# 在Microsoft CA伺服器配置上發佈ISE的證書撤銷 列表示例

## 目錄

簡介
必要條件
需求
採用元件
慣例
設定
組態
第1部分。在CA上建立並配置資料夾以儲存CRL檔案
第2部分。在IIS中建立站點以公開新的CRL分發點
第3部分。配置Microsoft CA伺服器以將CRL檔案發佈到分發點
第4節:驗證CRL檔案是否存在且可通過IIS訪問
第5部分。配置ISE以使用新的CRL分發點
驗證
疑難排解
相關資訊

## 簡介

本文檔介紹運行Internet Information Services(IIS)以發佈證書吊銷清單(CRL)更新的Microsoft證書頒 發機構(CA)伺服器的配置。還說明了如何配置思科身份服務引擎(ISE)(版本1.1及更高版本)以檢 索更新以用於證書驗證。可以將ISE配置為檢索它在證書驗證中使用的各種CA根證書的CRL。

## <u>必要條件</u>

### <u>需求</u>

本文件沒有特定需求。

### 採用元件

本文中的資訊係根據以下軟體和硬體版本:

• 思科身分識別服務引擎版本1.1.2.145

Microsoft Windows<sup>®</sup> Server<sup>®</sup> 2008 R2

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除(預設))的組態來啟動。如果您的網路正在作用,請確保您已瞭解任何指令可能造成的影響。



請參閱思科技術提示慣例以瞭解更多有關文件慣例的資訊。

## <u>設定</u>

本節提供用於設定本文件中所述功能的資訊。

註:使用Command Lookup Tool(僅供已註冊客戶使用)可獲取本節中使用的命令的詳細資訊。

#### <u>組態</u>

本檔案會使用以下設定:

- 第1部分。在CA上建立並配置資料夾以儲存CRL檔案
- 第2部分。在IIS中建立站點以公開新的CRL分發點
- 第3部分。配置Microsoft CA伺服器以將CRL檔案發佈到分發點
- 第4節:驗證CRL檔案是否存在且可通過IIS訪問
- 第5部分。配置ISE以使用新的CRL分發點

#### 第1部分。在CA上建立並配置資料夾以儲存CRL檔案

第一項任務是配置CA伺服器上的一個位置以儲存CRL檔案。預設情況下,Microsoft CA伺服器將檔 案發佈到C:\Windows\system32\CertSrv\CertEnroll\。不要使用此系統資料夾,而是為檔案建立一個 新資料夾。

 在IIS伺服器上,選擇檔案系統上的位置並建立新資料夾。在此示例中,建立資料夾 C:\CRLDistribution。



為了使CA將CRL檔案寫入新資料夾,必須啟用共用。按一下右鍵新資料夾,選擇屬性,按一下共用頁籤,然後按一下高級共用。

CRLDistribution Properties	×
General Sharing Security Previous Versions Customize	
Network File and Folder Sharing	1
CRLDistribution Not Shared	
Network Path: Not Shared	
Share	
Advanced Sharing Set custom permissions, create multiple shares, and set other advanced sharing options.	
Close Cancel Apply	

 若要共用資料夾,請選中共用此資料夾覈取方塊,然後在「共用名稱」欄位中為共用名稱末尾 新增一個美元符號(\$)以隱藏共用。

ttings	
CRLDistribut	tion\$
Add	Remove
Limit the num	ber of simultaneous users to: 👘 77216 🚔
Limit the num	ber of simultaneous users to: 77216 📑
Limit the num Comments:	iber of simultaneous users to: 77216 📑
Limit the num Comments:	iber of simultaneous users to: 77216 📑

4. 按一下Permissions(1),按一下Add(2),按一下Object Types(3),然後選中Computers覈取方 塊(4)。

Advanced Sharing	🔋 Permissions for CRLDistribution\$	Select Users, Computers, Service Accounts, or Groups	? ×
✓ Share this folder	Share Permissions	Select this object type:	
Setting	Group or user names	Users, Groups, or Built in security principals	3 Object Types
Share name:	& Everyone	From this location	_
CRUDistribution\$		tipasa.local	Locations
Add Remove		Enter the object names to select (examples):	
Limit the number of simultaneous us		Object Toring	Charle Marco
Commerks:	2 Add Re	mor Select the types of objects you want to find	
	Permissions for Everyone Allow D	areAObject type::	
	Full Control	🛛 🔛 🍇 Duit-in security principals	
1 Permissions 1 Caching	Change 🔲	Generators	
	11000		
OK C		🗹 👶 Users	
	Learn about access control and permissions		-
	OK Cencel	Apple0	K Cancel

