ISEの証明書失効リストを公開するための Microsoft CAサーバの設定

内容

[概要](#)
[前提条件](#)
[要件](#)
[使用するコンポーネント](#)
[設定](#)
[CRLファイルを格納するフォルダをCA上で作成および設定する](#)
[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](#)
[分散ポイントにCRLファイルを公開するためのMicrosoft CAサーバの設定](#)
[CRLファイルが存在し、IIS経由でアクセス可能であることを確認する](#)
[新しいCRL分散ポイントを使用するようにISEを設定します](#)

概要

このドキュメントでは、Internet Information Services(IIS)を実行して証明書失効リスト(CRL)の更新を公開するMicrosoft Certificate Authority(CA)サーバの設定について説明します。また、証明書検証で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特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、初期（デフォルト）設定の状態から起動しています。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

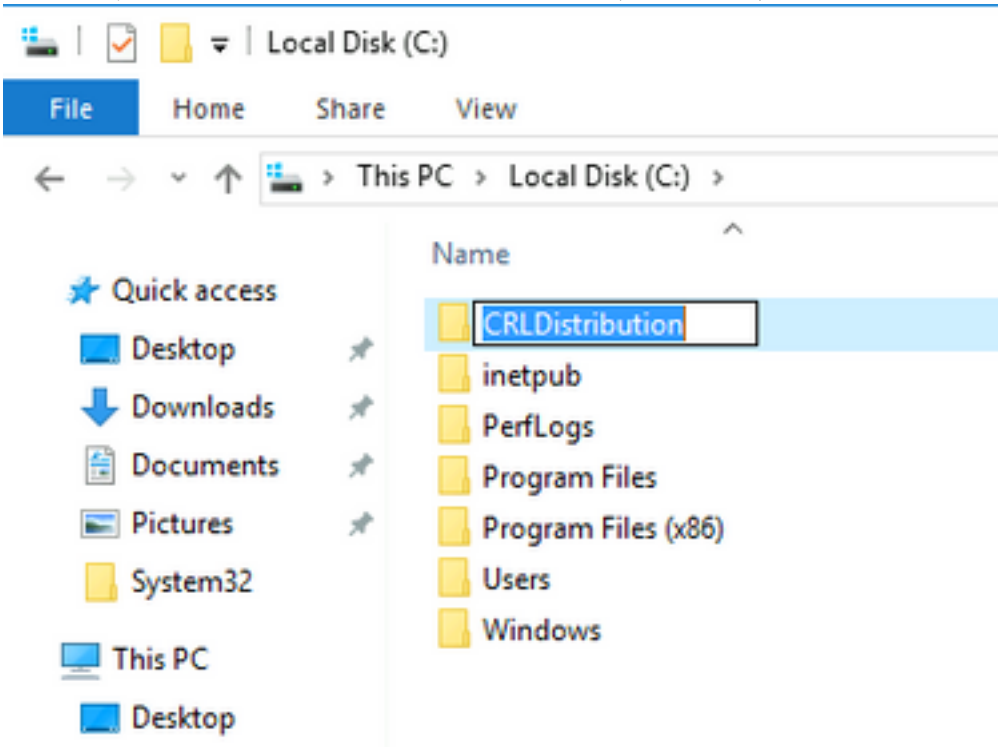
います。

CRLファイルを格納するフォルダをCA上で作成および設定する

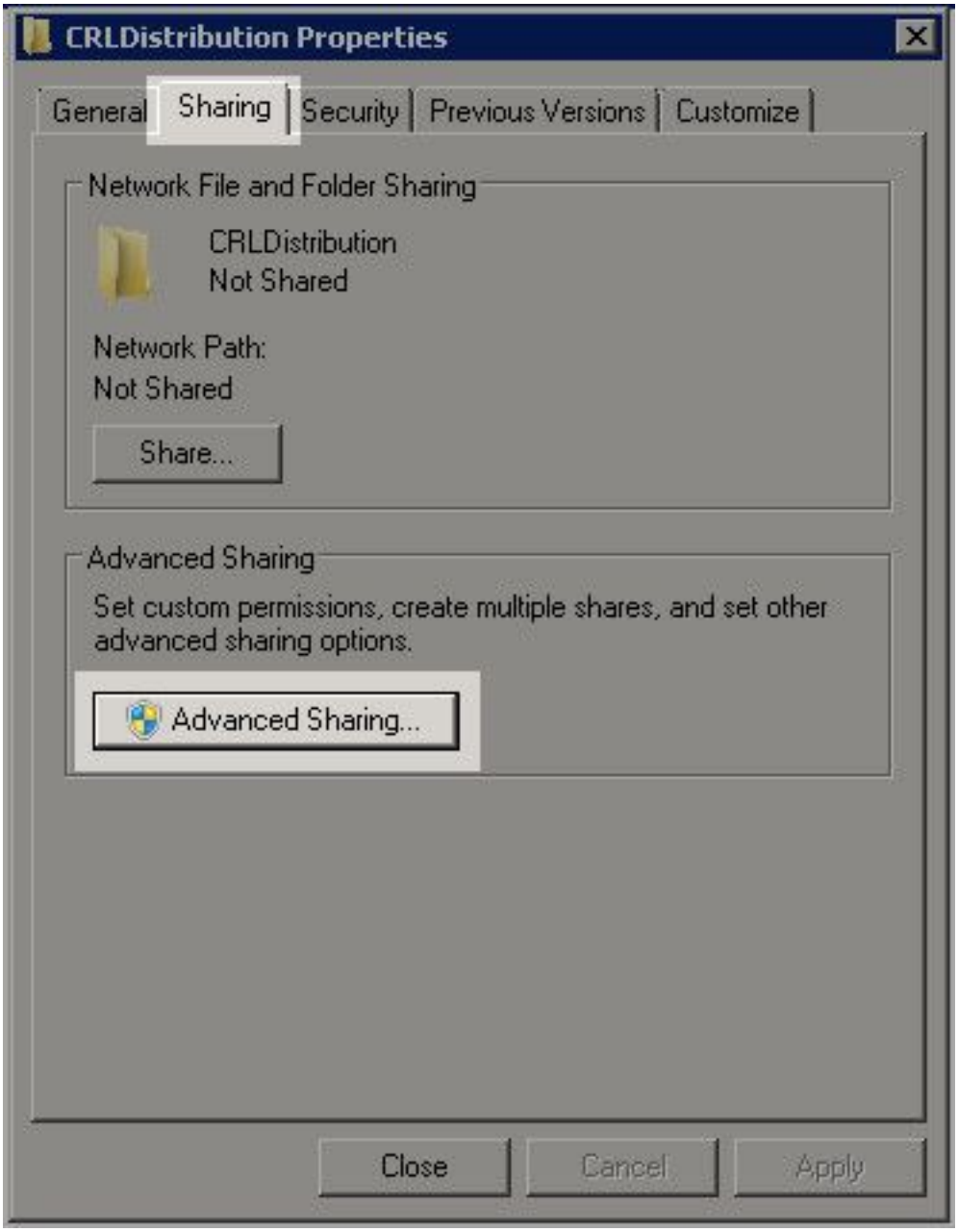
最初の作業は、CA サーバ上に CRL ファイルを保存する場所を設定することです。デフォルトでは、Microsoft CAサーバはファイルをC:\Windows\system32\CertSrv\CertEnroll\に発行**します**

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。

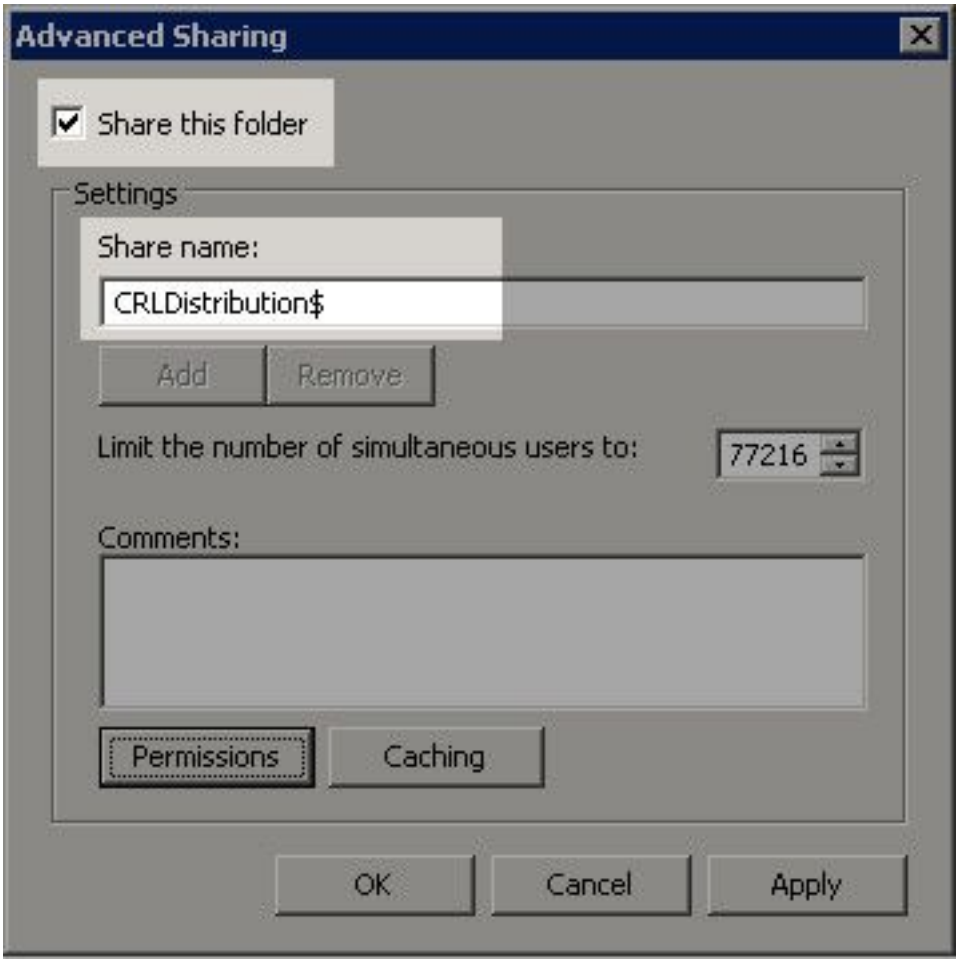
1. IISサーバで、ファイルシステム上の場所を選択し、新しいフォルダを作成します。この例では、フォルダ C:\CRLDistribution が作成されます。



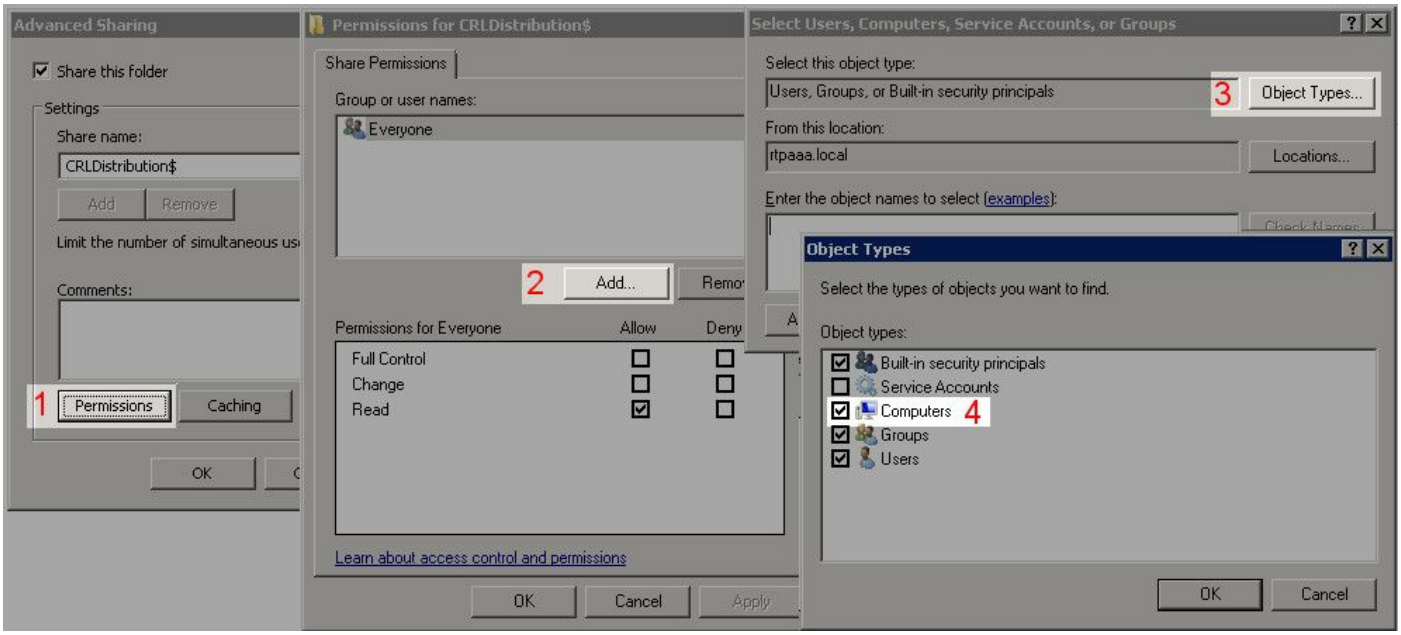
2. CAがCRLファイルを新しいフォルダに書き込むには、共有を有効にする必要があります。新しいフォルダを右クリックして [Properties] **を選択し、[Sharing]** タブをクリックしてから [Advanced Sharing] をクリックします。



