Publique los Lista de revocación de certificados (CRL) para ISE en un ejemplo de configuración del servidor de Microsoft CA

Contenido

Introducción

Este documento describe la configuración de un servidor de Microsoft Certificate Authority (CA) que dirija los Servicios de Internet Information Server (IIS) para publicar las actualizaciones del Listas de revocación de certificados (CRL). También explica cómo configurar el Cisco Identity Services Engine (ISE) (versiones 1.1 y más adelante) para extraer las actualizaciones para el uso en la validación de certificado. ISE se puede configurar para extraer los CRL para los diversos certificados raíz CA que utiliza en la validación de certificado.

prerrequisitos

Requisitos

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 1.1.2.145 del Cisco Identity Services Engine
- ® 2008 R2 del servidor del ® de Microsoft Windows

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 la red está funcionando, asegúrese de haber comprendido el impacto que puede tener cualquier comando.

Convenciones

Consulte Convenciones de Consejos Técnicos de Cisco para obtener más información sobre las convenciones sobre documentos.

Configurar

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

Nota: Utilice la herramienta de búsqueda de comandos (clientes registrados solamente) para obtener más información sobre los comandos usados en esta sección.

Configuraciones

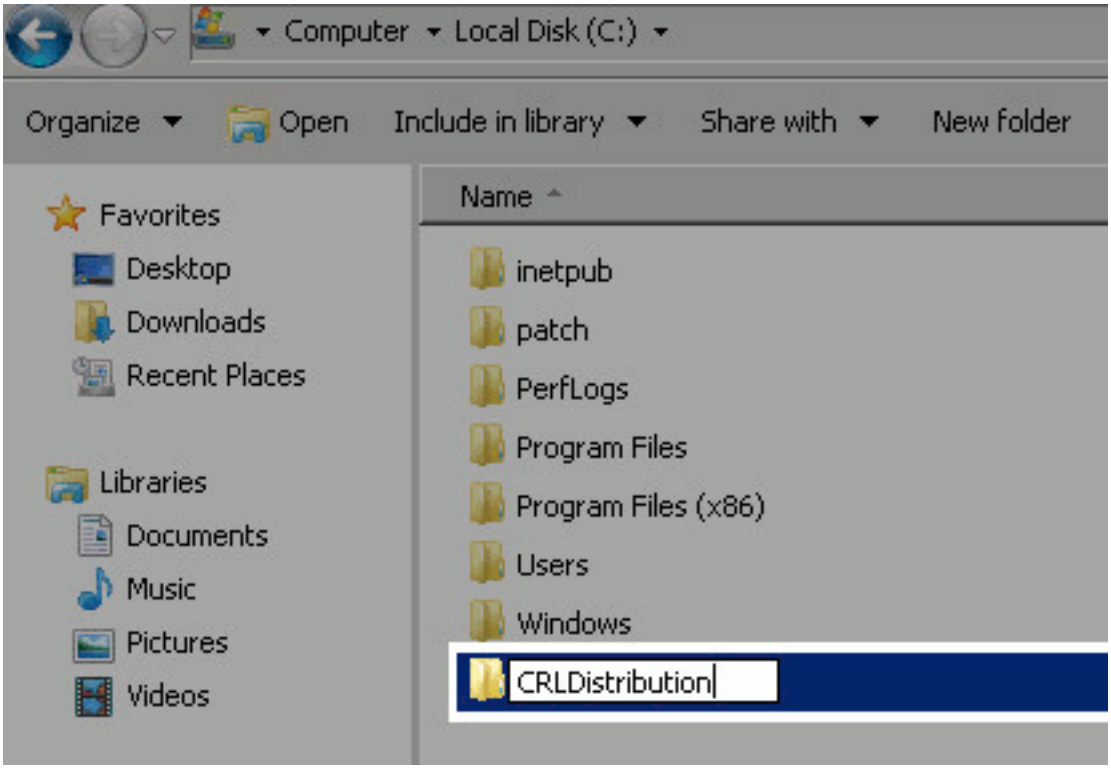
Este documento utiliza estas configuraciones:

- La sección 1. crea y configura una carpeta en el CA para contener los ficheros CRL
- La sección 2. crea un sitio en el IIS para exponer la nueva punta de la distribución CRL
- La sección 3. configura el servidor de Microsoft CA para publicar los ficheros CRL a la punta de la distribución
- La sección 4. verifica que el fichero CRL exista y que sea accesible vía el IIS
- La sección 5. configura ISE para utilizar la nueva punta de la distribución CRL

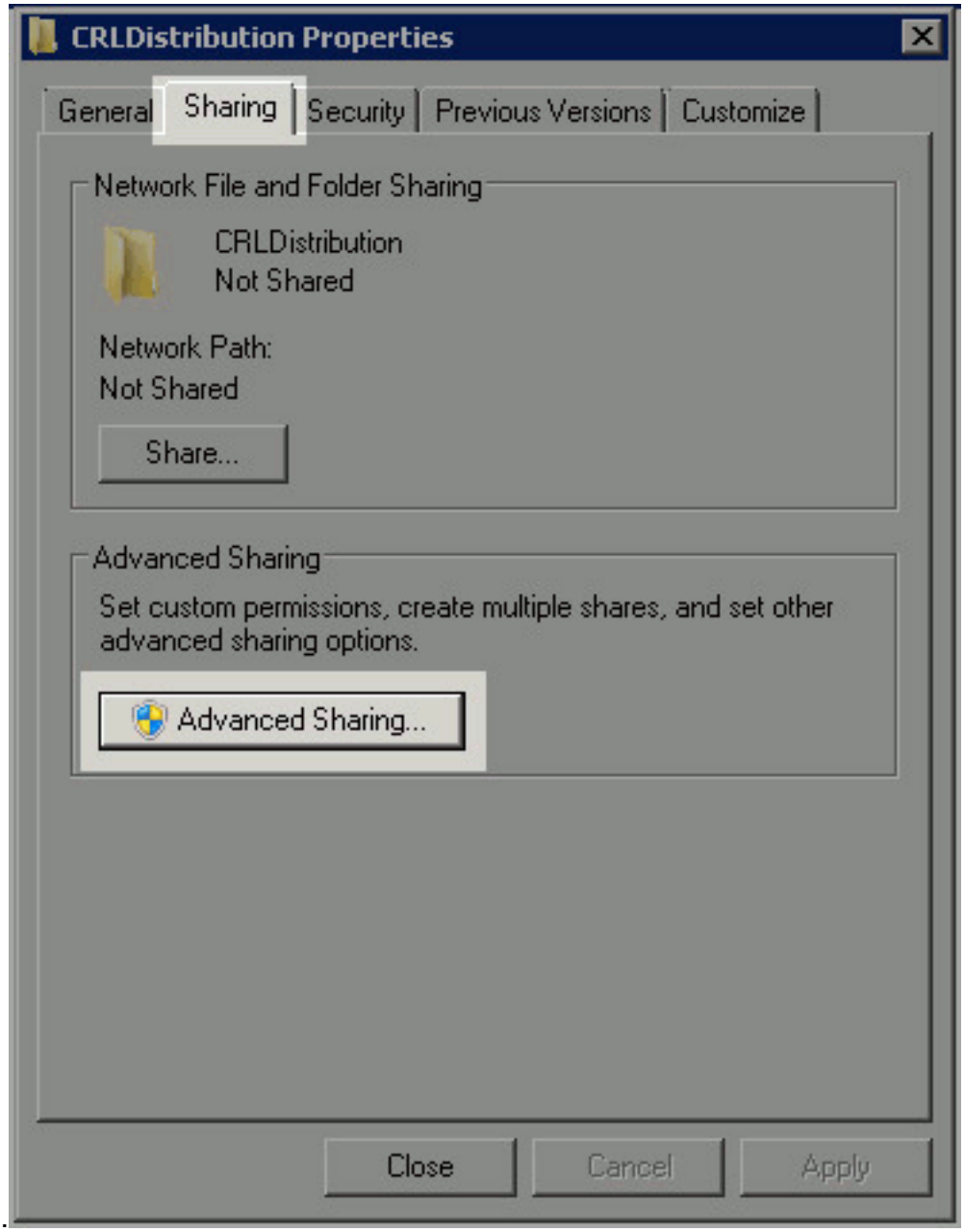
La sección 1. crea y configura una carpeta en el CA para contener los ficheros CRL

La primera tarea es configurar una ubicación en el servidor CA para salvar los ficheros CRL. Por abandono, el servidor de Microsoft CA publica los ficheros a C:\Windows\system32\CertSrv\CertEnroll\. Bastante que esta carpeta del sistema, crean una nueva carpeta para los ficheros.

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.

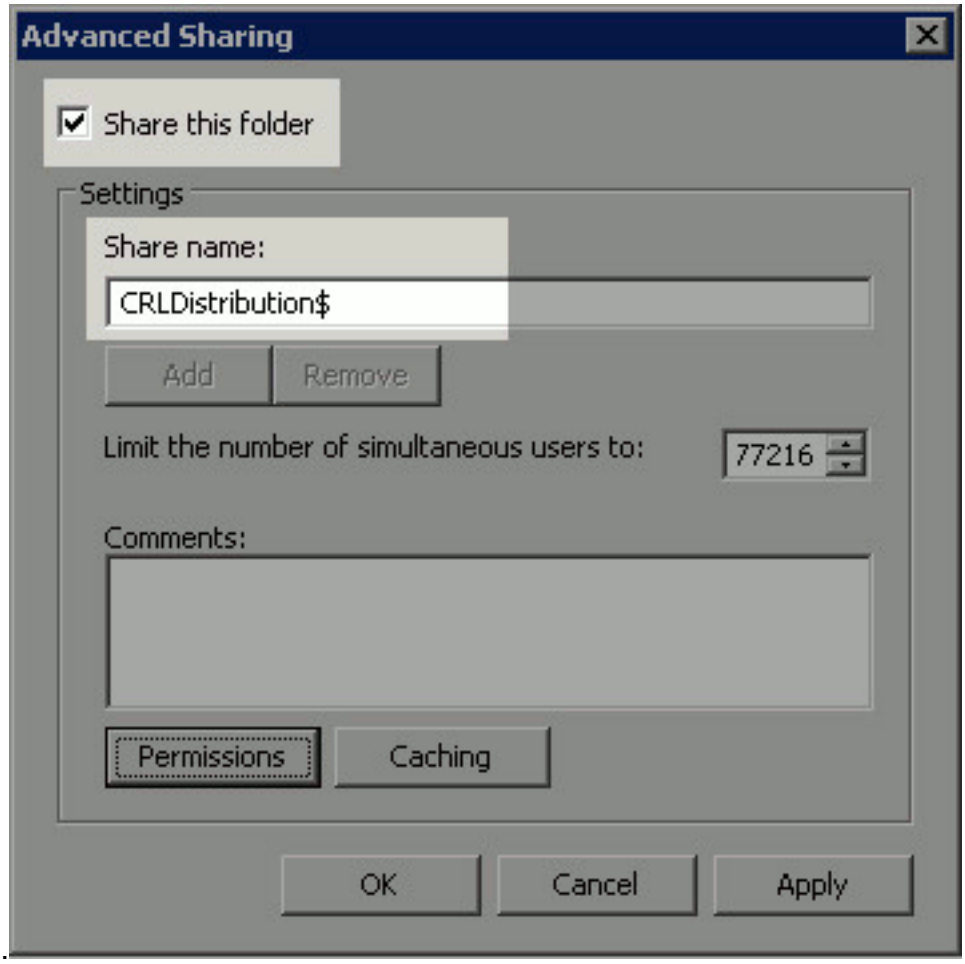


2. Para que el CA escriba los ficheros CRL a la nueva carpeta, compartiendo debe ser activado. Haga clic derecho la nueva carpeta, elija las **propiedades**, haga clic la tabulación de **distribución**, y después haga clic la **distribución**



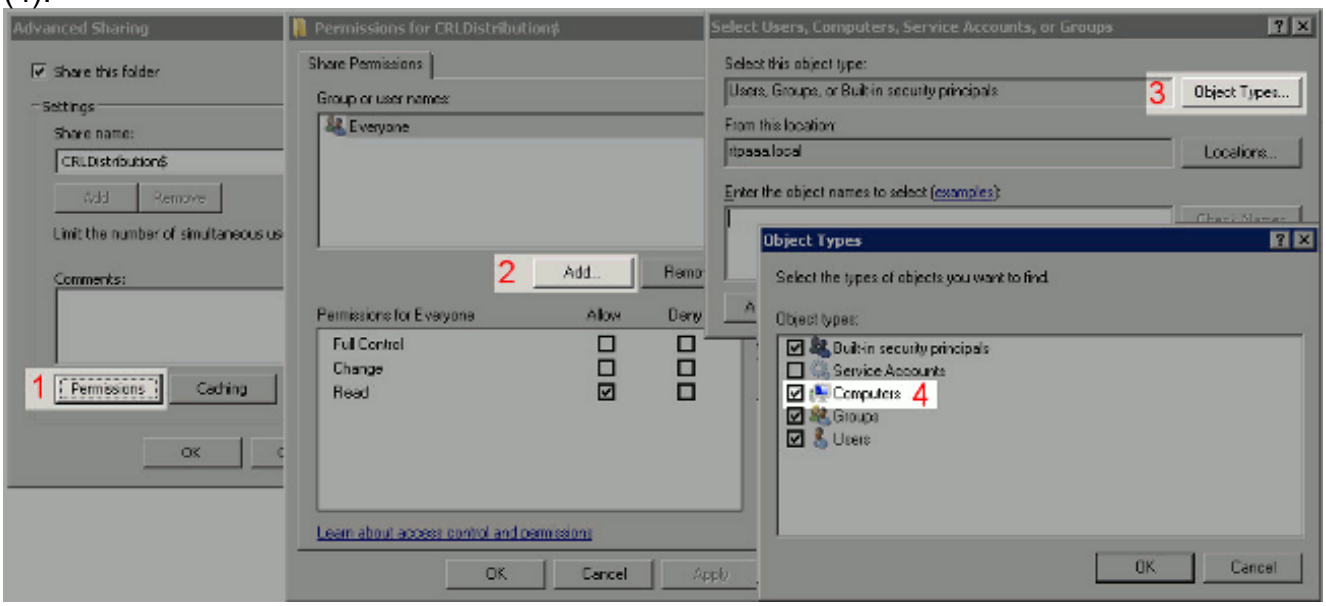
avanzada.