5. 要返回「選擇使用者」、「電腦」、「服務帳戶」或「組」視窗,請按一下**確定**。在「輸入要 選擇的對象名稱」欄位中,輸入CA伺服器的電腦名稱,然後按一下**檢查名稱**。如果輸入的名 稱有效,該名稱將刷新並帶有下劃線。按一下「**OK**」(確定)。

Select Users, Computers, Service Accounts, or Groups	? ×
Select this object type:	
Users, Computers, Groups, or Built-in security principals	Object Types
From this location:	
rtpaaa.local	Locations
Enter the object names to select ( <u>examples</u> ):	
RTPAAA-DC1	Check Names
Advanced	OK Cancel

6. 在「組或使用者名稱」欄位中,選擇CA電腦。選中Allow for Full Control以授予對CA的完全訪問許可權。按一下「OK」(確定)。再次按一下OK以關閉「高級共用」視窗並返回到「屬性

Permissions for CRLDistribut	ion\$	×
Share Permissions		
Group or user names:		
& Everyone		
RTPAAA-DC1 (RTPAAA\RT	PAAA-DC1\$J	_
		0 1
	Add	Hemove
Permissions for RTPAAA-DC1	Allow	Deny
Full Control		
Change Read		
neau		
Learn about access control and p	<u>permissions</u>	
ОК	Cancel	Apply

- 」視窗。
- 7. 為了允許CA將CRL檔案寫入新資料夾,請配置相應的安全許可權。按一下Security頁籤(1),按 一下Edit(2),按一下Add(3),按一下Object Types(4),然後選中Computers覈取方塊(5)。

🕌 CRLDistribution Properties 🛛 🛛	Permissions for CRLDistribution	×
General Shan Security Previous Versions Customize	Security	
Object name: C:\CRLDistribution	Object name: C.VCRLD istribution	
Group or user names:	Group or user names:	
CREATOR OWNER	CREATOR OWNER	
& Administrators (RTPAAA\Administrators)	& Administrators (RTPAAAVAdministrators)	
Sers (RTPAAA\Users)	& Users (RTPAAAVUsers)	
To change permissions, click Edit. 2 Edit		
Permissions for CREATOR OwnER Allow Deput	3 Add   Remove	
Full control	Permissions for CREATOR Allow Derv	
Modify		
Read & execute	Modify D D	
List folder contents	Read & exec	0.52
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:		
rtpasalocal	Locations	
Enter the object names to select (examples):	Users	
	Check Names	
Advanced	Cancel	OK Cancel

8. 在「輸入要選擇的對象名稱」欄位中,輸入CA伺服器的電腦名稱,然後按一下**檢查名稱**。如 果輸入的名稱有效,該名稱將刷新並帶有下劃線。按一下「**OK**」(確定)。

roups	? ×
	Object Types
	Locations
	Check Names
	80
OK	Cancel
	roups

9. 在「組或使用者名稱」欄位中選擇CA電腦,然後選中Allow以授予對CA的完全訪問許可權。按 一下OK,然後按一下Close以完成任務。

Security		
Object name: CACRI Distributio		
object name. C. (Chiebistiibuit	on	
Group or user names:		
& CREATOR OWNER		
SYSTEM .		
Administrators (RTPAAA\Adr	ministrators)	_
	PAAA-DC1\$)	
Marcel Users (HTPAAA\Users)		
	Add	Remove
Permissions for RTPAAA-DC1	Allow	Deny
Full control		
Modify		
Read & execute		
List folder contents		
Read		
Learn about access control and p		
ОК	Cancel	Apply

## <u>第2部分。在IIS中建立站點以公開新的CRL分發點</u>

為了讓ISE訪問CRL檔案,請通過IIS訪問包含CRL檔案的目錄。

1. 在IIS伺服器工作列上,按一下**開始**。選擇**管理工具> Internet資訊服務(IIS)管理器**。

2. 在左側窗格(稱為控制檯樹)中,展開IIS伺服器名稱,然後展開**站點。** 



3. 按一下右鍵Default Web Site,然後選擇Add Virtual Directory。

Internet Informati	on S	ervices	; (II	S) Ma	nag	jer	
	RTPA	AA-DC1	ł	Sites	۲	Defau	lt Web Sil
File View Help							
Connections							2.5
🔍 - 🔙 🖄 🔝							
Start Page RTPAAA-DC1 (R Application P Sites Default )	TPAA 'ools Meh 9	A\Admin She Explore	iistra e	ator)		_	
	-	Edit Pe	ermis	sions	î		_
		Add Ap	oplic	ation	•		
	<u>e</u>	Add Vi	rtua	l Direct	ory	i.,	
		Edit Bir	nding	gs			
		Manag	le W	eb Site			
	-	Refres	h				
	×	Remov	/e				
		Renam	ne				
		Switch	to (	Ionten	t Vie	ew	

