لاطبإ مئاوق رشنل Microsoft CA مداخ نيوكت ISE ل تاداەشلا

تايوتحملا

<u>قمدق مل ا</u>
<u>قي، س اس أل ا تابل طتمل ا</u>
<u>تابل طتمل ا</u>
<u>ةمدختسملاا تانبوكملا</u>
<u>نىيوك تارا</u>
<u>CRL تافليم نيمضتان قادصملاا عجزمانا دارع منيوكتو دل جم ءاشنا</u>
<u>قديدچل ا CRL عيزوت قطق فش كل IIS يف عقوم ءاش نا</u>
<u>عيزوتارا قطقن ديل CRL تافارم رشنال Microsoft CA مداخ نيوكت</u>
<u>ال ربع ميارا ليوصيولا فيناكماو CRL فارم دوجو نيم قيقرحتارا</u>
<u>قديدچل، CRL عيزوت قطق، مادختسال ISE نيوكت</u>
<u>قحصلا نم قىقىچىلا</u>
<u>امحال صاو ءاطخاًل ا فاش كت سا</u>

ةمدقملا

ليغشتب موقي يذلا Microsoft Certificate Authority (CA) مداخ نيوكت دنتسملا اذه فصي اضيأ حرشي وهو .(CRL) تاداهشلا لاطبا ةمئاق تاثيدحت رشنل (IIS) تنرتنإلا تامولعم تامدخ دادرتسال (ثدحألا تارادصإلاو 3.0 تارادصإلا) Cisco نم (ISE) ةيوهلا تامدخ كرحم نيوكت ةيفيك CRLs دادرتسال SE نيوكت نكمي .ةداهشلا ةحص نم ققحتلا يف اهمادختسال تاثيدحتلا .قداهشلا قحص نم ققحتلا يف اهمدختسي يتلا قفل تخمل CA رذج تاداهشل

ةىساسألا تابلطتملا

تابلطتملا

دنتسملا اذهل ةصاخ تابلطتم دجوت ال.

ةمدختسملا تانوكملا

ةيلاتلا ةيداملا تانوكملاو جماربلا تارادصإ ىلإ دنتسملا اذه يف ةدراولا تامولعملا دنتست

- Cisco Identity Services Engine، رادصإلاا 3.0
- ليغشتا Microsoft Windows Server 2008 R2 ل

ةصاخ ةيلمعم ةئيب يف ةدوجوملا ةزهجألاا نم دنتسملا اذه يف ةدراولا تامولعملا ءاشنإ مت. تناك اذإ .(يضارتفا) حوسمم نيوكتب دنتسملا اذه يف ةمدختسُملا ةزهجألا عيمج تأدب رمأ يأل لمتحملا ريثأتلل كمهف نم دكأتف ،ليغشتلا ديق كتكبش.

نيوكتلا

دنتسملا اذه يف ةحضوملا تازيملا نيوكت تامولعم كل مّدقُت ،مسقلا اذه يف.

CRL تافلم نيمضتل قدصملا عجرملا ىلع ەنيوكتو دلجم ءاشنإ

مداخ موقي .CRL تافلم نيزختل CA مداخ ىلع عقوم نيوكت يف ىلوألاا ةمەملا لثمتت Microsoft CA مداخ ىلع عقوم نيوكت يف ىلوألاا ةمەملا لشت

تافلملل ديدج دلجم ءاشنإب مق ،اذه ماظنلا دلجم مادختسإ نم الدب.

، لاثملا اذه يف .ديدج دلجم ءاشنإب مقو تافلملا ماظن ىلع اعقوم رتخأ ،IIS مداخ ىلع 1. دلجملا ءاشنإ C:\CRLDistribution ، دلجملا عاشن



نيكمت بجي ،ديدجلا دلجملا ىلإ CRL تافلم ةباتك نم قدصملا عجرملا نكمتي يكل .2 قوف رقناو ،Properties رتخاو ،ديدجلا دلجملا قوف نميألا سواملا رزب رقنا .ةكراشملا Sharing قوف رقنا مث ،بيوبتلا ةمالع

CRLDistribution Properties	X
General Sharing Security Previous Versions Customize	
Network File and Folder Sharing	1
Not Shared	
Network Path: Not Shared	
Share	
Advanced Sharing	
Set custom permissions, create multiple shares, and set other advanced sharing options.	
Advanced Sharing	
	-18
Close Cancel Apply	128

ىلإ (\$) رالود ةمالع ةفاضإب مق مث رايتخالا ةناخ ددح ،دلجملا ةكراشمل 3. Share this folder .ةكراشملا ءافخإل ةكراشملا مسا لقح يف ةكراشملا مس

Advanced Sharing	×
Share this folder	
Settings	
Share name:	
CRLDistribution\$	
Add Remove	
Limit the number of simultaneous users to:	
Comments:	
Permissions Caching	
OK Cancel Apply	100

4. ددحو، (3) Computers ددحو، (3) Add (2)، رايتخالا ةناخ Computers ددحو، (4) (4).

