Configurar Microsoft CA Server para publicar las listas de revocación de certificados para ISE

Contenido

Introducción

Este documento describe la configuración de un servidor de la Autoridad de certificados (CA) de Microsoft que ejecuta Servicios de Internet Information Server (IIS) para publicar las actualizaciones de la Lista de revocación de certificados (CRL). También se explica cómo configurar Cisco Identity Services Engine (ISE) (versiones 3.0 y posteriores) para recuperar las actualizaciones para su uso en la validación de certificados. ISE se puede configurar para recuperar CRL para los distintos certificados raíz de CA que utiliza en la validación de certificados.

Requisito previo

Requirements

No hay requisitos específicos para este documento.

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Cisco Identity Services Engine versión 3.0
- Microsoft Windows Server 2008 R2

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Configurar

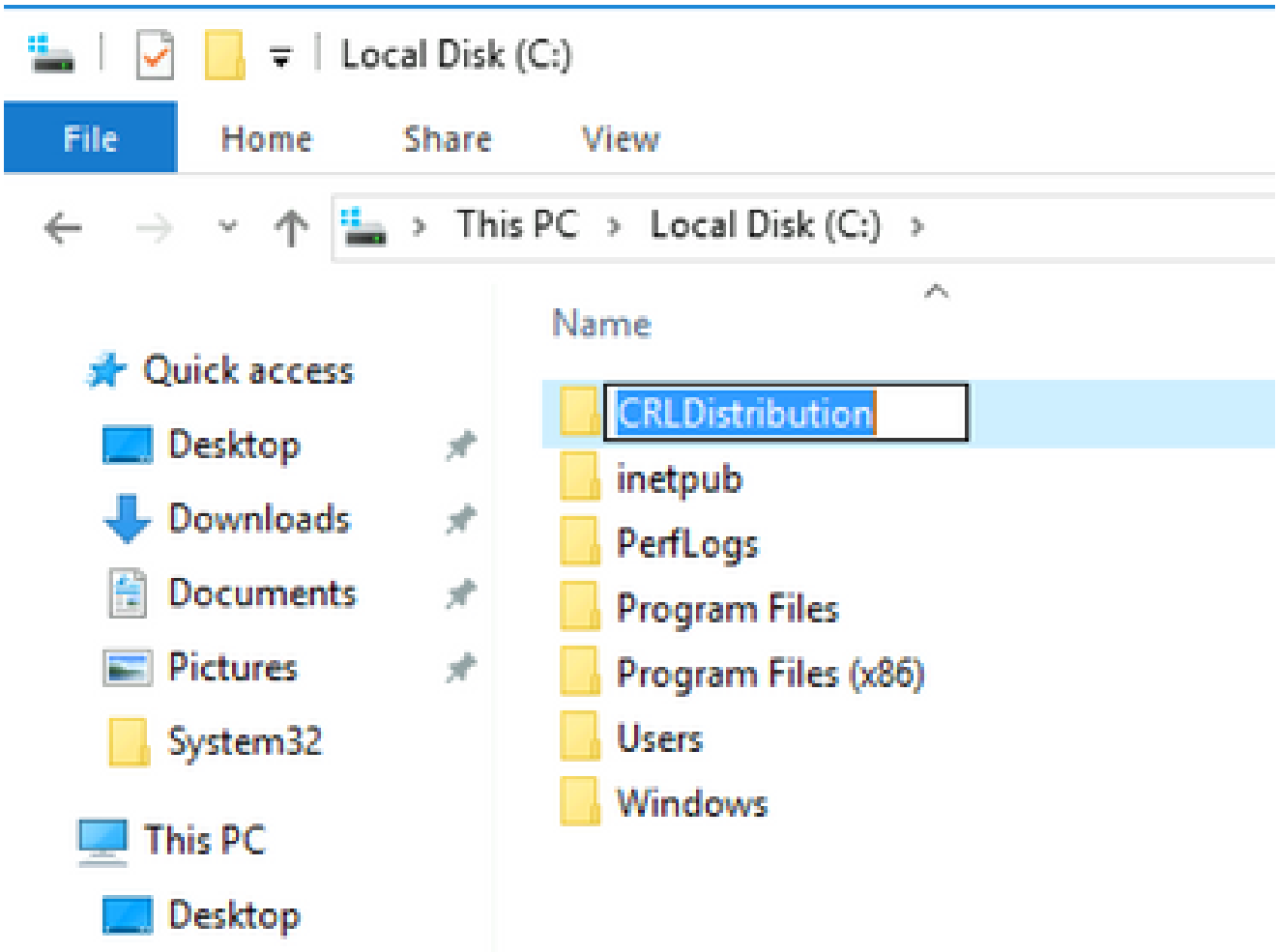
En esta sección encontrará la información para configurar las funciones descritas en este documento.

Crear y configurar una carpeta en la CA para alojar los archivos CRL

La primera tarea consiste en configurar una ubicación en el servidor de la CA para almacenar los archivos CRL. De forma predeterminada, el servidor de Microsoft CA publica los archivos en **C:\Windows\system32\CertSrv\CertEnroll**

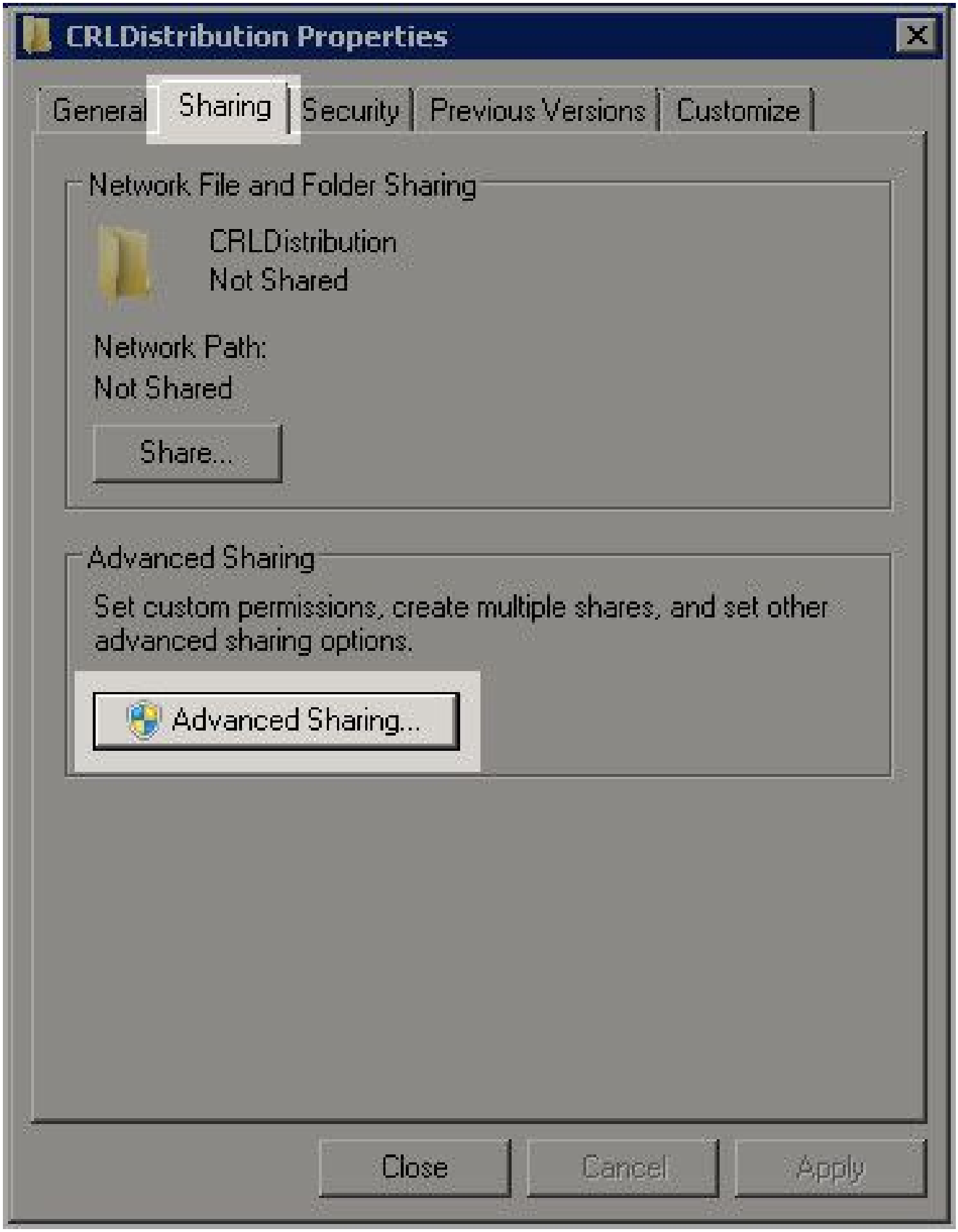
En lugar de utilizar esta carpeta del sistema, cree una nueva carpeta para los archivos.

1. En el servidor IIS, elija una ubicación en el sistema de archivos y cree una nueva carpeta. En este ejemplo, se **C:\CRLDistribution** crea la carpeta.

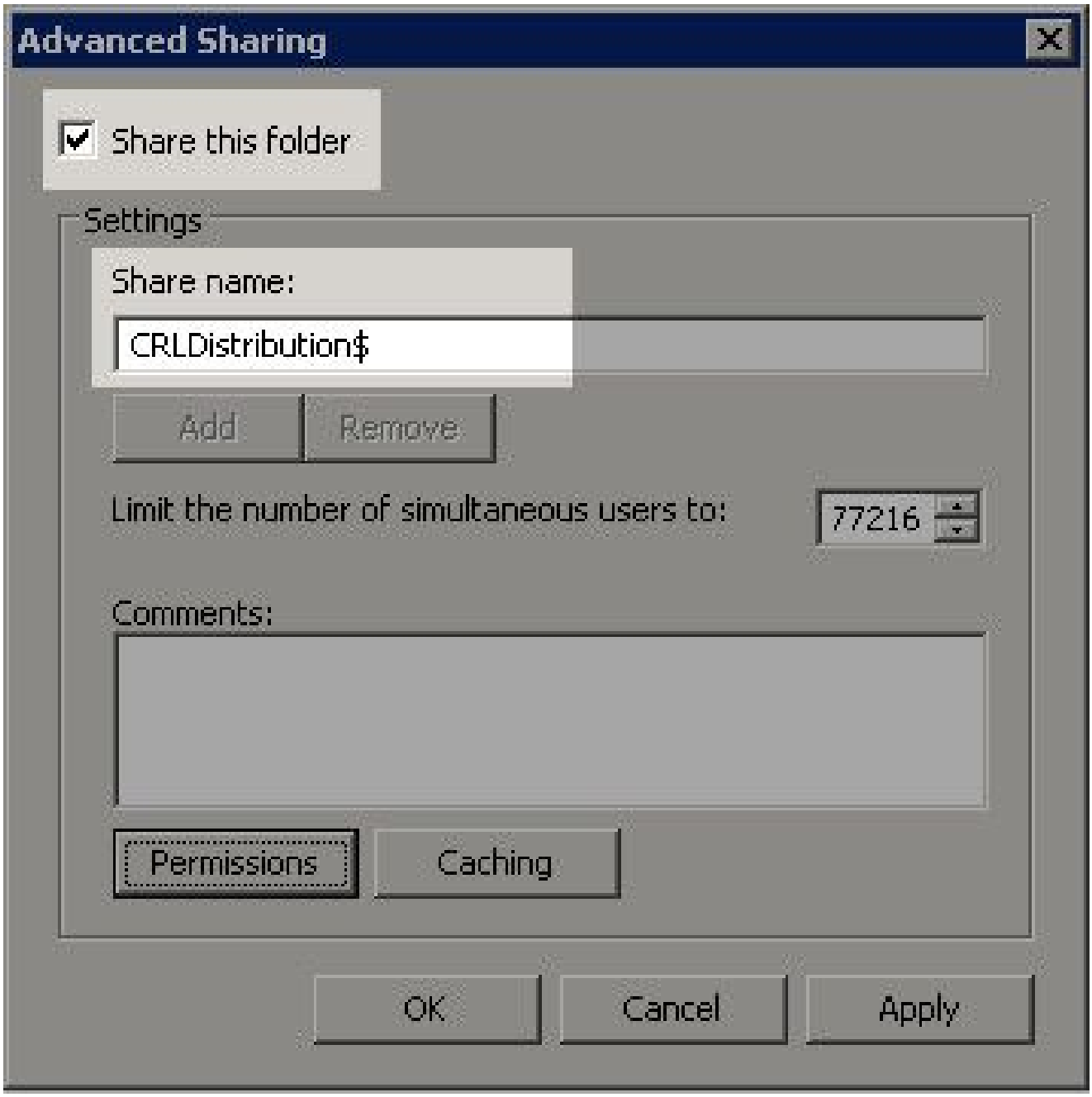


2. Para que la CA escriba los archivos CRL en la nueva carpeta, debe estar habilitado el uso compartido. Haga clic con el botón secundario en la nueva carpeta, elija **Properties**, haga clic