4. 在「別名」欄位中,輸入CRL分發點的站點名稱。在此示例中,輸入了CRLD。

			-	
Site				
				_
n -				
tings				
		ок		Cancel
	5ite	Site	Site	Site

5. 按一下省略號(。..)在「物理路徑」(Physical path)欄位的右側,瀏覽到在第1部分中建立的資 料夾。選擇該資料夾,然後按一下**確定**。按一下**OK**以關閉Add Virtual Directory視窗。

Add Virtual D	irectory	? ×
Site name: Path:	Default Web Site /	
Alias:		
CRLD		
Example: ima	ages	
Physical path	n:	
C:\CRLDistrib	bution	
Pass-through	h authentication	
Connect as	Test Settings	
	ОК Са	ancel

6. 在步驟4中輸入的站點名稱應在左窗格中突出顯示。如果沒有,現在就選擇。在中心窗格中 ,按兩下**Directory Browsing**。



7. 在右窗格中,按一下Enable以啟用目錄瀏覽。

	Alerts
Directory Browsing	i Directory br disabled,
Use this feature to specify the information that displays in a directory listing.	Actions
✓ Time	D Apply
Size	🖳 Cancel
Extension	Enable
Date	🕜 Help
<ul> <li>Size</li> <li>Extension</li> <li>Date</li> </ul>	Enable Opline H

8. 在左窗格中,再次選擇站點名稱。在中心窗格中,按兩下Configuration Editor。



9. 在「部分」下拉選單中,選擇**system.webServer/security/requestFiltering**。在 allowDoubleEscaping下拉選單中,選擇**True**。在右窗格中,按一下**Apply**。

CRLD >		0
Section: System webServer/security/reque	stFikering - From: Default Web Site/CRLD Web.config	<ul> <li>Actions</li> <li></li></ul>
E Deepest Path: MACHINE/WEBROOT	APPHOST	Generate Script
allowDoubleEscaping	True	Configuration
allowHighBitCharacters	True	Search Configuration
alwaysAllowedQueryStrings	False	Search Conngurat
alwaysAllowedLirls	(count=o)	Section
denyQueryStringSequences	(Count=0)	Lock Section
denyUrlSequences	(Count=0)	Lock Section
fileExtensions		'allowDoubleEscapi
filteringRules	(Count=0)	Attribute
hiddenSegments		Lock Attribute
requestLimits		9 Help
unescapeQueryString	True	e nep
1 verbs		Online Help

現在應可通過IIS訪問該資料夾。

### <u>第3部分。配置Microsoft CA伺服器以將CRL檔案發佈到分發點</u>

現在,已配置了一個新資料夾來容納CRL檔案,並且該資料夾已在IIS中公開,請配置Microsoft CA伺服器以將CRL檔案發佈到新位置。

- 1. 在CA伺服器工作列上,按一下**開始**。選擇Administrative Tools > Certificate Authority。
- 2. 在左窗格中,按一下右鍵CA名稱。選擇**Properties**,然後按一下**Extensions**頁籤。要新增新的 CRL分發點,請按一下**Add**。

oaaa-CA Properties			? ×
Enrollment Agents   Aud General   F Extensions   9	diting   Re Policy Module Storage	covery Agents Exi Certificate I	Security t Module Managers
Select extension:			
CRL Distribution Point (CDP)			-
Specify locations from which u (CRL). C:\Windows\system32\Cert9 Idap:///CN= <catruncatedn http://<serverdnsname>/C</serverdnsname></catruncatedn 	isers can obtair irv\CertEnroll\< ame> <crlnan ertEnroll/<can< td=""><td>n a certificate rev CaName&gt;<crlm neSuffix&gt;,CN=<si ame&gt;<crlname< td=""><td>ocation list NameSuffix&gt;<i erverShortNar Suffix&gt;<delta< td=""></delta<></i </td></crlname<></si </crlm </td></can<></crlnan 	n a certificate rev CaName> <crlm neSuffix&gt;,CN=<si ame&gt;<crlname< td=""><td>ocation list NameSuffix&gt;<i erverShortNar Suffix&gt;<delta< td=""></delta<></i </td></crlname<></si </crlm 	ocation list NameSuffix> <i erverShortNar Suffix&gt;<delta< td=""></delta<></i 
Publish CRLs to this locati	on	Add	Remove
Include in all CRLs. Speci when publishing manually.	iies where to pu	Iblish in the Activ	e Directory
🔲 Include in CRLs. Clients u	se this to find D	elta CRL location	18.
Include in the CDP extens	ion of issued ce	ertificates	
🔲 Publish Delta CRLs to this	location		
Include in the IDP extensi	on of issued CF	Ls	
ОК	Cancel	Apply	Help

