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

# Contents

Introdução
Pré-requisito
Requisitos
Componentes Utilizados
Configurar
Criar e Configurar uma Pasta no CA para Armazenar os Arquivos CRL
Criar um Site no IIS para Expor o Novo Ponto de Distribuição de 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 de CRL
Verificar
Troubleshooting

# 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.

Advanced Sharing	
Share this folder	
Settings	
Share name:	
CRLDistribution\$	
Add Remove	
Limit the number of simultaneous users to:	
Comments:	
Permissions Caching	
OK Cancel Apply	

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

Advanced Sharing	🔋 Permissions for CRLDistributi	on\$	Se	elect Users, Computers, Service Account	s, or Groups
Share this folder Settings Share name: CRLDistribution\$ Add Remove	Share Permissions   Group or user names:			Select this object type: Users, Groups, or Built-in security principals From this location: Intpaaa.local Enter the object names to select ( <u>examples</u> );	3 Object Types Locations
Limit the number of simultaneous us Comments: 1 Permissions Caching OK C	2 Permissions for Everyone Full Control Change Read	Add	Remo	Object Types         Select the types of objects you want to         A         Object types:         Image: Service Accounts         Image: Computers         Image: Service Accounts         Image: Service Acco	find.
	Learn about access control and pr	ermissions			
	OK	Cancel	Apply		OK Cancel

5. Para retornar à janela Selecionar usuários, computadores, contas de serviço ou grupos, clique em ок. 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 ок.

Select Users, Computers, Service Accounts, or Groups	×
Select this object type: Users, Computers, Groups, or Built-in security principals	Object Types
From this location:	
abtomar.local	Locations
Enter the object names to select ( <u>examples</u> ):	
WIN-231PNBS4IPH	Check Names
Advanced OK	Cancel

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 ок. Clique ок novamente para fechar a janela Compartilhamento Avançado e retornar à janela Propriedades.

Permissions for CRLDistribu	utionS	>
Share Permissions		
Group or user names:		
Everyone	DMAR\WIN-231PNE	BS4IPH\$)
	Add	Remove
Permissions for WIN-231PNBS4IPH	Allow	Deny
Full Control Change Read	$\leq$	

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.

🚺 CRLDistribution Properties 🛛 🔀	Permissions for CRLDistribution
General Sharir Security Previous Versions Customize	Security
Object name: C:\CRLDistribution	Object name: C:\CRLDistribution
Group or user names:	Group or user names:
CREATOR OWNER	CREATOR OWNER
SYSTEM	SYSTEM
Administrators (H FRAA vadministrators)	Administrators (n 1 PAAA Vadministrators)
To okango porpissione oliok Edit	
Permissions for CBEATOB	
OWNER Allow Deny	Bermineiene for CREATOR
Full control	OWNER Allow Deny
Read & execute	Full control
List folder contents	Modify L L L
Read	List folder co
Select Users, Computers, Service Accounts, or Groups	Select the types of objects you want to find.
Select this object type:	ac Object types:
Users, Groups, or Built-in security principals 4	Object Types
From this location:	
rtpaaa.local	Locations
Enter the object names to select ( <u>examples</u> ):	Users
	Check Names
Advanced	

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.

Select Users, Computers, Service Accounts, or Groups	×
Select this object type:	
Users, Computers, Groups, or Built-in security principals	Object Types
From this location:	
abtomar.local	Locations
Enter the object names to select ( <u>examples</u> ):	
WIN-231PNBS4IPH	Check Names
Advanced OK	Cancel

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.

Permissions for CRLDistrib	oution	>
Security		
Object name: C:\CRLDistribu	ution	
Group or user names:		
SECREATOR OWNER		
SYSTEM		
Administrators (ABTOMAR	R\Administrators)	
MUN 221 DNDC 41DLL (ADT	OMADUWIN 221DND	
WIN-23 IPINBS4IPH (ABT	OMAR\WIN-23TPINE	(54IPH\$)
	Add	Remove
Permissions for		
WIN-231PNBS4IPH	Allow	Deny
Full control		□ <u>^</u>
Modify	$\checkmark$	
Read & execute	$\checkmark$	
List folder contents	$\checkmark$	
Read	$\checkmark$	
L	_	
OK	Cancel	Apply

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.

