RSA SecureID يف مكحتلا تادحو عم زهاج نيوكت لاثمو ةيكلساللا ةيلحملا ةكبشلا Cisco Secure ACS

المحتويات

المقدمة المتطلبات الأساسية المتطلبات المكونات المستخدمة الاصطلاحات معلومات أساسية التكوين تكوين م<u>ضيف الوكيل</u> إستخدام Cisco Secure ACS كخادم RADIUS إستخدام خادم RADIUS لمدير مصادقة RSA 6.1 تكوين وكيل المصادقة تكوين ACS من Cisco تكوين تكوين وحدة تحكم شبكة LAN اللاسلكية من Cisco ل 802.1x تكوين العميل اللاسلكي 802.11 مشكلات معروفة معلومات ذات صلة

<u>المقدمة</u>

يشرح هذا المستند كيفية إعداد وتكوين نقاط الوصول من Cisco التي تعمل ببروتوكول نقطة الوصول في الوضع Lightweight (LWAPP) ووحدات التحكم في الشبكة المحلية (LAN) اللاسلكية (WLCs)، وكذلك خادم التحكم في الوصول الآمن (ACS) من Cisco الذي سيتم إستخدامه في بيئة شبكة محلية لاسلكية (WLAN) مصدق عليها بواسطة RSA SecureID. يمكن العثور على أدلة التنفيذ الخاصة ب RSA SecurID على www.rsasecured.com.

<u>المتطلبات الأساسية</u>

<u>المتطلبات</u>

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

- معرفة التحكم في الشبكة المحلية اللاسلكية (WLCs) وكيفية تكوين معلمات WLC الأساسية.
- معرفة كيفية تكوين ملف تعريف Cisco Wireless Client باستخدام ADU).
 - معرفة وظائف Cisco Secure ACS.
 - معرفة أساسية ب LWAPP.

• لديهم فهم أساسي لخدمات Microsoft Windows Active Directory (AD)، بالإضافة إلى مفاهيم وحدة التحكم بالمجال و DNS.**ملاحظة:** قبل أن تحاول إجراء هذا التكوين، تأكد من أن ACS وخادم إدارة مصادقة RSA موجودين في نفس المجال وأن ساعة النظام الخاصة بهما متزامنة تماما. إذا كنت تستخدم Microsoft موجودين في نفس المجال وأن ساعة النظام الخاصة بهما متزامنة تماما. إذا كنت تستخدم Microsoft المجال موجودين في نفس المجال وأن ساعة النظام الخاصة بهما متزامنة تماما. إذا كنت تستخدم Microsoft أسجال موجودين في نفس المجال وأن ساعة النظام الخاصة بهما متزامنة تماما. إذا كنت تستخدم Microsoft المجال المجال و المعلومات ذات المجال. ارجع إلى <u>تكوين Active Director وقاعدة بيانات مستخدم Windows</u> للحصول على المعلومات ذات الصلة.

<u>المكونات المستخدمة</u>

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

- مدير مصادقة RSA 6.1
- وكيل مصادقة RSA 6.1 لنظام التشغيل Microsoft Windows
- Cisco Secure ACS 4.0(1) Build 27**ملاحظة:** يمكن إستخدام خادم RADIUS المضمن بدلا من مصدر المحتوى الإضافي من Cisco. راجع وثائق RADIUS التي تم تضمينها مع مدير مصادقة RSA حول كيفية تكوين الخادم.
 - نقاط الوصول من Cisco WLCs وخفيف الوزن الإصدار 4.0 (الإصدار 4.0.155.0)

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>

نظام RSA SecureID هو حل مصادقة مستخدم ثنائي العوامل. عند إستخدامه بالاقتران مع مدير مصادقة RSA ووكيل مصادقة RSA، يتطلب مصدق RSA SecureID من المستخدمين تعريف أنفسهم باستخدام آلية مصادقة ثنائية العوامل.

أحدهما هو رمز RSA SecureID، وهو رقم عشوائي يتم إنشاؤه كل 60 ثانية على جهاز مصدق RSA SecureID. والآخر هو رقم التعريف الشخصي (PIN).