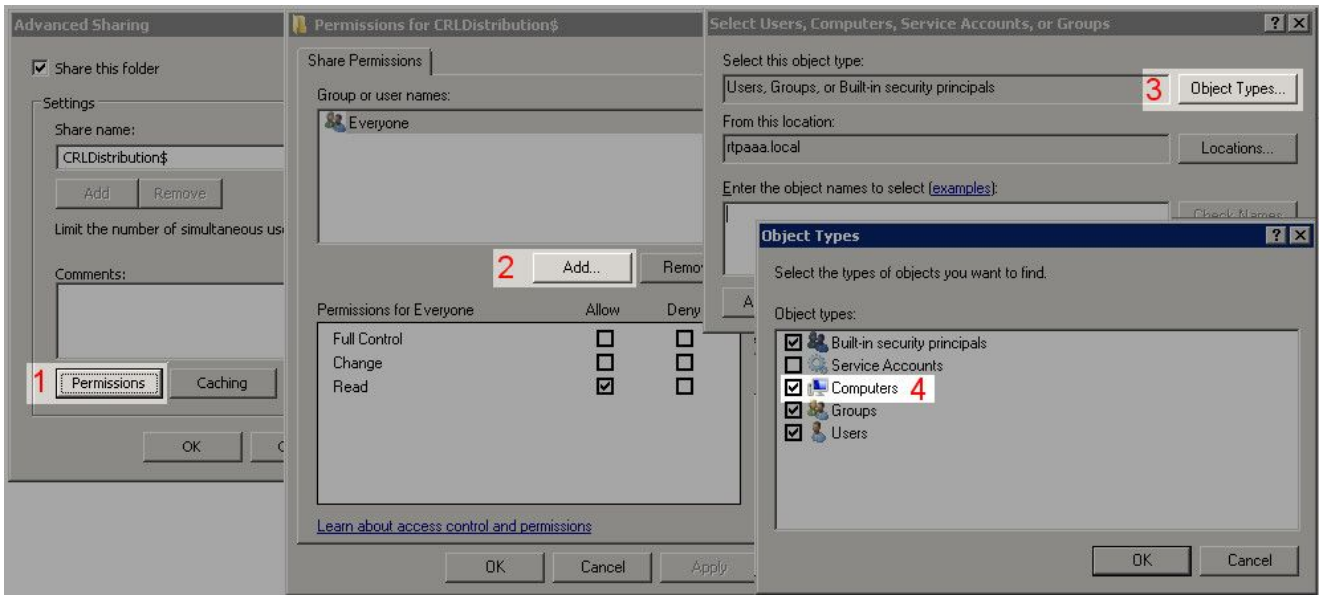
en la **Sharing** ficha y, a continuación, haga clic en **Advanced Sharing**.



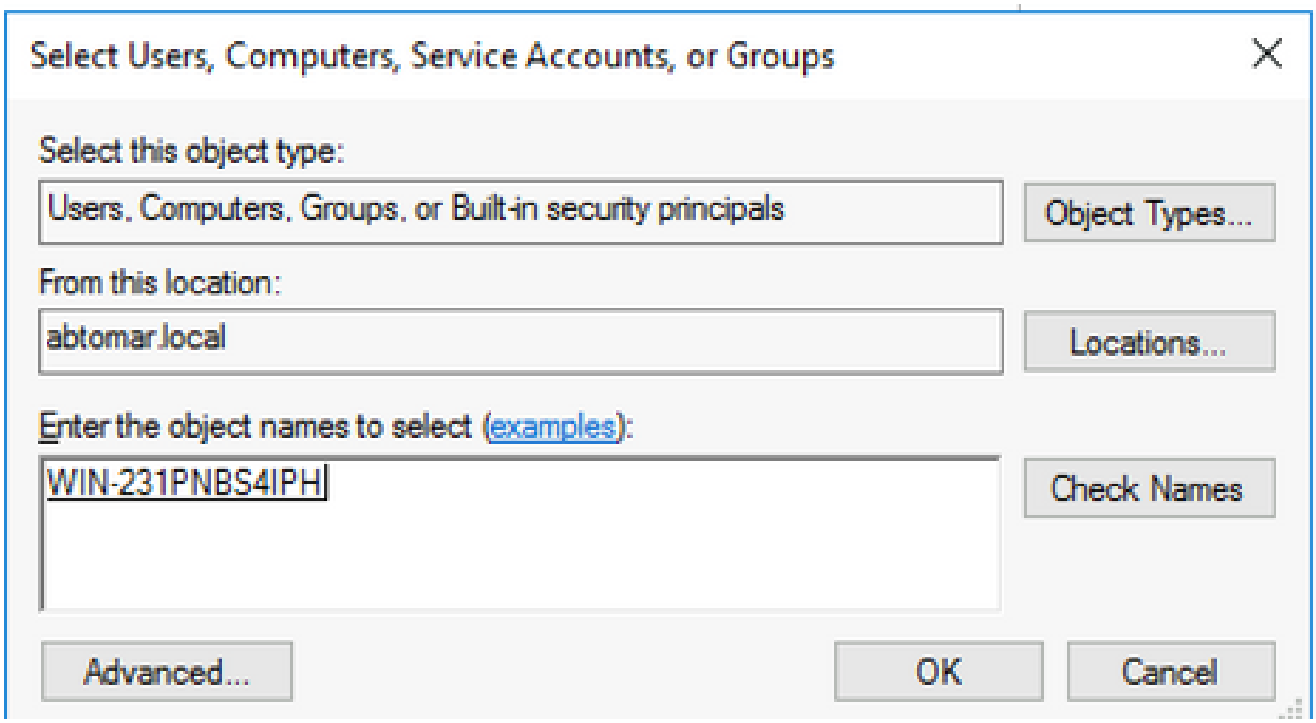
3. Para compartir la carpeta, active la **Share this folder** casilla de verificación y, a continuación, agregue un símbolo de dólar ($) al final del nombre del recurso compartido en el campo Nombre del recurso compartido para ocultar el recurso compartido.



4. Haga clic en **Permissions** (1), haga clic en **Add** (2), haga clic en **Object Types** (3) y active la **Computers** casilla de verificación (4).

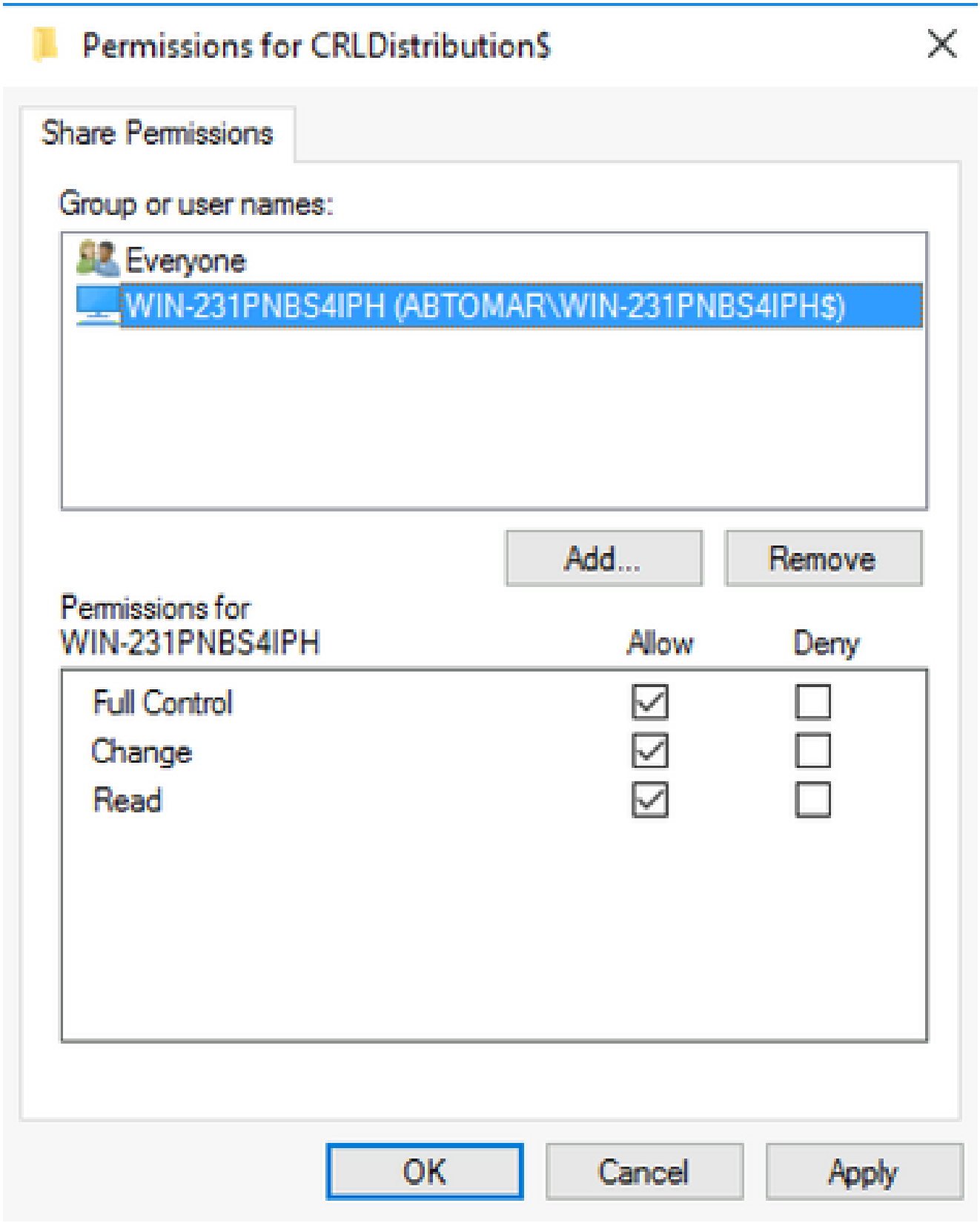


5. Para volver a la ventana Seleccionar usuarios, equipos, cuentas de servicio o grupos, haga clic en **OK**. En el campo Escriba los nombres de objeto que desea seleccionar, escriba el nombre de equipo del servidor de la CA en este ejemplo: WIN0231PNBS4IPH y haga clic en **Check Names**. Si el nombre introducido es válido, se actualiza y aparece subrayado. Haga clic en **OK**.

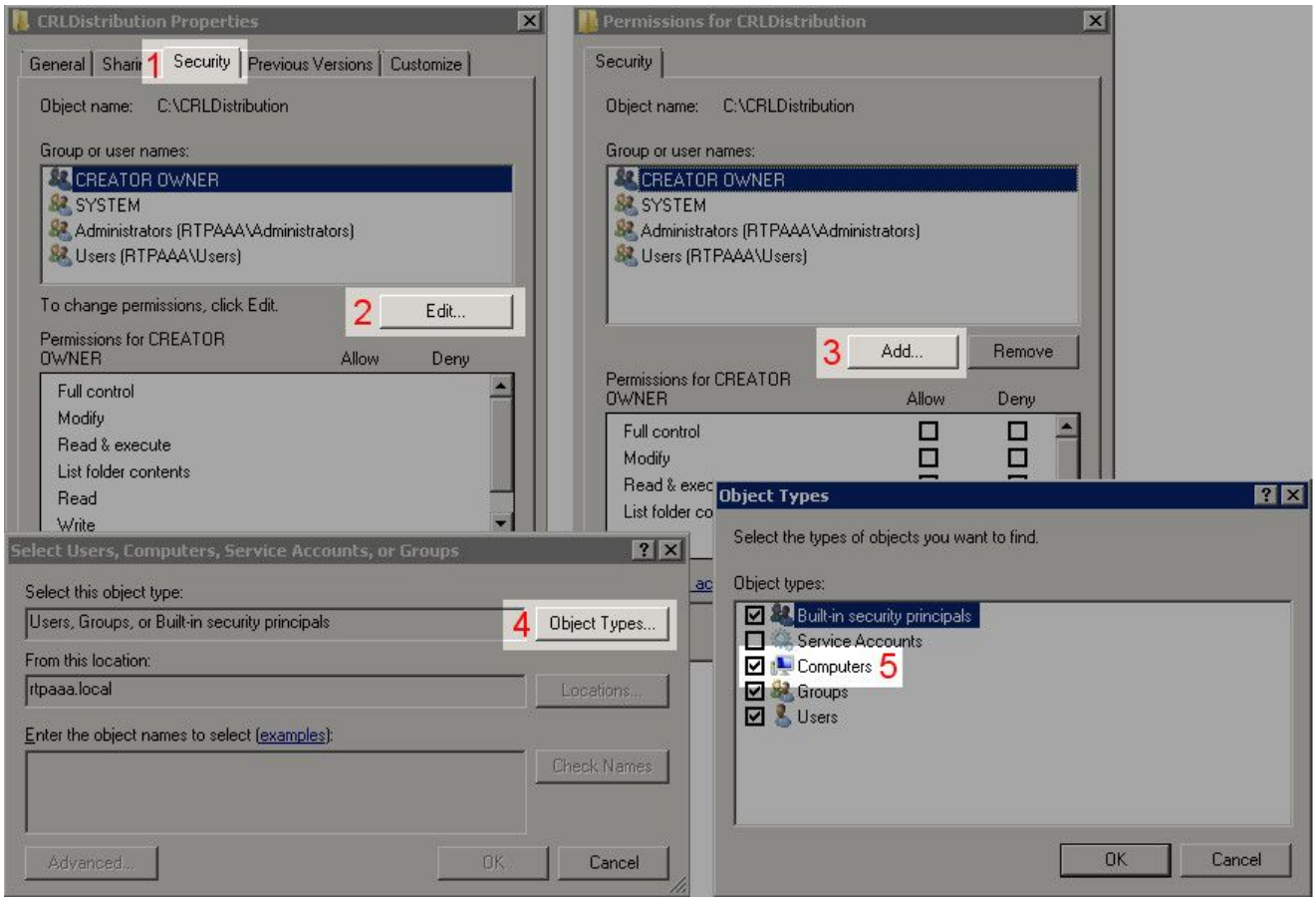


6. En el campo Nombres de grupos o usuarios, elija el equipo de la CA. Compruebe **Allow** el Control total para conceder acceso completo a la CA.

