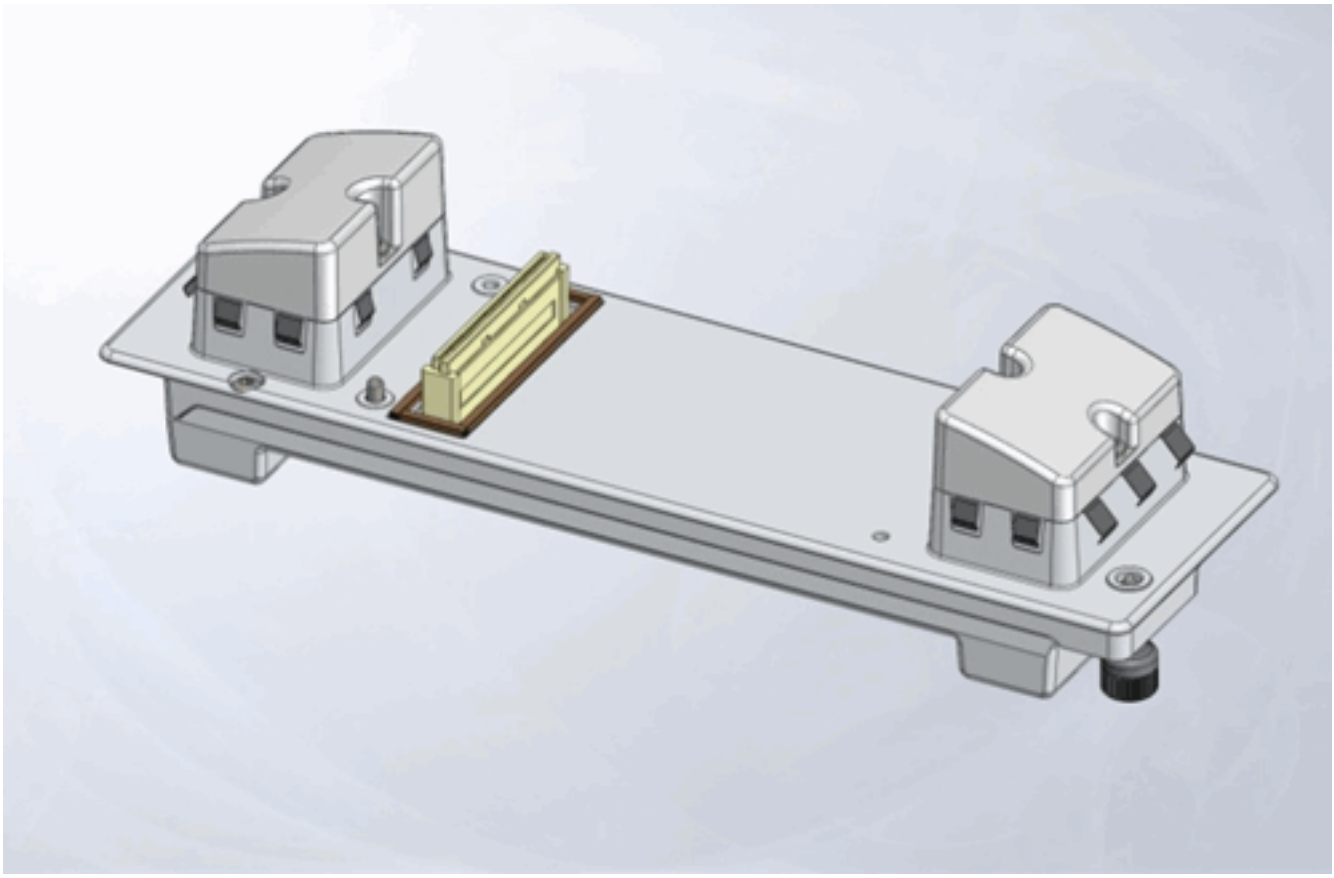
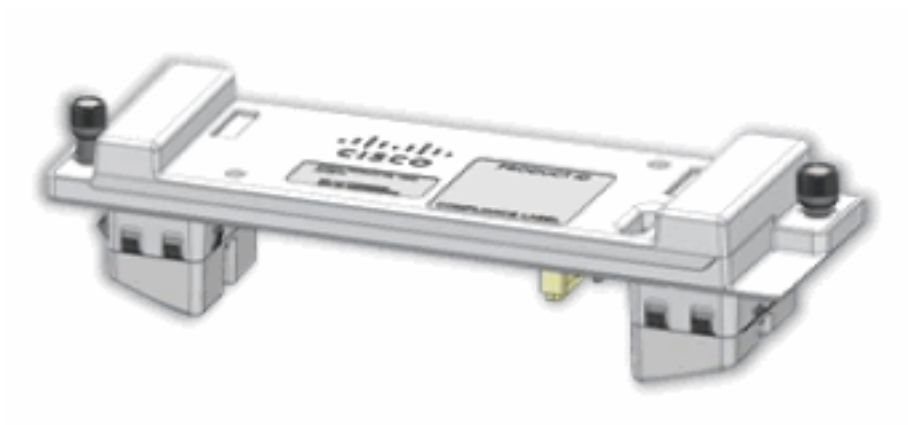
Guida all'installazione del modulo Aironet AP per WSSI

Sommario

Introduzione

Questo documento offre linee guida generali per la configurazione e l'implementazione di Cisco Aironet Access Point Module per la sicurezza wireless e le funzionalità di intelligence dello spettro (WSSI). Il WSSI è un modulo aggiuntivo che può essere inserito in punti di accesso modulari, ad esempio i Cisco serie 3600 AP.





