# ISE용 인증서 해지 목록을 게시하도록 Microsoft CA 서버 구성

목차
<u>소개</u>
<u>사전 요구 사항</u>
<u>요구 사항</u>
<u>사용되는 구성 요소</u>
<u>구성</u>
<u>CA에서 CRL 파일을 저장할 폴더 생성 및 구성</u>
<u>새 CRL 배포 지점을 표시하는 IIS에서 사이트 만들기</u>
<u>배포 지점에 CRL 파일을 게시하도록 Microsoft CA 서버 구성</u>
<u>CRL 파일이 있으며 IIS를 통해 액세스할 수 있는지 확인</u>
<u>새 CRL 배포 지점을 사용하도록 ISE 구성</u>
<u>다음을 확인합니다.</u>
문제 해결

# 소개

이 문서에서는 CRL(Certificate Revocation List) 업데이트를 게시하기 위해 IIS(인터넷 정보 서비스)를 실행하는 Microsoft CA(인증 기관) 서버의 구성에 대해 설명합니다. 또한 Cisco ISE(Identity Services Engine)(버전 3.0 이상)가 인증서 검증에 사용할 업데이트를 검색하도록 구성하는 방법에 대해서도 설명합니다. ISE는 인증서 검증에서 사용하는 다양한 CA 루트 인증서에 대한 CRL을 검 색하도록 구성할 수 있습니다.

# 사전 요구 사항

### 요구 사항

이 문서에 대한 특정 요건이 없습니다.

### 사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- Cisco Identity Services Engine 릴리스 3.0
- Microsoft Windows Server 2008 R2

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바 이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

## 구성

이 섹션에는 이 문서에서 설명하는 기능을 구성하기 위한 정보가 표시됩니다.

CA에서 CRL 파일을 저장할 폴더 생성 및 구성

첫 번째 작업은 CA 서버에서 CRL 파일을 저장할 위치를 구성하는 것입니다. 기본적으로 Microsoft CA 서버는 C:\Windows\system32\CertSrv\CertEnroll\

이 시스템 폴더를 사용하는 대신 파일의 새 폴더를 만듭니다.

1. IIS 서버에서 파일 시스템의 위치를 선택하고 새 폴더를 만듭니다. 이 예에서는 폴더가 C:\CRLDistribution 생성됩니다.

🏪   🛃 📙 🗣   Local Disk	: (C:)
File Home Share	View
← → × ↑ 🏪 > Th	is PC > Local Disk (C:) >
	Name
📌 Quick access	CRI Distribution
📃 Desktop 🛛 🖈	inetrub
👆 Downloads 🛛 🖈	Deflare
😭 Documents 🖈	Program Files
📰 Pictures 🛛 🖈	Program Files (x86)
System32	Users
💻 This PC	Windows
Desktop	

2. CA가 CRL 파일을 새 폴더에 기록하려면 공유를 활성화해야 합니다. 새 폴더를 마우스 오른쪽 단추로 클릭하고 Properties을 선택하고 탭을 Sharing 클릭한 다음 을 Advanced Sharing클릭합니다.

CRLDistribution Properties	×
General Sharing Security Previous Versions Customize	-8
Network File and Folder Sharing	Ť
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 Apply	

3. 폴더를 공유하려면 확인란을 Share this folder 선택한 다음 공유 이름 필드의 공유 이름 끝에 달러 기호(\$)를 추가하여 공유를 숨깁니다.

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

4. (Permissions1), (Add2), Object Types (3)을 차례로 클릭하고 확인란Computers(4)를 선택합니다.

