無線LAN控制器上的受信任AP策略

目錄

[簡介](#)
[必要條件](#)
[需求](#)
[慣例](#)
[受信任的AP策略](#)
[什麼是受信任的AP?](#)
[如何從WLC GUI將AP配置為受信任AP?](#)
[瞭解受信任的AP策略設定](#)
[如何在WLC上配置受信任的AP策略？](#)
[受信任AP策略違規警報消息](#)
[相關資訊](#)

簡介

本檔案介紹無線LAN控制器(WLC)上的*受信AP*無線保護策略，定義受信AP策略，並提供所有受信AP策略的簡短說明。

必要條件

需求

確保您已基本瞭解無線LAN安全引數（例如SSID、加密、身份驗證等）。

慣例

如需文件慣例的詳細資訊，請參閱思科技術提示慣例。

受信任的AP策略

受信任AP策略是控制器中的一項安全功能，旨在用於客戶與控制器具有並行自主AP網路的方案。在這種情況下，自治AP可以在控制器上標籤為可信AP，並且使用者可以定義這些可信AP的策略（這些策略應僅使用WEP或WPA、我們自己的SSID、短前導碼等）。 如果其中任何AP無法滿足這些策略，控制器會向網路管理裝置（無線控制系統）發出警報，指出受信任的AP違反了配置的策略。

什麼是受信任的AP?

受信任的AP是不屬於組織的AP。但是，它們不會對網路造成安全威脅。這些AP也稱為友好AP。存

在多種情況，您可能希望將AP配置為受信任AP。

例如，您的網路中可能有不同類別的AP，例如：

- **您擁有的不運行LWAPP的AP（可能運行IOS或VxWorks）**
- 員工引入的LWAPP AP（在管理員知情的情況下）
- 用於測試現有網路的LWAPP AP
- 鄰居擁有的LWAPP AP

通常，受信任的AP是屬於**類別1**的AP，它們是您擁有的不運行LWAPP的AP。它們可能是運行VxWorks或IOS的舊AP。為了確保這些AP不會損壞網路，可以實施某些功能，如正確的SSID和身份驗證型別。在WLC上配置受信任AP策略，並確保受信任AP符合這些策略。如果沒有，可以將控制器配置為採取多種措施，例如向網路管理裝置(WCS)發出警報。

屬於鄰居的已知AP可以配置為受信任AP。

通常，MFP（管理幀保護）應阻止非合法LWAPP AP加入WLC。如果NIC卡支援MFP，則不允許它們接受來自實際AP以外的裝置的取消身份驗證。有關MFP的詳細資訊，請參閱具有WLC和LAP的基礎設施管理幀保護(MFP)配置示例。

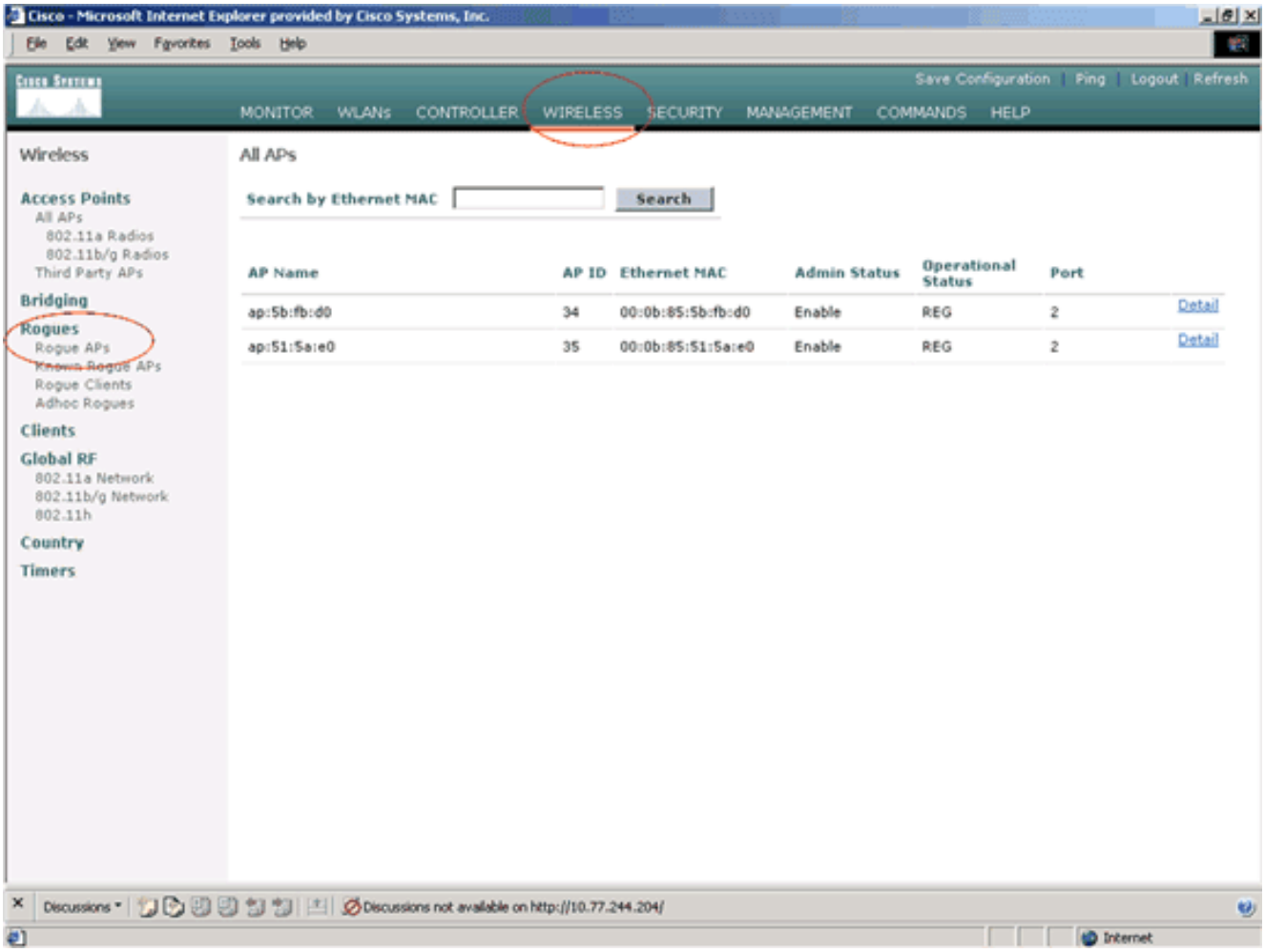
如果您有運行VxWorks或IOS的AP（如類別1），它們永遠不會加入LWAPP組或執行MFP，但您可能要強制實施該頁面上列出的策略。在這種情況下，需要在控制器上為感興趣的AP配置受信任的AP策略。

一般來說，如果您知道某個惡意AP並發現它不會對您的網路構成威脅，您可以將該接入點識別為已知的受信任AP。

如何從WLC GUI將AP配置為受信任AP?