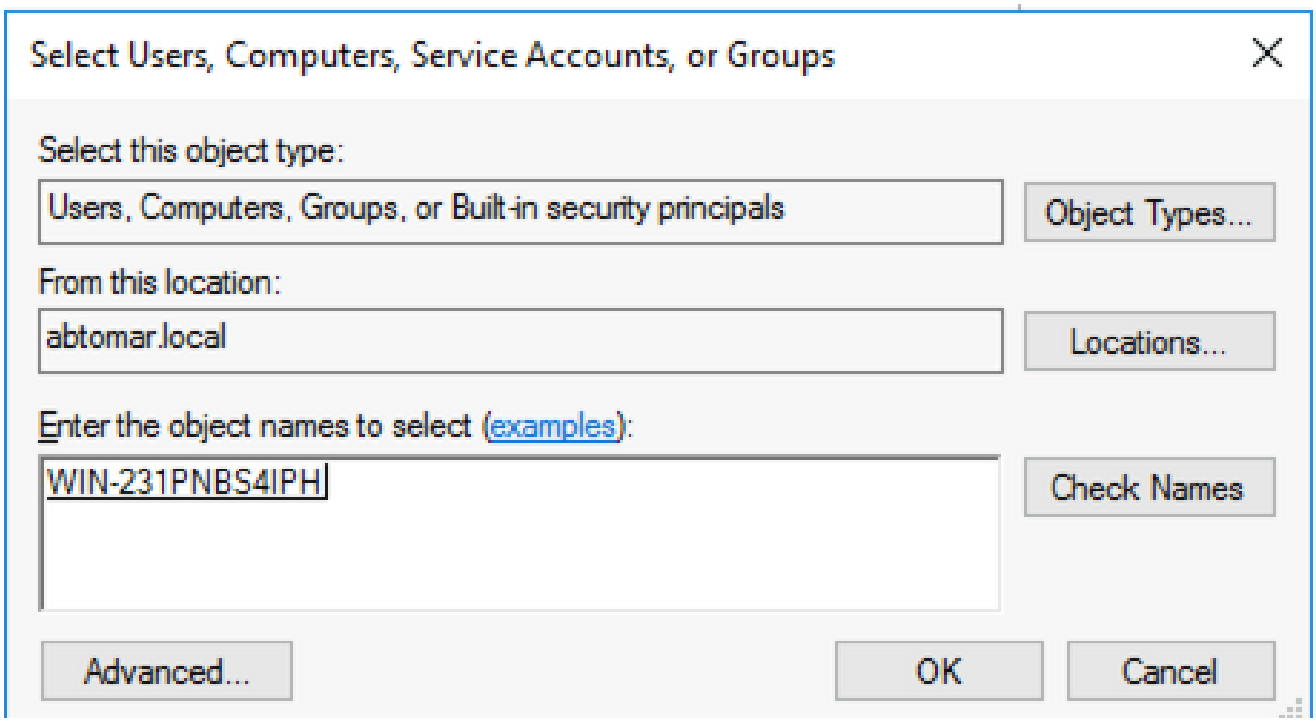
   Haga clic en **OK**. Vuelva **OK** a hacer clic para cerrar la ventana Uso compartido avanzado y volver a la ventana Propiedades.



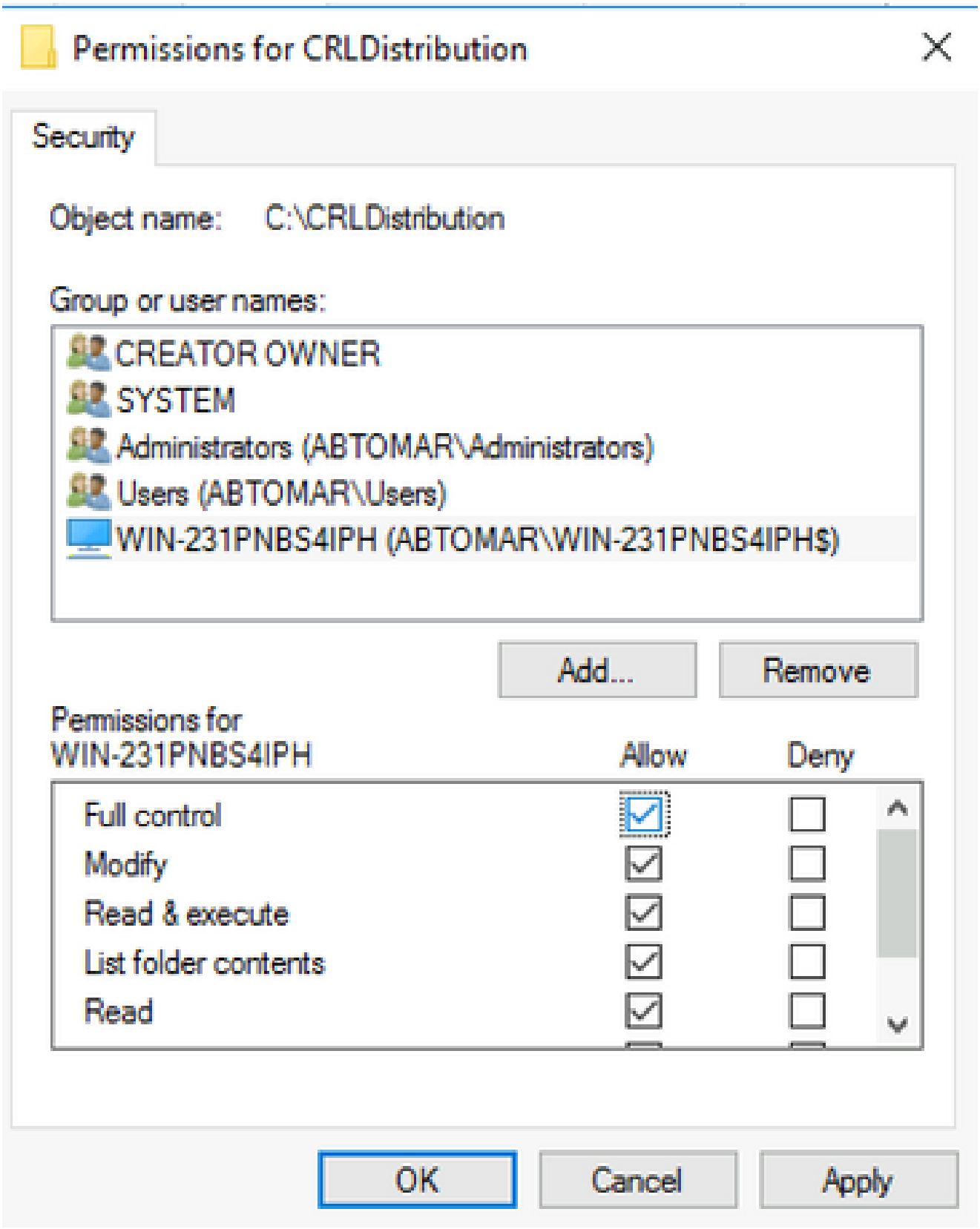
7. Para permitir que la CA escriba los archivos CRL en la nueva carpeta, configure los permisos de seguridad adecuados. Haga clic en las**Security** fichas (1), haga clic en **Edit** (2), haga clic en **Add** (3), haga clic en **Object Types** (4) y active la **Computers** casilla de verificación (5).



8. En el campo Escriba los nombres de objeto que desea seleccionar, escriba el nombre de equipo del servidor de la CA y haga clic en **Check Names**. Si el nombre introducido es válido, se actualiza y aparece subrayado. Haga clic en **OK**.



9. Elija el equipo de la CA en el campo Nombres de grupos o usuarios y, a continuación, compruebe si hay Control total **Allow** para conceder acceso completo a la CA. Haga clic **OK** y, a continuación, haga clic **Close** para completar la tarea.

