

IIS(Windows Server) 보안서버인증서 설치 가이드

보안서버인증서 구성파일 안내

Private.key	개인키 (후이즈에 CSR 생성을 요청하신 경우에만 제공됩니다)
도메인명_cert.pem	보안서버인증서 (CRT 파일)
ChainCA.crt	체인인증서
RootCA.crt	루트인증서
CSR.pem	CSR (인증서 신청 시 사용된 CSR 값)

예스닉 보안서버인증서는 기본적으로 PEM 형식으로 제공되고 있으며, IIS 서버에 인증서를 설치하는 경우 PFX 형식의 인증서 파일이 필요합니다.

제공된 PEM 형식의 인증서를 서버에 업로드 하고, 아래 단계를 통해 PFX 형식으로 변환합니다. (openssl 필요)

```
cat 도메인명_cert.pem ChainCA.crt RootCA.crt > 도메인명_bundle.pem
openssl pkcs12 -export -name 도메인명 -in 도메인명_bundle.pem -inkey Private.key -out 도메인명.pfx
```

IIS서버에서 '인증서 요청 만들기'를 통해 CSR을 생성하여 인증서를 신청하셨다면, PFX 형식의 인증서로 변환하지 않고 4페이지에 있는 PEM 형식의 인증서 설치방법을 참고하여 설정합니다.

서버에 openssl 이 설치되어 있지 않거나 직접 변환하기 어려운 경우,

[1:1 친절상담](#)이나 [메일](#)로 PFX 형식의 인증서 파일을 요청하세요.

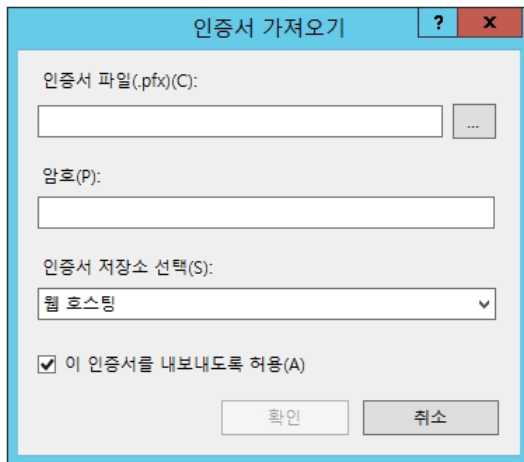
(openssl로 CSR을 생성하신 경우엔 개인키와 개인키 비밀번호를 첨부하여 요청해 주세요.)

1. PFX 형식의 인증서 파일 설치하기

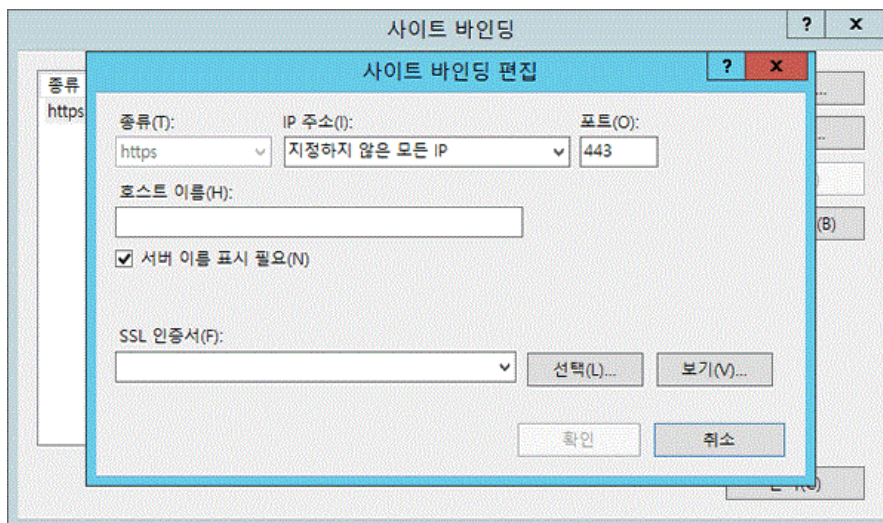
PFX 형식의 인증서 파일을 IIS 서버 내 임의의 인증서 폴더에 업로드 하고, 아래 내용을 참고하여 설정합니다.

