

Windows Server 2008

IIS7

(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



한국기업보안
Korea Corporation Security

※ 이 문서는 일반적인 설정이며 서버 및 네트워크 환경에 따라 달라질 수 있습니다.

인증기관 별 Root & Chain 인증서 구분 방법입니다.

※ 발급 받은 인증서를 아래 표를 참고하여 Root 및 Chain 인증서를 구분 합니다.

[GlobalSign] - 인증기관

설정구분	인증서 형식
중간 인증 기관	GLOBALSIGN_RSA_DV_SSL_CA_2018.crt [DV] GLOBALSIGN_RSA_OV_SSL_CA_2018.crt [OV] ALPHASSL_CA_SHA256_G2.crt [Alpha] GLOBALSIGN_EXTENDED_VALIDATION_CA_SHA256_G3.crt [EV] GLOBALSIGN.crt
신뢰할 수 있는 루트 인증 기관	GLOBALSIGN Root CA.crt

[Comodo] - 인증기관

설정구분	인증서 형식
중간 인증 기관	SECTIGO_RSA_DOMAIN_VALIDATION_SECURE_SERVER_CA.crt USERTRUST_RSA_CERTIFICATION_AUTHORITY.crt
신뢰할 수 있는 루트 인증 기관	AAA Certificate Services.crt

[Digicert] - 인증기관

설정구분	인증서 형식
중간 인증 기관	THAWTE_RSA_CA_2018.crt
신뢰할 수 있는 루트 인증 기관	DIGICERT_GLOBAL_ROOT_CA.crt

www.ucert.co.kr

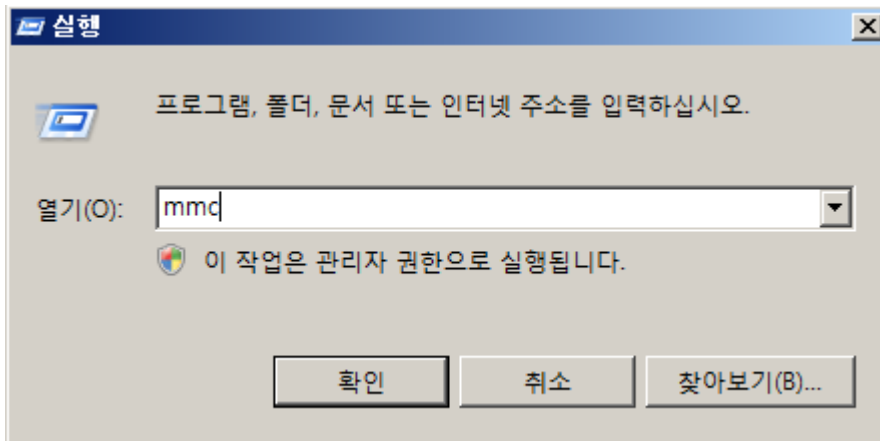


본 문서는 주식회사 한국기업보안에서 SSL보안서버인증서 설치를 위해 작성된 문서로
주식회사 한국기업보안의 동의 없이 무단으로 사용하실 수 없습니다

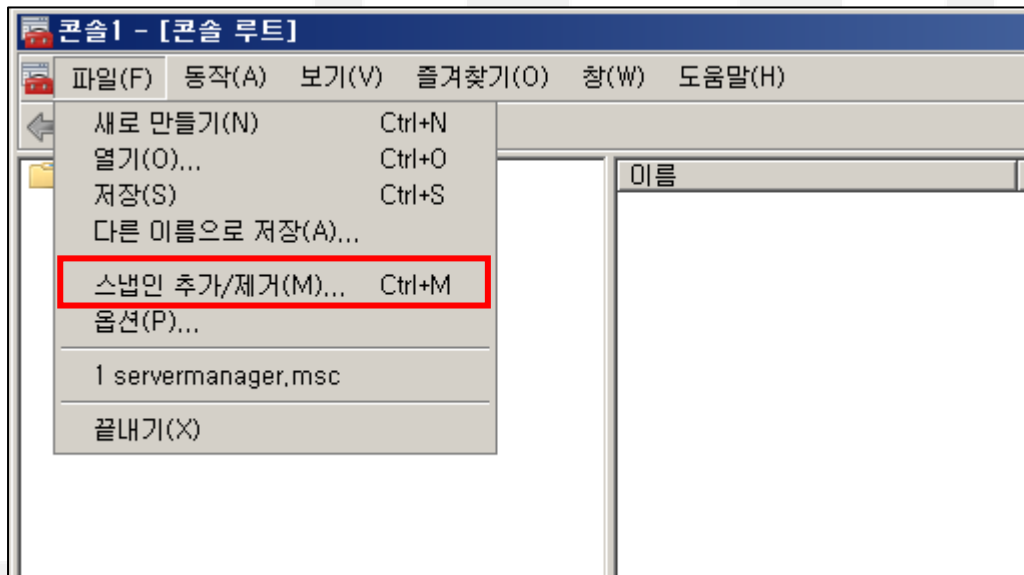
Copyright 2018-2023. Korea Corporation Security Co., Ltd All pictures cannot be copied without permission.

