Configurar o Microsoft CA Server para publicar as Listas de Certificados Revogados para ISE

Contents

Introdução

Este documento descreve a configuração de um servidor de Autoridade de Certificação (CA) da Microsoft que executa o IIS (Serviços de Informações da Internet) para publicar as atualizações da Lista de Revogação de Certificados (CRL). Ele também explica como configurar o Cisco Identity Services Engine (ISE) (versões 3.0 e posteriores) para recuperar as atualizações para uso na validação do certificado. O ISE pode ser configurado para recuperar CRLs para os vários certificados raiz de CA que ele usa na validação do certificado.

Pré-requisito

Requisitos

Não existem requisitos específicos para este documento.

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

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

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma

configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Configurar

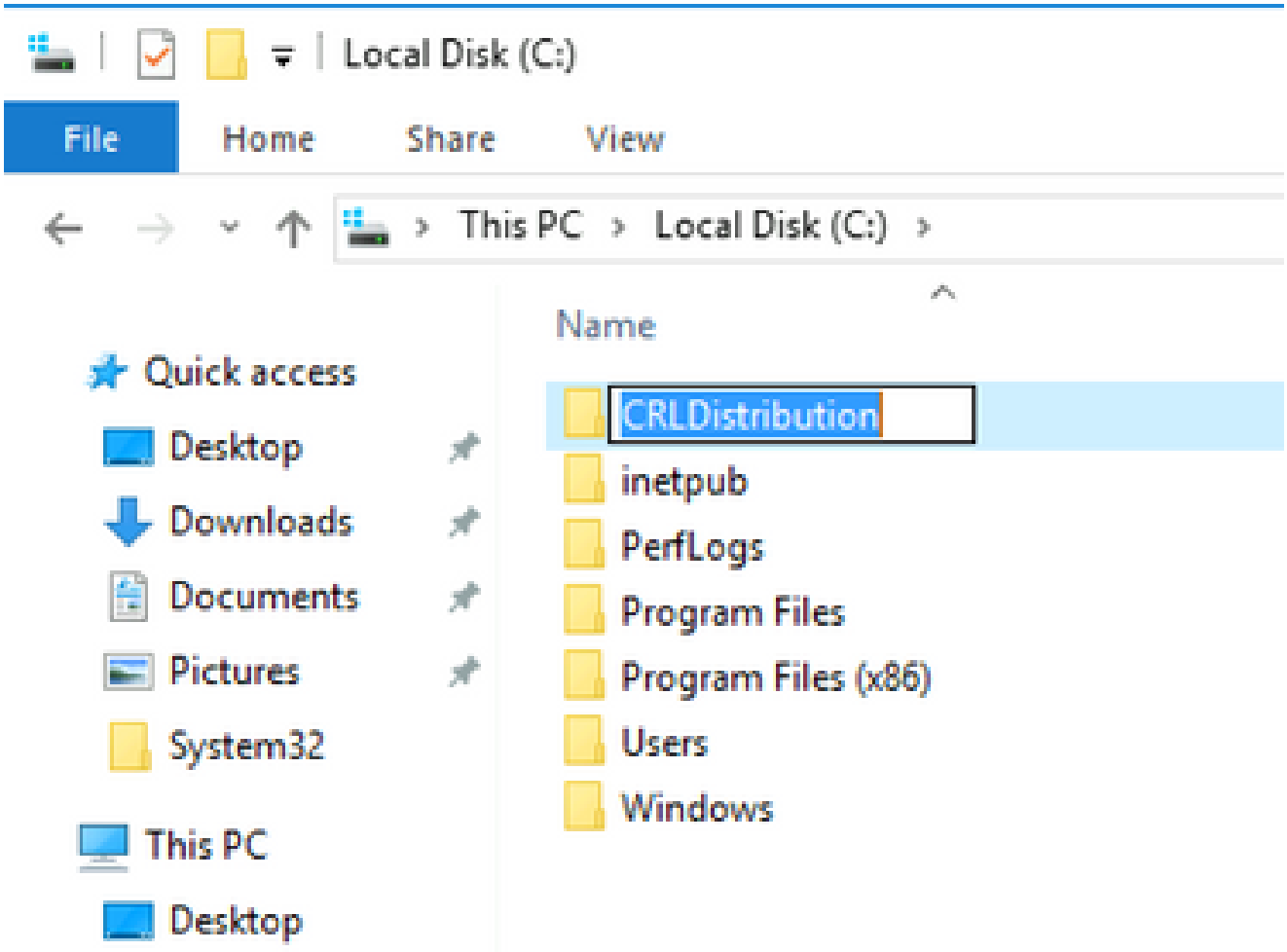
Nesta seção, você encontrará informações para configurar os recursos descritos neste documento.

Criar e Configurar uma Pasta no CA para Armazenar os Arquivos CRL

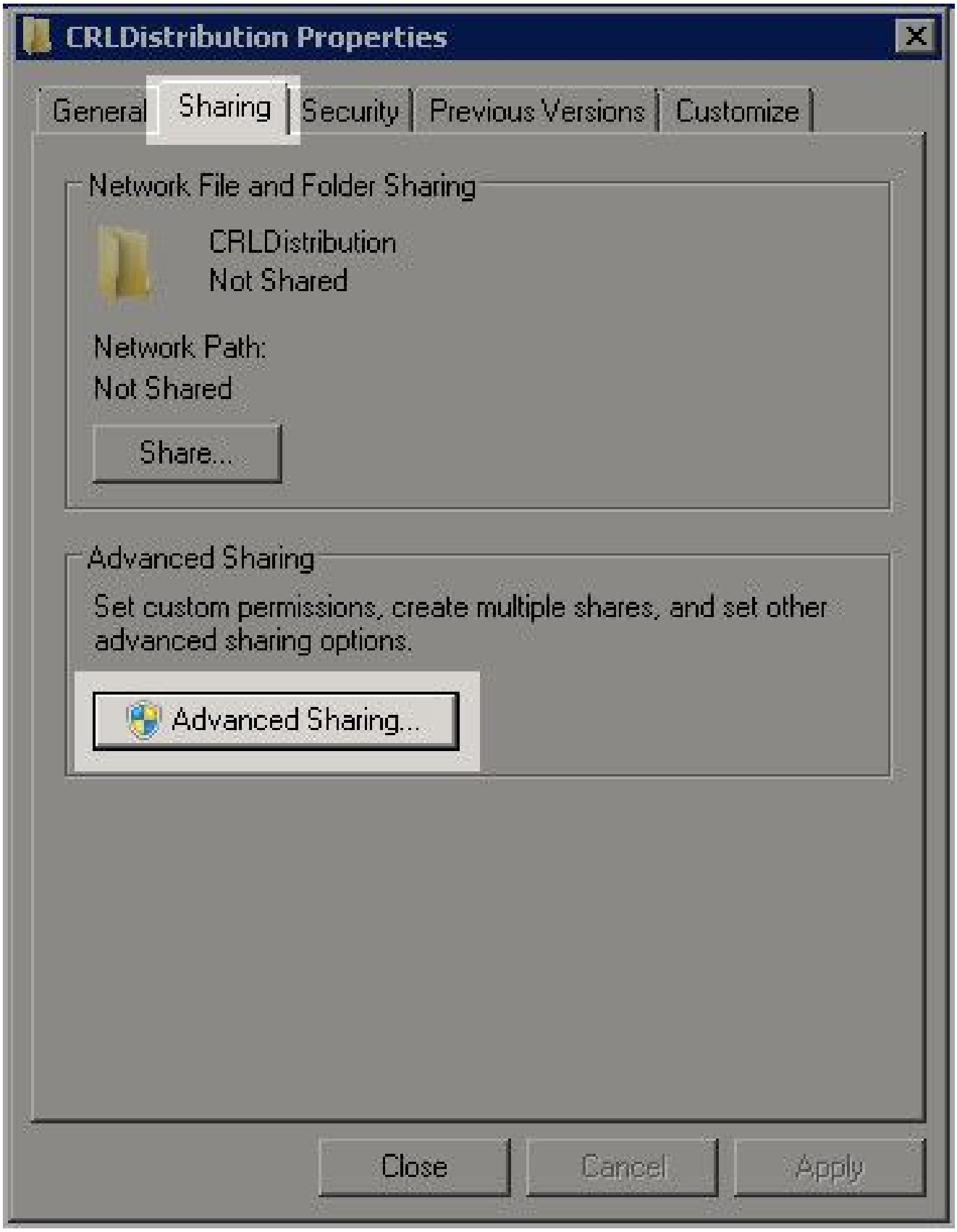
A primeira tarefa é configurar um local no servidor de CA para armazenar os arquivos de CRL. Por padrão, o servidor de autoridade de certificação da Microsoft publica os arquivos em **C:\Windows\system32\CertSrv\CertEnroll**

Em vez de usar essa pasta do sistema, crie uma nova pasta para os arquivos.

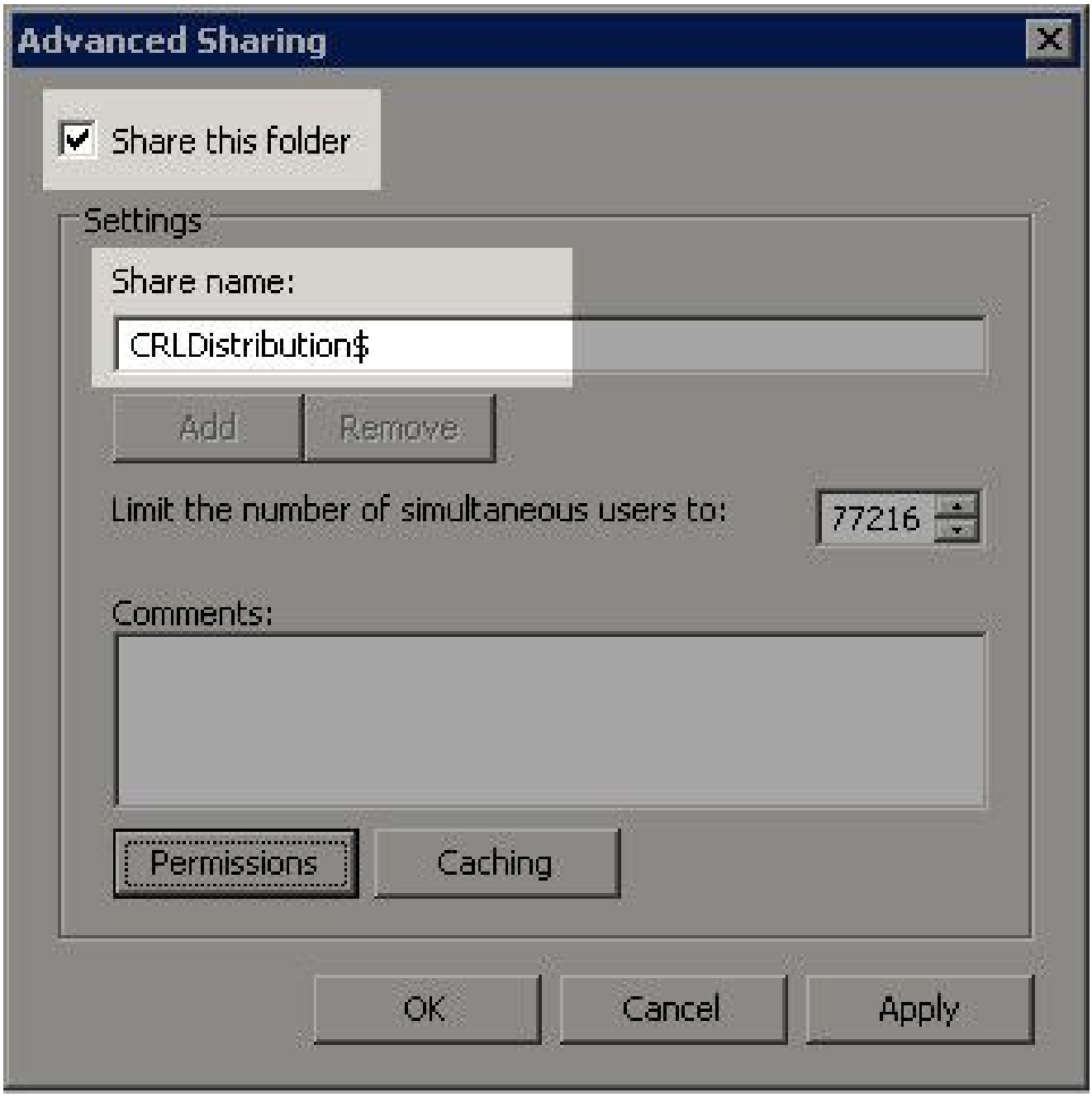
1. No servidor IIS, escolha um local no sistema de arquivos e crie uma nova pasta. Neste exemplo, a pasta **C:\CRLDistribution** é criada.



