Configurer Microsoft CA Server pour publier les listes de révocation de certificats pour ISE

Contenu

[Introduction](#)
[Prérequis](#)
[Conditions requises](#)
[Components Used](#)
[Configuration](#)
[Créer et configurer un dossier sur l'autorité de certification pour héberger les fichiers CRL](#)
[Créer un site dans IIS pour exposer le nouveau point de distribution CRL](#)
[Configurer Microsoft CA Server pour publier les fichiers CRL sur le point de distribution](#)
[Vérifier que le fichier CRL existe et est accessible via IIS](#)
[Configurer ISE pour utiliser le nouveau point de distribution CRL](#)

Introduction

Ce document décrit la configuration d'un serveur d'autorité de certification Microsoft qui exécute les services IIS (Internet Information Services) pour publier les mises à jour de la liste de révocation de certificats (CRL). Il explique également comment configurer Cisco Identity Services Engine (ISE) (versions 3.0 et ultérieures) pour récupérer les mises à jour à utiliser dans la validation de certificat. ISE peut être configuré pour récupérer des LCR pour les différents certificats racine de l'autorité de certification qu'il utilise dans la validation des certificats.

Prérequis

Conditions requises

Aucune spécification déterminée n'est requise pour ce document.

Components Used

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

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

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l’incidence possible des commandes.

Configuration

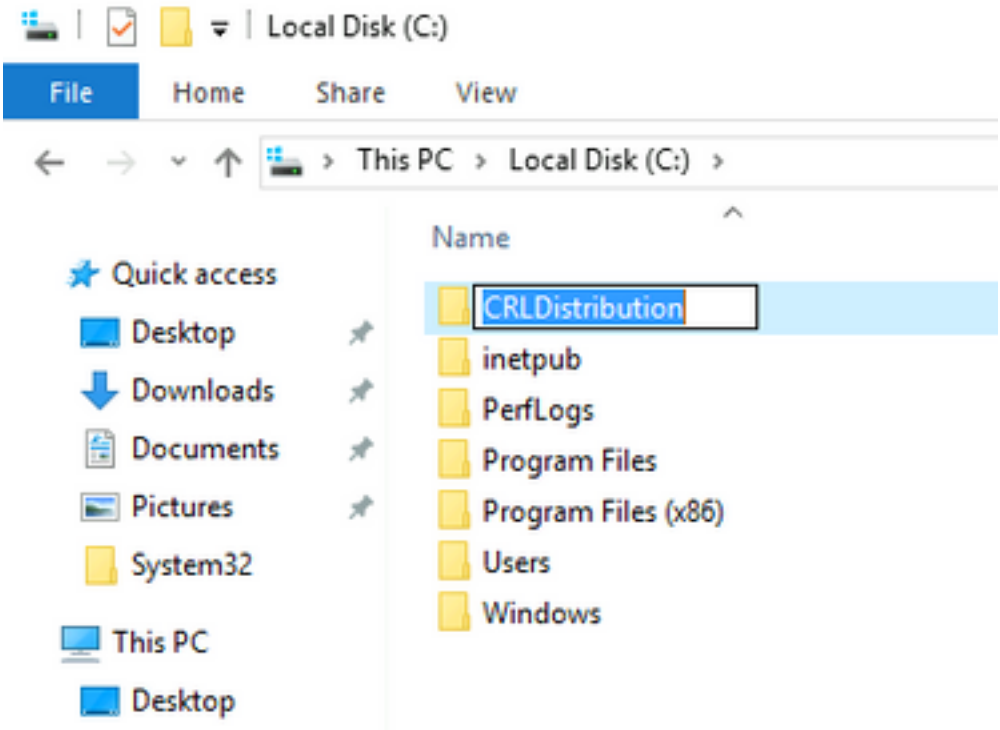
Cette section vous fournit des informations pour configurer les fonctionnalités décrites dans ce document.

Créer et configurer un dossier sur l'autorité de certification pour héberger les fichiers CRL

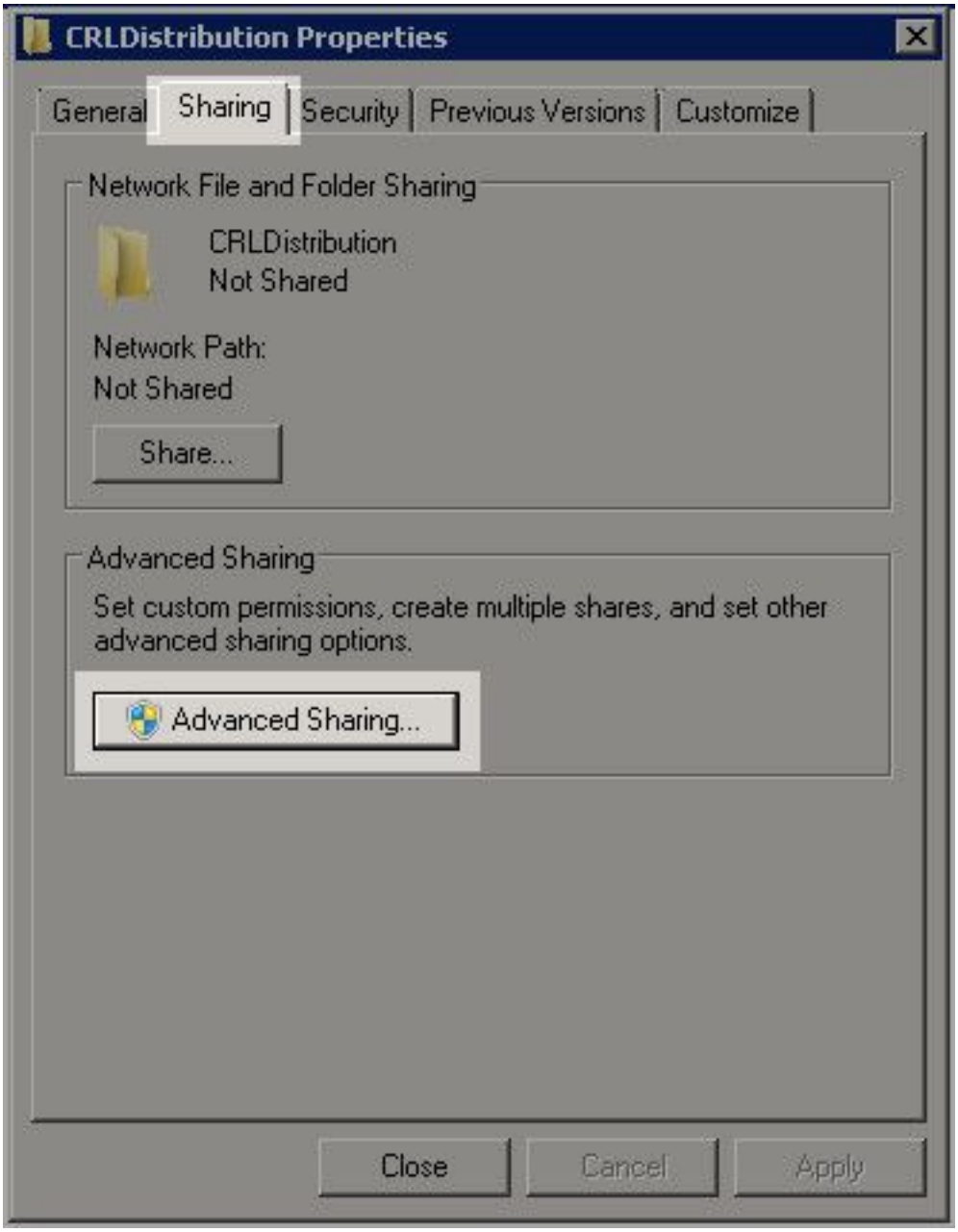
La première tâche consiste à configurer un emplacement sur le serveur AC pour stocker les fichiers CRL. Par défaut, le serveur Microsoft CA publie les fichiers sur **C:\Windows\system32\CertSrv\CertEnroll**

Plutôt que d'utiliser ce dossier système, créez un nouveau dossier pour les fichiers.

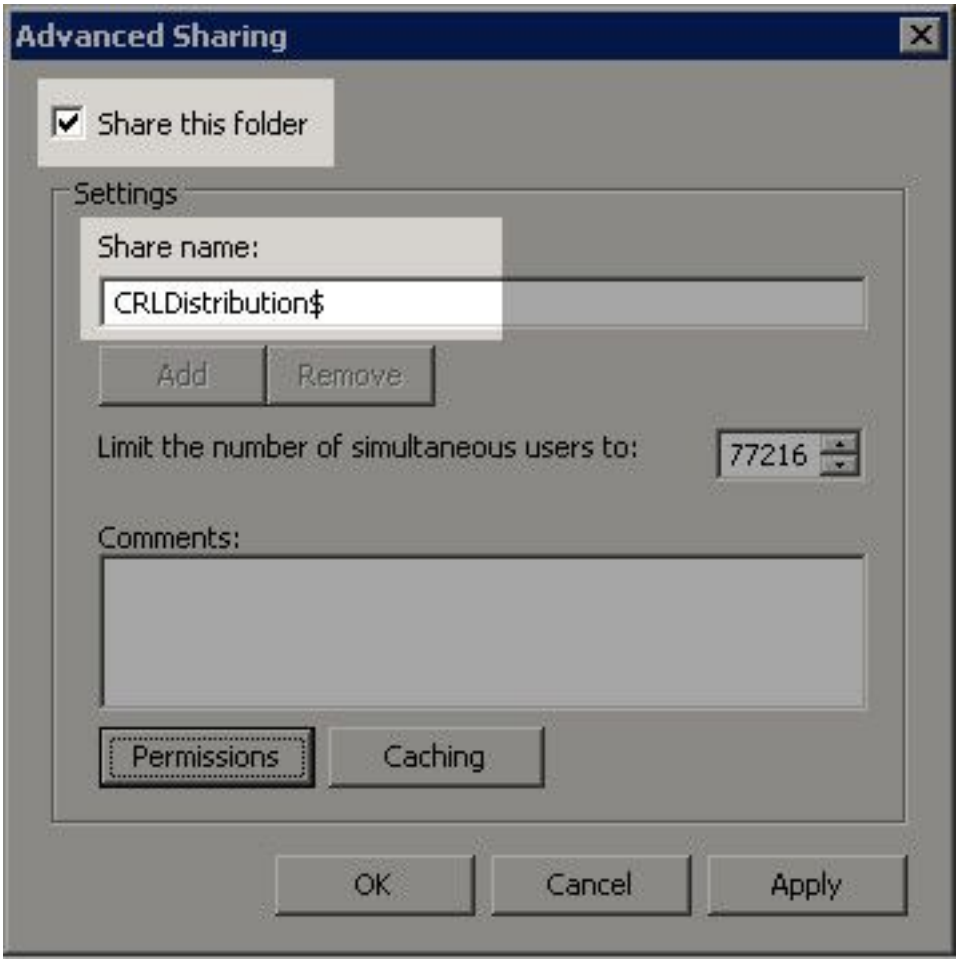
1. Sur le serveur IIS, choisissez un emplacement sur le système de fichiers et créez un nouveau dossier. Dans cet exemple, le dossier **C:\CRLDistribution** est créé.



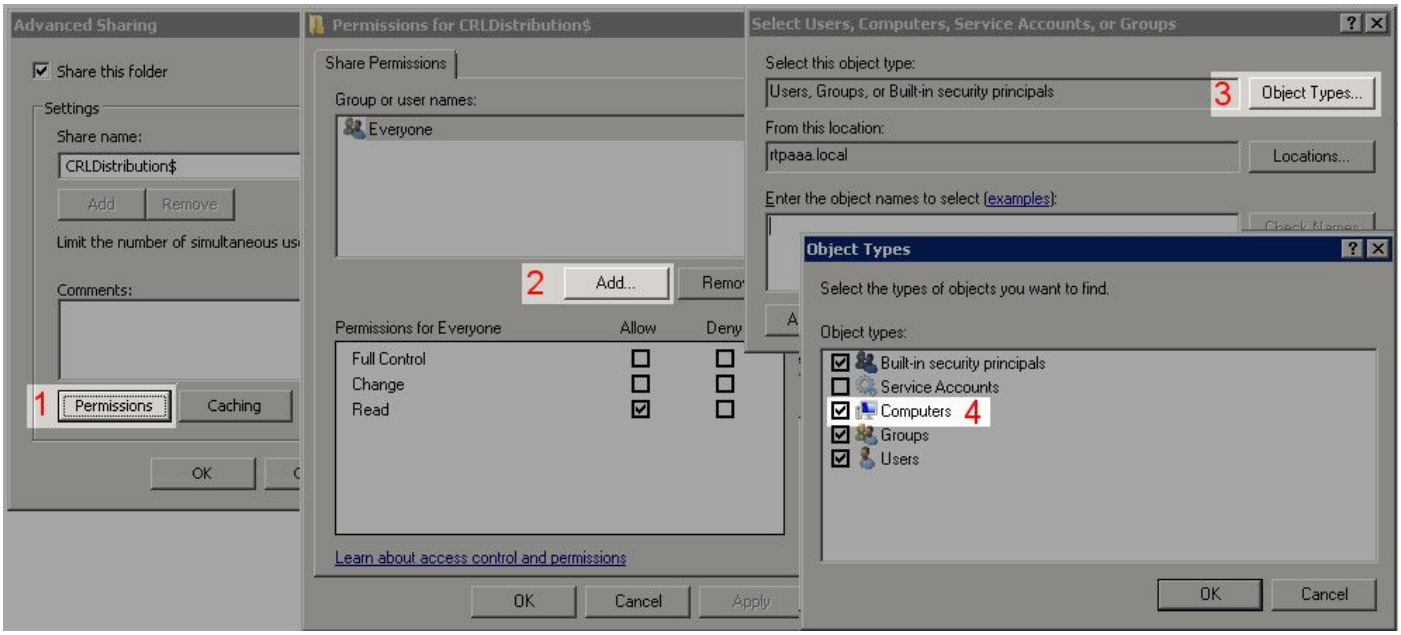
2. Pour que l'autorité de certification puisse écrire les fichiers CRL dans le nouveau dossier, le partage doit être activé. Cliquez avec le bouton droit sur le nouveau dossier, choisissez **Propriétés**, cliquez sur l'onglet **Partage**, puis cliquez sur **Partage avancé**.



