Comodo Korea
국제표준인증 제휴기관

(BEA) WebLogic server 6.0 서버에 인증서 설치하기

SSL 웹서버인증서가 발급되면 메일을 통하여 기술담당자에게 전달된다.
담당자는 메일로 받은 인증서를 확인한 후에 가이드에 따라 설치한다.
인증서를 메모장으로 열어 내용을 확인하면 다음과 같은 형식을 갖는다.

```
-----BEGIN CERTIFICATE-----
MIISDOIUlkmlsRRlkSlIWLISdsSKJlalOSISLKjwBgNVBAg
AALOJdlwjam4gQ2FwZTESMBAGA1UEBxMJQ2FwZSBUb3duMR
QwEgYDVQQKEwHLOWDvcnR1bmlOaTEYMBYGKi2UECxMPT25s
aW5lIFNlcnZpY2VzMRowGAYDVQQDExF3d3cuZm9yd2FyZC5
jby56YTBaMAOGCSqGSIb3DQEHHKJWAAklmLKSuljSOIjsfB
Wu5WLHD/G4BJ+PobiC9d7S6pDvAjuyC+dPAnLOd91tXdm2j
19OD1kgDoSp5ZyGSgwJh2V7diuuPlHDAgEDoAAwDQYJVVjk
ksohvcNAQEEBQADQQBf8LSLKknlsklSSLlworrr334ZmXD1
AvUjuDPCWzFupRIIIiq7UR8ZOwiJUUsllkfq/IuuIlz6oq6
htdJklil/wdhh
-----END CERTIFICATE-----
```

웹서버인증서 : [인증받은 도메인 이름으로 된].crt
체인인증서 : Bundle.crt

웹서버 인증서 설치

1. 메일로 받은 인증서를 첫줄(-----BEGIN CERTIFICATE-----)부터 끝줄(-----END CERTIFICATE-----)까지 복사하여 'Weblogic server 설치 디렉터리'(\wlserver6.0\config\mydomain)에 각각 저장한다. 'Certificate servlet'으로 생성하였던 key 파일도 동일한 디렉터리에 저장한다.

   ※ 인증서파일의 파일명은 임의로 하되 확장자는 반드시 .pem(또는 .der)으로 하여야 한다.
   예를 들어 이 가이드에서는 comodokorea.pem 으로 이름을 지어 저장하였다.

2. Administration Console 을 구동 시킨 후 'Server Configuration'을 연다.
3. 'SSL' tap 을 선택하여 key file, certificate file, certificate chain file 이 저장된 경로를 작성한다.

4. 변경사항을 저장하기 위해 'Apply'버튼을 클릭한다.
5. 서버를 restart 한다.
6. https://hostname:7002 로 접속하여 브라우저 우측 하단에 '노란자물쇠' 표시가 나타나는지 확인한다. (SSL port 를 443 으로 변경한 경우에는 https://hostname:443 으로 접속)

Field	Description
Enabled	SSL 을 이용하기 위해 반드시 체크.
SSL Listen Port Server Certificate File Name	일반적으로 443 을 사용한다. default 값은 7002. key 파일이 있는 절대경로 입력.
Server Certificate File Name Server Certificate Chain File Name	웹서버 인증서 파일이 있는 절대경로 입력. 체인 인증서 파일이 있는 절대경로 입력
Client Certificate Enforced	클라이언트 인증 필요.(이곳을 클릭하면 클라이언트 인증서가 있는 접속자만 접속이 가능하다) 일반 고객을 대상으로 할 경우에는 클릭하지 않는다.
Trusted CA File Name	Default
CertAuthenticator	Default
Use Java	Checkbox that enables the use of native Java libraries. WebLogic Server provides a pure-Java implementation of the SSL protocol: native Java libraries enhance the performance for SSL operations on the Solaris, Windows NT, and IBM AIX platforms. By default, this field is not enabled.
Use Encrypted Keys	Field that specifies that the private key for the WebLogic Server has been encyrpted with a password. The default is false.
Handler Enabled	Field that specifies whether or not WebLogic Server rejects SSL connections that fail client authentication for one of the following reasons: • The requested client digital certificate was •

	not furnished. • The client did not submit a digital certificate • The digital certificate from the client was not issued by a certificate authority specified by the Trusted CA Filename field. By default, the SSL Handler allows one WebLogic Server to make outgoing SSL connections to another WebLogic Server. For example, an EJB in WebLogic Server may open an HTTPS stream on another Web server. With the HandlerEnabled field enabled, the WebLogic Server acts as a client in an SSL connection. By default this field is enabled. Disable this field only if you want to provide your own implementation for outgoing SSL connections. **Note:** The SSL Handler has no effect on the ability of WebLogic Server to manage incoming SSL connections.
Export Key Lifespan	The number of times WebLogic Server uses an exportable key between a domestic server and an exportable client before generating a new one. The more secure you want WebLogic Server to be the fewer times the key should be used before a new one is generated. The default is to use it 500 times.
Login Timeout Millis	The number of milliseconds that WebLogic Server should wait for an SSL connection before timing out. The default value is 25,000 milliseconds. SSL connections take longer to negotiate than regular connections. If clients are connecting over the Internet, raise the default number to accommodate additional network latency.
Certificate Cache Size	The number of digital certificates that are tokenized and stored by WebLogic Server. The default is 3.

Comodo Korea
국제표준인증 제휴기관

인증서 백업하기

1. 개인키 파일, 웹서버 인증서, 체인 인증서를 백업해 둡니다.

<인증서는 개인키와 함께 꼭 백업을 해두셔야 하며, 백업을 하지 않아 발생하는 문제에 대해서는 재발급 비용이 추가될 수 있습니다.>