نشر قوائم إبطال الشهادات ل ISE على مثال تكوين Microsoft CA Server

المحتويات

المقدمة

يصف هذا المستند تكوين خادم Microsoft Certificate Authority (CA) الذي يقوم بتشغيل خدمات معلومات الإنترنت (IIS) لنشر تحديثات قائمة إبطال الشهادات (CRL). وهو يشرح أيضا كيفية تكوين محرك خدمات تعريف Cisco (ISE) (الإصدارات 1.1 والإصدارات الأحدث) لاسترداد التحديثات لاستخدامها في التحقق من صحة الشهادة. يمكن تكوين ISE لاسترداد CRLs لشهادات جذر CA المختلفة التي يستخدمها في التحقق من صحة الشهادة.

المتطلبات الأساسية

المتطلبات

لا توجد متطلبات خاصة لهذا المستند.

المكونات المستخدمة

تستند المعلومات الواردة في هذا المستند إلى إصدارات البرامج والمكونات المادية التالية:

- Cisco Identity Services Engine، الإصدار 1.1.2.145
- نظام التشغيل Microsoft Windows® Server® 2008 R2

تم إنشاء المعلومات الواردة في هذا المستند من الأجهزة الموجودة في بيئة معملية خاصة. بدأت جميع الأجهزة

المُستخدمة في هذا المستند بتكوين ممسوح (افتراضي). إذا كانت شبكتك مباشرة، فتأكد من فهمك للتأثير المحتمل لأي أمر.

الاصطلاحات

راجع اصطلاحات تلميحات Cisco التقنية للحصول على مزيد من المعلومات حول اصطلاحات المستندات.

التكوين

في هذا القسم، تُقدّم لك معلومات تكوين الميزات الموضحة في هذا المستند.

ملاحظة: أستخدم أداة بحث الأوامر (للعملاء المسجلين فقط) للحصول على مزيد من المعلومات حول الأوامر المستخدمة في هذا القسم.

التكوينات

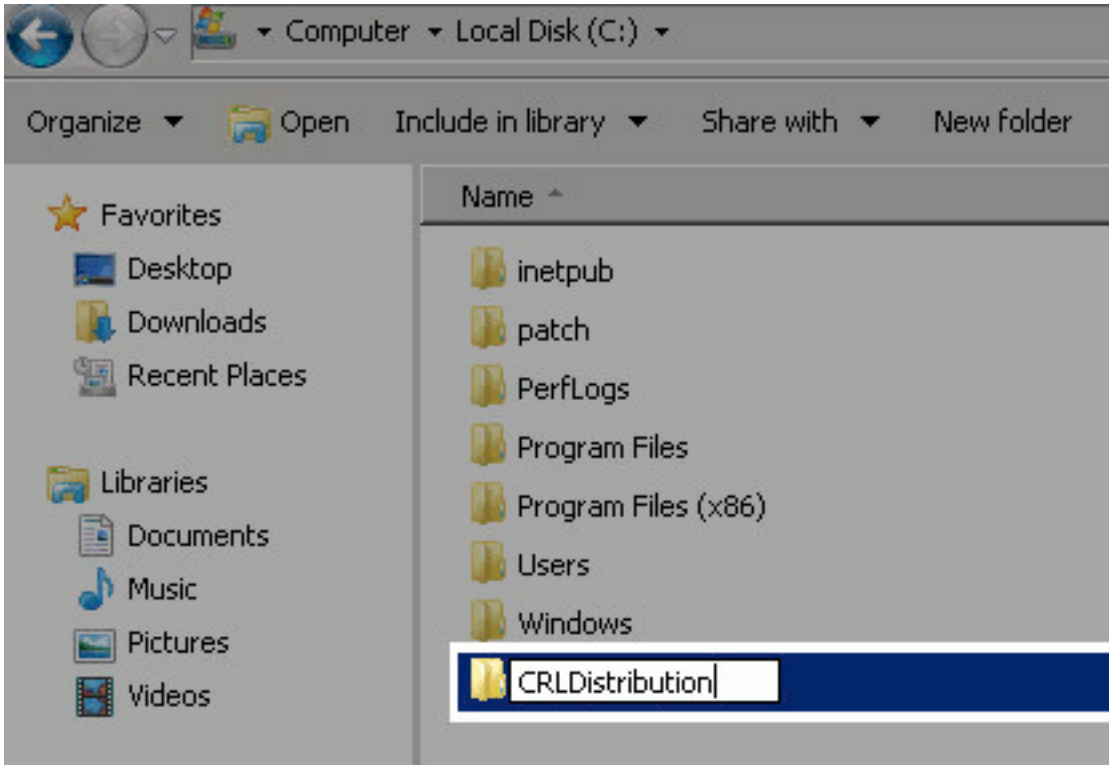
يستخدم هذا المستند التكوينات التالية:

- الباب 1. إنشاء مجلد وتكوينه على المرجع المصدق لتضمين ملفات CRL
- الباب 2. إنشاء موقع في IIS لكشف نقطة توزيع CRL الجديدة
- الباب 3. تكوين خادم Microsoft CA لنشر ملفات CRL إلى نقطة التوزيع
- الباب 4. التحقق من وجود ملف CRL وإمكانية الوصول إليه عبر IIS
- الباب 5. تكوين ISE لاستخدام نقطة توزيع CRL الجديدة

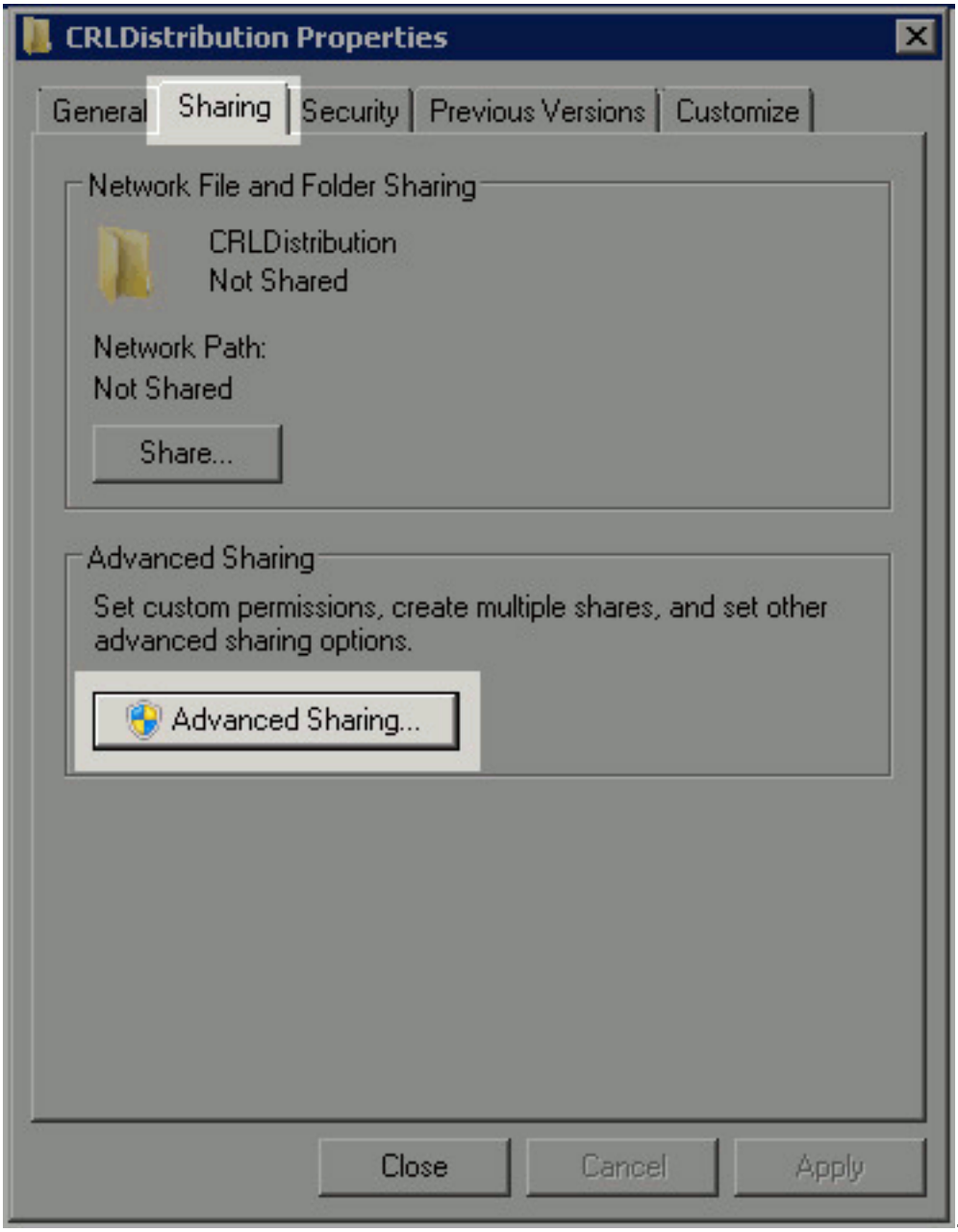
الباب 1. إنشاء مجلد وتكوينه على المرجع المصدق لتضمين ملفات CRL

تتمثل المهمة الأولى في تكوين موقع على خادم CA لتخزين ملفات CRL. بشكل افتراضي، يقوم خادم Microsoft CA بنشر الملفات إلى C:\Windows\system32\CertSrv\CertEnroll\ . بدلا من إستخدام مجلد النظام هذا، قم بإنشاء مجلد جديد للملفات.

1. على خادم IIS، أختر موقعا على نظام الملفات وقم بإنشاء مجلد جديد. في هذا المثال، يتم إنشاء المجلد C:\CRLDistribution.

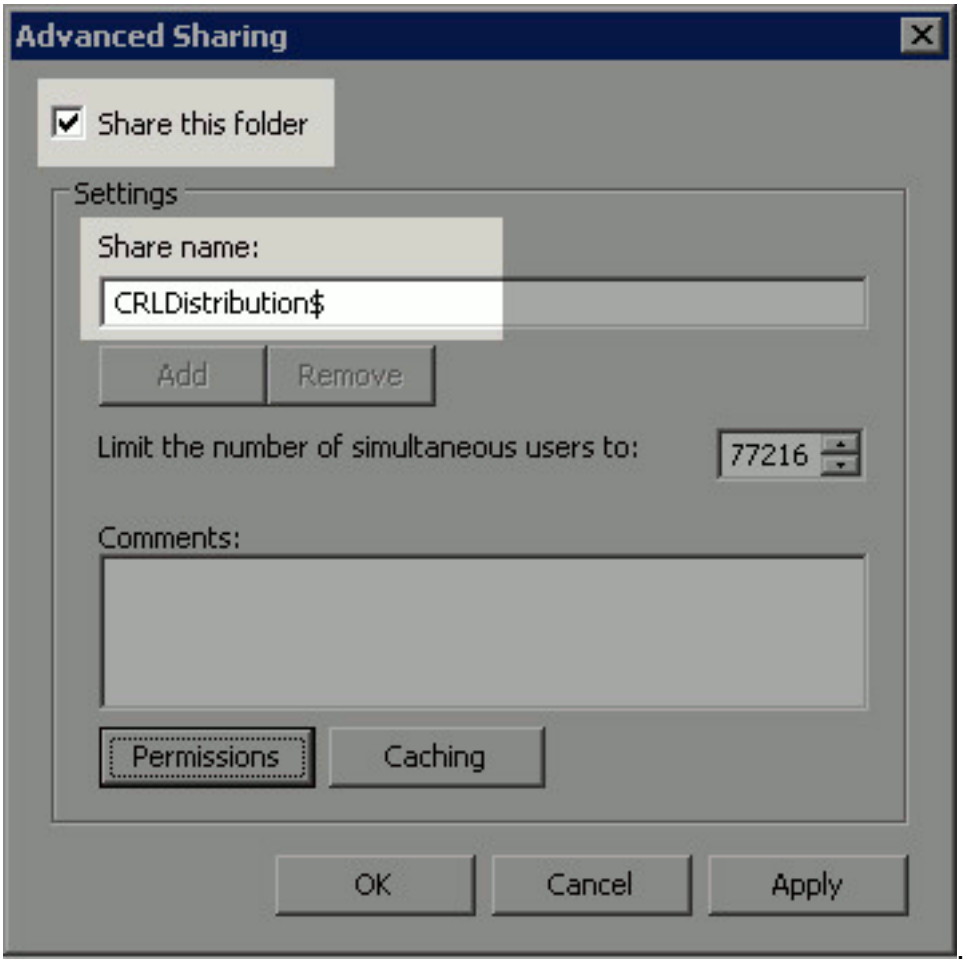


2. لكي يتمكن المرجع المصدق من كتابة ملفات CRL إلى المجلد الجديد، يجب تمكين المشاركة. انقر بزر الماوس الأيمن فوق المجلد الجديد، واختر **خصائص**، وانقر فوق علامة التبويب **مشاركة**، ثم انقر فوق **مشاركة**



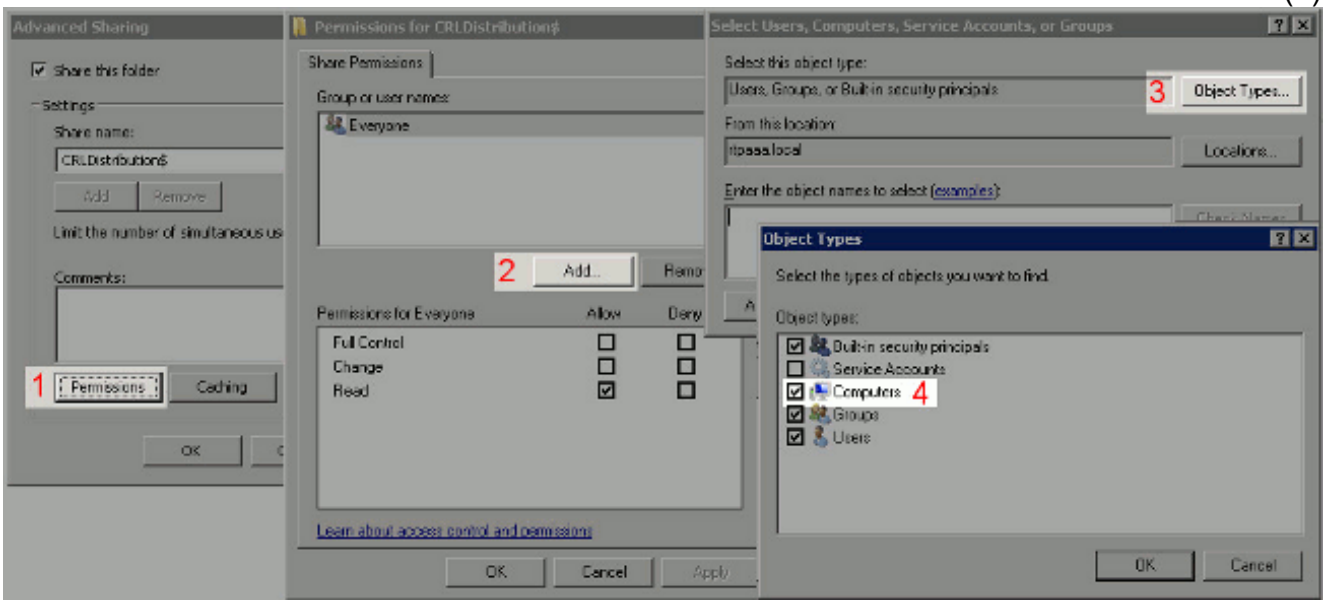
متقدمة.