Advanced Sharing	Permissions for CRLDistribution	1\$	Se	elect U	sers, Computers, Service Accounts, or Gr	oups	? ×
✓ Share this folder	Share Permissions			Select t	nis object type:		
	Group or user names:			Users,	Groups, or Built-in security principals	3	Object Types
Share name:	& Everyone			From thi	s location:		
CRLDistribution\$				rtpaaa.	ocal		Locations
Add Remove				Enter th	e object names to select ( <u>examples</u> ):		
Limit the number of simultaneous us					hiert Tynes		Check Namer
Comments:	2	Add	Remo		Select the types of objects you want to find.		
	Permissions for Everyone	Allow	Deny	A	Object types:		
	Full Control	□			🗹 🍇 Built-in security principals		
1 Permissions Caching	Change Bead				Service Accounts		
				138	Comparents 4		
ок с					🗹 👗 Users		
	Learn about access control and perr	nissions					
	OK	Cancel	Apply.			ОК	Cancel

5. 사용자, 컴퓨터, 서비스 계정 또는 그룹 선택 창으로 돌아가려면 을 ox클릭합니다. Enter the object names to select(선택할 개체 이름 입력) 필드에 이 예에서 CA 서버의 컴퓨터 이름 WIN0231PNBS4IPH를 입력하고 Check Names를 클릭합니다. 입력한 이름이 유효한 경우 이름이 새로 고쳐지고 밑줄이 그어진 상태로 나타납니다. 를 ox클릭합니다.

Select Users, Computers, Service Accounts, or Group	5	×
Select this object type:		
Users, Computers, Groups, or Built-in security principals		Object Types
From this location:		
abtomar.local		Locations
Enter the object names to select ( <u>examples</u> ):		
WIN-231PNBS4IPH		Check Names
Advanced	OK	Cancel

6. Group or user names(그룹 또는 사용자 이름) 필드에서 CA 컴퓨터를 선택합니다. CAAllow에 대한 전체 액세스 권한을 부여하려면 Full Control(전체 제어)을 선택합니다.

를 ок클릭합니다. Advanced Sharing(고급 공유) 창을 닫고 Properties(속성) 창으로 돌아 가려면 ок 다시 클릭합니다.

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

7. CA가 CRL 파일을 새 폴더에 쓸 수 있도록 하려면 적절한 보안 권한을 구성합니다. (1) 탭을 Security 클릭하고 (Edit2), Add (3), Object Types (4)를 차례로 클릭한 다음 Computers 확인란(5)을 선택 합니다.

CRLDistribution Properties	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	CREATOR OWNER	
SYSTEM	SYSTEM	
Administrators (TTT AAA (Administrators)     Set Users (RTPAAA/Users)	& Users (RTPAAAUsers)	
I To change permissions, click Edit		
Permissions for CREATOR		
OWNER Allow Deny	Bermissions for CBEATOB	
Full control	OWNER Allow Deny	
Read & execute	Full control	
List folder contents		2 2
Write I	List folder co	
Select Users, Computers, Service Accounts, or Groups	? X 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:		
jitpaaa.local	Locations	
Enter the object names to select ( <u>examples</u> )		
	Check Names	
Advanced	Cancel OK. (	Cancel

8. Enter the object names to select(선택할 개체 이름 입력) 필드에 CA 서버의 컴퓨터 이름을 입 력하고 를 Check Names클릭합니다. 입력한 이름이 유효한 경우 이름이 새로 고쳐지고 밑줄이 그 어진 상태로 나타납니다. 를 oK클릭합니다.

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. Group or user names(그룹 또는 사용자 이름) 필드에서 CA 컴퓨터를 선택한 다음 Full control(전체 제어)을 선택하여 CA에 대한 전체 액세스 권한을 Allow 부여합니다. 을 OK 클릭한 다음 을 클릭하여 작업Close을 완료합니다.

Permissions for CRLDistribut	ion	>
Security		
Object name: C:\CRLDistributio	n	
Group or user names:		
SCREATOR OWNER		
SYSTEM		
Administrators (ABTOMAR\A	dministrators)	
Sers (ABTOMAR\Users)		
WIN-231PNBS4IPH (ABTON	MAR\WIN-231PNB	S4IPH\$)
-	Add	Remove
Permissions for WIN-231PNBS4IPH	Allow	Deny
Full control		□ ^
Modify		
Read & execute	$\checkmark$	
List folder contents	$\checkmark$	
List folder contents Read		
List folder contents Read		
List folder contents Read		

새 CRL 배포 지점을 표시하는 IIS에서 사이트 만들기

ISE가 CRL 파일에 액세스하려면 IIS를 통해 CRL 파일이 들어 있는 디렉터리에 액세스할 수 있도록 합니다.

