配置Microsoft CA服务器以发布ISE的证书撤销列表

目录

简介

本文档介绍运行Internet Information Services(IIS)以发布证书吊销列表(CRL)更新的Microsoft证书颁发机构(CA)服务器的配置。它还说明如何配置思科身份服务引擎(ISE)（3.0版及更高版本）以检索更新以用于证书验证。ISE可以配置为检索它在证书验证中使用的各种CA根证书的CRL。

前提条件

要求

本文档没有任何特定的要求。

使用的组件

本文档中的信息基于以下软件和硬件版本：

- 思科身份服务引擎版本3.0
- Microsoft Windows Server 2008 R2

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

配置

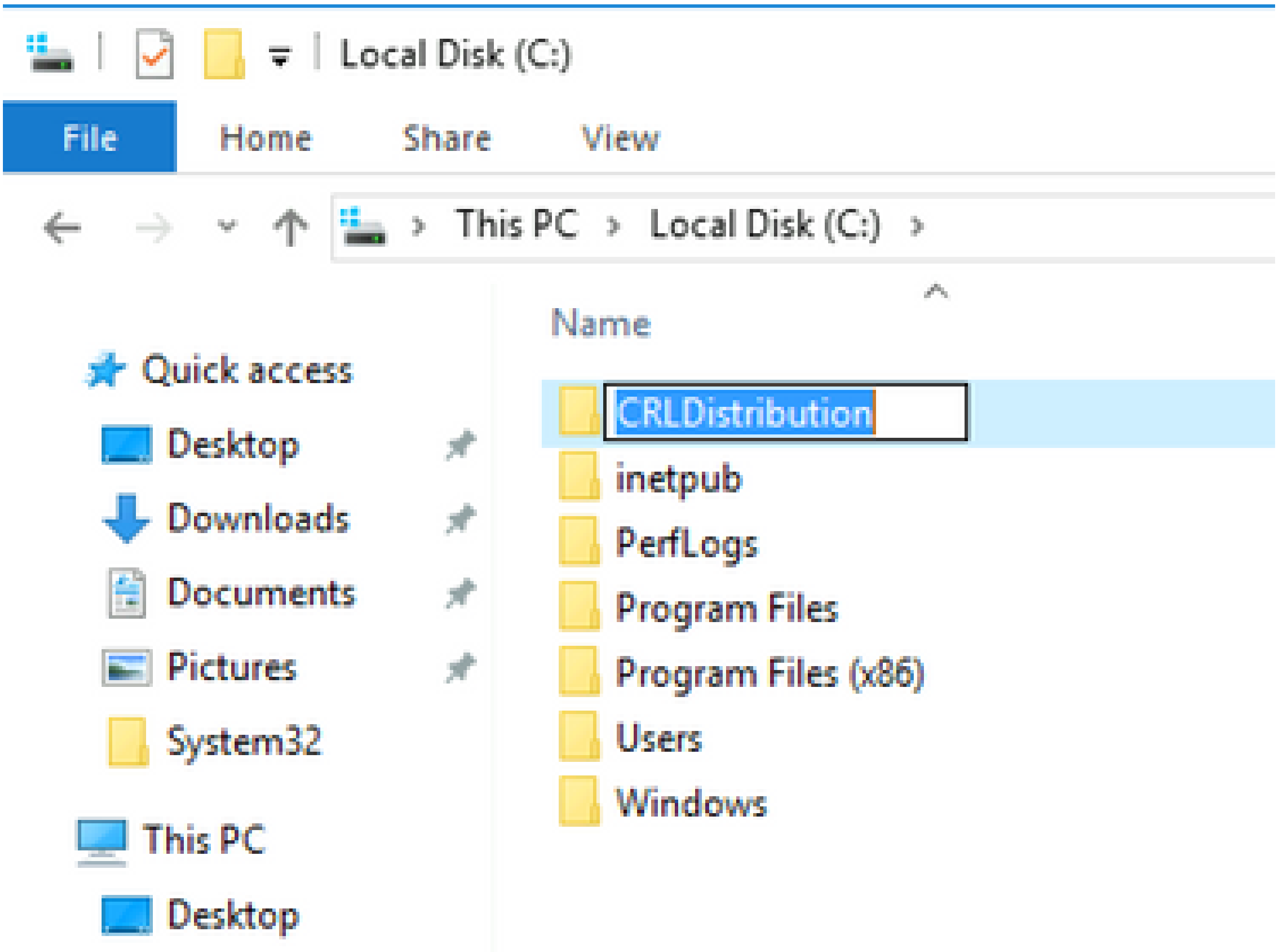
本部分提供有关如何配置本文档所述功能的信息。

在CA上创建并配置文件夹以容纳CRL文件

第一项任务是配置CA服务器上的位置以存储CRL文件。默认情况下，Microsoft CA服务器将文件发布到 **C:\Windows\system32\CertSrv\CertEnroll\**

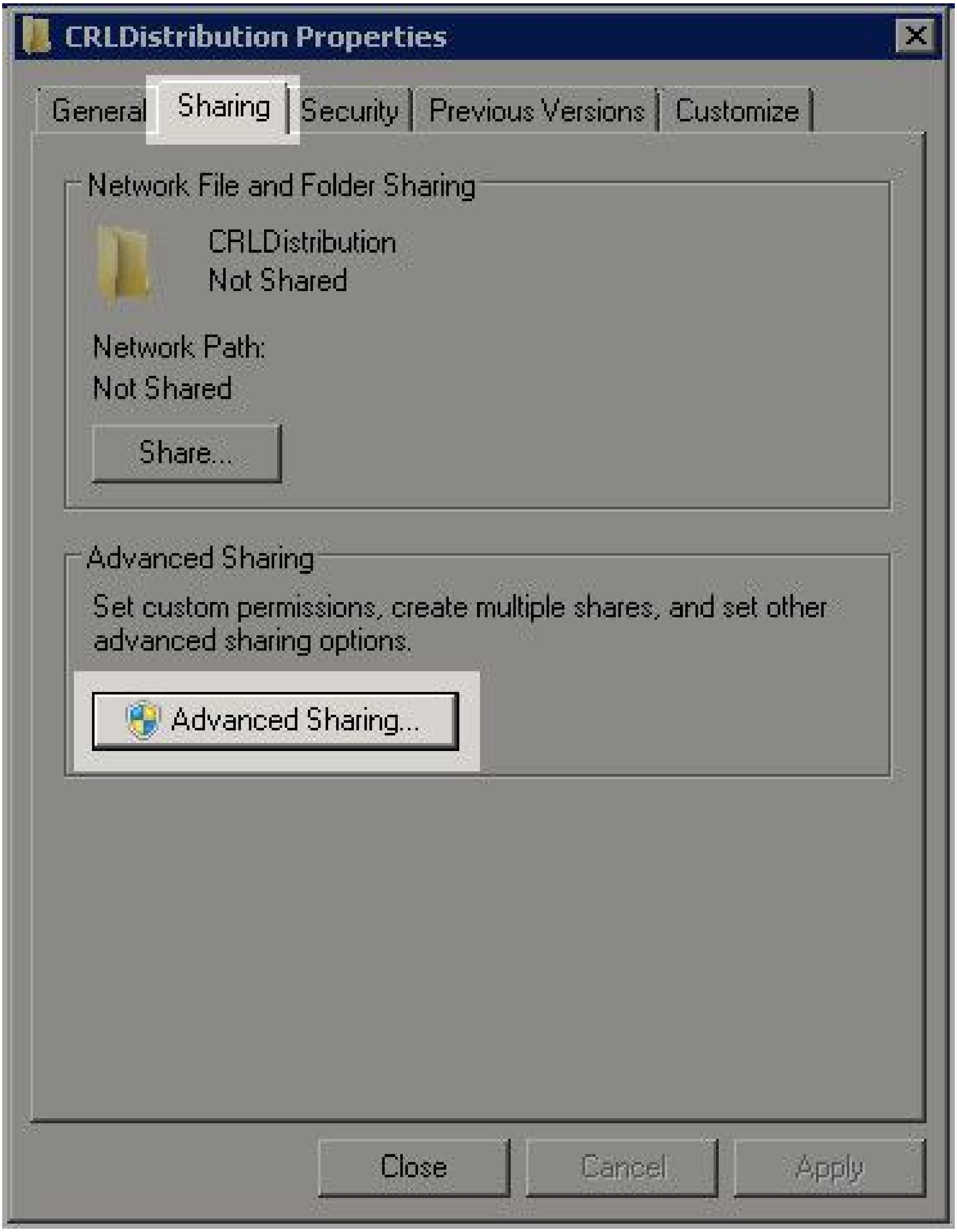
请为这些文件创建一个新文件夹，而不是使用此系统文件夹。

1. 在IIS服务器上，选择文件系统上的位置并创建新文件夹。在本示例中，创建了**C:\CRLDistribution**文件夹。

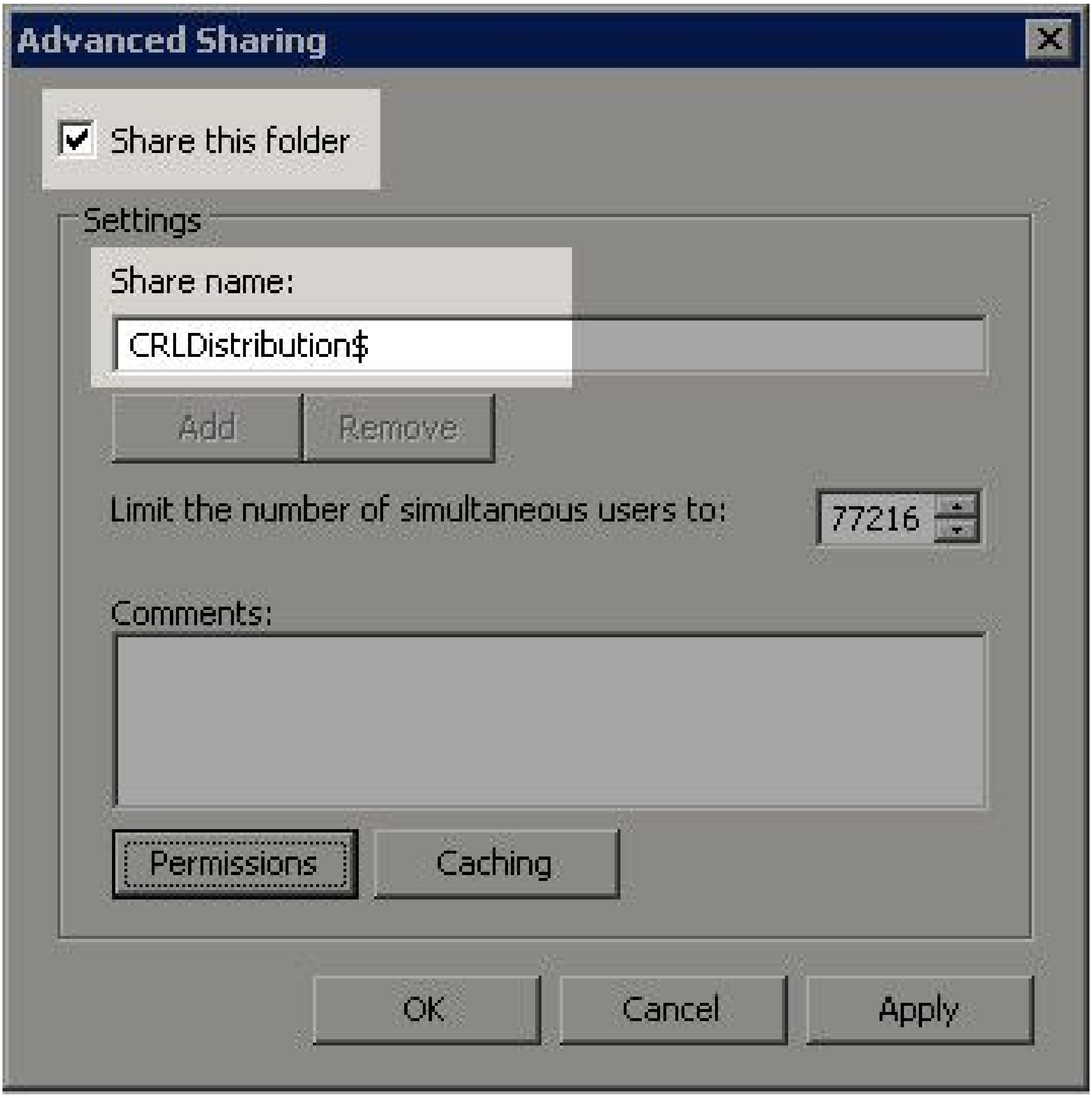


2. 要使CA将CRL文件写入新文件夹，必须启用共享。右键单击新文件夹，选择**Properties**并单击选**Sharing**项卡，然后单击**Advanced Sharing**它。