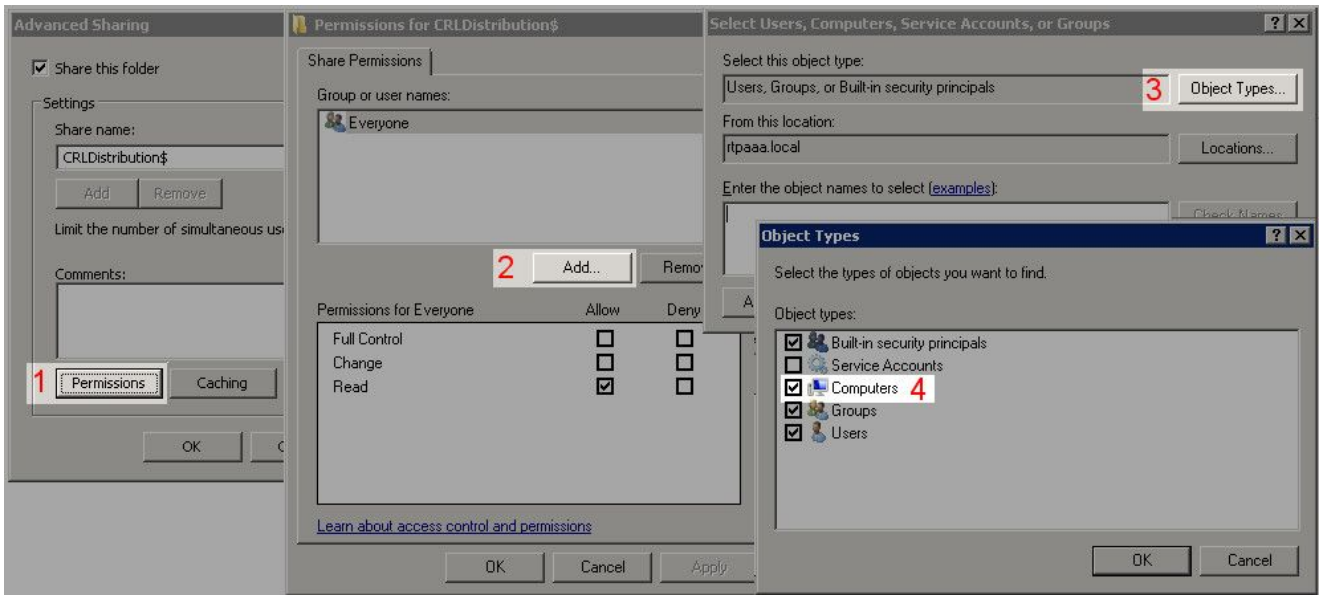
2. Para que a autoridade de certificação grave os arquivos de CRL na nova pasta, o compartilhamento deve estar habilitado. Clique com o botão direito do mouse na nova pasta, escolha **Properties**, clique na **Sharing** guia e clique em **Advanced Sharing**.



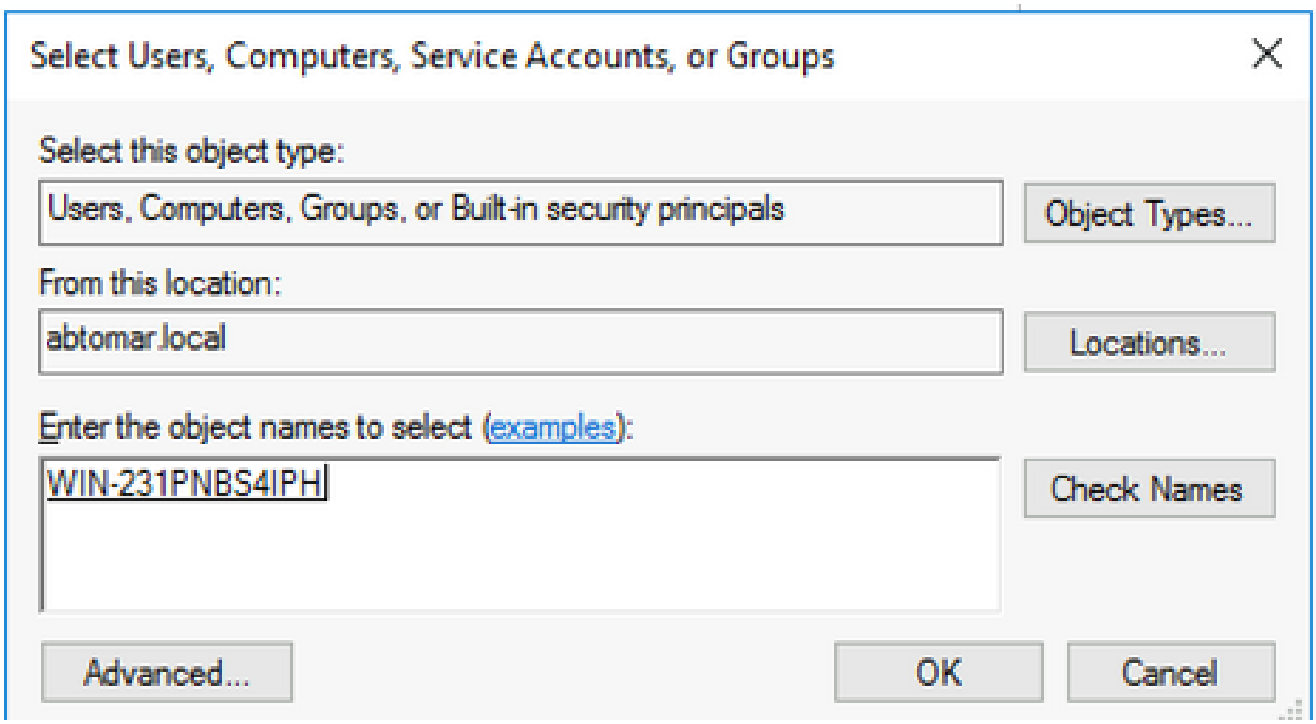
3. **Share this folder** Para compartilhar a pasta, marque a caixa de seleção e adicione um cifrão ($) ao final do nome do compartilhamento no campo Nome do compartilhamento para ocultar o compartilhamento.



4. Clique em **Permissions** (1), clique em **Add** (2), clique em **Object Types** (3) e marque a caixa de seleção **Computers** (4).

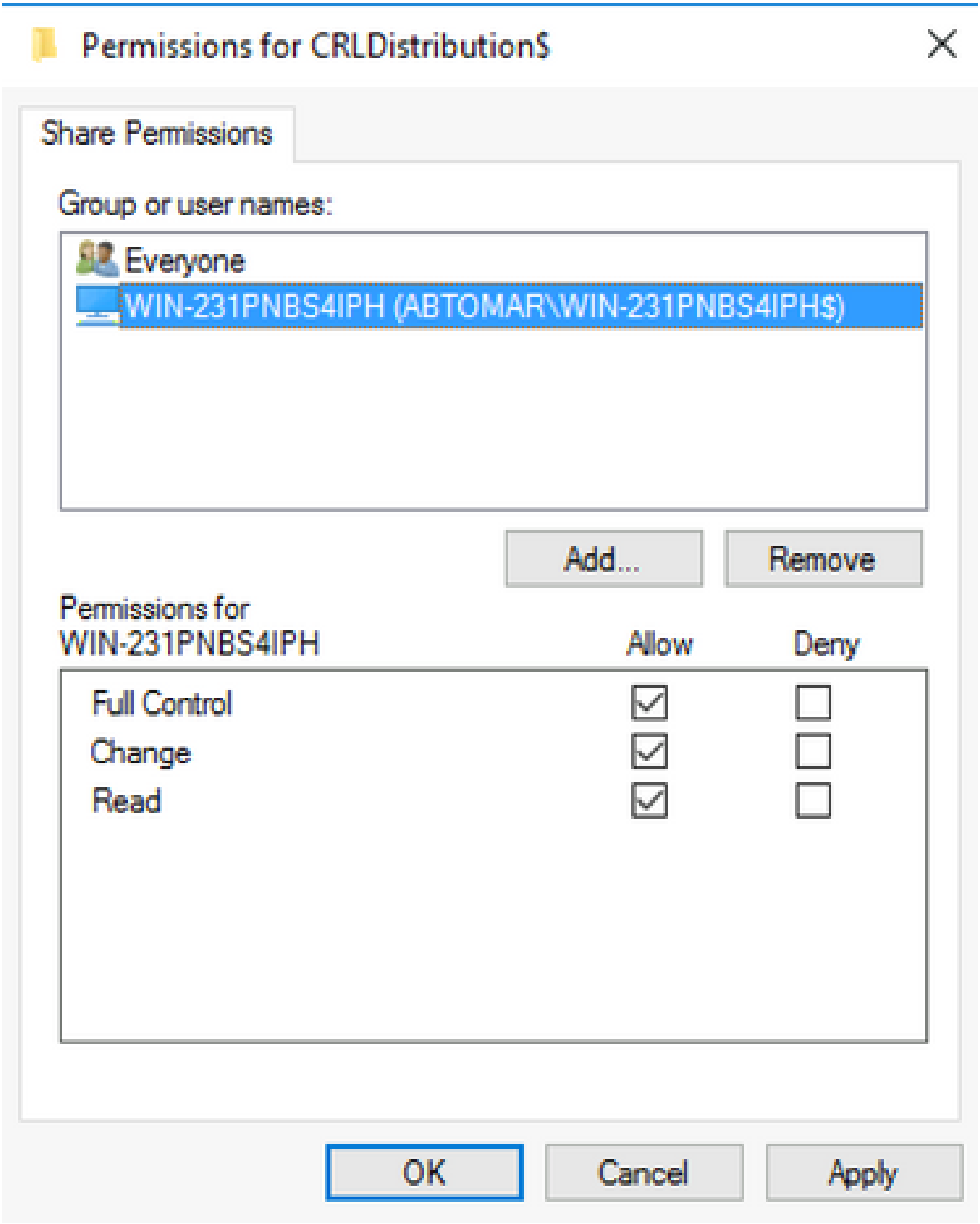


5. Para retornar à janela Selecionar usuários, computadores, contas de serviço ou grupos, clique em **OK**. No campo Digite os nomes dos objetos a serem selecionados, digite o nome do computador do servidor CA neste exemplo: WIN0231PNBS4IPH e clique em **Check Names**. Se o nome inserido for válido, ele será atualizado e aparecerá sublinhado. Clique em **OK**.

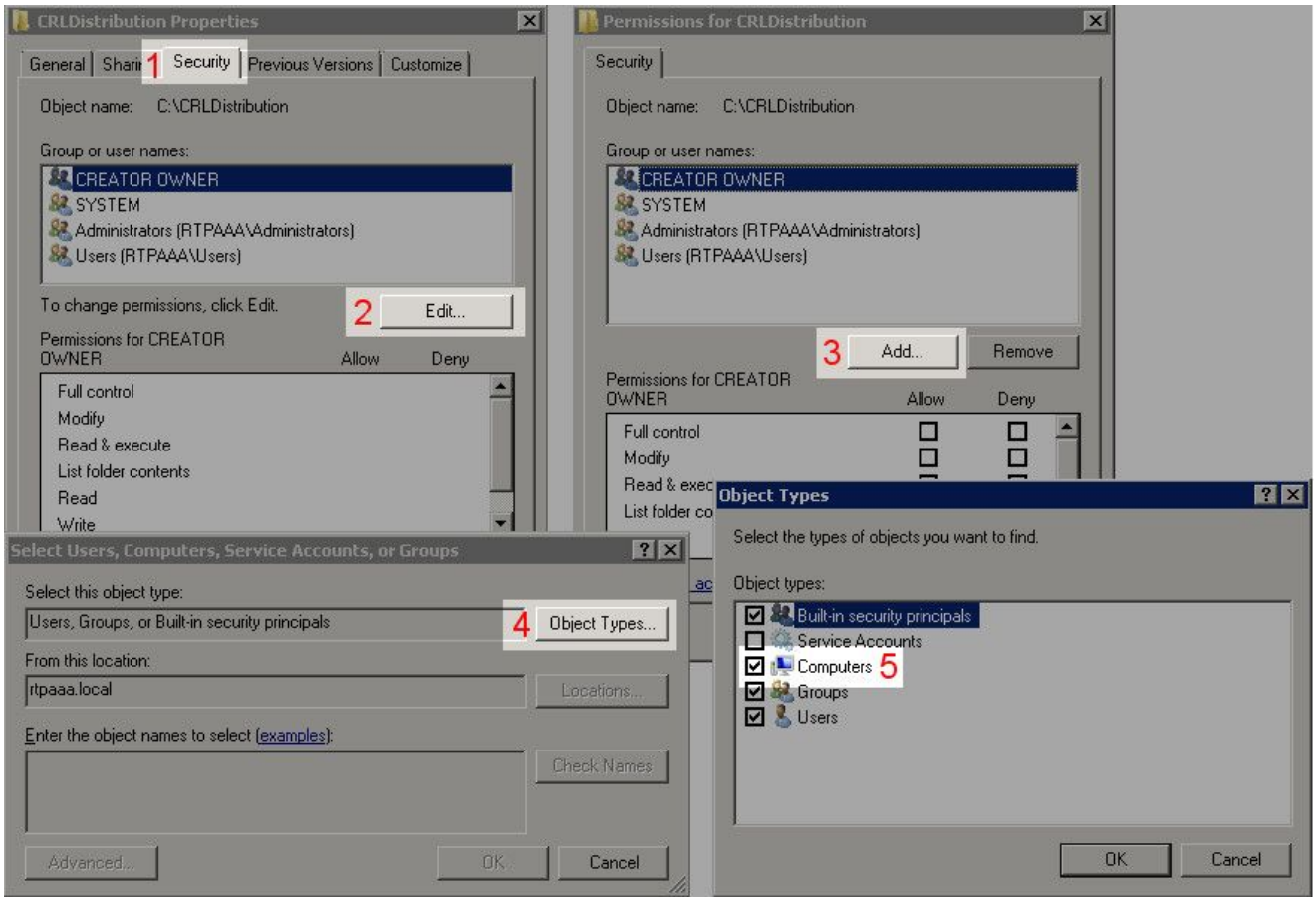


6. No campo Nomes de grupo ou de usuário, escolha o computador da autoridade de certificação. Marque **Allow** Controle Total para conceder acesso total à CA.