3. Para compartir la carpeta, controle la **parte esto casilla de selección de carpeta** y después agregue una muestra de dólar ($) al final del nombre de la parte en el campo de nombre de la parte de ocultar la

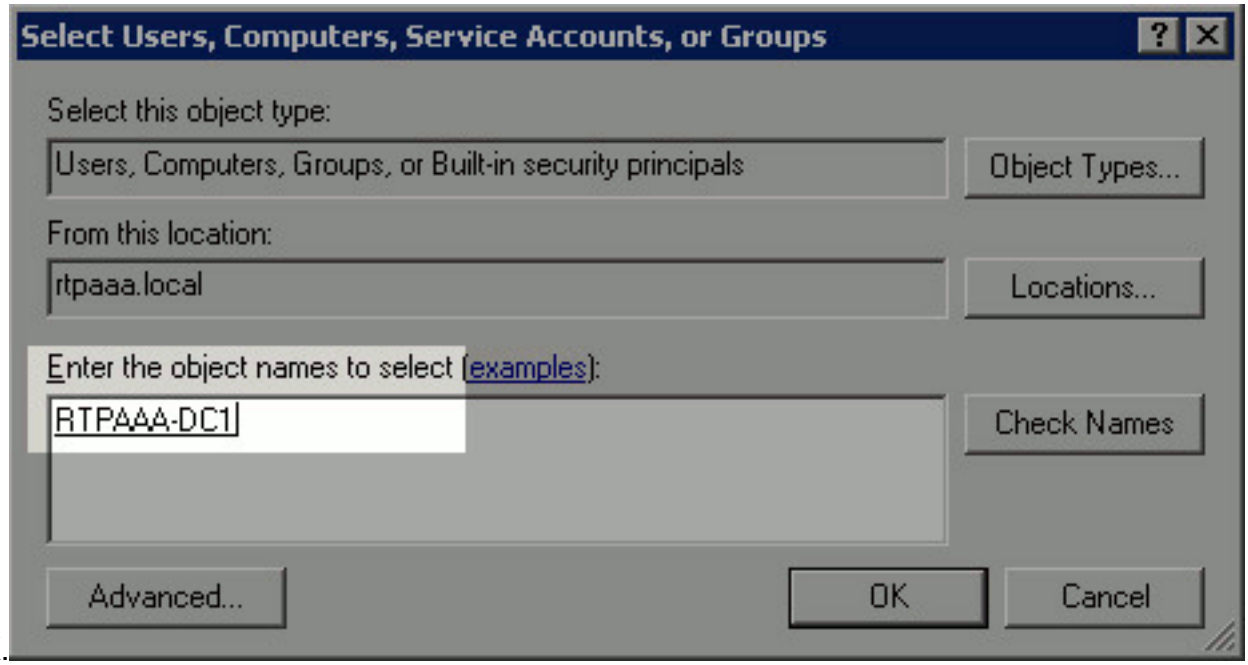


parte.

4. Haga clic los **permisos** (1), el tecleo **agrega** (2), hace clic los **tipos de objeto** (3), y controla la casilla de verificación de los **ordenadores** (4).

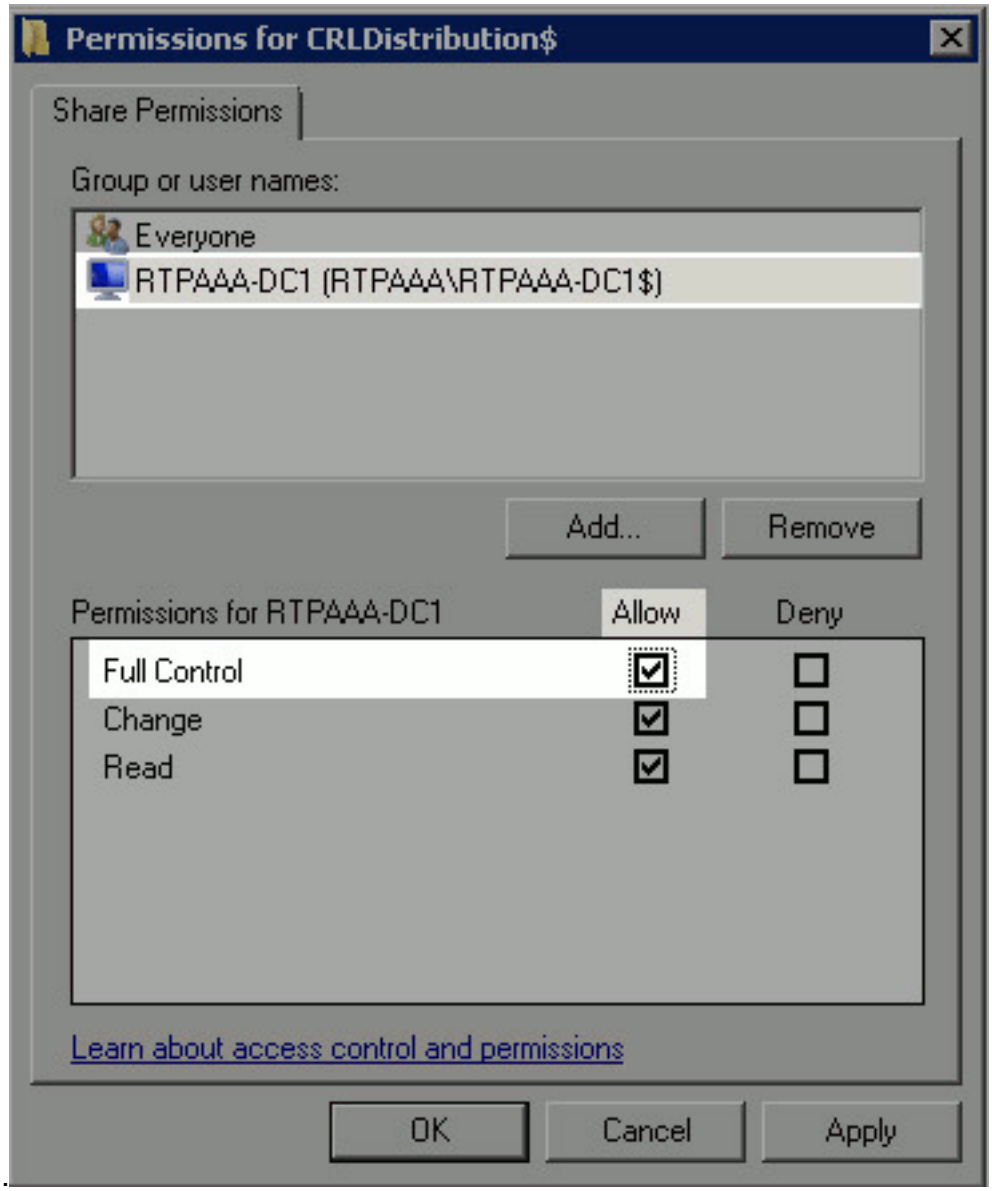


5. Para volver a la ventana selecta de los usuarios, de los ordenadores, de las Cuentas de servicio, o de grupos, **AUTORIZACIÓN del** tecleo. En el ingresar los nombres del objeto para seleccionar el campo, ingresar el nombre de computadora del servidor y del tecleo CA **controlan los nombres**. Si el nombre ingresado es válido, el nombre restaura y aparece subrayado. Click



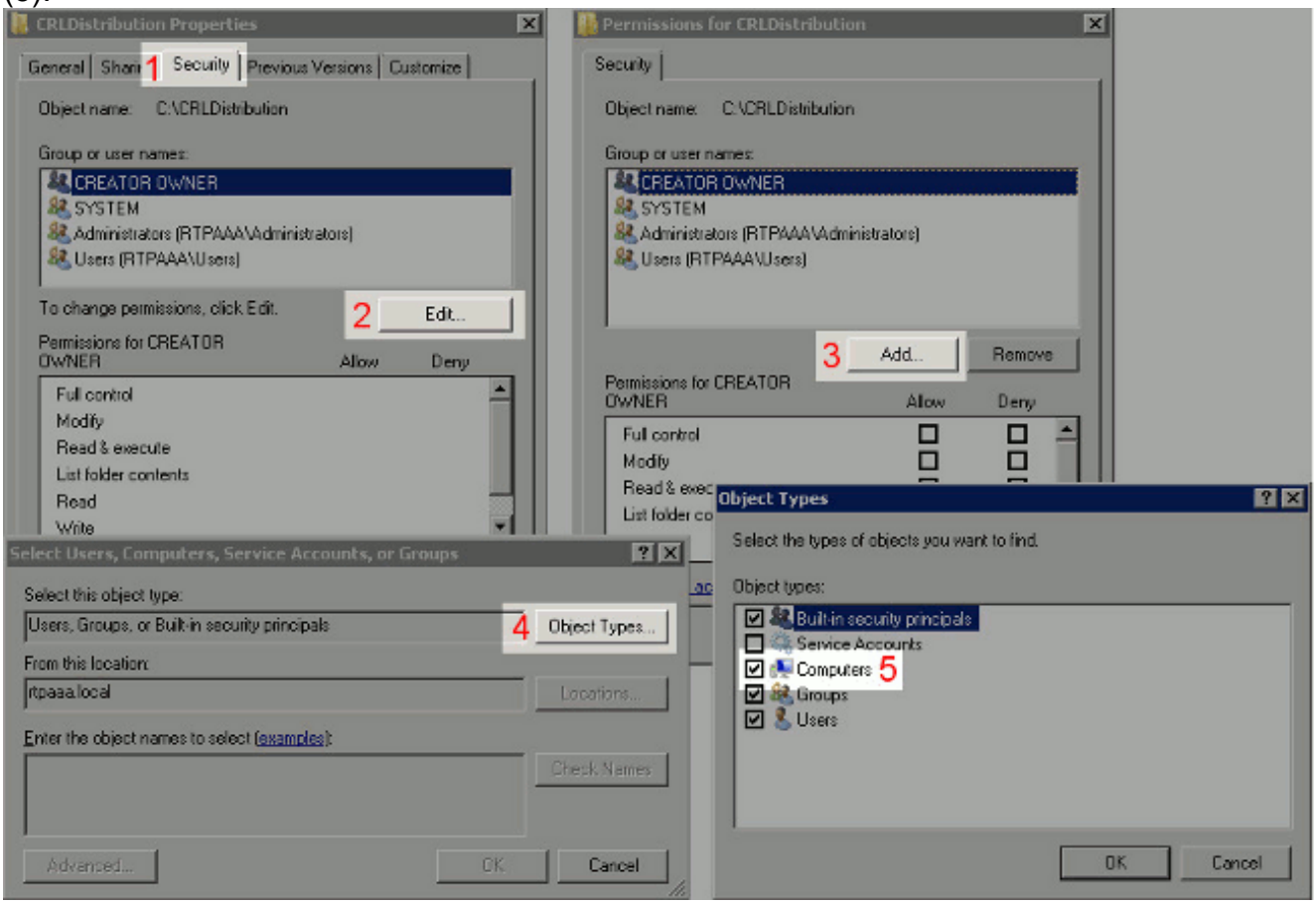
OK.

6. En el grupo o el campo de Nombres de usuario, elija el ordenador CA. El control **permite** para que el control total conceda el acceso total a la **AUTORIZACIÓN del** tecleo CA. Haga clic la **AUTORIZACIÓN** otra vez para cerrar la ventana de distribución avanzada y para volver a la ventana de

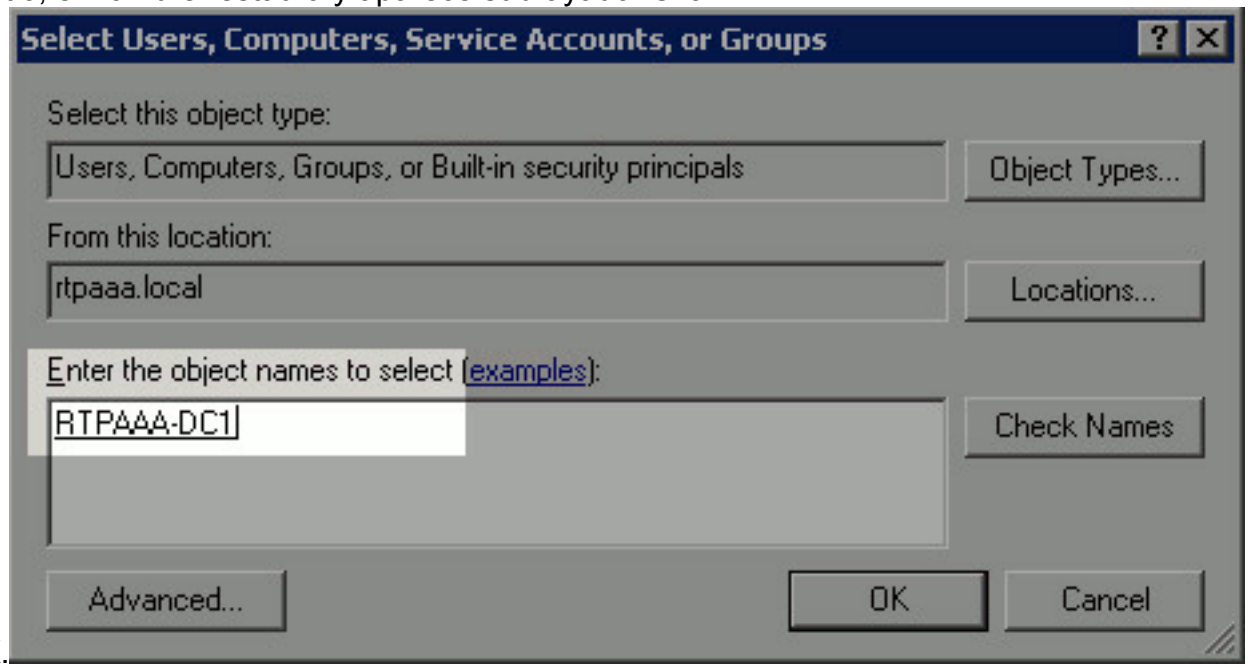


pPropiedades.

