ISEの証明書失効リストを公開するための Microsoft CAサーバの設定

内容

概要 <u>前提条件</u> <u>要件</u> 使用するコンポーネント <u>設定</u> <u>CRLファイルを格納するフォルダをCA上で作成および設定する</u> <u>新しいCRL分散ポイントを公開するサイトをIISに作成する</u> <u>分散ポイントにCRLファイルを公開するためのMicrosoft CAサーバの設定</u> <u>CRLファイルが存在し、IIS経由でアクセス可能であることを確認する</u> 新しいCRL分散ポイントを使用するようにISEを設定します

概要

このドキュメントでは、Internet Information Services(IIS)を実行して証明書失効リスト(CRL)の更 新を公開するMicrosoft Certificate Authority(CA)サーバの設定について説明します。また、証明書 検証で使用する更新を取得するようにCisco Identity Services Engine(ISE)(バージョン3.0以降)を設定する方法についても説明します。証明書の検証で使用する各種 CA ルート証明書の CRL を取得するように、ISE を設定できます。

前提条件

要件

このドキュメントに特有の要件はありません。

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- Cisco Identity Services Engineリリース3.0
- Microsoft Windows[®] Server^{® 2008 R2}

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このド キュメントで使用するすべてのデバイスは、初期(デフォルト)設定の状態から起動しています 。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してく ださい。

設定

このセクションでは、このドキュメントで説明する機能を設定するために必要な情報を提供して

います。

CRLファイルを格納するフォルダをCA上で作成および設定する

最初の作業は、CA サーバ上に CRL ファイルを保存する場所を設定することです。デフォルトでは、Microsoft CAサーバはファイルをC:\Windows\system32\CertSrv\CertEnroll\に発行**します**

このシステム フォルダを使用する代わりに、ファイル用の新しいフォルダを作成します。

1. IISサーバで、ファイルシステム上の場所を選択し、新しいフォルダを作成します。この例で は、フォルダ C:\CRLDistribution が作成されます。

🏪 📔 🛃 🚽 🕹 Local Disk	: (C:)
File Home Share	View
← → × ↑ 🏪 > Thi	is PC → Local Disk (C:) →
 Quick access Desktop Downloads Documents Documents Pictures System32 This PC Desktop 	Name CRLDistribution DerfLogs PerfLogs Program Files Visers Windows

2. CAがCRLファイルを新しいフォルダに書き込むには、共有を有効にする必要があります。新し いフォルダを右クリックして [Properties] **を選択し、[Sharing]** タブをクリックしてから [Advanced Sharing] をクリックします。

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

3.フォルダを共有するには、[このフォルダを共有する]チェックボックスをオンにして、[共有名]フィールドの共有名の最後にドル記号(\$)を追加して共有を非表示にします。

Settings Share name: CRLDistribution\$ Add Remove Limit the number of simultaneous users to: 77216	Settings Share name: CRLDistribution\$ Add Remove Limit the number of simultaneous users to: 77216 •	Share th	aring is folder
Share name: CRLDistribution\$ Add Remove Limit the number of simultaneous users to: 77216	Share name: CRLDistribution\$ Add Remove Limit the number of simultaneous users to: 77216 Comments: Permissions Caching	Settings -	
CRLDistribution\$ Add Remove Limit the number of simultaneous users to: 77216 🛬 Comments:	CRLDistribution\$ Add Remove Limit the number of simultaneous users to: 77216 Comments: Comments: Caching	Share na	ame:
Add Remove Limit the number of simultaneous users to: 77216 🛬 Comments:	Add Remove Limit the number of simultaneous users to: 77216 🔆 Comments: Comments: Caching	CRLDist	tribution\$
Limit the number of simultaneous users to: 77216	Limit the number of simultaneous users to: 77216	Add	Remove
	Permissions Caching	Commen	ts:

4. [**Permissions**] (1)をクリックし、[**Add**] (2)、[**Object Types**] (3)をクリックし、[Computers] チェ ックボックスをオンにします(4)。

