سياسات نقطة الوصول الموثوق بها على وحدة تحكم الشبكة المحلية (LAN) اللاسلكية

المحتويات

المقدمة

يصف هذا المستند سياسات الحماية اللاسلكية لنقطة الوصول *الموثوق بها* على وحدة تحكم شبكة محلية لاسلكية (WLC)، ويحدد سياسات نقطة الوصول الموثوق بها، ويقدم وصفا موجزا لجميع سياسات نقطة الوصول (AP) الموثوق بها.

المتطلبات الأساسية

المتطلبات

تأكد من فهمك الأساسي لمعلمات أمان شبكة LAN اللاسلكية (مثل SSID والتشفير والمصادقة وما إلى ذلك).

الاصطلاحات

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

سياسات نقطة الوصول الموثوق بها

سياسات نقطة الوصول الموثوق بها هي ميزة أمان في وحدة التحكم تم تصميمها ليتم إستخدامها في السيناريوهات التي يتمتع فيها العملاء بشبكة نقطة وصول (AP) مستقلة متوازية بالإضافة إلى وحدة التحكم. في هذا السيناريو، يمكن تمييز نقطة الوصول المستقلة على أنها نقطة وصول موثوقة على وحدة التحكم، ويمكن للمستخدم تحديد سياسات لنقاط الوصول الموثوقة هذه (التي يجب أن تستخدم WEP أو WPA فقط، و SSID الخاصة بنا، والديباجة

القصيرة، وما إلى ذلك). في حالة فشل أي من نقاط الوصول هذه في الوفاء بهذه السياسات، تقوم وحدة التحكم بتوجيه تنبيه إلى جهاز إدارة الشبكة (نظام التحكم اللاسلكي) الذي يفيد بأن نقطة الوصول الموثوق بها قامت بخرق سياسة تم تكوينها.

ما هي نقطة الوصول الموثوقة؟

نقاط الوصول الموثوقة هي نقاط وصول لا تشكل جزءا من مؤسسة. ومع ذلك، فهي لا تتسبب في تهديد أمان للشبكة. وتسمى نقاط الوصول هذه أيضا نقاط وصول (AP) صديقة. توجد عدة سيناريوهات حيث قد تريد تكوين نقطة وصول كنقطة وصول موثوقة.

على سبيل المثال، قد يكون لديك فئات مختلفة من نقاط الوصول في شبكتك مثل:

- **نقاط الوصول التي تملكها والتي لا تشغل LWAPP (ربما تقوم بتشغيل IOS أو VxWorks)**
- نقاط الوصول من LWAPP التي يجلبها الموظفون (بعلم المسؤول)
- نقاط الوصول LWAPP المستخدمة لاختبار الشبكة الموجودة
- نقاط وصول LWAPP التي يملكها الجيران

عادة، تكون نقاط الوصول الموثوق بها هي نقاط وصول (AP) تقع في **الفئة 1**، وهي نقاط وصول (AP) تملكها ولا تقوم بتشغيل LWAPP. قد تكون نقاط وصول قديمة تشغل VxWorks أو IOS. لضمان ألا تضر نقاط الوصول هذه الشبكة، يمكن فرض ميزات معينة، مثل أنواع SSID والمصادقة الصحيحة. قم بتكوين سياسات نقطة الوصول الموثوق بها على عنصر التحكم في الشبكة المحلية اللاسلكية (WLC)، وتأكد من تطابق نقاط الوصول الموثوق بها مع هذه السياسات. وإذا لم تكن هناك مساحة، فيمكنك تكوين وحدة التحكم لاتخاذ العديد من الإجراءات، مثل التنبيه لجهاز إدارة الشبكة (WCS).

يمكن تكوين نقاط الوصول المعروفة التي تنتمي إلى الجيران على أنها نقاط وصول موثوقة.

عادة، يجب أن تمنع MFP (حماية إطار الإدارة) نقاط الوصول (APs) التي لا تعتبر نقاط وصول LWAPP مشروعة من الانضمام إلى عنصر التحكم في الشبكة المحلية اللاسلكية (WLC). إذا كانت بطاقات واجهة الشبكة (NIC) تدعم MFP، فلا يسمح لها بقبول عمليات إلغاء المصادقة من الأجهزة الأخرى بخلاف نقاط الوصول الحقيقية. راجع حماية إطار إدارة البنية الأساسية (MFP) مع WLC ومثال تكوين نقاط الوصول في الوضع Lightweight للحصول على مزيد من المعلومات حول MFP.

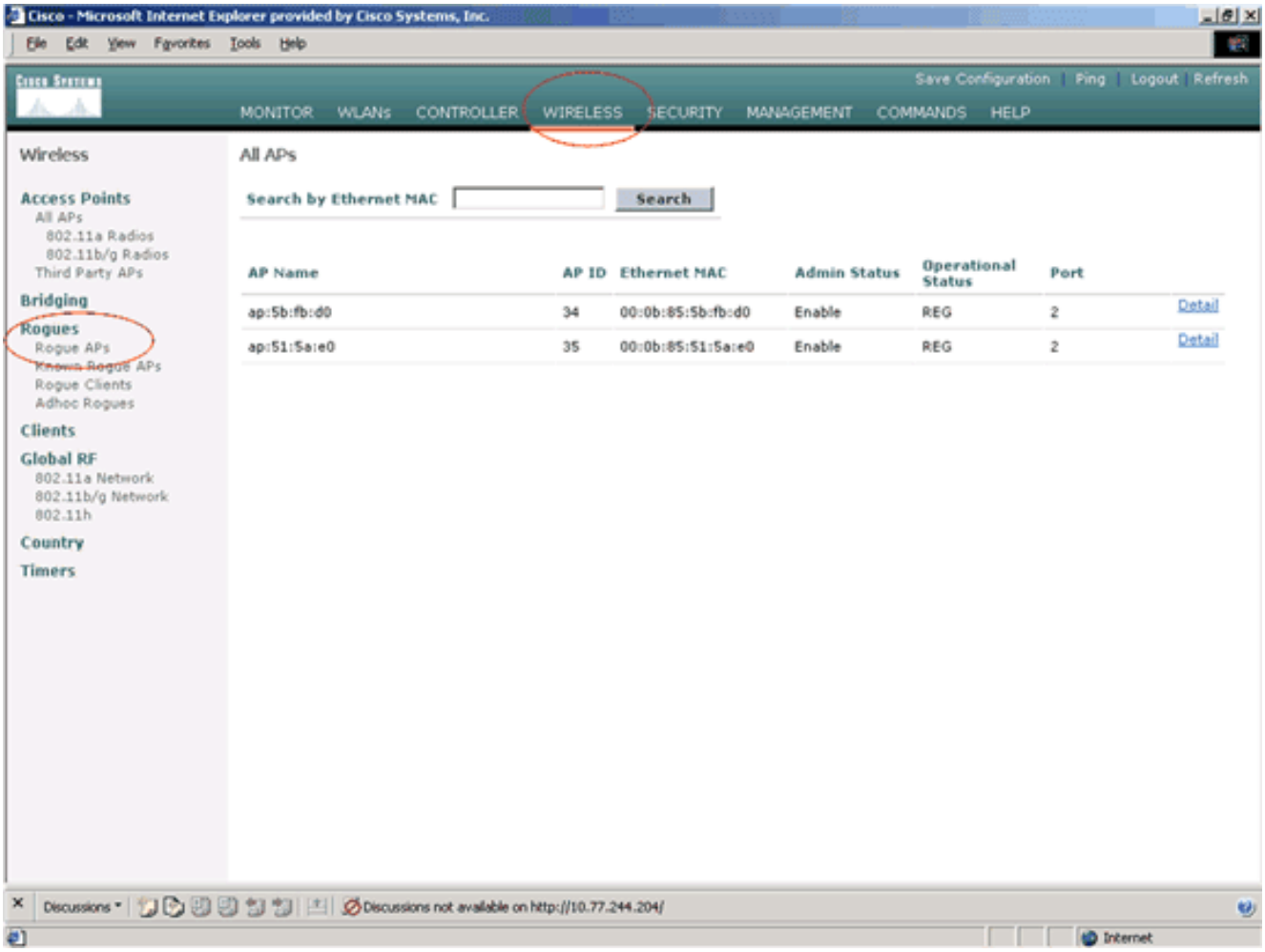
إذا كانت لديك نقاط وصول تشغل VxWorks أو IOS (كما هو الحال في الفئة 1)، فلن تنضم أبدا إلى مجموعة LWAPP أو تقوم ب MFP، ولكن قد ترغب في فرض النهج المدرجة في تلك الصفحة. في مثل هذه الحالات، يلزم تكوين سياسات نقاط الوصول الموثوق بها على وحدة التحكم لنقاط الوصول ذات الاهتمام.