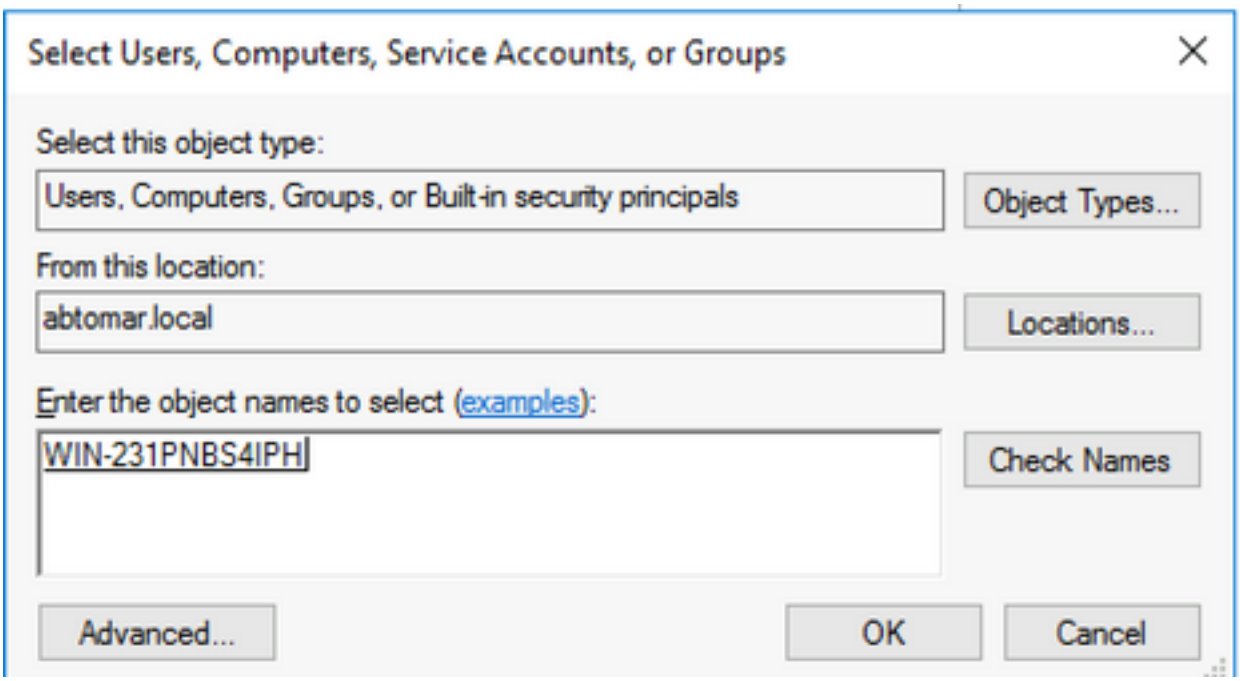
3.フォルダを共有するには、[このフォルダを共有する]チェックボックスをオンにして、[共有名]フィールドの共有名の最後にドル記号($)を追加して共有を非表示にします。



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

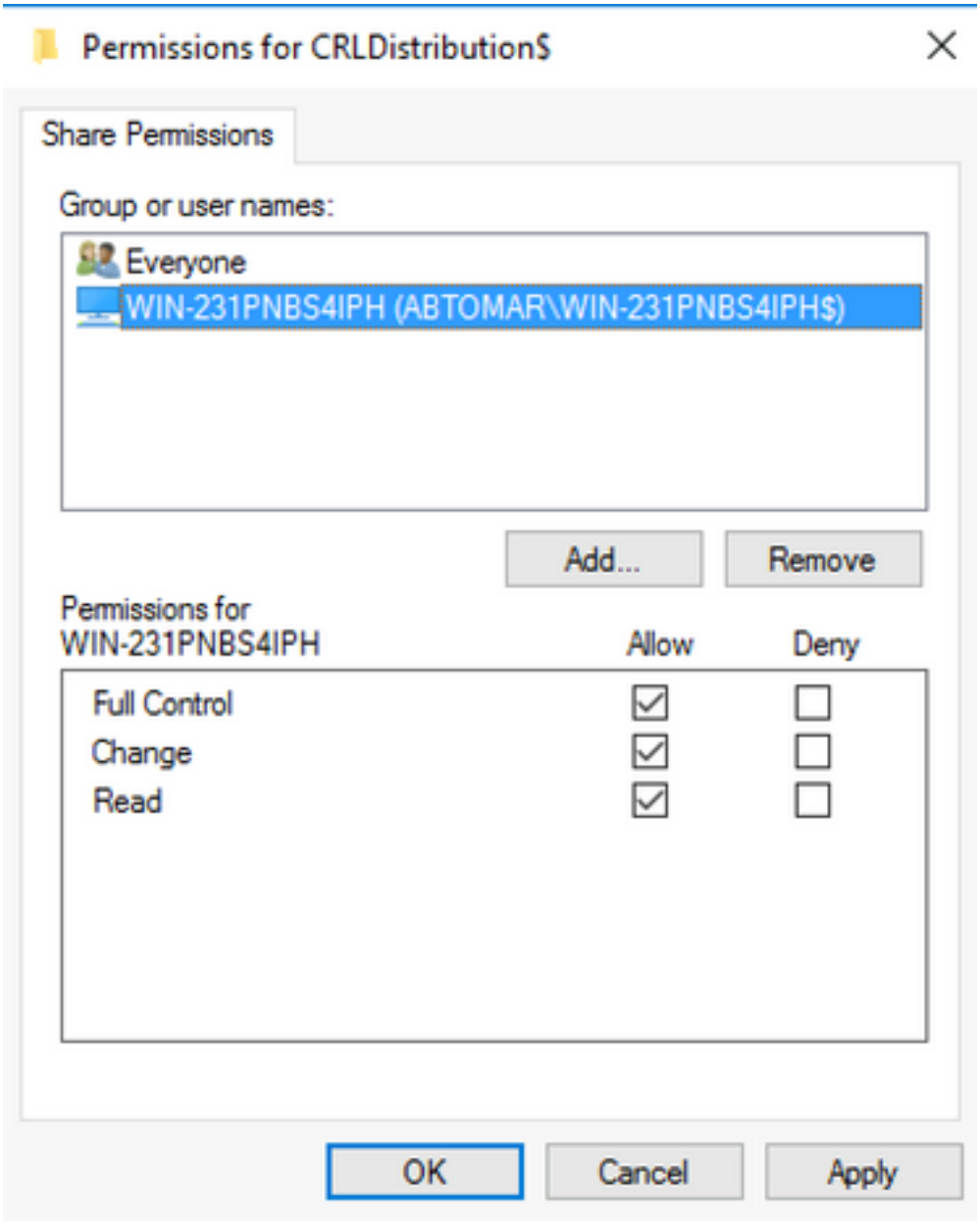


5. [OK] をクリックして、[Select Users, Computers, Service Accounts, or Groups] ウィンドウに戻ります。[Enter the object names to select]フィールドに、この例のCAサーバのコンピュータ名を入力します。WIN0231PNBS4IPHを選択し、[名前の確認]をクリックします。入力された名前が有効な場合は、名前が更新されて下線が付きます。[OK] をクリックします。



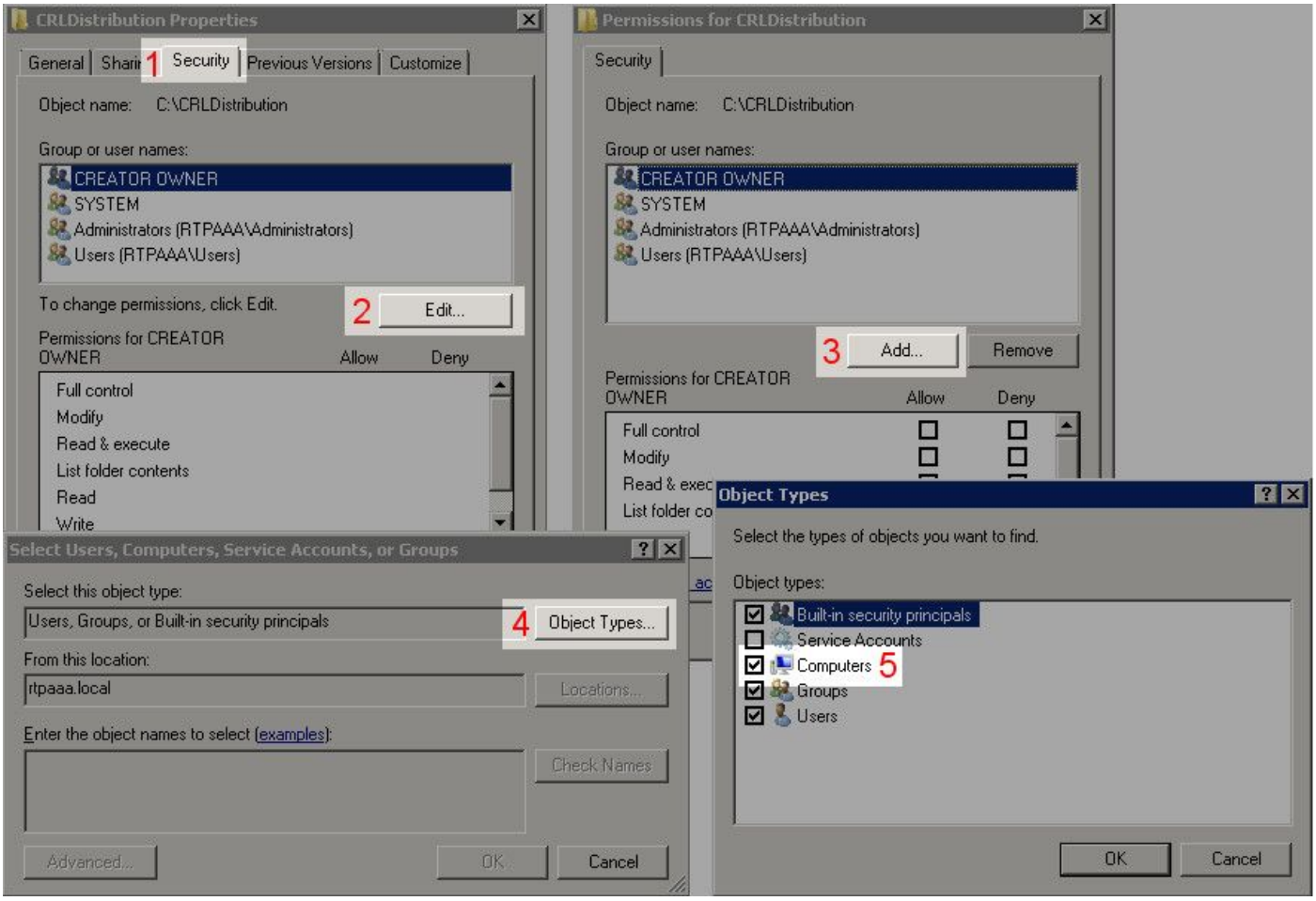
6. [Group or user names] フィールドで CA コンピュータを選択します。CAへのフルアクセスを許可するには、[Full Control]の[Allow]をオンにします。

[OK] をクリックします。[OK] を再度クリックして [Advanced Sharing] ウィンドウを閉じ、[Properties] ウィンドウに戻ります。

