Konfigurieren des Microsoft CA-Servers zum Veröffentlichen der Zertifikatswiderrufslisten für die ISE

Inhalt

Einführung

Dieses Dokument beschreibt die Konfiguration eines Servers der Microsoft Certificate Authority (CA), auf dem Internetinformationsdienste (IIS) ausgeführt werden, um die CRL-Updates (Certificate Revocation List) zu veröffentlichen. Außerdem wird erläutert, wie die Cisco Identity Services Engine (ISE) (Version 3.0 und höher) so konfiguriert wird, dass die Aktualisierungen zur Verwendung bei der Zertifikatsvalidierung abgerufen werden. Die ISE kann so konfiguriert werden, dass sie CRLs für die verschiedenen CA-Root-Zertifikate abruft, die sie bei der Zertifikatsvalidierung verwendet.

Voraussetzung

Anforderungen

Es gibt keine spezifischen Anforderungen für dieses Dokument.

Verwendete Komponenten

Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

- Cisco Identity Services Engine Version 3.0
- Microsoft Windows® Server® 2008 R2

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher,

dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Konfiguration

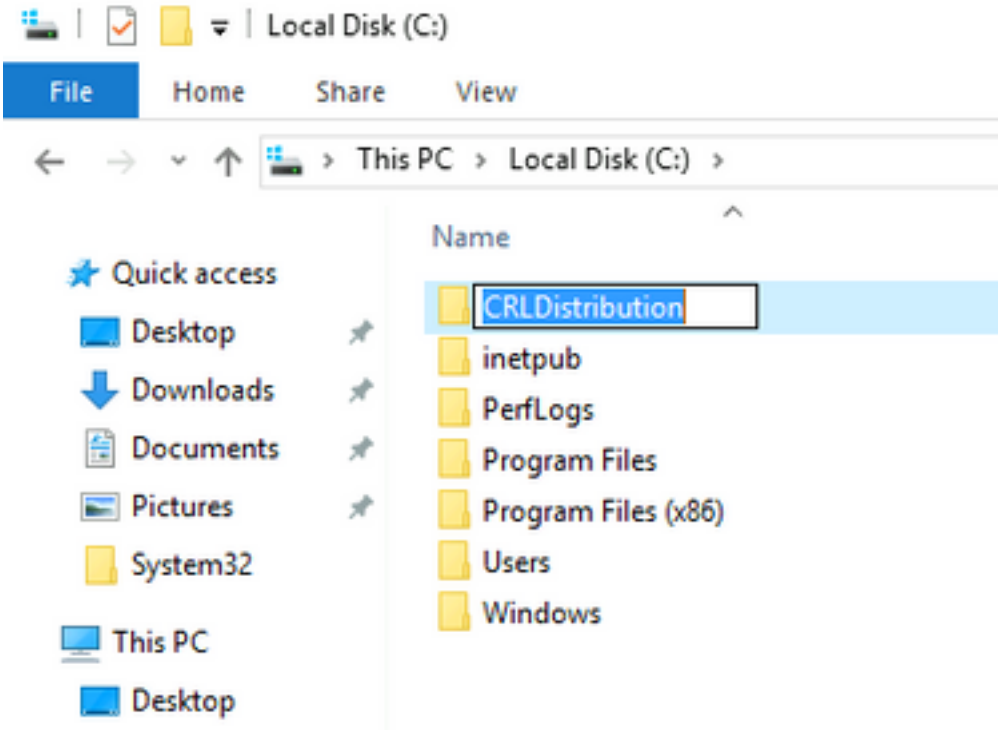
In diesem Abschnitt erfahren Sie, wie Sie die in diesem Dokument beschriebenen Funktionen konfigurieren können.

Erstellen und Konfigurieren eines Ordners auf der CA zum House der CRL-Dateien

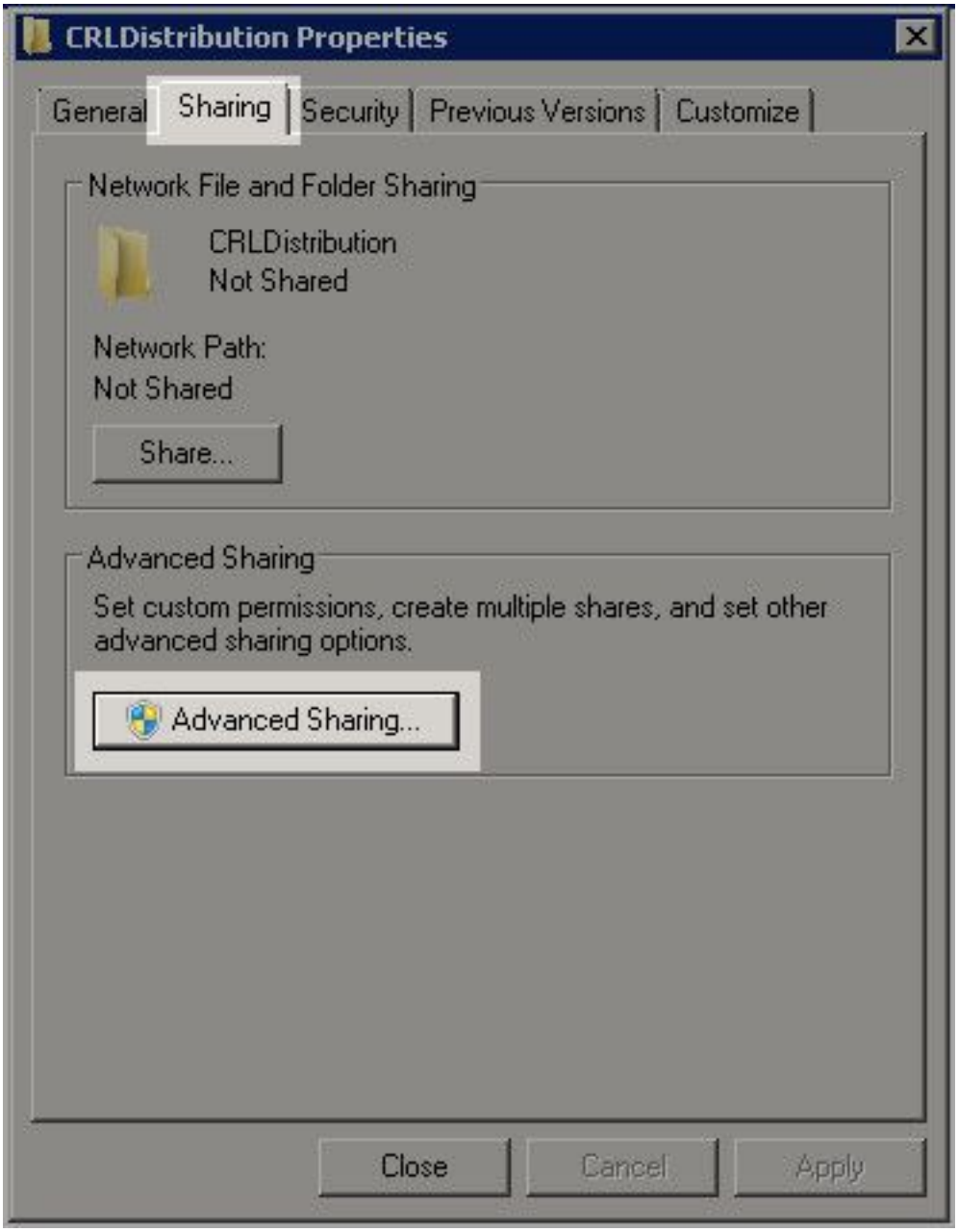
Die erste Aufgabe besteht darin, einen Speicherort auf dem CA-Server zu konfigurieren, an dem die CRL-Dateien gespeichert werden. Standardmäßig veröffentlicht der Microsoft CA-Server die Dateien an **C:\Windows\system32\CertSrv\CertEnroll**

Erstellen Sie statt dieses Systemordners einen neuen Ordner für die Dateien.

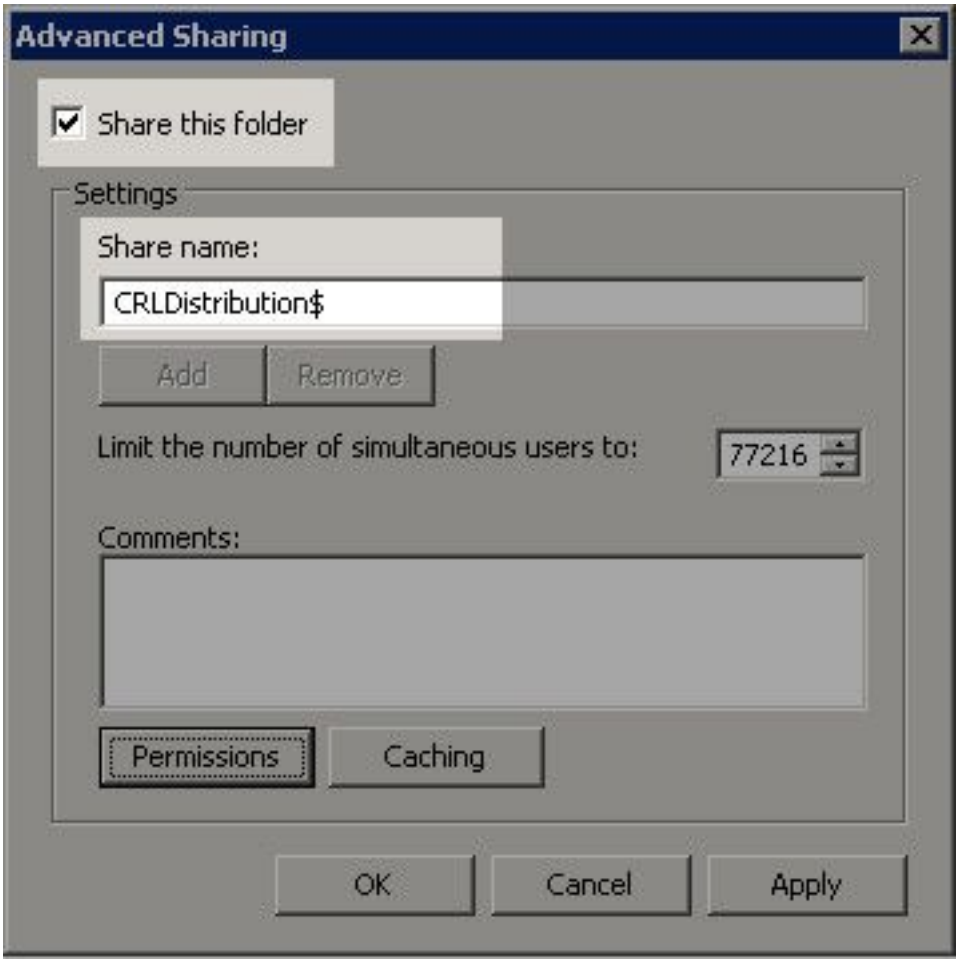
1. Wählen Sie auf dem IIS-Server einen Speicherort im Dateisystem aus, und erstellen Sie einen neuen Ordner. In diesem Beispiel wird der Ordner **C:\CRLDistribution** erstellt.



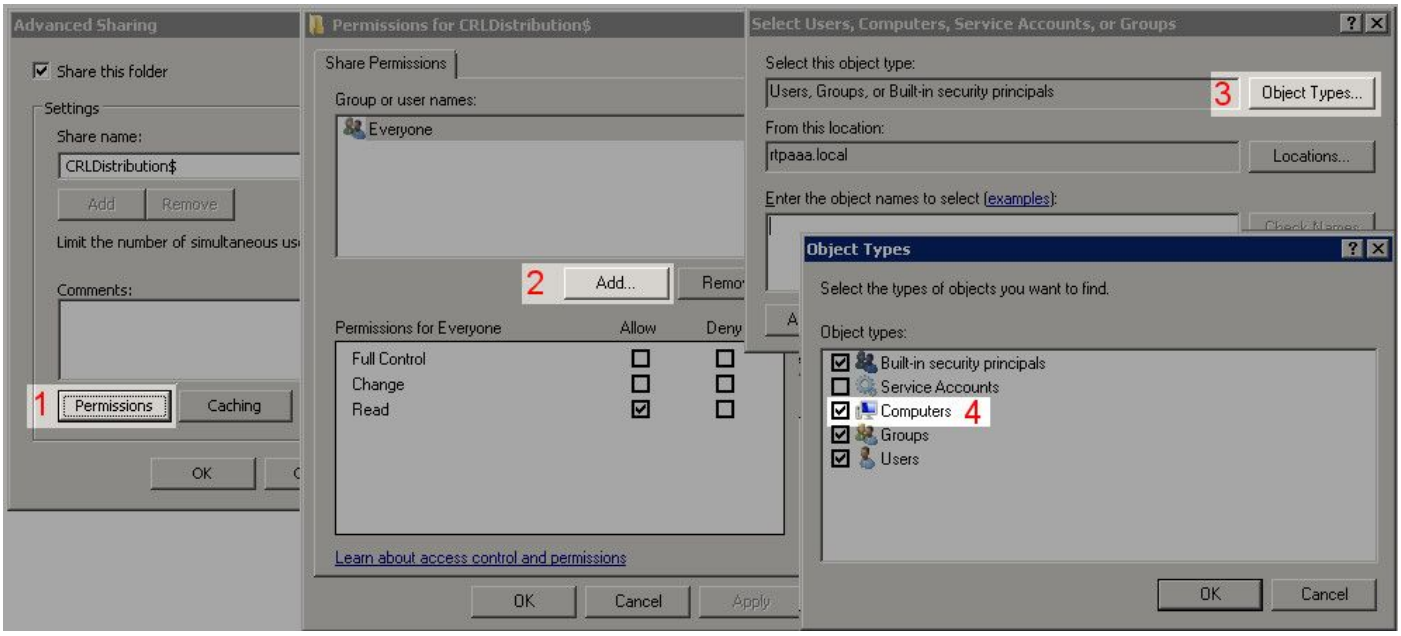
2. Damit die CA die CRL-Dateien in den neuen Ordner schreiben kann, muss die Freigabe aktiviert werden. Klicken Sie mit der rechten Maustaste auf den neuen Ordner, wählen Sie **Eigenschaften aus**, klicken Sie auf die Registerkarte **Freigabe** und klicken Sie dann auf **Erweiterte Freigabe**.



