إضافة دليل شهادة موقعة ذاتيا إلى وحدة التحكم بواسطة نقاط الوصول المحولة LWAPP

المحتويات

المقدمة

يشرح هذا المستند الطرق التي يمكنك إستخدامها لإضافة الشهادات الموقعة ذاتيا (SSCs) يدويا إلى وحدة التحكم في شبكة LAN اللاسلكية (WLC) من Cisco.

يجب أن يكون SSC لنقطة الوصول (AP) موجودا على جميع قوائم التحكم في الشبكة المحلية اللاسلكية (WLC) في الشبكة التي يتوفر لنقطة الوصول على إذن التسجيل لها. كقاعدة عامة، قم بتطبيق بروتوكول SSC على جميع قوائم التحكم في الشبكة المحلية اللاسلكية (WLCs) في مجموعة التنقل نفسها. عندما لا تحدث إضافة SSC إلى عنصر التحكم في الشبكة المحلية اللاسلكية (WLC) من خلال الأداة المساعدة للترقية، يجب عليك إضافة عنصر التحكم في الشبكة المحلية اللاسلكية (SSC) يدويا إلى عنصر التحكم في الشبكة المحلية اللاسلكية (WLC) باستخدام الإجراء الوارد في هذا المستند. تحتاج أيضا إلى هذا الإجراء عندما يتم نقل نقطة وصول إلى شبكة أخرى أو عندما تتم إضافة قوائم التحكم في الشبكة المحلية اللاسلكية (WLC) إضافية إلى الشبكة الموجودة.

يمكنك التعرف على هذه المشكلة عندما لا تقترن نقطة وصول محولة من بروتوكول AP خفيف الوزن (LWAPP) ب WLC. عندما تقوم باستكشاف مشكلة الاقتران وإصلاحها، سترى المخرجات التالية عند إصدار تصحيح الأخطاء التالية:

- عندما يصدر أنت **debug pm pki enable** الـ أمر، أنت ترى:

```
Cisco Controller) >debug pm pki enable)
Thu Jan 26 20:22:50 2006: sshpmGetIssuerHandles: locking ca cert table
Thu Jan 26 20:22:50 2006: sshpmGetIssuerHandles: calling x509_alloc() for user cert
()Thu Jan 26 20:22:50 2006: sshpmGetIssuerHandles: calling x509_decode
=Thu Jan 26 20:22:50 2006: sshpmGetIssuerHandles: <subject> L=San Jose, ST
California, C=US, O=Cisco Systems, MAILTO=support@cisco.com, CN=C1130-00146a1b3744
```

```
=Thu Jan 26 20:22:50 2006: sshpmGetIssuerHandles: <issuer>  L=San Jose, ST
California, C=US, O=Cisco Systems, MAILTO=support@cisco.com, CN=C1130-00146a1b3744
Thu Jan 26 20:22:50 2006: sshpmGetIssuerHandles: Mac Address in subject is
                                                              XX:XX:XX:XX:00
.Thu Jan 26 20:22:50 2006: sshpmGetIssuerHandles: Cert is issued by Cisco Systems
;Thu Jan 26 20:22:50 2006: sshpmGetIssuerHandles: SSC is not allowed by config
                                                                  ...bailing
(Thu Jan 26 20:22:50 2006: sshpmFreePublicKeyHandle: called with (nil
.Thu Jan 26 20:22:50 2006: sshpmFreePublicKeyHandle: NULL argument
```