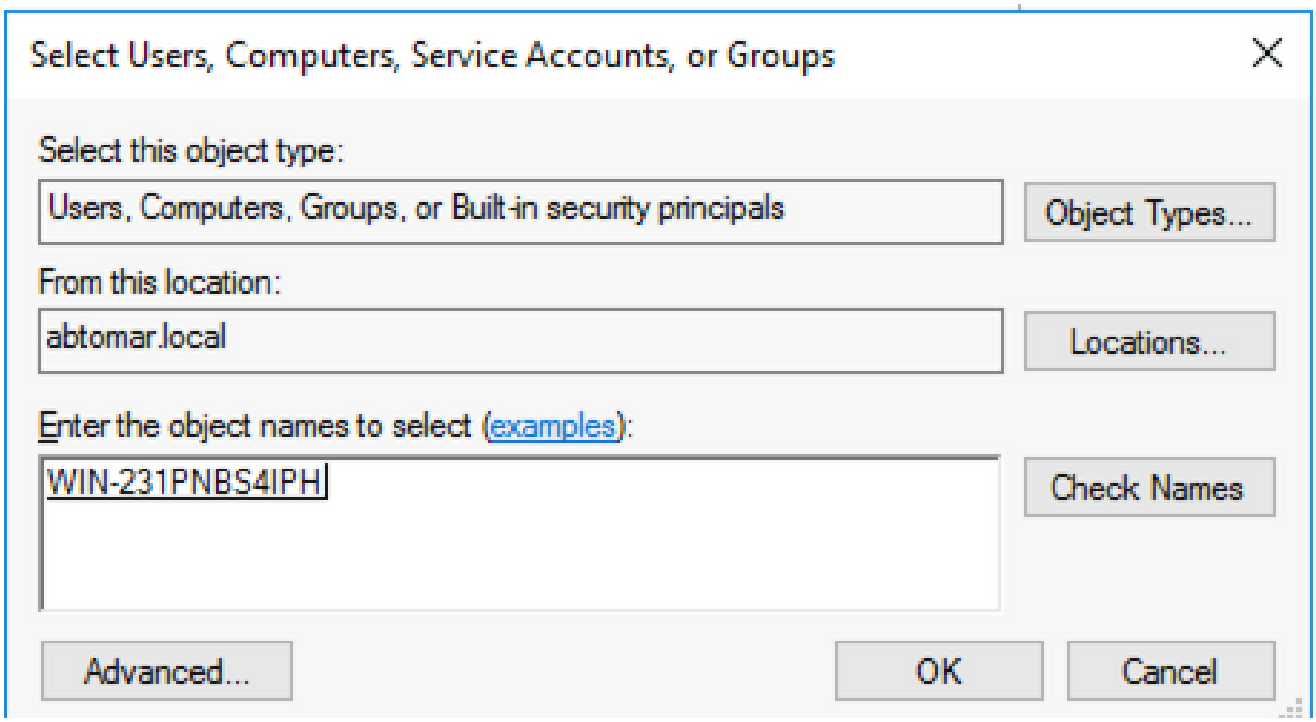
Clique em **OK**. Clique **OK** novamente para fechar a janela Compartilhamento Avançado e retornar à janela Propriedades.



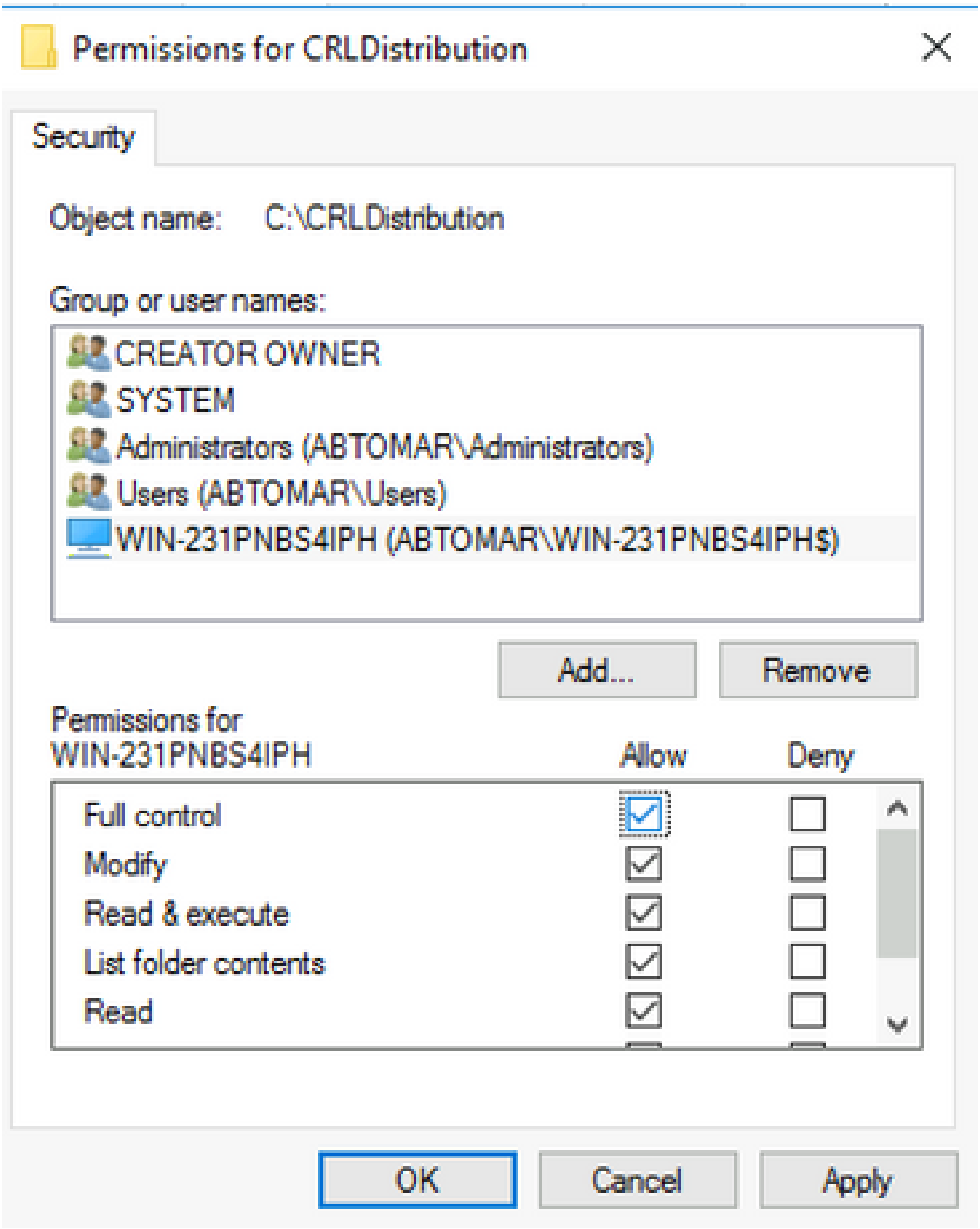
7. Para permitir que a CA grave os arquivos CRL na nova pasta, configure as permissões de segurança apropriadas. Clique na guia (1),**Security** clique em **Edit** (2), clique em **Add** (3), clique em **Object Types** (4) e marque a caixa de seleção (5). Marque **Computers** a caixa de seleção.



8. No campo Digite os nomes dos objetos a serem selecionados, digite o nome do computador do servidor CA e clique em **Check Names**. Se o nome inserido for válido, ele será atualizado e aparecerá sublinhado. Clique em **OK**.



9. Escolha o computador da autoridade de certificação no campo Nomes de grupo ou de usuário e, em seguida, verifique **Allow** Controle total para conceder acesso total à autoridade de certificação. Clique em **OK** e em **Close** para concluir a tarefa.