3. 要共享文件夹，请选中此复选框，然后在“共享名称”字段中的共享名称末尾添加一个美元符号



3. 要共享文件夹，请选中此复选框，然后在“共享名称”字段中的共享名称末尾添加一个美元符号($)以隐藏共享**Share this folder**。



Advanced Sharing

☑ Share this folder

Settings

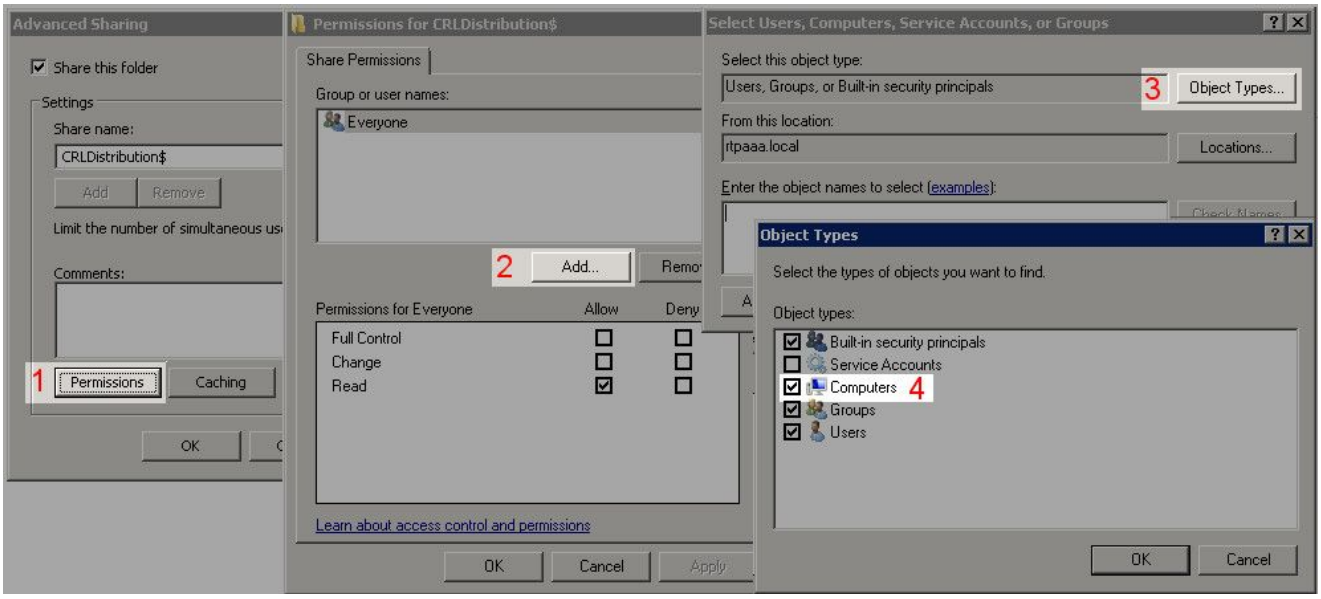
Share name:

CRLDistribution$

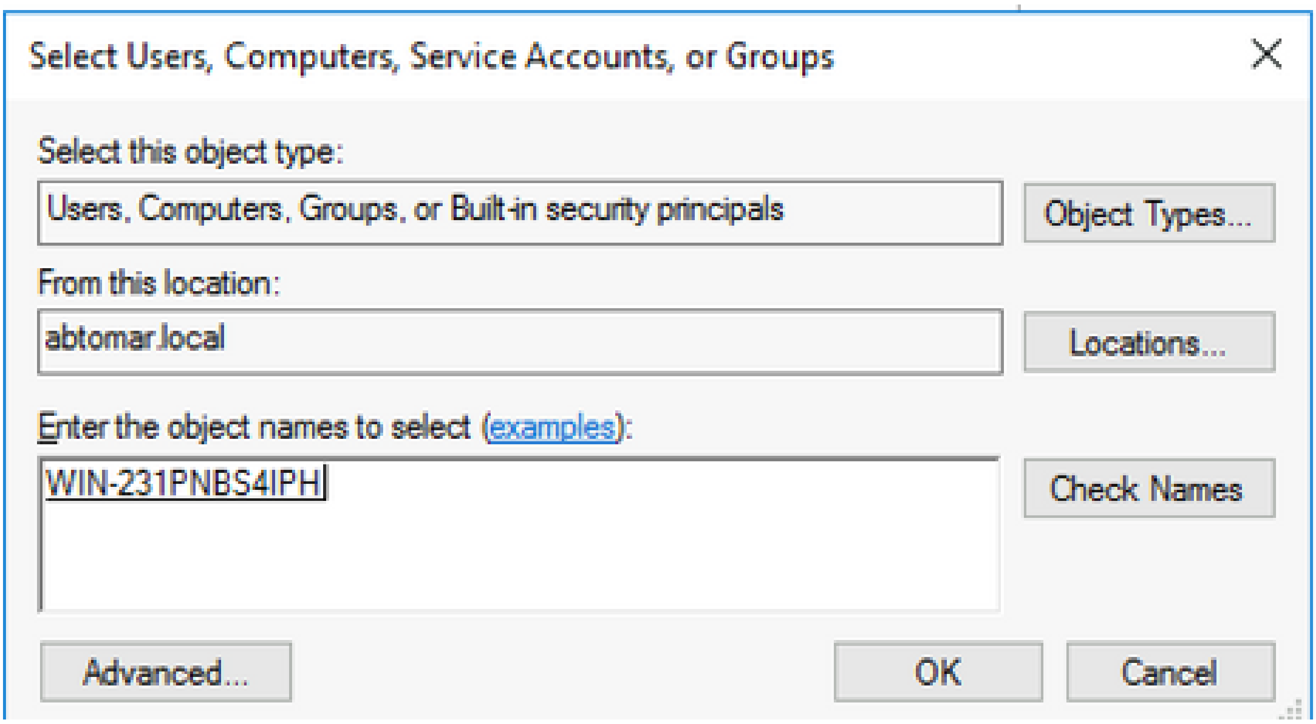
Limit the number of simultaneous users to: 77216

Comments:

4. 单**Permissions**击(1)，单**Add**击(2)，单**Object Types**击(3)，然后选中**Computers**复选框(4)。

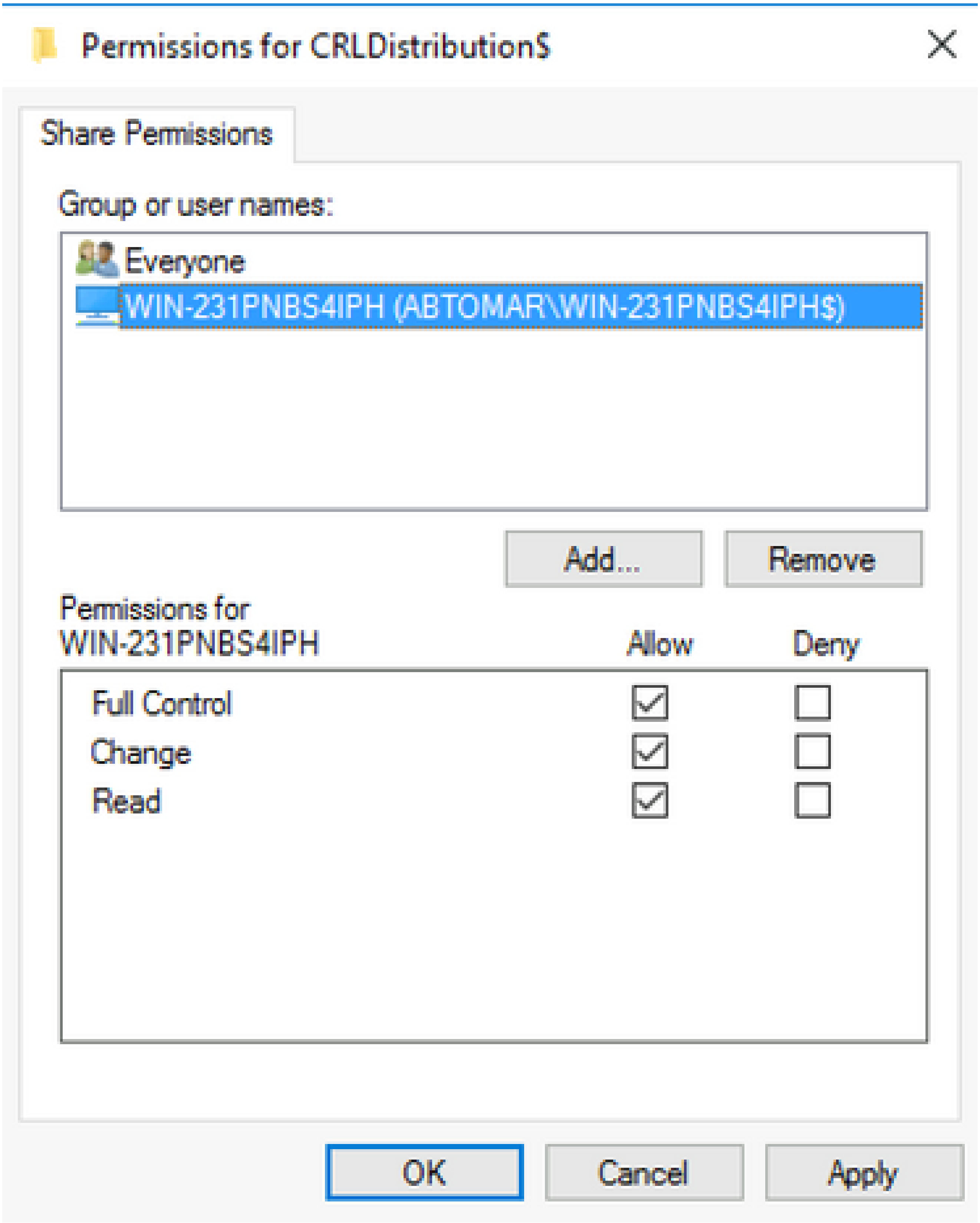


5. 要返回“选择用户”、“计算机”、“服务帐户”或“组”窗口，请单**OK**击。在Enter the object names to select（输入要选择的对象名称）字段中，输入CA服务器的计算机名称（本例中为WIN0231PNBS4IPH），然后单**Check Names**击。如果输入的名称有效，该名称将刷新并显示下划线。单击。**OK**


Select Users, Computers, Service Accounts, or Groups
Select this object type:
Users, Computers, Groups, or Built-in security principals
Object Types...
From this location:
abtomar.local
Locations...
Enter the object names to select (examples):
WIN-231PNBS4IPH
Check Names
Advanced...
OK
Cancel

6. 在“组或用户名”字段中，选择CA计算机。检查**Allow**Full Control以授予对CA的完全访问权限。

单击。**OK**再次**OK**单击以关闭“高级共享”窗口并返回到“属性”窗口。



Permissions for CRLDistribution$

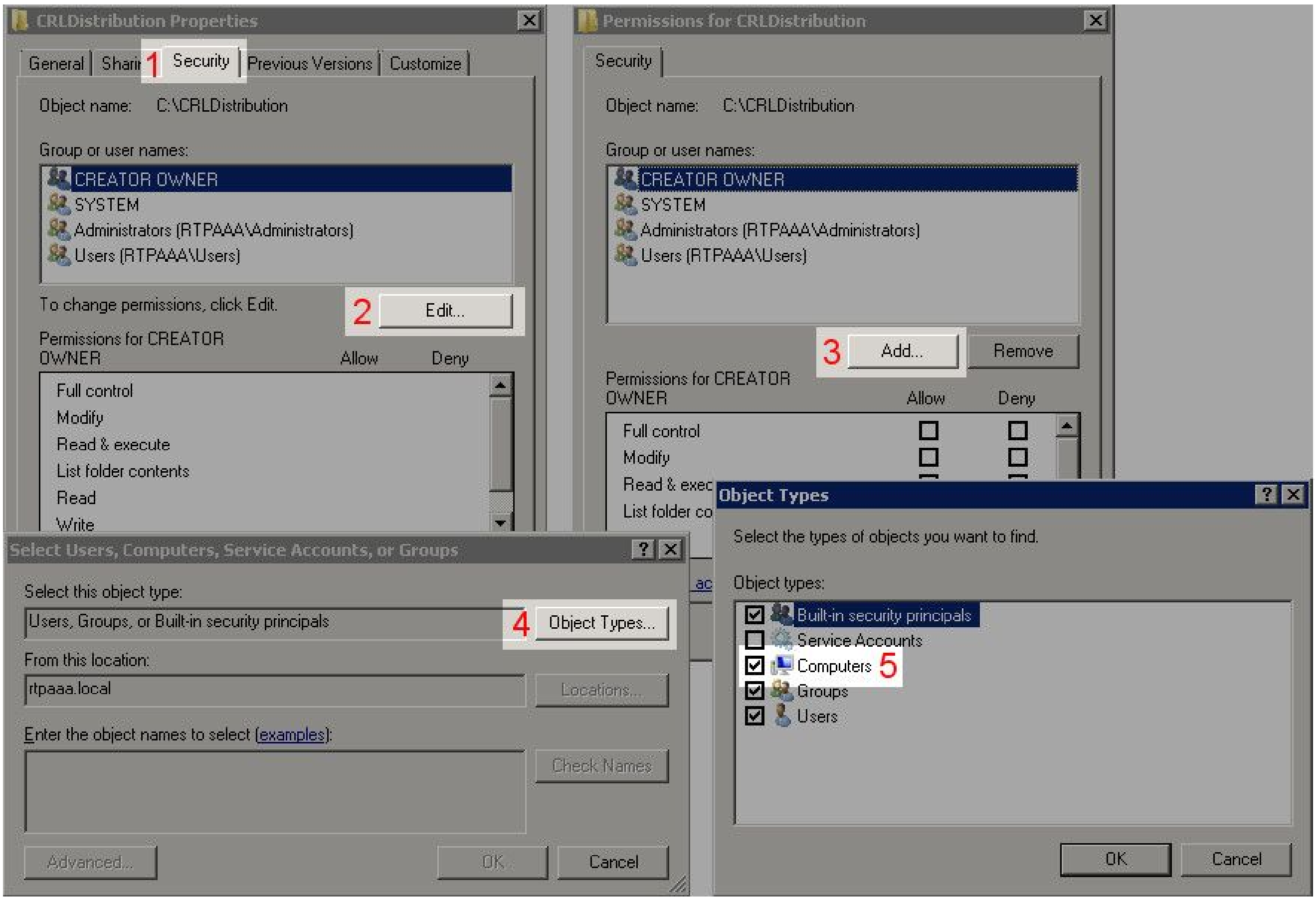
Share Permissions

Group or user names:

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

Permissions for WIN-231PNBS4IPH	Allow	Deny
Full Control	☑	□
Change	☑	□
Read	☑	□

7. 要允许CA将CRL文件写入新文件夹，请配置相应的安全权限。单击**Security**(1)选项卡，单击(**Edit**2)，单击(**Add**3)，单击**Object Types**(4)，然后选中**Computers**复选框(5)。



Object name: C:\CRLDistribution

Group or user names:
CREATOR OWNER
SYSTEM
Administrators (RTPAAA\Administrators)
Users (RTPAAA\Users)

To change permissions, click Edit.