- عندما تقوم بإصدار الأمر **debug lwapp events enable**، ترى:

```
Cisco Controller) >debug lwapp errors enable)
....
Thu Jan 26 20:23:27 2006: Received LWAPP DISCOVERY REQUEST from AP
'00:13:5f:f8:c3:70 to ff:ff:ff:ff:ff:ff on port '1
Thu Jan 26 20:23:27 2006: Successful transmission of LWAPP Discovery-Response to
AP 00:13:5f:f8:c3:70 on Port 1
Thu Jan 26 20:23:27 2006: Received LWAPP JOIN REQUEST from AP 00:13:5f:f9:dc:b0 to
'06:0a:10:10:00:00 on port '1
Thu Jan 26 20:23:27 2006: sshpmGetIssuerHandles: locking ca cert table
Thu Jan 26 20:23:27 2006: sshpmGetIssuerHandles: calling x509_alloc() for user cert
()Thu Jan 26 20:23:27 2006: sshpmGetIssuerHandles: calling x509_decode
=Thu Jan 26 20:23:27 2006: sshpmGetIssuerHandles: <subject> L=San Jose, ST
California, C=US, O=Cisco Systems, MAILTO=support@cisco.com, CN=C1130-00146a1b321a
=Thu Jan 26 20:23:27 2006: sshpmGetIssuerHandles: <issuer>  L=San Jose, ST
California, C=US, O=Cisco Systems, MAILTO=support@cisco.com, CN=C1130-00146a1b321a
Thu Jan 26 20:23:27 2006: sshpmGetIssuerHandles: Mac Address in subject is
                                                              00:14:6a:1b:32:1a

.Thu Jan 26 20:23:27 2006: sshpmGetIssuerHandles: Cert is issued by Cisco Systems
;Thu Jan 26 20:23:27 2006: sshpmGetIssuerHandles: SSC is not allowed by config
                                                                  ...bailing
Thu Jan 26 20:23:27 2006: LWAPP Join-Request does not include valid certificate
                                .in CERTIFICATE_PAYLOAD from AP 00:13:5f:f9:dc:b0
(Thu Jan 26 20:23:27 2006: sshpmFreePublicKeyHandle: called with (nil
.Thu Jan 26 20:23:27 2006: sshpmFreePublicKeyHandle: NULL argument
Thu Jan 26 20:23:27 2006: Unable to free public key for AP  00:13:5F:F9:DC:B0
Thu Jan 26 20:23:27 2006: spamDeleteLCB: stats timer not initialized for AP
                                                              00:13:5f:f9:dc:b0
Thu Jan 26 20:23:27 2006: spamProcessJoinRequest : spamDecodeJoinReq failed
```

المتطلبات الأساسية

المتطلبات

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

- لا يحتوي عنصر التحكم في الشبكة المحلية اللاسلكية (WLC) على عنصر التحكم في الشبكة المحلية اللاسلكية (SSC) الذي قامت الأداة المساعدة للترقية بتكوينه.
- تحتوي نقاط الوصول على SSC.
- تم تمكين Telnet على عنصر التحكم في الشبكة المحلية اللاسلكية (WLC) ونقاط الوصول (AP).
- يوجد الإصدار الأدنى من رمز برنامج Cisco IOS® Software السابق ل LWAPP في نقطة الوصول المراد ترقيته.

المكونات المستخدمة

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

- Cisco 2006 WLC الذي يشغل البرنامج الثابت 3.2.116.21 مع عدم تثبيت SSC
- نقطة الوصول من السلسلة Cisco Aironet 1230 Series مع SSC

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

الاصطلاحات

راجع اصطلاحات تلميحات Cisco التقنية للحصول على مزيد من المعلومات حول اصطلاحات المستندات.

معلومات أساسية

في بنية الشبكة المحلية اللاسلكية (WLAN) المركزية من Cisco، تعمل نقاط الوصول (AP) في وضع الوزن الخفيف. ترتبط نقاط الوصول (APs) ب Cisco WLC باستخدام LWAPP. LWAPP هو مشروع بروتوكول لفرقة عمل هندسة الإنترنت (IETF) يحدد رسائل التحكم للإعداد ومصادقة المسار وعمليات وقت التشغيل. كما يحدد LWAPP آلية الاتصال النفقي لحركة مرور البيانات.

