لكل (ACL) لوصولا يف مكحتلا ةمئاق ةكبشلا يف مكحتلا تادحو عم مدختسم نيوكت لاثمو ةيكلساللا (LAN) ةيلحملا ACS نم نمآلا كisco

المحتويات

المقدمة المتطلبات الأساسية المتطلبات المكونات المستخدمة الاصطلاحات معلوما<u>ت أساسية</u> الرسم التخطيطي للشبكة التكوين <u>تكوين وحدة التحكم في الشبكة المحلية (LAN) اللاسلكية</u> خلقت VLAN للمستخدمين اللاسلكي قم بتكوين عنصر التحكم في الشبكة المحلية اللاسلكية (WLC) للمصادقة مع Cisco Secure ACS إنشاء شبكة WLAN جديدة للمستخدمين اللاسلكيين تحديد قوائم التحكم في الوصول (ACL) للمستخدمين <u>تكوين خادم ACS الآمن من Cisco</u> تكوين وحدة التحكم في الشيكة المحلية اللاسلكية كعميل AAA على Cisco Secure ACS تكوين المستخدمين وملف تعريف المستخدم على ACS الآمن من <u>Cisco</u> التحقق من الصحة استكشاف الأخطاء وإصلاحها تلميحات استكشاف المشكلات واصلاحها معلومات ذات صلة

<u>المقدمة</u>

يشرح هذا المستند من خلال مثال كيفية إنشاء قوائم التحكم في الوصول (ACLs) على قوائم التحكم في الوصول (WLCs) وتطبيقها على المستخدمين الذين يعتمدون على تفويض RADIUS.

<u>المتطلبات الأساسية</u>

<u>المتطلبات</u>

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

- معرفة أساسية بكيفية تكوين خادم Cisco Secure ACS لمصادقة العملاء اللاسلكيين
- معرفة تكوين نقاط الوصول في الوضع Lightweight (LAPs) و Cisco Wireless LAN Controllers (WLCs (WLCs))
 - معرفة حلول الأمان اللاسلكية الموحدة من Cisco

<u>المكونات المستخدمة</u>

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

- وحدة التحكم في شبكة LAN اللاسلكية Cisco 4400 Series التي تشغل الإصدار 5.0.148.0
 - نقاط الوصول في الوضع Lightweight (LAPs) من سلسلة Cisco Aironet 1231
- مهايئ عميل شبكَة LAN اللاسلكية من LAN Client مهايئ عميل شبكَة Ab/g Cisco Wireless LAN Client الذي يشغل الإصدار 3.6
 - . Cisco Aironet Desktop Utility الإصدار
 - خادم ACS الآمن من Cisco، الإصدار 4.1
- موجه الخدمات المتكاملة Cisco 2800 Series Integrated Services Router الذي يعمل بنظام التشغيل IOS[®]، الإصدار 12.4(T
 - cisco مادة حفازة sery مفتاح أن يركض صيغة WC3b(5)12.0 •

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>

قائمة التحكم في الوصول لكل مستخدم (ACL) هي جزء من شبكة هوية Cisco. يدعم حل Cisco Wireless LAN شبكات الهوية، والتي تسمح للشبكة بالإعلان عن معرف SSID واحد، كما تسمح لمستخدمين محددين بتوريث سياسات مختلفة استنادا إلى ملفات تعريف المستخدمين الخاصة بهم.

توفر ميزة قائمة التحكم في الوصول (ACL) لكل مستخدم إمكانية تطبيق قائمة تحكم في الوصول (ACL) تم تكوينها على وحدة التحكم في الشبكة المحلية اللاسلكية على مستخدم استنادا إلى تفويض RADIUS. ويتم تحقيق ذلك باستخدام السمة المحددة للمورد (VSA) ل Airespace-ACL-Name.

تشير هذه السمة إلى اسم قائمة التحكم في الوصول (ACL) المطلوب تطبيقه على العميل. عندما تكون سمة قائمة التحكم في الوصول (ACL) موجودة في "قبول الوصول إلى RADIUS"، يطبق النظام اسم قائمة التحكم في الوصول (ACL) على محطة العميل بعد مصادقته. يتخطى هذا الإجراء أي قوائم تحكم في الوصول (ACL) يتم تعيينها إلى الواجهة. فهو يتجاهل قائمة التحكم في الوصول (ACL) الخاصة بالواجهة المعينة ويطبق القائمة الجديدة.

يوجد أدناه ملخص لتنسيق سمة اسم قائمة التحكم في الوصول (ACL). يتم إرسال الحقول من اليسار إلى اليمين

لمزيد من المعلومات حول شبكة معرف الشبكة اللاسلكية الموحدة من Cisco، ارجع إلى قسم <u>تكوين شبكات الهوية</u> في المستند <u>تكوين حلول الأمان</u>.

<u>الرسم التخطيطي للشبكة</u>

يستخدم هذا المستند إعداد الشبكة التالي:

في هذا الإعداد، يتم إستخدام وحدة تحكم الشبكة المحلية اللاسلكية (LAN) ووحدة التحكم في الشبكة المحلية اللاسلكية (WLC) ونقطة الوصول في الوضع Lightweight (LAP) لتوفير الخدمات اللاسلكية للمستخدمين في القسم A والقسم B. يستخدم جميع المستخدمين اللاسلكيين مكتب شبكة WLAN (SSID) مشتركة للوصول إلى الشبكة وهم في شبكة VLAN Office-VLAN).



يتم إستخدام خادم ACS الآمن من Cisco لمصادقة المستخدمين اللاسلكيين. تستخدم مصادقة EAP لمصادقة

المستخدمين. يتم توصيل خادم WLC و LAP و Cisco ACS الآمن بمحول الطبقة 2 كما هو موضح.

يعمل الموجه R1 على توصيل الخوادم على الجانب السلكي من خلال محول الطبقة 2 كما هو موضح. يعمل الموجه R1 أيضا كخادم DHCP، الذي يوفر عناوين IP إلى عملاء اللاسلكي من الشبكة الفرعية DHCP،16.0.0.

أنت تحتاج أن يشكل الأداة أن هذا يقع:

المستخدم1 من القسم A لديه حق الوصول إلى الخادم 172.16.1.100 فقط

المستخدم 2 من القسم ب لديه حق الوصول إلى الخادم 172.16.1.50 فقط

ومن أجل تحقيق ذلك، تحتاج إلى إنشاء 2 قائمة تحكم في الوصول (ACL) على عنصر التحكم في الشبكة المحلية اللاسلكية (WLC): واحدة للمستخدم1، والأخرى للمستخدم 2. بمجرد إنشاء قوائم التحكم في الوصول، يلزمك تكوين خادم Cisco Secure ACS لإرجاع سمة اسم قائمة التحكم في الوصول إلى عنصر التحكم في الوصول (WLC) عند المصادقة الناجحة للمستخدم اللاسلكي. تطبق عنصر التحكم في الشبكة المحلية اللاسلكية (WLC) بعد ذلك قائمة التحكم في الوصول (ACL) على المستخدم، وبالتالي يتم تقييد الشبكة المحلية مل على من الوصول.

ملاحظة: يستخدم هذا المستند مصادقة LEAP لمصادقة المستخدمين. تكون تقنية LEAP من Cisco عرضة لهجمات القاموس. في شبكات الوقت الفعلي، يجب إستخدام أساليب مصادقة أكثر أمانا مثل EAP FAST. بما أن تركيز الوثيقة ينصب على شرح كيفية تكوين ميزة قائمة التحكم بالوصول لكل مستخدم، فإنه يتم إستخدام LEAP من أجل التبسيط.

يوفر القسم التالي إرشادات خطوة بخطوة لتكوين الأجهزة لهذا الإعداد.

<u>التكوين</u>

قبل تكوين ميزة قوائم التحكم في الوصول (ACL) لكل مستخدم، يجب تكوين عنصر التحكم في الشبكة المحلية اللاسلكية (WLC) للعملية الأساسية وتسجيل نقاط الوصول في الوضع Lightweight إلى عنصر التحكم في الشبكة المحلية اللاسلكية (WLC). يفترض هذا المستند أن عنصر التحكم في الشبكة المحلية اللاسلكية (WLC) تم تكوينه للعملية الأساسية وأن نقاط الوصول في الوضع Lightweight تم تسجيلها إلى عنصر التحكم في الشبكة المحلية اللاسلكية (WLC). إذا كنت مستخدما جديدا، والذي يحاول إعداد عنصر التحكم في الشبكة المحلية المحلية اللاسلكية (WLC) للعملية الأساسية باستخدام نقاط الوصول في الوضع Lightweight تم تسجيلها إلى عنصر التحكم في الشبكة المحلية اللوضع (WLC). إذا كنت مستخدما جديدا، والذي يحاول إعداد عنصر التحكم في الشبكة المحلية اللاسلكية (WLC) العملية الأساسية باستخدام نقاط الوصول في الوضع Lightweight (LAP)، فارجع إلى <u>تسجيل نقطة الوصول في</u> الوضع Lightweight (LAP)، إلى وحدة تحكم شبكة محلية لاسلكية (WLC).

