Konfigurieren von Microsoft CA Server zum Veröffentlichen der Zertifikatsperrlisten für ISE

Inhalt

Einleitung

Voraussetzung

- Anforderungen
- Verwendete Komponenten

Konfigurieren

- Erstellen und Konfigurieren eines Ordners auf der Zertifizierungsstelle, in dem die Sperrlisten-Dateien gespeichert werden
- Erstellen einer Site in IIS zum Verfügbarmachen des neuen Zertifikatsperrlisten-Verteilungspunkts
- Konfigurieren von Microsoft CA Server zum Veröffentlichen von CRL-Dateien am Verteilungspunkt
- Überprüfen Sie, ob die Sperrlisten-Datei vorhanden und über IIS zugänglich ist.
- Konfigurieren der ISE zur Verwendung des neuen CRL-Verteilungspunkts

Überprüfung

Fehlerbehebung

Einleitung

In diesem Dokument wird die Konfiguration eines Microsoft Certificate Authority (CA)-Servers beschrieben, der Internetinformationsdienste (IIS) ausführt, um die Zertifikatsperrlisten-Updates (Certificate Revocation List, CRL) zu veröffentlichen. Außerdem wird erläutert, wie Sie die Cisco Identity Services Engine (ISE) (Version 3.0 und höher) konfigurieren, um die Updates zur Verwendung bei der Zertifikatsvalidierung abzurufen. Die ISE kann so konfiguriert werden, dass sie Zertifikatsperrlisten für die verschiedenen Zertifizierungsstellen-Stammzertifikate 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 möglichen Auswirkungen aller Befehle kennen.

Konfigurieren

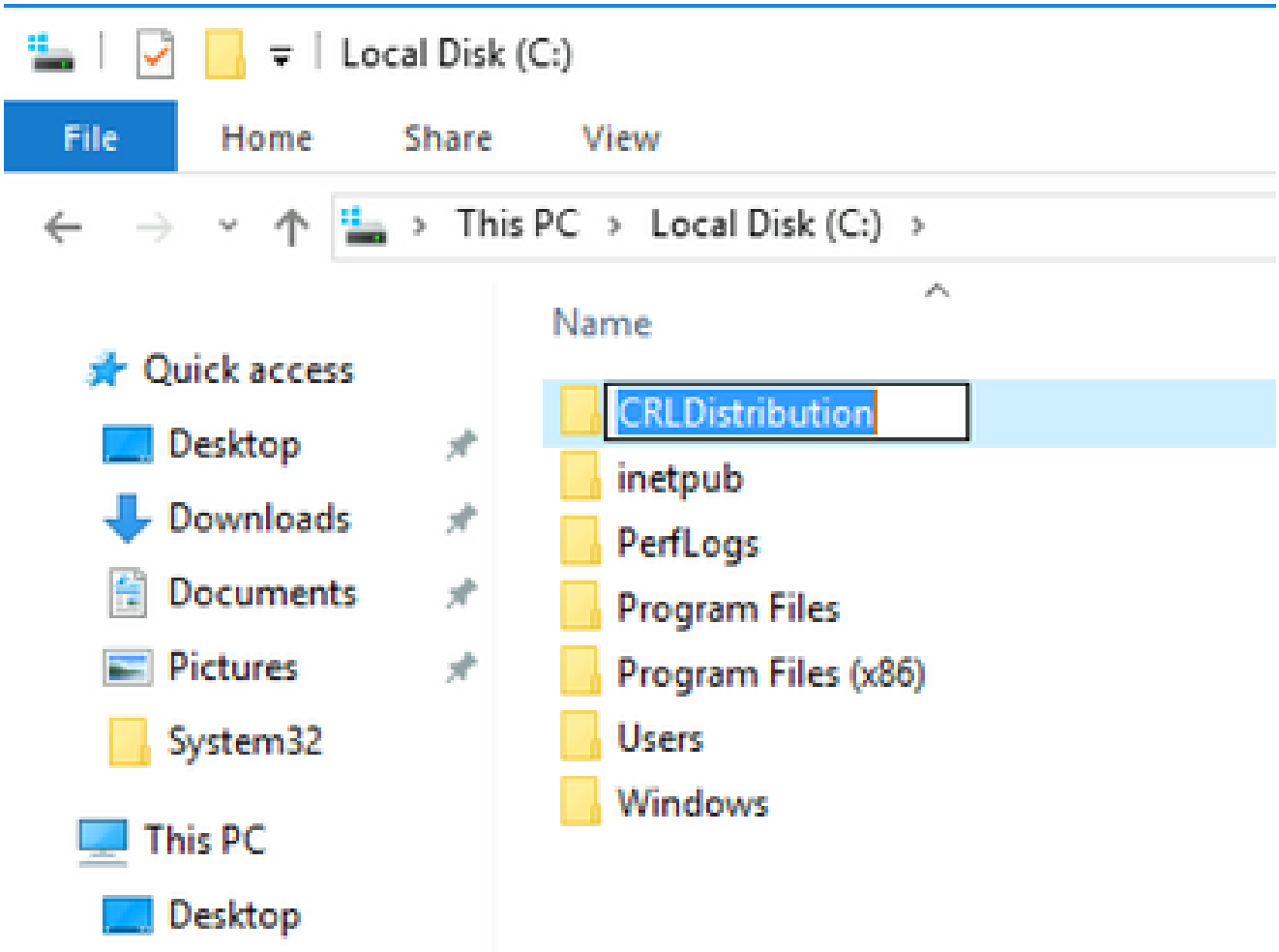
In diesem Abschnitt erfahren Sie, wie Sie die in diesem Dokument beschriebenen Funktionen konfigurieren können.

Erstellen und Konfigurieren eines Ordners auf der Zertifizierungsstelle, in dem die Sperrlisten-Dateien gespeichert werden

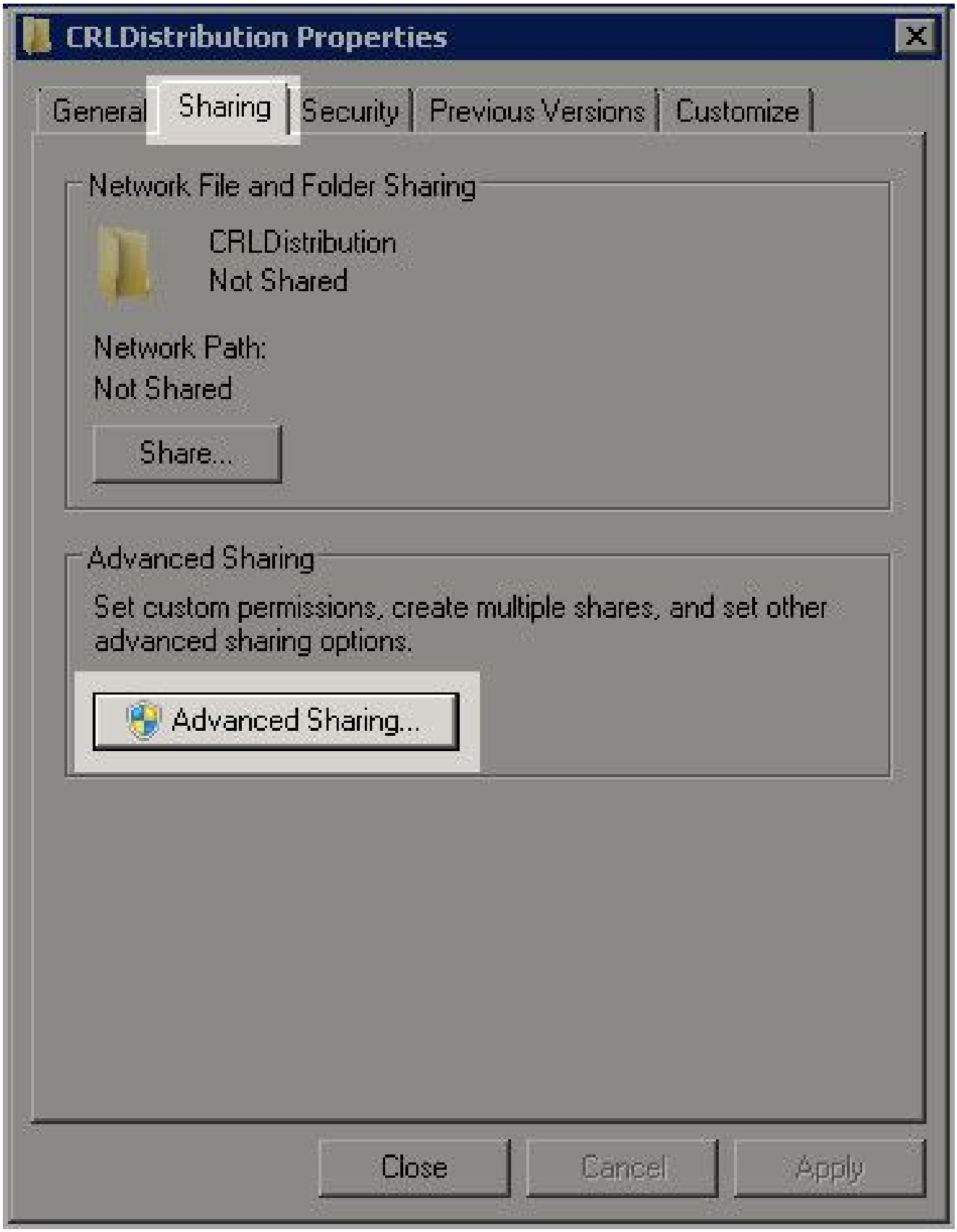
Die erste Aufgabe besteht darin, einen Speicherort auf dem Zertifizierungsstellenserver zum Speichern der Zertifikatsperrlisten-Dateien zu konfigurieren. Standardmäßig veröffentlicht der Microsoft CA-Server die Dateien auf **C:\Windows\system32\CertSrv\CertEnroll**

Anstatt diesen Systemordner zu verwenden, erstellen Sie 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 **C:\CRLDistribution** wird der Ordner erstellt.

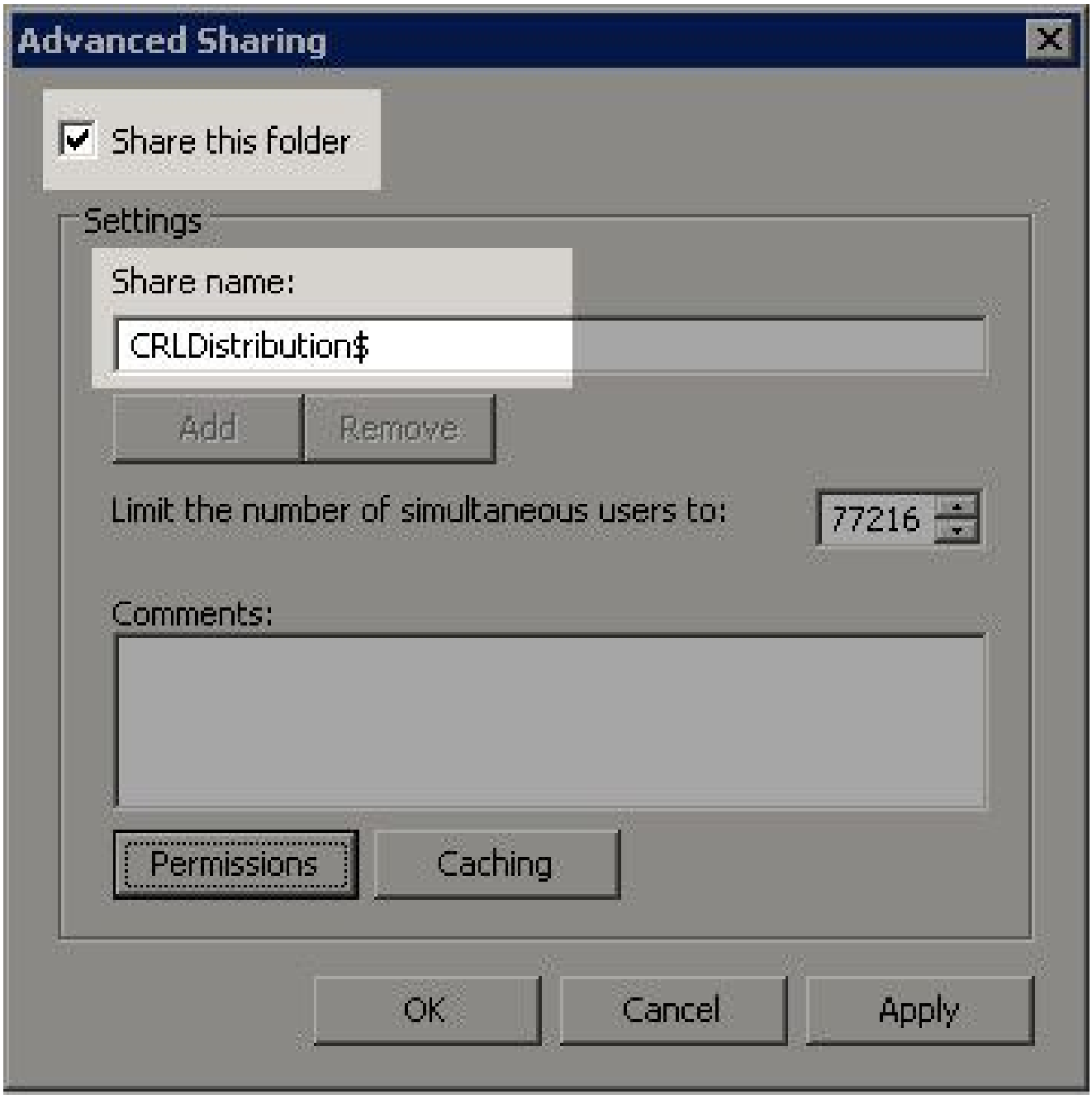


2. Damit die Zertifizierungsstelle die Zertifikatsperrlisten-Dateien in den neuen Ordner schreiben kann, muss die Freigabe aktiviert sein. Klicken Sie mit der rechten Maustaste auf den neuen Ordner, wählen Sie **Properties**, klicken Sie auf die **Sharing** Registerkarte und dann auf **Advanced Sharing**.

