## 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<sup>®</sup> Server<sup>®</sup> 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**.

CRLDistribution Properties	×
General Sharing Security Previous Versions Customize	
Network File and Folder Sharing CRLDistribution Not Shared Network Path: Not Shared	
Share	
Advanced Sharing Set custom permissions, create multiple shares, and set other advanced sharing options.	
	400
Close Cancel Apply	10.00

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.

e: pution\$			
e: pution\$			
oution\$			
Remove			
1263011150.37502			
ons Cach	ing		
	ons Cach	ons	; ons Caching

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

Advanced Sharing	🔋 Permissions for CRLDistributio	n\$	Se	elect l	lsers, Computers, Service Accounts, or Gro	oups	? ×
Share this folder	Share Permissions			Select	this object type:		
- Settings	Group or user names:			Users,	Groups, or Built-in security principals	3	Object Types
Share name:	& Everyone			From th	is location:		
CRLDistribution\$				rtpaaa	local		Locations
Add Remove				<u>E</u> nter ti	ne object names to select ( <u>examples)</u> :		
Limit the number of simultaneous us				0			Charle Names 1
cinic dis names of similar boas as					Jbject Types		Y X
Comments:	Z _	Add	Hemo'		Select the types of objects you want to find.		
	Permissions for Everyone	Allow	Deny		Object types:		
	Full Control		<u> </u>		🗹 🍇 Built-in security principals		
1 Permissions Caching	Change Bead		H		Service Accounts		
			-		☑ & Groups		
ок 1 с					🗹 🤱 Users		
			_				
	Learn about access control and per	missions	~				
	OK	Cancel	Apply	۶ <u>ــــــــــــــــــــــــــــــــــــ</u>		OK	Cancel

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**.

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 (examples):	
WIN-231PNBS4IPH	Check Names
Advanced OK	Cancel

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.

Permissions for CRLD	Distributio	on\$		Х
Share Permissions				
Group or user names:				
Everyone	I (ABTOM	AR\WIN-231PNI	BS4IPH\$)	
		Add	Remove	
Permissions for WIN-231PNBS4IPH		Allow	Deny	
Full Control		$\mathbf{\nabla}$		
Change				Н
11680		Ľ.		Н
				Н
				Н
				1
	OK	Cancel	Apply	

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).

🚺 CRLDistribution Properties 🛛 💌	Example 2 Permissions for CRLDistribution
General Sharii 1 Security Previous Versions Customize	Security
Object name: C:\CRLDistribution	Object name: C:\CRLDistribution
Group or user names:	Group or user names:
CREATOR OWNER	A CREATOR OWNER
SYSTEM	SYSTEM     Administrators (BTRAAA\Administrators)
& Users (RTPAAA/Users)	& Users (RTPAAA\Users)
Permissions for CREATOR	
OWNER Allow Deny	Add Remove
Full control	OWNER Allow Deny
Read & execute	Full control
List folder contents	
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 (examples):	Service Servic
	Check Names
Advanced	Cancel OK Cancel

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**.

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 (examples):	
WIN-231PNBS4IPH	Check Names
Advanced	OK Cancel

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.

Permissions for CRLDistributi	on	×
Security		
Object name: C:\CRLDistribution	n	
Group or user names:		
SECREATOR OWNER		
SYSTEM Redministrators (ABTOMAR\A)	dministrators)	
Users (ABTOMAR\Users)	anni nacideora/	
WIN-231PNBS4IPH (ABTOM	IAR\WIN-231PNB	S4IPH\$)
	Add	Remove
Permissions for WIN-231PNBS4IPH	Allow	Deny
Full control		□ ^
Modify		
Read & execute	$\checkmark$	
List folder contents	$\checkmark$	
Read		
-		
ОК	Cancel	Apply

#### 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.

#### 💐 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 Directory	?	×
Site name: Default Web Site		
Path: /		
Alias:		
CRLD		
Example: images		
Physical path:		
C:\CRLDistribution		
Pass-through authentication		
Connect as Test Settings		
ОК	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.

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

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.

Internet Information Services (IIS)	Manager	– 🗆 X
← → 21 + WIN-231PNB54I	PH + Sites + Default Web Site + CRLD +	🔤 🖂 🔂 🔍 •
File View Help		
Connections	Cirectony Browsing	Alerts
Q	Directory browshig	Directory browsing has been     disabled
WIN-231PNBS4IPH (ABTOMA	Use this feature to specify the information that displays in a directory listing.	Actions
- Application Pools	✓ Time	Rf Analy
V 😔 Sites	Size	Be Cancel
> 😴 CertEnroll	C Extension	Enable
> CRLD	✓ Date	😢 Help
	Long date	

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**.
- 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.

