ISE용 인증서 해지 목록을 게시하도록 Microsoft CA 서버 구성

목차

[소개](#)

[사전 요구 사항](#)

- [요구 사항](#)
- [사용되는 구성 요소](#)

[구성](#)

- [CA에서 CRL 파일을 저장할 폴더 생성 및 구성](#)
- [새 CRL 배포 지점을 표시하는 IIS에서 사이트 만들기](#)
- [배포 지점에 CRL 파일을 게시하도록 Microsoft CA 서버 구성](#)
- [CRL 파일이 있으며 IIS를 통해 액세스할 수 있는지 확인](#)
- [새 CRL 배포 지점을 사용하도록 ISE 구성](#)

[다음을 확인합니다.](#)

[문제 해결](#)

소개

이 문서에서는 CRL(Certificate Revocation List) 업데이트를 게시하기 위해 IIS(인터넷 정보 서비스)를 실행하는 Microsoft CA(인증 기관) 서버의 구성에 대해 설명합니다. 또한 Cisco ISE(Identity Services Engine)(버전 3.0 이상)가 인증서 검증에 사용할 업데이트를 검색하도록 구성하는 방법에 대해서도 설명합니다. ISE는 인증서 검증에서 사용하는 다양한 CA 루트 인증서에 대한 CRL을 검색하도록 구성할 수 있습니다.

사전 요구 사항

요구 사항

이 문서에 대한 특정 요건이 없습니다.

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- Cisco Identity Services Engine 릴리스 3.0
- Microsoft Windows Server 2008 R2

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

구성

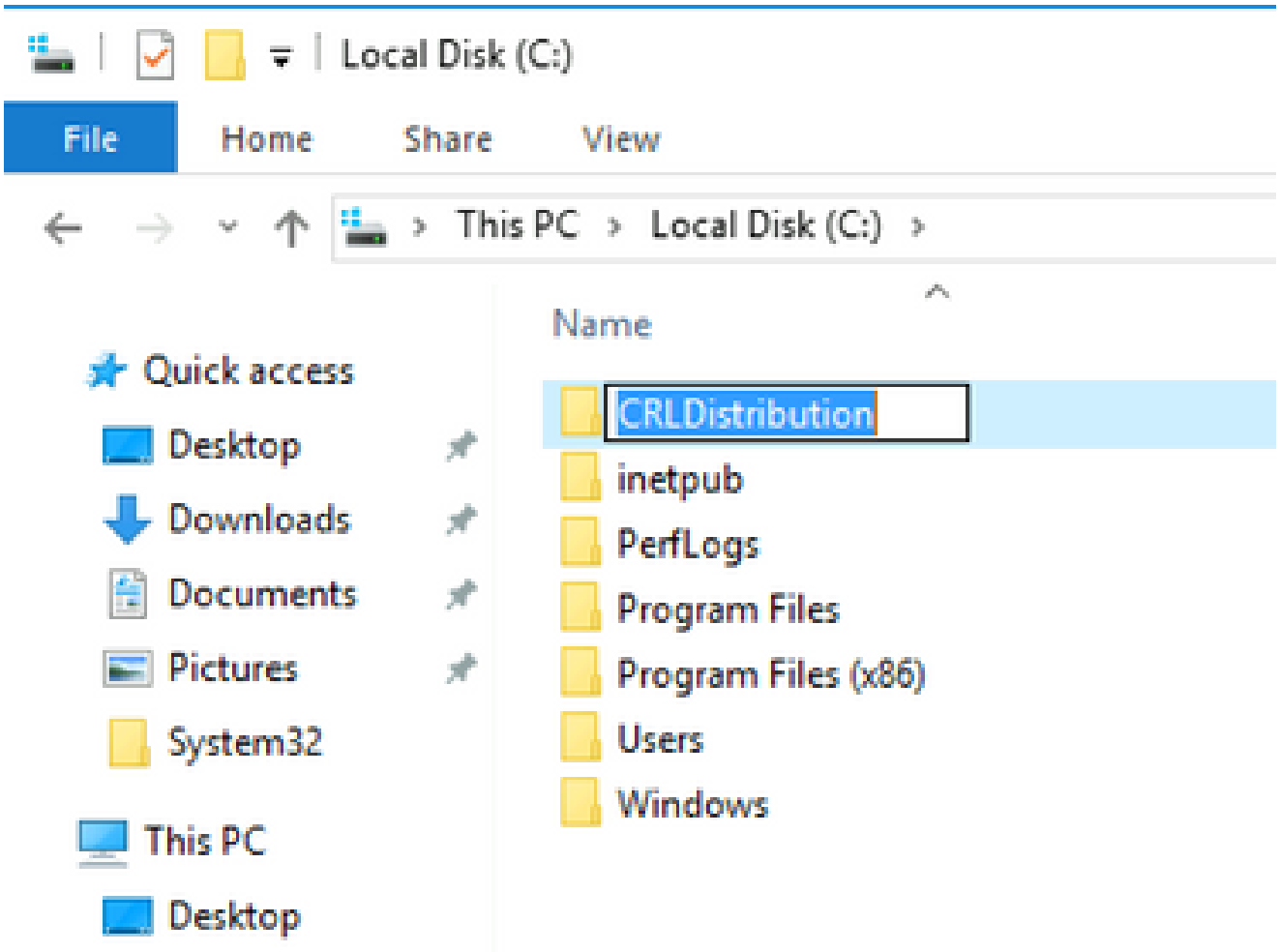
이 섹션에는 이 문서에서 설명하는 기능을 구성하기 위한 정보가 표시됩니다.

CA에서 CRL 파일을 저장할 폴더 생성 및 구성

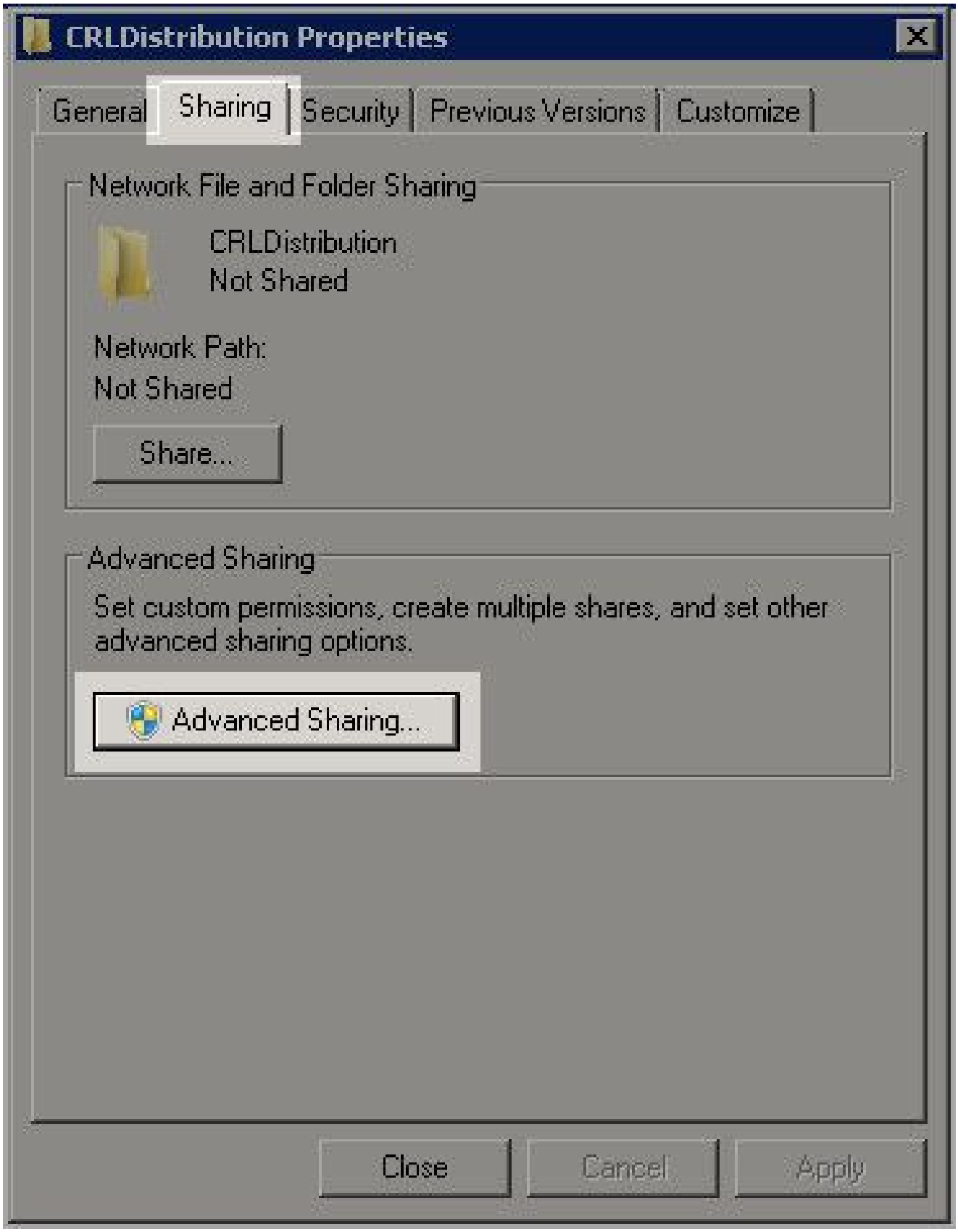
첫 번째 작업은 CA 서버에서 CRL 파일을 저장할 위치를 구성하는 것입니다. 기본적으로 Microsoft CA 서버는 **C:\Windows\system32\CertSrv\CertEnroll**

이 시스템 폴더를 사용하는 대신 파일의 새 폴더를 만듭니다.

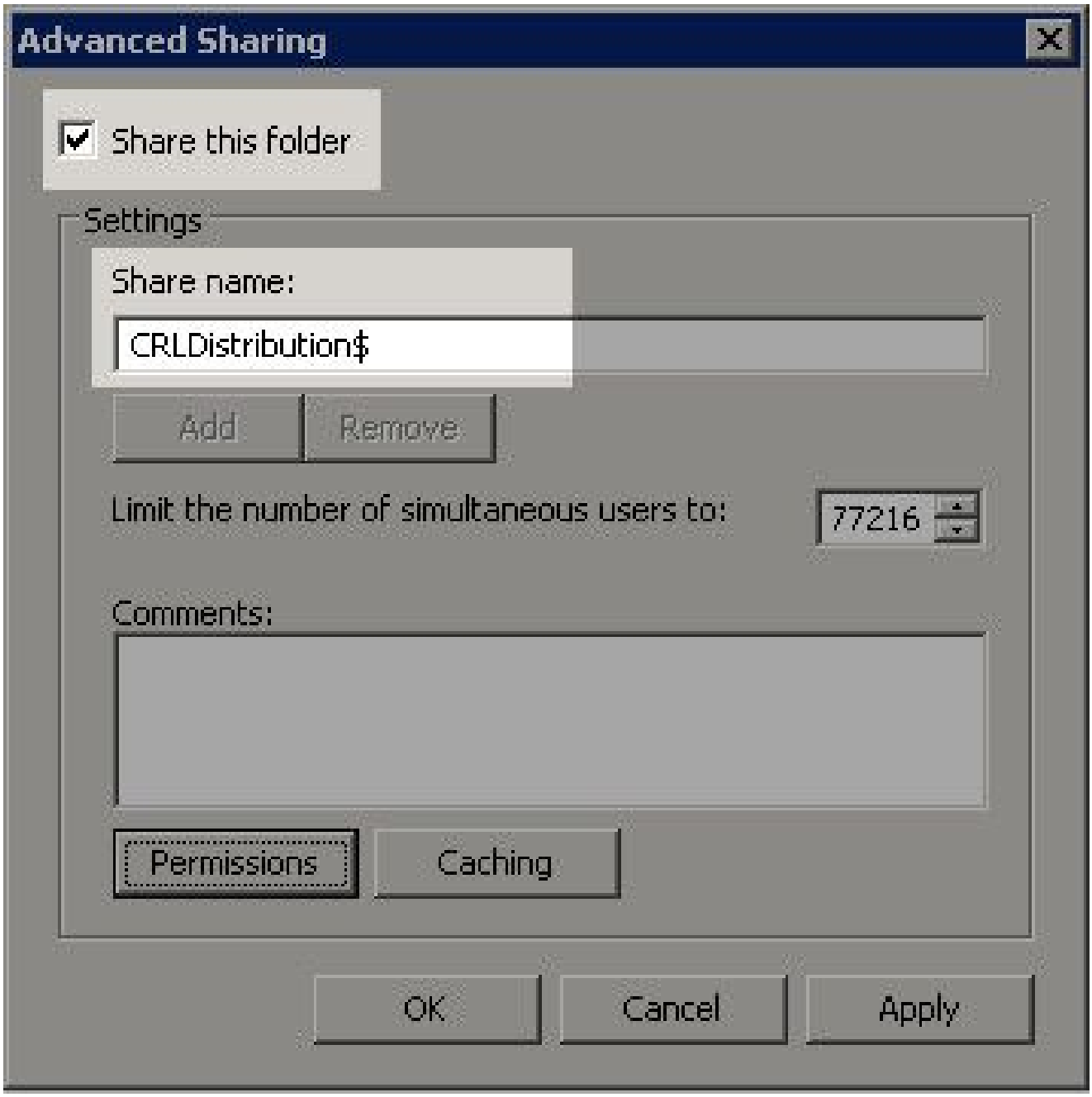
1. IIS 서버에서 파일 시스템의 위치를 선택하고 새 폴더를 만듭니다. 이 예에서는 폴더가 **C:\CRLDistribution** 생성됩니다.



