

Configurar o Microsoft CA Server para publicar as listas de revogação de certificado do ISE

Contents

[Introduction](#)

[Pré-requisito](#)

[Requirements](#)

[Componentes Utilizados](#)

[Configurar](#)

[Criar e configurar uma pasta na CA para abrigar os arquivos CRL](#)

[Crie um site no IIS para expor o novo ponto de distribuição da CRL](#)

[Configurar o Microsoft CA Server para publicar arquivos CRL no ponto de distribuição](#)

[Verifique se o arquivo CRL existe e está acessível via IIS](#)

[Configurar o ISE para usar o novo ponto de distribuição CRL](#)

Introduction

Este documento descreve a configuração de um servidor de Autoridade de Certificação da Microsoft (AC) que executa o Internet Information Services (IIS) 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 de certificado.

Pré-requisito

Requirements

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

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. 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

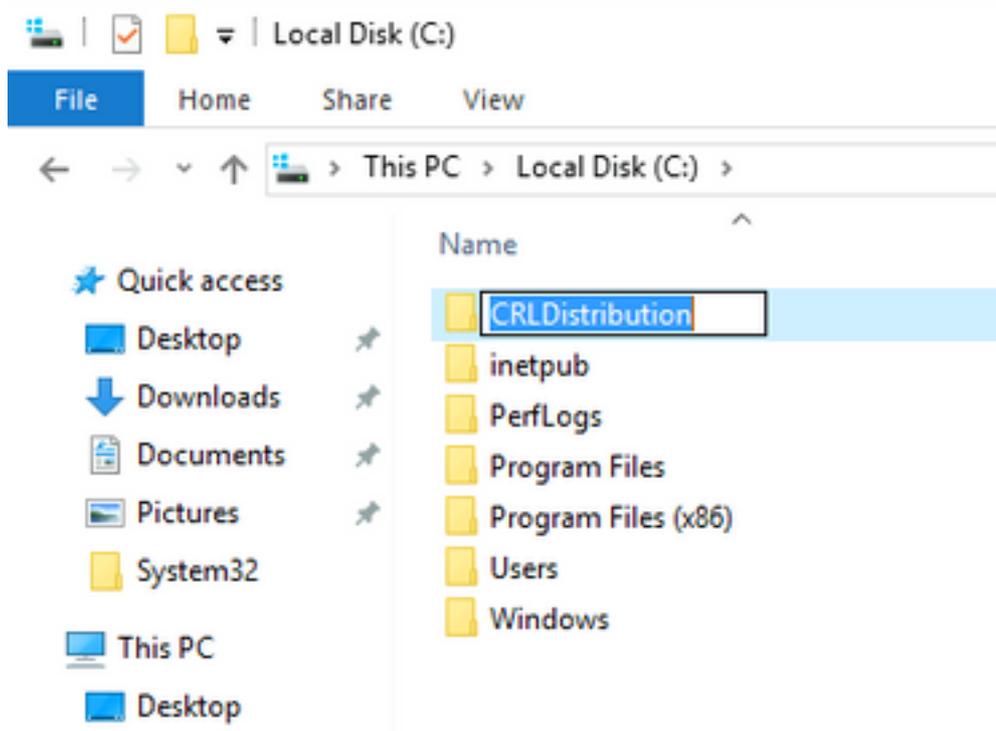
documento.

Criar e configurar uma pasta na CA para abrigar os arquivos CRL

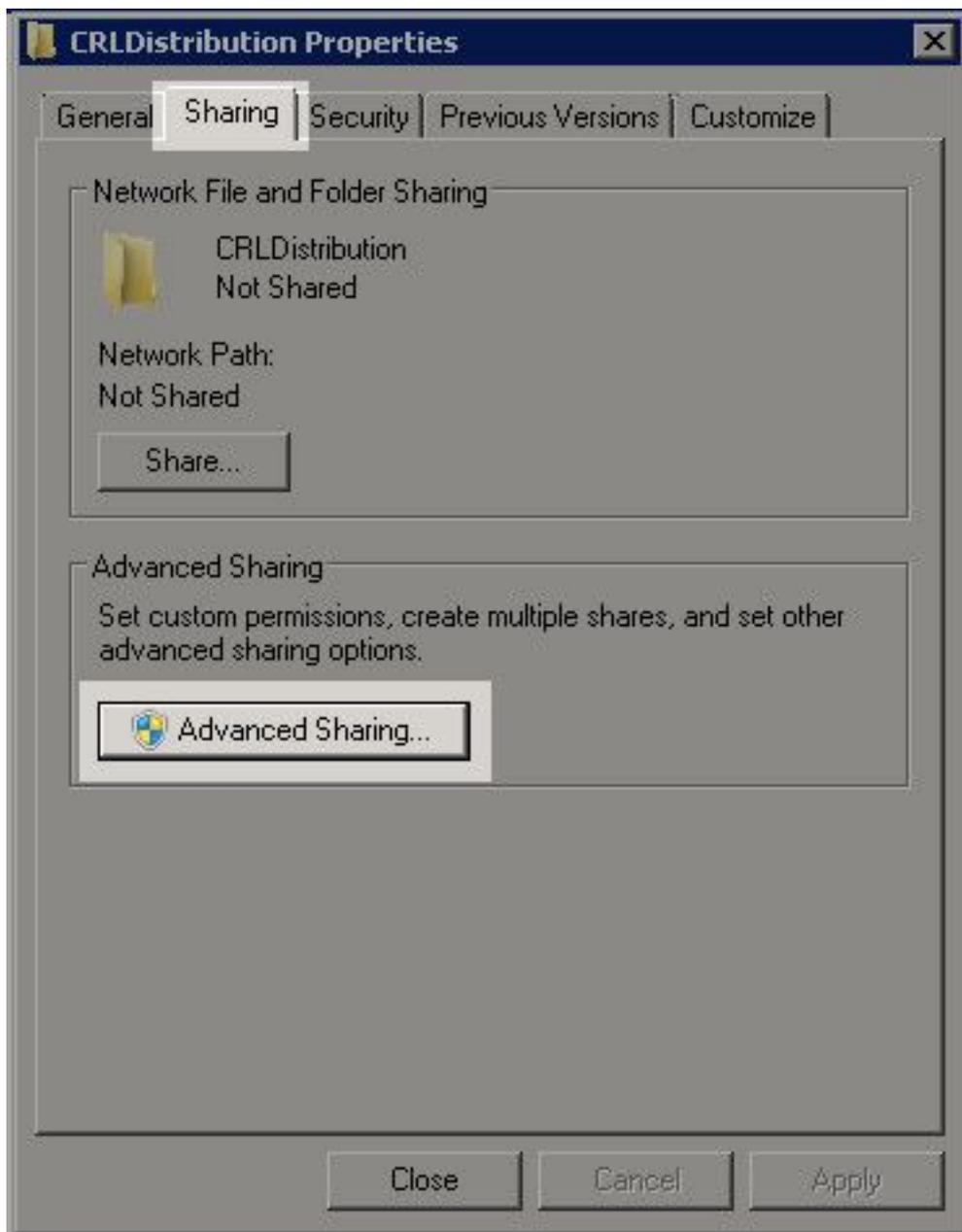
A primeira tarefa é configurar um local no servidor CA para armazenar os arquivos CRL. Por predefinição, o servidor Microsoft CA publica os ficheiros em **C:\Windows\system32\CertSrv\CertEnroll**

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

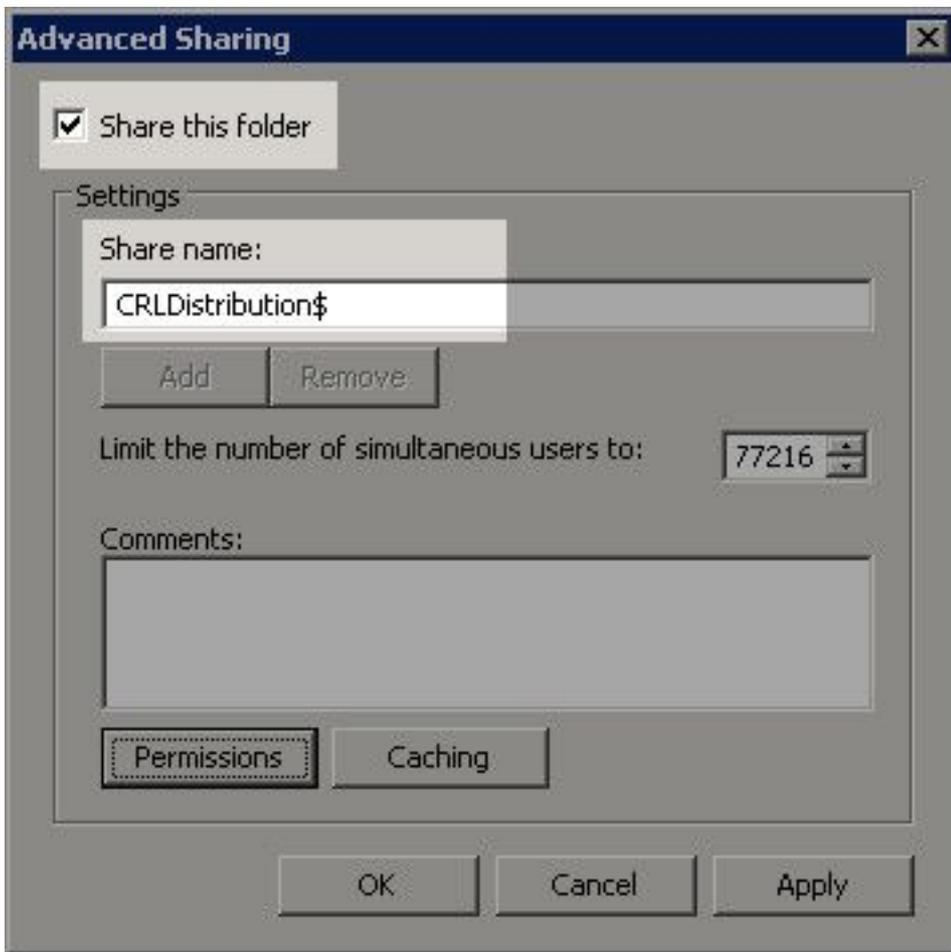
1. No servidor IIS, escolha um local no sistema de arquivos e crie uma nova pasta. Neste exemplo, a pasta **C:\CRLDistribution** é criada.



