Microsoft CA Server configureren om lijst met certificaatherroeping voor ISE te publiceren

Inhoud

Inleiding

Dit document beschrijft de configuratie van een Microsoft certificaatserver (CA) van de Autoriteit die Internet Information Services (IS) beheert om de updates van de Revocatielijst (CRL) van het Certificaat te publiceren. Het legt ook uit hoe te om de Cisco Identity Services Engine (ISE) (versies 3.0 en hoger) te configureren om de updates voor gebruik in certificatie op te halen. ISE kan worden ingesteld om CRL's te herstellen voor de verschillende CA root certificaten die het gebruikt bij certificatie.

Voorwaarden

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 levend is, zorg er dan voor dat u de mogelijke impact van om het even welke opdracht begrijpt.

Configureren

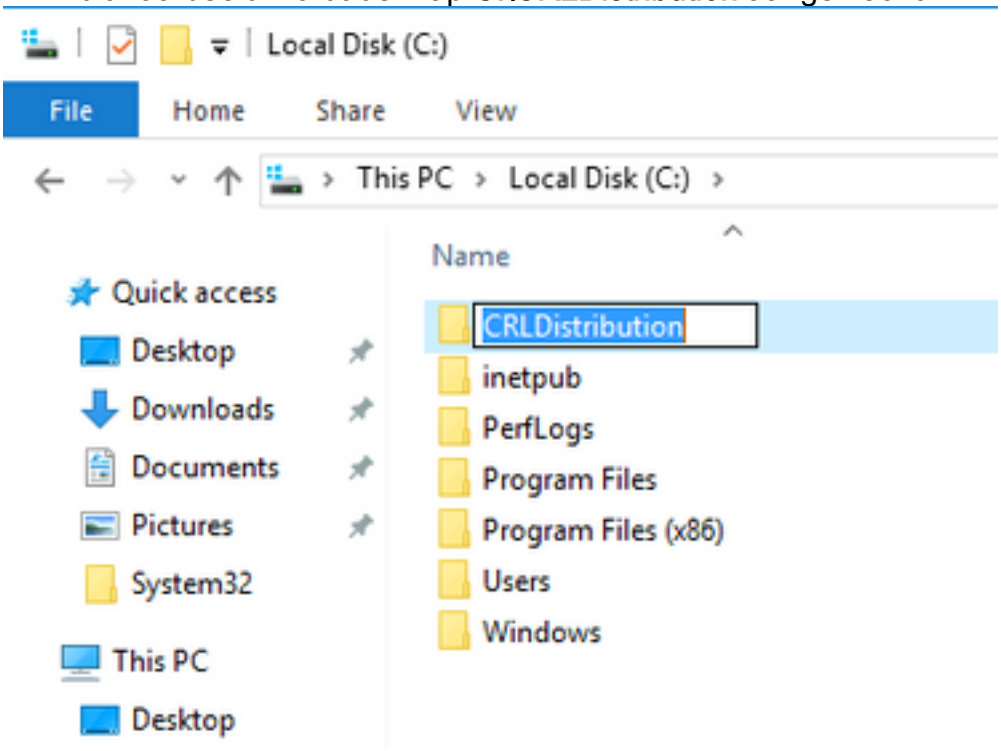
Deze sectie bevat informatie over het configureren van de functies die in dit document worden beschreven.

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

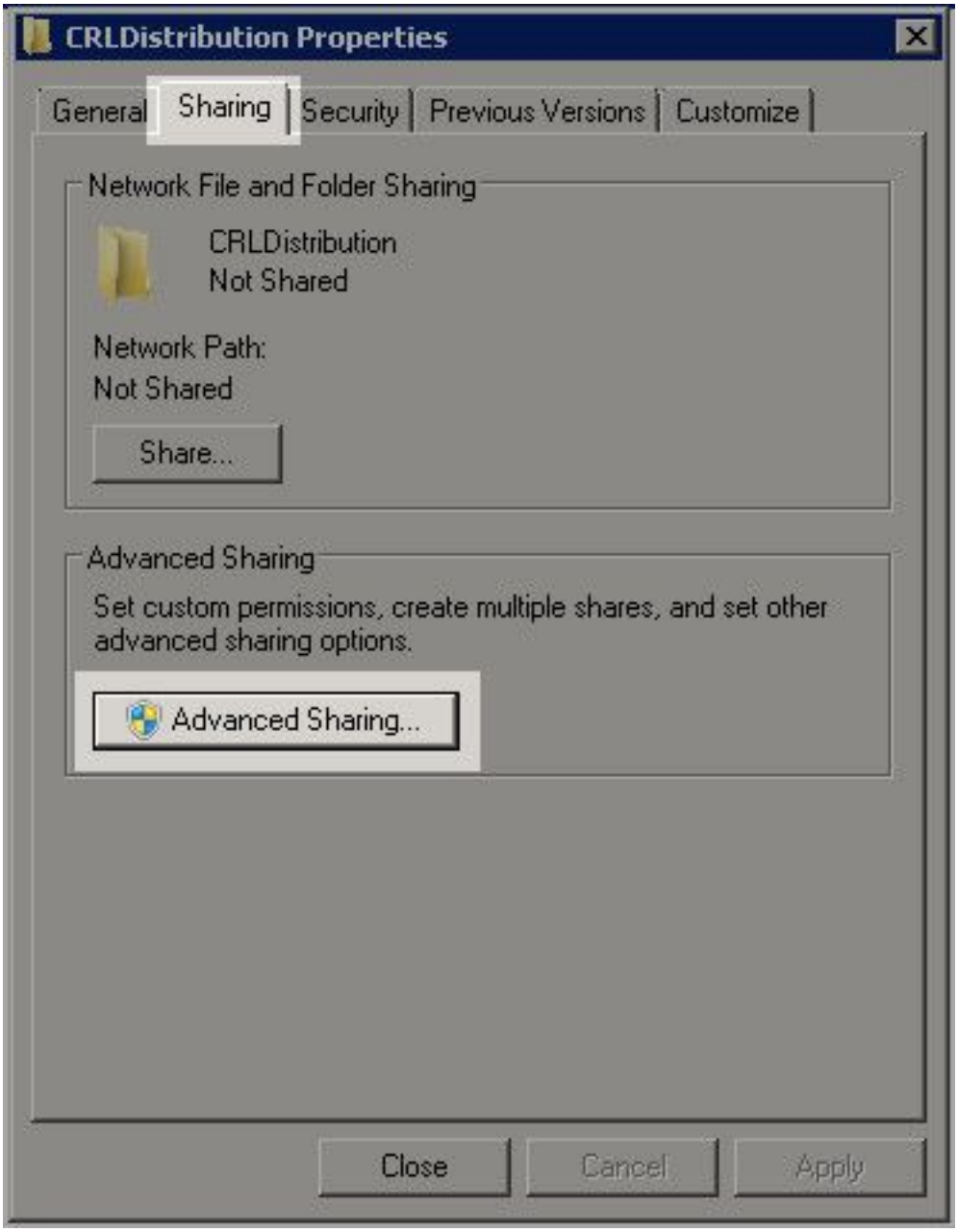
De eerste taak is het configureren van een locatie op de CA server om de CRL bestanden op te slaan. Standaard publiceert de Microsoft CA-server de bestanden naar **C:\Windows\system32\CertSrv\CertEnroll**

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

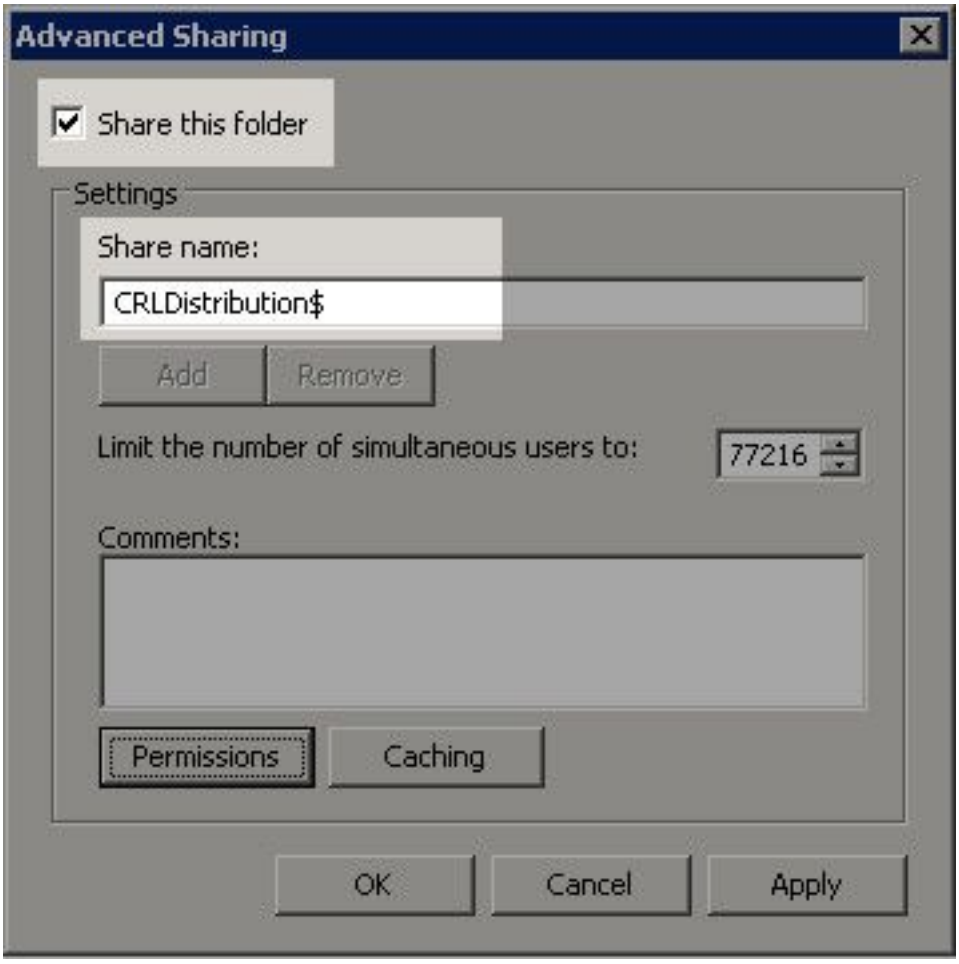
1. Kies een locatie in het bestandssysteem op de IIS-server en maak een nieuwe map aan. In dit voorbeeld wordt de map **C:\CRLDistribution** aangemaakt.



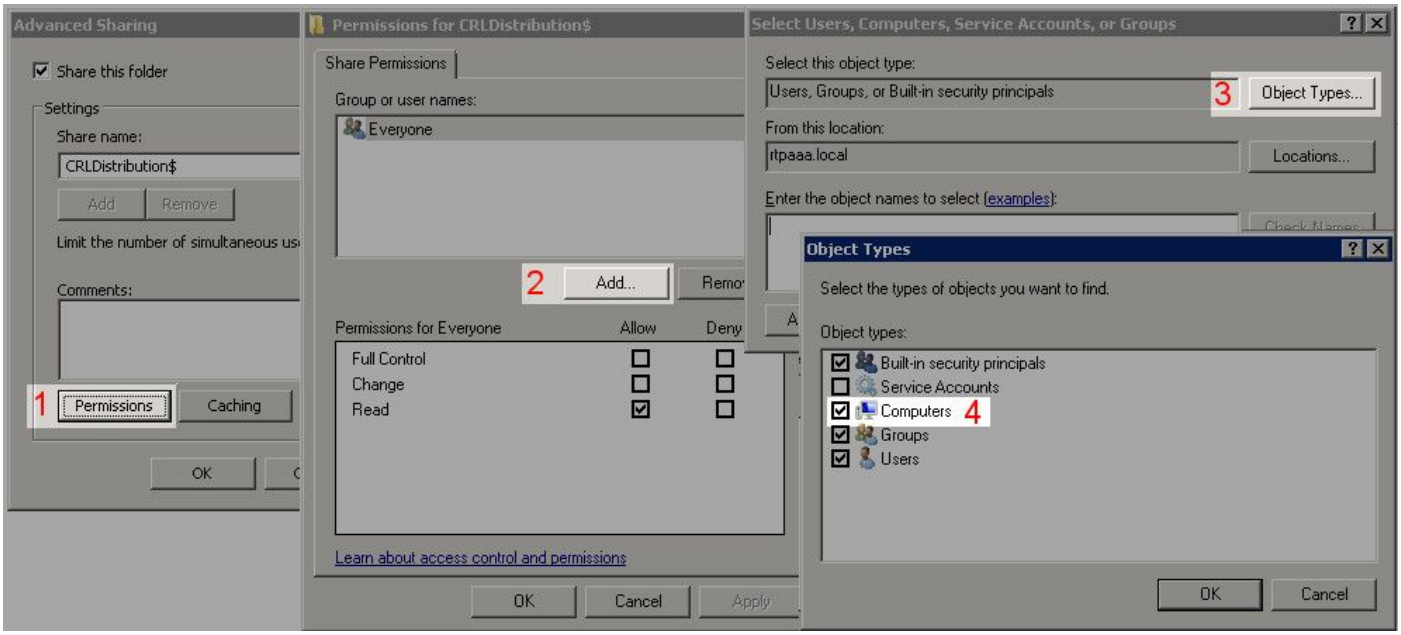
2. Om de CA-bestanden naar de nieuwe map te kunnen schrijven, moet het delen zijn ingeschakeld. Klik met de rechtermuisknop op de nieuwe map, kies **Eigenschappen**, klik op het **tabblad** Delen en klik vervolgens op **Geavanceerd delen**.



