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

02-3442-7230



www.kcs.kr
한국기업보안
Korea Corporation Security

※ 이 문서는 일반적인 설정이며 서버 및 네트워크 환경에 따라 달라질 수 있습니다.

1. OHS 환경 파일 httpd.conf 파일을 확인 합니다.

```
[oracle@ucert default]$ vi /Middleware/Oracle_WT1/instances/instance1/config/OHS/ohs1/httpd.conf
```

```
<IfDefine SSL>
LoadModule ossl_module      "${ORACLE_HOME}/ohs/modules/mod_ssl.so"
* 설명 : 주석 처리 되어있을 경우 해제하여 설정을 활성화 합니다.
</IfDefine>
# Include the SSL definitions and Virtual Host container
include "${ORACLE_INSTANCE}/config/${COMPONENT_TYPE}/${COMPONENT_NAME}/ssl.conf"
* 설명 : include 된 파일을 확인 합니다.
```

2. ssl.conf 파일을 확인하여 인증서 경로 확인 및 설정 확인.

```
[oracle@ucert default]$ vi /Middleware/Oracle_WT1/instances/instance1/config/OHS/ohs1/ssl.conf
```

Listen 443

* 설명 : 포트번호를 기입하도록 합니다.

```
<IfModule ssl_module>
    AddType application/x-x509-ca-cert .crt
    AddType application/x-pkcs7-crl .crl
    SSLPassPhraseDialog builtin
    SSLSessionCache
"shmcb:${ORACLE_INSTANCE}/diagnostics/logs/${COMPONENT_TYPE}/${COMPONENT_NAME}/ssl_scache(51200
0)"
    SSLSessionCacheTimeout 300

    <IfModule mpm_winnt_module>
        SSLMutex "none"
    </IfModule>
    <IfModule !mpm_winnt_module>
        SSLMutex pthread
    </IfModule>
```

<VirtualHost *:443>

```
<IfModule ssl_module>
    SSLEngine on
    SSLVerifyClient None
```



SSLProtocol nzos_Version_1_0 nzos_Version_3_0

SSLCipherSuite

SSL_RSA_WITH_RC4_128_MD5,SSL_RSA_WITH_RC4_128_SHA,SSL_RSA_WITH_3DES_EDE_CBC_SHA,SSL_RSA_WITH_DES_CBC_SHA,TLS_RSA_WITH_AES_128_CBC_SHA,TLS_RSA_WITH_AES_256_CBC_SHA

SSLCheck Off

SSLWallet

"\${ORACLE_INSTANCE}/config/\${COMPONENT_TYPE}/\${COMPONENT_NAME}/keystores/default"

* 설명 : 인증서 경로를 파악하여 업로드 하도록 합니다.

<FilesMatch "^(.cgi|shtml|phtml|php)\$">

SSLOptions +StdEnvVars

</FilesMatch>

<Directory "\${ORACLE_INSTANCE}/config/\${COMPONENT_TYPE}/\${COMPONENT_NAME}/cgi-bin">

SSLOptions +StdEnvVars

</Directory>

BrowserMatch ".MSIE.*" %

nokeepalive ssl-unclean-shutdown %

downgrade-1.0 force-response-1.0

</IfModule>

</VirtualHost>

</IfModule>

3. 인증서 파일을 백업할 수 있도록 합니다.

[oracle@ucert default]\$ ll

drwxr-xr-x. 2 root root 4096 2016-06-14 14:03 cwallet.sso

[oracle@ucert default]\$ mkdir 20190101

[oracle@ucert default]\$ cp cwallet.sso 20190101

[oracle@ucert default]\$ ll 20190101

drwxr-xr-x. 2 root root 4096 2019-01-01 14:03 cwallet.sso



4. ssl.conf 파일의 "SSLWallet"에 설정한 경로에 발급 받으신 인증서를 업로드 합니다.

```
[oracle@ucertdefault]$ pwd  
/Middleware/Oracle_WT1/instances/instance1/config/OHS/ohs1/keystores/default
```

5. OHS 프로세스 재시작을 진행 합니다

```
[oracle@ucert default]$ opmnctl stopall  
[oracle@ucert default]$ opmnctl startall
```

6. 서버 내에서 명령어로 SSL 포트 Listen 상태 및 인증서 기간을 확인 합니다.

```
[root@localhost ~]# netstat -nap | grep httpd
```

```
tcp 0 0 :::80 :::* LISTEN  
tcp 0 0 :::443 :::* LISTEN
```

*설명: 설정한 SSL 포트가 Listen 상태인지 확인 합니다.

```
[root@localhost ~]# openssl s_client -connect localhost:443 < /dev/null 2>&1 | openssl x509 -noout -enddate
```

```
notAfter=Dec 20 23:59:59 2016 GMT
```

* 설명: 인증서 만료일을 확인 합니다.

UCERT
www.ucert.co.kr



본 문서는 주식회사 한국기업보안에서 SSL보안서버인증서 설치를 위해 작성된 문서로
주식회사 한국기업보안의 동의 없이 무단으로 사용하실 수 없습니다

Copyright 2018-2023. Korea Corporation Security Co., Ltd All pictures cannot be copied without permission.

7. 웹페이지에서 인증서를 확인 합니다.

익스플로러 확인 방법 <https://www.ucert.co.kr> 접속 예

The screenshot shows the Internet Explorer browser window with the address bar displaying <https://www.ucert.co.kr>. The 'File' menu is open, and the 'Properties' option is highlighted. A text box explains the steps: '도메인 접속 후에 Alt 키를 누르고 파일 → 속성 → 인증서 클릭 후 인증서 보기를 선택하시면 인증서정보를 확인 할 수 있습니다.' (After connecting to the domain, press the Alt key and click File → Properties → Certificate, then click View Certificate to check the certificate information.) Another text box points to the 'Certificate' dialog box, stating: '발급 대상 과 유효 기간이 맞는지 확인합니다.' (Check if the issuance target and validity period are correct.) The 'Certificate' dialog box shows the 'Certificates' tab with the 'View Certificate' button highlighted. The 'View Certificate' dialog box is also shown, displaying the 'Certificate Information' tab with details about the certificate issued to www.ucert.co.kr by GlobalSign Extended Validation CA - SHA256 - G2, valid from 2015-11-09 to 2016-08-12.

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

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

발급자: GlobalSign Extended Validation CA - SHA256 - G2

유효 기간: 2015- 11- 09 부터 2016- 08- 12

발급자 설명(S)

인증서에 대해 자세히 알아보십시오.

확인