# ISEの証明書失効リスト(CRL)を発行するためのMicrosoft CAサーバの設定

## 内容



## はじめに

このドキュメントでは、証明書失効リスト(CRL)の更新を発行するためにインターネットインフォメーションサービス(IIS)を実行するMicrosoft認証局(CA)サーバの設定について説明します。また、証明書の検証に使用する更新を取得するようにCisco Identity Services Engine(ISE)（バージョン3.0以降）を設定する方法についても説明します。証明書の検証で使用する各種 CA ルート証明書の CRL を取得するように、ISE を設定できます。

## 前提条件

### 要件

このドキュメントに関する固有の要件はありません。

### 使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- Cisco Identity Services Engineリリース3.0
- Microsoft Windows Server 2008 R2

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認して

ください。

# 設定

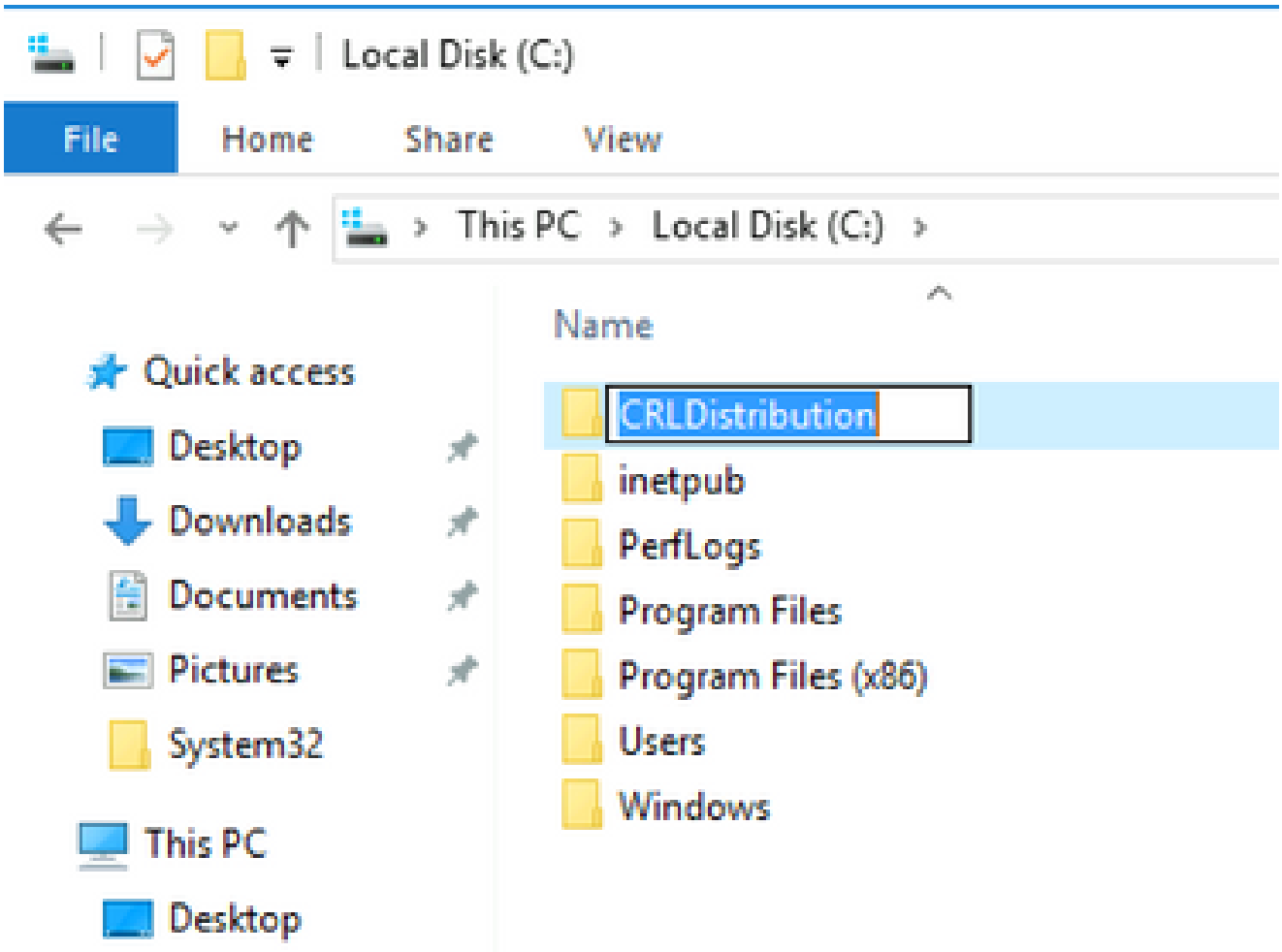
このセクションでは、このドキュメントで説明する機能を設定するために必要な情報を提供しています。

## CRLファイルを格納するためのフォルダをCAに作成して設定する

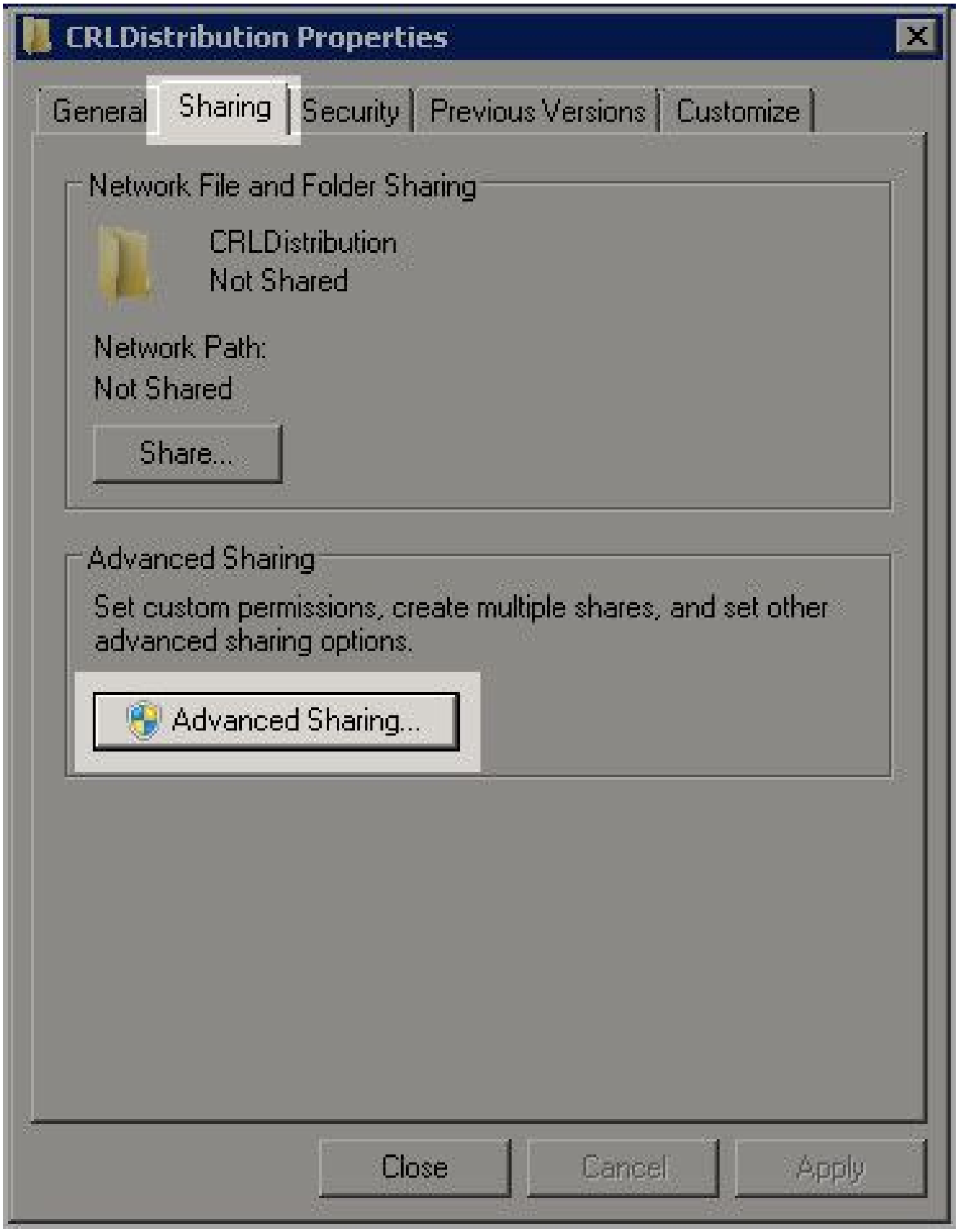
最初の作業は、CA サーバ上に CRL ファイルを保存する場所を設定することです。デフォルトでは、Microsoft CAサーバは次の場所にファイルを発行します **C:\Windows\system32\CertSrv\CertEnroll**

このシステム フォルダを使用する代わりに、ファイル用の新しいフォルダを作成します。

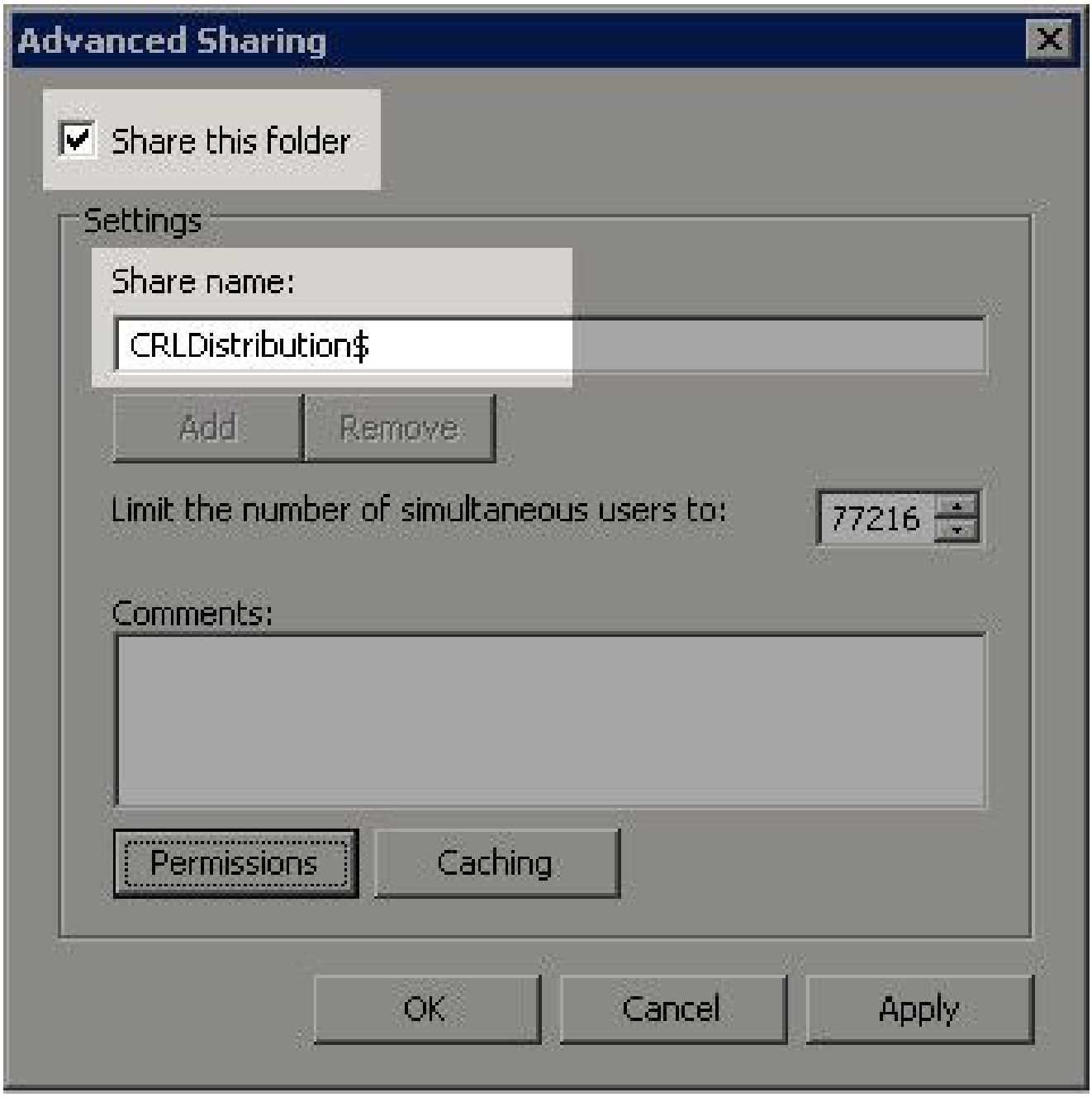
1. IISサーバで、ファイルシステム上の場所を選択し、新しいフォルダを作成します。この例では、フォルダが作成さ**C:\CRLDistribution**れます。



