

配置Microsoft CA伺服器以發佈ISE的證書吊銷清單

目錄

[簡介](#)

[必備條件](#)

[需求](#)

[採用元件](#)

[設定](#)

[在CA上建立並配置資料夾以容納CRL檔案](#)

[在IIS中建立網站以公開新的CRL分發點](#)

[配置Microsoft CA伺服器以將CRL檔案發佈到分發點](#)

[驗證CRL檔案存在且可通過IIS訪問](#)

[配置ISE以使用新的CRL分發點](#)

[驗證](#)

[疑難排解](#)

簡介

本文檔介紹運行Internet Information Services(IIS)以發佈證書吊銷清單(CRL)更新的Microsoft證書頒發機構(CA)伺服器的配置。還說明了如何配置思科身份服務引擎(ISE) (3.0及更高版本) 以檢索更新以用於證書驗證。可以將ISE配置為檢索它在證書驗證中使用的各種CA根證書的CRL。

必備條件

需求

本文件沒有特定需求。

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- 思科身分識別服務引擎版本3.0
- Microsoft Windows Server 2008 R2

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除 (預設) 的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

設定

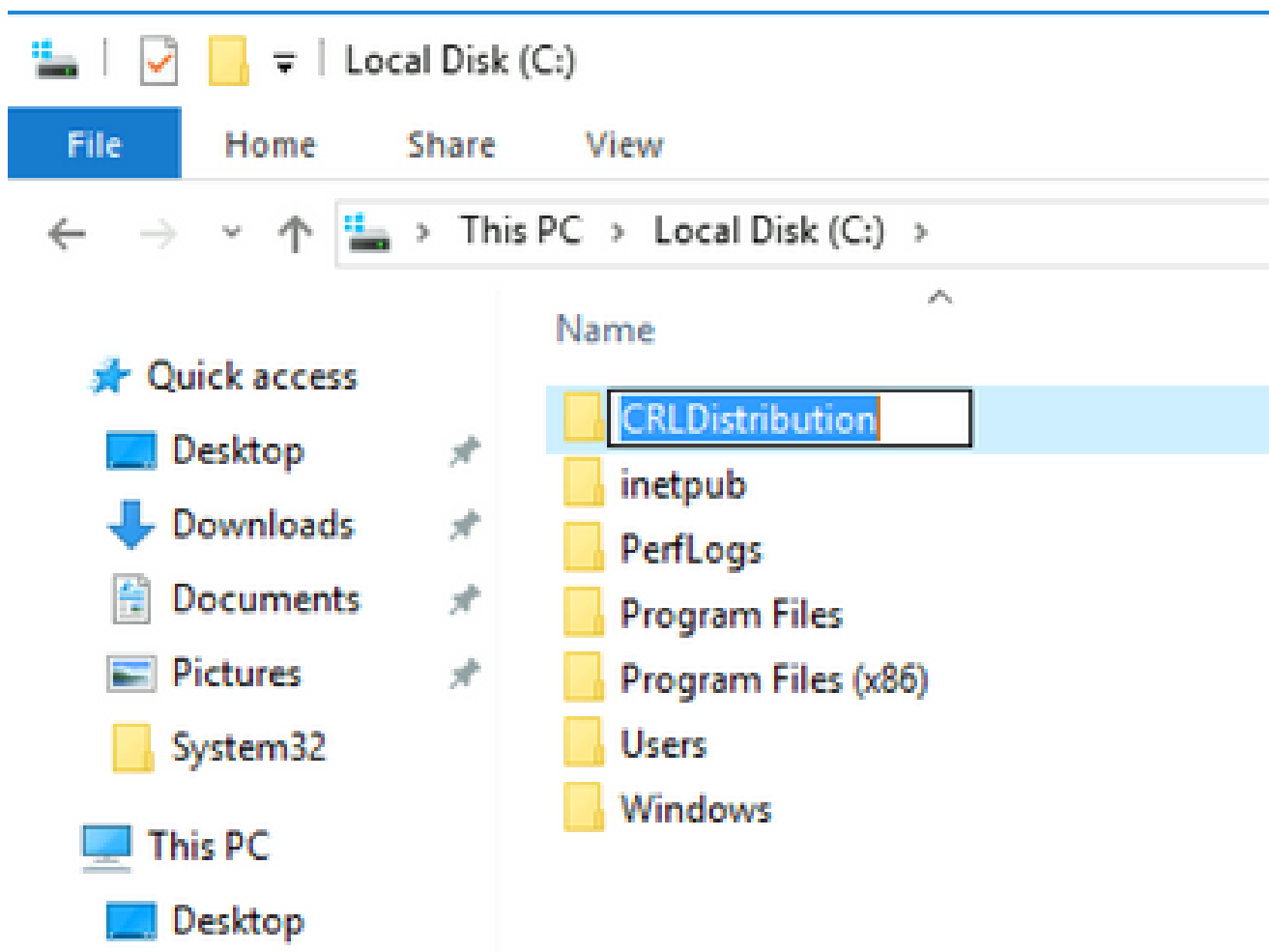
本節提供用於設定本文件中所述功能的資訊。

在CA上建立並配置資料夾以容納CRL檔案

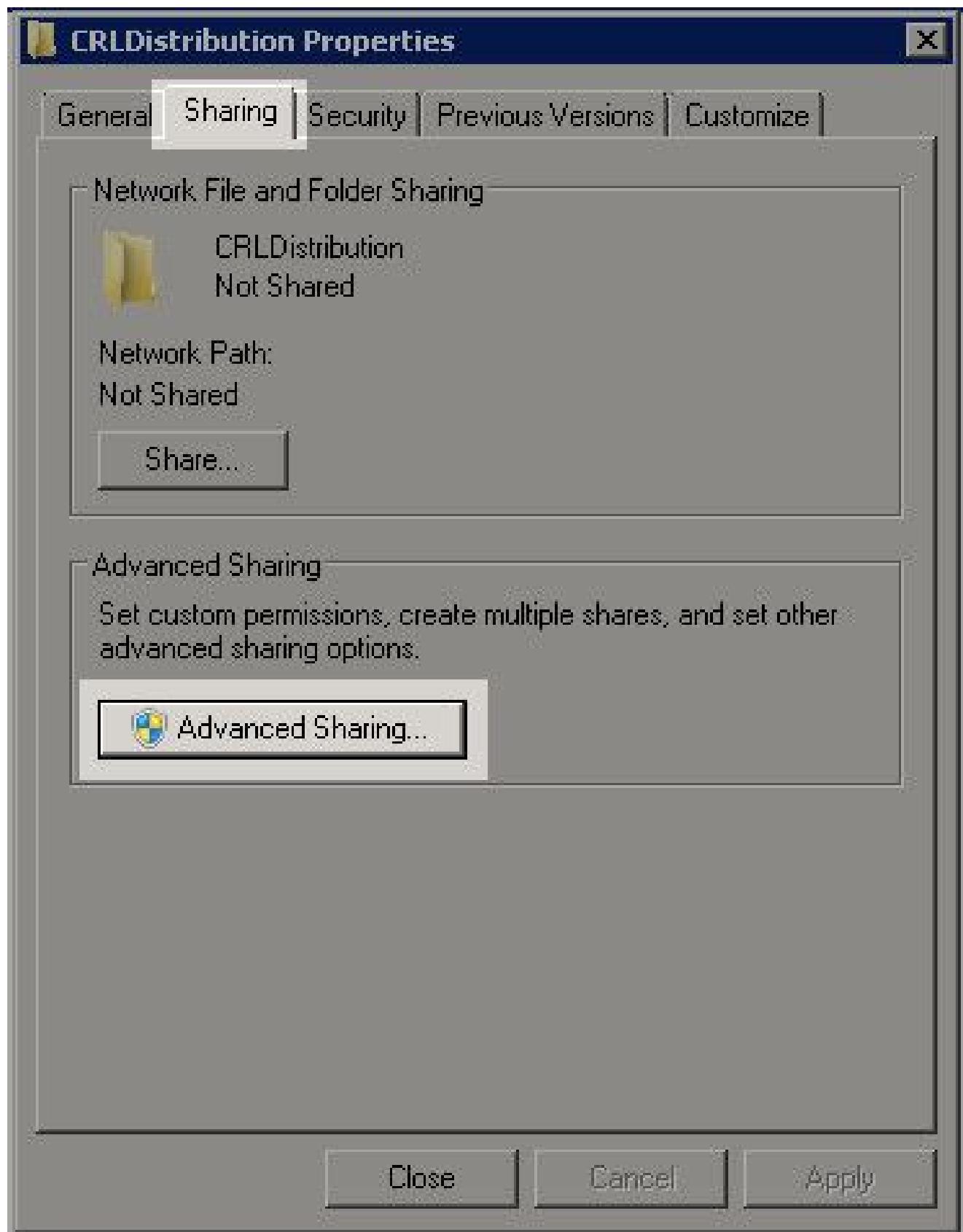
第一項任務是配置CA伺服器上的一個位置以儲存CRL檔案。預設情況下，Microsoft CA伺服器將檔案發佈到 `C:\Windows\system32\CertSrv\CertEnroll\`