Advanced Sharing	Permissions for CRLDistribut	ion\$	Se	lect Users, Computers, Service Accounts, or Gro	ups ?X
Share this folder Settings Share name: CRLDistribution\$ Add Remove	Share Permissions		99 	ielect this object type: Users, Groups, or Built-in security principals from this location: ttpaaa.local Enter the object names to select (<u>examples</u>):	3 Object Types Locations
Comments:	2 Permissions for Everyone Full Control Change Read	Add	Remov	Object Types Select the types of objects you want to find. Object types: Image: Service Accounts Image: Service Accounts	
	Learn about access control and p			_	OK Cancel
	OK	Uancel	Apply		

رقنا ،تاعومجم وأ ةمدخ تاباسح وأ رتويبمك ةزهجأ وأ نيمدختسم ديدحت راطإ ىلإ ةدوعلل .5 CA مداخل رتويبمكلا مسا لخدأ ،لقحلا ديدحتل تانئاكلا ءامسأ لاخدا لقحلا يف .0K قوف ،احلاص هلاخدا مت يذلا مسالا ناك اذا .Check Names رقناو WIN0231PNBS4IPH :لاثملاا اذه يف ،متحت متي مسالا ناك .0K

Select Users, Computers, Service Accounts, or Group	s	Х
Select this object type:		
Users, Computers, Groups, or Built-in security principals		Object Types
From this location:		
abtomarJocal		Locations
Enter the object names to select (examples):		
WIN-231PNBS4IPH		Check Names
Advanced	ОК	Cancel

مكحت دوجو Allow نم ققحت .CA بساح رتخأ ،نيمدختسملا ءامسأ وأ ةعومجملا لقح يف .6 قدصملا عجرملا ىلٍ لماكلا لوصولا حنمل لماك.

راطإ ىلإ عوجرلاو "ةمدقتملا ةكراشملا" راطإ قالغإل ىرخأ ةرم ox رقنا ox.رقنا "صئاصخ"

Permissions for CRLDistribution	utionS	>
Share Permissions		
Group or user names:		
Everyone WIN-231PNBS4IPH (ABTO	OMAR\WIN-231PNI	BS4IPH\$)
	Add	Remove
Permissions for WIN-231PNBS4IPH	Allow	Deny
Full Control Change Read	\triangleleft	
OK	Cancel	Apply

7. نامألا تانوذأ نيوكتب مق ،ديدجلا دلجملا ىل CRL تافلم ةباتكب CA ل حامسلل. رقنا ،(1) بيوبتلا قمالع Securityرقنا ،(3)، رقنا ،(1) بيوبتلا تمالع Object Types(3)، رقنا . ددحو Computers ددخالا قناخ Computers ددخو

🖡 CRLDistribution Properties 🛛 💌	X 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 (RTPAAA/Users)	& Users (RTPAAA\Users)	
To change permissions click Edit		
Permissions for CBEATOB		
OW/NER Allow Deny	Add Remove	
Full control	OWNER Allow Deny	
Read & execute		
List folder contents		
Read	List folder co	/ X
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:		
Itpaaa.local	Locations	
Enter the object names to select (<u>examples</u>):	Users	
	Check Names	
Advanced	Cancel OK Cancel	

8. عجرملا مداخب صاخلا رتويبمكلا مسا لخدأ ، ديدحتل تانئاكلا ءامسأ لاخدا لقحلا يف مثيدحت متي مسالا نإف ،احلاص هلاخدا مت يذلا مسالا ناك اذا .Check Names رقناو ، قدصملا مرقنا .طخ هتحت رهظيو.

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

ققحت مث "نيمدختسملا ءامسأ" وأ "ةعومجملا" لقح يف قدصملا عجرملا رتويبمك رتخأ .9 مث ٥K رقنا .قدصملا عجرملا ىلإ لماكلا لوصولا قح حنمل لماكلا مكحتلا رفوت نم Allow رقنا .

Permissions for CRLDistributi	on	×
Security		
Object name: C:\CRLDistribution	n	
Group or user names:		
Secretaria CREATOR OWNER		
SYSTEM		
Administrators (ABTOMAR\Ad	aministrators)	
WIN-231PNBS4IPH (ABTOM	AR\WIN-231PNB	S4IPHS)
	Add	Remove
Permissions for WIN-231PNBS4IPH	Allow	Deny
Full control		□ ^
Modify		
Read & execute	\checkmark	
List folder contents	\checkmark	
Read		
OK	Cancel	Acoby
UK	Cancel	мрру

ةديدجلا CRL عيزوت ةطقن فشكل IIS يف عقوم ءاشنإ

نكمي CRL تافلم مضي يذلا ليلدلا لعجأ ،CRL تافلم ىلإ لوصولا نم ISE نيكمتل ربع هيلإ لوصولا IIS.

