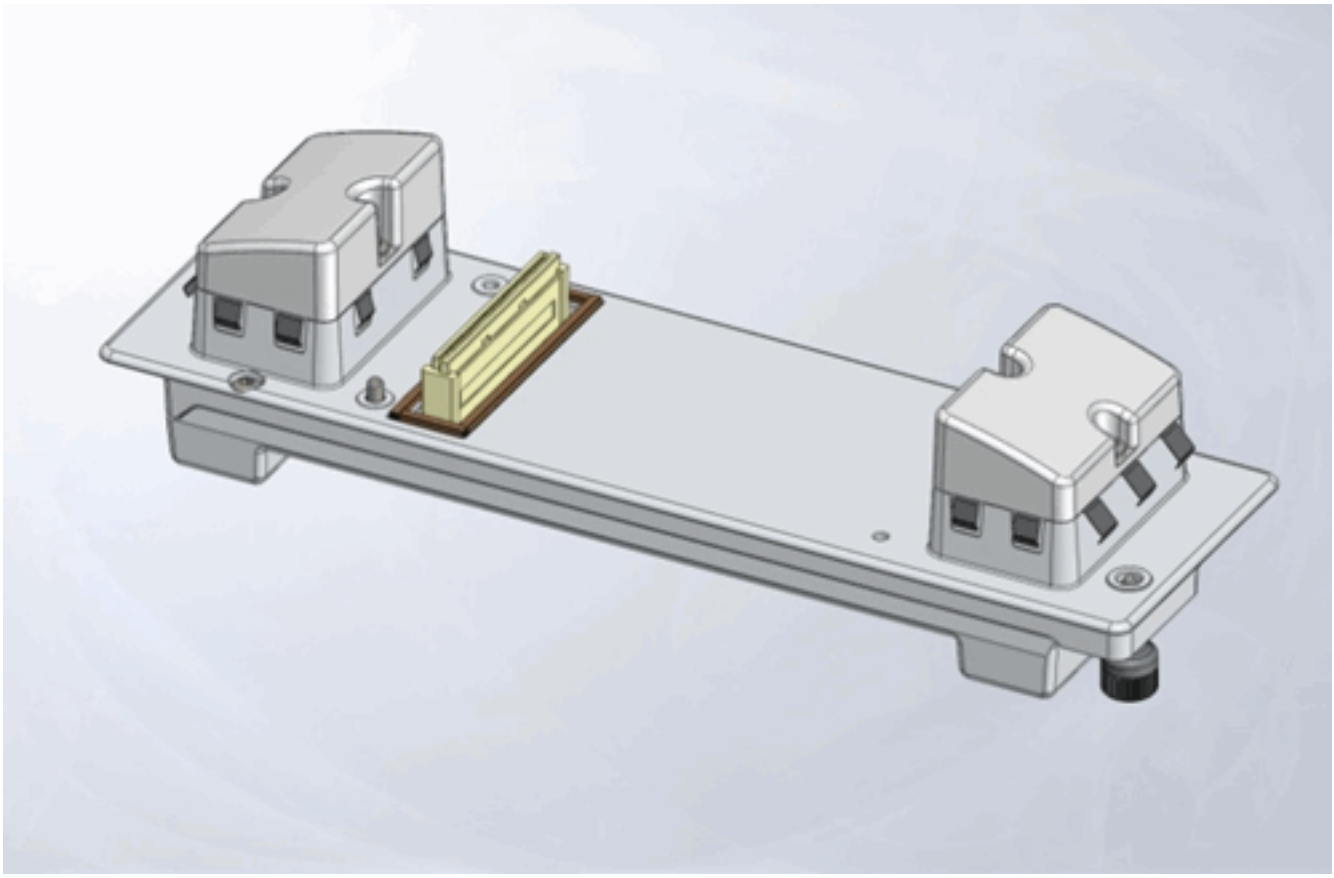
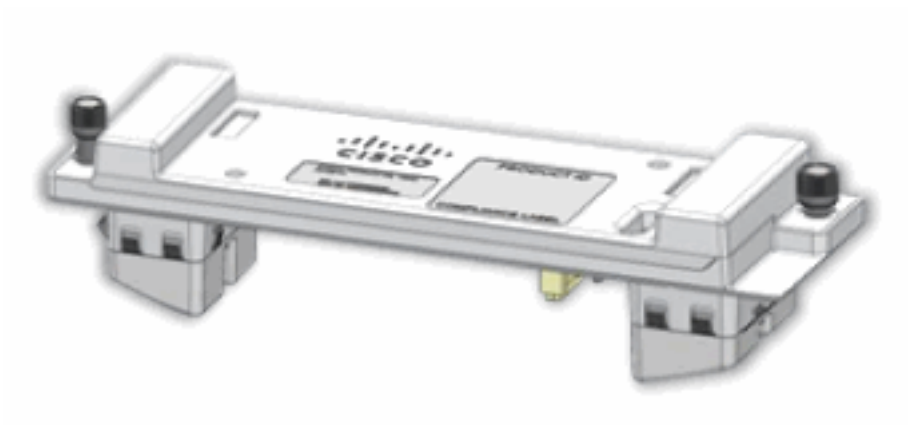
Aironet AP-module voor WSSI-implementatiegids

Inhoud

Inleiding

Dit document biedt algemene configuratie en implementatierichtlijnen voor Cisco Aironet access point module voor draadloze security en spectrumintelligentie (WSSI). WSSI is een add-on module die in modulaire access points (AP's) zoals Cisco 3600 Series AP kan worden ingevoegd.





Voorwaarden

Vereisten

Er zijn geen specifieke vereisten van toepassing op dit document.

Gebruikte componenten

De module voor draadloze beveiliging en spectrumintelligentie heeft de minimum codeversies nodig:

- Draadloze LAN-controller (WLC) - versie 7.4.xx.xx of hoger
- Access Point (AP) - versie 7.4.xx.xx of hoger
- Prime-infrastructuur (PI) - versie 1.3.xx.xx of hoger
- Mobility Services Engine (MSE) - versie 7.4.xx.xx of hoger

Conventies

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

Productoverzicht

De module Cisco Wireless Security and Spectrum Intelligence, die gebruik maakt van het flexibele modulaire ontwerp van Cisco Aironet 3600 Series AP, levert ongekend, altijd-on security scannen en spectrumintelligentie. Dit helpt u interferentie met radiofrequentie (RF) te voorkomen, zodat u betere dekking en prestaties krijgt op uw draadloze netwerk.

- 24 x 7 volledige spectrumbewaking en -beperking voor WIPS, schone lucht, contextbewustzijn, detectie en beheer van radiobronnen

- 24 x 7 on-kanaals WIPS-bedreigingsbescherming
- 23 keer meer veiligheid en spectrumdekking
- 30%+ CAPEX kostenbesparingen in vergelijking met AP voor speciale monitor
- Aanraakconfiguratie op nul stellen

De WSSI-module voor veldomzetting is een speciale radio die alle bewaking- en beveiligingsdiensten van de client/gegevens die radio's aan de beveiligingscontrolemodule doorgeeft, verwijdert. Dit maakt niet alleen betere clientprestaties mogelijk, maar vermindert ook de kosten door de noodzaak te elimineren van speciale monitormodus AP's en de Ethernet-infrastructuur die nodig is om deze apparaten in hun netwerk aan te sluiten.

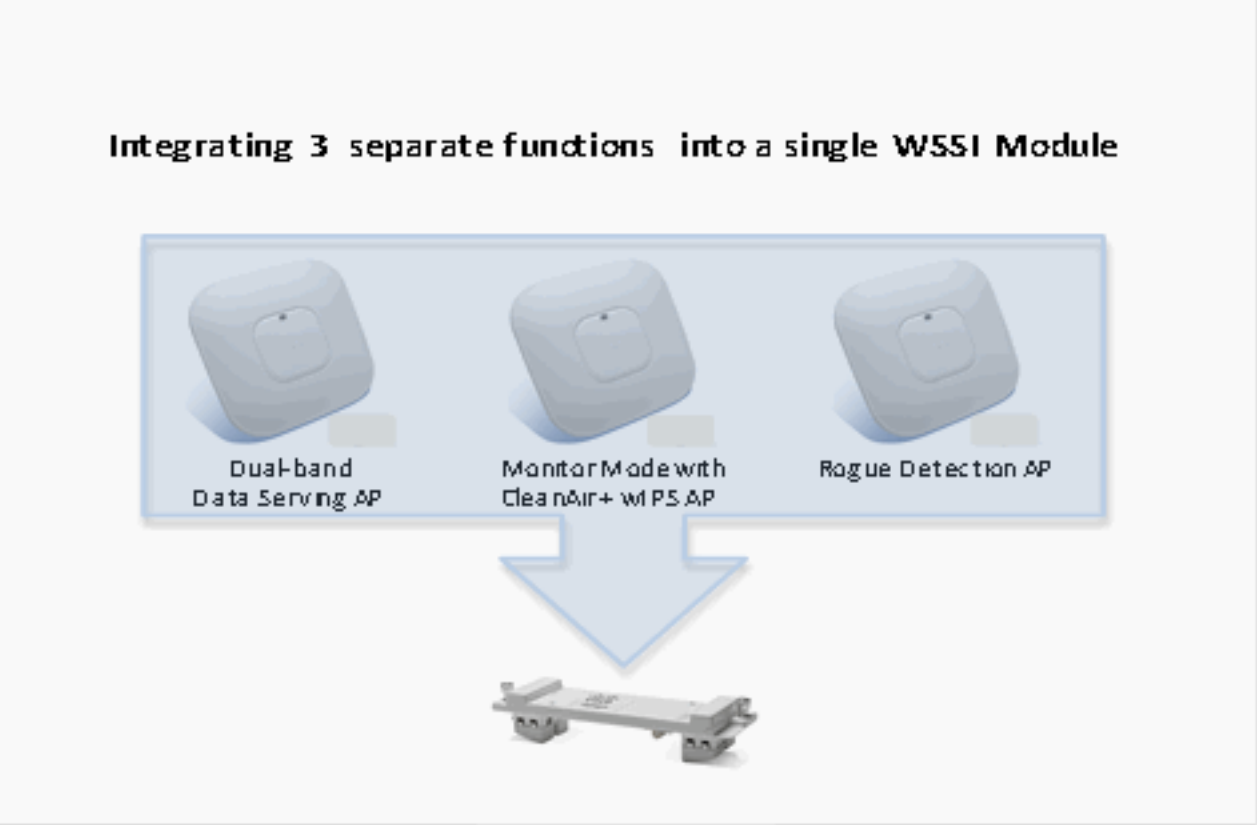
Samen stellen de 3600 Series APs en WSSI module u in staat om gelijktijdig state-of-the-art veiligheids- en spectrumanalysefuncties te bieden voor Wi-Fi-clients op alle kanalen, in zowel de 2,4-GHz als de 5-GHz banden.

