

دليل اهب قووملا لوصول اةطقن تاسايس (LAN) اةلحمل اةكبشلا مكحت اءحو اةكللساللا

المحتويات

[المقدمة](#)

[المتطلبات الأساسية](#)

[المتطلبات](#)

[الاصطلاحات](#)

[سياسات نقطة الوصول الموثوق بها](#)

[ما هي نقطة الوصول الموثوقة؟](#)

[كيف أن بشكل ap ك ap موثوق من ال WLC GUI؟](#)

[فهم إعدادات نهج نقطة الوصول الموثوق بها](#)

[كيف أن بشكل AP سياسة على ال WLC؟](#)

[رسالة تنبيه انتهاك نهج نقطة الوصول الموثوق بها](#)

[معلومات ذات صلة](#)

[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 لمعلومات 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 استخدامها 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 تتضمن 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 بشكل ap ك ap موثوق من ال WLC GUI؟

أتمت هذا steps in order to شكلت AP ك ap موثوق:

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

Rogue APs

Items 1 to 20 of 26 [Next](#)

MAC Address	SSID	# Detecting Radios	Number of Clients	Status	
00:02:8a:0e:33:f5	Unknown	1	0	Pending	Edit
00:07:50:d5:cf:b9	Unknown	1	0	Pending	Edit
00:0b:85:51:5a:ee	Unknown	0	0	Containment Pending	Edit
00:0c:85:eb:de:62	Unknown	1	0	Alert	Edit
00:0d:ed:be:f6:70	Unknown	2	0	Alert	Edit
00:12:01:a1:f5:10	auto-2	1	0	Pending	Edit

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

The screenshot shows the Cisco WLC GUI with the 'Wireless' tab selected. The 'Rogue AP Detail' page is displayed, showing the following information:

- MAC Address: 00:12:01:a1:f5:10
- Type: AP
- Is Rogue On Wired Network?: No
- First Time Reported On: Wed Dec 12 12:27:28 2007
- Last Time Reported On: Wed Dec 12 13:13:09 2007
- Current Status: Known

The 'Update Status' dropdown menu is open, showing the following options:

- Choose New Status
- Choose New Status
- Contain Rogue
- Alert Unknown
- Known Internal
- Acknowledge External

The 'Apply' button is circled in red. Below the 'Update Status' dropdown, there are two tables:

APs that detected this Rogue

Base Radio MAC	AP Name	SSID	Channel	Radio Type	WEP	WPA	Pre-Ambble	RSSI	St
00:0b:85:51:5a:e0	ap:51:5a:e0	auto-2	1	802.11g	Enabled	Enabled	Short	-71	2

Clients associated to this Rogue AP

MAC Address	Last Time Heard
-------------	-----------------

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 دقت أن شكلت ال AP بشكل صحيح ك ap 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.

The screenshot shows the Cisco Wireless LAN Controller (WLC) configuration interface. The 'WIRELESS' tab is selected and circled in red. The 'Rogues' section is also circled in red, showing a list of rogue APs. The table lists AP Name, AP ID, Ethernet MAC, Admin Status, Operational Status, and Port.

AP Name	AP ID	Ethernet MAC	Admin Status	Operational Status	Port
ap:5b:fb:d0	34	00:0b:85:5b:fb:d0	Enable	REG	2
ap:51:5a:e0	35	00:0b:85:51:5a:e0	Enable	REG	2

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

MAC Address	SSID	# Detecting Radios	Number of Clients	Status
00:02:8a:0e:33:f5	Unknown	2	0	Known
00:07:85:92:4d:c9	Unknown	2	0	Known
00:0b:fc:fc:15:00	Unknown	1	0	Known
00:12:01:a1:f5:10	auto-2	2	0	Known

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 الدباجة 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 التمهيدي 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)