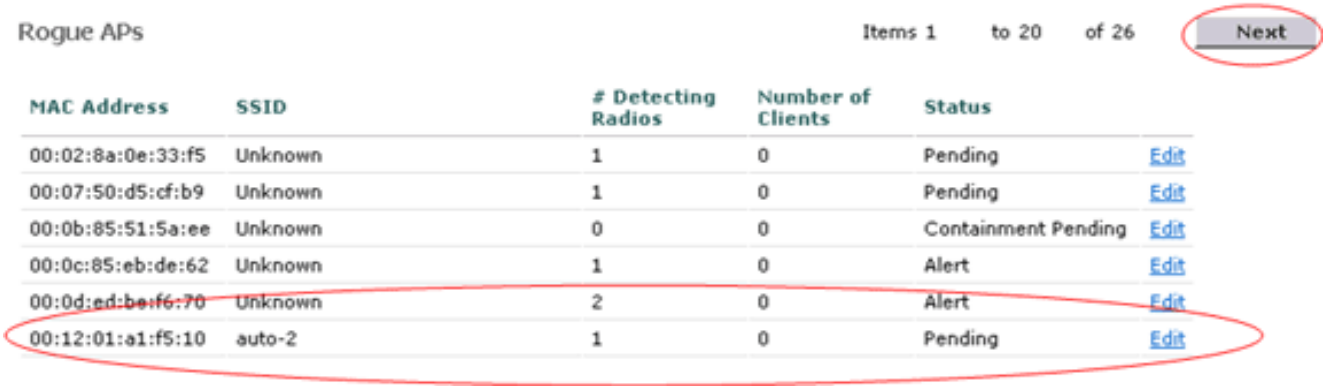
完成以下步驟，將AP配置為受信任AP:

1. 透過HTTP或https登入登入WLC的GUI。
2. 在控制器主選單中，按一下**Wireless**。
3. 在Wireless（無線）頁面左側的選單中，按一下**Rogue APs**。



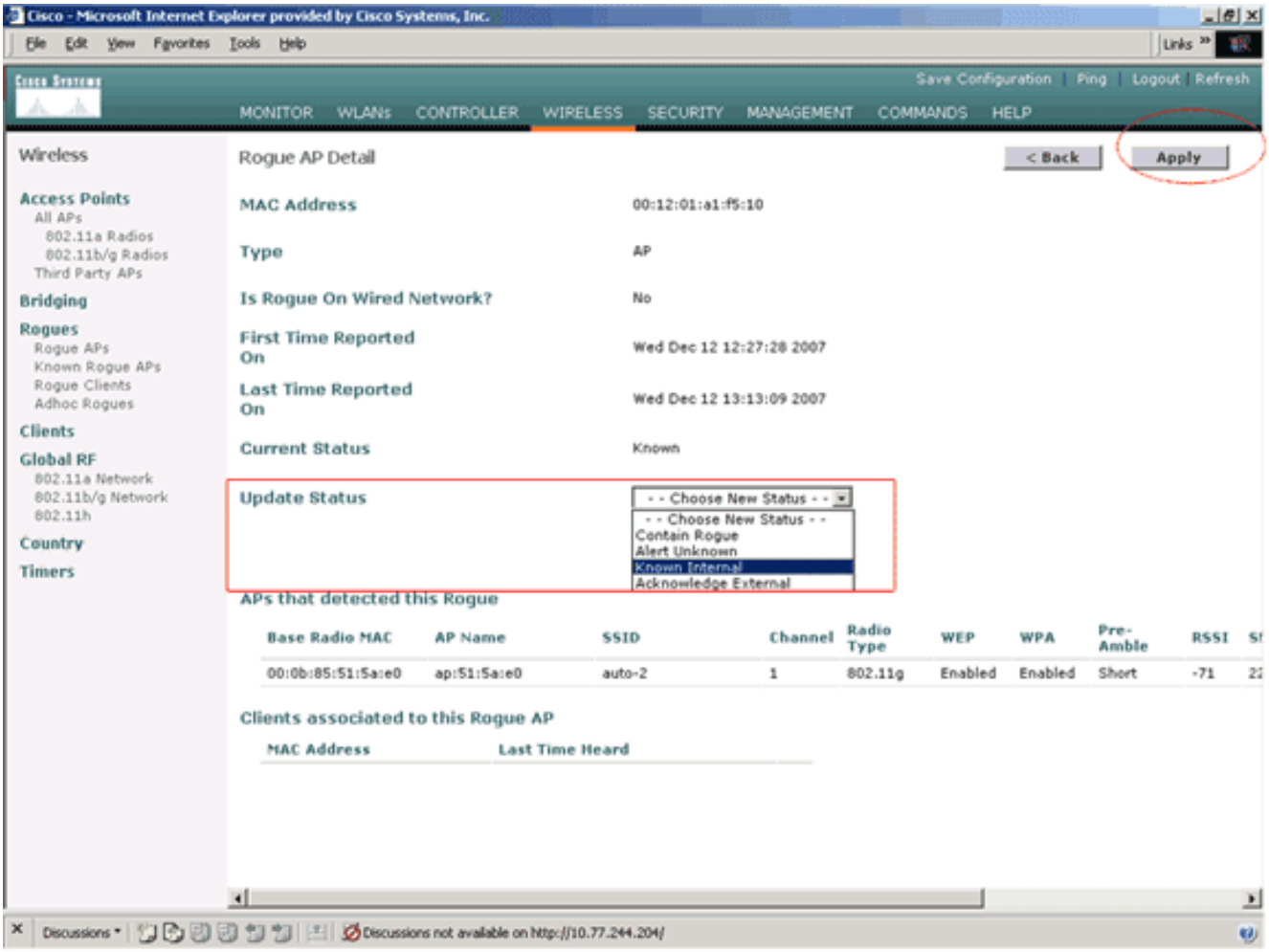
Rogue APs頁面列出了網路中檢測到作為欺詐AP的所有接入點。

4. 從非法AP清單中，找到要配置為屬於類別1的受信任AP的AP（如上一節所述）。您可以查詢Rogue AP頁上列出了MAC地址的AP。如果所需AP未在此頁面中，請按一下**下一步**以從下一頁面識別該AP。
5. 從Rogue AP清單中找到所需的AP後，點選與AP對應的**Edit**按鈕，該按鈕將引導您進入AP的詳細資訊頁面。



