ISE용 인증서 해지 목록을 게시하도록 Microsoft CA Server 구성

목차

소개

이 문서에서는 IIS(인터넷 정보 서비스)를 실행하여 CRL(인증서 해지 목록) 업데이트를 게시하는 Microsoft CA(Certificate Authority) 서버의 구성에 대해 설명합니다.또한 인증서 검증에 사용할 업데이트를 검색하도록 Cisco ISE(Identity Services Engine)(버전 3.0 이상)를 구성하는 방법에 대해서도 설명합니다.인증서 검증에서 사용하는 다양한 CA 루트 인증서에 대한 CRL을 검색하도록 ISE를 구성할 수 있습니다.

전제 조건

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.네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 이해해야 합니다.

구성

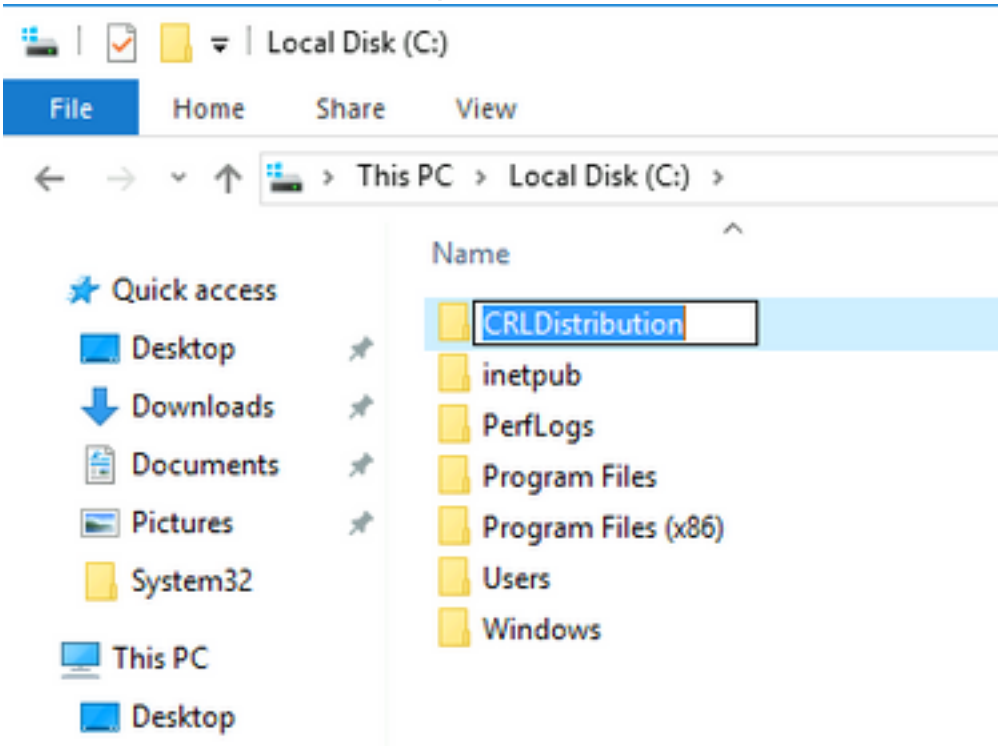
이 섹션에서는 이 문서에 설명된 기능을 구성하는 정보를 제공합니다.

CRL 파일을 보관할 CA의 폴더 생성 및 구성

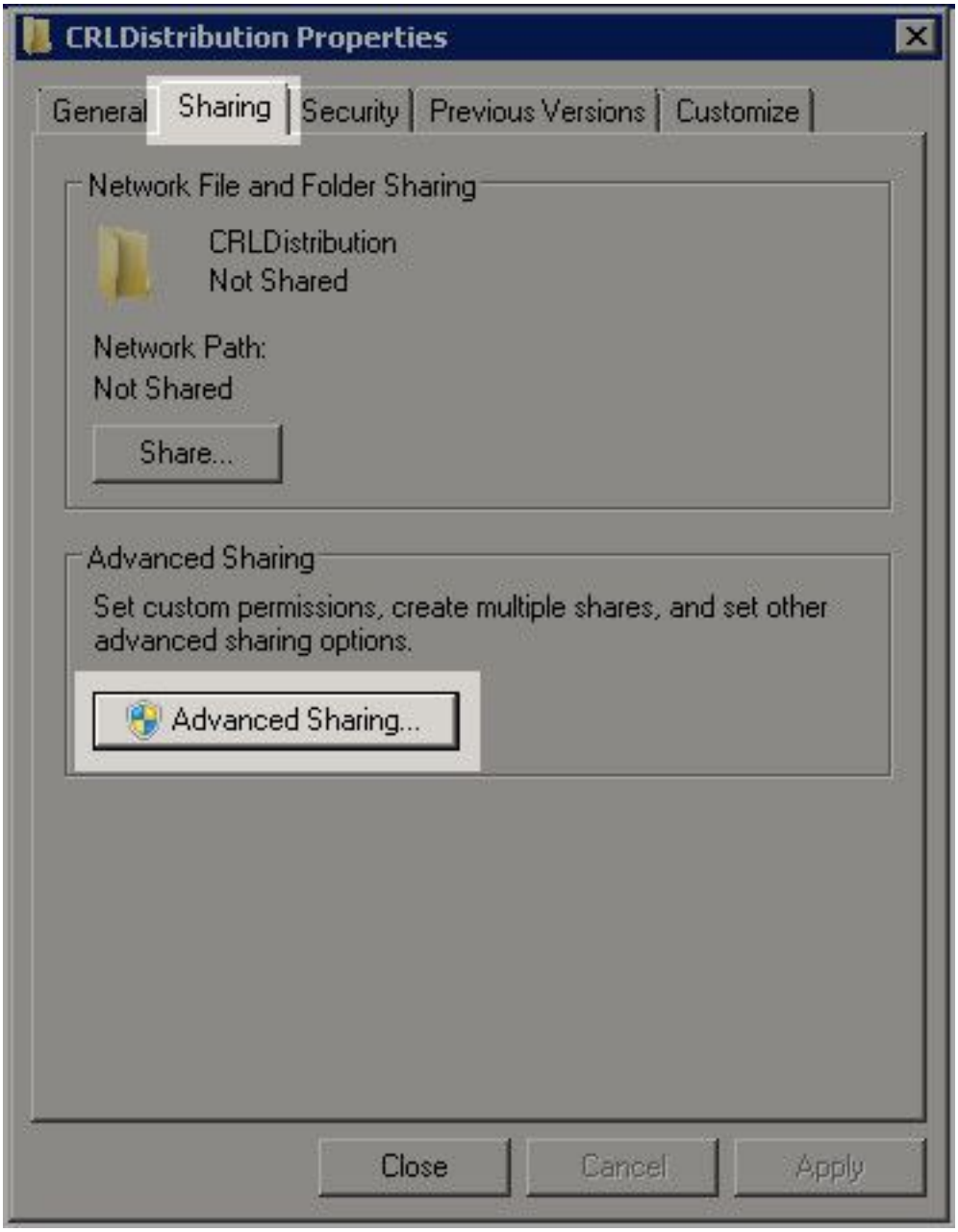
첫 번째 작업은 CA 서버에서 CRL 파일을 저장할 위치를 구성하는 것입니다.기본적으로 Microsoft CA 서버는 C:\Windows\system32\CertSrv\CertEnroll\에 파일을 게시합니다.

이 시스템 폴더를 사용하지 않고 파일의 새 폴더를 만듭니다.

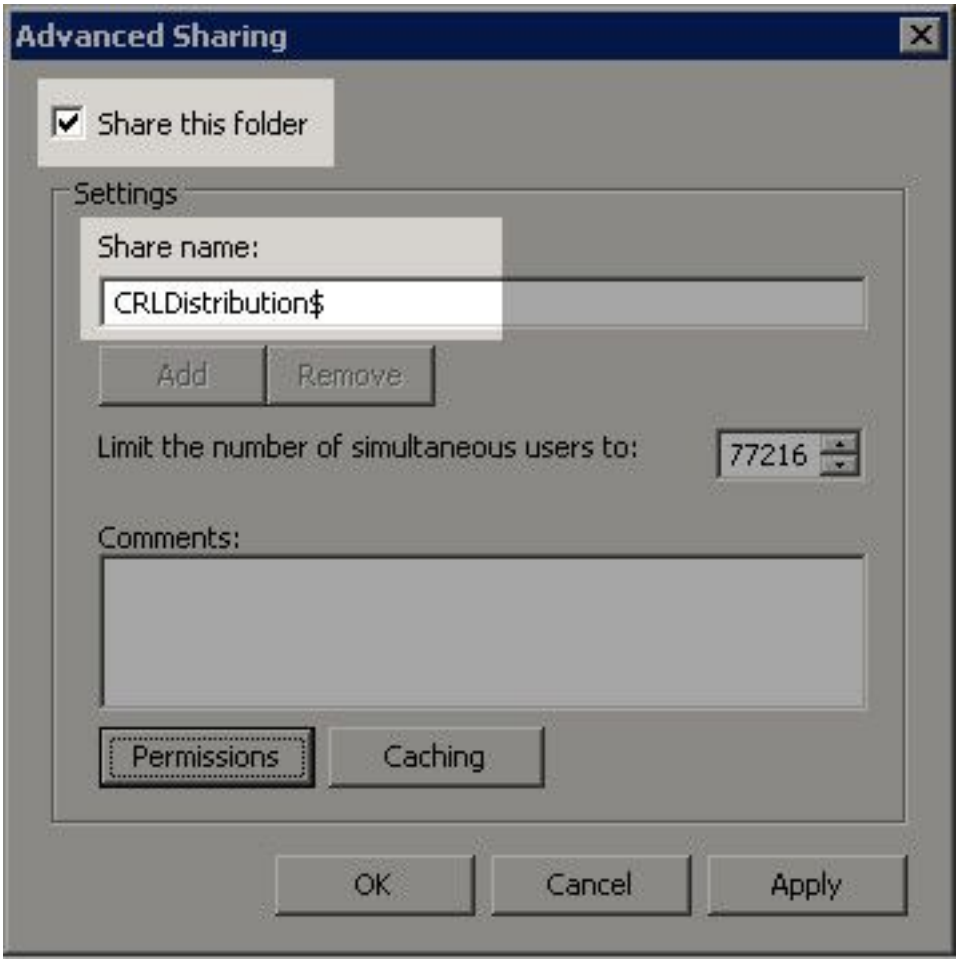
1. IIS 서버에서 파일 시스템의 위치를 선택하고 새 폴더를 만듭니다.이 예에서는 C:\CRLDistribution 폴더**가** 생성됩니다.



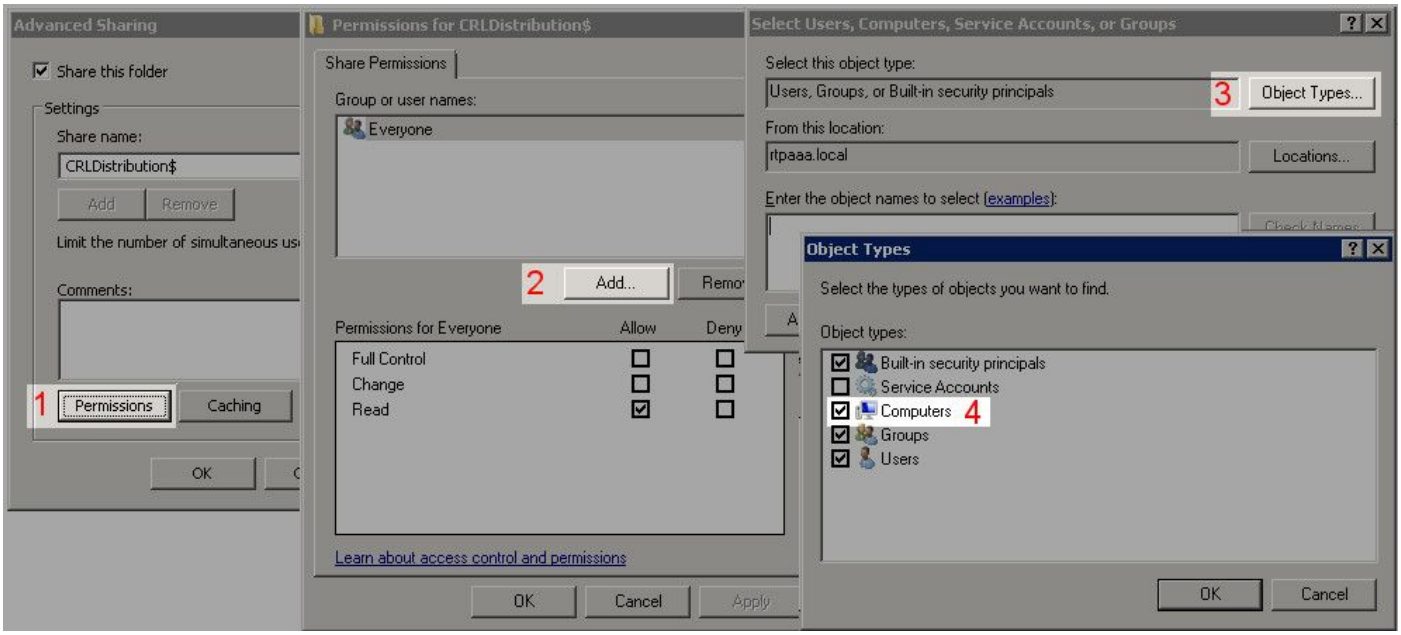
2. CA가 CRL 파일을 새 폴더에 쓰려면 공유를 활성화해야 합니다.새 폴더를 마우스 오른쪽 단추로 클릭하고 **속성**을 선택하고 **공유** 탭을 클릭한 다음 **고급 공유**를 클릭합니다.