تتميز مصادقة RSA SecurID بالسهولة نفسها التي يتم إستخدامها عند إدخال كلمة المرور. يتم تعيين مصدق RSA SecureID لكل مستخدم نهائي يقوم بإنشاء رمز إستخدام مرة واحدة. عند تسجيل الدخول، يقوم المستخدم بإدخال هذا الرقم ببساطة وإدخال رمز PIN سري للمصادقة عليه بنجاح. وكميزة إضافية، عادة ما تكون رموز أجهزة RSA SecureID المميزة مبرمجة بشكل مسبق لتعمل بشكل كامل عند الاستلام.

يشرح عرض الفلاش هذا كيفية إستخدام جهاز مصدق RSA SecureID: <u>عرض RSA</u>.

من خلال برنامج RSA SecureID Ready، تدعم خوادم Cisco WLCs و Cisco Secure ACS مصادقة RSA SecureID بمجرد إخراج الجهاز من عبوته. يعترض برنامج وكيل مصادقة RSA طلبات الوصول، سواء كانت محلية أو عن بعد، من المستخدمين (أو مجموعات المستخدمين) ويوجههم إلى برنامج مدير مصادقة RSA للمصادقة.

يعد برنامج مدير مصادقة RSA هو مكون الإدارة لحل RSA SecureID. ويتم إستخدامه للتحقق من طلبات المصادقة والإدارة المركزية لسياسات المصادقة لشبكات المؤسسات. يعمل بالاقتران مع أجهزة مصادقة RSA SecureID وبرنامج وكيل مصادقة RSA. في هذا المستند، يتم إستخدام خادم Cisco ACS كعميل مصادقة RSA من خلال تثبيت البرنامج الوكيل عليه. WLC هو خادم الوصول إلى الشبكة (NAS) (عميل AAA) الذي يقوم بدوره بإعادة توجيه مصادقة العميل إلى ACS. يوضح المستند المفاهيم والإعداد باستخدام مصادقة عميل بروتوكول المصادقة المتوسع المحمي (PEAP).

لمعرفة المزيد عن مصادقة PEAP، ارجع إلى <u>بروتوكول المصادقة المتوسع المحمي من Cisco</u>.

<u>التكوين</u>

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

يستخدم هذا المستند التكوينات التالية:

- <u>تكوين مضيف الوكيل</u>
- <u>تكوين وكيل المصادقة</u>

<u>تكوين مضيف الوكيل</u>

إستخدام Cisco Secure ACS كخادم RADIUS

من أجل تسهيل الاتصال بين Cisco Secure ACS وتطبيق RSA Authentication Manager / RSA SecureID من أجل تسهيل الاتصال Appliance، يجب إضافة سجل مضيف وكيل إلى قاعدة بيانات مدير مصادقة RSA. يحدد سجل مضيف الوكيل ACS الآمن من Cisco ضمن قاعدة بياناته ويحتوي على معلومات حول الاتصال والتشفير.

لإنشاء سجل مضيف الوكيل، تحتاج إلى هذه المعلومات:

- اسم المضيف لخادم Cisco ACS
- عناوين IP لجميع واجهات الشبكة لخادم ACS من Cisco

أكمل الخطوات التالية:

- 1. افتح تطبيق وضع مضيف مدير مصادقة RSA.
 - 2. حدد **مضيف الوكيل > إضافة مضيف**



تری هذه النافذة:

t Agent Host	
Name: SB ACS	hostname of the ACS Server
Network address: 192.168.30.18	
Site:	Select
Agent type: Communication Set Single-Transaction	rver A
Net OS Agent	
Encryption Type: 🔿 SDI 💿 DES	
I Node Secret Create	ed
🔽 Open to All Locally	Known Users
F Search Other Real	ms for Unknown Users
🗖 Requires Name Lo	ck
☑ Enable Offline Auth	entication
E Enable Windows B	accuord lategration
	assword incyration
Create Verifiable A	uthentications
Group Activations	Uscr Activations
Secondary Nodes	Delete Agent Host
Edit Agent Host Extension Data	Configure RADIUS Connection
Assign Acting Servers	Create Node Secret File

3. أدخل المعلومات المناسبة لاسم خادم Cisco ACS وعنوان الشبكة. أختر **NetOS** لنوع العامل وحدد خانة الاختيار **فتح لجميع المستخدمين المعروفين محليا**. 4. وانقر فوق OK.