1. IIS 서버 작업 표시줄에서 를 Start클릭합니다. 를 Administrative Tools > Internet Information Services (IIS) Manager 선택합니다. 2. 왼쪽 창(콘솔 트리라고도 함)에서 IIS 서버 이름을 확장한 다음 확장합니다Sites.



3. 이 이미지에 표시된 Default Web Site 것처럼 마우스 오른쪽 버튼Add Virtual Directory을 클릭하고 을 선택합니다.

# 🝓 Internet Information Services (IIS) Manager



4. Alias(별칭) 필드에 CRL 배포 지점의 사이트 이름을 입력합니다. 이 예제에서는 CRLD를 입력 합니다.

Add Virtual Dire	ectory	?	×
Site name: Path:	Default Web Site /		
Alias: CRLD Example: ima	ges		
Physical path: C:\CRLDistrib	ution		
Pass-through Connect as.	authentication Test Settings		
	ОК	Cance	4

5. 줄임표(.)를 클릭합니다..) Physical path(물리적 경로) 필드의 오른쪽에서 섹션 1에 생성된 폴 더를 찾습니다. 폴더를 선택하고 을 oĸ누릅니다. Add Virtual Directory(가상 디렉토리 추가) 창 을 oĸ 닫으려면 클릭합니다.

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

6. 4단계에서 입력한 사이트 이름은 왼쪽 창에서 강조 표시되어야 합니다. 그렇지 않은 경우 지 금 선택합니다. 중앙 창에서 두 번 클릭합니다Directory Browsing.

Internet Information Services (IIS) N	Manager					
← → WIN-231PNBS4IF	PH → Sites →	Default Web	Site + CRLD	•		
File View Help						
Connections	CRI	LD Home	•			
→ Start Page → Start Page WIN-231PNBS4IPH (ABTOMA	Filter:		• 🦻 Go - 🖣	Show All	Group by:	
Application Pools    Application Pools	IIS ASP	Authentic	2 Compression	Default Document	Directory Browsing	Error Pages
> 🔁 CRLD	Failed Request Tra	<b>Handler</b> Mappings	HTTP Redirect	HTTP Respon	Logging	MIME Types
	Modules	Output Caching	Contract Request Filtering	SSL Settings		
	Managemen	nt				^

7. 오른쪽 창에서 를 클릭하여 디렉토리 Enable 찾아보기를 활성화합니다.

Internet Information Services (IIS) Manager							
← → 🛃 ► WIN-231PNB54	PH + Sites + Default Web Site + CRLD +		-	2	0.		
File View Help							
Connections	Directory Browsing Use this feature to specify the information that displays in a directory listing. Time Size Extension Date Long date	Alerts Directory disabled. Actions Actions Apply Cancel Enable Help Help	brows	ing has t	>een		

8. 왼쪽 창에서 사이트 이름을 다시 선택합니다. 중앙 창에서 두 번 클릭합니다Configuration Editor.



9. 섹션 드롭다운 목록에서 을 선택합니다system.webServer/security/requestFiltering. 드롭다운 allowDoubleEscaping 목록에서 을 선택합니다True. 오른쪽 창에서 을 클릭합니다(이 이미지Apply에 표시됨).



이제 IIS를 통해 폴더에 액세스할 수 있어야 합니다.

### 배포 지점에 CRL 파일을 게시하도록 Microsoft CA 서버 구성

CRL 파일을 보관하도록 새 폴더가 구성되었고 IIS에서 폴더가 노출되었으므로 CRL 파일을 새 위치 에 게시하도록 Microsoft CA 서버를 구성합니다.