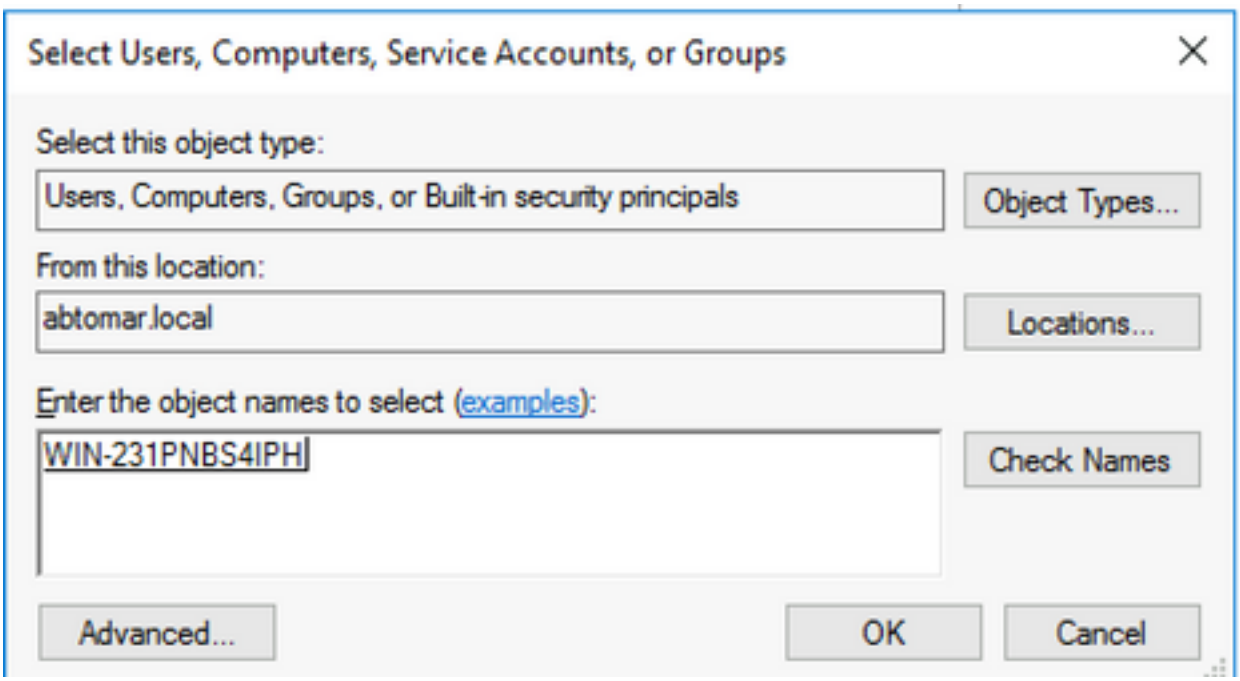
3. Um den Ordner freizugeben, aktivieren Sie das Kontrollkästchen **Diesen Ordner freigeben**, und fügen Sie dann im Feld Freigabename ein Dollarzeichen ($) zum Ende des Freigabenamens hinzu, um die Freigabe auszublenden.



4. Klicken Sie auf **Berechtigungen** (1), klicken Sie auf **Hinzufügen** (2), klicken Sie auf **Objekttypen** (3), und aktivieren Sie das Kontrollkästchen **Computer** (4).

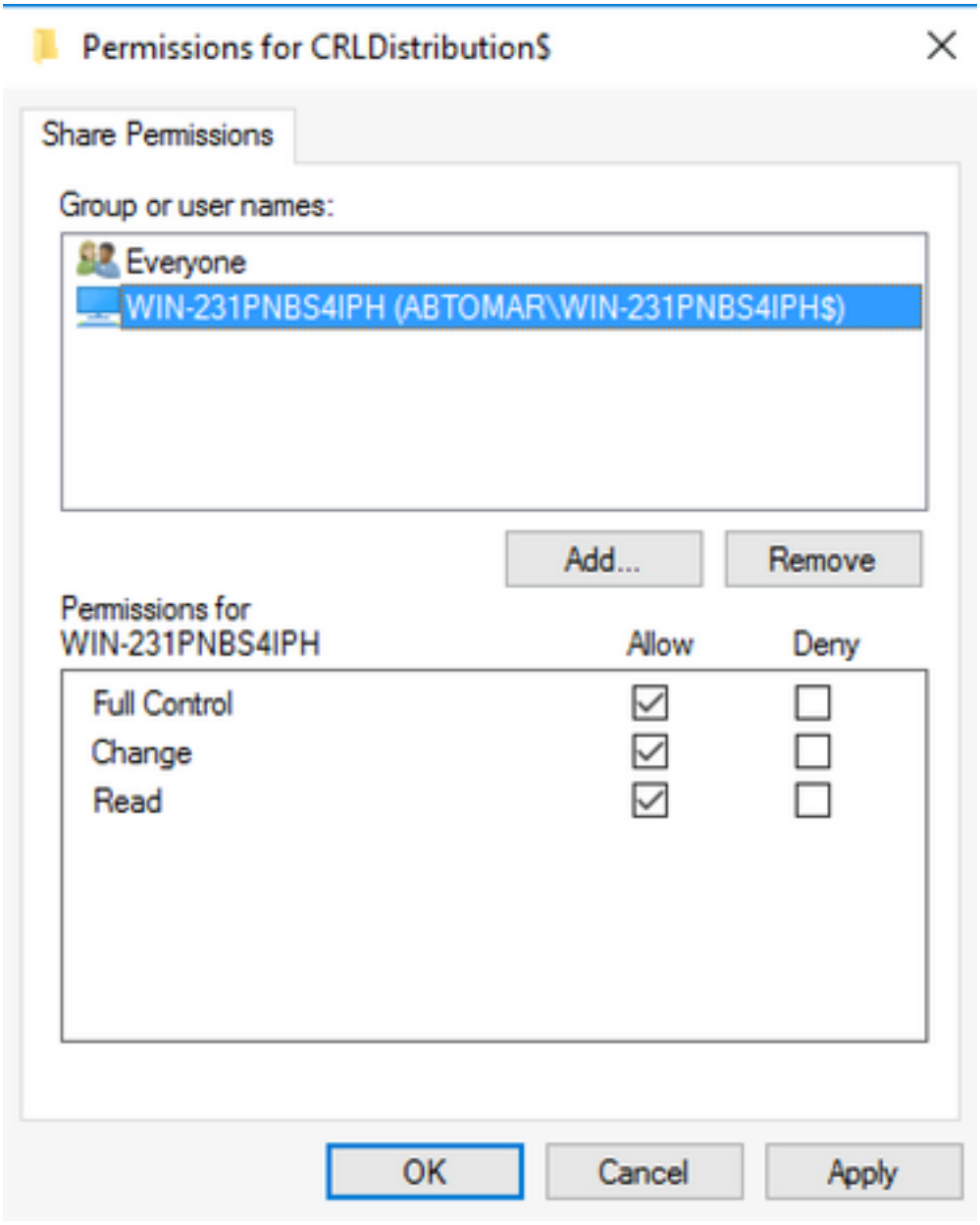


5. Um zum Fenster Benutzer, Computer, Dienstkonten oder Gruppen auswählen zurückzukehren, klicken Sie auf **OK**. Geben Sie im Feld Geben Sie die zu verwendenden Objektnamen ein den Computernamen des CA-Servers in diesem Beispiel ein: WIN0231PNBS4IPH und klicken Sie auf **Namen überprüfen**. Wenn der eingegebene Name gültig ist, wird der Name aktualisiert und unterstrichen angezeigt. Klicken Sie auf **OK**.



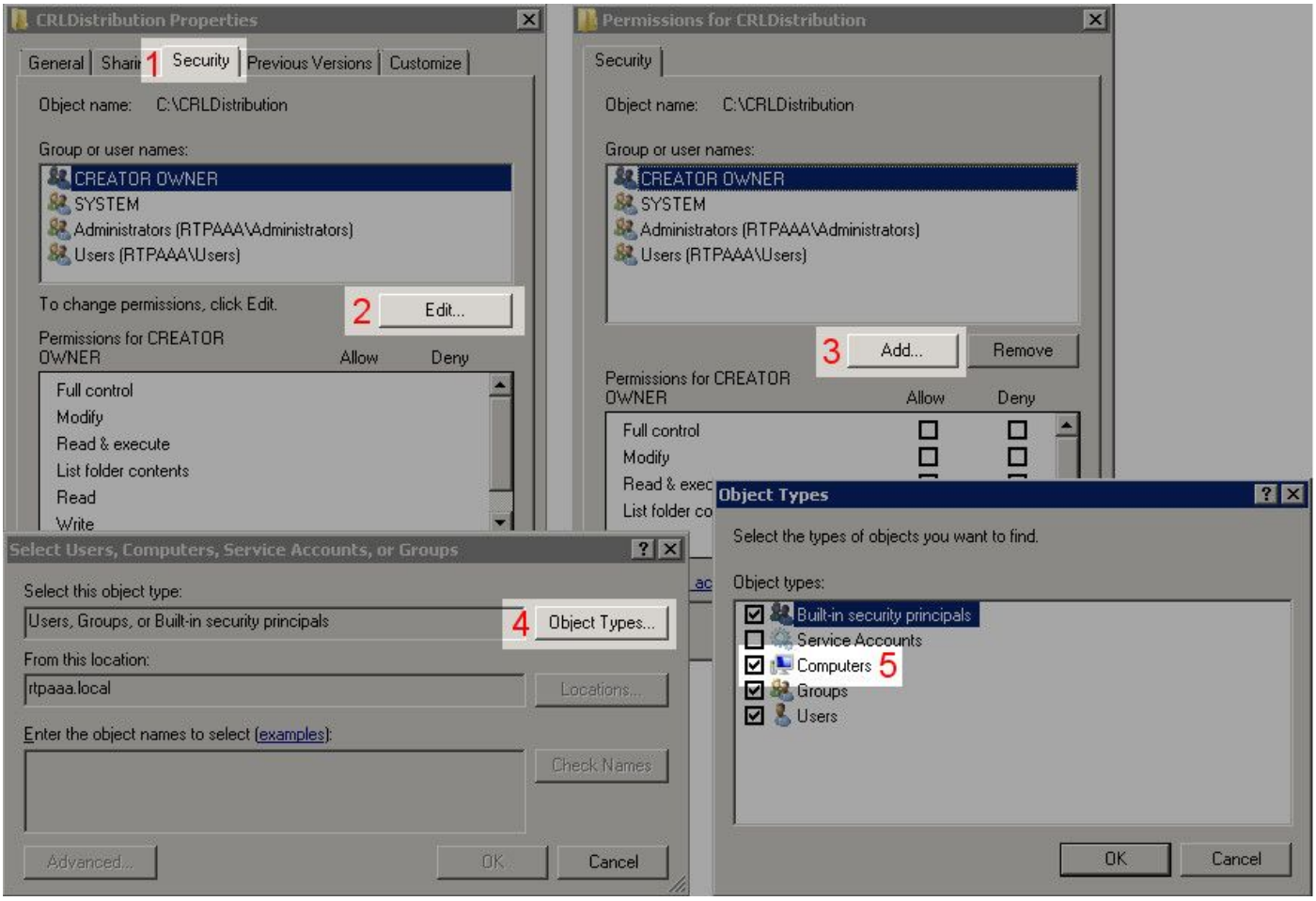
6. Wählen Sie im Feld Gruppe oder Benutzernamen den CA-Computer aus. Aktivieren Sie **Allow** for Full Control (Vollzugriff zulassen), um vollständigen Zugriff auf die CA zu gewähren.

Klicken Sie auf **OK**. Klicken Sie erneut auf **OK**, um das Fenster Erweiterte Freigabe zu schließen und zum Fenster Eigenschaften zurückzukehren.