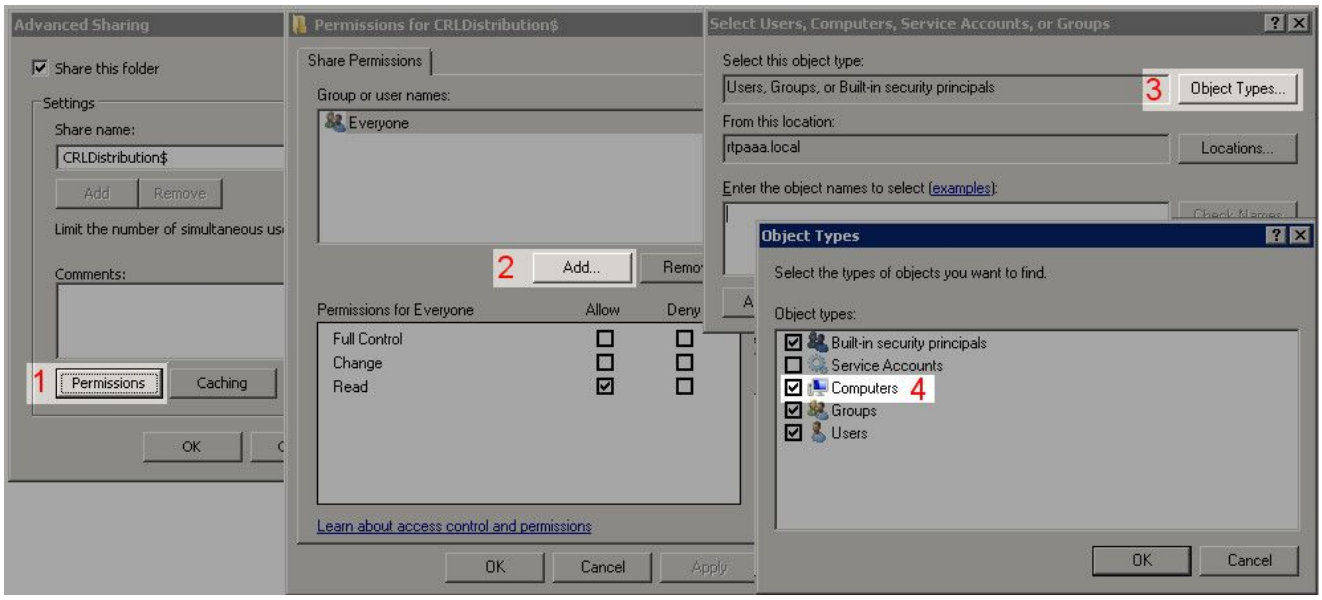


3. Um den Ordner freizugeben, aktivieren Sie das **Share this folder** Kontrollkästchen, und fügen Sie

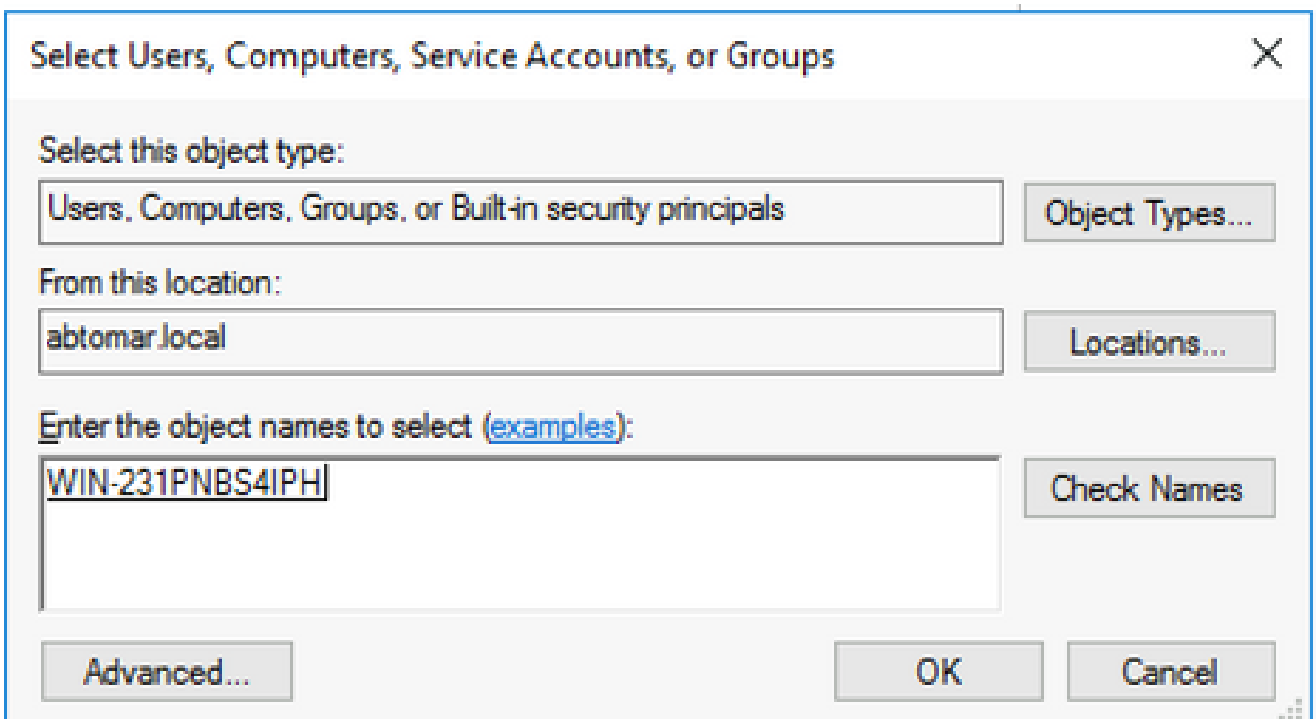
dann am Ende des Freigabenamens im Feld Freigabename ein Dollarzeichen ($) hinzu, um die Freigabe auszublenden.



4. Klicken Sie auf **Permissions** (1), klicken Sie auf **Add** (2), klicken Sie auf **Object Types** (3), und aktivieren Sie das **Computers** Kontrollkästchen (4).

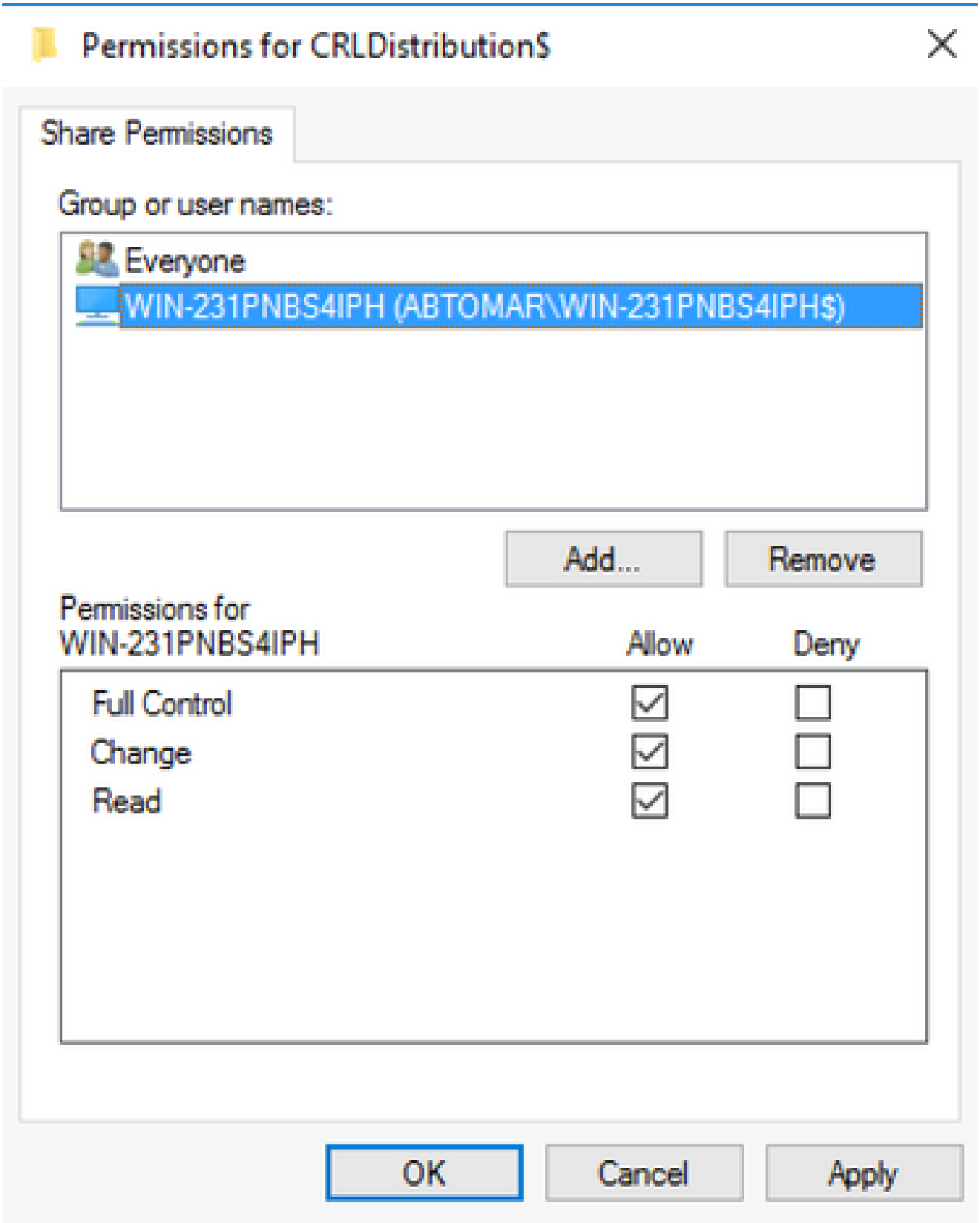


5. Um zum Fenster Benutzer, Computer, Dienstkonten oder Gruppen auswählen zurückzukehren, klicken Sie auf **OK**. Geben Sie im Feld Geben Sie die zu verwendenden Objektnamen ein den Computernamen des Zertifizierungsstellenservers in diesem Beispiel ein: WIN0231PNBS4IPH, und klicken Sie auf **Check Names**.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

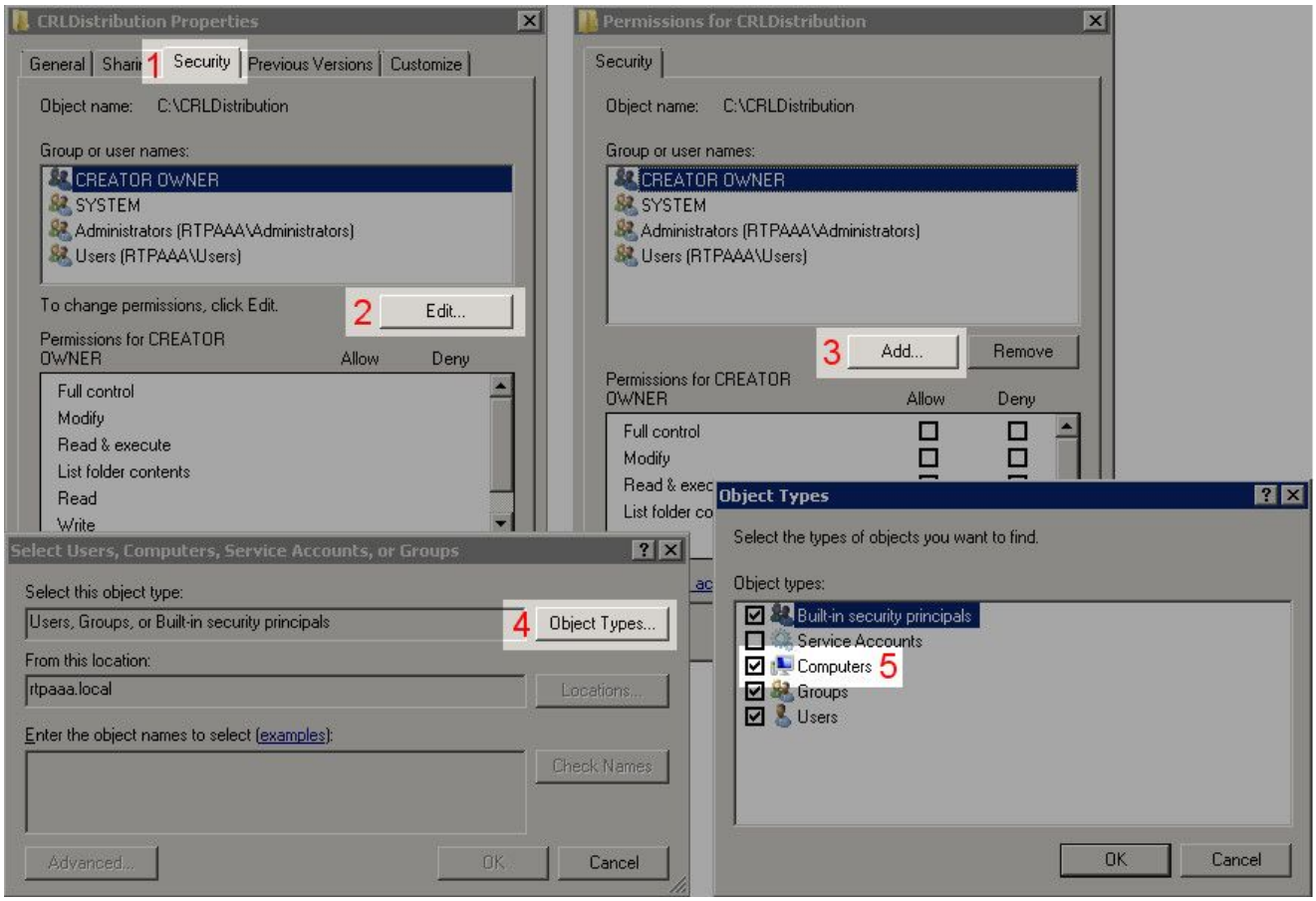


6. Wählen Sie im Feld "Group or user names" (Gruppen- oder Benutzernamen) den CA-Computer aus. Überprüfen Sie**Allow**, ob Vollzugriff gewährt wird, um vollständigen Zugriff auf die Zertifizierungsstelle zu erhalten.

