무선 LAN 컨트롤러의 신뢰할 수 있는 AP 정책

목차

소개

이 문서에서는 *WLC*(Wireless LAN Controller)의 *신뢰할 수 있는 AP* 무선 보호 정책에 대해 설명하고, 신뢰할 수 있는 AP 정책을 정의하며, 모든 신뢰할 수 있는 AP 정책에 대한 간략한 설명을 제공합니다.

사전 요구 사항

요구 사항

무선 LAN 보안 매개변수(예: SSID, 암호화, 인증 등)에 대한 기본적인 이해가 있는지 확인합니다.

표기 규칙

문서 규칙에 대한 자세한 내용은 Cisco 기술 팁 표기 규칙을 참고하십시오.

신뢰할 수 있는 AP 정책

신뢰할 수 있는 AP 정책은 컨트롤러와 함께 병렬 자동 AP 네트워크가 있는 시나리오에서 사용하도록 설계된 컨트롤러의 보안 기능입니다.이 시나리오에서는 자동 AP를 컨트롤러에서 신뢰할 수 있는 AP로 표시할 수 있으며, 사용자는 이러한 신뢰할 수 있는 AP에 대한 정책을 정의할 수 있습니다(WEP 또는 WPA, 자체 SSID, 짧은 프리앰블 등만 사용해야 함). 이러한 AP 중 하나라도 이러한 정책을 충족하지 못하면 컨트롤러는 네트워크 관리 디바이스(Wireless Control System)에 경고를 발생시키고, 이는 신뢰할 수 있는 AP가 구성된 정책을 위반했음을 나타냅니다.

신뢰할 수 있는 AP란?

신뢰할 수 있는 AP는 조직의 일부가 아닌 AP입니다.그러나 네트워크에 보안 위협이 되지 않습니다.이러한 AP는 친화적 AP라고도 합니다.AP를 신뢰할 수 있는 AP로 구성할 수 있는 몇 가지 시나리오가 있습니다.

예를 들어, 네트워크에 다음과 같은 여러 카테고리 AP가 있을 수 있습니다.

- **LWAPP를 실행하지 않는 AP(IOS 또는 VxWorks 실행)**
- 직원이 가져오는 LWAPP AP(관리자 지식 포함)
- 기존 네트워크를 테스트하는 데 사용되는 LWAPP AP
- 인접 디바이스가 소유한 LWAPP AP

일반적으로 신뢰할 수 있는 AP는 **범주 1**에 속하는 AP이며, LWAPP를 실행하지 않는 AP입니다.VxWorks 또는 IOS를 실행하는 이전 AP일 수 있습니다.이러한 AP가 네트워크를 손상시키지 않도록 올바른 SSID 및 인증 유형과 같은 특정 기능을 적용할 수 있습니다.WLC에서 신뢰할 수 있는 AP 정책을 구성하고 신뢰할 수 있는 AP가 이러한 정책을 충족하는지 확인합니다.그렇지 않은 경우, WCS(네트워크 관리 디바이스)에 경보를 올리는 등의 여러 작업을 수행하도록 컨트롤러를 구성할 수 있습니다.

네이버에 속하는 알려진 AP는 신뢰할 수 있는 AP로 구성할 수 있습니다.

일반적으로 MFP(Management Frame Protection)는 합법적인 LWAPP AP가 아닌 AP가 WLC에 가입하는 것을 방지해야 합니다.NIC 카드가 MFP를 지원하는 경우 실제 AP가 아닌 디바이스에서 인증을 수락할 수 없습니다.MFP에 대한 자세한 내용은 WLC와 LAP 구성의 MFP(Infrastructure Management Frame Protection)를 참조하십시오.

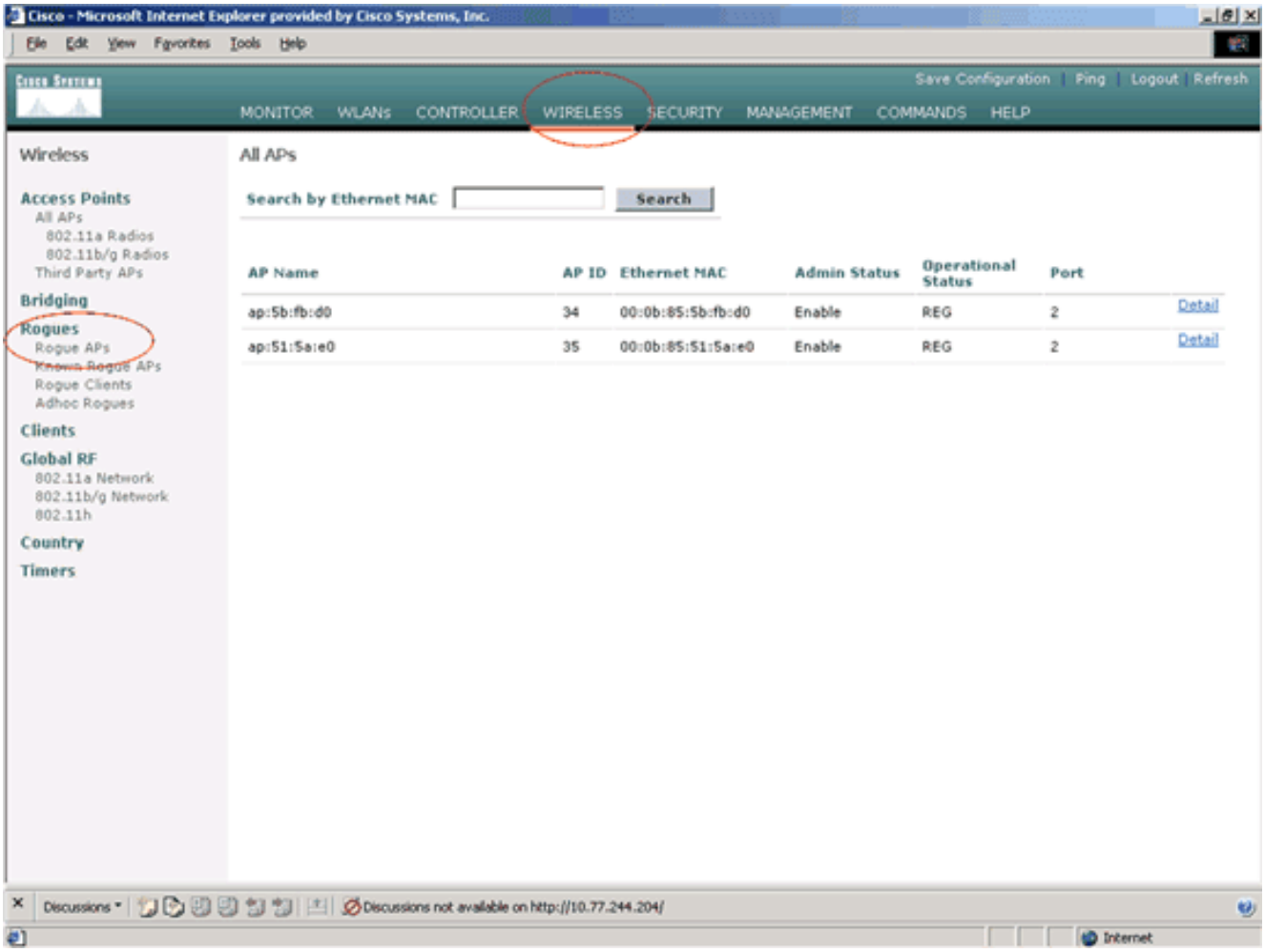
VxWorks 또는 IOS를 실행하는 AP가 있는 경우(범주 1과 같이) AP는 LWAPP 그룹에 가입하거나 MFP를 수행하지 않지만, 해당 페이지에 나열된 정책을 적용할 수 있습니다.이러한 경우, 관심 있는 AP를 위해 컨트롤러에 신뢰할 수 있는 AP 정책을 구성해야 합니다.