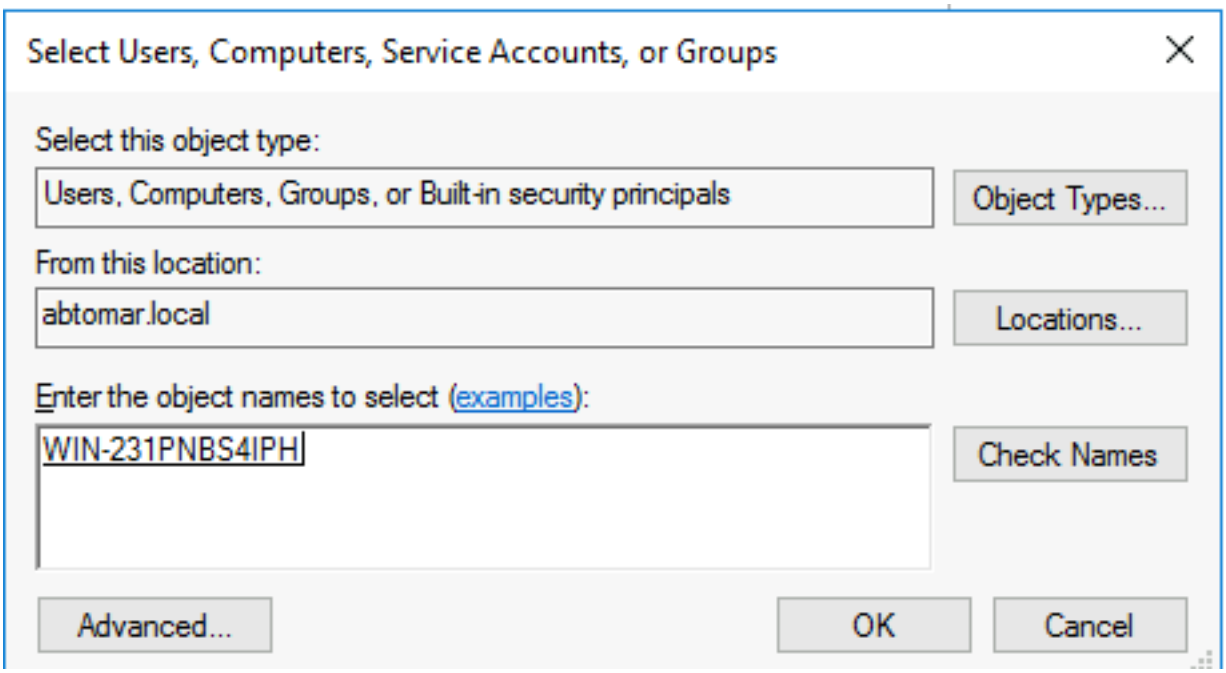


---

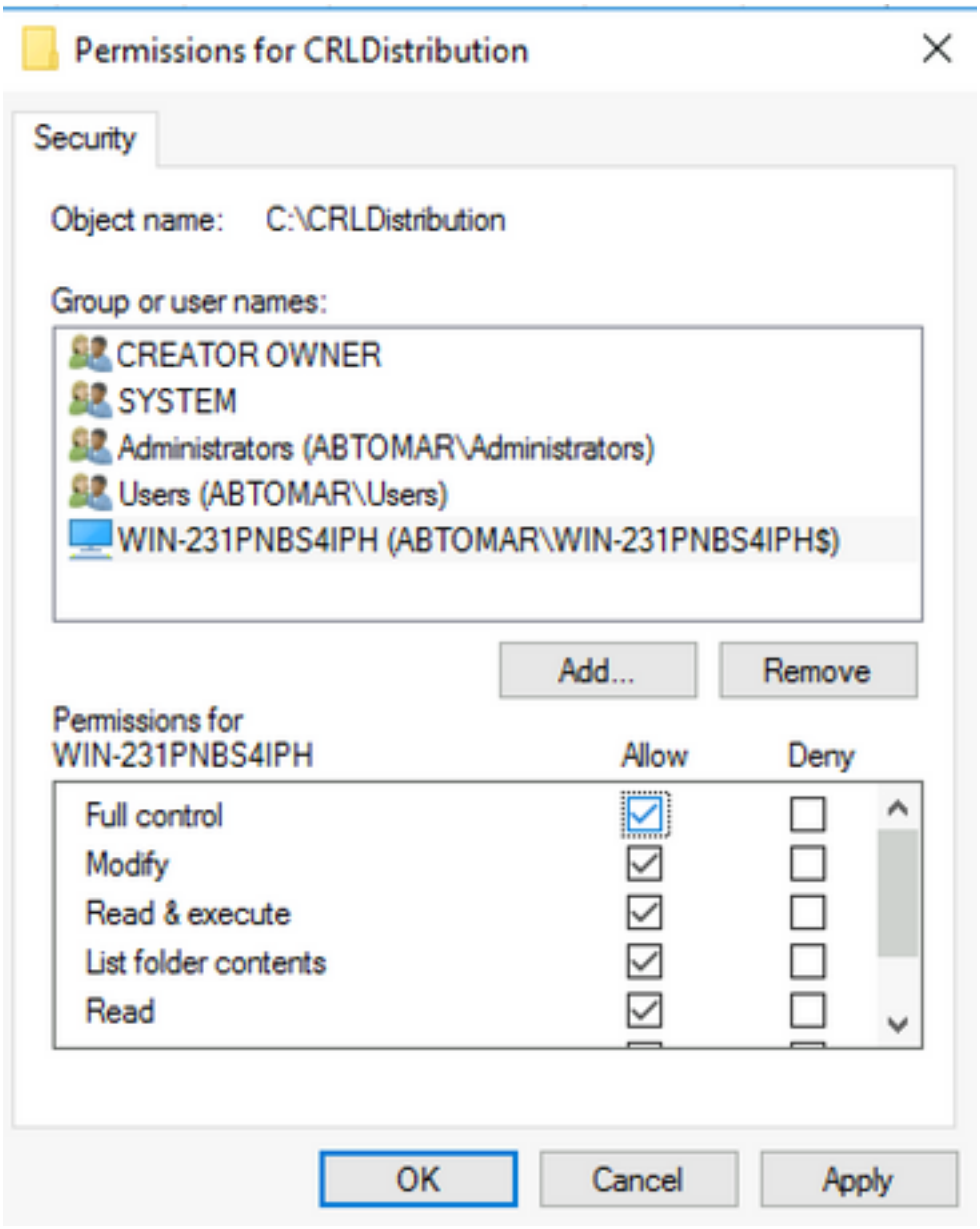
7. CAがCRLファイルを新しいフォルダに書き込むようにするには、適切なセキュリティ権限を設定します。[Security] **タブをクリックし（1）、[Edit]** をクリックして（2）、[Add] をクリックしてから（3）、[Object Types] **をクリックして（4）、[Computers] チェック ボックスをオンにします（5）。**



8. [Enter the object names to select]フィールドで、CAサーバのコンピュータ名を入力し、**[Check Names]をクリックします。**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。[OK] をクリックします。



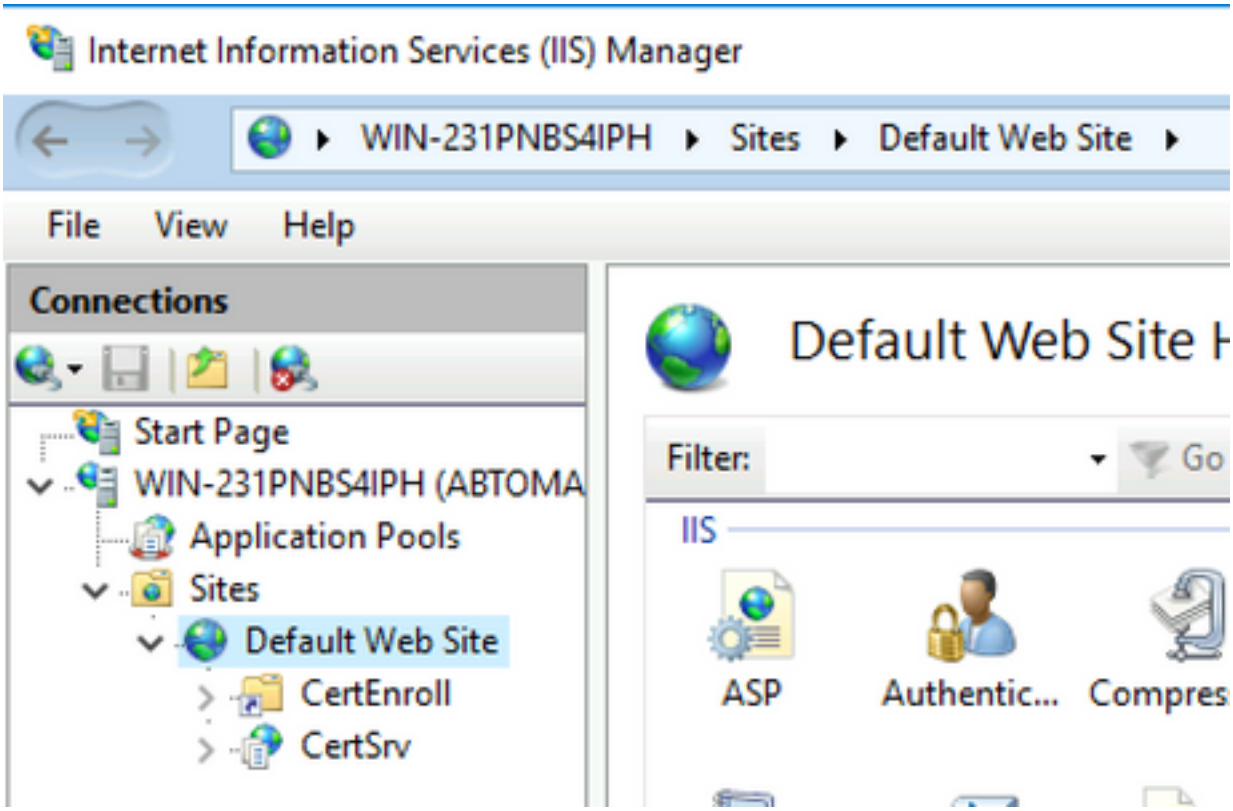
9. [Group or user names]フィールドでCAコンピュータを選択し、[Allow for Full control]をオンにしてCAへのフルアクセスを許可します。**[OK]をクリックし、[閉じる]をクリックして**タスクを完了します。



