Microsoft CA サーバの ISE の証明書失効リストの発行の設定例

目次

はじめに

このドキュメントでは、証明書失効リスト（CRL）のアップデート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。 証明書の検証の使用に関するアップデートを取得するために Cisco Identity Services Engine（ISE）（バージョン 1.1 以降）を設定する方法についても説明します。 ISE は、証明書検証で使用する各種 CA ルート証明書の CRL を取得するように設定できます。

前提条件

要件

このドキュメントに関しては個別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くものです。

- Cisco Identity Services Engine Release 1.1.2.145
- Microsoft Windows® Server® 2008 R2

本書の情報は、特定のラボ環境にあるデバイスに基づいて作成されたものです。 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。 稼働中のネットワークで作業を行う場合、コマンドの影響について十分に理解したうえで作業してください。

表記法

ドキュメント表記の詳細は、『シスコ テクニカル ティップスの表記法』を参照してください。

設定

この項では、このドキュメントで説明する機能の設定に必要な情報を提供します。

注: このセクションで使用されているコマンドの詳細を調べるには、Command Lookup Tool（登録ユーザ専用）を使用してください。

設定

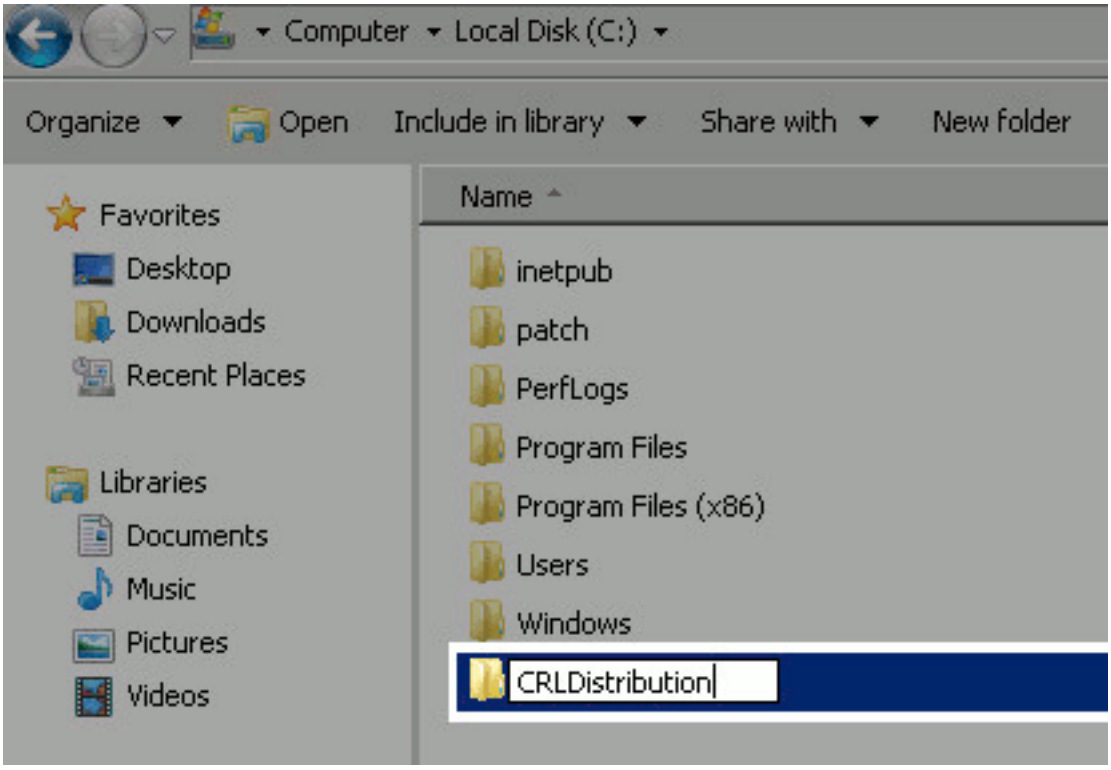
このドキュメントでは、次の設定を使用します。

- セクション 1. CRL ファイルを格納するためのフォルダを CA に作成および設定する
- セクション 2. 新しい CRL 分散ポイントを公開するには、サイトを IIS で作成する
- セクション 3. 分散ポイントに CRL ファイルを発行するように Microsoft CA サーバを設定する
- セクション 4. CRL ファイルが存在しており、IIS からアクセスできることを確認する
- セクション 5. 新しい CRL 分散ポイントを使用するように、ISE を設定する

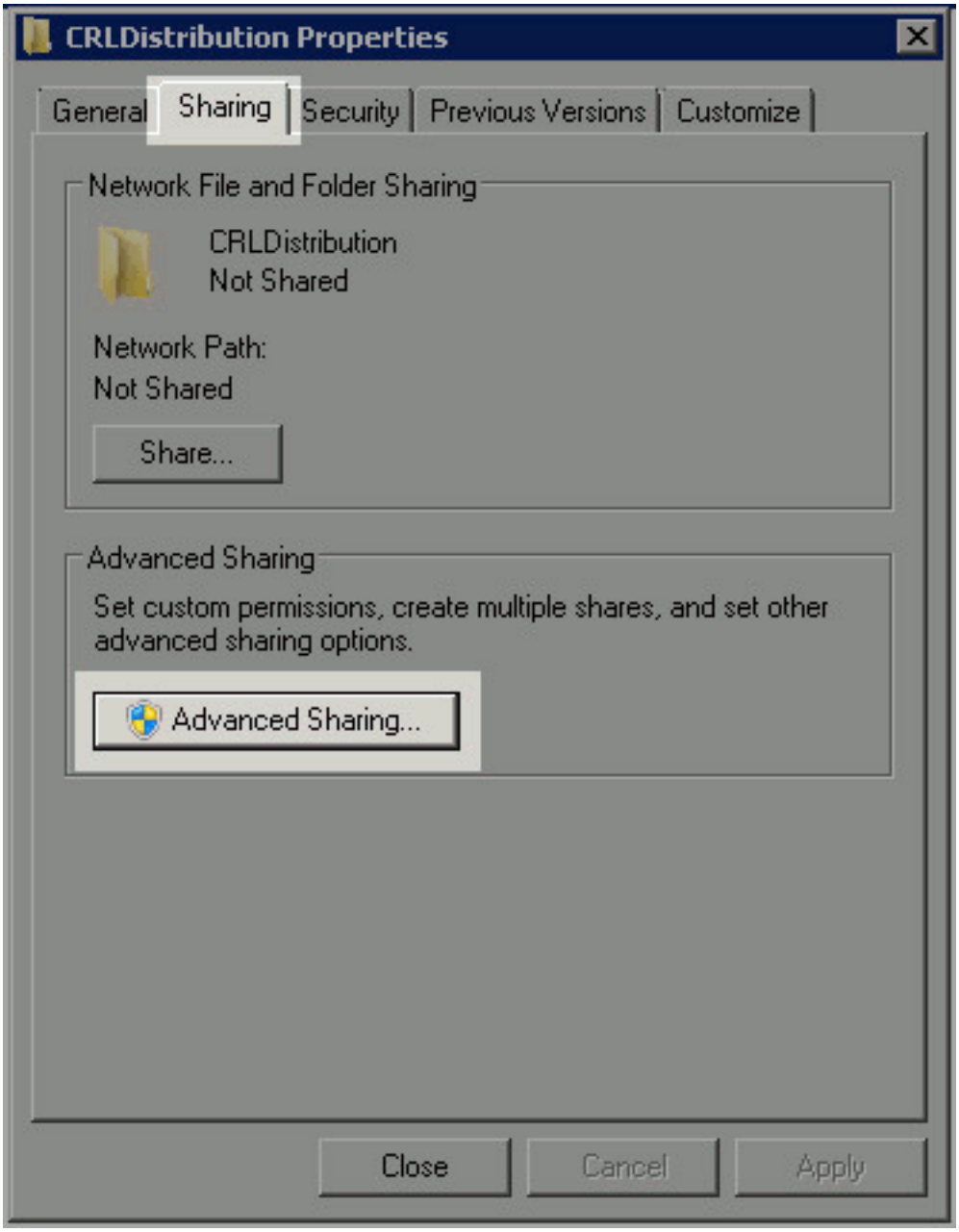
セクション 1. CRL ファイルを格納するためのフォルダを CA に作成および設定する

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

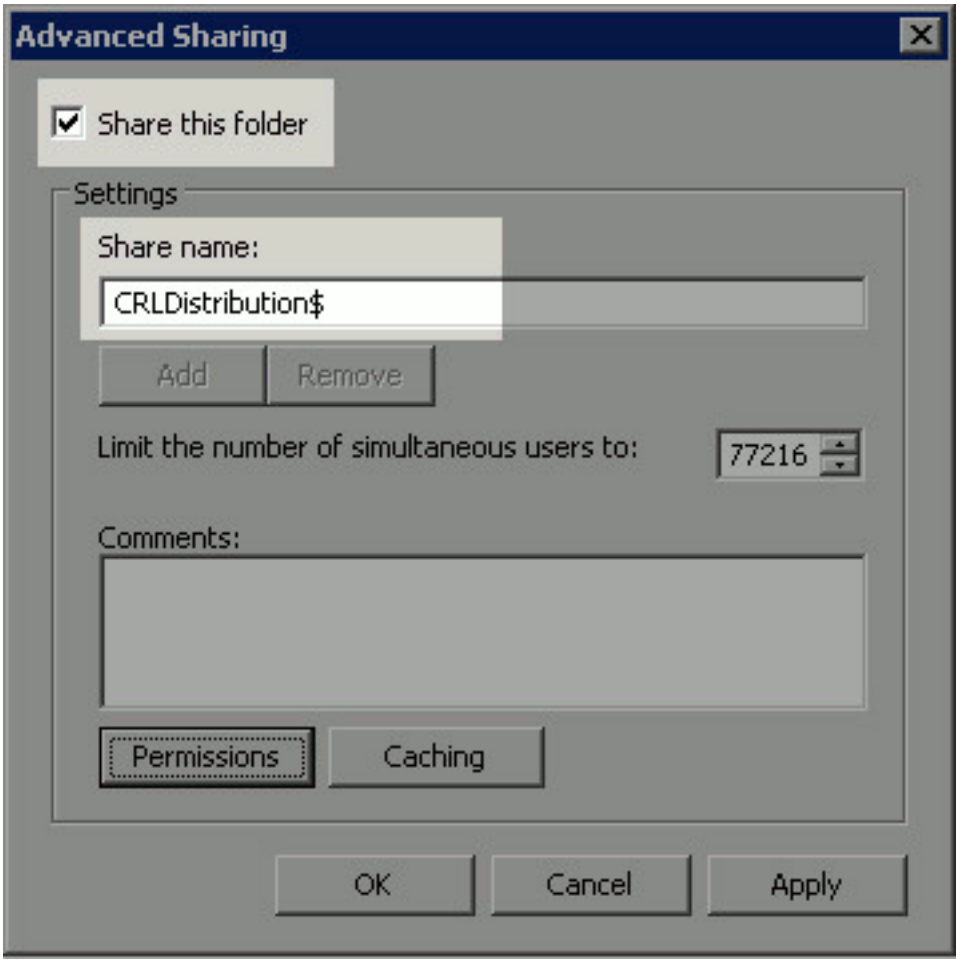
1. IIS サーバで、ファイル システムの場所を選択し、新しいフォルダを作成します。 この例では、フォルダ C:\CRLDistribution を作成します。



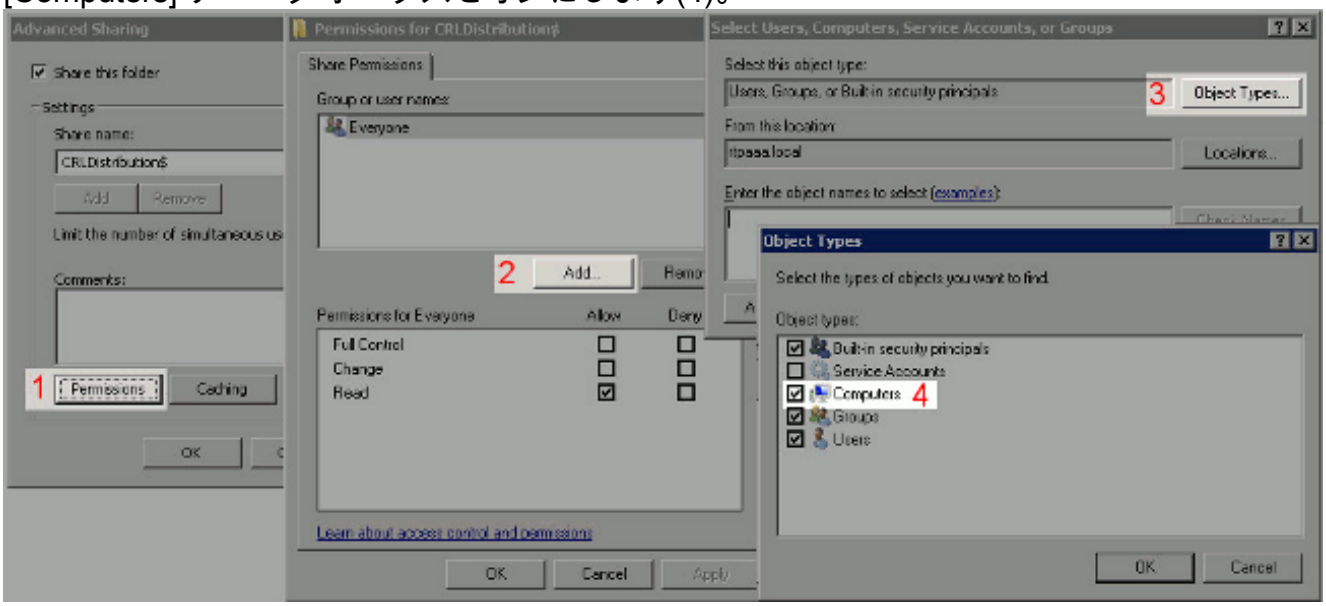
2. 新しいフォルダに CA が CRL ファイルを書き込むようにするには、共有をイネーブルにする必要があります。 新しいフォルダを右クリックし、[Properties] を選択し、[Sharing] タブをクリックしてから [Advanced Sharing] をクリックします。