- 1. CA 서버 작업 표시줄에서 를 Start클릭합니다. 를 Administrative Tools > Certificate Authority선택합니다.
- 2. 왼쪽 창에서 CA 이름을 마우스 오른쪽 버튼으로 클릭합니다. 선택 Properties 한 다음 탭을 클릭 Extensions 합니다. 새 CRL 배포 지점을 추가하려면 를 Add클릭합니다.

Enrollment Agents	Auditing	Recover	y Agents	Secu	urit
General	Policy Mod	Policy Module		Sat Module	
Extensions	Storage	Storage Certificate			
Calact automaian:					
CDL Distribution Deiter	(000)				
CRL Distribution Point	(CDP)				<u> </u>
Specify locations from	which users can o	btain a ce	rtificate rev	ocation lis	st
(CRL).					
C:\Windows\system3	2\CertSrv\CertEn	oll\ <cana< td=""><td>me&gt;<crli< td=""><td>VameSuff</td><td>ix&gt;</td></crli<></td></cana<>	me> <crli< td=""><td>VameSuff</td><td>ix&gt;</td></crli<>	VameSuff	ix>
Idan:///CN=/CATain	catedName> <cr< td=""><td>NameSuff</td><td>ix&gt;,CN=<s< td=""><td>erverShor</td><td>tN.</td></s<></td></cr<>	NameSuff	ix>,CN= <s< td=""><td>erverShor</td><td>tN.</td></s<>	erverShor	tN.
luap.///CN=CCATION				100 DEC. 100 DEC. 100 DEC.	
http:// <serverdnsna< td=""><td>ame&gt;/CertEnroll/&lt;</td><td>CaName&gt;</td><td>CRLName</td><td>Suffix&gt;<e< td=""><td>)elt</td></e<></td></serverdnsna<>	ame>/CertEnroll/<	CaName>	CRLName	Suffix> <e< td=""><td>)elt</td></e<>	)elt
http:// <serverdnsna file://<serverdnsnar< th=""><th>ame&gt;/CertEnroll/&lt; me&gt;/CertEnroll/&lt;</th><th>CaName&gt; aName&gt;&lt;</th><th>CRLName CRLName</th><th>Suffix&gt;<d Suffix&gt;<d< th=""><th>)elt elta</th></d<></d </th></serverdnsnar<></serverdnsna 	ame>/CertEnroll/< me>/CertEnroll/<	CaName> aName><	CRLName CRLName	Suffix> <d Suffix&gt;<d< th=""><th>)elt elta</th></d<></d 	)elt elta
http:// <serverdnsna file://<serverdnsnar< th=""><th>ame&gt;/CertEnroll/&lt; me&gt;/CertEnroll/&lt;</th><th>CaName&gt;&lt; aName&gt;&lt;</th><th><crlname CRLName</crlname </th><th>Suffix&gt;<d Suffix&gt;<de< th=""><th>Delt elta</th></de<></d </th></serverdnsnar<></serverdnsna 	ame>/CertEnroll/< me>/CertEnroll/<	CaName>< aName><	<crlname CRLName</crlname 	Suffix> <d Suffix&gt;<de< th=""><th>Delt elta</th></de<></d 	Delt elta
http:// <serverdnsna file://<serverdnsnar< td=""><td>ame&gt;/CertEnroll/&lt; me&gt;/CertEnroll/&lt;</td><td>CaName&gt; aName&gt;&lt;</td><td><crlname CRLNameS</crlname </td><td>Suffix&gt;<d Suffix&gt;<d< td=""><td>elta</td></d<></d </td></serverdnsnar<></serverdnsna 	ame>/CertEnroll/< me>/CertEnroll/<	CaName> aName><	<crlname CRLNameS</crlname 	Suffix> <d Suffix&gt;<d< td=""><td>elta</td></d<></d 	elta
