Configuración de Microsoft CA Server para Publicar las Listas de Revocación de Certificados para ISE

Contenido

Introducción

Este documento describe la configuración de un servidor de Microsoft Certificate Authority (CA) que ejecuta Servicios de Internet Information Server (IIS) para publicar las actualizaciones de la lista de revocación de certificados (CRL). También explica cómo configurar Cisco Identity Services Engine (ISE) (versiones 3.0 y posteriores) para recuperar las actualizaciones para usarlas en la validación de certificados. ISE se puede configurar para recuperar CRL para los diversos 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.

- Versión 3.0 de Cisco Identity Services Engine
- Microsoft Windows® Server® 2008 R2

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Configurar

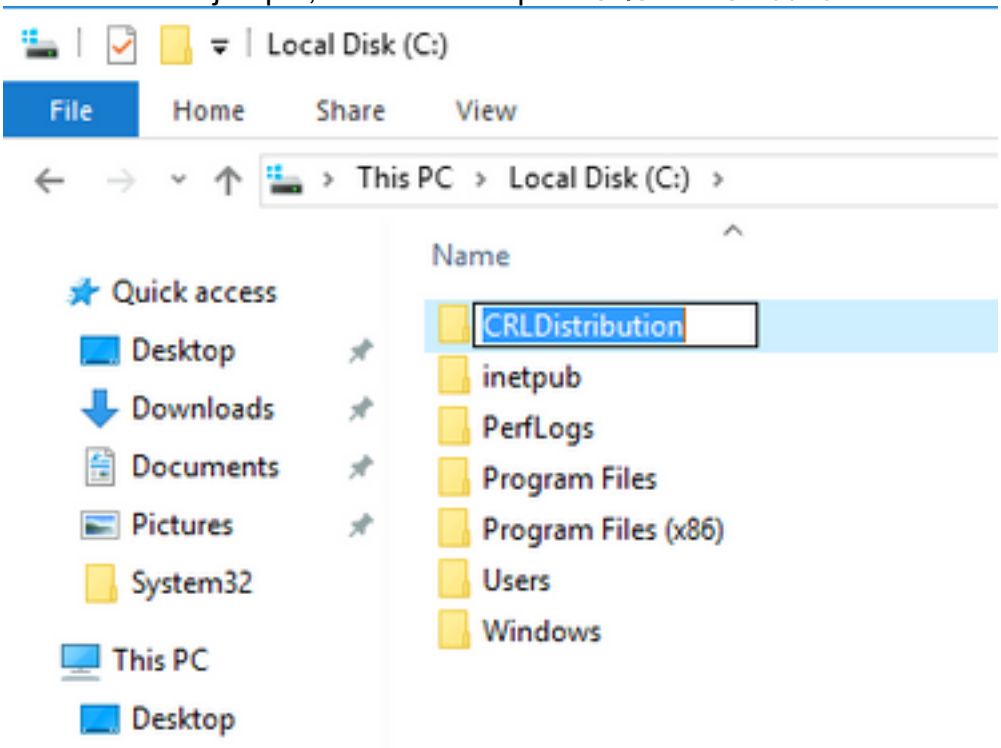
En esta sección encontrará la información para configurar las funciones descritas en este documento.

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

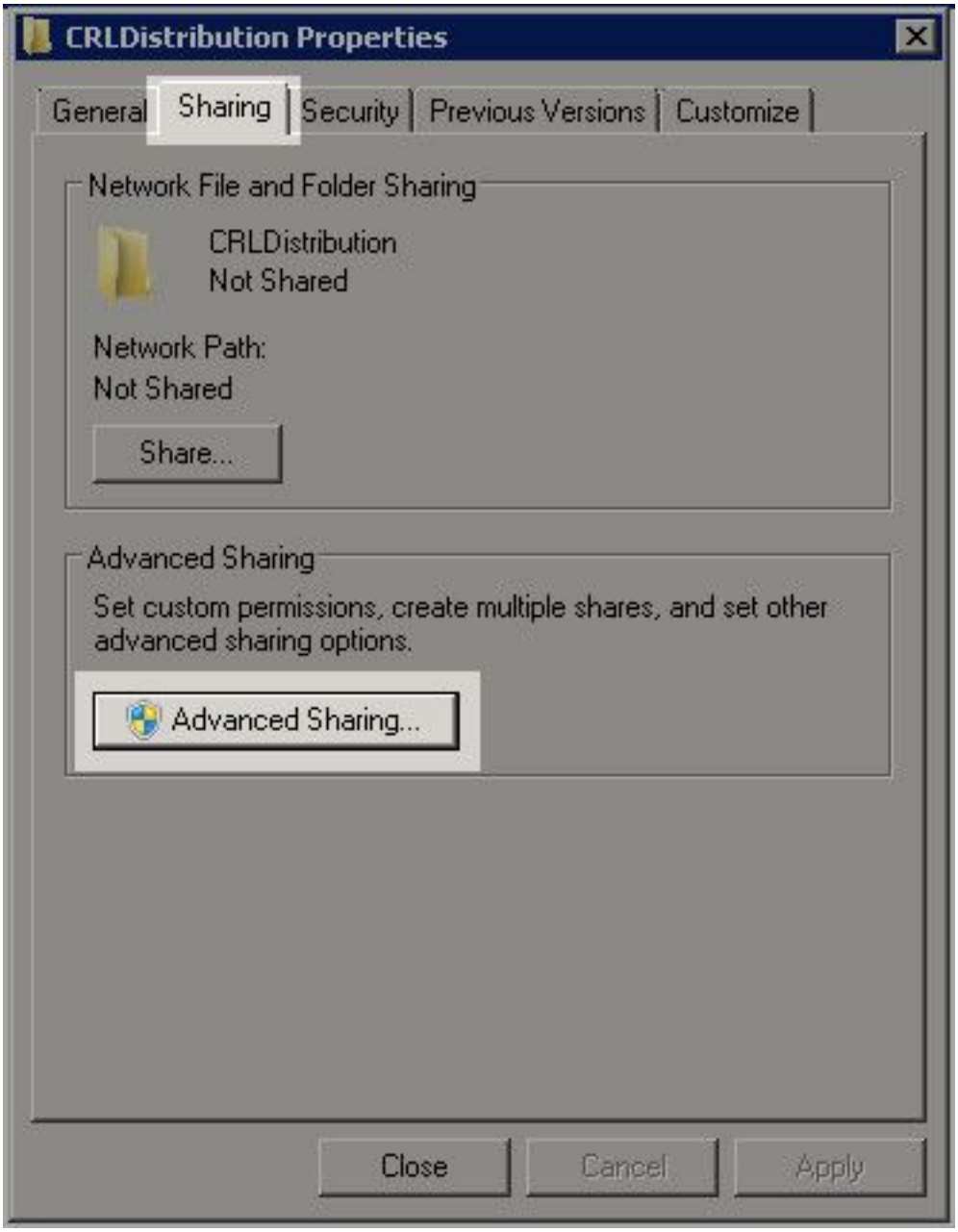
La primera tarea es configurar una ubicación en el servidor de la CA para almacenar los archivos CRL. De forma predeterminada, el servidor de Microsoft CA publica los archivos en **C:\Windows\system32\CertSrv\CertEnroll**

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

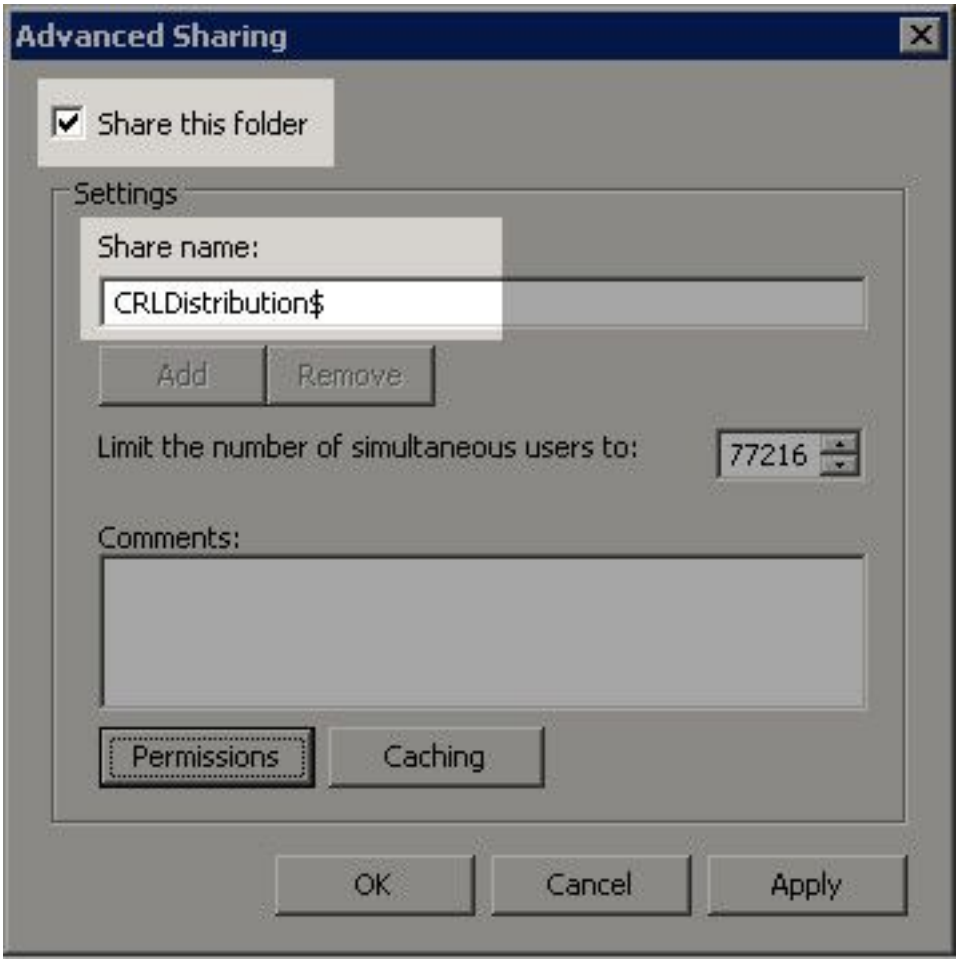
1. En el servidor IIS, elija una ubicación en el sistema de archivos y cree una nueva carpeta. En este ejemplo, se crea la carpeta **C:\CRLDistribution**.



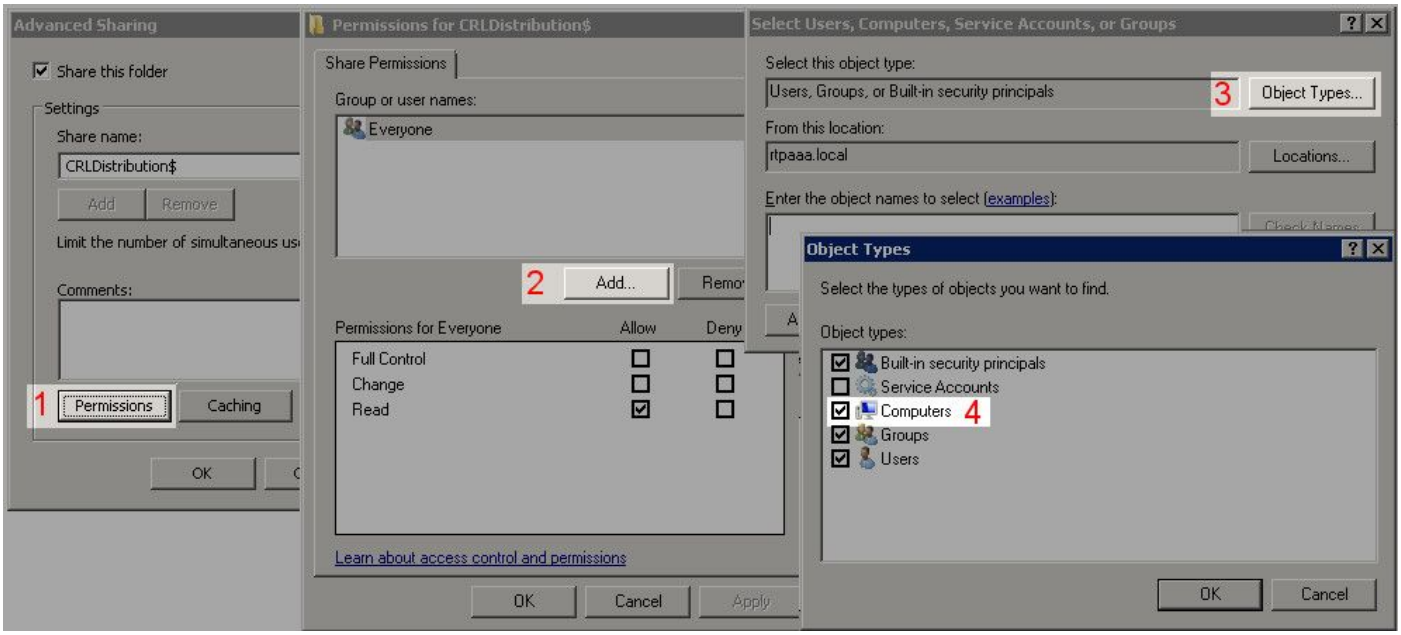
2. Para que la CA escriba los archivos CRL en la nueva carpeta, se debe habilitar el uso compartido. Haga clic con el botón derecho del ratón en la nueva carpeta, elija **Propiedades**, haga clic en la **ficha Compartir** y, a continuación, haga clic en **Uso compartido avanzado**.



