Trusted AP-beleid op een draadloze LAN-controller

Inhoud

Inleiding

Dit document beschrijft het *vertrouwde AP* draadloze beschermingsbeleid op een Draadloze LAN controller (WLC), definieert een betrouwbaar AP-beleid en biedt een korte beschrijving van al het vertrouwde AP-beleid.

Voorwaarden

Vereisten

Zorg ervoor dat u een basisbegrip van de draadloze LAN veiligheidsparameters (zoals SSID, encryptie, authenticatie, etc.) hebt.

Conventies

Raadpleeg Cisco Technical Tips Conventions (Conventies voor technische tips van Cisco) voor meer informatie over documentconventies.

Trusted AP-beleid

Trusted AP-beleid is een beveiligingsfunctie in de controller die ontworpen is om te worden gebruikt in scenario's waar klanten naast de controller een parallel autonoom AP-netwerk hebben. In dat scenario kan de autonome AP als vertrouwde AP op de controller worden gemarkeerd en kan de gebruiker beleid voor deze vertrouwde AP's definiëren (die alleen EVN of WAP, onze eigen

SSID, korte preambule enzovoort zouden moeten gebruiken). Als een van deze AP er niet in slaagt aan dit beleid te voldoen, heft de controller een alarm in het netwerkbeheerapparaat (Wireless Control System) dat stelt dat een vertrouwde AP een geconfigureerd beleid heeft overtreden.

Wat is een Trusted AP?

Betrouwbare AP's zijn AP's die geen deel uitmaken van een organisatie. Ze veroorzaken echter geen veiligheidsbedreiging voor het netwerk. Deze AP's worden ook vriendelijke AP's genoemd. Er zijn meerdere scenario's waar u een AP als een vertrouwde AP zou willen configureren.

U kunt bijvoorbeeld verschillende categorieën AP's in uw netwerk hebben zoals:

- **APs u die niet LWAPP (wellicht lopen zij IOS of VxWorks) uitvoeren**
- LWAPP AP's die werknemers inbrengen (met kennis van de beheerder)
- LWAPP APs die worden gebruikt om het bestaande netwerk te testen
- LWAPP APs die buren bezitten

Normaal gesproken zijn vertrouwde APs APs die in **categorie 1** vallen, die APs zijn die u bezit die geen LWAPP lopen. Het kunnen oude APs zijn die VxWorks of IOS runnen. Om ervoor te zorgen dat deze APs het netwerk niet beschadigen, kunnen bepaalde eigenschappen worden afgedwongen, zoals correcte SSIDs en authenticatie-types. Configureer het vertrouwde AP-beleid op de WLC en zorg ervoor dat de vertrouwde APs aan dit beleid voldoen. Als dit niet het geval is, kunt u de controller configureren om verschillende handelingen uit te voeren, zoals een alarm afslaan naar het netwerkbeheerapparaat (WCS).

Bekende AP's die tot de buren behoren kunnen als vertrouwde APs worden gevormd.

Normaal gesproken zou MFP (Management Frame Protection) AP's die geen legitieme LWAPP AP's zijn moeten verhinderen om zich bij de WLC aan te sluiten. Als NIC-kaarten MFP ondersteunen, mogen zij geen afwijkingen van andere apparaten dan de echte AP's accepteren. Raadpleeg MFP (Infrastructuur Management Frame Protection) met WLC en LAP Configuration Voorbeeld voor meer informatie over MFP.

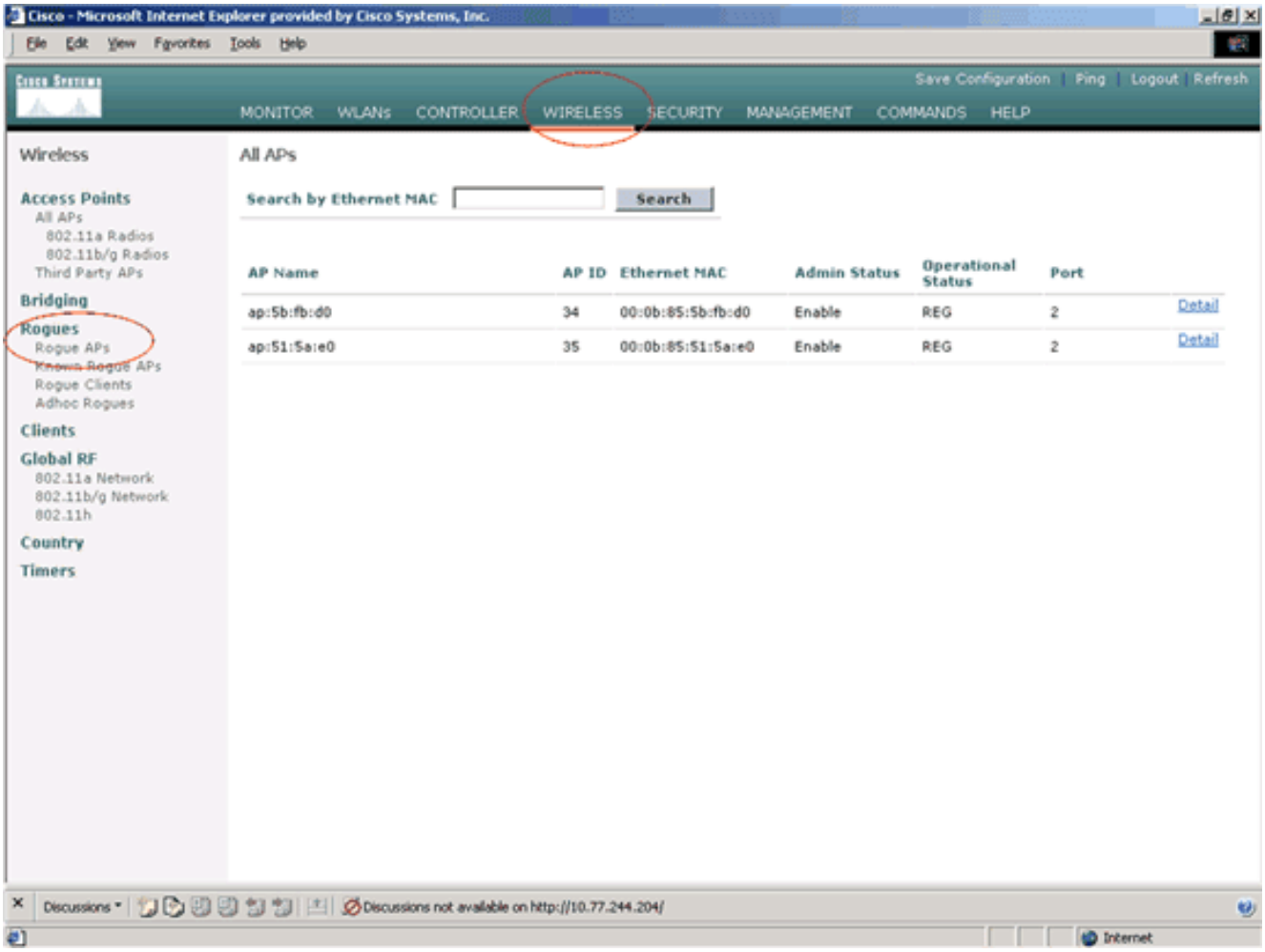
Als u AP's hebt die VxWorks of IOS (zoals in categorie 1) lopen, zullen zij zich nooit bij de LWAPP groep aansluiten of MFP doen, maar u zou het beleid kunnen willen afdwingen dat op die pagina vermeld staat. In dergelijke gevallen moet het vertrouwde AP-beleid op de controller worden ingesteld voor de AP's van belang.