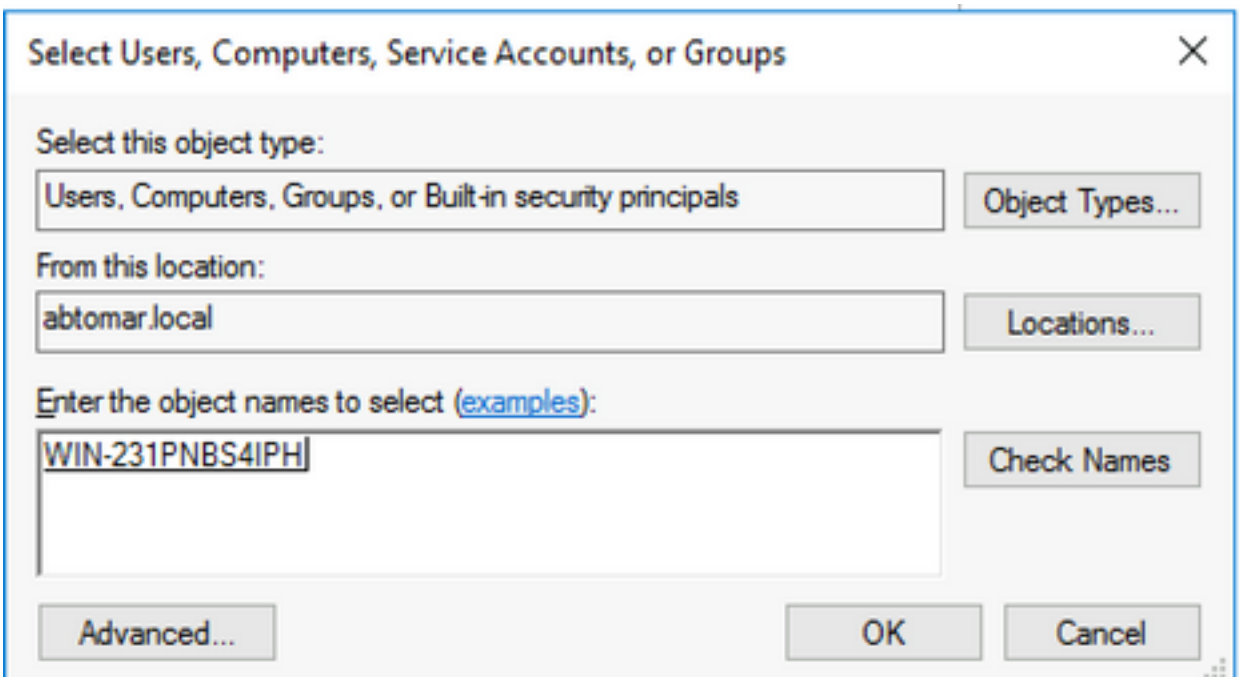
3. 폴더를 공유하려면 **이 폴더 공유** 확인란을 선택한 다음 공유 이름 필드에서 공유 이름의 끝에 달러 기호($)를 추가하여 공유를 숨깁니다.



4. **사용 권한**(1)을 클릭하고 **추가**(2)**를** 클릭하고 **개체 유형**(3)을 클릭한 다음 **컴퓨터** 확인란(4)을 선택합니다.

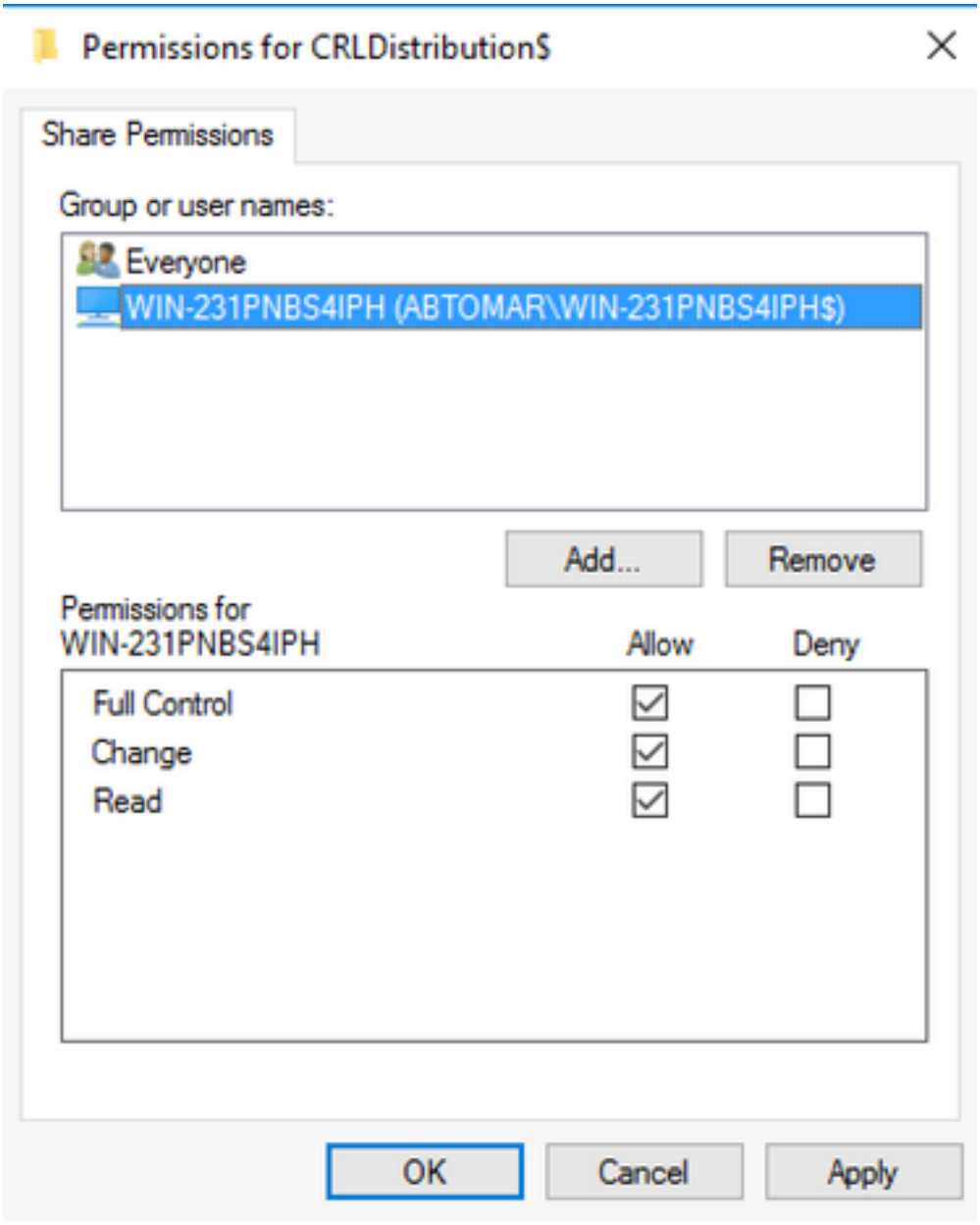


5 . 사용자, 컴퓨터, 서비스 계정 또는 그룹 선택 창으로 돌아가려면 **확인**을 클릭합니다.Enter the object names to select(선택할 개체 이름 입력) 필드에 다음 예에 CA 서버의 컴퓨터 이름을 입력합니다.WIN0231PNBS4IPH를 클릭하고 **이름 확인을** 클릭합니다.입력한 이름이 유효하면 이름이 새로 고쳐지고 밑줄이 표시됩니다.**확인**을 **클릭합니다**.



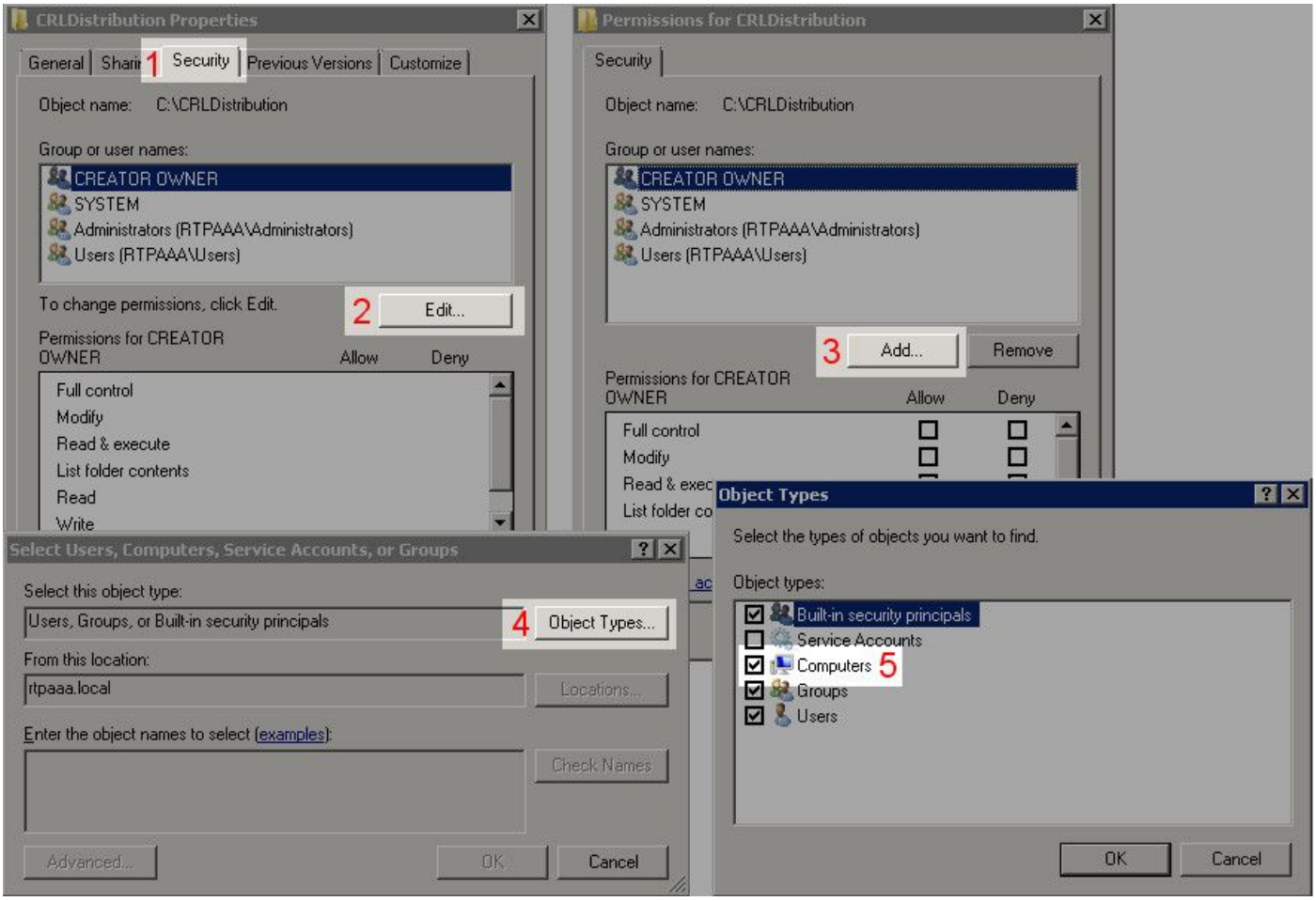
6 . Group or user names(그룹 또는 사용자 이름) 필드에서 CA 컴퓨터를 선택합니다.Allow for Full Control을 선택하여 CA에 대한 전체 액세스 권한을 부여합니다.

확인을 클릭합니다.확인을 다시 클릭하여 고급 공유 창을 닫고 속성 창으로 돌아갑니다.