Prerequisiti

Requisiti

Nessun requisito specifico previsto per questo documento.

Componenti usati

Il modulo Wireless Security and Spectrum Intelligence richiede almeno le versioni del codice:

- Wireless LAN Controller (WLC) - Versione 7.4.xx.xx o successiva
- Access Point (AP) - Versione 7.4.xx.xx o successiva
- Prime Infrastructure (PI) - Versione 1.3.xx.xx o successiva
- Mobility Services Engine (MSE) - Versione 7.4.xx.xx o successiva

Convenzioni

Per ulteriori informazioni sulle convenzioni usate, consultare il documento Cisco sulle convenzioni nei suggerimenti tecnici.

Panoramica del prodotto

Il modulo Cisco Wireless Security and Spectrum Intelligence sfrutta il design modulare flessibile del Cisco Aironet serie 3600 AP e assicura una scansione della sicurezza e una funzionalità di intelligence dello spettro senza precedenti e sempre attive. In questo modo è possibile evitare le interferenze della radiofrequenza (RF) per ottenere una copertura e prestazioni migliori sulla rete wireless.

- Monitoraggio e mitigazione 24 ore su 24, 7 giorni su 7 dello spettro completo per WIPS, CleanAir, consapevolezza del contesto, rilevamento di anomalie e gestione delle risorse radio

- Protezione contro le minacce aWIPS 24 ore su 24, 7 giorni su 7
- Protezione e copertura dello spettro 23 volte superiore
- Oltre il 30% di risparmio sui costi in conto capitale rispetto alla modalità di monitoraggio dedicata AP
- Configurazione Zero Touch

Il modulo WSSI aggiornabile sul campo è una radio dedicata che scarica tutti i servizi di monitoraggio e sicurezza dal client/data serving radio al modulo security monitor. Ciò consente non solo di migliorare le prestazioni dei client, ma anche di ridurre i costi eliminando la necessità di punti di accesso in modalità monitor dedicati e dell'infrastruttura Ethernet necessaria per collegare tali dispositivi alla rete.

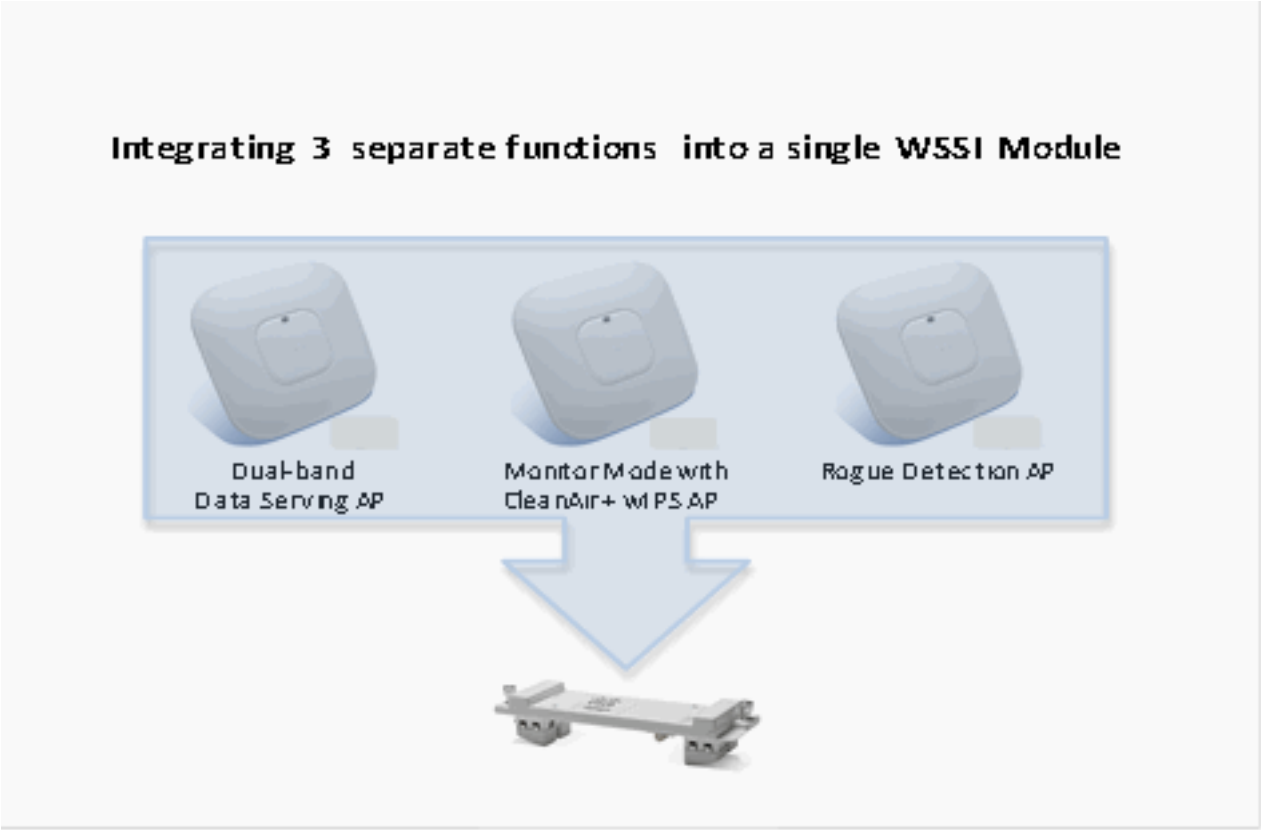
Insieme, i punti di accesso serie 3600 e il modulo WSSI consentono di fornire funzioni di sicurezza e analisi dello spettro allo stato dell'arte per i client Wi-Fi su tutti i canali, sia nelle bande a 2,4 GHz che a 5 GHz.