تكتشف نقطة الوصول في الوضع Lightweight (LAP) عنصر تحكم في الشبكة المحلية اللاسلكية (WLC) باستخدام آليات اكتشاف LWAPP. يرسل ال{lap{upper بعد ذلك ال WLC و LWAPP ربط طلب. يرسل عنصر التحكم في الشبكة المحلية اللاسلكية (WLC) إستجابة الانضمام إلى LWAPP التي تسمح لنقطة الوصول (LAP) بالانضمام إلى عنصر التحكم في الشبكة المحلية اللاسلكية (WLC). عندما يتم ضم نقاط الوصول إلى عنصر التحكم في الشبكة المحلية اللاسلكية (WLC)، تقوم نقطة الوصول في الوضع Lightweight بتنزيل برنامج WLC إذا كانت المراجعات على نقطة الوصول Lightweight (LAP) ووحدة التحكم في الشبكة المحلية اللاسلكية (WLC) غير متطابقة. وفيما بعد، أصبحت نقطة الوصول في الوضع Lightweight تحت سيطرة لجنة التحكم في الشبكة المحلية اللاسلكية.

يؤمن LWAPP اتصال التحكم بين AP و WLC من خلال توزيع مفتاح آمن. يتطلب توزيع المفتاح الآمن شهادات رقمية X.509 مزودة مسبقا على كل من نقطة الوصول في الوضع Lightweight (LAP) ووحدة التحكم في الشبكة المحلية اللاسلكية (WLC). وتتم الإشارة إلى الشهادات التي يتم تثبيتها في المصنع مع مصطلح "MIC"، وهو إختصار لتصنيع الشهادة المثبتة. لا تحتوي نقاط الوصول Aironet APs التي تم شحنها قبل 18 يوليو 2005 على ميكروفونات. لذلك تنشئ نقاط الوصول هذه SSC عندما يتم تحويلها للعمل في وضع Lightweight. تتم برمجة وحدات التحكم لقبول وحدات SSC لمصادقة نقاط الوصول المحددة.

هذه هي عملية الترقية:

1. يقوم المستخدم بتشغيل أداة مساعدة للترقية تقبل ملف إدخال بقائمة نقاط الوصول وعناوين IP الخاصة بها، بالإضافة إلى بيانات اعتماد تسجيل الدخول الخاصة بهم.
2. تنشئ الأداة المساعدة جلسات عمل Telnet مع نقاط الوصول وترسل سلسلة من أوامر برنامج Cisco IOS في ملف الإدخال لإعداد نقطة الوصول للترقية. تتضمن هذه الأوامر الأوامر الخاصة بإنشاء SSCs. أيضا، تحدد الأداة المساعدة جلسة عمل Telnet مع عنصر التحكم في الشبكة المحلية اللاسلكية (WLC) من أجل برمجة الجهاز للسماح بالتفويض الخاص بنقاط الوصول (APs) الخاصة ببروتوكول SSC.
3. ثم تقوم الأداة المساعدة بتحميل الإصدار JX(7)12.3 من برنامج Cisco IOS Software على نقطة الوصول حتى يمكن أن تنضم نقطة الوصول إلى عنصر التحكم في الشبكة المحلية اللاسلكية (WLC).
4. بعد انضمام نقطة الوصول إلى عنصر التحكم في الشبكة المحلية اللاسلكية (WLC)، تقوم نقطة الوصول بتنزيل إصدار برنامج Cisco IOS Software كامل من عنصر التحكم في الشبكة المحلية اللاسلكية (WLC). تقوم الأداة المساعدة للترقية بإنشاء ملف إخراج يتضمن قائمة نقاط الوصول (APs) وقيم تجزئة مفاتيح SSC المطابقة التي يمكن إستيرادها إلى برنامج إدارة نظام التحكم اللاسلكي (WCS).
5. يمكن أن يرسل ال WCS بعد ذلك هذا معلومة إلى WLCs آخر على الشبكة.

بعد أن تنضم نقطة الوصول إلى عنصر التحكم في الشبكة المحلية اللاسلكية (WLC)، يمكنك إعادة تعيين نقطة الوصول إلى أي عنصر تحكم في الشبكة المحلية اللاسلكية (WLC) على الشبكة، إذا لزم الأمر.

