

# Iplanet 7 (Single & Multi) SSL 인증서 신규 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.

## 1. 서버 환경 확인 (도메인 설정 확인)

- 1) 해당 서버 선택 후 서버설정 -> 일반탭에서 호스트 명이 신청할 도메인으로 되어 있는지 확인합니다.

The screenshot shows the 'Korsec - 가상 서버 일반 등록 정보' (Korsec - Virtual Server General Registration Information) page. The '일반' (General) tab is selected. The '호스트' (Host) field is highlighted with a red box and contains the value 'www.ucert.co.kr, ucert.co.kr'. Below the '호스트' field, there is a note: '둘 이상의 URL 호스트를 쉼표로 구분하여 입력할 수 있습니다.' (You can enter two or more URL hosts separated by commas).

구성 > Korsec > 가상 서버 > Korsec

서버 설정 | 웹 응용 프로그램 | 내용 처리 | WebDAV | 검색 | 액세스 제어 | 요약

일반 | 로그 기본 설정 | 모니터링 설정 | 요청 제한

### Korsec - 가상 서버 일반 등록 정보

모든 가상 서버에는 하나 이상의 HTTP Listener가 지정되어 있습니다. 새 요청이 들어오면 서버는 구성된 HTTP Listener를 사용할 수 있습니다. 이 페이지에서 가상 서버 등록 정보를 구성합니다.

- 일반
- 서비스 품질
- P3P 설정
- HTTP Listener
- 현지화
- 변수

일반

이름: Korsec

가상 서버: ☒ 사용 가능

문서 루트:   
가상 서버에 대한 문서 루트(절대 경로 또는 서버의 구성 디렉토리에 대한 상대 경로)

호스트:   
둘 이상의 URL 호스트를 쉼표로 구분하여 입력할 수 있습니다.

맨 위로 돌아가기

### HTTP Listener

HTTP Listener (1)

<input checked="" type="checkbox"/> <input type="checkbox"/>	이름	IP 주소	포트
<input type="checkbox"/>	http-listener-1	* [모든 IP 주소]	80

맨 위로 돌아가기

- 2) 해당 가상 서버에 SSL 포트추가를 위해 HTTP Listener를 추가 합니다.

(일반 포트를 사용하지 않고 SSL 포트만 사용할 경우에는 기존 HTTP Listener의 포트만 변경하면 됩니다)

The screenshot shows the 'Korsec - HTTP Listener' configuration page. The 'HTTP Listener' tab is selected. The '새로 만들기...' (Create New) button is highlighted with a red box. The table below shows the existing listener 'http-listener-1' with IP address '\* [모든 IP 주소]' and port '80'. The 'SSL' column shows '사용 불가능' (Not available) and the '기본 가상 서버' (Default virtual server) is 'Korsec'.

구성 > Korsec

가상 서버 | HTTP Listener | 인스턴스 | 일반 | 성과 | 액세스 제어 | 인증서 | Java | 요약

### Korsec - HTTP Listener

서버는 구성된 가상 서버로 요청을 전달하기 전에 HTTP Listener를 통해 HTTP 요청을 수락합니다. 이 페이지에서는 HTTP Listener를 추가하고 구성할 수 있습니다. IP 주소는 IPv4 또는 IPv6 주소를 사용할 수 있습니다. IP 주소를 "\*"로 설정하면 해당 포트의 모든 IP 주소를 수신하는 HTTP Listener를 생성합니다.

### HTTP Listener (1)

<input checked="" type="checkbox"/> <input type="checkbox"/>	이름	IP 주소	포트	SSL	기본 가상 서버
<input type="checkbox"/>	http-listener-1	* [모든 IP 주소]	80	사용 불가능	Korsec

### 3) 추가 할 SSL 포트 입력 하고 서버 이름을 입력합니다

(서버 이름은 도메인으로 해도 되고 가상 서버명으로 하셔도 됩니다.)

Oracle iPlanet Web Server

새 HTTP Listener 마법사

단계 도움말 단계 1: HTTP Listener 추가

→ 1. HTTP Listener 추가  
2. 검토  
3. 결과

다음 필수 값을 제공하여 새 HTTP Listener를 구성에 추가합니다.

\* 필수 필드 표시

\* 이름:   
HTTP Listener를 고유하게 식별하는 이름

\* 포트:   
수신할 포트

\* IP 주소:   
IP 주소 또는 모든 IP 주소를 수신하는 경우 \*

\* 서버 이름:   
기본 서버 이름

\* 기본 가상 서버:   
호스트와 일치하지 않았던 요청을 처리하는 가상 서버의 이름

이전 다음 취소

### 4) 확인 -> 닫기 후 다시 서버설정 -> 일반으로 이동 후 HTTP Listener에 추가합니다.

맨 위로 돌아가기

HTTP Listener

HTTP Listener (1)

추가... 삭제

<input checked="" type="checkbox"/>	이름	IP 주소	포트
<input type="checkbox"/>	http-listener-1	* [모든 IP 주소]	80

HTTP Listener를 가상 서버에 추가

이 페이지에서는 구성에서 사용할 수 있는 HTTP Listener를 나열합니다. 이 가상 서버와 연결할 Listener를 선택합니다. 선택한 Listener를 이 가상 서버와 연결하려면 추가를 누릅니다.