3. 在「位置」欄位中,輸入在第1部分中建立和共用的資料夾的路徑。在第1部分的示例中,路徑為:

Add Location			×
A location car or enter a UN the variable b	n be any valid URL or pa C or local path. To insert elow and click Insert.	th. Enter an HTTP, LD, a variable into the URL	AP, file address, . or path, select
Location:	)C1\CRLDistribution\$\		
Variable:			-
<caname></caname>		•	Insert
Description of	selected variable:		
Used in URL Inserts the DI Example loca	s and paths NS name of the server ation: http:// <serverdns< td=""><td>Name&gt;/CertEnroll/<ca< td=""><td>Name&gt;<crlna< td=""></crlna<></td></ca<></td></serverdns<>	Name>/CertEnroll/ <ca< td=""><td>Name&gt;<crlna< td=""></crlna<></td></ca<>	Name> <crlna< td=""></crlna<>
•			Þ
		ОК	Cancel
4. 填充Location欄	I位後,從Variable下 <b>拉</b>	: <b>列</b> 表中選擇 <canam< th=""><th>ne&gt;,然後按一下<b>Inser</b></th></canam<>	ne>,然後按一下 <b>Inser</b>
Add to see the second			No. of the second se
Add Location A location car or enter a UNI the variable b	n be any valid URL or pat C or local path. To insert elow and click Insert.	h. Enter an HTTP, LD/ a variable into the URL	AP, file address, . or path, select
Add Location A location car or enter a UNI the variable b Location:	n be any valid URL or pat C or local path. To insert elow and click Insert.	h. Enter an HTTP, LD/ a variable into the URL	AP, file address, . or path, select
Add Location A location car or enter a UNI the variable but Location:	n be any valid URL or pat C or local path. To insert elow and click Insert. 1C1\CRLDistribution\$\ <c< td=""><td>h. Enter an HTTP, LD/ a variable into the URL aName&gt;</td><td>AP, file address, . or path, select</td></c<>	h. Enter an HTTP, LD/ a variable into the URL aName>	AP, file address, . or path, select
Add Location A location car or enter a UNI the variable b Location: \\RTPAAA-D Variable:	n be any valid URL or pat C or local path. To insert elow and click Insert. C1\CRLDistribution\$\ <c< td=""><td>h. Enter an HTTP, LD/ a variable into the URL aName&gt;</td><td>AP, file address, or path, select</td></c<>	h. Enter an HTTP, LD/ a variable into the URL aName>	AP, file address, or path, select
Add Location A location car or enter a UNI the variable by Location: \\RTPAAA-D Variable: <caname></caname>	n be any valid URL or pa C or local path. To insert elow and click Insert. (C1\CRLDistribution\$\ <c< td=""><td>h. Enter an HTTP, LD/ a variable into the URL aName&gt;</td><td>AP, file address, or path, select</td></c<>	h. Enter an HTTP, LD/ a variable into the URL aName>	AP, file address, or path, select
Add Location A location car or enter a UNi the variable b Location: \\RTPAAA-D Variable: <caname> Description of</caname>	n be any valid URL or pat C or local path. To insert elow and click Insert. (C1\CRLDistribution\$\ <c< td=""><td>h. Enter an HTTP, LD/ a variable into the URL aName&gt;</td><td>AP, file address, or path, select</td></c<>	h. Enter an HTTP, LD/ a variable into the URL aName>	AP, file address, or path, select
Add Location A location car or enter a UNI the variable bi Location: \\RTPAAA-D Variable: <caname> Description of Used in URL: Inserts the Di Example loca</caname>	n be any valid URL or pa C or local path. To insert elow and click Insert. (C1\CRLDistribution\$\ <c selected variable: s and paths NS name of the server tion: http://<serverdns1< td=""><td>h. Enter an HTTP, LD/ a variable into the URL aName&gt;</td><td>AP, file address, or path, select</td></serverdns1<></c 	h. Enter an HTTP, LD/ a variable into the URL aName>	AP, file address, or path, select
Add Location A location car or enter a UNI the variable bi Location: \\RTPAAA-D Variable: <caname> Description of Used in URL: Inserts the DI Example loca</caname>	n be any valid URL or pal C or local path. To insert elow and click Insert. C1\CRLDistribution\$\ C1\CRLDIS\ C1\CRLDistribution\$\ C1\CRLDIS\ C1\CR	h. Enter an HTTP, LD/ a variable into the URL aName>	AP, file address, or path, select