<u>إستخدام خادم RADIUS لمدير مصادقة RSA 6.1</u>

من أجل تسهيل الاتصال بين Cisco WLC ومدير مصادقة RSA، يجب إضافة سجل مضيف وكيل إلى قاعدة بيانات مدير مصادقة RSA وقاعدة بيانات خادم RADIUS. يحدد سجل مضيف الوكيل عنصر التحكم في الشبكة المحلية اللاسلكية (WLC) من Cisco داخل قاعدة البيانات الخاصة به ويحتوي على معلومات حول الاتصال والتشفير.

لإنشاء سجل مضيف الوكيل، تحتاج إلى هذه المعلومات:

- اسم مضيف WLC
- إدارة عنوان من ال WLC
- سر RADIUS، والذي يجب أن يطابق سر RADIUS على Cisco WLC

عند إضافة سجل مضيف الوكيل، يتم تكوين دور WLC كخادم إتصالات. يتم إستخدام هذا الإعداد من قبل إدارة مصادقة RSA لتحديد كيفية حدوث الاتصال مع عنصر التحكم في الشبكة المحلية اللاسلكية (WLC).

ملاحظة: يجب حل أسماء المضيف داخل إدارة مصادقة RSA / جهاز أمان RSA إلى عناوين IP صالحة على الشبكة

المحلية.

أكمل الخطوات التالية:

- 1. افتح تطبيق وضع مضيف مدير مصادقة RSA.
 - 2. حدد **مضيف الوكيل > إضافة مضيف**

T	a auth	ontical	tion Ma	Dager	5.1.0 dminist	ration	tmo-	63			.ر
2	System	User	Token	Group	Agent Host	Realm	Site	RADIUS	Log	Report	Help
į		-	-	C	Add Agen	t Host		-	5	_	
					Edit Agen	t Host		Ч			
					Copy Age	nt Host.					
					List Agent	Hosts			100		
					Delete Ag	ent Hos	s				
					Server As	signmen	t				
					Generate	Configu	ration	Files			
	Add Age	nt Host								×	
	(Na	ame: 192	.168.10.1	02	Point	to WLC	when			
			192	160 10 1	02	using	RSA's F	ADIUS			
	Netw	ork addr	299: 192	.100.10.1	02		361461	·			
			Site:						Select		
		Agent t	ype: UN	IX Agent				*			
			Sin	gle-Trans	on Server action Comm S	erver		-			
	Encr	untion T	var C S	DI @ DE	s			_			
	Linci	ypuon i	ype.		(here and a set						
			T NO	de secret	Created						
		(I Op	cn to All L	ocally Known U	Isers:					
			□ Sea	arch Other	r Realms for Ur	iknown U	BCIS				
			E Rec	quires Na	me Lock						
			F Ena	able Offlin	e Authenticatio	n					
			🖻 Ena	able Wind	lows Password	Integratio	on				
			□ Cre	ate Verifi	able Authentica	tions					
		Grou	p Activati	ions		User Ac	tivatio	NS	Ĩ.		
		Seco	ndary No	des		Delete	Agenti	fost			
	Edit	t Agent H	lost Exte	nsion Dat	a Conti	gure RAD	IUS Co	nnection			
		Assign	Acting Se	envers	Cr	cate Nod	e Secr	et File	1		

- 3. أدخل المعلومات المناسبة لاسم مضيف WLC (a FQDN قابل للحل، إذا لزم الأمر) وعنوان الشبكة. أختر لنوع الوكيل وحدد خانة الاختيار **فتح لجميع المستخدمين المعروفين محليا**.
 - 4. وانقر فوق OK.
 - 5. من القائمة، حدد **RADIUS > إدارة خادم** RADIUS.