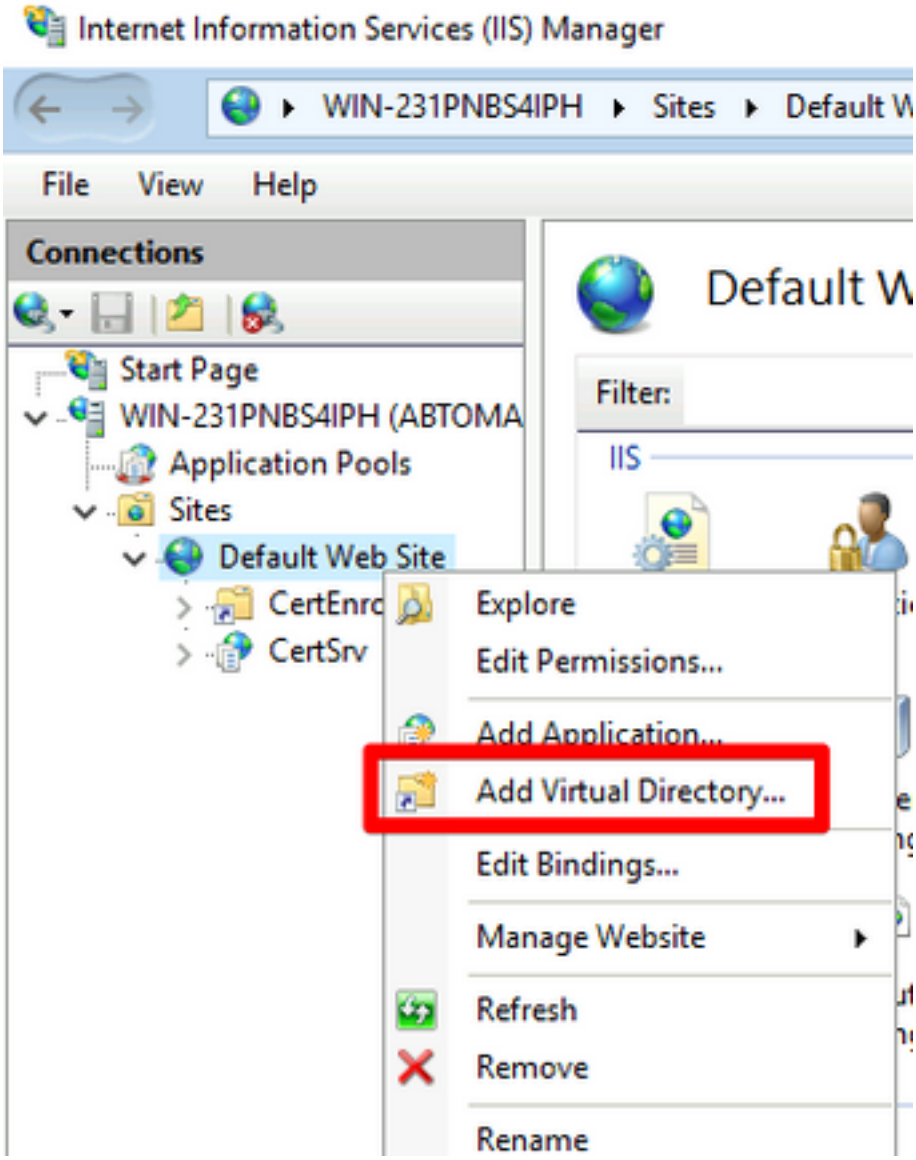
新しいCRL分散ポイントを公開するサイトをIISに作成する

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。

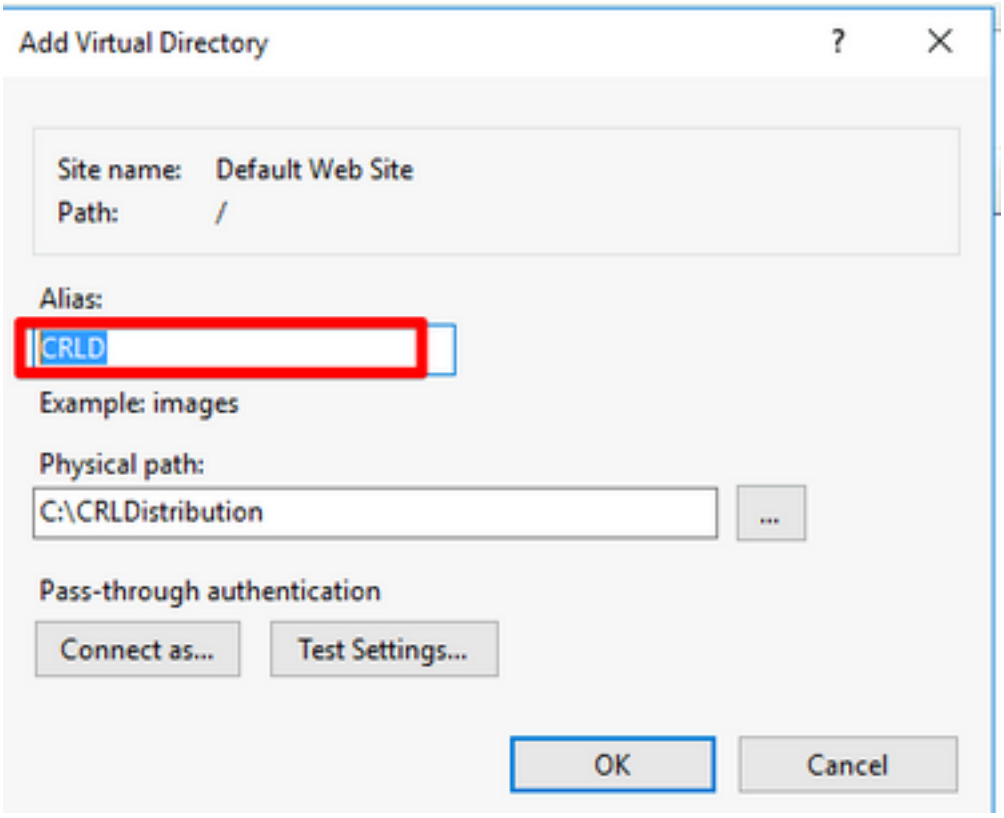
1. IIS サーバのタスクバーで、[Start] をクリックします。[Administrative Tools] > [Internet Information Services (IIS) Manager] を選択します。
2. 左側のペイン（コンソール ツリー）で、IIS のサーバ名を展開し、次に [Sites] **を展開します**。



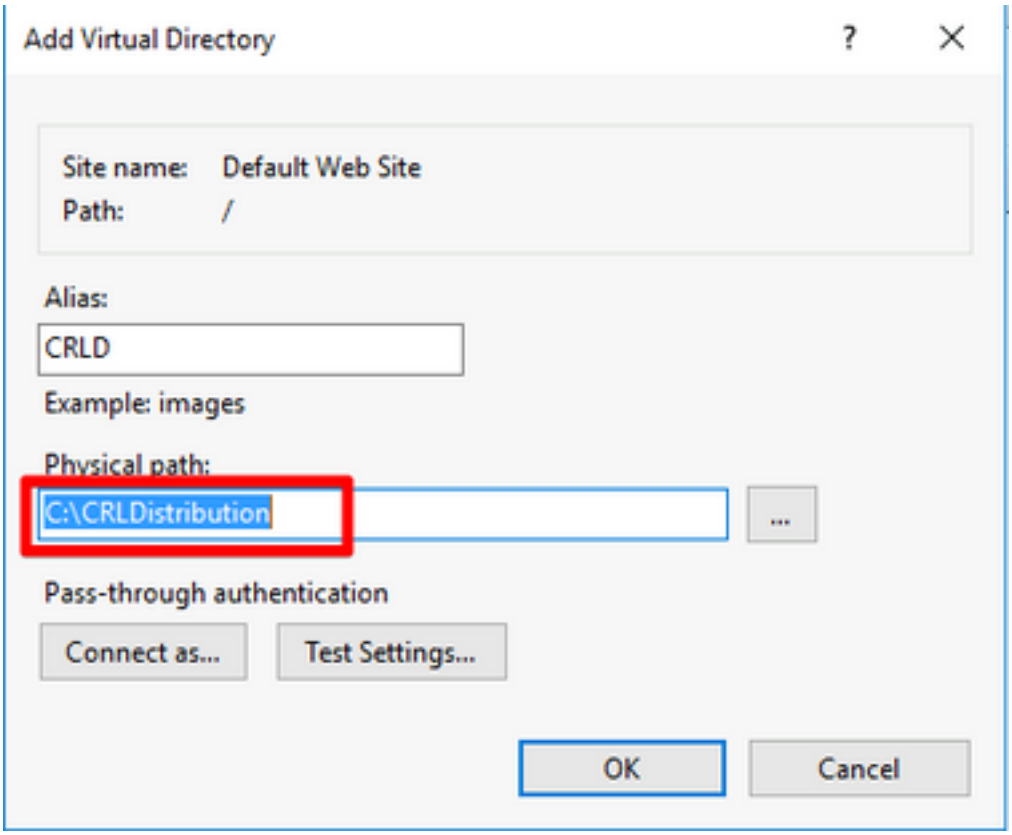
3.次の図に示すように、**[Default Web Site]を右クリックし、[Add Virtual Directory]**を選択します。



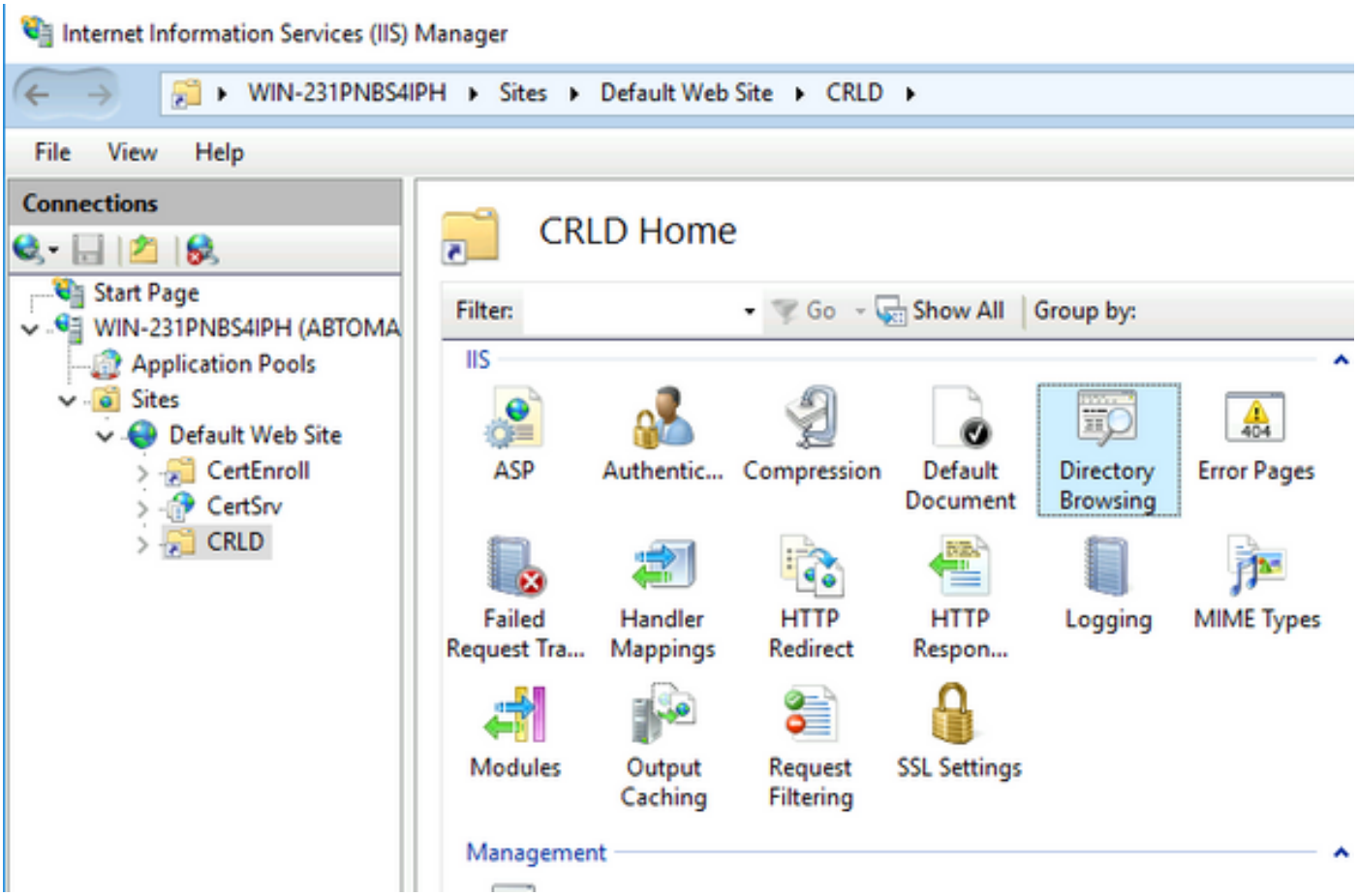
4. [Alias]フィールドに、CRL分散ポイントのサイト名を入力します。この例では、「CRLD」と入力されています。



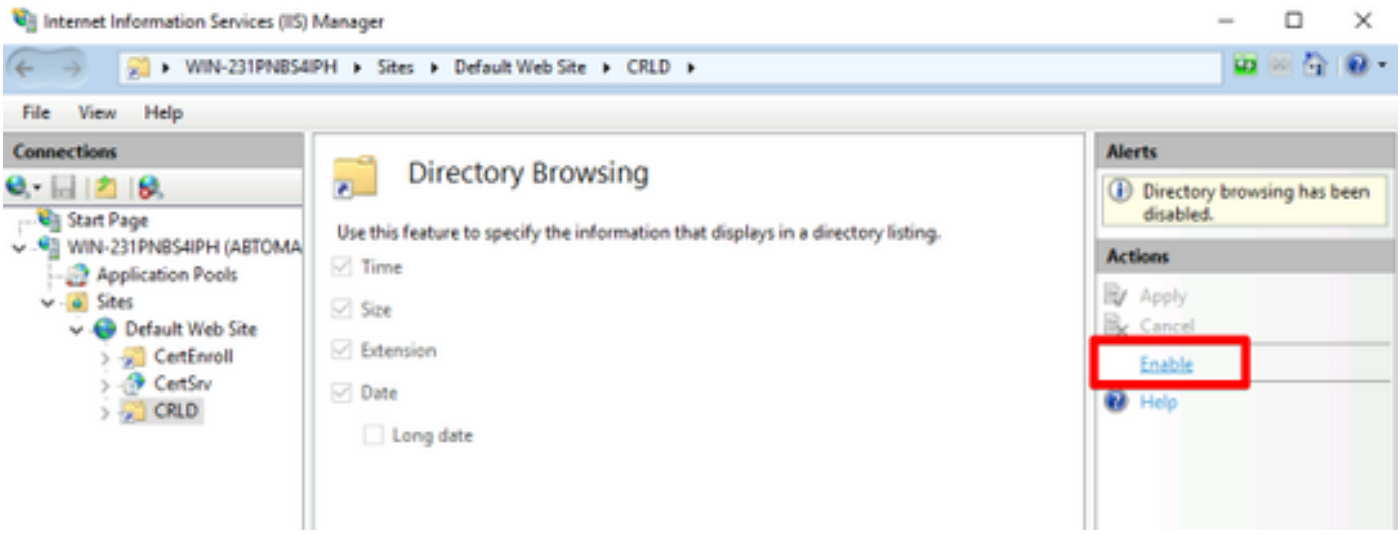
5.省略記号(...)[物理パス]フィールドの右側で、セクション1で作成したフォルダを参照します。フォルダを選択し、[OK]をクリックします。[OK] をクリックして [Add Virtual Directory] ウィンドウを閉じます。