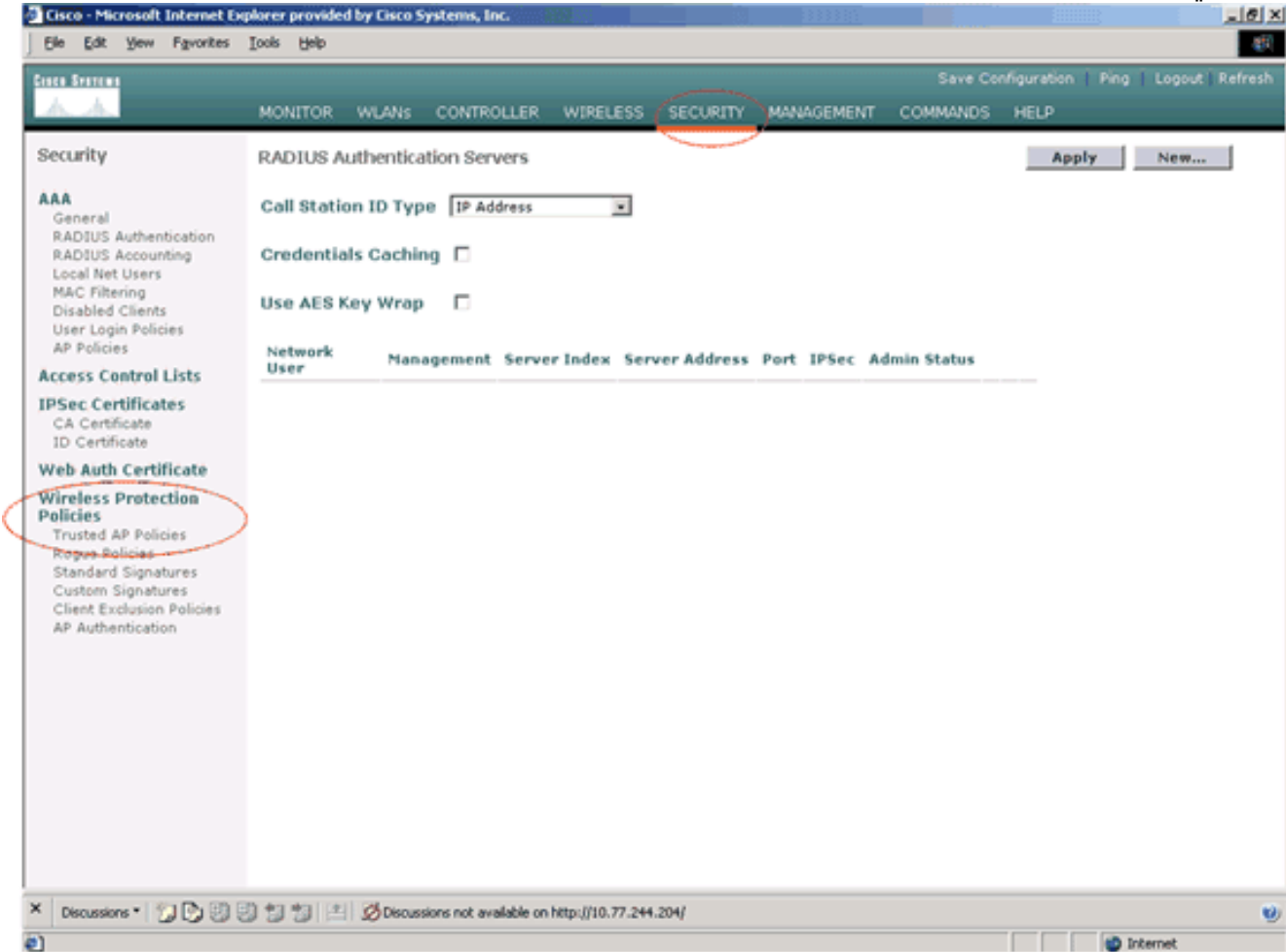
تحدد قيمة مهلة انتهاء الصلاحية هذه عدد الثواني قبل اعتبار نقطة الوصول الموثوق بها منتهية الصلاحية ومسحوبة من إدخال عنصر التحكم في الشبكة المحلية اللاسلكية (WLC). يمكنك تحديد قيمة المهلة هذه بالثواني (120 - 3600 ثانية).