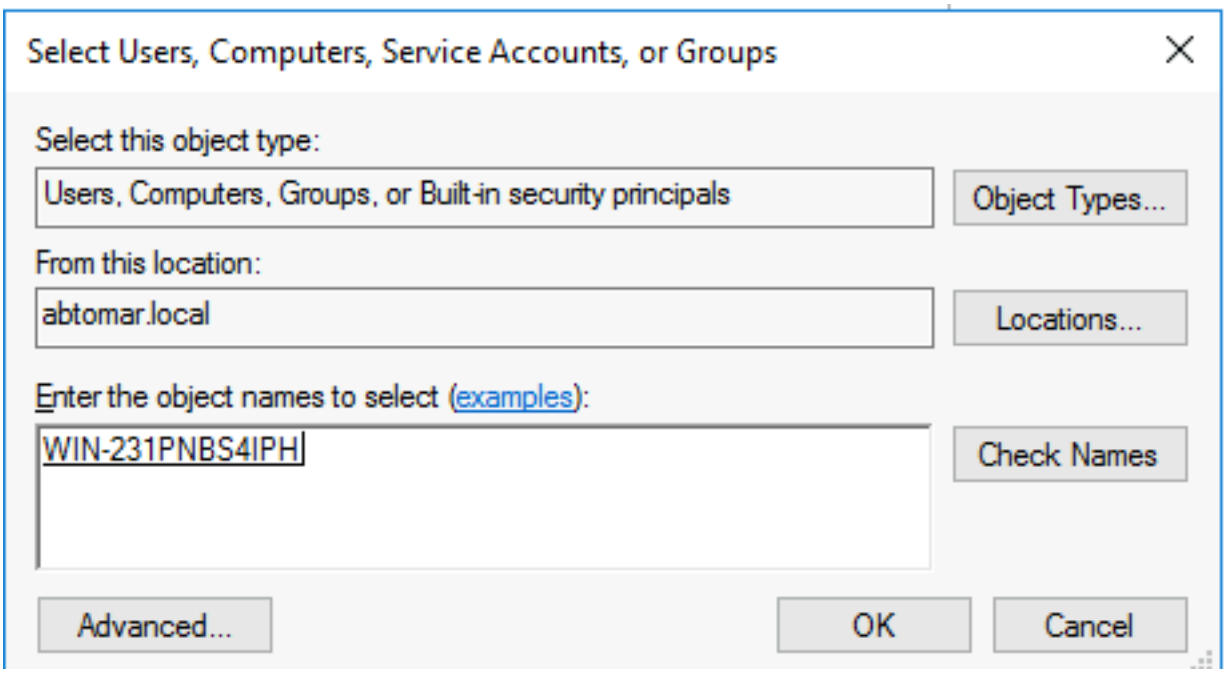


---

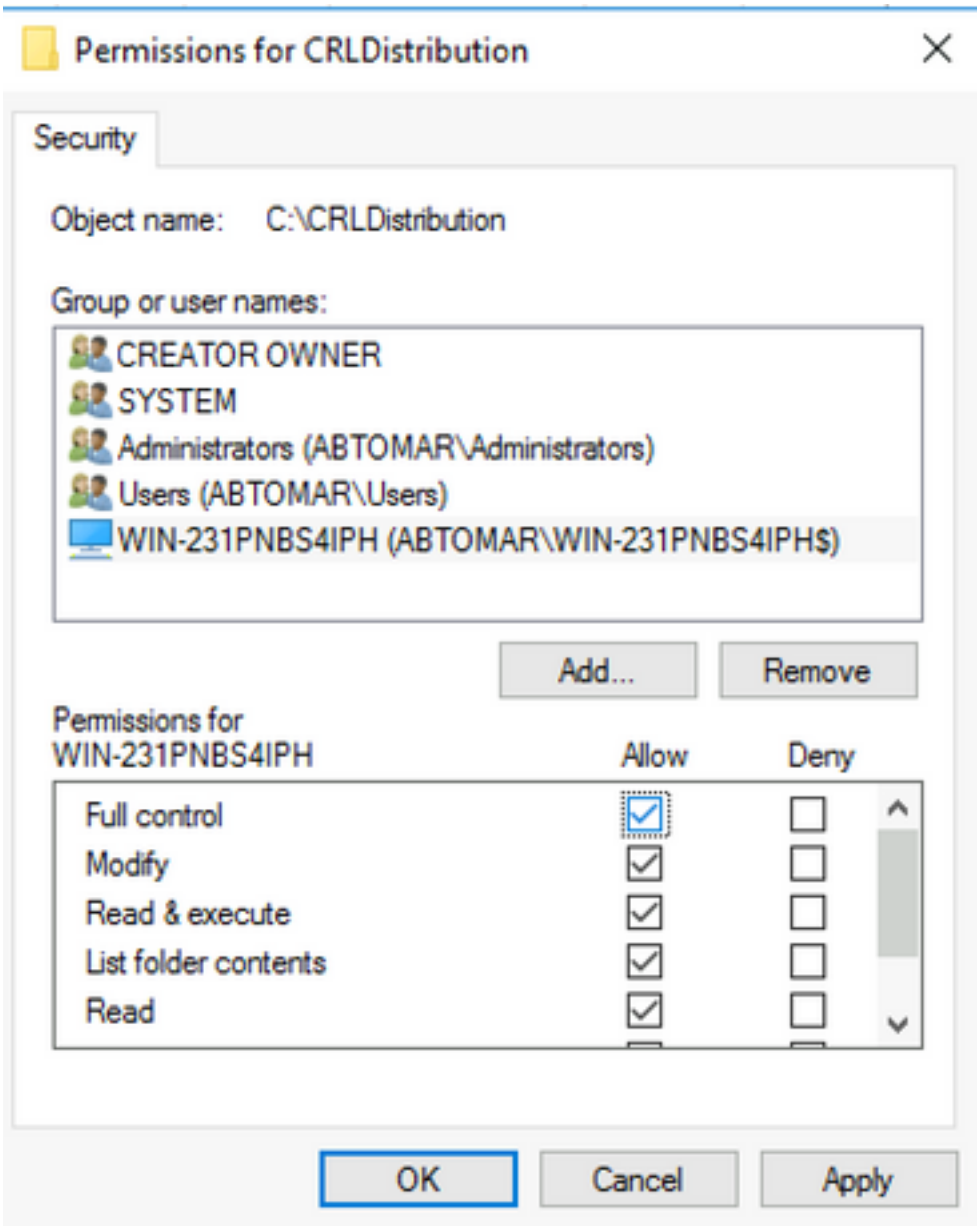
7. Damit die CA die CRL-Dateien in den neuen Ordner schreiben kann, konfigurieren Sie die entsprechenden Sicherheitsberechtigungen. Klicken Sie auf die Registerkarte **Sicherheit** (1), klicken Sie auf **Bearbeiten** (2), klicken Sie auf **Hinzufügen** (3), klicken Sie auf **Objekttypen** (4), und aktivieren Sie das **Kontrollkästchen Computer (5).**



8. Geben Sie im Feld Geben Sie die zu verwendenden Objektnamen ein den Computernamen des CA-Servers ein, und klicken Sie auf **Namen überprüfen**. Wenn der eingegebene Name gültig ist, wird der Name aktualisiert und unterstrichen angezeigt. Klicken Sie auf **OK**.



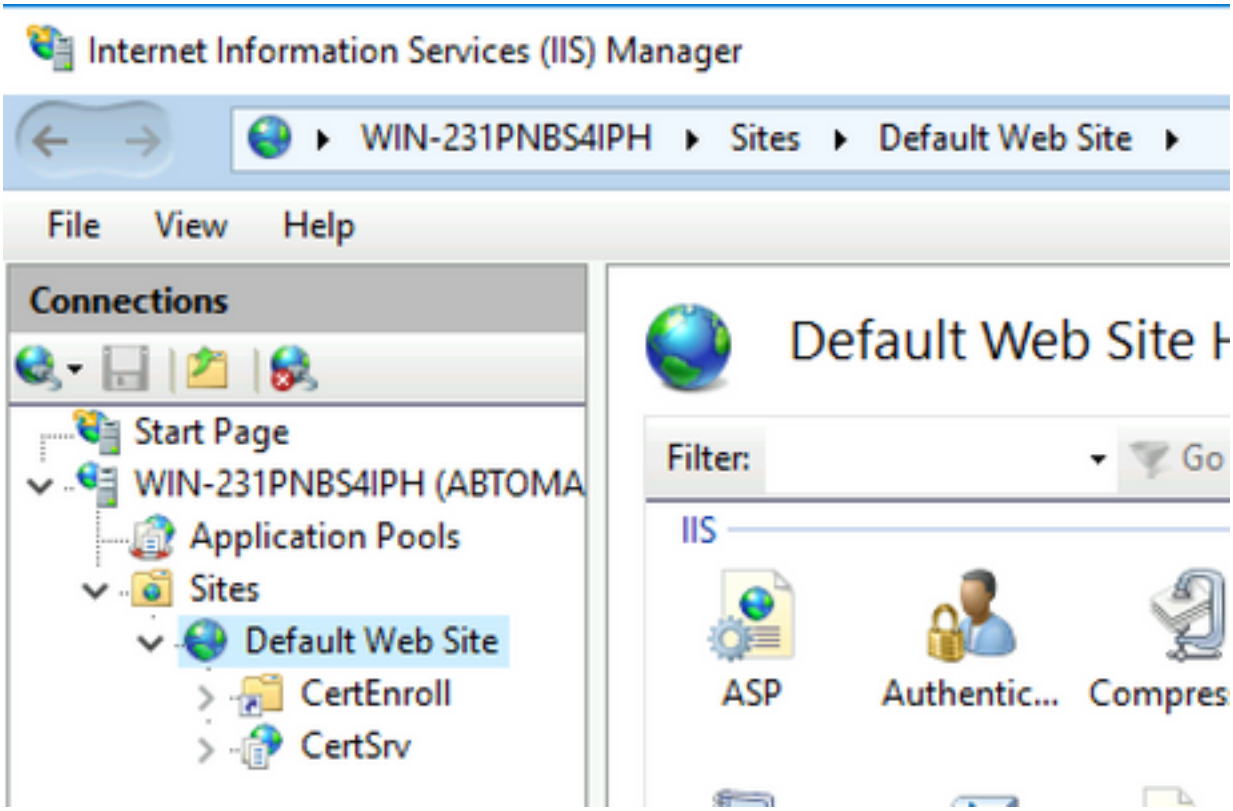
9. Wählen Sie den CA-Computer im Feld "Gruppe" oder im Feld "Benutzernamen" aus, und aktivieren Sie dann **Allow** for Full control, um vollständigen Zugriff auf die CA zu gewähren. Klicken Sie auf **OK** und dann auf **Schließen**, um den Vorgang abzuschließen.



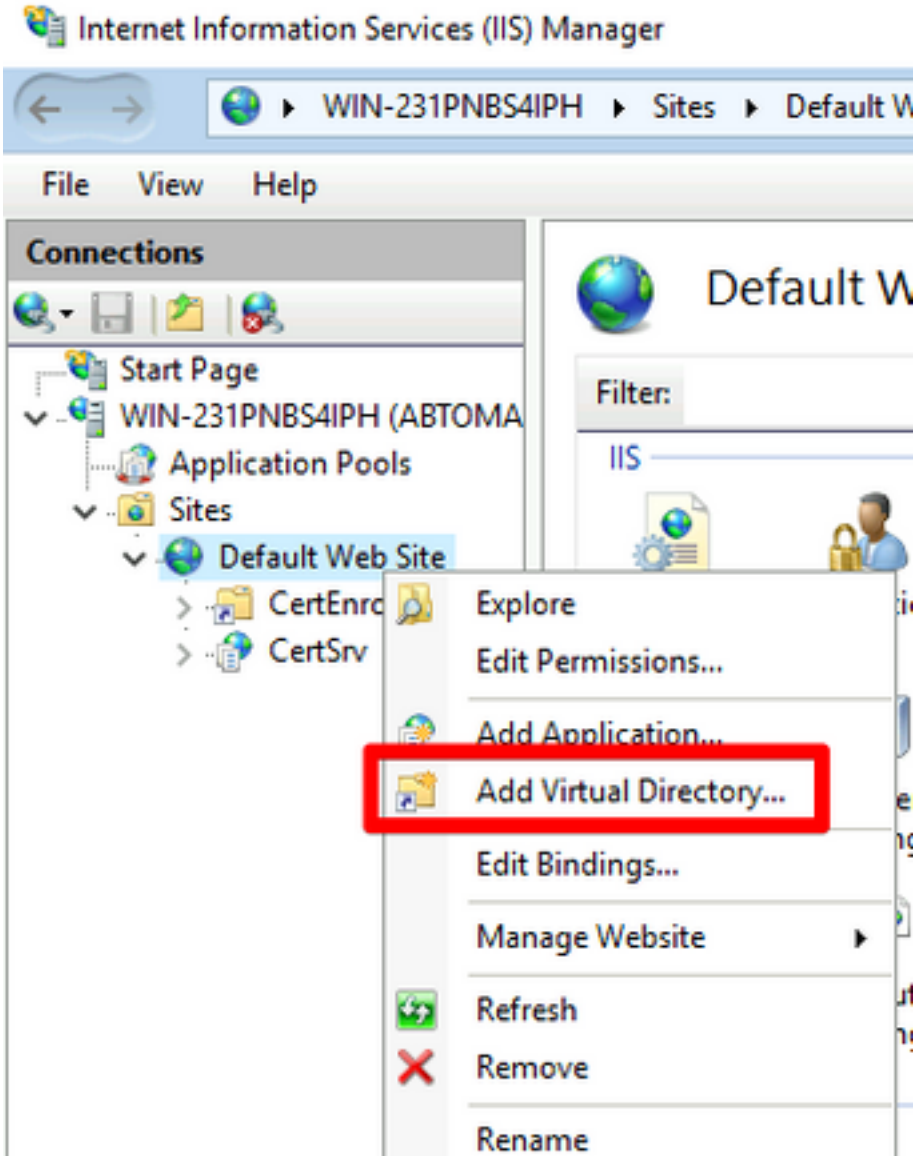
Erstellen einer Site in IIS, um den neuen CRL-Verteilungspunkt verfügbar zu machen

Damit ISE auf die CRL-Dateien zugreifen kann, müssen Sie das Verzeichnis, in dem sich die CRL-Dateien befinden, über IIS zugänglich machen.