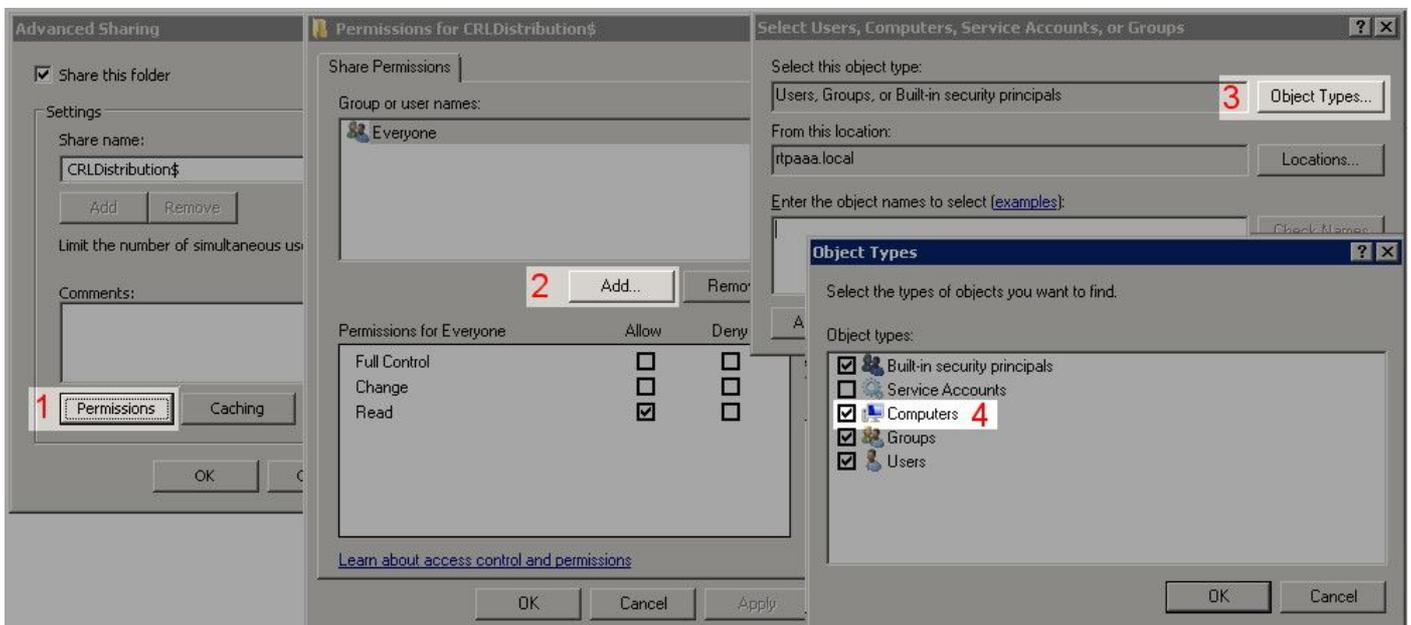
2. Para que a CA grave os arquivos CRL na nova pasta, o compartilhamento deve estar habilitado. Clique com o botão direito do mouse na nova pasta, escolha **Propriedades**, clique na guia **Compartilhamento** e clique em **Compartilhamento Avançado**.



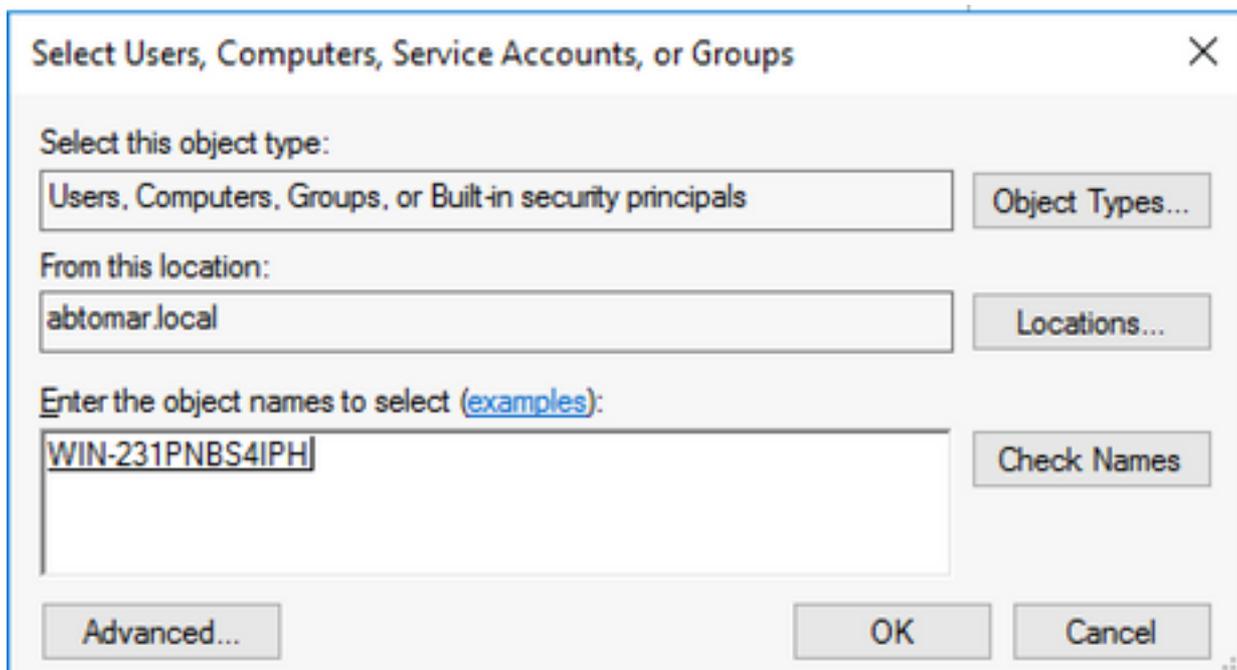
3. Para compartilhar a pasta, marque a caixa de seleção **Compartilhar esta pasta** e adicione um sinal de dólar (\$) ao final do nome do compartilhamento no campo Nome do compartilhamento para ocultar o compartilhamento.



4. Clique em **Permissões** (1), clique em **Adicionar** (2), clique em **Tipos de Objeto** (3) e marque a caixa de seleção **Computadores** (4).

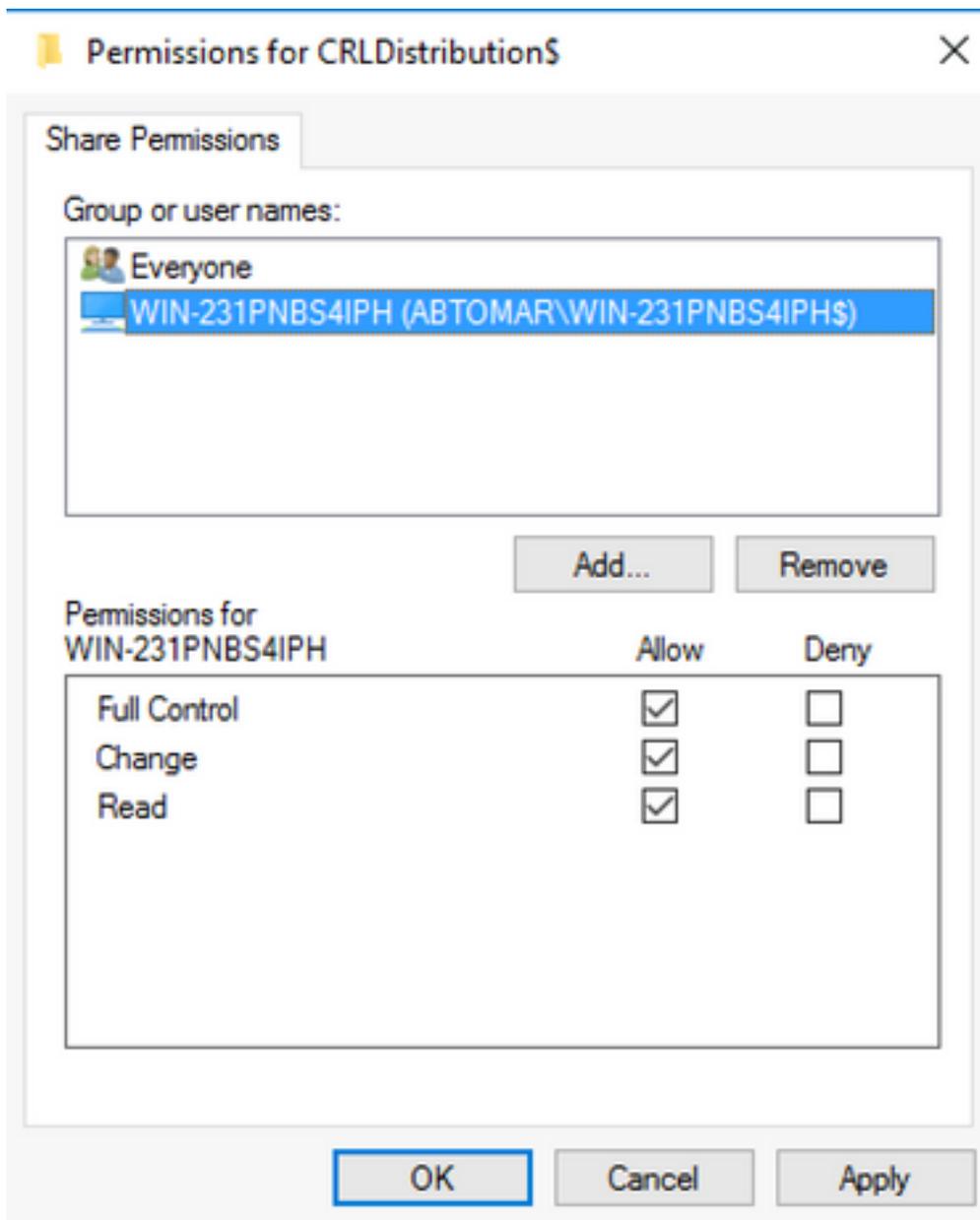


5. Para retornar à janela Selecionar Usuários, Computadores, Contas de Serviço ou Grupos, clique em **OK**. No campo Insira os nomes dos objetos a serem selecionados, insira o nome do computador do servidor CA neste exemplo: WIN0231PNBS4IPH e clique em **Verificar nomes**. Se o nome inserido for válido, o nome será atualizado e aparecerá sublinhado. Click **OK**.

