# مكحت ةدحو ةحفص ەيجوت ةداعإ نيوكت لاتم ةيكلساللا LAN قكبش

## المحتويات

<u>المتطلبات الأساسية</u> المتطلبات المكونات المستخدم<u>ة</u> الاصطلاحات معلومات أساسية التكوين التكوين التكوين عنصر التحكم في الشبكة المحلية اللاسلكية (WLC) لمصادقة RADIUS من خلال خادم ACS الأمن من Cisco رائد من الخطوة 3. قم يتكوين شبكات WLAN لقسم "الإدارة" و"العمليات". الخطوة 3. قم يتكوين RCS الآمن من Cisco لدعم ميزة إعادة توجيه صفحة splash. التحقق من الصحة التحقق من الصحة

### <u>المقدمة</u>

يوضح هذا المستند كيفية تكوين ميزة إعادة توجيه صفحة البداية على وحدات التحكم في الشبكة المحلية (LAN) اللاسلكية.

### <u>المتطلبات الأساسية</u>

#### <u>المتطلبات</u>

تأكد من استيفاء المتطلبات التالية قبل أن تحاول إجراء هذا التكوين:

- معرفة حلول أمان LWAPP
- معرفة كيفية تكوين ACS الآمن من Cisco

#### <u>المكونات المستخدمة</u>

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

• وحدة التحكم في شبكة LAN اللاسلكية (WLC) من Cisco 4400 Series التي تشغل الإصدار 5.0 من البرنامج الثابت

- نقطة الوصول (LAP) خفيفة الوزن للسلسلة Cisco 1232 Series
- مهايئ العميل اللاسلكي Cisco Aironet 802.a/b/g الذي يشغل الإصدار 4.1 من البرنامج الثابت
  - خادم ACS الآمن من Cisco الذي يشغل الإصدار 4.1
    - أي خادم ويب خارجي تابع لجهة خارجية

تم إنشاء المعلومات الواردة في هذا المستند من الأجهزة الموجودة في بيئة معملية خاصة. بدأت جميع الأجهزة المُستخدمة في هذا المستند بتكوين ممسوح (افتراضي). إذا كانت شبكتك مباشرة، فتأكد من فهمك للتأثير المحتمل لأي أمر.

#### <u>الاصطلاحات</u>

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

## <u>معلومات أساسية</u>

إعادة توجيه صفحة البداية على الويب هي ميزة مقدمة مع وحدة التحكم في الشبكة المحلية اللاسلكية الإصدار 5.0. باستخدام هذه الميزة، تتم إعادة توجيه المستخدم إلى صفحة ويب معينة بعد اكتمال مصادقة 802.1x. تحدث عملية إعادة التوجيه عندما يفتح المستخدم متصفح (تم تكوينه بصفحة رئيسية افتراضية) أو يحاول الوصول إلى URL. بعد اكتمال عملية إعادة التوجيه إلى صفحة الويب، يصبح للمستخدم حق الوصول الكامل إلى الشبكة.

يمكنك تحديد صفحة إعادة التوجيه على خادم خدمة مصادقة طلب اتصال المستخدم البعيد (RADIUS). يجب تكوين خادم RADIUS لإرجاع سمة RADIUS الخاصة ب Cisco AV-pair url-redirect إلى وحدة التحكم في الشبكة المحلية اللاسلكية عند مصادقة 802.1x الناجحة.

تتوفر ميزة إعادة توجيه صفحة البداية للشبكة المحلية اللاسلكية (WLANs) فقط للشبكات المحلية اللاسلكية (WLANs) التي تم تكوينها لتأمين 802.1x أو تأمين WPA/WPA2 من الطبقة 2.

## <u>(إعداد الشبكة) Network Setup</u>

في هذا مثال، cisco 4404 WLC و cisco 1232 sery {upper}lap ربطت من خلال طبقة 2 مفتاح. كما يتم توصيل خادم Cisco Secure ACS (الذي يعمل كخادم RADIUS خارجي) بنفس المحول. توجد جميع الأجهزة في الشبكة الفرعية نفسها.

يتم تسجيل نقاط الوصول في الوضع Lightweight (LAP) في البداية إلى وحدة التحكم. يجب إنشاء شبكتي WLAN: واحدة لمستخدمي **قسم** الإدارة والأخرى لمستخدمي **قسم العمليات**. تستخدم كلا شبكتي الشبكة المحلية اللاسلكية WPA2/ AES (يستخدم EAP-FAST للمصادقة). تستخدم كلتا شبكتي WLAN ميزة إعادة توجيه صفحة البداية من أجل إعادة توجيه المستخدمين إلى عناوين URL المناسبة للصفحة الرئيسية (على خوادم الويب الخارجية).

يستخدم هذا المستند إعداد الشبكة التالي:



Cisco Secure ACS server

WLC Management IP address: WLC AP Manager IP address: Wireless Client IP address:	10.77.244.204 10.77.244.205 10.77.244.221
Cisco Secure ACS server IP address	10.77.244.196
Subnet Mask used in this example	255.255.255.224

يشرح القسم التالي كيفية تكوين الأجهزة لهذا الإعداد.