3. لمشاركة المجلد، حدد خانة الاختيار **مشاركة هذا المجلد** ثم قم بإضافة علامة دولار ($) إلى نهاية اسم المشاركة في حقل اسم المشاركة لإخفاء

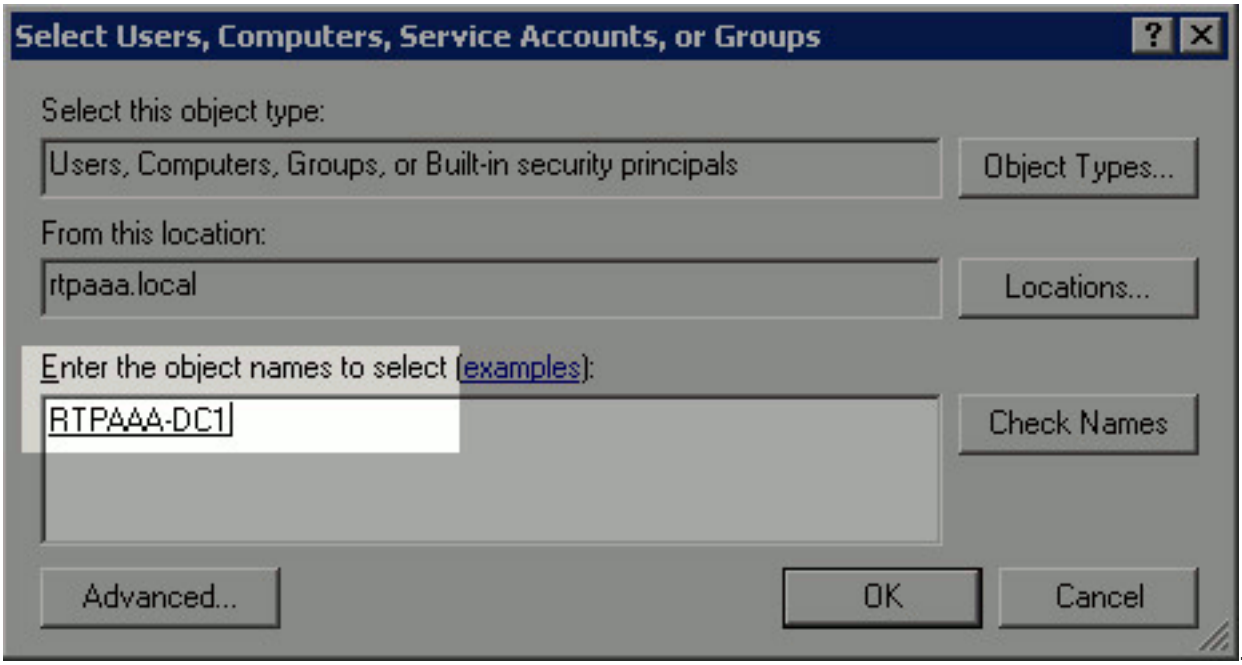


المشاركة.

4. انقر فوق **أذون** (1)، وانقر فوق **إضافة** (2)، وانقر فوق **أنواع الكائن** (3)، وحدد خانة الاختيار **أجهزة الكمبيوتر** (4).

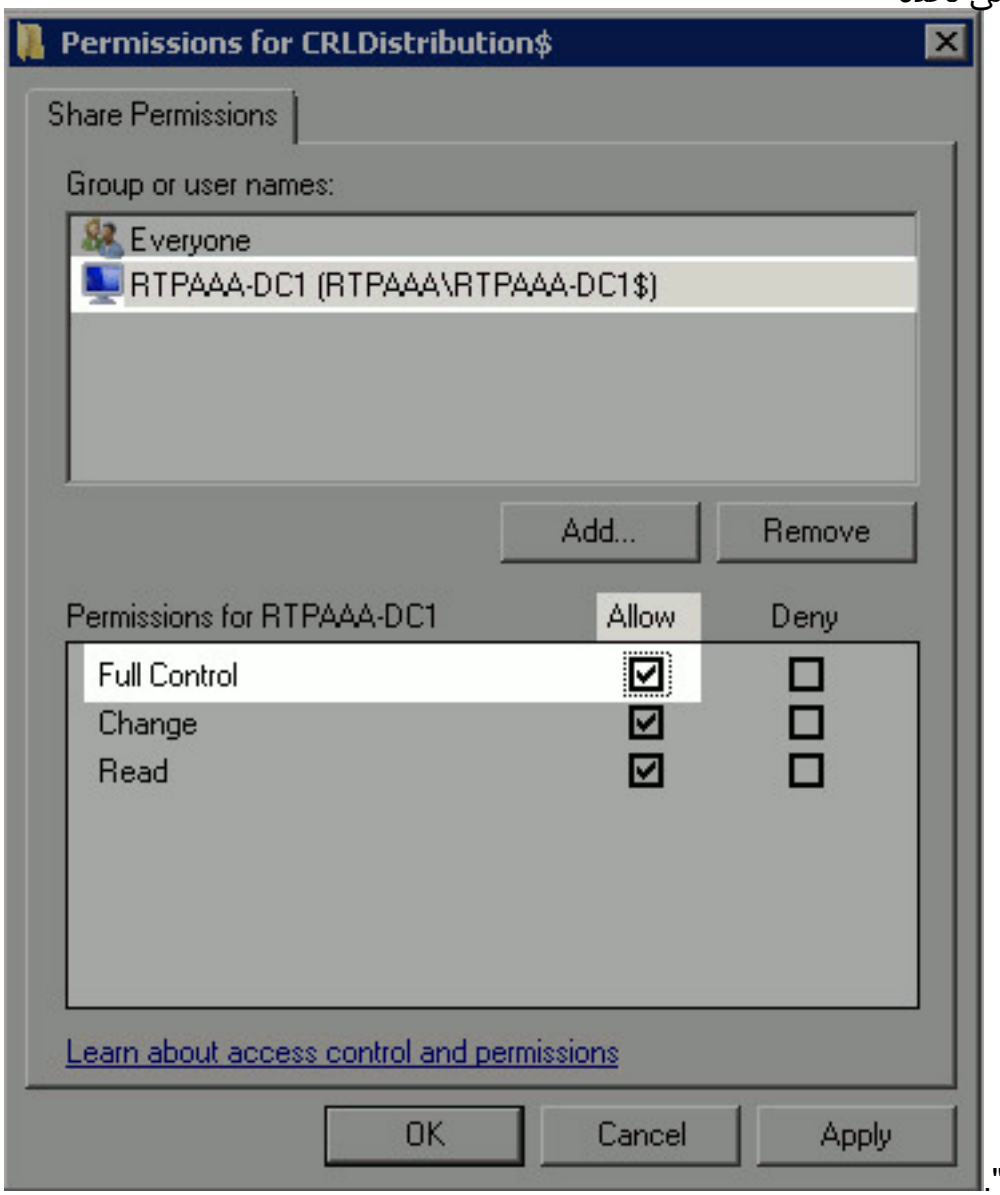


5. للعودة إلى إطار تحديد المستخدمين أو أجهزة الكمبيوتر أو حسابات الخدمات أو المجموعات، انقر فوق **موافق**. في الحقل إدخال أسماء الكائنات لتحديد ، أدخل اسم الكمبيوتر الخاص بخادم المرجع المصدق وانقر فوق **التحقق من الأسماء**. إذا كان الاسم الذي تم إدخاله صالحا، فإن الاسم يتم تحديثه ويظهر تحته خط. وانقر فوق



.OK

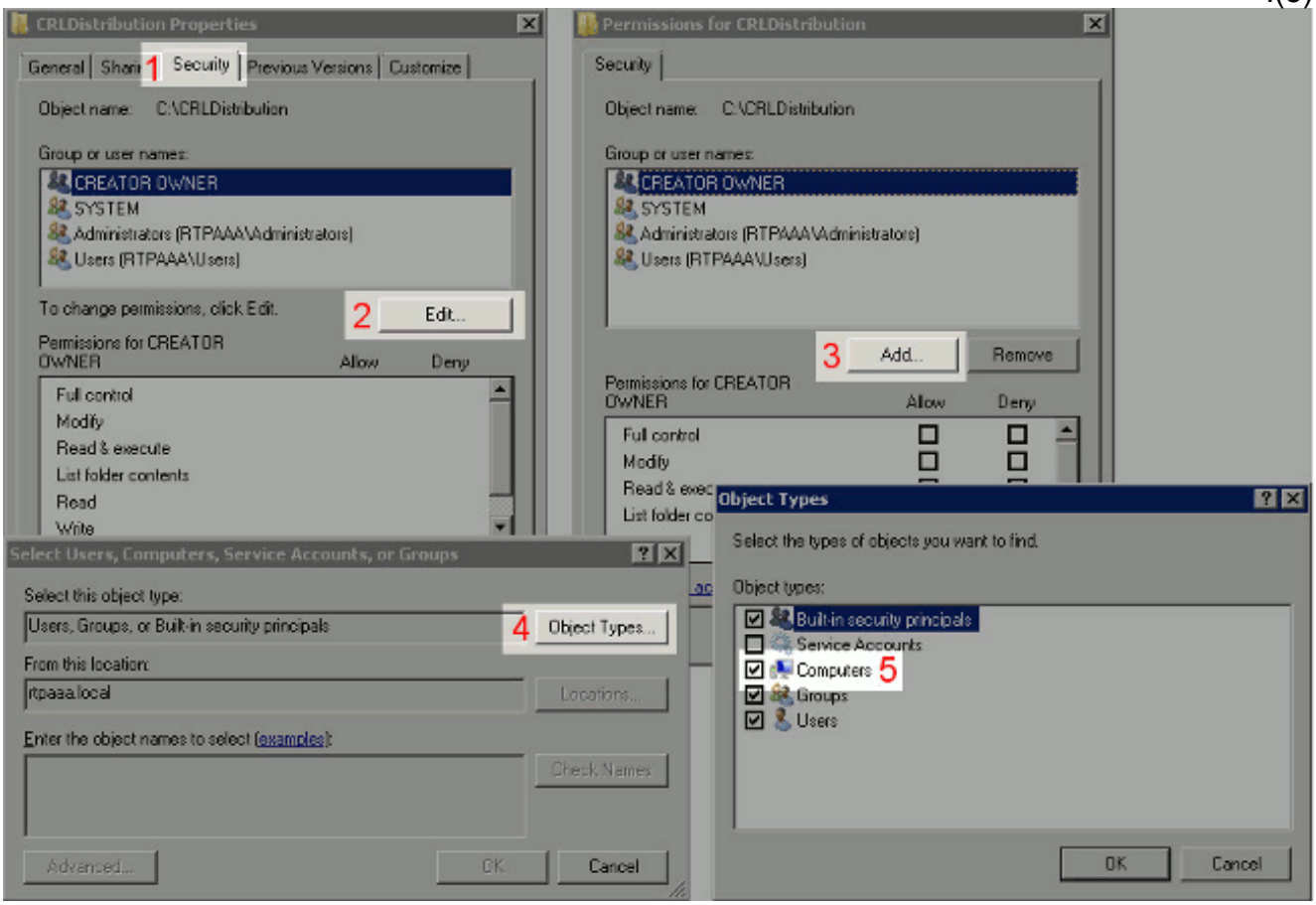
6. في حقل المجموعة أو أسماء المستخدمين، أختر حاسب CA. حدد **السماح** بالتحكم الكامل لمنح الوصول الكامل إلى المرجع المصدق. وانقر فوق OK. انقر فوق **موافق** مرة أخرى لإغلاق نافذة "المشاركة المتقدمة" والرجوع إلى نافذة



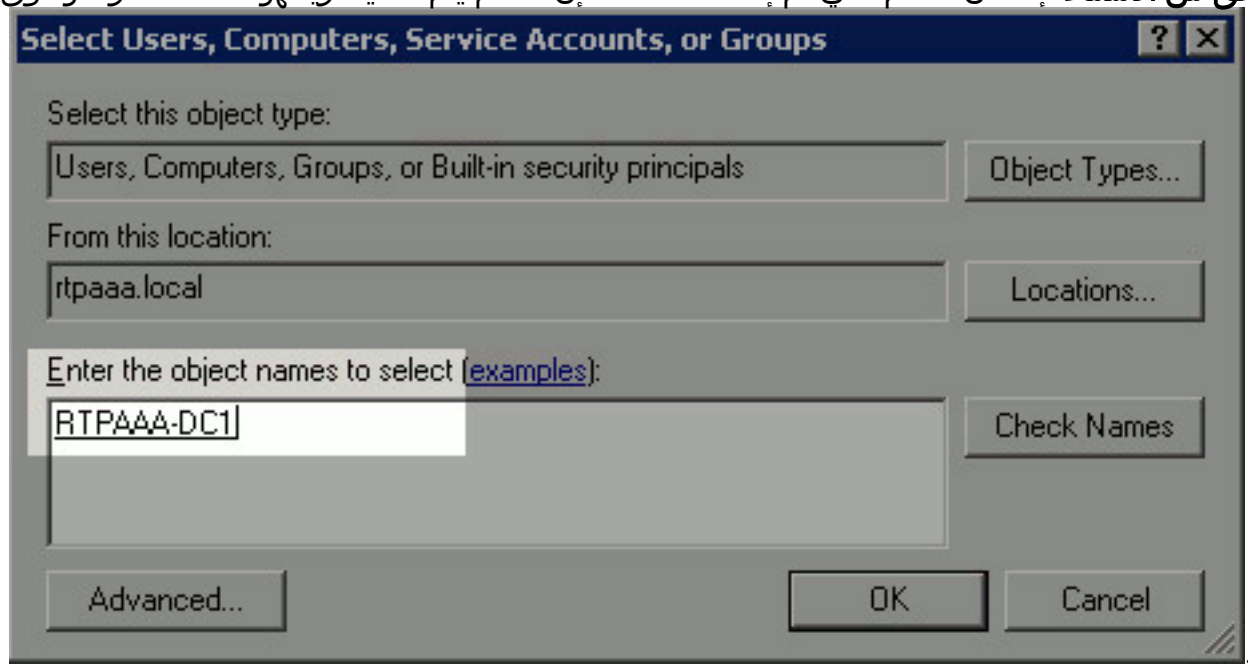
"خصائص".

