

Publiceer de lijsten van de intrekking van het certificaat voor ISE in een Configuratievoorbeeld van de Microsoft CA-server

Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Conventies](#)

[Configureren](#)

[Configuraties](#)

[Sectie 1. Maak en vorm een map op de CA om de CRL-bestanden te huisvesten](#)

[Sectie 2. Maak een site in IS om het nieuwe CRL-distributiepoint te onthullen](#)

[Sectie 3. Configuratie van Microsoft CA-server om CRL-bestanden naar het distributiepoint te publiceren](#)

[Sectie 4. Controleer of het CRL-bestand bestaat en is toegankelijk via IS](#)

[Sectie 5. Configureer de ISE om het nieuwe CRL-distributiepoint te gebruiken](#)

[Verifiëren](#)

[Problemen oplossen](#)

[Gerelateerde informatie](#)

Inleiding

Dit document beschrijft de configuratie van een Microsoft certificaatserver (CA) van de Autoriteit die Internet Information Services (IS) beheert om updates van de Revocatielijst van het Certificaat (CRL) te publiceren. Het legt ook uit hoe u Cisco Identity Services Engine (ISE) (versies 1.1 en later) kunt 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 1.1.2.15
- 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 de potentiële impact van elke opdracht begrijpen.

Conventies

Raadpleeg de [Cisco Technical Tips Convention](#) voor meer informatie over documentconventies.

Configureren

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

Opmerking: Gebruik het [Opname Gereedschap](#) (alleen geregistreerde klanten) om meer informatie te verkrijgen over de opdrachten die in deze sectie worden gebruikt.

Configuraties

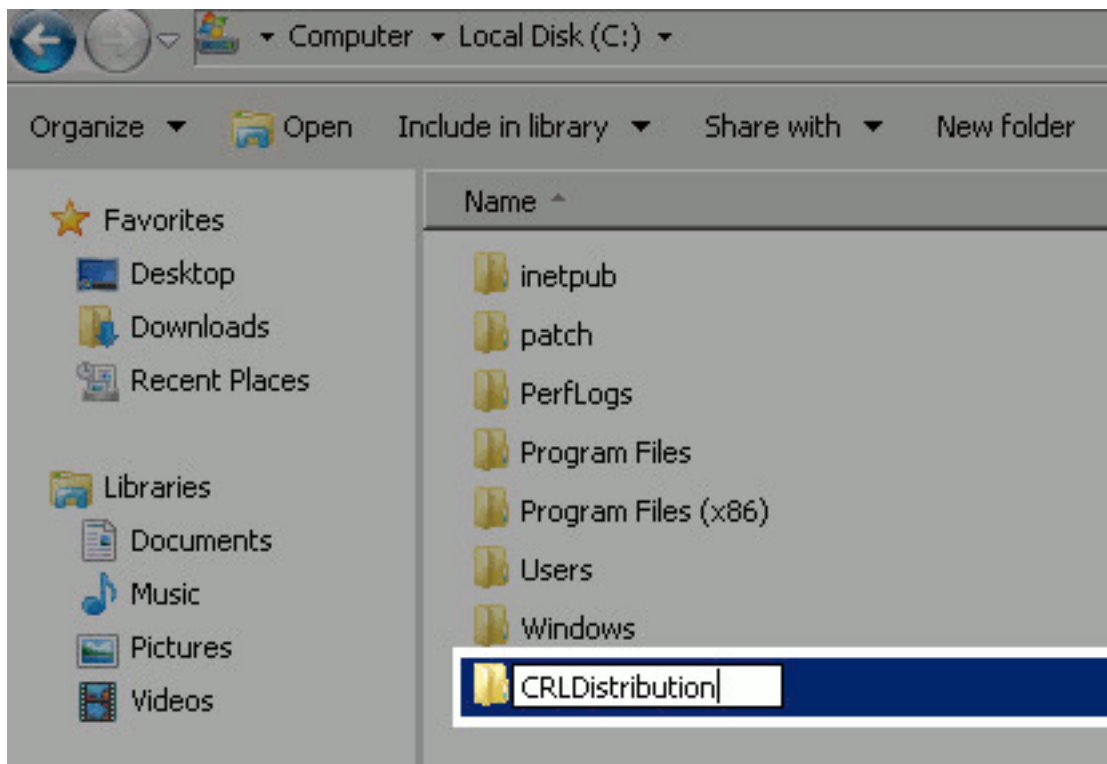
Dit document gebruikt deze configuraties:

- Sectie 1. Maak en vorm een map op de CA om de CRL-bestanden te huisvesten
- Sectie 2. Maak een site in IS om het nieuwe CRL-distributiepunt te onthullen
- Sectie 3. Configuratie van Microsoft CA-server om CRL-bestanden naar het distributiepunt te publiceren
- Sectie 4. Controleer of het CRL-bestand bestaat en is toegankelijk via IS
- Sectie 5. Configureer de ISE om het nieuwe CRL-distributiepunt te gebruiken

Sectie 1. Maak en vorm een map op de CA om de CRL-bestanden te huisvesten

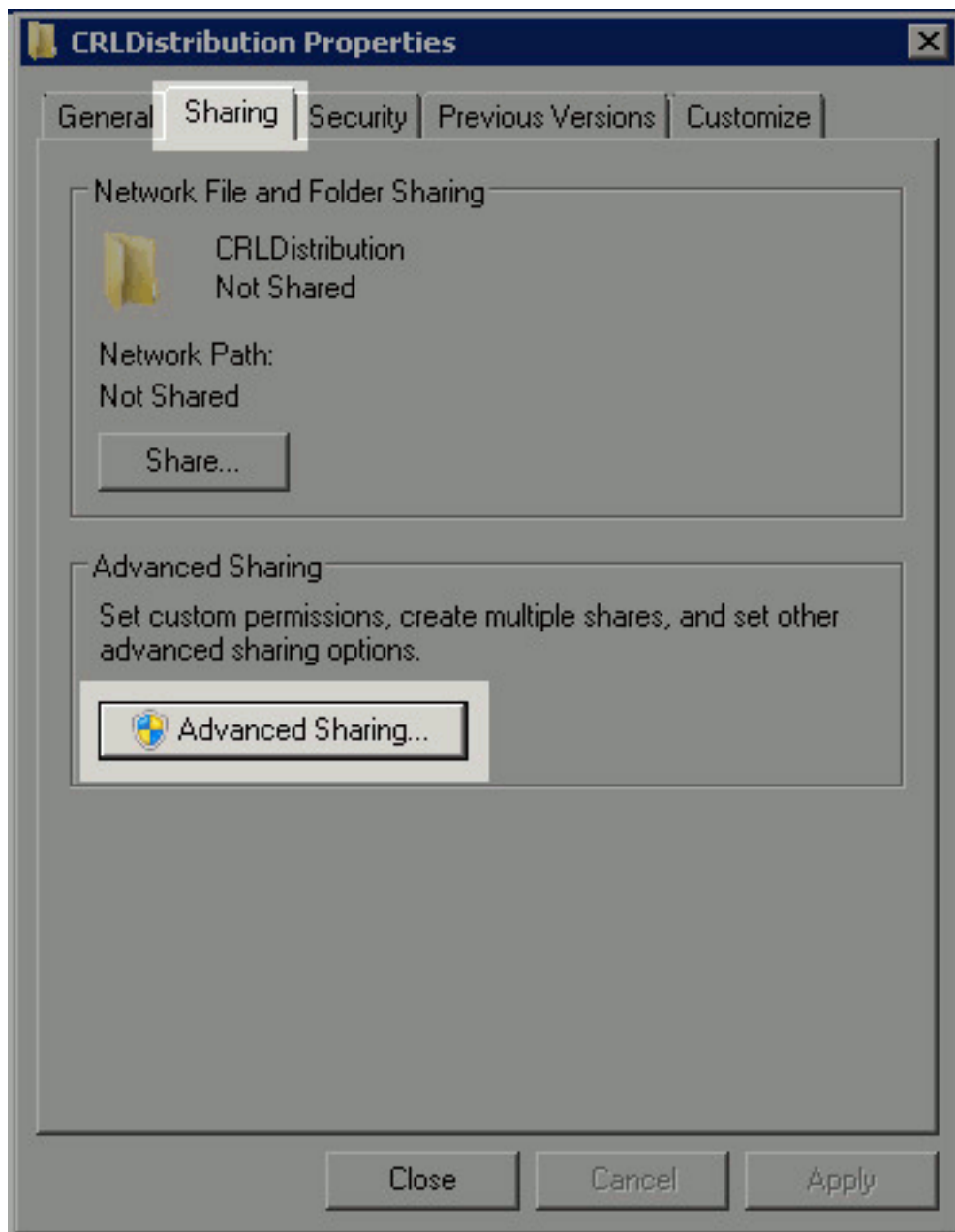
De eerste taak is het configureren van een locatie op de CA server om de CRL bestanden op te slaan. Standaard publiceert de Microsoft CA-server de bestanden naar C:\Windows\system32\CertSrv\CertEnroll\ . Maak geen nieuwe map voor de bestanden in plaats van deze systeemap te gebruiken.

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



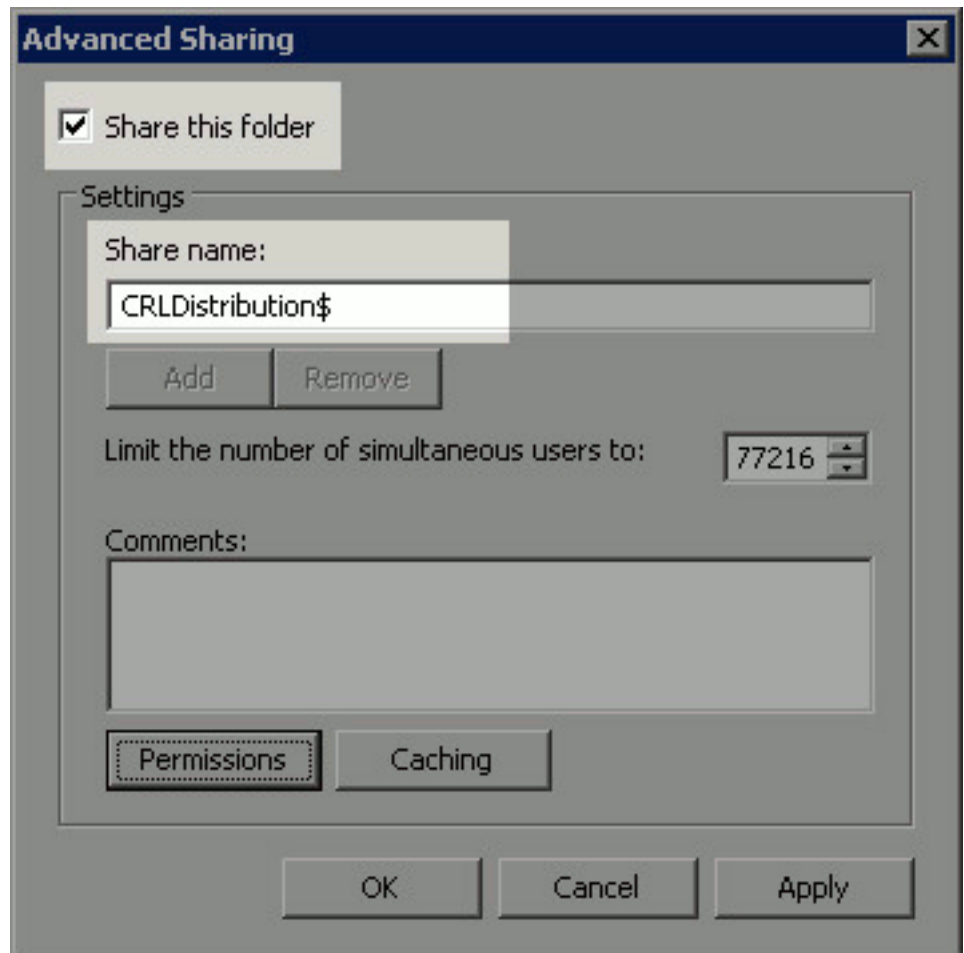
created.