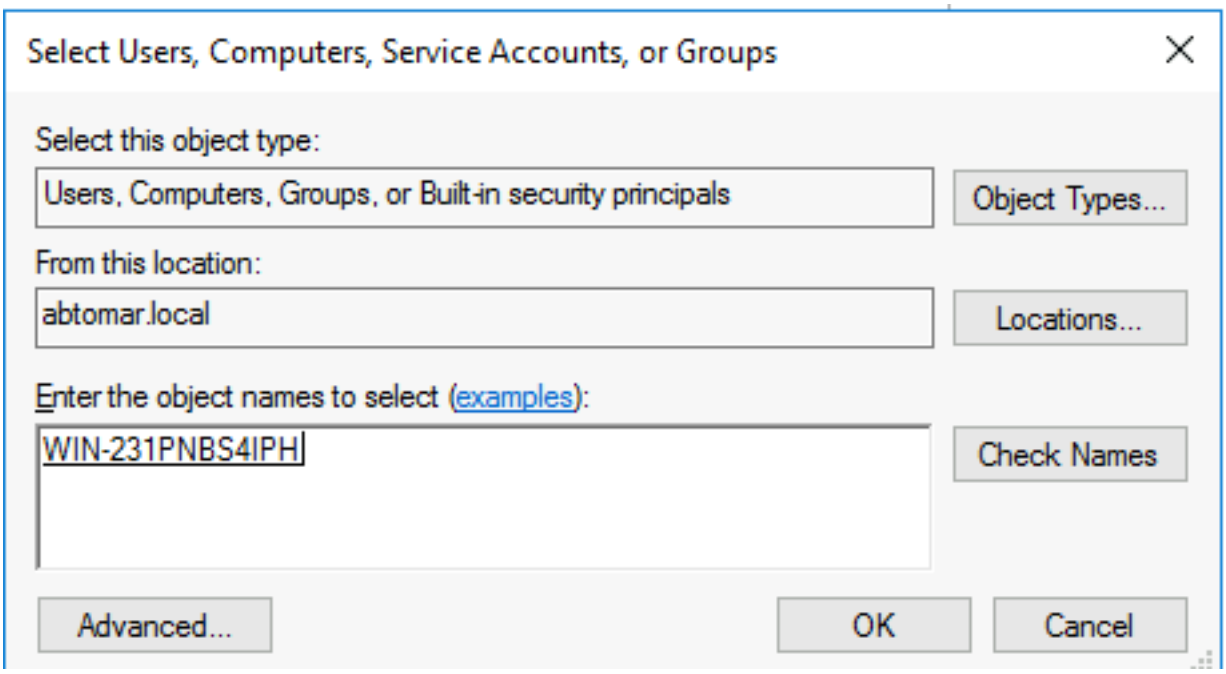


---

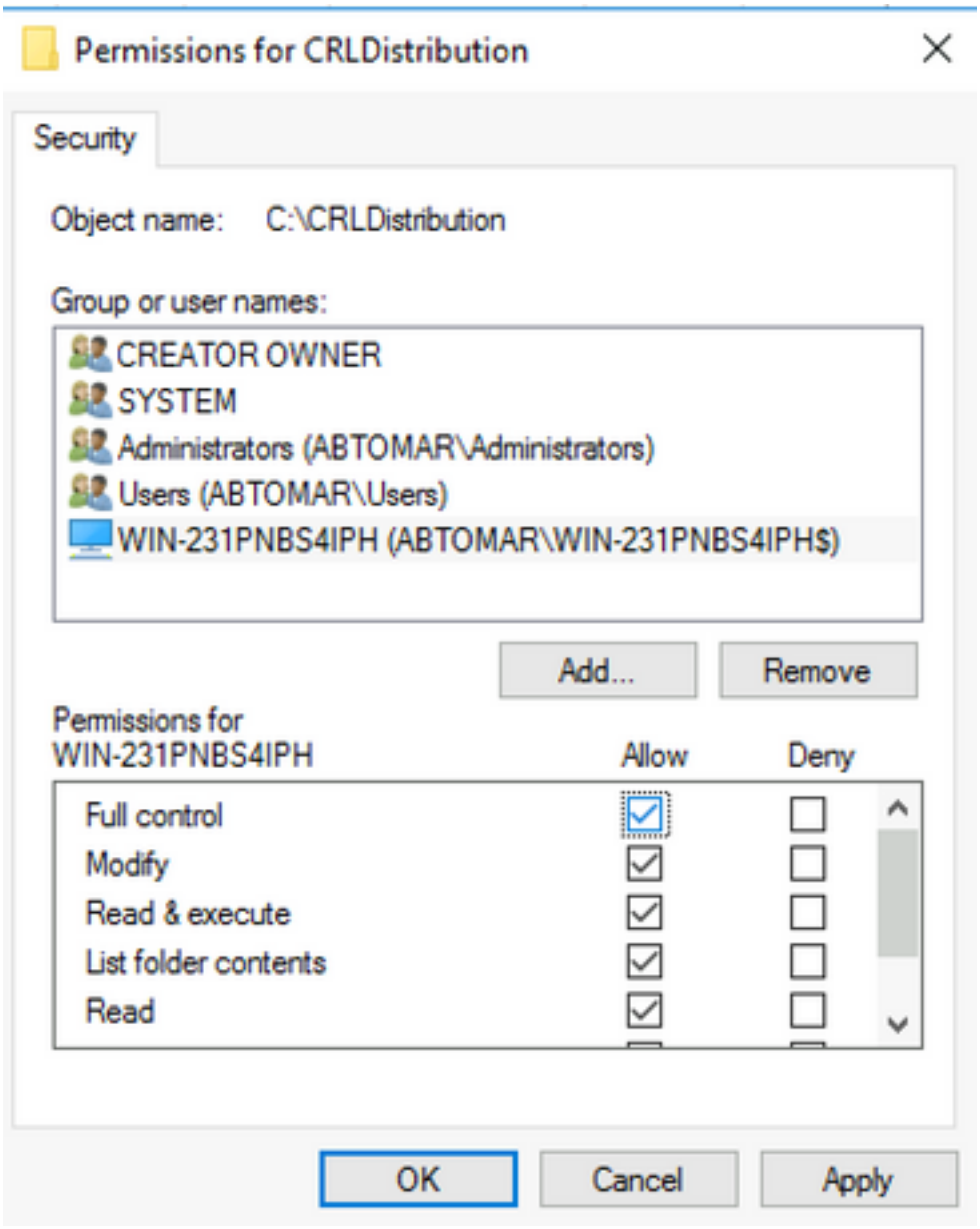
7. CA가 CRL 파일을 새 폴더에 쓸 수 있도록 하려면 적절한 보안 권한을 구성합니다.**보안** 탭(1)을 클릭하고 **편집**(2)을 클릭하고 **추가**(3)를 클릭하고 **개체 유형**(4)을 클릭한 다음 **컴퓨터 확인란(5)을 선택합니다.**



8. 선택할 개체 이름 입력 필드에 CA 서버의 컴퓨터 이름을 입력하고 **이름 확인**을 클릭합니다.입력한 이름이 유효하면 이름이 새로 고쳐지고 밑줄이 표시됩니다.**확인**을 **클릭합니다**.



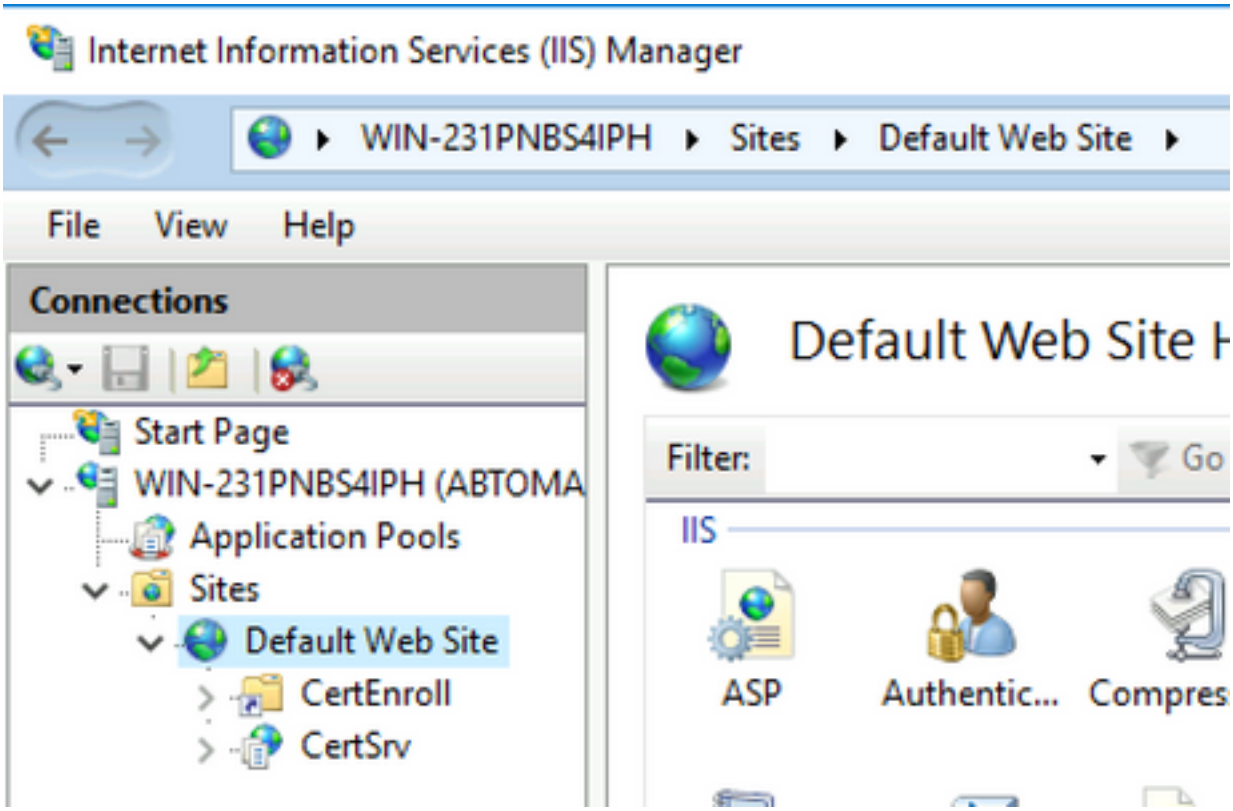
9. Group or user names(그룹 또는 사용자 이름) 필드에서 CA 컴퓨터를 선택한 다음 **Allow** for Full control(전체 제어 허용)에서 CA에 대한 전체 액세스 권한을 부여하도록 선택합니다.확인**을** 클릭한 다음 **닫기**를 클릭하여 작업을 완료합니다.



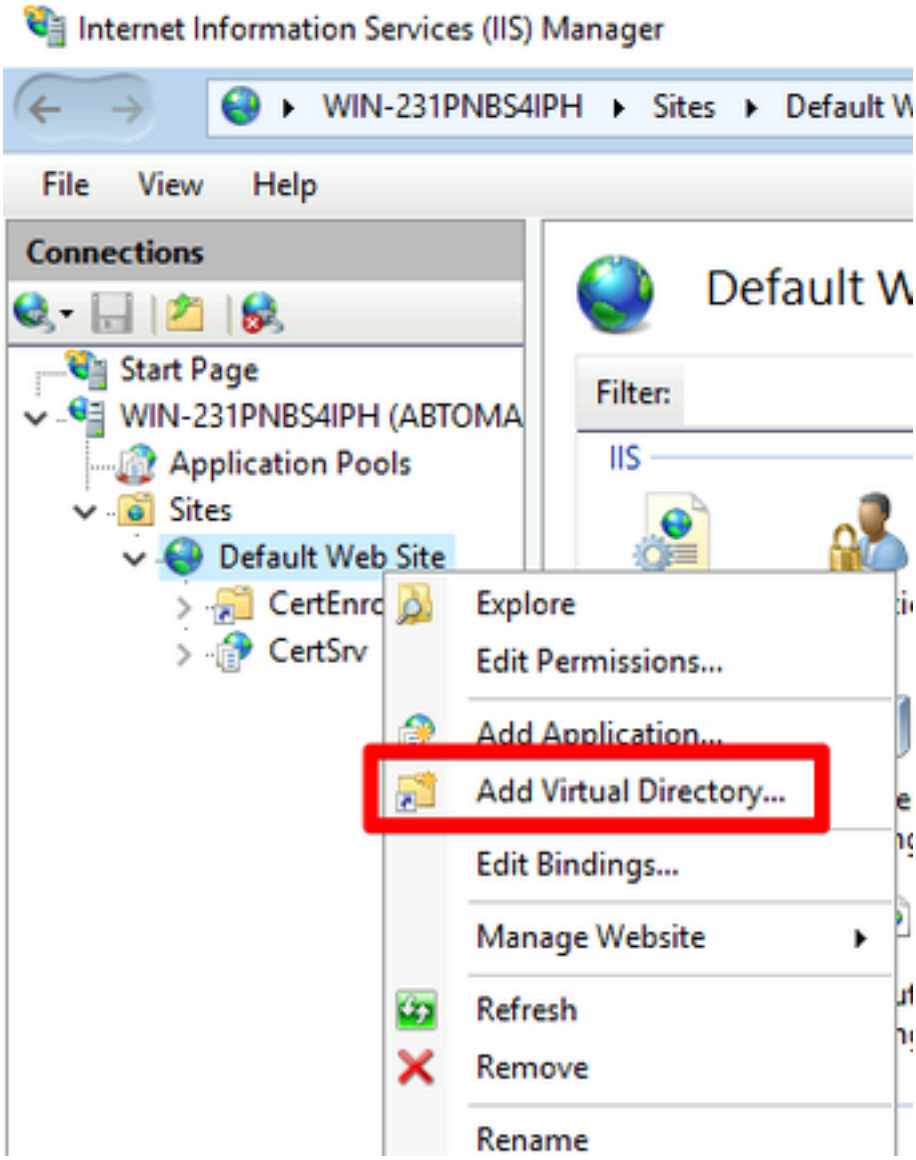
IIS에서 사이트를 만들어 새 CRL 배포 지점을 노출합니다.