不要使用此系統資料夾，而是為檔案建立一個新資料夾。

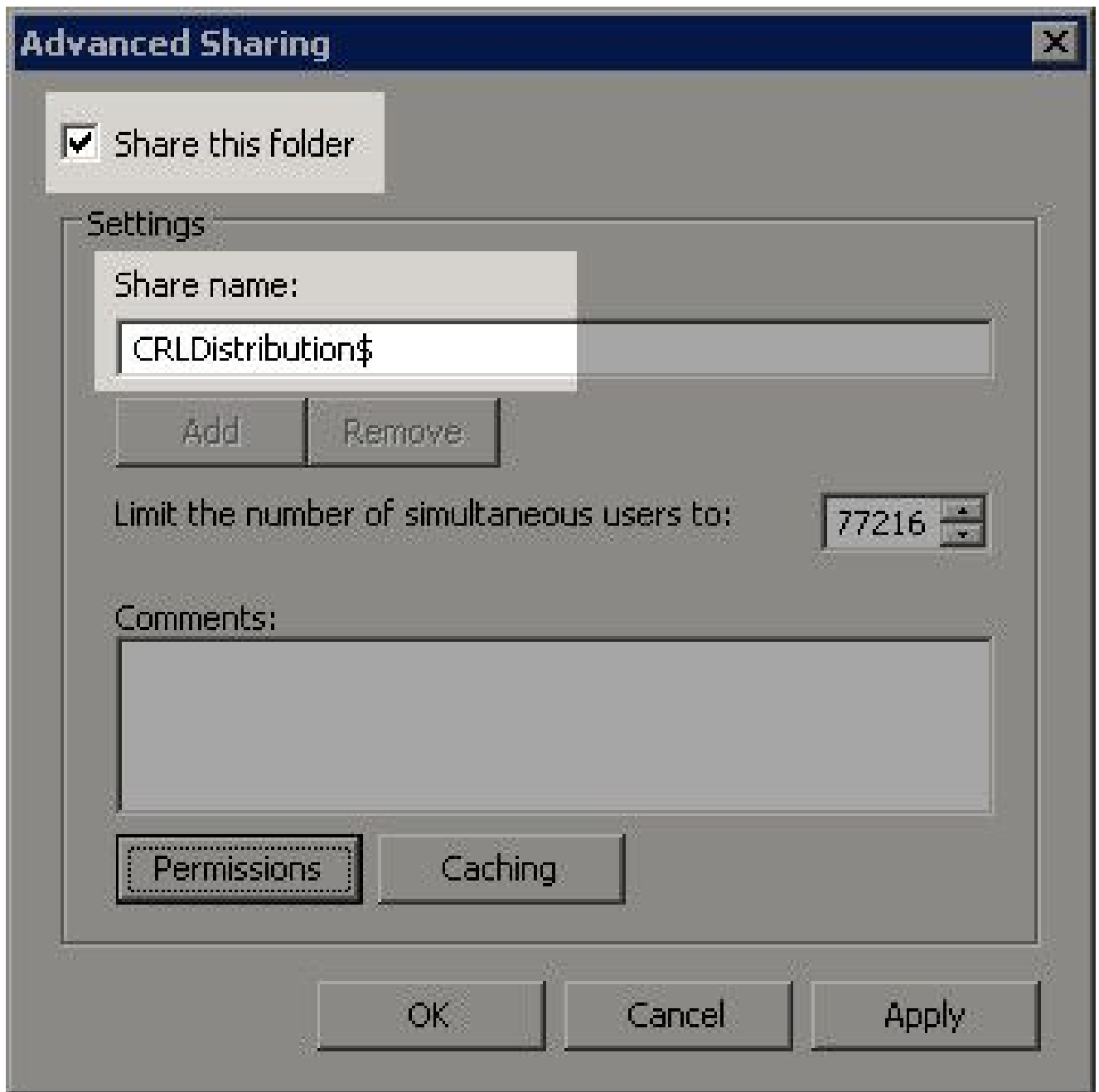
1. 在IIS伺服器上，選擇檔案系統上的位置並建立新資料夾。在此示例中，將建立 `C:\CRLDistribution` 資料夾。



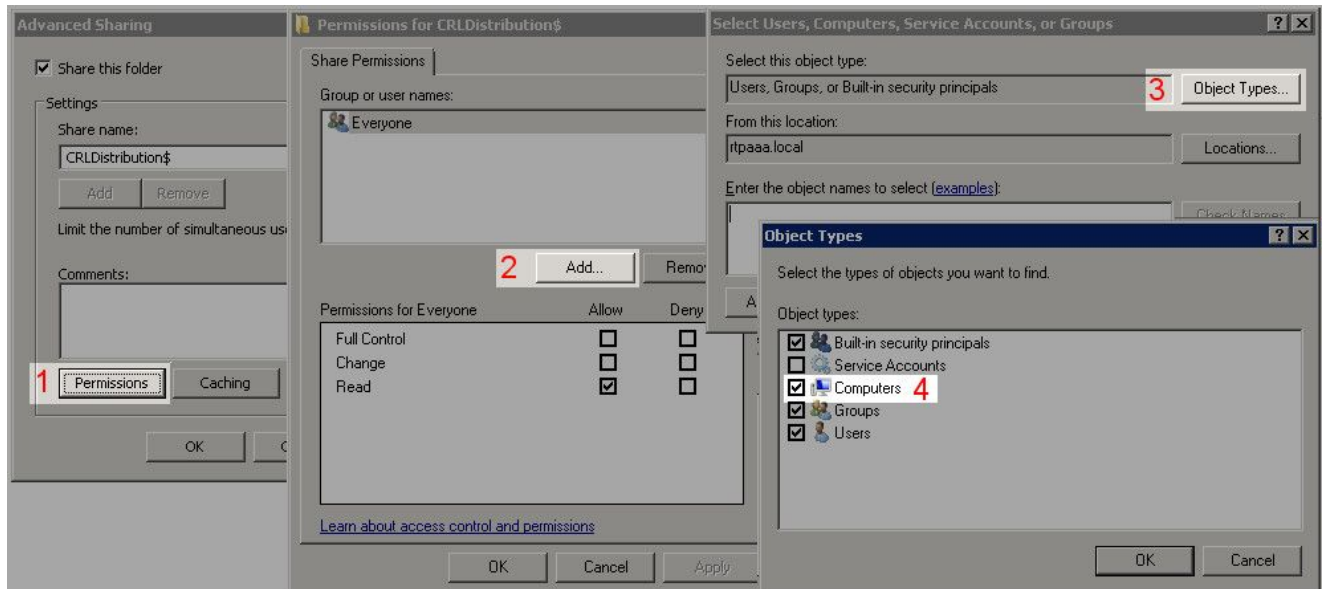
2. 為了使CA將CRL檔案寫入新資料夾，必須啟用共用。按一下右鍵新資料夾，選擇，Properties按一下該選Sharing項卡，然後按一下Advanced Sharing它。



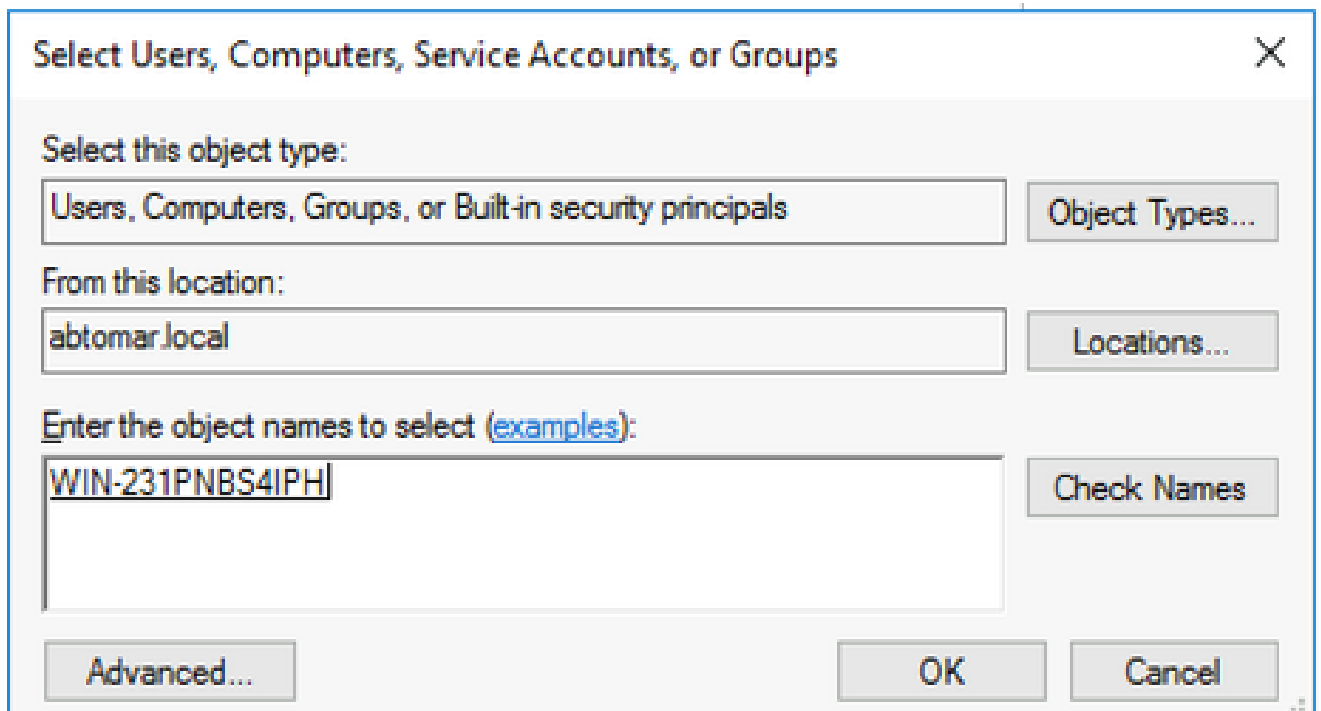
3. 若要共用資料夾，請選中此覈取方塊，然後在「共用名稱」欄位中為共用名稱末尾新增一個美元符號(\$)以隱藏共用Share this folder。



4. 單Permissions擊(1)，單Add擊(2)，單Object Types擊(3)，然後選中Computers覈取方塊(4)。



5. 要返回「選擇使用者」、「電腦」、「服務帳戶」或「組」視窗，請按一下OK。在「Enter the object names to select (輸入要選擇的對象名稱)」欄位中，在此示例中輸入CA伺服器的電腦名稱：WIN0231PNBS4IPH，然後單Check Names擊。如果輸入的名稱有效，該名稱將刷新並帶有下列線。按一OK下。



6. 在「組或使用者名稱」欄位中，選擇CA電腦。檢查Allow「完全控制」以授予對CA的完全訪問許可權。

按一OK下。再次OK按一下以關閉「高級共用」視窗並返回到「屬性」視窗。

Permissions for CRLDistribution\$



Share Permissions

Group or user names:

Everyone
WIN-231PNBS4IPH (ABTOMAR\WIN-231PNBS4IPH\$)

Add...