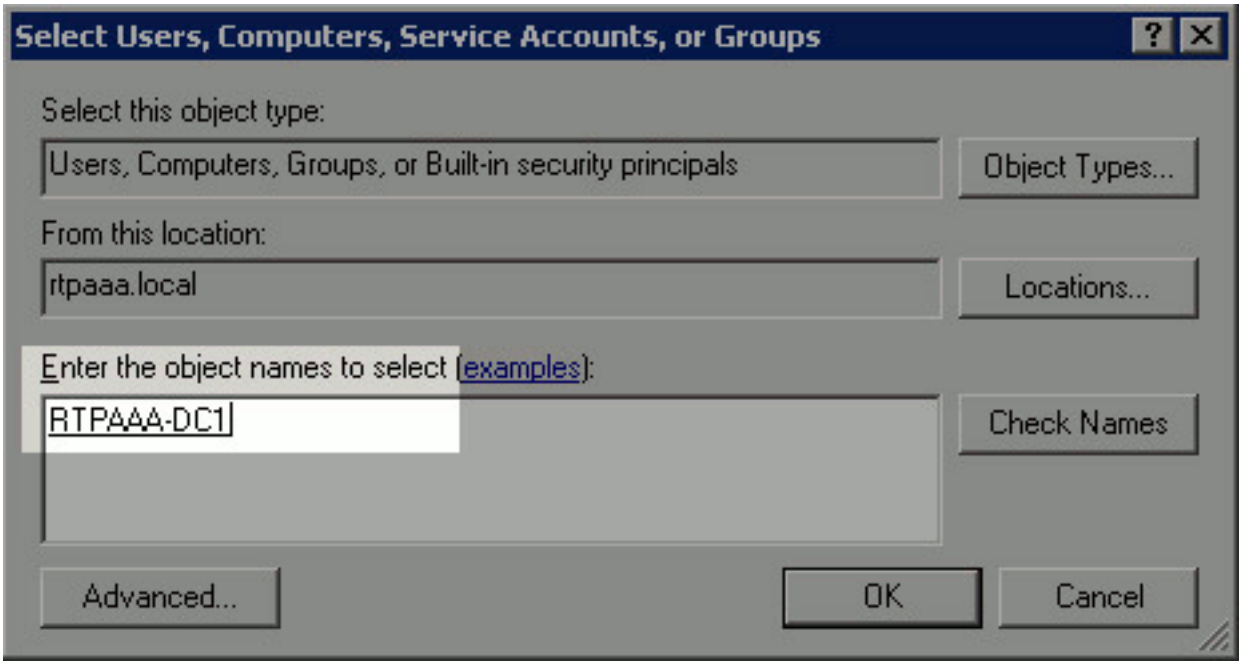
3. フォルダを共有するために、[Share this folder] チェック ボックスをオンにし、共有を非表示にするために [Share name] フィールドで共有名の最後にドル記号（$）を追加します。



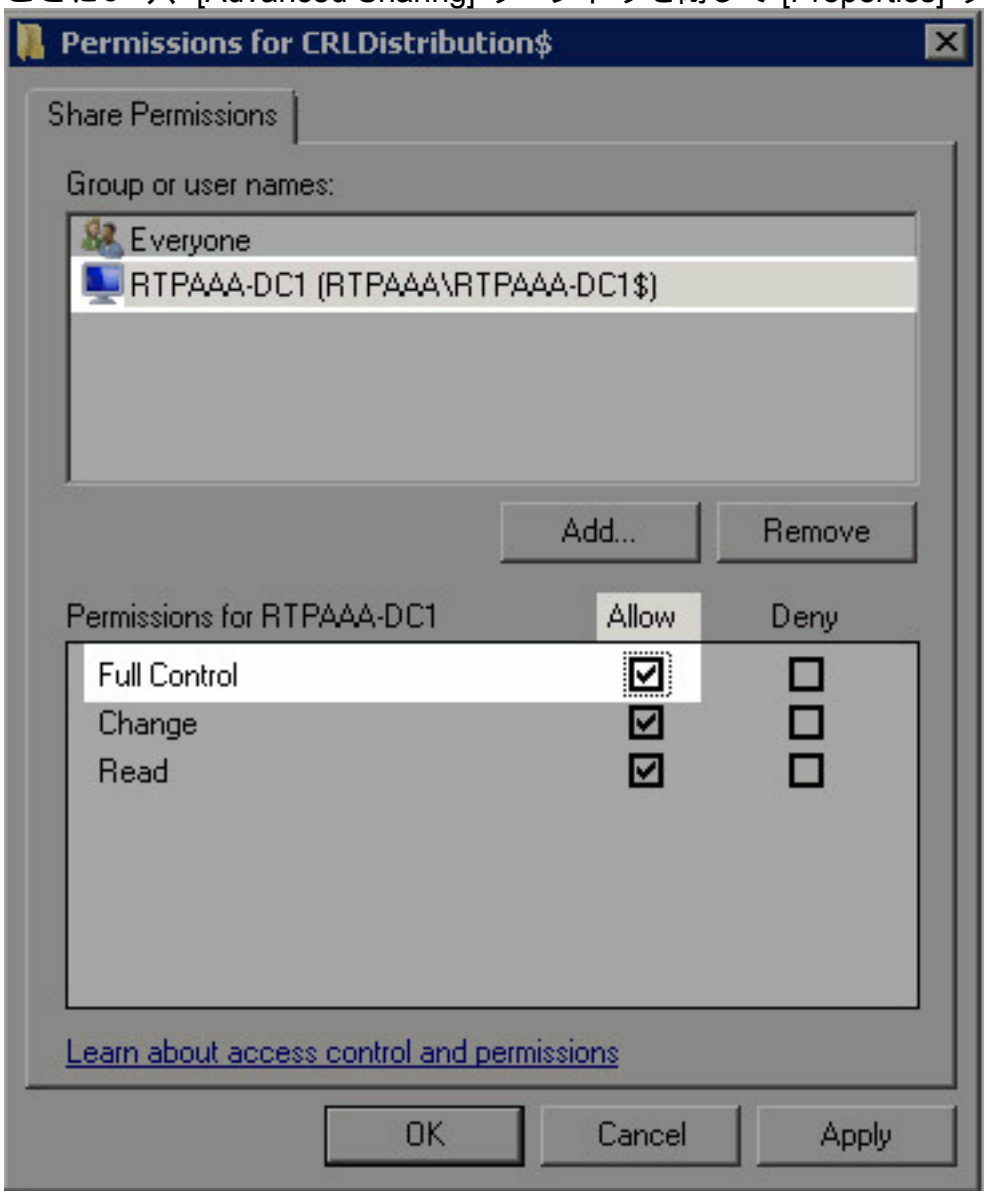
4. [Permissions] をクリック(1)、[Add] をクリック(2)、[Object Types] をクリックし(3)、[Computers] チェック ボックスをオンにします(4)。



5. [Select Users, Computers, Service Accounts, or Groups] ウィンドウに戻るために [OK] をクリックします。 [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、名前が更新されて下線が引かれます。 [OK] をクリックします。

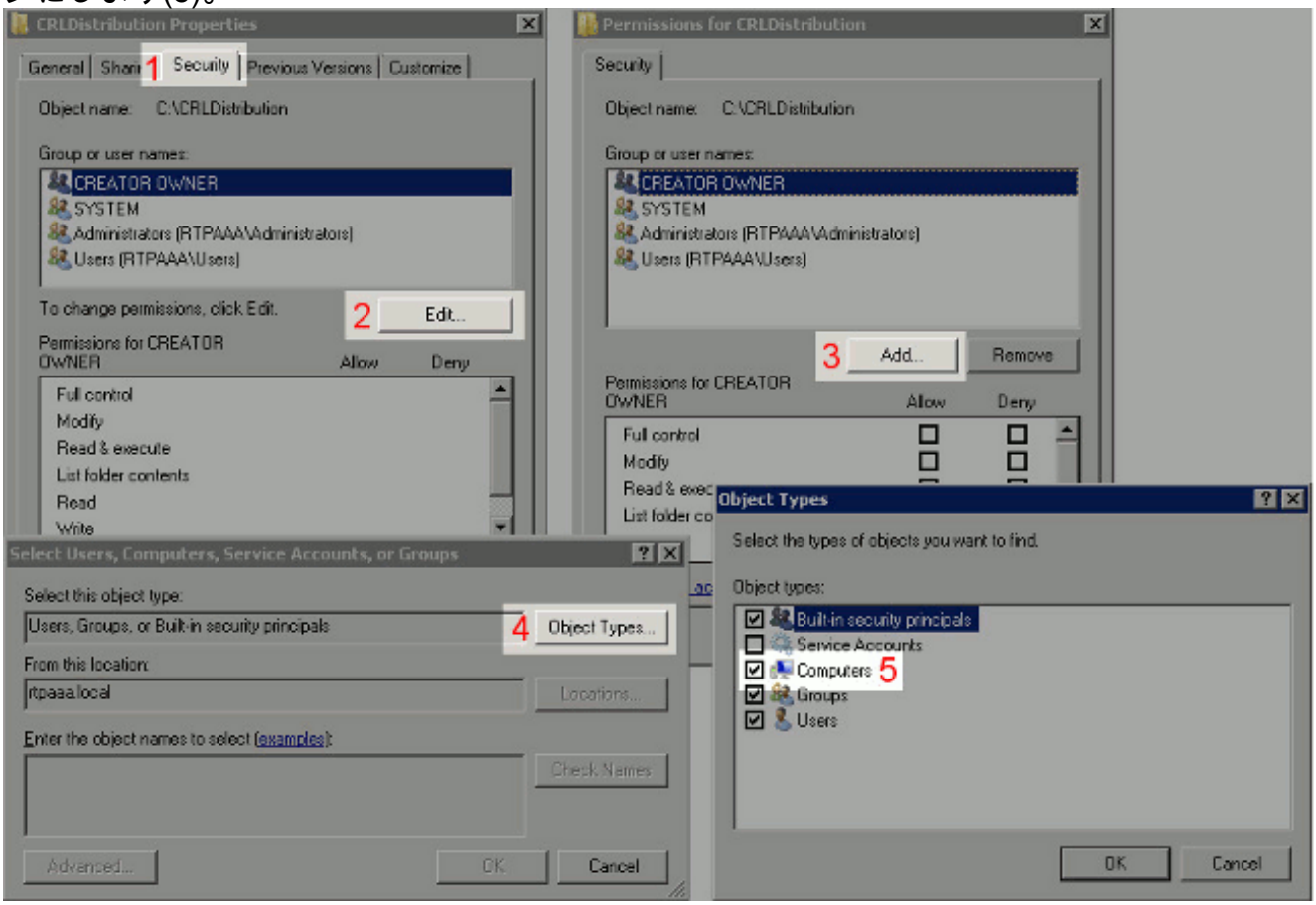


6. [Group or user names] フィールドで、CA のコンピュータを選択します。 [Full Control] の [Allow] をオンにして CA にフル アクセスを許可します。[OK] をクリックします。 [OK] を再度クリックすることにより、[Advanced Sharing] ウィンドウを閉じて [Properties] ウィンドウに戻ります。