ISE가 CRL 파일에 액세스하려면 IIS를 통해 CRL 파일을 포함하는 디렉토리를 액세스 가능하게 하십시오.

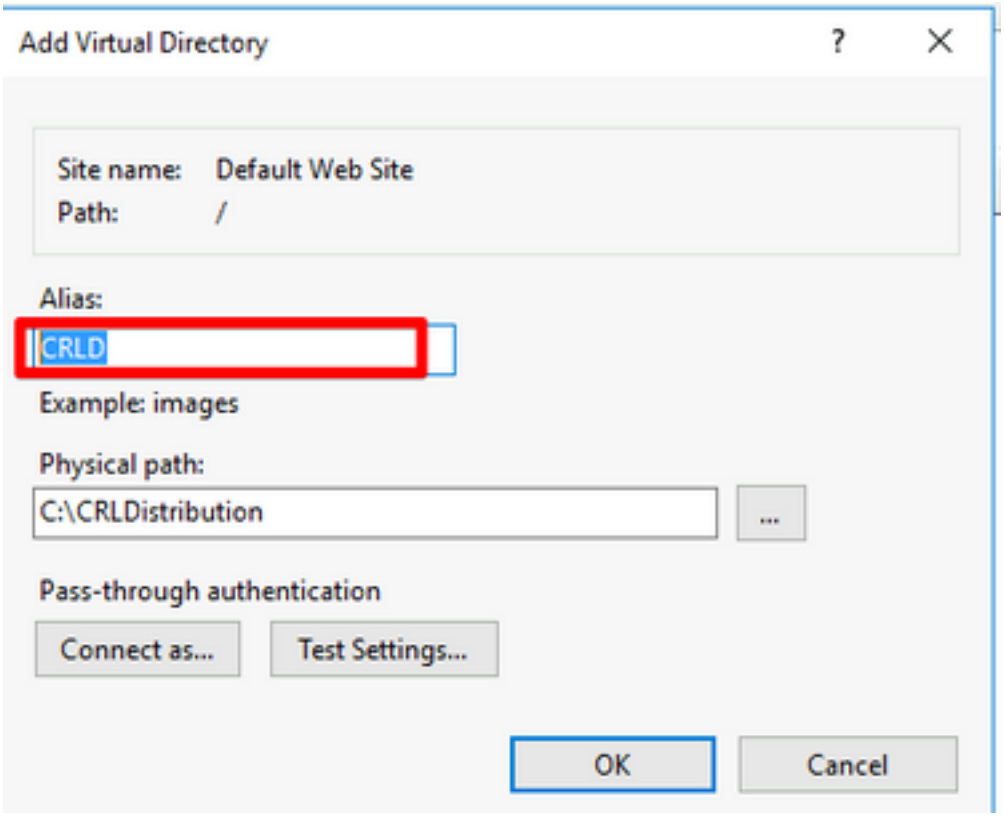
1. IIS 서버 작업 표시줄에서 **시작**을 클릭합니다.관리 **도구 > 인터넷 정보 서비스(IIS) 관리자를 선택합니다**.
2. 왼쪽 창(콘솔 트리라고 함)에서 IIS 서버 이름을 확장한 다음 사이트를 **확장합니다.**



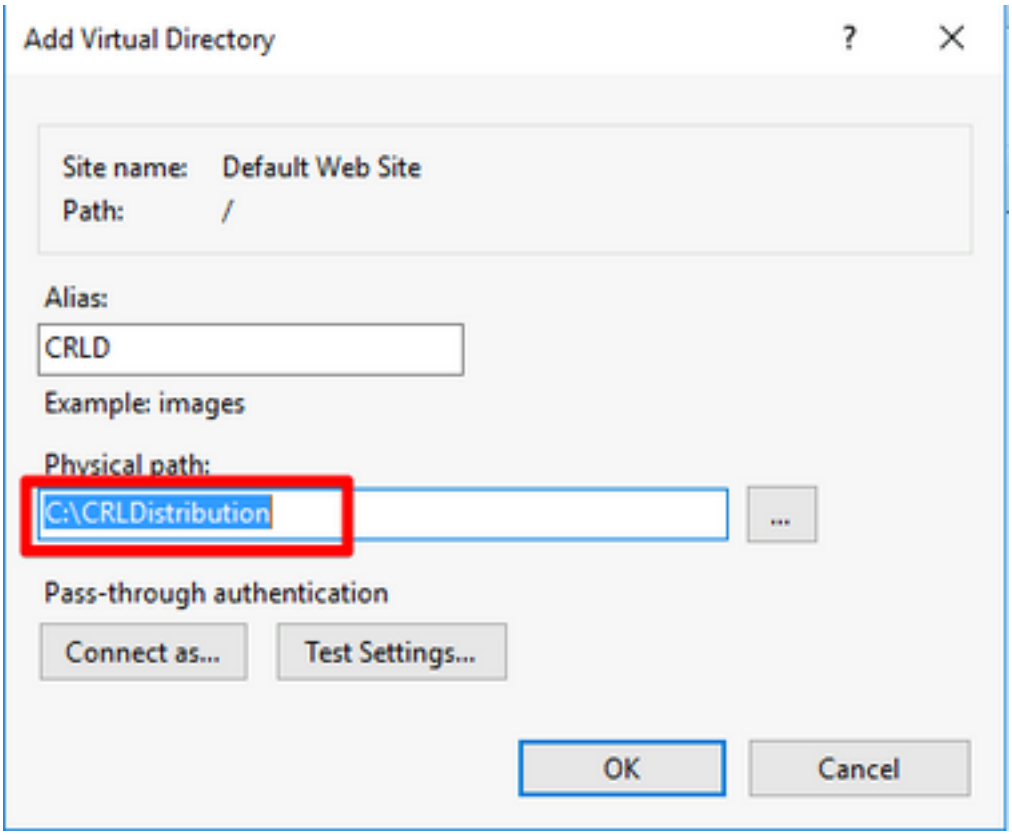
3. 기본 **웹 사이트**를 마우스 오른쪽 버튼으로 클릭하고 **가상 디렉터리 추가**(이 이미지에 표시됨)를 선택합니다.



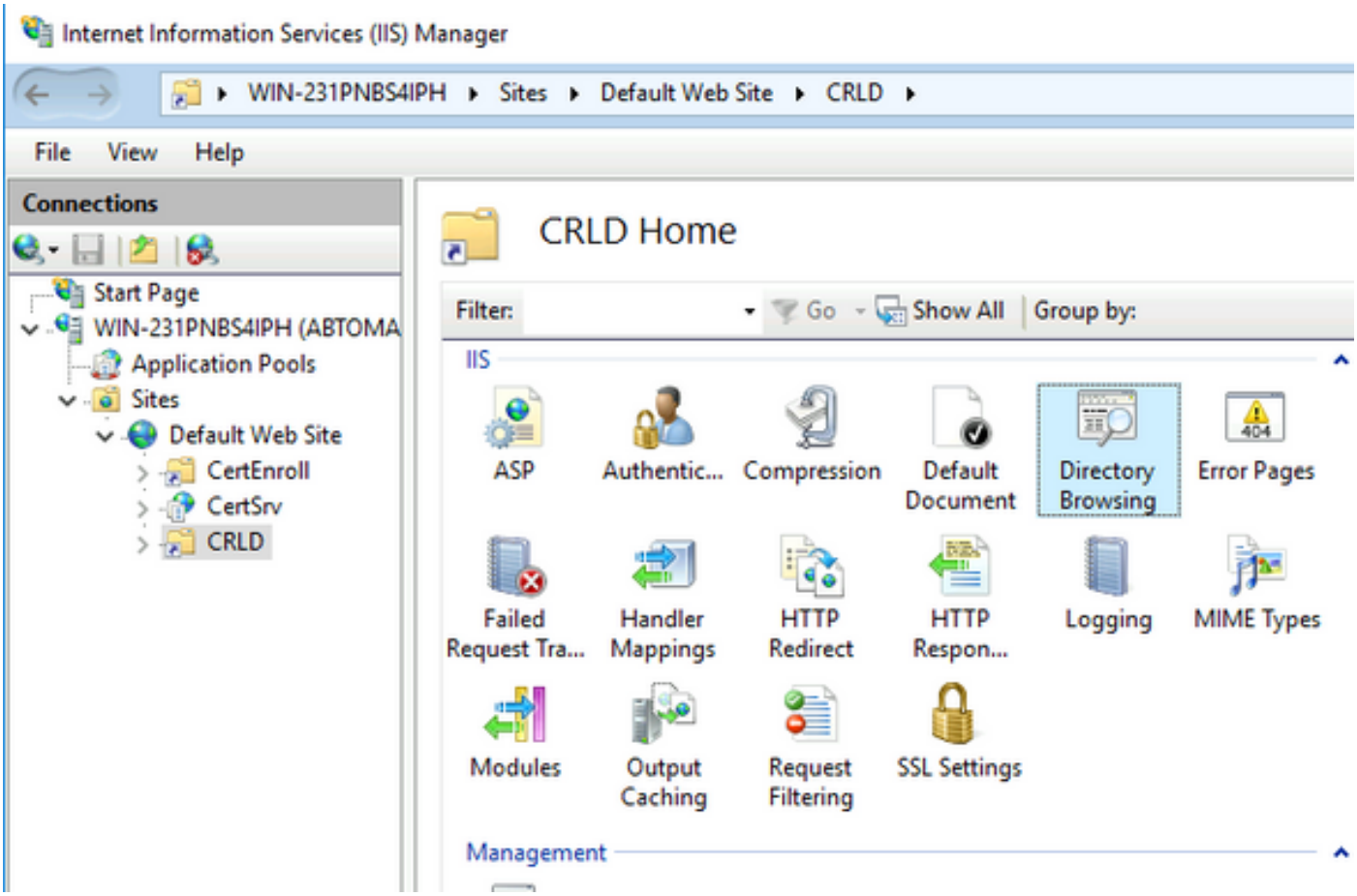
4. Alias(별칭) 필드에 CRL 배포 지점의 사이트 이름을 입력합니다.이 예에서는 CRLD를 입력합니다.



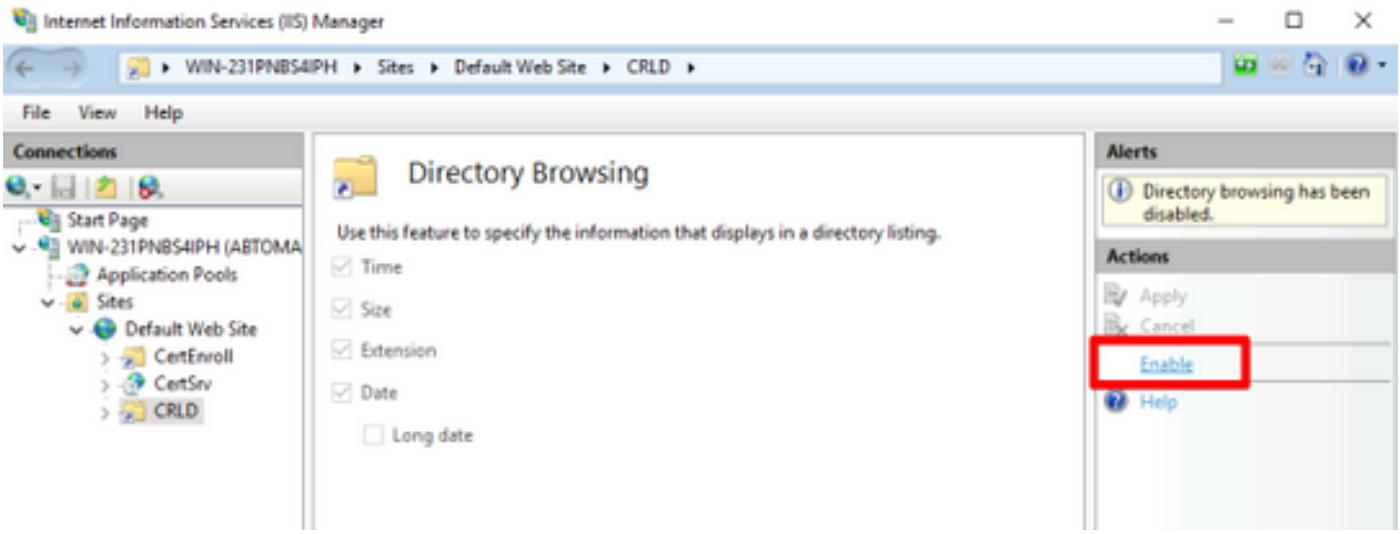
5. 줄임표(.)를 클릭합니다...) [물리적 경로] 필드 오른쪽에 있는 섹션 1에서 만든 폴더를 찾습니다. 폴더를 선택하고 **확인**을 클릭합니다.OK(**확인**)를 클릭하여 Add Virtual Directory(가상 디렉토리 추가) 창을 닫습니다.



