ةكبشلل يلحملا EAP مداخ نيوكت لاثم ةدحوملا ةيكلساللا

المحتويات

<u>المقدمة</u> المتطلبات الأساسية المتطلبات المكونات المستخدمة الاصطلاحات تكوين EAP المحلي على وحدة التحكم في شبكة LAN اللاسلكية من <u>Cisco</u> تكوين EAP المحلي <u>هيئة شهادة Microsoft</u> التثبيت تثبيت الشهادة في وحدة التحكم في شبكة LAN اللاسلكية من Cisco تثبيت شهادة الجهاز على وحدة تحكم الشبكة المحلية اللاسلكية تنزيل شهادة CA للمورد إلى وحدة التحكم في الشبكة المحلية اللاسلكية قم بتكوين وحدة التحكم في الشبكة المحلية اللاسلكية لاستخدام EAP-TLS تثبيت "شهادة المرجع المصدق" على "الجهاز العميل" تنزيل شهادة مرجع مصدق جذري للعميل وتثبيتها إنشاء شهادة عميل لجهاز عميل EAP-TLS مع عميل Cisco Secure Services على جهاز العميل أوامر التصحيح معلومات ذات صلة

<u>المقدمة</u>

يصف هذا المستند تكوين خادم بروتوكول المصادقة المتوسع المحلي (EAP) في وحدة تحكم شبكة LAN اللاسلكية (WLC) من Cisco لمصادقة المستخدمين اللاسلكيين.

EAP المحلي هو أسلوب مصادقة يسمح للمستخدمين والعملاء اللاسلكيين بالمصادقة محليا. وقد تم تصميمه للاستخدام في المكاتب البعيدة التي ترغب في الحفاظ على الاتصال بالعملاء اللاسلكيين عند تعطل النظام الطرفي الخلفي أو تعطل خادم المصادقة الخارجي. عندما تقوم بتمكين EAP المحلي، فإن وحدة التحكم تعمل كخادم المصادقة وقاعدة بيانات المستخدم المحلية، وبالتالي إزالة الاعتماد على خادم مصادقة خارجي. يسترجع EAP المحلي مسوغات المستخدم من قاعدة بيانات المستخدم المحلية أو قاعدة بيانات الطرف الخلفي لبروتوكول الوصول إلى الدليل الخفيف (LDAP) لمصادقة المستخدمين. يدعم EAP المحلي المصادقة خارجي. يسترجع EAP المحلي والمصادقة المرنة EAP عبر الاتصال النفقي الآمن (EAP المحلي المصادقة خفيفة الوزن EAP) (EAP بين وحدة التحكم والعملاء اللاسلكيين.

لاحظ أن خادم EAP المحلي غير متوفر إذا كان هناك تكوين عالمي خارجي لخادم RADIUS في عنصر التحكم في الشبكة المحلية اللاسلكية (WLC). تتم إعادة توجيه جميع طلبات المصادقة إلى RADIUS الخارجي العام حتى يتوفر خادم EAP المحلي. إذا فقد عنصر التحكم في الشبكة المحلية اللاسلكية (WLC) الاتصال بخادم RADIUS الخارجي، يصبح خادم EAP المحلي نشطا. في حالة عدم تكوين خادم RADIUS العمومي، يصبح خادم EAP المحلي نشطا فورا. لا يمكن إستخدام خادم EAP المحلي لمصادقة العملاء، المتصلين بمجموعات WLC أخرى. بمعنى آخر، يتعذر على عنصر التحكم في الشبكة المحلية اللاسلكية (WLC) إعادة توجيه طلب EAP الخاص به إلى عنصر تحكم في الشبكة المحلية اللاسلكية (WLC) آخر للمصادقة. يجب أن يكون لكل عنصر تحكم في الشبكة المحلية اللاسلكية (WLC) خادم EAP محلي خاص به وقاعدة بيانات فردية.

ملاحظة: أستخدم هذه الأوامر لمنع WLC من إرسال الطلبات إلى خادم RADIUS خارجي .

config wlan disable config wlan radius_server auth disable config wlan enable

ويدعم خادم EAP المحلي هذه البروتوكولات في إصدار البرنامج 4.1.171.0 والإصدارات الأحدث:

- قفزة
- EAP-FAST (اسم المستخدم/كلمة المرور، والشهادات)
 - EAP-TLS •

<u>المتطلبات الأساسية</u>

<u>المتطلبات</u>

توصي Cisco بأن تكون لديك معرفة بالمواضيع التالية:

- معرفة كيفية تكوين نقاط الوصول في الوضع Lightweight (LAPs) و WLCs للتشغيل الأساسي
- معرفة ببروتوكول نقطة الوصول في الوضع Lightweight (LWAPP) وطرائق الأمان اللاسلكية
 - معرفة أساسية بمصادقة EAP المحلية.

<u>المكونات المستخدمة</u>

تستند المعلومات الواردة في هذا المستند إلى إصدارات البرامج والمكونات المادية التالية:

- Windows XP مع بطاقة مهايئ CB21AG و Cisco Secure Services Client، الإصدار 4.05
 - وحدة التحكم في شبكة LAN اللاسلكية 4.1.171.0 Cisco
 - المرجع المصدق ل Microsoft على خادم Windows 2000

<u>الاصطلاحات</u>

راجع <u>اصطلاحات تلميحات Cisco التقنية للحصول على مزيد من المعلومات حول اصطلاحات المستندات.</u>

<u>تكوين EAP المحلي على وحدة التحكم في شبكة LAN اللاسلكية من Cisco</u>

يفترض هذا وثيقة أن التشكيل أساسي من ال WLC أتمت بالفعل.

<u>تكوين EAP المحلي</u>

أتمت هذا steps in order to شكلت EAP محلي:

1. إضافة مستخدم صاف محلي:من واجهة المستخدم الرسومية. أختر **تأمين > مستخدمي الشبكة المحلية > جديد**،

أدخل اسم المستخدم، كلمة المرور، مستخدم الضيف، معرف WLAN، والوصف، وانقر تطبية

					58 <u>v</u> e Ci	ningurauon <u>P</u>	تطبيق.
cisco	MONITOR WLANS (WIRELESS	<u>S</u> ECURITY	MANAGEMENT	C <u>O</u> MMANDS	HELP
Security	Local Net Users > N	lew	Ľ		1	< Back	Apply
General	User Name	eapuser2					/
■ RADIUS Authentication	Password	•••••				· · · · ·	
TACACS+	Confirm Password	•••••					
Local Net Users MAC Filtering	Guest User						
User Login Policies AP Policies	WLAN ID	1	*				
Local EAP General	Description	Employee us	er local databa	ase			

من ال CLI أنت يستطيع استعملت **ال** <wlan id> description **/ CLI أ**نت يستطيع استعملت **ال** <**config netuser add** */ وpassword* (المر إلى سطر ثان لأسباب مكانية.