		perties		?	×
Enrollment Agents	Auditing	Recov	ery Agents	Sec	urity
General	Policy Mo	dule	E	xit Module	
Extensions	Storage		Certificate	Manager	s
Select extension:					
Select extension:	(000)				
CRL Distribution Point	(CDP)				~
Specify locations from v	which users car	n obtain a c	ertificate re	vocation I	ist
(CRL).					
C:\Windows\system3	2\CertSrv\Cert	Enroll\ <cal< td=""><td>lame&gt;<crl< td=""><td>NameSuf</td><td>fix&gt;&lt;</td></crl<></td></cal<>	lame> <crl< td=""><td>NameSuf</td><td>fix&gt;&lt;</td></crl<>	NameSuf	fix><
Idap:///CN= <catrunc< td=""><td>atedName&gt;<c< td=""><td>RLNameSu (CaName</td><td>iffix&gt;,CN=&lt;</td><td>ServerSho</td><td>ortNar Dolta</td></c<></td></catrunc<>	atedName> <c< td=""><td>RLNameSu (CaName</td><td>iffix&gt;,CN=&lt;</td><td>ServerSho</td><td>ortNar Dolta</td></c<>	RLNameSu (CaName	iffix>,CN=<	ServerSho	ortNar Dolta
file:// <serverdnsnan< td=""><td>ne&gt;/CertEnroll/</td><td><caname></caname></td><td><crlname< td=""><td>Suffix&gt;<d< td=""><td>)eltaC</td></d<></td></crlname<></td></serverdnsnan<>	ne>/CertEnroll/	<caname></caname>	<crlname< td=""><td>Suffix&gt;<d< td=""><td>)eltaC</td></d<></td></crlname<>	Suffix> <d< td=""><td>)eltaC</td></d<>	)eltaC
<		_			>
		A	dd	Remov	/e
Publish CRLs to this	location	A	dd	Remov	/e
Publish CRLs to this Include in all CRLs. when publishing ma	s location Specifies when nually.	A e to publish	dd	Remov	re ny
Publish CRLs to this Include in all CRLs. when publishing ma Include in CRLs. Cli	s location Specifies when nually. ents use this to	e to publish	dd n in the Activ CRL locatio	Remov ve Directo ns.	re Iry
<ul> <li>Publish CRLs to this</li> <li>Include in all CRLs. when publishing ma</li> <li>Include in CRLs. Cli</li> <li>Include in the CDP</li> </ul>	s location Specifies when nually. ents use this to extension of iss	e to publish find Delta ued certific	dd in the Activ CRL locatio	Remov ve Directo ns.	ny
<ul> <li>Publish CRLs to this</li> <li>Include in all CRLs. when publishing ma</li> <li>Include in CRLs. Cli</li> <li>Include in the CDP</li> <li>Publish Delta CRLs</li> </ul>	s location Specifies when nually. ents use this to extension of iss to this location	e to publish find Delta ued certific	dd in the Activ CRL locatio	Remov ve Directo ns.	ny
Publish CRLs to this Include in all CRLs. when publishing ma Include in CRLs. Cli Include in the CDP Publish Delta CRLs Include in the IDP a	s location Specifies when nually. ents use this to extension of iss to this location	e to publish find Delta ued certific	dd n in the Activ CRL locatio	Remov ve Directo ns.	re ny
<ul> <li>Publish CRLs to this</li> <li>Include in all CRLs. when publishing ma</li> <li>Include in CRLs. Cli</li> <li>Include in the CDP</li> <li>Publish Delta CRLs</li> <li>Include in the IDP e</li> </ul>	s location Specifies when nually. ents use this to extension of iss to this location extension of issu	e to publish find Delta ued certific	dd n in the Activ CRL locatio	Remov ve Directo ns.	re ny
<ul> <li>Publish CRLs to this</li> <li>Include in all CRLs. when publishing ma</li> <li>Include in CRLs. Cli</li> <li>Include in the CDP</li> <li>Publish Delta CRLs</li> <li>Include in the IDP e</li> </ul>	s location Specifies when nually. ents use this to extension of iss to this location extension of issu	e to publish find Delta ued certific	dd n in the Activ CRL locatio	Remov ve Directo ns.	re ny
<ul> <li>Publish CRLs to this</li> <li>Include in all CRLs. when publishing ma</li> <li>Include in CRLs. Cli</li> <li>Include in the CDP</li> <li>Publish Delta CRLs</li> <li>Include in the IDP e</li> </ul>	s location Specifies when nually. ents use this to extension of iss to this location extension of issu	e to publish find Delta ued certific	dd n in the Activ CRL locatio	Remov ve Directo ns.	re iry

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 address or enter a UNC or local path. To insert a variable into the URL or path, selec the variable below and click Insert.	i. t
Location:	
\\WIN-231PNBS4IPH\CRLDistribution\$\	
Variable:	
<caname> V Insert</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>а</td></crln<></caname></serverdnsname>	а
< 2	,
OK Cancel	

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

Д		L		<b>c</b>	a	tı	o	n
		-	~	-	•	•••	~	•••

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\CRI	Distribution\$\ <cal< td=""><td>Name&gt;</td><td></td></cal<>	Name>	
Variable:			
<caname></caname>		~	Insert
Description of selected varia	ble:		
Used in URLs and paths Inserts the DNS name of th Example location: http:// <s< td=""><td>e server erverDNSName&gt;/</td><td>CertEnroll/<ca< td=""><td>aName&gt;<crlna< td=""></crlna<></td></ca<></td></s<>	e server erverDNSName>/	CertEnroll/ <ca< td=""><td>aName&gt;<crlna< td=""></crlna<></td></ca<>	aName> <crlna< td=""></crlna<>
<			>
	_		
		ОК	Cancel