1. 인증서 가져오기

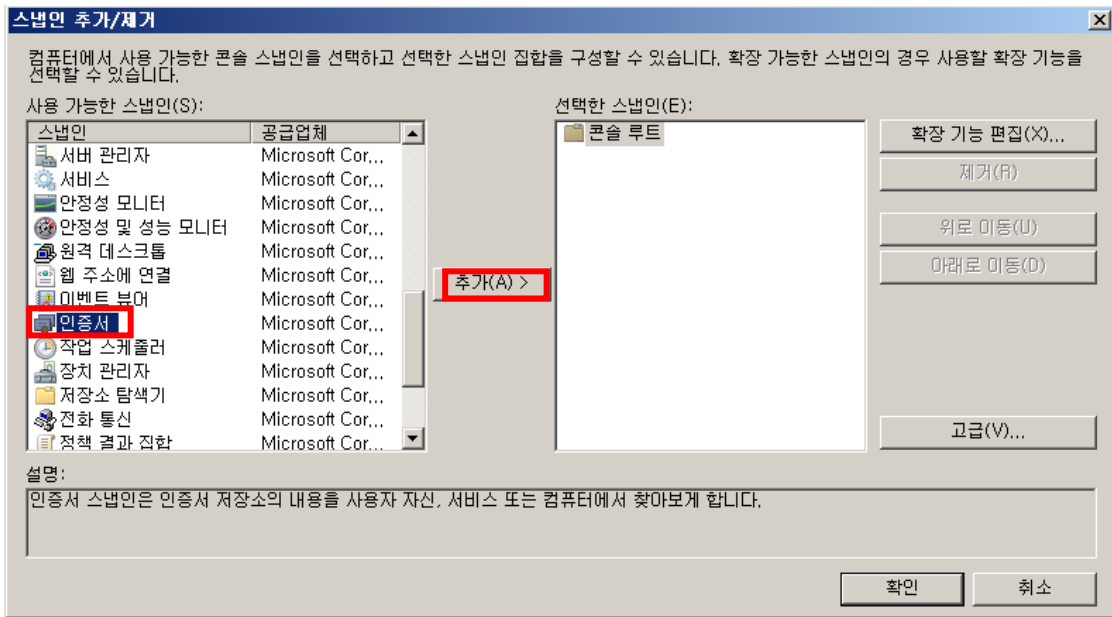
- 1). "실행" 창을 실행하여 MMC 를 실행 합니다. [Windows 키 + R 키 > mmc]



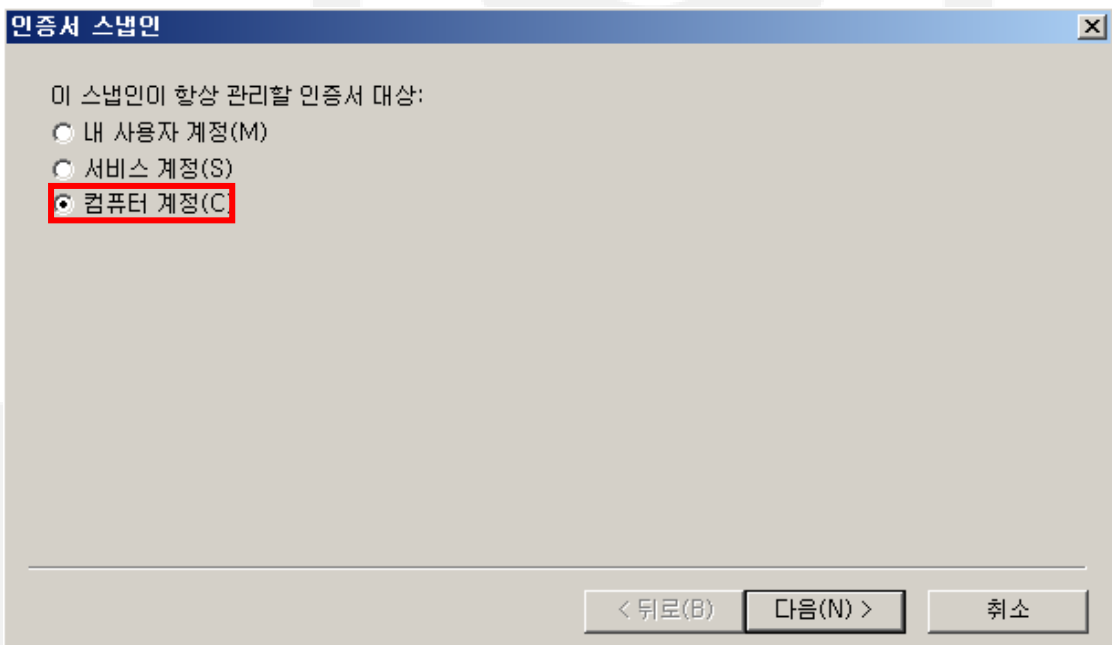
- 2). 파일 > 스냅인 추가/제거를 선택합니다.