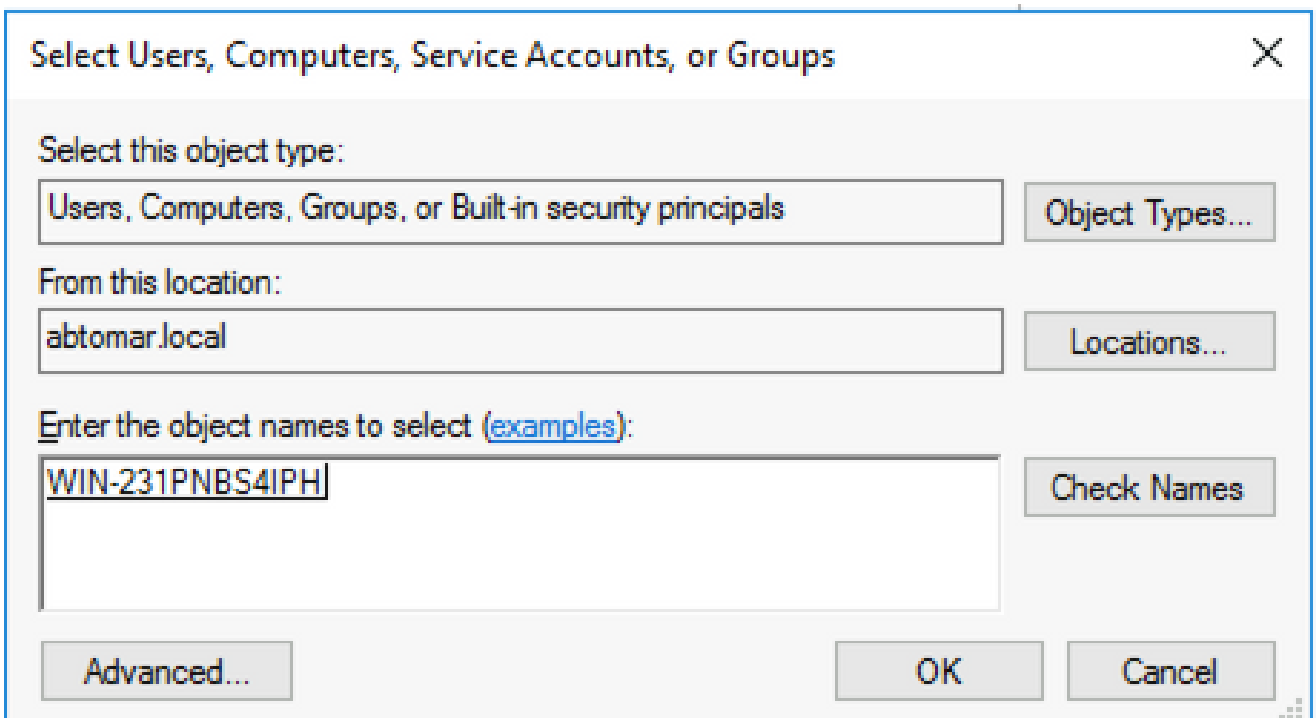
   Klicken Sie auf .**OK** Klicken Sie **OK** erneut auf, um das Fenster Erweiterte Freigabe zu schließen und zum Fenster Eigenschaften zurückzukehren.



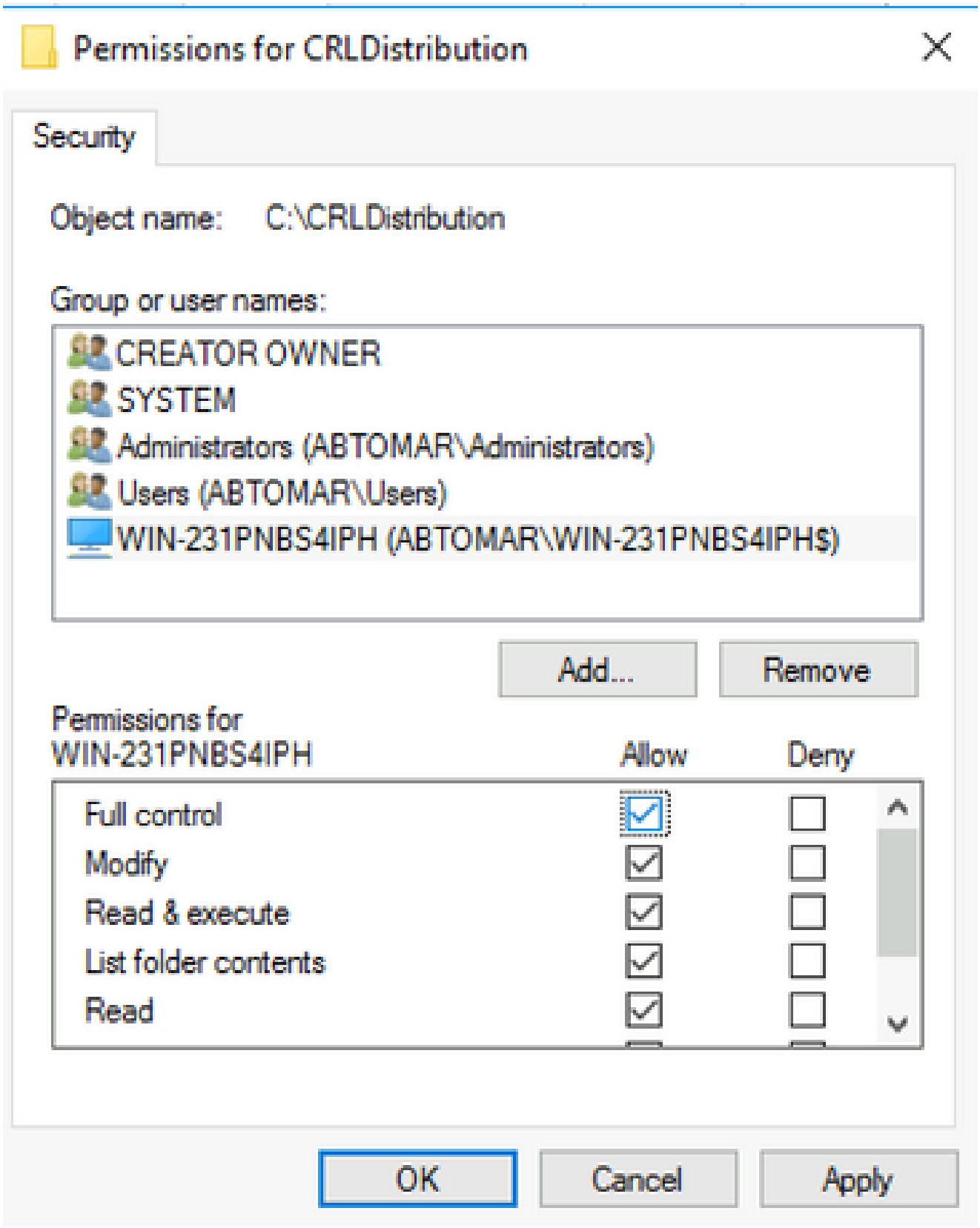
7. Damit die Zertifizierungsstelle die Sperrlisten-Dateien in den neuen Ordner schreiben kann, müssen Sie die entsprechenden Sicherheitsberechtigungen konfigurieren. Klicken Sie auf die**Security** Registerkarte (1), klicken Sie auf **Edit** (2), klicken Sie auf **Add** (3), klicken Sie auf **Object Types** (4), und aktivieren Sie das **Computers** Kontrollkästchen (5).



8. Geben Sie im Feld Geben Sie die zu verwendenden Objektnamen ein den Computernamen des Zertifizierungsstellenservers ein, und klicken Sie auf **Check Names**. Wenn der eingegebene Name gültig ist, wird der Name aktualisiert und unterstrichen angezeigt. Klicken Sie auf .**OK**



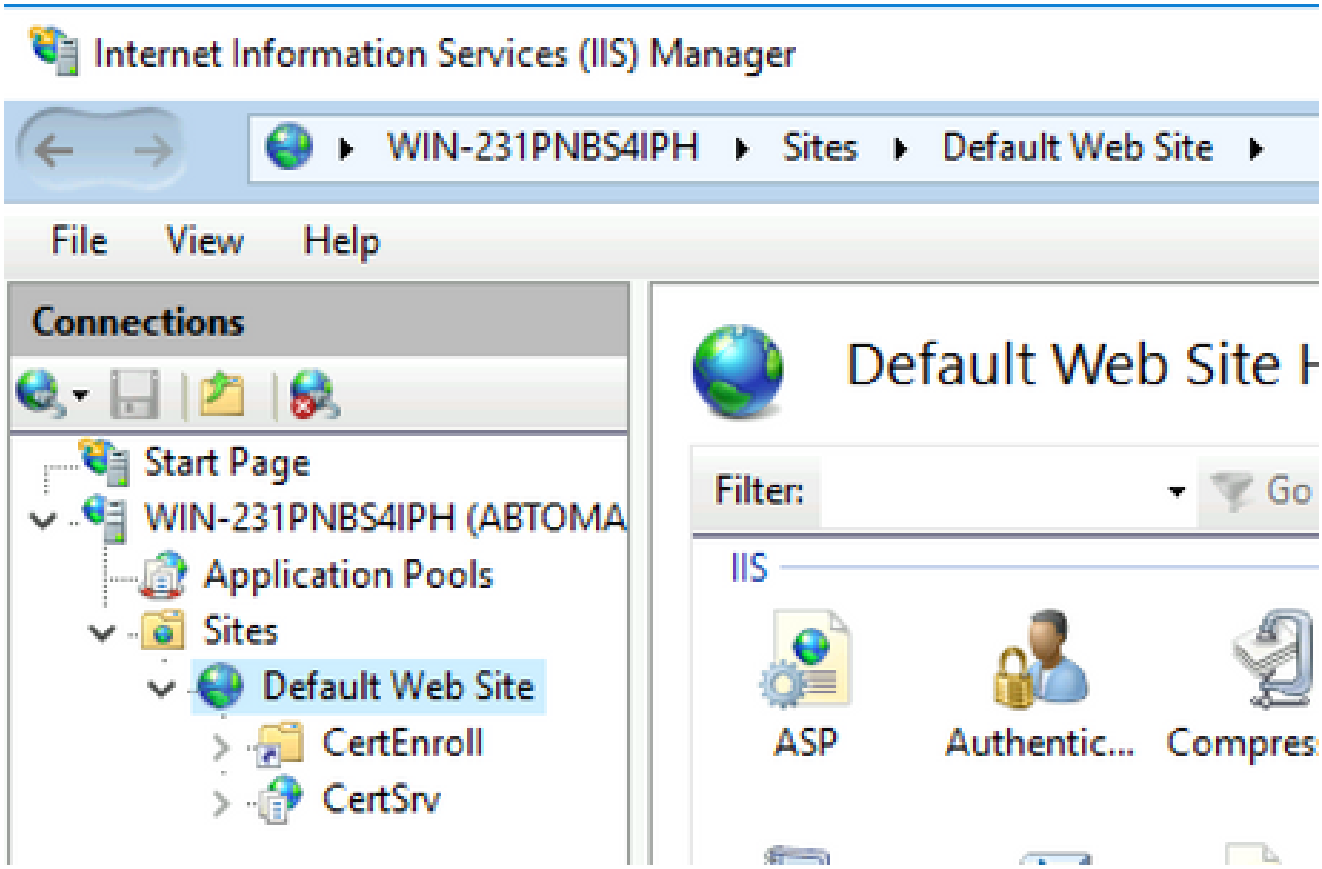
9. Wählen Sie den CA-Computer im Feld "Group or user names" (Gruppen- oder Benutzernamen) aus, und überprüfen Sie**Allow**, ob die CA den vollen Zugriff erhält. Klicken Sie auf **OK** , und klicken Sie dann auf**Close**, um die Aufgabe abzuschließen.



