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信息服务(IIS)以发布证书撤销列表(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)（版本3.0及更高版本）以检索更新以用于证书验证。ISE可配置为检索其在证书验证中使用的各种CA根证书的CRL。

先决条件

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。

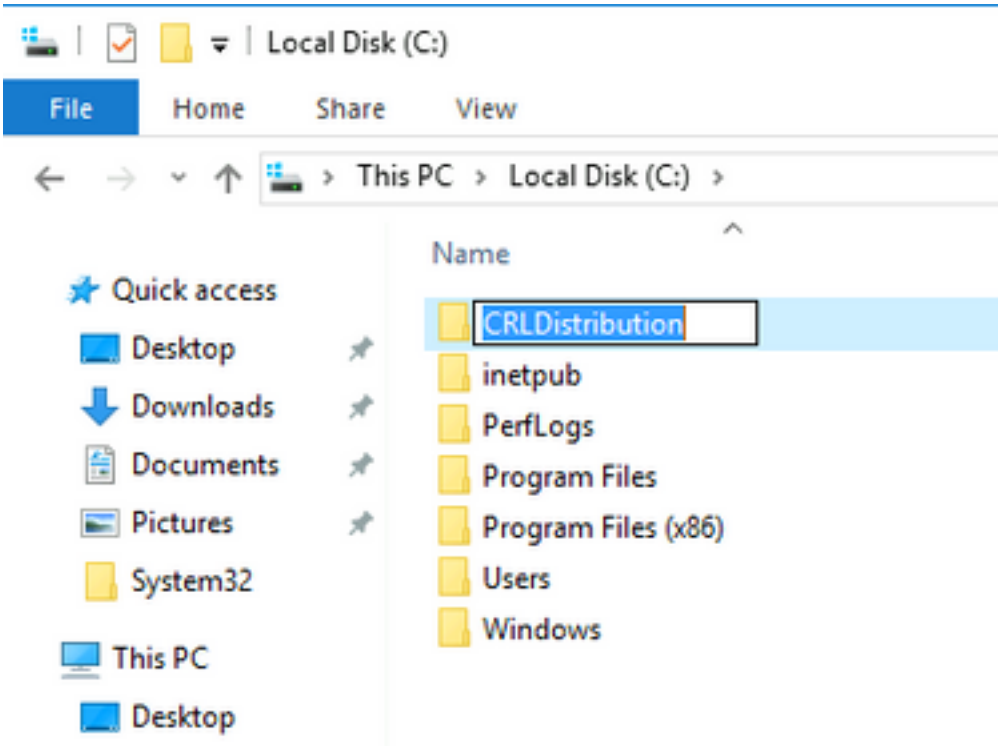
在CA上创建并配置文件夹以容纳CRL文件

第一项任务是在CA服务器上配置一个位置以存储CRL文件。默认情况下，Microsoft CA服务器将文

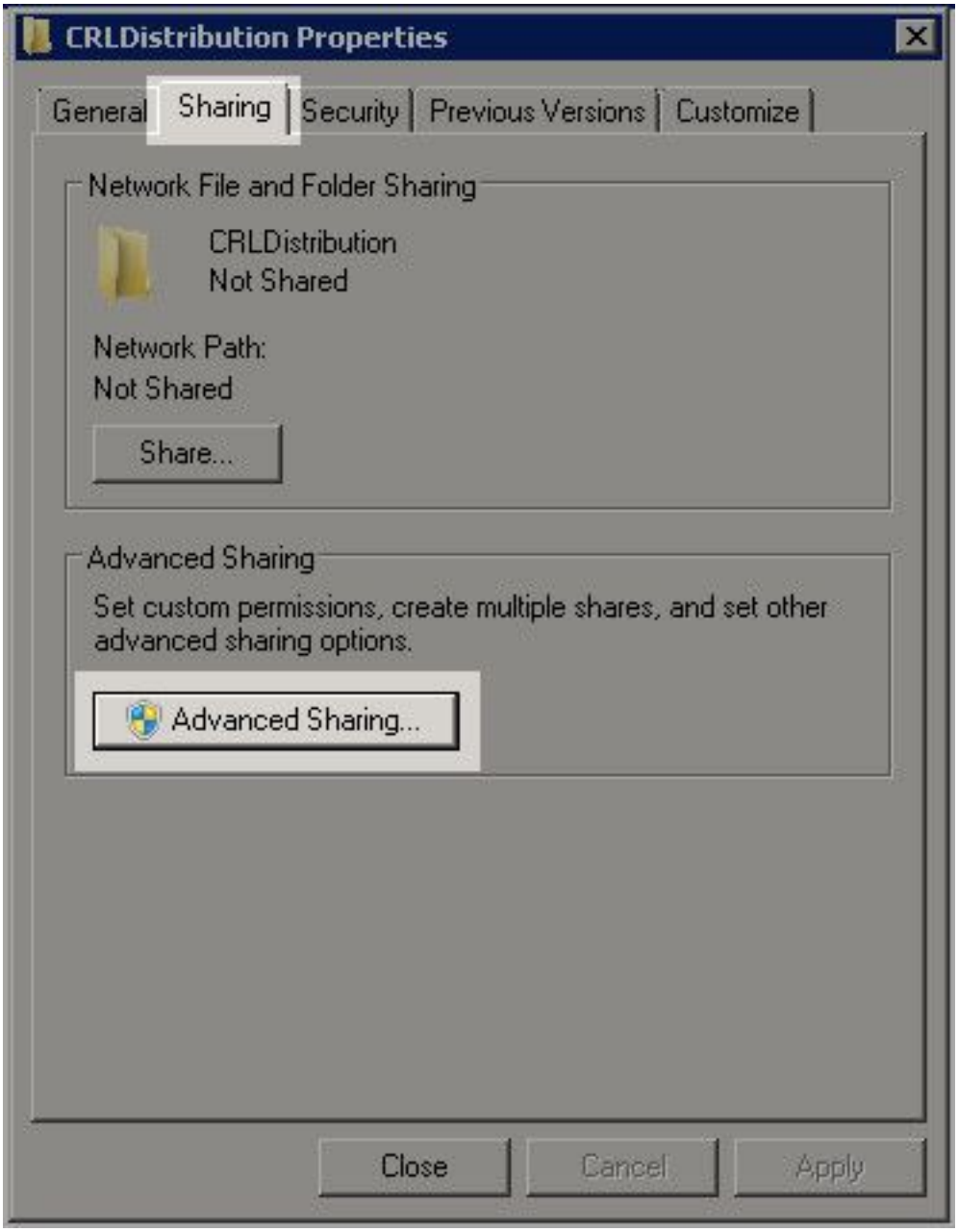
件发布到C:\Windows\system32\CertSrv\CertEnroll\

不使用此系统文件夹，而是为文件创建新文件夹。

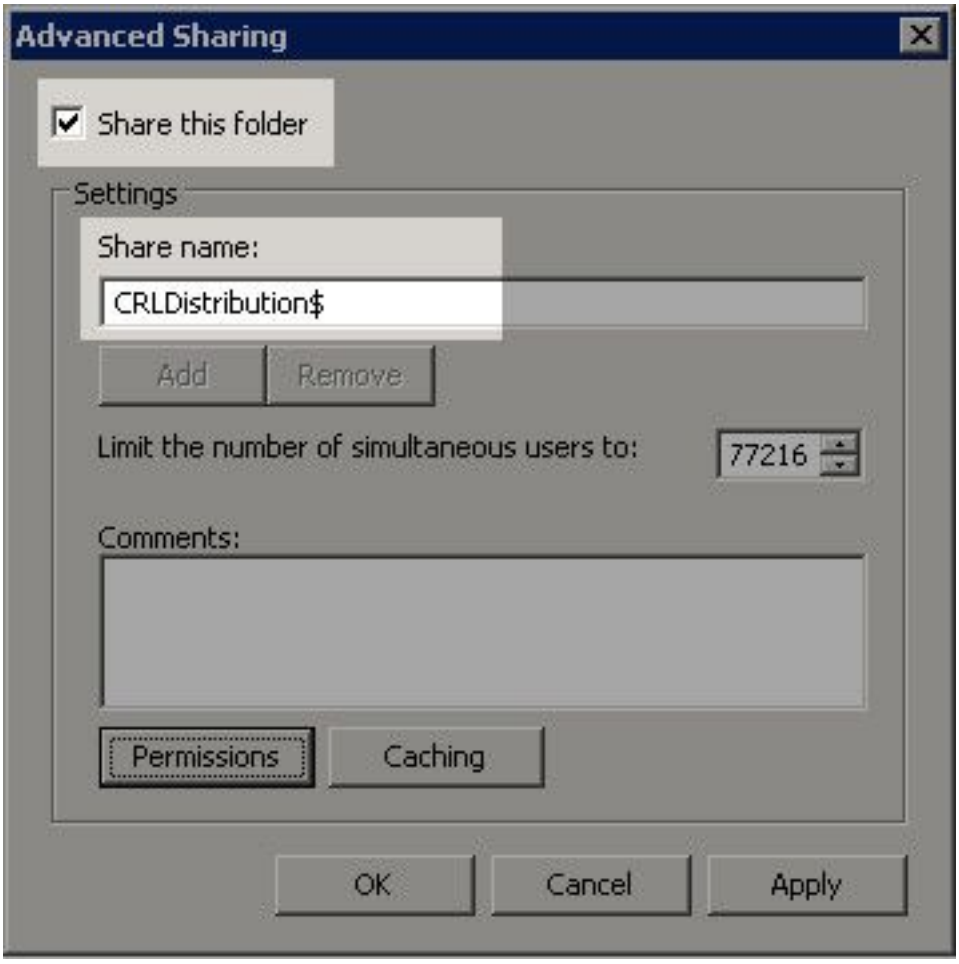
1. 在IIS服务器上，选择文件系统上的位置并创建新文件夹。在本例中，创建了C:\CRLDistribution文件夹。



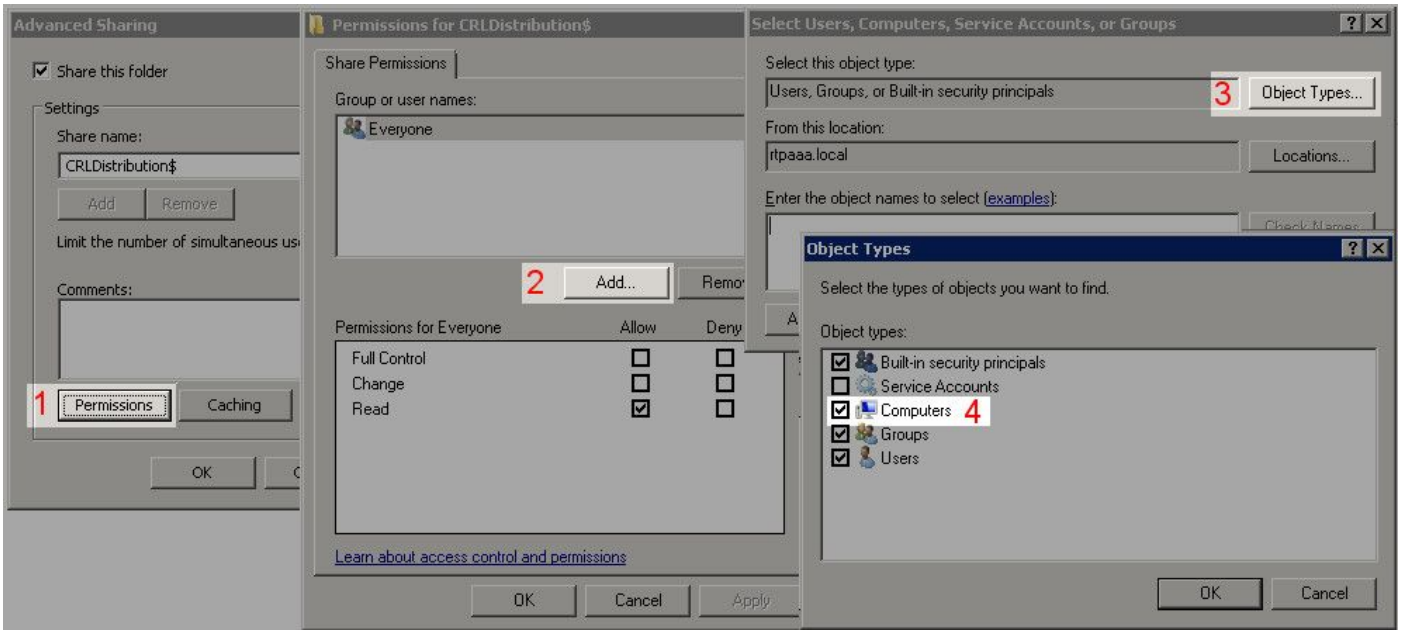
2.为使CA将CRL文件写入新文件夹，必须启用共享。右键单击新文件夹，选择“属性”，单击“共享”选项卡，然后单击“高级共享”。