7. للسماح ل CA بكتابة ملفات CRL إلى المجلد الجديد، قم بتكوين أذونات الأمان المناسبة. انقر فوق علامة

التبويب تأمين (1)، وانقر فوق **تحرير** (2)، وانقر فوق **إضافة** (3)، وانقر فوق **أنواع الكائن** (4)، وحدد خانة الاختيار أجهزة الكمبيوتر
(5).

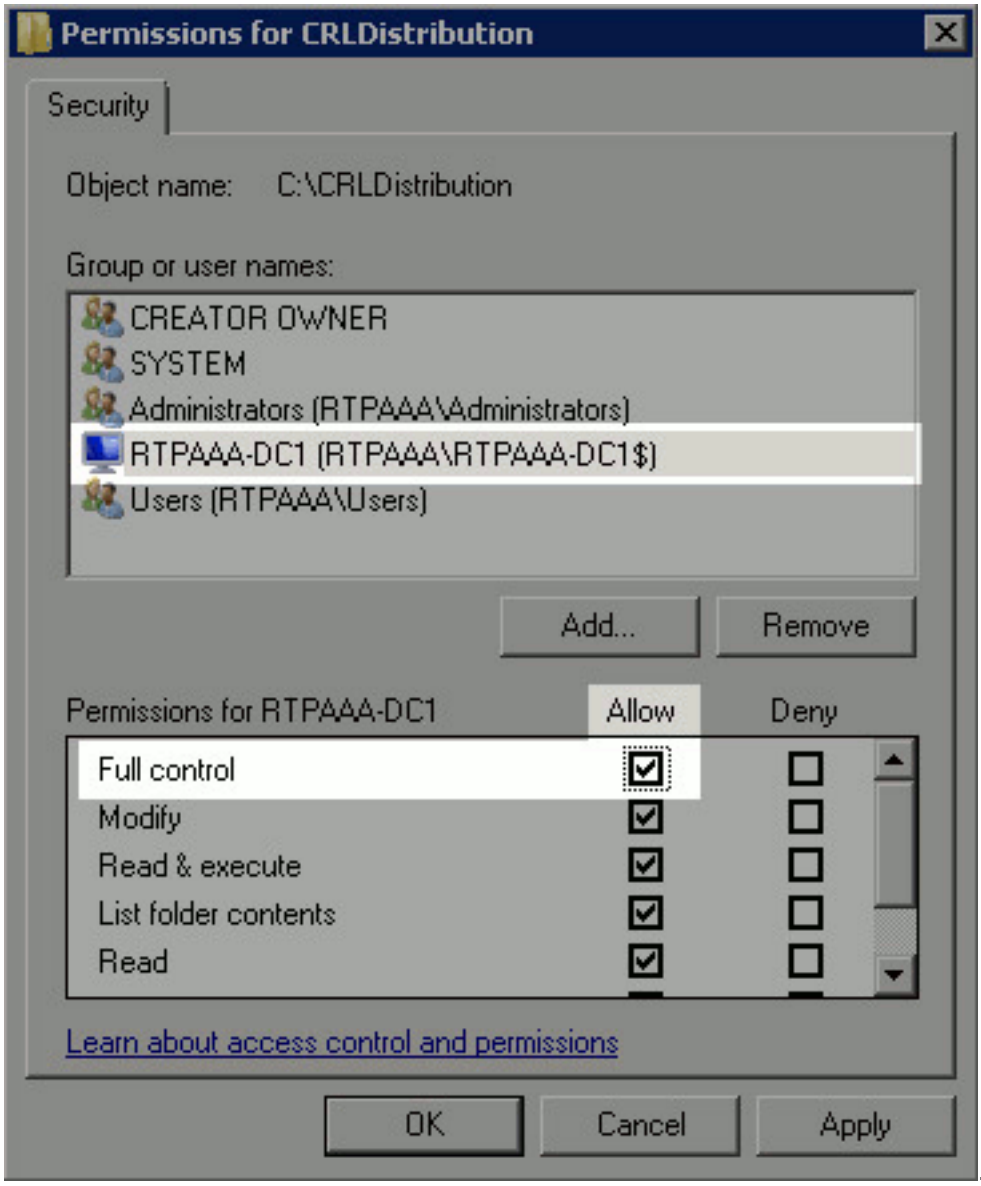


8. في الحقل إدخال أسماء الكائنات لتحديد ، أدخل اسم الكمبيوتر الخاص بخادم المرجع المصدق وانقر فوق **التحقق من الأسماء**. إذا كان الاسم الذي تم إدخاله صالحا، فإن الاسم يتم تحديثه ويظهر تحته خط. وانقر فوق



.OK

9. أختر كمبيوتر المرجع المصدق في حقل المجموعة أو أسماء المستخدمين ثم حدد **السماح** بالتحكم الكامل لمنح الوصول الكامل إلى المرجع المصدق. انقر فوق **موافق** ثم انقر فوق **إغلاق** لإكمال

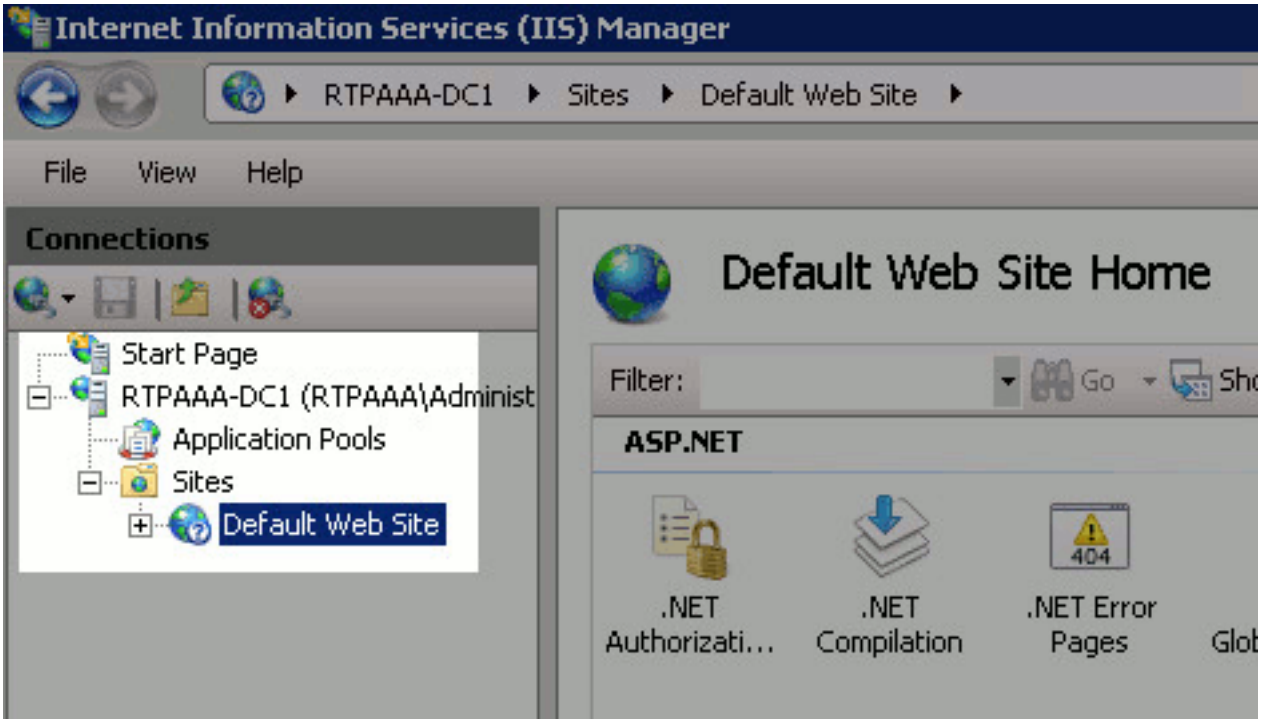


المهمة.

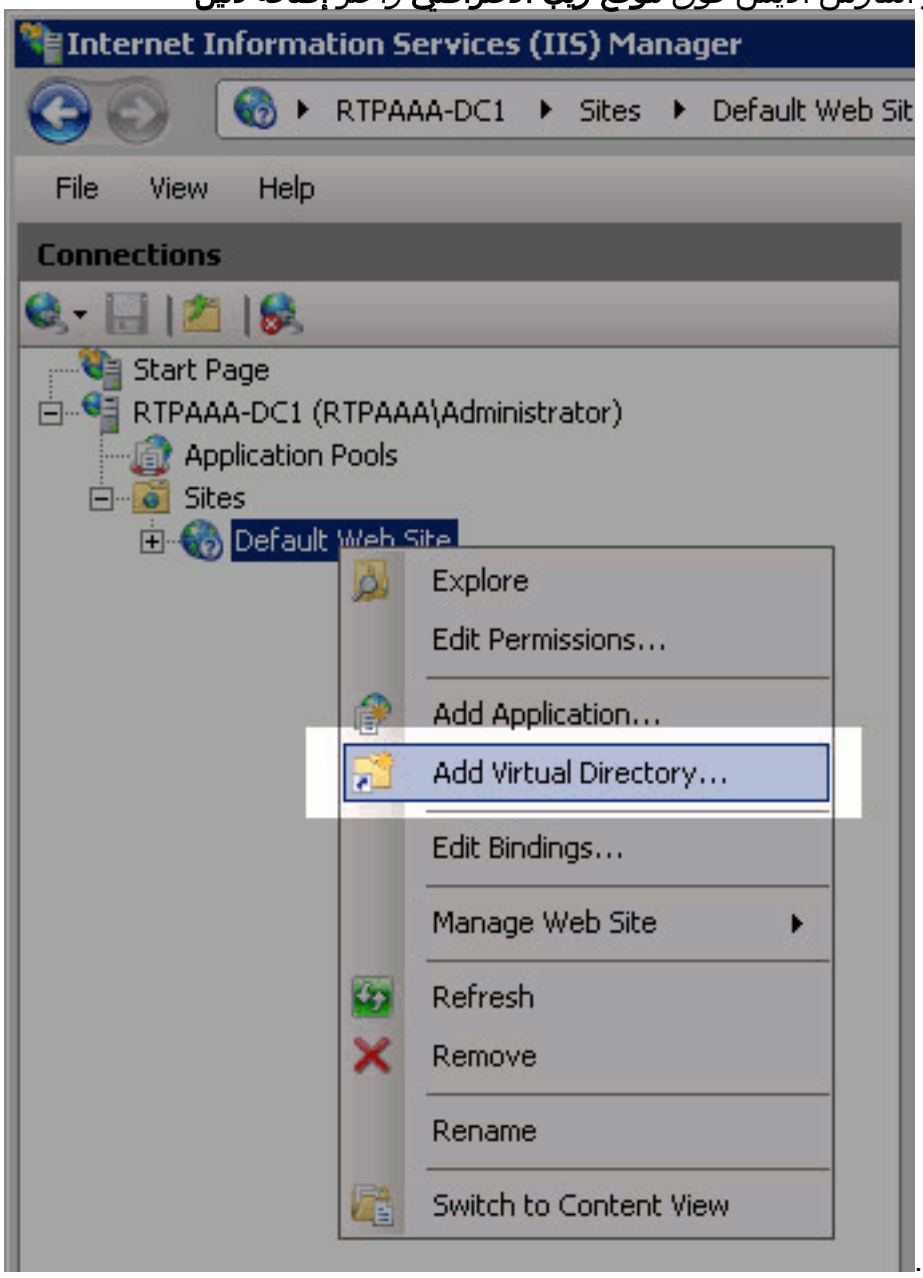
الباب 2. إنشاء موقع في IIS لكشف نقطة توزيع CRL الجديدة

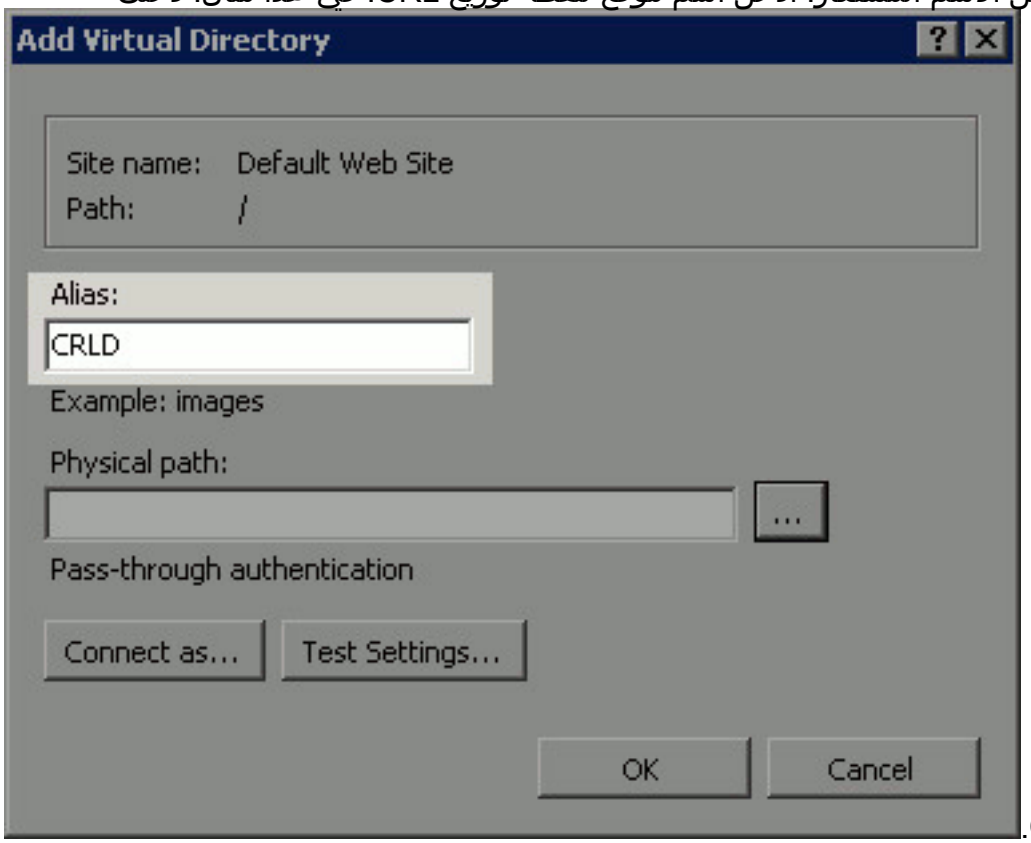
لتمكين ISE من الوصول إلى ملفات CRL، أجعل الدليل الذي يضم ملفات CRL يمكن الوصول إليه عبر IIS.