بشكل عام، إذا كنت تعرف عن نقطة وصول مخادعة وتعرف أنها لا تشكل تهديدا لشبكتك، فيمكنك تعريف نقطة الوصول هذه بأنها نقطة وصول موثوقة معروفة.

كيف أن يشكل ap كapموثوق من ال WLC GUI؟

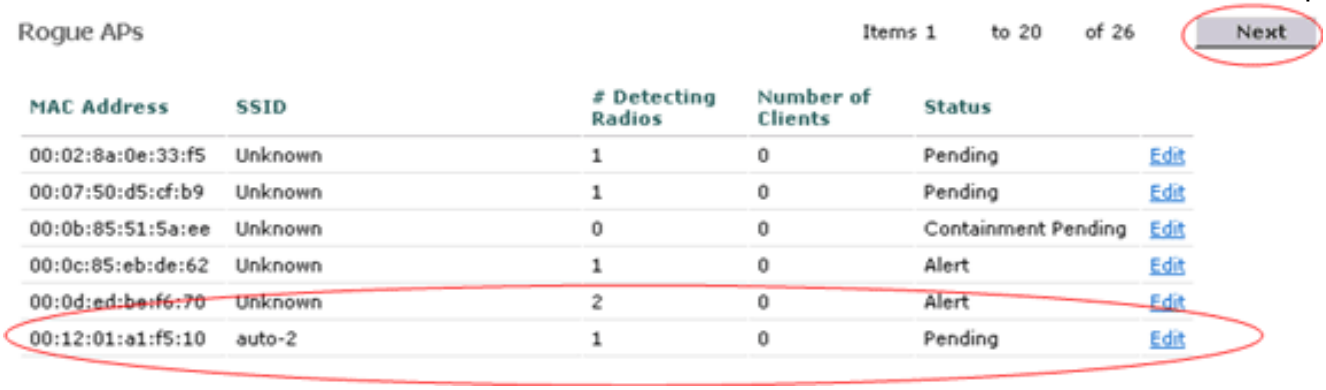
أتمت هذا steps in order to شكلت AP كapموثوق:

1. قم بتسجيل الدخول إلى واجهة المستخدم الرسومية (GUI) الخاصة بوحدة التحكم في الشبكة المحلية اللاسلكية (WLC) من خلال تسجيل الدخول إلى بروتوكول HTTP أو HTTPS.
2. من القائمة الرئيسية لوحدة التحكم، انقر على **لاسلكي**.
3. في القائمة الموجودة على الجانب الأيسر من الصفحة اللاسلكية، انقر فوق **نقاط الوصول المخادعة**.



تسرد صفحة نقاط الوصول المخادعة جميع نقاط الوصول التي يتم الكشف عنها على أنها نقاط وصول (AP) مخادعة على الشبكة.

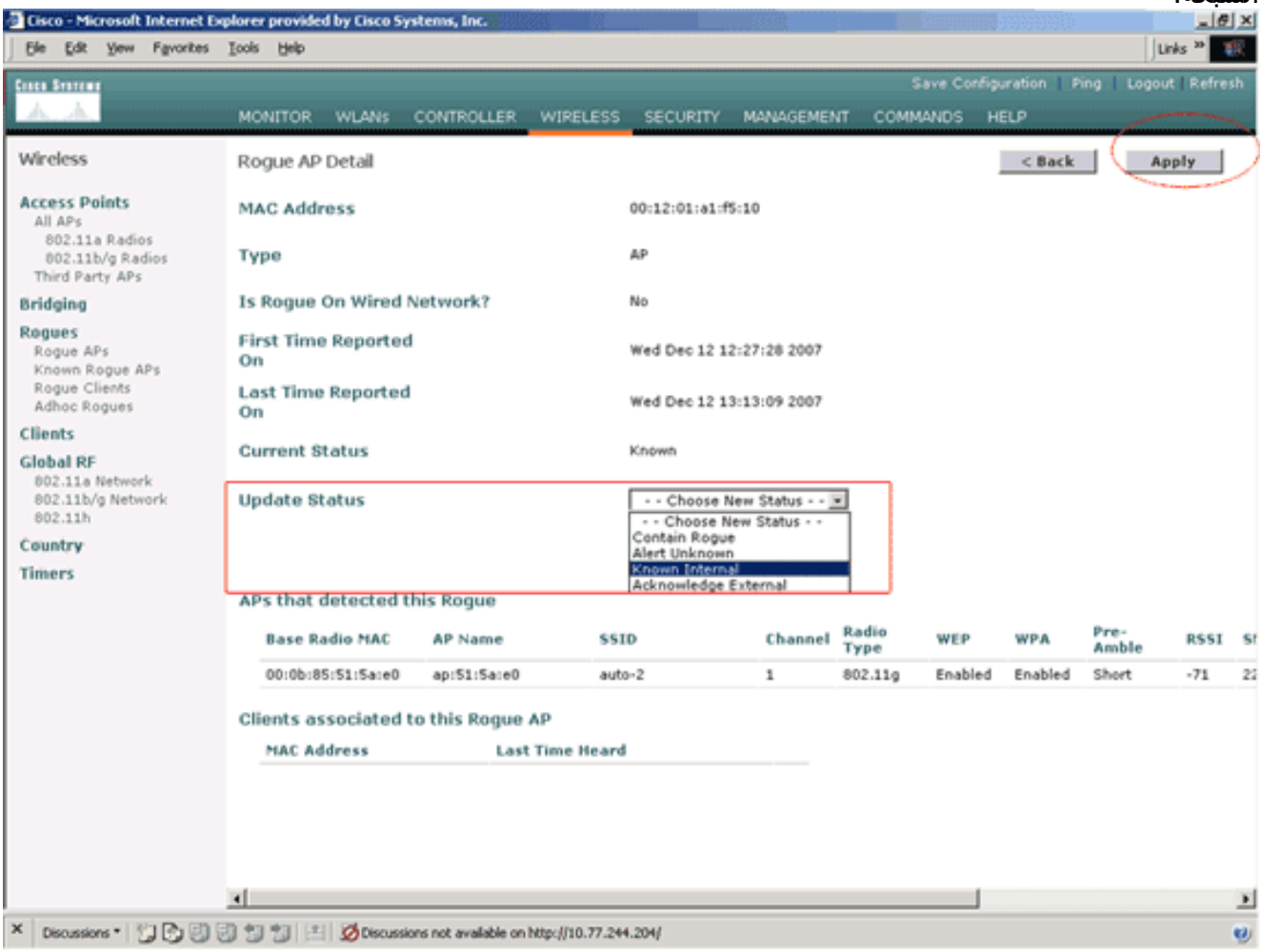
4. من هذه القائمة من نقاط الوصول الدخيلة، حدد موقع نقطة الوصول التي تريد تكوينها كنقطة وصول موثوق بها تقع ضمن الفئة 1 (كما هو موضح في القسم السابق).يمكنك تحديد موقع نقاط الوصول ذات عناوين MAC المدرجة في صفحة نقاط الوصول المخادعة. إذا لم تكن نقطة الوصول المطلوبة في هذه الصفحة، انقر فوق **التالي** للتعرف على نقطة الوصول من الصفحة التالية.
5. ما إن ال AP يكون ب رغب يكون من ال{upper}ap قائمة، طقطقت **ال edit** زر أن يماثل ال ap، أي يأخذك إلى صفحة التفاصيل من ال ap.