7. Para permitir que el CA escriba los ficheros CRL a la nueva carpeta, configure los permisos de seguridad apropiados. Haga clic la **ficha de seguridad** (1), el tecleo **corrige** (2), el tecleo **agrega** (3), hace clic los **tipos de objeto** (4), y controla la casilla de verificación de los **ordenadores** (5).

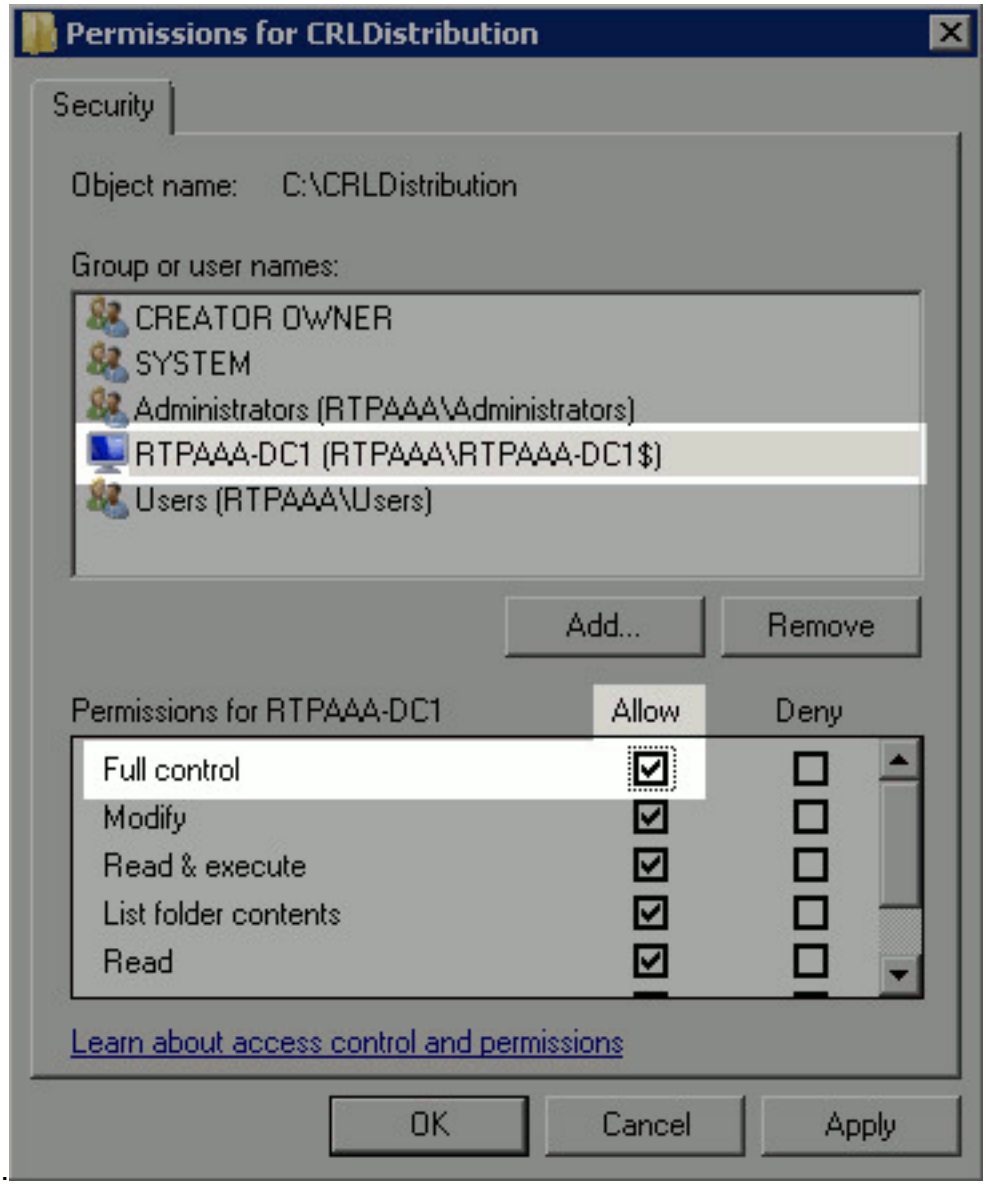


8. En el ingresar los nombres del objeto para seleccionar el campo, ingresar el nombre de computadora del servidor y del tecleo CA **controlan los nombres**. Si el nombre ingresado es válido, el nombre restaura y aparece subrayado. Click OK.



9. Elija el ordenador CA en el grupo o el campo de Nombres de usuario y después controle **tienen en cuenta** para que el control total conceda el acceso total a la **AUTORIZACIÓN del** tecleo CA y después haga clic **cerca de** completo la

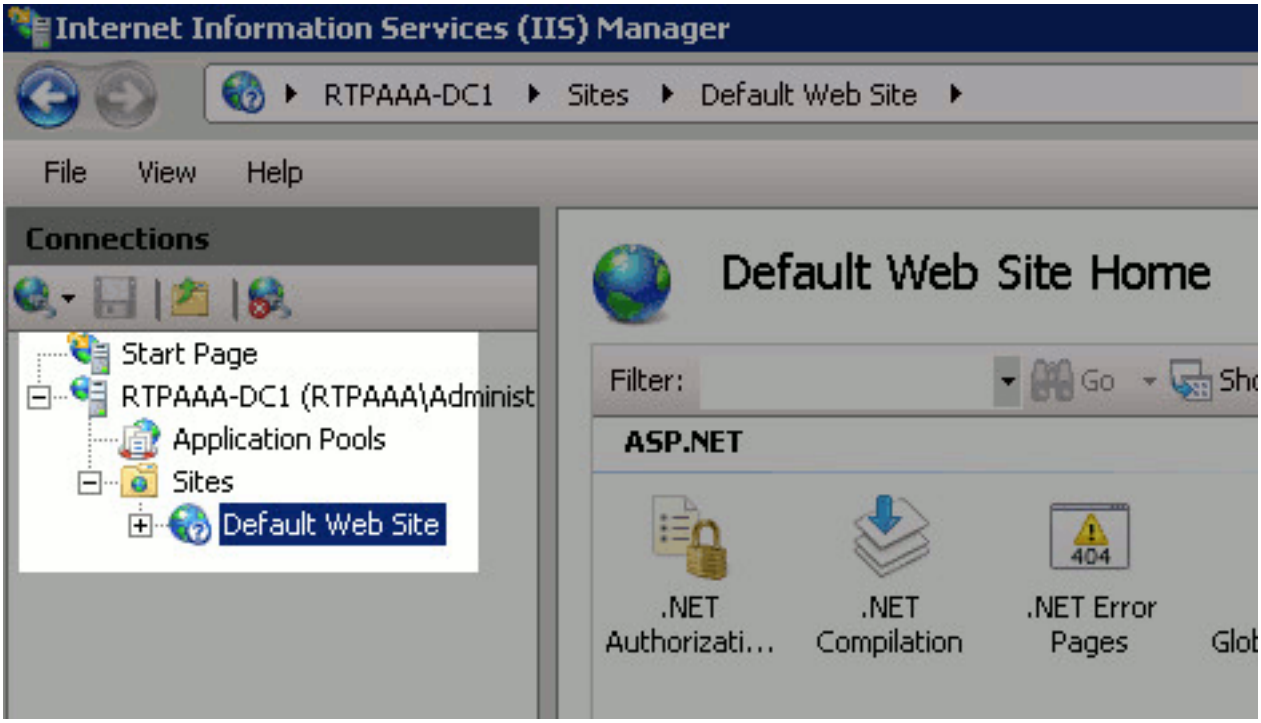
tarea.



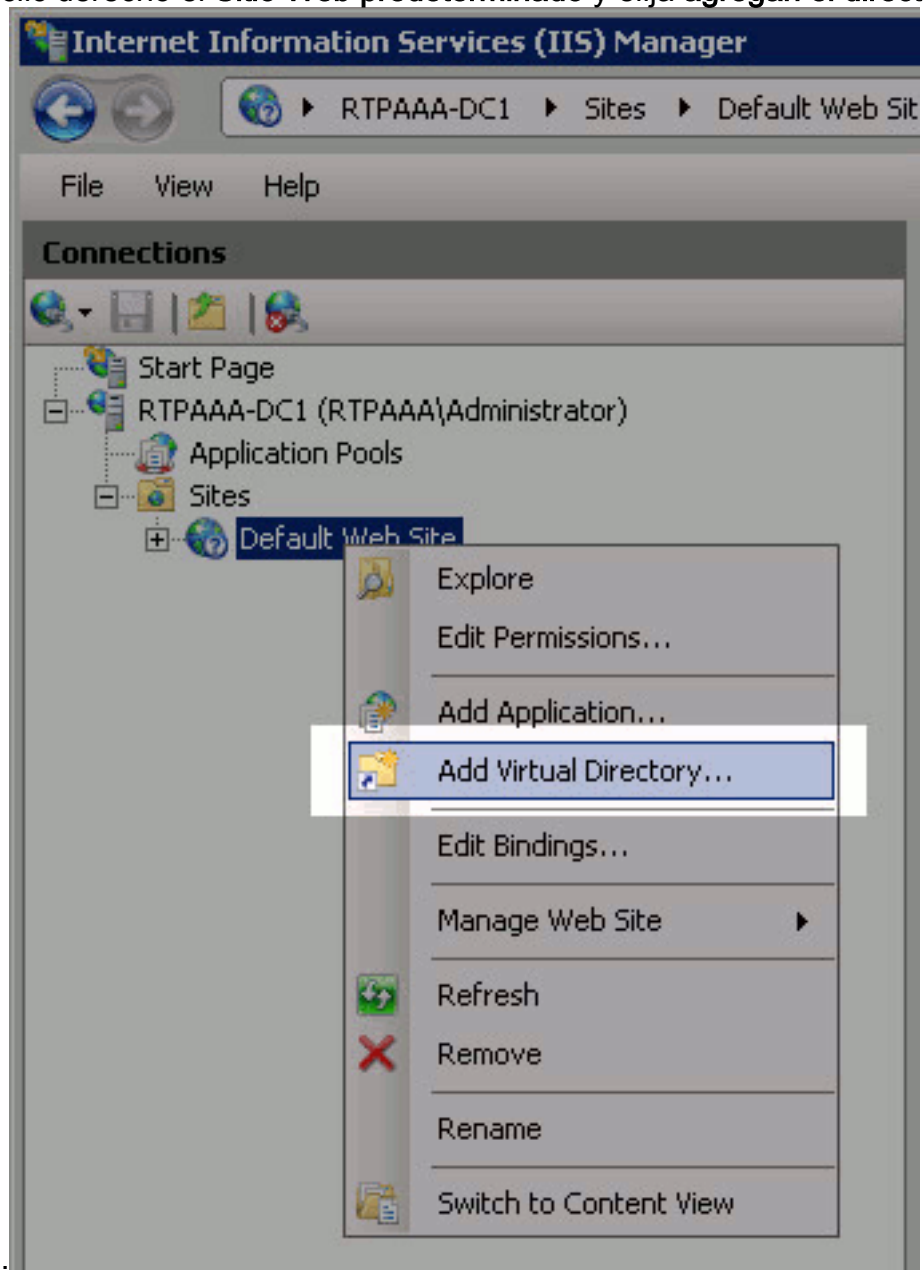
La sección 2. crea un sitio en el IIS para exponer la nueva punta de la distribución CRL

Para que ISE tenga acceso a los ficheros CRL, haga el directorio que contiene los ficheros CRL accesibles vía el IIS.