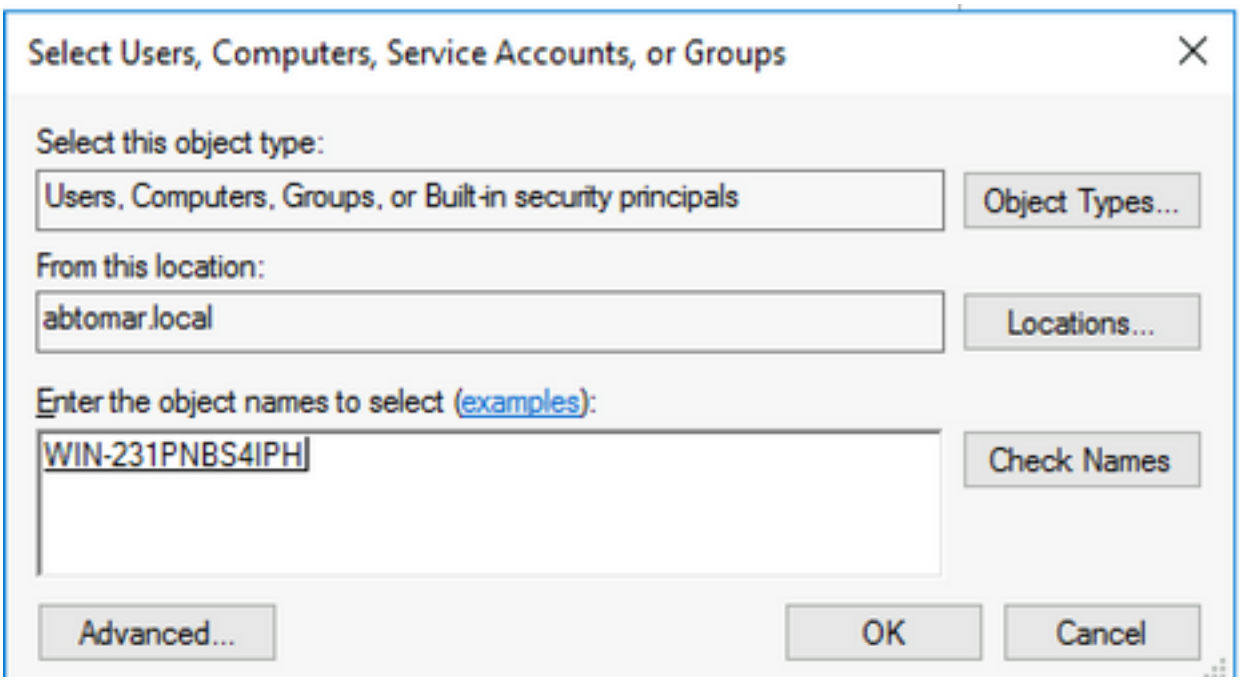
3. Als u de map wilt delen, controleert u het vakje **Deze map delen** en voegt u vervolgens een dollarteken ($) toe aan het einde van de naam van het aandeel in het veld Naam delen om het aandeel te verbergen.



4. Klik op **toegangsrechten** (1), klik op **Add** (2), klik op **Objecttypen** (3) en controleer het vakje **Computers** (4).

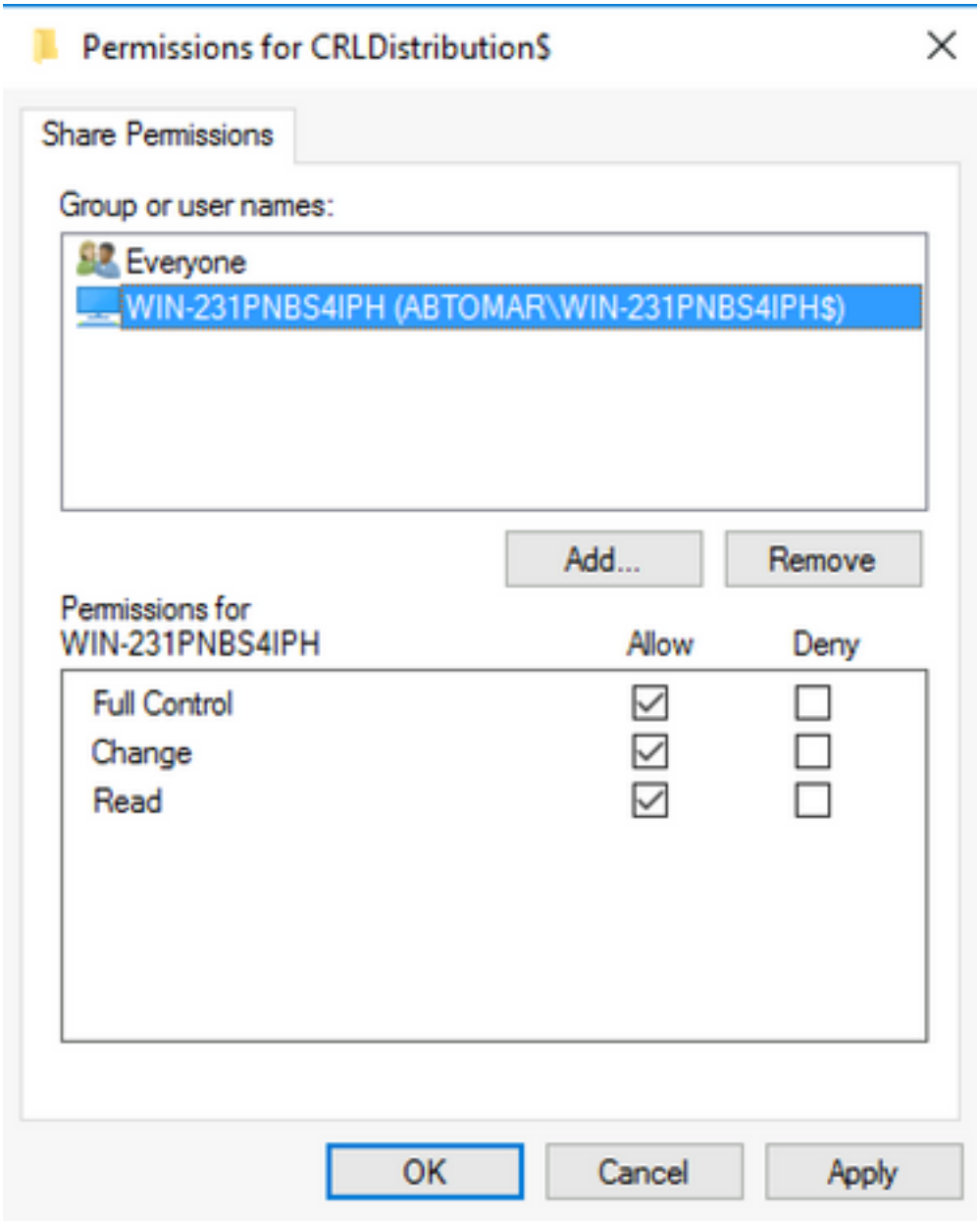


5. Klik op **OK** om terug te keren naar het venster Gebruikers, computers, servicerekeningen of groepen. In het veld Voer de doelnamen in om een veld te selecteren, typt u de computernaam van de CA-server in dit voorbeeld: WIN0231PNBS4IPH en klik op **Naam controleren**. Als de ingevoerde naam geldig is, wordt de naam vernieuwd en onderstreept. Klik op **OK**.

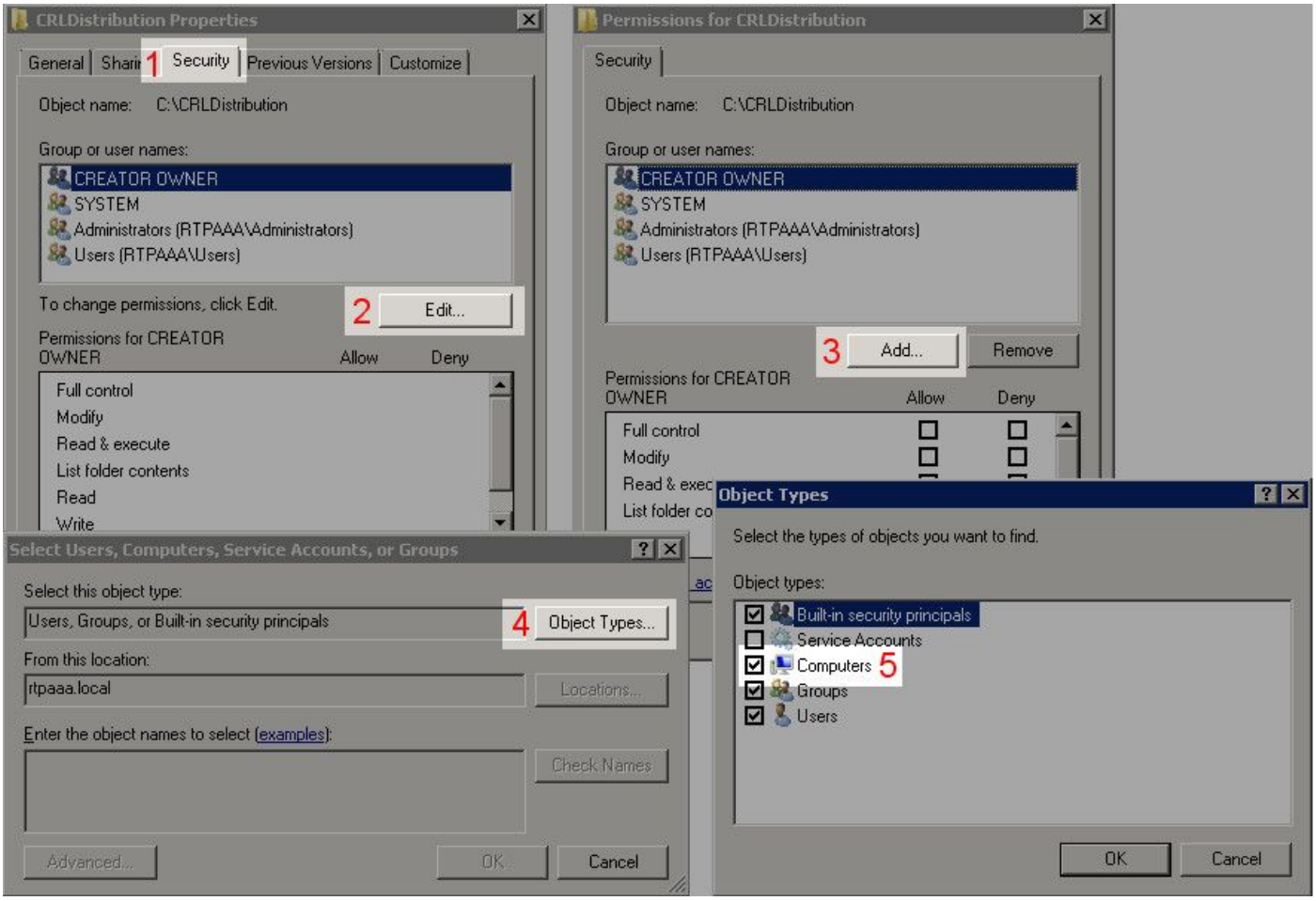


6. Kies de CA-computer in het veld Groep of gebruikersnamen. Controleer **toestaan** dat volledige controle volledige toegang tot de CA verleent.