في صفحة تفاصيل نقطة الوصول المخادعة، يمكنك العثور على معلومات تفصيلية حول نقطة الوصول هذه (مثل ما إذا كانت نقطة الوصول هذه متصلة بشبكة سلكية، بالإضافة إلى الحالة الحالية لنقطة الوصول وما إلى ذلك).

6. من أجل تكوين نقطة الوصول هذه كنقطة وصول موثوق بها، حدد **داخلي معروف** من القائمة المنسدلة حالة التحديث، وانقر فوق **تطبيق**.عندما تقوم بتحديث حالة نقطة الوصول إلى *نقطة الوصول الداخلية المعروفة*، يتم تكوين نقطة الوصول هذه كنقطة الوصول الموثوق بها لهذه

الشبكة.

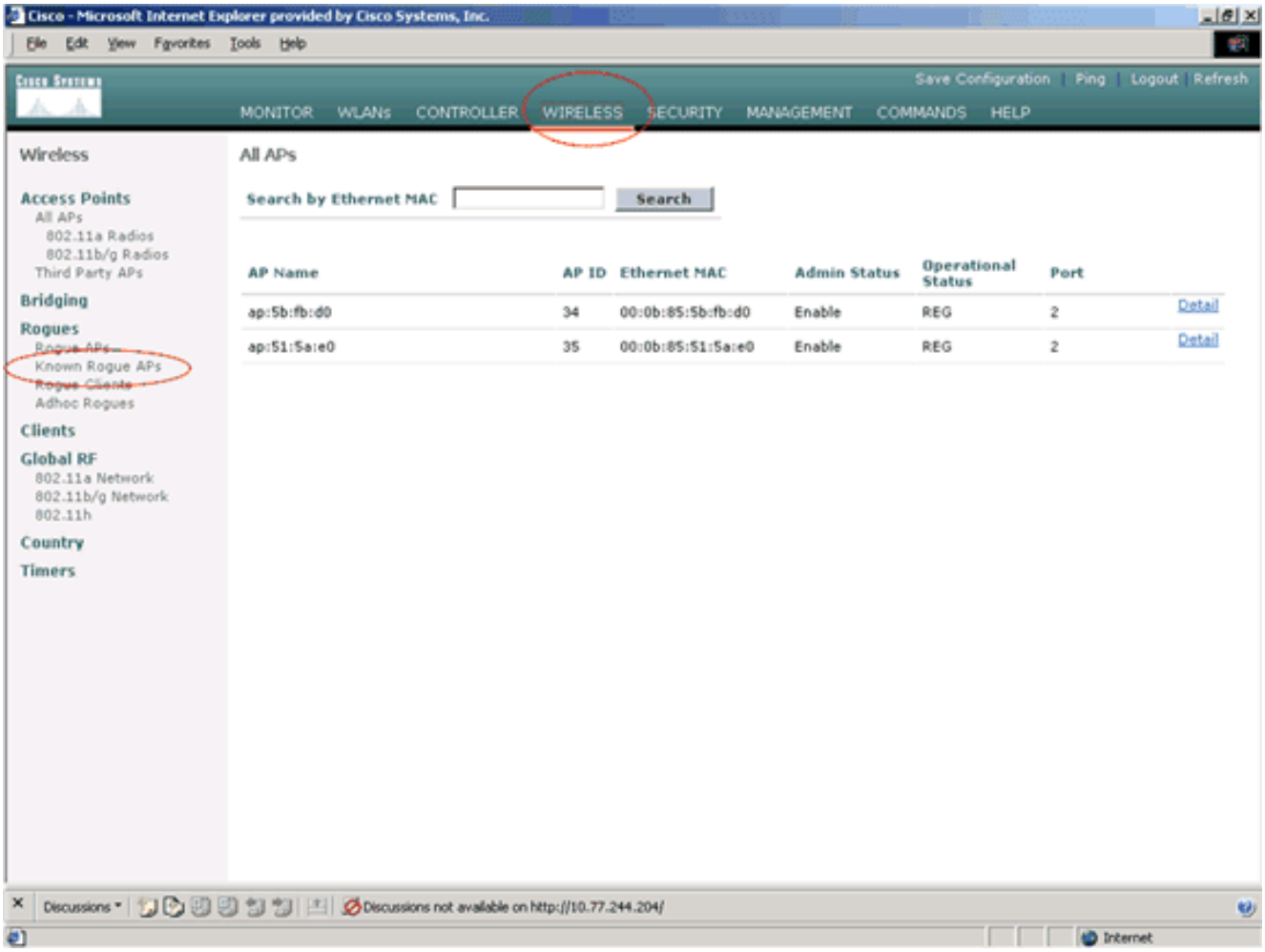


7. كرر هذه الخطوات لجميع نقاط الوصول التي تريد تكوينها كنقاط وصول موثوقة.