이름: Korsec

Listener 선택:

여러 Listener를 선택하려면 Ctrl 키를 누른 상태로 선택합니다.

Add 취소

HTTP Listener

HTTP Listener (2)

추가... 삭제

<input checked="" type="checkbox"/> 	이름	IP 주소	포트
<input type="checkbox"/>	http-listener-1	* [모든 IP 주소]	80
<input type="checkbox"/>	http-listener-2	* [모든 IP 주소]	443

맨 위로 돌아가기

## 2. PKCS11 토큰 생성하기 (인증서 DB 생성하기)

1) 서버 설정에서 인증서 -> pkcs11 토큰 으로 이동합니다. 그 후 internal를 선택합니다.

구성 > Korsec

가상 서버 HTTP Listener 인스턴스 일반 성과 액세스 제어 인증서 Java 요약

서버 인증서 인증 기관 CRL 업데이트 PKCS11 토큰

Korsec 구성 - PKCS11 토큰

PKCS11 토큰은 원시 PKCS#11 인터페이스를 가진 모든 하드웨어 및 소프트웨어 토큰을 나타냅니다. 하드웨어 토큰은 하드웨어 가속기 및 스마트 카드 소프트웨어 토큰은 전적으로 소프트웨어에서 구현되는 PKCS#11 토큰입니다. 이 페이지에서는 구성에서 사용할 수 있는 토큰을 나열합니다. 이 테이블을 사용하여 토큰 이름을 눌러 토큰에 대한 등록 정보를 편집합니다.

일반 설정

PKCS11: ☒ 사용 가능

무시 허용: ☒ 사용 가능

토큰이 PKCS11 계층을 지원하는 경우 이 계층을 무시하도록 허용합니다. 이 옵션을 선택하면 성능이 향상될 수 있습니다.

PKCS11 토큰 (1)

이름	토큰 상태
internal	사용 가능

2) "토큰 상태"에 사용 가능 체크 후 원하는 패스워드를 입력합니다. (절대 잊으면 안 됩니다.)

- 만약 패스워드 입력을 원치 않는다면 "비밀번호 설정 해체" 하시면 됩니다.
- 인스턴스 시작시 패스워드 묻지 않도록 하고 싶을 시 아래와 같이 체크합니다.

Korsec 토큰 등록 정보

새 토큰 비밀번호를 설정합니다.

\* 필수 필드 표시

이름: internal

토큰 상태: ☒ 사용 가능

☒ 토큰 비밀번호 편집

\* 현재 비밀번호: .....

☐ 비밀번호 변경

새 비밀번호: .....

비밀번호 다시 입력: .....

토큰에 대한 새 비밀번호 설정

☐ 인스턴스 시작 시 새 비밀번호 확인 메시지 표시 안 함

새 비밀번호는 구성에 저장됩니다.