1) IIS 7.X 서버 이상

- (1) IIS 관리자 > 중앙에서 '서버인증서' > 오른쪽 탭에 '가져오기' 클릭
 - > 업로드한 인증서 파일 선택하고, 인증서 비밀번호 입력, 인증서 저장소 선택(기본값: 웹 호스팅)
 - > 하단 [확인] 클릭하여 가져오기 완료



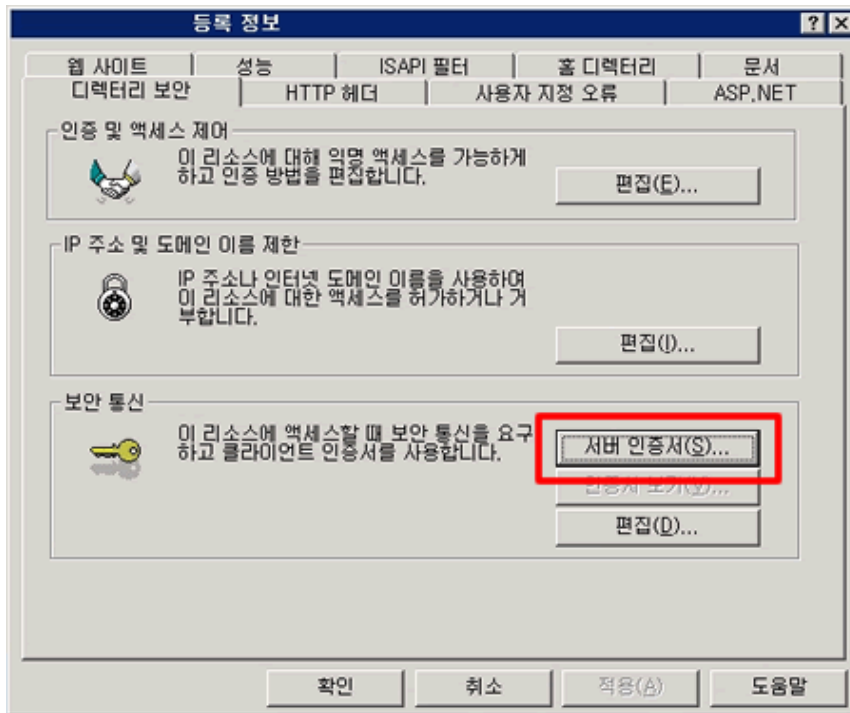
- (2) IIS 관리자 > 왼쪽 탭에 인증서를 적용할 웹사이트 선택 > 오른쪽 탭에 바인딩 선택 > 추가(갱신은 편집) 클릭
 - > IP주소와 포트를 지정한 후 SSL 인증서 부분에 설치한 인증서 이름 선택 > 하단 [확인] 클릭하여 완료



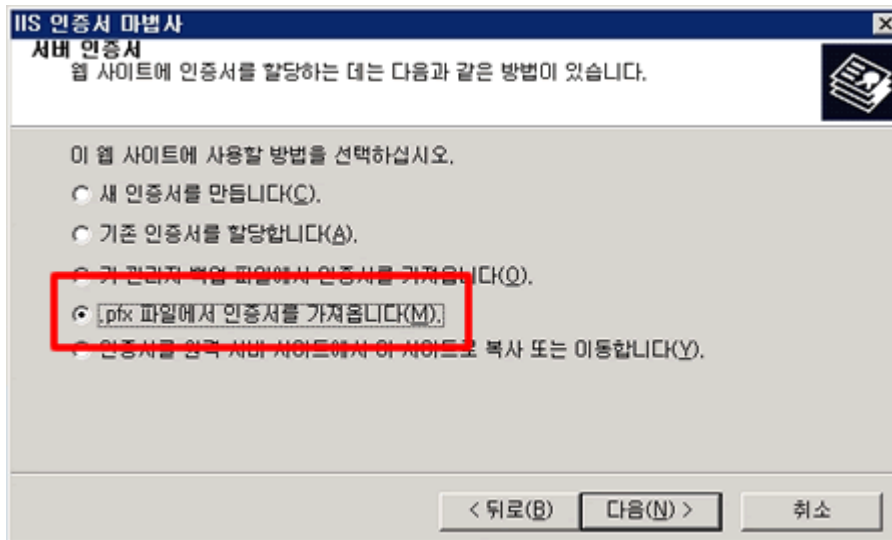
- (3) IIS 서버 재시작 하여 정상적으로 구동되는지 확인 후, https:// 로 인증서가 적용되었는지 확인합니다.