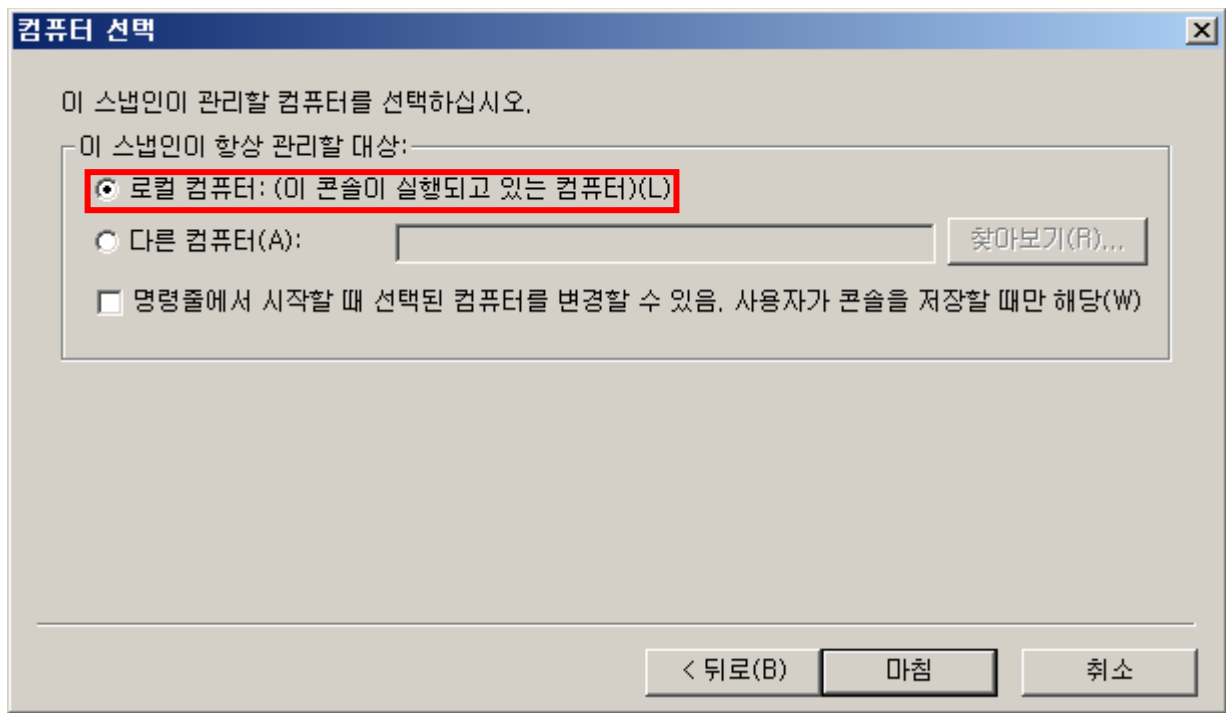
3). 인증서 스냅인을 추가합니다.



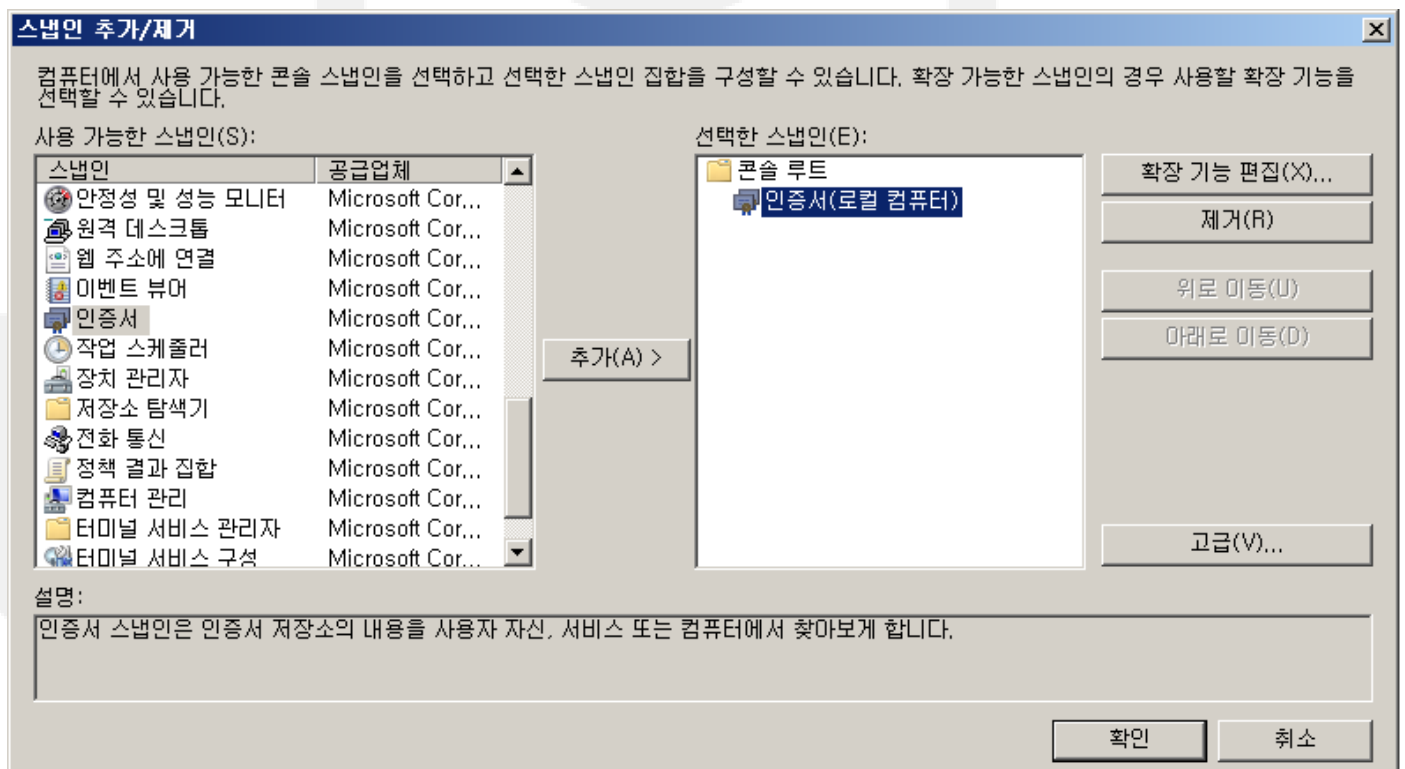
4). 컴퓨터 계정을 선택합니다.