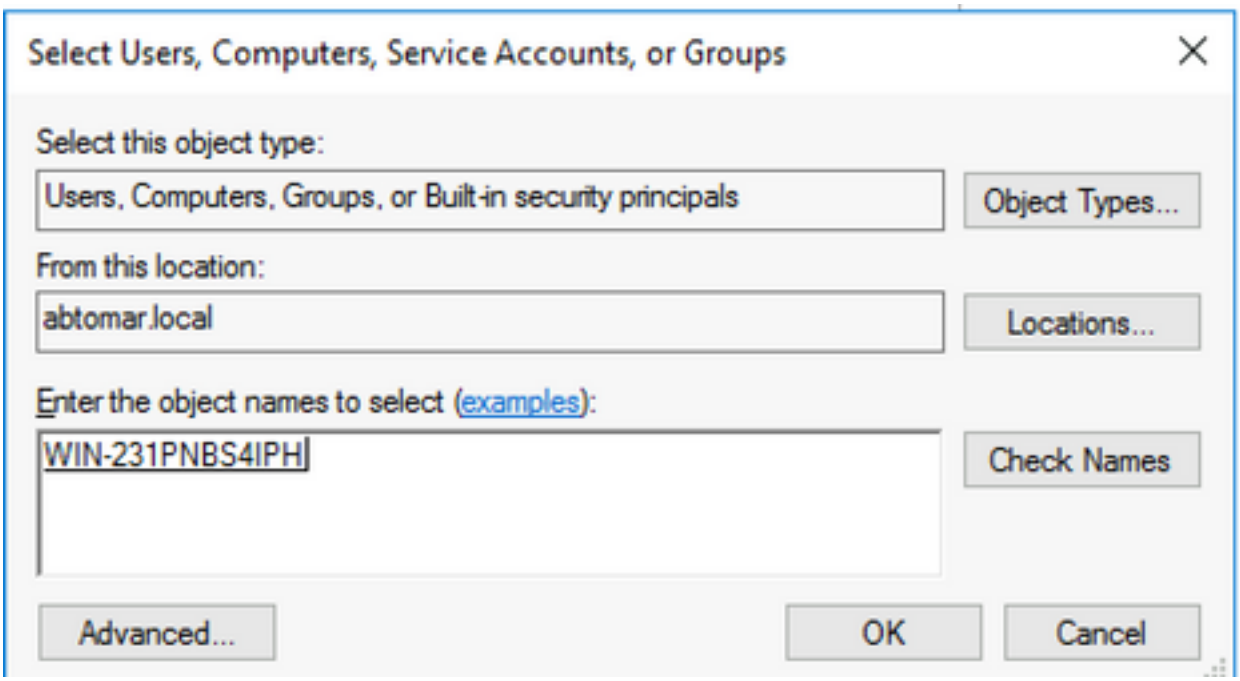
3. Pour partager le dossier, cochez la case **Partager ce dossier**, puis ajoutez un signe dollar ($) à la fin du nom du partage dans le champ Nom du partage pour masquer le partage.



4. Cliquez sur **Autorisations** (1), sur **Ajouter** (2), sur **Types d'objets** (3) et activez la case à cocher **Ordinateurs** (4).

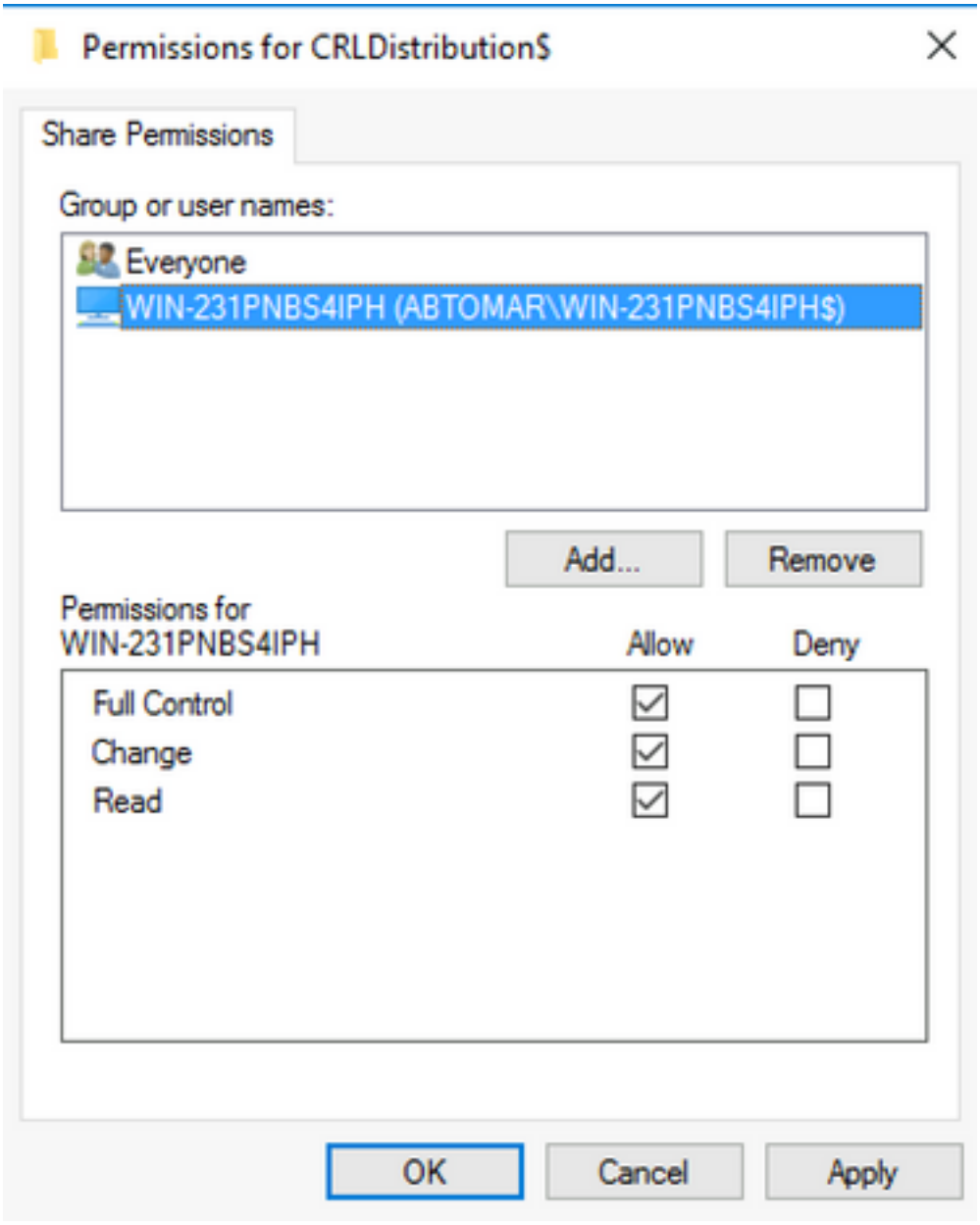


5. Pour revenir à la fenêtre Sélectionner des utilisateurs, des ordinateurs, des comptes de service ou des groupes, cliquez sur **OK**. Dans le champ Entrez les noms d'objet à sélectionner, entrez le nom d'ordinateur du serveur AC dans cet exemple : WIN0231PNBS4IPH et cliquez sur **Vérifier les noms**. Si le nom saisi est valide, il est actualisé et apparaît souligné. Click OK.



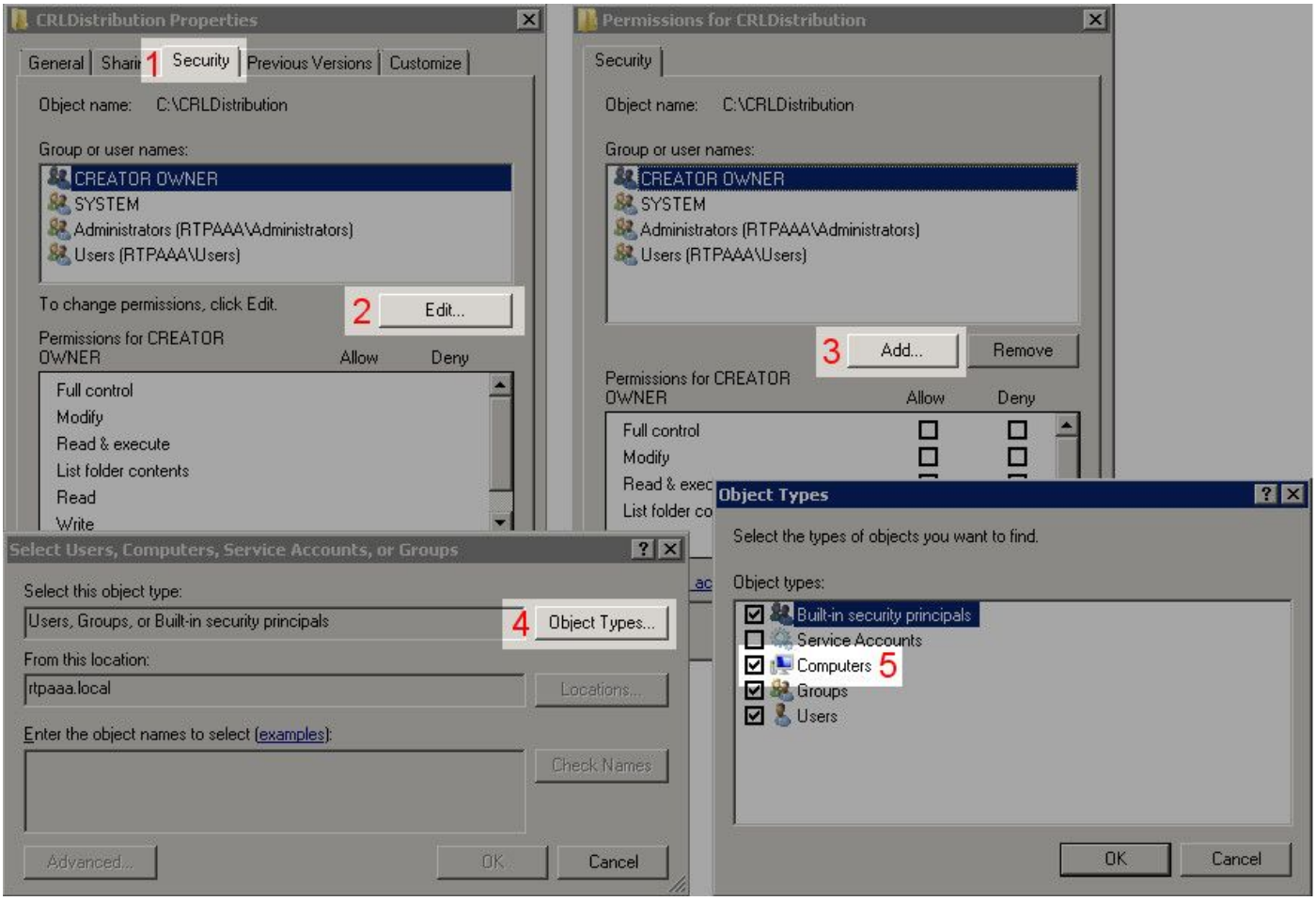
6. Dans le champ Group or user names, sélectionnez l'ordinateur AC. Cochez **Allow** for Full Control pour accorder un accès complet à l'AC.

Click OK. Cliquez de nouveau sur **OK** pour fermer la fenêtre Partage avancé et revenir à la fenêtre Propriétés.