2. Om CA te kunnen de CRL bestanden naar de nieuwe map 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**



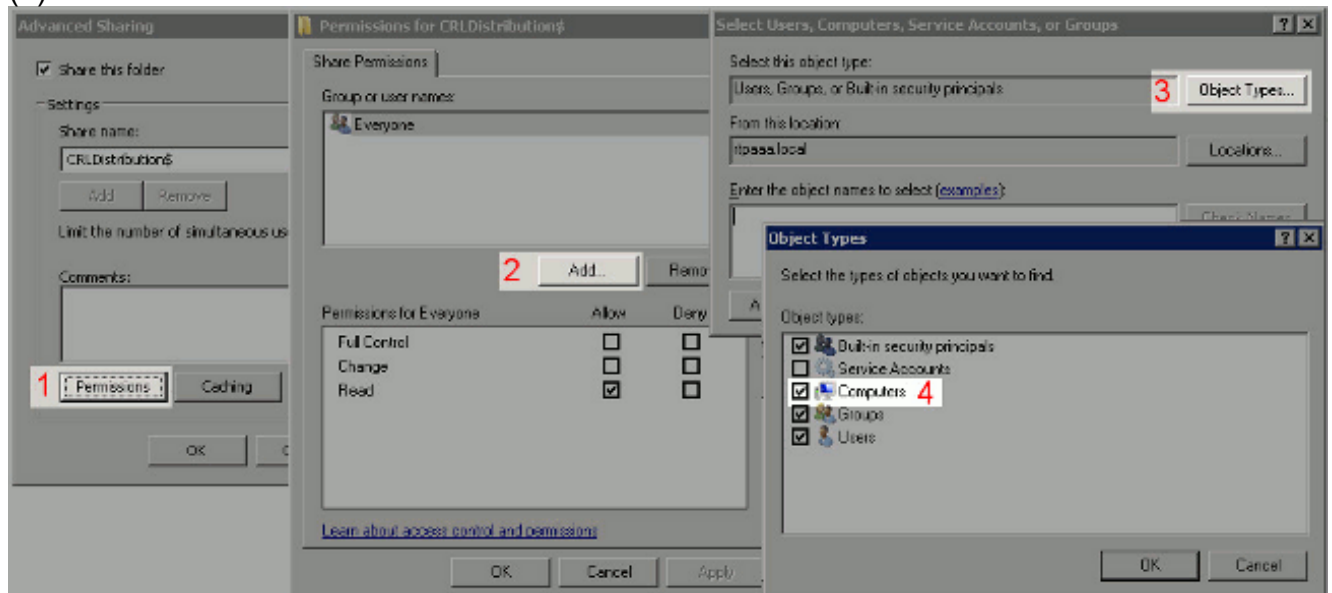
delen.

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

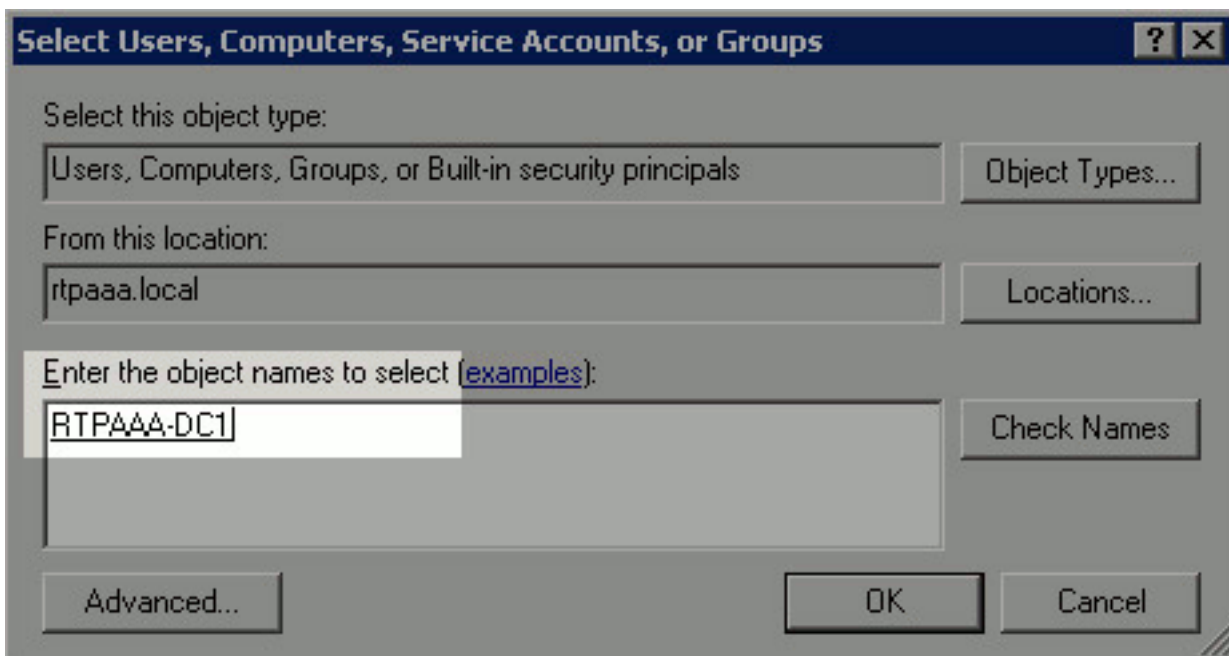


het aandeel te verbergen.

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

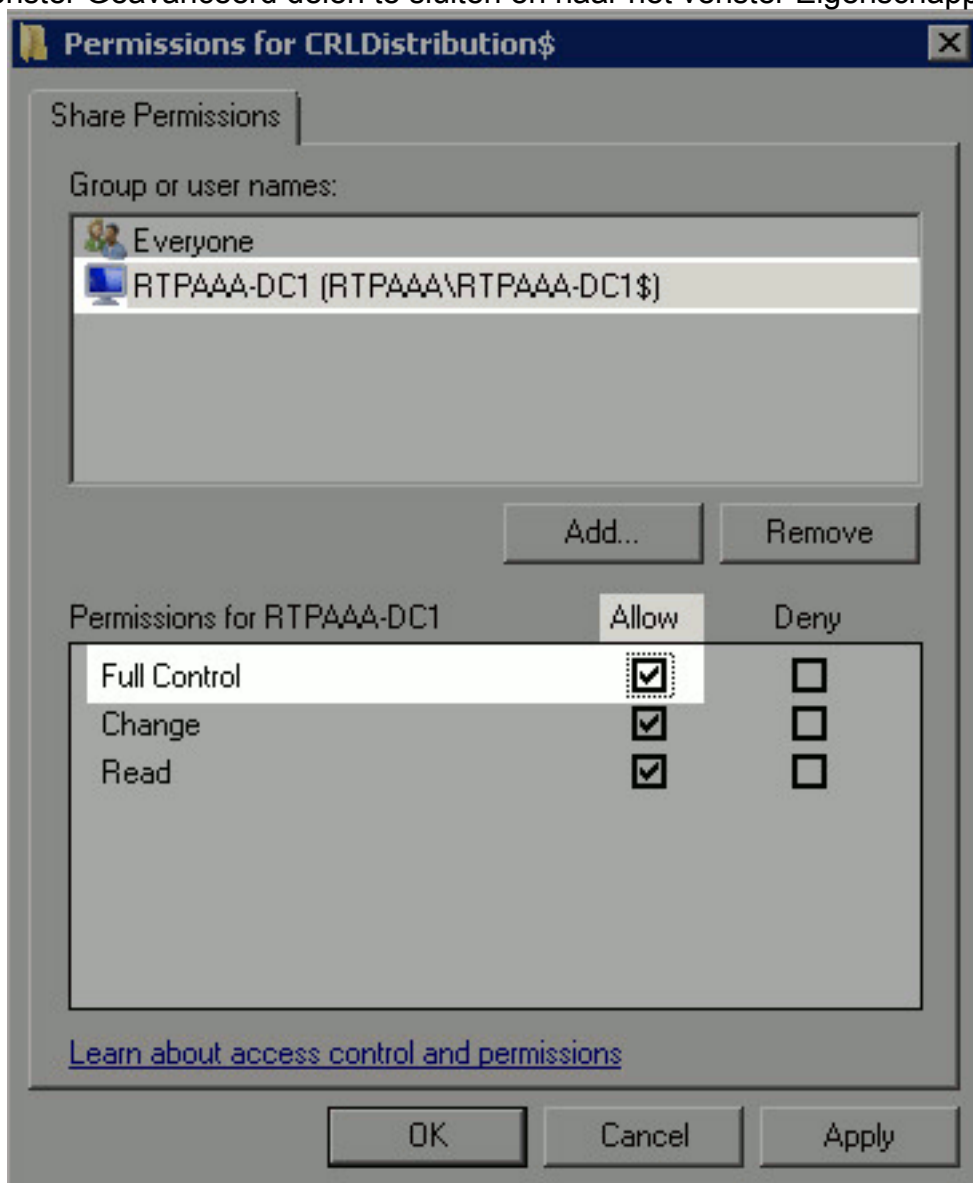


5. Klik op **OK** om terug te keren naar het venster Gebruikers, computers, servicerekeningen of groepen. Typ in het veld Voer de objectnamen in om het veld te selecteren, de computernaam van de CA-server in en klik op **Namen controleren**. Als de ingevoerde naam geldig is, wordt de naam vernieuwd en onderstreept. Klik op



OK.

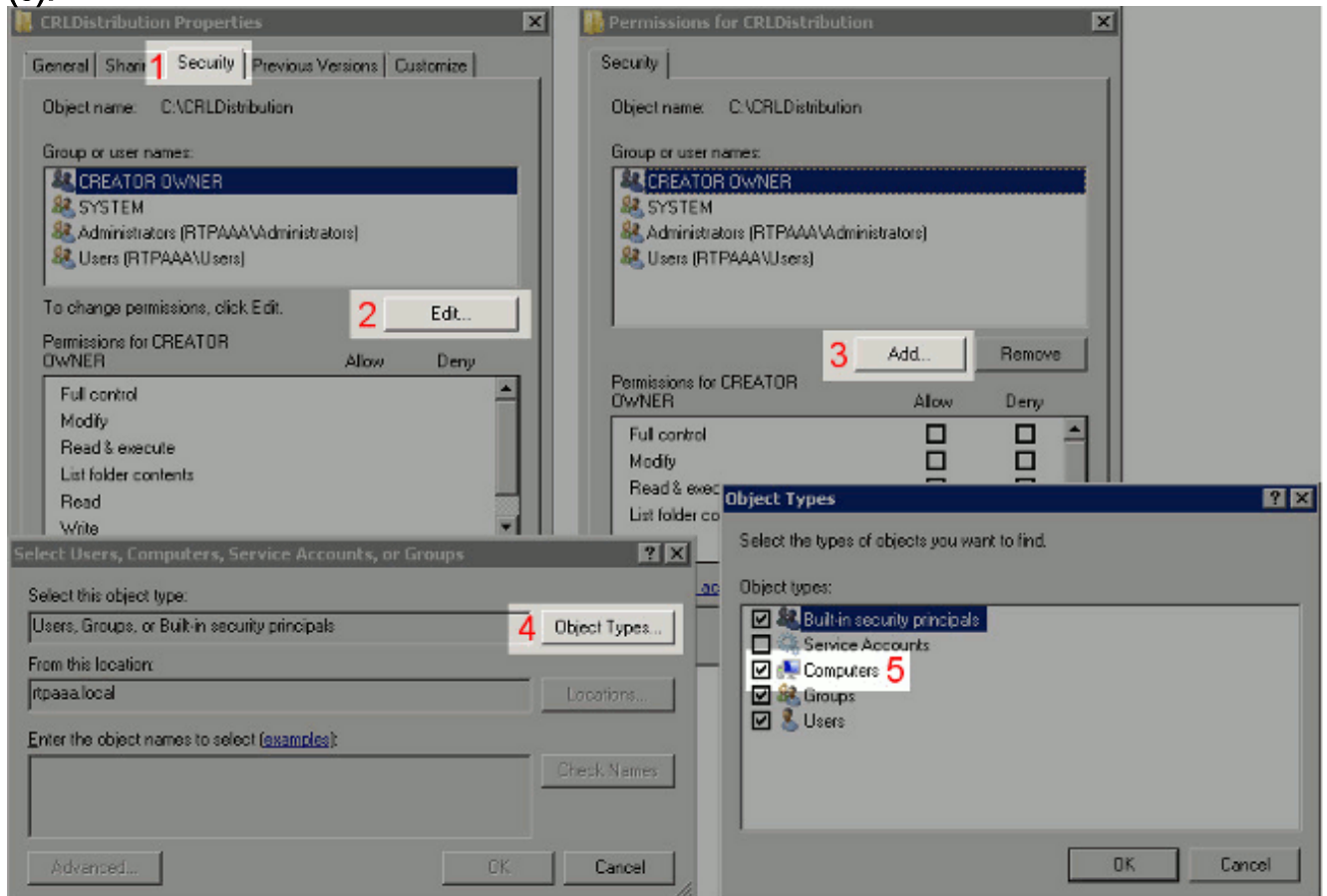
6. Kies de CA-computer in het veld Groep of gebruikersnamen. Controleer **toestaan** dat volledige controle volledige toegang tot de CA verleent. Klik op **OK**. Klik nogmaals op **OK** om het venster Geavanceerd delen te sluiten en naar het venster Eigenschappen terug te