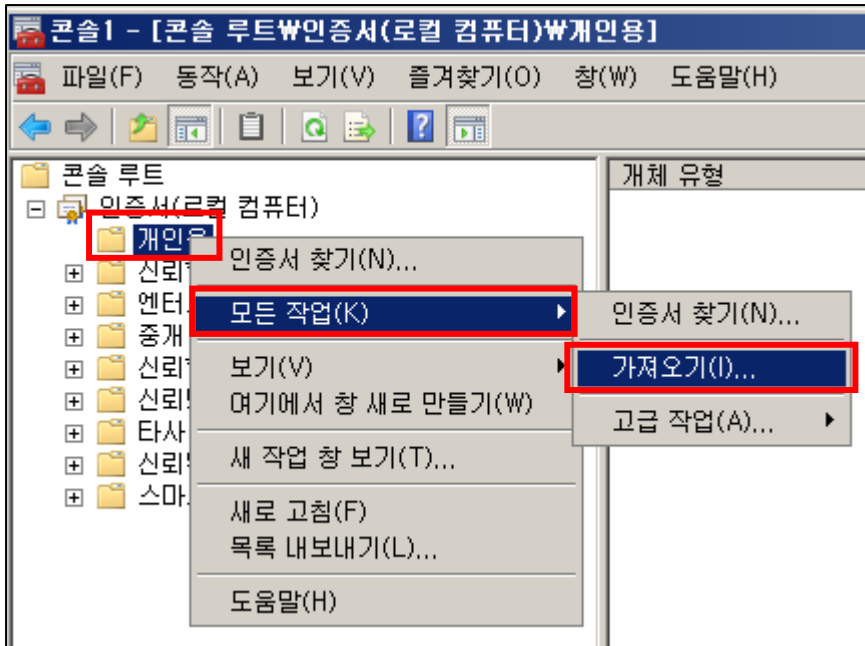
5). 로컬 컴퓨터를 선택하도록 합니다.



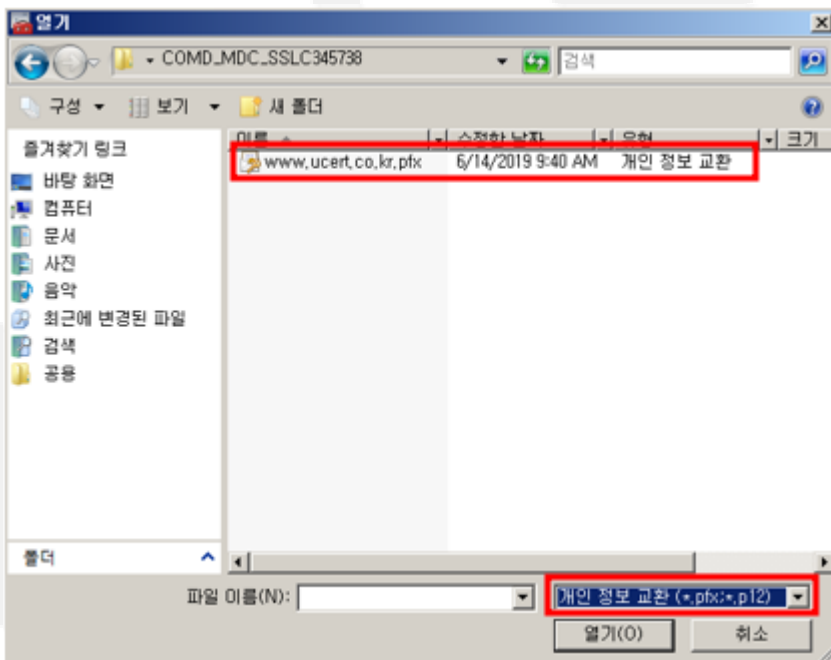
6). 추가 확인을 하도록 합니다.



7). 추가된 인증서 스냅인에서 "개인용" 마우스 우클릭 -> 모든 작업 -> "가져오기"

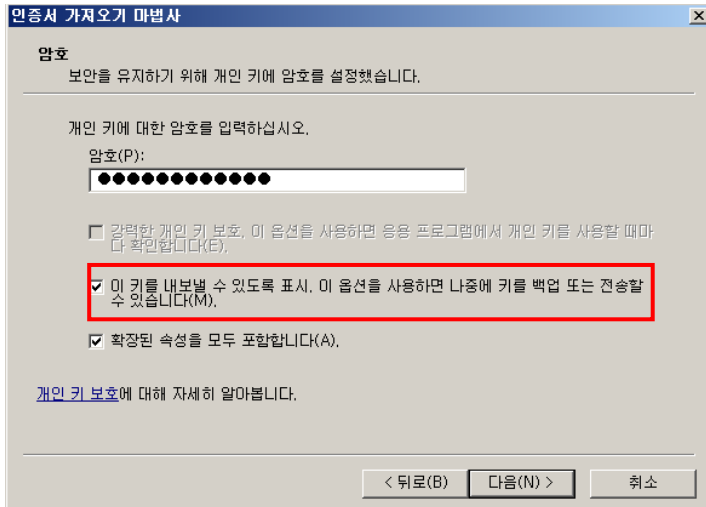


8). "가져오기"에서 인증서를 선택하도록 합니다.