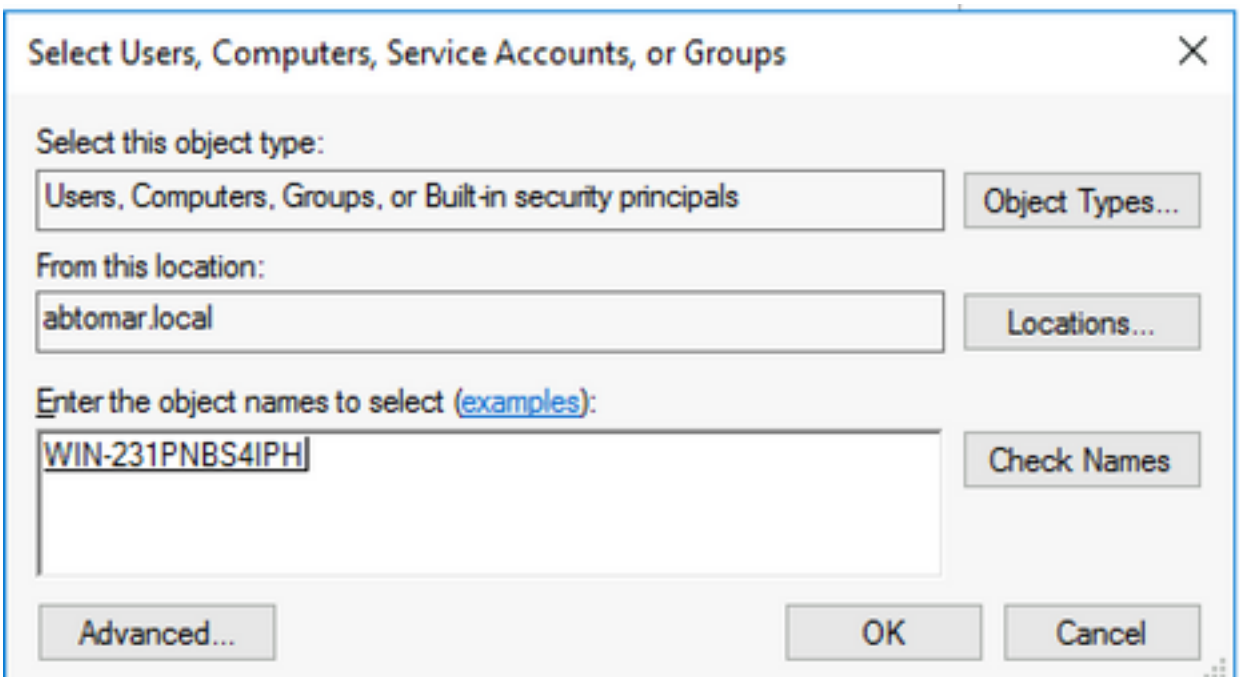
3.要共享文件夹，请选中**共享此文件夹**复选框，然后在“共享名”字段的共享名末尾添加美元符号($)以隐藏共享。



4.单击“**权限**(1)”，单击“**添加**(2)”，单击“对象类型(3)”，然后选中“计算机”复选框(4)。

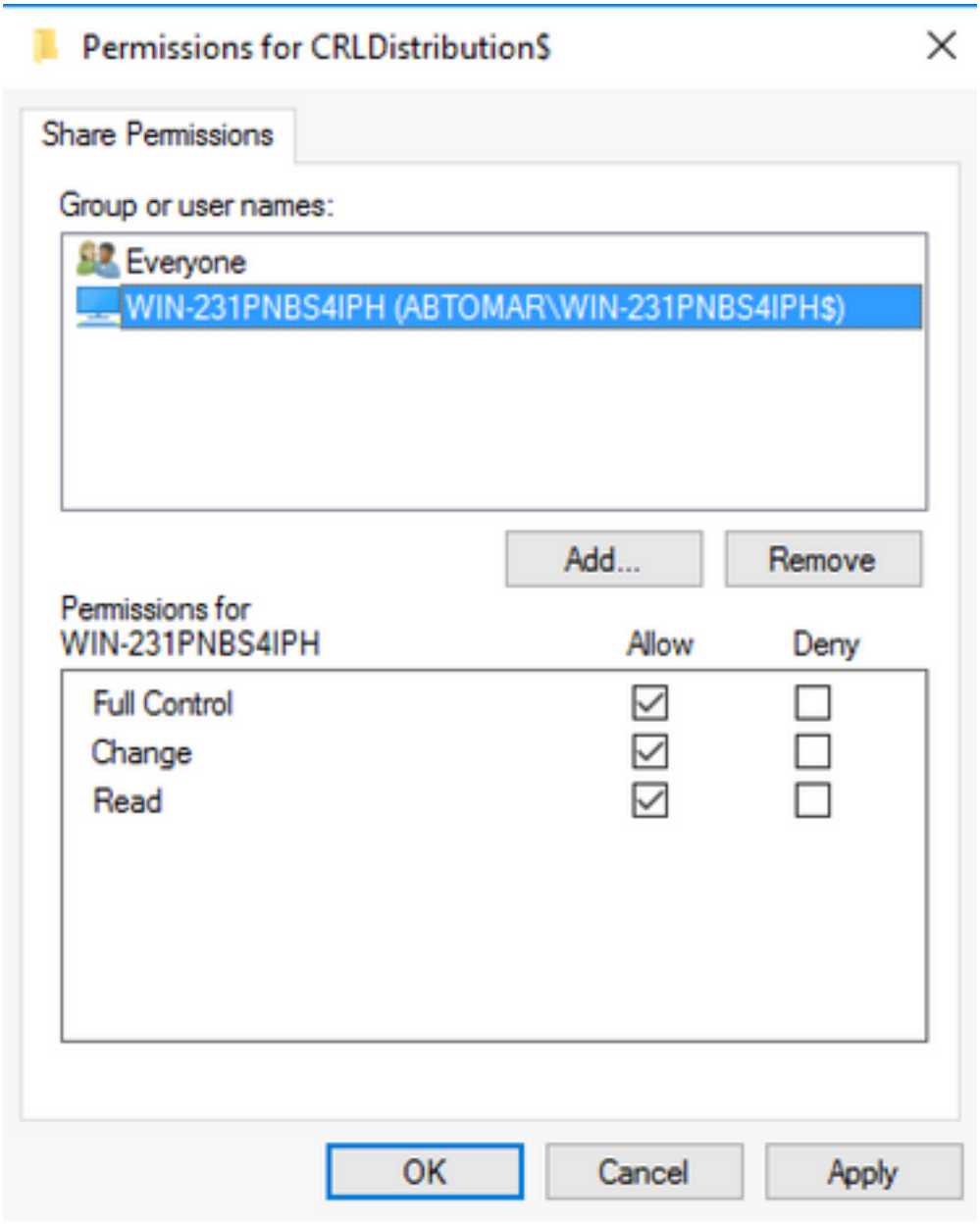


5. 要返回“选择用户、计算机、服务帐户或组”窗口，请单击**确定**。在“输入要选择的对象名称”字段中，在本示例中输入CA服务器的计算机名称：WIN0231PNBS4IPH，然后单击“**检查名称**”。如果输入的名称有效，则名称将刷新并显示下划线。Click **OK**.

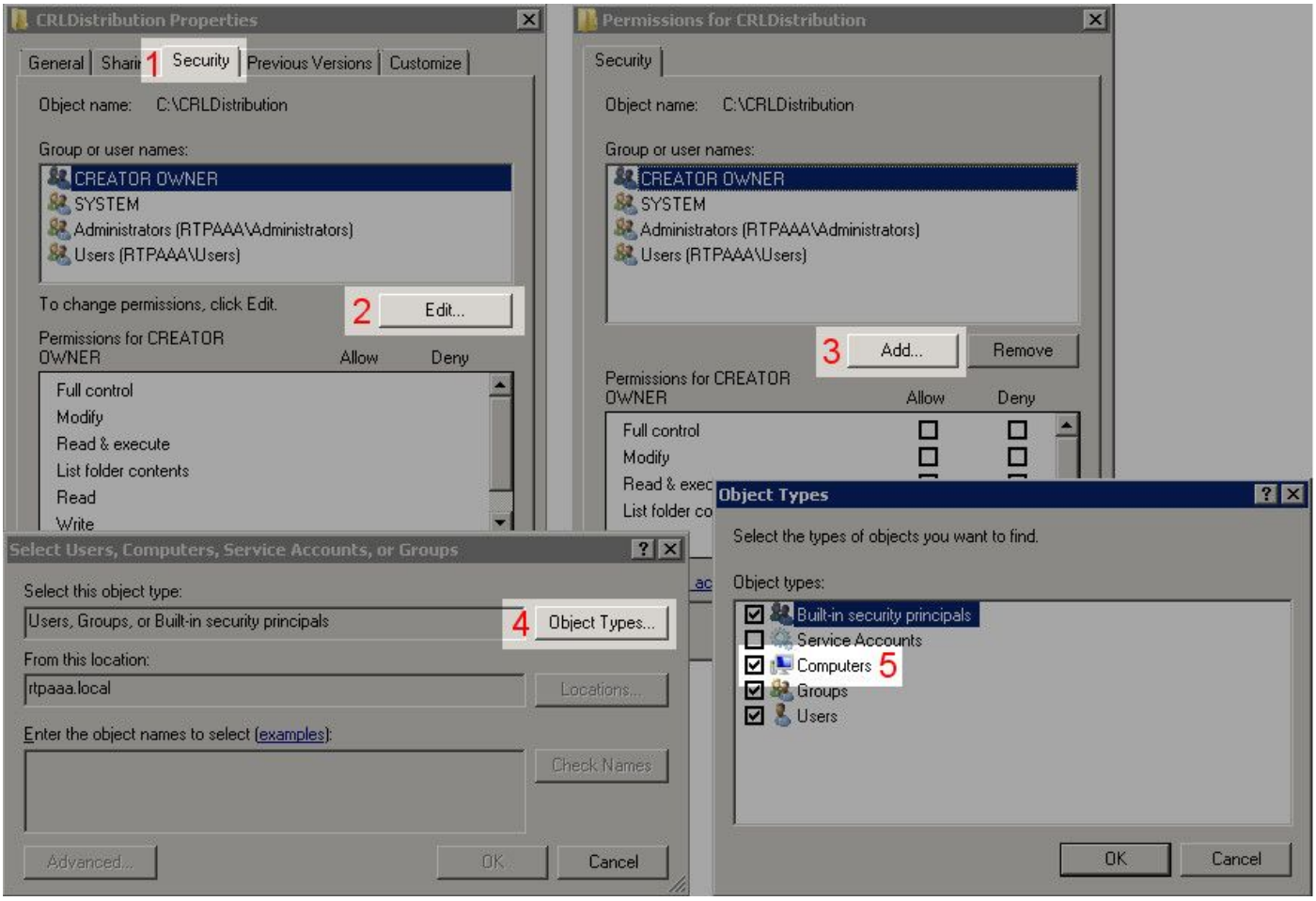


6. 在组或用户名字段中，选择CA计算机。选中**Allow** for Full Control可授予对CA的完全访问权限。

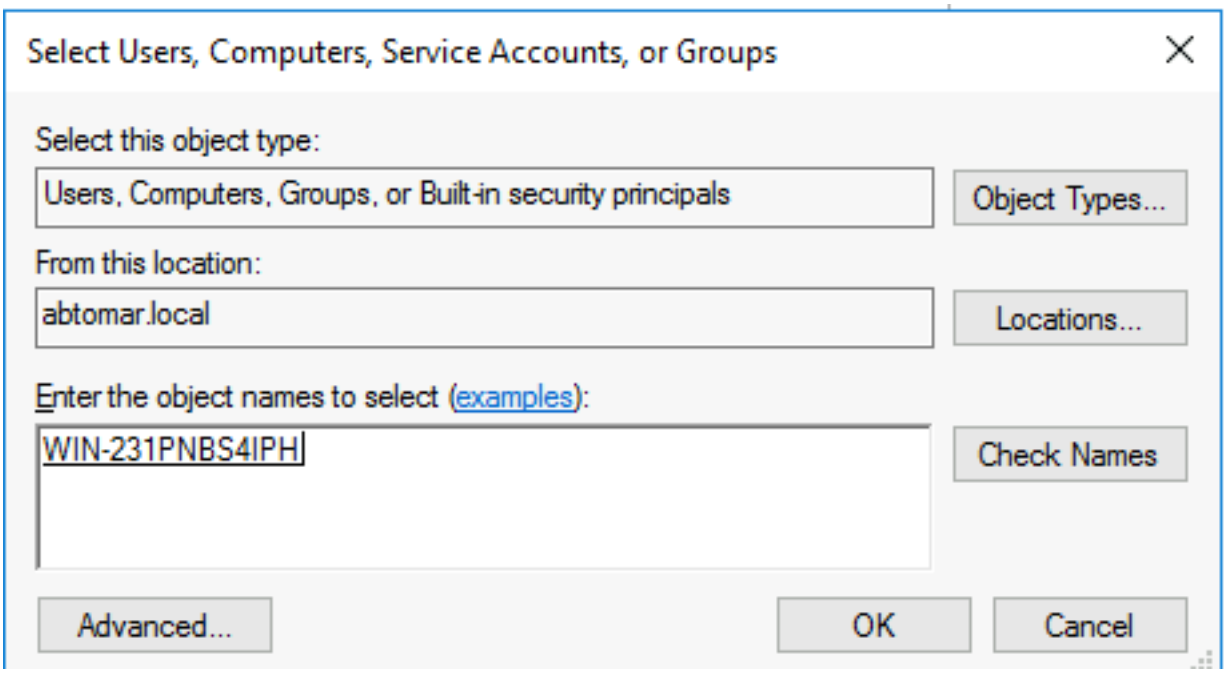
Click **OK**.再次单**击确**定以关闭“高级共享”窗口并返回“属性”窗口。