Remove

Permissions for
WIN-231PNBS4IPH

Allow

Deny

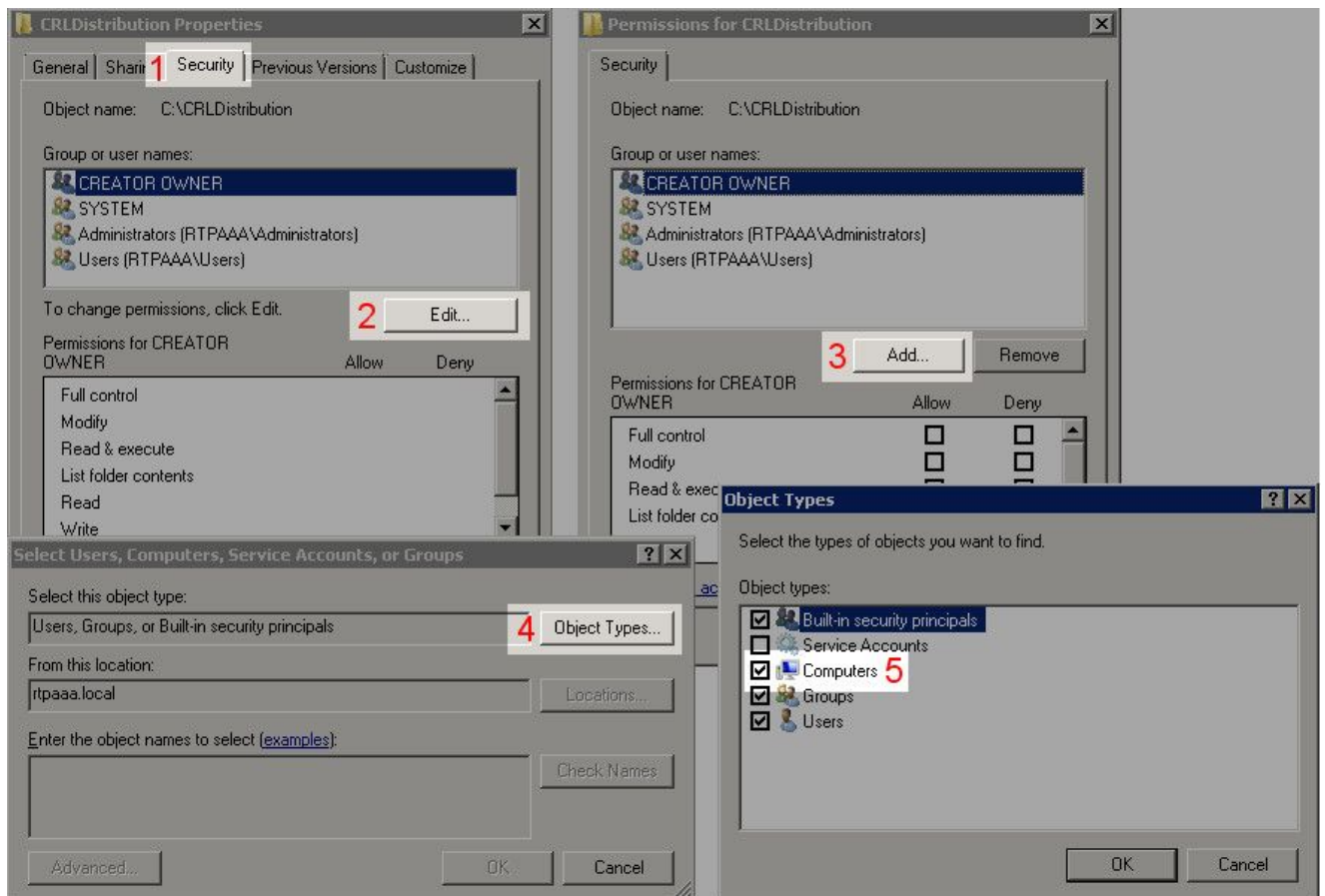
	Allow	Deny
Full Control	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Change	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Read	<input checked="" type="checkbox"/>	<input type="checkbox"/>

OK

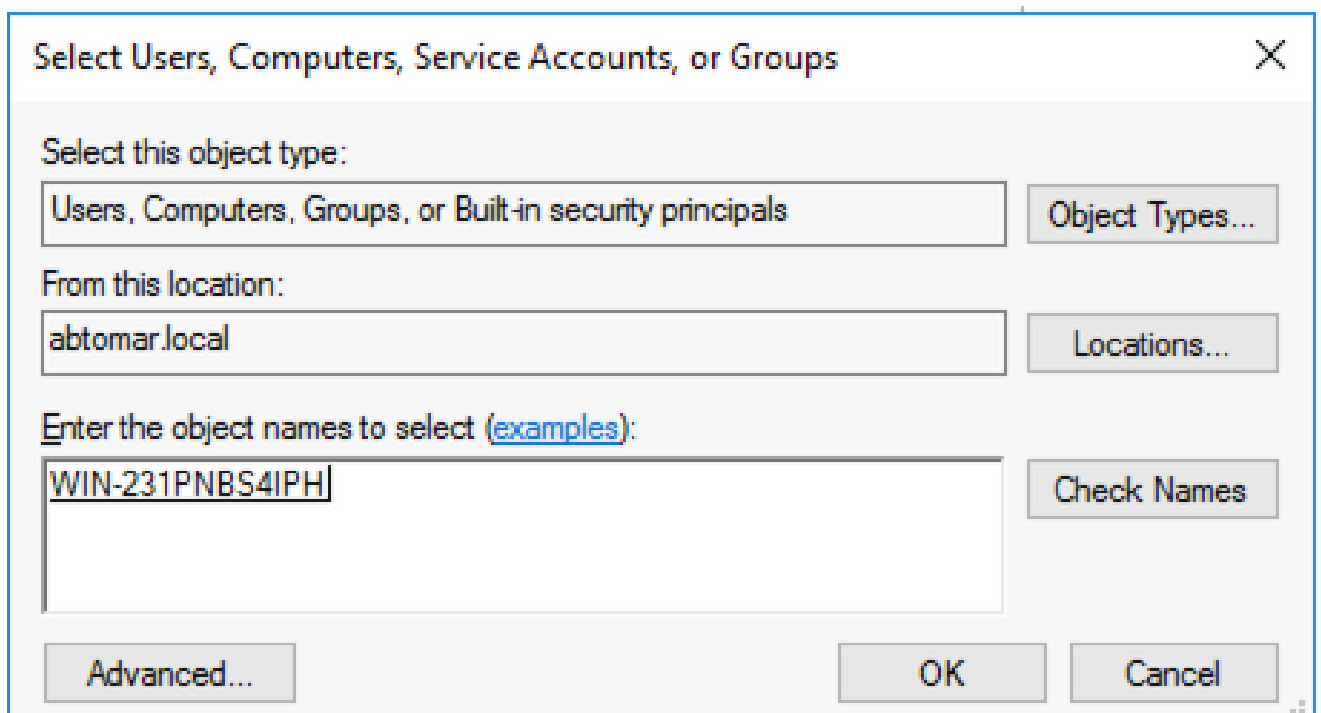
Cancel

Apply

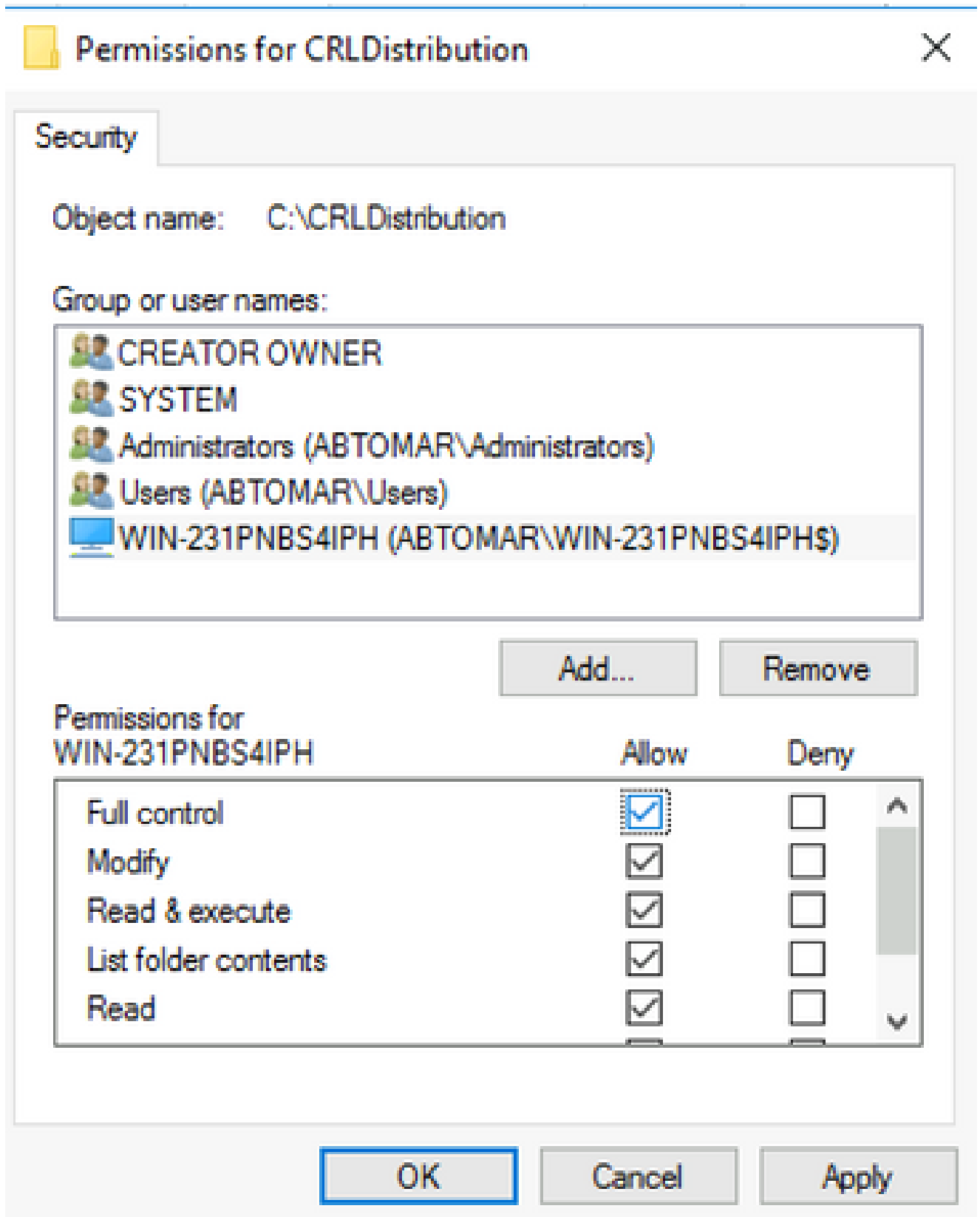
7. 為了允許CA將CRL檔案寫入新資料夾，請配置相應的安全許可權。按一下Security(1)，按一下>Edit(2)，按一下>Add(3)，按一下Object Types(4)，然後選中Computers覈取方塊(5)。