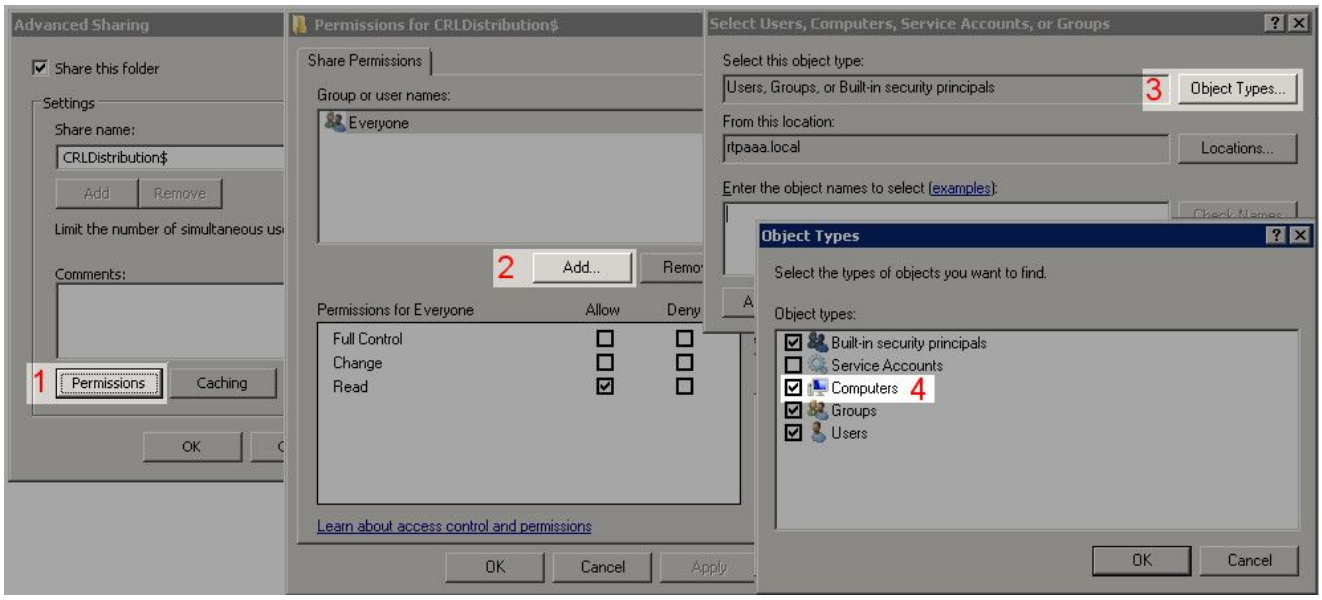

2. CA が新しいフォルダに CRL ファイルを書き込めるように、共有を有効にします。新しいフォルダを右クリックし、を選択し**Properties**てタ**Sharing**ブをクリックし、をクリックし**Advanced Sharing**ます。



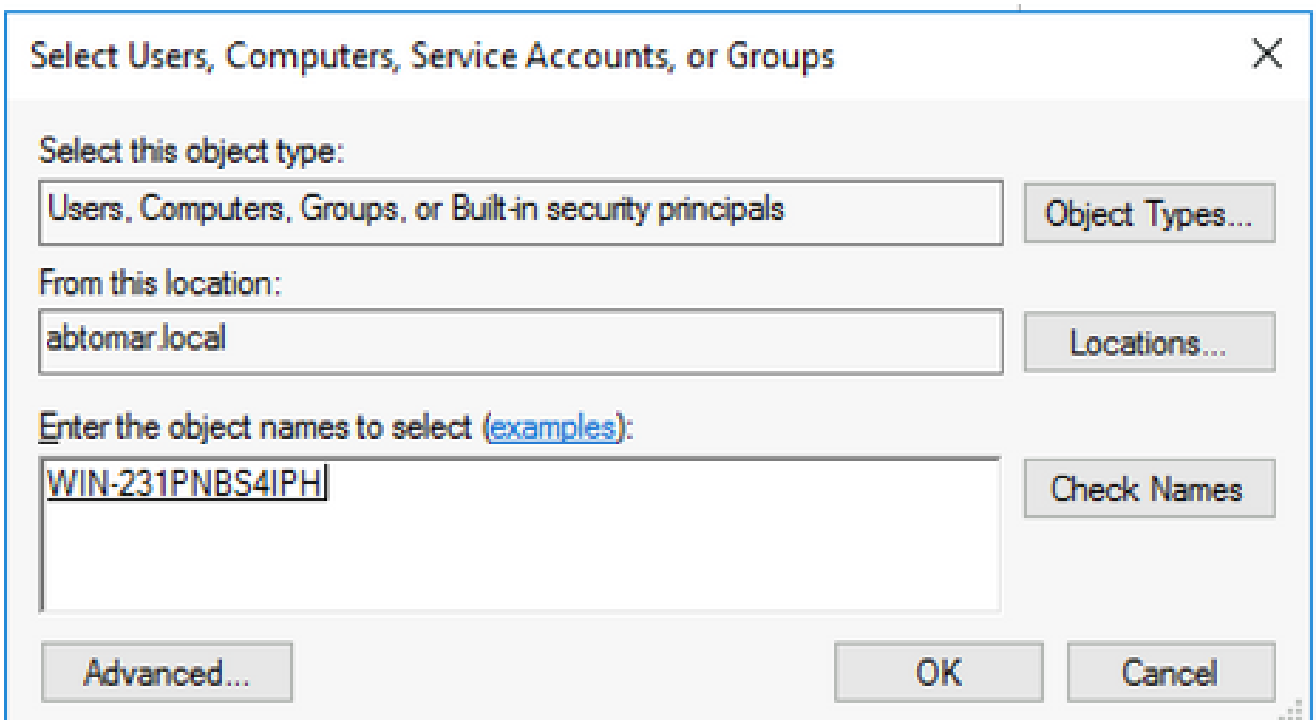

3. フォルダを共有するには、チェックボックスをオンにし**Share this folder**、[共有名]フィールドの共有名の末尾にドル記号($)を追加して、共有を非表示にします。




4. (**Permissions**1)をクリックし、 (2)**Add**をクリックし、 (**Object Types**3)をクリックして、**Computers**チェックボックス(4)をオンにします。

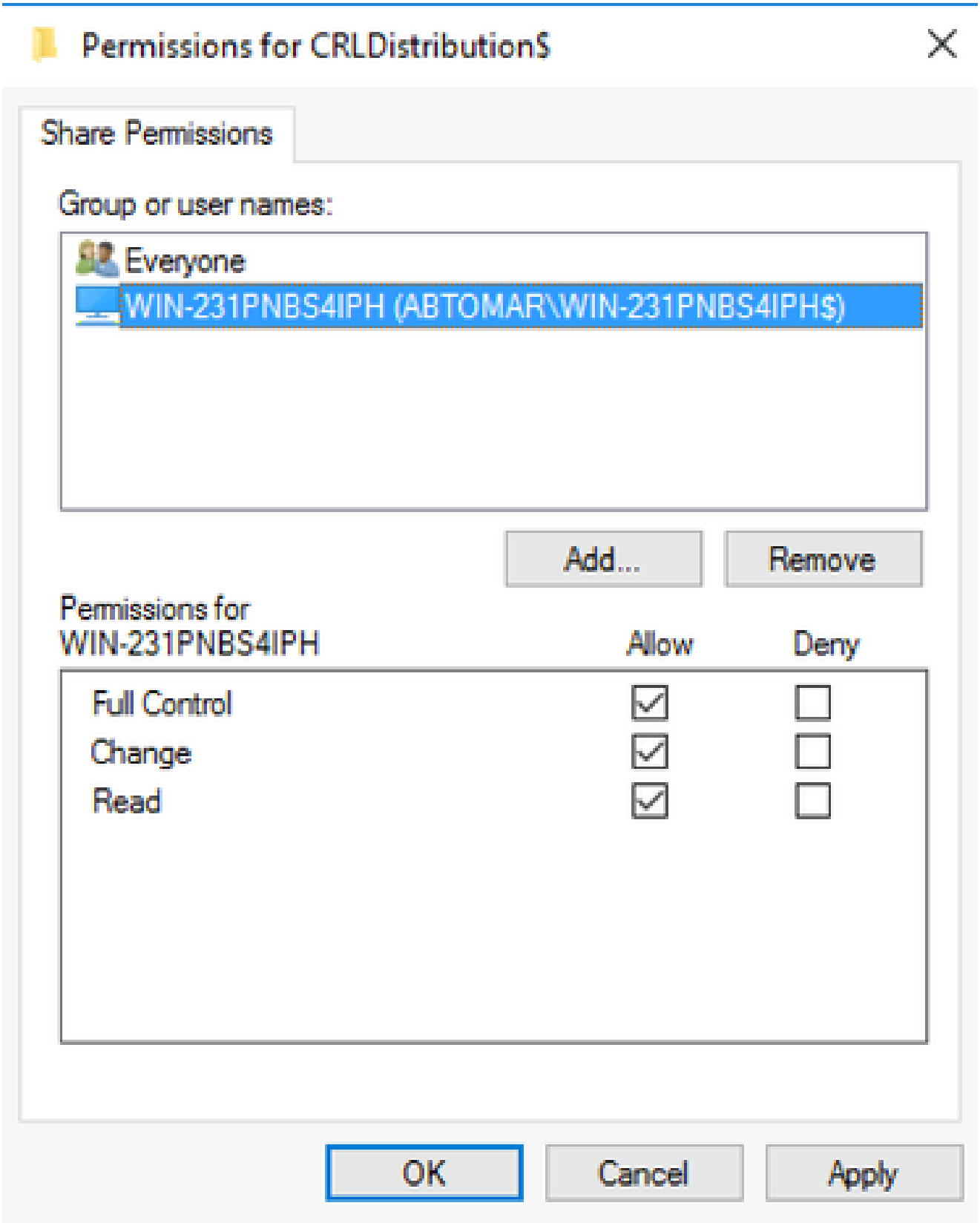



5. Select Users, Computers, Service Accounts, or Groupsウィンドウに戻るには、をクリックしOKます。Enter the object names to selectフィールドに、CAサーバのコンピュータ名（この例ではWIN0231PNBS4IPH）を入力し、をクリックしCheck Namesます。入力された名前が有効な場合は、名前が更新されて下線が付きます。をクリックします。OK

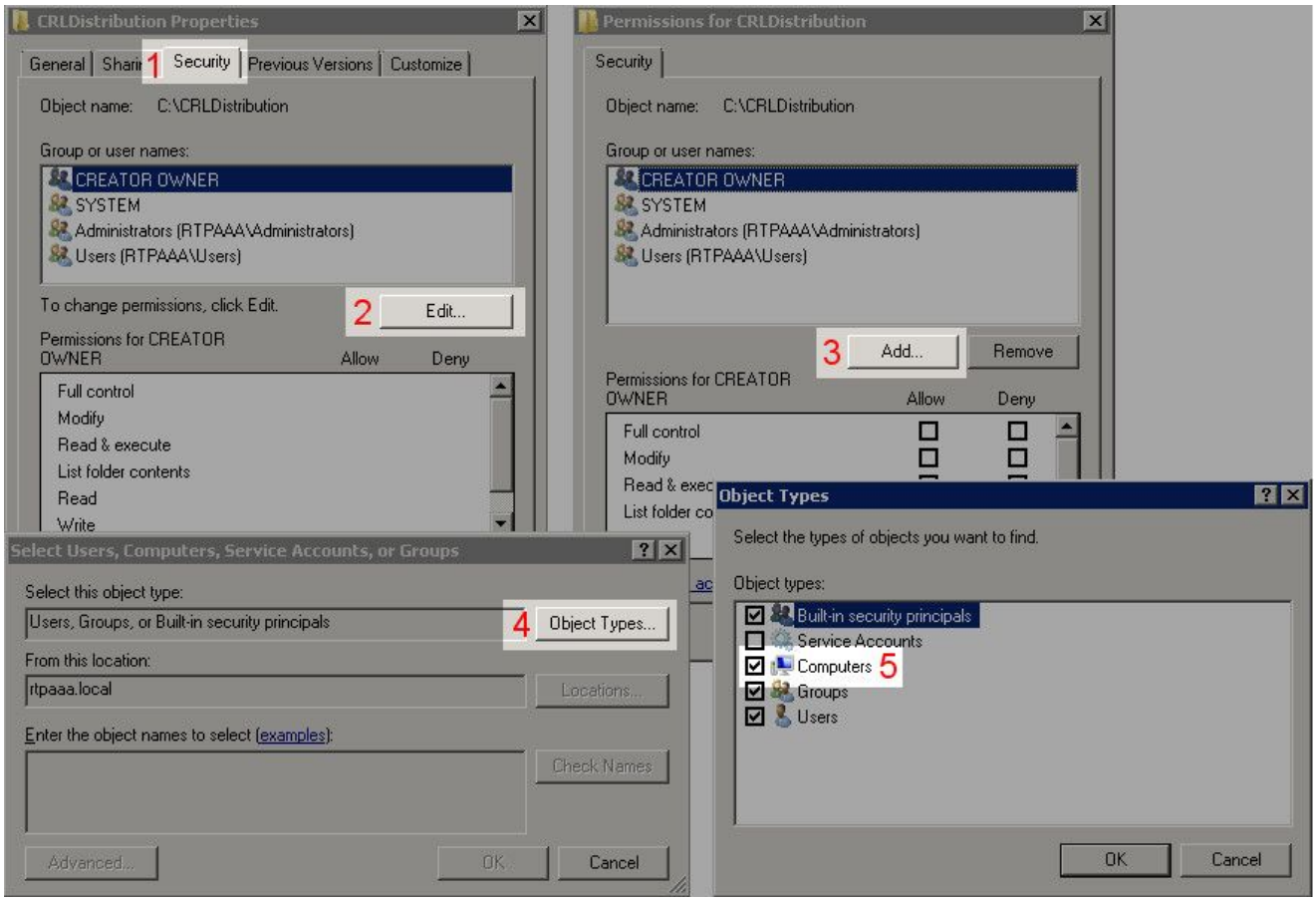



6. [Group or user names] フィールドで CA コンピュータを選択します。CAへのフルアクセスを許可するFull ControlAllowをチェックします。