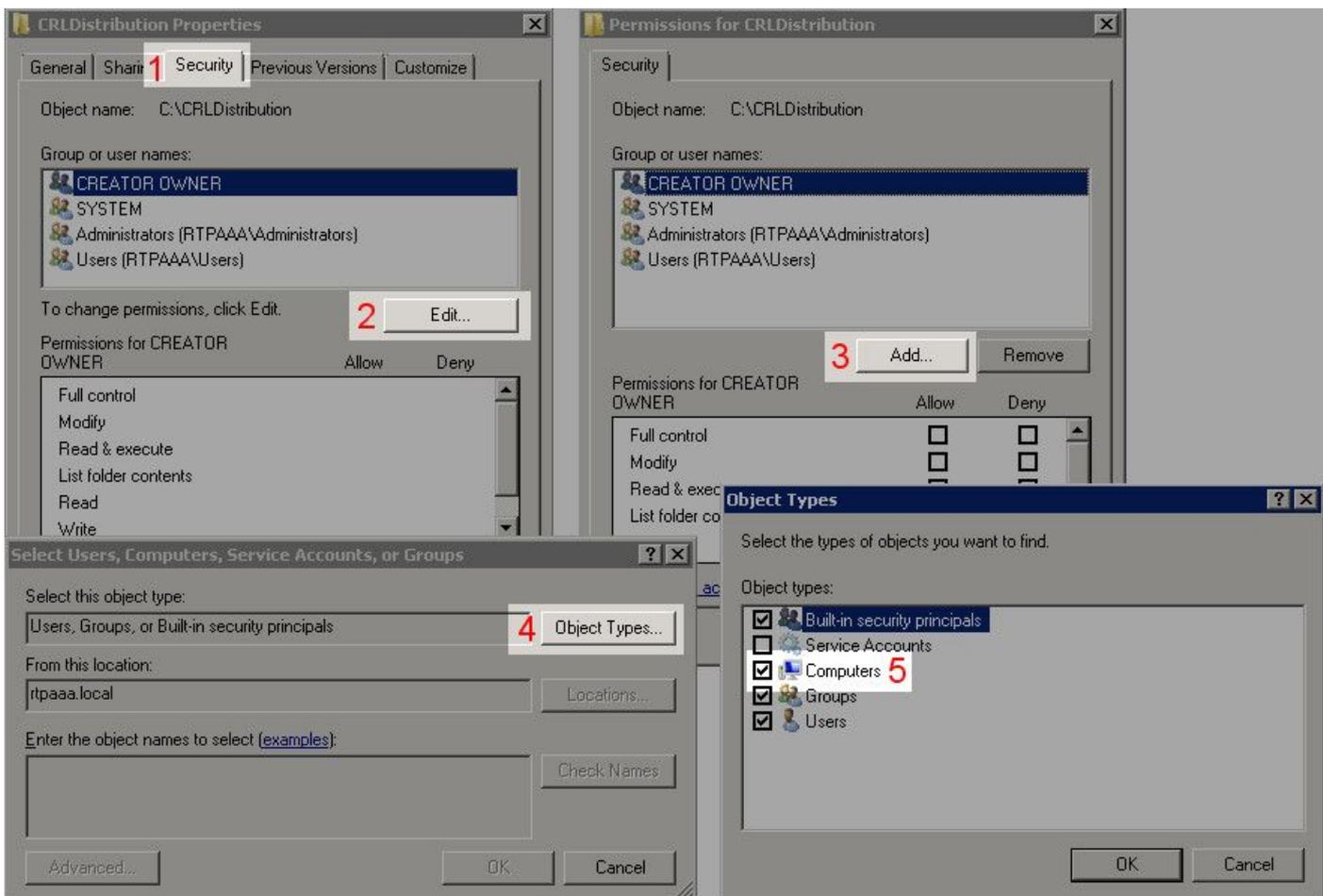


6. No campo Grupo ou nomes de usuário, escolha o computador CA. Marque **Permitir Controle Completo** para conceder acesso total à CA.

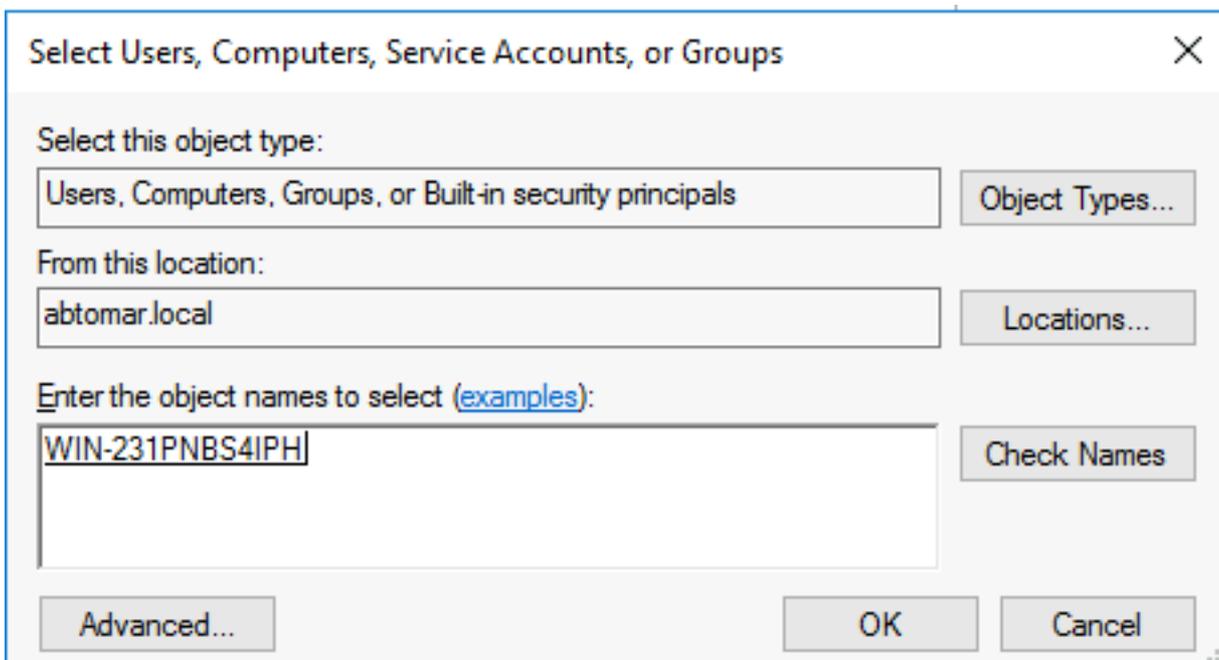
Click **OK**. Clique em **OK** novamente para fechar a janela Compartilhamento avançado e retornar à janela Propriedades.



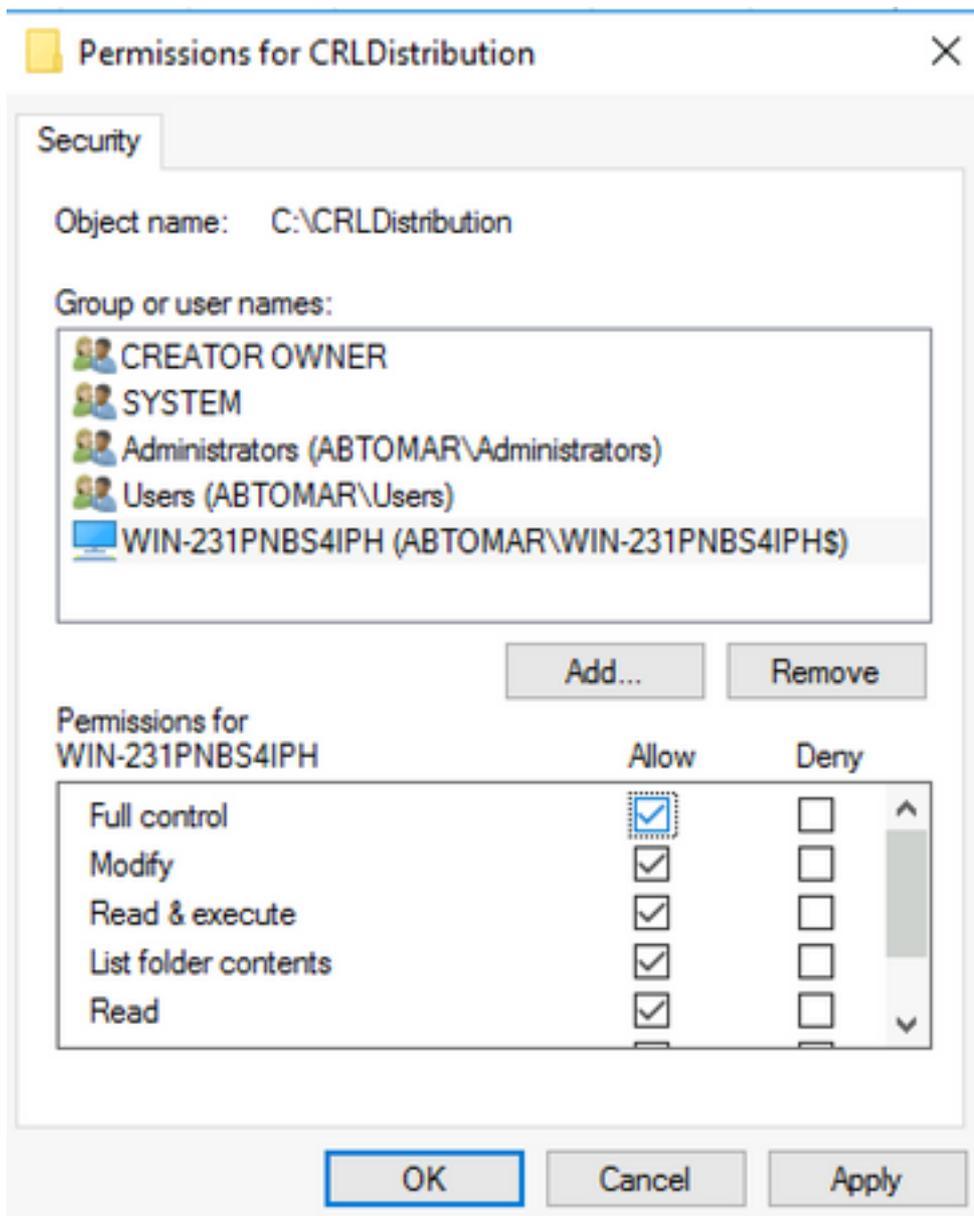
7. Para permitir que a CA grave os arquivos CRL na nova pasta, configure as permissões de segurança apropriadas. Clique na guia Segurança (1), clique em **Editar** (2), clique em **Adicionar** (3), clique em **Tipos de Objeto** (4) e marque a caixa de seleção Computadores (5).