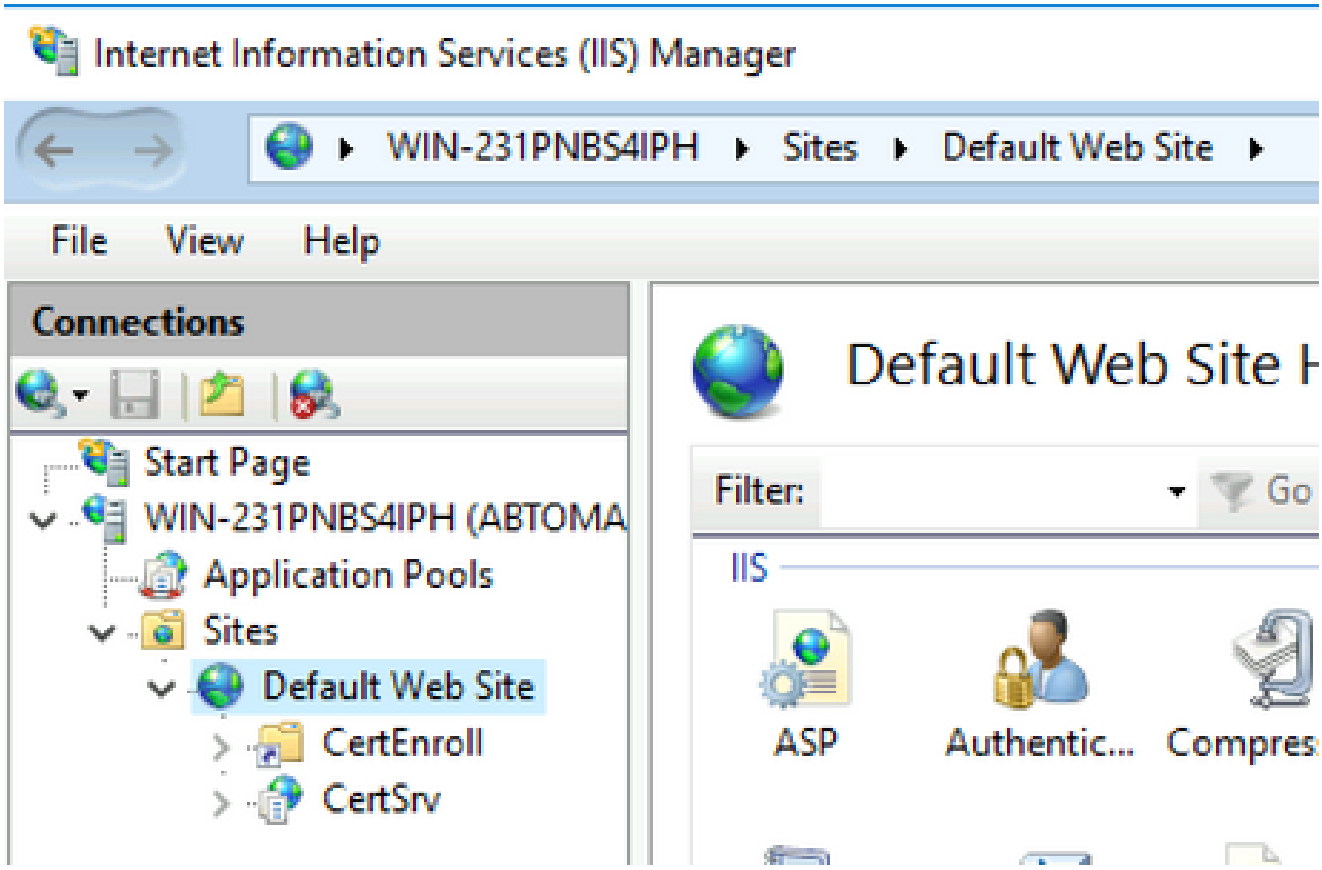


Criar um Site no IIS para Expor o Novo Ponto de Distribuição de CRL

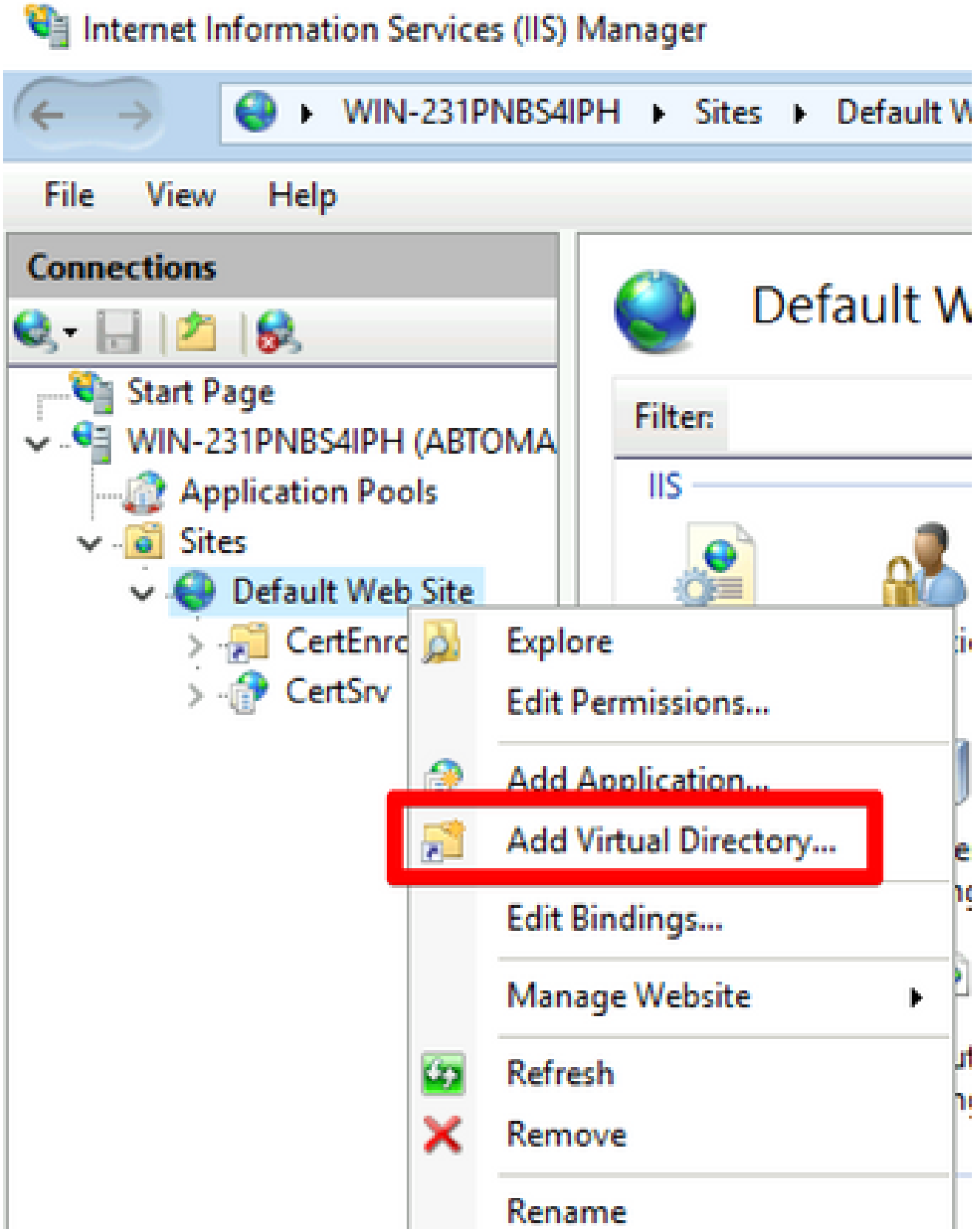
Para que o ISE acesse os arquivos CRL, torne o diretório que hospeda os arquivos CRL acessível via IIS.

1. Na barra de tarefas do servidor IIS, clique em **Start**. Escolha **Administrative Tools** > **Internet Information Services (IIS) Manager**.

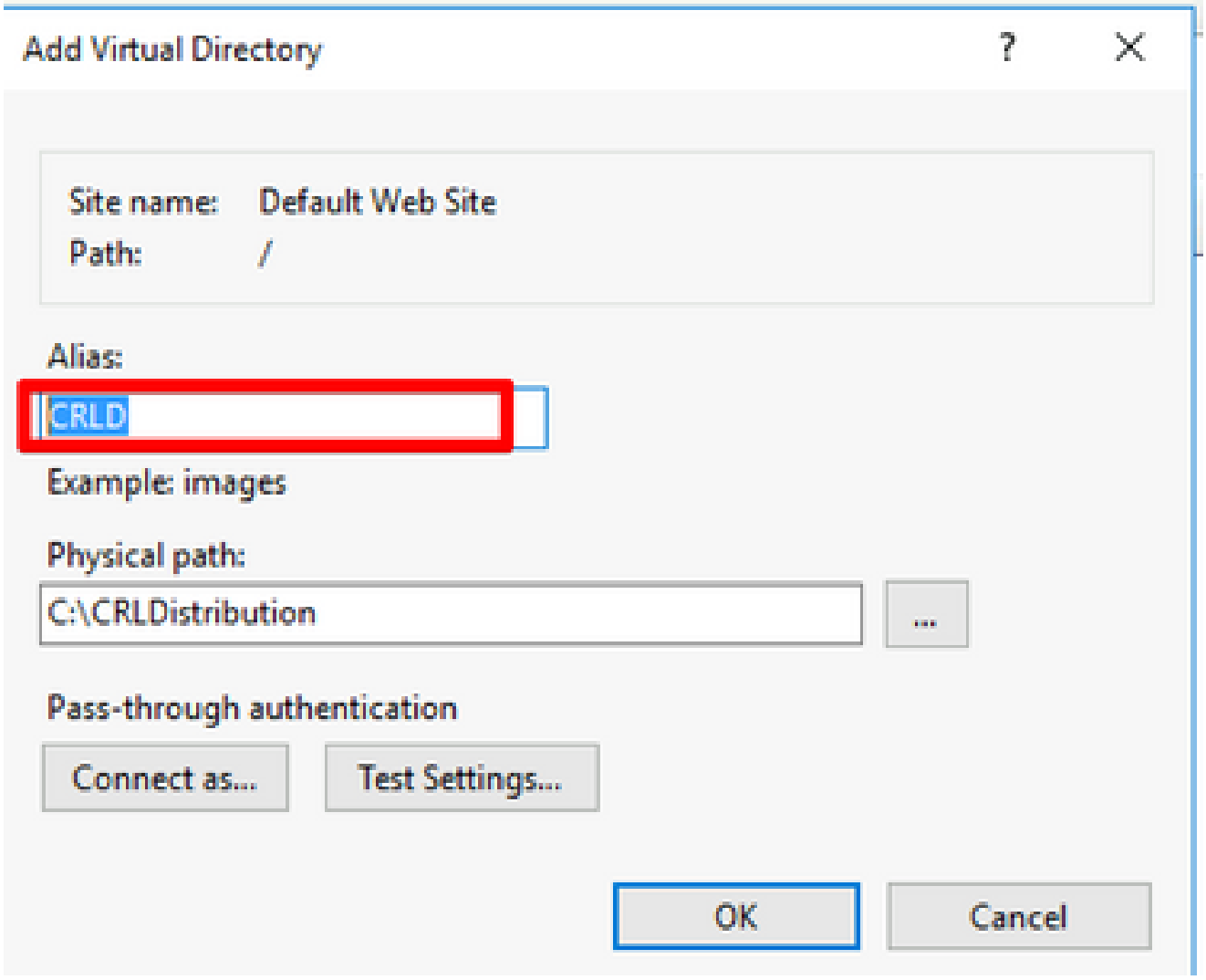
2. No painel esquerdo (conhecido como Árvore do Console), expanda o nome do servidor IIS e, em seguida, expanda **Sites**.



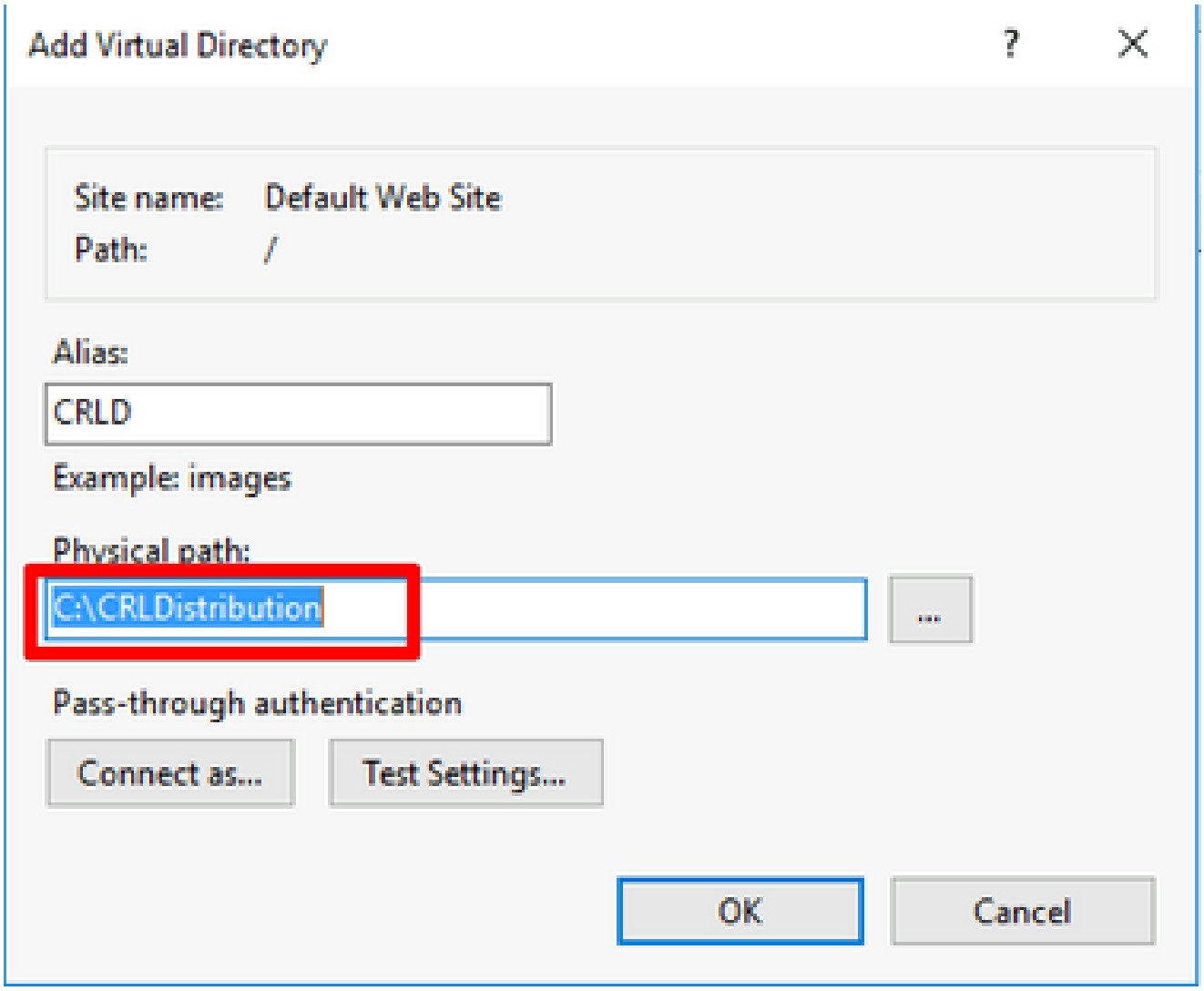
3. Clique com o botão direito do mouse **Default Web Site** e escolha **Add Virtual Directory**, conforme mostrado nesta imagem.



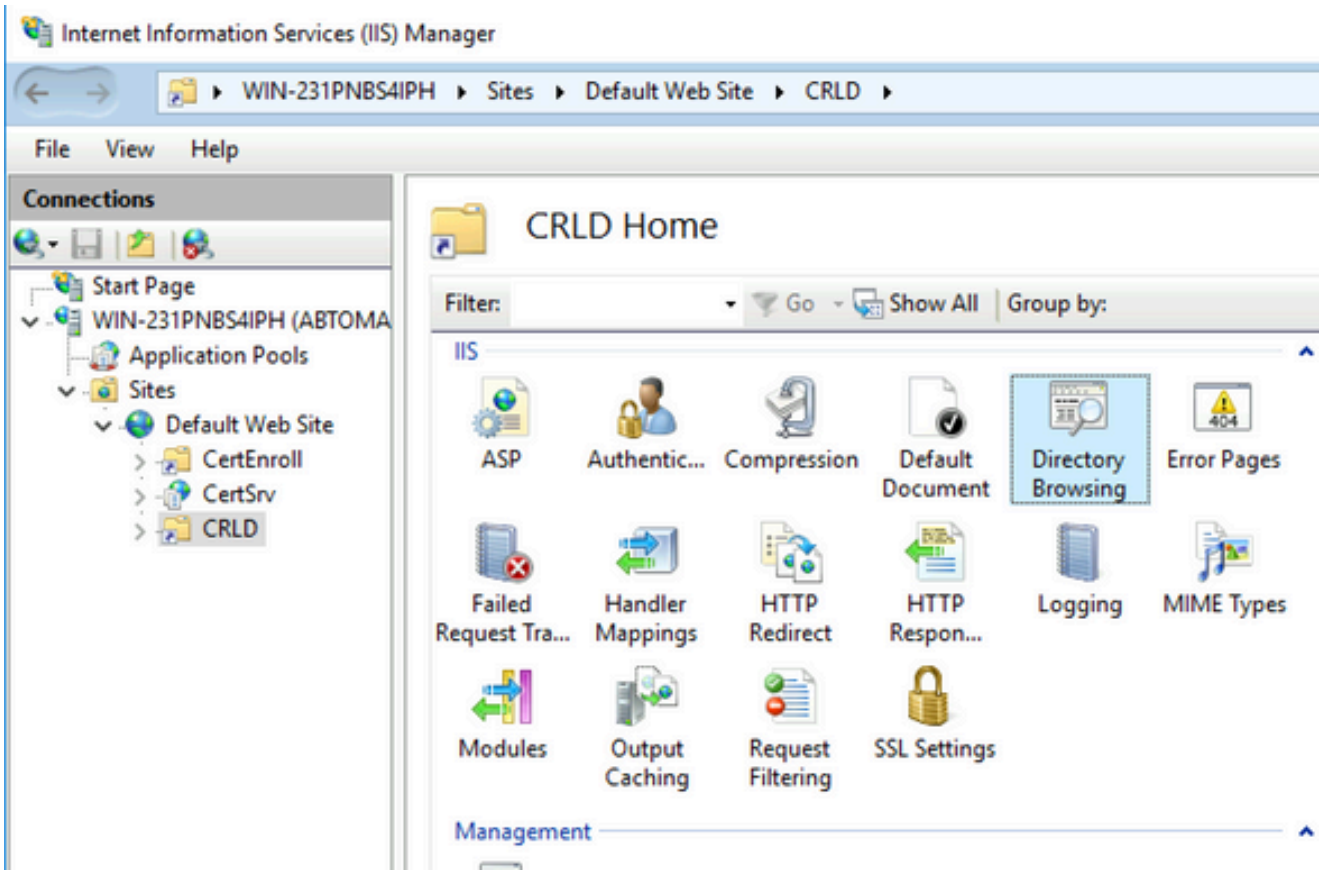
4. No campo Alias, insira um nome de site para o Ponto de Distribuição da CRL. Neste exemplo, o CRLD é inserido.