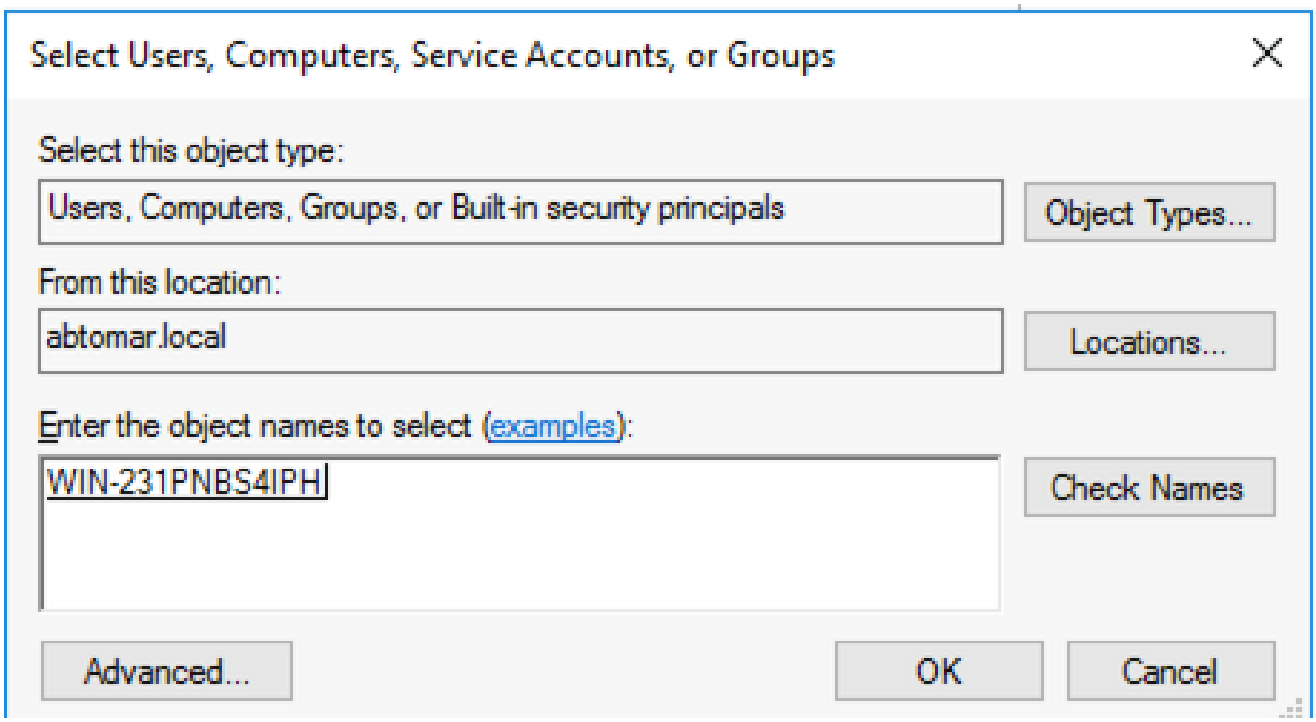
　　をクリックします。OKもうOK一度クリックして[詳細な共有]ウィンドウを閉じ、[プロパティ]ウィンドウに戻ります。



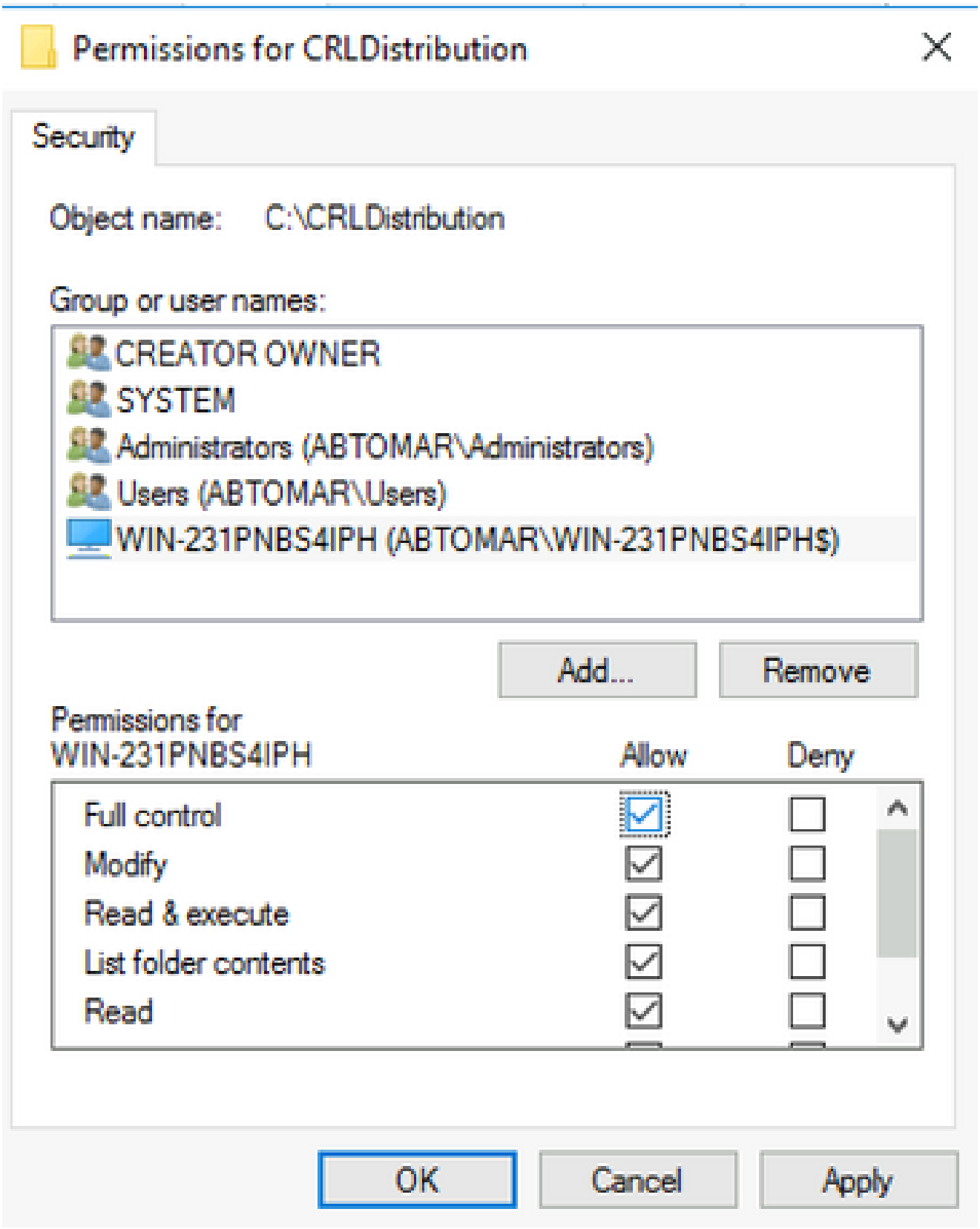

7. CA が新しいフォルダに CRL ファイルを書き込めるように、適切なセキュリティ権限を設定します。タブをクリックしSecurity(1)、 (2)、 Edit(Add3)、 Object Types(4)の順にクリックし、Computersチェックボックスをオンにします(5)。




8. Enter the object names to selectフィールドに、CAサーバのコンピュータ名を入力し、をクリックしCheck Namesます。入力された名前が有効な場合は、名前が更新されて下線が付きます。をクリックします。OK