Cisco Controller) >config netuser add eapuser2 cisco123 1 Employee user local database)

حدد أمر إسترجاع بيانات اعتماد المستخدم.من واجهة المستخدم الرسومية، أختر **تأمين > EAP محلي > أولوية⁄**. **المصادقة**. ثم حدد LDAP، وانقر زر <" وانقر **تطبيق**. وهذا يضع بيانات اعتماد المستخدم في قاعدة البيانات المحلية

								ولا.
cisco	MONITOR	WLANS	CONTROLLER	WIRELESS	SECURITY	MANAGEMENT	COMMANDS	HErb
Security	Priority 0	rder > L	ocal-Auth					
 AAA General RADIUS Authentication Accounting TACACS+ Authentication Accounting Authentication Accounting Authentication LDAP Local Net Users MAC Filtering Disabled Clients User Login Policies AP Policies 	LDAP	ientials C	LOCAL U	P WN	,			-
▼ Local EAP Profiles EAP-FAST Parameters Authentication Priority								

من واجهة سطر الاوامر: (Cisco Controller) >**config local-auth user-credentials local**

3. إضافة توصيف EAP:أخترت in order to أتمت هذا من ال gui، **أمن>محلي EAP>توصيفات** وطقطقة **جديد**. عندما تظهر النافذة الجديدة، اكتب اسم ملف التخصيص وانقر **تطبيق**.

	MON	ITOR	WLANS	CONTROLLE	R WIREL	ESS SECU	RITY MANA	GEMENT	COMMANDS	HELP						
	Loc	al EAR	Profiles										Net	m	A	pply
	Pro	file Na	me	U	EAP	EAP-FAST		EAP-TI	.5				1			
													/			
												/				
												-				
rs																
ty																
WORK	100	us Mir	000750115	D WIDE EEE	SECTION V	MANAGEMENT	004844405	HE D								gout Befri
Loca		Drafile	- S Man	w marcoo	Secondit	Personal	Characters	nep.						1 Bach	1.2	Analy
F0CI	U EAP	Prome	5 > 146W											< SACK		Apply
Profi	le Narr	se				EAP-test										

يمكنك أيضا القيام بذلك باستخدام أمر CLI **config local-auth eap-profile add** <profile-name>. في المثال الخاص بنا، يكون اسم التوصيف هو *إختبار EAP*. (Cisco Controller) >**config local-auth eap-profile add** *EAP-test*

4. إضافة أسلوب إلى ملف تعريف EAP.من واجهة المستخدم الرسومية أختر **تأمين > EAP محلي > توصيفات** وانقر على اسم التوصيف الذي تريد إضافة أساليب المصادقة له. يستخدم هذا المثال LEAP و EAP-FAST و EAP-TLS. طقطقة **يطبق** in order to ثبتت الأسلوب.

CISCO MONITOR MUNITOR CONTROLLER WIRELESS SECURITY MUNAGEMENT COMMANDS HELP
Security Local EAP Profiles
* AAA Profile Name LEAP EAP-FAST EAP-TLS General * PADEUS R
CISCO MONITOR MUNIT CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP
Security Local EAP Profiles > Edit
* AAA Profile Name EAF-test
EADIUS Authentication LEAP
Accounting 9 TACACS+ EAP-FAST
Local Net Users EAP-TLS
Disabled Clients User Login Policies AP Policies AP Policies AP Policies
Local EAP Client Certificate Required P Enabled
Profiles EAP-FAST Parameters Certificate Issuer Vendor
Authentication Priority Priority Order Check against CA certificates F Enabled
Access Central Lists Verify Certificate CN Identity Enabled
IPSec Certs

يمكنك أيضا إستخدام أمر CLI config local-auth eap-profile **طريقة إضافة <-sprofile> sprofile ه**ي كلك أيضا إستخدام أمر CLI config local-auth eap-profile طريقة إضافة <-sprofile هي **chame** . في مثال التكوين الخاص بنا نضيف ثلاث طرق إلى إختبار EAP لملف التعريف. وهذه الأساليب هي LEAP و EAP-FAST و EAP على التوالي. يبدي هذا إنتاج ال CLI تشكيل أمر:

Cisco Controller) >config local-auth eap-profile method add leap EAP-test) Cisco Controller) >config local-auth eap-profile method add fast EAP-test) Cisco Controller) >config local-auth eap-profile method add tls EAP-test) قم بتكوين معلمات أسلوب EAP. لا يستخدم هذا إلا مع EAP-FAST. المعلمات التي سيتم تكوينها هي:**مفتاح**ً. **الخادم (مفتاح الخادم)**—مفتاح الخادم لتشفير/فك تشفير مسوغات الوصول المحمي (PACs) (بالسداسي العشري).**مدة البقاء ل PAC (PAC-TTL)** - يحدد وقت عيش PAC.**معرف السلطة (معرف السلطة)** — يحدد معرف السلطة.ا**لحكم المسمى (anon-provn)** - يحدد ما إذا كان الحكم المغفل مسموحا به. مكنت هذا افتراضيا.للتكوين من خلال واجهة المستخدم الرسومية، أختر **التأمين > EAP محلي > معلمات (لعدا**م وأدخل مفتاح الخادم، ووقت للعيش من أجل مسوغ الوصول المحمي (PAC)، وقيم معلومات معرف

المرجع.

المثال:

MONITOR WLANS CONTROLLER WIRELESS	RITY MANAGEMENT COMMANDS	HELP
EAP-FAST Method Parameters		
Server Key (in hex)		
Confirm Server Key		
Time to live for the PAC	10	days
Authority ID (in hex)	43697	36367
Authority ID Information	Cisco	A-ID
Anonymous Provision	RE	nabled

هذه هي أوامر تكوين CLI التي يجب إستخدامها لتعيين هذه المعلمات ل EAP-FAST: Cisco Controller) >config local-auth method fast server-key 12345678) Cisco Controller) >config local-auth method fast authority-id 43697369f1 CiscoA-ID) Cisco Controller) >config local-auth method fast pac-tt1 10)

6. تمكين المصادقة المحلية لكل شبكة محلية لاسلكية:من واجهة المستخدم الرسومية (GUI) أختر **شبكات WLAN** من القائمة العليا وحدد شبكة WLAN التي تريد تكوين المصادقة المحلية لها. تظهر نافذة جديدة. انقر فوق **التأمين >** تبويبات AAA. تحقق من **مصادقة EAP المحلية** وحدد اسم ملف تعريف EAP الأيمن من القائمة المنسدلة كما يوضح هذا

lili. cisco	MONITOR WLANS CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP	
WLANs	WLANs > Edit	
 WLANS WLANS AP Groups VLAN 	General Security QoS Advanced Layer 2 Layer 3 AAA Servers	
	Select AAA servers below to override use of default servers on this WLAN Radius Servers Authentication Servers Accounting Servers	LDAP Servers Server 1 None
	Server 1 None None Server 2 None None None Server 3 None None Server 3 N	Server 3 None
	Local EAP Authentication F Enabled EAP Profile Name EAP-test	