Permissions for CREATOR OWNER — Allow / Deny: Full control, Modify, Read & execute, List folder contents, Read, Write

Select this object type: Users, Groups, or Built-in security principals

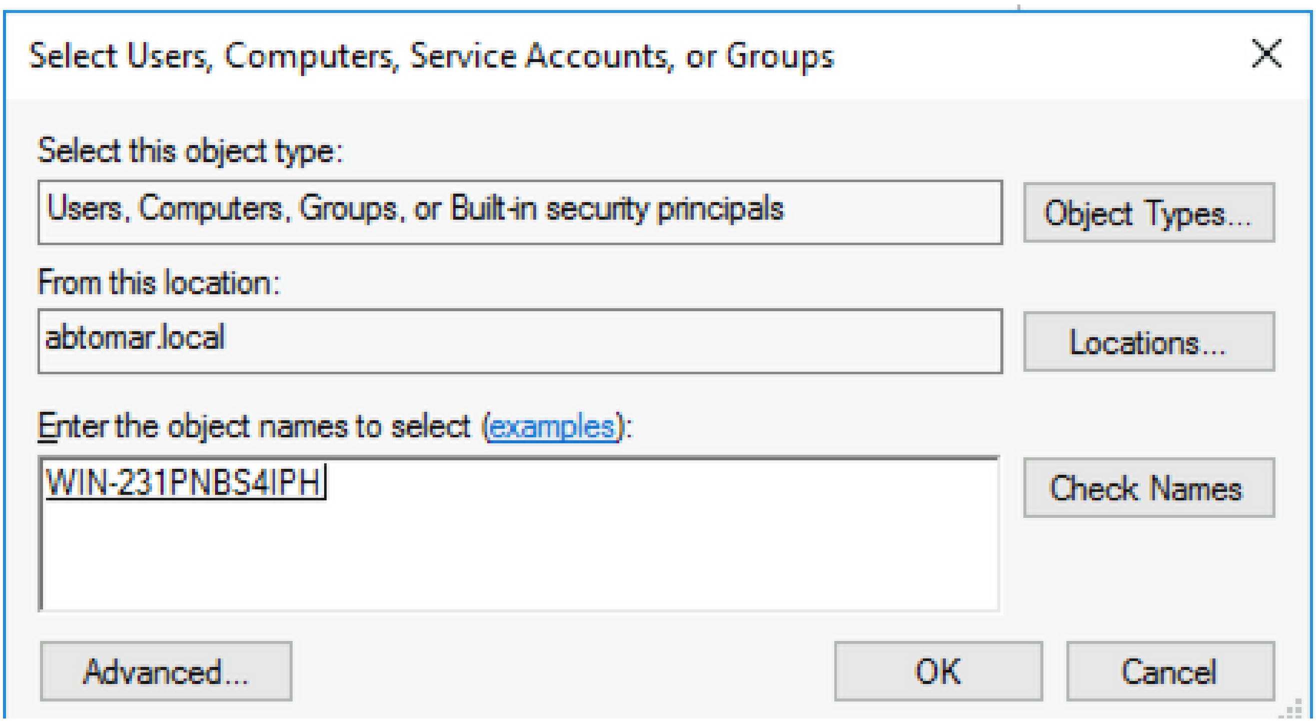
From this location: rtpaaa.local

Enter the object names to select (examples):

Select the types of objects you want to find.

Object types:
☑ Built-in security principals
□ Service Accounts
☑ Computers
☑ Groups
☑ Users

8. 在“输入要选择的对象名称”字段中，输入CA服务器的计算机名称，然后单**Check Names**击。如果输入的名称有效，该名称将刷新并显示下划线。单击。**OK**

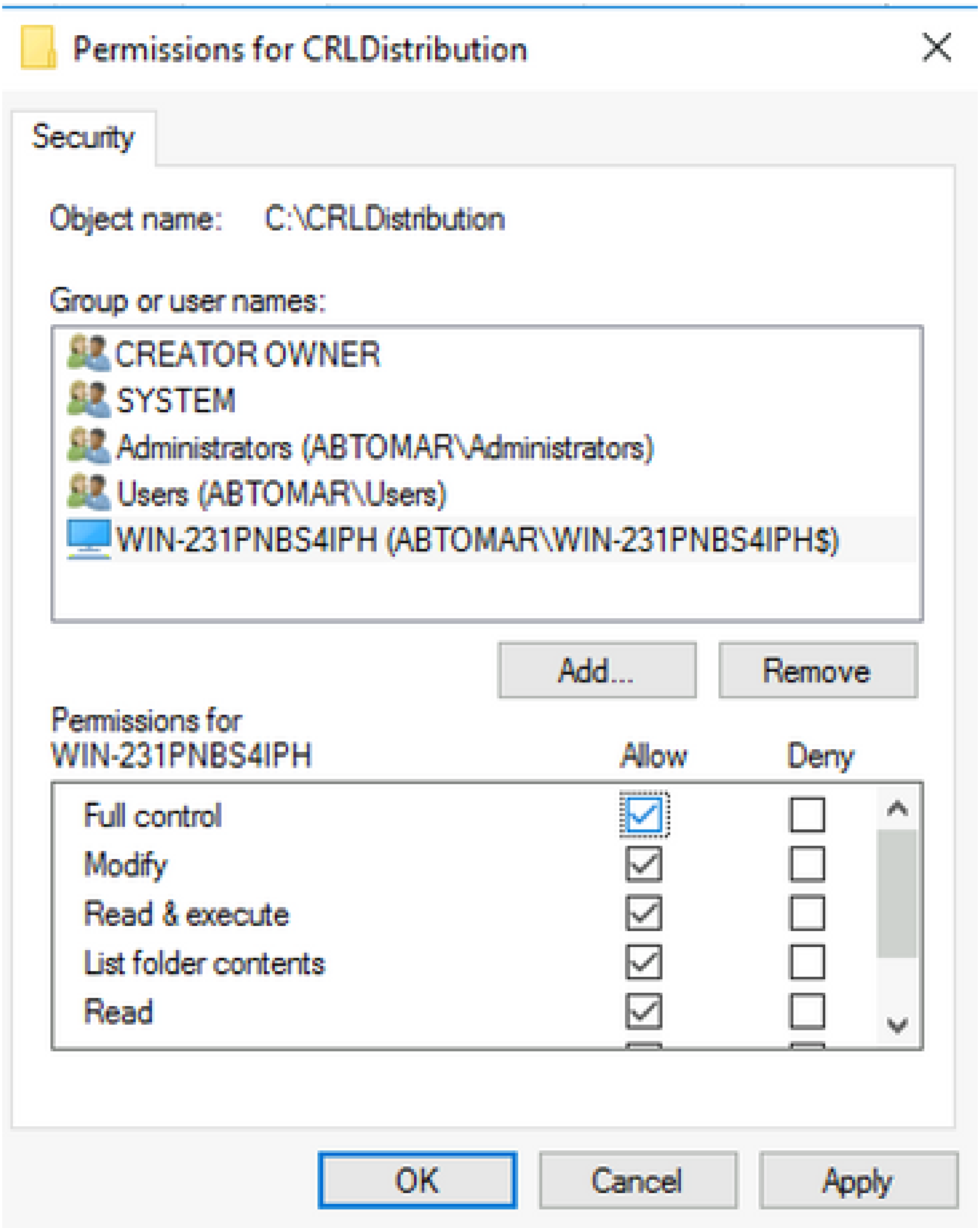


Select this object type: Users, Computers, Groups, or Built-in security principals

From this location: abtomar.local

Enter the object names to select (examples): WIN-231PNBS4IPH

9. 在Group or user names字段中选择CA计算机，然后选中**Allow**Full control以授予对CA的完全访问权限。单击**OK**，然后单击**Close**以完成任务。



Permissions for CRLDistribution

Security

Object name: C:\CRLDistribution

Group or user names:

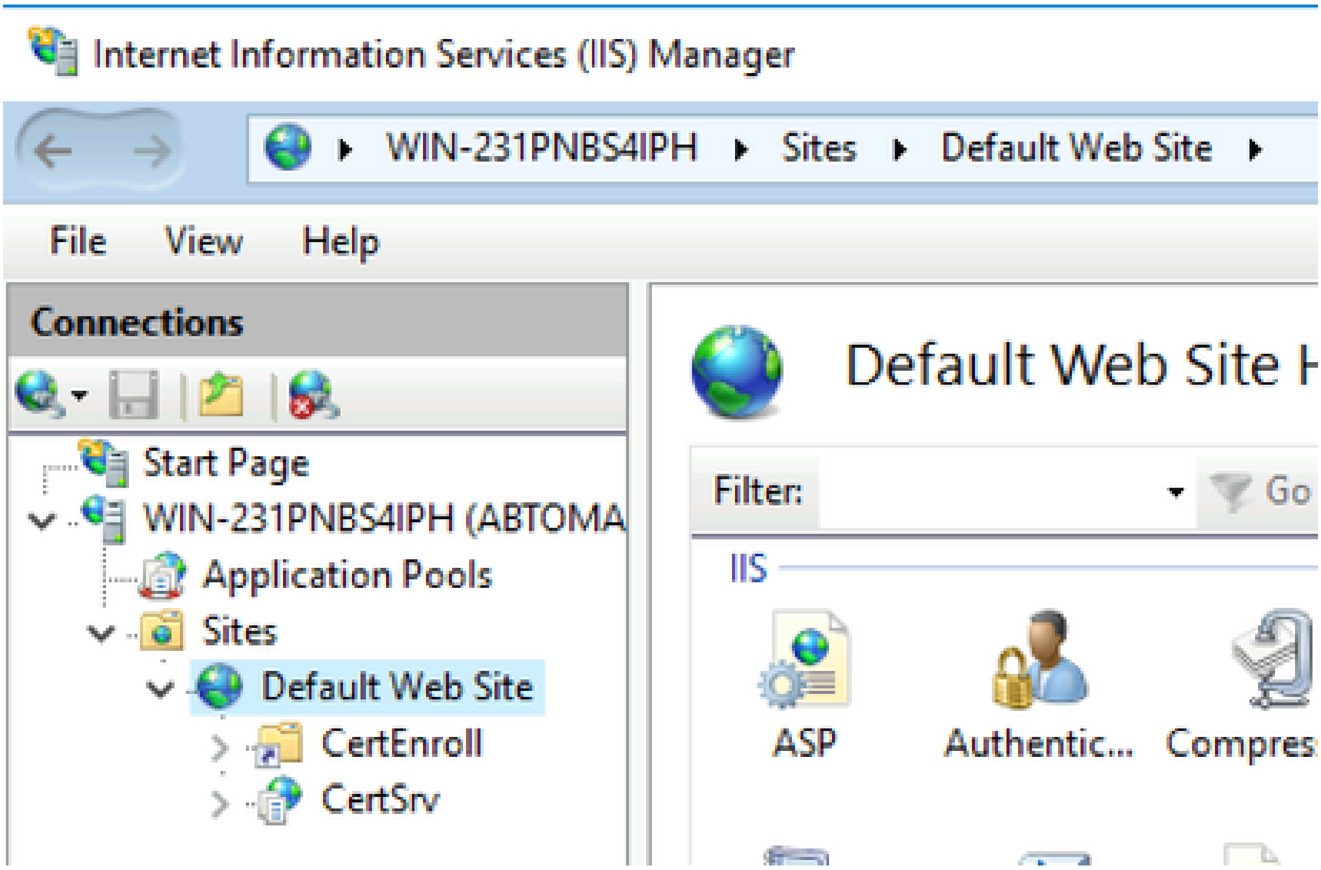
- CREATOR OWNER
- SYSTEM
- Administrators (ABTOMAR\Administrators)
- Users (ABTOMAR\Users)
- WIN-231PNBS4IPH (ABTOMAR\WIN-231PNBS4IPH$)

Permissions for WIN-231PNBS4IPH	Allow	Deny
Full control	☑	□
Modify	☑	□
Read & execute	☑	□
List folder contents	☑	□
Read	☑	□

