Konfigurieren von Microsoft CA Server zum Veröffentlichen der Zertifikatsperrlisten für ISE

Inhalt

<u>Einleitung</u>

Voraussetzung

Anforderungen

Verwendete Komponenten

Konfigurieren

Erstellen und Konfigurieren eines Ordners auf der Zertifizierungsstelle, in dem die Sperrlisten-Dateien gespeichert werden Erstellen einer Site in IIS zum Verfügbarmachen des neuen Zertifikatsperrlisten-Verteilungspunkts

Konfigurieren von Microsoft CA Server zum Veröffentlichen von CRL-Dateien am Verteilungspunkt

Überprüfen Sie, ob die Sperrlisten-Datei vorhanden und über IIS zugänglich ist.

Konfigurieren der ISE zur Verwendung des neuen CRL-Verteilungspunkts

<u>Überprüfung</u>

Fehlerbehebung

Einleitung

In diesem Dokument wird die Konfiguration eines Microsoft Certificate Authority (CA)-Servers beschrieben, der Internetinformationsdienste (IIS) ausführt, um die Zertifikatsperrlisten-Updates (Certificate Revocation List, CRL) zu veröffentlichen. Außerdem wird erläutert, wie Sie die Cisco Identity Services Engine (ISE) (Version 3.0 und höher) konfigurieren, um die Updates zur Verwendung bei der Zertifikatsvalidierung abzurufen. Die ISE kann so konfiguriert werden, dass sie Zertifikatsperrlisten für die verschiedenen Zertifizierungsstellen-Stammzertifikate abruft, die sie bei der Zertifikatsvalidierung verwendet.

Voraussetzung

Anforderungen

Es gibt keine spezifischen Anforderungen für dieses Dokument.

Verwendete Komponenten

Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

Cisco Identity Services Engine Version 3.0

Microsoft Windows Server 2008 R2

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

Konfigurieren

In diesem Abschnitt erfahren Sie, wie Sie die in diesem Dokument beschriebenen Funktionen konfigurieren können.

Erstellen und Konfigurieren eines Ordners auf der Zertifizierungsstelle, in dem die Sperrlisten-Dateien gespeichert werden

Die erste Aufgabe besteht darin, einen Speicherort auf dem Zertifizierungsstellenserver zum Speichern der Zertifikatsperrlisten-Dateien zu konfigurieren. Standardmäßig veröffentlicht der Microsoft CA-Server die Dateien auf C:\Windows\system32\CertSrv\CertEnroll\

Anstatt diesen Systemordner zu verwenden, erstellen Sie einen neuen Ordner für die Dateien.

1. Wählen Sie auf dem IIS-Server einen Speicherort im Dateisystem aus, und erstellen Sie einen neuen Ordner. In diesem Beispiel C:\CRLDistribution wird der Ordner erstellt.



 Damit die Zertifizierungsstelle die Zertifikatsperrlisten-Dateien in den neuen Ordner schreiben kann, muss die Freigabe aktiviert sein. Klicken Sie mit der rechten Maustaste auf den neuen Ordner, wählen Sie Properties, klicken Sie auf die Sharing Registerkarte und dann auf 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.	
Close Cancel Apply	

3. Um den Ordner freizugeben, aktivieren Sie das Share this folder Kontrollkästchen, und fügen Sie

dann am Ende des Freigabenamens im Feld Freigabename ein Dollarzeichen (\$) hinzu, um die Freigabe auszublenden.

Adv	anced Sharing
	Settings Share name:
	CRLDistribution\$
	Add Remove
	Limit the number of simultaneous users to: 77216
1.1	Permissions Caching OK Cancel

4. Klicken Sie auf Permissions (1), klicken Sie auf Add (2), klicken Sie auf Object Types (3), und aktivieren Sie das Computers Kontrollkästchen (4).