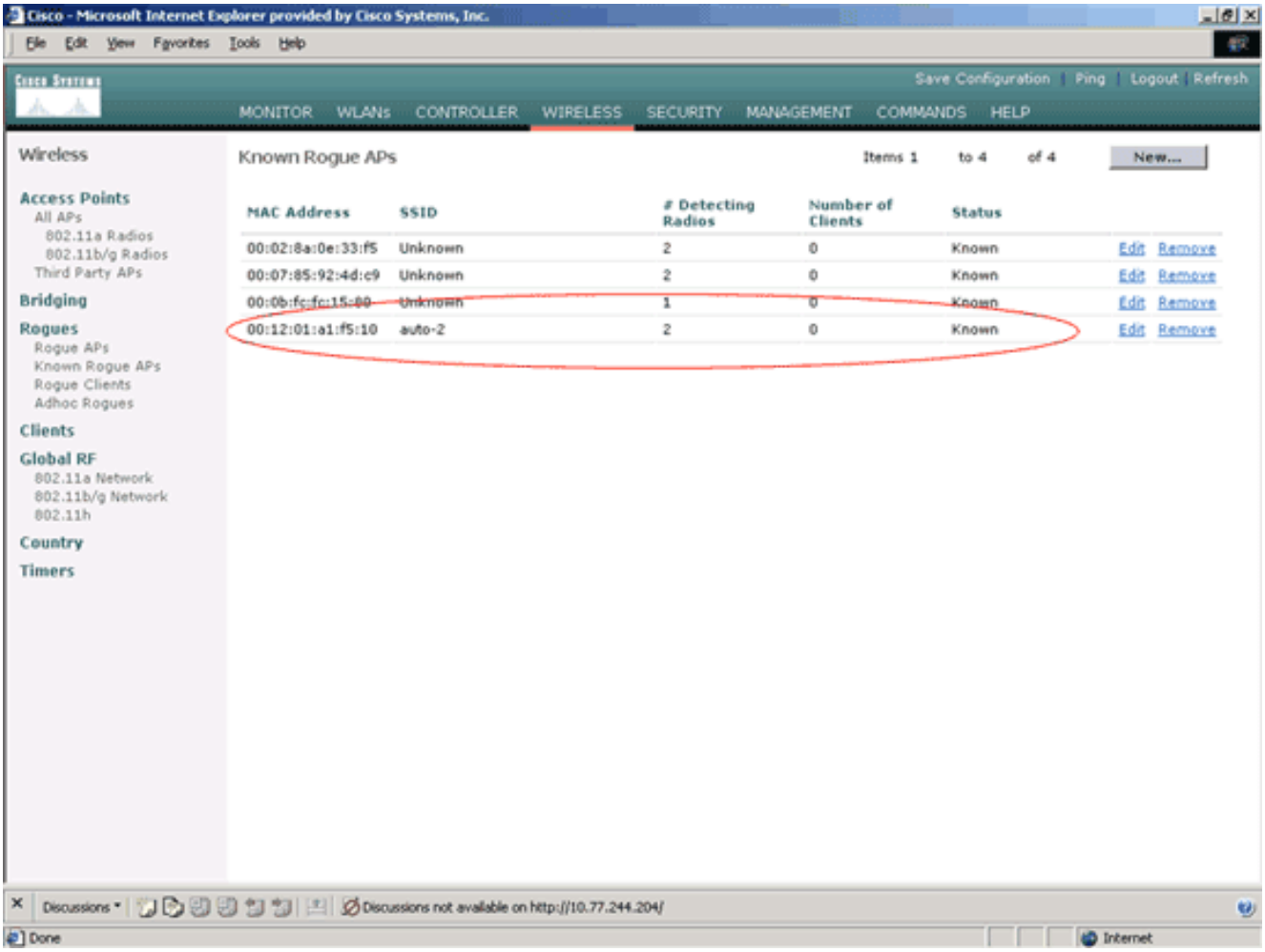
التحقق من تكوين نقطة الوصول الموثوق بها

أتمت هذا steps in order to دققت أن شكلت ال AP بشكل صحيح كap موثوق من الجهاز تحكم gui:

1. انقر على **لاسلكي**.
2. في القائمة الموجودة على الجانب الأيسر من الصفحة اللاسلكية، انقر فوق **نقاط الوصول المخادعة المعروفة**.



يجب أن تظهر نقطة الوصول المرغوبة في صفحة نقاط الوصول الدخيلة المعروفة مع الحالة المدرجة على أنها *معروفة*.



فهم إعدادات نهج نقطة الوصول الموثوق بها

يحتوي عنصر التحكم في الشبكة المحلية اللاسلكية (WLC) على سياسات نقطة الوصول (AP) الموثوقة التالية:

- نهج التشفير المفروض
- سياسة الديباجة المفروضة
- فرض نهج نوع الراديو
- التحقق من صحة SSID
- تنبيه في حالة فقدان نقطة الوصول الموثوق بها
- مهلة انتهاء الصلاحية لإدخالات نقطة الوصول الموثوق بها (بالثواني)

نهج التشفير المفروض

يستخدم هذا النهج لتعريف نوع التشفير الذي يجب أن تستخدمه نقطة الوصول الموثوق بها. يمكنك تكوين أي من أنواع التشفير هذه بموجب نهج التشفير الإجباري:

- None
- فتح
- WEP
- WPA/802.11i

يتحقق عنصر التحكم في الشبكة المحلية اللاسلكية (WLC) مما إذا كان نوع التشفير الذي تم تكوينه على نقطة الوصول الموثوق بها يطابق نوع التشفير الذي تم تكوينه في الإعداد **فرض نهج التشفير**". إذا لم تستخدم نقطة الوصول الموثوق بها نوع التشفير المعين، فإن عنصر التحكم في الشبكة المحلية اللاسلكية (WLC) يوجه إنذار إلى نظام الإدارة لاتخاذ الإجراءات المناسبة.

سياسة الديباجة المفروضة

ديباجة الراديو (تسمى أحيانا رأس) هي قسم من البيانات في رأس الحزمة يحتوي على معلومات تحتاجها الأجهزة اللاسلكية عند إرسال واستقبال الحزم. **تساعد** التمهيد **القصير** على تحسين أداء الخرج، بحيث يتم تمكينها بشكل افتراضي. ومع ذلك، تتطلب بعض الأجهزة اللاسلكية، مثل هواتف SpectraLink NetLink، **مقدمات طويلة**. يمكنك تكوين أي من خيارات الديباجة هذه تحت فرض سياسة الديباجة:

- None
- قصير
- طويل

يتحقق عنصر التحكم في الشبكة المحلية اللاسلكية (WLC) مما إذا كان نوع الديباجة الذي تم تكوينه على نقطة الوصول الموثوق بها يطابق نوع الديباجة التي تم تكوينها على الإعداد **فرض سياسة** الديباجة. إذا لم تستخدم نقطة الوصول الموثوق بها نوع الديباجة المحدد، فإن عنصر التحكم في الشبكة المحلية اللاسلكية (WLC) يوجه إنذار إلى نظام الإدارة لاتخاذ الإجراءات المناسبة.

فرض نهج نوع الراديو

يستخدم هذا النهج لتعريف نوع الراديو الذي يجب أن تستخدمه نقطة الوصول الموثوق بها. يمكنك تكوين أي من أنواع الراديو هذه تحت نهج نوع الراديو الإجباري:

- None
- 802.11b فقط
- 802.11a فقط
- 802.11b/g فقط

يتحقق عنصر التحكم في الشبكة المحلية اللاسلكية (WLC) مما إذا كان نوع الراديو الذي تم تكوينه على نقطة الوصول الموثوق بها يطابق نوع الراديو الذي تم تكوينه في الإعداد **فرض نهج** نوع الراديو. إذا لم تستخدم نقاط الوصول الموثوق بها الأجهزة اللاسلكية المحددة، فإن عنصر التحكم في الشبكة المحلية اللاسلكية (WLC) يوجه إنذار إلى نظام الإدارة لاتخاذ الإجراءات المناسبة.

التحقق من صحة SSID

يمكنك تكوين وحدة التحكم للتحقق من صحة APs موثوق بها مقابل SSIDs المكونة على وحدة التحكم. إذا تطابقت نقطة الوصول (APs) الموثوق بها مع أحد SSIDs لوحدة التحكم يقوم جهاز التحكم بتشغيل جهاز إنذار.

تنبيه عند فقدان نقطة الوصول الموثوق بها

في حالة تمكين هذا النهج، يقوم عنصر التحكم في الشبكة المحلية اللاسلكية (WLC) بتنبيه نظام الإدارة في حالة فقدان نقطة الوصول الموثوق بها من قائمة نقاط الوصول (AP) المخادعة المعروفة.

مهلة انتهاء الصلاحية لإدخالات نقطة الوصول الموثوق بها (بالثواني)