在Rogue AP details（無管理AP詳細資訊）頁面中，可以找到有關此AP的詳細資訊（例如AP是否連線到有線網路，以及AP的當前狀態等）。

6. 若要將此AP配置為受信任AP，請從Update Status下拉選單中選擇**Known Internal**，然後按一下**Apply**。將AP狀態更新為*Known Internal*時，此AP被配置為此網路的受信任AP。

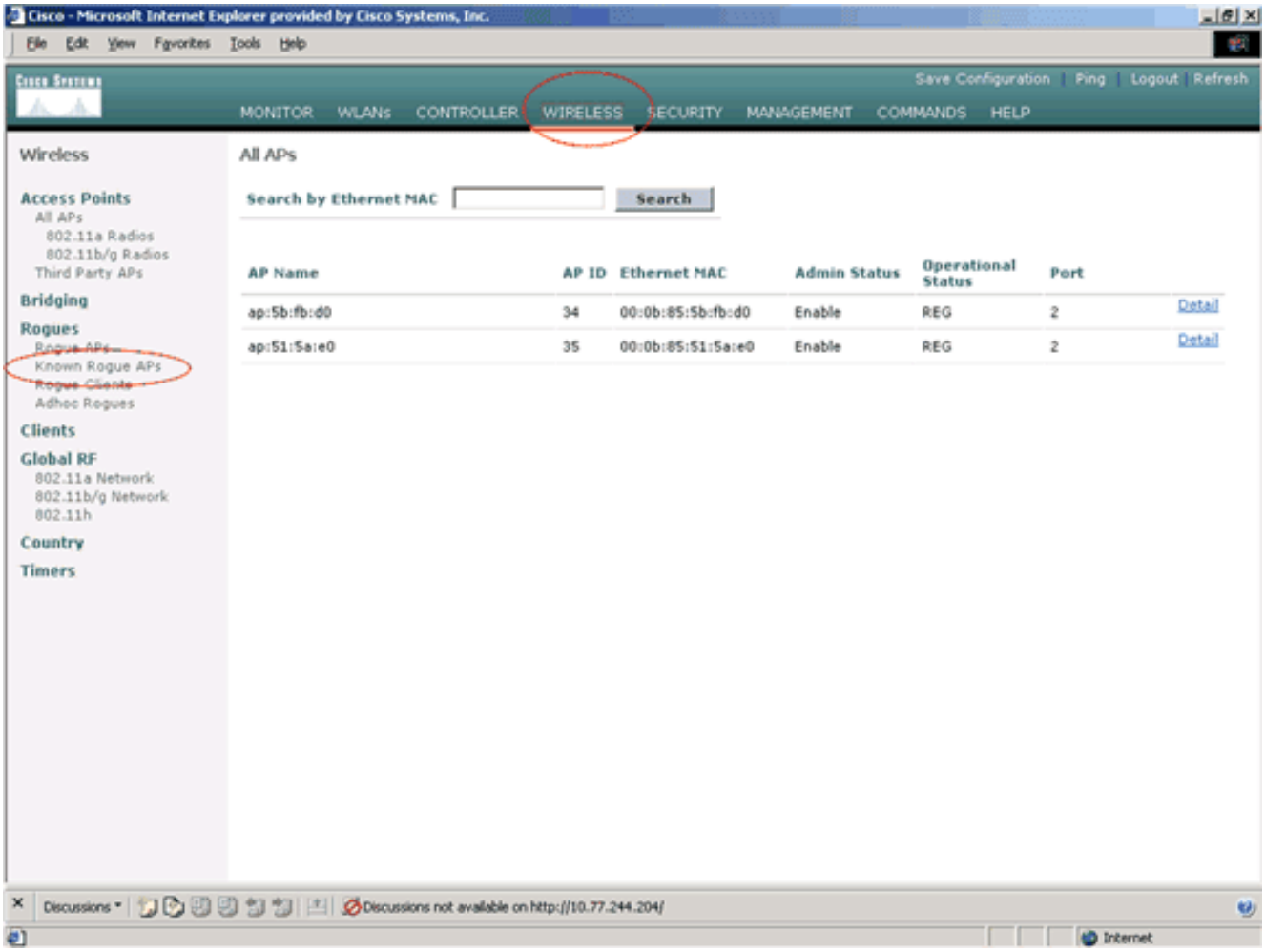


7. 對要配置為受信任AP的所有AP重複這些步驟。

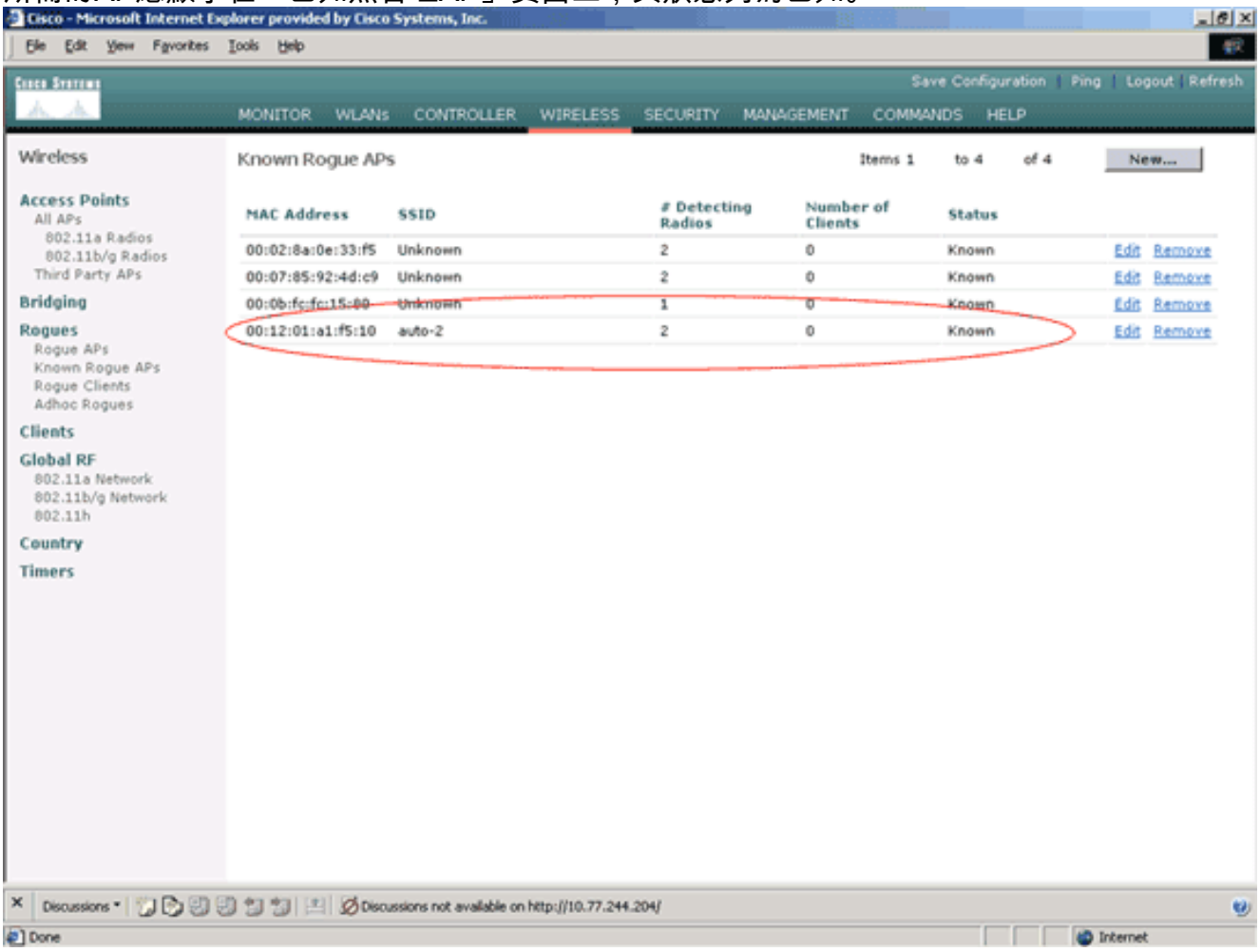
驗證受信任的AP配置

完成以下步驟，從控制器GUI驗證AP是否正確配置為受信任AP:

1. 按一下「**Wireless**」。
2. 在Wireless（無線）頁面左側的選單中，按一下**Known Rogue APs**。



所需的AP應顯示在「已知無管理AP」頁面上，其狀態列為*已知*。



瞭解受信任的AP策略設定

WLC具有以下受信任的AP策略：

- 強制加密策略
- 強制前導碼策略
- 實施的無線電型別策略
- 驗證SSID
- 缺少受信任的AP時發出警報
- 受信任AP條目的過期超時（秒）

強制加密策略

此策略用於定義受信任AP應使用的加密型別。您可以在Enforced encryption policy下配置以下任何加密型別：

- 無
- 未解決
- WEP
- WPA/802.11i

WLC驗證受信任AP上配置的加密型別是否與「強制加密策略」設定中配置**的加密類**型匹配。如果受信任的AP不使用指定的加密型別，WLC會向管理系統發出警報，以便採取適當的措施。

強制前導碼策略