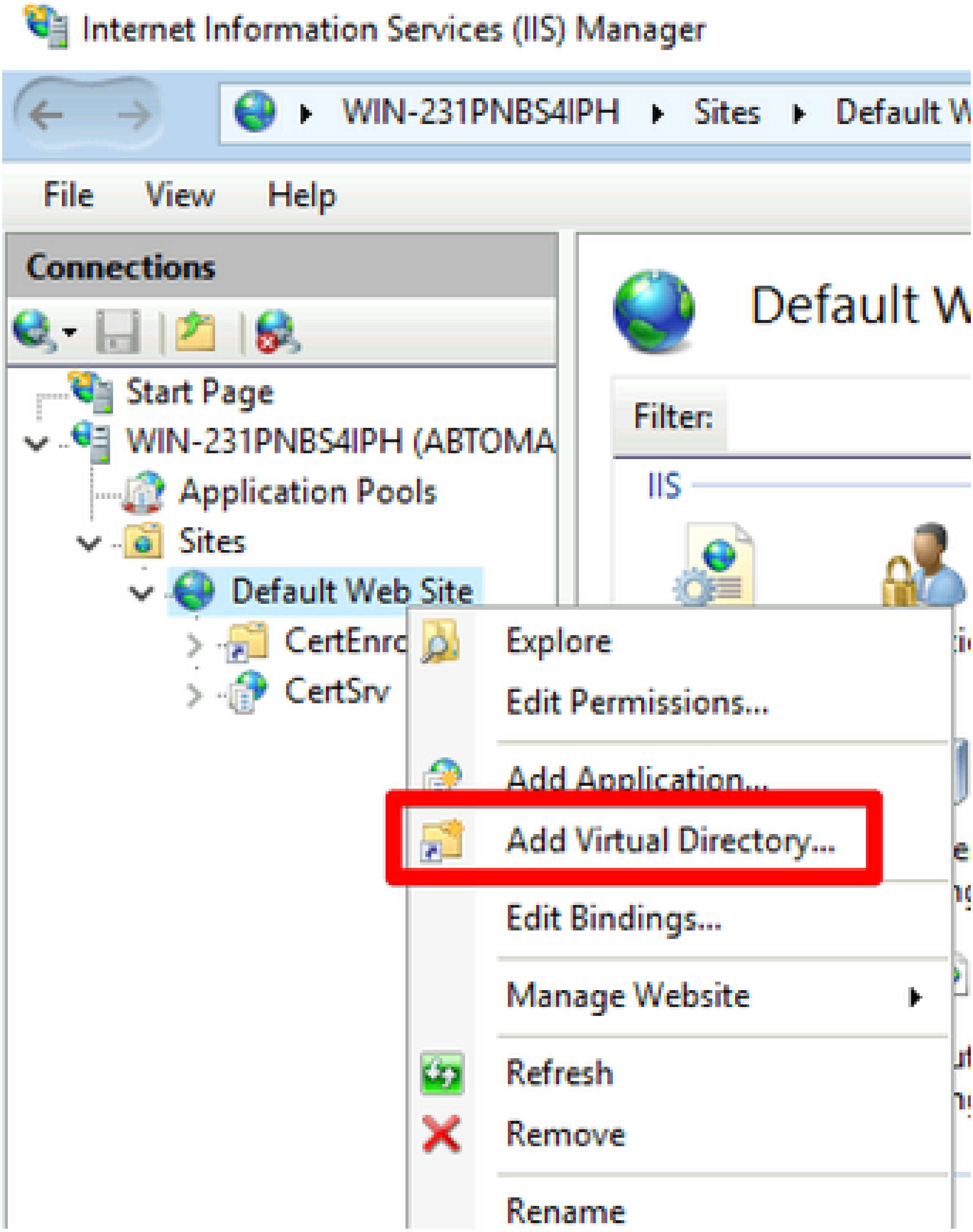
在IIS中创建站点以公开新的CRL分发点

要使ISE访问CRL文件，请使包含CRL文件的目录可通过IIS访问。

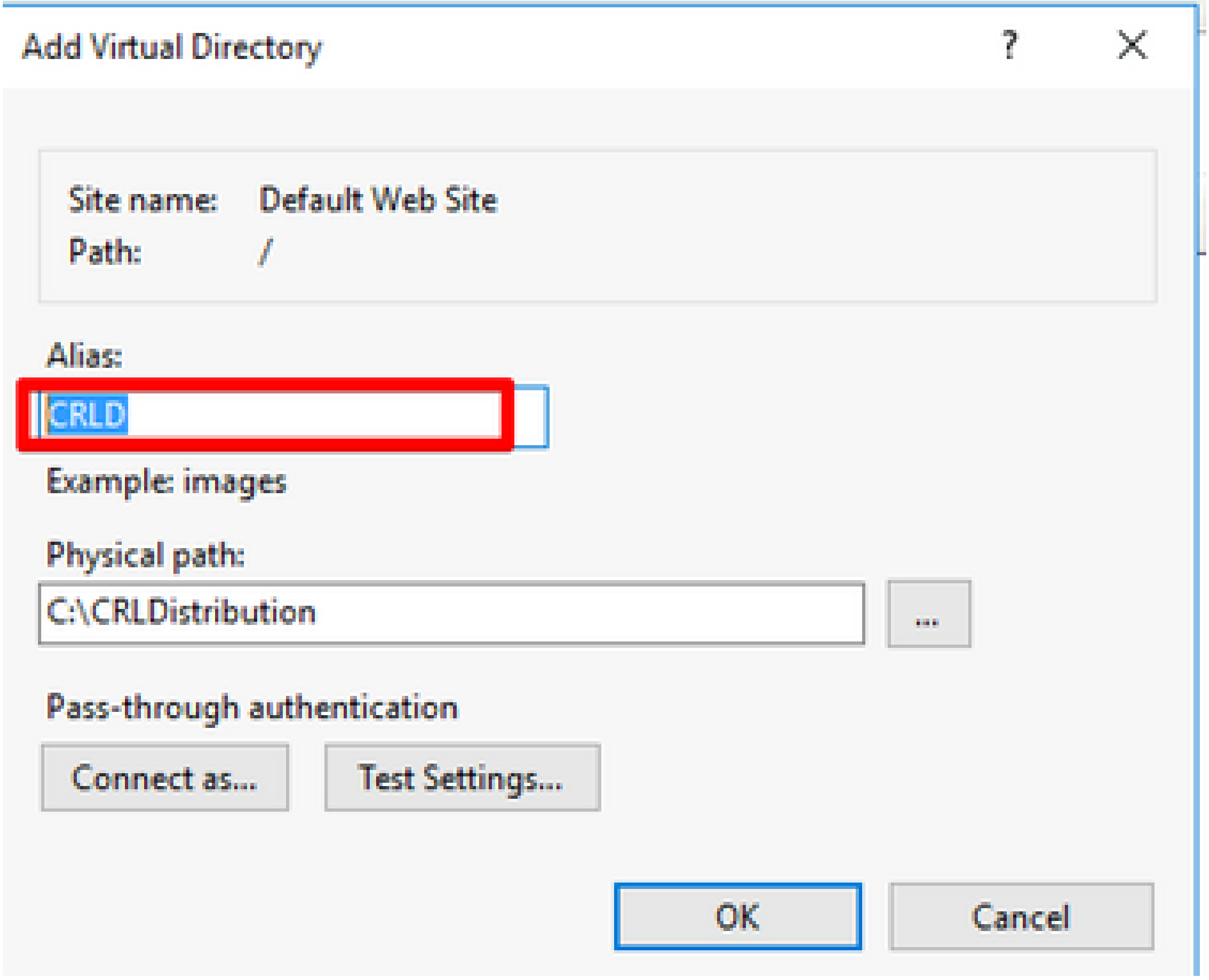
1. 在IIS服务器任务栏上，单击**Start**。选择 。 **Administrative Tools > Internet Information Services (IIS) Manager**
2. 在左侧窗格（称为控制台树）中，展开IIS服务器名称，然后展开**Sites**。



3. 右键单**Default Web Site**击并选**Add Virtual Directory**择，如下图所示。



4. 在“别名”字段中，输入CRL分发点的站点名称。在本示例中，输入CRLD。



Add Virtual Directory

Site name: Default Web Site

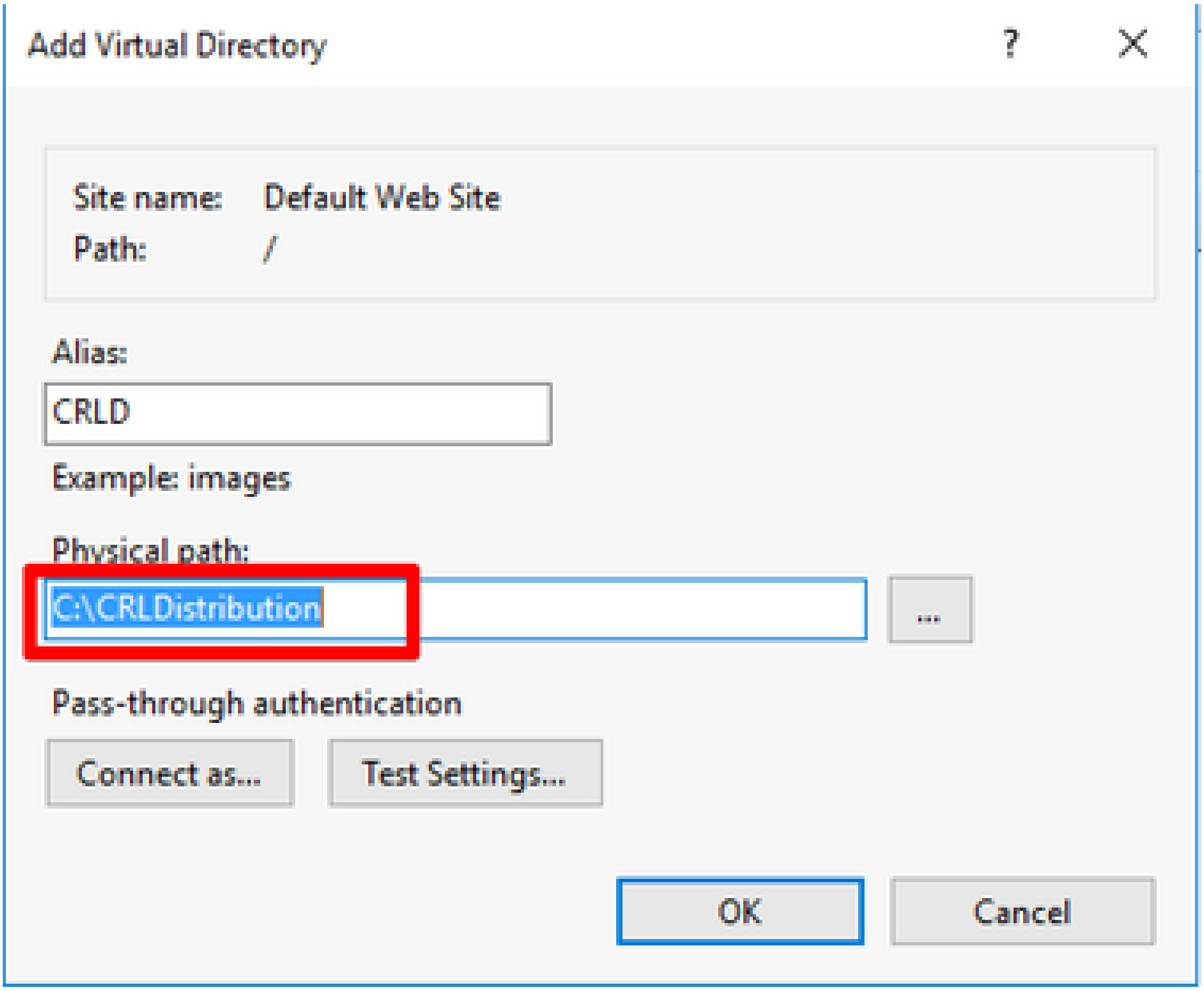
Path: /

Alias: CRLD

Example: images

Physical path: C:\CRLDistribution

5. 单击省略号(. ..)在Physical path（物理路径）字段右侧并浏览到第1部分中创建的文件夹。选择文件夹并单击OK。点击OK以关闭“添加虚拟目录”窗口。