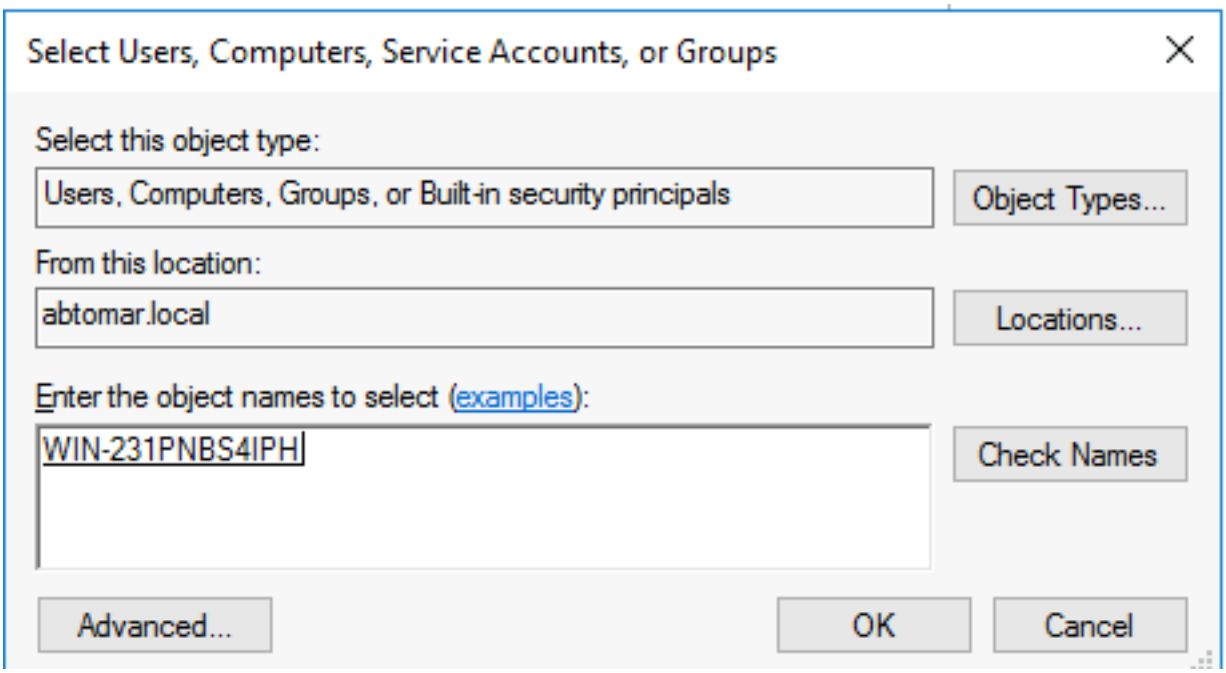


---

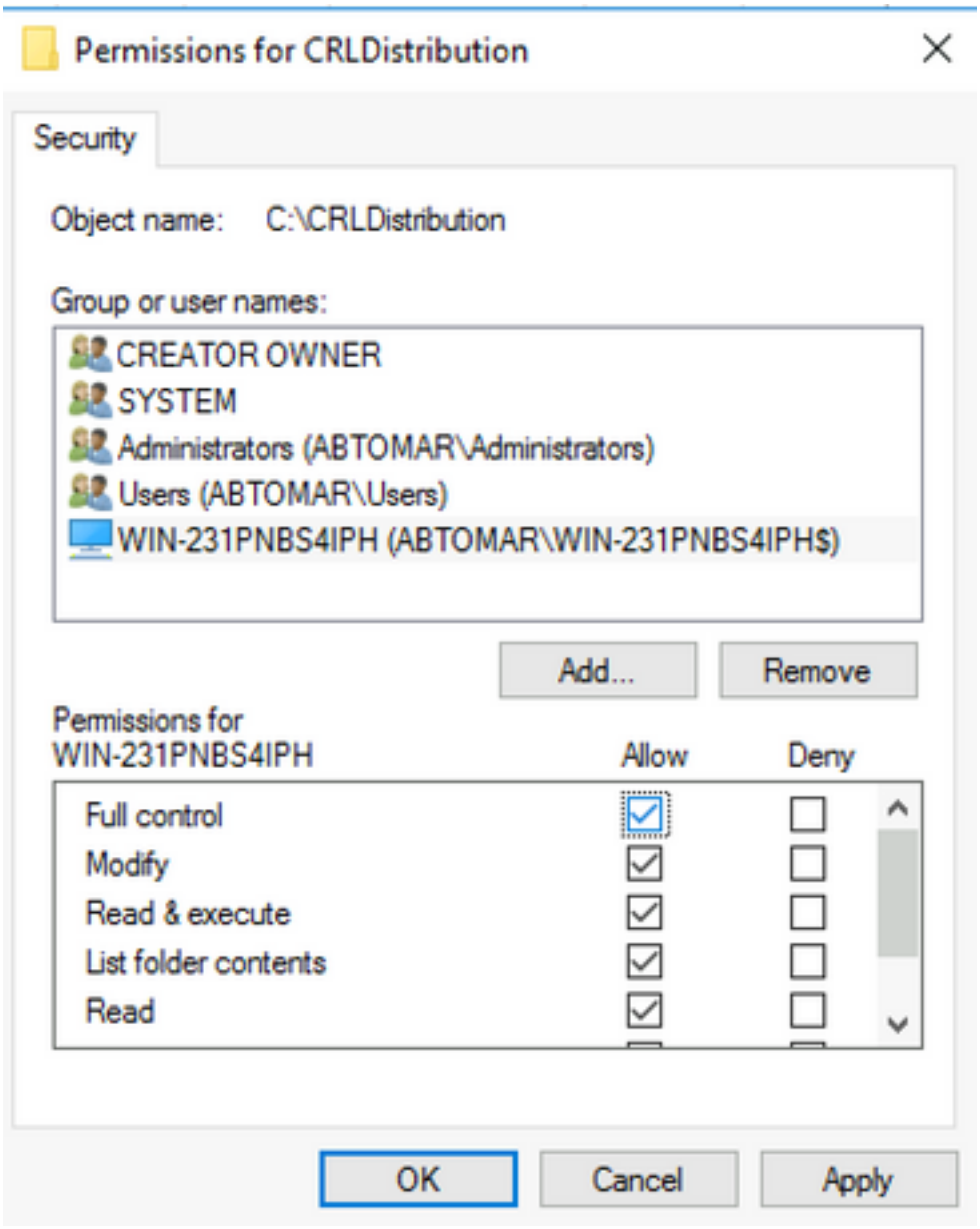
7. Afin de permettre à l'autorité de certification d'écrire les fichiers CRL dans le nouveau dossier, configurez les autorisations de sécurité appropriées. Cliquez sur l'onglet Sécurité (1), cliquez sur **Modifier** (2), sur **Ajouter** (3), sur **Types d'objets** (4) et activez la case à cocher **Ordinateurs** (5).



8. Dans le champ Entrez les noms d'objet à sélectionner, entrez le nom d'ordinateur du serveur AC, puis cliquez sur **Vérifier les noms**. Si le nom saisi est valide, il est actualisé et apparaît souligné. Click OK.



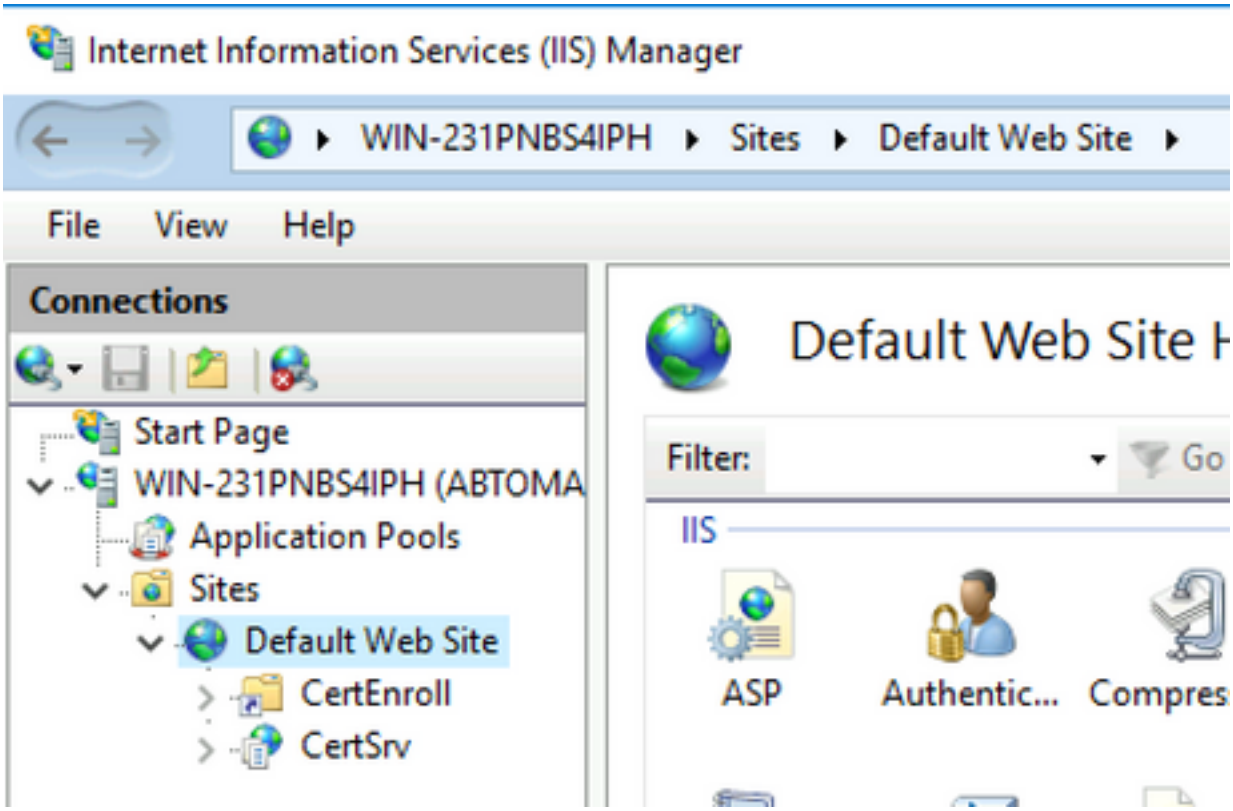
9. Choisissez l'ordinateur de l'Autorité de certification dans le champ Groupe ou noms d'utilisateurs, puis cochez la case **Autoriser** le contrôle complet pour accorder un accès complet à l'Autorité de certification. Cliquez sur **OK** puis sur **Fermer** pour terminer la tâche.



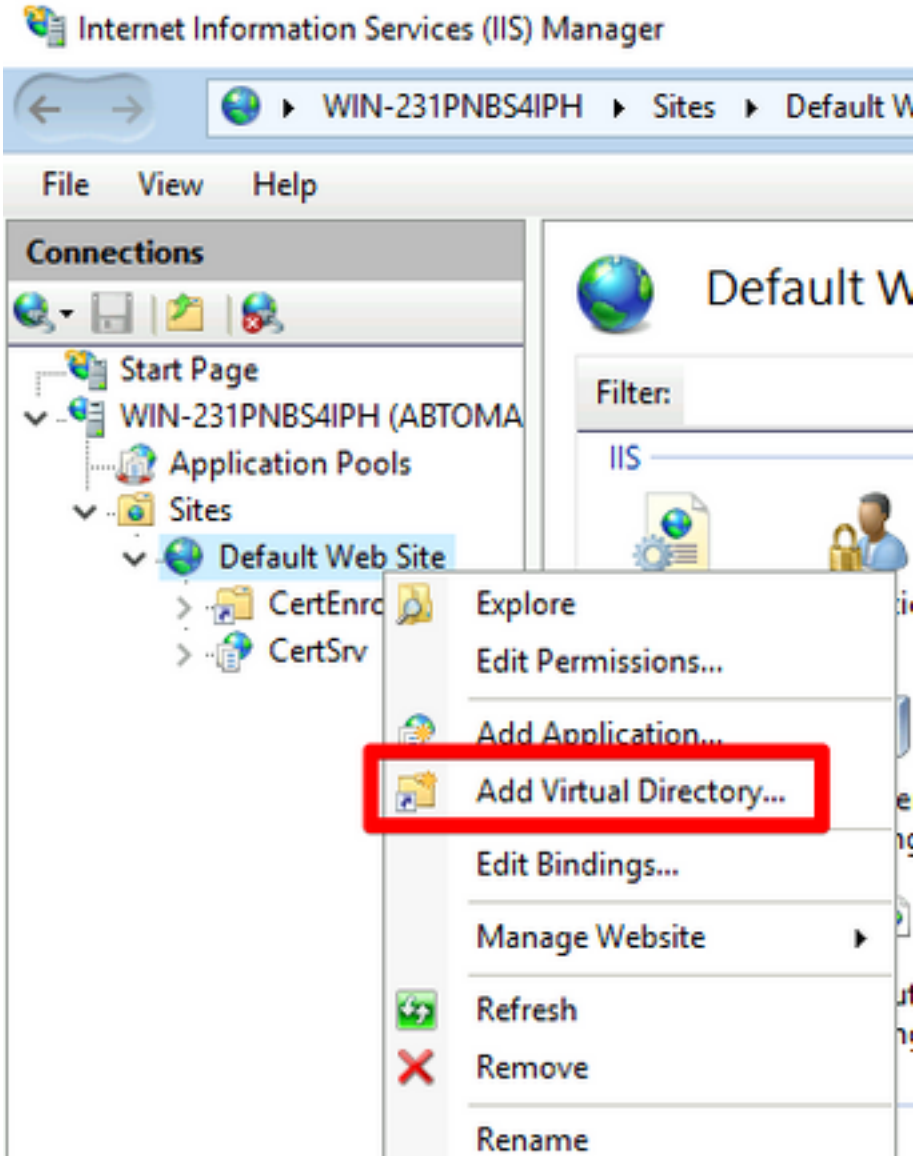
Créer un site dans IIS pour exposer le nouveau point de distribution CRL

Pour que ISE puisse accéder aux fichiers CRL, rendez le répertoire qui héberge les fichiers CRL accessible via IIS.