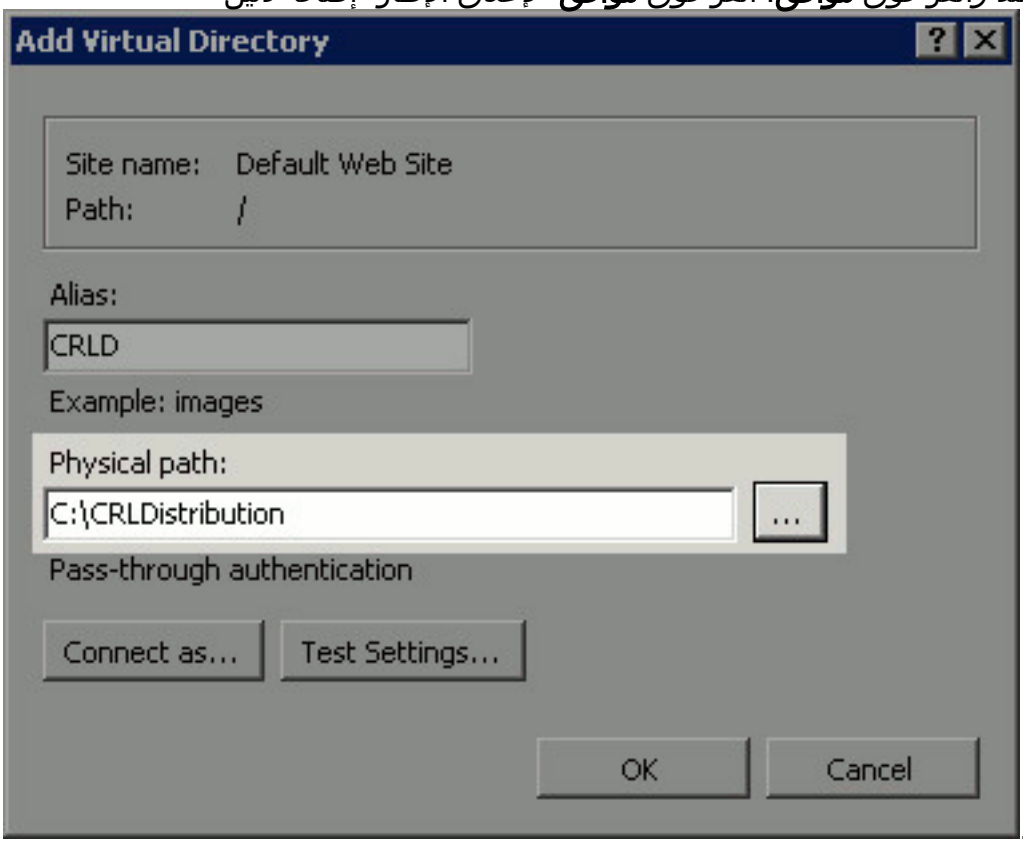
1. في شريط مهام خادم IIS، انقر فوق **بدء**. أختر **أدوات إدارية > إدارة خدمات معلومات الإنترنت (IIS)**.
2. في الجزء الأيسر (المعروف باسم شجرة وحدة التحكم)، قم بتوسيع اسم خادم IIS ثم قم بتوسيع **المواقع**.



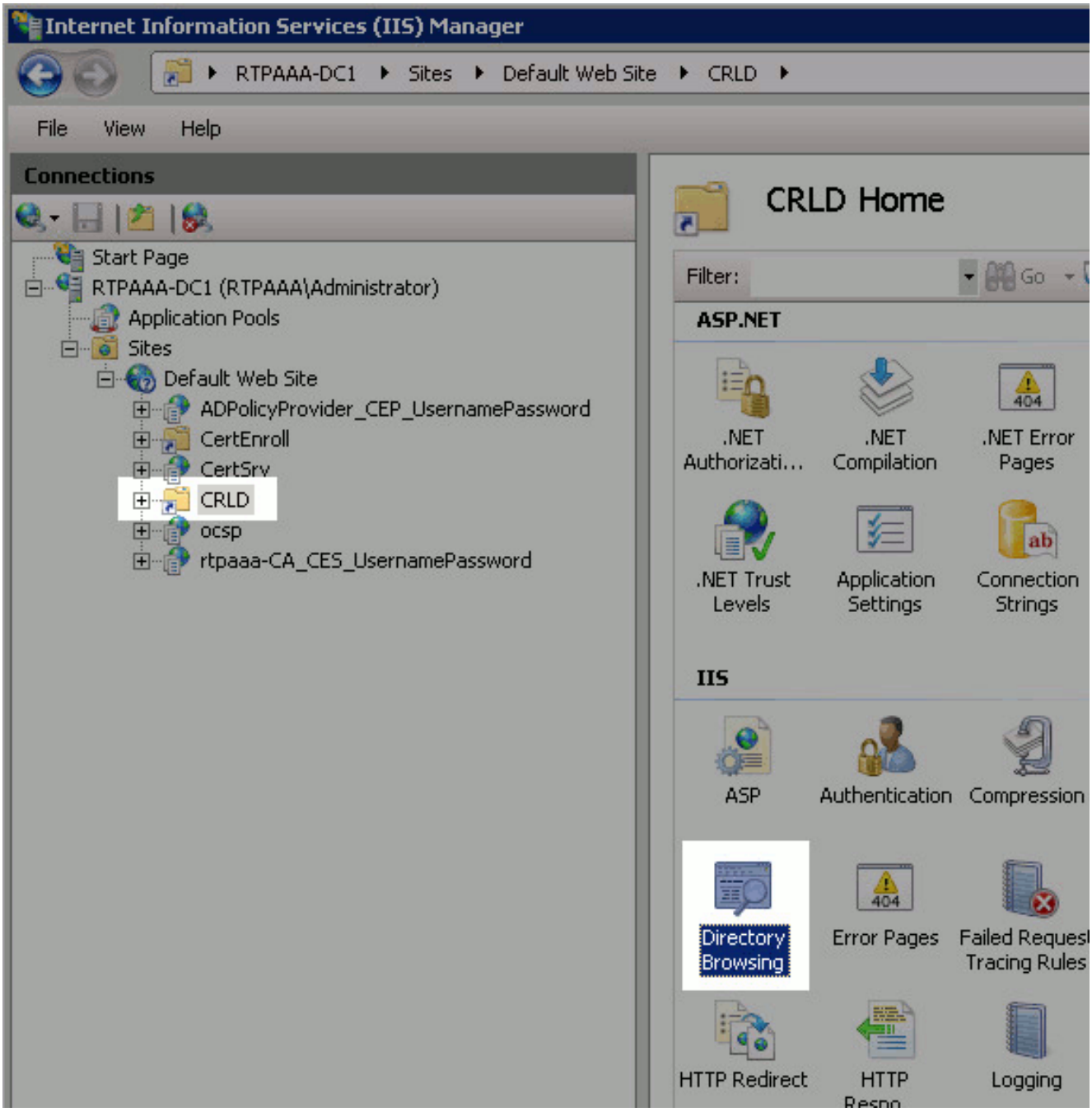
3. انقر بزر الماوس الأيمن فوق **موقع ويب الافتراضي** واختر **إضافة دليل ظاهري**.



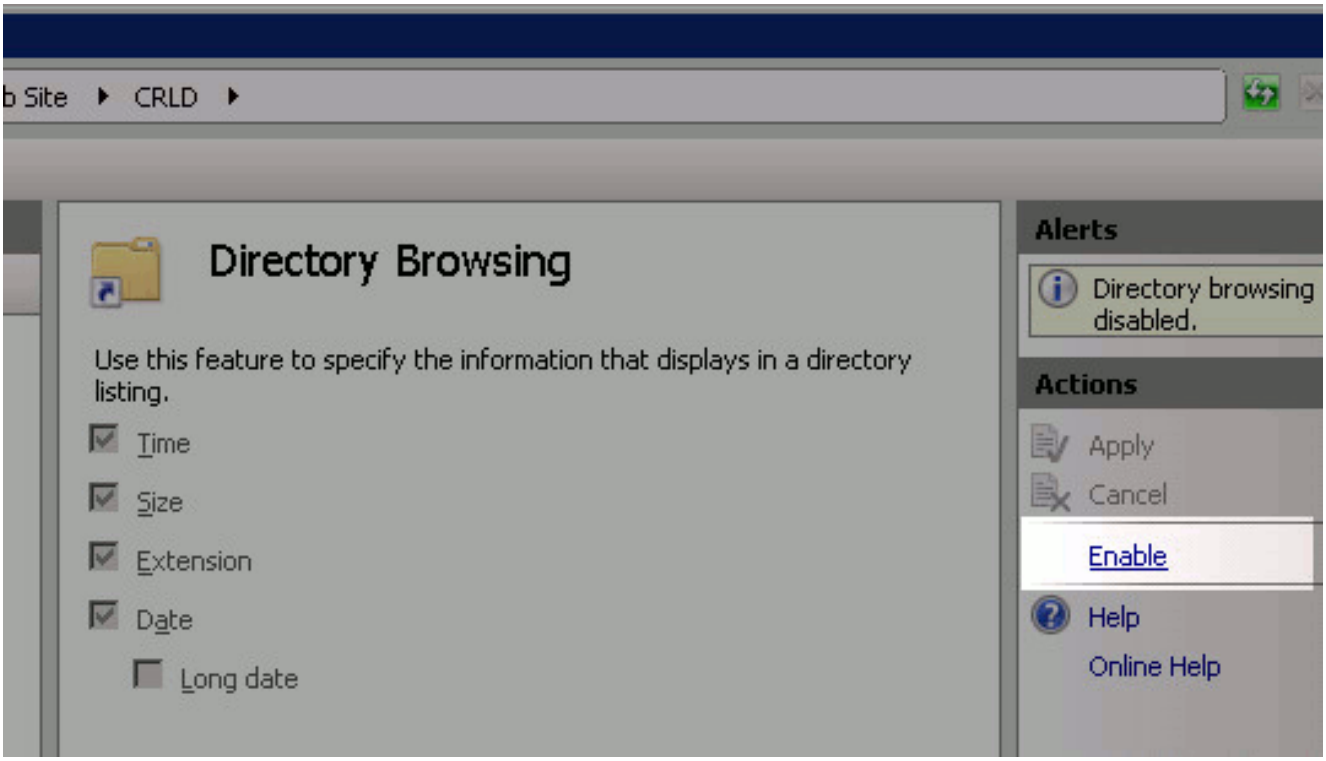
4. في حقل الاسم المستعار، أدخل اسم موقع لنقطة توزيع CRL. في هذا مثال، دخلت


CRLD.
5. انقر فوق البيضاوي (. . .) إلى يمين حقل المسار الفعلي واستعرض إلى المجلد الذي تم إنشاؤه في القسم 1. حدد المجلد وانقر فوق **موافق**. انقر فوق **موافق**" لإغلاق الإطار "إضافة دليل


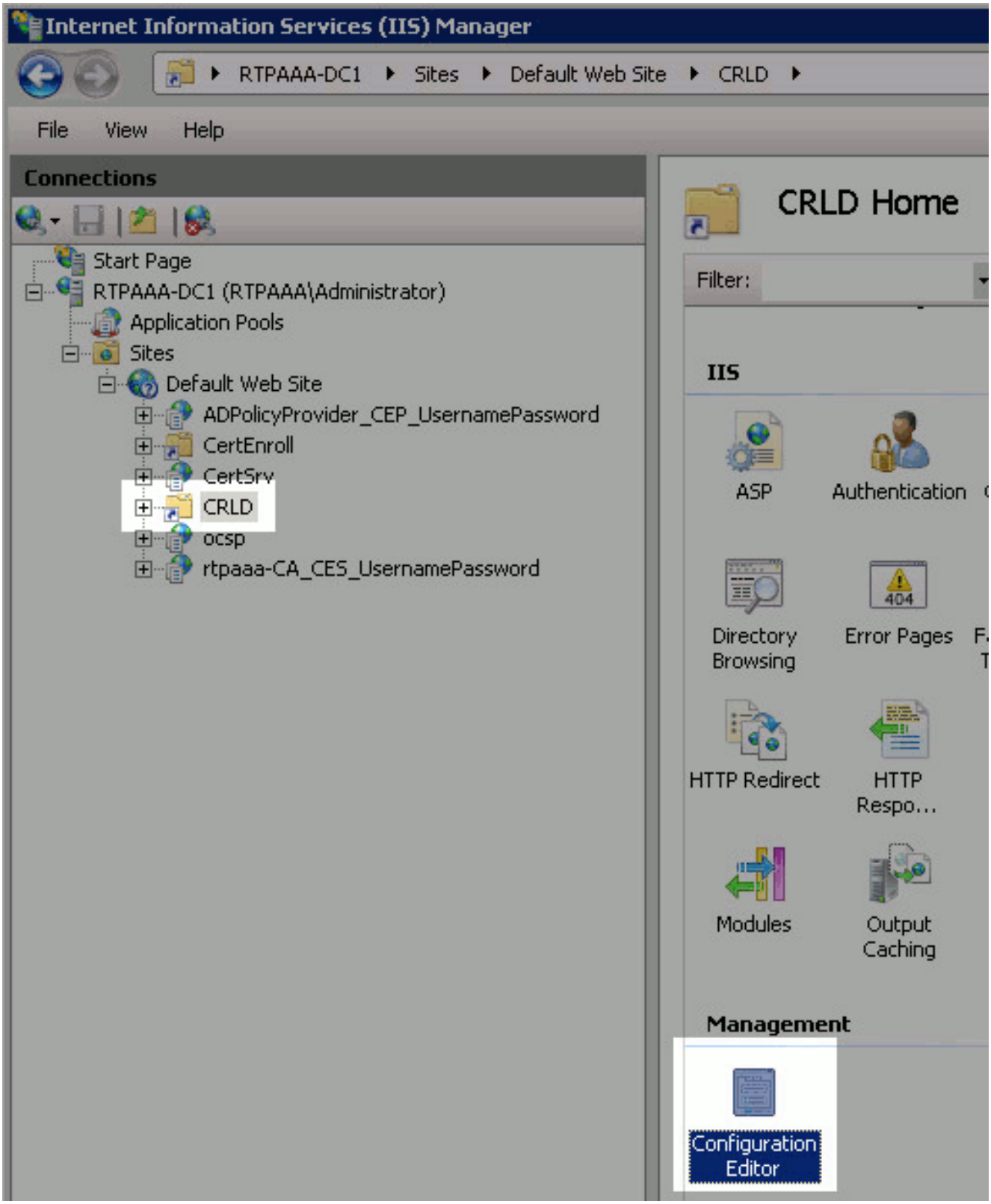
ظاهري".
6. يجب إبراز اسم الموقع الذي تم إدخاله في الخطوة 4 في الجزء الأيسر. إذا لم تكن كذلك، فعليك باختياره الآن. في الجزء الأوسط، انقر نقرا مزدوجا فوق **إستعراض الدليل**.