بمجرد تسجيل نقاط الوصول في الوضع Lightweight، أكمل الخطوات التالية لتكوين الأجهزة الخاصة بهذا الإعداد:

- 1. <u>قم بتكوين وحدة التحكم في الشبكة المحلية (LAN) اللاسلكية.</u>
 - 2. <u>قم بتكوين خادم ACS الآمن من Cisco.</u>
 - 3. <u>التحقق من التكوين.</u>

ملاحظة: يناقش هذا المستند التكوين المطلوب على الجانب اللاسلكي. يفترض المستند أن التكوين السلكي في موضعه.

<u>تكوين وحدة التحكم في الشبكة المحلية (LAN) اللاسلكية</u>

على وحدة التحكم في الشبكة المحلية اللاسلكية، يجب القيام بما يلي:

- <u>خلقت VLAN للمستخدمين اللاسلكي.</u>
- <u>قم بتكوين عنصر التحكم في الشبكة المحلية اللاسلكية (WLC) لمصادقة المستخدمين اللاسلكيين مع Cisco.</u> Secure ACS<u>.</u>
 - إنشاء شبكة WLAN جديدة للمستخدمين اللاسلكيين.
 - <u>تحديد قوائم التحكم في الوصول (ACL) للمستخدمين اللاسلكيين.</u>

<u>خلقت VLAN للمستخدمين اللاسلكي</u>

أتمت in order to خلقت VLAN للمستخدمين اللاسلكي، هذا steps.

- 1. انتقل إلى واجهة المستخدم الرسومية (GUI) الخاصة بوحدة التحكم في الشبكة المحلية اللاسلكية (WLC) واختر **وحدة التحكم > الواجهات**. تظهر نافذة الواجهات. تسرد هذه النافذة الواجهات التي تم تكوينها على وحدة التحكم.
 - 2. انقر فوق **جديد** لإنشاء واجهة ديناميكية جديدة.
 - 3. دخلت في **القارن > جديد** نافذة، القارن إسم وال VLAN id. ثم انقر فوق تطبيق. في هذا المثال، يتم تسمية الواجهة الديناميكية باسم Office-VLAN، ويتم تعيين معرف شبكة VLAN على 20

cisco	MONITOR WL		WIRELESS	SECURITY	MANAGEMENT	Saye C COMMANDS	sofiguration Eing L HELP	ogout <u>R</u> efri
ntroller	Interfaces > N	lew					< Back	Apply
General	Interface Nan	Office-VLAN						
Inventory Interfaces	VLAN Id	20						
Internal DHCP Server								
Mobility Management								
Perts								
Master Controller Mode								
Network Time Protocol								
QoS								

4. في نافذة **الواجهات > تحرير**، ادخل عنوان IP وقناع الشبكة الفرعية والبوابة الافتراضية للواجهة الديناميكية. عينت هو إلى ميناء طبيعي على ال WLC، وأدخل العنوان من ال DHCP نادل. ثم انقر فوق **تطبيق**.

G • O • E E 🚯 🔑	🛧 🕘 📀 🖏 🖂							A - 8 >
cisco	MONITOR MLANS		WIRELESS	SECURITY	MANAGEMENT	Saya C COMMANDS	enfiguration Eing HELP	Logout Refres
Controller General Javentory Jaterfaces Internal DHCP Server Mobility Management Ports Master Controller Mode Network Time Protocol Potocol QoS CDP	MONITOR WLANS Interfaces > Edit General Informatio Interface Name MAC Address Interface Address Interface Address VLAN Identifier IP Address Netmask Gateway Physical Informatio Port Number Configuration Quarantine DHCP Information Primary DHCP Serve	CONTROLLER an Office-V 00:0b:0 20 372 255 372 00 372 255 372 00 372 172 00 172 00 172 00 172 172 00 172 172 00 172 172 00 172 172 172 172 172 172 172 172 172 172	WIRELESS			Seye C	enfiguration Eing HELP <back< td=""><td>Apply</td></back<>	Apply
	Secondary DHCP Se Access Control Lis ACL Name Note: Changing the Inte temporarily disabled an some clients.	t nor nave parameters d thus may result	ne 💌 s causes the Wi t In Joss of conr	LANs to be sectivity for				

Office-VLAN Office-VLAN IP address: 172.16.1.25 Netmask: 255.255.0.0 (Default gateway: 172.16.1.75 (sub-interface on Router R1 Port on WLC: 1 DHCP server: 172.16.1.75

<u>قم بتكوين عنصر التحكم في الشبكة المحلية اللاسلكية (WLC) للمصادقة مع Cisco Secure ACS</u>

يلزم تكوين عنصر التحكم في الشبكة المحلية اللاسلكية (WLC) لإعادة توجيه بيانات اعتماد المستخدم إلى خادم RADIUS خارجي (في هذه الحالة، مصدر المحتوى الإضافي الآمن من Cisco). يتحقق خادم RADIUS بعد ذلك من مسوغات المستخدم ويعيد سمة اسم قائمة التحكم بالوصول (ACL) إلى عنصر التحكم في الشبكة المحلية اللاسلكية (WLC) عند نجاح مصادقة المستخدم اللاسلكي.

أتمت هذا steps in order to شكلت ال WLC لنادل RADIUS:

- 1. أخترت **أمن** و**RADIUS مصادقة** من الجهاز تحكم gui أن يعرض **ال RADIUS صحة هوية نادل** صفحة. ثم انقر فوق **جديد** لتحديد خادم RADIUS.
- 2. قم بتعريف معلمات خادم RADIUS في **خوادم مصادقة RADIUS >** صفحة **جديدة**. وتتضمن هذه المعلمات عنوان IP لخادم RADIUS والسر المشترك ورقم المنفذ وحالة الخادم.

cisco	MONITOR WLANS CONTR	Sa <u>v</u> e Configuration Eing Logout OLLER WIRELESS <u>SECURITY</u> MANAGEMENT C <u>O</u> MMANDS HELP
Security	RADIUS Authentication 5	Servers > New < Back App
General	Server Index (Priority)	1 .
Authentication Accounting	Server IPAddress	10.77.244.196
TACACS+ LDAP	Shared Secret Format	ASCII -
Local Net Users MAC Filtering Disabled Clients	Shared Secret	•••••
User Login Policies AP Policies	Confirm Shared Secret	****
Local EAP	Key Wrap	(Designed for FIPS customers and requires a key wrap compliant RADIUS server)
Access Control Lists	Port Number	1812
IPSec Certs	Server Status	Enabled .
Policies	Support for RFC 3576	Enabled *
Web Auth CIDS	Retenend Timond	50
	Retransmit Timeout	ju seconas
	Network User	Enable
	Management	R Enable
	IPSec	Enable

3. تحدد خانات الاختيار **Network User** and **Management** ما إذا كانت المصادقة المستندة إلى RADIUS تنطبق على الإدارة ومستخدمي الشبكة. يستعمل هذا مثال ال cisco يأمن ACS كخادم RADIUS مع عنوان 10.77.244.196. طقطقة **يطبق**.

إنشاء شبكة WLAN جديدة للمستخدمين اللاسلكيين

بعد ذلك، يلزمك إنشاء شبكة WLAN يمكن للمستخدمين اللاسلكيين الاتصال بها. أتمت in order to خلقت WLAN جديد، هذا steps:

- 1. من واجهة المستخدم الرسومية (GUI) لوحدة تحكم الشبكة المحلية اللاسلكية، انقر على **شبكات WLAN**. تسرد هذه الصفحة شبكات WLAN الموجودة على وحدة التحكم.
- 2. أخترت **جديد** in order to خلقت WLAN جديد. أدخل معرف الشبكة المحلية اللاسلكية (WLAN) واسم ملف التعريف واسم شبكة WLAN للشبكة المحلية اللاسلكية (WLAN)، ثم انقر على **تطبيق**. لهذا الإعداد، قم بإنشاء Office لشبكة WLAN.