يمكنك أيضا إصدار أمر التكوين CLI **config wlan local-auth enable** *<profile-name> <wlan-id* **كما هو موضح هنا:** 7. ضبط معاملات أمان الطبقة 2.من واجهة واجهة المستخدم الرسومية، في نافذة تحرير الشبكة المحلية اللاسلكية (WLAN)، انتقل إلى **التأمين >** علامات تبويب **الطبقة 2** واختر WPA+WPA2 من القائمة المنسدلة تأمين الطبقة 2. تحت قسم معلمات WPA+WPA2، اضبط تشفير WPA على TKIP و WPA2 تشفير AES. ثم انقر فوق

	طبيق.	ü
	Sage Configuration Bing Logout Befrest	1
CISCO	MONITOR WLANS CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP	
WLANs	WLANs > Edit < Back Apply	^
	General Security Qo5 Advanced	
WLANS	Laver 7 Laver 3 AAA Servers	
AP Groups VLAN		
	Layer 2 Security WPA+WPA2	
	MAC Filtering	
	WPA+WPA2 Parameters	
	WPA Policy	
	WPA Encryption	
	Auth Key Mamt 802.1X Y	
	ين ال CLI، استعملت هذا أمر:	٥
	Cisco Controller) >config wlan security wpa enable 1)
	Cisco Controller) >config wlan security wpa wpa1 ciphers tkip enable 1)
	Cisco Controller) >config wlan security wpa wpa2 ciphers aes enable 1)
	لتحقق من التكوين:	8. 1
	Cisco Controller) > show local-auth config)
	:User credentials database search orde:	r
	:Time:	r
	Active timeout Undefined	
	:Configured EAP profile:	S
	Certificate issuer	
	:Peer verification options	
	Check against CA certificates Enabled	
	Verify certificate CN identity Disabled	
	Check certificate date validity Enabled	
	:EAP-FAST configuration	
	Client certificate required	
	Enabled methods leap fast tls	
	Configured on WLANs 1	
	:EAP Method configuration	a
	More or (g)uit-	_

Cisco Controller) >**show wlan 1**)

WLAN Identifier..... 1

<Server key <hidden TTL for the PAC 10 Anonymous provision allowed Yes

I	Profile Name austinlab
1	Network Name (SSID)austinlab
	Status Disabled
	MAC Filtering Disabled
	Broadcast SSID Enabled
	AAA Policy Override Disabled
	Number of Active Clients 0
Ez	cclusionlist Timeout
Ses	sion Timeout 1800 seconds
II	iterface management
WLAI	1 ACL unconfigured DHCP Server Default
	DHCP Address Assignment Required Disabled
(Quality of	Service Silver (best effort
	WMM Disabled CCX - Aironetle Support Enabled
	CCX - Gratuitous ProbeResponse (GPR) Disabled
	Dot11-Phone Mode (7920) Disabled
	Wired Protocol None
	TPuc Support Disabled
	Radio Policy All
('Local EAP Authent'	ication Enabled (Profile 'EAP-test
(local lin nationed	Security
Aut	chentication:
	Static WEP Keys Disabled
	802.1X Disabled
	Wi-Fi Protected Access (WPA/WPA2) Enabled
	WPA (SSN IE) Enabled
	TKIP Cipher Enabled
	AES Cipher Disabled
	WPA2 (RSN IE) Enabled
	TKIP Cipher Disabled
	AES Cipher Enabled
Auth Key Management	
	802.1x Enabled
	PSK Disabled
	CCKM Disabled
	CKIP Disabled
	IP Security Disabled
	IP Security Passthru Disabled
	Web Based Authentication Disabled
	More or (q)uit
	Web-PassthroughDisabled
	Conditional Web Redirect Disabled
	Auto Anchor Disabled
	Cranite Passtnru
	Fortress Passtnru
	H-REAP Local Switching
	Intrastructure MFP protection Enabled
(GIODAL INTRASTRUCT)	ITE MFF UISADIEA)
	Tkin MIC Countermeasure Hold-down Timer 60
	TATE THE Councerneasure nota-down timer 00
	Mobility Anchor List
	WLAN ID IP Address Status
النشطة. يقوم هذا المؤفت بتكوين	هناك معلمات مصادقة محلية اخرى يمكن تكوينها، وخاصة مؤفت المهلة
RADIU.م∴ واجهة المستخدم	الفترة التي يتم خلالها استخدام EAP المحلي بعد فشل جميع خوادم S
	السببية أخترت أمركمها وحملته المقترقية فرانقر فر
وق	الرسومية، اخترت امن<محني ====================================

تطبيق.



يمكنك التحقق من القيمة التي تم إعداد هذا المؤقت لها عند إصدار الأمر show local-auth config. (Cisco Controller) >show local-auth config

:Configured EAP profiles Name EAP-test Skip ...

9. إذا احتجت إلى إنشاء مسوغ الوصول المحمي اليدوي وتحميله، فيمكنك إستخدام واجهة المستخدم الرسومية (GUI) أو واجهة سطر الأوامر (CLI).من واجهة المستخدم الرسومية، حدد **الأوامر** من القائمة العليا واختر **تحميل الملف** من القائمة في الجانب الأيمن. حدد **PAC (مسوغات الوصول المحمي)** من القائمة المنسدلة نوع الملف. أدخل كافة المعلمات وانقر فوق

սիսիս						Sa⊻e Configur	ation <u>P</u> ing	تحميل. Logout <u>R</u> efres
CISCO	MONITOR <u>W</u> U	ANS <u>C</u> ONTROLLER	WIRELESS	<u>S</u> ECURITY	MANAGEMENT	COMMANDS	HELP	
Commands	Upload file fro	om Controller					Clear	Upload
Download File	File Type		PAC (Protect	ed Access Cred	fential) 🔽			
Reboot	User (Identity)	test1				/	
Reset to Factory Default Set Time	Validity (in da	γs)	60]				
	Password		•••••					
	Confirm Passy	vord	•••••					
	TFTP Server							
	IP Address		10.1.1.1					
	File Path		1					
	File Name		manual.pac					

? Cisco Controller) >transfer upload pac) username Enter the user (identity) of the PAC ? Cisco Controller) >transfer upload pac test1) Enter the PAC validity period (days> (validity> ? Cisco Controller) >transfer upload pac test1 60) password> Enter a password to protect the PAC> Cisco Controller) >transfer upload pac test1 60 cisco123) Cisco Controller) >transfer upload serverip 10.1.1.1) Cisco Controller) >transfer upload filename manual.pac) Cisco Controller) >transfer upload start) Mode..... TFTP TFTP Server IP..... 10.1.1.1 /TFTP Path TFTP Filename..... manual.pac Data Type..... PAC PAC User..... test1 PAC Password..... cisco123 Are you sure you want to start? (y/N) y .PAC transfer starting

هيئة شهادة Microsoft

من أجل إستخدام مصادقة EAP-FAST الإصدار 2 و EAP-TLS، يجب أن يكون لدى عنصر التحكم في الشبكة المحلية اللاسلكية (WLC) وجميع أجهزة العميل شهادة صالحة ويجب أن تعرف أيضا الشهادة العامة الخاصة بالمرجع المصدق.

