Microsoft CA Server configureren om de lijsten met certificaatintrekking voor ISE te publiceren

Inhoud

Inleiding

Dit document beschrijft de configuratie van een Microsoft Certificate Authority (CA)-server die Internet Information Services (IIS) uitvoert om de CRL-updates (Certificate Revocation List) te publiceren. Het legt ook uit hoe u de Cisco Identity Services Engine (ISE) (versies 3.0 en hoger) moet configureren om de updates op te halen voor gebruik in certificaatvalidatie. ISE kan worden geconfigureerd om CRL's op te halen voor de verschillende CA-basiscertificaten die worden gebruikt bij de validatie van certificaten.

Voorwaarde

Vereisten

Er zijn geen specifieke vereisten van toepassing op dit document.

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

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

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een

opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

Configureren

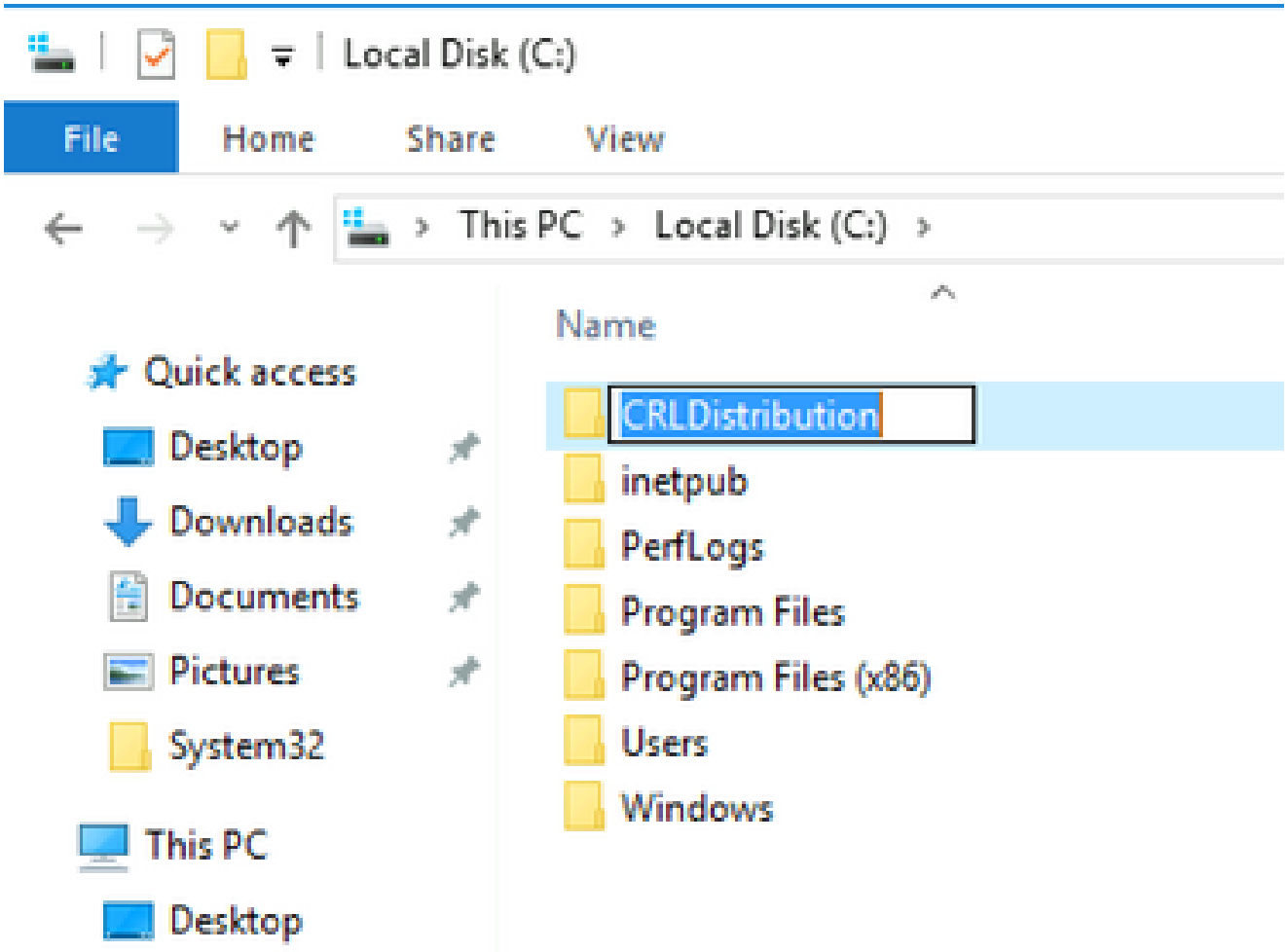
Deze sectie bevat informatie over het configureren van de functies die in dit document worden beschreven.

Een map op de CA maken en configureren om de CRL-bestanden te huisvesten

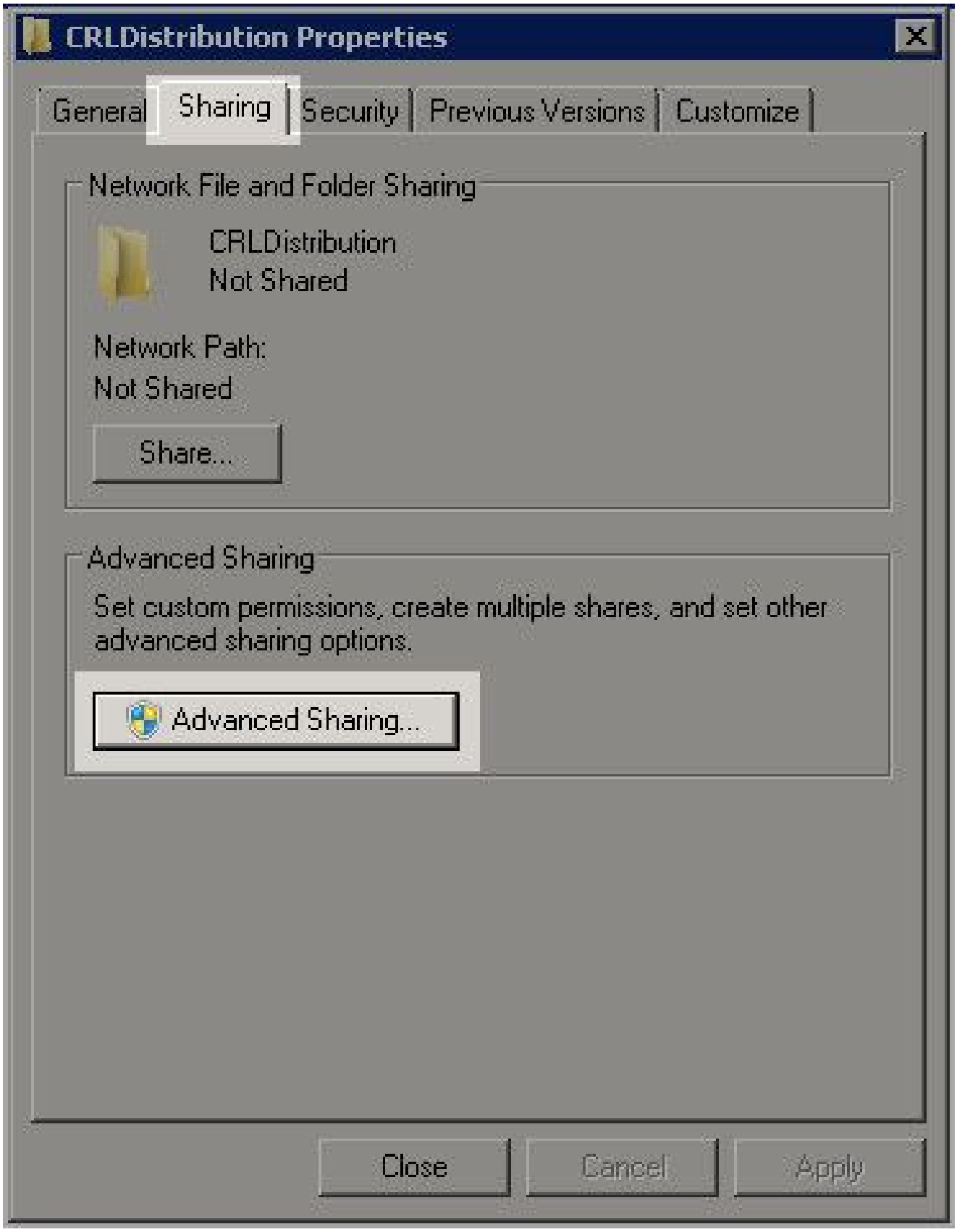
De eerste taak is om een locatie op de CA-server te configureren voor het opslaan van de CRL-bestanden. Standaard worden de bestanden op de Microsoft CA-server gepubliceerd op **C:\Windows\system32\CertSrv\CertEnroll**

Maak een nieuwe map voor de bestanden in plaats van deze systeemmap te gebruiken.

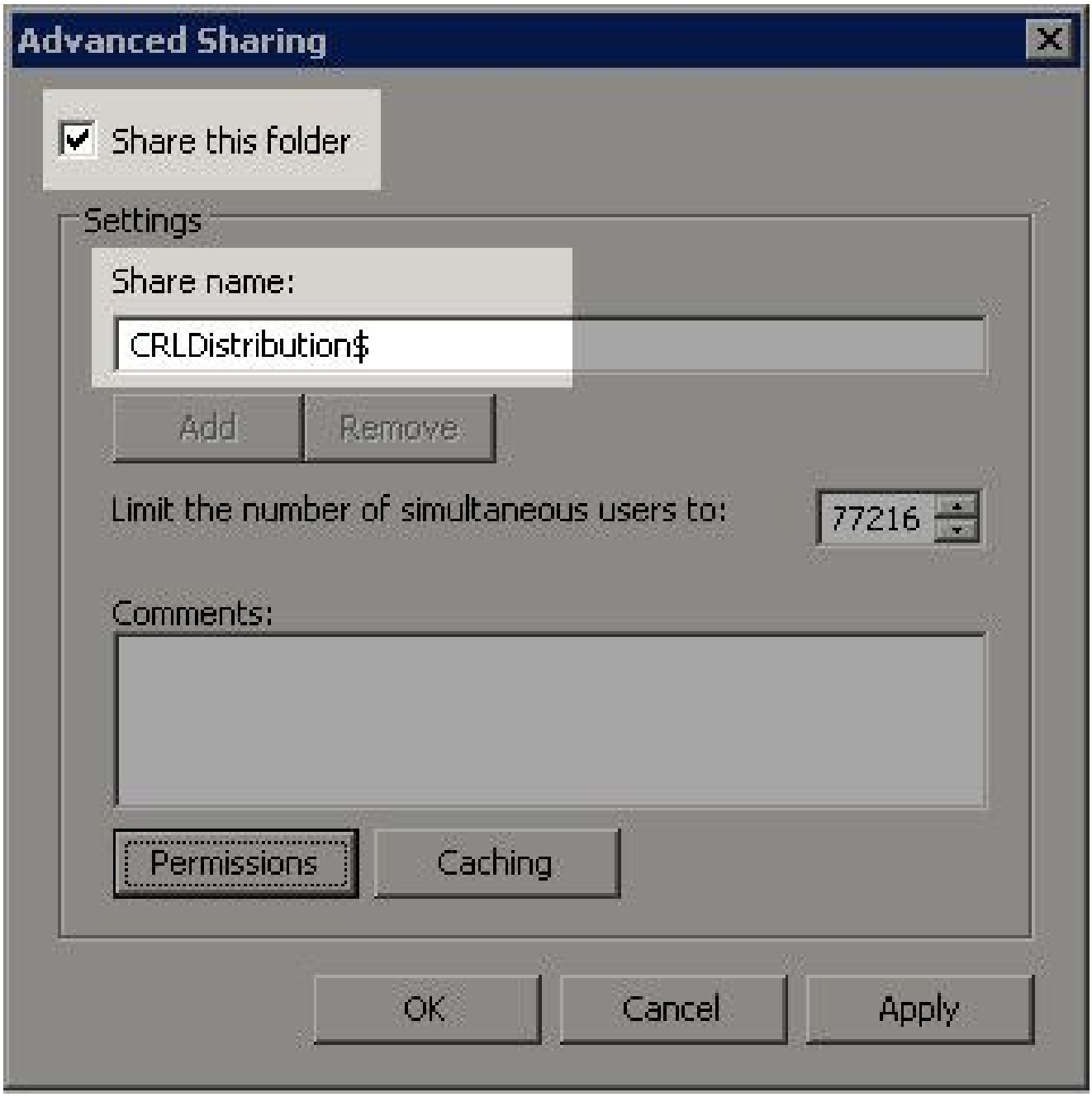
1. Kies op de IIS-server een locatie op het bestandssysteem en maak een nieuwe map. In dit voorbeeld wordt de map **C:\CRLDistribution** gemaakt.