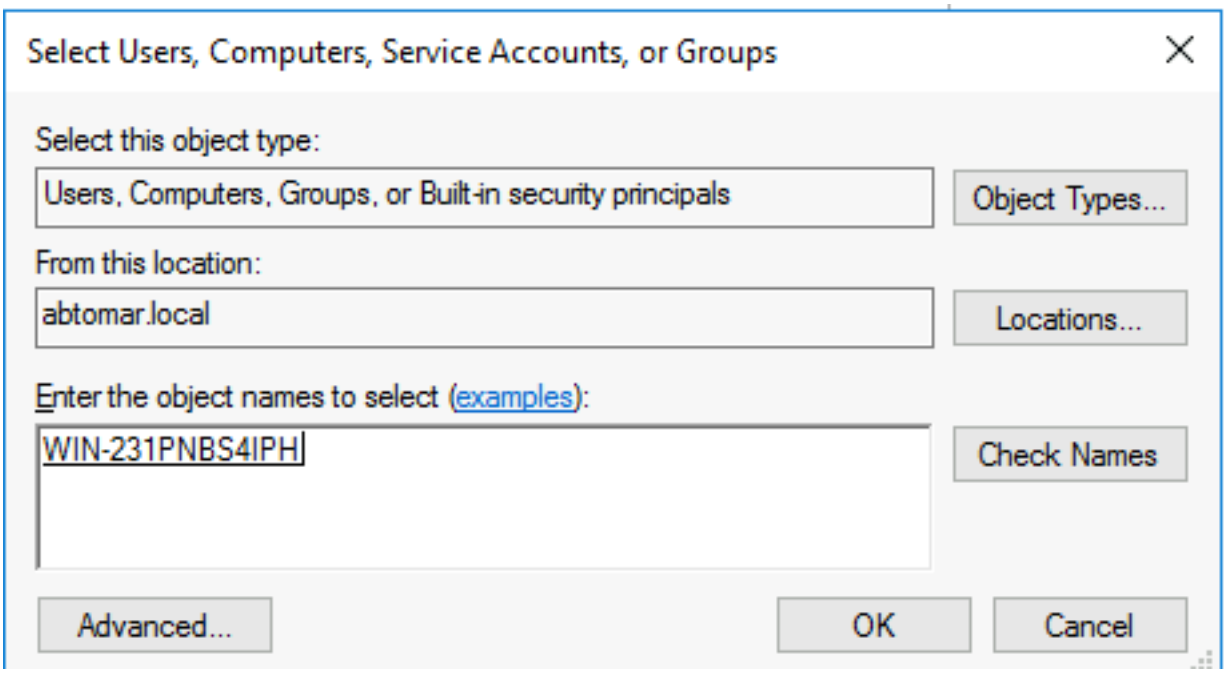
Klik op **OK**. Klik nogmaals op **OK** om het venster Geavanceerd delen te sluiten en naar het venster Eigenschappen terug te keren.



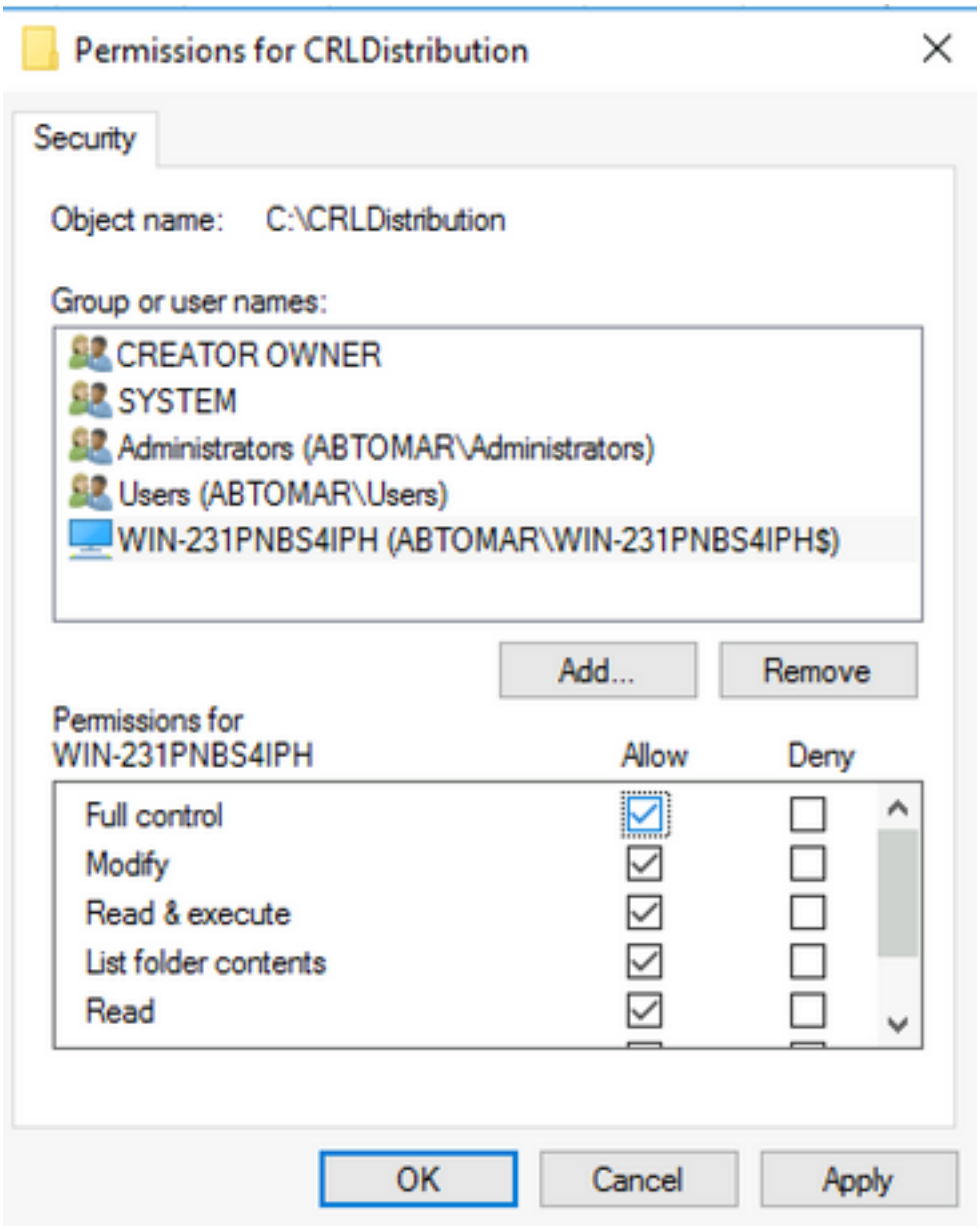
7. Om de CA in staat te stellen de CRL bestanden naar de nieuwe map te schrijven, moet u de juiste beveiligingsrechten configureren. Klik op het tabblad **Beveiliging** (1), klik op **Bewerken** (2), klik op **Add** (3), klik op **Objecttypen** (4) en controleer **het vakje Computers (5).**



8. Typ in het veld Voer de objectnamen in om het veld te selecteren, voer de computernaam van de CA-server in en klik op **Namen controleren**. Als de ingevoerde naam geldig is, wordt de naam vernieuwd en onderstreept. Klik op **OK**.



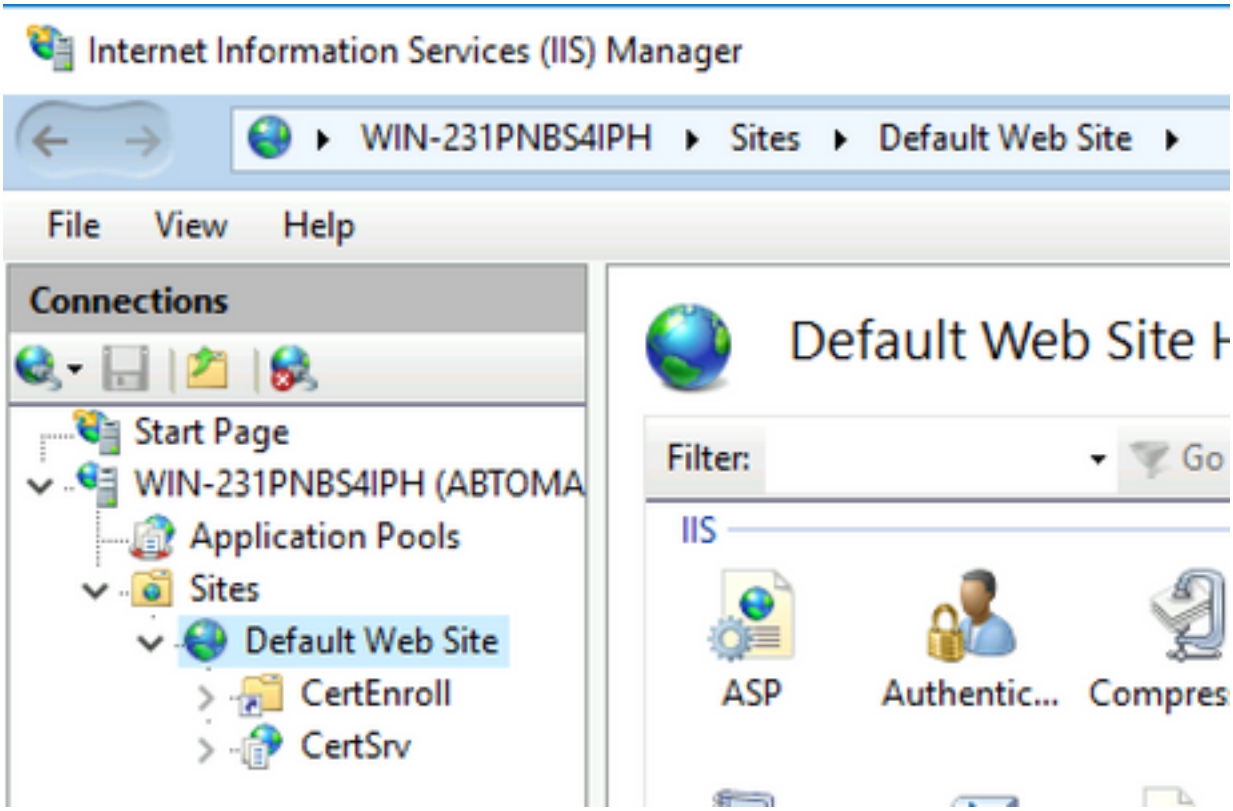
9. Kies de CA-computer in het veld Groep of gebruikersnamen en controleer vervolgens om volledige controle **mogelijk** te maken om volledige toegang tot de CA te verlenen. Klik op **OK** en vervolgens op **Sluiten** om de taak te voltooien.



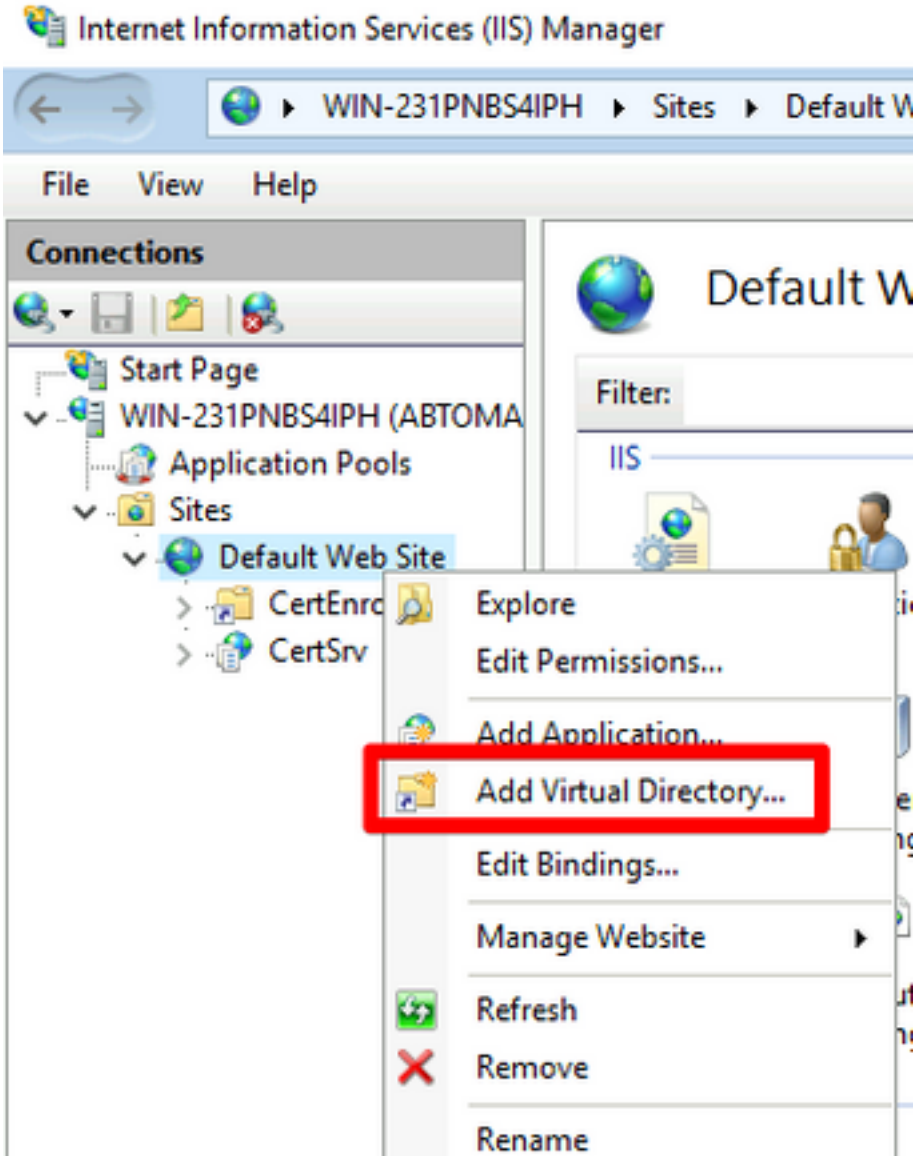
Een website in IS maken om het nieuwe CRL-distributiepoint te tonen

Maak de map waarin de CRL-bestanden zich bevinden toegankelijk via ISE zodat ISE toegang kan krijgen tot de CRL-bestanden.