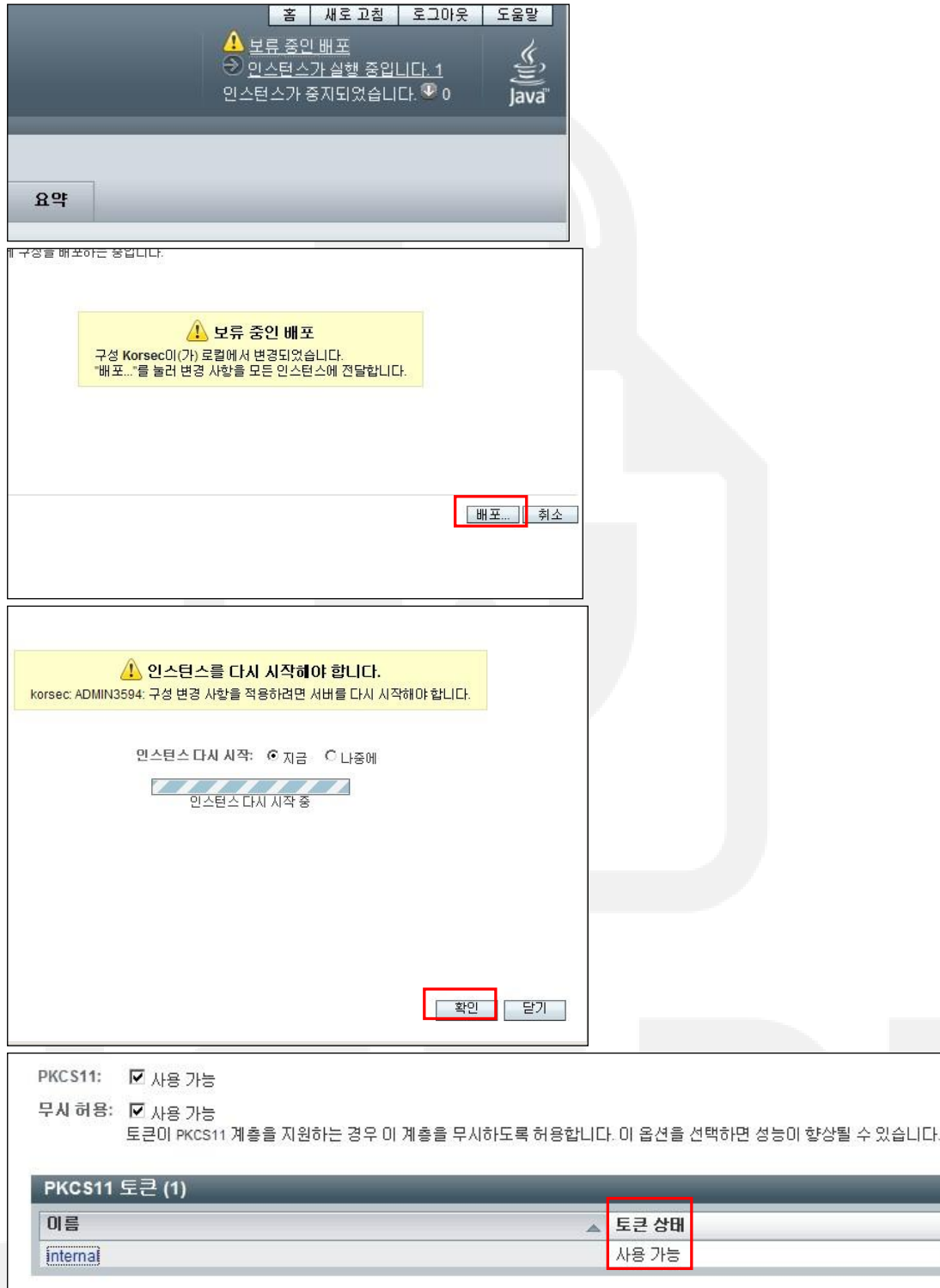
☐ 비밀번호 설정 해체

☒ 인스턴스 시작 시 현재 비밀번호 확인 메시지 표시 안 함

현재 비밀번호가 구성에 저장됩니다.

확인 취소

3) “보류 중인 배포” 클릭하여 배포후 인스턴스 재시작합니다.

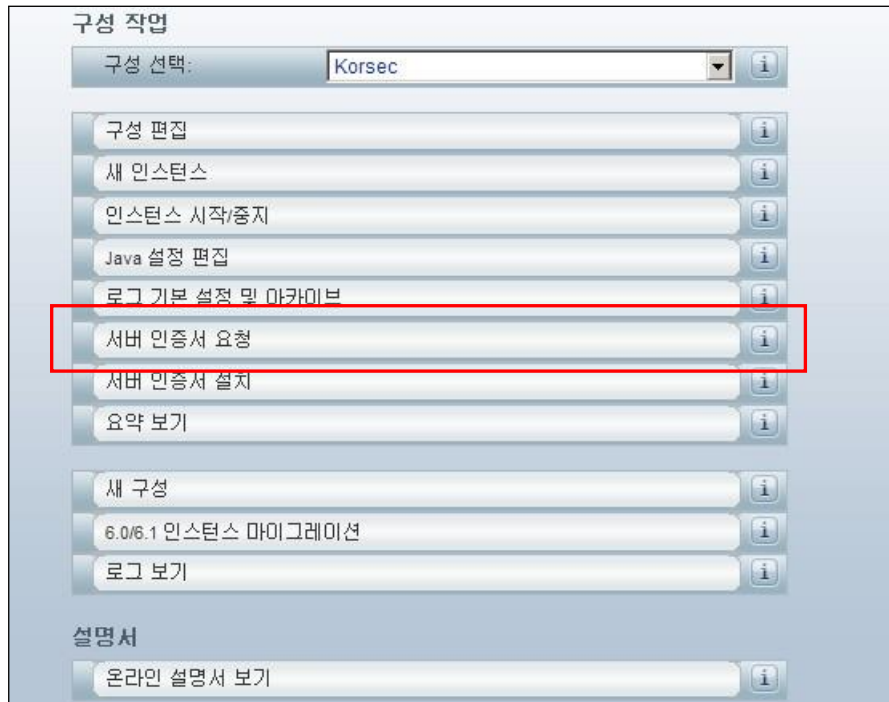


토큰상태가 사용가능인지 확인합니다. (F5새로고침 또는 다른 페이지 접속 후 현재페이지로 접속합니다.)