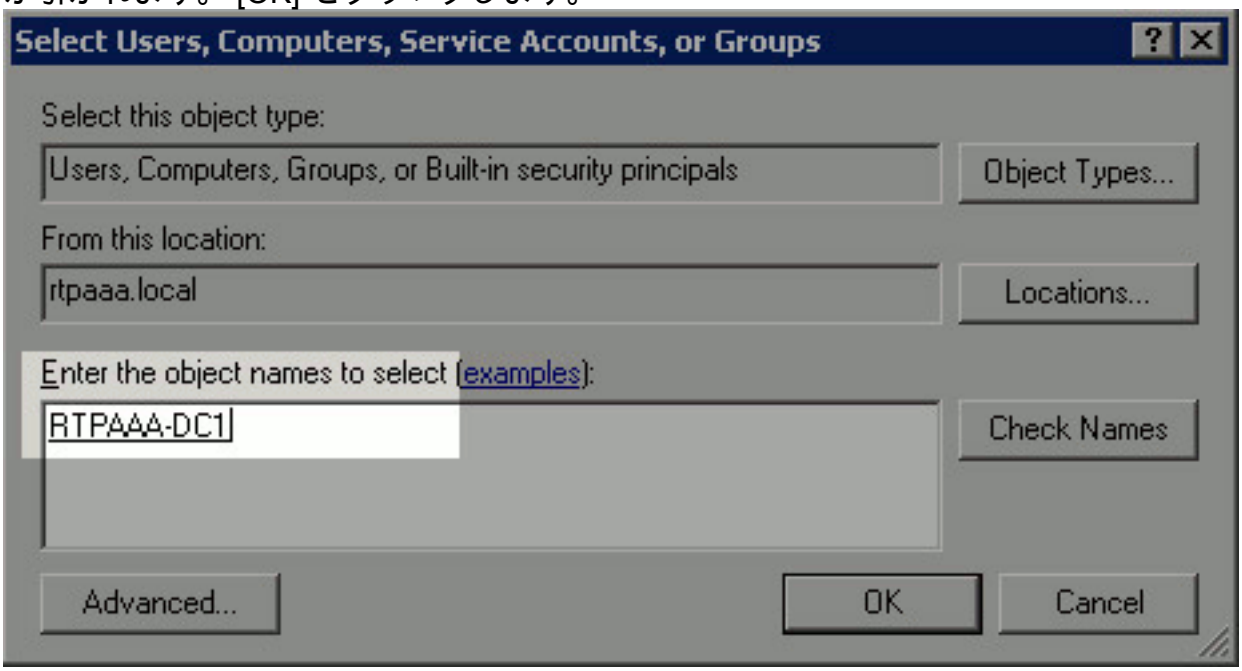


7. 新しいフォルダに対する CRL ファイルの書き込みを CA に許可するために、適切なセキュ

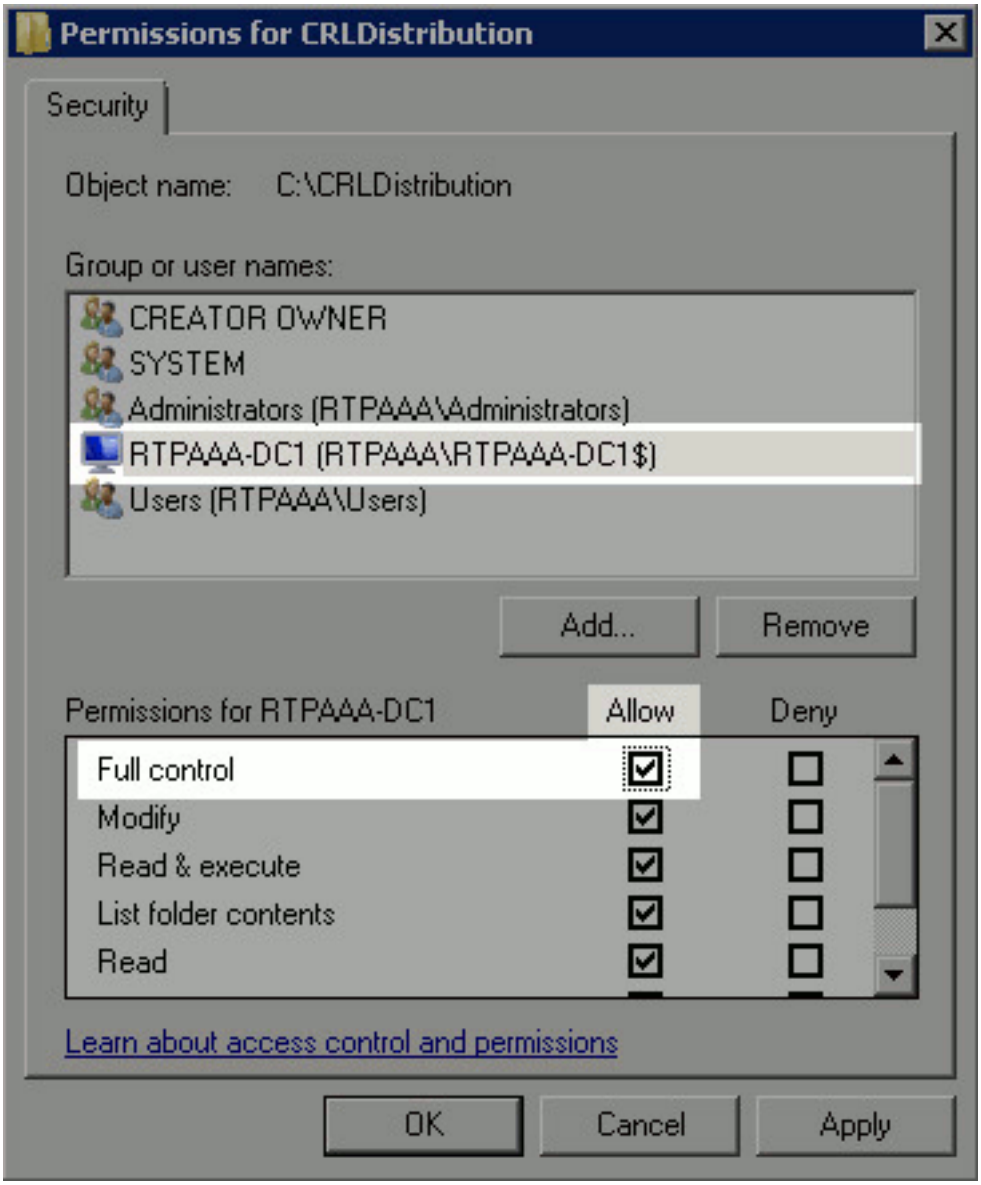
リティのアクセス許可を設定します。 [Security] タブをクリック(1)、[Edit] をクリック(2)、[Add] をクリック(3)、[Object Types] をクリックし(4)、[Computers] チェック ボックスをオンにします(5)。



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、名前が更新されて下線が引かれます。 [OK] をクリックします。



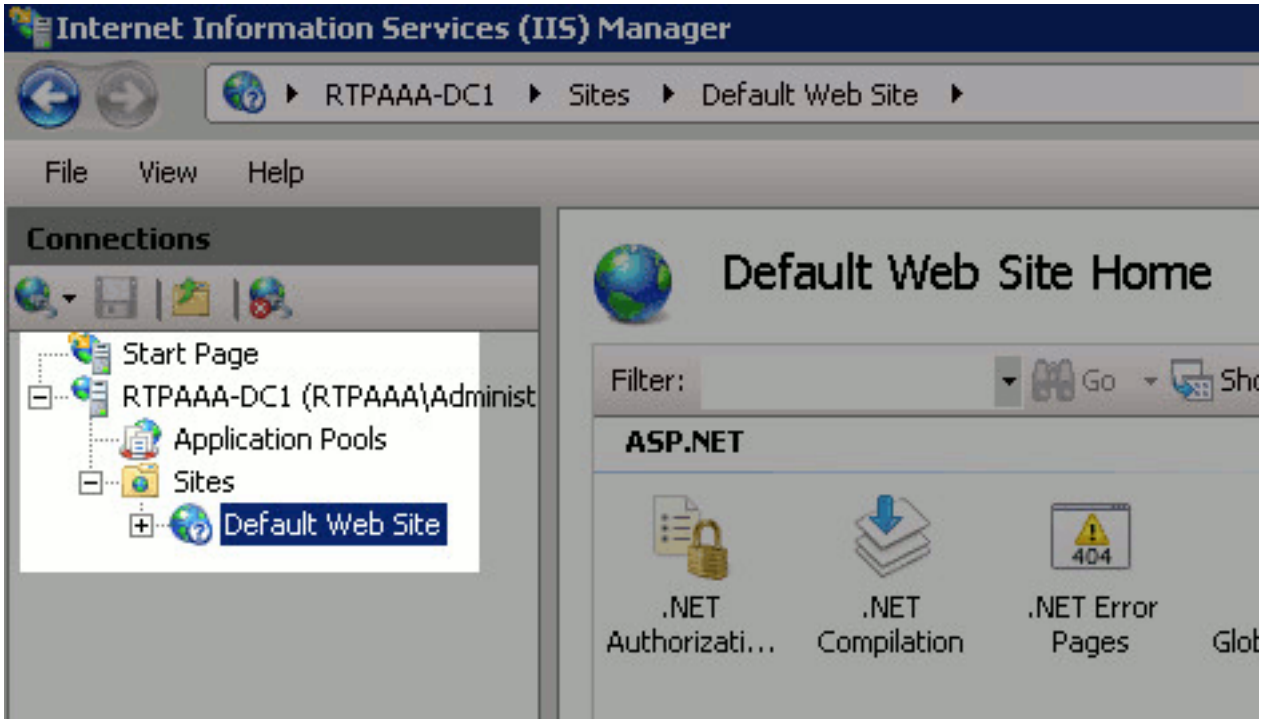
9. [Group or user names] フィールドで CA のコンピュータを選択してから、CA へのフル アクセスを許可するために [Full control] の [Allow] をオンにします。[OK]、[Close] の順にクリックして作業を完了します。



セクション 2. 新しい CRL 分散ポイントを公開するには、サイトを IIS で作成する

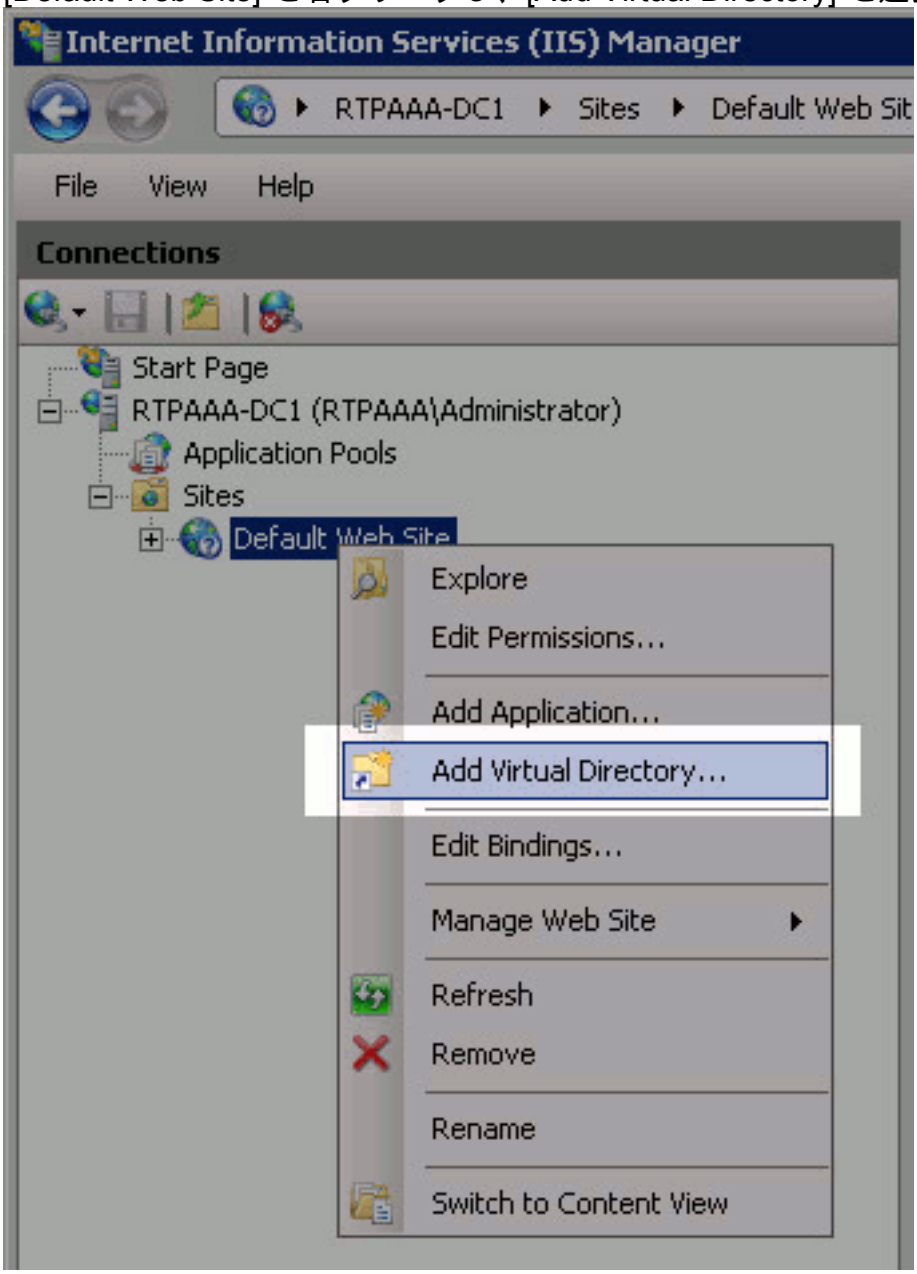
ISE が CRL ファイルにアクセスするために、CRL ファイルを格納する、IIS からアクセス可能なディレクトリを作成します。

