مادختساب EAP-TLS ىلع EAP-TLS نيوكت ISE Internal CA

تايوتحملا

<u>ةمدقملا</u> <u>قىساسألا تابلطتملا</u> <u>ةمدختسملا تانوكملا</u> <u>قيساساً تامولعم</u> EAP-TLS ةقداصم قفدت <u>EAP-TLS قڧدت يف تاوطخ</u> <u>نىوكتلا</u> <u>ةكېشلل يطيطختلا مسرلا</u> <u>تانيوكتاا</u> <u>ISE نيوكت</u> <u>ةكبش زاهج ةفاضا</u> <u>يلخادلا قدصملا عجرماا نم ققحتاا</u> <u>قق داص مل ا بول س أ قف اض ا</u> <u>قداەشلا بلاق دىدەت</u> <u>ةداەش لخدم ءاشنا</u> <u>يلخاد مدختسم ةفاضا</u> <u>RADIUS جەنو ISE ةداەش رېفوت لىخدم نېوكت</u> <u>9800 WLC نىوكت</u> <u>ا ا ا ا ا ا ا ا ا مداخ ةفاض ISE مداخ ةفاض </u> <u>9800 WLC ىلع مداوخ ةعومجم ةفاضا</u> <u>AAA قرط ةمئاق نېوكت</u> WLC <u>9800 WLC ىلع ضيوفتلا قرط ةمئاق نيوكت</u> <u>9800 WLC دارع جەن فېرعت فالم ءاش، ا</u> <u> 9800 WLA ةكبش ءاشنا</u> WLAN <u>المحا</u> 9800 WLC ياع جەنلا فېرغت فالم عم WLAN قطىرخ <u>9800 WLC يا يا يا ماري المحقون عالما جون المالي مجرت</u> <u>لامتكا دعب (WLC) ةيكل سال لا قول حملا ةكبش لا يف مكحتالا رص نع نوكت ل يغشت متي</u> دادعالا <u>مدختسملل ةداهش ليزنتو ءاشنا</u> <u>Windows 10 ليغشتارا ماظنب لمعي زامج يالع قدامشارا تيبثت</u> <u>قحصالا نم ققحتاا</u> <u>اهحالصاو ءاطخألا فاشكتسا</u> <u>عجارملا</u>

ةمدقملا

ةقداصم دنتسملا اذه فصي EAP-TLS تامدخ كرحمل قدصملا اذه فصي نيمدختسملا ققداصمل.

ةيساسألا تابلطتملا

ةمدختسملا تانوكملا

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

- تىكرى C9800-40-K9 تەيكلساللا مكحتلا ةدحو.
- Cisco ISE: ليغشتلا ديق 3 رادصإلا حيحصت جمانرب
- C9130AXI-D زارطلا :لوصولا ةطقن جذومن
- الوحمل: 9200-L-24P

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

ةيساسأ تامولعم

نيمدختسملل تاداهش ردصي يذلا اهب صاخلا قدصملا عجرملا اهل تاسسؤملا مظعم ءاشنال همادختسإ نكمي جمدم تاداهش عجرم ISE نمضتي EAP-TLS ةقداصمل نييئاهنلاا ال يتلا تاهويرانيسلا يف EAP-TLS ةقداصم يف همادختسإ متيل نيمدختسملل تاداهش قدصملا عجرملا مادختسإ حبصي ،انكمم لماكلا قدصملا عجرملا مادختسإ اهيف نوكي اديفم ارمأ مدختسملا ةقداصمل ISE قدصملا

ةقداصمل لاعف لكشب ISE CA مادختسال ةبولطملا نيوكتلا تاوطخ دنتسملا اذه حضوي ققداصم قفدت .نييكلساللا نيمدختسملا

EAP-TLS ةقداصم قفدت



EAP-TLS ةقداصم قفدت

EAP-TLS قفدت يف تاوطخ

- 1. لوصولا ةطقنب يكلساللا ليمعلا طبتري (AP).
- .ةقداصم بلط لسرتو تانايبلا لاسرإب لوصولا ةطقن حمست ال ،ةلحرملا هذه يف .2
- 3. هباجتسإ ةيوهب بالطمك لمعي يذلا ليمعلا بيجتسي EAP.
- 4. تامولعم ەيجوت ةداعإب (WLC) ةيكلسالللا ةيلحملا ةكبشلا يف مكحتلا ةدحو موقت ةقداصملا مداخ ىلإ مدختسملا فرعم.
- .5 عدب ةمزح مادختساب ليمعلا ىلع RADIUS مداخ دري .5 EAP-TLS.
- .ةطقنلا هذه نم EAP-TLS ةثداحم أدبت .6
- ةحفاصم ةلااسر كلذ يف امب ،ةقداصملا مداخ ىلإ ىرخأ ةرم EAP-Response ليمعلا لسري .7 client_hello ىلإ ريفشت نييعت عم NULL.
- 8. ىلع يوتحت يتلا لوصولا يدحت ةمزح مادختساب ةقداصملا مداخ بيجتسي.

TLS server_hello Handshake message Certificate Server_key_exchange Certificate request Server_hello_done

:نمضتت يتلا EAP-RESPONSE ةلاسرب ليمعلا دري .9

Certificate (for server validation) Client_key_exchange Certificate_verify (to verify server trust) Change_cipher_spec TLS finished

:نمضتي لوصولل ايدحت RADIUS مداخ لسري ،ليمعلا ةقداصم حاجن دنع .10

Change_cipher_spec Handshake finished message

المداخ ةقداصمل ةئزجتلا نم ليمعلا ققحتي .11 RADIUS.

.TLS ةحفاصم ءانثأ رسلا نم ايكيمانيد ديدج ريفشت حاتفم قاقتشا متي .12

.سمتلملا ىلإ مث قدصملا ىل مداخلا نم EAP-SUCCESS ةل اسر لسرت .13

ةكبشلا ىلإ لوصولا EAP-TLS نيكمت مت يذلا يكلساللا ليمعلا عيطتسي .14 نآلا ةيكلساللا.

نيوكتلا

ةكبشلل يطيطختلا مسرلا



لماعملا ايجولوبوط

تانيوكتلا

.se و 9800 WLC و ISE :نينوكم نيوكتب موقن ،مسقلاا اذه يف

ISE نيوكت

مسقلاا اذه يف ةشاش تاطقل ةوطخ لك بحاصت .ISE مداخل نيوكتلا تاوطخ يلي اميف يئرملا هيجوتلا ريفوتل.



ISE مداخ نيوكت تاوطخ

ةكبش زاهج ةفاضإ

مدختساً ،ةكبش زاهجك (WLC) ةيكلساللاا ةيلحملا ةكبشلا يف مكحتلا ةدحو ةفاضإل ةيلاتلا تاداشرإلا:

- .ةكبشلا ةزهجأ < ةكبشلا دراوم < ةرادإ ىلإ لقتنا .1
- ةيلحملا ةكبشلا يف مكحتلا رصنع ةفاضإ ةيلمع ءدبل ةفاضإ+ ةنوقيأ رقنا .2 ةيكلساللاا (WLC).
- ةكبشلا يف مكحتلا رصنع نم لك عم اقبسم كرتشملا حاتفملا قباطت نم دكأت .3 بسانملا لاصتالا نيكمتل ISE مداخو (WLC) ةيكلساللا ةيلحملا.
- رسيألا نكرلا يف لاسراٍ قوف رقنا ،حيحص لكشب ليصافتلا عيمج لاخداٍ درجمب .4 نيوكتلا ظفحل يلفسلا

🔽 🗸 RADIUS Auth	entication Setting	gs		
RADIUS UDP Sett	ings			
Protocol	RADIUS			
Shared Secret	<u></u>		Show	
Use Second Sha	red Secret 🕠			
Se Se	cond Shared cret			Show
CoA Port	1700		Set To Default	

```
ةكبش زاهج ةفاضإ
```

