Configure Microsoft CA Server to Publish the Certificate Revocation Lists for ISE

Contents

Introduction Prerequisite Requirements Components Used Configure Create and Configure a Folder on the CA to House the CRL Files Create a Site in IIS to Expose the New CRL Distribution Point Configure Microsoft CA Server to Publish CRL Files to the Distribution Point Verify the CRL File Exists and is Accessible via IIS Configure ISE to use the New CRL Distribution Point

Introduction

This document describes the configuration of a Microsoft Certificate Authority (CA) server that runs Internet Information Services (IIS) to publish the Certificate Revocation List (CRL) updates. It also explains how to configure the Cisco Identity Services Engine (ISE) (versions 3.0 and later) to retrieve the updates for use in certificate validation. ISE can be configured to retrieve CRLs for the various CA root certificates it uses in certificate validation.

Prerequisite

Requirements

There are no specific requirements for this document.

Components Used

The information in this document is based on these software and hardware versions:

- Cisco Identity Services Engine Release 3.0
- Microsoft Windows[®] Server[®] 2008 R2

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Configure

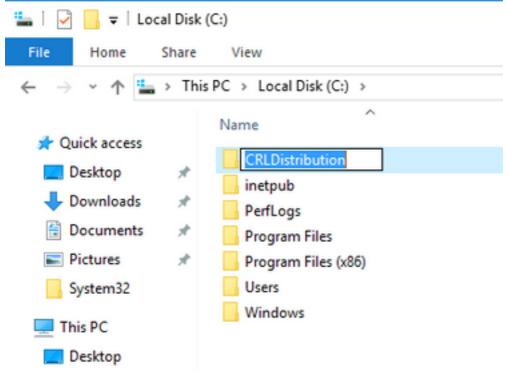
In this section, you are presented with the information to configure the features described in this document.

Create and Configure a Folder on the CA to House the CRL Files

The first task is to configure a location on the CA server to store the CRL files. By default, the Microsoft CA server publishes the files to C:\Windows\system32\CertSrv\CertEnroll\

Rather than use this system folder, create a new folder for the files.

1. On the IIS server, choose a location on the file system and create a new folder. In this example, the folder **C:\CRLDistribution** is created.



2. In order for the CA to write the CRL files to the new folder, sharing must be enabled. Right-click the new folder, choose **Properties**, click the **Sharing** tab, and then click **Advanced Sharing**.

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.	
Advanced Sharing	
Close Cancel App	ly

3. In order to share the folder, check the **Share this folder** check box and then add a dollar sign (\$) to the end of the share name in the Share name field to hide the share.

anced Shar	
5ettings	
Share name	ei and an
CRLDistrib	ution\$
Add	Remove
Comments:	
Permissio	ons Caching

4. Click **Permissions** (1), click **Add** (2), click **Object Types** (3), and check the **Computers** check box (4).

Advanced Sharing	📔 Permissions for CRLDistributio	n\$	Selec	t Users, Computers, Service Accounts, or Grou	ips ?X
Share this folder	Share Permissions		Sele	ect this object type:	
	Group or user names:		Us	ers, Groups, or Built-in security principals	3 Object Types
Share name:	& Everyone		From	n this location:	
CRLDistribution\$			rtpa	aaa.local	Locations
Add Remove			Ent	er the object names to select (<u>examples</u>):	
Limit the number of simultaneous us					Check Mamor
Comments:	Permissions for Everyone Full Control Change Read			Object Types Select the types of objects you want to find. Object types: Image: Select types: Select types: Image: Select types: Select types: Image: Select type: S	? X
	Learn about access control and per	missions			
	ОК	Cancel	Apply		OK Cancel

5. In order to return to the Select Users, Computers, Service Accounts, or Groups window, click **OK**. In the Enter the object names to select field, enter the computer name of the CA server in this example: WIN0231PNBS4IPH and click **Check Names**. If the name entered is valid, the name refreshes and appears underlined. 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. In the Group or user names field, choose the CA computer. Check **Allow** for Full Control to grant full access to the CA.