Wanneer de module wordt ingezet, scant hij constant alle kanalen om de best veilige en robuuste draadloze ervaring die in de industrie beschikbaar is te verzekeren.

Voordelen van WSSI-modus

Uitgebreide lokale modus (ELM):

- Vermindert netwerkkosten en bewerkingen. Door de WSSI-module in de 3600-serie te integreren, kunt u maximaal drie afzonderlijke apparaten vervangen. Dit biedt drie afzonderlijke functies in één enkele, multifunctionele 3600 Series

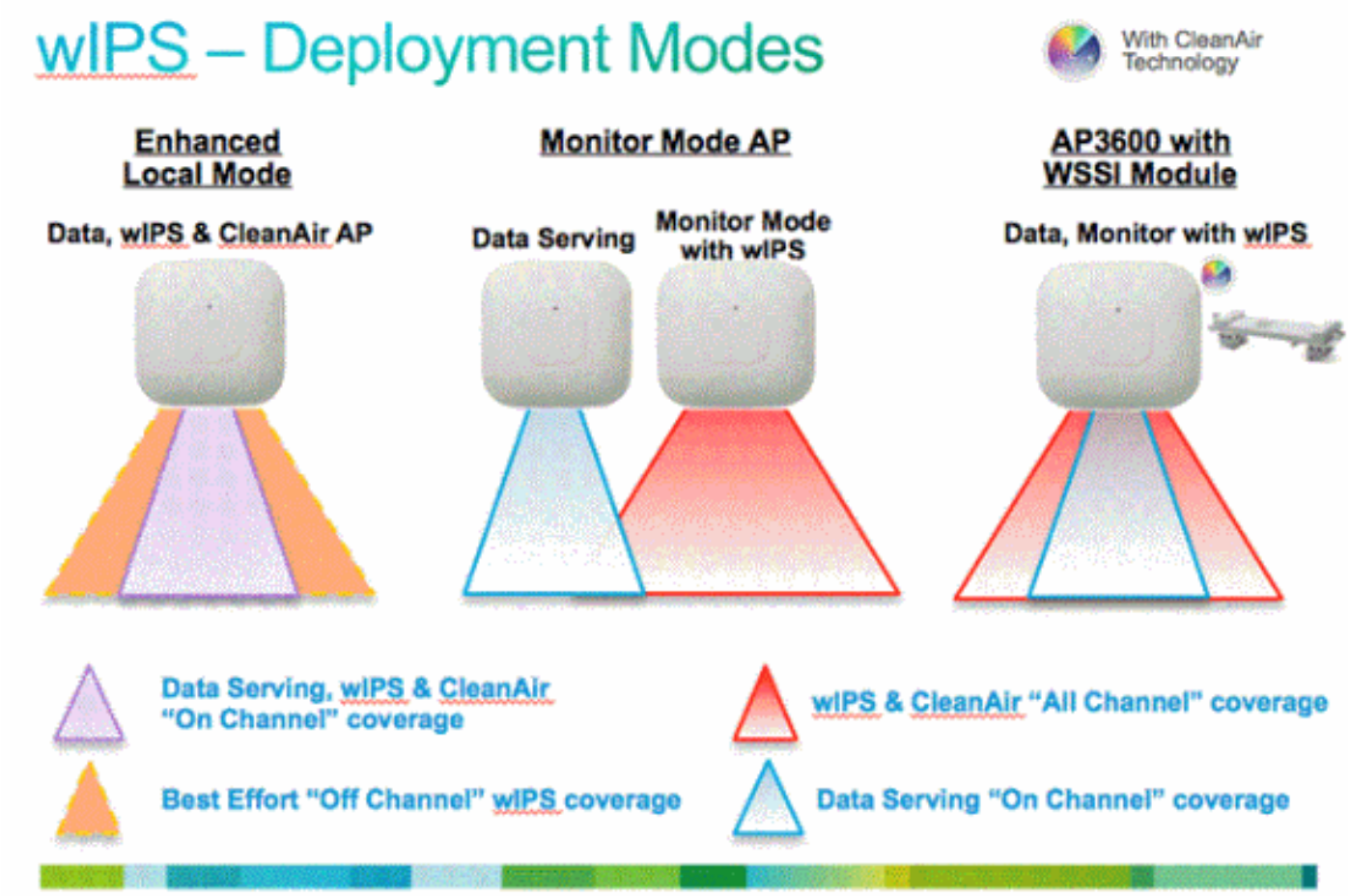


AP.
- Klanten kunnen nu één Ethernet-verbinding (kabel en poort) gebruiken in hun bekabeld netwerk, in plaats van wat typisch tot drie afzonderlijke Ethernet kabels en een toegangshaven in hun bekabeld netwerk zou vereisen. Dit vermindert hun CAPEX aanzienlijk.
- Door al deze functies in één AP te integreren, vereenvoudigen klanten het dagelijkse beheer en de controle van hun draadloze infrastructuur en netwerk met een zeer beperkt aantal APs.

De WSSI-module lijkt op de WLC- en beheersystemen als een extra radio ter ondersteuning van 802.11b/g/a/n-clientapparaten (2,4 en 5 GHz) binnen de specifieke 3600 Series AP.

- *Aanraakconfiguratie op nul zetten*, Installatie, Aan/uit en ga. Er is absoluut geen configuratie vereist om de WSSI-module in bedrijf te stellen, en onmiddellijk uw draadloze netwerk te controleren en te beveiligen. De WSSI-module wordt ingevoegd en beveiligd met AP van 3600 Series. Wanneer het AP wordt aangedreven wordt de module gelanceerd samen met de andere radio's in het AP en begint onmiddellijk met het controleren van alle kanalen op zowel 2,4 als 5 GHz op mogelijke veiligheidsbedreigingen en bronnen van interferentie.
- Adaptieve wIPS biedt een nauwkeurige en efficiënte detectie van bedreigingen op alle kanalen van overluchtaanvallen, schurkenblabders en ad-hocverbindingen, evenals de mogelijkheid om de classificatie, kennisgeving, beperking en rapportage voor constant toezicht en proactief beheer te classificeren. Werkt in combinatie met Cisco Mobility Services Engine (MSE).

ELM:



- Hiermee voegt u IPS security scannen toe voor 7x24 bij kanaalscannen (2,4 GHz en 5 GHz), met ondersteuning voor kanalen.
- Dankzij de AP worden klanten ook bediend en dankzij de G2 Series van AP's kan er op kanalen (2,4 GHz en 5 GHz) een spectrumanalyse worden uitgevoerd.

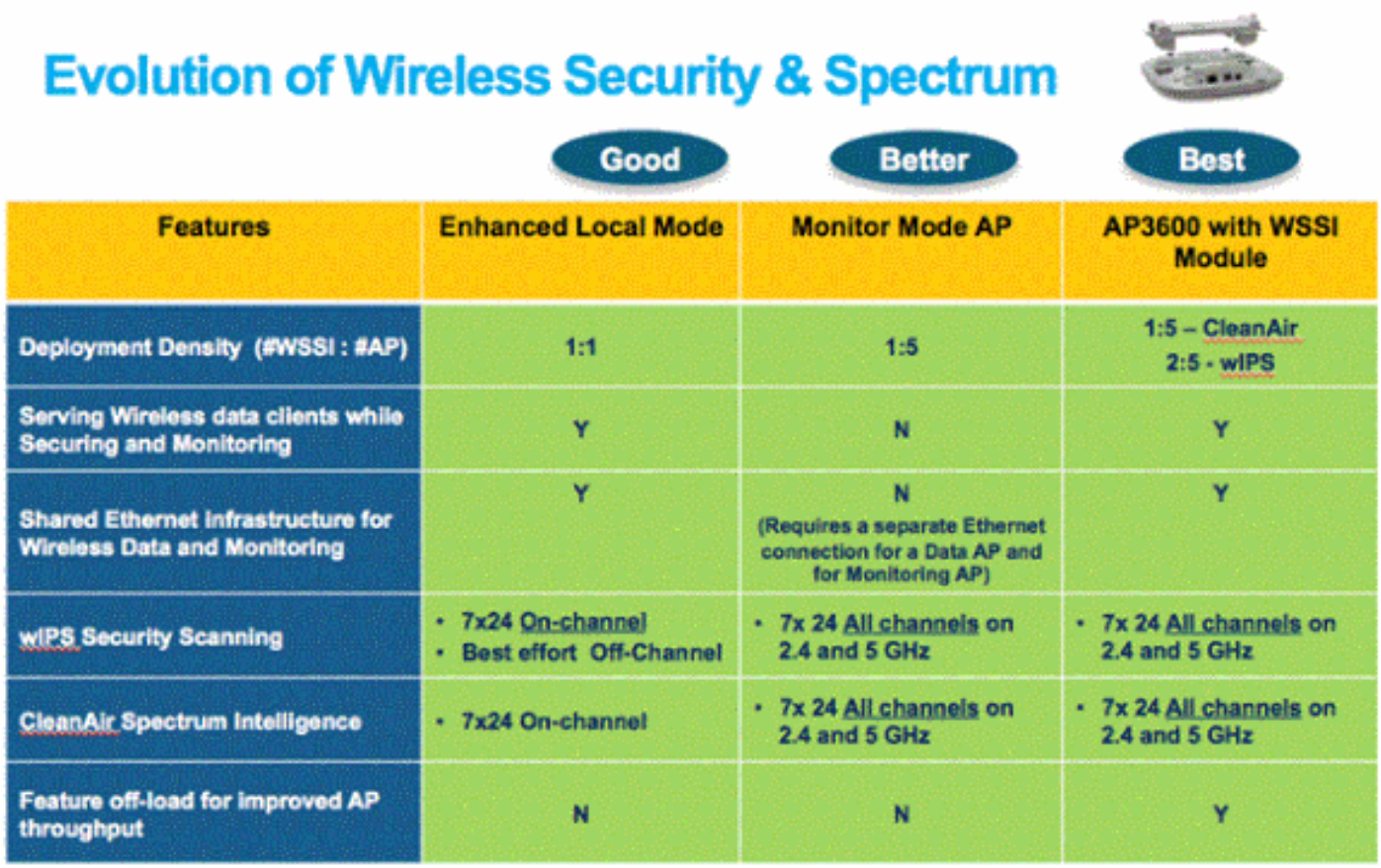
Monitormodus:

- De Monitor Mode AP (MMAP) is gewijd aan de bediening in Monitor Mode en heeft de optie om wIPS security scannen van alle kanalen (2,4 GHz en 5 GHz) toe te voegen.
- De G2-Series van AP's maakt het mogelijk om het spectrum op alle kanalen te analyseren (2,4 GHz en 5 GHz).

- MMAP's dienen geen klanten.

AP3600 met WSSI-module: De evolutie van draadloze beveiliging en spectrum

- Het eerste AP van de industrie dat de gelijktijdige klantenservice, het scannen van de veiligheid en de spectrumanalyse vergemakkelijkt met behulp van CleanAir Technology.
- Speciale 2,4 GHz- en 5 GHz-radio met zijn eigen antennes die het scannen van alle draadloze kanalen in de 2,4 GHz- en 5 GHz-banden mogelijk maken.
- Een enkele Ethernet-infrastructuur biedt vereenvoudigde werking met minder apparaten om het rendement op investeringen van de AP3600 draadloze infrastructuur en de Ethernet bekabelde infrastructuur te beheren en te optimaliseren.



- Cisco CleanAir Technology: biedt proactieve hogesnelheidsspectrumintinformatie om prestatieproblemen als gevolg van draadloze interferentie te bestrijden. De eerste state-of-the-art technologie voor RF-analyse die de energiepatronen (handtekeningen) van apparaten die de kwaliteit van een draadloos netwerk aanzienlijk kunnen beïnvloeden, inspecteert en classificeert.
- Radio Resource Management (RRM): Dankzij het vereenvoudigde, geavanceerde RF-beheer wordt automatisch aangepast aan de draadloze netwerkomgeving op basis van de informatie die wordt ontvangen van Cisco CleanAir Technology. Zodra interferenten zijn geïdentificeerd kan RRM clientapparaten verplaatsen om afstand te bewaren tot de interferentie en de doorvoerkracht aanpassen om afstand te doen van de bron van interferentie. Dit biedt een betere RF-kwaliteit voor de gebruiker.
- Ruggendetectie: detecteert en meldt de toegang tot het netwerk in de achterdeur en de toegang tot draadloze klanten.
- Locatie en contextbewustzijn: biedt realtime bewustzijn en de mogelijkheid om draadloos endpoints op te sporen.

Dankzij deze functies biedt de module Cisco Wireless Security and Spectrum Intelligence, in

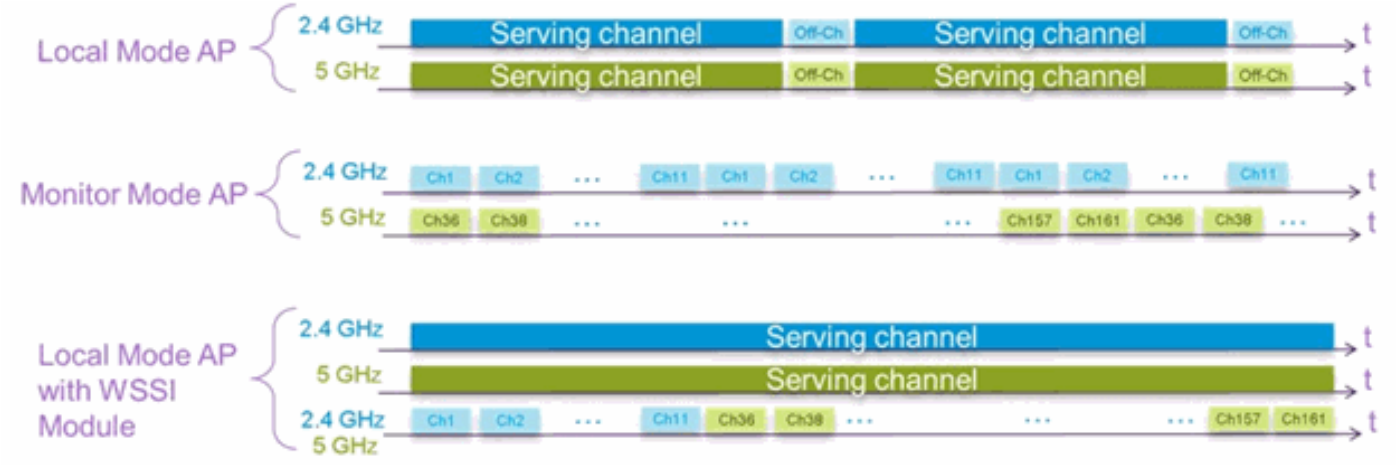
combinatie met Cisco 3600 Series AP, het best beveiligde en robuuste draadloze netwerk van ondernemingsklasse mogelijk voor uw zakelijke gebruikers en gegevens.

On-channel vs. Off-channel gebruik van de WSSI-module

Een lokale modus AP scans voor CleanAir interferers en WIPs aanvallen op het kanaal. Dit betekent dat AP alleen het kanaal scant dat het bedient. Een lokale mode AP met een 2,4 GHz radio die kanaal 1 en 5 GHz radio uitzendt, biedt alleen bescherming op kanalen 1 en 64.

Een MMAP-scan voor CleanAir interferers en WIPs-aanvallers buiten het kanaal. Dit betekent dat AP alle kanalen scant. De 2,4 GHz radio scant alle 2,4 GHz kanalen en het 5 GHz kanaal scant alle 5 GHz kanalen.

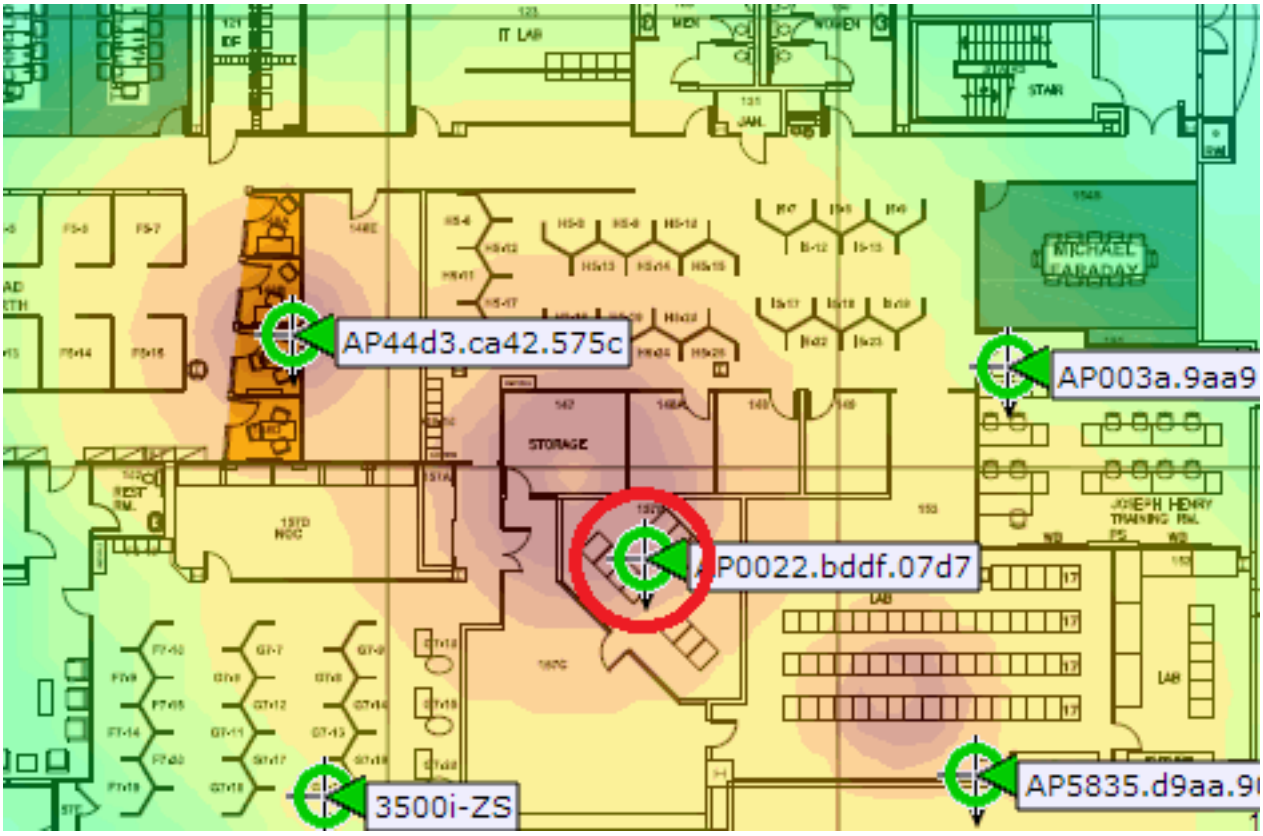
Cisco 3600 Series AP gebruikt een combinatie van on-kanaal en off-kanaal. De 2,4 GHz- en 5 GHz-radio's scannen op kanaal en de WSSI-module scans off-kanaal, waarbij wordt gescand tussen alle 2,4 GHz- en 5 GHz-kanalen.