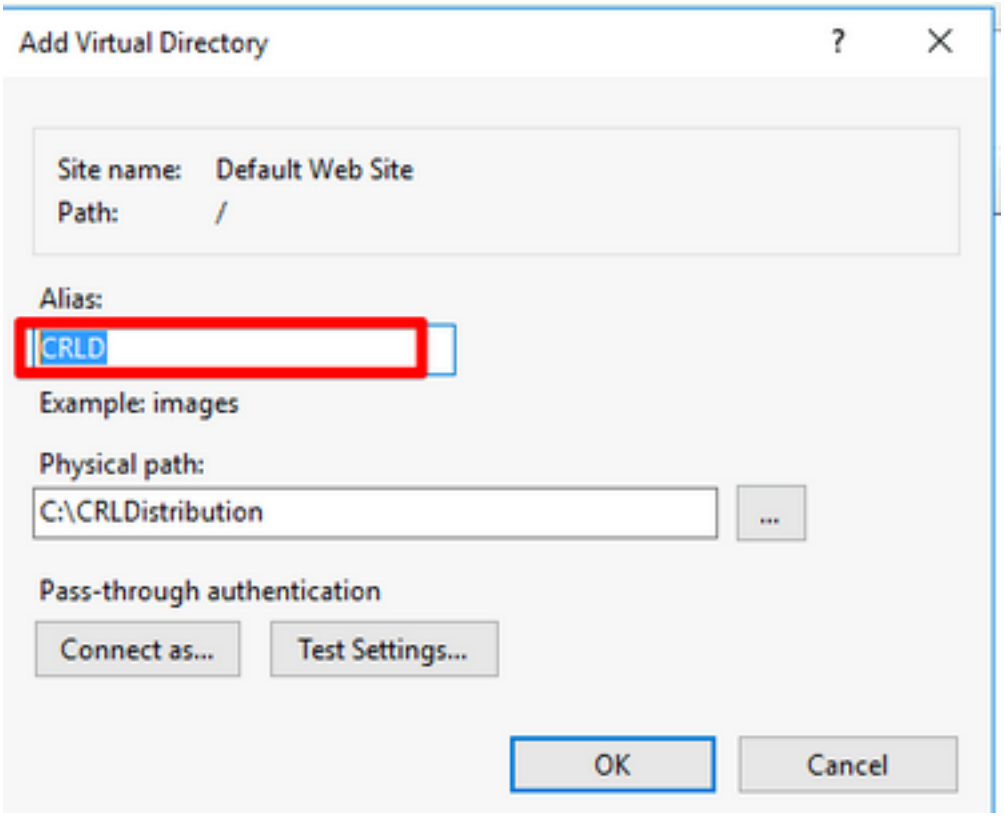
1. Klicken Sie in der Taskleiste des IIS-Servers auf **Start**. Wählen Sie **Verwaltung > Internetinformationsdienste (IIS)-Manager aus**.
2. Erweitern Sie im linken Bereich (Konsolenstruktur) den IIS-Servernamen, und erweitern Sie dann **Sites.**



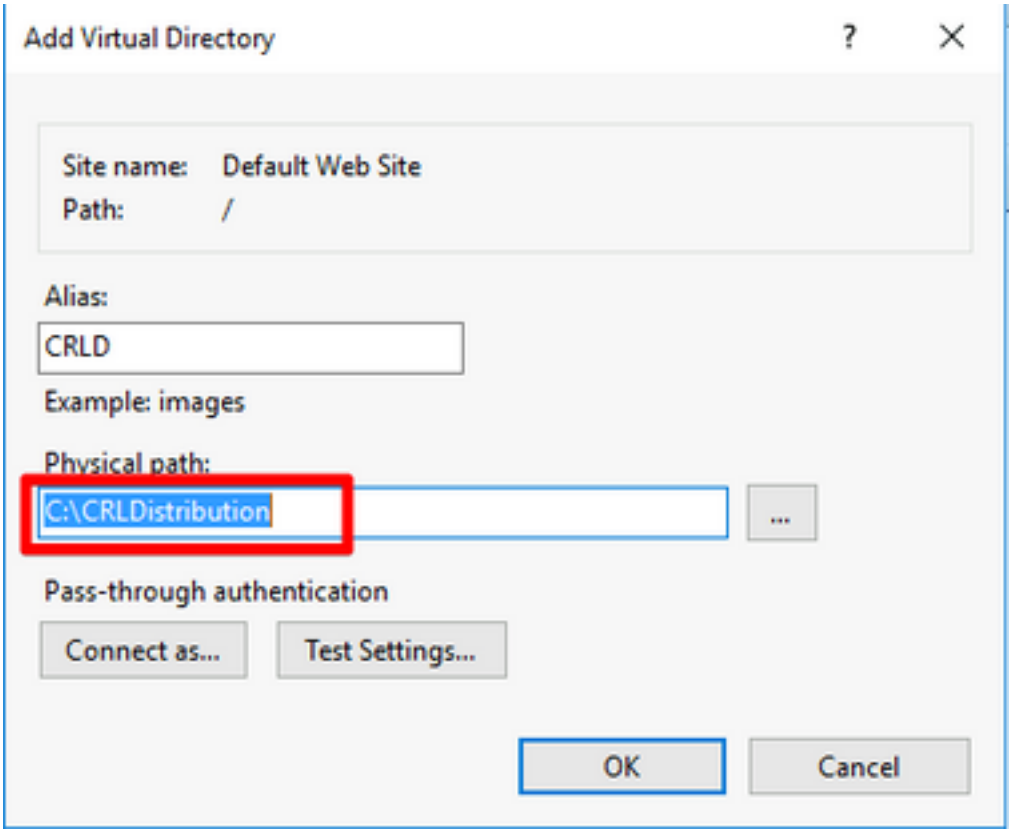
3. Klicken Sie mit der rechten Maustaste auf **Standardwebsite**, und wählen Sie **Virtuelles Verzeichnis hinzufügen aus**, wie in diesem Bild gezeigt.



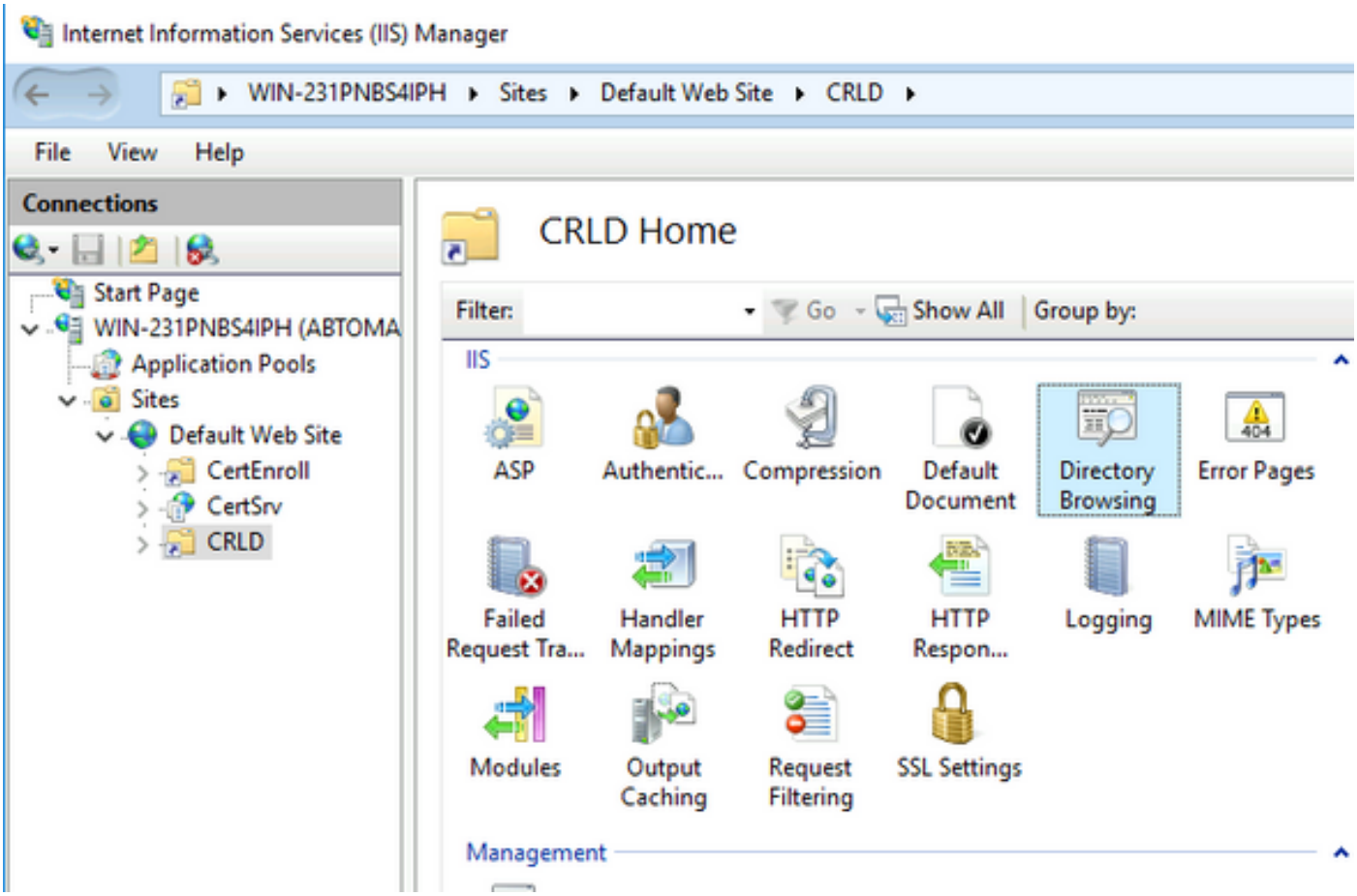
4. Geben Sie im Feld Alias einen Standortnamen für den CRL Distribution Point ein. In diesem Beispiel wird CRLD eingegeben.



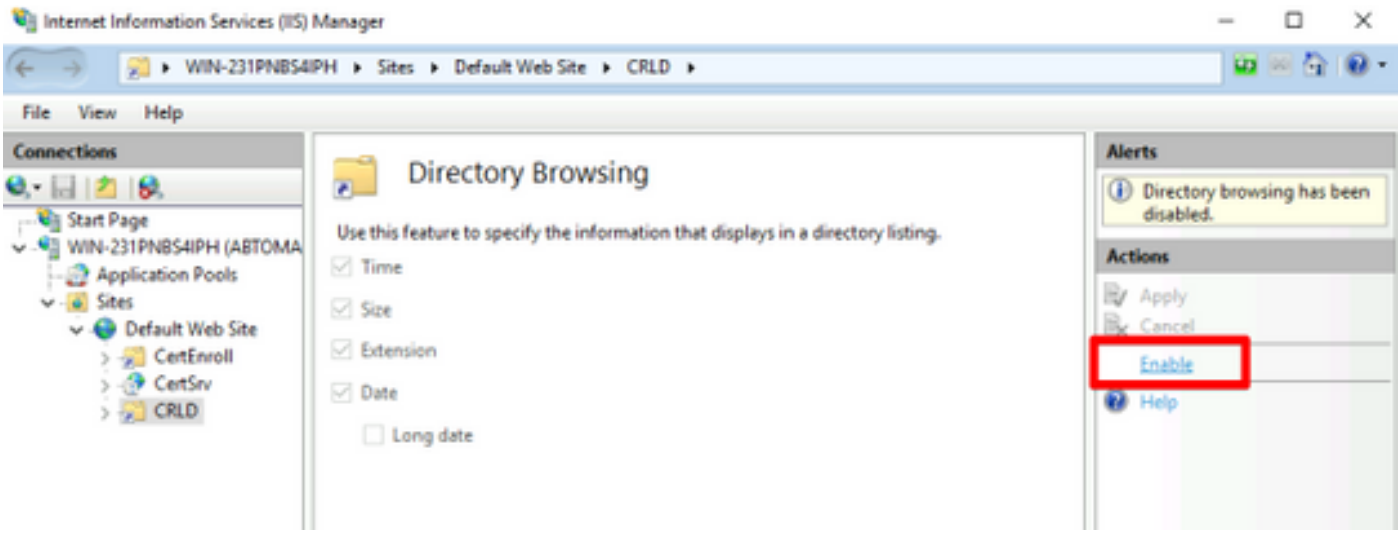
5. Klicken Sie auf die Auslassungszeichen (. . .) rechts neben dem Feld Physical path (Physischer Pfad) einen Ordner anlegen, der in Abschnitt 1 erstellt wurde. Wählen Sie den Ordner aus, und klicken Sie auf **OK**. Klicken Sie auf **OK**, um das Fenster Virtuelles Verzeichnis hinzufügen zu schließen.