Click **OK**. Click **OK** again to close the Advanced Sharing window and return to the Properties window.

Permissions for CRLDistributi	ion\$	×
Share Permissions		
Group or user names:		
Everyone	MAR\WIN-231PN	BS4IPH\$)
Permissions for	Add	Remove
WIN-231PNBS4IPH	Allow	Deny
Full Control Change Read	[
ОК	Cancel	Apply

7. In order to allow the CA to write the CRL files to the new folder, configure the appropriate security permissions. Click the **Security** tab (1), click **Edit** (2), click **Add** (3), click **Object Types** (4), and check the **Computers** check box (5).

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 SRAdministrators	SYSTEM Administrators (RTPAAA\Administrators)
& Users (RTPAAA/Users)	Section in statutes (111 Accessed and interesting)
To change permissions, click Edit. 2 Edit	
Permissions for CREATOR	3 Add Remove
OWNER Allow Deny	Permissions for CREATOR
Full control	OWNER Allow Deny
Read & execute	Full control
List folder contents	Read & exec bits (class of the sector) and the sector of t
Read Write	
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 OK	Cancel OK Cancel
UN.	

8. In the Enter the object names to select field, enter the computer name of the CA server, and click **Check Names**. If the name entered is valid, the name refreshes and appears underlined. 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 (<u>examples</u>):	
WIN-231PNBS4IPH	Check Names
Advanced OK	Cancel

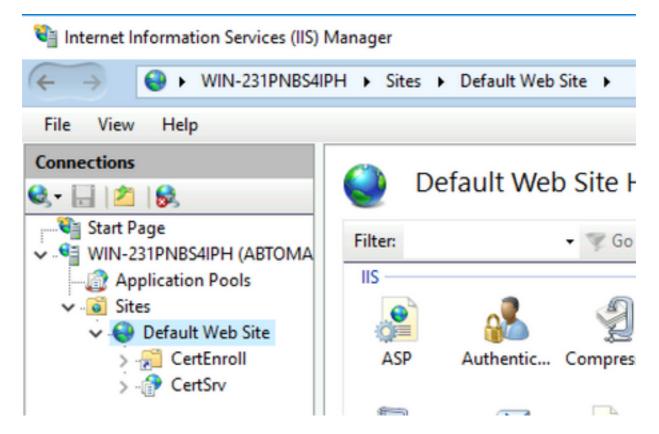
9. Choose the CA computer in the Group or user names field and then check to **Allow** for Full control to grant full access to the CA. Click **OK** and then click **Close** to complete the task.

Permissions for CRLDistribution	on	×
Security		
Object name: C:\CRLDistribution	n	
Group or user names:		
Secretaria CREATOR OWNER		
SYSTEM		
Administrators (ABTOMAR\Ad	dministrators)	
Series (ABTOMAR\Users)		
	IAN WIN-23 IF ND	54IFH3)
	Add	Remove
Permissions for WIN-231PNBS4IPH	Allow	Deny
Full control		□ ^
Modify		
Read & execute	\checkmark	
List folder contents	\checkmark	
Read	\checkmark	
ОК	Cancel	Apply

Create a Site in IIS to Expose the New CRL Distribution Point

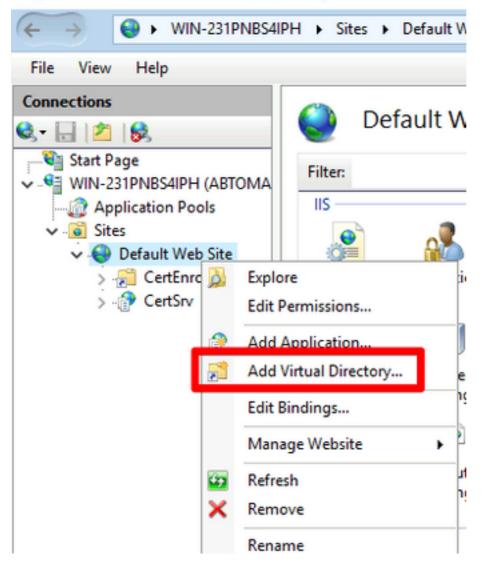
In order for ISE to access the CRL files, make the directory that houses the CRL files accessible via IIS.