http:// <serverdnsna file://<serverdnsnar< td=""><td>ame&gt;/CertEnroll/&lt; me&gt;/CertEnroll/&lt;</td><td>CaName&gt; aName&gt;&lt; Ade</td><td>CRLName CRLName</td><td>Suffix&gt;<d Suffix&gt;<de Remove</de </d </td><td>Delt elta 2</td></serverdnsnar<></serverdnsna 	ame>/CertEnroll/< me>/CertEnroll/<	CaName> aName>< Ade	CRLName CRLName	Suffix> <d Suffix&gt;<de Remove</de </d 	Delt elta 2
A publish CRLs to this	ame>/CertEnroll/< me>/CertEnroll/<	CaName> aName>< Ade	CRLName CRLName	Suffix> <de Suffix&gt;<de Remove</de </de 	elta e
Include in all CRLs	ame>/CertEnroll/< me>/CertEnroll/< s location	CaName> aName> Add	CRLName CRLName d	Suffix> <de Suffix&gt;<de Remove</de </de 	)elt elta ) e
Include in all CRLs when publishing ma	ame>/CertEnroll/< me>/CertEnroll/< s location . Specifies where t anually.	CaName> aName> Add	CRLName CRLName d	Suffix> <d Suffix&gt;<d Remove</d </d 	)elta 2 e
Publish CRLs to this when publishing ma	ame>/CertEnroll/< me>/CertEnroll/< s location . Specifies where t anually. ients use this to fir	CaName> aName> Add o publish i	CRLName CRLName d	e Director	elta y
Publish CRLs to this when publishing ma	ame>/CertEnroll/< me>/CertEnroll/< s location . Specifies where t anually. lients use this to fir	CaName> aName> Add o publish i id Delta Cl	CRLName CRLName d	e Director	elta y
Publish CRLs to this when publishing ma Include in CRLs. Cl Include in the CDP	ame>/CertEnroll/< me>/CertEnroll/< s location . Specifies where t anually. lients use this to fir extension of issue	CaName> aName> Add o publish i id Delta Cl id certifical	CRLName CRLName d n the Active RL location tes	e Director	elta y
Include in all CRLs. Cl Include in the CDP Publish Delta CRLs	ame>/CertEnroll/< me>/CertEnroll/< s location . Specifies where t anually. lients use this to fir extension of issue s to this location	CaName> aName> Add o publish i id Delta Cl id certifical	CRLName CRLName d	e Director	elta y
Include in the CDP Include in the CDP Include in the CDP Include in the CDP Include in the IDP	ame>/CertEnroll/< me>/CertEnroll/< s location . Specifies where t anually. lients use this to fir extension of issue s to this location extension of issue	CaName> aName> Add o publish i d Delta Cl d certificat	CRLName CRLName d	e Director	e y
Include in the CDP Publish Delta CRLs	ame>/CertEnroll/< me>/CertEnroll/< s location . Specifies where t anually. lients use this to fir extension of issue s to this location extension of issue	CaName> aName> Add o publish i d Delta Cl d certificat	CRLName CRLName d n the Active RL location tes	e Director	elta y