In het algemeen, als je weet over een schurkenpas en identificeert dat het geen bedreiging voor je netwerk is, kun je dat AP als bekend vertrouwde AP identificeren.

Hoe te om AP als Betrouwbare AP te configureren vanuit de WLC GUI?

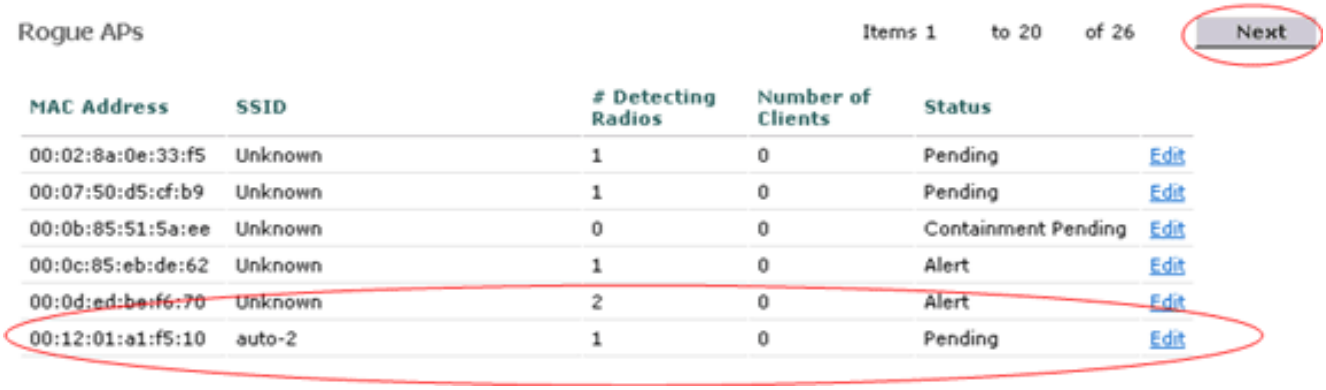
Voltooi deze stappen om een AP als vertrouwde AP te configureren:

1. Log in op de GUI van de WLC via HTTP of https inloggen.
2. Klik in het hoofdmenu van de controller op **Draadloos**.
3. Klik in het menu aan de linkerkant van de draadloze pagina op **AP's van de Roep**.



De pagina Verkennende APs maakt een lijst van alle APs die als schurk APs op het netwerk worden gedetecteerd.

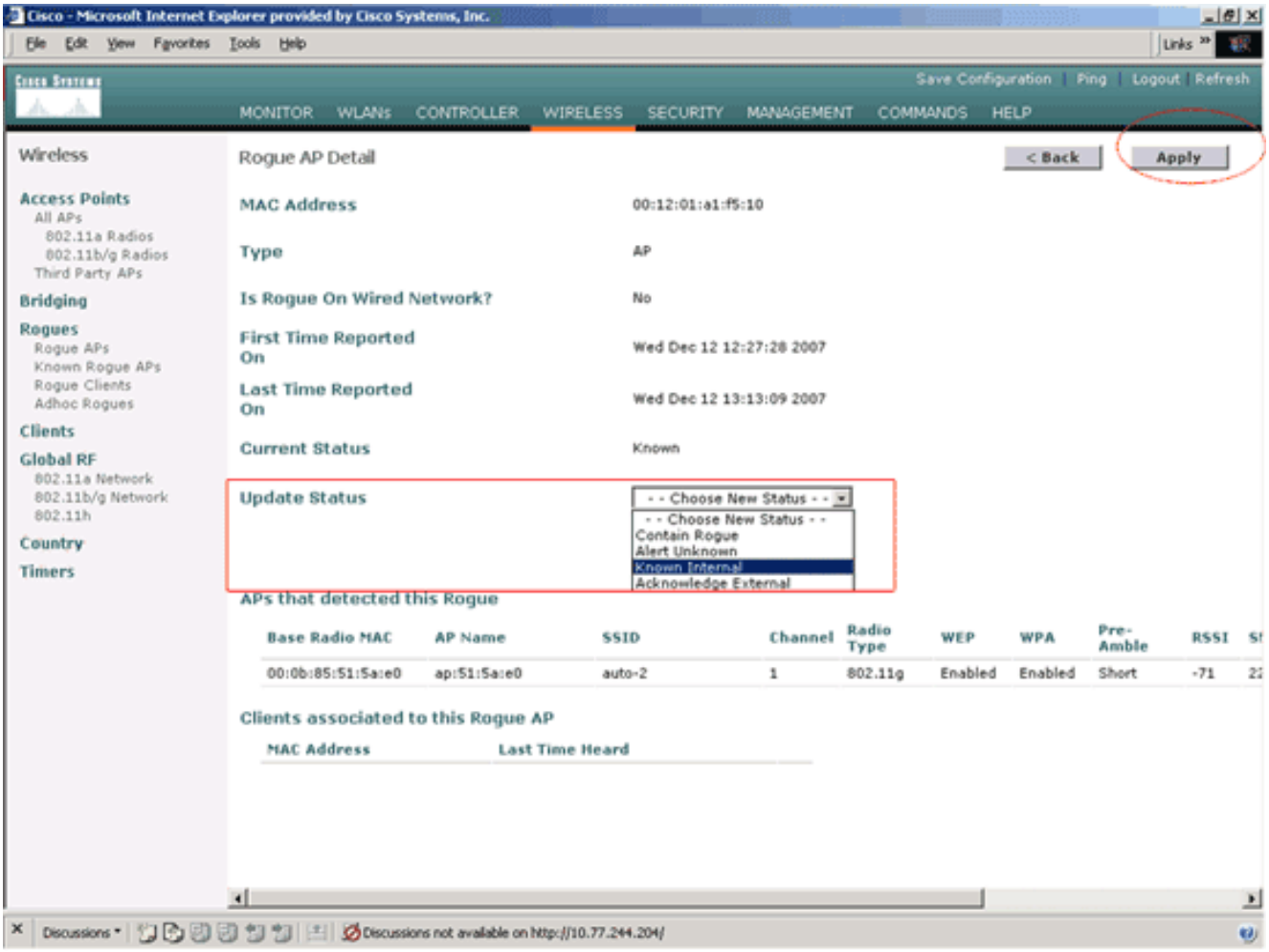
4. Van deze lijst van schurkenAP's, plaats AP die u als vertrouwde AP wilt configureren dat onder categorie 1 valt (zoals uitgelegd in de vorige sectie).U kunt APs met de MAC adressen vinden die op de pagina van Rogue APs worden vermeld. Als het gewenste AP niet in deze pagina staat, klik op **Volgende** om het AP van de volgende pagina te identificeren.
5. Zodra het gewenste AP van de lijst van AP van de Rogue is gevestigd, klik de knop **Bewerken** die aan AP correspondeert, wat u aan de detailpagina van AP neemt.