9. Group or user namesフィールドでCAコンピュータを選択し、CAへのフルアクセスを許可するFull controlAllowにチェックマークを付けます。をクリックOKし、をクリックしてタスクCloseを完了します。

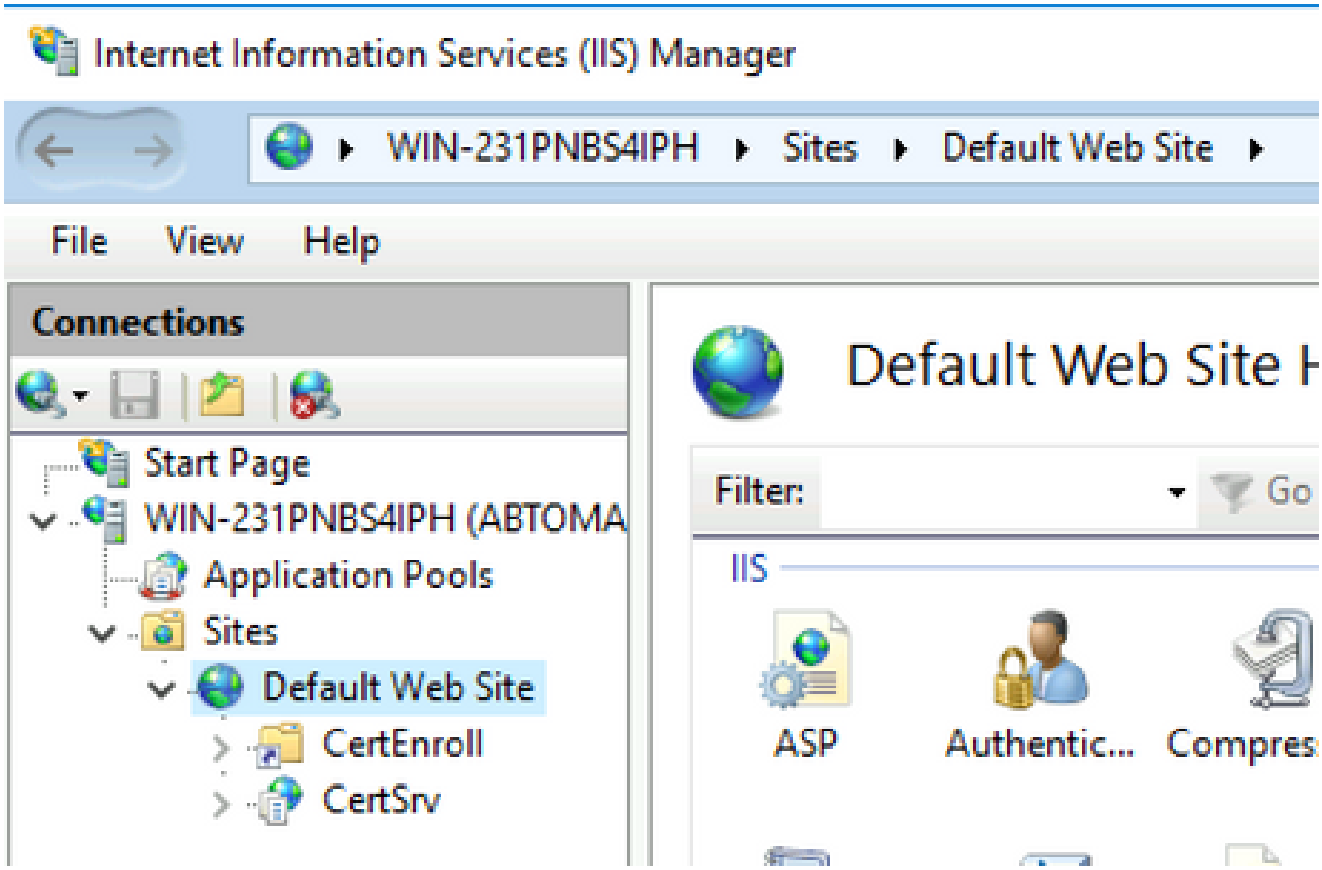



## 新しいCRL分散ポイントを公開するサイトをIISに作成する

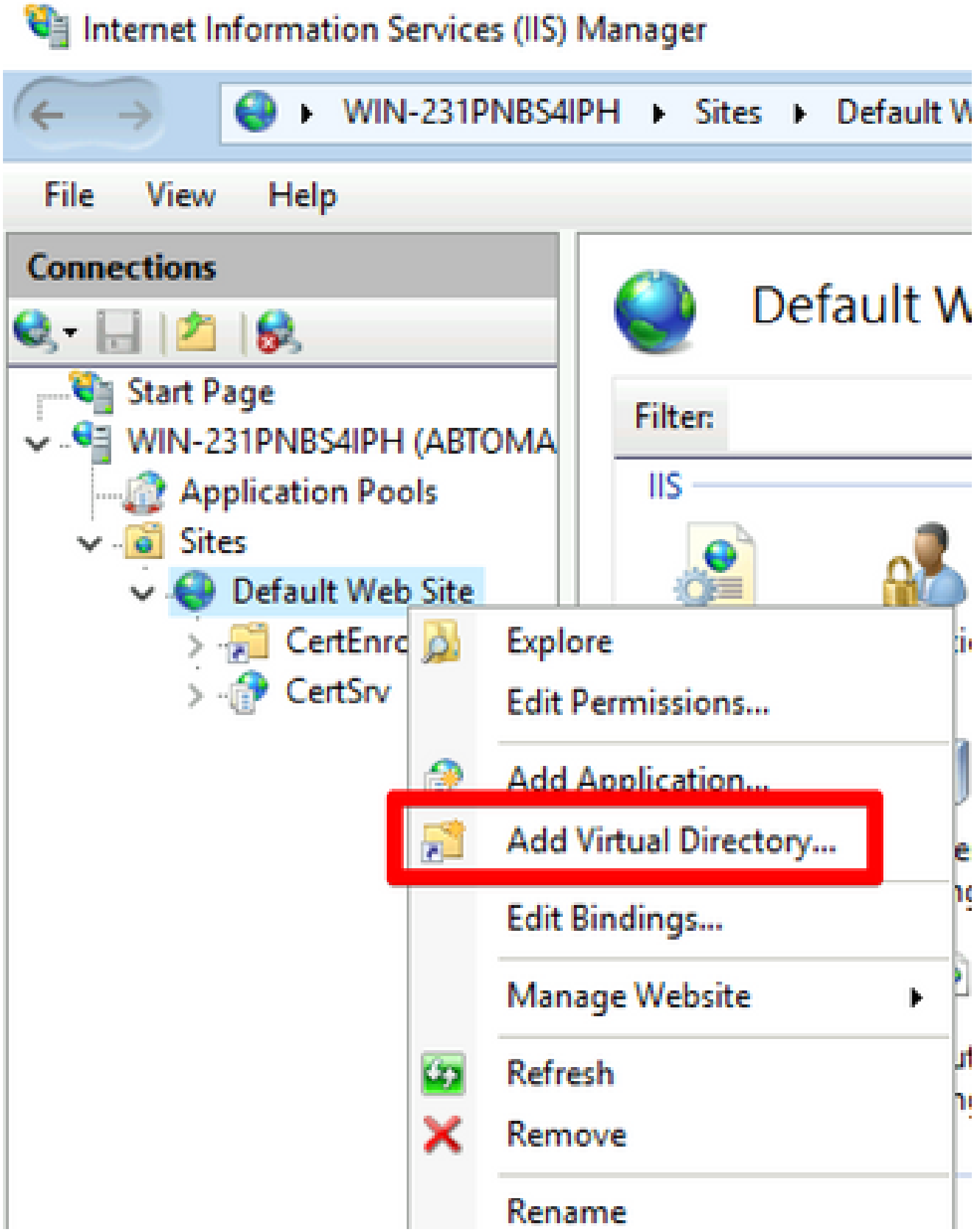
ISE が CRL ファイルにアクセスできるように、CRL ファイルを格納するディレクトリを IIS 経由でアクセス可能にします。

1. IISサーバのタスクバーで、をクリックし**Start**ます。選択.**Administrative Tools > Internet Information Services (IIS) Manager**

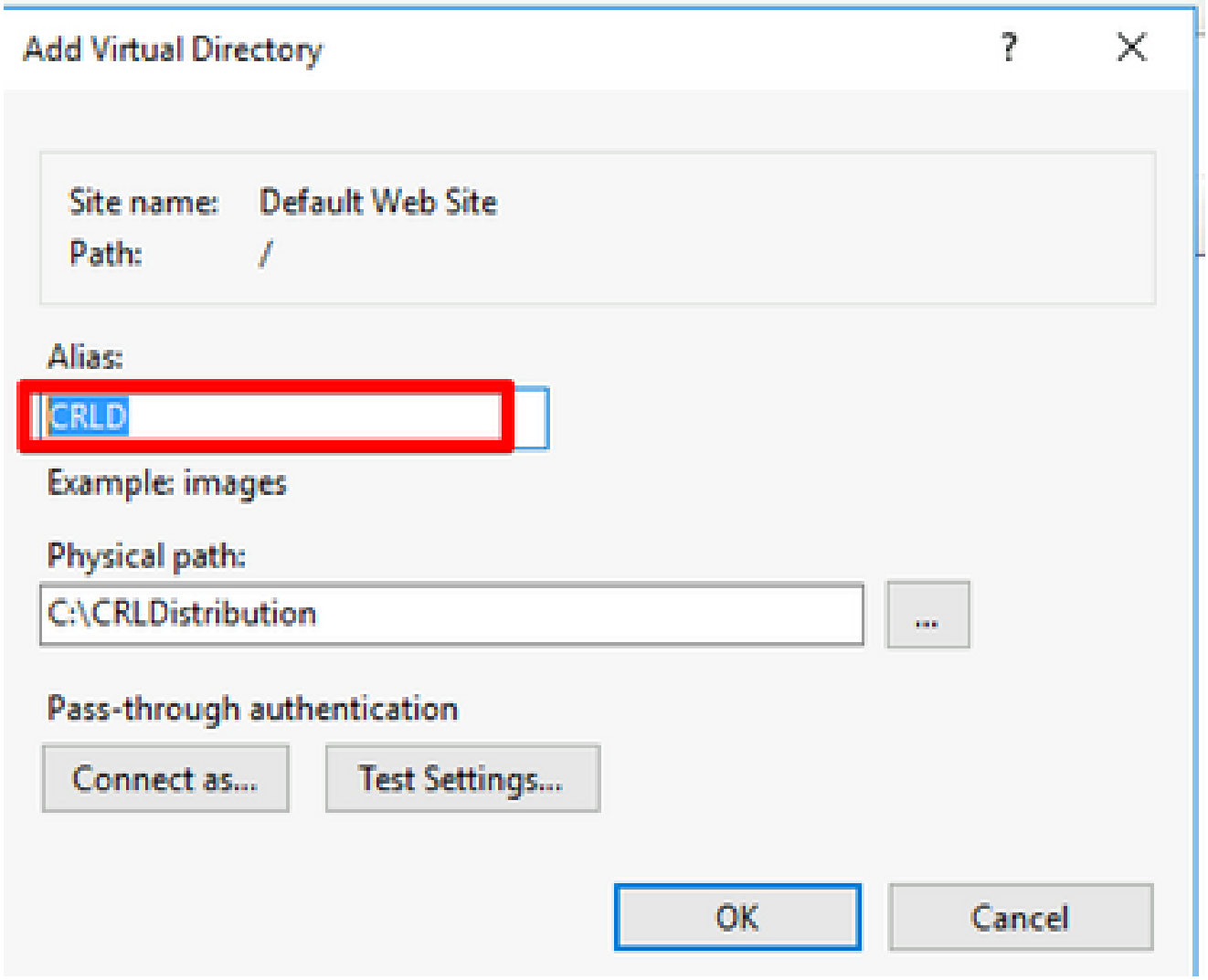
2. 左側のペイン（コンソールツリー）で、IISサーバ名を展開し、を展開しSitesます。