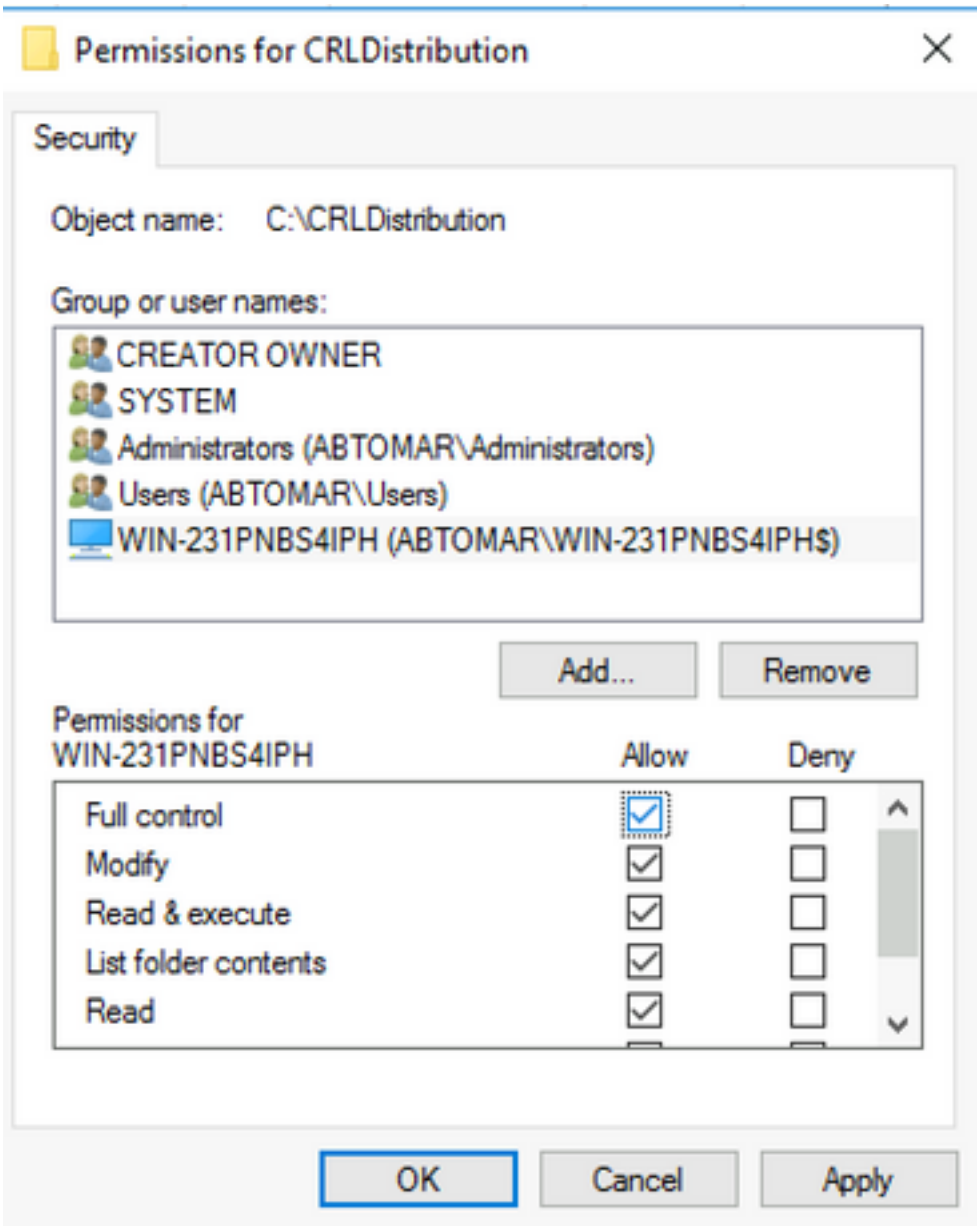
7.要允许CA将CRL文件写入新文件夹，请配置适当的安全权限。单击“Security(安全)”选项卡(1)，单击“**Edit**(2)”，单击“Add(3)”，单击“Object Types(4)”，然后选中“**Computers**(5))”复选框。



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，然后单击“检查**名称”**。如果输入的名称有效，则名称将刷新并显示下划线。Click **OK**.



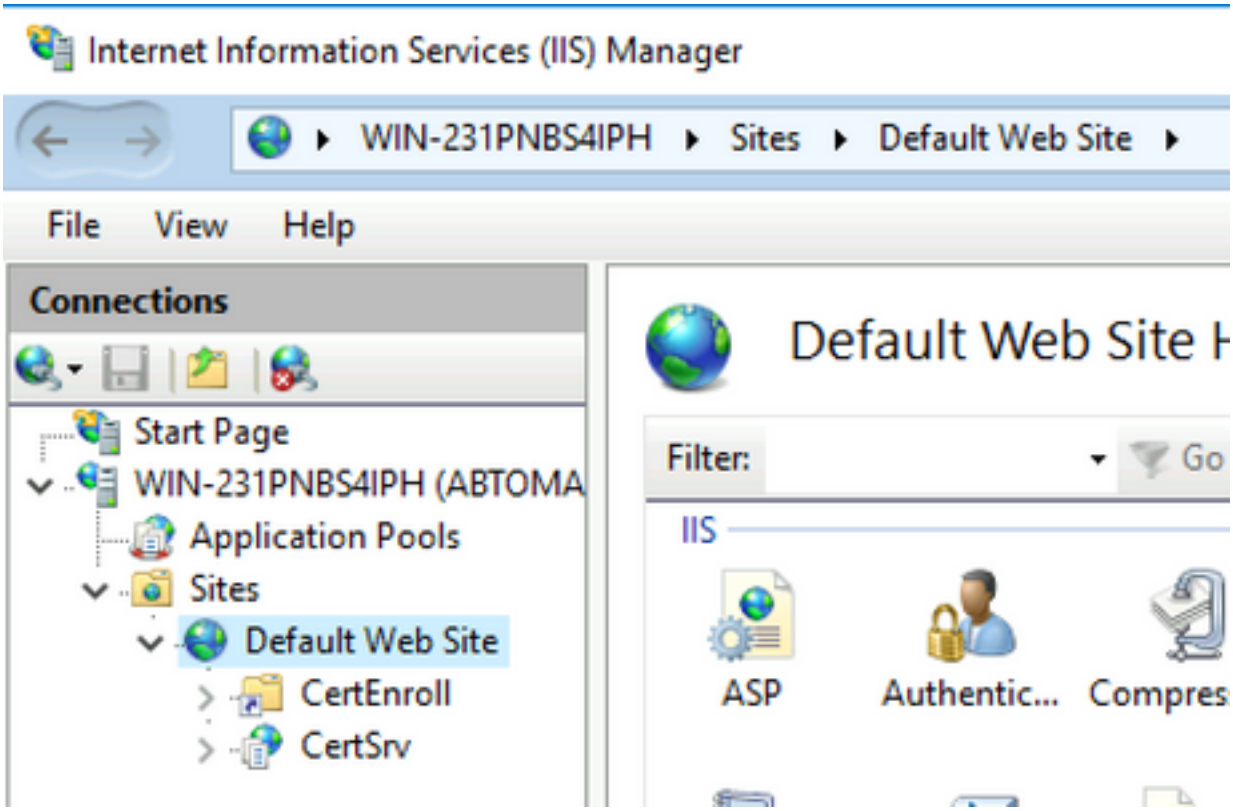
9.在“组”或“用户名”字段中选择CA计算机，然后选中“允许完全控制”以授予对CA的完全访问权限。单击**OK(确**定)，然**后单**击Close（关闭）完成任务。