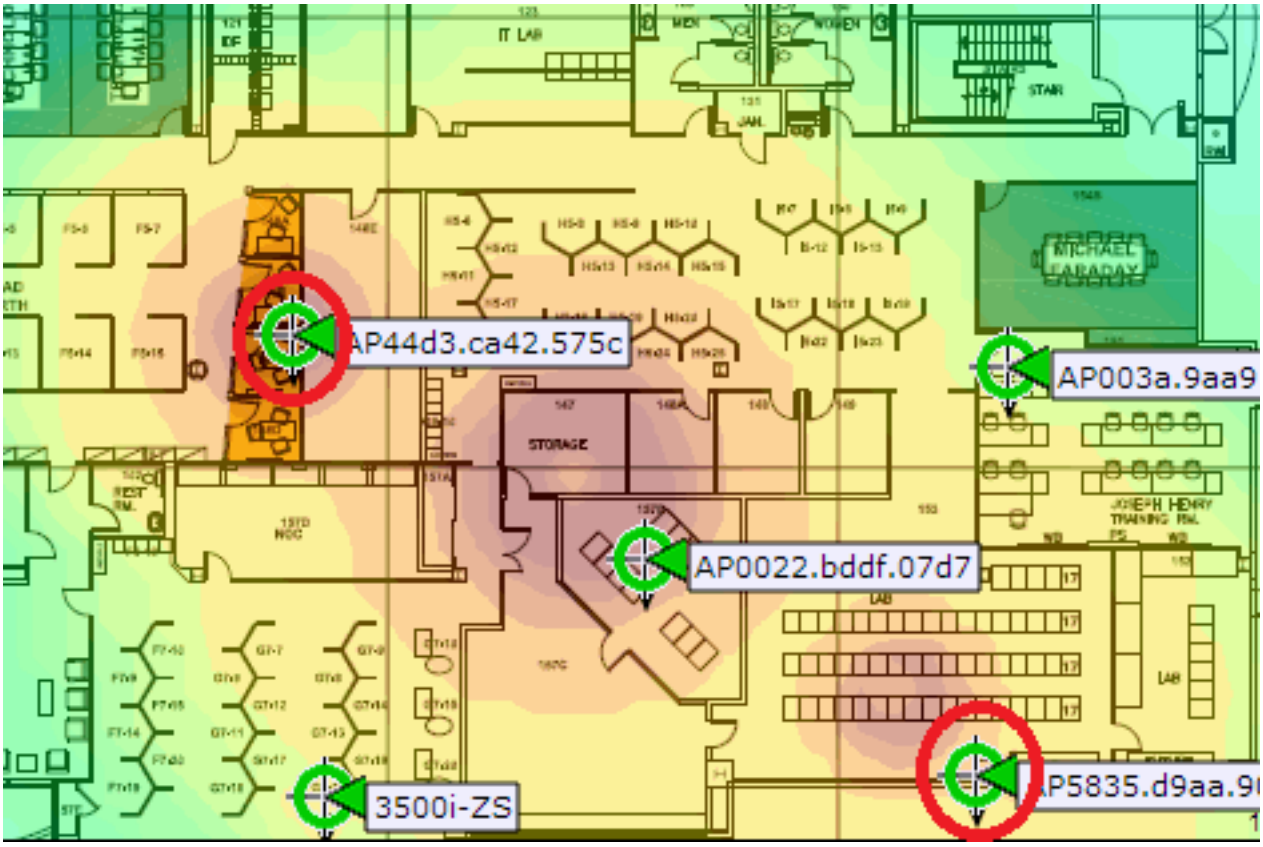
Aanbevolen implementatiedichtheid voor de WSSI-module

In traditionele AP van de monitor plaatsing, adviseert Cisco een verhouding van 1 MMAP aan elke 5 lokale wijze APs. Dit kan variëren op basis van netwerkontwerp en deskundige begeleiding voor de beste dekking. Met de WSSI-module zijn er verschillende implementatieaanbevelingen gebaseerd op functionaliteit om dekking pariteit met een MMAP te bereiken.

Voor CleanAir wordt aanbevolen om 1 WSSI-module te implementeren voor elke 5 lokale of Flexconnect AP's. Deze 1:5-inzet biedt dezelfde prestaties als een CleanAir-enabled MMAP, maar laat nog steeds AP toe om klanten te dienen. Dit is een aanbevolen inzet voor een WSSI-module die CleanAir uitvoert:

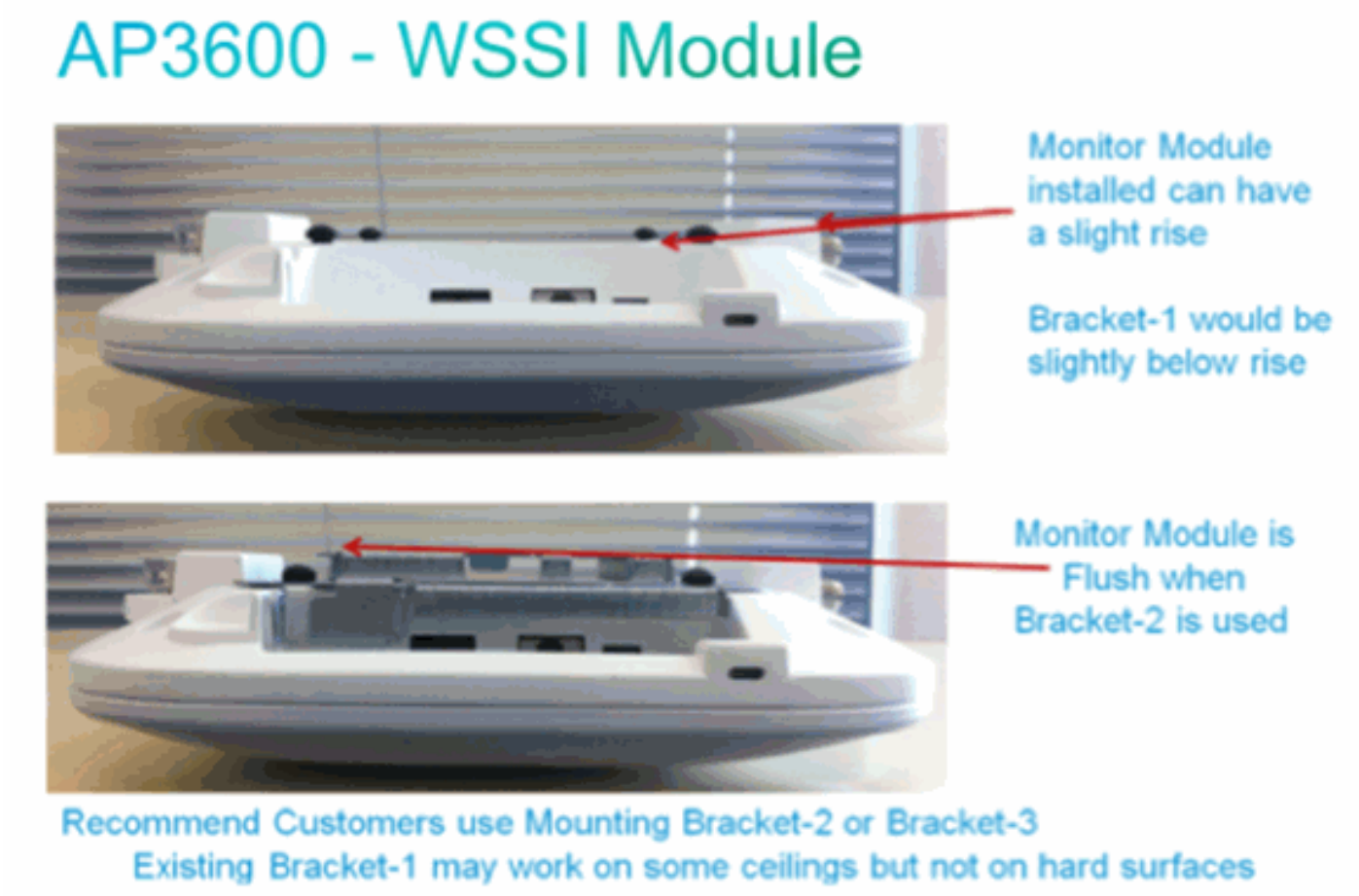


Voor WIPS-bescherming wordt aanbevolen 2 WSSI-modules in te stellen voor elke 5 lokale of FlexConnect APs. De wIPS-detectietijd voor een off-kanaal aanval is ongeveer twee keer die van een MMAP. Daarom is een 2:5-toepassing vereist om wIPS-detectiepariteit te bieden. Dit is de aanbevolen inzet voor een WSSI-module die wIPS-bescherming uitvoert:



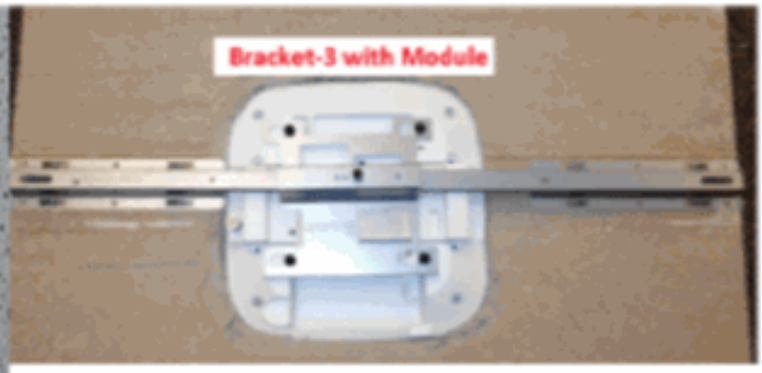
Cisco 3600 AP met een WSSI module gebruikt zowel on-kanaal als off-kanaal scanning om een industrie leidende oplossing te bieden terwijl het dienen van cliënten.