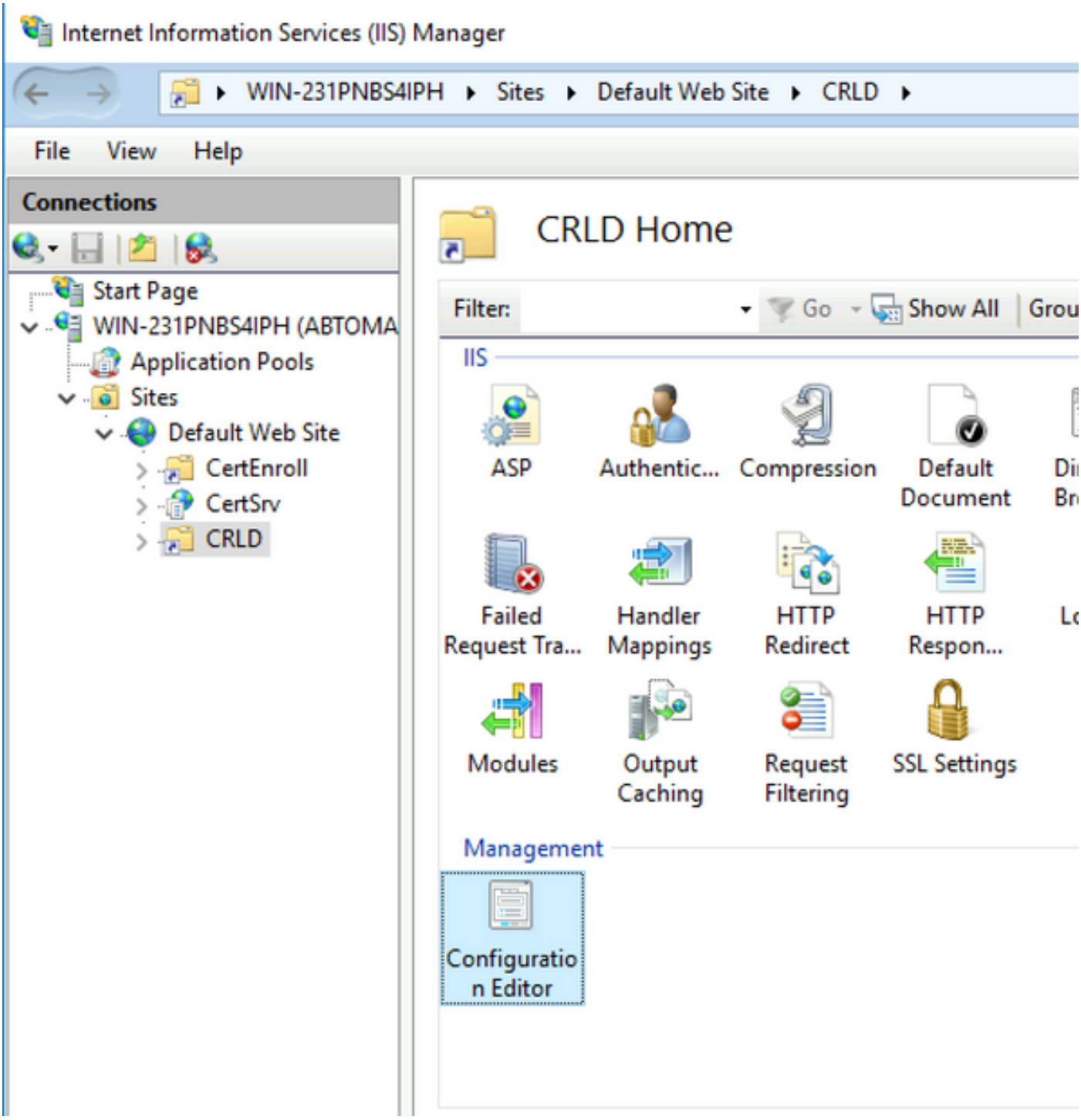
6. Der in Schritt 4 eingegebene Standortname muss im linken Bereich hervorgehoben werden. Wenn nicht, wählen Sie es jetzt aus. Doppelklicken Sie im mittleren Bereich auf **Verzeichnissuche**.



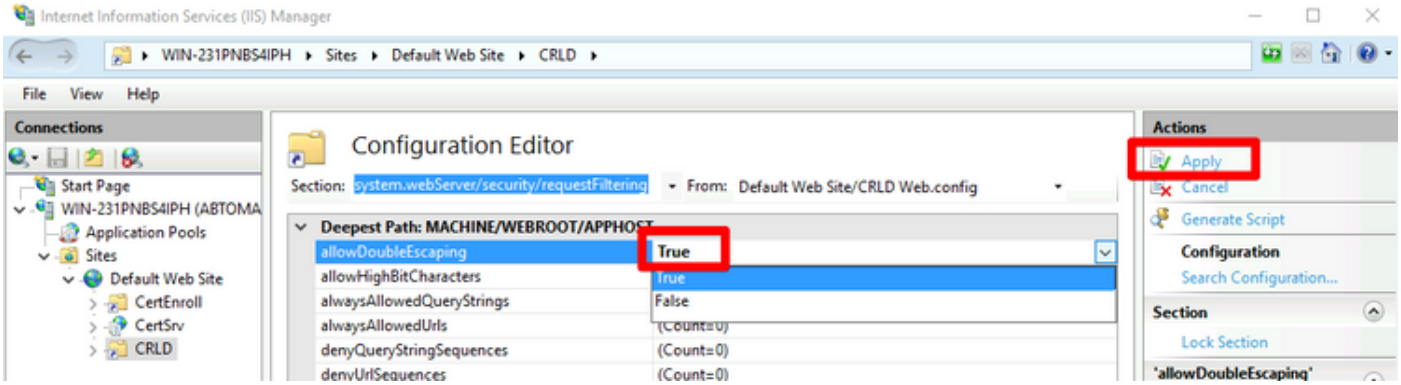
7. Klicken Sie im rechten Teilfenster auf **Aktivieren**, um die Verzeichnissuche zu aktivieren.



8. Wählen Sie im linken Teilfenster erneut den Standortnamen aus. Doppelklicken Sie im mittleren Bereich auf **Konfigurationseditor**.



9. Wählen Sie in der Dropdown-Liste Abschnitt die Option **system.webServer/security/requestFiltering aus**. Wählen Sie in der Dropdownliste **allowDoubleEscaping** die Option **True aus**. Klicken Sie im rechten Teilfenster auf **Übernehmen**, wie in diesem Bild gezeigt.

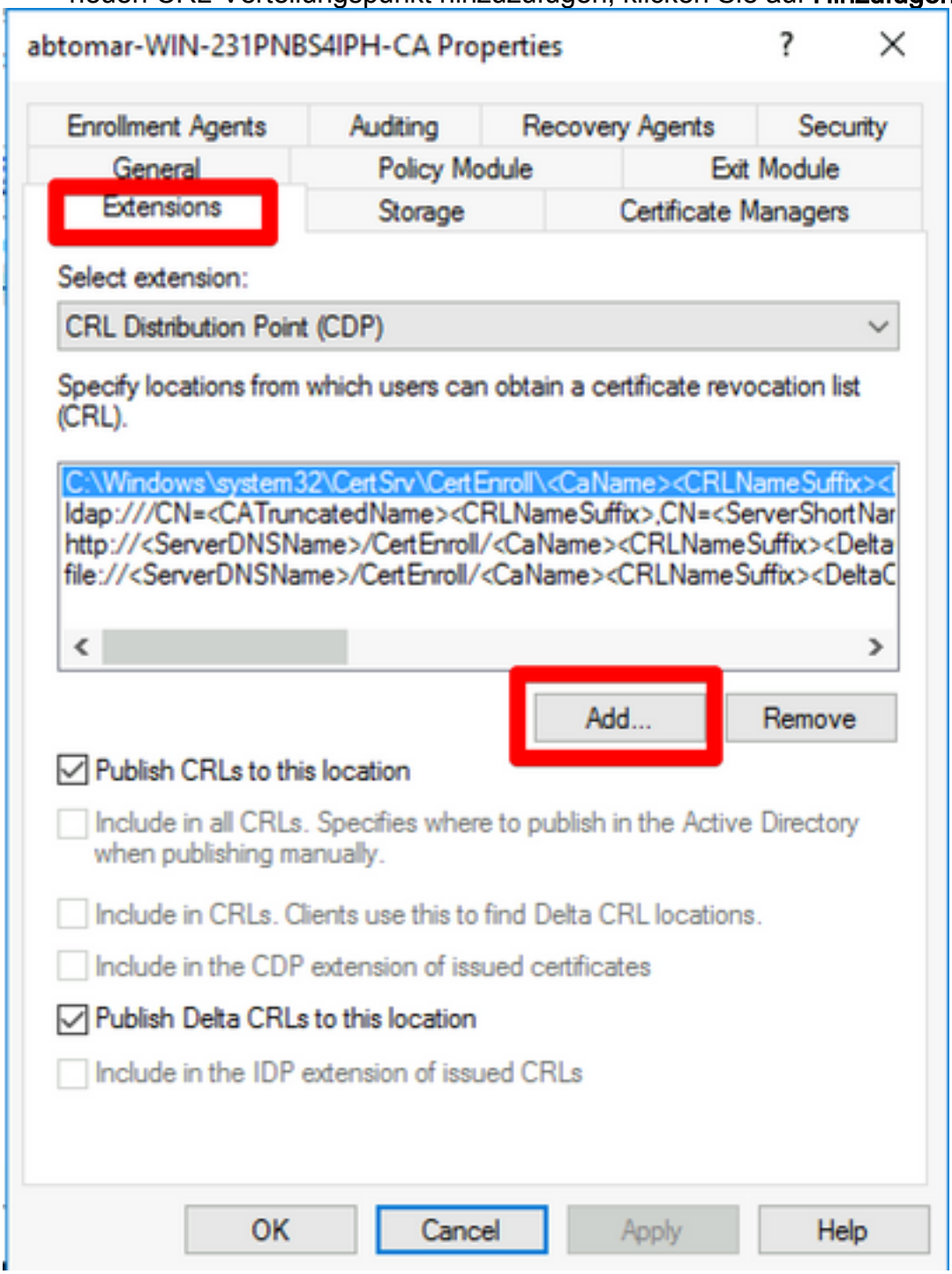


Der Zugriff auf den Ordner muss jetzt über IIS möglich sein.

Konfigurieren des Microsoft CA-Servers zum Veröffentlichen von CRL-Dateien am Distribution Point

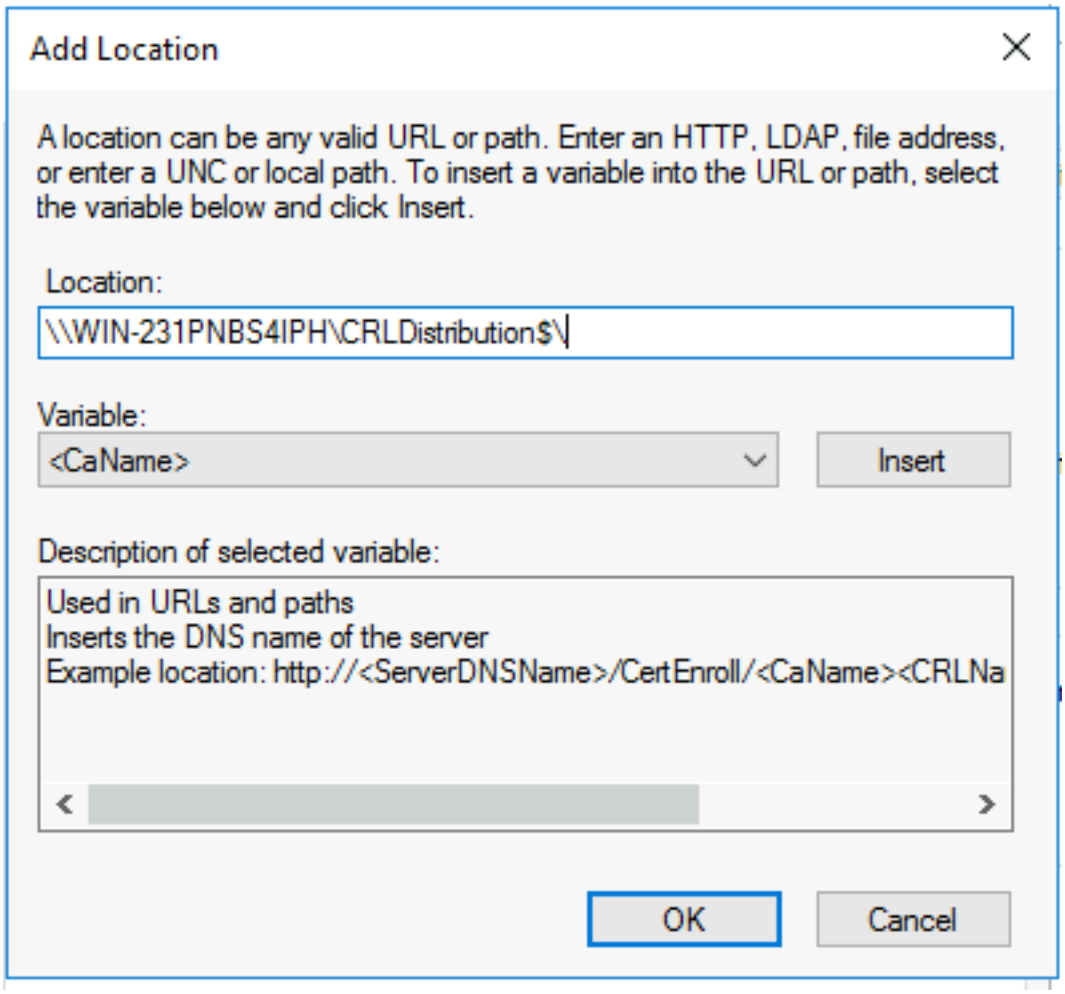
Nachdem ein neuer Ordner konfiguriert wurde, in dem die CRL-Dateien gespeichert sind und der Ordner in IIS verfügbar gemacht wurde, konfigurieren Sie den Microsoft CA-Server so, dass die CRL-Dateien am neuen Speicherort veröffentlicht werden.

1. Klicken Sie in der Taskleiste des CA-Servers auf **Start**. Wählen Sie **Verwaltung > Zertifizierungsstelle aus**.
2. Klicken Sie im linken Teilfenster mit der rechten Maustaste auf den Namen der CA. Wählen Sie **Eigenschaften** aus, und klicken Sie dann auf die Registerkarte **Erweiterungen**. Um einen neuen CRL-Verteilungspunkt hinzuzufügen, klicken Sie auf **Hinzufügen**.