2) IIS 6.X 서버 (TLS 1.2 이상을 지원하는 Windows 2008 서비스팩2 이상만 설치 가능합니다.)

- (1) IIS 관리자 > 왼편 탭에 인증서를 설치할 웹사이트에 우클릭 > 메뉴에서 '속성' 선택
> '디렉토리 보안' 탭 선택 > '보안 통신' 에 [서버 인증서] 선택



- (2) '.pfx 파일에서 인증서를 가져옵니다.' 선택하고 하단 [다음] 클릭
> [찾아보기]로 업로드한 인증서 선택하고 하단 [다음] 클릭 > 비밀번호 입력하고 가져오기 완료
(**'현재 인증서 할당 수정'** 메뉴가 표시되면, **'현재 인증서를 제거합니다.'** 하고 위 단계를 진행합니다.)



- (3) IIS 서버 재시작 하여 정상적으로 구동되는지 확인 후, https:// 로 인증서가 적용되었는지 확인합니다.

2. PEM 형식의 인증서 파일 설치하기

openssl 로 CSR을 생성하신 경우에는 첫 페이지를 참고하여 PFX 형식의 인증서로 변환하여 진행합니다.

'인증서 요청 만들기' 를 통해 CSR을 생성하여 인증서를 신청하셨다면,

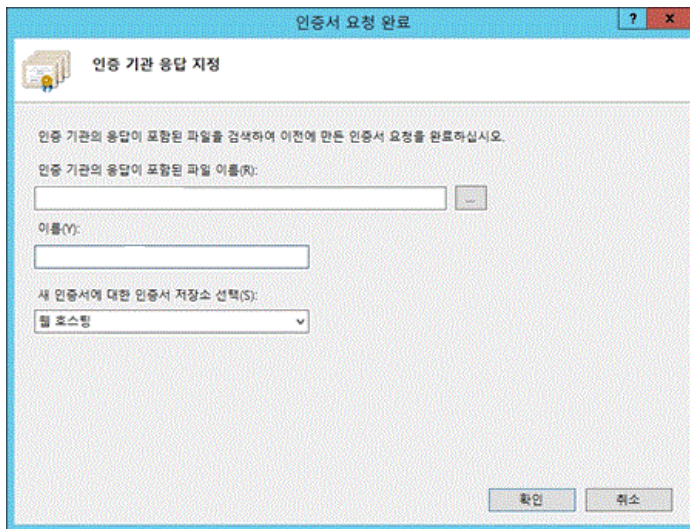
IIS 서버 내 임의의 인증서 폴더에 기본 제공된 인증서 파일을 모두 업로드 하고, 아래 내용을 참고하여 설정합니다.