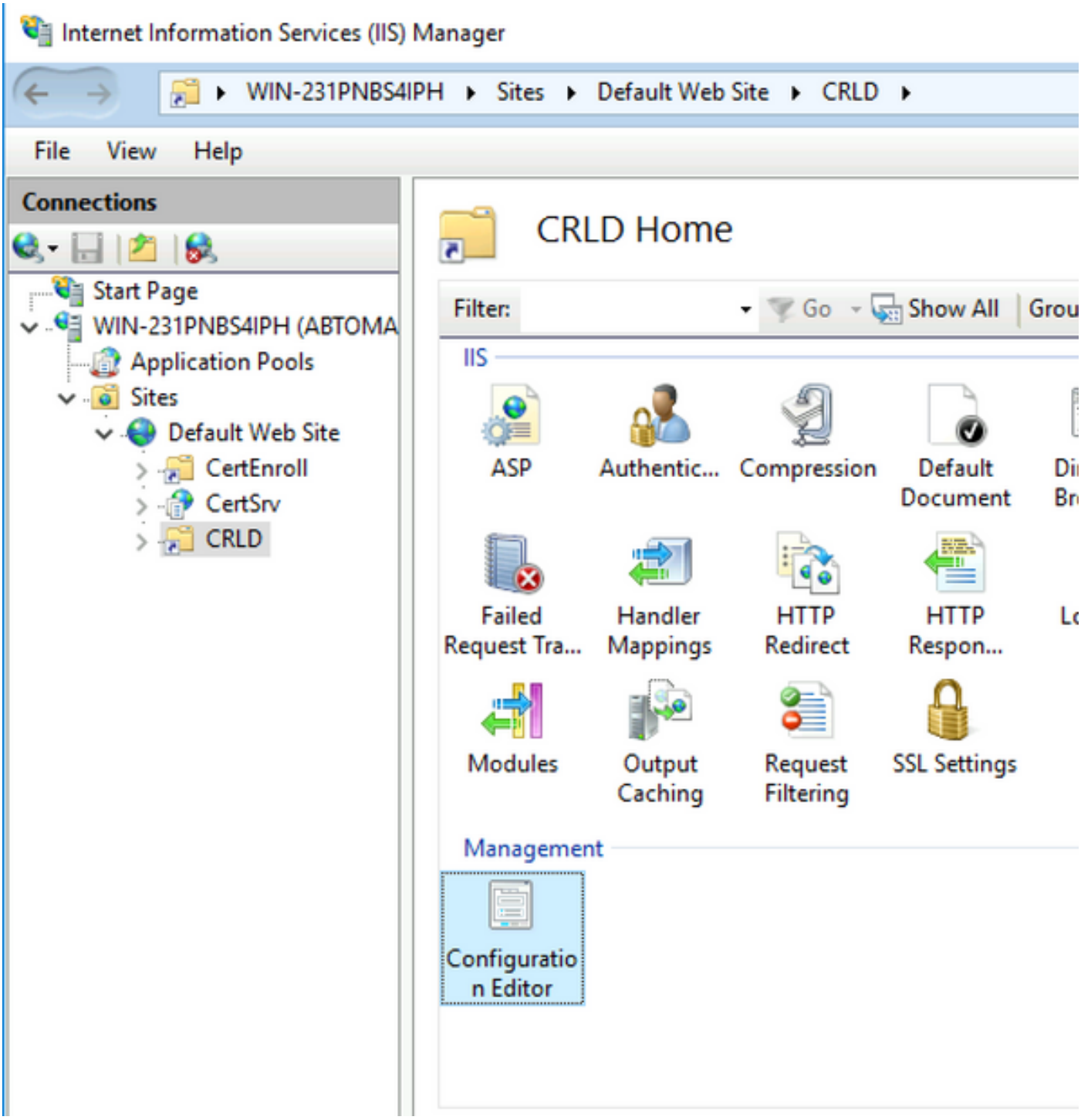
6.手順4で入力したサイト名は、左側のペインで強調表示する必要があります。強調表示されない場合は、ここで選択します。中央のペインで、[Directory Browsing] をダブルクリックします。



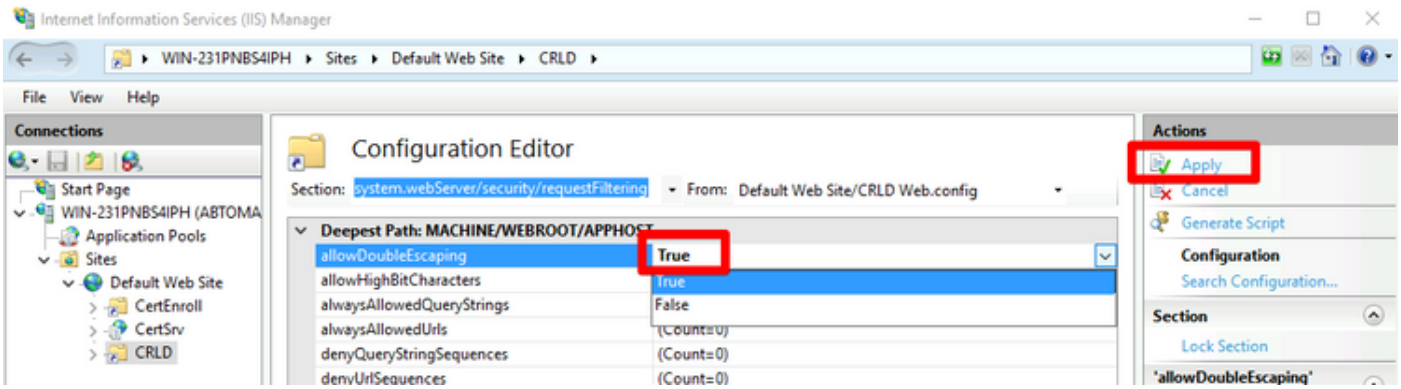
7.右側のペインで**Enable**をクリックして、ディレクトリの参照を有効にします。



