# EAP-TLS وأ PEAP ل APs ىلع 802.1X تلكش LSC عم

### تايوتحملا

<u>قمدق مل ا</u>
<u>قي س اس أل ا ت ابل طت مل ا</u>
<u>تابل طتمل ا</u>
<u>قمدختس مل اتان وكمل ا</u>
<u>قي س اس أ ت امول عم</u>
<u>قكېشلل يطيطختلا مسرلا</u>
<u>ىنىوكەتلا</u>
Windows Server 2016 SCEP CA
<u>اەل.يچس.تو قداەش.ل.ا ب.ل.اق نىيوكت</u>
<u>LSC دارع S800 نوروكت</u>
<u>AP LSC ل (GUI) ةيموس ل ا مدخت مل ا ةمجاو نيوكت تاوطخ</u>
<u>AP LSC ل (CLI) رماوأل ا رطس ةمچاو نېوكت تاوطخ</u>
AP LSC نم قاقرحتا ا
<u>امحال صاو LSC دادعا ءاطخأ فاشكتس أ</u>
<u>LSC مادختس اب 802.1X قق داصم قېكل س ل ا ل وصول ا قطق ن</u>
<u>ل.وص.ول.ا قطق.نل قيكل.س.ل.ا 802.1x قق.داصم ني.وكت تاوطخ</u>
<u>802.1x ققداصمل (GUI) قيموس رل المدخت سمل القمجاو نيوكت قيكل سل الروصول القطق ن</u>
<u>ل.يكشت CLI ةيوه ةحص AP Wired 802.1x</u>
<u>لى،كشت جاتفم قېوه قحص 802.1x يكل،س ap</u>
RADIUS مداخ قداهش تېپېثت
<u>قيكل سلام 802.1x قوداصم نم قرقرحتايا :لوصول قطقن</u>
<u>امحال،صاو 802.1X ةقداصم ءاطخأ فاشكتسأ</u>

### ەمدقملا

مه ىلع ةطقن ذفنم cisco قداصي نأ فيك ةقيثو اذه فصي cisco مه ىلع ةطقن ذفنم عالي عنا فيك المعتسي EAP-TLS وأ

ةيساسألا تابلطتملا

تابلطتملا

:ةيلاتا عيضاوملاب ةفرعم كيدل نوكت نأب Cisco يصوت

ةيكلساللا مكحتلا ةدحو •

- لوصولا ةطقن •
- ليدبت •
- ISE مداخ •
- . ةداەشلا حنم ةەج •

#### ةمدختسملا تانوكملا

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

- 17.09.02 رادصإلاا لغشت يتلا C9800-40-K9 :ةيكلساللا مكحتلا ةدحو
- C9117AXI-D :لوصولاا ةطقن
- 17.06.04 ضڬري C9200L-24P-4G لوحملا
- مداخ AAA: ISE-VM-K9 لغشي يذلا 3.1.0.518 م
- تداەشلا حنم قەج: Windows Server 2016

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

# ةيساسأ تامولعم

اهنإف ،802.1X مادختساب اهب صاخلا switchport عم قداصت نأ (APs) لوصولا طاقن تدرأ اذإ لا تنأ ديري نإ .تاداهش بلطتي ال يذلا EAP-FAST ققداصم لوكوتورب ايضارتفا مدختست ريغ بناج ap لا ىلع تاغوسم لمعتسي يأ) ققيرط PEAP-MSCHAPV2 لا لمعتسي نأ APs تنأ ،(بناج الك ىلع قداهش لمعتسي يأ) ققيرط EAP-TLS لا وأ (بناج RADIUS لا ىلع قداهش قطقن ىلع رذج/اهب قوثوم قداهش ريفوتل قديحولا ققيرطلا يهو .الوأ SAC لكشي نأ رطضي لهاجتو PEAP ءارج لوصول قطقنل نكمي ال .(EAP-TLS قلاح يف زاهج قداهش كلذكو) لوصو

ددحتو ،(CA) صيخرتلاا عجرم يف مكحتو ،لضفأ نيمأت PKI رفوت نأ ديرت تنك اذإ LSC مدختسأ اهؤاشنإ مت يتلا تاداهشلا ىلع تامادختسالاو ،دويقلاو ،تاسايسلا

لوصولاا ةطقن لصتت ال .CA نع ةرداص ةداەش ىلع مكحتلا زاەج لصحي ،LSC مادختساب (WLC) ةيكلساللا ةيلحملا ةكبشلا يف مكحتلا ةدحو بلطتت نكلو CA مداخب ةرشابم ىلوصولا طاقن نع قباين تاداەش اەيلإ لوصولا بچيو مكحتلا ةدحو.

تابلطلا هيجوت ةداعإل (SCEP) طيسبلا ةداهشلا ليجست لوكوتورب مكحتلا ةدحو مدختست تاداهشلا ىلع لوصحلل ىرخأ ةرم SCEP مدختستو CA ىلا ةزهجألا ىلع اهؤاشنا مت يتلا نم ةعقوملا

ةداهشلا ليجست معدل CA مداوخو PKI ءالمع همدختسي تاداهش ةرادإ لوكوتورب وه SCEP يف عساو قاطن ىلع مدختسم وهو .اهلاطبإو لوكوتورب نم يساسألا فدهلا. PKI لئاسرل لقن لوكوتوربك HTTP مادختسإ متي SCEP، SCEP، لقام ياسال المالا فدهلا.

ةكبشلل يطيطختلا مسرلا



### نيوكتلا

.SCEP CA و SCEP CA :يساسأ لكشب نيوكتلل نارمأ كانه

#### Windows Server 2016 SCEP CA

لوصولا ةطقنل ةيساسأ تيبثت ةيلمع دنتسملا اذه يطغي Windows Server لوصولا ةطقنل ةيساسأ تيبثت ةيلمع دنتسملا اذه يطغي بسانمو نمآ لكشب جاتنإلا ةئف نم يلعفلا Windows CA نيوكت بجي .ةيلمعم ضارغأل نأ نع الضف ربتخملا يف وه ربتخت تنأ دعاسي نأ مسق اذه فدهي .ليغشتلا تايلمعل : تاوطخلا يه هذه .لمعي ليكشت اذه لعجي نأ ةبولطملا تادادعإلا نم مهلتسي

.ةديدج Windows Server 2016 بتكم حطس ةبرجت تيبثتب مق.1 ةوطخلا

.تباث IP ناونع مادختساب مداخلا نيوكت نم دكأت .2 ةوطخلا

DNS. مداخو Active Directory ةمدخ لاجم تامدخب أدبا ،نيديدج ةمدخو رود ليغشت ءدب .3 ةوطخلا

👝 Se	rver Manager			– 0 ×
	🚵 Add Roles and Features Wizard		- 🗆 ×	age Tools View Help
Ī	Select server roles		DESTINATION SERVER WIN-3E202T1QD0U	
ī	Before You Begin	Select one or more roles to install on the selected server.		
	Installation Type	Roles	Description	
Ϊĝ	Server Selection Server Roles Features DNS Server AD DS Confirmation Results	<ul> <li>Active Directory Certificate Services</li> <li>Active Directory Domain Services</li> <li>Active Directory Federation Services</li> <li>Active Directory Lightweight Directory Services</li> <li>Active Directory Rights Management Services</li> <li>Device Health Attestation</li> <li>DHCP Server</li> <li>Fax Server</li> <li>Pile and Storage Services (1 of 12 installed)</li> <li>Host Guardian Services</li> <li>Network Policy and Access Services</li> <li>Print and Document Services</li> <li>Remote Access</li> <li>Remote Desktop Services</li> <li>Volume Activation Services</li> <li>Web Server (IIS)</li> <li>Windows Deployment Services</li> </ul>	Active Directory Domain Services (AD DS) stores information about objects on the network and makes this information available to users and network administrators. AD DS uses domain controllers to give network users access to permitted resources anywhere on the network through a single logon process.	Hide
er a		< Previous Next	> Install Cancel	
		Events 1 Events Performance 5 Service	es la	_
		BPA results Perfor BPA re	mance esults	
L			111117/1012 1126 AM	

Active Directory تيبثت

🚖 S	erver Manager								- 0	×
	ᡖ Add Roles and Features Wizard	3		-		×	age	Tools	View	Help
111	Installation progr	ress		DESTINA WIN-3	TION SER	VER DOU				^
i	Before You Begin	View installation progress								
	Installation Type	i Feature installation								
i	Server Selection		1.1							
Ē	Server Roles	Configuration required. Installation su	cceeded on WIN-3E2O211QD00.							
	Features	Active Directory Domain Services	is machine a domain controller			^				
	DNS Server	Promote this server to a domain control	ler							
	Confirmation	DNS Server								
	Results	Group Policy Management								
		Remote Server Administration Tools Role Administration Tools								
		DNS Server Tools							Hid	e
		AD DS and AD LDS Tools	Windows DowerShall							
		AD DS Tools	Wildows PowerShell			~				
		You can close this wizard without interpage again by clicking Notifications in Export configuration settings	rrupting running tasks. View task pro n the command bar, and then Task D	ogress or o etails.	open thi	5				
		< Pr	evious Next > Cla	ose	Cance	el				
		Events	Events				_			
		Services	Services							
		Performance	Performance							
		BPA results	BPA results							
										~