8. No campo Insira os nomes dos objetos a serem selecionados, insira o nome do computador do servidor CA e clique em **Verificar nomes**. Se o nome inserido for válido, o nome será atualizado e aparecerá sublinhado. Click **OK**.



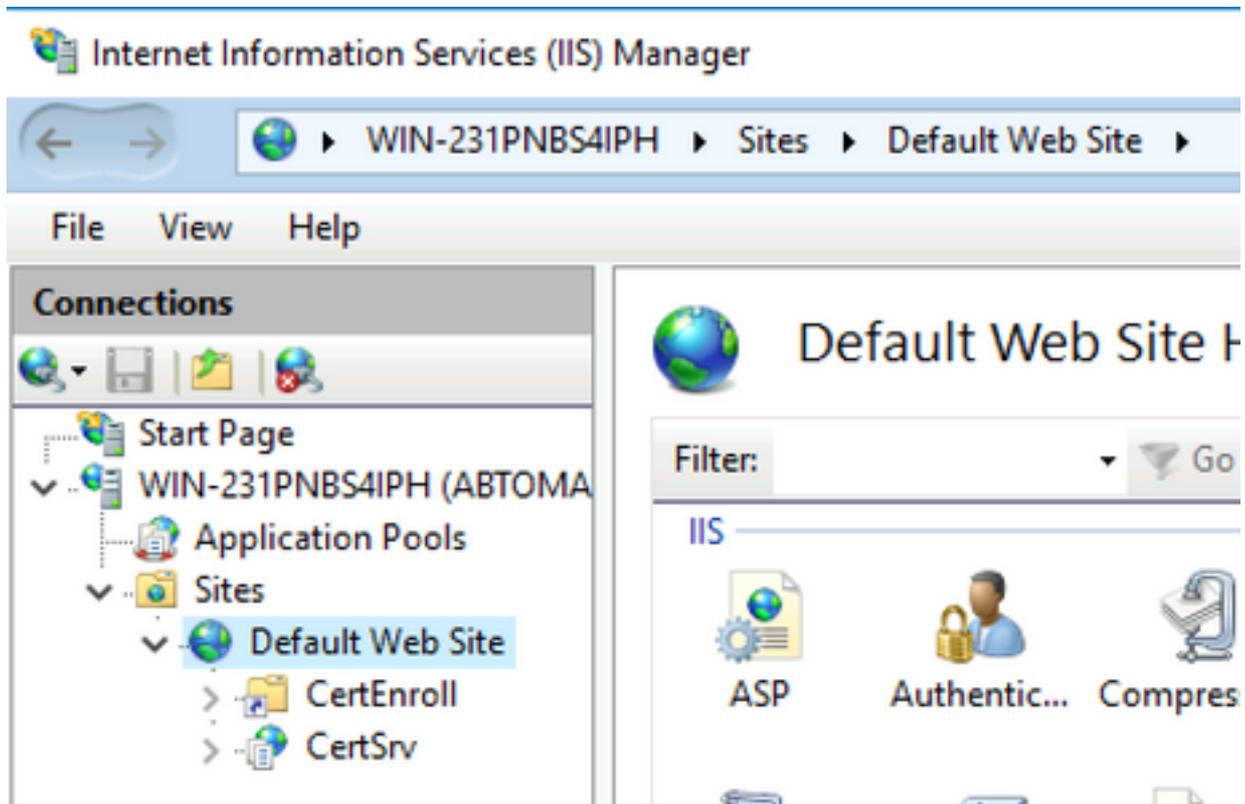
9. Escolha o computador CA no campo Grupo ou nomes de usuário e marque **Permitir** controle total para conceder acesso total à CA. Clique em **OK** e, em seguida, clique em **Fechar** para concluir a tarefa.



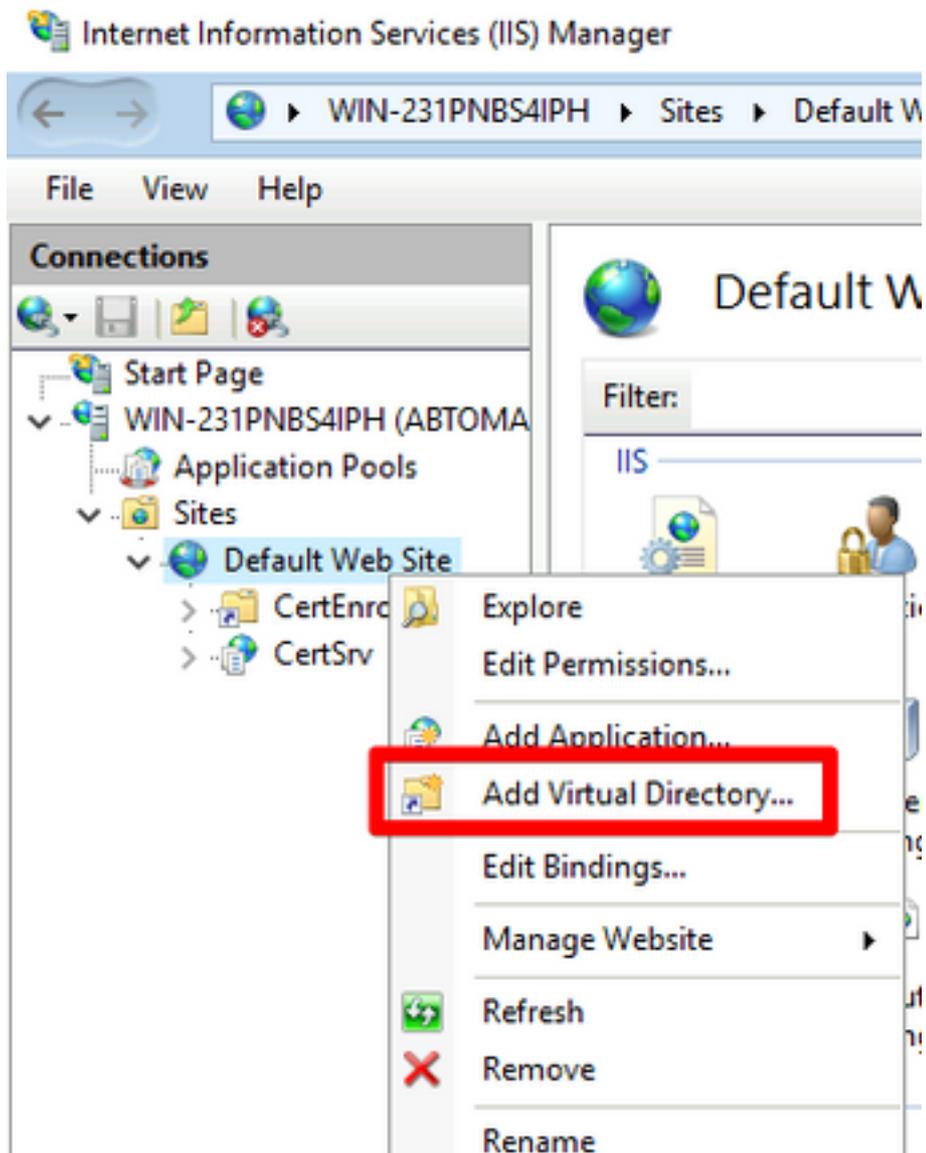
Crie um site no IIS para expor o novo ponto de distribuição da CRL

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

1. Na barra de tarefas do servidor IIS, clique em **Iniciar**. Escolha **Administrative Tools > Internet Information Services (IIS) Manager**.
2. No painel esquerdo (conhecido como **Árvore de console**), expanda o nome do servidor IIS e expanda **Sites**.



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



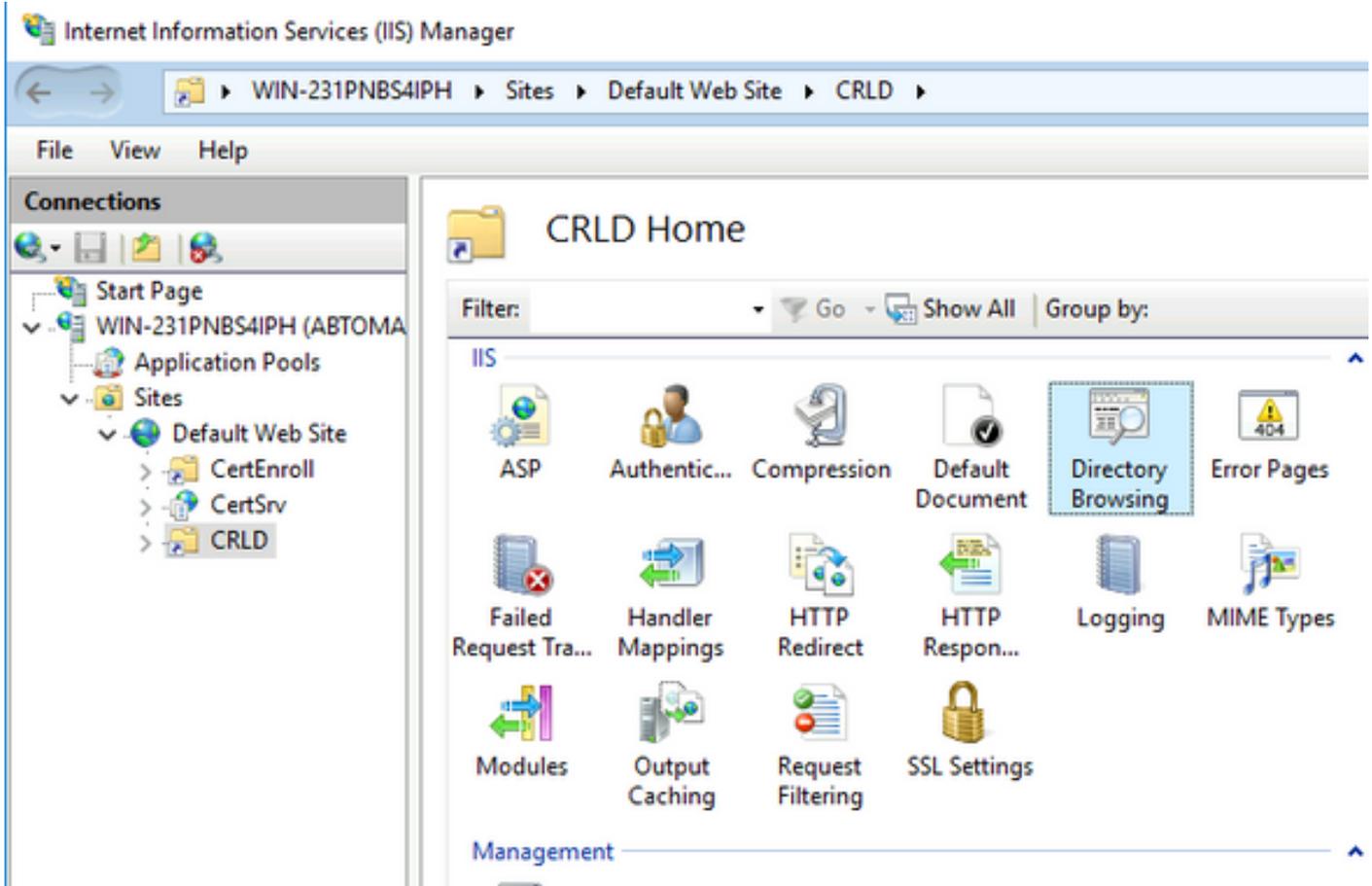
4. No campo Alias, insira um nome de site para o Ponto de distribuição da CRL. Neste exemplo, o CRLD é inserido.