تحديد موقع تجزئة المفتاح SHA1

إذا كان الكمبيوتر الذي أجرى تحويل نقطة الوصول متاحا، فيمكنك الحصول على تجزئة المفتاح 1 (SHA1) لخوارزمية التجزئة الآمنة من ملف csv الموجود في دليل أداة ترقية Cisco. إذا كان ملف csv غير متاح، فيمكنك إصدار أمر **debug** على عنصر التحكم في الشبكة المحلية اللاسلكية (WLC) لاسترداد تجزئة المفتاح SHA1.

أكمل الخطوات التالية:

1. قم بتشغيل نقطة الوصول واتصلها بالشبكة.
2. قم بتمكين تصحيح الأخطاء على واجهة سطر أوامر (CLI) WLC).الأمر **debug pm pki enable**.

```
Cisco Controller) >debug pm pki enable)
...Mon May 22 06:34:10 2006: sshpmGetIssuerHandles: getting (old) aes ID cert handle
    <Mon May 22 06:34:10 2006: sshpmGetCID: called to evaluate <bsnOldDefaultIdCert
                Mon May 22 06:34:10 2006: sshpmGetCID: comparing to row 0, CA cert
                                                        >bsnOldDefaultCaCert<
                Mon May 22 06:34:10 2006: sshpmGetCID: comparing to row 1, CA cert
                                                    >bsnDefaultRootCaCert<
                Mon May 22 06:34:10 2006: sshpmGetCID: comparing to row 2, CA cert
                                                       >bsnDefaultCaCert<
                Mon May 22 06:34:10 2006: sshpmGetCID: comparing to row 3, CA cert
                                                        >bsnDefaultBuildCert<
                Mon May 22 06:34:10 2006: sshpmGetCID: comparing to row 4, CA cert
                                                   >cscoDefaultNewRootCaCert<
                Mon May 22 06:34:10 2006: sshpmGetCID: comparing to row 5, CA cert
                                                    >cscoDefaultMfgCaCert<
                Mon May 22 06:34:10 2006: sshpmGetCID: comparing to row 0, ID cert
                                                        >bsnOldDefaultIdCert<
  Mon May 22 06:34:10 2006: sshpmGetIssuerHandles: Calculate SHA1 hash on Public Key
                                                                          Data
        Mon May 22 06:34:10 2006: sshpmGetIssuerHandles: Key Data  30820122 300d0609
                                                                   2a864886 f70d0101
        Mon May 22 06:34:10 2006: sshpmGetIssuerHandles: Key Data  01050003 82010f00
                                                                   3082010a 02820101
        Mon May 22 06:34:10 2006: sshpmGetIssuerHandles: Key Data  00c805cd 7d406ea0
                                                                   cad8df69 b366fd4c
        Mon May 22 06:34:10 2006: sshpmGetIssuerHandles: Key Data  82fc0df0 39f2bff7
                                                                   ad425fa7 face8f15
        Mon May 22 06:34:10 2006: sshpmGetIssuerHandles: Key Data  f356a6b3 9b876251
                                                                   43b95a34 49292e11
        Mon May 22 06:34:10 2006: sshpmGetIssuerHandles: Key Data  038181eb 058c782e
                                                                   56f0ad91 2d61a389
        Mon May 22 06:34:10 2006: sshpmGetIssuerHandles: Key Data  f81fa6ce cd1f400b
                                                                   b5cf7cef 06ba4375
        Mon May 22 06:34:10 2006: sshpmGetIssuerHandles: Key Data  dde0648e c4d63259
                                                                   774ce74e 9e2fde19
        Mon May 22 06:34:10 2006: sshpmGetIssuerHandles: Key Data  0f463f9e c77b79ea
                                                                   65d8639b d63aa0e3
        Mon May 22 06:34:10 2006: sshpmGetIssuerHandles: Key Data  7dd485db 251e2e07
                                                                   9cd31041 b0734a55
        Mon May 22 06:34:14 2006: sshpmGetIssuerHandles: Key Data  463fbacc 1a61502d
                                                                   c54e75f2 6d28fc6b
        Mon May 22 06:34:14 2006: sshpmGetIssuerHandles: Key Data  82315490 881e3e31
                                                                   02d37140 7c9c865a
        Mon May 22 06:34:14 2006: sshpmGetIssuerHandles: Key Data  9ef3311b d514795f
                                                                   7a9bac00 d13ff85f
        Mon May 22 06:34:14 2006: sshpmGetIssuerHandles: Key Data  97e1a693 f9f6c5cb
                                                                   88053e8b 7fae6d67
        Mon May 22 06:34:14 2006: sshpmGetIssuerHandles: Key Data  ca364f6f 76cf78bc
                                                                   bc1acc13 0d334aa6
        Mon May 22 06:34:14 2006: sshpmGetIssuerHandles: Key Data  031fb2a3 b5e572df
```

```
                                                        2c831e7e f765b7e5
Mon May 22 06:34:14 2006: sshpmGetIssuerHandles: Key Data  fe64641f de2a6fe3
                                                        8302b8b8 23311756
Mon May 22 06:34:14 2006: sshpmGetIssuerHandles: Key Data  1bfae1a8 eb076940
                                                        280cbed1 49b2d50f
    Mon May 22 06:34:14 2006: sshpmGetIssuerHandles: Key Data  f7020301 0001
        Mon May 22 06:34:14 2006: sshpmGetIssuerHandles: SSC Key Hash is
                                                        9e4ddd8dfcdd8458ba7b273fc37284b31a384eb9
  Mon May 22 06:34:14 2006: LWAPP Join-Request MTU path from AP 00:0e:84:32:04:f0
                                                    is 1500, remote debug mode is 0
Mon May 22 06:34:14 2006: spamRadiusProcessResponse: AP Authorization failure for
                                                        00:0e:84:32:04:f0
```