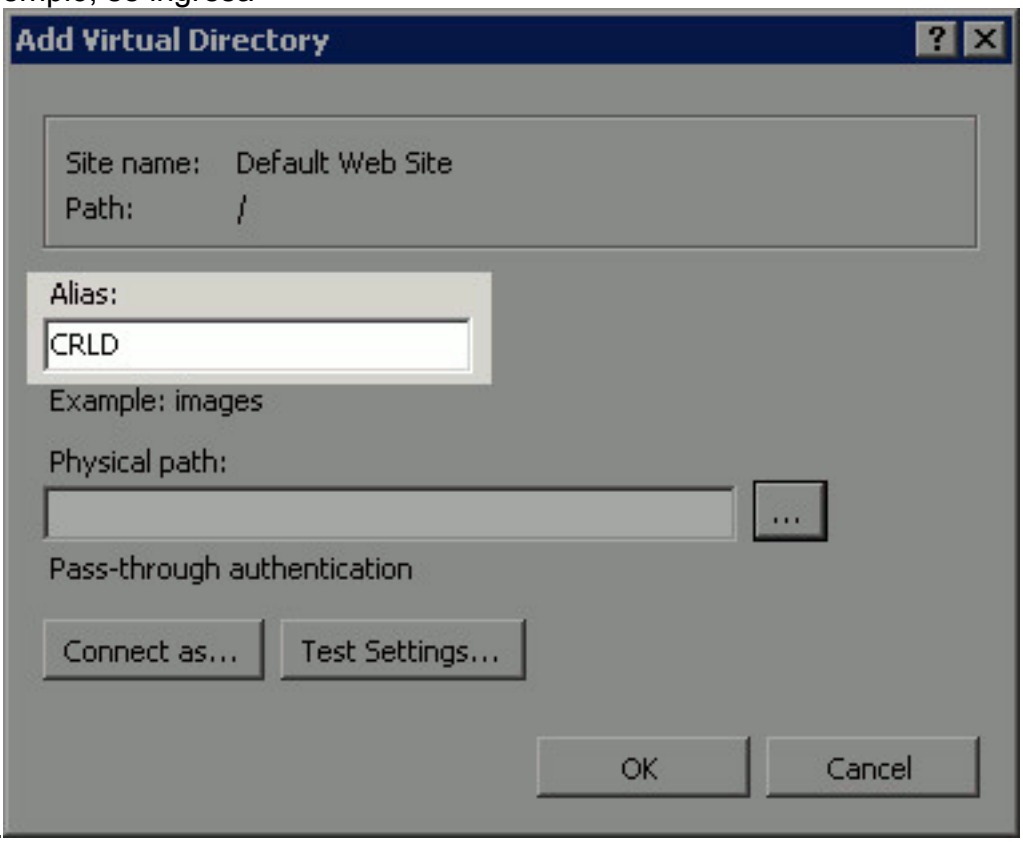
1. En el servidor IIS taskbar, haga clic el **comienzo**. Elija las **herramientas > al encargado administrativos de los Servicios de Internet Information Server (IIS)**.
2. En el panel izquierdo (conocido como el árbol de la consola), amplíe el nombre de servidor IIS y después amplíe los
sitios.



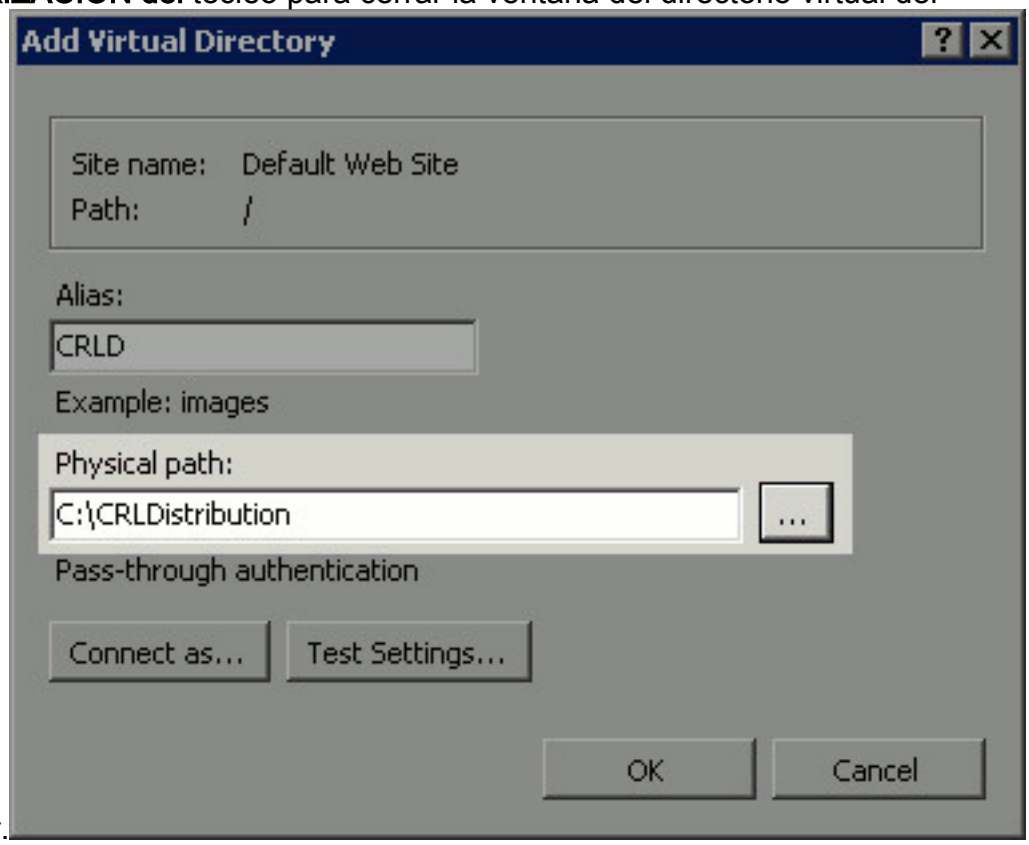
3. Haga clic derecho el **Sitio Web predeterminado** y elija **agregan el directorio virtual**.



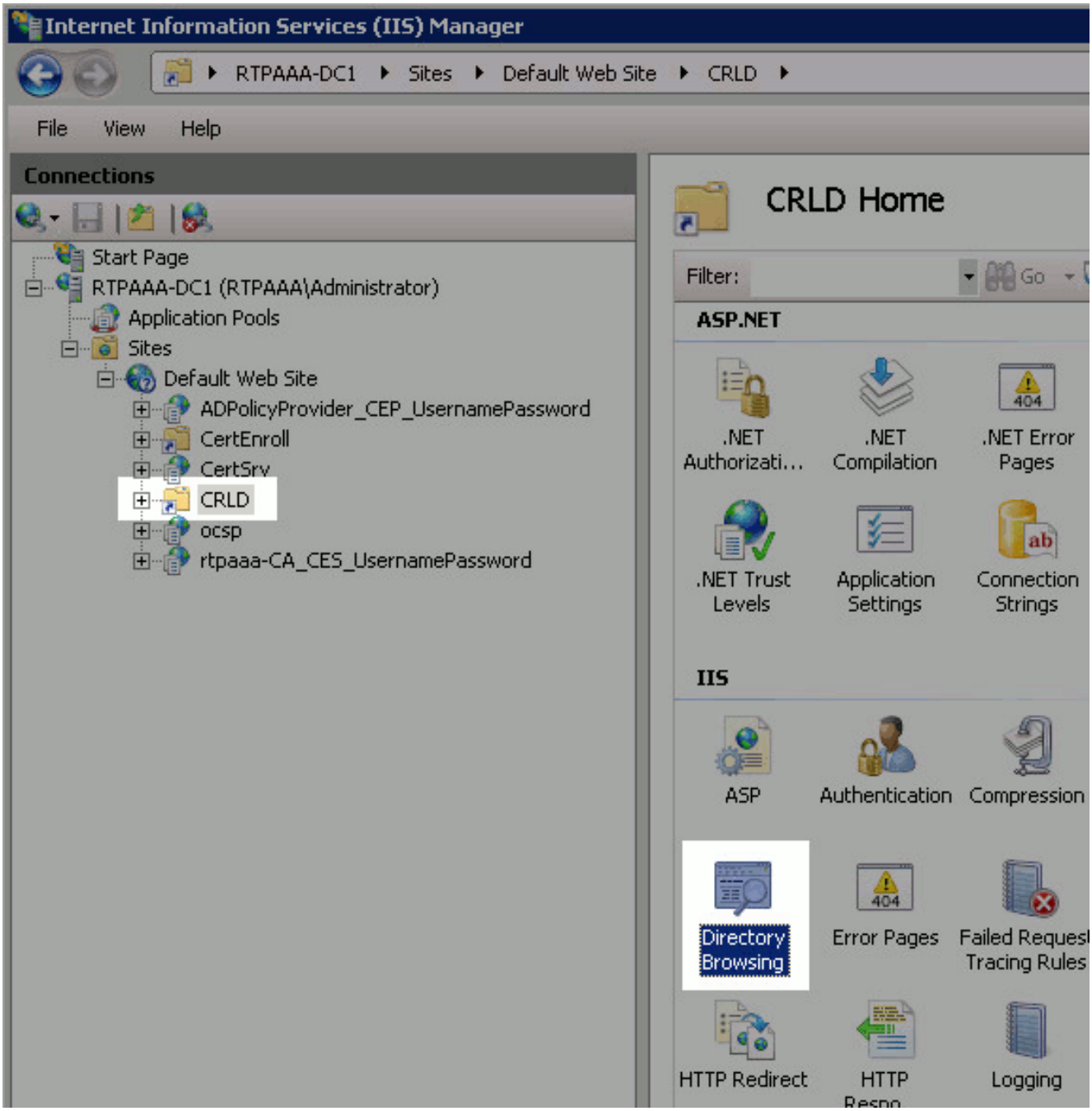
4. En el campo del alias, ingrese un nombre del sitio para la punta de la distribución CRL. En este ejemplo, se ingresa CRLD.



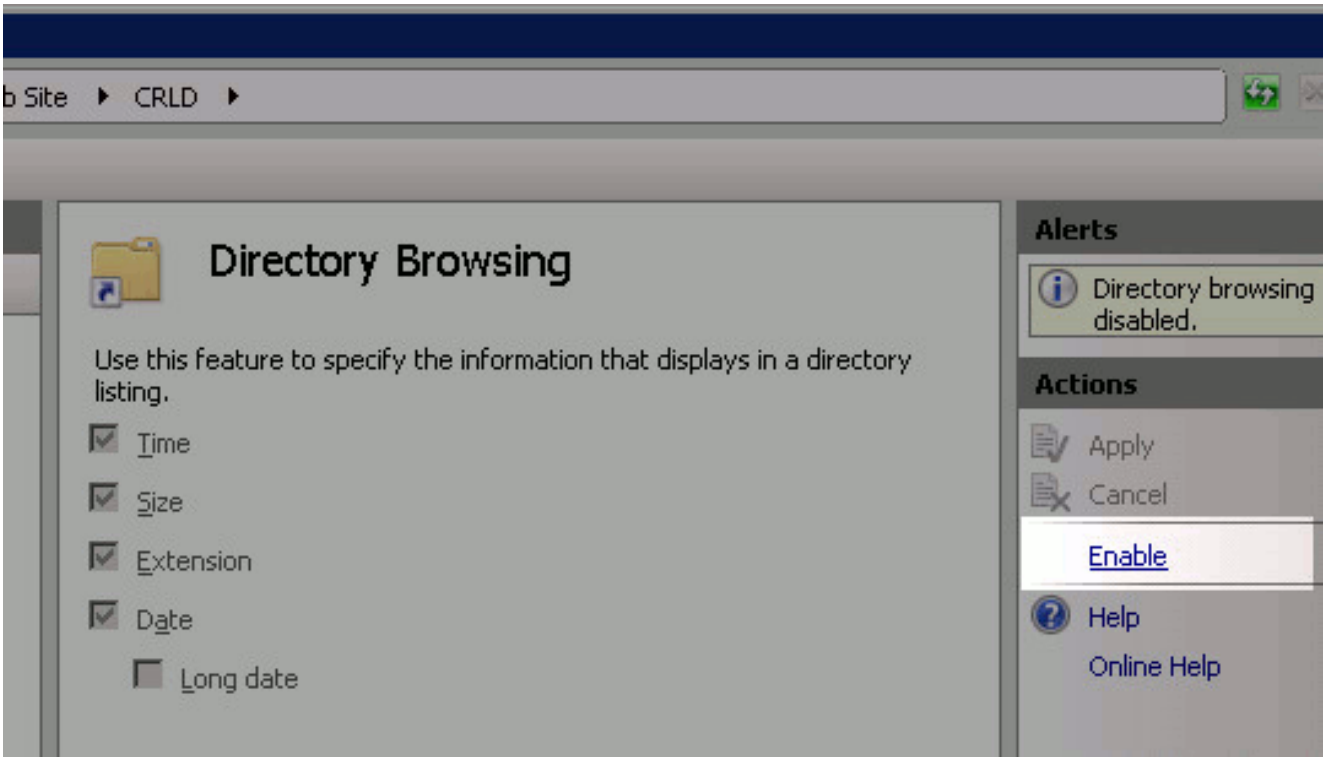
5. Haga clic los puntos de suspensión (…) a la derecha del campo de la ruta física y hojee a la carpeta creada en la sección 1. selecta la carpeta y haga clic la **AUTORIZACIÓN**. **AUTORIZACIÓN del** tecleo para cerrar la ventana del directorio virtual del agregar.