1. رَتخا .Administrative Tools > Internet Information Services (IIS) Manager رقنا .1

مق مث IIS مداخ مسا عيسوتب مق ،(مكحتلا ةدحو ةرجشُ مساب فورعملاً) رُسْيأْلاً ءزجلاً يف .2



3. هذه يف حضوم وه امك ،Add Virtual Directory رتخاو Default Web Site نميألا سواملا رزب رقنا. ةروصلا.

💐 Internet Information Services (IIS) Manager



تلخد ،لاثم اذه يف CRL عيزوت ةطقنل عقوم مسا لخدأ ،راعتسملا مسالا لقح يف .4 CRLD.

Add Virtual Director	у		?	×
Site name: Del Path: /	fault Web Site			
Alias:				
CRLD Example: images				
Physical path:				
C:\CRLDistribution	n			
Pass-through aut	nentication			
Connect as	Test Settings			
		OK	Cancel	

دلجملا ىلٍ ضرعتساو يلعفلا راسملا لقح نيمي ىلٍ (. . .) صقانلا عطقلا قوف رقنا .5 ةفاضاٍ ةذفان قالغإل סג رقنا .סג رقناو دلجملا ددح .1 مسقلا يف هؤاشناٍ مت يذلا يرهاظلا ليلدلا.

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	

،كلذك نكت مل اذإ .رسيألا عزجلا يف 4 ةوطخلا يف هلاخدا مت يذلا عقوملا مسا زاربإ بجي .6 اجودزم ارقن رقنا ،طسوألا عزجلا يف .نآلا هرايتخاب كيلعف Directory Browsing.

← → WIN-231PNBS4I	PH 🕨 Sites 🕨	Default Web	Site + CRLD	•		
File View Help						
Connections	CRI	LD Home	•			
V Start Page	Filter:		• 🐨 Go - 🕻	Show All	Group by:	
Application Pools Sites Sites Sites CertEnroll Sites Site	ASP	Authentic	2 Compression	Default Document	Directory Browsing	Error Pages
> 🔁 CRLD	Failed Request Tra	Handler Mappings	HTTP Redirect	HTTP Respon	Logging	MIME Types
	Modules	Output Caching	Content of the second s	SSL Settings		
	Managemer	nt				

7. ليلدلا ضارعتسإ نيكمتل Enable رقنا ،نميألا ءزجلا يف.

Internet Information Services (IIS)	Manager		×
← → 🛃 ► WIN-231PNB54	PH + Sites + Default Web Site + CRLD +	10	🗟 🔞 -
File View Help			
Connections	Directory Browsing Use this feature to specify the information that displays in a directory listing. Time Size Estension Date Long date	Alerts Directory browsing disabled. Actions Actions Apply Cancel Enable Help Help	has been

8. اجودزم ارقن رقنا ،طسوألا ءزجلا يف .ىرخأ ةرم عقوملا مسا رتخأ ،رسيألا ءزجلا يف Configuration Editor.



9. تمى اقلا يف system.webServer/security/requestFiltering. رتخأ ،"مسق" ةلدسنملا ةمئاقلا يف allowDoubleEscaping رقنا ،ىنميلا ةحوللا يف True. يف حضوم وه امك Apply، رقنا ،ىنميلا مي ةروصلا هذه.

🐚 Internet Information Services (IIS) I	nager	- 🗆 X
← → ² → WIN-231PNBS4II	Sites Default Web Site CRLD	📴 🖂 🔂 I 🔞 •
File View Help		
Connections	Section: system.webServer/security/requestFiltering • From: Default Web Site/CRLD Web.config •	Actions By Apply Ux Cancel Generate Script
Application Pools Sites Offer Default Web Site	allowDoubleEscaping True allowHighBitCharacters Irue	Configuration Search Configuration
> 💮 CertEnroll > 💮 CertSrv > 💭 CRLD	alwaysAllowedQueryStrings Faise alwaysAllowedUrls (Count=0) denyQueryStringSequences (Count=0)	Section Cock Section
I	denyUrlSequences (Count=0)	'allowDoubleEscaping'

IIS. ربع نآلا دلجملا ىلإ لوصولا بجي

عيزوتلا ةطقن ىلإ CRL تافلم رشنل Microsoft CA مداخ نيوكت

مداخ نيوكتب مق IIS، يف دلجملا ضرع متو CRL تافلم نيمضتل ديدج دلجم نيوكت دعب نآلا Microsoft CA ديدجلا عقوملا يلإ CRL تافلم رشنل

- Administrative Tools > Certificate Authority.رَتخا .Administrative Tools > Certificate Authority
- مث Properties رتخأ .قدصملا عجرملا مسا ىلع نميألا سواملا رزب رقنا ،رسيألا حوللا يف .2 يرقنا Extensions قوف رقنا ،ةديدج CRL عيزوت ةطقن ةفاضإل .بيوبتلا ةمالع Add.