كيف أن بشكل AP سياسة على ال WLC؟

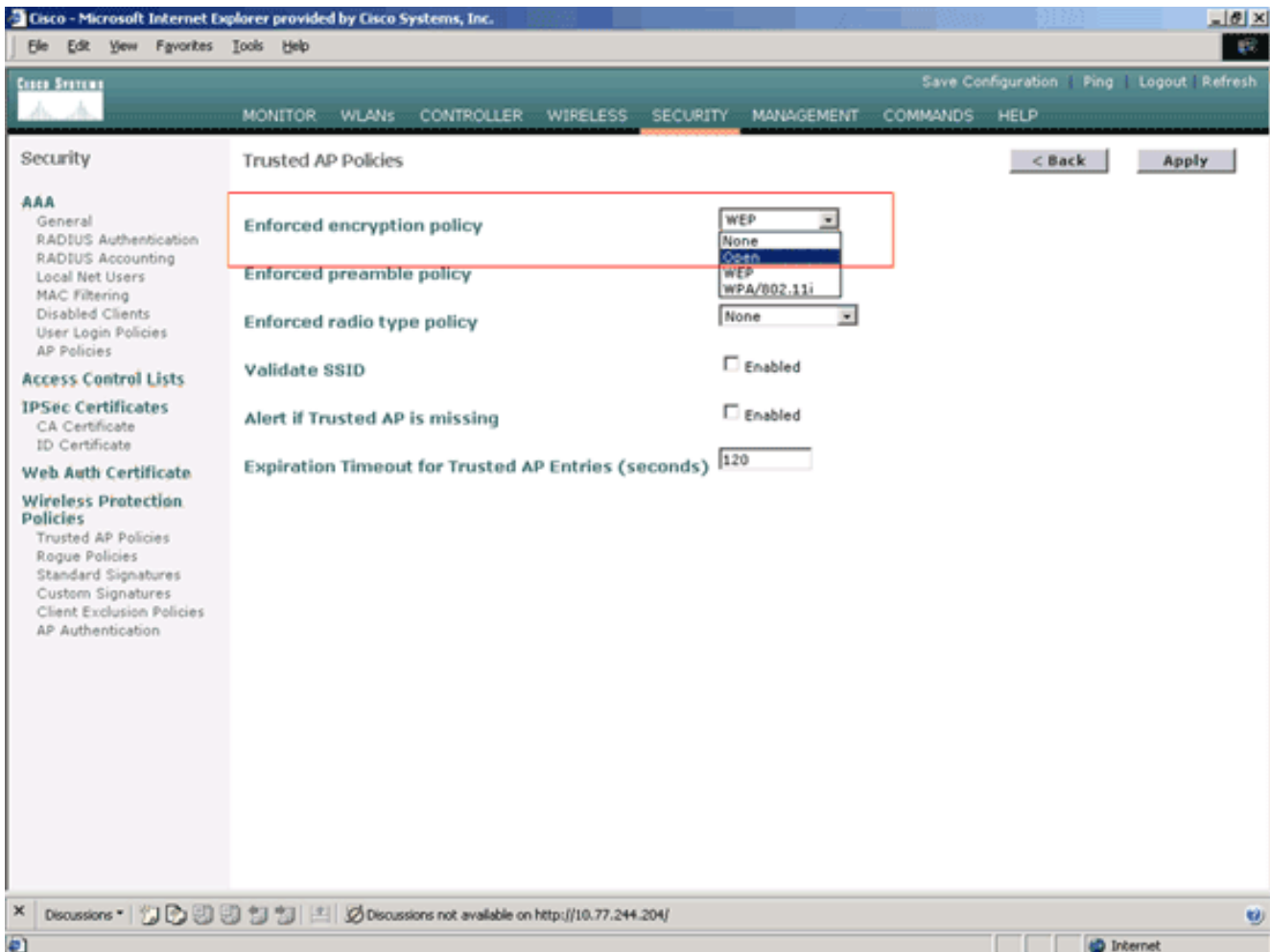
أتمت هذا steps in order to شكلت Trusted AP سياسة على ال WLC من خلال ال gui:

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

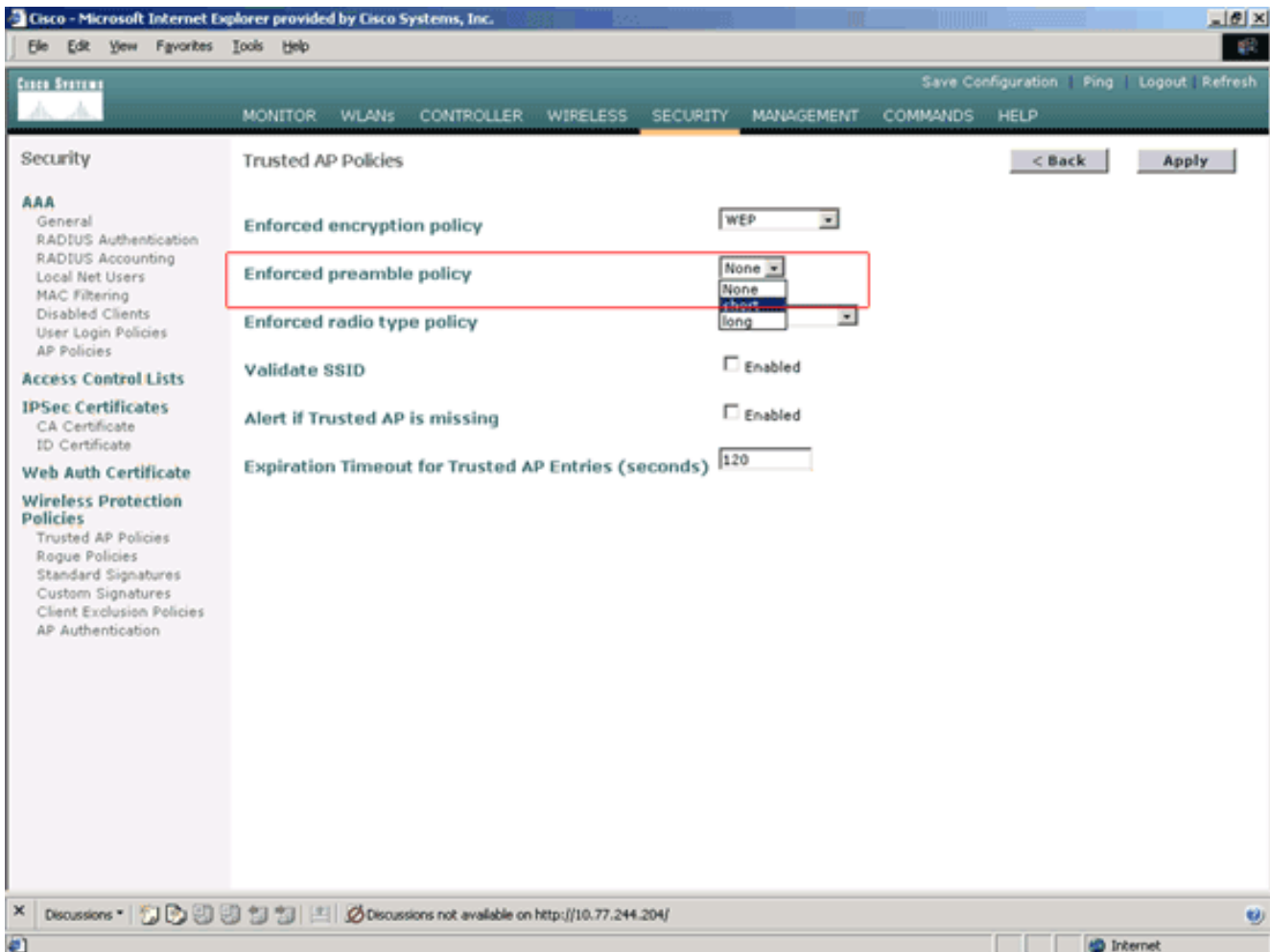
1. من القائمة الرئيسية لواجهة المستخدم الرسومية (GUI) الخاصة بوحدة التحكم في الشبكة المحلية اللاسلكية (WLC)، انقر فوق الأمان.
2. من القائمة الموجودة على الجانب الأيسر من صفحة الأمان، انقر على سياسات نقطة الوصول الموثوق بها المدرجة تحت عنوان نهج الحماية اللاسلكية.