Una volta installato, il modulo esegue costantemente la scansione di tutti i canali per garantire la massima sicurezza e affidabilità dell'esperienza wireless del settore.

Vantaggi della modalità WSSI

Modalità locale avanzata (ELM):

- Riduzione dei costi e delle operazioni di rete. Integrando il modulo WSSI nella serie 3600, è possibile sostituire fino a tre dispositivi separati. In questo modo è possibile disporre di tre funzioni distinte in un unico access point serie 3600 multifunzione.

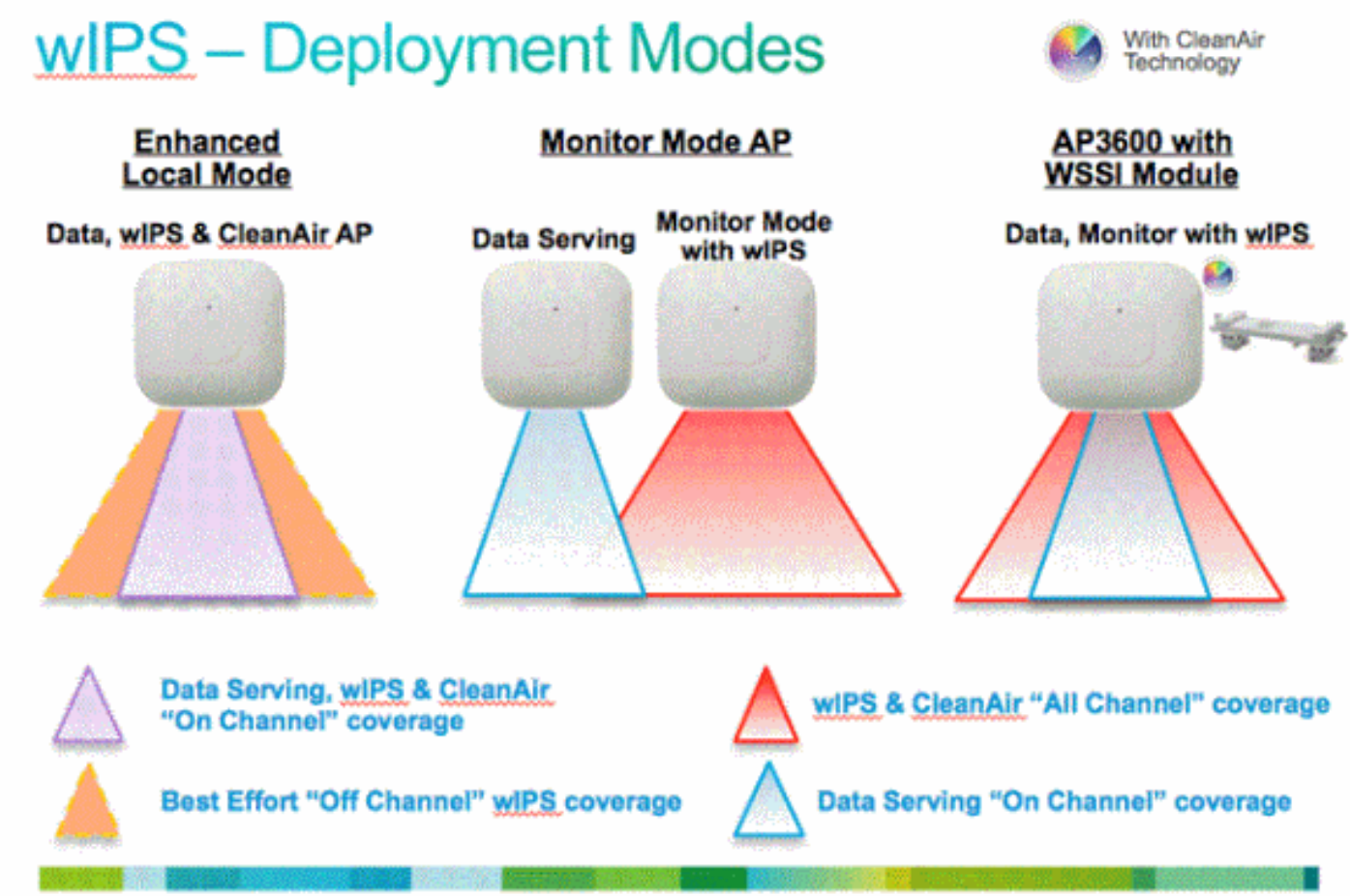


- I clienti possono ora utilizzare un'unica connessione Ethernet (cavo e porta) nella propria rete cablata, in alternativa a quelli che normalmente richiederebbero fino a tre cavi Ethernet separati e una porta di accesso nella propria rete cablata. Ciò riduce notevolmente i costi di

capitale.

- Integrando tutte queste funzionalità in un unico punto di accesso, i clienti semplificano la gestione e il monitoraggio giornaliero dell'infrastruttura e della rete wireless con un numero di punti di accesso notevolmente ridotto. Il modulo WSSI viene visualizzato al WLC e ai sistemi di gestione come una radio aggiuntiva che supporta i dispositivi client 802.11b/g/a/n (2,4 e 5 GHz) all'interno dello specifico access point serie 3600.
- *Zero Touch Configuration*, Install, Power-up and Go. Non è assolutamente necessaria alcuna configurazione per consentire al modulo WSSI di essere operativo e per monitorare e proteggere immediatamente la rete wireless. Il modulo WSSI è inserito e protetto in qualsiasi access point serie 3600. Quando il punto di accesso viene riacceso, il modulo viene inizializzato insieme alle altre radio del punto di accesso e inizia immediatamente il monitoraggio di tutti i canali a 2,4 e 5 GHz per rilevare potenziali minacce alla sicurezza e fonti di interferenza.
- La tecnologia WIPS adattiva consente di rilevare in modo accurato ed efficiente le minacce su tutti i canali derivanti da attacchi via etere, punti di accesso non autorizzati e connessioni ad hoc, nonché di classificare, notificare, mitigare e creare report per un monitoraggio costante e una gestione proattiva. Lavora in abbinamento a Cisco Mobility Services Engine (MSE).

OLMO:



- Aggiunge la scansione di sicurezza wIPS per la scansione 24 ore su 24, 7 giorni su 7, su canali (2,4 GHz e 5 GHz), con il miglior supporto fuori canale.