1. IIS サーバ 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てから [Sites] を展開します

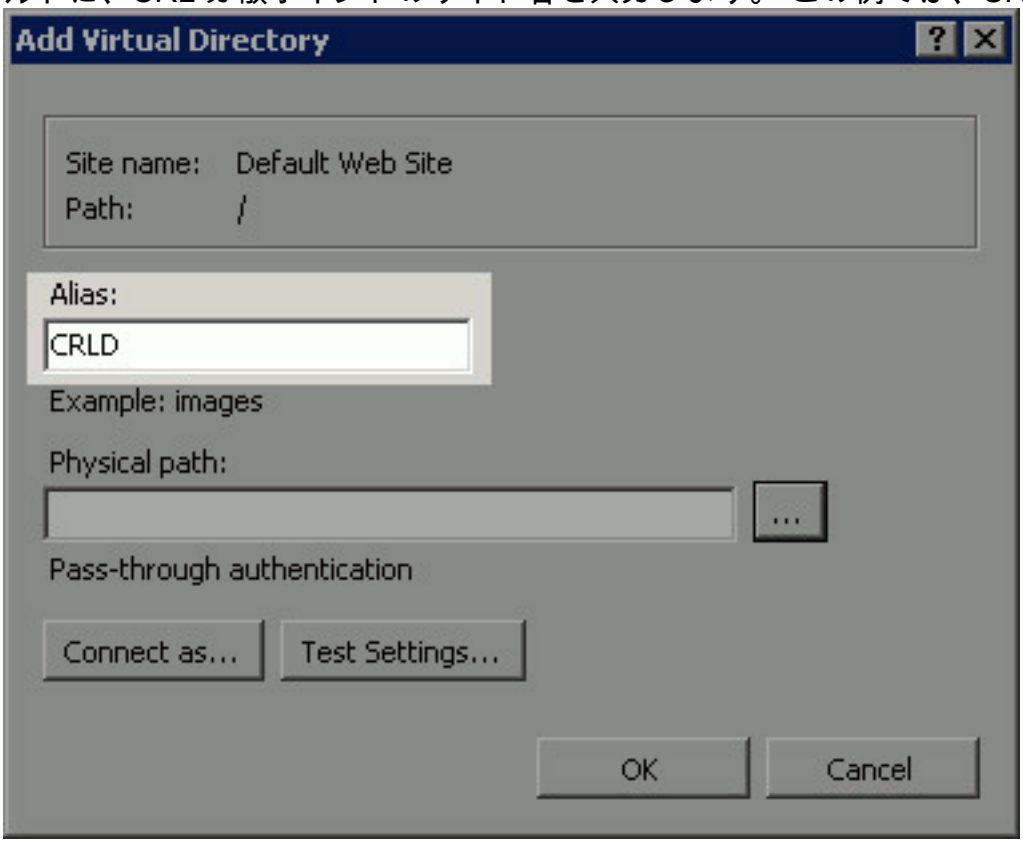


。

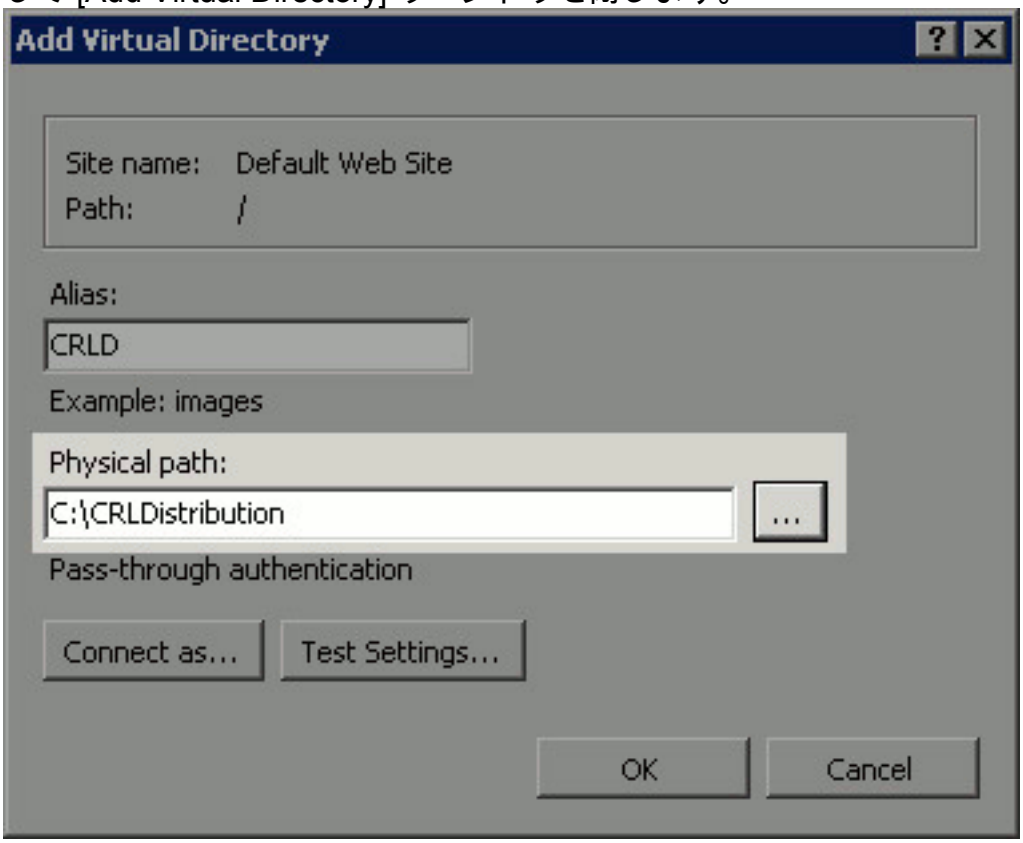
3. [Default Web Site] を右クリックし、[Add Virtual Directory] を選択します。



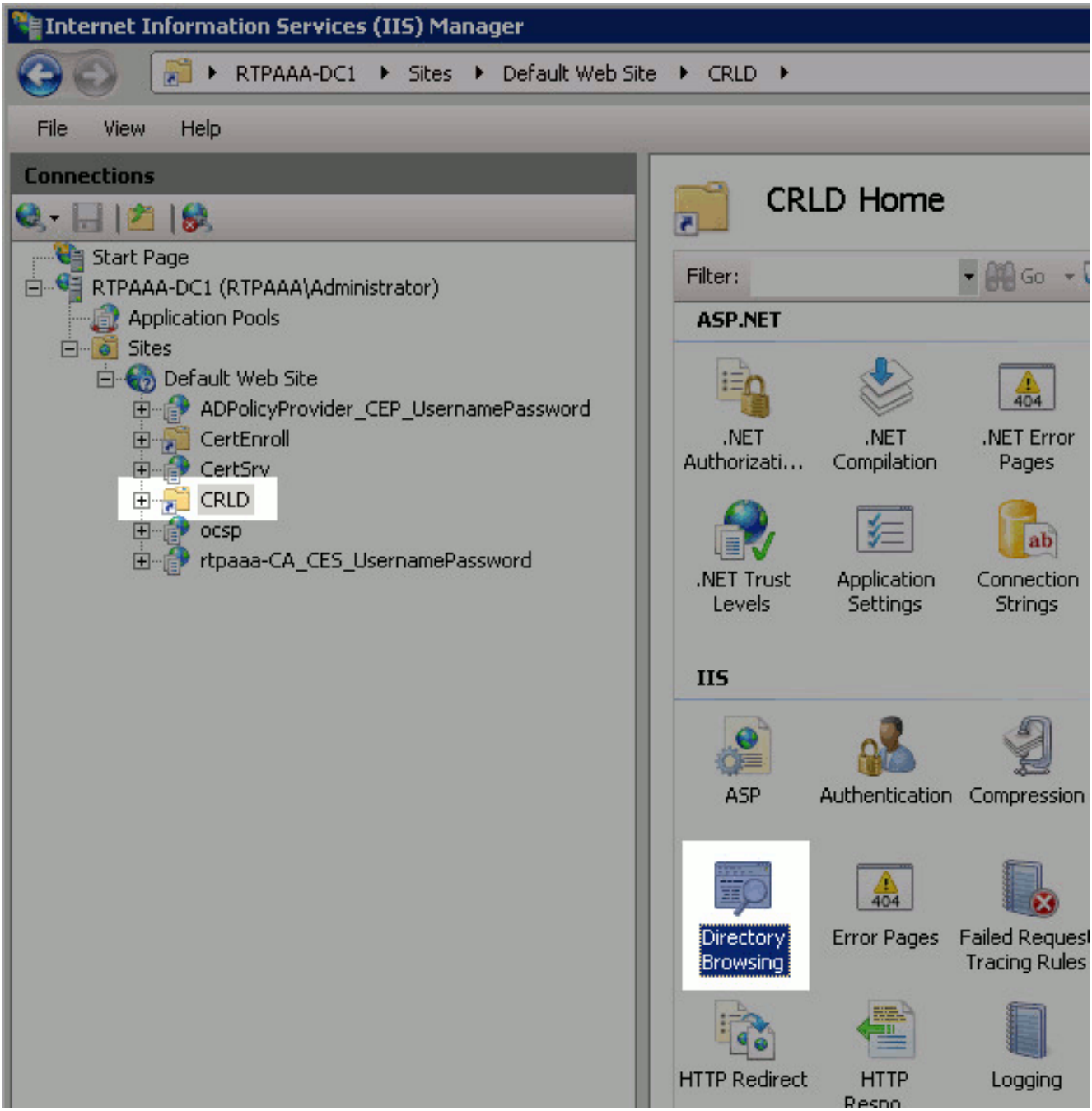
4. [Alias] フィールドに、CRL 分散ポイントのサイト名を入力します。 この例では、CRLD を入力します。



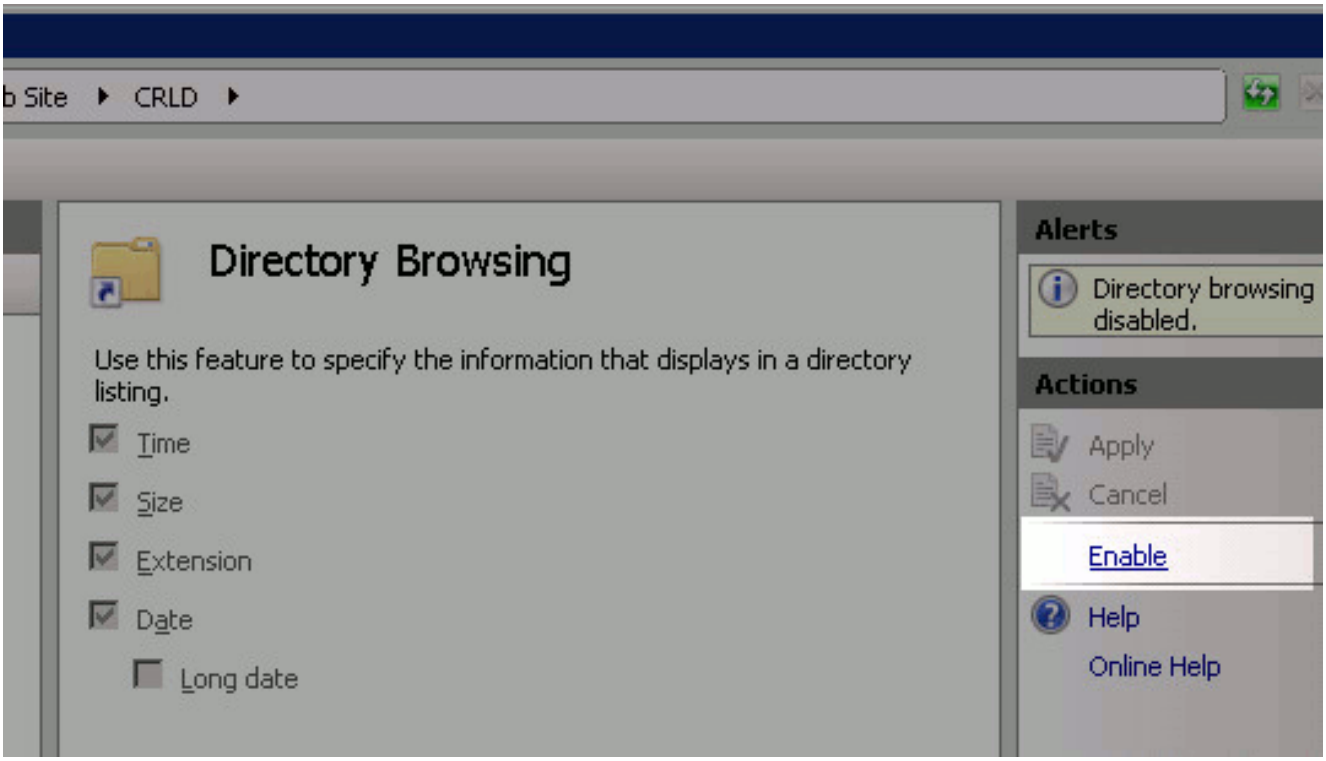
5. [Physical path] フィールドの右にある省略記号 ([…]) をクリックし、セクション 1 で作成したフォルダを表示します。フォルダを選択し、[OK] をクリックします。 [OK] をクリックして [Add Virtual Directory] ウィンドウを閉じます。