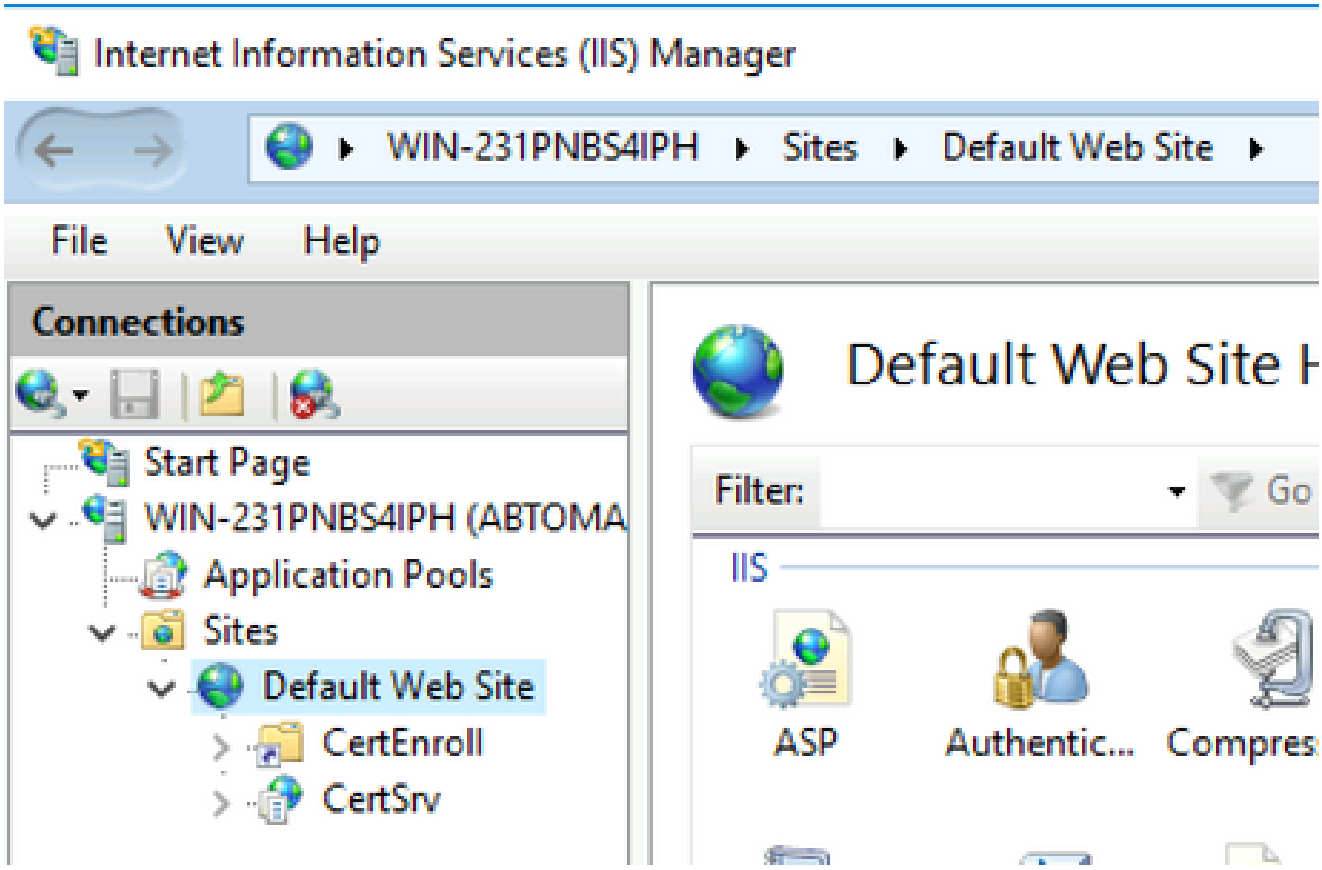


Crear un sitio en IIS para exponer el nuevo punto de distribución CRL

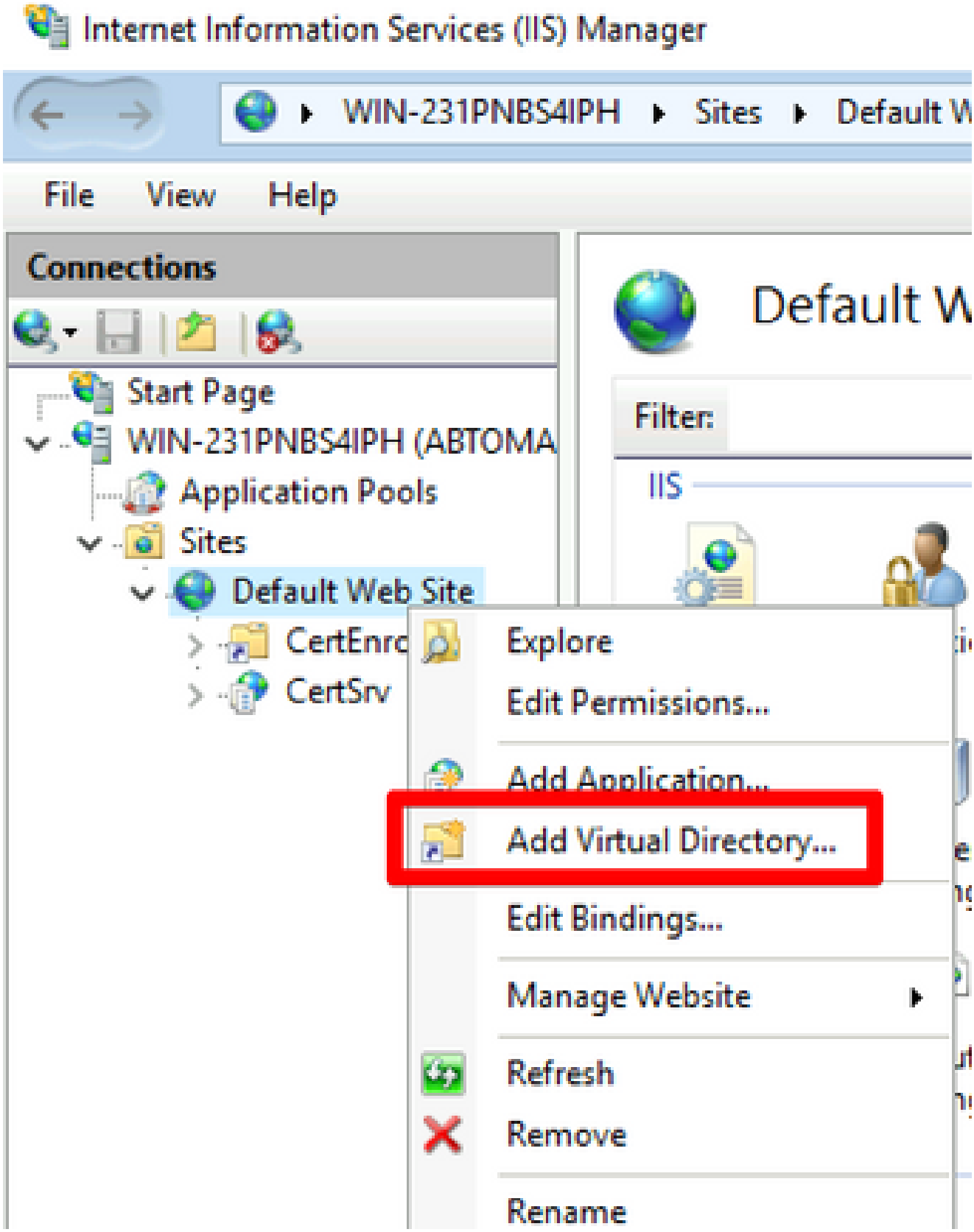
Para que ISE tenga acceso a los archivos CRL, haga que el directorio que contiene los archivos CRL sea accesible a través de IIS.

1. En la barra de tareas del servidor IIS, haga clic en **Start**. Seleccione **Administrative Tools** > **Internet Information Services (IIS) Manager**.

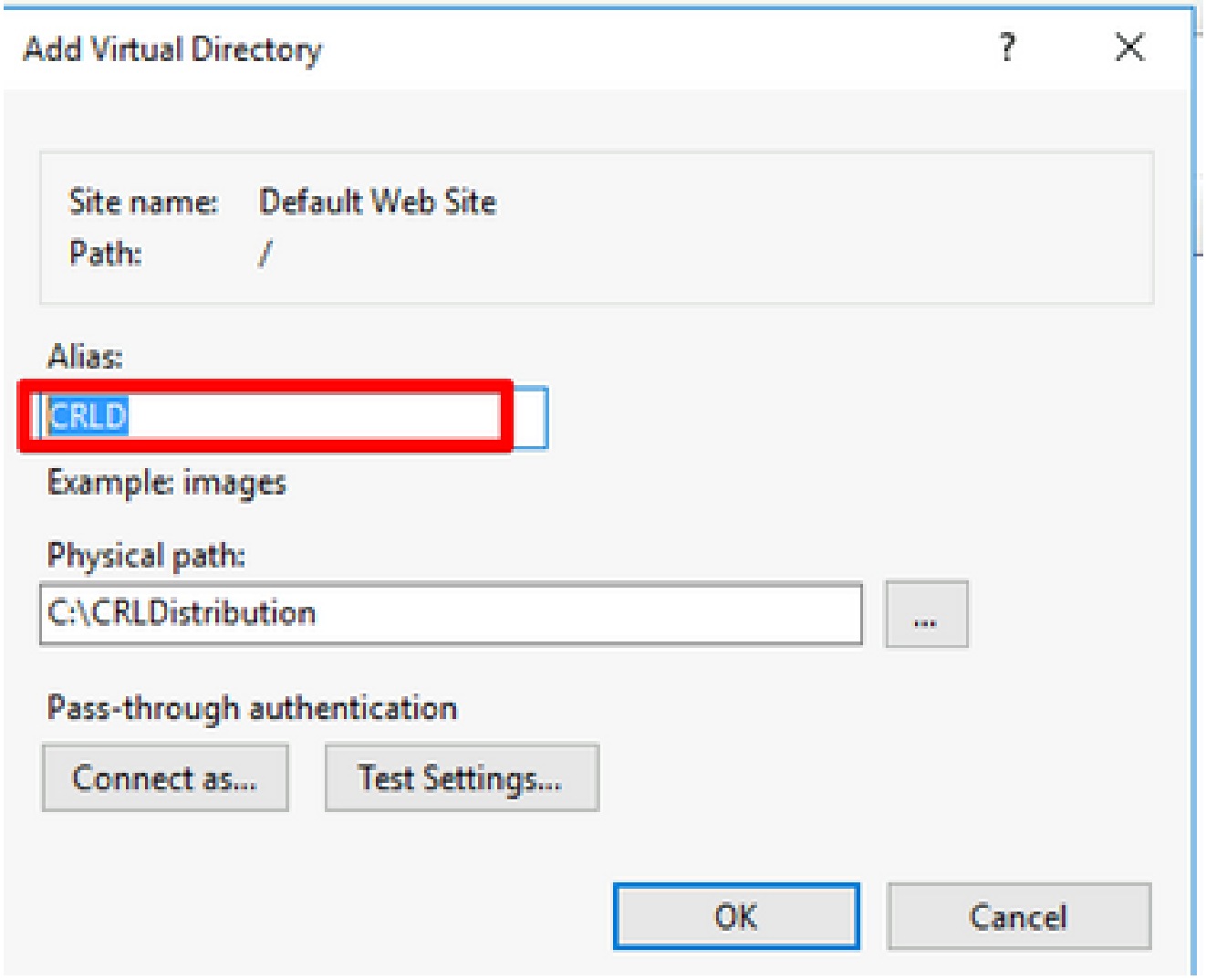
2. En el panel izquierdo (denominado árbol de la consola), expanda el nombre del servidor IIS y, a continuación, expanda **Sites**.



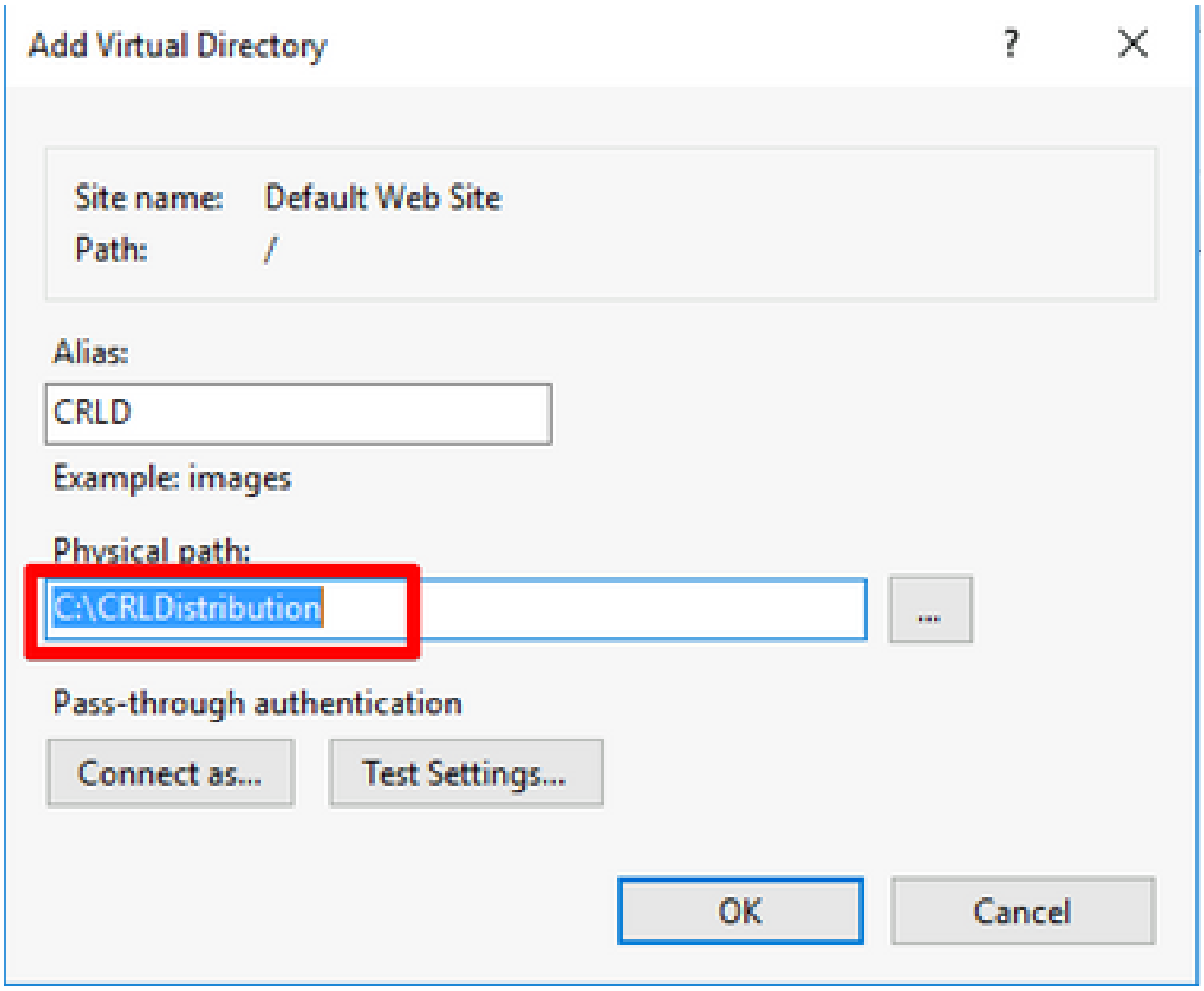
3. Haga clic con el botón derecho del ratón **Default Web Site** y seleccione **Add Virtual Directory**, como se muestra en esta imagen.



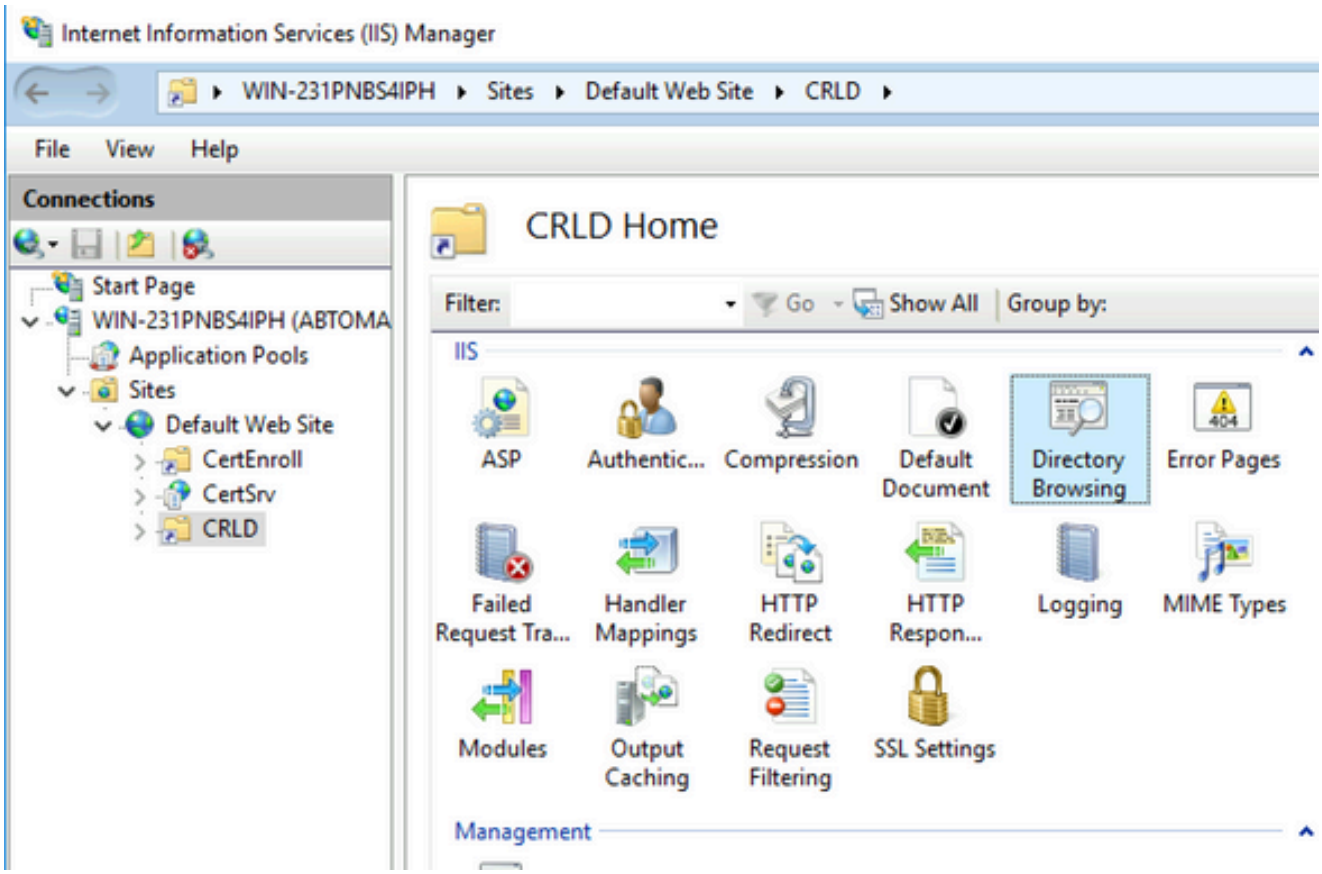
4. En el campo Alias, introduzca un nombre de dirección para el punto de distribución de CRL. En este ejemplo, se ingresa CRLD.