ሕ R	💑 RSA Authentication Manager 6.1 Administration ps037.pe.rsa.net														
Eile	∑ys	tem	User	Ιo	ken	Grou	р	Ageni	t Host	<u>R</u> ealm	Sįte	RADIUS	Log	Report	Help
												Add P	rofile		
												Edit Pr	ofile		
												List Pr	ofiles.		
												Delete	Profil	es	
												Manar		TI IS Serv	or
1													JO KAL	103 3614	

يفتح نافذة إدارة جديد.

6. في هذا الإطار، حدد **عملاء RADIUS**، ثم انقر فوق

				إضافة.
👆 RSA RADIUS Powered by Stee	l-Belted Radio	ıs (P5037)		
<u>File Panel Web H</u> elp				
GRefresh OPrint OAdd	ait 🚯 Cyt	C 2099 C	Paste, 🛞 Delet	ĉ
RSA RADIUS Server Administration	Name 🛆	IP Address	Make.Model	
RADIUS Clients	CISCO2500	192.168.40.1.	Standard R	*
Profiles	PH016.PE.RS.	. 10.100.51.16	- Standard R	
Replication	PH017.PE.RS.	. 10.100.51.17	- Standard R	
- Statistics	PH018.PE.RS.	. 10.100.51.18	- Standard R	
	PH031.SECU.	10.100.51.31	 Standard R 	12
	PH034.SECU.	10.100.51.34	- Standard R	1.
	PH071.PE.RS.	. 10.100.51.71	- Standard R	_

7. دخلت المعلومة مناسب ل ال cisco WLC. يجب أن يطابق السر المشترك السر المشترك المعرف على Cisco WI C

E

dd RADIUS Client			X
Nome:	ascoaronet	Any RADIUS Client	0
Description:			
P Address:	10.100.10.11		
Shared secret:	12345678	🔽 Unmask	
Make/model:	- Standard Radius -	<u>VV</u> eb Info	
Advanced			
Use different	shared secret for Accounting		
Assume dow	n if no keepalive packets after	seconds	
	<u>O</u> K <u>C</u> ance		

8. وانقر فوق **OK**.

<u>تكوين وكيل المصادقة</u>

يمثل هذا الجدول وظيفة وكيل مصادقة RSA ل ACS:

Partner Integration Overview	
Authentication Methods Supported	Native RSA SecurID Authentication, RADIUS, Both
List Library Version Used	5.0.3
RSA Authentication Manager Name Locking	Yes
RSA Authentication Manager Replica Support	Full Replica Support
Secondary RADIUS Server Support	N/A
Location of Node Secret on Agent	'None stored'
RSA Authentication Agent Host Type	Communication Server
RSA SecurID User Specification	Designated Users, All Users, Default Method
RSA SecurID Protection of Administrative Users	No
RSA Software Token API Integration	No
Use of Cached Domain Credentials	No

ملاحظة: راجع وثائق RADIUS التي تم تضمينها مع مدير مصادقة RSA حول كيفية تكوين خادم RADIUS، إذا كان ذلك خادم RADIUS الذي سيتم إستخدامه.

<u>تكوين ACS من Cisco</u>

<u>تنشيط مصادقة RSA SecureID</u>

يدعم مصدر المحتوى الإضافي الآمن من Cisco مصادقة RSA SecureID للمستخدمين. أتمت هذا steps in order to شكلت cisco يؤمن ACS أن يصدق مستعمل مع صحة هوية مدير 6.1:

- 1. قم بتثبيت وكيل مصادقة RSA 5.6 أو إصدار أحدث ل Windows على نفس النظام الخاص بخادم ACS الآمن من Cisco.
 - 2. تحقق من الاتصال من خلال تشغيل وظيفة إختبار المصادقة الخاصة بوكيل المصادقة.
 - RSA **c:\Program Files\RSA Security\RSA Authentication** من خادم acecInt.dll من خادم. ACS**:\WINNT\System32** إلى **دليل** خادم Manager\prog Directory
- 4. في شريط التنقل، انقر فوق **قاعدة بيانات المستخدم الخارجي**. ثم انقر فوق **تكوين قاعدة البيانات** في صفحة قاعدة البيانات الخارجية.