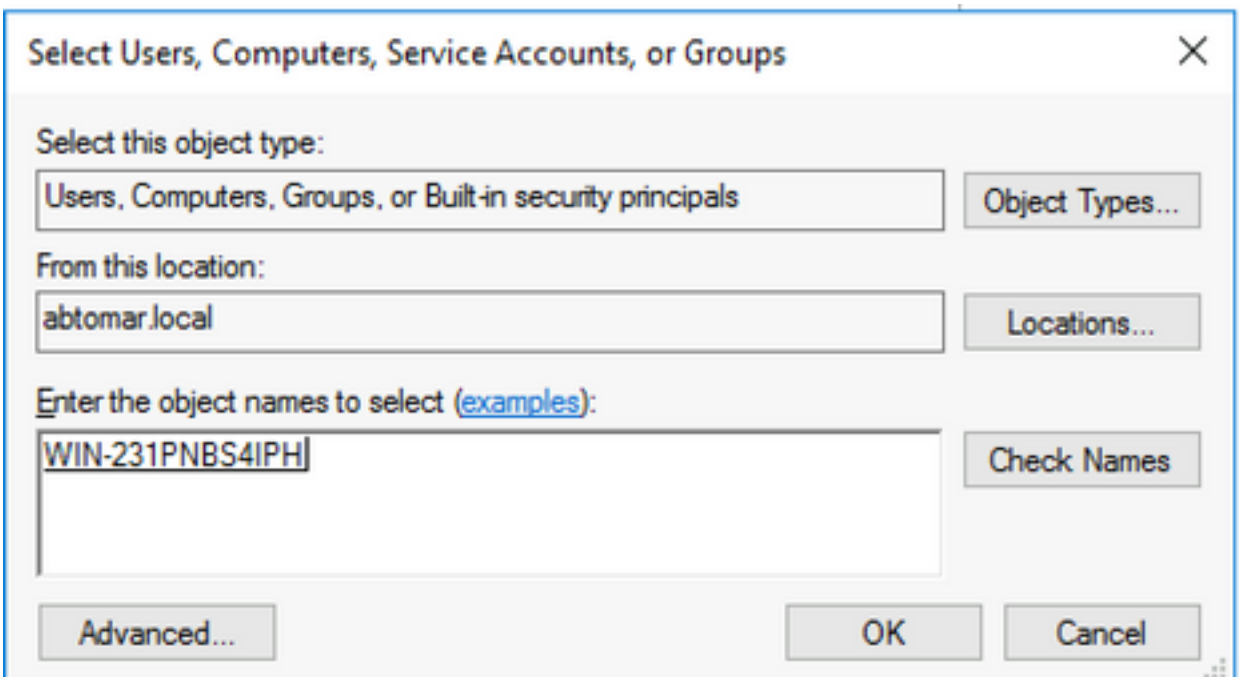
3. Para compartir la carpeta, marque la casilla de verificación **Compartir esta carpeta** y, a continuación, agregue un signo en dólares ($) al final del nombre del recurso compartido en el campo Nombre del recurso compartido para ocultar el recurso compartido.



4. Haga clic en **Permisos** (1), haga clic en **Agregar** (2), haga clic en **Tipos de objetos** (3) y active la casilla de verificación **Equipos** (4).

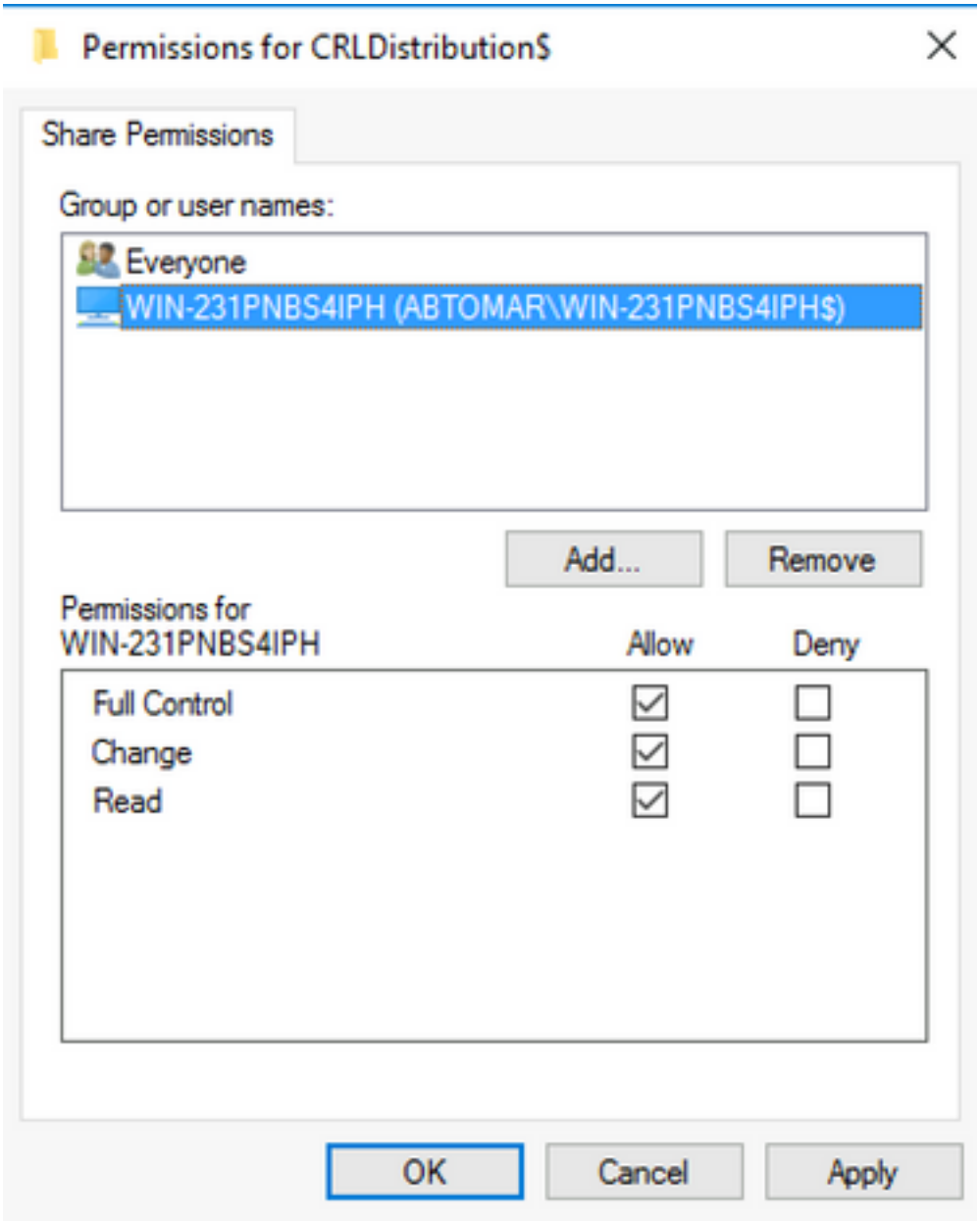


5. Para volver a la ventana Seleccionar usuarios, equipos, cuentas de servicio o grupos, haga clic en **Aceptar**. En el campo Introduzca los nombres de objeto que desea seleccionar, introduzca el nombre del equipo del servidor de la CA en este ejemplo: WIN0231PNBS4IPH y haga clic en **Comprobar nombres**.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

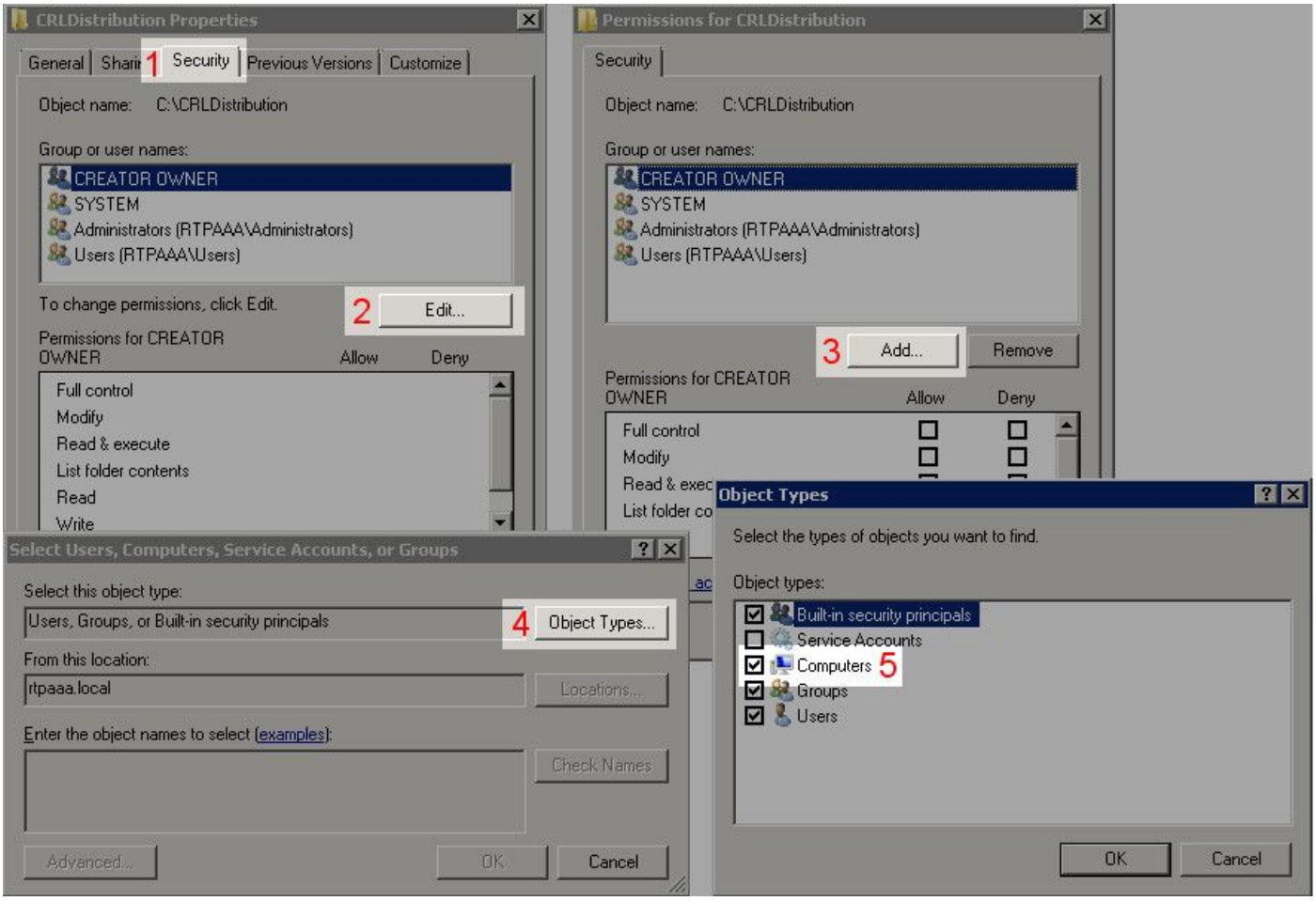


6. En el campo Group (Grupo) o user names (Nombres de usuario), elija el equipo CA. Marque **Allow** for Full Control (Permitir **el** control completo) para conceder acceso completo a la CA.