<u>التثبيت</u>

إذا لم يكن Windows 2000 Server مثبتا عليه خدمات المرجع المصدق، يجب تثبيته.

.File transfer operation completed successfully

أكمل الخطوات التالية لتنشيط "مرجع مصدق Microsoft" على خادم Windows 2000:

1. من لوحة التحكم، أختر **إضافة/إزالة برامج**.



2. حدد **إضافة/إزالة مكونات Windows** على الجانب



Vindows Components Wizard	×
Windows Components You can add or remove components of Windows 2000.	
To add or remove a component, click the checkbox. A sha part of the component will be installed. To see what's inclu Details.	aded box means that only ded in a component, click
Components:	
- 🖂 📻 Accessories and Utilities	12.1 MB
🔍 😫 Certificate Services	1.4 MB
Indexing Service	0.0 MB
Internet Information Services (IIS)	21.6 MB
Management and Monitoring Tools	52MB
Description: Installs a certification authority (CA) to issue or public key security applications.	ertificates for use with
Total disk space required: 0.0 MB	Details
Space available on disk: 4205.9 MB	
< <u>B</u> ack	<u>N</u> ext > Cancel
	ِاجع هذا التحذير قبل
	لمتابعة:
licrosoft Certificate Services	×
After installing Certificate Services, the computer cannot be renamed a from a domain. Do you want to continue?	and the computer cannot join or be removed
<u>Y</u> es <u>N</u> o	

4. حدد نوع المرجع المصدق الذي تريد تثبيته. من أجل إنشاء مرجع مستقل بسيط، حدد المرجع المصدق CA الجذري المستقل.

lows Components Wizard		
Certification Authority Type There are four types of certification authorities.		
Certification Authority types:	Description:	
C Enterprise root CA	The most trusted CA in a CA	^
C Enterprise subordinate CA	Active Directory.	
Stand-alone root CA		
Stand-alone subordinate CA		Ŧ
Advanced options		
	(Back Next)	Canaal
		Cancel

5. إدخال المعلومات الضرورية حول المرجع المصدق. تنشئ هذه المعلومات شهادة موقعة ذاتيا للمرجع المصدق الخاص بك. تذكر اسم المرجع المصدق الذي تستخدمه.يخزن المرجع المصدق الشهادات في قاعدة بيانات. يستخدم هذا المثال الإعداد الافتراضي المقترح من قبل Microsoft:

dows Components Wizard	
Data Storage Location Specify the storage location for the configuration data, database	and log
<u>C</u> ertificate database:	
C:\WINNT\system32\CertLog	Browse
Certificate database log:	
C:\WINNT\system32\CertLog	Browse
Store configuration information a shared folder Shared folder:	Browse
Reserve existing certificate database	
Preserve existing certificate database	

6. تستخدم خدمات مصدقة Microsoft خادم ويب IIS من أجل إنشاء شهادات العميل والخادم وإدارتها. يجب إعادة تشغيل خدمة IIS لهذا

Microsoft	الغرض: 🗙
<u>.</u>	Internet Information Services is running on this computer. You must stop this service before proceeding. Do you want to stop the service now?
	OK Cancel

يقوم Microsoft Windows 2000 Server الآن بتثبيت الخدمة الجديدة. يجب أن يكون لديك القرص المضغوط الخاص بتثبيت Windows 2000 Server لتثبيت مكونات Windows الجديدة.تم تثبيت "المرجع المصدق" الآن.

<u>تثبيت الشهادة في وحدة التحكم في شبكة LAN اللاسلكية من Cisco</u>

لاستخدام EAP-FAST الإصدار 2 و EAP-TLS على خادم EAP المحلي لوحدة تحكم الشبكة المحلية اللاسلكية من Cisco، اتبع الخطوات الثلاث التالية:

- 1. <u>قم بتثبيت شهادة الجهاز على وحدة تحكم الشبكة المحلية اللاسلكية.</u>
- 2. <u>قم بتنزيل شهادة CA للمورد إلى وحدة التحكم في الشبكة المحلية اللاسلكية.</u>
- 3. <u>قم بتكوين وحدة التحكم في الشبكة المحلية اللاسلكية لاستخدام EAP-TLS.</u>

لاحظ أنه في المثال الموضح في هذا المستند، يتم تثبيت "خادم التحكم في الوصول" (ACS) على نفس المضيف الخاص ب Microsoft Active Directory و Microsoft Certificate Authority، ولكن يجب أن يكون التكوين هو نفسه إذا كان خادم ACS على خادم مختلف.

تثبيت شهادة الجهاز على وحدة تحكم الشبكة المحلية اللاسلكية

أكمل الخطوات التالية:

- 1. . أتمت هذا steps in order to خلقت الشهادة أن يستورد إلى ال WLC:انتقل إلى http://<serverAddr>/certsrv.أختر **طلب شهادة** وانقر **التالي**.أخترت **طلب متقدم** وطقطقة **بعد ذلك**.أختر **إرسال طلب شهادة إلى المرجع المصدق هذا باستخدام نموذج** وانقر فوق **التالي**.أختر **خادم ويب** لقالب الشهادة وأدخل المعلومات ذات الصلة. ثم وضع علامة **قابلة للتصدير على** المفاتيح.تتلقى الآن شهادة تحتاج إلى تثبيتها في جهازك.
 - 2. أتمت هذا steps in order to إستردت الشهادة من pc:افتح مستعرض Internet Explorer واختر **أدوات > خيارات الإنترنت > المحتوى**.انقر على **شهادات**.حدد الشهادة المثبتة حديثا من القائمة المنسدلة.طقطقة **يصدر**.طقطقت **بعد ذلك** مرتين واخترت **نعم يصدر المفتاح الخاص**. هذا التنسيق هو PKCS#12.) PKCS#12 تنسيق).أختر **تمكين الحماية القوية**.اكتب كلمة مرور.احفظه في ملف <tme2.pfx>.
 - 9. انسخ الشهادة بتنسيق PKCS#12 إلى أي حاسب حيث يكون OpenSSL مثبتا لتحويلها إلى تنسيق PKCS#12 مثبتا لتحويلها إلى تنسيق . openssl pkcs12 -in tme2.pfx -out tme2.pem The command to be given, -in Enter Import Password: --- Enter the password given ---! previously, from step 2g. MAC verified OK Enter PEM pass phrase: --- Enter a phrase. :Verifying - Enter PEM pass phrase
 - 4. قم بتنزيل شهادة جهاز تنسيق PEM المحولة على عنصر التحكم في الشبكة المحلية اللاسلكية (WLC). (Cisco Controller) >transfer download datatype eapdevcert