일반적으로 비인가 AP에 대해 알고 있고 네트워크에 위협이 되지 않는다고 판단하면 해당 AP를 신뢰할 수 있는 알려진 AP로 식별할 수 있습니다.

WLC GUI에서 AP를 신뢰할 수 있는 AP로 구성하는 방법

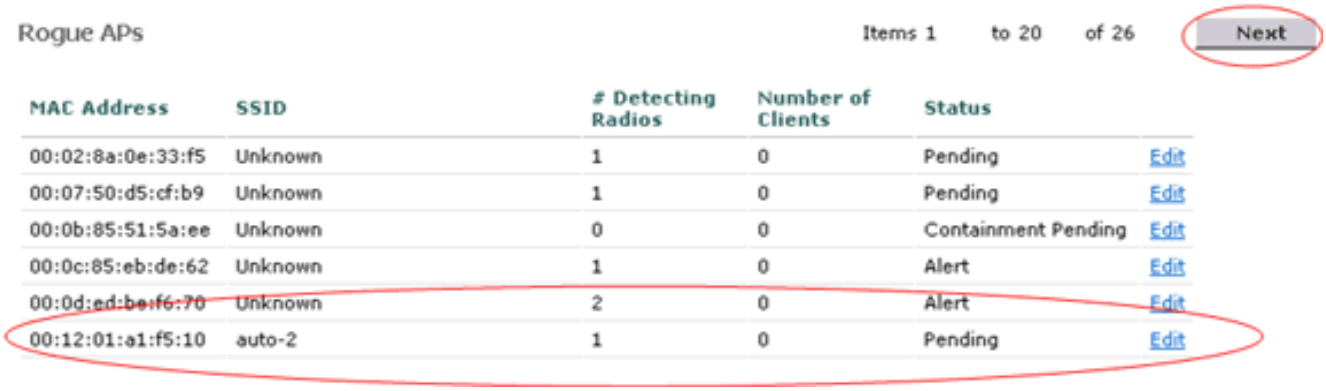
AP를 신뢰할 수 있는 AP로 구성하려면 다음 단계를 완료하십시오.

1. HTTP 또는 https 로그인을 통해 WLC의 GUI에 로그인합니다.
2. 컨트롤러 주 메뉴에서 **무선**을 클릭합니다.
3. Wireless(무선) 페이지의 왼쪽에 있는 메뉴에서 Rogue **APs(비인가 AP)를** 클릭합니다.



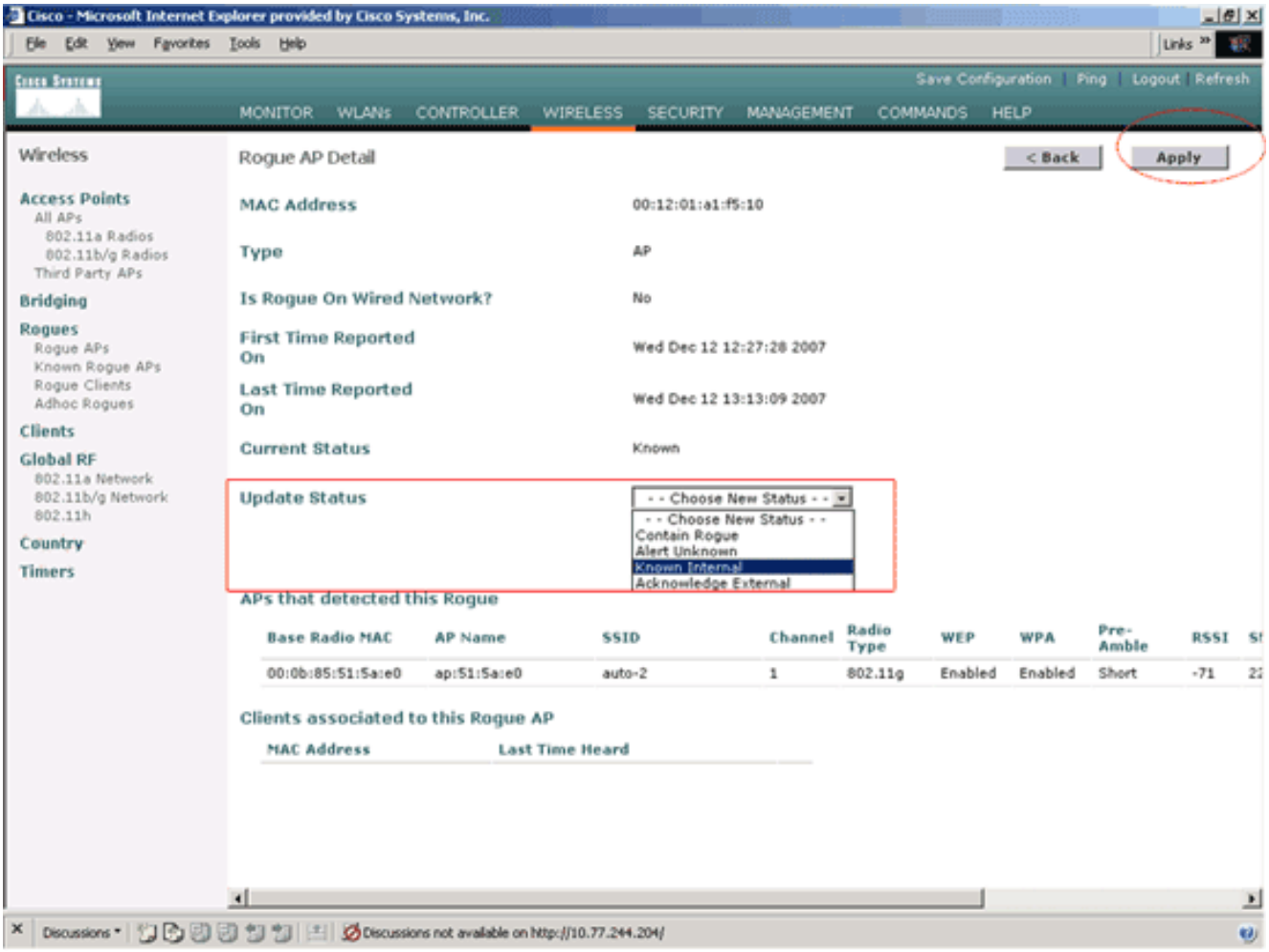
Rogue APs(비인가 AP) 페이지에는 네트워크에서 비인가 AP로 탐지된 모든 AP가 나열됩니다
.

4. 이 비인가 AP 목록에서 카테고리 1에 해당하는 신뢰할 수 있는 AP로 구성하려는 AP를 찾습니다(이전 섹션에서 설명).Rogue APs(비인가 AP) 페이지에 나열된 MAC 주소가 있는 AP를 찾을 수 있습니다.원하는 AP가 이 페이지에 없으면 **다음**을 클릭하여 다음 페이지에서 AP를 확인합니다.
5. 원하는 AP가 Rogue AP(비인가 AP) 목록에서 AP에 해당하는 **Edit(수정)** 버튼을 클릭하면 AP의 세부사항 페이지로 이동합니다
.