## <u>التكوين</u>

في هذا القسم، تُقدّم لك معلومات تكوين الميزات الموضحة في هذا المستند.

**ملاحظة:** أستخدم <u>أداة بحث الأوامر</u> (للعملاء <u>المسجلين</u> فقط) للحصول على مزيد من المعلومات حول الأوامر المستخدمة في هذا القسم.

أتمت هذا steps in order to شكلت الأداة أن يستعمل الطفرة صفحة redirect سمة:

- 1. <u>قم بتكوين عنصر التحكم في الشبكة المحلية اللاسلكية (WLC) لمصادقة RADIUS من خلال خادم ACS الآمن من Cisco من خلال خادم ACS الآمن من Cisco.</u>
  - 2. قم بتكوين شبكات WLAN لقسم "الإدارة" وقسم "العمليات".
  - 3. <u>قم بتكوين ACS الآمن من Cisco لدعم ميزة إعادة توجيه صفحة البداية.</u>

<u>الخطوة 1. قم بتكوين عنصر التحكم في الشبكة المحلية اللاسلكية (WLC) لمصادقة RADIUS من</u> <u>خلال خادم ACS الآمن من Cisco.</u> يلزم تكوين عنصر التحكم في الشبكة المحلية اللاسلكية (WLC) لإعادة توجيه بيانات اعتماد المستخدم إلى خادم RADIUS خارجي.

أتمت هذا steps in order to شكلت ال WLC لخادم خارجي RADIUS:

- 1. أخترت **أمن** و**RADIUS صحة هوية** من الجهاز تحكم gui in order to عرضت ال RADIUS صحة هوية نادل صفحة.
  - 2. انقر فوق **جدید** لتحدید خادم RADIUS.
- 3. قم بتعريف معلمات خادم RADIUS على خوادم مصادقة RADIUS > صفحة جديدة.وتتضمن هذه المعلمات ما يلي:عنوان IP لخادم RADIUSسر مشتركرقم المنفذحالة

a a desta a a				Save Co	onfiguration Find 1	الحادم Refresh
cisco	MONITOR WLANS CONTRO	LLER WIRELESS SECURIT	Y MANAGEMENT	COMMANDS	нер	college and the second
Security	RADIUS Authentication S	ervers > New			< Back	Apply
* AAA General	Server Index (Priority)	1 1				
RADIUS     Authentication	Server IPAddress	10.77.244.196				
TACACS+     LDAP	Shared Secret Format	ASCII 💌				
Local Net Users MAC Filtering	Shared Secret	•••••				
Disabled Clients User Login Policies AP Policies	Confirm Shared Secret	•••••				
Local EAP	Key Wrap	(Designed for FIPS custome	rs and requires a ke	y wrap complian	t RADIUS server)	
Priority Order	Port Number	1812				
▶ Access Control Lists	Port Humber	line				
Wireless Protection     Policies	Server Status	Enabled 💌				
▶ Web Auth	Support for RFC 3576	Enabled 💌				
Advanced	Server Timeout	2 seconds				
	Network User	R Enable				
	Management	Enable				
	IPSec	Enable				

يستعمل هذا وثيقة ال ACS نادل مع عنوان 10.77.244.196. 4. طقطقة **يطبق**.

الخطوة 2. قم بتكوين شبكات WLAN لقسم "الإدارة" و"العمليات".

في هذه الخطوة، تقوم بتكوين شبكتي WLAN (واحدة لقسم "الإدارة" وأخرى لقسم "العمليات") اللتين سيستخدمهما العملاء للاتصال بالشبكة اللاسلكية.

سيكون WLAN SSID لقسم "الإدارة" هو *Admin*. ستكون SSID WLAN لقسم "العمليات" هي "العمليات".

أستخدم مصادقة EAP-FAST لتمكين WPA2 كآلية تأمين الطبقة 2 على كل من شبكات WLAN ونهج الويب - ميزة إعادة توجيه صفحة البداية للويب كطريقة تأمين الطبقة 3.

أكمل هذه الخطوات لتكوين شبكة WLAN والمعلمات المرتبطة بها:

- 1. طقطقت WLANs من ال gui من الجهاز تحكم in order to عرضت WLANs صفحة.تسرد هذه الصفحة شبكات WLAN الموجودة على وحدة التحكم.
  - 2. طقطقت **جديد** in order to خلقت WLAN

						Sa <u>v</u> e Co	nfiguration   Eing	Logout   Befresh
CISCO	MONITOR WLANS		WIRELESS	SECURITY	MANAGEMENT	COMMANDS	HELP	
WLANs	WLANs > New						< Back	Apply
WLANS	Туре	WLAN	×					
Advanced	Profile Name	Admin						
	WLAN SSID	Admin						