無線電報頭（有時稱為報頭）是資料包頭部的資料部分，包含無線裝置傳送和接收資料包時所需的資訊。**短前導**碼可提高吞吐量效能，因此預設情況下啟用短前導碼。但是，某些無線裝置（例如SpectraLink NetLink電話）需要長**的前**導符。您可以在Enforced preamble（實施前導碼）策略下配置以下任何前導碼選項：

- 無
- 短
- 長

WLC驗證受信任AP上配置的前導碼型別是否與「強制的前導碼策略」設定**上配置的前**導碼型別。如果受信任的AP不使用指定的報頭型別，WLC會向管理系統發出警報，以便採取適當的措施。

實施的無線電型別策略

此策略用於定義受信任AP應使用的無線電型別。您可以在Enforced radio type policy下配置以下任何無線電型別：

- 無
- 僅802.11b
- 僅802.11a
- 僅802.11b/g

WLC驗證受信任AP上配置的無線電型別是否與「強制無線電型別策略」設定**上配置的無線電類**型匹配。如果受信任的AP不使用指定的無線電，WLC會向管理系統發出警報，以便採取適當的措施。

驗證SSID

您可以配置控制器，以根據控制器上配置的SSID驗證受信任的AP SSID。如果受信任的AP SSID與控制器SSID之一匹配，控制器將發出警報。

缺少受信任的AP時發出警報

如果啟用此策略，則如果已知無管理AP清單中缺少受信任AP，則WLC會向管理系統發出警報。

受信任AP條目的過期超時（秒）

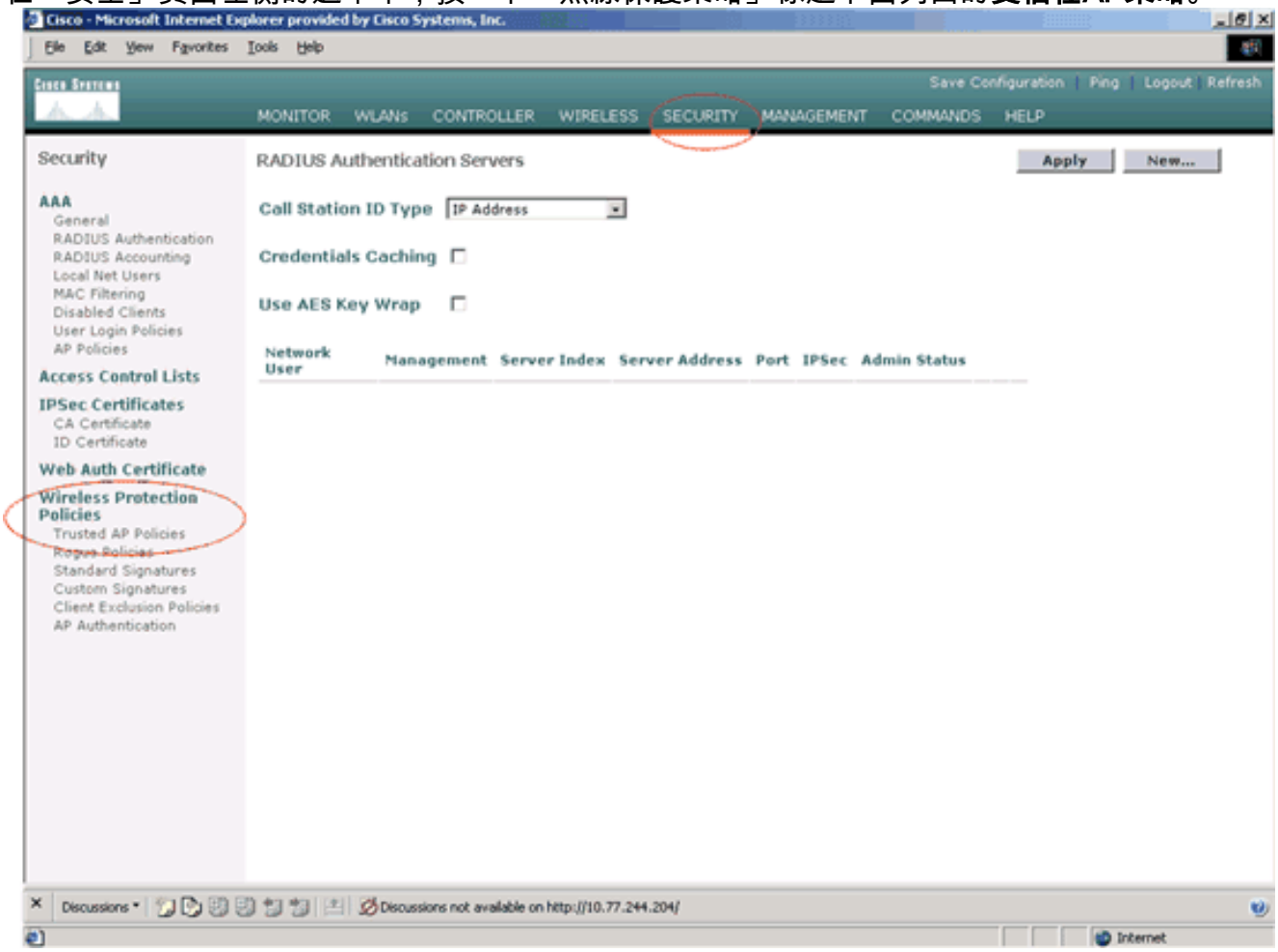
此Expiration Timeout值指定受信任AP被視為已過期並從WLC條目中刷新之前的秒數。可以指定此超時值（秒）（120 - 3600秒）。