In de pagina met informatie over Rogue AP kunt u gedetailleerde informatie over deze AP vinden (zoals of die AP verbonden met verbonden netwerk, zowel als de huidige status van AP etc.).

6. Om deze AP als vertrouwde AP te configureren selecteert u **Bekende Interne** van de vervolgkeuzelijst Stand van de Update Status en klikt u op **Toepassen**.Wanneer u de AP status aan *gekend intern* bijwerken, wordt deze AP gevormd als vertrouwde AP van dit

netwerk.

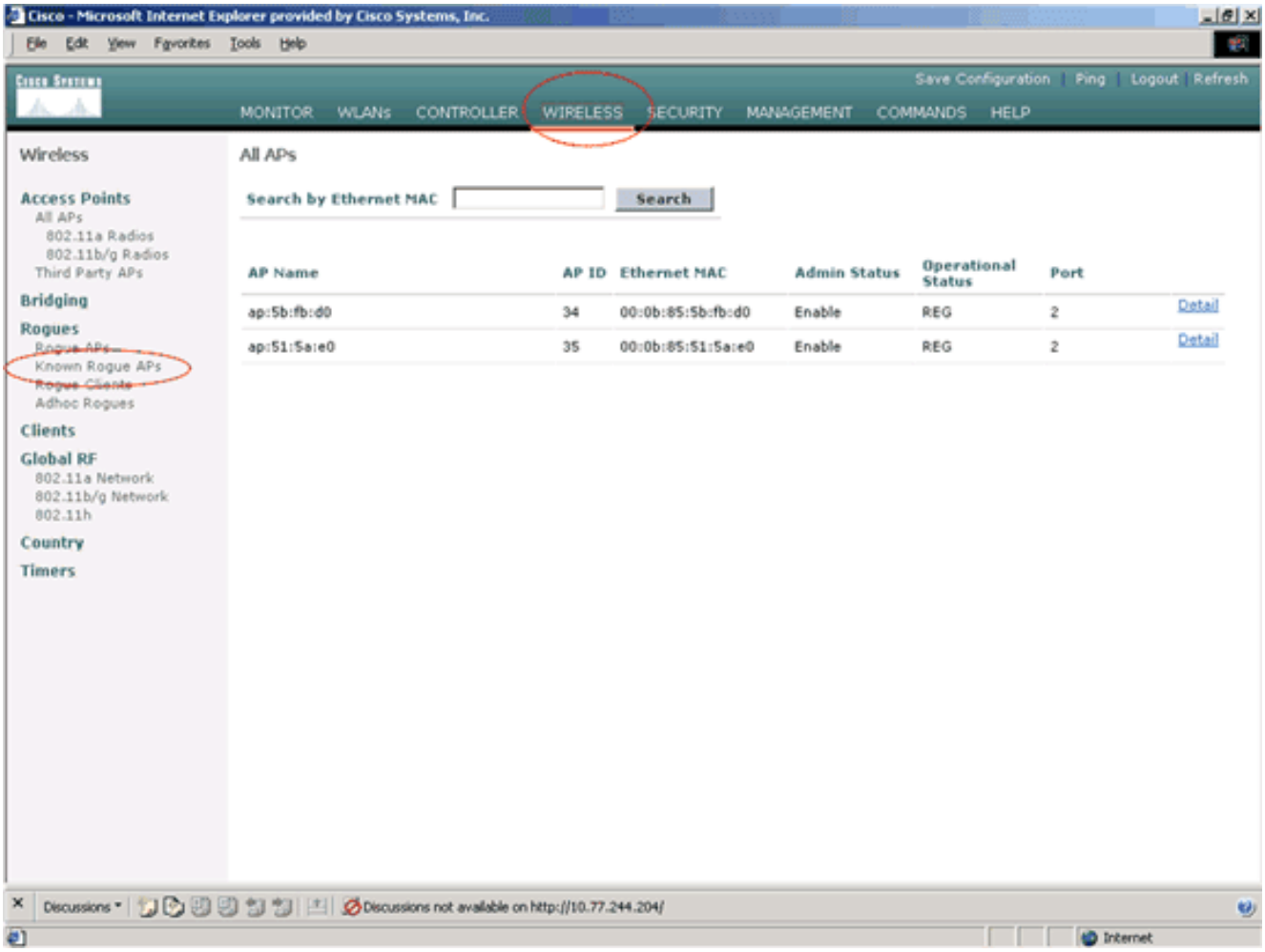


7. Herhaal deze stappen voor alle AP's die u als vertrouwde APs wilt configureren.

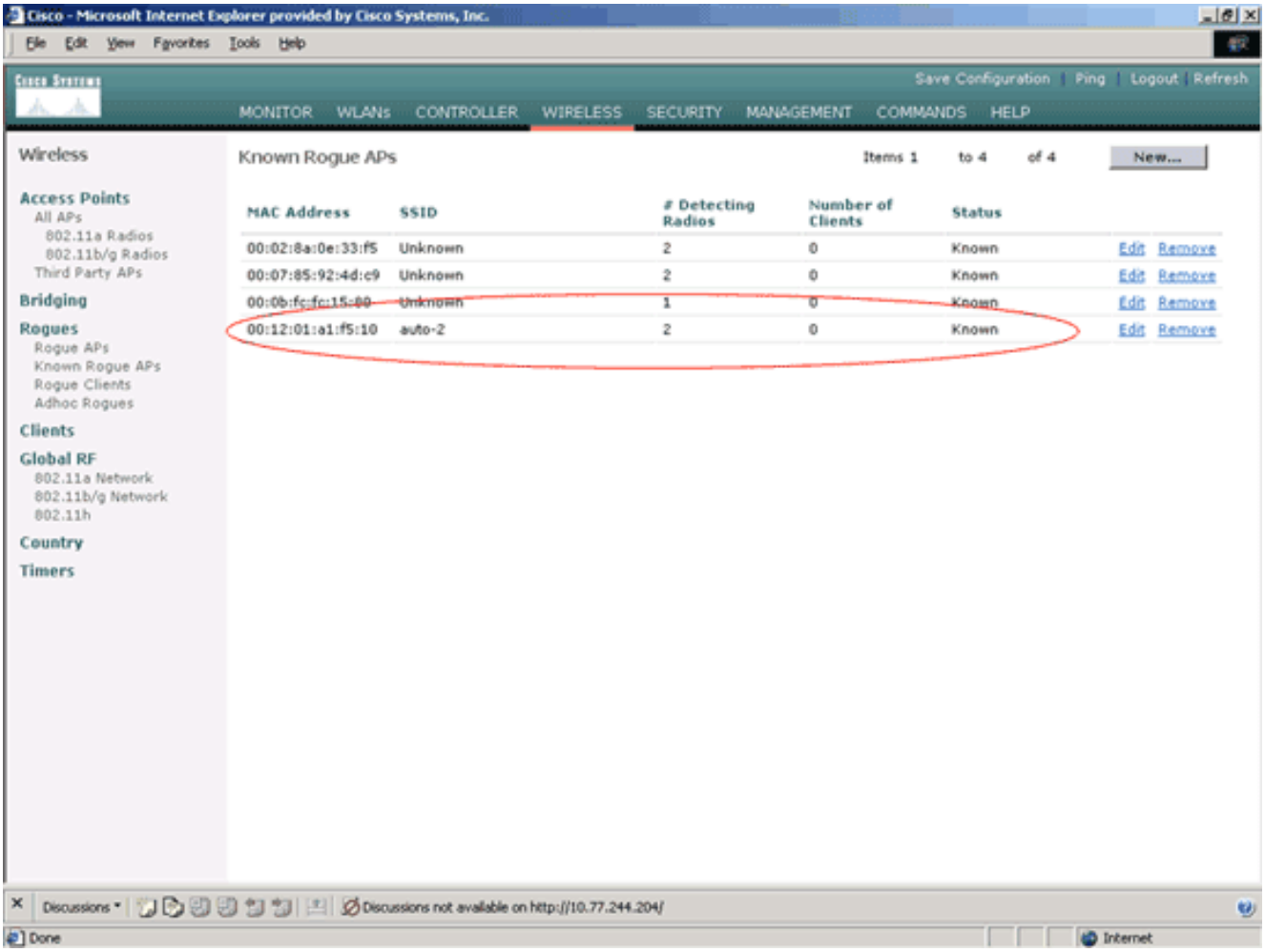
Controleer de Trusted AP-configuratie

Voltooi deze stappen om te controleren of de AP correct is ingesteld als vertrouwde AP van de controller GUI:

1. Klik op **Draadloos**.
2. Klik in het menu aan de linkerkant van de draadloze pagina op **Known Rogue AP**'s.



Het gewenste AP moet op de Known Rogue APs pagina met de status weergegeven zoals *bekend*.



De betekenis van Trusted AP-beleidsinstellingen

De WLC heeft dit vertrouwde AP beleid:

- Geavanceerd encryptiebeleid
- Afdwingbaar beleid
- Afgedwongen beleid op het gebied van radio
- SSID valideren
- Waarschuwing als vertrouwde AP ontbreekt
- Time-out bij overschrijding voor Trusted AP-vermeldingen (seconden)

Geavanceerd encryptiebeleid

Dit beleid wordt gebruikt om het coderingstype te definiëren dat de vertrouwde AP zou moeten gebruiken. U kunt een van deze coderingstypen configureren onder Afgedwongen coderingsbeleid:

- None
- Open (Openstaand)
- medegebruik
- WAP/802.11i

De WLC verifieert of het coderingstype dat op de vertrouwde AP wordt ingesteld overeenkomt met het coderingstype dat is ingesteld op "**Enforced Encryption Policy**". Indien het vertrouwde AP het aangewezen coderingstype niet gebruikt, werpt de WLC een alarm naar het beheersysteem om

passende maatregelen te nemen.

Afdwingbaar beleid