8. 在輸入要選擇的對象名稱欄位中，輸入CA伺服器的電腦名稱，然後單Check Names擊。如果輸入的名稱有效，該名稱將刷新並帶有下列劃線。按一下OK下。



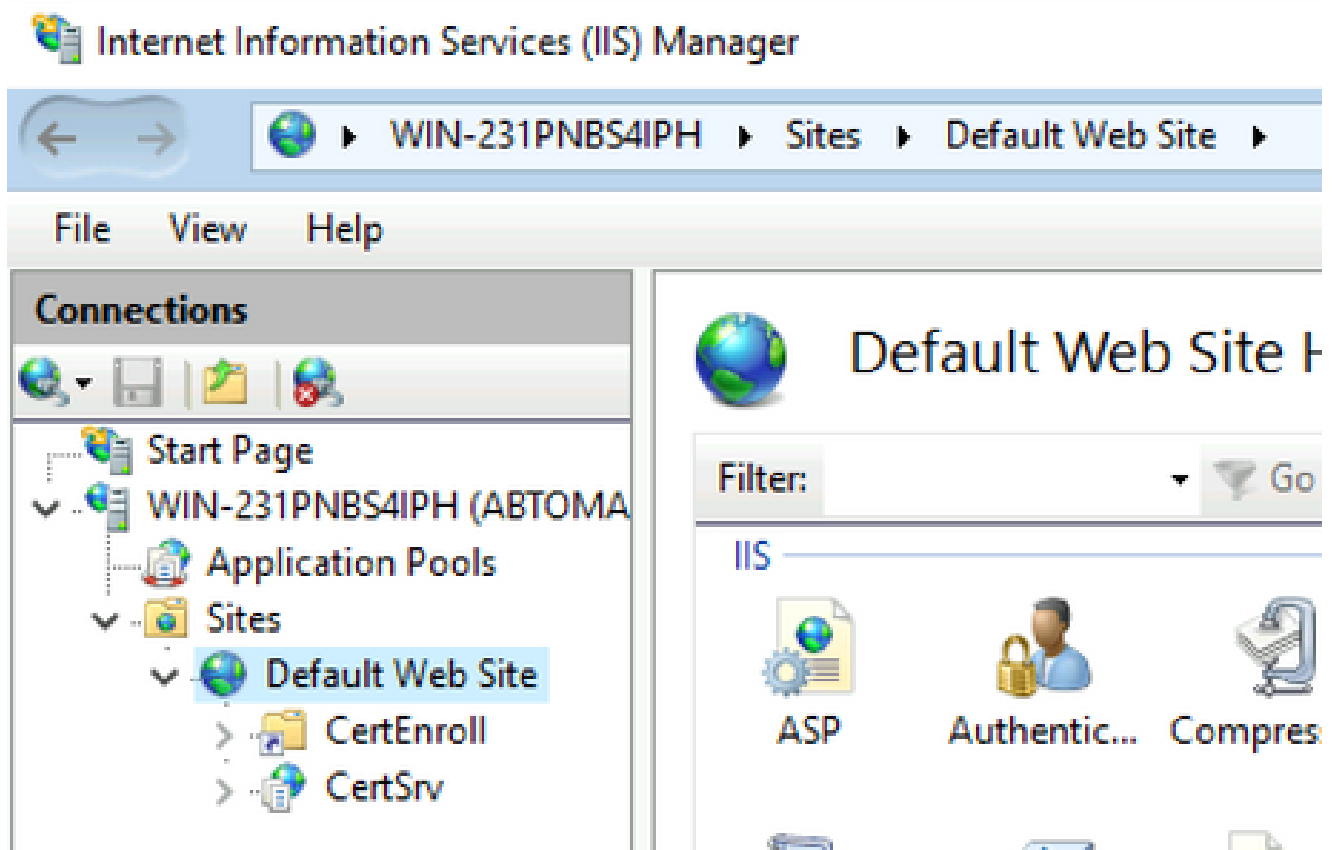
9. 在「組或使用者名稱」欄位選擇CA電腦，然後檢查「Allow完全控制」以授予對CA的完全訪問許可權。按一下OK，然後按一下Close以完成任務。



在IIS中建立網站以公開新的CRL分發點

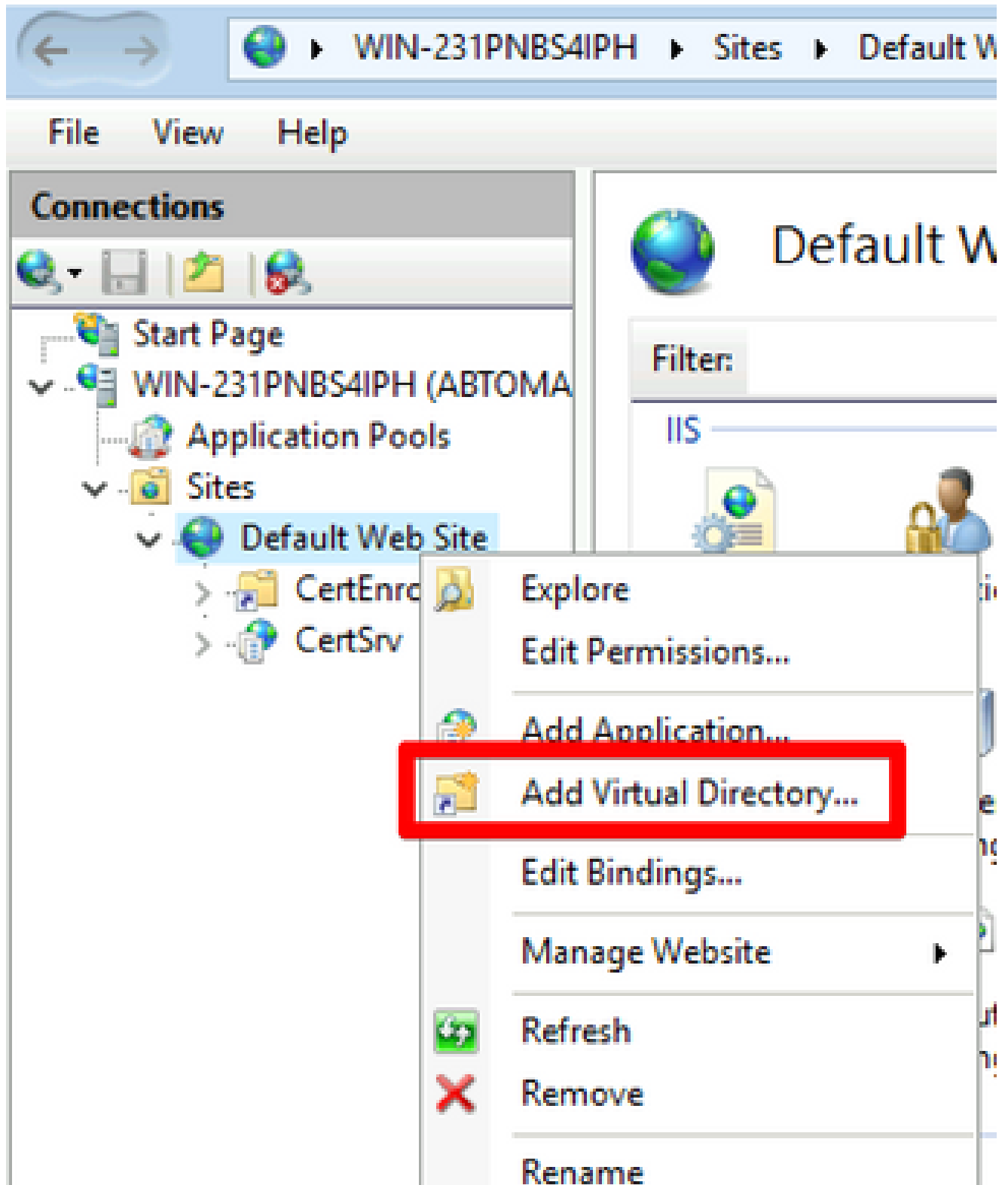
為了讓ISE訪問CRL檔案，請通過IIS訪問包含CRL檔案的目錄。

1. 在IIS伺服器工作列上，按一下Start。選擇Administrative Tools > Internet Information Services (IIS) Manager
2. 在左側窗格（稱為控制檯樹）中，展開IIS伺服器名稱，然後展開Sites。



3. 按一下右鍵並Default Web Site進行選Add Virtual Directory擇，如下圖所示。

Internet Information Services (IIS) Manager



4. 在「別名」欄位中，輸入CRL分發點的站點名稱。在此示例中，輸入了CRLD。

Add Virtual Directory

Site name: Default Web Site
Path: /

Alias:
CRLD

Example: images

Physical path:
C:\CRLDistribution

Pass-through authentication

Connect as... Test Settings...