如何在WLC上配置受信任的AP策略？

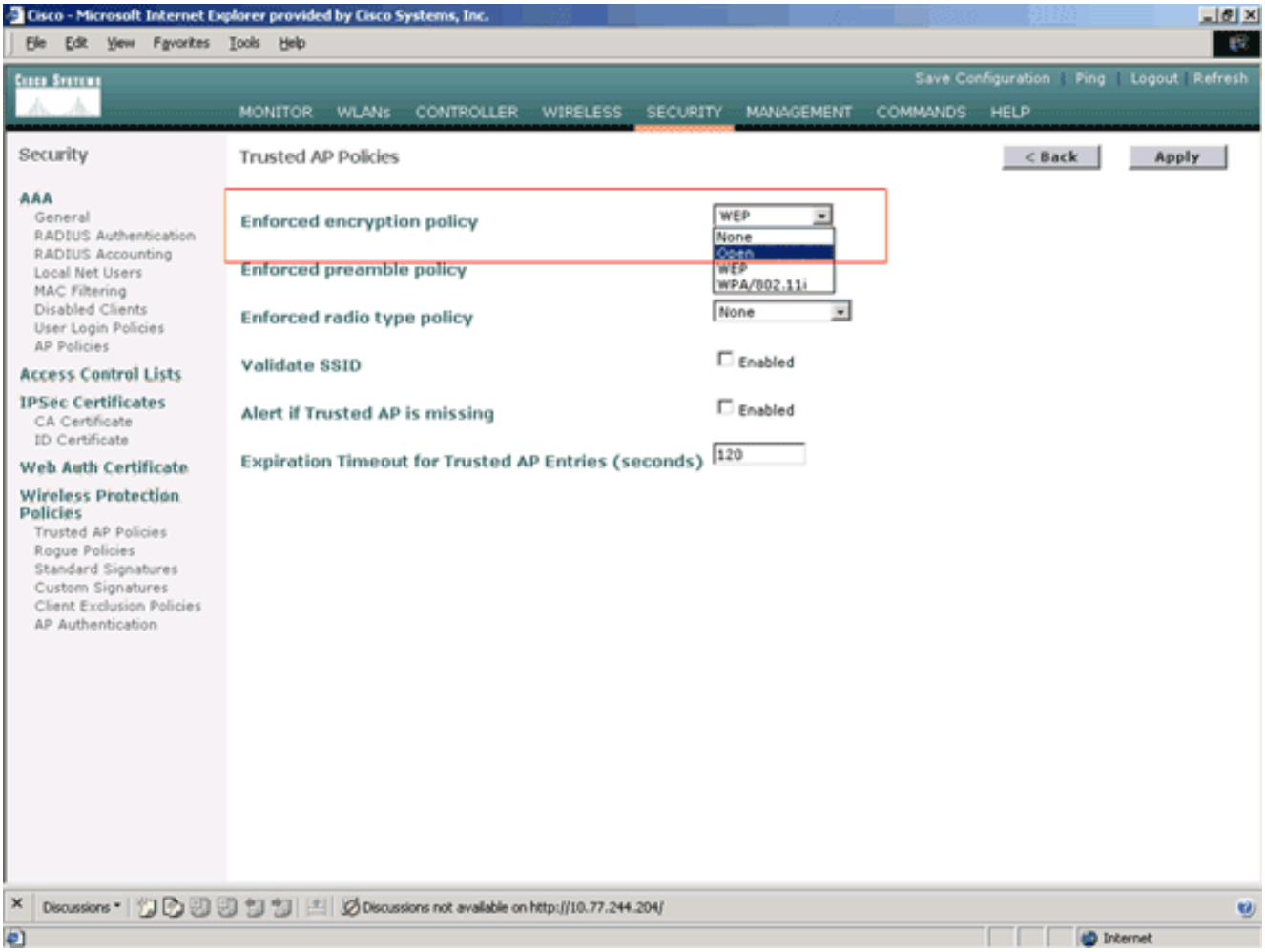
完成以下步驟，以便透過GUI在WLC上設定受信任AP原則：

注意：所有受信任的AP策略都位於同一WLC頁面上。

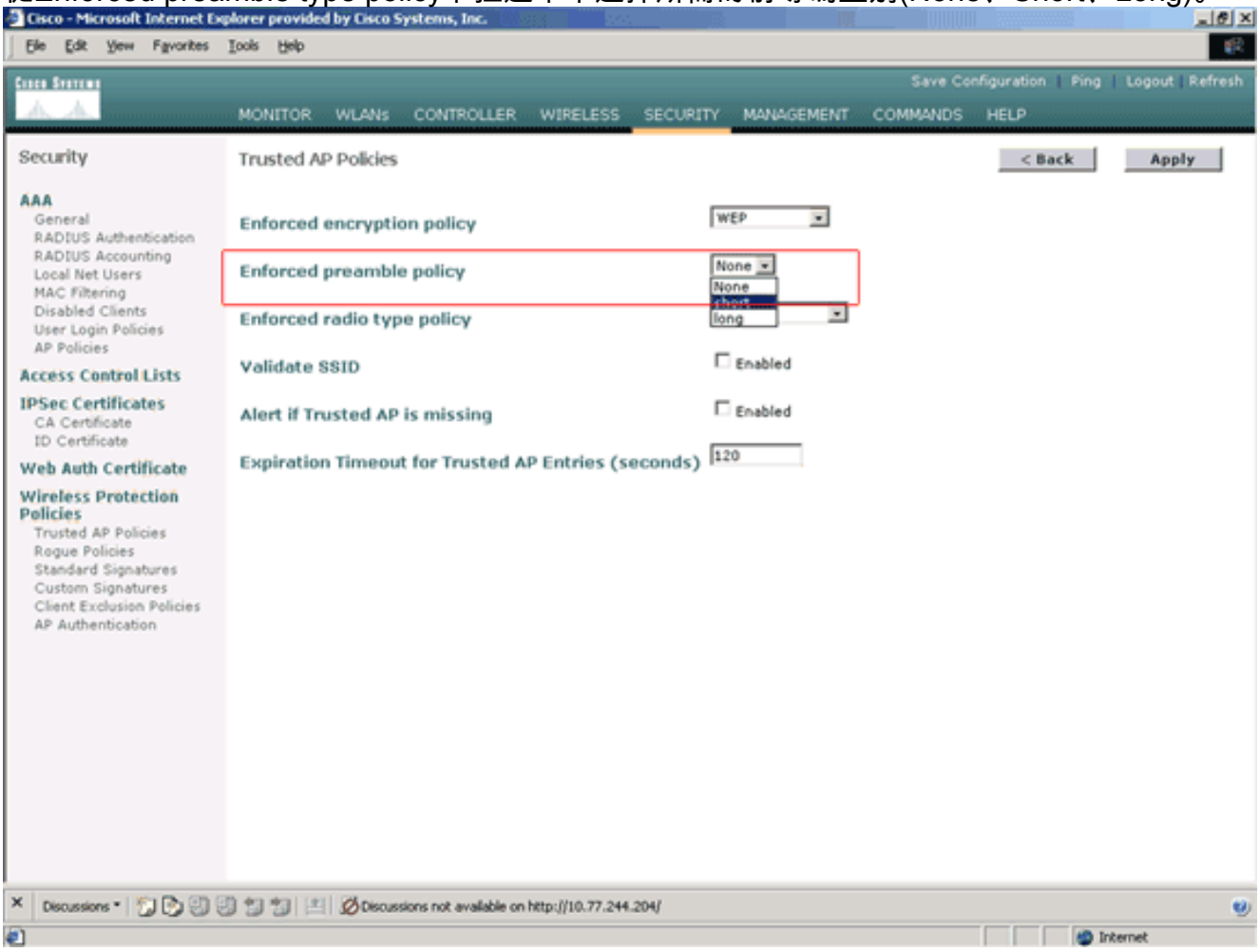
1. 在WLC GUI主功能表中，按一下「**Security**」。