يلخادلا قدصملا عجرملا نم ققحتلا

:ةيلاتلا تاوطخلا مدختسأ ،(CA) يلخادلا قدصملا عجرملا تادادعا نم ققحتلل

- قدصملا عجرملا تادادعإ < قدصملا عجرملا < تاداەشلا < ماظنلا < قرادالا ىلا لقتنا .1 .ةيلخادلا
- يلخادلا قدصملا عجرملا طيشنت ديكأتل قدصملا عجرملا دومع نيكمت نم دكأت .2

Щ	Bookmarks	Deployment	Licensing	Certificates	Loggin	g Maintenance	Upgrad	e Health	Checks Backu	р&
55	Dashboard	Contractor Marca								
망	Context Visibility	Certificate Mana	igement	Inter	nal C/	A Settings	📥 For disaste	r recovery it is re	commended to Export Inte	ernal
×	Operations	Certificate Authority ~								
U	Policy	Issued Certific	cates	Host Na	ame ^	Personas		Role(s)	CA, EST & OCSP Re	. (
20	Administration	Certificate Authority Certificat Internal CA Settings		ise3gen	vc	Administration, Monito	ring, Poli	STANDAL		ł
កា	Work Centers	Certificate Ter	mplates							

يلخادلا قدصملا عجرملا نم ققحتلا

ةقداصملا بولسأ ةفاضإ

صصخم ةيوه لسلست ةفاضإ .ةيوهلا ردصم تالسلست < ةيوهلا ةرادإ < ةرادا ىلإ لقتنا لخدملا ىلإ لوخدلا ليجست ردصم يف مكحتلل.

Identities	Groups	External Identity	Sources	Identity Sour	rce Sequences	Settings					
Identity S	ource Sequences										
Identity	dentity Source Sequence										
∽ Ider	ntity Source										
* Nam	e A	llow_EMP_Cert		7							
Descri	iption										
∼ Ce	Select Certific	sed Authentication	n Preio	oaded_Certific∽							
∽ Au	thenticatior	n Search List									
	A set of ident	ity sources that will be	accessed i	n sequence until fi	rst authentication s	ucceeds					
	Available			Selected							
	Internal Er	ndpoints		Internal Users]						
	Guest Use	ers									
	All_AD_Jo	oin_Points									
			$\overline{\mathbf{A}}$			\langle					

ةقداصملا بولسأ

ةداەشلا بلاق ديدحت

:ةيلاتلا تاوطخلا مدختسأ ،ةداهش بلاق ديدحتل

.تاداەشلا بلاوق < قدصملا عجرملا < تاداەشلا < ماظنلا < ةرادالا ىلإ لقتنا .1 ةوطخلا

ديدج ةداهش بلاق ءاشنإل ةفاضإ+ ةنوقيأ قوف رقنا .2 ةوطخلا

.بالاقل اSE مداخل يلحم ديرف مسا ريفوت 2.1

.\$UserName ىلع (CN) عئاشلا مسالا نييعت نم دكأت 2.2

.04 ناونع يلع (SAN) عوضوملل ليدبلا مسالا نييعت نم قرقحت 2.3 MAC.

2. 4 فيرعت فلم نييعت SCEP RA الا SCEP RA الا SCEP RA ال

ليمعلا ةقداصم نيكمتب مق ،عسوملا حاتفملا مادختسإ مسق يف 2.5.

Certificate Management >	Edit Certificate Template	
Certificate Authority ~	* Name	EAP_Authentication_Certificate_Template
Issued Certificates	Description	This template will be used to issue certificates for EAP Authentication
Certificate Authority Certificat	Subject	2
Internal CA Settings	Common Name (CN)	\$UserName\$ 🕠
Certificate Templates	Organizational Unit (OU)	Example unit
External CA Settings	Organization (O)	Company name
	City (L)	City
	State (ST)	State
	Country (C)	us
	Subject Alternative Name (SAN)	
	Кеу Туре	RSA 🗸
	Key Size	2048 ~ 4
	* SCEP RA Profile	ISE Internal CA
	Valid Period	730 Day(s) (Valid Range 1 - 3652)
	Extended Key Usage	Client Authentication Server Authentication

ةداەشلا بلاق

ةداەش لخدم ءاشنإ

ةيلاتلا تاوطخلا مدختسأ ،ليمعلا ةداهش ءاشنإل ةداهش لخدم ءاشنإل:

ةداەشلا ميدقت < ةزەجألا لخدم ةرادإ < ةرادإلا ىلإ لقتنا .1 ةوطخلا.

ةديدج لخدم ةحفص دادعإل ءاشنإ قوف رقنا .2 ةوطخلا.

ةلوەسب ەيلع فرعتلل لخدملل ديرف مسا ريفوتب مق .3 ةوطخلا.

8443. ىلإ اذه نييعت ؛ەيلع ةباوبلا لمعتل ذفنملا مقر رتخأ .3.1

3.2. لخدملا اذهل اهيلإ ISE عمتسي يتلا تاهجاولا ددح.

.ةيضارتفا لخدم تاداهش ةعومجمك تاداهشلا ةعومجم ةمالع ددح .3.3

مدختسملا ةيوەلا نزخم لسلست ىلإ ريشي يذلا ،ةقداصملا بولسأ ديدحت 4-3 لخدملا اذه ىلإ لوخدلا ليجست ةقداصمل.

ىلع .ةباوبلا ىلإ لوصولا اەئاضعأل نكمي يتلا ةدمتعملا تاعومجملا نيمضت -5-3 ىلإ نومتني نومدختسملا ناك اذإ نيفظوملا نيمدختسملا ةعومجم ددح ،لاثملا ليبس ةعومجملا ەذە.

.تاداەشلا ريڧوت تادادعإ نمض اەب حومسملا تاداەشلا بلاوق ديدحتب مق .3.6

Į	Bookmarks	Blocked List	BYOD	Certificate Prov	visioning	Client Provisioning
5	Dashboard	Port	als Se	ttings and	Custor	nization
Ъ	Context Visibility					
×	Operations	Portal Nar	ne:		Descri	ption:
U	Policy	EMP CE	RTIFICATE P	ORTAL		
•	Administration		- 54-			
•	Administration	Languag	e File			
ส์เ	Work Centers	Portal tes	t URL			
?	Interactive Features	Portal B	ehavior and	I Flow Settings	Portal Page	e Customization



Configure authorized groups

User account with Super admin privilege or ERS admin privilege will have access to the portal

Available	Chosen
Q ALL_ACCOUNTS (default) GROUP_ACCOUNTS (default) OWN_ACCOUNTS (default)	Employee
Choose all Fully qualified domain name (FODN):	Clear all

> Login Page Settings						
> Acceptable Use Polic	y (AUP) Page Settings					
> Post-Login Banner Page Settings						
> Change Password Settings						
 Certificate Portal Settings 						
Certificate Templates: *	EAP_Authentication_Certificate_Template × 🗸					

ةداەشلا لخدم نيوكت

ةباوبلا رابتخال URL ناونع قوف رقنلاب ةباوبلا رابتخإ كنكمي ،دادعإلا اذه لامتكا درجمبو. لخدملا ةحفص ءارجإلا اذه حتفي.

Customization
Description:

رابتخالاا لخدم ةحفصل URL ناونع

е	https://10.106.32.31:8443/certprovportal/PortalSetup.action?portal=45aea9cb-29c8-4f73-98bb-63543bba423a							
	CISCO Certificate Provisioning Portal							
	Sign On Welcome to the Certificate Provisioning Portal. Sign on with the username and password supplied to you. Username:							
	emp Password:							
	Sign On							

لخدملا ةحفص

يلخاد مدختسم ةفاضإ

ةيلاتان تاوطخلا مدختسأ ،صيخرتانا لخدم ربع ةقداصملل مدختسم ءاشنإل:

- .نيمدختسملا < تايوهلا < ةيوهلا ةرادإ < ةرادالا ىلإ لقتنا .
- . ماظنلا ىل مدختسم ةفاضإل رايخلا قوف رقنا.
- مق ،لاثملا ليبس ىلع .مدختسملا اەيلإ يمتني يتلا مدختسملا ةيوە تاعومجم ددح .3 نيفظوملا ةعومجم ىلإ مدختسملا نييعتب.