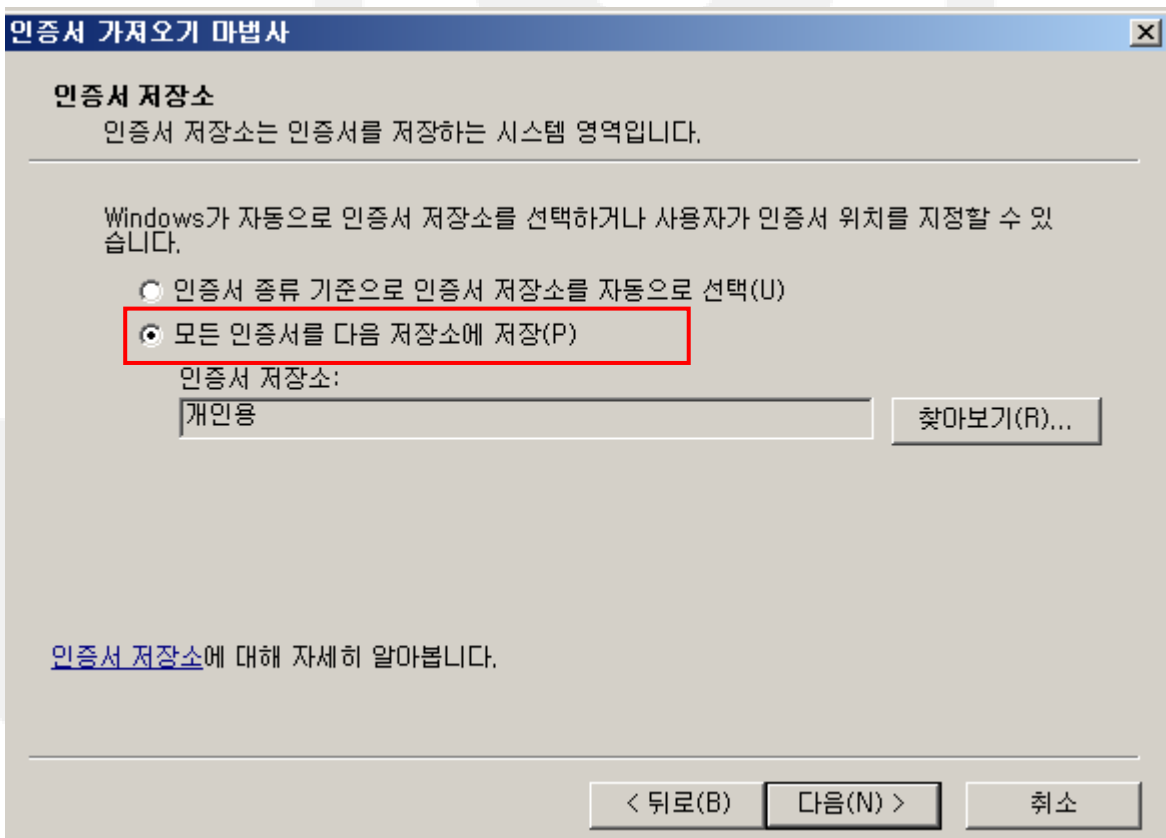


※ (필수)파일 형식을 개인 정보 교환으로 변경 시 PFX파일 확인 가능

9). 암호를 입력하도록 합니다.



10). 인증서 종류 기준으로 인증서 저장소를 자동으로 선택하도록 합니다.



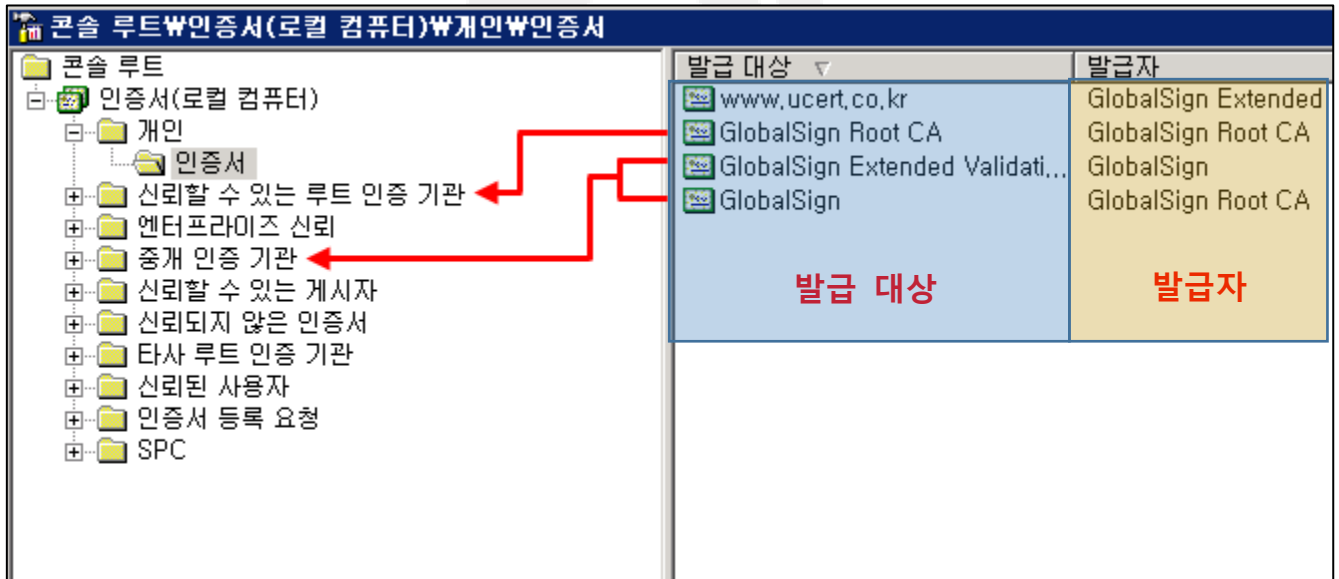
1). 각각의 인증서를 위의 [표\(2 페이지\)](#)에 맞추어 옮기도록 한다.