The screenshot shows the 'Add Virtual Directory' dialog box. At the top, the title bar reads 'Add Virtual Directory' with a question mark and a close button. Below the title bar, there are two input fields: 'Site name: Default Web Site' and 'Path: /'. Underneath, the 'Alias:' label is followed by a text box containing 'CRLD', which is highlighted with a red rectangular border. Below the alias box, the text 'Example: images' is displayed. The 'Physical path:' label is followed by a text box containing 'C:\CRLDistribution' and a small '...' button to its right. At the bottom left, there are two buttons: 'Connect as...' and 'Test Settings...'. At the bottom right, there are two buttons: 'OK' and 'Cancel'.

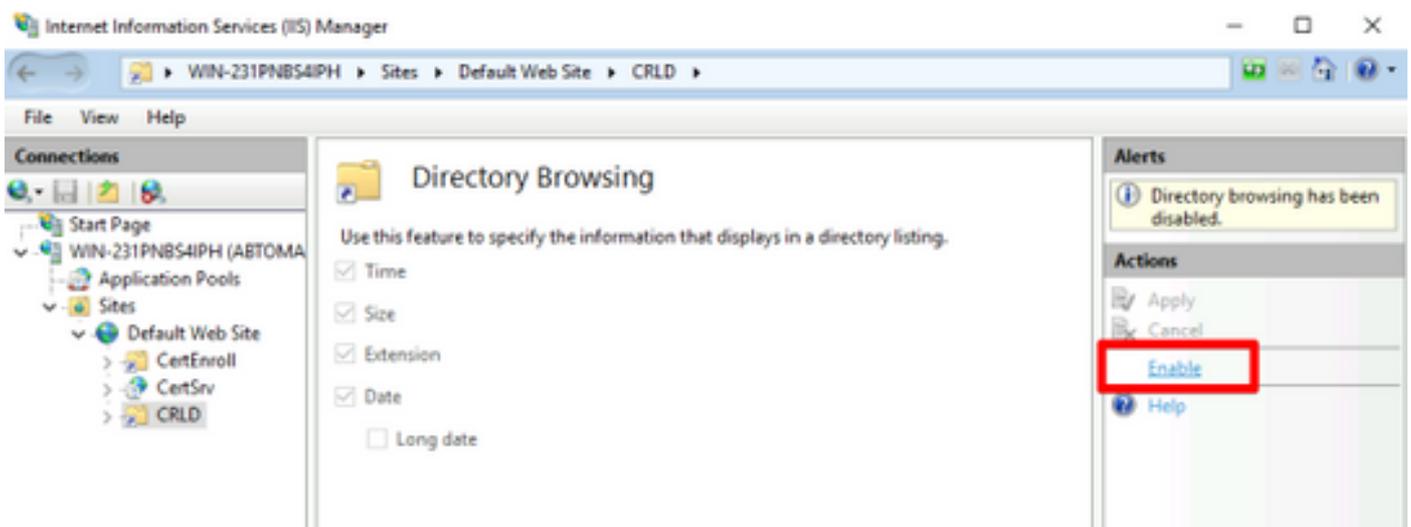
5. Clique nas reticências (. . .) à direita do campo Physical path (Caminho físico) e navegue até a pasta criada na seção 1. Selecione a pasta e clique em **OK**. Clique em **OK** para fechar a janela Adicionar diretório virtual.

This screenshot shows the same 'Add Virtual Directory' dialog box. In this view, the 'Alias' field contains 'CRLD'. The 'Physical path' field contains 'C:\CRLDistribution' and is highlighted with a red rectangular border. The '...' button to the right of the physical path field is visible. The 'Connect as...' and 'Test Settings...' buttons are at the bottom left, and the 'OK' and 'Cancel' buttons are at the bottom right.

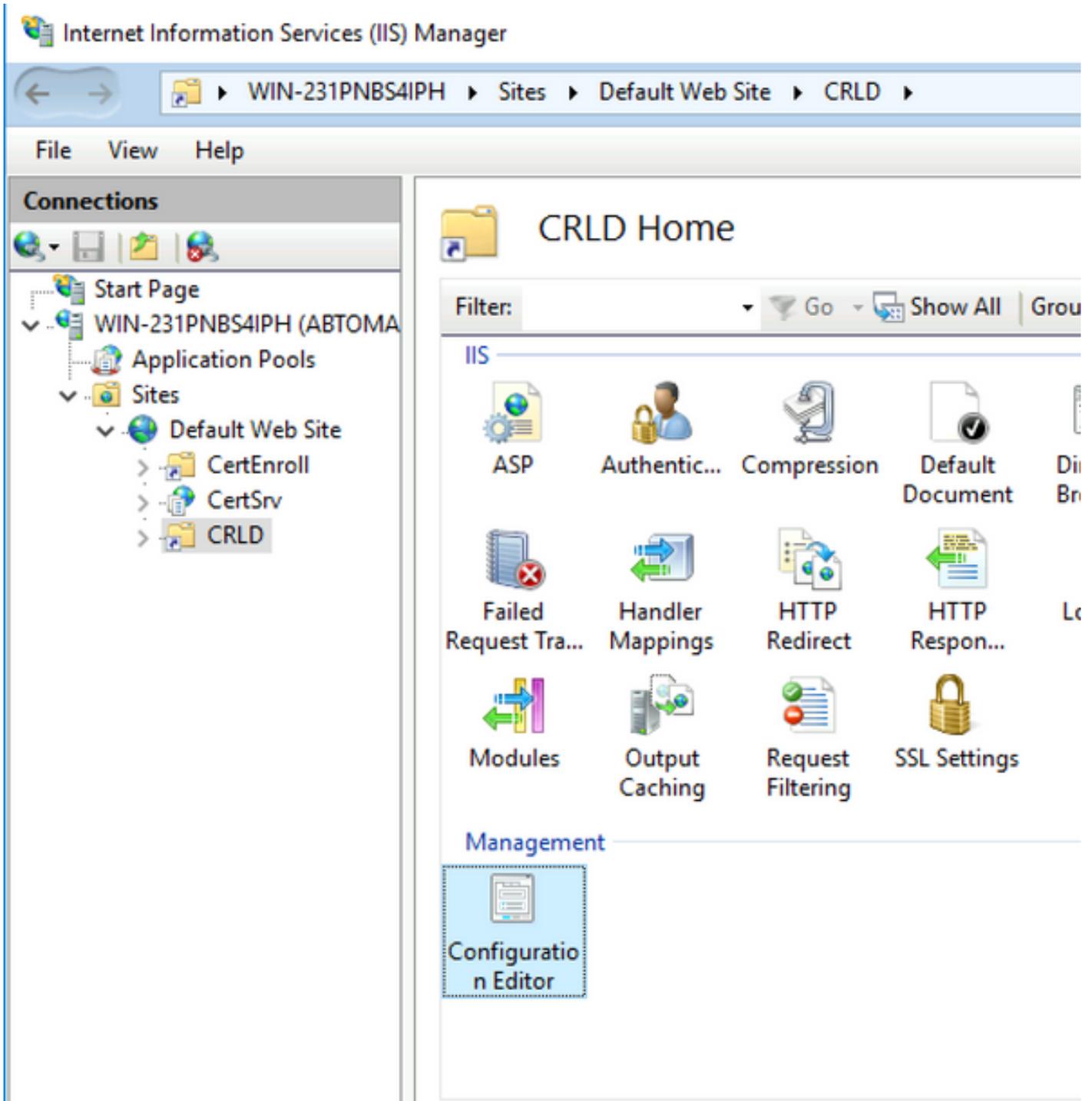
6. O nome do site inserido na etapa 4 deve ser destacado no painel esquerdo. Caso contrário, escolha agora. No painel central, clique duas vezes em **Navegação de diretório**.



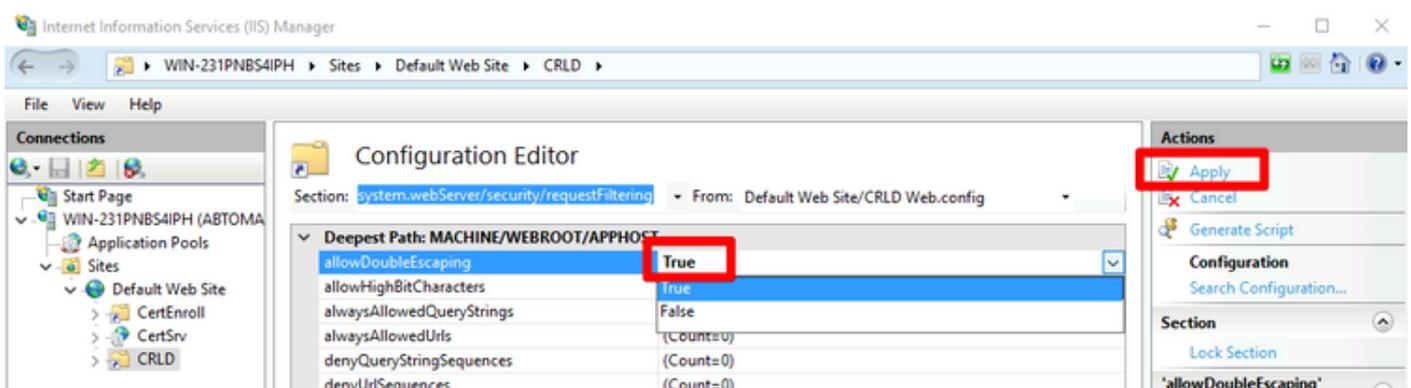
7. No painel direito, clique em **Enable (Habilitar)** para habilitar a navegação no diretório.