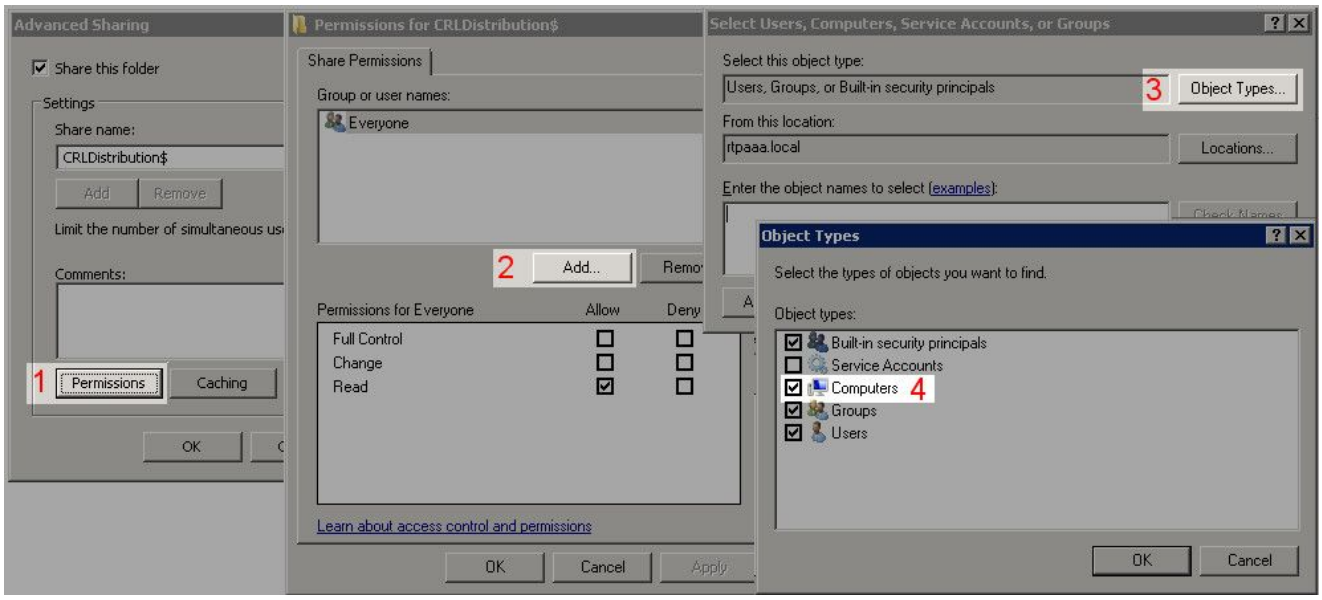
2. CA가 CRL 파일을 새 폴더에 기록하려면 공유를 활성화해야 합니다. 새 폴더를 마우스 오른쪽 단추로 클릭하고 **Properties**을 선택하고 탭을 **Sharing** 클릭한 다음 을 **Advanced Sharing**클릭합니다.



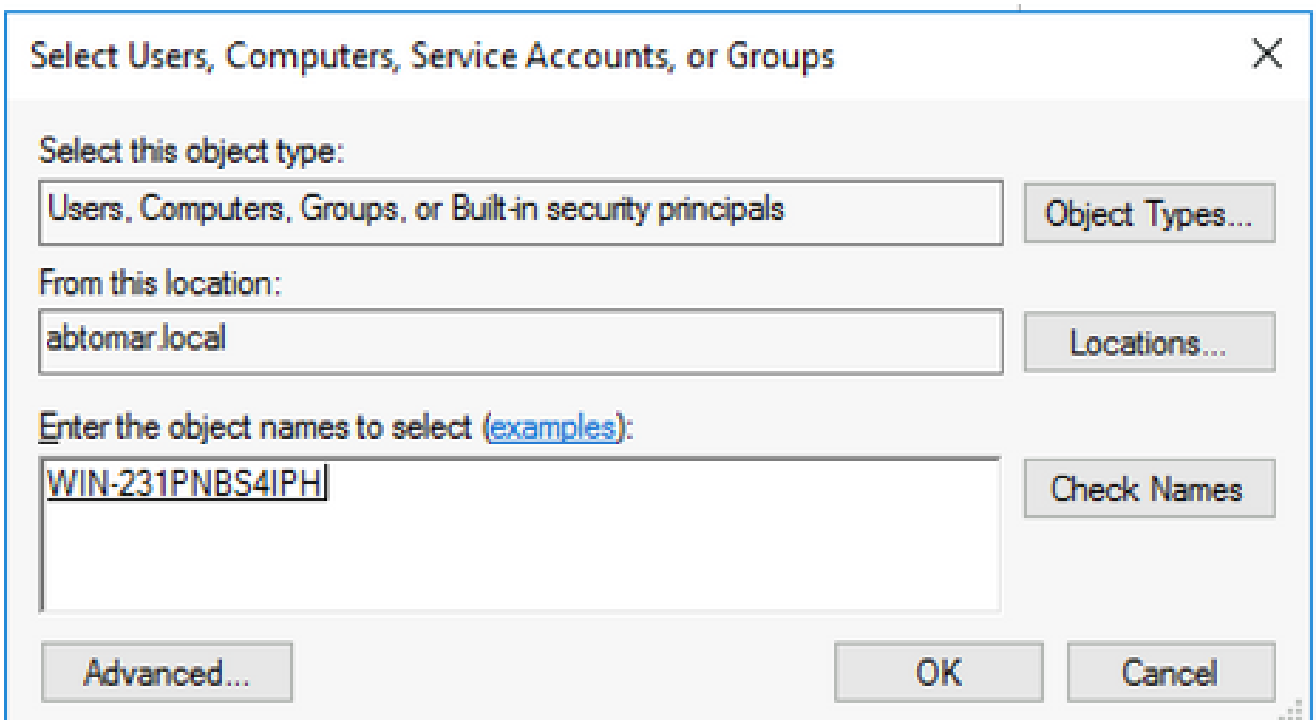
3. 폴더를 공유하려면 확인란을 **Share this folder** 선택한 다음 공유 이름 필드의 공유 이름 끝에 달러 기호($)를 추가하여 공유를 숨깁니다.



4. (**Permissions**1), (**Add**2), **Object Types** (3)을 차례로 클릭하고 확인란**Computers**(4)를 선택합니다.

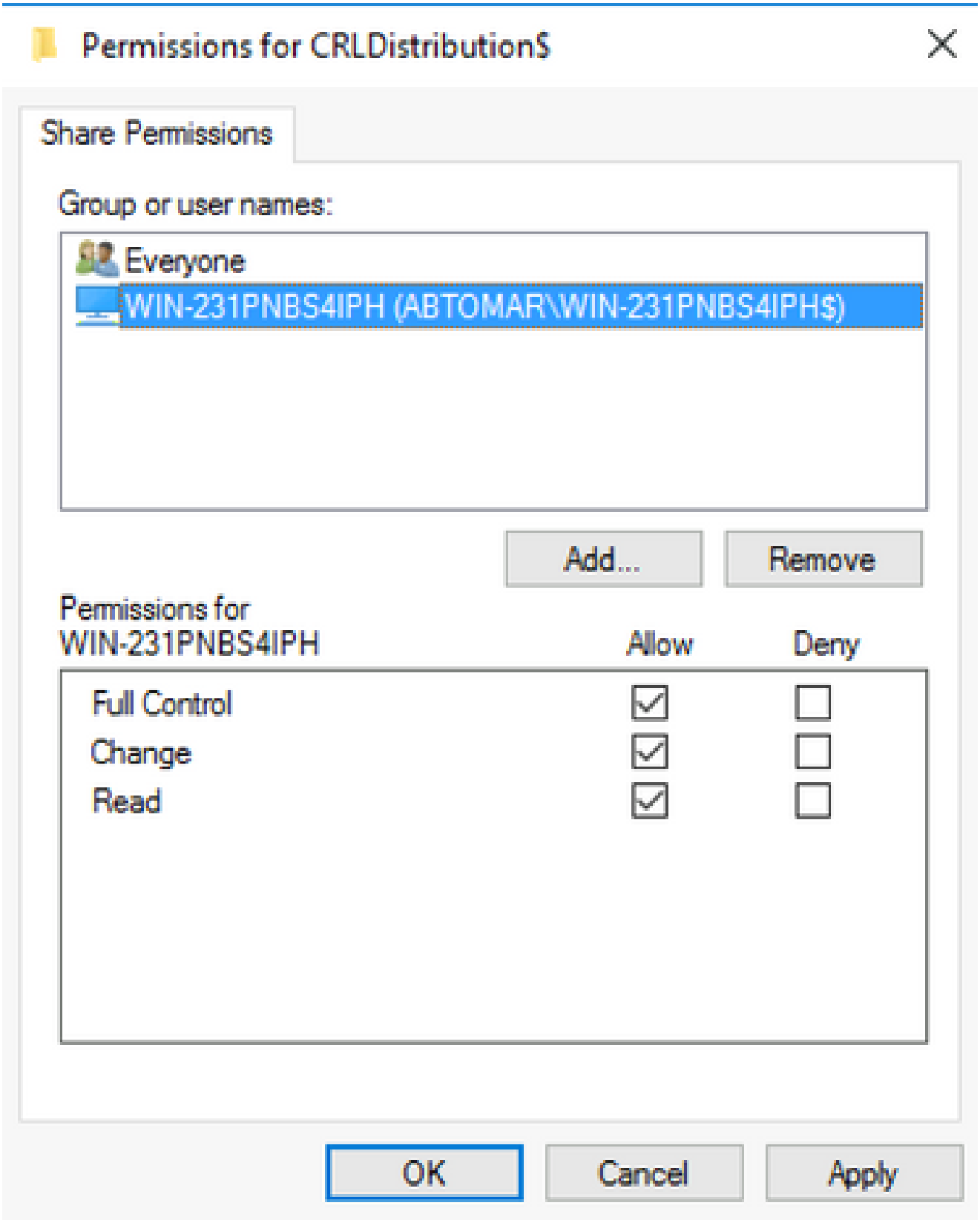


5. 사용자, 컴퓨터, 서비스 계정 또는 그룹 선택 창으로 돌아가려면 을 **OK**클릭합니다. Enter the object names to select(선택할 개체 이름 입력) 필드에 이 예에서 CA 서버의 컴퓨터 이름 WIN0231PNBS4IPH를 입력하고 **Check Names**를 클릭합니다. 입력한 이름이 유효한 경우 이름이 새로 고쳐지고 밑줄이 그어진 상태로 나타납니다. 를 **OK**클릭합니다.