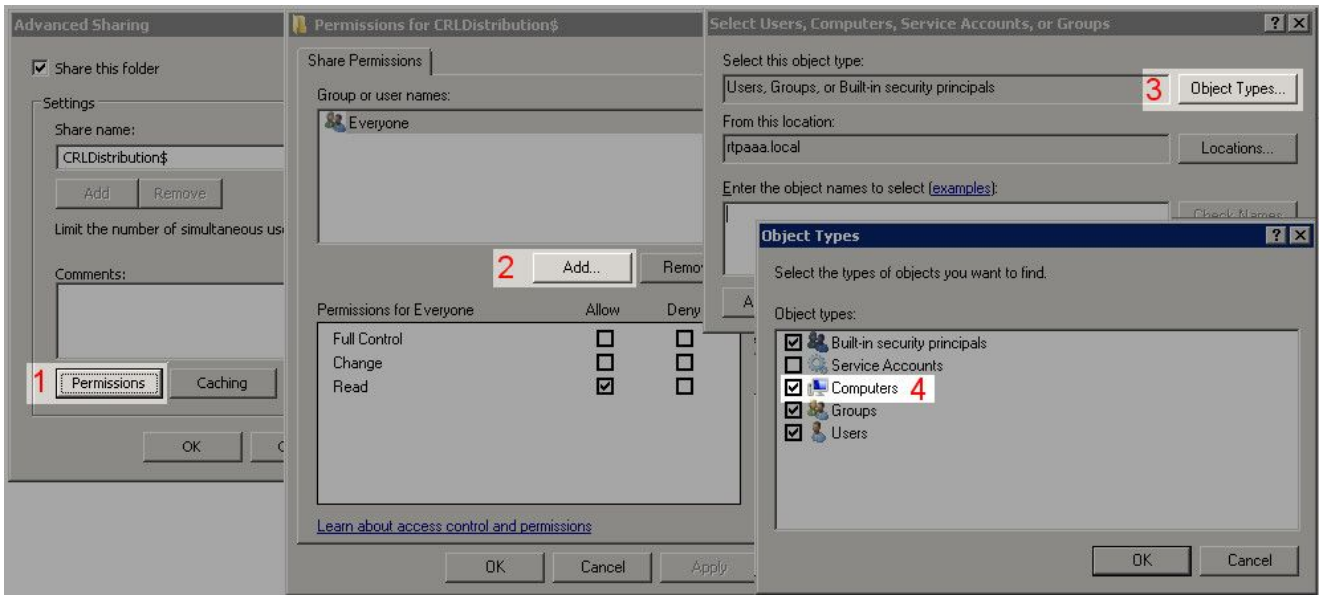
2. Als de CA de CRL-bestanden naar de nieuwe map wil schrijven, moet delen zijn ingeschakeld. Klik met de rechtermuisknop op de nieuwe map, kies **Properties**, klik op het **Sharing** tabblad en klik vervolgens **Advanced Sharing**.



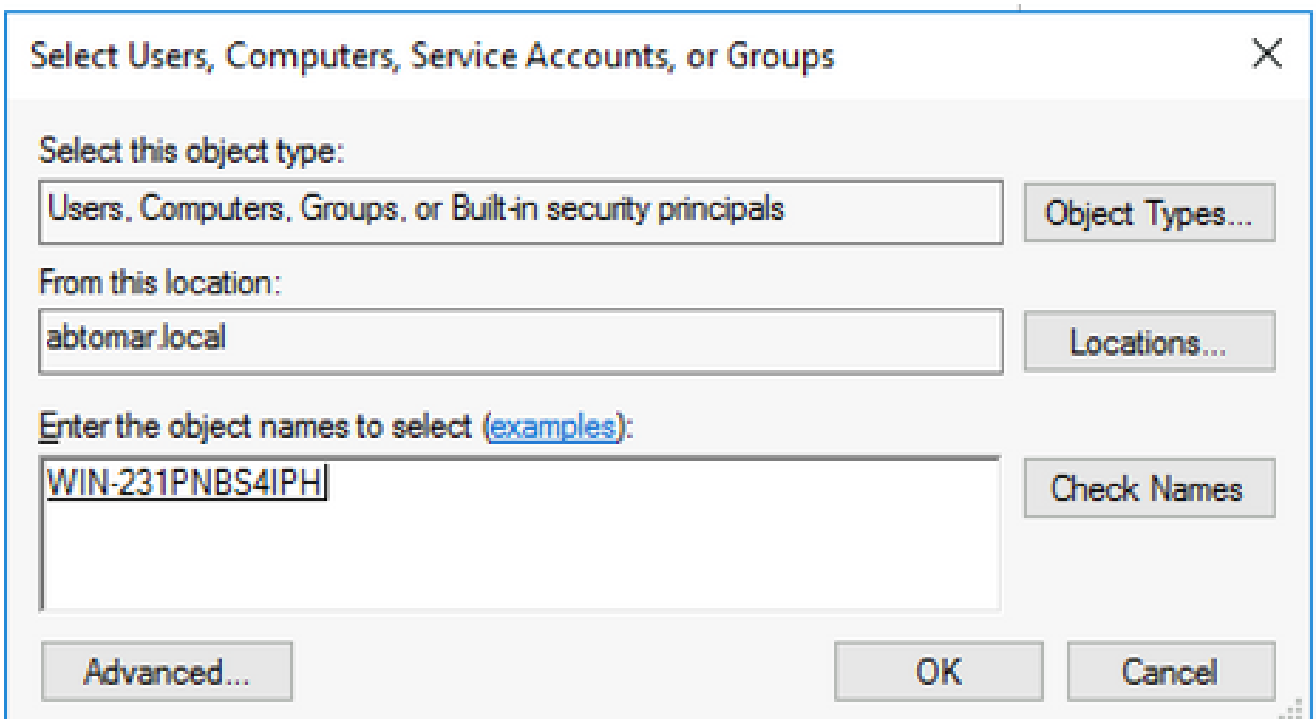
3. Als u de map wilt delen, schakelt u het **Share this folder** aankruisvakje in en voegt u vervolgens een dollarteken ($) toe aan het einde van de naam van het aandeel in het veld Naam van het aandeel om het aandeel te verbergen.



4. Klik **Permissions** (1), klik **Add** (2), klik op **Object Types** (3) en controleer het **Computers** aankruisvakje (4).

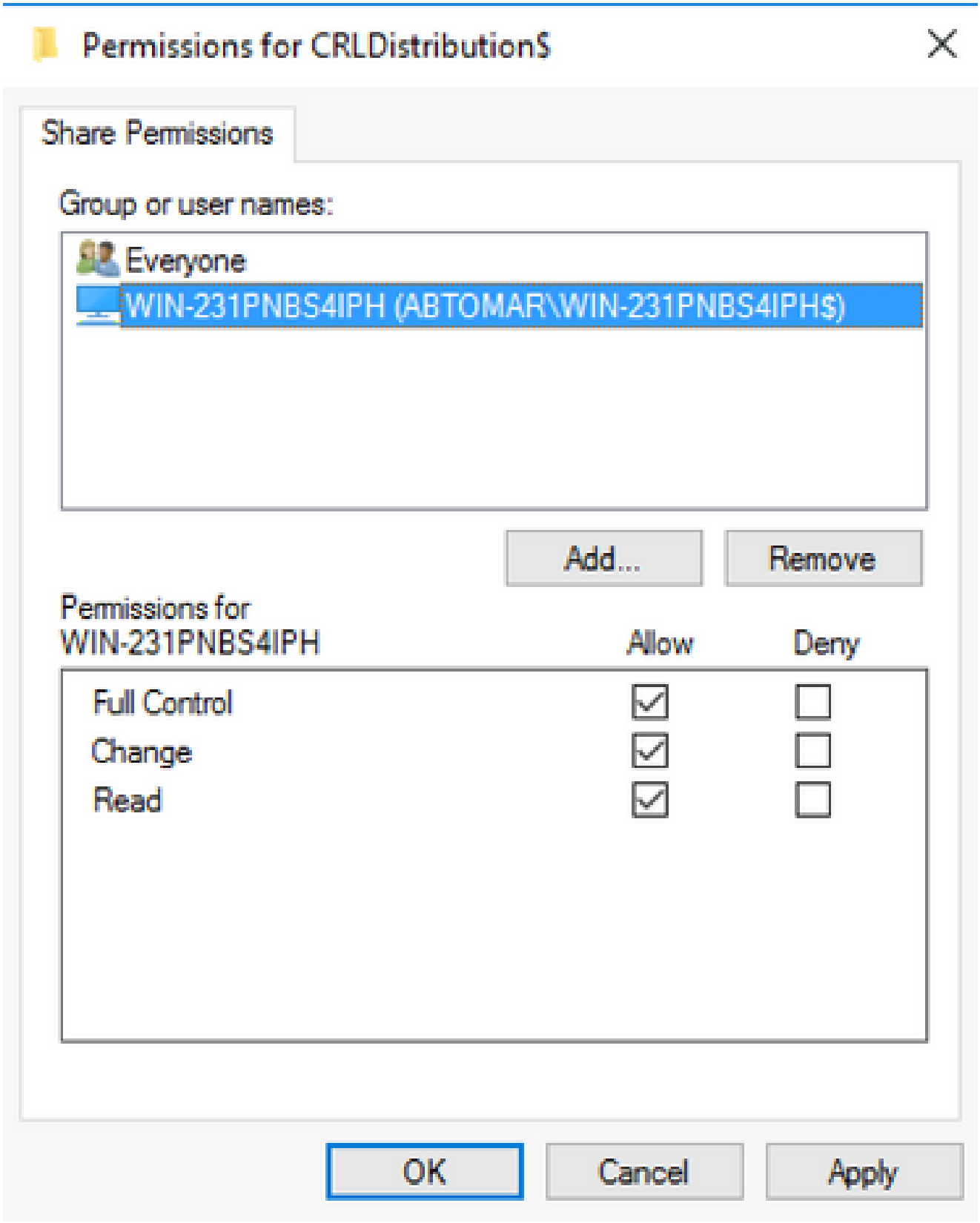


5. Klik op **OK**om terug te keren naar het venster Gebruikers, computers, serviceaccounts of groepen selecteren. Voer in het veld Voer de objectnamen in om de computernaam van de CA-server in dit voorbeeld in: WIN0231PNBS4IPH en klik **Check Names**. Als de ingevoerde naam geldig is, wordt de naam vernieuwd en onderstreept weergegeven. Klik op de knop **.OK**

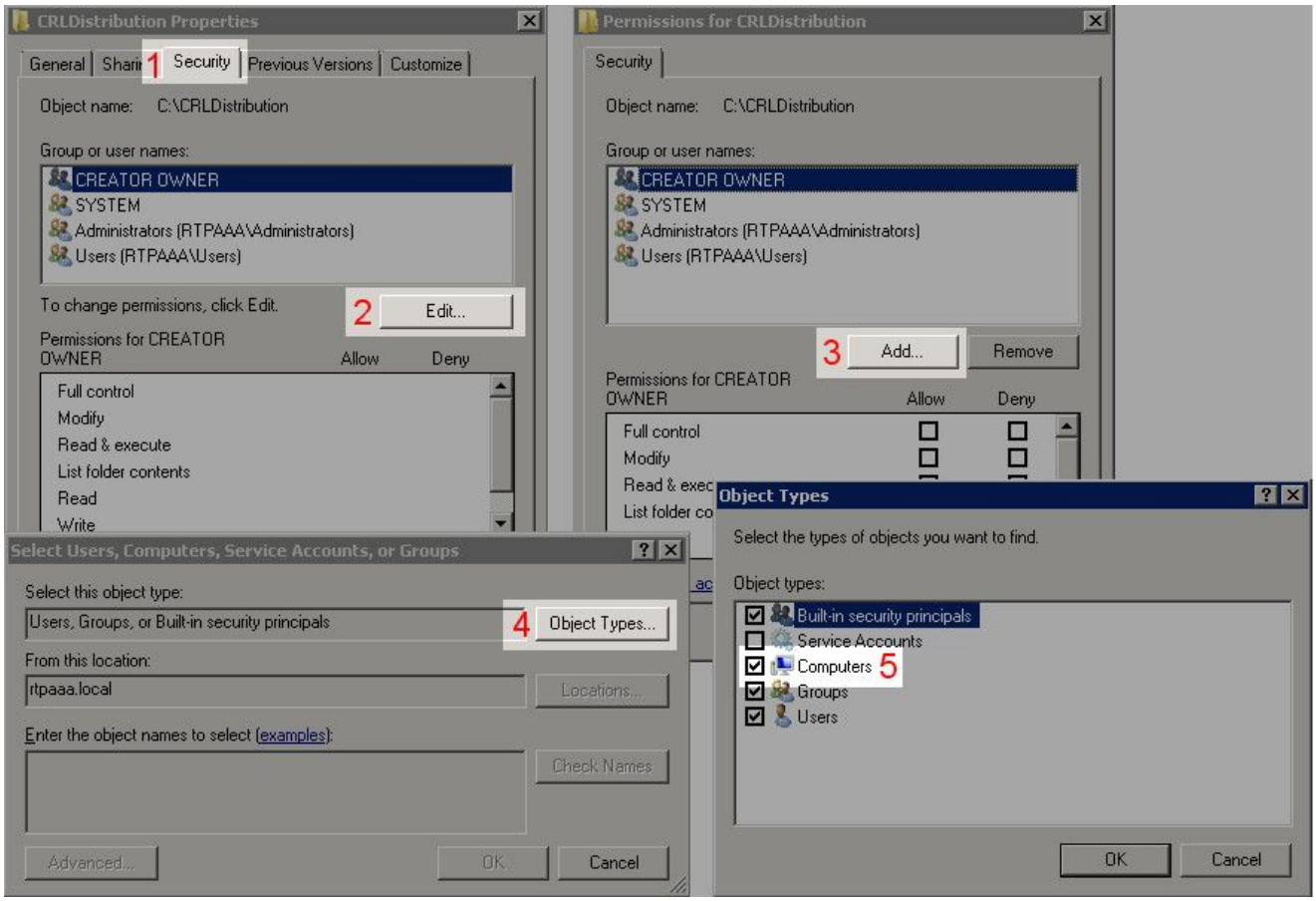


6. Kies in het veld Groep- of gebruikersnamen de CA-computer. Controleer **Allow** op volledige controle om volledige toegang tot de CA te verlenen.

