

Windows Server 2008

IIS7

(Single)

SSL 인증서 갱신 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

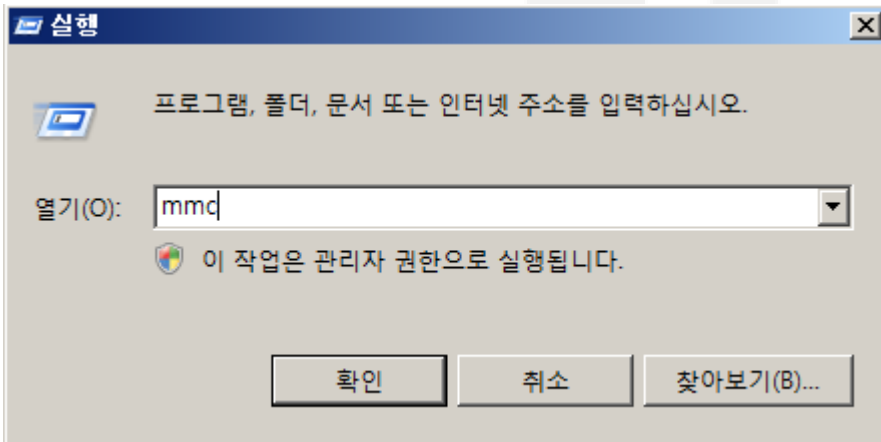


본 문서는 주식회사 한국기업보안에서 SSL보안서버인증서 설치를 위해 작성된 문서로
주식회사 한국기업보안의 동의 없이 무단으로 사용하실 수 없습니다

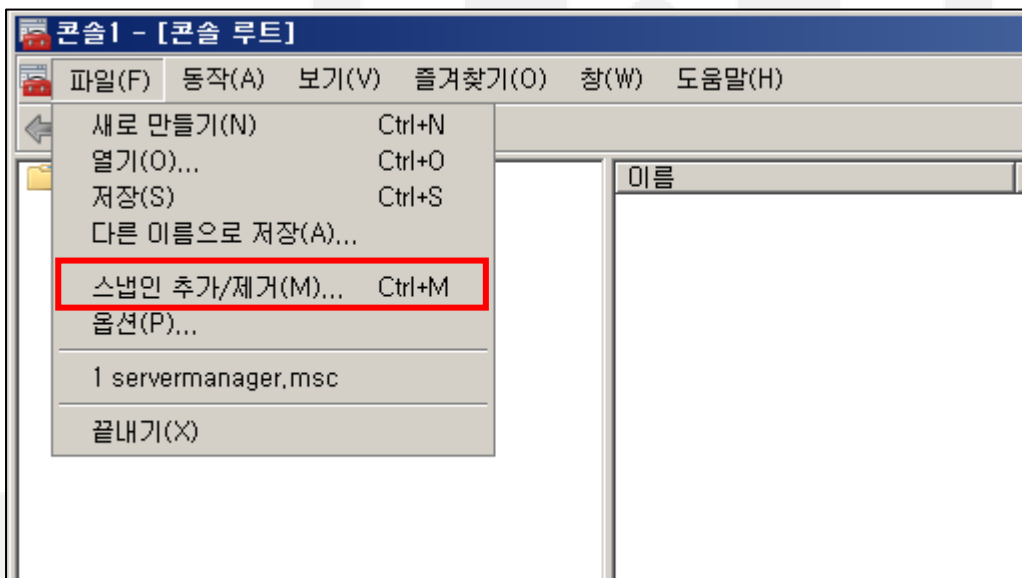
Copyright 2018-2023. Korea Corporation Security Co., Ltd All pictures cannot be copied without permission.