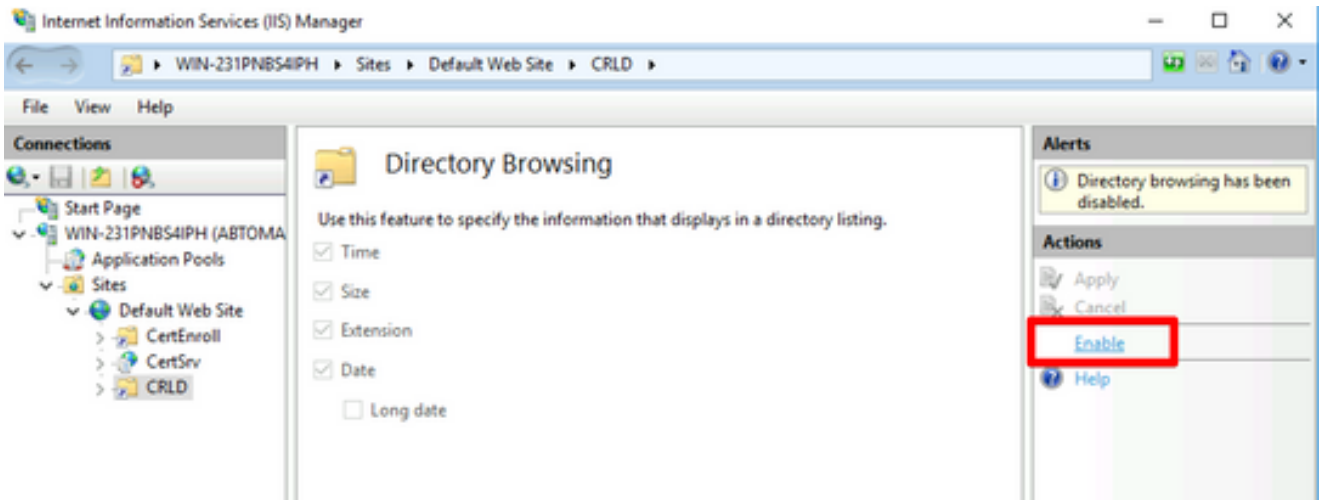
5. Clique nas reticências (. . .) à direita do campo Caminho físico e navegue até a pasta criada na seção 1. Selecione a pasta e clique em OK. Clique OK para fechar a janela Adicionar Diretório Virtual.



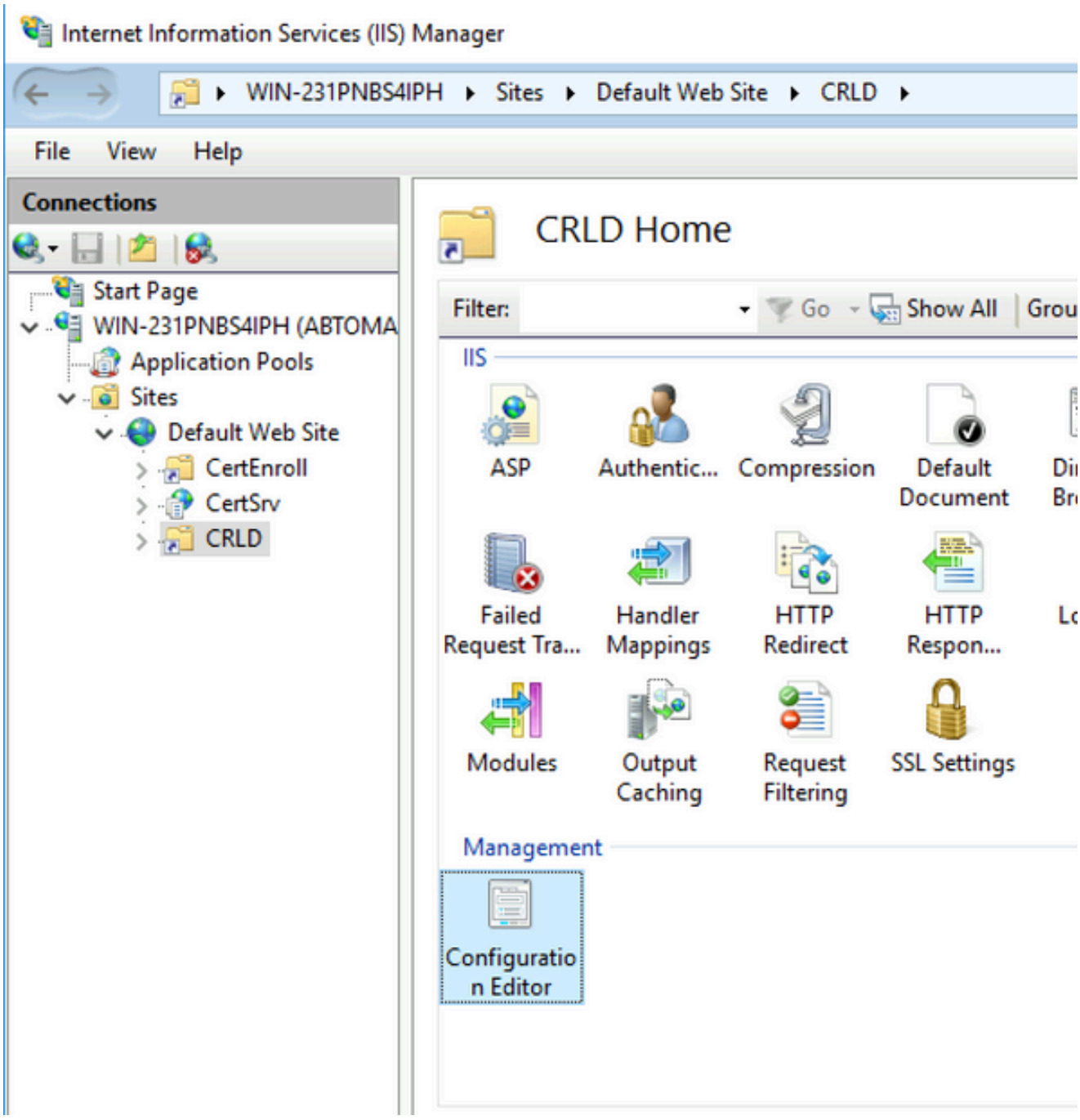
6. O nome do site inserido na etapa 4 deve ser realçado no painel esquerdo. Caso contrário, escolha-o agora. No painel central, clique duas vezes em **Directory Browsing**.



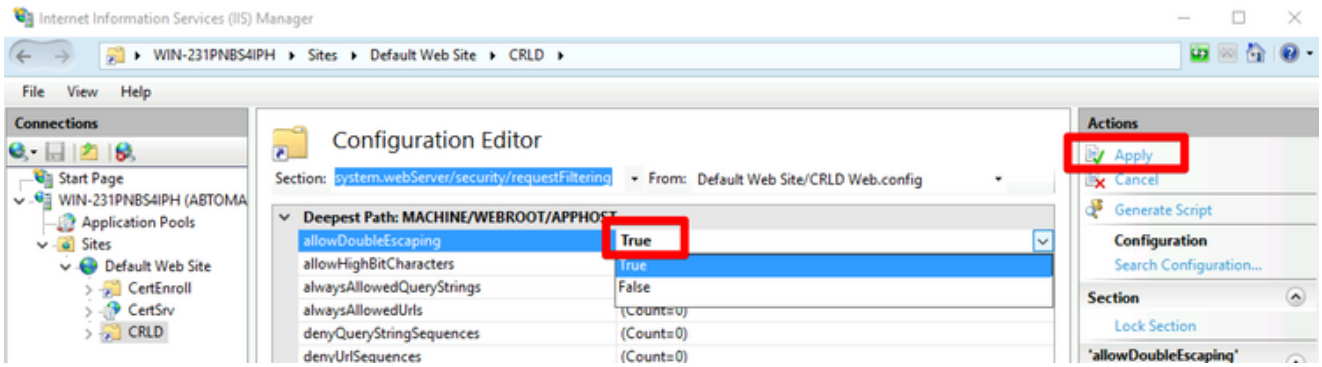
7. No painel direito, clique em **Enable** para habilitar a navegação no diretório.



8. No painel esquerdo, escolha novamente o nome do site. No painel central, clique duas vezes em **Configuration Editor**.



9. Na lista suspensa Seção, escolha **system.webServer/security/requestFiltering**. Na lista suspensa**allowDoubleEscaping**, escolha **True**. No painel direito, clique em **Apply**, conforme mostrado nesta imagem.

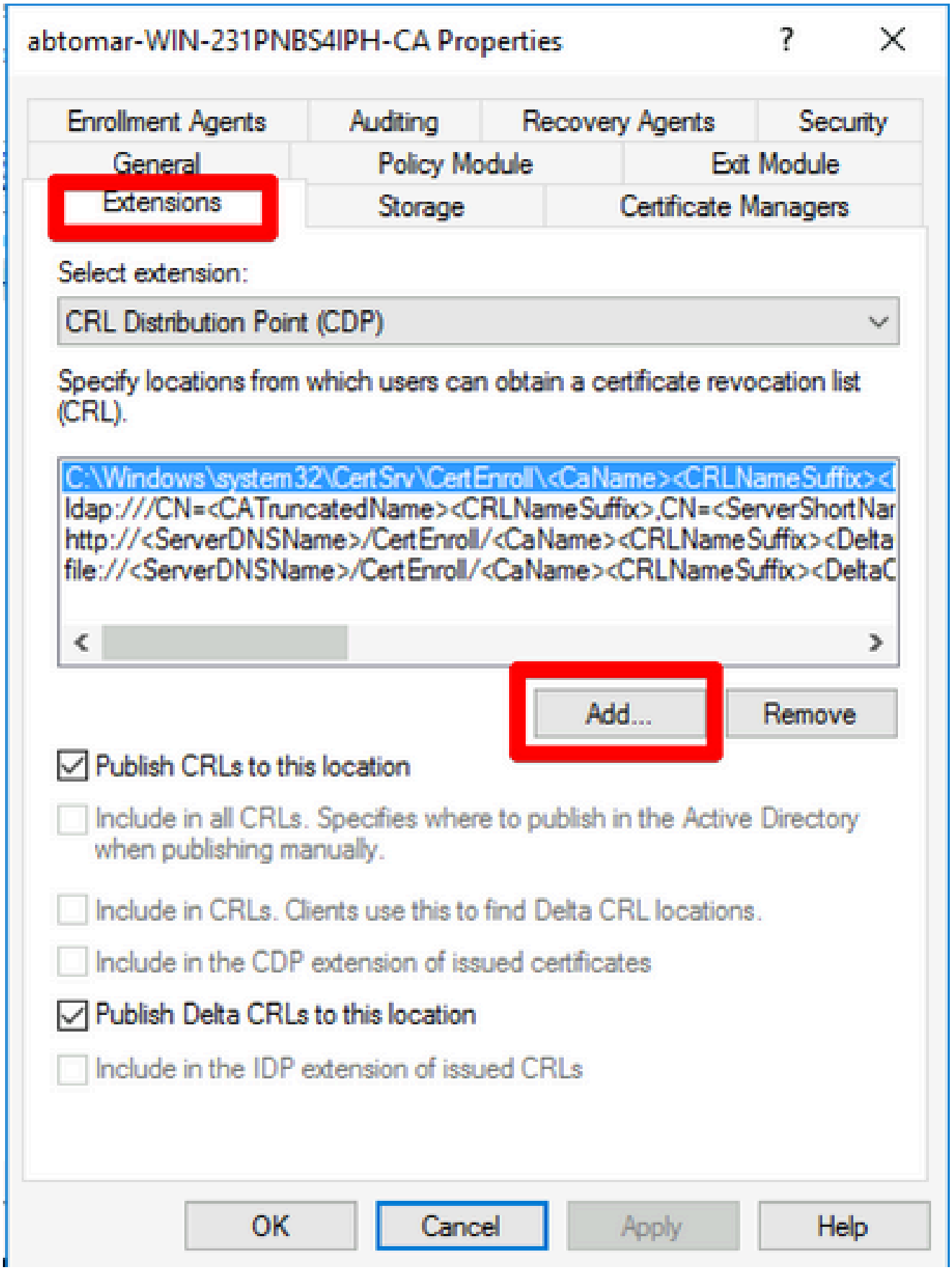


A pasta deve agora estar acessível via IIS.