2. 在「安全」頁面左側的選單中，按一下「無線保護策略」標題下面列出的**受信任AP策略**。



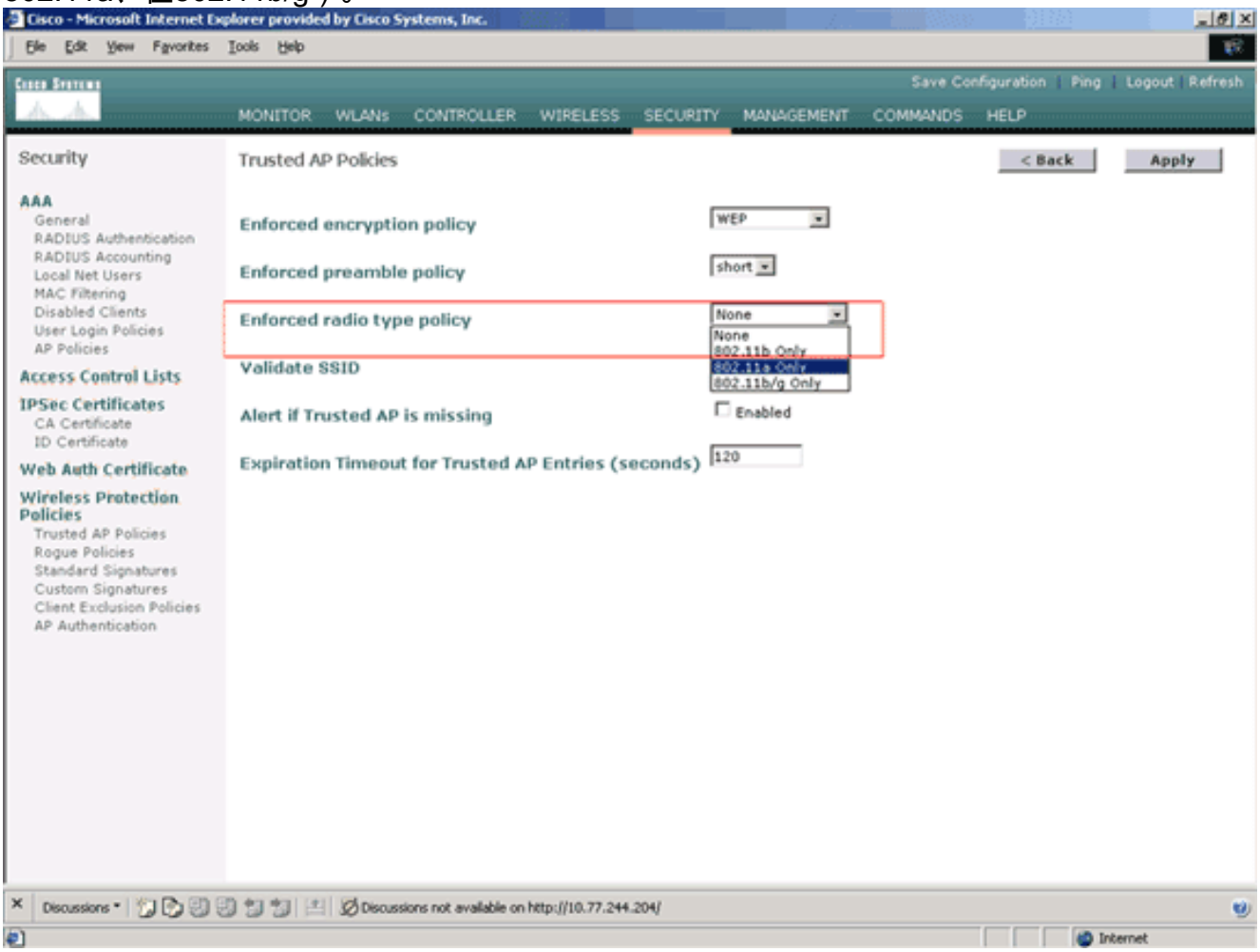
3. 在Trusted AP policies（受信任AP策略）頁上，從Enforced encryption policy（實施加密策略）下拉選單中選擇所需的加密型別(None、Open、WEP、WPA/802.11i)。