- L'access point è inoltre al servizio dei clienti e, con la serie G2 di access point, consente l'analisi dello spettro CleanAir sui canali (2,4 GHz e 5 GHz).

Modalità monitor:

- Il punto di accesso in modalità monitor (MMAP) è dedicato al funzionamento in modalità monitor e ha la possibilità di aggiungere la scansione di sicurezza wIPS di tutti i canali (2,4 GHz e 5 GHz).
- La serie G2 di punti di accesso consente l'analisi dello spettro CleanAir su tutti i canali (2,4 GHz e 5 GHz).
- Le MMAP non servono i client.

AP3600 con modulo WSSI: L'evoluzione della sicurezza wireless e dello spettro

- Il primo punto di accesso del settore che facilita il servizio clienti simultaneo, la scansione di sicurezza wIPS e l'analisi dello spettro utilizzando la tecnologia CleanAir.
- Radio dedicata da 2,4 e 5 GHz con antenne che consente la scansione 24 ore su 24, 7 giorni su 7 di tutti i canali wireless nelle bande da 2,4 e 5 GHz.
- Un'unica infrastruttura Ethernet semplifica il funzionamento con un numero inferiore di dispositivi per gestire e ottimizzare il ritorno sull'investimento dell'infrastruttura wireless AP3600 e dell'infrastruttura cablata Ethernet.

Evolution of Wireless Security & Spectrum

	Good	Better	Best
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

- Tecnologia Cisco CleanAir: fornisce uno spettro intelligente proattivo ad alta velocità per contrastare i problemi di prestazioni dovuti alle interferenze wireless. La prima tecnologia di analisi RF all'avanguardia del settore che controlla e classifica i modelli energetici (firme) dei dispositivi che possono influire in modo significativo sulla qualità di una rete wireless.
- Gestione risorse radio (RRM): gestione RF avanzata e semplificata, che si adatta automaticamente all'ambiente di rete wireless in base alle informazioni ricevute dalla tecnologia Cisco CleanAir. Una volta identificati gli interferenti, RRM è in grado di spostare i dispositivi client verso i canali lontani dall'interferenza e di regolare la potenza di transito per allontanarla dalla fonte di interferenza. In questo modo si ottiene una migliore qualità RF per l'utente.
- Rilevamento server non autorizzati: rileva e segnala l'accesso alla rete backdoor e l'accesso

ai client wireless.
- Riconoscimento di località e contesto: consente di rilevare in tempo reale l'endpoint wireless e di tenerne traccia.