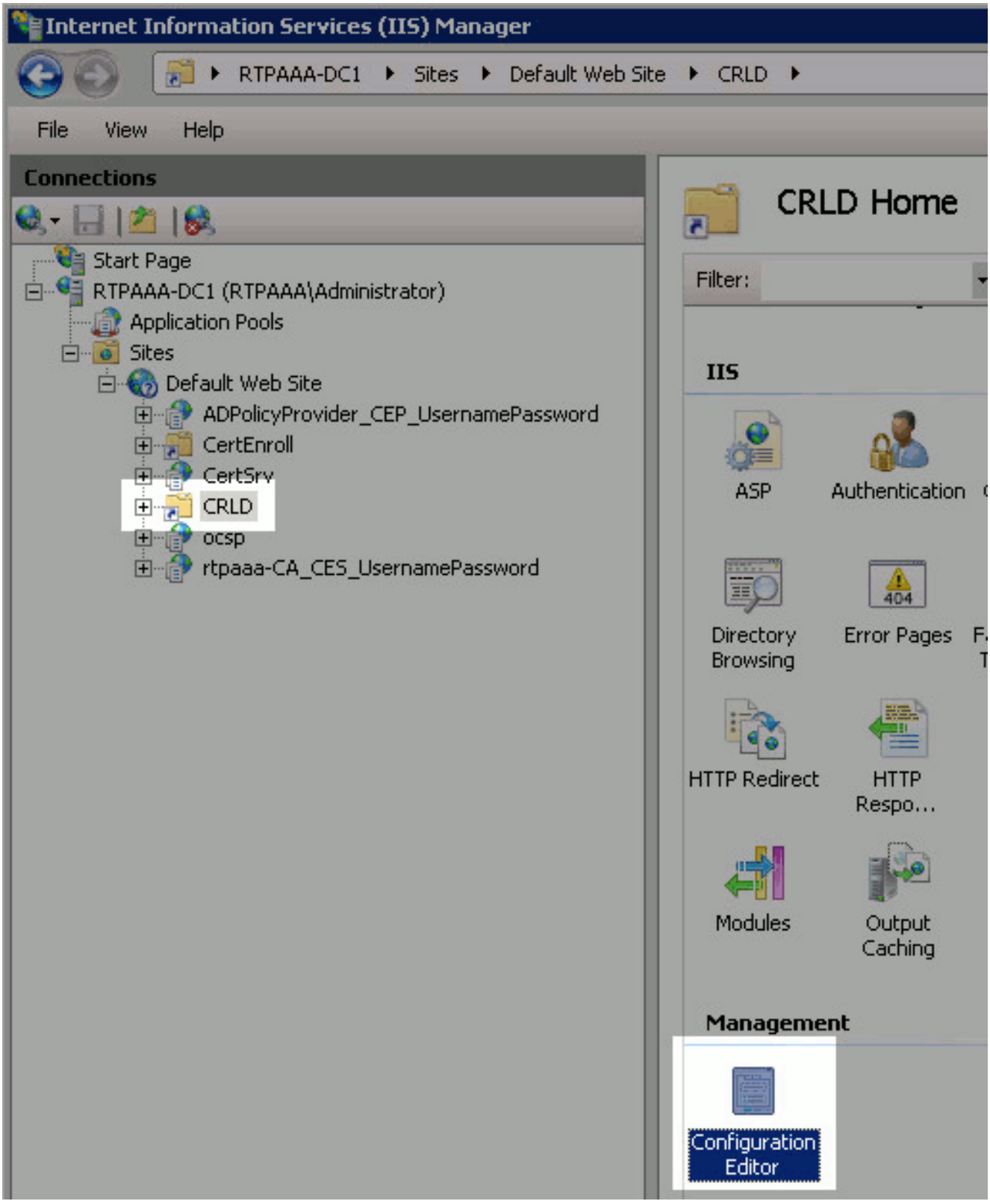
6. El nombre del sitio ingresado en el paso 4 se debe destacar en el panel izquierdo. Si no, ahora elíjalo. En el centro cristal, **directorio del** doble clic **que hojea**.



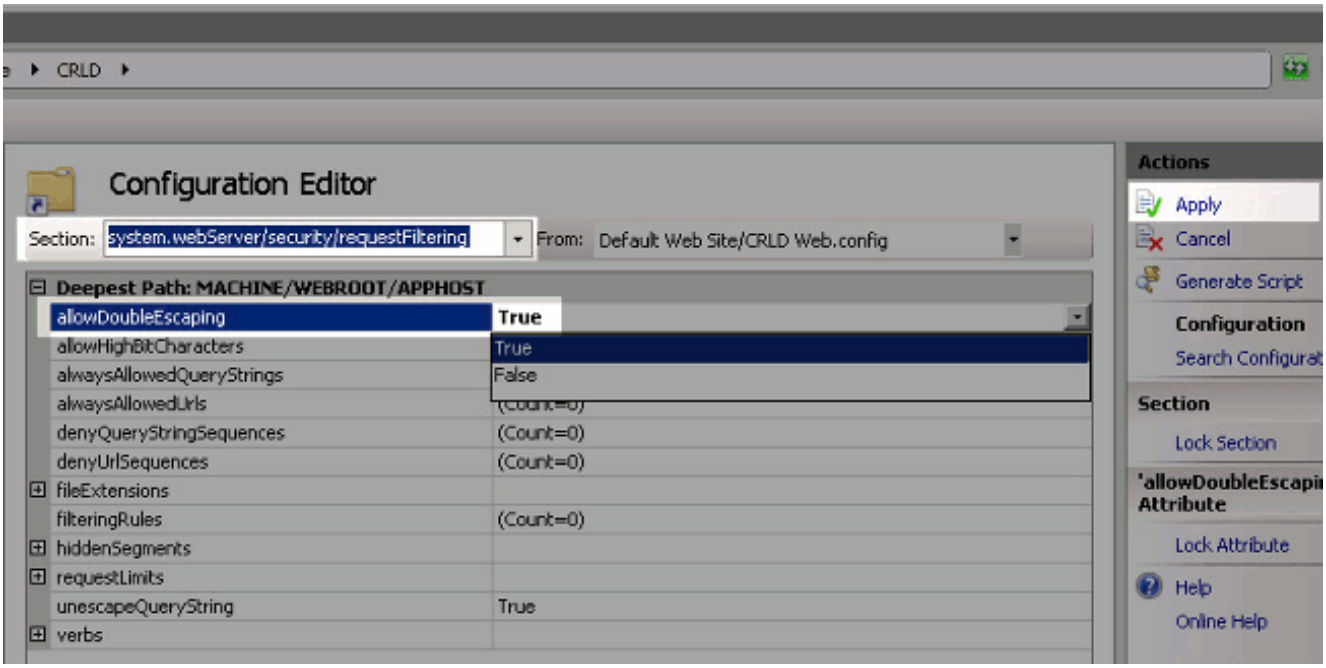
7. En el panel derecho, **permiso del** tecleo para activar el directorio que hojea.



8. En el panel izquierdo, elija el nombre del sitio otra vez. En el centro cristal, **editor de la configuración del** doble
clic.



9. En la lista desplegable de la sección, elija **system.webServer/la Seguridad/requestFiltering. En la** lista desplegable allowDoubleEscaping, elija verdad**. En el** panel derecho, el tecleo se aplica**.**

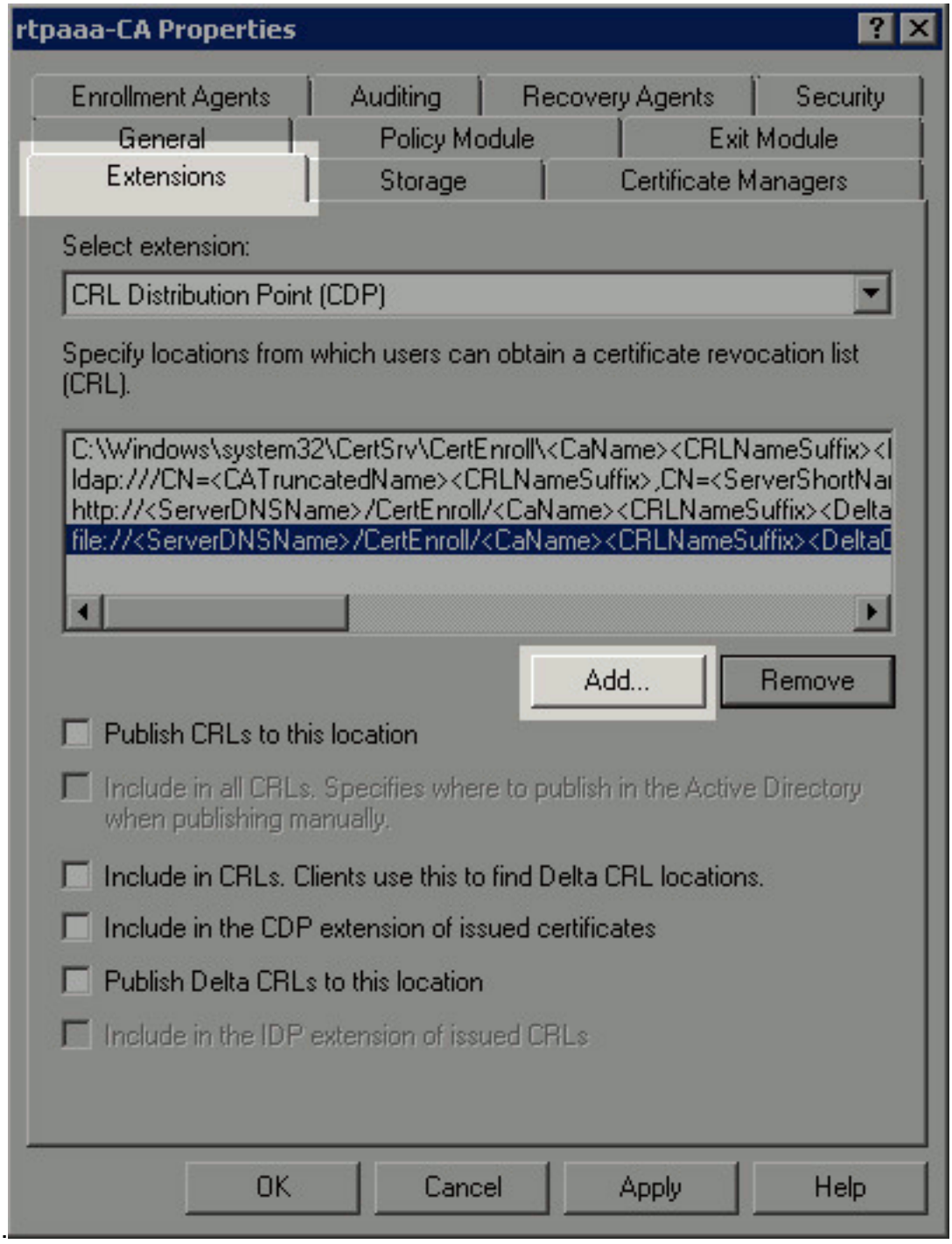


La carpeta debe ahora ser accesible vía el IIS.

La sección 3. configura el servidor de Microsoft CA para publicar los ficheros CRL a la punta de la distribución

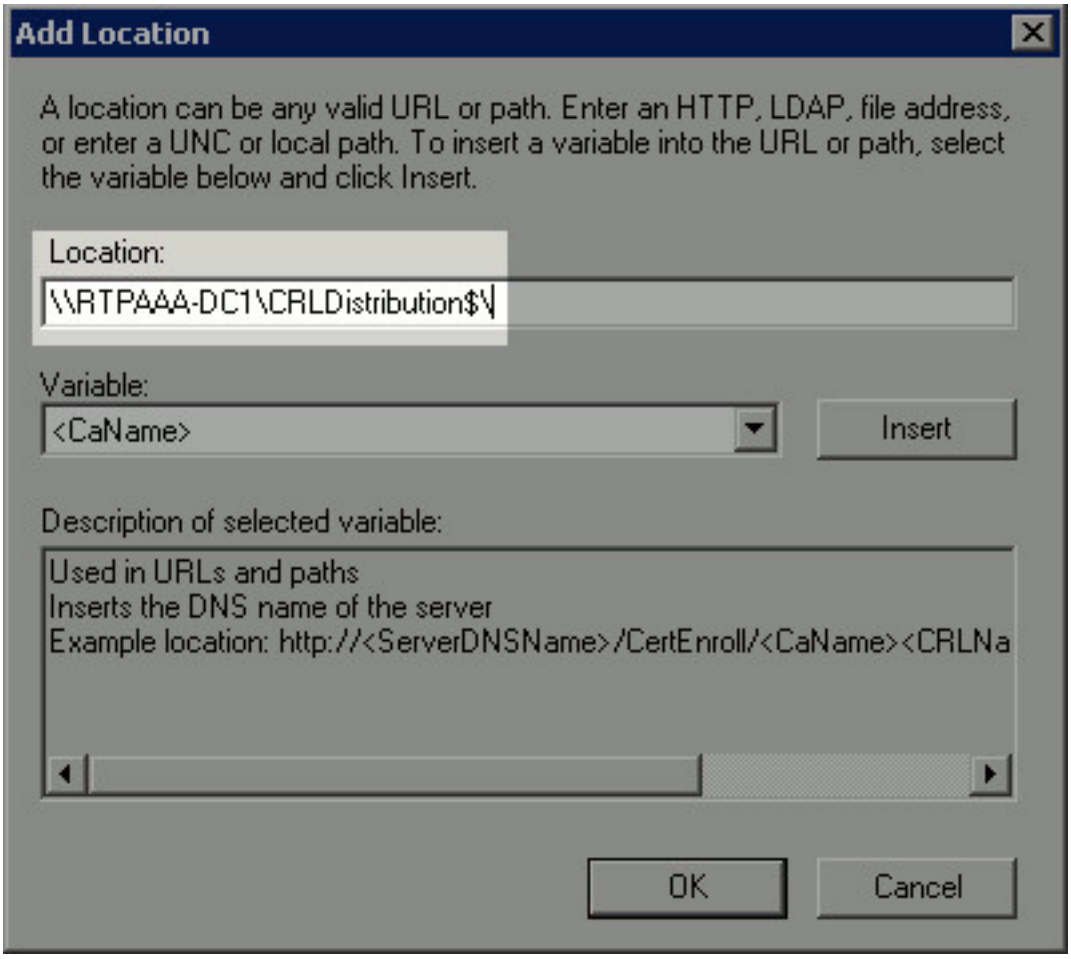
Ahora que una nueva carpeta se ha configurado para contener los ficheros CRL y la carpeta se ha expuesto en el IIS, configure el servidor de Microsoft CA para publicar los ficheros CRL a la nueva ubicación.