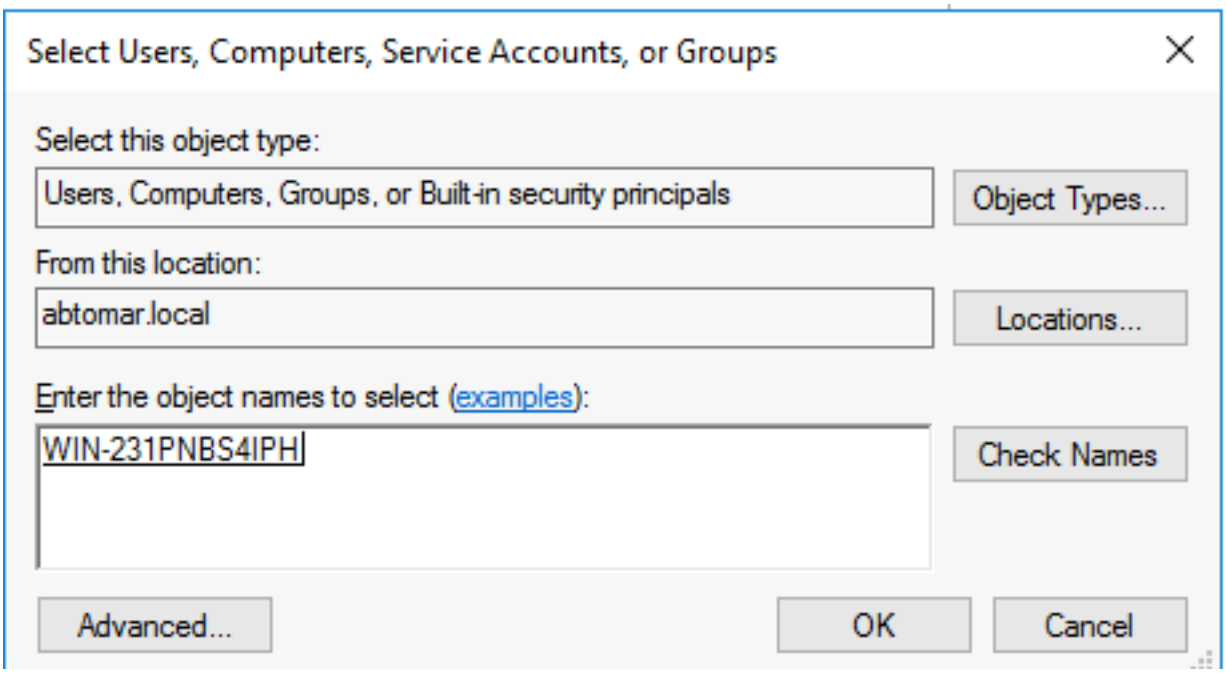
Click OK. Haga clic en **Aceptar** de nuevo para cerrar la ventana Uso compartido avanzado y volver a la ventana Propiedades.



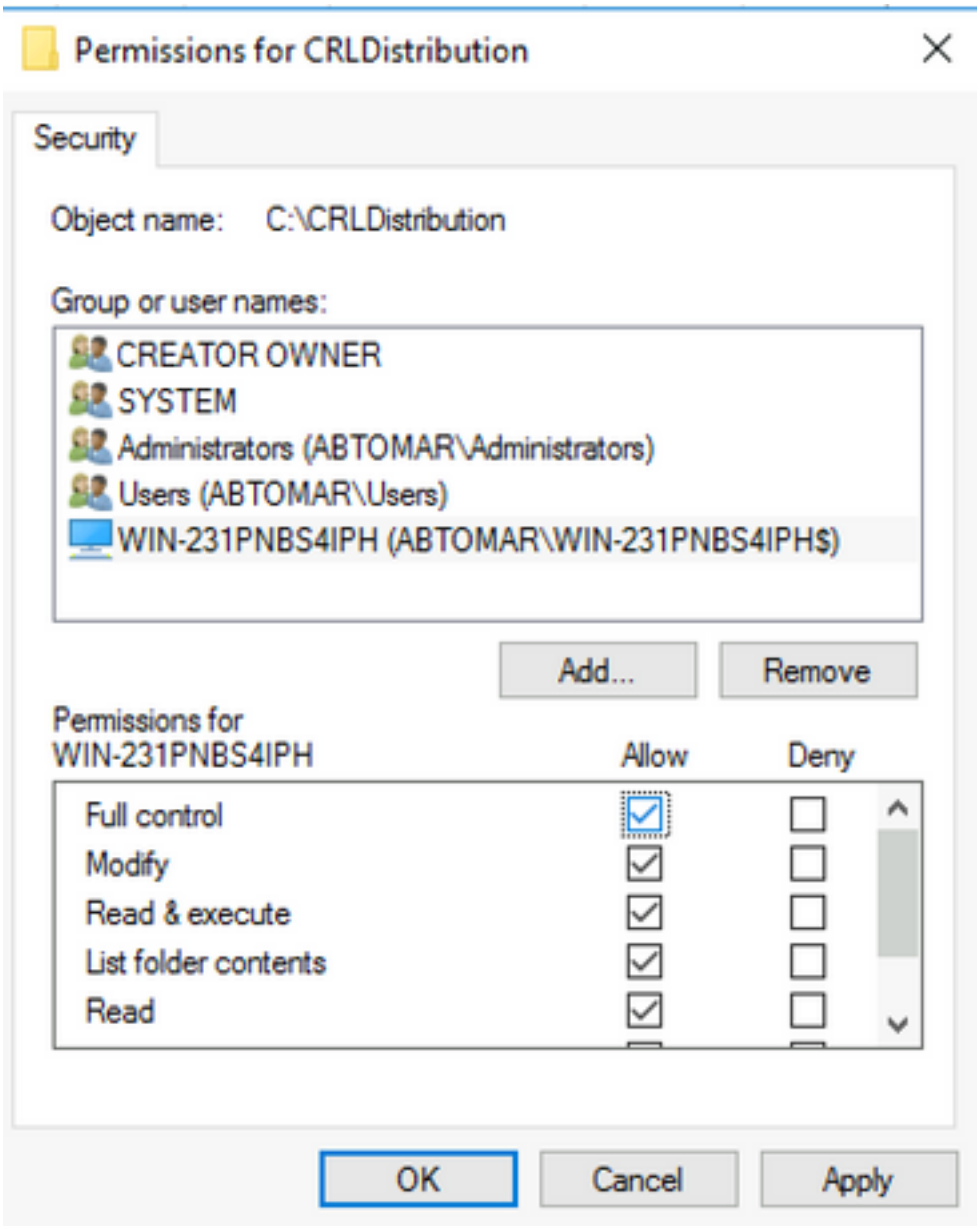
7. Para permitir que la CA escriba los archivos CRL en la nueva carpeta, configure los permisos de seguridad adecuados. Haga clic en la ficha Seguridad (1), haga clic en **Editar** (2), haga clic en **Agregar** (3), haga clic en **Tipos de objeto** (4) y marque la casilla de verificación **Equipos** (5).



8. En el campo Introduzca los nombres de objeto que desea seleccionar, introduzca el nombre del equipo del servidor de la CA y haga clic en **Comprobar nombres**. Si el nombre introducido es válido, el nombre se actualiza y aparece subrayado. Click OK.



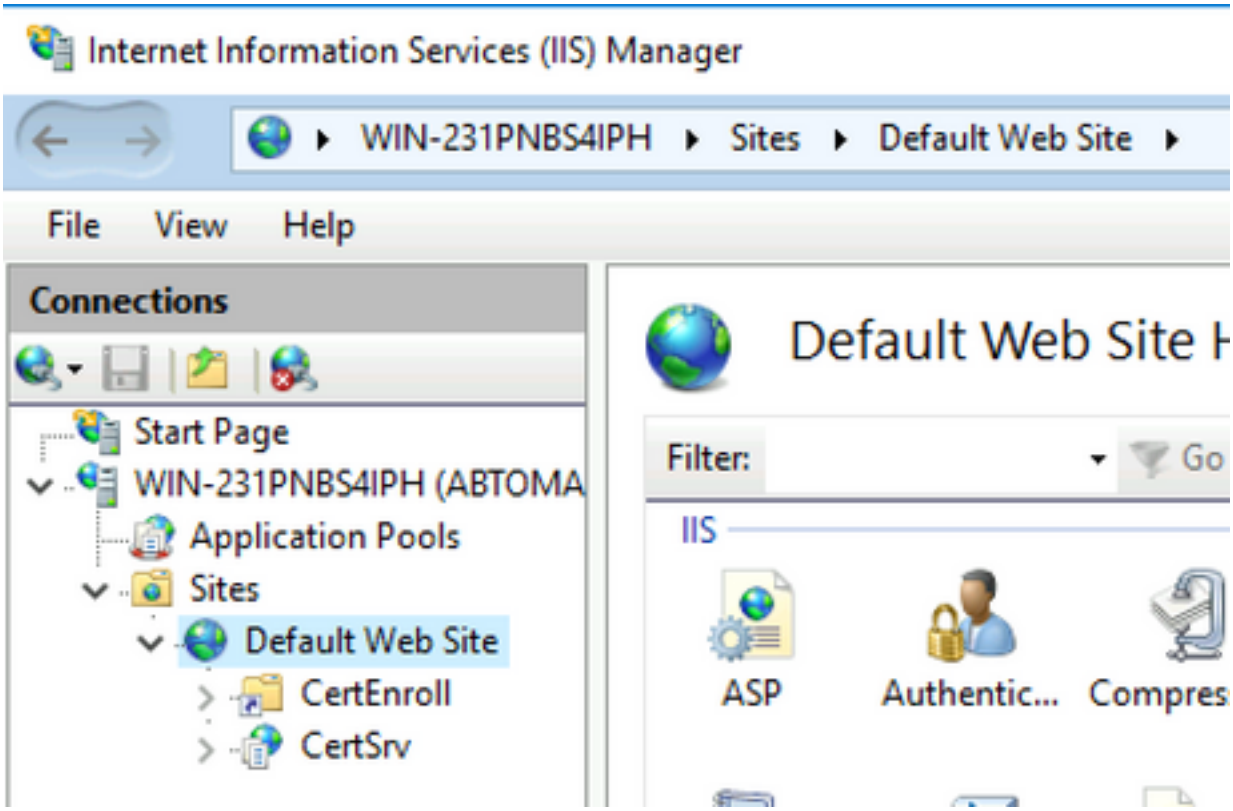
9. Elija el equipo CA en el campo Group o user names y luego marque **Allow** for Full control para conceder acceso completo a la CA. Haga clic en **Aceptar** y después haga clic en **Cerrar** para completar la tarea.



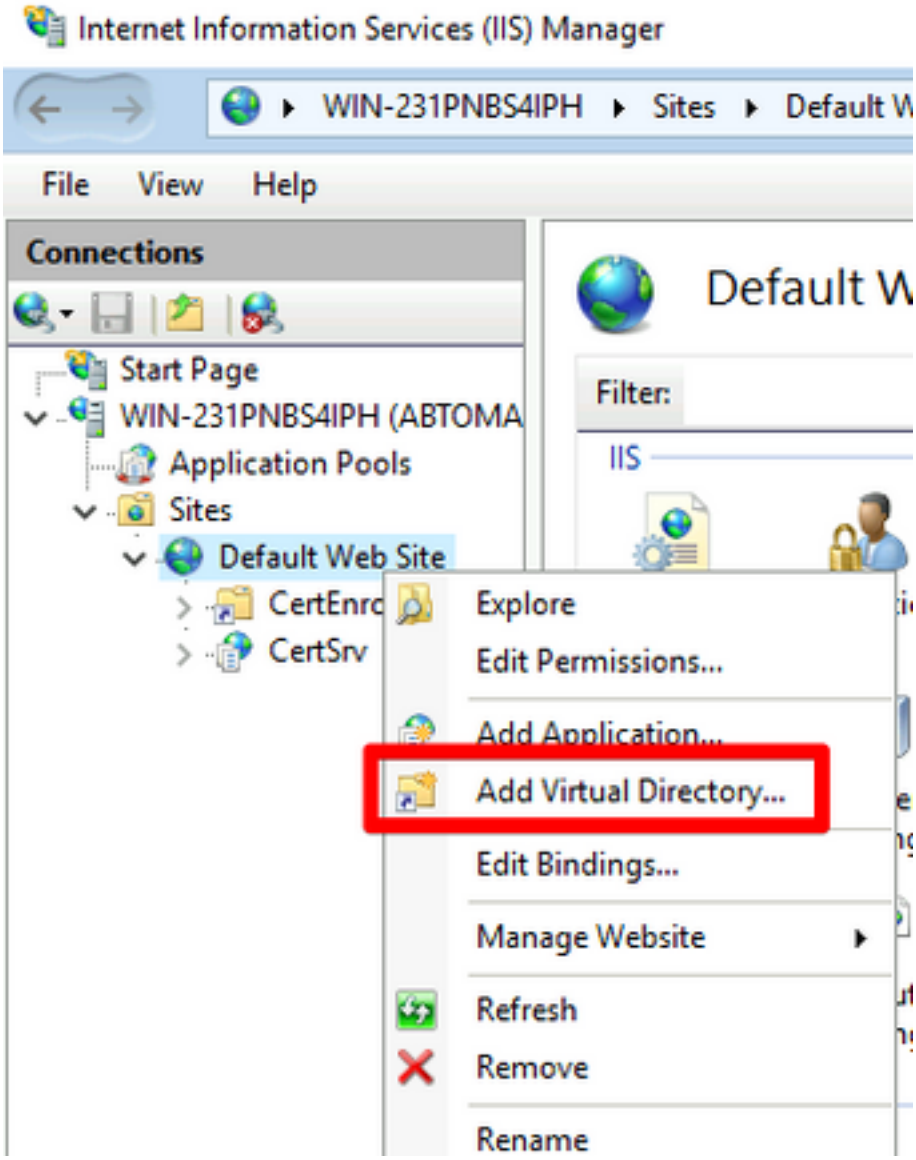
Crear un sitio en IIS para exponer el nuevo punto de distribución CRL