1. 인증서 가져오기

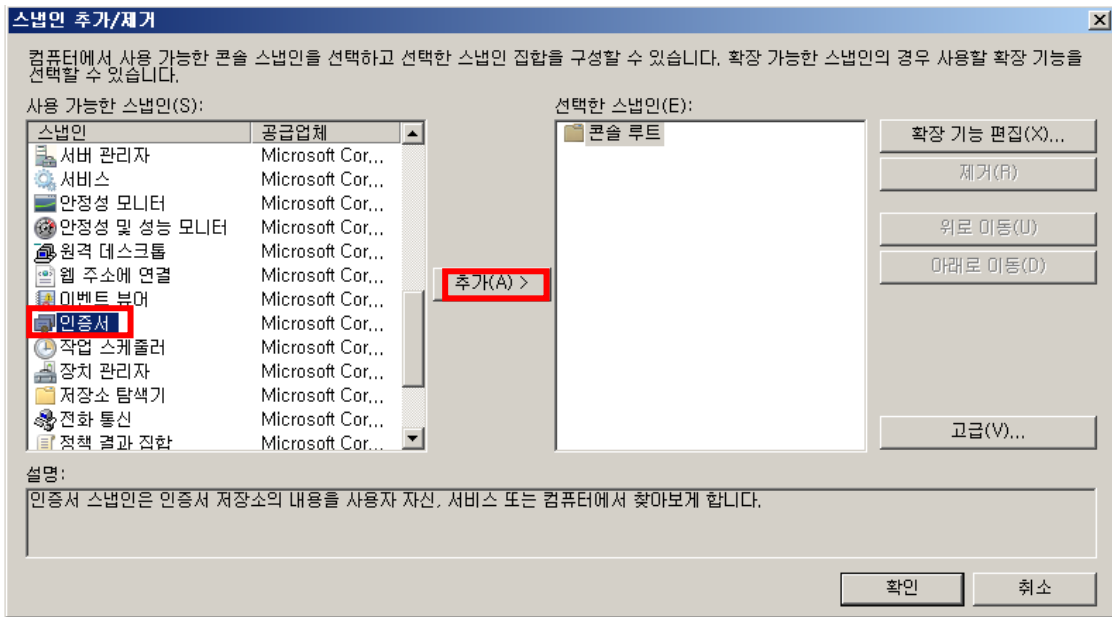
- 1). "실행" 창을 실행하여 MMC 를 실행 합니다. [Windows 키 + R 키 > mmc]



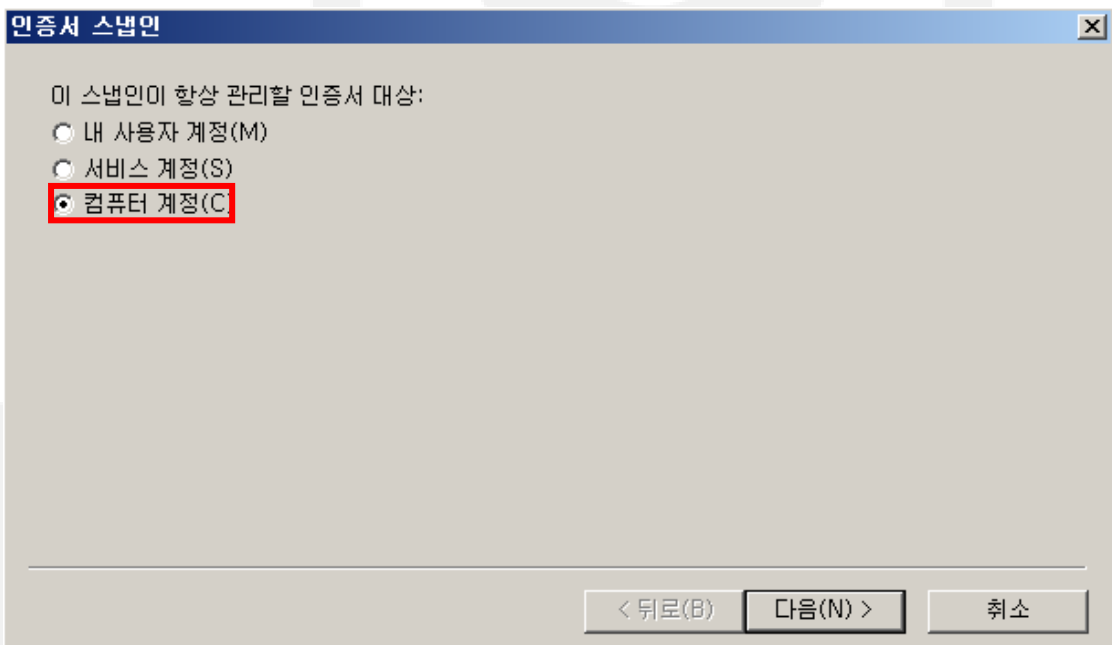
- 2). 파일 > 스냅인 추가/제거를 선택합니다.