1. En el servidor CA taskbar, haga clic el **comienzo**. Elija las **herramientas > la autoridad de certificación administrativas**.
2. En el panel izquierdo, haga clic derecho el nombre CA. Elija las **propiedades** y después haga clic las **Extensiones** cuadro para agregar una nueva punta de la distribución CRL, tecleo

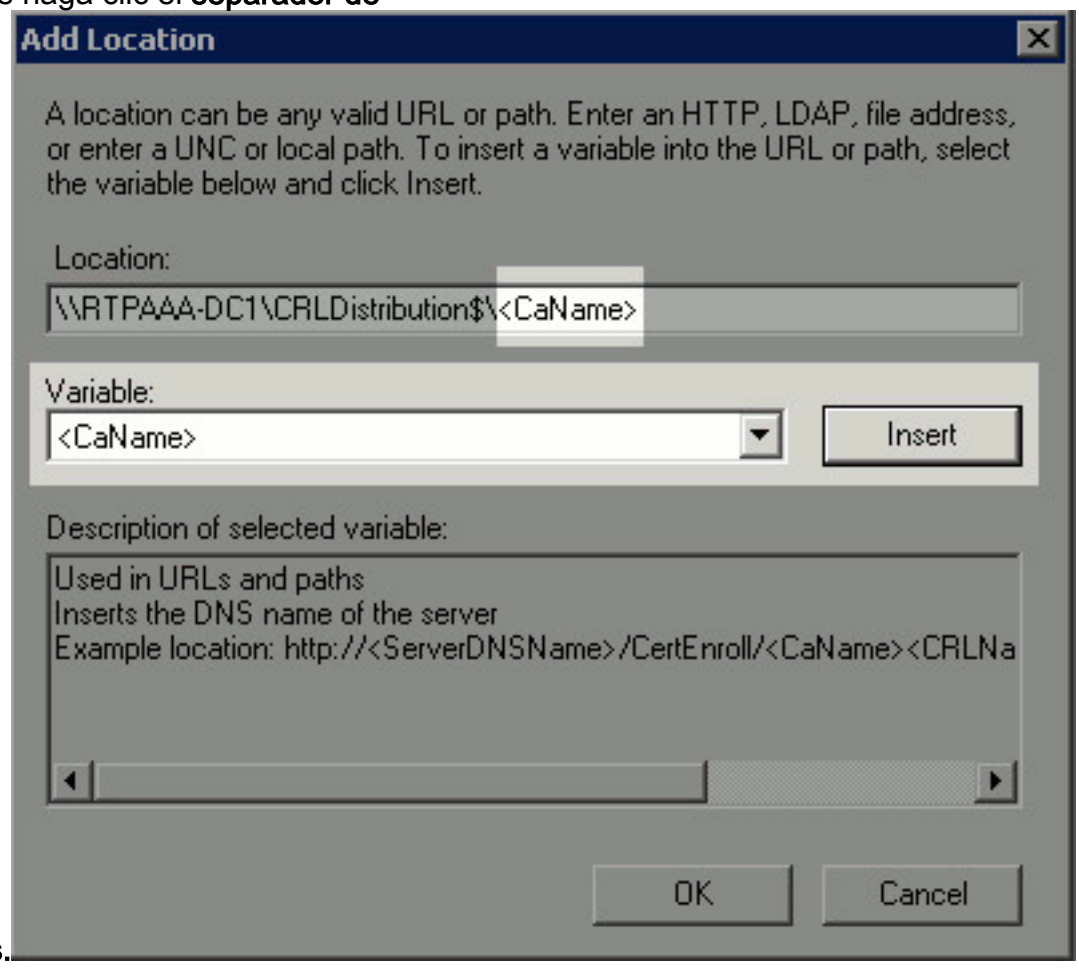


agregan.

3. En el campo de la ubicación, ingrese la trayectoria a la carpeta creada y compartida en la sección 1. En el ejemplo en la sección 1, la trayectoria es:
   `\\RTPAAA-DC1\CRLDistribution$\`

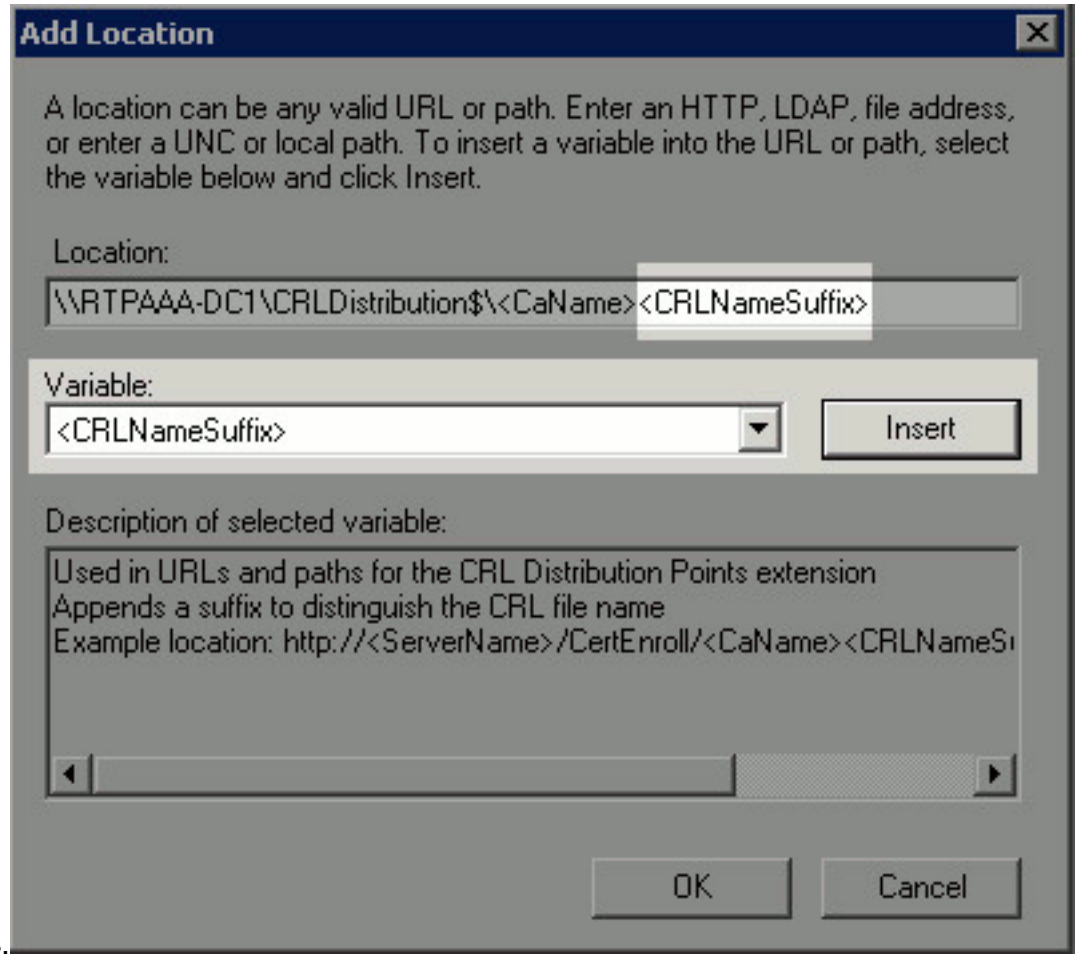


4. Con el campo de la ubicación poblado, elija el **<CaName> de la** lista desplegable variable y después haga clic el **separador de**



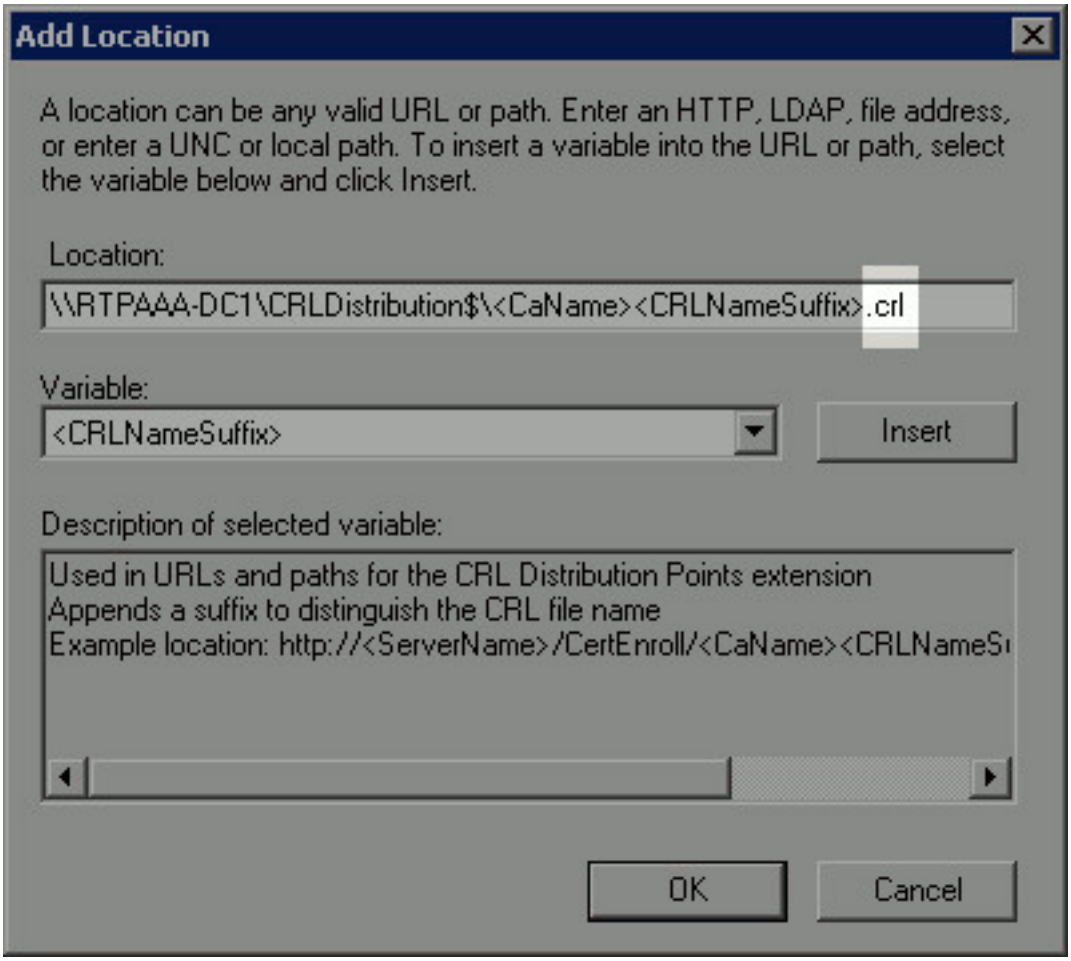
millares.

5. De la lista desplegable variable, elija el **<CRLNameSuffix>** y después haga clic el **separador**

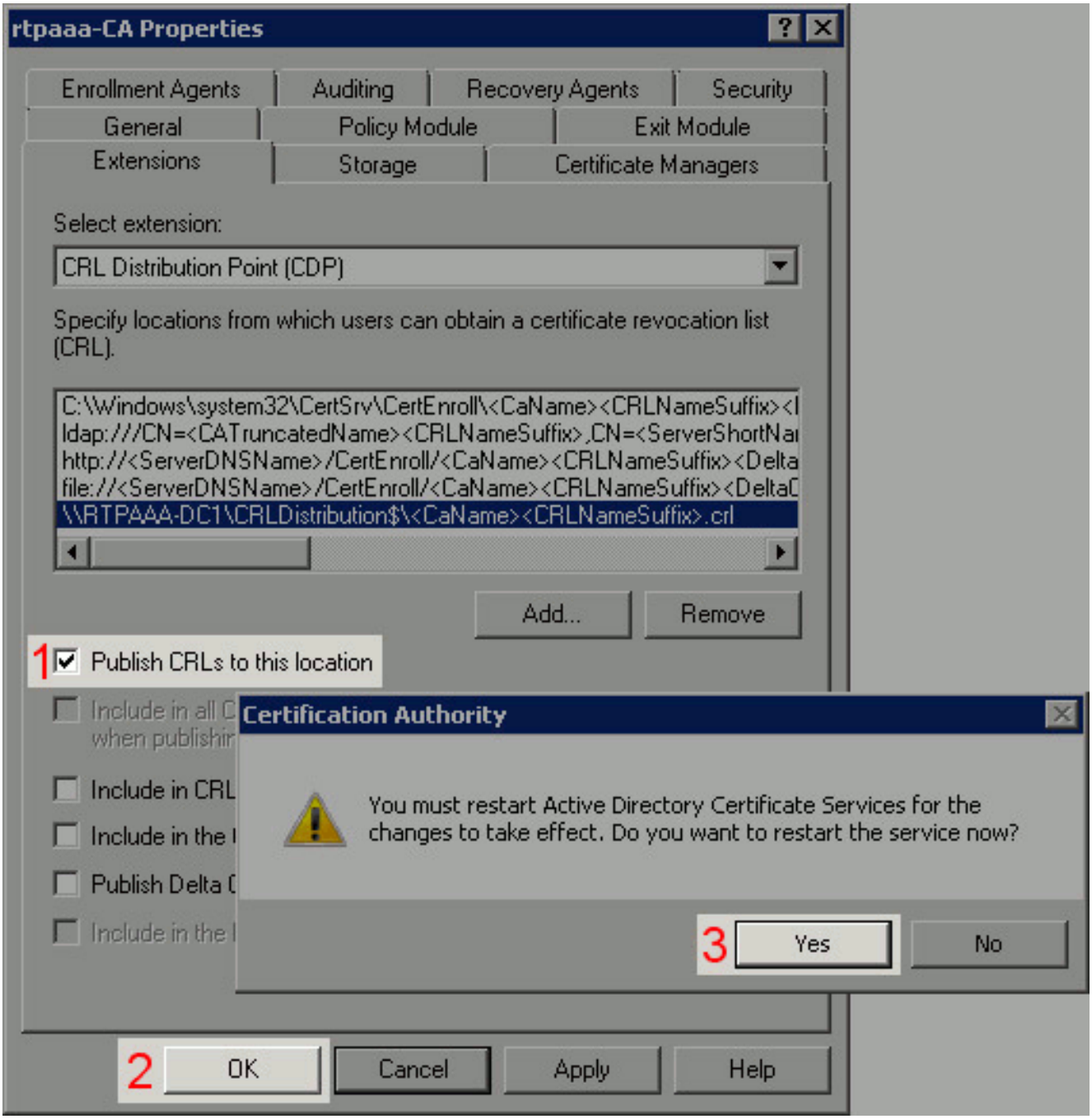


de millares.