Rogue AP details(비인가 AP 세부사항) 페이지에서 이 AP에 대한 자세한 정보(예: AP가 유선 네트워크에 연결되었는지 여부, AP의 현재 상태 등)를 확인할 수 있습니다.

6. 이 AP를 신뢰할 수 있는 AP로 구성하려면 Update **Status** 드롭다운 목록에서 Known Internal을 선택하고 **Apply**를 클릭합니다.AP 상태를 *Known Internal*(알려진 내부)로 업데이트하면 이 AP는 이 네트워크의 신뢰할 수 있는 AP로 구성됩니다
.

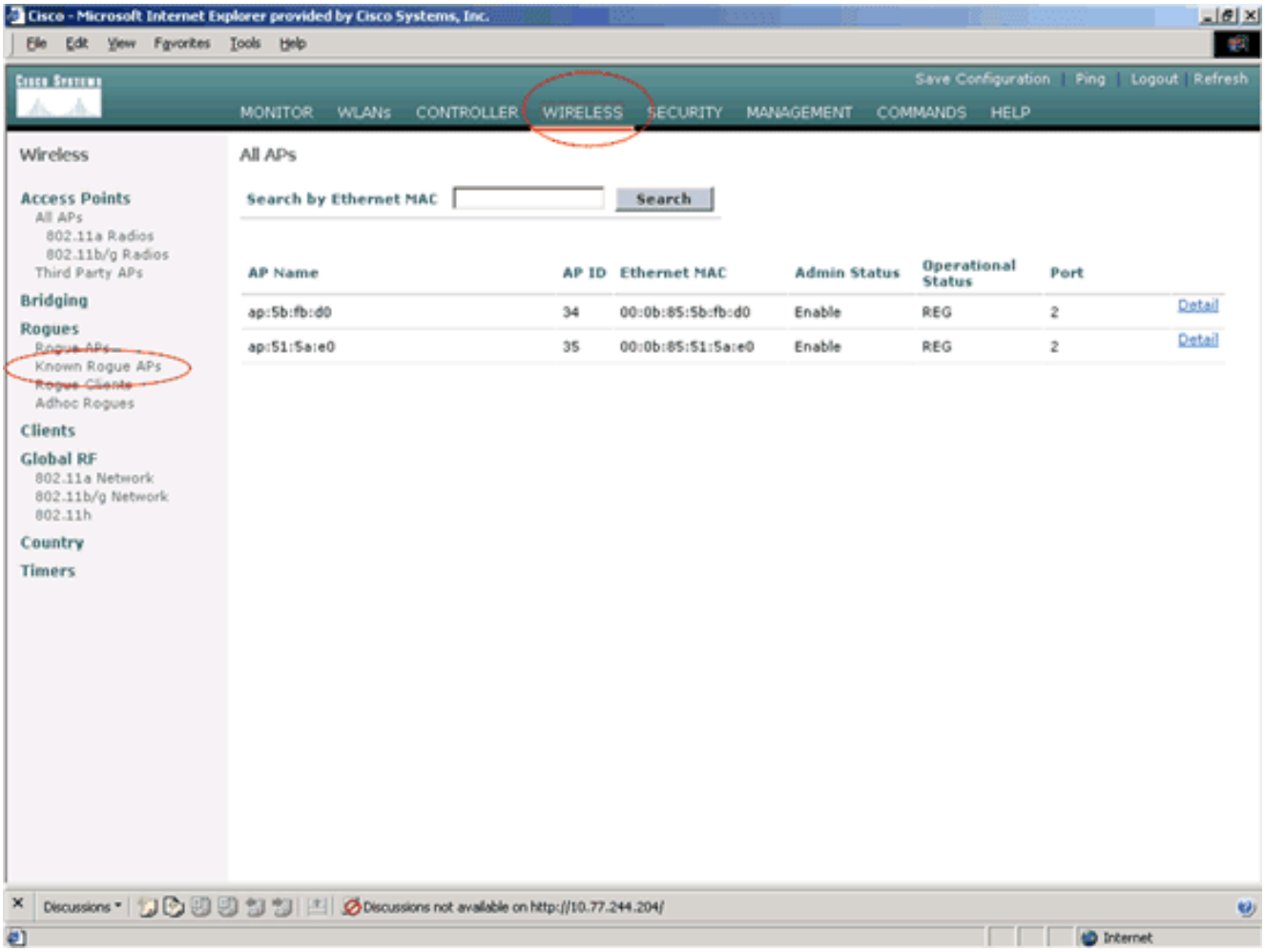


7. 신뢰할 수 있는 AP로 구성할 모든 AP에 대해 이 단계를 반복합니다.

신뢰할 수 있는 AP 컨피그레이션 확인

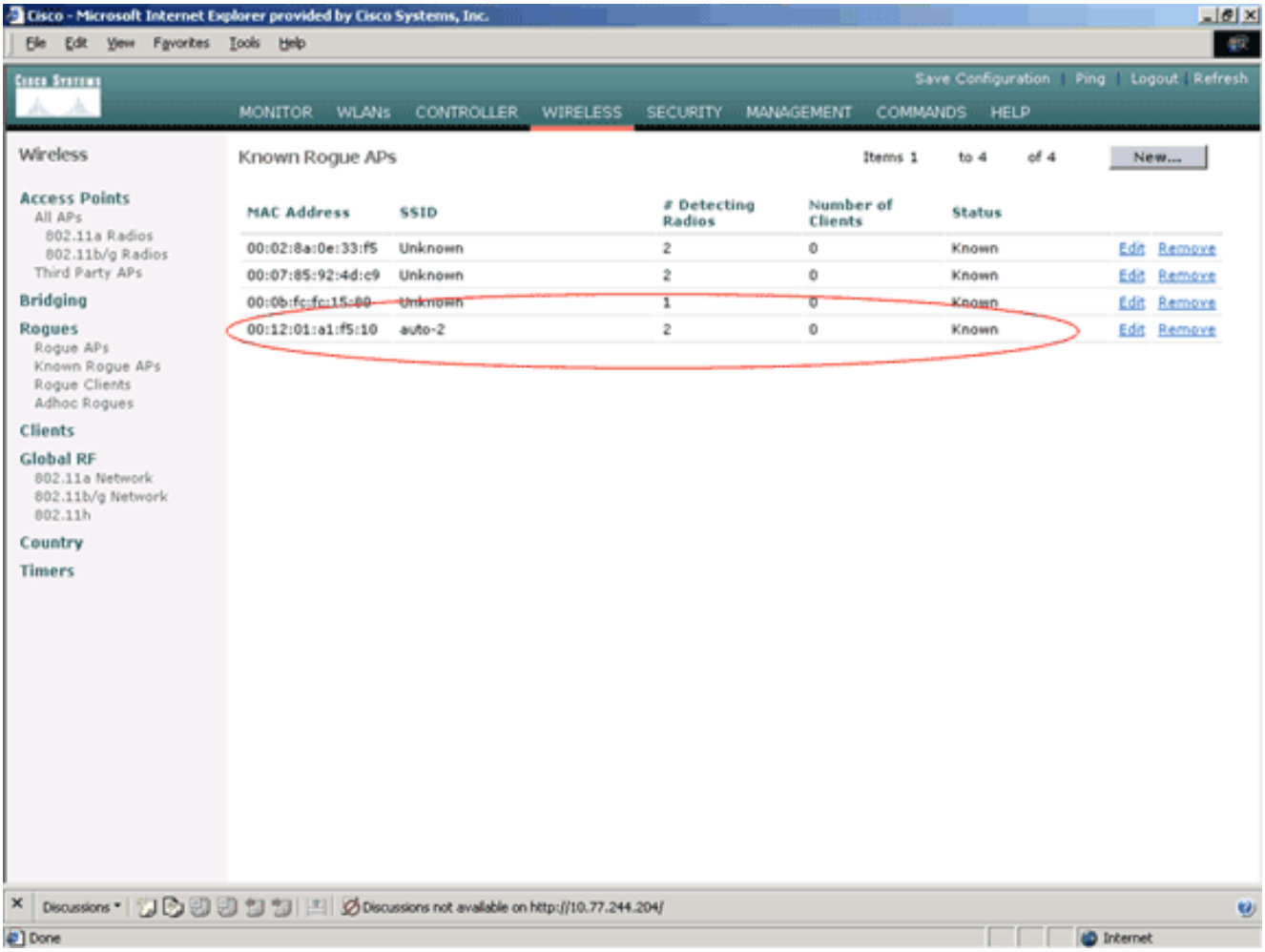
컨트롤러 GUI에서 AP가 신뢰할 수 있는 AP로 올바르게 구성되었는지 확인하려면 다음 단계를 완료하십시오.