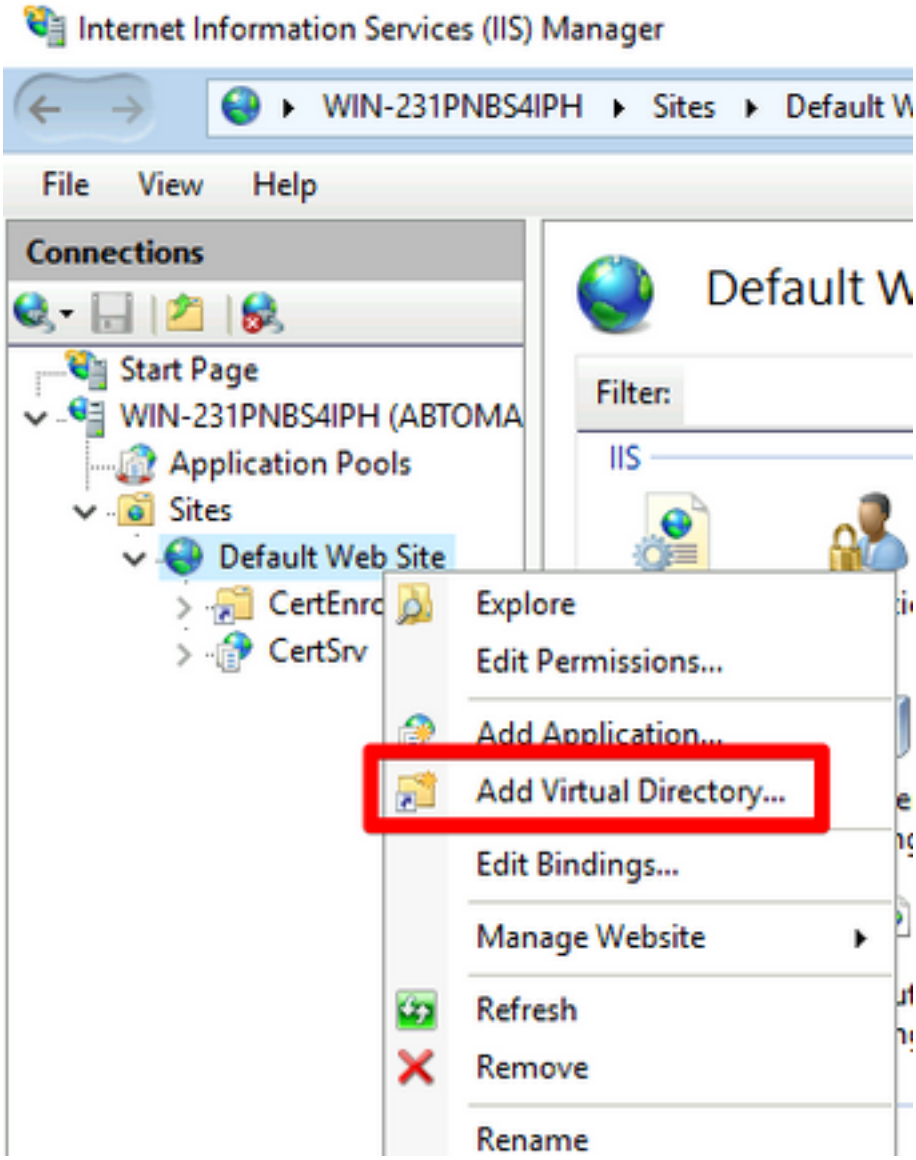
在IIS中创建站点以公开新的CRL分发点

要使ISE访问CRL文件，请使包含CRL文件的目录可通过IIS访问。

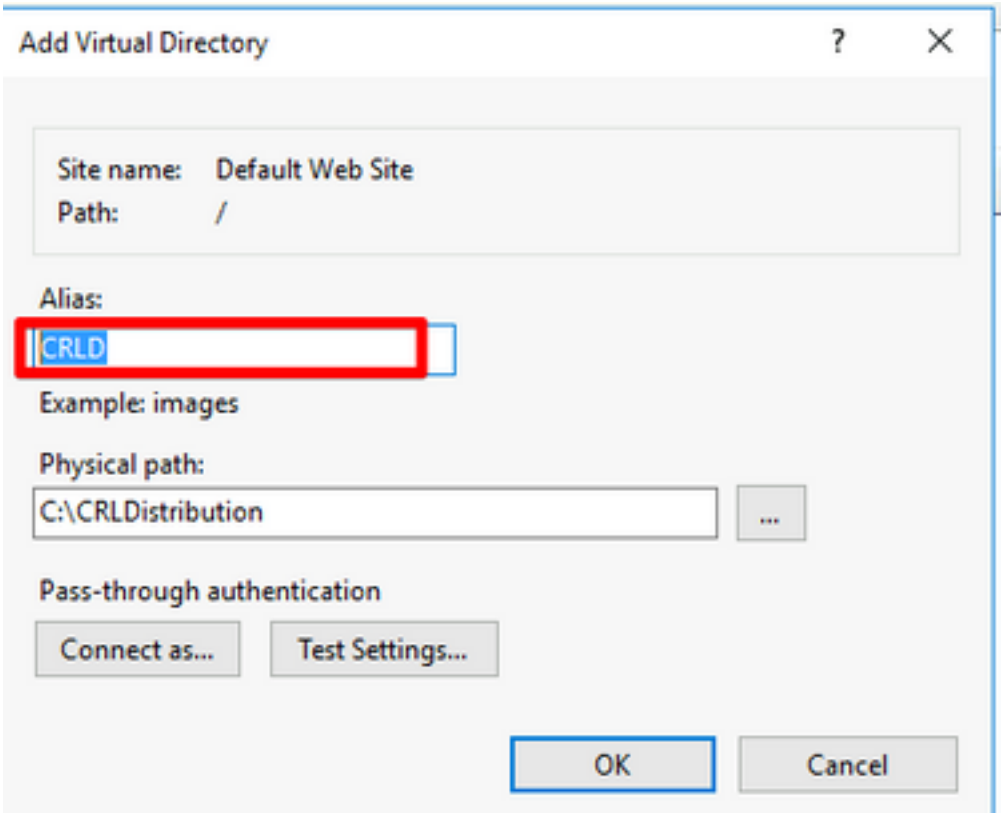
1. 在IIS服务器任务栏上，单击“**开始**”。选择**管理工具> Internet Information Services(IIS)管理器**。
2. 在左窗格中（称为控制台树），展开IIS服务器名称，然后展开“站**点**”。



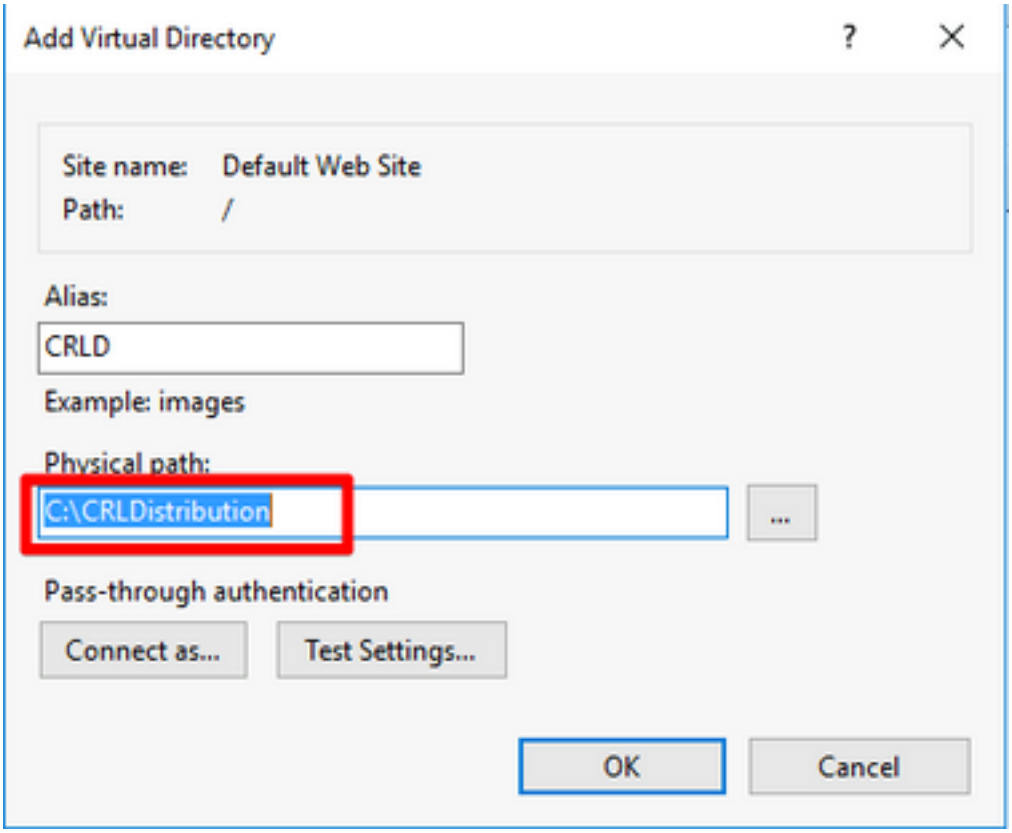
3.右键单击“**默认网站”**，然后选择**“添加虚**拟目录”，如下图所示。



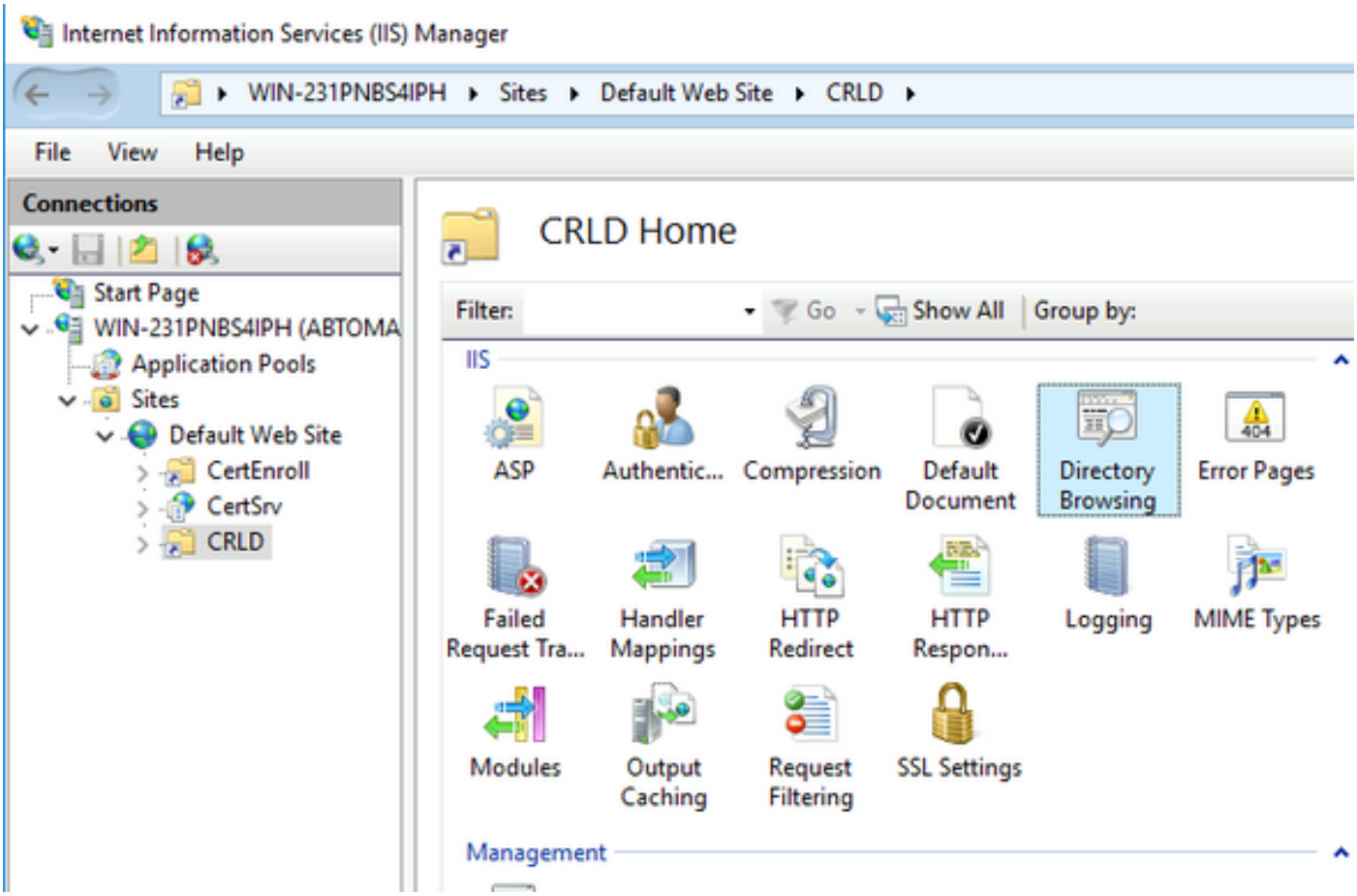
4.在“别名”字段中，输入CRL分发点的站点名称。在本例中，输入CRLD。



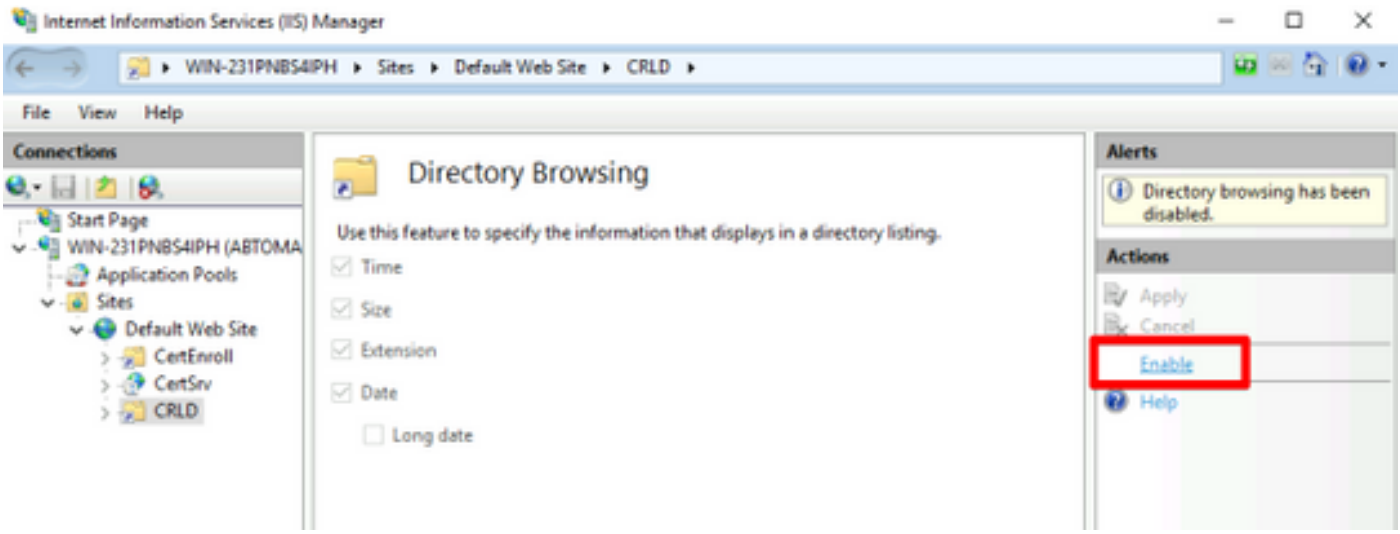
5.单击省略号(.。.)位于“物理路径”字段右侧，并浏览到在第1节中创建的文件夹。选择该文件夹，然后单击“**确定”**。单击**OK**关闭“Add Virtual Directory”窗口。



