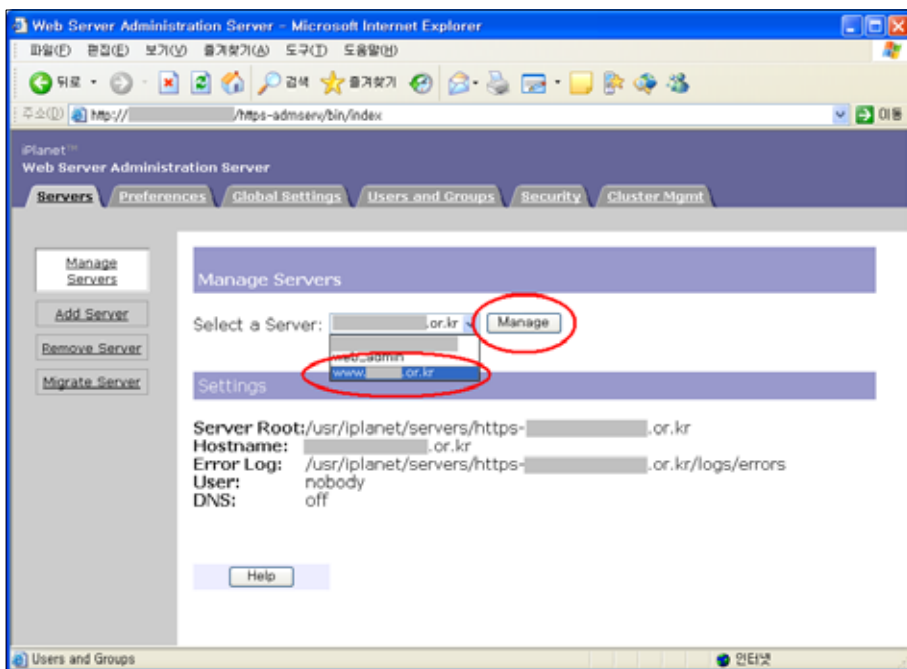


2.4 iPlanet 서버에서 보안서버 구축하기

가. 개인키 생성 및 CSR 생성 방법

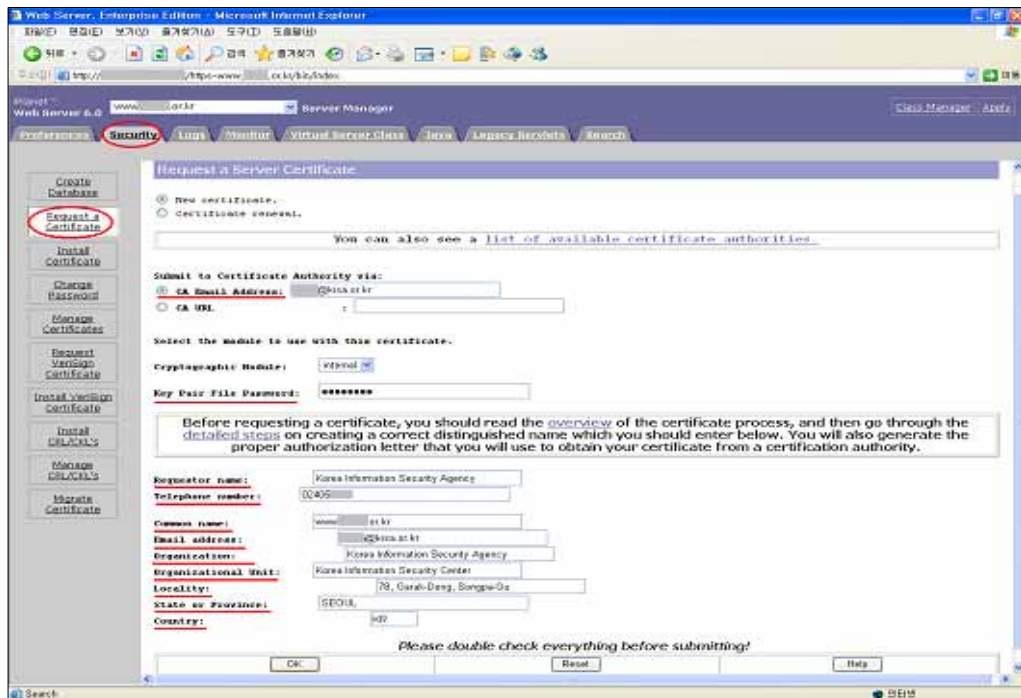
① 서버관리 화면에서 서버 선택

서버관리 화면의 콤보박스에서 보안서버를 구축하고자 하는 웹 서버를 선택하고 "Manage" 버튼을 누릅니다.



