

Jboss (Single&Multi) SSL 인증서 신규·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.한국기업보안.kr
Korea Corporation Security

- ※ 이 문서는 일반적인 설정이며 서버 및 네트워크 환경에 따라 달라질 수 있습니다.
- ※ JBoss의 웹 컨테이너는 Jakarta Tomcat으로
Jboos_home/server/default/deply/jboss-web.deployer/server.xml 파일을 확인하면 tomcat의 SSL 설정과 같습니다.

- ※ 인증서 형식을 .crt 로 발급 받으신 경우, 가이드 1 번부터 진행이 필요하며, .jks 파일로 발급 받으신 경우, 2 번(5page)부터 진행해주시기 바랍니다.

1. Crt 형식에서 JKS 형식으로 변환

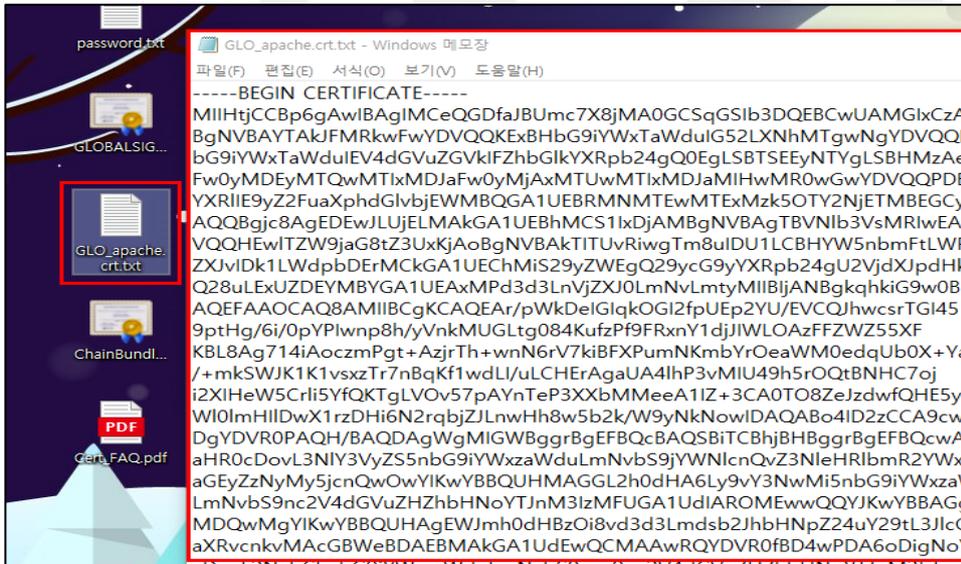
발급받은 인증서의 형식이 .crt 이실 경우, jks 인증서 변환이 필요하므로 아래 항목 순으로 변환 부탁드립니다.

1. crt 파일을 pem으로 변환

pem 형식은 ".key" 파일과 ".pem" 파일로 구분 됩니다.

".key" 파일은 개인키(private key)이며, ".pem" 파일은 public(도메인)/체인/루트 인증서가 하나의 bundle로 구성 되어야합니다.

받으신 각각의 ".crt" 인증서들은 .txt 확장자로 변경 하시면 text 형식으로 key 값을 확인 하실 수 있습니다.