- 1. On the IIS server taskbar, click **Start**. Choose **Administrative Tools > Internet Information Services (IIS) Manager**.
- 2. In the left pane (known as the Console Tree), expand the IIS server name and then expand **Sites.**



3. Right-click **Default Web Site** and choose **Add Virtual Directory**, as shown in this image.

💐 Internet Information Services (IIS) Manager



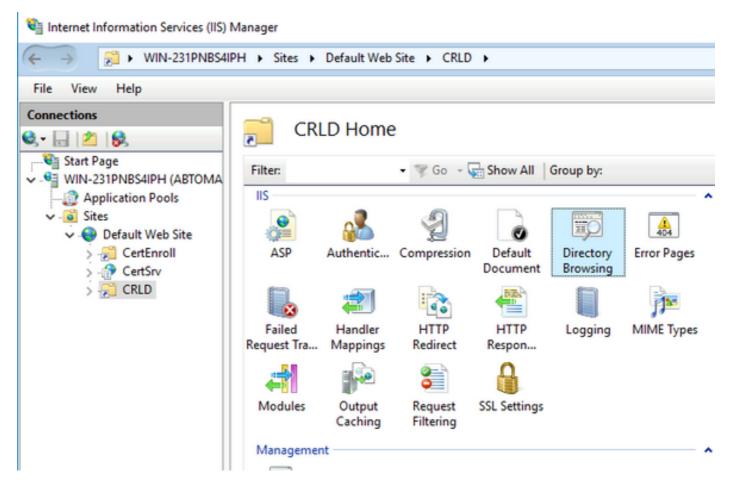
4. In the Alias field, enter a site name for the CRL Distribution Point. In this example, CRLD is entered.

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	Cano	el :

5. Click the ellipsis (. . .) to the right of the Physical path field and browse to the folder created in section 1. Select the folder and click **OK**. Click **OK** to close the Add Virtual Directory window.

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	

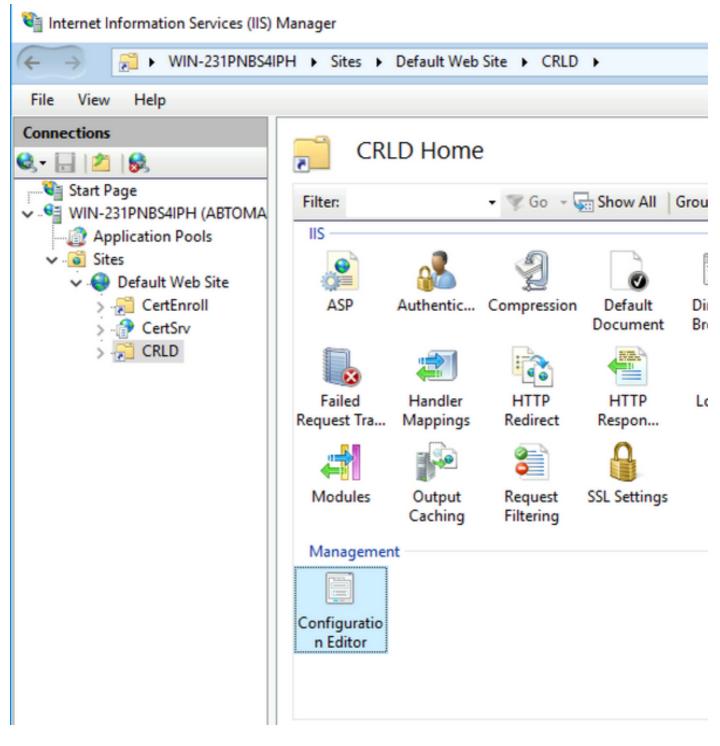
6. The site name entered in step 4 must be highlighted in the left pane. If not, choose it now. In the center pane, double-click **Directory Browsing**.