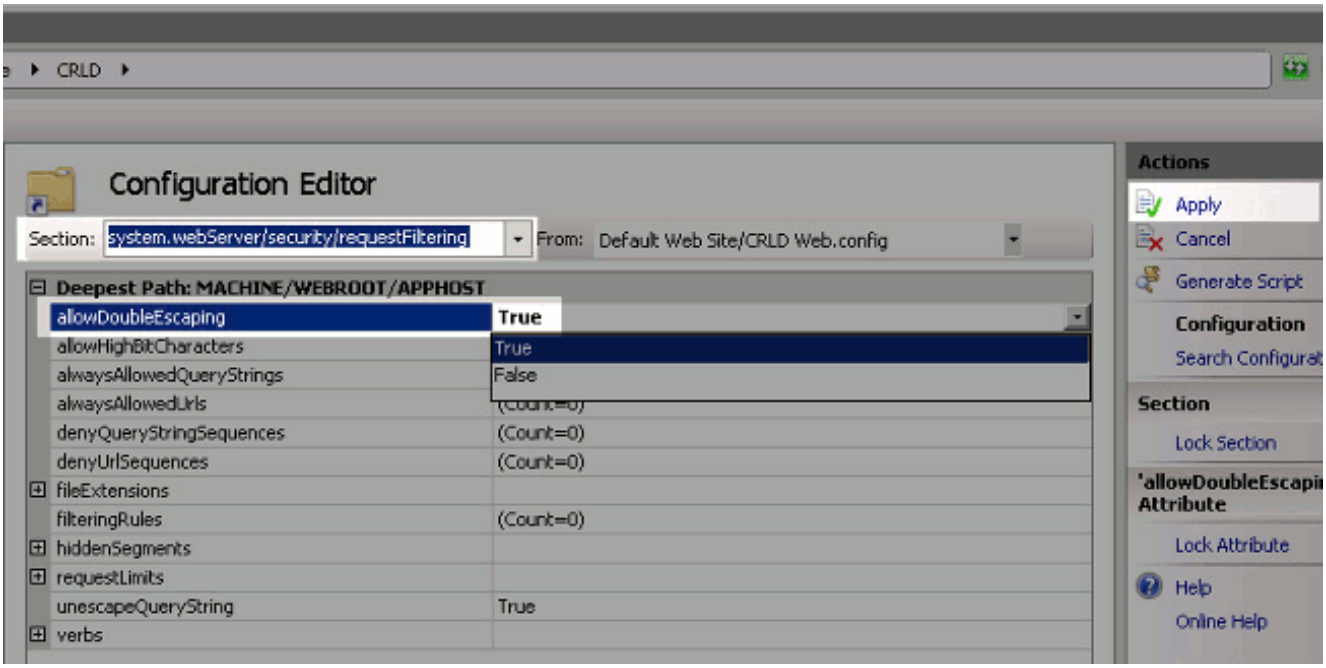
7. في الجزء الأيمن، انقر فوق **تمكين** لتمكين إستعراض الدليل.



8. في الجزء الأيسر، أختر اسم الموقع مرة أخرى. في الجزء الأوسط، انقر نقرا مزدوجا فوق **محرر التكوين**.



9. في القائمة المنسدلة "قسم"، أختر **system.webServer/security/requestFiltering**. في القائمة المنسدلة allowDoubleEscape، أختر **True**. في اللوحة اليمنى، انقر فوق **تطبيق**.

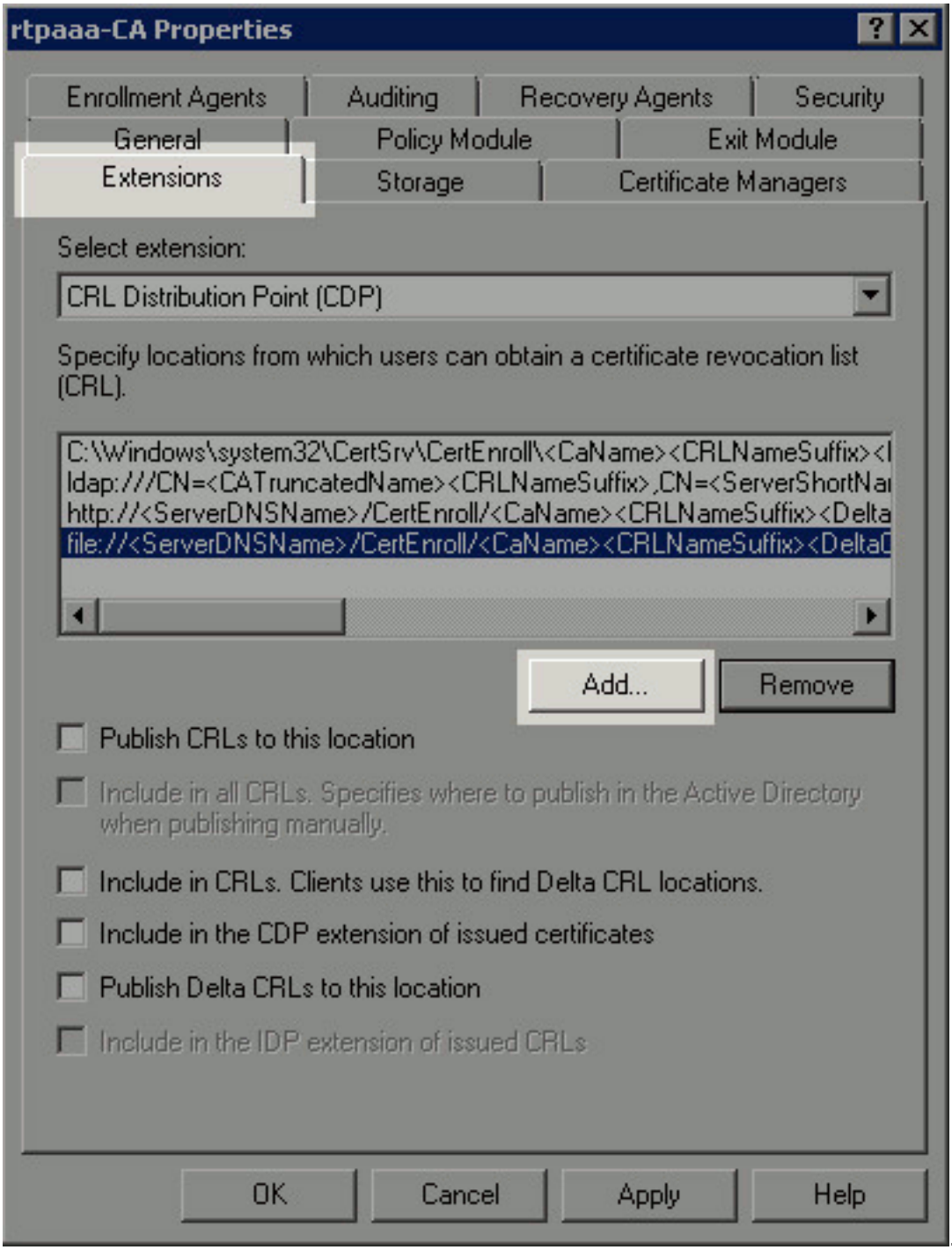


يجب الوصول إلى المجلد الآن عبر IIS.

الباب 3. تكوين خادم Microsoft CA لنشر ملفات CRL إلى نقطة التوزيع

الآن بعد تكوين مجلد جديد لتضمين ملفات CRL، وبعد أن تم عرض المجلد في IIS، قم بتكوين خادم Microsoft CA لنشر ملفات CRL إلى الموقع الجديد.

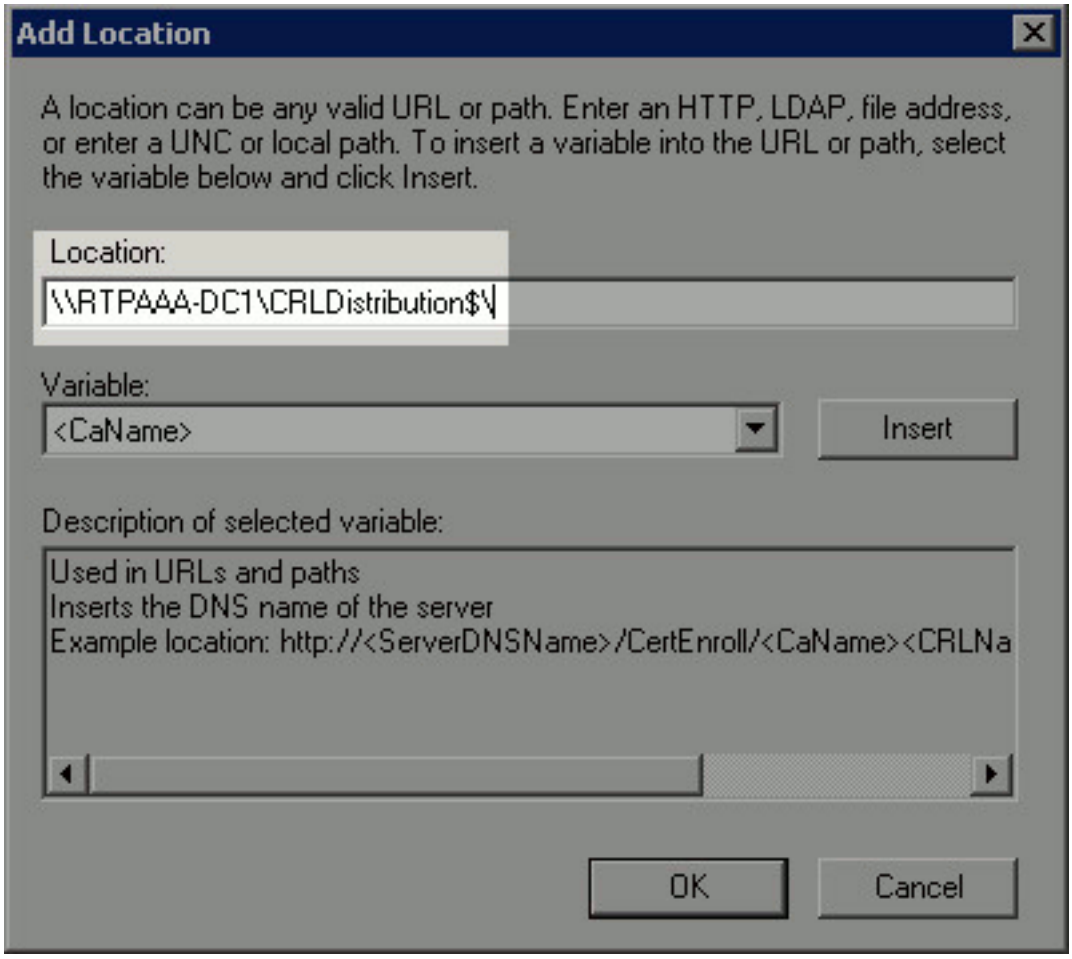
1. في شريط مهام خادم CA، انقر فوق **بدء**. أختر **أدوات إدارية > المرجع المصدق**.
2. في اللوح الأيسر، انقر بزر الماوس الأيمن على اسم المرجع المصدق. أختر **خصائص** ثم انقر على علامة التبويب **الملحقات**. لإضافة نقطة توزيع CRL جديدة، انقر فوق



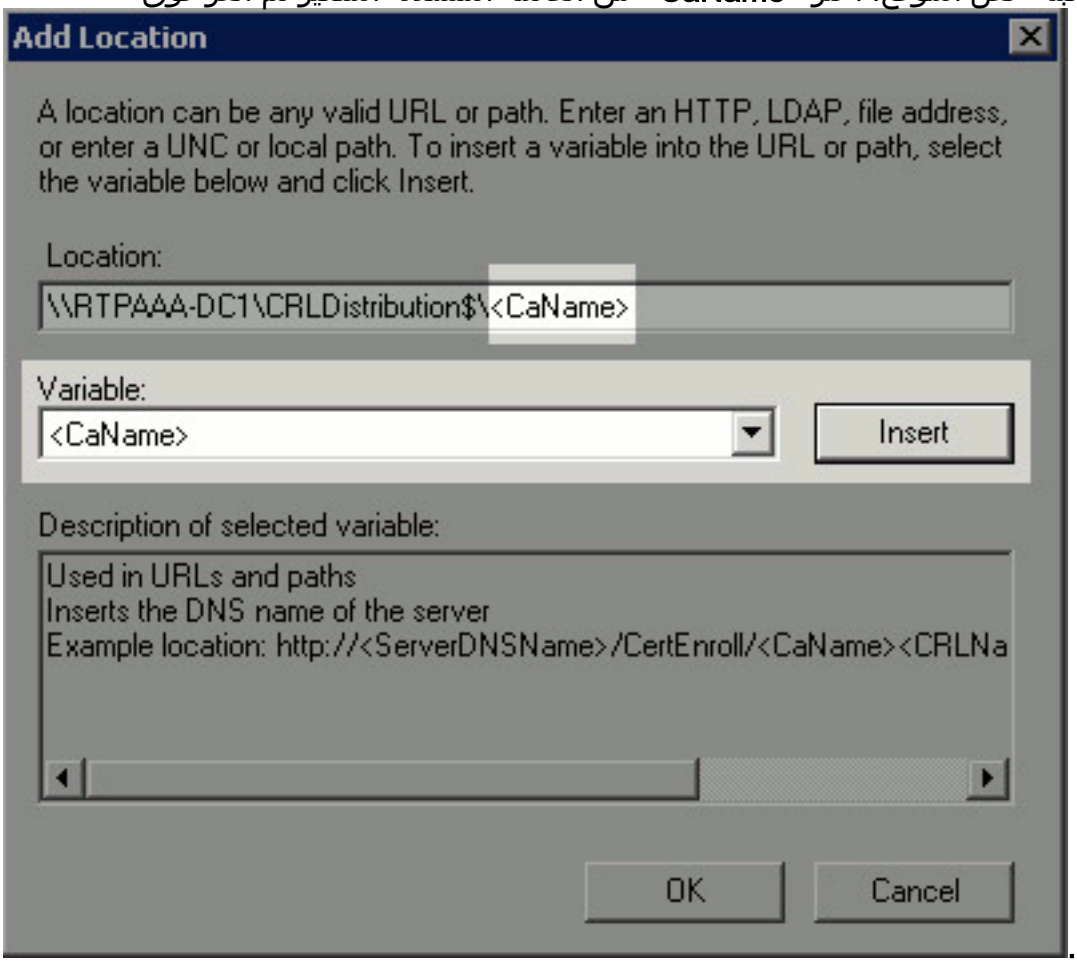
إضافة.