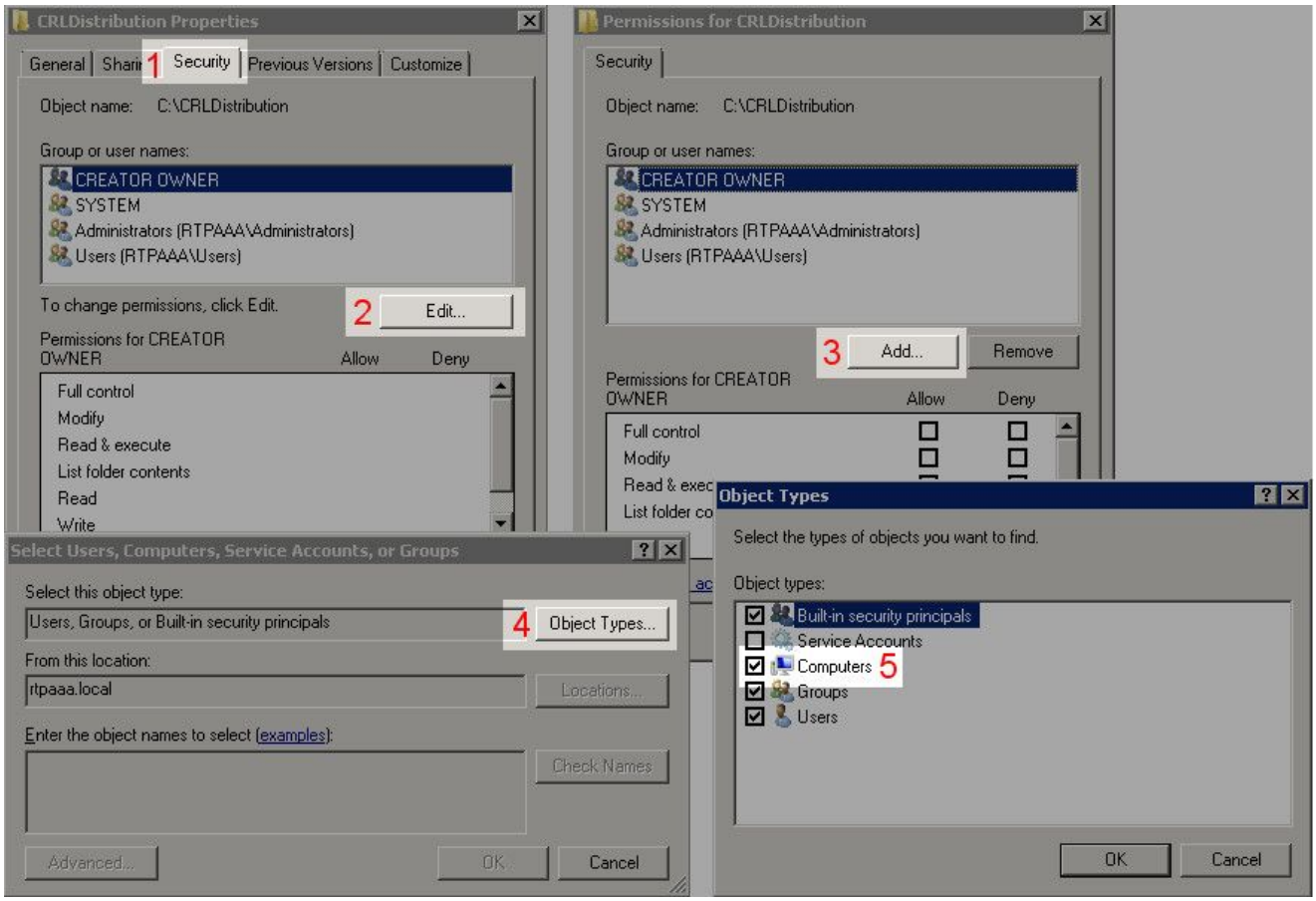


6. Group or user names(그룹 또는 사용자 이름) 필드에서 CA 컴퓨터를 선택합니다. CA**Allow**에 대한 전체 액세스 권한을 부여하려면 Full Control(전체 제어)을 선택합니다.

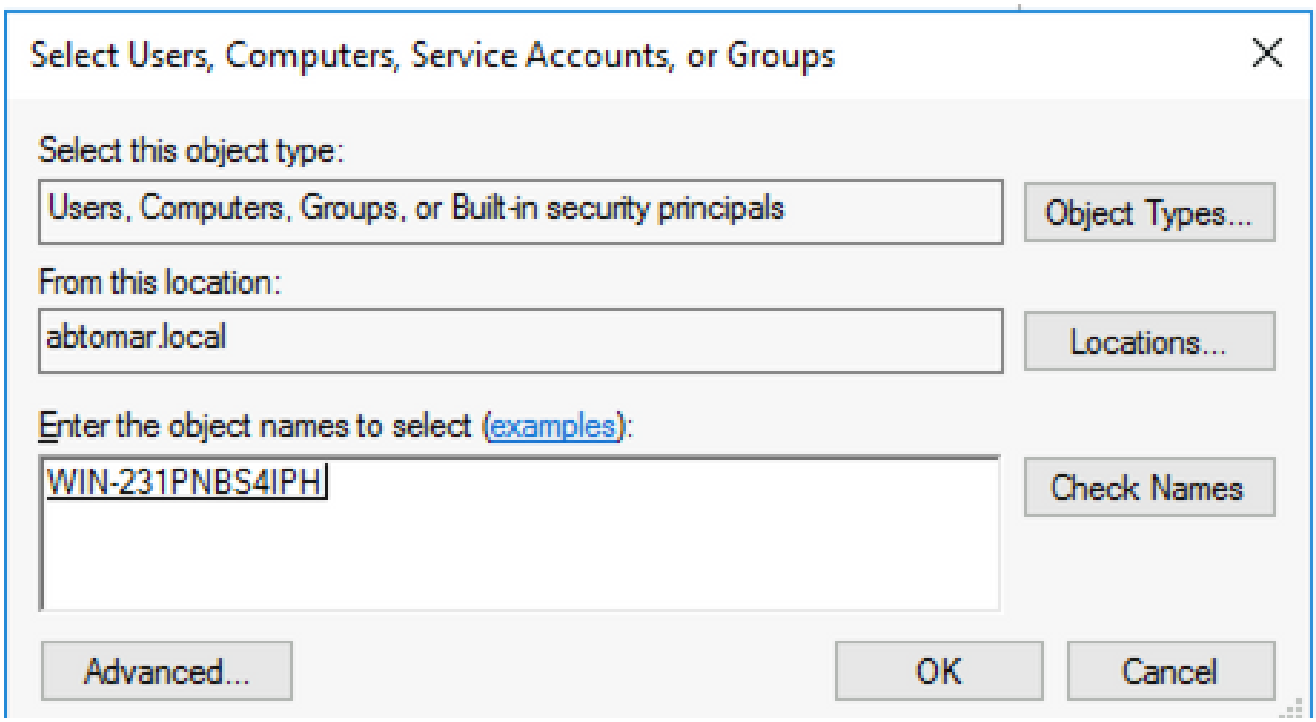
   를 **OK**클릭합니다. Advanced Sharing(고급 공유) 창을 닫고 Properties(속성) 창으로 돌아가려면 **OK** 다시 클릭합니다.



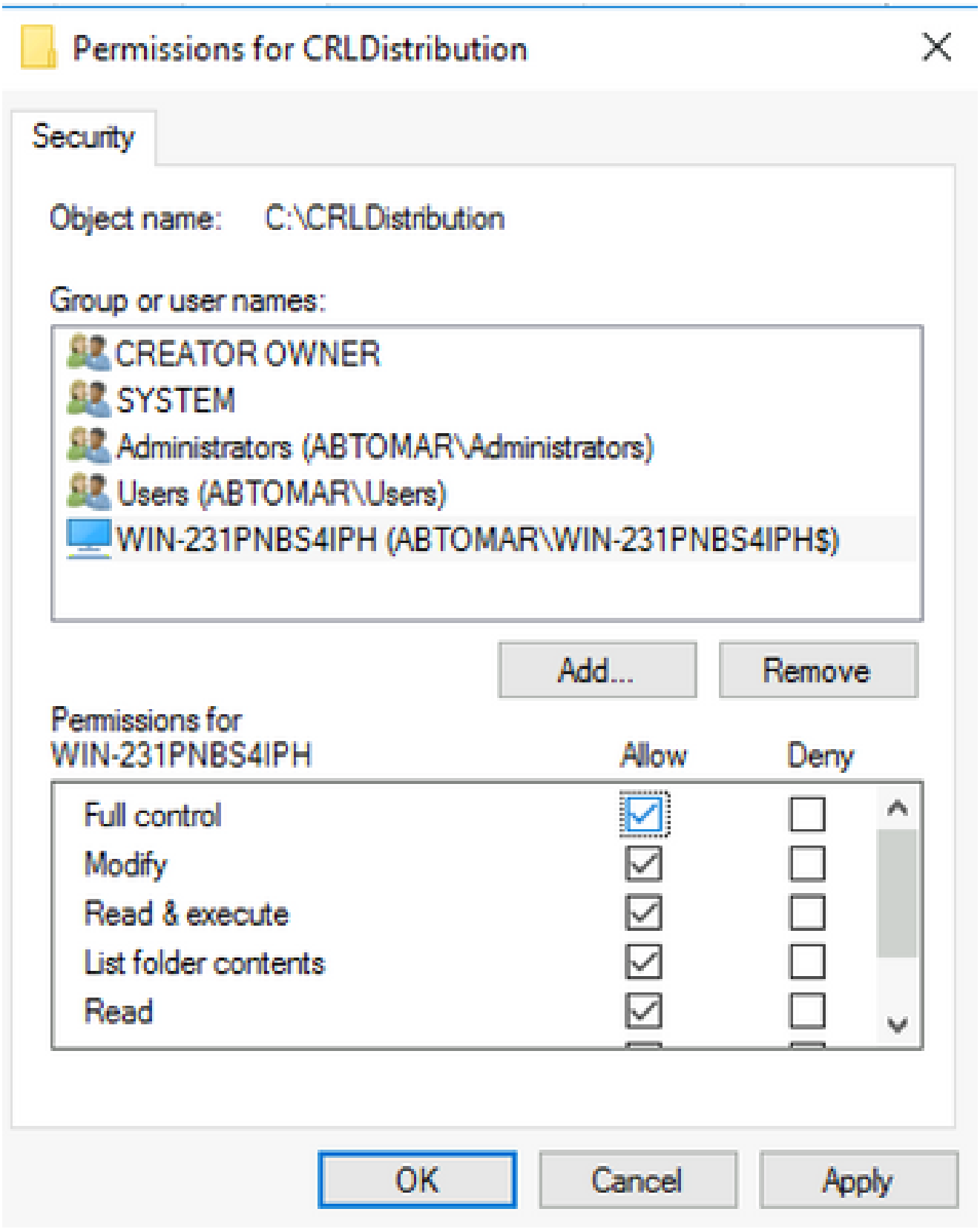
7. CA가 CRL 파일을 새 폴더에 쓸 수 있도록 하려면 적절한 보안 권한을 구성합니다. (1) 탭을 **Security** 클릭하고 (**Edit**2), **Add** (3), **Object Types** (4)를 차례로 클릭한 다음 **Computers** 확인란(5)을 선택합니다.



8. Enter the object names to select(선택할 개체 이름 입력) 필드에 CA 서버의 컴퓨터 이름을 입력하고 를 **Check Names**클릭합니다. 입력한 이름이 유효한 경우 이름이 새로 고쳐지고 밑줄이 그어진 상태로 나타납니다. 를 **OK**클릭합니다.



9. Group or user names(그룹 또는 사용자 이름) 필드에서 CA 컴퓨터를 선택한 다음 Full control(전체 제어)을 선택하여 CA에 대한 전체 액세스 권한을 **Allow** 부여합니다. 을 **OK** 클릭한 다음 을 클릭하여 작업**Close**을 완료합니다.