- 3. أدخل اسم SSID الخاص بشبكة WLAN واسم التوصيف على شبكات WLAN > صفحة جديدة.
  - 4. طقطقة **يطبق**.
- 5. أولا، فلنقم بإنشاء شبكة WLAN لقسم "الإدارة".ما إن يخلق أنت WLAN جديد، ال WLAN > تحرير صفحة ل ال WLAN جديد يظهر. في هذه الصفحة، يمكنك تحديد معلمات مختلفة خاصة بشبكة WLAN هذه. ويتضمن ذلك السياسات العامة، وسياسات الأمان، ونهج جودة الخدمة، والمعلمات المتقدمة.
  - 6. تحت سياسات عامة، حدد خانة الاختيار **الحالة** لتمكين الشبكة المحلية اللاسلكية (WLAN).

								onfiguration   Ping	Logout Refre
CISCO	MONITOR	<u>W</u> LANs		WIRELESS	SECURITY	MANAGEMENT	C <u>O</u> MMANDS	нејр	
WLANs	WLANs >	Edit						< Back	Apply
▼ WLANs	General	Secur	ity QoS	Advanced					
WLANs	Des Els I		A desire						
Advanced	Profile P	same	Admin						
	1 ype		Admin						
	Status		Finabl	ed					
	Security Radio P Interfac Broadce	y Policies olicy xe ast SSID	Splash (Modificat All admin R Enable	Page-Web-Re ions done unde	edirect[WPA: r security tab	2][Auth(802.1X)] will appear after ap	plying the chan	ges.)	

- 7. انقر صفحة **التأمين**، ثم انقر صفحة **الطبقة 2**.
- 8. أختر **WPA+WPA2** من القائمة المنسدلة تأمين الطبقة 2.تمكن هذه الخطوة مصادقة WPA للشبكة المحلية اللاسلكية (WLAN).
  - 9. تحت معلمات WPA+WPA2، تحقق من خانات تأشير **سياسة WPA2 وتشفير** AES.

Sage Configuration Bing Lo	lout   Befre
CISCO MONITOR WLANS CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP	
WLANS WLANS > Edit WLANS WLANS > Edit General Security QoS Advanced Layer 2 Layer 3 AAA Servers Layer 2 Security WPA+WPA2 MAC Filtering WPA+WPA2 Parameters WPA Policy WPA2 Encryption PAES TKIP Auth Key Mgmt 802.1X 	Apply

- 10. أختر **802.1x م**ن القائمة المنسدلة إدارة مفتاح المصادقة. يتيح هذا الخيار WPA2 مع مصادقة 802.1x/EAP وتشفير AES للشبكة المحلية اللاسلكية (WLAN).
  - 11. انقر صفحة **تأمين الطبقة 3**.
  - 12. حدد مربع **نهج الويب**، ثم انقر فوق الزر **إعادة توجيه صفحة البداية** على الويب.يتيح هذا الخيار ميزة إعادة توجيه صفحة الإملية

									البداية.
								nfiguration   Ping	Logout   Befree
cisco	MONITOR	<u>W</u> LANS <u>C</u> C	ONTROLLER	WIRELESS	SECURITY	MANAGEMENT	C <u>O</u> MMANDS	HELP	
WLANS WLANS WLANS Advanced	WLANS > I General Layer 2 Layer © W © Aut © Co © Spi Preaut ACL	Edit Security Layer 3 3 Security [1 reb Policy <sup>2</sup> thentication sathrough anditional Web lash Page Web thentication	QoS AAA St None Redirect b Redirect None	Advanced				< Back	Apply

- 13. انقر فوق علامة التبويب **خوادم AAA**.
- 14. تحت مصادقة الخادم، أختر عنوان IP المناسب للخادم من القائمة المنسدلة الخادم
  - .1

	Sa <u>v</u> e Configuration   <u>P</u> ing   Log	jout I <u>R</u> efri
CISCO	MONITOR WLANS CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP	
WLANS	WLANs > Edit < Back General Security QoS Advanced	Apply
WLANS Advanced	Layer 2       Layer 3       AAA Servers         Select AAA servers below to override use of default servers on this WLAN         Radius Servers       LDAP Servers         Authentication Servers       Accounting Servers         Server       Inne         Server       Inne         Server       Inne         Server       Inne         Server       Inne         Server       None         Authentication       Enabled         Local EAP Authentication       Enabled	
	veb-auth user	-

- في هذا المثال، يتم إستخدام 10.77.244.196 كخادم RADIUS.
  - 15. طقطقة **يطبق**.
- 16. كرر الخطوات من 2 إلى 15 لإنشاء شبكة WLAN لقسم "العمليات".تسرد صفحة شبكات WLAN شبكتي اللتين

						0	
							أنشأتهما.
					Sa <u>v</u> e Co	onfiguration   Ping	Logout Refresh
cisco	MONITOR WLANS	CONTROLLER WIREL	ESS SECURITY	MANAGEMENT	C <u>O</u> MMANDS	HELP	
WLANs	WLANs						New
WLANS WLANS	Profile Name	Туре	WLAN SSID		Admin Status	Security Policies	
Advanced	Admin	WLAN	Admin		Enabled	[WPA2][Auth(802.1X	)], Splash-Page
	Operations	WLAN	Operations		Enabled	[WPA2][Auth(802.1X	)], Splash-Page

لاحظ أن سياسات التأمين تتضمن إعادة توجيه صفحة البداية.

