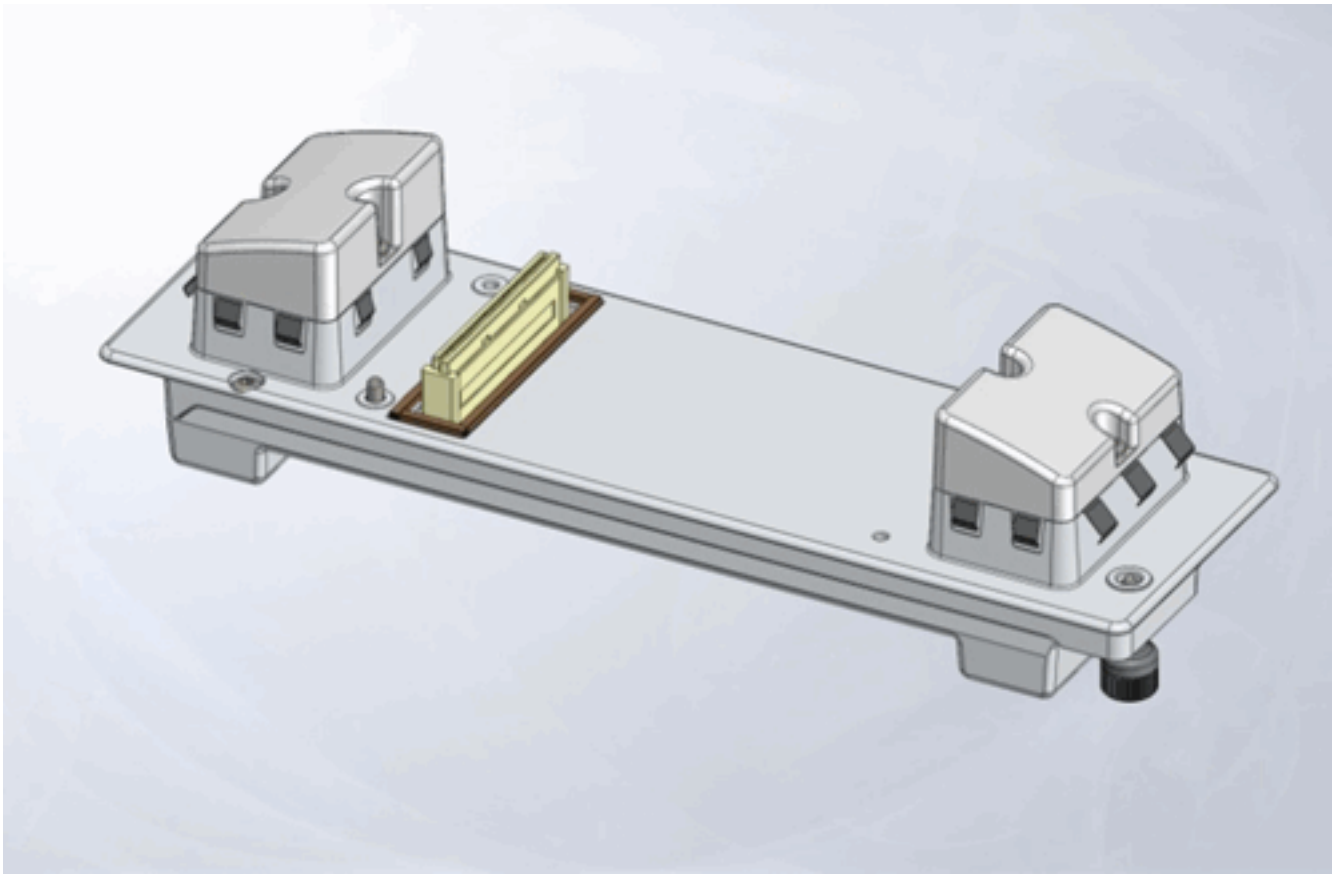
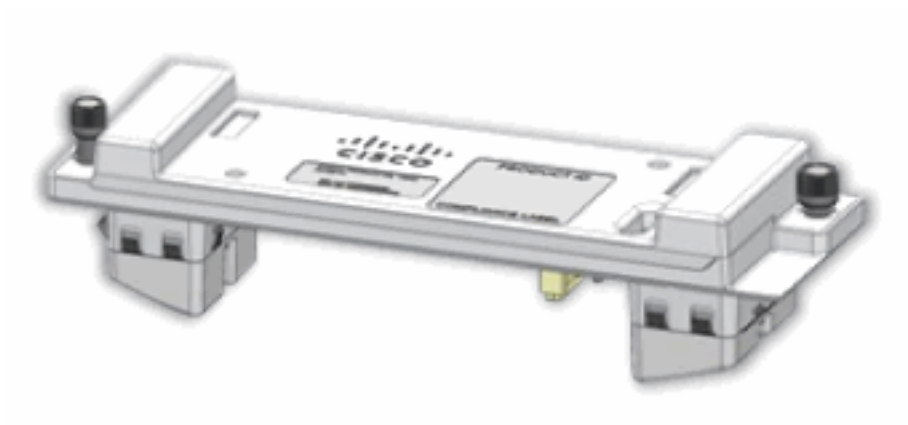
Módulo del Cisco Aironet AP para la seguridad de red inalámbrica y el Guía de despliegue de la inteligencia del espectro (WSSI)

Contenido

Introducción

Este documento proporciona la Configuración general y las Pautas para la instrumentación para el módulo del Punto de acceso del Cisco Aironet para la inteligencia de la seguridad de red inalámbrica y del espectro (WSSI). El WSSI es un módulo complementario que se puede insertar en el (APS) de las puntas de acceso modular tal como las Cisco 3600 Series AP.





prerrequisitos

Requisitos

No hay requisitos específicos para este documento.

Componentes Utilizados

El módulo de la inteligencia de la seguridad de red inalámbrica y del espectro necesita las versiones del código mínimo:

- Regulador del Wireless LAN (WLC) – Versión 7.4.xx.xx o más adelante
- Punto de acceso – Versión 7.4.xx.xx o más adelante
- Infraestructura primera (PI) – Versión 1.3.xx.xx o más adelante
- Motor de los Servicios de movilidad (MSE) – Versión 7.4.xx.xx o más adelante

Convenciones

Consulte Convenciones de Consejos TécnicosCisco para obtener más información sobre las convenciones del documento.

Descripción general del producto

El módulo de la inteligencia de la seguridad de Red Inalámbrica Cisco y del espectro, aprovechándose del diseño modular flexible de las 3600 Series AP del Cisco Aironet, entrega sin precedente, siempre-en la exploración de la Seguridad y la inteligencia del espectro. Esto le ayuda a evitar interferencia del Radiofrecuencia (RF) de modo que usted consiga una mejores cobertura y funcionamiento en su red inalámbrica.

- monitor lleno y mitigación del espectro 24 x 7 para el aWIPS, CleanAir, la conciencia del

contexto, la detección rogue y la administración de recursos de la radio
- protección de la amenaza del aWIPS de 24 x 7 en-canales
- 23 veces más cobertura de la Seguridad y del espectro
- Ahorros de costos 30%+ CAPEX contra el modo monitor dedicado AP
- Configuración cero del tacto

El módulo campo-mejorable WSSI es una radio dedicada que descarga toda la supervisión y los Servicios de seguridad de las radios del cliente/de la porción de los datos a la Seguridad monitorean el módulo. Esto no sólo permite un mejor rendimiento del cliente, pero también reduce los costes eliminando la necesidad del modo monitor dedicado AP y de la infraestructura Ethernet requerida para conectar esos dispositivos en su red.

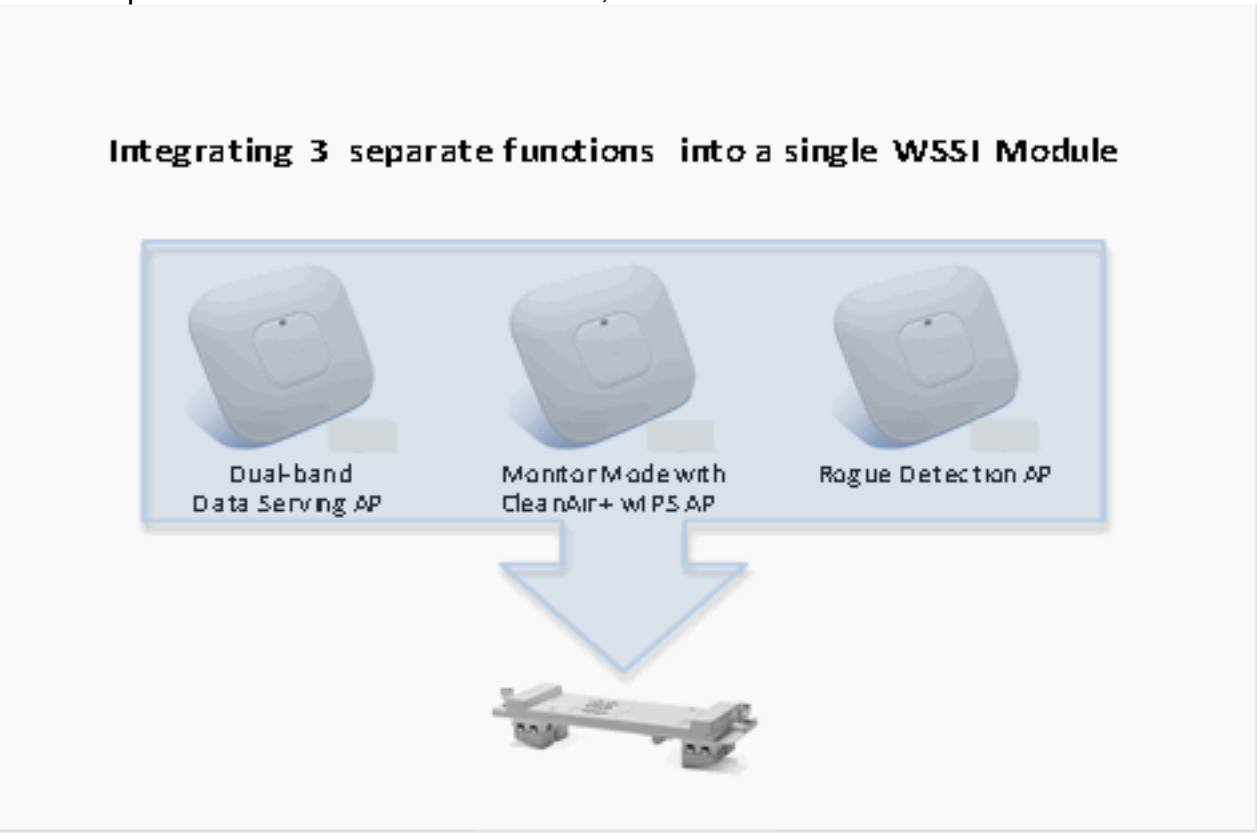
Junto, las 3600 Series AP y permiso del módulo WSSI usted para proporcionar en paralelo la Seguridad y la análisis de espectro avanzadas funciona para los clientes del Wi-Fi en todos los canales, en las bandas 2.4-GHz y 5-GHz.

