

Nginx (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 참고 부탁드립니다.

1. 서버에 발급 받은 인증서를 기존 인증서 파일 백업 후 업로드 합니다.

```
[root@localhost ssl]$ ls -l
-rw-r--r--. 1 root root 1744 Jan 1 00:00 sslinstall.ucert.co.kr.pem
-rw-r--r--. 1 root root 1931 Jan 1 00:00 KeyFile_sslinstall.ucert.co.kr.key
-rw-r--r--. 1 root root 1744 Jan 1 00:00 password.txt
```

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

2. [\$Nginx_Home]/conf/nginx.conf 파일을 열어 SSL 환경 설정을 확인 합니다.

설명 : [\$Nginx_Home] = Nginx 디렉토리

```
# HTTPS server //설명: 아래에 주석을 해제하여 SSL 을 사용설정토록 한다.
server {
    listen      443 ssl; //설명: 포트번호 설정.
    server_name sslinstall.ucert.co.kr; //설명: 도메인 명을 기입한다.

    ssl_certificate      /usr/local/nginx/ssl/sslinstall.ucert.co.kr.pem;
                        //설명: 인증서 위치를 설정하고 파일 명을 동일하게 한다.
    ssl_certificate_key  /usr/local/nginx/ssl/KeyFile_sslinstall.ucert.co.kr.key;
                        //설명: 인증서 키 파일 경로 설정 및 파일명 동일하게 한다.

    ssl_session_cache    shared:SSL:1m;
    ssl_session_timeout  5m;

    ssl_ciphers  HIGH:!aNULL:!MD5;
    ssl_prefer_server_ciphers  on;

    location / {
        root    html;
        index   index.html index.htm;
    }
}
```

3. Nginx 재시작

```
[root@localhost sbin]# ls -l
total 7292
-rwxr-xr-x. 1 root root 4720496 Jan  1 19:36 nginx //설명: 실행 파일 확인 완료

[root@localhost sbin]# ./nginx -s stop
[root@localhost sbin]# ./nginx
```

※ 재기동 명령어는 서버마다 상이하여 확인 후 진행이 필요합니다.

4. 포트 확인 : 설정하신 SSL 포트가 Listen 상태 인지 확인합니다.

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

5. 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
```

UCERT

www.ucert.co.kr



6. 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

일반 자세히 인증 경로

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