Advanced Sharing	Permissions for CRLDistribution\$		Select Users, Computers, Service Accounts, or Groups	? ×
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 this location:	
CRLDistribution\$			jrtpaaa.local	Locations
Add Remove			Enter the object names to select (<u>examples</u>):	
Limit the number of simultaneous us			Object Types	Check Names
Comments:	2 _	Add Remo	Select the types of objects you want to find.	
	Permissions for Everyone	Allow Deny	vA Object types:	
	Full Control	<u> </u>	E Built-in security principals	
1 Permissions Caching	Change Bead		Service Accounts	
			Groups	
ок (с			Users	
	Learn about access control and permis	ssions		
	ОК	Cancel A	Apply	OK Cancel

5. [OK] をクリックして、[Select Users, Computers, Service Accounts, or Groups] ウィンドウに 戻ります。[Enter the object names to select]フィールドに、この例のCAサーバのコンピュータ名 を入力します。WIN0231PNBS4IPHを選択し、[名前の確認]をク**リックします**。入力された名前 が有効な場合は、名前が更新されて下線が付きます。[OK] をクリックします。

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. [Group or user names] フィールドで CA コンピュータを選択します。CAへのフルアクセスを 許可するには、[Full Control]の[Allow]をオンにします。

[OK] をクリックします。[OK] を再度クリックして [Advanced Sharing] ウィンドウを閉じ、 [Properties] ウィンドウに戻ります。

Permissions for CRLDistribution	on\$	2	×
Share Permissions			
Group or user names: Everyone WIN-231PNBS4IPH (ABTOM	AR\WIN-231PNE	3S4IPH \$)	
D	Add	Remove	
WIN-231PNBS4IPH	Allow	Deny	
Full Control Change Read	NN		

7. CAがCRLファイルを新しいフォルダに書き込むようにするには、適切なセキュリティ権限を設定します。[Security] **タブをクリックし(1)、[Edit]** をクリックして(2)、[Add] をクリックしてから(3)、[Object Types] **をクリックして(4)、[Computers] チェック ボックスをオンにします(5)。**

🚶 CRLDistribution Properties 🛛 🛛 🗙	Permissions for CRLDistribution	1
General Sharir 1 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 (A FFAAA (Administrators)	& Users (RTPAAA\Users)	
T. dama and T. C. T. T. D.		
Permissions for CREATOR		
OWNER Allow Deny	3 Add Remove	
Full control	OWNER Allow Deny	
Modify Read & everyte	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 chiect ture:	ac Object types:	
Users, Groups, or Built-in security principals	Object Types	
From this location		
rtpaaa.local	Locations	
Enter the object names to select (examples)	🗹 🤱 Users	
	Check Names	
<u></u>		
Advanced	Cancel	OK Cancel

8. [Enter the object names to select]フィールドで、CAサーバのコンピュータ名を入力し、[**Check Names]をクリックします**。入力された名前が有効な場合は、名前が更新されて下線が付きます。 [OK] をクリックします。

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

9. [Group or user names]フィールドでCAコンピュータを選択し、[Allow for Full control]をオンに してCAへのフルアクセスを許可します。[**OK**]をク**リック**し、[閉じる]をク**リック**してタスクを完 了します。

Permissions for Crebistibut	on	×
Security		
Object name: C:\CRLDistribution	n	
Group or user names:		
SECREATOR OWNER		
SYSTEM		
Administrators (ABTOMAR\Ad	dministrators)	
Sers (ABTOMAR\Users)		
WIN-231PNBS4IPH (ABTOM	IAR\WIN-231PNB	S4IPHS)
	Add	Remove
Permissions for	Add	Remove
Permissions for WIN-231PNBS4IPH	Add Allow	Remove Deny
Permissions for WIN-231PNBS4IPH Full control	Allow	Deny
Permissions for WIN-231PNBS4IPH Full control Modify	Add Allow	Deny
Permissions for WIN-231PNBS4IPH Full control Modify Read & execute	Add Allow	Deny
Permissions for WIN-231PNBS4IPH Full control Modify Read & execute List folder contents	Add Allow	Deny
Permissions for WIN-231PNBS4IPH Full control Modify Read & execute List folder contents Read	Add	Remove
Permissions for WIN-231PNBS4IPH Full control Modify Read & execute List folder contents Read	Add	Remove
Permissions for WIN-231PNBS4IPH Full control Modify Read & execute List folder contents Read	Add	Remove