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

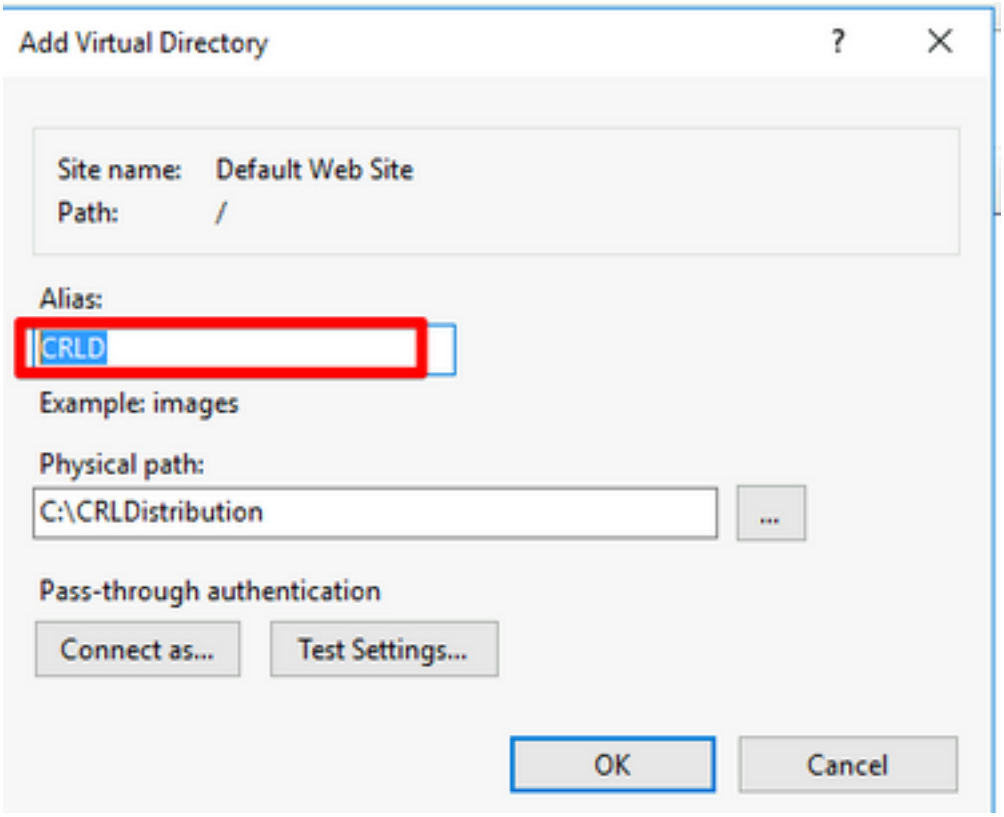
1. En la barra de tareas del servidor IIS, haga clic en **Inicio**. Elija **Administrative Tools > Internet Information Services (IIS) Manager**.
2. En el panel izquierdo (conocido como árbol de consola), expanda el nombre del servidor IIS y, a continuación, expanda **Sitios.**



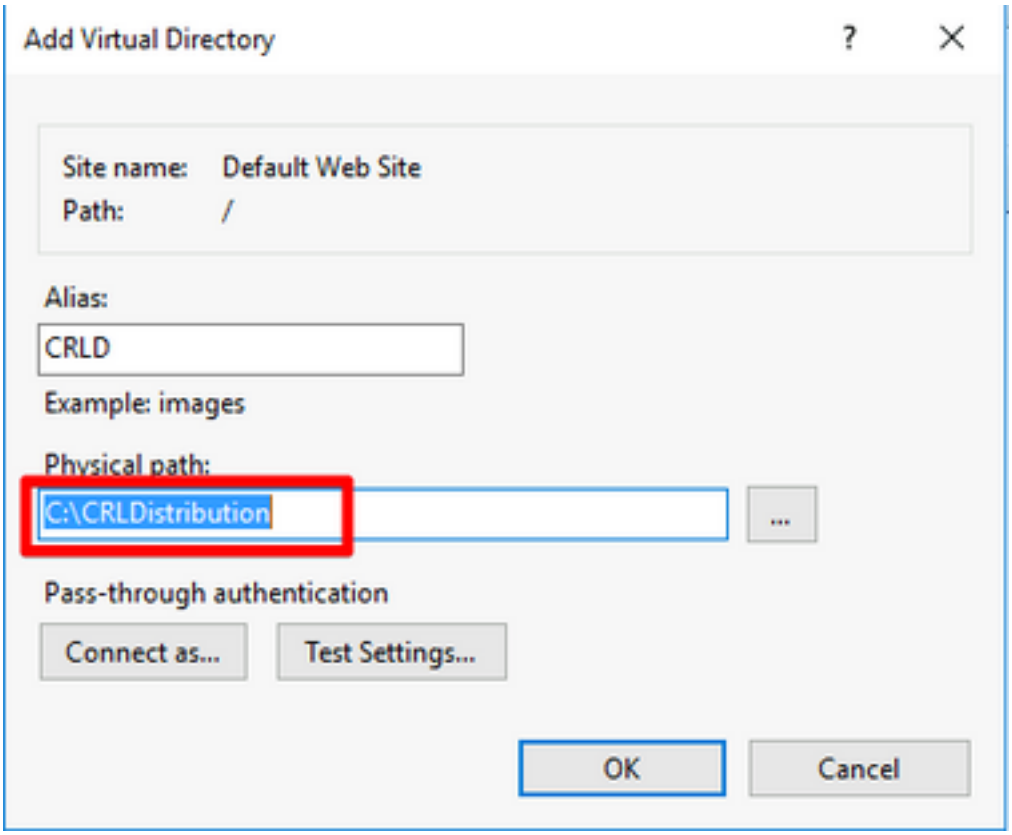
3. Haga clic con el botón derecho del mouse en **Sitio Web predeterminado** y elija **Agregar directorio virtual**, como se muestra en esta imagen.



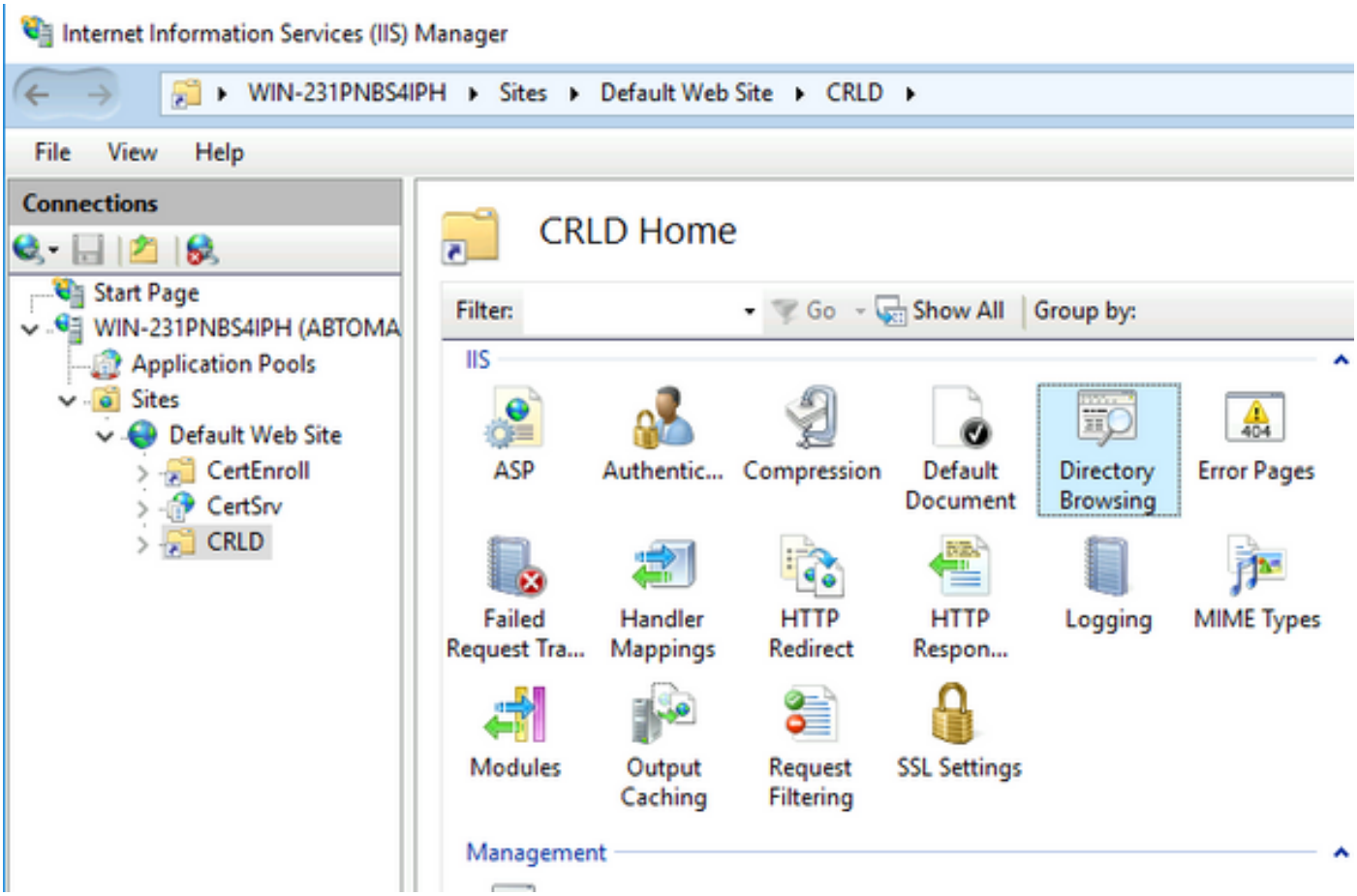
4. En el campo Alias, introduzca un nombre de sitio para el punto de distribución CRL. En este ejemplo, se ingresa CRLD.



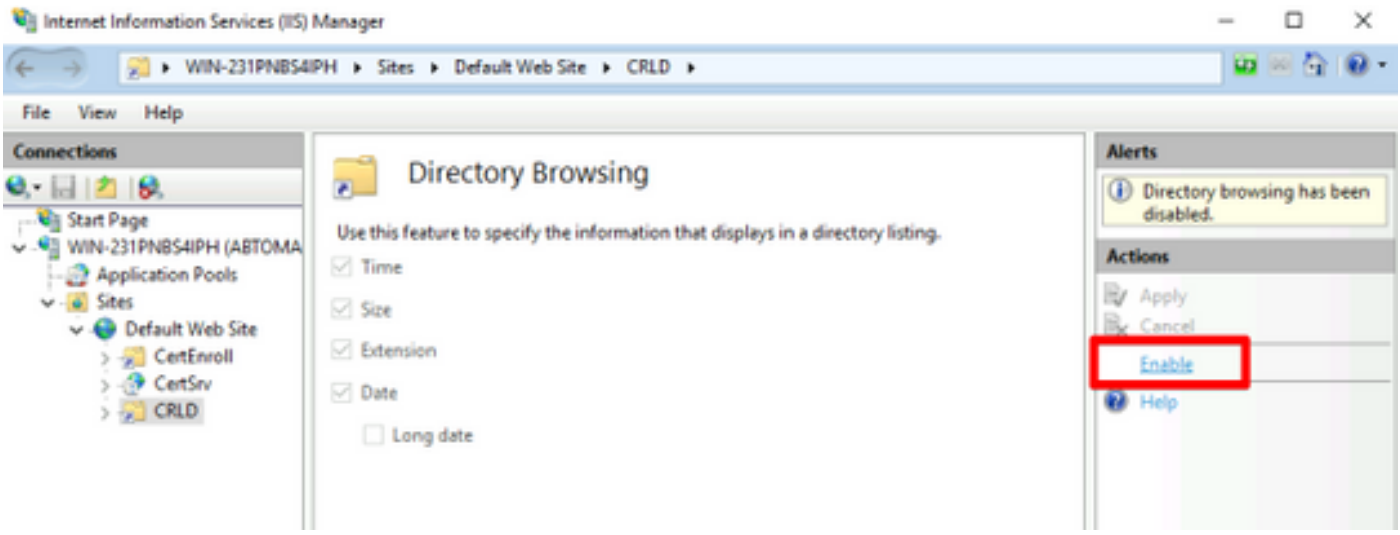
5. Haga clic en los puntos suspensivos (. . .) a la derecha del campo Ruta física y busque la carpeta creada en la sección 1. Seleccione la carpeta y haga clic en **Aceptar**. Haga clic en **Aceptar** para cerrar la ventana Agregar directorio virtual.