② CSR 생성을 위한 정보 입력

Security Tab을 누르고 왼쪽 메뉴에서 "Request a Certificate"를 선택하여 필요한 정보를 입력한 후 "OK" 버튼을 선택합니다.



입력해야 할 정보는 다음과 같습니다. (그림의 빨간색 밑줄 참고)

- CA Email Address : 관리자의 이메일 주소
- Key Pair File Password : 관리 패스워드
- Requestor Name : Korea Information Security Agency
- Telephone Number : 관리자의 전화번호
- Common Name : 웹서버의 주소
- Email Address : 관리자의 이메일 주소
- Organization : 회사명(Full Name 입력)
- Organizational Unit : 부서명
- Locality : 주소
- State or Province : 도시명
- Country : KR(대한민국)

③ CSR 생성

‘OK’ 버튼을 선택하면 다음과 같은 정보가 생성됩니다. CSR 내용을 인증기관에게 메일로 송부하거나 인증서 신청화면에 붙여 넣으신 후 인증서 신청을 진행하시면 됩니다.

인증기관의 발급 절차에 따라서 인증서가 발급됩니다.

```

Your certificate request has been sent.
When the response arrives, you can use the Install Certificate page to put it in place.
A copy of the certificate request has been saved in the file:
/tmp/mailtmp.18623

To: @kisa.or.kr
Subject: Certificate request
Email: @kisa.or.kr

Webmaster: @kisa.or.kr
Phone: 02405

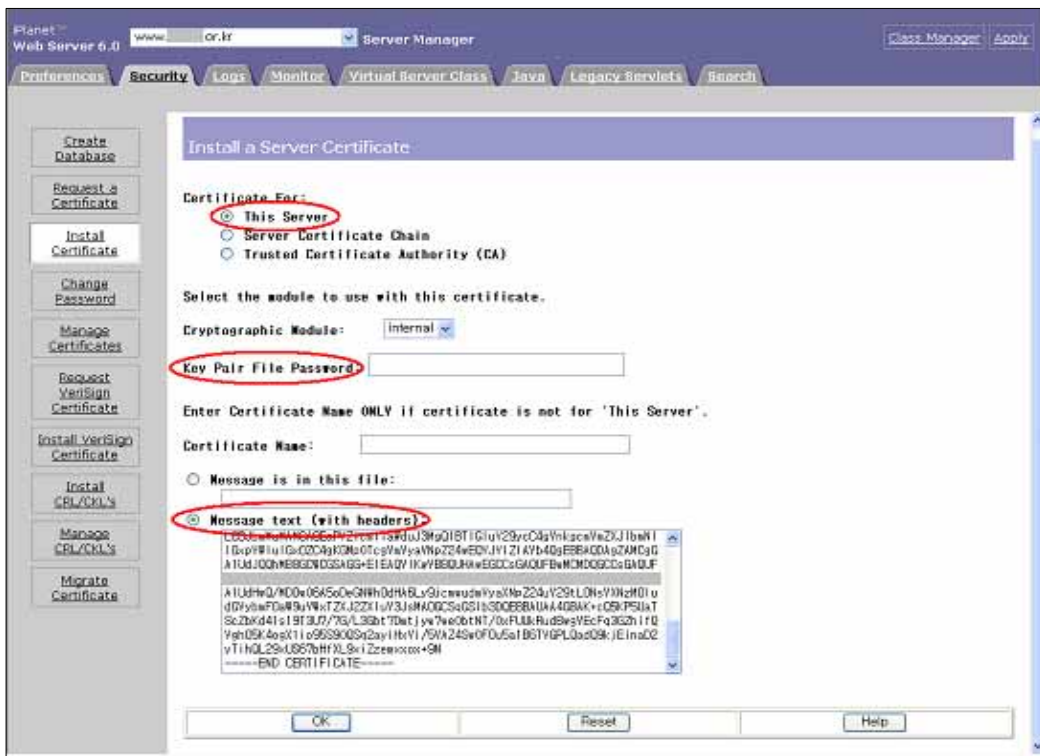
Common-name: www. .or.kr
Email: @kisa.or.kr