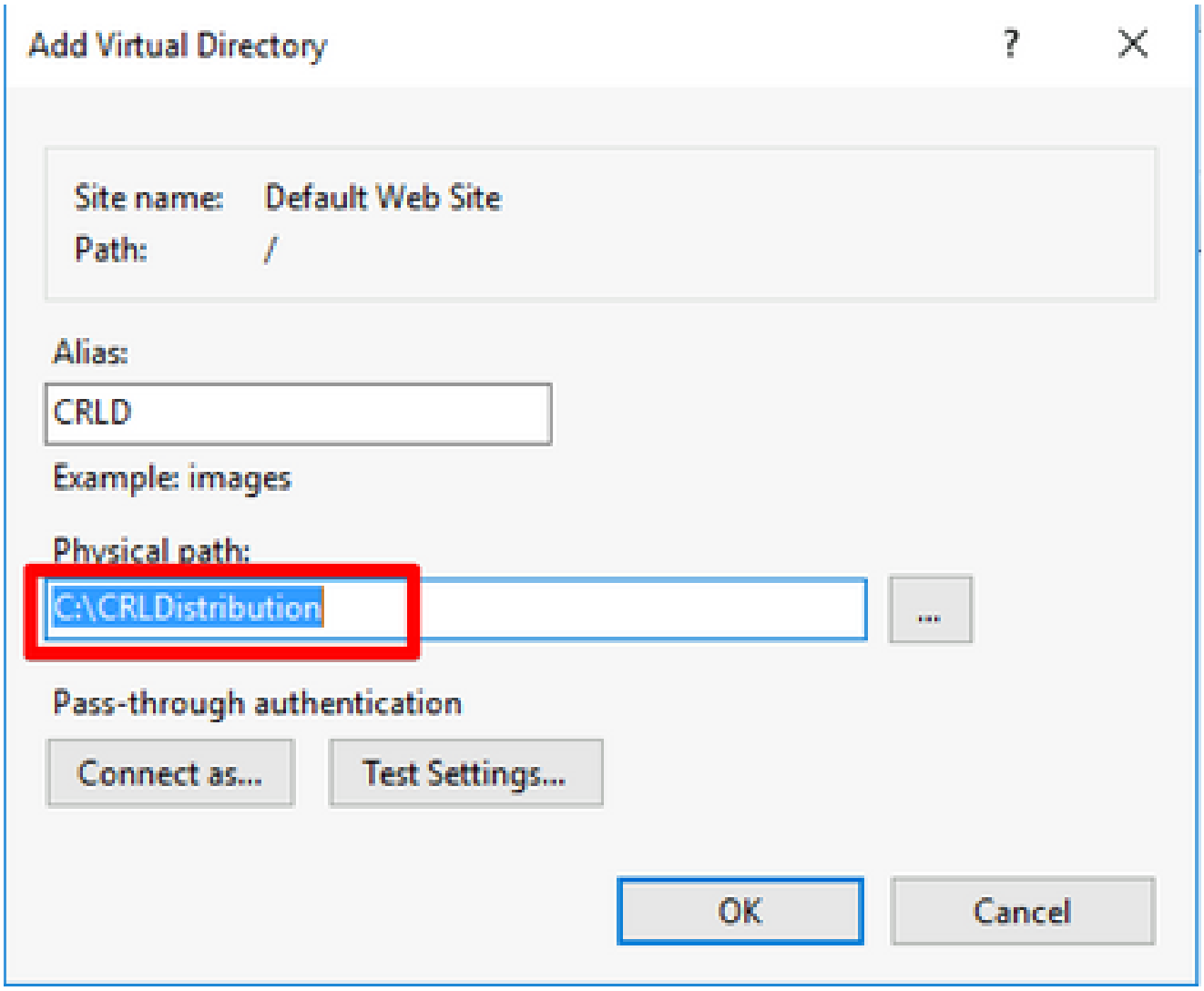

3. 右クリックDefault Web Siteし、次の図に示すようにAdd Virtual Directoryを選択します。



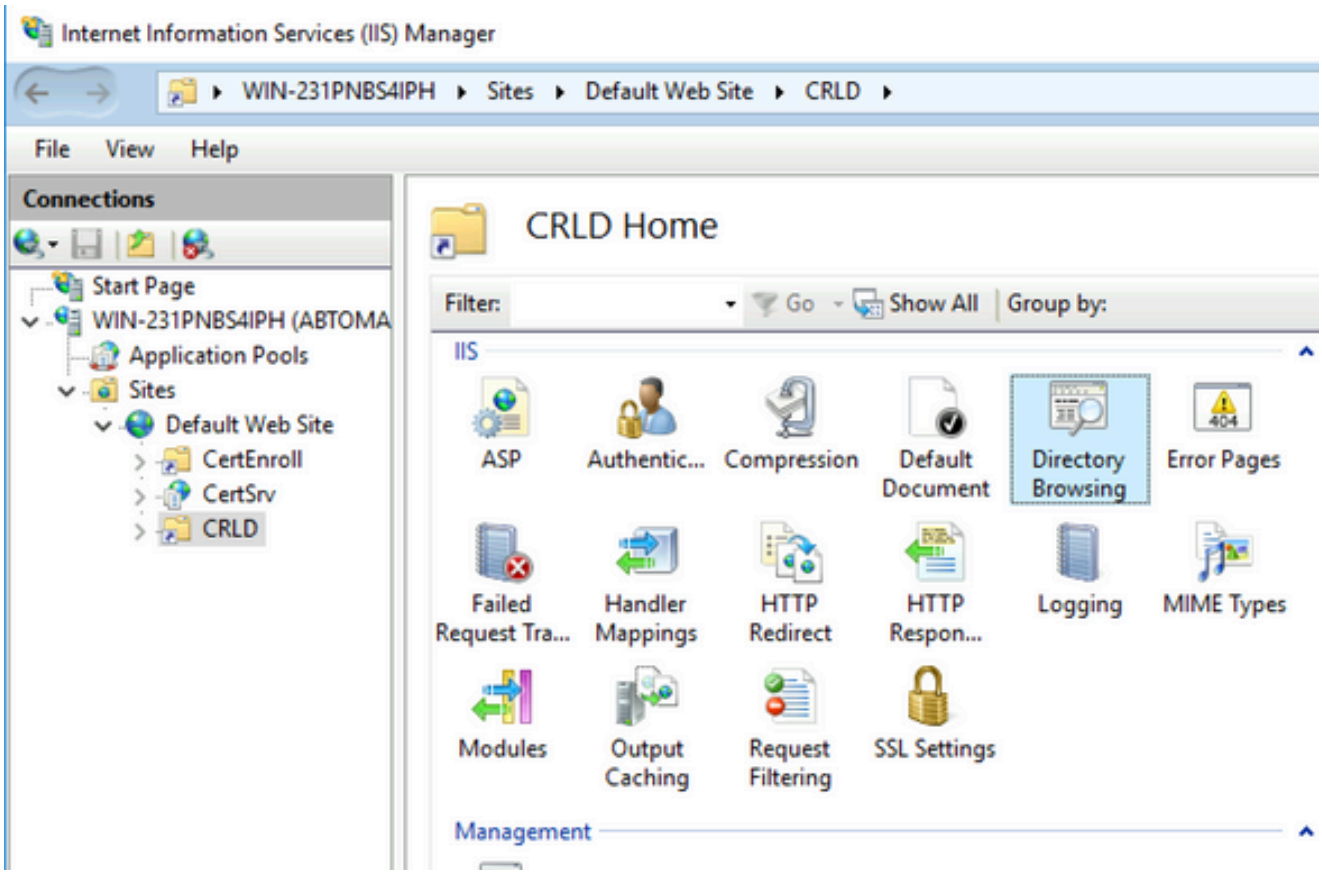

4. [Alias] フィールドに CRL 分散ポイントのサイト名を入力します。この例では、「CRLD」と入力されています。



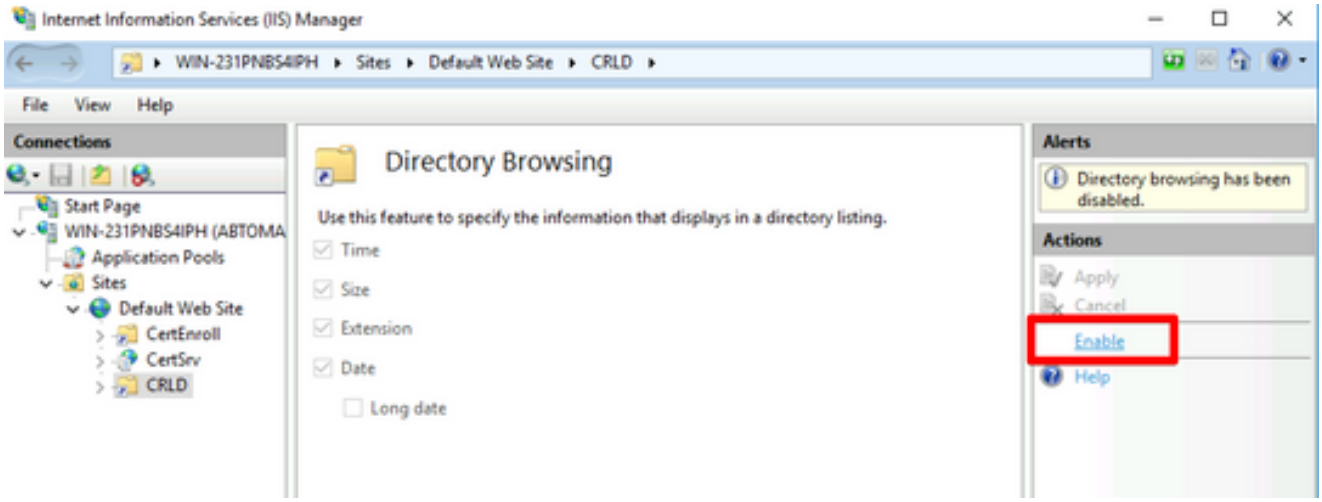

5. 省略記号(.)をクリックします。.) Physical pathフィールドの右側で、セクション1で作成したフォルダを参照します。フォルダを選択し、をクリックしOKます。をクリックOKして、Add Virtual Directoryウィンドウを閉じます。



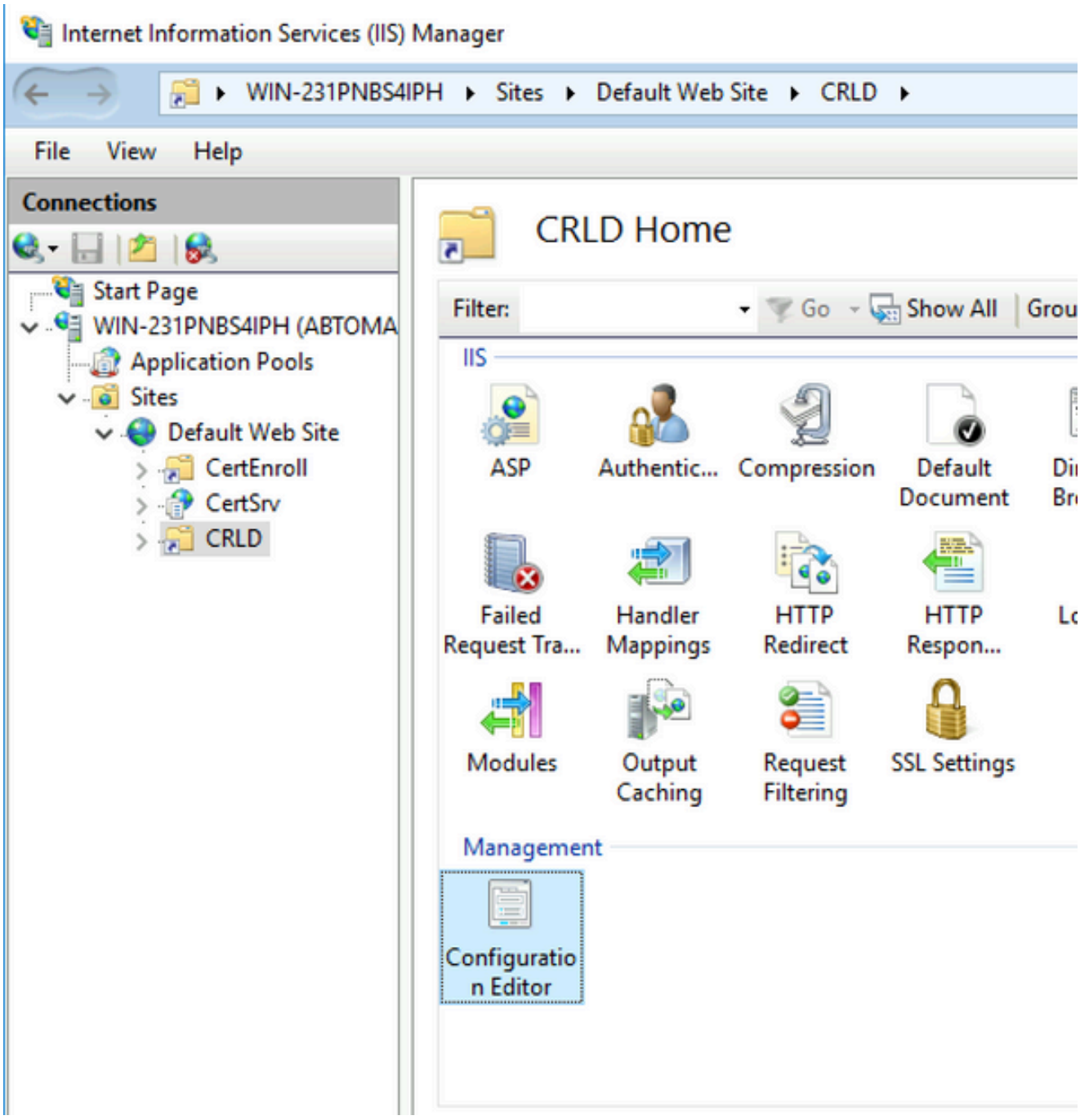

6. 手順4で入力したサイト名は、左側のペインで強調表示されている必要があります。強調表示されない場合は、ここで選択します。中央のペインで、をダブルクリックし**Directory Browsing**ます。



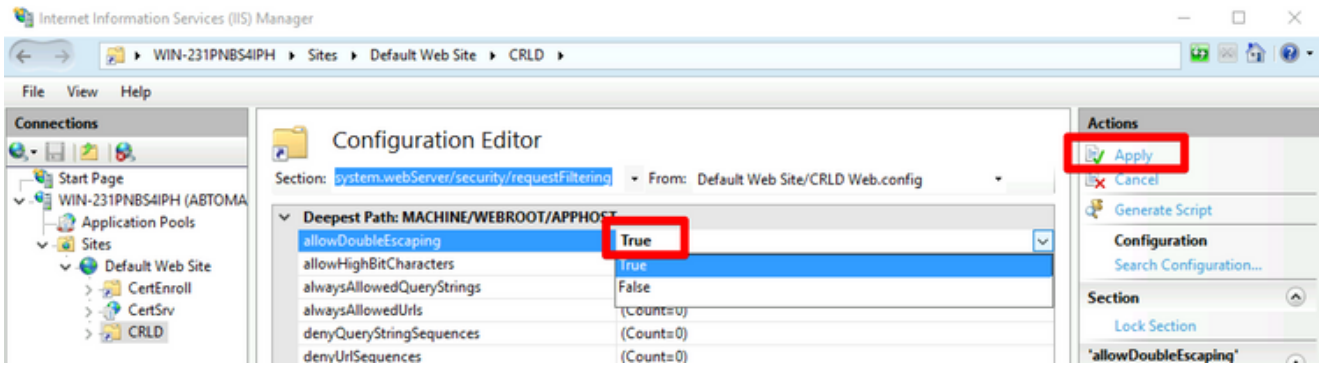

7. 右側のペインで、をクリックしてディレクトリ**Enable**の参照を有効にします。




8. 左側のペインで、サイト名を再び選択します。中央のペインで、をダブルクリックし**Configuration Editor**ます。




9. [断面]ドロップダウンリストで、を選択しsystem.webServer/security/requestFilteringます。ドロップダウallowDoubleEscapingンリストで、を選択しTrueます。右ペインで、次の図に示すようにApplyをクリックします。