Identities	Groups	External	Identity S	ources	Identity Sour	ce Sequences	Settings				
Users Latest Manual Network Scan Res		Res	Netw	vork A	CCESS U	Sers		ी Delete	✓ Duplicate		
				Status	Username 🔨	Description	First Name	Last Name	Email Address	User Identity Groups	Admin
				Enabled	👤 emp				٢	Employee	

يلخاد مدختسم ةفاضإ

RADIUS جەنو ISE ةداەش ريڧوت لخدم نيوكت

ا جەن تاعومجم نيوكتب موقن ،نآلرا .ISE ةداەش ريڧوت لخدم دادعإ قباسلا مسقلا ىطغ ISE جەن تاعومجم نيوكتب موقن ،نآلر مدختسملا ةقداصمب حامسلل RADIUS

- ISE RADIUS جەن تاعومجم نيوكت .1
- . تاسايسلا تاعومجم < ةسايسلا ىلإ لقتنا.
- ةديدج جەن ةعومجم ءاشنإل (+) عمجلا ةمالع قوف رقنا .3.

نيمدختسملا ةقداصمل ةممصم ةطيسب تاسايس ةعومجم دادعإب مق ،لاثملا اذه يف مەتاداەش مادختساب.

Policy Sets		Reset Policyset Hitcounts Save							
Status Policy Set Name Description	Conditions	Allowed Protocols / Server Sequence Hits Actions View							
Q Search									
	E Wreiess_902.1X	Default Network Access							
ENP WIBBOS 022.1A MUU	Airespace-Airespace-Wian-Id EQUALS 17								

تاسايس ةعومجم

	entication	Policy(2)					
	Status	Rule Name	Conditions		Use	Hits	Actions
c							
					Allow_EMP_Cert 🛛 😒 🗸		
	0	Allow Certificate Authentication	E FAP-TIS		> Options		¢
					DenyAccess 🤕 🗸		
	0	Default			> Options		ŵ
> Auth	orization F	Policy - Local Exceptions					
> Auth	orization F	Policy - Globel Exceptions					
⊂Auth	orization F	Policy(2)					
				Results			
\odot	Status	Rule Name	Conditions	Profiles	Security Groups	Hits	Actions
c							
	۲	Authz Employee	E LAP-ILS	PermitAccess 0 +	Employees 🥒 +		¢
	۲	Default		DenyAccess 0 +			ŵ

ضيوفتلاو ةقداصملا تاسايس ضرعت جەن ةعومجم

9800 WLC نيوكت

ا ميف (WLC) قيكلساللاا قيلحملاا قكبشلا يف مكحتلا ةدحوب ةصاخلا نيوكتلا تاوطخ يلي اميف يئرملا هيجوتلا ريفوتل مسقلا اذه يف ةشاش تاطقلب ةوطخ لك قافرا متي .9800 زارط.



WLC نيوكت تاوطخ

9800 WLC داخ ةفاضإ

- مداخ جمدل .1 مداخ جمدل .1 مداخ جمدل اللا من مكحتلال الله عن الله عن الله عن الله عن الله عن الله عن المداخ م الما تاوطخل :
- 2. نامألا < نيوكتلا يلإ لقتنا AAA.
- .3 نيوكت يف ISE مداخ نيمضتل ةفاضإ رزلا قوف رقنا.

Configuration * > Security * > AAA	Show Me How			
+ AAA Wizard				
Somers / Crowne Add Mathed Link				
Servers / Groups AAA Method List	Create AAA Radius Server			
	Name*	ISE3	Support for CoA (1)	ENABLED
RADIUS	Server Address*	10.106.32.31	CoA Server Key Type	Clear Text 🚽
TACACS+	PAC Key	0	CoA Server Key 👔	
LDAP	Кеу Туре	Clear Text 🗸	Confirm CoA Server Key	
	Key* 👔		Automate Tester	0
	Confirm Key*			
	Auth Port	1812		
	Acct Port	1813		
	Server Timeout (seconds)	1-1000		
	Retry Count	0-100		

مداوخلا ةمئاق يف رەظي ،مداخلا ةفاضإ درجمب.

Servers / Groups	AAA Method Lis	t AAA Au	dvanced							
+ Add	× Delete									
RADIUS		Servers	Server Groups							
TACACS+										
1040			Name	Ŧ	Address	т	Auth Port	٢	Acct Port	Ŧ
LDAP			ISE3		10.106.33.23		1812		1813	

RADIUS مداوخ ضرع

9800 WLC ىلع مداوخ ةعومجم ةفاضإ

لمكأ ،9800 ةيكلساللا (LAN) ةيلحملا ةكبشلا يف مكحتلا ةدحو ىلع مداوخ ةعومجم ةفاضإل ةيلاتلا تاوطخلا:

- 1. نامألا < نيوكتلا يلإ لقتنا 1. AAA <
- مداوخ ةعومجم ءاشنإل ةفاضإ قوف رقنا مث ،مداوخلا ةعومجم بيوبتلا ةمالع قوف رقنا .2 ةديدج.

Configuration * > Security * > AA	A Show Me How 📀		Edit AAA Radius Server G	roup
+ AAA Wizard	Ŧ		Name*	ISE
Servers / Groups AAA Method Lis	st AAA Advanced		Group Type	RADIUS
-+ Add X Delete			MAC-Delimiter	none 🔻
			MAC-Filtering	none 👻
RADIUS	Servers Server Groups		Dead-Time (mins)	1-1440
TACACS+			Load Balance	DISABLED
LDAP	Name	▼ Server 1		
	ISE ISE	ISE3	Source interface VLAN ID	2124
	H ≺ 1 ≻ H 10 ▼		Available Servers	Assigned Servers
				ISE3
				- <
				×
				(C)

RADIUS مداوخ ةعومجم ىلإ ISE مداوخ طيطخت

9800 WLC ىلع AAA قرط ةمئاق نيوكت

ةيلاتلا تاوطخلا مادختساب ةقداصملا قرط ةمئاق نيوكتب مق ،مداوخلا ةعومجم ءاشنإ دعب:

- AAA قرط ةمئاق < AAA < نامألا < نيوكتلا ىلإ لقتنا .1.
- .ةديدج ةقداصم قرط ةمئاق فضأ ،ةقداصملا بيوبت ةمالع يف .2
- .dot1x ىلع عونلا طبضا .3
- .ةعومجم عونك ةعومجم ددح .4
- .مداوخ تاعومجمك اقبسم اهئاشنإب تمق يتلا ISE مداوخ تاعومجم نيمضتب مق .5

Configuration * > Security * > AA	A Show Me How 💽	Quick Setup: AAA Authenti	cation
+ AAA Wizard		Method List Name*	CERT_AUTH
Servers / Groups AAA Method L	.ist AAA Advanced	Туре*	dot1x v (
		Group Type	Buonb 🔺 🔅
Authentication	+ Add × Delete	Failback to local	0
Authorization		Available Server Groups	Assigned Server Groups
Accounting	Name Y Type Y Group Type	radius	
- Subbanang	CERT_AUTH dot1x group	Idap	
			с Ж
			٢

ةقداصملا قرط مئاوق ءاشنإ

9800 WLC ىلع ضيوفتلا قرط ةمئاق نيوكت

ةيلاتا تاوطخلا مدختسأ ،ليوختلا قرط ةمئاق دادعإل:

- 1. قرط ةمئاق مسق لخاد ضيوفتلا بيوبتلا ةمالع ىلإ لقتنا.
- .ةديدج ليوخت قرط ةمئاق ءاشنإل ةفاضإ قوف رقنا .2
- .عونك ةكبشلا رتخأ .3
- .ةعومجم عونك ةعومجم ددح .4
- .مداوخ ةعومجمك ISE مداوخ ةعومجم نيمضتب مق .5