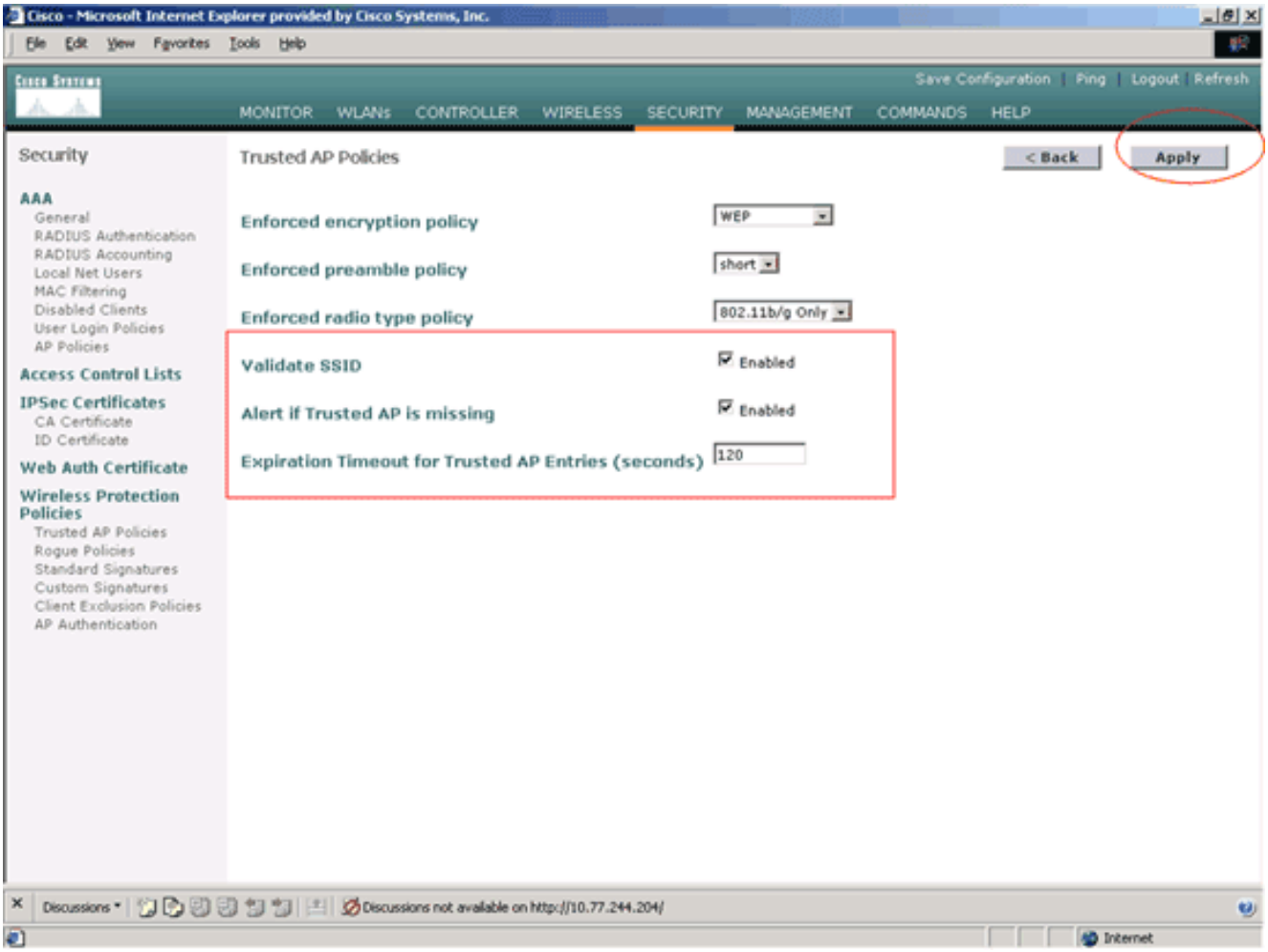
4. 從Enforced preamble type policy下拉選單中選擇所需的前導碼型別(None、Short、Long)。



5. 從Enforced radio type policy下拉選單中選擇所需的無線電型別（無、僅802.11b、僅802.11a、僅802.11b/g）。



6. 選中或取消選中**Validate SSID Enabled**覈取方塊以啟用或禁用Validate SSID設定。
7. 選中或取消選中**Alert if trusted AP is missing Enabled**覈取方塊，以啟用或禁用Alert if trusted AP is missing設定。
8. 為**Expiration Timeout for Trusted AP entries**選項輸入**一個值(以秒為單位)**。



9. 按一下「Apply」。

注意：為了從WLC CLI配置這些設定，您可以使用帶有適當策略選項的**config wps trusted-ap**命令。

```
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.
```

受信任AP策略違規警報消息

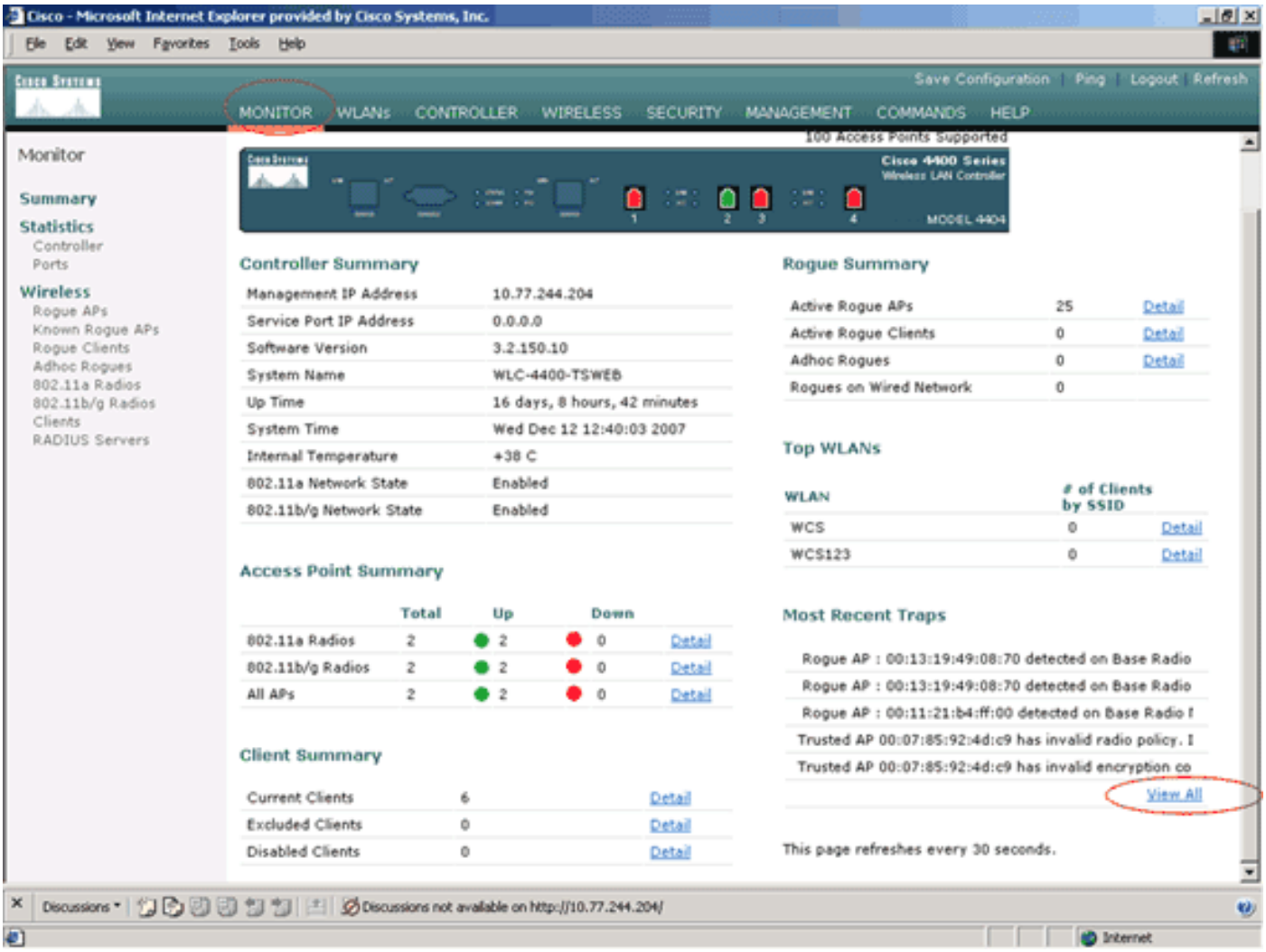
以下是控制器顯示的受信任AP策略違規警報消息的示例。

```
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
```