OK Cancel

5. 按一下省略號(. ..)在「物理路徑」欄位的右側，瀏覽到在第1部分中建立的資料夾。選擇資料夾並按一下OK。按一下OK關閉「新增虛擬目錄」視窗。

Add Virtual Directory ? X

Site name: Default Web Site
Path: /

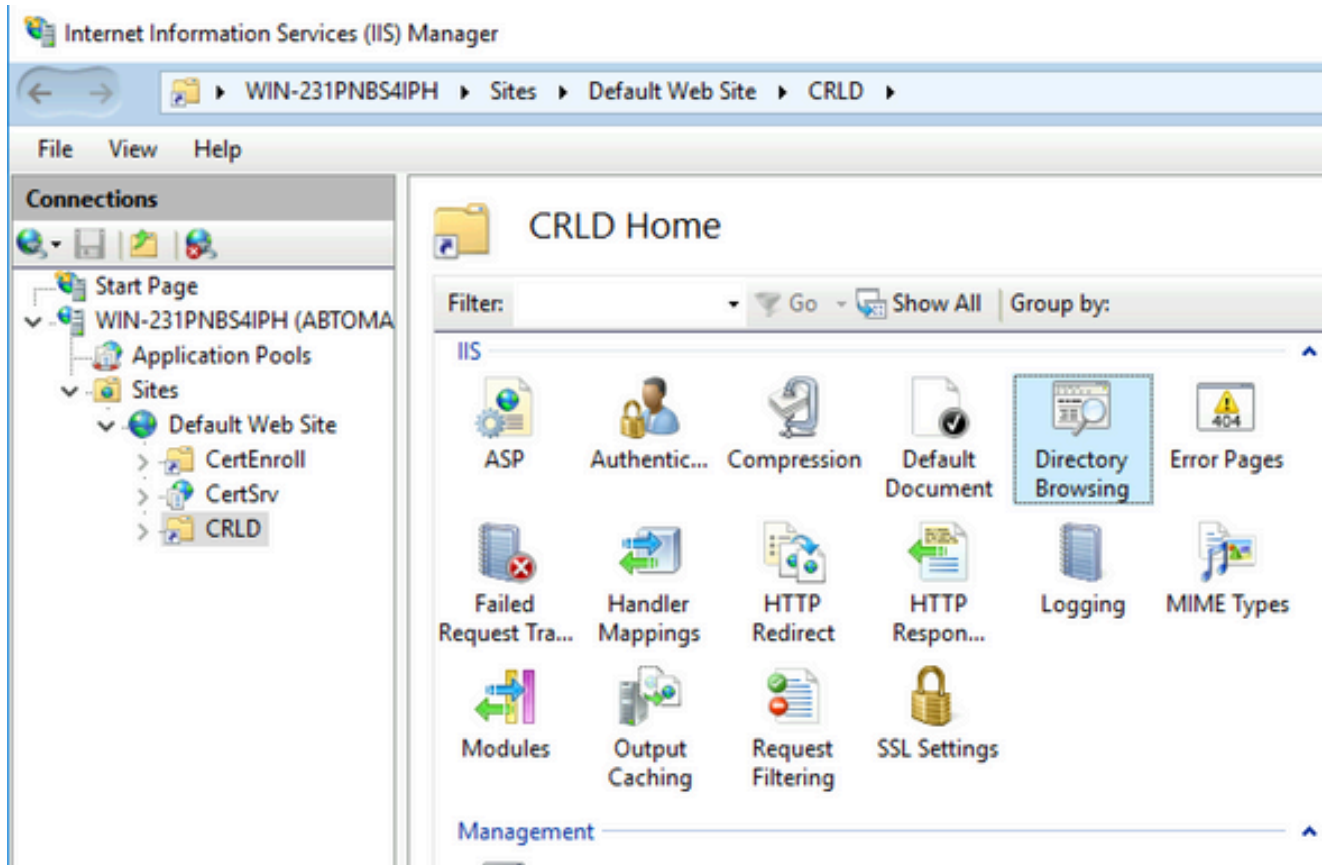
Alias:
CRLD
Example: images

Physical path:
C:\CRLDistribution ...

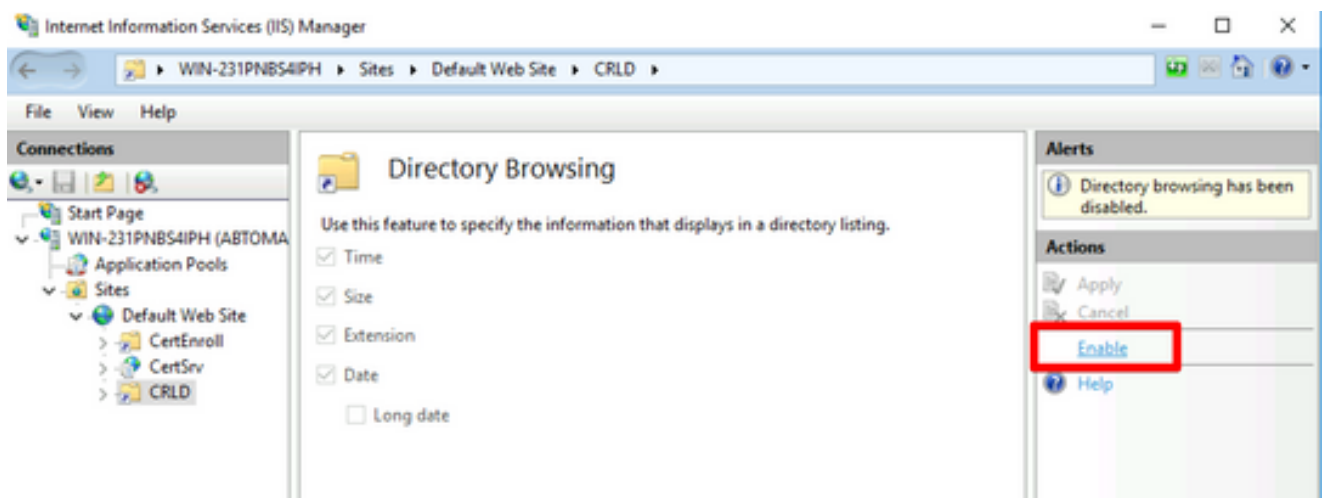
Pass-through authentication
Connect as... Test Settings...

OK Cancel

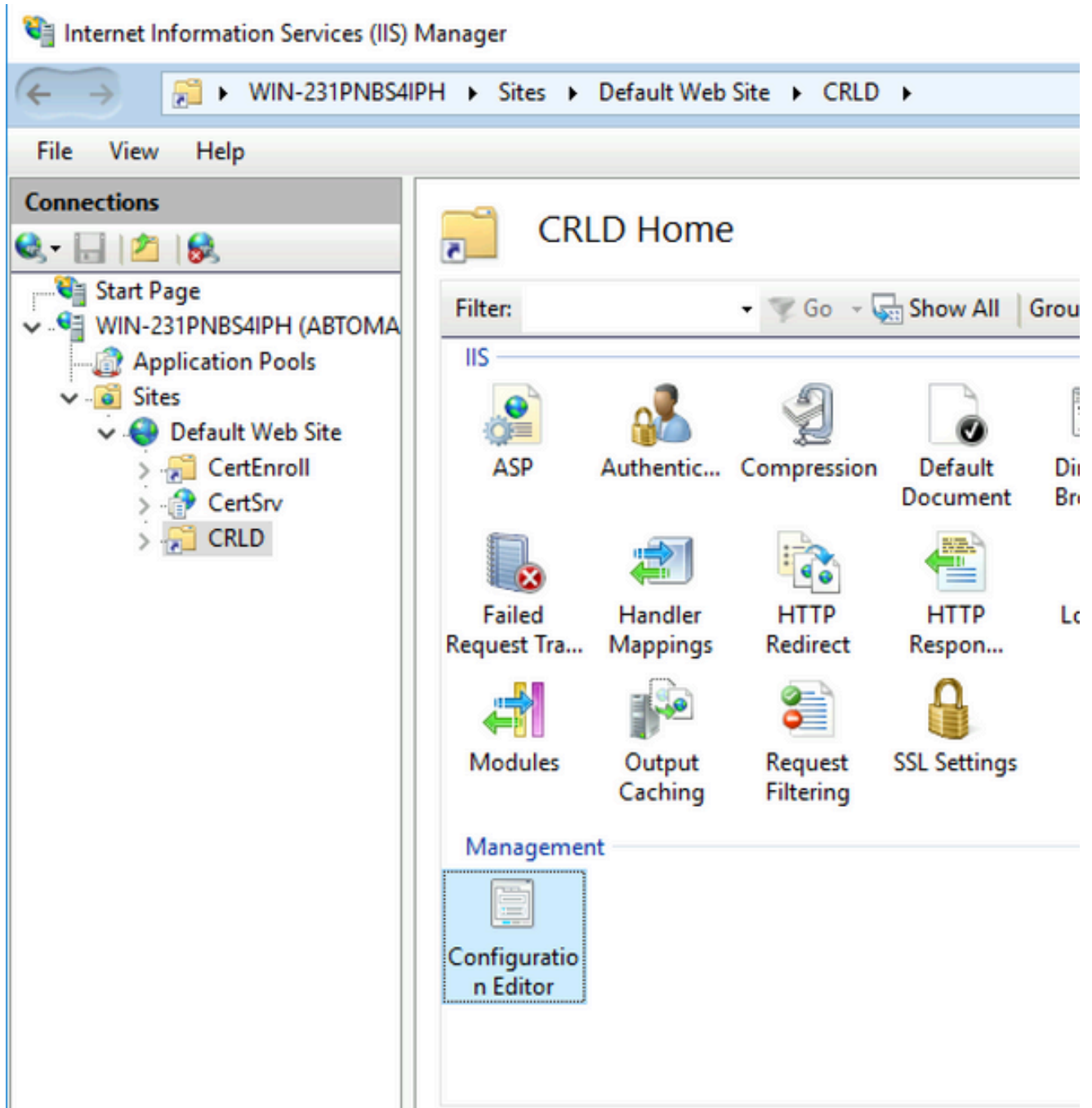
6. 在步驟4中輸入的站點名稱必須在左窗格中突出顯示。如果沒有，現在選擇它。在中心窗格中，按兩下 **Directory Browsing**。