Configuration * > Security * >	> AAA Show Me How 📀	Quick Setup: AAA Authoriza	ation
+ AAA Wizard		Method List Name*	CERT_AUTH
Servers / Groups AAA Meth	thod List AAA Advanced	Type*	network 🔹
		Group Type	
Authentication		Fallback to local	0
Authorization		Authenticated	
Accounting	Name Y Type Y Group Type	Ausilable Server Groune	Assimed Server Groups
	CERT_AUTH network group	mature control control	
	H ≪ 1 ▶ H 10 ₹	Idap	
		tacacs+	<

ليوختاا قرط ةمئاق ةفاضإ

9800 WLC ىلع جەن فيرعت فلم ءاشنإ

جهن فيرعت فلم ءاشنإ يف رمتسا ،RADIUS ةعومجم نيوكت لامتكا عم:

- .ةسايسلا < فيرعتلا تافلمو تامالعلا < نيوكتلا ىلإ لقتنا .1
- ديدج جەن فيرعت فلم ءاشنإل ةفاضإ قوف رقنا .2
- ايزكرم ءيش لك نوكي ،لاثملا اذه يف .جەنلا فيرعت فلمل ةبسانملا تاملعملا رتخاً .3 ليمعلاب ةصاخلا VLAN ةكبشك ربتخملاب ةصاخلا VLAN ةكبش مادختسا متيو.

Confi	guration * >	Tags & Profiles	> Policy	Edit P	olicy Profile			
+	Add >	: Delete	1 Clone		A Disabling a Policy or conf	iguring it in 'Enabled' state, will result in los	s of connectivity for clients associate	d with this Policy profile.
	Admin Y Status	Associated 0 🔻 Policy Tags	Policy Profile Name	Genera	a Access Policies (QOS and AVC Mobility Adva		
		۰.	CERT-AUTH					
			default-policy-profile	۱ I	lame*	CERT-AUTH	WLAN Switching Policy	
м	4 1 →	⊨ 10 ₹			Description	Enter Description	Central Switching	
				5	Status	ENABLED	Central Authentication	
					Passive Client	DISABLED	Central DHCP	ENABLED
					P MAC Binding	ENABLED	Flex NAT/PAT	DISABLED
					incrypted Traffic Analytics	DISABLED		

ةسايسلا فيرعت فلم نيوكت

General Access foncies QOS and AVC Wobling	
RADIUS Profiling	
HTTP TLV Caching	
DHCP TLV Caching	
WLAN Local Profiling	
Global State of Device Enabled i	
Local Subscriber Policy Name Search or Select	▼ 2
VLAN	
VLAN/VLAN Group 2124	• i
Multicast VLAN Enter Multicast VLAN	

ةسايسلا طيطخت ىلإ VLAN

ضيوفت نيوكت دنع RADIUS، بيوبتلا ةمالع يف AAA زواجت رايخ نيكمت نم دكأت يف مكحتلا ةدحول دادعإلا اذه حمسي .ةسايسلا فيرعت فلم تادادعإب ةصاخلا ةمدقتملا

Access Policies QOS and AVC Mobility Advanced General Fabric WLAN Timeout Link-L Session Timeout (sec) 1800 mDNS Idle Timeout (sec) 300 Policy Idle Threshold (bytes) 0 Hotspo Client Exclusion Timeout (sec) \checkmark User I 60 Guest LAN Session Timeout Status Drop L DHCP DNS I $\overline{}$ IPv4 DHCP Required DHCP Server IP Address DNS L Param Show more >>> Flex D for DN AAA Policy Flex D Redire \square Allow AAA Override

ىلع RADIUS ىلإ ةدنتسملا ليوختلا تاسايس قيبطتب ةيكلساللا ةيلحملا ةكبشلا ةزهجألاو نيمدختسملا.

AAA زواجت

9800 WLC ىلع WLAN ةكبش ءاشنإ

:ةيلاتلا تاوطخلا مدختسأ ،802.1x ةقداصمب ةديدج WLAN ةكبش دادعإل

1. تاكبش < فيرعتلا تافلمو تامالعلا < نيوكتلا ىلإ لقتنا.

2. ةديدج WLAN ةكبش ءاشنإل ةفاضإ رقنا.

. 802.1x ةقداصم نيكمتب مقو 2 ةقبطلا ةقداصم تادادعإ ددح .3

Configuration * > Tags & Profiles * > WLANs	Edit WLAN	;
Add × Delete Cione Enable WLAN Disable WLAN Selected WLANs : 0	General Security Advanced Add To Policy Tags	
Status y Name y ID	Layer3 AAA	
R-webauth 10 0	• WPA + WPA2 • WPA3 • WPA3 • Static WEP • None	
	MAC Filtering	
	Lobby Admin Access	
	MPSK Configuration Enable MPSK	

WLAN فيرعت فلم نيوكت

General	Security	Advance	d Add To Poli	cy Tags
Layer2	Layer3	AAA		
Authe	ntication List		CERT_AUTH	▼ 2
Local	EAP Authentica	tion		

قرطلا ةمئاق ةطيرخ ىلإ WLAN فيرعت فلم

9800 WLC ىلع جەنلا فيرعت فلم عم WLAN ةطيرخ

:ةيلاتلا تاوطخلا مدختسأ ،ةسايس فيرعت فلمب كب ةصاخلا WLAN ةكبش نارقإل

- .زييمت تامالع < فيرعت تافلمو زييمت تامالع < نيوكتلا ىلإ لقتنا
- .ةديدج زييمت ةمالع ةفاضإل ةفاضإ قوف رقنا .2
- 3. فيرعت فلم ىلإ اثيدح هؤاشنإ مت يذلا WLAN نييعتب مق WLAN-policy مسق يف بسانملا ةسايسلا.

Configuration * > Tags & Profiles * > Tags	Edit Policy Tag
Policy Site RF AP	▲ Changes may result in lass of connectivity for some clients that are associated to APs with this Policy Tag.
+ Add X Delete	Name* CERT_POLICY_TAG
Policy Tag Name	Description Enter Description
CERT_POLICY_TAG	
default-policy-tag	V WLAN-POLICY Maps: 1
N 4 1 > N 10 v	
	+ Add × Delete
	WLAN Profile Y Policy Profile Y
	CERT-AUTH CERT-AUTH
	1 - 1 of 1 items

ةسايسلا ةمالع نيوكت

9800 WLC ىلع لوصولا ةطقن ىلإ جەنلا ةمالع ةمجرت

:ةيلاتلا تاوطخلا لمكأ ،(AP) لوصو ةطقنل جەنلا ةمالع نييعتل

- .AP < زييمت تامالع < تافيصوتو زييمت تامالع < نيوكتلا ىلإ لقتنا .1
- 2. لوصولا ةطقن نيوكت نمض "يكيتاتسإ نكاس" مسقلا ىل لقتنا.
- اەنيوكت ديرت يتلا ةددحملا لوصولا ةطقن ىلع رقنا .3.
- . ةددحملا لوصولا ةطقنل اهئاشنإب تمق يتلا جەنلا ةمالع نييعتب مق

Policy	Site RF	AP				▲ Changing Tags wi	I cause the AP to moment not all	arily lose a owed while	ssociation changing
Tag So	ource Static	Location Filter							
						AP MAC Address*	cc7f.75ae.1fc0		
Numb	per of AP Tag mapping	as selected : 0			Select File	Policy Tag Name	CERT_POLICY_TAG 🔻		
	AP MAC Address		Ţ	Policy Tag Name		Site Tag Name	default-site-tag 🗸		
	a4b4.392a.8dfc			default-policy-tag		RF Tag Name	default-rf-tag 👻		
4	cc7f.75ae.1fc0 < 1 ▶ ×	10 🔻		CERT_POLICY_TAG					

لوصولا ةطقن ةمالع نييعت

(WLC) ةيكلساللاا ةيلحملا ةكبشلا يف مكحتلا رصنع نيوكت ليغشت متي دادعإلا لامتكا دعب

```
aaa group server radius ISE
server name ISE3
ip radius source-interface Vlan2124
aaa authentication dot1x CERT_AUTH group ISE
aaa authorization network CERT_AUTH group ISE
aaa server radius dynamic-author
client 10.106.32.31 server-key Cisco!123
!
wireless profile policy CERT-AUTH
aaa-override
ipv4 dhcp required
vlan 2124
```

```
no shutdown
```

wlan CERT-AUTH policy CERT-AUTH
wlan CERT-AUTH 17 CERT-AUTH
security dot1x authentication-list CERT_AUTH
no shutdown
!
wireless tag policy CERT_POLICY_TAG
wlan CERT-AUTH policy CERT-AUTH

مدختسملل ةداهش ليزنتو ءاشنإ

ةيلاتات المعامية المردخة المرابع المرابع

اقبسم ەدادعإ مت يذلا ةداەشلا لخدم ىل مدختسملا لوخد ليجستب مق .1.