إضافة SSC إلى WLC

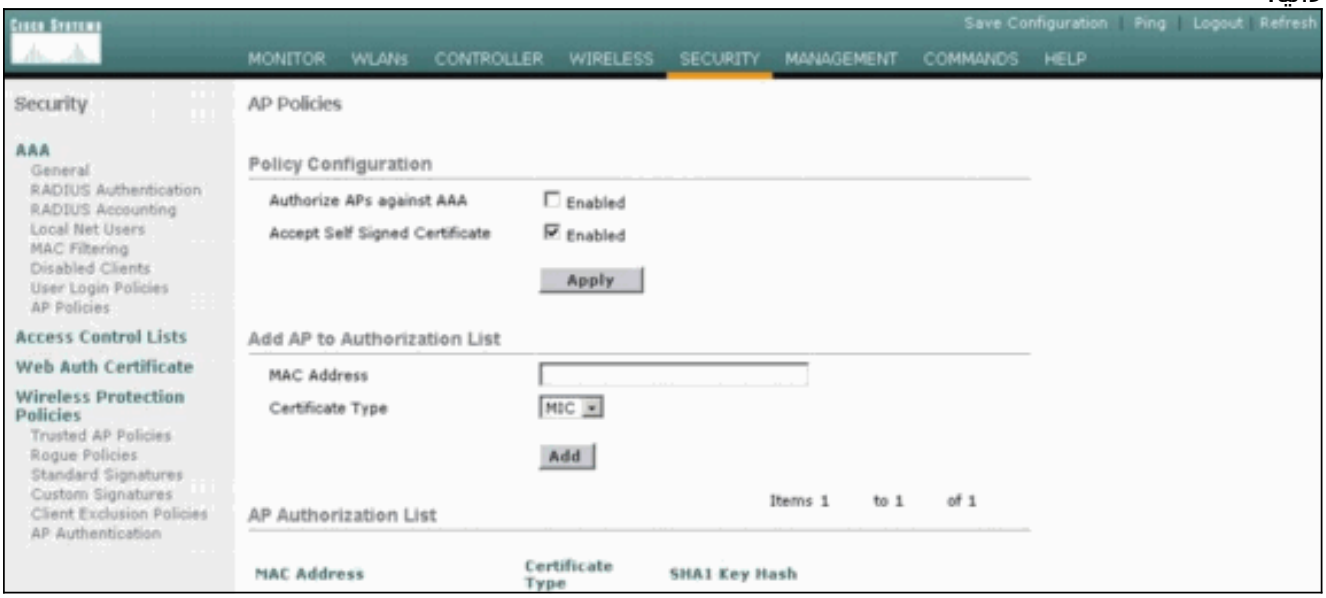
المهمة

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

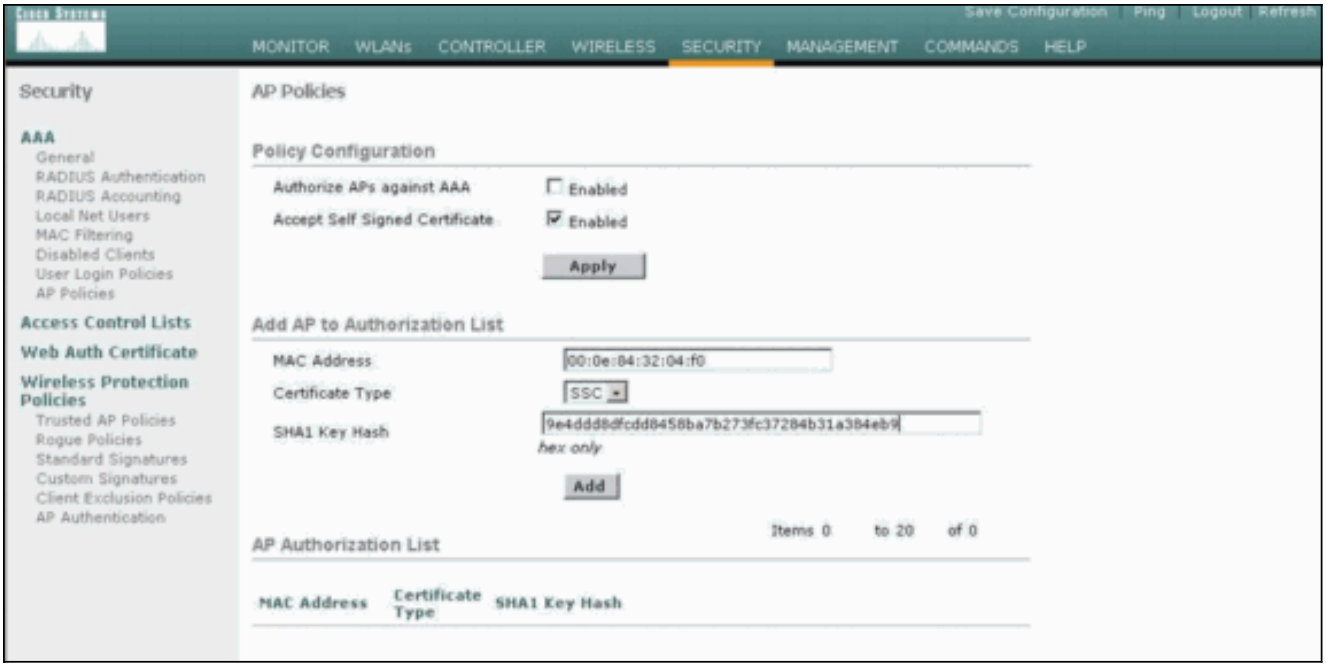
تكوين GUI

أتمت هذا steps من ال gui:

1. أختر **التأمين > سياسات نقطة الوصول** وانقر **يمكن** بالإضافة إلى قبول الترخيص الموقع ذاتيا.



2. حدد **SSC** من القائمة المنسدلة نوع الشهادة.



3. أدخل عنوان MAC لنقطة الوصول ومفتاح التجزئة، وانقر **إضافة**.