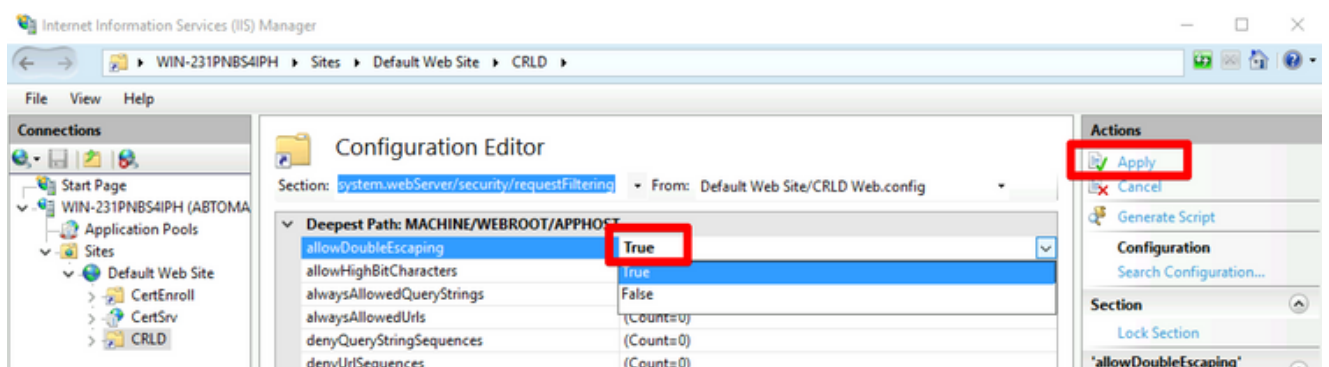
7. 在右窗格中，按一下 **Enable** 以啟用目錄瀏覽。



8. 在左窗格中，再次選擇站點名稱。在中心窗格中，按兩下 **Configuration Editor**。



9. 在Section下拉選單中，選擇system.webServer/security/requestFiltering。在下allowDoubleEscaping拉清單中，選擇True。在右窗格中，單Apply擊，如下圖所示。

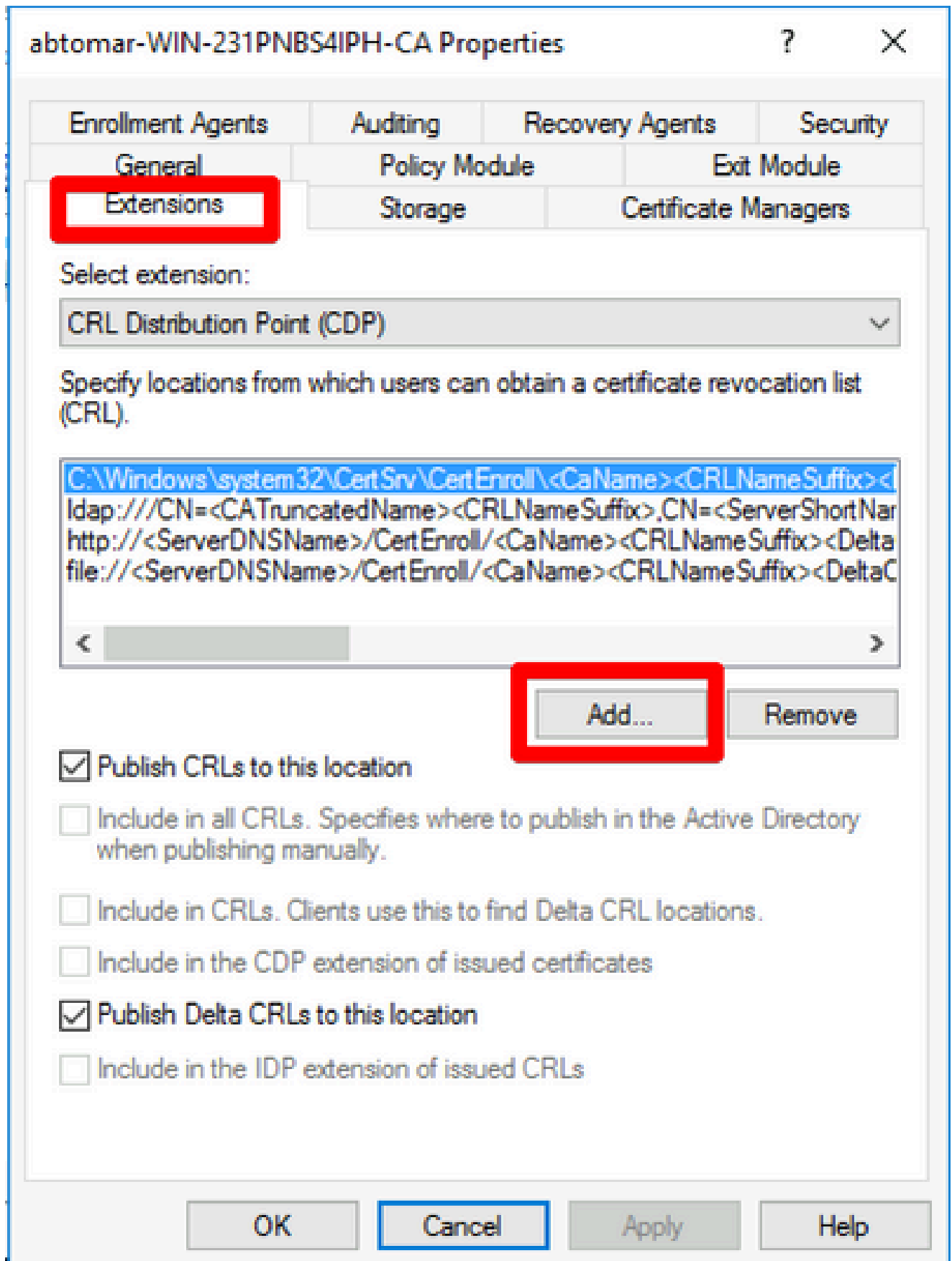


現在必須通過IIS訪問該資料夾。

配置Microsoft CA伺服器以將CRL檔案發佈到分發點

現在，已配置了一個新資料夾來容納CRL檔案，並且該資料夾已在IIS中公開，請配置Microsoft CA伺服器以將CRL檔案發佈到新位置。

1. 在CA伺服器工作列上，按一下Start。選擇Administrative Tools > Certificate Authority
2. 在左窗格中，按一下右鍵CA名稱。選擇Properties，然後按一下選Extensions項卡。要新增新的CRL分發點，請按一下Add。



3. 在「位置」欄位中，輸入在第1部分中建立和共用的資料夾的路徑。在第1節的範例中，路徑為：

\\WIN-231PNBS4IPH\CRL分配\$

Add Location ✕

A location can be any valid URL or path. Enter an HTTP, LDAP, file address, or enter a UNC or local path. To insert a variable into the URL or path, select the variable below and click Insert.

Location:

Variable:

Description of selected variable:
Used in URLs and paths
Inserts the DNS name of the server
Example location: http://<ServerDNSName>/CertEnroll/<CaName><CRLNa

4. 填充Location欄位後，從 Variable下拉選單中選擇，然後按一下 Insert.

Add Location



A location can be any valid URL or path. Enter an HTTP, LDAP, file address, or enter a UNC or local path. To insert a variable into the URL or path, select the variable below and click Insert.

Location:

\\WIN-231PNBS4IPH\CRLDistribution\$\<CaName>

Variable:

<CaName>



Insert

Description of selected variable:

Used in URLs and paths

Inserts the DNS name of the server

Example location: http://<ServerDNSName>/CertEnroll/<CaName><CRLNa



OK

Cancel

5. 從「變數」(Variable)下拉選單中，選擇並按一下Insert它。

Add Location ✕

A location can be any valid URL or path. Enter an HTTP, LDAP, file address, or enter a UNC or local path. To insert a variable into the URL or path, select the variable below and click Insert.

Location:

Variable:

Description of selected variable:

< >

6. 在Location欄位中，.crl追加到路徑末尾。在此示例中，位置為：

\\WIN-231PNBS4IPH\CRLDistribution\$\

.crl

Add Location ✕

A location can be any valid URL or path. Enter an HTTP, LDAP, file address, or enter a UNC or local path. To insert a variable into the URL or path, select the variable below and click Insert.