8 Not Secure	https://10.106.32.31:8443/certprovportal/PortalSetup.action?portal=45aea9cb-29c8-4f73-98bb-63543bba423a
	Certificate Provisioning Portal
	Sign On Welcome to the Certificate Provisioning Portal. Sign on with the username and password supplied to you. Username:
	emp Password:
	Sign On

ةداهشلا لخدم ىلإ لوصولا

- .ةداەشلا ءاشنإل ةحفص كلذ دعب ISE مدقي .(AUP) لوبقملا مادختسالا ةسايس لوبق .2
- .(ةداەش عيقوت بلط نودب) ةدرفم ةداەش ءاشنإ ددح .3



Certificate Provisioning	
	I want to: *
	Generate a single certif 1 (without a certificat
	Common Name (CN): *
	emp 2
	MAC Address: *
	242f.d0da.a563
	Choose Certificate Template: *
	EAP_Authentication_Certificate_Template
	Description:
	Certificate Download Format: *
	PKCS12 format, including certificate chain (
	Certificate Password: * 5
	Enter password to download and view/install the certificate
	Confirm Password: *
	Generate Reset

ةداەشلا ءاشنإ

ةيمازلإلاا لوقحلا هذه لاامتكا نم دكأت ،ةداهشلا ريفوت لخدم ربع ةداهش ءاشنإل:

- ةداەش يف عئاشلا مسالا لقح يف ةمدقملا ةميقلا ةقداصملا مداخ مدختسي :نإ يس يذلا) مدختسملا مسا لخدأ ،"عئاشلا مسالا" لقح يف .ام مدختسم ةقداصمل ليمعلا (ةداەشلا ريفوت لخدم ىلإ لوخدلا ليجستل ەتمدختسأ.
- تاونع MAC: Subject Alternative Names (SAN) قحلم وه (X.509 قحلم وه Cisco ISE، اناونع بنامأ قداهشب ناونع لقح يف ،يلاتلابو .طقف MAC ناونع 2.0 رادصإلا SAN/MAC.
 - عجرملا اهمدختسي يتلا لوقحلا نم ةعومجم ةداهشلا بلاق ىدحتي :ةداهشلا بلاق لثم لوقح مادختسإ متي .ةداهش رادصإو ام بلط ةحص نم ققحتلا دنع قدصملا مسا CN قباطي نأ بجي) بلطلا ةحص نم ققحتلل (CN) عئاشلا مسالا رادصإ ءانثأ قدصملا عجرملا لبق نم ىرخألا لوقحلا مدختست .(مدختسملا

.ةداەشلا

- ريفوت كيلع بجي .كتداهش نيمأتل صيخرت رورم ةملك ىلإ جاتحت :ةداهشلا رورم ةملك زاهجلا ىلع ةداهشلا داريتساو ةداهشلا تايوتحم ضرعل ةداهشلا رورم ةملك.
- ياتا دعاوقلا عم كب ةصاخلا رورملا ةملك قفاوتت نأ بجي:
- مقرو دحاو ريغص فرجو لڨألا ىلع دحاو يلالهتسإ فرح ىلع رورملا ةملك يوتحت نأ بجي دحاو
 - افرح 15 و 8 نيب رورملا ةملك لوط حوارتي نأ بجي 🔹
 - ⊮ ,. a-z، a-z، 0-9 اهب حومسملا فرحألا نمضتت ∘

ةداەشلا ليزنتو ءاشنإل ءاشنإ ددح ،لوقحلا لك ةئبعت درجمب.

ليغشتلا ماظنب لمعي زاهج ىلع ةداەشلا تيبثت 10

ل ةيرادإلا مكحتلا ةدحو حتفا ،Windows 10 ليغشتلا ماظنب لمعي زاهج ىلع ةداهش تيبثتل Microsoft (MMC) :قيلاتا تاوطخلا مادختساب (MMC):



ةراشتساب حصني اذل ،Windows دادعإ ىلع ءانب تاميلعتلا هذه فلتخت دق :ةظحالم قئاثو Microsoft قئاثو

- .ليغشت مث ءدب ىلع رقنا .1
- 2. ابتكا mmc حتف متي للخدإلا حاتفم طغضاو "ليغشت" عبرملا يف Microsoft Management Console.
- :ةداەشلل ةيفاضإلا ةادألا ةفاضإ .3
- .ةيفاضإ ةادأ ةلازإ/ةفاضإ < فلم ىلإ لقتنا .4
- .ةفاضإ رقناو تاداهش رتخأ مث ،ةفاضإ ددح .5
- .ءاەنإ قوف رقناو ،يلحملا رتويبمكلا مث ،رتويبمكلا باسح ددح .6

يلحملا رتويبمكلا ىلع تاداەشلا ةرادإ تاوطخلا ەذە كل حيتت.

Console1 - [Console Root]					-	□_ ×
File Action View Favorites Window Help						- & ×
🗢 🔿 📷 🗟 🖬						
Console Root Add or Remov	ve Snap-ins			×	Actions	
					Console Root	-
You can select extensible snap	snap-ins for this console from the p-ins, you can configure which ex	se available on yo tensions are enabl	ur computer and configure the selected s ed.	set of snap-ins. For	More Actions	•
Available snap	ins:		Selected snap-ins:	1		
Snap-in	Vendor	^	Console Root	Edit Extensions		
activeX C	ontrol Microsoft Cor		Q ^I Certificates (Local Computer)	Remove		
G Authoriza	tion Manager Microsoft Cor					
 Component 	nt Services Microsoft Cor			Move Up		
Computer	Managem Microsoft Cor			Move Down		
T Device Ma	anager Microsoft Cor agement Microsoft and	Add >				
Event View	wer Microsoft Cor					
Folder	Microsoft Cor					
🕄 IP Securit	y Monitor Microsoft Cor					
📵 IP Securit	y Policy M Microsoft Cor					
Link to We	eb Address Microsoft Cor	~		Advanced		
Description:						
The Certificat	es snap-in allows you to browse t	he contents of the	certificate stores for yourself, a service	, or a computer.		
			_	OK Cancel	1.1	

Windows ل MMC مكحت ةدحو

:ةداەشلا داريتسإ .1 ةوطخلا

- .ةمئاقلا يف ءارجإ قوف رقنا .1.1
- .داريتسإ ددح مث ،ماهملا ةفاك ىلإ لقتنا .1.2
- ا.ەديدحتو كزاەج ىلع نزخملا تاداەشلا فلم عقوم دىدحتل تابلاطملا ربع مدقت .

← 😺 Certificate Import Wizard

File to Import

Specify the file you want to import.