Cisco Controller) >transfer download certpassword password) From step 3. Setting password to <cisco123> (Cisco Controller) >transfer download ----! filename tme2.pem

Cisco Controller) >transfer download start)

	1	Iode	 		TFTP
Data	Туре		 Vendor	Dev	Cert
	TFTP S	Server IP	 	10.1	.1.12
		TFTP Packet Timeout	 	• • • •	6
		TFTP Max Retries	 	• • • •	10
		/	 	TFTP	Path
	TFTP	Filename	 	tme2	2.pem

. This may take some time Are you sure you want to start? (y/N) y

.TFTP EAP Dev cert transfer starting

.Certificate installed .Reboot the switch to use new certificate

5. بعد إعادة التشغيل، تحقق من الشهادة. Cisco Controller) >show local-auth certificates)

:Certificates available for Local EAP authentication

Certificate issuer vendor :CA certificate Subject: C=US, ST=ca, L=san jose, O=cisco, OU=wnbu, CN=tme Issuer: C=US, ST=ca, L=san jose, O=cisco, OU=wnbu, CN=tme Valid: 2007 Feb 28th, 19:35:21 GMT to 2012 Feb 28th, 19:44:44 GMT :Device certificate Subject: C=US, ST=ca, L=san jose, O=cisco, OU=wnbu, CN=tme Issuer: C=US, ST=ca, L=san jose, O=cisco, OU=wnbu, CN=tme Valid: 2007 Mar 28th, 23:08:39 GMT to 2009 Mar 27th, 23:08:39 GMT

<u>تنزيل شهادة CA للمورد إلى وحدة التحكم في الشبكة المحلية اللاسلكية</u>

أكمل الخطوات التالية:

- 1. أتمت هذا steps in order to إستردت البائع ca شهادة:انتقل إلى h**ttp://<serverAddr>/certsrv**.أخترت **يسترد ال CA شهادة** وطقطقة **بعد ذلك**.أختر شهادة المرجع المصدق.انقر فوق DER **المرمز**.انقر على **تنزيل شهادة** واحفظ الشهادة على هيئة **rootca.cer**.
- 2. قم بتحويل المرجع المصدق للمورد من تنسيق DER إلى تنسيق PEM باستخدام **الأمر openssl x509 -in** مر.ملف المخرجات هو rootca.cer -information der -out rootca.pem أمر.ملف المخرجات هو rootca.pem بتنسيق PEM.

```
3. تنزيل شهادة المرجع المصدق للمورد:
      Cisco Controller) >transfer download datatype eapcacert)
            ? Cisco Controller) >transfer download filename)
            Enter filename up to 16 alphanumeric characters>
.filename>
     Cisco Controller) >transfer download filename rootca.pem)
              ? Cisco Controller) >transfer download start)
                Cisco Controller) >transfer download start)
       Mode..... TFTP
Data Type..... Vendor CA Cert
   TFTP Server IP..... 10.1.1.12
          TFTP Packet Timeout...... 6
         TFTP Max Retries..... 10
          / .....TFTP Path
   TFTP Filename..... rootca.pem
                               .This may take some time
                   Are you sure you want to start? (y/N) y
                      .TFTP EAP CA cert transfer starting
                                .Certificate installed
                .Reboot the switch to use new certificate
```

<u>قم بتكوين وحدة التحكم في الشبكة المحلية اللاسلكية لاستخدام EAP-TLS</u>

أكمل الخطوات التالية:

من واجهة المستخدم الرسومية، أختر **تأمين > EAP محلي > توصيفات**، أختر التوصيف وفحص لهذه الإعدادات:

- تم تمكين الشهادة المحلية المطلوبة.
 - تم تمكين شهادة العميل المطلوبة.
 - مصدر الشهادة هو المورد.
- تم تمكين الفحص مقابل شهادات المرجع المصدق.

cisco	MONITOR MLANS CONTROLLER WIREL	ESS SECURITY MANAGEMENT COMMANDS HELP
Security	Local EAP Profiles > Edit	
- AAA	Profile Name	EAP-test
RADIUS Authentication	LEAP	7
* TACACS+	EAP-FAST	2
Local Net Users MAC Filtering	EAP-TLS	9
Disabled Clients User Login Policies AP Policies	Local Certificate Required	P Enabled
* Local EAP	Client Certificate Required	R trabled
Profiles EAP-FAST Parameters	Certificate Issuer	Vendor 🗵
Priority Order	Check against CA certificates	P Enabled
	Verify Certificate CN Identity	C Enabled
IPSec Certs Wireless Protection	Check Certificate Date Validity	C Enabled

تثبيت "شهادة المرجع المصدق" على "الجهاز العميل"

<u>تنزيل شهادة مرجع مصدق جذري للعميل وتثبيتها</u>

يجب أن يحصل العميل على شهادة مرجع مصدق الجذر من خادم مرجع مصدق. هناك عدة طرق يمكنك إستخدامها للحصول على شهادة عميل وتثبيتها على جهاز Windows XP. للحصول على شهادة صالحة، يجب تسجيل دخول مستخدم Windows XP باستخدام معرف المستخدم الخاص به ويجب أن يكون لديه اتصال شبكة.

تم إستخدام مستعرض ويب على عميل Windows XP واتصال سلكي بالشبكة للحصول على شهادة عميل من خادم المرجع المصدق الجذر الخاص. يستخدم هذا الإجراء للحصول على شهادة العميل من خادم مرجع مصدق من Microsoft:

- 1. أستخدم مستعرض ويب على العميل وقم بتوجيه المستعرض إلى خادم المرجع المصدق. للقيام بذلك، أدخل http://IP-address-of-Root-CA/certsrv.
- 2. سجل الدخول باستخدام Domain_name\user_name. يجب عليك تسجيل الدخول باستخدام اسم المستخدم الخاص بالشخص المراد إستخدام عميل XP.
 - 3. في نافذة الترحيب، أختر **إسترجاع شهادة CA** وانقر **بعد ذلك**.
 - 4. حدد **ترمیز Base64** و**تنزیل شهادة CA**.
 - 5. في الإطار "تم إصدار الشهادة"، انقر على **تثبيت هذه الشهادة** وانقر على **التالي**.
 - 6. أختر **تحديد مخزن الشهادات تلقائيا** وانقر فوق **التالي**، لرسالة إستيراد ناجحة.
 - 7. الاتصال بالمرجع المصدق لاسترداد شهادة المرجع المصدق:

Welcome

You use this web site to request a certificate for your web browser, e-mail client, or other secure program. Once you acquire a certificate, you will be able to securely identify yourself to other people over the web, sign your e-mail messages, encrypt your e-mail messages, and more depending upon the type of certificate you request.