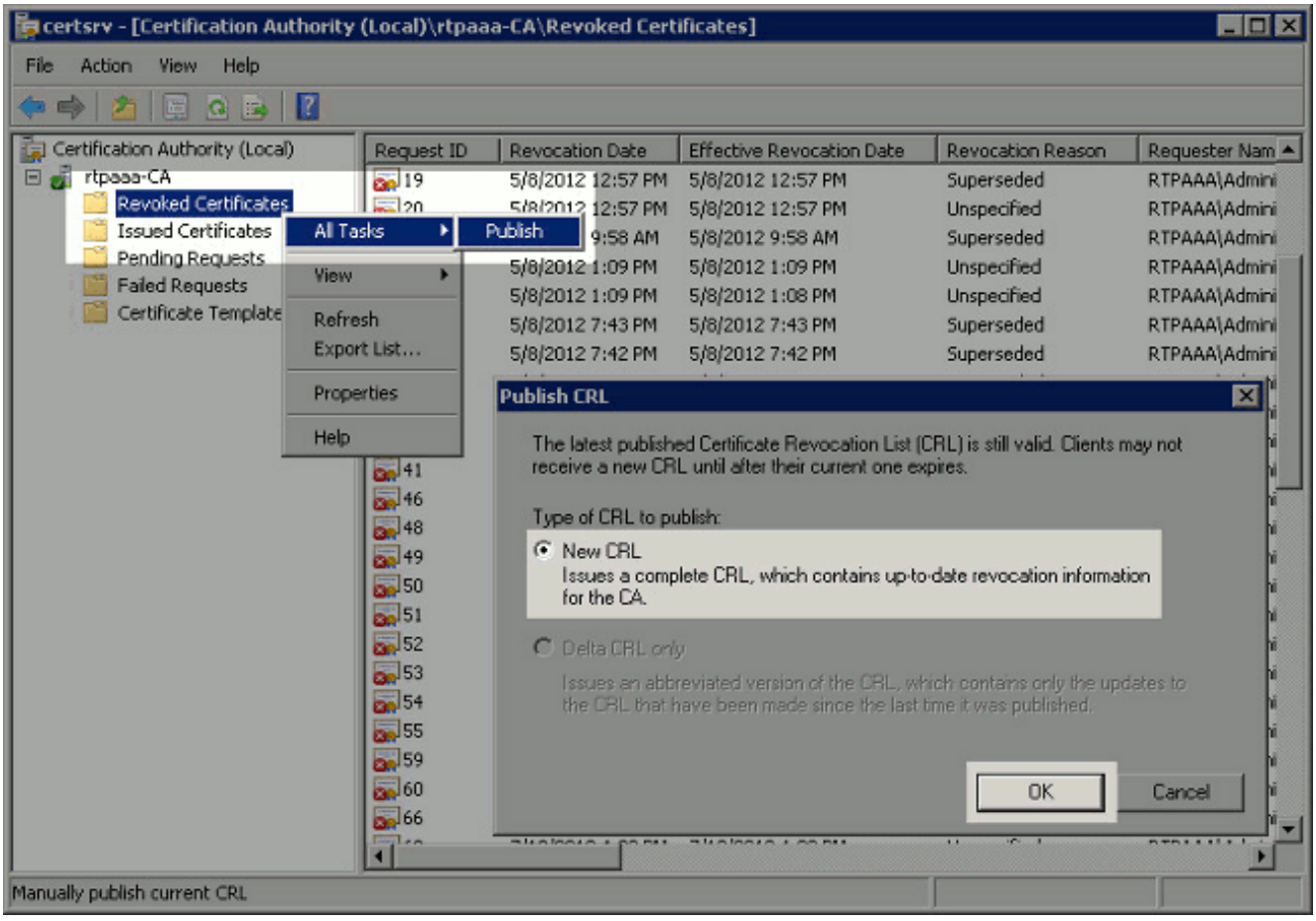
6. En el campo de la ubicación, añada .crl al final del fichero al extremo de la trayectoria. En este ejemplo, la ubicación es:
   `\\RTPAAA-DC1\CRLDistribution$\<CaName><CRLNameSuffix>.crl`



7. Haga clic la **AUTORIZACIÓN** para volver a las Extensiones cuadro. Controle la **publicación CRL a esta** casilla de verificación de la **ubicación** (1) y después haga clic la **AUTORIZACIÓN** (2) para cerrar la ventana de pPropiedades. Un mensaje aparece para que el permiso recomience los servicios del certificado del Active Directory. Tecleo **sí** (3).



8. En el panel izquierdo, el clic derecho **revocó los Certificados**. Elija **todas las tareas > publican**. Asegúrese de que el nuevo CRL esté seleccionado y después haga clic la **AUTORIZACIÓN.**

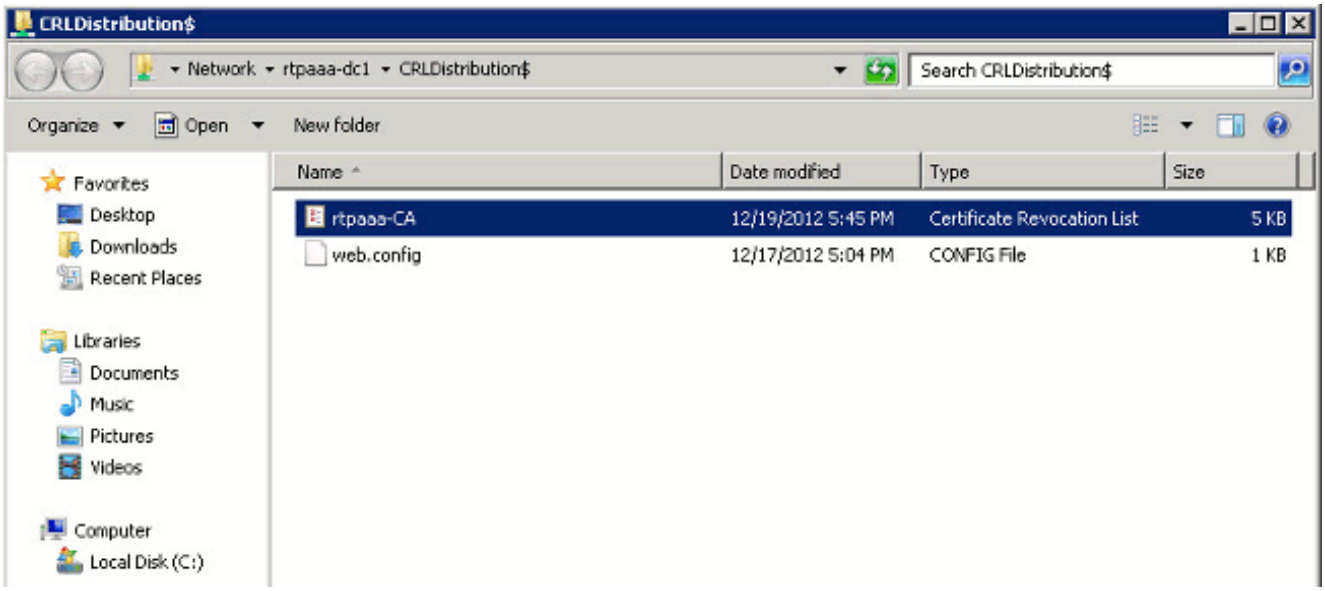


El servidor de Microsoft CA debe crear un nuevo fichero .crl en la carpeta creada en la sección 1. Si el nuevo fichero CRL se crea con éxito se hace clic no habrá diálogo después de que sea ACEPTABLE. Si un error se vuelve con respecto a la nueva carpeta de la punta de la distribución, relance cuidadosamente cada paso en esta sección.

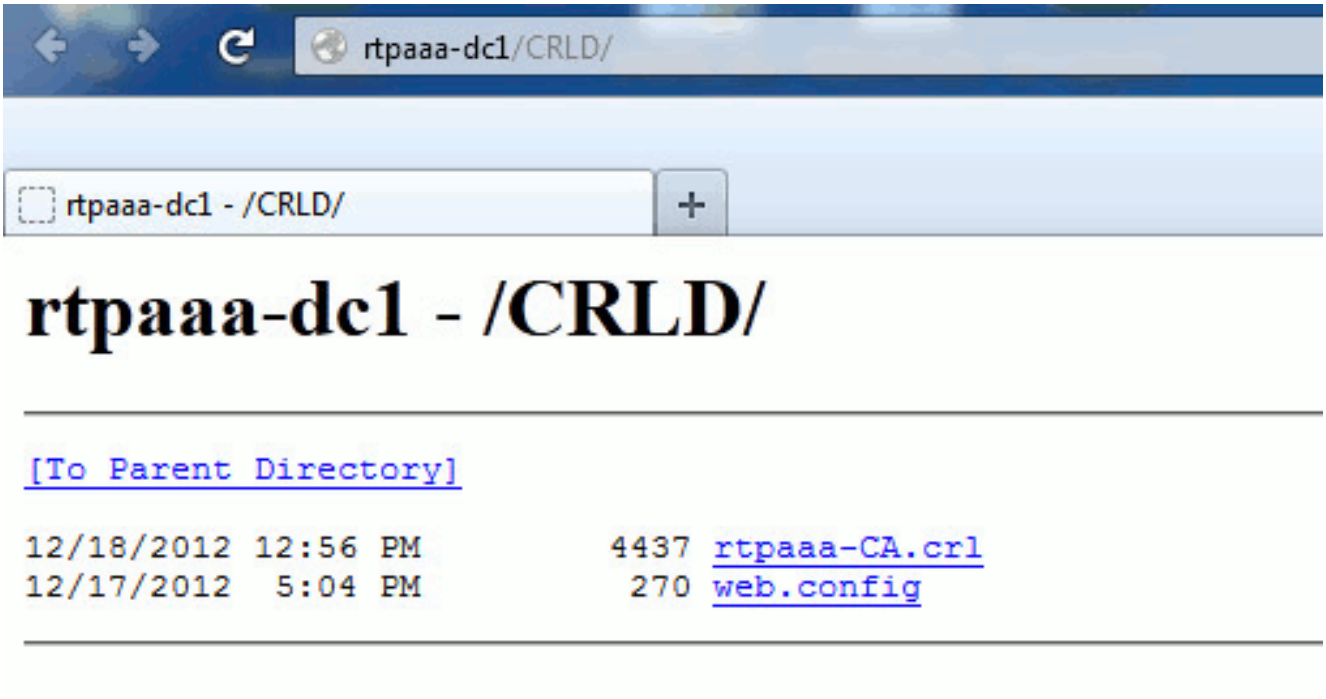
La sección 4. verifica que el fichero CRL exista y que sea accesible vía el IIS

Verifique que existan los nuevos ficheros CRL y eso son accesibles vía el IIS de otro puesto de trabajo antes de que usted comience esta sección.

1. En el servidor IIS, abra la carpeta creada en la sección 1. Debe haber un solo fichero .crl presente con la forma <CANAME>.crl donde está el nombre <CANAME> del servidor CA. En este ejemplo, el nombre de fichero es:
   `rtpaaa-CA.crl`



2. De un puesto de trabajo en la red (idealmente en la misma red que el nodo primario ISE Admin), abra a un buscador Web y hojee a http:// <SERVER>/<CRLSITE> donde está el nombre <SERVER> de servidor del servidor IIS configurado en la sección 2 y <CRLSITE> es el nombre del sitio elegido para la punta de la distribución en la sección 2. En este ejemplo, el URL es:
`http://RTPAAA-DC1/CRLD`
Las visualizaciones del índice del directorio, que incluye el fichero observaron en el paso 1.



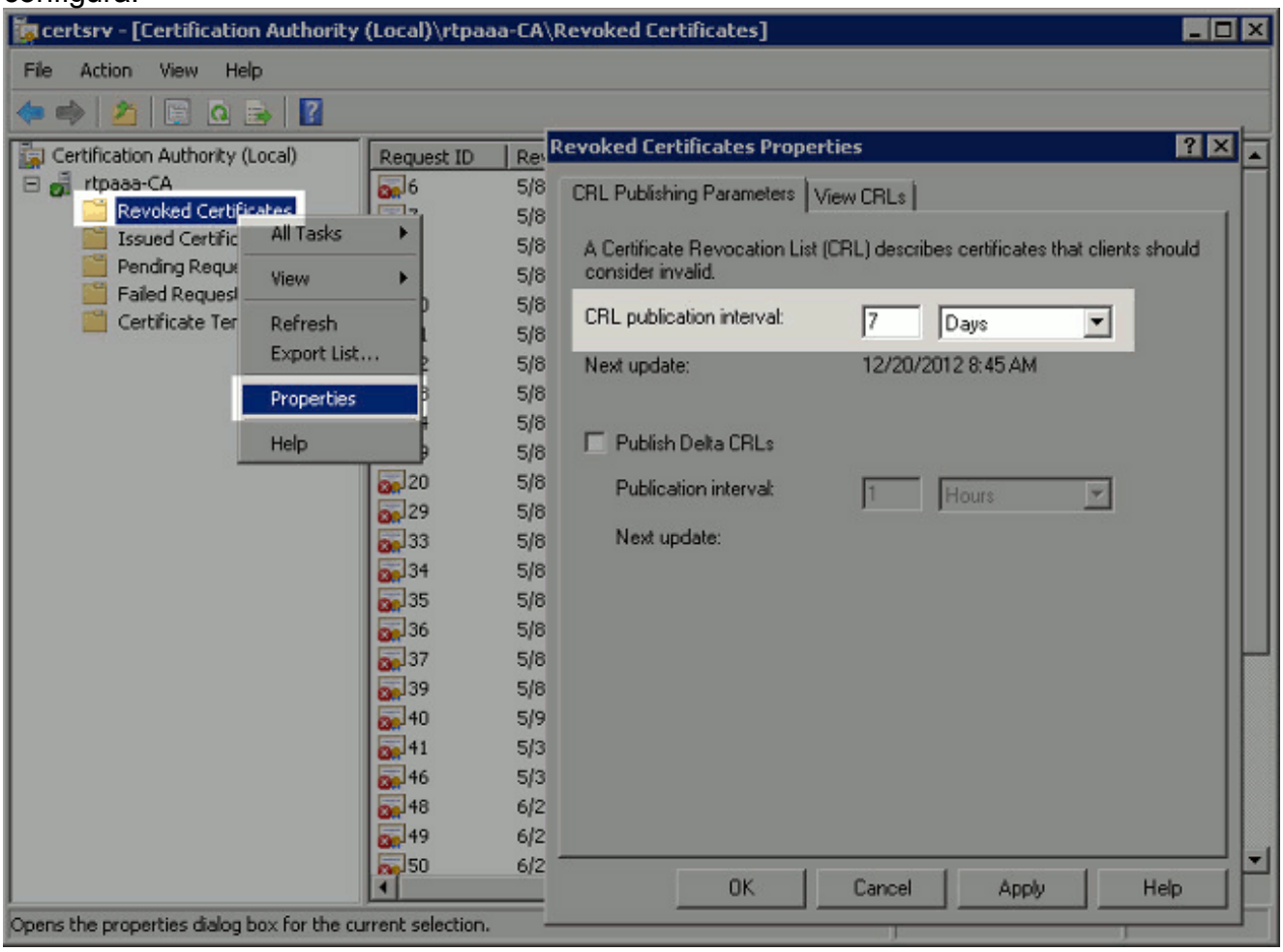
La sección 5. configura ISE para utilizar la nueva punta de la distribución CRL