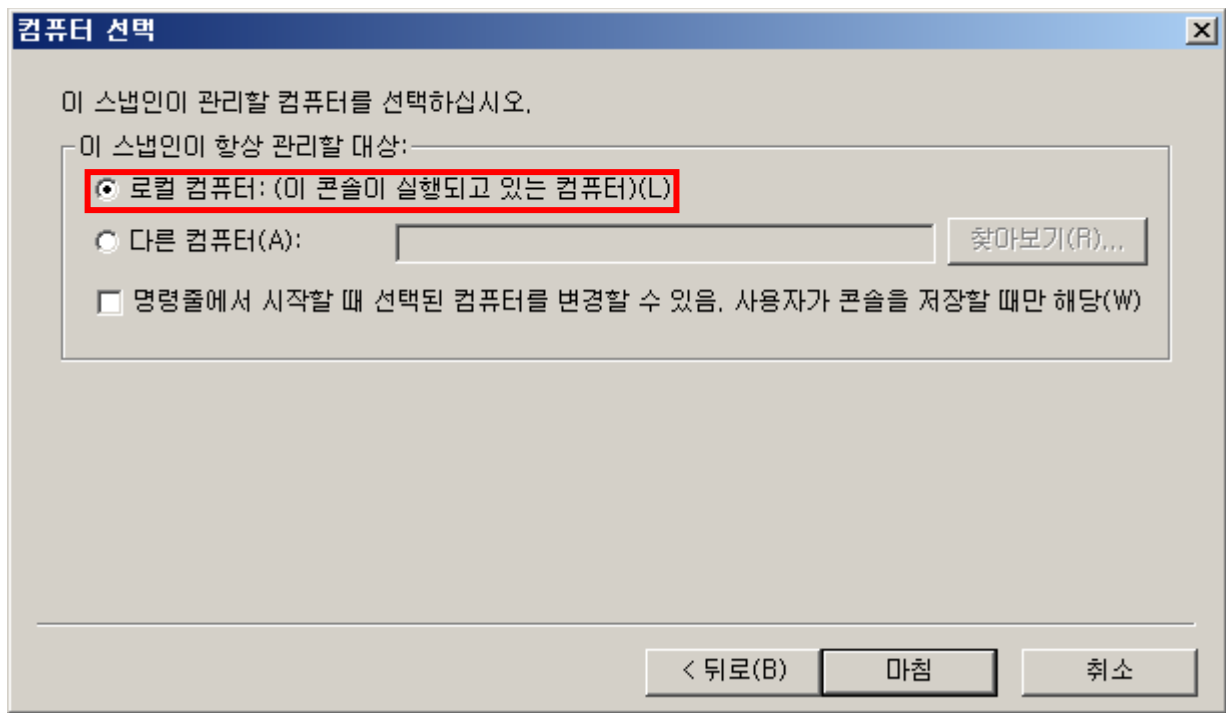
3). 인증서 스냅인을 추가합니다.