Una vez que está desplegado, el módulo está analizando constantemente todos los canales para ayudar a asegurar la experiencia inalámbrica más segura y más robusta disponible en la industria.

Ventajas del modo WSSI

Modo local aumentado (OLMO):

- Reduce los costos de la red y las operaciones. Integrando el módulo WSSI en las 3600 Series, usted puede substituir hasta tres dispositivos diferentes. Esto proporciona tres funciones separadas en las 3600 Series solas, multiusos

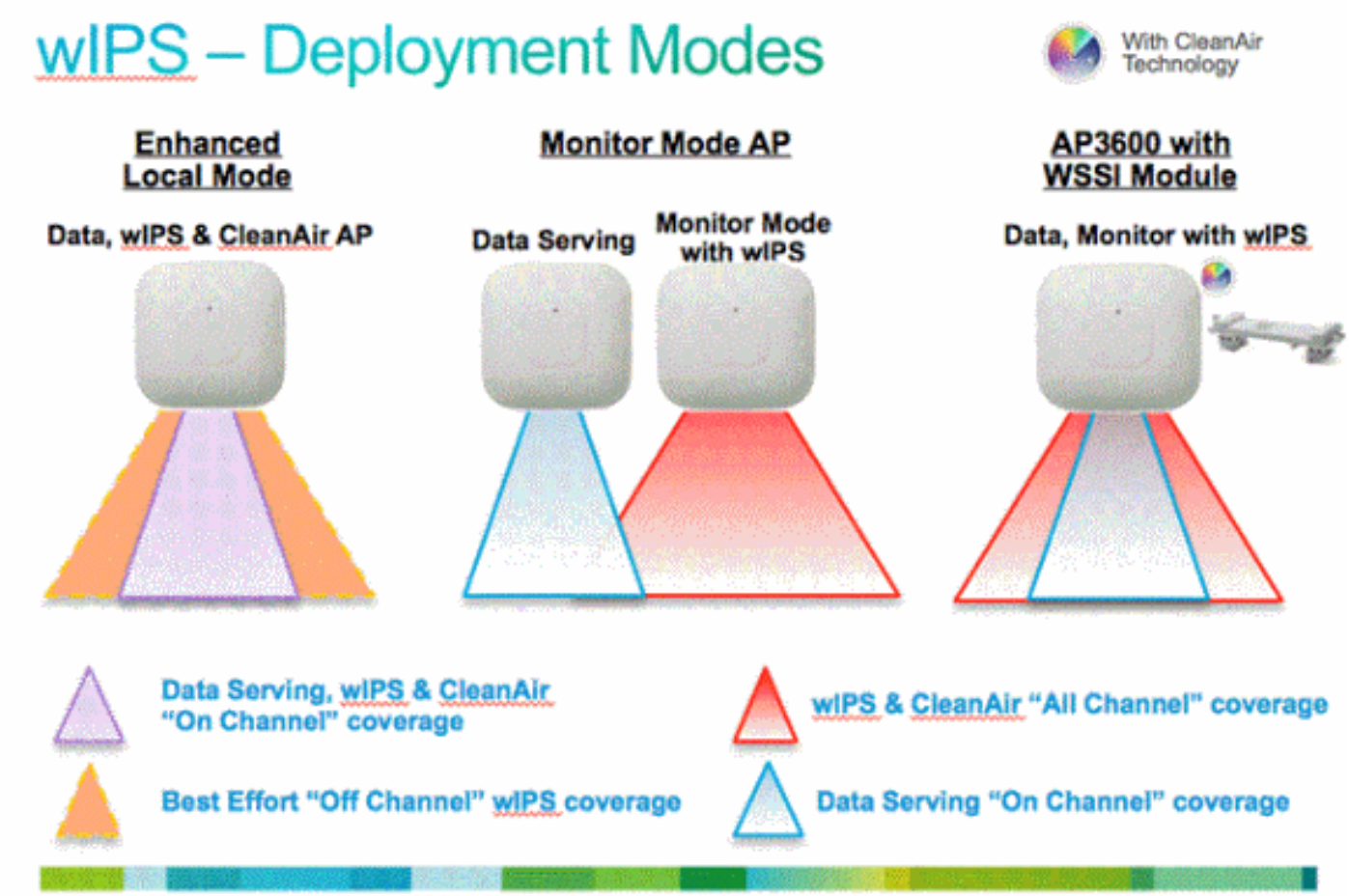


AP.
- Los clientes pueden ahora leverage una sola conexión de Ethernet (cable y puerto) en su red alámbrica, en lugar de qué requeriría típicamente hasta tres cables Ethernet separados y un puerto de acceso en su red alámbrica. Esto reduce perceptiblemente su CAPEX.
- Integrando todas estas características a un solo AP, los clientes simplifican la Administración

y monitorear cotidianos de su infraestructura de red inalámbrica y red con un número grandemente reducido de AP. El módulo WSSI aparece al WLC y a los sistemas de administración como radio adicional que soporta los dispositivos del cliente 802.11b/g/a/n (2.4 y 5 gigahertz) dentro de las 3600 Series específicas AP.

- *La configuración cero del tacto*, instala, ciclo inicial y va. No hay absolutamente configuración requerida para permitir al módulo WSSI para ser en servicio, e inmediatamente que monitorea y de sujeción de su red inalámbrica. El módulo WSSI se inserta y se asegura a cualquier 3600 Series AP. Cuando el AP es salvaguardia accionada el módulo se inicializa junto con las otras radios en el AP y comienza inmediatamente a monitorear todos los canales en 2.4 y 5 gigahertz para cualesquiera amenazas para la seguridad y origen de la interferencia.
- El wIPS adaptante proporciona la detección exacta y eficiente de la amenaza en todos los canales sobre - de los ataques aéreos, los AP rogue, y las conexiones ad hoc, así como la capacidad de clasificar, de notificar, de atenuar y de señalar para la supervisión y la administración proactiva constantes. Trabajos conjuntamente con el motor de los Servicios de movilidad de Cisco (MSE).

OLMO:



- Agrega la exploración de la Seguridad del wIPS para 7x24 en la exploración del canal (2.4GHz y 5 gigahertz), con mejor esfuerzo del soporte del canal.
- El AP está sirviendo además a los clientes y con las G2 Series de AP, habilita la análisis de espectro de CleanAir en los canales (2.4GHz y 5GHz).