😋 • 😋 • 🖻 🖻 🏠 .	A 🛪 🙆 🐼 🖗 🖂 .				8999562	ense aver		🧾 🥂 – 8 ×
ululu cisco	MONITOR WEAKS	CONTROLLER	WIRELESS	SECURITY	MANAGEMENT	Sage Co	nfiguration Bing	Logout Refresh
WLANs	WLANs > New	CONTROLLER	WINCESS	gecontri	Management	CQM044D5	< Back	Apply
WLANS	WLAN ID	1 💌						
ar groups vitan	Profile Name	Office						
	HLAN SOLU	- Contract						

3. ما إن يخلق أنت WLAN جديد، ال **WLAN > تحرير** صفحة ل WLAN جديد يظهر. في هذه الصفحة، يمكنك تحديد معلمات مختلفة خاصة بشبكة WLAN هذه تتضمن السياسات العامة والأمان وجودة الخدمة والمعلمات المتقدمة.

cisco	Sage Configuration Eing Logout Bet
/LANs	WLANs > Edit Apply
WLANS WLANS AP Groups VLAN	General Security QoS Advanced Profile Name Office WLAN SSID Office WLAN Status Image: Control of the control of t
	Foot Notes I CKIP is not supported by I0xx model APs 3 H-REAP Local Switching is not supported with IPsec, CRANITE and FORTRESS authentication 4 When client exclusion is enabled, a Timeout Value of zero means infinity (will require administrative override to reset excluded clients) 5 Client MFP is not active unless WPA2 is configured

تحقق من **حالة شبكة WLAN** ضمن السياسات العامة لتمكين شبكة WLAN. أختر الواجهة المناسبة من القائمة المنسدلة. في هذا المثال، أستخدم الواجهة Office-VLAN. يمكن تعديل المعلمات الأخرى في هذه الصفحة استنادا إلى متطلبات شبكة WLAN.

4. أختر **علامة التبويب تأمين**. أختر **802.1x** من قائمة المنسدلة أمان الطبقة 2 (لأنها مصادقة LEAP). أختر حجم مفتاح WEP المناسب تحت معاملات 802.1x.

cisco	Sage Configuration Eing MONITOR WLANS CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP	Logout Befr
ANs.	WLANs > Edit < Back	Apply
WLANS WLANS AP Groups VLAN	General Security QoS Advanced Layer 2 Layer 3 AAA Servers	
	Layer 2 Security 802.1X	
	802.11 Data Encryption Type Key Size	
	@ WEP 104 bits +	
	ter i fan den de nationale de desense de la sense de la desense de la desense de la desense de la desense de la Not	SPHILLIPSIS
	1 CKIP is not supported by 10xx model APs	
	3 H-REAP Local Switching is not supported with IPsec, CRANITE and FORTRESS authentication 4 When client exclusion is enabled, a Timeout Value of zero means infinity (will require administrative override to reset excli	uded clients)
	5 Client MFP is not active unless WPA2 is configured	

5. تحت علامة التبويب تأمين، أختر علامة التبويب الفرعية **AAA server**. أختر خادم AAA الذي يتم إستخدامه لمصادقة العملاء اللاسلكيين. في هذا المثال، أستخدم خادم ACS 10.77.244.196 لمصادقة العملاء اللاسلكيين.

ANS WI	LANs > Edit < Back	Apply
/LANS		
WLANS AP Groups VLAN	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 1 None . R Enabled Server 2 None .	
<	Server 3 None Se	
	2 None None	
	Server None · None ·	
	Local EAP Authentication	
	Local CAP AddiendLadon 1. Englied	
	Foot Notes	
-	I CKIP is not supported by 10xx model APs 3 H-REAP Local Switching is not supported with IPsec, CRANITE and FORTRESS authentication 4 When client exclusion is enabled, a Timeout Value of zero means infinity (will require administrative override to reset ex 5 Client MRP is not active unless WPA2 is configured	cluded clients

6. أختر علامة التبويب **خيارات متقدمة**. تحقق من **السماح بتجاوز AAA** لتكوين تجاوز سياسة المستخدم من خلال AAA على شبكة LAN لاسلكية.

cisco	Save Configuration Engl Logout Br MONITOR WLANS CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP
/LANS WLANS WLANS AP Groups VLAN	WLANs > Edit < Back Apply General Security QoS Advanced Allow AAA Override Isebled DHCP Override H-REAP Local Switching & Enabled DHCP Server Override Session Timeout (secs) Is00 DHCP Addr. Assignment Required Aironet IE It Enabled DHCP Addr. Assignment Required Override Interface ACL None Imagement Frame Protection (MFP) (Global MPP Disabled) Override Interface ACL None Imagement Value (secs) MPP Client Optional Imagement Protection 1 Client Exclusion 1 If Enabled MPP Client Optional Imagement Protection 2 Optional Imagement Protection 3 Foot Notes If the supported by 10xx model APx Section 1 Imagement Protection 3 Optional Imagement Protection 3

عند تمكين تجاوز AAA، ولدى العميل معلمات مصادقة AAA متعارضة مع وحدة تحكم الشبكة المحلية (LAN) اللاسلكية من Cisco ووحدة تحكم الشبكة المحلية اللاسلكية من Cisco، يتم إجراء مصادقة العميل بواسطة خادم AAA. كجزء من هذه المصادقة، ينقل نظام التشغيل العملاء من حل شبكة LAN اللاسلكية الافتراضي من Cisco إلى شبكة VLAN اللاسلكية إلى شبكة VLAN التي يتم إرجاعها بواسطة خادم AAA والمحددة مسبقا في تكوين واجهة وحدة التحكم في شبكة LAN اللاسلكية من Cisco، والتي تحدث فقط عند تكوينها لتصفية MAC، و/أو XLAN، و/أو عملية AAA في شبكة LAN اللاسلكية من Cisco، والتي تحدث فقط عند تكوينها لمونية MAC، ورأو XLAN، ورأو عملية AAA، وفي جميع الحالات، يستخدم نظام التشغيل أيضا قيم الأولوية لجودة الخدمة (QoS) و DSCP وقيم علامات الأولوية المتوافقة مع معيار 20.19 وقوائم التحكم في الوصول (ACL) المقدمة من خادم AAA، طالما تم تعريفها مسبقا في تكوين واجهة وحدة التحكم في المحلية اللاسلكية من Cisco.

7. أختر المعلمات الأخرى استنادا إلى متطلبات الشبكة. طقطقة **يطبق**.

<u>تحديد قوائم التحكم في الوصول (ACL) للمستخدمين</u>

تحتاج إلى إنشاء قوائم التحكم في الوصول (ACL) لهذا الإعداد:

- ACL1: لتوفير الوصول إلى User1 إلى الخادم 172.16.1.100 فقط
 - ACL2: لتوفير الوصول إلى User2 إلى الخادم 172.16.1.50 فقط

أتمت هذا steps أن يشكل ال ACLs على ال WLC:

- 1. من واجهة المستخدم الرسومية (GUI) الخاصة بوحدة التحكم في الوصول اللاسلكية (WLC)، أختر **الأمان > قوائم التحكم في الوصول**. تظهر صفحة قوائم التحكم في الوصول. تسرد هذه الصفحة قوائم التحكم في الوصول (ACL) التي تم تكوينها على عنصر التحكم في الوصول (WLC). كما يتيح لك تحرير أي من قوائم التحكم في الوصول (ACL) أو إزالته. لإنشاء قائمة تحكم في الوصول (ACL) جديدة، انقر فوق **جديد**.
- 2. تسمح لك هذه الصفحة بإنشاء قوائم التحكم في الوصول (ACL) جديدة. أدخل اسم قائمة التحكم في الوصول (ACL) وانقر فوق **تطبيق**. بمجرد إنشاء قائمة التحكم في الوصول (ACL)، انقر فوق **تحرير** لإنشاء قواعد

لقائمة التحكم في الوصول (ACL).