C: \Users \admin \De	sktop\emp-2025-01-06_	_08-30-59\emp_C4-E9	-0. Browse
Note: More than on	e certificate can be stor	ed in a single file in the	e following formats:
Personal Informa	tion Exchange- PKCS #:	12 (.PFX,.P12)	
Cryptographic Me	essage Syntax Standard	- PKCS #7 Certificates	; (.P7B)
Microsoft Serializ	ed Certificate Store (.SS	т)	

ةداەشلا داريتسإ

ءاشنإ دنع اەتأشنأ يتلا رورملا ةملك لاخدإ كنم بلطي ،ةداەشلا داريتسإ ةيلمع ءانثأ ةداەشلا داريتسإ نم نكمتت ىتح ةقدب ەذە رورملا ةملك لاخدإ نم دكأت .لخدملا ىلع ةداەشلا حاجنب كزاەج ىلع اەتيبثتو.

I	Private key protection
	To maintain security, the private key was protected with a password.
	Type the password for the private key.
	Password:
	••••••
	Display Password
	Import options:
	Enable strong private key protection. You will be prompted every time the private key is used by an application if you enable this option.
	Mark this key as exportable. This will allow you to back up or transport your keys at a later time.
	Protect private key using virtualized-based security(Non-exportable)
	Include all extended properties.

ةداەشلا رورم ةملك لاخدإ

ةبسانملا تادلجملا ىلإ تاداەشلا لقن .2 ةوطخلا:

2.1. (يلحم رتويبمك) تاداەشلا ىلإ لقتناو (Microsoft (MMC) نم ةرادإلا مكحت ةدحو حتفا .يصخش دلجم

قدصملا عجرملا وأ رذجلا قدصملا عجرملا لثم) اهعاوناً ديدحتو تاداهشلا ةعجارم -2-2 (يصخشلا وأ طيسولا).

:بسانملا نزخملا ىل المداهش لك لقن 2.3

اهيف قوثوملا رذجلا ةداهش عجارم ىلإ لاقتنالا :رذجلا قدصملا عجرملا تاداهش 4-2.

.ةطسوتملا قيدصتلا تاطلس يلإ لاقتنالا :ةطيسولا CA تاداهش 5-2

🗧 🐓 Certificate Import Wizard	×
Certificate Store Certificate stores are system areas where certificates are kept.	
Windows can automatically select a certificate store, or you can specify a location for the certificate. Automatically select the certificate store based on the type of certificate Place all certificates in the following store Certificate store:	
Personal Browse	
Next Can	icel
يصخشلا دلجملا يف تاداهشلا نيزخت	

Console Root	Issued To	Issued By	Expiration Date	Intended Purposes	Friendly Name	Statu
 Certificates (Local Computer) 	Gentificate Services Endpoint Sub CA - ise3genvc	Certificate Services Node CA - ise3genvc	1/3/2035	<all></all>	EndpointSubCA	
V Personal	Certificate Services Node CA - ise3genvc	Certificate Services Root CA - ise3genvc	1/3/2035	<all></all>	certificate_nodeCA	
Certificates	Certificate Services Root CA - ise3genvc	Certificate Services Root CA - ise3genvc	1/3/2035	<all></all>	certificate	
Certificater	😰 emp	Certificate Services Endpoint Sub CA - ise3genvc	1/6/2027	Client Authentication	emp_C4-E9-0A-00	
Enterprise Trust	📮 ise3genvc.lab.local	ise3genvc.lab.local	1/3/2027	Server Authentication, Client Authentication	Self-Signed	
> intermediate Certification Auth						



Windows زاهج ليصوت

ةكبشلاب لاصتالل ةيلاتا تاوطخلا مدختساً ،ةحيحصلا نزاخملا ىلا تاداەشلا لقن درجمب (WLAN) قيكلساللا قيلحملا

- . ةحاتملا ةيكلساللا تاكبشلا ضرعل ماظنلا جرد يف ةكبشلا زمر ىلع رقنا .1
- ِلاصتالا يَّف بُغرت َيتلاأ (WLAN) ةيكلساللاا ةيلحملا ةكبشلا مسا ىلع رقناو ثحبا .2 اهب.
- مادختساب ليصوتلا ةيلمع لامكإل ةيفاضإ تابلاطم ةيأ عباتو ليصوت ىلع رقنا .3 ةقداصملل كتداهش.

臣	AVctest Connected
₽ <i>(</i> (,	blizzard
°.	CERT-AUTH Secured
	Connect automatically
	Connect

ةيكلساللا ةكبشلاب ليصوتلا

رايخ ددح ،(WLAN) ةيكلساللاا ةيلحملا ةكبشلاب ليصوتلا ةيلمع ءانثأ كنم بلطي امدنع صيخرت مادختساب ليصوتلا.

17.	CERT-AUTH Secured						
	Enter your user name and password						
	User name						
	Password						
[Connect using a certificate						
	ОК	Cancel					

دامتعا تانايبك ةداەشلا مادختسإ

حاجنب صيخرتاا مادختساب ةيكلسالالا ةكبشاب ليصوتاا اذه كل حيتي.

C:\>netsh wlan show interface 200% There is 1 interface on the system: : Wi-Fi 3 Name Description : TP-Link Wireless USB Adapter : ee5d1c47-43cc-4873-9ae6-99e2e43c39ea GUID Physical address : 24:2f:d0:da:a5:63 State : connected SSID : CERT-AUTH BSSID : a4:88:73:9e:8d:af Network type : Infrastructure Radio type : 802.11ac Authentication : WPA2-Enterprise Cipher : CCMP Connection mode : Profile Channel : 36 Receive rate (Mbps) : 360 Transmit rate (Mbps) : 360 Signal : 100% Profile : CERT-AUTH

Hosted network status : Not available

C:\>netsh wlan show profiles CERT-AUTH | find "Smart" EAP type : Microsoft: Smart Card or other certificate

يكلساللا فيصوتلا نم ققحتلا

ةحصلا نم ققحتلا

:WLC لا ةطساوب ثبلا ديق نوكي WLAN لا نأ تققد

<#root>

POD6_9800#show wlan summ Number of WLANs: 2 ID Profile Name SSID Status Security

17

CERT-AUTH

CERT-AUTH

UP [WPA2][802.1x][AES]

: WLC لا قوف نوكي ap لا نأ تققد

:WLAN ةكبش ثبت لوصولا ةطقن نأ نم دكأت

<#root>

POD6_9800#show ap name AP1 wlan dot11 24ghz Slot id : 0 WLAN ID BSSID

17 a488.739e.8da0

POD6_9800#show ap name AP1 wlan dot11 5ghz Slot id : 1 WLAN ID BSSID

17

a488.739e.8daf

EAP-TLS: مادختساب ليمعلا لاصتا

<#root>

POD6_9800#show wire cli summ Number of Clients: 1 MAC Address AP Name Type ID State Protocol Method Role

242f.dOda.a563 AP1 WLAN

17

IP Learn 11ac

Dot1x

Local

POD6_9800#sho wireless client mac-address 242f.d0da.a563 detail | in username|SSID|EAP|AAA|VLAN

Wireless LAN Network Name (SSID): CERT-AUTH

BSSID : a488.739e.8daf

EAP Type : EAP-TLS

VLAN : 2124 Multicast VLAN : 0 Cisco Radius ISE: ل ةيحلا تالجسلا

Ø	← Reset Rep	peat Counts	$ riangle$ Export To \checkmark				
	Status	Details	Identity	Endpoint ID	Authentication Policy	Authoriz	Authoriz If
			Identity	Endpoint ID	Authentication Policy	Authorizatic	Authorizatic I
	•	G			EMP Wireless 802.1x Auth >> Allow Certificate Authenti	EMP Wirel	PermitAcc
		G			EMP Wireless 802.1x Auth >> Allow Certificate Authenti	EMP Wirel	PermitAcc