 위치 필드에 섹션 1에서 생성하고 공유하는 폴더의 경로를 입력합니다. 섹션 1의 예에서 경로 는 다음과 같습니다.

\\WIN-231PNBS4IPH\CRLDidistribution\$

Add Location	×
A location can be any valid URL or path. Enter an HTTP, LDAP, file addres or enter a UNC or local path. To insert a variable into the URL or path, selec the variable below and click Insert.	s. t
Location:	
\\WIN-231PNBS4IPH\CRLDistribution\$\	
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>la</td></crln<></caname></serverdnsname>	la
< I I I I I I I I I I I I I I I I I I I	>
OK Cancel	

4.

Location(위치) 필드가 채워진 상태에서 Variable(변수) 드롭다운 목록에서 선택한 다음 Insert.

### Add Location

A location can be any valid URL or path. Enter an HTTP, LDAP, file address, or enter a UNC or local path. To insert a variable into the URL or path, select the variable below and click Insert.

Location:

\\WIN-231PNBS4IPH\CRLDistribution\$\ <caname></caname>	
--	--

Variable:

<CaName>

Insert

Description of selected variable:

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

5. Variable 드롭다운 목록에서 을 선택하고 를 클릭합니다Insert.

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><crlnamesuffix></crlnamesuffix></caname>	
Variable: <crlnamesuffix> V Insert Description of selected variable:</crlnamesuffix>	]
Used in URLs and paths for the CRL Distribution Points extension	
Appends a suffix to distinguish the CRL file name Example location: http://cServerName>/CertEnroll/ <caname><crlname< td=""><td>Si</td></crlname<></caname>	Si
< 2	>
OK Cancel	

6. Location 필드에서 경로의 끝.crl에 추가합니다. 이 예에서 위치는 다음과 같습니다.

\\WIN-231PNBS4IPH\CRLDistribution\$\

.crl

### Add Location

A location can be any valid URL or path. Enter an HTTP, LDAP, file address, or enter a UNC or local path. To insert a variable into the URL or path, select the variable below and click Insert.

#### Location:

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

#### Variable:

<CRLNameSuffix> V Insert

### 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><CRLNameSt <</td>

OK

7. Extensions(확장) 탭으로 돌아가려면 OK 클릭합니다. 확인란을 Publish CRLs to this location 선택한 다음 를 클릭하여 속성 창OK을 닫습니다.

Active Directory 인증서 서비스를 다시 시작할 수 있는 권한을 묻는 메시지가 나타납니다. 를 Yes클릭합니다.

×

chroiment Agents	Auditing	Recovery Agents	Security	
General	Policy Mo	dule Ex	t Module	
Extensions	Storage	Certificate	Managers	
Select extension:				
CRL Distribution Point	(CDP)		~	
Specify locations from (CRL). C:\Windows\system3 Idap:///CN= <catrun http://<serverdnsna< th=""><th>2\C Certificat ame ne&gt;</th><th>ion Authority</th><th>rocation list</th><th>rtificate Censicer for the changer to</th></serverdnsna<></catrun 	2\C Certificat ame ne>	ion Authority	rocation list	rtificate Censicer for the changer to
file:// <serverdnsnar \\WIN-231PNBS4IP1 &lt;</serverdnsnar 	<u> </u>	You must restart A take effect. Do you	ctive Directory Ce want to restart th	te service now?

8. 왼쪽 창에서 마우스 오른쪽 버튼을 Revoked Certificates클릭합니다. 를 All Tasks > Publish 선택합니다. New CRL(새 CRL)이 선택되었는지 확인한 다음 을 OK클릭합니다.

Certification Author	ity (Local)\abtoma	r-Wit	N-231PNBS4IPH-	CA\Revoked Certificates]
(***) 21 [1] Q (**) 100				
Certification Authority (Local)	Request ID	Re	vocation Date	Effective Revocation Date
Revoked Certificator			The	re are no items to show in this vi
Sured Certificates	All Tasks	>	Publish	
Pending Requests	View	>		
Certificate Templa	Refresh Export List			
	Properties			
	Help			

Microsoft CA 서버는 섹션 1에서 만든 폴더에 새 .crl 파일을 만들어야 합니다. 새 CRL 파일이

성공적으로 생성되면 OK(확인)를 클릭한 후 대화 상자가 표시되지 않습니다. 새 배포 지점 폴 더에 대한 오류가 반환되면 이 섹션의 각 단계를 신중하게 반복합니다.

CRL 파일이 있으며 IIS를 통해 액세스할 수 있는지 확인

이 섹션을 시작하기 전에 새 CRL 파일이 존재하며 다른 워크스테이션에서 IIS를 통해 액세스할 수 있는지 확인하십시오.