# 💐 Internet Information Services (IIS) Manager



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

Add Virtual Dire	ectory			? ×
Site name: Path:	Default Web Site /			
Alias:				
Example: ima	ges			
Physical path				
C:\CRLDistrib	ution			
Pass-through	authentication			
Connect as.	Test Settings	]		
		ОК	0	Cancel

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 οκ. Clique οκ para fechar a janela Adicionar Diretório Virtual.

Add Virtual Directory	?	$\times$
Site name: Default Web Site		
Path: /		
Alias:		
CRLD		
Example: images		
Physical path:	_	
C:\CRLDistribution .		
Pass-through authentication		
Connect as Test Settings		
ОК	Cancel	I

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.

Sinternet Information Services (IIS)	Manager					
← → E → WIN-231PNBS4II	PH 🕨 Sites 🕨	Default Web	Site + CRLD	•		
File View Help						
Connections	CR	LD Home	•			
Start Page     WIN-231PNBS4IPH (ABTOMA     Application Pools	Filter:		• 🐨 Go - 🕻	Show All	Group by:	
<ul> <li>✓ Image: Application Pools</li> <li>✓ Image: Sites</li> <li>✓ Image: Default Web Site</li> <li>&gt; Image: Defau</li></ul>	ASP	Authentic	2 Compression	Default Document	Directory Browsing	Error Pages
> 🔂 CRLD	Failed Request Tra	<b>Handler</b> Mappings	HTTP Redirect	HTTP Respon	Logging	MIME Types
	Modules	Output	Request	SSL Settings		
	Managemen	Caching	Filtering			^

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 suspensaallowDoubleEscaping, 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.