AD تيبثت ءاەتنا

#### ةدحو ىلإ مداخلا اذه ةيقرتب ةصاخلا تامولعملا ةحول قوف رقنا ،ءاهتنالا درجمب .4 ةوطخلا لا جمل اب مكّحت.

🚘 Server Manager			– 0 ×
Server M	lanager • Dashboard	• ©   🍢	Manage Tools View Help
📰 Dashboard	WELCOME TO SERVER MANAGE	Post-deployment Configuration     Configuration required for Active Directory Domain	
Local Server     All Servers	1 0	Services at WIN-3E202T1QD0U Promote this server to a domain controller	
DNS	QUICK START	i Feature installation	
File and Storage Services	3	Configuration required. Installation succeeded on WIN-3E2O2T1QD0U. Add Roles and Features	
	WHAT'S NEW 4	Task Details	
	5	Connect this service to cloud services	

AD تامدخ نيوكت

لاجم مسا رتخاو ةديدج ةباغ ءاشنإب مق .5 ةوطخلا.

æ	Server	Mana	ader
h and	oci vei	TADALLA	agei

(	🚡 Active Directory Domain Services	Configuration Wizard		- 🗆 ×
	Active Directory Domain Services  Deployment Configuration  Domain Controller Options  Additional Options  Paths  Review Options  Prerequisites Check  Installation Results	Configuration Wizard Guration Select the deployment opera Add a domain controller Add a new domain to an Add a new forest Specify the domain informat Root domain name:	ation to an existing domain existing forest ion for this operation mydomain.loca	- C X
		More about deployment cor	figurations          < Previous       Next >         Events	Install

ةباغ مسا رايتخإ

### مداخلا ىلإ تاداەشلا تامدخ رود فضأ .6 ةوطخلا:

🚖 Server Manager						-	- ć	) ×
Ser	ver Manager • Das	hboard	• ③	I 🗗	Manage	Tools	View	Help
<ul> <li>Dashboard</li> <li>Local Server</li> </ul>	WELCOME TO SEE	RVER MANAGER						
All Servers	📥 Add Roles and Features Wizard				-		х	
DNS	Select server role	s		WIN	DESTIN -3E2O2T1QD0U.r	ATION SERV nydomain.lo	'ER cal	
■ File and Storage Ser	Before You Begin Installation Type Server Selection Server Roles Features AD CS Role Services Confirmation	Select one or more roles to install on the selected server. Roles   Active Directory Certificate Services  Active Directory Domain Services (Installed)  Active Directory Lightweight Directory Services  Active Directory Rights Management Services Device Health Attestation DHCP Server  DNS Server (Installed)	^	Descripti Active Dir (AD CS) is certificati role servi and mana variety of	on rectory Certific sused to creat on authorities ces that allow age certificates applications.	ate Service e and relate you to issu used in a	e d e -	de

تاداەش تامدخ ةڧاضإ



طقف قدصملا عجرملا ةفاضإ

#### .كب صاخلا قدصملا عجرملا نيوكتب مق ،ءاەتنالا درجمب .7 ةوطخلا

🚖 Server	Manager					-	ð X
$\mathbf{E}$	AD CS Configuration		-	■	age Too	ols Viev	w Help
III Loc III Loc III All III AD III AD III AD III File	Role Services Credentials Role Services Setup Type CA Type Private Key Cryptography CA Name Validity Period Certificate Database Confirmation Progress Results	Select Role Services to configure Certification Authority Certification Authority Web Enrollment Online Responder Network Device Enrollment Service Certificate Enrollment Web Service Certificate Enrollment Policy Web Service	DESTINATION WIN-3E2O2TIQD0U.mydon	N SERVER main.local	DESTINATION QDOU.mydom	I SERVER nain.local	ide
		< Previous	Next > Configure	Cancel			
					ess or open	this	

Enterprise CA. رتخأ 8. ةوطخلا



ةسسؤملل قدصم عجرم

.LSC ل ةعباتلا CAs معد متي ،Cisco IOS XE 17.6 ذنم .رذجلا قدصملا عجرملا هلعجأ .9 ةوطخلا



يرذج قدصم عجرم رايتخإ

ةعومجم نم اءزج قدصملا عجرملا نوكي يكل ەمدختست يذلا باسحلا كيدل نوكي نأ مەملا نم IIS\_IUSRS. قمئاقلا ىلإ لاقتنال او Administrator باسح مادختسإ كنكمي ،لاثملا اذه يف Directory Users and Computers اقعومجم ىلإ نيلوؤسملا نيمدختسملا قفاضإل

📤 Server Manag	ger							- 0	$\times$
$\odot$	Server Manag	er • Dashbo	ard			• @   P	Manage 1 3	ools View	Help
<ul> <li>Dashbc</li> <li>Local Se</li> <li>All Serv</li> <li>AD CS</li> <li>AD DS</li> <li>DNS</li> <li>File and</li> <li>IIS</li> </ul>	Active Directory Users and File Action View Help Active Directory Users and ( Active Directory Users and ( Saved Queries Saved Queries Computers Domain Local Builtin Computers Domain Controllers Computers Managed Service Action Users	Administrator Properti Remote control General Address Member Of Member of: Name Administrators Domain Admins Domain Users Enterprise Admins Group Policy Cre IIS_IUSRS Schema Admins Primary group: Do Set Primary Group OH BPA results	es           Remote Desktop           Account         Profile           Dial-in         E           Active Directory Dommin Jocal/Usern         mydomain Jocal/Usern           mydomain Jocal/Usern         mydomain Jocal/Usern           Remove         There is no need t           you have Macinto applications.         applications.	Services Profile Telephones rvironment ain Services Folder a b b b c c change Primary of sh clients or POSIX sh clients or POSIX < Previous BPA res	? × COM+ Organization Sessions	Configure	Cancel	Hide	
م 🖿	o 🤅 📄 🖡	-					^ 🔂 🕼	ENG 10:47 PM BEFR 10/19/2023	, 1

IIS\_USER ةعومجم ىلإ كب صاخلا لوؤسملا باسح ةفاضإ

راودألاا ةفاضإب مق ،ةحيحصلا IIS ةعومجم يف مدختسم كيدل نوكي نأ درجمب .10 ةوطخلا كب صاخلا قيدصتلا عجرم ىلإ NDES و Online Responder تامدخ فضأ مث .تامدخلاو.

đ ×



تنرتنإلا ربع بيجتسملا تامدخو NDES تيبثت

تامدخلا هذه نيوكتب مق ،كلذب مايقلا درجمب .11 ةوطخلا.



NDES و NDES قمدخ تيبثت

ىلٍ لبق نم ەتفضأ يذلا باسحلا وە اذە .ةمدخ باسح رايتخاب كتبلاطم متت .12 ةوطخلا قعومجم IIS\_IUSRS.



IIS ةعومجم ىلإ ەتڧضأ يذلا مدختسملا ءاقتنا

تايلمعل يفكي اذه.13 ةوطخلا SCEP، تيبثت اضيأ كمزلي ،802.1X قوطخلا ىتح ةلوەسب اەنيوكتو بيولا ليجست ةمدخ تيبثتب مق ،كلذل .RADIUS مداخ ىلع قداەش مداخ ىلع ISE قداەش بلط قصلو خسن نم نكمتت



بيولا ليجست ةمدخ تيبثت

AD CS Configuration		– 🗆 X
Role Services		DESTINATION SERVER WIN-3E2O2T1QD0U.mydomain.local
Credentials Role Services Confirmation Progress Results	<ul> <li>Select Role Services to configure</li> <li>Certification Authority</li> <li>Certification Authority Web Enrollment</li> <li>Online Responder</li> <li>Network Device Enrollment Service</li> <li>Certificate Enrollment Web Service</li> <li>Certificate Enrollment Policy Web Service</li> </ul>	
	< Previous	Next > Configure Cancel

بيولا ليجست ةمدخ نيوكت

ةرايز لالخ نم حيحص لكشب SCEP ةمدخ ليغشت نم ققحتلا كنكمي .14 ةوطخلا http://<serverify>/certsrv/mscep/mscep.dll :