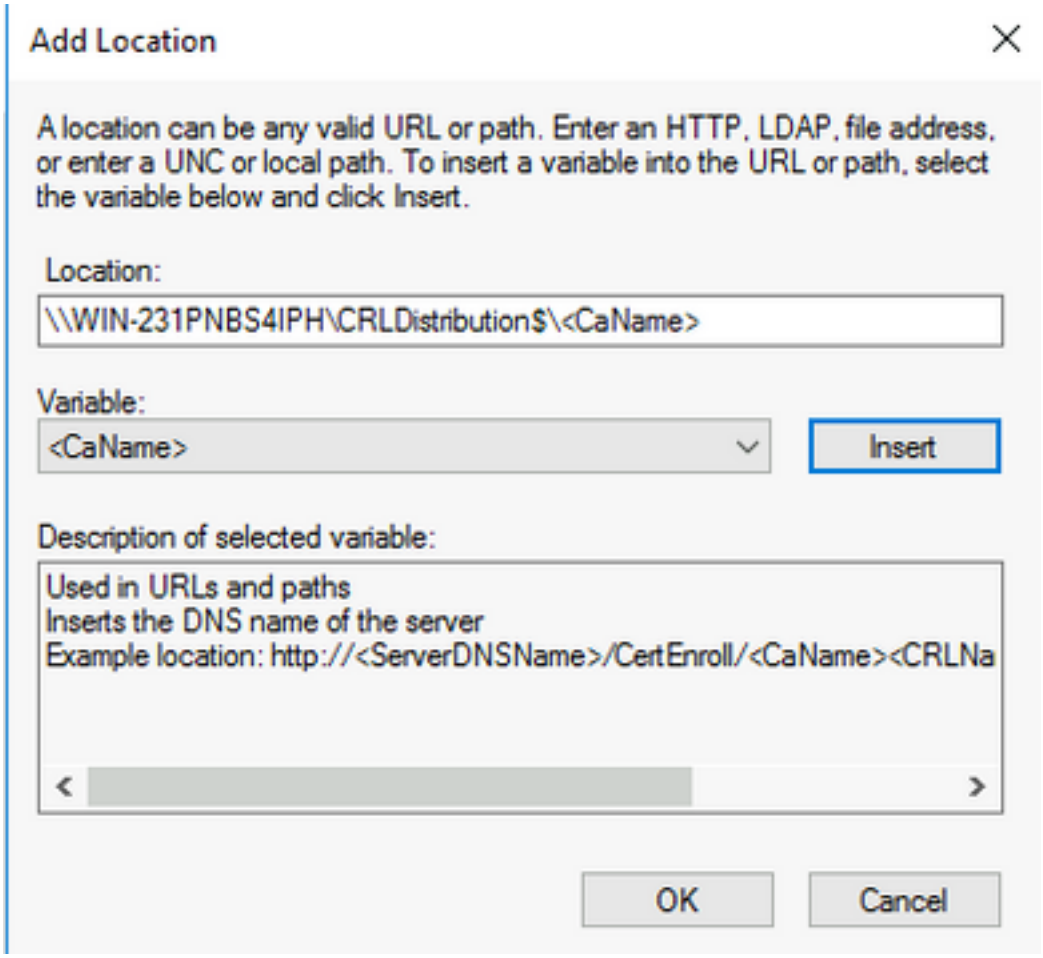


3. Geben Sie im Feld Speicherort den Pfad zu dem Ordner ein, der in Abschnitt 1 erstellt und freigegeben wurde. Im Beispiel in Abschnitt 1 lautet der Pfad:

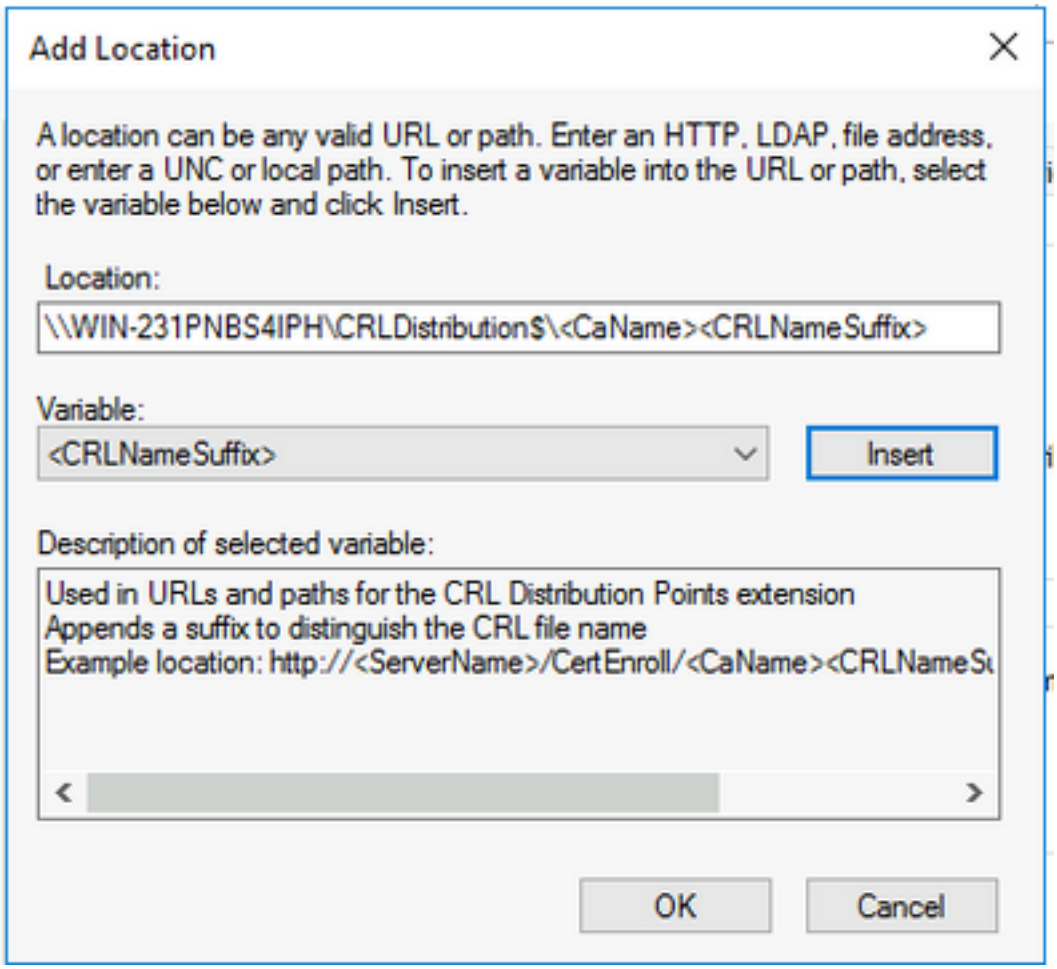
\\WIN-231PNBS4IPH\CRLDistribution



4. Wenn das Feld Speicherort ausgefüllt ist, wählen Sie **<CaName>** aus der Dropdown-Liste Variable aus, und klicken Sie dann auf **Einfügen.**

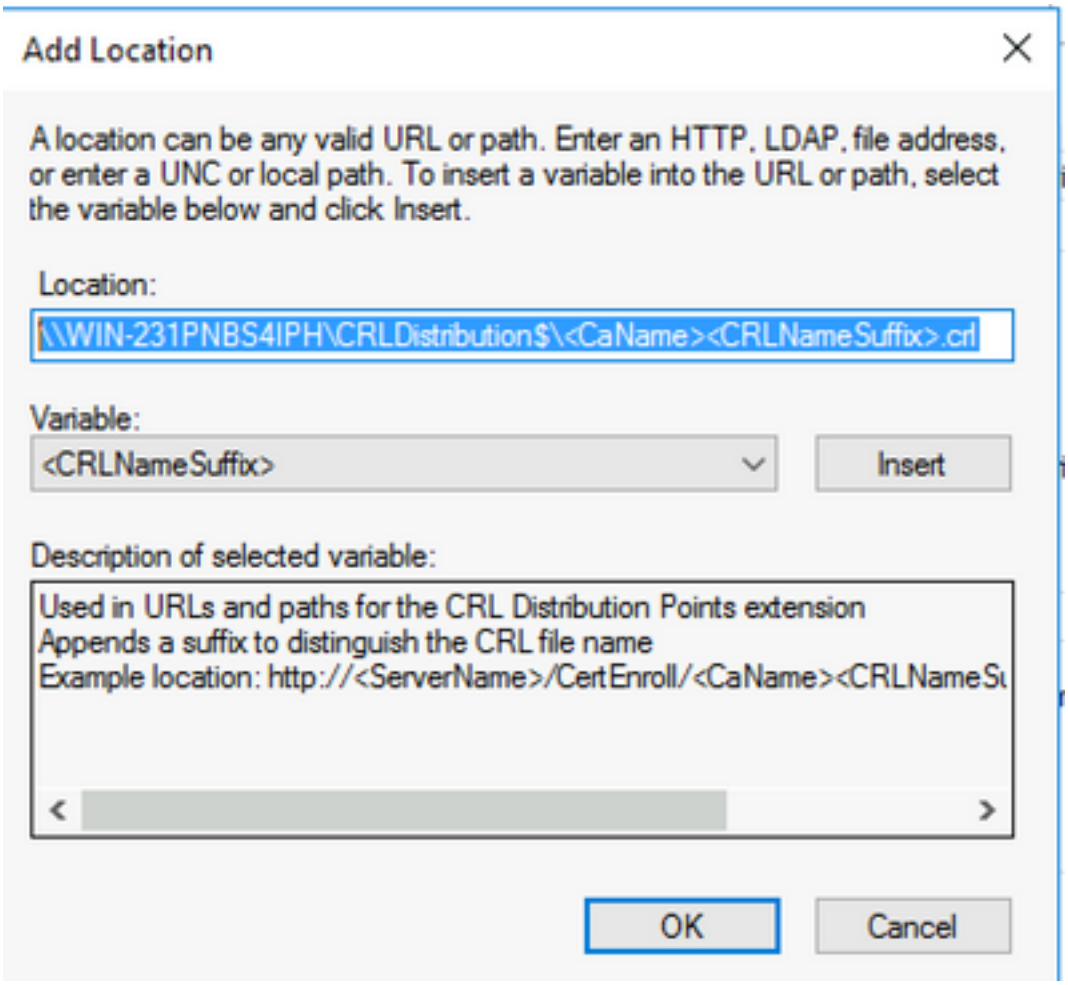


5. Wählen Sie aus der Dropdown-Liste Variable die Option **<CRLNameSuffix>** und klicken Sie dann auf **Einfügen**.



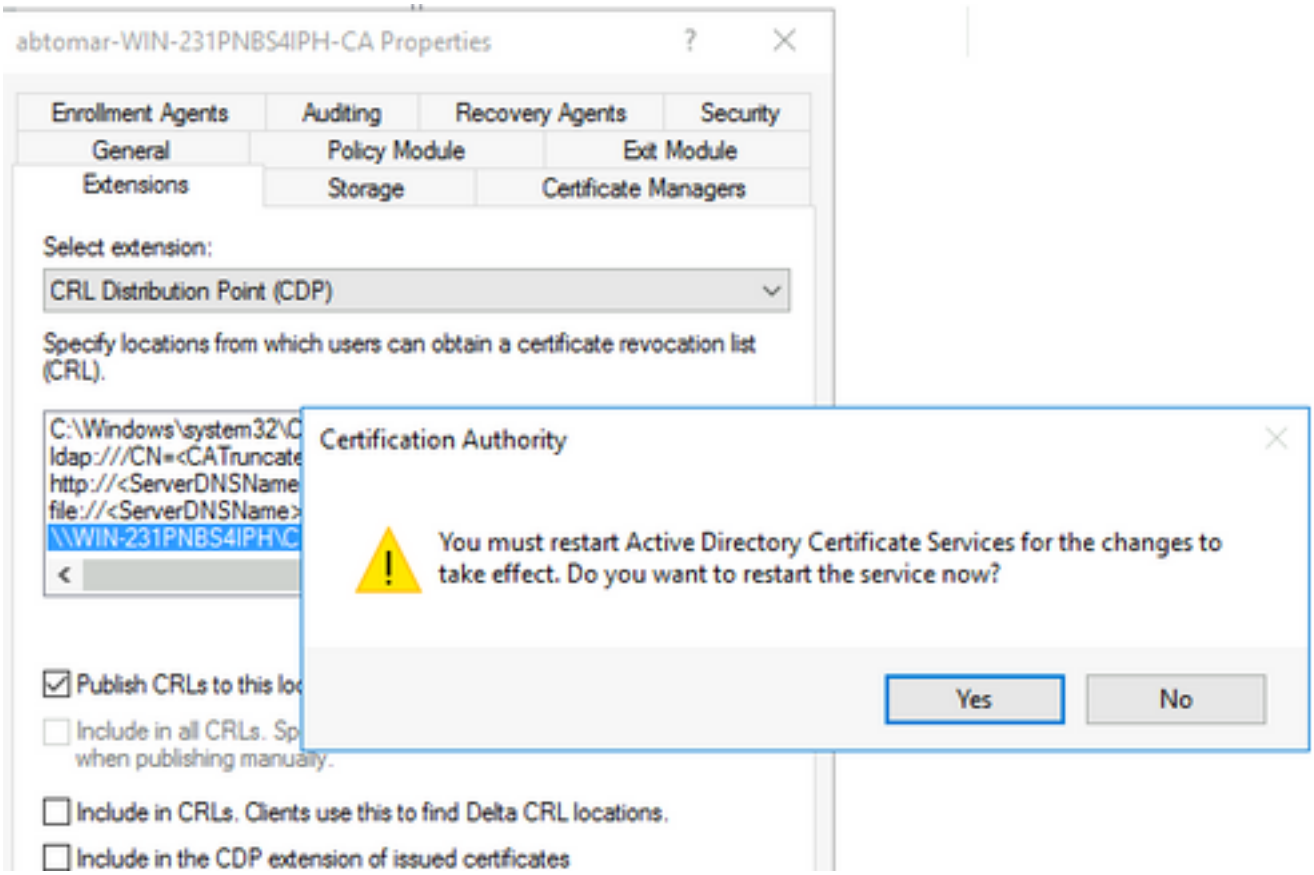
6. Im Feld Location (Speicherort) wird **.crl** am Ende des Pfads angehängt. In diesem Beispiel lautet der Location:

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

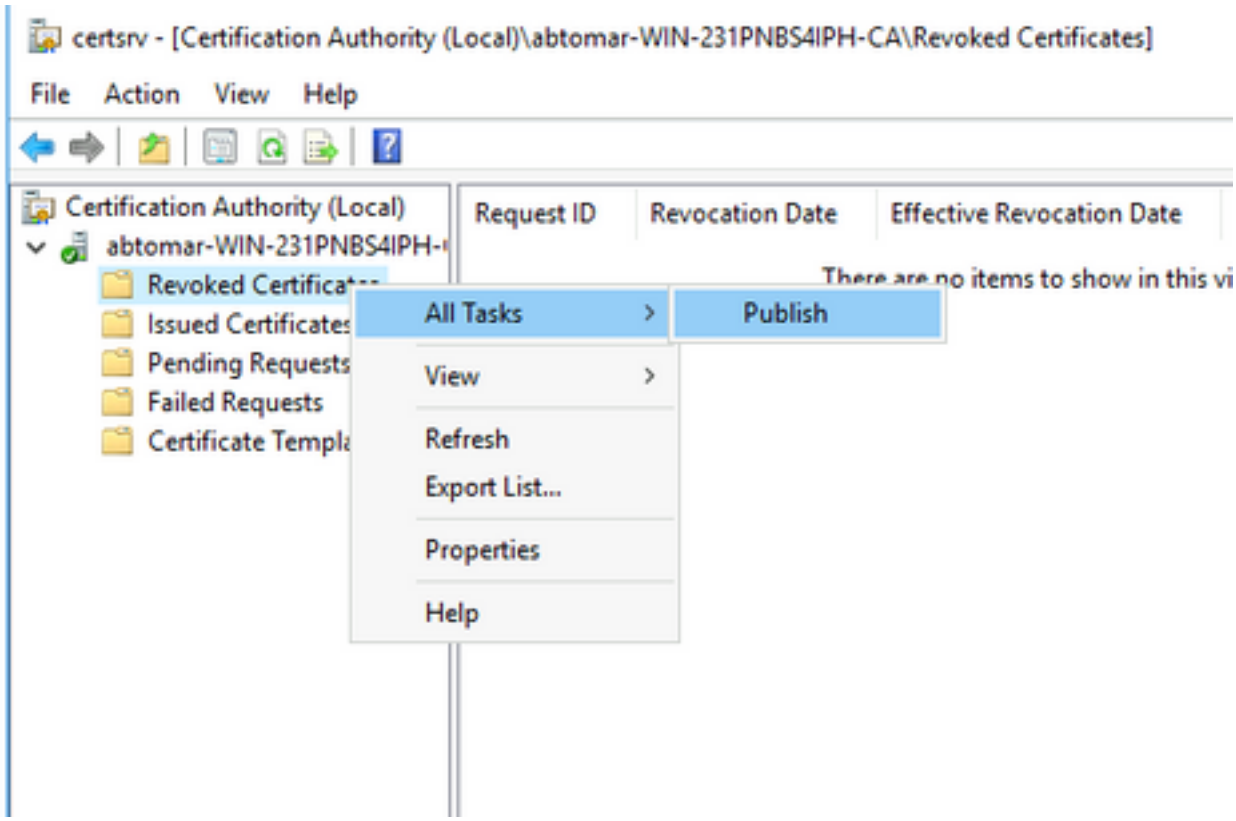


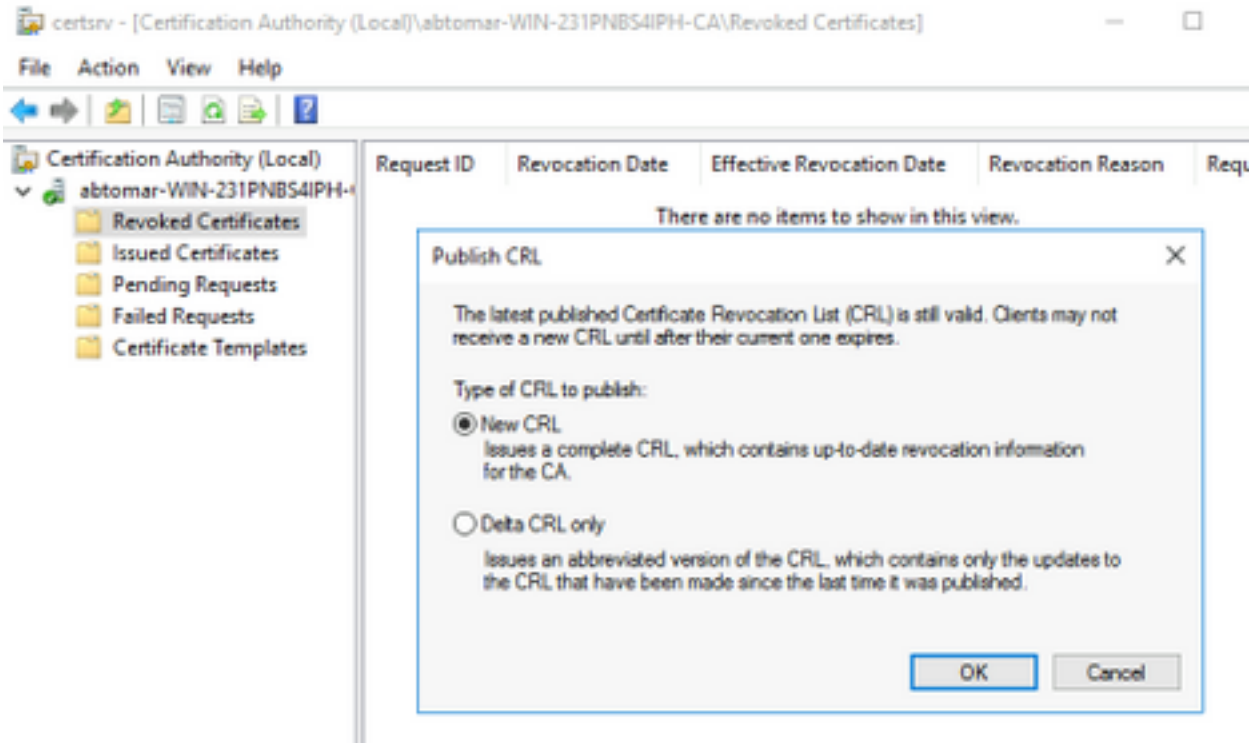
7. Klicken Sie auf **OK**, um zur Registerkarte Erweiterungen zurückzukehren. Aktivieren Sie das Kontrollkästchen **CRLs an diesem Speicherort veröffentlichen**, und klicken Sie dann auf **OK**, um das Eigenschaftenfenster zu schließen.

Eine Eingabeaufforderung wird angezeigt, um die Berechtigung zum Neustart der Active Directory-Zertifizierungsdienste zu erhalten. Klicken Sie auf **Ja**.



8. Klicken Sie im linken Teilfenster mit der rechten Maustaste auf **Widergerufene Zertifikate**. Wählen Sie **Alle Aufgaben > Veröffentlichen aus**. Stellen Sie sicher, dass New CRL (Neue CRL) ausgewählt ist, und klicken Sie dann auf **OK.**





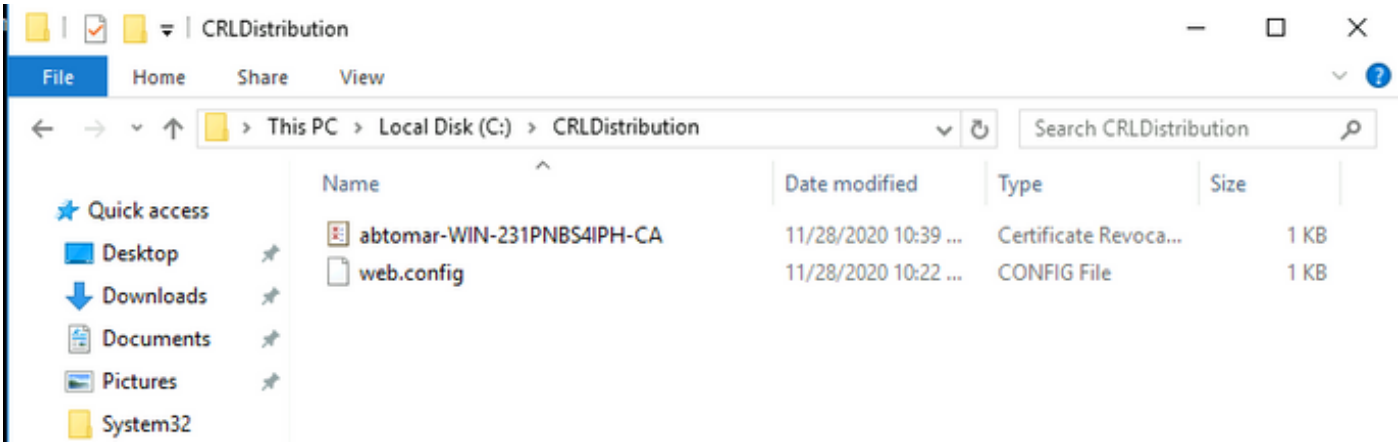
Der Microsoft CA-Server muss im Ordner, der in Abschnitt 1 erstellt wurde, eine neue Crl-Datei erstellen. Wenn die neue CRL-Datei erfolgreich erstellt wurde, wird nach dem Klicken auf OK kein Dialog angezeigt. Wenn in Bezug auf den neuen Verteilungspunkt-Ordner ein Fehler zurückgegeben wird, wiederholen Sie jeden Schritt in diesem Abschnitt sorgfältig.

Überprüfen Sie, ob die CRL-Datei vorhanden ist und über IIS zugänglich ist.

Überprüfen Sie, ob die neuen CRL-Dateien vorhanden sind und ob sie über IIS von einer anderen Workstation aus zugänglich sind, bevor Sie diesen Abschnitt starten.

1. Öffnen Sie auf dem IIS-Server den in Abschnitt 1 erstellten Ordner. Es muss eine einzige Crl-Datei mit dem Formular **<CANAME>.crl** vorhanden sein, wobei <CANAME> der Name des CA-Servers ist. In diesem Beispiel lautet der Dateiname:

abtomar-WIN-231PNBS4IPH-CA.crl



2. Öffnen Sie von einer Workstation im Netzwerk (idealerweise im selben Netzwerk wie der primäre ISE-Admin-Knoten) einen Webbrowser, und navigieren Sie zu http://<SERVER>/<CRLSITE>, wobei <SERVER> der in Abschnitt 2 konfigurierte Servername des IIS-Servers ist und <CRLSITE> der für den Verteilungspunkt in Abschnitt 2 ausgewählte Standortname ist. In diesem Beispiel lautet die URL:

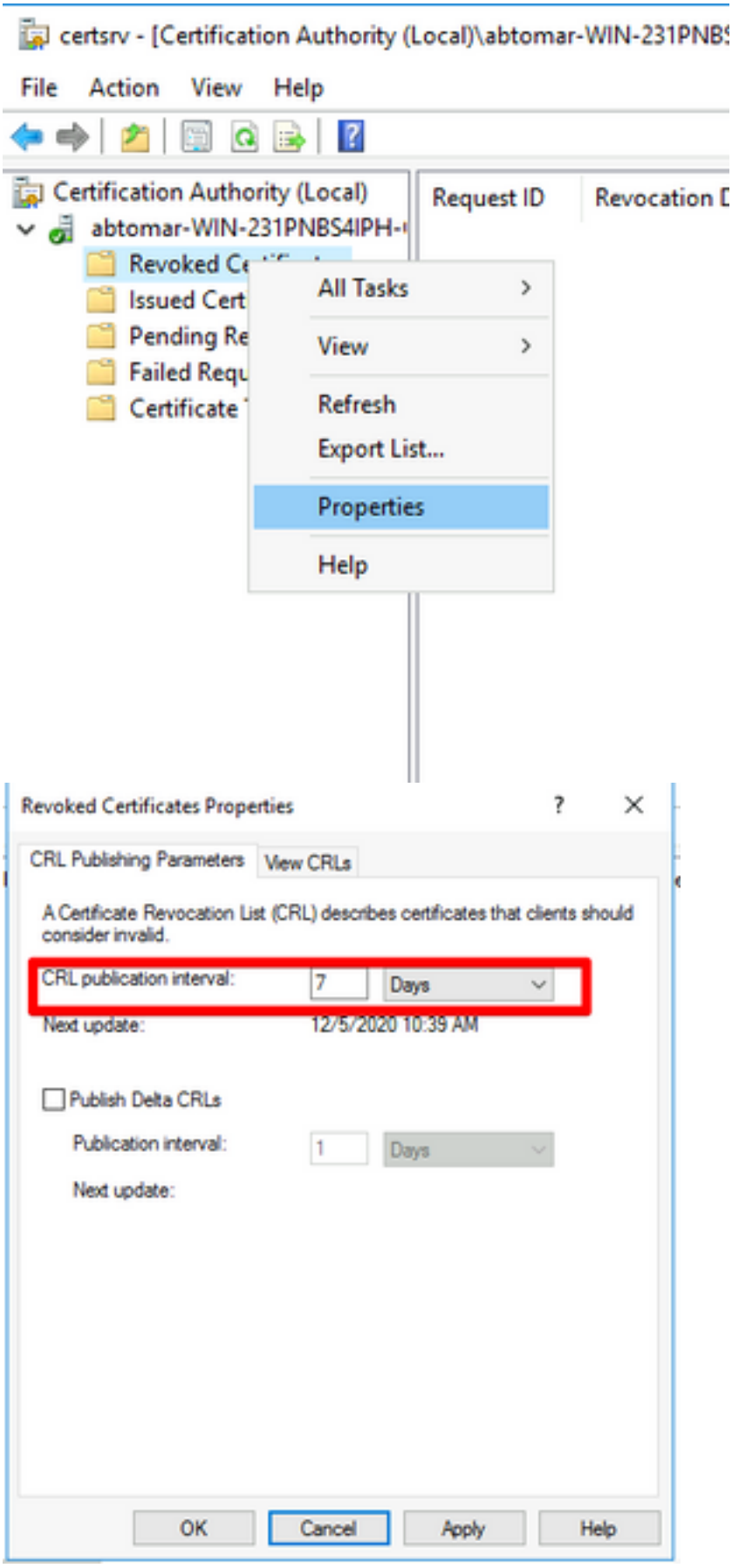
http://win-231pnbs4iph/CRLD

Der Verzeichnisindex wird angezeigt, der die in Schritt 1 beobachtete Datei enthält.