Advanced Sharing	🖡 Permissions for CRLDistributio	n\$	Se	elect Users, Computers, Service Accounts,	or Groups
Share this folder Settings Share name: CRLDistribution\$ Add Remove	Share Permissions Control Share Permissions			Select this object type: Users, Groups, or Built-in security principals From this location: Itpaaa.local Enter the object names to select (<u>examples</u>)	Object Types Locations Object Manager
Comments:	Permissions for Everyone Full Control Change Read	Add	Remor	Object Types Select the types of objects you want to fin Object types:	d.
	Learn about access control and per	missions			
	ОК	Cancel	Apply		OK Cancel

5. Um zum Fenster Benutzer, Computer, Dienstkonten oder Gruppen auswählen zurückzukehren, klicken Sie auf ok. Geben Sie im Feld Geben Sie die zu verwendenden Objektnamen ein den Computernamen des Zertifizierungsstellenservers in diesem Beispiel ein: WIN0231PNBS4IPH, und klicken Sie auf Check Names. Wenn der eingegebene Name gültig ist, wird der Name aktualisiert und unterstrichen angezeigt. Klicken Sie auf .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. Wählen Sie im Feld "Group or user names" (Gruppen- oder Benutzernamen) den CA-Computer aus. Überprüfen SieAllow, ob Vollzugriff gewährt wird, um vollständigen Zugriff auf die Zertifizierungsstelle zu erhalten.

Klicken Sie auf .ok Klicken Sie ok erneut auf, um das Fenster Erweiterte Freigabe zu schließen und zum Fenster Eigenschaften zurückzukehren.

Permissions for CRLDistribu	utionS	>
Share Permissions		
Group or user names:		
Everyone	DMAR\WIN-231PNE	BS4IPH\$)
	Add	Remove
Permissions for WIN-231PNBS4IPH	Allow	Deny
Full Control Change Read	\leq	

7. Damit die Zertifizierungsstelle die Sperrlisten-Dateien in den neuen Ordner schreiben kann, müssen Sie die entsprechenden Sicherheitsberechtigungen konfigurieren. Klicken Sie auf diesecurity Registerkarte (1), klicken Sie auf Edit (2), klicken Sie auf Add (3), klicken Sie auf Object Types (4), und aktivieren Sie das Computers Kontrollkästchen (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 Administrators (BTPAAA\Administrators)	SYSTEM SAdministrators (RTPAAA\Administrators)
Service (RTPAAA\Users)	Kusers (RTPAAA\Users)
To change permissions, click Edit.	
Permissions for CREATOR	
OWNER Allow Deny	Permissions for CREATOR
Modify	OWNER Allow Deny
Read & execute	Full control
List folder contents	Read & exec
Write -	List folder co
Select Users, Computers, Service Accounts, or Groups	? X
Select this object type:	ac Object types:
Users, Groups, or Built-in security principals 4_0	Dbject Types
From this location:	Computers 5
Itpaaa.local	Locations
Enter the object names to select (<u>examples</u>):	
	Check Names
Advanced	Cancel OK Cancel

8. Geben Sie im Feld Geben Sie die zu verwendenden Objektnamen ein den Computernamen des Zertifizierungsstellenservers ein, und klicken Sie auf Check Names. Wenn der eingegebene Name gültig ist, wird der Name aktualisiert und unterstrichen angezeigt. Klicken Sie auf .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. Wählen Sie den CA-Computer im Feld "Group or user names" (Gruppen- oder Benutzernamen) aus, und überprüfen SieAllow, ob die CA den vollen Zugriff erhält. Klicken Sie auf ok , und klicken Sie dann aufclose, um die Aufgabe abzuschließen.

ecurity		
Object name: C:\CRLDistrib	oution	
Group or user names:		
SCREATOR OWNER		
SYSTEM		
Administrators (ABTOMA	R\Administrators)	
Series (ABTOMAR\Users)	
	TOTAL	
WIN-231PNBS4IPH (AB	TOMAR\WIN-231PNE	S4IPH\$)
WIN-231PNBS4IPH (AB	TOMAR\WIN-231PNE	S4IPH\$)
WIN-231PNBS4IPH (AB	TOMAR\WIN-231PNE	S4IPH\$) Remove
Permissions for	TOMAR\WIN-231PNE	S4IPH\$) Remove
Permissions for WIN-231PNBS4IPH (AB Permissions for WIN-231PNBS4IPH	TOMAR\WIN-231PNE Add Allow	S4IPH\$) Remove Deny
Permissions for WIN-231PNBS4IPH (AB WIN-231PNBS4IPH Full control	TOMAR\WIN-231PNE Add Allow	S4IPH\$) Remove Deny
Permissions for WIN-231PNBS4IPH (AB WIN-231PNBS4IPH Full control Modify	TOMAR\WIN-231PNE Add Allow	S4IPH\$) Remove Deny
Permissions for WIN-231PNBS4IPH (AB WIN-231PNBS4IPH Full control Modify Read & execute	TOMAR\WIN-231PNE Add Allow	S4IPH\$) Remove Deny
Permissions for WIN-231PNBS4IPH (AB WIN-231PNBS4IPH Full control Modify Read & execute List folder contents	TOMAR\WIN-231PNE Add Allow	S4IPH\$) Remove Deny
Permissions for WIN-231PNBS4IPH Full control Modify Read & execute List folder contents Read	TOMAR\WIN-231PNE Add Allow	S4IPH\$)