1. **무선**을 클릭합니다.
2. Wireless(무선) 페이지의 왼쪽에 있는 메뉴에서 Known Rogue **APs(알려진 비인가 AP)를 클릭합니다**
.



원하는 AP가 Known(알려진 비인가 AP) 페이지에 나타나야 하며 상태가 Known(*알려짐)으로 표시됩니다*

.



신뢰할 수 있는 AP 정책 설정 이해

WLC에는 다음과 같은 신뢰할 수 있는 AP 정책이 있습니다.

- 적용된 암호화 정책
- 적용된 프리앰블 정책
- 적용된 무선 유형 정책
- SSID 검증
- 신뢰할 수 있는 AP가 누락된 경우 알림
- 신뢰할 수 있는 AP 항목에 대한 만료 시간 제한(초)

적용된 암호화 정책

이 정책은 신뢰할 수 있는 AP에서 사용해야 하는 암호화 유형을 정의하는 데 사용됩니다.Enforced encryption policy(강제 암호화 정책)에서 다음 암호화 유형을 구성할 수 있습니다.

- 없음
- 열기
- WEP
- WPA/802.11i

WLC는 신뢰할 수 있는 AP에 구성된 암호화 유형이 **"Enforced encryption policy(강제 암호화 정책)"** 설정에 구성된 암호화 유형과 일치하는지 확인합니다.신뢰할 수 있는 AP가 지정된 암호화 유형을 사용하지 않는 경우 WLC는 적절한 조치를 취하기 위해 관리 시스템에 경보를 울립니다.

적용된 프리앰블 정책

무선 프리앰블(헤더라고도 함)은 무선 장치가 패킷을 보내고 받을 때 필요한 정보를 포함하는 패킷 헤드의 데이터 섹션입니다.**짧은** 전문은 처리량 성능을 개선하므로 기본적으로 활성화됩니다.그러나 SpectraLink NetLink 전화기와 같은 일부 무선 장치에는 **긴** 전문이 필요합니다.Enforced preamble(강제 프리앰블) 정책에서 다음 프리앰블 옵션을 구성할 수 있습니다.

- 없음
- 짧은
- 긴

WLC는 신뢰할 수 있는 AP에 구성된 프리앰블 유형이 "Enforced preamble **policy**" 설정에 구성된 프리앰블 유형과 일치하는지 확인합니다.신뢰할 수 있는 AP가 지정된 프리앰블 유형을 사용하지 않으면 WLC가 적절한 조치를 취하도록 관리 시스템에 경보를 발효합니다.

적용된 무선 유형 정책

이 정책은 신뢰할 수 있는 AP에서 사용해야 하는 라디오 유형을 정의하는 데 사용됩니다 .Enforced(강제 적용) 라디오 유형 정책에서 다음 라디오 유형을 구성할 수 있습니다.

- 없음
- 802.11b 전용
- 802.11a 전용
- 802.11b/g 전용

WLC는 신뢰할 수 있는 AP에 구성된 라디오 유형이 "**Enforced radio type policy(**강제 적용 **라디오 유형 정책)**" 설정에 구성된 라디오 유형과 일치하는지 확인합니다.신뢰할 수 있는 AP가 지정된 라디오를 사용하지 않는 경우 WLC는 적절한 조치를 취하기 위해 관리 시스템에 경보를 표시합니다.

SSID 검증

컨트롤러에 구성된 SSID에 대해 신뢰할 수 있는 AP SSID를 검증하도록 컨트롤러를 구성할 수 있습니다.신뢰할 수 있는 AP SSID가 컨트롤러 SSID 중 하나와 일치하면 컨트롤러는 경보를 발생시킵니다.

신뢰할 수 있는 AP가 없는 경우 알림

이 정책을 활성화하면 WLC는 신뢰할 수 있는 AP가 알려진 비인가 AP 목록에 없으면 관리 시스템에 알림을 보냅니다.

신뢰할 수 있는 AP 항목에 대한 만료 시간 제한(초)

이 Expiration Timeout 값은 신뢰할 수 있는 AP가 만료되어 WLC 항목에서 플러시되기 전까지 경과해야 하는 시간(초)을 지정합니다.이 시간 제한 값을 초(120 - 3600초)로 지정할 수 있습니다.