De radio preamble (soms een header genoemd) is een gedeelte van gegevens aan het hoofd van een pakket dat informatie bevat die draadloze apparaten nodig hebben wanneer ze pakketten verzenden en ontvangen. **Korte** preambule verbeteren de doorvoerprestaties, zodat ze standaard ingeschakeld zijn. Voor sommige draadloze apparaten, zoals SpectraLink NetLink-telefoons, zijn echter **lange** preambule nodig. U kunt een van deze voorvoegselopties configureren onder Afdwingbaar voorvoegsel-beleid:

- None
- Kort
- lang

De WLC verifieert of het Preamble-type dat op de vertrouwde AP is geconfigureerd overeenkomt met het preambule-type dat is ingesteld in de instelling "**Afdwingbaar beleid**". Indien de vertrouwde AP het gespecificeerde preambule type niet gebruikt, roept de WLC een alarm op in het beheersysteem om passende maatregelen te nemen.

Afgedwongen beleid op het gebied van radio

Dit beleid wordt gebruikt om het radiotype te definiëren dat de vertrouwde AP zou moeten gebruiken. U kunt een van deze radiotypen configureren onder Afgedwongen radiotypebeleid:

- None
- alleen 802.11b
- alleen 802.11a
- Alleen 802.11b/g

De WLC verifieert of het radiotype dat op de vertrouwde AP is geconfigureerd overeenkomt met het radiatype dat is ingesteld in de instelling "**Afgedwongen radiotype beleid**". Indien de vertrouwde AP de gespecificeerde radio's niet gebruikt, werpt de WLC een alarm in het beheersysteem op om passende maatregelen te nemen.

SSID valideren

U kunt de controller configureren om een vertrouwde APs SSID te valideren tegen de SSID’s die zijn ingesteld op de controller. Als de vertrouwde APs SSID's één van de controller SSID's aanpast, roept de controller een alarm op.

Waarschuwing als Trusted AP ontbreekt

Als dit beleid is geactiveerd, waarschuwt de WLC het beheersysteem als de vertrouwde AP van de bekende AP van de Rogue APs lijst ontbreekt.

Time-out bij overschrijding voor betrouwbare AP-vermeldingen (seconden)

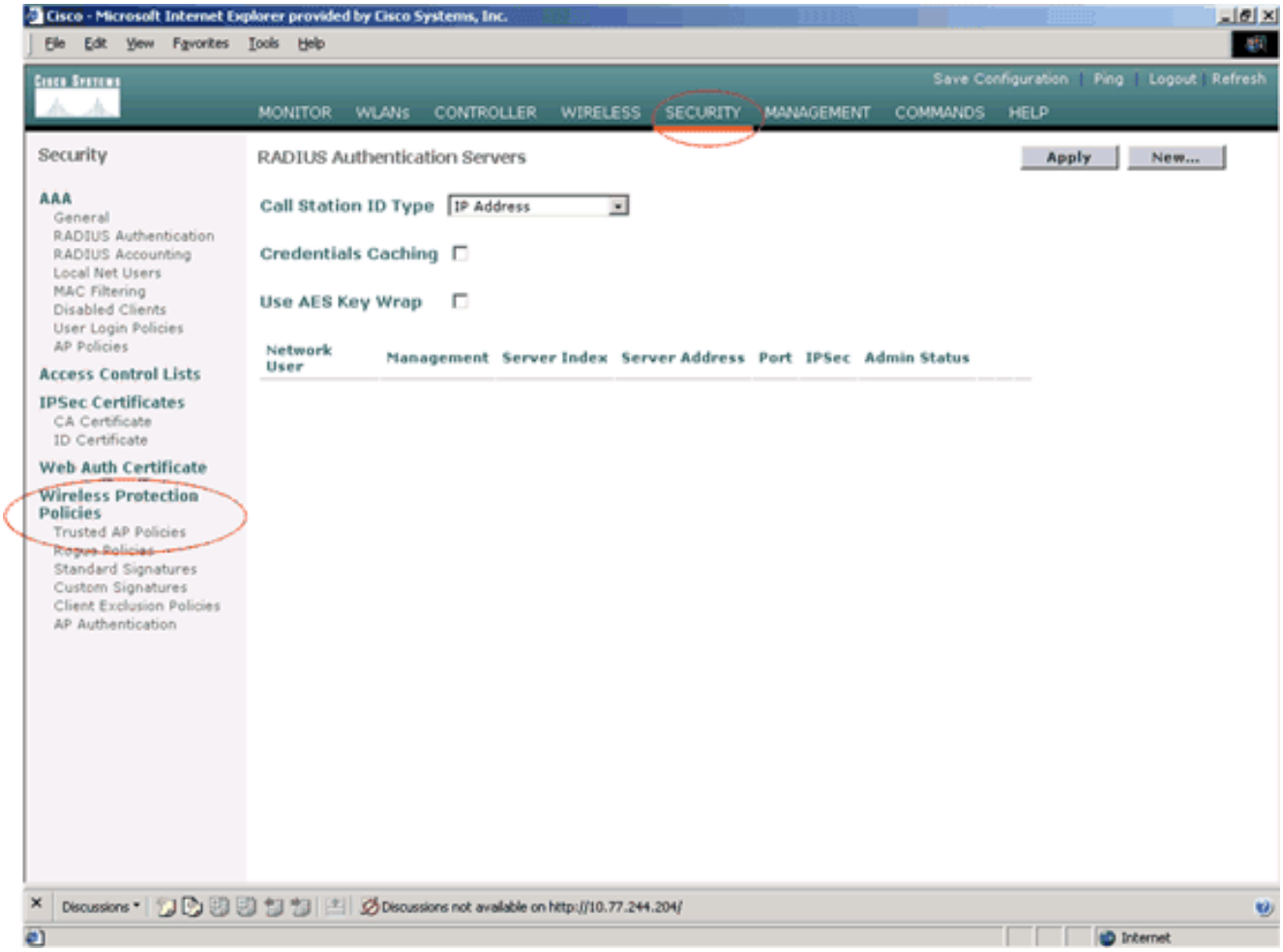
Deze Time-outwaarde voor beëindiging van het programma specificeert het aantal seconden voordat de vertrouwde AP wordt beschouwd als verlopen en wordt gespoeld vanaf de WLC-ingang. U kunt deze waarde in seconden specificeren (120-3600 seconden).