新しいCRL分散ポイントを公開するサイトをIISに作成する

ISE が CRL ファイルにアクセスできるように、CRL ファイルを格納するディレクトリを IIS 経由 でアクセス可能にします。

- 1. IIS サーバのタスクバーで、[Start] をクリックします。[Administrative Tools] > [Internet Information Services (IIS) Manager] を選択します。
- 2. 左側のペイン(コンソール ツリー)で、IIS のサーバ名を展開し、次に [Sites] **を展開します**。



3.次の図に示すように、[**Default Web Site]を右**クリック**し、[Add Virtual Directory]**を選択します 。

📬 Internet Information Services (IIS) Manager



4. [Alias]フィールドに、CRL分散ポイントのサイト名を入力します。この例では、「CRLD」と入 力されています。

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.省略記号(...)[物理パス]フィールドの右側で、セクション1で作成したフォルダを参照します。フォルダを選択し、[**OK**]をクリックします。[OK] をクリックして [Add Virtual Directory] ウィンドウを閉じます。

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

6.手順4で入力したサイト名は、左側のペインで強調表示する必要があります。強調表示されない 場合は、ここで選択します。中央のペインで、[Directory Browsing] をダブルクリックします。



7.右側のペインでEnableをクリックして、ディレクトリの参照を有効にします。

Internet Information Services (IIS)	Manager	– 🗆 X
← → 21 + WIN-231PNB54I	PH + Sites + Default Web Site + CRLD +	🖬 🖂 🏠 🛞 •
File View Help		
Connections Q III 2 B.	Directory Browsing	Alerts Directory browsing has been disabled.
 WIN-231PNBS4IPH (ABTOMA Application Pools Sites CertEnroll CertEnroll CertSrv CRLD 	Use this feature to specify the information that displays in a directory listing.	Actions R/ Apply Rc Cancel Enable Help

8.左側のペインで、サイト名を再度選択します。中央のペインで、[Configuration Editor] をダブル クリックします。



9. [セクション]ドロップダウンリストで、[system.webServer/security/requestFiltering]を選択しま す。[allowDoubleEscaping] ドロップダウンリストで、[True] を選択します。次の図に示すように 、右側のペインでApplyをクリックします。



これで、フォルダにIIS経由でアクセスできるようになります。

分散ポイントにCRLファイルを公開するためのMicrosoft CAサーバの設定

CRLファイルを格納するように新しいフォルダが設定され、そのフォルダがIISで公開されるよう になったので、CRLファイルを新しい場所に公開するようにMicrosoft CAサーバを設定します。

- 1. CA サーバのタスクバーで、[Start] をクリックします。[Administrative Tools] > [Certificate Authority] を選択します。
- 2. 左側のペインで、CA の名前を右クリックします。[Properties] を選択し、[Extensions] タブ をクリックします。新しい CRL 分散ポイントを追加するために、[Add] をクリックします。

abtomar-WIN-231PNB	S4IPH-CA Pro	perties		?	×		
Enrollment Agents	Auditing	Recov	ery Agents	Sec	urity		
General	Policy Mo	odule	Exi	t Module			
Extensions	Storage		Certificate	Managers	3		
Select extension:							
CRL Distribution Point	(CDP)				\sim		
Specify locations from (CRL).	which users car 2\CertSrv\Cert	n obtain a c	Vame> <crli< td=""><td>ocation li</td><td>st</td></crli<>	ocation li	st		
Idap:///CN= <catruncatedname><crlnamesuffix>,CN=<servershortnar http://<serverdnsname>/CertEnroll/<caname><crlnamesuffix><delta file://<serverdnsname>/CertEnroll/<caname><crlnamesuffix><deltac< td=""></deltac<></crlnamesuffix></caname></serverdnsname></delta </crlnamesuffix></caname></serverdnsname></servershortnar </crlnamesuffix></catruncatedname>							
					2		
		A	dd	Remov	e		
Publish CRLs to this	s location						
Include in all CRLs. Specifies where to publish in the Active Directory when publishing manually.							
Include in CRLs. Clients use this to find Delta CRL locations.							
Include in the CDP extension of issued certificates							
Publish Delta CRLs to this location							
Include in the IDP e	extension of issu	ued CRLs					
ОК	Canc	el	Apply	He	lp		

3. 「場所」フィールドに、セクション1で作成および共有したフォルダへのパスを入力します。 セクション1の例では、パスは次のとおりです。

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.	s. t
Location:	
\\WIN-231PNBS4IPH\CRLDistribution\$\	
Variable	_
<pre>valiable. </pre>	
Kourrance - Inder	
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	Þ
OK Cancel	