Konfigurieren der ISE zur Verwendung des neuen CRL Distribution Point

Bevor die ISE zum Abrufen der CRL konfiguriert wird, legen Sie das Intervall für die Veröffentlichung der CRL fest. Die Strategie, dieses Intervall zu bestimmen, geht über den Rahmen dieses Dokuments hinaus. Die potenziellen Werte (in Microsoft CA) liegen zwischen 1 Stunde und 411 Jahren einschließlich. Der Standardwert ist 1 Woche. Nachdem Sie ein geeignetes Intervall für Ihre Umgebung festgelegt haben, legen Sie das Intervall mit den folgenden Anweisungen fest:

1. Klicken Sie in der Taskleiste des CA-Servers auf **Start**. Wählen Sie **Verwaltung > Zertifizierungsstelle aus**.
2. Erweitern Sie im linken Teilfenster die CA. Klicken Sie mit der rechten Maustaste auf den Ordner **Freigegebene Zertifikate**, und wählen Sie **Eigenschaften aus.**
3. Geben Sie in die Felder für das CRL-Veröffentlichungsintervall die gewünschte Nummer ein, und wählen Sie den Zeitraum aus. Klicken Sie auf **OK**, um das Fenster zu schließen und die Änderung zu übernehmen. In diesem Beispiel wird ein Veröffentlichungsintervall von 7 Tagen konfiguriert.



4. Geben Sie den Befehl **certutil -getreg CA\Clock*** ein, um den ClockSkew-Wert zu bestätigen. Der Standardwert ist 10 Minuten.

Beispielausgabe:

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

5. Geben Sie den Befehl **certutil -getreg CA\CRLov*** ein, um zu überprüfen, ob die CRLOverlapPeriod manuell festgelegt wurde. Standardmäßig ist der CRLOverlapUnit-Wert 0, der angibt, dass kein manueller Wert festgelegt wurde. Wenn der Wert ein anderer Wert als 0 ist, notieren Sie den Wert und die Einheiten.

Beispielausgabe:

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

6. Geben Sie den Befehl **certutil -getreg CA\CRLpe*** ein, um den in Schritt 3 festgelegten CRLPeriod zu überprüfen.

Beispielausgabe:

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

7. Berechnen Sie den CRL-Kulanzzeitraum wie folgt:

a) Wenn CRLOverlapPeriod in Schritt 5 festgelegt wurde: OVERLAP = CRLOverlapPeriod, in Minuten;

Sonstige: OVERLAP = (CRLPeriod / 10), in Minuten

b) Bei einer OVERLAP > 720 dann OVERLAP = 720

c) Wenn OVERLAP < (1,5 * ClockSkewMinutes), dann OVERLAP = (1,5 * ClockSkewMinutes)

d) Wenn OVERLAP > CRLPeriod, in Minuten dann OVERLAP = CRLPeriod in Minuten

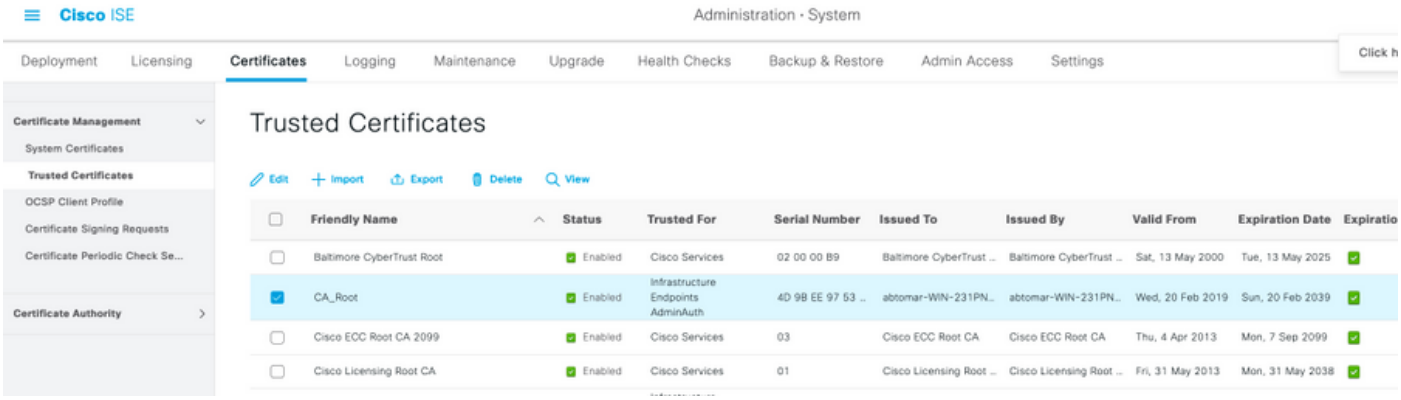
e Nachfrist = OVERLAP + ClockSkew-Minuten

```
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
```

Die Kulanzfrist wird berechnet als die Zeitspanne zwischen dem Zeitpunkt, zu dem die CA das nächste CRL veröffentlicht, und dem Ablauf des aktuellen CRL. Die ISE muss so konfiguriert werden, dass die CRLs entsprechend abgerufen werden.

8. Melden Sie sich beim Knoten ISE Primary Admin an, und wählen Sie **Administration > System >**

Certificates aus. Wählen Sie im linken Teilfenster die Option **Vertrauenswürdiges Zertifikat**



9. Aktivieren Sie das Kontrollkästchen neben dem Zertifizierungsstellenzertifikat, für das Sie CRLs konfigurieren möchten. Klicken Sie auf **Bearbeiten**.

10. Aktivieren Sie unten im Fenster das Kontrollkästchen **CRL herunterladen**.

11. Geben Sie im Feld CRL Distribution URL (CRL-Distributions-URL) den Pfad zum CRL Distribution Point ein, der die in Abschnitt 2 erstellte Crl-Datei enthält. In diesem Beispiel lautet die URL:

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

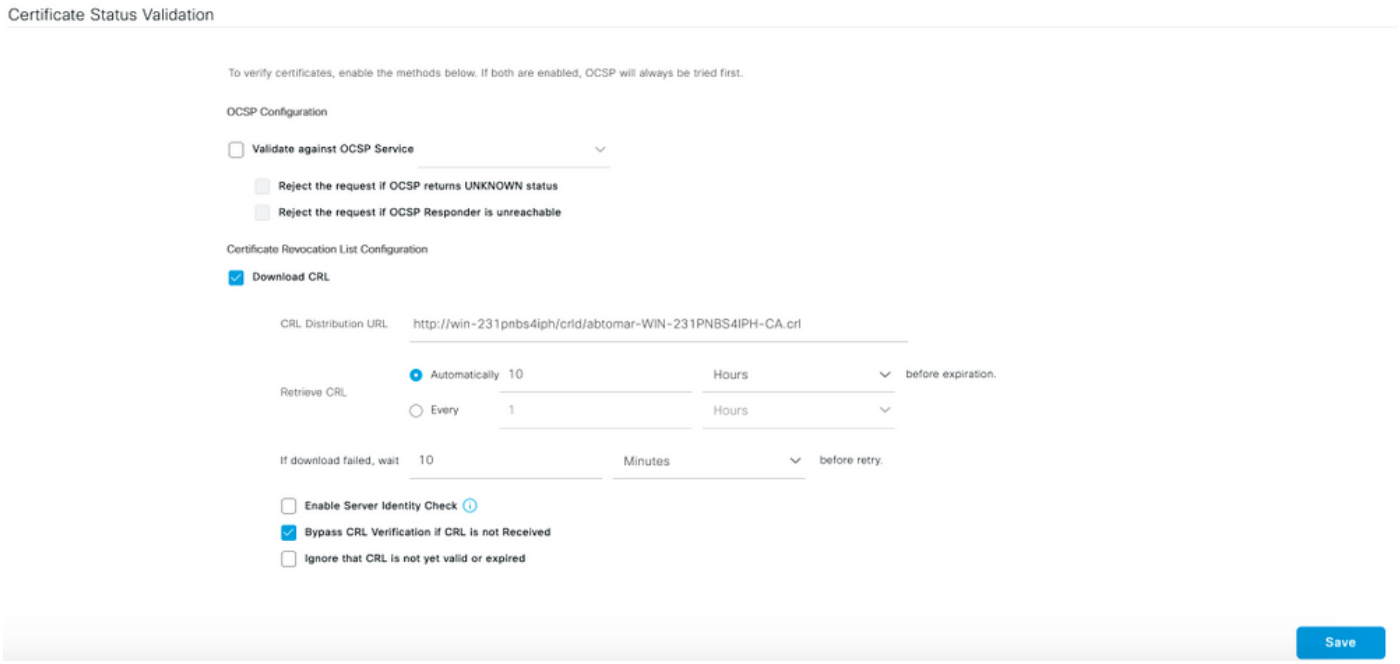
12. Die ISE kann so konfiguriert werden, dass sie die CRL in regelmäßigen Abständen abruft oder basierend auf dem Ablauf (das im Allgemeinen auch ein reguläres Intervall ist). Wenn das CRL-Veröffentlichungsintervall statisch ist, werden schnellere CRL-Aktualisierungen erhalten, wenn die letztgenannte Option verwendet wird. Klicken Sie auf das Optionsfeld **Automatisch**.

13. Legen Sie den Wert für den Abruf auf einen Wert fest, der kleiner ist als der in Schritt 7 berechnete Kulanzzeitraum. Wenn der Wert länger als der Kulanzzeitraum ist, prüft die ISE den CRL-Verteilungspunkt, bevor die CA die nächste CRL veröffentlicht hat. In diesem Beispiel wird die Kulanzfrist auf 730 Minuten oder 12 Stunden und 10 Minuten berechnet. Für den Abruf wird ein Wert von 10 Stunden verwendet.

14. Legen Sie das Wiederholungsintervall entsprechend Ihrer Umgebung fest. Wenn die ISE die CRL im vorherigen Schritt im konfigurierten Intervall nicht abrufen kann, wird in diesem kürzeren Intervall erneut versucht.

15. Aktivieren Sie das Kontrollkästchen **Bypass CRL Verification if CRL is not Received (CRL wird nicht empfangen)**, um die zertifikatsbasierte Authentifizierung normal (und ohne CRL-Prüfung) zu ermöglichen, wenn die ISE die CRL für diese CA beim letzten Download-Versuch nicht abrufen konnte. Wenn dieses Kontrollkästchen nicht aktiviert ist, schlägt die gesamte zertifikatbasierte Authentifizierung mit Zertifikaten dieser Zertifizierungsstelle fehl, wenn die CRL nicht abgerufen werden kann.

16. Aktivieren Sie das Kontrollkästchen **CRL nicht gültig oder abgelaufen ignorieren**, um ISE die Verwendung abgelaufener (oder noch nicht gültiger) CRL-Dateien als gültig zuzulassen. Wenn dieses Kontrollkästchen nicht aktiviert ist, stuft die ISE eine CRL vor dem Datum des In-Kraft-Tretens und nach dem Datum der nächsten Aktualisierung als ungültig ein. Klicken Sie auf **Speichern**, um die Konfiguration abzuschließen.



Interne Informationen von Cisco

1. Microsoft. "Konfigurieren eines CRL-Verteilungspunkts für Zertifikate." http://technet.microsoft.com/en-us/library/ee649260%28v=ws.10%29.aspx, 7. Oktober 2009 [18. Dez. 2012]

2. Microsoft. "Veröffentlichen Sie die Zertifikatswiderrufsliste manuell." http://technet.microsoft.com/en-us/library/cc778151%28v=ws.10%29.aspx, 21. Januar 2005 [18. Dez. 2012]

3. Microsoft. "Konfigurieren von CRL- und Delta CRL-Überlappungszeiträumen." http://technet.microsoft.com/en-us/library/cc731104.aspx, 11. April 2011 [18. Dez. 2012]

4. MS2065 [MSFT] "How EffectiveDate (thisUpdate), NextUpdate und NextCRLPublish are are berechnet." http://blogs.technet.com/b/pki/archive/2008/06/05/how-effectivedate-thisupdate-nextupdate-and-nextcrlpublish-are-calculated.aspx, 4. Juni 2008 [18. Dez. 2012]