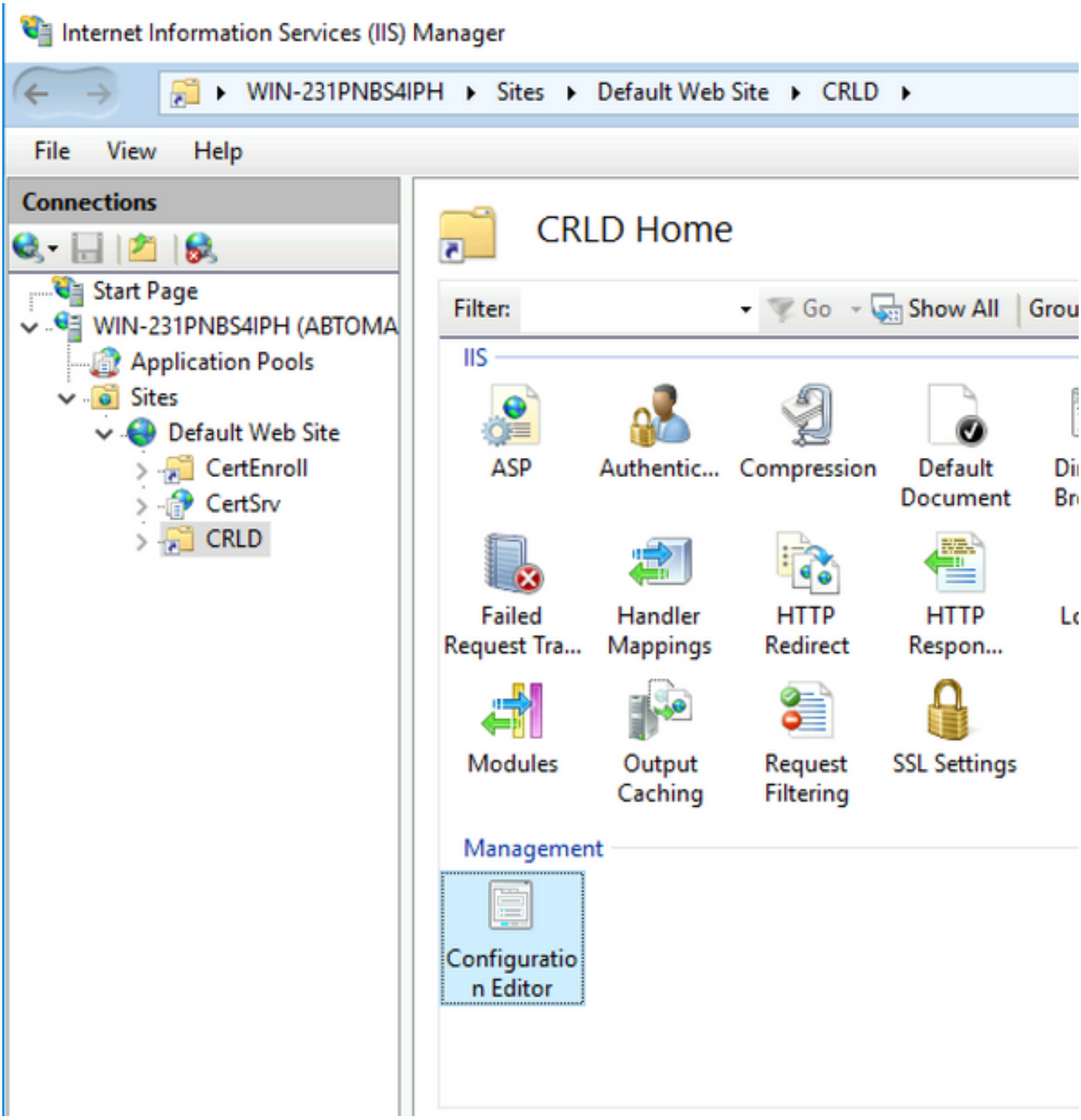
6. 4단계에서 입력한 사이트 이름이 왼쪽 창에서 강조 표시되어야 합니다.그렇지 않으면 지금 선택하십시오.가운데 창에서 **디렉터리 찾아보기**를 두 번 클릭합니다.



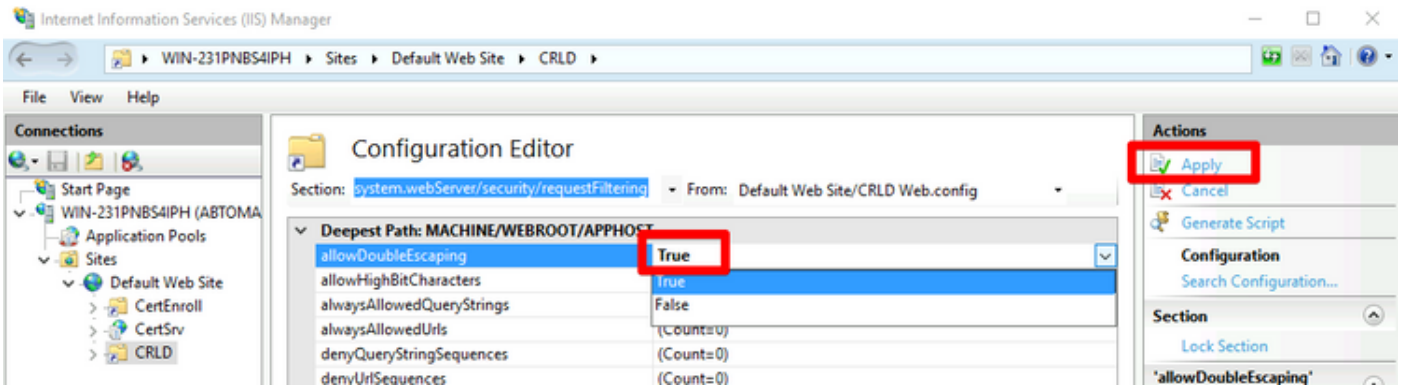
7. 오른쪽 창에서 **사용**을 클릭하여 디렉토리 검색을 활성화합니다.



8. 왼쪽 창에서 사이트 이름을 다시 선택합니다.중앙 창에서 구성 **편집기**를 두 번 클릭합니다.



9. 섹션 드롭다운 목록에서 system.webServer/security/requestFiltering을 선택합니다 .allowDoubleEscape 드롭다운 목록에서 True를 **선택합니다**.오른쪽 창에서 이 이미지에 표시된 대로 **적용**을 클릭합니다.

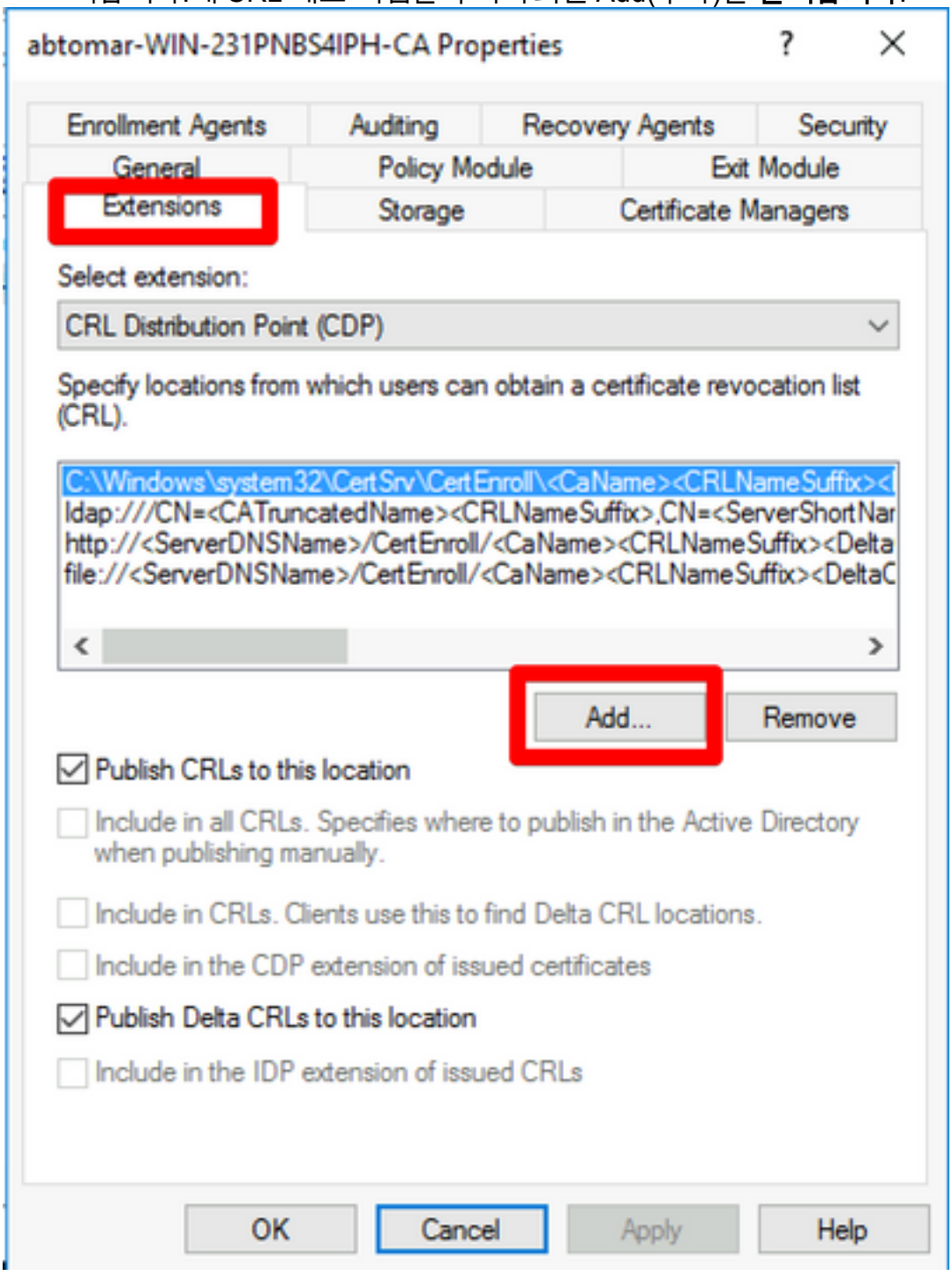


이제 IIS를 통해 폴더에 액세스할 수 있어야 합니다.

배포 지점에 CRL 파일을 게시하도록 Microsoft CA 서버 구성

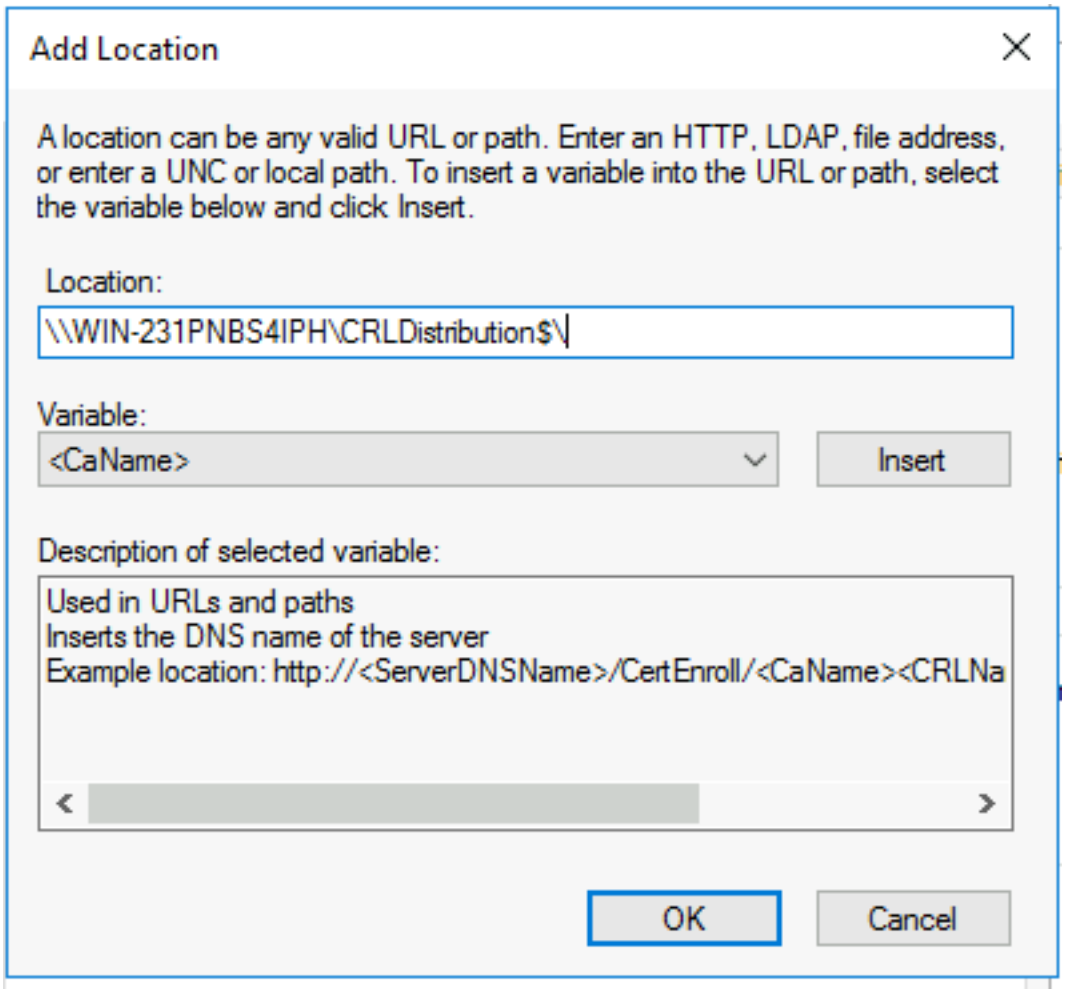
CRL 파일을 포함하도록 새 폴더가 구성되고 폴더가 IIS에 노출되었으므로 Microsoft CA 서버가 CRL 파일을 새 위치에 게시하도록 구성합니다.