5. 從「變數」下拉選單中,選擇**<CRLNameSuffix>,**然後按一下**插入**。

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:
\\RTPAAA-DC1\CRLDistribution\$\ <caname><crlnamesuffix></crlnamesuffix></caname>
Variable:
<crlnamesuffix> 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><crlnamesi< td=""></crlnamesi<></caname></servername>
OK Cancel

6. 在Location欄位中,將.crl附加到路徑的末尾。在此示例中,位置為: \\RTPAAA-DC1\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:	
\\RTPAAA-DC1\CRLDistribution\$\ <caname><crlnamesuffix>.crl</crlnamesuffix></caname>	
Variable:	
<crlnamesuffix> 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><crlnamesi< td=""><td></td></crlnamesi<></caname></servername>	
<u>∢</u>	
OK Cancel	

7. 按一下OK返回到「擴展」頁籤。選中Publish CRLs to this location覈取方塊(1),然後按一下 OK(2)以關閉「Properties(屬性)」視窗。出現一個提示符,提示獲得重新啟動Active Directory證書服務的許可權。按一下「Yes」(3)。

· · · · · · · · · · · · · · · · · · ·		
paaa-CA Properties		? ×
Enrollment Agents General Extensions	Auditing Recovery Agents Policy Module Exit M Storage Certificate Ma	Security   fodule   magers
Select extension:		
CRL Distribution Point (CI	DP)	
Specify locations from whi (CRL).	ch users can obtain a certificate revoc	ation list
C:\Windows\system32\C Idap:///CN= <catruncate http://<serverdnsname> file://<serverdnsname> \\RTPAAA-DC1\CRLDis</serverdnsname></serverdnsname></catruncate 	CertSrv\CertEnroll\ <caname><crlnar edName&gt;<crlnamesuffix>,CN=<serv &gt;/CertEnroll/<caname><crlnamesuf /CertEnroll/<caname><crlnamesuffix tribution\$\<caname><crlnamesuffix< th=""><th>meSuffix&gt;<i /erShortNai /ffix&gt;<delta fix&gt;<deltac &gt;&gt;.crl</deltac </delta </i </th></crlnamesuffix<></caname></crlnamesuffix </caname></crlnamesuf </caname></serv </crlnamesuffix></crlnar </caname>	meSuffix> <i /erShortNai /ffix&gt;<delta fix&gt;<deltac &gt;&gt;.crl</deltac </delta </i 
•		▶
	Add F	Remove
Publish CRLs to this lo	cation	
Include in all C	ication Authority	
Include in CRL		
Include in the I	You must restart Active Director changes to take effect. Do you	y Certificate Services for the want to restart the service now?
Publish Delta (		
Include in the I		2 Vec No
2_ ок	Cancel Apply	Help

8. 在左窗格中,按一下右鍵**Revoked Certificates**。選擇**所有任務>發佈**。確保選中「New CRL(新建CRL)」,然後按一下**「OK(確定)」。** 

📴 certsrv - [Certification Aut	hority	(Local)\rtpaa	aa-CA\Revoked Cert	ificates]		_ 🗆 🗵
File Action View Help						
🗢 🔿 🖄 🖾 🔒 📘	?					
in Certification Authority (Local)		Request ID	Revocation Date	Effective Revocation Date	Revocation Reason	Requester Nam 🔺
Certification Authority (Local)  rtpaaa-CA  Sevoked Certificates  Sending Requests  Failed Requests  Certificate Template	Al Ta: View Refre Expor Prope Help	Request ID sks → sh t List rties 41 448 449 550 551 552 553 554 555 559 60	Revocation Date 5/6/2012 12:57 PM 5/6/2012 12:57 PM 9:58 AM 5/6/2012 1:09 PM 5/8/2012 1:09 PM 5/8/2012 7:43 PM 5/8/2012 7:42 PM Publish CRL The latest publish receive a new CR Type of CRL to pu © New CRL Issues a comp for the CA. © Delta CRL orl Issues an abb the CRL that H	Effective Revocation Date 5/8/2012 12:57 PM 5/8/2012 12:57 PM 5/8/2012 9:58 AM 5/8/2012 1:09 PM 5/8/2012 1:09 PM 5/8/2012 7:43 PM 5/8/2012 7:43 PM 5/8/2012 7:42 PM ed Certificate Revocation List ( L until after their current one ex- ablish: lete CRL, which contains up to y reviated version of the DBL, which rave been made since the last	Revocation Reason Superseded Unspecified Superseded Unspecified Superseded Superseded CRL) is still valid. Clients r ordete revocation informat rich contains only the upo time it was published. OK	Requester Nam A RTPAAA\Admini RTPAAA\Admini RTPAAA\Admini RTPAAA\Admini RTPAAA\Admini RTPAAA\Admini RTPAAA\Admini inay not
Manually publish current CR1		<b>1</b> 66		71/0/00/07 / 00 00		