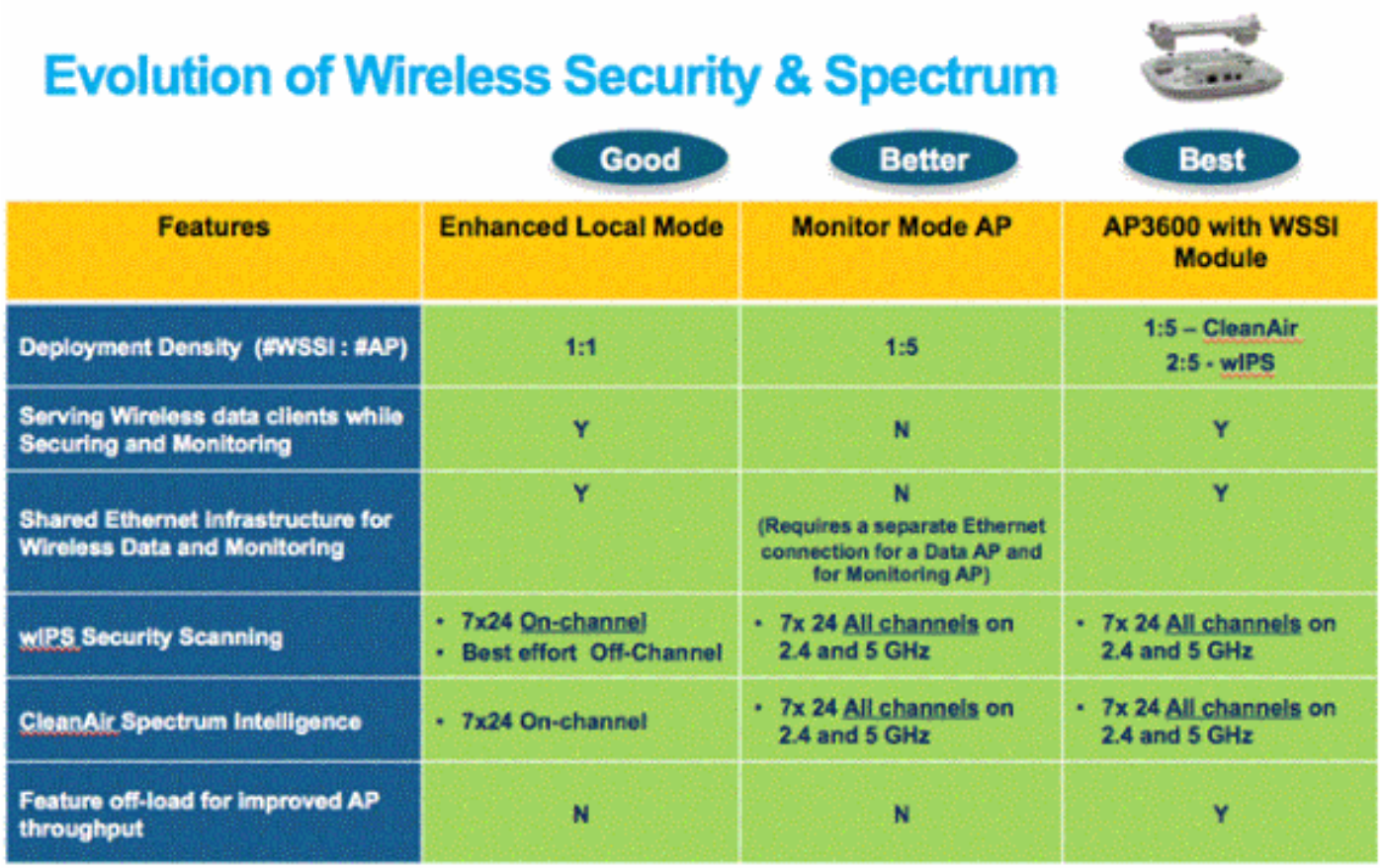
Modo monitor:

- Dedican para actuar en el modo monitor y tiene al modo monitor AP (MMAP) la opción para

agregar la exploración de la Seguridad del wIPS de todos los canales (2.4GHz y 5GHz).
- Las G2 Series de AP habilitan la análisis de espectro de CleanAir en todos los canales (2.4GHz y 5GHz).
- MMAPs no sirve a los clientes.

AP3600 con el módulo WSSI: La evolución de la seguridad de red inalámbrica y del espectro

- El primer AP de la industria que facilita el Servicio al cliente, la exploración de la Seguridad del wIPS y la análisis de espectro simultáneos usando la tecnología de CleanAir.
- Radio dedicada 2.4GHz y 5GHz con sus propias Antenas que habilita la exploración 7x24 de todos los canales inalámbricos en las bandas 2.4GHz y 5GHz.
- Una sola infraestructura Ethernet proporciona la operación simplificada con menos dispositivos para manejar y el retorno en la inversión optimizado de la infraestructura de red inalámbrica AP3600 y de la infraestructura cableada de los Ethernetes.



Features	Enhanced Local Mode	Monitor Mode AP	AP3600 with WSSI Module
Deployment Density (#WSSI : #AP)	1:1	1:5	1:5 – CleanAir 2:5 - wIPS
Serving Wireless data clients while Securing and Monitoring	Y	N	Y
Shared Ethernet Infrastructure for Wireless Data and Monitoring	Y	N (Requires a separate Ethernet connection for a Data AP and for Monitoring AP)	Y
wIPS Security Scanning	• 7x24 On-channel • Best effort Off-Channel	• 7x 24 All channels on 2.4 and 5 GHz	• 7x 24 All channels on 2.4 and 5 GHz
CleanAir Spectrum Intelligence	• 7x24 On-channel	• 7x 24 All channels on 2.4 and 5 GHz	• 7x 24 All channels on 2.4 and 5 GHz
Feature off-load for improved AP throughput	N	N	Y

- Tecnología de Cisco CleanAir: proporciona la inteligencia dinámica, de alta velocidad del espectro de combatir los problemas de rendimiento debido a interferencia inalámbrica. La primera tecnología avanzada del análisis RF de la industria que examina y clasifica los modelos de la energía (firmas) de los dispositivos que pueden afectar perceptiblemente la calidad de una red inalámbrica.
- Administración de recursos de radio (RRM): la Administración simplificada, avanzada RF, se adapta automáticamente al entorno de red inalámbrica basado en la información recibida de la tecnología de Cisco CleanAir. Una vez que se identifican los interferers, RRM puede mover los dispositivos del cliente a los canales lejos de la interferencia y ajustar el poder del transitar de moverse lejos del origen de la interferencia. Esto proporciona una mejor calidad RF al usuario.
- Detección rogue: detecta y señala el acceso a la red y el acceso traseros a los clientes de red inalámbrica.

- Conciencia de la ubicación y del contexto: proporciona la conciencia en tiempo real y la capacidad de seguir el punto final de red inalámbrica.

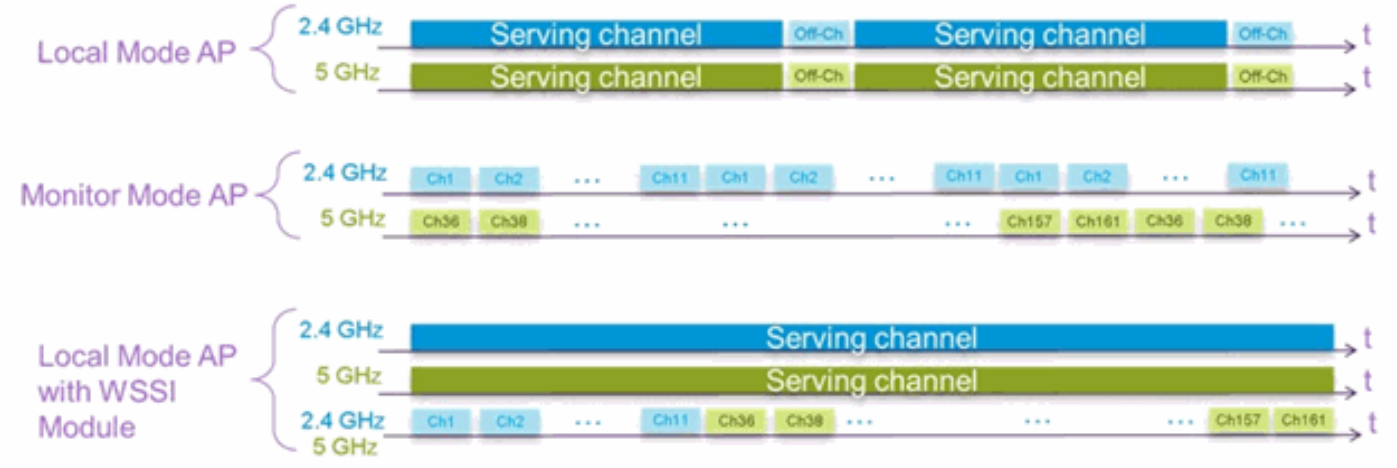
Con estas características, el módulo de la inteligencia de la seguridad de Red Inalámbrica Cisco y del espectro, junto con las Cisco 3600 Series AP, proporciona la red inalámbrica más segura y más robusta de la clase de la empresa posible para sus usuarios corporativos y datos.

En-canal contra el Apagado-canal usando el módulo WSSI

Un modo local AP analiza para el en-canal de los atacantes de los interferers y de los wIPs de CleanAir. Esto significa las exploraciones AP solamente el canal que está sirviendo. Un modo local AP con un canal de porción de la radio 2.4GHz 1 y el canal de porción de radio 5GHz 64, proporciona solamente la protección en los canales 1 y 64.

Un MMAP analiza para el apagado-canal de los atacantes de los interferers y de los wIPs de CleanAir. Esto significa que el AP analiza todos los canales. La radio 2.4GHz analiza todos los canales 2.4GHz y el canal 5GHz analiza todos los canales 5GHz.