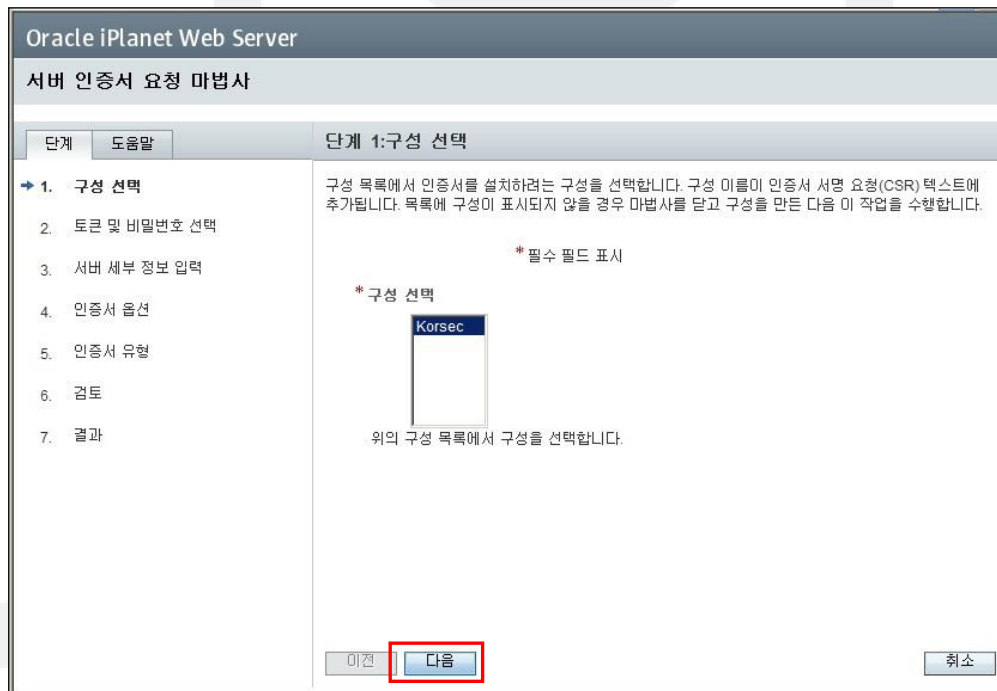
www.ucert.co.kr

### 3. CSR 생성하기

1) 웹 콘솔에 접속하여 “서버인증서 요청”을 클릭합니다.



2) 서버 인증서 요청 마법사가 실행되면 서버를 선택합니다.



### 3) 다음을 클릭합니다.

서버 인증서 요청 마법사

단계 도움말 단계 1:토큰 및 비밀번호 선택

→ 1. 토큰 및 비밀번호 선택

2. 서버 세부 정보 입력

3. 인증서 옵션

4. 인증서 유형

5. 검토

6. 결과

구성에 사용할 수 있는 토큰 목록이 페이지에 표시됩니다. 필요한 경우 선택한 토큰의 비밀번호를 입력합니다.

구성: Korsec

토큰: internal

위 목록에서 토큰 이름을 선택합니다. Oracle iPlanet Web Server 7.0에서 유지 관리하는 로컬 키 데이터베이스에 키가 저장되어 있으면 내부를 선택합니다. 스마트 카드 또는 기타 외부 장치나 엔진에 키가 저장되어 있으면 드롭다운 목록 상자에서 외부 토큰의 이름을 선택합니다.

비밀번호: .....

선택한 토큰의 비밀번호를 입력합니다. 비밀번호 필드는 선택한 토큰에 비밀번호가 필요한 경우에만 활성화됩니다.

이전 다음 취소

### 4) CSR생성 정보를 입력합니다.

Oracle iPlanet Web Server

서버 인증서 요청 마법사

단계 도움말 단계 2:서버 세부 정보 입력

1. 토큰 및 비밀번호 선택

→ 2. 서버 세부 정보 입력

3. 인증서 옵션

4. 인증서 유형

5. 검토

6. 결과

인증서 요청을 생성하기 위한 정보를 입력합니다.

\* 필수 필드 표시

\* 서버 이름: www.ucert.co.kr

www.sun.com과 같은 단일 서버 이름이나 www.sun.com.java.sun.com과 같이 서버 이름을 목록을 실패로 구분하여 입력할 수 있습니다.

조직(o): ucert

조직 구성 단위(ou): Korea Corporation Security

구/군/시(i): Seocho-gu

시/도(st): Seoul

국가(c): 대한민국 KR

국가를 선택하거나 두 자리 국가 코드를 지정합니다.

이전 다음 취소



5) 키 유형에서 RSA -> 2048 bit를 선택합니다.

Oracle iPlanet Web Server

서버 인증서 요청 마법사

단계 도움말 단계 3:인증서 옵션

1. 토큰 및 비밀번호 선택  
2. 서버 세부 정보 입력  
→ 3. 인증서 옵션  
4. 인증서 유형  
5. 검토  
6. 결과

인증서의 키 유형을 지정하십시오.

키 유형

☒ RSA  
키 크기: 2048 비트  
키 길이가 길수록 마법사에서 키를 생성하는 데 더 오랜 시간이 걸립니다.

☐ ECC  
곡선 이름: prime256v1

이전 다음 취소

6) CA 서명이 있는 인증서를 선택합니다.

Oracle iPlanet Web Server

서버 인증서 요청 마법사

단계 도움말 단계 4:인증서 유형

1. 토큰 및 비밀번호 선택  
2. 서버 세부 정보 입력  
3. 인증서 옵션  
→ 4. 인증서 유형  
5. 검토  
6. 결과

인증서에 대한 인증서 서명 기관(CSA)을 선택합니다.

\* 필수 필드 표시

☐ 자체 서명된 인증서  
\* 별명: cert-Korsec  
\* 유효 기간: 12 개월  
수신기: --없음--

☒ CA 서명이 있는 인증서

이전 다음 취소



7) 정보를 확인 후 “마침”을 클릭합니다.

8) 생성된 CSR 코드를 마우스로 드래그 하여 복사 한 후 메모장에 복사합니다..

복사한 CSR 코드 값에서 공백 제거 하여 ssl@ucert.co.kr 보내주시면 됩니다.