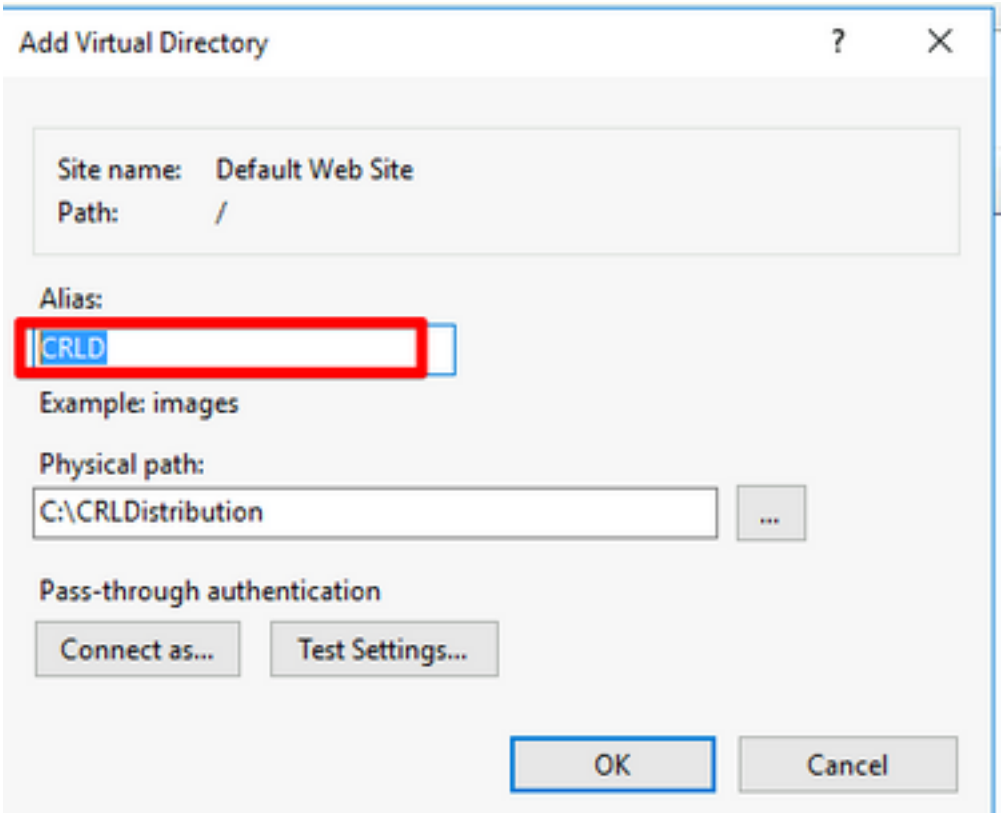
1. Dans la barre des tâches du serveur IIS, cliquez sur **Démarrer**. Choisissez **Outils d'administration > Gestionnaire des services Internet (IIS)**.
2. Dans le volet gauche (appelé arborescence de la console), développez le nom du serveur IIS, puis développez **Sites.**



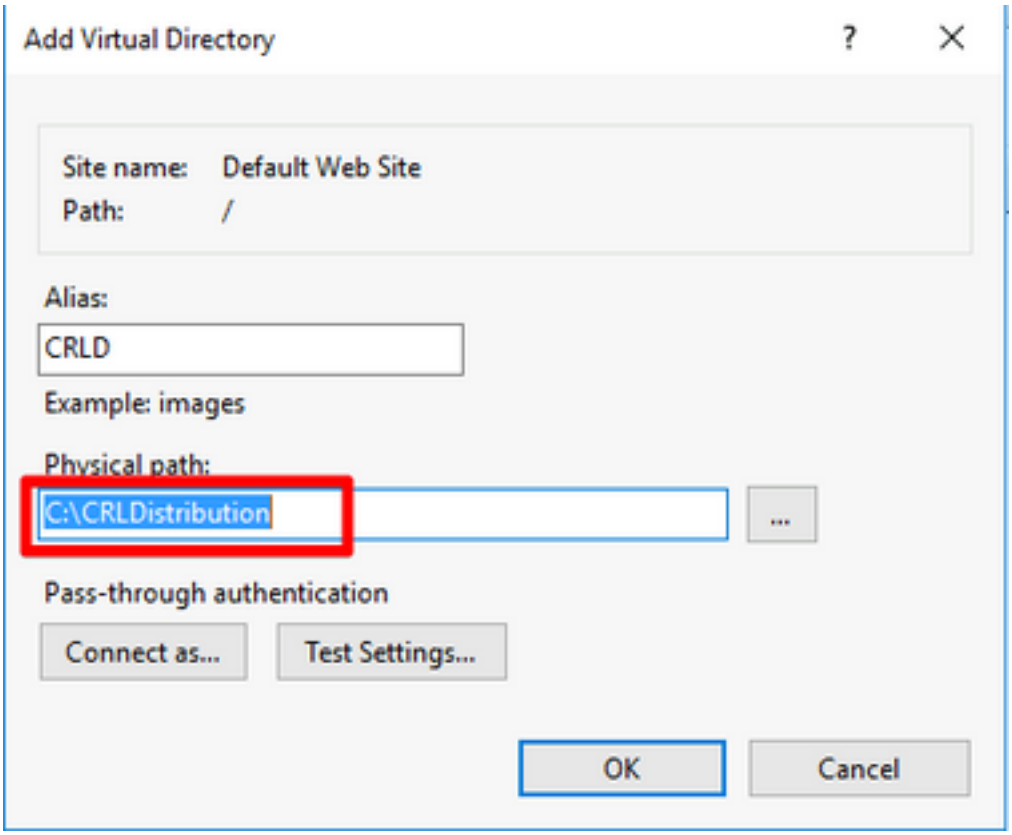
3. Cliquez avec le bouton droit sur **Site Web par défaut** et choisissez **Ajouter un répertoire virtuel**, comme illustré dans cette image.



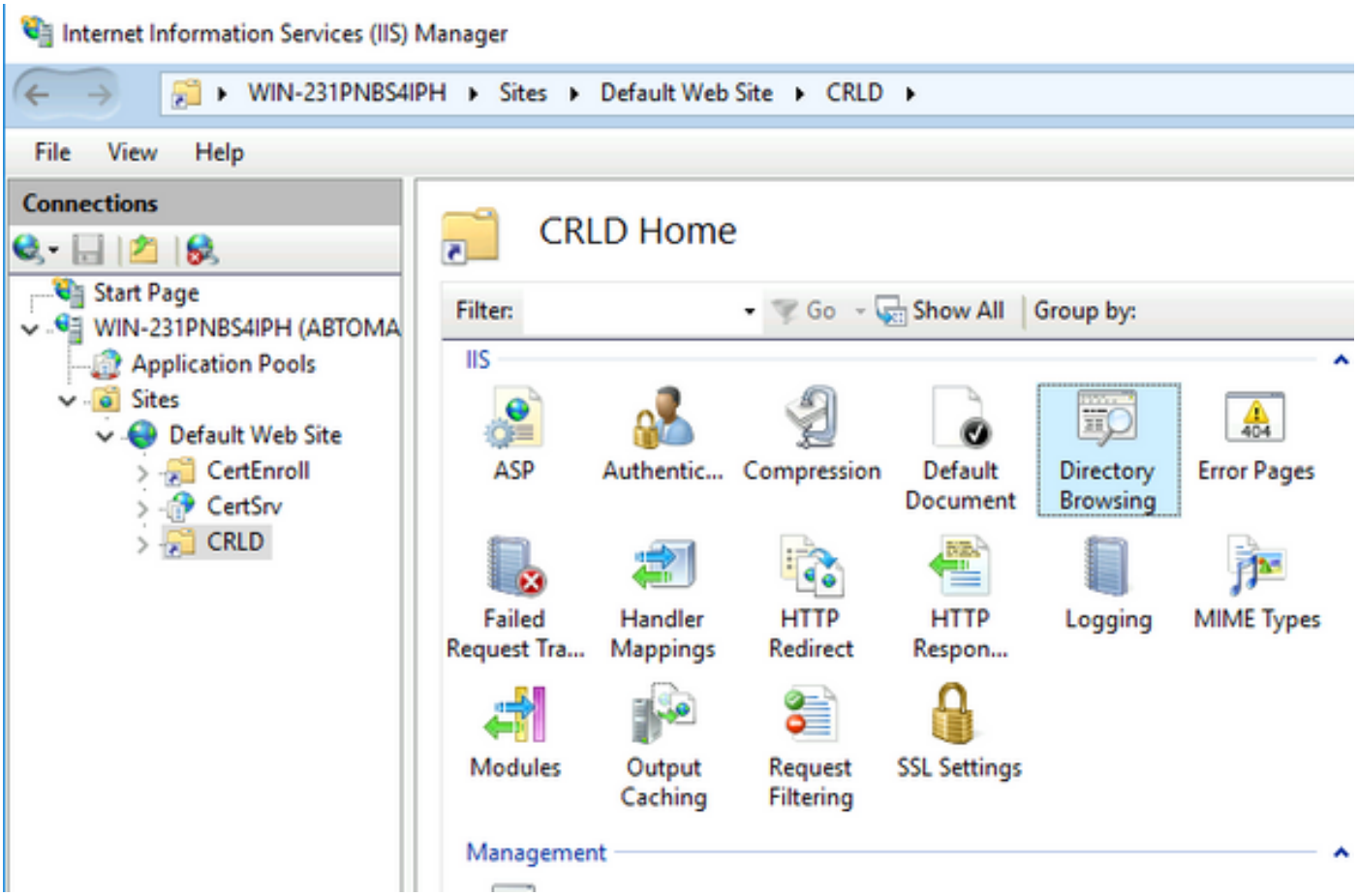
4. Dans le champ Alias, saisissez un nom de site pour le point de distribution CRL. Dans cet exemple, CRLD est saisi.



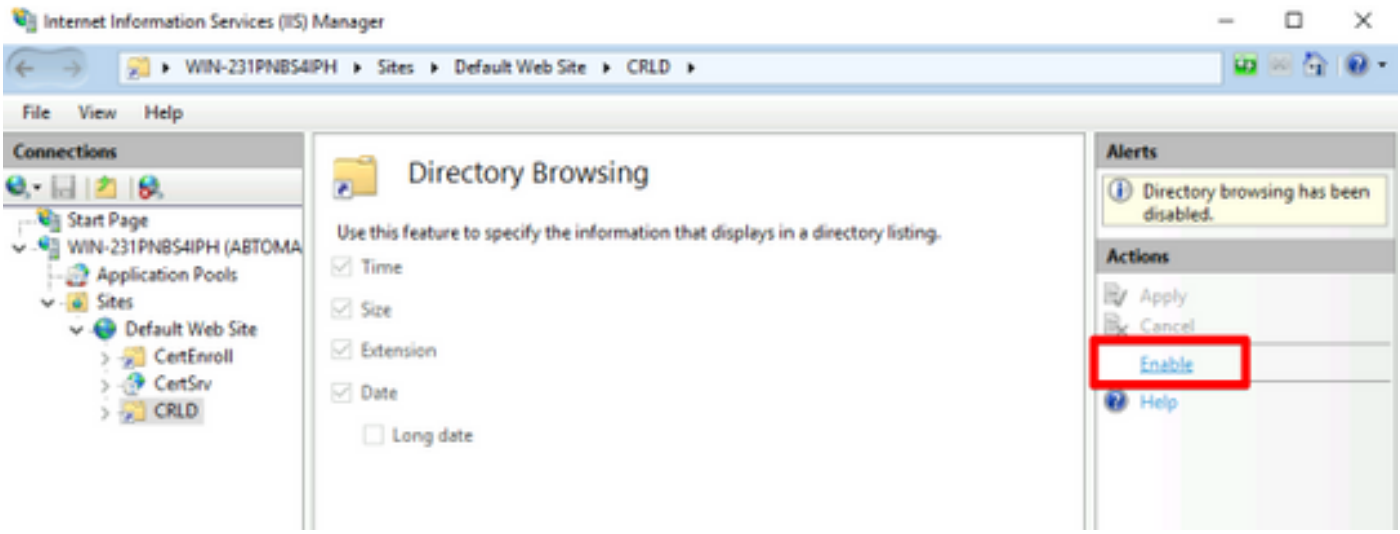
5. Cliquez sur l'ellipse (. . .) à droite du champ Physical path et accédez au dossier créé dans la section 1. Sélectionnez le dossier et cliquez sur **OK**. Cliquez sur **OK** pour fermer la fenêtre Ajouter un répertoire virtuel.