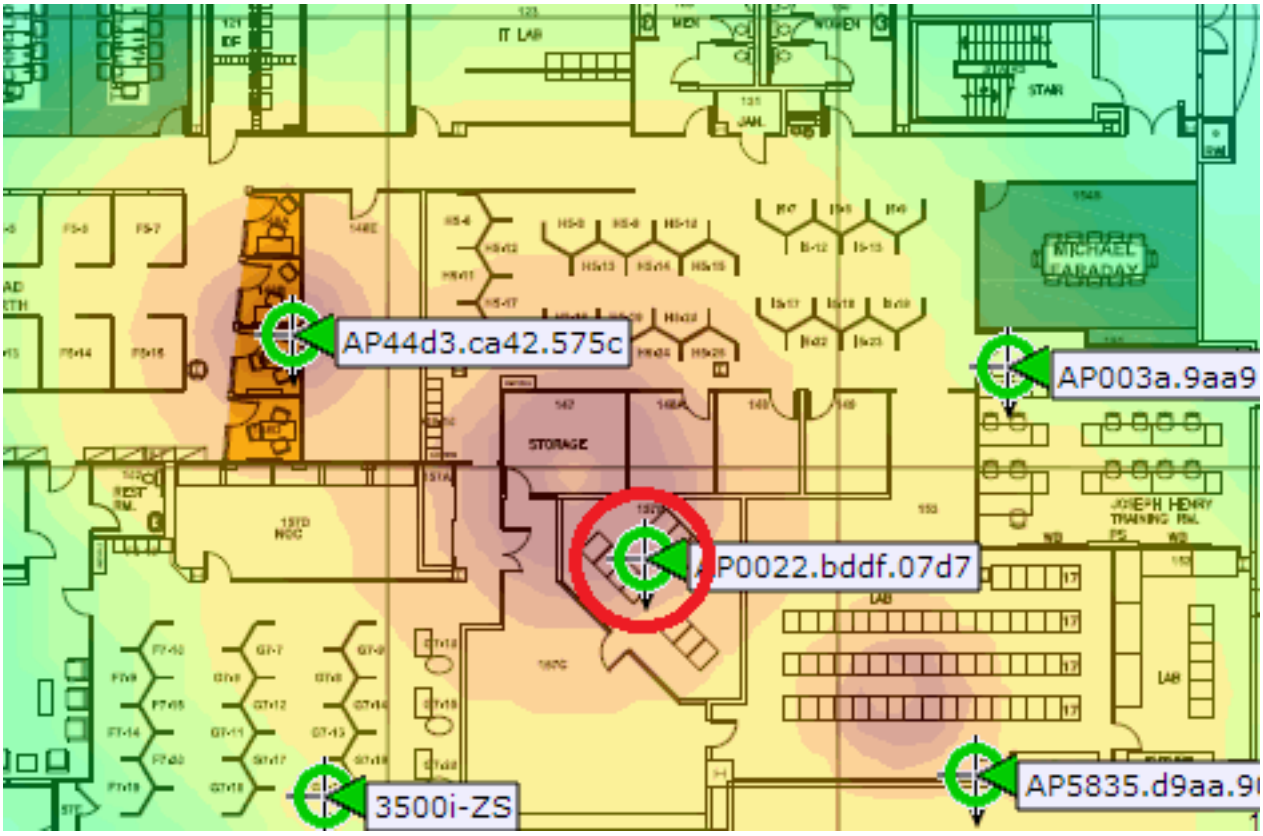
Las Cisco 3600 Series AP utilizan una combinación de en-canal y de apagado-canal. Las radios 2.4GHz y 5GHz analizan el en-canal y el módulo WSSI analiza el apagado-canal, completando un ciclo entre todos los canales 2.4GHz y 5GHz.



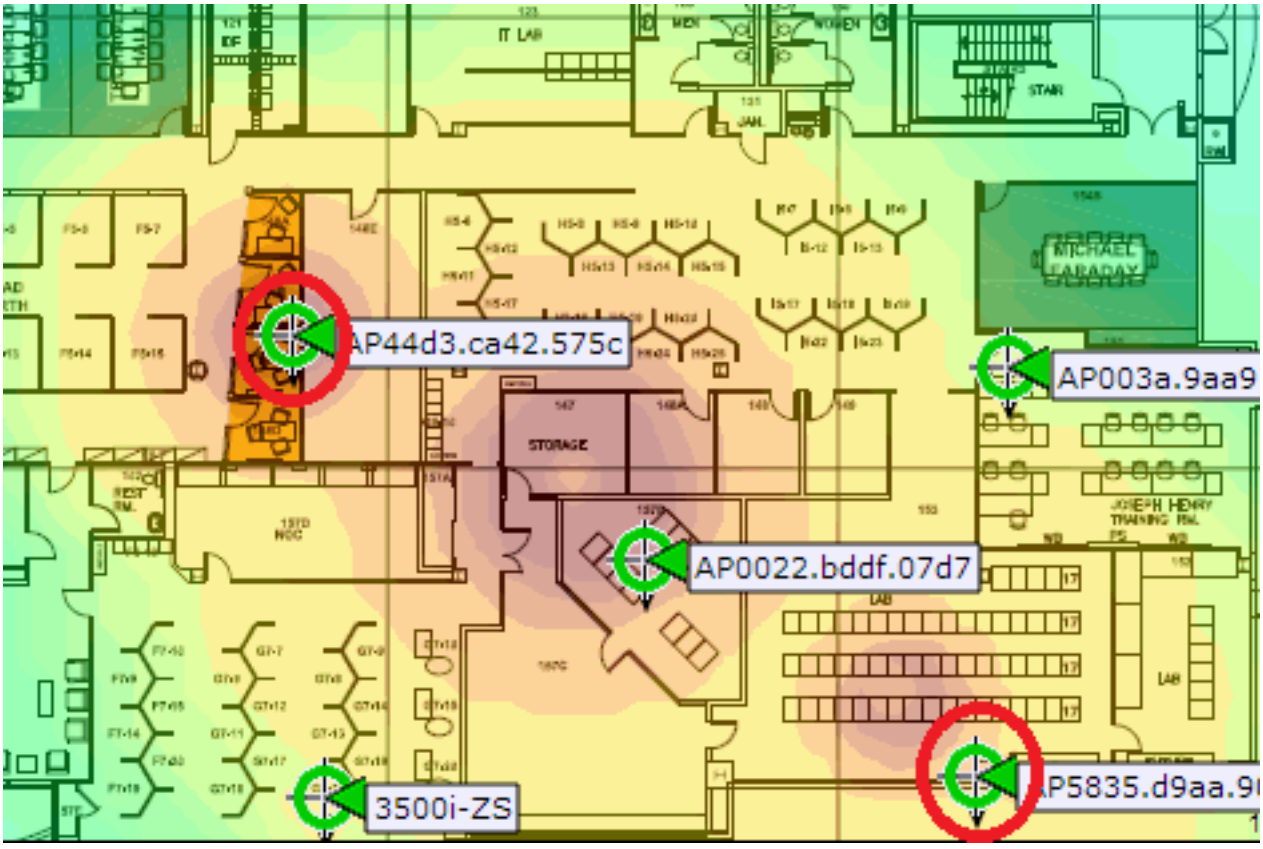
Densidad sugerida del despliegue para el módulo WSSI

En el despliegue tradicional del monitor AP, Cisco recomienda una relación de transformación de 1 MMAP a cada 5 modo local AP. Esto puede variar basado en el diseño de red y la dirección del experto para la mejor cobertura. Con el módulo WSSI, hay diversas recomendaciones de instrumentación basadas en las funciones para alcanzar la paridad de la cobertura con un MMAP.

Para CleanAir, se recomienda para desplegar 1 módulo WSSI para cada 5 locales o Flexconnect AP. Este despliegue de 1:5 ofrece el mismo funcionamiento que un MMAP habilitado CleanAir, pero todavía permite que el AP sirva a los clientes. Esto es un despliegue recomendado para un módulo CleanAir de ejecución WSSI:

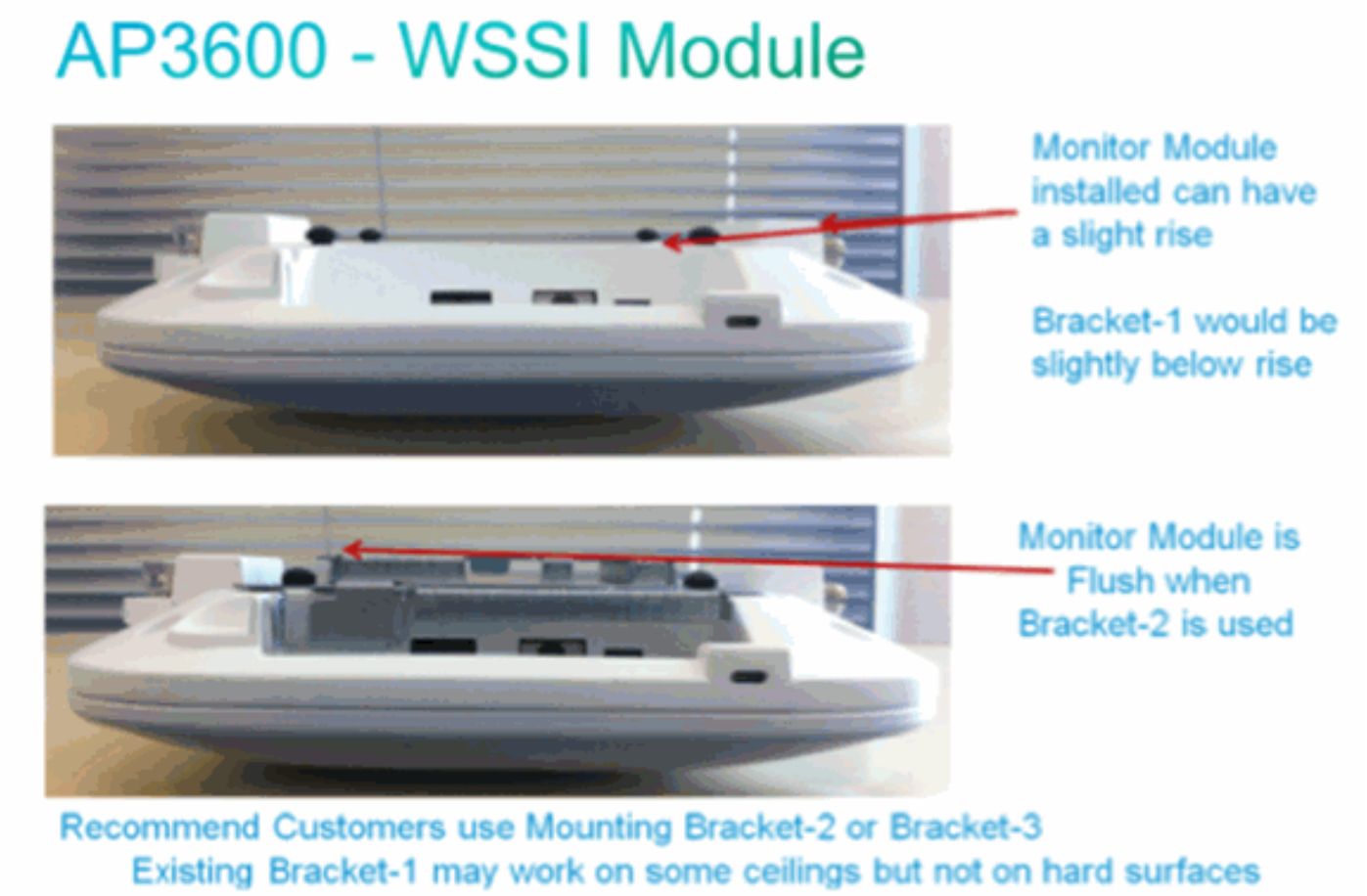


Para la protección del wIPS, se recomienda para desplegar 2 módulos WSSI para cada 5 locales o FlexConnect AP. El tiempo de detección del wIPS para un ataque del apagado-canal es cerca de dos veces que de un MMAP. Por lo tanto, un despliegue de 2:5 se requiere para proporcionar la paridad de la detección del wIPS. Éste es el despliegue recomendado para un módulo WSSI que realiza la protección del wIPS:



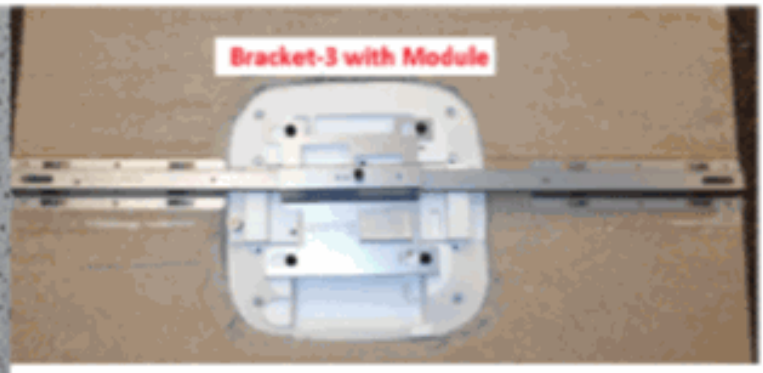
El Cisco 3600 AP con un módulo WSSI utiliza el en-canal y la exploración del apagado-canal para proporcionar una industria solución principal mientras que sirve a los clientes.

[Instalar el módulo WSSI]



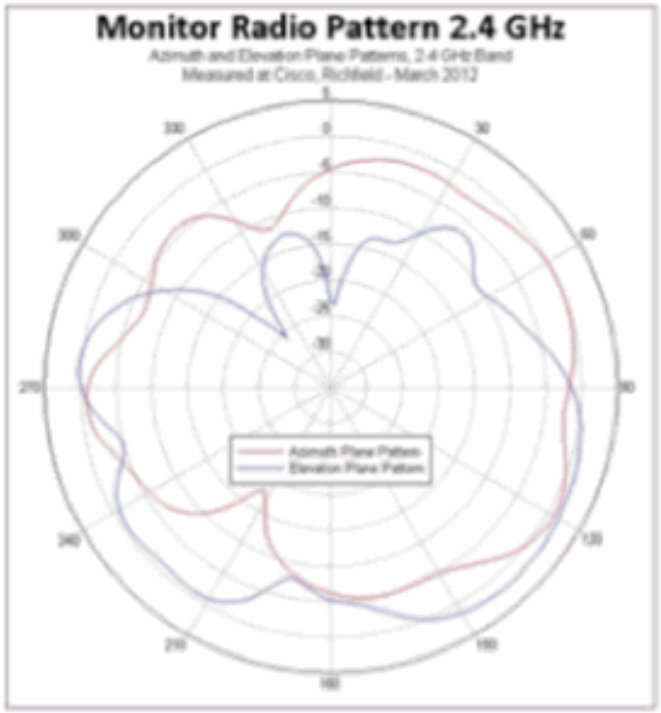
AP3600 with WSSI Module and Bracket-3

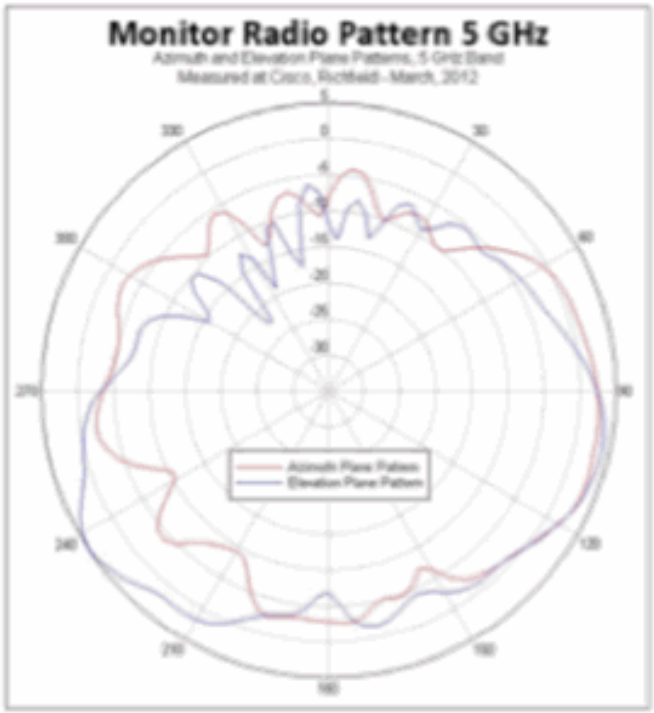
Elegant in-tile flush mount



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





Configuración para el módulo AP3600 WSSI

No hay configuración para el módulo WSSI necesario. El módulo analiza automáticamente todos los canales en ambas bandas usando su 0x4 las Antenas (RO) de 0 tx x 4 Antenas del rx.

Observe que el módulo WSSI es solamente activo en AP3600s configurado en el modo local o el modo de FlexConnect. El módulo WSSI se inhabilita en el resto de los modos.

Requisito de alimentación eléctrica para el módulo WSSI

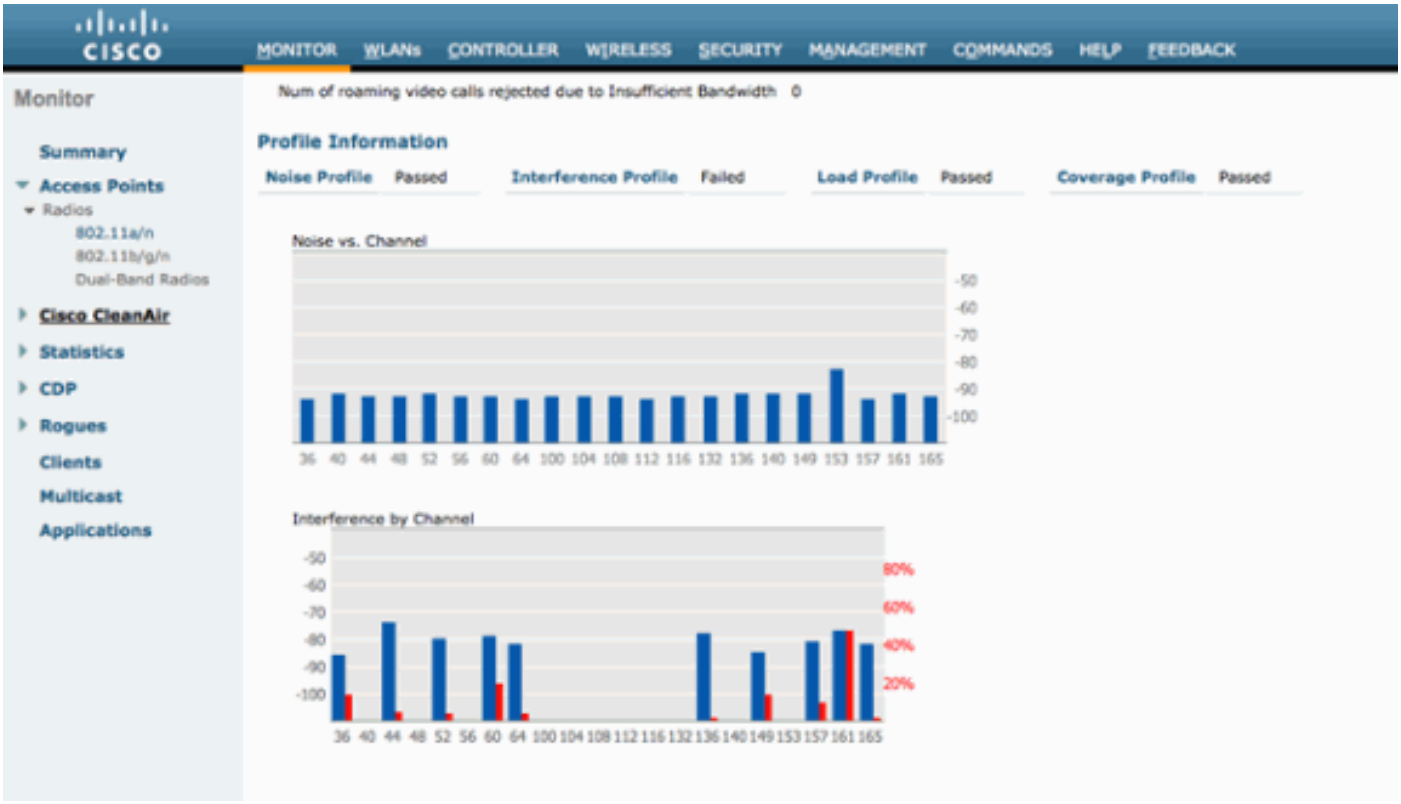
El AP3600 con un módulo WSSI instalado excede 15.4 vatios (802.3af). El AP requiere cualquiera (802.3at - PoE+), PoE aumentado, una fuente de alimentación de CA local, o el inyector de PoE de Cisco (AIR-PWRINJ4).