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.

```

www.ucert.co.kr.csr - 메모장
파일(F) 편집(E) 서식(O) 보기(V) 도움말(H)

-----BEGIN NEW CERTIFICATE REQUEST-----
MIIDGzCCAgMCAQAwYACzAJBgNVBAYTAktSMQ4wDAYDUQIEwUTZW91bDESMBAQ
A1UEBxMJU2UvY2hvdW1MQ4wDAYDUQKEwU1Y2Uyde jMCEGA1UECzMaS29yZWeg
Q29ycG9yYXRpb24gU2UjdXJpdHkxGDAwBgNVBAMTD3d3dy51Y2Uyde j5y5rc jCC
ASiwdQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAM80Jk0j/qnhco4ygMxmiSKS
U+XUv75BB21L2EXYci0t1oMKpTnUwh4keFyE94AqFpDfN08tWtSib9R6+zjb5+fx
onuRwFbou/F6p6q1C/+9Bnc09gEuhIeSqozDjKE0M6i6eoZWazFWJ+j9QAQic61
PcoDpRlN/iLFvLhc23ZuAVNpFQpBSbn1UmVaTzFR7W4yG/8je8I+2R6kQ/iDK2uD
T/z1NX06B2pp1GUHQvFSIHYPQN5y7dhJX45+hUHa1f/zx3M2j0j3oLRglwIyoqrq
kXNxBS/NmgUv2X08X0hicG0GWe18ytcL0JsskGnr7FA6H1gCuWhKZR02creUw2cc
AwEAABUMFMCsGSIb3DQEJDjFGEQwGgYDUR0RBBMwEYIPd3d3LnUjZXJ0LnNv
LmtyMBYGA1UdJQEB/wQMMAoGCCsGAQUFBwMBMA4GA1UdDwEB/wQEAwIDKDBgkq
hkiG9w0BAQUFAAOCACAEAwXb5/4NzL3Fsa4FrXB73mWBKZrggrT6n0Mp30WP7R9a9
tqIs44HS2NohdKu1j7HT9G0m0MJ9doZRD0PttaIumdGuRi2owoWFK8MsLSPWyCBD
u8puNkJ9T61qT0ZJlGH0Nihjau1XLxY0vXTCUvuvDULYXrLsFd1zcHwg0mdUTWWf
+vdDGYRbMY495TukUsMKooo5JMansMzJ4wy2FUBTH2qBPcFuzBwu9aSuIdxJ0pTU
zm3QvNXN4UWZ2duc1n9e7xokr5wgiDiIgbqsc1H20rwi4uZe+gmge2iJX1uyUQ+
8a6zURmz3YamiPTB0chWmpPCKRkk/SKORb16XwN0Lw==
-----END NEW CERTIFICATE REQUEST-----

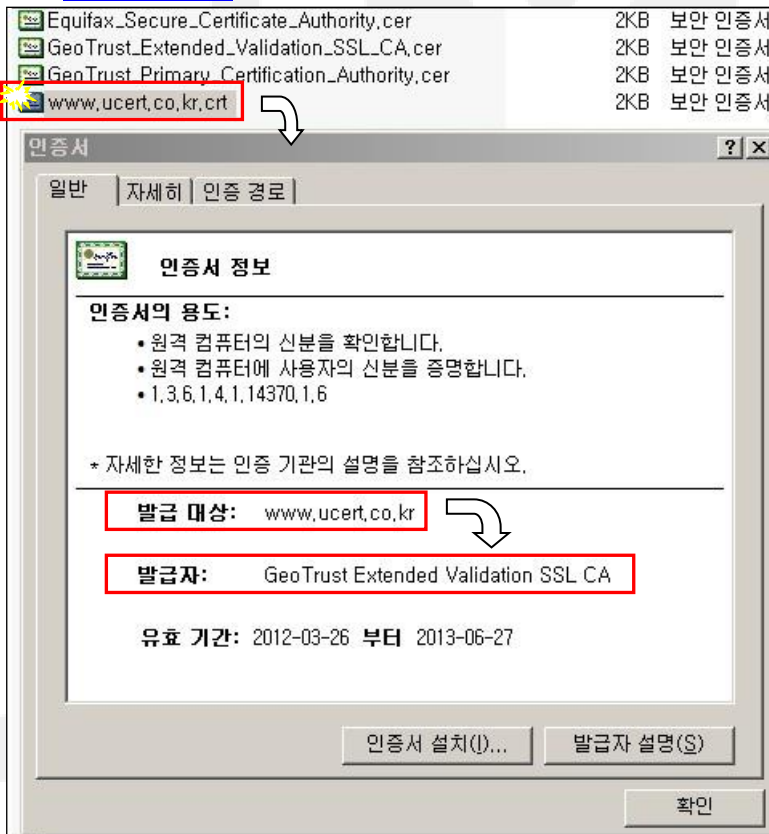
```