Enroliment Agents	Auditing	Recovery	y Agents	Securit
General	Policy Mode	ıle	Exit	Module
Extensions	Storage		Certificate I	Managers
Select extension:				
CDI Distribution Baist	(CDD)			
CRL Distribution Foint	(CDF)			
Specify locations from	which users can c	btain a ce	rtificate revo	ocation list
(CRL).				
C:\Windows\system3	2\CertSrv\CertEn	oll\ <cana< td=""><td>me&gt;<crln< td=""><td>lameSuffix&gt;</td></crln<></td></cana<>	me> <crln< td=""><td>lameSuffix&gt;</td></crln<>	lameSuffix>
Idap:///CN= <catrun< td=""><td>catedName&gt;<cri< td=""><td>NameSuff</td><td>ix&gt;,CN=<se< td=""><td>erverShortN</td></se<></td></cri<></td></catrun<>	catedName> <cri< td=""><td>NameSuff</td><td>ix&gt;,CN=<se< td=""><td>erverShortN</td></se<></td></cri<>	NameSuff	ix>,CN= <se< td=""><td>erverShortN</td></se<>	erverShortN
http://cServerDNSNs	ame>/CertEnroll/<	CaName>	<crlname< td=""><td>Suffix&gt;<del< td=""></del<></td></crlname<>	Suffix> <del< td=""></del<>
file://cControl DNCN	nas /CadEnnell / /	Mamaxel	CDI Mama C	Aller Bally
file:// <serverdnsnar< td=""><td>me&gt;/CertEnroll/<c< td=""><td>aName&gt;&lt;</td><td>CRLNameS</td><td>uffix&gt;<delta< td=""></delta<></td></c<></td></serverdnsnar<>	me>/CertEnroll/ <c< td=""><td>aName&gt;&lt;</td><td>CRLNameS</td><td>uffix&gt;<delta< td=""></delta<></td></c<>	aName><	CRLNameS	uffix> <delta< td=""></delta<>
file:// <serverdnsnar< td=""><td>me&gt;/CertEnroll/<c< td=""><td>aName&gt;&lt;</td><td>CRLNameS</td><td>uffix&gt;<delta< td=""></delta<></td></c<></td></serverdnsnar<>	me>/CertEnroll/ <c< td=""><td>aName&gt;&lt;</td><td>CRLNameS</td><td>uffix&gt;<delta< td=""></delta<></td></c<>	aName><	CRLNameS	uffix> <delta< td=""></delta<>
file:// <serverdnsnar< td=""><td>me&gt;/CertEnroll/<c< td=""><td>aName&gt;&lt;</td><td>CRLNameS</td><td>uffix&gt;<delta< td=""></delta<></td></c<></td></serverdnsnar<>	me>/CertEnroll/ <c< td=""><td>aName&gt;&lt;</td><td>CRLNameS</td><td>uffix&gt;<delta< td=""></delta<></td></c<>	aName><	CRLNameS	uffix> <delta< td=""></delta<>
file:// <serverdnsnar< td=""><td>me&gt;/CertEnroll/<c< td=""><td>aName&gt;&lt;</td><td>CRLNameS</td><td>uffix&gt;<delta< td=""></delta<></td></c<></td></serverdnsnar<>	me>/CertEnroll/ <c< td=""><td>aName&gt;&lt;</td><td>CRLNameS</td><td>uffix&gt;<delta< td=""></delta<></td></c<>	aName><	CRLNameS	uffix> <delta< td=""></delta<>
file:// <serverdnsnar< td=""><td>ne&gt;/CertEnroll/<c< td=""><td>aName&gt;&lt;</td><td>d</td><td>uffix&gt;<delta< td=""></delta<></td></c<></td></serverdnsnar<>	ne>/CertEnroll/ <c< td=""><td>aName&gt;&lt;</td><td>d</td><td>uffix&gt;<delta< td=""></delta<></td></c<>	aName><	d	uffix> <delta< td=""></delta<>
file:// <serverdnsnar< td=""><td>ne&gt;/CertEnroll/<c< td=""><td>aName&gt;&lt; Add</td><td>d</td><td>Remove</td></c<></td></serverdnsnar<>	ne>/CertEnroll/ <c< td=""><td>aName&gt;&lt; Add</td><td>d</td><td>Remove</td></c<>	aName>< Add	d	Remove
file:// <serverdnsnar all="" crls="" crls.="" in="" include="" ma<="" publish="" publishing="" td="" this="" to="" when=""><td>s location Specifies where tanually.</td><td>aName&gt;&lt; Add o publish in</td><td>d</td><td>Remove</td></serverdnsnar>	s location Specifies where tanually.	aName>< Add o publish in	d	Remove
File:// <serverdnsnar< td=""><td>s location Specifies where t anually.</td><td>aName&gt;&lt; Add o publish i</td><td>CRLNameS</td><td>e Directory</td></serverdnsnar<>	s location Specifies where t anually.	aName>< Add o publish i	CRLNameS	e Directory
File:// <serverdnsnar all="" cdp<="" cli="" crls="" crls.="" in="" include="" ma="" publish="" publishing="" td="" the="" this="" to="" when=""><td>s location Specifies where t anually.</td><td>aName&gt;&lt; Add o publish in d Delta Cl</td><td>n the Active</td><td>Remove Directory</td></serverdnsnar>	s location Specifies where t anually.	aName>< Add o publish in d Delta Cl	n the Active	Remove Directory
File:// <serverdnsnar all="" cdp<="" cli="" crls="" crls.="" in="" include="" ma="" publish="" publishing="" td="" the="" this="" to="" when=""><td>s location Specifies where t anually. ients use this to fir extension of issue</td><td>aName&gt;&lt; Add o publish in d Delta Cl d certificat</td><td>CRLNameS</td><td>Remove Directory</td></serverdnsnar>	s location Specifies where t anually. ients use this to fir extension of issue	aName>< Add o publish in d Delta Cl d certificat	CRLNameS	Remove Directory
file:// <serverdnsnar all="" cdp="" cli="" crls="" crls.="" crls<="" delta="" in="" include="" ma="" publish="" publishing="" td="" the="" this="" to="" when=""><td>ne&gt;/CertEnroll/<c s location Specifies where t anually. ients use this to fir extension of issue to this location</c </td><td>aName&gt;&lt; Add o publish in d Delta Cl d certificat</td><td>CRLNameS</td><td>e Directory</td></serverdnsnar>	ne>/CertEnroll/ <c s location Specifies where t anually. ients use this to fir extension of issue to this location</c 	aName>< Add o publish in d Delta Cl d certificat	CRLNameS	e Directory
file:// <serverdnsnar all="" cdp="" cli="" crls="" crls.="" delta="" e<="" idp="" in="" include="" ma="" publish="" publishing="" td="" the="" this="" to="" when=""><td>ne&gt;/CertEnroll/<c s location Specifies where t anually. ients use this to fir extension of issue to this location extension of issued</c </td><td>aName&gt;&lt; Add o publish in d Delta Cl d certificat</td><td>CRLNameS</td><td>e Directory</td></serverdnsnar>	ne>/CertEnroll/ <c s location Specifies where t anually. ients use this to fir extension of issue to this location extension of issued</c 	aName>< Add o publish in d Delta Cl d certificat	CRLNameS	e Directory
file:// <serverdnsnar all="" cdp="" cli="" crls="" crls.="" delta="" e<="" idp="" in="" include="" ma="" publish="" publishing="" td="" the="" this="" to="" when=""><td>ne&gt;/CertEnroll/<c s location Specifies where t anually. ients use this to fir extension of issue to this location extension of issued</c </td><td>aName&gt;&lt; Add o publish in d Delta Cl d certificat</td><td>CRLNameS</td><td>e Directory</td></serverdnsnar>	ne>/CertEnroll/ <c s location Specifies where t anually. ients use this to fir extension of issue to this location extension of issued</c 	aName>< Add o publish in d Delta Cl d certificat	CRLNameS	e Directory