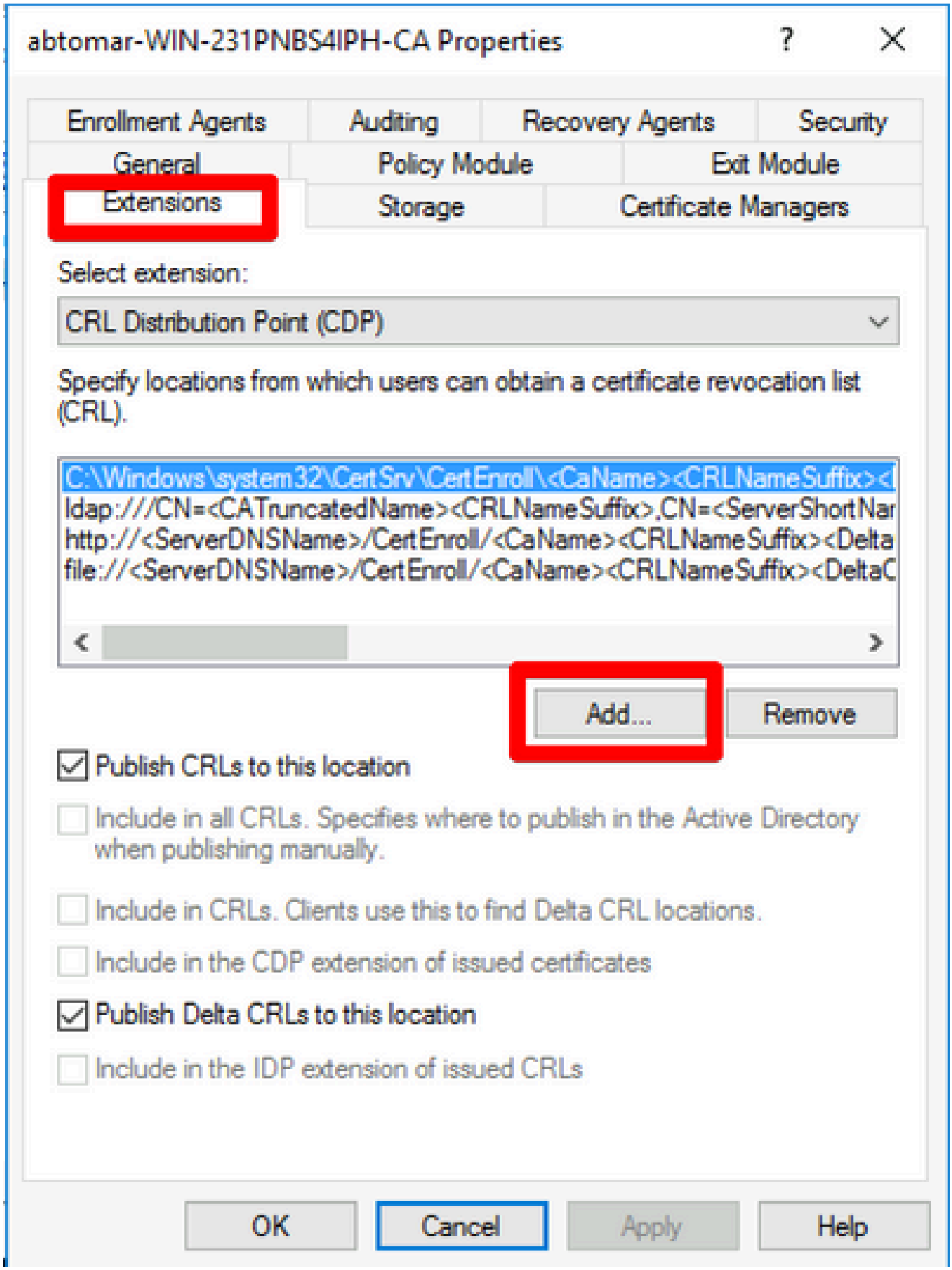


これで、フォルダはIISを介してアクセスできる必要があります。

## 配布ポイントにCRLファイルを発行するためのMicrosoft CAサーバの設定

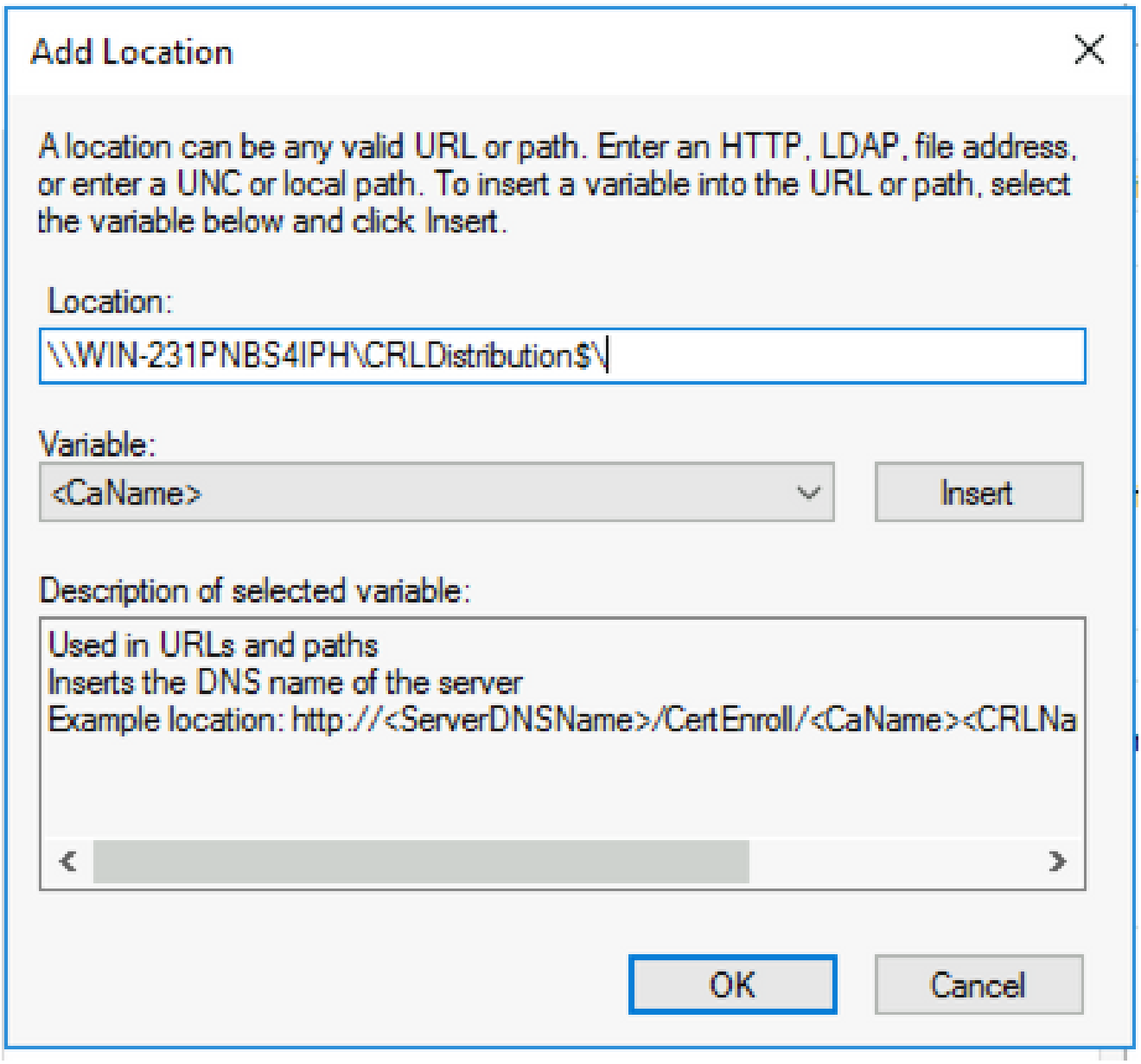
CRLファイルを格納するように新しいフォルダが設定され、そのフォルダがIISで公開されました。次に、CRLファイルを新しい場所に発行するようにMicrosoft CAサーバを設定します。

1. CAサーバのタスクバーで、をクリックし**Start**ます。選択.**Administrative Tools > Certificate Authority**
2. 左側のペインで、CA の名前を右クリックします。を選択**Properties**し、タ**Extensions**ブをクリックします。新しいCRL分散ポイントを追加するには、をクリックし**Add**ます。