#### 4. SSL 인증서 확인

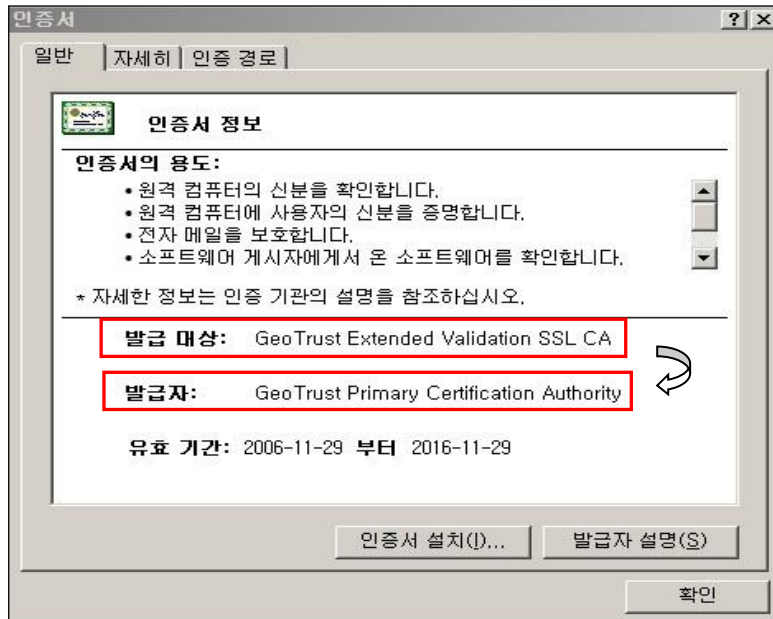
##### 1) 받은 인증서를 더블 클릭하여 확인합니다.

※ 인증서 상품별로 파일명이 달라질 수 있습니다.

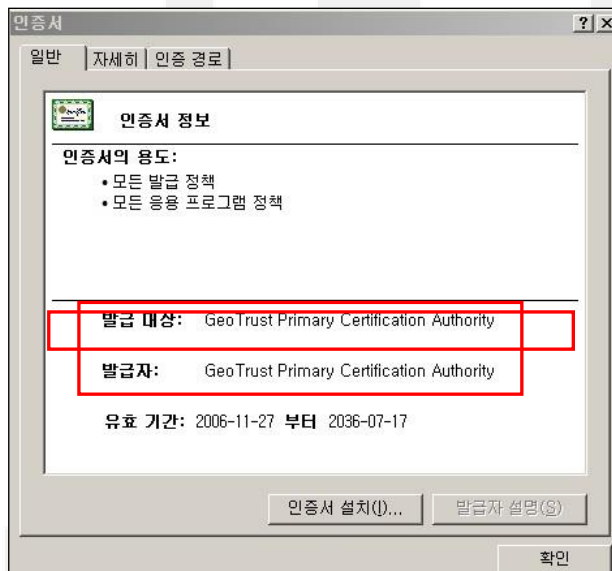
① [www.ucert.co.kr](http://www.ucert.co.kr) 의 발급 CA는 Geotrust Extended Validation SSL CA 임을 확인



② Geotrust Extended Validation SSL CA를 더블 클릭하여 발급자 확인 (ChainCA 인증서임을 확인)



- ③ Geotrust Primary Certificate Authority 의 발급자 확인  
(자기 자신이 서명한 인증서이므로 최상위 Root CA인증서임을 확인)



인증서 설치 시 Root CA -> Chain CA -> 도메인 인증서 순으로 설치 하게 되므로 어느 인증서가 Root CA 이며 Chain CA인지 파악해 둔 후 메모장이나 워드패드로 열어 코드 값을 붙여 넣거나 가지고 오도록 합니다.

www.ucert.co.kr

## 5. 서버 인증서 설치 (도메인 인증서)

### 1) 설치를 클릭합니다.

### 2) 패스워드 입력합니다. (패스워드 생성하지 않았다면 다음을 선택합니다)

### 3) 받은 인증서를 워드 패드 혹은 메모장으로 열어 복사 후 인증서 데이터에 붙여 넣습니다.

4) 별명을 입력 후 SSL Listener를 선택 후 “다음”을 클릭합니다.


서버 인증서 설치 마법사

단계	도움말	단계 3:인증서 세부 정보
1. 토큰 및 비밀번호 선택		<p>자체 서명 유형인 경우에는 별명, 유효 기간(개월) 및 보안 요청을 커 입력합니다.</p> <p>* 필수 필드 표시</p> <p>* 별명: <input type="text" value="cert"/></p> <p>Listener: <input type="text" value="http-listener-2"/></p>
2. 인증서 데이터 입력		
→ 3. 인증서 세부 정보		
4. 검토		
5. 결과		

서버 인증서 설치 마법사

단계	도움말	단계 4:검토
1. 토큰 및 비밀번호 선택		<p>여기에서 설정을 검토하십시오. 계속하려면 마침을 누릅니다.</p> <p>구성: Korsec</p> <p>별명: cert</p> <p>토큰: internal</p> <p>수신기: http-listener-2</p> <p>인증서 세부 정보</p> <p>주제: CN=www.ucert.co.kr,OU=KCS,O=Dev Team,L=Seocho-gu,ST=Seoul,C=KR</p> <p>발급자: E=ucert@ucert.co.kr,CN=Korea Corporation Security (www.ucert.co.kr),OU=UCERT,O=Korea Corporation Security,L=Seocho-gu,ST=Seoul,C=KR</p> <p>키 유형: RSA</p> <p>키 크기: 2048</p> <p>유효 기간: Mon Sep 24 19:02:18 KST 2012</p> <p><input type="button" value="이전"/> <input type="button" value="마침"/></p>
2. 인증서 데이터 입력		
3. 인증서 세부 정보		
→ 4. 검토		
5. 결과		

서버 인증서 설치 마법사

단계	도움말	단계 5:결과
1. 토큰 및 비밀번호 선택		<p>서버 인증서 설치 결과</p> <div style="border: 2px solid red; padding: 10px; text-align: center;"> <p> <b>Installation of Certificate</b></p> <p>successful</p> </div>
2. 인증서 데이터 입력		
3. 인증서 세부 정보		
4. 검토		
→ 5. 결과		

5) 성공했다고 나왔지만 서버 인증서 란에는 인증서가 없습니다. 비밀번호 설정을 클릭합니다.