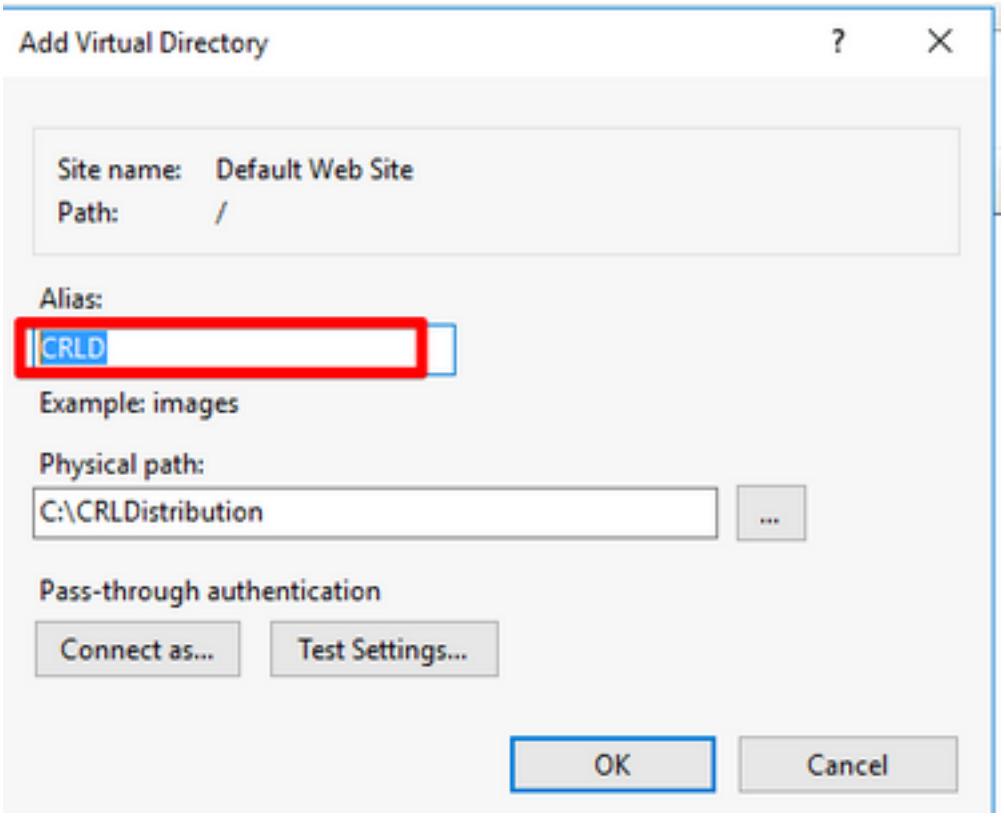
1. Klik in de taakbalk van de Iis-server op **Start**. Kies **Administratieve tools > Internet Information Services (IS) Manager**.
2. In het linker deelvenster (bekend als de Console Tree) vouwt u de naam van de IIS-server uit en vouwt u vervolgens **locaties** uit.



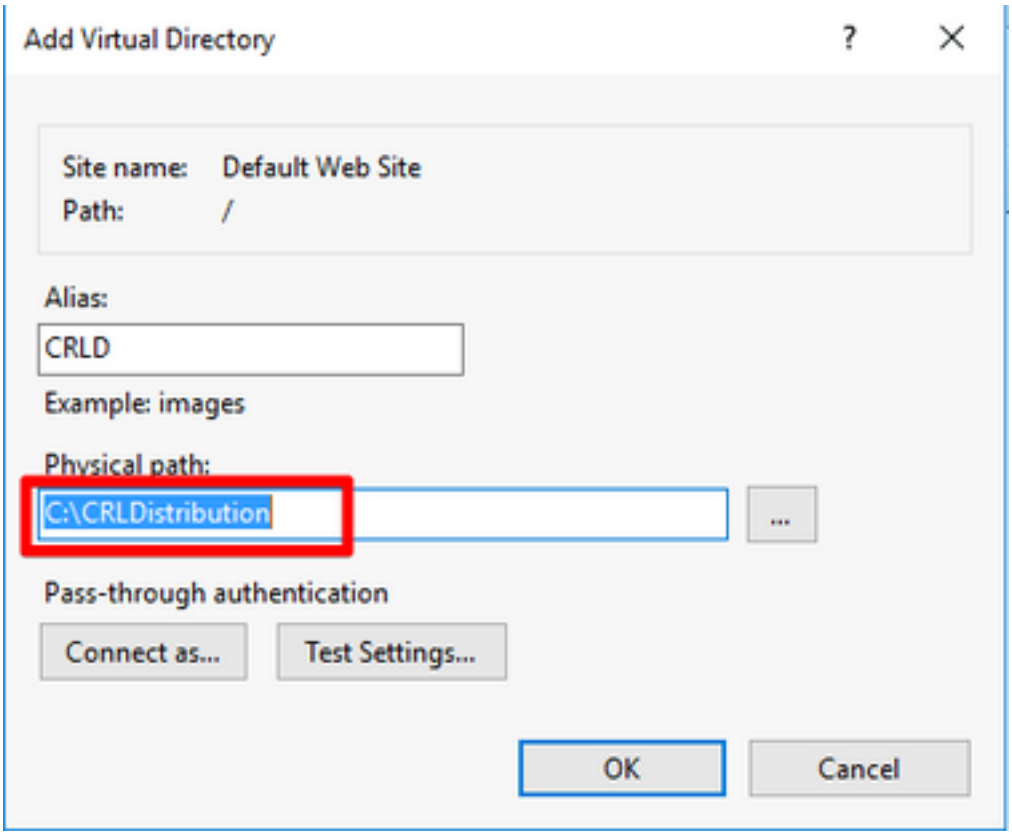
3. Klik met de rechtermuisknop op **Standaardwebsite** en kies **Virtuele map toevoegen** zoals in deze afbeelding.



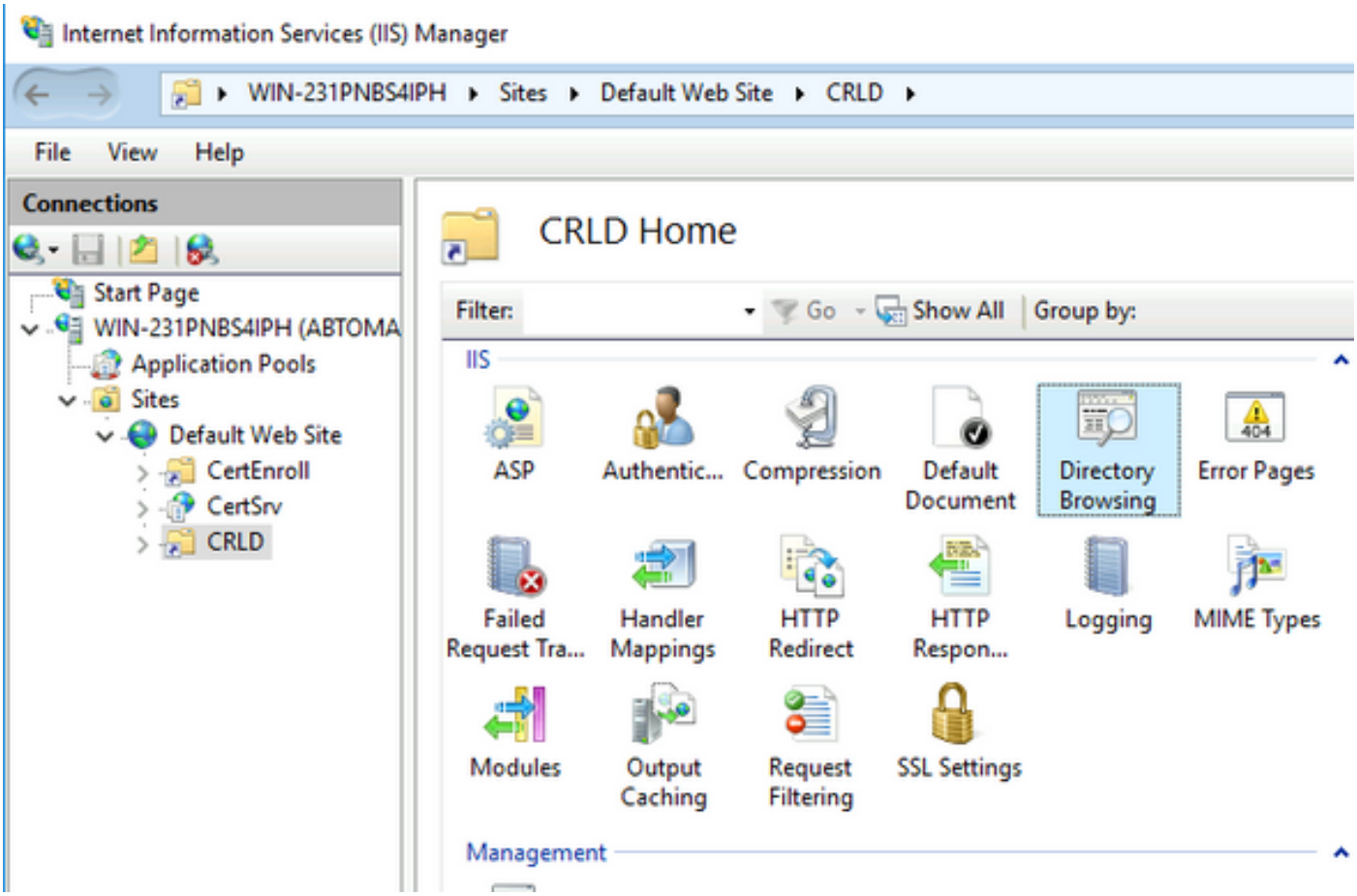
4. Voer in het veld Alias een achternaam in voor het CRL Distribution Point. In dit voorbeeld wordt CRLD ingevoerd.



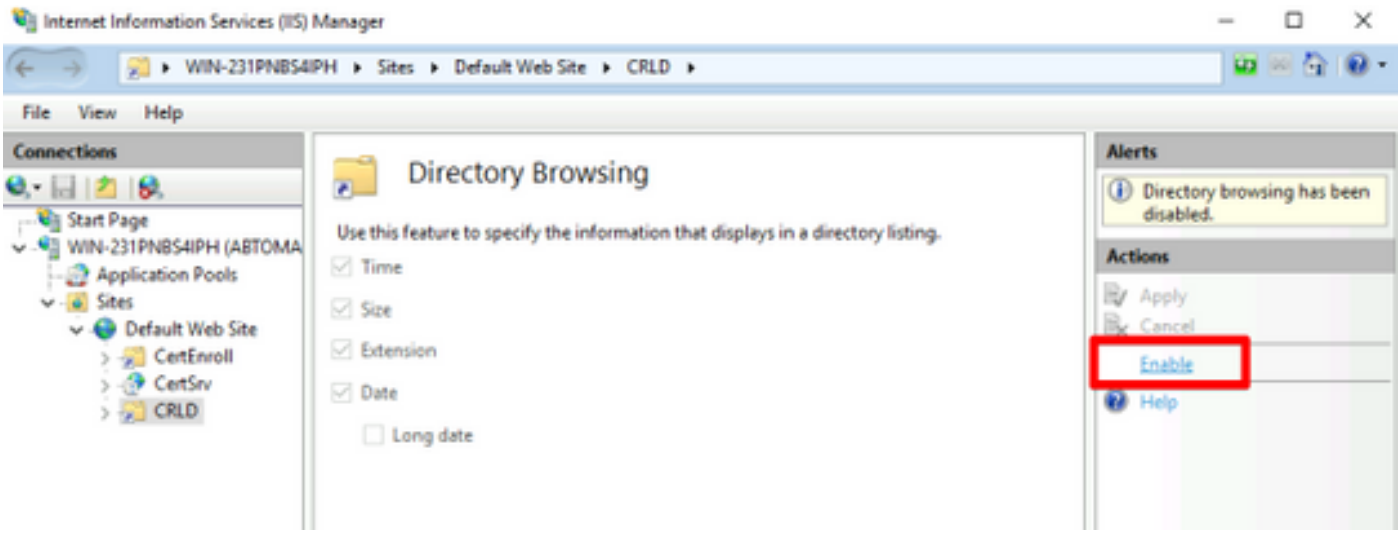
5. Klik op de ellips (..) . .) rechts van het veld Fysiek pad en blader naar de map die in sectie 1 is gemaakt. Selecteer de map en klik op **OK**. Klik op **OK** om het venster Add Virtual Directory te sluiten.