4. [Location]フィールドに値を入力し、[Variable]ドロップダウンリストから**<CaName>を選択**し 、[**Insert**]をクリック**します。**

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.	s. t
Location:	
\\WIN-231PNBS4IPH\CRLDistribution\$\ <caname></caname>	
Variable:	
<caname> V Insert</caname>	1
Description of selected variable:	
Used in URLs and paths Inserts the DNS name of the server Example location: http:// <serverdnsname>/CertEnroll/<caname><crlna< td=""><td>a</td></crlna<></caname></serverdnsname>	a
< >	·
OK Cancel	

5.「変数」ドロップダウン・リストから<CRLNameSuffix>を選択し、「挿入」をクリックします o

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.	s. t
Location:	
\\WIN-231PNBS4IPH\CRLDistribution\$\ <caname><crlnamesuffix></crlnamesuffix></caname>	
Vadabla	_
	- I
<crlname suffix=""> V Insert</crlname>	
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>×</td></crlnames<></caname></servername>	×
< 2	•
OK Cancel	

6. [場所]フィールドで、パス**の最後**に.crlを追加します。この例では、[Location] は次のようにな ります。

\\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>	
Variable:	
<crlnamesuffix> V Insert</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><crlnames< td=""><td>ic</td></crlnames<></caname></servername>	ic
< >	
OK Cancel	

7. [OK] をクリックして [Extensions] タブに戻ります。[Publish CRLs to **this location]チェックボ ックスをオン**にし、[**OK**]をクリックして[Properties]ウィンドウを閉じます。

Active Directory 証明書サービスを再開する許可を求めるメッセージが表示されます。[Yes] を クリックします。

Enrollment Agents	Auditing	Recovery Agents	Security	
General	Policy Mod	dule Ext	Module	
Extensions	Storage	Certificate I	Managers	
Select extension:				
CRL Distribution Point	(CDP)		~	
Specify locations from CRL). C:\Windows\system3 Idap:///CN= <catrun http://<serverdnsna file://<serverdnsna< td=""><td>2\C cate me</td><td>obtain a certificate rev</td><td>ocation list</td><td></td></serverdnsna<></serverdnsna </catrun 	2\C cate me	obtain a certificate rev	ocation list	
<		You must restart Ac take effect. Do you	tive Directory Ce want to restart th	rtificate Services for the changes to ie service now?
Debter CDL et a thi				
Publish CRLs to this	s loc			Yes No

8.左側のペインで、[Revoked **Certificates**]を右クリ**ックします**。[All Tasks] > [Publish] を選択しま す。[New CRL] が選択されていることを確認し、[OK] をクリックします。

🙀 certsrv - [Certification Autho	rity (Local)\abtoma	r-WIN	I-231PNBS4IPH-	CA\Revoked Certificates]
File Action View Help				
🗢 🔿 🙍 🔚 🙍				
Certification Authority (Local) Request ID	Re	vocation Date	Effective Revocation Date
Bevoked Certificat			The	re are no items to show in this vi
Ssued Certificates	All Tasks	>	Publish	
Pending Requests	View	>		
Certificate Templa	Refresh Export List			
	Properties			
	Help			

.



Microsoft CAサーバは、セクション1で作成したフォルダに新しい.crlファイルを作成する必要が あります。新しいCRLファイルが正常に作成された場合、[OK]をクリックしてもダイアログは表 示されません。新しい分散ポイント フォルダに関するエラーが返された場合は、このセクション の各ステップを慎重に繰り返してください。

CRLファイルが存在し、IIS経由でアクセス可能であることを確認する

このセクションを開始する前に、新しい CRL ファイルが存在しており、そのファイルに IIS を介 して別のワークステーションからアクセスできることを確認してください。

1. IISサーバーで、セクション1で作成したフォルダを開きます。<CANAME>.crlという形式の 単一の.crlファイルが存在する必要があります。<CANAME>はCAサーバーの名前です。この 例では、ファイル名は次のとおりです。

abtomar-WIN-231PNBS4IPH-CA.crl

📙 🛃 📕 🖛 CRL	Distrib	ution			-	-		\times
File Home S	Share	View						~ 🕐
← → • ↑ 📙	> Thi	s PC > Local Disk (C:) > CRLDistribution	~ (5	Search CRLDistrib	oution		P
 Quick access Desktop Downloads Documents Pictures System32 	* * * *	Name abtomar-WIN-231PNBS4IPH-CA web.config	Date modified 11/28/2020 10:39 11/28/2020 10:22	Tyr Cei CO	pe rtificate Revoca INFIG File	Size	1 KB 1 KB	