5. في صفحة "تكوين قاعدة بيانات المستخدم الخارجي"، انقر فوق **خادم الرمز المميز RSA** SecurID.



Die Foit Jiew Lähoutes Toole Dalo	2
🔾 Back + 🔿 - 💌 😰 🐔 🔎 Search 🧄 Favorites 🔮 Media 🐵 ⊘ + 🌭 😥 + 🥪	
Address 🔄 http://127.0.0.1:3342/	💌 🎒 Go Links **
Google - 💽 😵 Search Web - 🤯 🖓 Oblocked 🗐 Arto ST 🔤 Opl	ins 🌶
Cises Stratus External User Databases	x
the the	
Edit	Halp
The Little Control of	
Clifteenb	Network Admission Control
Database Configuration Creation	<u>Windows Database</u>
	Novell NDS Construction
Components (Tick here to create a new configuration for the RS& Security)	<u>Generic LDAP</u> <u>External ODBC Database</u>
Token Server database	LEAP Prevy RADIUS Server
Real Configuration	Token Card Server Support
Zin Suten	RADIUS Token Server
Create New Configuration	RSA SecurIDToken Server
Configuration	8
Gontrel	Network Admission Control
Cancel	
Did Dutnaarer	Click to configure Network Admission Control (NAC)
Reports and	databases, external policies, local policies, and rules.
P Back to Help	Cisco Secure ACS uses NAC databases to process
Decumentation	posture validation requests.
	[Back to Top]
	Windows Database
	Click to configure Windows SAM and Artive Directory
	databases with which Cisco Secure ACS can
	authenticate users.

7. أدخل اسما، ثم انقر فوق

. .



8. طقطقة

Elle Edit View Favorites Iools Help		2
😋 Back: + 🔘 - 📧 🧝 🐔 🔎 Search 🔅 Pavortes 😽 Nedia 🕘 🔅 + 🌭 🐼 + 🔛 -		
Agdress 🔯 https://127.0.0.1:3342/	💌 🍝 😡	Links 30
Google - 💽 🍘 Search Web - 🚳 🗗 O blocked 🗐 A.coli 🔛 Op	tions 🥒	
tore Surrent External User Databases		×
Edit Edit Edit	Network Admission Centrol Windows Database Novell NDS Generic LDAP External ODBC Database LEAP froxy RADIUS Server Token Card Server Support RADIUS Token Server RADIUS Token Server Network Admission Centrol Click to configure Network Admission Control (NAC) databases, external policies, local policies, and rules. Cisco Secure ACS uses NAC databases to process posture validation requests. [Back to Top] Windows Database Click to configure Windows SAM and Active Directory databases with which Cisco Secure ACS can authenticate users	

يعرض Cisco Secure ACS اسم خادم الرمز المميز ومسار مكتبة الارتباط الديناميكي (DLL) المصدق. تؤكد هذه المعلومات أنه يمكن ل Cisco Secure ACS الاتصال بوكيل مصادقة RSA. يمكنك إضافة قاعدة بيانات المستخدم الخارجي RSA SecureID إلى نهج المستخدم غير المعروف أو تعيين حسابات مستخدمين معينة لاستخدام قاعدة البيانات هذه



إضافة/تكوين مصادقة RSA SecureID إلى نهج المستخدم غير المعروف

أكمل الخطوات التالية:

1. في شريط تنقل ACS، انقر على **قاعدة بيانات المستخدم الخارجي > سياسة مستخدم غير**



2. في صفحة **نهج المستخدم غير المعروف**، حدد **التحقق من قواعد بيانات المستخدم الخارجية التالية**، وقم بتمييز ونقلها إلى مربع قواعد البيانات المحدد. بعد ذلك، انقر فوق RSA SecurID Token Server