Erstellen einer Site in IIS zum Verfügbarmachen des neuen Zertifikatsperrlisten-Verteilungspunkts

Damit die ISE auf die CRL-Dateien zugreifen kann, machen Sie das Verzeichnis, in dem sich die CRL-Dateien befinden, über IIS zugänglich.

- 1. Klicken Sie in der Taskleiste des IIS-Servers auf start. Wählen Sie Administrative Tools > Internet Information Services (IIS) Manager.
- 2. Erweitern Sie im linken Bereich (Konsolenstruktur) den IIS-Servernamen, und erweitern Sie dann sites.



3. Klicken Sie mit der rechten Maustaste, Default Web Site und wählen Sie Add Virtual Directory, wie in diesem Bild dargestellt.

💐 Internet Information Services (IIS) Manager



4. Geben Sie im Feld Alias einen Standortnamen für den Zertifikatsperrlisten-Verteilungspunkt ein. In diesem Beispiel wird CRLD eingegeben.

Add Virtual Dire	ectory			? ×
Site name: Path:	Default Web Site /			
Alias: CRLD Example: ima	ges			
Physical path C:\CRLDistrib	: ution			
Pass-through	authentication	1		
Connect as	Test Settings	OK	0	ancel

5. Klicken Sie auf die Auslassungszeichen (. . .) rechts vom Feld Physical path (Physischer Pfad) angezeigt und navigieren Sie zu dem in Abschnitt 1 erstellten Ordner. Wählen Sie den Ordner aus, und klicken Sie auf ok. Klicken Sie aufok, um das Fenster Virtuelles Verzeichnis hinzufügen zu schließen.

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		
ОК	Cancel	

6. Der in Schritt 4 eingegebene Standortname muss im linken Bereich hervorgehoben werden. Wenn nicht, wählen Sie es jetzt aus. Doppelklicken Sie im mittleren Bereich auf Directory Browsing.

Internet Information Services (IIS) N	Manager					
← → ² → WIN-231PNBS4IF	PH 🕨 Sites 🕨	Default Web	Site + CRLD	•		
File View Help						
Connections	CRI	LD Home	;			
VIII Start Page	Filter:		• 🦻 Go - 🖣	Show All	Group by:	
Application Pools Sites Oefault Web Site			- Aliana and a second s			404
> - Centenroll > - CentSrv	ASP	Autnentic	Compression	Document	Browsing	Error Pages
/ <u>Ma</u> circo	8	2				132
	Failed Request Tra	Handler Mappings	Redirect	HTTP Respon	Logging	MIME Types
	4		8	9		
	Modules	Output Caching	Request Filtering	SSL Settings		
	Managemer	nt				

7. Klicken Sie im rechten Bereich aufEnable, um die Verzeichnissuche zu aktivieren.



8. Wählen Sie im linken Bereich erneut den Standortnamen aus. Doppelklicken Sie im mittleren Bereich auf Configuration Editor.



9. Wählen Sie in der Dropdown-Liste Abschnitt die Option system.webServer/security/requestFiltering. Wählen Sie in der allowDoubleEscaping Dropdown-Liste die Option True. Klicken Sie im rechten Fensterbereich auf Apply, wie in diesem Bild dargestellt.

🐚 Internet Information Services (IIS)	Manager			- 🗆 ×
← → [®] ► WIN-231PNBS4I	PH + Sites + Default Web Site + CRLD +			📴 🖂 🟠 i 🔞 •
File View Help				
Connections	Configuration Editor Section: system.webServer/security/requestFit	Hering + From: Default Web Site/CRLD Web.config	•	Actions Actions Apply Apply Actions Cancel Configuration
 ✓ Sites ✓ ● Default Web Site > 20 CertEnroll > 20 CertSrv > 20 CertD 	allowboudescaping allowHighBitCharacters alwaysAllowedQueryStrings alwaysAllowedUrls denyQueryStringSequences denyUrlSequences	False (Count=0) (Count=0)		Section Lock Section 'allowDoubleEscaping'

Der Zugriff auf den Ordner muss nun über IIS möglich sein.