الخطوة 3. قم بتكوين ACS الآمن من Cisco لدعم ميزة إعادة توجيه صفحة Splash.

تتمثل الخطوة التالية في تكوين خادم RADIUS لهذه الميزة. يحتاج خادم RADIUS إلى إجراء مصادقة EAP-FAST للتحقق من مسوغات العميل، وعند نجاح المصادقة، لإعادة توجيه المستخدم إلى URL (على خادم الويب الخارجي) المحدد في سمة RADIUS **لإ***عادة توجيه عنوان URL* **م**زدوج من Cisco.

تكوين مصدر المحتوى الإضافي الآمن من Cisco لمصادقة EAP-FAST

**ملاحظة:** يفترض هذا المستند إضافة وحدة التحكم في الشبكة المحلية اللاسلكية إلى Cisco ACS الآمن كعميل AAA.

أكمل هذه الخطوات لتكوين مصادقة EAP-FAST في خادم RADIUS:

1. انقر فوق **تكوين النظام** من واجهة المستخدم الرسومية (GUI) لخادم RADIUS، ثم أختر **إعداد المصادقة العامة** من صفحة تكوين

le Edit Yew Fr	gvorites Iools Help	Links ** Co
dress ) http://127	.0.0.1:1065/	• 🖸 😡
Cittee Statem	System Configuration	Halp
Betrop     Setop     Setop	<ul> <li>Service Control</li> <li>Logging</li> <li>Date Format Control</li> <li>Local Password Management</li> <li>ACS Internal Database Replication</li> <li>ACS Backup</li> <li>ACS Restore</li> <li>ACS Certificate Setup</li> <li>Global Authentication Setup</li> </ul>	<ul> <li>Service Centrel</li> <li>Leasting</li> <li>Data Format Centrel</li> <li>Least Desirement Mutukese Realisation</li> <li>MCS Internal Database Recovery</li> <li>IP Predu Address Recovery</li> <li>IP Predu Addr</li></ul>
		(Back to Tao)

2. من صفحة إعداد المصادقة العامة، انقر على **تكوين EAP-FAST** للانتقال إلى صفحة إعدادات -EAP FAST.

CiscoSecure ACS - !	Microsoft Internet Explorer	
the Edit Yew Fa	ivonities Iools Belp	Links "
gdress an http://127.	0.0.1:1065/	 
Crees Systems	System Configuration	2
	EAP Configuration	P Help
Setup Setup Setup Barred Brodle Components Disreed Prodle Components Partern Configuration Configurati	PEAP         Allow EAP-MSCHAPv2         Allow EAP-GTC         Allow EAP-TLS         Select one or more of the following options:         If Certificate SAN comparison         If Certificate Binary comparison         EAP-TLS session timeout (minutes):         120         Cisco client initial message:         PEAP session timeout (minutes):         I20         Enable Fast Reconnect:	Use this page to specify settings for various authentication protocols. • CAP Configuration • PSAP • CAPINS • CONSPICTION • AP Configuration EAP
D   Online	EAP-FAST	PEAP is the outer layer protocol for the secure tunnel.
Spil Documentation	EAP-TLS EAP-TLS Select one or more of the following options: ECertificate SAN comparison Submit Submit + Restart Cancel	Noter MAP is a certificate-based authentication protocol. MAP     authentication can occur only after you have completed the required     stops so the ACS Certificate Setup page.     Allow EAP-MSCHAPv2 — Use to enable EAP-MSCHAPv2 within MS PEAP     authentication. Enable this protocol for any repository that supports MS- CHAPv2, such as Microsoft AD, and the ACS Internal Database.
		(1)
Sant G .	Chronie ACS - Mir	Tita Da
start 0	Uscosecure ACS - Mic	151 7/30 PP

3. من صفحة إعدادات EAP-FAST، حدد خانة الاختيار **السماح EAP-FAST** لتمكين EAP-FAST في خادم RADIUS.