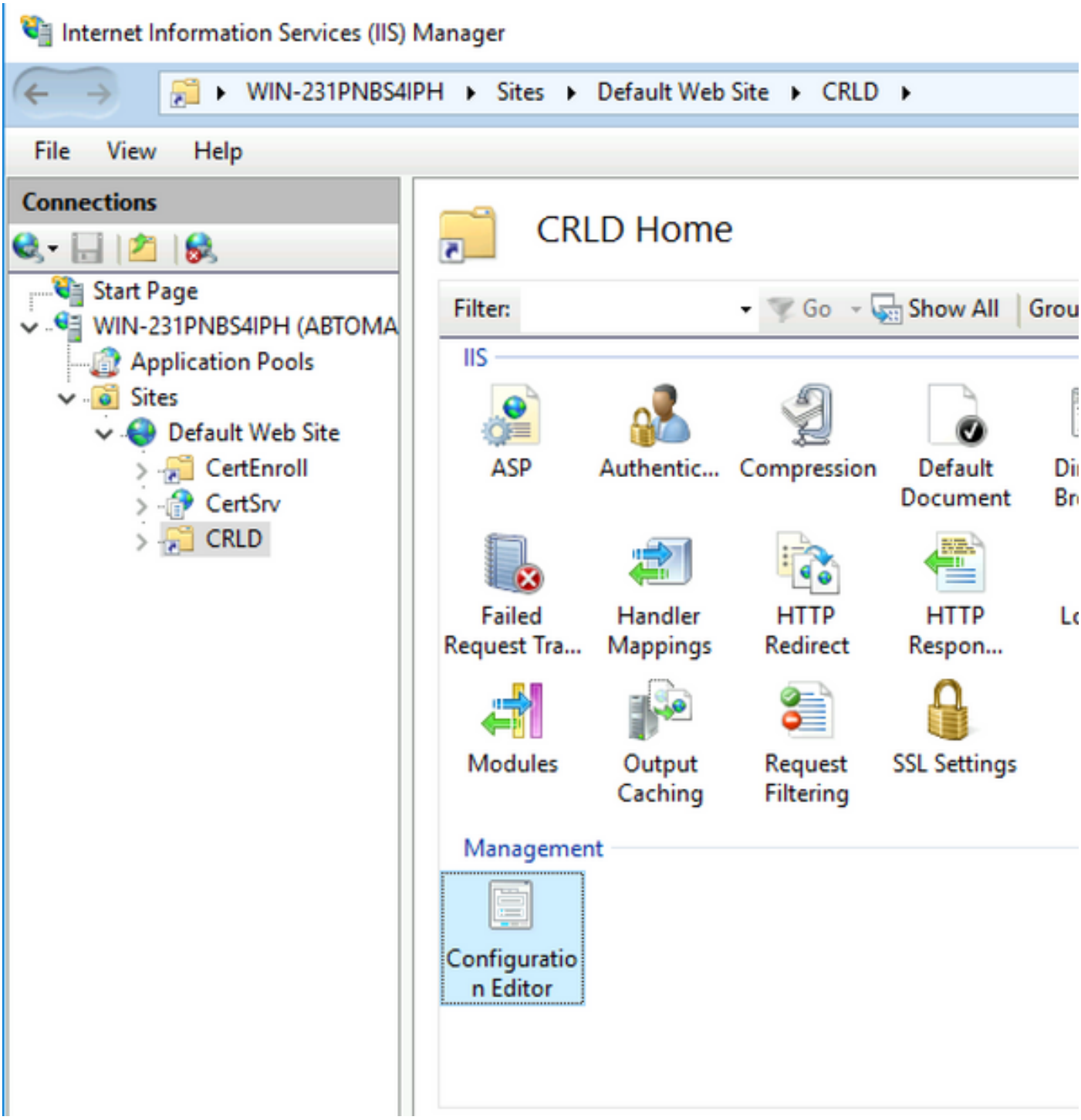
6. El nombre del sitio introducido en el paso 4 debe resaltarse en el panel izquierdo. Si no es así, selecciónelo ahora. En el panel central, haga doble clic en **Exploración del directorio**.



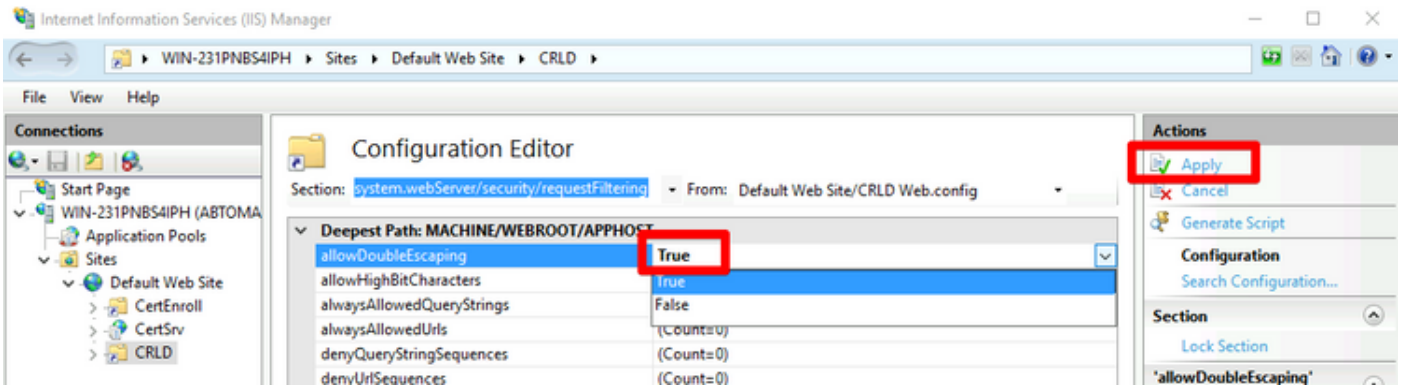
7. En el panel derecho, haga clic en **Enable** para habilitar la exploración del directorio.



8. En el panel izquierdo, vuelva a elegir el nombre del sitio. En el panel central, haga doble clic en **Editor de configuración**.



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

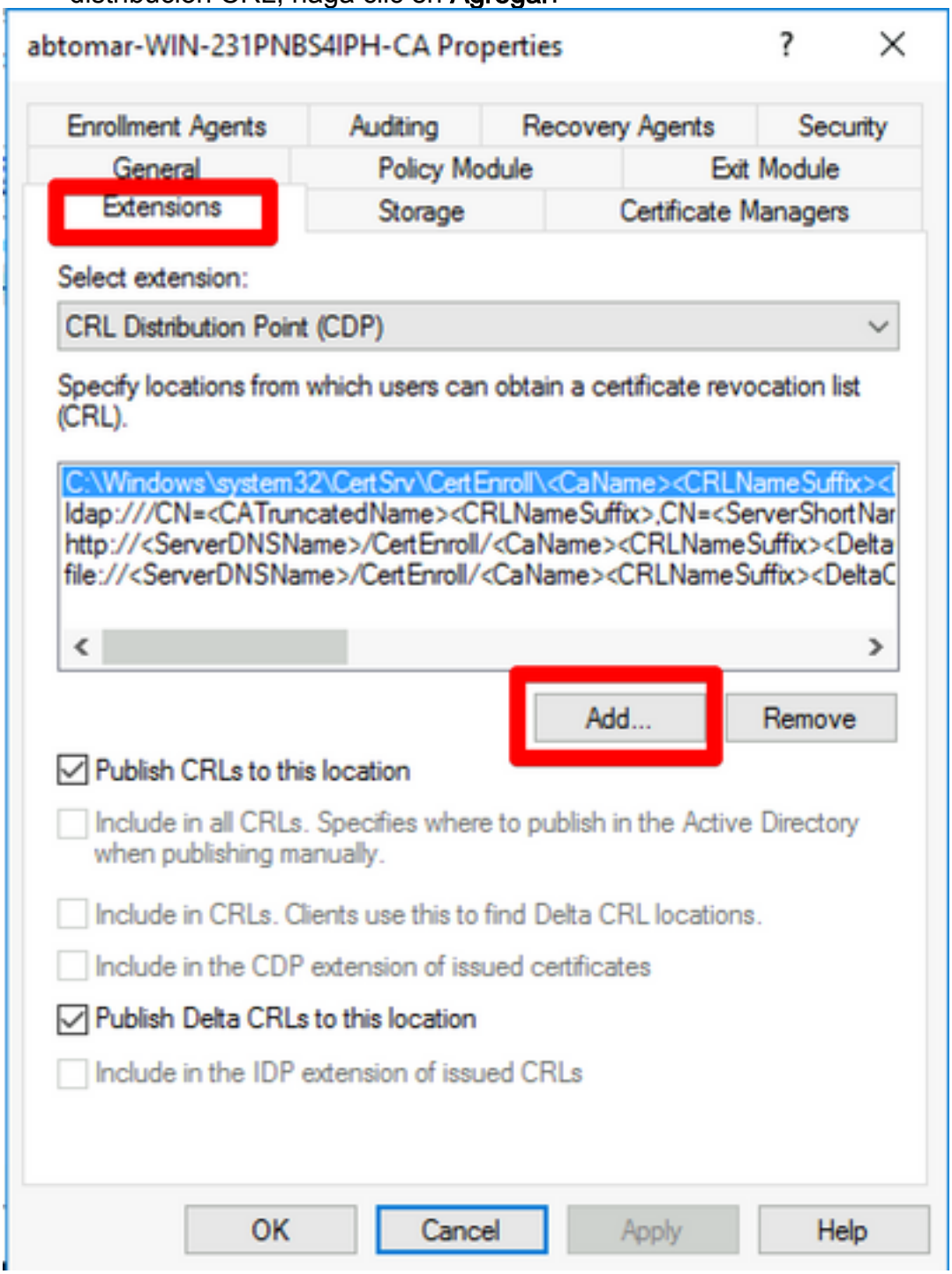


La carpeta ahora debe estar accesible a través de IIS.

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

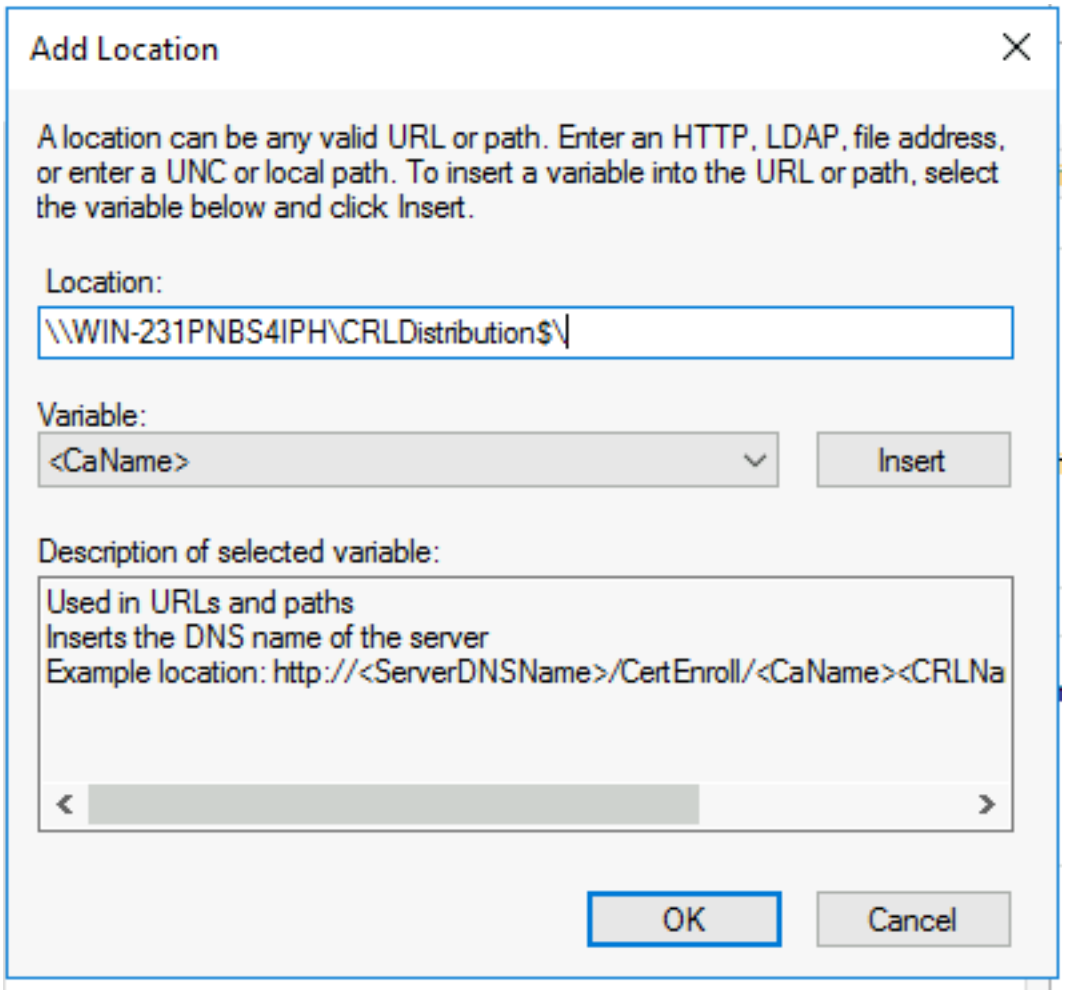
Ahora que se ha configurado una nueva carpeta para alojar los archivos CRL y la carpeta se ha visto expuesta en IIS, configure el servidor de Microsoft CA para publicar los archivos CRL en la nueva ubicación.