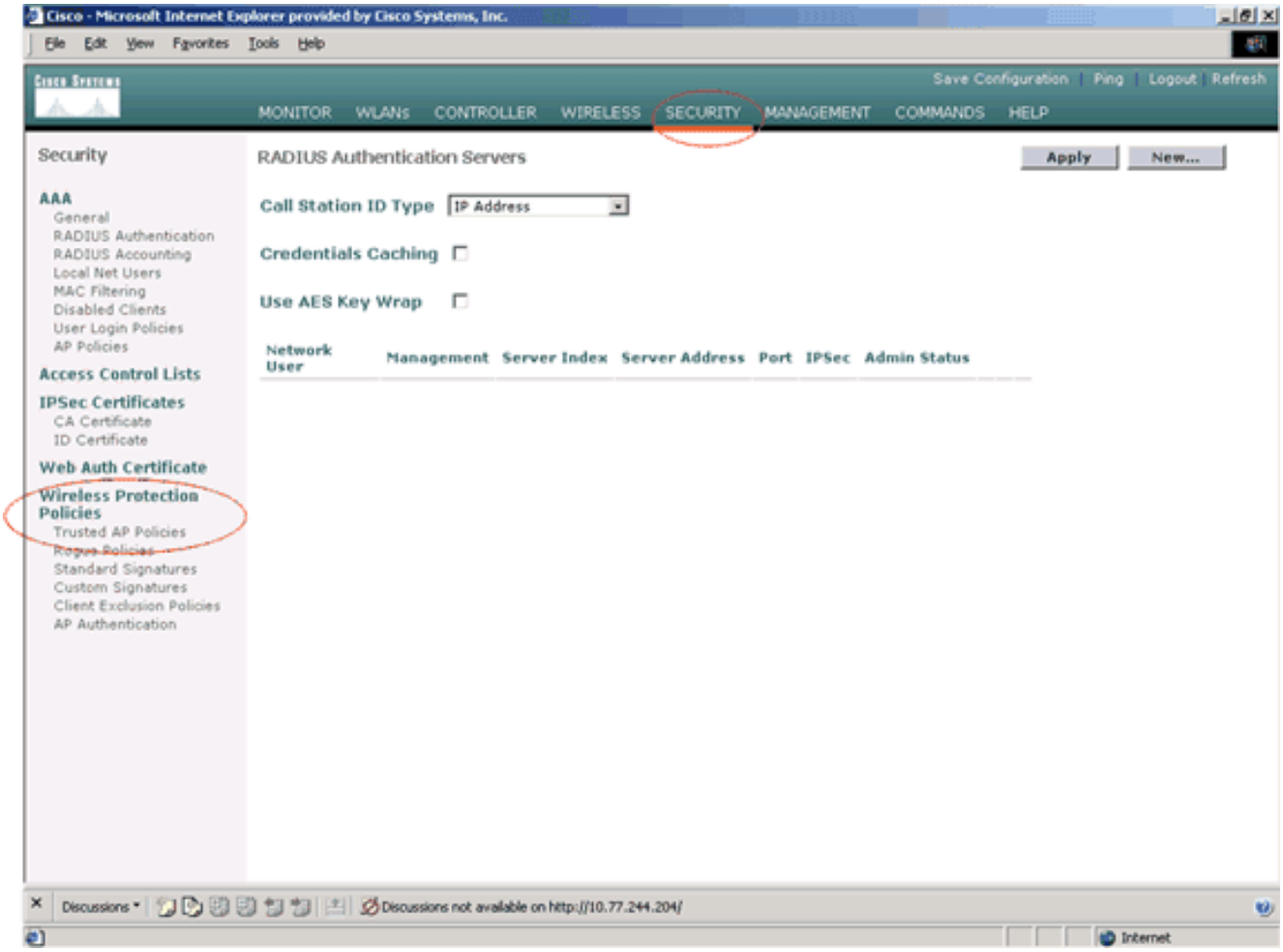
WLC에서 신뢰할 수 있는 AP 정책을 구성하는 방법?

GUI를 통해 WLC에서 신뢰할 수 있는 AP 정책을 구성하려면 다음 단계를 완료합니다.

참고: 모든 신뢰할 수 있는 AP 정책은 동일한 WLC 페이지에 있습니다.

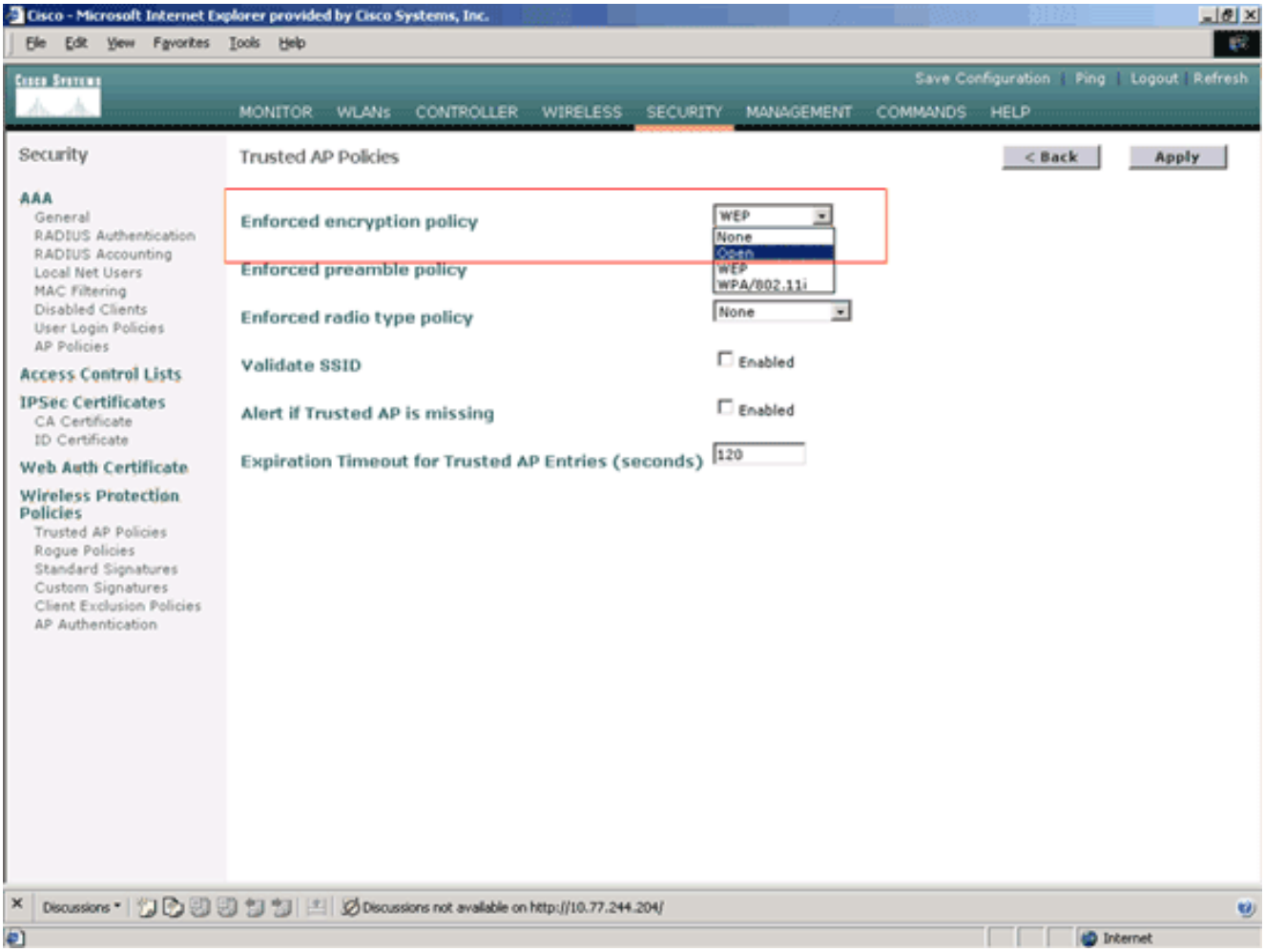
1. WLC GUI 주 메뉴에서 Security(**보안**)를 클릭합니다.
2. Security(보안) 페이지의 왼쪽에 있는 메뉴에서 Wireless Protection Policies(무선 보호 정책) 제목 아래 나열된 **Trusted AP policies(신뢰할 수 있는 AP 정책)**를 클릭합니다

.