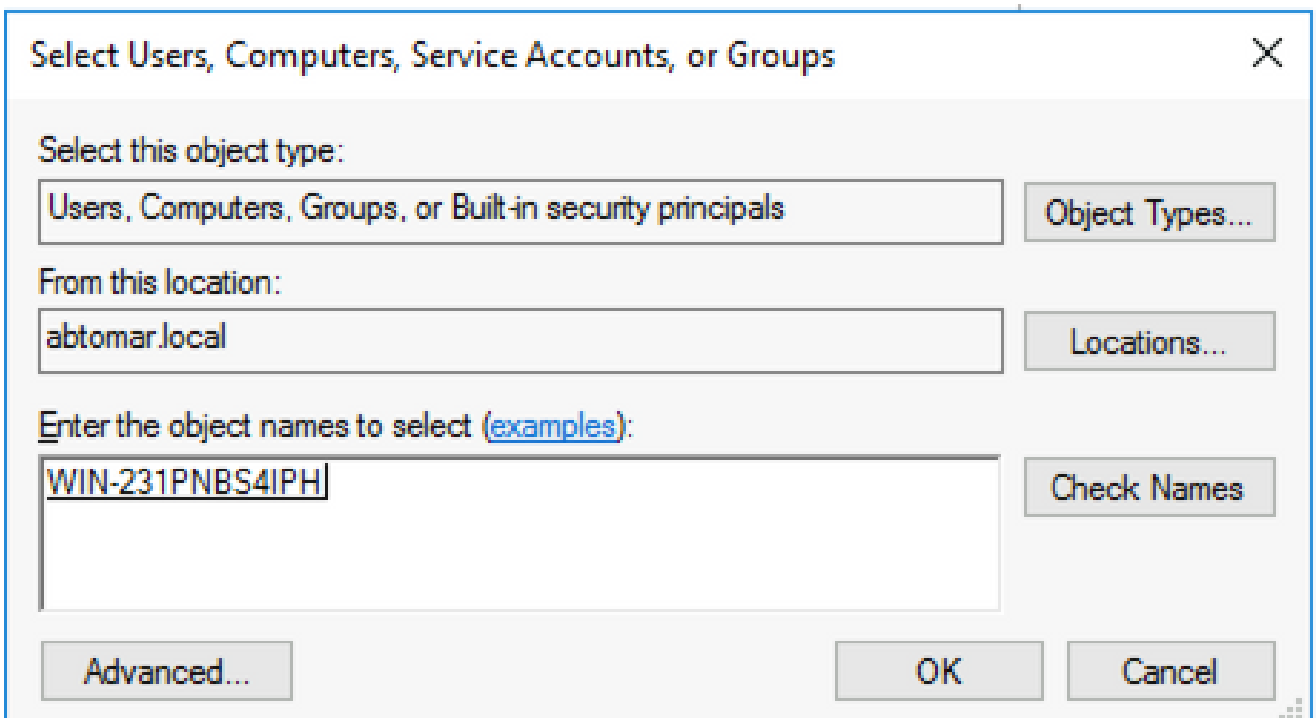
Klik op de knop **.OK OK** Klik nogmaals op deze knop om het venster Geavanceerd delen te sluiten en terug te keren naar het venster Eigenschappen.



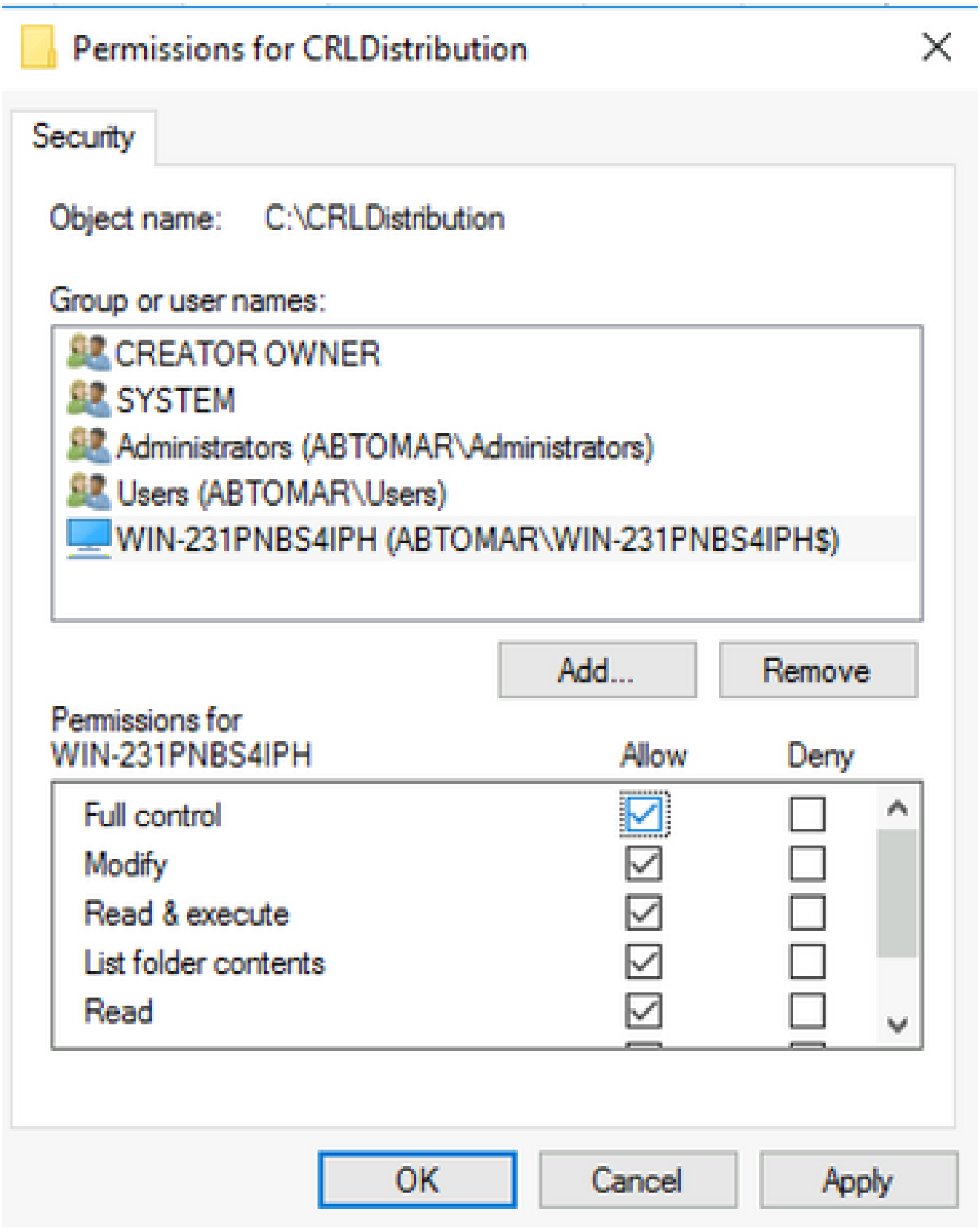
7. Om CA in staat te stellen de CRL-bestanden naar de nieuwe map te schrijven, moet u de juiste beveiligingstoestemmingen configureren. Klik op het**Security** tabblad (1), klik **Edit** (2), klik **Add** (3), klik **Object Types** (4) en controleer het **Computers** aankruisvakje (5).



8. Typ in het veld Voer de namen van de objecten in die u wilt selecteren de computernaam van de CA-server en klik op **Check Names**. Als de ingevoerde naam geldig is, wordt de naam vernieuwd en onderstreept weergegeven. Klik op de knop .**OK**



9. Kies de CA-computer in het veld Groep- of gebruikersnamen en controleer vervolgens **Allow** op Volledig beheer om volledige toegang tot de CA te verlenen. Klik op **OK** en klik om de taak te **Close** voltooien.