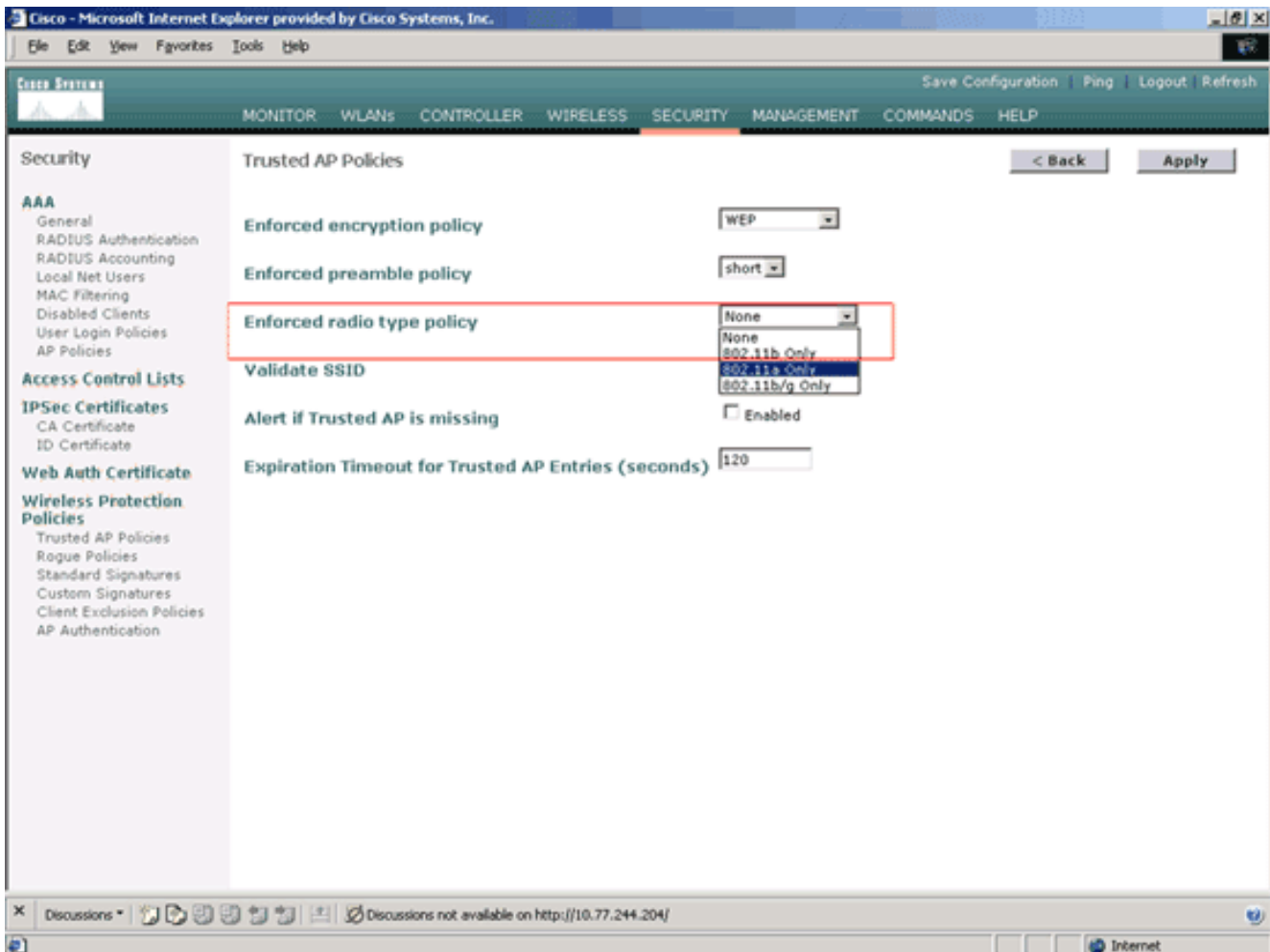
3. في صفحة سياسات نقطة الوصول الموثوق بها، حدد نوع التشفير المرغوب (None و Open و WEP و WPA/802.11i) من القائمة المنسدلة لنهج التشفير القسري.