[De WSSI-module installeren]



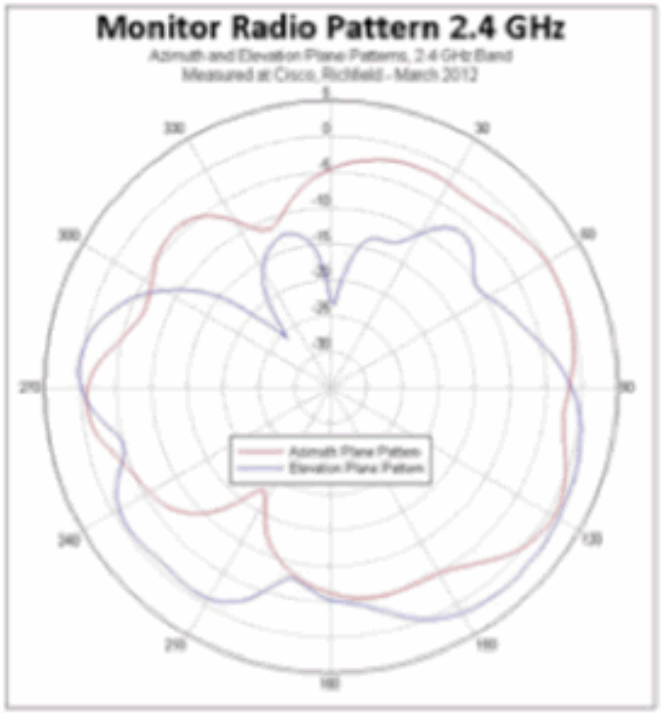
AP3600 with WSSI Module and Bracket-3

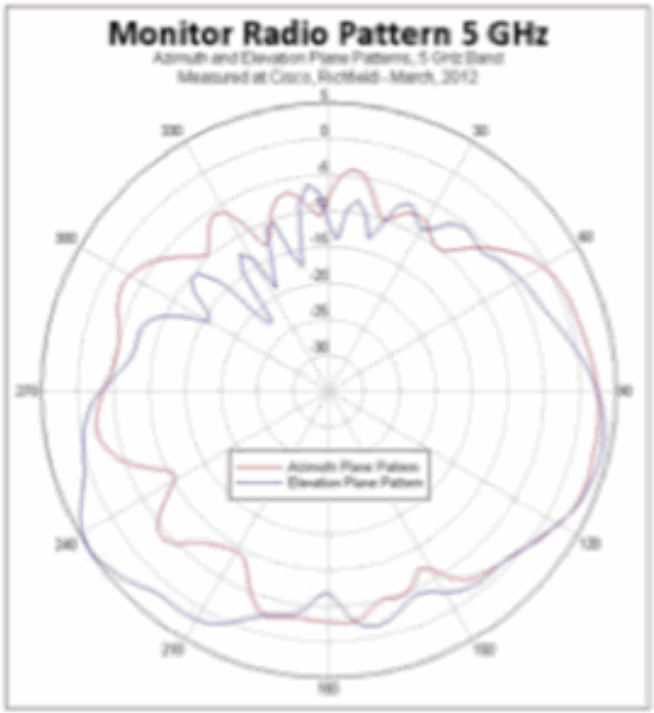
Elegant in-tile flush mount



Monitor Module easily integrates into Bracket-3. Since it spans two tile rails it distributes the weight and is an ideal bracket for use in earthquake prone areas. The bracket and AP can also be supported with a wire to the "I" beams or support structures

WSSI Module Antenna Patterns





Configuratie voor de AP3600 WSSI-module

Er is geen configuratie voor de WSSI-module nodig. De module scant automatisch alle kanalen op beide banden met 0x4 (slechts ontvangen) 0 Tx Antennes x 4RX Antennes.

Merk op dat de WSSI-module alleen actief is op AP3600s, geconfigureerd in of Local Mode of FlexConnect-modus. De WSSI-module is uitgeschakeld in alle andere modi.

Voedingseis voor de WSSI-module

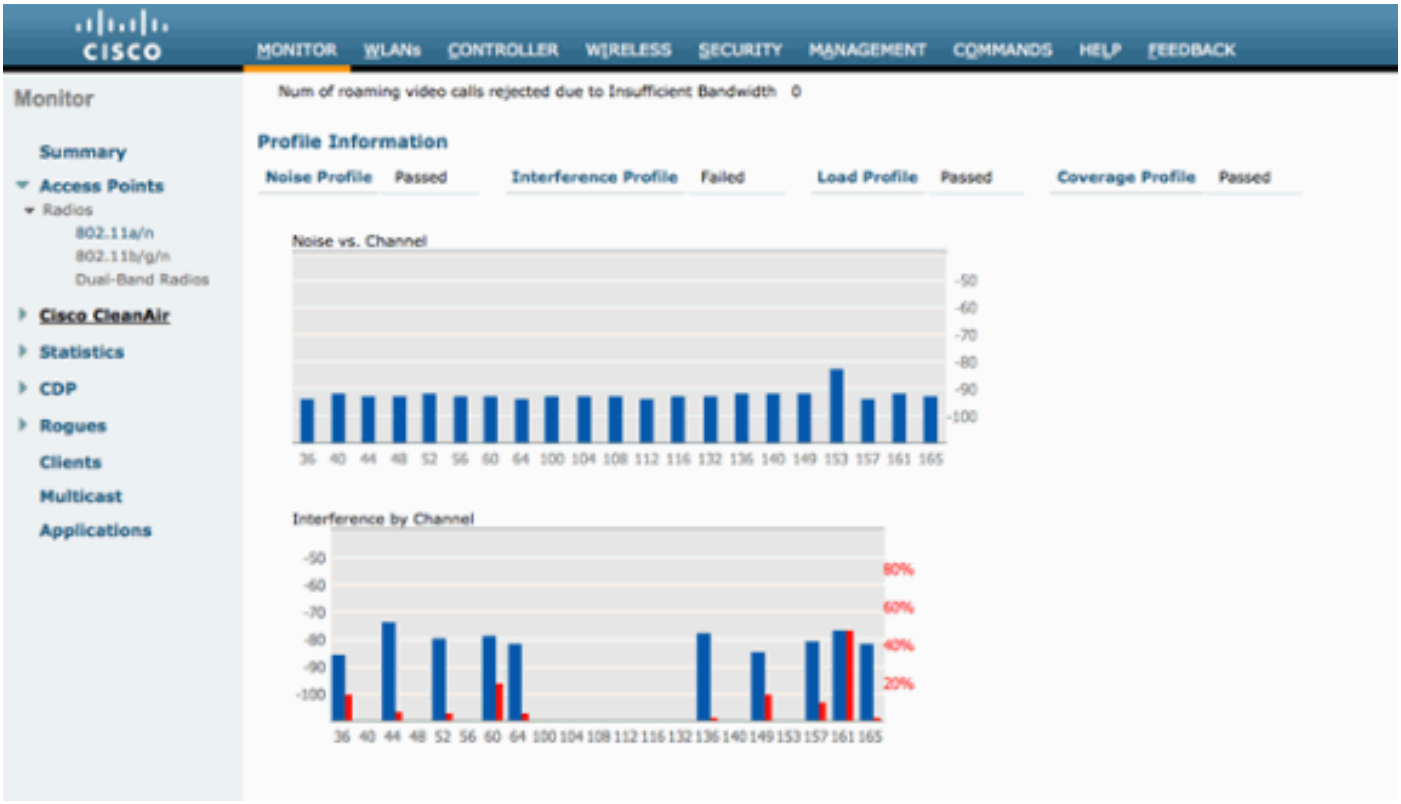
De AP3600 met een geïnstalleerde WSSI module overschrijdt 15.4 Watts (802.3af). AP vereist of (802.3at - PoE+), Uitgebreide PoE, een lokale AC voeding of de Cisco PoE injector (AIR-PWRINJ4).

Opmerkingen:

- Enhanced PoE is gemaakt door Cisco en een voorloper van 802.3at PoE+. Het levert maximaal 20 W vermogen.
- PoE+ kan een stroomverbruik van maximaal 30 W opleveren.

Radio Resource Management op de WSSI-module

De WSSI-module neemt alle RRM-metingen op zowel de 2,4 GHz-band als de 5 GHz-band. De metingen worden in de WLC GUI weergegeven onder ofwel Monitor > Access Point > 802.11a/n > AP_NAME > Details of monitor > Access points > 802.11b/g/n > AP_NAME > Details.