Configurar o Microsoft CA Server para Publicar Arquivos CRL no Ponto de Distribuição

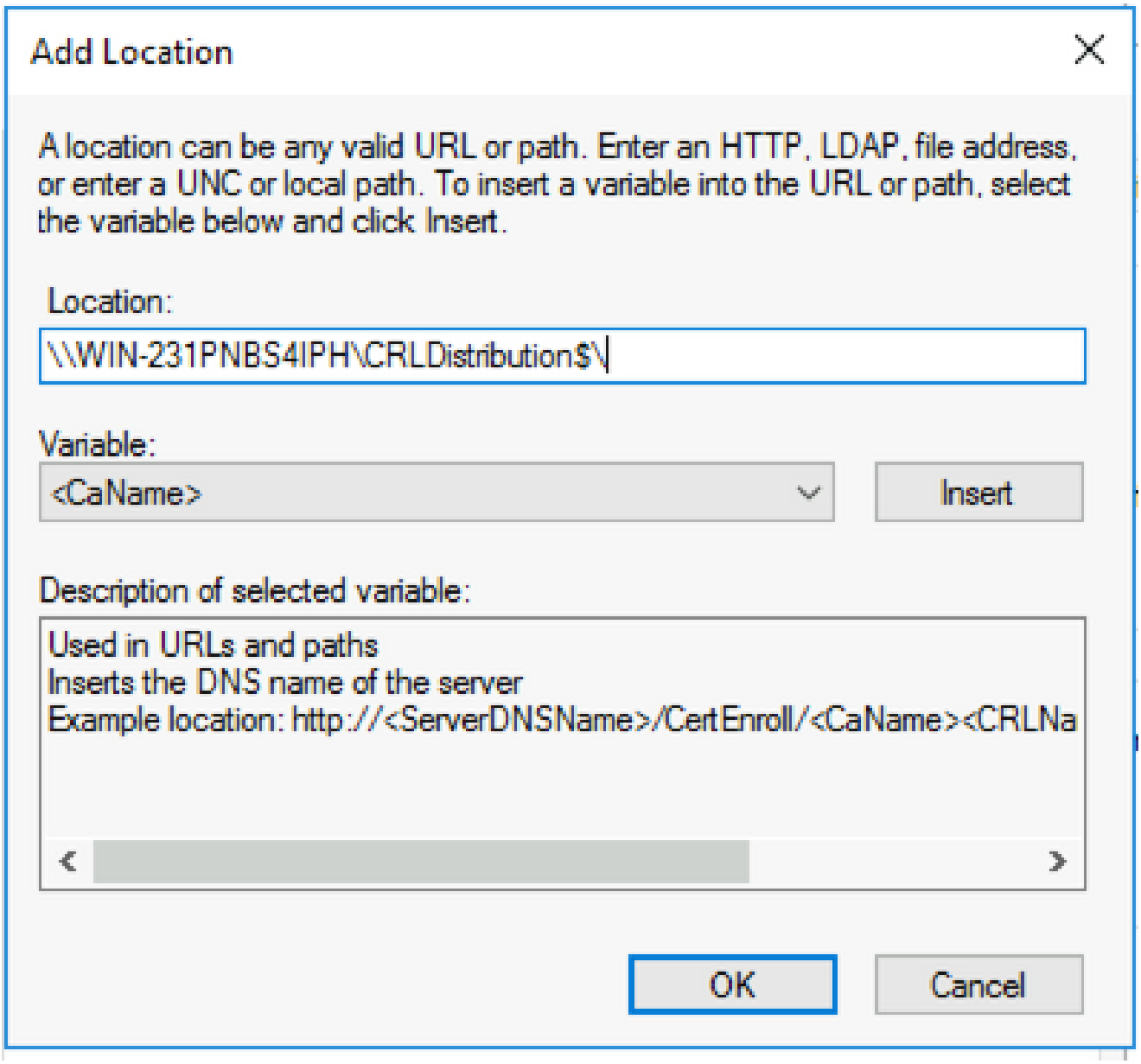
Agora que uma nova pasta foi configurada para hospedar os arquivos de CRL e a pasta foi exposta no IIS, configure o servidor de CA da Microsoft para publicar os arquivos de CRL no novo local.

1. Na barra de tarefas do servidor de CA, clique em **Start**. Escolha **Administrative Tools** > **Certificate Authority**.
2. No painel esquerdo, clique com o botão direito do mouse no nome da CA. Escolha **Properties** e clique na **Extensions** guia . Para adicionar um novo ponto de distribuição de CRL, clique em **Add**.