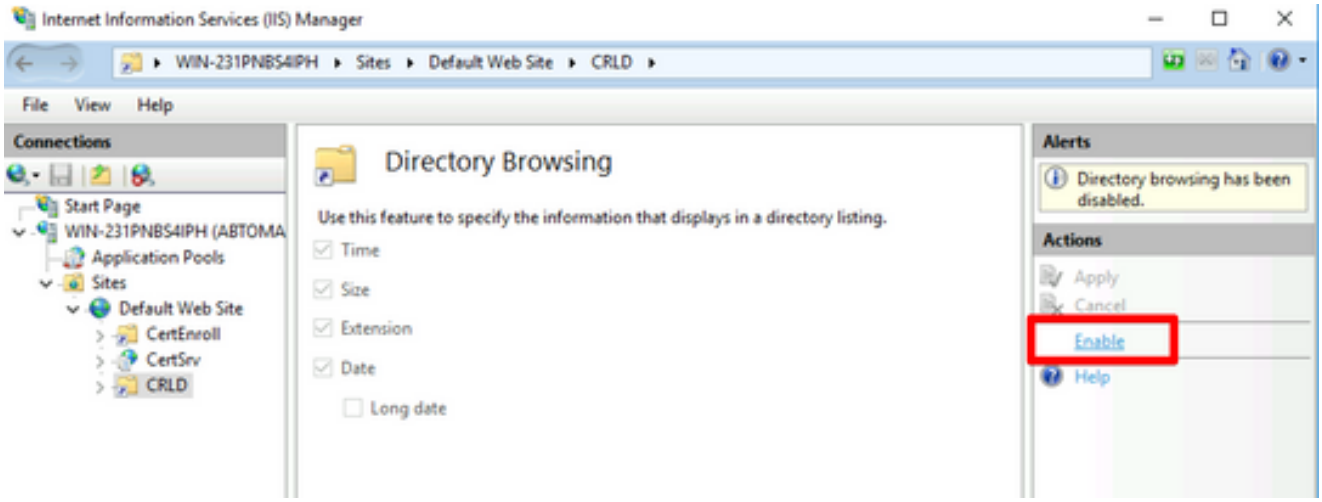
5. Haga clic en los puntos suspensivos (. . .) a la derecha del campo Ruta física y busque la carpeta creada en la sección 1. Seleccione la carpeta y haga clic en OK. Haga clic OK para cerrar la ventana Agregar directorio virtual.



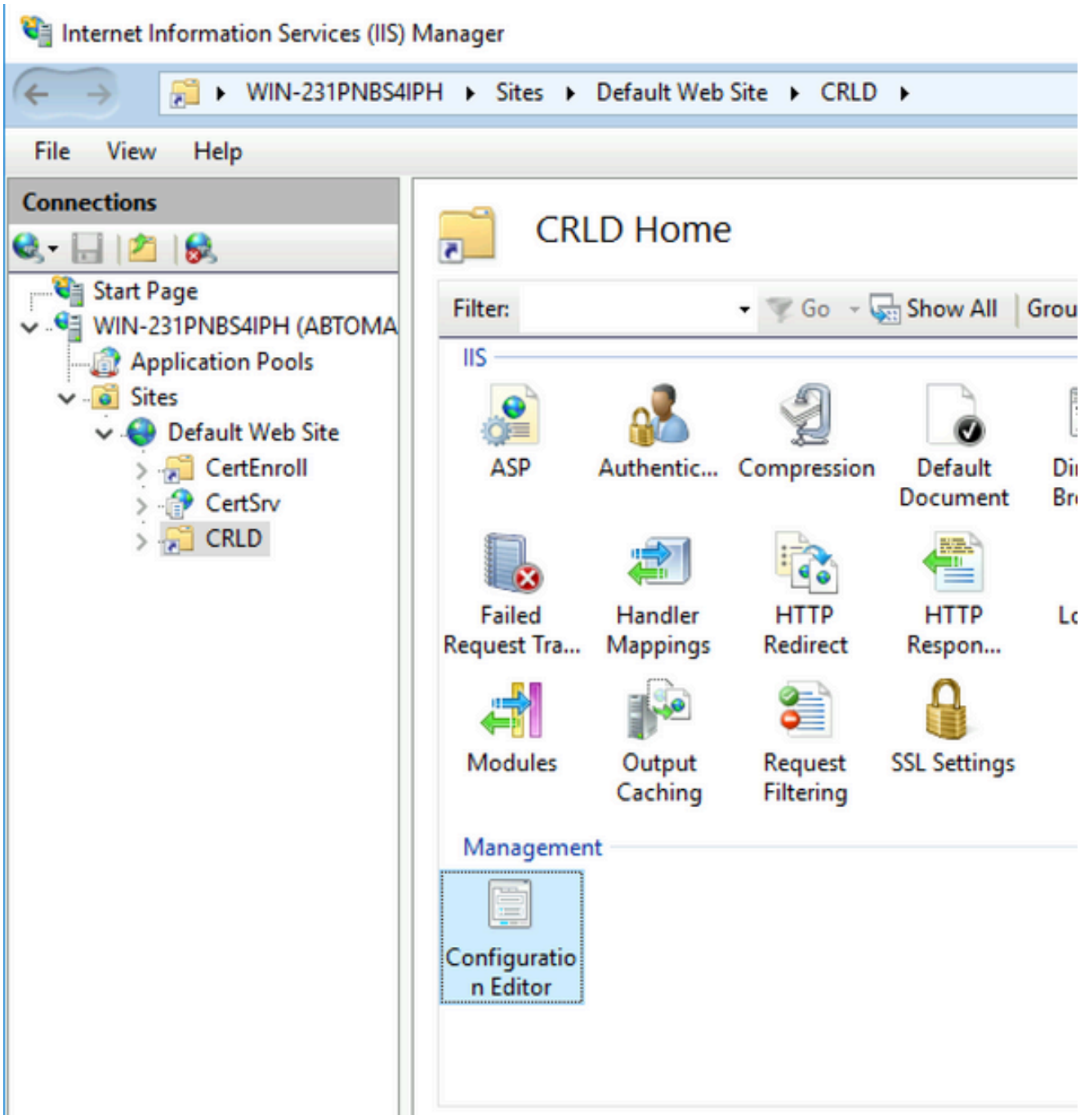
6. El nombre del sitio introducido en el paso 4 debe estar resaltado en el panel izquierdo. Si no es así, selecciónela ahora. En el panel central, haga doble clic en **Directory Browsing**.



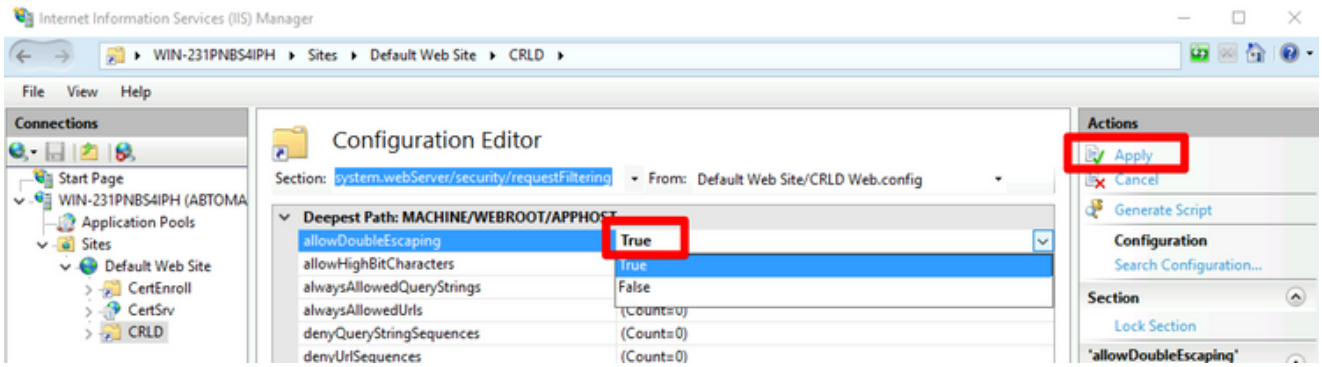
7. En el panel derecho, haga clic **Enable** para habilitar la exploración de directorios.



8. En el panel izquierdo, elija de nuevo el nombre del sitio. En el panel central, haga doble clic en **Configuration Editor**.



9. En la lista desplegable Sección, seleccione **system.webServer/security/requestFiltering**. En la lista **allowDoubleEscaping** desplegable, seleccione **True**. En el panel derecho, haga clic en **Apply**, como se muestra en esta imagen.

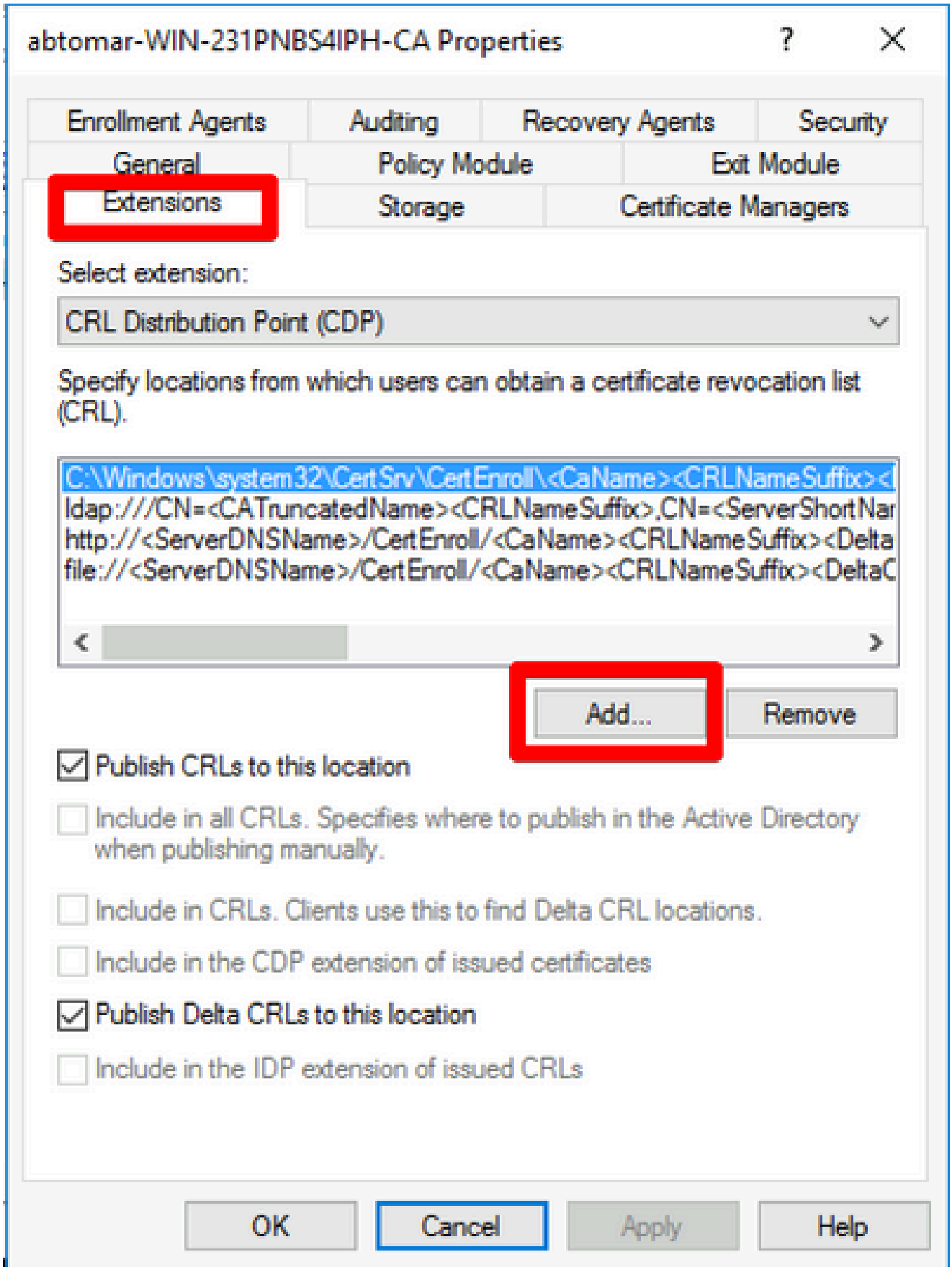


Ahora se debe poder tener acceso a la carpeta mediante IIS.