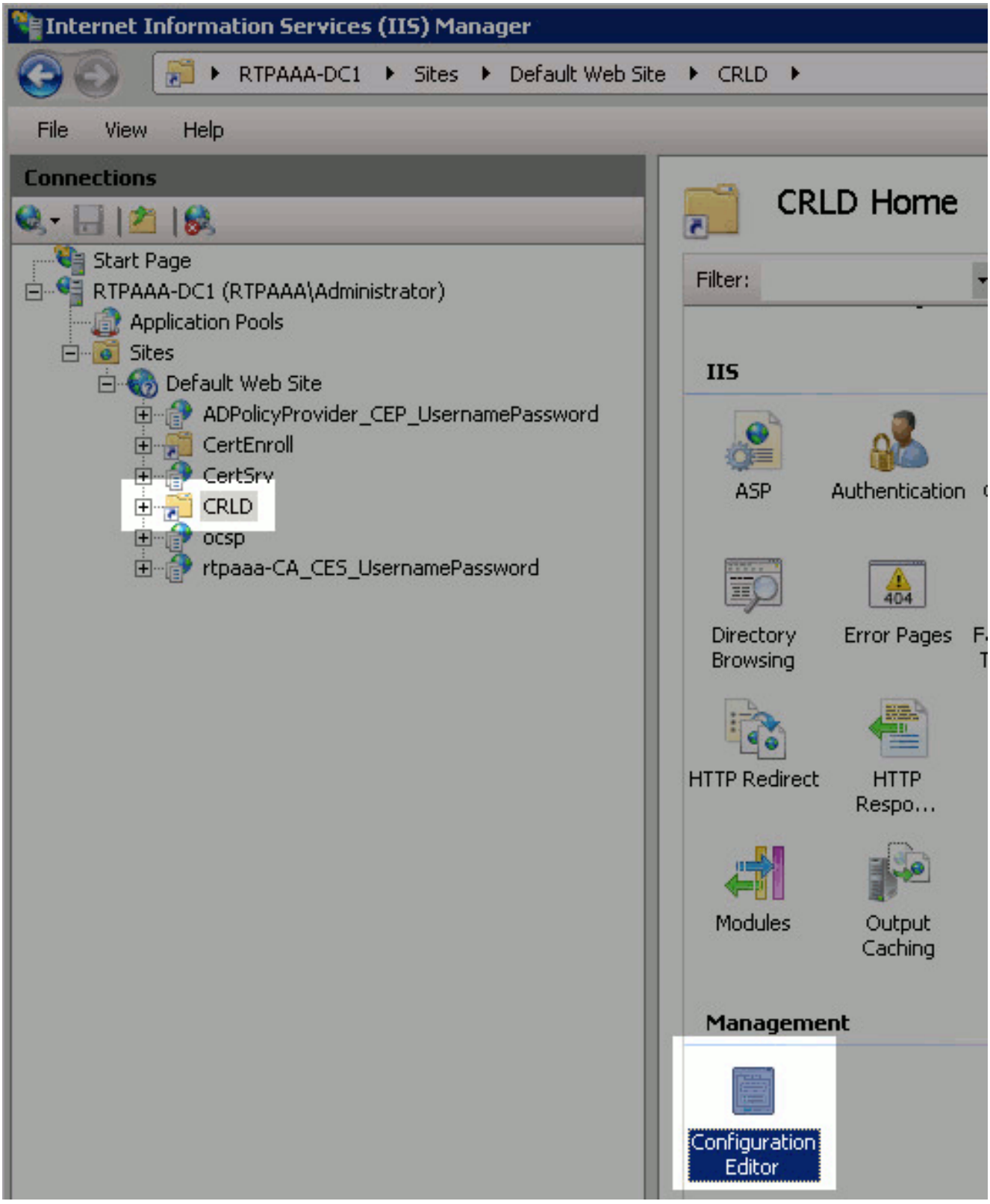
6. ステップ 4 で入力したサイト名が左側のペインで強調表示されています。 強調表示されていない場合は、ここで選択します。 中央のペインで、[Directory Browsing] をダブルクリックします。



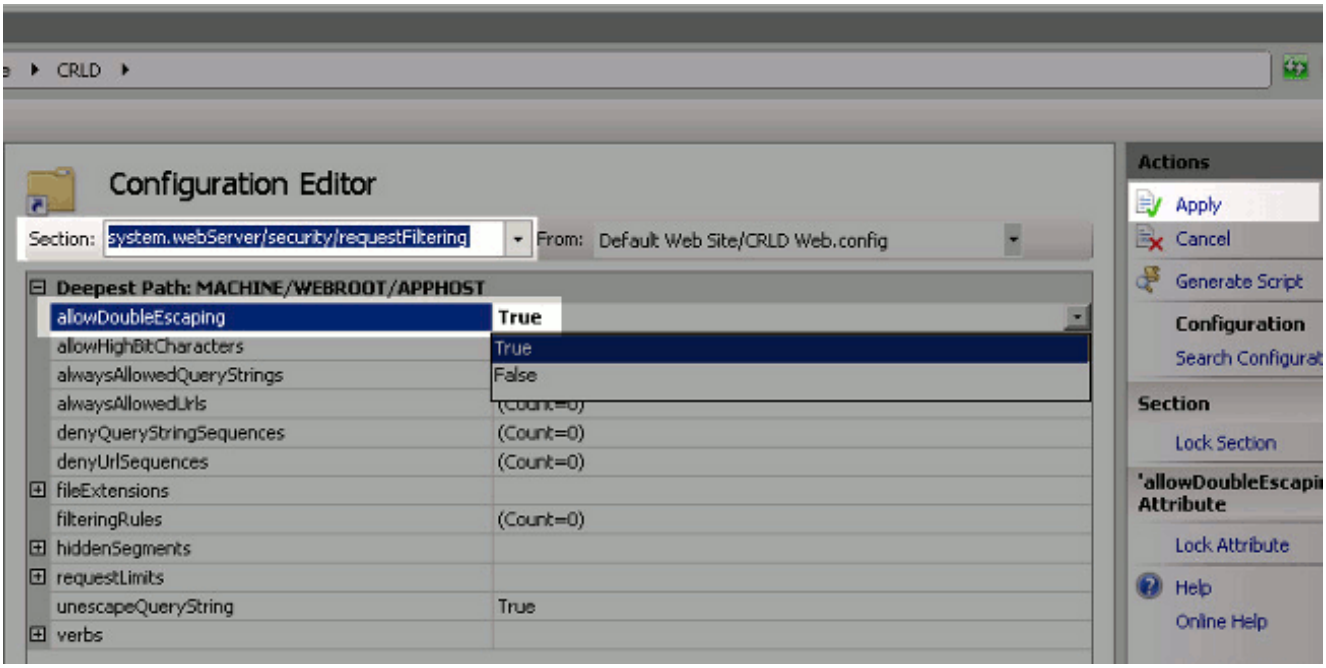
7. 右側のペインで、[Enable] をクリックしてディレクトリの参照をイネーブルにします。



8. 左側のペインで、サイト名をもう一度選択します。 中央のペインで、[Configuration Editor] をダブルクリックします。



9. [Section] 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。 右側のペインで [Apply] をクリックします。

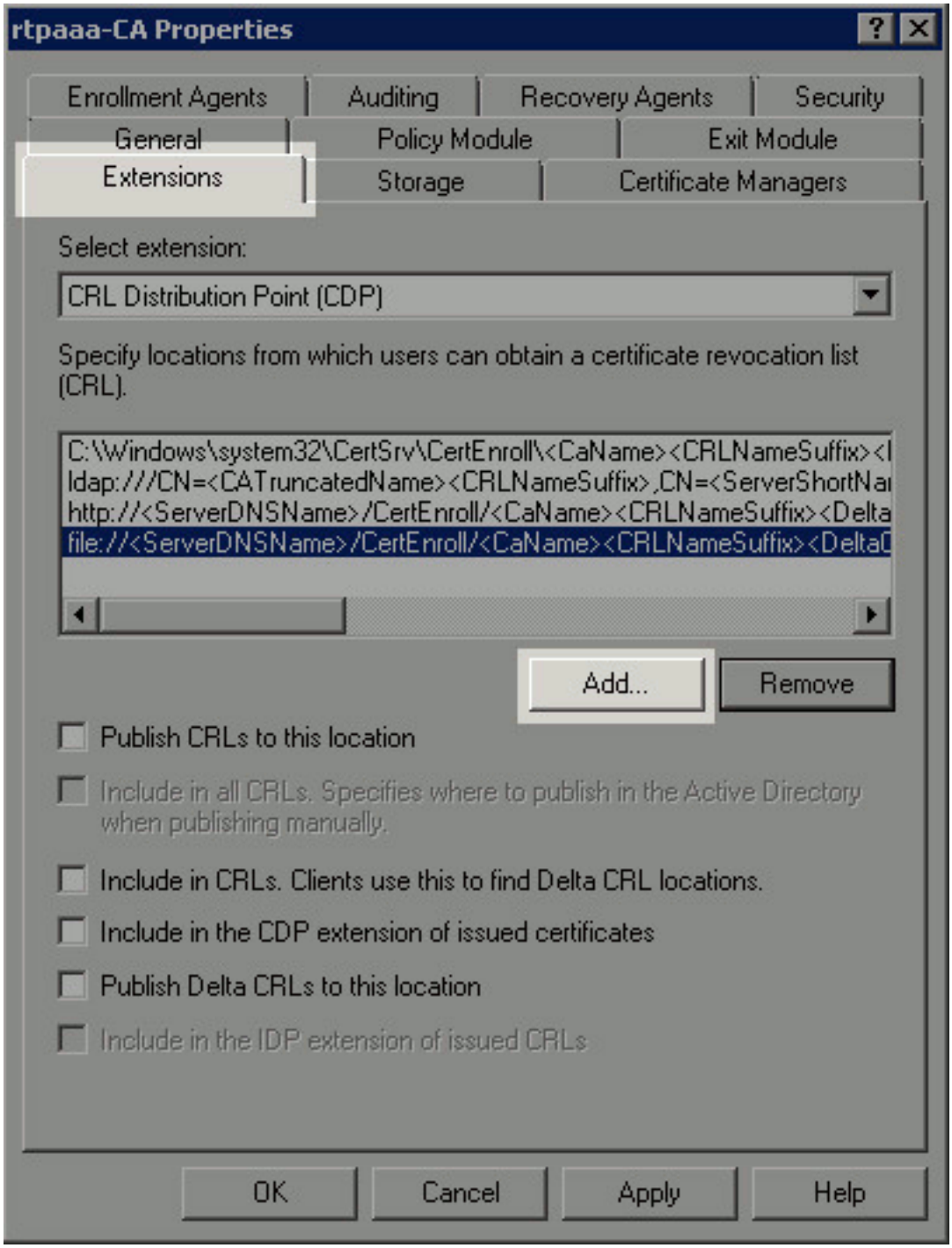


これで、フォルダは、IIS からアクセス可能になりました。

セクション 3. 分散ポイントに CRL ファイルを発行するように Microsoft CA サーバを設定する

これで、CRL ファイルを格納する新しいフォルダが設定され、このフォルダが IIS で公開されているため、新しい場所に CRL ファイルを発行するように Microsoft CA サーバを設定します。

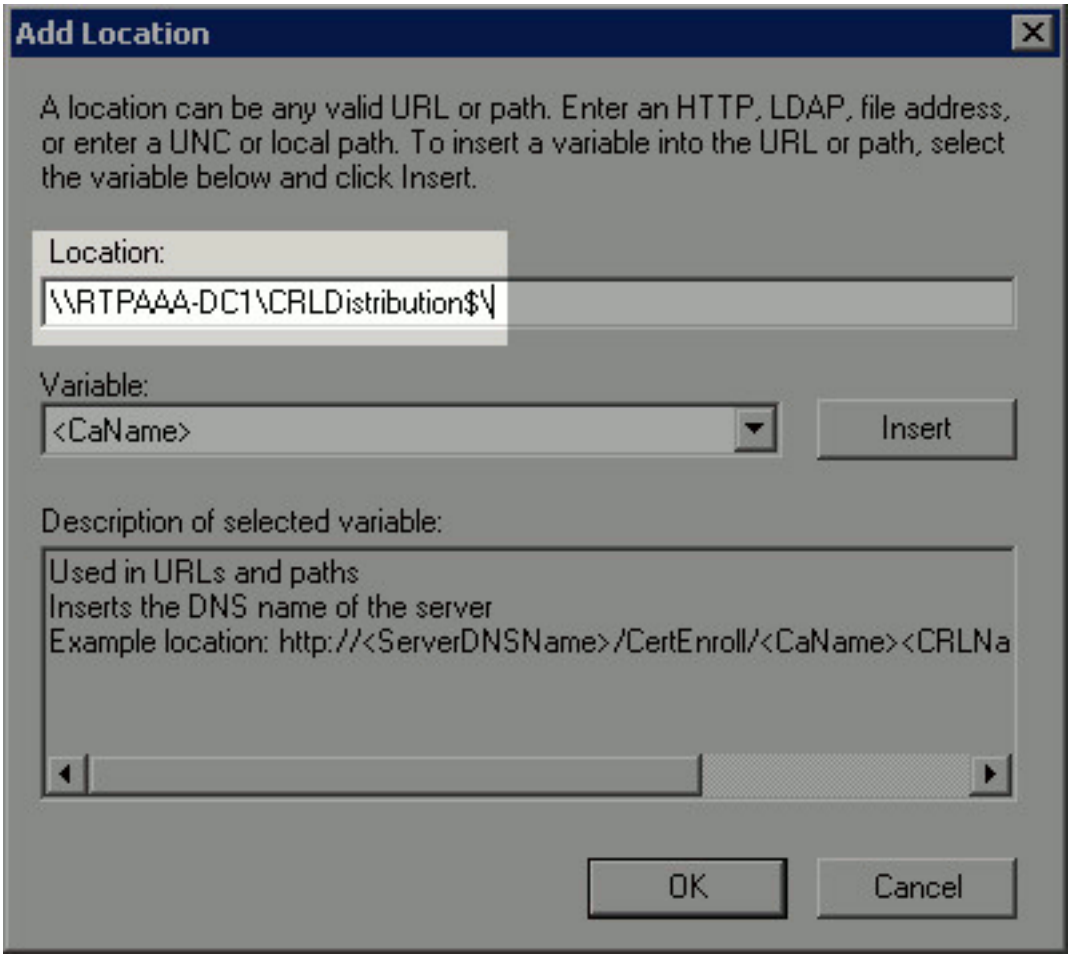
1. CA サーバ タスクバーで、[Start] をクリックします。 [Administrative Tools] > [Certificate Authority] を選択します。
2. 左側のペインで、CA の名前を右クリックします。 [Properties] を選択してから [Extensions] タブをクリックします。 新しい CRL 分散ポイントを追加するために、[Add] をクリックし