1. CA 서버 작업 표시줄에서 **시작**을 클릭합니다.Administrative **Tools > Certificate Authority를 선택합니다**.
2. 왼쪽 창에서 CA 이름을 마우스 오른쪽 버튼으로 클릭합니다.속성**을** 선택한 다음 확장 탭을 클릭합니다.새 CRL 배포 지점을 추가하려면 Add(추가)를 **클릭합니다**.

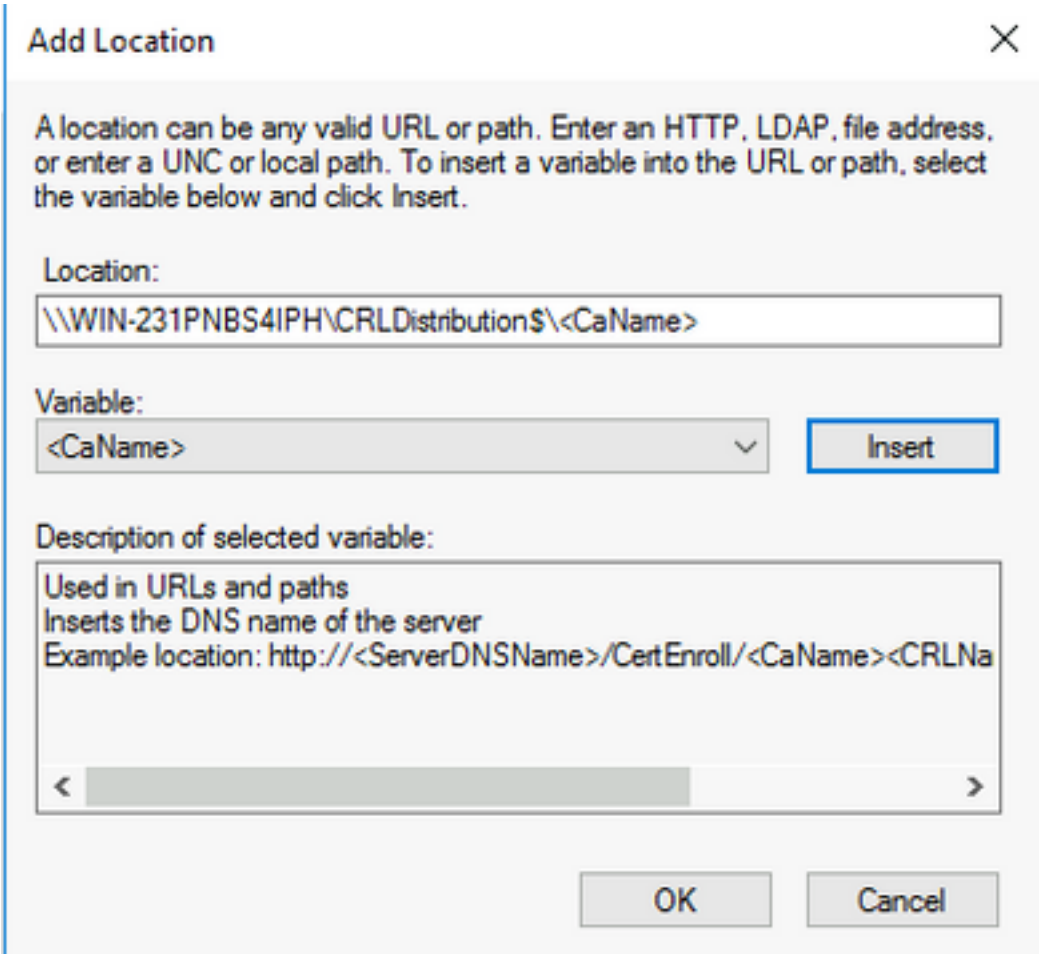


3. 위치 필드에 섹션 1에서 생성 및 공유된 폴더의 경로를 입력합니다. 섹션 1의 예에서 경로는 다음과 같습니다.

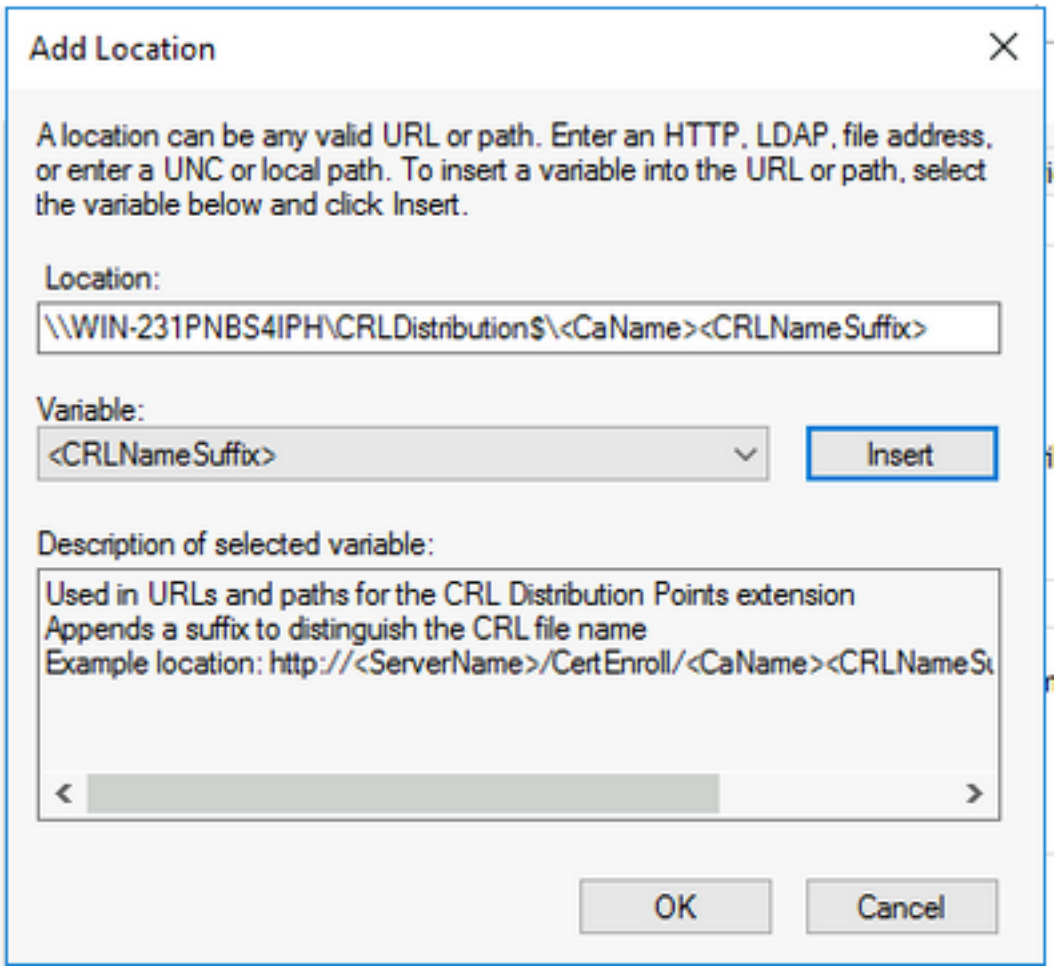
\\WIN-231PNBS4IPH\CRLDistribution$



4. 위치 필드가 채워진 상태에서 변수 드롭다운 목록에서 **<CaName>**을 선택하고 **삽입**을 클릭합니다.

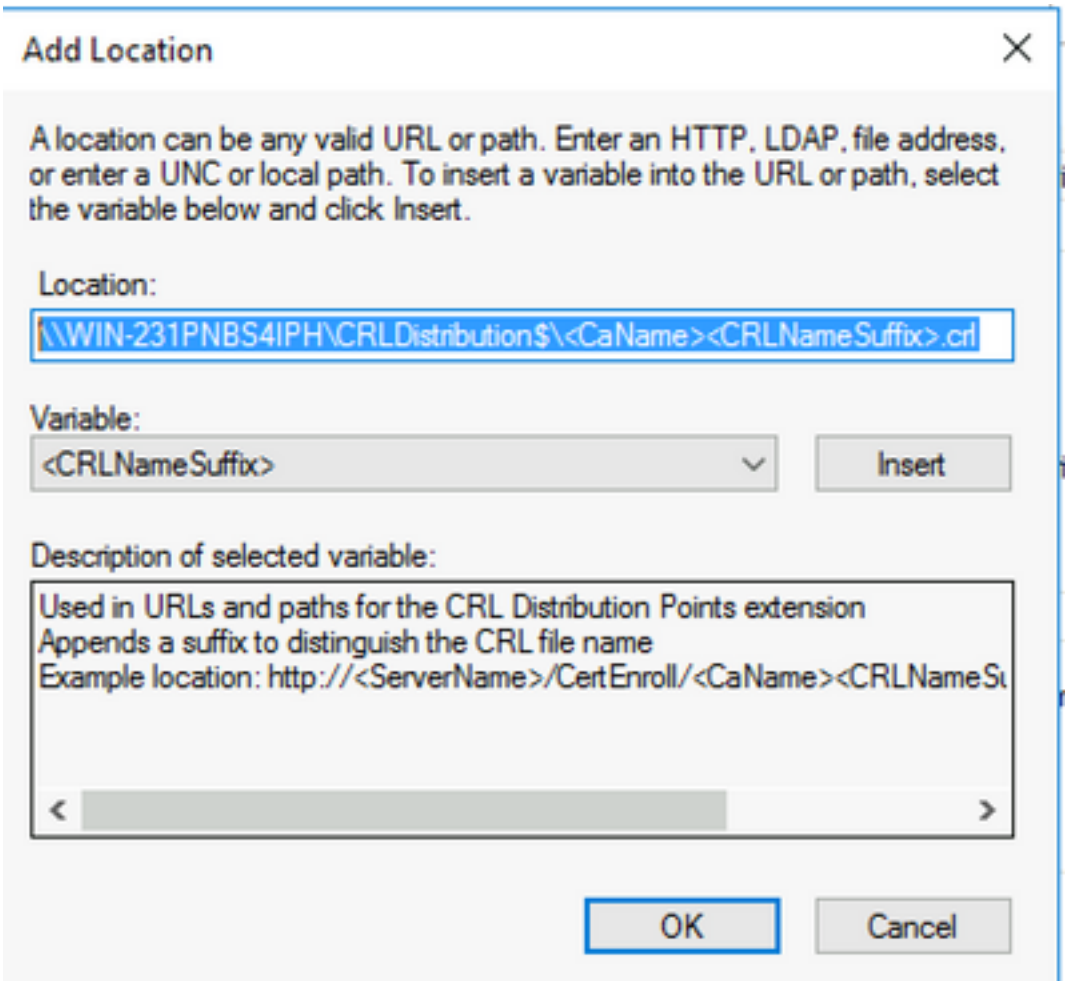


5. 변수 드롭다운 목록에서 **<CRLNameSuffix>를** 선택한 다음 **삽입**을 클릭합니다.