Organization: Korea Information Security Agency
Org-unit: Korea Internet Security Center
Locality: 78, Garak-Dong, Songpa-Gu
State: SEOUL
Country: KR

-----BEGIN NEW CERTIFICATE REQUEST-----
MIIB8jCCAUsCAQAwgExCzAJBgNVBAYTaktSMQ4wDAYDUQQIEwUTRU9UTDEiMCAG
A1UEBxMZNzgsIEEdhcncFrLURvbmc5IFNobmdwYS1HdTEqMCgGA1UEChMsS29yZWEG
SM5mb3JtYXRpb2gU2UjdXJpdHkgQWdlbmN5SHScwJQVUQQLEx5L3JlYSBjb3R1
cm51dCBTZWVncml0eSB0ZS02X1xGTAXBgNVBAMTEHd3dy5rcmNlcnQub3Iua3Iw
gZBwDQYJKoZIhvcNAQEBBQADgYQAMIGJAoGBALFKqpG1inUdrqWwUTO0yc7w0kuv
G2rnfUHonEazWwKGHjGF1ue48m4SuxJyoo1ESAhtv6HoHbw3w7xsEgK0aC9QUKRZ
rFUNPb1UAEAtunphAgHBAAGGADANBgkqhkiG9w0BAQQFAA0BgQCChDN7KiFT5+1ak
hwNsyAzPirklvKogSHyz10sVniEHUvF48jCEa7wL19dTkTf+r1268p569o2jyBEy
9Nd1cYndTLc8HIJp+ucg9Zr2/hr+0ySRAMSaphk5SP/Ln0Ir1hpEurLF0xtHZycC
Izrycu6KwFHUCk1qUoaBap1abQeAAQ-----
-----END NEW CERTIFICATE REQUEST-----

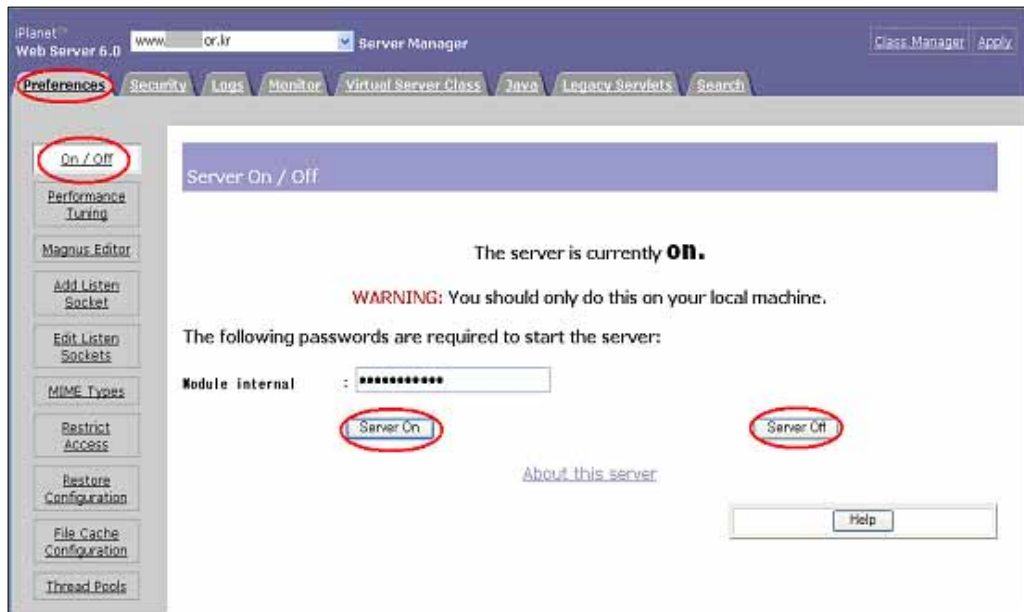
```

나. 인증서 설치 방법

- ① Server Certificate를 iPlanet 웹 서버에 설치
 - 관리자 화면에서 Security -> Install a Certificate를 선택한 후, 아래 화면에서 빨간색 표시 된 부분의 정보를 채워 넣습니다.

