

Webtob (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

※ (필독)이 문서는 일반적인 설정이며, 서버마다 설정이 상이할 수 있어 인증서 설치 시 해당 문서 참고 부탁드립니다.

- 작업 전 참고사항 입니다.

인증기관 별 Root & Chain 인증서 구분 방법 입니다.

※ 발급 받은 인증서를 아래표를 참고하여 Root 및 Chain 인증서를 구분 합니다.

[GlobalSign] 인증기관

설정구분	인증서 형식
SSLCertificateChainFile	GLOBALSIGN_RSA_DV_SSL_CA_2018.crt [DV]
	GLOBALSIGN_RSA_OV_SSL_CA_2018.crt [OV]
	GLOBALSIGN_EXTENDED_VALIDATION_CA_SHA256_G3.crt [EV]
	ALPHASSL_CA_SHA256_G2.crt (Domain)_ChainBundle.crt
SSLCACertificateFile	GLOBALSIGN_ROOT_CA.crt

[Comodo] - 인증기관

설정구분	인증서 형식
SSLCertificateChainFile	(Domain)_ChainBundle.crt
SSLCACertificateFile	AAA_CERTIFICATE_SERVICES.crt

[Digicert] - 인증기관

설정구분	인증서 형식
SSLCertificateChainFile	THAWTE_RSA_CA_2018.crt
SSLCACertificateFile	DIGICERT_GLOBAL_ROOT_CA.crt

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.

1. 발급 받으신 인증서를 해당 SSL 폴더에 업로드 또는 저장합니다.
 2. [\$Webtob_Home]/config/ http.m 파일을 열어 SSL 환경 설정을 확인합니다.
- 설명 : [\$Webtob_Home] = Webtob 디렉토리

```
[root@localhost webtob]$ vi config/http.m
```

*NODE

```
UCERT      WEBTOBDIR="/usr/local/webapp/webtob ",
            SHMKEY = 54000,
            DOCROOT="/usr/local/webapp/webtob/docs/ucert/", //기본 홈디렉토리
            PORT = "80",           #설명 : 기본 http 포트
            HTH = 2                #설명 : Jesus 연동 Count
            JSVPORT = 9900,        #설명 : Jesus 연동 포트
            IPCPERM = 0777,
            NODENAME = "${NODENAME}",
            SERVICEORDER = "ext,uri",
            INDEXNAME = "index.jsp,index.html,index.htm",
            LOGGING = "log1",
            ERRORLOG = "log2"
```

*VHOST

```
ucert_ssl  DOCROOT="/usr/local/webapp/webtob/docs/ucert/" #홈 디렉토리,
            NODENAME=ucert,
            PORT="443",
            SSLFLAG=Y,
            SSLNAME="ucertssl",
            HOSTNAME = "sslinstall.ucert.co.kr",
            HOSTALIAS = "111.222.111.222", #대표 도메인 외 지정하실 별칭
            ServiceOrder="uri,ext",
            LOGGING="log1_vhmytx",
            ERRORLOG="log2_vhmytx"
```

*SSL

```
ucertssl   CertificateFile = "/usr/local/webtob/config/ssl/File_sslinstall.ucert.co.kr_webtob.crt",
            #설명 : 인증서 경로 설정 및 파일 명
            CertificateKeyFile = "/usr/local/webtob/config/ssl/KeyFile_sslinstall.ucert.co.kr_webtob.key",
            #설명 : 개인키 경로 설정 및 파일 명
            CertificateChainFile = "/usr/local/webtob/config/ssl/ChainFile_ChainBundle.crt",
            #설명 : Chain 인증서 경로 설정 및 파일 명
            CACertificateFile = "/usr/local/webtob/config/ssl/CA_GLOBALSIGN_ROOT_CA.crt"
            #설명 : Root 인증서 경로 설정 및 파일 명
```



*SVRGROUP

```
htmlg      SVRTYPE = HTML
jspx      SVRTYPE = JSV, VhostName = "ucert, ucert_ssl"
# Servlet 호출을 위한 Jeus 연동 할 가상 호스트 선언합니다.
```

*SERVER

```
html      SVGNAME = htmlg, MinProc = 50, MaxProc = 50, ASQCount = 1
MyGroup   SVGNAME =jspx, MinProc = 100, MaxProc = 200
```

*URI

```
uri1 Uri = "/", Svrtype = JSV, SvrName = MyGroup, VhostName = " ucert, ucert_ssl "
# Servlet 호출을 위한 Jeus 연동 할 가상 호스트 선언합니다.
```

※ 인증서파일의 파일명은 예시이므로 사용자 설정에 따라 인증서 파일명이 달라질 수 있습니다.