※간단하게 구분하는 방법

개인 → 인증서 : 발급 대상이 도메인으로 된 인증서

신뢰할 수 있는 루트 인증 기관 → 인증서 : 발급 대상과 발급자가 **동일한** 인증서

중개 인증 기관 → 인증서 : 발급 대상과 발급자가 **동일하지 않은** 인증서

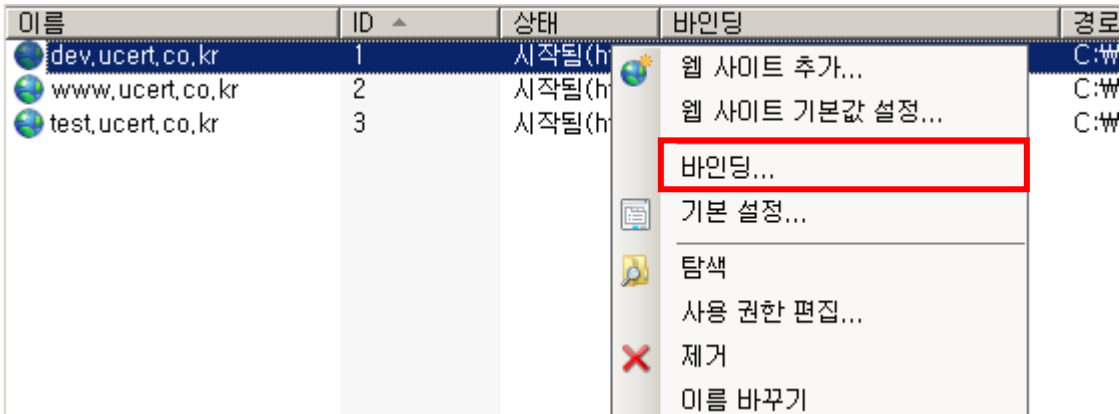


※ ucert 에서 판매량이 많은 GlobalSign 인증서 기준이며 인증서별로 이름은 달라질 수 있습니다.

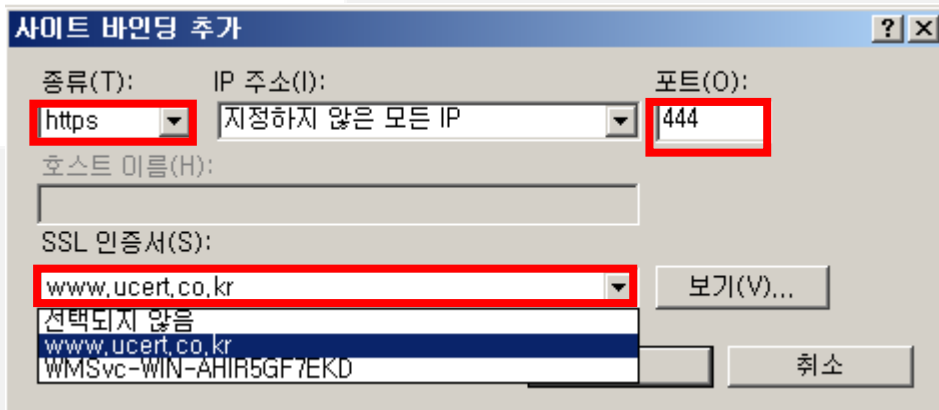
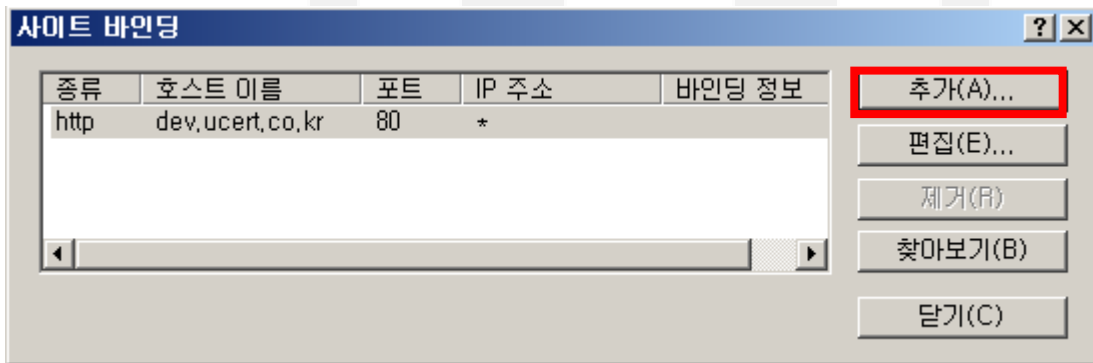
UCERT
www.ucert.co.kr

2. 인증서 설치

1) IIS를 실행하고 설치 할 웹 사이트에 바인딩 클릭.