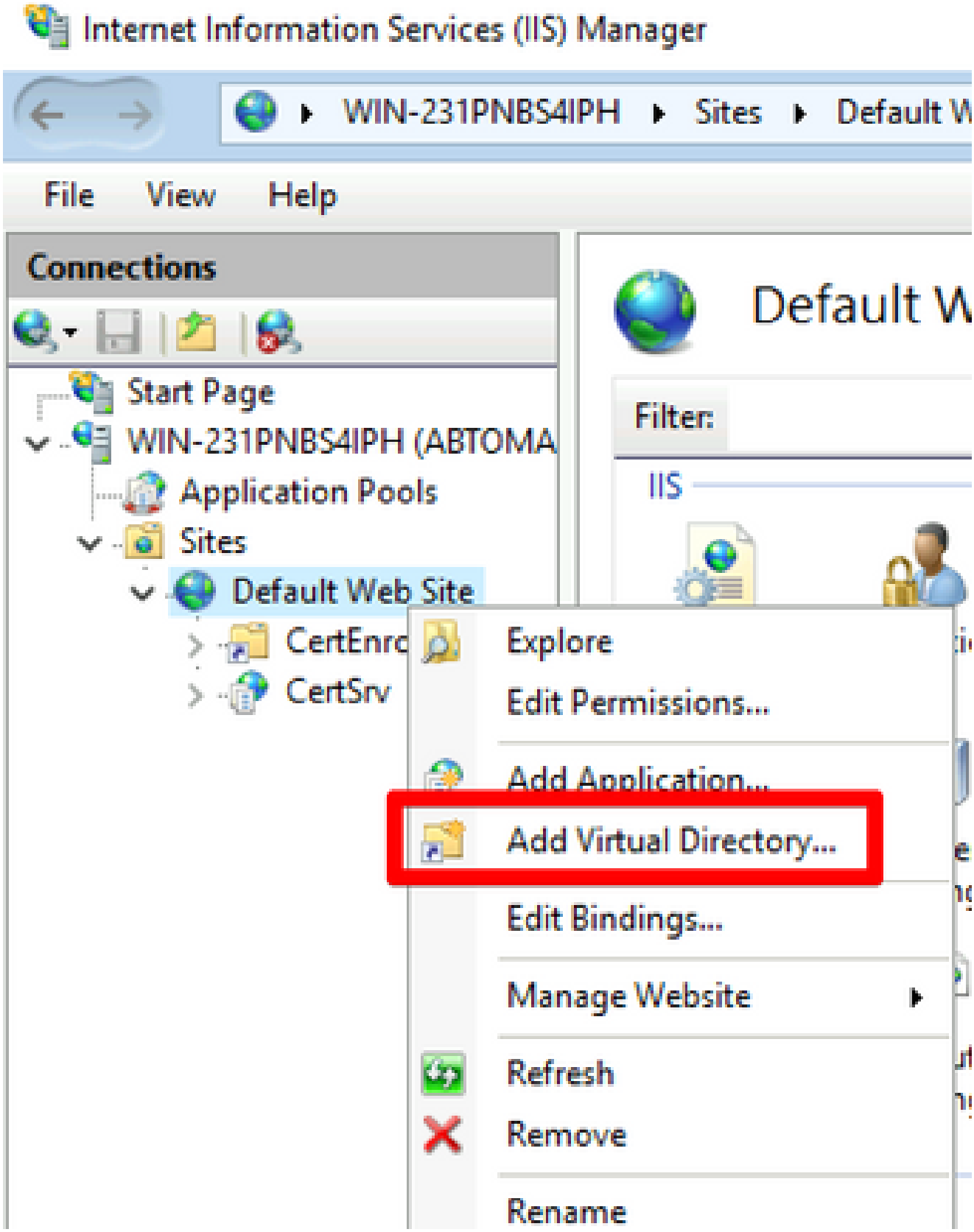
Erstellen einer Site in IIS zum Verfügbarmachen des neuen Zertifikatsperrlisten-Verteilungspunkts

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

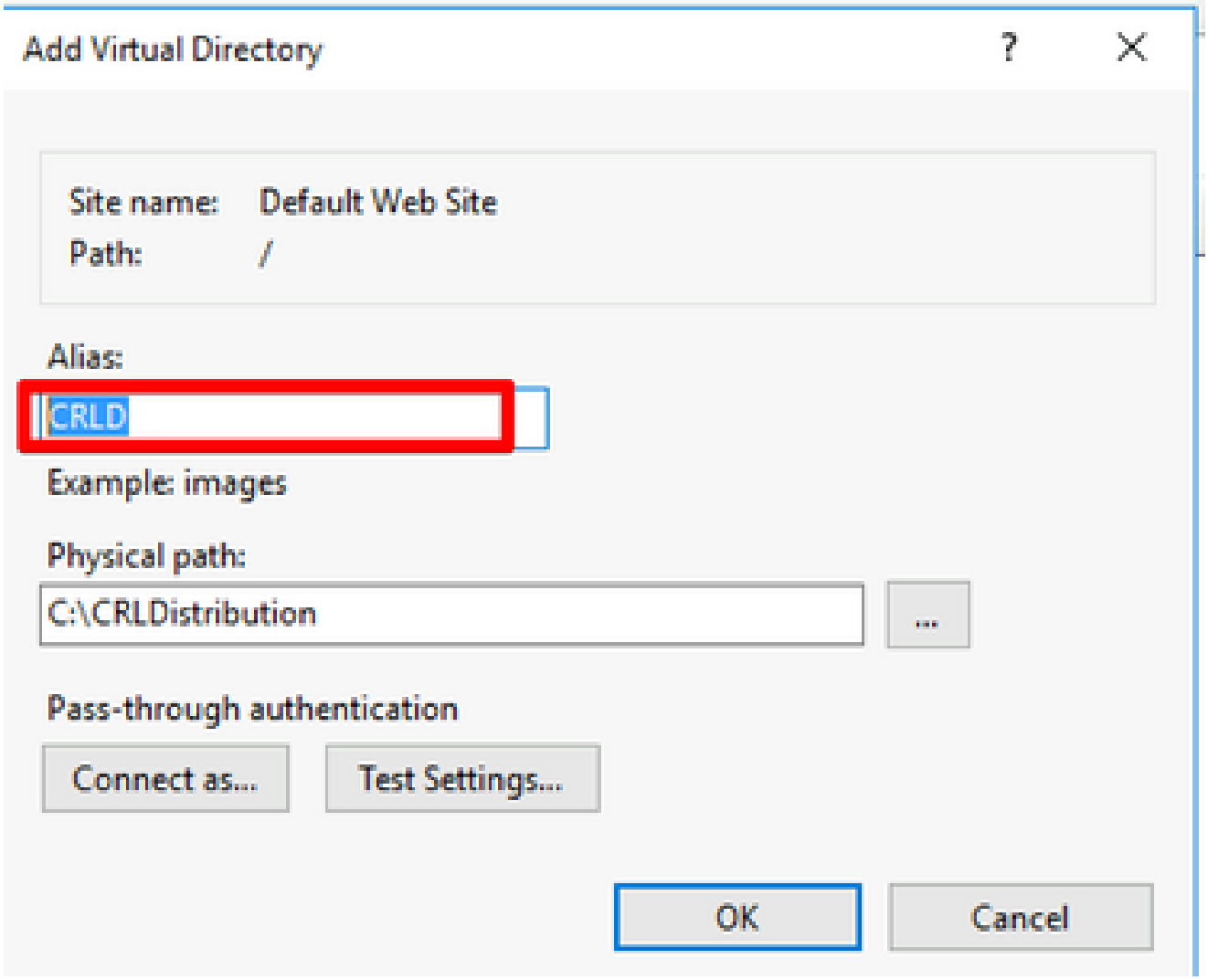
1. Klicken Sie in der Taskleiste des IIS-Servers auf **Start**. Wählen Sie **Administrative Tools** > **Internet Information Services (IIS) Manager**.
2. Erweitern Sie im linken Bereich (Konsolenstruktur) den IIS-Servernamen, und erweitern Sie dann **Sites**.



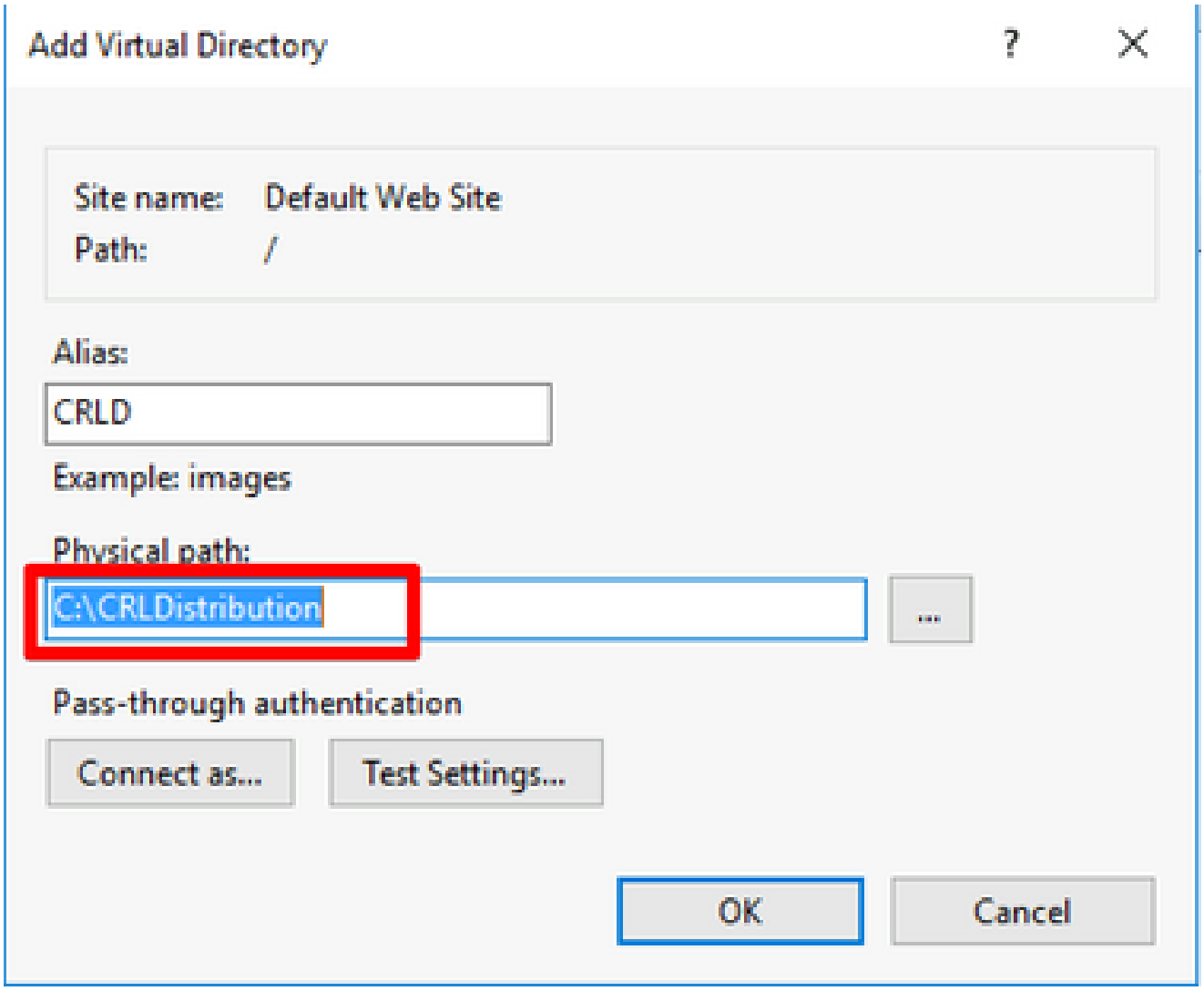
3. Klicken Sie mit der rechten Maustaste, **Default Web Site** und wählen Sie **Add Virtual Directory**, wie in diesem Bild dargestellt.



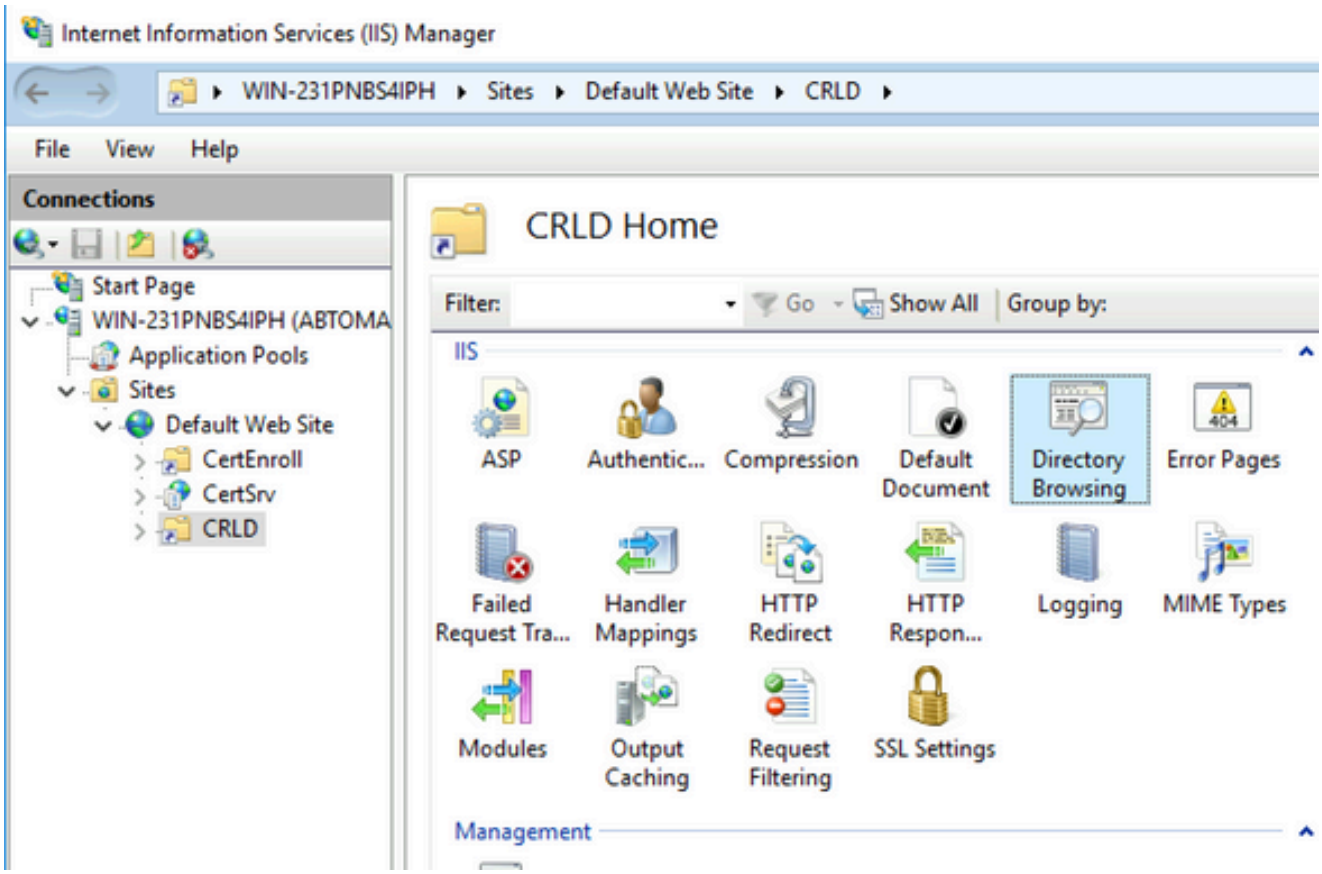
4. Geben Sie im Feld Alias einen Standortnamen für den Zertifikatsperrlisten-Verteilungspunkt ein. In diesem Beispiel wird CRLD eingegeben.