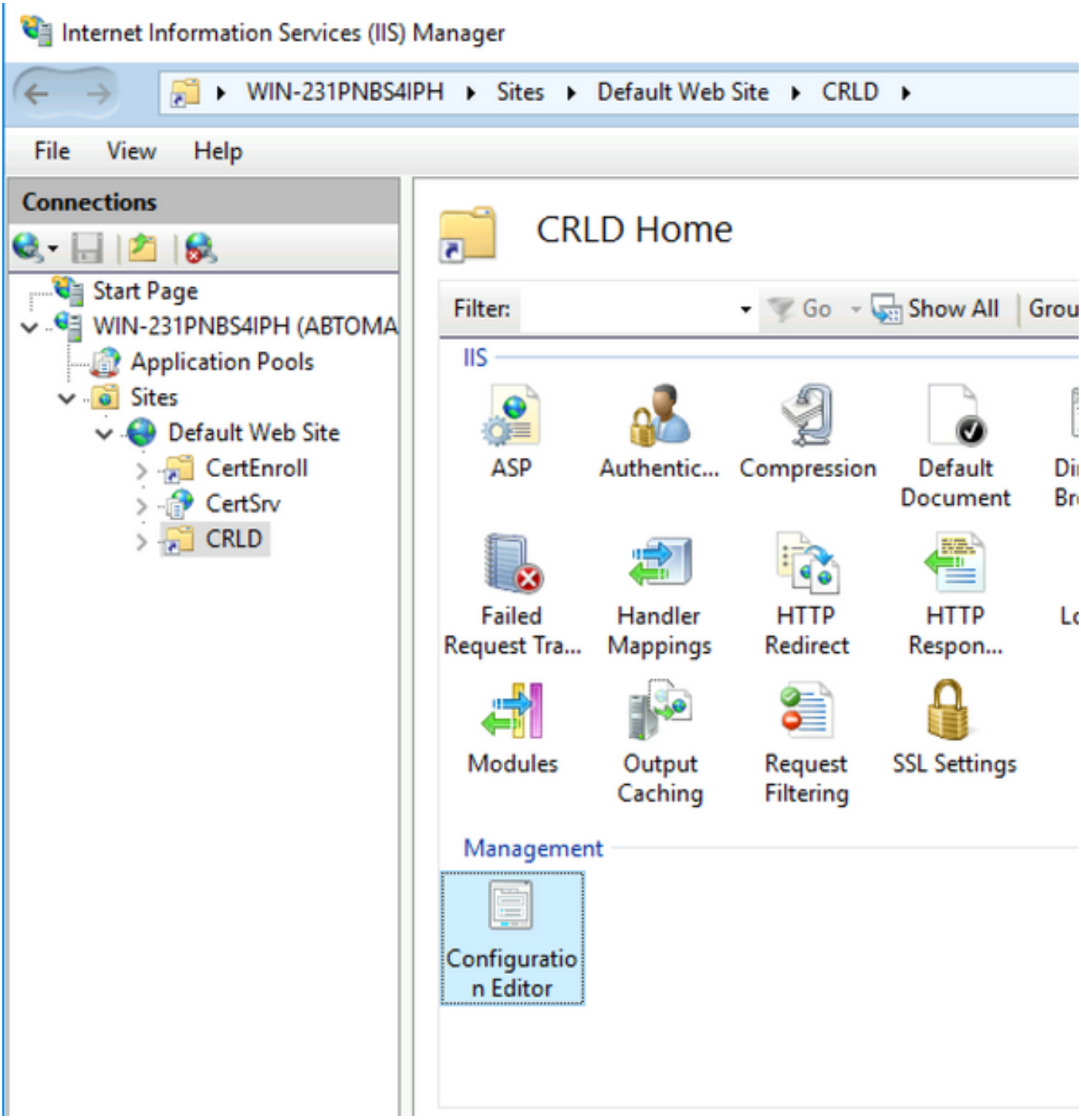
6.在步骤4中输入的站点名称必须在左窗格中突出显示。否则，请立即选择。在中心窗格中，双击“目录**浏览”**。



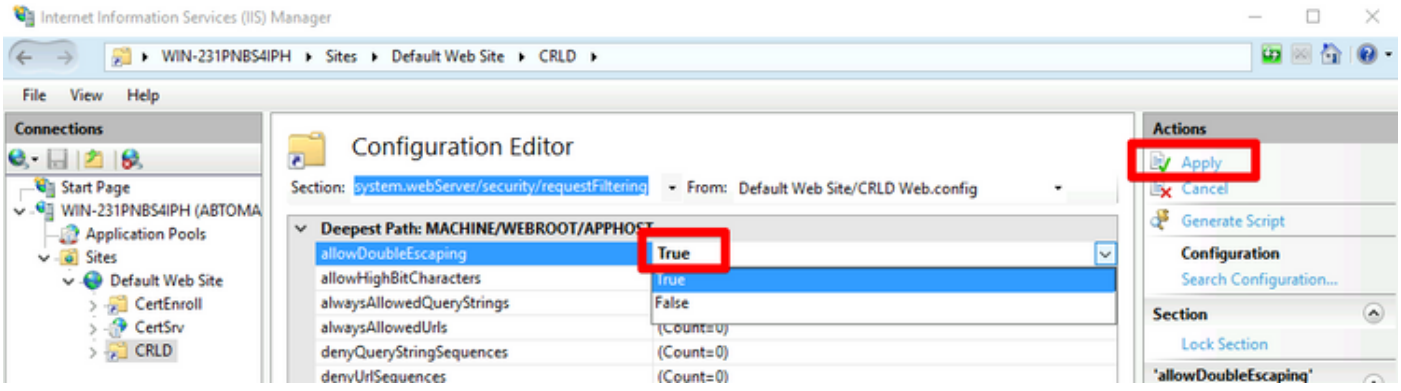
7.在右窗格中，单击“**启用**”以启用目录浏览。



8.在左窗格中，再次选择站点名称。在中间窗格中，双击“配置编**辑器**”。



9.在“部分”下拉列表中，选择**system.webServer/security/requestFiltering**。在**allowDoubleEscenig**下拉列**表中，选择True**。在右窗格中，单击**Apply**，如此图所示。

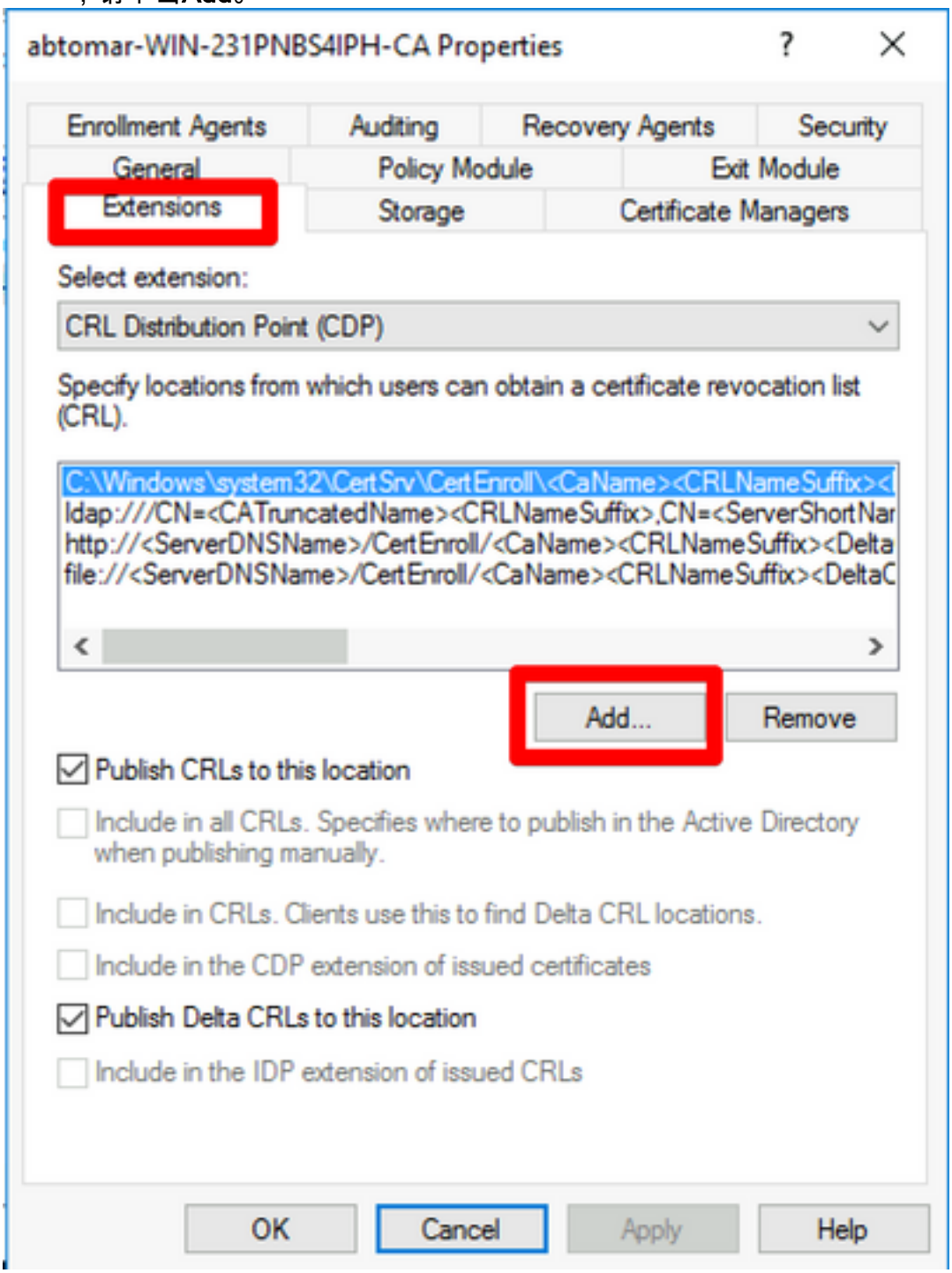


现在必须可通过IIS访问该文件夹。

配置Microsoft CA服务器以将CRL文件发布到分发点

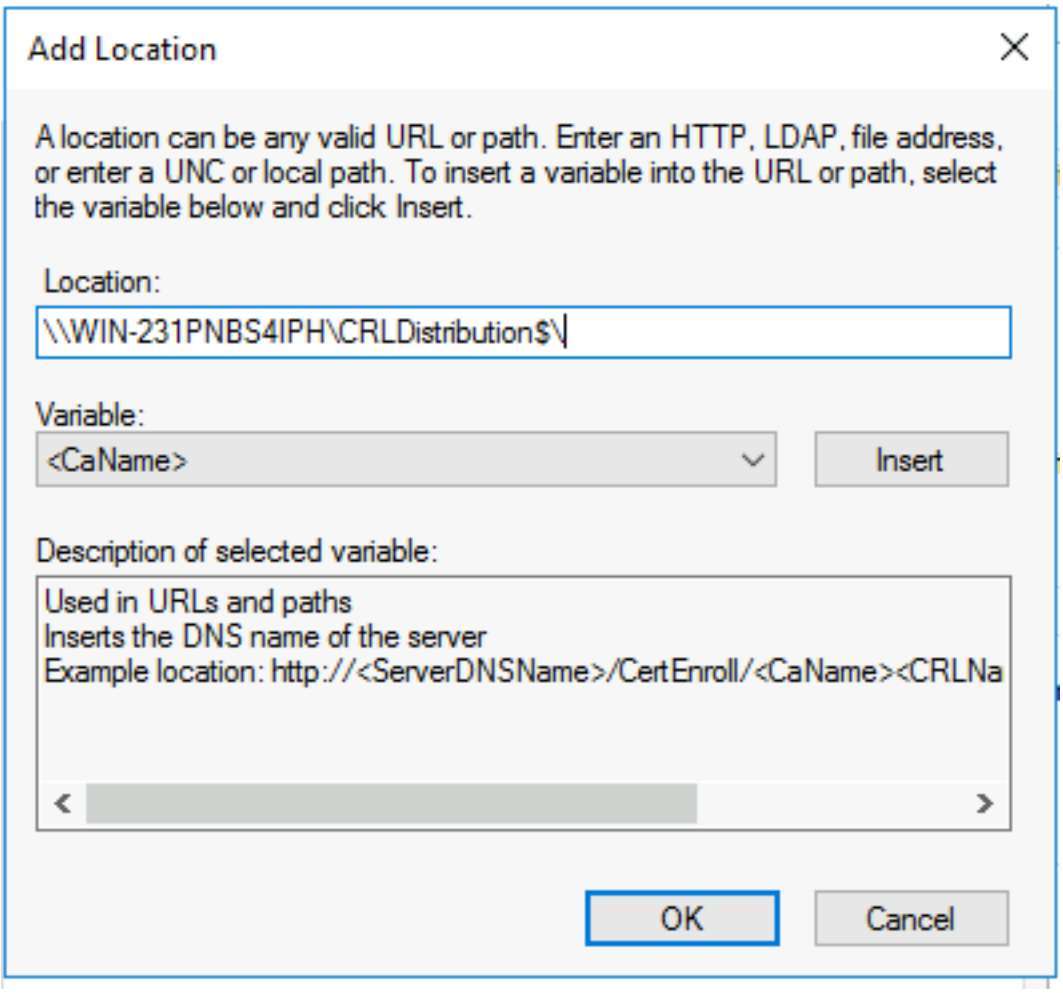
现在，已将新文件夹配置为容纳CRL文件，且该文件夹已在IIS中公开，请配置Microsoft CA服务器以将CRL文件发布到新位置。