2.ネットワーク上のワークステーション(ISEプライマリ管理ノードと同じネットワーク上)から Webブラウザを開き、http://<SERVER>/<CRLSITE>を参照します。<SERVER>はセクション2で 設定されたIISサーバのサーバ名、<CRLSITE>はです。

http://win-231pnbs4iph/CRLD

ステップ1で確認したファイルを含むディレクトリインデックスが表示されます。



新しいCRL分散ポイントを使用するようにISEを設定します

CRL を取得するように ISE を設定する前に、CRL を発行する間隔を定義します。この間隔を決 定するための方策については、このドキュメントの範囲外です。(Microsoft CA の場合)有効な 値は 1 時間~ 411 年です。デフォルト値は 1 週間です。環境に適した間隔を決定したら、以下の 手順で間隔を設定します。

- 1. CA サーバのタスクバーで、[Start] をクリックします。[Administrative Tools] > [Certificate Authority] を選択します。
- 左側のペインで、CAを展開します。[Revoked Certificates]フォルダを右クリックし、 [Properties]を選択します。
- [CRL publication interval] フィールドで、必要な数値を入力して期間単位を選択します。
 [OK] をクリックしてウィンドウを閉じ、変更を適用します。この例では、発行間隔が7日に設定されています。

File Action View	Help		
Certification Authors	ority (Local) 231PNBS4IPH-1	Request ID	Revocation [
Revoked Comparison Control Revoked Control	All Tasks	>	
Pending Re	View	>	
Certificate	Refresh		
	Export List		
	Properties		
	Help		
CRL Publishing Parameters A Certificate Revocation I consider invalid.	View CRLs list (CRL) describes cer	tificates that client	s should
CRL Publishing Parameters A Certificate Revocation I consider invalid. CRL publication interval: Next update:	View CRLs List (CRL) describes cer 7 Days 12/5/2020 10	tificates that client s v	s should
CRL Publishing Parameters A Certificate Revocation I consider invalid. CRL publication interval: Next update: Publish Delta CRLs Publication interval: Next update:	View CRLs List (CRL) describes cer 7 Days 12/5/2020 10 1 Days	tificates that client 39 AM	s should

4. **certutil -getreg CA\Clock*コマンドを入力し**て、ClockSkew値を確認します。デフォルト値は 10 分です。

出力例:

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

5. **certutil -getreg CA\CRLov***コマンドを入力して、CRLOverlapPeriodが手動で設定されているか どうかを確認します。デフォルトでは、CRLOverlapUnit 値は 0 です。これは、値が手動で設定 されていないことを示しています。この値が 0 以外の場合は、その値と単位を記録します。

出力例:

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

6. certutil -getreg CA\CRLpe* コマンドを入力して、ステップ 3 で設定した CRLPeriod を確認し ます。

出力例:

Values:

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

7. CRLの猶予期間を次のように計算します。

a.CRLOverlapPeriod をステップ 5 で設定した場合:OVERLAP = CRLOverlapPeriod (分)

それ以外の場合:OVERLAP = (CRLPeriod / 10)(分)

b.OVERLAP > 720 の場合、OVERLAP = 720

c. OVERLAP < (1.5 * ClockSkewMinutes)の場合、OVERLAP = (1.5 * ClockSkewMinutes)

d.OVERLAP > CRLPeriod (分)の場合、OVERLAP = CRLPeriod (分)

e.猶予期間= OVERLAP + ClockSkewMinutes

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 算出した猶予期間は、CA が次の CRL を発行する時点と現在の CRL が失効する時点との間の時 間数です。状況に応じて CRL を取得するように ISE を設定する必要があります。