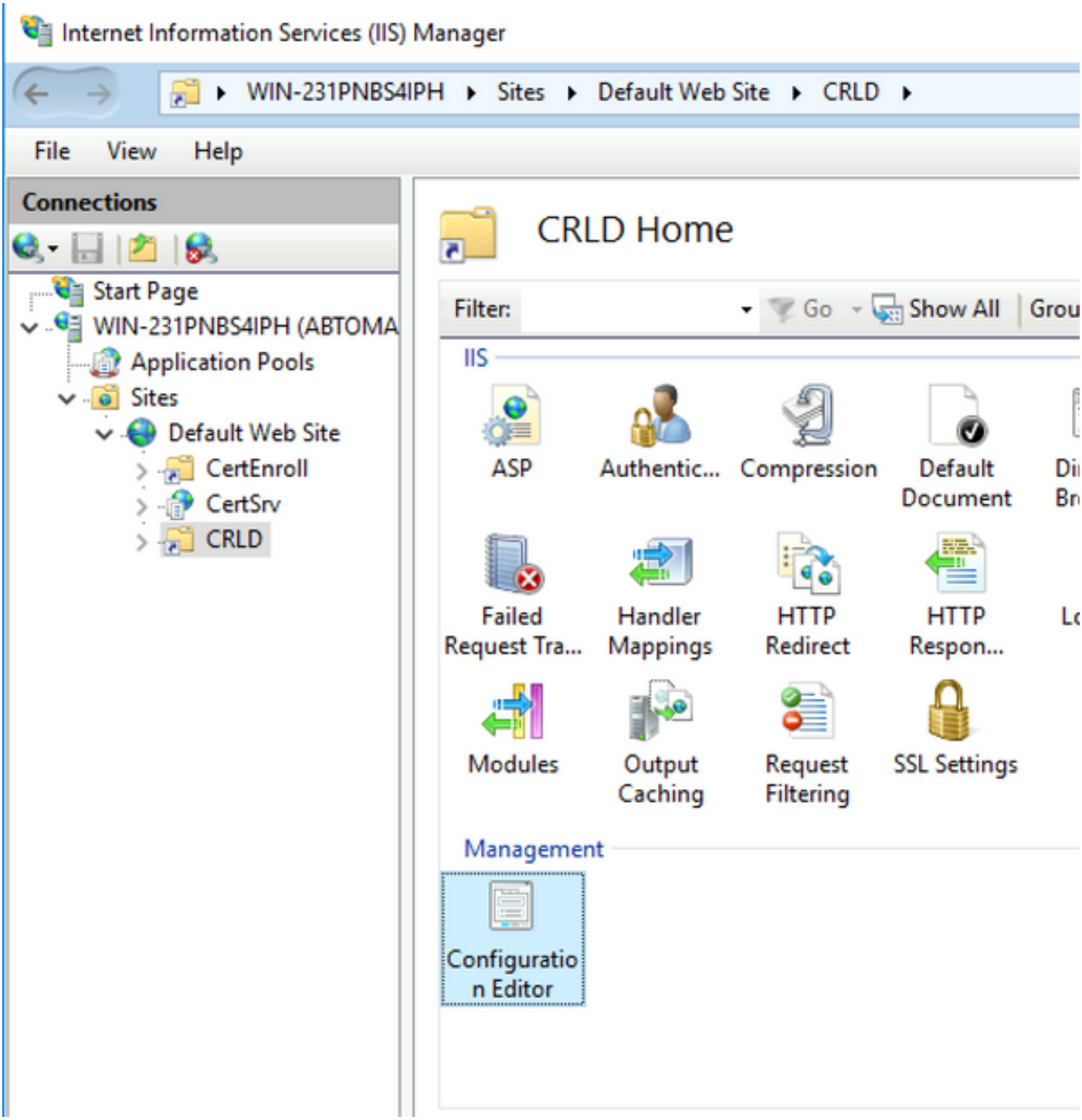
6. De in stap 4 ingevoerde gebiedsnaam moet in het linker deelvenster worden gemarkeerd. Zo niet, kies dan nu. Dubbelklik in het midden op **Directory Browsing**.



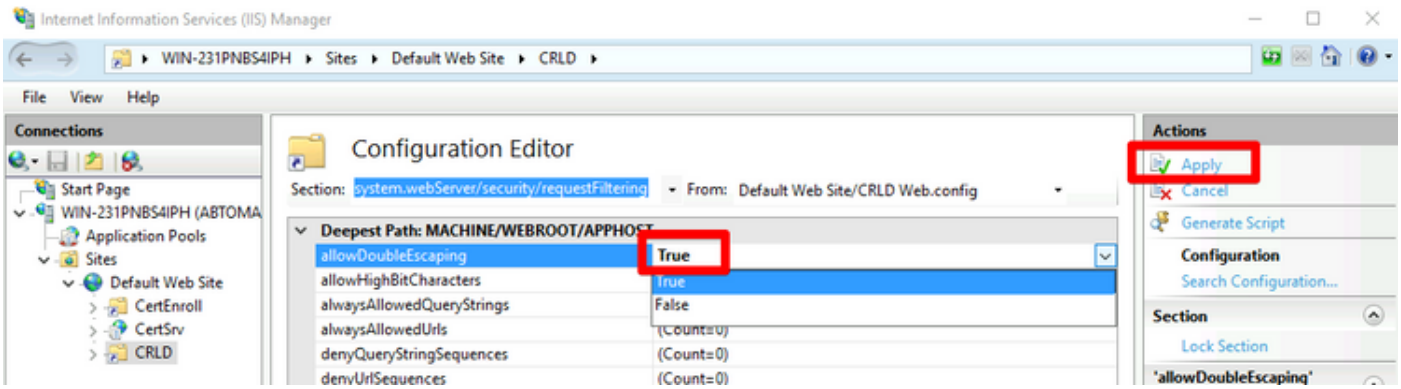
7. Klik in het rechter venster op **Schakel** het bladeren door directory in.



8. Kies in het linker deelvenster de naam van de site opnieuw. Dubbelklik in het midden op **de Configuration Editor**.



9. Selecteer in de vervolgkeuzelijst Sectie **system.webServer/security/requestFiltering**. Selecteer **True** in de vervolgkeuzelijst **allowDubbelscherm** en kies **True**. Klik in het rechtervenster op **Toepassen**, zoals in deze afbeelding.

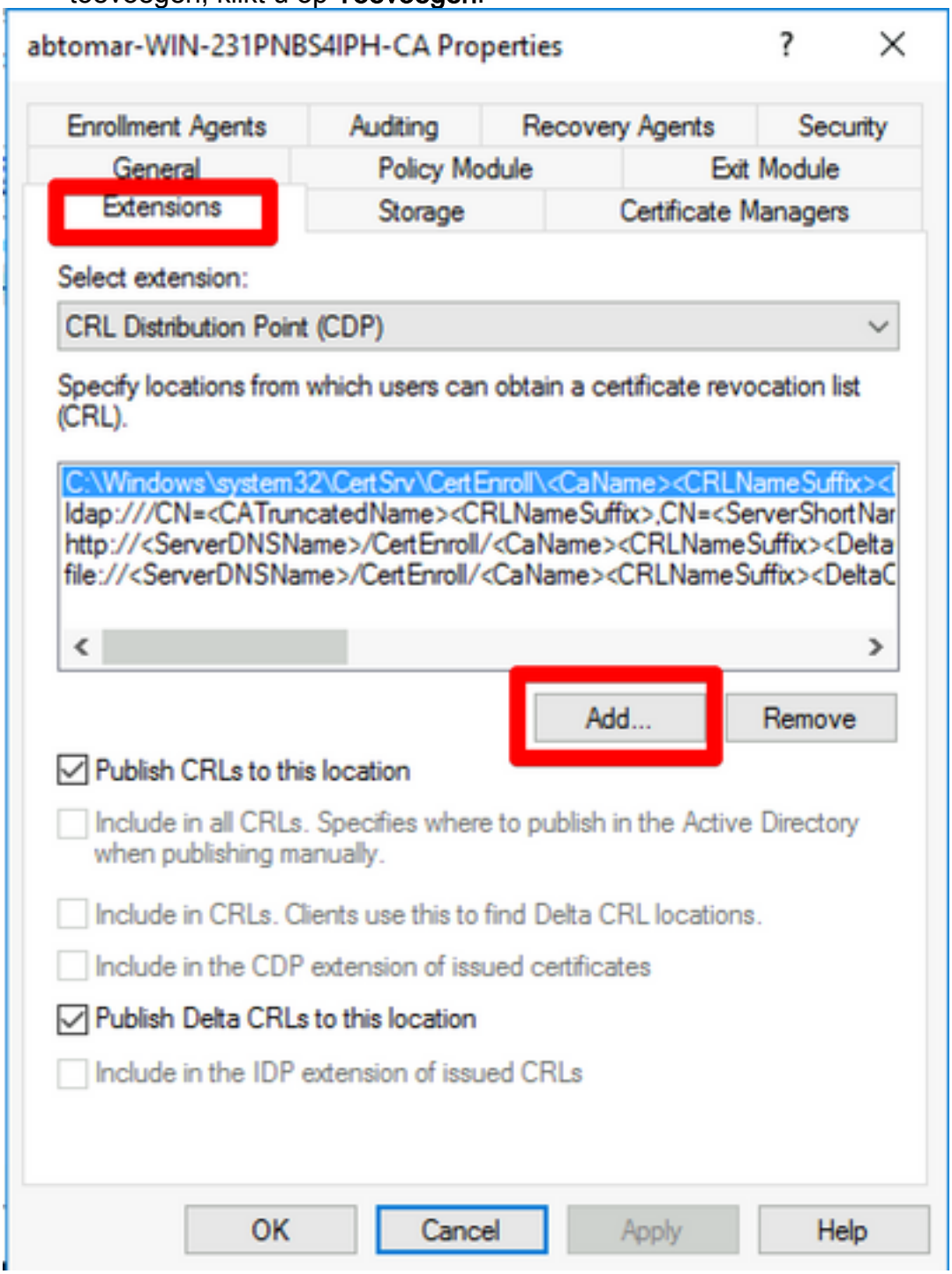


De map moet nu toegankelijk zijn via IS.

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

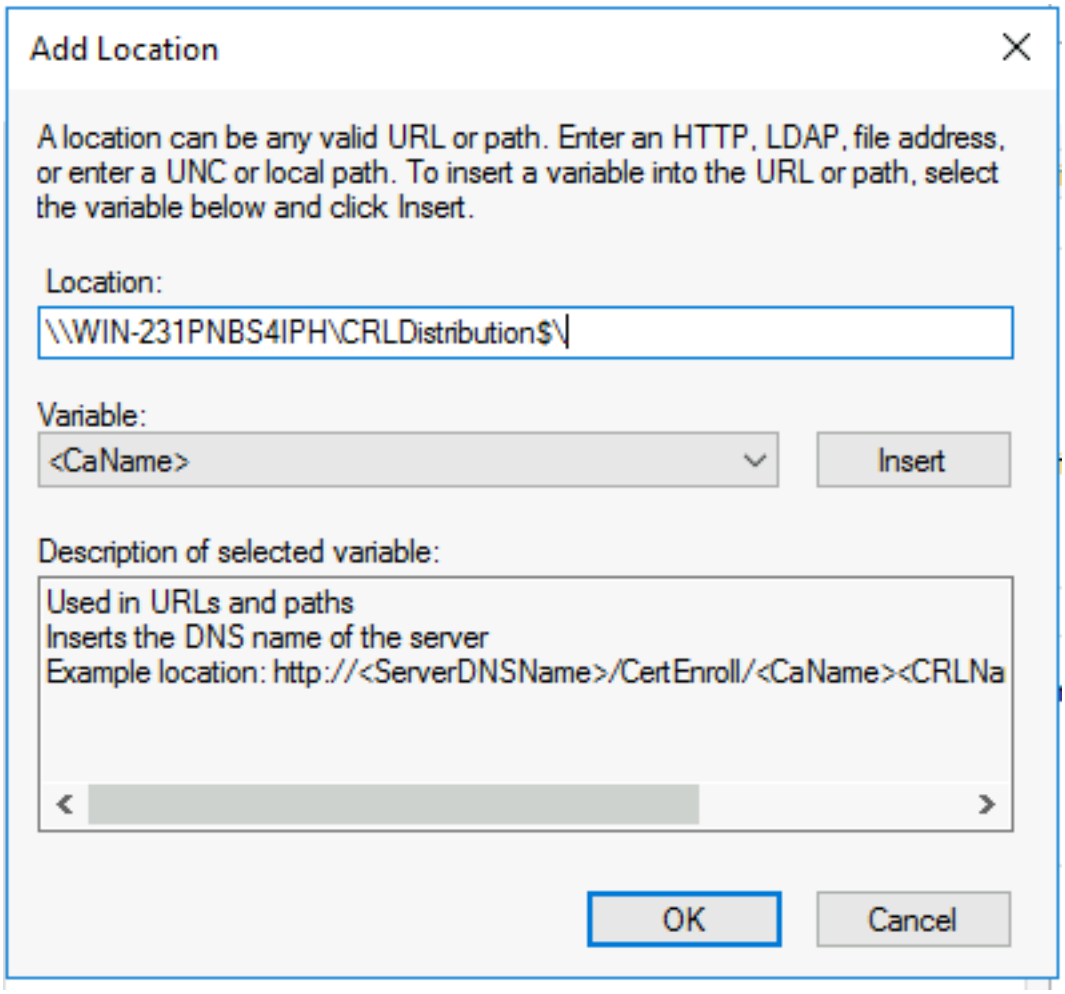
Nu een nieuwe map is ingesteld om de CRL-bestanden te huisvesten en de map is blootgesteld in IS, moet u de Microsoft CA-server configureren om de CRL-bestanden naar de nieuwe locatie te publiceren.