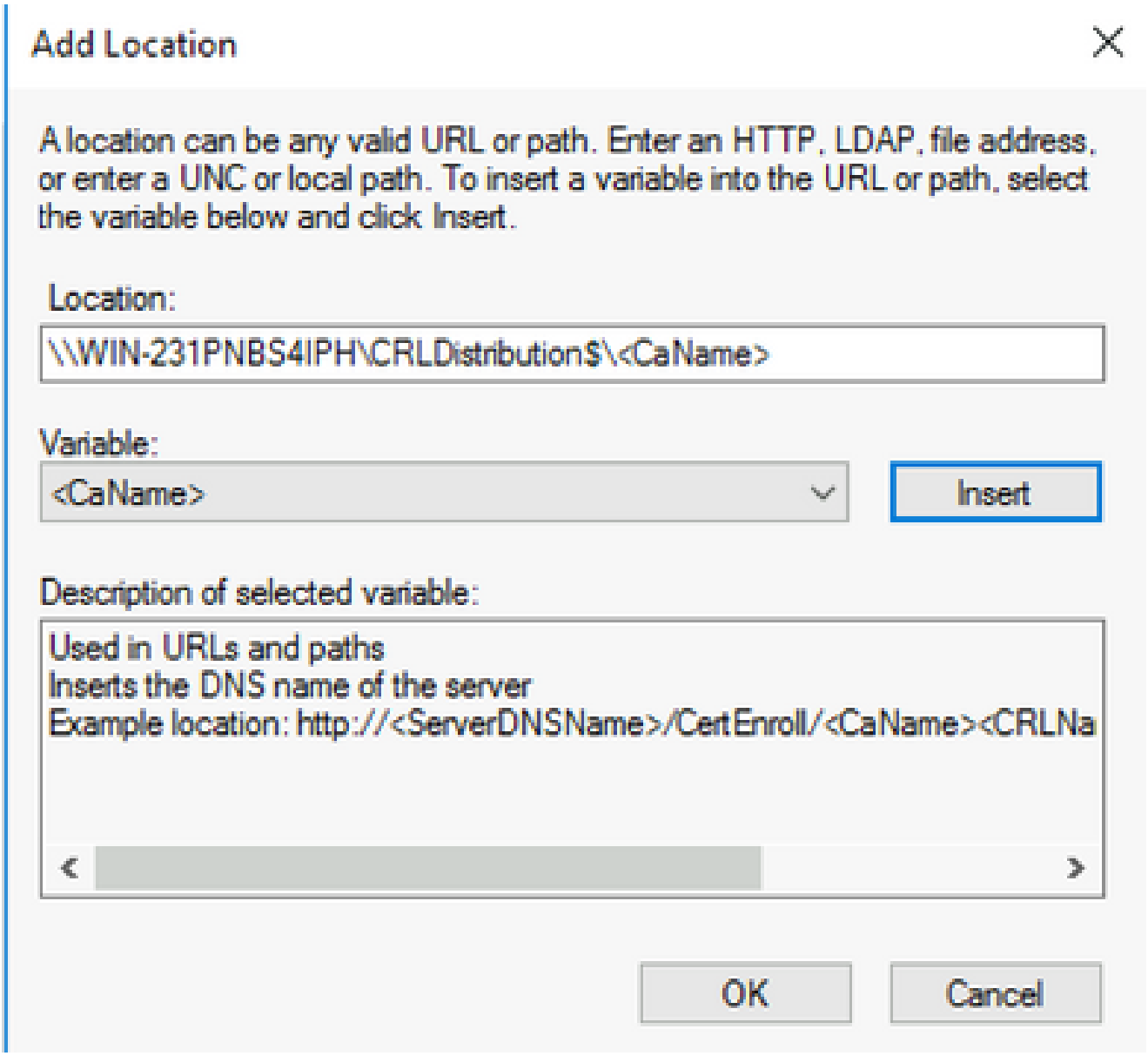



3. [Location] フィールドに、セクション 1 で作成して共有設定したフォルダのパスを入力します。セクション 1 の例では、パスは次のようになります。

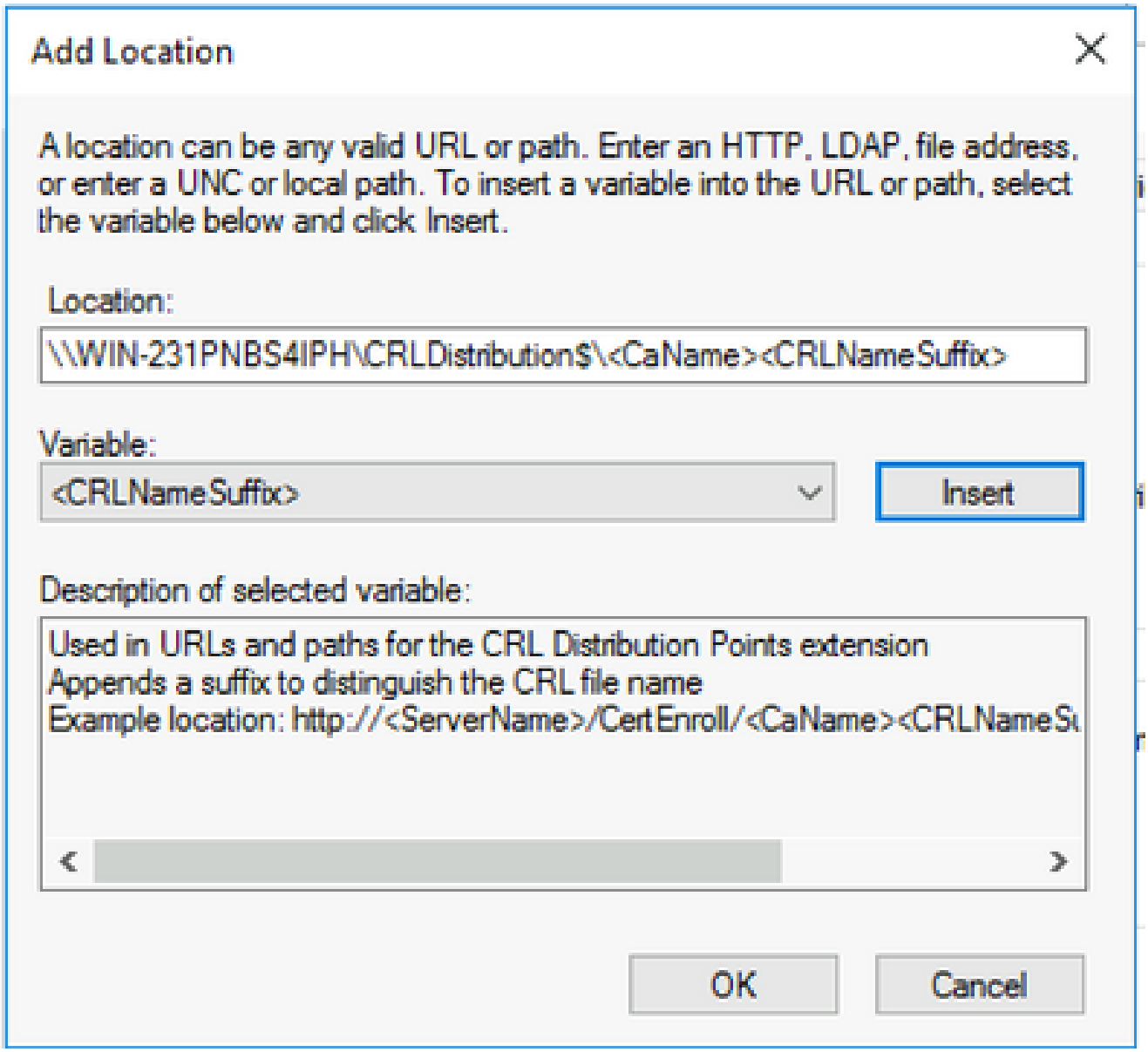
   \\WIN-231PNBS4IPH\CRLDistribution$




4. 「ロケーション」フィールドに値が入力された状態で、「変数」ドロップダウンリストから選択し、 **Insert.**




5. [変数]ドロップダウンリストから、を選択し、をクリックしInsertます。

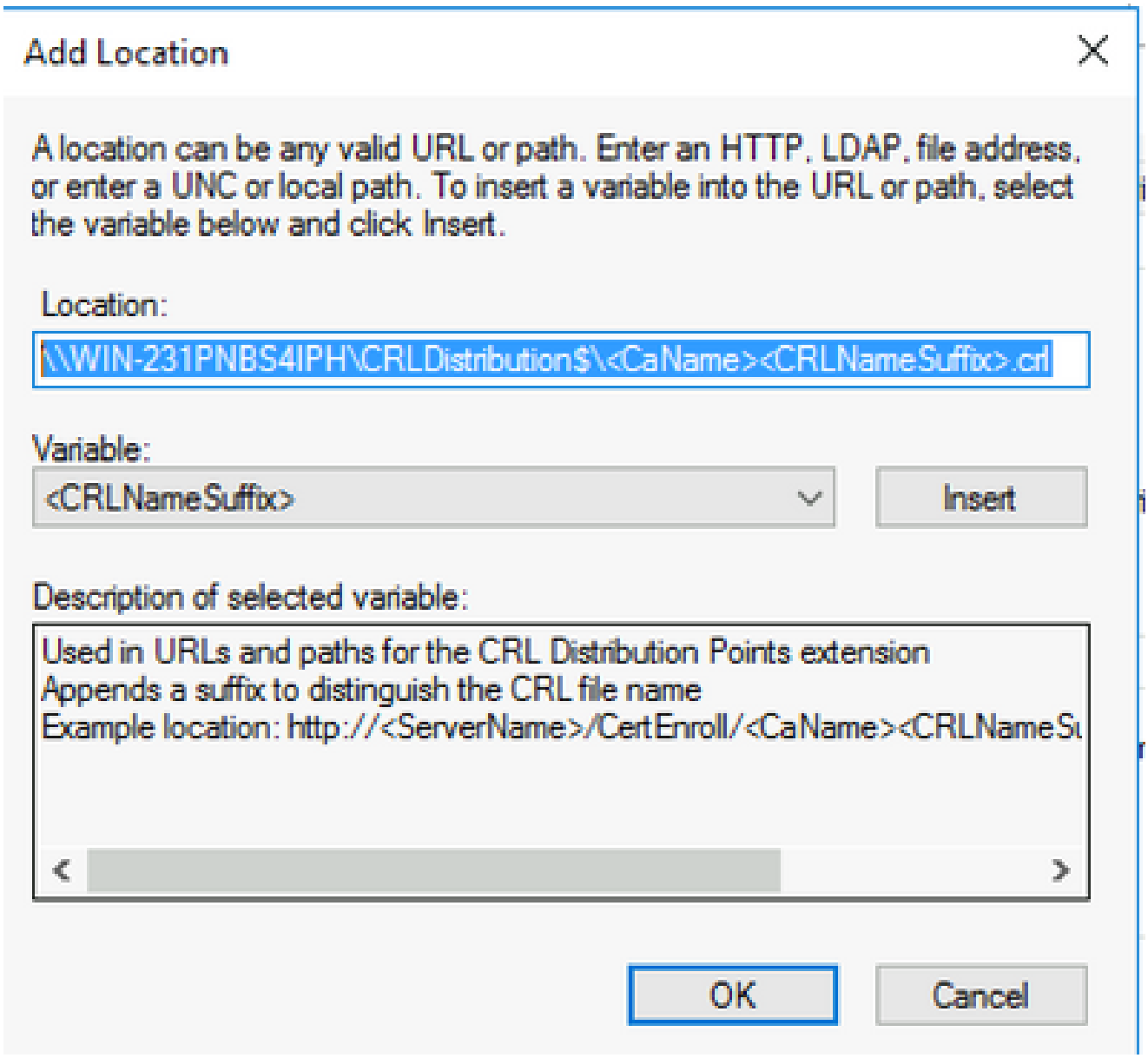



6. [場所]フィールドで、パス.crlの末尾に追加します。この例では、[Location] は次のようになります。

**\\WIN-231PNBS4IPH\CRLDistribution$**

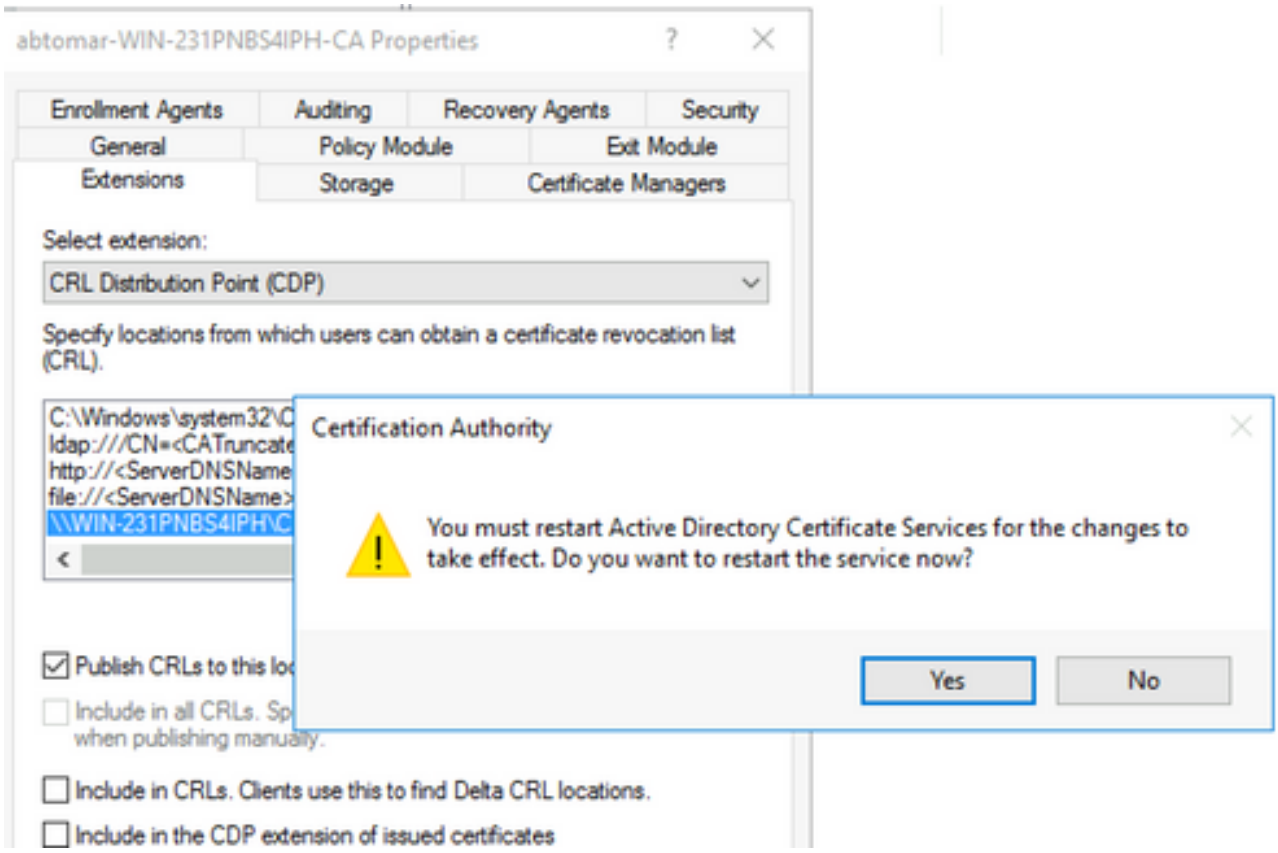
**<CaName><CRLNameSuffix>**

**.crl**

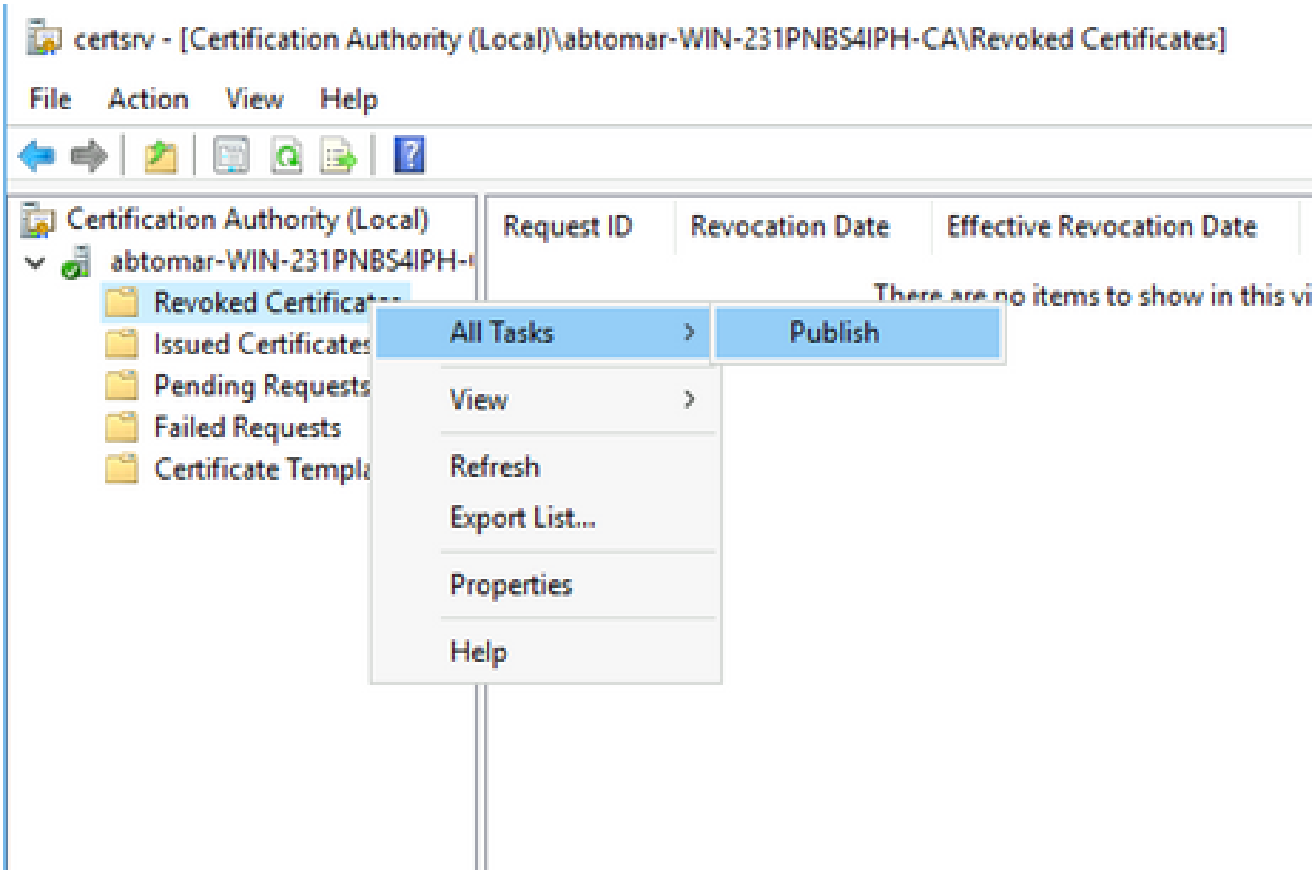



7. [拡張機能]タブOKに戻るには、をクリックします。チェックボックスをオンにしPublish CRLs to this location、をクリックして[プロパティ]ウィンドウOKを閉じます。

   Active Directory 証明書サービスを再開する許可を求めるメッセージが表示されます。をクリックします。Yes




8. 左ペインで右クリックし**Revoked Certificates**ます。選択.**All Tasks** > **Publish**New CRLが選択されていることを確認し、をクリックし**OK**ます。




Microsoft CAサーバは、セクション1で作成したフォルダに新しい.crlファイルを作成する必

要があります。新しい CRL ファイルが正常に作成された場合は、[OK] をクリックしてもダイアログは表示されません。新しい分散ポイント フォルダに関するエラーが返された場合は、このセクションの各ステップを慎重に繰り返してください。

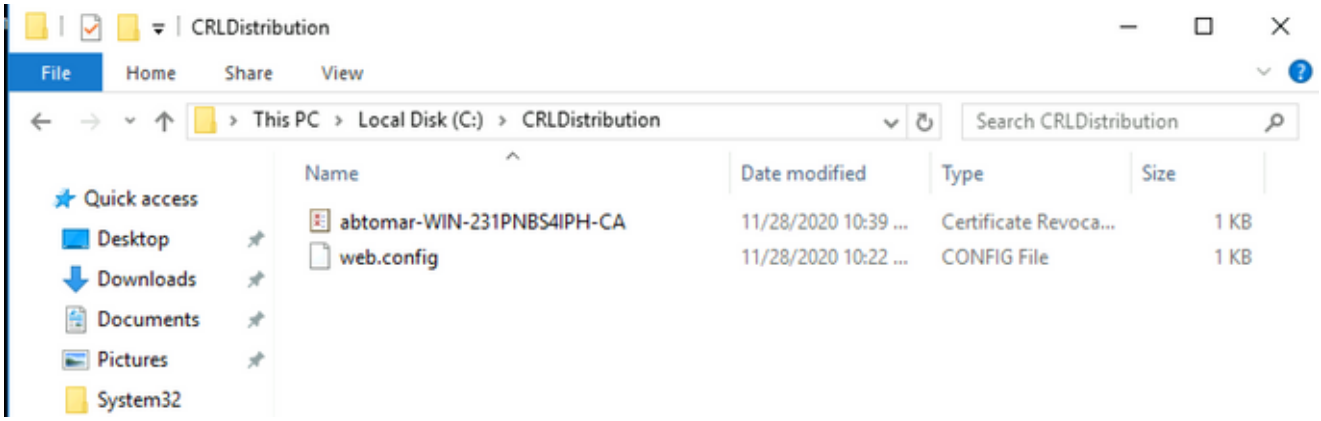
## CRLファイルが存在し、IISからアクセス可能であることを確認する

このセクションを開始する前に、新しい CRL ファイルが存在しており、そのファイルに IIS を介して別のワークステーションからアクセスできることを確認してください。