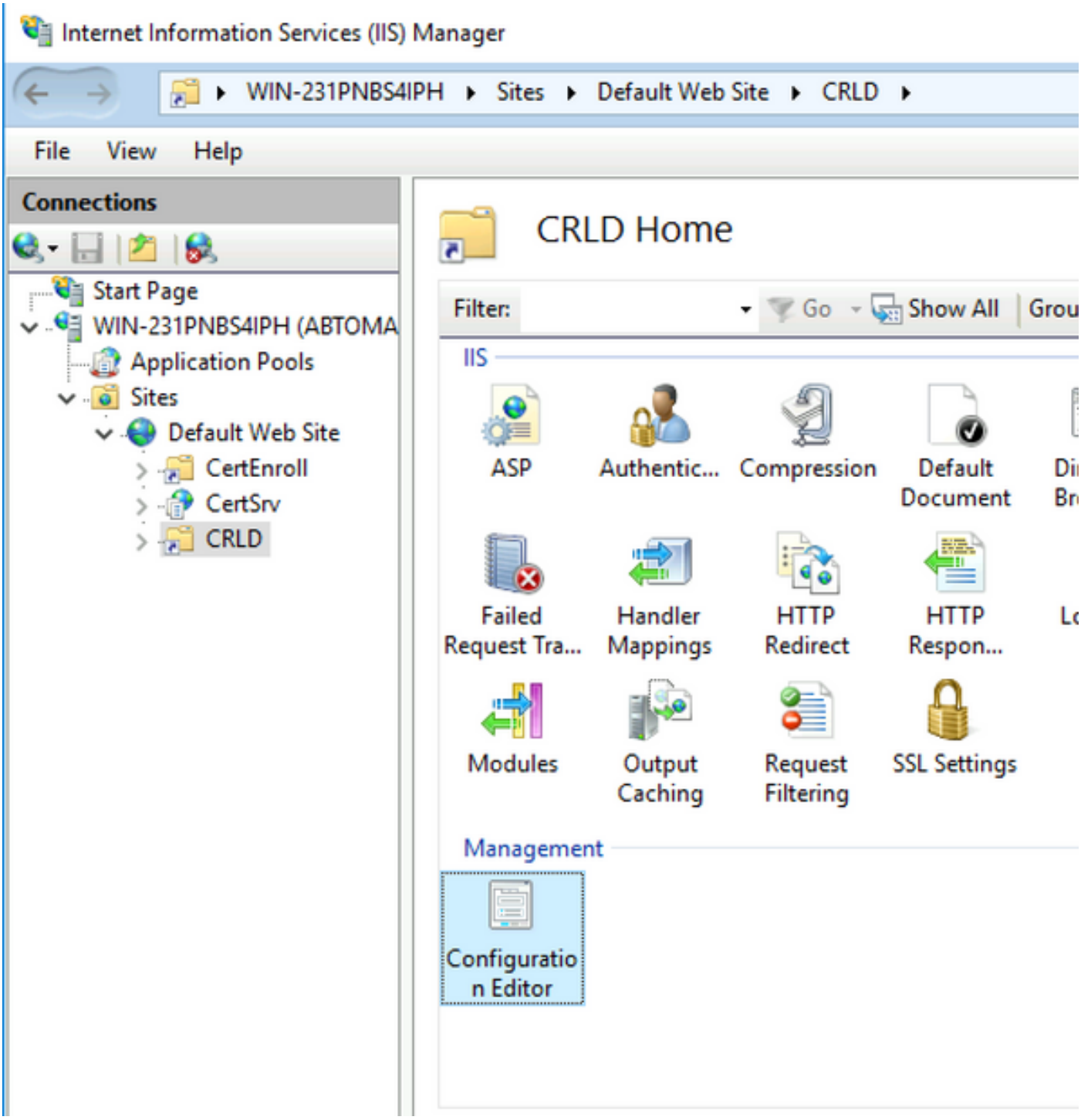
6. Le nom de site saisi à l'étape 4 doit être mis en surbrillance dans le volet gauche. Sinon, choisissez-le maintenant. Dans le volet central, double-cliquez sur **Navigation dans les répertoires**.



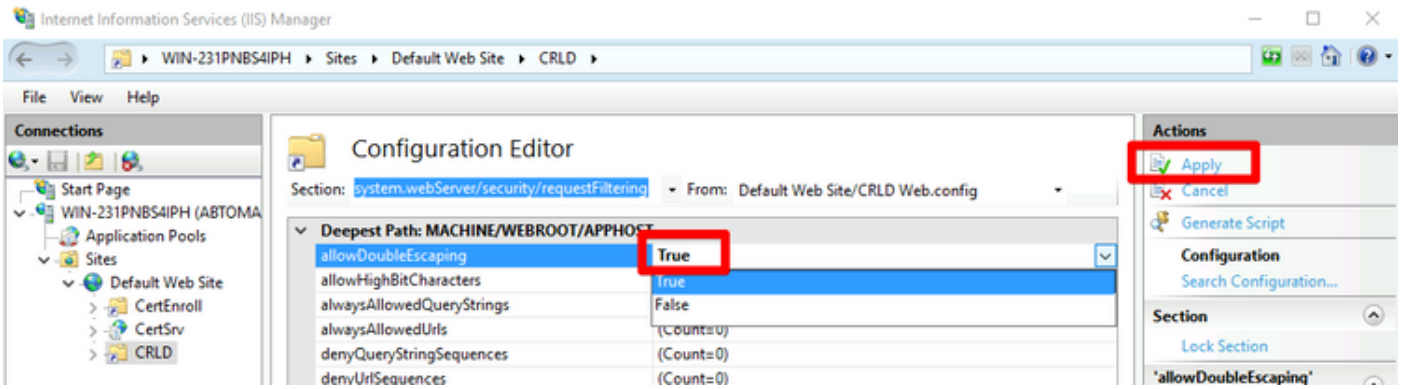
7. Dans le volet droit, cliquez sur **Activer** pour activer la navigation dans les répertoires.



8. Dans le volet gauche, sélectionnez à nouveau le nom du site. Dans le volet central, double-cliquez sur **Éditeur de configuration**.



9. Dans la liste déroulante Section, sélectionnez **system.webServer/security/requestFiltering**. Dans la liste déroulante **allowDoubleEscaping**, sélectionnez **True**. Dans le volet droit, cliquez sur **Appliquer**, comme illustré dans cette image.

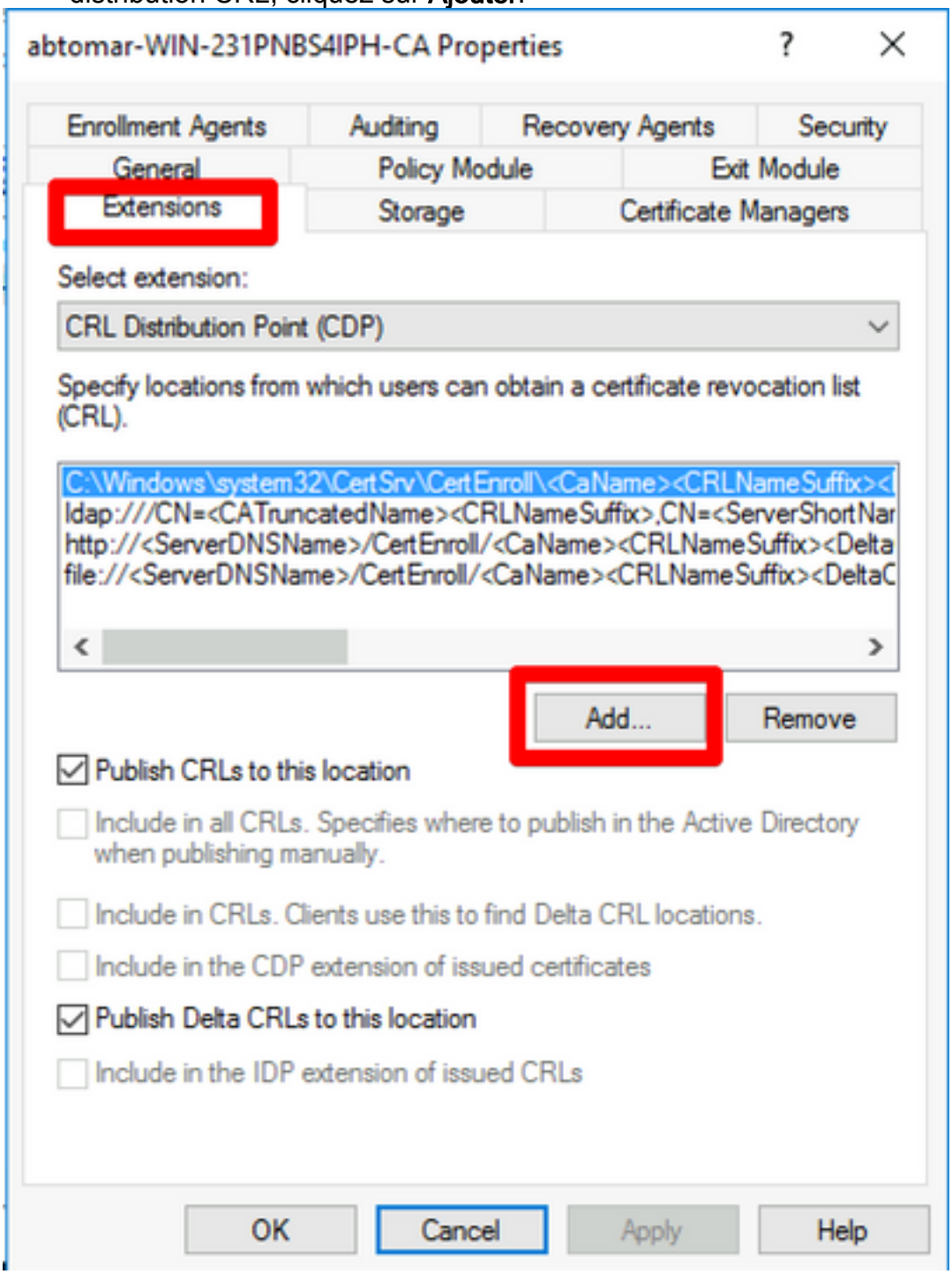


Le dossier doit maintenant être accessible via IIS.

Configurer Microsoft CA Server pour publier les fichiers CRL sur le point de distribution

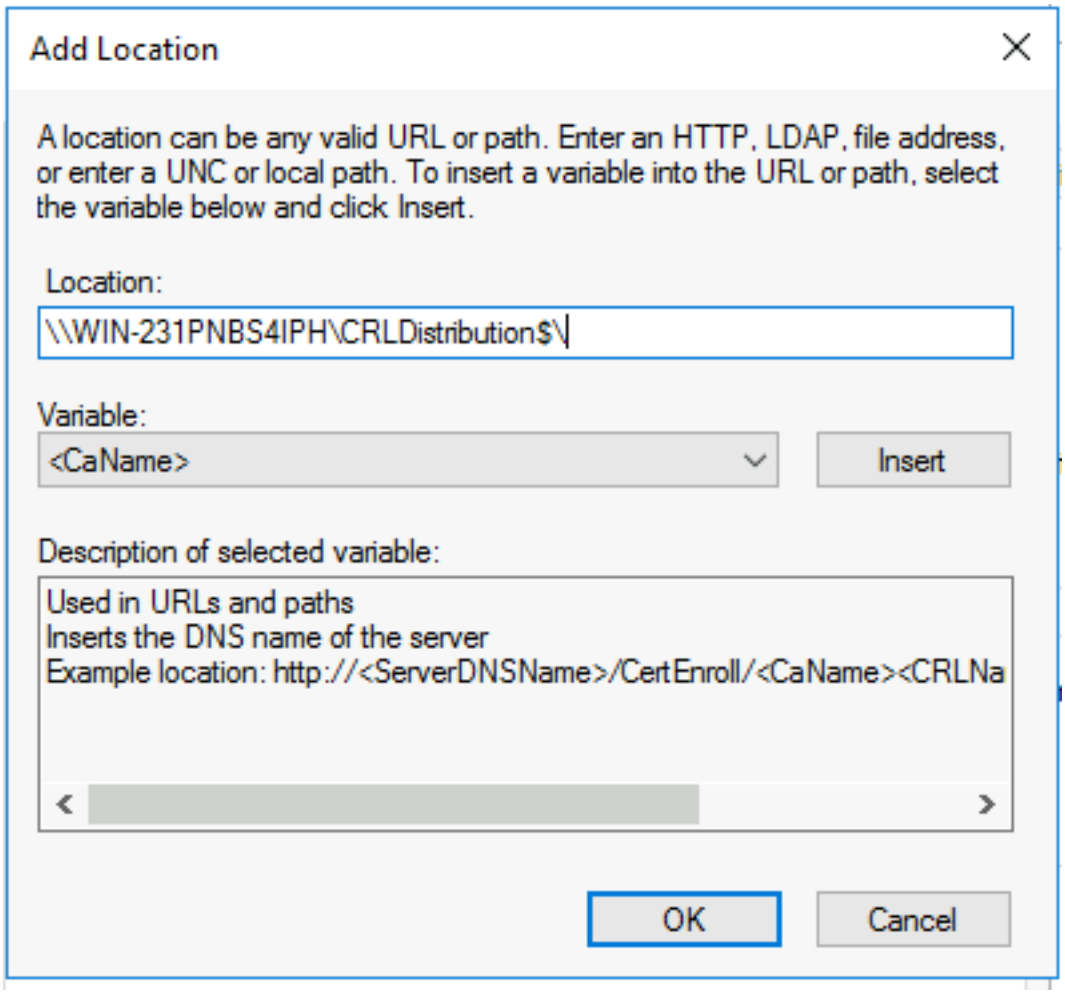
Maintenant qu'un nouveau dossier a été configuré pour héberger les fichiers CRL et que le dossier a été exposé dans IIS, configurez le serveur AC Microsoft pour publier les fichiers CRL dans le nouvel emplacement.