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



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

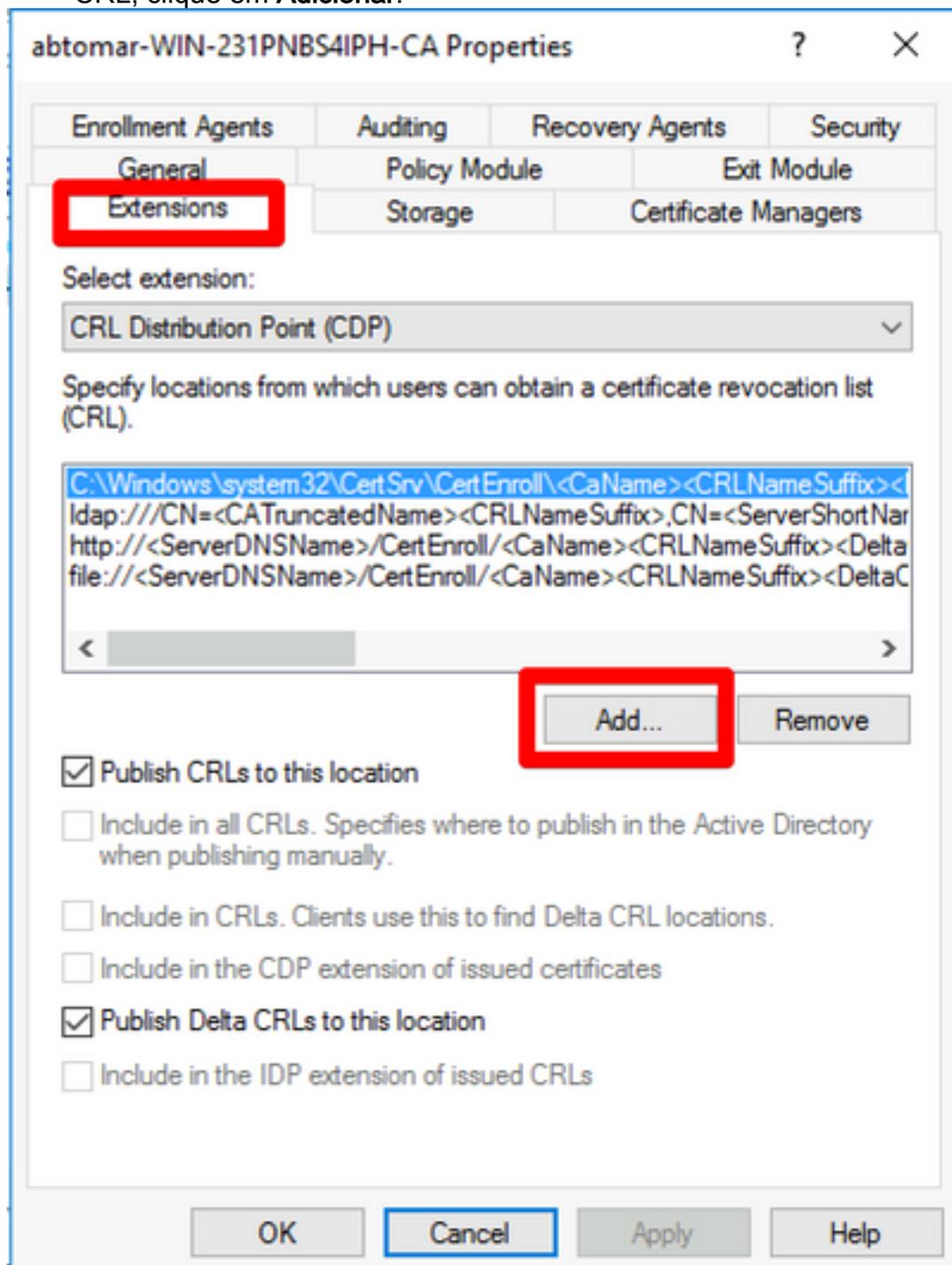


A pasta agora deve estar acessível via IIS.

Configurar o Microsoft CA Server para publicar arquivos CRL no ponto de distribuição

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

1. Na barra de tarefas do servidor CA, clique em **Iniciar**. Escolha **Ferramentas Administrativas > Autoridade de Certificação**.
2. No painel esquerdo, clique com o botão direito do mouse no nome da CA. Escolha **Propriedades** e clique na guia **Extensões**. Para adicionar um novo ponto de distribuição de CRL, clique em **Adicionar**.



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\$\

Add Location [X]

A location can be any valid URL or path. Enter an HTTP, LDAP, file address, or enter a UNC or local path. To insert a variable into the URL or path, select the variable below and click Insert.

Location:
\\WIN-231PNBS4IPH\CRLDistribution\$\

Variable:
<CaName> [v] [Insert]

Description of selected variable:
Used in URLs and paths
Inserts the DNS name of the server
Example location: http://<ServerDNSName>/CertEnroll/<CaName><CRLNa

[<] []

[OK] [Cancel]

4. Com o campo Local preenchido, escolha **<CaName>** na lista suspensa Variável e clique em **Inserir**.

Add Location ✕

A location can be any valid URL or path. Enter an HTTP, LDAP, file address, or enter a UNC or local path. To insert a variable into the URL or path, select the variable below and click Insert.

Location:

Variable:

Description of selected variable:
Used in URLs and paths
Inserts the DNS name of the server
Example location: http://<ServerDNSName>/CertEnroll/<CaName><CRLNameSuffix>

5. Na lista suspensa Variável, escolha **<CRLNameSuffix>** e clique em **Inserir**.

Add Location ✕

A location can be any valid URL or path. Enter an HTTP, LDAP, file address, or enter a UNC or local path. To insert a variable into the URL or path, select the variable below and click Insert.

Location:

Variable:

Description of selected variable:
Used in URLs and paths for the CRL Distribution Points extension
Appends a suffix to distinguish the CRL file name
Example location: http://<ServerName>/CertEnroll/<CaName><CRLNameSuffix>

6. No campo Location (Local), anexe .crl ao final do caminho. Neste exemplo, o local é:

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

Add Location

A location can be any valid URL or path. Enter an HTTP, LDAP, file address, or enter a UNC or local path. To insert a variable into the URL or path, select the variable below and click Insert.

Location:

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

Variable:

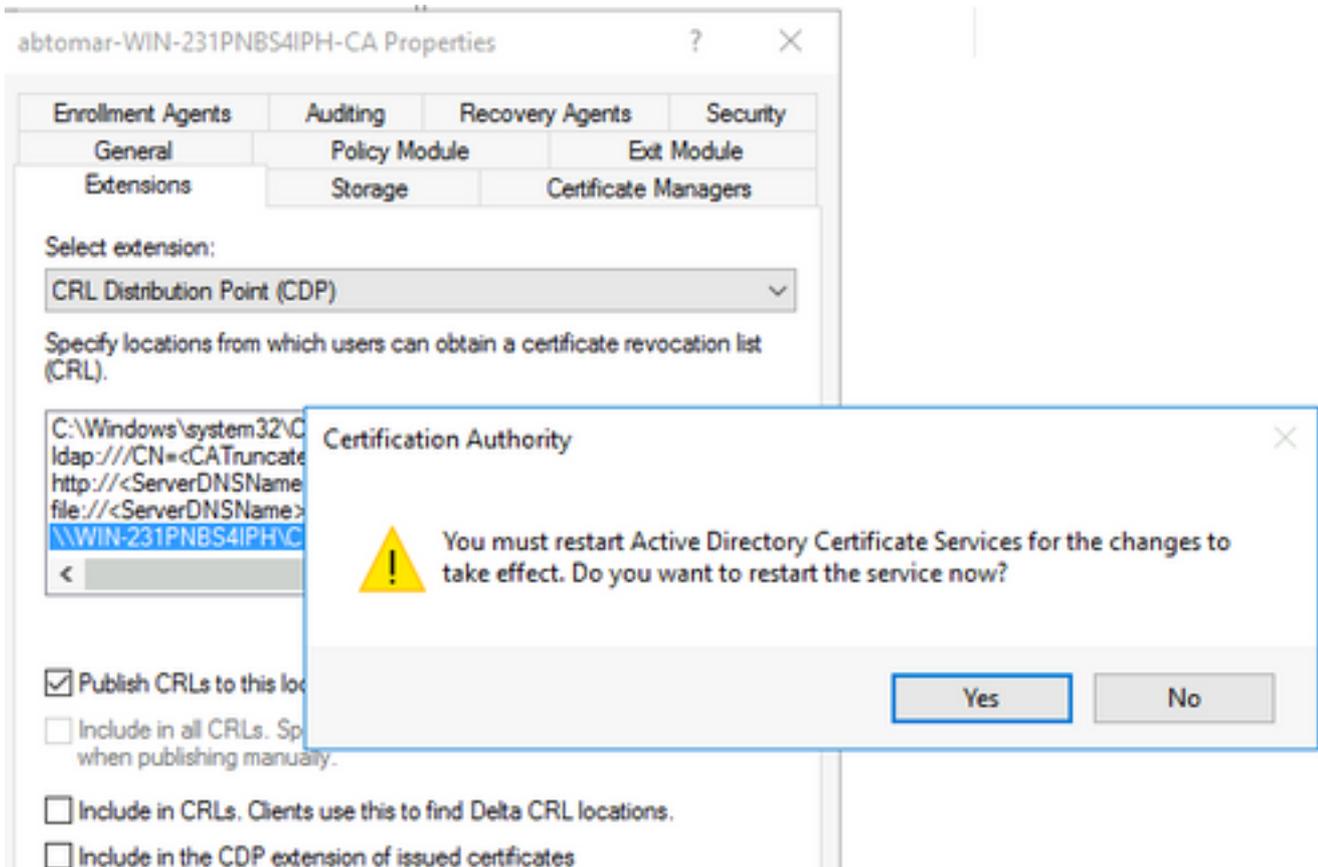
<CRLNameSuffix>

Description of selected variable:

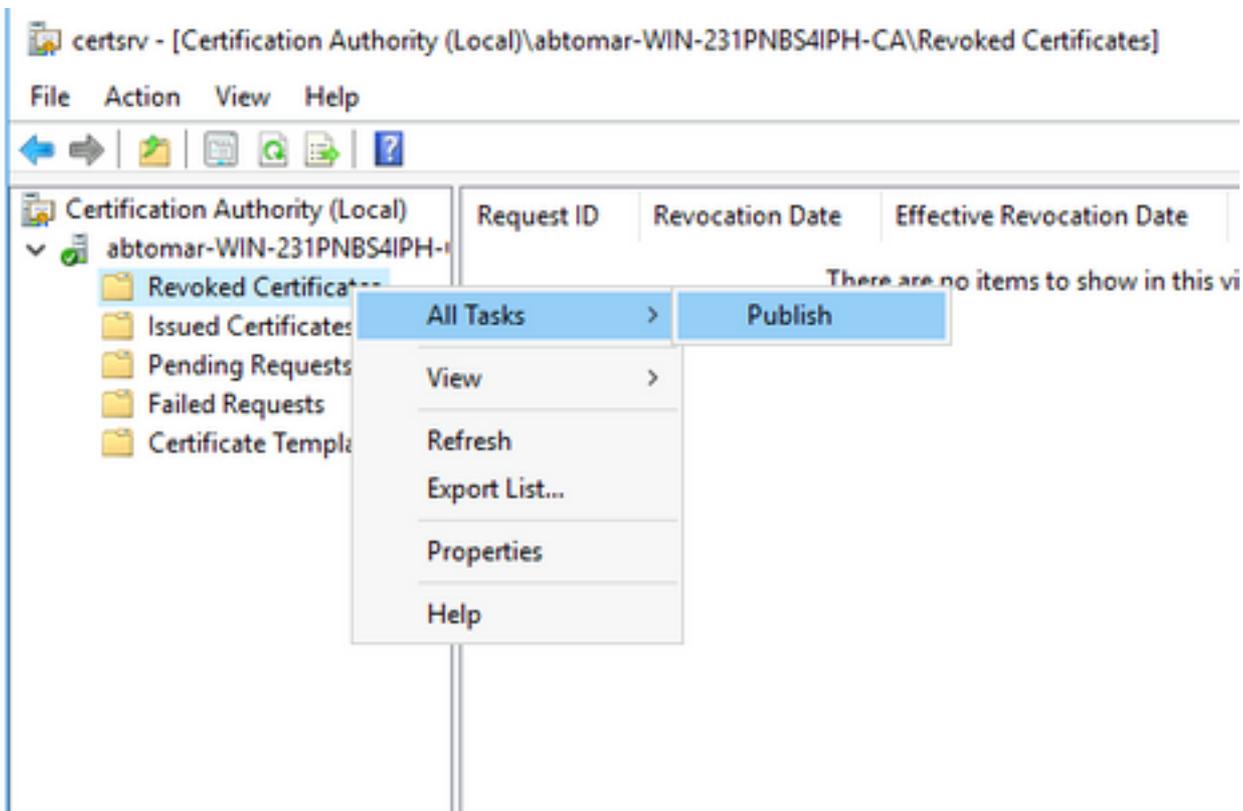
Used in URLs and paths for the CRL Distribution Points extension
Appends a suffix to distinguish the CRL file name
Example location: http://<ServerName>/CertEnroll/<CaName><CRLNameSt...

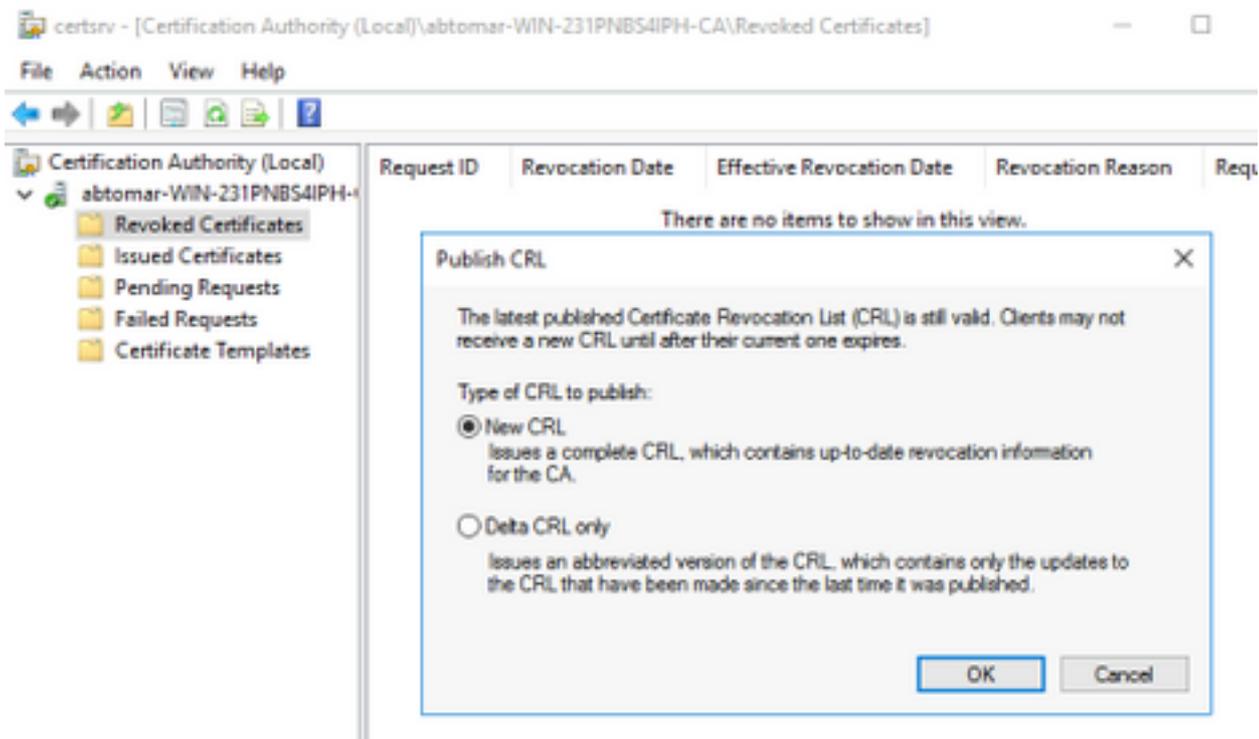
7. Clique em **OK** para retornar à guia Extensões. Marque a caixa de seleção **Publicar CRLs neste local** e clique em **OK** para fechar a janela Propriedades.

Um prompt é exibido para permitir a reinicialização dos Serviços de Certificados do Active Directory. Clique em Sim.



8. No painel esquerdo, clique com o botão direito do mouse em **Certificados Revogados**. Escolha **Todas as Tarefas > Publicar**. Verifique se New CRL (Nova CRL) está selecionado e clique em **OK**.





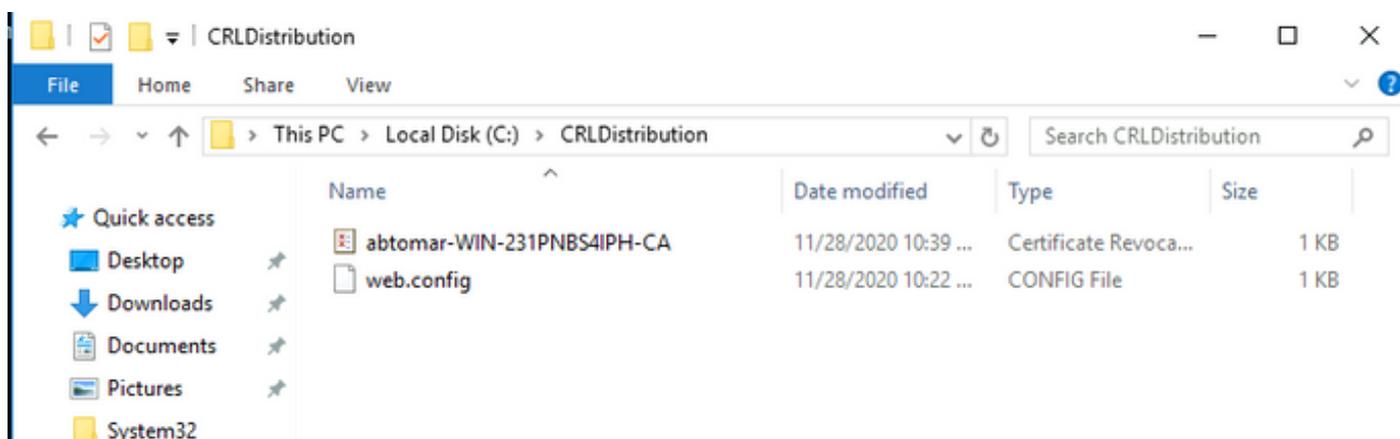
O servidor do Microsoft CA deve criar um novo arquivo .crl na pasta criada na seção 1. Se o novo arquivo de CRL for criado com êxito, não haverá nenhum diálogo depois de clicar em OK. Se um erro for retornado em relação à nova pasta do ponto de distribuição, repita cuidadosamente cada etapa desta seção.