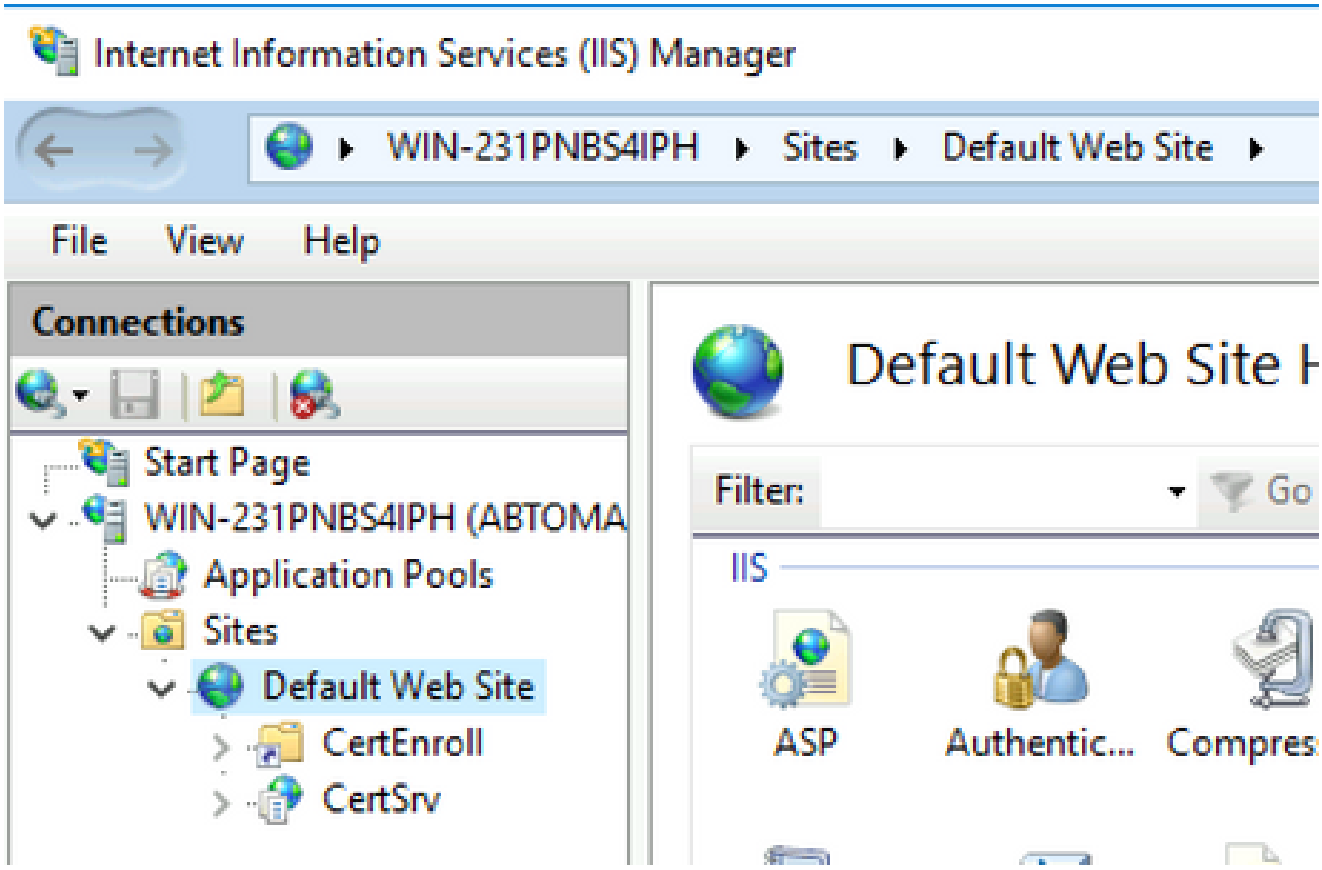


Maak een site in IIS om het nieuwe CRL distributiepunt bloot te stellen

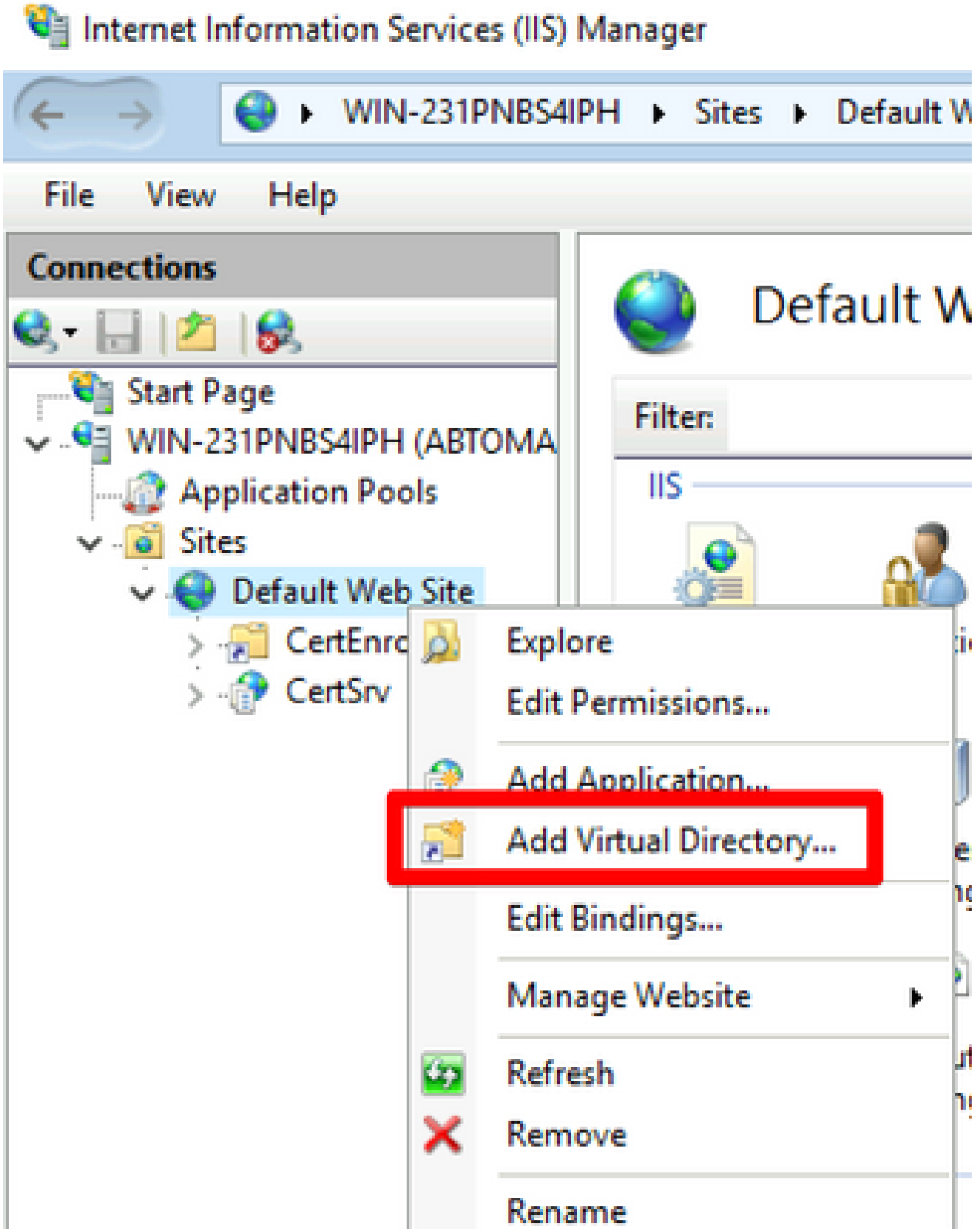
Om ISE toegang te geven tot de CRL-bestanden, maakt u de map waarin de CRL-bestanden zich bevinden toegankelijk via IIS.

1. Klik in de taakbalk van IIS-server op **Start**. Kies **Administrative Tools** > **Internet Information Services (IIS) Manager**.

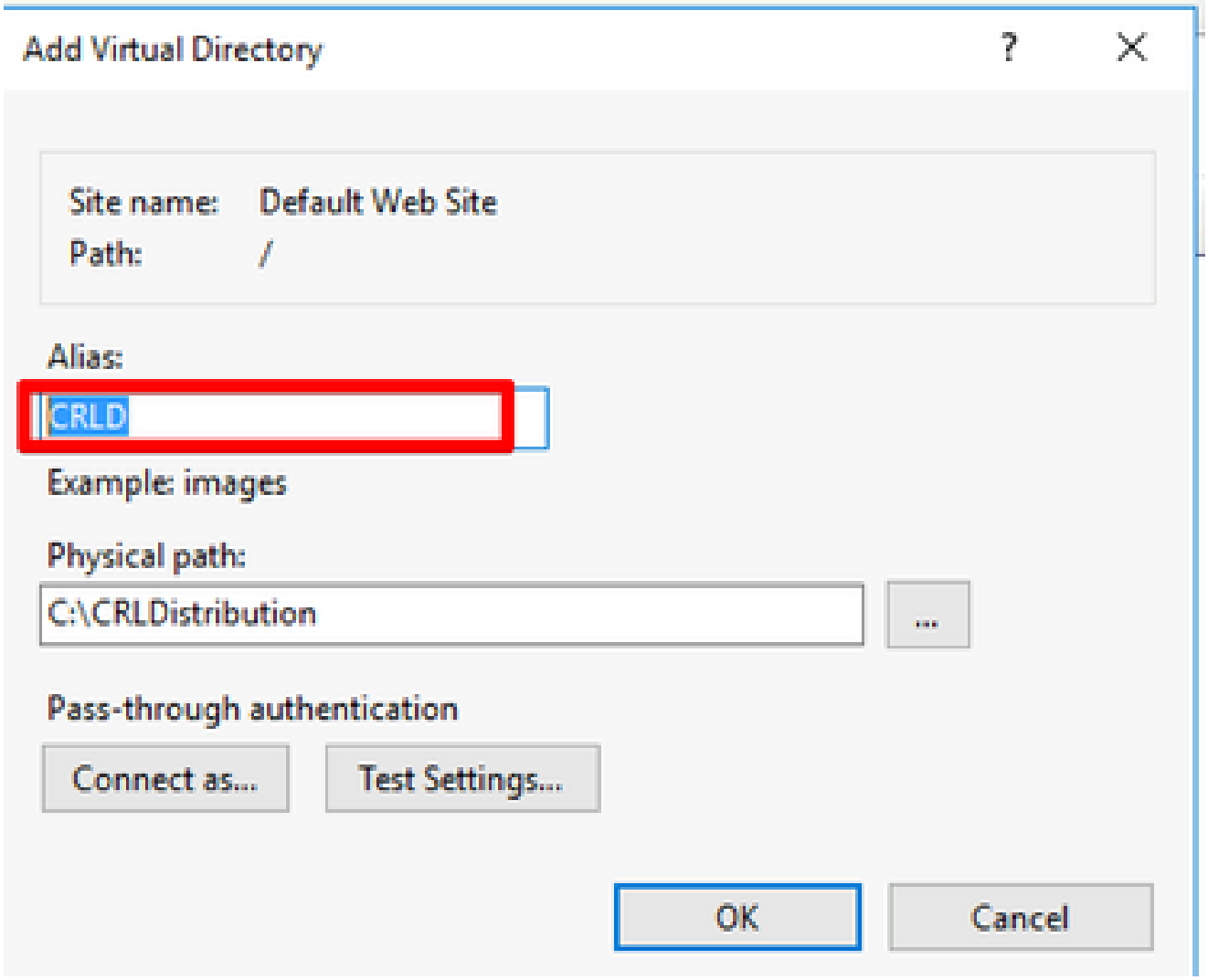
2. Vouw in het linker deelvenster (bekend als de consolestructuur) de naam van de IIS-server uit en vouw deze vervolgens uit **Sites**.



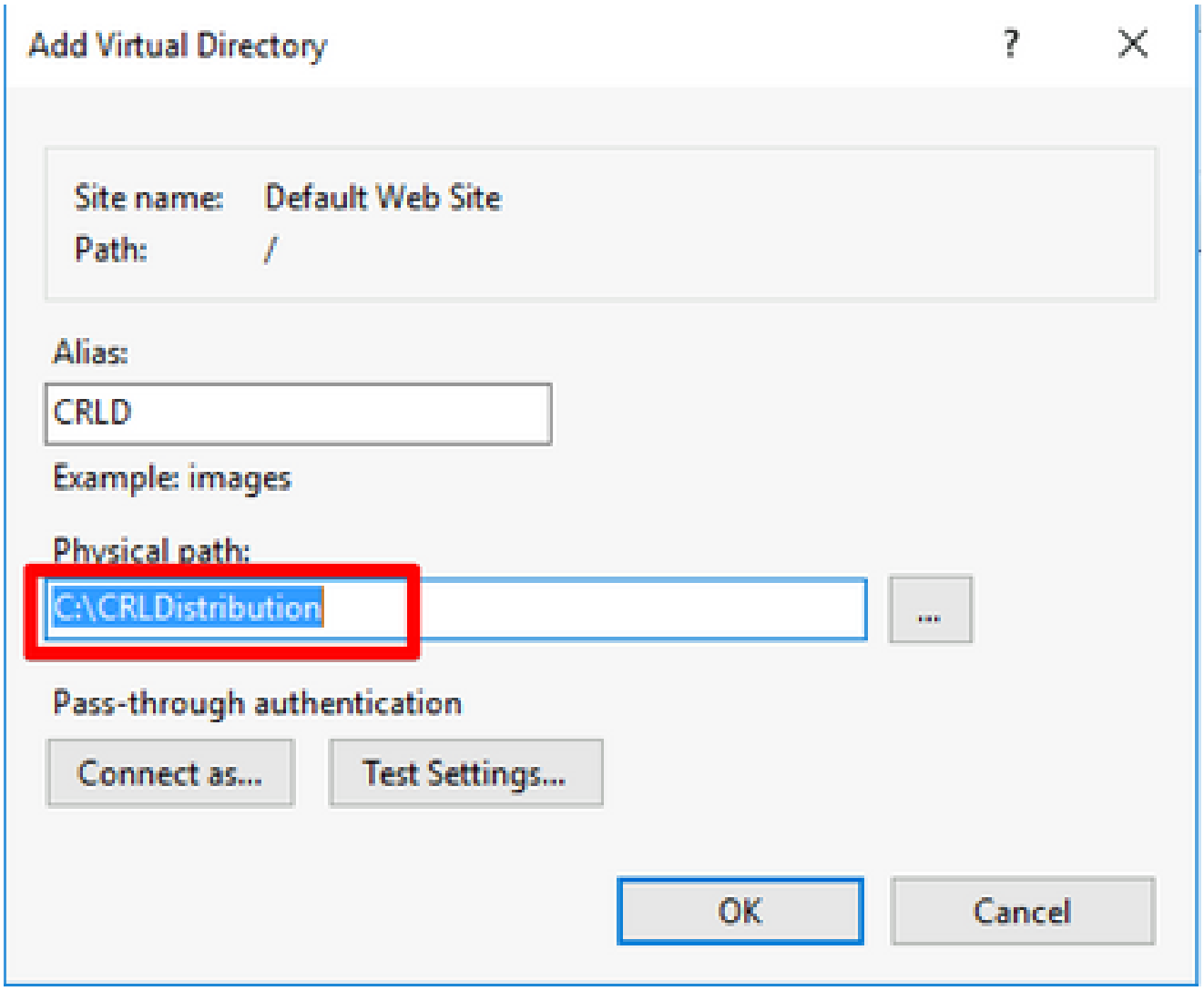
3. Klik met de rechtermuisknop **Default Web Site** en kies **Add Virtual Directory**, zoals in deze afbeelding.



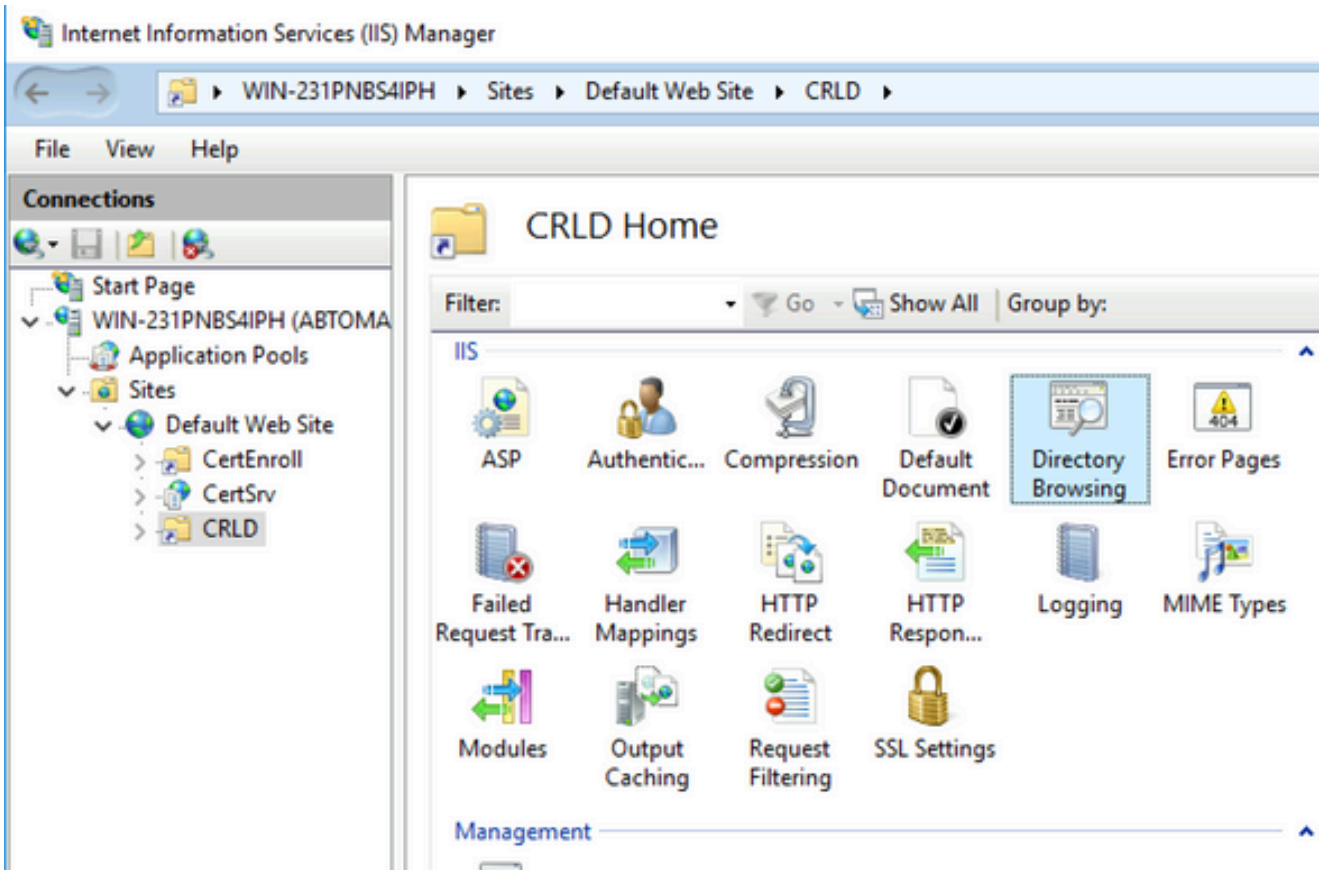
4. Voer in het veld Alias een sitenaam in voor het CRL-distributiepunt. In dit voorbeeld is CRLD ingevoerd.