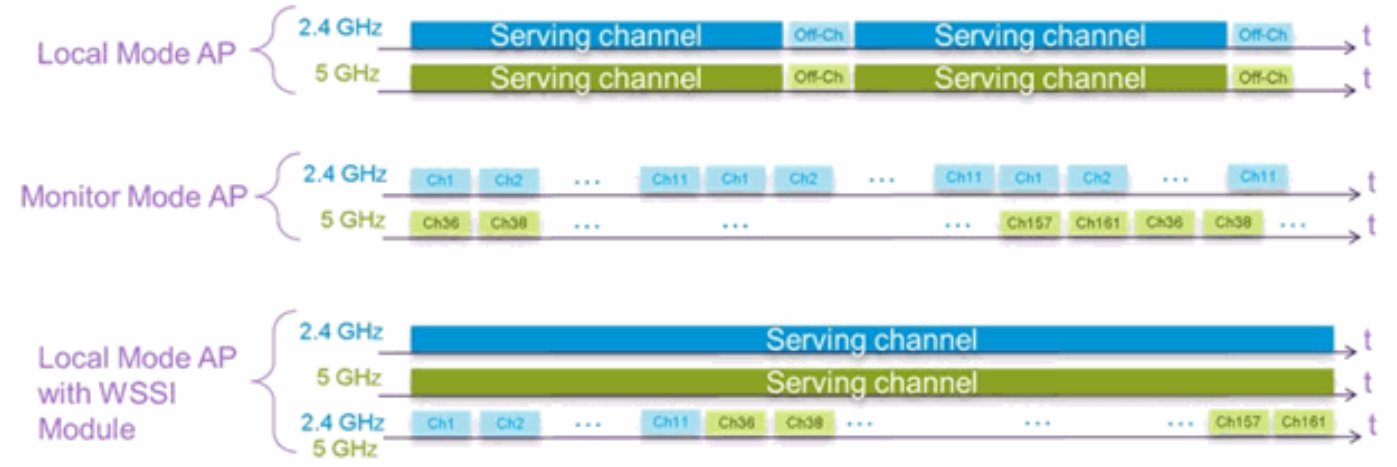
Grazie a queste caratteristiche, il modulo Cisco Wireless Security and Spectrum Intelligence, insieme al Cisco serie 3600 AP, fornisce la rete wireless di classe enterprise più sicura e solida possibile per gli utenti e i dati aziendali.

On-channel e Off-channel tramite il modulo WSSI

Un punto di accesso in modalità locale cerca gli interferenti CleanAir e gli attaccanti wIPs sul canale. Questo significa che l'access point esegue la scansione solo del canale che sta servendo. Un access point in modalità locale con un canale di servizio radio da 2,4 GHz 1 e un canale di servizio radio da 5 GHz 64, fornisce protezione solo sui canali 1 e 64.

Una MMAP cerca gli interferenti CleanAir e gli attaccanti wIP fuori dal canale. Ciò significa che l'access point esegue la scansione di tutti i canali. La radio a 2,4 GHz esegue la scansione di tutti i canali a 2,4 GHz, mentre il canale a 5 GHz esegue la scansione di tutti i canali a 5 GHz.

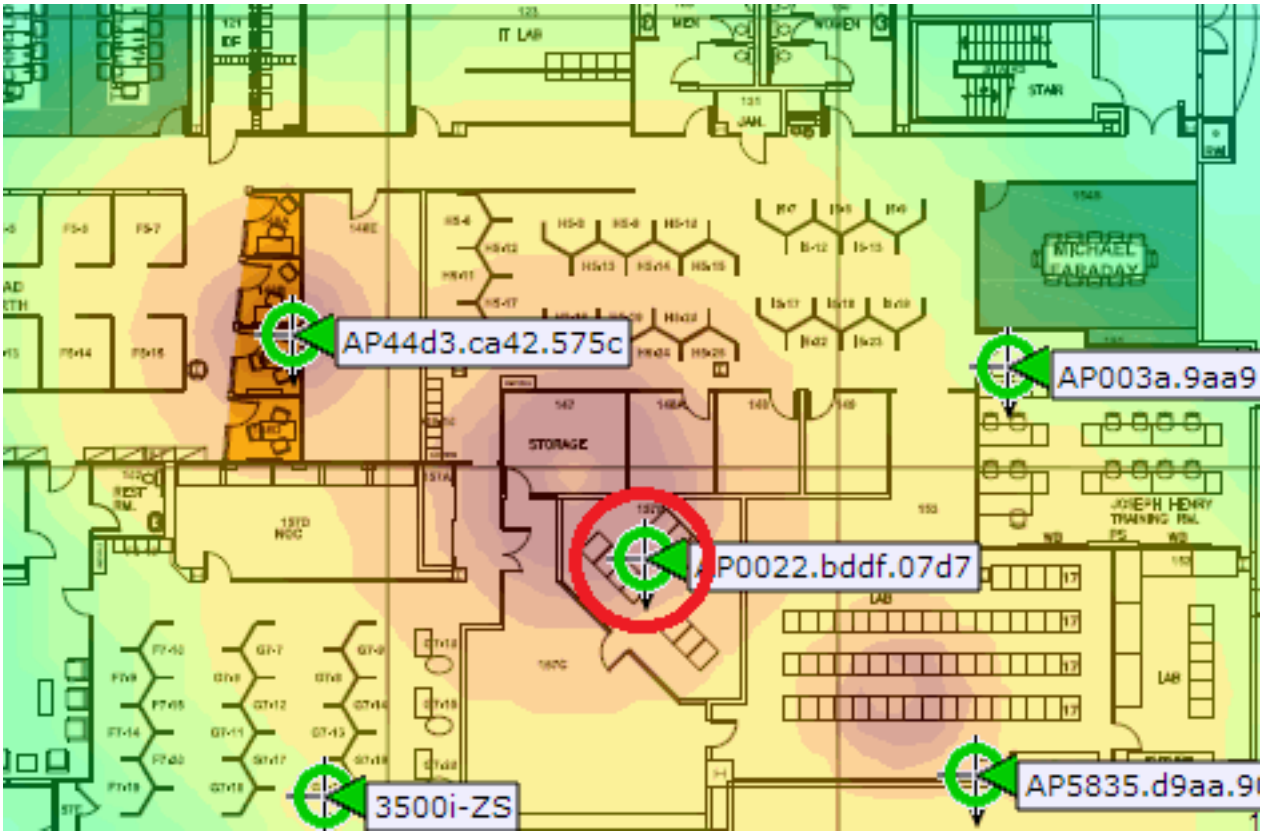
Un Cisco serie 3600 AP utilizza una combinazione di canali on-channel e off-channel. Le radio da 2,4 GHz e 5 GHz eseguono la scansione su canale, mentre il modulo WSSI esegue la scansione fuori canale, passando da un canale all'altro tra i canali da 2,4 GHz e 5 GHz.