Hoe moet u het vertrouwde AP-beleid op de WLC configureren?

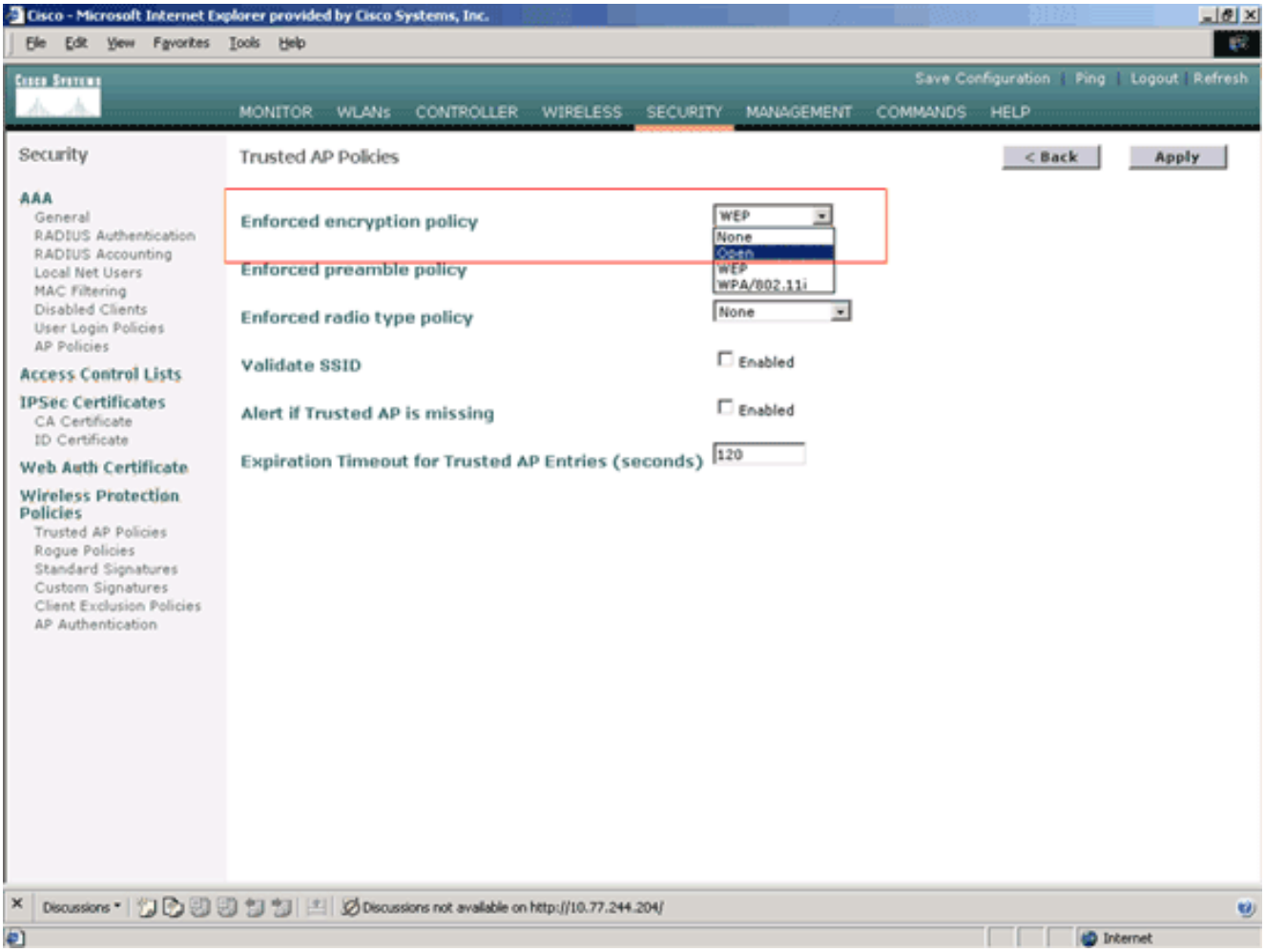
Voltooi deze stappen om een betrouwbaar AP-beleid op de WLC te configureren via de GUI:

Opmerking: al het vertrouwde AP beleid zit op dezelfde WLC pagina.