Notas:

- El PoE aumentado fue creado por Cisco y es un precursor a 802.3at PoE+. Proporciona hasta 20W del poder.
- PoE+ puede entregar hasta 30W del poder.

Administración de recursos de radio en el módulo WSSI

El módulo WSSI toma a todos RRM las medidas en la banda banda 2.4GHz y 5GHz. Las medidas se visualizan en el WLC GUI bajo el monitor > los Puntos de acceso > 802.11a/n > AP_NAME > detalles o el monitor > los Puntos de acceso > 802.11b/g/n > AP_NAME > los detalles.



CleanAir en el módulo WSSI

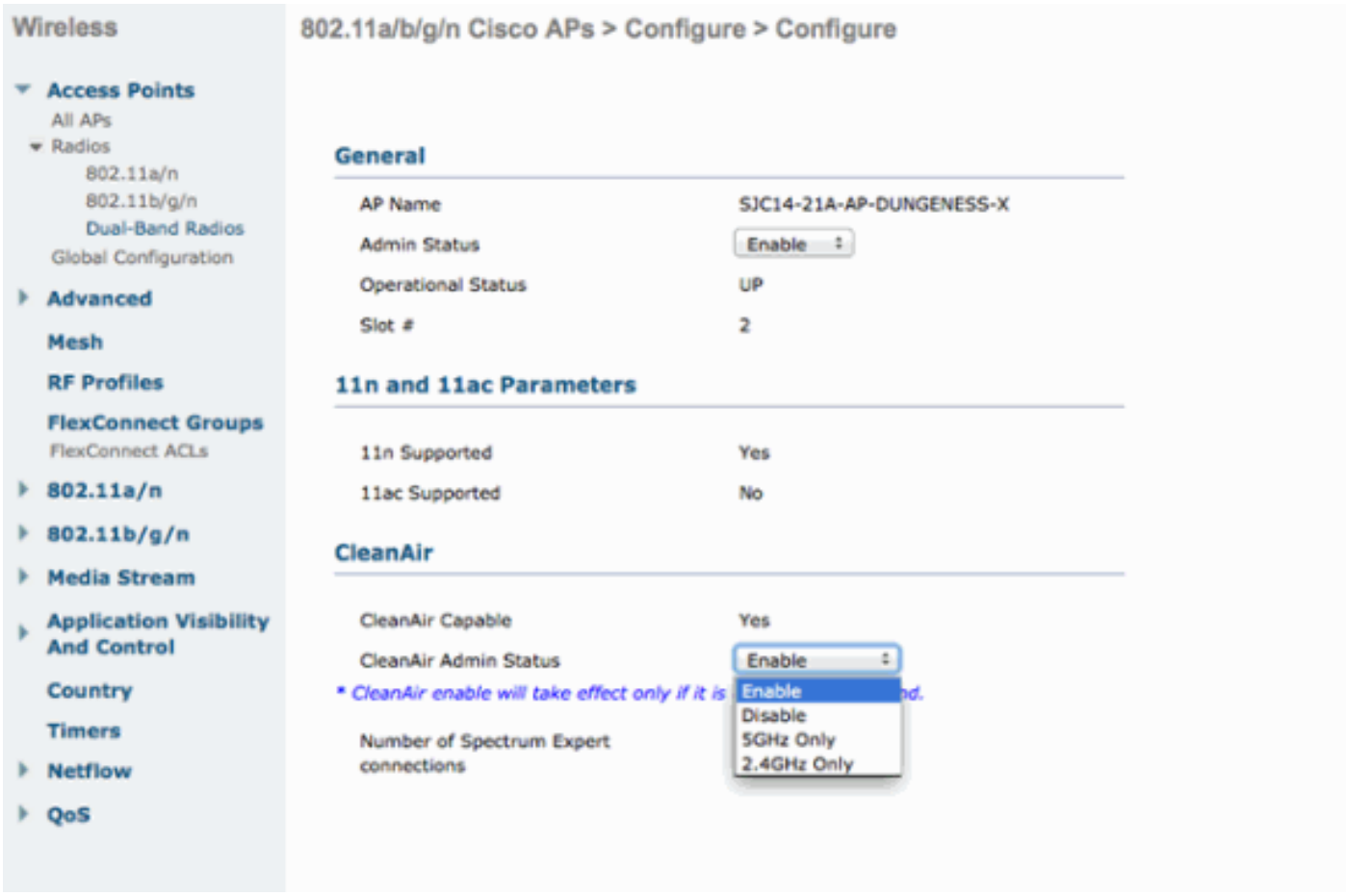
El módulo WSSI detecta los interferers de CleanAir con la misma precisión que un MMAP. Cisco recomienda que el módulo WSSI esté desplegado con una densidad de 1:5, donde debe haber 1 módulo WSSI para cada 5 AP. Ésta es la misma densidad recomendada que para un MMAP.

Cuando el módulo WSSI se habilita sin el sub-MODE, el módulo analiza la banda banda 2.4GHz y 5GHz. El módulo mora en cada canal para 1.2secs y analiza para los interferers de CleanAir.

CleanAir se puede habilitar en 2.4GHz solamente, 5GHz solamente, y 2.4GHz y 5GHz. Esto es a elección del WLC CLI o del GUI. Aquí está un ejemplo de configurar CleanAir en el WLC CLI:

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

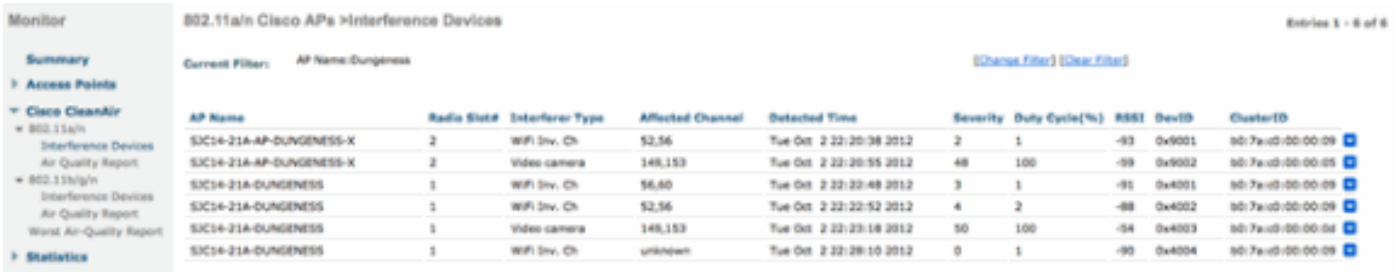
La misma configuración se puede aplicar en el GUI vía la Tecnología inalámbrica > las radios > la configuración de la Dual-banda. Aquí está un ejemplo de esto:



Para verificar que el interferer de CleanAir fuera detectado por el módulo WSSI, publique los **interferers del cleanair de la demostración** ordenan de la consola AP:

```
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
```

La misma configuración se puede aplicar en el GUI vía la Tecnología inalámbrica > las radios > la configuración de la Dual-banda. Aquí tiene un ejemplo:



Los interferers de CleanAir están señalados en el WLC GUI. Interferers se visualiza POR LA BANDA. Esto significa que los interferers detectados en el módulo WSSI en la banda 5GHz están visualizados bajo el monitor > 802.11a/n > dispositivos de interferencia.

Para verificar que el interferer de CleanAir fuera detectado por el módulo WSSI, publique los **interferers del cleanair de la demostración de la** consola AP:

```
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
```