Configurar Microsoft CA Server para publicar archivos CRL en el punto de distribución

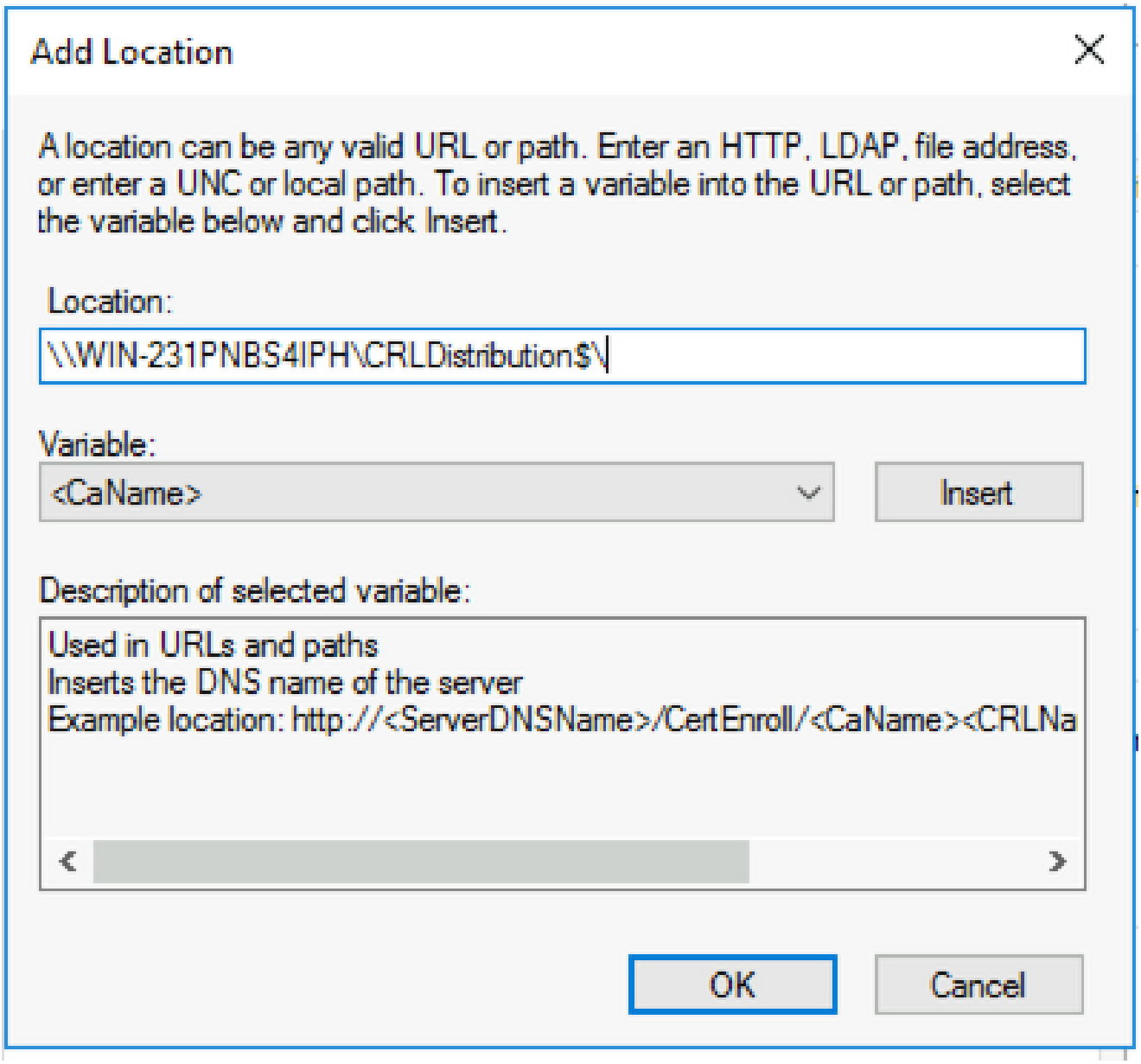
Ahora que se ha configurado una nueva carpeta para alojar los archivos CRL y que la carpeta se ha expuesto en IIS, configure el servidor de la CA de Microsoft para publicar los archivos CRL en la nueva ubicación.

1. En la barra de tareas del servidor de la CA, haga clic en **Start**. Seleccione **Administrative Tools** > **Certificate Authority**.
2. En el panel izquierdo, haga clic con el botón secundario en el nombre de la CA. Elija **Properties** y haga clic en la **Extensions** ficha. Para agregar un nuevo punto de distribución CRL, haga clic en **Add**.

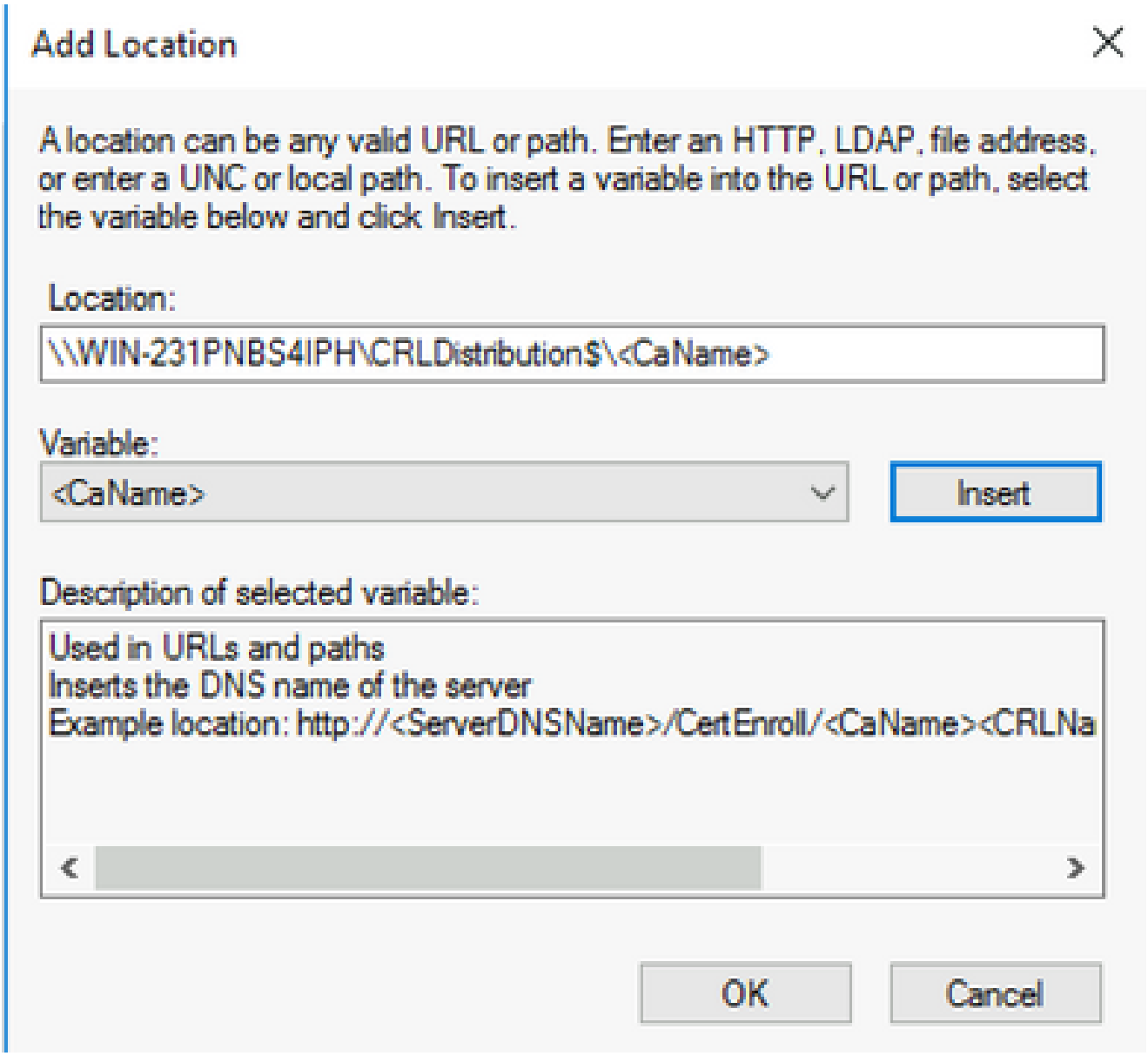


3. En el campo Ubicación, introduzca la ruta de la carpeta creada y compartida en la sección 1. En el ejemplo de la sección 1, la ruta de acceso es:

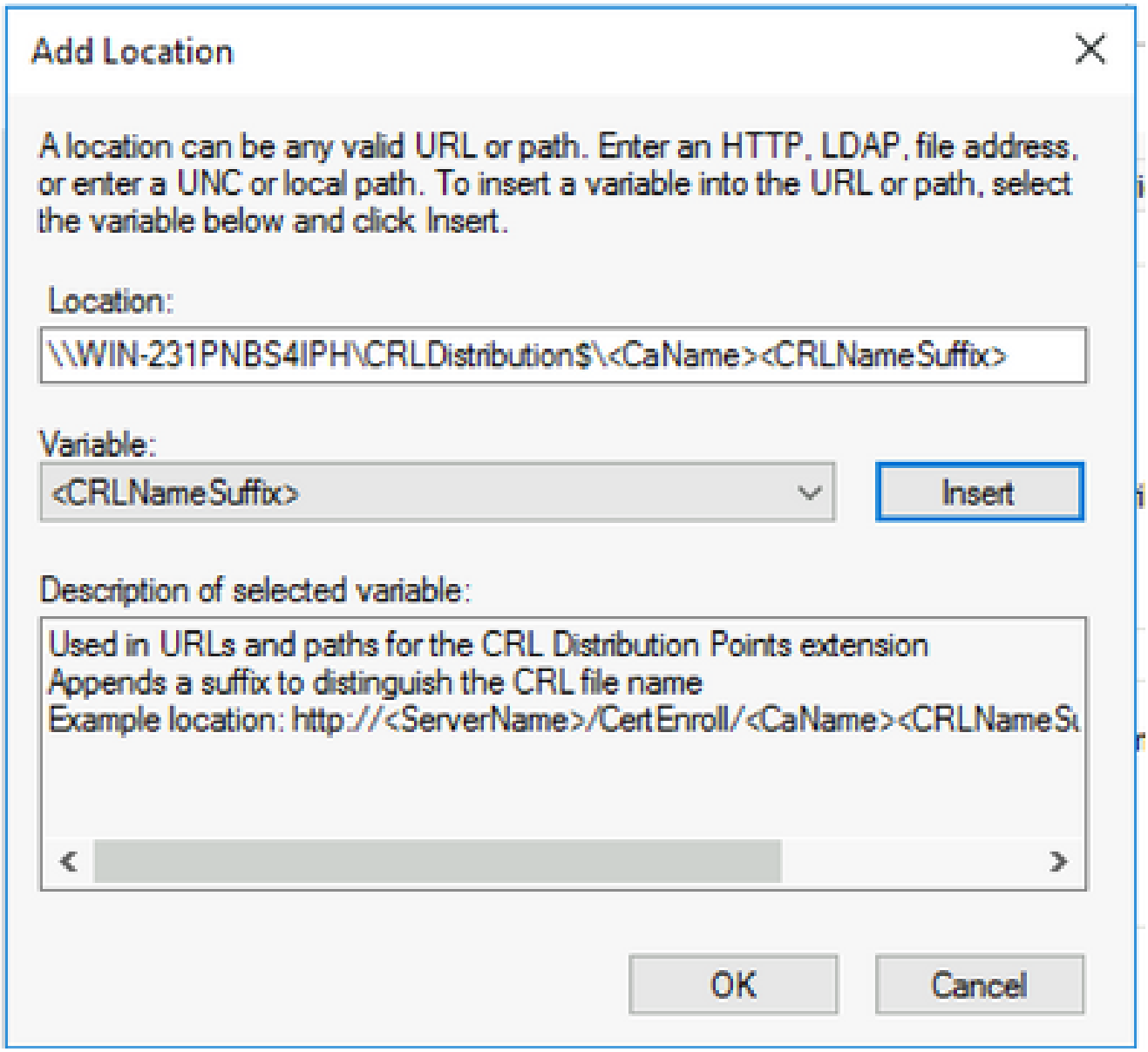
\\WIN-231PNBS4IPH\CRLDistribution$



4. Con el campo Ubicación rellenado, selecciónelo en la lista desplegable Variable y haga clic en **Insert**.



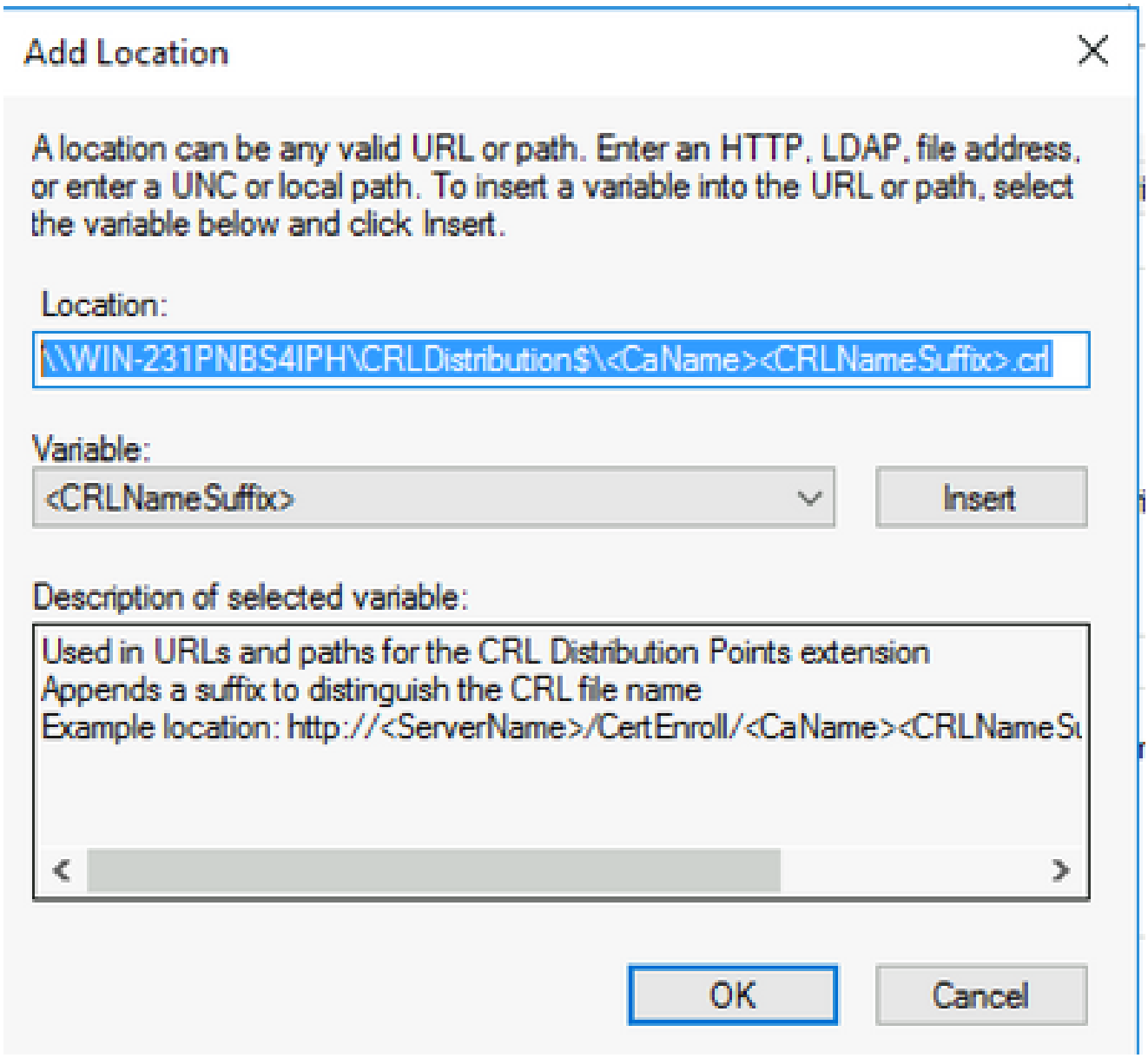
5. En la lista desplegable Variable, elija
y haga clic en **Insert**.



6. En el campo Ubicación, anexe **.crl** al final de la ruta. En este ejemplo, Location es:

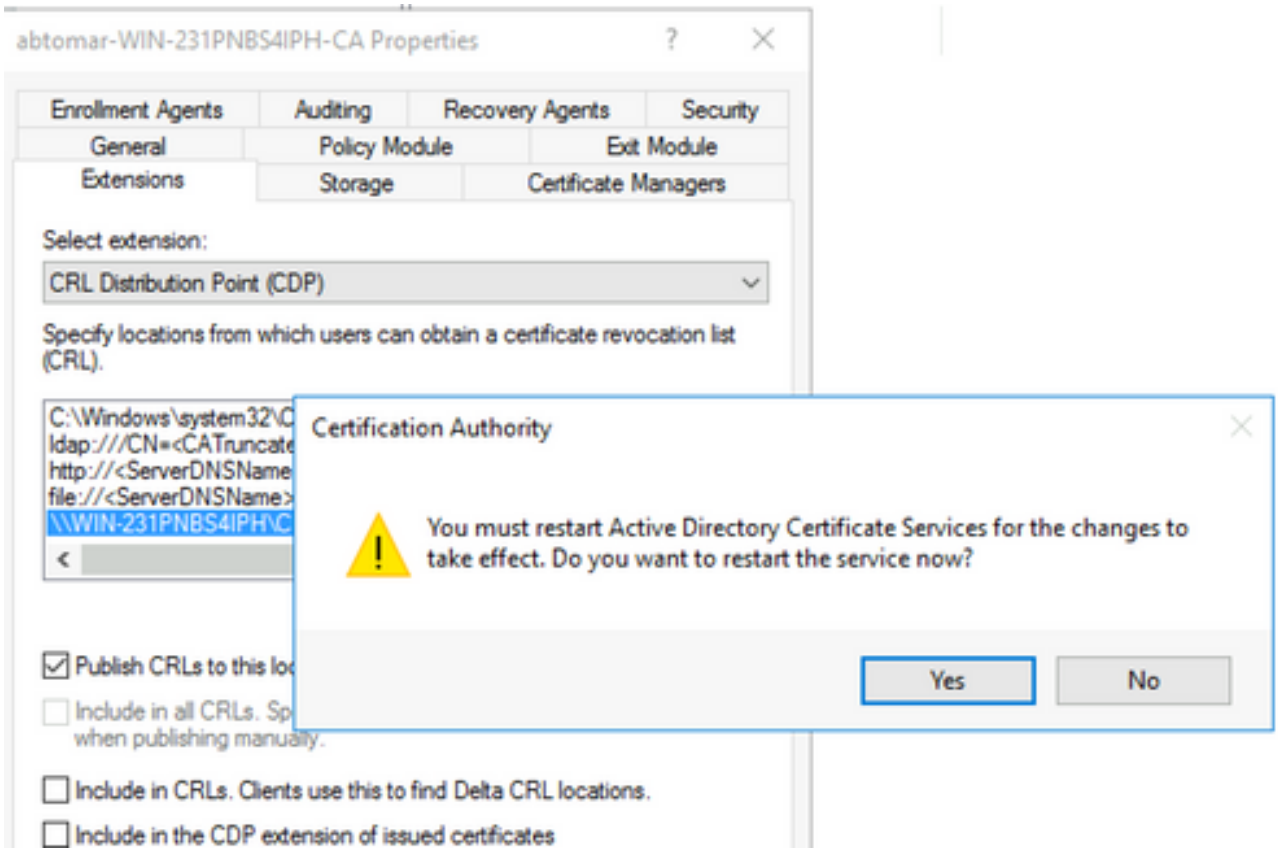
\\WIN-231PNBS4IPH\CRLDistribution$

.crl

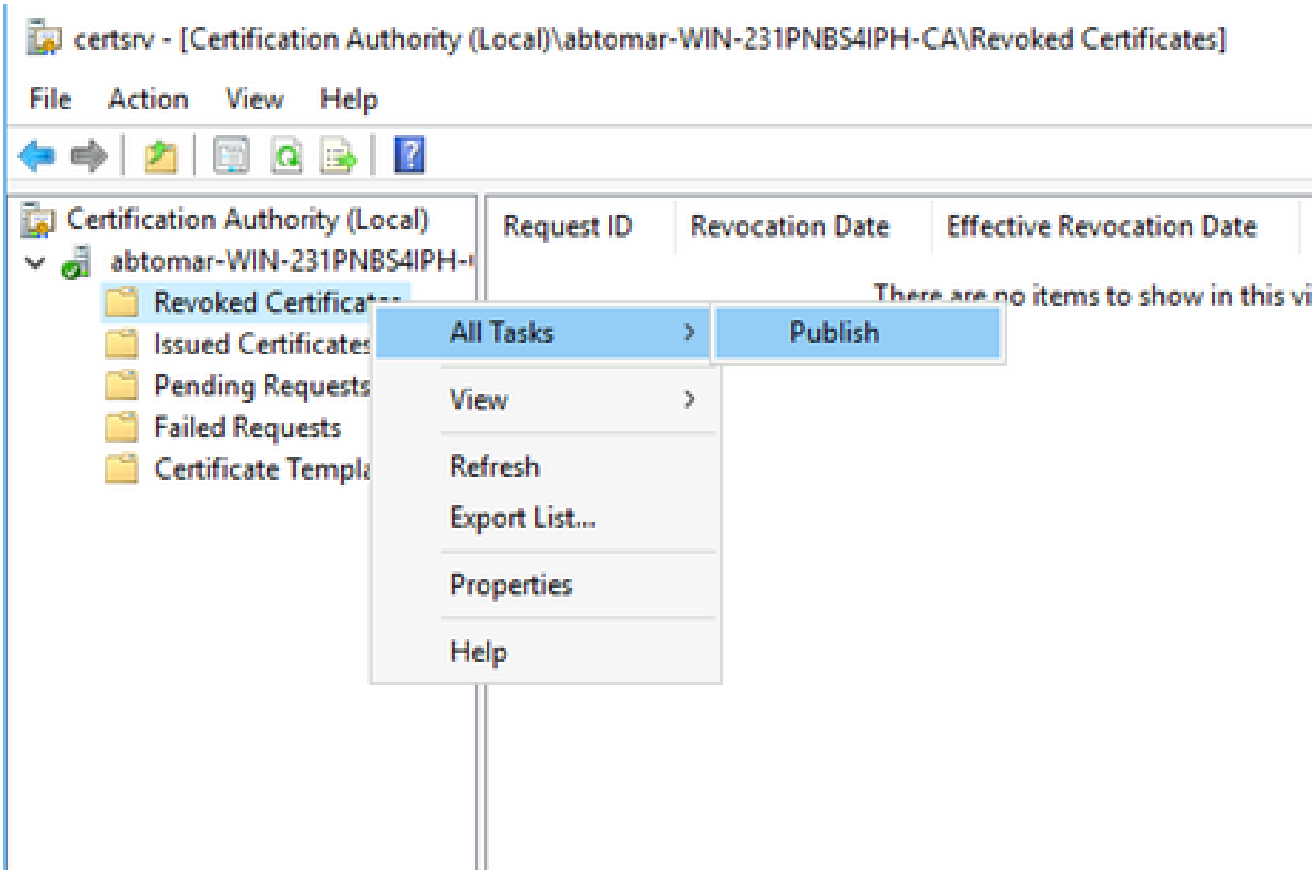


7. Haga clic **OK** para volver a la ficha Extensiones. Marque la **Publish CRLs to this location** casilla de verificación y haga clic **OK** para cerrar la ventana Propiedades.

   Aparece una solicitud de permiso para reiniciar Servicios de certificados de Active Directory. Haga clic en **Yes**.



8. En el panel izquierdo, haga clic con el botón derecho del ratón **Revoked Certificates**. Seleccione **All Tasks** > **Publish**. Asegúrese de que está seleccionada la opción Nueva CRL y, a continuación, haga clic en **OK**.



El servidor de la CA de Microsoft debe crear un nuevo archivo .crl en la carpeta creada en la sección 1. Si el nuevo archivo CRL se crea correctamente, no habrá ningún cuadro de diálogo después de hacer clic en Aceptar. Si se devuelve un error con respecto a la nueva carpeta de puntos de distribución, repita cuidadosamente cada paso de esta sección.

Compruebe que el archivo CRL existe y que se puede obtener acceso a él mediante IIS

Compruebe que los nuevos archivos CRL existen y que se puede obtener acceso a ellos a través de IIS desde otra estación de trabajo antes de iniciar esta sección.

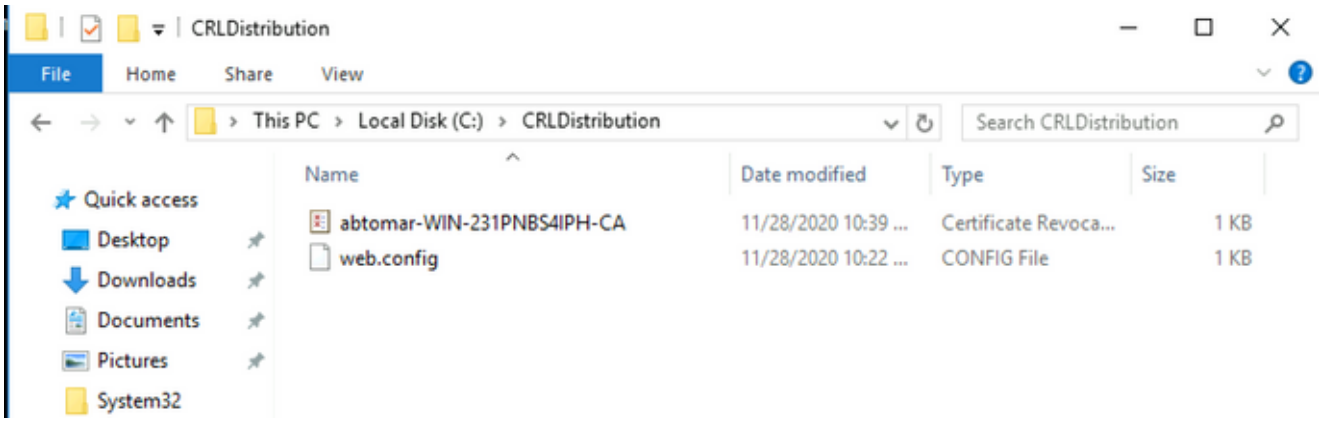
1. En el servidor IIS, abra la carpeta creada en la sección 1. Debe haber un único archivo .crl con el formulario

   .crl

   donde

   es el nombre del servidor de la CA. En este ejemplo, el nombre de archivo es:

   abtomar-WIN-231PNBS4IPH-CA.crl



2. Desde una estación de trabajo de la red (idealmente en la misma red que el nodo de administración principal de ISE), abra un navegador web y navegue hasta http://