3. يجب أن يكون المستخدم1 قادرا على الوصول إلى الخادم 172.16.1.100 فقط ويجب رفضه من الوصول إلى جميع الأجهزة الأخرى. لهذا، تحتاج إلى تعريف هذه القواعد.راجع <u>قوائم التحكم في الوصول (ACL) على مثال</u> <u>تكوين وحدة تحكم الشبكة المحلية اللاسلكية</u> للحصول على مزيد من المعلومات حول كيفية تكوين قوائم التحكم في الوصول (ACL) على وحدات التحكم في الشبكة المحلية

cisco	MONI	TOR W	LANS CONTR	OLLE	R WIRELESS	SECU	RITY Mé	NAGEMENT	COMMANDS	HELP	Eing	.ogout <u>R</u> efre
Security	Acce	ess Con	trol Lists > E	dit					< 8	ack	Add New	Rule
▼ AAA General ▼ RADIUS	Gene	s List Nam	e User1									
Accounting + TACACS+	Seq	Action	Source IP/M	sk	Destination IP/Mask	,	Protocol	Source Port	Dest Port	DSCP	Direction	
LDAP Local Net Users MAC Filtering	1	Permit	172.16.0.0 255.255.0.0	/	172.16.1.100 255.255.255.255	/	Any	Any	Αογ	Any	Inbound	
Disabled Clients User Login Policies AP Policies	2	Permit	172.16.1.100 255.255.255.25	, 55	172.16.0.0 255.255.0.0	<i>'</i>	Any	Any	Any	Any	Outbound	۵
Local EAP	L											
Priority Order												
Access Control Lists Access Control Lists CPU Access Control Lists												
IPSec Certs												
Wireless Protection Policies												
Web Auth												
▶ CIDS												

4. وبالمثل، يلزمك إنشاء قائمة تحكم في الوصول (ACL) للمستخدم 2، والتي تتيح للمستخدم 2 إمكانية الوصول إلى الخادم 172.16.1.50 فقط. هذه هي قائمة التحكم في الوصول (ACL) المطلوبة للمستخدم 2.

cisco	MONT	TOR W	LANS <u>C</u> ONTRO	DLLE	R WIRELESS	Se	CURITY M	SNAGEMENT	Saye Co COMMANDS	nfiguration HELP	Eing	Logout (
Security	Acce	ss Con	trol Lists > Eq	dit					< 84	ick	Add Net	v Rule
• AAA General • RADIUS	Gene	rral s List Nam	e User2									
Accounting + TACACS+	Seq	Action	Source IP/Ma	sk	Destination IP/Mask		Protocol	Source Port	Dest Port	DSCP	Direction	
LDAP Local Net Users MAC Filtering	4	Permit	172.16.0.0 255.255.0.0	/	172.16.1.50 255.255.255.255	/	Any	Any	Απγ	Any	Inbound	۰
Disabled Clients User Login Policies AP Policies	2	Permit	172.16.1.50 255.255.255.25	s ′	172.16.0.0 255.255.0.0	/	Any	Any	Any	Any	Outbound	٠
Local EAP												
Priority Order												
Access Control Lists Access Control Lists CPU Access Control Lists												
IPSec Certs												
Wireless Protection Policies												
Web Auth												
) CIDS												

لقد انتهيت الآن من تكوين وحدة التحكم في الشبكة المحلية اللاسلكية لهذا الإعداد. تتمثل الخطوة التالية في تكوين خادم التحكم في الوصول الآمن من Cisco لمصادقة العملاء اللاسلكي وإعادة سمة اسم قائمة التحكم في الوصول (ACL) إلى عنصر التحكم في الوصول الآمن (WLC) عند المصادقة الناجحة.

<u>تكوين خادم ACS الآمن من Cisco</u>

لكي يتمكن ACS الآمن من Cisco من مصادقة الأجهزة اللاسلكية العميلة، يلزمك استكمال الخطوات التالية:

• <u>قم بتكوين وحدة التحكم في الشبكة المحلية اللاسلكية كعميل AAA على Cisco Secure ACS.</u>

• <u>قم بتكوين المستخدمين وملفات تعريف المستخدمين على ACS الآمن من Cisco.</u>

<u>تكوين وحدة التحكم في الشبكة المحلية اللاسلكية كعميل AAA على Cisco Secure ACS</u>

لتكوين وحدة التحكم في الشبكة المحلية اللاسلكية كعميل AAA على Cisco ACS الآمن، أكمل الخطوات التالية:

1. انقر فوق **تكوين الشبكة > إضافة عميل AAA**. تظهر صفحة **إضافة عميل AAA**. في هذه الصفحة، قم بتعريف اسم نظام WLC وعنوان IP لواجهة الإدارة والسر المشترك والمصادقة باستخدام **Radius Airespace**. فيما يلي «الب

مثال:

isco Statema	Network Configuration	
	Edit	Help
User Setup Setup Satup Shared Profile Composed Is Composed Is Configuration Settem Configuration Interface Configuration	Add AAA Client AAA Client Hostname wlc AAA Client IP Address 10.77.244.210 Shared Secret cisco	AAA Client Hestmann AAA Client IP Address Shared Secret Network Device Group BADIUS Key Youg Authenticate Using Single Connect TACACS - AAA Client Los Badate/Wathdeg Packets from th AAA Client Los Badate/Wathdeg Packets from th AAA Client Beplace BADIUS Part info with Usernar from this AAA Client Math Franch IP Address with user IP
Administration Control External User Databases Validation Validation	RADIUS Key Wrap Key Encryption Key Message Authenticator Code Key Key Input Format C ASCII Hexadecimal	Address for accounting packets from the AAA Client AAA Client Hestname The AAA Client Hostname is the name assigned to the AAA client.
Reports and	Authenticate Using RADIUS (Cisco Airespace)	[Back to Top]
Online	Single Connect TACACS+ AAA Client (Record stop in accounting on failure)	AAA Client IP Address
Documentation	Log Update/Watchdog Packets from this AAA Client Log RADIUS Tunneling Packets from this AAA Client	The AAA Client IP Address is the IP address assigned to the AAA client.
	Replace RADIUS Port info with Username from this AAA Client Match Framed-IP-Address with user IP address for accounting packets from this AAA Client	If you want to designate more than one AAA client with a single AAA client entry in ACB, you can specify the IP address for each AAA client to be represented by this AAA client entry. To separate each IP address, press Enter.
	Submit Submit + Apply Cancel	You can use the wildcard asterisk (*) for an octet in the IP address. For example, if you want every AAA client in your 192.168.13.1

مع السر المشترك الذي تم تكوينه على Cisco Secure ACS مع السر المشترك الذي تم تكوينه على عنصر التحكم في الشبكة المحلية اللاسلكية (WLC) تحت **خوادم مصادقة RADIUS > جديد**. 2. انقر فوق **إرسال+تطبيق**.

<u>تكوين المستخدمين وملف تعريف المستخدم على ACS الآمن من Cisco</u>

أتمت in order to شكلت مستعمل على ال cisco يأمن ACS، هذا steps:

1. أخترت **مستعمل setup** من ال ACS gui، دخلت ال username، وطقطقة **يضيف/يحرر**. في هذا المثال، المستخدم هو Us**er1**.

Intervention Store Image: Store Heip Image: Store Heip Image: Store Image: Store
 Setep <
Note: User Setup does not add or delete usernames in an exter database. [Back to Top] Finding a Specific User in the ACS Internal Database To find a user already in the ACS internal database, type the Sc of the username in the User field, add an asterisk (*) as a vildo. Find. From the list of usernames displayed, click the username information you want to view or change. [Back to Top]
Adding a User to the ACS Internal Database

2. عندما تظهر صفحة **إعداد المستخدم**، قم بتعريف كافة المعلمات الخاصة بالمستخدم. في هذا المثال، يتم تكوين اسم المستخدم وكلمة المرور ومعلومات المستخدم التكميلية وسمات RADIUS لأنك تحتاج فقط إلى هذه المعلمات لمصادقة EAP.

Cisco Systems	User Setup	
adillinadillina	Edit	Help
User Setup	User: UserA (New User)	Account Disabled Deloting a Disensity Supplementary liser Infe
Shared Profile	C Account Disabled	Password Authentication Group to which the user is assigned
Network Configuration	Supplementary User Info	Calback Client IP Address Assignment Advanced Settings
Sustem Configuration	Real Name User 1 Description	histwork Access Restrictions Hast Sessions Diago Questas
Administration		Account Disable Downloadable ACLs Advanced TACACS+ Settings TREATS For Control
Centrel Disternal User Databases	User Setup	TACACS - Enable Password TACACS - Dathend Password TACACS - Outbound Password TACACS - Shell Command Authorization Command Authorization
Pesture Validation	CiscoSecure PAP (Also used for CHAP/MS-	TACACS - Unknown Services IETE RADIUS Attributes RADIUS Yeador-Specific Attributes
Reports and Activity	CHAP/ARAP, if the Separate field is not checked.) Password	
Documentation	Password Separate (CHAP/MS-CHAP/ARAP)	Account Disabled Status Select the Account Disabled check box to disable this accounty clear the check box to enable the account.
	Password	[Back to Tee]
	Confirm	Deleting a Username
	When a token server is used for authentication, supplying a separate CHAP password for a token card user allows CHAP authentication. This is	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 Delete . When asked to confirm your action, click DK .
	especially useful when token caching is enabled.	[Back to Top]
	Group to which the user is assigned:	▼ Supplementary User Info
	Submit Cancel	Type the applicable information in any supplemental user information boxes that appear. To add or chance fields, click interface