각 key 값을 복사하시어 도메인/체인/루트 인증서 순으로 빈 메모장에 복사 합니다.



```

*새 텍스트 문서.txt - Windows 메모장
파일(F) 편집(E) 서식(O) 보기(V) 도움말(H)
hYIXAgMBAAGjggEiMIIBHjAObGNVHQ8BAf8EBAMCAQYwDwYDVR0TAQH/BAUwAwEB
/zAdBgNVHQ4EFgQUj/BLf6guRSSuTVdY6Y5qL3uLdG7wwHwYDVR0jBBgwFoAUUYHtm
GkUNl8qJUC99Bm00qP/8/UswPQYIKwYBBQUHAQEEMTAwMC0GCCsGAQUFBzABHiFo
dHRwOi8vb2NzcC5nbG9iYWxzawduLmNvbS9yb290cjEwMwYDVR0fBCwwKjAooCag
JlYiaHR0cDovL2NybcC5nbG9iYWxzawduLmNvbS9yb290LmNybDBHBGNVHSAEQDA+
MDwGBFUdIAAwNDAYBggrBgEFBQcCARYmaHR0cHM6Ly93d3cuZ2xvYmFsc2lnbi5j
b20vcMvWb3NpdG9yeS8wDQYJKoZIhvcNAQELBQADggEBACNw6c/iwVZrpRCb8RD
M6rNPzq5ZBfyYgZLSPFAiAYXof6r0V88xjPy847dHx0+zBpgmYlRmF8fpqHKqV9
D6ZX7qw7aoXW3r1AY/itpsilsBL89kHfDwmXHjjqU5++BfQ+6tOfUBJ2vgmLwgtl
fR4uUfaNU9OrH0Abio7tfftPeVZwXwzTjhuzp3ANNyUxLava4BJrHED0xcd+7cJi
WOx37XMiwor1hkOlreoTbv3Y/klvuX1erRjvJDKPSerJpSzdcl03v3yKzTr1Eh
kluEFsuffT90y1HonoMOFm8b50bOI7355KKL0jlrqkckSziYSQjplcJDEHsXo
4HA=
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIIDdTCCAIGAwIBAgILBAAAAAABFUtaW5QwDQYJKoZIhvcNAQEFBQAwwVzELMAkG
A1UEBHMCAQXGTAxBGNVBAoTEEdsb2JhbFNpZ24gbnYtc2ExEDA0BgNVBAwTB1Jv
b3QgQ0ExGzAZBgNVBAMTEkdsb2JhbFNpZ24gUm9vdCBDQTAeFw05ODAsMDExMjAw
MDBaFw0yODAxMjg0MjAwMDBaMFcxZCZAJBgNVBAYTAkFMRkwkFwYDQkExBHBG9i
YWxTaWduIG52LXNhMRwDgYDVQQLEwdSb290LENBMRswGQYDVQQDEXJHbG9iYWxT
aWduIFJvb3QgQ0EwggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQAQDaDuaZ
jc6j40+Kfvxi4Mla+plH/EqsLmVEQS98GPR4mdmzxdzxtIK+6NiY6arymAZavp
xy0Sy6scTHAHOtOKMM0VjU/43dSMUBUc71DuxC73/OIS8pF94G3VNTCOXkNz8kHp
1Wrsok6Vjk4bwY8iGlbKk3Fp1S4blnMm/k8yuX9ifUSPJJ4ltbcdG6TRGHRjcdG
snUOhugZitVtbNV4FpWi6cgKOOvyJBnPC1STE4U6G7weNLWLBYY5d4ux2x8gkasJ
U26Qzns3dLwR5EiUWMMWea6xrEmCMgZK9FGqjWZCrXgzT/LCrBbBIDSgef59N8
9iFo7+rvUp9/k5DPAgMBAAGiQIBAMA4GA1UdDwEBw/QEAWIBBjAPBoNVRMBAf8E

```

빈 메모장은 cert.pem 으로 리네임 합니다.
 (“.pem”파일의 해당 인증서들은 “-----BEGIN CERTIFICATE-----” ~ “-----END CERTIFICATE-----” 한 단락으로 정의됩니다.)

```

cert.pem - Windows 메모장
파일(F) 편집(E) 서식(O) 보기(V) 도움말(H)
hYIXAgMBAAGjggEiMIIBHjAObGNVHQ8BAf8EBAMCAQYwDwYDVR0TAQH/BAUwAwEB
/zAdBgNVHQ4EFgQUj/BLf6guRSSuTVdY6Y5qL3uLdG7wwHwYDVR0jBBgwFoAUUYHtm
GkUNl8qJUC99Bm00qP/8/UswPQYIKwYBBQUHAQEEMTAwMC0GCCsGAQUFBzABHiFo
dHRwOi8vb2NzcC5nbG9iYWxzawduLmNvbS9yb290cjEwMwYDVR0fBCwwKjAooCag
JlYiaHR0cDovL2NybcC5nbG9iYWxzawduLmNvbS9yb290LmNybDBHBGNVHSAEQDA+
MDwGBFUdIAAwNDAYBggrBgEFBQcCARYmaHR0cHM6Ly93d3cuZ2xvYmFsc2lnbi5j
b20vcMvWb3NpdG9yeS8wDQYJKoZIhvcNAQELBQADggEBACNw6c/iwVZrpRCb8RD
M6rNPzq5ZBfyYgZLSPFAiAYXof6r0V88xjPy847dHx0+zBpgmYlRmF8fpqHKqV9
D6ZX7qw7aoXW3r1AY/itpsilsBL89kHfDwmXHjjqU5++BfQ+6tOfUBJ2vgmLwgtl
fR4uUfaNU9OrH0Abio7tfftPeVZwXwzTjhuzp3ANNyUxLava4BJrHED0xcd+7cJi
WOx37XMiwor1hkOlreoTbv3Y/klvuX1erRjvJDKPSerJpSzdcl03v3yKzTr1Eh
kluEFsuffT90y1HonoMOFm8b50bOI7355KKL0jlrqkckSziYSQjplcJDEHsXo
4HA=
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIIDdTCCAIGAwIBAgILBAAAAAABFUtaW5QwDQYJKoZIhvcNAQEFBQAwwVzELMAkG
A1UEBHMCAQXGTAxBGNVBAoTEEdsb2JhbFNpZ24gbnYtc2ExEDA0BgNVBAwTB1Jv
b3QgQ0ExGzAZBgNVBAMTEkdsb2JhbFNpZ24gUm9vdCBDQTAeFw05ODAsMDExMjAw
MDBaFw0yODAxMjg0MjAwMDBaMFcxZCZAJBgNVBAYTAkFMRkwkFwYDQkExBHBG9i
YWxTaWduIG52LXNhMRwDgYDVQQLEwdSb290LENBMRswGQYDVQQDEXJHbG9iYWxT
aWduIFJvb3QgQ0EwggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQAQDaDuaZ
jc6j40+Kfvxi4Mla+plH/EqsLmVEQS98GPR4mdmzxdzxtIK+6NiY6arymAZavp
xy0Sy6scTHAHOtOKMM0VjU/43dSMUBUc71DuxC73/OIS8pF94G3VNTCOXkNz8kHp
1Wrsok6Vjk4bwY8iGlbKk3Fp1S4blnMm/k8yuX9ifUSPJJ4ltbcdG6TRGHRjcdG
snUOhugZitVtbNV4FpWi6cgKOOvyJBnPC1STE4U6G7weNLWLBYY5d4ux2x8gkasJ
U26Qzns3dLwR5EiUWMMWea6xrEmCMgZK9FGqjWZCrXgzT/LCrBbBIDSgef59N8
9iFo7+rvUp9/k5DPAgMBAAGiQIBAMA4GA1UdDwEBw/QEAWIBBjAPBoNVRMBAf8E