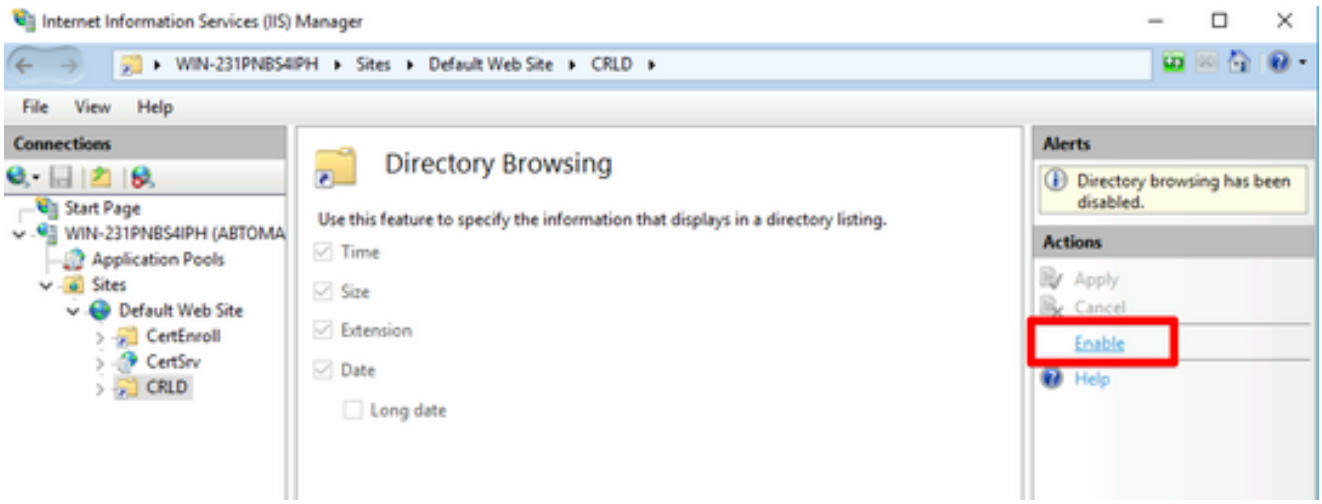
5. Klicken Sie auf die Auslassungszeichen (. . .) rechts vom Feld Physical path (Physischer Pfad) angezeigt und navigieren Sie zu dem in Abschnitt 1 erstellten Ordner. Wählen Sie den Ordner aus, und klicken Sie auf OK. Klicken Sie aufOK, um das Fenster Virtuelles Verzeichnis hinzufügen zu schließen.



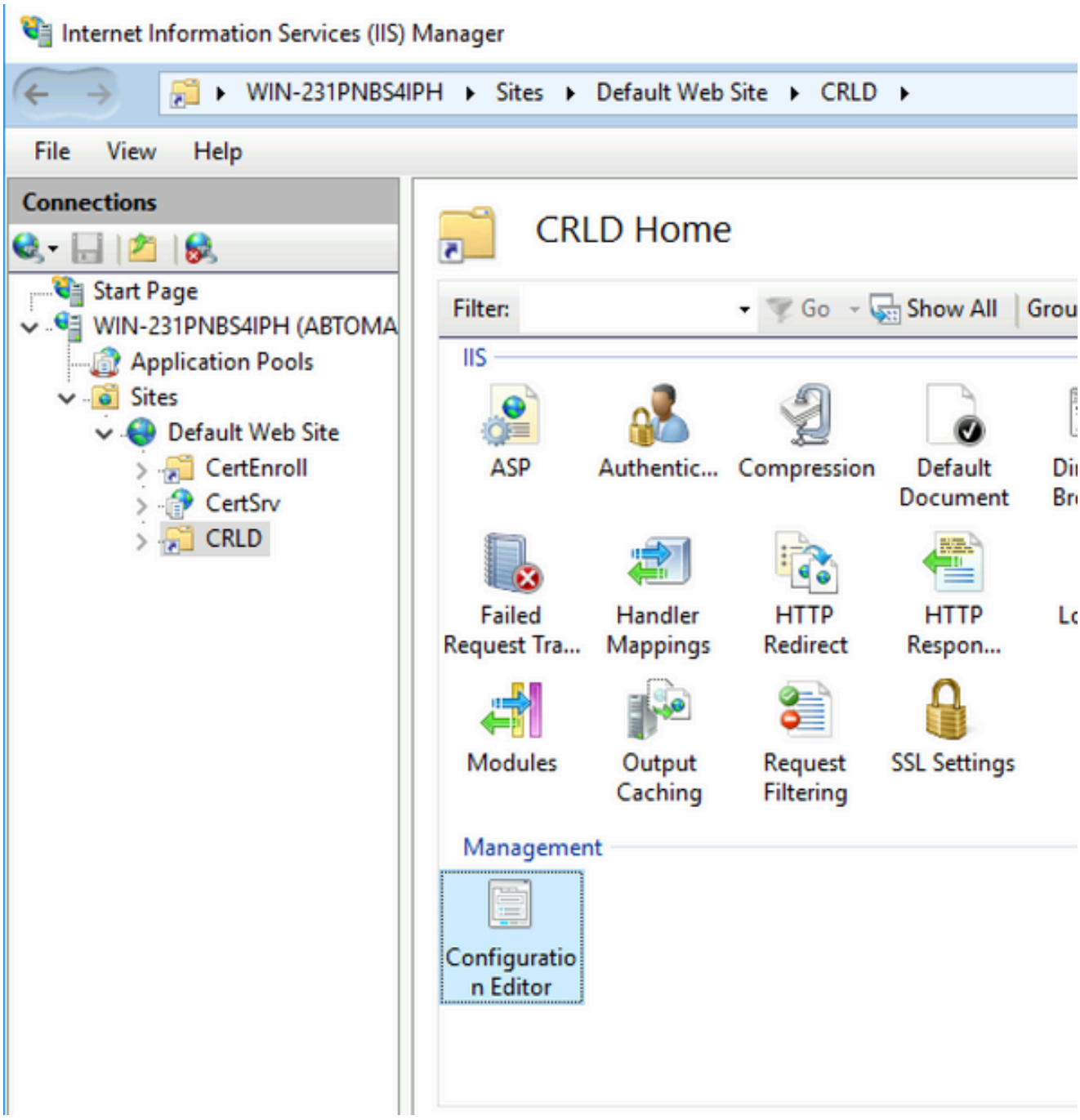
6. Der in Schritt 4 eingegebene Standortname muss im linken Bereich hervorgehoben werden. Wenn nicht, wählen Sie es jetzt aus. Doppelklicken Sie im mittleren Bereich auf **Directory Browsing**.



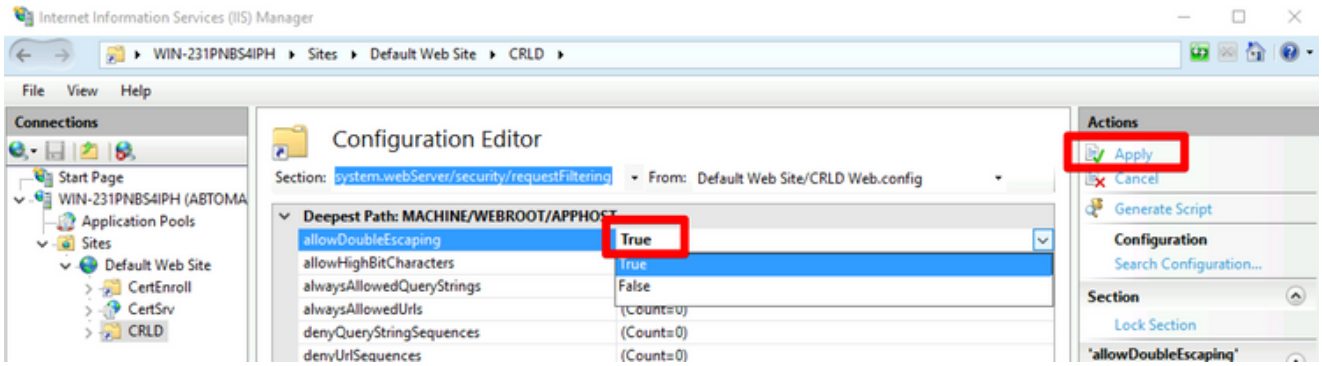
7. Klicken Sie im rechten Bereich auf**Enable**, um die Verzeichnissuche zu aktivieren.



8. Wählen Sie im linken Bereich erneut den Standortnamen aus. Doppelklicken Sie im mittleren Bereich auf **Configuration Editor**.



9. Wählen Sie in der Dropdown-Liste Abschnitt die Option **system.webServer/security/requestFiltering**. Wählen Sie in der **allowDoubleEscaping** Dropdown-Liste die Option **True**. Klicken Sie im rechten Fensterbereich auf **Apply**, wie in diesem Bild dargestellt.

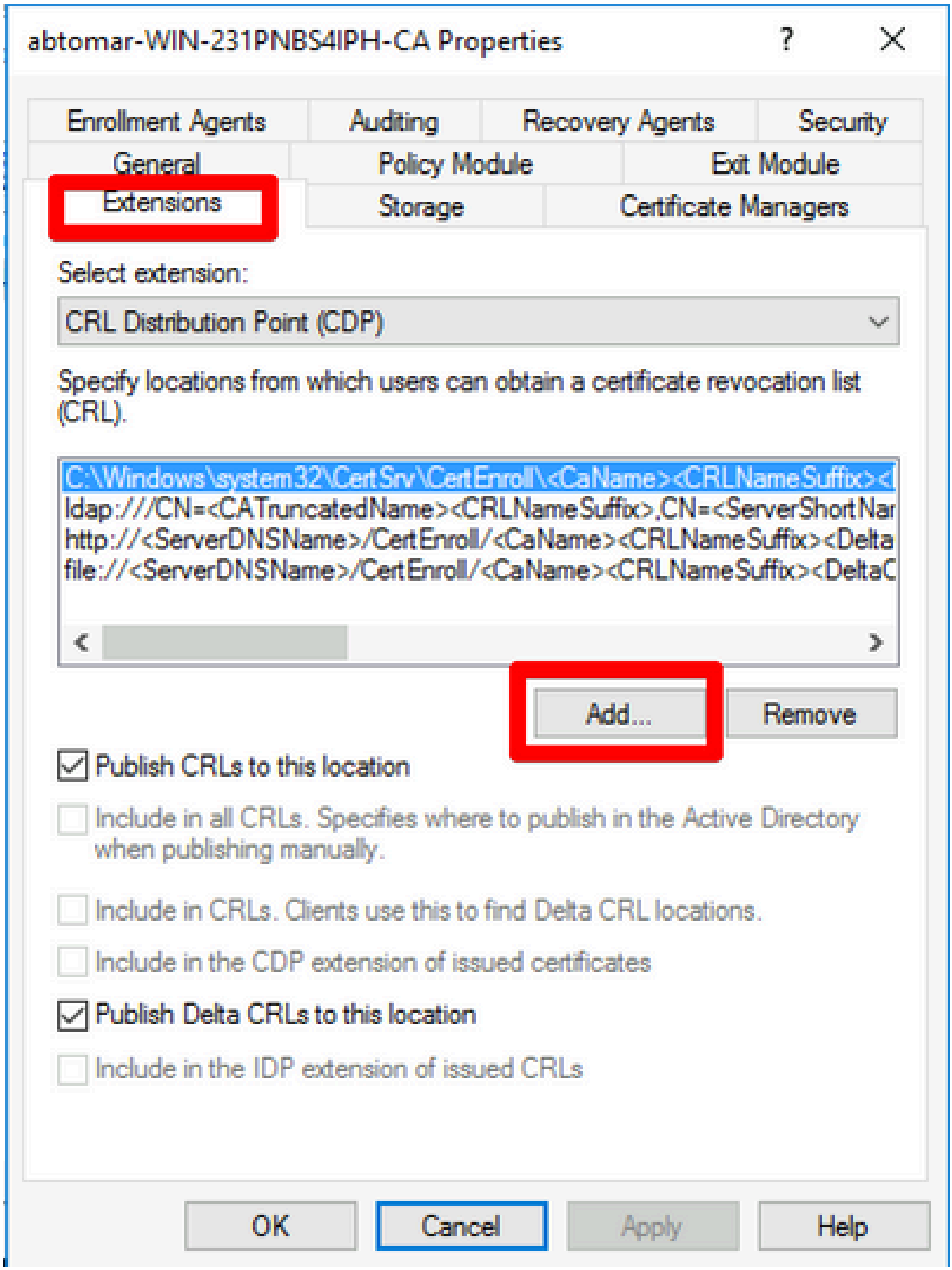


Der Zugriff auf den Ordner muss nun über IIS möglich sein.