1. 在CA服务器任务栏上，单击**Start**。选择**Administrative Tools > Certificate Authority**。
2. 在左窗格中，右键点击CA名称。选择“**属性**”，然后单击“**扩展**”选项卡。要添加新的CRL分发点，请单击**Add**。

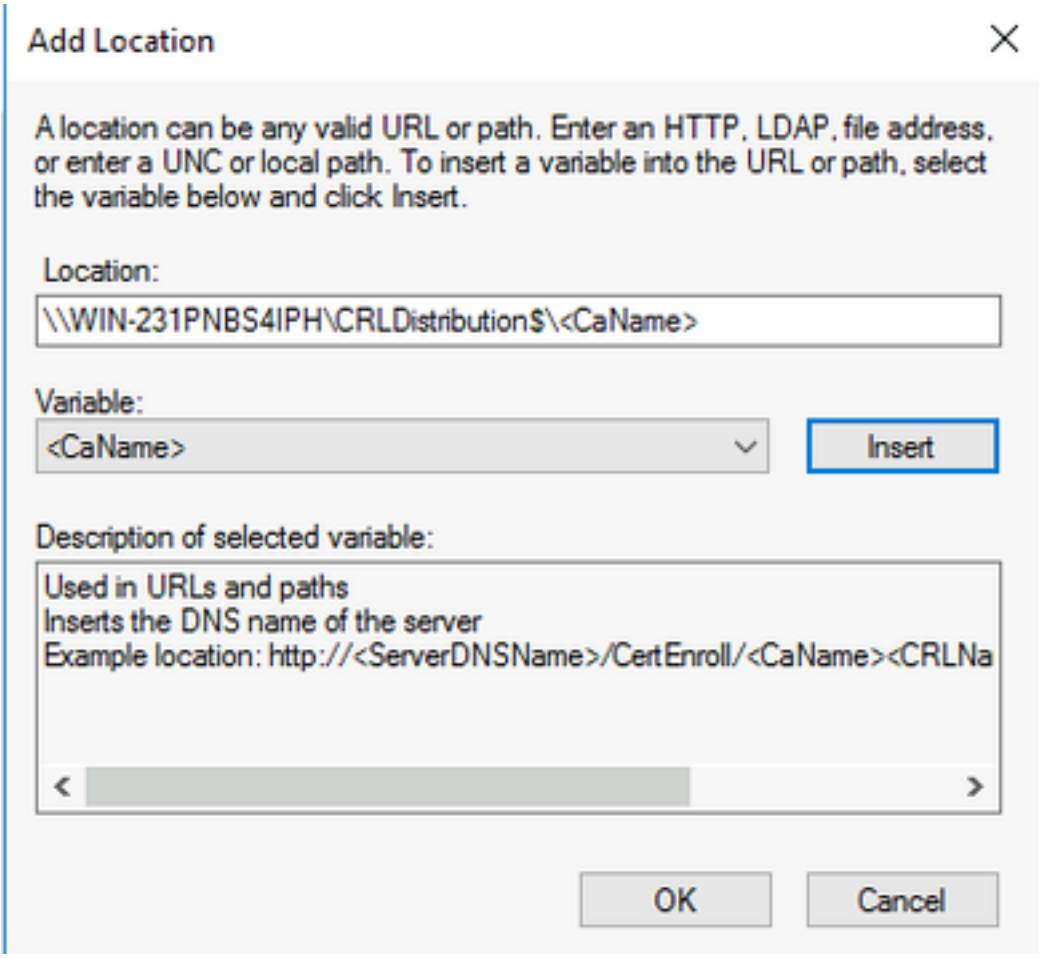


3.在“位置”字段中，输入在第1节中创建和共享的文件夹的路径。在第1节的示例中，路径为：

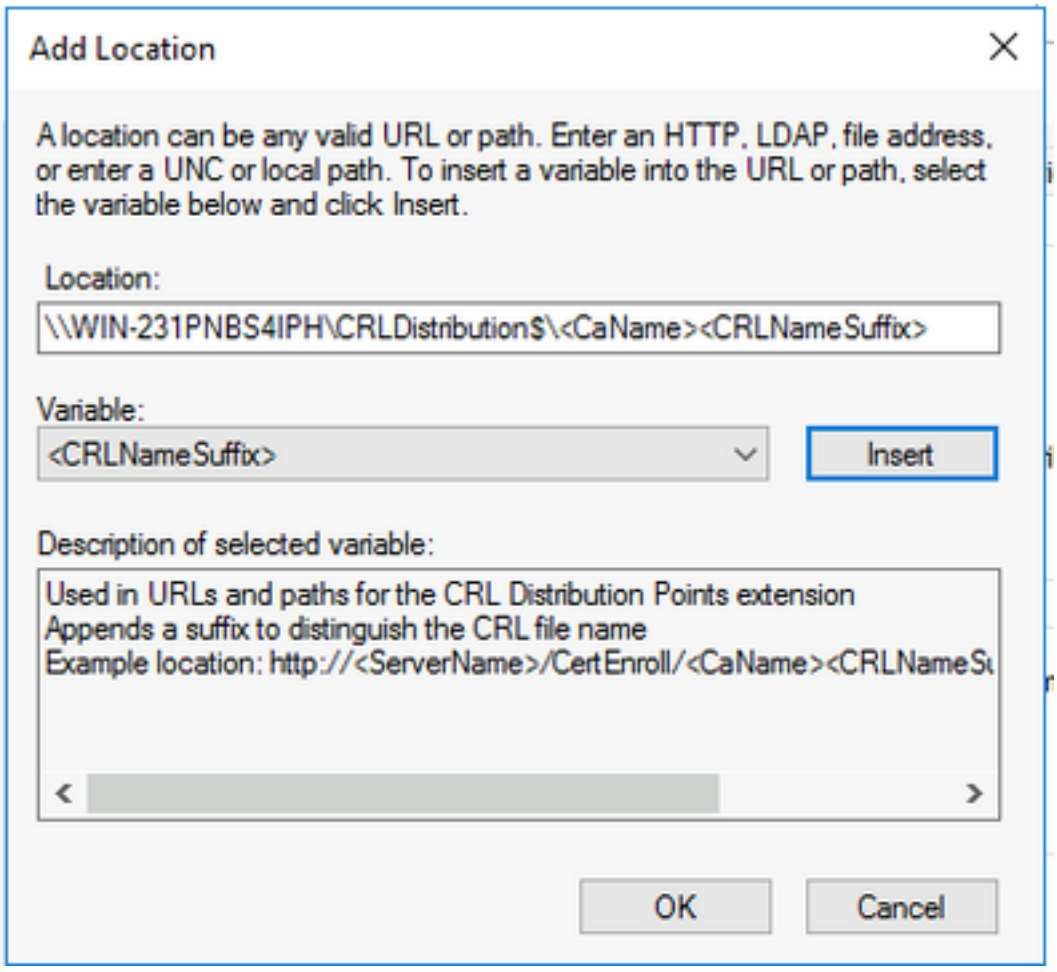
\\WIN-231PNBS4IPH\CRLDistribution$



4.填写“位置”字段后，从“变量”下拉列表中选择<CaName>，然后单击“插入”。

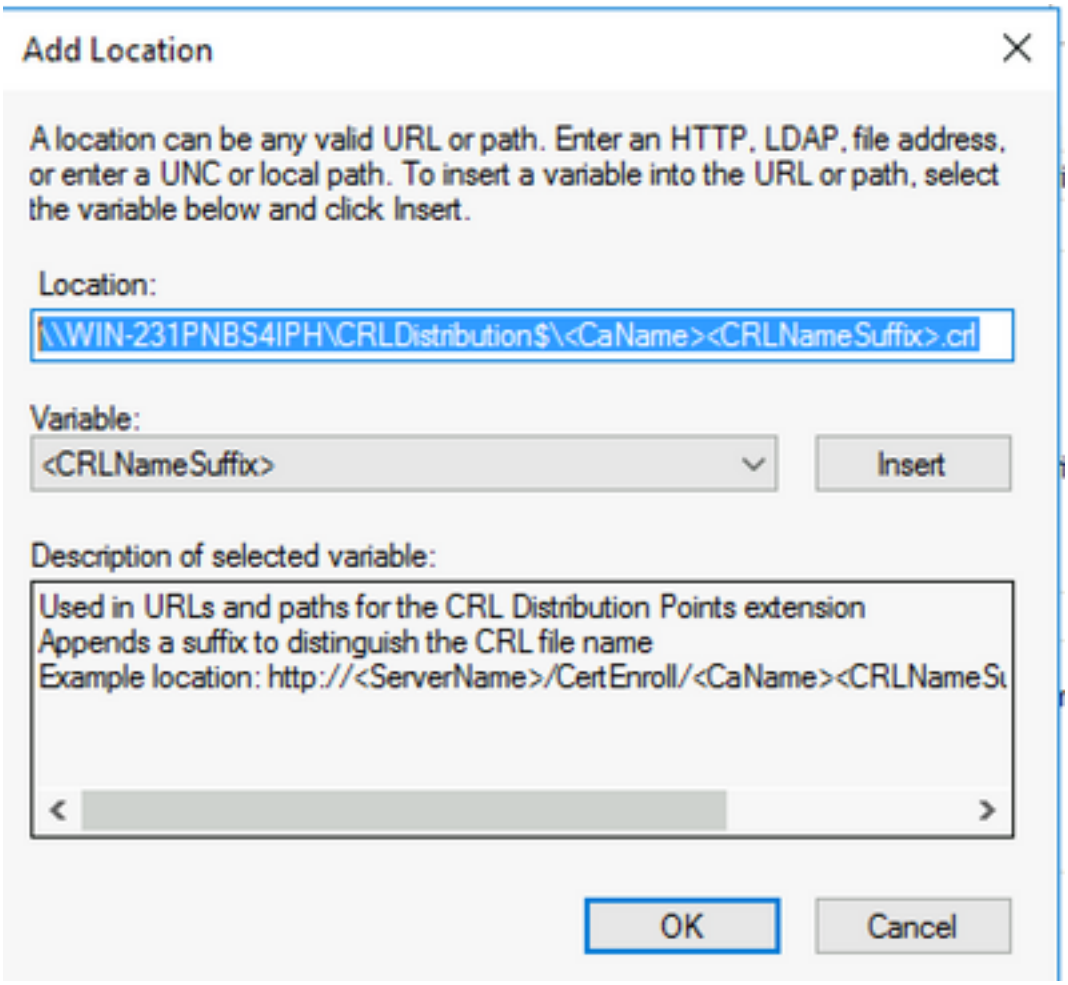


5.从“变量”下拉列表中，选择**<CRLNameSuffix>，然**后单击“插入”。



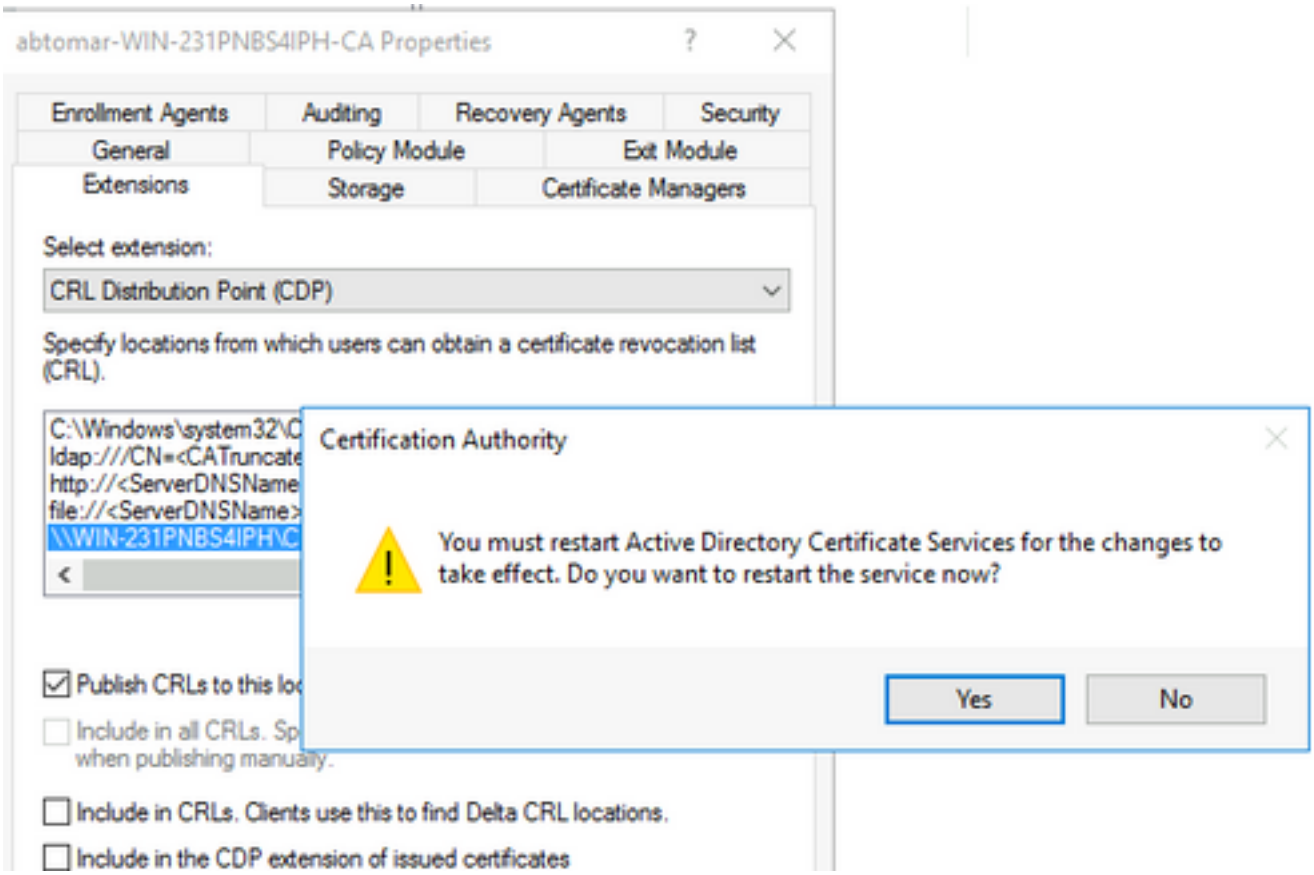
6.在“位置”字段中，**将。**crl附加到路径的末尾。在本例中，位置为：

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

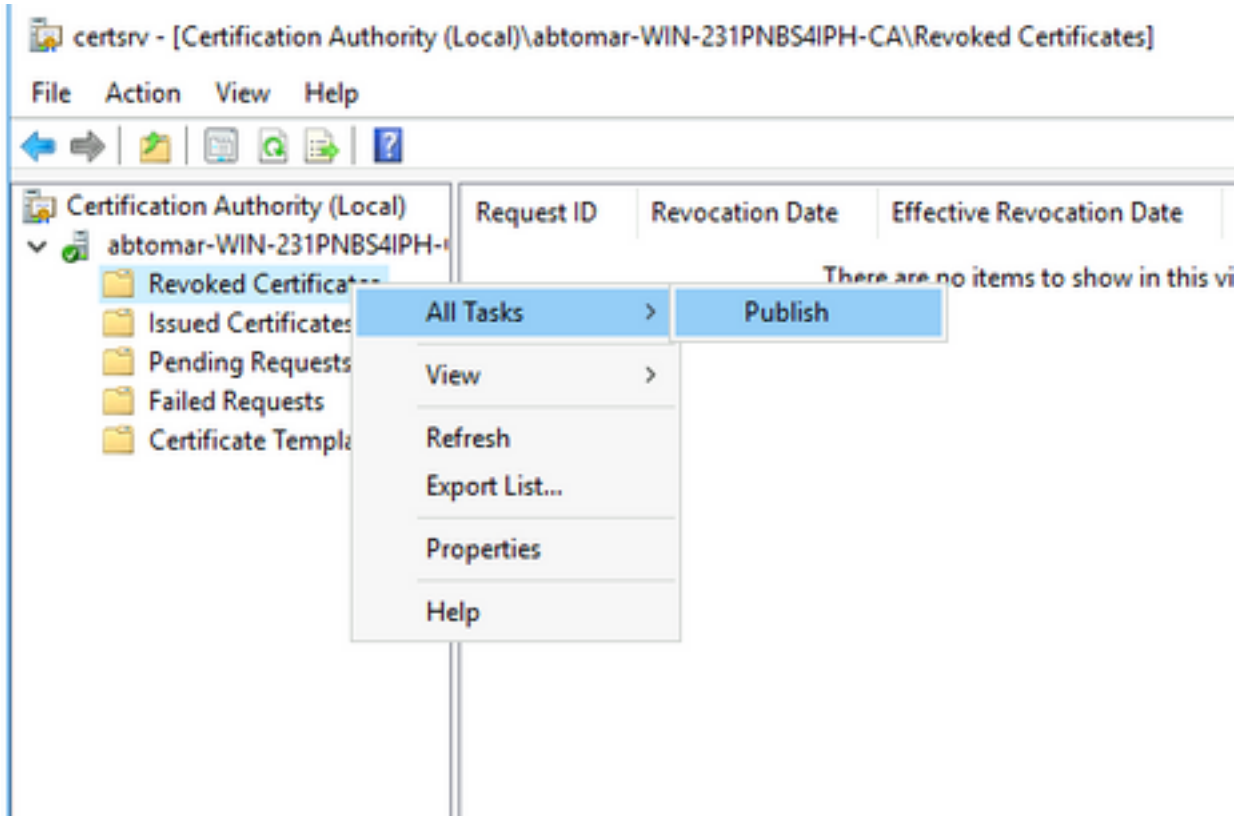


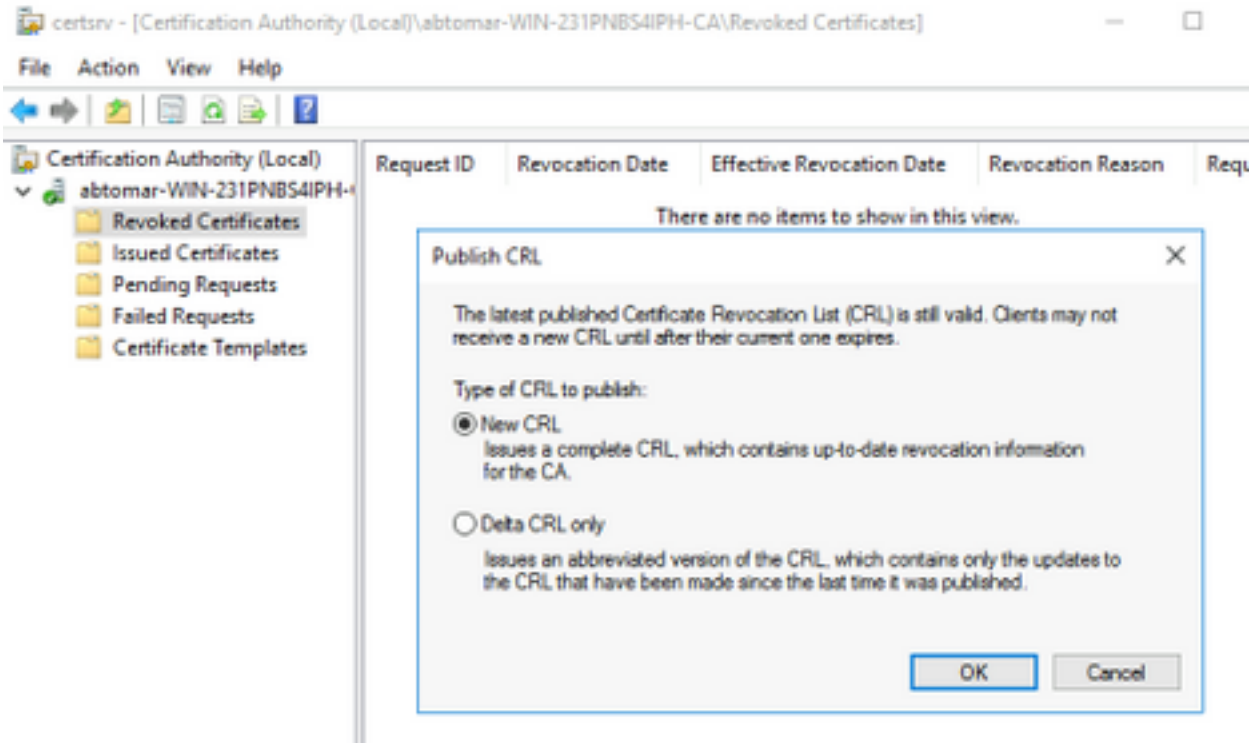