1. Dans la barre des tâches du serveur AC, cliquez sur **Démarrer**. Choisissez **Outils d'administration > Autorité de certification**.
2. Dans le volet gauche, cliquez avec le bouton droit sur le nom de l'autorité de certification. Choisissez **Propriétés**, puis cliquez sur l'onglet **Extensions**. Pour ajouter un nouveau point de distribution CRL, cliquez sur **Ajouter**.

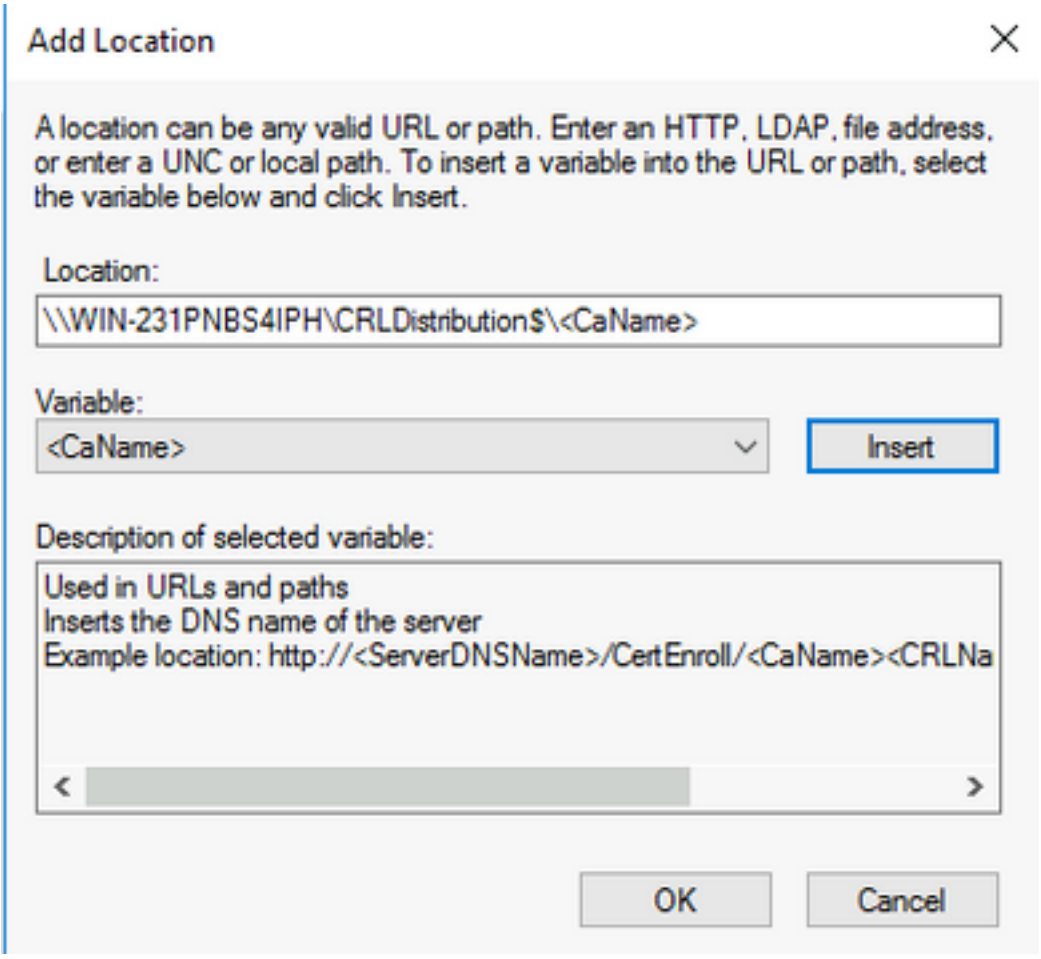


3. Dans le champ Emplacement, saisissez le chemin d'accès au dossier créé et partagé dans la section 1. Dans l'exemple de la section 1, le chemin est :

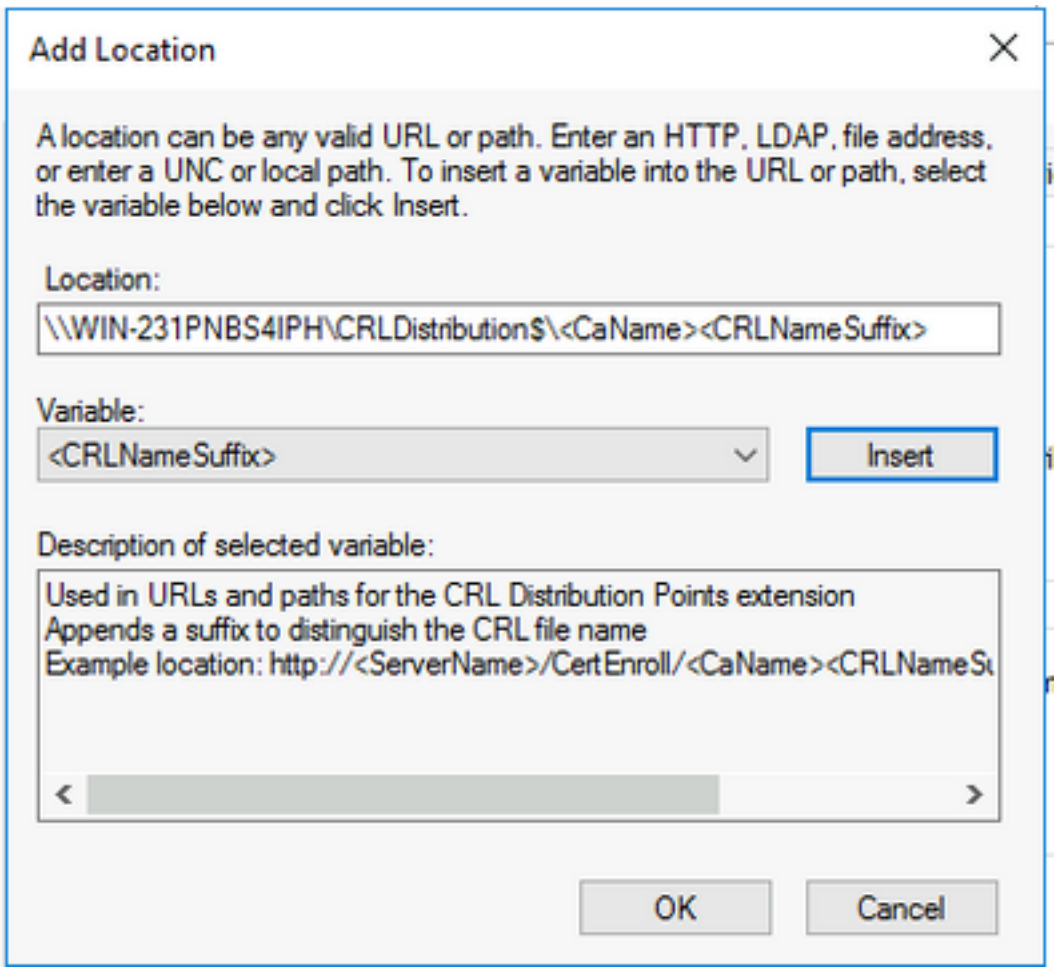
\\WIN-231PNBS4IPH\CRLDistribution$



4. Lorsque le champ Emplacement est renseigné, sélectionnez **<CaName>** dans la liste déroulante Variable, puis cliquez sur **Insérer.**

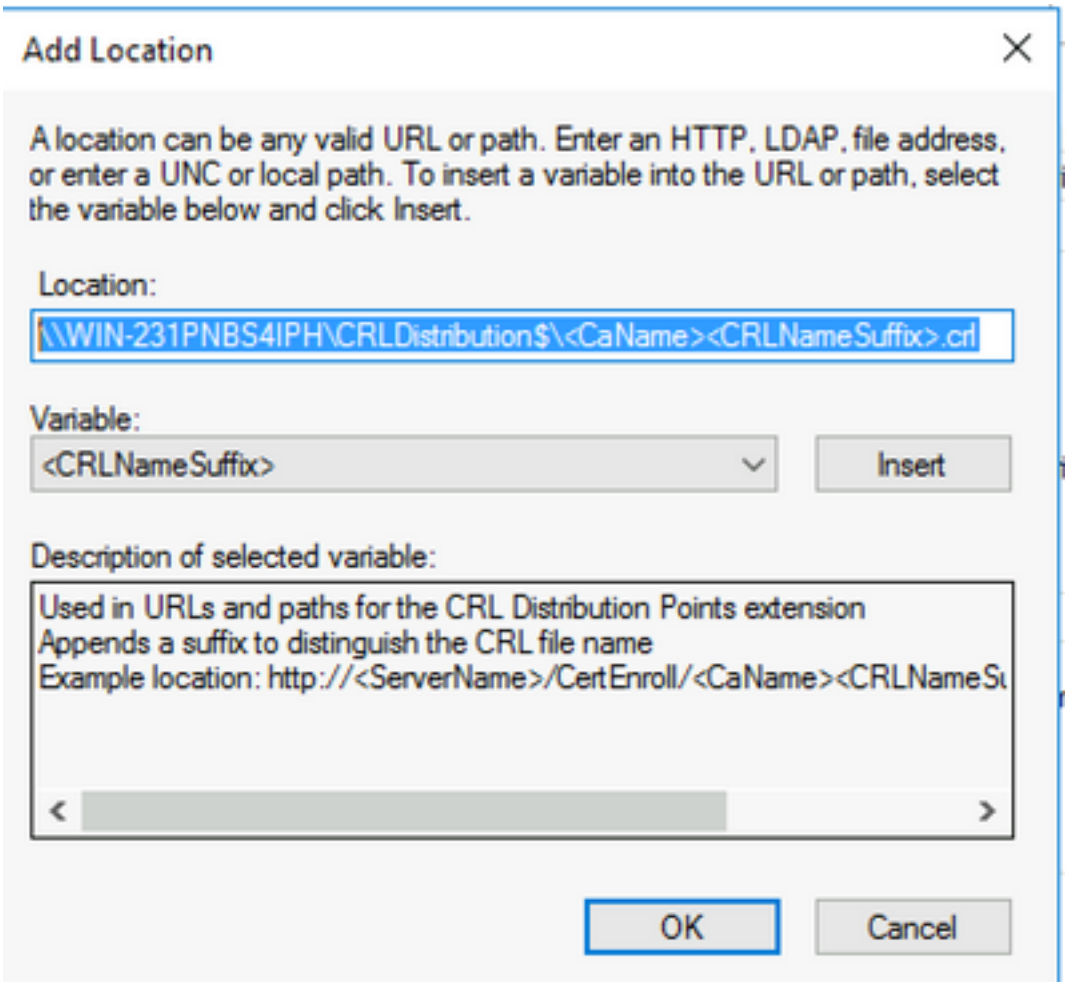


5. Dans la liste déroulante Variable, sélectionnez **<CRLNameSuffix>**, puis cliquez sur **Insérer**.



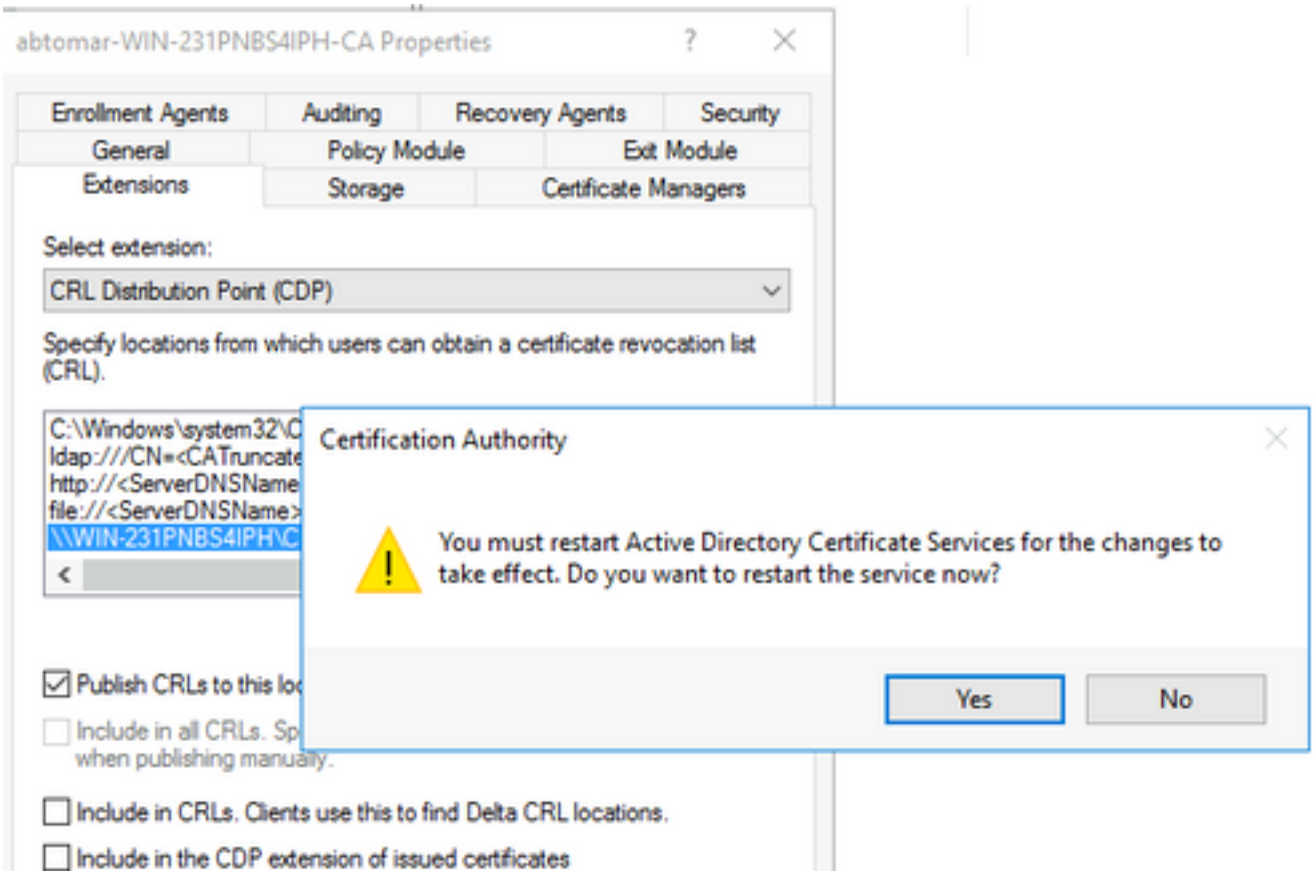
6. Dans le champ Emplacement, ajoutez **.crl** à la fin du chemin. Dans cet exemple, l'emplacement est le suivant :