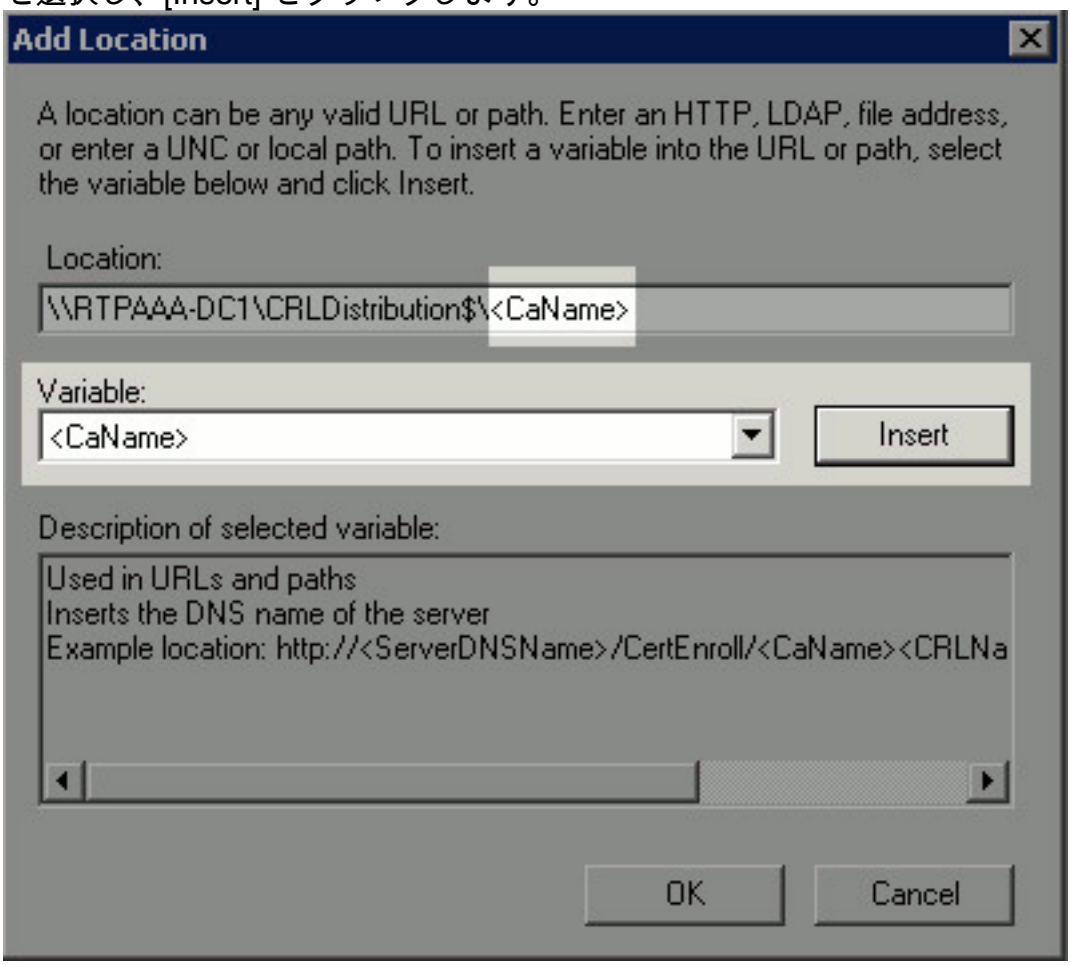
ます。

3. [Location] フィールドに、セクション 1 で作成して共有したフォルダのパスを入力します。セクション 1 の例で、パスは次のとおりです。

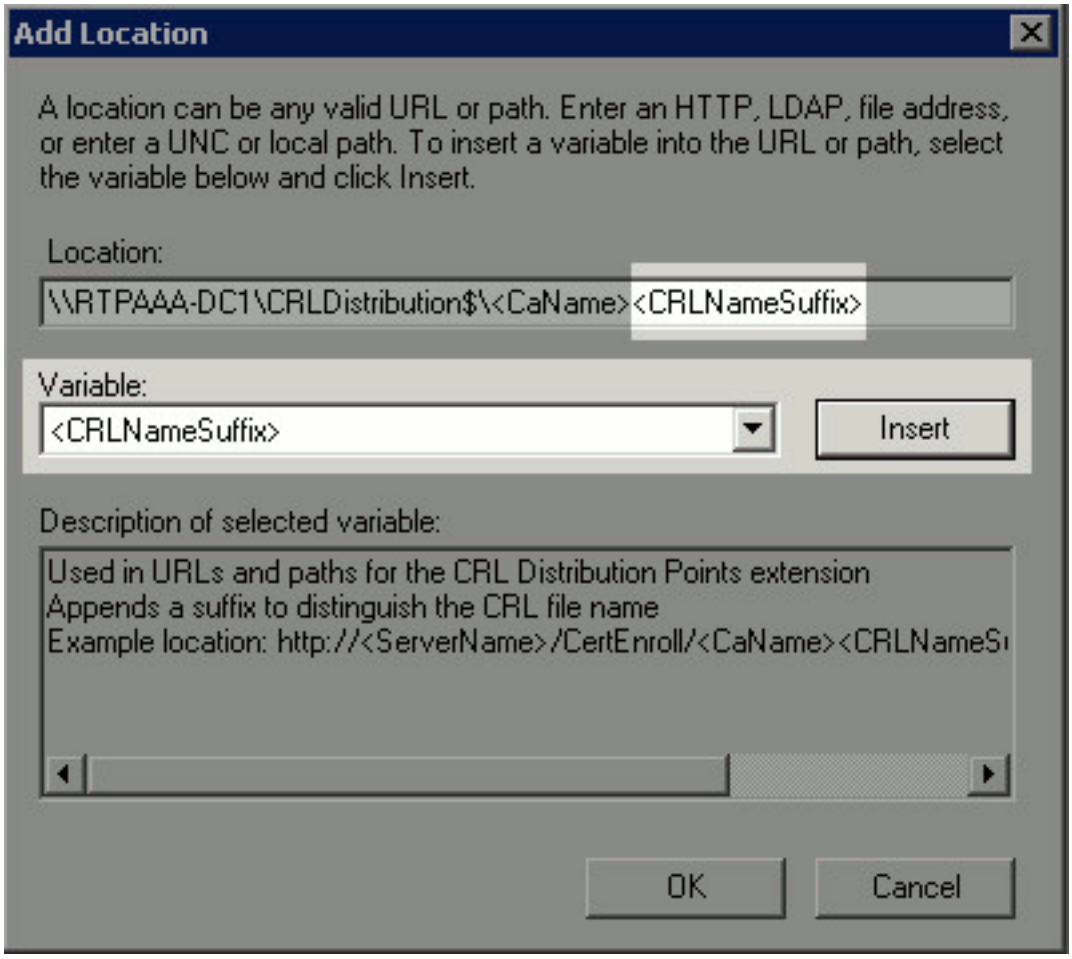
```
\\RTPAAA-DC1\CRLDistribution$\
```



4. [Location] フィールドに入力した状態で [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。



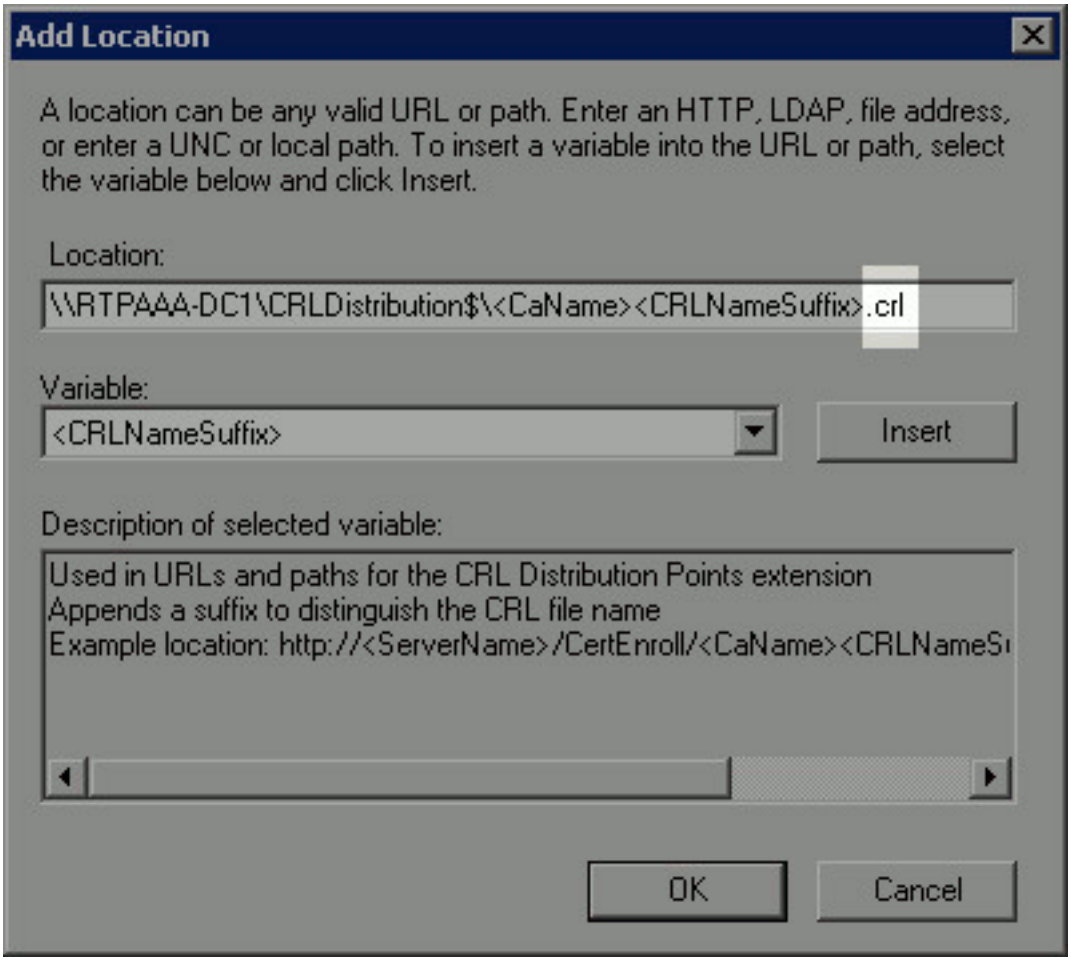
5. [Variable] ドロップダウン リストから、[<CRLNameSuffix>] を選択し、[Insert] をクリック