Reiniging van de lucht op de WSSI-module

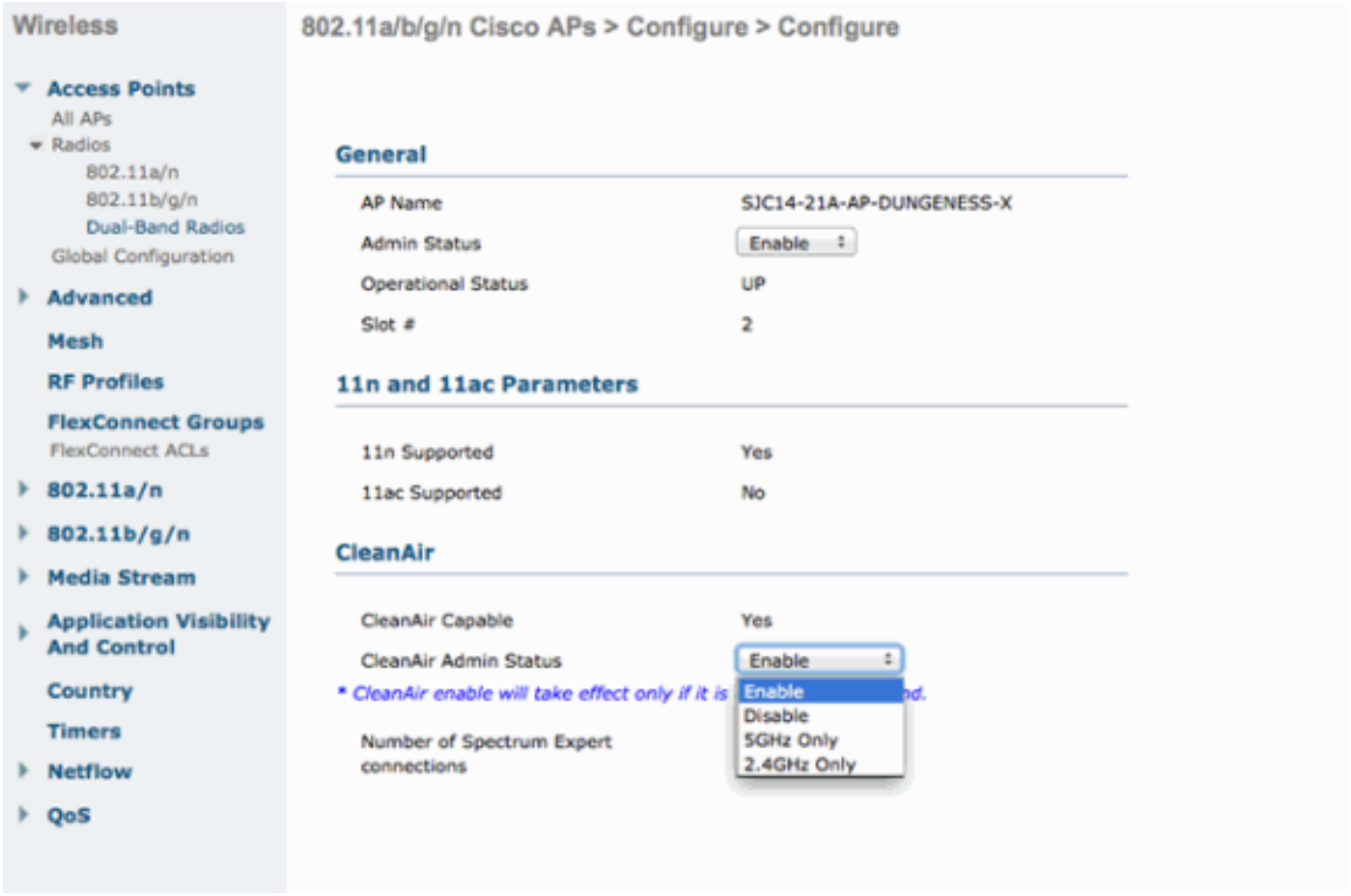
De WSSI-module detecteert CleanAir interferers met dezelfde precisie als een MMAP. Cisco raadt aan de WSSI-module te implementeren met een dichtheid van 1:5, waar er 1 WSSI-module moet zijn voor elke 5 AP's. Dit is dezelfde aanbevolen dichtheid als voor een MMAP.

Wanneer de WSSI-module zonder submodus is ingeschakeld, scant de module zowel de 2,4 GHz band als de 5 GHz band. De module hangt af van elk kanaal, gedurende 1,2 seconden en scans voor reinigingsmiddelen.

CleanAir kan alleen worden ingeschakeld op 2,4 GHz, alleen 5 GHz en zowel 2,4 GHz als 5 GHz. Dit kan worden geselecteerd vanuit de WLC CLI of GUI. Hier is een voorbeeld van het configureren van CleanAir op de WLC CLI:

```
(Cisco Controller) >config 802.11-abgn cleanair enable APNAME 2.4GHz
(Cisco Controller) >config 802.11-abgn cleanair enable APNAME 5GHz
```

Dezelfde configuratie kan op de GUI worden toegepast via draadloze > dubbele-band radio's > Configureren. Hier is een voorbeeld van:



Om te controleren of de CleanAir-interferer werd gedetecteerd door de WSSI-module, geeft u het bevel **over** de **show** reinigingsinterferers uit de AP-console uit:

```
SJC14-21A-AP-DUNGENESS-X# show cleanair interferers
CleanAir: slot 0 band 2.4 number of devices 0:
CleanAir: slot 1 band 5.0 number of devices 0:
CleanAir: slot 2 band 2.4 number of devices 0:
CleanAir: slot 2 band 5.0 number of devices 1:
IDR: 24(3159) Video Camera
     ISI=0, -74 dBm, duty=100
     c=00180000 sig(4)=1057CA80
     on/report/seen 22/22/22 secs ago
```

Dezelfde configuratie kan op de GUI worden toegepast via draadloze > dubbele-band radio's > Configureren. Hierna volgt een voorbeeld:

De interferenten met CleanAir worden gemeld op de WLC GUI. Interfermers worden per BAND weergegeven. Dit betekent dat interferenten die op de WSSI-module op de 5 GHz-band worden gedetecteerd, worden weergegeven onder monitor > 802.11a/n > Interference Devices.

Om te controleren of de CleanAir interferer werd gedetecteerd door de WSSI-module, geeft u de **show-reinigingsinterferers** uit de AP-console af:

```
SJC14-21A-AP-DUNGENESS-X# show cleanair interferers
CleanAir: slot 0 band 2.4 number of devices 0:
CleanAir: slot 1 band 5.0 number of devices 0:
CleanAir: slot 2 band 2.4 number of devices 0:
CleanAir: slot 2 band 5.0 number of devices 1:
IDR: 24(3159) Video Camera
     ISI=0, -74 dBm, duty=100
     c=00180000 sig(4)=1057CA80
     on/report/seen 22/22/22 secs ago
```