Konfigurieren von Microsoft CA Server zum Veröffentlichen von CRL-Dateien am Verteilungspunkt

Nachdem ein neuer Ordner konfiguriert wurde, in dem die Zertifikatsperrlisten-Dateien gespeichert sind, und der Ordner in IIS verfügbar gemacht wurde, konfigurieren Sie den Microsoft-Zertifizierungsstellenserver so, dass die Zertifikatsperrlisten-Dateien am neuen Speicherort veröffentlicht werden.

- 1. Klicken Sie in der Taskleiste des CA-Servers auf start. Wählen Sie Administrative Tools > Certificate Authority.
- Klicken Sie im linken Bereich mit der rechten Maustaste auf den Namen der Zertifizierungsstelle. Wählen Sie Properties, und klicken Sie dann auf die Extensions Registerkarte. Um einen neuen CRL-Verteilungspunkt hinzuzufügen, klicken Sie auf Add.

Enrollment Agents	Auditing	Recove	ry Agents	Secu	irîty
General	Policy Mo	Policy Module E			
Extensions	Storage	Storage Certificate I			
Coloct extension:					
Select extension.					
CRL Distribution Point	(CDP)				V
Specify locations from	which users can	i obtain a ce	ertificate rev	ocation lis	t
(CRL).					
CAME down and and	2\C-+C-+\C-+C	and a Cali		Jama C. ffi	
C:\Windows\systems	catedName> <c< td=""><td>RI Name Sud</td><td>ame><urli fix> CN=<s< td=""><td>everShod</td><td>i Na</td></s<></urli </td></c<>	RI Name Sud	ame> <urli fix> CN=<s< td=""><td>everShod</td><td>i Na</td></s<></urli 	everShod	i Na
http://cServerDNSNa	me>/CertForoll	<pre>/cCaName></pre>	CRI Name	Suffix> <d< td=""><td>urve Ieltz</td></d<>	urve Ieltz
Thep 37 Cool Verbitshe		veaname,			CURE
Ifile:// <serverdnsnar< td=""><td>me>/CertEnroll/</td><td><caname><</caname></td><td>CRLNameS</td><td>Suffix><de< td=""><td>tal</td></de<></td></serverdnsnar<>	me>/CertEnroll/	<caname><</caname>	CRLNameS	Suffix> <de< td=""><td>tal</td></de<>	tal
file:// <serverdnsnar< th=""><th>me>/CertEnroll/</th><th><caname><</caname></th><th>CRLName</th><th>Suffix><de< th=""><th>lta</th></de<></th></serverdnsnar<>	me>/CertEnroll/	<caname><</caname>	CRLName	Suffix> <de< th=""><th>lta</th></de<>	lta
file:// <serverdnsnar< th=""><th>me>/CertEnroll/</th><th><caname><</caname></th><th>(CRLName)</th><th>Suffix><de< th=""><th>ita ></th></de<></th></serverdnsnar<>	me>/CertEnroll/	<caname><</caname>	(CRLName)	Suffix> <de< th=""><th>ita ></th></de<>	ita >
file:// <serverdnsnar< td=""><td>me>/CertEnroll/</td><td><caname></caname></td><td>CRLName</td><td>Suffix><de< td=""><td>ita ></td></de<></td></serverdnsnar<>	me>/CertEnroll/	<caname></caname>	CRLName	Suffix> <de< td=""><td>ita ></td></de<>	ita >
file:// <serverdnsnar< td=""><td>me>/CertEnroll/</td><td><caname><</caname></td><td>CRLNames</td><td>Suffix><de Remove</de </td><td>ita ></td></serverdnsnar<>	me>/CertEnroll/	<caname><</caname>	CRLNames	Suffix> <de Remove</de 	ita >
file:// <serverdnsnar< td=""><td>me>/CertEnroll/</td><td><caname> Ad</caname></td><td>CRLName</td><td>Suffix><de Remove</de </td><td>ita ></td></serverdnsnar<>	me>/CertEnroll/	<caname> Ad</caname>	CRLName	Suffix> <de Remove</de 	ita >
File:// <serverdnsnar< td=""><td>s location</td><td><caname> Ad</caname></td><td>CRLNames</td><td>Remove</td><td>ita ></td></serverdnsnar<>	s location	<caname> Ad</caname>	CRLNames	Remove	ita >
File:// <serverdnsnar< p=""> Include in all CRLs.</serverdnsnar<>	s location	<caname> Ad e to publish</caname>	CRLNames	Remove	> >
 File://<serverdnsnar< li=""> Publish CRLs to this Include in all CRLs. when publishing ma </serverdnsnar<>	s location Specifies where anually.	<caname> Ad</caname>	CRLNames	Remove	/ >
 File://<serverdnsnar< li=""> Publish CRLs to this Include in all CRLs. when publishing ma Include in CRLs. Cl </serverdnsnar<>	me>/CertEnroll/ s location . Specifies where anually. ients use this to r	<caname>< Ad e to publish find Delta C</caname>	CRLNames	Remove Remove	elta >