Enrollment Agents	Auditina	Auditing Recovery Agents				
General	Policy Mod	lule	Exi	t Module		
Extensions	Storage		Certificate	Managers		
Select extension:					_	
CRL Distribution Point	(CDP)				1	
Specify locations from w	which users can	obtain a ce	rtificate rev	ocation list		
(CRL).						
CAMbe downa a metodo 22		well's Calla	max (CDL)	Jama C. His		
Liter CATerror	atedName>cCB	I Name Suff	ivo CN=cS	enverShort	O No	
luap.///CN=CCATIONC	ateunaniezcon	LINGING JUI	WY,CIN-CO	erver Short	1.00	
http://cServerDNSNar	me>/CertEnroll/	CaName>	CRI Name	CHIMING CLU	elt	
http:// <serverdnsnar file://<serverdnsnam< th=""><th>me>/CertEnroll/</th><th><caname>< CaName><</caname></th><th><crlname CRLName</crlname </th><th>Suffix><de< th=""><th>elt Ita</th></de<></th></serverdnsnam<></serverdnsnar 	me>/CertEnroll/	<caname>< CaName><</caname>	<crlname CRLName</crlname 	Suffix> <de< th=""><th>elt Ita</th></de<>	elt Ita	
http:// <serverdnsnar file://<serverdnsnam< th=""><th>me>/CertEnroll/ e>/CertEnroll/<</th><th><caname> CaName><</caname></th><th><crlname CRLName</crlname </th><th>Suffix><de Suffix><de< th=""><th>elt Ita</th></de<></de </th></serverdnsnam<></serverdnsnar 	me>/CertEnroll/ e>/CertEnroll/<	<caname> CaName><</caname>	<crlname CRLName</crlname 	Suffix> <de Suffix><de< th=""><th>elt Ita</th></de<></de 	elt Ita	
http:// <serverdnsnar file://<serverdnsnam< th=""><th>me>/CertEnroll/ ie>/CertEnroll/<</th><th><caname> CaName><</caname></th><th><crlname CRLNameS</crlname </th><th>Suffix><de< th=""><th>elt Ita</th></de<></th></serverdnsnam<></serverdnsnar 	me>/CertEnroll/ ie>/CertEnroll/<	<caname> CaName><</caname>	<crlname CRLNameS</crlname 	Suffix> <de< th=""><th>elt Ita</th></de<>	elt Ita	
http:// <serverdnsnar file://<serverdnsnam< td=""><td>me>/CertEnroll/ e>/CertEnroll/<</td><td><caname> CaName><</caname></td><td><crlname CRLName</crlname </td><td>Suffix><de< td=""><td>elt Ita</td></de<></td></serverdnsnam<></serverdnsnar 	me>/CertEnroll/ e>/CertEnroll/<	<caname> CaName><</caname>	<crlname CRLName</crlname 	Suffix> <de< td=""><td>elt Ita</td></de<>	elt Ita	
http:// <serverdnsnar file://<serverdnsnam< td=""><td>me>/CertEnroll/ ie>/CertEnroll/<</td><td><caname> CaName>< Ade</caname></td><td><crlname CRLName d</crlname </td><td>Suffix><de Suffix><de Remove</de </de </td><td>elt Ita</td></serverdnsnam<></serverdnsnar 	me>/CertEnroll/ ie>/CertEnroll/<	<caname> CaName>< Ade</caname>	<crlname CRLName d</crlname 	Suffix> <de Suffix><de Remove</de </de 	elt Ita	
http:// <serverdnsnam< td=""><td>me>/CertEnroll/ le>/CertEnroll/<</td><td><caname> CaName>< Add</caname></td><td><crlname CRLNameS</crlname </td><td>Suffix><de Suffix><de< td=""><td>elt Ita</td></de<></de </td></serverdnsnam<>	me>/CertEnroll/ le>/CertEnroll/<	<caname> CaName>< Add</caname>	<crlname CRLNameS</crlname 	Suffix> <de Suffix><de< td=""><td>elt Ita</td></de<></de 	elt Ita	
http:// <serverdnsnam< td=""><td>ne>/CertEnroll/ e>/CertEnroll/<</td><td><caname> CaName>< Add</caname></td><td><crlname CRLName d</crlname </td><td>Remove</td><td>elt Ita</td></serverdnsnam<>	ne>/CertEnroll/ e>/CertEnroll/<	<caname> CaName>< Add</caname>	<crlname CRLName d</crlname 	Remove	elt Ita	
 http://<serverdnsnam< li=""> Publish CRLs to this Include in all CRLs. when publishing mar </serverdnsnam<>	me>/CertEnroll/ we>/CertEnroll/<	<caname> CaName>< Add to publish i</caname>	CRLName CRLNameS	Suffix> <de Suffix><de Remove</de </de 	elt Ita	
 http://<serverdnsnam< li=""> Publish CRLs to this Include in all CRLs. when publishing mar </serverdnsnam<>	ne>/CertEnroll/ e>/CertEnroll/<	<caname> CaName>< Add to publish i</caname>	CRLName	Remove	elt Ita	
http:// <serverdnsnam< td=""><td>me>/CertEnroll/ we>/CertEnroll/< location Specifies where nually. ents use this to fi</td><td><caname> CaName>< Add to publish i nd Delta Cl</caname></td><td>CRLName CRLName d</td><td>Buffix><de Buffix><de Remove e Directory s.</de </de </td><td>elt Ita</td></serverdnsnam<>	me>/CertEnroll/ we>/CertEnroll/< location Specifies where nually. ents use this to fi	<caname> CaName>< Add to publish i nd Delta Cl</caname>	CRLName CRLName d	Buffix> <de Buffix><de Remove e Directory s.</de </de 	elt Ita	
 http://<serverdnsnam< li=""> Publish CRLs to this Include in all CRLs. when publishing mar Include in CRLs. Clie Include in the CDP et </serverdnsnam<>	me>/CertEnroll/ we>/CertEnroll/< location Specifies where nually. ents use this to fi extension of issu	<caname> CaName> Add to publish i nd Delta Cl ed certifical</caname>	<crlname CRLName d d n the Active RL location tes</crlname 	Buffix> <de Buffix><de Remove e Directory s.</de </de 	elt Ita	
http:// <serverdnsnam< td=""><td>me>/CertEnroll/ we>/CertEnroll/<</td><td>CaName> CaName> Add to publish i nd Delta Cl ed certifical</td><td>CRLName CRLName d d n the Active RL location tes</td><td>Buffix><de Buffix><de Remove</de </de </td><td>elt lta</td></serverdnsnam<>	me>/CertEnroll/ we>/CertEnroll/<	CaName> CaName> Add to publish i nd Delta Cl ed certifical	CRLName CRLName d d n the Active RL location tes	Buffix> <de Buffix><de Remove</de </de 	elt lta	
http:// <serverdnsnam file://<serverdnsnam Publish CRLs to this Include in all CRLs. when publishing man Include in CRLs. Clie Include in the CDP e</serverdnsnam </serverdnsnam 	me>/CertEnroll/ we>/CertEnroll/ location Specifies where nually. ents use this to fi extension of issue to this location	CaName> CaName> CaName> Add to publish i and Delta Cl ed certificat	CRLName CRLName d	Buffix> <de Buffix><de Remove</de </de 	elt Ita	
http:// <serverdnsnam file://<serverdnsnam Publish CRLs to this Include in all CRLs. when publishing man Include in CRLs. Clie Include in the CDP et Publish Delta CRLs for Include in the IDP et</serverdnsnam </serverdnsnam 	me>/CertEnroll/ we>/CertEnroll/ location Specifies where nually. ents use this to fi extension of issue to this location	CaName> CaName> Add to publish i and Delta Cl ed certificat	CRLName CRLName d d n the Active RL location tes	e Directory	elt ita	