1) IIS 7.X 서버 이상

IIS 관리자 > 중앙에서 '서버인증서' > 오른쪽 탭에 '인증서 요청 완료' 클릭

> 업로드한 인증서 파일(*도메인명.crt.pem*)을 선택하고, 이름 및 인증서 저장소 설정(기본값: 웹 호스팅)

> 하단 [확인] 클릭하여 인증서 요청 완료하기

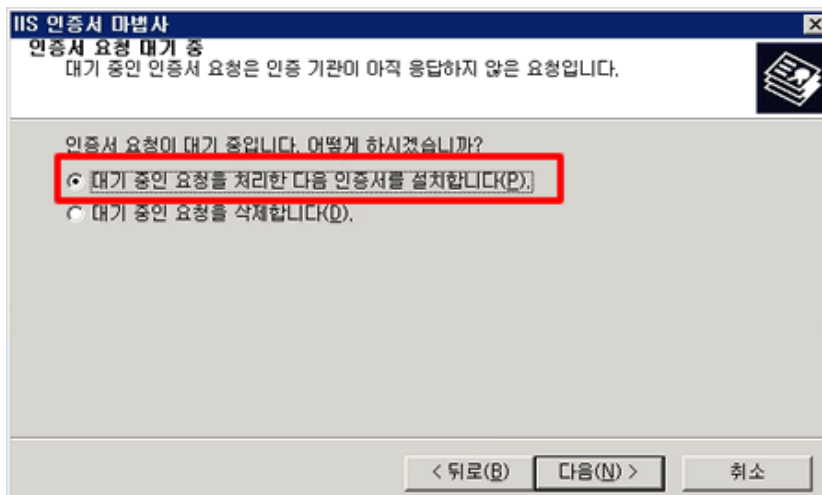


2) IIS 6.X 서버

IIS 관리자 > 중앙에서 '서버인증서' > 오른쪽 탭에 '인증서 요청 완료' 클릭

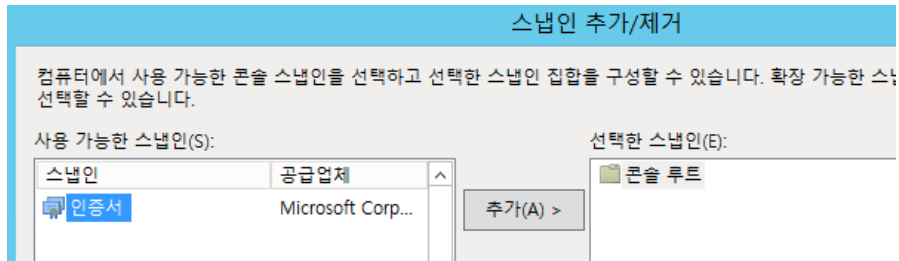
> 업로드한 인증서 파일(*도메인명.crt.pem*)을 선택하고, 이름 및 인증서 저장소 설정(기본값: 웹 호스팅)

> 하단 [확인] 클릭하여 인증서 요청 완료하기



3) 루트 및 체인인증서 적용 과정 (IIS서버 최신 업데이트가 되었거나, 인증서 갱신이면 생략 가능합니다.)

- (1) 시작 메뉴 > 실행 클릭 > 프롬프트에서 mmc 입력 > 열린 창에서 상단 메뉴바에 '파일' 클릭 > '스냅인 추가/제거' 클릭 > 왼편 '사용 가능한 스냅인' 에서 인증서 선택하고 중앙 [추가] 클릭 > '컴퓨터 계정' 선택하고 [다음] 클릭 > '로컬 컴퓨터' 선택하고 하단 [마침] 클릭 > 하단 [확인] 클릭



- (2) 콘솔 루트 > 인증서 > 중간 인증 기관 > 인증서 에 우클릭 > 모든 작업 > 가져오기 클릭 > ChainCA.crt 파일 선택 > [열기] > [다음] 진행하여 완료
- (3) 콘솔 루트 > 인증서 > 신뢰할 수 있는 루트 인증 기관 > 인증서 에 우클릭 > 모든 작업 > 가져오기 클릭 > RootCA.crt 파일 선택 > [열기] > [다음] 진행하여 완료

4) IIS 서버 재시작 하여 정상적으로 구동되는지 확인 후, https:// 로 인증서가 적용되었는지 확인합니다.

적용 과정에 오류가 있는 경우 오류내용, 로그, 스크린샷 등을 첨부하여 [1:1 친절상담](#)이나 [메일](#)로 문의해 주세요.