File:// <serverdnsnar all="" cdp<="" cl="" crls="" crls.="" in="" include="" ma="" publish="" publishing="" td="" the="" this="" to="" when=""><td>s location Specifies where anually.</td><td><caname> Ad to publish find Delta C ued certifica</caname></td><td>CRLNames</td><td>Remove Remove</td><td> ta ></td></serverdnsnar>	s location Specifies where anually.	<caname> Ad to publish find Delta C ued certifica</caname>	CRLNames	Remove Remove	ta >
File:// <serverdnsnar all="" c="" cdp="" cl="" crls="" crls.="" crls.<="" data="" in="" include="" ma="" publish="" publishing="" td="" the="" this="" to="" when=""><td>s location Specifies where anually. ients use this to extension of issue</td><td><caname>< Ad e to publish find Delta C ued certifica</caname></td><td>CRLNames</td><td>Remove Remove</td><td>lta</td></serverdnsnar>	s location Specifies where anually. ients use this to extension of issue	<caname>< Ad e to publish find Delta C ued certifica</caname>	CRLNames	Remove Remove	lta
file:// <serverdnsnar Publish CRLs to this Include in all CRLs. when publishing ma Include in CRLs. Cl Include in the CDP Publish Delta CRLs</serverdnsnar 	me>/CertEnroll/ s location . Specifies where anually. ients use this to extension of issu to this location	<caname>< Ad e to publish find Delta C ued certifica</caname>	CRLNameS Id	Remove Remove	lta
file:// <serverdnsnar Publish CRLs to this Include in all CRLs. when publishing ma Include in CRLs. Cl Include in the CDP Publish Delta CRLs Include in the IDP e</serverdnsnar 	me>/CertEnroll/ s location . Specifies where anually. ients use this to extension of issu to this location extension of issu	CaName> Ad to publish find Delta C ued certifica ed CRLs	CRLNameS Id	Remove Remove	lta
file:// <serverdnsnar all="" cdp="" cl="" crls="" crls.="" delta="" e<="" idp="" in="" include="" ma="" publish="" publishing="" td="" the="" this="" to="" when=""><td>me>/CertEnroll/ s location . Specifies where anually. ients use this to extension of issu to this location extension of issu</td><td>CaName> Ad e to publish find Delta C ued certifica ed CRLs</td><td>CRLNames</td><td>Remove Remove</td><td>lta</td></serverdnsnar>	me>/CertEnroll/ s location . Specifies where anually. ients use this to extension of issu to this location extension of issu	CaName> Ad e to publish find Delta C ued certifica ed CRLs	CRLNames	Remove Remove	lta
 file://<serverdnsnar< li=""> < Publish CRLs to this □ Include in all CRLs. cli □ Include in CRLs. cli □ Include in the CDP ✓ Publish Delta CRLs □ Include in the IDP e </serverdnsnar<>	me>/CertEnroll/ s location . Specifies where anually. ients use this to extension of issu to this location extension of issu	CaName> Ad e to publish find Delta C ued certifica ed CRLs	CRLNameS Id	Remove Remove	lta

3. Geben Sie im Feld Location (Speicherort) den Pfad zu dem in Abschnitt 1 erstellten und freigegebenen Ordner ein. Im Beispiel in Abschnitt 1 lautet der Pfad:

\\WIN-231PNBS4IPH\CRLDistribution\$

Add Location	Х
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.	is, ct
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
<	>
OK Cancel	

4. Wählen Sie bei ausgefülltem Feld "Location" aus der Dropdown-Liste "Variable" aus, und klicken Sie dann auf 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 < OK Cancel

5. Wählen Sie in der Dropdown-Liste Variable die Option aus, und klicken Sie dann auf 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, selec the variable below and click Insert.	s. t
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><crlname< td=""><td>Sı</td></crlname<></caname></servername>	Sı
<	>
OK Cancel	

6. Hängen Sie im Feld Location (Ort) .crl das Ende des Pfades an. In diesem Beispiel lautet der Speicherort:

\\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></crlnamesuffix>	~	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><CRLNameSu

7. Klicken Sie auf OK, um zur Registerkarte Erweiterungen zurückzukehren. Aktivieren Sie das Publish CRLs to this location Kontrollkästchen, und klicken Sie dann auf, OK um das Eigenschaftenfenster zu schließen.