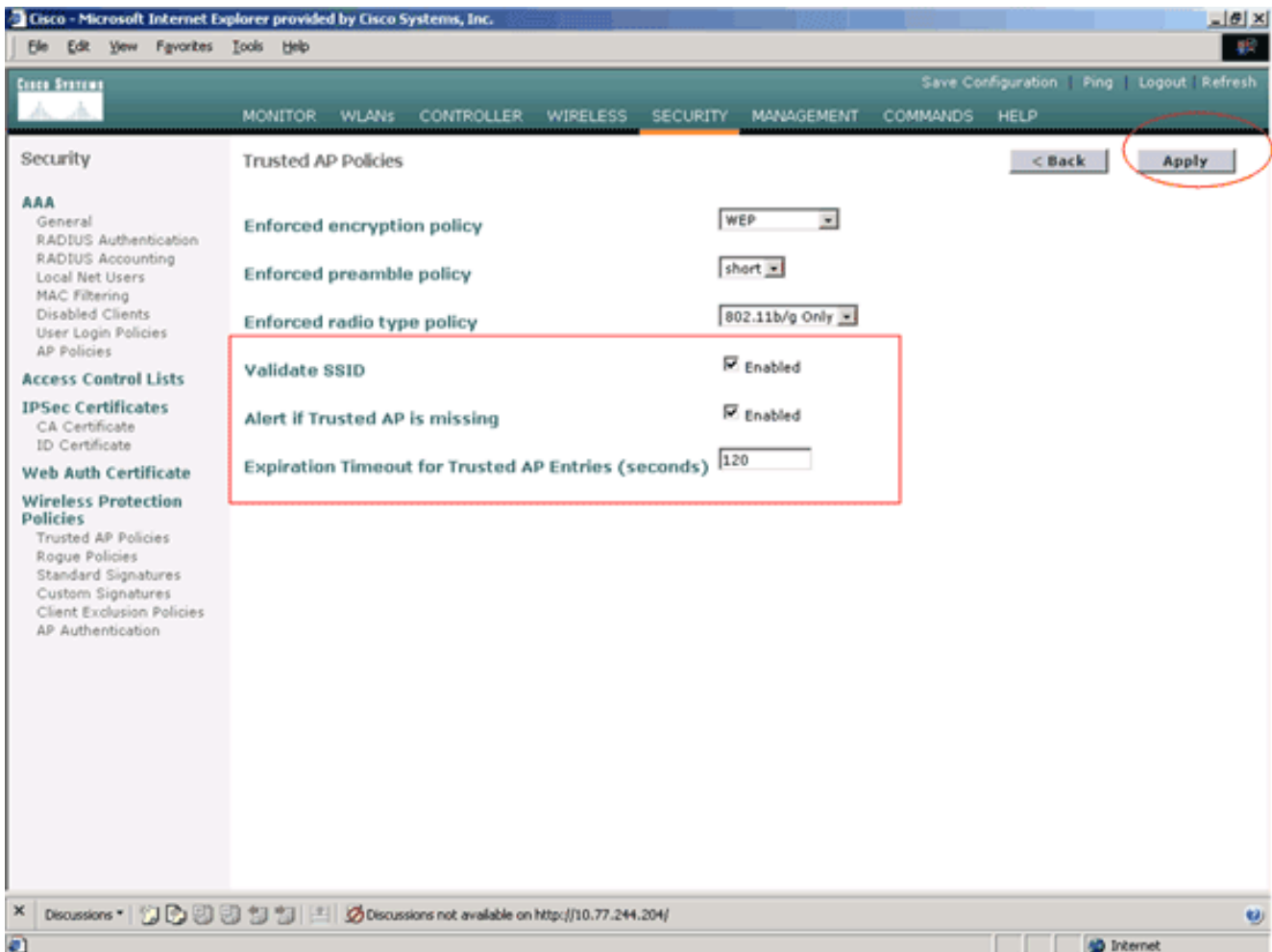
4. حدد نوع التمهيد المطلوب (بلا، قصير، طويل) من القائمة المنسدلة لنهج نوع التمهيد الذي تم فرضه.