Antes de que ISE se configure para extraer el CRL, defina el intervalo para publicar el CRL. La estrategia para determinar este intervalo está fuera del alcance de este documento. Los valores potenciales (en Microsoft CA) son 1 hora a 411 años, de inclusivo. El valor predeterminado es 1 semana. Una vez que un intervalo apropiado para su entorno se ha determinado, fije el intervalo con estas instrucciones:

1. En el servidor CA taskbar, haga clic el **comienzo**. Elija las **herramientas > la autoridad de**

certificación administrativas.

2. En el panel izquierdo, amplíe el clic derecho CA la carpeta **revocada de los Certificados** y elija las **propiedades.**
3. En los campos del intervalo de la publicación CRL, ingrese el número requerido y elija el período de tiempo. Haga clic la **AUTORIZACIÓN** para cerrar la ventana y para aplicar el cambio. En este ejemplo, un intervalo de la publicación de 7 días se configura.



Usted debe ahora confirmar varios valores de registro, que ayudarán a determinar las configuraciones de la extracción CRL en ISE.

4. Ingrese el **certutil - el getreg CA ** comando de **Clock*** de confirmar el valor de ClockSkew. El valor predeterminado es 10 minutos.Salida de ejemplo:

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

5. Ingrese el **certutil - el getreg CA ** comando de **CRLov*** de verificar si el CRLOverlapPeriod se ha fijado manualmente. Por abandono el valor de CRLOverlapUnit es 0, que indica que no se ha fijado ningún valor manual. Si el valor es un valor con excepción de 0, registre el valor y las unidades.Salida de ejemplo:

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

6. Ingrese el **certutil - el getreg CA ** comando de **CRLpe*** de verificar el CRLPeriod, que fue fijado en el paso 3.Salida de ejemplo:

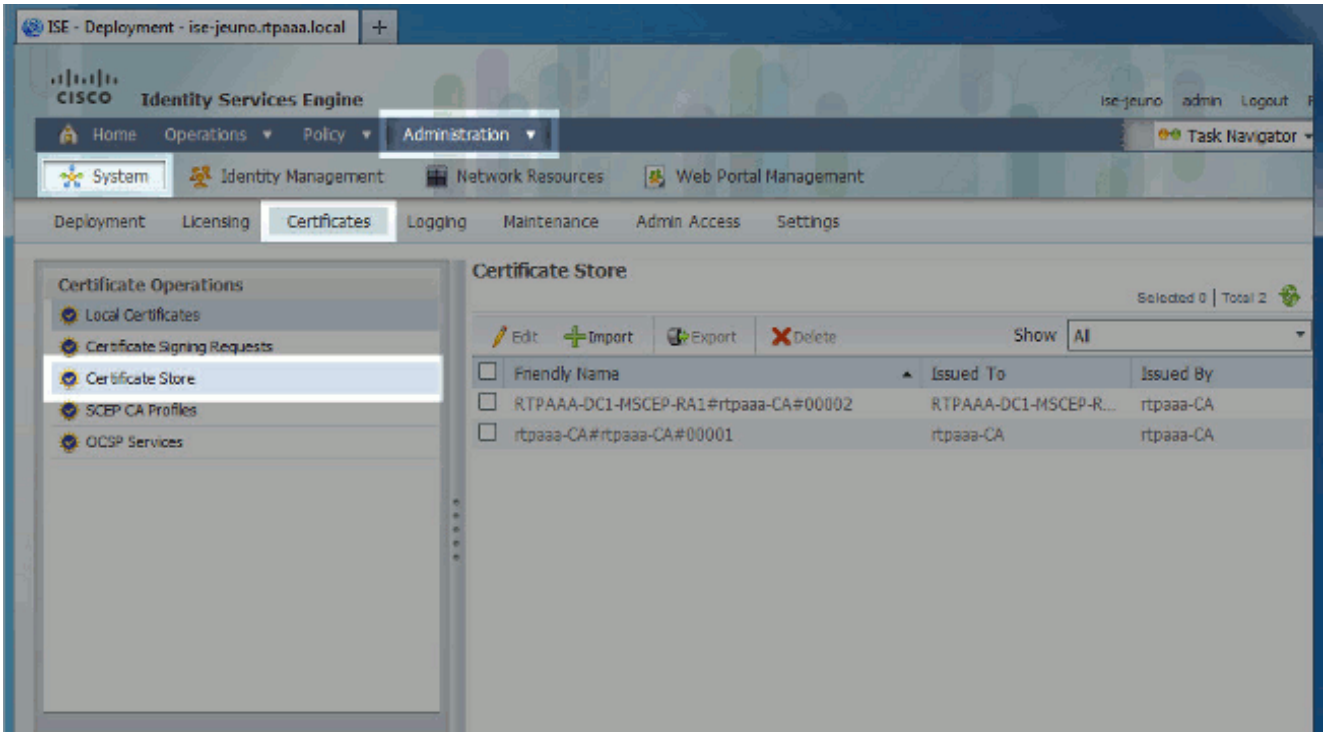
```
Values:
```

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

7. Calcule el período de gracia CRL como sigue:Si CRLOverlapPeriod fue fijado en el paso 5: COINCIDENCIA = CRLOverlapPeriod, en los minutos;: COINCIDENCIA = (CRLPeriod/10), en los minutosSi COINCIDENCIA > entonces COINCIDENCIA 720 = 720Si COINCIDENCIA < (1.5 * COINCIDENCIA de ClockSkewMinutes) entonces = (1.5 * ClockSkewMinutes)Si COINCIDENCIA > CRLPeriod, en la COINCIDENCIA de los minutos entonces = CRLPeriod en los minutosPeríodo de gracia = 720 minutos + 10 minutos = 730 minutosEjemplo:
   ```
   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
   ```

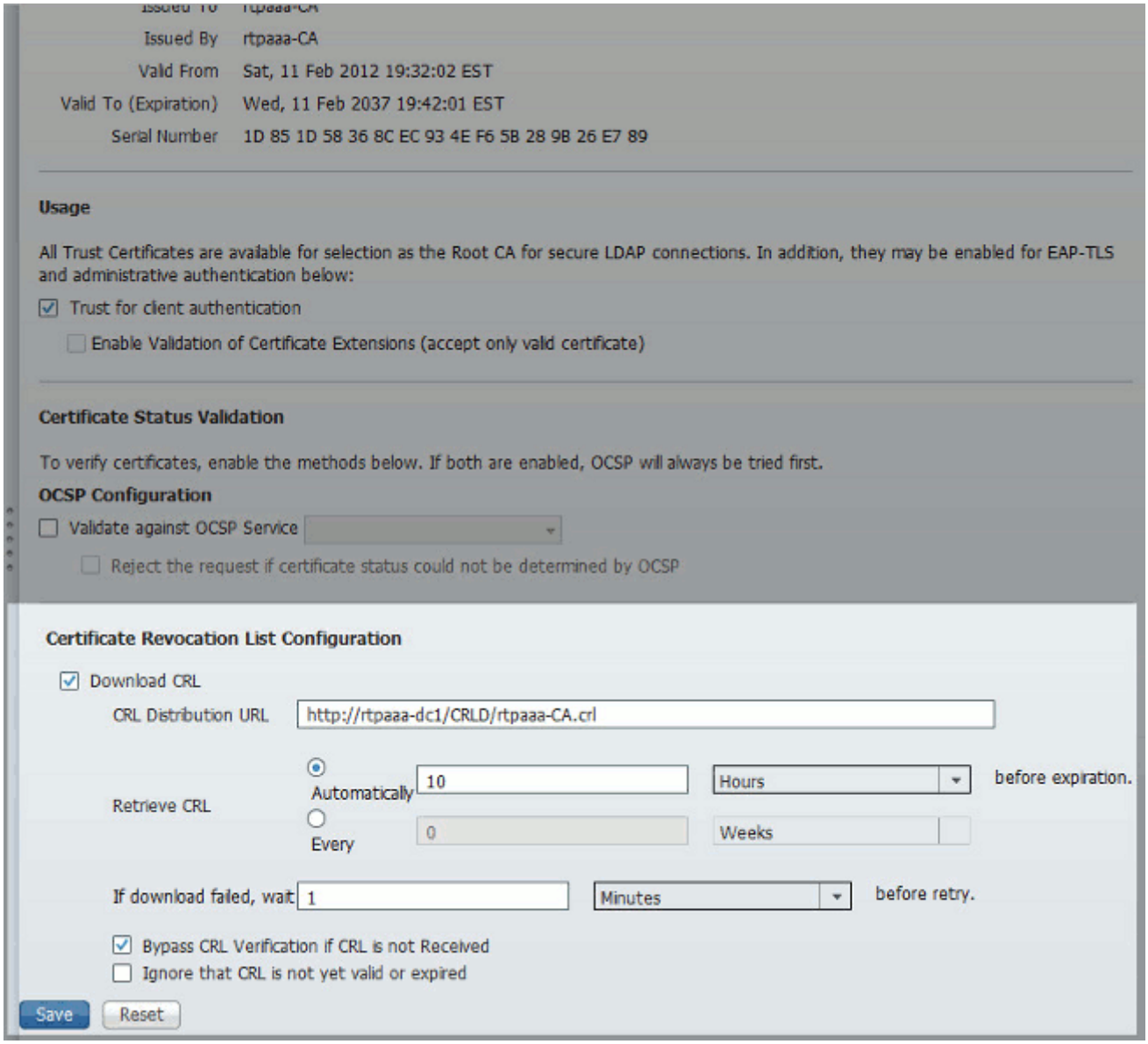
   El período de gracia calculado es la cantidad de tiempo entre cuando el CA publica el CRL siguiente y cuando expira el CRL actual. ISE necesita ser configurado para extraer los CRL por consiguiente.
8. Ábrase una sesión al nodo primario Admin y elija la **administración > el sistema > los Certificados**. En el panel izquierdo, seleccione el **almacén de certificados**.



9. Controle la casilla de verificación del almacén de certificados al lado del certificado CA para el cual usted se prepone configurar los CRL. Haga clic en **Editar**.
10. Cerca de la parte inferior de la ventana, controle la casilla de verificación de la **transferencia directa CRL**.
11. En el campo URL de la distribución CRL, ingrese la trayectoria a la punta de la distribución CRL, que incluye el fichero .crl, creada en la sección 2. En este ejemplo, el URL es:
    ```
    http://RTPAAA-DC1/CRLD/rtpaaa-ca.crl
    ```
12. ISE se puede configurar para extraer el CRL a intervalos regulares o basar en la expiración

(que, es generalmente también un intervalo regular). Cuando el CRL publica se obtiene el intervalo es parásitos atmosféricos, actualizaciones más oportunas CRL cuando se utiliza la última opción. Haga clic **automáticamente el** botón de radio.

13. Fije el valor para la extracción a un valor menos que el período de gracia calculado en el paso 7. Si el valor establecidovalor establecido es más largo que el período de gracia, ISE controla la punta de la distribución CRL antes de que el CA haya publicado el CRL siguiente. En este ejemplo, el período de gracia se calcula para ser 730 minutos, o 12 horas y 10 minutos. Un valor de 10 horas será utilizado para la extracción.
14. Fije el intervalo entre reintentos como apropiado para su entorno. Si ISE no puede extraer el CRL en el intervalo configurado en el paso anterior, revisará en este intervalo más corto.
15. Controle la **verificación de puente CRL si el CRL no es** casilla de verificación **recibida** para permitir que proceda la autenticación certificado-basada normalmente (y sin un control CRL) si ISE no podía extraer el CRL para este CA en su tentativa pasada de la transferencia directa. Si esta casilla de verificación no se controla, toda la autenticación certificado-basada con los Certificados publicados por este CA fallará si el CRL no puede ser extraído.
16. Controle la **negligencia que el CRL no es** casilla de verificación **todavía válida o expirada** permitir que ISE utilice (o no todavía válido) los ficheros expirados CRL como si eran válidos. Si esta casilla de verificación no se controla, ISE considera un CRL ser inválido antes de su fecha de entrada en vigor y después de sus horas de actualización próximas. **Salvaguardia del** tecleo para completar la configuración.



Verificación

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

Troubleshooting

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

Información Relacionada

- Soporte Técnico y Documentación - Cisco Systems