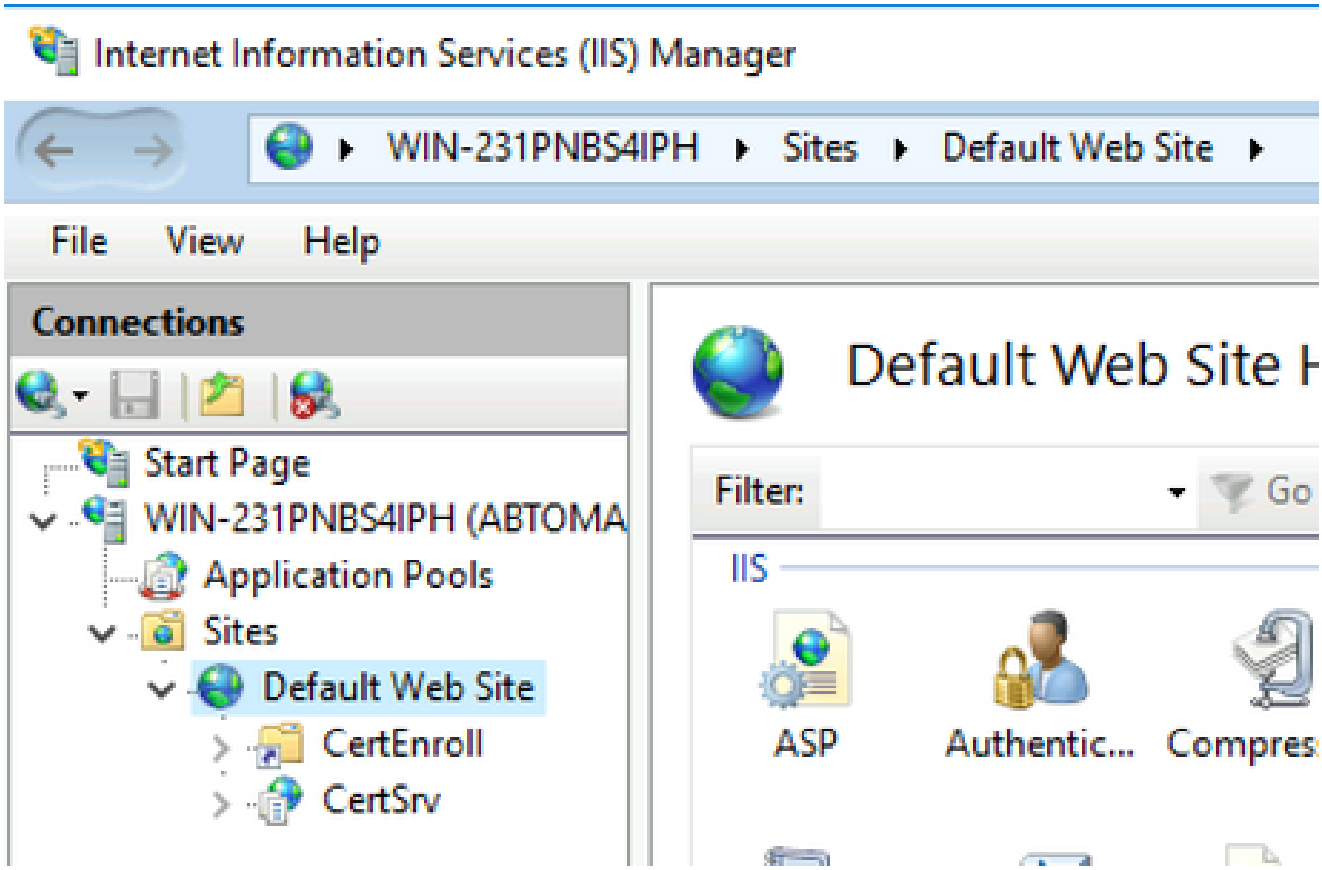


새 CRL 배포 지점을 표시하는 IIS에서 사이트 만들기

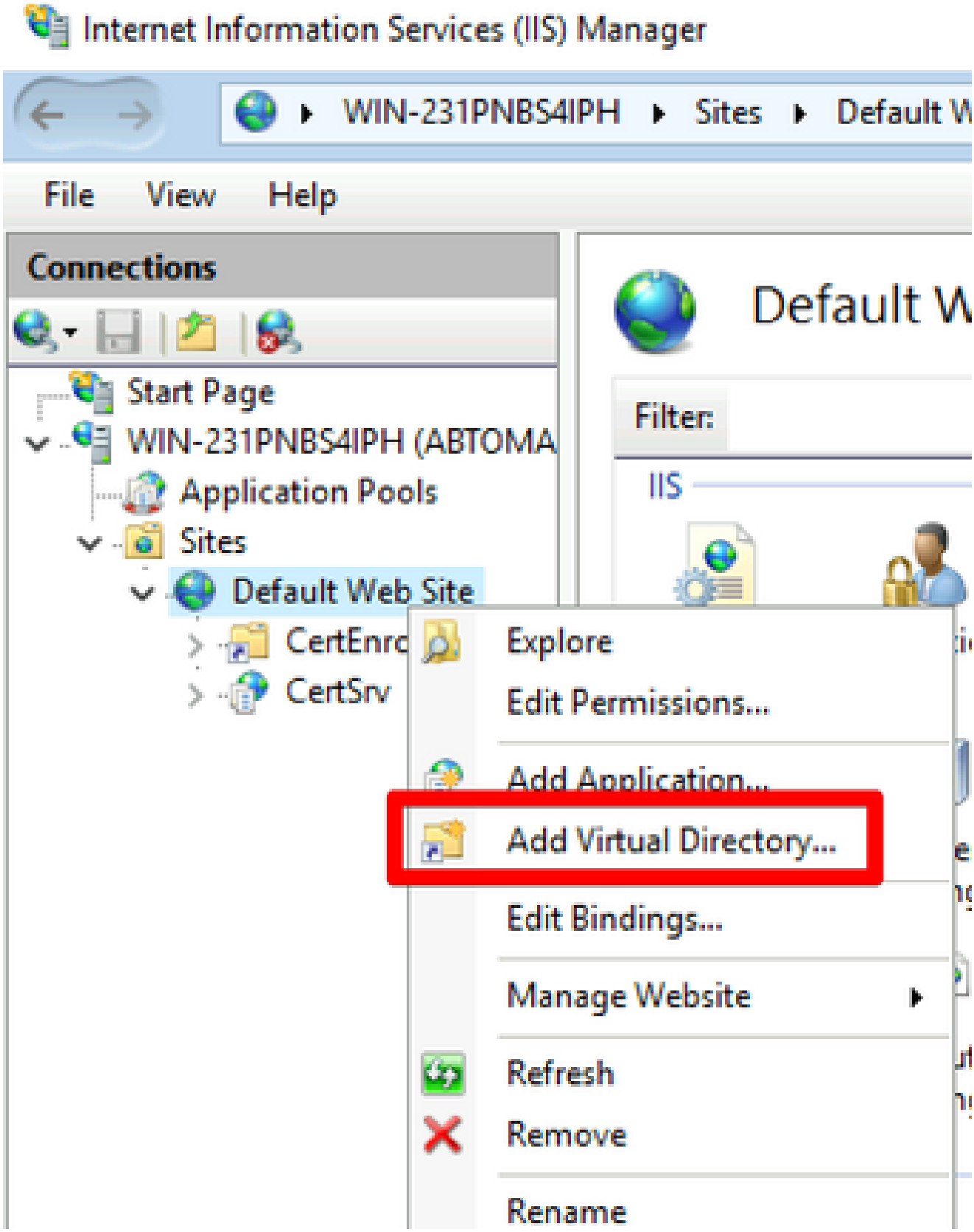
ISE가 CRL 파일에 액세스하려면 IIS를 통해 CRL 파일이 들어 있는 디렉터리에 액세스할 수 있도록 합니다.

1. IIS 서버 작업 표시줄에서 를 **Start**클릭합니다. 를 **Administrative Tools > Internet Information Services (IIS) Manager**선택합니다.

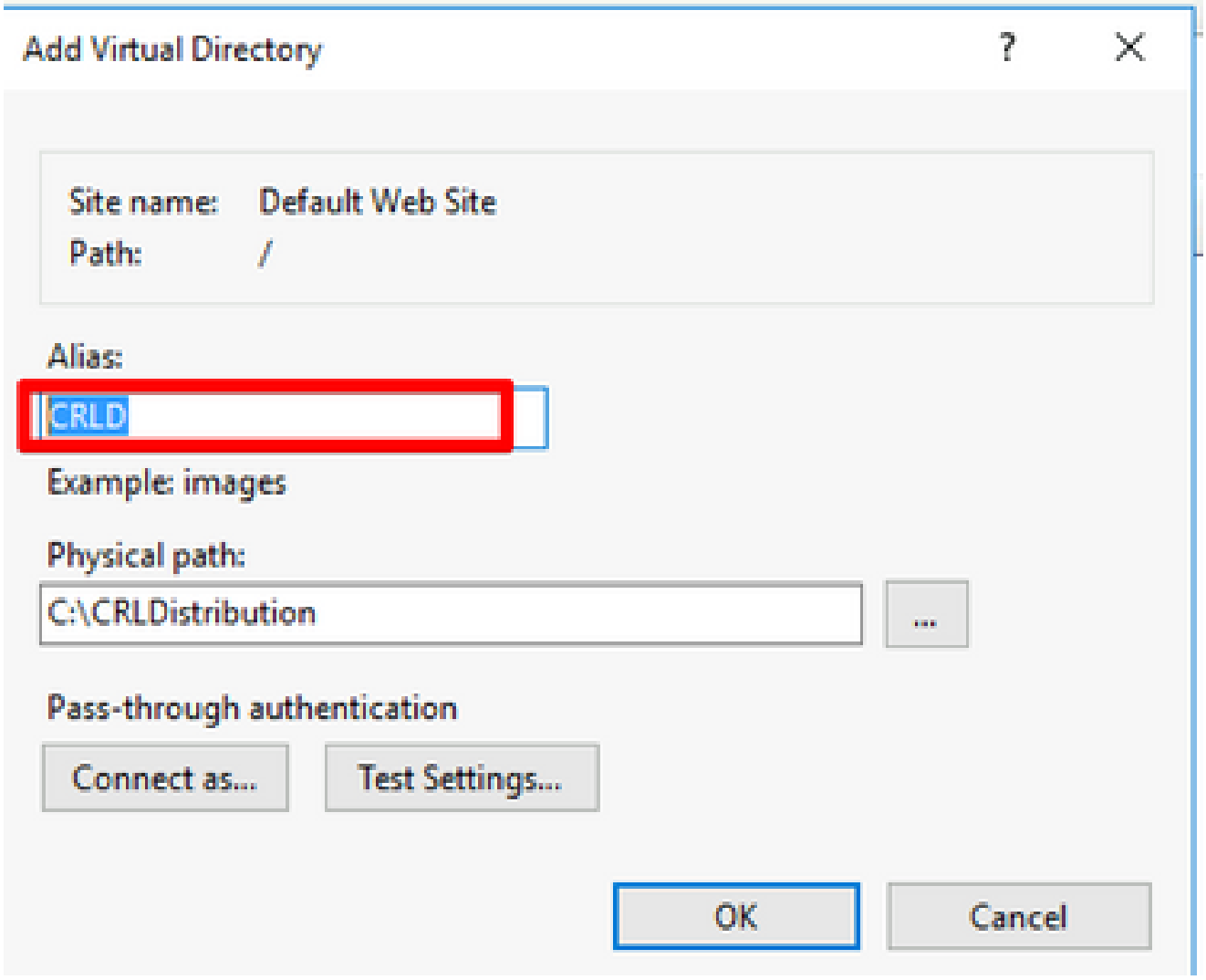
2. 왼쪽 창(콘솔 트리라고도 함)에서 IIS 서버 이름을 확장한 다음 확장합니다**Sites**.



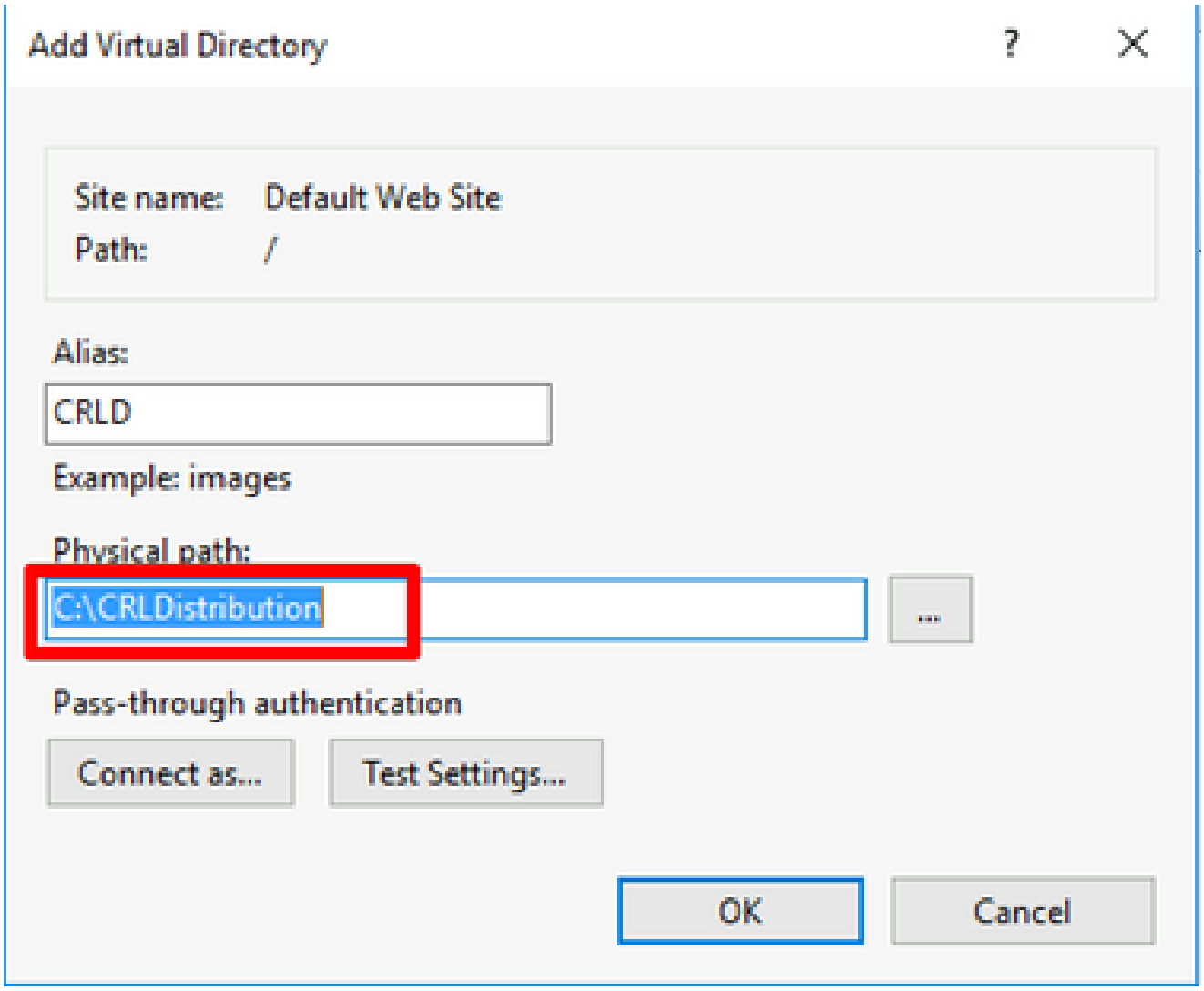
3. 이 이미지에 표시된 **Default Web Site** 것처럼 마우스 오른쪽 버튼**Add Virtual Directory**을 클릭하고 을 선택합니다.



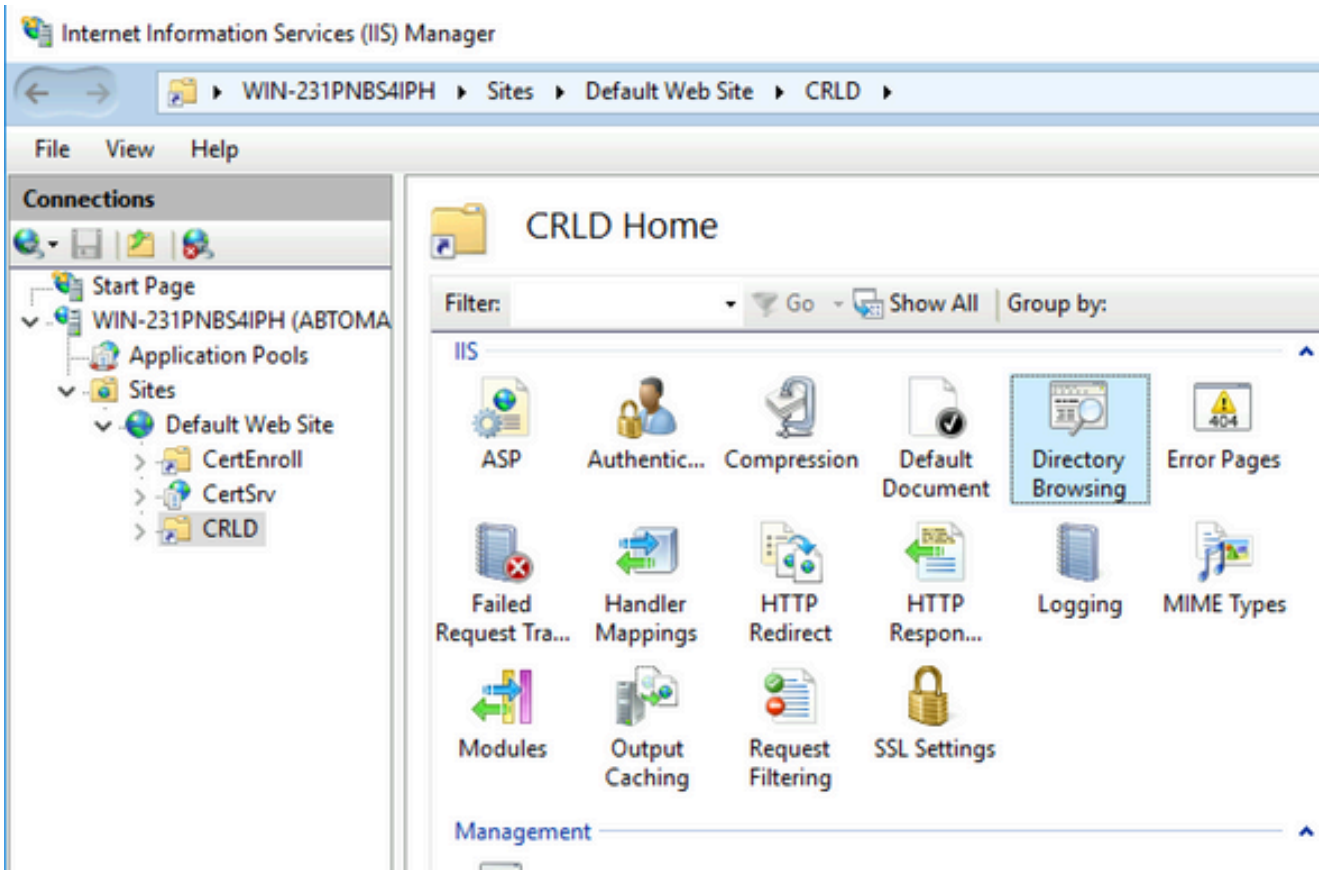
4. Alias(별칭) 필드에 CRL 배포 지점의 사이트 이름을 입력합니다. 이 예제에서는 CRLD를 입력합니다.