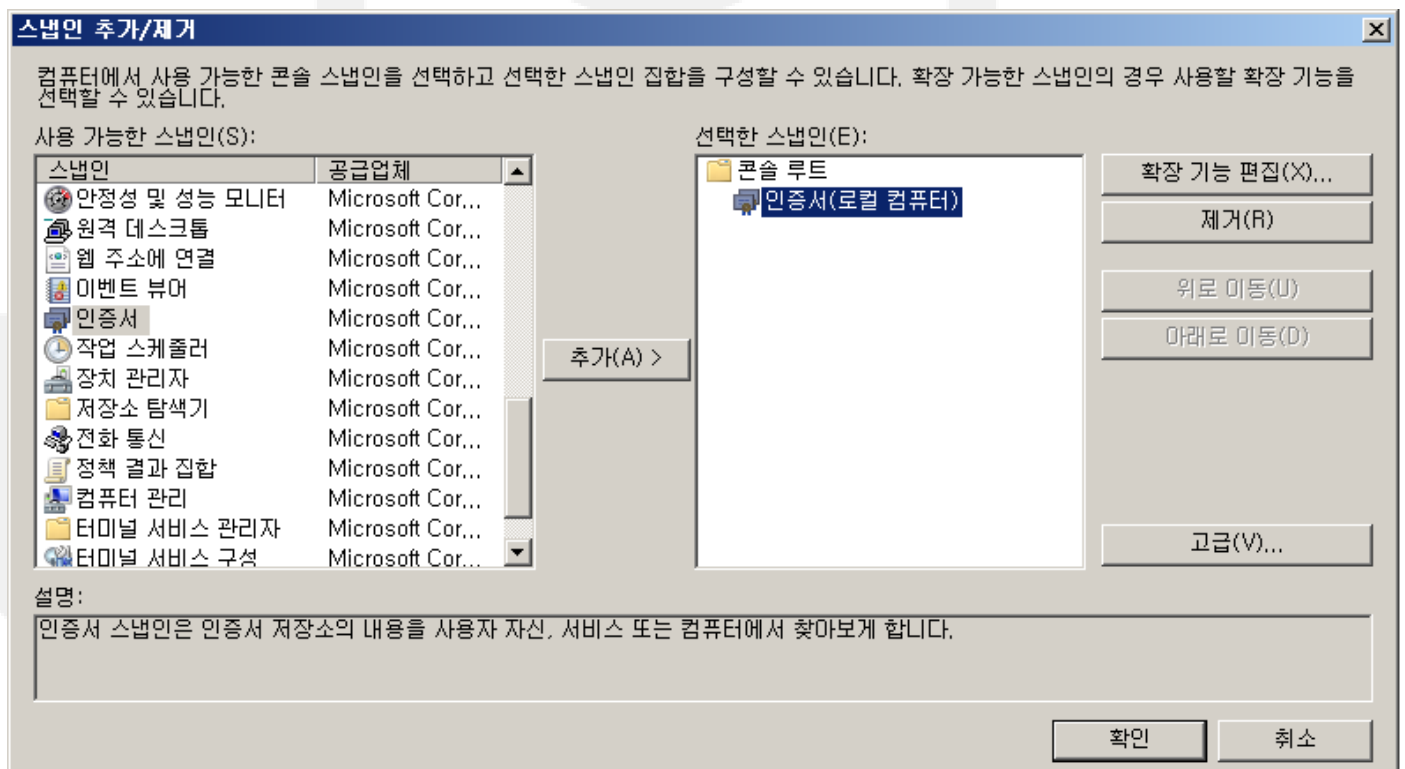
4). 컴퓨터 계정을 선택합니다.



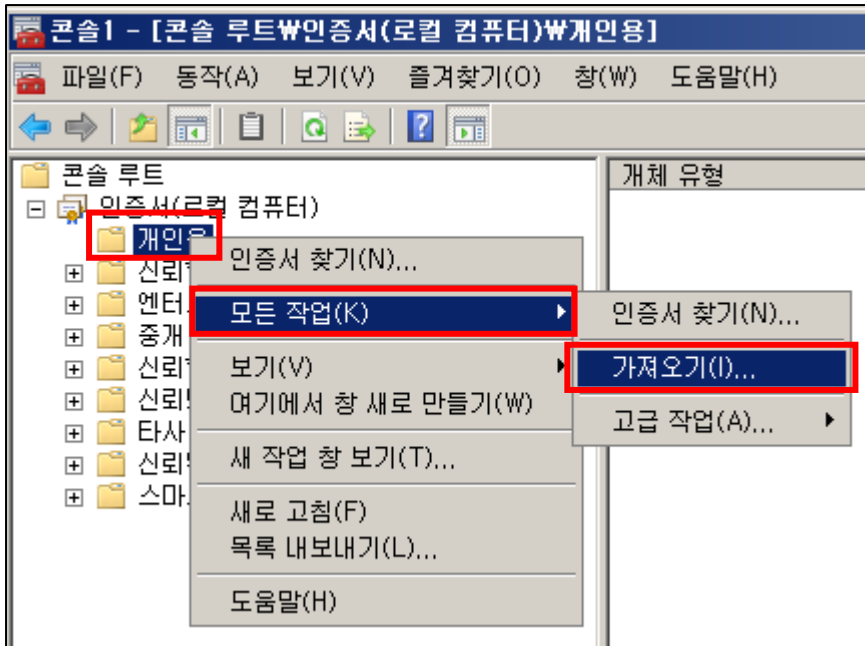
5). 로컬 컴퓨터를 선택하도록 합니다.