   /

   donde

   sea el nombre del servidor de IIS configurado en la sección 2 y

   sea el nombre del sitio elegido para el punto de distribución en la sección 2. En este ejemplo, la dirección URL es:

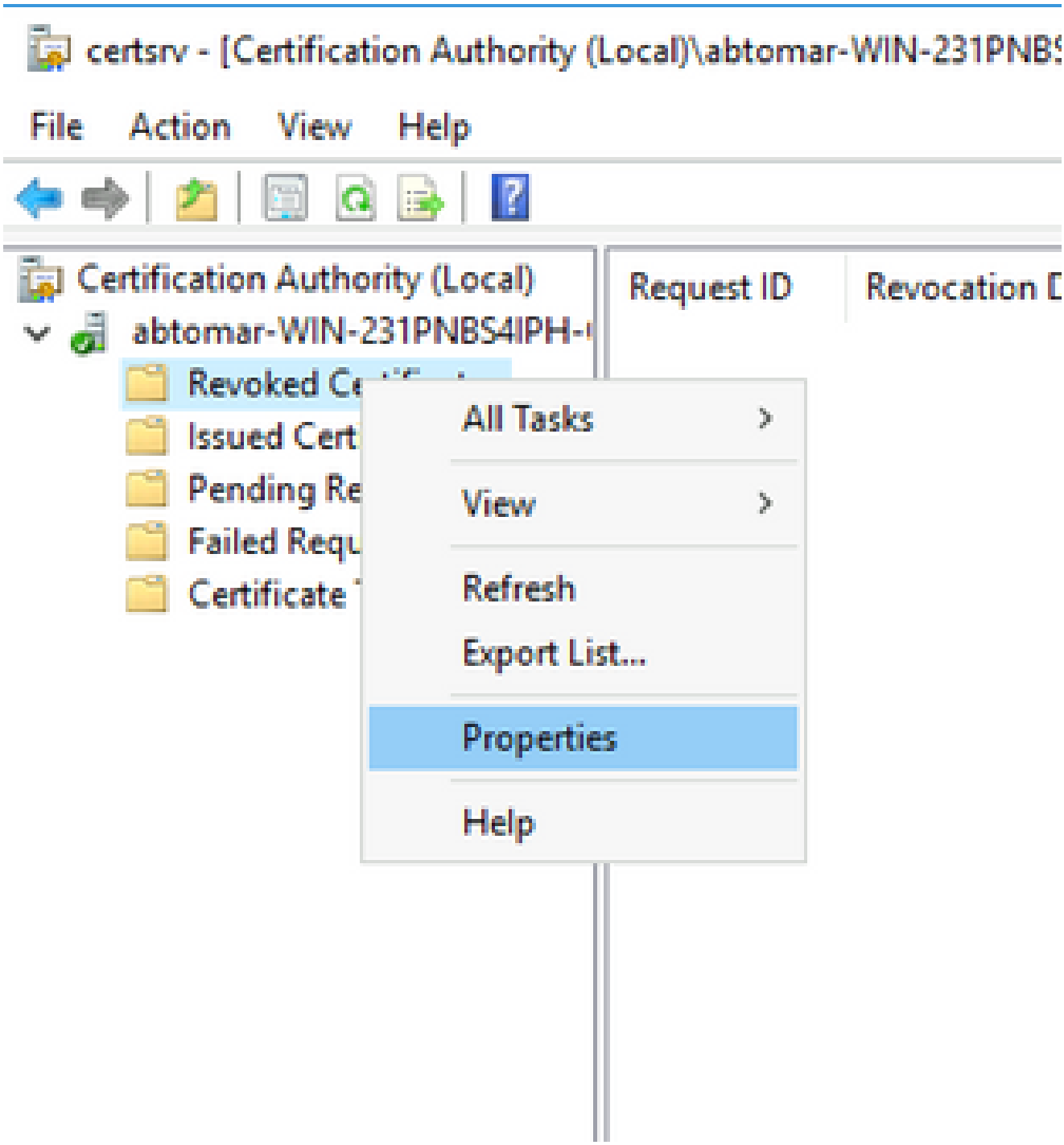
   http://win-231pnbs4iph/CRLD

   Aparece el índice de directorio, que incluye el archivo observado en el paso 1.

Configuración de ISE para utilizar el nuevo punto de distribución de CRL

Antes de configurar ISE para recuperar la CRL, defina el intervalo para publicar la CRL. La estrategia para determinar este intervalo está fuera del alcance de este documento. Los valores potenciales (en Microsoft CA) oscilan entre 1 hora y 41 años, ambos incluidos. El valor predeterminado es 1 semana. Una vez determinado el intervalo adecuado para su entorno, configúrelo con estas instrucciones:

1. En la barra de tareas del servidor de la CA, haga clic en **Start**. Seleccione **Administrative Tools** > **Certificate Authority**.
2. En el panel izquierdo, expanda la CA. Haga clic con el botón secundario en la **Revoked Certificates** carpeta y seleccione **Properties**.
3. En los campos Intervalo de publicación de CRL, escriba el número necesario y elija el período de tiempo. Haga clic **OK** para cerrar la ventana y aplicar el cambio. En este ejemplo, se configura un intervalo de publicación de siete días.



4. Ingrese el **certutil -getreg CA\Clock*** comando para confirmar el valor ClockSkew. El valor predeterminado es 10 minutos.

   Ejemplo de salida:

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

5. Ingrese el **certutil -getreg CA\CRLov*** comando para verificar si CRLOverlapPeriod se ha configurado manualmente. De forma predeterminada, el valor de CRLOverlapUnit es 0, lo

que indica que no se ha establecido ningún valor manual. Si el valor es un valor distinto de 0, registre el valor y las unidades.

Ejemplo de salida:

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

6. Ingrese el **certutil -getreg CA\CRLpe*** comando para verificar el CRLPeriod, que se estableció en el paso 3.

   Ejemplo de salida:

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

7. Calcule el período de gracia de CRL de la siguiente manera:

   a. Si CRLOverlapPeriod se estableció en el paso 5: OVERLAP = CRLOverlapPeriod, en minutos;

   Else: OVERLAP = (CRLPeriod / 10), en minutos

   b. Si SUPERPOSICIÓN > 720, entonces SUPERPOSICIÓN = 720

   c. Si SUPERPOSICIÓN < (1,5 * ClockSkewMinutes), entonces SUPERPOSICIÓN = (1,5 * ClockSkewMinutes)

   d. Si SOLAPAMIENTO > CRLPeriod, en minutos entonces SOLAPAMIENTO = CRLPeriod en minutos

   e. Período de gracia = SUPERPOSICIÓN + MinutosSesgadoReloj

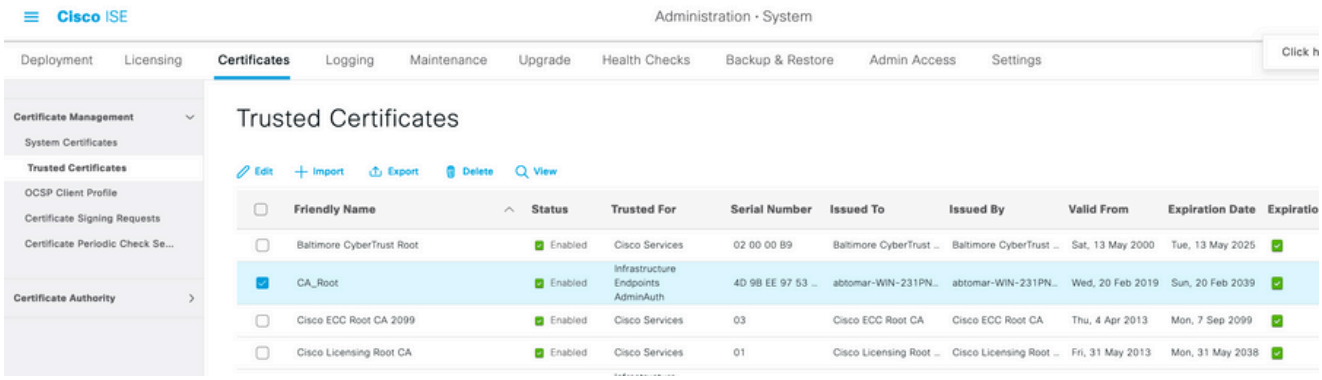
```
Example:

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
```

El período de gracia calculado es la cantidad de tiempo entre el momento en que la CA publica la siguiente CRL y el momento en que caduca la CRL actual. ISE debe configurarse para recuperar las CRL en consecuencia.

8. Inicie sesión en el nodo ISE Primary Admin y elija **Administration** > **System** > **Certificates**. En el panel izquierdo, elija **Trusted Certificate**.

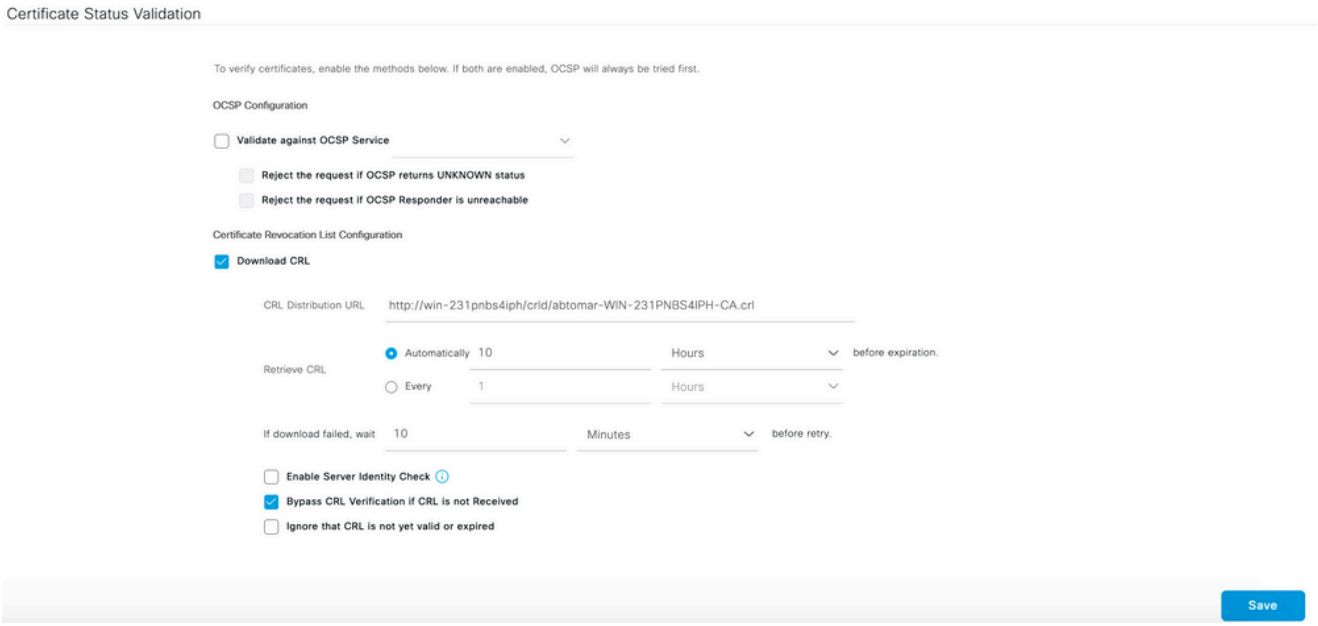


9. Active la casilla de verificación situada junto al certificado de CA para el que desea configurar CRL. Haga clic en **Edit**.
10. Cerca de la parte inferior de la ventana, marque la **Download CRL** casilla de verificación.
11. En el campo URL de distribución CRL, escriba la ruta de acceso al punto de distribución CRL, que incluye el archivo .crl, creado en la sección 2. En este ejemplo, la dirección URL es:

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

12. ISE se puede configurar para recuperar la CRL a intervalos regulares o en función del vencimiento (que, en general, también es un intervalo regular). Cuando el intervalo de publicación de CRL es estático, se obtienen actualizaciones de CRL más oportunas cuando se utiliza esta última opción. Haga clic en el botón de **Automatically** opción.
13. Establezca el valor de recuperación en un valor inferior al período de gracia calculado en el paso 7. Si el valor establecido es superior al período de gracia, ISE comprueba el punto de distribución de CRL antes de que la CA haya publicado la siguiente CRL. En este ejemplo, el período de gracia se calcula en 730 minutos, o 12 horas y 10 minutos. Se utilizará un valor de 10 horas para la recuperación.
14. Defina el intervalo de reintento como corresponda a su entorno. Si ISE no puede recuperar la CRL en el intervalo configurado en el paso anterior, volverá a intentarlo en este intervalo más corto.
15. Marque la **Bypass CRL Verification if CRL is not Received** casilla de verificación para permitir que la autenticación basada en certificados continúe normalmente (y sin una comprobación de CRL) si ISE no pudo recuperar la CRL para esta CA en su último intento de descarga. Si esta casilla de verificación no está activada, se producirá un error en toda la autenticación basada en certificados con certificados emitidos por esta CA si no se puede recuperar la CRL.
16. Marque la **Ignore that CRL is not yet valid or expired** casilla de verificación para permitir que ISE utilice

archivos CRL caducados (o que aún no sean válidos) como si fueran válidos. Si esta casilla de verificación no está activada, ISE considera que una CRL no es válida antes de la fecha en vigor y después de la siguiente actualización. Haga clic **Save** para completar la configuración.



Verificación

Actualmente, no hay un procedimiento de verificación disponible para esta configuración.

Troubleshoot

Actualmente, no hay información específica de troubleshooting disponible para esta configuración.

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).