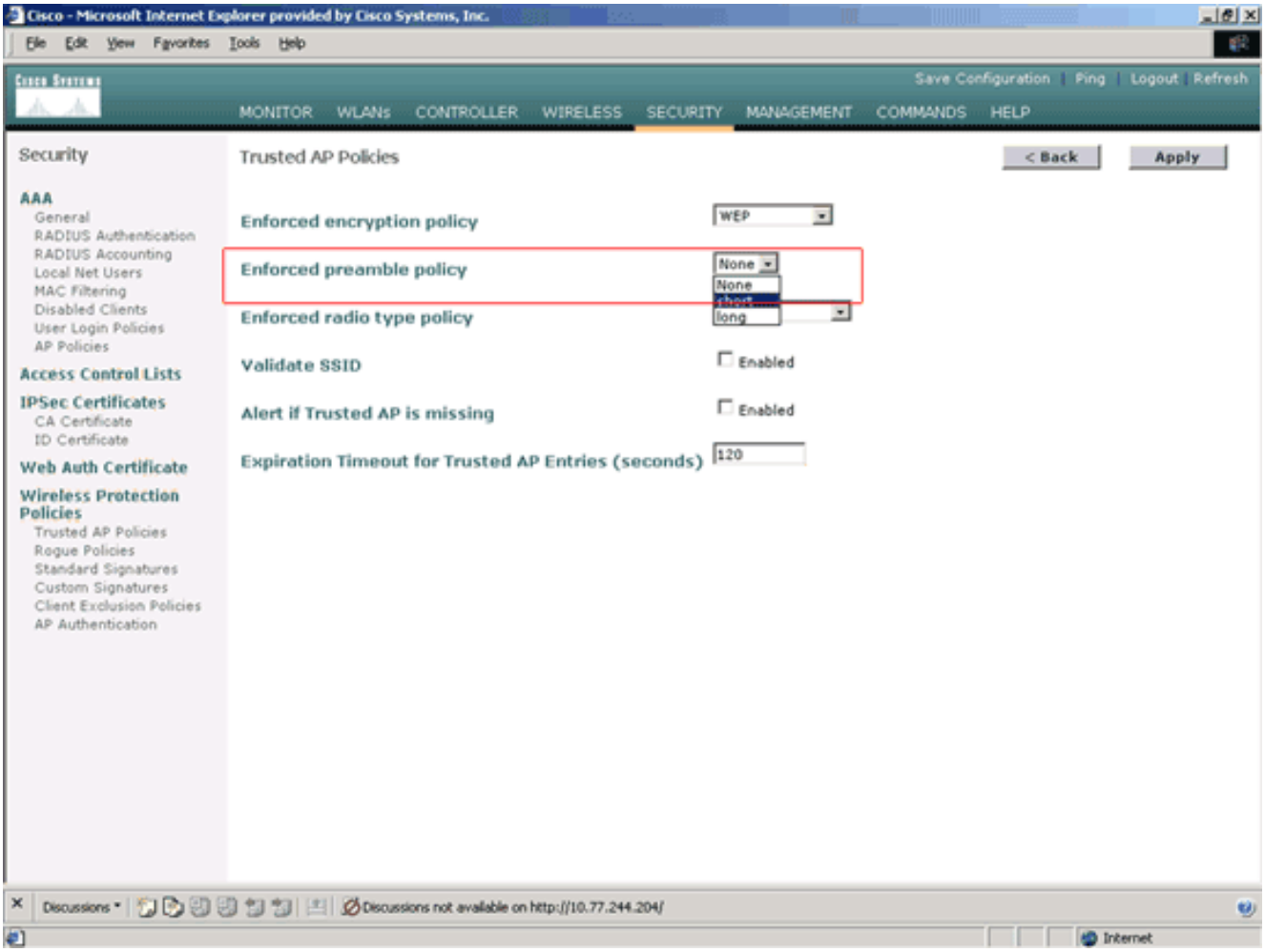
3. Trusted AP policies(신뢰할 수 있는 AP 정책) 페이지의 Enforced encryption policy(강제 암호화 정책) 드롭다운 목록에서 원하는 암호화 유형(None(없음), Open(열기), WEP, WPA/802.11i)을 선택합니다

.



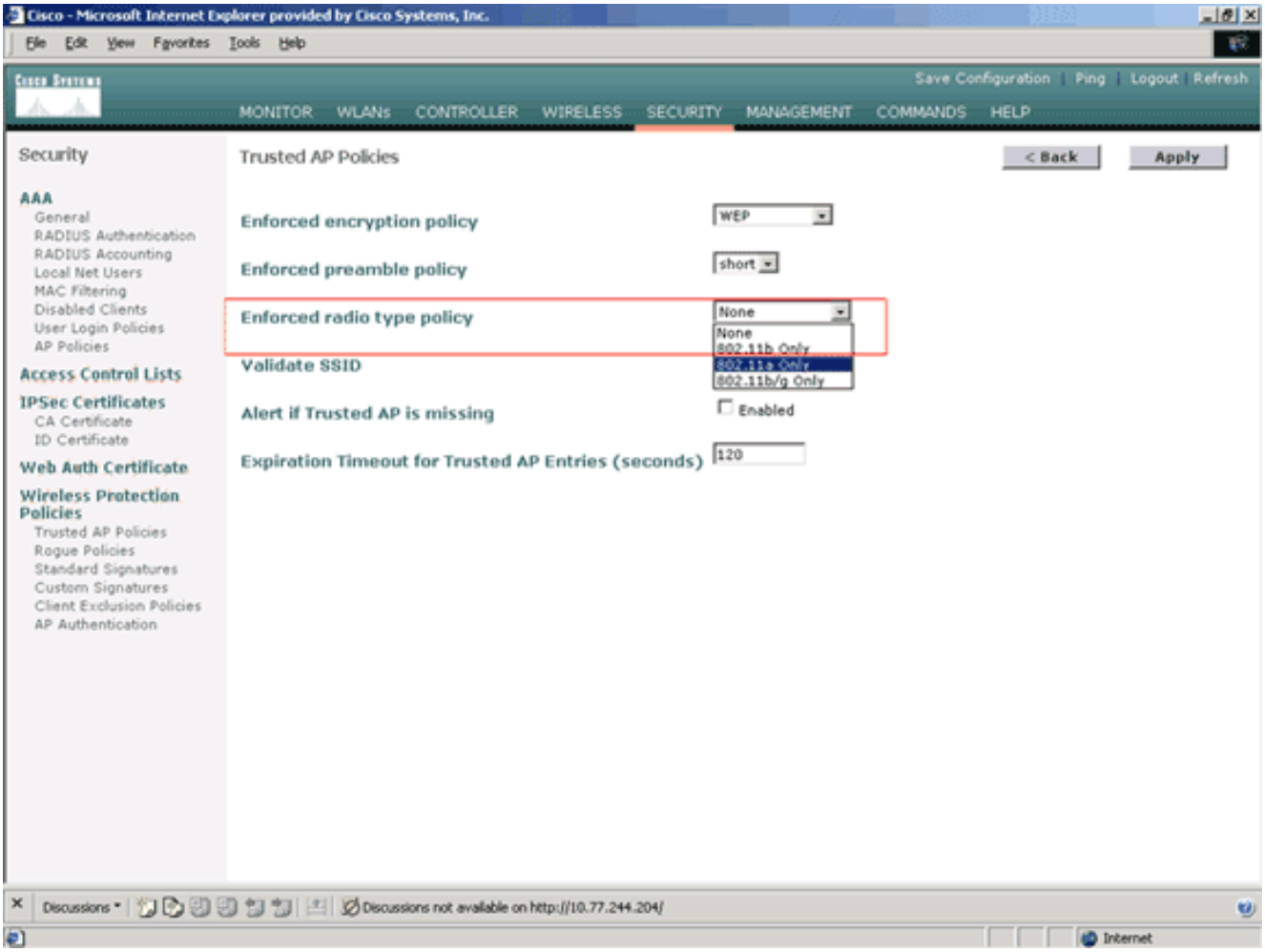
4. Enforced preamble type policy 드롭다운 목록에서 원하는 프리앰블 유형(None, Short, Long)을 선택합니다

.