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



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 استخدام 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 الأحداث من صفحة المراقبة، انقر فوق عرض الكل لعرض جميع التنبيهات الأخيرة على عنصر التحكم في الشبكة المحلية اللاسلكية (WLC).

The screenshot shows the Cisco WLC GUI in Internet Explorer. The 'MONITOR' tab is highlighted in the top navigation bar. The main content area is divided into several sections:

- Controller Summary:**

Management IP Address	10.77.244.204
Service Port IP Address	0.0.0.0
Software Version	3.2.150.10
System Name	WLC-4400-TSWEB
Up Time	16 days, 8 hours, 42 minutes
System Time	Wed Dec 12 12:40:03 2007
Internal Temperature	+38 C
802.11a Network State	Enabled
802.11b/g Network State	Enabled
- Access Point Summary:**

	Total	Up	Down	
802.11a Radios	2	2	0	Detail
802.11b/g Radios	2	2	0	Detail
All APs	2	2	0	Detail
- Client Summary:**

Current Clients	6	Detail
Excluded Clients	0	Detail
Disabled Clients	0	Detail
- Most Recent Traps:**
 - Rogue AP : 00:13:19:49:08:70 detected on Base Radio
 - Rogue AP : 00:13:19:49:08:70 detected on Base Radio
 - Rogue AP : 00:11:21:b4:ff:00 detected on Base Radio f
 - Trusted AP 00:07:85:92:4d:c9 has invalid radio policy. I
 - Trusted AP 00:07:85:92:4d:c9 has invalid encryption co

[View All](#)

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:

Cisco - Microsoft Internet Explorer provided by Cisco Systems, Inc.

File Edit View Favorites Tools Help

Cisco Systems Save Configuration Ping Logout Refresh

MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP

Monitor

Summary

Statistics
Controller
Ports

Wireless
Rogue APs
Known Rogue APs
Rogue Clients
Adhoc Rogues
802.11a Radios
802.11b/g Radios
Clients
RADIUS Servers