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.	i. t
Location:	
\\WIN-231PNBS4IPH\CRLDistribution\$\ <caname><crlnamesuffix></crlnamesuffix></caname>	٦
Madaklar	_
Vanable:	1
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><crlnames< td=""><td>it.</td></crlnames<></caname></servername>	it.
< >	
OK Cancel	

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</crlnamesuffix></caname>	7
Variable:	
Description of selected variable:	1
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><crlnames< td=""><td></td></crlnames<></caname></servername>	
< >	
OK Cancel	

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 Ative Diretory. Clique em Sim.

Enrollment Agents	Auditing	Recovery Agents	Security		
General	Policy Mo	dule Ex	t Module		
Extensions	Storage	Storage Certificate Managers			
Select extension:					
CRL Distribution Point	t (CDP)		~		
Specify locations from (CRL).	which users car	n obtain a certificate rev	rocation list		
C:\Windows\system3 Idao:///CN= <catrun< th=""><th>2\C cate</th><th>ion Authority</th><th></th><th></th><th></th></catrun<>	2\C cate	ion Authority			
http:// <serverdnsn file://<serverdnsna WWIN-231PNBS4IP &lt;</serverdnsna </serverdnsn 	ame HVC	You must restart A take effect. Do you	ctive Directory Co want to restart t	ertificate Services for the changes to he service now?	
http:// <serverdnsn file://<serverdnsna WWIN-231PNBS4IP C Publish CRLs to thi</serverdnsna </serverdnsn 	ame me> HNC	You must restart Ad take effect. Do you	ctive Directory Co want to restart t	ertificate Services for the changes to he service now? Yes No	

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.

 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:

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**.
- 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.

Certification	Authorit -WIN-231	y (Local) PNBS4IPH-1	Request ID	Revocatio	on (
Revol	ked Ce d Cert	All Tasks	>		
Pend	ing Re	View	>		
Certif	ficate '	Refresh			
		Export List			
		Properties			
		Help			
CRL Publishing Par A Certificate Revo	ameters M	ew CRLs CRL) describes cer	tificates that client	s should	
CDL exhibition in	terval:	7 Dave	s ~		
CRL publication in Next update:		12/5/2020 10	39 AM	-	

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\_DWORS = 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				Admin	istration · System					
Deployment Licensing	Certificate	s Logging Ma	intenance Upgrade	Health Checks	Backup & Resto	re Admin Acce	ss Settings			Click h
Certificate Management ~ System Certificates	Trus	ted Certifica	tes							
Trusted Certificates	0 Edit	+ Import 🏾 🕁 Export	Delete Q View							
OCSP Client Profile Certificate Signing Requests		Friendly Name	∧ Status	Trusted For	Serial Number	Issued To	Issued By	Valid From	Expiration Date	Expiratio
Certificate Periodic Check Se		Baltimore CyberTrust 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 98 EE 97 53	abtomar-WIN-231PN	abtomar-WIN-231PN	Wed, 20 Feb 2019	Sun, 20 Feb 2039	
	0	Cisco ECC Root CA 2099	Enabled	Cisco Services	03	Cisco ECC Root CA	Cisco ECC Root CA	Thu, 4 Apr 2013	Mon, 7 Sep 2099	
		Cisco Licensing Root CA	Z 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 **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.

Certificate	Status	Validation
-------------	--------	------------

Validate against OCSP Service	:e		/				
Reject the request if OC	SP returns UNKNO	WN status					
Reject the request if OC	SP Responder is u	inreachable					
Certificate Revocation List Configur	ation						
Download CRL							
CRL Distribution URL	http://win-231	pnbs4iph/crld/at	tomar-WIN-23	1PNBS4IPH-C	CA.crl		
	<ul> <li>Automatically</li> </ul>	10		Hours		~	before expiration.
Retrieve CRL	<ul> <li>Every</li> </ul>	1		Hours		~	
If download failed, wait	10		Minutes		~	before retry.	
Enable Server Iden	tity Check 🕕						

Informações internas da Cisco

1. Microsoft. "Configure um ponto de distribuição de CRL para certificados." <u>http://technet.microsoft.com/en-us/library/ee649260%28v=ws.10%29.aspx</u>, 7 de outubro de 2009 [18 de dezembro de 2012]

2. Microsoft. "Publicar manualmente a lista de revogação de certificados." <u>http://technet.microsoft.com/en-us/library/cc778151%28v=ws.10%29.aspx</u>, 21 de janeiro de 2005 [18 de dezembro de 2012]

3. Microsoft. "Configure períodos de sobreposição de CRL e CRL Delta." <u>http://technet.microsoft.com/en-us/library/cc731104.aspx</u>, 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." <u>http://blogs.technet.com/b/pki/archive/2008/06/05/how-effectivedate-thisupdate-nextupdate-and-nextcrlpublish-are-calculated.aspx</u>, 4 de junho de 2008 [18 de dezembro de 2012]