3. في حقل الموقع، أدخل المسار إلى المجلد الذي تم إنشاؤه ومشاركته في القسم 1. في المثالفي القسم 1، يكون المسار:

```
\\$RTPAAA-DC1\CRLDistribution\\
```

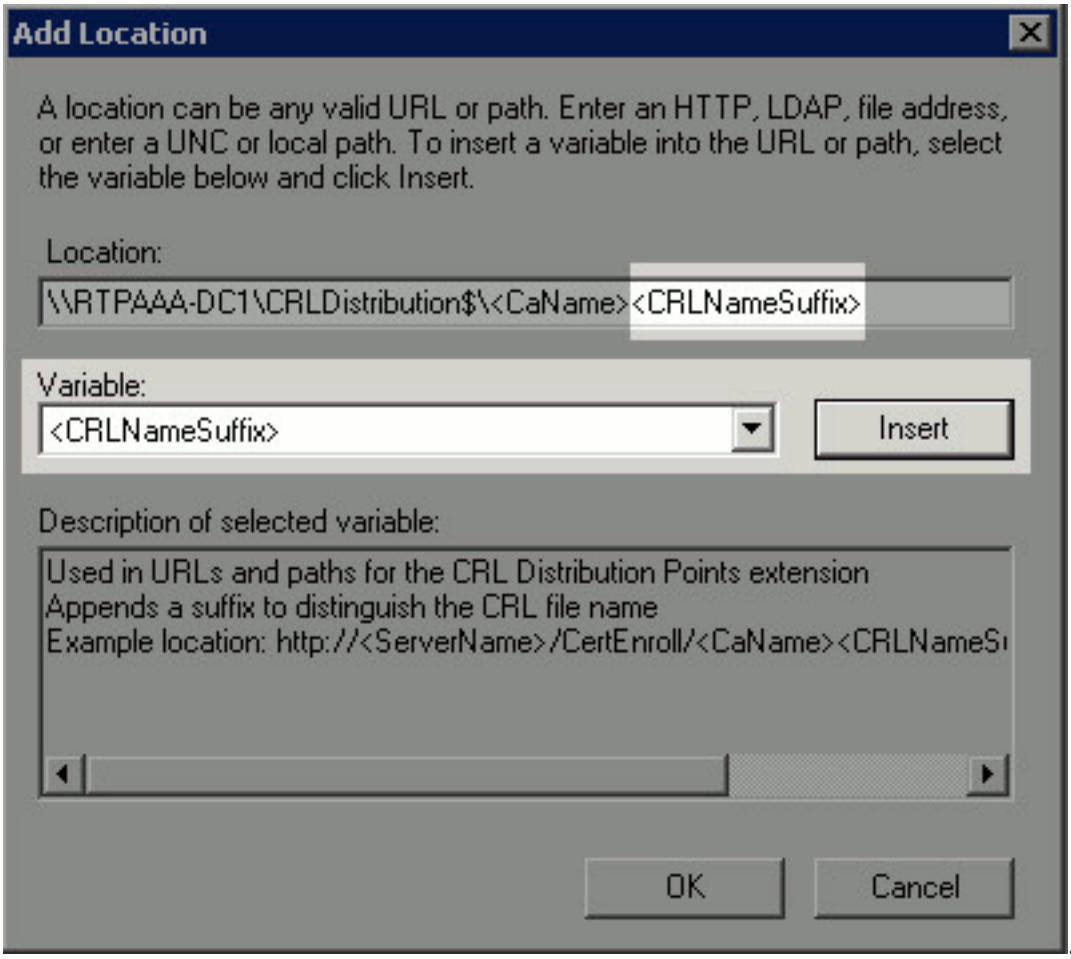


4. مع تعبئة حقل الموقع، أختر **<CaName>** من القائمة المنسدلة المتغير ثم انقر فوق



إدراج.

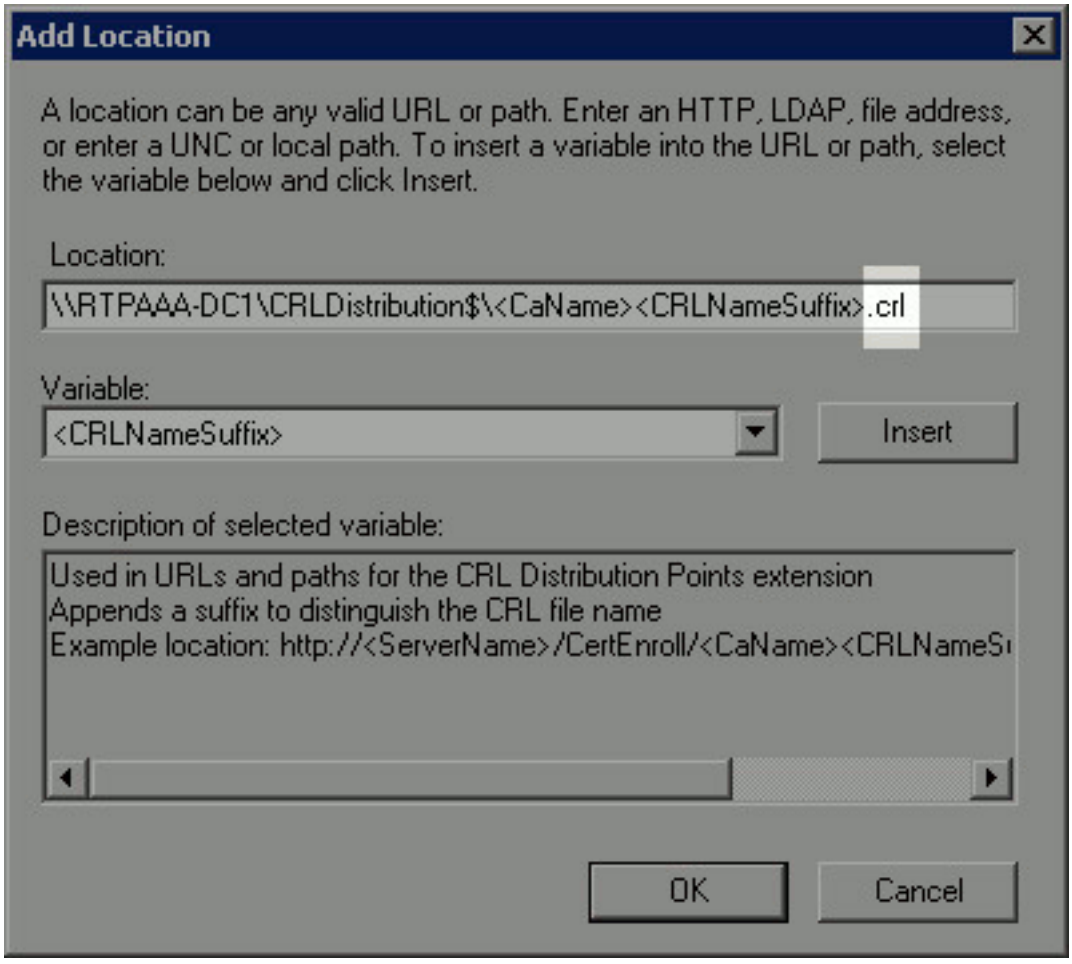
5. من القائمة المنسدلة "متغير"، أختر **<CRLNameSuffix>**ثم انقر فوق



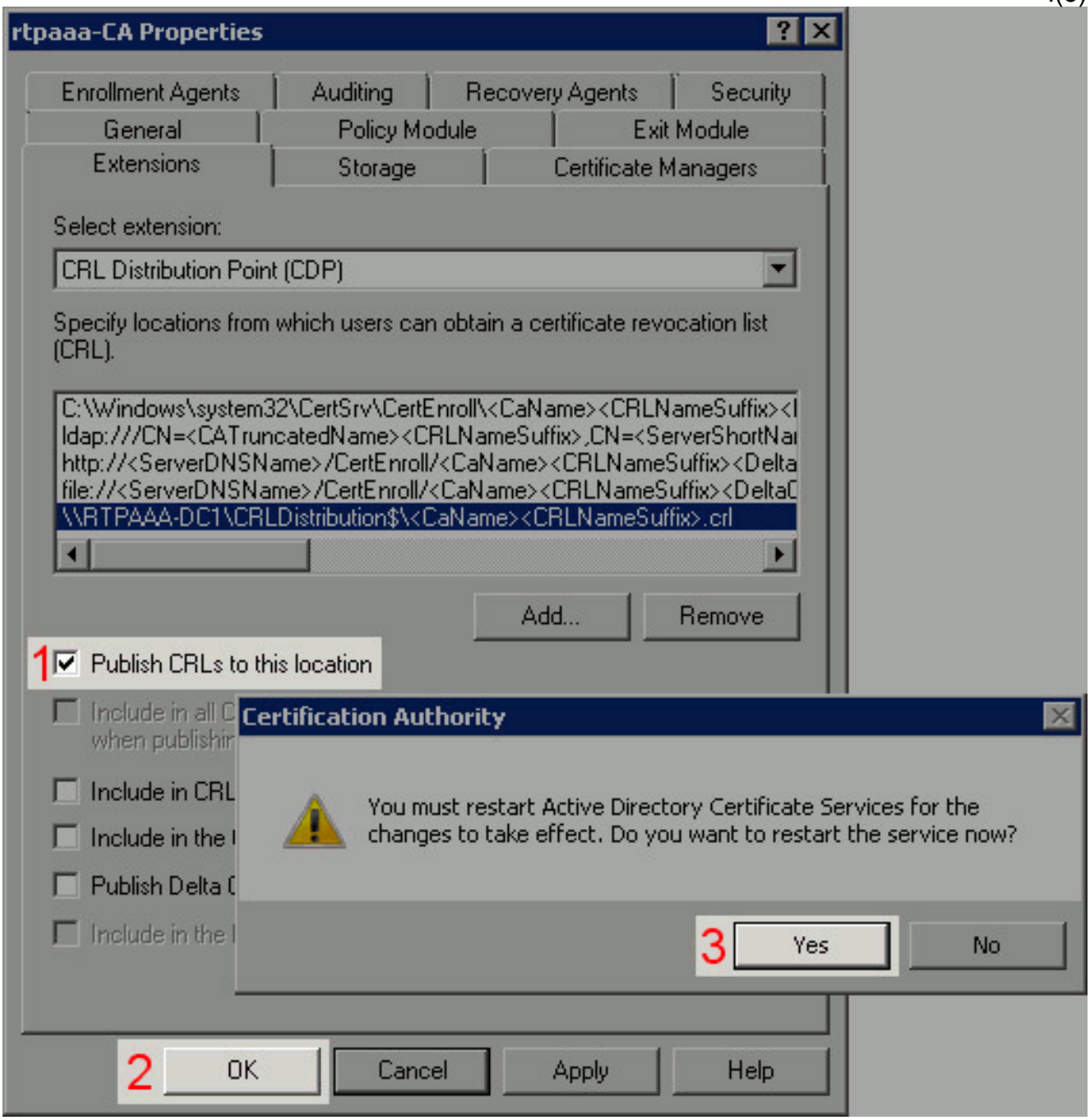
إدراج.