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

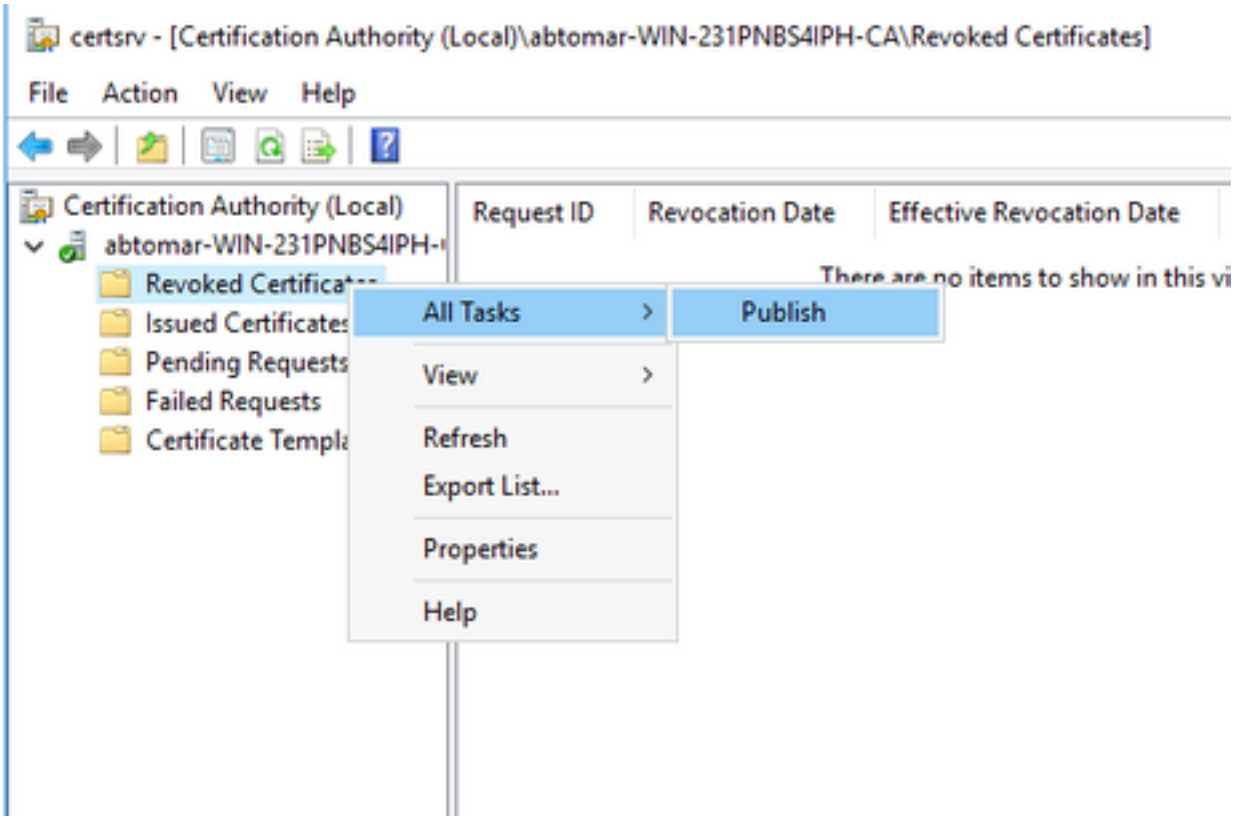


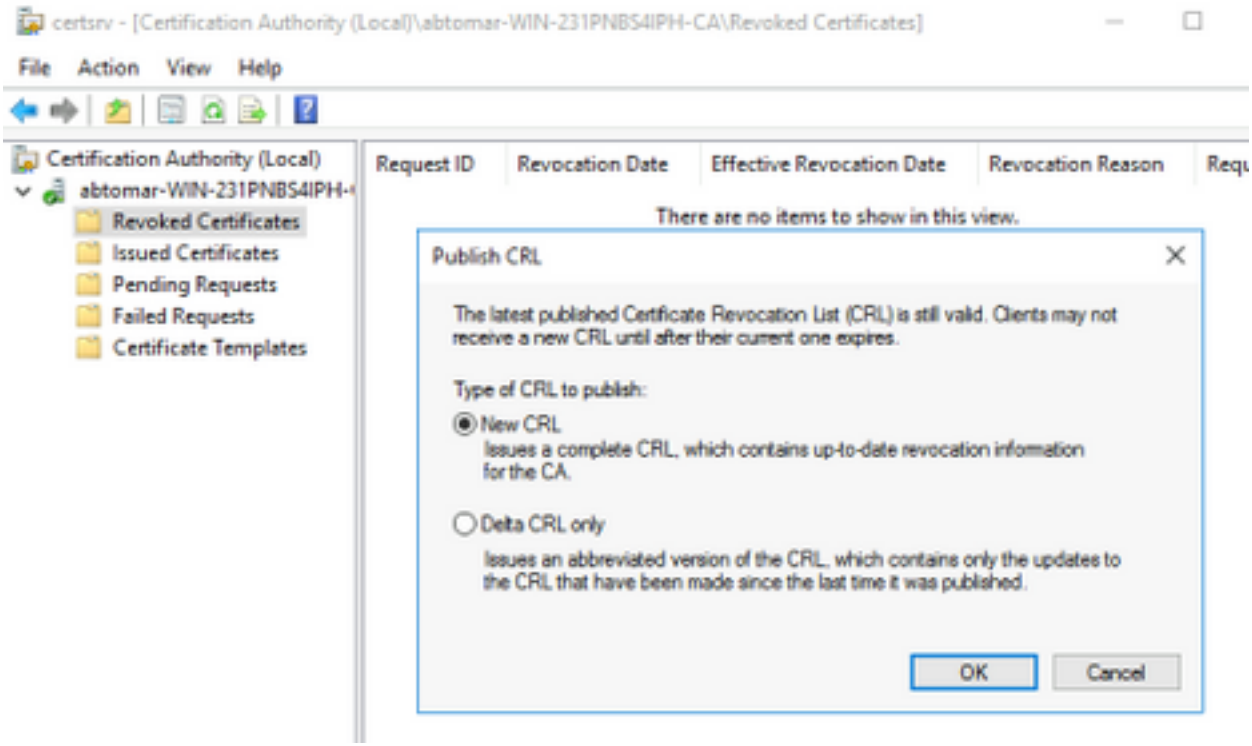
7. Cliquez sur **OK** pour revenir à l'onglet Extensions. Cochez la case **Publier les LCR à cet emplacement**, puis cliquez sur **OK** pour fermer la fenêtre Propriétés.

Une invite s'affiche pour demander l'autorisation de redémarrer les services de certificats Active Directory. **Cliquez sur Yes.**



8. Dans le volet gauche, cliquez avec le bouton droit sur **Certificats révoqués**. Choisissez **Toutes les tâches > Publier**. Assurez-vous que la nouvelle liste de révocation de certificats est sélectionnée, puis cliquez sur **OK.**





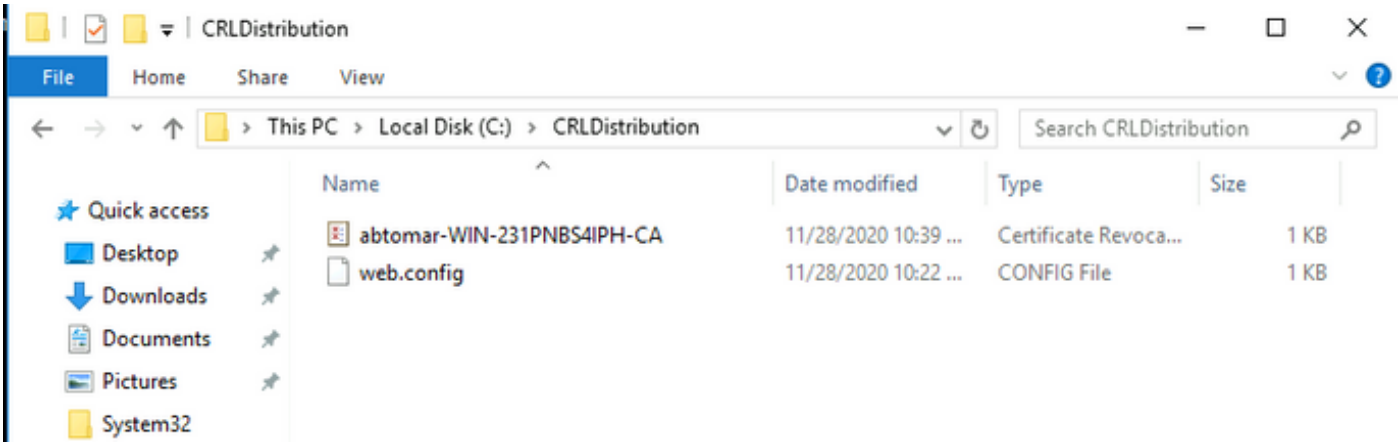
Le serveur AC Microsoft doit créer un nouveau fichier .crl dans le dossier créé dans la section 1. Si le nouveau fichier CRL est créé avec succès, aucune boîte de dialogue ne s'affiche après avoir cliqué sur OK. Si une erreur est renvoyée en ce qui concerne le nouveau dossier du point de distribution, répétez soigneusement chaque étape de cette section.

Vérifier que le fichier CRL existe et est accessible via IIS

Vérifiez que les nouveaux fichiers CRL existent et qu'ils sont accessibles via IIS à partir d'une autre station de travail avant de démarrer cette section.

1. Sur le serveur IIS, ouvrez le dossier créé dans la section 1. Un fichier .crl unique doit être présent avec le formulaire **<CANAME>.crl** où <CANAME> est le nom du serveur AC. Dans cet exemple, le nom de fichier est :

abtomar-WIN-231PNBS4IPH-CA.crl



2. À partir d'une station de travail sur le réseau (idéalement sur le même réseau que le noeud principal d'administration ISE), ouvrez un navigateur Web et accédez à http://<SERVER>/<CRLSITE> où <SERVER> est le nom du serveur IIS configuré dans la section 2 et <CRLSITE> le nom du site choisi pour le point de distribution dans la section 2. Dans cet exemple, l'URL est :