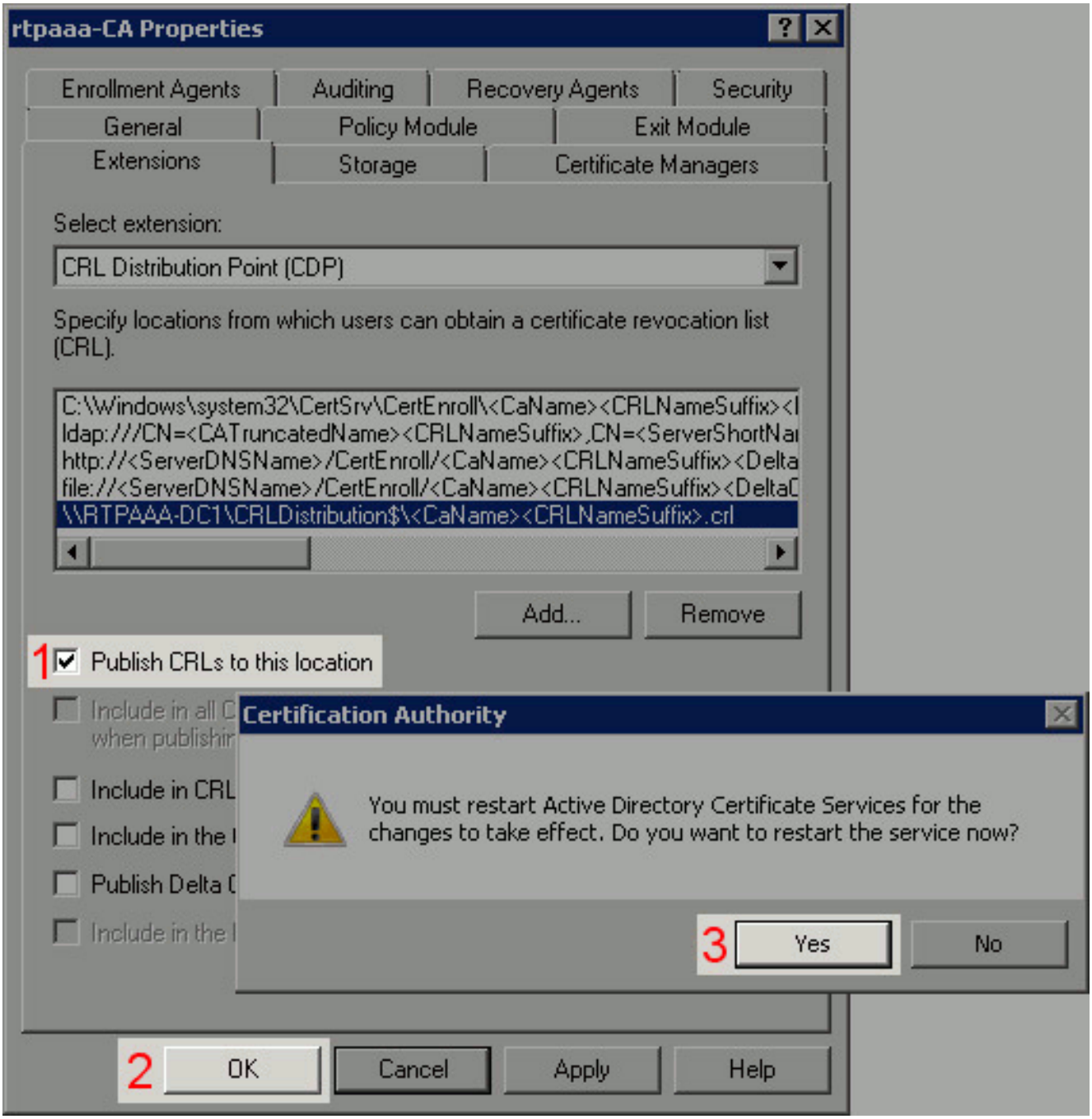
します。

6. [Location] 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] は次のとおりです。

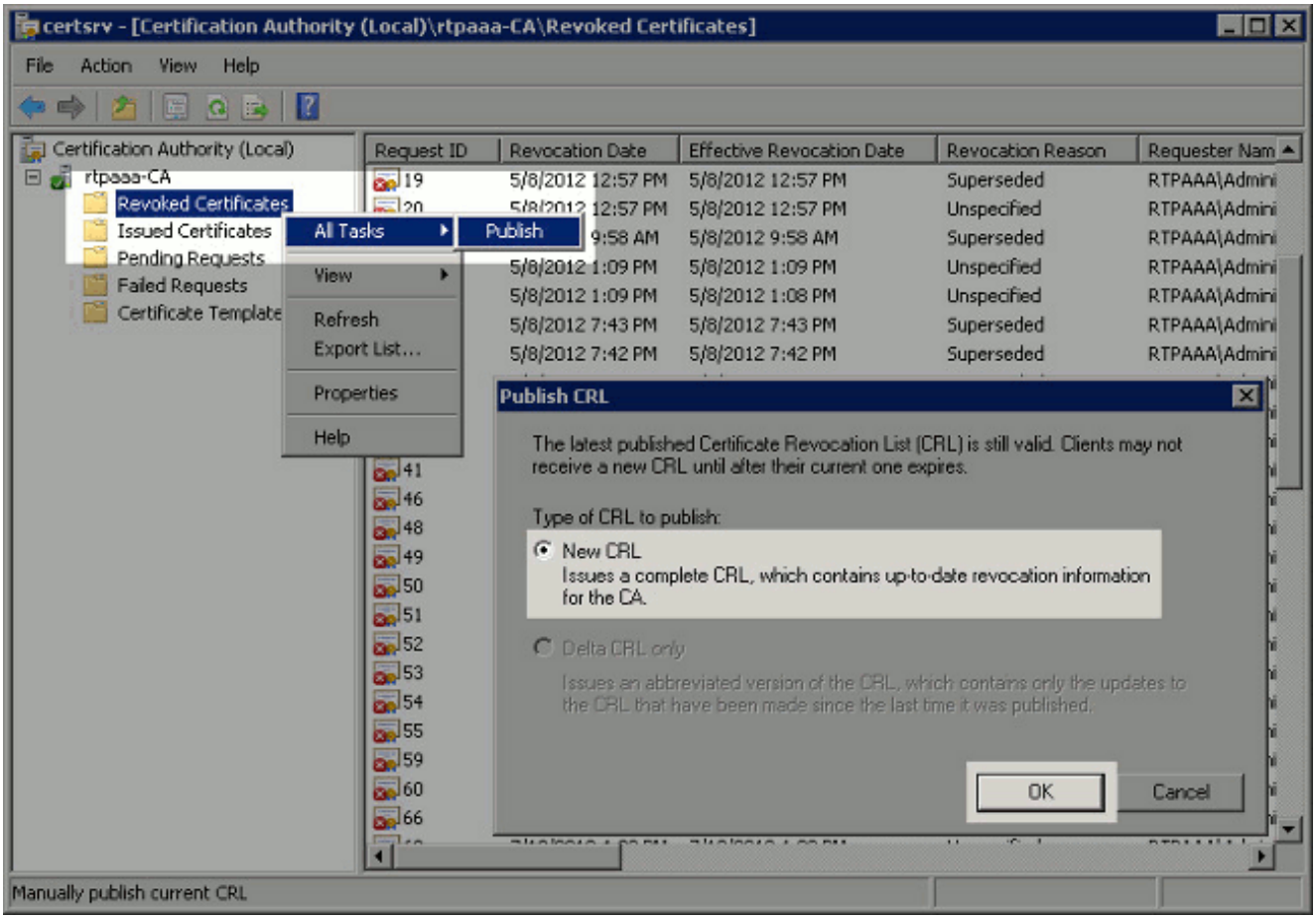
```
\\RTPAAA-DC1\CRLDistribution$\<CaName><CRLNameSuffix>.crl
```



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(1)をオンにしてから [OK] をクリック(2)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ためのアクセス許可を確認するメッセージが表示されます。 [Yes](3) 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。 新しい CRL が選択されていることを確認してから、[OK] をクリックします。

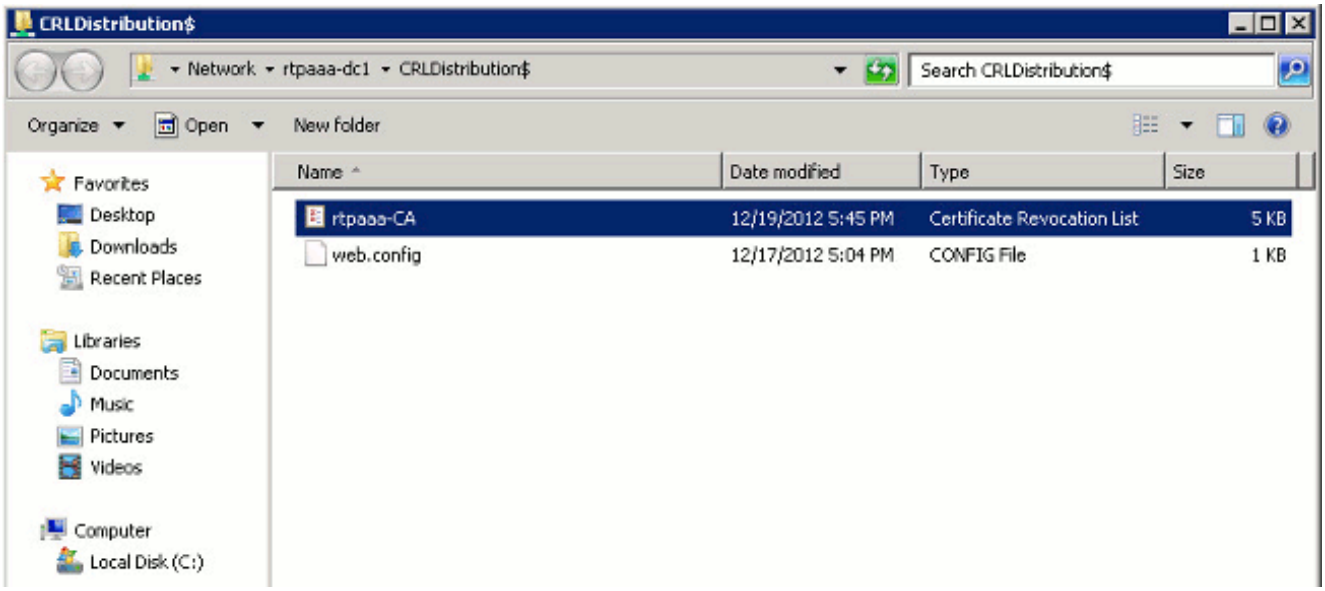


Microsoft CA サーバは、セクション 1 で作成したフォルダに新しい .crl ファイルを作成します。新しい CRL ファイルが正常に作成された場合は、[OK] をクリックした後にダイアログは表示されません。 新しい分散ポイント フォルダに関するエラーが戻る場合は、このセクションの各ステップを慎重に繰り返してください。

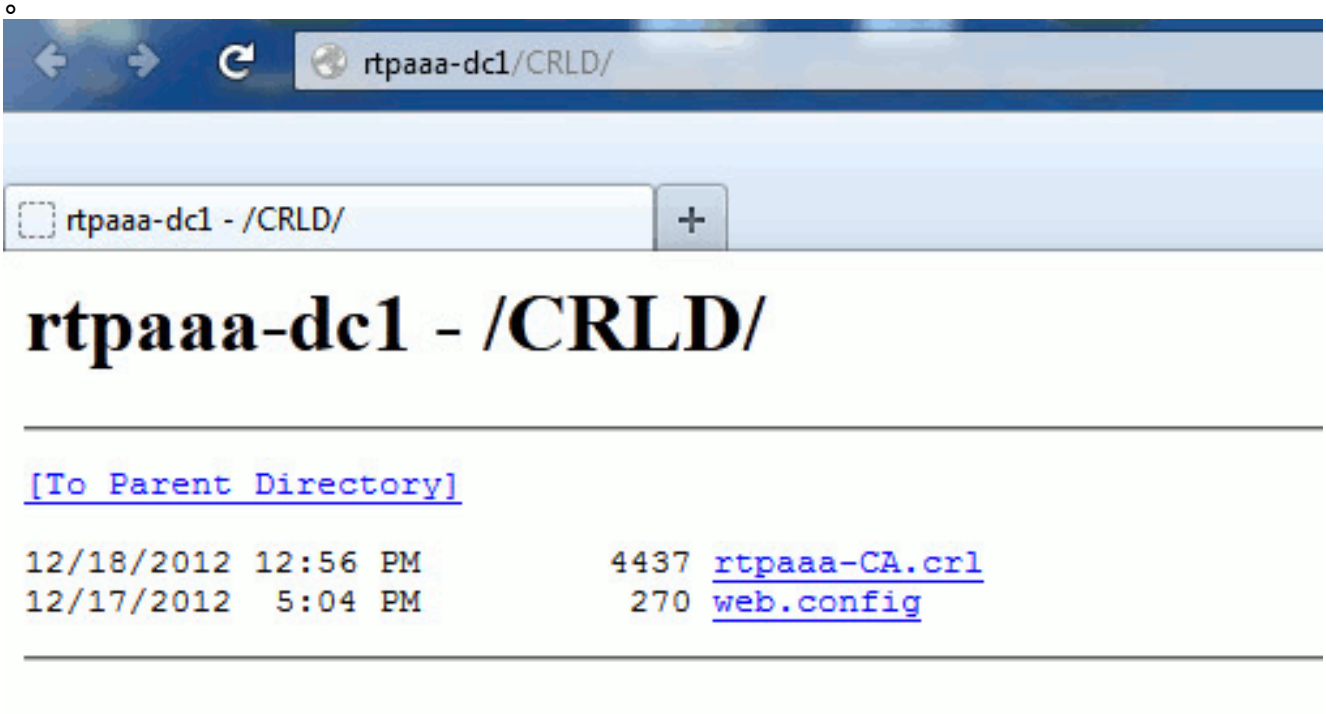
セクション 4. CRL ファイルが存在しており、IIS からアクセスできることを確認する

この手順を開始する前に、新しい CRL ファイルがあり、別のワークステーションから IIS を介してアクセス可能であることを確認します。

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。 <CANAME>.crl という形式の単一の .crl ファイルが存在しています。<CANAME> 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。
   `rtpaaa-CA.crl`



2. ネットワーク上のワークステーション（ISE のプライマリ管理ノードと同じネットワークであれば理想的）から、Web ブラウザを開き、http://<SERVER>/<CRLSITE> を表示します。ここで、<SERVER> は、セクション 2 で設定した IIS サーバのサーバ名、<CRLSITE> は、セクション 2 で分散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://RTPAAA-DC1/CRLD`
ディレクトリ インデックスが表示され、ステップ 1 で確認したファイルが含まれています。