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



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

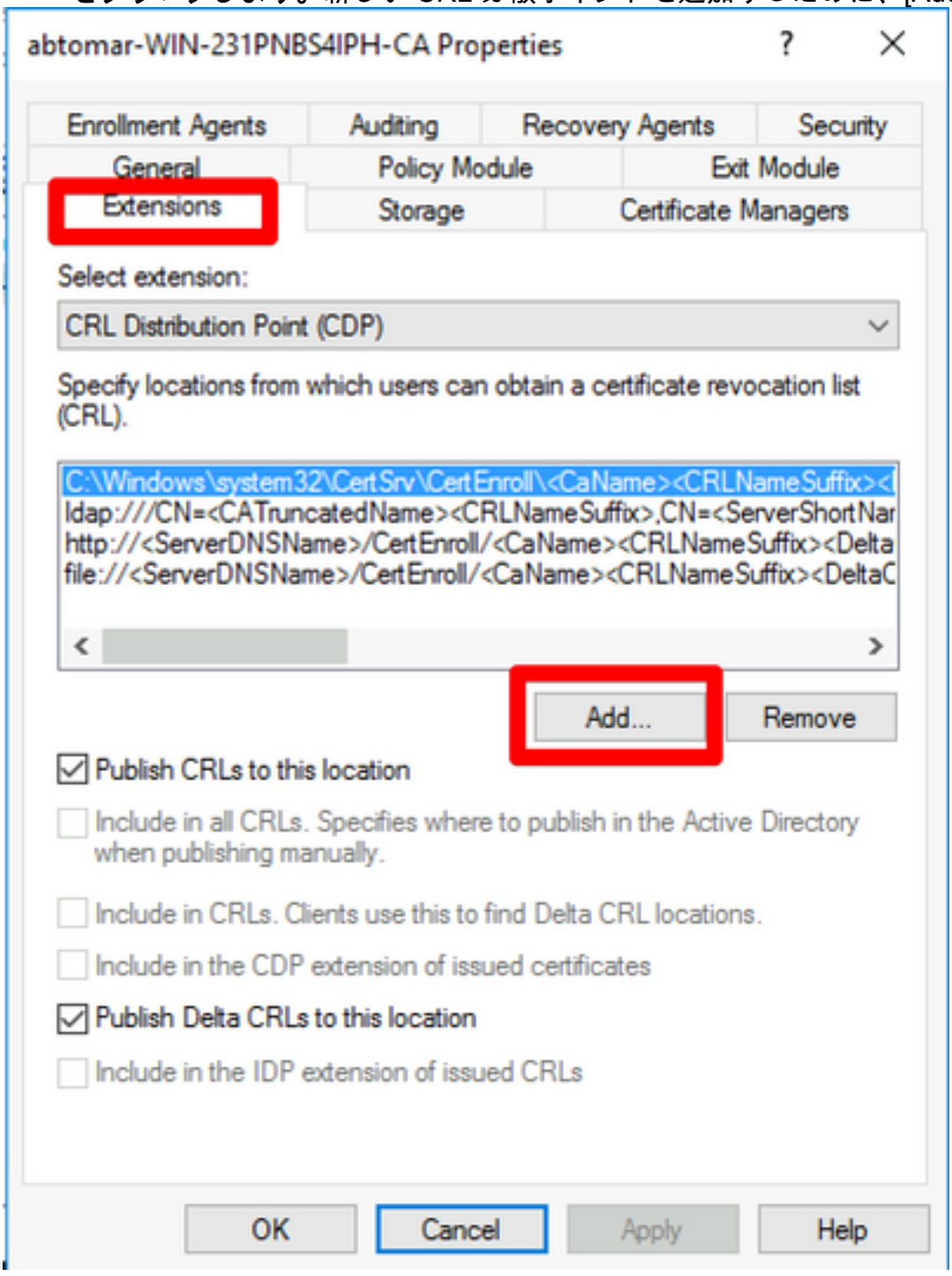


これで、フォルダにIIS経由でアクセスできるようになります。

分散ポイントにCRLファイルを公開するためのMicrosoft CAサーバの設定

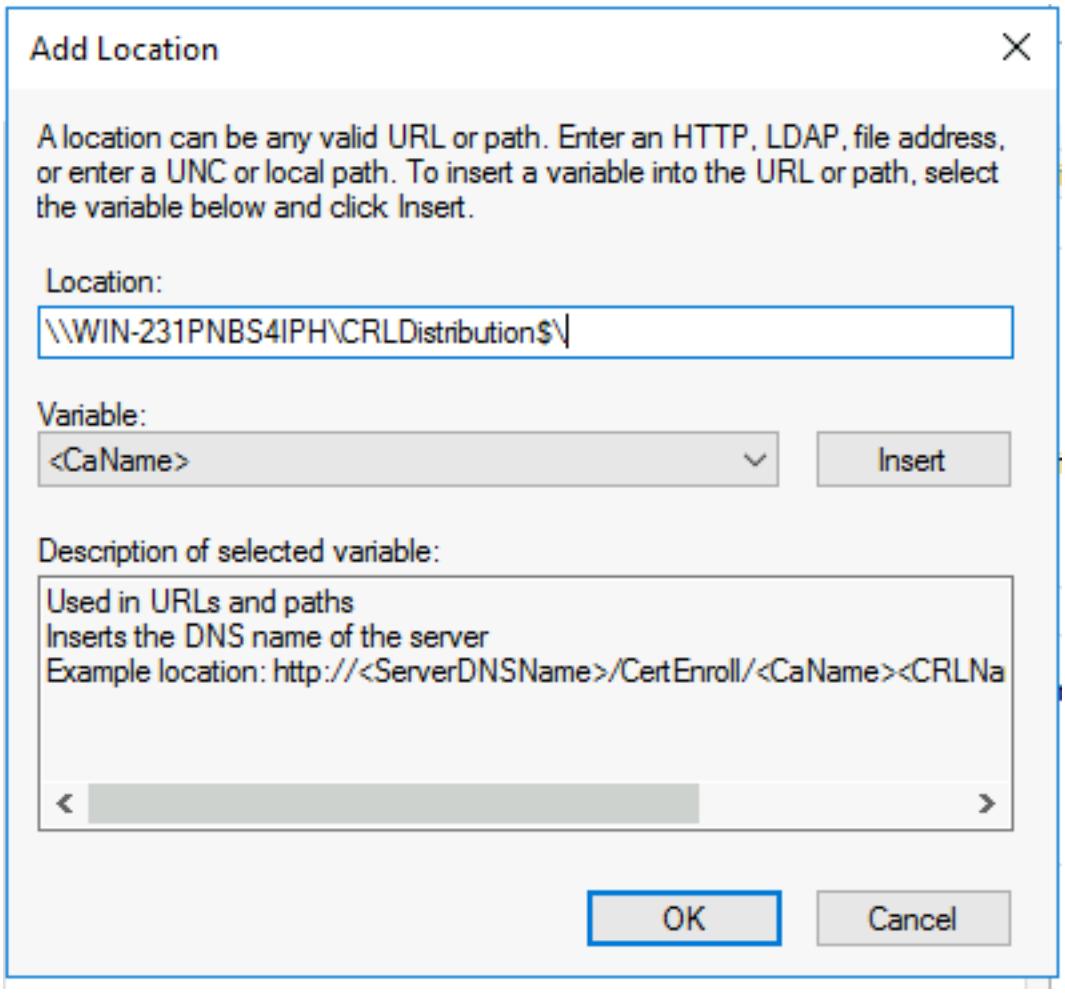
CRLファイルを格納するように新しいフォルダが設定され、そのフォルダがIISで公開されるようになったので、CRLファイルを新しい場所に公開するようにMicrosoft CAサーバを設定します。

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

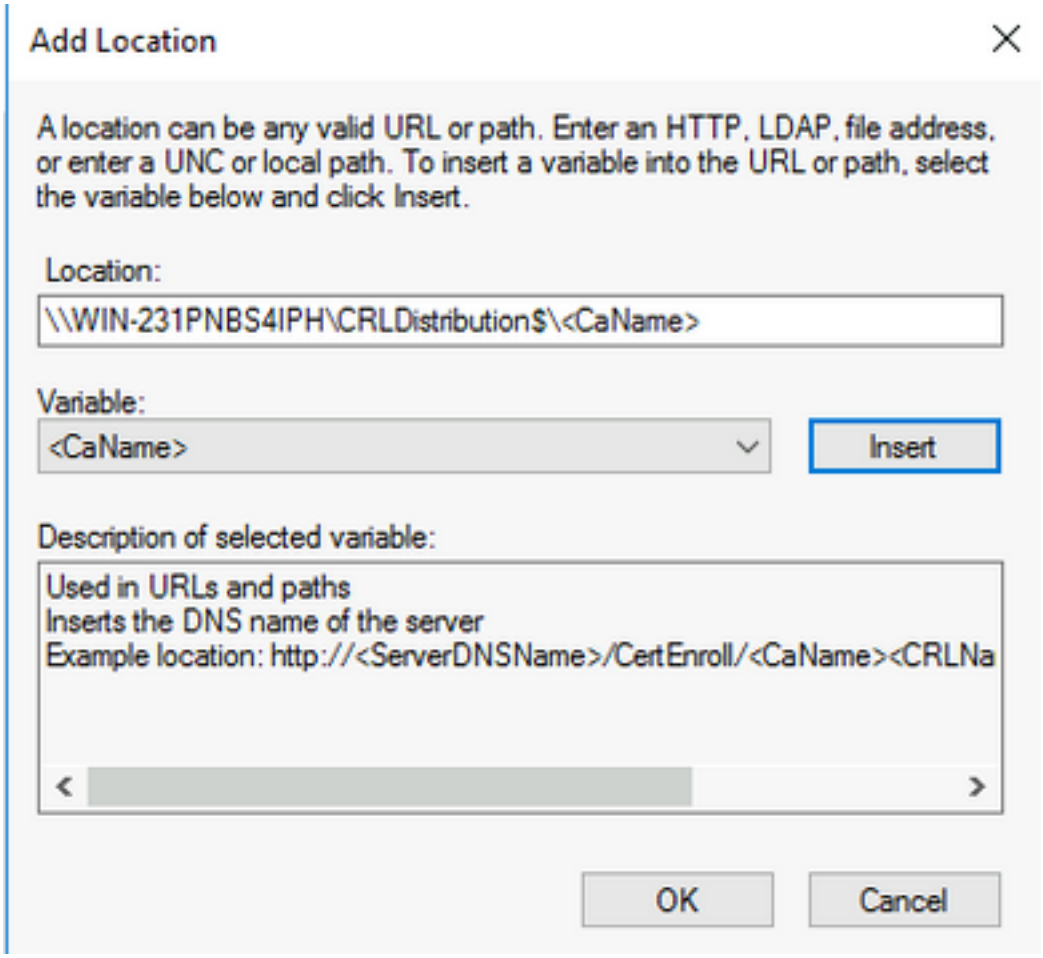


3.「場所」フィールドに、セクション1で作成および共有したフォルダへのパスを入力します。セクション1の例では、パスは次のとおりです。

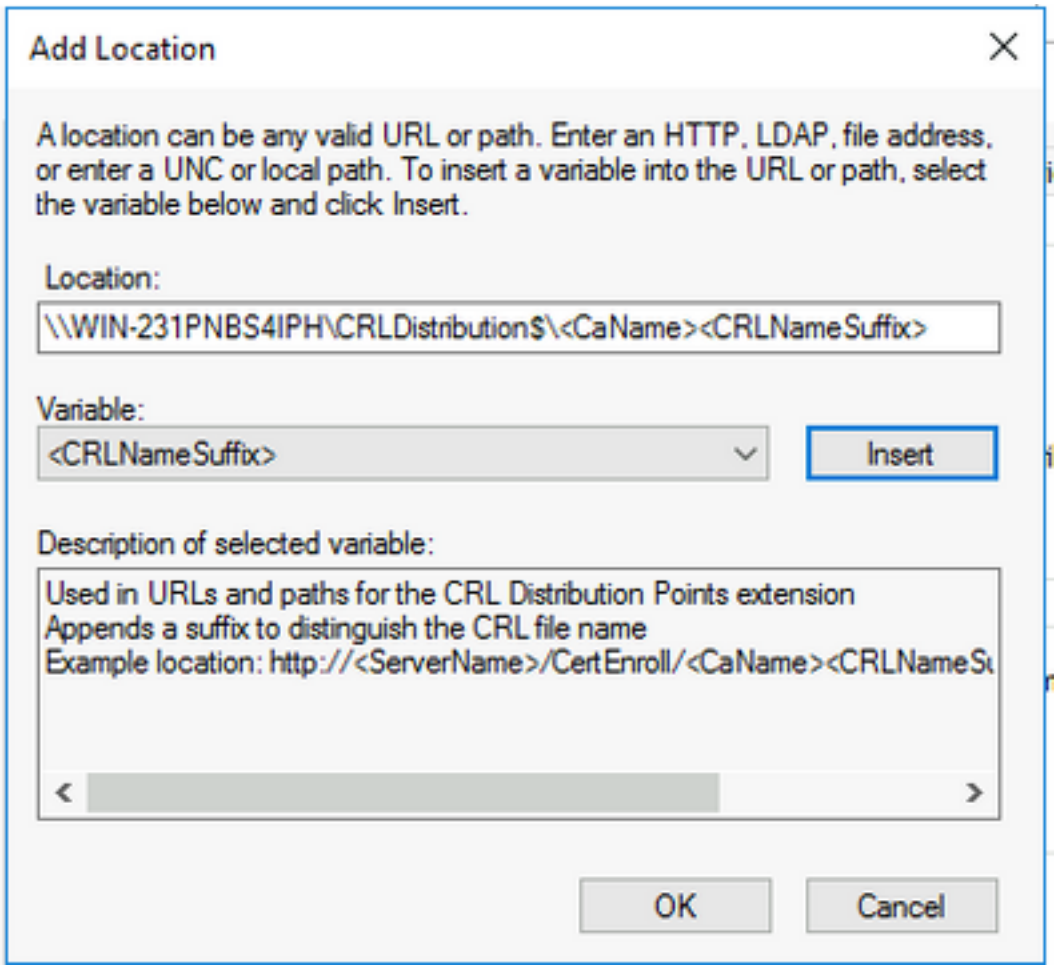
\\WIN-231PNBS4IPH\CRLDistribution$



4. [Location]フィールドに値を入力し、[Variable]ドロップダウンリストから**<CaName>を選択**し、[**Insert**]をクリック**します。**