6. في حقل الموقع، قم بإلحاق .crl إلى نهاية المسار. في هذا المثال، الموقع:

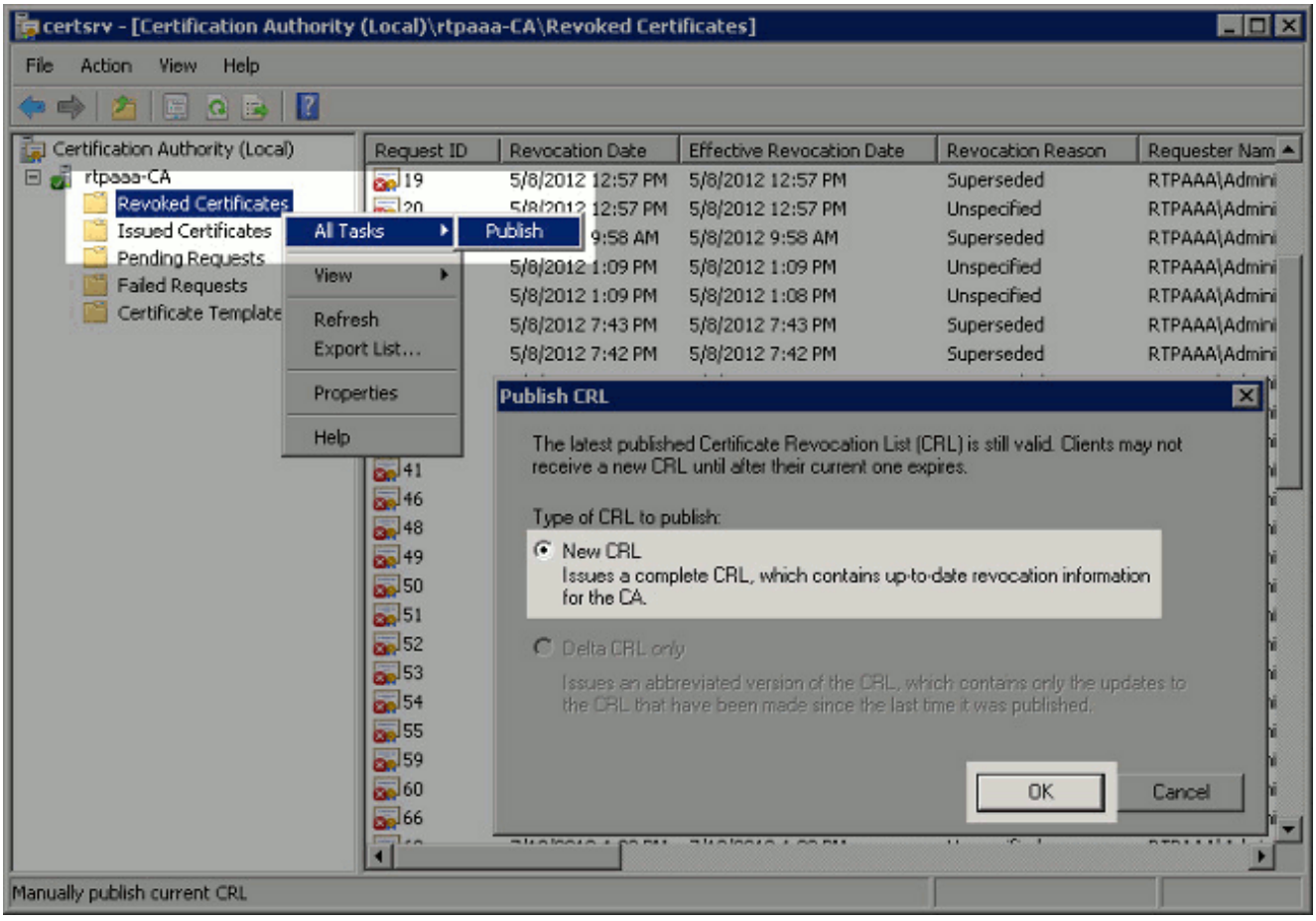
```
RTPAAA-DC1\CRLDistribution$\<CaName><CRLNameSuffix>.crl\\
```



7. انقر فوق **موافق** للعودة إلى علامة التبويب الملحقات. حدد خانة الاختيار **نشر قوائم التحكم في الوصول (CRL) لهذا الموقع** (1) ثم انقر فوق **موافق** (2) لإغلاق نافذة "الخصائص". تظهر مطالبة للحصول على إذن لإعادة تشغيل خدمات شهادات Active Directory. طقطقة **نعم** (3).



8. في اللوحة اليسرى، انقر بزر الماوس الأيمن على **الشهادات الملغاة**. أختر **كل المهام > نشر**. تأكد من تحديد CRL جديد ثم انقر فوق **موافق**.

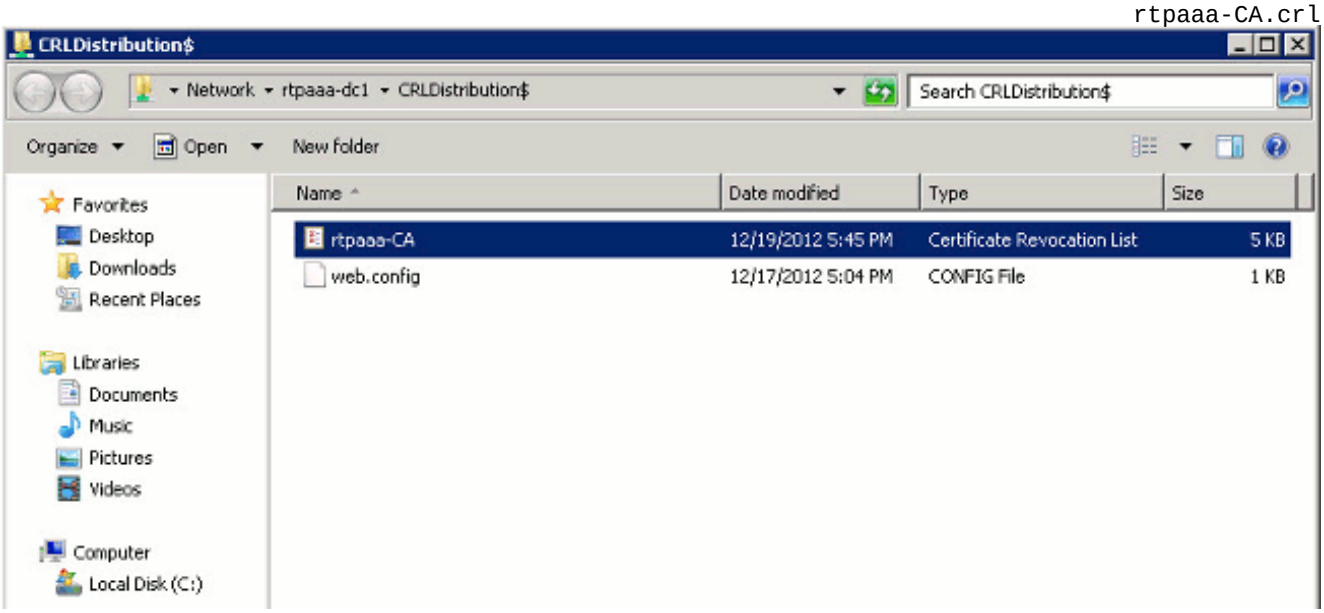


يجب أن يقوم خادم Microsoft CA بإنشاء ملف .crl جديد في المجلد الذي تم إنشاؤه في القسم 1. إذا تم إنشاء ملف CRL الجديد بنجاح، فلن يكون هناك مربع حوار بعد النقر فوق "موافق". إذا تم إرجاع خطأ بخصوص مجلد نقطة التوزيع الجديدة، فقم بتكرار كل خطوة في هذا القسم بعناية.

الباب 4. التحقق من وجود ملف CRL وإمكانية الوصول إليه عبر IIS

تحقق من وجود ملفات CRL الجديدة ومن إمكانية الوصول إليها عبر IIS من محطة عمل أخرى قبل بدء هذا القسم.

1. على خادم IIS، افتح المجلد الذي تم إنشاؤه في القسم 1. يجب أن يكون هناك ملف .crl واحد موجود مع النموذج <CANAME>.crl حيث <CANAME> هو اسم خادم CA. في هذا المثال، اسم الملف هو:
`rtpaaa-CA.crl`

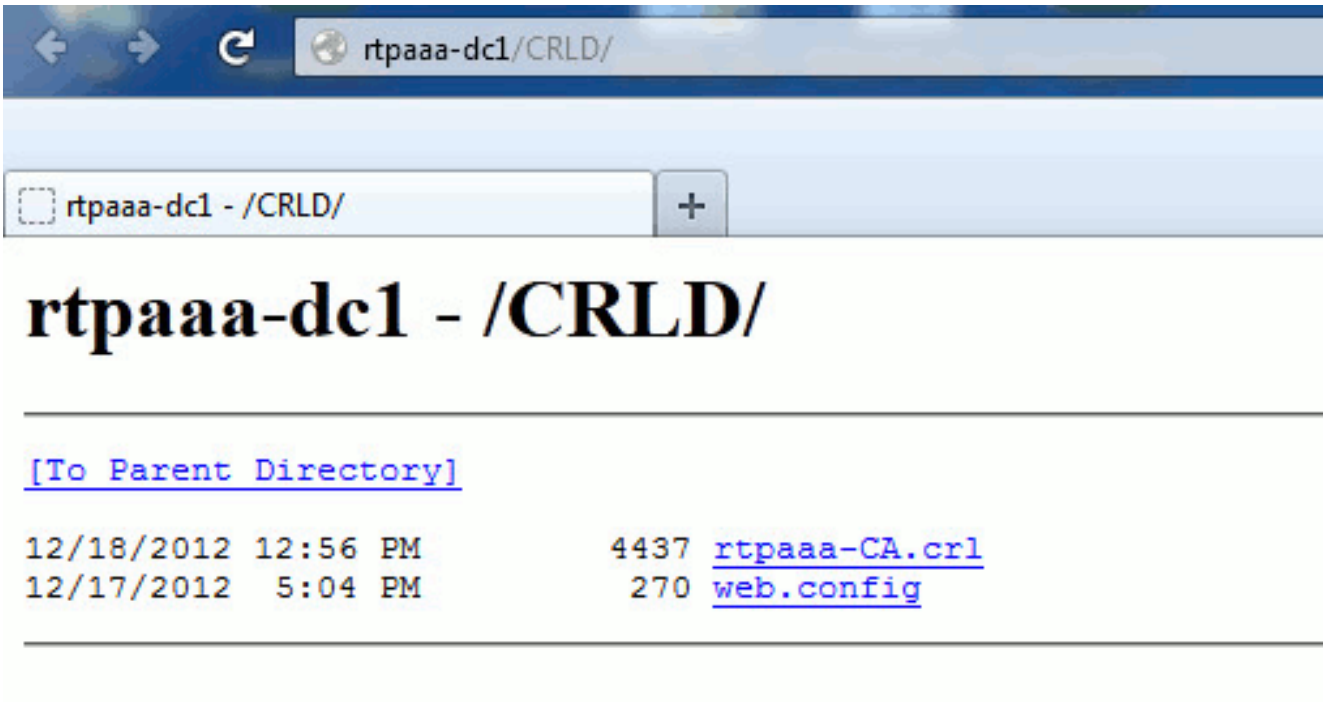


2. من محطة عمل على الشبكة (بشكل مثالي على نفس الشبكة مثل عقدة إدارة ISE الأساسية)، افتح مستعرض ويب واستعرض إلى http://<SERVER>/<CRLSITE> حيث يكون <SERVER> هو اسم خادم خادم

خادم IIS الذي تم تكوينه في القسم 2 ويكون <CRLSITE> هو اسم الموقع الذي تم إختياره لنقطة التوزيع في القسم 2. في هذا المثال، عنوان URL:

```
http://RTPAAA-DC1/CRLD
```

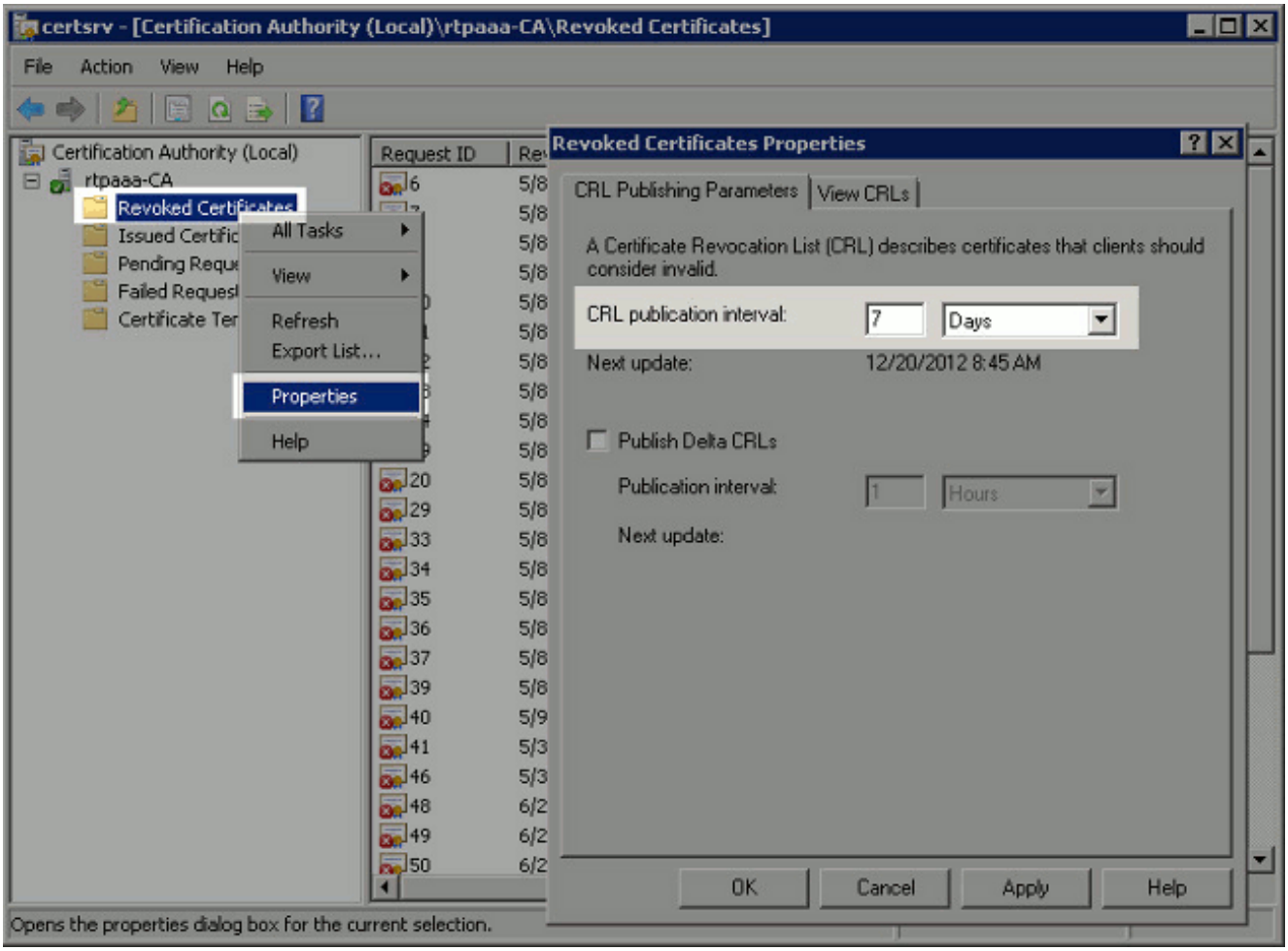
يعرض فهرس الدليل، والذي يتضمن الملف الملاحظ في الخطوة 1.