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 <CANAME>.crl onde <CANAME> é o nome do servidor CA. Neste exemplo, o nome do arquivo é:

abtomar-WIN-231PNBS4IPH-CA.crl



2. Em uma estação de trabalho na rede (idealmente na mesma rede do nó de administração principal do ISE), abra um navegador da Web e navegue até <http://<SERVER>/<CRLSITE>>, onde <SERVER> é o nome do servidor do IIS configurado na seção 2 e <CRLSITE> é o nome do site escolhido para o ponto de distribuição na seção 2. Neste exemplo, a URL é:

http://win-231pnbs4iph/CRLD

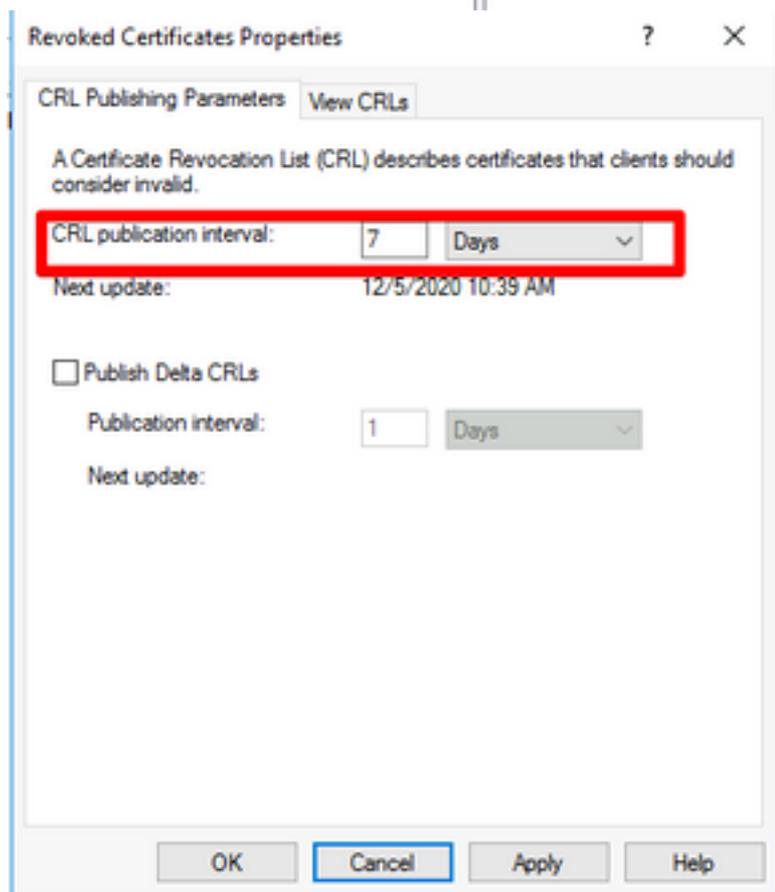
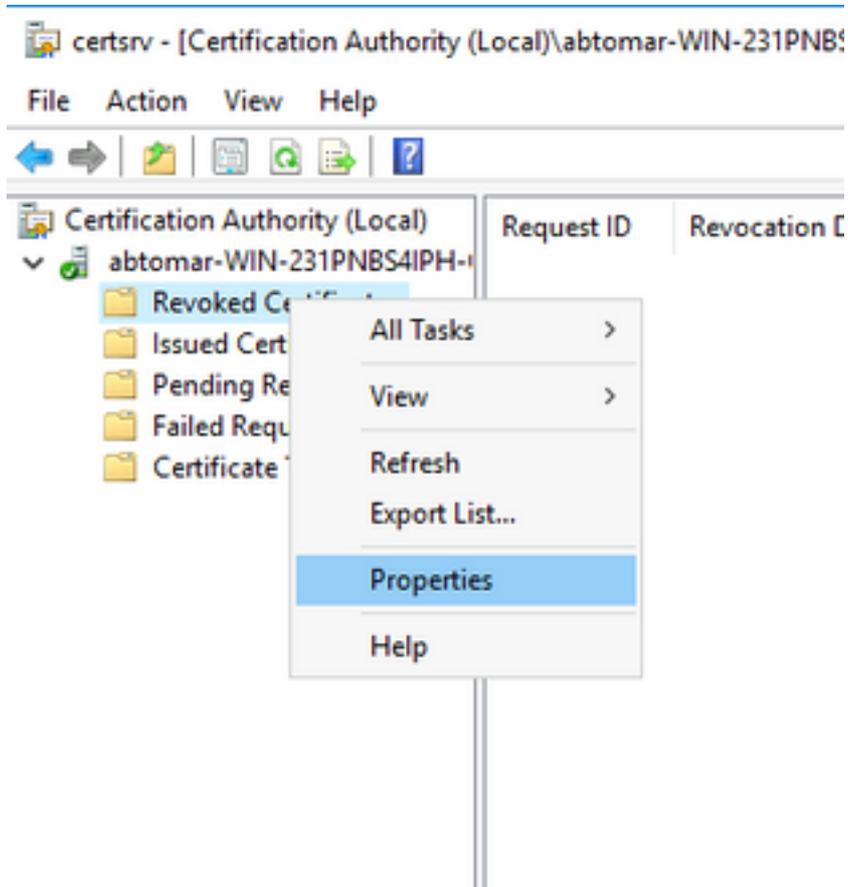
O índice do diretório é exibido, incluindo o arquivo observado na etapa 1.



Configurar o ISE para usar o novo ponto de distribuição 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 em potencial (no Microsoft CA) são de 1 hora a 411 anos, inclusive. O valor padrão é 1 semana. Depois que um intervalo apropriado para seu ambiente for determinado, defina o intervalo com estas instruções:

1. Na barra de tarefas do servidor CA, clique em **Iniciar**. Escolha **Ferramentas Administrativas > Autoridade de Certificação**.
2. No painel esquerdo, expanda a CA. Clique com o botão direito do mouse na pasta **Certificados Revogados** e escolha **Propriedades**.
3. Nos campos de intervalo de publicação da CRL, insira o número necessário e escolha o período. Clique em **OK** para fechar a janela e aplicar a alteração. Neste exemplo, um intervalo de publicação de 7 dias é configurado.



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

Saída de exemplo:

Values:

```
ClockSkewMinutes          REG_DWORDS = a (10)
```

CertUtil: -getreg command completed successfully.

5. Digite o comando **certutil -getreg CA\CRLov*** 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 comando **certutil -getreg CA\CRLpe*** para verificar o CRLPeriod, 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 carência da CRL da seguinte forma:

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

Else : SOBREPOSIÇÃO = (CRLPeriod / 10), em minutos

b. Se SOBREPOSIÇÃO > 720 então SOBREPOSIÇÃO = 720

c. Se SOBRELAP < (1,5 * ClockSkewMinutos) então SOBRELAP = (1,5 * ClockSkewMinutos)

d. Se SOBRELAP > CRLPeriod, em minutos, SOBRELAP = CRLPeriod em minutos

e. Período de carência = SOBREPOSIÇÃO + MinutosDeCaptura

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 Administrador primário do ISE e escolha **Administração > Sistema > Certificados**. No painel esquerdo, selecione **Certificado confiável**

Cisco ISE Administration - System

Deployment Licensing **Certificates** Logging Maintenance Upgrade Health Checks Backup & Restore Admin Access Settings Click h

Certificate Management System Certificates Trusted Certificates OSCP Client Profile Certificate Signing Requests Certificate Periodic Check Se... Certificate Authority >

Trusted Certificates

[Edit](#) [+ Import](#) [Export](#) [Delete](#) [View](#)

<input type="checkbox"/>	Friendly Name	Status	Trusted For	Serial Number	Issued To	Issued By	Valid From	Expiration Date	Expiration
<input type="checkbox"/>	Baltimore CyberTrust Root	Enabled	Cisco Services	02 00 00 B9	Baltimore CyberTrust ...	Baltimore CyberTrust ...	Sat, 13 May 2000	Tue, 13 May 2025	<input checked="" type="checkbox"/>
<input checked="" type="checkbox"/>	CA_Root	Enabled	Infrastructure Endpoints AdminAuth	4D 9B EE 97 53 ...	abtomar-WIN-231PN...	abtomar-WIN-231PN...	Wed, 20 Feb 2019	Sun, 20 Feb 2039	<input checked="" type="checkbox"/>
<input type="checkbox"/>	Cisco ECC Root CA 2009	Enabled	Cisco Services	03	Cisco ECC Root CA	Cisco ECC Root CA	Thu, 4 Apr 2013	Mon, 7 Sep 2009	<input checked="" type="checkbox"/>
<input type="checkbox"/>	Cisco Licensing Root CA	Enabled	Cisco Services	01	Cisco Licensing Root ...	Cisco Licensing Root ...	Fri, 31 May 2013	Mon, 31 May 2038	<input checked="" type="checkbox"/>

9. Marque a caixa de seleção ao lado do certificado CA para o qual você pretende configurar CRLs. Clique em **Editar**.

10. Perto da parte inferior da janela, marque a caixa de seleção **Download CRL**.

11. No campo URL de distribuição da CRL, insira o caminho para o Ponto de distribuição da CRL, que inclui o arquivo .crl, criado na seção 2. Neste exemplo, a 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 de CRL é estático, atualizações de CRL mais oportunas são obtidas quando a última opção é usada. Clique no botão de opção **Automatically (Automaticamente)**.

13. Defina o valor para recuperação para um valor menor que o período de cortesia calculado na etapa 7. Se o valor definido for maior que o período de carência, o ISE verificará o ponto de distribuição da CRL antes que a CA tenha publicado a próxima CRL. Neste exemplo, o período de carência é calculado em 730 minutos, ou 12 horas e 10 minutos. Um valor de 10 horas será usado para a recuperação

14. Defina o intervalo de nova tentativa como apropriado para o seu ambiente. Se o ISE não puder recuperar a CRL no intervalo configurado na etapa anterior, ele tentará novamente nesse intervalo mais curto.

15. Marque a caixa de seleção **Ignorar verificação de CRL se a CRL não for recebida** 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 na última tentativa de download. Se essa caixa de seleção não estiver 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 **Ignorar que a CRL ainda não é válida ou expirou** 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 considera uma CRL inválida antes da data de efetivação e depois dos tempos da próxima atualização. Clique em **Salvar** para concluir a configuração.

To verify certificates, enable the methods below. If both are enabled, OCSP will always be tried first.

OCSP Configuration

- Validate against OCSP Service
- Reject the request if OCSP returns UNKNOWN status
- Reject the request if OCSP Responder is unreachable

Certificate Revocation List Configuration

- Download CRL

CRL Distribution URL

Retrieve CRL

Automatically 10 Hours before expiration.

Every 1 Hours

If download failed, wait 10 Minutes before retry.

Enable Server Identity Check ⓘ

Bypass CRL Verification if CRL is not Received

Ignore that CRL is not yet valid or expired

Save

Informações internas da Cisco

1. Microsoft. "Configure um ponto de distribuição de CRL para certificados." <http://technet.microsoft.com/en-us/library/ee649260%28v=ws.10%29.aspx>, 7 de outubro de 2009 [18 de dezembro de 2012]
2. Microsoft. "Publicar manualmente a lista de revogação de certificados." <http://technet.microsoft.com/en-us/library/cc778151%28v=ws.10%29.aspx>, 21 de janeiro de 2005 [18 de dezembro de 2012]
3. Microsoft. "Configure períodos de sobreposição de CRL e CRL Delta." <http://technet.microsoft.com/en-us/library/cc731104.aspx>, 11 de abril de 2011 [18 de dezembro de 2012]
4. MS2065 [MSFT]. "Como se calcula a Data de Efetivação (esta atualização), NextUpdate e NextCRLPublish." <http://blogs.technet.com/b/pki/archive/2008/06/05/how-effectivedate-thisupdate-nextupdate-and-nextcrlpublish-are-calculated.aspx>, 4 de junho de 2008 [18 de dezembro de 2012]