ق**م** بالتمريز إلى اشقل حتى ترى شمات ACS لتمكين ACS لإعادة اسم قائمة التحكم في الوصول (ACL) إلى عنصر التحكم في الشبكة المحلية اللاسلكية (WLC) مع إستجابة المصادقة الناجحة. بالنسبة للمستخدم 1، قم بإنشاء مستخدم قائمة تحكم في الوصول (1 (ACL على عنصر التحكم في الشبكة المحلية اللاسلكية (WLC). أدخل اسم قائمة التحكم في الوصول (ACL) ك

.User1

Sep v 9 2007 uccessful rempts count IS Amributes	Holp Account Disabled Beloting a Bromans Supplementary User Info Password Authentication Group to which the user is assigned Callback Callback Callback Chron IP Address Assignment Advanced Settings Natural Account Disable Bowelsadable Afts Advanced IACACS+ Sattings TACACS- Coubel
Sep 9 2007 uccessful compts count IS Antributes	Account Disabled Defiction a Biommann Supplementary User Info Password Authentication Group to which the user is assigned Caliback Client IP Address Assignment Advanced Settlings Natwork Access Restrictions Hax Sessions Bioage Qustas Account Disable Downloadable AtLs Advanced IACACS - Settings TACACS - Enable Control
uccessful rempts count 15 Attributes	Account Disabled Deleting a Breemense Supplementary User Info Password Authentication Group to which the user is assigned Calback Client IP Address Assignment Advanced Settings Natwork Access Restrictions Has Sessions Disage Quotas Account Disable Downloadable ACLs Advanced IACACS - Settings TACACS + Enable Control
uccessful rempts count 15 Antributes	Best ting a Supermann Supplementary User Info Password Authentication Group To which the user is assigned Callback Client IP Address Assignment Advanced Settings Natwork Access Restrictions Max Sessions Disage Quotas Accessnt Disable Downloadable ACLs Advanced IACACs Settings TACACS + Enable Control
uccessful compts count IS Antributes	Password Authentication Group to which the user is assigned Callback Client IP Address Assignment Advanced Settings Natwork Access Restrictions Max Sessions Usage Quotas Accessnt Disable Downloadable Downloadable Downloadable TACACS - Settings TACACS - Enable Control
IS Antributes	Group In which the user is assigned Callback Client IP Address Assignment Advanced Settings Nativerk Access Restrictions Max Sessions Disage Quotas Accessnt Disable Downloadable Downloadable TACACS - Settings TACACS - Enable Control
IS Antributes	Calman Clent ID Advance Assignment Advanced Settings National Access Restrictions Hax Sessions Disage Questas Accessnt Disable Downloadable Alt_s Advanced IACACS= Settings TACACS+ Enable Control
IS Antributes	Advanced Settings National Access Restrictions Hax Sessions Disage Questas Account Disable Downloadable ACLs Advanced IACACS - Settings TACACS - Enable Control
IS Antributes 👔	Nativark Access Restrictions Hax Sessions Brage Qustas Accesst Disable Bowelsadable ACLs Advanced IACACS - Settings TACACS - Enable Control
IS Antributes 👔	Plan Sessions Plan Sessions Plan Sessions Account Disable Powwels-adable Afts Advanced TACACS- Settings TACACS- Enable Control
IS Antributes 👔	Account Disable Bownloadable ACLs Advanced TACACS+ Settings TACACS+ Enable Control
IS Attributes 🦹	Bownloadable ACLs Advanced TACACS+ Settings TAEACS+ Enable Control
US Antributes ?	Advanced TACACS+ Settings TACACS+ Enable Control
US ANDARES	There are an and a second and a
	TACACS + Enable Password
	TACACS+ Outbound Password
	TACACS+ Shell Command Authorization Command Authorization
Bronze	TACACS+ Unknown Services
	1ETF RADIUS Attributes
0	RADIUS Veador-Specific Attributes
	-
0	Aurorat Bio Mind States
	Account disasted scalas
	 Select the Account Disabled check box to disable this account clear the check box to enable the account.
	IBack to Tapl
	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 Delete . When asked to
	confirm your action, click OK.
	[Back to Tap]
andp	further to be be
	apprenentary User Into
Cancel	Type the applicable information in any supplemental user information
	Cancel

هنا.

user Setup User Setup user Setup S	0 · O · E E :	\$1,2 \$ € @·\$ ⊒	🔊 - 8 ×
Extra series Ex	Cisco Systems	User Setup	×
 	adlinadiina	Select	Help
Constant Research And Constant Research Res	Userp Setup Setup Setup Setup Setup Setup Setup Components Seture Configuration Seture Configuration Seture Validation Petiture Validation Seture Validation Seture Validation Seture Validation Security Seture Validation Security Seture Validation Security Seture Validation	User: User2 Find Add/Edit List users beginning with letter/number: ABCPEISENIUYVXI DIRIGING STARE List all users Remove Dynamic Users	 9. Nex Setse and Satemal Back Databases 9. Nex Setse is the ACS Internal Databases 9. Next Setse is the Action of Setse is and External User Databases 9. Next Setse is the Action of Setse is and External Servers. For Setse and Databases is the Action of Setse is the Action of Setse is and Setseral User Databases. 9. Next User Setse configuration oriented Setseral User Databases is server music is and properly configuration oriented Setseral User Databases is setting in the ACS Internal Actions of Setse is and Setseral User Databases is setting. Next User Setse configuration oriented Setseral User Databases for setseral databases is setting. Next User Setse is the ACS Internal Actions and the setseral server is a setteral user latabases is setting. Next User Setse is setting is the ACS internal database for setseral database. Next User Setse is the ACS internal Database. Next User Setse is setseral and an delete usernames in an external user fate. Next User Setse is setseral and an action of the setseral is a set in the ACS internal Database. Next User Setse is setse is setserais (f¹) as a violation and catabase is i
Lists Strifter User Setup Edit User: UserA (New User) Image: Setup Image: Setup Image: Setup Image: Setup <tr< th=""><th>0 · 0 · E =</th><th>\$ P 🛪 🖶 🗇 🖏 🖽</th><th></th></tr<>	0 · 0 · E =	\$ P 🛪 🖶 🗇 🖏 🖽	
Image: State of the second disable Image: State of the second disable Image: State of the second disable Image: State of the second disable Image: State of the second disable Image: State of the second disable Image: State of the second disable Image: State of the second disable Image: State of the second disable Image: State of the second disable Image: State of the second disable Image: State of the second disable Image: State of the second disable Image: State of the second disable Image: State of the second disable Image: State of the second disable Image: State of the second disable Image: State of the second disable Image: State of the second disable Image: State of the second disable Image: State of the second disable Image: State of the second disable Image: State of the second disable Image: State of the second disable Image: State of the second disable	Cisco Systems	User Setup	X
User: User: UserA (New User) User: User: User Info User: User: User: User Info User:	dbdb	Edit	A Help
Submit Cancel Type the applicable information in any supplemental user information benes that appear. To add or chance fields, click Interface	User Setup Setup Setup Setup Setup Setup Setup Retwork Configuration Con	User: UserA (New User)	 Account Disabled Babinton a Stremments Basinementary User Jarks Basine Jarks Basinementary User J
		Submit Cancel	Type the applicable information in any supplemental user information boxes that appear. To add or change fields, click laterface

🔾 • 🗇 • 🖻 🗐 (81 A 🖉 🗢 🕼 😼 🖬	👘 – 🕫 🛪
Cisco Systems	User Setup	×
-dbdb	Date exceeds:	Help
User Setup Setup Components Components Configuration	Sep 9 2007 Failed attempts exceed: Failed attempts since last successful login: 0 Reset current failed attempts count on submit Clicce Alirespace RADIUS Attributes [141794002] Aire-QoS-Level Bronze [141794003] Aire-DSCP	 Account Disabled Defining a Biogname Supplementary User Info Supplementary User Info Supplementary User Info Calback Calback Calback Client IP Address Assignment Advanced Settings Nationark Access Restrictions Max Session Usage Outlas Account Disable Maxage Outlas Account Disable Advanced Settings Advanced Interventions Maxage Outlas Account Disable Advanced IACACS - Settings MACACS - Enable Control MACACS - Enable Control MACACS - Setting Outlas MACACS - Contheous Password MACACS - Contheous Password MACACS - United Command Authorization Command Authorization for Network Device Management Applications MACAS - United Services IETE BADIUS Attributes
Reports and Activity Documentation		Account Disabled Status Select the Account Disabled check box to disable this account; clear the check box to enable the account; [Acct to Tap] Deleting a Utername Account, not 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 Delete. When asked to certify your action, click DK. [Rack to Tap] Supplementary User Info
	Submit Cancel	Type the applicable information in any supplemental user information boxes that appear. To add or change fields, click Interface

4. انقر على **تكوين النظام وإعداد المصادقة العامة** لضمان تكوين خادم المصادقة لتنفيذ أسلوب مصادقة EAP المطلوب. تحت إعدادات تكوين EAP، أختر أسلوب EAP المناسب. يستخدم هذا المثال مصادقة LEAP. انقر فوق **إرسال** عند الانتهاء.