SCEP لخدم نم ققحتلا

.15 ةوطخلا

تابلط ةقداصمل "يكيمانيد يدحت" رورم ةملك Windows مداخ مدختسأ ،يضارتفا لكشبو باسح اذه بلطتي .(Microsoft SCEP (MSCEP لخاد ليجستلا لبق ةياهنلا ةطقنو ليمعلا بسح رورم ةملك ءاشنإل بيولل (GUI) ةيموسرلا مدختسملا ةهجاو ىلإ حفصتلل لوؤسم نيمضت مكحتلا ةدحو ىلع رذعتي.(بلطلا نمض رورملا ةملك نيمضت بجي) بلط لكل بلطلا ليدعت مزلي ،ةزيملا هذه ةلازال .مداخلا ىل اهلسرت يتلا تابلطلا نمض هذه رورملا ةملك NDES:

Start. ةمئاقلاا نمض Regedit نع ثحبا ،"ليجستلا ررحم" حتفا

رتويبمكلا ىلإ لقتنا HKEY\_LOCAL\_MACHINE < جمانرب Microsoft < ريفشت MSCEP < Stressword < Stressword

يه امك اهكرتاف ،لعفلاب 0 تناك اذإ .0 ىلإ EnforcementPassword ةميق رييغتب مق

₫ <b></b>		Registry Editor		_ 🗆 🗙
File Edit View Favorites Help				
- MSCEP	^	Name	Туре	Data
— 📜 САТуре		(Default)	REG SZ	(value not set)
CertsInMYStore		88 EnforcePassword	REG_DWORD	0x00000000 (0)
		, - <u>4</u>		
PasswordVDir				
UseSinglePassword				
- OID	Ξ			
- Protect	-			
- Providers				
CTE				
DataAccess				
DevDiv				
Device Association Framework				N
Dfra				43
DFS				
DHCPMibAgent				
DirectDraw				
DirectInput				
DirectPlay8				
DirectPlayNATHelp	$\sim$			
< III >		<	III	>
Computer\HKEY_LOCAL_MACHINE\	SOFT	WARE\Microsoft\Crypt	ography\MSCEP\Enfor	cePassword

ديدحتلا ضرف ةملك ةميق نييعت

#### اەليجستو ةداەشلا بلاق نيوكت

ضارغأل ةددعتم تاهويرانيس يف اهب ةنرتقملا حيتافمل او تاداهشلا مادختسا نكمي جهن نيزخت متي .قدصملا عجرملا مداخ لخاد قيبطتلا جهن ةطساوب اهديدحت مت ةفلتخم لقحلا اذه ليلحت متي .قداهشلل "(EKU) عسوملا حاتفملا مادختسا" لقح يف قيبطتلا نم دكأتلل .هنم دوصقملا ضرغلل ليمعلا لبق نم همادختسا نم ققحتلل قدصملا ةطساوب بسانملا قداهشلا بلاق ءاشناب مق AP، و WLC تاداهشل قبسانملا قي محتل قي عرد مقو

.قدصملا عجرملا < ةيرادإ تاودأ < أدبا ىلإ لقتنا .1 ةوطخلا

قوف نميألا سواملا رزب رقنا ،قدصملا عجرملا مداخ دلجم ةرجش عيسوتب مق .2 ةوطخلا ةرادإ ددحو صيخرتلا بلاوق تادلجم.

يف بلاقلا راركت ددح مث ،نيمدختسملا ةداهش بلاق قوف نميألا سواملا رزب رقنا .3 ةوطخلا قايسلا ةمئاق.

بسح ةيحالصلا ةرتفو بلاقلا مسا رييغتب مقو ،ماع بيوبتلا ةمالع ىلإ لقتنا .4 ةوطخلا

رذج ةداهش ةيحالص نم ربكاً تسيل اهناً نم دكاًت ،ةيحالصلا ةرتف ليدعت دنع :ريذحت 🗥 قدصملا عجرملا.

# Properties of New Template

Х

Subject Name	Sen	ver	Issuance R	equirements				
Superseded Templa	tes	Exte	nsions	Security				
Compatibility General	Request	Handling	Cryptography	Key Attestation				
Template display name: 9800-LSC								
Template name: 9800-LSC								
Validity period: 2 years  4 6 weeks  4								
Publish certificate in Active Directory           Do not automatically reenroll if a duplicate certificate exists in Active Directory								
OK		Cancel	Apply	Help				

ببلطلا يف ديروتلا ديدحت نم دكأتو ،عوضوملا مسا بيوبتلا ةمالع ىلإ لقتنا .5 ةوطخلا. ىلع لوصحلل لوؤسملا ةقفاومل نوجاتحي ال نيمدختسملا نأ ىلإ ريشي قثبنم نأ ودبي قفاوم ددح ،ةداهشلا ىلع مەعيقوت.

Properties of New Template							
Compatibility General Request Handling Cryptography Key Attestation							
Superseded Templa	tes	Exte	nsions	Security			
Subject Name	Sen	ver	Issuance Re	equirements			
Use subject information from existing certificates for autoenrollment renewal requests (*)							
O Build from this Active Directory information							
Select this option to e simplify certificate add	enforce co ministratior	Select this option to enforce consistency among subject names and to simplify certificate administration.					

بلطلا يف ديروتلا

رزلا ددحو تاقيبطتلا جەن رايخ ددح مث ،تاقحلملا بيوبتلا ةمالع ىلإ لقتنا .6 ةوطخلا ةفاضإ ددح ،الإو ،قيبطتلا تاسايس ةذفان يف ةدوجوم ليمعلا ةقداصم نأ نم دكأت ....ريرحت ەفضأو

Properties of New Template						X		
Compatibility	General	Request	Request Handling Cryptography Key Attestation					
Subject N	lame	Ser	ver	Issuance	Requirements			
Supersec	ded Templa	tes	Exte	nsions	Security			
To modify an	n extension,	, select it,	and then c	lick Edit.				
Extensions in Applicati	Extensions included in this template: Application Policies							
Edit Application Policies Extension								
An application policy defines how a certificate can be used.								
Application policies: Client Authentication Encrypting File System Secure Email								

تاقحلملا نم ققحتلا

نم 6 ةوطخلا يف ددحملا ةمدخلا باسح نأ نم دكأتو ،نامأ بيوبتلا ةمالع ىلإ لقتنا .7 ةوطخلا مث ،بلاقلاب ةصاخلا لماكلا مكحتلا تانوذأ هيدل Windows Server يف SCEP تامدخ نيكمت قفاومو قيبطت ددح.

# Properties of New Template

X

Subject I	Jame	Server	.um ig	Issuance R	equirements	
Superse	ded Templa	tes	Exte	nsions	Security	
Superseded Templates Extensions						
Group or user names:						
Authen	ticated Use	18				
A Domain	stator Admine (C	HILLDOMAI	1\Dom	ain Admine)		
St. Domain	Users (CH	UU-DOMAIN	Domai	n Users)		
St Enterpr	ise Admins	(CHUU-DOM	AIN\En	terprise Admins)		
				Add	Remove	
					_	
Permissions	for Adminis	trator		Allow	Deny	
Permissions Full Contro	for Administ ol	trator		Allow	Deny	
Full Contro Read	for Administ ol	trator		Allow	Deny	
Permissions Full Contro Read Write	for Administ	trator		Allow	Deny	
Permissions Full Contro Read Write Enroll	for Administ	trator		Allow	Deny	
Permissions Full Contro Read Write Enroll Autoenrol	for Administ ol	trator		Allow	Deny	
Permissions Full Contro Read Write Enroll Autoenrol	for Administ	trator		Allow	Deny	
Permissions Full Contro Read Write Enroll Autoenrol	for Administ	trator		Allow V V V V	Deny	
Permissions Full Contro Read Write Enroll Autoenrol	for Administ ol	or advanced	settings	Allow	Deny	
Permissions Full Contro Read Write Enroll Autoenrol	for Administ ol	or advanced	settings	Allow	Deny	
Permissions Full Contro Read Write Enroll Autoenrol	for Administ	or advanced	settings	Allow	Deny	
Permissions Full Contro Read Write Enroll Autoenrol	for Administ	or advanced	settings	Allow	Deny	

لماكلا مكحتلا حنم

بلاوق دلجملا يف نميألا سواملا رزب رقناو ،قدصملا عجرملا ةذفان ىلإ عجرا .8 ةوطخلا ەرادصإ دارملا ةداەشلا بلاق < ديدج ددحو ةداەشلا.

.قفاوم ددحو ،LSC-1800 لاثملا اذه يف ،اقبسم هؤاشنإ مت يذلا ةداهشلا بلاق ددح .9 ةوطخلا

يف جاردإلل لوطأ اتقو اثيدح هؤاشنإ مت يذلا ةداهشلا بلاق قرغتسي نأ نكمي :ةظحالم مداوخلا ةفاك ىلع لثامتملا خسنلا ىلإ جاتحي هنأل ةددعتم مداوخ رشن تايلمع.