Trap Logs Clear Log

Log	System Time	Trap
0	Wed Dec 12 12:40:32 2007	Rogue : 00:0f:f0:50:a0:5c removed from Base Radio MAC : 00:0b:85:5b:fb:d0 Interface no:1(802.11b/g)
1	Wed Dec 12 12:40:32 2007	Rogue : 00:13:19:ab:99:00 removed from Base Radio MAC : 00:0b:85:5b:fb:d0 Interface no:1(802.11b/g)
2	Wed Dec 12 12:40:32 2007	Rogue : 00:13:19:ab:99:00 removed from Base Radio MAC : 00:0b:85:51:5ae0 Interface no:1(802.11b/g)
3	Wed Dec 12 12:39:31 2007	Rogue AP : 00:13:19:49:08:70 detected on Base Radio MAC : 00:0b:85:51:5ae0 Interface no:1(802.11b/g) with RSSI: -47 and SNR: 48
4	Wed Dec 12 12:39:31 2007	Rogue AP : 00:13:19:49:08:70 detected on Base Radio MAC : 00:0b:85:5b:fb:d0 Interface no:1(802.11b/g) with RSSI: -55 and SNR: 44
5	Wed Dec 12 12:39:31 2007	Rogue AP : 00:11:21:b4:ff:00 detected on Base Radio MAC : 00:0b:85:5b:fb:d0 Interface no:1(802.11b/g) with RSSI: -95 and SNR: 4
6	Wed Dec 12 12:39:29 2007	Trusted AP 00:07:85:92:4d:c9 has invalid radio policy. It's using 802.11a instead of 802.11b/g
7	Wed Dec 12 12:39:29 2007	Trusted AP 00:07:85:92:4d:c9 has invalid encryption configuration. It's using Open instead of WEP
8	Wed Dec 12 12:39:29 2007	Trusted AP 00:02:8a:0e:33:f5 has invalid radio policy. It's using 802.11a instead of 802.11b/g
9	Wed Dec 12 12:39:29 2007	Trusted AP 00:02:8a:0e:33:f5 has invalid encryption configuration. It's using Open instead of WEP
10	Wed Dec 12 12:39:29 2007	Trusted AP 00:12:01:a1:f5:10 is advertising an invalid SSID.
11	Wed Dec 12 12:38:12 2007	Rogue : 00:11:5e:93:d3:00 removed from Base Radio MAC : 00:0b:85:51:5ae0 Interface no:1(802.11b/g)
12	Wed Dec 12 12:38:10 2007	Rogue : 00:14:f1:ae:9d:70 removed from Base Radio MAC : 00:0b:85:51:5ae0 Interface no:1(802.11b/g)
13	Wed Dec 12 12:38:10 2007	Rogue : 00:07:50:d5:cf:b9 removed from Base Radio MAC : 00:0b:85:51:5ae0 Interface no:1(802.11b/g)
14	Wed Dec 12 12:38:10 2007	Rogue : 00:19:a9:41:12:b4 removed from Base Radio MAC : 00:0b:85:51:5ae0 Interface no:1(802.11b/g)
15	Wed Dec 12 12:37:32 2007	Rogue : 00:14:1b:b6:23:60 removed from Base Radio MAC : 00:0b:85:5b:fb:d0 Interface no:1(802.11b/g)
16	Wed Dec 12 12:37:18 2007	Rogue AP : 00:12:d9:e2:b9:20 detected on Base Radio MAC : 00:0b:85:51:5ae0 Interface no:0(802.11a) with RSSI: -83 and SNR: 8

Discussions Discussions not available on http://10.77.244.204/

Done Internet

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

ةمچرتل هذه لوج

ةللأل تاي نقتل نمة ومة مادختساب دن تسمل اذة Cisco تمةرت
ملاعلاء انء مء مء نمة دختسمل معد و تمة مء دقتل ةر شبل او
امك ةق قء نوك ت نل ةللأل ةمچرت لصف أن ةظحال مء ءرء. ةصاأل مء تءل ب
Cisco ةلخت. فرتمة مچرت مء دقء ةل ةل ةفارتحال ةمچرتل عم لالحل وه
ىل إأمءءاد ءوچرلاب ةصوء و تامةرتل هذه ةقء نء اهءل وئس م Cisco
Systems (رفوتم طبارل) ةلصلأل ةزىل ءن إل دن تسمل