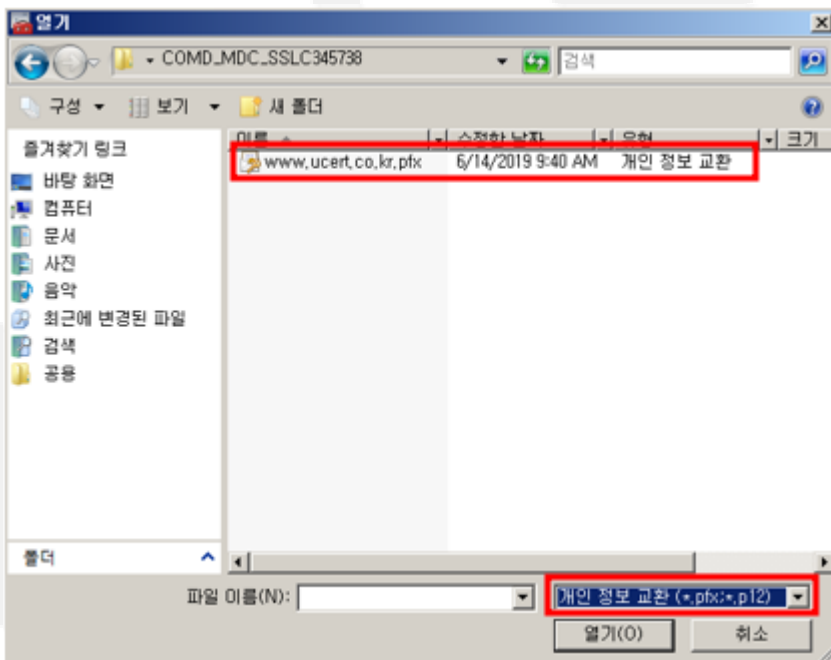
6). 추가 확인을 하도록 합니다.



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

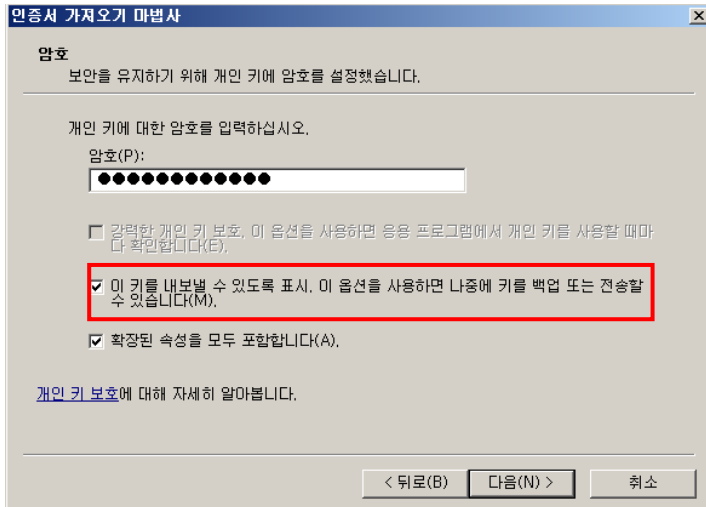


8). "가져오기"에서 인증서를 선택하도록 합니다.