u 0 f	2 및 3 및 1 · · · · · · · · · · · · · · · · · ·	ارسال. * ^م • ۱۹۹۰ ا
Cinco Statema	External User Databases	×
LeffBhoardDhair	Edit	Help
Bill Strup	Configure Unknown User Policy	 <u>Unknown User Policy</u> <u>Eail the Attempt</u> <u>Check the following external users databases</u>
Berrysharten Berrysharten	Del rise attempt Check the following external user databases	Unknown User Policy Use this window to define how to handle usernames not found in the Circo Secure ACS database. Fail the attempt If you do not want Cisco Secure ACS to try authenticating users who do not exist in its internal database (unknown users), select this option [Bark to Top]
	Concel	Check the following external user databases If you want Cisco Secure ACS to use specific external user databases to authenticate takaoawa users, select this option. You can choose the databases and the order is which Cisco Secure ACS uses them to try to authenticate unknown users. For each database that Cisco Secure ACS should use to try to authenticate unknown users, select the database name in the Enternal Databases last and clock the right arrow button to move it to the Selected Databases list determines the sequence of databases that Cisco Secure

إضافة/تكوين مصادقة RSA SecureID لحسابات مستخدمين محددة

أكمل الخطوات التالية:

1. انقر على **إعداد المستخدم** من واجهة المستخدم الرسومية الرئيسية لمسؤول ACS. أدخل اسم المستخدم وانقر فوق **إضافة** (أو حدد مستخدما موجودا ترغب في تعديله).

2. تحت إعداد المستخدم > مصادقة كلمة المرور، أختر RSA SecureID Token Server. بعد ذلك، انقر فوق

rstews L	Jser Setup
Illiu.	dit
vp	User: sbrsa
d Profile ments	Account Disabled
rk juration	Supplementary User Info 🤶
n unation Goe guration	Real Name Description
I User Sk	User Setup
k Accera	RSA SecurID Token Server CiscoSecure PAP (Also used for CHAP/MS- CHAP/ARAP, if the Separate field is not checked.)
s and s	Password Confirm Password
	Separate (CHAP/MS-CHAP/ARAP) Password
	Confirm Password
	When a token server is used for authentication,

إضافة عميل RADIUS في ACS من <u>Cisco</u>

ستحتاج عملية تثبيت خادم Cisco ACS إلى عناوين IP الخاصة بوحدة التحكم في الشبكة المحلية اللاسلكية (WLC) للعمل كوحدة تخزين متصلة بالشبكة (NAS) لإعادة توجيه مصادقة PEAP الخاصة بالعميل إلى ACS.

أكمل الخطوات التالية:

1. تحت **تكوين الشبكة**، أضف/حرر عميل AAA ل WLC الذي سيتم إستخدامه. أدخل المفتاح "سري مشترك" (مشترك مع WLC) الذي يتم إستخدامه بين عميل AAA و ACS. حدد **المصادقة باستخدام > RADIUS** هذا. ثم انقر فوق **إرسال +**

CIECO STATEMA	Network Configuration
with the filter.	Edit
User Setup	
Breup Setup	AAA Client Setup For
Shared Profile Components	WLC4404
Nat work Configuration	AAA Client IP 192.168.10.102
System Configuration	Address
Configuration	Key RSA
Administration Centrol	Authenticate RADIVS (Cisco Airespace)
Detabases	Single Connect TACACS+ AAA Client (Record stop in
nome Posture Nome Validation	accounting on failure).
Network Access Profiles	Log RADIUS Tunneling Packets from this AAA Client
Reports and Activity	Replace RADIUS Port info with Usemame from this AAA Client
Documentation	
	Submit Submit + Apply Delete Delete + Apply Cancel

تطبيق.

- 2. قدم طلبا لشهادة خادم من مرجع مصدق موثوق به معروف مثل مرجع شهادة RSA Keon وقم بتثبيتها.للحصول على مزيد من المعلومات حول هذه العملية، ارجع إلى الوثائق التي يتم شحنها مع Cisco ACS. إذا كنت تستخدم مدير شهادات RSA، فيمكنك عرض دليل تنفيذ RSA Keon Aironet للحصول على تعليمات إضافية. يجب إكمال هذه المهمة بنجاح قبل المتابعة.**ملاحظة:** يمكن أيضا إستخدام الشهادات الموقعة ذاتيا. ارجع إلى وثائق ACS الآمنة من Cisco حول كيفية إستخدام هذه الملوات.
 - 3. تحت **تشكيل النظام > إعداد المصادقة العامة**، حدد خانة الاختيار **للسماح** بمصادقة PEAP.