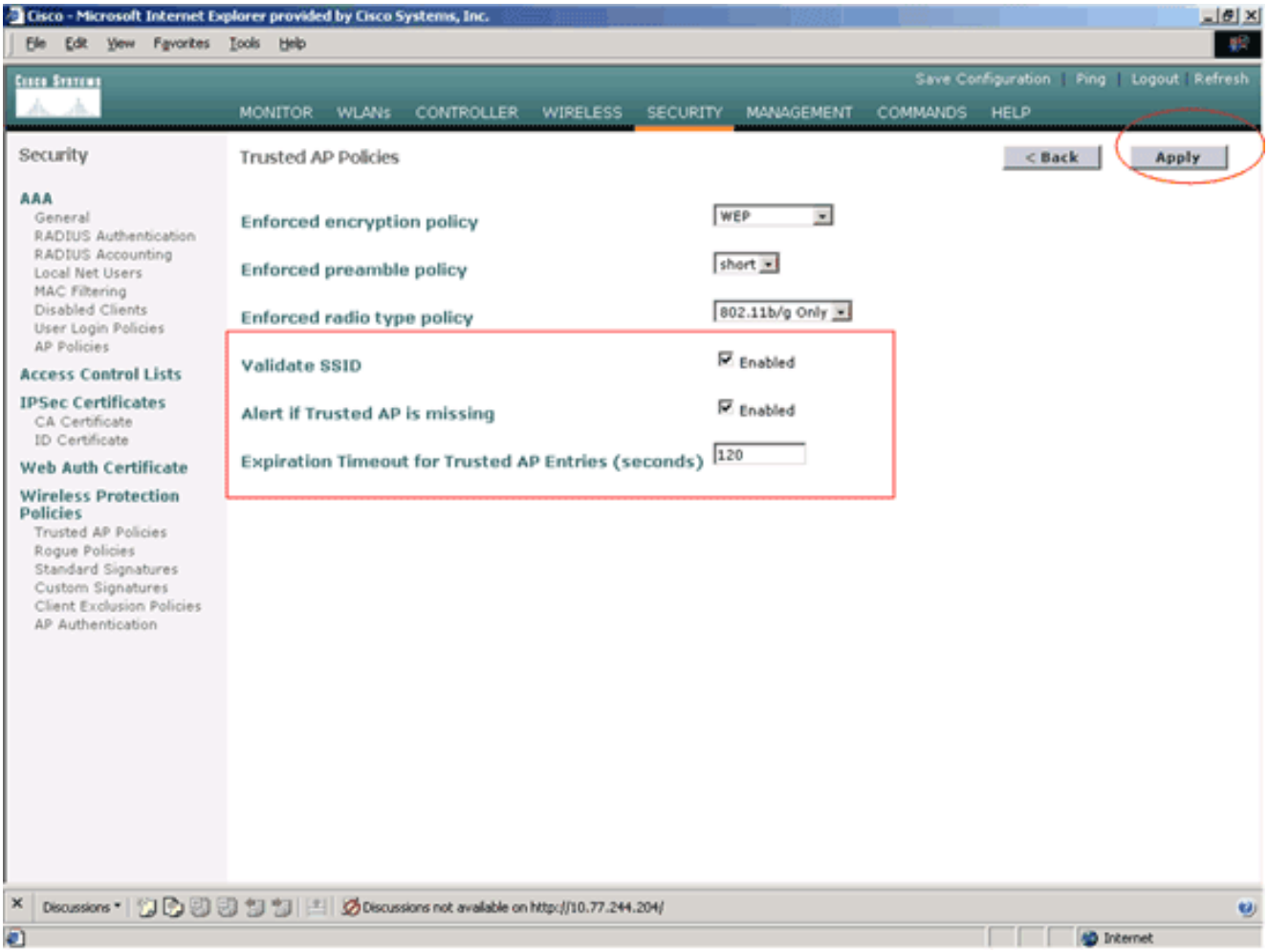
5. Enforced radio type policy 드롭다운 목록에서 원하는 라디오 유형(None, 802.11b only, 802.11a only, 802.11b/g only)을 선택합니다

.



6. Validate SSID 설정을 활성화 또는 비활성화하려면 Validate SSID Enabled(**SSID 활성화** 확인) 확인란을 선택하거나 선택 취소합니다.
7. 신뢰할 수 있는 **AP가** 없는 경우 경고를 활성화하거나 비활성화하려면 Alert if trusted AP is missing Enabled(**신뢰할 수 있는 AP에** Enabled가 없는 경우 경고) 확인란을 선택하거나 선택 취소합니다.
8. Expiration Timeout for Trusted **AP entries** 옵션의 값(초)**을** 입력합니다

.



9. Apply를 **클릭합니다**.

참고: WLC CLI에서 이러한 설정을 구성하려면 적절한 정책 옵션과 함께 **config wps trusted-ap** 명령을 사용할 수 있습니다.

```
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.
```

신뢰할 수 있는 AP 정책 위반 경고 메시지

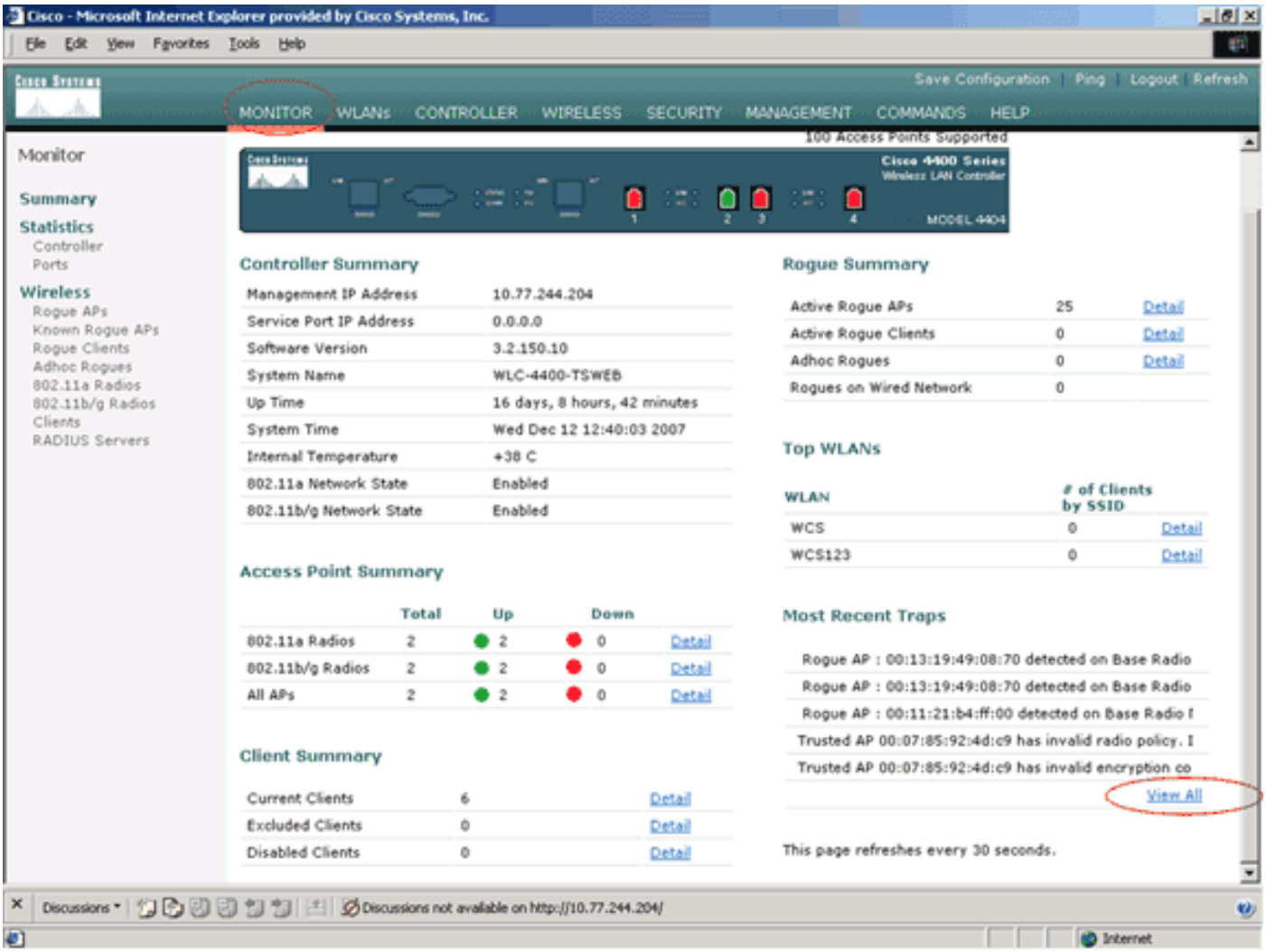
다음은 컨트롤러에서 표시하는 신뢰할 수 있는 AP 정책 위반 알림 메시지의 예입니다.

```
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
```