Select one Certificate Template to Note: If a certificate template that information about this template has All of the certificate templates in th For more information, see <u>Cert</u>	Enable Certificate Templates enable on this Certification Authority. was recently created does not appear on this list, you may need to wait us been replicated to all domain controllers. e organization may not be available to your CA. <u>ifficate Template Concepts.</u>	nti
Name	Intended Purpose	^
@ 9800-LSC	Client Authentication, Secure Email, Encrypting File System	
R CA Exchange	Private Key Archival	
Code Signing	Code Signing	=
Cross Certification Authority	<al></al>	
Enrollment Agent	Certificate Request Agent	
Renrollment Agent (Computer)	Certificate Request Agent	
Rechange Signature Only	Secure Email	
R Exchange User	Secure Email	
IPSec	IP security IKE intermediate	
Key Recovery Agent	Key Recovery Agent	_
OCSP Response Signing	OCSP Signing	~
	ОК	Cancel

بلاقلا رايتخإ

تاداەشلا بلاوق دلجم ىوتحم نمض نآلا دىدجلا ةداەشلا بلاق درس متي.

🧔 certsrv - [Cer	tification Authority (Local)\CHUU-WIN	V12-CA\Certificate Templates]	x
File Action View Help			
🗢 🏟 🙎 🙆 🔒 📓			
Certification Authority (Local)  CHUU-WIN12-CA  Revoked Certificates  Pending Requests Failed Requests Certificate Templates	Name 9800-LSC Authenticated Session Exchange Enrollment Agent (Offline r IPSec (Offline request) CEP Encryption Directory Email Replication Domain Controller Authentication Kerberos Authentication EFS Recovery Agent Basic EFS Domain Controller Web Server Computer User Subordinate Certification Authority Administrator	Intended Purpose Client Authentication, Secure Email, En Client Authentication Certificate Request Agent IP security IKE intermediate Certificate Request Agent Directory Service Email Replication Client Authentication, Server Authentic Client Authentication, Server Authentic File Recovery Encrypting File System Client Authentication, Server Authentic Server Authentication Client Authentication Client Authentication Client Authentication, Server Authentic Server Authentication Client Authentication, Server Authentic Encrypting File System, Secure Email, Cl <all></all>	

LSC ددح

الق تناو لجسلا ررحم ةذف ان يل عجرا .10 ةوطخل Computer > HKEY\_LOCAL\_MACHINE > Software > Microsoft > Cryptography > MSCEP.

وطخلا EncryptionTemplate و EncryptionTemplate تالجس ريرحتب مق 11. ةوطخلا اثيدح مؤاشنإ مت يذلا ةداهشلا بلاق ىلإ ريشت ثيحب SignatureTemplate

<u>گ</u>	Registry Editor		_ 🗆 🗙
File Edit View Favorites Help			
File       Edit       View       Favorites       Help         Image: Provider source       Image: Provider source       Image: Provider source       Image: Provider source         Image: Provider source       Image: Provider source       Image: Provider source       Image: Provider source         Image: Provider source       Image: Provider source       Image: Provider source       Image: Provider source         Image: Provider source       Image: Provider source       Image: Provider source       Image: Provider source         Image: Provider source       Image: Provider source       Image: Provider source       Image: Provider source         Image: Provider source       Image: Provider source       Image: Provider source       Image: Provider source         Image: Provider source       Image: Provider source       Image: Provider source       Image: Provider source         Image: Provider source       Image: Provider source       Image: Provider source       Image: Provider source         Image: Provider source       Image: Provider source       Image: Provider source       Image: Provider source         Image: Provider source       Image: Provider source       Image: Provider source       Image: Provider source         Image: Provider source       Image: Provider source       Image: Provider source       Image: Provider source         Image: Pro	Name (Default) (Defa	Type REG_SZ REG_SZ REG_SZ REG_SZ	Data (value not set) 9800-LSC 9800-LSC 9800-LSC
< <p>DirectInput</p>	<	III.	>
Computer\HKEY_LOCAL_MACHINE\SOFT	WARE\Microsoft\Crypto	ography\MSCEP	

لجسلا يف بلاقلا رييغت

مداخ ليغشت دعأ .12 ةوطخلا ،مداخلا مسا ددحو ،قدصملا عجرملا ةذفان ىلإ عجرا كلذل ،NDES مداخ ليغشت دعأ .12 ةوطخلا حاجنب ليغشتو فاقيإ رز ددحو.

<b>b</b>	certsrv - [Certification Authority (Local)\CHUU-WIN12-CA]	_ 🗆 🗙
File     Action     View     Help       Image: Constraint of the second seco	▶ ■	
Certification Authority (Local)	Name Revoked Certificates Sued Certificates Pending Requests Failed Requests Certificate Templates	

### 9800 ىلع LSC نيوكت

.WLC يف ap ل LSC لكشي ل لسلست يف steps لا انه

- ا. التعالي التعالي التعالي التعامي الذي مادختسا متي .RSA حاتفم ءاشنإب مق .PKI TrustPoint
- .ەؤاشنإ مت يذلا RSA حاتفم نييعتو ةقث ةطقن ءاشنإب مق .2
- 3. نييعتو لوصولاطاقنل LSC دادعإ نيكمتب مق
  - .ةمضنملا لوصولا طاقن عيمجل LSC نيكمتب مق .1
  - .ريفوتلا ةمئاق ربع ةددحملا لوصولا طاقنل LSC نيكمت .2
- .LSC ةقث ةطقن ىلإ رشأو ةيكلساللا ةرادإلا ةقث ةطقن رييغتب مق .4

#### AP LSC ل (GUI) ةيموسرلا مدختسملا ةهجاو نيوكت تاوطخ

.حيتافملا جوز ءاشنإ < PKI ةرادإ < نامألا < نيوكتلا ىلإ لقتنا .1 ةوطخلا

- .بسانم مسا هيطعيو فيضي ةقطقط .1
- .RSA حاتفم مجح ةفاضإب مق .2
- ريدصت ديرت تنك اذإ طقف بولطم اذه .يرايتخإ ريدصتلل لباقلا حاتفملا رايخ نإ .3 عبرملا جراخ حاتفملا.
- ءاشنإ ددح .4

<ul> <li>Monitoring</li> <li>Configuration</li> <li>Administration</li> <li>Licensing</li> <li>Troubleshooting</li> <li>Cisco_IDEVID_SUDI_LEGACY_RSA</li> <li>No</li> <li>To ubleshooting</li> </ul>	Dashboard		Trustpoints CA Server	Key Pai	r Generation	Add Ce	rtificate Trustp	bool
Administration       TP-self-signed-2147029136       RSA       No       Image: Constraint of the self-signed of the s		>	+ Add Key Name	Кеу Туре	Key Exportable	T Zeroize		10.0050
Administration       9800-40.cisco.com       RSA       No       Image: Comparison of the system of the	S		TP-self-signed-2147029136	RSA	No	🖹 Zer	Key Name*	AP-SCEP
Licensing       TP-self-signed- 2147029136.server       RSA       No       Image: Constraint of the server       Modulus Size*       2048         CISCO_IDEVID_SUDI       RSA       No       Image: Constraint of the server       Key Exportable*       Image: Constraint of the server         Image: CISCO_IDEVID_SUDI_LEGACY       RSA       No       Image: Constraint of the server       Image: Constraint of the server <td>Administration</td> <td>&gt;</td> <td>9800-40.cisco.com</td> <td>RSA</td> <td>No</td> <td>i ⊇ Zer</td> <td>Key Type*</td> <td>● RSA Key ○ EC Key</td>	Administration	>	9800-40.cisco.com	RSA	No	i ⊇ Zer	Key Type*	● RSA Key ○ EC Key
CISCO_IDEVID_SUDI     RSA     No     Image: Constraints       CISCO_IDEVID_SUDI_LEGACY     RSA     No     Image: Constraints       Image: I	Licensing		TP-self-signed- 2147029136.server	RSA	No	i≣ Zer	Modulus Size*	2048
Troubleshooting     CISCO_IDEVID_SUDI_LEGACY_RSA     No     Image: Zero     Key Exportable*       Image: Imag			CISCO_IDEVID_SUDI	RSA	No	🖹 Zer	INIGUIUS OIZC	
H         I	Troubleshooting		CISCO_IDEVID_SUDI_LEGACY	RSA	No	🗎 Zer	Key Exportable*	
			H - I - H	10 🔻	1 - 5 of	5 items	D Cancel	✓ Generate
	Walk Me Through >							

ةقثلا طاقن < PKI ةرادإ < نامألا < نيوكتلا ىلإ لقتنا .2 ةوطخلا

- .بسانم مسا هيطعيو فيضي ةقطقط .1
- وه انه URL ناونع) ليجستلل URL وه انه URL وه انه. <u>http://10.106.35.61:80/certsrv/mscep/mscep.dll</u>
- .1 ةوطخلا يف اهؤاشنإ مت يتلا RSA حيتافم جاوزأ ددح .3
- .ةقداصملا ىلع رقنا .4
- .رورم ةملك لخدأو TrustPoint ليجست قوف رقنا .5
- .زاهجلا ىلع قيبطت قوف رقنا .6

Q Search Menu Items	Configuration • > Set	curity * > PKI Management		
Dashboard	Add Trustpoint			×
	Label*	Access_Point-MS-CA	Enrollment Type	SCEP () Terminal
( Monitoring >	Subject Name			
Configuration >	Country Code	IN	State	КА
() Administration >	Location	Bengaluru	Domain Name	TAC-LAB.cisco.local
© Licensing	Organization	TAC	Email Address	mail@tac-lab.local
X Troubleshooting	Enrollment URL	/certsrv/mscep/mscep.dll	Authenticate	
	Key Generated		Available RSA Keypairs	AP-SCEP 👻
	Enroll Trustpoint			
	Password*			
	Re-Enter Password*			
	Cancel			Apply to Device

ددحو لفسأل ريرمتلاب مق .لوصولا طاقن < يكلسال < نيوكتلا ىلإ لقتنا.3 ةوطخلا ريفوت LSC.