2) 사이트 바인딩에서 추가 버튼을 누르고 종류를 https 인증서를 선택한다.



3) 아래의 바인딩 처리가 이루어지도록 한다. 포트 번호는 각자 나누어 지도록 한다.

이름	ID	상태	바인딩
dev.ucert.co.kr	1	시작됨(http)	dev.ucert.co.kr on *:80 (http),*:444 (https)
www.ucert.co.kr	2	시작됨(http)	www.ucert.co.kr on *:80 (http),*:446 (https)
test.ucert.co.kr	3	시작됨(http)	test.ucert.co.kr on *:80 (http),*:447 (https)

- 4) 관리자권한으로 CMD 창 실행 -> C:\Windows\System32\Winetsrv 이동합니다
 appcmd set site /site.name:"이름" /+bindings.[protocol='https',bindingInformation='*:443:도메인']

[명령어를 통하여 시큐어 바인딩 실행]

```

관리자: Microsoft Windows 7 x64 DEBUG Build Environment

C:\Windows\System32>cd C:\Windows\System32\Winetsrv

C:\Windows\System32\Winetsrv>appcmd set site /site.name:"test1" /+bindings.[protocol='https',bindingInformation='*:443:test1.co.kr']
SITE 개체 "test1"을(를) 변경했습니다.

C:\Windows\System32\Winetsrv>appcmd set site /site.name:"test2" /+bindings.[protocol='https',bindingInformation='*:443:test2.co.kr']
SITE 개체 "test2"을(를) 변경했습니다.

C:\Windows\System32\Winetsrv>appcmd set site /site.name:"test3" /+bindings.[protocol='https',bindingInformation='*:443:test3.co.kr']
SITE 개체 "test3"을(를) 변경했습니다.

C:\Windows\System32\Winetsrv>
  
```

- 5) 443 포트로 바인딩이 완료됩니다

이름	ID	상태	바인딩
dev.ucert.co.kr	1	시작됨(http)	dev.ucert.co.kr on *:80 (http),*:444 (https),dev.ucert.co.kr on *:443 (https)
www.ucert.co.kr	2	시작됨(http)	www.ucert.co.kr on *:80 (http),*:446 (https),www.ucert.co.kr on *:443 (https)
test.ucert.co.kr	3	시작됨(http)	test.ucert.co.kr on *:80 (http),*:447 (https),test.ucert.co.kr on *:443 (https)

- 6) 인증서를 등록합니다.

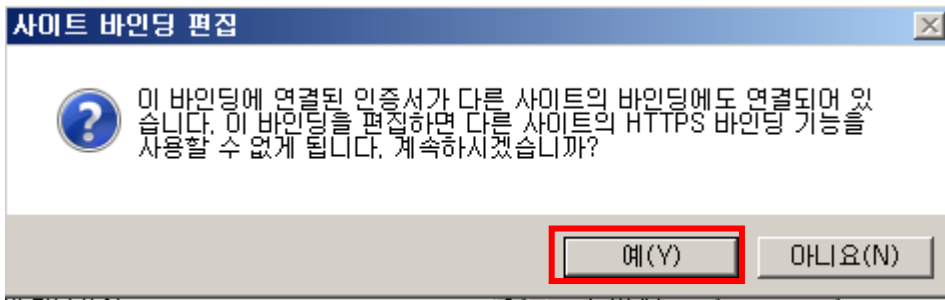
사이트 바인딩 편집

종류(T): https IP 주소(I): 지정하지 않은 모든 IP 포트(O): 443

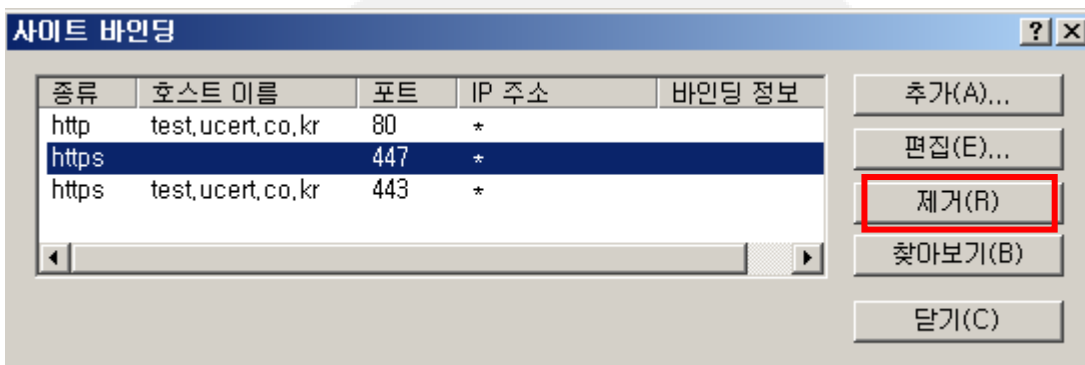
호스트 이름(H):

SSL 인증서(S): www.ucert.co.kr 보기(V)...

확인 취소



7) 바인딩 메뉴에서 임의의 포트를 제거합니다.



IIS7 멀티인증서 설치의 경우 시큐어바인딩 작업 후 하나의 도메인만 인증서 설정을 하여도 443포트가 설정된 모든 도메인이 적용 됩니다.