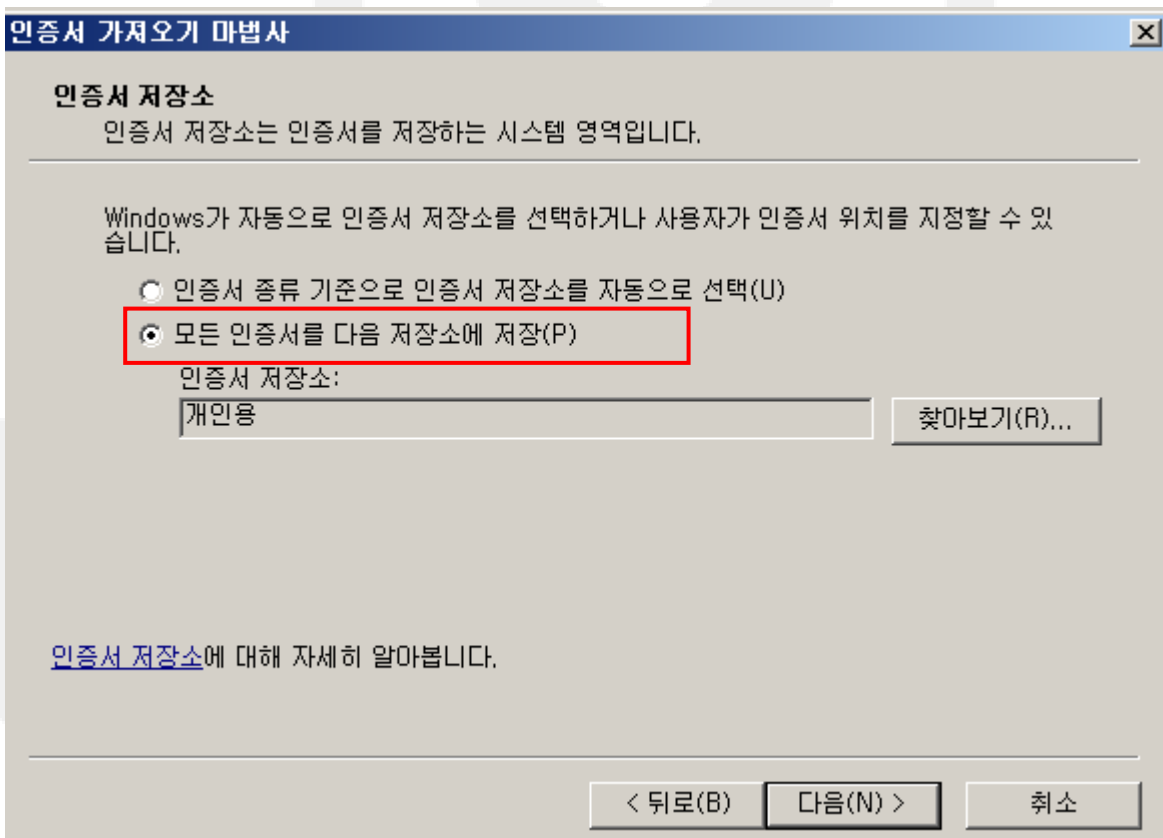


※ (필수)파일 형식을 개인 정보 교환으로 변경 시 PFX파일 확인 가능

9). 암호를 입력하도록 합니다.



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



11) 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

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

| 콘솔 루트\인증서(로컬 컴퓨터)\개인\인증서 | |
|--------------------------|--|
| 콘솔 루트 | |
| 인증서(로컬 컴퓨터) | |
| 개인 | |
| 인증서 | |
| 신뢰할 수 있는 루트 인증 기관 | |
| 엔터프라이즈 신뢰 | |
| 중개 인증 기관 | |
| 신뢰할 수 있는 게시자 | |
| 신뢰되지 않은 인증서 | |
| 타사 루트 인증 기관 | |
| 신뢰된 사용자 | |
| 인증서 등록 요청 | |
| SPC | |

| 발급 대상 | 발급자 |
|---------------------------------|---------------------|
| www.ucert.co.kr | GlobalSign Extended |
| GlobalSign Root CA | GlobalSign Root CA |
| GlobalSign Extended Validati... | GlobalSign |
| GlobalSign | GlobalSign Root CA |
| 발급 대상 | 발급자 |