- .WLC اذه ىلإ تطبر نوكي نأ all the APs ل LSC نكمي اذه .ةنكممك ةلاحلا ديدحت .1
- .2 ةوطخلا يف هانأشنأ يذلI TrustPoint مسا ددح .2

كتاجايتحال اقفو ليصافتلا ةيقب ألما.

Q. Search Menu Items	Configuration * > Wireless * > Access Points			
🚃 Dashboard	<ul> <li>All Access Points</li> </ul>			
Monitoring >	Total APs : 1		Tag: 0 Country C	ode : 0 LSC Failback : 0 Select an Action 👻
Configuration	AP Name I AP Model I	Admin I: Stots I: Status Up Time I: IP Address	Base Radio MAC : Ethernet MAC :	AP i Power Derate i Operation i Config Mode Capable Status Status
(⊙) Administration →	AP0CD0-F89A-46E0 4 C9117AXI-D	2 0 days 0 hrs 26 10.105.101.16 mins 42 secs	8 d0ec.3579.0300 0cd0.189a.46e0	Local Yes Registered Healthy
Y Troubleshooting				1 - 1 of 1 access points
-	> 6 GHz Radios			
	> 5 GHz Radios			
	> 2.4 GHz Radios			
	> Dual-Band Radios			
	> Country			
	<ul> <li>LSC Provision</li> </ul>			
	Status	Enabled	Subject Name Parameters	E Apply
	Trustpoint Name	Access_Point-MS.x •	Country IN	
	Number of Join Attempts	3 2048 v	State KA	
	Certificate chain status	Not Ausiisble	City Bengaluru Organization TAC	
	Number of certificates on chain	0	-	

ةدحو لمع ةسلج يف .ديەمت دعأو WLC قيرط نع ةداەشلا تبلج LSC، APs تنأ نكمي نإ ام

ةصاصقلا هذه لثم ائيش ىرتس ،لوصولا ةطقنب مكحتلا.

[*09/25/2023 10:03:28.0993]	
[+09/25/2023 10:03:28.7016]	
[+09/25/2023 10:03:28.7663]	writing new private key to '/tmp/lsc/priv_key'
[+09/25/2023 10:03:28.7666]	
[+09/25/2023 10:03:28.9212]	LSC_ENABLE: saving ROOT_CERT
[+09/25/2023 10:03:28.9212]	
[+09/25/2023 10:03:28.9293]	LSC_ENABLE: saving DEVICE_CERT
[+09/25/2023 10:03:28.9293]	
[+09/25/2023 10:03:28.9635]	LSC certs and private key verified
[+09/25/2023 10:03:28.9635]	
[+09/25/2023 10:03:29.4997]	LSC private key written to hardware TAM
[+09/25/2023 10:03:29.4997]	
[*09/25/2023 10:03:29.5526]	A[09/25/2023 10:03:29.6099] audit_printk_skb: 12 callbacks suppressed

ل TrustPoint قباطتل ةيكلساللا ةرادإلاا ةداهش رييغت كنكمي ،LSC نيكمت درجمب .4 ةوطخلا LSC. لعجي اذه APs ل قداهش LSC وه لمعتسي WLC لاو قداهش LSC مه عم ىقالتي APs لعجي اذه لوصولا طاقنل 802.1X ةقداصم لمعب طقف امتهم تنك اذا ةيرايتخا ةوطخ هذه .ىقالتي لكب ةصاخلا

- ا قەجاو قوف رقناو Configuration (نيوكتلا) > Interface (قەجاولا) > Wireless دەجاو قوف رقناو قوف رقناو دادال
- .2 ةوطخلا يف مانأشنأ يذلا TrustPoint قباطتل TrustPoint رييغتب مق .2

لوصولا طاقن نوكت نأ بجي .LSC ل (GUI) ةيموسرلا مدختسملا ةمجاو نيوكت ءزج متتخي اذهو مادختساب (WLC) ةيكلساللا ةيلحملا ةكبشلا يف مكحتلا رصنع ىلإ مامضنالا ىلع ةرداق .نآلا LSC ةداهش

Q. Search Menu Items	Configuration * > Interface * > Wireless	Edit Management Interface *
Desthoard	+ Add V Delete	Changing the interface or trustpoint will cause APs to disconnect and disrupt clients.
	Interface Name Y Interface Type Y VLAN ID Y IP Address Y IP Netmask	Martine Van101 • ①
Monitoring >	Vian101 Management 101 10.105.101.160 255.255.25	Trustpoint Access_Point-MS.x v 2
Configuration >		There is no investpoint configured on the controller. CISCO_IDEVIO_SUDI is used as the default trustpoint.
{O} Administration →		NAT IPv4/IPv6 Server Address 0.0.0.0
C Licensing		
X Troubleshooting		
		Cancel
		Cipdete & Apply to Device

AP LSC ل (CLI) رماوألا رطس ةهجاو نيوكت تاوطخ

.رمألاا اذه مادختساب RSA حاتفم ءاشنإب مق .1

% You already have RSA keys defined named AP-SCEP. % They will be replaced % The key modulus size is 2048 bits % Generating 2048 bit RSA keys, keys will be non-exportable... [OK] (elapsed time was 0 seconds) Sep 27 05:08:13.144: %CRYPTO\_ENGINE-5-KEY\_DELETED: A key named AP-SCEP has been removed from key storag Sep 27 05:08:13.753: %CRYPTO\_ENGINE-5-KEY\_ADDITION: A key named AP-SCEP has been generated or imported

2. ليجستلاب صاخلا URL ناونع لخداً RSA حيتافم جوز نييعتو PKI ةقث ةطقن ءاشنإ ليصافتلا يقابو.

```
9800-40(config)#crypto pki trustpoint Access_Point-MS-CA
9800-40(ca-trustpoint)#enrollment url http://10.106.35.61:80/certsrv/mscep/mscep.dll
9800-40(ca-trustpoint)#subject-name C=IN,L=Bengaluru,ST=KA,0=TAC,CN=TAC-LAB.cisco.local,E=mail@tac-lab.
9800-40(ca-trustpoint)#rsakeypair AP-SCEP
9800-40(ca-trustpoint)#revocation none
9800-40(ca-trustpoint)#exit
```

3. مداخ عم اهليجستو PKI قوث ةطقن ةقداصم crypto pki authenticate رمألا مادختساب CA مداخ عم اهليجستو trustPoint>. روزم الم يف روزم قملك لخدأ.