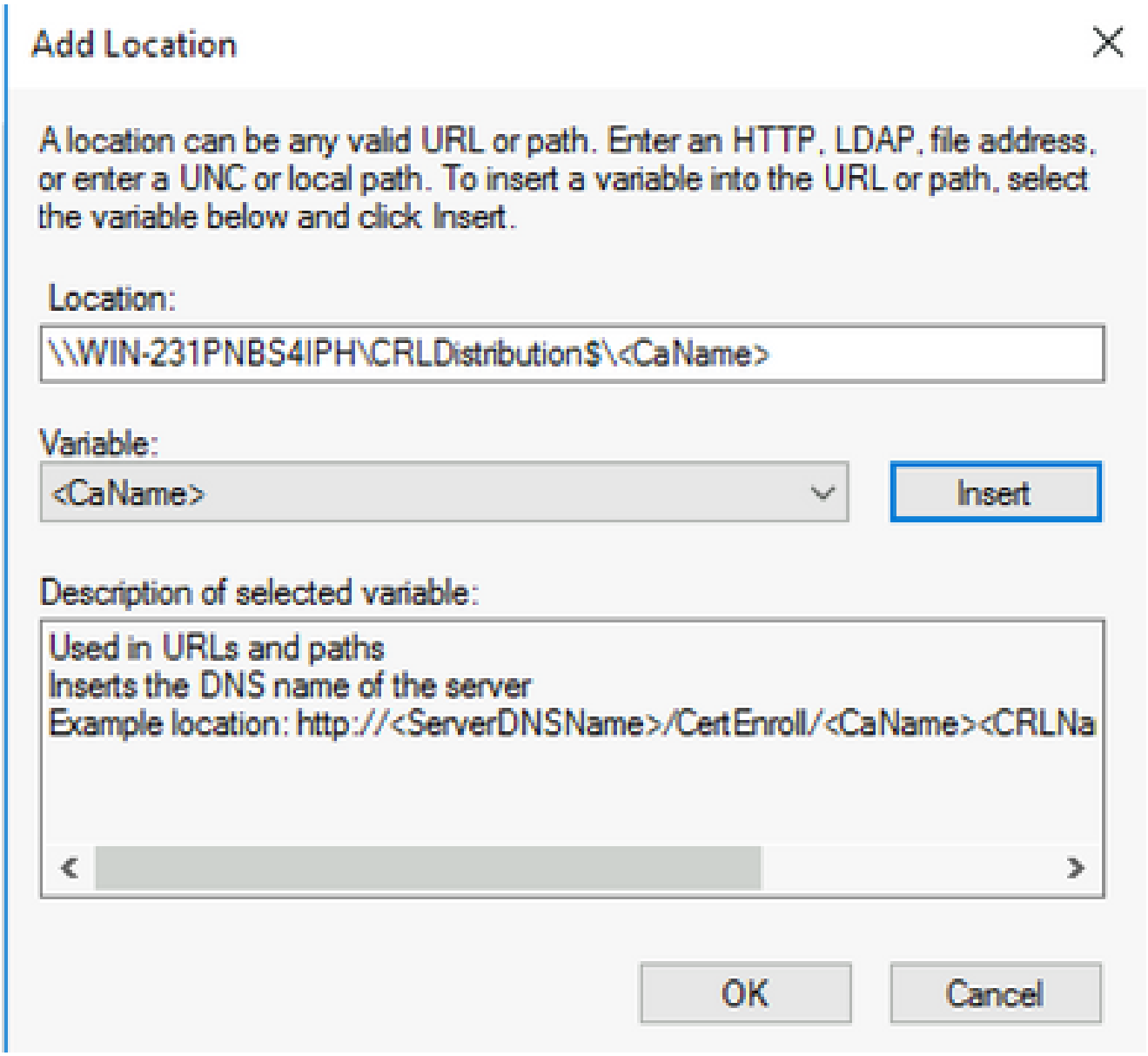


3. No campo Local, insira o caminho para a pasta criada e compartilhada na seção 1. No exemplo na seção 1, o caminho é:

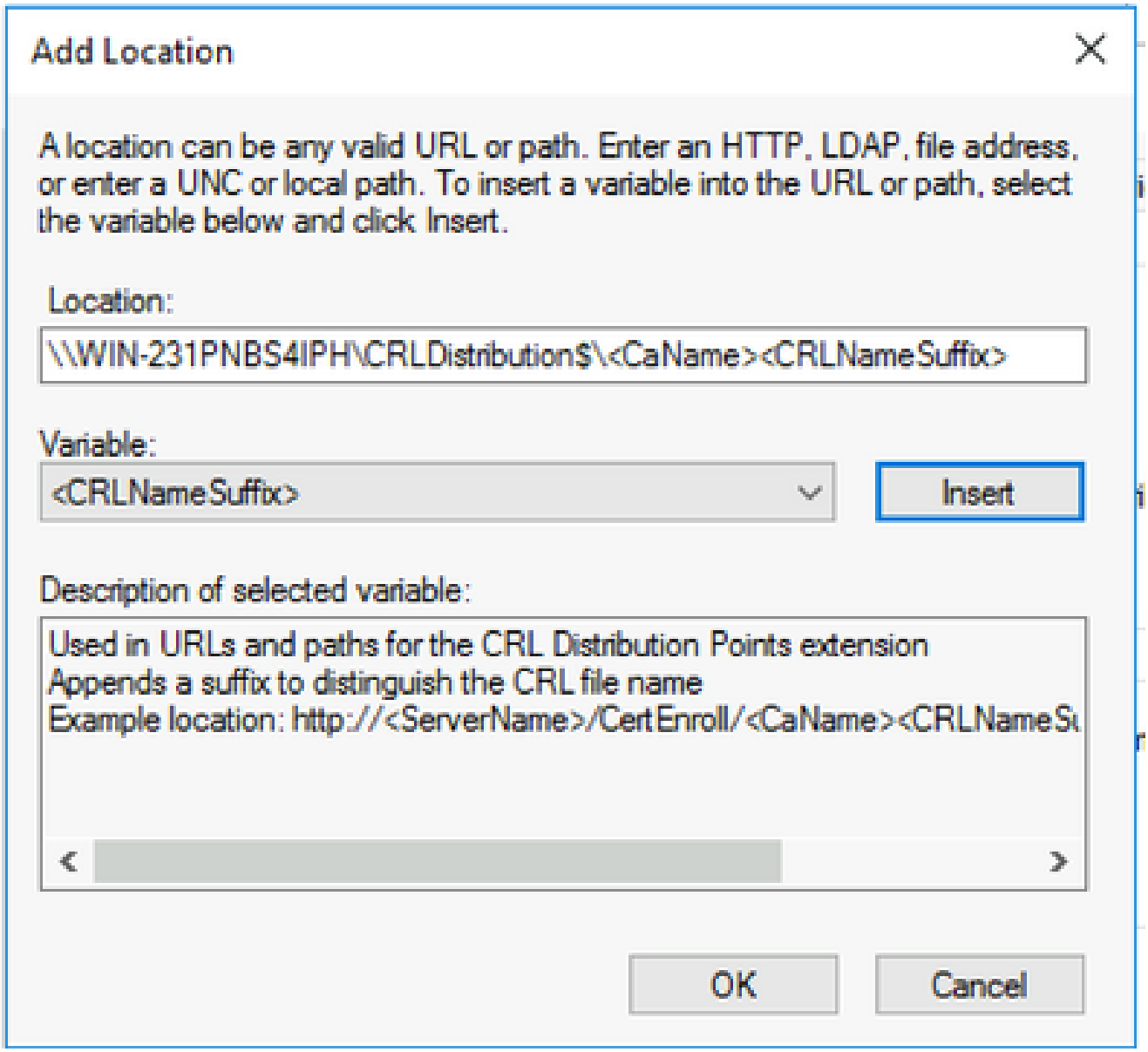
\\WIN-231PNBS4IPH\CRLDistribution$



4. Com o campo Local preenchido, escolha na lista suspensa Variável e clique em **Insert**.



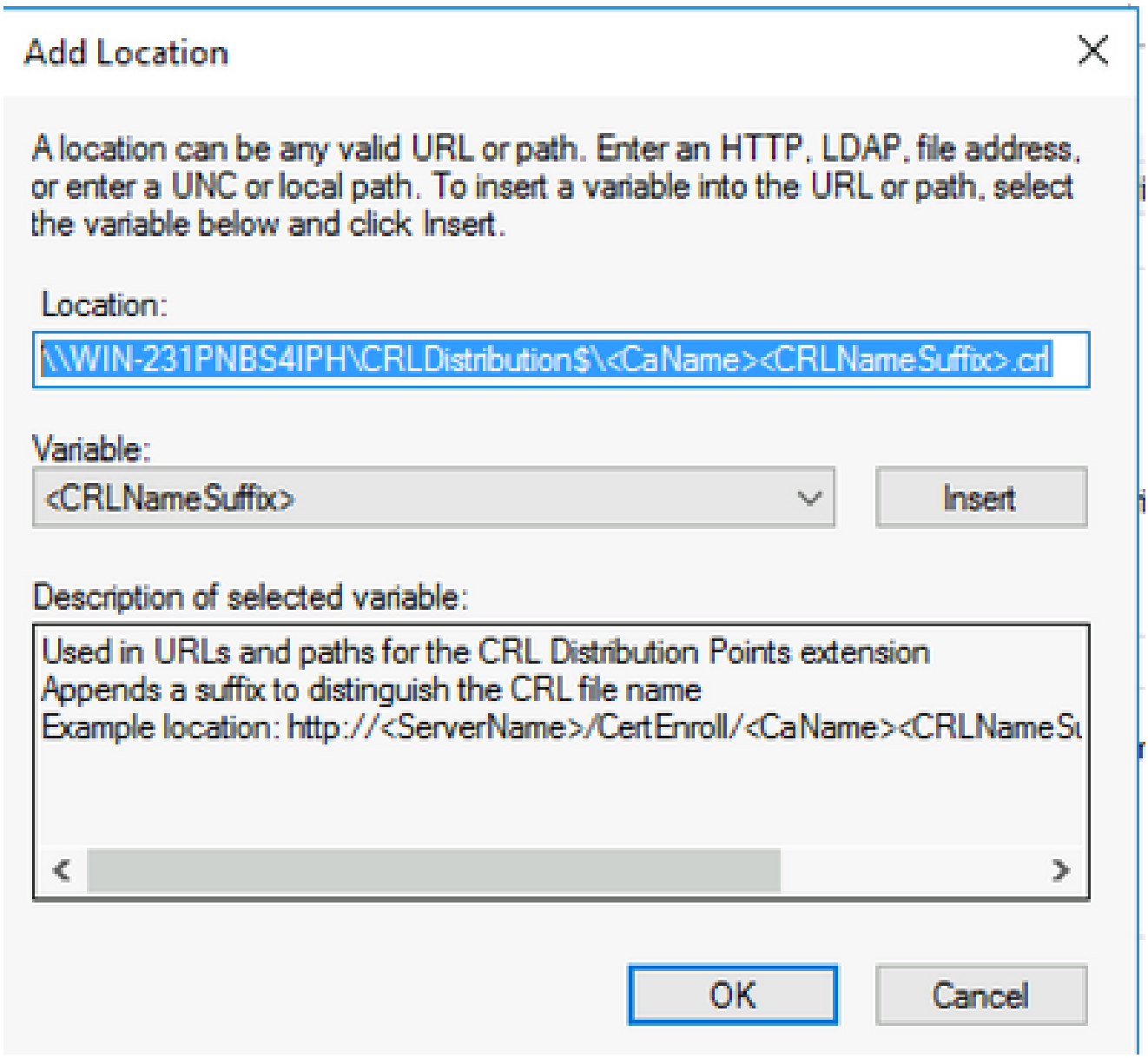
5. Na lista suspensa Variável, escolha
e clique em **Insert**.



6. No campo Local, anexe **.crl** ao final do caminho. Neste exemplo, o Local é:

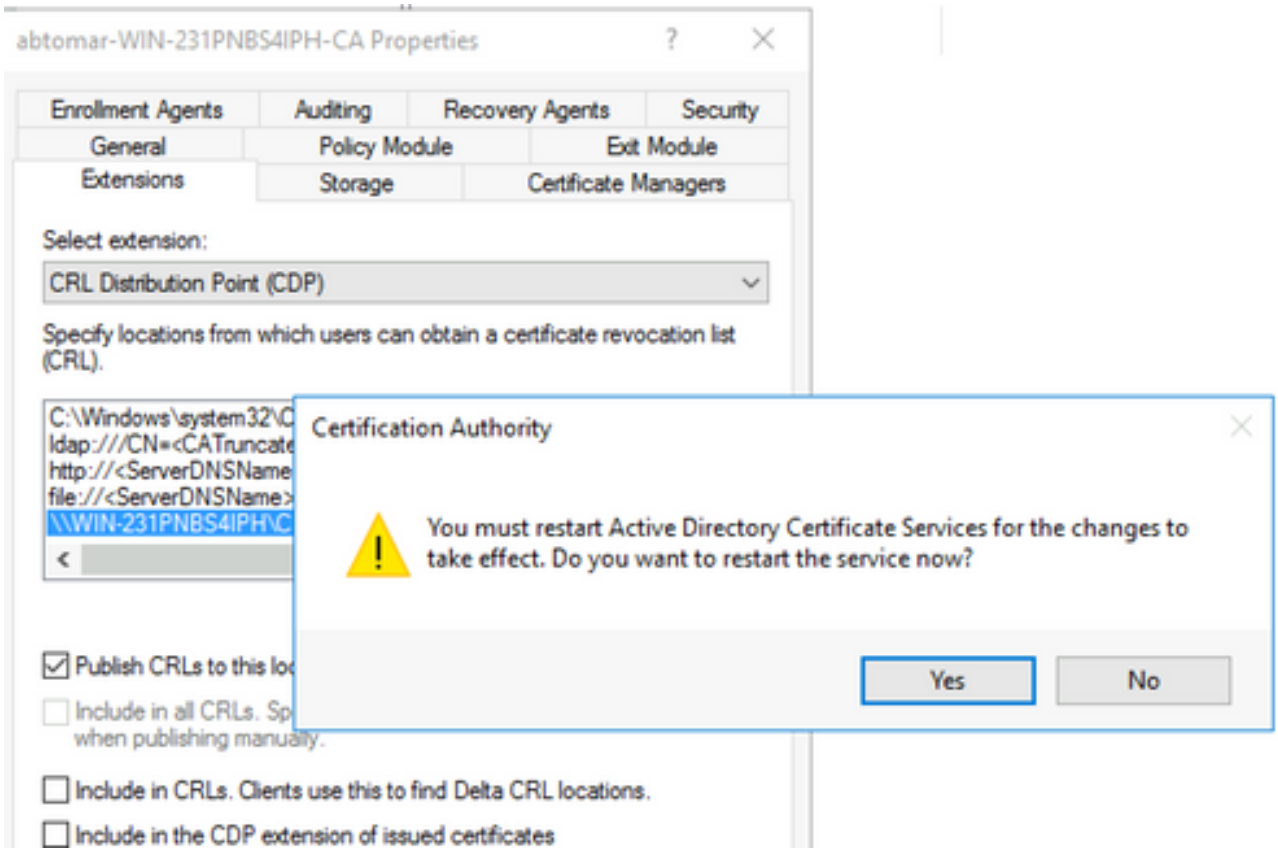
\\WIN-231PNBS4IPH\CRLDistribution$

.crl

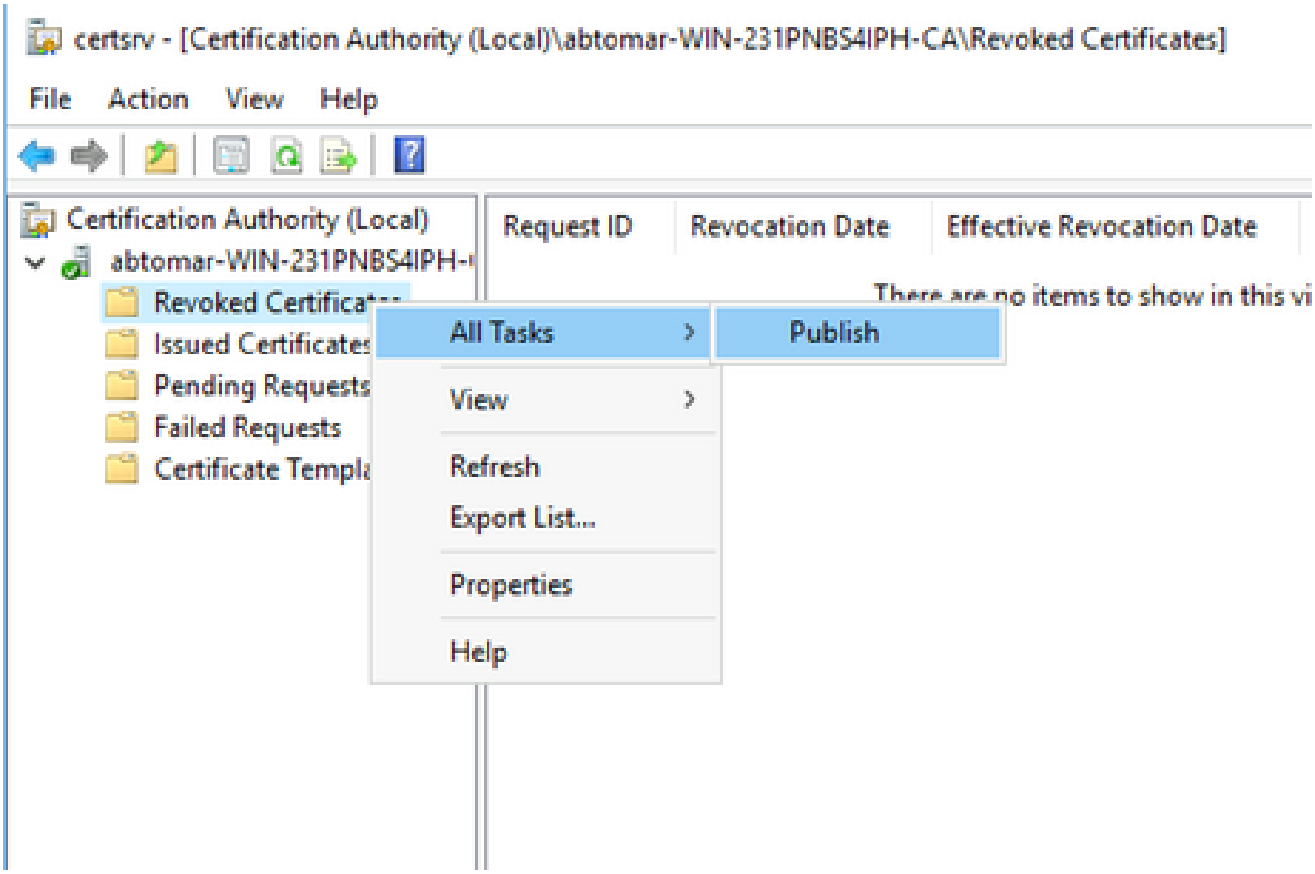


7. Clique em **OK** para retornar à guia Extensões. Marque a caixa de seleção **Publish CRLs to this location** e clique em **OK** para fechar a janela Propriedades.

   Será exibido um prompt de permissão para reiniciar os Serviços de Certificados do Ative Diretory. Clique em **Yes**.



8. No painel esquerdo, clique com o botão direito do mouse em **Revoked Certificates**. Escolha **All Tasks** > **Publish**. Verifique se a opção Nova CRL está selecionada e clique em **OK**.



O servidor de autoridade de certificação da Microsoft deve criar um novo arquivo .crl na

pasta criada na seção 1. Se o novo arquivo CRL for criado com sucesso, não haverá diálogo após clicar em OK. Se um erro for retornado em relação à nova pasta de ponto de distribuição, repita cuidadosamente cada etapa nesta seção.

Verifique se o arquivo CRL existe e está acessível via IIS

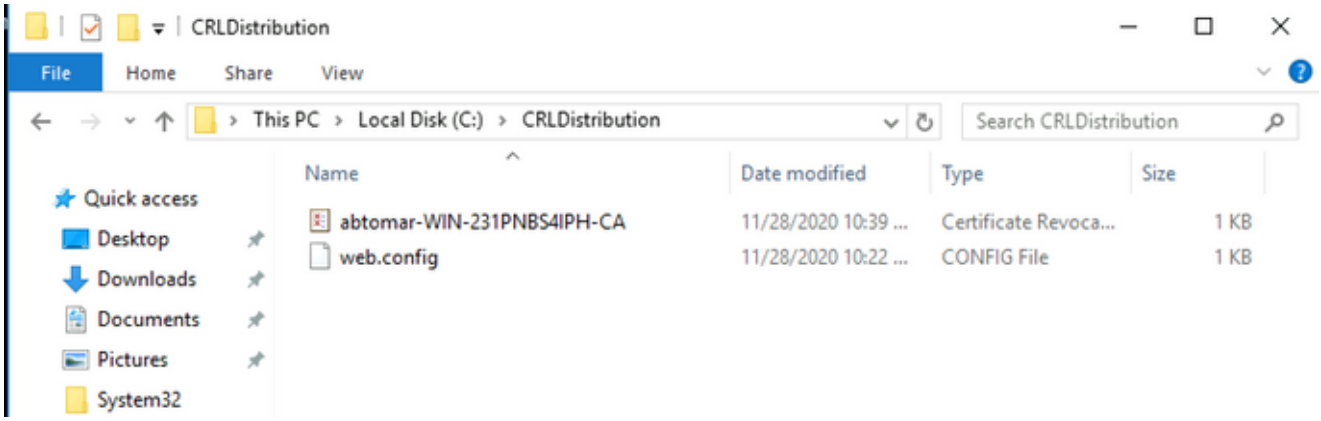
Verifique se os novos arquivos CRL existem e se estão acessíveis via IIS de outra estação de trabalho antes de iniciar esta seção.