الباب 5. تكوين ISE لاستخدام نقطة توزيع CRL الجديدة

قبل تكوين ISE لاسترداد CRL، حدد الفاصل الزمني لنشر CRL. تتجاوز إستراتيجية تحديد هذا الفاصل الزمني نطاق هذا المستند. القيم المحتملة (في Microsoft CA) هي من ساعة واحدة إلى 411 سنة، شاملة. القيمة الافتراضية هي 1 أسبوع. بمجرد تحديد الفاصل الزمني المناسب لبيئة عملك، قم بتعيين الفاصل الزمني باستخدام التعليمات التالية:

1. في شريط مهام خادم CA، انقر فوق **بدء**. أختر **أدوات إدارية > المرجع المصدق**.
2. في الجزء الأيسر، قم بتوسيع المرجع المصدق. انقر بزر الماوس الأيمن على مجلد **الشهادات الملغاة** واختر **خصائص**.
3. في حقول الفاصل الزمني لنشر CRL، أدخل الرقم المطلوب واختر الفترة الزمنية. انقر فوق **موافق**" لإغلاق الإطار وتطبيق التغيير. في هذا المثال، تم تكوين فاصل زمني للنشر لمدة 7 أيام.



يجب الآن تأكيد العديد من قيم السجل، التي ستساعد في تحديد إعدادات إسترداد CRL في ISE.

4. أدخل الأمر **certutil -getreg ca\Clock*** لتأكيد قيمة ClockSkew. القيمة الافتراضية هي 10 دقائق.مثال الإخراج:

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

5. أدخل الأمر **certutil -getreg ca\CRLov*** للتحقق مما إذا كان قد تم تعيين CRLOverlapPeriod يدويا. بشكل افتراضي تكون قيمة CRLOverlapUnit هي 0، وهو ما يشير إلى أنه لم يتم تعيين أي قيمة يدوية. إذا كانت القيمة قيمة غير 0، فقم بتسجيل القيمة والوحدات.مثال الإخراج:

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

6. أدخل الأمر **certutil -getreg ca\CRLpe*** للتحقق من CRLPeriod، الذي تم تعيينه في الخطوة 3.مثال الإخراج:

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

7. قم بحساب فترة سماح CRL كما يلي:إذا تم تعيين CRLOverlapPeriod في الخطوة 5: التداخل = CRLOverlapPeriod، بالدقائق؛غير ذلك: التداخل = (CrlpEriod / 10)، بالدقائقإذا كان تداخل > 720 ثم تداخل = 720إذا كان التداخل < (1. 5 * ClockSkewMinutes)، فإن التداخل = (1. 5 * ClockSkewMinutes)إذا تداخل > CrlpEriod، في دقائق ثم تداخل = CrlpEriod في دقائقفترة السماح = 720 دقيقة + 10 دقائق = 730 دقيقةمثال:

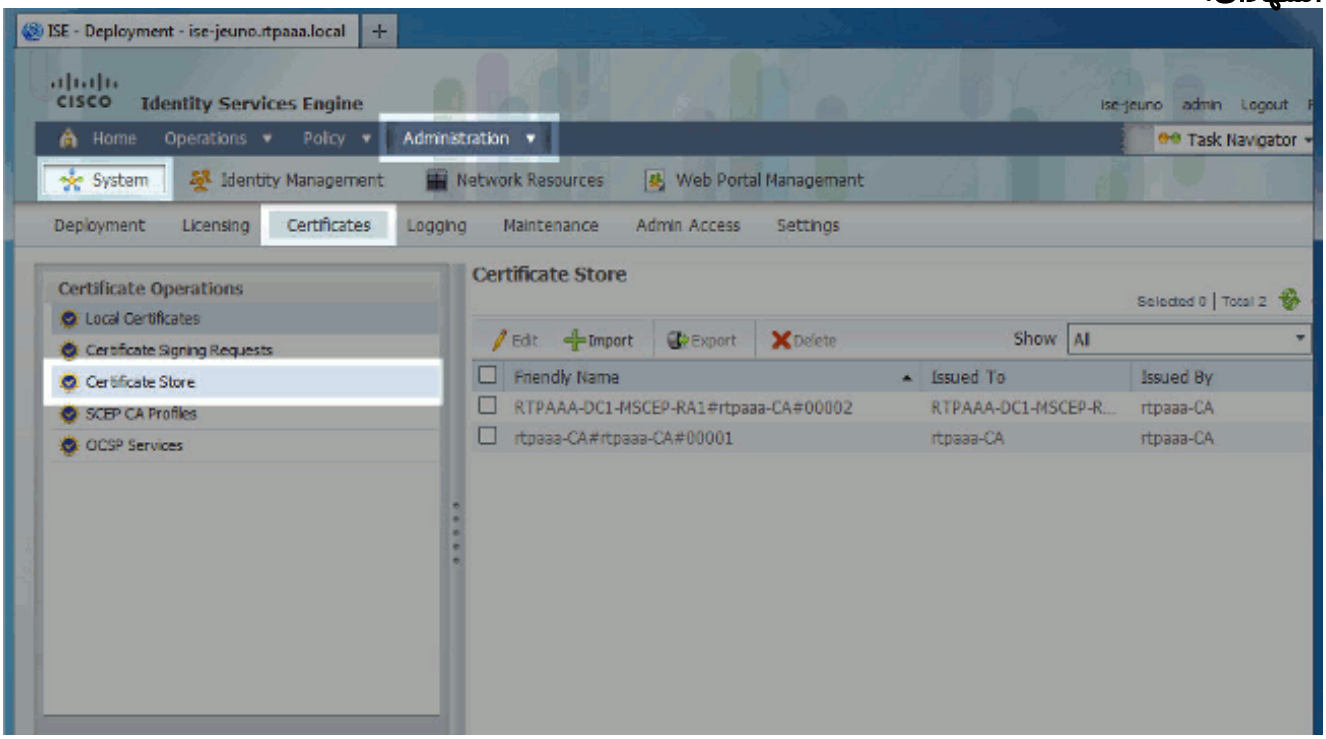
```
As stated above, CRLPeriod was set to 7 days, or 10248 minutes and
```

```
.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
```

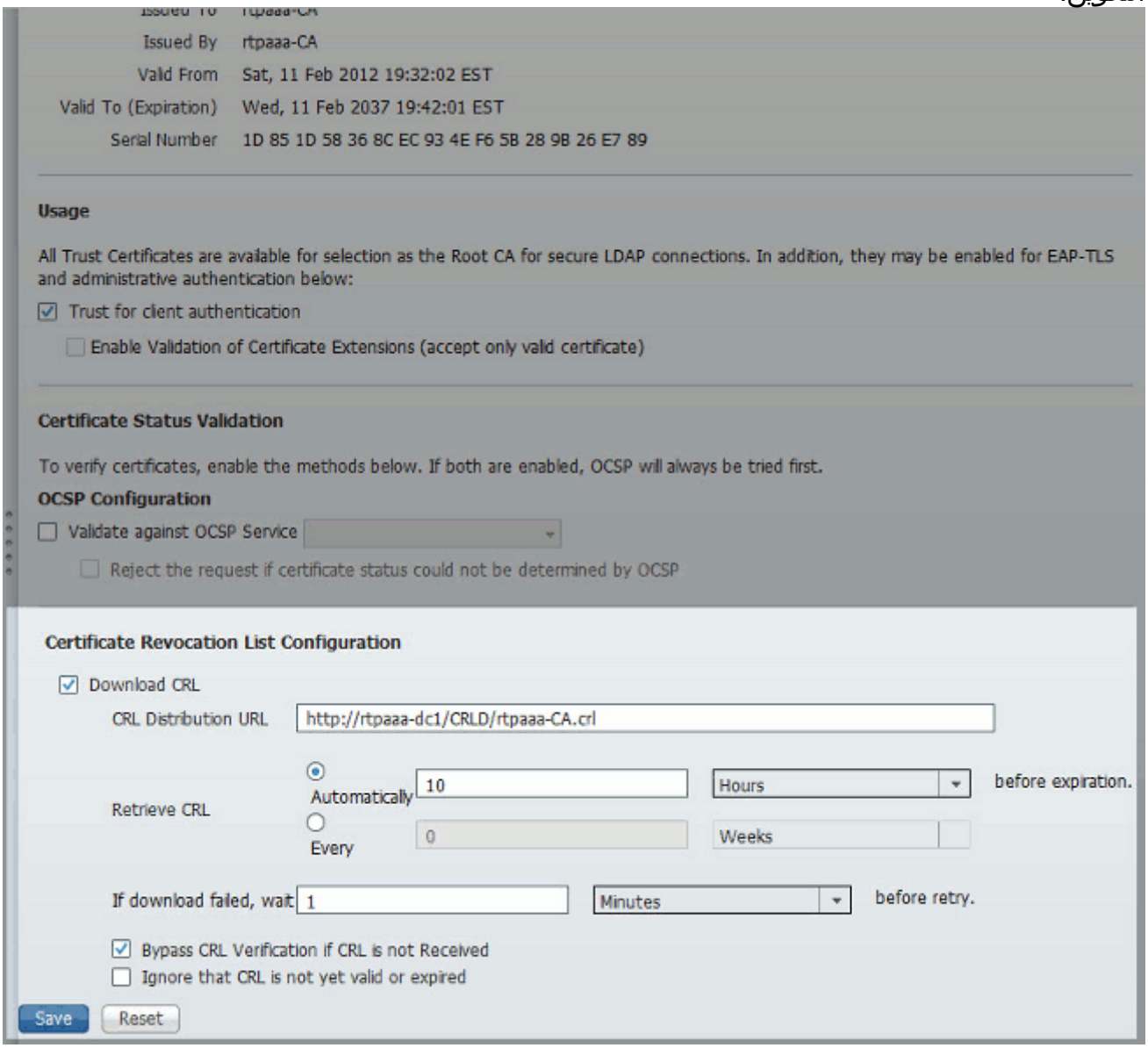
فترة السماح المحسوبة هي مقدار الوقت بين وقت نشر CRL التالي وتاريخ انتهاء صلاحية CRL الحالي. يلزم تكوين ISE لاسترداد قوائم التحكم في الوصول (CRLs) وفقا لذلك.

8. قم بتسجيل الدخول إلى عقدة الإدارة الأساسية واختر **إدارة > نظام > شهادات**. في الجزء الأيسر، حدد **مخزن الشهادات**.



9. حدد خانة الاختيار "مخزن الشهادات" المجاورة لشهادة CA التي تنوي تكوين قوائم التحكم في الوصول الخاصة بها. انقر فوق **تحرير**.
10. بالقرب من أسفل النافذة، حدد خانة الاختيار **تنزيل CRL** .
11. في حقل عنوان URL الخاص بتوزيع CRL، أدخل المسار إلى نقطة توزيع CRL، والتي تتضمن ملف .crl، الذي تم إنشاؤه في القسم 2. في هذا المثال، عنوان URL:
```
http://RTPAAA-DC1/CRLD/rtpaaa-ca.crl
```
12. يمكن تكوين ISE لاسترداد CRL على فترات زمنية منتظمة أو استنادا إلى انتهاء الصلاحية (الذي هو أيضا، بصفة عامة، فاصل زمني منتظم). عندما يكون الفاصل الزمني لنشر CRL ثابتا، يتم الحصول على تحديثات CRL أكثر ملاءمة عند إستخدام الخيار الأخير. انقر زر انتقاء **آلي**.
13. قم بتعيين قيمة الاسترداد إلى قيمة أقل من فترة السماح المحسوبة في الخطوة 7. إذا كانت مجموعة القيمة أطول من فترة السماح، فإن ISE يتحقق من نقطة توزيع CRL قبل أن يقوم CA بنشر CRL التالية. في هذا المثال، يتم حساب فترة السماح على أنها 730 دقيقة، أو 12 ساعة و 10 دقائق. سيتم إستخدام قيمة 10 ساعات للاسترداد.
14. تعيين الفاصل الزمني لإعادة المحاولة على أنه مناسب لبيئتك. إذا تعذر على ISE إسترداد قائمة التحكم في الوصول (CRL) في الفترة التي تم تكوينها في الخطوة السابقة، فسيعيد المحاولة في هذه الفترة الأقصر.
15. حدد خانة الاختيار **تجاوز التحقق من CRL إذا لم يتم إستلام CRL** للسماح بالمصادقة المستندة إلى الشهادة بالمتابعة بشكل طبيعي (وبدون فحص CRL) إذا لم يتمكن ISE من إسترداد CRL لهذا المرجع المصدق في محاولة التنزيل الأخيرة. في حالة عدم تحديد خانة الاختيار هذه، ستفشل كافة المصادقة المستندة إلى الشهادة مع الشهادات التي تم إصدارها من قبل المرجع المصدق هذا في حالة تعذر إسترداد قائمة التحكم في الوصول (CRL).

16. حدد خانة الاختيار **تجاهل أن CRL غير صالح أو منتهية الصلاحية** للسماح ل ISE باستخدام ملفات CRL منتهية الصلاحية (أو غير صالحة بعد) كما لو كانت صحيحة. إذا لم يتم تحديد خانة الاختيار هذه، فإن ISE يعتبر قائمة التحكم في الوصول (CRL) غير صالحة قبل تاريخ السريان الخاص بهم وبعد أوقات التحديث التالية الخاصة بهم. انقر فوق **حفظ** لإكمال التكوين.



التحقق من الصحة

لا يوجد حاليًا إجراء للتحقق من صحة هذا التكوين.

استكشاف الأخطاء وإصلاحها

لا تتوفر حاليًا معلومات محددة لاستكشاف الأخطاء وإصلاحها لهذا التكوين.

معلومات ذات صلة

- الدعم التقني والمستندات - Cisco Systems

حول هذه الترجمة
ترجمت Cisco هذا المستند باستخدام مجموعة من التقنيات الآلية والبشرية لتقديم محتوى دعم للمستخدمين في جميع أنحاء العالم بلغتهم الخاصة. يُرجى ملاحظة أن أفضل ترجمة آلية لن تكون دقيقة كما هو الحال مع الترجمة الاحترافية التي يقدمها مترجم محترف. تخلي Cisco Systems مسئوليتها عن دقة هذه الترجمات وتُوصي بالرجوع دائمًا إلى المستند الإنجليزي الأصلي (الرابط متوفر).