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	×
A location can be any valid URL or path. Enter an HTTP, LDAP, file addres or enter a UNC or local path. To insert a variable into the URL or path, sele the variable below and click Insert.	is, ct
Location:	
\\WIN-231PNBS4IPH\CRLDistribution\$\	
Variable: <caname> Variable</caname>	
Description of selected variable:	
Used in URLs and paths Inserts the DNS name of the server Example location: http:// <serverdnsname>/CertEnroll/<caname><crln< td=""><td>٧a</td></crln<></caname></serverdnsname>	٧a
<	>
OK Cancel	

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

## 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></caname>
--

Variable:

<CaName>

Insert

Description of selected variable:

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

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

Add Location	×
A location can be any valid URL or path. Enter an HTTP, LDAP, file addres or enter a UNC or local path. To insert a variable into the URL or path, selec the variable below and click Insert.	s, t
Location:	
\\WIN-231PNBS4IPH\CRLDistribution\$\ <caname><crlnamesuffix></crlnamesuffix></caname>	٦
Variable: <crlnamesuffix> V Insert Description of selected variable:</crlnamesuffix>	
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><crlname< td=""><td>Si</td></crlname<></caname></servername>	Si
< :	>
OK Cancel	

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

\\WIN-231PNBS4IPH\CRLDistribution\$\

.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.

1002	diam -
and the last	

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

Variable:

<crlnamesuffix></crlnamesuffix>	~	Insert
		-

Description of selected variable:

Use App Exa	d in URLs and paths for the CRL Distribution Point ends a suffix to distinguish the CRL file name mple location: http:// <servername>/CertEnroll/<c< th=""><th>ts extension CaName&gt;<crlnamesเ< th=""></crlnamesเ<></th></c<></servername>	ts extension CaName> <crlnamesเ< th=""></crlnamesเ<>
<		>
	OK	Cancel

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.