1. No servidor IIS, abra a pasta criada na seção 1. Deve haver um único arquivo .crl presente com o formulário

   .crl

   onde
   é o nome do servidor de autoridade de certificação. Neste exemplo, o nome do arquivo é:

   abtomar-WIN-231PNBS4IPH-CA.crl



2. Em uma estação de trabalho na rede (idealmente na mesma rede que o nó Admin primário do ISE), abra um navegador da Web e navegue até http://

   /

   onde
   é o nome do servidor do IIS configurado na seção 2 e
   é o nome do site escolhido para o ponto de distribuição na seção 2. Neste exemplo, o URL é:

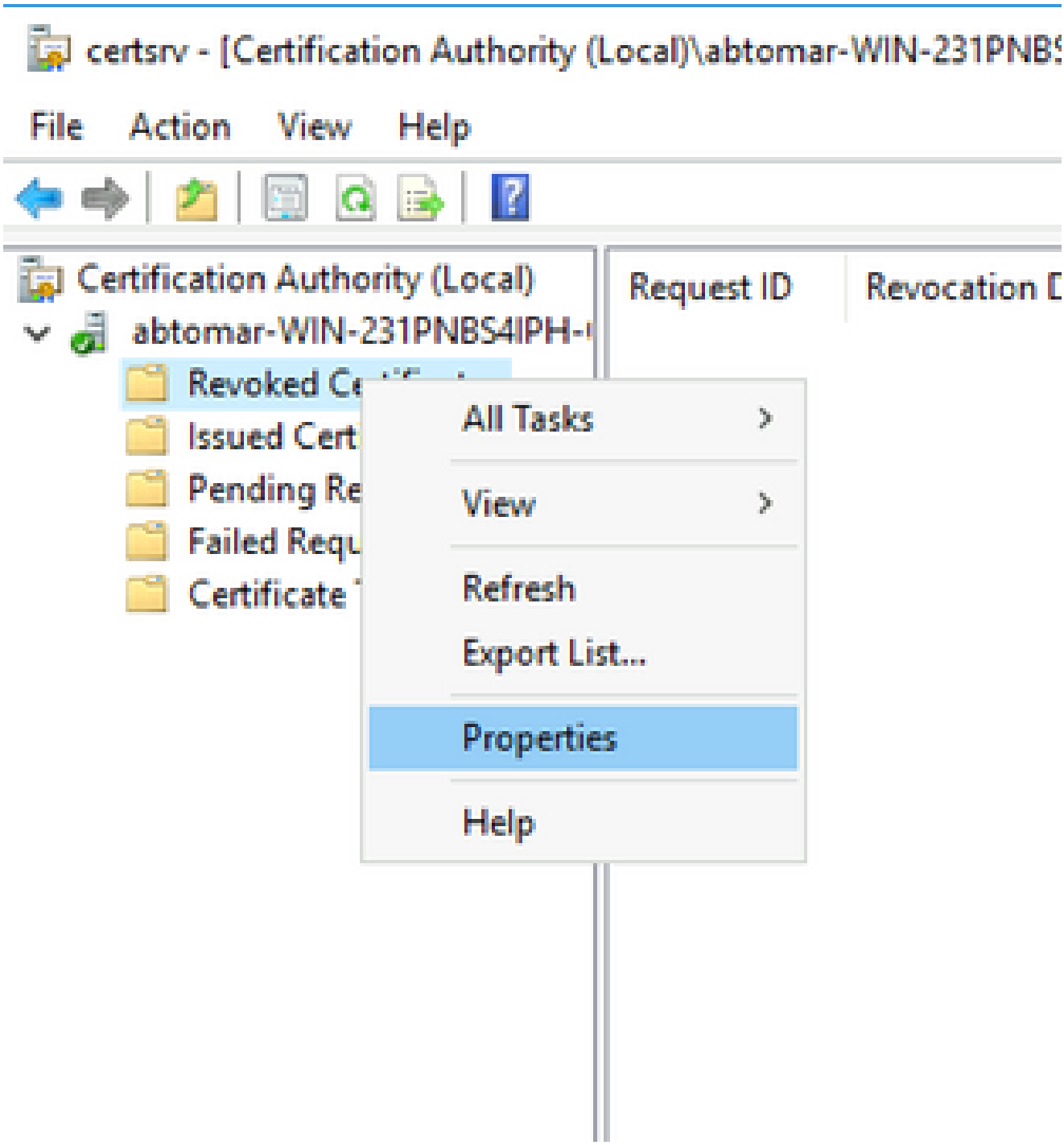
   http://win-231pnbs4iph/CRLD

   O índice de diretório é exibido, incluindo o arquivo observado na etapa 1.

Configurar o ISE para usar o Novo Ponto de Distribuição de CRL

Antes que o ISE seja configurado para recuperar a CRL, defina o intervalo para publicar a CRL. A estratégia para determinar esse intervalo está além do escopo deste documento. Os valores potenciais (no Microsoft CA) são de 1 hora a 411 anos, inclusive. O valor padrão é 1 semana. Uma vez determinado um intervalo apropriado para seu ambiente, defina o intervalo com estas instruções:

1. Na barra de tarefas do servidor de CA, clique em **Start**. Escolha **Administrative Tools** > **Certificate Authority**.
2. No painel esquerdo, expanda a autoridade de certificação. Clique com o botão direito do mouse na **Revoked Certificates** pasta e escolha **Properties**.
3. Nos campos de intervalo de publicação da CRL, insira o número necessário e escolha o período. Clique **OK** para fechar a janela e aplicar a alteração. Neste exemplo, um intervalo de publicação de sete dias é configurado.



4. Digite o **certutil -getreg CA\Clock*** comando para confirmar o valor ClockSkew. O valor padrão é 10 minutos.

   Saída de exemplo:

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

5. Digite o **certutil -getreg CA\CRLov*** comando para verificar se CRLOverlapPeriod foi definido manualmente. Por padrão, o valor de CRLOverlapUnit é 0, o que indica que nenhum valor

manual foi definido. Se o valor for um valor diferente de 0, registre o valor e as unidades.

Saída de exemplo:

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

6. Digite o **certutil -getreg CA\CRLpe*** comando para verificar o período CRLP, que foi definido na etapa 3.

   Saída de exemplo:

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

7. Calcule o Período de Cortesia da CRL da seguinte maneira:

   a. Se CRLOverlapPeriod foi definido na etapa 5: OVERLAP = CRLOverlapPeriod, em minutos;

   Senão: SOBREPOSIÇÃO = (período CRLP / 10), em minutos

   b. Se SOBREPOSIÇÃO > 720, SOBREPOSIÇÃO = 720

   c. Se OVERLAP < (1,5 * ClockSkewMinutes) então OVERLAP = (1,5 * ClockSkewMinutes)

   d. Se OVERLAP > CRLPeriod, em minutos então OVERLAP = CRLPeriod em minutos

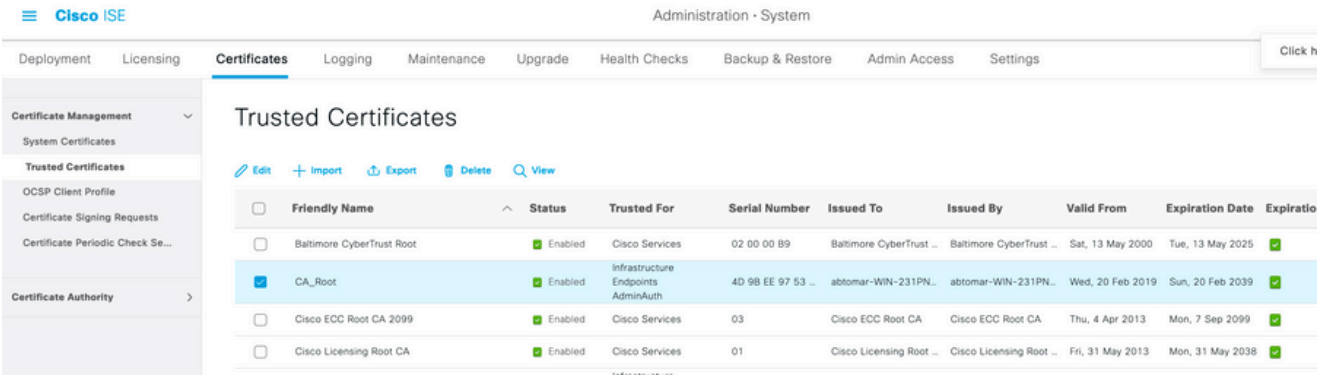
   e. Período de cortesia = SOBREPOSIÇÃO + MinutosDistorçãoDoRelógio

```
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
```

O período de carência calculado é o período de tempo entre o momento em que a CA

publica a próxima CRL e o momento em que a CRL atual expira. O ISE precisa ser configurado para recuperar as CRLs de acordo.

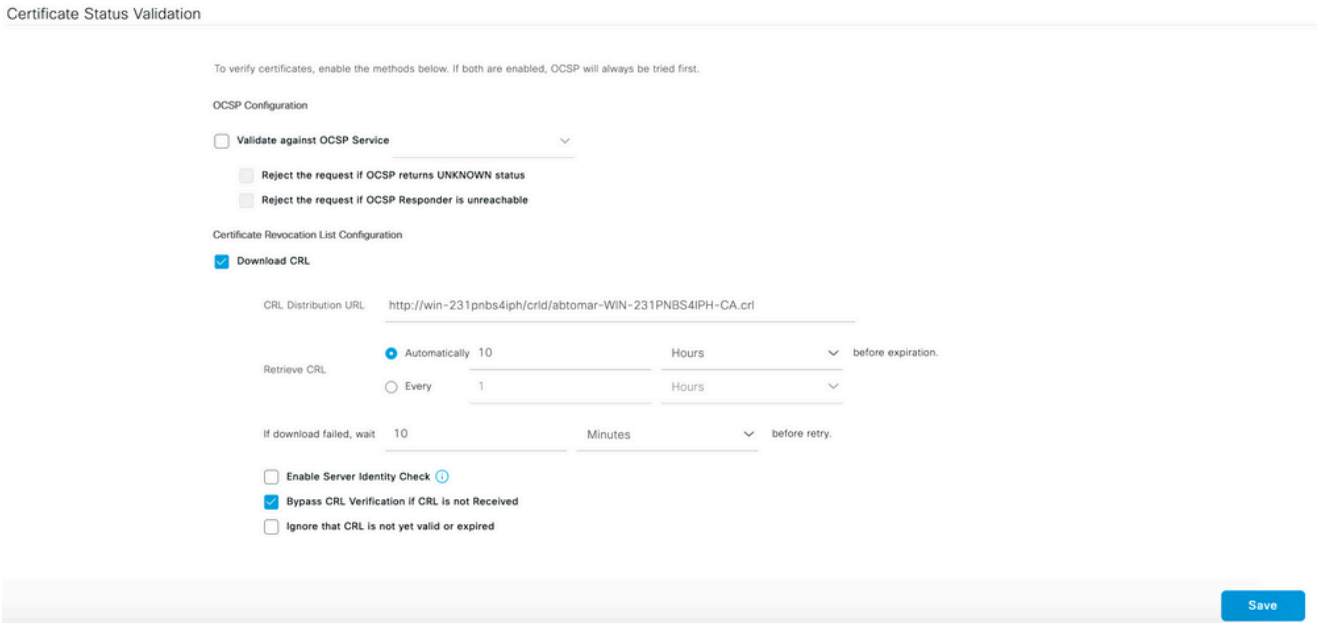
8. Faça login no nó ISE Primary Admin e escolha **Administration** > **System** > **Certificates**. No painel esquerdo, escolha **Trusted Certificate**.



9. Marque a caixa de seleção ao lado do certificado CA para o qual você pretende configurar CRLs. Clique em **Edit**.
10. Perto da parte inferior da janela, marque a caixa de seleção**Download CRL**.
11. No campo URL de Distribuição de CRL, digite o caminho para o Ponto de Distribuição de CRL, que inclui o arquivo .crl, criado na seção 2. Neste exemplo, o URL é:

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

12. O ISE pode ser configurado para recuperar a CRL em intervalos regulares ou com base na expiração (que, em geral, também é um intervalo regular). Quando o intervalo de publicação da CRL é estático, atualizações mais oportunas da CRL são obtidas quando a última opção é usada. Clique no botão de opção **Automatically** .
13. Defina o valor para recuperação como um valor menor que o período de tolerância calculado na etapa 7. Se o valor definido for maior que o período de cortesia, o ISE verificará o ponto de distribuição da CRL antes que a CA publique a próxima CRL. Neste exemplo, o período de cortesia é calculado como 730 minutos ou 12 horas e 10 minutos. Um valor de 10 horas será usado para a recuperação.
14. Defina o intervalo de repetição conforme apropriado para seu ambiente. Se o ISE não puder recuperar a CRL no intervalo configurado na etapa anterior, ele tentará novamente nesse intervalo mais curto.
15. **Bypass CRL Verification if CRL is not Received** Marque a caixa de seleção para permitir que a autenticação baseada em certificado continue normalmente (e sem uma verificação de CRL) se o ISE não puder recuperar a CRL para esta CA em sua última tentativa de download. Se esta caixa de seleção não for marcada, toda a autenticação baseada em certificado com certificados emitidos por esta CA falhará se a CRL não puder ser recuperada.
16. Marque a caixa de seleção **Ignore that CRL is not yet valid or expired** para permitir que o ISE use arquivos de CRL expirados (ou ainda não válidos) como se fossem válidos. Se essa caixa de seleção não estiver marcada, o ISE considerará uma CRL como inválida antes de sua Data de efetivação e após seus horários da Próxima atualização. Clique **Save** para concluir a configuração.



Verificar

No momento, não há procedimento de verificação disponível para esta configuração.

Troubleshooting

Atualmente, não existem informações disponíveis específicas sobre Troubleshooting para esta configuração.

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.