Konfigurieren von Microsoft CA Server zum Veröffentlichen von CRL-Dateien am Verteilungspunkt

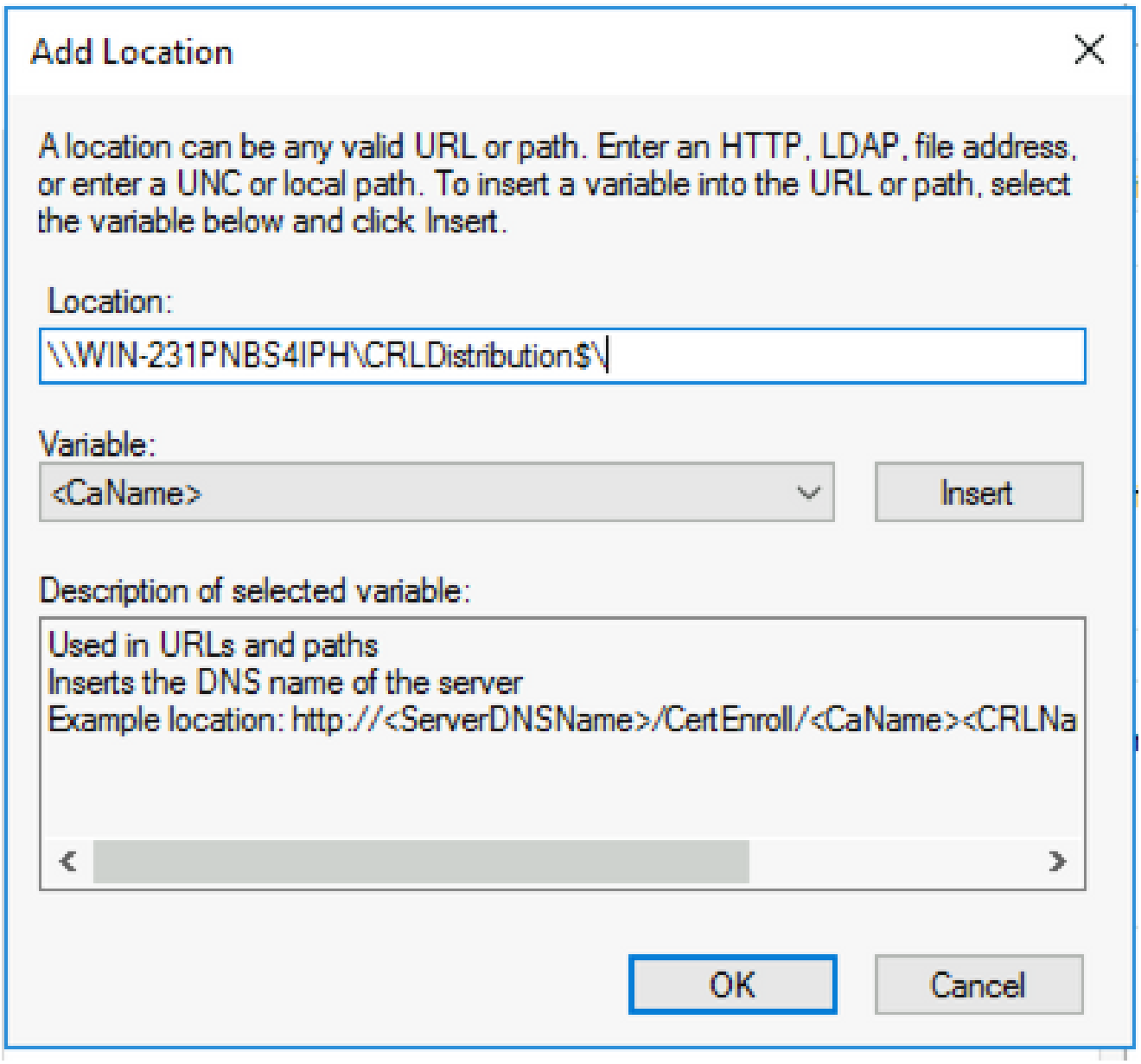
Nachdem ein neuer Ordner konfiguriert wurde, in dem die Zertifikatsperrlisten-Dateien gespeichert sind, und der Ordner in IIS verfügbar gemacht wurde, konfigurieren Sie den Microsoft-Zertifizierungsstellenserver so, dass die Zertifikatsperrlisten-Dateien am neuen Speicherort veröffentlicht werden.

1. Klicken Sie in der Taskleiste des CA-Servers auf **Start**. Wählen Sie **Administrative Tools** > **Certificate Authority**.
2. Klicken Sie im linken Bereich mit der rechten Maustaste auf den Namen der Zertifizierungsstelle. Wählen Sie **Properties** , und klicken Sie dann auf die **Extensions** Registerkarte. Um einen neuen CRL-Verteilungspunkt hinzuzufügen, klicken Sie auf **Add**.

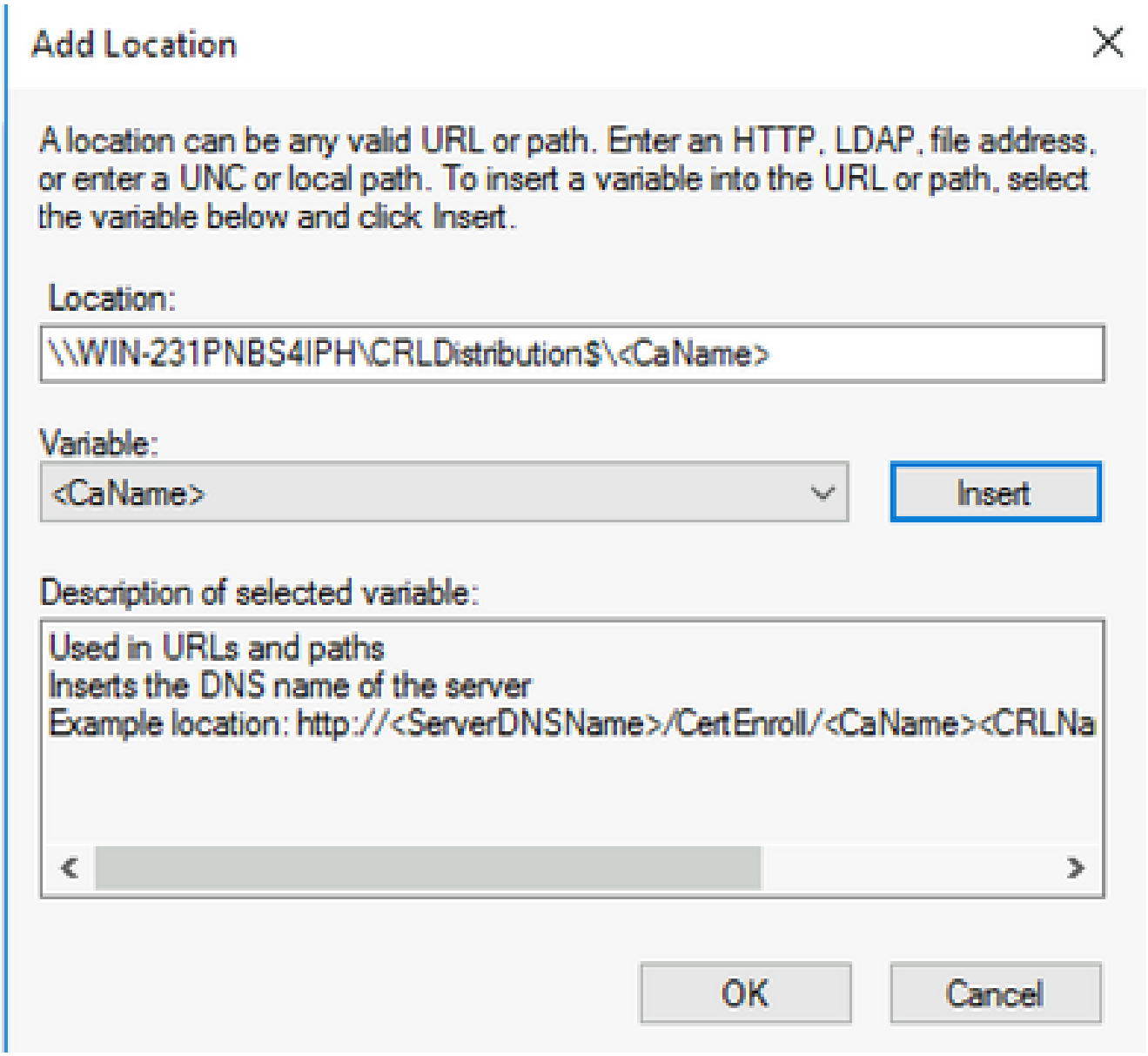


3. Geben Sie im Feld Location (Speicherort) den Pfad zu dem in Abschnitt 1 erstellten und freigegebenen Ordner ein. Im Beispiel in Abschnitt 1 lautet der Pfad:

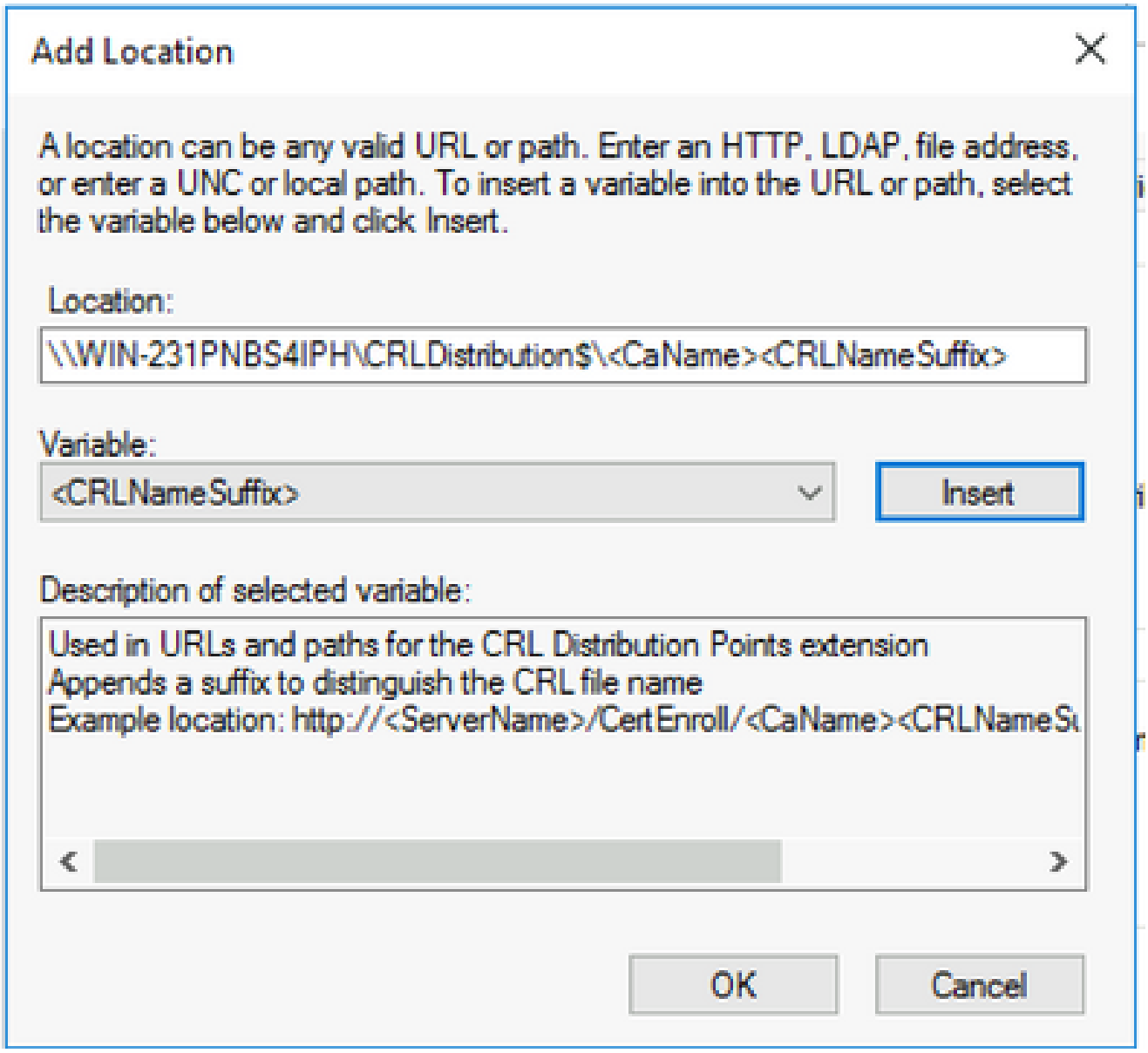
   \\WIN-231PNBS4IPH\CRLDistribution$



4. Wählen Sie bei ausgefülltem Feld "Location" aus der Dropdown-Liste "Variable" aus, und klicken Sie dann auf **Insert**.