Add Virtual Directory

Site name: Default Web Site

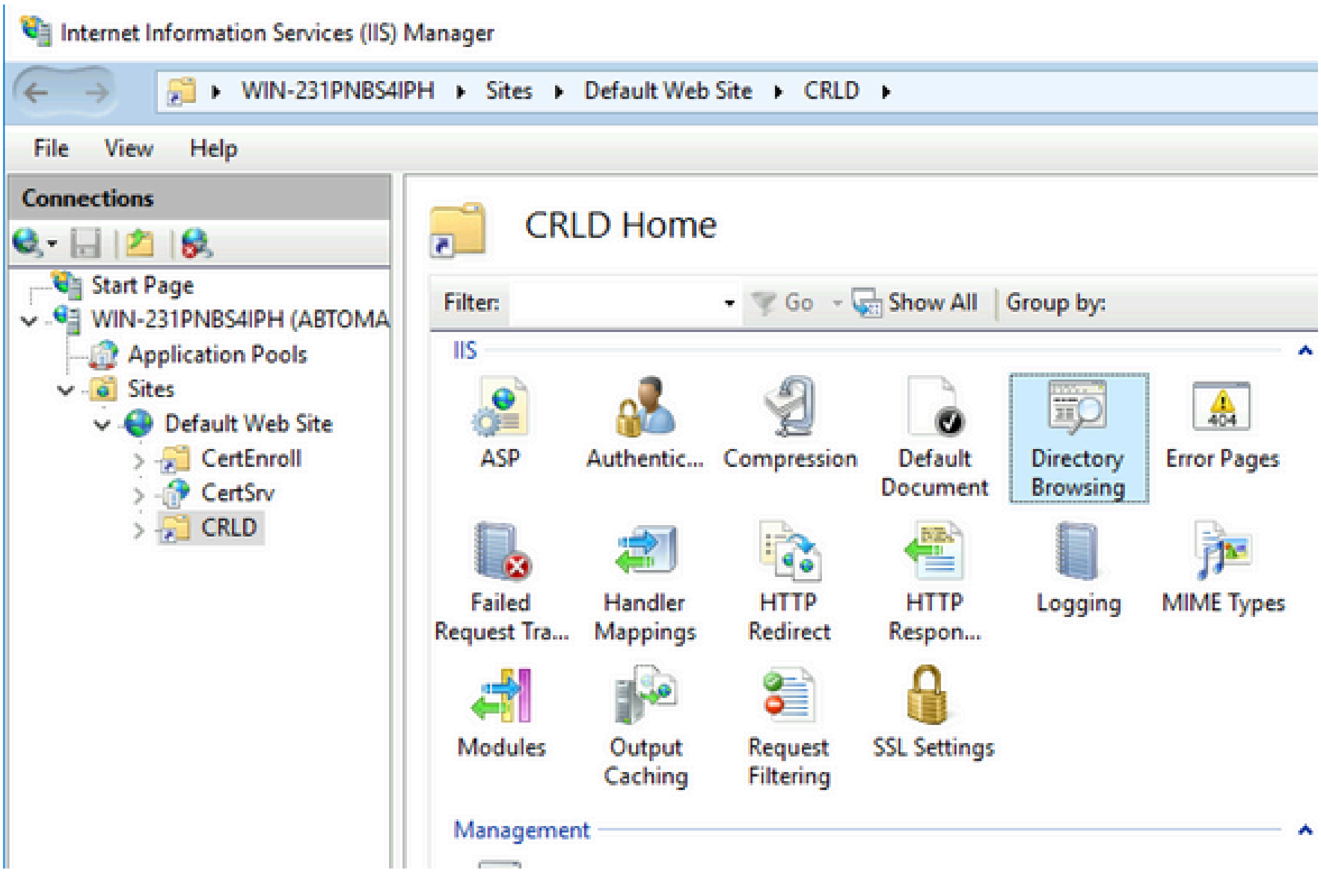
Path: /

Alias: CRLD

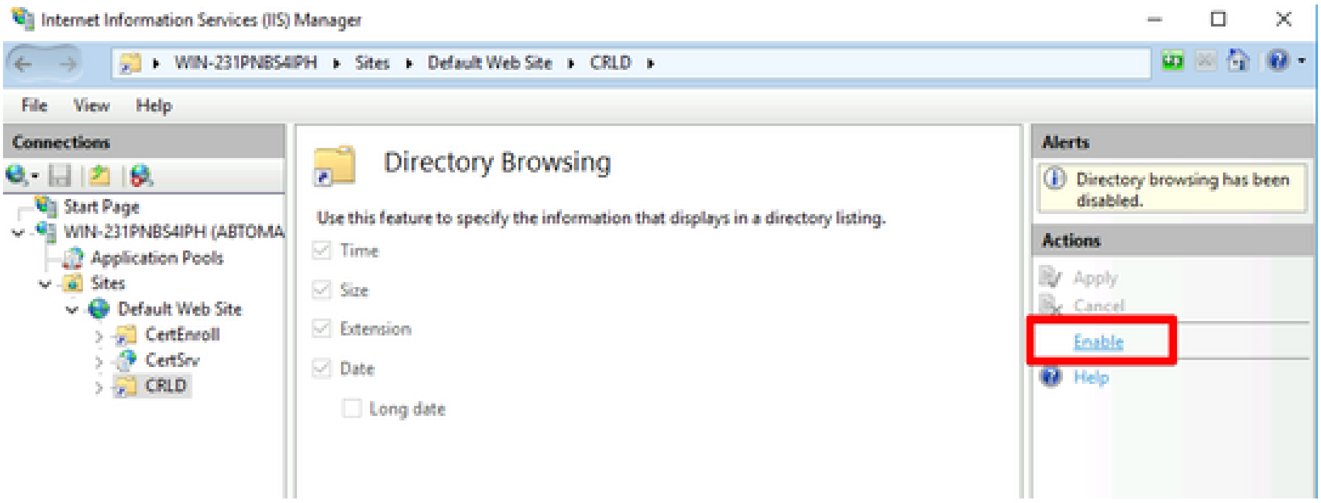
Example: images

Physical path: C:\CRLDistribution

6. 在步骤4中输入的站点名称必须在左窗格中突出显示。否则，请立即选择它。在中心窗格中，双击**Directory Browsing**。



7. 在右侧窗格中，**Enable**单击以启用目录浏览。



Directory Browsing

Use this feature to specify the information that displays in a directory listing.

☑ Time

☑ Size

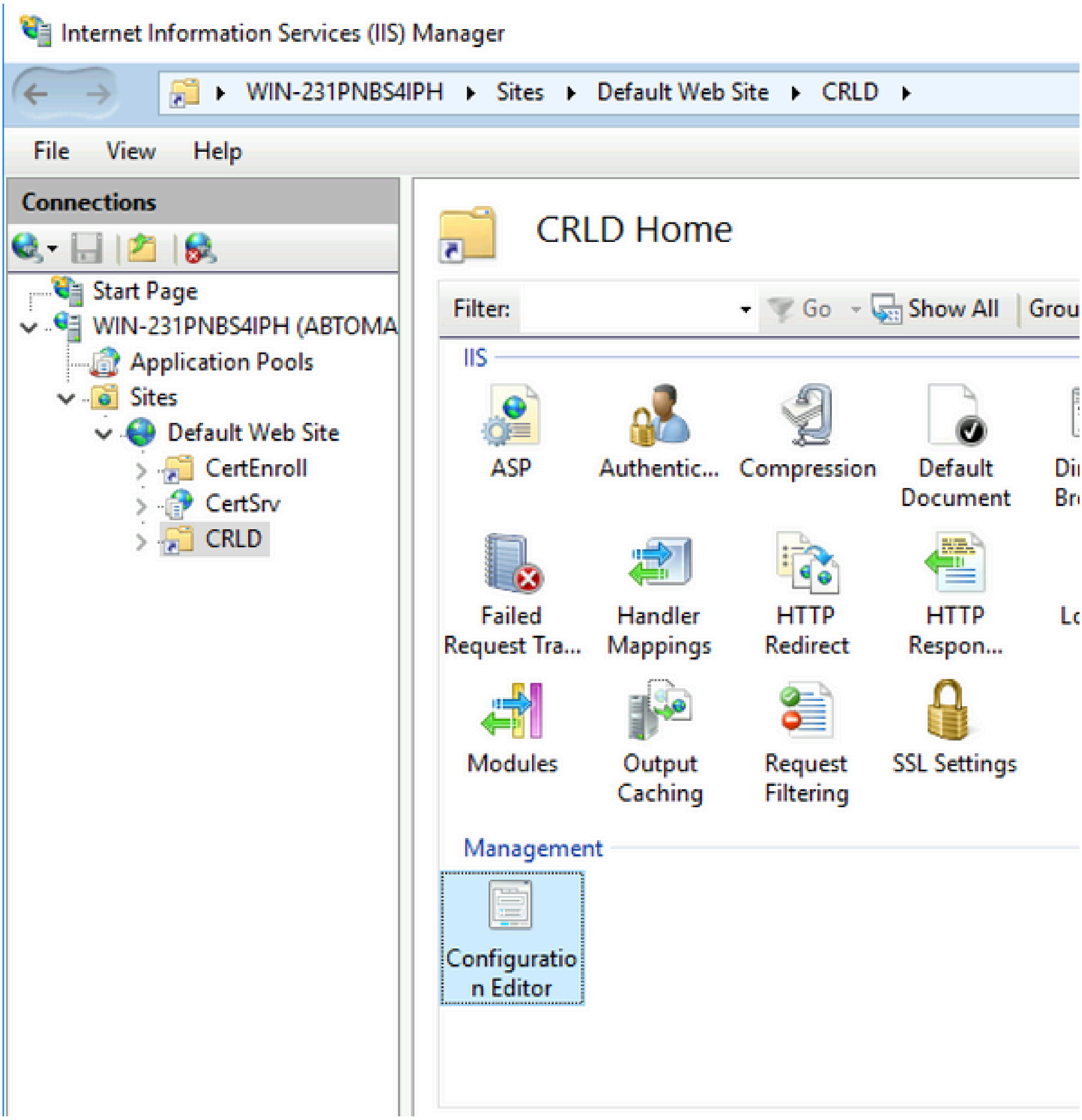
☑ Extension

☑ Date

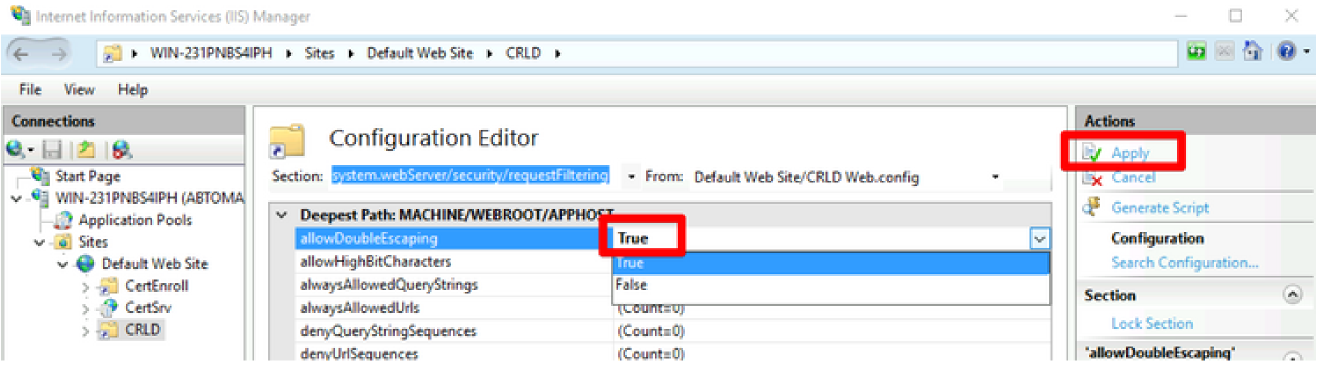
□ Long date

Directory browsing has been disabled.

8. 在左侧窗格中，再次选择站点名称。在中心窗格中，双击**Configuration Editor**。



9. 在Section下拉列表中，选择system.webServer/security/requestFiltering。在下allowDoubleEscaping拉列表中，选择True。在右侧窗格中，点Apply击，如下图所示。



Configuration Editor

Section: system.webServer/security/requestFiltering · From: Default Web Site/CRLD Web.config

Deepest Path: MACHINE/WEBROOT/APPHOST

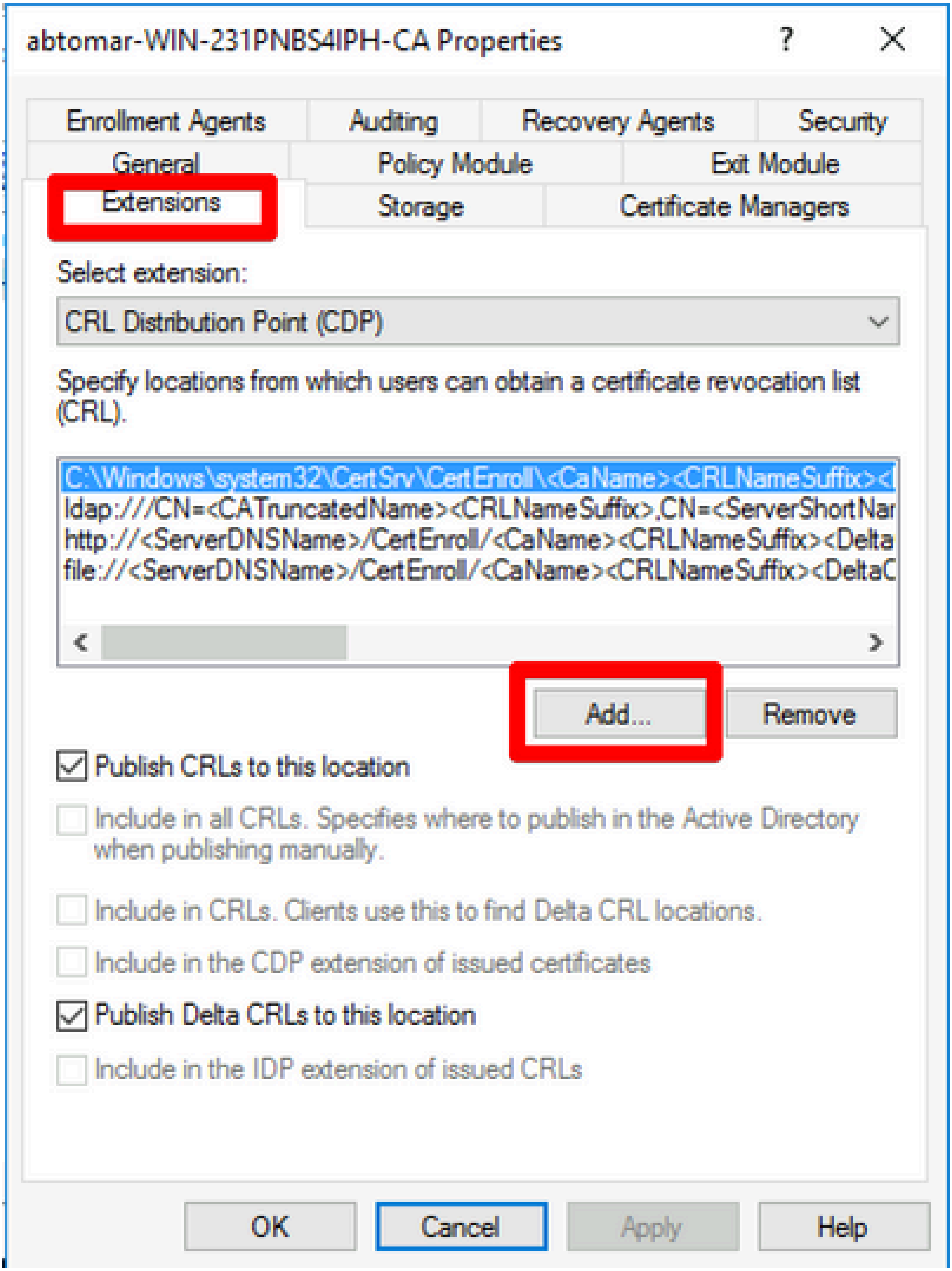
```
allowDoubleEscaping           True
allowHighBitCharacters        True
alwaysAllowedQueryStrings     False
alwaysAllowedUrls             (Count=0)
denyQueryStringSequences      (Count=0)
denyUrlSequences              (Count=0)
```

现在必须通过IIS访问该文件夹。

配置Microsoft CA服务器以将CRL文件发布到分发点

现在已配置新文件夹来容纳CRL文件，并且该文件夹已在IIS中公开，请将Microsoft CA服务器配置为将CRL文件发布到新位置。

1. 在CA服务器任务栏上，单**Start**击。选择 。**Administrative Tools > Certificate Authority**
2. 在左窗格中，右键单击CA名称。选择**Properties**并点击该选项**Extensions**卡。要添加新的CRL分发点，请点击**Add**。



abtomar-WIN-231PNBS4IPH-CA Properties

Select extension:

CRL Distribution Point (CDP)

Specify locations from which users can obtain a certificate revocation list (CRL).

```
C:\Windows\system32\CertSrv\CertEnroll\<CaName><CRLNameSuffix><[
ldap:///CN=<CATruncatedName><CRLNameSuffix>,CN=<ServerShortNar
http://<ServerDNSName>/CertEnroll/<CaName><CRLNameSuffix><Delta
file://<ServerDNSName>/CertEnroll/<CaName><CRLNameSuffix><DeltaC
```

☑ Publish CRLs to this location

□ Include in all CRLs. Specifies where to publish in the Active Directory when publishing manually.

□ Include in CRLs. Clients use this to find Delta CRL locations.