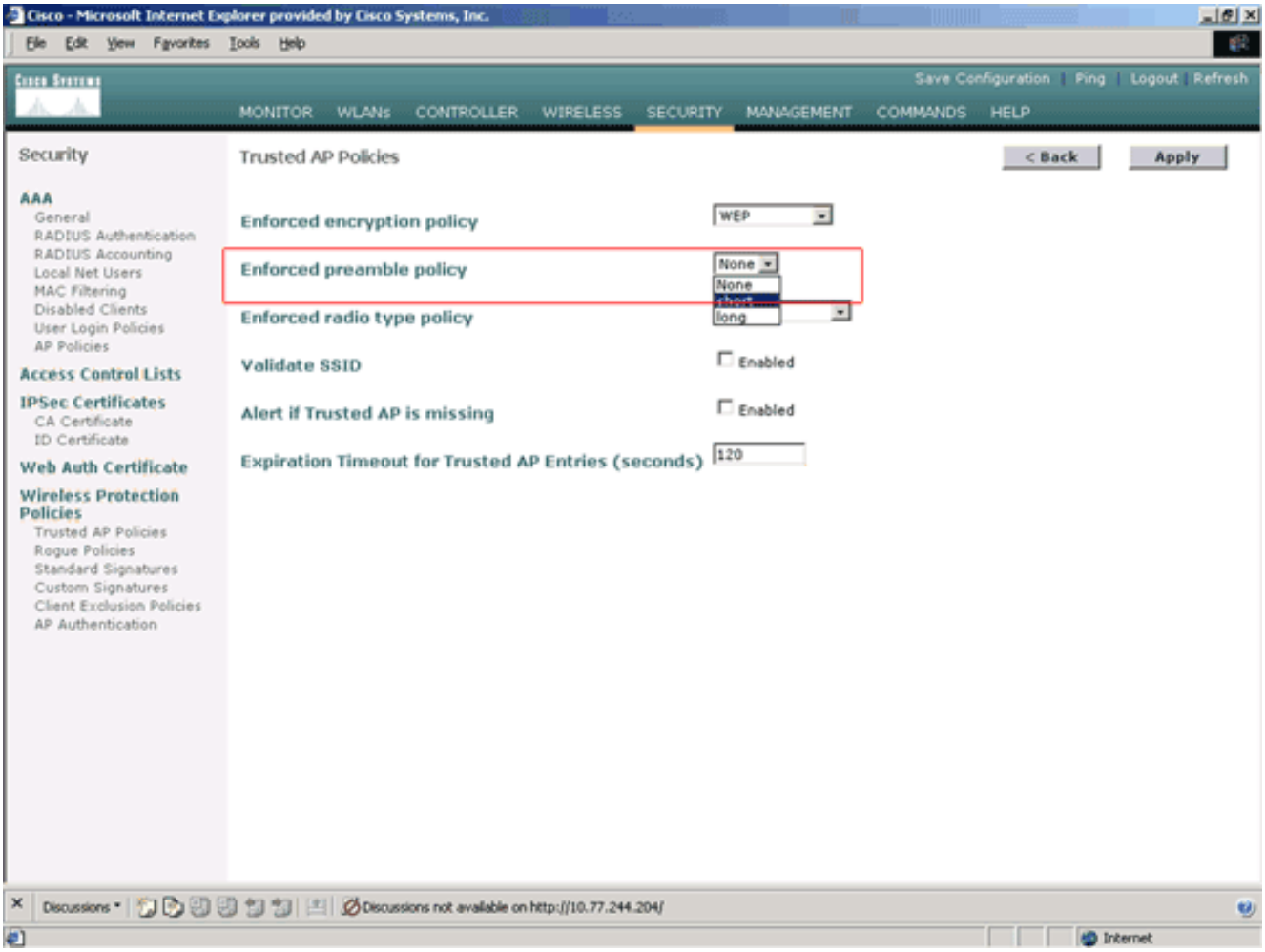
1. Klik in het hoofdmenu van de WLC GUI op **Beveiliging**.
2. Klik in het menu aan de linkerkant van de Security pagina op **Trusted AP-beleid** dat onder de rubriek Draadloos beschermingsbeleid staat.



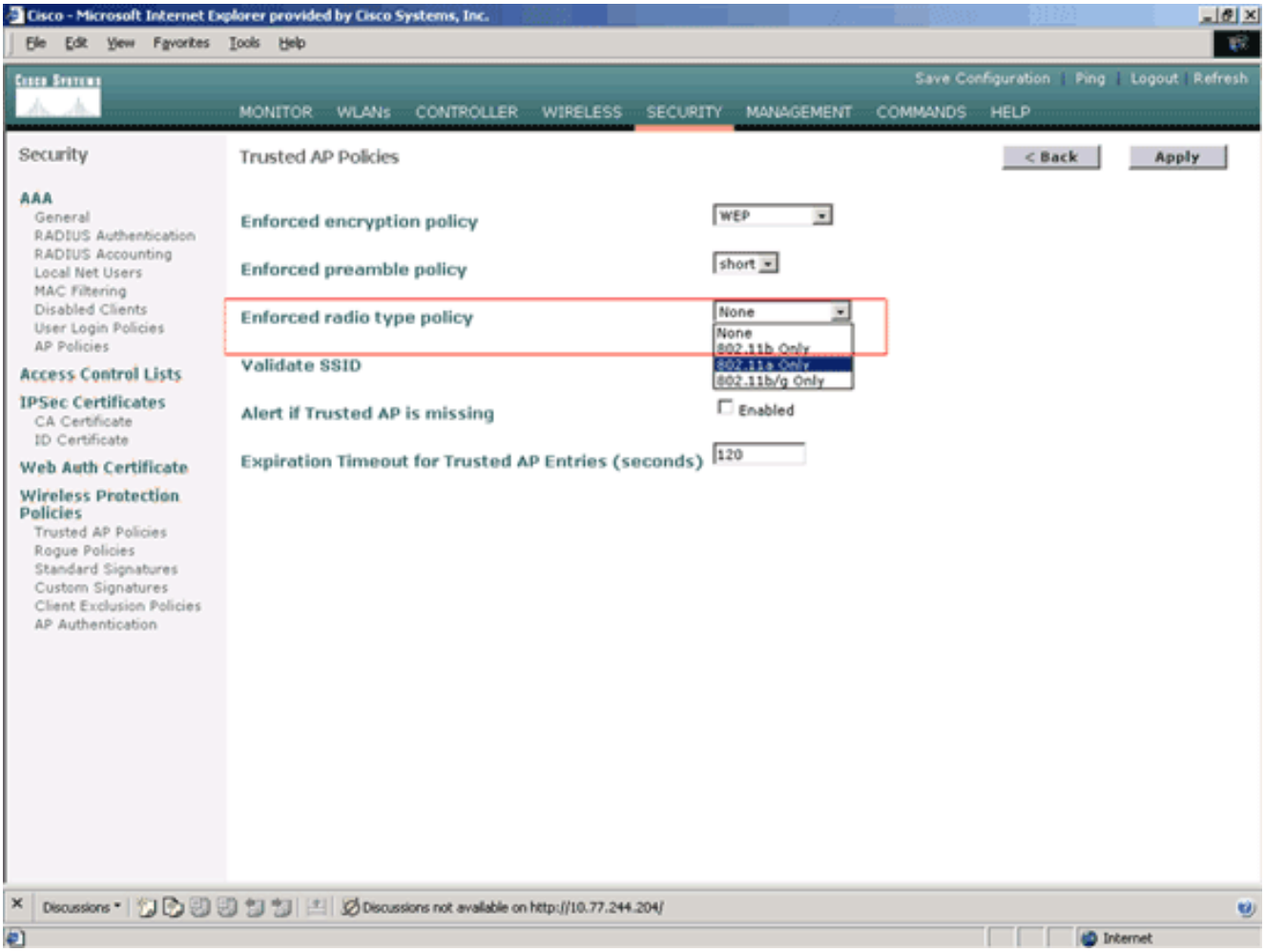
3. Selecteer in de pagina Betrouwbaar AP-beleid het gewenste coderingstype (Geen, Open, EVN, WAP/802.11i) in de vervolgkeuzelijst Afdwingingsbeleid.