iscoSecure ALS - 1	Microsoft Internet Explorer	SSEC		10
Edt Yew Fg	vonites Iools Help	*********	Lifes #	
ess an http://127.	0.0.1:1065/			÷ ¢
Lisco Systems	System Configuration			
ah. ah.	System Comiguration			
، دائلته، دائلته،	EAP-FAST Con	figuration	Hab	
User				
Setup			EAP-FAST Configuration Page	
Group	EAP-FAST Set	tings	? Use this pass to confirm FAD-FACT authentication sufficient	
1 Seriep	EAP-FAST		use this page to compare LAP FAST automocidon recongs.	
Shared Profile Components	R Allow EAP-FAST		EAP-EAST Settless	
	Active mester law TTI	1 months W	Chentinitial measure     Automatic ID Info	
Configuration	Active master key inc	a moners	<ul> <li>Allow approximate in band PAC provisioning</li> </ul>	
I Sustan	Retired master key TTL	3 months 💌	<ul> <li>Allers as the sticated in-band PAC previolening</li> </ul>	
Configuration	Tunnel PAC TTL	1 weeks	<ul> <li>Allers machine arthentication</li> </ul>	
I Interface		A	Allowed incer methods	
Configuration	Client initial message:	tacwebacs	Certificate Comparison	
Administration	Authority ID Info:	tacwebacs	<ul> <li>EAP: ILS session timesut (minutes)</li> </ul>	
Centrel	Allow approximate in-band BAC	ornulsioning	Actual EAP-EAST server states	
External User		provisioning		
Databases	L Allow authenticated in-band P	AC provisioning	EAP-FAST Settings	
Porture Validation	Accept client on authentic	ated provisioning	A Alima FAD FAST To souble FAD FAST subsetiestics relact this cher	
	Require client certificate for	or provisioning	best.	
Profiles	Allow Machine Authentication			
1 Based of and	Machine RAC TTL	1 weeks	<ul> <li>Active Haster Key TIL – Enter a value for the amount of time that a mast key is used to consiste new Protected Access Credentials (PACs). Who</li> </ul>	ter en i
Activity		a junters 22	time to live (TTL) defined for the Master Key expires, the master key is	
1 Online	CAllow Stateless session resum	·	considered retired and a new master key is generated.	
Documentation	Authorization PAC TTL	1 hours 💌	<ul> <li>Retired master key TR —Enter a value for the amount of time that PACs</li> </ul>	8
	Allowed inner methods		generated using a retired master key are acceptable for EAP-FAST authentication. When an end-user client gains network access using a P	
	EAP-GTC		based on a retired master key. ACS sends a new PAC to the end-user cl	lie
	EAP-MSCHAPv2		<ul> <li>Tennel DAC VIII - Entry &amp; only in the participant of the other is that is one</li> </ul>	
	D EAD-TIC		before it expires and must be replaced. If the master key used to general	vte
	I EAP-TLS		the Tunnel PAC has not expired, new PAC creation and assignment is automatic. If the master key used to generate the Tunnel PAC expired.	
	Submit Submit +	Restart Cancel	automatic or manual provisioning must be used to provide the end-user	
	-		1 Contra a Data Price	

- 4. قم بتكوين قيم مدة البقاء (TTL) للمفتاح الرئيسي النشط/المتقاعد كما هو مطلوب، أو قم بتعيينها على القيمة الافتراضية كما هو موضح في هذا المثال.يمثل حقل معلومات معرف المرجع الهوية النصية لخادم ACS هذا، والتي يمكن للمستخدم النهائي إستخدامها لتحديد خادم ACS الذي ستتم المصادقة عليه. ملء هذا الحقل إلزامي.يحدد حقل رسالة العرض الأولية للعميل الرسالة التي سيتم إرسالها إلى المستخدمين الذين يقومون بالمصادقة مع عميل EAP-FAST. الحد الأقصى للطول هو 40 حرفا. لن يرى المستخدم الرسالة الأولية إلا إذا كان عميل المستخدم النهائي يدعم العرض.
- 5. إذا كنت تريد أن يقوم ACS بتنفيذ تزويد PAC غير معروف داخل النطاق، حدد خانة الاختيار **السماح بإمداد PAC داخل النطاق المجهول**.
- 6. يحدد خيار *الأساليب الداخلية المسموح بها* أي طرق EAP داخلية يمكن أن تعمل داخل نفق EAP-FAST TLS. من أجل التقديم مجهول النطاق، يجب عليك تمكين EAP-GTC و EAP-MS-CHAP من أجل التوافق مع الإصدارات السابقة. إذا حددت السماح بتقديم مسوغات الوصول المحمي (PAC) المغفل داخل النطاق، فيجب عليك تحديد EAP-MS-CHAP (المرحلة صفر) و EAP-GTC (المرحلة الثانية).
  - 7. انقر على **إرسال**.**ملاحظة:** للحصول على معلومات وأمثلة مفصلة حول كيفية تكوين EAP FAST باستخدام تزويد PAC غير معروف داخل النطاق وإمداد معتمد داخل النطاق، راجع <u>مصادقة EAP-FAST مع وحدات</u> <u>تحكم الشبكة المحلية اللاسلكية ومثال تكوين خادم RADIUS الخارجي</u>.

قم بتكوين قاعدة بيانات المستخدم وحدد سمة RADIUS *لإعادة توجيه عنوان URL* 

يقوم هذا المثال بتكوين اسم المستخدم وكلمة المرور للعميل اللاسلكي ك User1 و User1، على التوالي.

أتمت هذا steps in order to خلقت مستعمل قاعدة بيانات:

- 1. من واجهة المستخدم الرسومية (GUI) ل ACS في شريط التنقل، أختر **إعداد المستخدم**.
- 2. قم بإنشاء مستخدم لاسلكي جديد، ثم انقر فوق **إضافة/تحرير** للانتقال إلى صفحة تحرير هذا المستخدم.