ISE Radius Live تالجس

:يليصفتلا ةقداصملا عون

Authentication Details

Source Timestamp	2025-01-08 11:58:21.055
Received Timestamp	2025-01-08 11:58:21.055
Policy Server	ise3genvc
Event	5200 Authentication succeeded
Username	emp
Endpoint Id	24:2F:D0:DA:A5:63
Calling Station Id	24-2f-d0-da-a5-63
Endpoint Profile	TP-LINK-Device
Identity Group	User Identity Groups:Employee,Profiled
Audit Session Id	4D084E0A0000007E46F0C6F7
Authentication Method	dot1x
Authentication Protocol	EAP-TLS
Service Type	Framed
Network Device	lab-9800
Device Type	All Device Types
Location	All Locations
NAS IPv4 Address	10.78.8.77
NAS Port Type	Wireless - IEEE 802.11
Authorization Profile	PermitAccess
Security Group	Employees

ةيليصفتلا ISE تالجس

مزح رەظي يذلاا WLC EPC طاقتلاا EAP-TLS:

I e	ар							× •
No.	Tin	me	Source	Destination	Protocol	Length	Info	
	65 17	7:36:58	Cisco_9e:8d:af	TpLinkPte_da:a5:63	EAP	95	Request, Identity	
	68 17	7:36:58	Cisco_9e:8d:af	TpLinkPte_da:a5:63	EAP	95	Request, Identity	
	69 17	7:36:58	TpLinkPte_da:a5:63	Cisco_9e:8d:af	EAP	110	Response, Identity	
	70 17	7:36:58	TpLinkPte_da:a5:63	Cisco_9e:8d:af	EAP	110	Response, Identity	
	73 17	7:36:58	Cisco_9e:8d:af	TpLinkPte_da:a5:63	EAP	96	Request, TLS EAP (EAP-TLS)	
	74 17	7:36:58	TpLinkPte_da:a5:63	Cisco_9e:8d:af	TLSv1.2	304	Client Hello	
	78 17	7:36:58	Cisco_9e:8d:af	TpLinkPte_da:a5:63	EAP	182	Request, TLS EAP (EAP-TLS)	
	79 17	7:36:58	TpLinkPte_da:a5:63	Cisco_9e:8d:af	EAP	110	Response, TLS EAP (EAP-TLS)	
	83 17	7:36:58	Cisco_9e:8d:af	TpLinkPte_da:a5:63	EAP	178	Request, TLS EAP (EAP-TLS)	
	84 17	7:36:58	TpLinkPte_da:a5:63	Cisco_9e:8d:af	EAP	110	Response, TLS EAP (EAP-TLS)	
	87 17	7:36:58	Cisco_9e:8d:af	TpLinkPte_da:a5:63	TLSv1.2	248	Server Hello, Certificate, Server Key Exchange, Certificate Request, Server Hello Done	
	95 17	7:36:58	TpLinkPte_da:a5:63	Cisco_9e:8d:af	EAP	640	Response, TLS EAP (EAP-TLS)	
	100 17	7:36:58	Cisco_9e:8d:af	TpLinkPte_da:a5:63	EAP	96	Request, TLS EAP (EAP-TLS)	
	102 17	7:36:58	TpLinkPte_da:a5:63	Cisco_9e:8d:af	EAP	640	Response, TLS EAP (EAP-TLS)	
	107 17	7:36:58	Cisco_9e:8d:af	TpLinkPte_da:a5:63	EAP	96	Request, TLS EAP (EAP-TLS)	
	109 17	7:36:59	TpLinkPte_da:a5:63	Cisco_9e:8d:af	EAP	640	Response, TLS EAP (EAP-TLS)	
	114 17	7:36:59	Cisco_9e:8d:af	TpLinkPte_da:a5:63	EAP	96	Request, TLS EAP (EAP-TLS)	
	115 17	7:36:59	TpLinkPte_da:a5:63	Cisco_9e:8d:af	TLSv1.2	347	Certificate, Client Key Exchange, Certificate Verify, Change Cipher Spec, Encrypted Hand	shake Message
	118 17	7:36:59	Cisco_9e:8d:af	TpLinkPte_da:a5:63	TLSv1.2	147	Change Cipher Spec, Encrypted Handshake Message	
	119 17	7:36:59	TpLinkPte_da:a5:63	Cisco_9e:8d:af	EAP	110	Response, TLS EAP (EAP-TLS)	
	126 17	7:36:59	Cisco_9e:8d:af	TpLinkPte_da:a5:63	EAP	94	Success	

EAP ةكرح رەظي يذلا WLC طاقتلا

- .ةقيثولاا ةيادب يف فصي قفدت EAP-TLS لا يف 8 ةوطخلا 87 مقر طبر لثامي •
- .ةقيثولاا ةيادب يف فصي قفدت EAP-TLS لا يف 9 ةوطخلاا 115 مقر طبر لثامي •
- .ةقيثولا ةيادب يف فصي قفدت EAP-TLS لا يف 10 ةوطخلا 118 مقر طبر لثامي •

عبتت Radio Active (RA) ددع ضرعل اذه RA عبت ةيفصت تمت :ليمعلا لاصتا رهظي يذلا ةقداصملا ةكرجل ةلصلا تاذ دونبلا نم ليلق.

متى (debug) [15655] approx [15655] approx [2025/01/08 11 58 20.816875191 {wncd_x_r0-2}] 499 لوطلا، [5256]DTLS .ةرفشملا DTLS ةراسر لاسرا بالط لاسرا RADIUS (تامولعم) [15655] wncd_x_r0-2}{1} [radius] [15655] (تامولعم) 2025/01/08 11 58 20.85139212 10.106.33.23 1812 id 0/25، len 390 يل إلوصول ا مت RADIUS (تامول عم) [15655] RADIUS (wncd_x_r0-2]{1} [radius] (تامول عم) RADIUS (م id 1812/25 10.106.33.23، Access-Challenge، len 123 نم ەيقلت 2025/01/08 11 58 20.872246323 {wncd_x_r0-2}{1} [dot1x] [15655] (تامولعم) [242f.d0da.a563 -EAP ،6، EAP قارمحلاا لوط ،EAP عونلاا عونلاا عونلاا - APOL قمزح لاسرا مت [2080005] -capwap_9080005 EAP-TLS = عونلا 2025/01/08 11 58 20.881960763 {wncd_x_r0-2}{1} [dot1x] [15655] (تامول عم) [242f.d0da.a563 ، 204، ةلومحلا لوط ،EAP عونلا APOL رادصإلا - EAPOL ةمزح مالتسإ مت [EAPOL مراح مالتس EAP-Type = EAP-TLS لالسرا RADIUS (تامولعم) [15655] wncd_x_r0-2}{1} [radius] (تامولعم) RADIUS (تامولعم) المحافي (1582292551 [wncd_x_r0-2} 10.106.33.23 1812 id 0/26، len 663 يل إلوص ول ابل ط مت RADIUS (تامولعم) [15655] wncd_x_r0-2}{1} [radius] (تامولعم) RADIUS (تامولعم) هي RADIUS (تامولعم) id 1812/26 10.106.33.23، Access-Challenge، len 1135 نم ەىقلت 2025/01/08 11 58 20.927390754 {wncd_x_r0-2}{1} [dot1x] [15655] (تامول عم) [242f.d0da.a563 ،1012 ةلومحلا لوط ،EAP عونلا المجافي المجافي المجافي المجافي المجافي المجافي المجافي (ما يوم ،capwap_9080005 والمجافي المجافي ا EAP-Type = EAP-TAP Is 2025/01/08 11 58 20.935081108 {wncd_x_r0-2}{1} [dot1x] [15655] (تامول عم) [242f.d0da.a563 عون ،6 ةلومحلا لوط ،EAP عونلا I،EAPOL رادصإلا - EAPOL ةمزح مالتسإ مت [EAPOL 2080005 مرز مالتس EAP = EAP-TLSلالسرا RADIUS (تامولعم) [15655] wncd_x_r0-2]{1} [radius] (تامولعم) RADIUS (تامولعم) المحافي (158 20.935405770) 10.106.33.23 1812 id 0/27، len 465 ىلإ لوصولا بلط مت RADIUS (تامولعم) [15655] RADIUS (مت المولعم) [15655] wncd_x_r0-2}{1} [radius] (تامولعم) [15655] مت id 1812/27 10.106.33.23، Access-Challenge، len 1131 نم ەىقلت 2025/01/08 11 58 20.939630108 {wncd_x_r0-2}{1} [dot1x] [15655] (تامول عم) [242f.d0da.a563 ، 1008 ةلومحلا لوط ،EAP عونلا S،EAPOL رادصإلا - EAPOL ةمزح لاسرا مت [EAPOL عونلا - 20800]