**Korsec - 구성 서버 인증서**

인증서는 개인, 회사 또는 기타 엔티티의 이름을 지정하는 디지털 데이터로 구성되며 인증서에 포함된 공용 키는 해당 엔티티에 속한다는 것을 인증합니다. SSL 사용 서버에는 인증서가 있어야 하고 클라이언트는 필요에 따라 인증서를 가질 수 있습니다. 이 페이지에서 서버 인증서를 요청, 설치, 갱신 및 삭제할 수 있습니다.

**서버 인증서 (0)**

요청... 설치... 갱신... 삭제... | 필터: 모든 항목

별명	발급자	토큰	만료일
인증서를 찾을 수 없습니다. 필터가 적용되어 이 테이블의 일부 열이 숨겨져 있을 수 있습니다. 모든 열을 표시하려면 필터 목록에서 '모든 항목'을 선택합니다.			

**구성 토큰 비밀번호 설정**

아래 테이블을 사용하여 보안 토큰에 대한 비밀번호를 설정합니다. "확인"을 눌러 구성 토큰에 대한 비밀번호를 저장합니다.

**보안 토큰 (1)**

구성	토큰	비밀번호
Korsec	internal	●●●●

**확인** **닫기**

6) 인증서를 확인합니다

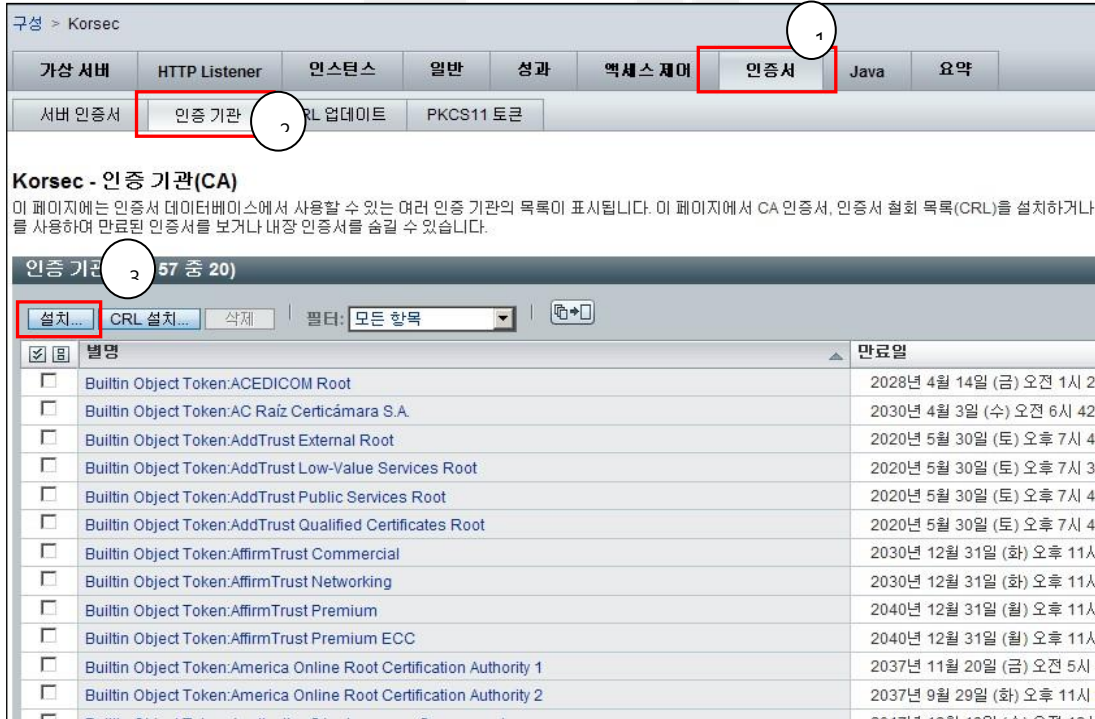


## 6. CA 인증서 설치

### 1) 해당 서버의 구성편집 -> 인증서로 이동합니다.



### 2) 인증서 탭으로 이동 후 인증기관 선택 후 "설치"를 클릭합니다.



### 3) CA 인증서 설치 마법사 실행되면 "다음" 후 최상위 Root 인증서 코드를 삽입합니다. 혹은 해당 파일 위치 및 파일명을 입력합니다.





- 4) 최상위 Root 이므로 CA 인증서를 선택 후 다음으로 선택합니다. (Chain CA는 인증서 체인 선택)



CA 인증서 설치 마법사

단계: 도움말 단계 3:인증서 유형

1. 토른 및 비밀번호 선택  
2. 인증서 데이터 입력  
→ 3. 인증서 유형  
4. 검토  
5. 결과

설치할 인증서의 유형을 선택합니다.

인증서 유형  
☒ CA 인증서  
☐ 인증서 체인

이전 다음 취소

- 5) 정보 확인 후 마침을 클릭 후 단기를 클릭하여 완료합니다.