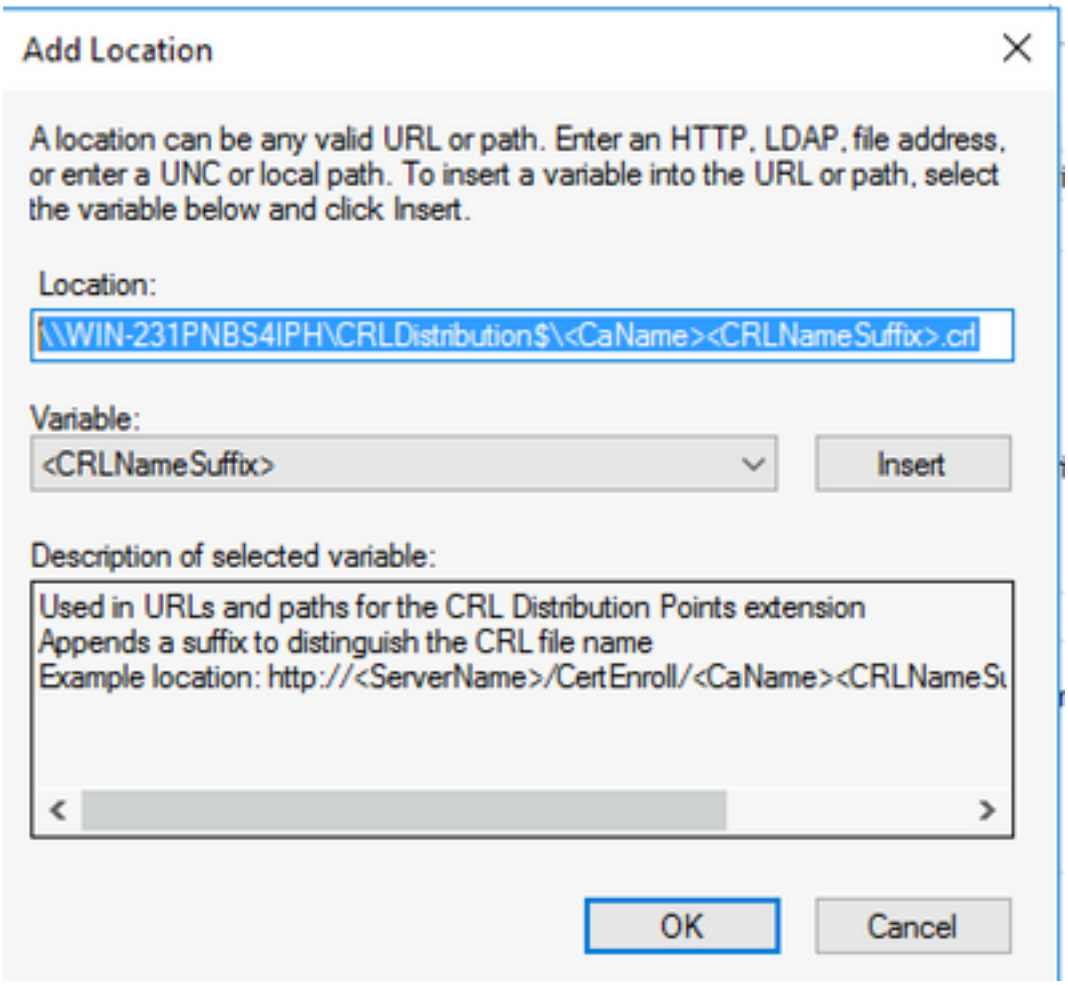


5. 「変数」ドロップダウン・リストから<CRLNameSuffix>を選択し、「挿入」をクリックします。



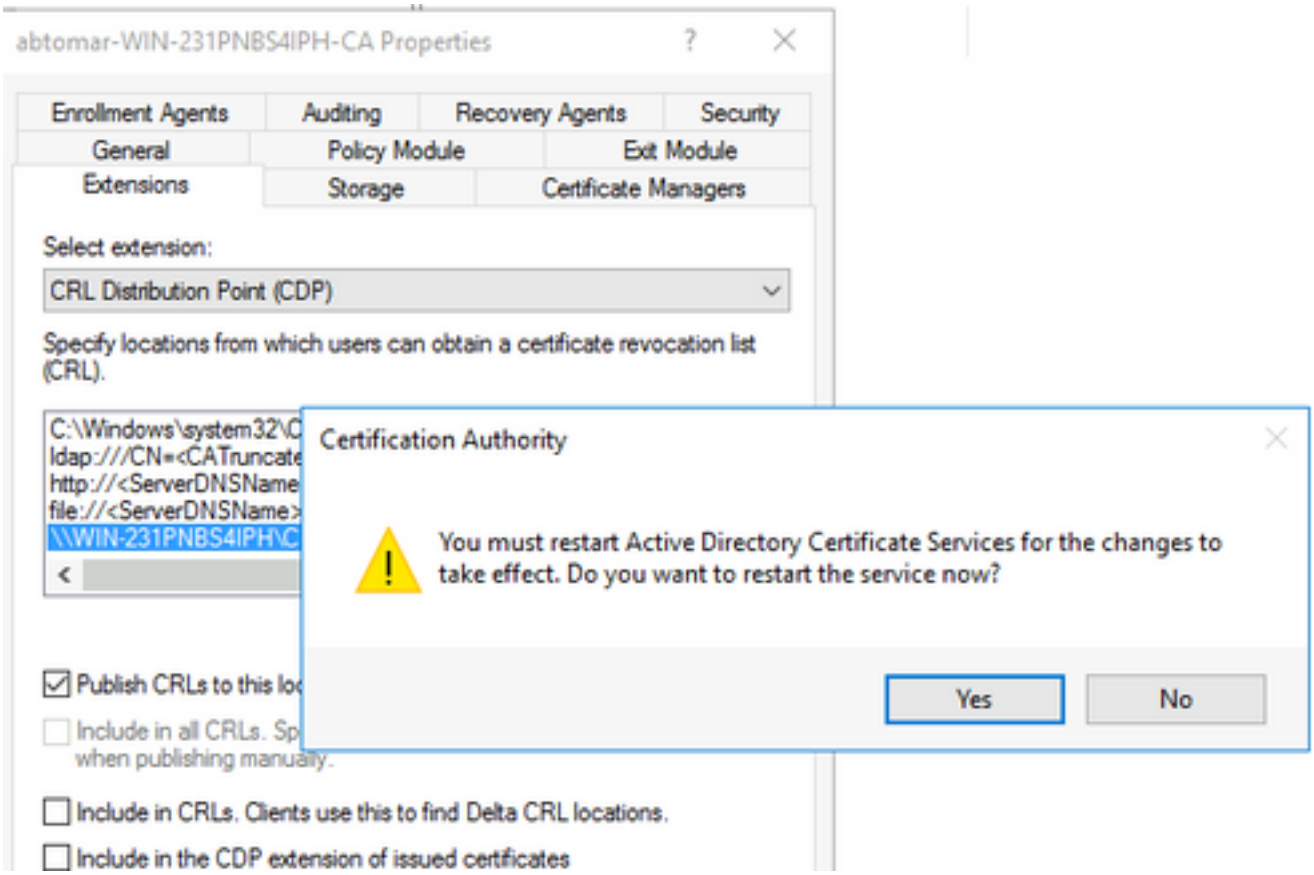
6. [場所]フィールドで、パス**の最後**に.crlを追加します。この例では、[Location] は次のようになります。

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

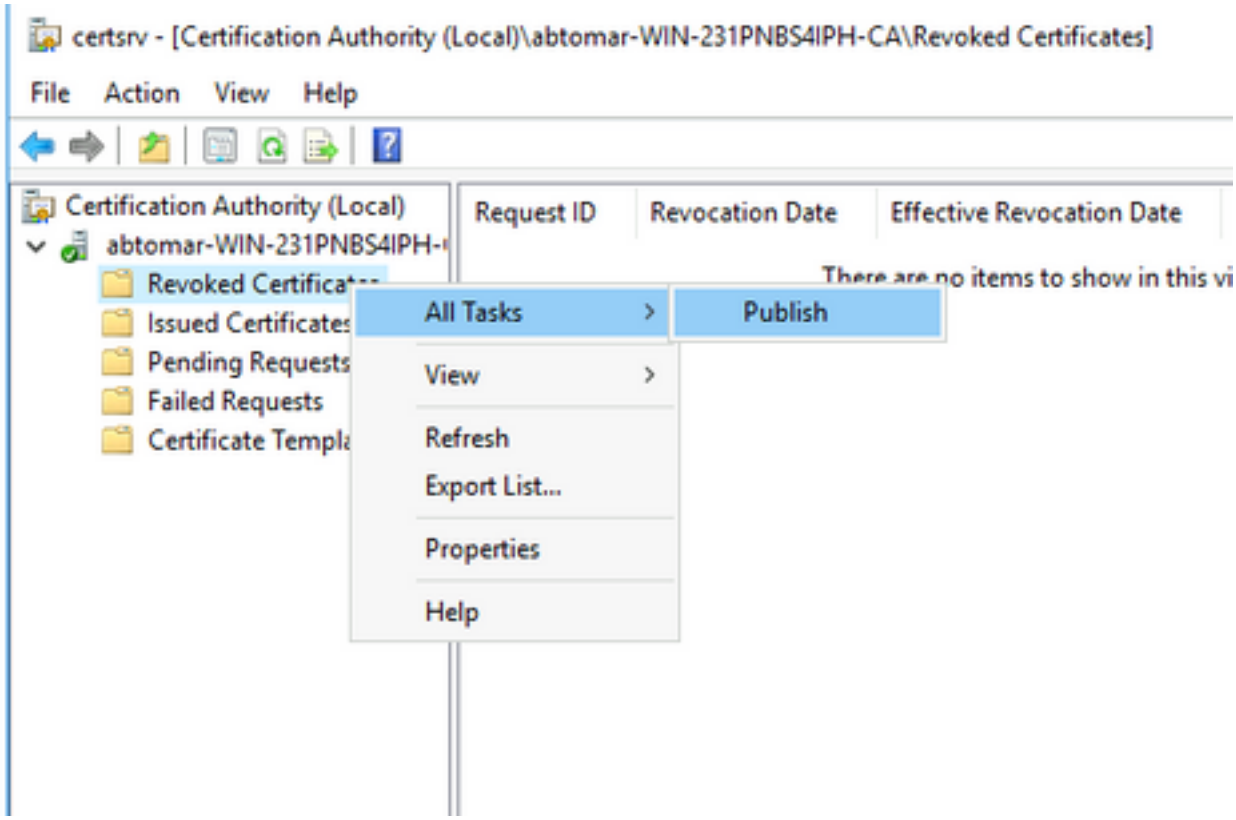


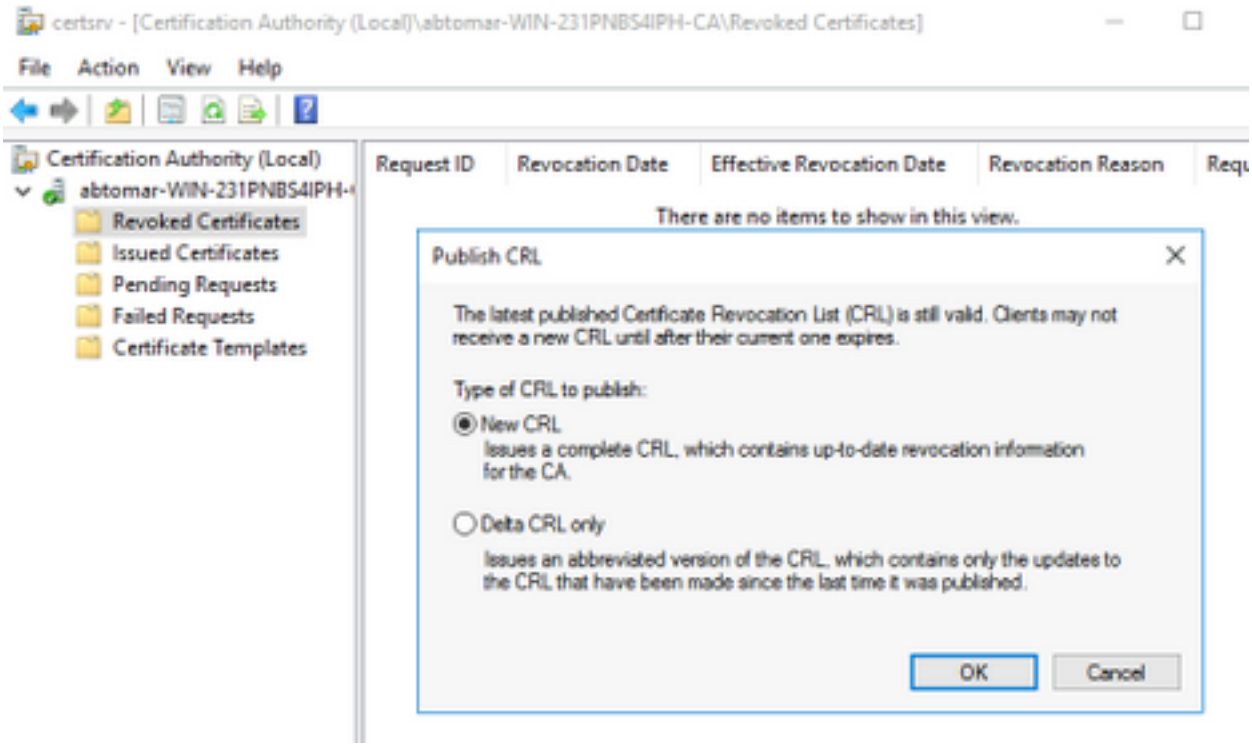
7. [OK] をクリックして [Extensions] タブに戻ります。[Publish CRLs to **this location]チェックボックスをオン**にし、[**OK**]をクリックして**[**Properties]ウィンドウを閉じます。

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。[Yes] をクリックします。



8.左側のペインで、[Revoked Certificates]を右クリックします。[All Tasks] > [Publish] を選択します。[New CRL] が選択されていることを確認し、[OK] をクリックします。





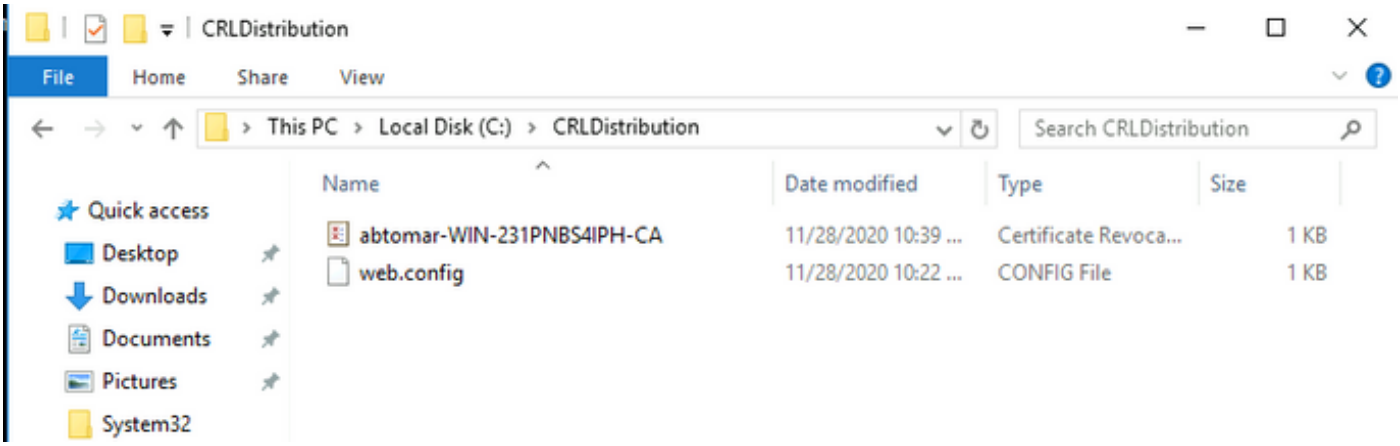
Microsoft CAサーバは、セクション1で作成したフォルダに新しい.crlファイルを作成する必要があります。新しいCRLファイルが正常に作成された場合、[OK]をクリックしてもダイアログは表示されません。新しい分散ポイント フォルダに関するエラーが返された場合は、このセクションの各ステップを慎重に繰り返してください。