Select a task:

Retrieve the CA certificate or certificate revocation list

Request a certificate

Check on a pending certificate

Microsoft Certificate Services - tme

Retrieve The CA Certificate Or Certificate Revocation List

Install this CA certification path to allow your computer to trust certificates issued from this certification authority.

It is not necessary to manually install the CA certification path if you request and install a certificate from this certification authority, because the CA certification path will be installed for you automatically.

Choose file to download:

CA Certificate: Current [tme]

OER encoded or OBase 64 encoded Download CA certificate Download CA certification path Download latest certificate revocation list

Download CA certification p

Download latest certificate

1

. • • 1 8

		٤. انقر على تنزيل شهادة المرجع
		المصدق.
Microsoft Certificate Services - tme		Home
Retrieve The CA Certificate Or Certifica	te Revocation List	
Install this CA certification path to allow you	r computer to trust certificates issued from this certification	authority.
It is not necessary to manually install the C/	File Download - Security Warning	this certification authority, because the
CA certification path will be installed for yo	Do you want to open or save this file?	,
Choose file to download:	Name: certnew.cer	
CA Certificate: Current [tme]	Error: 10.1.1.12	
⊙DER encoded or ⊘Ba	Dpen Save Cancel	
Download CA certificate		

While files from the Internet can be useful, this file type can potentially harm your computer. If you do not trust the source, do not open or save this software. What's the risk?

Next >

Home

Certificate Import Wizard



Welcome to the Certificate Import Wizard

This wizard helps you copy certificates, certificate trust lists, and certificate revocation lists from your disk to a certificate store.

A certificate, which is issued by a certification authority, is a confirmation of your identity and contains information used to protect data or to establish secure network connections. A certificate store is the system area where certificates are kept.

To continue, click Next.

< Back Next >

Cancel



Certificate Store

Certificate Import Wizard

he

Certificate stores are system areas where certificates are kept.

Windows can automatically select a certificate store, or you can specify a location for

Automatically select the certificate store based on the type of certificate

O Place all certificates in the following store

Certificate store:

Browse,..,

Next >

< Back

×



9. للتحقق من أن شهادة المرجع المصدق مثبتة بشكل صحيح، افتح Internet Explorer واختر **أدوات > خيارات** الإنترنت > المحتوى >



Internet Options ? 🔀
General Security Privacy Content Connections Programs Advanced
Content Advisor Ratings help you control the Internet content that can be viewed on this computer. Enable Settings
Certificates
Use certificates to positively identify yourself, certification authorities, and publishers.
Clear SSL State Certificates Publishers
Personal information
AutoComplete stores previous entries and suggests matches for you.
Microsoft Profile Assistant stores your My Profile
UK Cancel Apply

في هيئة شهادة الجذر الموثوق فيها، يجب أن ترى هيئة شهادة النظام التي تم تثبيتها حديثا:

Certificates						? 🗙
Intended purpose:	<all></all>	,				~
Intermediate Certifica	tion Au	thorities Trusted Root (Certification Aut	horities	Trusted Publ	< >
Issued To	[Issued By	Expiratio	Friend	ly Name	^
Thawte Server (Thawte Timestan tme UTN - DATACorp UTN-USERFirst-(UTN-USERFirst-1) UTN-USERFirst-1 UTN-USERFirst-1 UTN-USERFirst-1	CA mpi o SGC Clie Har Net Obj rcia	Thawte Server CA Thawte Timestamping tme UTN - DATACorp SGC UTN-USERFirst-Client UTN-USERFirst-Hardw UTN-USERFirst-Hardw UTN-USERFirst-Object VeriSign Commercial S	12/31/2020 12/31/2020 2/28/2012 6/24/2019 7/9/2019 7/9/2019 7/9/2019 7/9/2019 7/9/2019 12/31/1999	Thawte Thawte VNone UTN - U UTN - U UTN - U UTN - U VeriSign	e Server CA Timesta > DATACorp JSERFirst JSERFirst JSERFirst JSERFirst n Commer	
Import Exp Certificate intended p <all></all>	oort urpose	Remove			View	ed

إنشاء شهادة عميل لجهاز عميل

يجب على العميل الحصول على شهادة من خادم مرجع مصدق لمركز التحكم في الشبكة المحلية اللاسلكية (WLC) لمصادقة عميل WLAN EAP-TLS. هناك العديد من الطرق التي يمكنك إستخدامها للحصول على شهادة عميل وتثبيتها على جهاز Windows XP. للحصول على شهادة صالحة، يجب تسجيل دخول مستخدم Windows XP باستخدام معرف المستخدم الخاص به ويجب أن يكون لديه اتصال شبكة (إما اتصال سلكي أو اتصال WLAN مع تعطيل أمان 802.1x).

يتم إستخدام مستعرض ويب على عميل Windows XP واتصال سلكي بالشبكة للحصول على شهادة عميل من خادم المرجع المصدق الجذر الخاص. يستخدم هذا الإجراء للحصول على شهادة العميل من خادم مرجع مصدق من Microsoft:

- 1. أستخدم مستعرض ويب على العميل وقم بتوجيه المستعرض إلى خادم المرجع المصدق. للقيام بذلك، أدخل http://IP-address-of-Root-CA/certsrv.
 - 2. سجل الدخول باستخدام Domain_name\user_name. يجب تسجيل الدخول باستخدام اسم المستخدم الخاص بالشخص الذي يستخدم عميل XP. (يتم تضمين اسم المستخدم في شهادة العميل.)
 - 3. في نافذة الترحيب، أختر **طلب شهادة** وانقر **بعد ذلك**.
 - 4. أخترت **متقدم طلب** وطقطقة **بعد ذلك**.
 - 5. أختر **إرسال طلب شهادة إلى المرجع المصدق هذا باستخدام نموذج** وانقر فوق **التالي**.
- 6. في نموذج طلب الشهادة المتقدمة، أختر "قالب الشهادة" كمستخدم، وحدد حجم المفتاح على هيئة **1024** وانقر

علی **إرسال**.