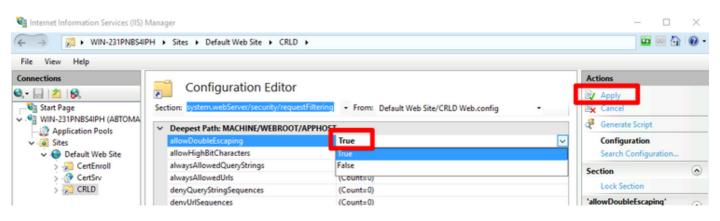
7. In the right pane, click Enable to enable directory browsing.

Internet Information Services (IIS)	Manager	-		\times
← → 21 + WIN-231PNB54	PH > Sites > Default Web Site > CRLD >		i 🖂 🖨	0.
File View Help				
Connections	Directory Browsing	Alerts	vsing has t	been
Start Page	Use this feature to specify the information that displays in a directory listing.	disabled.		
Application Pools Sites Offault Web Site	V 307	R Apply R Cancel		
> 2 CertEnroll > 2 CertEnroll	Etension	Enable		
S 💭 CRLD	Long date	Help		

8. In the left pane, choose the site name again. In the center pane, double-click **Configuration Editor**.



9. In the Section drop-down list, choose **system.webServer/security/requestFiltering**. In the **allowDoubleEscaping** drop-down list, choose **True**. In the right pane, click **Apply**, as shown in this image.



The folder must now be accessible via IIS.

Configure Microsoft CA Server to Publish CRL Files to the Distribution Point

Now that a new folder has been configured to house the CRL files and the folder has been exposed in IIS, configure the Microsoft CA server to publish the CRL files to the new location.

- 1. On the CA server taskbar, click **Start**. Choose **Administrative Tools > Certificate Authority**.
- 2. In the left pane, right-click the CA name. Choose **Properties** and then click the **Extensions** tab. In order to add a new CRL distribution point, click **Add**.

abtomar-WIN-231PNB	S4IPH-CA Pro	perties		?	×	
Enrollment Agents	Auditing	Auditing Recovery Agents		Sec	urity	
General	Policy Mo	odule	Exi	Exit Module		
Extensions	Storage		Certificate I	Managen	s	
Select extension:						
CRL Distribution Point	(CDP)				\sim	
Specify locations from (CRL). C:\Windows\system3 Idap:///CN= <catrunc http://<serverdnsna file://<serverdnsnar< td=""><td>2\CertSrv\Cert catedName><c ame>/CertEnrol</c </td><td>Enroll\<cana RLNameSuf /<caname></caname></cana </td><td>ame><crlm fix>,CN=<si <crlname< td=""><td>NameSuff erverSho Suffix><1</td><td>ix>< rtNar Delta</td></crlname<></si </crlm </td></serverdnsnar<></serverdnsna </catrunc 	2\CertSrv\Cert catedName> <c ame>/CertEnrol</c 	Enroll\ <cana RLNameSuf /<caname></caname></cana 	ame> <crlm fix>,CN=<si <crlname< td=""><td>NameSuff erverSho Suffix><1</td><td>ix>< rtNar Delta</td></crlname<></si </crlm 	NameSuff erverSho Suffix><1	ix>< rtNar Delta	
<					>	
		Ad	d	Remov	e	
Publish CRLs to this	s location					
Include in all CRLs. when publishing ma		re to publish i	in the Active	e Directo	ŋy	
Include in CRLs. Cli	ients use this to	find Delta C	RL location	s.		
Include in the CDP	extension of iss	ued certifica	tes			
Publish Delta CRLs	Publish Delta CRLs to this location					
Include in the IDP extension of issued CRLs						
ОК	Cano	æl	Apply	He	elp	

3. In the Location field, enter the path to the folder created and shared in section 1. In the example in section 1, the path is:

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\$\	
Variable:	
<pre><array control="" of="" sec<="" second="" td="" the=""><td></td></array></pre>	
	_
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>la</td></crln<></caname></serverdnsname>	la
<	>
OK Cancel	