Х

General       Policy Module       Ext Module         Extensions       Storage       Certificate Managers         elect extension:	Enrollment Agents	Auditing	Recovery Agents	Security	
Extensions       Storage       Certificate Managers         elect extension:	General	Policy Mo	dule Ext	t Module	
Gelect extension:         CRL Distribution Point (CDP)         opecify locations from which users can obtain a certificate revocation list CRL).         C:\Windows\system32\C         dap:///CN= <catruncate< td="">         http://<serverdnsname< td="">         WIN-231PRNES4IPHYC            You must restart Active Directory Certificate Services for the changes to take effect. Do you want to restart the service now?</serverdnsname<></catruncate<>	Extensions	Storage	Certificate	Managers	
CRL Distribution Point (CDP)       ✓         Specify locations from which users can obtain a certificate revocation list CRL).       ✓         C:\Windows\system32\C       Certification Authority         Idap:///CN= <catruncate< td="">       Certification Authority         http://<serverdnsname>       You must restart Active Directory Certificate Services for the changes to take effect. Do you want to restart the service now?</serverdnsname></catruncate<>	Select extension:				
Specify locations from which users can obtain a certificate revocation list CRL). C:\Windows\system32\C Idap:///CN= <catruncate http://<serverdnsname file://<serverdnsname You must restart Active Directory Certificate Services for the changes to take effect. Do you want to restart the service now?</serverdnsname </serverdnsname </catruncate 	CRL Distribution Point	(CDP)		~	
	Specify locations from [CRL).	which users car	n obtain a certificate rev	ocation list	

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 ок.

🙀 certsrv - [Certification Author	ity (Local)\abtoma	r-WIN	V-231PNBS4IPH-	CA\Revoked Certificates]	
File Action View Help					
🗢 🔿 🖄 🔛 🖾					
Certification Authority (Local)	Request ID	Re	vocation Date	Effective Revocation Date	
Bevoked Certificator			The	re are no items to show in th	is vi
Ssued Certificates	All Tasks	>	Publish		
Pending Requests Failed Requests	View	>			
Certificate Templa	Refresh				
	Export List				
	Properties				
	Help				

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.

E Cisco ISE					Admini	stration · System					
Deployment Licensing	Certificates	s Logging	Maintenance	Upgrade	Health Checks	Backup & Restor	e Admin Acce	ss Settings			Click h
Certificate Management ~ System Certificates	Trus	ted Certifi	cates								
Trusted Certificates	0 Edit	+ Import 🕁 Ex	port 🚦 Delete	Q View							
OCSP Client Profile Certificate Signing Requests	0	Friendly Name		∧ Status	Trusted For	Serial Number	Issued To	Issued By	Valid From	Expiration Date	Expiratio
Certificate Periodic Check Se	0	Baltimore CyberTrust P	Root	Enabled	Cisco Services	02 00 00 B9	Baltimore CyberTrust	Baltimore CyberTrust	Sat, 13 May 2000	Tue, 13 May 2025	
Certificate Authority >		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	
		Cisco ECC Root CA 20	099	Enabled	Cisco Services	03	Cisco ECC Root CA	Cisco ECC Root CA	Thu, 4 Apr 2013	Mon, 7 Sep 2099	
		Cisco Licensing Root (	CA	Enabled	Cisco Services	01	Cisco Licensing Root	Cisco Licensing Root	Fri, 31 May 2013	Mon, 31 May 2038	

- 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 seleçãoDownload 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.

Certificate Status Validation								
	To verify certificates, enable the m OCSP Configuration Validate against OCSP Servic Reject the request if OC Reject the request if OC Certificate Revocation List Configur Overliacet CRL	ethods below. If bo se SP returns UNKNC SP Responder is u ation	th are enabled, OC: WN status nreachable	3P will always be t ,	tried first.			
	CRL Distribution URL	http://win-231	pnbs4iph/crld/abt	omar-WIN-231	PNBS4IPH-CA.crl			
	Retrieve CRL	Automatically     Every	10 1		Hours	~	before expiration.	
	If download failed, wait	10		Minutes	~	before retry.		
	Enable Server Iden     Bypass CRL Verific     Ignore that CRL is	tity Check () ation if CRL is not not yet valid or exp	Received					
							Sa	ve

## 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.