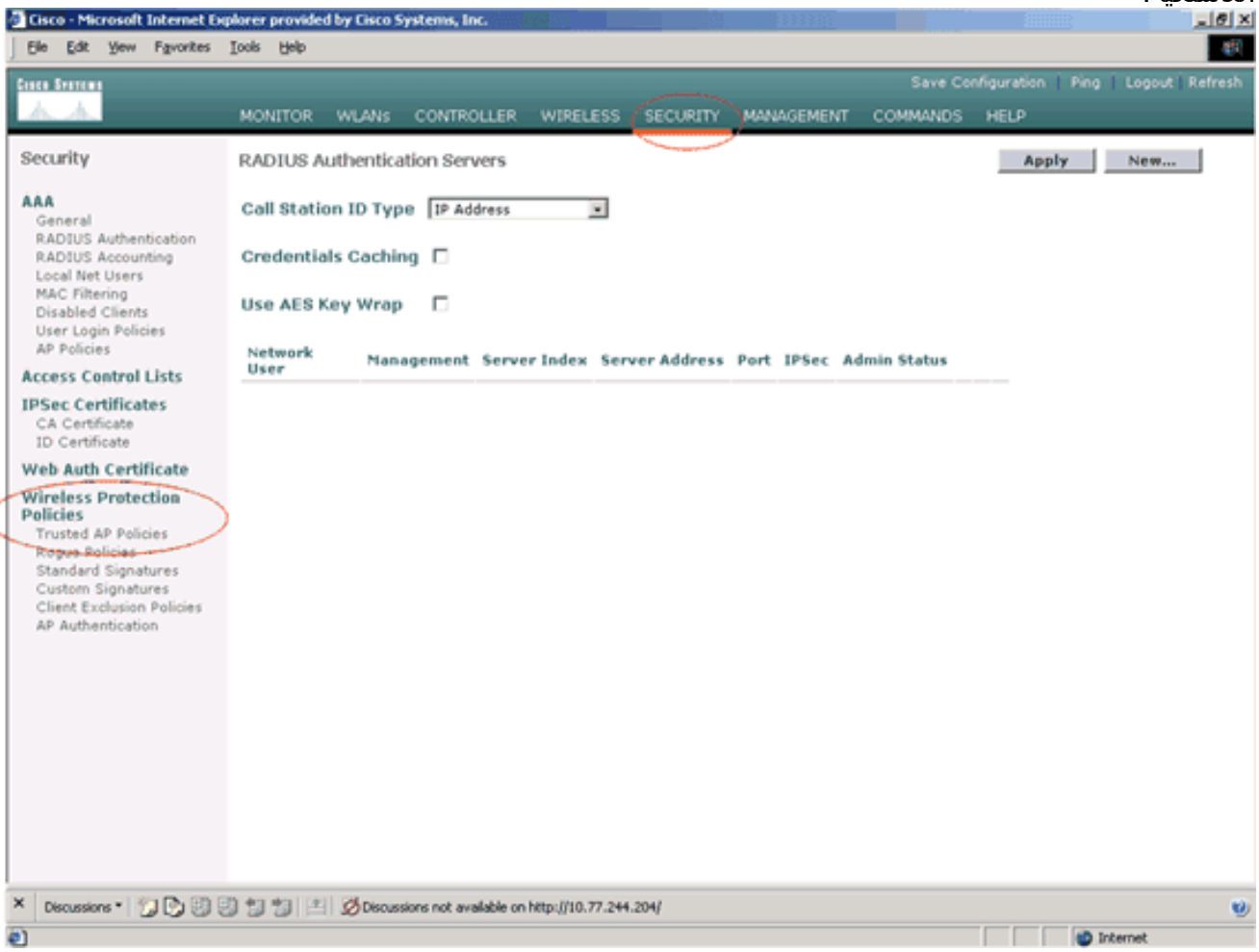
تحدد قيمة مهلة انتهاء الصلاحية هذه عدد الثواني قبل إعتبار نقطة الوصول الموثوق بها منتهية الصلاحية ومسحوبة من إدخال عنصر التحكم في الشبكة المحلية اللاسلكية (WLC). يمكنك تحديد قيمة المهلة هذه بالثواني (120 - 3600 ثانية).

كيف أن يشكل AP سياسة على ال WLC؟

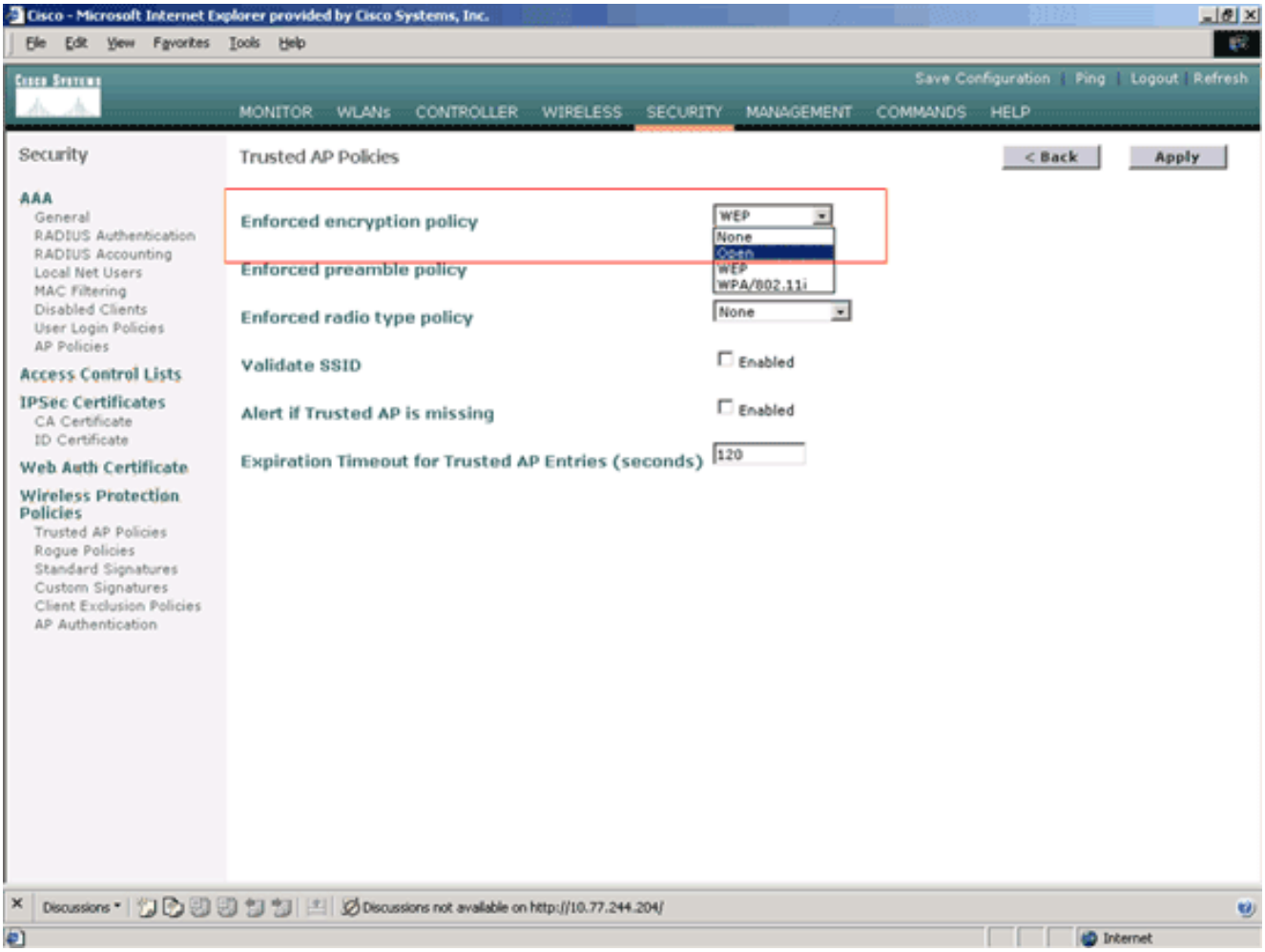
أتمت هذا steps in order to شكلت Trusted AP سياسة على ال WLC من خلال ال gui:

ملاحظة: تقع جميع سياسات نقطة الوصول الموثوق بها على نفس صفحة عنصر التحكم في الشبكة المحلية اللاسلكية (WLC).