EAP-TTAP Is عونلI-EAP

2025/01/08 11 58 20.947417061 {wncd_x_r0-2}{1} [dot1x] [15655] (تامولعم) [242f.d0da.a563 capwap_9080005] مزح مالتسإ مت EAPOL - ارادصإلاا EAP = EAP-TLS

لالسرا 2025/01/08 11 58 20.947722851 {wncd_x_r0-2}{1} [radius] [15655] (تامولعم) RADIUS (تامولعم) 8000 السرا ال

مت RADIUS (تامولعم) [15655] wncd_x_r0-2}{1} [radius] (تامولعم) RADIUS (تامولعم) مت 1812/28 10.106.33.23، Access-Challenge، len 275

2025/01/08 11 58 20.950432303 {wncd_x_r0-2}{1} [dot1x] [15655] (تامولعم) [242f.d0da.a563 capwap_9080005] قمزح لاسرإ مت EAPOL - رادصإلا - 3،EAPOL عونلا EAP-Type = EAP-TLS

2025/01/08 11 58 20.966862562 {wncd_x_r0-2}{1} [dot1x] [15655] (تامولعم) [242f.d0da.a563 capwap_9080005] قمزح يقالت مت EAPOL - ارادصإلاا EAP-Type = EAP-TAP Is

لااسرا RADIUS (تامولعم) [15655] wncd_x_r0-2}{1} [radius] (تامولعم) RADIUS (تامولعم) الماسرا (15653) عل الماسرا 2025/01/08 المراجع (15653) الماسرا (15653) الماسرا (15653) من الماط (15653) من الماط (15653) من الماط (

2025/01/08 11 58 20.97137739 {wncd_x_r0-2}{1} [radius] [15655] (تامولعم) RADIUS (تامولعم) نام id 1812/29 10.106.33.23، Access-Challenge، len 123

2025/01/08 11 58 20.971708100 {wncd_x_r0-2}{1} [dot1x] [15655] (تامولعم) [242f.d0da.a563 capwap_9080005] مزح لاسرا مت EAPOL - 3،EAPOL 3،EAPOL قمزح لاسرا مت EAP-TLS = عونلا

2025/01/08 11 58 20.978742828 {wncd_x_r0-2}{1} [dot1x] [15655] (تامولعم) [242f.d0da.a563 capwap_9080005] مزح يقلت مت EAPOL - ارادصإلاا EAP-Type = EAP-TAP Is

لالسراٍ RADIUS (تامولعم) [15655] RADIUS (تامولعم) [15655] wncd_x_r0-2} السراً 15655] (تامولعم) الماسراً 2025/01/08 ال

مت RADIUS (تامولعم) [15655] wncd_x_r0-2}{1} [radius] (تامولعم) RADIUS (تامولعم) مت 1 38 20.982535977 (التام في ال

2025/01/08 11 58 20.982907200 {wncd_x_r0-2}{1} [dot1x] [15655] (تامولعم) [242f.d0da.a563 capwap_9080005] مزح لاسرا مت EAPOL - الوط ،EAP عونلا APOL - عونلا عونلا عونلا عونلا عونلا عونلا عونلا عونلا عونل

2025/01/08 11 58 20.990141062 {wncd_x_r0-2}{1} [dot1x] [15655] (تامولعم) [242f.d0da.a563 capwap_9080005] قمزح يقالت مت EAPOL - ارادصإلا - 1،EAPOL قارومحال لوط ،EAP عونال EAP-Type = EAP-TAP Is

لالسراٍ RADIUS (تامولعم) [15655] RADIUS (سراٍ 150.3023 wncd_x_r0-2} السراً) [15655] (تامولعم) المولي المرابي ال علاّ الموصول الم

مت RADIUS (تامولعم) [15655] RADIUS (تامولعم) في المرابع (يامولعم) المحكون (يامولعم) من 105.323 (يام مي المحكون من ما مي المحكون (يام مي المحكون المحكو

2025/01/08 11 58 20.994722151 {wncd_x_r0-2}{1} [dot1x] [15655] (تامولعم) [242f.d0da.a563 capwap_9080005] مونال EAPOL - مونال 3،EAPOL عونال EAP، ما ترم مت المريام عرف الوط ، EAP عونال المراب عن المراب الم

2025/01/08 11 58 21.00173553 {wncd_x_r0-2}{1} [dot1x] [15655] (تامولعم) [242f.d0da.a563 capwap_9080005] قمزح مالتسإ مت EAPOL - رادصإلا EAP-Type = EAP-TLS

لالسرا 2025/01/08 11 58 21.002076369 {wncd_x_r0-2}{1} [radius] [15655] (تامولعم) RADIUS (تامولعم) RADIUS (تامولعم) الماسرا 10.106.33.23 1812 id 0/32، len 706

مت RADIUS (تامولعم) [15655] RADIUS (wncd_x_r0-2}{1} [radius] (تامولعم) من RADIUS (تامولعم) من id 1812/32 10.106.33.23، Access-Challenge، len 174

2025/01/08 11 58 21.013987785 {wncd_x_r0-2}{1} [dot1x] [15655] (تامولعم) [242f.d0da.a563 capwap_9080005] قمزح لاسرا مت EAPOL - 3،EAPOL الوط ،EAP عونلا 57، EAP-عونلا = EAP-TLS

2025/01/08 11 58 21.02429150 {wncd_x_r0-2}{1} [dot1x] [15655] (تامولعم) [242f.d0da.a563 capwap_9080005] مزح مالتسإ مت EAPOL - ارادصإلاا EAP = EAP-TLS

لالسرإ RADIUS (تامولعم) [15655] wncd_x_r0-2}{1} [radius] (تامولعم) RADIUS (تامولعم) السريا 10.106.33.23 الما فا ب

2025/01/08 11 58 21.057794929 {wncd_x_r0-2}{1} [radius] [15655] (تامولعم) RADIUS يقلت مت (تامولعم) id 1812/33 10.106.33.23 0، Access-Accept، len 324

2025/01/08 11 58 21.058149893 {wncd_x_r0-2}{1} [dot1x] [15655] (تامولعم) [242f.d0da.a563 capwap_9080005] بولسأل ةيوهلا ثيدحت ثدح

اهحالصإو ءاطخألا فاشكتسا

اهحالصإو ءاطخألا فاشكتسأ تاءارجإ زواجتي اميف ةلكشملا هذه لحل ةددحم تاوطخ دجوت ال ةيجذومنلا ةيكلساللا 802.1x ةكبشب ةصاخلا:

- .ةقداصملا ةيلمع نم ققحتلل ليمعلل RA عبتت ءاطخاً حيحصت ذخأب مق .1
- .RADIUS مداخو WLC و ليمعلا نيب مزحلا صحفل WLC EPC طاقتلا ذيفنت .2
- .حيحصلا جەنلل بلطلا ةقباطم نم ققحتلل ةرشابملا ISE تالجس نم ققحت
- 4. ةلسلس دوجو نمو Windows ةياهن ةطقن ىلع حيحص لكشب ةداهشلا تيبثت نم ققحت. لماكلاب ةقثلاا.

عجارملا

- <u>ادصإلام الخدمال قدامشارا ريفوت الوح قا وادتمارا قل عاس ألا</u>
- ال يلخادل قدصمل عجرمل تامدخ مهف
- ISE و WLC مادختساب ەنيوكتو EAP-TLS مەف

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