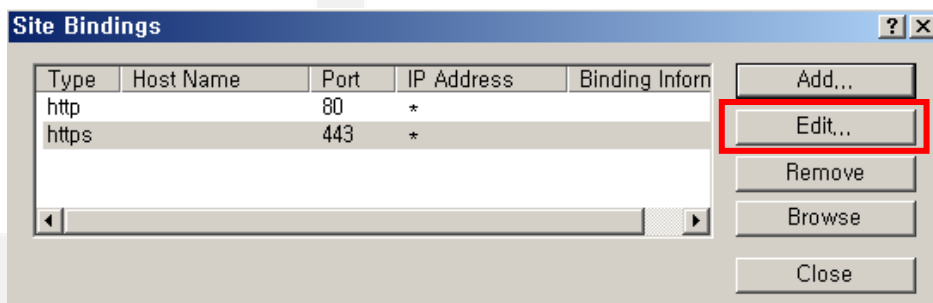
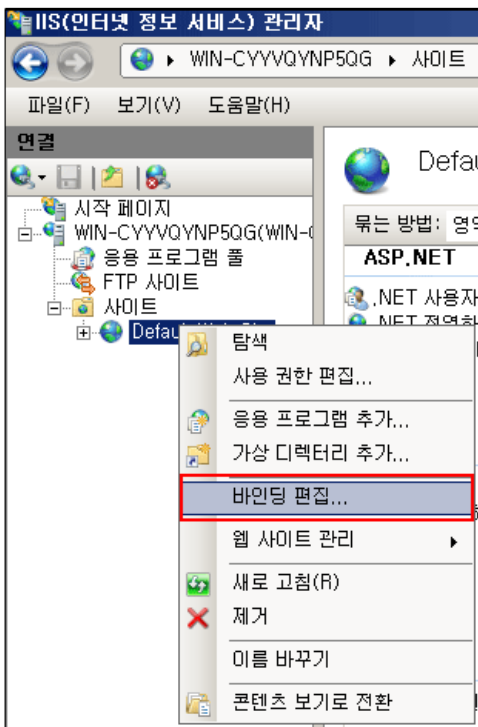
※ ucert 에서 판매량이 많은 GlobalSign 인증서 기준이며 인증서별로 이름은 달라질 수 있습니다.

UCERT

www.ucert.co.kr

2. 인증서 설치

- 1). SSL 인증서를 설치 할 웹사이트 목록의 마우스 오른쪽을 클릭하여 바인딩 편집을 선택 합니다.



2). 편집을 클릭하여 SSL 서비스를 클릭합니다.

- 종류: https > 포트번호 입력 (Default 는 443 입니다) > SSL 인증서 항목을 확장하신 후 등록하신 인증서를 선택합니다.

사이트 바인딩 추가

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

호스트 이름(H):

SSL 인증서(S): www.ucert.co.kr 보기(V)...

선택되지 않음

WMSvc-WIN-CYYVQYNP5QG

취소

3). 추가된 인증서를 확인하신 후 닫기를 클릭 합니다.

인증서

일반 | 자세히 | 인증 경로

인증서 정보

인증서의 용도:

- 원격 컴퓨터의 신분을 확인합니다.
- 원격 컴퓨터에 사용자의 신분을 증명합니다.
- 1.3.6.1.4.1.4146.1.1
- 2.23.140.1.1

* 자세한 정보는 인증 기관의 설명을 참조하십시오.

발급 대상: www.ucert.co.kr

발급자: GlobalSign Extended Validation CA - SHA256 - G3

유효 기간: 2019-07-09 부터 2019-11-13

사용자가 이 인증서와 일치하는 개인 키를 갖고 있습니다.