7. في الإطار "إصدار الشهادة"، انقر على **تثبيت هذه الشهادة**. يؤدي هذا إلى تثبيت شهادة عميل بنجاح على عميل Windows

Y	D

AX.
Microsoft Certificate Services true Home
Welcome
You use this web site to request a certificate for your web browser, e-mail client, or other secure program. Once you acquire a certificate, you will be able to securely identify yourself to other people over the web, sign your e-mail messages, encrypt your e-mail messages, and more depending upon the type of certificate you request.
Select a task: O Retrieve the CA certificate or certificate revocation list O Request a certificate O Check on a pending certificate
Next >
Microsoft Certificate Services tme Home
Choose Request Type
Please select the type of request you would like to make:
User Certificate request:
 Advanced request
Next >
Microsoft Certificate Services tme Home
Advanced Certificate Requests
You can request a certificate for yourself, another user, or a computer using one of the following methods. Note that the policy of the certification authority (CA) will determine the certificates that you can obtain.
 Submit a certificate request to this CA using a form.
Submit a certificate request using a base64 encoded PKCS #10 file or a renewal request using a base64 encoded PKCS #7 file.
 Request a certificate for a smart card on behalf of another user using the Smart Card Enrolment Station. You must have an enrolment agent certificate to submit a request for another user.
Next >

8. حدد **شهادة مصادقة**

Certificate Tem	plate:
	User
Key Options:	
CSP	Microsoft Base Cryptographic Provider v1.0
Key Usage:	○ Exchange ○ Signature
Key Size:	512 Min: 384 (common key sizes: 512 1024) Map: 1024
	Oreate new key set
	Use existing key set
	Enable strong private key protection
	Mark keys as exportable Export keys to file
	Use local machine store You must be an administrator to generate a key in the local machine store.
Additional Optic	ons:
Hash Algorithm:	SHA-1 Only used to sign request.
	Save request to a PKCS #10 file
Attributes	

Certificates			?	×
Intended purpose:	<all></all>			~
Personal Other Peo	ple Intermediate Certificat	ion Authorities Truste	ed Root Certificatior 🤸	>
Issued To	Issued By	Expiratio	Friendly Name	
🕮 Administrator	tme	3/27/2008	<none></none>	
Import Ex Certificate intended p Encrypting File System	port Remove purposes m, Secure Email, Client Auth	entication	Advanced. View	

EAP-TLS مع عميل Cisco Secure Services على جهاز العميل

أكمل الخطوات التالية:

- 1. تقوم وحدة التحكم في الشبكة المحلية اللاسلكية (WLC)، بشكل افتراضي، ببث SSID، لذلك يتم عرضه في قائمة إنشاء شبكات من SSID الممسوحة ضوئيا. لإنشاء توصيف شبكة يمكنك النقر على SSID في القائمة (مشروع) والنقر على إ**نشاء شبكة**.إذا تم تكوين البنية الأساسية للشبكة المحلية اللاسلكية (WLAN) مع تعطيل (مشروع) والنقر على إ**نشاء شبكة**.إذا تم تكوين البنية الأساسية للشبكة المحلية اللاسلكية (WLAN) مع تعطيل (مشروع) والنقر على إ**نشاء شبكة**.إذا تم تكوين البنية الأساسية للشبكة المحلية اللاسلكية (WLAN) مع تعطيل (مشروع) والنقر على إ**نشاء شبكة**.إذا تم تكوين البنية الأساسية للشبكة المحلية اللاسلكية (WLAN) مع تعطيل معروف) والنقر على إ**نشاء شبكة**.إذا تم تكوين البنية الأساسية للشبكة المحلية اللاسلكية (WLAN) مع تعطيل (مشروع) والنقر على إنشاء شبكة. إذا تم تكوين البنية الأساسية للشبكة المحلية اللاسلكية (Roadcast SSID معرف SSID) مع تعطيل معرف SSID معرف SSID ، تكوين سلوك الاستكشاف النشط للعميل. وهذا معرف SSID المناسب يدويا (على سببل المثال، Enterprise). تكوين سلوك الاستكشاف النشط للعميل. وهذا هو المكان الذي يبحث فيه العميل بنشاط عن SSID المكون الخاص به. حدد البحث النشط عن جهاز الوصول هذا هو المكان الذي يبحث فيه العميل بنشاط عن SSID المكون الخاص به. حدد البحث النشط عن جهاز الوصول هذا هو المكان الذي يبحث فيه العميل بنشاط عن SSID المكون الخاص به. حدد البحث النشط عن جهاز الوصول هذا هو المكان الذي يبحث أيه العميل بنشاط عن SSID المكون الخاص به. حدد البحث النشط عن جهاز الوصول. ملاحظة: لا تسمح إعدادات المنفذ بأوضاع المؤسسات (802.1X) إذا لم تكن إعدادات مصادقة EAP مكونة لأول مرة للتوصيف.
 - 2. انقر على **إنشاء شبكة** لتشغيل إطار ملف تعريف الشبكة، والذي يسمح لك بإقران SSID الذي تم إختياره (أو تكوينه) بآلية مصادقة. قم بتعيين اسم وصفي لملف التعريف.**ملاحظة:** يمكن إقران أنواع أمان متعددة لشبكة WLAN و/أو SSIDs ضمن ملف تعريف المصادقة هذا.

		-	
Licco	Sacura	C	 Lie of
LISLU	SECURE	-11-11-12	

Client Administration Help

Access 🛆	Data Security
aruba-ap-config-in-the-clear (2 accesses dete	🚹 WEP
SII 6	🗕 Open
ccx5 (2 accesses detected)	💢 Open
il con	X Open
an con-eap	The WEP
001907351aa3 High Signal	WEP
guestnet (5 accesses detected)	💢 Open
guestnetwork	💢 Open
N-Rogue	🖀 WEP
secure-1 (3 accesses detected)	? Mixed
tme-test (5 accesses detected)	🖀 WPA
II trng1 (2 accesses detected)	1 WEP
Create Netv	work

- 🗆 ×

- 3. قم بتشغيل المصادقة وفحص أسلوب EAP-TLS. ثم انقر على **تكوين** لتكوين خصائص EAP-TLS.
 - 4. تحت تشكيل خلاصة، انقر على **تعديل** in order to شكلت ال EAP / مسوغات عملية إعداد.
 - 5. حدد **تشغيل المصادقة**، واختر **EAP-TLS** ضمن البروتوكول، واختر **اسم المستخدم** كهوية.
- 6. حدد **إستخدام بيانات اعتماد تسجيل الدخول الأحادي** لاستخدام بيانات اعتماد تسجيل الدخول لمصادقة الشبكة. انقر على **تكوين** لإعداد معلمات -EAP