```



2. pem 형식에서 pfx 형식으로 변환

openssl pkcs12 -inkey {private key 파일이름} -in {도메인/체인/루트번들 파일이름} -export -out {생성될 pfx 이름}

(예시)

```
openssl pkcs12 -inkey cert.key -in cert.pem -export -out cert.pfx
```

```
[root@localhost test]# openssl pkcs12 -inkey cert.key -in cert.pem -export -out cert.pfx
Enter Export Password:
Verifying - Enter Export Password:
[root@localhost test]# ls -lrt
한계 20
-rw-r--r-- 1 root root 7129 2020-12-16 19:11 cert.pem
-rw-r--r-- 1 root root 1680 2020-12-16 19:12 cert.key
-rw-r--r-- 1 root root 6837 2020-12-16 19:12 cert.pfx
```

3. pfx 형식에서 jks 형식으로 변환

keytool -importkeystore -srckeystore {생성한 pfx 이름} -srcstorepass {패스워드} -deststorepass {생성될 jks의 패스워드} -srcstoretype PKCS12 -destkeystore {생성될 JKS 파일이름}

(예시)

```
keytool -importkeystore -srckeystore cert.pfx -srcstorepass a12345 -deststorepass a12345 -srcstoretype PKCS12 -destkeystore cert.jks
```

```
[root@localhost test]# keytool -importkeystore -srckeystore cert.pfx -srcstorepass a12345 -deststorepass a12345 -srcstoretype PKCS12 -destkeystore cert.jks
1 별칭에 대한 항목이 성공적으로 임포트되었습니다.
임포트 명령 완료: 성공적으로 임포트된 항목은 1개, 실패하거나 취소된 항목은 0개입니다.
[root@localhost test]# ls -lrt
한계 28
-rw-r--r-- 1 root root 7129 2020-12-16 19:11 cert.pem
-rw-r--r-- 1 root root 1680 2020-12-16 19:12 cert.key
-rw-r--r-- 1 root root 6837 2020-12-16 19:14 cert.pfx
-rw-r--r-- 1 root root 6479 2020-12-16 19:15 cert.jks
```

JBOSS 인증서 적용

1. server.xml 파일을 확인하여 SSL 인증서 설정을 합니다.

```
<!-- // 주석의 시작 부분을 제거하여 설정을 활성화 합니다.
<Connector protocol="org.apache.coyote.http11.Http11Protocol" port="443"
    minSpareThreads="5" maxSpareThreads="75"
    enableLookups="true" disableUploadTimeout="true"
    acceptCount="100" maxThreads="200"
    scheme="https" secure="true" SSLEnabled="true"
    keystoreFile="{Jboss_home}/conf/ssl/www.ucert.co.kr.jks"
    <!--인증서 업로드 경로 및 파일명을 지정 합니다. -->
    keystorePass="*****"
    <!--인증서 비밀번호를 기재 합니다. -->
    clientAuth="false" sslProtocol="TLS"/>
--> // 주석의 마지막 부분을 제거하여 설정을 활성화 합니다.
```

:wq

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

2. Jboss 프로세스 재시작을 진행 합니다. (재시작 커맨드는 localhost 재시작을 예로 들었습니다.)

```
[root@localhost ~]# shutdown.sh -S
[root@localhost ~]# run.sh
```

3. 인증서 설치를 확인 합니다.

```
[root@localhost ~]# echo "" | openssl s_client -connect localhost:443 | openssl x509 -noout -dates
* 설명 : 위의 명령어를 입력하여 인증서 갱신 날짜를 확인 합니다.
notBefore=Jan 1 00:24:14 2016 GMT #인증서 시작일
notAfter=Dec 31 :38:20 2017 GMT #인증서 만료일

* 명령어 형식 : echo "" | openssl s_client -connect [도메인 or IP]:[포트번호] | openssl x509 -noout -dates
```



4. 웹페이지에서 인증서를 확인 합니다.

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.

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

인증서에 대해 자세히 알아보십시오.