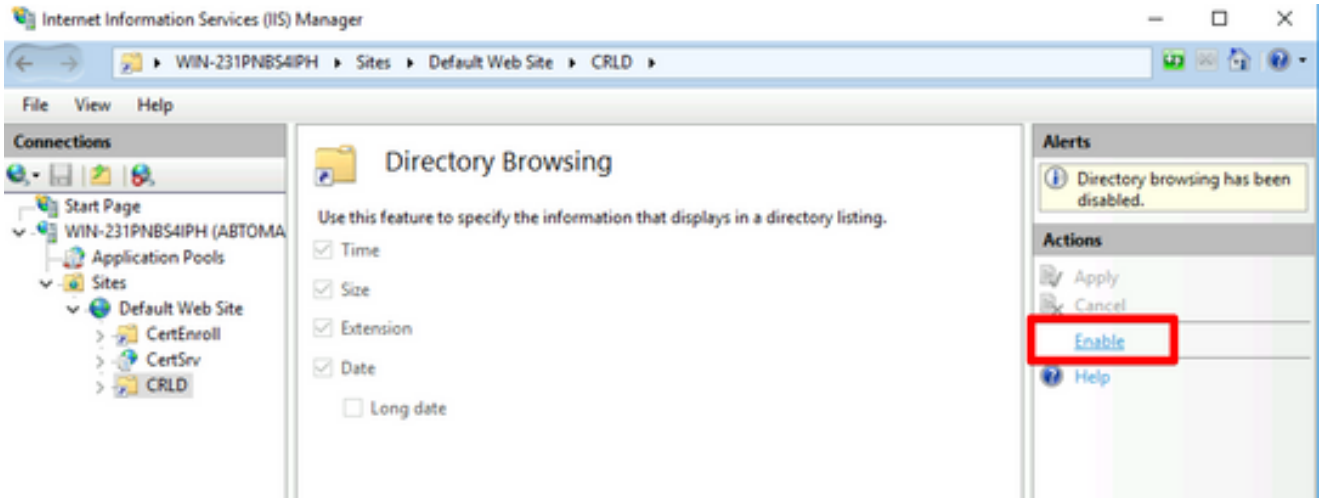
5. Klik op de ellips (. . .) rechts van het veld Fysiek pad en blader naar de map die in sectie 1 is gemaakt. Selecteer de map en klik op OK. Klik op OK om het venster Virtuele map toevoegen te sluiten.



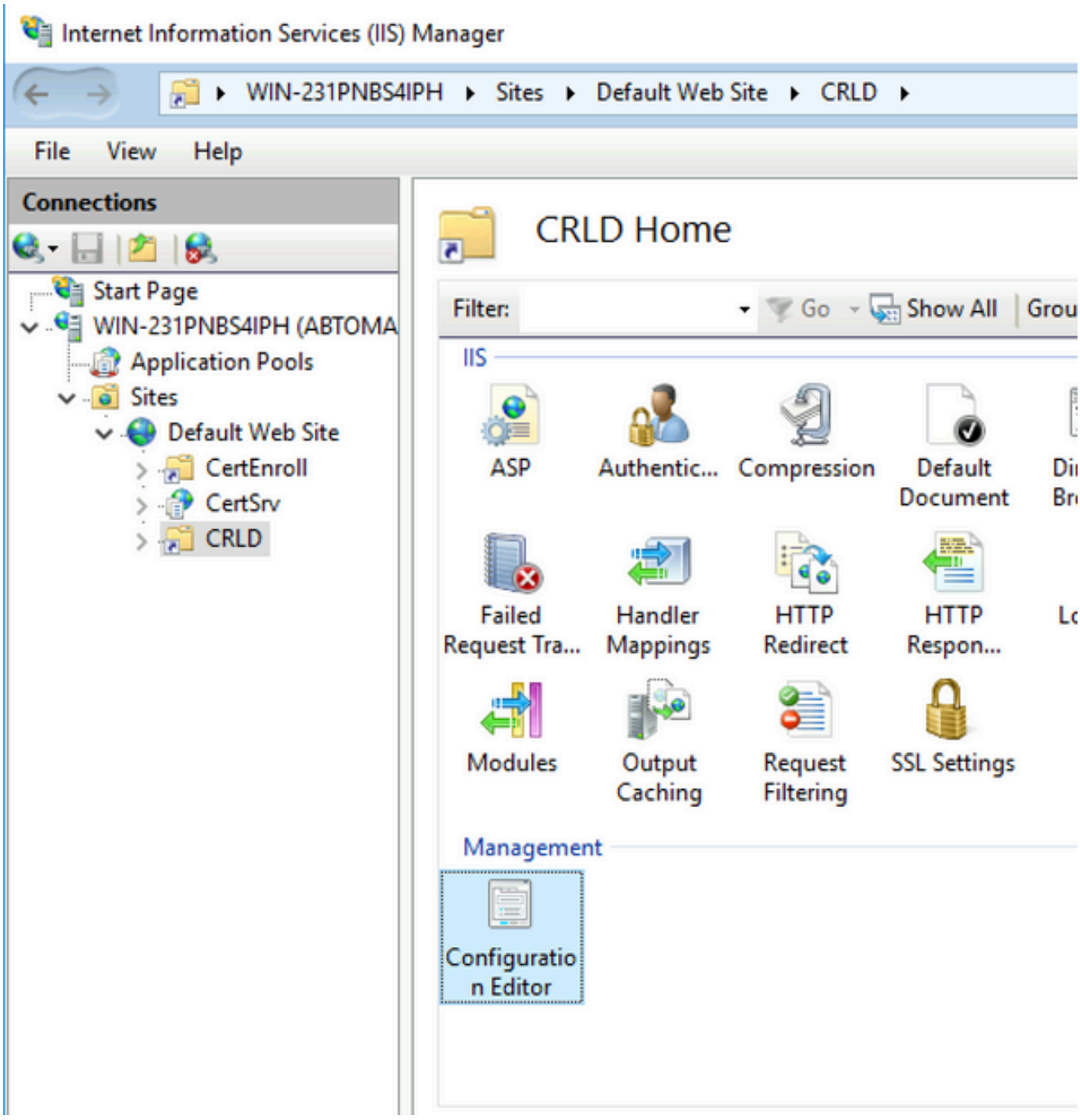
6. De in stap 4 ingevoerde sitenaam moet in het linker deelvenster worden gemarkeerd. Als dit niet het geval is, kies dan nu. Dubbelklik in het middendeelvenster **Directory Browsing**.



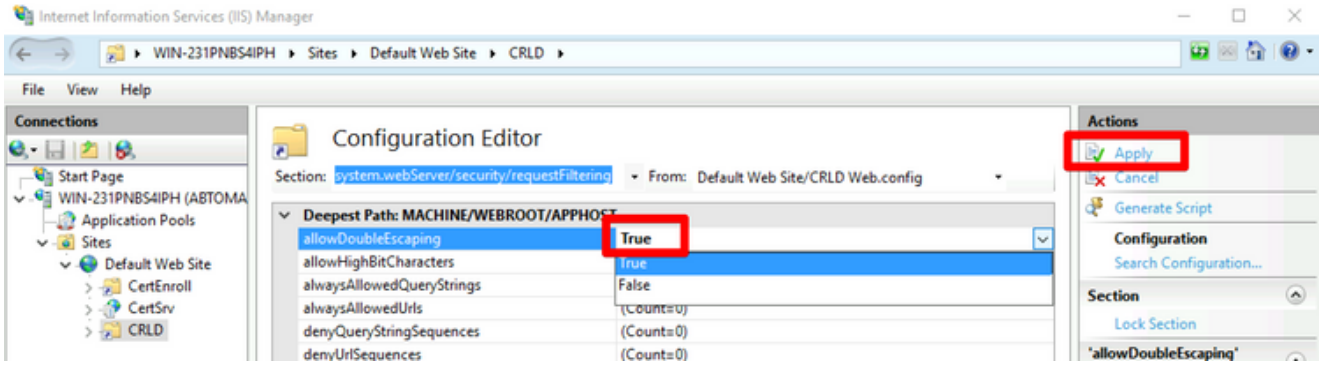
7. Klik in het rechter deelvenster op **Enable** om bladeren door mappen mogelijk te maken.



8. Kies in het linkerdeelvenster opnieuw de naam van de site. Dubbelklik in het middendeelvenster **Configuration Editor**.



9. Kies **system.webServer/security/requestFiltering**dit in de vervolgkeuzelijst Sectie. Kies een optie in de **allowDoubleEscaping** vervolgkeuzelijst **True**. Klik in het rechter deelvenster op **Apply**, zoals in deze afbeelding wordt weergegeven.

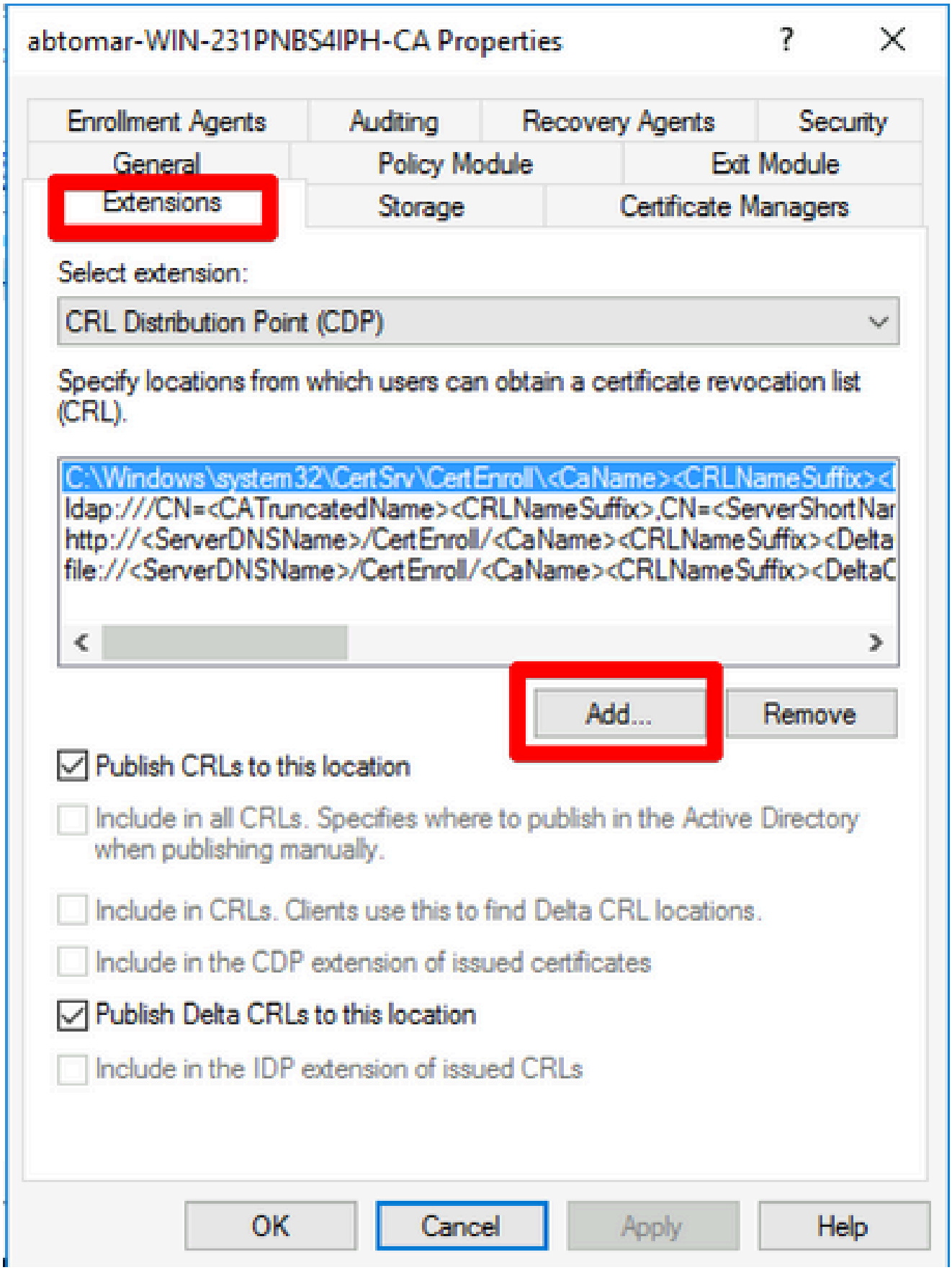


De map moet nu toegankelijk zijn via IIS.