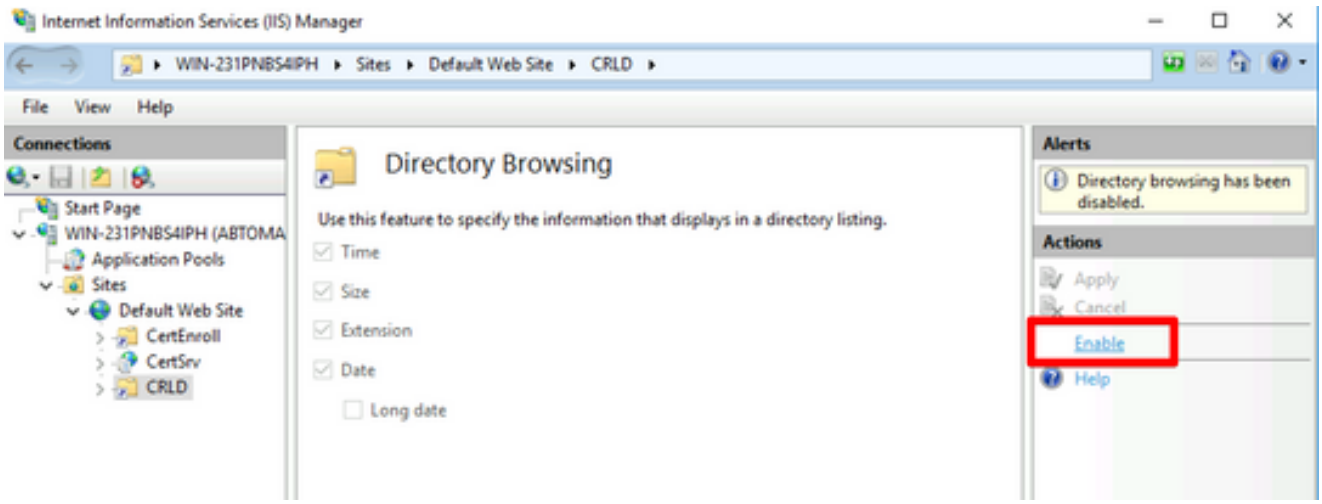
5. 줄임표(.)를 클릭합니다. .) Physical path(물리적 경로) 필드의 오른쪽에서 섹션 1에 생성된 폴더를 찾습니다. 폴더를 선택하고 을 ок누릅니다. Add Virtual Directory(가상 디렉토리 추가) 창을 ок 닫으려면 클릭합니다.



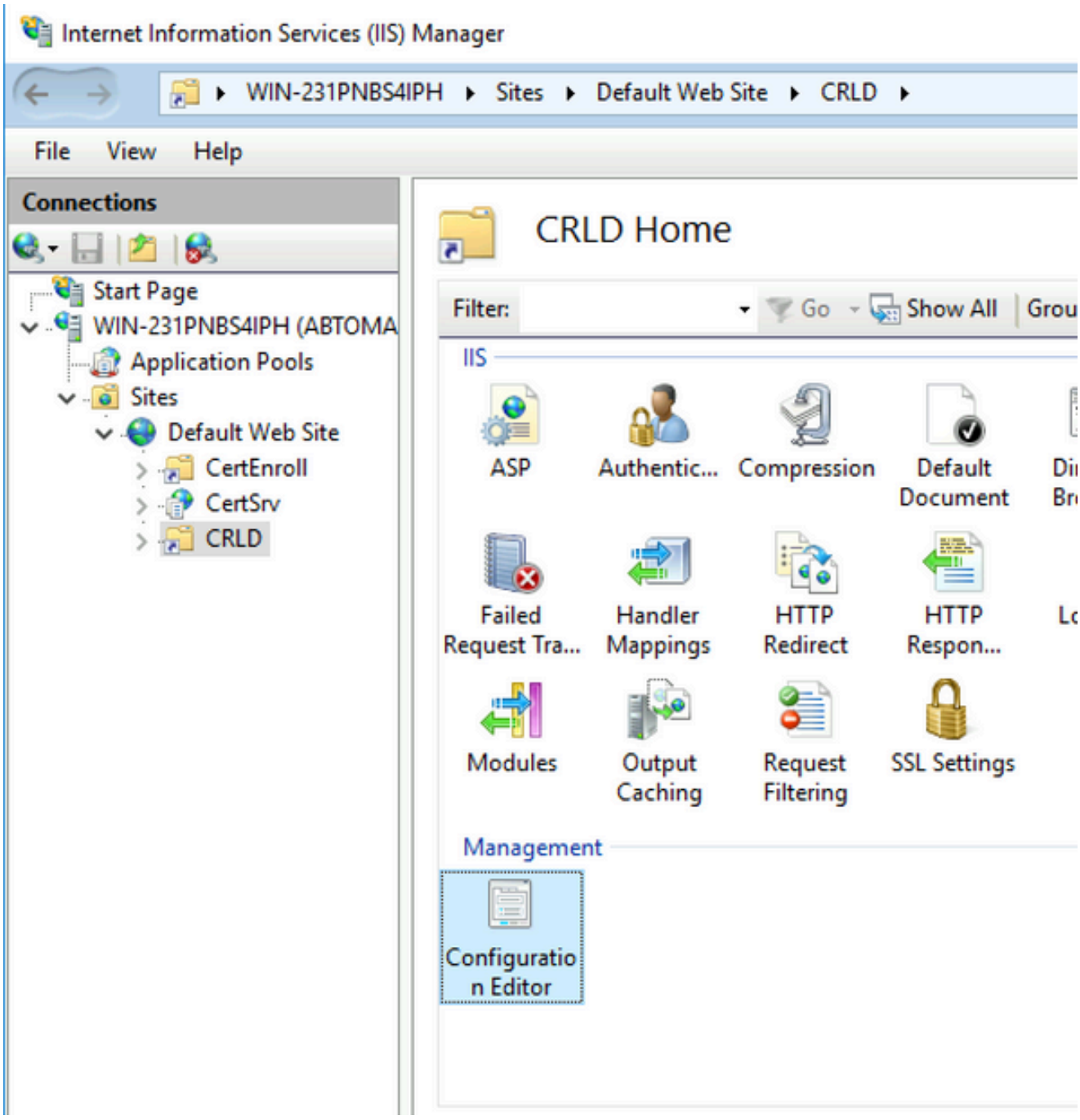
6. 4단계에서 입력한 사이트 이름은 왼쪽 창에서 강조 표시되어야 합니다. 그렇지 않은 경우 지금 선택합니다. 중앙 창에서 두 번 클릭합니다**Directory Browsing.**



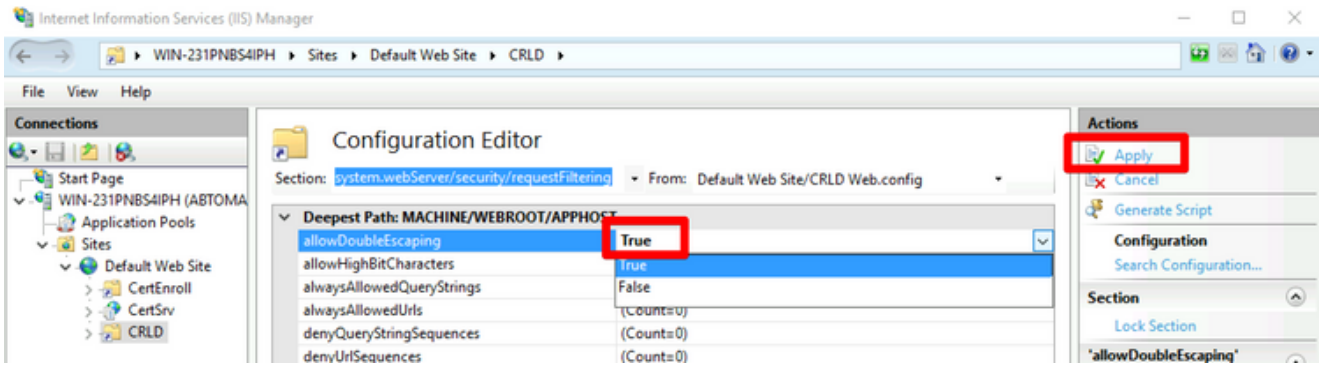
7. 오른쪽 창에서 를 클릭하여 디렉토리 **Enable** 찾아보기를 활성화합니다.



8. 왼쪽 창에서 사이트 이름을 다시 선택합니다. 중앙 창에서 두 번 클릭합니다**Configuration Editor**.



9. 섹션 드롭다운 목록에서 을 선택합니다**system.webServer/security/requestFiltering**. 드롭다운 **allowDoubleEscaping** 목록에서 을 선택합니다**True**. 오른쪽 창에서 을 클릭합니다(이 이미지**Apply**에 표시됨).

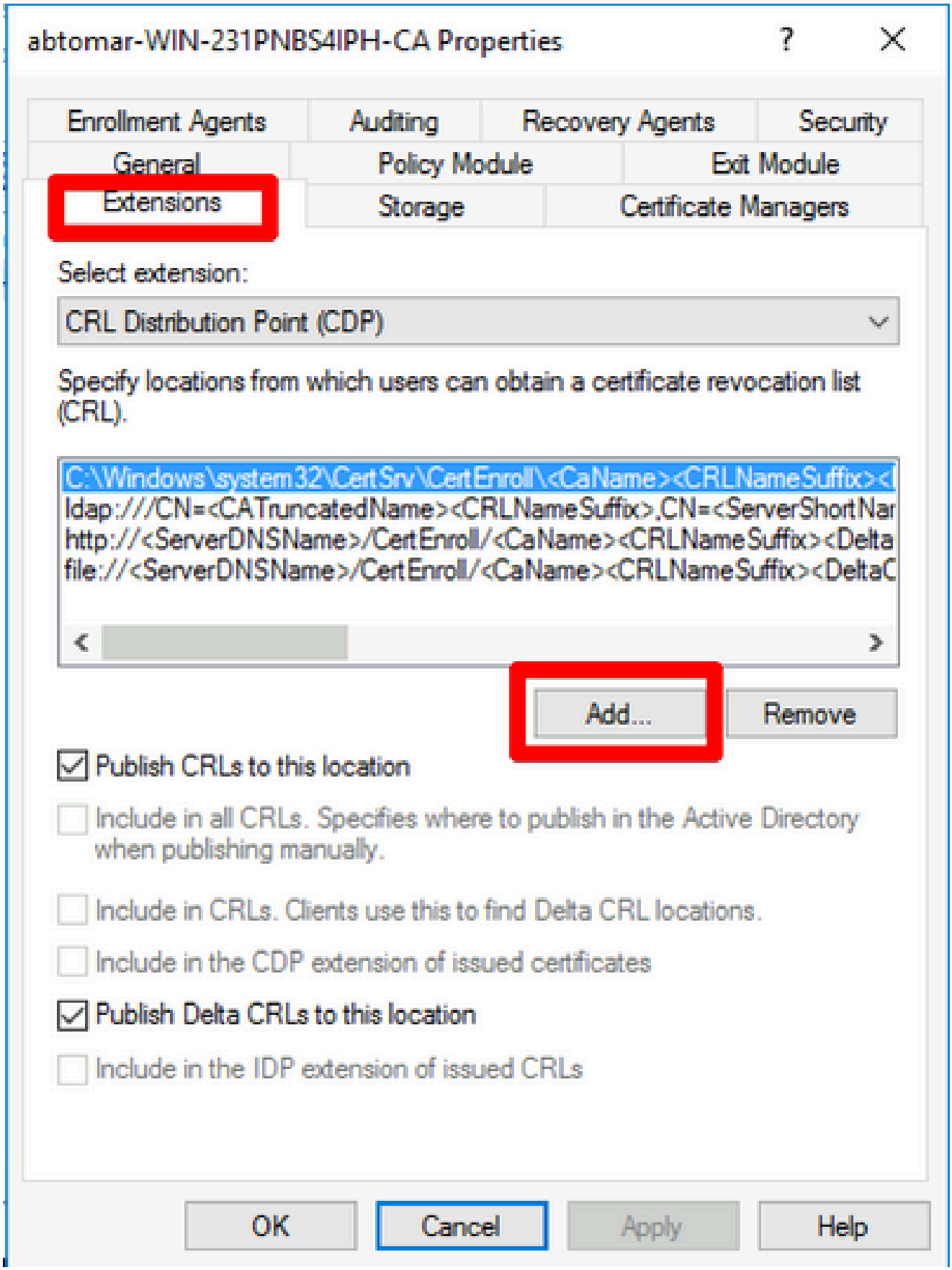


이제 IIS를 통해 폴더에 액세스할 수 있어야 합니다.