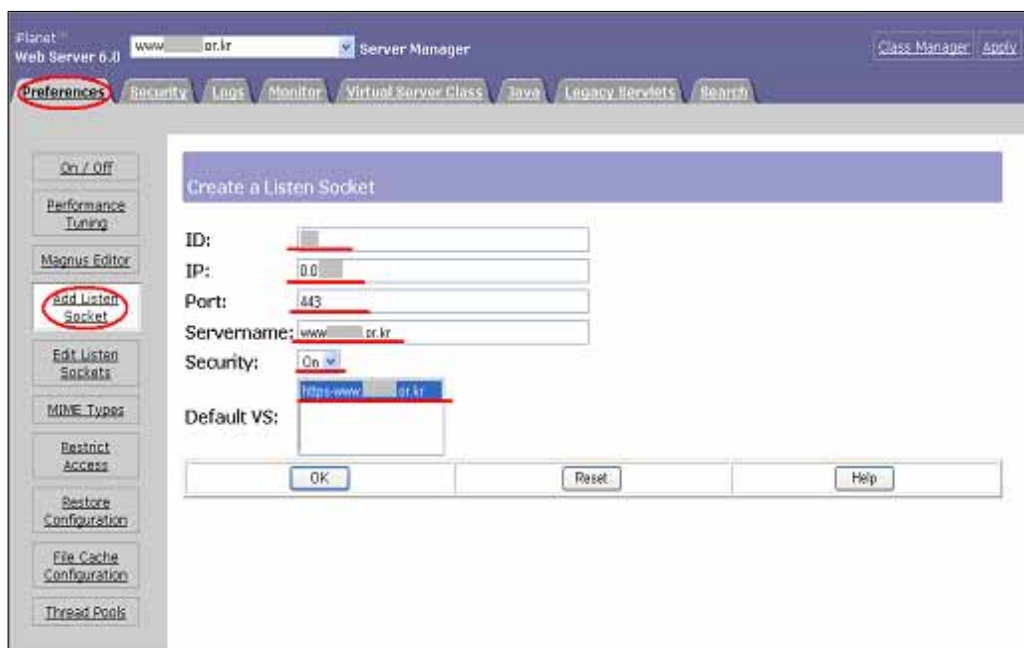


② iPlanet 웹 서버를 재시작(Server Off → Server On)



③ iPlanet 웹 서버 설정 변경

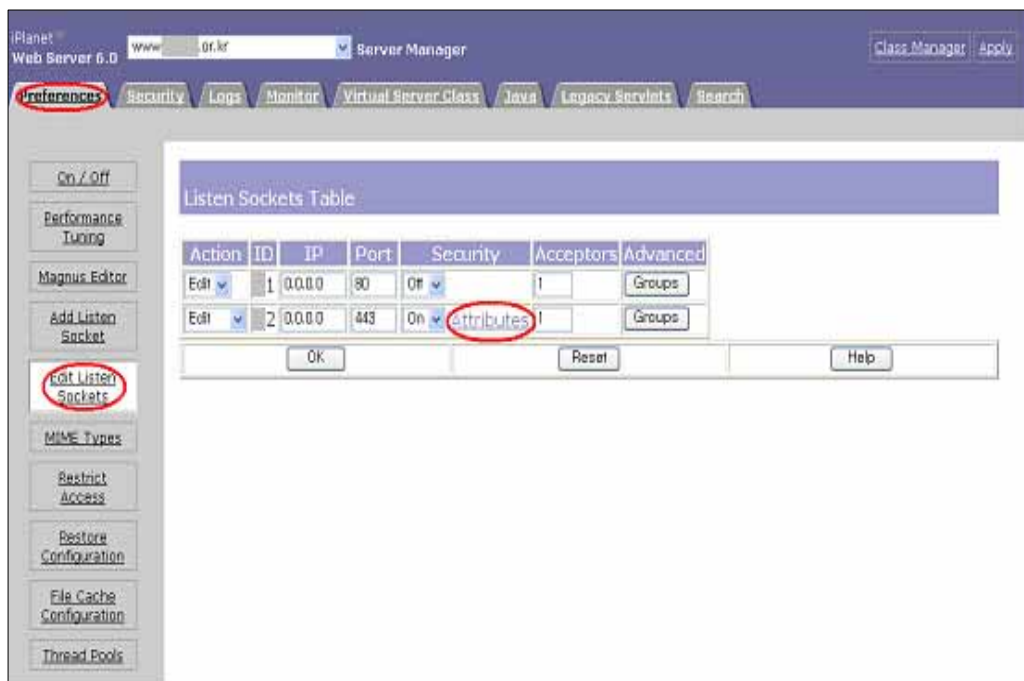
iPlanet서버에 인증서를 설치 완료했다면, 서버에서 443 포트에 대하여 대기(Listen)할 수 있도록 설정을 변경해야 합니다. 웹서버 관리자 화면에서 Preference → Add Listen Socket을 선택하여 아래와 같이 정보를 입력한 후 'OK'를 선택합니다.