발급자 설명(S)

인증서에 대한 자세한 정보

확인

사이트 바인딩

| 종류 | 호스트 이름 | 포트 | IP 주소 | 바인딩 정보 |
|-------|--------|-----|-------|--------|
| http | | 80 | * | |
| https | | 443 | * | |

추가(A)...

편집(E)...

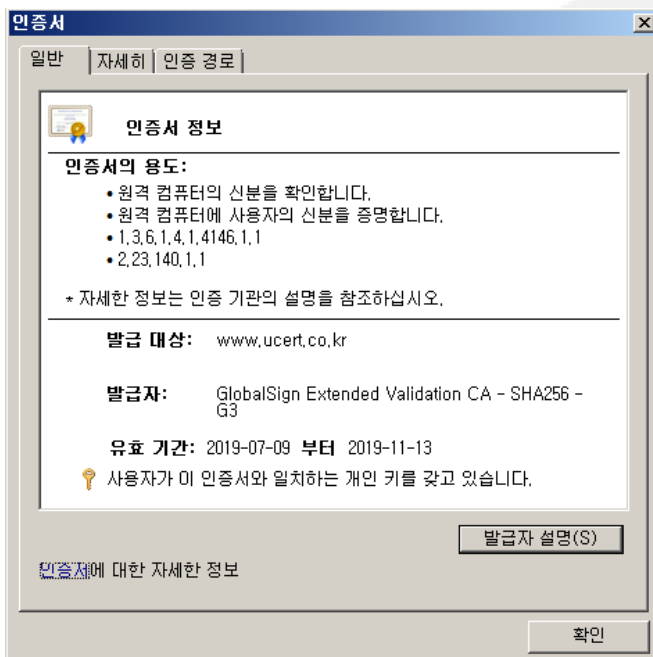
제거(R)

찾아보기(B)

닫기(C)

3. 인증서 확인

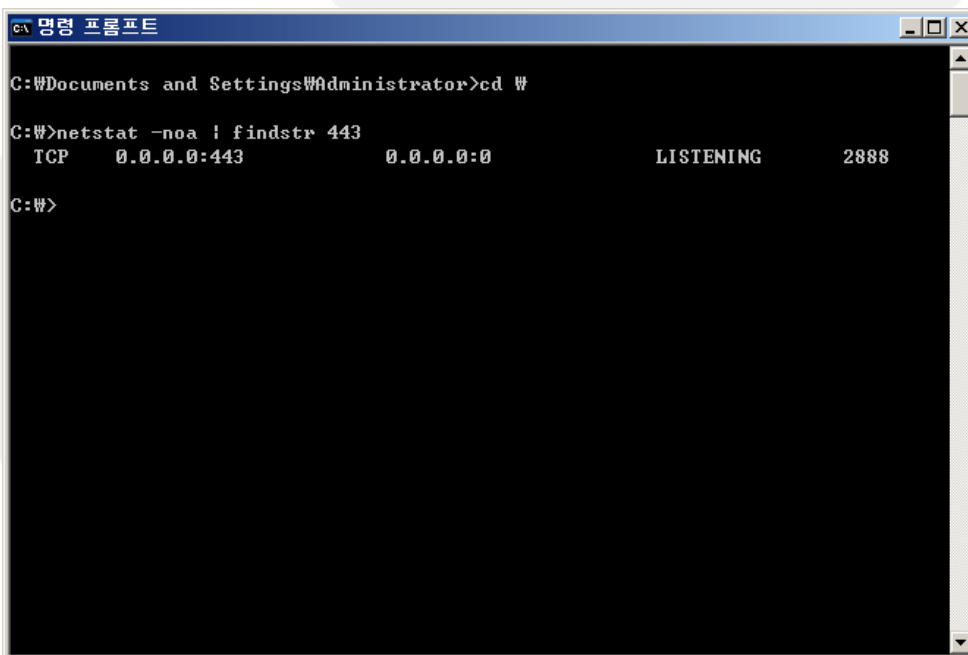
1). 바인딩 편집에서 인증서 보기를 클릭 합니다.



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

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.

인증서 정보

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

발급자 설명(S)

인증서에 대해 자세히 알아보십시오.

확인