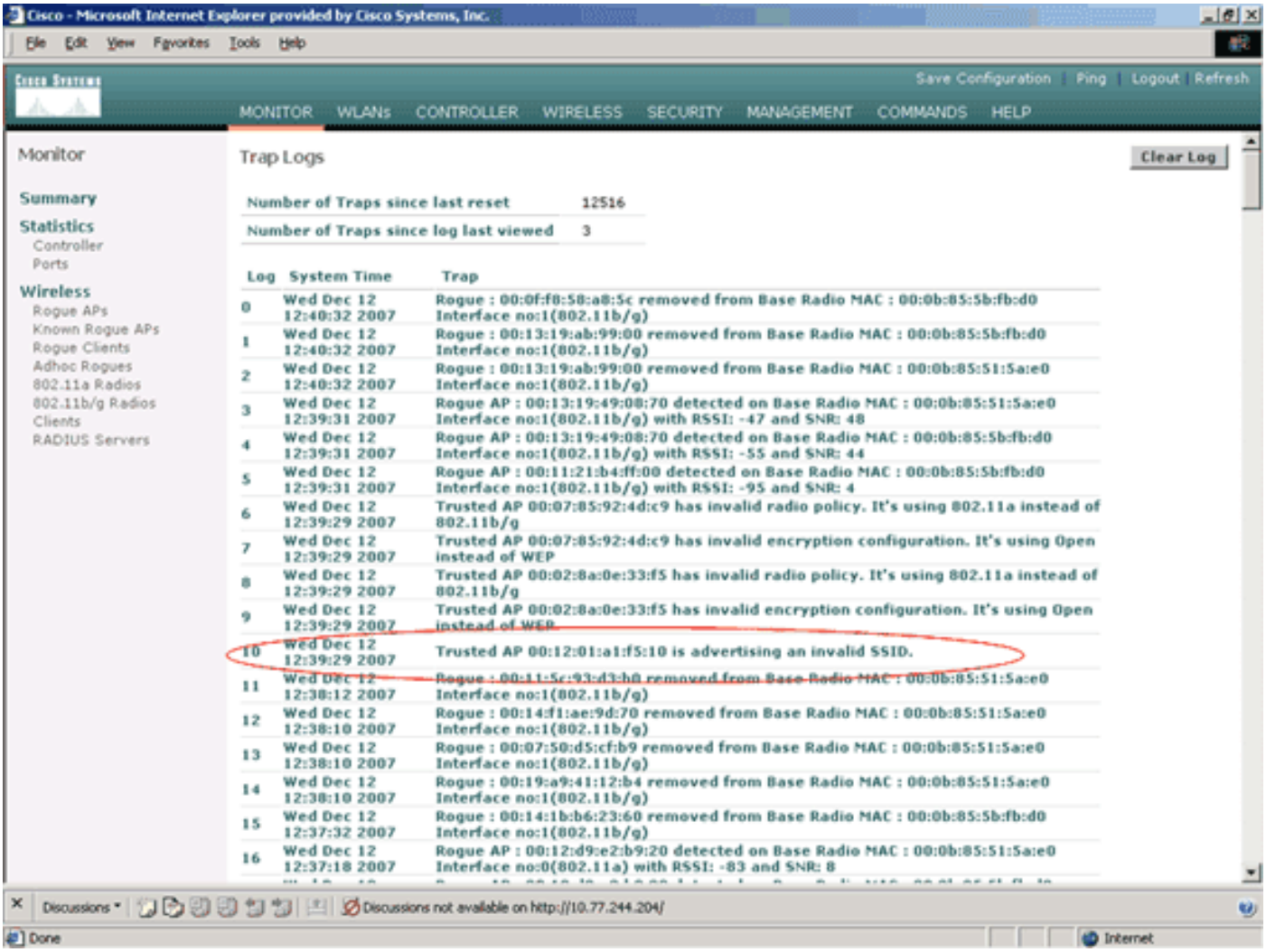
請注意此處突出顯示的錯誤消息。這些錯誤消息表示受信任AP上配置的SSID和加密型別與受信任AP策略設定不匹配。

可從WLC GUI看到相同的警報訊息。若要檢視此訊息，請前往WLC GUI主功能表，然後按一下「Monitor」。在「監視器」頁的「最新陷阱」部分中，按一下**檢視全部**以檢視WLC上的所有最新警報

。



在「最新陷阱」頁面上，您可以標識生成受信任AP策略違規警報消息的控制器，如下圖所示：



相關資訊

- Cisco無線LAN控制器組態設定指南5.2版 — 在RF組中啟用Rouge存取點偵測
- 思科無線LAN控制器組態設定指南4.0版 — 設定安全解決方案
- 統一無線網路下的惡意檢測
- SpectraLink電話設計和部署指南
- 基本無線 LAN 連線的組態範例
- 排除無線LAN網路中的連線故障
- 無線LAN控制器上的驗證組態範例
- 技術支援與文件 - Cisco Systems