배포 지점에 CRL 파일을 게시하도록 Microsoft CA 서버 구성

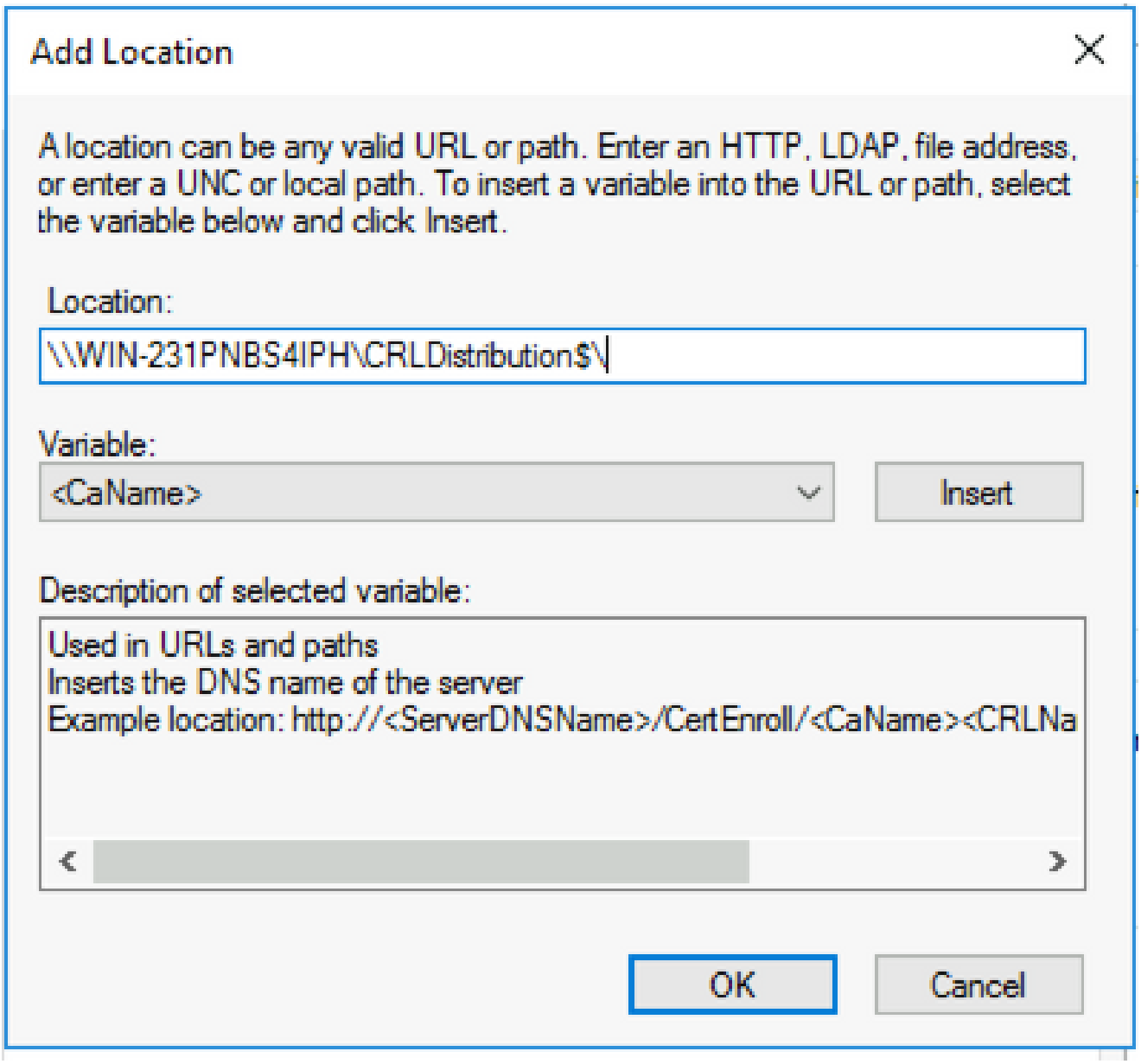
CRL 파일을 보관하도록 새 폴더가 구성되었고 IIS에서 폴더가 노출되었으므로 CRL 파일을 새 위치에 게시하도록 Microsoft CA 서버를 구성합니다.

1. CA 서버 작업 표시줄에서 를 **Start**클릭합니다. 를 **Administrative Tools** > **Certificate Authority**선택합니다.
2. 왼쪽 창에서 CA 이름을 마우스 오른쪽 버튼으로 클릭합니다. 선택 **Properties** 한 다음 탭을 클릭 **Extensions** 합니다. 새 CRL 배포 지점을 추가하려면 를 **Add**클릭합니다.

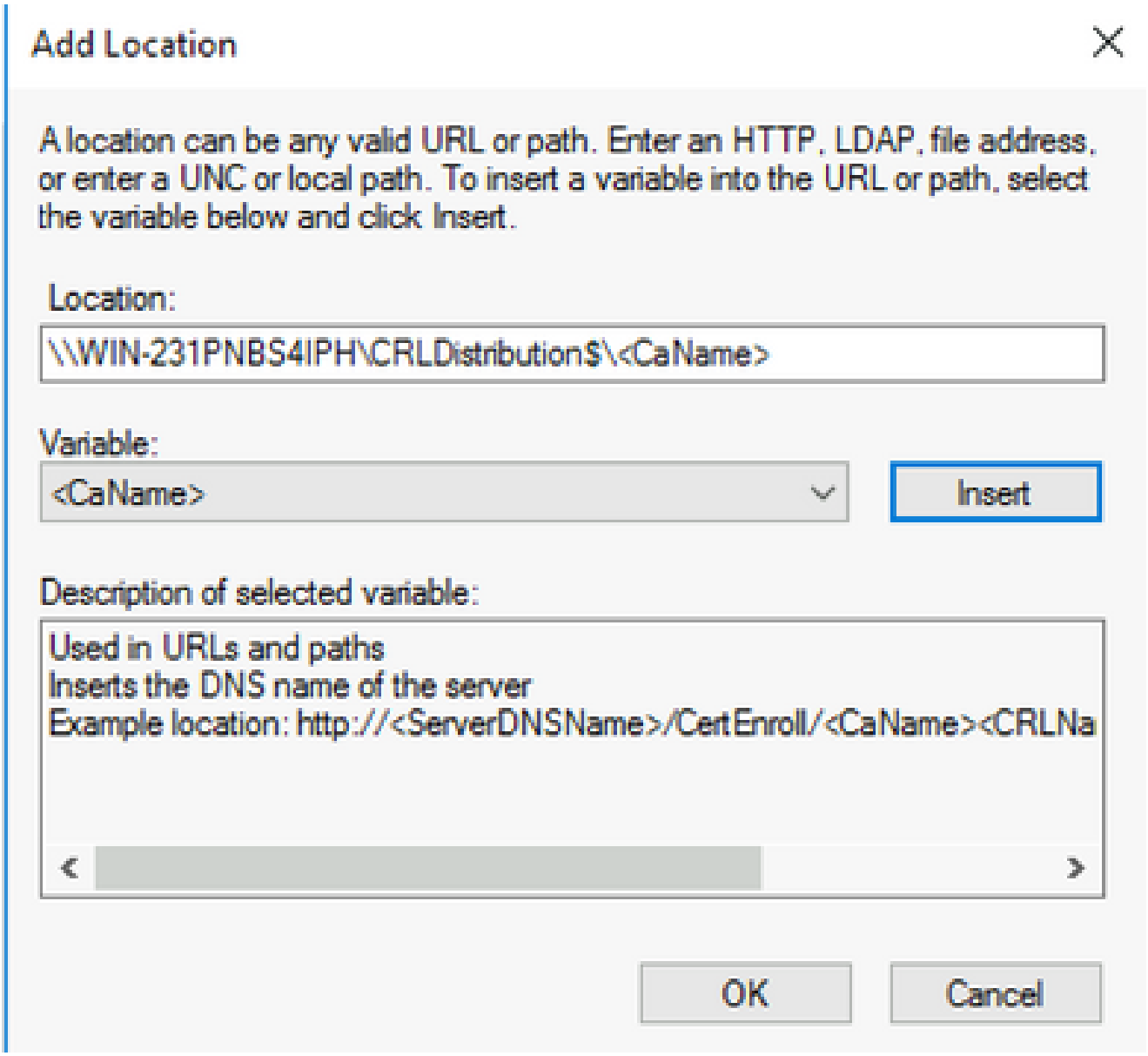


3. 위치 필드에 섹션 1에서 생성하고 공유하는 폴더의 경로를 입력합니다. 섹션 1의 예에서 경로는 다음과 같습니다.

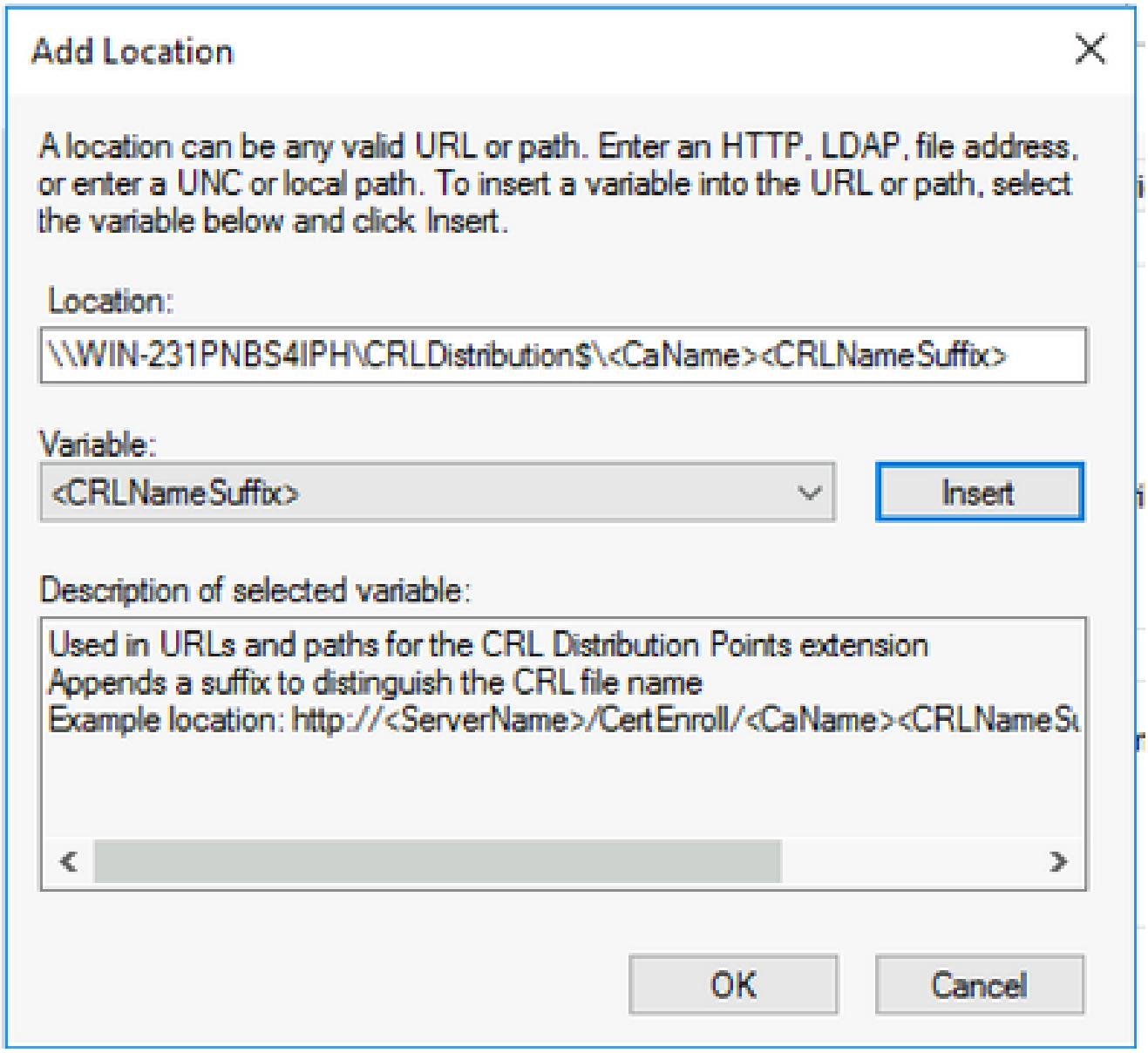
\\WIN-231PNBS4IPH\CRLDidistribution$



4. Location(위치) 필드가 채워진 상태에서 Variable(변수) 드롭다운 목록에서 선택한 다음 **Insert.**



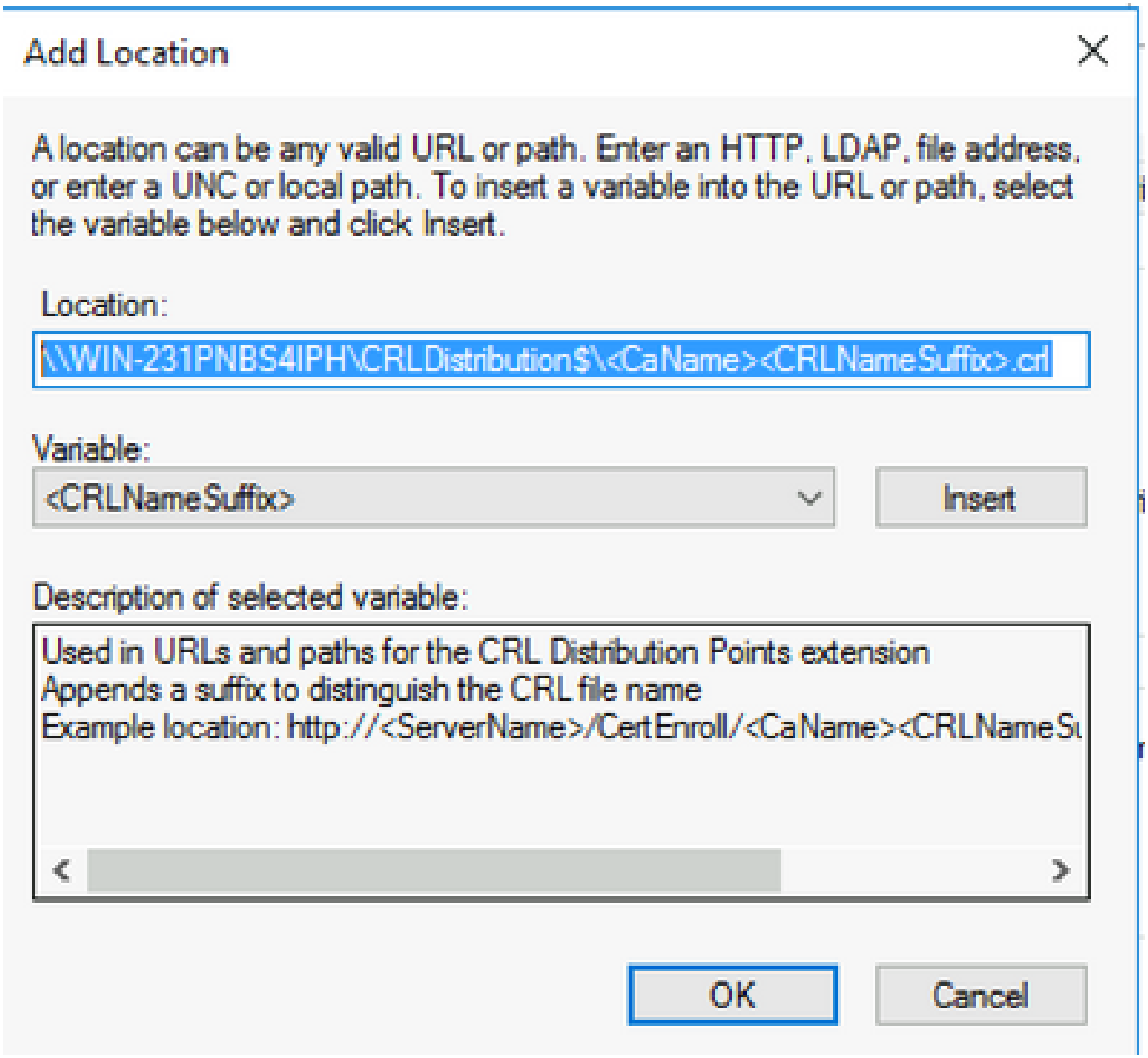
5. Variable 드롭다운 목록에서 을 선택하고
   를 클릭합니다**Insert**.