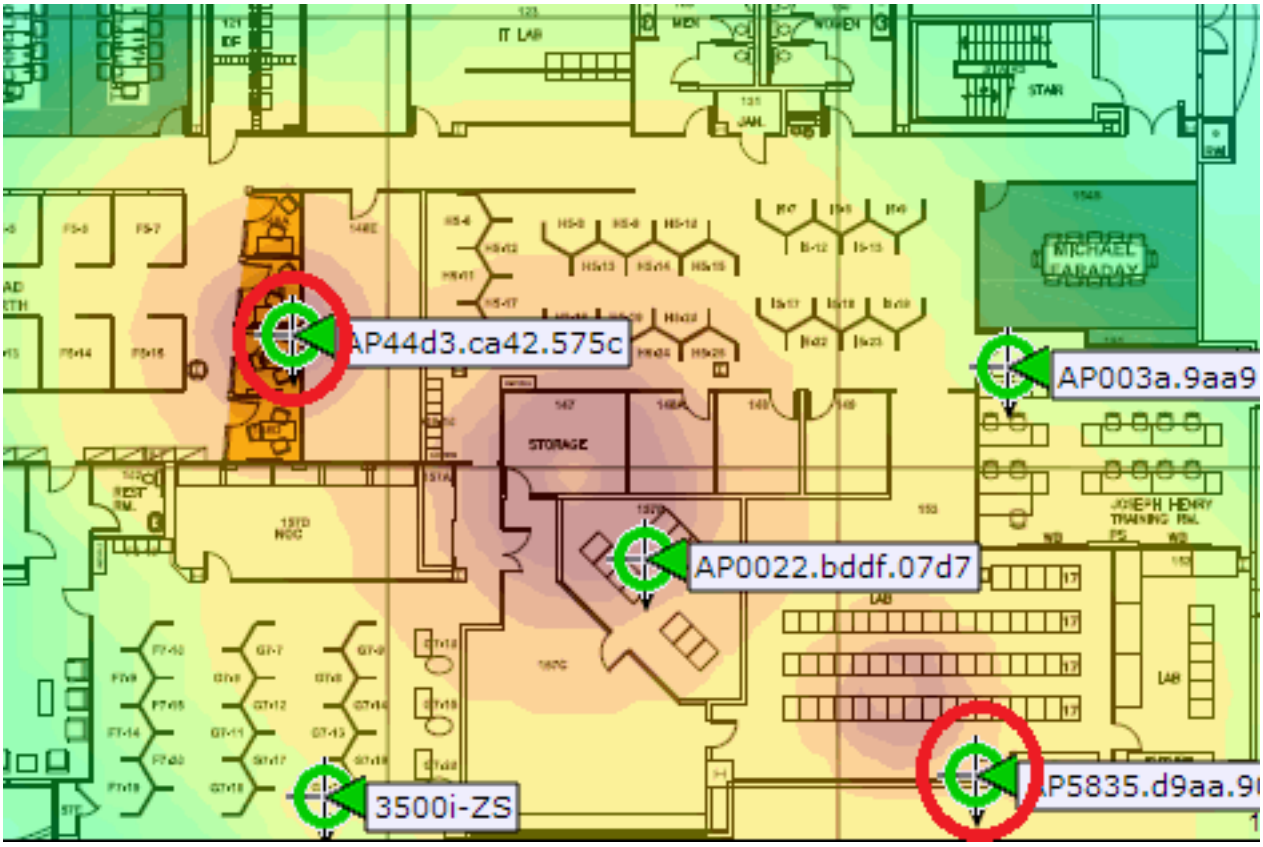
Densità di distribuzione consigliata per il modulo WSSI

Nelle implementazioni tradizionali di Monitor AP, Cisco consiglia un rapporto di 1 MMAP ogni 5 AP in modalità locale. La scelta può variare in base alla progettazione della rete e alle indicazioni degli esperti per una copertura ottimale. Con il modulo WSSI, esistono diversi suggerimenti di distribuzione basati sulla funzionalità per ottenere la parità di copertura con un MMAP.