Iteor States	etup	
Configuration     Configuration	Setup User: User1 Find Add/Edit List users beginning with letter/number: A R S R S R S C S N S S N S P S R S T S V S N S Q 1 2 2 1 5 5 2 8 2 List all users Remove Dynamic Users Remove Dynamic Users	<ul> <li>Versisting and External Over Databases</li> <li>Versisting and External Over Databases</li> <li>Addims a Specific User in the ACS Internal Database</li> <li>Addims a User to the ACS Internal Database</li> <li>Uniting Diversames that Benjin with a Particular Character</li> <li>Linking All Usersames in the ACS Internal Database</li> <li>Changing a Systemane in the ACS Internal Database</li> <li>Changing a Usersame in the ACS Internal Database</li> <li>Changing a Usersame in the ACS Internal User Database</li> <li>Changing a Usersame in the ACS Internal User Database</li> <li>Changing a Usersame in the ACS Internal User Database</li> <li>Semetre Opnamic Users</li> <li>User Setup anables you to configure individual user information, add user and delete users in the database. User Setup and External User Database</li> <li>Sefere ACS Can authenticate users with an external user database.</li> <li>You must have the database up and manning on the external User Databases for users with have configured the applicable parameters in the External User Databases section.</li> <li>You must have configuration overrides Group Setup configuration.</li> <li>If you rely on the Unknown User Policy in the External User Databases section to create entries in the ACS Internal database for users defined in automaticate users listed for users defined in a startabase, User Setup keeps the diversited ence.</li> <li>External user database modification must be located or listed hare used user database. User Setup keeps the diversite diversite with an external user database. User Setup keeps the diversite database.</li> <li>Note: User Setup does not add ar delete usernames in an external user database. (Back to Tree)</li> <li>Fields a Specific User is the ACS Internal Batabase.</li> <li>Fields the They for add ant activity is an internal user database. (Back to Tree)</li> </ul>

3. من صفحة تحرير إعداد المستخدم، قم بتكوين الاسم والوصف الحقيقيين، بالإضافة إلى إعدادات كلمة المرور، كما هو موضح في هذا المثال.يستخدم هذا المستند قاعدة بيانات ACS الداخلية لمصادقة كلمة المرور.

CiscoSecure ACS -	Microsoft Internet Explorer	<u>_0</u> _X
Ele Edt Yew Fa	pronities [looks Help	Links 🇯 🧞
Address a http://127.	.0.0.1:1065/	• 🔁 •
Crace Systems	User Setup	×
	Edit	Help 🌨
Uter Setop Group BaredProfile Components Met work Configuration Configuration Configuration Meterface Configuration Configuration Configuration Configuration Configuration Configuration Configuration Configuration Configuration	User: User1 (New User)  Account Disabled  Supplementary User Info Real Name Description  User Setup Password Authentication: ACS Internal Database CiscoSecure PAP (Also used for CHAP/MS-	Accessit, Disabled     Outris Sins, a. Username     Supplementary, Dany, Enfy     Reserved, A. Chemica, Hans, Reserved     Califiest     Califiest     Califiest     Califiest     Califiest, Disable, Constant, Co
Reports and Activity Documentation	CHAP/ARAP, if the Separate field is not checked.) Password •••••• Confirm •••••• Password •••••• Password •••••• Confirm Password •••••• Submit Cancel	Account Disabled Status Select the Account Disabled check how to disable this account: clear the check how to enable the account. [Back to Top] Deleting a Username The Delete button appears only when you are editing an existing user account, not when you are adding a new user account. To delete the current user account from the database, click <b>Delete</b> . To delete the confirm your action, click <b>OK</b> .
Done		internet
🎝 Start 🔀 🥭	CiscoSecure ACS - Mic	💆 7:56 PM

- 4. انزلق إلى أسفل الصفحة لتعديل خصائص RADIUS.
  - 5. حدد خانة الاختيار [000\Cisco-AV-pair [001.
- 6. أدخل أزواج Cisco الظاهرية هذه في مربع تحرير [000\URL لتحديد عنوان URL الذي يتم إعادة توجيه المستخدم إليه:-url-redirect=http://10.77.244.196/Admin Login.html

Cisco Systems	User Setup	l l
adheadhea	(useu iur benueass anu benukuun cherus such as routers)	- Help
User Setup	Password •••••	Account Disabled
Group Setup	Confirm Password	Ordeting, a Username     Supplementary User Info
Shared Profile Components	Cicca Alexandra PATHIS Artsbute	Passward Authentication     Group to which the user is assigned     Gibsch address and address and address and address ad
Network Configuration		Cleant IP. Address Assignment     Advanced Settings
System Configuration		Network Access Restrictions     New Sessions
Interface Configuration		Orange Chooles     Account Disable     Developedale ACLs
Administration Centrel	Cisco IOS/PIX 6 y RADIUS Attributes	Advanced TACACS - Settings     TACACS - Enable Control
Deternal Uper		TACACS - Enable Password     TACACS - Outbound Password     TACACS - Suthound Password     TACACS - Stall Command Arthretization
Posture Validation	ur1-	Command Authorization for Network Device Management Applications     TACACS - Unknown Services
Network Access	kdmin-login.html	IETE RADIUS Attributes     RADIUS Vendor-Specific Attributes
Reports and	×	
-Ch I Deline		Account Disabled Status
Documentation		Select the Account Disabled check box to disable this account clear the check box to enable the account.
	P Back to Help	(Back to Tee)
		Deleting a Username
	Submit Delete Cancel	The Delete button appears only when you are editing an existing user account, not when you are adding a new user account. To delete the