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

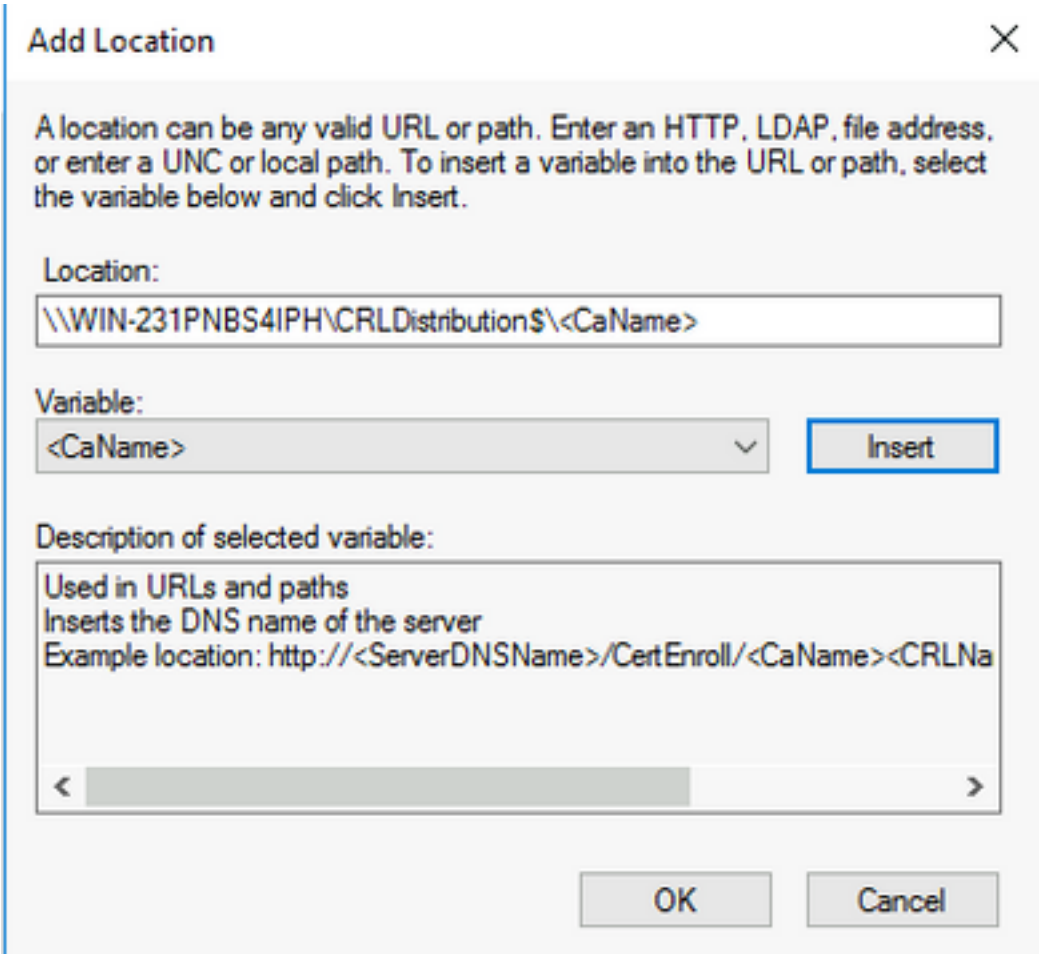


3. En el campo Ubicación, introduzca la ruta de acceso a la carpeta creada y compartida en la sección 1. En el ejemplo de la sección 1, la trayectoria es:

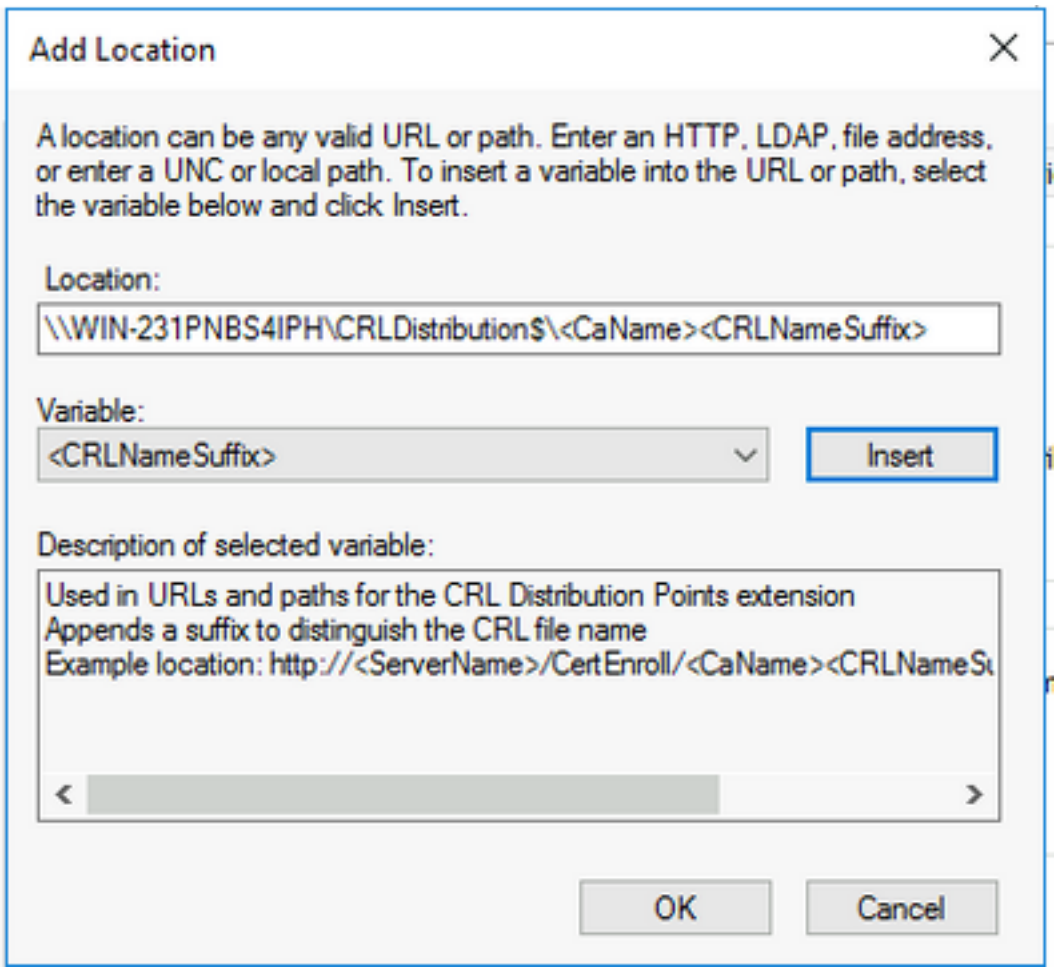
\\WIN-231PNBS4IPH\CRLDistribution$



4. Con el campo Location rellenado, elija **<CaName>** en la lista desplegable Variable y, a continuación, haga clic en **Insertar.**