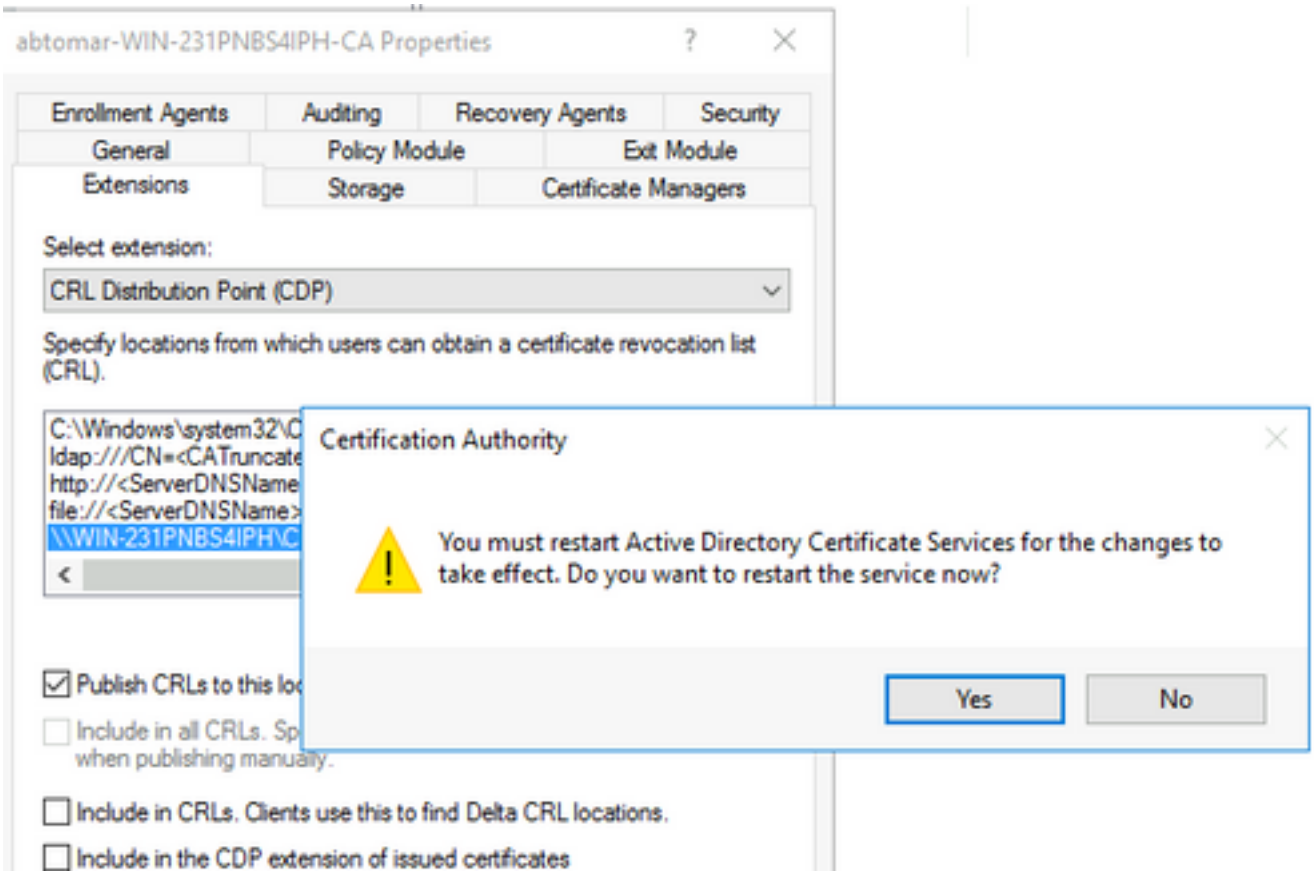
6. Location(위치) 필드에서 **.crl을** 경로의 끝에 추가합니다.이 예에서 위치는 다음과 같습니다.

\\WIN-231PNBS4IPH\CRLDistribution$\<CaName><CRLNameSuffix>.crl

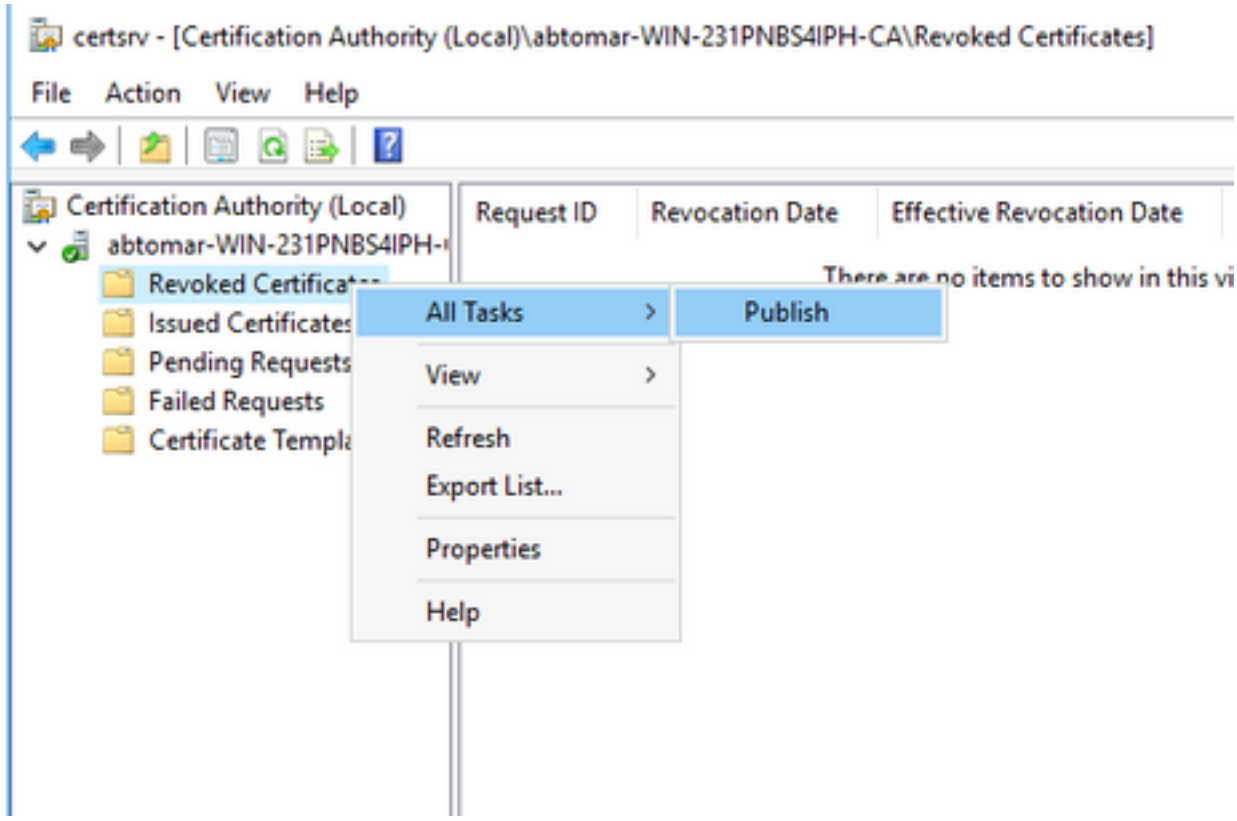


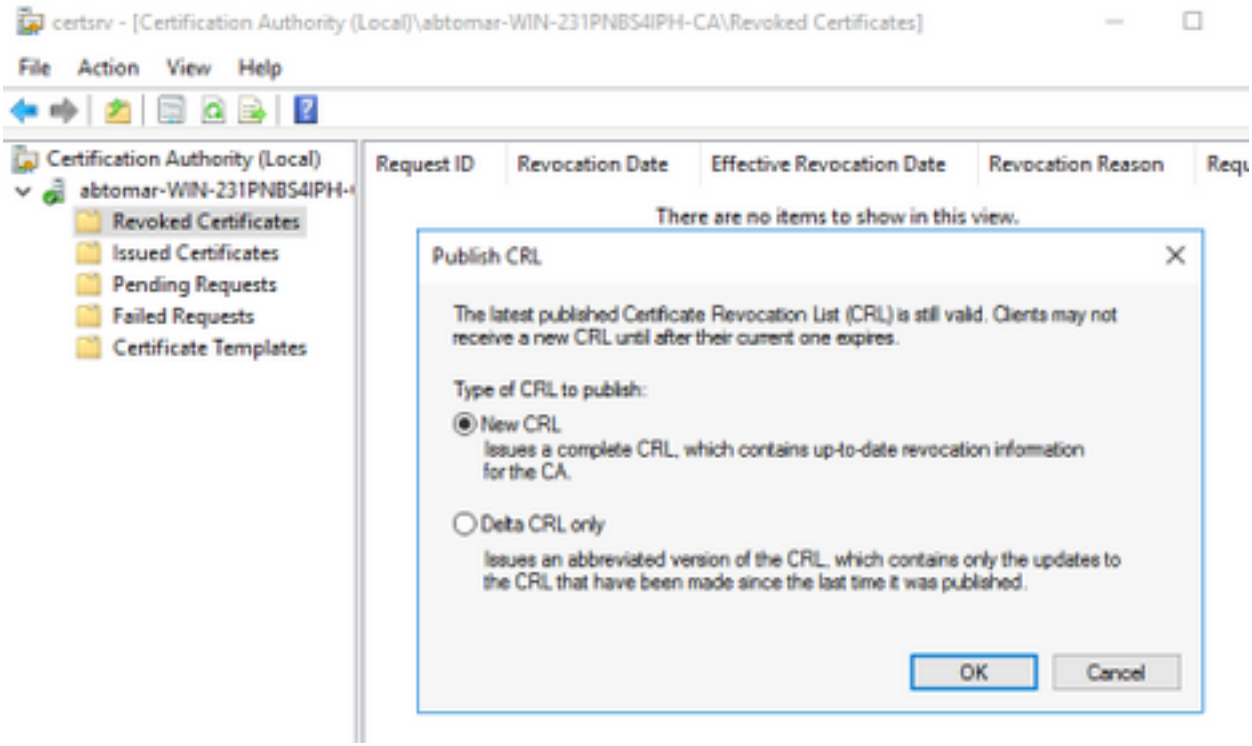
7 . OK(**확인**)를 클릭하여 Extensions(확장) 탭으로 돌아갑니다.Publish CRLs **to this location(이 위치에 CRL 게시**) 확인란을 선택한 다음 **OK(확인)를** 클릭하여 Properties(속성) 창을 닫습니다.

Active Directory 인증서 서비스를 다시 시작할 수 있는 권한에 대한 프롬프트가 나타납니다.**예**를 클릭합니다.



8. 왼쪽 창에서 해지된 **인증서**를 마우스 오른쪽 버튼으로 클릭합니다.모든 **작업 > 게시를 선택합니다**.New CRL이 선택되었는지 확인한 다음 **OK**를 클릭합니다.





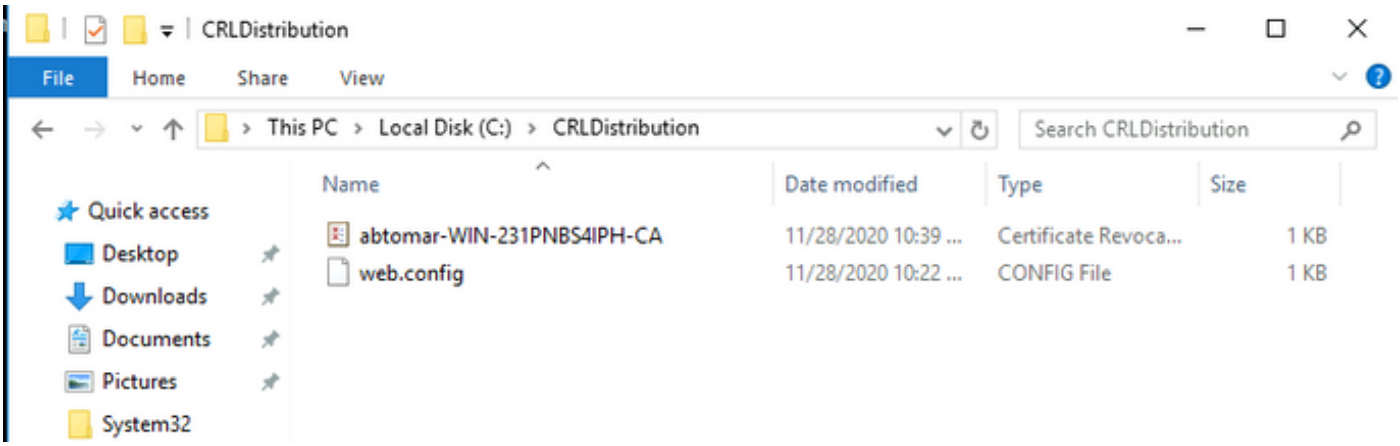
Microsoft CA 서버는 섹션 1에서 생성한 폴더에 새 .crl 파일을 생성해야 합니다. 새 CRL 파일이 성공적으로 생성되면 확인을 클릭한 후 대화 상자가 없습니다.새 배포 지점 폴더에 오류가 반환되면 이 섹션의 각 단계를 주의해서 반복합니다.

CRL 파일이 있으며 IIS를 통해 액세스할 수 있는지 확인합니다.

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

1. IIS 서버에서 섹션 1에서 만든 폴더를 엽니다. **<CANAME>.crl** 형식의 단일 .crl 파일이 있어야 합니다. 여기서 <CANAME>은 CA 서버의 이름입니다.이 예에서 파일 이름은 다음과 같습니다 .

abtomar-WIN-231PNBS4IPH-CA.crl



2. 네트워크의 워크스테이션에서(ISE 기본 관리 노드와 동일한 네트워크에 이상적으로) 웹 브라우저를 열고 http://<SERVER>/<CRLSITE>로 이동합니다. 여기서 <SERVER>는 섹션 2에 구성된 IIS 서버의 서버 이름이고 <CRLSITE>는 섹션 2에 있는 배포 지점에 대해 선택된 사이트 이름입니다. 이 예에서 URL은 다음과 같습니다.