Microsoft CA Server configureren om CRL-bestanden naar het distributiepunt te publiceren

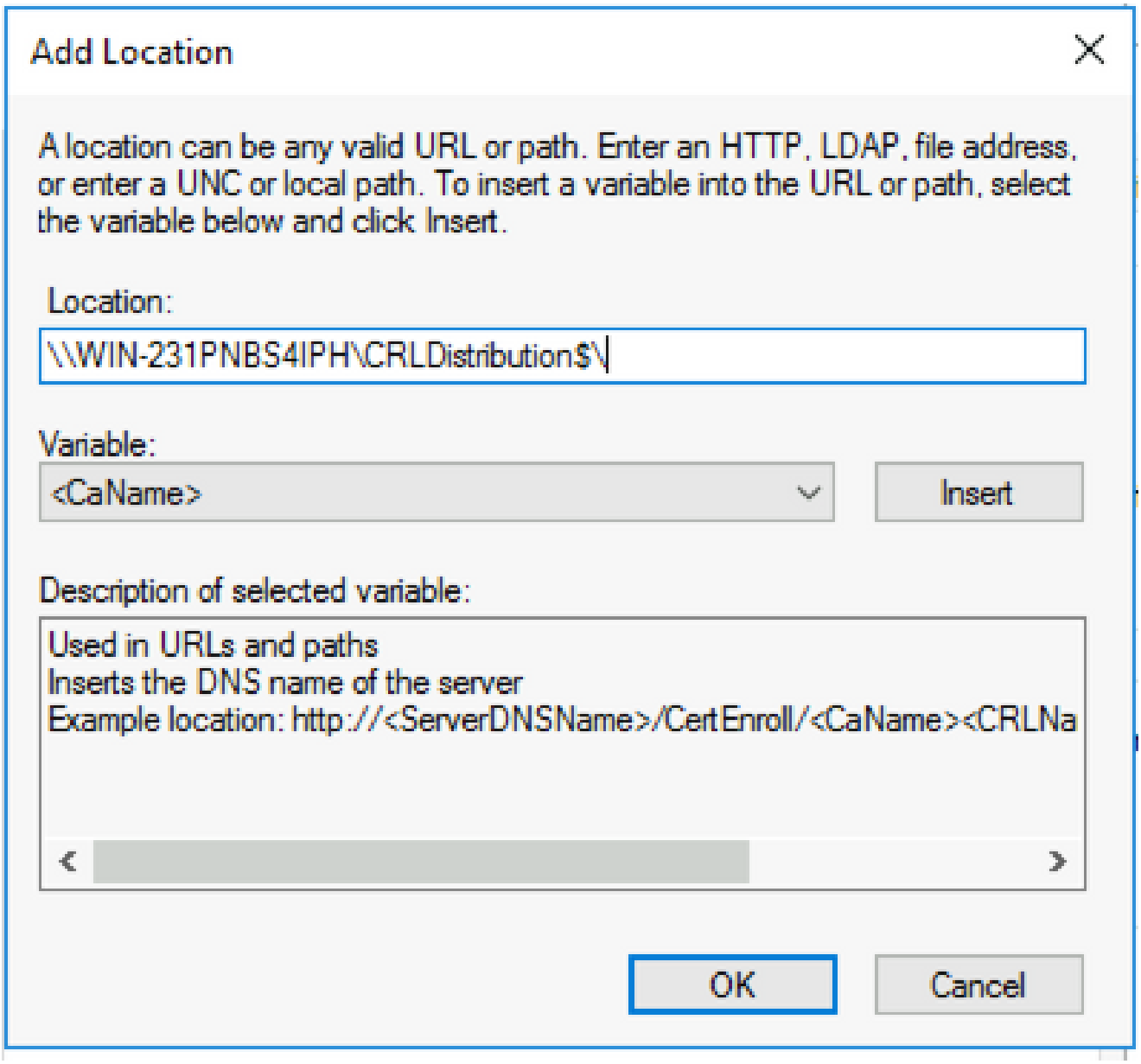
Nu een nieuwe map is geconfigureerd om de CRL-bestanden te huisvesten en de map is blootgesteld in IIS, configureer de Microsoft CA-server om de CRL-bestanden te publiceren naar de nieuwe locatie.

1. Klik in de taakbalk van CA-server op **Start**. Kies **Administrative Tools** > **Certificate Authority**.
2. Klik in het linkerdeelvenster met de rechtermuisknop op de CA-naam. Kies **Properties** en klik vervolgens op het **Extensions** tabblad. Om een nieuw CRL distributiepunt toe te voegen, klikt u op **Add**.

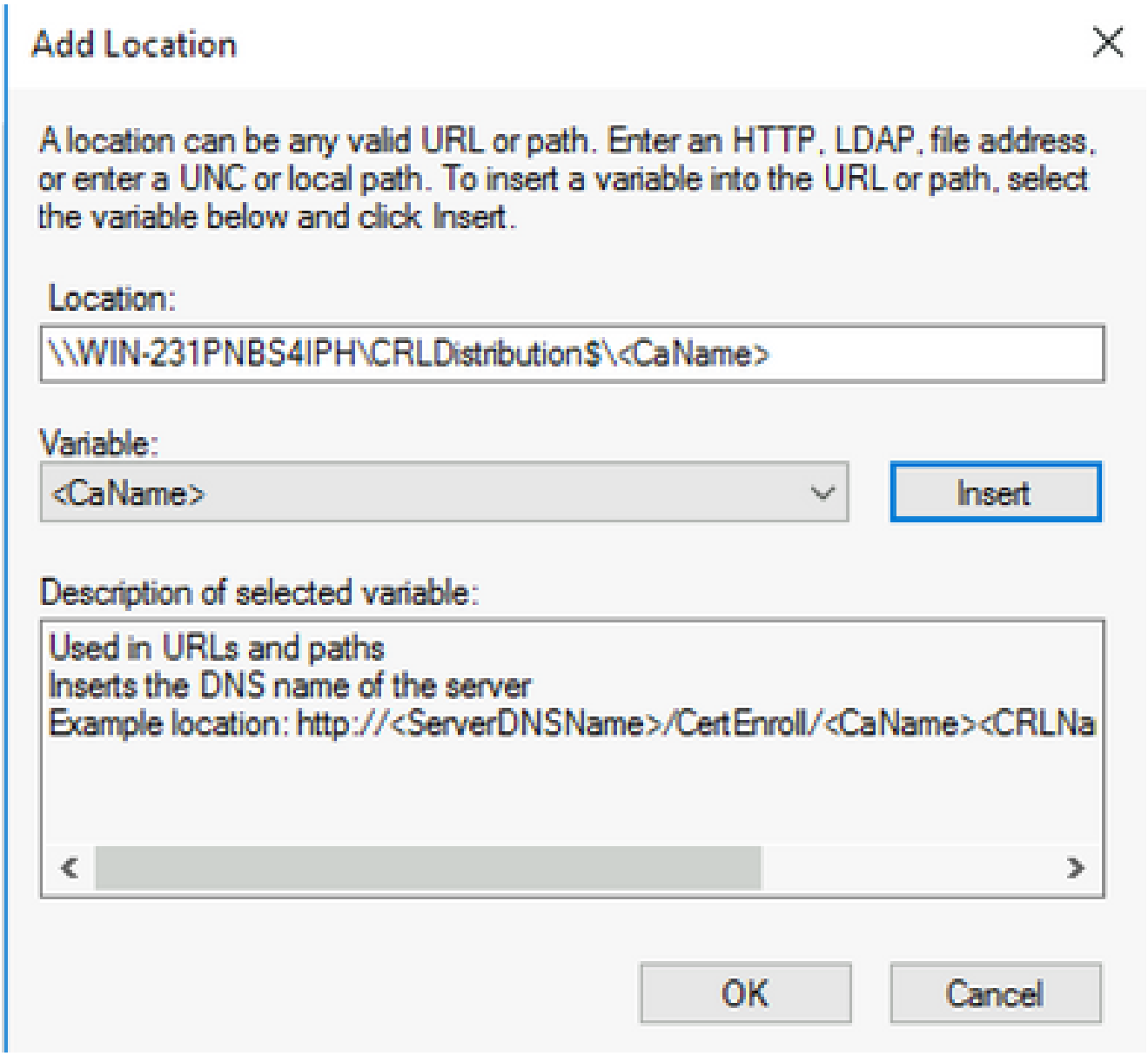


3. Voer in het veld Locatie het pad in naar de map die in sectie 1 is gemaakt en gedeeld. In het voorbeeld in sectie 1 is het pad:

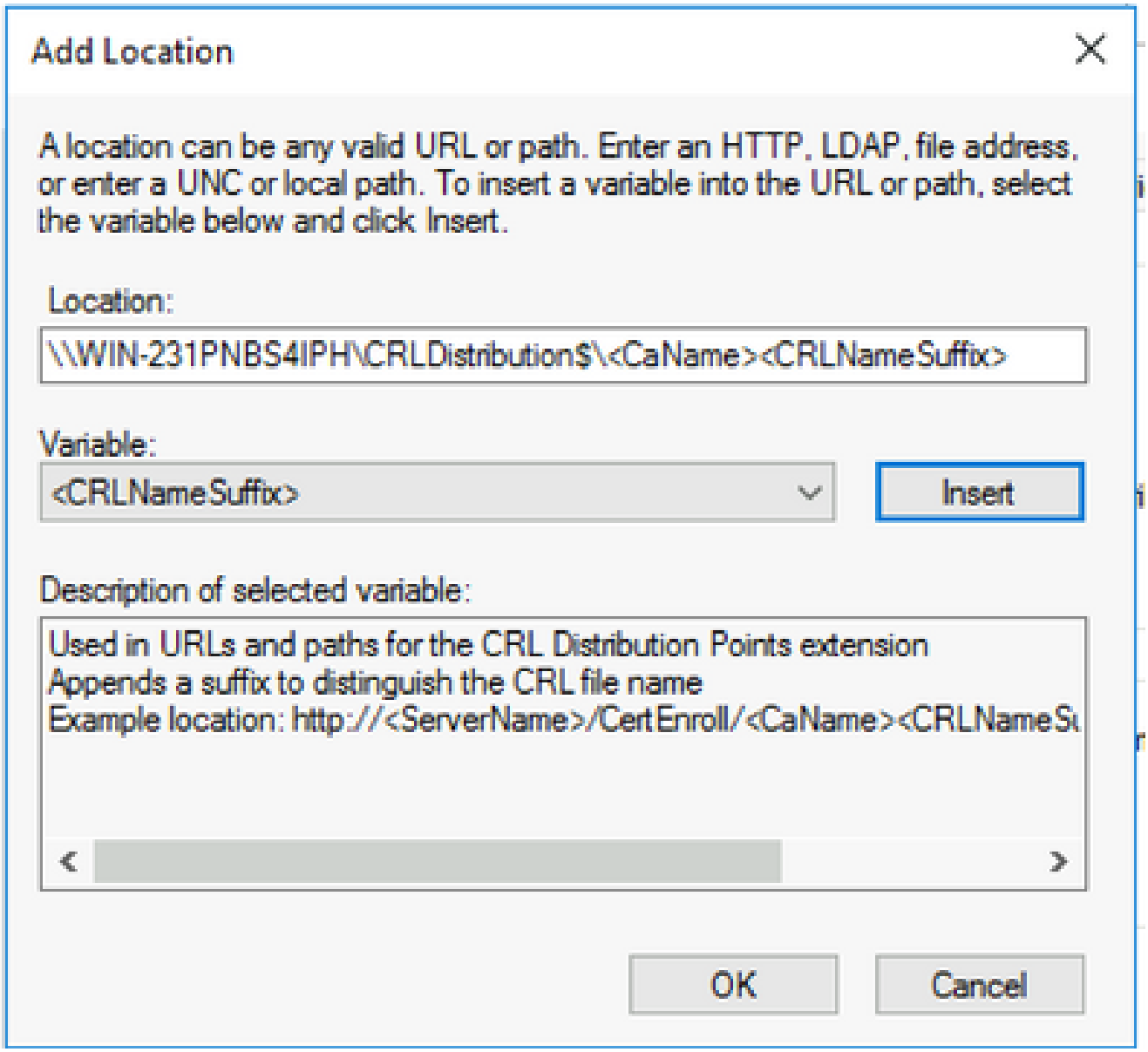
   \\WIN-231PNBS4IPH\CRLDolddistributie$