9800-40(config)#crypto pki authenticate Access\_Point-MS-CA Certificate has the following attributes: Fingerprint MD5: C44D21AA 9B489622 4BF548E1 707F9B3B Fingerprint SHA1: D2DE6E8C BA665DEB B202ED70 899FDB05 94996ED2 % Do you accept this certificate? [yes/no]: yes Trustpoint CA certificate accepted. 9800-40(config)#crypto pki enroll Access\_Point-MS-CA % % Start certificate enrollment .. % Create a challenge password. You will need to verbally provide this password to the CA Administrator in order to revoke your certificate. For security reasons your password will not be saved in the configuration. Please make a note of it. Password: Sep 26 01:25:00.880: %PKI-6-CERT\_ENROLL\_MANUAL: Manual enrollment for trustpoint Access\_Point-MS-CA Re-enter password: % The subject name in the certificate will include: C=IN,L=Bengaluru,ST=KA,O=TAC,CN=TAC-LAB.cisco.local % The subject name in the certificate will include: 9800-40.cisco.com % Include the router serial number in the subject name? [yes/no]: yes % The serial number in the certificate will be: TTM244909MX % Include an IP address in the subject name? [no]: no Request certificate from CA? [yes/no]: yes % Certificate request sent to Certificate Authority % The 'show crypto pki certificate verbose Access\_Point-MS-CA' commandwill show the fingerprint. Sep 26 01:25:15.062: %PKI-6-CSR\_FINGERPRINT: CSR Fingerprint MD5 : B3D551528B97DA5415052474E7880667 CSR Fingerprint SHA1: D426CE9B095E1B856848895DC14F997BA79F9005 CSR Fingerprint SHA2: B8CEE743549E3DD7C8FA816E97F2746AB48EE6311F38F0B8F4D01017D8081525 Sep 26 01:25:15.062: CRYPTO\_PKI: Certificate Request Fingerprint MD5 :B3D55152 8B97DA54 15052474 E78806 Sep 26 01:25:15.062: CRYPTO\_PKI: Certificate Request Fingerprint SHA1 :D426CE9B 095E1B85 6848895D C14F9 Sep 26 01:25:15.063: CRYPTO\_PKI: Certificate Request Fingerprint SHA2 :B8CEE743 549E3DD7 C8FA816E 97F27 Sep 26 01:25:30.239: %PKI-6-CERT\_INSTALL: An ID certificate has been installed under Trustpoint : Access\_Point-MS-CA Issuer-name : cn=sumans-lab-ca,dc=sumans,dc=tac-lab,dc=com Subject-name : e=mail@tac-lab.local,cn=TAC-LAB.cisco.local,o=TAC,l=Bengaluru,st=KA,c=IN,hostname=9800-4 Serial-number: 5C0000001400DD405D77E6FE7F00000000014 End-date : 2024-09-25T06:45:15Z 9800-40(config)#

.LSC ةداەش مادختساب لوصولا ةطقن مامضنا نيوكتب مق .4

9800-40(config)#ap lsc-provision join-attempt 10 9800-40(config)#ap lsc-provision subject-name-parameter country IN state KA city Bengaluru domain TAC-L 9800-40(config)#ap lsc-provision key-size 2048 9800-40(config)#ap lsc-provision trustpoint Access\_Point-MS-CA 9800-40(config)#ap lsc-provision In Non-WLANCC mode APs will be provisioning with RSA certificates with specified key-size configuration Are you sure you want to continue? (y/n): y

5. اەۋاشنإ مت يتلا TrustPoint قباطتل ةيكلساللا ةرادإلاب ةصاخلا TrustPoint رييغتب مق مالعأ.

9800-40(config)#wireless management trustpoint Access\_Point-MS-CA

AP LSC نم ققحتلا

.LSC لا ققدي نأ WLC ىلع رمأ اذه تضكر

#show wireless management trustpoint
#show ap lsc-provision summary
#show ap name < AP NAME > config general | be Certificate

```
9800-40#sho ap lsc-provision summ
AP LSC-provisioning : Enabled for all APs
Trustpoint used for LSC-provisioning : <u>Access_Point-MS-CA</u>
    Certificate chain status : Available
    Number of certs on chain : 2
    Certificate hash
                        : b7f12604ffe66b4d4abe01e32c92a417b5c6ca0c
LSC Revert Count in AP reboots : 10
AP LSC Parameters :
Country : IN
State : KA
City : Bengaluru
Orgn : TAC
Dept : TAC-LAB.cisco.local
Email : mail@tac-lab.local
Key Size : 2048
EC Key Size : 384 bit
AP LSC-provision List :
Total number of APs in provision list: 0
Mac Addresses :
9800-40#sho wire
9800-40#sho wireless man
9800-40#sho wireless management tru
9800-40#sho wireless management trustpoint
Trustpoint Name : Access_Point-MS-CA
Certificate Info : Available
Certificate Type : LSC
Certificate Hash : b7f12604ffe66b4d4abe01e32c92a417b5c6ca0c
Private key Info : Available
FIPS suitability : Not Applicable
9800-40#
```

986	0-40#sho ap name AP0CD0.F8	9A	.46E0 config general   begin Certificate
AP	Certificate type		: Locally Significant Certificate
AP	Certificate Expiry-time		: 09/25/2024 06:48:23
AP	Certificate issuer common-	na	me : sumans-lab-ca
AP	Certificate Policy		: Default
AP	CAPWAP-DTLS LSC Status		
	Certificate status	:	Available
	LSC fallback status	:	No
	Issuer certificate hash	:	611255bc69f565af537be59297f453593e432e1b
	Certificate expiry time	:	09/25/2024 06:48:23
AP	802.1x LSC Status		
	Certificate status	:	Not Available
4.0	100 authorities days		CANALD DELC

ةطقنل (CLI) رماوألا رطس ةهجاو ىلإ لوخدلا ليجستب مق ،لوصولا طاقن ليمحت ةداعإ درجمب نيوكت نم ققحتلل رماوألا هذه ليغشتب مق مث لوصولا LSC.

#show crypto | be LSC
#show capwap cli config | in lsc
#show dtls connection

```
AP0CD0.F89A.46E0#sho crypto | be LSC
LSC: Enabled
                           -- Device Certificate -
Certificate:
   Data:
       Version: 3 (0x2)
      Serial Number:
           5c:00:00:00:18:18:14:ed:da:85:f9:bf:d1:00:00:00:00:00:18
       Signature Algorithm: sha256WithRSAEncryption
       Issuer: DC = com, DC = tac-lab, DC = sumans, CN = sumans-lab-ca
       Validity
           Not Before: Sep 28 04:15:28 2023 GMT
           Not After : Sep 27 04:15:28 2024 GMT
       Subject: C = IN, ST = KA, L = Bengaluru, O = TAC, CN = ap1g6-0CD0F89A46E0, emailAddress = mail@tac-lab.local
       Subject Public Key Info:
           Public Key Algorithm: rsaEncryption
               RSA Public-Key: (2048 bit)
               Modulus:
```

AP0CD0.F89A.46E0#sho crypto	in LSC	
LSC: Enabled		
AP@CD@,F89A,46E@#sho capwap	cli config   in	lsc
AP lsc enable	: 1	
AP lsc reboot cnt	: 0	
AP lsc max num of retry	: 10	
AP lsc mode	: 0×1	
AP lsc dtls fallback state	: 0	
AP0CD0.F89A.46E0#		
Read timed out		

AP0CD0.F89A.46E0#sho dtls connections

Number of DTLS connection = 1

[ClientIP]:ClientPort <=> [ServerIP]:ServerPort Ciphersuit Version

[10.105.101.168]:5256 <=> [10.105.101.160]:5246 0xc02f 1.2

Current connection certificate issuer name: sumans-lab-ca

### اهحالصإو LSC دادعإ ءاطخأ فاشكتسأ

يتلا ةداهشلا نم ققحتلل AP وأ WLC ليصوت لوحم ذفنم نم EPC طاقتلاا ذخأ كنكمي قفن نيوكتل لوصولا ةطقن اهمدختست حاجنب.



.ةداەشلا ةلكشم مەفل WLC و AP ىلع DTLS ءاطخأ حيحصت ليغشت نكمي

#### LSC مادختساب 802.1X ةقداصم ةيكلسلا لوصولا ةطقن

لمعت .اەسفن ىلع ةقداصملل LSC ةداەش سفن مادختسال لوصولا ةطقن نيوكت مت مداخ ثدحتي .ISE مداخ لباقم لوحملا ةطساوب اەتقداصم متيو 802.1X ەجومك لوصولا ةطقن ISE . ةشاشلا ةرخۇم يف نالعإلاا ىل



طاقنل نكمي ال ،AP ليصوت لوحم ذفنم ىلع dot1x ةقداصم نيكمت درجمب :ةظحالم دادرتسال .ةقداصملا ريرمت متي ىتح رورم ةكرح يأ لابقتسإ وأ هيجوت ةداعإ لوصولا ةقداصم ليطعتب مق ،AP ىلإ لوصولاو ةحجان ريغ ةقداصمب (AP) لوصولا طاقن dot1x لوصولا ةطقنل يكلسلا لوحملا ذفنم ىلع

لﺉاسرلا لدابتو EAP-TLS ةقداصم لمع ريس



لوصولا ةطقنل ةيكلسلا 802.1x ةقداصم نيوكت تاوطخ

- .EAP عون ددحو CAPWAP ل DTLS عم dot1x ذفنملا ا قوداصم نيكمتب مق .1
- .لوصولا طاقنل dot1x دامتعا تانايب ءاشنإب مق .2
- .ءانيم حاتفملا ىلع dot1x تنكم .3
- 4. مداخ ىلع اەب قوثوم ةداەش تيبثت

ةقداصمل (GUI) ةيموسرلا مدختسملا ةهجاو نيوكت ةيكلسلا لوصولا ةطقن 802.1x

- . فيرعتلا فلم ىلع رقناو لوصولا ةطقن طبر فيرعت فلم ىلإ لقتنا .1
  - 1. ك AP ليوخت عونو EAP عون ددح .ماع < لوصولا ةطقن ىلع رقنا AP" ليوخت عونو dot1x Port auth".
  - ةطقنل رورم ةملكو مدختسم مسا ءاشنإب مقو دامتعا تانايب < ةرادإ ىلإ لقتنا .2 لوصولا dot1x auth.