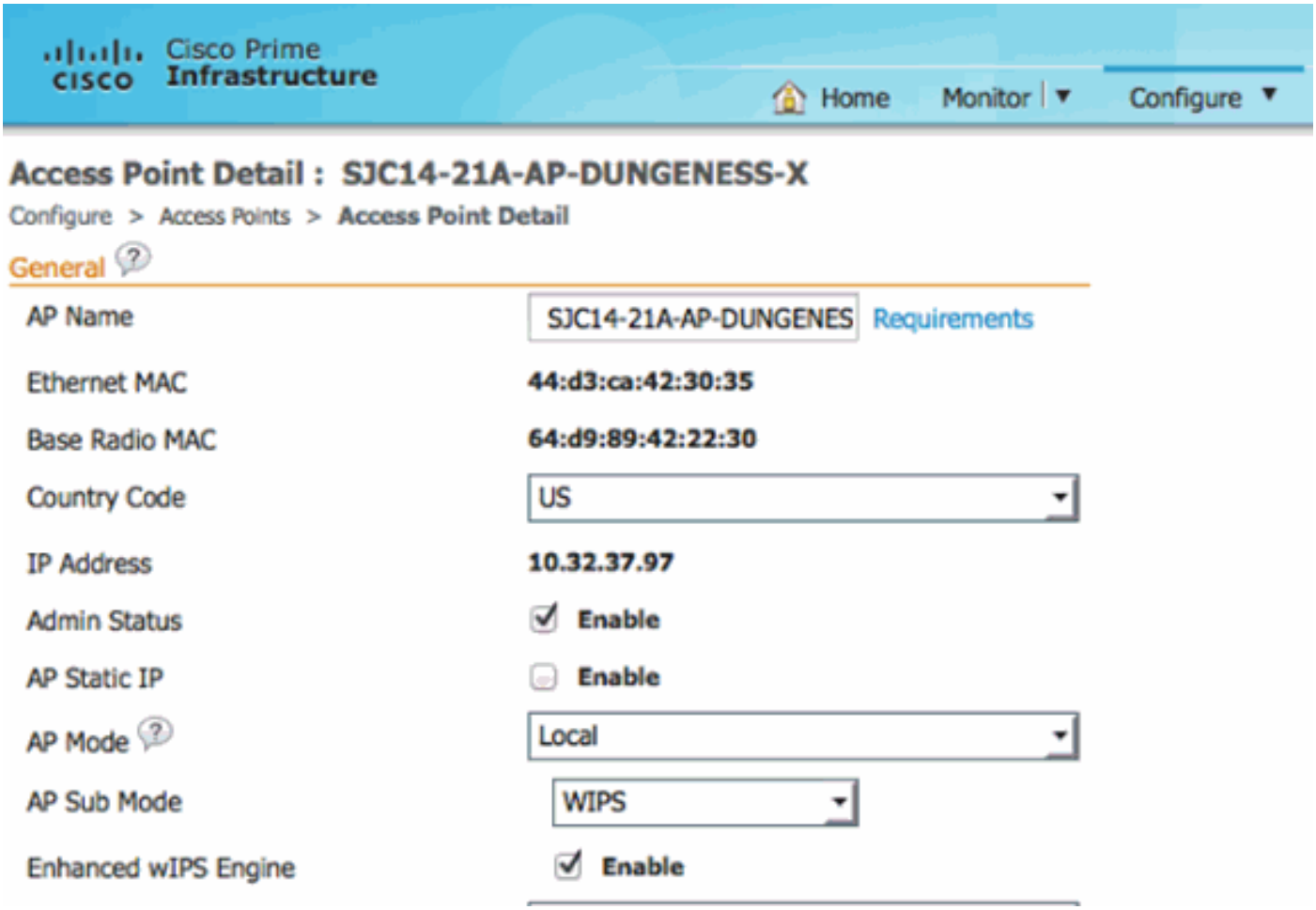
IPS op de WSSI-module

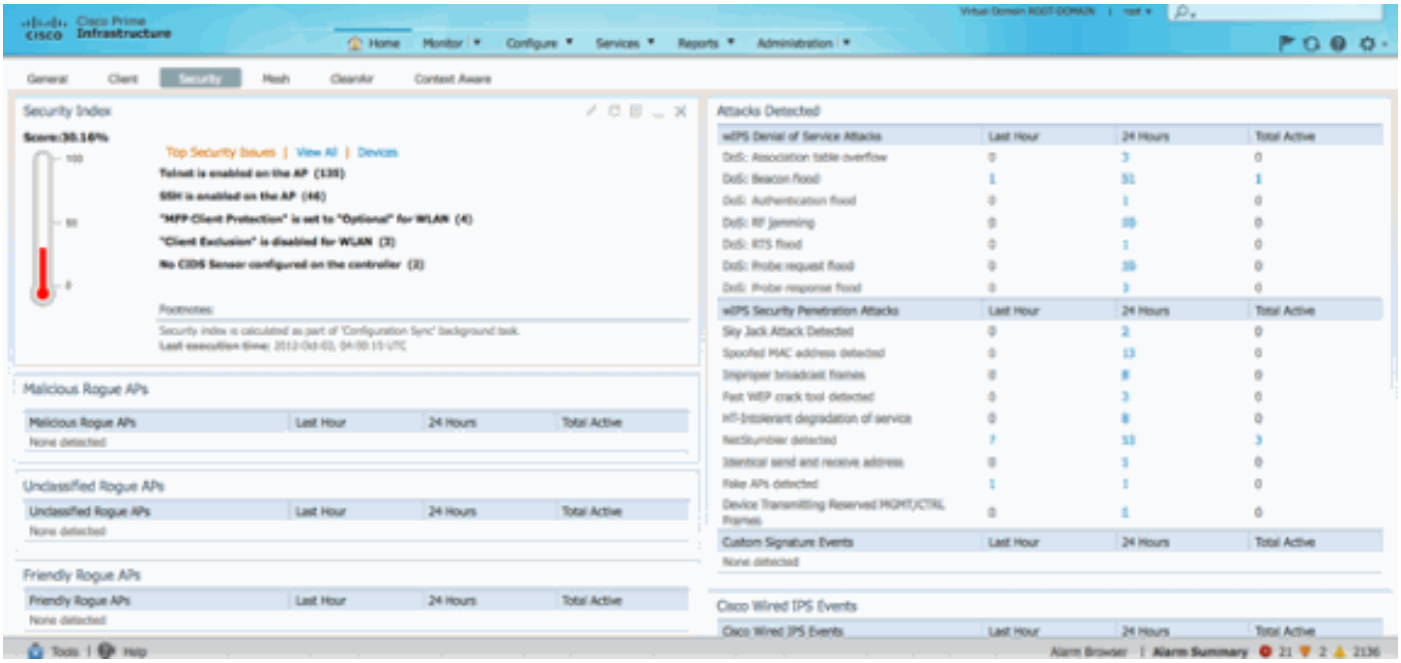
De WSSI-module detecteert wIPS-aanvallers met bijna dezelfde precisie als een MMAP. Voor wIPS, adviseert Cisco het opstellen van de WSSI module met een 2:5 verhouding tussen APs. Dit betekent dat voor elke 5 AP's twee AP's de WSSI module moeten bevatten.

Er zijn twee wIPS-modi die kunnen worden geconfigureerd:

- Met IPS-submodus - hiermee kan IPS-aanvallen worden gedetecteerd en alle kanalen voor 1.2s worden gescand. In deze modus kan AP nog steeds alle RRM rapporten opnemen naast wIPS-detecties.
- Uitgebreide wIPS-modus - Schakel IPS-detectie in en scant alle kanalen voor 250ms. De kleinere tijd van het kanaal staat de veiligheidsmodule toe om aanvallers sneller te detecteren.

Ga vanuit de PI-pagina (Prime Infrastructure) naar Configure > Access points > AP_NAME. De WSSI-module kan worden geconfigureerd voor de volgende IPS-submodus of voor de volgende IPS-submodus + uitgebreide ondersteuning voor IPS-engine. Dit kan ook worden geduwd als deel van een AP configuratie sjabloon.





De wIPS-aanvallen worden weergegeven in het tabblad Prime-infrastructuur van het tabblad Home > Security.

De IP geeft een op het netwerk gebaseerde weergave weer, maar u kunt de aanval op een AP3600 met een WSSI-module weergeven door de opdracht **showcapwap am ALARM_NUM** uit de AP-console uit te geven.

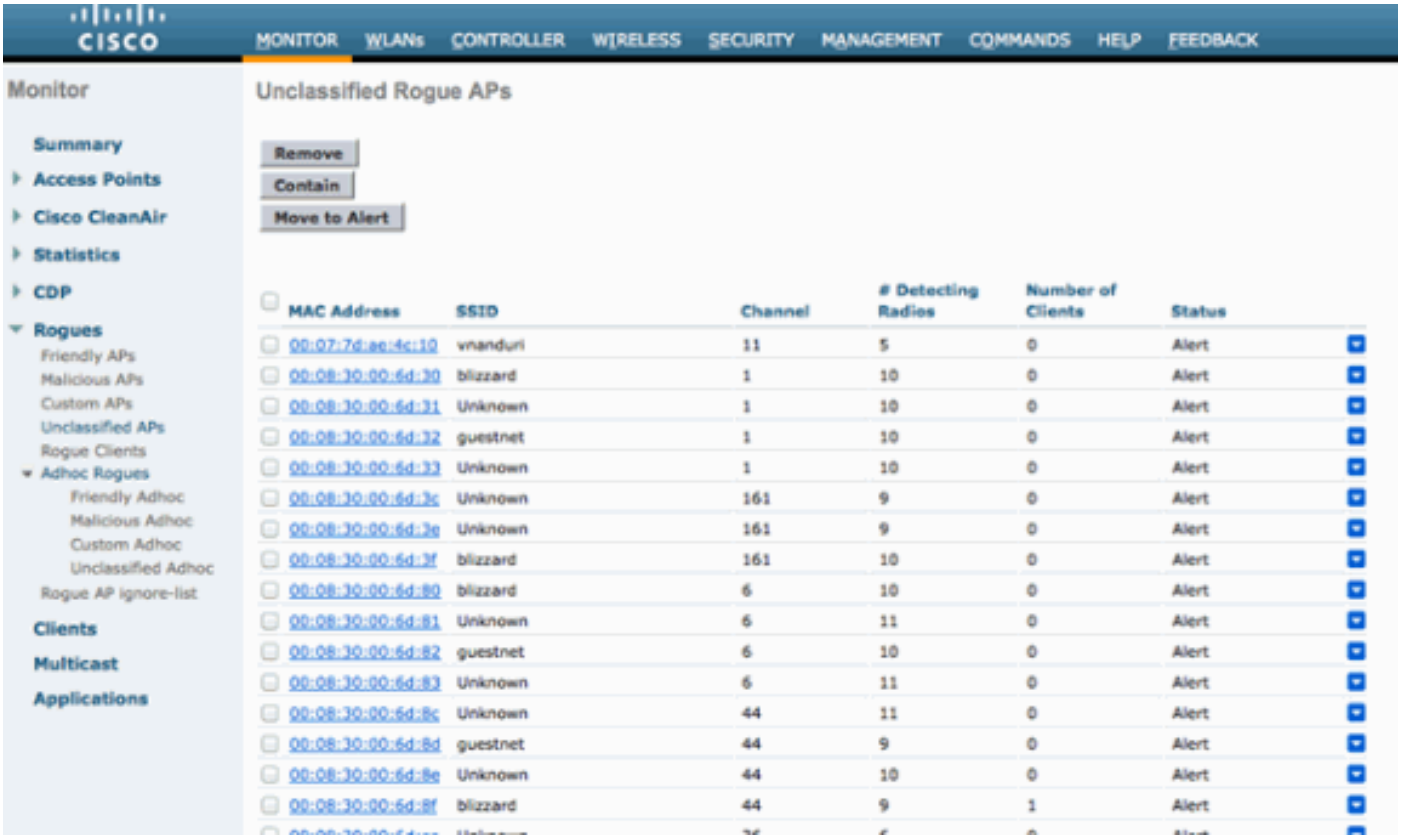
Bijvoorbeeld, alarm 52 is een Denial of Service, authenticatiestroom. Om te zien of die aanval op de WSSI-module werd gedetecteerd, geeft u de opdracht **Show capwap am alarm 52 uit**:

```
SJC14-21A-AP-DUNGENESS-X# show capw am alarm 52
capwap_am_show_alarm = 52

<A id='47C30C9E'>
<AT>52</AT>
<FT>2012/10/01 21:04:22</FT>
<LT>2012/10/01 21:04:49</LT>
<DT>2012/10/01 18:49:08</DT>
<SM>00:40:96:B5:85:8D-a</SM> <SNT>2</SNT>
<DM>00:22:55:F2:80:9F-a</DM> <DNT>1</DNT>
 <CH>11</CH>
 <FID>0</FID>
 pAlarm.bPendingUpload = 0
```

Spraakdetectie op WSSI-module

De WSSI-module detecteert scheerpunten met dezelfde nauwkeurigheid als een MMAP. Er wordt een lijst weergegeven van frauduleuze AP's in zowel de WLC als de PI.

Dit is de lijst van niet-gerubriceerde Rogue AP's van de WLC GUI. Rogue APs kunnen in de WLC GUI onder Bewaking > Rogues worden bekeken.