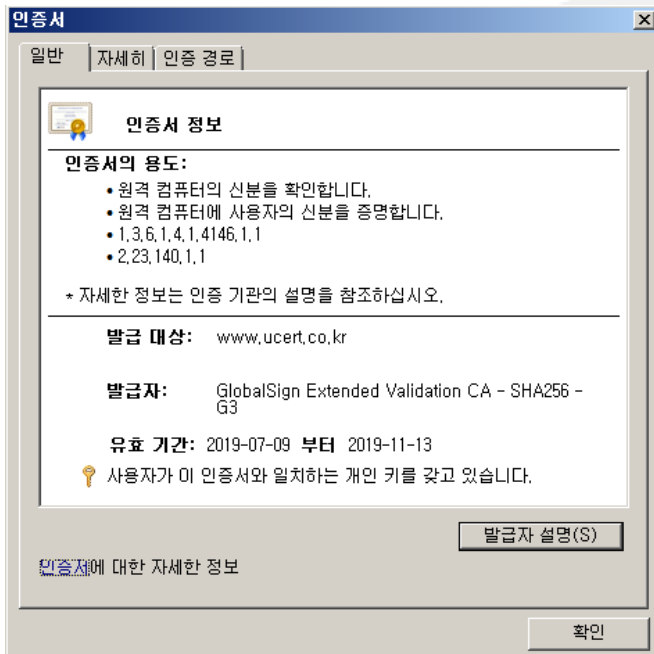
https://해당도메인:[ssl포트]로 접속이 되는지 확인합니다. 주소창 옆에 자물쇠를 클릭하여 '인증서 보기'를 클릭하여 인증서가 올바른지 확인합니다.

UCERT

www.ucert.co.kr

3. 인증서 확인

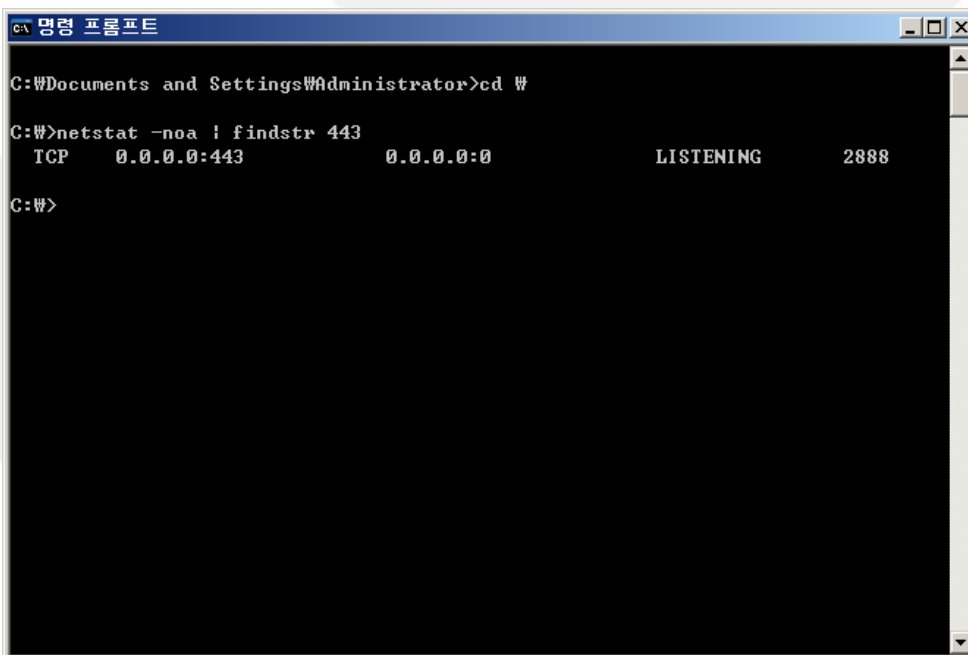
1). 바인딩 편집에서 인증서 보기를 클릭 합니다.



2). 지정한 SSL 포트를 확인 합니다.

- cmd 실행 후 **netstat -noa | findstr 443**

명령어로 인증서를 설치 한 포트가 Listen 상태인지 확인 합니다.



- 내/외부 방화벽에 SSL포트(기본443)가 비활성화 상태일 경우 SSL포트(기본443)를 활성화 합니다.

* 웹 방화벽이 있을 경우 ucert@ucert.co.kr로 웹 방화벽용 인증서를 신청하여 발급 받으신 후 웹 방화벽에 인증서를 설치 합니다.

- 외부에서 웹 브라우저로 [https://\[해당도메인\]:\[SSL포트\]](https://[해당도메인]:[SSL포트]) 로 접속하여 SSL포트가 열려있는지 확인합니다.

예:) <https://www.ucert.co.kr> or <https://www.korsec.co.kr:444>



UCERT

www.ucert.co.kr



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.

3). 웹페이지에서의 인증서 확인 방법

익스플로러 확인 방법 <https://www.ucert.co.kr> 접속 예

The screenshot shows the Internet Explorer browser window with the address bar displaying <https://www.ucert.co.kr>. The '파일(F)' (File) menu is open, and the '속성(R)' (Properties) option is highlighted. A blue arrow points from the text box to the '속성(R)' option.

**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.**

The '속성' (Properties) dialog box is open, showing the '인증서' (Certificates) tab. The '인증서 정보' (Certificate Information) section is visible, displaying the following details:

- 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

Buttons at the bottom include '확인' (OK), '취소' (Cancel), '적용(A)' (Apply), and '인증서(C)' (Certificates). A red dashed box highlights the '인증서(C)' button.