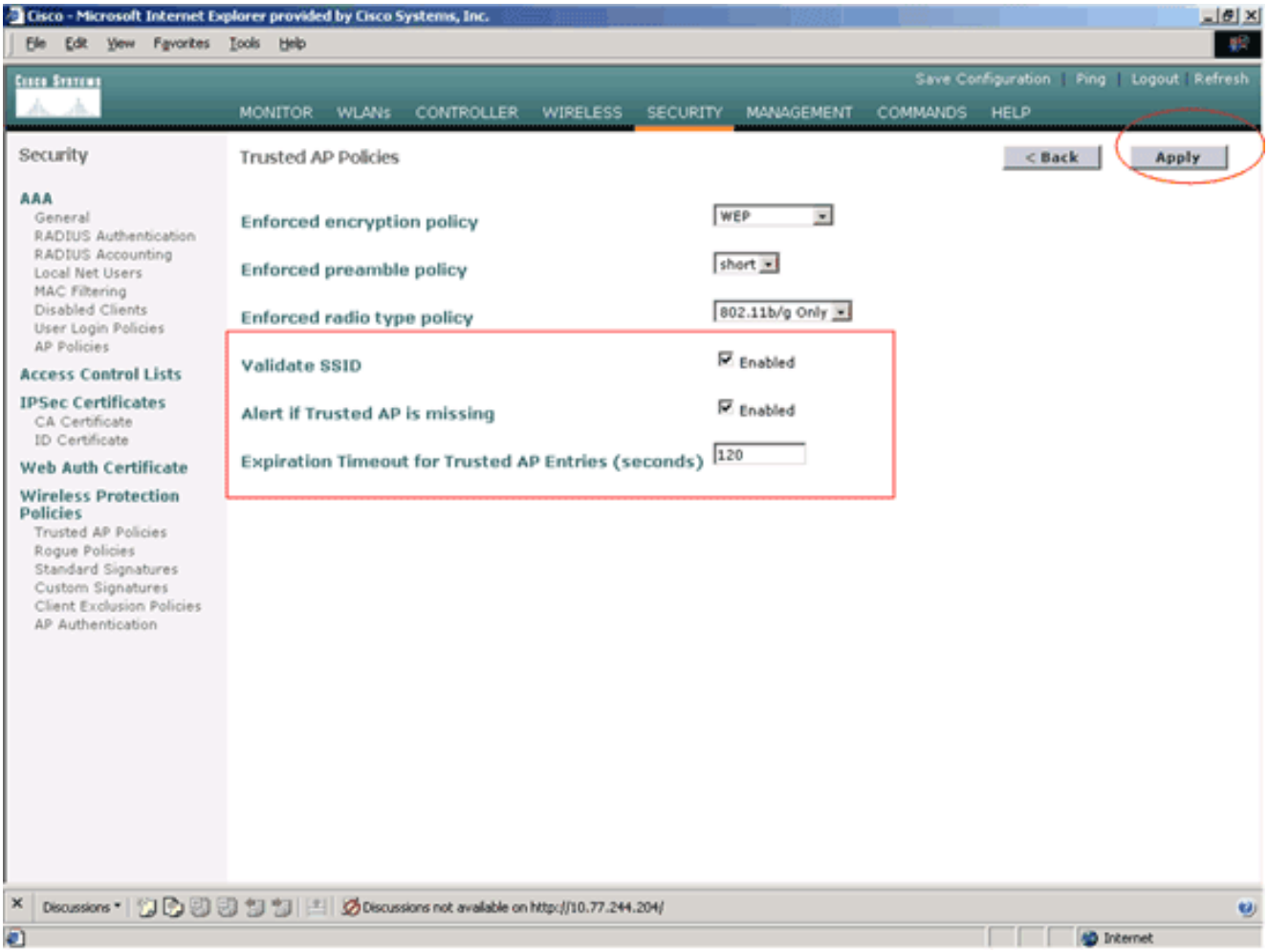
4. Selecteer het gewenste type preambule (Geen, Kort, Lang) in de vervolgkeuzelijst Afdruktype onderdeel Afbeeldingsbeleid
uitvoeren.



5. Selecteer het gewenste radiatype (alleen geen, 802.11b, 802.11a alleen, 802.11b/g alleen) in de vervolgkeuzelijst Toegedwongen radiobeleid.



6. Schakel het aanvinkvakje **SSID valideren** of uit om de instelling SSID valideren in of uit te schakelen.
7. Schakel de **waarschuwing** uit **als vertrouwde AP ontbreekt.** Schakel **het** aanvinkvakje **in** om de waarschuwing in te schakelen of uit te schakelen als vertrouwde AP ontbreekt.
8. Voer een waarde (in seconden) in voor de optie **Time-out bij** beëindiging **voor Trusted AP-items**.



9. Klik op **Apply** (Toepassen).

Opmerking: om deze instellingen te configureren vanuit de WLC CLI kunt u de **configuratie** van **de** WLC **vertrouwde-ap** opdracht gebruiken met de juiste beleidsoptie.

```
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.
```