Network Profile					×
Network					
Name: con-eap Ne	twork				_
🔽 Availabl	e to all users (pul	blic profile)			
T Automa	tically establish M	lachine conn	ection		
🔽 Automa	tically establish U	ser connecti	on		
I⊠ B	efore user accou	nt (supports :	martcard	/password only)	
Network Configuratio	n Summary:				
Authentication: E/	AP-TLS;				
Credentials: B	equest when nee	eded and rem	ember for	the session.	5
				[
				Modity	
Access Devices					
Access / SSID	Mode	Notes			-
con-eap	WPA2 Enterpris	se			-
Add	Modify (Configuration		Bemove	
			<u> </u>		
Help			OK	Cancel	

7. للحصول على تكوين EAP-TLS آمن يلزمك التحقق من شهادة خادم RADIUS. للقيام بذلك، تحقق من **التحقق من شهادة**

Configure EAP Metho	od	×
-EAP-TLS settings:		
Use Smartcard-base	ed Client Certificates Only	
Validate Server Cert	ificate	
🔽 Allow Fast Session F	Resumption	
Help	ОК	Cancel

8. للتحققُ من صحة شهادة خادم RADIUS، يلزمك منح معلومات Cisco Secure Services Client لقبول الشهادة الصحيحة فقط. أختر **عميل > خوادم موثوق بها > إدارة الخوادم الموثوق بها للمستخدم الحالي**.

Cisco Secure Services C	lient	
Client Administration Help		
Manage Adapters	and a l	
Trusted Servers 🔸	Manage Current User Trusted Ser	vers
Advanced Settings	Manage Machine / All Users Truste	ed Servers Data Seci
✓ Enable Client	vk Disconnected	
✓ Turn WiFi Radio On	Misconferred	
 Show System Tray 	Canable for	r web
Close Window	Configured	for: wpa2
Connect Manage Current User Tr	Configure Remove.	Details Status
Trusted Server Definition C	Current Users:	
Rule Name		Validation Method
Add Server Rule	Remove Selected	Edit Selected
Help		Close

9. قم بتسمية القاعدة وتحقق من اسم شهادة

	الخادم.
Trusted Server	×
Trusted Server Rule name: WLC-Config	
Validation method: Certificate	▼
Match ANY Certificate Validation Rule: Subject Alternative Name Exactly matches Subject/Common Name Exactly matches	▼ [tme
Help	OK Cancel

انتهی تکوین EAP-TLS.

10. التوصيل بتوصيف الشبكة اللاسلكية. يطلب Cisco Secure Services Client تسجيل دخول

Network 🛆	Enter Your Cred	lentials
E- Con Nei L- M con E- Con-eag		Please enter your credentials for network con-eap Network, access con-eap
		Username: Administrator
		Send Cancel
•		
		Details

ستقبل Cisco Secure Services Client شهادة الخادم ويتحقق منها (مع تكوين القاعدة وتثبيت المرجع

المصدق). ثم يطلب إستخدام الشهادة للمستخدم.

11. بعد مصادقة العميل، أختر SSID ضمن ملف التعريف في علامة التبويب إدارة الشبكات وانقر فوق **الحالة** للاستعلام عن تفاصيل الاتصال.يوفر إطار تفاصيل الاتصال معلومات عن جهاز العميل وحالة الاتصال وإحصاءاته وطريقة المصادقة. توفر علامة تبويب تفاصيل WiFi تفاصيل عن حالة توصيل 802. 11 الذي يتضمن RSSI والقناة 802. 11

التشفير.	المصادقة/ا	و
----------	------------	---

Selected Acces	\$	Status		Security
con-eap		Connected: Authentic	ated (AutoConn	WPA2
1:24:28.044 1:24:28.054 1:24:28.074 1:24:28.094 1:24:28.104 1:24:28.194 1:24:28.305 1:24:28.305 1:24:28.335 1:24:28.335 1:24:28.335 1:24:28.395 1:24:28.505 1:24:28.505 1:24:35.534	con-eap Networ Connection aut Port state transi Connection assi Connection assi Port state transi Identity has bee Identity has bee Authentication : The server has The client has is Validating the se Port state transi The authentica The following If	k Connection requested from hentication started using the log- tion to AC_PORT_STATE_UN ociation started using encryption ociation succeeded. tion to AC_PORT_STATE_CO tion to AC_PORT_STATE_AU in requested from the network. is sent to the network. started using method type EAP- requested using authentication equested using authentication river. tion to AC_PORT_STATE_AU tion process has succeeded. address has been assigned: 1	user context. gged in user's cred AUTHENTICATED n mode AC_ENCR, NNECTING(AC_P(THENTICATING(A -TLS, level 0 htype: EAP-TLS type: EAP-TLS type: EAP-TLS THENTICATED(A/ 10.10.80.24.	entials. JAC_PORT_STATUS_STARTED) _AES AC_ASSOC_111_8021X DRT_STATUS_LINK_UP) .c_PORT_STATUS_8021x_ACQUIRED C_PORT_STATUS_GROUP_KEY)
		Cle	ar	

Cisco Secure Services Client	
Client Administration Help	
Create Networks Manage Networks	1
Network 🛆	Status Data :
E- Con Network	Disconnected
💥 con	No Adapter Available (Suspended) 🛛 🗕 🕅
E- 🍋 con-eap Network	Connected: Authenticated
Con-eap	Connected: Authenticated (AutoConnect) 🔐 🔪
Disconnect Configure	Details Remove Status
	li.

Status:	Connected: Authenticated
Duration:	00:01:19
Network Profile:	con-eap Network
Cis Network Adapter:	co Aironet 802.11a/b/g Wireless Adapter (Microsoft's Packet Scheduler)
Client MAC Address:	00-40-96-A6-D6-F6
Access Device:	con-eap
Access Device MAC Address:	00-19-07-35-1A-AC
Transmitted packets:	346
Received packets:	3
Speed:	54.0 Mbps
Authentication Method:	EAP-TLS
Authentication Server:	tme2 (trusted)
IP Address:	10.10.80.24

أوامر التصحيح

تدعم <u>أداة مترجم الإخراج (للعملاءالمسجلين فقط) بعض أوامر</u> show. استخدم أداة مترجم الإخراج (OIT) لعرض تحليل مُخرَج الأمر show .

ملاحظة: ارجع إلى <u>معلومات مهمة حول أوامر التصحيح</u> قبل إستخدام أوامر debug.

يمكن إستخدام أوامر تصحيح الأخطاء هذه في عنصر التحكم في الشبكة المحلية اللاسلكية (WLC) لمراقبة تقدم تبادل المصادقة:

- debug aaa events enable •
- enable debug aaa detail •
- debug dot1x حادث یمکن
- enable الحالات debug dot1x •

- debug aaa local-auth eap events enable.
 - debug aaa all enable •

<u>معلومات ذات صلة</u>

- <u>دليل تكوين وحدة تحكم شبكة LAN اللاسلكية من Cisco، الإصدار 4.1</u>
 - <u>دعم تقنية WLAN</u>
 - الدعم التقني والمستندات Cisco Systems

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