1. IIS 서버에서 섹션 1에서 만든 폴더를 엽니다. 단일 .crl 파일이 있어야 하며

```
.crl
여기서
는 CA 서버의 이름입니다. 이 예에서 파일 이름은 다음과 같습니다.
```

abtomar-WIN-231PNBS4IPH-CA.crl



2. 네트워크의 워크스테이션(이상적으로 ISE 기본 관리 노드와 동일한 네트워크에 있음)에서 웹 브라우저를 열고 섹션 2에서 구성한 IIS 서버의 서버 이름과 섹션 2에서 배포 지점에 대해 선 택한 사이트 이름을 http://

/

찾습니다

. 여기서

는 IIS 서버의 서버 이름입니다. 이 예에서 URL은 다음과 같습니다.

http://win-231pnbs4iph/CRLD

1단계에서 관찰된 파일을 포함하는 디렉토리 인덱스가 표시됩니다.

-00	http://w	in-231pnbs4i	ph/crld/ 🕽	Q ▼ C 🦉 win-231pnbs4iph - /crld/ ×
win-23	5 <b>1</b> pi	nbs4i	ph -	/crld/
			<u> </u>	
To Parent	Direct	tory]		
	10:39	AM	979	abtomar-WIN-231PNRS4TPH-CA.crl
1/28/2020				de comar man sorrendo rarn orrora

새 CRL 배포 지점을 사용하도록 ISE 구성

ISE가 CRL을 검색하도록 구성되기 전에 CRL을 게시할 간격을 정의합니다. 이 간격을 결정하는 전 략은 이 문서의 범위를 벗어납니다. 잠재적 값(Microsoft CA)은 1시간 ~ 411년(포함)입니다. 기본값 은 1주입니다. 환경에 적합한 간격이 결정되면 다음 지침을 참조하여 간격을 설정합니다.

- 1. CA 서버 작업 표시줄에서 를 Start클릭합니다. 를 Administrative Tools > Certificate Authority 선택합니다.
- 2. 왼쪽 창에서 CA를 확장합니다. 폴더를 마우스 오른쪽 단추로 Revoked Certificates 클릭하고 을 선 택합니다Properties.
- 3. CRL 게시 간격 필드에 필수 번호를 입력하고 기간을 선택합니다. 창ox을 닫고 변경 사항을 적 용하려면 클릭합니다. 이 예에서는 게시 간격을 7일로 구성합니다.



4. ClockSkew certutil-getreg CA\Clock\* 값을 확인하려면 명령을 입력합니다. 기본값은 10분입니다.

출력 예:

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

5. 명령을 certutil -getreg CA\CRLov\* 입력하여 CRLOverlapPeriod가 수동으로 설정되었는지 확인합니다. 기본적으로 CRLOverlapUnit 값은 0이며, 이는 수동 값이 설정되지 않았음을 나타냅니다. 값이 0이 아닌 경우 값과 단위를 기록합니다.

Values: CRLOverlapPeriod REG\_SZ = Hours CRLOverlapUnits REG\_DWORD = 0 CertUtil: -getreg command completed successfully.

6. 명령을 certutil -getreg CA\CRLpe\* 입력하여 3단계에서 설정한 CRLPeriod를 확인합니다.

출력 예:

Values: CRLPeriod REG\_SZ = Days CRLUnits REG\_DWORD = 7 CertUtil: -getreg command completed successfully.

7. 다음과 같이 CRL 유예 기간을 계산합니다.

a. CRLOverlapPeriod가 5단계에서 설정된 경우: OVERLAP = CRLOverlapPeriod, 분 단위

기타: OVERLAP = (CRLPeriod / 10), 분 단위

b. OVERLAP이 720을 초과하는 경우 OVERLAP = 720

c. OVERLAP < (1.5 \* ClockSkewMinutes)이 발생하면 OVERLAP = (1.5 \* ClockSkewMinutes)

d. OVERLAP > CRLPeriod인 경우(분) OVERLAP = CRLPeriod(분)

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

계산된 유예 기간은 CA가 다음 CRL을 게시하는 시점과 현재 CRL이 만료되는 시점 사이의 시 간입니다. 그에 따라 CRL을 검색하도록 ISE를 구성해야 합니다.