هذه هي الصفحة الرئيسية لمستخدمي قسم "الإدارة".

- 7. انقر على **إرسال**.
- 8. كرر هذا الإجراء لإضافة User2 (مستخدم قسم العمليات).
- 9. كرر الخطوات من 1 إلى 6 لإضافة المزيد من مستخدمي قسم الإدارة ومستخدمي قسم العمليات إلى قاعدة البيانات.**ملاحظة:** يمكن تكوين سمات RADIUS على مستوى المستخدم أو مستوى المجموعة على مصدر المحتوى الإضافي الآمن من Cisco.

#### <u>التحقق من الصحة</u>

للتحقق من التكوين، قم بإقران عميل شبكات WLAN من قسم "الإدارة" وقسم "العمليات" بشبكات WLAN المناسبة الخاصة بهم.

عندما يتصل مستخدم من قسم الإدارة بمسؤول الشبكة المحلية اللاسلكية، يوعز للمستخدم بإدخال بيانات اعتماد 802.1x (بيانات اعتماد EAP-FAST في حالتنا). بمجرد أن يوفر المستخدم بيانات الاعتماد، يقوم عنصر التحكم في الشبكة المحلية اللاسلكية (WLC) بتمرير بيانات الاعتماد هذه إلى خادم ACS الآمن من Cisco. يتحقق خادم Cisco Secure ACS من مسوغات المستخدم مقابل قاعدة البيانات، وعند نجاح المصادقة، يرجع سمة url-redirect إلى وحدة التحكم في الشبكة المحلية اللاسلكية. تكتمل المصادقة في هذه الم حدم المرحلة.

🖻 Cisco Aironet Desktop Utility - Current Profile: Admin 🛛 🛛 🛛				
Action Options Help				
Current Status Profile Management	Diagnostics			
CISCO SYSTEMS				
Profile Name:	Admin			
Link Status:	Not Associated	Network Type: Infrastructure	•	
Wireless Mode:	5 GHz 54 Mbps	Current Channel: 149		
Server Based Authentication:	None	Data Encryption: AES		
IP Address:	10.77.244.221			
Signal Strength:		Good		
		Advanced		
Signal Strength:		Good Advanced		

عندما يقوم المستخدم بفتح مستعرض ويب، تتم إعادة توجيه المستخدم إلى عنوان URL الخاص بالصفحة الرئيسية لقسم "الإدارة". (يتم إرجاع عنوان URL هذا إلى عنصر التحكم في الشبكة المحلية اللاسلكية (WLC) من خلال سمة زوج-الصوت من Cisco). بعد إعادة التوجيه، يتمتع المستخدم بحق الوصول الكامل إلى الشبكة. هنا اللقطات:



يحدث نفس تسلسلات الأحداث عندما يتصل مستخدم من قسم العمليات بعمليات شبكة WLAN.

🖻 Cisco Aironet Desktop Utility - Current Profile: Operations 🛛 🔹 💽					
Action Options Help					
Current Status Profile Management	Diagnostics				
CISCO SYSTEMS					
ulluuulluu Profile Name:	Operations				
Link Status:	Authenticated	Network Type: Infrastructure			
Wireless Mode:	5 GHz 54 Mbps	Current Channel: 149			
Server Based Authentication:	EAP-FAST	Data Encryption: AES			
IP Address:	10.77.244.221				
Signal Strength:		Good			
		Advanced			



## استكشاف الأخطاء وإصلاحها

يوفر هذا القسم معلومات يمكنك استخدامها لاستكشاف أخطاء التكوين وإصلاحها.

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

يمكنك إستخدام الأوامر التالية لاستكشاف أخطاء التكوين وإصلاحها.