CA 인증서 설치 마법사

단계: 도움말 단계 4:검토

1. 토른 및 비밀번호 선택  
2. 인증서 데이터 입력  
3. 인증서 유형  
→ 4. 검토  
5. 결과

여기에서 설정을 검토하십시오. 계속하려면 마침을 누릅니다.

구성: Korsec  
토른: internal  
인증서 유형: CA 인증서

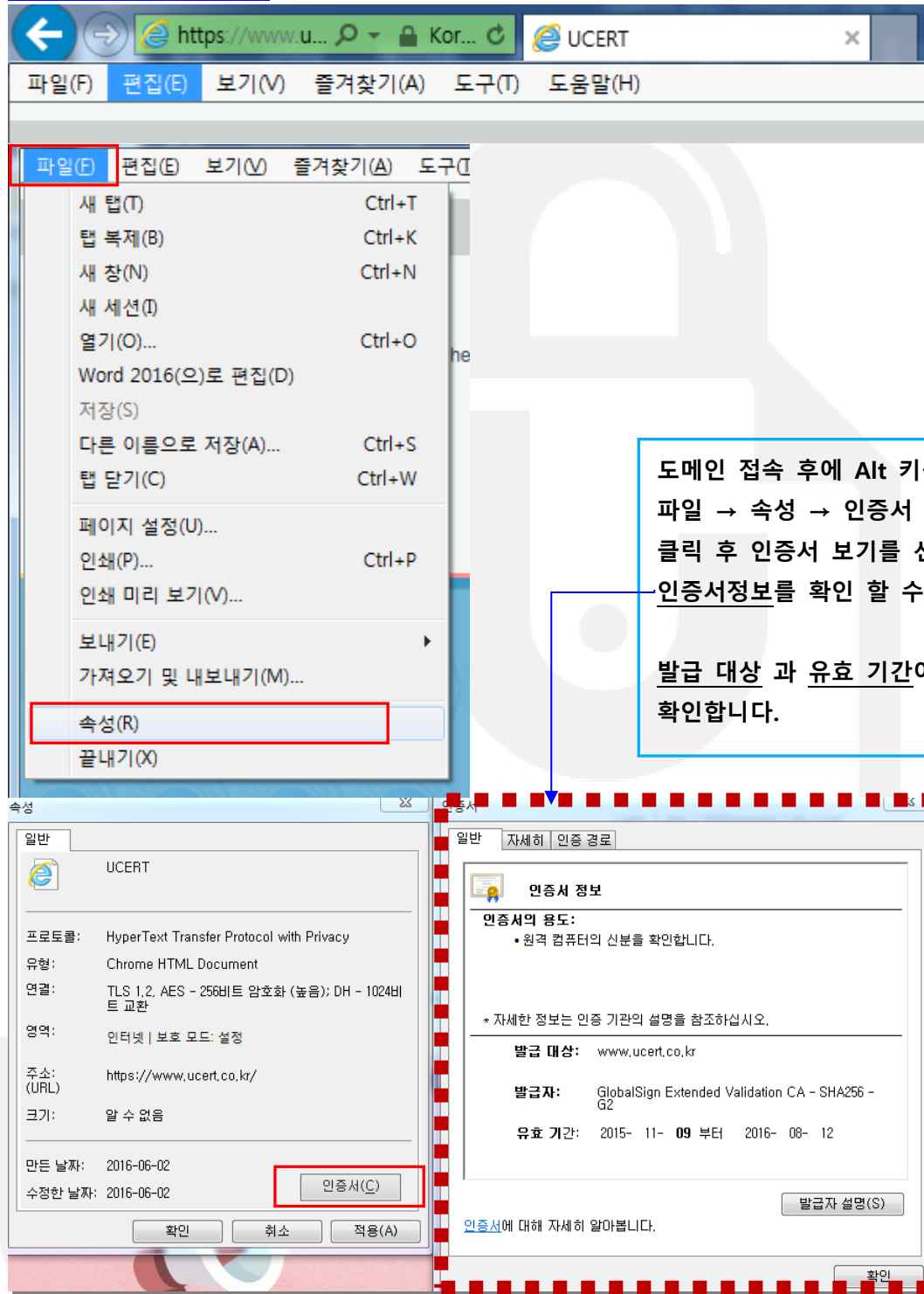
주제: CN=GeoTrust Primary Certification Authority,O=GeoTrust Inc.,C=US  
발급자: CN=GeoTrust Primary Certification Authority,O=GeoTrust Inc.,C=US  
키 유형: RSA  
키 크기: 2048  
유효 기간 시작일: Mon Nov 27 09:00:00 KST 2006  
유효 기간 종료일: Thu Jul 17 08:59:59 KST 2036  
알련 번호: 18:AC:B5:6A:FD:69:B6:15:3A:63:6C:AF:DA:FA:C4:A1  
핑거 프린트: 02:26:C3:01:5E:08:30:37:43:A9:D0:7D:CF:37:E6:BF

이전 마침 취소

- 6) 위와 같은 방법으로 Chain CA도 설치 합니다.

(SSL 인증서 확인가이드에서 나온 모든 Chain CA를 설치합니다.)

<https://www.ucert.co.kr> 접속 예



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.