6. Location 필드에서 경로의 끝.crl에 추가합니다. 이 예에서 위치는 다음과 같습니다.

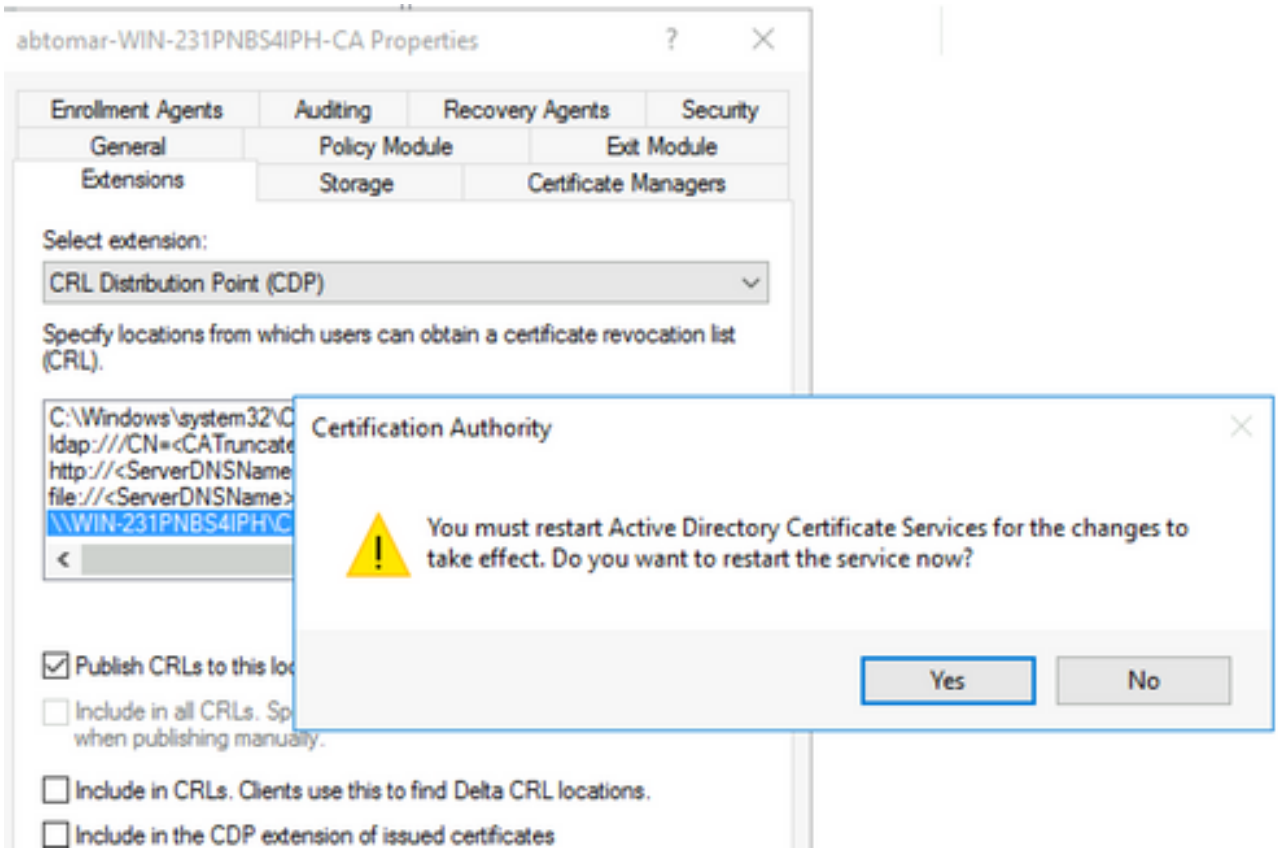
\\WIN-231PNBS4IPH\CRLDistribution$

.crl

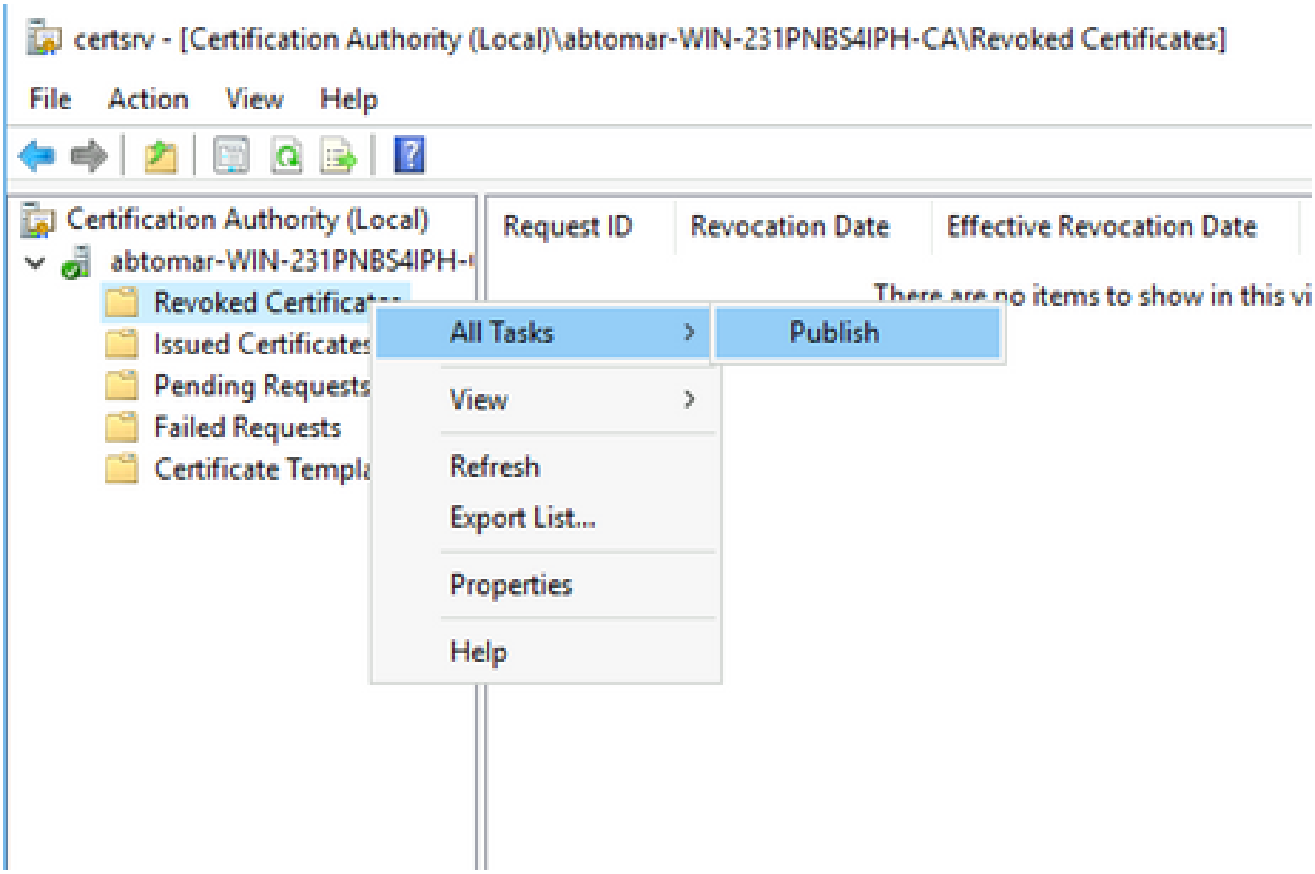


7. Extensions(확장) 탭으로 돌아가려면 **OK** 클릭합니다. 확인란을 **Publish CRLs to this location** 선택한 다음 를 클릭하여 속성 창**OK**을 닫습니다.

   Active Directory 인증서 서비스를 다시 시작할 수 있는 권한을 묻는 메시지가 나타납니다. 를 **Yes**클릭합니다.



8. 왼쪽 창에서 마우스 오른쪽 버튼을 **Revoked Certificates**클릭합니다. 를 **All Tasks** > **Publish**선택합니다. New CRL(새 CRL)이 선택되었는지 확인한 다음 을 **OK**클릭합니다.



Microsoft CA 서버는 섹션 1에서 만든 폴더에 새 .crl 파일을 만들어야 합니다. 새 CRL 파일이

성공적으로 생성되면 OK(확인)를 클릭한 후 대화 상자가 표시되지 않습니다. 새 배포 지점 폴더에 대한 오류가 반환되면 이 섹션의 각 단계를 신중하게 반복합니다.

CRL 파일이 있으며 IIS를 통해 액세스할 수 있는지 확인

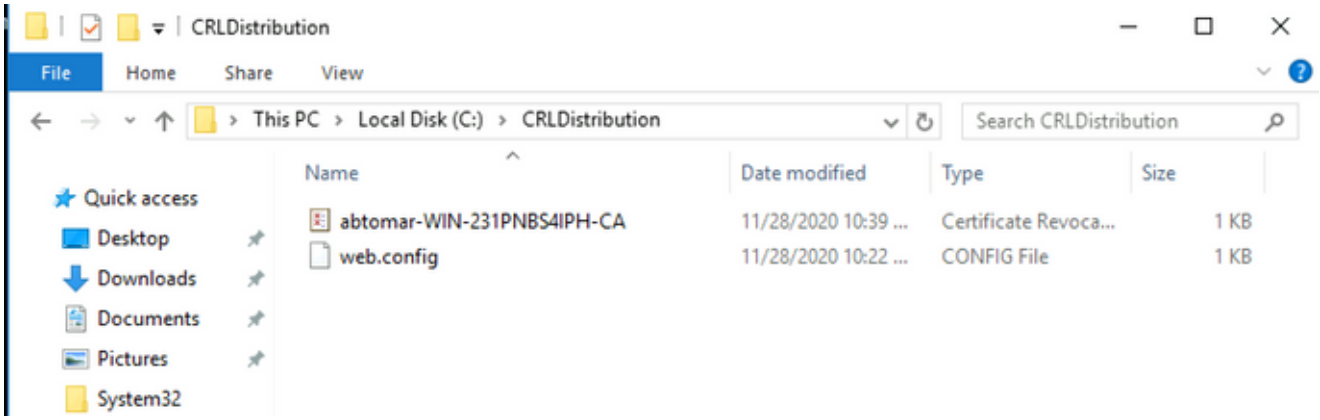
이 섹션을 시작하기 전에 새 CRL 파일이 존재하며 다른 워크스테이션에서 IIS를 통해 액세스할 수 있는지 확인하십시오.

1. IIS 서버에서 섹션 1에서 만든 폴더를 엽니다. 단일 .crl 파일이 있어야 하며

.crl

여기서
는 CA 서버의 이름입니다. 이 예에서 파일 이름은 다음과 같습니다.

abtomar-WIN-231PNBS4IPH-CA.crl



2. 네트워크의 워크스테이션(이상적으로 ISE 기본 관리 노드와 동일한 네트워크에 있음)에서 웹 브라우저를 열고 섹션 2에서 구성한 IIS 서버의 서버 이름과 섹션 2에서 배포 지점에 대해 선택한 사이트 이름을 http://

/

찾습니다
. 여기서
는 IIS 서버의 서버 이름입니다. 이 예에서 URL은 다음과 같습니다.