+ - → - 🕥 🗊	0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0	ndev2.htm 💽 💽 – 🖉 🗙
Cines Systems	System Configuration	×
Lattine, all the s	Edit	fielp 📫
User Setup	Global Authentication Setup	• FEAP • EAP-TLS • EAP-MD5
Shared Profile Compensats	EAP Configuration	<u>MS-CHAP Configuration</u>
Astronomical Astronomical Certification	PEAP PEAP PEAP client initial display message: PEAP season theore [minutes]]	This page specifies settings for EAP and MS-CHAP authentication requests. [Back to Top]
Administration Central User Devices Activity Online Documentation	(minutes): EAP-ILS C Certificate name comparison C Certificate binary comparison © Ether comparison type EAP-MD5 P Allow EAP-MD5 MS-CHAP Configuration P Allow MS-CHAP Version 1 Authentication P Allow MS-CHAP Version 2 Authentication P Allow MS-CHAP Version 2 Authentication	 FEAP PEAP is a certificate-based authentication protocol. PEAP authentication can occur only after you have completed the required steps on the ACS Certificate Setup page. To enable PEAP authentication, relect the Allow PEAP check box To specify a message that users authenticated with PEAP receive, type the message in the TEAP client initial display message" box The PEAP session timeout (min) box defines maximum PEAP session length, in minutes. PEAP supports a session returne feature. The session returne feature allows users to reauthenticate without entering a password provided that the session has not timed out. If Claco Secure ACS or the end-user client is restarted, the user must enter a password even if the session timeout interval has not ended.
	Submit Submit + Restart Gancel	[Back to Top]

<u>تكوين تكوين وحدة تحكم شبكة LAN اللاسلكية من Cisco ل 802.1x</u>

أكمل الخطوات التالية:

- 1. قم بالاتصال بواجهة سطر الأوامر الخاصة بوحدة التحكم في الشبكة المحلية اللاسلكية (WLC) لتكوين وحدة التحكم حتى يمكن تكوينها للاتصال بخادم ACS الآمن من Cisco.
- 2. أدخل الأمر **config radius auth ip-address** من عنصر التحكم في الشبكة المحلية اللاسلكية (WLC) لتكوين خادم RADIUS للمصادقة.**ملاحظة:** عند الاختبار باستخدام خادم RADIUS لمدير مصادقة RSA، أدخل عنوان IP الخاص بخادم RADIUS لمدير مصادقة RSA. عندما تختبر مع خادم Cisco ACS، أدخل عنوان IP الخاص بخادم ACS الآمن من Cisco.
- 3. أدخل الأمر **config radius auth port** من عنصر التحكم في الشبكة المحلية اللاسلكية (WLC) لتحديد منفذ UDP للمصادقة. تكون المنافذ 1645 أو 1812 نشطة بشكل افتراضي في كل من مدير مصادقة RSA وخادم ACS من Cisco.
- 4. أدخل الأمر **config radius auth secret** من عنصر التحكم في الشبكة المحلية اللاسلكية (WLC) لتكوين السر المشترك على عنصر التحكم في الشبكة المحلية اللاسلكية (WLC). يجب أن يتطابق هذا مع السر المشترك الذي تم إنشاؤه في خوادم RADIUS لعميل RADIUS هذا.
 - 5. أدخل الأمر config radius auth enable من عنصر التحكم في الشبكة المحلية اللاسلكية (WLC) لتمكين المصادقة. أدخل الأمر config radius auth disable لتعطيل المصادقة عندما ترغب. لاحظ أن المصادقة معطلة بشكل افتراضي.
 - 6. حدد خيار تأمين الطبقة 2 المناسب لشبكة WLAN المطلوبة في عنصر التحكم في الشبكة المحلية اللاسلكية (WLC).
- 7. أستخدم أوامر show radius auth statistics وshow radius summary للتحقق من تكوين إعدادات RADIUS بشكل صحيح.**ملاحظة:** وحدات التوقيت الافتراضية لمهلة طلب EAP منخفضة وقد تحتاج إلى التعديل. ويمكن القيام بذلك باستخدام الأمر config advanced eap request-timeout *<*seconds>. وقد يساعد أيضا

على تعديل مهلة طلب الهوية بناء على المتطلبات. ويمكن القيام بذلك باستخدام الأمر config advanced eap identity-request-timeout *<seconds*.