4. With the Location field populated, choose **<CaName>** from the Variable drop-down list and then click **Insert.**

Add Location		2
A location can be any valid URL or path. Enter an HTTP or enter a UNC or local path. To insert a variable into the the variable below and click Insert.		
Location:		
\\WIN-231PNBS4IPH\CRLDistribution\$\ <caname></caname>		
Variable:		
<caname></caname>	~	Insert
Description of selected variable:		
Used in URLs and paths Inserts the DNS name of the server Example location: http:// <serverdnsname>/CertEnroll/</serverdnsname>	/ <can< td=""><td>lame><crlna< td=""></crlna<></td></can<>	lame> <crlna< td=""></crlna<>
<		>
Example location: http:// <serverdnsname>/CertEnroll/</serverdnsname>	/ <can< td=""><td>lame><crlna< td=""></crlna<></td></can<>	lame> <crlna< td=""></crlna<>

5. From the Variable drop-down list, choose <CRLNameSuffix> and then click Insert.

ОК

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></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>à ,</td></crlnames<></caname></servername>	à ,
< >	·
OK Cancel	

Cancel

6. In the Location field, append .crl to the end of the path. In this example, the Location is:

\\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><crlnamesu< td=""><td></td></crlnamesu<></caname></servername>	
< >	
OK Cancel]

7. Click **OK** to return to the Extensions tab. Check the **Publish CRLs to this location** check box and then click **OK** to close the Properties window.

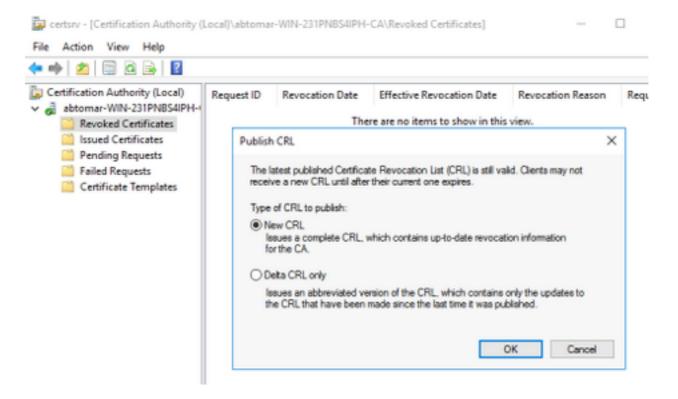
A prompt appears for permission to restart Active Directory Certificate Services. Click Yes.

Enrollment Agents	Auditing	Recovery Agents	Security		
General	Policy Mo	dule Ex	t Module		
Extensions	Storage	Storage Certificate Manag			
Select extension:					
CRL Distribution Point	(CDP)		~		
(CRL).		n obtain a certificate rev	rocation list		
C:\Windows\system3		ion Authority			
C:\Windows\system3 Idap:///CN= <catrun http://<serverdnsna file://<serverdnsnar \\\\\\231PNBS4IP <</serverdnsnar </serverdnsna </catrun 	cate ame me>	ion Authority You must restart Ac take effect. Do you		ertificate Services for the changes to ne service now?	
Idap:///CN=<ĆATrun http:// <serverdnsna file://<serverdnsnar< td=""><td></td><td>You must restart A</td><td></td><td></td><td></td></serverdnsnar<></serverdnsna 		You must restart A			

8. In the left pane, right-click **Revoked Certificates**. Choose **All Tasks > Publish**. Ensure that New CRL is selected and then click **OK**.

.

🙀 certsrv - [Certification Autho	ority (Local)\abtoma	r-WI	V-231PNBS4IPH-	CA\Re	voked Certificates]
File Action View Help					
🗢 🔿 🖄 🖾 🙆					
 Certification Authority (Local abtomar-WIN-231PNBS4 		Re	vocation Date	Effec	tive Revocation Date
Revoked Certifica*			The	re are r	o items to show in this vi
Ssued Certificates	All Tasks	>	Publish		
Pending Requests Failed Requests	View	>			
🧰 Certificate Templa	Refresh Export List				
	Properties				
	Help				



The Microsoft CA server must create a new .crl file in the folder created in section 1. If the new CRL file is created successfully there will be no dialog after OK is clicked. If an error is returned in regards to the new distribution point folder, carefully repeat each step in this section.