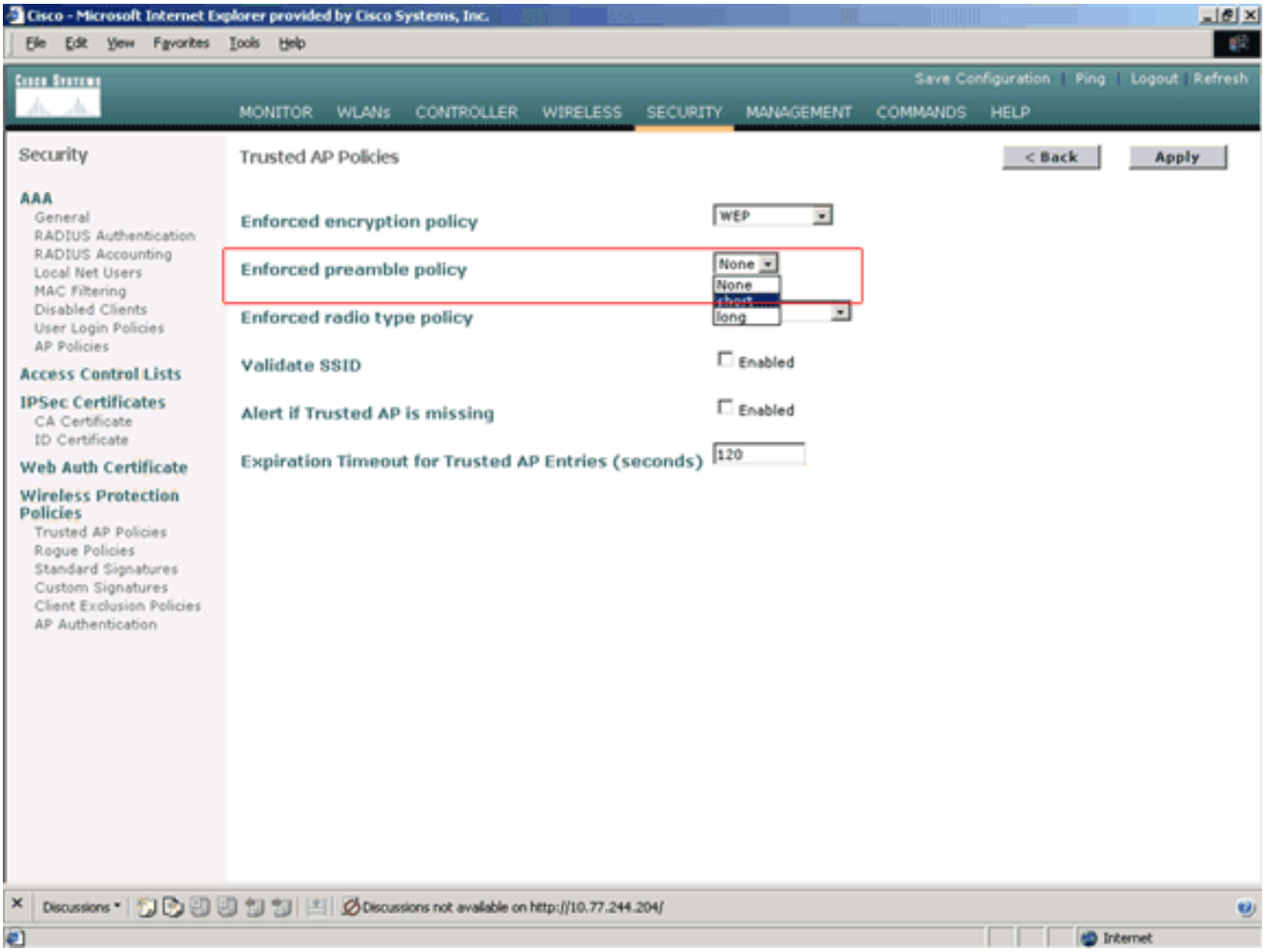
1. من القائمة الرئيسية لواجهة المستخدم الرسومية (GUI) الخاصة بوحدة التحكم في الشبكة المحلية اللاسلكية (WLC)، انقر فوق **الأمان**.
2. من القائمة الموجودة على الجانب الأيسر من صفحة الأمان، انقر على **سياسات نقطة الوصول الموثوق بها** المدرجة تحت عنوان نهج الحماية اللاسلكية.



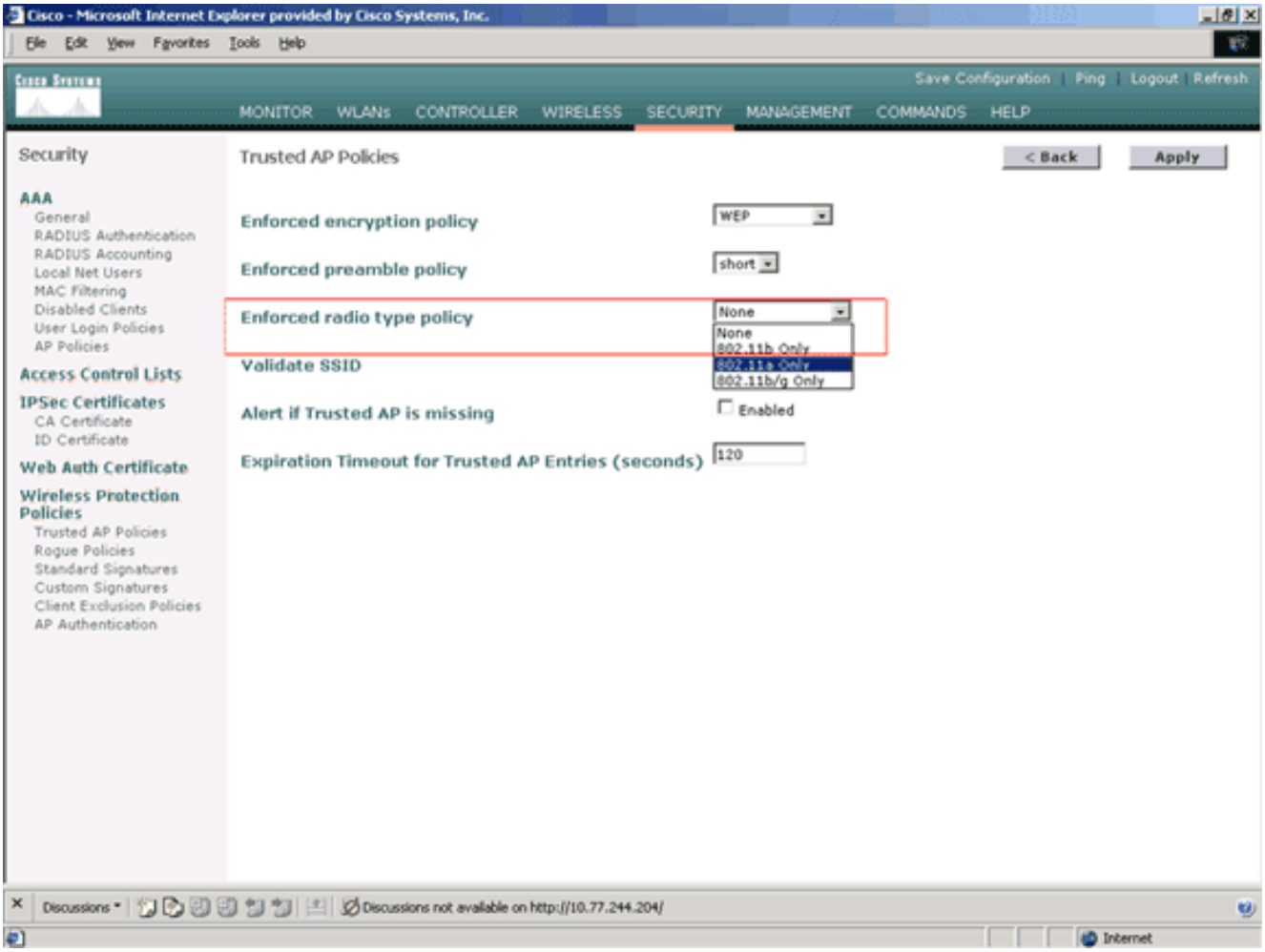
3. في صفحة سياسات نقطة الوصول الموثوق بها، حدد نوع التشفير المرغوب (None و Open و WEP و WPA/802.11i) من القائمة المنسدلة لنهج التشفير القسري.