تكوين واجهة سطر الأوامر (CLI)

أتمت هذا steps من ال CLI:

1. تمكين قبول الشهادة الموقعة ذاتيا على عنصر التحكم في الشبكة المحلية اللاسلكية (WLC).الأمر **config auth-list ap-policy ssc enable**.

```
Cisco Controller) >config auth-list ap-policy ssc enable)
```

2. إضافة عنوان MAC لنقطة الوصول ومفتاح التجزئة إلى قائمة التخويل.الأمر **config auth-list add ssc** *AP_MAC AP_Key* .

```
Cisco Controller) >config auth-list add ssc 00:0e:84:32:04:f0)
9e4ddd8dfcdd8458ba7b273fc37284b31a384eb9
.This command should be on one line ---!
```

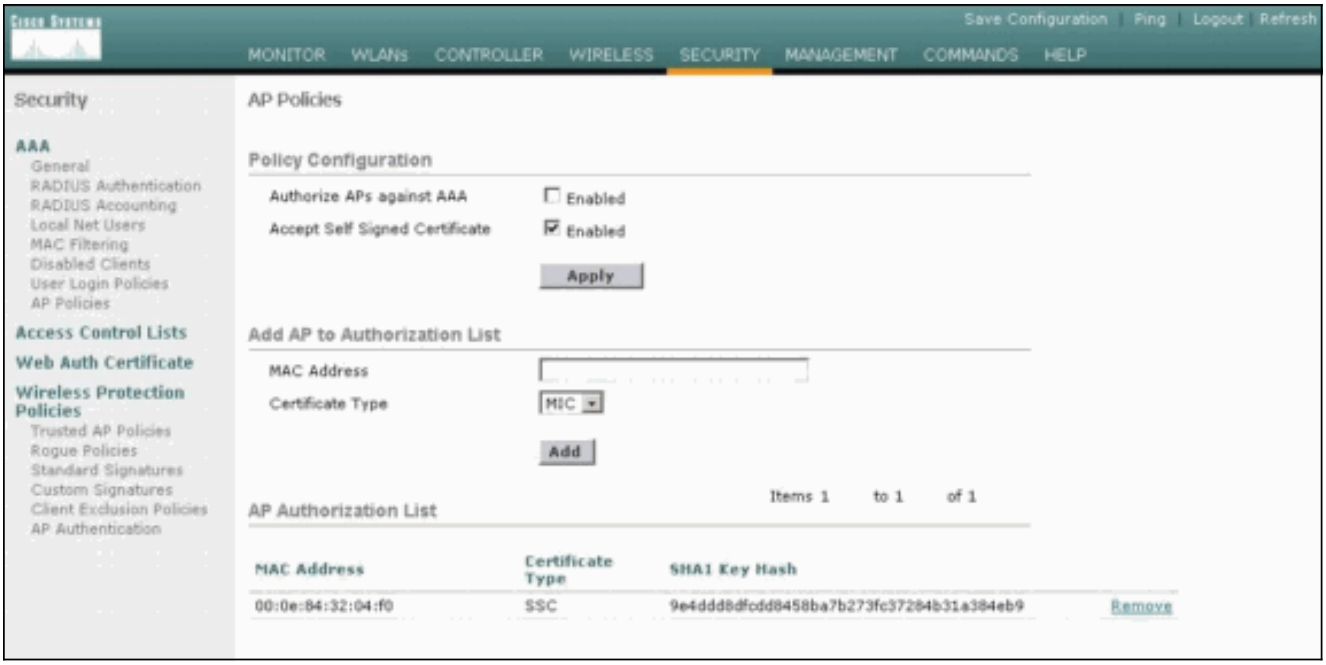
التحقق من الصحة

استخدم هذا القسم لتأكيد عمل التكوين بشكل صحيح.