Eine Eingabeaufforderung wird angezeigt, um die Berechtigung zum Neustart der Active Directory-Zertifikatdienste zu erhalten. Klicken Sie auf .Yes

×

Enrollment Agents	Auditing	Recovery Agents	Security	
General	Policy Mo	dule E	ot Module	
Extensions	Storage	Certificat	e Managers	
Select extension:				
CRL Distribution Point	(CDP)		~	
Specify locations from (CRL).	which users car	n obtain a certificate re	evocation list	
C:\Windows\system3	2\0	ing Authority		
C:\Windows\system3 Idap:///CN= <catrunk http://<serverdnsnar file://<serverdnsnar \\\\\\\\$ServerDNSAIP</serverdnsnar </serverdnsnar </catrunk 	2\C cate me me> TVC	ion Authority You must restart / take effect. Do yo	Active Directory Co u want to restart th	rtificate Services for the changes to te service now?
C:\Windows\system3 Idap:///CN= <catrun http://<serverdnsnar file://<serverdnsnar \\\\\\\.231PNBS4IPH < Publish CRLs to this</serverdnsnar </serverdnsnar </catrun 	2VC cate sme he> VC	ion Authority You must restart A take effect. Do yo	Active Directory Ce u want to restart ti	rtificate Services for the changes to te service now? Yes No

Klicken Sie im linken Bereich mit der rechten Maustaste Revoked Certificates. Wählen Sie All Tasks
 Publish. Stellen Sie sicher, dass Neue Zertifikatsperrliste ausgewählt ist, und klicken Sie dann auf ок.

🙀 certsrv - [Certification Autho	rity (Local)\abtoma	r-Wil	N-231PNBS4IPH-	CA\Revoked Certificates]
File Action View Help				
🗢 🔿 🖄 🔛 🖉				
Certification Authority (Local)) Request ID	Re	vocation Date	Effective Revocation Date
Bevoked Certificat			The	e are no items to show in this vi
Ssued Certificates	All Tasks	>	Publish	
Pending Requests Failed Requests	View			
📔 Certificate Templa	Refresh			
	Properties			
	Help			

Der Microsoft CA-Server muss in dem in Abschnitt 1 erstellten Ordner eine neue .crl-Datei erstellen. Wenn die neue CRL-Datei erfolgreich erstellt wurde, wird nach dem Klicken auf "OK" kein Dialogfeld angezeigt. Wenn ein Fehler bezüglich des neuen Verteilungspunktordners zurückgegeben wird, wiederholen Sie sorgfältig jeden Schritt in diesem Abschnitt.

Überprüfen Sie, ob die Sperrlisten-Datei vorhanden und über IIS zugänglich ist.

Überprüfen Sie, ob die neuen Sperrlisten-Dateien vorhanden sind und ob sie über IIS von einer anderen Workstation aus zugänglich sind, bevor Sie mit diesem Abschnitt beginnen.

1. Öffnen Sie auf dem IIS-Server den in Abschnitt 1 erstellten Ordner. Es muss eine einzelne .crl-Datei mit dem Formular vorhanden sein,

```
.crl
```

wobei

für den Namen des Zertifizierungsstellenservers steht. In diesem Beispiel lautet der Dateiname:

abtomar-WIN-231PNBS4IPH-CA.crl



2. Öffnen Sie von einer Workstation im Netzwerk (idealerweise im selben Netzwerk wie der primäre ISE-Admin-Knoten) einen Webbrowser, und navigieren Sie zu http://

/	
, wo	bei
der	in Abschnitt 2 konfigurierte Servername des IIS-Servers und
der	für den Verteilungspunkt in Abschnitt 2 ausgewählte Standortname ist. In diesem
Beis	piel lautet die URL:

http://win-231pnbs4iph/CRLD

Der Verzeichnisindex wird angezeigt, der die in Schritt 1 beobachtete Datei enthält.