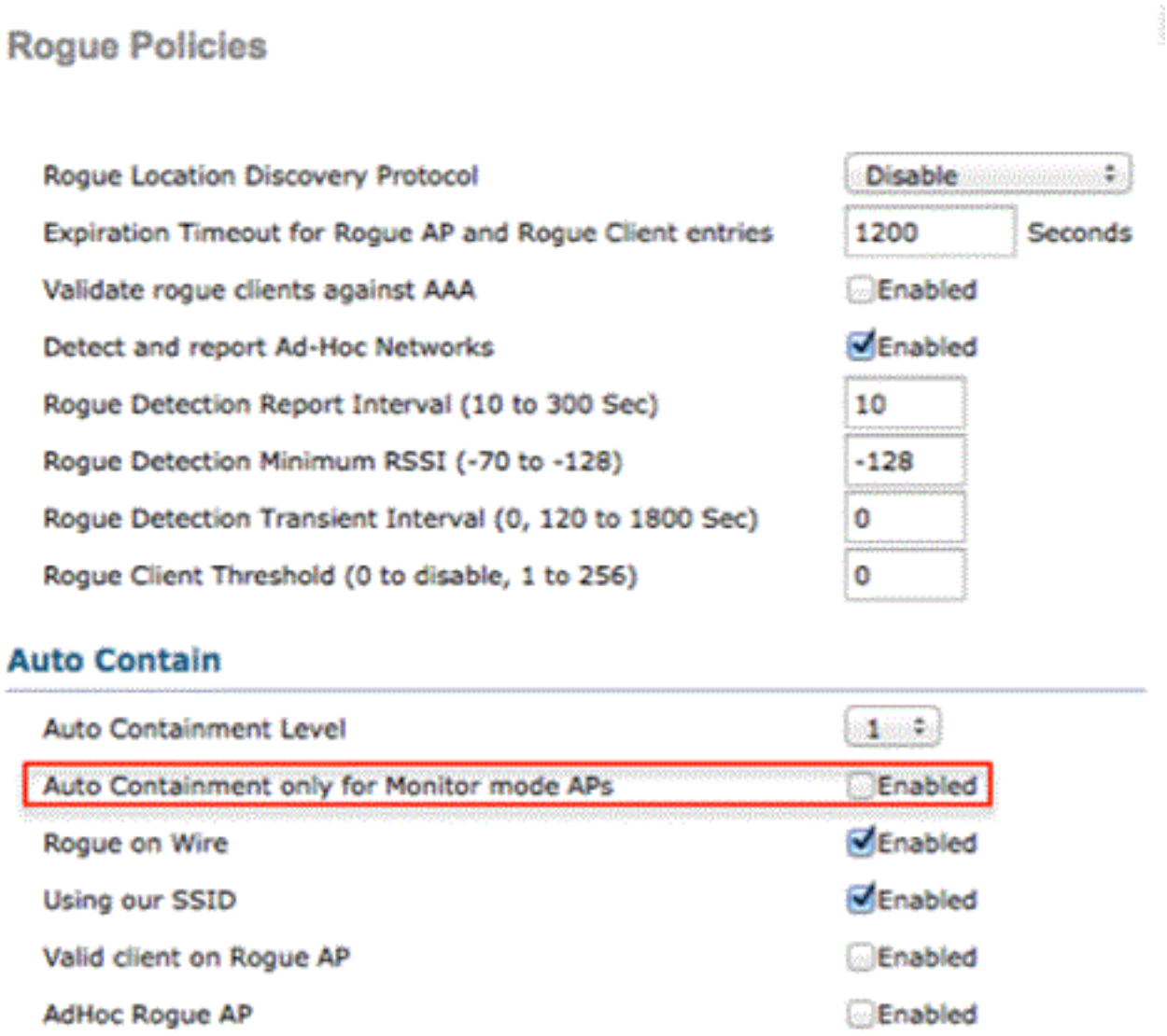
U kunt controleren of de WSSI-module met de AP-console een schurkenpas heeft gedetecteerd. Vanuit de console, voer de **show capwap rm rogue ap d2 alle** opdracht in. Dit toont alle schurkena's die bij de WSSI Module radio worden gezien.

```
SJC14-21A-AP-DUNGENESS-X# show capwap rm rogue ap dot11radio2 all
 ****************** CURRENT ROGUE APS ****************

ROGUE AP: 0  BSSID = 64:D9:89:42:24:3E, channel = 149
SSID = alpha_phone
```

```
heard 7 seconds ago
authFailedCount=0
NumOfPkts = 2, wep = 1, SP = 0, adHoc = 0, wpa = 1, 11g = 0, 11n=2
antenna 1 pkts 2 avgRssi -81 avgSnr 13


 ****************** MASTER ROGUE APS ****************

ROGUE AP: 0  BSSID = C4:3D:C7:8A:EE:90, channel = 1
SSID = NETGEAR_11ng
heard 7 seconds ago
authFailedCount=0
isBeingContained = 0
seen at 0 seconds for 0 times and valid = 1
NumOfPkts = 16108, wep = 0, SP = 1, adHoc = 0, wpa = 0, 11g = 1, 11n=2
antenna 1 pkts 16108 avgRssi -73 avgSnr 12

ROGUE AP: 1  BSSID = EC:44:76:81:C0:02, channel = 1
SSID = alpha_byod
heard 151 seconds ago
authFailedCount=0
isBeingContained = 0
seen at 0 seconds for 0 times and valid = 1
NumOfPkts = 413, wep = 1, SP = 1, adHoc = 0, wpa = 1, 11g = 1, 11n=2
antenna 1 pkts 413 avgRssi -84 avgSnr 5
```

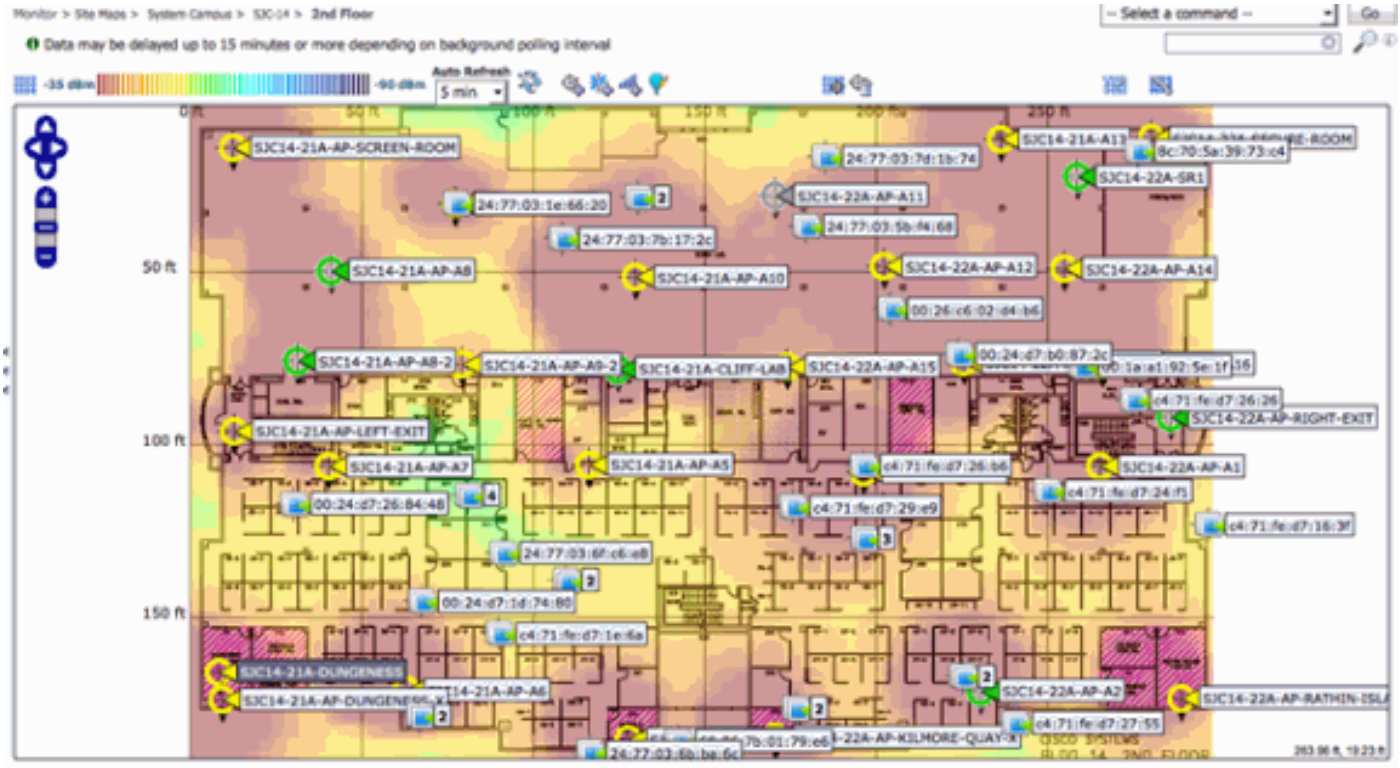
Gespreksbeheer met behulp van de WSSI-module

De WSSI-module is een 0x4-module (alleen antennes ontvangen), wat betekent dat een dergelijke insluiting zal worden uitgevoerd op de 2,4 GHz of 5 GHz-radio. Om de WSSI te kunnen configureren dat deze automatisch schurkenloze AP's bevat, moet u ervoor zorgen dat in de WLC GUI onder Beveiligingsbeleid > Regels voor draadloze bescherming > Handelsbeleid > Algemeen dat **Auto Containment alleen voor** monitormodi **is** ingeschakeld (zie de volgende screenshot). Alle andere aanvinkjes kunnen worden ingeschakeld.



Context bewuste locatie op de WSSI-module

Wanneer aangesloten op een Cisco MSE, verstrekt de WSSI module de gegevens van de Plaats van de Voorbereiding met de zelfde nauwkeurigheid als een MMAP.



Licentie voor WSSI-module

De WSSI-module maakt gebruik van licenties voor IPS-monitormodus.

Gerelateerde informatie

- Technische ondersteuning en documentatie – Cisco Systems