ISCO STATEMA	System Configuration	
. دالهدلله	PEAP	Help
User	Allow EAP-MSCHAPv2	
Setup	Allow EAP-GTC	Use this page to specify settings for various authentication protocols.
Greup Setup	Allow Posture Validation	EAP Configuration
Shared Profile Components	Allow FAR-TLS	• PCAP • EAP-FAST
1 But and	Select one or more of the following options:	• EAP-TLS • LEAP
Configuration	E Certificate SAN comparison	· EAP-HDS
System	E Certificate CN comparison	AP LAP Request Timeout MS-CHAP Configuration
Configuration	E Certificate Binary comparison	
Configuration	EAD-TI 5 session timeout (minutes)	
Administration	EXP-123 SESSION CENEOUS (INFIDIES), [120	EAP Configuration
	Cisco client initial message:	EAP is a flexible request-response protocol for arbitrary
Databases	PEAP session timeout (minutes): 120	authentication information (RPC 2204). EAP is layered on tap of another protocol such as UDP, 802.1x or RADIUS and supports
Pesture Validation	Enable Fast Reconnect:	multiple "authentication" types.
Network Access		[back to Tap]
Profiles	EAP-FAST	PEAD
Reports and Activity	EAP-FAST Configuration	PEAP is the outer layer protocol for the secure tunnel.
Online	EAP-TLS	
Documentation	Allow EAP-TLS	Notes IEAP is a curtificate-based authentication protocol. IEAP authentication can accur only after you have curealeted the required steps
	Select one or more of the following options:	to the ACS Centificate Setup page.
	Certificate SAN comparison	 Allow EAP-MSCHAPv2 — Use to enable EAP-MSCHAPv2 within MS PEAP
	Certificate CN comparison	authentication. Enable this protocol for any repository that supports MS-
	R Certificate Binary comparison	strate values as received on they and the received and the backbase.
	EAP-TLS session timeout (minutes): 120	 Allow EAP-GTC — Use to enable EAP-GTC within Cisce PEAP authenticati Enable this protocol to support any database that supports PAP, including LDAP, OTP Servers, and the ACS Internal Database.
C	LEAP	Allow Porture Validation Use to enable the PEAP (EAP-TLV) protocol for
-	Allow LEAP (For Aironet only)	posture validation of Network Admission Control (NAC) clients.
	Submit Submit + Restart Cancel	 Allow EAP-TLS - Use to enable the EAP-TLS protocol as an additional inst

<u>التحقق من الصحة</u>

استخدم هذا القسم لتأكيد عمل التكوين بشكل صحيح.

حاول إقران عميل لاسلكي مع نقطة الوصول في الوضع Lightweight مع مصادقة LEAP للتحقق مما إذا كان التكوين يعمل كما هو متوقع.

ملاحظة: يفترض هذا المستند تكوين ملف تعريف العميل لمصادقة LEAP. ارجع إلى <u>إستخدام مصادقة EAP</u> للحصول على مزيد من المعلومات حول كيفية تكوين مهايئ العميل اللاسلكي a/b/g 802.11 لمصادقة LEAP.

بمجرد تنشيط توصيف العميل اللاسلكي يطلب من المستخدم توفير اسم المستخدم/كلمة المرور لمصادقة LEAP. هذا ما يحدث عندما يحاول User1 المصادقة على نقطة الوصول في الوضع Lightweight (LAP).

Please enter your Lt network	AP username and password to log on to the wireless
User Name :	User1
Password :	•••••
Log on to :	
Card Name :	Cisco Aironet 802.11a/b/g Wireless Adapter
Profile Name	Office

تمرر نقطة الوصول في الوضع Lightweight ثم عنصر التحكم في الشبكة المحلية اللاسلكية (WLC) بيانات اعتماد المستخدم إلى خادم RADIUS الخارجي (Cisco Secure ACS) للتحقق من بيانات الاعتماد. يقوم خادم RADIUS بمقارنة البيانات بقاعدة بيانات المستخدم، وبعد نجاح المصادقة، يرجع اسم قائمة التحكم في الوصول (ACL) الذي تم تكوينه للمستخدم إلى عنصر التحكم في الشبكة المحلية اللاسلكية (WLC). في هذه الحالة، يرجع قائمة التحكم في الوصول (ACL User) إلى عنصر التحكم في الشبكة المحلية اللاسلكية (WLC). في هذه الحالة، يرجع قائمة التحكم في

😨 Cisco Aironet Desktop Utility	y - Current Profil	e: Office-TSWEB	? 🔀
Action Options Help			
Current Status Profile Management	Diagnostics		
CISCO SYSTEMS			
utilitumutilitu Profile Name:	Office-TSWEB		
Link Status:	Authenticated	Network Type: Infrastructure	
Wireless Mode:	5 GHz 54 Mbps	Current Channet: 64	
Server Based Authentication:	LEAP	Data Encryption: WEP	
IP Address:	172.16.0.14		
Signal Strength:		Excellent	
		Advanced	

تقوم وحدة التحكم في الشبكة المحلية اللاسلكية بتطبيق قائمة التحكم في الوصول (ACL) هذه على المستخدم 1.

يوضح إخراج إختبار الاتصال هذا أن User1 قادر على الوصول إلى الخادم 172.16.1.100 فقط، وليس إلى أي جهاز آخر.

```
D:\Documents and Settings\Administrator>ping 172.16.1.100
               :Pinging 172.16.1.100 with 32 bytes of data
       Reply from 172.16.1.100: bytes=32 time=3ms TTL=255
       Reply from 172.16.1.100: bytes=32 time=1ms TTL=255
       Reply from 172.16.1.100: bytes=32 time=1ms TTL=255
       Reply from 172.16.1.100: bytes=32 time=1ms TTL=255
                         :Ping statistics for 172.16.1.100
 ,(Packets: Sent = 4, Received = 4, Lost = 0 (0% loss
           :Approximate round trip times in milli-seconds
          Minimum = 1ms, Maximum = 3ms, Average = 1ms
 D:\Documents and Settings\Administrator>ping 172.16.1.50
                :Pinging 172.16.1.50 with 32 bytes of data
                                        .Request timed out
                                        .Request timed out
                                        .Request timed out
                                        .Request timed out
                          :Ping statistics for 172.16.1.50
, (Packets: Sent = 4, Received = 0, Lost = 4 (100% loss
```

بالمثل، عندما يحاول User2 الوصول إلى الشبكة المحلية اللاسلكية (WLAN)، يرجع خادم RADIUS، عند المصادقة الناجحة، مستخدم ACL2 إلى عنصر التحكم في الشبكة المحلية اللاسلكية (WLC).

Enter Wireless N	etwork Password 🗙 🗙
Please enter your LE network	EAP username and password to log on to the wireless
User Name :	User2
Password :	•••••
Log on to :	
Card Name :	Cisco Aironet 802.11 a/b/g Wireless Adapter
Profile Name :	Office
	OK Cancel

Authentication Status	? -
Card Name: Cisco Aironet 802.11	1 a/b/g Wireless Adapter
Profile Name: Office-TSWEB	
Steps	Status
1. Starting LEAP Authentication	Success
2. Checking Link Status	Success
3. Renewing IP address	Success
4. Detecting IPX Frame Type	Success
5. Finding Domain Controller	Skipped because the domain name was not configured

تقوم وحدة التحكم في الشبكة المحلية اللاسلكية بتطبيق قائمة التحكم في الوصول (ACL) هذه على المستخدم 2. يوضح إخراج إختبار الاتصال هذا أن User2 قادر على الوصول إلى الخادم 172.16.1.50 فقط، وليس إلى أي جهاز آخر.