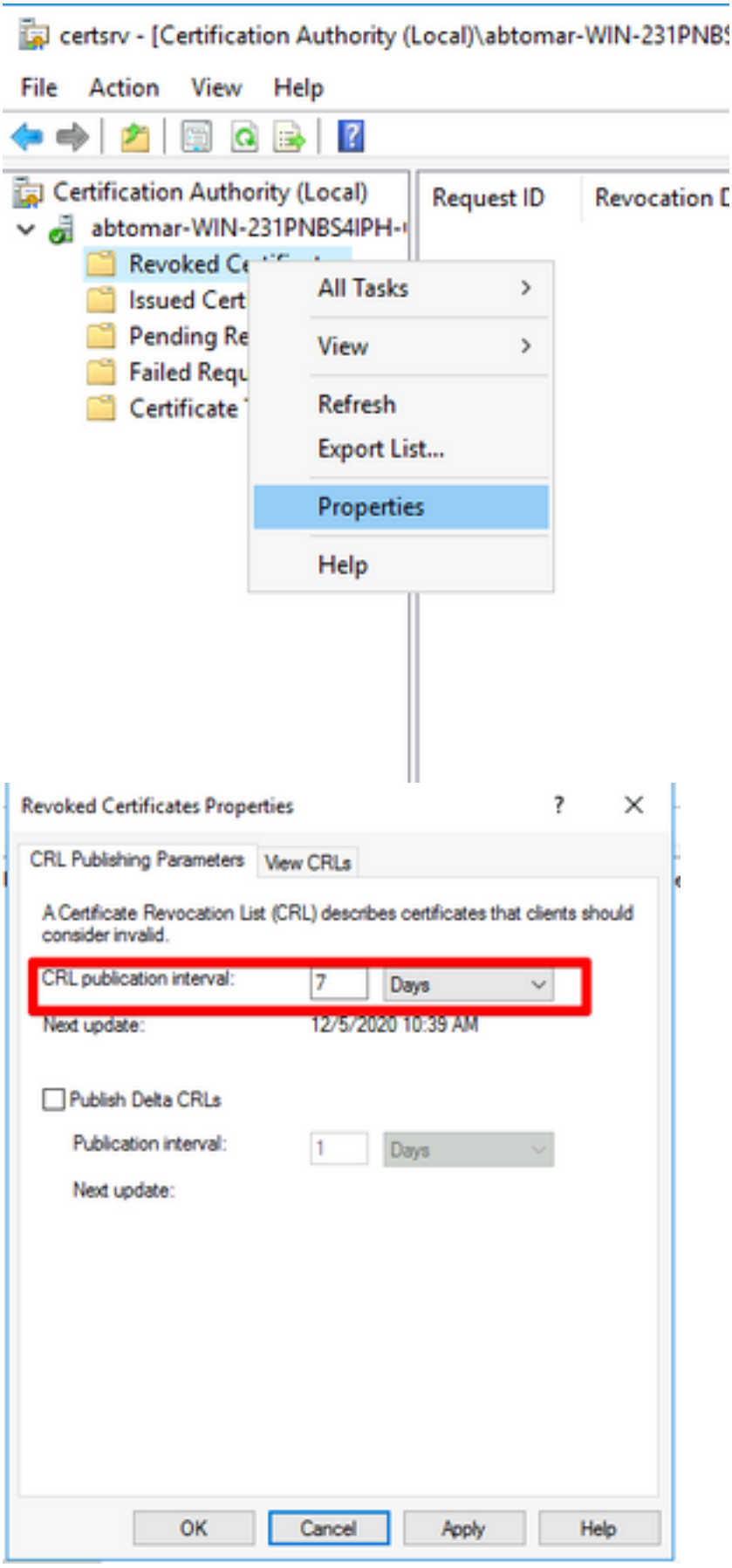
http://win-231pnbs4iph/CRLD

L'index du répertoire s'affiche, qui inclut le fichier observé à l'étape 1.

Configurer ISE pour utiliser le nouveau point de distribution CRL

Avant que ISE ne soit configuré pour récupérer la liste de révocation de certificats, définissez l'intervalle de publication de la liste de révocation de certificats. La stratégie de détermination de cet intervalle dépasse le cadre de ce document. Les valeurs potentielles (dans Microsoft CA) sont comprises entre 1 heure et 411 ans, inclusivement. La valeur par défaut est 1 semaine. Une fois qu'un intervalle approprié pour votre environnement a été déterminé, définissez l'intervalle avec les instructions suivantes :

1. Dans la barre des tâches du serveur AC, cliquez sur **Démarrer**. Choisissez **Outils d'administration > Autorité de certification**.
2. Dans le volet gauche, développez l'autorité de certification. Cliquez avec le bouton droit sur le dossier **Certificats révoqués** et sélectionnez **Propriétés.**
3. Dans les champs intervalle de publication CRL, saisissez le numéro requis et choisissez la période. Cliquez sur **OK** pour fermer la fenêtre et appliquer la modification. Dans cet exemple, un intervalle de publication de 7 jours est configuré.



4. Entrez la commande **certutil -getreg CA\Clock*** pour confirmer la valeur ClockSkew. La valeur par défaut est 10 minutes.

Exemple de rapport :

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

5. Entrez la commande **certutil -getreg CA\CRLov*** pour vérifier si CRLOverlapPeriod a été défini manuellement. Par défaut, la valeur CRLOverlapUnit est 0, ce qui indique qu'aucune valeur manuelle n'a été définie. Si la valeur est différente de 0, enregistrez la valeur et les unités.

Exemple de rapport :

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

6. Entrez la commande **certutil -getreg CA\CRLpe*** pour vérifier la période CRLP, définie à l'étape 3.

Exemple de rapport :

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

7. Calculez la période de grâce de la LCR comme suit :

a. Si CRLOverlapPeriod a été défini à l'étape 5 : OVERLAP = CRLOverlapPeriod, en minutes ;

Autre : OVERLAP = (période CRLP/10), en minutes

b. Si SURLAP > 720, alors SURLAP = 720

c. Si SURLAP < (1,5 * ClockSkewMinutes), alors SURLAP = (1,5 * ClockSkewMinutes)

d. Si OVERLAP > CRLPeriod, en minutes, OVERLAP = CRLPperiode en minutes

e. Période de grâce = SUPERLAP + minutes de décalage d'horloge

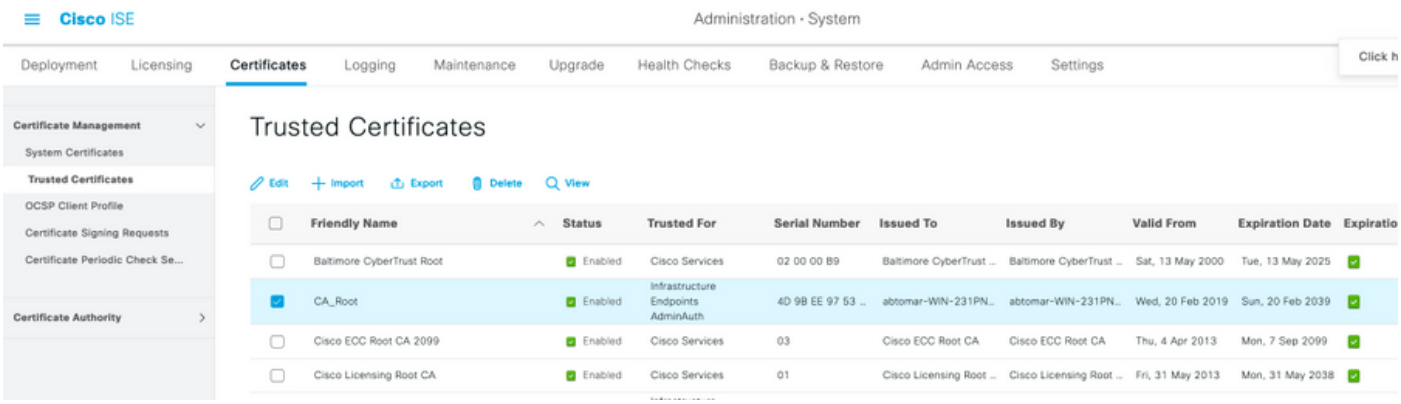
```
Example:

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
```

Le délai de grâce calculé est le délai entre le moment où l'autorité de certification publie la prochaine liste de révocation de certificats et l'expiration de la liste de révocation de certificats actuelle. ISE doit être configuré pour récupérer les LCR en conséquence.

8. Connectez-vous au noeud d'administration principal ISE et choisissez **Administration > System > Certificates**. Dans le volet gauche, sélectionnez **Certificat approuvé**



9. Cochez la case en regard du certificat CA pour lequel vous avez l'intention de configurer des LCR. Cliquez sur **Edit**.

10. En bas de la fenêtre, cochez la case **Télécharger la liste de révocation de certificats**.

11. Dans le champ URL de distribution CRL, saisissez le chemin d'accès au point de distribution CRL, qui inclut le fichier .crl, créé à la section 2. Dans cet exemple, l'URL est :

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

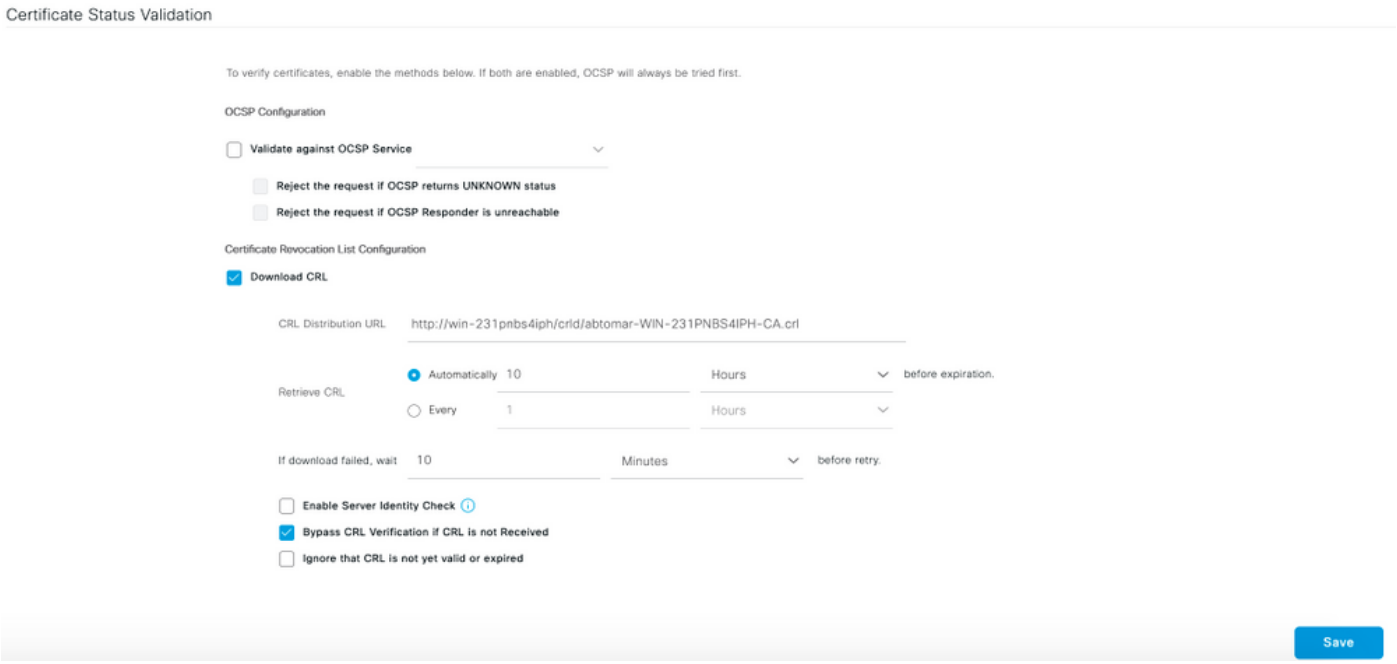
12. ISE peut être configuré pour récupérer la liste de révocation de certificats à intervalles réguliers ou en fonction de l'expiration (qui, en général, est également un intervalle régulier). Lorsque l'intervalle de publication CRL est statique, des mises à jour CRL plus opportunes sont obtenues lorsque cette dernière option est utilisée. Cliquez sur la case d'option **Automatically**.

13. Définissez la valeur de récupération sur une valeur inférieure à la période de grâce calculée à l'étape 7. Si le jeu de valeurs est plus long que la période de grâce, ISE vérifie le point de distribution de la liste de révocation de certificats avant que l'autorité de certification ait publié la liste de révocation de certificats suivante. Dans cet exemple, la période de grâce est calculée sur 730 minutes, soit 12 heures et 10 minutes. Une valeur de 10 heures sera utilisée pour la récupération

14. Définissez l'intervalle des nouvelles tentatives en fonction de votre environnement. Si ISE ne parvient pas à récupérer la liste de révocation de certificats à l'intervalle configuré à l'étape précédente, il réessaiera à cet intervalle plus court.

15. Cochez la case **Ignorer la vérification CRL si la liste de révocation de certificats n'est pas reçue** pour autoriser l'authentification basée sur le certificat à continuer normalement (et sans vérification CRL) si ISE n'a pas pu récupérer la liste de révocation de certificats pour cette autorité de certification lors de sa dernière tentative de téléchargement. Si cette case n'est pas cochée, toute authentification basée sur un certificat avec des certificats émis par cette autorité de certification échouera si la liste de révocation de certificats ne peut pas être récupérée.

16. Cochez la case **Ignorer que la liste de révocation de certificats n'est pas encore valide ou a expiré** pour permettre à ISE d'utiliser des fichiers de liste de révocation de certificats expirés (ou non encore valides) comme s'ils étaient valides. Si cette case n'est pas cochée, ISE considère qu'une liste de révocation de certificats n'est pas valide avant sa date d'entrée en vigueur et après sa prochaine mise à jour. Cliquez sur **Enregistrer** pour terminer la configuration.



Informations internes Cisco

1. Microsoft. « Configurer un point de distribution CRL pour les certificats. » http://technet.microsoft.com/en-us/library/ee649260%28v=ws.10%29.aspx, 7 octobre 2009 [18 décembre 2012]

2. Microsoft. « Publier manuellement la liste de révocation de certificats. » http://technet.microsoft.com/en-us/library/cc778151%28v=ws.10%29.aspx, 21 janvier 2005 [18 décembre 2012]

3. Microsoft. « Configurez les périodes de chevauchement CRL et Delta CRL. » http://technet.microsoft.com/en-us/library/cc731104.aspx, 11 avril 2011 [18 décembre 2012]

4. MS2065 [MSFT]. « Comment EffectiveDate (cette mise à jour), NextUpdate et NextCRLPublish sont calculés. » http://blogs.technet.com/b/pki/archive/2008/06/05/how-effectivedate-thisupdate-nextupdate-and-nextcrlpublish-are-calculated.aspx, 4 juin 2008 [18 décembre 2012]