7. 单击**OK**返回“Extensions”选项卡。选中“**将CRL发布到此位置**”复选框，然后单**击“**确定”关闭“属性”窗口。

系统将显示提示，要求您允许重新启动Active Directory证书服务。单击 **Yes**。



8.在左窗格中，右键单击“已撤销的证书”。选择**所有任务>发布**。确保已选中New CRL，然后单击**OK**。



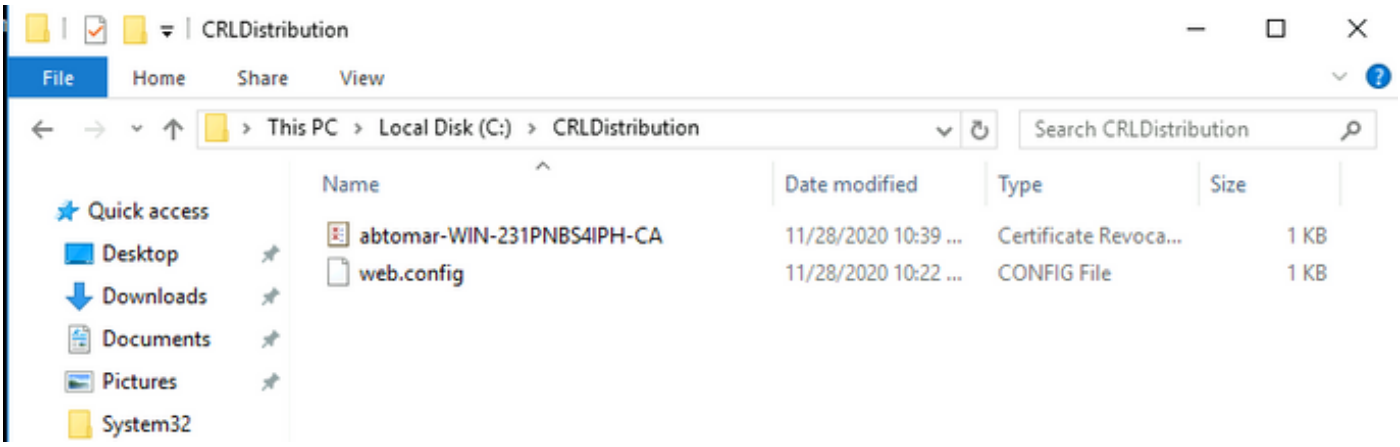


Microsoft CA服务器必须在第1节中创建的文件夹中创建新的.crl文件。如果新的CRL文件创建成功，单击“确定”后将不会出现对话框。如果返回有关新分发点文件夹的错误，请仔细重复本节中的每个步骤。

验证CRL文件是否存在并可通过IIS访问

在开始本节之前，请验证新CRL文件是否存在，以及它们是否可通过IIS从其他工作站访问。

1. 在IIS服务器上，打开在第1节中创建的文件夹。必须有一个.crl文件，其形式为 **<CANAME>.crl**，其中<CANAME>是CA服务器的名称。在本例中，文件名为：
abtomar-WIN-231PNBS4IPH-CA.crl



2.从网络上的工作站（最好与ISE主要管理节点位于同一网络），打开Web浏览器并浏览到http://<SERVER>/<CRLSITE>，其中<SERVER>是第2部分配置的IIS服务器的服务器名称，<CRLSITE>是第2部分中为分发点选择的站点名称。在本例中，URL为：