3. 기존 인증서 파일을 백업 합니다. (※기존 인증서는 반드시 백업을 할 수 있도록 합니다.)

```
[root@localhost ssl]$ mkdir ucert_2016
[root@localhost ssl]$ cp * ucert_2016/

[root@localhost ssl]$ ll
-rw-r--r--. 1 root root 1931 Jan 1 00:00 ChainFile_ChainBundle.crt
-rw-r--r--. 1 root root 1744 Jan 1 00:00 File_sslinstall.ucert.co.kr_webtob.crt
-rw-r--r--. 1 root root 1931 Jan 1 00:00 KeyFile_sslinstall.ucert.co.kr_webtob.key
-rw-r--r--. 1 root root 1931 Jan 1 00:00 CA_GLOBALSIGN_ROOT_CA.crt
drw-r--r--. 1 root root 1931 Jan 1 00:00 ucert_2016
```

4. Webtob 설정 파일 컴파일을 합니다.

```
[root@localhost webtob]# wscfl -i http.m #설정파일을 수정 후 컴파일 작업을 합니다.
urrent configuration:
Number of client handler(HTH) = 1
Supported maximum user per node = 4047
Supported maximum user per handler = 4047

Successfully created the configuration file (/root/webtob/config/wsconfig) for node UCERT.
The host name of the running machine is UCERT.
```

※ 컴파일 미진행 시 수정한 내용 적용이 되지 않아 필수 진행이 필요하며, 위와 같이 Successfully 확인 후 Webtob 재시작 진행 부탁드립니다.

5. Webtob 프로세스 재시작을 합니다.

```
[root@localhost webtob]# wsdown
Do you really want to shut down WebtoB? (y : n): y

WSDOWN for node(localhost) is starting:
WSDOWN: SERVER(html:1) downed: Fri Jan 1 00:00:00 2016
WSDOWN: SERVER(html:0) downed: Fri Jan 1 00:00:00 2016
WSDOWN: SERVER(cgi:11) downed: Fri Jan 1 00:00:00 2016
WSDOWN: SERVER(ssi:21) downed: Fri Jan 1 00:00:00 2016
WSDOWN: SERVER(ssi:20) downed: Fri Jan 1 00:00:00 2016
WSDOWN: SERVER(cgi:10) downed: Fri Jan 1 00:00:00 2016
WSDOWN: HTL downed: Fri Jan 1 00:00:00 2016
WSDOWN: HTH downed: Fri Jan 1 00:00:00 2016
WSDOWN: WSM downed: Fri Jan 1 00:00:00 2016
WSDOWN: WebtoB is down

[root@localhost webtob]# wsboot
Booting WebtoB on node (UCERT)
Welcome to WebtoB demo system. It will expire on 2016/06/27
Today is 2016/06/07
Starting WSM at Fri Jan 1 00:00:00 2016
Starting HTL at Fri Jan 1 00:00:00 2016
Starting HTH at Fri Jan 1 00:00:00 2016
Current WebtoB Configuration:
Number of client handlers (HTH) = 1
Supported maximum user per node = 4047
Supported maximum user per handler = 4047
Starting SVR(htmls) at Fri Jan 1 00:00:00 2016
Starting SVR(htmls) at Fri Jan 1 00:00:00 2016
Starting SVR(cgis) at Fri Jan 1 00:00:00 2016
Starting SVR(cgis) at Fri Jan 1 00:00:00 2016
Starting SVR(ssis) at Fri Jan 1 00:00:00 2016
Starting SVR(ssis) at Fri Jan 1 00:00:00 2016
```

6. 포트 확인 : 설정하신 SSL 포트가 Listen 상태인지 확인합니다.

```
[root@localhost ~]# netstat -nlp | grep htl
tcp      0 0 :::80          :::* LISTEN
tcp      0 0 :::443         :::* LISTEN
```



7. 서버 내에서 인증서 갱신을 확인하도록 합니다.

```
[root@localhost ~]# echo "" | openssl s_client -connect localhost:443 | openssl x509 -noout -dates
notBefore=Jan 1 00:24:14 2016 GMT #인증서 시작일
notAfter=Dec 31 :38:20 2017 GMT #인증서 만료일
```

※ openssl 명령어 적용이 안될 경우 wbssl 로 변경 후 진행 부탁드립니다.

8. 웹페이지에서의 인증서 확인 방법

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

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

일반

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
수정된 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