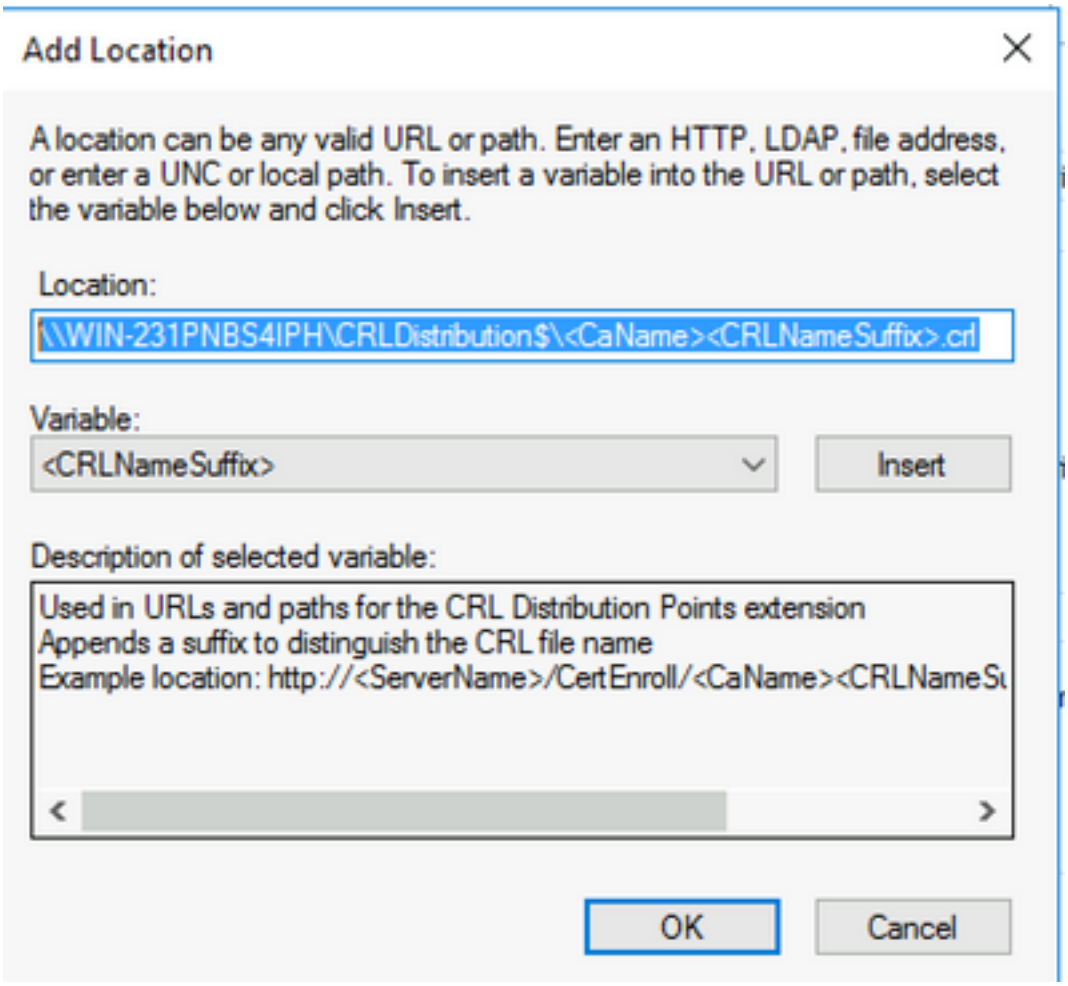


5. En la lista desplegable Variable, elija **<CRLNameSufijo>** y luego haga clic en **Insertar**.



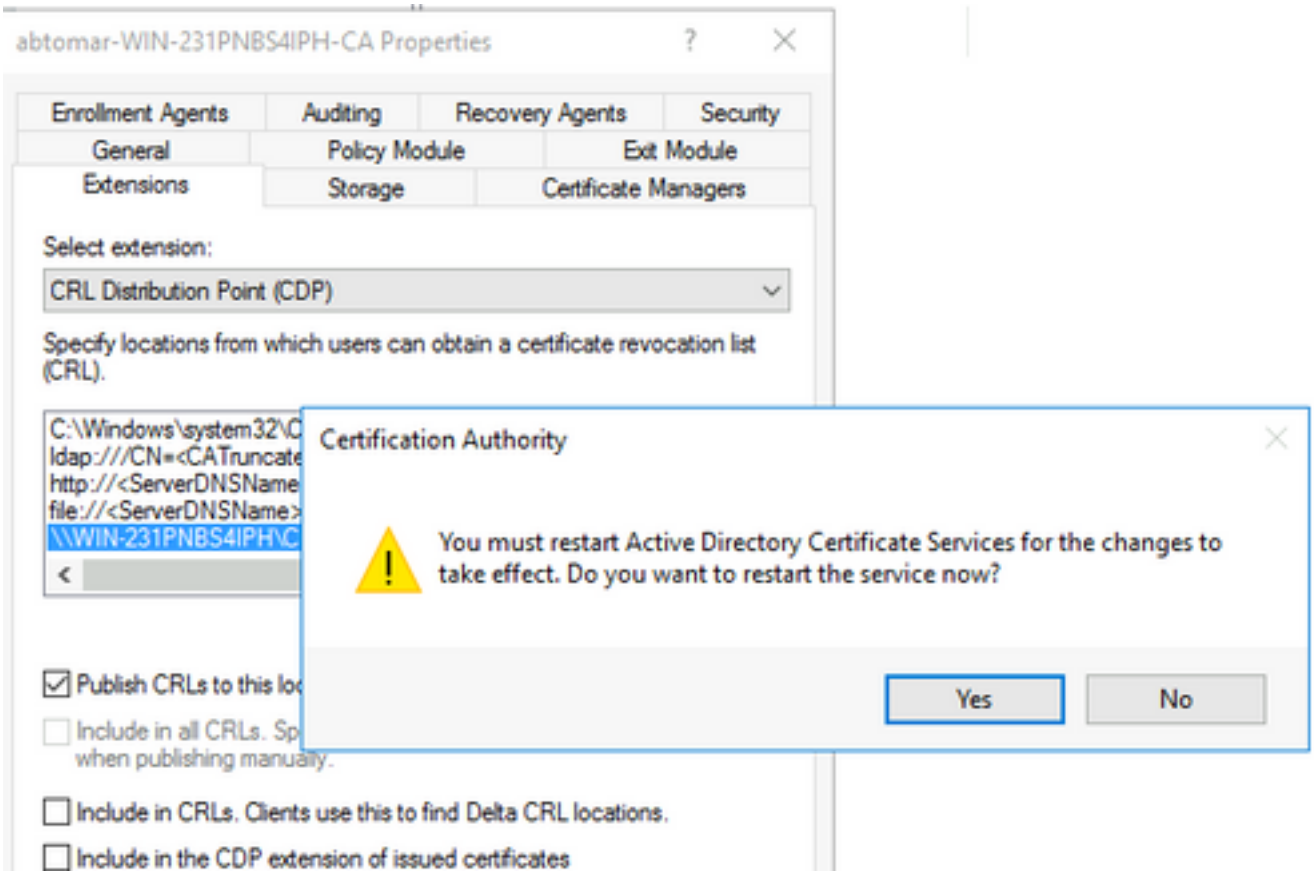
6. En el campo Location (Ubicación), añada **.crl** al final de la ruta. En este ejemplo, la Ubicación es:

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

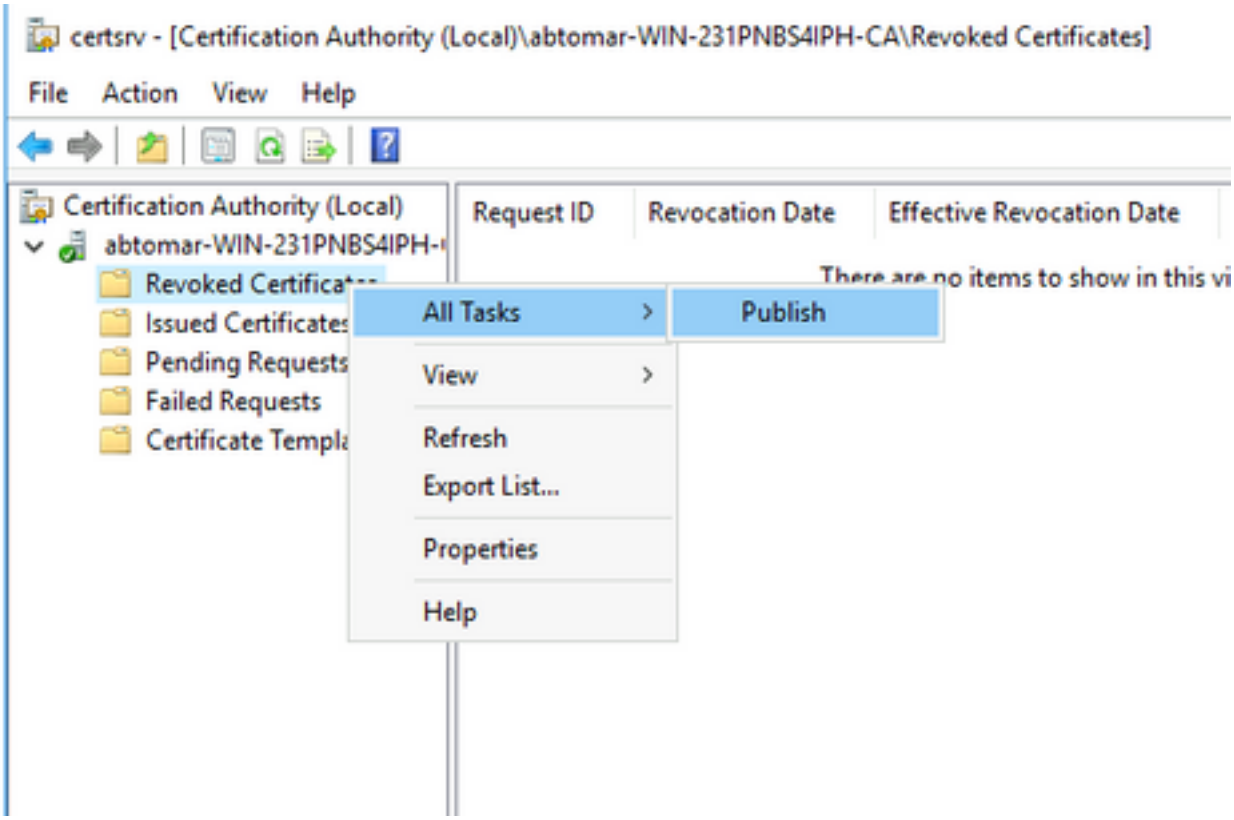


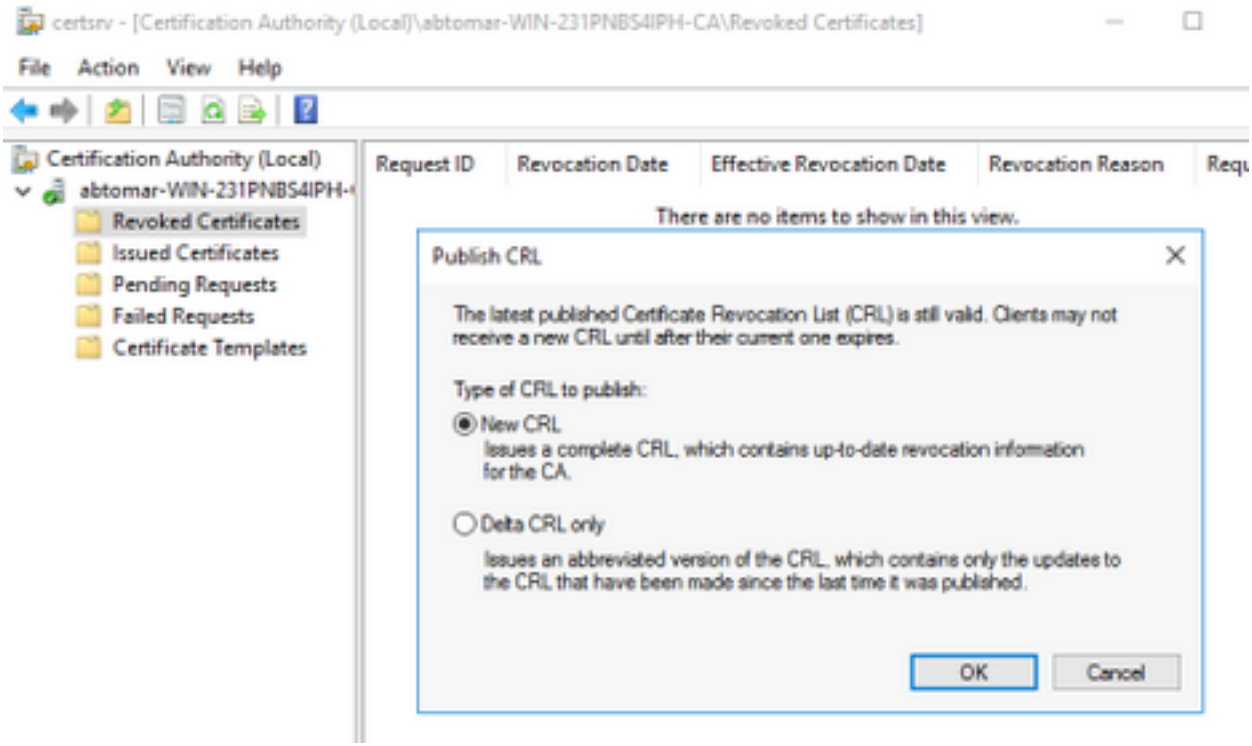
7. Haga clic en **Aceptar** para volver a la ficha Extensiones. Marque la casilla de verificación **Publicar CRL en esta ubicación** y, a continuación, haga clic en **Aceptar** para cerrar la ventana Propiedades.

Aparece un mensaje para obtener permiso para reiniciar Servicios de certificados de Active Directory. Haga clic en Sí



8. En el panel izquierdo, haga clic con el botón derecho en **Certificados revocados**. Elija **Todas las tareas > Publicar**. Asegúrese de que se ha seleccionado New CRL y, a continuación, haga clic en **Aceptar.**





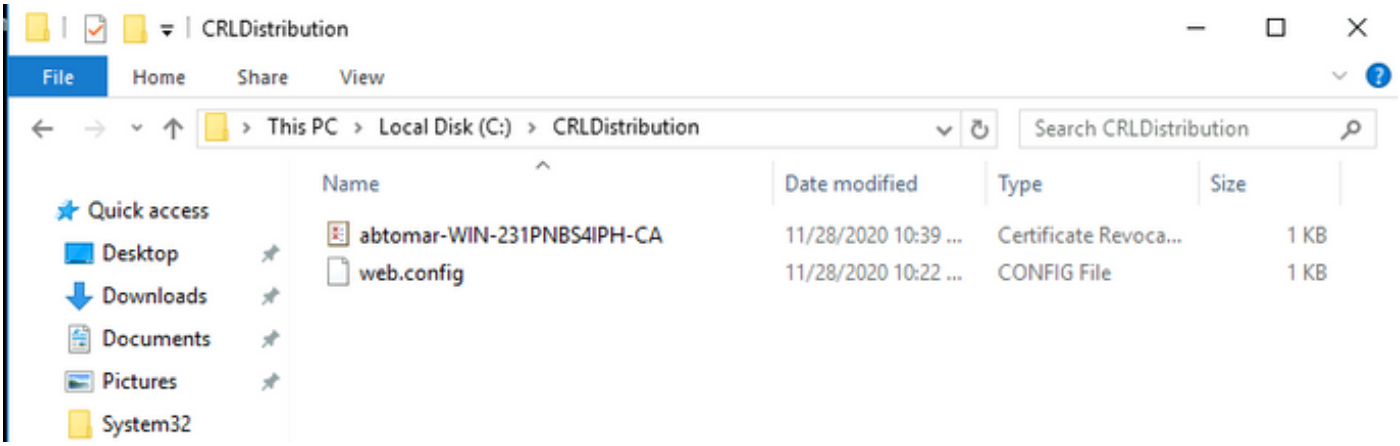
El servidor de Microsoft CA debe crear un nuevo archivo .crl en la carpeta creada en la sección 1. Si el nuevo archivo CRL se crea correctamente, no habrá diálogo después de hacer clic en Aceptar. Si se devuelve un error con respecto a la nueva carpeta de punto de distribución, repita cuidadosamente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

Verifique que el archivo CRL exista y que esté accesible a través de IIS

Verifique que los nuevos archivos CRL existan y que sean accesibles 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 presente con el formulario **<CANAME>.crl** donde <CANAME> 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 en la red (idealmente en la misma red que el nodo de administración principal de ISE), abra un explorador web y vaya a http://<SERVER>/<CRLSITE> donde <SERVER> es el nombre de servidor del servidor IIS configurado en la sección 2 y <CRLSITE> es el nombre del sitio elegido para el punto de distribución en la sección 2. En este ejemplo, la URL es:

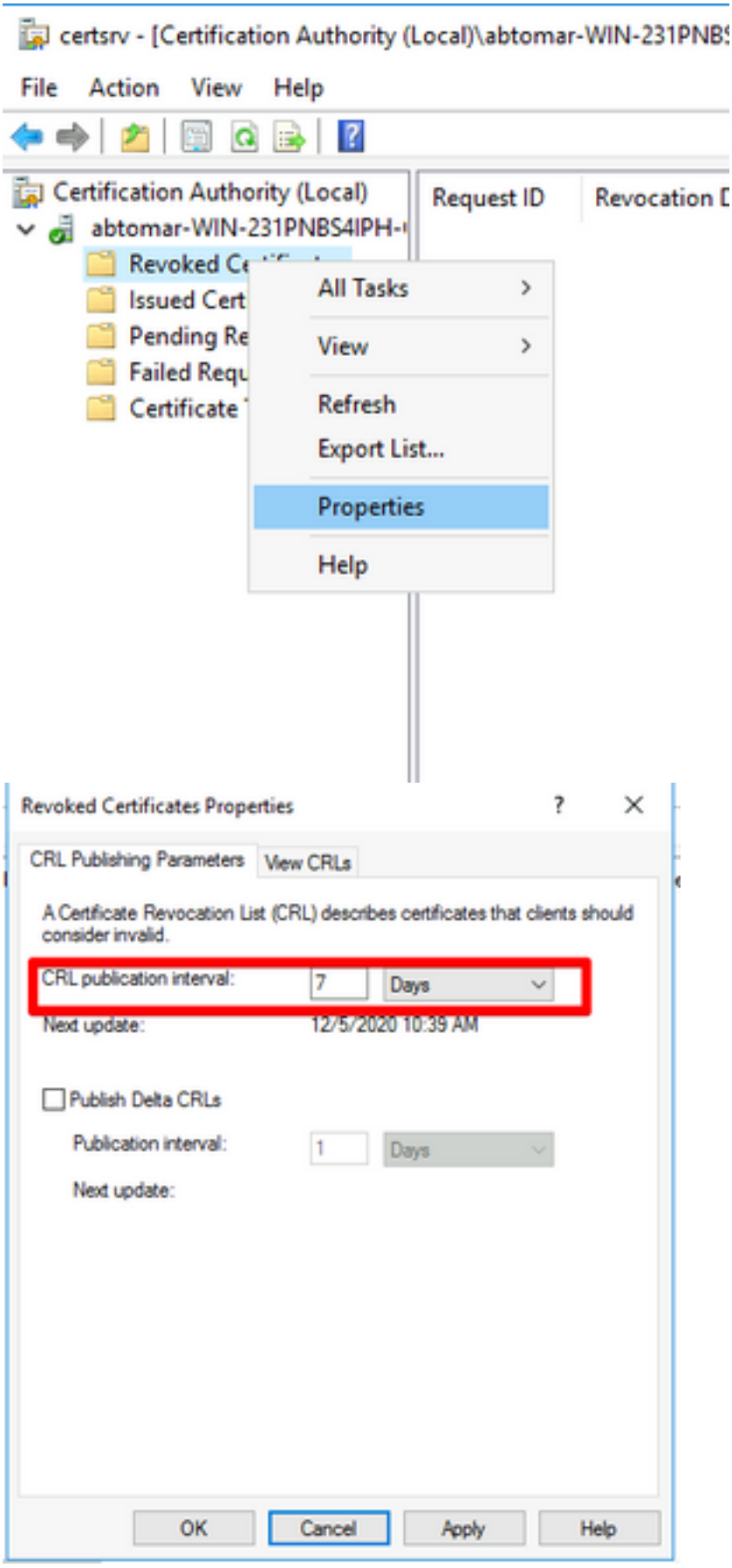
http://win-231pnbs4iph/CRLD

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

Configuración de ISE para utilizar el nuevo punto de distribución 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) son de 1 hora a 411 años, ambos inclusive. El valor predeterminado es 1 semana. Una vez determinado el intervalo adecuado para su entorno, establezca el intervalo con las siguientes instrucciones:

1. En la barra de tareas del servidor de la CA, haga clic en **Inicio**. Elija **Administrative Tools > Certificate Authority**.
2. En el panel izquierdo, expanda la CA. Haga clic con el botón derecho en la carpeta **Certificados revocados** y elija **Propiedades.**
3. En los campos Intervalo de publicación de CRL, introduzca el número necesario y elija el período de tiempo. Haga clic en **Aceptar** para cerrar la ventana y aplicar el cambio. En este ejemplo, se configura un intervalo de publicación de 7 días.



4. Ingrese el **comando certutil -getreg CA\Clock*** 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 **comando certutil -getreg CA\CRLov*** para verificar si CRLOverlapPeriod se ha establecido manualmente. De forma predeterminada, el valor 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 comando **certutil -getreg CA\CRLpe*** 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 periodo de gracia de CRL de la siguiente manera:

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

Otros: SOBRELAP = (CRLPeriod / 10), en minutos

b. Si SOBRELAP > 720, entonces OVERLAP = 720

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

d. Si OVERLAP > CRLPeriod, en minutos, OVERLAP = CRLPeriod en minutos

e. Período de gracia = SOBRELAP + ClockSkewMinutos

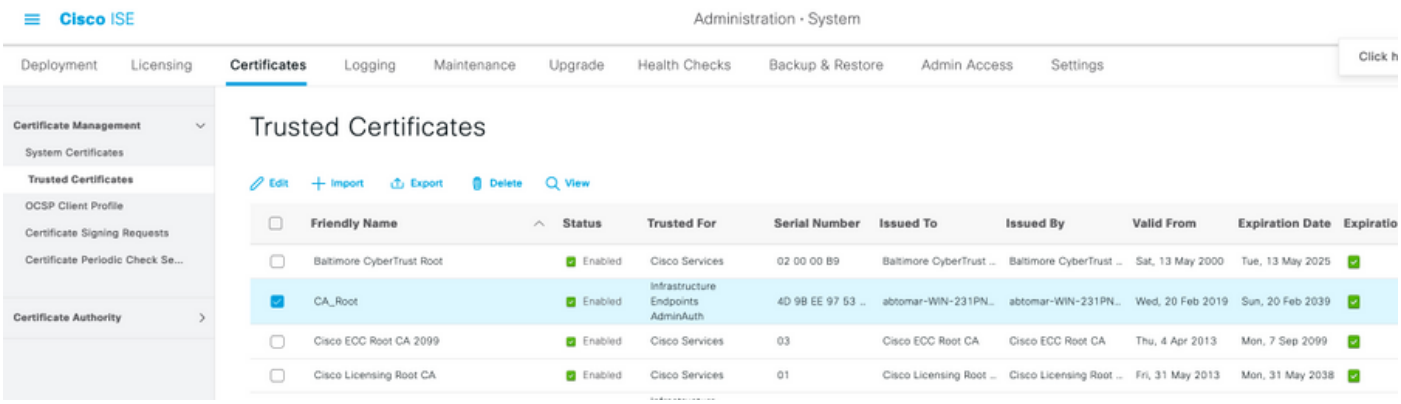
```
Example:

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 que la CA publica la siguiente CRL y cuando 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, seleccione **Certificado de confianza**



9. Active la casilla de verificación junto al certificado de CA para el que desea configurar las CRL. Haga clic en **Editar**.

10. Cerca de la parte inferior de la ventana, marque la casilla de verificación **Descargar CRL**.

11. En el campo URL de distribución de CRL, introduzca la ruta de acceso al punto de distribución de CRL, que incluye el archivo .crl, creado en la sección 2. En este ejemplo, la URL es:

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

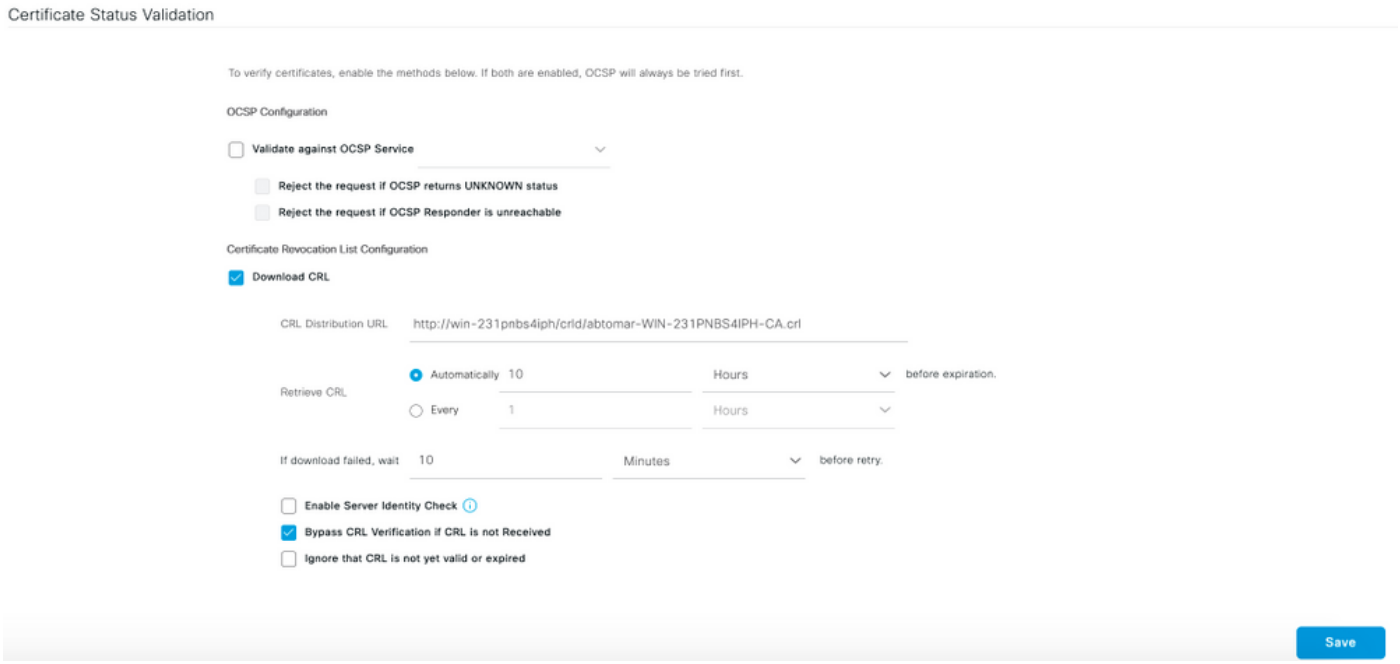
12. ISE se puede configurar para recuperar la CRL a intervalos regulares o en función de la caducidad (que, en general, es también un intervalo normal). Cuando el intervalo de publicación de CRL es estático, se obtienen actualizaciones de CRL más oportunas cuando se utiliza la segunda opción. Haga clic en el botón de opción **Automáticamente**.

13. Establezca el valor para la recuperación en un valor inferior al período de gracia calculado en el paso 7. Si el valor establecido es más largo que el 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. Configure el intervalo de reintento según corresponda para 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 casilla de verificación **Omitir verificación CRL si no se recibe CRL** para permitir que la autenticación basada en certificados continúe normalmente (y sin una verificación CRL) si ISE no pudo recuperar la CRL para esta CA en su último intento de descarga. Si esta casilla de verificación no está marcada, toda la autenticación basada en certificados con certificados emitidos por esta CA fallará si no se puede recuperar la CRL.

16. Active la casilla de verificación **Ignorar que CRL aún no es válida o ha caducado** para permitir que ISE utilice archivos CRL caducados (o aún no válidos) como si fueran válidos. Si esta casilla de verificación no está marcada, ISE considera que una CRL no es válida antes de su Fecha de entrada en vigor y después de sus horas de actualización siguiente. Haga clic en **Guardar** para completar la configuración.



Información interna de Cisco

1. Microsoft. "Configure un punto de distribución CRL para los certificados". http://technet.microsoft.com/en-us/library/ee649260%28v=ws.10%29.aspx, 7 oct. 2009 [18 dic. 2012]

2. Microsoft. "Publica manualmente la lista de revocación de certificados". http://technet.microsoft.com/en-us/library/cc778151%28v=ws.10%29.aspx, 21 ene. 2005 [18 dic. 2012]

3. Microsoft. "Configure los períodos de superposición de CRL y CRL Delta". http://technet.microsoft.com/en-us/library/cc731104.aspx, 11 abr. 2011 [18 dic. 2012]

4. MS2065 [MSFT]. "Cómo se calculan los datos de Fecha de entrada en vigor (sesupdate), NextUpdate y NextCRLPublish". http://blogs.technet.com/b/pki/archive/2008/06/05/how-effectivedate-thisupdate-nextupdate-and-nextcrlpublish-are-calculated.aspx, 4 jun. 2008 [18 dic. 2012]