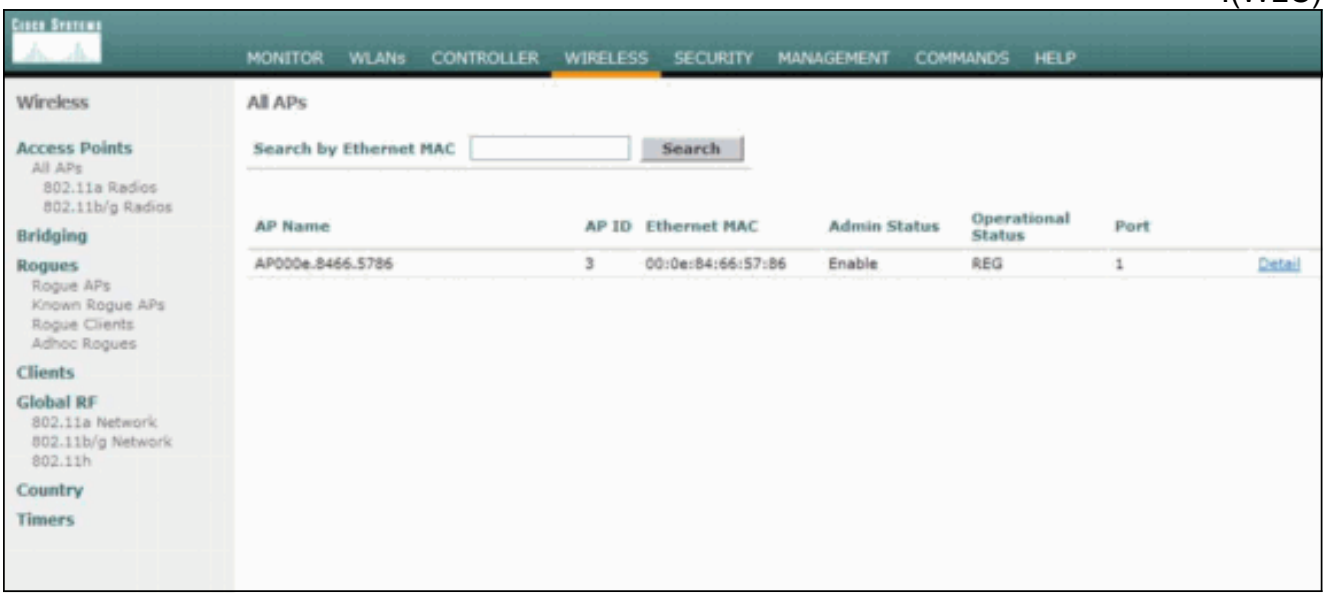
التحقق من واجهة المستخدم الرسومية (GUI)

أكمل الخطوات التالية:

1. في نافذة سياسات نقطة الوصول، تحقق من ظهور عنوان MAC لنقطة الوصول وتجزئة مفتاح SHA1 في منطقة قائمة تخويل نقطة الوصول.



2. في نافذة جميع نقاط الوصول، تحقق من تسجيل جميع نقاط الوصول في عنصر التحكم في الشبكة المحلية اللاسلكية (WLC).



التحقق من واجهة سطر الأوامر (CLI)

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

- show auth-list—يعرض قائمة تخويل نقطة الوصول.
- show ap summary— يعرض ملخصا لكل APs المتصلة.

استكشاف الأخطاء وإصلاحها

لا تتوفر حاليًا معلومات محددة لاستكشاف الأخطاء وإصلاحها لهذا التكوين.

معلومات ذات صلة

- أستكشاف أخطاء وحدة التحكم في الشبكة المحلية (LAN) اللاسلكية وإصلاحها
- دليل تكوين وحدة تحكم شبكة LAN اللاسلكية من Cisco، الإصدار 3.2
- مثال التكوين الأساسي لنقطة الوصول في الوضع Lightweight ووحدة تحكم الشبكة المحلية (LAN) اللاسلكية
- الدعم التقني والمستندات - Cisco Systems

حول هذه الترجمة
ترجمت Cisco هذا المستند باستخدام مجموعة من التقنيات الآلية والبشرية لتقديم محتوى دعم للمستخدمين في جميع أنحاء العالم بلغتهم الخاصة. يُرجى ملاحظة أن أفضل ترجمة آلية لن تكون دقيقة كما هو الحال مع الترجمة الاحترافية التي يقدمها مترجم محترف. تخلي Cisco Systems مسئوليتها عن دقة هذه الترجمات وتُوصي بالرجوع دائمًا إلى المستند الإنجليزي الأصلي (الرابط متوفر).