1. IIS サーバで、セクション 1 で作成したフォルダを開きます。という形式の.crlファイルが1つ存在している必要があります。

   **.crl**
   はCAサーバの名前
   です。この例では、ファイル名は次のとおりです。

   **abtomar-WIN-231PNBS4IPH-CA.crl**




2. ネットワーク上のワークステーション（理想的には、ISEプライマリ管理ノードと同じネットワーク上）でWebブラウザを開き、を参照します。は、セクション2で設定したIISサーバのサーバ名http://

   /

   で
   あり、はセクション2で配布ポイント用に選択したサイト名
   です。この例では、URL は次のとおりです。

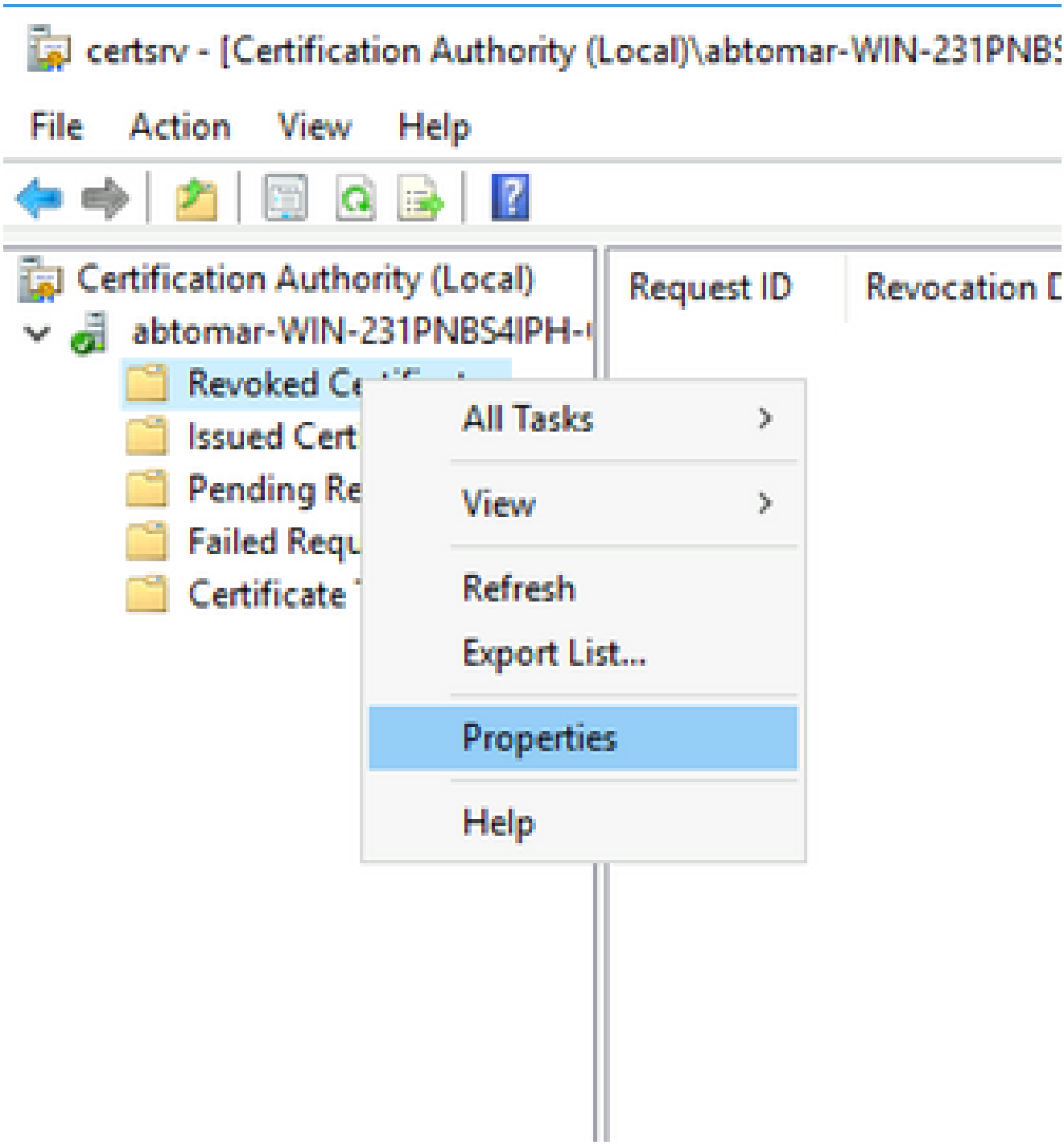
   **http://win-231pnbs4iph/CRLD**

   ステップ 1 で確認したファイルを含むディレクトリ インデックスが表示されます。


## 新しいCRL分散ポイントを使用するためのISEの設定

CRL を取得するように ISE を設定する前に、CRL を発行する間隔を定義します。この間隔を決定するための方策については、このドキュメントの範囲外です。（Microsoft CA の場合）有効な値は 1 時間 ~ 411 年です。デフォルト値は 1 週間です。環境に適した間隔を決定したら、以下の手順で間隔を設定します。

1. CAサーバのタスクバーで、をクリックしStartます。選択.Administrative Tools > Certificate Authority
2. 左側のペインで、CAを展開します。フォルダを右クリックしRevoked Certificatesて、を選択しPropertiesます。
3. [CRL publication interval] フィールドで、必要な数値を入力して期間単位を選択します。をクリックOKしてウィンドウを閉じ、変更を適用します。この例では、7日のパブリケーション間隔が設定されています。




4. ClockSkew値を確認する**certutil -getreg CA\Clock***コマンドを入力します。デフォルト値は 10 分です。

   出力例：

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

5. CRLOverlapPeriodが手動で設定されているかどうかを確認する**certutil -getreg CA\CRLov***コマンドを入力します。デフォルトでは、CRLOverlapUnit 値は 0 です。これは、値が手動で設定

されていないことを示しています。この値が 0 以外の場合は、その値と単位を記録します。

出力例：

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

6. ステップ3で設定したCRLPeriodを確認する**certutil -getreg CA\CRLpe***コマンドを入力します。

出力例：

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

7. 次のようにして、CRL の猶予期間を計算します。

a. CRLOverlapPeriodがステップ5で設定されている場合：OVERLAP = CRLOverlapPeriod（分）、

その他：OVERLAP = (CRLPeriod / 10)、単位：分

b. OVERLAP > 720の場合、OVERLAP = 720

c. OVERLAP < (1.5 * ClockSkewMinutes)の場合、OVERLAP = (1.5 * ClockSkewMinutes)になります。

d. OVERLAP > CRLPeriod（分）の場合、OVERLAP = CRLPeriod（分）

e.猶予期間= OVERLAP + ClockSkewMinutes

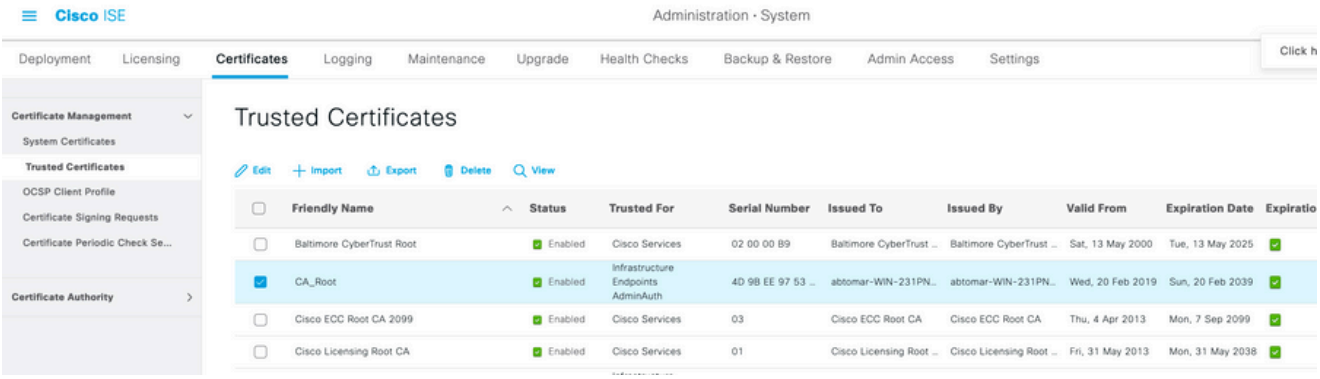
```
Example:

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
```

算出した猶予期間は、CA が次の CRL を発行する時点と現在の CRL が失効する時点との間の時間数です。状況に応じて CRL を取得するように ISE を設定する必要があります。

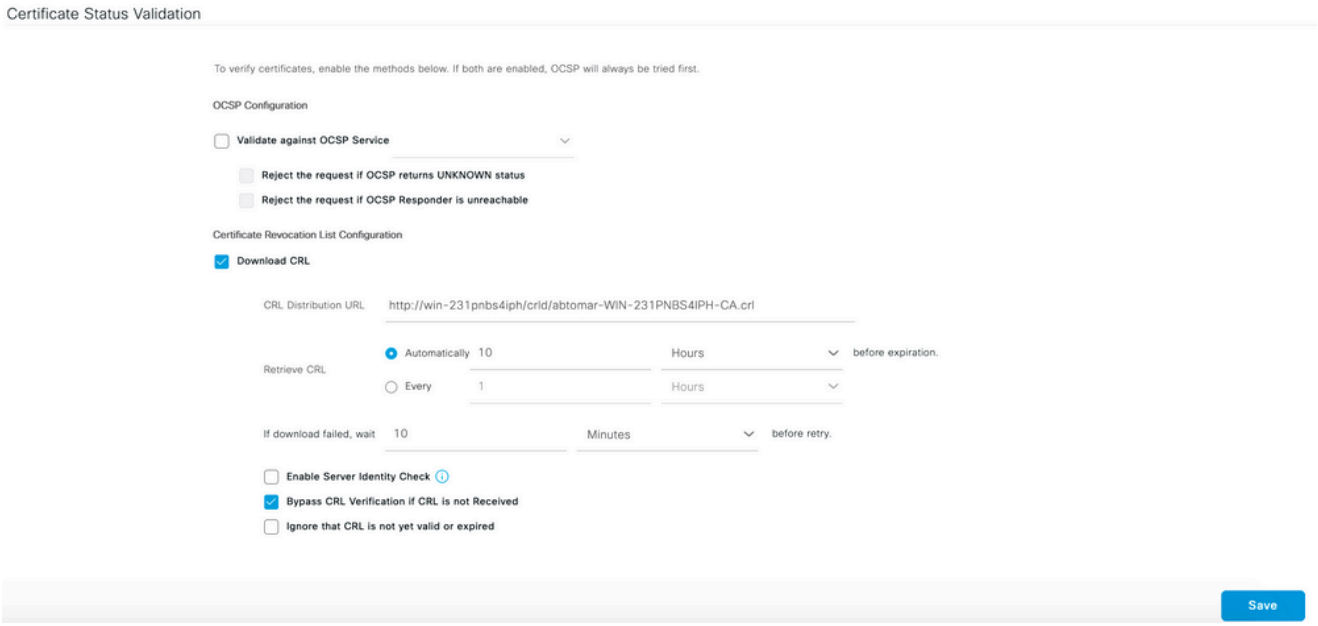
8. ISE Primary Adminノードにログインし、を選択しAdministration > System > Certificatesます。左側のペインで、を選択しTrusted Certificateます。




9. CRLを設定するCA証明書の横にあるチェックボックスをオンにします。をクリックします。Edit
10. ウィンドウの下部付近で、チェックボックスをオンにDownload CRLします。
11. [CRL Distribution URL] フィールドに、セクション 2 で作成した .crl ファイルが含まれている CRL 分散ポイントのパスを入力します。この例では、URL は次のとおりです。

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

12. 一定の間隔でまたは有効期限（通常は一定間隔）に基づいて CRL を取得するように、ISE を設定できます。CRL の発行間隔が固定されている場合は、後者のオプションのほうがタイムリーに CRL のアップデートを取得できます。オプションボタンをクAutomaticallyリックします。
13. 取得時間の値として、ステップ 7 で計算した猶予期間よりも小さい値を設定します。猶予期間よりも大きい値を設定すると、ISE は、CA が次の CRL を発行する前に CRL 分散ポイントをチェックしてしまいます。この例では、算出された猶予期間は 730 分、つまり 12 時間 10 分です。取得時間の値として 10 時間が使用されます。
14. 環境に応じた再試行間隔を設定します。前のステップで設定した間隔で CRL を取得できない場合、ISE はこの短い間隔で再試行します。
15. ISEが最後のダウンロード試行でこのCAのCRLを取得できなかった場合に、証明書ベースの認証を正常に（CRLチェックなしで）続行できるようにするには、このチェックボックスをBypass CRL Verification if CRL is not Receivedオンにします。このチェック ボックスをオンにしないと、CRL が取得できなかった場合に、この CA から発行された証明書による証明書ベースの認証がすべて失敗します。
16. ISEが期限切れIgnore that CRL is not yet valid or expired（またはまだ有効でない）CRLファイルを有効であるかのように使用できるようにするには、このチェックボックスをオンにします。このチェック ボックスをオンにしないと、ISE は [Effective Date] よりも前および [Next Update] の時間よりも後の CRL を無効と見なします。をクリックSaveして設定を完了します。




# 確認

現在、この設定に使用できる確認手順はありません。

# トラブルシュート

現在、この設定に関する特定のトラブルシューティング情報はありません。

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。