4. Als het veld Locatie is ingevuld, kiest u
uit de vervolgkeuzelijst Variabele en klikt u vervolgens op **Insert.**



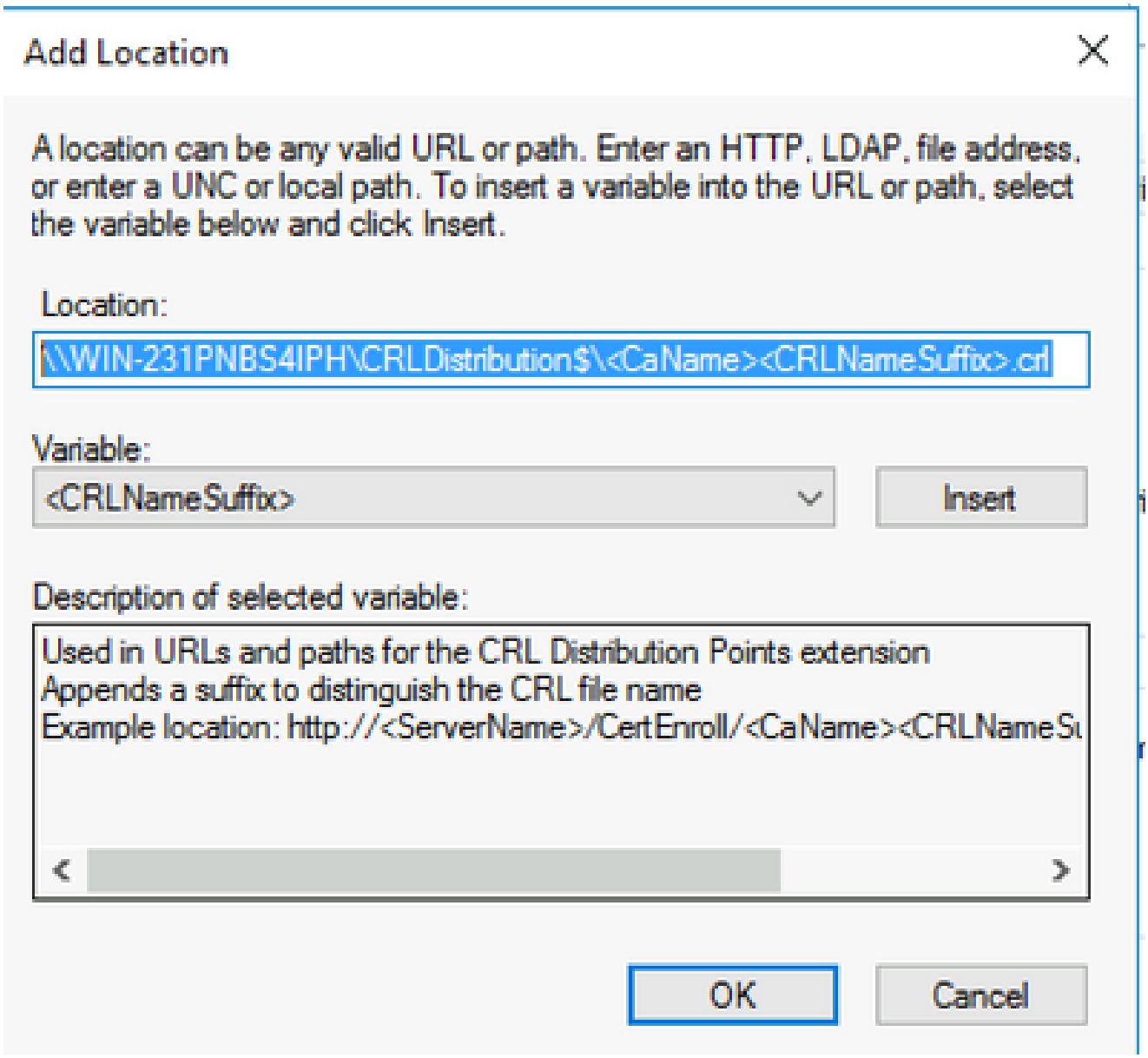
5. Kies
   en klik vervolgens in de vervolgkeuzelijst Variabele **Insert**.



6. **.crl** Aan het einde van het pad toevoegen in het veld Locatie. In dit voorbeeld is de locatie:

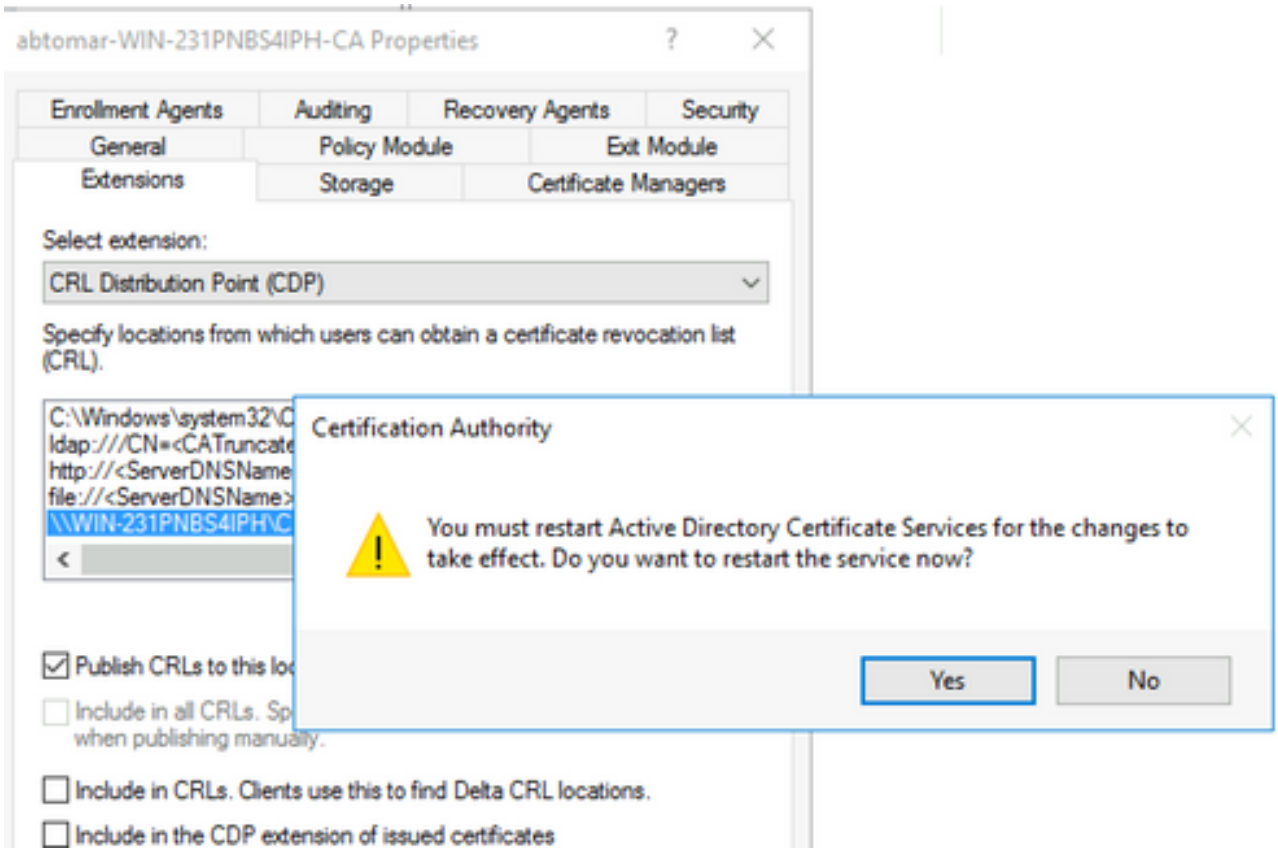
\\WIN-231PNBS4IPH\CRLDistribution$

.crl

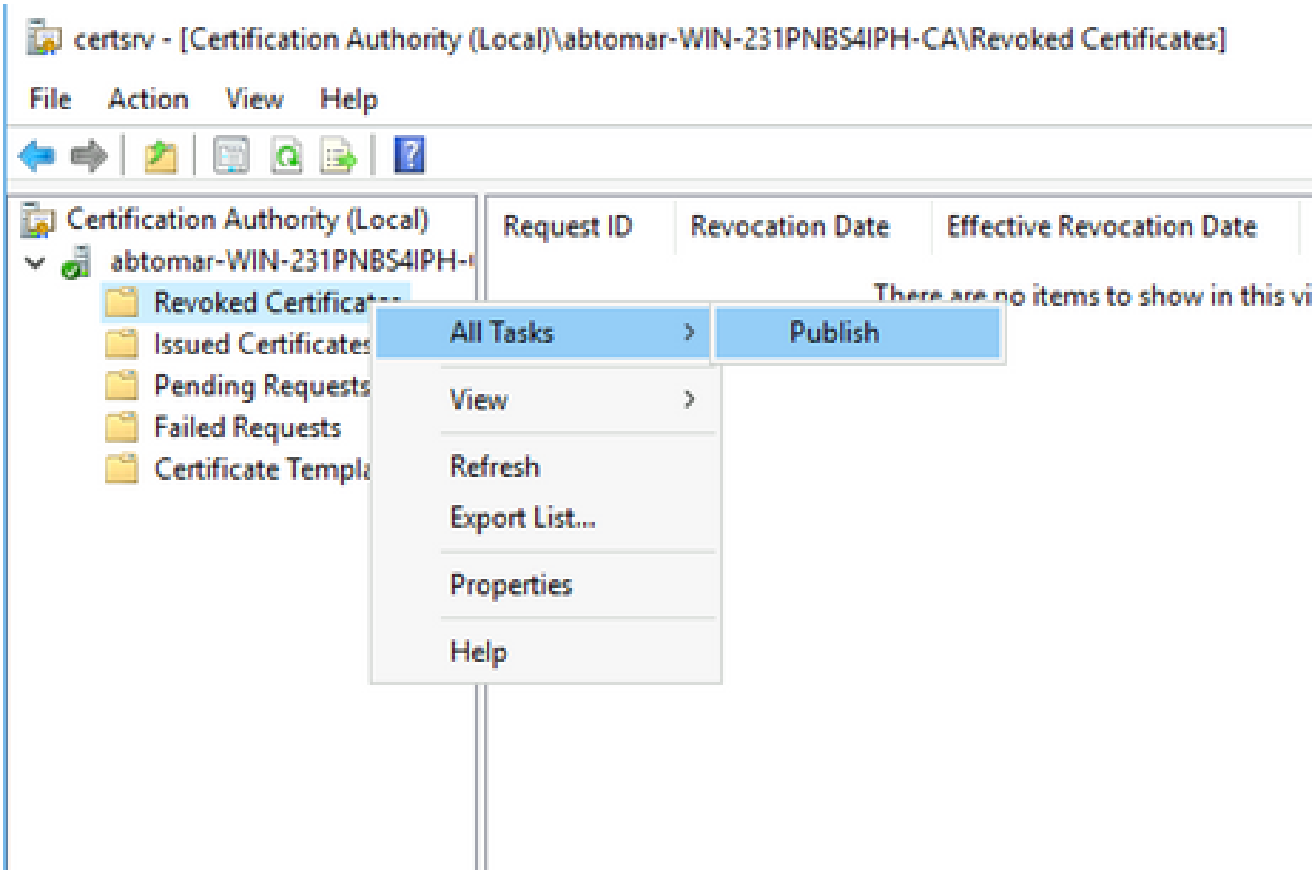


7. Klik op **OK** om terug te keren naar het tabblad Uitbreidingen. Schakel het **Publish CRLs to this location** aankruisvakje in en klik vervolgens op **OK** om het venster Eigenschappen te sluiten.

   Er wordt een prompt weergegeven voor toestemming om Active Directory Certificate Services opnieuw te starten. Klik op de knop .**Yes**



8. Klik met de rechtermuisknop in het linker deelvenster **Revoked Certificates**. Kies **All Tasks** > **Publish**. Zorg ervoor dat New CRL is geselecteerd en klik vervolgens op **OK**.



De Microsoft CA-server moet een nieuw .crl-bestand maken in de map die in sectie 1 is

gemaakt. Als het nieuwe CRL-bestand met succes is gemaakt, verschijnt er geen dialoogvenster nadat op OK is geklikt. Als een fout wordt teruggegeven met betrekking tot de nieuwe map voor distributiepunten, herhaalt u elke stap in deze sectie zorgvuldig.

Controleer of het CRL-bestand bestaat en toegankelijk is via IIS

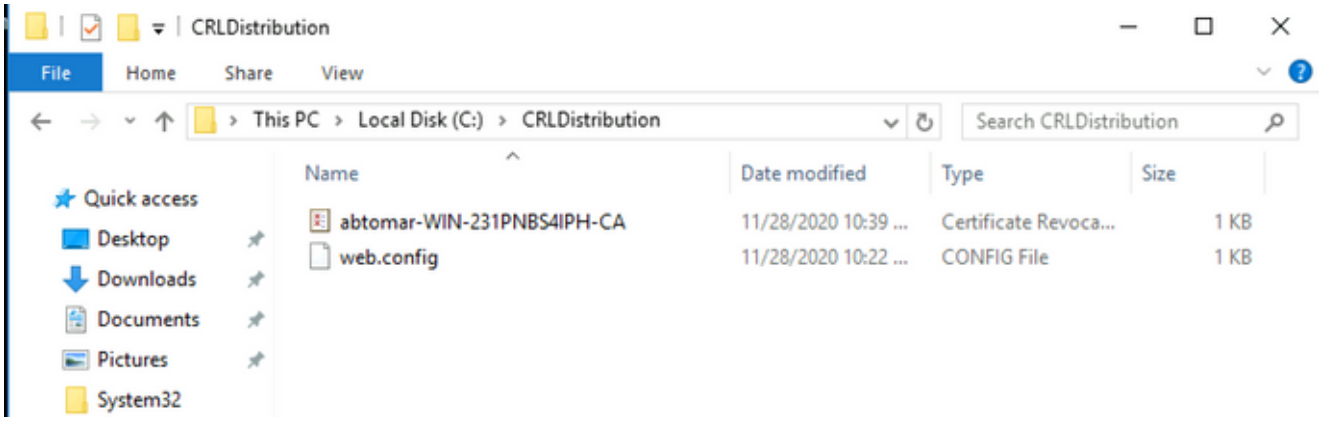
Controleer of de nieuwe CRL-bestanden bestaan en dat ze via IIS toegankelijk zijn vanaf een ander werkstation voordat u deze sectie start.