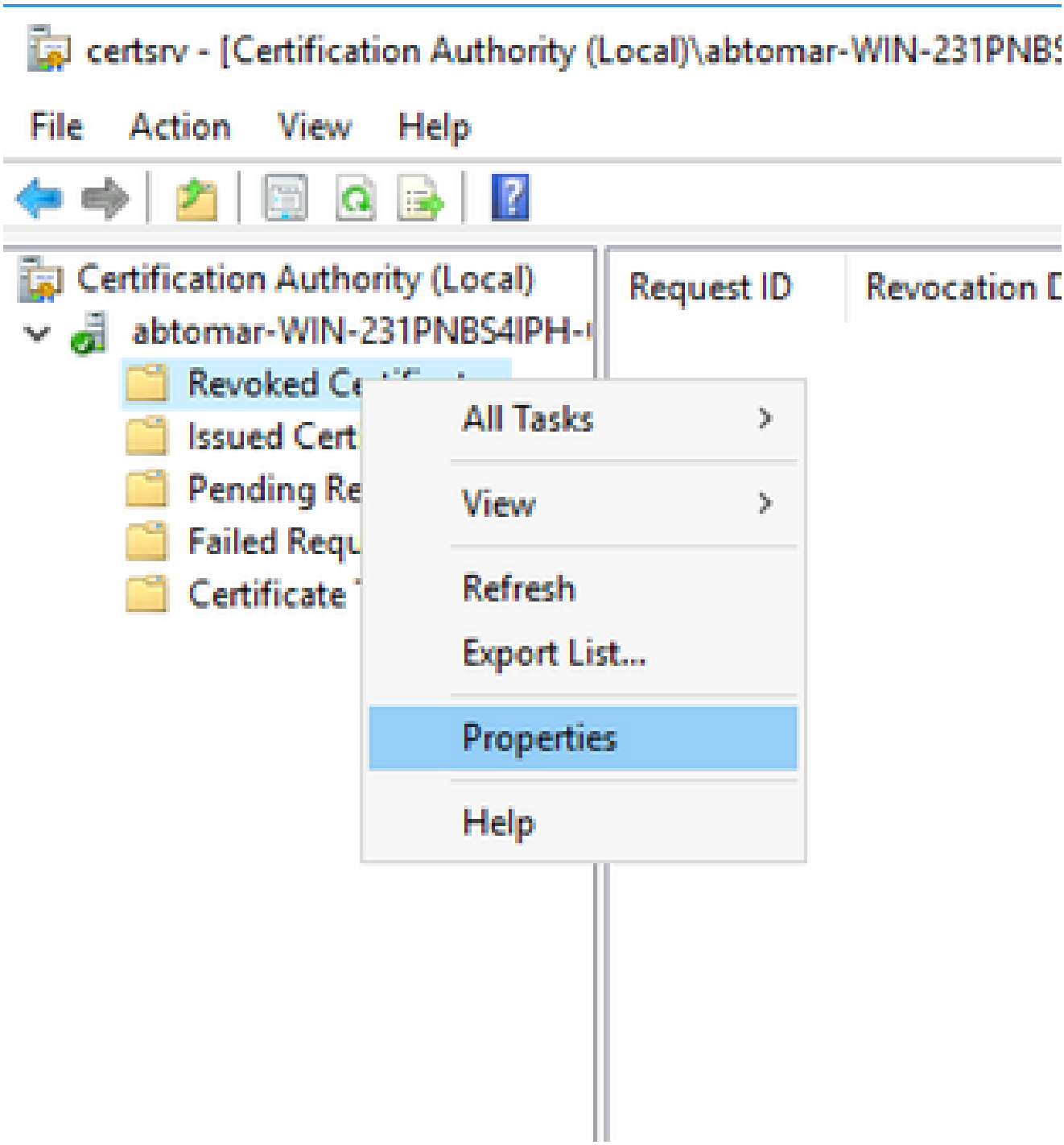
http://win-231pnbs4iph/CRLD

1단계에서 관찰된 파일을 포함하는 디렉토리 인덱스가 표시됩니다.

새 CRL 배포 지점을 사용하도록 ISE 구성

ISE가 CRL을 검색하도록 구성되기 전에 CRL을 게시할 간격을 정의합니다. 이 간격을 결정하는 전략은 이 문서의 범위를 벗어납니다. 잠재적 값(Microsoft CA)은 1시간 ~ 411년(포함)입니다. 기본값은 1주입니다. 환경에 적합한 간격이 결정되면 다음 지침을 참조하여 간격을 설정합니다.

1. CA 서버 작업 표시줄에서 를 **Start**클릭합니다. 를 **Administrative Tools** > **Certificate Authority**선택합니다.
2. 왼쪽 창에서 CA를 확장합니다. 폴더를 마우스 오른쪽 단추로 **Revoked Certificates** 클릭하고 을 선택합니다**Properties.**
3. CRL 게시 간격 필드에 필수 번호를 입력하고 기간을 선택합니다. 창**OK**을 닫고 변경 사항을 적용하려면 클릭합니다. 이 예에서는 게시 간격을 7일로 구성합니다.



4. ClockSkew **certutil -getreg CA\Clock*** 값을 확인하려면 명령을 입력합니다. 기본값은 10분입니다.

   출력 예:

```
Values:
    ClockSkewMinutes        REG_DWORS = a (10)
CertUtil: -getreg command completed successfully.
```

5. 명령을 **certutil -getreg CA\CRLov*** 입력하여 CRLOverlapPeriod가 수동으로 설정되었는지 확인합니다. 기본적으로 CRLOverlapUnit 값은 0이며, 이는 수동 값이 설정되지 않았음을 나타냅니다. 값이 0이 아닌 경우 값과 단위를 기록합니다.

출력 예:

```
Values:
    CRLOverlapPeriod      REG_SZ = Hours
    CRLOverlapUnits        REG_DWORD = 0
CertUtil: -getreg command completed successfully.
```

6. 명령을 **certutil -getreg CA\CRLpe*** 입력하여 3단계에서 설정한 CRLPeriod를 확인합니다.

출력 예:

```
Values:
    CRLPeriod      REG_SZ = Days
    CRLUnits        REG_DWORD = 7
CertUtil: -getreg command completed successfully.
```

7. 다음과 같이 CRL 유예 기간을 계산합니다.

a. CRLOverlapPeriod가 5단계에서 설정된 경우: OVERLAP = CRLOverlapPeriod, 분 단위

기타: OVERLAP = (CRLPeriod / 10), 분 단위

b. OVERLAP이 720을 초과하는 경우 OVERLAP = 720

c. OVERLAP < (1.5 * ClockSkewMinutes)이 발생하면 OVERLAP = (1.5 * ClockSkewMinutes)

d. OVERLAP > CRLPeriod인 경우(분) OVERLAP = CRLPeriod(분)

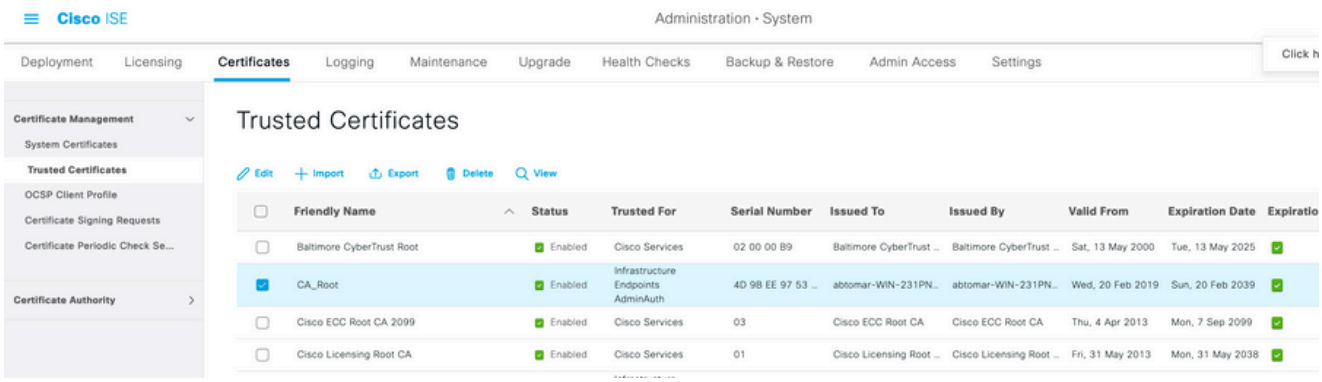
e. Grace Period = OVERLAP + ClockSkewMinutes

```
Example:

As stated above, CRLPeriod was set to 7 days, or 10248 minutes and CRLOverlapPeriod was not set.


a. OVERLAP = (10248 / 10) = 1024.8 minutes
b. 1024.8 minutes is > 720 minutes : OVERLAP = 720 minutes
c. 720 minutes is NOT < 15 minutes : OVERLAP = 720 minutes
d. 720 minutes is NOT > 10248 minutes : OVERLAP = 720 minutes
e. Grace Period = 720 minutes + 10 minutes = 730 minutes
```

계산된 유예 기간은 CA가 다음 CRL을 게시하는 시점과 현재 CRL이 만료되는 시점 사이의 시간입니다. 그에 따라 CRL을 검색하도록 ISE를 구성해야 합니다.

8. ISE 기본 관리 노드에 로그인하고 를 선택합니다**Administration** > **System** > **Certificates**. 왼쪽 창에서 를

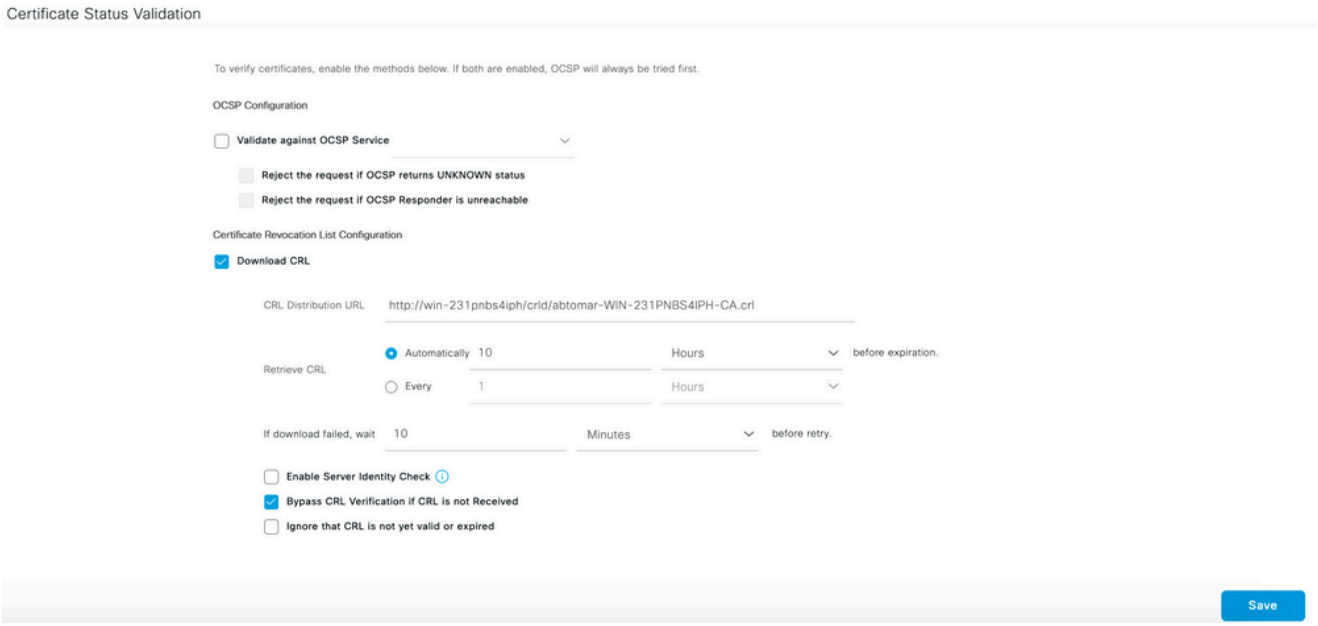
선택합니다**Trusted Certificate.**



9. CRL을 구성하려는 CA 인증서 옆의 확인란을 선택합니다. 를 **Edit**클릭합니다.
10. 창 아래쪽에서 확인란을 **Download CRL** 선택합니다.
11. CRL Distribution URL(CRL 배포 URL) 필드에 CRL 배포 지점의 경로를 입력합니다. 이 경로에는 섹션 2에서 생성한 .crl 파일이 포함됩니다. 이 예에서 URL은 다음과 같습니다.

    http://win-231pnbs4iph/crld/abtomar-WIN-231PNBS4IPH-CA.crl

12. ISE는 정기적으로 또는 만료에 따라 CRL을 검색하도록 구성할 수 있습니다(일반적으로 이 기간도 정기임). CRL 게시 간격이 정적일 경우, 후자 옵션을 사용할 때 더 적시에 CRL 업데이트를 얻을 수 있습니다. 라디오 버튼을 **Automatically** 클릭합니다.
13. 읽어들일 값을 단계 7에서 계산한 유예 기간보다 작은 값으로 설정합니다. 값 집합이 유예 기간보다 긴 경우 ISE는 CA가 다음 CRL을 게시하기 전에 CRL 배포 지점을 확인합니다. 이 예에서 유예 기간은 730분, 또는 12시간 10분으로 계산됩니다. 10시간 값이 검색에 사용됩니다.
14. 환경에 적합한 재시도 간격을 설정합니다. ISE는 이전 단계에서 구성된 간격으로 CRL을 검색할 수 없는 경우 이 짧은 간격으로 다시 시도합니다.
15. ISE가 **Bypass CRL Verification if CRL is not Received** 마지막 다운로드 시도에서 이 CA에 대한 CRL을 검색할 수 없는 경우 CRL 확인 없이 인증서 기반 인증이 정상적으로 진행되도록 허용하려면 확인란을 선택합니다. 이 확인란을 선택하지 않으면 CRL을 검색할 수 없는 경우 이 CA에서 발급한 인증서를 사용하는 모든 인증서 기반 인증이 실패합니다.
16. ISE가 **Ignore that CRL is not yet valid or expired** 만료된(또는 아직 유효하지 않은) CRL 파일을 유효한 것처럼 사용하도록 허용하려면 확인란을 선택합니다. 이 확인란을 선택하지 않으면 ISE는 CRL을 유효 날짜 이전 및 다음 업데이트 시간 이후에 유효하지 않은 것으로 간주합니다. 컨피그레이션**Save**을 완료하려면 클릭하십시오.



다음을 확인합니다.

현재 이 설정에 사용 가능한 확인 절차는 없습니다.

문제 해결

현재 이 설정에 사용할 수 있는 특정 문제 해결 정보가 없습니다.

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.