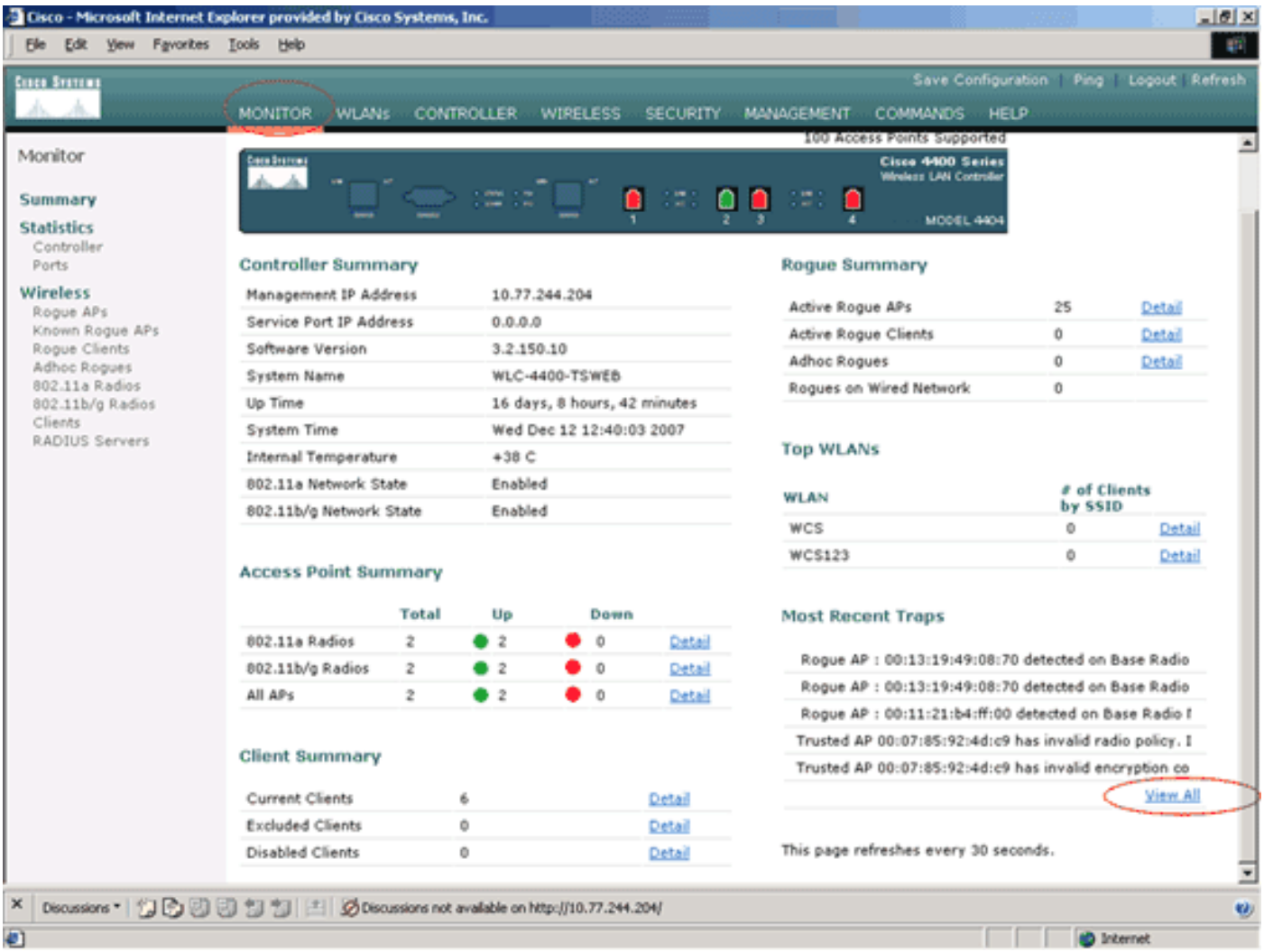
Trusted AP-waarschuwingsbericht

Hier is een voorbeeld van een betrouwbaar waarschuwingsbericht van AP-beleidsschending dat door de controller wordt getoond.

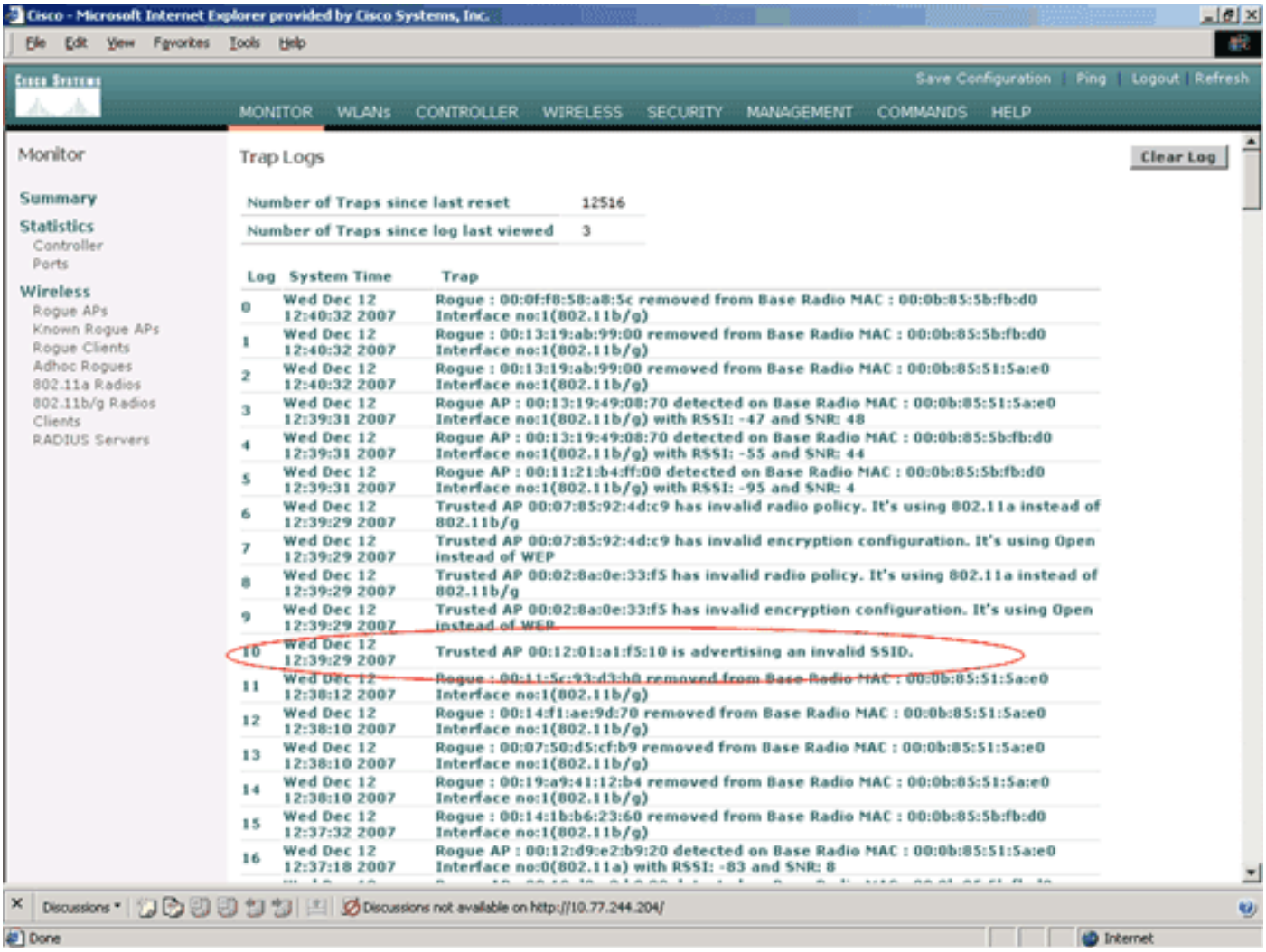
```
Thu Nov 16 12:39:12 2006  [WARNING] apf_rogue.c 1905: Possible AP
impersonation of xx:xx:xx:xx:xx:xx, using source address of
00:16:35:9e:6f:3a, detected by 00:17:df:7d:e1:70 on slot 0
 Thu Nov 16 12:39:12 2006  [SECURITY] apf_rogue.c 1490: Trusted AP Policy
failed for AP xx:xx:xx:xx:xx:xx - invalid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

Let hier op de gemarkeerde foutmeldingen. Deze foutmeldingen geven aan dat SSID en het coderingstype dat op de vertrouwde AP is ingesteld, niet overeenkomen met de Trusted AP-beleidsinstelling.

Hetzelfde waarschuwingsbericht kan worden gezien vanaf de WLC GUI. Ga naar het hoofdmenu van de WLC GUI en klik op **Monitor** om dit bericht te bekijken. In het gedeelte Recentste trappen van de pagina Monitor klikt u op **Alles bekijken** om alle recente waarschuwingen op de WLC te bekijken.



Op de pagina Recentste overgangen kunt u de controller identificeren die het vertrouwde waarschuwingsbericht voor AP-beleidsschending genereert zoals in deze afbeelding:



Gerelateerde informatie

- Cisco-configuratiegids voor draadloze LAN-controllers, release 5.2 - Routedetectie in RF-groepen mogelijk
- Cisco-configuratiegids voor draadloze LAN-controllers, release 4.0 - Beveiligingsoplossingen configureren
- Ruggendetectie onder Unified draadloze netwerken
- Ontwerphandleiding en implementatiehandleiding voor SpectraLink-telefoon
- Configuratievoorbeeld van draadloze LAN-verbinding
- Connectiviteit met probleemoplossing in een draadloos LAN-netwerk
- Verificatie van configuratievoorbeelden voor draadloze LAN-controllers
- Technische ondersteuning en documentatie – Cisco Systems