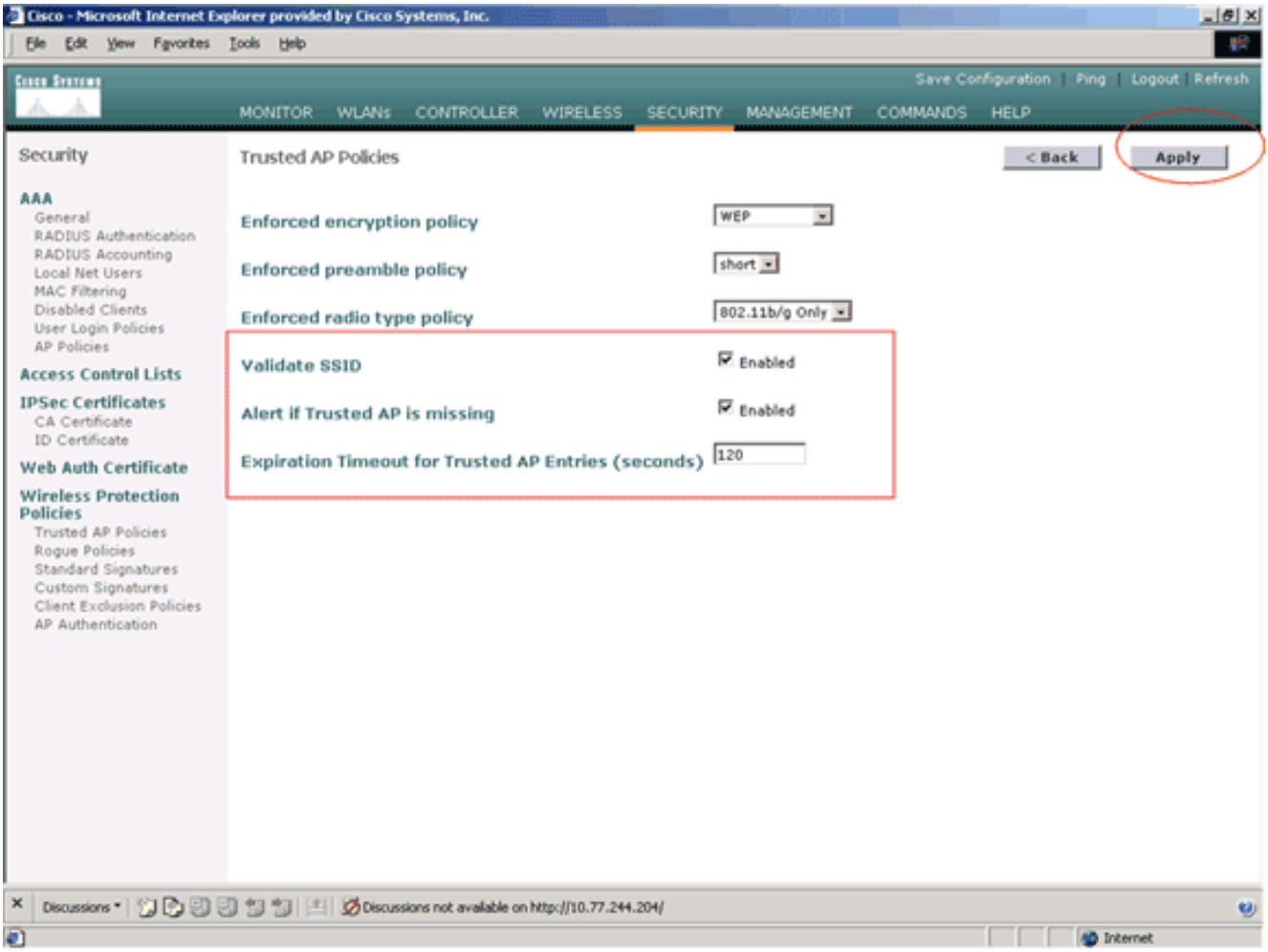
4. حدد نوع التمهيد المطلوب (بلا، قصير، طويل) من القائمة المنسدلة لنهج نوع التمهيد الذي تم فرضه.



5. حدد نوع الراديو المطلوب (بدون، 802.11b فقط، 802.11a فقط، 802.11b/g فقط) من القائمة المنسدلة لسياسة نوع الراديو
الإجباري.



6. حدد أو قم بإلغاء تحديد خانة الاختيار **التحقق من تمكين SSID** لتمكين إعداد SSID أو تعطيله.
7. حدد أو قم بإلغاء تحديد **التنبيه إذا كانت نقطة الوصول الموثوق بها تفتقد** خانة الاختيار **تمكين** لتمكين أو تعطيل التنبيه إذا كانت نقطة الوصول الموثوق بها تفتقد الإعداد.
8. أدخل قيمة (بالثواني) **لخيار مهلة انتهاء الصلاحية لإدخالات نقطة الوصول الموثوق بها**.



9. طقطقة **يطبق**.

ملاحظة: لتكوين هذه الإعدادات من واجهة سطر الأوامر (CLI) الخاصة بوحدة التحكم في الشبكة المحلية اللاسلكية (WLC)، يمكنك إستخدام الأمر **config wps trusted-ap** باستخدام خيار السياسة المناسب.

```
? Cisco Controller) >config wps trusted-ap

.encryption     Configures the trusted AP encryption policy to be enforced
    .missing-ap     Configures alert of missing trusted AP
.preamble       Configures the trusted AP preamble policy to be enforced
.radio          Configures the trusted AP radio policy to be enforced
.timeout        Configures the expiration time for trusted APs, in seconds
```

رسالة تنبيه انتهاك نهج نقطة الوصول الموثوق بها

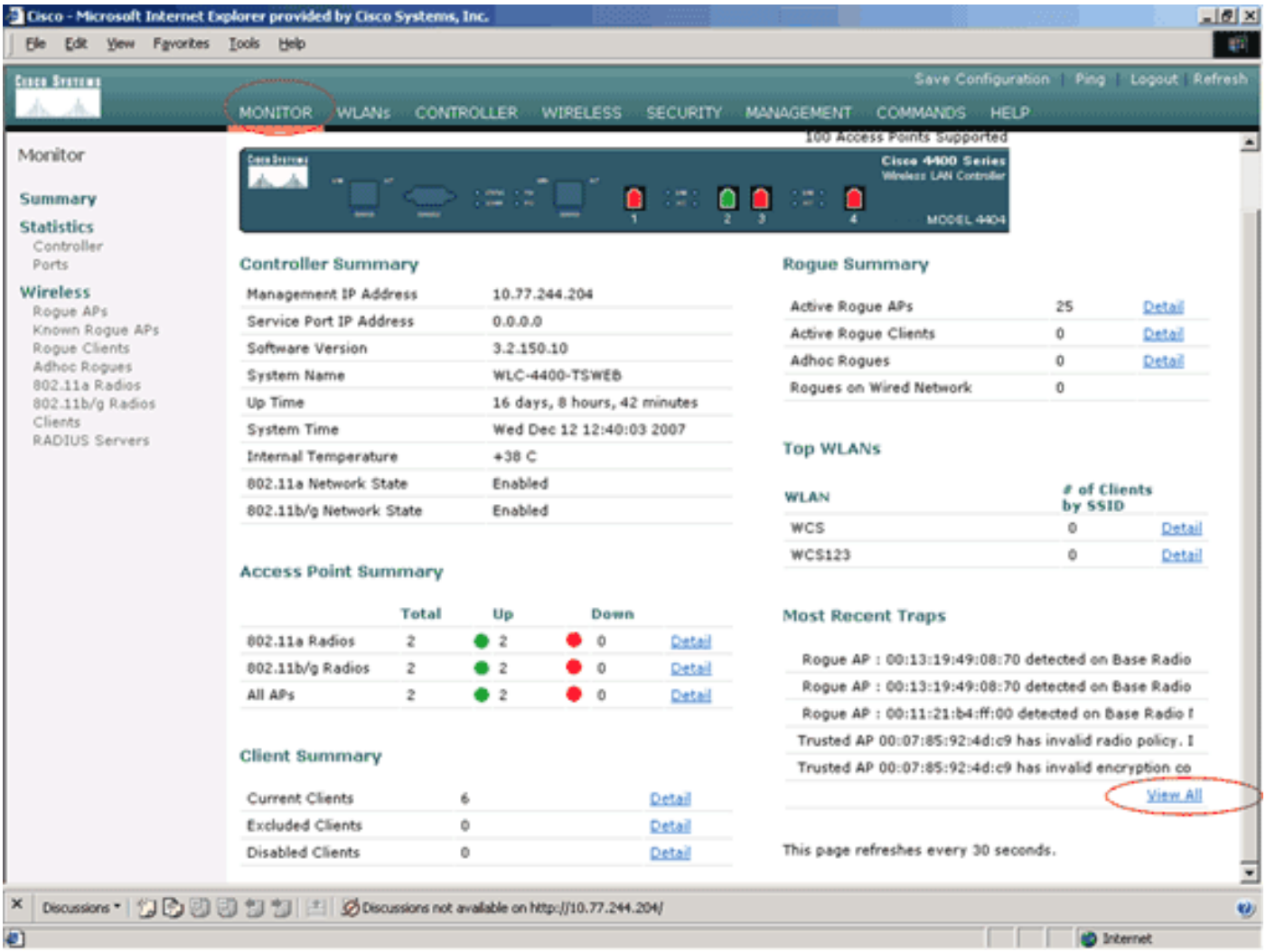
فيما يلي مثال على رسالة تنبيه انتهاك نهج AP الموثوق بها التي يتم عرضها بواسطة وحدة التحكم.

```
Thu Nov 16 12:39:12 2006  [WARNING] apf_rogue.c 1905: Possible AP
impersonation of xx:xx:xx:xx:xx:xx, using source address of
00:16:35:9e:6f:3a, detected by 00:17:df:7d:e1:70 on slot 0
Thu Nov 16 12:39:12 2006  [SECURITY] apf_rogue.c 1490: Trusted AP Policy
'failed for AP xx:xx:xx:xx:xx:xx - invalid SSID 'SSID1
Thu Nov 16 12:39:12 2006  [SECURITY] apf_rogue.c 1457: Trusted AP Policy
failed for AP xx:xx:xx:xx:xx:xx - invalid encryption type
Thu Nov 16 12:39:12 2006  Previous message occurred 6 times
```