5. Wählen Sie in der Dropdown-Liste Variable die Option aus, und klicken Sie dann auf **Insert**.

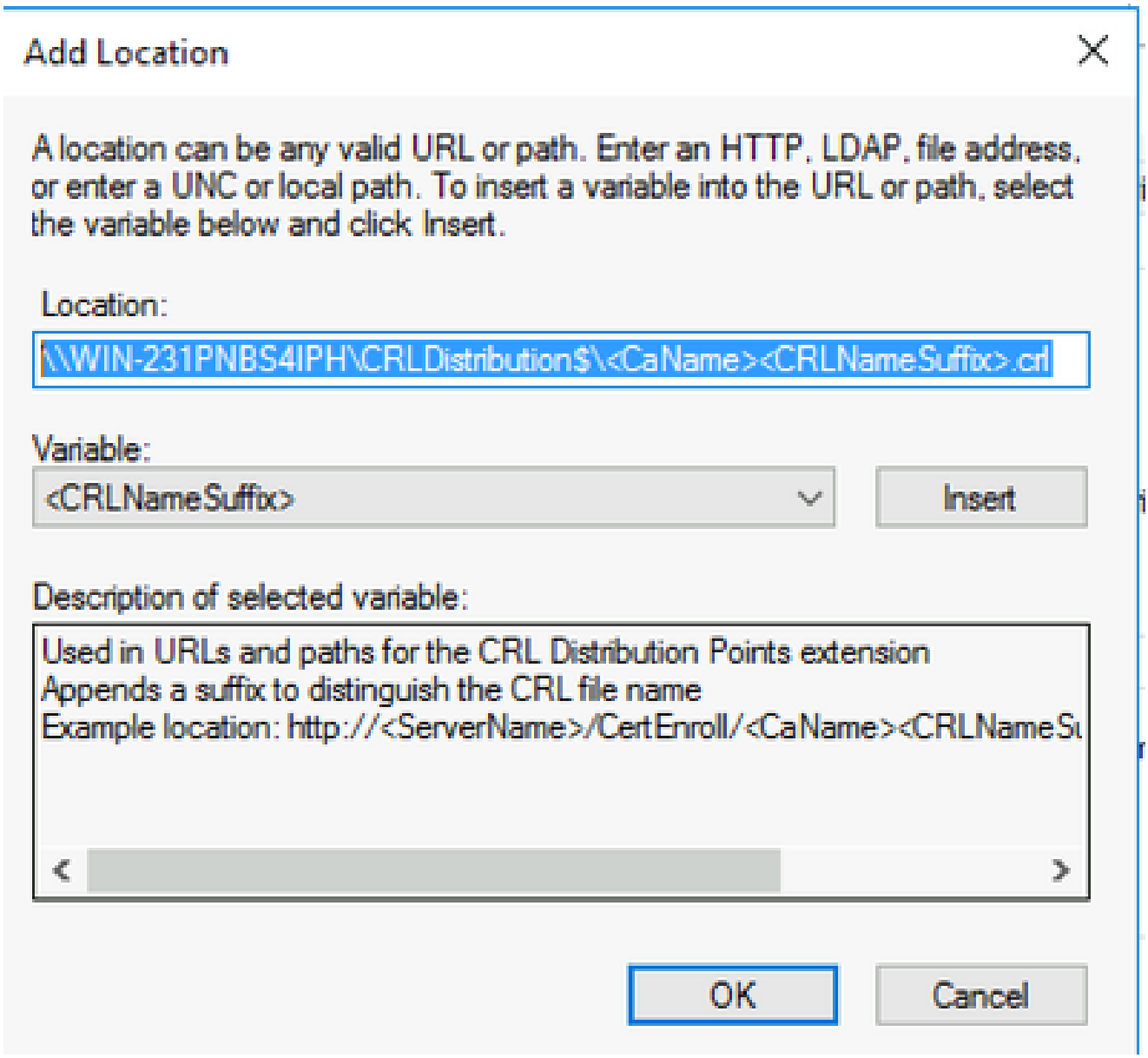


6. Hängen Sie im Feld Location (Ort) **.crl** das Ende des Pfades an. In diesem Beispiel lautet der Speicherort:

\\WIN-231PNBS4IPH\CRLDistribution$

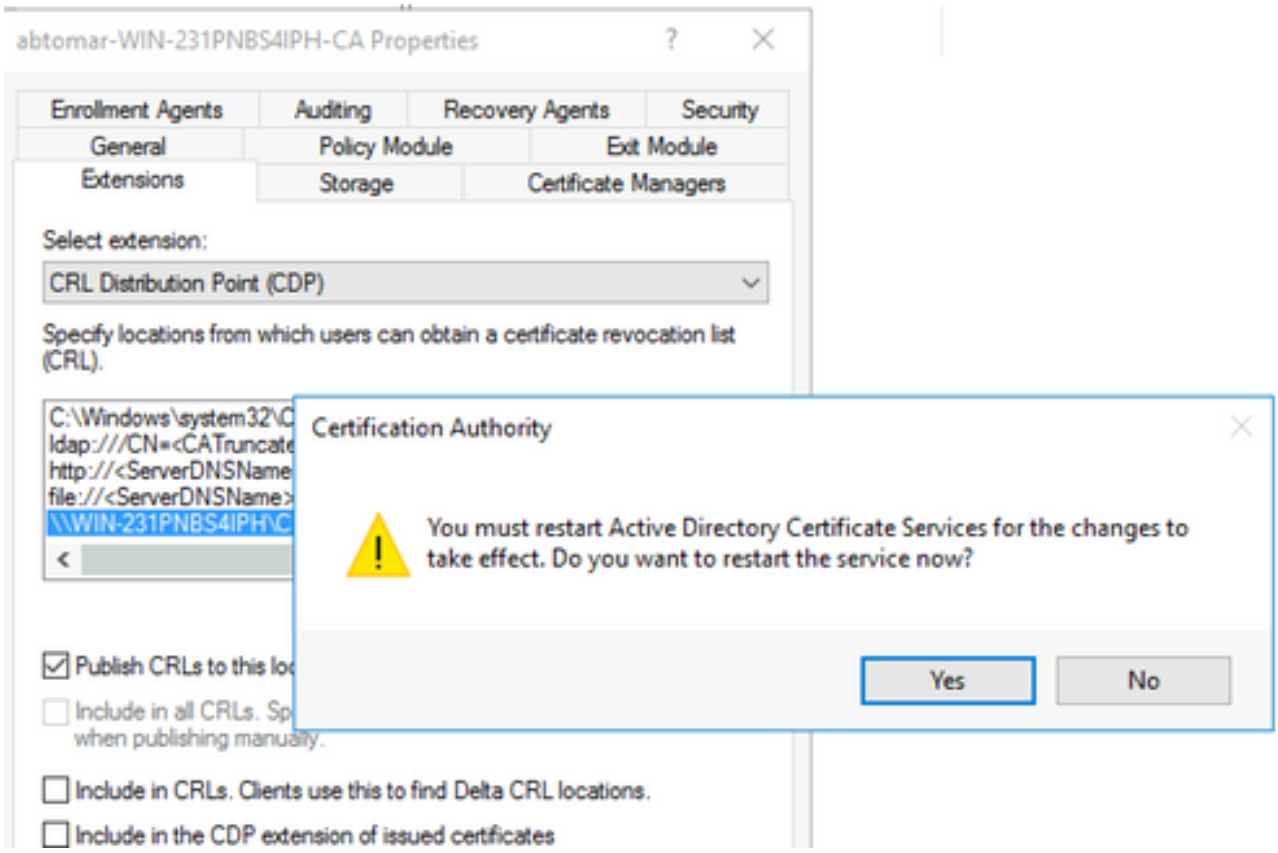
<CaName><CRLNameSuffix>

.crl

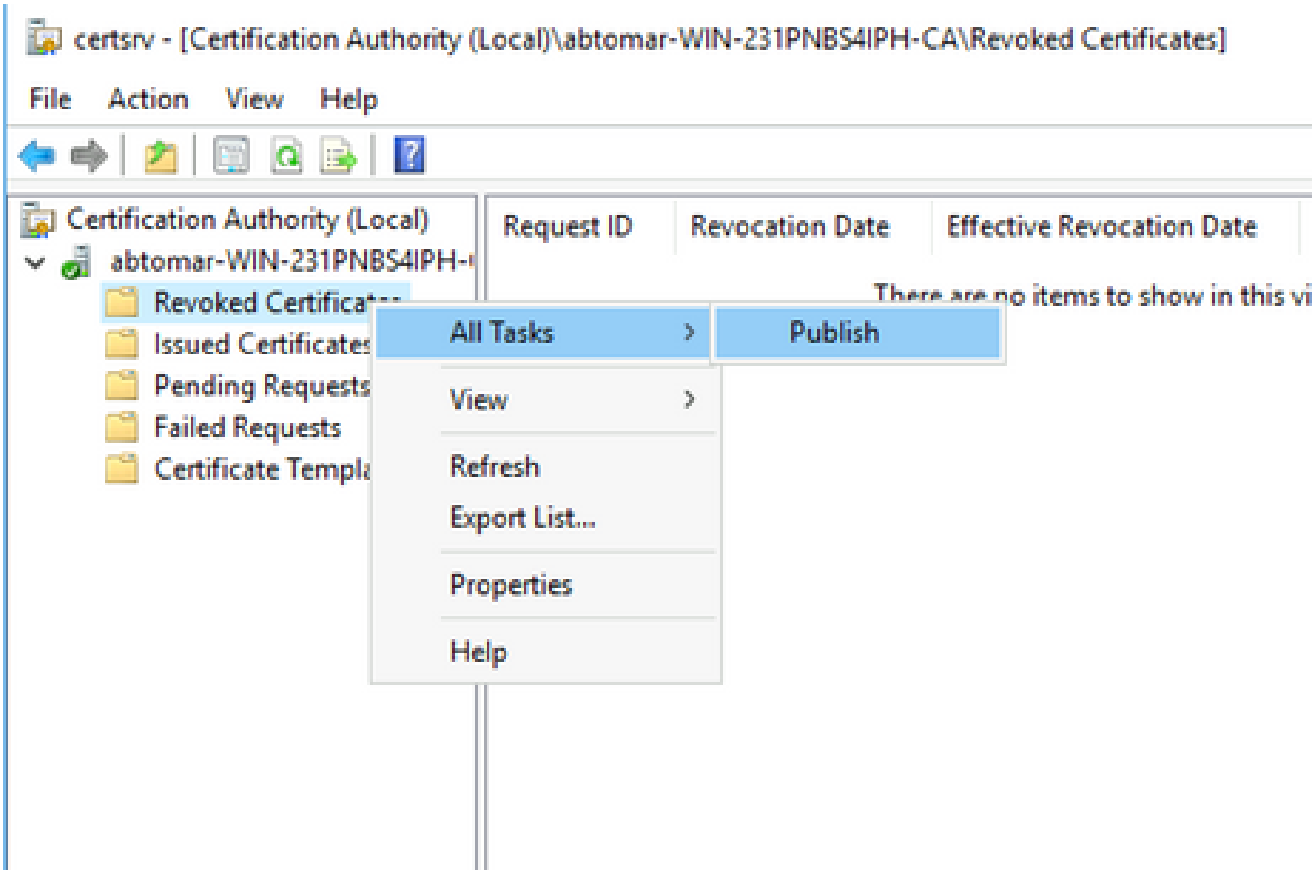


7. Klicken Sie auf **OK** , um zur Registerkarte Erweiterungen zurückzukehren. Aktivieren Sie das **Publish CRLs to this location** Kontrollkästchen, und klicken Sie dann auf, **OK** um das Eigenschaftenfenster zu schließen.

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



8. Klicken Sie im linken Bereich mit der rechten Maustaste **Revoked Certificates**. Wählen Sie **All Tasks** > **Publish**. Stellen Sie sicher, dass Neue Zertifikatsperrliste ausgewählt ist, und klicken Sie dann auf **OK**.



Der Microsoft CA-Server muss in dem in Abschnitt 1 erstellten Ordner eine neue .crl-Datei erstellen. Wenn die neue CRL-Datei erfolgreich erstellt wurde, wird nach dem Klicken auf "OK" kein Dialogfeld angezeigt. Wenn ein Fehler bezüglich des neuen Verteilungspunktordners zurückgegeben wird, wiederholen Sie sorgfältig jeden Schritt in diesem Abschnitt.

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

Überprüfen Sie, ob die neuen Sperrlisten-Dateien vorhanden sind und ob sie über IIS von einer anderen Workstation aus zugänglich sind, bevor Sie mit diesem Abschnitt beginnen.

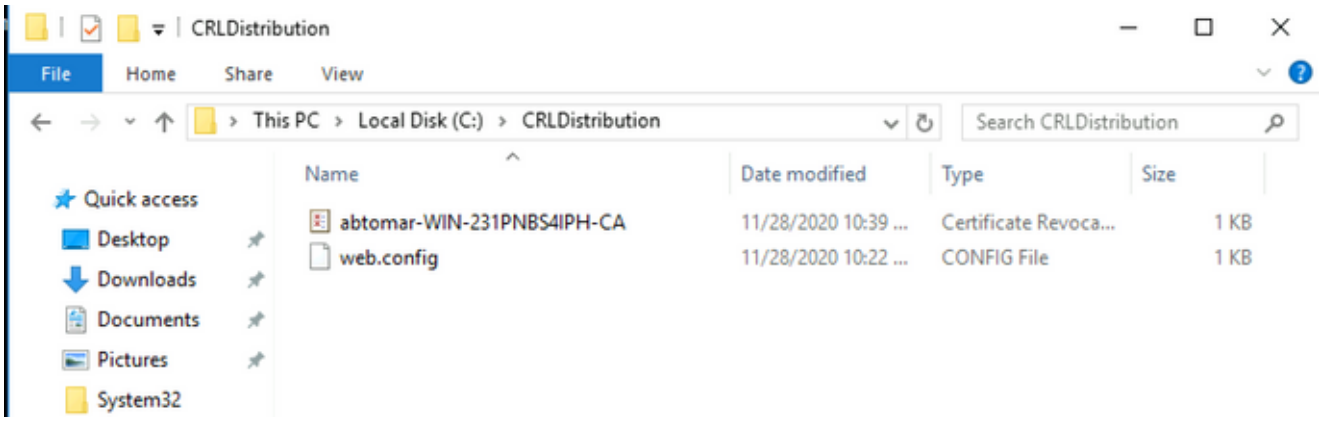
1. Öffnen Sie auf dem IIS-Server den in Abschnitt 1 erstellten Ordner. Es muss eine einzelne .crl-Datei mit dem Formular vorhanden sein,

   .crl

   wobei

   für den Namen des Zertifizierungsstellenservers steht. 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://

   /

   , wobei

   der in Abschnitt 2 konfigurierte Servername des IIS-Servers und

   der für den Verteilungspunkt in Abschnitt 2 ausgewählte Standortname ist. In diesem Beispiel lautet die URL:

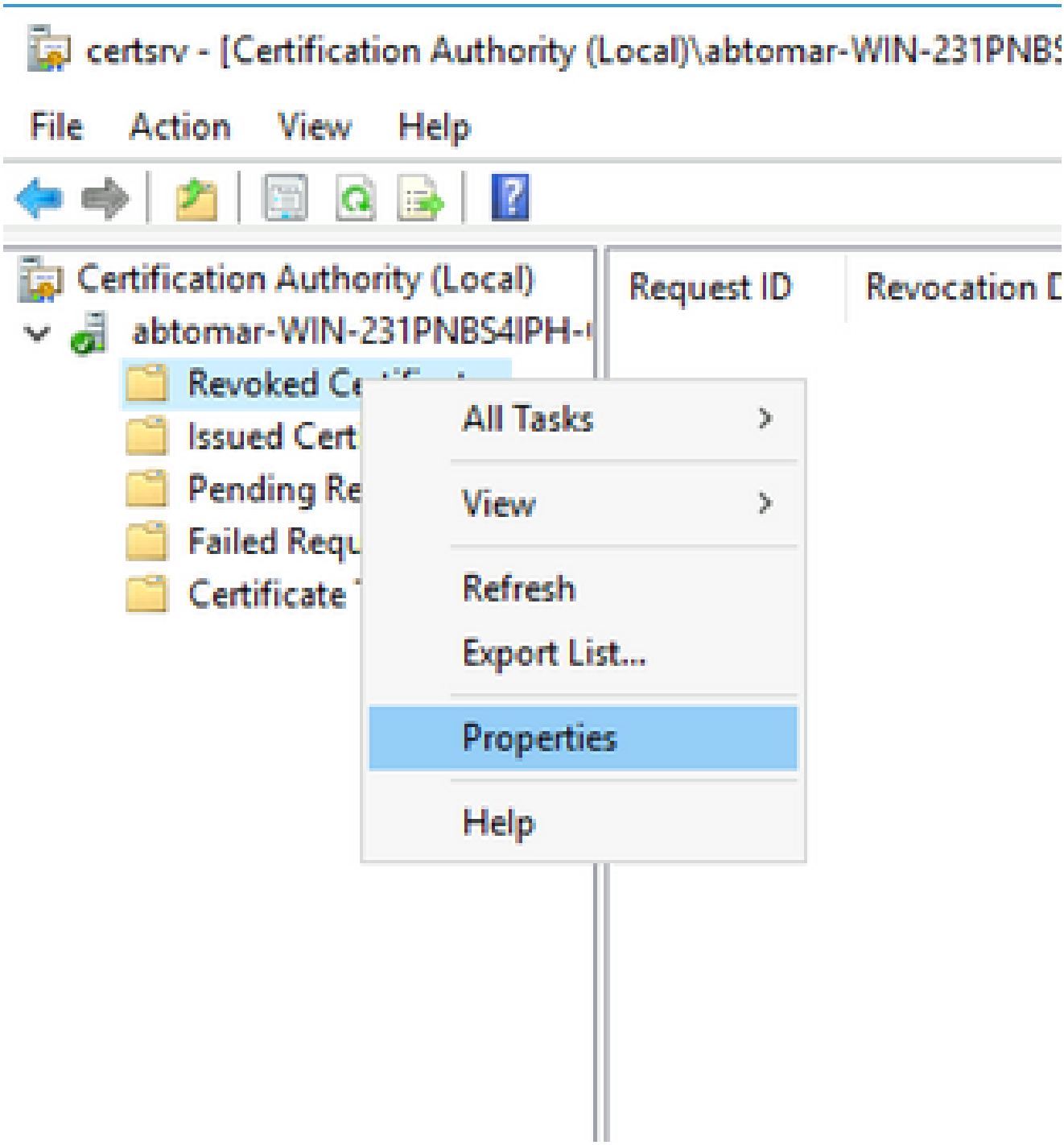
   http://win-231pnbs4iph/CRLD

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

Konfigurieren der ISE zur Verwendung des neuen CRL-Verteilungspunkts

Bevor die ISE zum Abrufen der Zertifikatsperrliste konfiguriert wird, definieren Sie das Intervall zum Veröffentlichen der Zertifikatsperrliste. Die Strategie zur Bestimmung dieses Intervalls geht über den Rahmen dieses Dokuments hinaus. Die potenziellen Werte (in Microsoft CA) betragen 1 Stunde bis einschließlich 411 Jahre. Der Standardwert ist 1 Woche. Wenn Sie ein für Ihre Umgebung geeignetes Intervall festgelegt haben, gehen Sie wie folgt vor, um das Intervall festzulegen:

1. Klicken Sie in der Taskleiste des CA-Servers auf **Start**. Wählen Sie **Administrative Tools** > **Certificate Authority**.
2. Erweitern Sie im linken Bereich die Zertifizierungsstelle. Klicken Sie mit der rechten Maustaste auf den **Revoked Certificates** Ordner, und wählen Sie **Properties**.
3. Geben Sie in die Felder für das Veröffentlichungsintervall der Zertifikatsperrliste die erforderliche Anzahl 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 sieben Tagen konfiguriert.



4. Geben Sie den **certutil -getreg CA\Clock*** Befehl zur Bestätigung des ClockSkew-Werts ein. Der Standardwert ist 10 Minuten.

   Beispiel:

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

5. Geben Sie den **certutil -getreg CA\CRLov*** Befehl ein, um zu überprüfen, ob CRLOverlapPeriod manuell festgelegt wurde. Standardmäßig ist der CRLOverlapUnit-Wert 0, was darauf

hinweist, dass kein manueller Wert festgelegt wurde. Wenn der Wert ein anderer Wert als 0 ist, zeichnen Sie den Wert und die Einheiten auf.

Beispiel:

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

6. Geben Sie den **certutil -getreg CA\CRLpe*** Befehl zum Überprüfen der CRLPeriod ein, der in Schritt 3 festgelegt wurde.

   Beispiel:

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

7. Berechnen Sie die Sperrlisten-Kulanzfrist wie folgt:

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

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

   b. Wenn ÜBERLAPPUNG > 720, dann ÜBERLAPPUNG = 720

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

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

   e. Toleranzperiode = ÜBERLAPPUNG + UhrVerzerrungMinuten

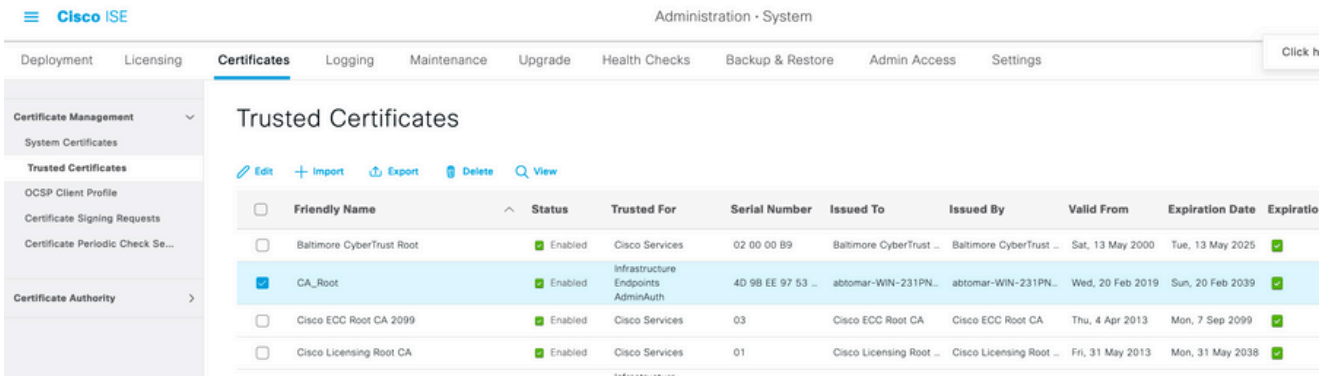
```
Example:

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 berechnete Kulanzfrist ist der Zeitraum zwischen dem Veröffentlichen der nächsten Zertifikatsperrliste durch die Zertifizierungsstelle und dem Ablauf der aktuellen Zertifikatsperrliste. Die ISE muss so konfiguriert werden, dass die Zertifikatsperrlisten entsprechend abgerufen werden können.

8. Melden Sie sich beim ISE-Knoten "Primärer Admin" an, und wählen Sie **Administration** > **System** > **Certificates**. Wählen Sie im linken Bereich **Trusted Certificate**.

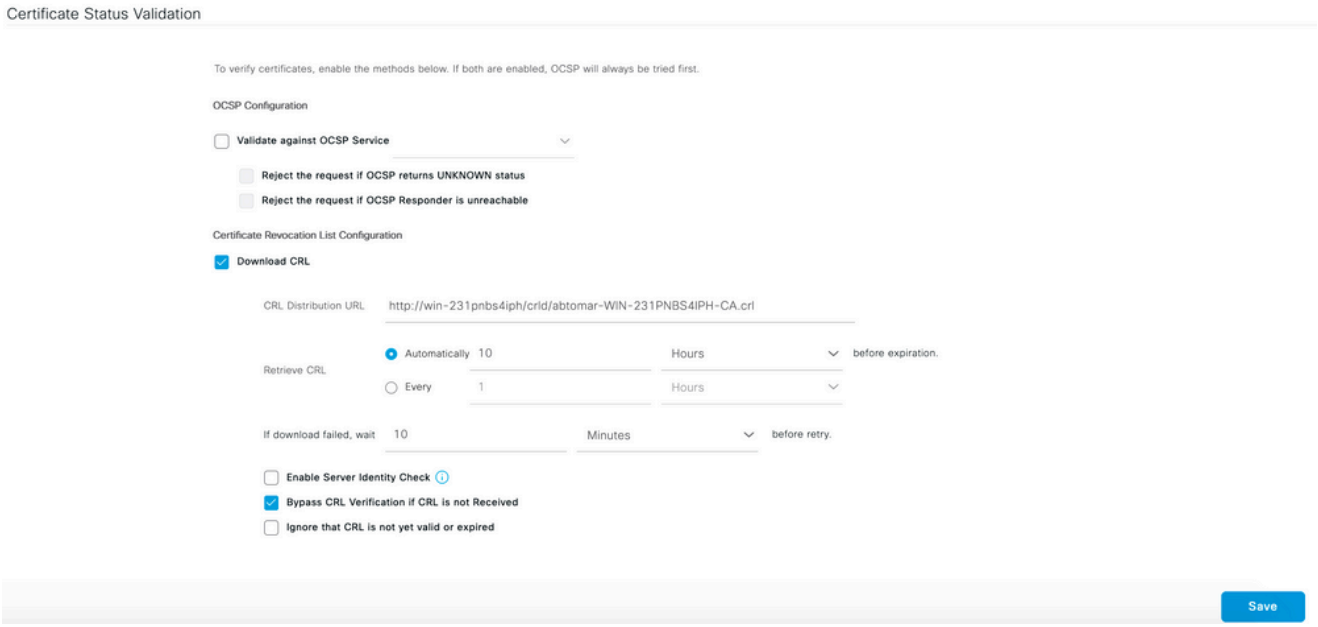


9. Aktivieren Sie das Kontrollkästchen neben dem Zertifizierungsstellenzertifikat, für das Sie Zertifikatsperrlisten konfigurieren möchten. Klicken Sie auf **.Edit**
10. Aktivieren Sie das **Download CRL** Kontrollkästchen unten im Fenster.
11. Geben Sie im Feld "CRL Distribution URL" (URL für Zertifikatsperrlisten-Verteilung) 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 die Zertifikatsperrliste in regelmäßigen Abständen oder auf Basis des Ablaufdatums abgerufen wird (was im Allgemeinen ebenfalls ein regelmäßiges Intervall ist). Wenn das CRL-Veröffentlichungsintervall statisch ist, werden bei Verwendung der zweiten Option schnellere CRL-Updates abgerufen. Klicken Sie auf das **Automatically** Optionsfeld.
13. Stellen Sie den Wert für den Abruf auf einen Wert ein, der kleiner ist als der in Schritt 7 berechnete Kulanzzeitraum. Wenn der eingestellte Wert die Toleranzperiode überschreitet, überprüft die ISE den Sperrlisten-Verteilungspunkt, bevor die Zertifizierungsstelle die nächste Sperrliste veröffentlicht hat. In diesem Beispiel wird die Kulanzfrist auf 730 Minuten bzw. 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 Zertifikatsperrliste im vorigen Schritt nicht im konfigurierten Intervall abrufen kann, wird in diesem kürzeren Intervall ein erneuter Versuch unternommen.
15. Aktivieren Sie das **Bypass CRL Verification if CRL is not Received** Kontrollkästchen, damit die zertifikatbasierte Authentifizierung normal (und ohne CRL-Prüfung) fortgesetzt werden kann, wenn ISE die CRL für diese CA beim letzten Downloadversuch nicht abrufen konnte. Wenn dieses Kontrollkästchen nicht aktiviert ist, schlägt die gesamte zertifikatbasierte Authentifizierung mit von dieser Zertifizierungsstelle ausgestellten Zertifikaten fehl, wenn die Zertifikatsperrliste nicht abgerufen werden kann.

16. Aktivieren Sie das **Ignore that CRL is not yet valid or expired** Kontrollkästchen, damit ISE abgelaufene (oder noch nicht gültige) Sperrlisten-Dateien so verwenden kann, als wären sie gültig. Wenn dieses Kontrollkästchen nicht aktiviert ist, betrachtet die ISE eine Sperrliste vor dem Datum des In-Kraft-Tretens und nach dem Zeitpunkt der nächsten Aktualisierung als ungültig. Klicken Sie hier**Save**, um die Konfiguration abzuschließen.



Überprüfung

Für diese Konfiguration ist derzeit kein Überprüfungsverfahren verfügbar.

Fehlerbehebung

Für diese Konfiguration sind derzeit keine spezifischen Informationen zur Fehlerbehebung verfügbar.

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.