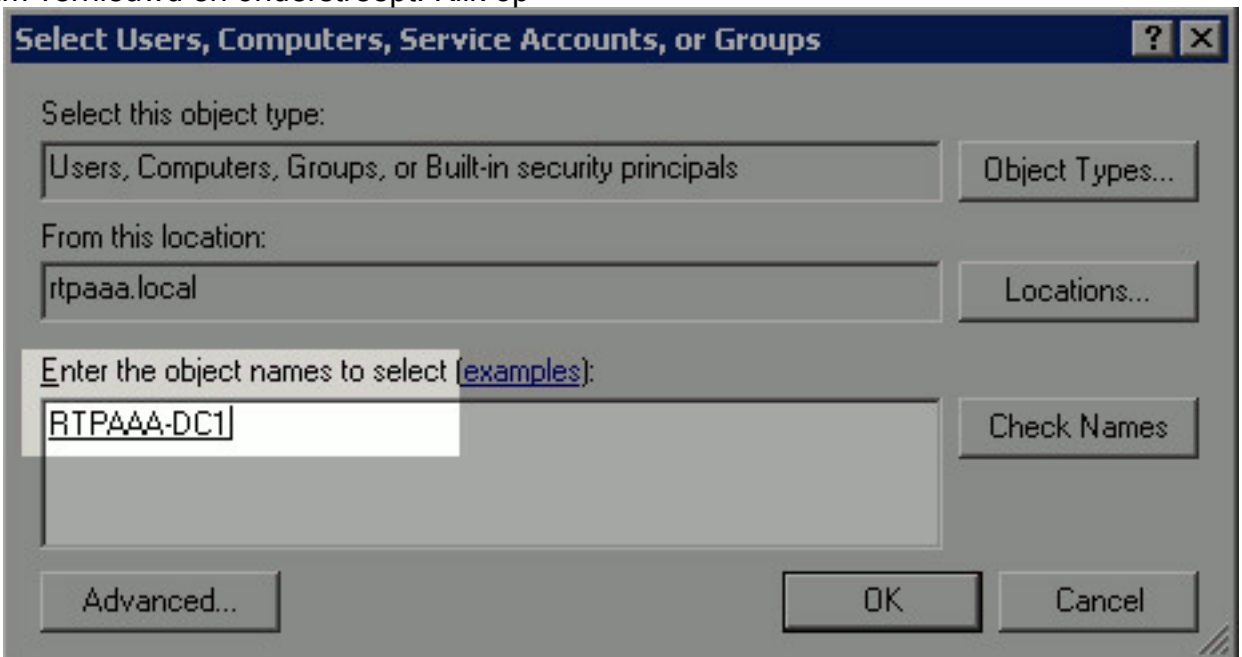
keren.

7. Om CA toe te staan om 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).

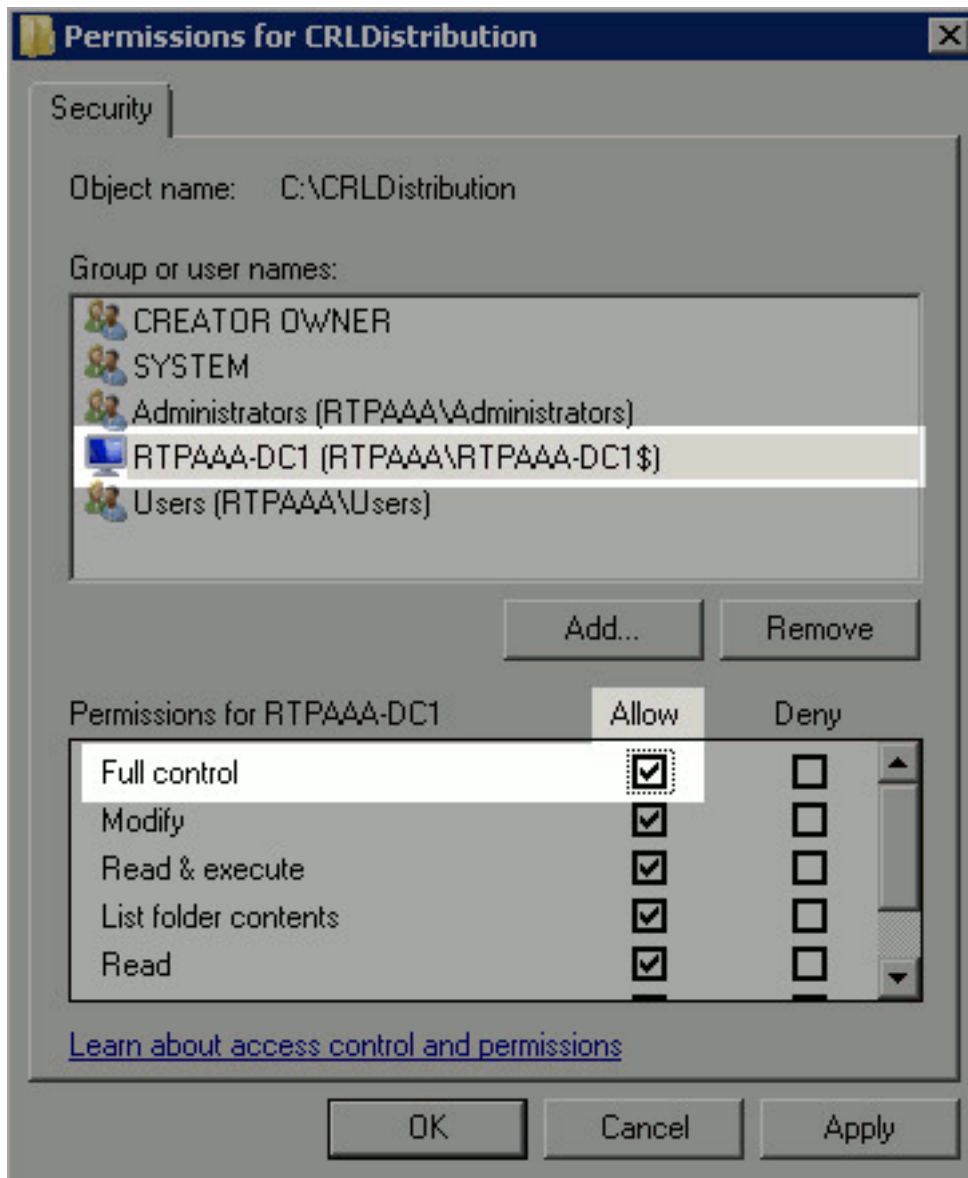


8. Typ in het veld Voer de objectnamen in om het veld te selecteren, de computernaam van de CA-server in en klik op **Namen controleren**. Als de ingevoerde naam geldig is, wordt de naam vernieuwd en onderstreept. Klik op



OK.

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

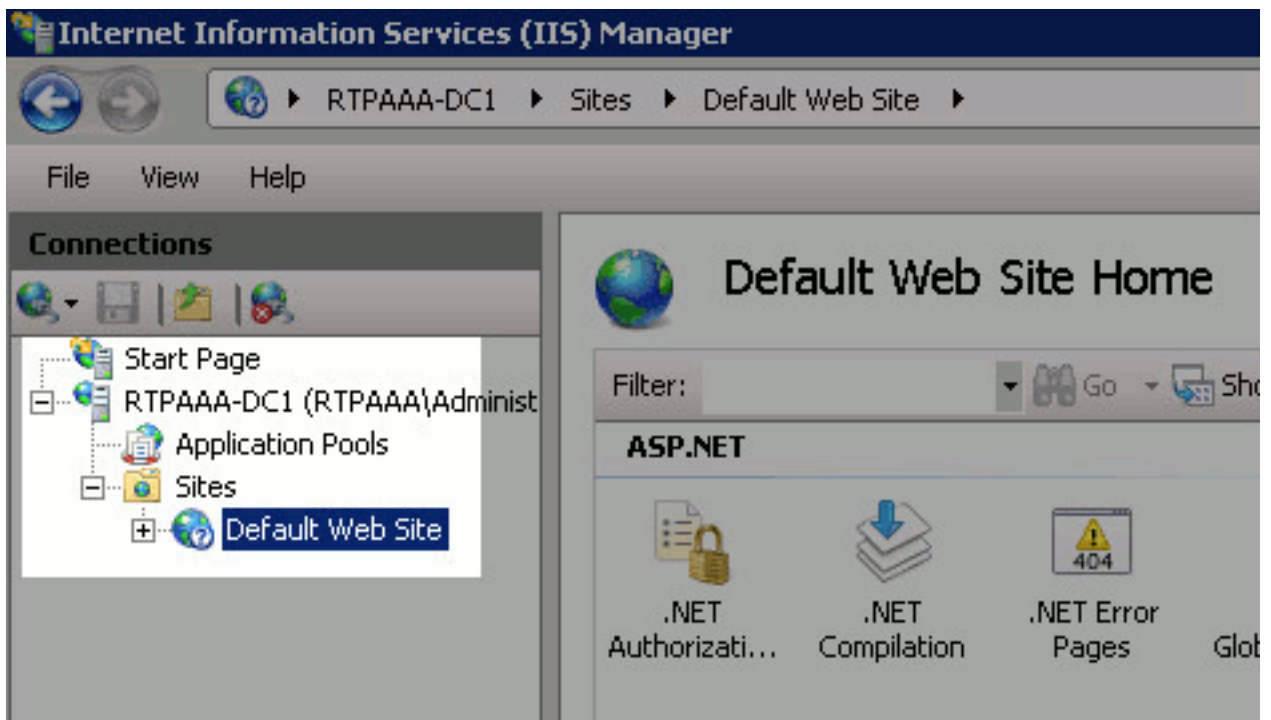


voltoeien.

[Sectie 2. Maak een site in IS om het nieuwe CRL-distributiepunt te onthullen](#)

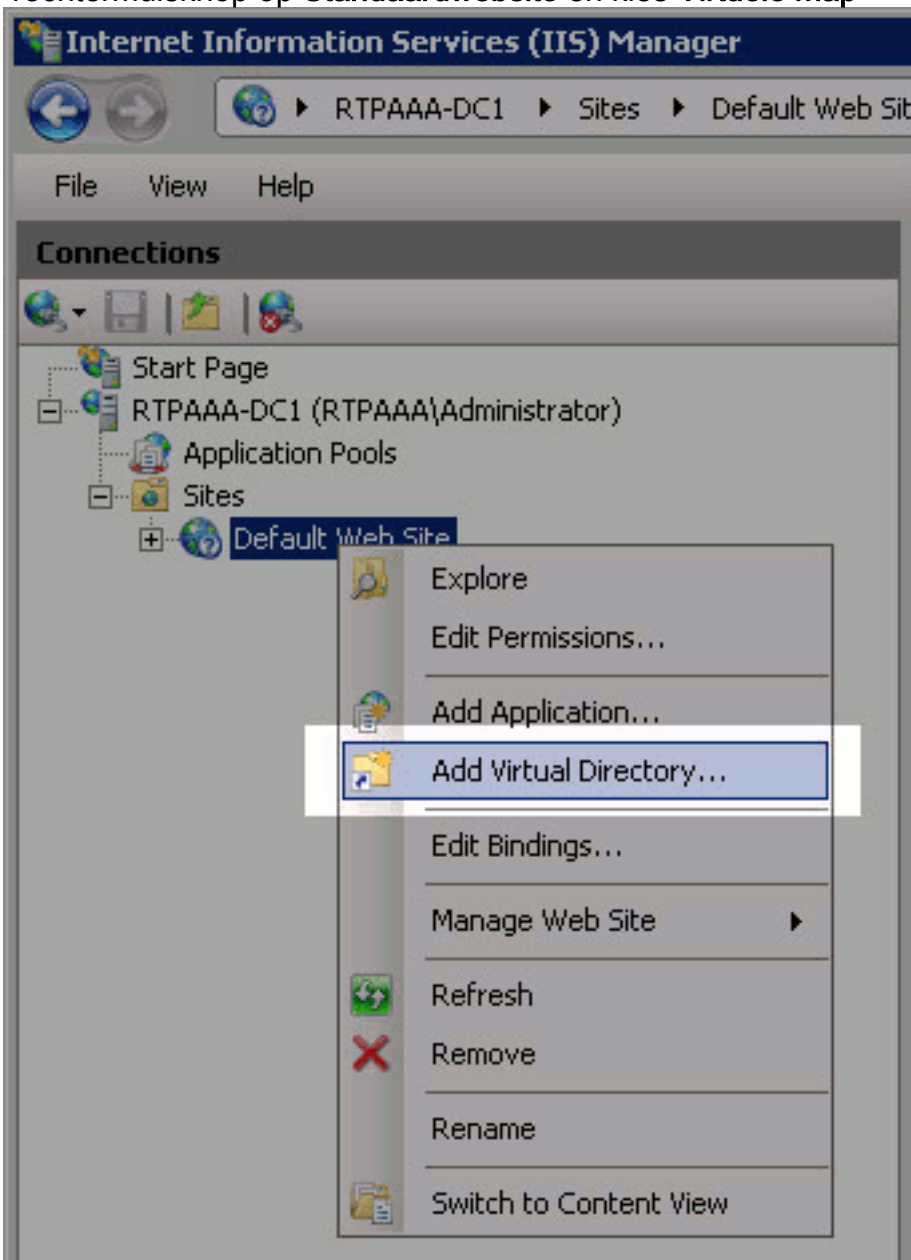
Maak de map waarin de CRL-bestanden zich bevinden toegankelijk via ISE zodat ISE toegang kan krijgen tot de CRL-bestanden.