يف .1 مسقلاا يف ەتكراشمو ەؤاشنإ مت يذلا دلجملا ىلإ راسملا لخدأ ،عقوملا لقح يف .3 راسملا نوكي ،1 مسقلا يفلاثملا:

\\WIN-231PNBS4IPH\CRLDistribution\$

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. 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. رتخأ ،عقوملا لقح ةئبعت عم قوف رقنا مث ريغتملا ةلدسنملا ةمئاقلا نم 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

رتخأ ،"ريغتم" ةلدسنملا ةمئاقلا نم .5 قوف رقنا مث Insert.

Add Leasting	
Add Location	\times
A location can be any valid URL or path. Enter an HTTP, LDAP, fi or enter a UNC or local path. To insert a variable into the URL or p the variable below and click Insert.	ile address, ath, select
Location:	
\\WIN-231PNBS4IPH\CRLDistribution\$\ <caname><crlnames< td=""><td>Suffix></td></crlnames<></caname>	Suffix>
Variable: <crlnamesuffix></crlnamesuffix>	Insert
Description of selected variable:	
Description of selected variable: Used in URLs and paths for the CRL Distribution Points extension	
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><c< td=""><td>RLNameSu</td></c<></caname></servername>	RLNameSu
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><c< td=""><td>RLNameSu</td></c<></caname></servername>	RLNameSu
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><c< td=""><td>RLNameSι ≻</td></c<></caname></servername>	RLNameSι ≻
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><c< td=""></c<></caname></servername>	RLNameSι ≯

:عقوملا ،لاثملا اذه يف .راسملا ةياهن crı. قاحلإب مق ،عقوملا لقح يف .6

\\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 OK

7. رايتخالl Publish CRLs to this location ةناخ ددح .تاقحلملا بيوبتلا ةمالع ىلإ OK عوجرلل رقنا صئاصخلا ةذفان قالغإل OK رقنا مث.