Microsoft CA伺服器應在第1節中建立的資料夾中建立新的.crl檔案。如果成功建立新的CRL檔案 ,則按一下「確定」後將不會出現對話方塊。如果返回有關新分發點資料夾的錯誤,請仔細重複本 節中的步驟。

### <u>第4節:驗證CRL檔案是否存在且可通過IIS訪問</u>

開始本節之前,請確認新的CRL檔案是否存在,以及是否可以通過另一工作站的IIS訪問這些檔案。

1. 在IIS伺服器上,開啟第1部分中建立的資料夾。應存在一個.crl檔案,其格式為 <CANAME>.crl,其中<CANAME>是CA伺服器的名稱。在此範例中,檔案名稱為:

CRLDistribution\$				_ 🗆 ×
🕥 🛛 🗜 - Network	✓ rtpaaa-dc1	- 🖽	Search CRLDistribution\$	<u>,</u>
Organize 👻 📆 Open 🔹	<ul> <li>New folder</li> </ul>		8	- 🔳 🔞
🚖 Favorites	Name ^	Date modified	Туре	Size
🧱 Desktop	💐 rtpaaa-CA	12/19/2012 5:45 PM	Certificate Revocation List	5 KB
🎉 Downloads 🔝 Recent Places	web.config	12/17/2012 5:04 PM	CONFIG File	1 KB
🥽 Libraries				
Documents				
J Music				
Videos				
🜉 Computer				
🏭 Local Disk (C:)				

2. 從網路上的工作站(最好與ISE主管理節點位於同一網路),開啟Web瀏覽器並瀏覽到 http://<SERVER>/<CRLSITE>,其中<SERVER>是在第2部分中配置的IIS伺服器的伺服器名 稱, <CRLSITE>是在第2部分中為分發點選擇的站點名稱。在此示例中, URL為: http://RTPAAA-DC1/CRLD



### <u>第5部分。配置ISE以使用新的CRL分發點</u>

在將ISE配置為檢索CRL之前,定義發佈CRL的時間間隔。確定此間隔的策略不在本檔案的範圍之 內。潛在值(在Microsoft CA中)為1小時到411年(含)。預設值為1週。確定適合您環境的間隔後 ,請使用以下說明設定間隔:

1. 在CA伺服器工作列上,按一下**開始**。選擇Administrative Tools > Certificate Authority。

2. 在左窗格中,展開CA。按一下右鍵Revoked Certificates資料夾,然後選擇Properties。

 在「CRL發佈間隔」欄位中,輸入所需的數字並選擇時間段。按一下OK關閉視窗並應用更改 。在本示例中,配置了7天的發佈間隔。

File       Action       View       Help         Image: Certification Authority (Local)       Request ID       Revoked Certificates Properties       ?       ?         Image: Certification Authority (Local)       Image:	🗽 certsrv - [Certification	n Authority	(Local)\rtpaa	a-CA\R	Revoked Certificates]				
Image: Certification Authority (Local)       Request ID       Rev       Revoked Certificates Properties       Image: Certification Authority (Local)         Image: Certification Authority (Local)       Image: Certification Interval:       Image: Telephone       Image: Certification Interval:       Image: Telephone       Image: Certification Interval:       Image: C	File Action View Hel	p							
Certification Authority (Local) Request ID Revoked Certificates Properties   rtpaaa-CA side   Pending Reque Side   Pending Reque Side   View Side   Pending Reque Side   View Side   Paied Request ID Side   Certificates Ter Side   Properties Side   Side Side   Properties Side   Side Side   Side Side   Properties Side   Side Side   Side Side   Side Side   Properties Side   Side	🗢 🤿 🖄 🔚 🖪 🗉	• ?							
Pending Reques   Failed Reques   Failed Reques   Refresh   Export List   S/8   Properties   S/8   Help   S/8   Publish Deta CRLs   Publication interval:   Publish Deta CRLs   Publish Deta CRLs   S/8   S/8   S/8   Help   S/8   Publish Deta CRLs   S/8   Publish Deta CRLs   S/8	Certification Authority (I rtpasa-CA Revoked Certific Issued Certific	.ocal) atos All Tasks	Request ID	Re <sup>1</sup> 5/8 5/8 5/8	CRL Publishing Parameters	ties /iew CRLs	]		? 🗙 🛓
Signature       5/8       CRL publication interval:       7       Days         Export List       5/8       Next update:       12/20/2012 8:45 AM         Properties       5/8       Publich Delta CRLs         Bar 20       5/8       Publication interval:       1         Bar 20       5/8       Publicati	Pending Reque	View	•	5/8	A Certificate Revocation List consider invalid.	(URL) desc	ribes certificates t	hat clients sh	hould
Export list       5/8       Next update:       12/20/2012 8:45 AM         Properties       5/8       S/8         Help       5/8       Publish Delta CRLs         20       5/8       Publication interval:       1         20       5/8       Next update:       1         29       5/8       Next update:       1         33       5/8       Next update:       1         34       5/8       35       5/8         36       5/8       39       5/8         39       5/8       39       5/8         40       5/9       41       5/3         46       5/3       46       5/3         48       6/2       48       6/2	Certificate Ter	Refresh	ĥ	5/8 5/8	CRL publication interval:	7	Days	•	
Help       5/8       Publish Delta CRLs         20       5/8       Publication interval:       1         29       5/8       Next update:         33       5/8       Next update:         34       5/8         35       5/8         36       5/8         37       5/8         40       5/9         46       5/3         48       6/2		Properties	··· 2	5/8 5/8	Next update:	12/20	/2012 8:45 AM		
Image: 20       5/8       Publication interval:       Image: 20       Image: 20         Image: 29       5/8       Image: 20       Next update:         Image: 33       5/8       Next update:       Image: 20         Image: 33       5/8       Image: 20       Next update:         Image: 340       5/9       Image: 20       Next update:         Image: 411       5/3       Image: 416       S/4         Image: 416       5/8       Image: 416       S/8         Image: 416		Help	ţ	5/8 5/8	🔲 Publish Delta CRLs				
33       5/6       Next update:         34       5/8         35       5/8         36       5/8         37       5/8         39       5/8         39       5/8         40       5/9         41       5/3         46       5/3         48       6/2			20	5/8 5/8	Publication interval:	1	Hours	¥	
35 5/8 36 5/8 37 5/8 39 5/8 40 5/9 41 5/3 46 5/3 48 6/2			33	5/8 5/8	Next update:				
37 5/8 39 5/8 30 5/			35	5/8					
5/8 40 5/9 41 5/3 46 5/3 48 6/2			37	5/8					
41 5/3 46 5/3 48 6/2			an 139 an 140	5/8 5/9					
48 6/2			00 41 00 46	5/3 5/3					
6/2			48	6/2 6/2					
50 6/2 OK Cancel Apply Help		6 11	50	6/2	ОК	Cancel	Apply	н	

您現在應該確認幾個登錄檔值,這將有助於確定ISE中的CRL檢索設定。

4. 輸入certutil -getreg CA\Clock\*命令以確認ClockSkew值。預設值為10分鐘。輸出示例:

Values: ClockSkewMinutes REG\_DWORS = a (10) CertUtil: -getreg command completed successfully.

5. 輸入**certutil -getreg CA\CRLov\*命令**以驗證是否已手動設定CRLOverlapPeriod。預設情況下 ,CRLOverlapUnit值為0,表示未設定手動值。如果該值不是0,請記錄該值和單位。輸出示

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

6. 輸入**certutil -getreg CA\CRLpe\***命令以驗證CRLeriod(已在步驟3中設定)。輸出示例: values:

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

7. 按如下方式計算CRL寬限期:如果在步驟5中設定CRLOverlapPeriod:重疊=

CRLOverlapPeriod(分鐘);其他:重疊=(CRLeriod / 10),分鐘如果重疊大於720,則重疊= 720如果重疊<(1.5 \* ClockSkewMinutes),則重疊=(1.5 \* ClockSkewMinutes)如果OVERLAP > CRLPeriod,則重疊= CRLPeriod,以分鐘為單位寬限期= 720分鐘+ 10分鐘= 730分鐘範例 .