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**



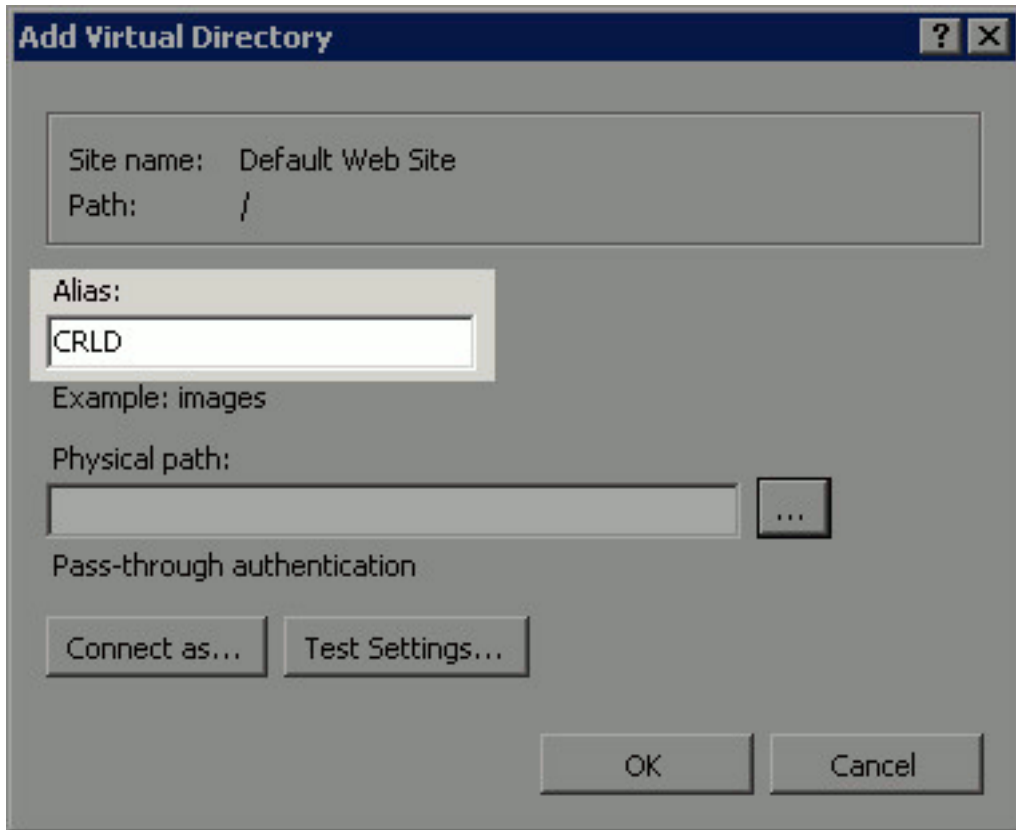
uit.

3. Klik met de rechtermuisknop op **Standaardwebsite** en kies **Virtuele map**



toevoegen.

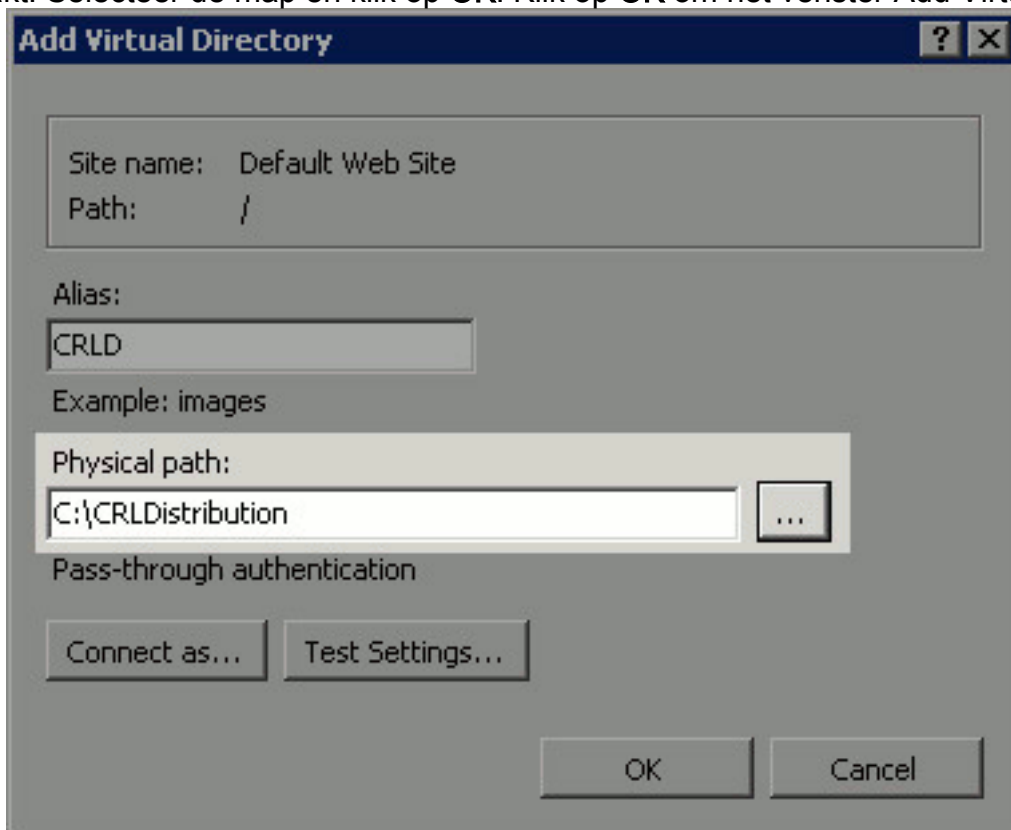
4. Voer in het veld Alias een achternaam in voor het CRL Distribution Point. In dit voorbeeld wordt CRLD



The screenshot shows the 'Add Virtual Directory' dialog box. The 'Site name' is 'Default Web Site' and the 'Path' is '/'. The 'Alias' field contains 'CRLD'. Below it, 'Example: images' is shown. The 'Physical path' field is empty, and the ellipsis button is visible to its right. At the bottom, there are buttons for 'Connect as...', 'Test Settings...', 'OK', and 'Cancel'.

ingevoerd.

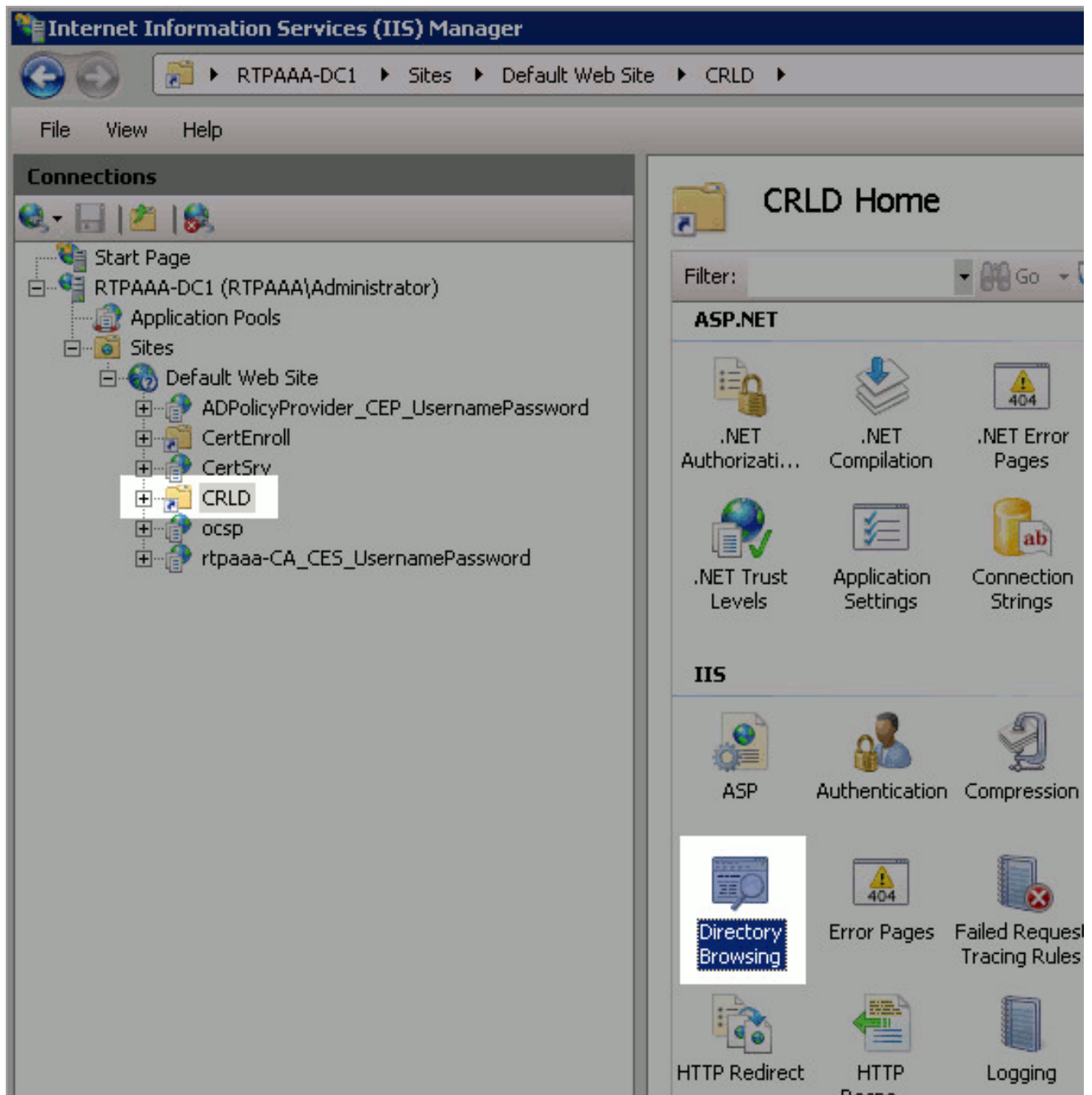
5. Klik op de ellips (. . .) rechts van het veld Fysiek pad en blader naar de map die in sectie 1 is gemaakt. Selecteer de map en klik op **OK**. Klik op **OK** om het venster Add Virtual Directory te



The screenshot shows the 'Add Virtual Directory' dialog box. The 'Site name' is 'Default Web Site' and the 'Path' is '/'. The 'Alias' field contains 'CRLD'. Below it, 'Example: images' is shown. The 'Physical path' field now contains 'C:\CRLDistribution'. At the bottom, there are buttons for 'Connect as...', 'Test Settings...', 'OK', and 'Cancel'.

sluiten.