Konfigurieren der ISE zur Verwendung des neuen CRL-Verteilungspunkts

Bevor die ISE zum Abrufen der Zertifikatsperrliste konfiguriert wird, definieren Sie das Intervall zum Veröffentlichen der Zertifikatsperrliste. Die Strategie zur Bestimmung dieses Intervalls geht über den Rahmen dieses Dokuments hinaus. Die potenziellen Werte (in Microsoft CA) betragen 1 Stunde bis einschließlich 411 Jahre. Der Standardwert ist 1 Woche. Wenn Sie ein für Ihre Umgebung geeignetes Intervall festgelegt haben, gehen Sie wie folgt vor, um das Intervall festzulegen:

- 1. Klicken Sie in der Taskleiste des CA-Servers auf Start. Wählen Sie Administrative Tools > Certificate Authority.
- 2. Erweitern Sie im linken Bereich die Zertifizierungsstelle. Klicken Sie mit der rechten Maustaste auf den Revoked Certificates Ordner, und wählen Sie Properties.
- 3. Geben Sie in die Felder für das Veröffentlichungsintervall der Zertifikatsperrliste die erforderliche Anzahl ein, und wählen Sie den Zeitraum aus. Klicken Sie auf ok, um das Fenster zu schließen und die Änderung zu übernehmen. In diesem Beispiel wird ein Veröffentlichungsintervall von sieben Tagen konfiguriert.



4. Geben Sie den certutil -getreg CA\Clock* Befehl zur Bestätigung des ClockSkew-Werts ein. Der Standardwert ist 10 Minuten.

Beispiel:

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

5. Geben Sie den certutil-getreg CA\CRLov* Befehl ein, um zu überprüfen, ob CRLOverlapPeriod manuell festgelegt wurde. Standardmäßig ist der CRLOverlapUnit-Wert 0, was darauf

hinweist, dass kein manueller Wert festgelegt wurde. Wenn der Wert ein anderer Wert als 0 ist, zeichnen Sie den Wert und die Einheiten auf.

Beispiel:

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

6. Geben Sie den certutil-getreg CA\CRLpe* Befehl zum Überprüfen der CRLPeriod ein, der in Schritt 3 festgelegt wurde.

Beispiel:

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

7. Berechnen Sie die Sperrlisten-Kulanzfrist wie folgt:

a. Wenn CRLOverlapPeriod in Schritt 5 festgelegt wurde: OVERLAP = CRLOverlapPeriod, in Minuten;

Sonst: OVERLAP = (CRLPeriod / 10), in Minuten

b. Wenn ÜBERLAPPUNG > 720, dann ÜBERLAPPUNG = 720

c. Wenn OVERLAP < (1,5 * ClockSkewMinutes), dann OVERLAP = (1,5 * ClockSkewMinutes)

d. Wenn OVERLAP > CRLPeriod, in Minuten, dann OVERLAP = CRLPeriod in Minuten

e. Toleranzperiode = ÜBERLAPPUNG + UhrVerzerrungMinuten

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

Die berechnete Kulanzfrist ist der Zeitraum zwischen dem Veröffentlichen der nächsten Zertifikatsperrliste durch die Zertifizierungsstelle und dem Ablauf der aktuellen Zertifikatsperrliste. Die ISE muss so konfiguriert werden, dass die Zertifikatsperrlisten entsprechend abgerufen werden können.

8. Melden Sie sich beim ISE-Knoten "Primärer Admin" an, und wählen Sie Administration > System > Certificates. Wählen Sie im linken Bereich Trusted Certificate.

≡ Cisco ISE	SE Administration - System										
Deployment Licensing	Certificate	s Logging Ma	aintenance	Upgrade	Health Checks	Backup & Resto	re Admin Acce	ss Settings			Click h
Certificate Management ~ System Certificates	Trus	ted Certifica	tes								
Trusted Certificates	/ Edit	+ Import 🕁 Export	C Delete	Q View							
OCSP Client Profile											
Certificate Signing Requests	0	Friendly Name		Status	Trusted For	Serial Number	Issued To	Issued By	Valid From	Expiration Date	Expiratio
Certificate Periodic Check Se	0	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	
	0	Cisco ECC Root CA 2099		Enabled	Cisco Services	03	Cisco ECC Root CA	Cisco ECC Root CA	Thu, 4 Apr 2013	Mon, 7 Sep 2099	
	0	Cisco Licensing Root CA		Enabled	Cisco Services	01	Cisco Licensing Root	Cisco Licensing Root	Fri, 31 May 2013	Mon, 31 May 2038	