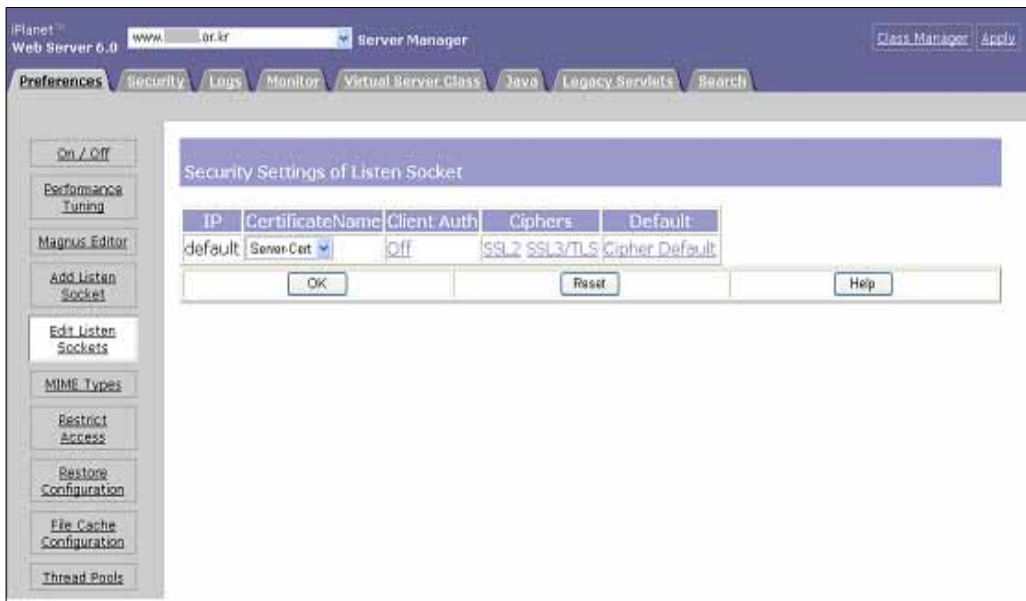


- 입력해야 할 정보는 다음과 같습니다. (그림의 빨간색 밑줄 참고)
- ID : 이전 80포트에 대한 ID를 참고하여 SSL 포트를 위한 ID를 부여
 - IP : 0.0.0.0 / any 로 설정
 - Port : 443, SSL 포트는 443이 디폴트 포트이며, 서버 관리자와 상의하여 다른 포트를 사용하도록 설정 변경도 가능
 - Servername : 웹서버명
 - Security : 'On' 선택
 - Default VS : 디폴트로 사용할 Virtual Server url을 입력

④ iPlanet 웹 서버 설정 추가변경

SSL에 대한 443 Listen 기능을 입력한 후, 추가로 설정해야 할 부분이 있다면 동일 화면에서 "Edit Listen Sockets"를 선택한 후 "Attributes" 링크를 클릭하여 수정합니다. 이 화면에서 SSL2, SSL3/TLS에 대한 설정을 변경하거나 iPlanet 기본 설정값으로 리셋할 수 있습니다.





- ⑤ 이제 SSL 인증서의 설치가 완료되었습니다. VI장으로 이동하셔서 실제 웹 페이지를 어떻게 수정해야 하는지 알아보겠습니다.

2.5 체인 인증서 설정하기

국산 인증서의 경우 2006년 2월에 인터넷 익스플로러(IE) 브라우저의 신뢰된 루트 인증기관으로 등록되었으며 Windows XP SP2 버전 이상부터 IE 브라우저에 적용되었습니다.

Windows XP SP2 버전 이상부터는 국산인증서가 신뢰된 기관에서 발급받은 인증서로 인식되기 때문에 경고창 등의 문제점이 없이 사용이 가능하지만 그 이하 버전에서는 신뢰된 인증기관이 아닌 곳에서 발급 받은 인증서로 인식하기 때문에 '3. 오류 발생시 대처방법' 내용 중 ③번과 같이 브라우저가 웹 서버를 신뢰하지 못하는 경고 메시지가 나타납니다.

그렇기 때문에 Windows XP SP2 버전 이상을 사용하지 않는 사용자는 브라우저에 국산인증서의 체인 인증서를 강제적으로 신뢰된 루트 인증기관으로 설치해야만 브라우저에서 신뢰된 인증서로 인식하여 정상적으로 사용이 가능합니다.