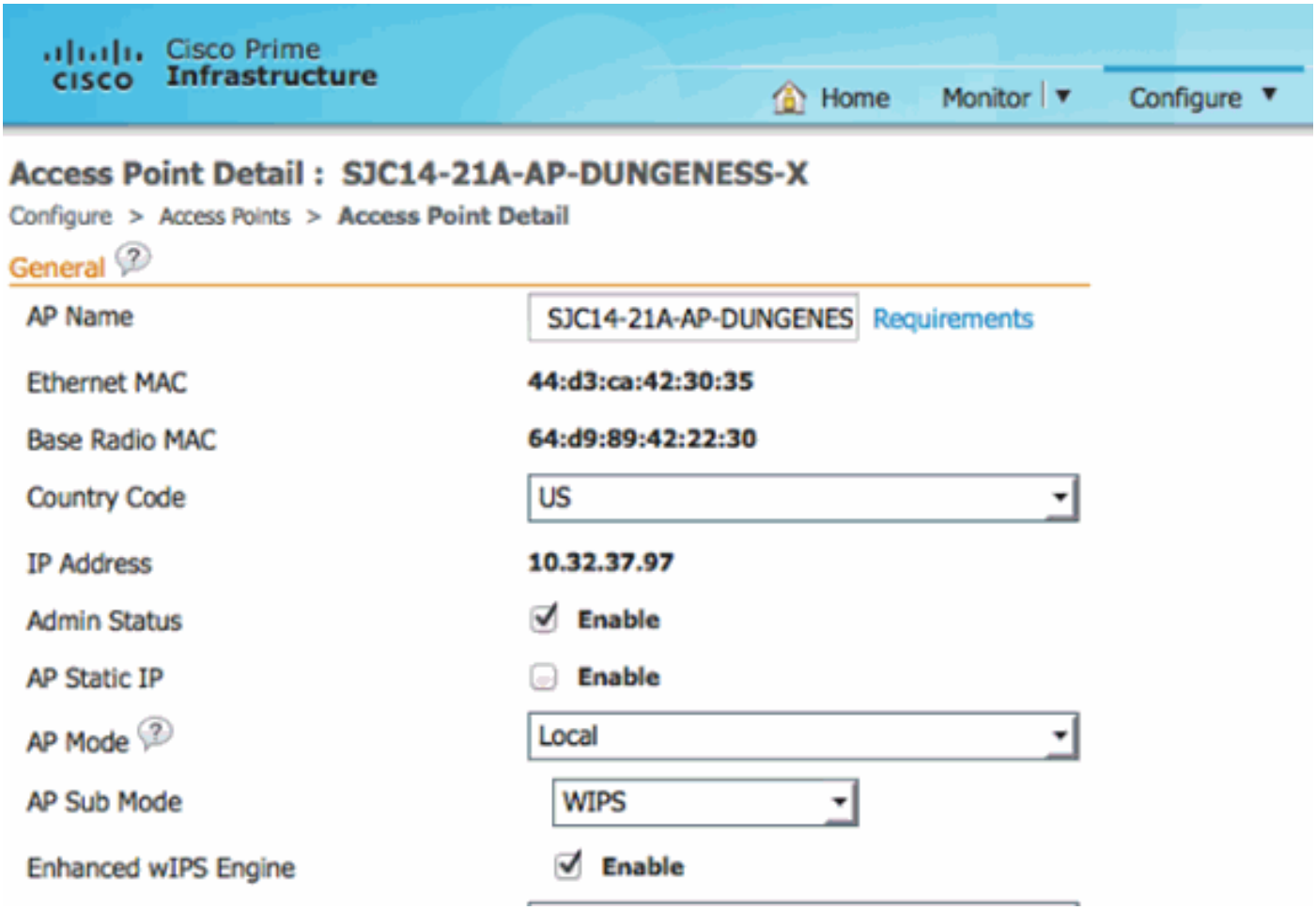
wIPS en el módulo WSSI

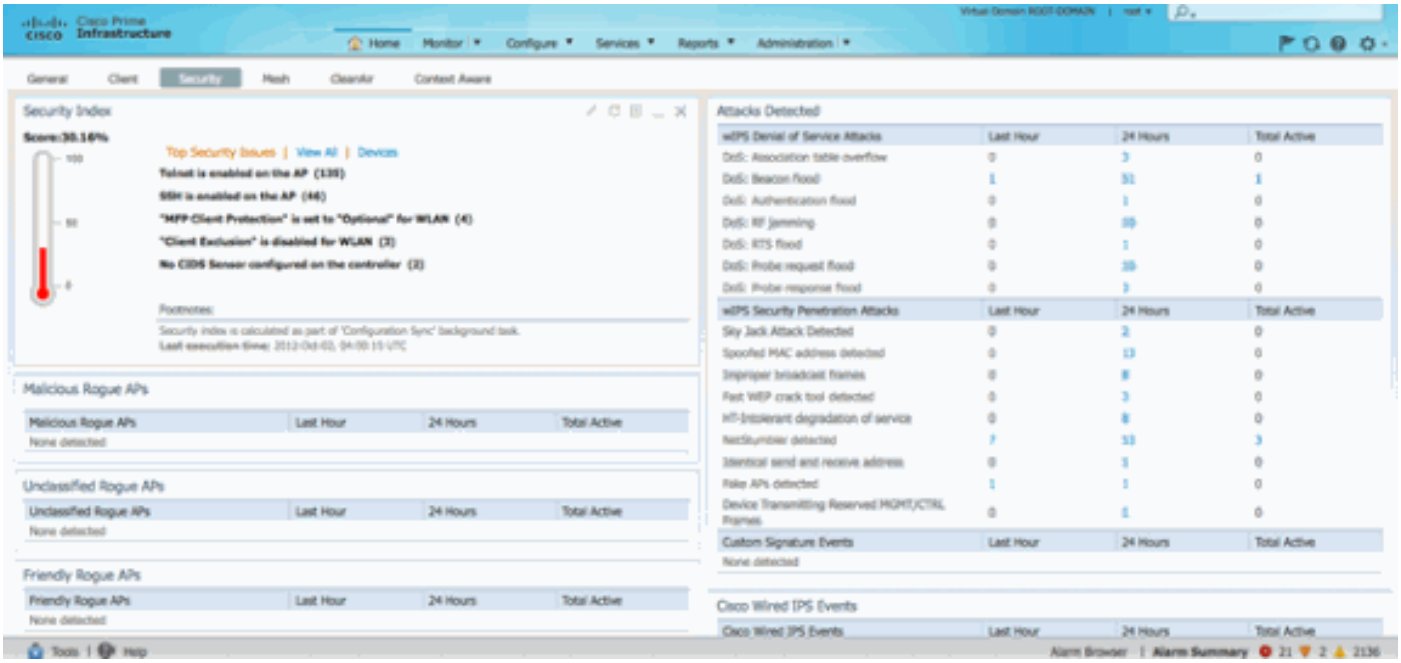
El módulo WSSI detecta los atacantes del wIPS con casi la misma precisión que un MMAP. Para el wIPS, Cisco recomienda el desplegar del módulo WSSI con una relación de transformación de 2:5 entre los AP. Este los medios para cada 5 AP, dos de los AP deben contener el módulo WSSI.

Hay dos modos del wIPS que pueden ser configurados:

- submode del wIPS - Habilita la Detección de ataque del wIPS y analiza todos los canales para 1.2s. Este modo permite que el AP todavía capture todos RRM señala además de las detecciones del wIPS.
- Modo aumentado del wIPS - Habilite la Detección de ataque del wIPS y analiza todos los canales para 250ms. El tiempo de detención más pequeño del canal permite que el módulo de la Seguridad detecte los atacantes más aprisa.

De la página primera de la infraestructura (PI), van a la configuración > a Acesss señalan > AP_NAME. El módulo WSSI se puede configurar al submode del wIPS o al submode del wIPS + soporte de motor aumentado del wIPS. Esto se puede también avanzar como parte de una plantilla de configuración AP.





Los ataques del wIPS se visualizan en la infraestructura primera de la lengueta casera del > Security (Seguridad).

El PI visualiza una Vista de nivel de red, pero usted puede visualizar el ataque en un AP3600 con un módulo WSSI publicando el comando de la **alarma ALARM_NUM del capwap de la demostración de la** consola AP.

Por ejemplo, la alarma 52 es una negación de servicio, inundación de la autenticación. Para ver si ese ataque fue detectado en el módulo WSSI, publique el comando de la **alarma 52 del capwap**

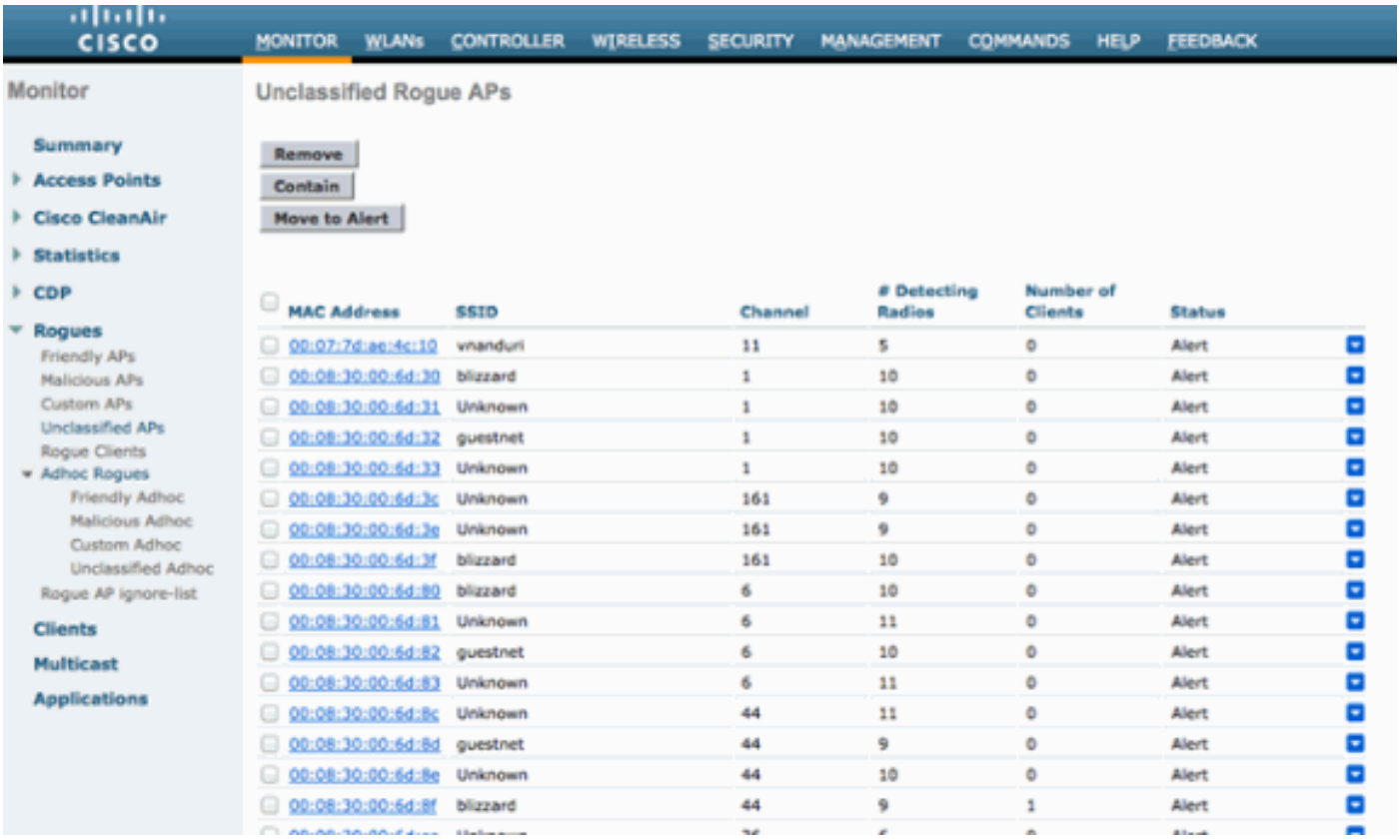
de la demostración:

```
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
```

El granuja detecta en el módulo WSSI

El módulo WSSI detecta los AP rogue con la misma precisión que un MMAP. Una lista del granuja AP se visualiza en el WLC y el PI.