- 9. Aktivieren Sie das Kontrollkästchen neben dem Zertifizierungsstellenzertifikat, für das Sie Zertifikatsperrlisten konfigurieren möchten. Klicken Sie auf .Edit
- 10. Aktivieren Sie das Download CRL Kontrollkästchen unten im Fenster.
- 11. Geben Sie im Feld "CRL Distribution URL" (URL für Zertifikatsperrlisten-Verteilung) den Pfad zum CRL Distribution Point ein, der die in Abschnitt 2 erstellte CRL-Datei enthält. In diesem Beispiel lautet die URL:

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

- 12. Die ISE kann so konfiguriert werden, dass die Zertifikatsperrliste in regelmäßigen Abständen oder auf Basis des Ablaufdatums abgerufen wird (was im Allgemeinen ebenfalls ein regelmäßiges Intervall ist). Wenn das CRL-Veröffentlichungsintervall statisch ist, werden bei Verwendung der zweiten Option schnellere CRL-Updates abgerufen. Klicken Sie auf das Automatically Optionsfeld.
- 13. Stellen Sie den Wert für den Abruf auf einen Wert ein, der kleiner ist als der in Schritt 7 berechnete Kulanzzeitraum. Wenn der eingestellte Wert die Toleranzperiode überschreitet, überprüft die ISE den Sperrlisten-Verteilungspunkt, bevor die Zertifizierungsstelle die nächste Sperrliste veröffentlicht hat. In diesem Beispiel wird die Kulanzfrist auf 730 Minuten bzw. 12 Stunden und 10 Minuten berechnet. Für den Abruf wird ein Wert von 10 Stunden verwendet.
- 14. Legen Sie das Wiederholungsintervall entsprechend Ihrer Umgebung fest. Wenn die ISE die Zertifikatsperrliste im vorigen Schritt nicht im konfigurierten Intervall abrufen kann, wird in diesem kürzeren Intervall ein erneuter Versuch unternommen.
- 15. Aktivieren Sie das Bypass CRL Verification if CRL is not Received Kontrollkästchen, damit die zertifikatbasierte Authentifizierung normal (und ohne CRL-Prüfung) fortgesetzt werden kann, wenn ISE die CRL für diese CA beim letzten Downloadversuch nicht abrufen konnte. Wenn dieses Kontrollkästchen nicht aktiviert ist, schlägt die gesamte zertifikatbasierte Authentifizierung mit von dieser Zertifizierungsstelle ausgestellten Zertifikaten fehl, wenn die Zertifikatsperrliste nicht abgerufen werden kann.

16. Aktivieren Sie das Ignore that CRL is not yet valid or expired Kontrollkästchen, damit ISE abgelaufene (oder noch nicht gültige) Sperrlisten-Dateien so verwenden kann, als wären sie gültig. Wenn dieses Kontrollkästchen nicht aktiviert ist, betrachtet die ISE eine Sperrliste vor dem Datum des In-Kraft-Tretens und nach dem Zeitpunkt der nächsten Aktualisierung als ungültig. Klicken Sie hiersave, um die Konfiguration abzuschließen.

Certificate Status Validation					
To verify certificates, enable the m	ethods below. If bo	oth are enabled, OCSP will alway	s be tried first.		
OCSP Configuration					
Validate against OCSP Service	e	~			
Reject the request if OC Reject the request if OC	SP returns UNKNO	WWN status			
Certificate Revocation List Configure	ation				
Download CRL					
CRL Distribution URL	http://win-231	pnbs4iph/crld/abtomar-WIN	-231PNBS4IPH-CA.crl		
Retrieve CRL	 Automatically 	10	Hours	~	before expiration.
	O Every	1	Hours	~	
If download failed, wait	10	Minutes	· ~	before retry.	
Enable Server Iden	tity Check 🕕				
Sypass CRL Verific	ation if CRL is not	Received			
Ignore that CRL is	not yet valid or exp	pired			

Überprüfung

Für diese Konfiguration ist derzeit kein Überprüfungsverfahren verfügbar.

Fehlerbehebung

Für diese Konfiguration sind derzeit keine spezifischen Informationen zur Fehlerbehebung verfügbar.

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.