Active Directory. رقنا .۲es تاداهش تامدخ ليغشت ةداعإل نذإ ىلع لوصحلل ةبلاطم رهظت

Х

Enrollment Agents	Auditing	Recovery Agents	Security			
General	Policy Mo	dule Ext	t Module			
Extensions	Storage	Certificate	Managers			
Select extension:						
CRL Distribution Point	(CDP)		~			
Specify locations from	which users car	n obtain a certificate rev	ocation list			
C:\Windows\system3 Idap:///CN= <catrun http://<serverdnsna file://<serverdnsnar< th=""><th>2\C cate me ne></th><th>ion Authority You must restart Ac</th><th>tive Directory Ce</th><th>rtificate Services for the changes to</th></serverdnsnar<></serverdnsna </catrun 	2\C cate me ne>	ion Authority You must restart Ac	tive Directory Ce	rtificate Services for the changes to		
C:\Windows\system3 Idap:///CN= <catrun http://<serverdnsna file://<serverdnsnar \\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\</serverdnsnar </serverdnsna </catrun 	2\C cate me ivC ivC	tion Authority You must restart Ac take effect. Do you	tive Directory Ce want to restart th	rtificate Services for the changes to the service now?		

نم دكأت All Tasks > Publish.رَتخا .Revoked Certificates نميألا سواملا رزب رقنا ،رسيألاا ءزجلا يف .8 قوف رقنا مث ديدج CRL ديدحت OK.

🙀 certsrv - [Certification Author	ity (Local)\abtoma	r-WIN	V-231PNBS4IPH-	CA\Revoked Certificates]	
File Action View Help					
🗢 🔿 🖄 🔛 🖾					
Certification Authority (Local)	Request ID	Re	vocation Date	Effective Revocation Date	
Bevoked Certificator			The	re are no items to show in th	is vi
Ssued Certificates	All Tasks	>	Publish		
Pending Requests Failed Requests	View	>			
Certificate Templa	Refresh				
	Export List				
	Properties				
	Help				

يف هؤاشنإ مت يذلا دلجملا يف ديدج crl. فلم ءاشنإب Microsoft CA مداخ موقي نأ بجي

رقنلا دعب راوح عبرم كانه نوكي نلف ،حاجنب ديدجلا CRL فلم ءاشنإ مت اذإ .1 مسقلا لك راركتب مقف ،ةديدجلا عيزوتلا ةطقن دلجم صوصخب أطخ عاجراٍ مت اذإ ."قفاوم" قوف .ةيانعب مسقلا اذه يف ةوطخ

IIS ربع ەيلإ لوصولا ةيناكمإو CRL فلم دوجو نم ققحتلا

ىرخأ لمع ةطحم نم IIS ربع اەيلإ لوصولا ةيناكمإ نمو ةديدجلا CRL تافلم دوجو نم ققحت مسقلا اذه ءدب لبق.

اr. فلم كانه نوكي نأ بجي .1 مسقلا يف هؤاشنإ مت يذلا دلجملا حتفا ،IIS مداخ ىلع .c جذومنلا عم دوجوم دحاو

```
crl
ثيح
وه فلملا مسا ،لاثملا اذه يف .CA مداخ مسا نوكي:
```

abtomar-WIN-231PNBS4IPH-CA.crl



2. ةرادإ ةدقع لثم ةكبشلا سفن ىلع يلاثم لكشب) ةكبشلا ىلع لمع ةطحم نم ISE ةرادإ ةدقع لثم ةكبشلا سفن علي الثم الع /// ملا علي المرعتساو بيو ضرعتسم حتفا ،(قيساسألا

نىأ

ةطقنل ەرايتخإ مت يذلا عقوملا مسا وەو 2 مسقلا يف IIS مداخ مسا نيوكت متي ناونع ،لاثملا اذه يف .2 مسقلا يف عيزوتلا URL:

http://win-231pnbs4iph/CRLD

.1 ةوطخلا يف ظحالملا فلملا نمضتي يذلاو ،ليلدلا سرهف ضرعي

win-231pnbs4	iph - /crld/
To Parent Directory]	
1/28/2020 10:39 AM	979 abtomar-WIN-231PNBS4IPH-CA.crl
1/28/2020 10:39 AM	979 abtomar-WIN-231PNBS4IPH-CA.crl

ةديدجلا CRL عيزوت ةطقن مادختسال ISE نيوكت

ديدجت ةيجيتارتسإ زواجتت .CRL رشنل ينمزلا لصافلا ددح ،CRL دادرتسال ISE نيوكت لبق ةعاس نم يه (Microsoft CA يف) ةلمتحملا ميقلا .دنتسملا اذه قاطن ينمزلا لصافلا اذه ينمزلا لصافلا ديدجت درجمب .عوبسأ 1 يه ةيضارتفالا ةميقلا .ةلماش ،ةنس 411 ىل ا قدداو :ةيلاتلا تاميلعتلا مادختساب ينمزلا لصافلا نييعتب مق ،كلمع ةئيبل بسانملا