CRLファイルが存在し、IIS経由で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サーバーで、セクション1で作成したフォルダを開きます。<CANAME>.crlという形式の単一の.crlファイルが存在する必要があります。<CANAME>はCAサーバーの名前です。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（ISEプライマリ管理ノードと同じネットワーク上）からWebブラウザを開き、http://<SERVER>/<CRLSITE>を参照します。<SERVER>はセクション2で設定されたIISサーバのサーバ名、<CRLSITE>はです。

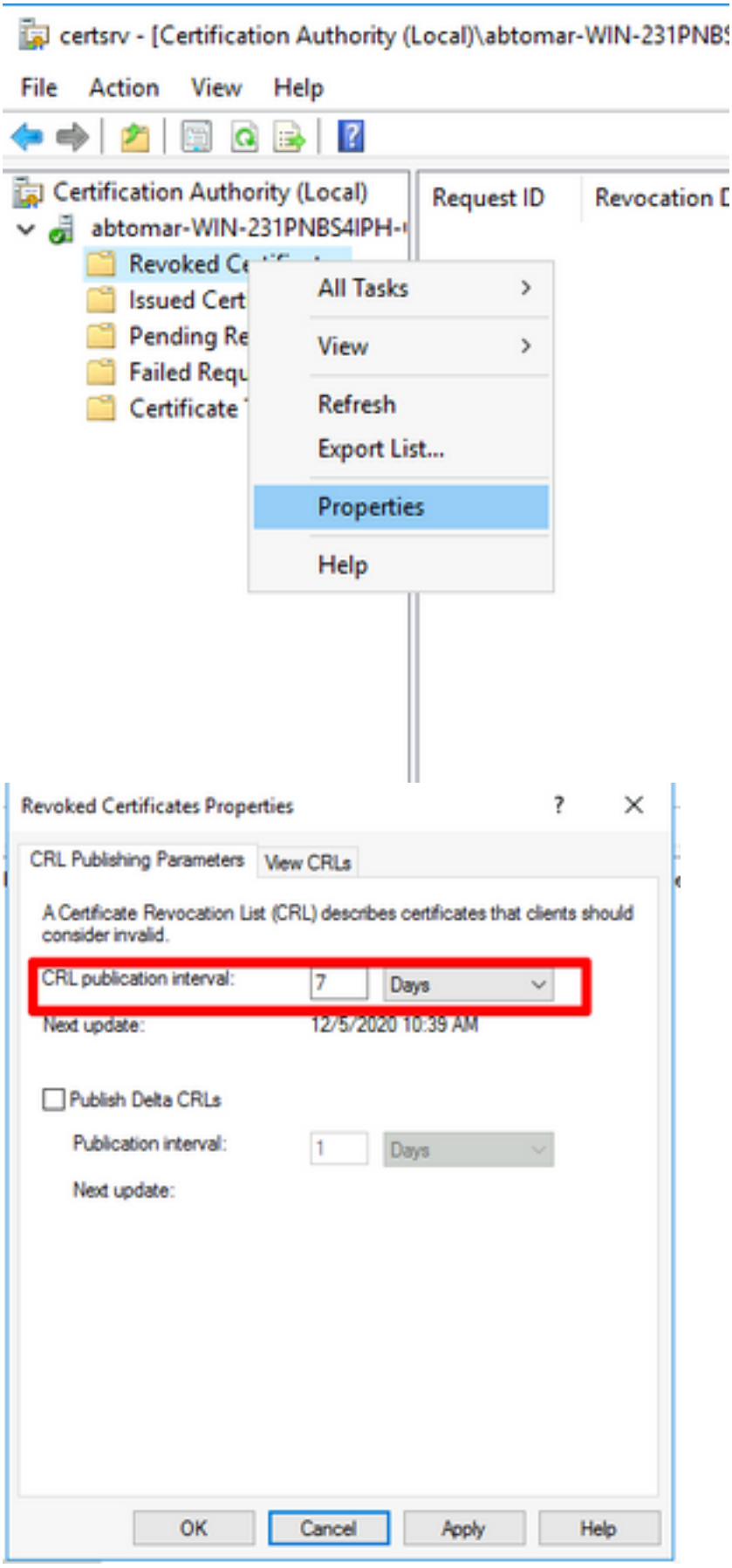
http://win-231pnbs4iph/CRLD

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ようにISEを設定します

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、[Start] をクリックします。[Administrative Tools] > [Certificate Authority] を選択します。
2. 左側のペインで、CAを展開します。[Revoked Certificates]フォルダを右クリックし、[Properties]を選択します。
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。[OK] をクリックしてウィンドウを閉じ、変更を適用します。この例では、発行間隔が 7 日に設定されています。



4. **certutil -getreg CA\Clock*コマンドを入力して**、ClockSkew値を確認します。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. **certutil -getreg CA\CRLov***コマンドを入力して、CRLOverlapPeriodが手動で設定されているかどうかを確認します。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. **certutil -getreg CA\CRLpe* コマンドを入力して、ステップ 3 で設定した CRLPeriod を確認します。**

出力例：

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

7. CRLの猶予期間を次のように計算します。

a.CRLOverlapPeriod をステップ 5 で設定した場合：OVERLAP = CRLOverlapPeriod（分）

それ以外の場合：OVERLAP = (CRLPeriod / 10)（分）

b.OVERLAP > 720 の場合、OVERLAP = 720

c. OVERLAP < (1.5 * ClockSkewMinutes)の場合、OVERLAP = (1.5 * ClockSkewMinutes)

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

e.猶予期間= OVERLAP + ClockSkewMinutes

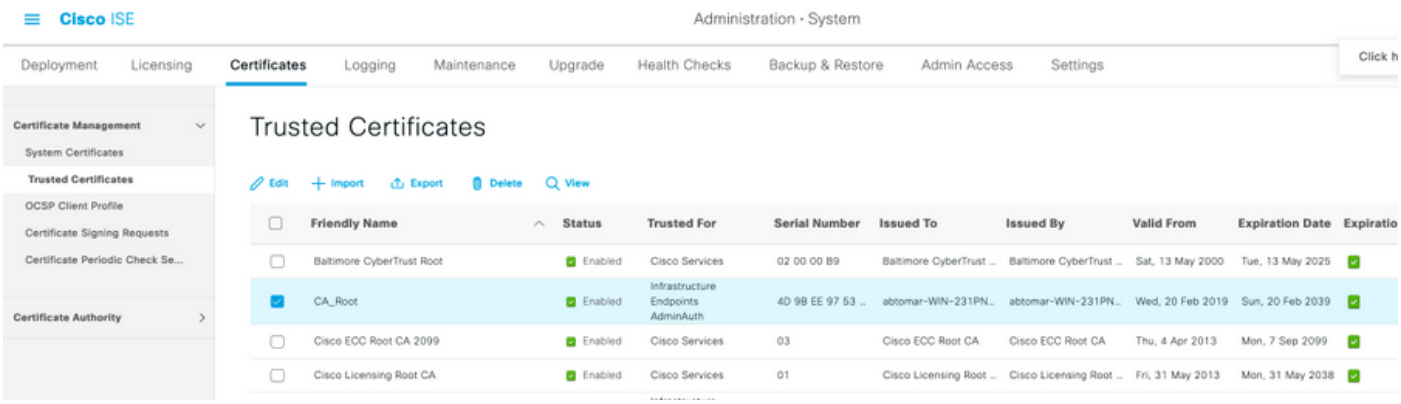
```
Example:

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プライマリ管理ノードにログインし、**[Administration] > [System] > [Certificates]の順に選択します。**左側のペインで、 **信頼できる証明書**



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。[Edit] をクリックします。

10.ウィンドウの下部にある[Download CRL]チェックボックスをオンにします。

11. [CRL Distribution URL]フィールドに、セクション2で作成した.crlファイルを含むCRL分散ポイントへ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

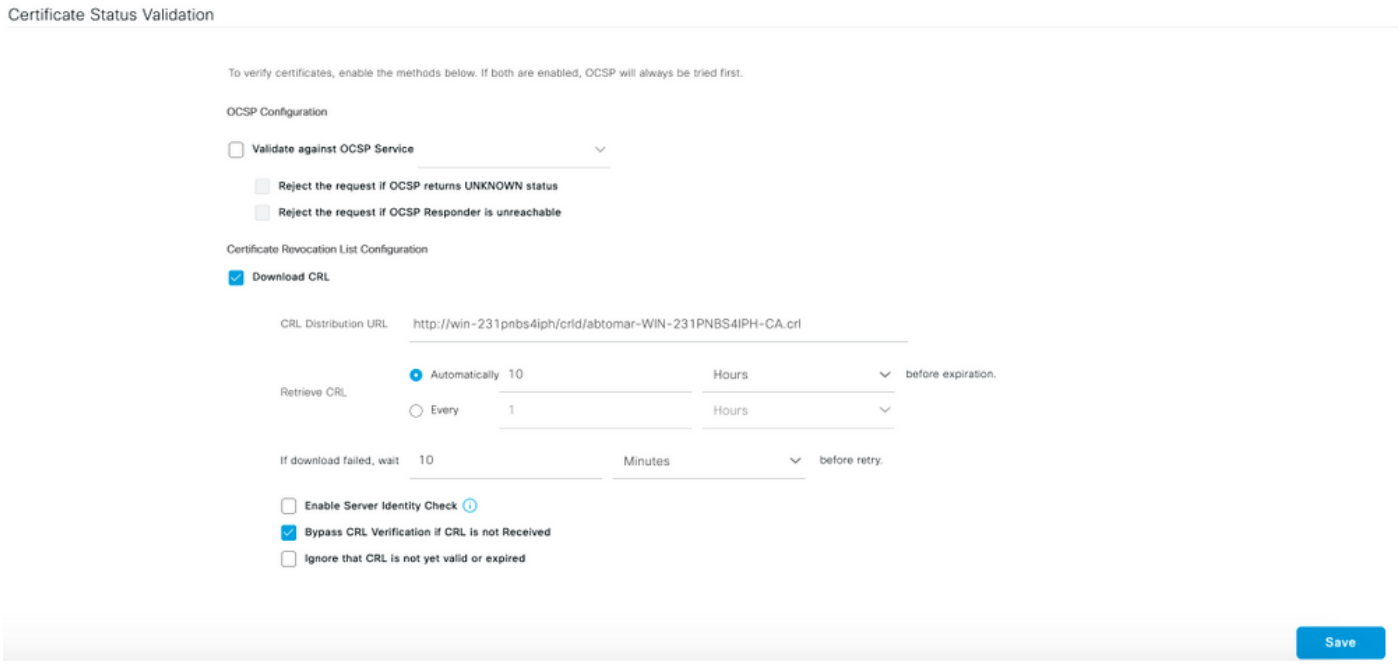
12. ISEは、定期的な間隔で、または有効期限に基づいてCRLを取得するように設定できます（一般的には、定期的な間隔でもあります）。 CRL の発行間隔が固定されている場合は、後者のオプションのほうがタイムリーに CRL のアップデートを取得できます。[Automatically] **オプションボタンをクリックします。**

13.取得の値をステップ7で計算した猶予期間より小さい値に設定します。設定した値が猶予期間より長い場合、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。取得には10時間の値が使用されます

14.環境に応じて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（およびCRLチェックなしで）続行できるようにするには、**[Bypass CRL Verification if CRL is not Received]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、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. **Ignore that CRL is not yet valid or expiredチェックボックスにチェックマークを入れ**て、ISEが期限切れ（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。[Save] をクリックして設定を完了します。



シスコ内部情報

1. Microsoft「証明書のCRL分散ポイントを設定します。」 http://technet.microsoft.com/en-us/library/ee649260%28v=ws.10%29.aspx、2009年10月7日[2012年12月18日]

2. Microsoft「証明書失効リストを手動で発行します。」 http://technet.microsoft.com/en-us/library/cc778151%28v=ws.10%29.aspx, 2005年1月21日[2012年12月18日]

3. Microsoft「CRLとDelta CRLのオーバーラップ期間を設定します。」 http://technet.microsoft.com/en-us/library/cc731104.aspx、2011年4月11日[2012年12月18日]

4. MS2065 [MSFT].「How EffectiveDate (this update), NextUpdate, and NextCRLPubrish are calculated.」 http://blogs.technet.com/b/pki/archive/2008/06/05/how-effectivedate-thisupdate-nextupdate-and-nextcrlpublish-are-calculated.aspx、2008年6月4日[2012年12月18日]