Verify the CRL File Exists and is Accessible via IIS

Verify the new CRL files exist and that they are accessible via IIS from another workstation before you start this section.

 On the IIS server, open the folder created in section 1. There must be a single .crl file present with the form **<CANAME>.crl** where **<**CANAME> is the name of the CA server. In this example, the filename is:

abtomar-WIN-231PNBS4IPH-CA.crl

I I I I CRLDistrib File Home Share	View		-	-	□ × ~ ()
\leftrightarrow \rightarrow \checkmark \uparrow \square \Rightarrow Thi	is PC > Local Disk (C:) > CRLDistribution	× 5	Search CRLDistrib	ution	<i>م</i>
 ✓ 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	Type Certificate Revoca CONFIG File	Size	1 KB 1 KB

2. From a workstation on the network (ideally on the same network as the ISE primary Admin node), open a web browser and browse to http://<SERVER>/<CRLSITE> where <SERVER> is the server name of the IIS server configured in section 2 and <CRLSITE> is the site name chosen for the distribution point in section 2. In this example, the URL is:

http://win-231pnbs4iph/CRLD

The directory index displays, which includes the file observed in step 1.



Configure ISE to use the New CRL Distribution Point

Before ISE is configured to retrieve the CRL, define the interval to publish the CRL. The strategy to determine this interval is beyond the scope of this document. The potential values (in Microsoft CA) are 1 hour to 411 years, inclusive. The default value is 1 week. Once an appropriate interval for your environment has been determined, set the interval with these instructions:

- 1. On the CA server taskbar, click **Start**. Choose **Administrative Tools > Certificate Authority**.
- 2. In the left pane, expand the CA. Right-click the **Revoked Certificates** folder and choose **Properties.**
- 3. In the CRL publication interval fields, enter the required number and choose the time period. Click **OK** to close the window and apply the change. In this example, a publication interval of 7 days is configured.

Certification Author		Request ID	Revocation D
Revoked Ce Issued Cert	All Tasks	>	
🦳 Pending Re 🎬 Failed Requ	View	>	
Certificate	Refresh		
	Export List.		
	Properties		
	Help		
Revoked Certificates Proper	ties	?	×
CRL Publishing Parameters A Certificate Revocation Lis consider invalid.	View CRLs t (CRL) describes cert	ficates that client	
CRL Publishing Parameters A Certificate Revocation Lis	View CRLs	ficates that client	
CRL Publishing Parameters A Certificate Revocation Lis consider invalid. CRL publication interval:	Vew CRLs t (CRL) describes cert 7 Days	ficates that client	

4. Enter the **certutil -getreg CA\Clock*** command to confirm the ClockSkew value. The default value is 10 minutes.

Example output:

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

5. Enter the **certutil -getreg CA\CRLov*** command to verify whether the CRLOverlapPeriod has been manually set. By default the CRLOverlapUnit value is 0, which indicates that no manual value has been set. If the value is a value other than 0, record the value and units.

Example output:

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

6. Enter the **certutil -getreg CA\CRLpe*** command to verify the CRLPeriod, which was set in step 3.

Example output:

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

7. Calculate the CRL Grace Period as follows:

a. If CRLOverlapPeriod was set in step 5: OVERLAP = CRLOverlapPeriod, in minutes;

Else: OVERLAP = (CRLPeriod / 10), in minutes

b. If OVERLAP > 720 then OVERLAP = 720

c. If OVERLAP < (1.5 * ClockSkewMinutes) then OVERLAP = (1.5 * ClockSkewMinutes)

d. If OVERLAP > CRLPeriod, in minutes then OVERLAP = CRLPeriod in minutes

e. Grace Period = 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 The grace period calculated is the amount of time between when the CA publishes the next CRL and when the current CRL expires. ISE needs to be configured to retrieve the CRLs accordingly.