1. Open op de IIS-server de map die in sectie 1 is gemaakt. Er moet één .crl bestand aanwezig zijn met het formulier

   .crl

   waar
   de naam van de CA server is. In dit voorbeeld is de bestandsnaam:

   abtomar-WIN-231PNBS4IPH-CA.crl



2. Vanuit een werkstation op het netwerk (idealiter op hetzelfde netwerk als de ISE primaire Admin-knooppunt), opent u een webbrowser en bladert u naar http://

   /

   waar
   de servernaam is van de IIS-server die in sectie 2 is geconfigureerd en
   is de sitenaam die voor het distributiepunt in sectie 2 is gekozen. In dit voorbeeld is de URL:

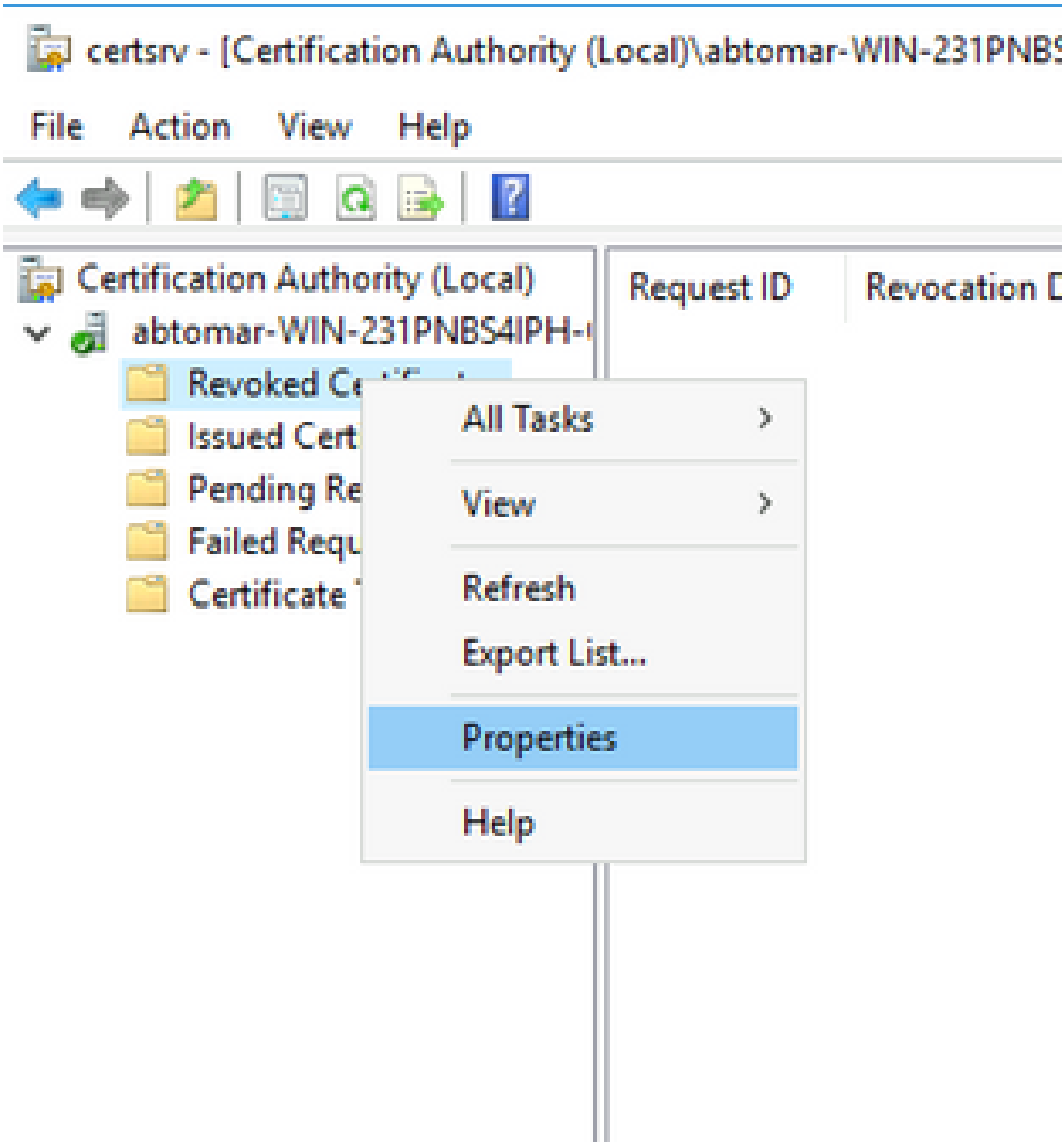
   http://win-231pnbs4iph/CRLD

   De indexbeeldjes, waaronder het in stap 1 geobserveerde bestand.

Configureer ISE om het nieuwe CRL-distributiepunt te gebruiken

Alvorens ISE wordt gevormd om CRL terug te winnen, het interval bepalen om CRL te publiceren. De strategie om deze interval te bepalen valt buiten het bereik van dit document. De potentiële waarden (in Microsoft CA) zijn 1 uur tot 411 jaar, inclusief. De standaardwaarde is 1 week. Zodra een geschikt interval voor uw milieu is bepaald, stel het interval met deze instructies in:

1. Klik in de taakbalk van CA-server op **Start**. Kies **Administrative Tools** > **Certificate Authority**.
2. Vouw in het linker deelvenster de CA uit. Klik met de rechtermuisknop op de **Revoked Certificates** map en kies **Properties**.
3. Voer in de velden voor het CRL-publicatieinterval het gewenste nummer in en kies de tijdsperiode. Klik op **OK** om het venster te sluiten en de wijziging toe te passen. In dit voorbeeld is een publicatieinterval van zeven dagen ingesteld.



4. **certutil -getreg CA\Clock*** Voer de opdracht in om de waarde ClockSkew te bevestigen. De standaardwaarde is 10 minuten.

   Voorbeelduitvoer:

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

5. **certutil -getreg CA\CRLov*** Voer de opdracht in om te controleren of de CRLOoverlapPeriod handmatig is ingesteld. Standaard is de waarde voor CRLOoverlapUnit 0, wat aangeeft dat

er geen handmatige waarde is ingesteld. Als de waarde een andere waarde is dan 0, registreert u de waarde en de eenheden.

Voorbeelduitvoer:

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

6. **certutil -getreg CA\CRLpe*** Voer de opdracht in om de CRLP-periode te controleren die is ingesteld in stap 3.

   Voorbeelduitvoer:

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

7. Bereken de CRL-respijtperiode als volgt:

   a. Indien CRLOverlapPeriod werd ingesteld in stap 5: OVERLAP = CRLOverlapPeriod, in minuten;

   Anders: OVERLAP = (CRLPeriod / 10), in minuten

   b. Bij OVERLAP > 720, OVERLAP = 720

   c. Als OVERLAP < (1,5 * ClockSkewMinutes) is, dan OVERLAP = (1,5 * ClockSkewMinutes)

   d. Bij OVERLAP > CRLPeriod, in minuten dan OVERLAP = CRLPeriod in minuten

   e. respijtperiode = OVERLAP + klokminuten

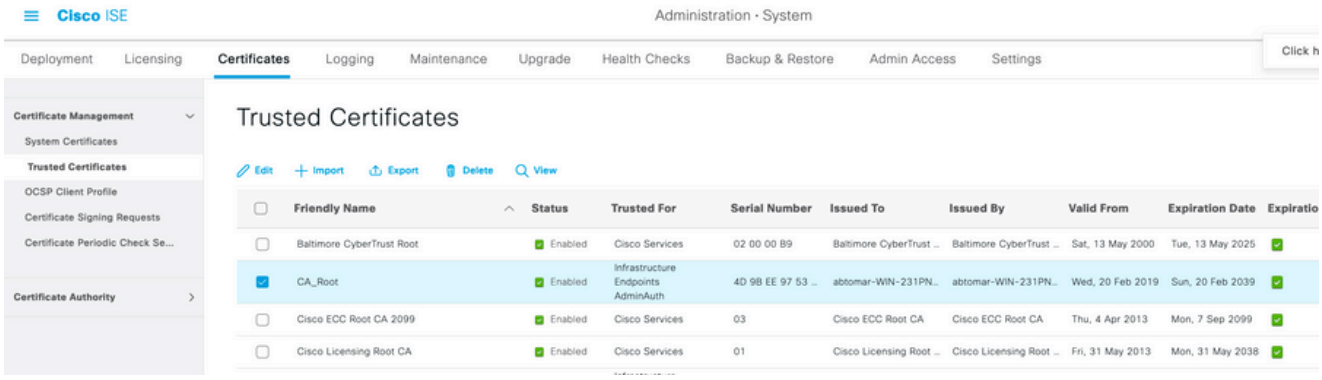
```
Example:

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
```

De berekende respijtperiode is de hoeveelheid tijd tussen het tijdstip waarop de CA het volgende CRL publiceert en het moment waarop het huidige CRL afloopt. ISE moet worden geconfigureerd om de CRL's op te halen.

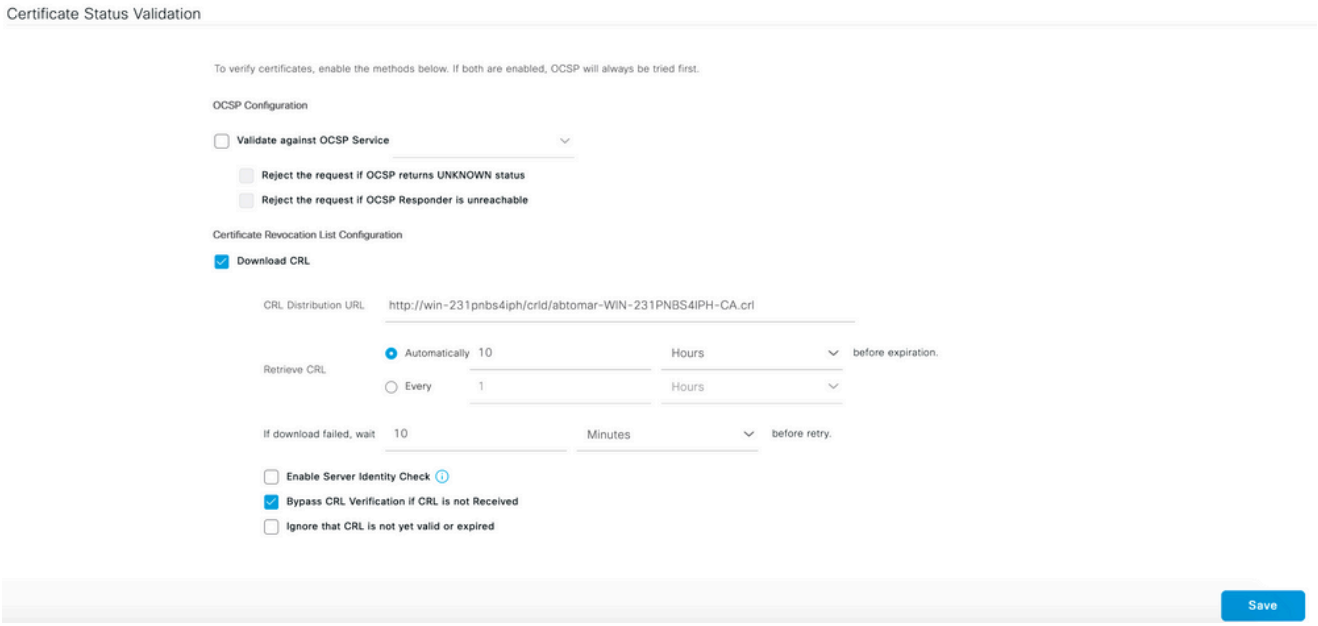
8. Log in op de ISE Primary Admin knooppunt en kies **Administration** > **System** > **Certificates**. Kies in het linkerdeelvenster **Trusted Certificate**.



9. Schakel het aanvinkvakje naast het CA-certificaat in waarvoor u CRL's wilt configureren. Klik op de knop **.Edit**
10. Schakel het selectievakje onder in het **Download CRL** venster.
11. Voer in het veld CRL Distribution URL het pad naar het CRL Distribution Point in, dat het .crl-bestand bevat dat in sectie 2 is gemaakt. In dit voorbeeld is de URL:

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

12. ISE kan worden geconfigureerd om het CRL op regelmatige intervallen terug te halen of op basis van de verloopdatum (die in het algemeen ook een regelmatig interval is). Wanneer het CRL publicatieinterval statisch is, worden de tijdigere updates van CRL verkregen wanneer de laatstgenoemde optie wordt gebruikt. Klik op het **Automatically** keuzerondje.
13. Stel de waarde voor ophalen in op een waarde kleiner dan de respijtperiode die in stap 7 is berekend. Als de waardenreeks langer is dan de respijtperiode, controleert ISE het CRL-distributiepunt voordat CA het volgende CRL heeft gepubliceerd. In dit voorbeeld wordt de respijtperiode berekend op 730 minuten, of 12 uur en 10 minuten. Voor het ophalen wordt een waarde van 10 uur gebruikt.
14. Stel het herhalingsinterval in zoals geschikt voor uw omgeving. Als ISE in de vorige stap het CRL niet met het ingestelde interval kan ophalen, zal het met dit kortere interval opnieuw proberen.
15. Schakel het **Bypass CRL Verification if CRL is not Received** aanvinkvakje in om op certificaat gebaseerde verificatie normaal te laten verlopen (en zonder CRL-controle) als ISE het CRL voor deze CA bij haar laatste downloadpoging niet kon ophalen. Als dit aanvinkvakje niet is ingeschakeld, zal alle op certificaten gebaseerde verificatie met door deze certificeringsinstantie afgegeven certificaten mislukken als het CRL niet kan worden opgehaald.
16. Schakel het **Ignore that CRL is not yet valid or expired** aanvinkvakje in om ISE toe te staan verlopen (of nog niet geldig) CRL-bestanden te gebruiken alsof ze geldig waren. Als dit aanvinkvakje niet is ingeschakeld, beschouwt ISE een CRL als ongeldig vóór de datum van inwerkingtreding en na de volgende update. Klik op **Save** om de configuratie te voltooien.



Verifiëren

Er is momenteel geen verificatieprocedure beschikbaar voor deze configuratie.

Problemen oplossen

Er is momenteel geen specifieke troubleshooting-informatie beschikbaar voor deze configuratie.

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.