As stated above, CRLPeriod was set to 7 days, or 10248 minutes and CRLOverlapPeriod was not set.

```
b. 1024.8 minutes is > 720 minutes : OVERLAP = 720 minutes
c. 720 minutes is NOT < 15 minutes : OVERLAP = 720 minutes</li>
d. 720 minutes is NOT > 10248 minutes : OVERLAP = 720 minutes
e. Grace Period = 720 minutes + 10 minutes = 730 minutes
```

計算出的寬限期是CA發佈下一個CRL到當前CRL到期之間的時間量。需要配置ISE以相應地檢 索CRL。

8. 登入到主Admin節點,然後選擇Administration > System > Certificates。在左窗格中,選擇 Certificate Store。

🔆 System 🛛 💐 Identity Management 🛛 🏢	Network Resources 🛛 🥵 Web Portal Management		
Deployment Licensing Certificates Loggi	g Maintenance Admin Access Settings		
Certificate Operations	Certificate Store		courses a literation
🔹 Local Certificates	Ander Anternet Chilingart Malata	Show AL	Selected of Total 2
Certificate Signing Requests	Conside theme	forward Ta	Include Day
O Certificate Store	Prendy Name     RT0444_DC1_MSCE0_R41#rtrpsp_C4#00002	RTDAAA,DC1,MSCED,R	rtpaga_CA
SCEP CA Profiles	d draaa-CA#draaa-CA#00001	itnaaa-CA	rtpaaa-CA

9. 選中要為其配置CRL的CA證書旁邊的證書儲存覈取方塊。按一下「Edit」。

- 10. 在視窗底部附近, 選中Download CRL覈取方塊。
- 11. 在「CRL分發URL」欄位中,輸入CRL分發點的路徑,該分發點包括第2部分建立的.crl檔案 。在此示例中,URL為:

http://RTPAAA-DC1/CRLD/rtpaaa-ca.crl

- 12. 可以將ISE配置為定期或根據過期時間(通常也是定期間隔)檢索CRL。 當CRL發佈間隔為 靜態時,使用後一個選項可獲得更及時的CRL更新。按一下Automatically單選按鈕。
- 13. 將檢索的值設定為小於在步驟7中計算的寬限期的值。如果值集大於寬限期,ISE將在CA發佈 下一個CRL之前檢查CRL分發點。在此示例中,寬限期計算為730分鐘或12小時10分鐘。檢 索將使用10小時的值。
- 14. 根據您的環境設定重試間隔。如果ISE無法按上一步中配置的間隔檢索CRL,它將按此較短間 隔重試。
- 15. 選中Bypass CRL Verification if CRL is not Received覈取方塊,如果ISE在其上次下載嘗試中 無法檢索此CA的CRL,則允許基於證書的身份驗證正常進行(並且不進行CRL檢查)。如果 未選中此覈取方塊,則如果無法檢索CRL,則此CA頒發的證書的所有基於證書的身份驗證都 將失敗。
- 16. 選中Ignore that CRL is not not valid or expired覈取方塊,以允許ISE使用已過期(或尚未有效)的CRL檔案,就好像這些檔案有效。如果未選中此覈取方塊,則ISE會將CRL視為在其生效日期之前和下次更新時間之後無效。按一下「Save」以完成設定。

1220160 10	Tupaaa-CA
Issued By	rtpaaa-CA
Valid From	Sat, 11 Feb 2012 19:32:02 EST
Valid To (Expiration)	Wed, 11 Feb 2037 19:42:01 EST
Serial Number	1D 85 1D 58 36 8C EC 93 4E F6 5B 28 9B 26 E7 89
Usage	
All Trust Certificates are a and administrative auther	valable for selection as the Root CA for secure LDAP connections. In addition, they may be enabled for EAP-TLS itication below:
Trust for client authe	ntication
Enable Validation o	f Certificate Extensions (accept only valid certificate)
To verify certificates, ena DCSP Configuration Validate against OCSP	Service
Reject the requ	est if certificate status could not be determined by OCSP
Certificate Revocation	List Configuration
CPL Distribution	UPI http://docen.det/CDID/docen.CA.ed
CRL Distribution	UKL http://rtpaaa-dci/CKLD/rtpaaa-CA.cn
	Automatically 10     Hours + before expiration
Retrieve CRL	
	Every
If download faile	ed, wait 1 Minutes
Bynass CRI	Varification if CRL is not Received
Ignore that	CRL is not yet valid or expired
Porot	
ineser	

## <u>驗證</u>

目前沒有適用於此組態的驗證程序。

## <u>疑難排解</u>

目前尚無適用於此組態的具體疑難排解資訊。

## 相關資訊

• 技術支援與文件 - Cisco Systems