Location:

Variable:

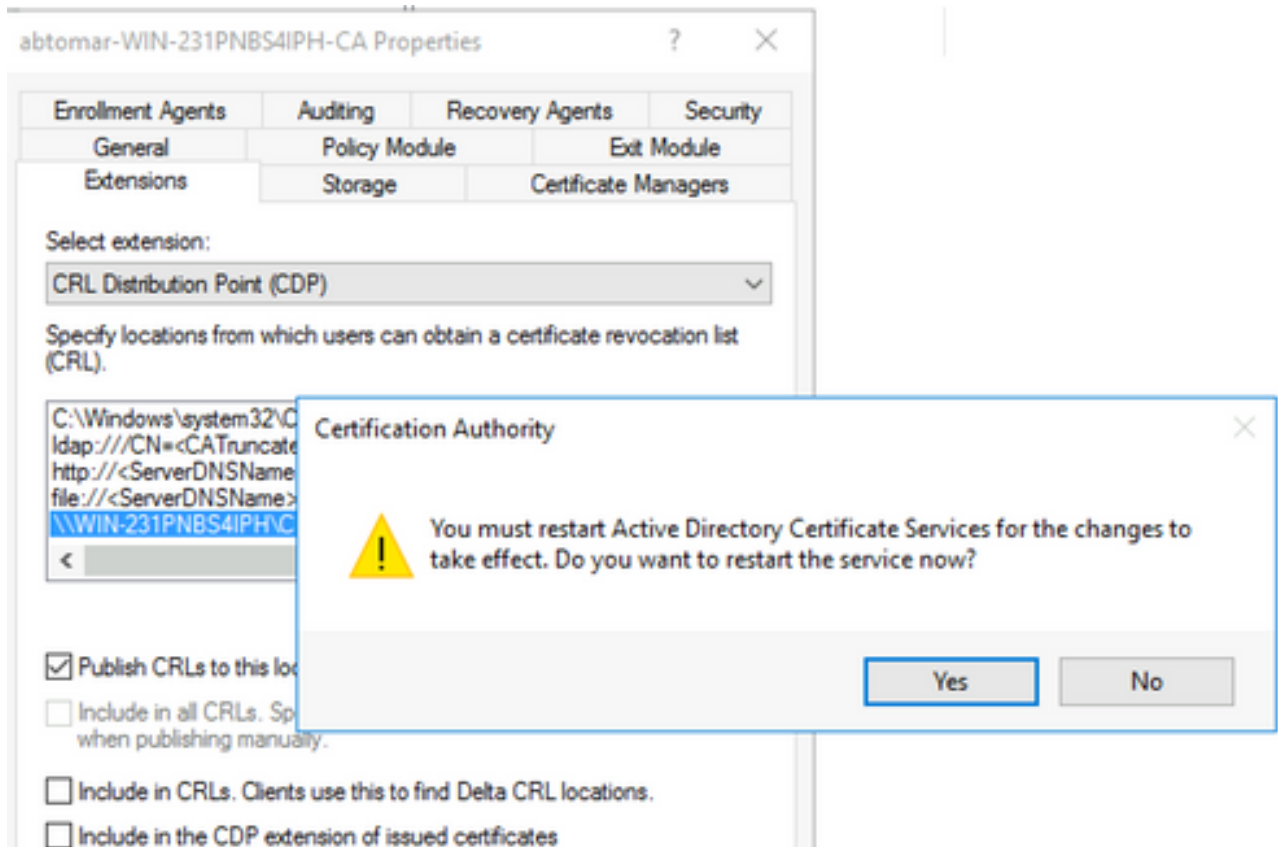
Description of selected variable:

Used in URLs and paths for the CRL Distribution Points extension
Appends a suffix to distinguish the CRL file name
Example location: http://<ServerName>/CertEnroll/<CaName><CRLNameSu

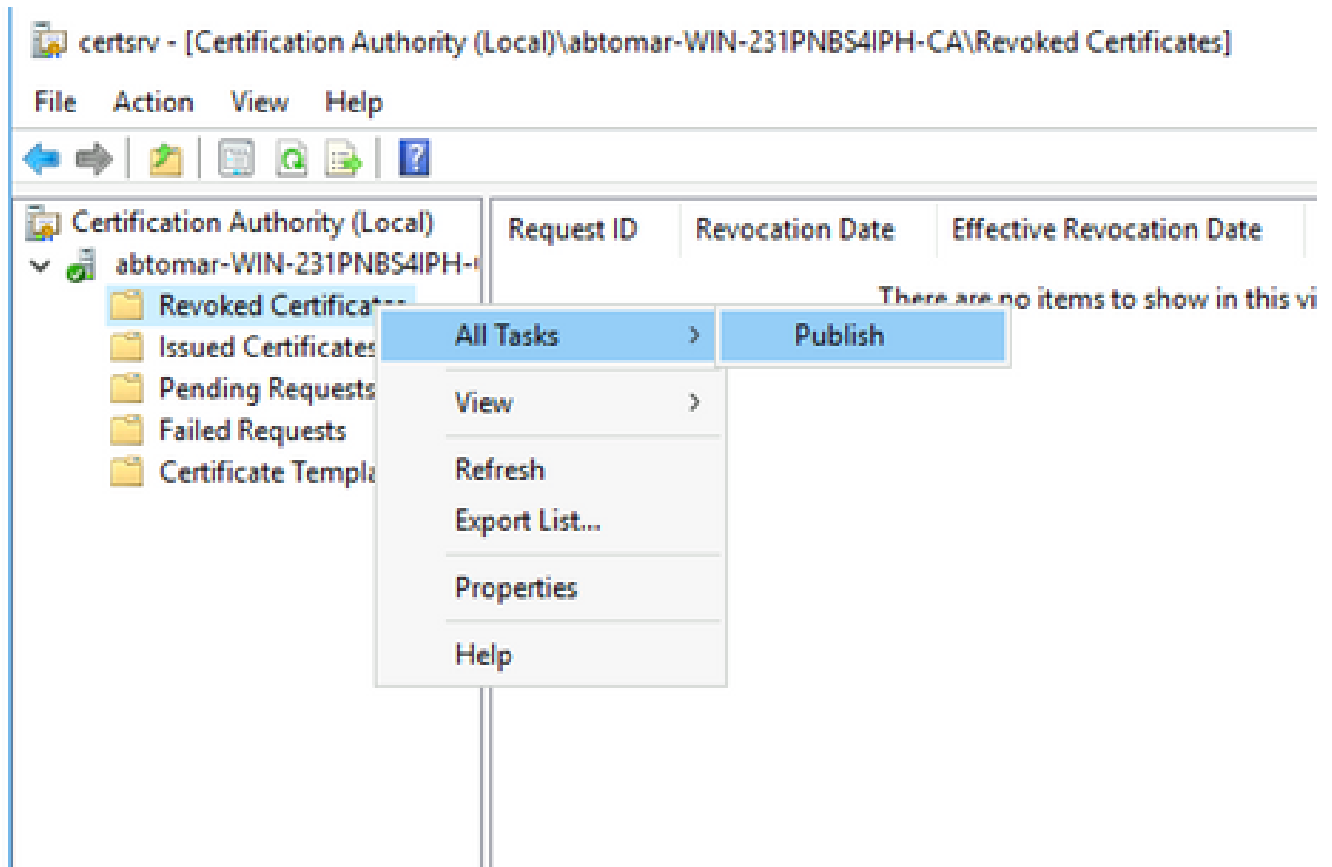
< >

- 按一下OK返回到「擴展」頁籤。選中此復Publish CRLs to this location選框，然後按一下以OK關閉「屬性」視窗。

出現一個提示符，提示獲得重新啟動Active Directory證書服務的許可權。按一下Yes下。



8. 在左窗格中，按一下右Revoked Certificates鍵。選擇.All Tasks > Publish確保已選中「New CRL (新建 CRL)」，然後按一下OK按鈕。



Microsoft CA伺服器必須在第1節中建立的資料夾中建立新的.crl檔案。如果成功建立新的

CRL檔案，則按一下「確定」(OK)後將不會出現對話方塊。如果返回有關新分發點資料夾的錯誤，請仔細重複本節中的每一個步驟。

驗證CRL檔案存在且可通過IIS訪問

開始本節之前，請確認新的CRL檔案是否存在，以及是否可以通過另一工作站的IIS訪問這些檔案。

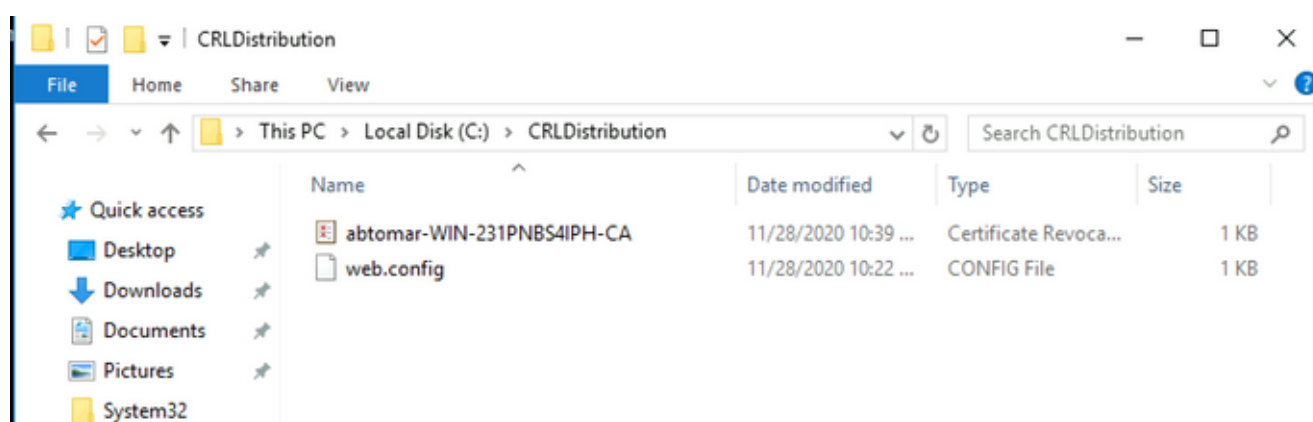
1. 在IIS伺服器上，開啟第1部分中建立的資料夾。必須存在一個.crl檔案，其形