8. ISEプライマリ管理ノードにログインし、[Administration] > [System] > [Certificates]の順に選択 します。左側のペインで、 信頼できる証明書

Cisco ISE					Admini	stration · System					
Deployment Licensing	Certificate	s Logging M	Maintenance	Upgrade	Health Checks	Backup & Resto	re Admin Acce	ss Settings			Click h
Certificate Management ~ System Certificates	Trus	ted Certific	ates								
Trusted Certificates	Ø Edit	+ Import 🖒 Expo	t 📋 Delete	Q View							
OCSP Client Profile	0	P. J H. Marra				Control Number	1	locus d Bu	Mall d Passar	E-station Date	
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 Roo	a.	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	
	0	Cisco ECC Root CA 2099	·	Enabled	Cisco Services	0.3	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. CRLを設定するCA証明書の横にあるチェックボックスをオンにします。[Edit] をクリックします。

10.ウィンドウの下部にある[Download CRL]チェックボックスをオンにします。

11. [CRL Distribution URL]フィールドに、セクション2で作成した.crlファイルを含むCRL分散ポイントへのパスを入力します。この例では、URLは次のとおりです。

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

12. ISEは、定期的な間隔で、または有効期限に基づいてCRLを取得するように設定できます(一 般的には、定期的な間隔でもあります)。 CRL の発行間隔が固定されている場合は、後者のオプ ションのほうがタイムリーに CRL のアップデートを取得できます。[Automatically] **オプション ボタンをクリックします。**

13.取得の値をステップ7で計算した猶予期間より小さい値に設定します。設定した値が猶予期間 より長い場合、ISEはCAが次のCRLを発行する前にCRL分散ポイントをチェックします。この例 では、算出された猶予期間は 730 分、つまり 12 時間 10 分です。取得には10時間の値が使用さ れます

14.環境に応じて再試行間隔を設定します。前のステップで設定した間隔で CRL を取得できない 場合、ISE はこの短い間隔で再試行します。

15. ISEが最後のダウンロード試行でこのCAのCRLを取得できなかった場合に、証明書ベースの 認証を正常に(およびCRLチェックなしで)続行できるようにするには、[**Bypass CRL Verification if CRL is not Received]チェックボックスをオンにします。**このチェック ボックスを オンにしないと、CRL が取得できなかった場合に、この CA から発行された証明書による証明書 ベースの認証がすべて失敗します。

16. Ignore that CRL is not yet valid or expiredチェックボックスにチェックマークを入れて、 ISEが期限切れ(まだ有効でない)CRLファイルを有効であるかのように使用できるようにしま す。このチェック ボックスをオンにしないと、ISE は [Effective Date] よりも前および [Next Update] の時間よりも後の CRL を無効と見なします。[Save] をクリックして設定を完了します。

001010000 00000 10100000	Certificate	Status	Validation
--------------------------	-------------	--------	------------

To verify certificates, enable the m	ethods below. If bo	oth are enabled, OCSP	will always be	tried first.		
OCSP Configuration						
Validate against OCSP Service	2e	~				
Reject the request if OC Reject the request if OC Certificate Revocation List Configur	SP returns UNKNC SP Responder is u	WN status				
CRL Distribution URL	http://win-231	pnbs4iph/crid/abto	mar-WIN-231	PNBS4IPH-CA.crl		
Retrieve CRL	 Automatically Every 	10		Hours	~	before expiration.
If download failed, wait	10		Minutes	~	before retry.	
Enable Server Iden	tity Check 🕕					
Bypass CRL Verific	ation if CRL is not	Received				
Ignore that CRL is	not yet valid or exp	bired				

シスコ内部情報

1. Microsoft「証明書のCRL分散ポイントを設定します。」 <u>http://technet.microsoft.com/en-</u> <u>us/library/ee649260%28v=ws.10%29.aspx</u>、2009年10月7日[2012年12月18日]

2. Microsoft「証明書失効リストを手動で発行します。」 <u>http://technet.microsoft.com/en-</u> <u>us/library/cc778151%28v=ws.10%29.aspx</u>, 2005年1月21日[2012年12月18日]

3. Microsoft「CRLとDelta CRLのオーバーラップ期間を設定します。」 <u>http://technet.microsoft.com/en-us/library/cc731104.aspx</u>、2011年4月11日[2012年12月18日]

4. MS2065 [MSFT].「How EffectiveDate (this update), NextUpdate, and NextCRLPubrish are calculated.」 <u>http://blogs.technet.com/b/pki/archive/2008/06/05/how-effectivedate-thisupdate-nextupdate-and-nextcrlpublish-are-calculated.aspx</u>、2008年6月4日[2012年12月18日]