> D:\Documents and Settings\Administrator>ping 172.16.1.50 :Pinging 172.16.1.50 with 32 bytes of data Reply from 172.16.1.50: bytes=32 time=3ms TTL=255 Reply from 172.16.1.50: bytes=32 time=18ms TTL=255 Reply from 172.16.1.50: bytes=32 time=1ms TTL=255 Reply from 172.16.1.50: bytes=32 time=1ms TTL=255 :Ping statistics for 172.16.1.50 ,(Packets: Sent = 4, Received = 4, Lost = 0 (0% loss :Approximate round trip times in milli-seconds Minimum = 1ms, Maximum = 18ms, Average = 5ms D:\Documents and Settings\Administrator>ping 172.16.1.100 :Pinging 172.16.1.100 with 32 bytes of data .Request timed out .Request timed out .Request timed out .Request timed out :Ping statistics for 172.16.1.100 , (Packets: Sent = 4, Received = 0, Lost = 4 (100% loss

<u>استكشاف الأخطاء وإصلاحها</u>

يوفر هذا القسم معلومات يمكنك استخدامها لاستكشاف أخطاء التكوين وإصلاحها.

على وحدة التحكم في الشبكة المحلية اللاسلكية، يمكنك أيضا إستخدام أوامر تصحيح الأخطاء هذه لاستكشاف أخطاء مصادقة AAA وإصلاحها • debug aaa all enable—يشكل تصحيح أخطاء جميع رسائل AAA

• debug dot1x ربط enable يمكن ال debug dot1x لكل ربط debug

• تصحيح أخطاء العميل <MAC Address>—تمكين تصحيح أخطاء العميل اللاسلكي

هنا مثال من **ال debug aaa all enable** أمر

ملاحظة: تم نقل بعض البنود في الناتج إلى السطر الثاني بسبب قيود المساحة.

Thu Aug 16 14:42:54 2007: AuthenticationRequest: 0xb1ab104 Thu Aug 16 14:42:54 2007: Callback.....0x85ed228 Thu Aug 16 14:42:54 2007: protocolType.....0x00140001 Thu Aug 16 14:42:54 2007: proxyState.....00:40:96:AF:3E:93-03:01 (Thu Aug 16 14:42:54 2007: Packet contains 16 AVPs (not shown Thu Aug 16 14:42:54 2007: 00:40:96:af:3e:93 Successful transmission of Authentication Packet id 1) to 10.77.244.196:1812, proxy state 00:40:96:af:3e:93-00:00) Thu Aug 16 14:42:54 2007: 00000000: 01 01 00 d0 2d 34 f5 99 b4 19 27 28 eb 5f 35 9c .5_.)'...-4.... Thu Aug 16 14:42:54 2007: 00000010: 8f a9 00 dd 01 07 75 73 65 72 31 1f 13 30 30 2d user1..00-.... Thu Aug 16 14:42:54 2007: 00000020: 34 30 2d 39 36 2d 41 46 2d 33 45 2d 39 33 1e 20 ..40-96-AF-3E-93 Thu Aug 16 14:42:54 2007: 00000030: 30 30 2d 30 42 2d 38 35 2d 35 42 2d 46 42 2d 44 00-0B-85-5B-FB-D Thu Aug 16 14:42:54 2007: 00000040: 30 3a 4f 66 66 69 63 65 2d 54 53 57 45 42 05 06 .. Office-TSWEB:0 Thu Aug 16 14:42:54 2007: 00000050: 00 00 01 04 06 0a 4d f4 d2 20 05 77 6c 63 1a .M....wlc..... Thu Aug 16 14:42:54 2007: 00000060: 0c 00 00 37 63 01 06 00 00 00 01 06 06 00 00 007c... Thu Aug 16 14:42:54 2007: 00000070: 02 0c 06 00 00 05 14 3d 06 00 00 00 13 40 06 00 ...@.....=..... Thu Aug 16 14:42:54 2007: 0000080: 00 00 0d 41 06 00 00 00 06 51 04 32 30 4f 27 02 .'A....Q.200... Thu Aug 16 14:42:54 2007: 00000090: 01 00 25 11 01 00 18 1d 87 9d 0b f9 dd e5 39 0d .9....%.. Thu Aug 16 14:42:54 2007: 000000a0: 2e 82 eb 17 c6 23 b7 96 dc c3 55 ff 7c 51 4e 75 U. |QNu....#.... Thu Aug 16 14:42:54 2007: 000000b0: 73 65 72 31 18 0a 53 56 43 3d 30 2e 31 3b 50 12 .ser1..SVC=0.1;P Thu Aug 16 14:42:54 2007: 000000c0: 1a d5 3b 35 5e 93 11 c0 c6 2f 5e f5 65 e9 3e 2d -<.e.^/...^5;.. Thu Aug 16 14:42:54 2007: 00000000: 0b 01 00 36 8c 31 6a b4 27 e6 d4 0e 1b 8e 5d 19 .[....'.6.1j... Thu Aug 16 14:42:54 2007: 00000010: 60 1c c2 16 4f 06 03 01 00 04 18 0a 53 56 43 3d =0....SVC... Thu Aug 16 14:42:54 2007: 00000020: 30 2e 31 3b 50 12 6c fb 90 ec 48 9b fb d7 ce caH;0.1Thu Aug 16 14:42:54 2007: 00000030: 3b 64 93 10 fe 09 ;d Thu Aug 16 14:42:54 2007: ****Enter processIncomingMessages: response code=11 Thu Aug 16 14:42:54 2007: ****Enter processRadiusResponse: response code=11 Thu Aug 16 14:42:54 2007: 00:40:96:af:3e:93 Access-Challenge received from RADIUS server for mobile 00:40:96:af:3e:93 receiveId = 3 10.77.244.196 Thu Aug 16 14:42:54 2007: AuthorizationResponse: 0x9c27800 Thu Aug 16 14:42:54 2007: structureSize.....104 Thu Aug 16 14:42:54 2007: resultCode.....255 Thu Aug 16 14:42:54 2007: protocolUsed.....0x00000001Thu Aug 16 14:42:54 2007: proxyState AF:3E:93-03:01:00:40:96

(Thu Aug 16 14:42:54 2007: Packet contains 3 AVPs (not shown

Thu Aug 16 14:42:54 2007: AuthenticationRequest: 0xblab104 Thu Aug 16 14:42:54 2007: Callback.....0x85ed228 Thu Aug 16 14:42:54 2007: protocolType.....0x00140001Thu Aug 16 14:42:54 2007: proxyState AF:3E:93-03:02:00:40:96 (Thu Aug 16 14:42:54 2007: Packet contains 16 AVPs (not shown Thu Aug 16 14:42:54 2007: 00:40:96:af:3e:93 ,Successful transmission of Authentication Packet (id 2) to 10.77.244.196:1812 proxy state 00:40:96:af:3e:93-00:00 Thu Aug 16 14:42:54 2007: 00000000: 01 02 00 c0 38 b6 b2 20 ff 5b f2 16 64 df 02 61 d..a..]....8.... Thu Aug 16 14:42:54 2007: 00000010: cf f5 93 4b 01 07 75 73 65 72 31 1f 13 30 30 2d K..User1..00-... Thu Aug 16 14:42:54 2007: 00000020: 34 30 2d 39 36 2d 41 46 2d 33 45 2d 39 33 1e 20 ..40-96-AF-3E-93 Thu Aug 16 14:42:54 2007: 00000030: 30 30 2d 30 42 2d 38 35 2d 35 42 2d 46 42 2d 44 00-0B-85-5B-FB-D 2d 54 53 57 45 42 05 06 Thu Aug 16 14:42:54 2007: 00000040: 30 3a 4f 66 66 69 63 65 ..Office:0 Thu Aug 16 14:42:54 2007: 00000050: 00 00 01 04 06 0a 4d f4 d2 20 05 77 6c 63 1a .M....wlc..... Thu Aug 16 14:42:54 2007: 00000060: 0c 00 00 37 63 01 06 00 00 00 01 06 06 00 00 007c... Thu Aug 16 14:42:54 2007: 00000070: 02 0c 06 00 00 05 14 3d 06 00 00 00 13 40 06 00 ..@....=.... Thu Aug 16 14:42:54 2007: 00000080: 00 00 0d 41 06 00 00 00 06 51 04 32 30 4f 17 01 ..A....Q.200... Thu Aug 16 14:42:54 2007: 00000090: 01 00 15 11 01 00 08 0f 14 05 65 1b 28 61 c9 75 e.(a.u.... Thu Aug 16 14:42:54 2007: 000000a0: 73 65 72 31 18 0a 53 56 43 3d 30 2e 31 3b 50 12 .ser1..SVC=0.1;P Thu Aug 16 14:42:54 2007: 000000b0: 05 ba 6b af fe a4 b0 d1 a2 94 f8 39 80 ca 3c 96 .>..k.....9.. Thu Aug 16 14:42:54 2007: 00000000: 02 02 00 ce c9 3d 5d c8 6c 07 8e fb 58 84 8d f6 ...l...x.[=.... Thu Aug 16 14:42:54 2007: 00000010: 33 6d 93 21 08 06 ff ff ff ff 4f 27 02 01 00 25 %...'3m.!....0 Thu Aug 16 14:42:54 2007: 00000020: 11 01 00 18 e5 e5 31 1e 33 b5 4e 69 90 e7 84 25 %...Ni.1.3..... Thu Aug 16 14:42:54 2007: 00000030: 42 a9 20 ac 84 33 9f 87 ca dc c9 b3 75 73 65 72 B....3....user Thu Aug 16 14:42:54 2007: 00000040: 31 1a 3b 00 00 00 09 01 35 6c 65 61 70 3a 73 65 5leap:se....;.1 Thu Aug 16 14:42:54 2007: 00000050: 73 73 69 6f 6e 2d 6b 65 79 3d 29 80 1d 2c 1c 85 (=ssion-kev Thu Aug 16 14:42:54 2007: 00000060: db 1c 29 7e 40 8a b8 93 69 2a 55 d2 e5 46 89 8b ..i*U..F...@~(.. Thu Aug 16 14:42:54 2007: 00000070: 2c 3b 65 49 3e 44 cf 7e 95 29 47 54 1a 1f 00 00eI>D.~.)GT;, 2d 61 6c 67 6f 2d 74 79 Thu Aug 16 14:42:54 2007: 00000080: 00 09 01 19 61 75 74 68 auth-algo-ty.... Thu Aug 16 14:42:54 2007: 00000090: 70 65 3d 65 61 70 2d 6c 65 61 70 1a 0d 00 00 37 pe=eap-leap....7 Thu Aug 16 14:42:54 2007: 000000a0: 63 06 07 55 73 65 72 31 19 14 43 41 43 53 3a 30 c..User1..CACS:0 Thu Aug 16 14:42:54 2007: 000000b0: 2f 39 2f 61 34 64 66 34 64 32 2f 31 50 12 9a 71 a4df4d2/1P..q/9/ Thu Aug 16 14:42:54 2007: 000000c0: 09 99 7d 74 89 ad af e5 c8 b1 71 94 97 d1 Thu Aug 16 14:42:54 2007: ****Enter processIncomingMessages: response code=2 Thu Aug 16 14:42:54 2007: ****Enter processRadiusResponse: response code=2