.crl

式

中是CA伺服器的名稱。在此範例中，檔案名稱為：

abtomar-WIN-231PNBS4IPH-CA.crl



2. 從網路上的工作站（最好與ISE主管理節點位於同一網路），開啟Web瀏覽器並瀏覽到http://

/

第2部分中配置的IIS伺服器的伺服器名稱和第2部分中為分發點選擇的站點名稱。在此範例中，URL為：

<http://win-231pnbs4iph/CRLD>

將顯示目錄索引，其中包括步驟1中觀察到的檔案。



win-231pnbs4iph - /crld/

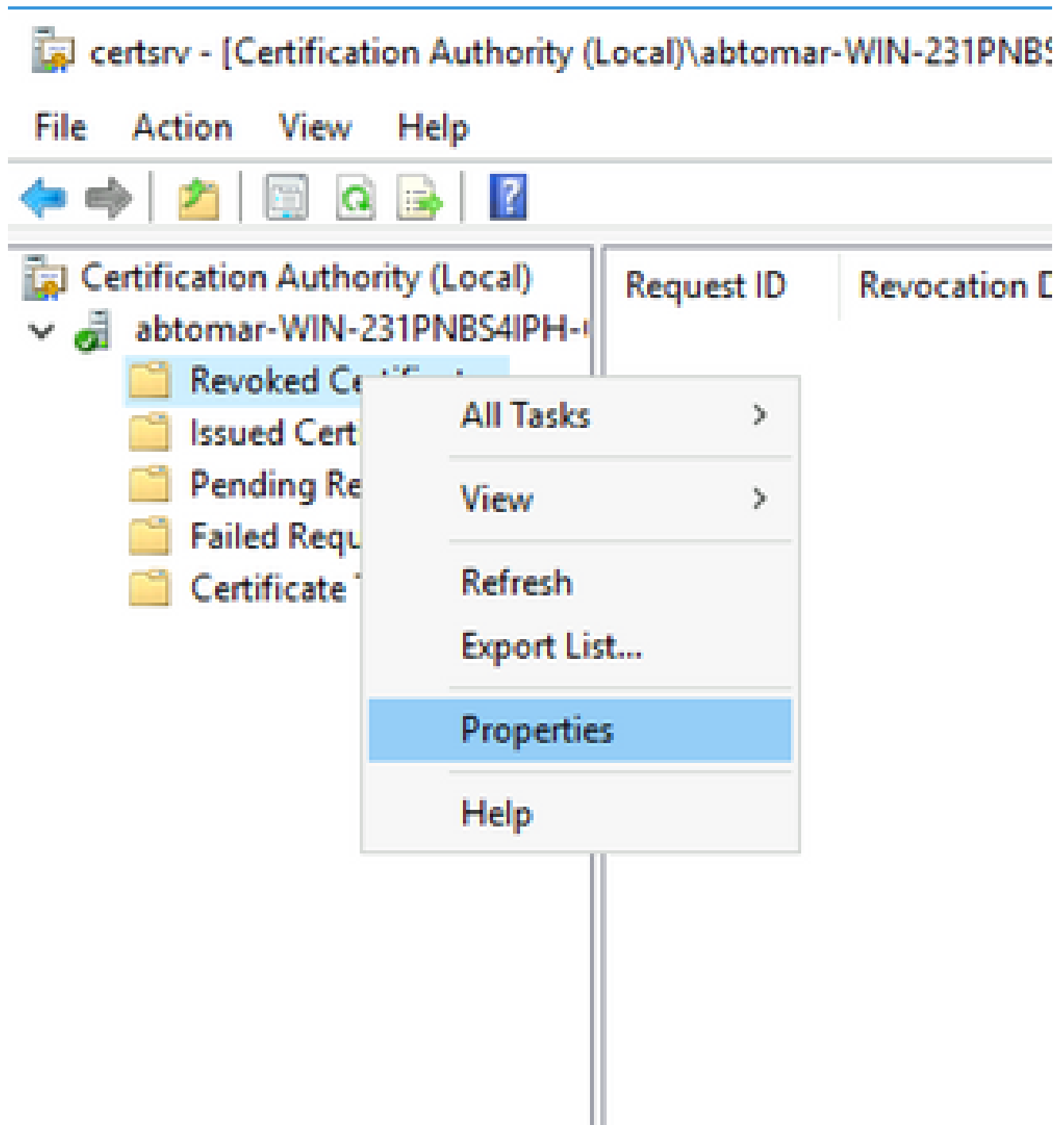
[\[To Parent Directory\]](#)

11/28/2020 10:39 AM	979	abtomar-WIN-231PNBS4IPH-CA.crl
11/28/2020 10:22 AM	270	web.config

配置ISE以使用新的CRL分發點

在將ISE配置為檢索CRL之前，定義發佈CRL的時間間隔。確定此間隔的策略不在本檔案的範圍之內。潛在值（在Microsoft CA中）為1小時到411年（含）。預設值為1週。確定適合您環境的間隔後，請使用以下說明設定間隔：

1. 在CA伺服器工作列上，按一下Start。選擇 **.Administrative Tools > Certificate Authority**
2. 在左窗格中，展開CA。按一下右鍵該資料夾 **Revoked Certificates**，然後選擇 **Properties** 它。
3. 在「CRL發佈間隔」欄位中，輸入所需的數字並選擇時間段。按一下OK關閉視窗並應用更改。在本例中，配置的發佈間隔為七天。



4. 輸入命令 `certutil -getreg CA\Clock*` 以確認 `ClockSkew` 值。預設值為 10 分鐘。

輸出示例：

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

5. 輸入命令 `certutil -getreg CA\CRLov*` 以驗證 `CRLOverlapPeriod` 是否已手動設定。預設情況下，`CRLOverlapUnit` 值為 0，表示未設定手動值。如果該值不是 0，請記錄該值和單位。

輸出示例：

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

6. 輸入命令 `certutil -getreg CA\CRLpe*` 以驗證 CRLPeriod (已在步驟3中設定)。

輸出示例：

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

7. 按如下方式計算 CRL 寬限期：

a. 如果在步驟5中設定 `CRLOverlapPeriod:OVERLAP = CRLOverlapPeriod` (分鐘)；

其他：重疊 = $(CRLPeriod / 10)$ ，以分鐘為單位

b. 如果重疊超過 720，則重疊為 720

c. 如果重疊 $< (1.5 * ClockSkewMinutes)$ ，則重疊 = $(1.5 * ClockSkewMinutes)$

d. 如果 `OVERLAP > CRLPeriod`，則重疊 = CRLPeriod (分鐘)

e. 寬限期 = 重疊 + 時鐘偏差分鐘

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

計算出的寬限期是 CA 發佈下一個 CRL 到當前 CRL 到期之間的時間量。需要配置 ISE 以相應地檢索 CRL。

8. 登入到 ISE 主管理節點並選擇 `Administration > System > Certificates`。在左窗格中選擇 `Trusted Certificate`。

Cisco ISE Administration - System

Deployment Licensing **Certificates** Logging Maintenance Upgrade Health Checks Backup & Restore Admin Access Settings

Certificate Management

- System Certificates
- Trusted Certificates**
- OCSP Client Profile
- Certificate Signing Requests
- Certificate Periodic Check Se...

Certificate Authority

Trusted Certificates

[Edit](#) [+ Import](#) [Export](#) [Delete](#) [View](#)

<input type="checkbox"/>	Friendly Name	Status	Trusted For	Serial Number	Issued To	Issued By	Valid From	Expiration Date	Expiration
<input type="checkbox"/>	Baltimore CyberTrust Root	Enabled	Cisco Services	02 00 00 B9	Baltimore CyberTrust ...	Baltimore CyberTrust ...	Sat, 13 May 2000	Tue, 13 May 2025	<input checked="" type="checkbox"/>
<input checked="" type="checkbox"/>	CA_Root	Enabled	Infrastructure Endpoints AdminAuth	4D 9B EE 97 53 ...	abtomar-WIN-231PN...	abtomar-WIN-231PN...	Wed, 20 Feb 2019	Sun, 20 Feb 2039	<input checked="" type="checkbox"/>
<input type="checkbox"/>	Cisco ECC Root CA 2099	Enabled	Cisco Services	03	Cisco ECC Root CA	Cisco ECC Root CA	Thu, 4 Apr 2013	Mon, 7 Sep 2099	<input checked="" type="checkbox"/>
<input type="checkbox"/>	Cisco Licensing Root CA	Enabled	Cisco Services	01	Cisco Licensing Root ...	Cisco Licensing Root ...	Fri, 31 May 2013	Mon, 31 May 2038	<input checked="" type="checkbox"/>

- 選中要為其配置CRL的CA證書旁邊的覈取方塊。按一Edit下。
- 在視窗底部附近，選中復Download CRL選框。
- 在CRL分發URL欄位中，輸入CRL分發點的路徑，其中包括第2部分中建立的.crl檔案。在此範例中，URL為：

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

- 可以將ISE配置為定期或根據過期時間（通常也是定期間隔）檢索CRL。當CRL發佈間隔為靜態時，使用後一個選項可獲得更及時的CRL更新。按一下單Automatically選按鈕。
- 將檢索的值設定為小於在步驟7中計算的寬限期的值。如果值集長於寬限期，ISE將在CA發佈下一個CRL之前檢查CRL分發點。在此示例中，寬限期計算為730分鐘或12小時10分鐘。檢索將使用10小時的值。
- 根據您的環境設定重試間隔。如果ISE無法按上一步中配置の間隔檢索CRL，它將按此較短間隔重試。
- 如果Bypass CRL Verification if CRL is not ReceivedISE在其上次下載嘗試中無法檢索此CA的CRL，請選中此覈取方塊以允許基於證書的身份驗證正常進行（並且不進行CRL檢查）。如果未選中此覈取方塊，則如果無法檢索CRL，則此CA頒發的證書的所有基於證書的身份驗證都將失敗。
- 選中此復Ignore that CRL is not yet valid or expired選框允許ISE使用已過期（或尚未有效）的CRL檔案，就像它們有效一樣。如果未選中此覈取方塊，則ISE會將CRL視為在其生效日期之前和下次更新時間之後無效。按一下Save以完成配置。

Certificate Status Validation

To verify certificates, enable the methods below. If both are enabled, OCSP will always be tried first.

OCSP Configuration

Validate against OCSP Service

Reject the request if OCSP returns UNKNOWN status

Reject the request if OCSP Responder is unreachable

Certificate Revocation List Configuration

Download CRL

CRL Distribution URL:

Retrieve CRL

Automatically 10 Hours before expiration.

Every 1 Hours

If download failed, wait 10 Minutes before retry.

Enable Server Identity Check

Bypass CRL Verification if CRL is not Received

Ignore that CRL is not yet valid or expired

Save

驗證

目前沒有適用於此組態的驗證程序。

疑難排解

目前尚無適用於此組態的具體疑難排解資訊。

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。