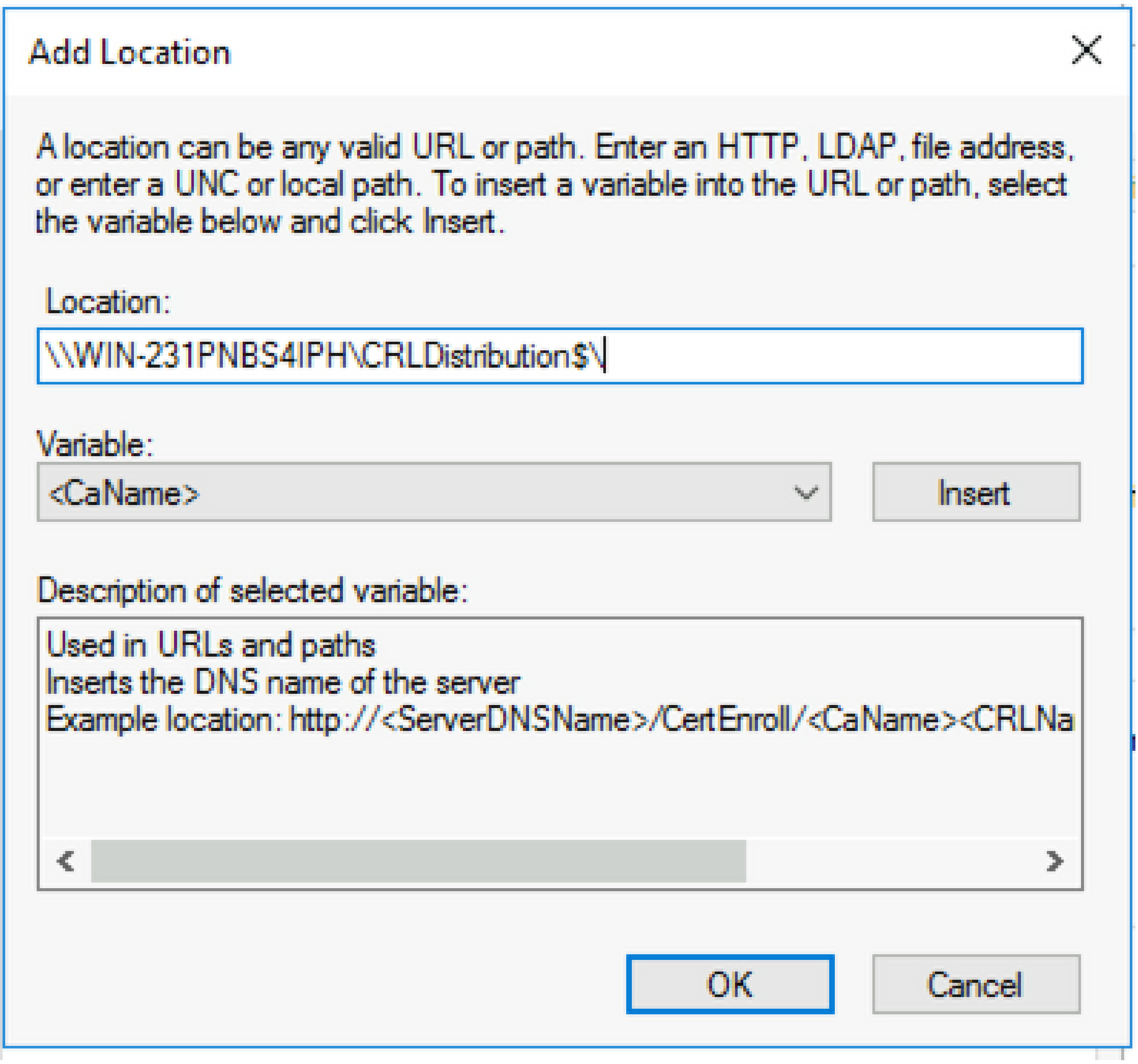
□ Include in the CDP extension of issued certificates

☑ Publish Delta CRLs to this location

□ Include in the IDP extension of issued CRLs

3. 在Location字段中，输入在第1部分创建和共享的文件夹的路径。在第1部分的示例中，路径为：

\\WIN-231PNBS4IPH\CRLDISTRIBUTION$



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$\

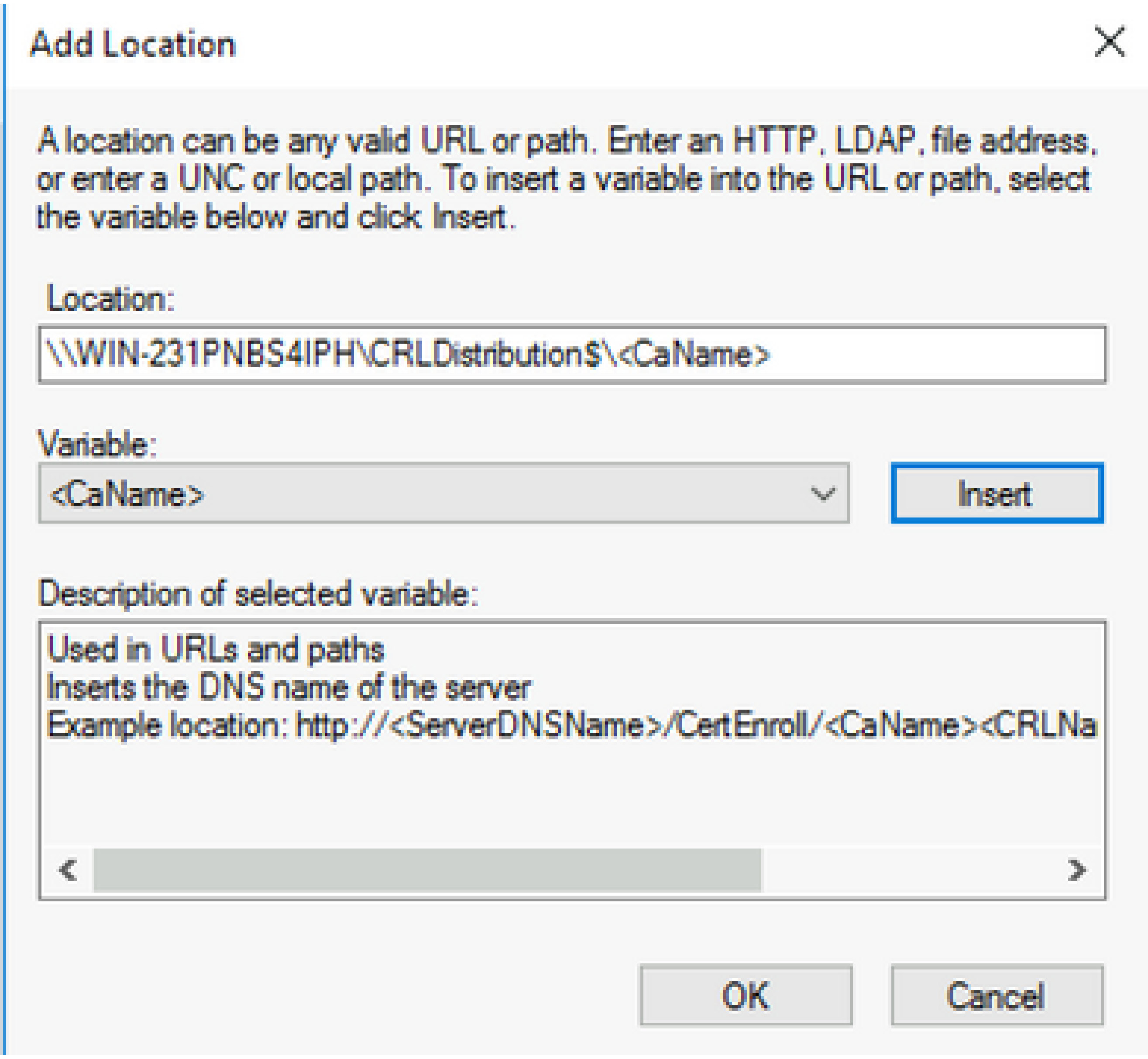
Variable:

<CaName>

Description of selected variable:

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

4. 填写Location字段后，从
   Variable下拉列表中选择，然后点击 **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>

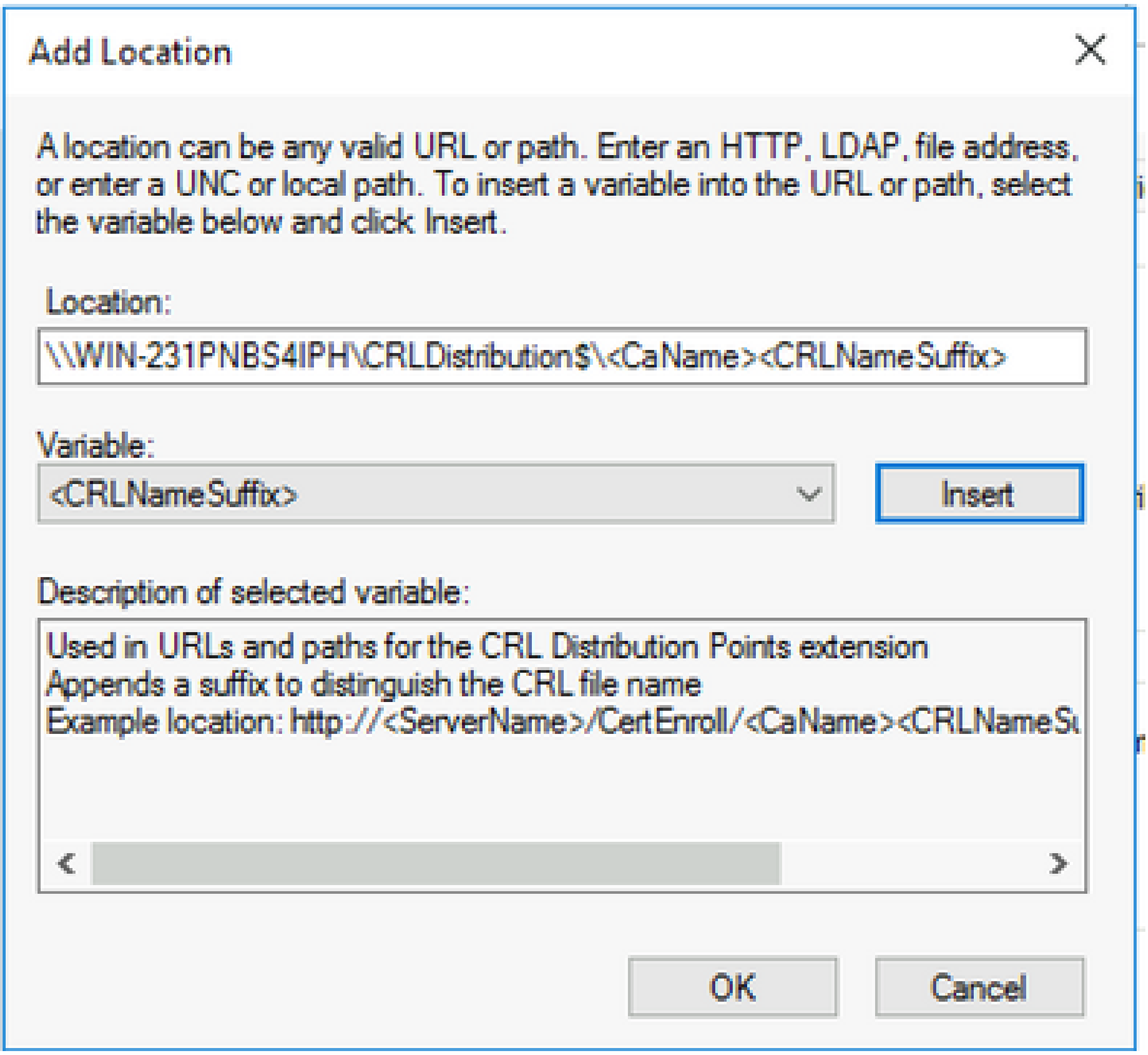
Variable:

<CaName>

Description of selected variable:

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

5. 从变量(Variable)下拉列表中，选择并
   单击“变量”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><CRLNameSuffix>

Variable:

<CRLNameSuffix>

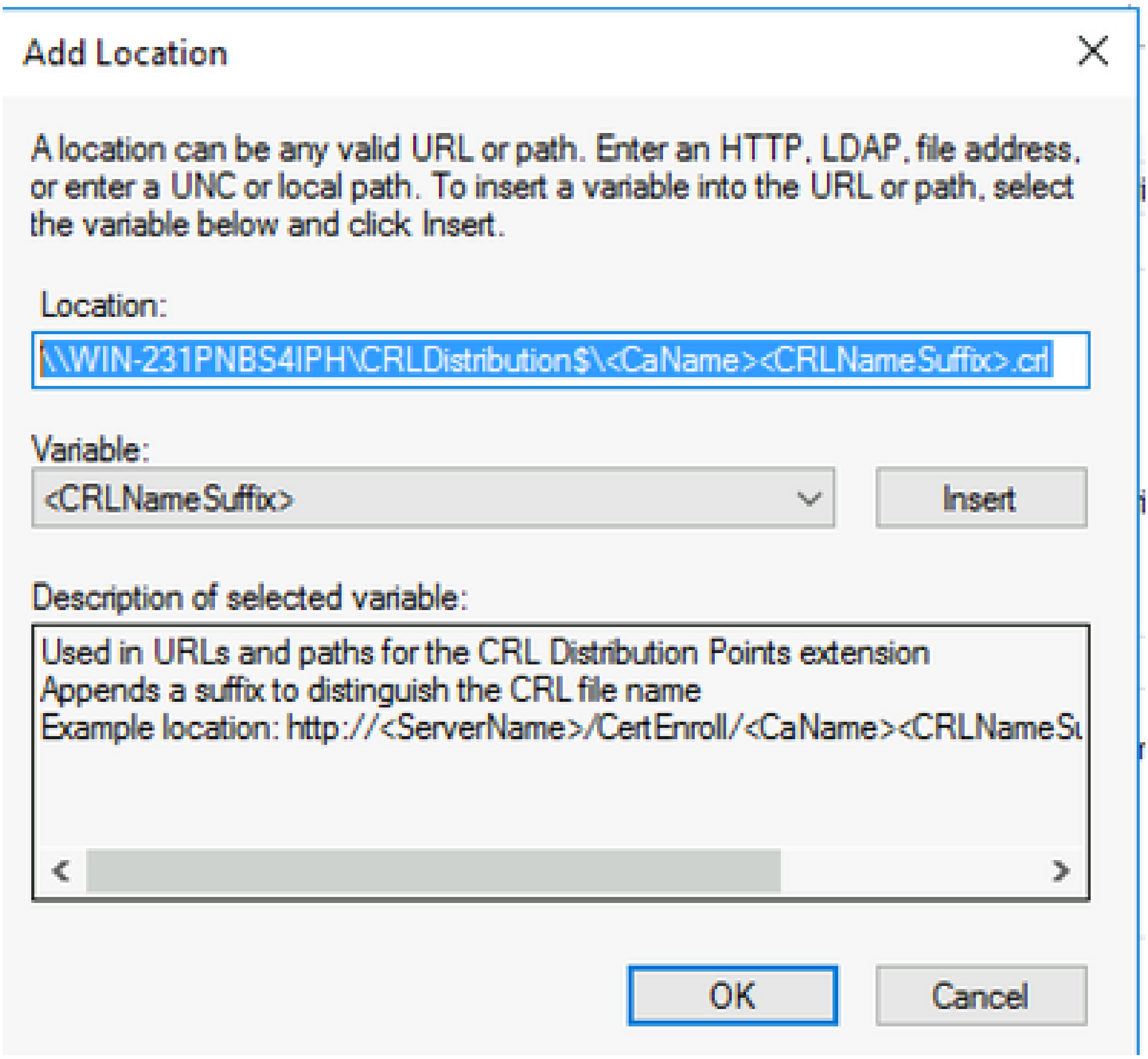
Description of selected variable:

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

6. 在Location字段中，.crl追加到路径末尾。在本示例中，位置为：

\\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:

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

Variable:

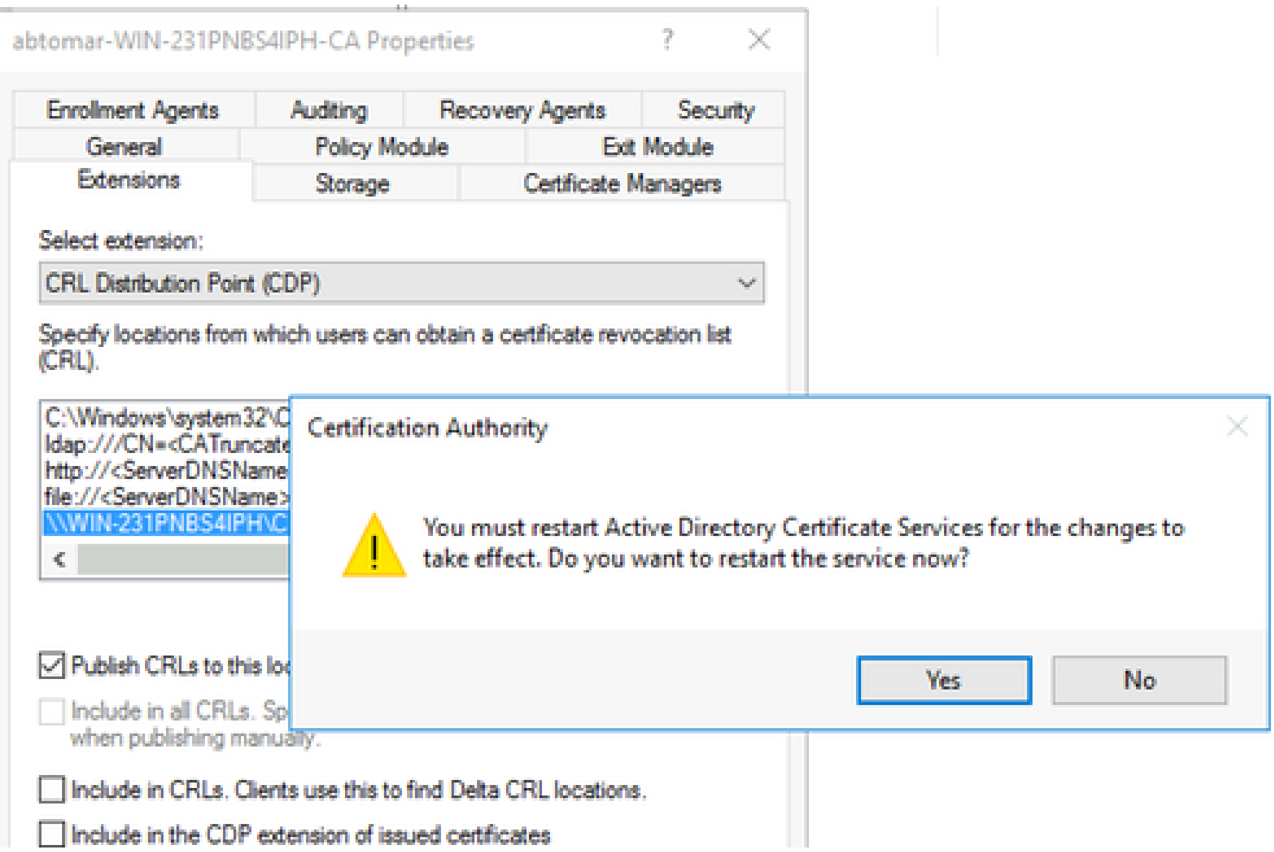
<CRLNameSuffix>

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

7. 点击**OK**以返回到Extensions（分机）选项卡。选中此复**Publish CRLs to this location**选框，然后单击关**OK**闭“属性”窗口。

   系统将显示一个提示符，询问是否有权重新启动Active Directory证书服务。单击。**Yes**



abtomar-WIN-231PNBS4IPH-CA Properties

Select extension:

CRL Distribution Point (CDP)

Specify locations from which users can obtain a certificate revocation list (CRL).

```
C:\Windows\system32\C
ldap:///CN=<CATruncate
http://<ServerDNSName
file://<ServerDNSName>
\\WIN-231PNBS4IPH\C
```

☑ Publish CRLs to this lo

□ Include in all CRLs. Sp
when publishing manually.

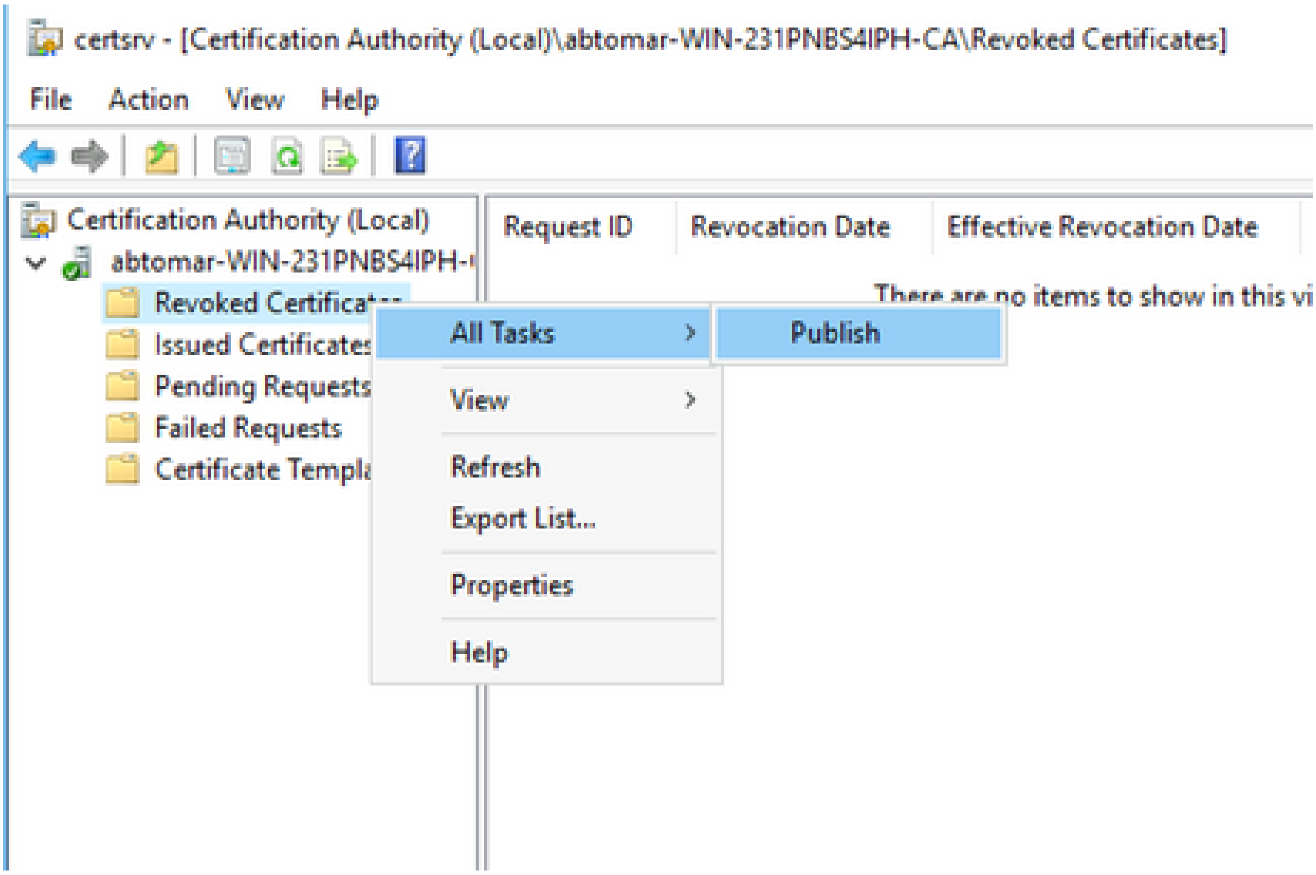
□ Include in CRLs. Clients use this to find Delta CRL locations.

□ Include in the CDP extension of issued certificates

Certification Authority

You must restart Active Directory Certificate Services for the changes to take effect. Do you want to restart the service now?

8. 在左窗格中，右键单Revoked Certificates击。选择 。All Tasks > Publish确保选中“New CRL（新建CRL）”，然后单OK击。



certsrv - [Certification Authority (Local)\abtomar-WIN-231PNBS4IPH-CA\Revoked Certificates]

There are no items to show in this vi

Microsoft CA服务器必须在第1节中创建的文件夹中创建新的.crl文件。如果成功创建新的

CRL文件，则单击“确定”(OK)后将不会出现对话框。如果返回有关新分发点文件夹的错误，请仔细重复本节中的步骤。

验证CRL文件存在且可通过IIS访问

在开始本部分之前，验证新的CRL文件是否存在，以及是否可以从其他工作站通过IIS访问这些文件。

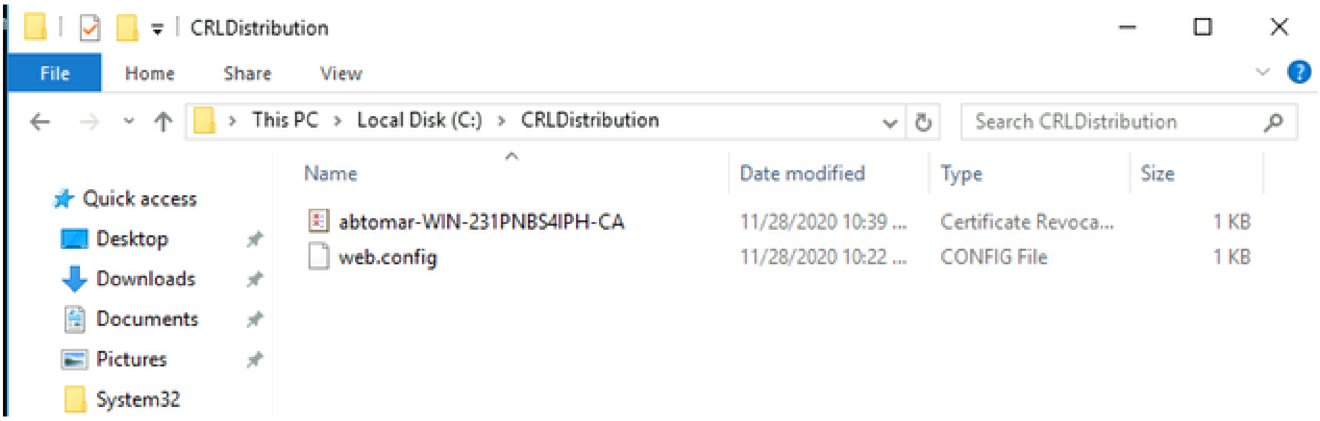
1. 在IIS服务器上，打开第1部分中创建的文件夹。必须存在一个.crl文件，其格

   .crl

   式

   为CA服务器的名称。在本示例中，文件名是：

   abtomar-WIN-231PNBS4IPH-CA.crl


CRLDistribution

File Home Share View

This PC > Local Disk (C:) > CRLDistribution

Search CRLDistribution

Quick access
Desktop
Downloads
Documents
Pictures
System32

Name	Date modified	Type	Size
abtomar-WIN-231PNBS4IPH-CA	11/28/2020 10:39 ...	Certificate Revoca...	1 KB
web.config	11/28/2020 10:22 ...	CONFIG File	1 KB