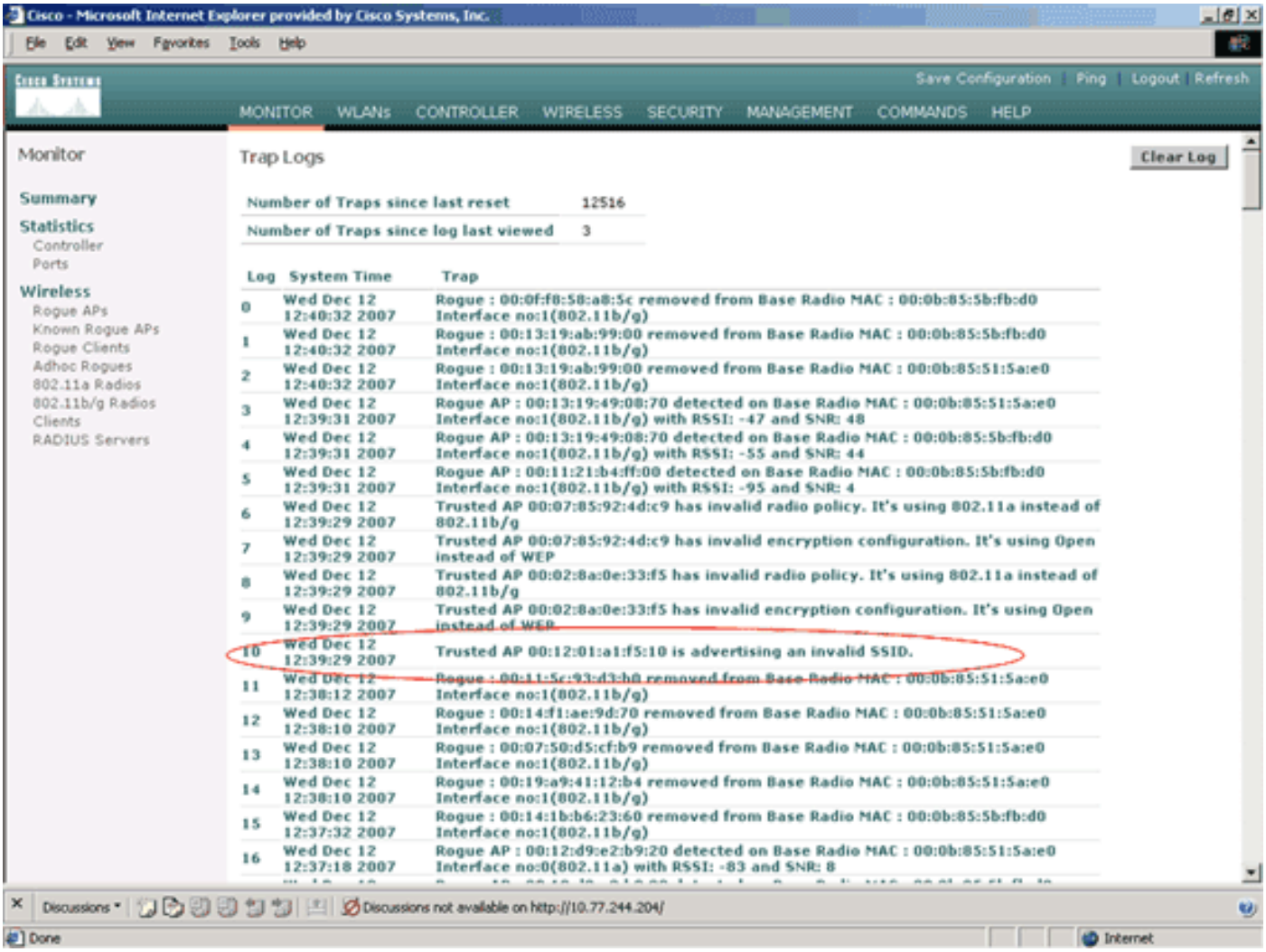
강조 표시된 오류 메시지를 확인합니다.이러한 오류 메시지는 신뢰할 수 있는 AP에 구성된 SSID 및 암호화 유형이 신뢰할 수 있는 AP 정책 설정과 일치하지 않음을 나타냅니다.

WLC GUI에서 동일한 경고 메시지를 볼 수 있습니다.이 메시지를 보려면 WLC GUI 주 메뉴로 이동

하여 **Monitor**(모니터)를 클릭합니다.Monitor(모니터) 페이지의 Most Recent Traps(최근 트랩) 섹션에서 **View All(모두 보기)**을 클릭하여 WLC의 모든 최근 알림을 확인합니다.



Most Recent Traps(최근 트랩) 페이지에서 다음 이미지와 같이 신뢰할 수 있는 AP 정책 위반 경고 메시지를 생성하는 컨트롤러를 식별할 수 있습니다.



관련 정보

- Cisco Wireless LAN Controller 컨피그레이션 가이드, 릴리스 5.2 - RF 그룹에서 Enabling Rouge Access Point Detection
- Cisco Wireless LAN Controller 컨피그레이션 가이드, 릴리스 4.0 - 보안 솔루션 구성
- 통합 무선 네트워크에서 비인가 탐지
- SpectraLink Phone 설계 및 구축 설명서
- 기본 무선 LAN 연결 구성 예
- 무선 LAN 네트워크에서 연결 문제 해결
- 무선 LAN 컨트롤러 인증 컨피그레이션 예
- 기술 지원 및 문서 – Cisco Systems