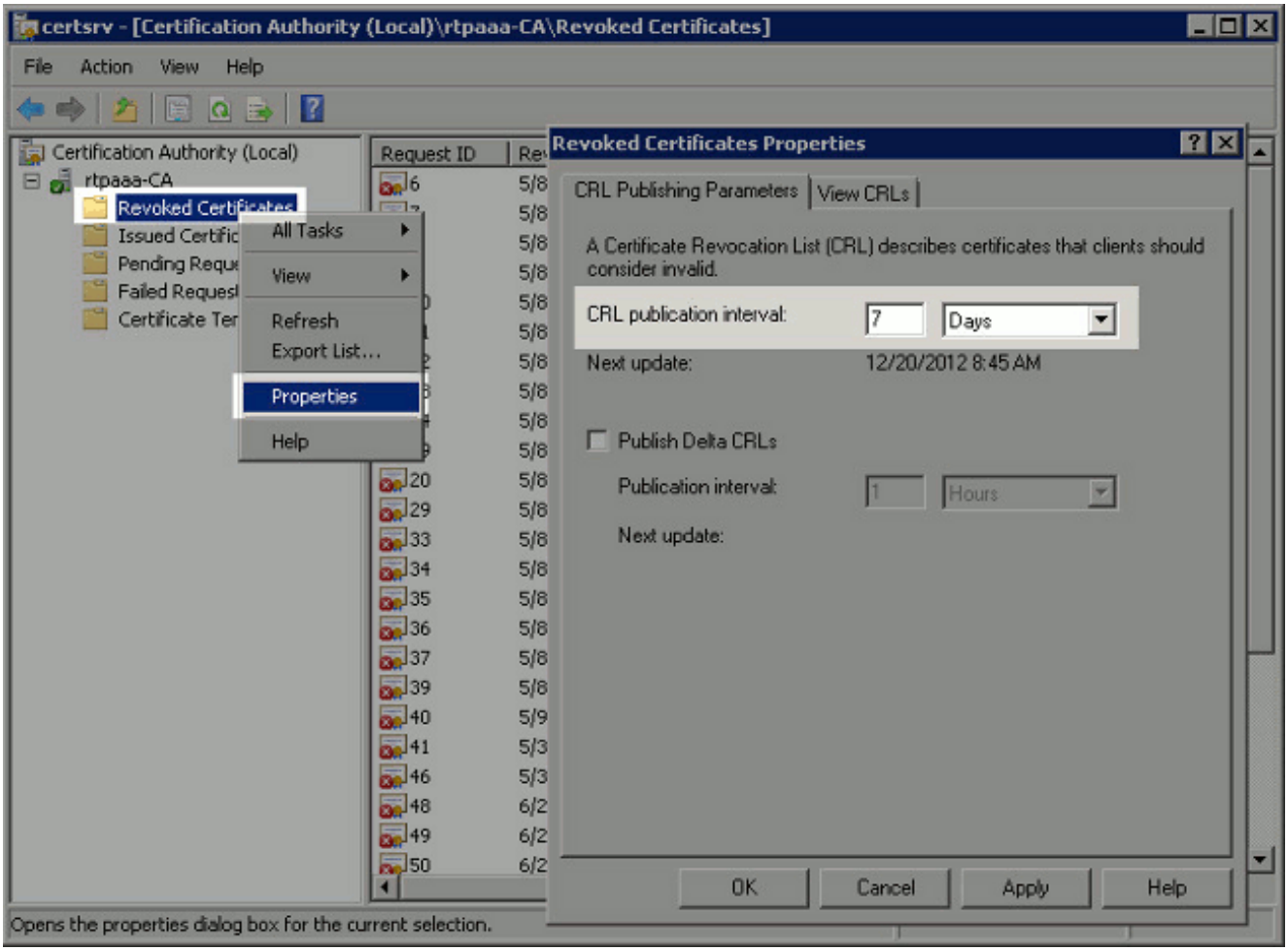


セクション 5. 新しい CRL 分散ポイントを使用するように、ISE を設定する

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。 この間隔を設定するための戦略は、このドキュメントの範囲外です。 有効な値（Microsoft CA の場合）は、1 時間以上から 411 年以下です。 デフォルト値は 1 週間です。 環境に適した間隔が決まったら、以下の手順に従って間隔を設定します。

1. CA サーバ 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 の発行間隔のフィールドで、必要な数値を入力し、期間を選択します。 ウィンドウを閉じて変更を適用するために、[OK] をクリックします。 この例では、発行間隔 7 日を設定しています。



ここで、いくつかのレジストリ値を確認する必要があります。これらは、ISE での CRL 取得設定を判別するために役立ちます。

4. ClockSkew 値を確認するために **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ために **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、手動で値が設定されていないことを示します。 この値が 0 以外の場合は、値および単位を記録します。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 を確認するために **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.
```

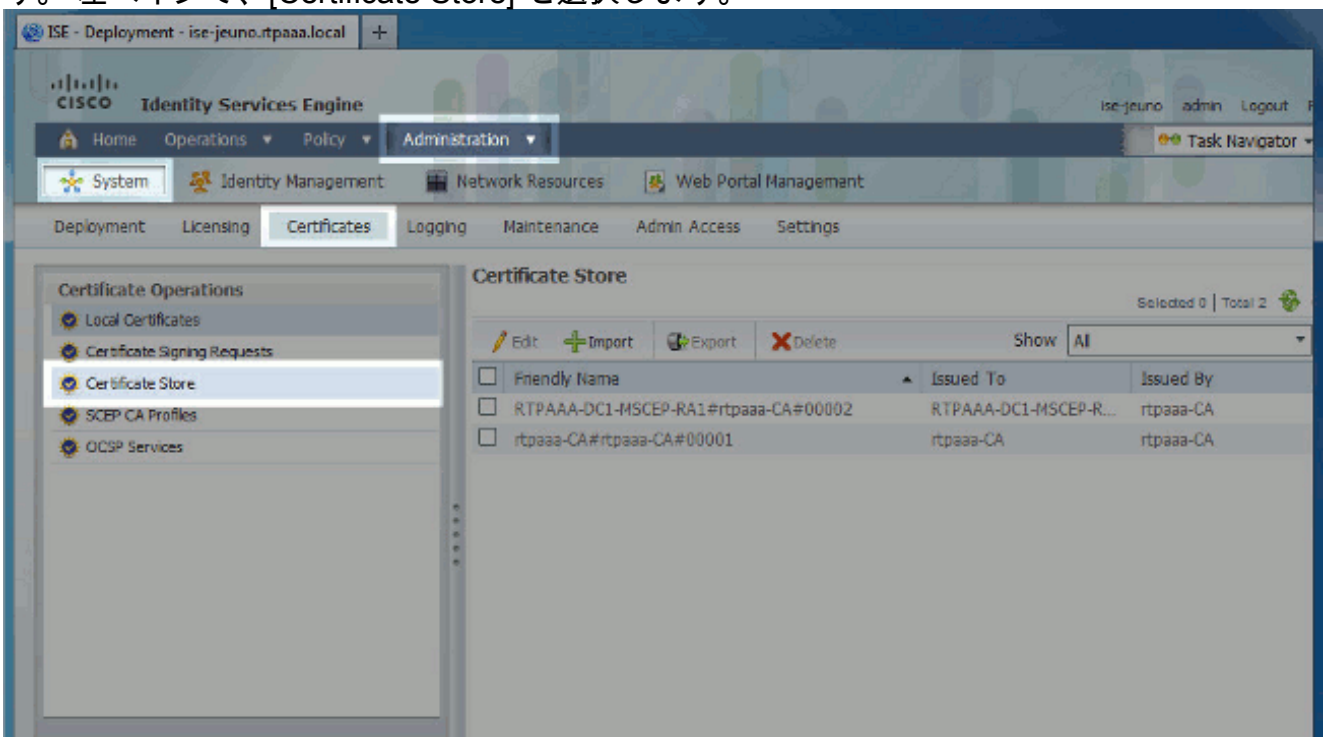
7. 次のように、CRL の猶予期間を計算します。CRLOverlapPeriod をステップ 5 で設定した場合 OVERLAP = CRLOverlapPeriod（分）その他の場合 OVERLAP = (CRLPeriod / 10)（分）OVERLAP > 720 の場合、OVERLAP = 720OVERLAP < (1.5 * ClockSkewMinutes) の場合、OVERLAP = (1.5 * ClockSkewMinutes)OVERLAP > CRLPeriod（分）の場合、OVERLAP = CRLPeriod（分）猶予期間 = 720 分 + 10 分 = 730 分例：

```
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
```

計算された猶予期間は、CA が次の CRL を発行する時点から現在の CRL が失効する時点までの時間です。 CRL を適宜取得するように ISE を設定する必要があります。

8. プライマリ管理ノードにログインし、[Administration] > [System] > [Certificates] を選択します。 左ペインで、[Certificate Store] を選択します。



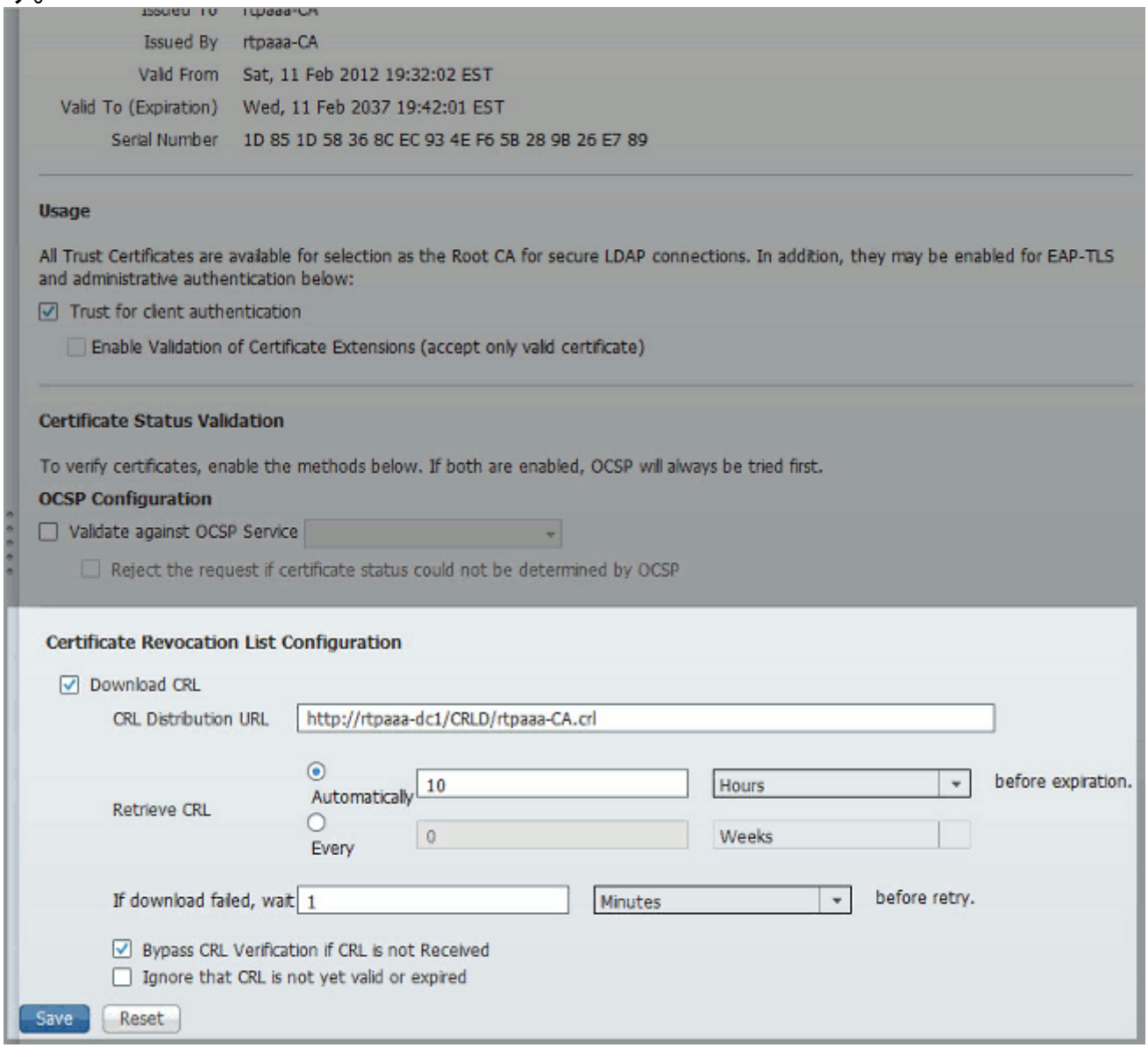
9. CRL を設定する CA 証明書の横にある [Certificate Store] チェック ボックスをオンにします。 [Edit] をクリックします。
10. ウィンドウの下部にある、[Download CRL] チェック ボックスをオンにします。
11. [CRL Distribution URL] フィールドに、CRL 分散ポイントのパスを入力します。ここに、セクション 2 で作成した .crl ファイルがあります。 この例では、URL は次のとおりです。

```
http://RTPAAA-DC1/CRLD/rtpaaa-ca.crl
```

12. ISE は一定の間隔によってか、有効期限（これも通常は一定間隔）によって CRL を取得するように設定できます。 CRL の発行間隔が固定の場合は、後者のオプションのほうが CRL のアップデートをタイムリーに取得できます。 [Automatically] オプション ボタンをクリックします。
13. 取得のための値にステップ 7 で計算した猶予期間よりも短い値を設定します。 設定する値が猶予期間を超えている場合、ISE では、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、算出した猶予期間は 730 分、つまり 12 時間 10 分で

す。 取得のための値には 10 時間を使用します。

14. 環境に応じた再試行間隔を設定します。 ISE では前のステップで設定した間隔で CRL を取得できない場合、この短い間隔で再試行します。
15. 直近のダウンロード試行で ISE がこの CA の CRL を取得できなかった場合に、証明書ベースの認証が正常に進む（CRL の検査も行わない）ように、[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 ボックスがオンでない場合、この CA によって発行された証明書によるすべての証明書ベースの認証は、CRL が取得できないと失敗します。
16. [Ignore that CRL is not yet valid or expired] チェック ボックスをオンにして、期限切れ（またはまだ有効でない）CRL ファイルを有効として ISE で使用できるようにします。 このチェック ボックスがオンでない場合、ISE では、有効日よりも前および次回アップデート時刻よりも後の CRL を無効であると見なします。 [Save] をクリック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。

トラブルシューティング

現在のところ、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。

関連情報

- テクニカル サポートとドキュメント – Cisco Systems