> Thu Aug 16 14:42:54 2007: 00:40:96:af:3e:93 Access-Accept received from RADIUS server

for mobile 00:40:96:af:3e:93 receiveId = 3 10.77.244.196

Thu Aug 16 14:42:54 2007: AuthorizationResponse: 0x9c27800 Thu Aug 16 14:42:54 2007: structureSize......236

 Thu Aug 16 14:42:54 2007:
 resultCode.....0

 Thu Aug 16 14:42:54 2007:
 protocolUsed.....0x0

 0000001 :Thu Aug 16 14:42:54 2007: proxyState.....00 AF:3E:93-03:02:40:96 :Thu Aug 16 14:42:54 2007: Packet contains 6 AVPs (Thu Aug 16 14:42:54 2007: AVP[01] Framed-IP-Address......0xffffffff (-1 (bytes 4) (Thu Aug 16 14:42:54 2007: AVP[02] EAP-Message.....DATA (37 bytes (Thu Aug 16 14:42:54 2007: AVP[03] Cisco / LEAP-Session-Key...DATA (16 bytes (Thu Aug 16 14:42:54 2007: AVP[04] Airespace / ACL-Name.....User1 (5 bytes Thu Aug 16 14:42:54 2007: AVP[05] Class.....CACS:0/9/a4df4d2/1 (bvtes 18) (Thu Aug 16 14:42:54 2007: AVP[06] Message-Authenticator.....DATA (16 bytes Thu Aug 16 14:42:54 2007: 00:40:96:af:3e:93 Applying new AAA override for station 00:40:96:af:3e:93 Thu Aug 16 14:42:54 2007: 00:40:96:af:3e:93 Override values for station 00:40:96:af:3e:93 source: 4, valid bits: 0x400 qosLevel: -1, dscp: 0xfffffff, dot1pTag: 0xffffffff, sessionTimeout: -1 dataAvgC: -1, rTAvgC: -1, dataBurstC: -1, rTimeBurstC: -1 ,'' :vlanIfName aclName:User1 Thu Aug 16 14:42:54 2007: 00:40:96:af:3e:93 Inserting new RADIUS override into chain for station 00:40:96:af:3e:93

يمكنك إستخدام مجموعة من الأمر show wlan summary للتعرف على أي من شبكات WLAN تستخدم مصادقة خادم RADIUS. ثم يمكنك عرض الأمر show client summary لترى أي عناوين MAC (العملاء) تتم مصادقتها بنجاح على شبكات WLAN RADIUS. يمكنك أيضا ربط هذا مع Cisco Secure ACS يمر بمحاولات أو محاولات فاشلة سجل.

توصي Cisco باختبار تكوينات قائمة التحكم في الوصول (ACL) باستخدام عميل لاسلكي لضمان تكوينها بشكل صحيح. إذا فشلت في العمل بشكل صحيح، فتحقق من قوائم التحكم في الوصول (ACL) على صفحة ويب قائمة التحكم في الوصول والتحقق من تطبيق تغييرات قائمة التحكم في الوصول (ACL) على واجهة وحدة التحكم.

أنت يستطيع أيضا استعملت هذا عرض أمر in order to دققت تشكيلك:

• show acl summary — لعرض قوائم التحكم في الوصول (ACL) التي تم تكوينها على وحدة التحكم، أستخدم الأمر show acl summary.

فيما يلي مثال:

Cisco Controller) >**show acl summary**) ACL Name Applied _______ User1 Yes User2 Yes

• إظهار قائمة التحكم في الوصول (ACL) التفصيلية <ACL_Name> — يعرض معلومات تفصيلية حول قوائم التحكم في الوصول (ACL) التي تم تكوينها.فيما يلي مثال:**ملاحظة:** تم نقل بعض البنود في الناتج إلى السطر الثاني بسبب قيود المساحة. Cisco Controller) -show acl detailed User1

Destination Source Source Port Dest Port I Dir IP Address/Netmask IP Address/Netmask Prot Range Range DSCP Action _____ _____ _____ _____ _____ _____ 172.16.0.0/255.255.0.0 172.16.1.100/255.255.255.255 1 Τn Any 0-65535 0-65535 Any Permit 172.16.0.0/255.255.0.0 2 172.16.1.100/255.255.255.255 Out Any 0-65535 0-65535 Any Permit Cisco Controller) > show acl detailed User2) Destination Source Source Port Dest Port T Dir IP Address/Netmask IP Address/Netmask Prot Range Range DSCP Action ___ ____ _____ ____ ____ 172.16.0.0/255.255.0.0 172.16.1.50/255.255.255.255 1 In Any 0-65535 0-65535 Any Permit 172.16.1.50/255.255.255.255 172.16.0.0/255.255.0.0 2 Out Any 0-65535 0-65535

• إظهار تفاصيل العميل <MAC Address الخاص بالعميل> - يعرض معلومات تفصيلية حول العميل اللاسلكي.

تلميحات استكشاف المشكلات وإصلاحها

استعملت هذا طرف أن يتحرى:

Any Permit

- تحقق من وحدة التحكم أن خادم RADIUS في حالة نشطة، وليس في وضع الاستعداد أو معطل.
- على وحدة التحكم، تحقق مما إذا تم إختيار خادم RADIUS من القائمة المنسدلة للشبكة المحلية اللاسلكية .(WLAN) (SSID)
 - تحقق من تلقي خادم RADIUS لطلب المصادقة من العميل اللاسلكي والتحقق من صحته.
- تحقق من المصادقة التي تم تمريرها والمحاولات الفاشلة على خادم ACS للقيام بذلك. وهذه التقارير متاحة في إطار التقارير والأنشطة على خادم ACS.

<u>معلومات ذات صلة</u>

- قوائم التحكم في الوصول على وحدات التحكم في الشبكة المحلية اللاسلكية: القواعد والحدود والأمثلة
 - مثال على تكوين ACL على وحدة تحكُّم الشبكة المحلية اللاسلكية
 - <u>مثال على تكوين عوامل تصفية MAC المزوّدة بوحدات التحكّم في شبكة LAN اللاسلكية (WLC)</u>
 - <u>دليل تكوين وحدة تحكم شبكة LAN اللاسلكية من Cisco، الإصدار 5.2</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