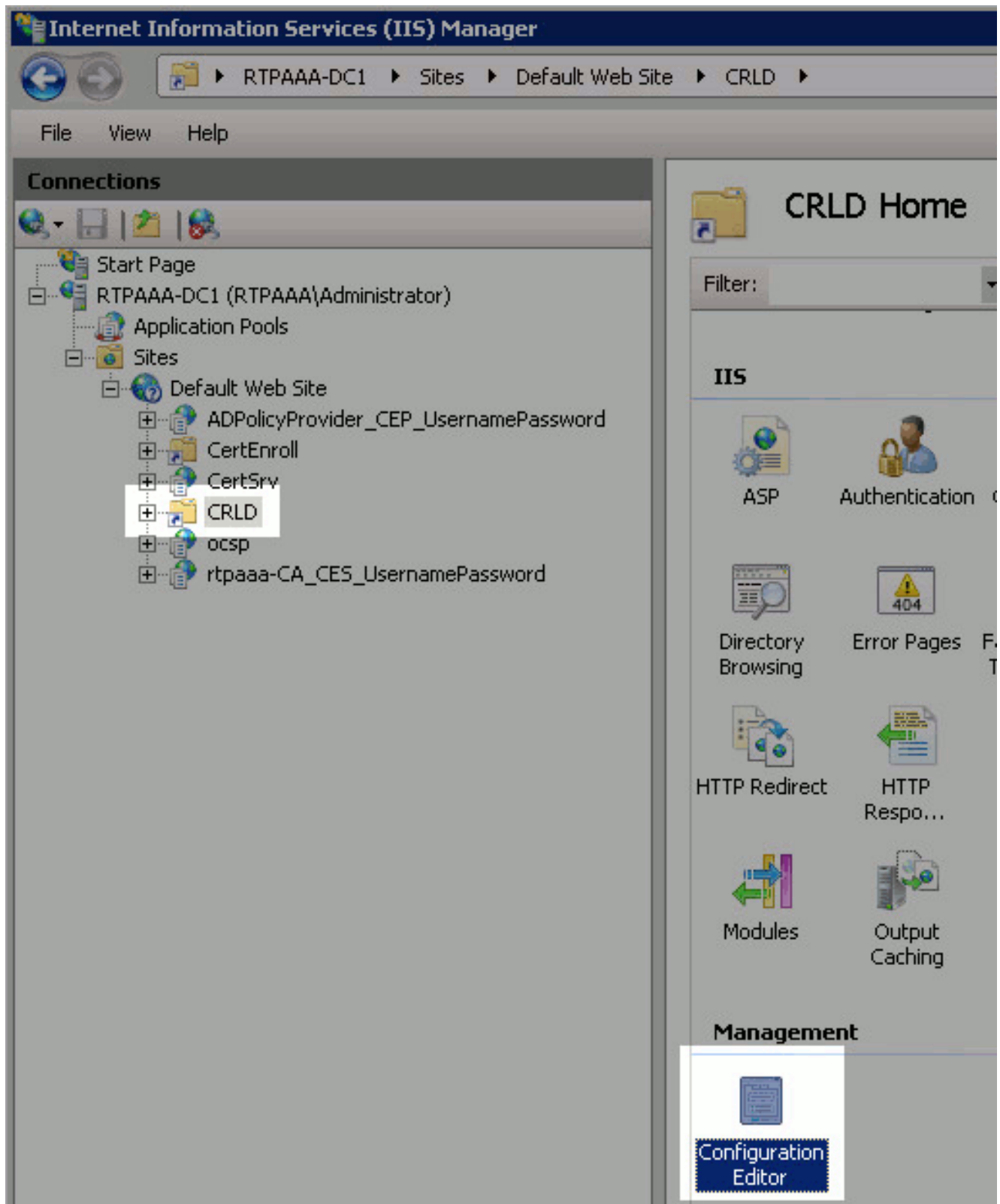
6. De in stap 4 ingevoerde gebiedsnaam moet in het linker deelvenster worden gemarkeerd. Zo niet, kies dan nu. Dubbelklik in het midden op **Directory Browsing**.



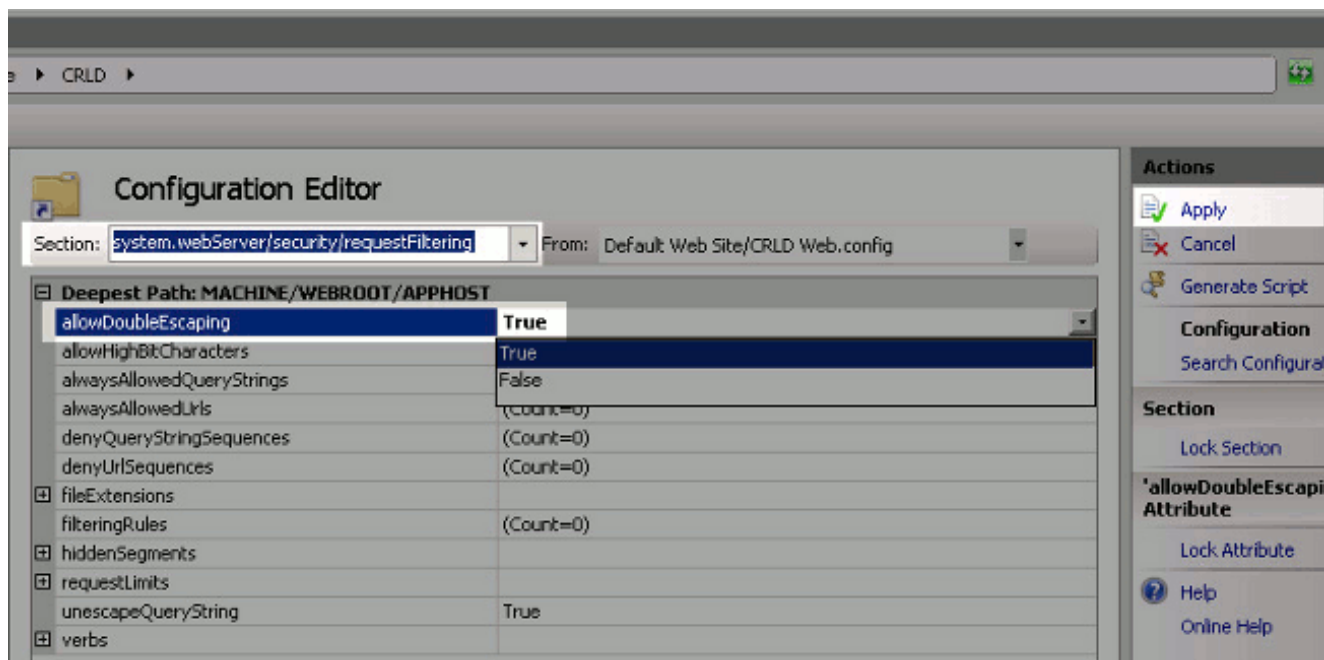
7. Klik in het rechter venster op **Schakel** de directory in om het bladeren in te schakelen.



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



9. Kies in de vervolgkeuzelijst Sectie **system.webServer/security/requestFiltering**. Kies **True** in de vervolgkeuzelijst **allowDubbelscherm**. Klik in het rechtervenster op **Toepassen**.

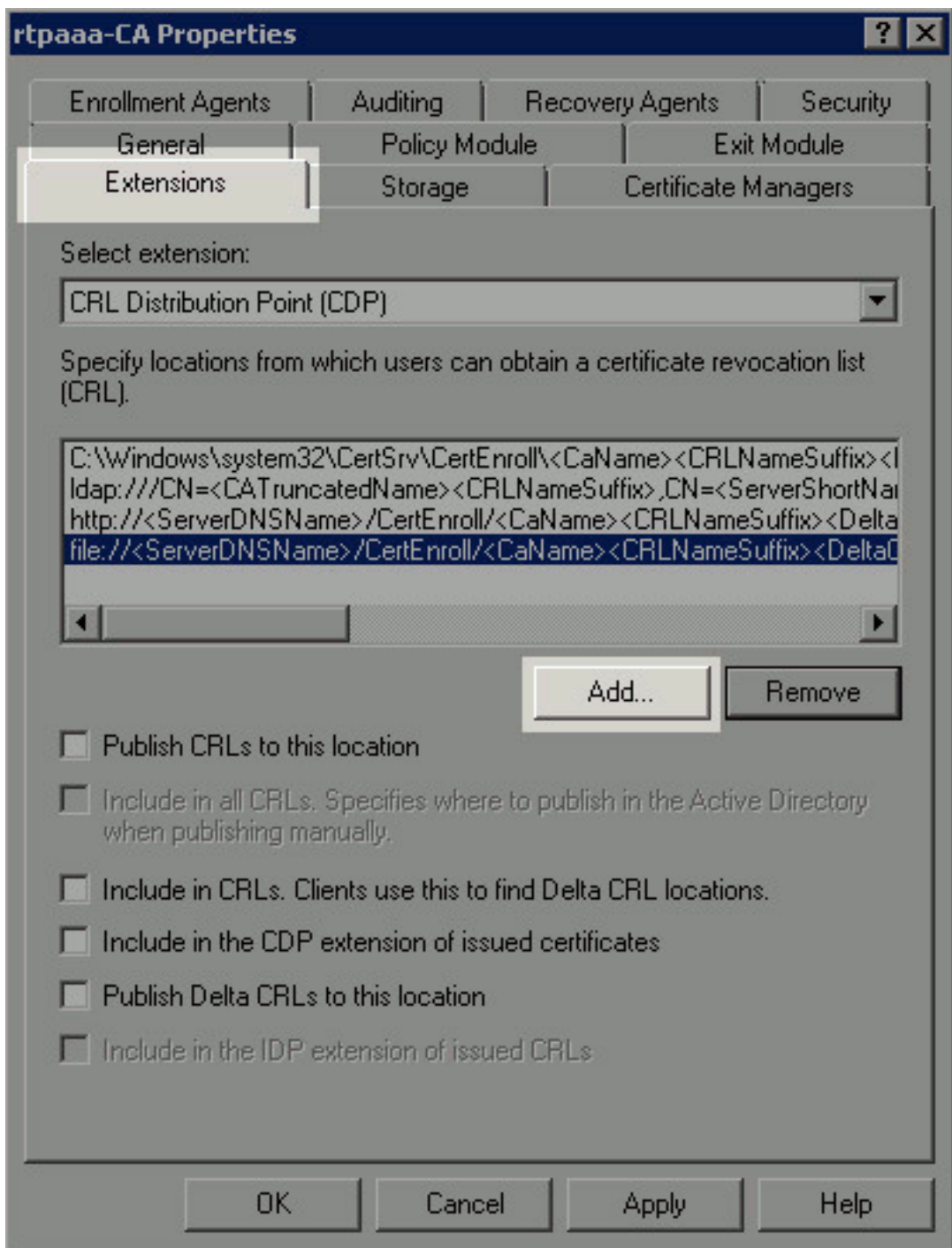


De map moet nu toegankelijk zijn via IS.