show wlan wlan_id— يعرض حالة ميزات إعادة توجيه الويب لشبكة WLAN معينة.فيما يلي مثال:
WLAN Identifier 1
Profile Name Admin
Network Name (SSID) Admin
Web Based Authentication Disabled
Web-Passthrough Disabled
Conditional Web Redirect Disabled
Splash-Page Web Redirect Enabled
• eldene events enable • • x1 202
rii Feb 29 10:27:10 2008: 00:40:96:ac:dd:05 Sending EAP Request from AAA to
(MODILE 00:40:90:ac:ad:05 (EAP 10 10
Fri Feb 29 10:27:16 2008: 00:40:96:ac:dd:05 Received EAPOL EAPPRT from
modile 00:40:96:ac:dd:05
FIL FED 29 10:27:10 2008: 00:40:96:ac:dd:05 Received EAF Response fiom
(MODILE 00:40:90:ac:dd:05 (EAF 10 10, EAF 1996 45
rii feb 29 10:27:10 2008: 00:40:90:ac:dd:05 Fiotessing Access-chailenge ior
Eri Ech 20 10.27.16 2008. 00.40.06.cor.dd.05 Cotting to such timeout to 1800
FIL FED 29 10:27:16 2008: 00:40:96:ac:dd:05 Setting re-auth thmeout to 1800
.seconds, got from whan config
Fri Feb 29 10:27:16 2008: 00:40:96:ac:dd:05 Station 00:40:96:ac:dd:05
setting dotix reauth timeout = 1800
Fri Feb 29 10:27:16 2008: 00:40:96:ac:dd:05 Creating a new PMK Cache Entry
(for station 00:40:96:ac:dd:05 (RSN 2

Fri Feb 29 10:27:16 2008: 00:40:96:ac:dd:05 Adding BSSID 00:1c:58:05:e9:cf to PMKID cache for station 00:40:96:ac:dd:05 (Fri Feb 29 10:27:16 2008: New PMKID: (16 Fri Feb 29 10:27:16 2008: [0000] 79 ee 88 78 9c 71 41 f0 10 7d 31 ca fb fa 8e 3c Fri Feb 29 10:27:16 2008: 00:40:96:ac:dd:05 Disabling re-auth since PMK .lifetime can take care of same Fri Feb 29 10:27:16 2008: 00:40:96:ac:dd:05 Sending EAP-Success to mobile (ac:dd:05 (EAP Id 17:00:40:96 (Fri Feb 29 10:27:16 2008: Including PMKID in M1 (16 Fri Feb 29 10:27:16 2008: [0000] 79 ee 88 78 9c 71 41 f0 10 7d 31 ca fb fa 8e 3c Fri Feb 29 10:27:16 2008: 00:40:96:ac:dd:05 Sending EAPOL-Key Message to mobile 00:40:96:ac:dd:05 state INITPMK (message 1), replay counter 00.00.00.00.00.00.00 Fri Feb 29 10:27:16 2008: 00:40:96:ac:dd:05 Received Auth Success while in Authenticating state for mobile 00:40:96:ac:dd:05 • debug aaa events enable— يمكن إخراج تصحيح الأخطاء لجميع أحداث AAA.فيما يلي مثال: Thu Feb 28 07:55:18 2008: 00:40:96:ac:dd:05 Successful transmission of Authentication Packet (id 103) to 10.77.244.196:1812, proxy state ac:dd:05-00:00:00:40:96 Thu Feb 28 07:55:18 2008: \*\*\*\*Enter processIncomingMessages: response code=11 Thu Feb 28 07:55:18 2008: \*\*\*\*Enter processRadiusResponse: response code=11 Thu Feb 28 07:55:18 2008: 00:40:96:ac:dd:05 Access-Challenge received from RADIUS server 10.77.244.196 for mobile 00:40:96:ac:dd:05 receiveId = 3 Thu Feb 28 07:55:18 2008: 00:40:96:ac:dd:05 Successful transmission of Authentication Packet (id 104) to 10.77.244.196:1812, proxy state ac:dd:05-00:00:00:40:96 Thu Feb 28 07:55:18 2008: \*\*\*\*Enter processIncomingMessages: response code=2 Thu Feb 28 07:55:18 2008: \*\*\*\*Enter processRadiusResponse: response code=2 Thu Feb 28 07:55:18 2008: 00:40:96:ac:dd:05 Access-Accept received from RADIUS server 10.77.244.196 for mobile 00:40:96:ac:dd:05 receiveId = 3 Thu Feb 28 07:55:18 2008: 00:40:96:ac:dd:05 AAA Override Url-Redirect http://10.77.244.196/Admin-login.html' set' Thu Feb 28 07:55:18 2008: 00:40:96:ac:dd:05 Applying new AAA override for station 00:40:96:ac:dd:05 Thu Feb 28 07:55:18 2008: 00:40:96:ac:dd:05 Override values for station ac:dd:05:00:40:96 source: 4, valid bits: 0x0 qosLevel: -1, dscp: 0xfffffff, dot1pTag: 0xffffffff, sessionTimeout: -1 dataAvgC: -1, rTAvgC: -1, dataBurstC: -1, rTimeBurstC: -1 ' :vlanIfName: '', aclName

#### <u>معلومات ذات صلة</u>

- دليل تكوين وحدة تحكم شبكة LAN اللاسلكية، الإصدار 5.0 من Cisco
- مثال تكوين مصادقة الويب لوحدة تحكم الشبكة المحلية (LAN) اللاسلكية
- مثال تكوين المصادقة الخارجية للويب مع وحدات تحكم الشبكة المحلية (LAN) اللاسلكية
  - <u>صفحة الدعم اللاسلكي</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