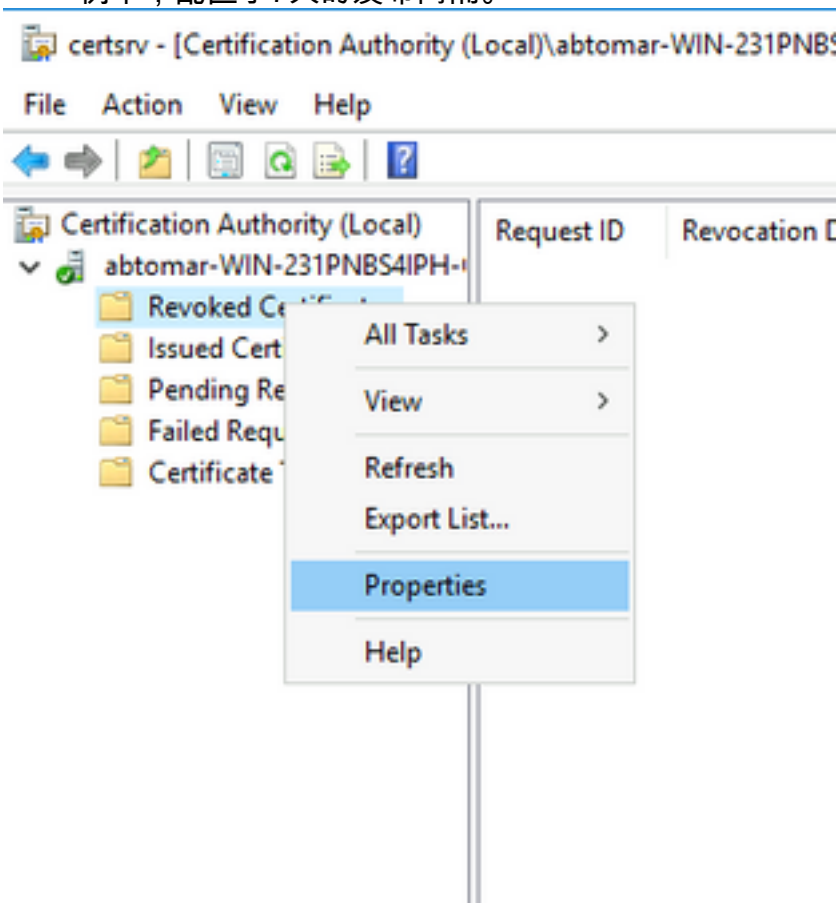
http://win-231pnbs4iph/CRLD

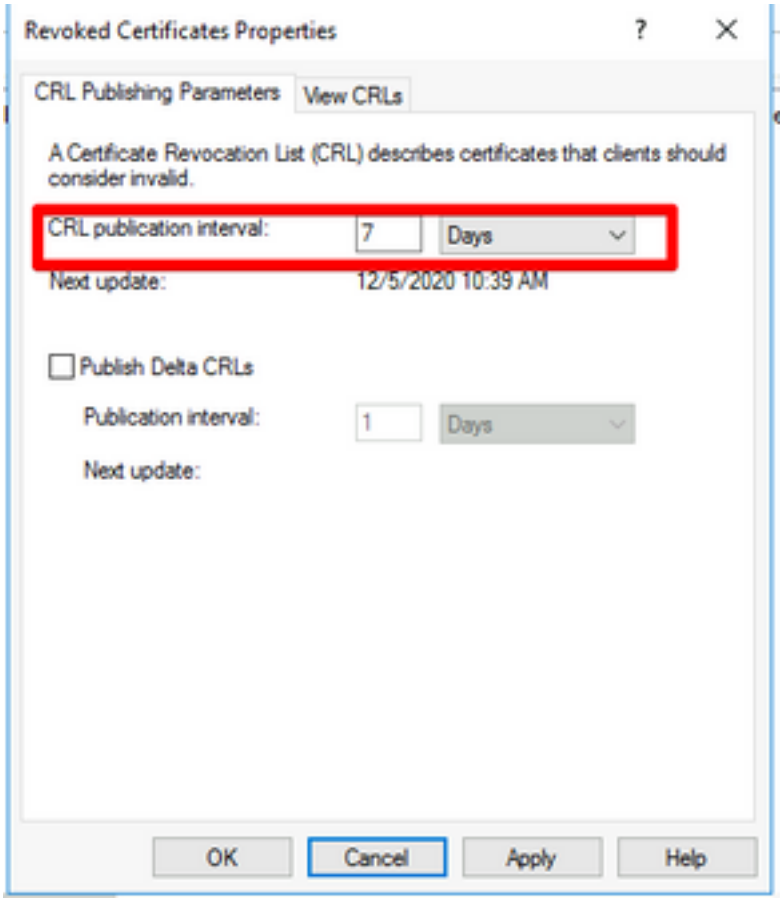
系统随即会显示目录索引，其中包括步骤1中观察到的文件。

配置ISE以使用新CRL分发点

在将ISE配置为检索CRL之前，定义发布CRL的间隔。确定此间隔的策略不在本文档的范围内。潜在值（在Microsoft CA中）为1小时到411年（包括1小时）。默认值为1周。确定环境的适当间隔后，使用以下说明设置间隔：

1. 在CA服务器任务栏上，单击**Start**。选择**Administrative Tools > Certificate Authority**。
2. 在左窗格中，展开CA。右键单击“已撤销**的证书”**文件夹，然后选择**“属性”。**
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，配置了7天的发布间隔。





4.输入certutil -getreg **CA\Clock*命令**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certutil -getreg CA**\CRLov*命令**，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。如果值是0以外的值，请记录值和单位。

示例输出：

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

6. 输入**certutil -getreg CA\CRLpe*命**令以验证步骤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.计算CRL宽限期，如下所示：

a.如果在步骤5中设置了CRLOverlapPeriod:OVERLAP = CRLOverlapPeriod，以分钟为单位；

否则：重叠=(CRLPeriod / 10)，分钟

b.如果OVERLAP > 720，则OVERLAP = 720

c.如果OVERLAP <(1.5 * ClockSkewMinutes)，则OVERLAP =(1.5 * ClockSkewMinutes)

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

e.宽限期= OVERLAP + ClockSkewMinutes

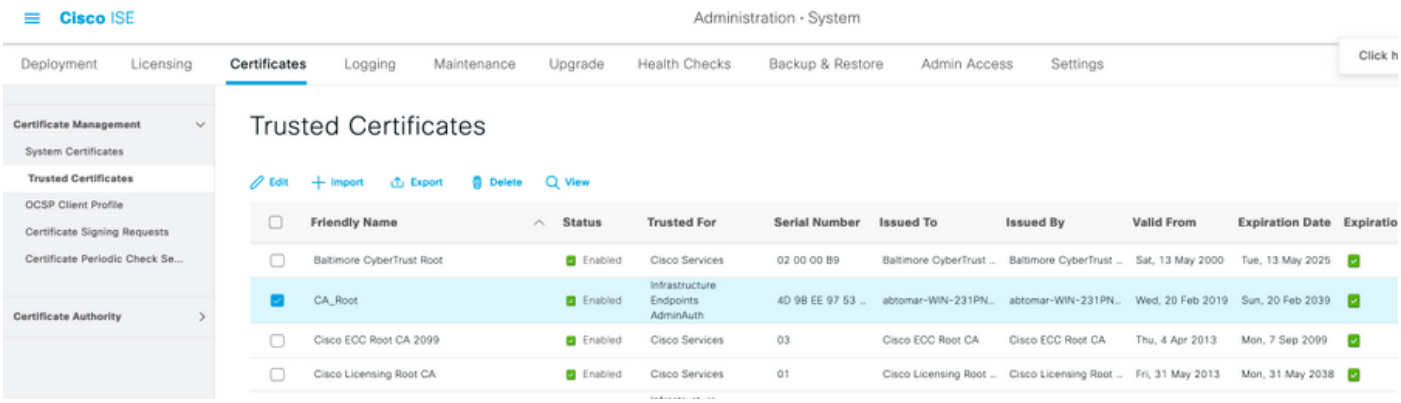
```
Example:

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
```

计算的宽限期是CA发布下一个CRL和当前CRL到期之间的时间量。ISE需要配置为相应地检索CRL。

8.登录到ISE主要管理节点，然后选择Administration > System > Certificates。在左窗格中，选择**受信任证书**



9.选中要为其配置CRL的CA证书旁的复选框。单击 **Edit**。

10.在窗口底部附近，选中Download CRL**复选**框。

11.在CRL Distribution URL字段中，输入CRL分发点的路径，该路径包括在第2节中创建的.crl文件。在本例中，URL为：

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

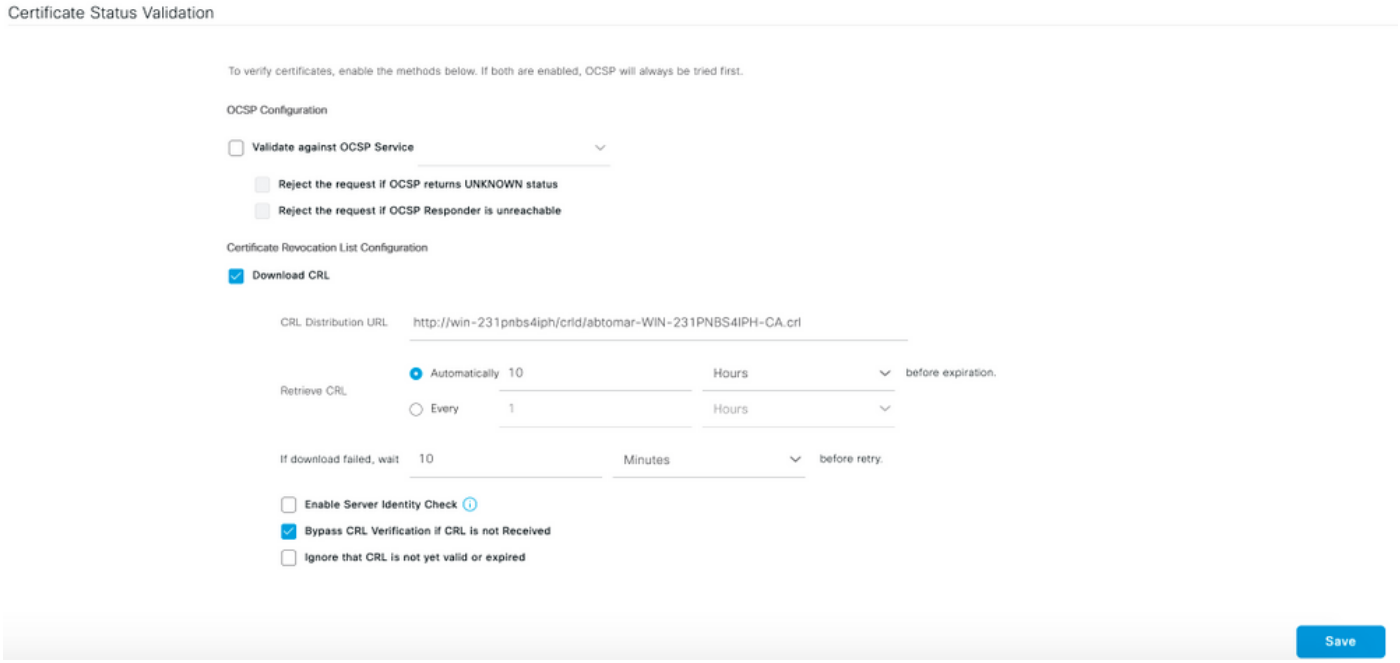
12. ISE可以配置为定期或基于到期（通常也是定期间隔）检索CRL。 当CRL发布间隔为静态时，使用后一个选项时会获得更及时的CRL更新。单击“Automatically(自**动)**”单选按钮。

13.将检索值设置为小于步骤7中计算的宽限期的值。如果设置的值长于宽限期，ISE会在CA发布下一个CRL之前检查CRL分发点。在本例中，宽限期计算为730分钟，即12小时10分钟。值为10小时将用于检索

14.根据您的环境设置重试间隔。如果ISE无法在上一步中配置的间隔内检索CRL，它将以较短的间隔重试。

15.选中**Bypass CRL Verification if CRL is not Received**复选框，以允许在ISE无法检索此CA的CRL的上次下载尝试中，以正常（且不检索CRL检查）进行基于证书的身份验证。如果未选中此复选框，则如果无法检索CRL，则使用此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**Ignore that CRL is not valid or expired复选框**，以允许ISE使用过期（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，ISE会认为CRL在其有效日期之前和其下一次更新时间之后无效。单击**Save**以完成配置。



思科内部信息

1.微软。"配置证书的CRL分发点。" 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.微软。"手动发布证书撤销列表。" 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.微软。"配置CRL和增量CRL重叠期。" http://technet.microsoft.com/en-us/library/cc731104.aspx,2011年4月11日[2012年12月18日]

4. MS2065 [MSFT]。“如何计算EffectiveDate（此更新）、NextUpdate和NextCRLPublish。” 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]