<u>تكوين العميل اللاسلكي 802.11</u>

للحصول على شرح تفصيلي حول كيفية تكوين أجهزتك اللاسلكية ومطالب العميل، راجع وثائق Cisco المختلفة.

<u>مشكلات معروفة</u>

هذه بعض المشاكل المعروفة جيدا مع مصادقة RSA SecureID:

- رمز برنامج RSA المميز. لا يتم دعم وضع رقم التعريف الشخصي (PIN) الجديد وأوضاع رمز الرمز المميز التالي عند إستخدام هذا النموذج من المصادقة مع XP2. (ثابت كنتيجة ل -ACS-4.0.1-RSA-SW-CSCsc12614 (CSCsd41866.zip)
 - إذا كان تنفيذ ACS الخاص بك أقدم أو لم يكن لديك التصحيح المذكور أعلاه، فلن يتمكن العميل من المصادقة حتى انتقال المستخدم من "ممكن؛ وضع PIN الجديد" إلى "ممكن". يمكنك تحقيق ذلك من خلال جعل المستخدم يكمل مصادقة غير لاسلكية، أو باستخدام تطبيق "إختبار المصادقة" RSA.
 - رفض 4 أرقام / أرقام PIN أبجدية رقمية. إذا كان المستخدم في وضع رقم التعريف الشخصي (PIN) الجديد يتعارض مع نهج رقم التعريف الشخصي (PIN)، فإن عملية المصادقة تفشل، ولا يعلم المستخدم كيف أو لماذا. في العادة، إذا قام المستخدم بمخالفة النهج، فسيتم إرسال رسالة رفض رقم التعريف الشخصي (PIN) وتتم مطالبته مرة أخرى أثناء إظهار نهج رقم التعريف الشخصي (على سبيل المثال، إذا كان نهج رقم التعريف الشخصي (PIN) يتكون من 5 إلى 7 أرقام، يدخل المستخدم 4 أرقام).

معلومات ذات صلة

- تعيين شبكة VLAN الديناميكية مع WLCs استنادا إلى ACS إلى مثال تكوين تعيين مجموعة ACS ا
 - <u>شبكة VPN للعميل عبر شبكة LAN اللاسلكية مع مثال تكوين WLC</u>
 - <u>المصادقة على أمثلة تكوين وحدات تحكم الشبكة المحلية (LAN) اللاسلكية</u>
 - <u>مصادقة EAP-FAST مع وحدات تحكم الشبكة المحلية اللاسلكية ومثال تكوين خادم RADIUS الخارجي</u>
 - أنواع المصادقة اللاسلكية على ISR الثابت من خلال مثال تكوين SDM
 - أنواع المصادقة اللاسلكية على مثال تكوين ISR الثابت
 - بروتوكول المصادقة المتوسع المحمي من <u>Cisco</u>
 - <u>مصادقة EAP مع خادم RADIUS</u>
 - <u>الدعم التقني والمستندات Cisco Systems</u>

ةمجرتاا مذه لوح

تمجرت Cisco تايان تايانق تال نم قعومجم مادختساب دنتسمل اذه Cisco تمجرت ملاعل العامي عيمج يف نيم دختسمل لمعد يوتحم ميدقت لقيرشبل و امك ققيقد نوكت نل قيل قمجرت لضفاً نأ قظعالم يجرُي .قصاخل امهتغلب Cisco ياخت .فرتحم مجرتم اممدقي يتل القيفارت عال قمجرت اعم ل احل اوه يل إ أم اد عوجرل اب يصوُتو تامجرت الاذة ققد نع اهتي لوئسم Systems الما يا إ أم الا عنه يل الان الانتيام الال الانتيال الانت الما