8. ISE 기본 관리 노드에 로그인하고 를 선택합니다Administration > System > Certificates. 왼쪽 창에서 를

#### 선택합니다Trusted Certificate.

≡ Cisco ISE	Administration · System										
Deployment Licensing	Certificates	s Logging	Maintenance	Upgrade	Health Checks	Backup & Resto	re Admin Acce	ss Settings			Click h
Certificate Management ~ System Certificates	Trus	ted Certifi	icates								
Trusted Certificates	0 Edit	+ Import 🕁 D	sport 👩 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 9B EE 97 53	abtomar-WIN-231PN	abtomar-WIN-231PN	Wed, 20 Feb 2019	Sun, 20 Feb 2039	
		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	

- 9. CRL을 구성하려는 CA 인증서 옆의 확인란을 선택합니다. 를 Edit클릭합니다.
- 10. 창 아래쪽에서 확인란을 Download CRL 선택합니다.
- 11. CRL Distribution URL(CRL 배포 URL) 필드에 CRL 배포 지점의 경로를 입력합니다. 이 경로 에는 섹션 2에서 생성한 .crl 파일이 포함됩니다. 이 예에서 URL은 다음과 같습니다.

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

- 12. ISE는 정기적으로 또는 만료에 따라 CRL을 검색하도록 구성할 수 있습니다(일반적으로 이 기 간도 정기임). CRL 게시 간격이 정적일 경우, 후자 옵션을 사용할 때 더 적시에 CRL 업데이트 를 얻을 수 있습니다. 라디오 버튼을 Automatically 클릭합니다.
- 13. 읽어들일 값을 단계 7에서 계산한 유예 기간보다 작은 값으로 설정합니다. 값 집합이 유예 기 간보다 긴 경우 ISE는 CA가 다음 CRL을 게시하기 전에 CRL 배포 지점을 확인합니다. 이 예 에서 유예 기간은 730분, 또는 12시간 10분으로 계산됩니다. 10시간 값이 검색에 사용됩니다.
- 14. 환경에 적합한 재시도 간격을 설정합니다. ISE는 이전 단계에서 구성된 간격으로 CRL을 검색 할 수 없는 경우 이 짧은 간격으로 다시 시도합니다.
- 15. ISE가 Bypass CRL Verification if CRL is not Received 마지막 다운로드 시도에서 이 CA에 대한 CRL을 검 색할 수 없는 경우 CRL 확인 없이 인증서 기반 인증이 정상적으로 진행되도록 허용하려면 확 인란을 선택합니다. 이 확인란을 선택하지 않으면 CRL을 검색할 수 없는 경우 이 CA에서 발 급한 인증서를 사용하는 모든 인증서 기반 인증이 실패합니다.
- 16. ISE가 Ignore that CRL is not yet valid or expired 만료된(또는 아직 유효하지 않은) CRL 파일을 유효한 것처럼 사용하도록 허용하려면 확인란을 선택합니다. 이 확인란을 선택하지 않으면 ISE는 CRL을 유효 날짜 이전 및 다음 업데이트 시간 이후에 유효하지 않은 것으로 간주합니다. 컨피 그레이션Save을 완료하려면 클릭하십시오.

Certificate Status Validation							
	To verify certificates, enable the m OCSP Configuration Validate against OCSP Servic Reject the request if OC Reject the request if OC Certificate Revocation List Configure Ownload CRL						
	CRL Distribution URL	http://win-231	pnbs4iph/crld/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     Bypass CRL Verific     Ignore that CRL is i	tity Check () ation if CRL is not not yet valid or exp	Received				

Save

# 다음을 확인합니다.

현재 이 설정에 사용 가능한 확인 절차는 없습니다.

# 문제 해결

현재 이 설정에 사용할 수 있는 특정 문제 해결 정보가 없습니다.

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번 역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.