8. Log in to the ISE Primary Admin node and choose **Administration > System > Certificates**. In the left pane, select **Trusted Certificate**

Cisco ISE					Adminis	stration · System					
Deployment Licensing	Certificate	s Logging	Maintenance	Upgrade	Health Checks	Backup & Resto	ore Admin Acce	ss Settings			Click h
Certificate Management ~ System Certificates Trusted Certificates	Trus	ted Certifi		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 9B EE 97 53	abtomar-WIN-231PN	abtomar-WIN-231PN	Wed, 20 Feb 2019	Sun, 20 Feb 2039	8
	0	Cisco ECC Root CA 2	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	
					1-8						

9. Check the check box next to the CA certificate for which you intend to configure CRLs. Click **Edit**.

10. Near the bottom of the window, check the **Download CRL** check box.

11. In the CRL Distribution URL field, enter the path to the CRL Distribution Point, which includes the .crl file, created in section 2. In this example, the URL is:

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

12. ISE can be configured to retrieve the CRL at regular intervals or based on the expiration (which, in general, is also a regular interval). When the CRL publish interval is static, more timely CRL updates are obtained when the latter option is used. Click the **Automatically** radio button.

13. Set the value for retrieval to a value less than the grace period calculated in step 7. If the value set is longer than the grace period, ISE checks the CRL distribution point before the CA has published the next CRL. In this example, the grace period is calculated to be 730 minutes, or 12 hours and 10 minutes. A value of 10 hours will be used for the retrieval

14. Set the retry interval as appropriate for your environment. If ISE cannot retrieve the CRL at the configured interval in the previous step, it will retry at this shorter interval.

15. Check the **Bypass CRL Verification if CRL is not Received** check box to allow certificatebased authentication to proceed normally (and without a CRL check) if ISE was unable to retrieve the CRL for this CA in its last download attempt. If this check box is not checked, all certificatebased authentication with certificates issued by this CA will fail if the CRL cannot be retrieved.

16. Check the **Ignore that CRL is not yet valid or expired** check box to allow ISE to use expired (or not yet valid) CRL files as though they were valid. If this check box is not checked, ISE considers a CRL to be invalid prior to their Effective Date and after their Next Update times. Click **Save** to complete the configuration.

Certificate	Status	Val	idation
-------------	--------	-----	---------

Validate against OCSP Servi	ce	\sim				
Reject the request if OC	SP returns UNKNO	OWN status				
Reject the request if OC	CSP Responder is u	inreachable				
Certificate Revocation List Configur	ation					
Download CRL						
CRL Distribution URL	http://win-231	pnbs4iph/crld/abto	mar-WIN-231	PNBS4IPH-CA.crl		
	• Automatically	10		Hours	~	before expiration.
Retrieve CRL	O Every	1		Hours	~	
If download failed, wait	10		Minutes	~	before retry.	
	the Oberth O					
Enable Server Ider	tity check					

Save

Cisco Internal Information

1. Microsoft. "Configure a CRL Distribution Point for Certificates." <u>http://technet.microsoft.com/en-us/library/ee649260%28v=ws.10%29.aspx</u>, Oct. 7, 2009 [Dec 18, 2012]

2. Microsoft. "Manually publish the certificate revocation list." <u>http://technet.microsoft.com/en-us/library/cc778151%28v=ws.10%29.aspx</u>, Jan. 21, 2005 [Dec. 18, 2012]

3. Microsoft. "Configure CRL and Delta CRL Overlap Periods." <u>http://technet.microsoft.com/en-us/library/cc731104.aspx</u>, Apr. 11, 2011 [Dec 18, 2012]

4. MS2065 [MSFT]. "How EffectiveDate (thisupdate), NextUpdate and NextCRLPublish are calculated." <u>http://blogs.technet.com/b/pki/archive/2008/06/05/how-effectivedate-thisupdate-nextupdate-and-nextcrlpublish-are-calculated.aspx</u>, Jun. 4, 2008 [Dec 18, 2012]