- 1. رَتخا .Administrative Tools > Certificate Authority رَتخا .Administrative Tools > Certificate Authority
- 2. قوف نميألا سواملا رزب رقنا .قدصملا عجرملا عيسوتب مق ،رسيألا ءزجلا يف Certificates رتخاو دلجمل Properties.
- .ةينمزلاا ةرتفلاا رتخاو بولطملا مقرلاا لخدأ ،CRL رشنل ينمزلاا لصافلا لوقح يف .3 ينمز لصاف نيوكت مت ،لاثملا اذه يف .رييغتلا قيبطتو ةذفانلاا قالغإل ox رقنا مايأ ةعبس ةدمل رشنلل.



4. مألا لخدأ certutil -getreg CA\Clock قميق ديكأتل *Clock قميق ديكأتل di Licertutil -getreg CA\Clock دم أل الخدأ . قاقد.

جارخإلا لاثم:

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

5. نييعت مت دق ناك *certutil -getreg CA\CRLov اذإ امم ققحتلل رمألا لخدأ مل هنأ ىلإ ريشي ام وهو ،0 يه CRLOverlapUnit ةميق نوكت يضارتفا لكشب .ايودي ةميقلا ليجستب مقف ،0 ريغ ةميق ةميقلا تناك اذإ .ةيودي ةميق يأ نييعت متي تادحولاو.

جارخإلا لاثم:

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

.6 ةوطخلا يف ەنييعت مت يذلاو ،CRLPeriod نم ققحتلل *certutil -getreg CA\CRLpe رمألا لخدأ .6

جارخإلا لاثم:

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

:يلي امك CRL حامس ةرتف باسحب مق

```
اني مت اذإ .أ CRLOverlapPeriod لخادتلا :5 ةوطخلا يف CRLOverlapPeriod نييعت مت اذإ .أ
بقﺉاقدلاب
```

قئاقدلاب ،(10 / CrlpEriod) = لخادتلاا :كلذ ريغ

720 = لخادتلا نإف 720 < لخادتلا ناك اذإ .ب

c. لخادت ا مث (1.5 * ClockSkewMinutes) الخادت ا ا مث (1.5 * ClockSkewMinutes) الخادت ا ن اك اذا (1.5 * ClockSkewMinutes)