2. 从网络上的工作站（最好与ISE主管理节点位于同一网络中），打开Web浏览器，浏览到第2部分中配置的IIS服务器的服务器名称http://

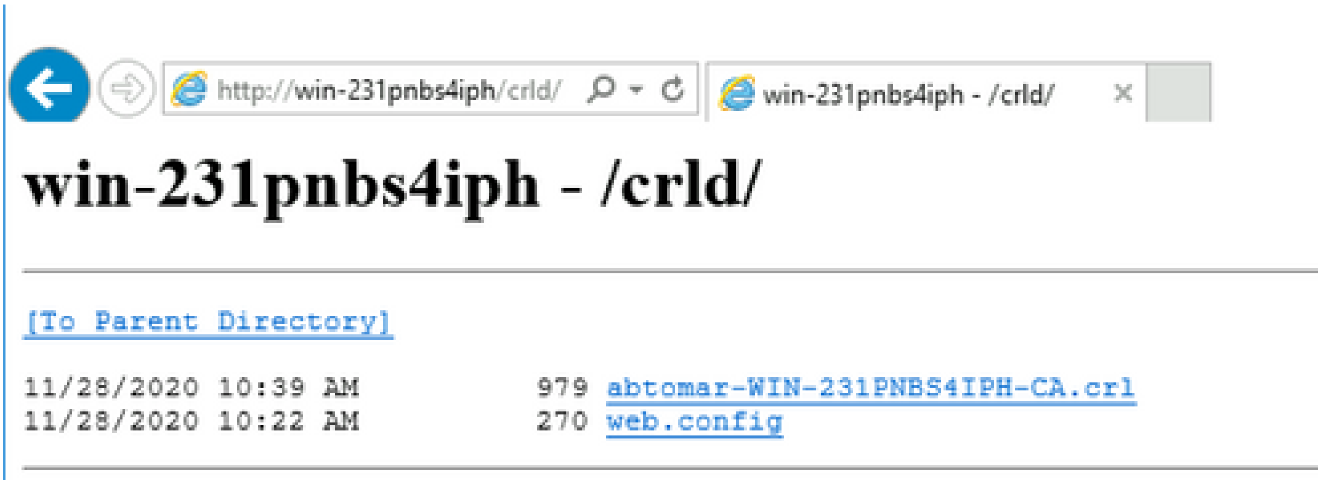
   /

   ，以及第2部分中为分发点选择的站点名

   。在本示例中，URL为：

   http://win-231pnbs4iph/CRLD

   系统随即会显示目录索引，其中包括在步骤1中观察到的文件。



win-231pnbs4iph - /crld/

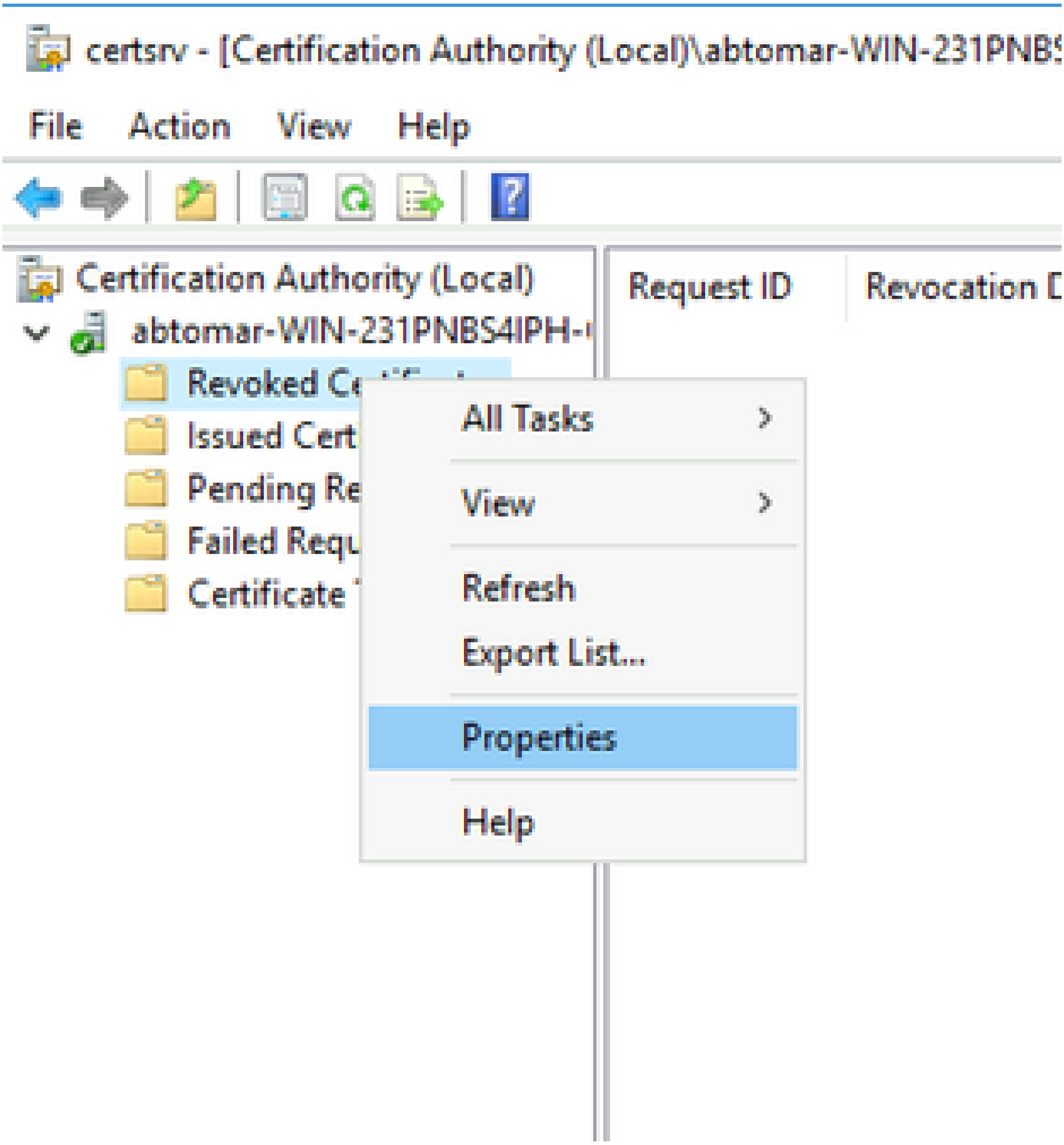
[To Parent Directory]

```
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分发点

在将ISE配置为检索CRL之前，请定义发布CRL的时间间隔。确定此间隔的策略不在本文档的讨论范围之内。潜在值（在Microsoft CA中）为1小时到411年（含）。默认值为1周。确定适合您环境的间隔后，请使用以下说明设置间隔：

1. 在CA服务器任务栏上，单**Start**击。选择 。**Administrative Tools > Certificate Authority**
2. 在左侧窗格中，展开CA。右键单击该文件**Revoked Certificates**夹并选择**Properties**它。
3. 在CRL发布间隔字段中，输入所需的编号并选择时间段。单击**OK**关闭窗口并应用更改。在本例中，配置七天的发布间隔。



4. 输入命**certutil -getreg CA\Clock***令以确认ClockSkew值。默认值为10分钟。

   示例输出：

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

5. 输入命**certutil -getreg CA\CRLov***令以验证是否已手动设置CRLOverlapPeriod。默认情况下，CRLOverlapUnit值为0，表示未设置手动值。如果该值不是0，请记录该值和单位。

示例输出：

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

6. 输入命**certutil -getreg CA\CRLpe***令以验证在步骤3中设置的CRLPeriod。

   示例输出：

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

7. 按如下方式计算CRL宽限期：

   a.如果在第5步中设置CRLOverlapPeriod:OVERLAP = CRLOverlapPeriod，以分钟为单位；

   否则：重叠=(CRLeriod / 10)，以分钟为单位

   b.如果重叠超过720，则重叠为720

   c.如果重叠<(1.5 * ClockSkewMinutes)，则重叠=(1.5 * ClockSkewMinutes)

   d.如果OVERLAP > CRLPeriod，则重叠= CRLPeriod，以分钟为单位

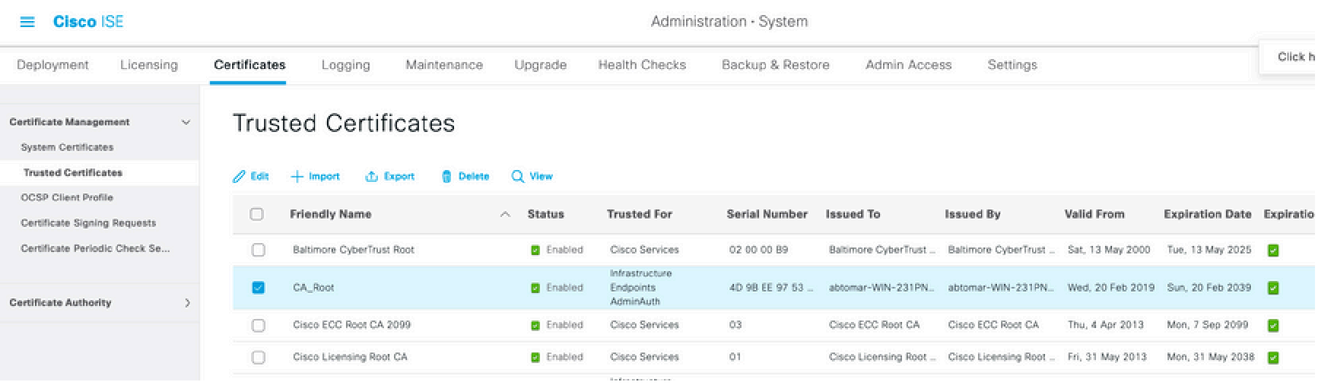
   e.宽限期=重叠+时滞Minutes

```
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
```

计算出的宽限期是CA发布下一个CRL到当前CRL到期之间的时间量。需要配置ISE以相应地检索CRL。

8. 登录到ISE主管理节点并选择**Administration** > **System** > **Certificates**。在左侧窗格中，选择**Trusted Certificate**

。



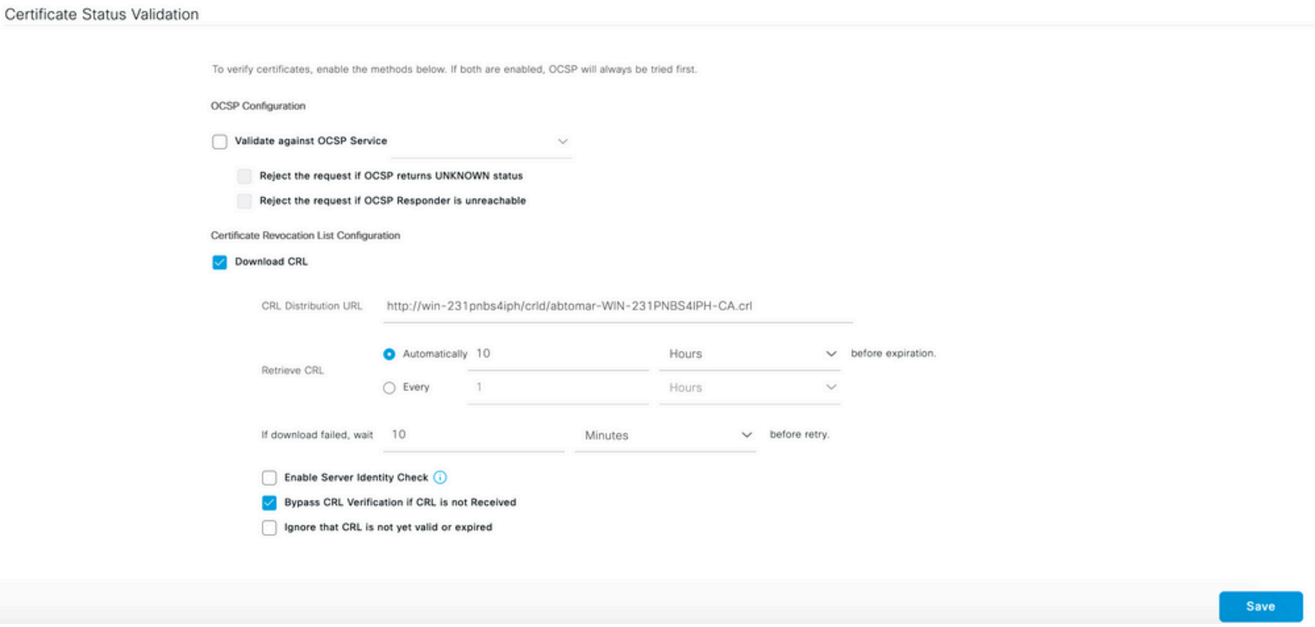
Trusted Certificates

	Friendly Name	Status	Trusted For	Serial Number	Issued To	Issued By	Valid From	Expiration Date	Expiratio
□	Baltimore CyberTrust Root	Enabled	Cisco Services	02 00 00 B9	Baltimore CyberTrust ...	Baltimore CyberTrust ...	Sat, 13 May 2000	Tue, 13 May 2025	✓
☑	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	✓
□	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	✓
□	Cisco Licensing Root CA	Enabled	Cisco Services	01	Cisco Licensing Root ...	Cisco Licensing Root ...	Fri, 31 May 2013	Mon, 31 May 2038	✓

9. 选中要为其配置CRL的CA证书旁边的复选框。单击。**Edit**
10. 在窗口底部附近，选中此**Download CRL**复选框。
11. 在CRL分发URL字段中，输入CRL分发点的路径，其中包括第2部分中创建的.crl文件。在本示例中，URL为：

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

12. ISE可配置为按固定间隔或基于到期时间（通常也是固定间隔）检索CRL。当CRL发布间隔为静态时，使用后一个选项可获得更及时的CRL更新。单击单**Automatically**选按钮。
13. 将检索值设置为小于在步骤7中计算的宽限期的值。如果值集大于宽限期，ISE会在CA发布下一个CRL之前检查CRL分发点。在此示例中，宽限期计算为730分钟或12小时10分钟。检索将使用10小时的值。
14. 根据您的环境设置重试间隔。如果ISE无法按上一步中配置的间隔检索CRL，它将按此较短间隔重试。
15. 如果**Bypass CRL Verification if CRL is not Received**ISE在上次下载尝试时无法检索此CA的CRL，请选中此复选框以允许基于证书的身份验证正常进行（并且不选中CRL检查）。如果未选中此复选框，则在无法检索CRL时，使用此CA颁发的证书的所有基于证书的身份验证都将失败。
16. 选中此**Ignore that CRL is not yet valid or expired**复选框可允许ISE使用已过期（或尚未有效）的CRL文件，就像它们有效一样。如果未选中此复选框，则ISE会将CRL视为在其生效日期之前和下次更新时间之后无效。点击**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: http://win-231pnbs4iph/crld/abtomar-WIN-231PNBS4IPH-CA.crl

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

验证

当前没有可用于此配置的验证过程。

故障排除

目前没有针对此配置的故障排除信息。

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。