Ésta es la lista del granuja sin clasificar AP del WLC GUI. Los AP rogue se pueden ver en el WLC GUI bajo el monitor > los granujas.



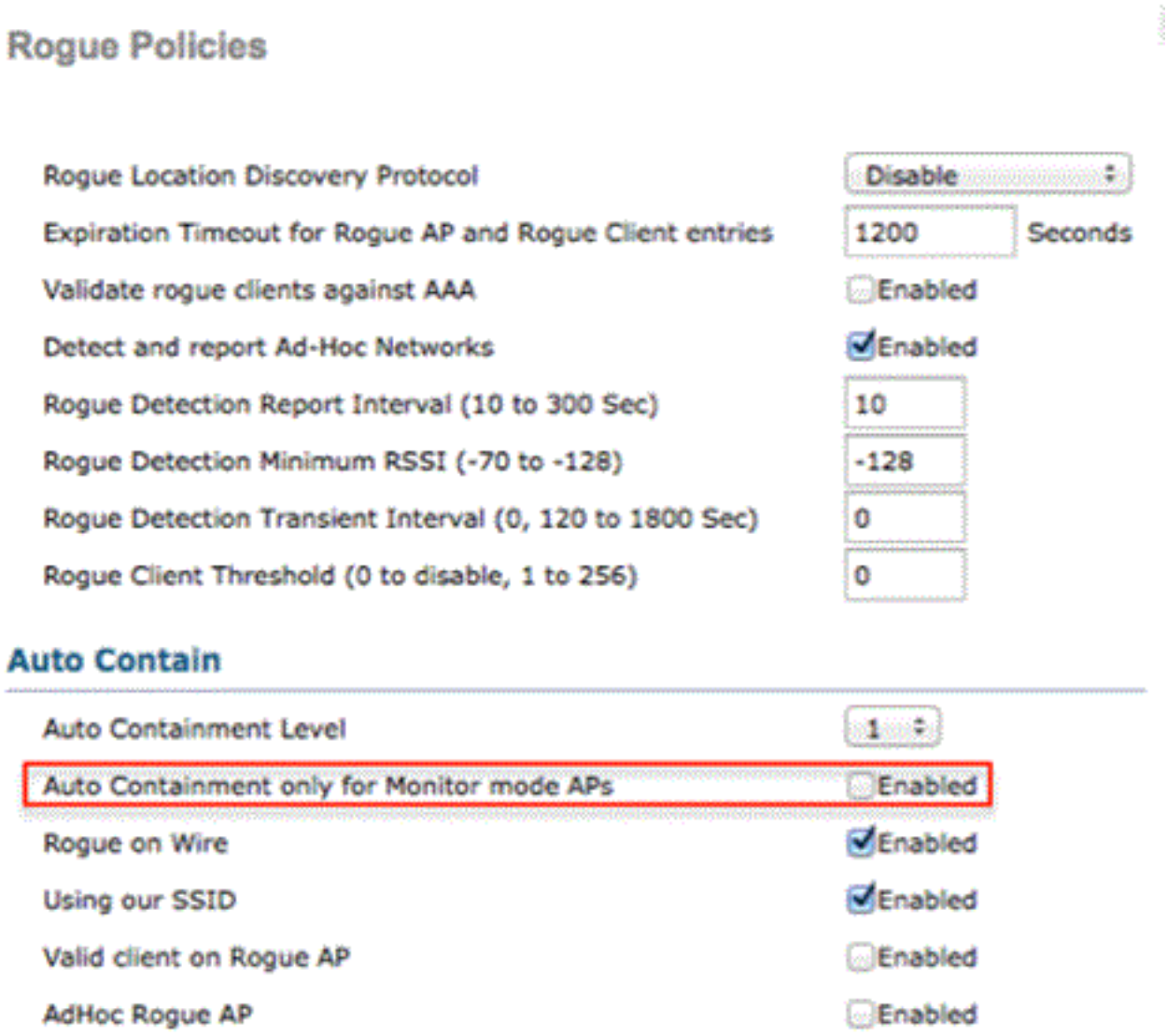
Usted puede verificar que el módulo WSSI usando la consola AP detectara a un granuja AP. De la consola, ingrese el **comando all ap d2 del granuja del rm del capwap de la demostración**. Esto visualiza a todo el granuja AP visto en la radio del módulo WSSI.

```
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
```

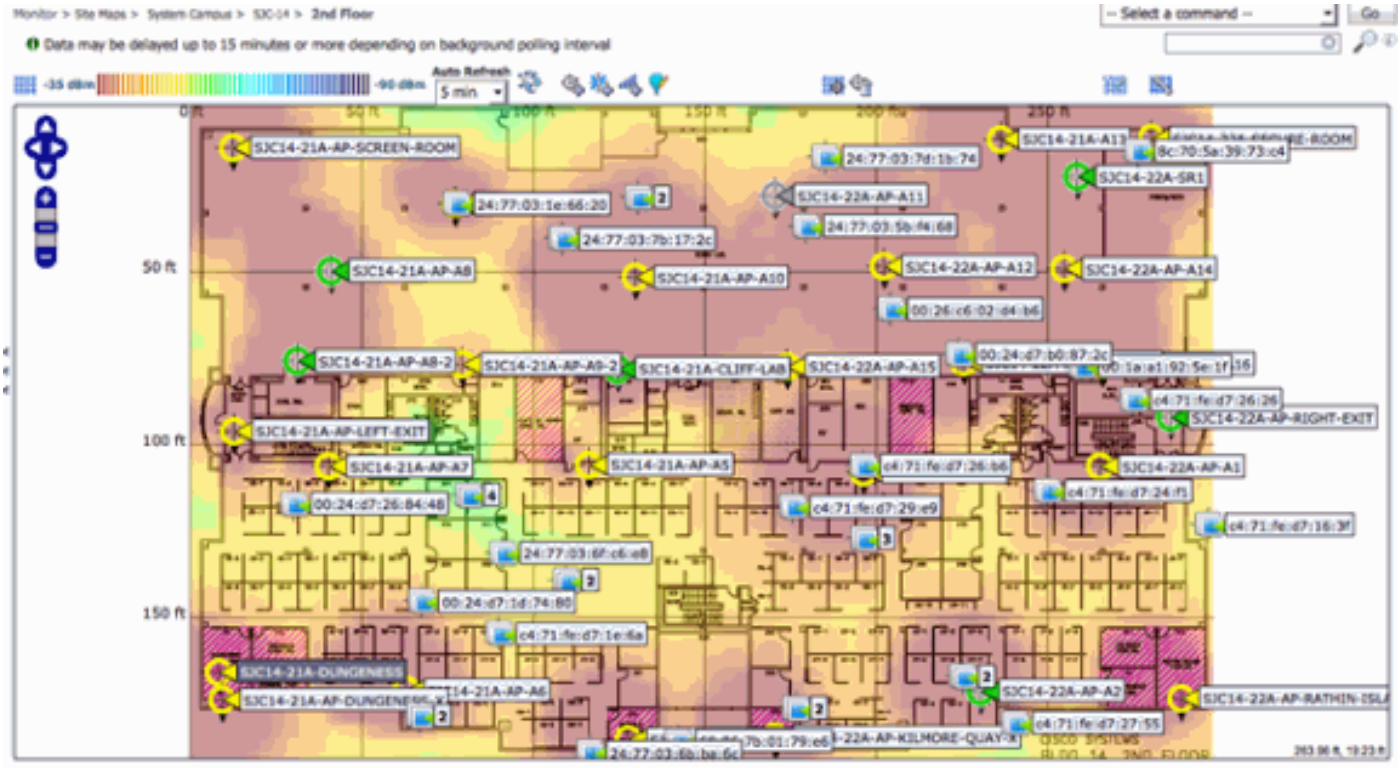
Contención rogue usando el módulo WSSI

El módulo WSSI es un módulo 0x4 (reciba las Antenas solamente), significando que la contención del granuja será realizada en la radio 2.4GHz o 5GHz. Para configurar el WSSI para contener automáticamente los AP rogue, usted debe asegurarse de que en el WLC GUI bajo Seguridad > las directivas inalámbricas de la protección > eliminan las plantas débiles las directivas > al general que la **contención auto solamente para el modo monitor AP** no está habilitada (véase el tiro de siguiente pantalla). El resto de las casillas de verificación pueden ser habilitadas.



Enterado-ubicación del contexto en el módulo WSSI

Cuando está conectado con Cisco MSE, el módulo WSSI proporciona el contexto enterado – los datos de la ubicación con la misma exactitud que un MMAP.



Autorización del módulo WSSI

El módulo WSSI utiliza las licencias del modo monitor del wIPS.

Información Relacionada

- Soporte Técnico y Documentación - Cisco Systems