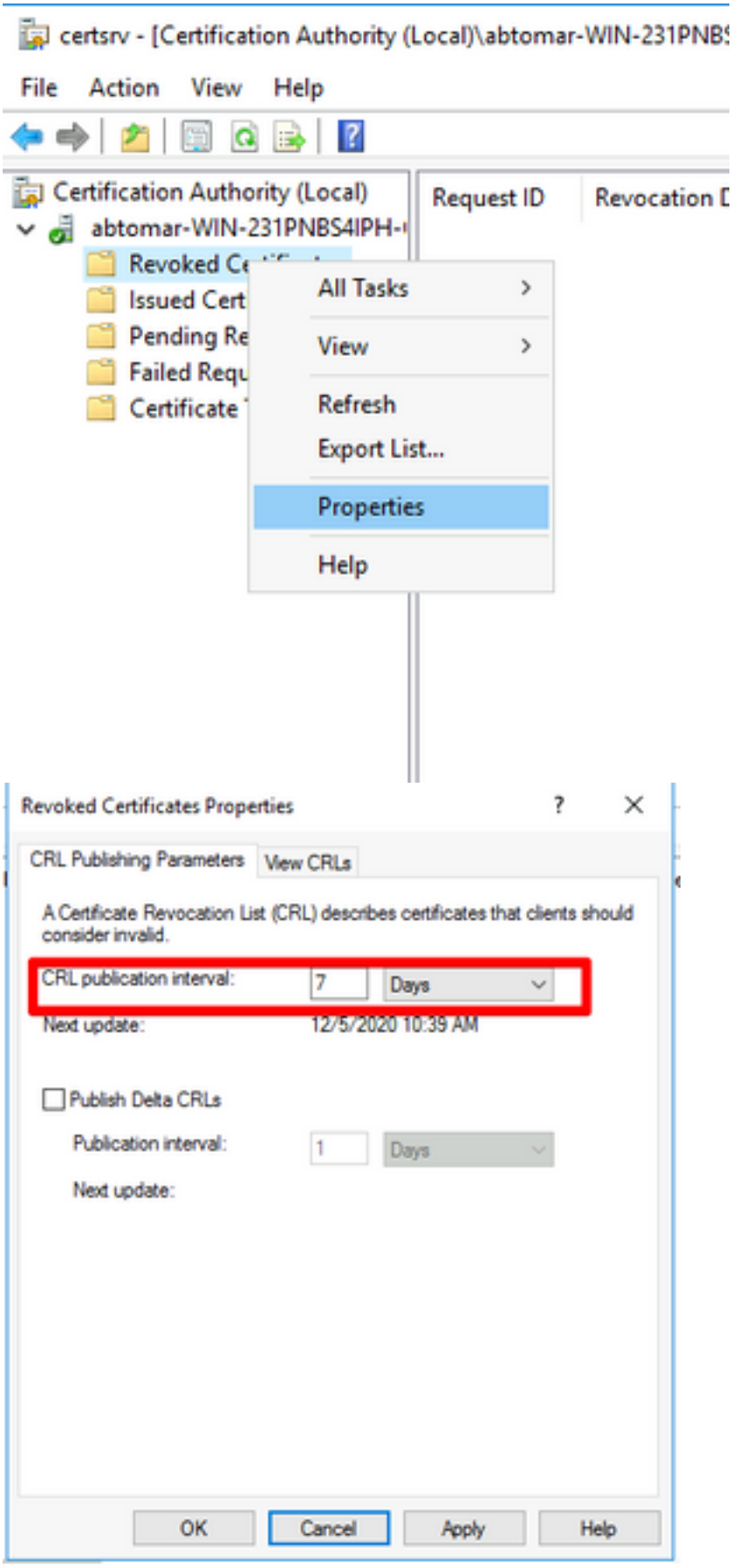
http://win-231pnbs4iph/CRLD

1단계에서 관찰된 파일을 포함하는 디렉토리 인덱스가 표시됩니다.

새 CRL 배포 지점을 사용하도록 ISE 구성

CRL을 검색하도록 ISE를 구성하기 전에 CRL을 게시할 간격을 정의합니다.이 간격을 결정하는 전략은 이 문서의 범위를 벗어납니다.잠재적 값(Microsoft CA에서)은 1시간~411년(포함)입니다.기본값은 1주입니다.환경에 적합한 간격이 결정되면 다음 지침에 따라 간격을 설정합니다.

1. CA 서버 작업 표시줄에서 **시작**을 클릭합니다.Administrative **Tools > Certificate Authority를 선택합니다**.
2. 왼쪽 창에서 CA를 확장합니다.Revoked **Certificates** 폴더를 마우스 오른쪽 버튼으로 클릭하고 Properties(속성)를 **선택합니다.**
3. CRL 게시 간격 필드에 필수 번호를 입력하고 기간을 선택합니다.확인**을** 클릭하여 창을 닫고 변경 사항을 적용합니다.이 예에서는 7일의 게시 간격이 구성됩니다.



4. certutil -**getreg CA\Clock*** 명령을 입력하여 ClockSkew 값을 확인합니다.기본값은 10분입니다.

출력 예:

```
Values:
```

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

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

출력 예:

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

6 . certutil **-getreg CA\CRLpe*** 명령을 입력하여 3단계에서 설정된 CRLPperiod를 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.5단계에서 CRLOverlapPeriod가 설정된 경우OVERLAP = CRLOverlapPeriod(분)

기타:OVERLAP = (CRLPperiod / 10)(분)

b.겹치기 720보다 크면 겹치기 = 720

c. 겹치는 경우 < (1.5 * ClockSkewMinutes) OVERLAP = (1.5 * ClockSkewMinutes)

d.겹치기 > CRLPperiod인 경우 분 단위로 겹치기 = CRLPperiod(분)

e.유예 기간 = OVERLAP + ClockSkewMinutes

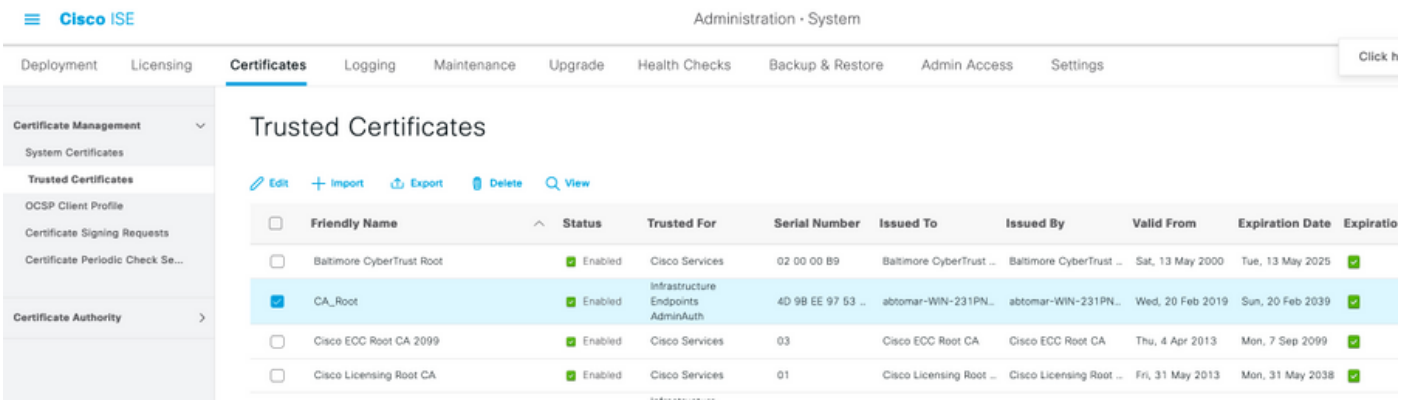
```
Example:

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 게시한 시간과 현재 CRL이 만료되는 시간 사이의 시간입니다.그에 따라 CRL을 검색하도록 ISE를 구성해야 합니다.

8. ISE 기본 관리 노드에 로그인하고 관리 **> 시스템 > 인증서를** 선택합니다.왼쪽 창에서 **신뢰할 수 있는 인증서**



9. CRL을 구성하려는 CA 인증서 옆의 확인란을 선택합니다.Edit를 **클릭합니다**.

10. 창 하단에서 Download CRL(**CRL 다운로드**) 확인란을 선택합니다.

11. CRL Distribution URL 필드에 섹션 2에서 생성된 .crl 파일을 포함하는 CRL 배포 지점의 경로를 입력합니다. 이 예에서 URL은 다음과 같습니다.

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

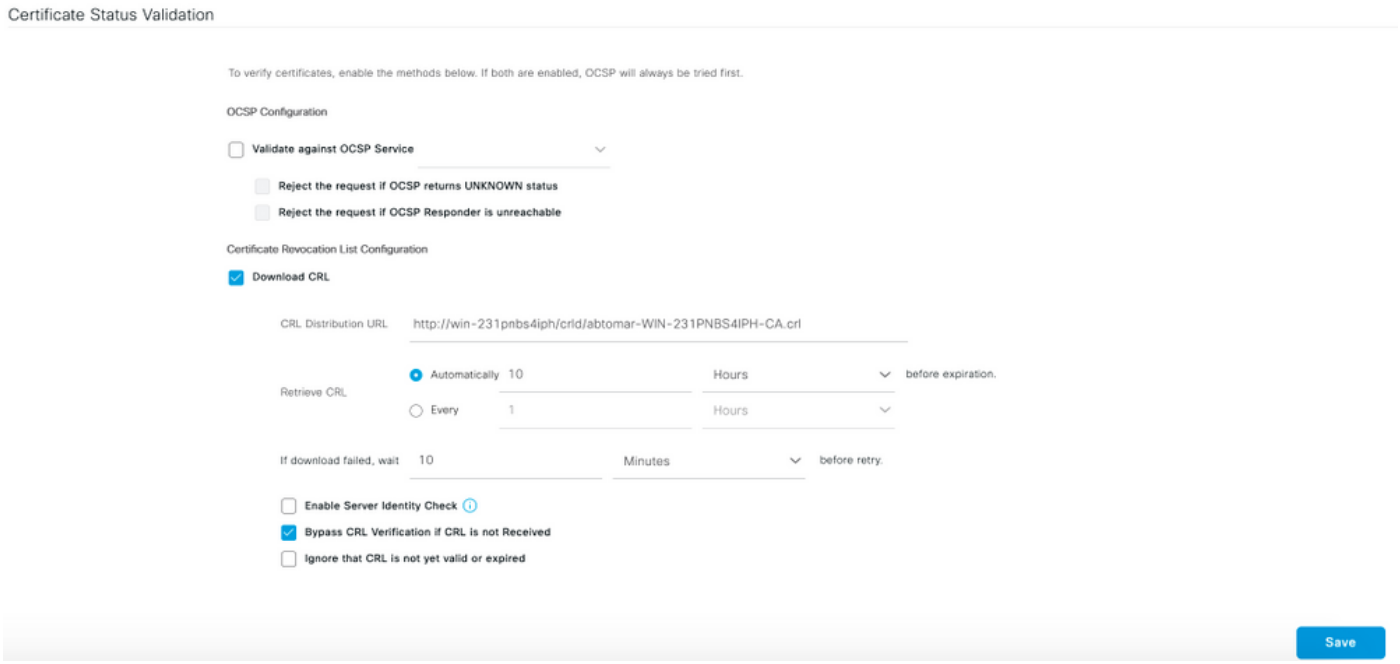
12. ISE는 정기적으로 또는 만료를 기준으로 CRL을 검색하도록 구성할 수 있습니다(일반적으로 정규 간격이기도 함). CRL 게시 간격이 정적인 경우, CRL 업데이트가 필요할 때 CRL의 후자 옵션이 사용됩니다.Automatically(자동) 라디오 버튼을 클릭합니다.

13. 검색할 값을 7단계에서 계산된 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, 즉 12시간 10분으로 계산됩니다.10시간의 값이 검색에 사용됩니다.

14. 환경에 적합한 재시도 간격을 설정합니다.ISE가 이전 단계에서 구성된 간격으로 CRL을 검색할 수 없는 경우 이 짧은 간격으로 다시 시도합니다.

15. ISE가 마지막 다운로드 시도**에서** 이 CA에 대한 CRL을 검색할 수 없는 경우 인증서 기반 인증이 정상적으로 진행되도록(CRL 검사 없이) 하려면 Bypass CRL Verification if CRL is not Received(CRL이 수신되지 **않은 경우 CRL 확인** 우회) 확인란을 선택합니다.이 확인란을 선택하지 않으면 CRL을 검색할 수 없는 경우 이 CA에서 발급한 인증서를 사용하는 모든 인증서 기반 인증이 실패합니다.

16. Ignore that CRL is **not yet valid or expired(CRL is not yet valid or expired) 확인란을 선택하여 ISE가** 만료된(또는 아직 유효하지 않음) CRL 파일을 유효한 것처럼 사용하도록 허용합니다.이 확인란을 선택하지 않으면 ISE는 유효 날짜 이전 및 다음 업데이트 시간 이후에 CRL이 유효하지 않은 것으로 간주합니다.Save(**저장**)를 클릭하여 컨피그레이션을 완료합니다.



Cisco 내부 정보

1. Microsoft"인증서에 대한 CRL 배포 지점을 구성합니다." http://technet.microsoft.com/en-us/library/ee649260%28v=ws.10%29.aspx, 2009년 10월 7일 [2012년 12월 18일]

2. 마이크로소프트"인증서 해지 목록을 수동으로 게시합니다." http://technet.microsoft.com/en-us/library/cc778151%28v=ws.10%29.aspx, 2005년 1월 21일 [2012년 12월 18일]

3. 마이크로소프트"CRL 및 델타 CRL 중복 기간을 구성합니다." http://technet.microsoft.com/en-us/library/cc731104.aspx, 2011년 4월 11일 [2012년 12월 18일]

4. MS2065 [MSFT]. "How EffectiveDate (this update), NextUpdate 및 NextCRLPublish가 계산됩니다." http://blogs.technet.com/b/pki/archive/2008/06/05/how-effectivedate-thisupdate-nextupdate-and-nextcrlpublish-are-calculated.aspx, 2008년 6월 4일 [2012년 12월 18일]