قئاقد يف CrlpEriod = لخادت مث ،قئاقد يف ،CrlpEriod < لخادت اذإ .د

- ClockSkewMinutes لخادت = حامسال ةرتف .ه

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
```

```
ءاهتنا خيراتو يلاتال CRL رشن تقو نيب تقولا رادقم يه ةبوسحملا حامسلا ةرتف
```

ةيحالص (CRLs) لوصولا يف مكحتلا مئاوق دادرتسال ISE نيوكت مزلي .يلاحلا CRL ةيحالص (CRLs) كلذل اقفو.

8. رتخاو "يساسألا ISE لوؤسم" ةدقع ىل| لوخدلا ليجستب مقا Administration > System > Certificates. رتخأ ،ىرسيلا ةحوللا يف Trusted Certificate.

E Cisco ISE	Administration - System										
Deployment Licensing	Certificate	s Logging	Maintenance	Upgrade	Health Checks	Backup & Resto	re Admin Acce	ss Settings			Click h
Certificate Management ~ System Certificates	Trus	ted Certific	cates								
Trusted Certificates	/ Edit	+ Import 🕁 Exp	ort 👩 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 Ro	pot	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 98 EE 97 53	abtomar-WIN-231PN	abtomar-WIN-231PN	Wed, 20 Feb 2019	Sun, 20 Feb 2039	8
		Cisco ECC Root CA 201	99	Enabled	Cisco Services	03	Cisco ECC Root CA	Cisco ECC Root CA	Thu, 4 Apr 2013	Mon, 7 Sep 2099	
		Cisco Licensing Root C	A	Enabled	Cisco Services	01	Cisco Licensing Root	Cisco Licensing Root	Fri, 31 May 2013	Mon, 31 May 2038	

- يف مكحتلا مئاوق نيوكت يف بغرت يتلا CA ةداهشل ةرواجملا رايتخالا ةناخ ددح .9 يل الوصول Edit يل المل CRLs كل
- .رايتخالا ةناخ Download CRL ددح ،ةذفانلا لفسأ نم برقلاب .10
- يتلاو ،CRL عيزوت ةطقن ىلإ راسملا لخدأ ،CRL عيزوتب صاخلا URL ناونع لقح يف .11 ناونع ،لاثملا اذه يف .2 مسقلا يف هؤاشنإ مت يذلا ،crl. فلم نمضتت

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

- ءاەتنا ىلإ ادانتسا وأ ةمظتنم ةينمز تارتف ىلع CRL دادرتسال ISE نيوكت نكمي .12 لصافلا نوكي امدنع .(مظتنم ينمز لصاف ،ةماع ةفصب ،اضيأ وه يذلا) ةيحالصلا مادختسإ دنع ةمءالم رثكأ CRL تاثيدحت ىلع لوصحلا متي ،اتباث CRL رشنل ينمزلا .رايتخالا Automatically رز رقنا .ريخألاا رايخلا
- .7 ةوطخلاا يف ةبوسحملا حامسلا ةرتف نم لقأ ةميق ىلإ دادرتسالا ةميق نييعتب مق .13 عيزوت ةطقن نم ققحتي ISE نإف ،حامسلا ةرتف نم لوطأ ةميقلا ةعومجم تناك اذإ ىلع حامسلا ةرتف باسح متي ،لاثملا اذه يف .ةيلاتلا CRL رشنب CA موقي نأ لبق دادرتسالل تاعاس 10 ةميق مادختسإ متيس .قئاقد 10 و ةعاس 12 وأ ،ةقيقد 730 اهنأ
- ا ىلع رذعت اذإ .كتئيبل بسانم ەنأ ىلع ةلواحملا ةداعإل ينمزلا لصافلا نييعت .14 ةوطخلا يف اەنيوكت مت يتلا ةرتفلا يف (CRL) لوصولا يف مكحتلا ةمئاق دادرتسإ رصقألا ةرتفلا ەذە يف ةلواحملا ديعيسف ،ةقباسلا
- ا عن المعروة عن العن المعروة ال Bypass CRL Verification if CRL is not Received قناخ ددح 5. دادرتسإ نم ISE نكمتي مل اذإ (CRL صحف نودو) يعيبط لكشب ةعباتملاب ةداهشلا رايتخالا ةناخ ديدحت مدع ةلاح يف .ةريخألا ليزنتلاا ةلواحم يف قدصملا عجرملا اذهل CRL اهرادصإ مت يتلا تاداهشلا عم ةداهشلا ىل المن الملاء قلام من الما قلام من الما الما الما (CRL) لوصولا يف مكحتلا ةمئاق دادرتسإ رذعت قلاح يف اذه قدصملا عجرملا لبق
- 16. تافلم مادختساب ISE ل حامسلل رايتخالا Ignore that CRL is not yet valid or expired قناخ ددح Sec متناف دوج قحلاص ريغ وأ) قيحالصلا قيەتنم قناخ ديدحت متي مل اذإ .ةحيحص تناك ول امك (دعب قحلاص ريغ وأ) قيحالصلا قيەتنم خيرات لبق قحلاص ريغ (CRL) لوصولا يف مكحتلا قمئاق ربتعي ISE ناف ،هذه رايتخالا لامكإل save رقنا .مهب قصاخلا قيلاتلا ثيدحتلا تاقوأ دعبو مهب صاخلا نايرسلا .نيوكتلا

Certificate Status Validation									
	To verify certificates, enable the methods below. If both are enabled, OCSP will always be tried first. OCSP Configuration Validate against OCSP Service Reject the request if OCSP returns UNKNOWN status Reject the request if OCSP Responder is unreachable Certificate Revocation List Configuration Validate Revocation List Configuration Validate OCEN								
	CRL Distribution URL	http://win-231	pnbs4iph/crld/a	abtomar-WIN-231	PNBS4IPH-CA.c	rl			
	Retrieve CRL	 Automatically Every 	10 1		Hours		 ✓ before expiration. ✓ 		
	If download failed, wait	10		Minutes		 before retry 	I.		
	Enable Server Iden Bypass CRL Verific Ignore that CRL is	atity Check () ation if CRL is not not yet valid or ex	Received						

ةحصلا نم ققحتلا

نيوكتلا اذه ةحص نم ققحتلل ءارجإ أَيلاح دجوي ال.

اهحالصإو ءاطخألا فاشكتسا

نيوكتلا اذهل امحالصإو ءاطخألا فاشكتسال ةددحم تامولعم أًيلاح رفوتت ال.

ةمجرتاا مذه لوح

تمجرت Cisco تايان تايانق تال نم قعومجم مادختساب دنتسمل اذه Cisco تمجرت ملاعل العامي عيمج يف نيم دختسمل لمعد يوتحم ميدقت لقيرشبل و امك ققيقد نوكت نل قيل قمجرت لضفاً نأ قظعالم يجرُي .قصاخل امهتغلب Cisco ياخت .فرتحم مجرتم اممدقي يتل القيفارت عال قمجرت اعم ل احل اوه يل إ أم اد عوجرل اب يصوُتو تامجرت الاذة ققد نع اهتي لوئسم Systems الما يا إ أم الا عنه يل الان الانتيام الال الانتيال الانت الما