[Sectie 3. Configuratie van Microsoft CA-server om CRL-bestanden naar het distributiepunt te publiceren](#)

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

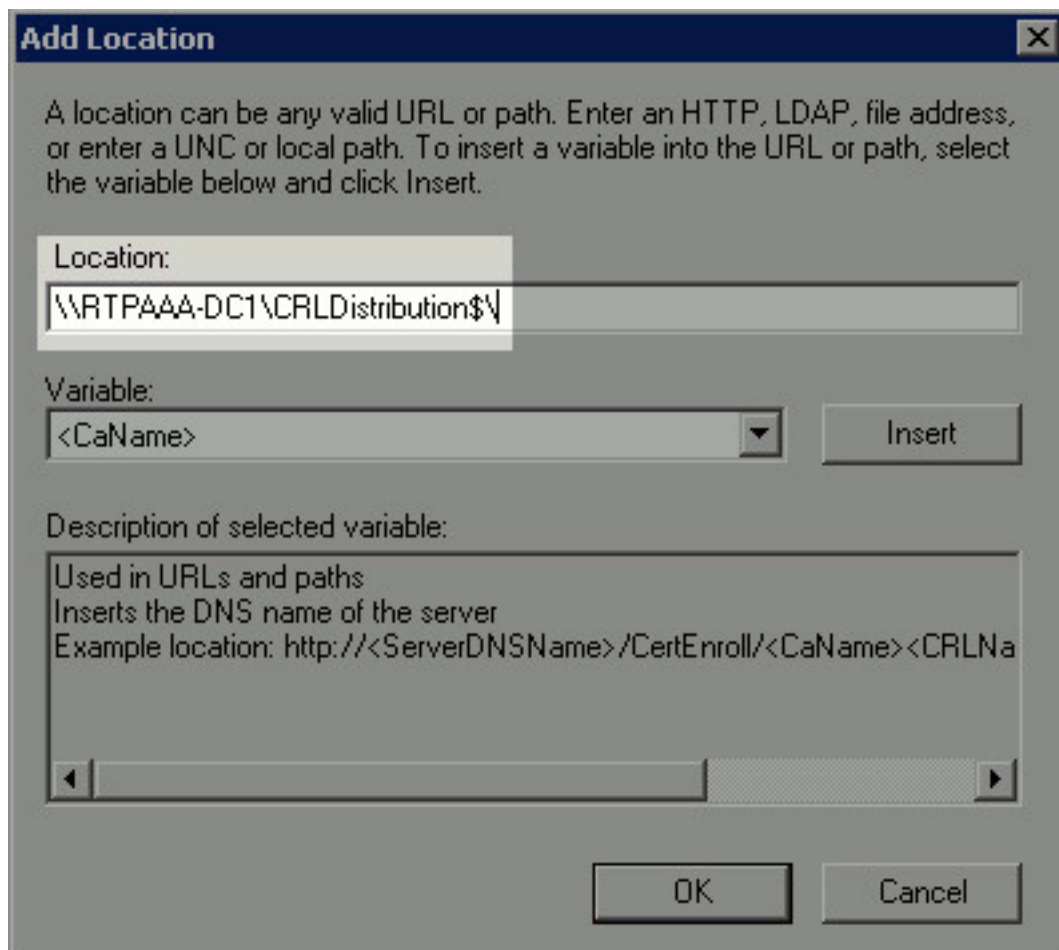
1. Klik in de taakbalk van de CA-server op **Start**. Kies **administratieve hulpmiddelen > certificaatinstantie**.
2. Klik in het linker deelvenster met de rechtermuisknop op de CA-naam. Kies **Eigenschappen** en klik vervolgens op het tabblad **Uitbreidingen**. Als u een nieuw CRL-distributiepunt wilt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



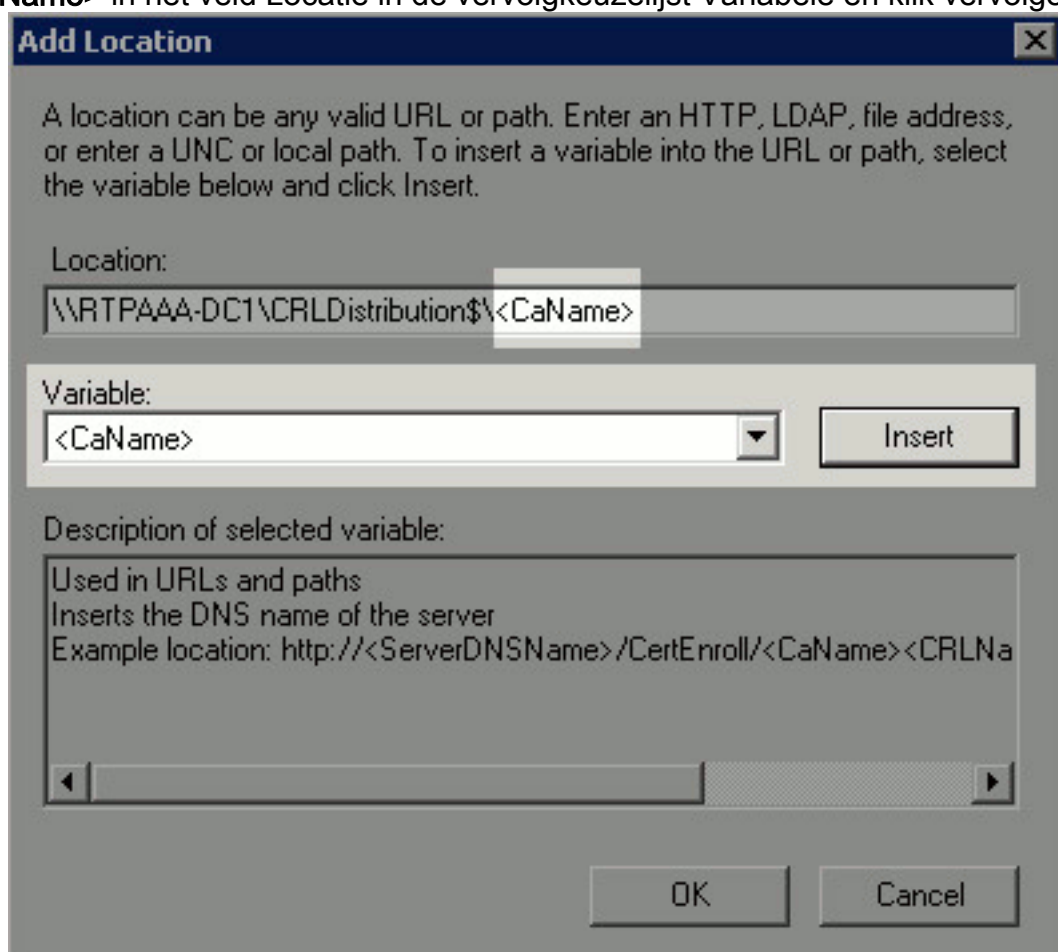
Toevoegen.

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

\\RTPAAA-DC1\CRLDistribution\$\

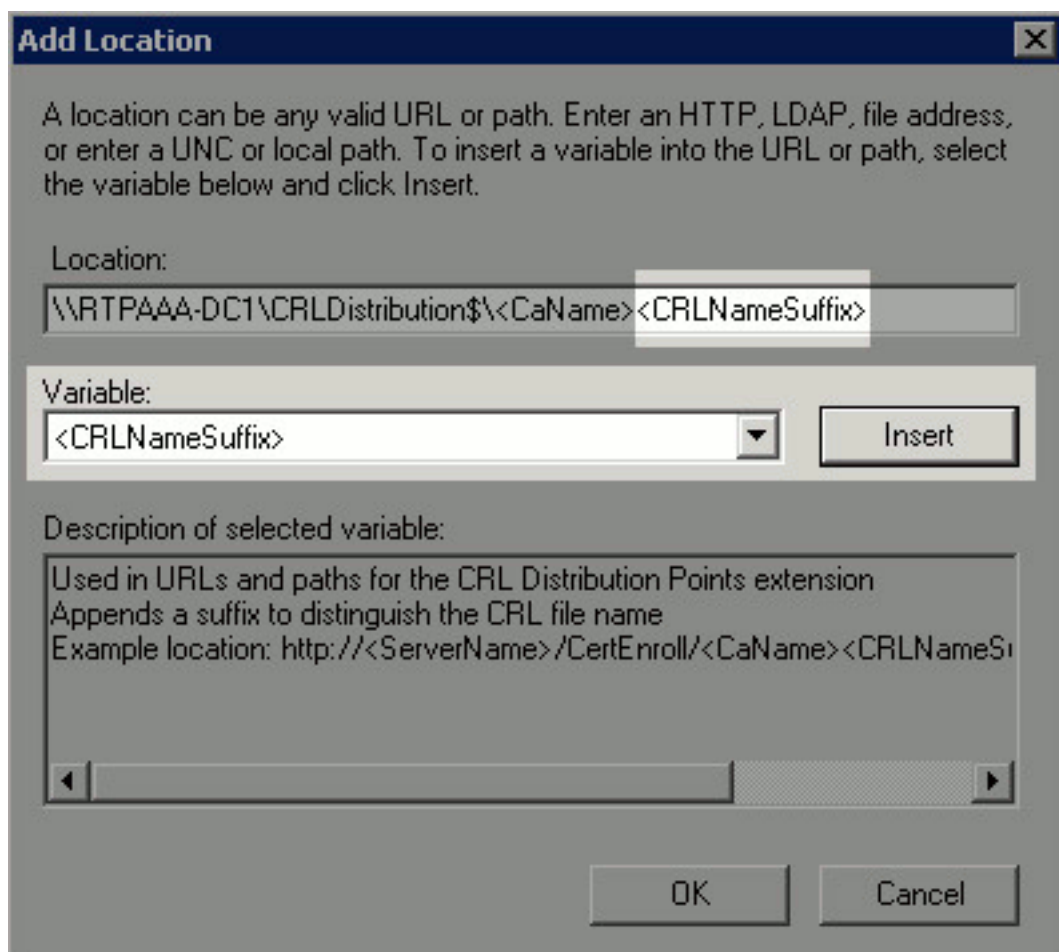


4. Kies **<CaName>** in het veld Locatie in de vervolgkeuzelijst Variabele en klik vervolgens op



Invoegen.

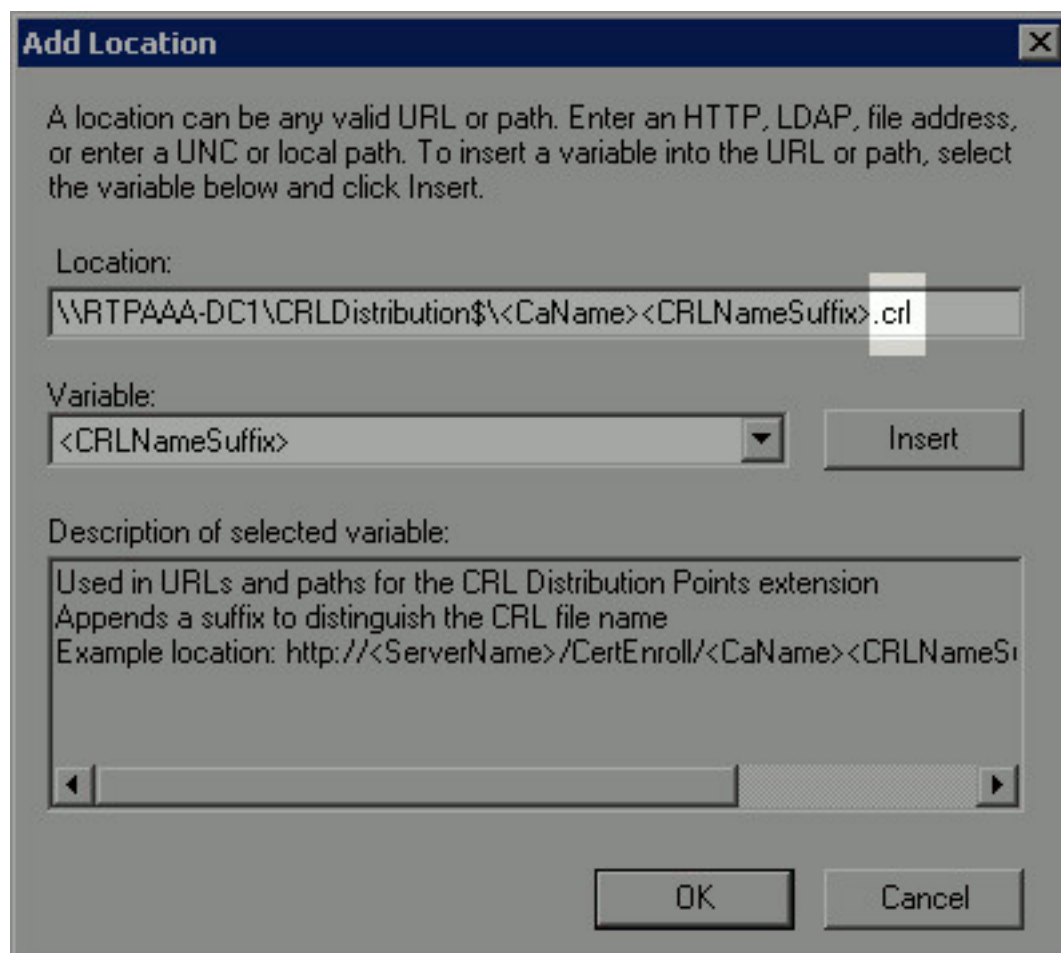
5. Selecteer in de vervolgkeuzelijst Variabele de optie **<CRNameSuffix>** en klik vervolgens op