Cisco Ca	talyst 9800-40 Wireless Controller		Welcome admin 🛛 🛠 🌾 🛕 🖺 🏟 🗐 📿	Search APs and Clents Q
Q. Search Manu Items	Configuration * > Tags & Profiles * > AP Join		Edit AP Join Profile General Client CAPWAP AP Management Si	x iecurity ICap QoS
Dashboard     Monitoring	AP Join Profile Name	▼ Des	General Power Management Hyperlocation AP Statis	Client Statistics Reporting Internal
	APG_test tootSte		Switch Flag	5 GHz (soc) 90
{⊙} Administration → (©) Licensing	APG_3rd-Fir-APs APG_4th-Fir-APs		Power Injector State Power Injector Type Unknown	2.4 GHz (sec) 90 Extended Module
💥 Troubleshooting	APG_00+Fr-APs     APG_70+Fr-APs     APG_80+Fr-APs		AP EAP Auth Configuration	Enable  Mesh
Walk Me Through 2	APG_11th-Fir-APs APG_12th-Fir-APs APG_12th-Fir-APs		EAP Type EAP-TLS v AP Authorization Type CAPVAP DTLS + DDTs. CAPVAP DTLS +	Profile Name default-mesh-pro • Clear
	H < 1 2 3 → H 10 v		DOTTx port auth CAPWAP DTLS Dottx port auth	
			"D Cancel	🗄 Update & Apply to Device

Cisco Ca	talyst 9800-40 Wireless Controller	W	elcome admin	* *		000	<b>c</b>		Q	oodback <sub>K</sub> * ()
Q. Search Menu Items	Configuration * > Tags & Profiles * > AP Join	Edit A	P Join Profile							×
Dashboard	-+ Add 🛛 × Delete 🕄 Clone	Genera	l Client	CAPWAP Credentials	AP M	anagement face	Security	ICap	QoS	
	AP Join Profile Name	T Des								
(1) Monitoring >	ap-auth	Dot	1x Credentials	_						
🗞 Configuration 🔷 🔸	APG_test	Det	x Username		ap-wired-user	t				
중 Administration	testSite	Dot	x Password	1						
(c) · · · · · ·	APG_3rd-Fir-APs	Der	v Dassword Tupo	, i	clear	_				
C Licensing	APG_4th-Fk-APs		x rassnora ryps							
1 Troubleshooting	APG_6th-Fit-APs									
	APO_7th-FH-APs									
	APG_801-FP-APs									
	APG_11th-Fir-APs									
Walk Me Through 1										
	H I Z 3 F H 10 F									
		00	ncel						Update	& Apply to Device

ليكشت CLI ةيوه ةحص AP Wired 802.1x

ةقداصملا نيكمت ىلإ الإ اذه يدؤي ال .CLI لا نم APs ل dot1x نكمي نأ رمأ اذه تلمعتسا نيعملا طبرلا فيصوت مدختست يتلا لوصولا طاقنل ةيكلسلا.

#ap profile ap-auth
#dot1x eap-type eap-tls
#dot1x lsc-ap-auth-state both
#dot1x username ap-wired-user password 0 cisco!123

#### ليكشت حاتفم ةيوه ةحص 802.1x يكلس ap

كنكمي .ةيكلسلا AP ةقداصم نيكمتل LAB يف هذه لوحملا تانيوكت مادختسا متي ميمصتلا ىلإ ادانتسا ةفلتخم ةئيهت ىلع لوصحلا.

aaa new-model dot1x system-auth-control aaa authentication dot1x default group radius aaa authorization network default group radius radius server ISE address ipv4 10.106.34.170 auth-port 1812 acct-port 1813 key cisco!123 1 interface GigabitEthernet1/0/2 description "AP-UPLINK-PORT-AUTH-ENABLED" switchport access vlan 101 switchport mode access authentication host-mode multi-host authentication order dot1x authentication priority dot1x authentication port-control auto dot1x pae authenticator end

RADIUS مداخ ةداەش تيبثت

لك قثي نأ بجي .RADIUS مداخو (سمتلمك لمعت يتلا) لوصولا ةطقن نيب ةقداصملا ثدحت مداخ ةداهش يف لوصولا ةطقن اهب قثت يتلا ةديحولا ةقيرطلا .رخآلا ةداهش يف امهنم RADIUS عجرم نم ةرداص ةداهش RADIUS مداخ مدختسي نأ يه RADIUS اضيأ.

تاداهش عيقوت تابلط ءاشنإ < تاداهش < ةرادإلا ىل لقتنا ISE، يف

.كب ةصاخلا ISE ةدقع تامولعمب لوقحلا ةئبعتو CSR ءاشنإب مق

Cisco ISE

Administration · System

Deployment Licensing	Certificates Logging Maintenance Upgrade Health Checks Backup & Restore Admin Access Settings	
Deployment Licensing Certificate Management System Certificates Trusted Certificates OCSP Client Profile Certificate Signing Requests Certificate Periodic Check Se Certificate Authority	<ul> <li>Certificate Loging Mainence Upgrade Health Checks Backup &amp; Restore Admin Access Settings</li> <li>Certificate Signing Requests</li> <li>Certificate Signing Requests</li> <li>Certificate Signing Report of the state state state date ways usages. The list below outlines which extended key usages are required for each certificate type:</li> <li>Main - Server Authentication</li> <li>Certificate Signing Certificate Signing Certificate or generate a brand new Messaging Certificate.</li> <li>Otal Authentication</li> <li>Stati - Salver Authentication</li> <li>Otal Authentication</li> <li>Stati - Salver Authentication</li></ul>	
	Node CSR Friendly Name	
	Viseo Subject	
	Subject         Common Name (CN)         SFQDNS         Organizational Unit (OU)         Organization (O)         Organization (C)         City (L)         State (ST)	

#### اضيأ صنك اهقصل خسنو اهريدصت كنكمي ،اهديلوت متي نأ درجمب.

URL ناونع ىلإ /certsrv/ فضأو Windows CA ب صاخلا IP ناونع ىلإ لقتنا

#### ةداەش بلط ىلع رقنا

← → C ▲ Non sécurisé | 192.168.1.98/certsrv/
 Microsoft Active Directory Certificate Services - mydomain-WIN-3E202T1QD0U-CA
 Welcome
 Use this Web site to request a certificate for your Web browser, e-mail client, or other program. By using a certificate, you can verify your identity to people you communicate with

You can also use this Web site to download a certificate authority (CA) certificate, certificate chain, or certificate revocation list (CRL), or to view the status of a pending request. For more information about Active Directory Certificate Services, see <u>Active Directory Certificate Services Documentation</u>.

Select a task: <u>Request a certificate</u> <u>View the status of a pending certificate request</u> <u>Download a CA certificate, certificate chain, or CRL</u>

```
... base-64 مادختساب ةداەش بلط لاسرا كلع رقنا
```

Microsoft Active Directory Certificate Services -- mydomain-WIN-3E2O2T1QD0U-CA

#### Advanced Certificate Request

The policy of the CA determines the types of certificates you can request. Click one of the following options to: <u>Create and submit a request to this CA.</u>

Submit a certificate request by using a base-64-encoded CMC or PKCS #10 file, or submit a renewal request by using a base-64-encoded PKCS #7 file,

#### بيولا مداخ ةداهش بلاق رتخأ .صنلا عبرم يف CSR صن قصلا.

← C ▲ Non sécurisé   192.168.1.98/certsrv/certrqxt.asp
Microsoft Active Directory Certificate Services – mydomain-WIN-3E202T1QD0U-CA
Submit a Certificate Request or Renewal Request
To submit a saved request to the CA, paste a base-64-encoded CMC or PKCS #10 certificate request or PKCS #7 renewal request generated by an external source (such as a Web server) in the Saved Request box.
Saved Request:           Base-64-encoded           certificate request           (CMC or PKCS #10 or PKCS #7):
Certificate Template: (No templates found!) >
Additional Attributes:

ةداەشلا عيقوت بلط ةمئاق ىلإ عوجرلاب ISE ىلع ةداەشلا ەذە تيبثت كلذ دعب كنكمي نم اەيلع تلصح يتلا ةداەشلا ليمحت كلذ دعب كنكمي .ةداەشلا طبر قوف رقنلاو C.