1. Klik in de taakbalk van de CA-server op **Start**. Kies **administratieve hulpmiddelen > certificaatinstantie**.
2. Klik in het linker deelvenster met de rechtermuisknop op de CA-naam. Kies **Eigenschappen** en klik vervolgens op het tabblad **Uitbreidingen**. Als u een nieuw CRL-distributiepunt wilt toevoegen, klikt u op **Toevoegen**.

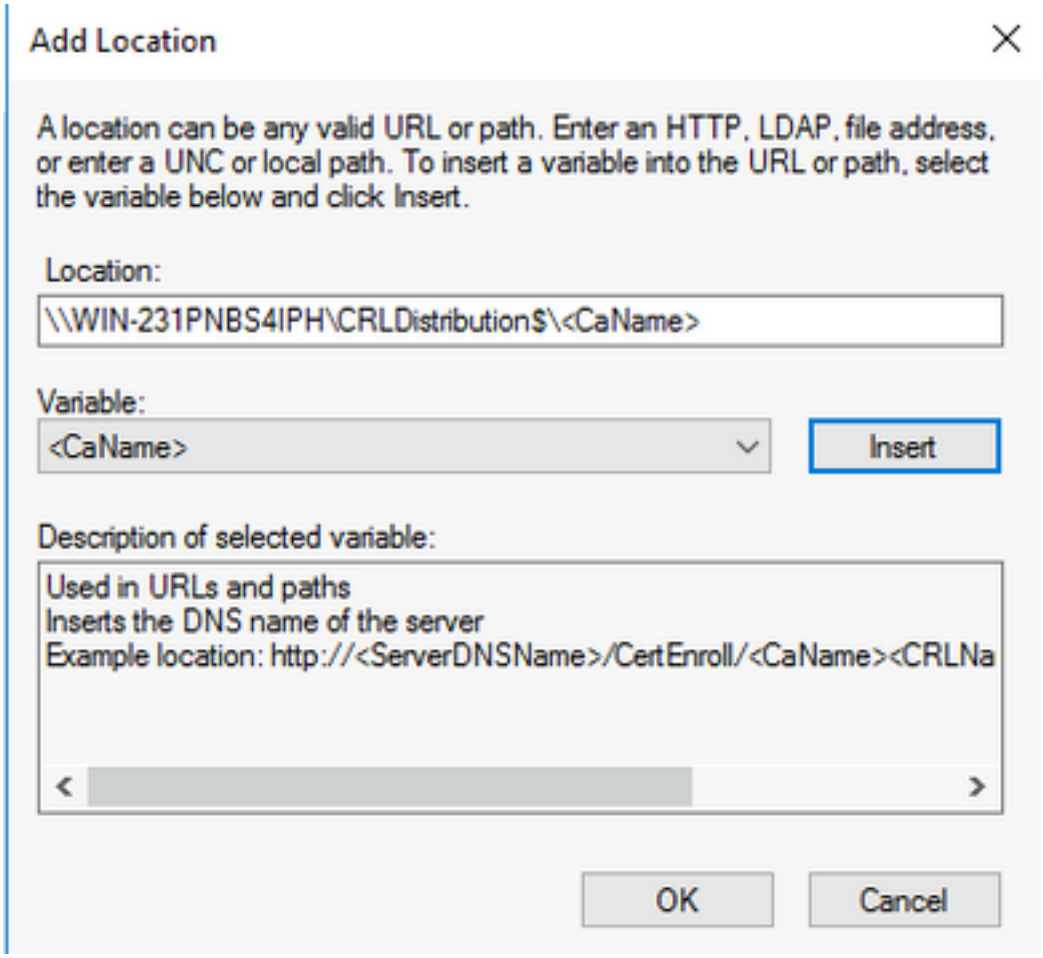


3. In het veld Locatie specificeert u het pad naar de map die in sectie 1 is gemaakt en gedeeld. In het voorbeeld in sectie 1 is het pad:

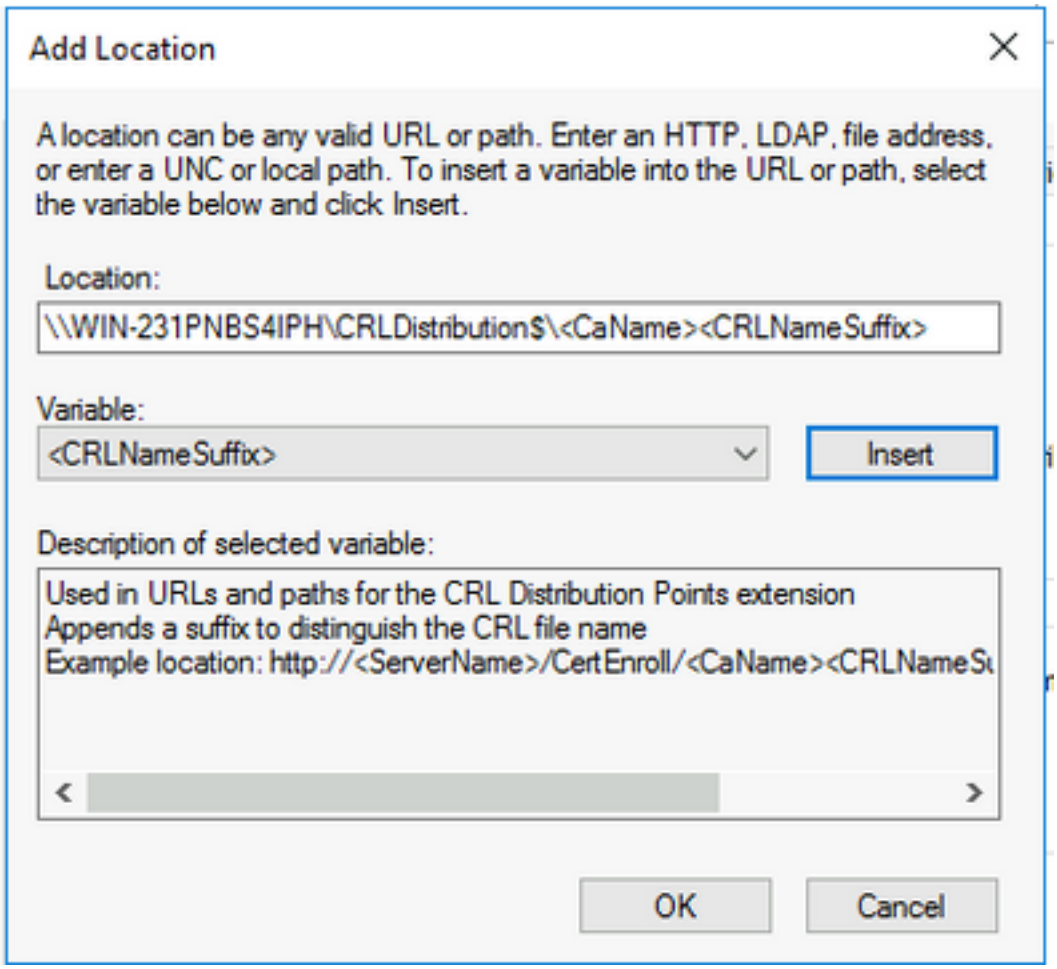
\\WIN-231PNBS4IPH\CRLDistribution$



4. Kies **<CaName>** in het veld Locatie, uit de vervolgkeuzelijst Variabele en klik vervolgens op **Invoegen.**

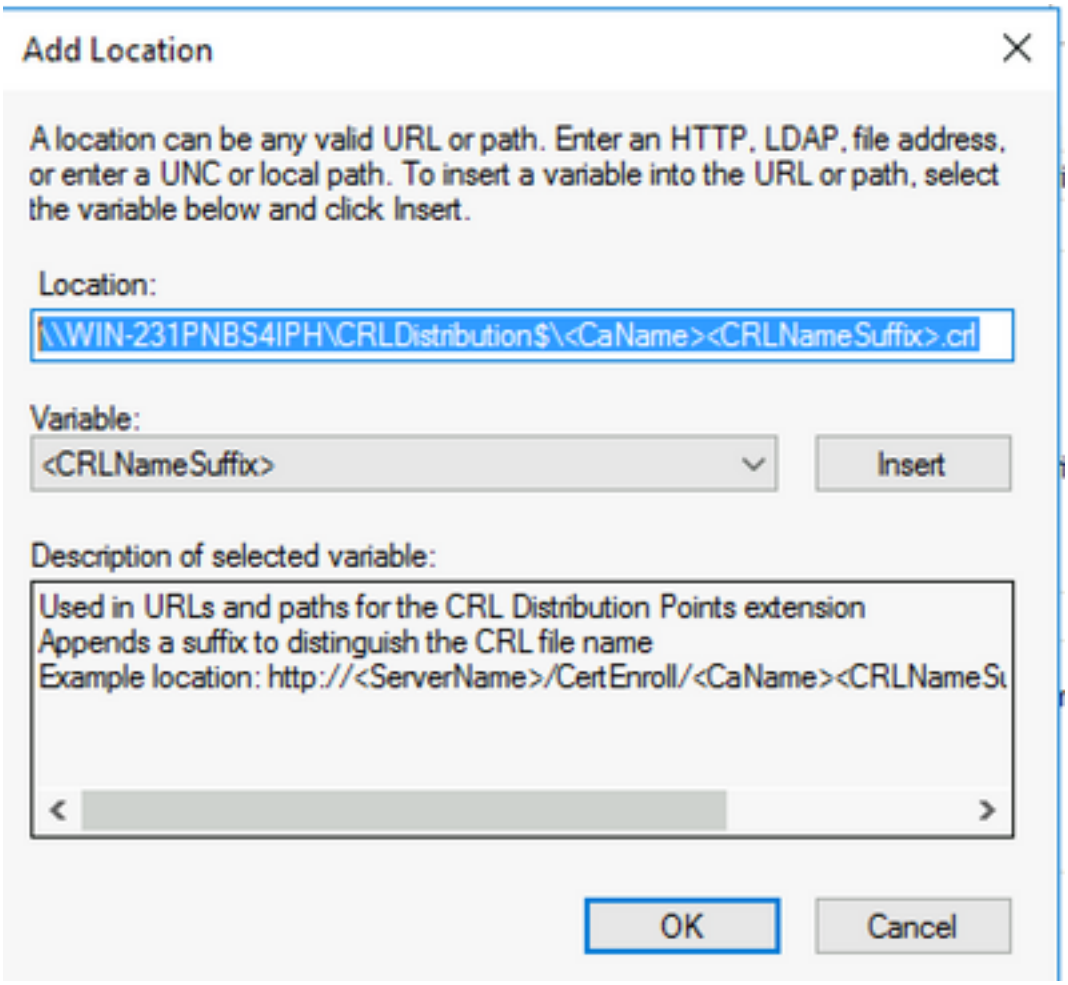


5. Selecteer in de vervolgkeuzelijst Variabele de optie **<CRNameSuffix>** en klik vervolgens op **Invoegen**.



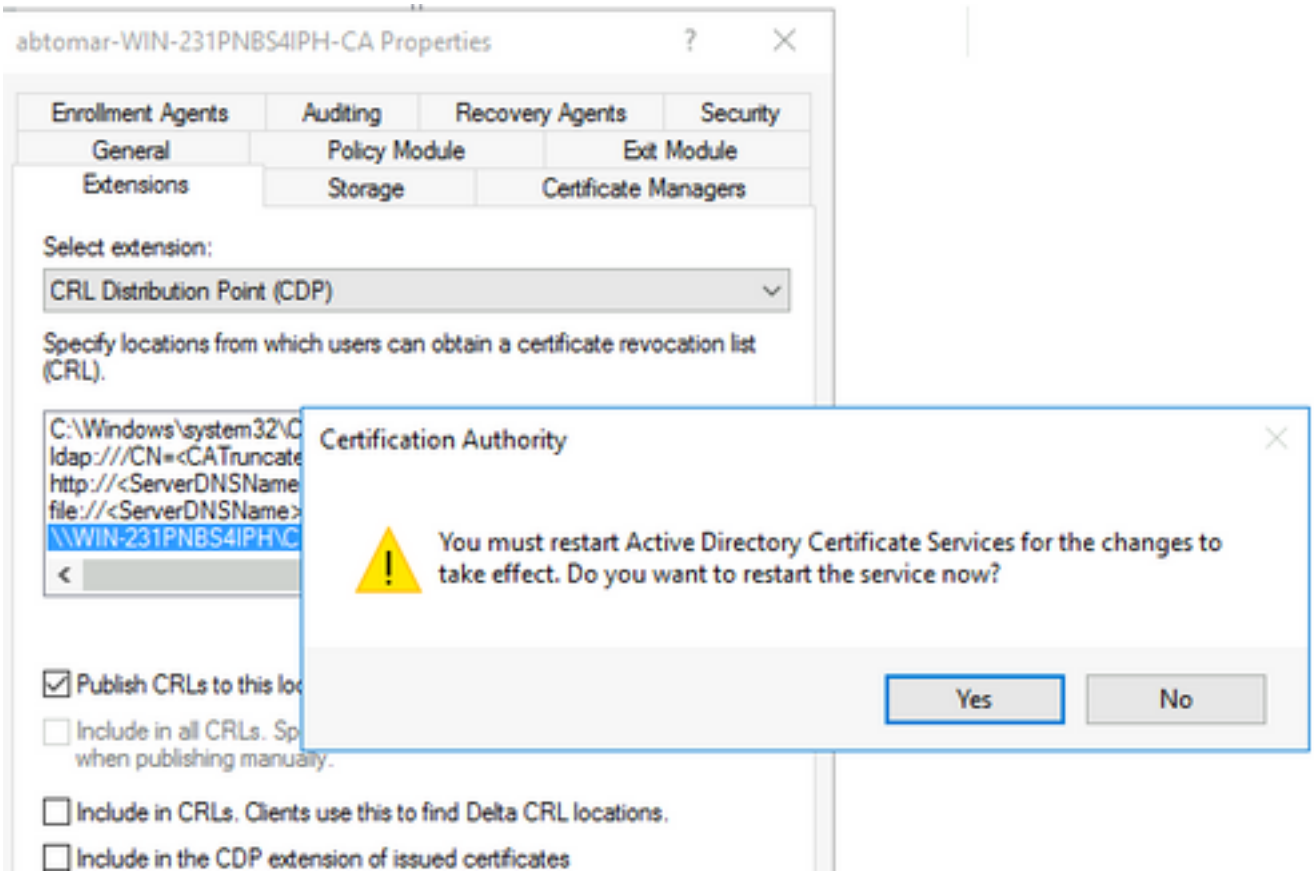
6. In het veld Locatie voegt u **.crl** toe aan het einde van het pad. In dit voorbeeld is de Locatie:

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

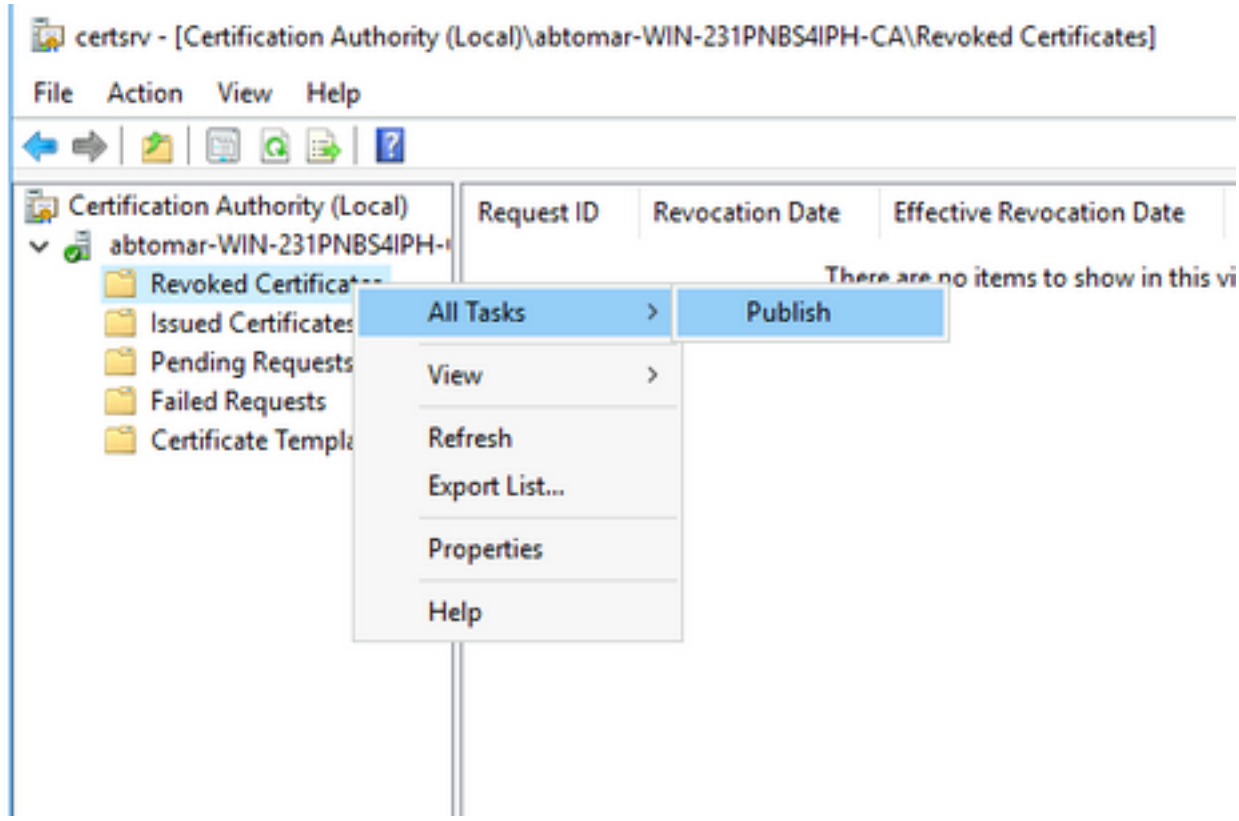


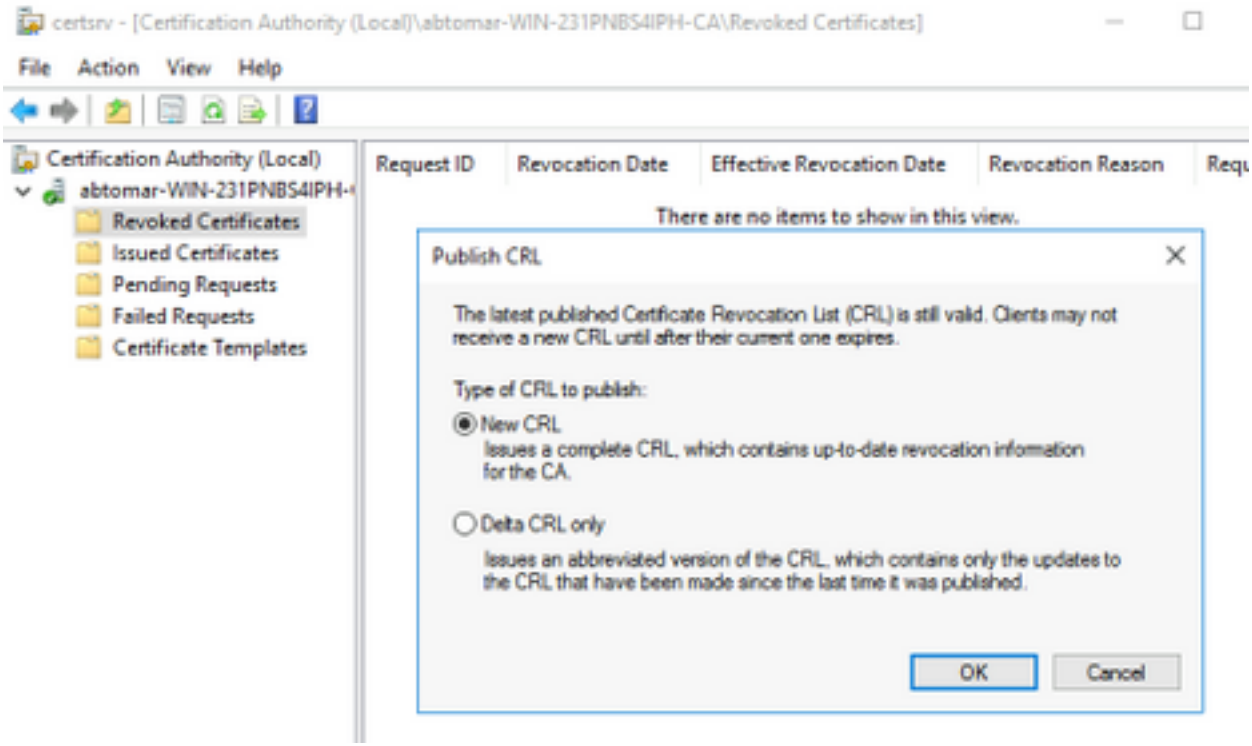
7. Klik op **OK** om naar het tabblad Uitbreidingen terug te keren. Controleer de optie **CRLs op deze locatie** publiceren en klik vervolgens op **OK** om het venster Properties te sluiten.

Er verschijnt een melding voor toestemming om de Active Directory certificaatservices opnieuw in te voeren. Klik op **Ja**.



8. Klik in het linker venster met de rechtermuisknop op **ingetrokken certificaten**. Kies **Alle taken > Publiceren**. Zorg ervoor dat Nieuw CRL is geselecteerd en klik vervolgens op **OK.**





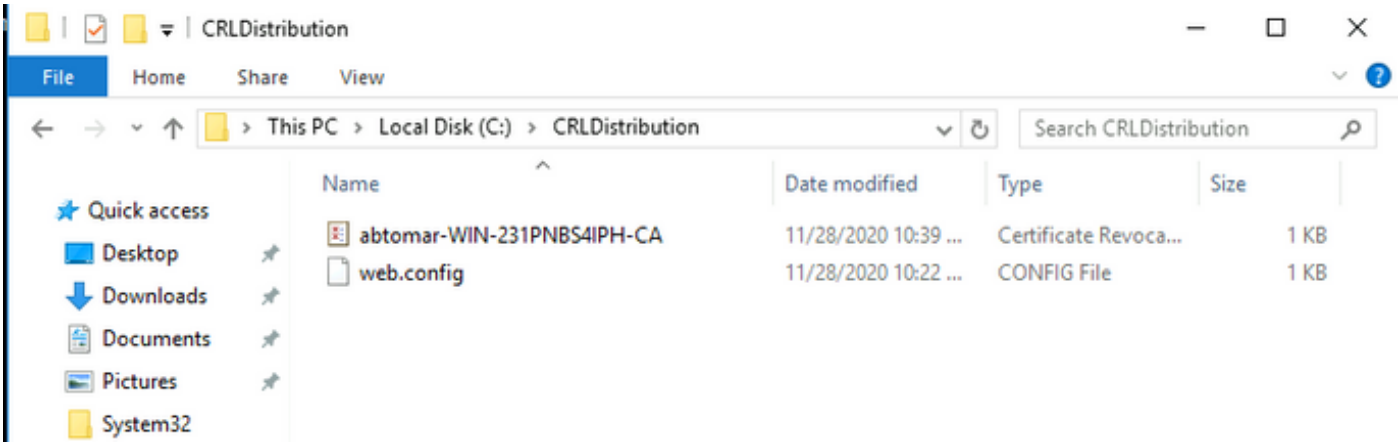
De Microsoft CA-server moet een nieuw .crl-bestand maken in de map die in sectie 1 is gemaakt. Als het nieuwe CRL-bestand met succes is gemaakt, wordt er geen dialoogvenster geopend nadat op OK is gedrukt. Als er een fout wordt teruggegeven in de map van het nieuwe distributiepunt, herhaalt u elke stap in dit gedeelte zorgvuldig.

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

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

1. Open de map die in sectie 1 is gemaakt op de IIS-server. Er moet één .crl-bestand aanwezig zijn met het formulier **<CANAME>.crl** waar <CANAME> de naam van de CA-server is. In dit voorbeeld is filename:

abtoar-WIN-231PNBS4IPH-CA.crl



2. Open een webbrowser van een werkstation op het netwerk (idealiter op hetzelfde netwerk als het ISE-primaire Admin-knooppunt) en blader naar http://<SERVER>/<CRLSITE> waarin <SERVER> de servernaam van de IIS-server is die in sectie 2 is geconfigureerd en <CRLSITE> de achternaam is die voor het distributiepunt in sectie 2 is gekozen. In dit voorbeeld is de URL:

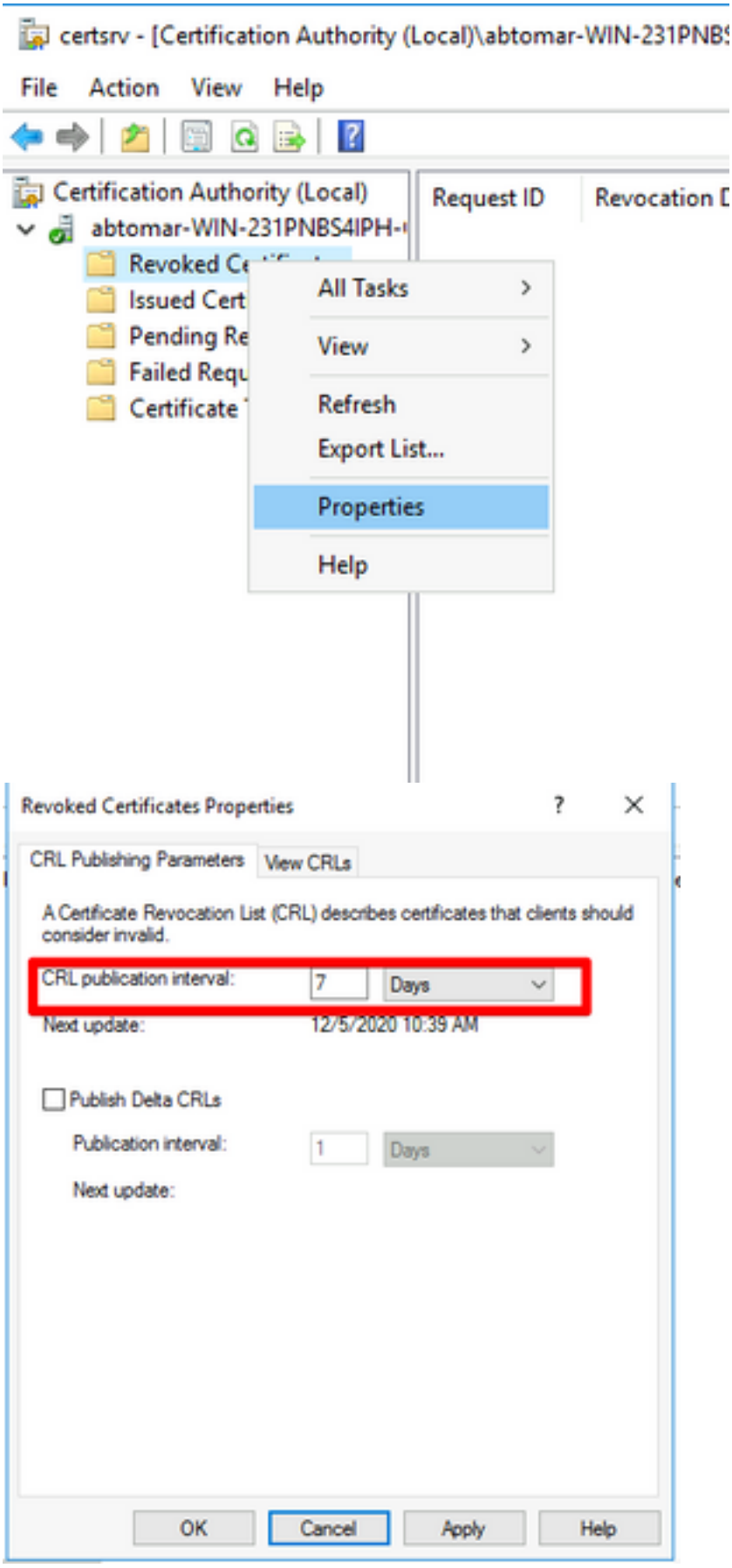
http://win-231pnbs4iph/CRLD

De directory index wordt weergegeven, met inbegrip van het bestand dat in stap 1 is waargenomen.

ISE configureren voor gebruik van het nieuwe CRL-distributiepoint

Voordat ISE wordt geconfigureerd om het CRL terug te halen, moet u het interval definiëren om het CRL te publiceren. De strategie om deze tussenpozen vast te stellen valt buiten het toepassingsgebied van dit document. De potentiële waarden (in Microsoft CA) zijn 1 uur tot 411 jaar, inclusief. De standaardwaarde is 1 week. Zodra een geschikte interval voor uw omgeving is vastgesteld, dient u het interval met deze instructies in te stellen:

1. Klik in de taakbalk van de CA-server op **Start**. Kies **administratieve hulpmiddelen > certificaatinstantie**.
2. Vouw in het linker deelvenster de CA uit. Klik met de rechtermuisknop op de map **Ingetrokken certificaten** en kies **Eigenschappen.**
3. Voer in de velden met 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 wordt een publicatieinterval van 7 dagen ingesteld.



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

Uitvoer van voorbeeld:

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

5. Voer de **certutil-getreg CA\CRLov*** opdracht in om te controleren of de CRLOverlapPeriod handmatig is ingesteld. Standaard is de waarde voor CRLOverlapUnit 0, wat aangeeft dat er geen handmatige waarde is ingesteld. Indien de waarde een andere waarde is dan 0, registreert u de waarde en de eenheden.

Uitvoer van voorbeeld:

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

6. Voer de opdracht certutil -getreg CA\CRLpe* in om de CRLPsperiode te controleren, die in stap 3 was ingesteld.

Uitvoer van voorbeeld:

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

7. Bereken de CRL-Grace-periode als volgt:

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

Elders: OVERLAP = (CRLP-periode / 10), in minuten

b. Bij OVERLAP > 720 dan overLAP = 720

c. Als overLAP < (1,5 * KloktijdSkewMinutes) is overLAP = (1,5 * ClockSkewMinutes)

d. Indien overLAP > CRLPeriod, in minuten, dan overLAP = CRLPd in minuten

e. Grace Period = OVERLAP + ClockSkewMinutes

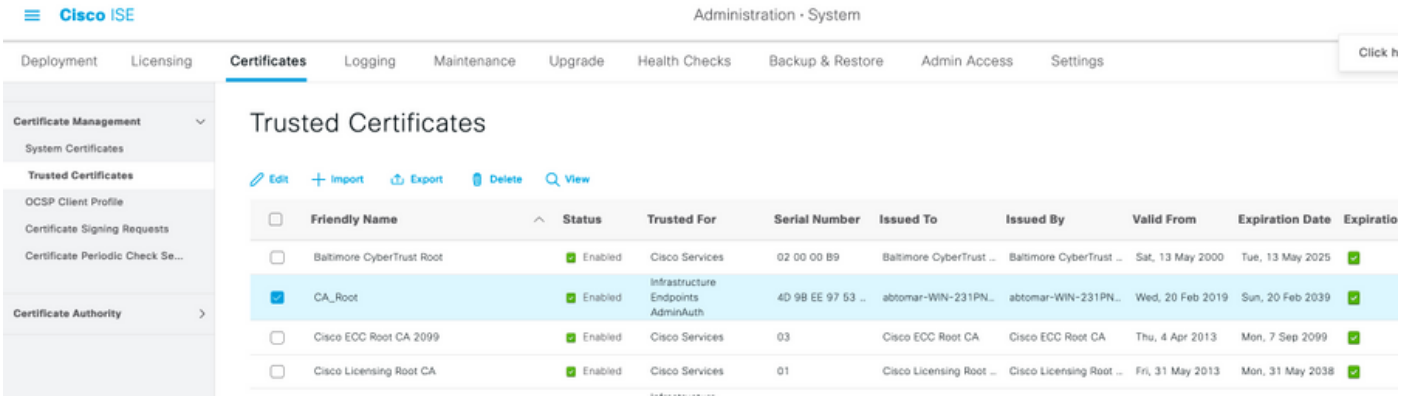
```
Example:

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
```

De berekende aflossingsvrije periode is de tijd tussen het tijdstip waarop de CA het volgende CRL publiceert en het tijdstip waarop het huidige CRL afloopt. ISE moet worden geconfigureerd om de CRL's dienovereenkomstig te herstellen.

8. Meld u aan bij het ISE Primaire Admin-knooppunt en kies **Beheer > Systeem > Certificaten**.

Selecteer in het linker deelvenster de optie **Trusted-certificaat**



9. Controleer het aankruisvakje naast het CA-certificaat waarvoor u CRL's wilt configureren. Klik op **Edit** (Bewerken).

10. Controleer onder in het venster het vakje **Download CRL**.

1. In het veld CRL Distribution URL specificeert u het pad naar het CRL Distribution Point, 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

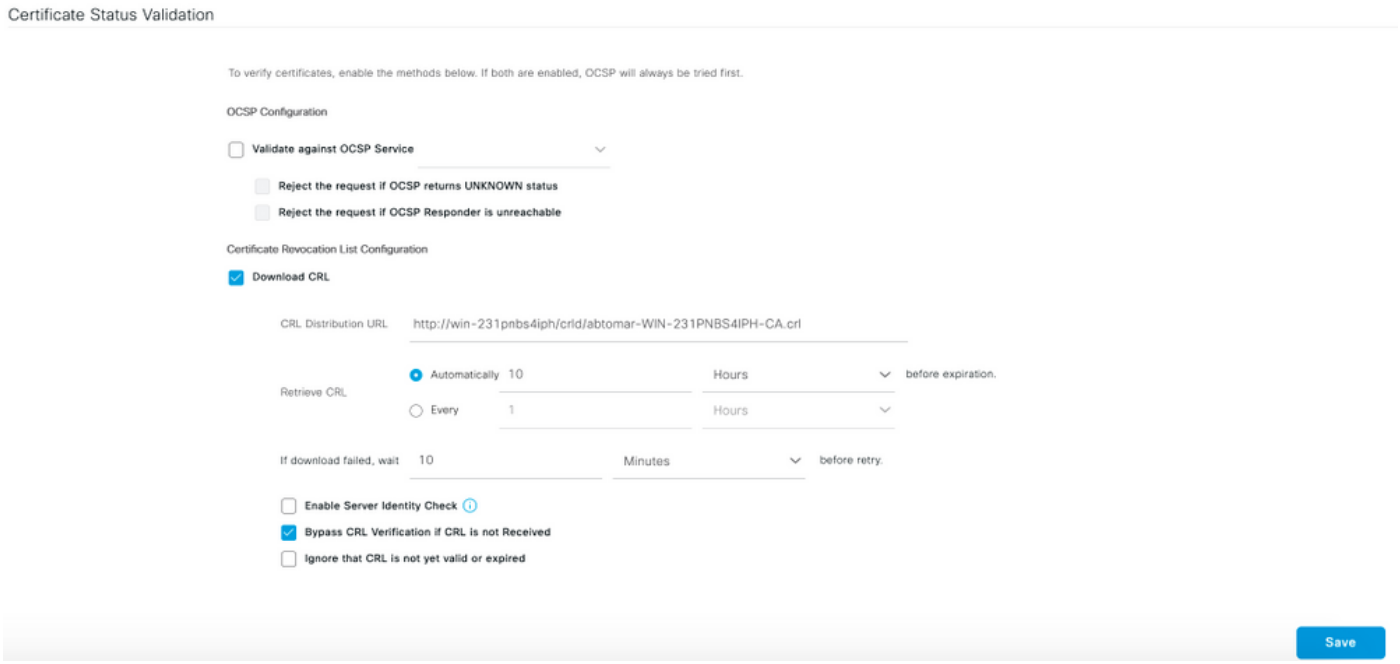
12. ISE kan worden ingesteld om het CRL met regelmatige tussenpozen terug te halen of op basis van de verloopdatum (die in het algemeen ook een regelmatig interval is). Wanneer het CRL publicatieinterval statisch is, worden tijdigere CRL-updates verkregen wanneer de laatste optie wordt gebruikt. Klik op de knop **Automatisch** selecteren.

13. Stel de waarde voor herwinning in op een waarde die lager is dan de aflossingsvrije periode die in stap 7 is berekend. Als de ingestelde waarde langer is dan de aflossingsvrije periode, controleert ISE het CRL-distributiepunt voordat de CA het volgende CRL heeft gepubliceerd. In dit voorbeeld wordt de aflossingsvrije periode berekend op 730 minuten, ofwel 12 uur en 10 minuten. Voor het ophalen wordt een waarde van 10 uur gebruikt

14. Stel de interval voor het opnieuw proberen in, afhankelijk van uw omgeving. Als ISE het CRL niet kan herstellen met het ingestelde interval in de vorige stap, zal het opnieuw proberen met dit kortere interval.

15. Controleer de **CRL-verificatie omzeilen indien CRL niet is ontvangen,** aanvinkvakje om op certificaat gebaseerde verificatie normaal te laten verlopen (en zonder een CRL-controle) indien ISE het CRL voor deze CA niet kon terugkrijgen in haar laatste downloadpoging. Als dit aankruisvakje niet is ingeschakeld, zal alle op certificaten gebaseerde echtheidscontrole met door deze CA afgegeven certificaten mislukken als het CRL niet kan worden opgehaald.

16. Controleer **of CRL nog niet geldig is of verlopen** aanvinkvakje om ISE toe te staan verlopen (of nog niet geldig) CRL-bestanden te gebruiken alsof ze geldig zijn. Als dit aanvinkvakje niet is ingeschakeld, beschouwt ISE een CRL als ongeldig vóór hun effectieve datum en na hun volgende update. Klik op **Opslaan** om de configuratie te voltooien.



Cisco interne informatie

1. Microsoft. "Een CRL-distributiepunt voor certificaten configureren." http://technet.microsoft.com/en-us/library/ee649260%28v=ws.10%29.aspx, 7 okt. 2009 [18 dec. 2012]

2. Microsoft. "publiceren de lijst met intrekkingen van certificaat." http://technet.microsoft.com/en-us/library/cc778151%28v=ws.10%29.aspx, 21 januari 2005 [18 dec. 2012]

3. Microsoft. "CRL- en Delta CRL-overlappingsperiodes instellen." http://technet.microsoft.com/en-us/library/cc731104.aspx, 11 april 2011 [18 dec. 2012]

4. MS2065 [MSFT]. "Hoe effectiefDate (deze update), NextUpdate en NextCRLPublish worden berekend." http://blogs.technet.com/b/pki/archive/2008/06/05/how-effectivedate-thisupdate-nextupdate-and-nextcrlpublish-are-calculated.aspx, 4 jun. 2008 [18 dec. 2012]