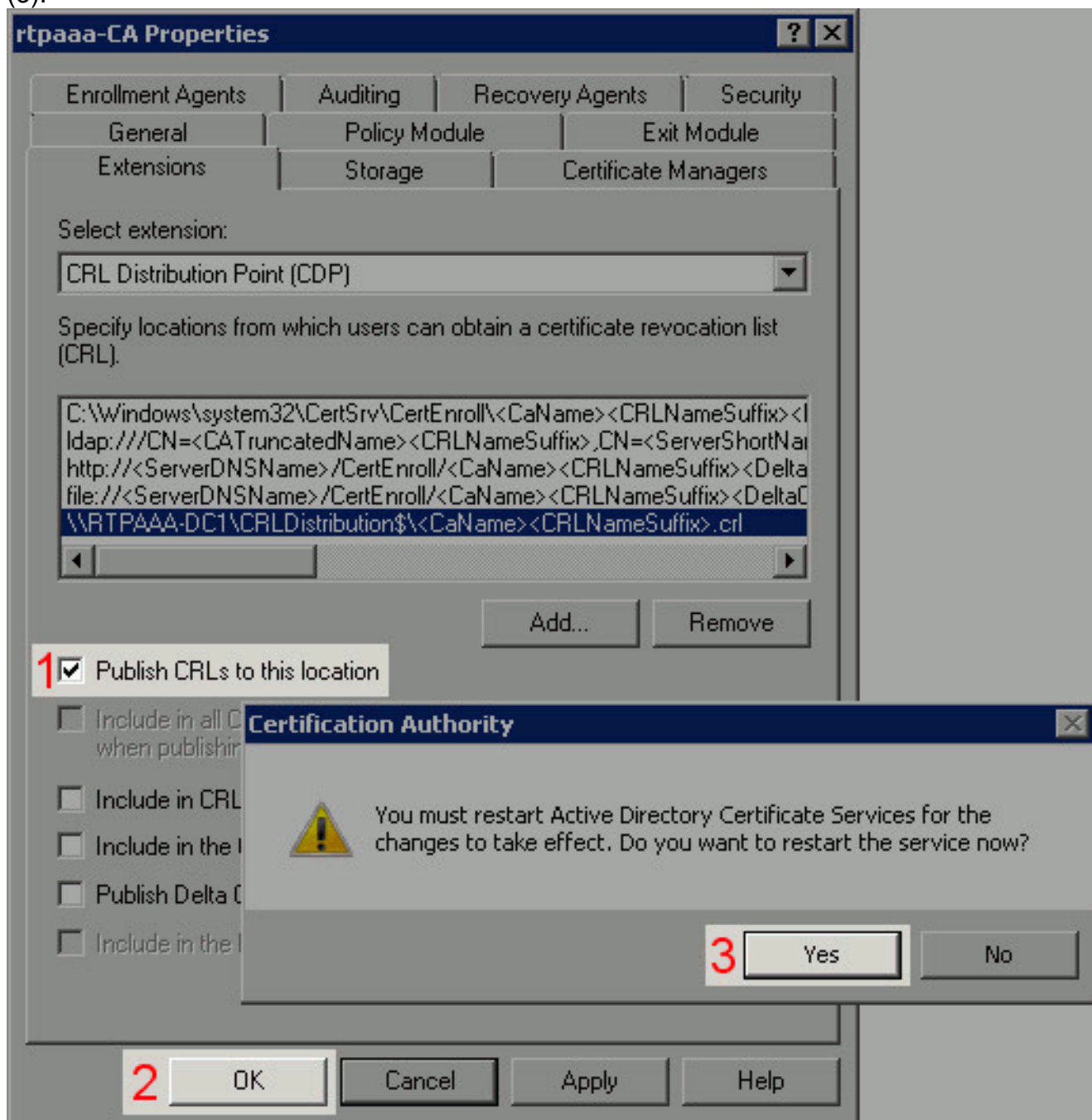
Invoegen.

6. Voeg in het veld Locatie .crl toe aan het einde van het pad. In dit voorbeeld is de Locatie:

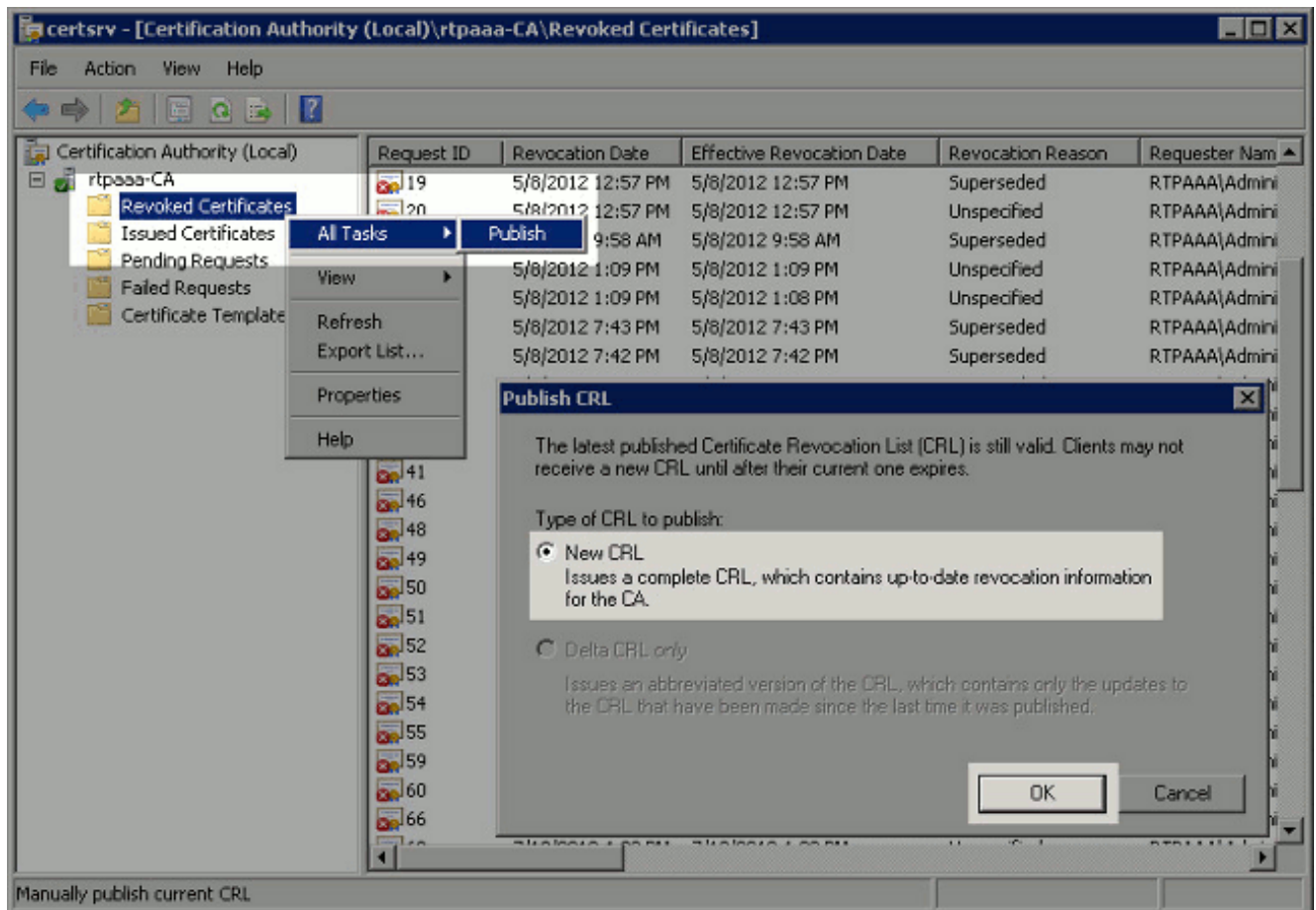
\\RTPAAA-DC1\CRLDistribution\$\<CaName><CRLNameSuffix>.crl



7. Klik op **OK** om naar het tabblad Uitbreidingen terug te keren. Controleer de **openbare CRLs op deze locatie** en klik vervolgens op **OK (2)** om het venster Properties te sluiten. Er verschijnt een melding voor toestemming om de Active Directory certificaatservices opnieuw in te voeren. Klik op **Ja (3)**.



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**.



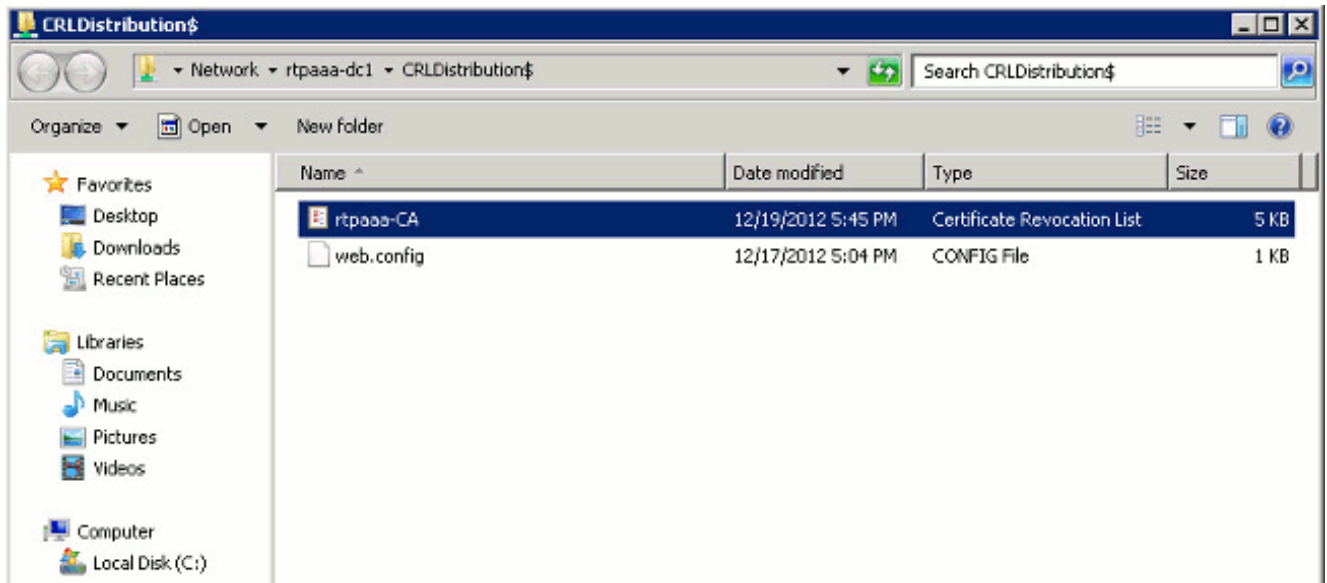
De Microsoft CA-server moet een nieuw .crl-bestand maken in de map die in sectie 1 is gemaakt. Als het nieuwe CRL-bestand met succes is gemaakt, wordt er geen dialoogvenster geopend nadat op OK is gedrukt. Als er een fout wordt teruggegeven in de map van het nieuwe distributiepunt, herhaalt u elke stap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

[Sectie 4. Controleer of het CRL-bestand bestaat en is toegankelijk via 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 is gemaakt in sectie 1 op de lis-server. Er moet één .crl-bestand zijn dat aanwezig is bij het formulier <CANAME>.crl waar <CANAME> de naam van de CA-server is. In dit voorbeeld is filename:

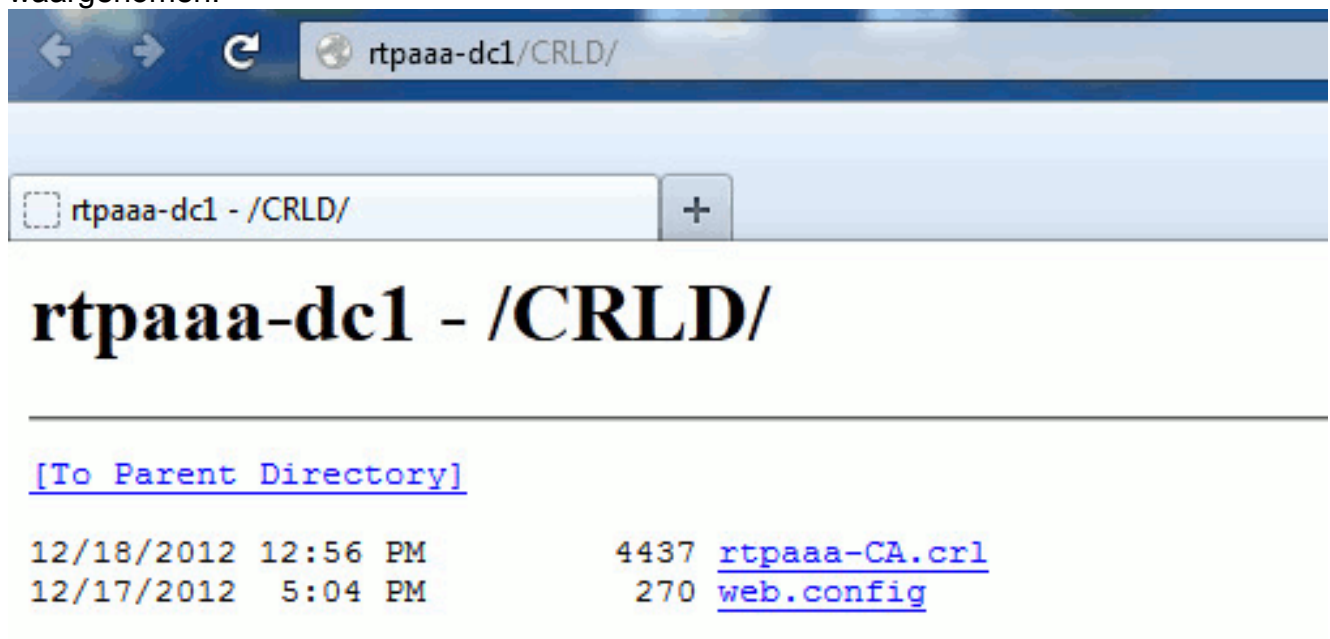
rtpaaa-CA.crl



- Van een werkstation op het netwerk (idealiter op hetzelfde netwerk als het ISE-primaire Admin-knooppunt) opent u een webbrowser en bladert naar `http://<SERVER>/<CRLSITE>` waarin `<SERVER>` de servernaam is van de IIS-server 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://RTPAAA-DC1/CRLD`

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



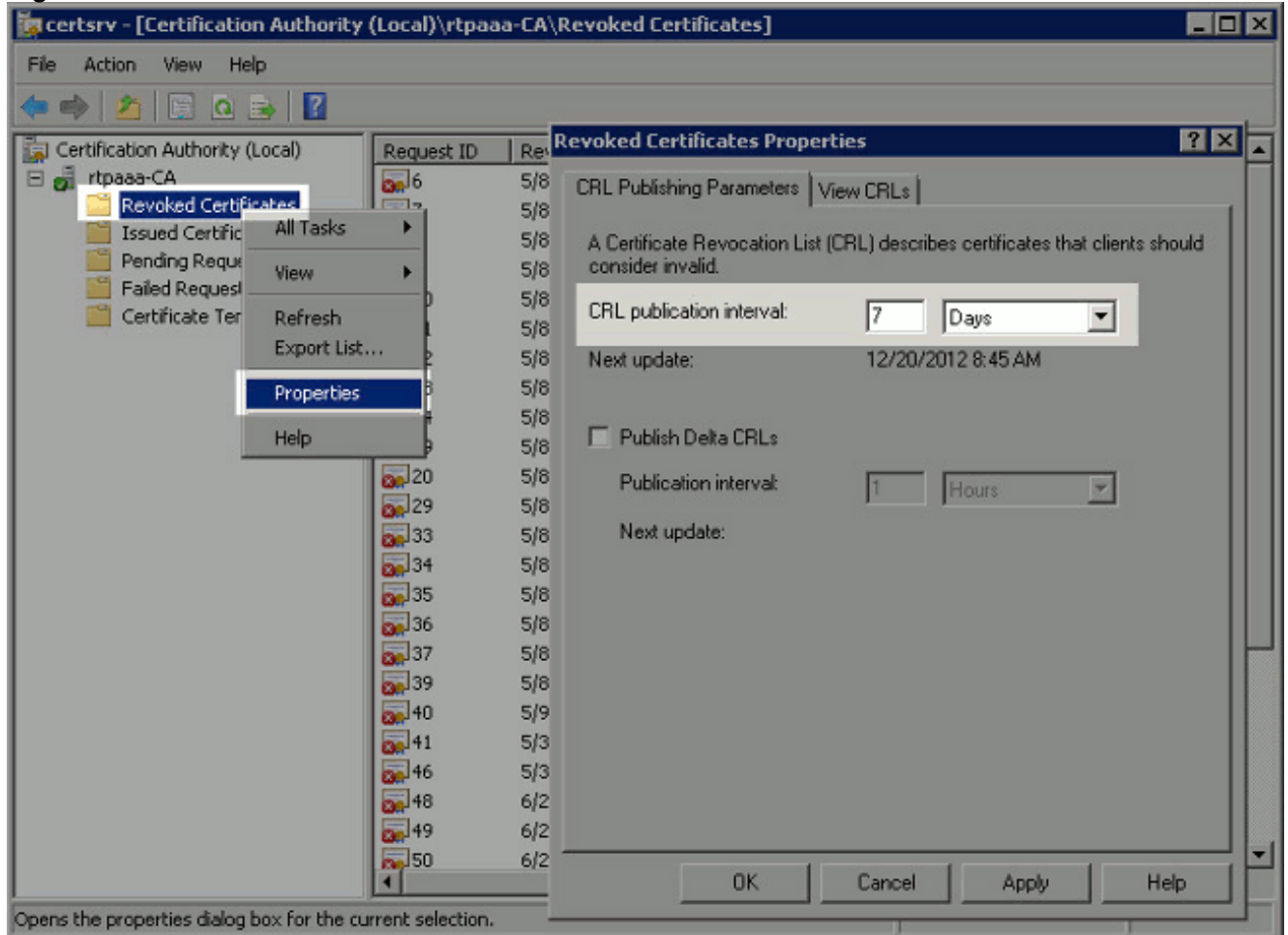
[Sectie 5. Configureer de ISE om het nieuwe CRL-distributiepunt te gebruiken](#)

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:

- 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.



U dient nu meerdere registratiewaarden te bevestigen, die helpen de instellingen voor CRL-herkenning in ISE te bepalen.

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_DWORD = 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 CRLPperiode 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.
```

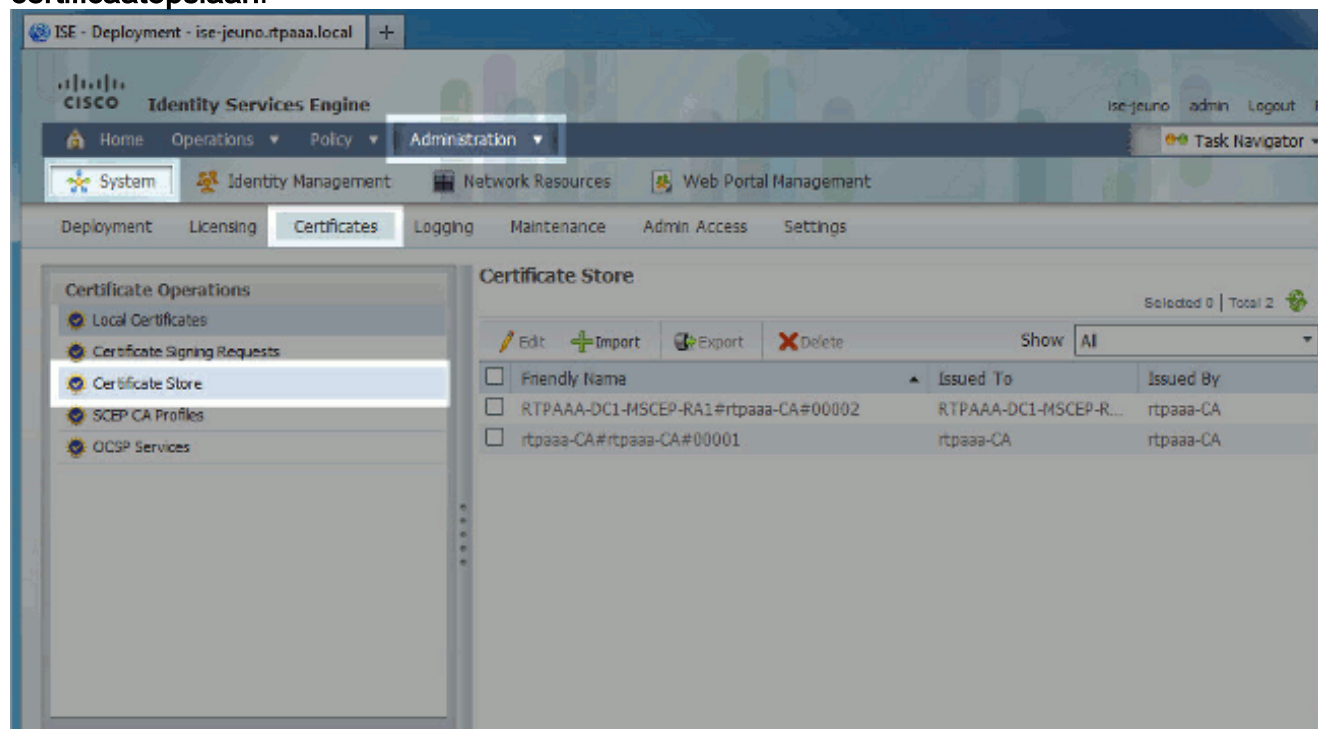
7. Bereken de CRL-Grace-periode als volgt: Indien CRLOverlapPeriod in stap 5 was ingesteld: OVERLAP = CRLOverlapPeriod, in minuten; Elders: OVERLAP = (CRLP-periode / 10), in minuten. Bij OVERLAP > 720 dan overLAP = 720. Als overLAP < (1,5 * KloktijdSkewMinutes) is het mogelijk dat u overLAP maakt = (1,5 * ClockSkewMinutes). Indien overLAP > CRLPeriod, in minuten, dan overLAP = CRLPd in minuten. Grace Periode = 720 minuten + 10 minuten = 730 minuten. Voorbeeld:

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

- OVERLAP = (10248 / 10) = 1024.8 minutes
- 1024.8 minutes is > 720 minutes : OVERLAP = 720 minutes
- 720 minutes is NOT < 15 minutes : OVERLAP = 720 minutes
- 720 minutes is NOT > 10248 minutes : OVERLAP = 720 minutes
- 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 primaire Admin-knooppunt en kies **Beheer > Systeem > Certificaten**. Selecteer in het linker venster de optie **certificaatopslaan**.



9. Controleer het aanvinkvakje in de certificaatwinkel naast het CA-certificaat waarvoor u CRL's wilt configureren. Klik op **Bewerken**.
10. Controleer bij de onderkant van het venster het vakje **CRL downloaden**.
11. In het veld CRL Distribution URL specificieert 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://RTPAAA-DC1/CRLD/rtpaaa-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 waarde is ingesteld 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 doorgaan (en zonder een CRL-controle) indien ISE in zijn laatste downloadpoging de CRL voor deze CA niet heeft kunnen ophalen. 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 het **negeren dat CRL nog niet geldig is of verlopen** aanvinkvakje om ISE toe te staan verlopen (of nog niet geldige) 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.

Issued To	rtpaaa-CA
Issued By	rtpaaa-CA
Valid From	Sat, 11 Feb 2012 19:32:02 EST
Valid To (Expiration)	Wed, 11 Feb 2037 19:42:01 EST
Serial Number	1D 85 1D 58 36 8C EC 93 4E F6 5B 28 9B 26 E7 89

Usage

All Trust Certificates are available for selection as the Root CA for secure LDAP connections. In addition, they may be enabled for EAP-TLS and administrative authentication below:

Trust for client authentication

Enable Validation of Certificate Extensions (accept only valid certificate)

Certificate Status Validation

To verify certificates, enable the methods below. If both are enabled, OCSP will always be tried first.

OCSP Configuration

Validate against OCSP Service

Reject the request if certificate status could not be determined by OCSP

Certificate Revocation List Configuration

Download CRL

CRL Distribution URL

Retrieve CRL

Automatically before expiration.

Every

If download failed, wait before retry.

Bypass CRL Verification if CRL is not Received

Ignore that CRL is not yet valid or expired

[Verifiëren](#)

Er is momenteel geen verificatieprocedure beschikbaar voor deze configuratie.

[Problemen oplossen](#)

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

[Gerelateerde informatie](#)

- [Technische ondersteuning en documentatie – Cisco Systems](#)