≡ Cisco ISE	Administration · System
Deployment Licensing	rtificates Logging Maintenance Upgrade Health Checks Backup & Restore Admin Access Settings
Certificate Management System Certificates	Certificate Signing Requests
Trusted Certificates OCSP Client Profile	Generate Certificate Signing Requests (CSR)
Certificate Signing Requests	A Certificate Signing Requests (CSRs) must be sent to and signed by an external authority. Click "export" to download one or more CSRs so that they may be signed by an external authority. After a request has been signed, click this list.
Certificate Periodic Check Se	Q, View 🖒 Export 📋 Delete Bind Certificate
Certificate Authority >	Eriendly Name Certificate Subject Key Length Portal gro Timestamp Abox
	ISE99#EAP Authentication         CN=ISE99.mydomain.local         4096         Mon, 30 Oct 2023         ISE99

ةيكلسلا 802.1x ةقداصم نم ققحتلا :لوصولا ةطقن

رمألا ليغشتب مقو لوصولا ةطقن ىلإ مكحتلا ةدحو لوصو ىلع لصحا:

#show ap authentication status

```
لوصولا ةطقن ةقداصم نيكمت متي مل:
```

#### :AP ةقداصم نيكمت دعب AP نم مكحتلا ةدحو تالجس

AP0CD0.F89A.46E0#[\*09/26/2023 08:57:40.9154] [\*09/26/2023 08:57:40.9154] Restart for both CAPWAP DTLS & 802.1X LSC mode [\*09/26/2023 08:57:40.9719] AP Rebooting: Reset Reason - LSC mode ALL

#### :حاجنب AP ةقداصم تمت



#### :WLC نم ققحتلا

9800-40#sho ap name AP0CD0.F89A.46E0 config general   begin Certificate
AP Certificate Expiry-time : 09/25/2024 06:48:23
AP Certificate issuer common-name : sumans-lab-ca
AP Certificate Policy : Default
AP CARWAP-DILS LSC Status
Issuer certificate hash : 611255bc69f565af537be59297f453593e432e1b
Certificate expiry time : 09/25/2024 06:48:23
AP 802.1x LSC Status
Certificate status : Available
Issuer certificate hash : 611255bc691565af537bc59297f453593e432e1b
Certificate expiry time : 89/75/2824 BB:48:73
AP LSC authentication state : CAPNAP-DILS and 002.1X authentication

#### :ةحجانلا ةقداصملا دعب Switchport ةەجاو ةلاح

Switch#sho authentication Interface	MAC Address	rface gi Method	gabitEth Domain	ernet 1/0/2 Status Fg	Session ID
Gi1/0/2	0cd0.f89a.46e0	dot1x	DATA	Auth	9765690A0000005CCEED0FBF

#### ةحجان ةقداصم ىلإ ريشت لوصولا ةطقن مكحت ةدحو تالجس نم ةنيع هذه:

```
[*09/26/2023 07:33:57.5512] hostapd:dot1x: RX EAPOL from 40:f0:78:00:a1:02
[*09/26/2023 07:33:57.5513] hostapd:EAP: Status notification: started (param=)
[*09/26/2023 07:33:57.5513] hostapd:EAP: EAP-Request Identity
[*09/26/2023 07:33:57.5633] hostapd:dot1x: RX EAPOL from 40:f0:78:00:a1:02
[*09/26/2023 07:33:57.5634] hostapd:EAP: Status notification: accept proposed method (param=TLS)
[*09/26/2023 07:33:57.5673] hostapd:dot1x: CTRL-EVENT-EAP-METHOD EAP vendor 0 method 13 (TLS) selected
[*09/26/2023 07:33:57.5907] hostapd:dot1x: RX EAPOL from 40:f0:78:00:a1:02
[*09/26/2023 07:33:57.5977] hostapd:dot1x: RX EAPOL from 40:f0:78:00:a1:02
[*09/26/2023 07:33:57.6045] hostapd:dot1x: RX EAPOL from 40:f0:78:00:a1:02
[*09/26/2023 07:33:57.6126] hostapd:dot1x: RX EAPOL from 40:f0:78:00:a1:02
[*09/26/2023 07:33:57.6137] hostapd:dot1x: CTRL-EVENT-EAP-PEER-CERT depth=1 subject='/DC=com/DC=tac-lab
[*09/26/2023 07:33:57.6145] hostapd:dot1x: CTRL-EVENT-EAP-PEER-CERT depth=0 subject='/C=IN/ST=KA/L=BLR/
[*09/26/2023 07:33:57.6151] hostapd:EAP: Status notification: remote certificate verification (param=su
[*09/26/2023 07:33:57.6539] hostapd:dot1x: RX EAPOL from 40:f0:78:00:a1:02
[*09/26/2023 07:33:57.6601] hostapd:dot1x: RX EAPOL from 40:f0:78:00:a1:02
[*09/26/2023 07:33:57.6773] hostapd:dot1x: RX EAPOL from 40:f0:78:00:a1:02
[*09/26/2023 07:33:57.7812] hostapd:dot1x: RX EAPOL from 40:f0:78:00:a1:02
[*09/26/2023 07:33:57.7812] hostapd:EAP: Status notification: completion (param=success)
[*09/26/2023 07:33:57.7812] hostapd:dot1x: CTRL-EVENT-EAP-SUCCESS EAP authentication completed successf
[*09/26/2023 07:33:57.7813] hostapd:dot1x: State: ASSOCIATED -> COMPLETED
[*09/26/2023 07:33:57.7813] hostapd:dot1x: CTRL-EVENT-CONNECTED - Connection to 01:80:c2:00:00:03 compl
```

## اهحالصإو 802.1X ةقداصم ءاطخأ فاشكتسأ

.ةحجانلا ةقداصملا نم ءزج يلي اميف .RADIUS ةقداصم نم ققحتو AP ةلصو ىلع PCAP ذخ

479. 07:47:17.192983 Cisco_9a:46:e0 Nearest-non-TP.	EAP	Response, Identity[Packet size limited during capture]
470. 07:47:17.205983 Cisco_9a:46:e8 Nearest-non-TP.	TLSv1.2 1812 55431	Encrypted Handshake Message
475. 67:47:17.253954 10.100.34.170 10.105.101.151 479 07:47:17.256975 Cisco_9a:46:e0 Nearest-non-TP	RADIUS 1812 55431 EAP	Access-Canllenge Labit Response, TLS EAP (EAP-TLS)[Packet size limited during capture]
475. 67:47:17.762971 10.104.34.176 10.105.101.151 479 07:47:17.267976 Cisco_9a:46:e0 Nearest-non-TP	RADIUS 1812 55431 EAP	Response, TLS EAP (EAP-TLS)[Packet size limited during capture]
472. 07347117.270982 10.105.34.170 16.105.101.131 479 07:47:17.274979 Cisco 9a:46:e8 Nearest-non-TP	RADIUS 1812 55431 EAP	Response, TLS EAP (EAP-TLS)[Packet size limited during capture]
479. 07:47:17.277985 10.185.34.170 10.185.101.151 479. 07:47:17.311980 Cisco 9a:46:e0 Nearest-non-TP.	RADIUS 1812 55431 EAP	Access-Chullenge 10-207 Response, TLS EAP (EAP-TLS)
474 87147117.314919 10.141.34.178 10.141.181.351 4 d79. 07:d7:17.318968 Cisco 9a:d6:e8 Nearest-non-TP_	RADIUS 1812 55431 EAP	Response, TLS FAP (FAP-TLS)
471. 67141:17.321914 10.165.14.178 10.165.161.151 470. 67:47:17.324088 Cisco 9146:08 Newrost-non-10	RADIUS 1812 55431	Archi-Cuilinge 10-24 Incontellingehikk Massane   Encrunted Handshake Massane   Encrunted Handshake Massane   Channe Cinher Sner   Encrunted Handshake M
479. 07:47:17.339978 10.106.34.178 10.105.101.151 470. 07:47:17.339978 00.106.34.178 10.105.101.151	RADIUS 1812 55431	Accepted National Accepted States (Second States and States and States) and a state of the states
479. 07:47:17.376979 10.106.34.170 10.105.101.151	RADIUS 1812 55431	Access-Ac

.ةقداصملا طاقتلال ISE نم TCPdump عمجي



نم نمازتم لكشب مزحلا طاقتلا مزليسف ،ةقداصملا ءانثأ ظحالت ةلكشم كانه تناك اذإ بناجو ةيكلسلا AP ةلصو

AP: ل ءاطخألا حيحصت رمأ

#debug ap authentication packet

### ةلص تاذ تامولعم

- <u>اليزنتلاوينقتلا معدلا</u> Cisco
- <u>AireOS مادختساب AP ىلع 802.1X نيوكت</u> •
- <u>LSC ل 9800 نيوكتلا ليلد</u> •
- <u>LSC ل لاثم ليكشت LSC</u>
- <u>9800 ىلع لوصولاطاق نل 802.1X نيوكت</u>

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