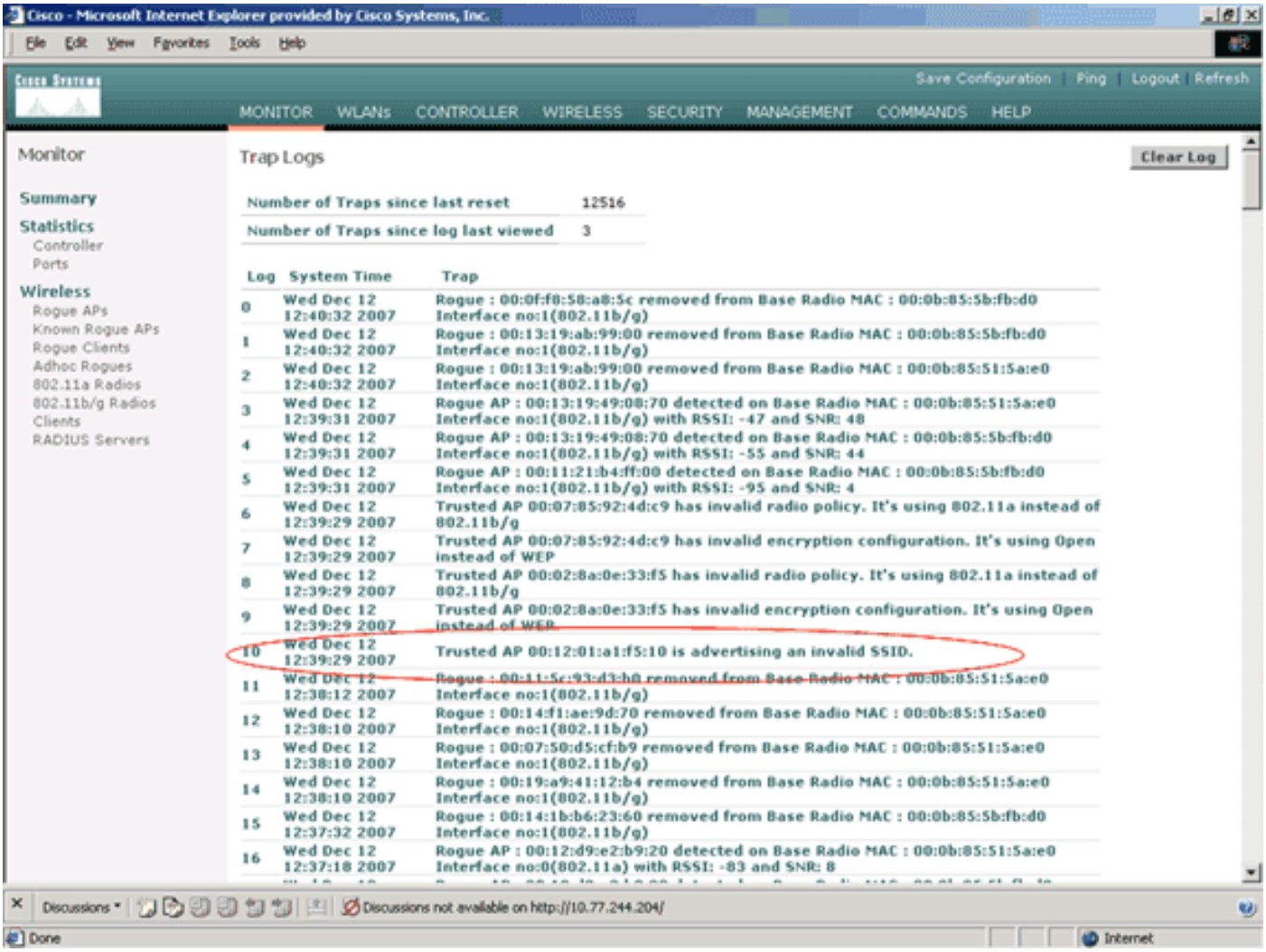
لاحظ رسائل الخطأ المميزة هنا. تشير رسائل الخطأ هذه إلى أن SSID ونوع التشفير الذي تم تكوينه على نقطة الوصول الموثوق بها لا يتطابق مع إعداد نهج نقطة الوصول الموثوق بها.

يمكن رؤية رسالة التنبيه نفسها من واجهة المستخدم الرسومية (GUI) الخاصة بوحدة التحكم في الشبكة المحلية

اللاسلكية (WLC). لعرض هذه الرسالة، انتقل إلى القائمة الرئيسية لواجهة المستخدم الرسومية (GUI) الخاصة بوحدة التحكم في الشبكة المحلية اللاسلكية (WLC)، وانقر فوق **مراقبة**. في القسم الأحدث من صفحة المراقبة، انقر فوق **عرض الكل** لعرض جميع التنبيهات الأخيرة على عنصر التحكم في الشبكة المحلية اللاسلكية (WLC).



في صفحة أحدث الملائمات، يمكنك تعريف وحدة التحكم التي تقوم بإنشاء رسالة تنبيه انتهاك سياسة نقطة الوصول الموثوق بها كما هو موضح في هذه الصورة:



معلومات ذات صلة

- دليل تكوين وحدة تحكم الشبكة المحلية اللاسلكية من Cisco، الإصدار 5.2 - تمكين اكتشاف نقطة وصول الموجه في مجموعات التردد اللاسلكي
- دليل تكوين وحدة تحكم شبكة LAN اللاسلكية من Cisco، الإصدار 4.0 - تكوين حلول الأمان
- الكشف المخادع بموجب الشبكات اللاسلكية الموحدة
- دليل تصميم الهاتف ونشره عبر SpectraLink
- مثال على التكوين الأساسي لاتصال شبكة LAN اللاسلكية
- استكشاف أخطاء الاتصال في شبكة LAN اللاسلكية وإصلاحها
- المصادقة على أمثلة تكوين وحدات 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).