Per CleanAir, si consiglia di installare 1 modulo WSSI ogni 5 access point locali o Flexconnect. Questa distribuzione 1:5 offre le stesse prestazioni di una MMAP abilitata per CleanAir, ma consente comunque all'AP di servire i client. Questa è una distribuzione consigliata per un modulo WSSI che esegue CleanAir:

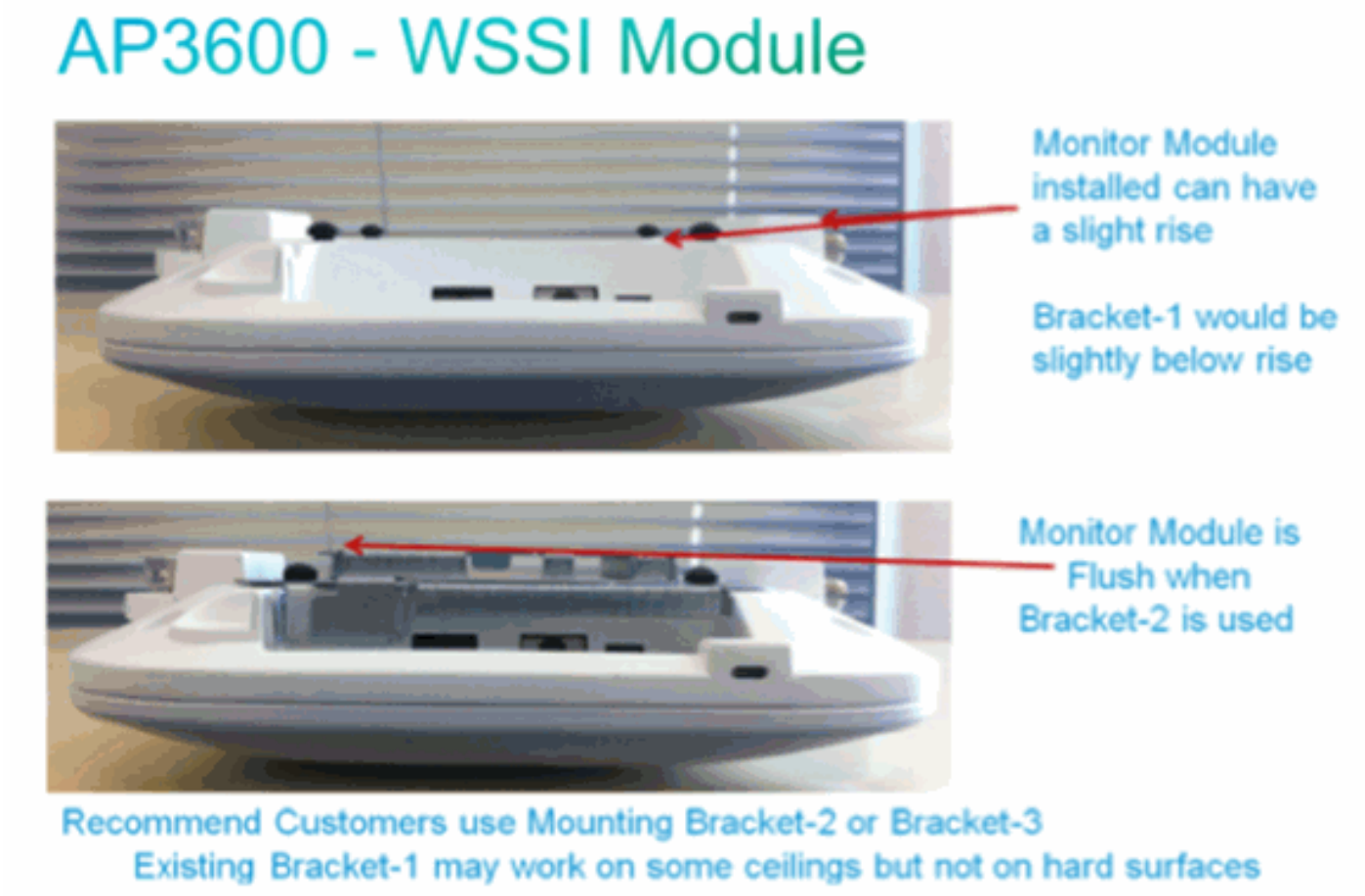


Per la protezione IPS, si consiglia di distribuire 2 moduli WSSI ogni 5 punti di accesso locali o FlexConnect. Il tempo di rilevamento wIPS per un attacco off-channel è circa il doppio di quello di un MMAP. Per fornire la parità di rilevamento wIPS è pertanto necessaria una distribuzione 2:5. Questa è la distribuzione consigliata per un modulo WSSI che esegue la protezione IPS:



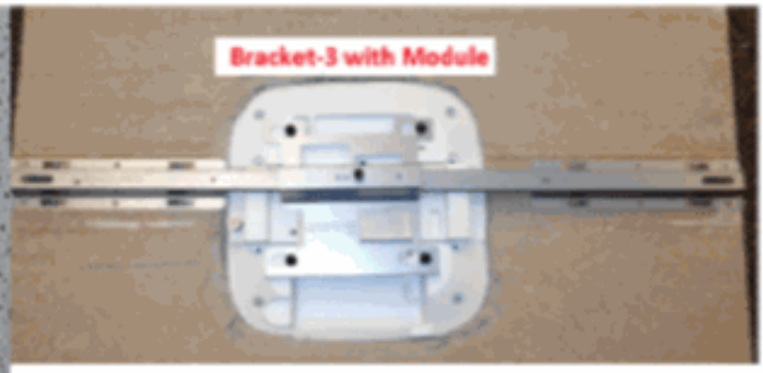
Cisco 3600 AP con modulo WSSI utilizza la scansione sia su canale che fuori canale per fornire una soluzione leader del settore servendo i client.

[Installazione del modulo WSSI]



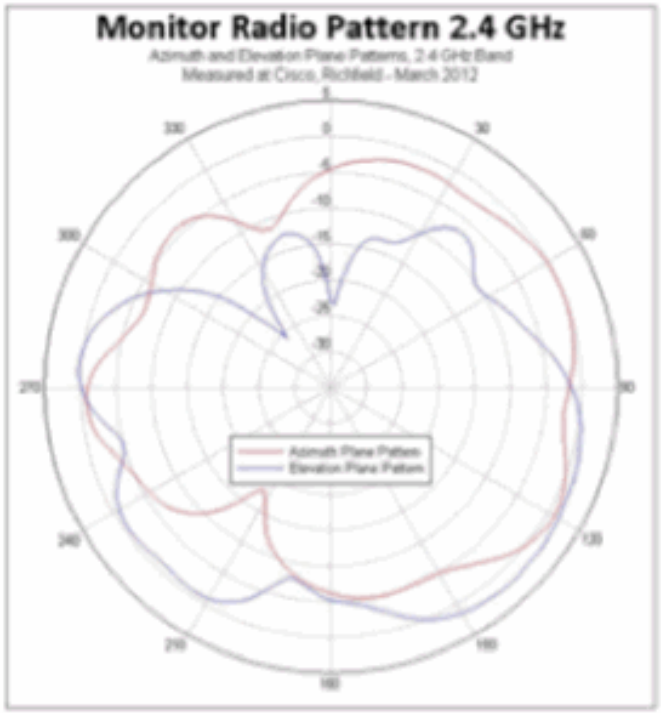
AP3600 with WSSI Module and Bracket-3

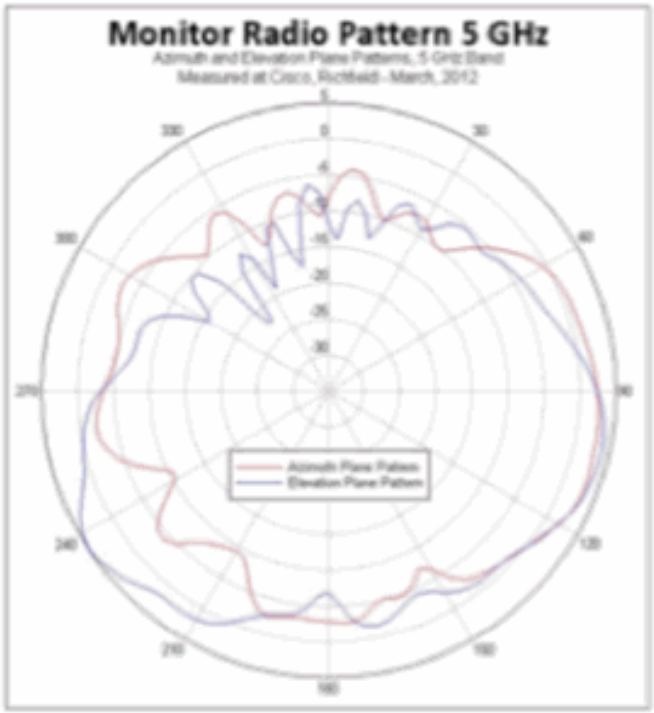
Elegant in-tile flush mount



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





Configurazione per il modulo WSSI AP3600

Nessuna configurazione necessaria per il modulo WSSI. Il modulo analizza automaticamente tutti i canali su entrambe le bande usando le sue 0x4 (solo ricezione) Antenne 0 Tx x x 4 Antenne Rx.

Il modulo WSSI è attivo solo sugli AP3600 configurati in modalità locale o FlexConnect. Il modulo WSSI è disattivato in tutte le altre modalità.

Requisiti di alimentazione per il modulo WSSI

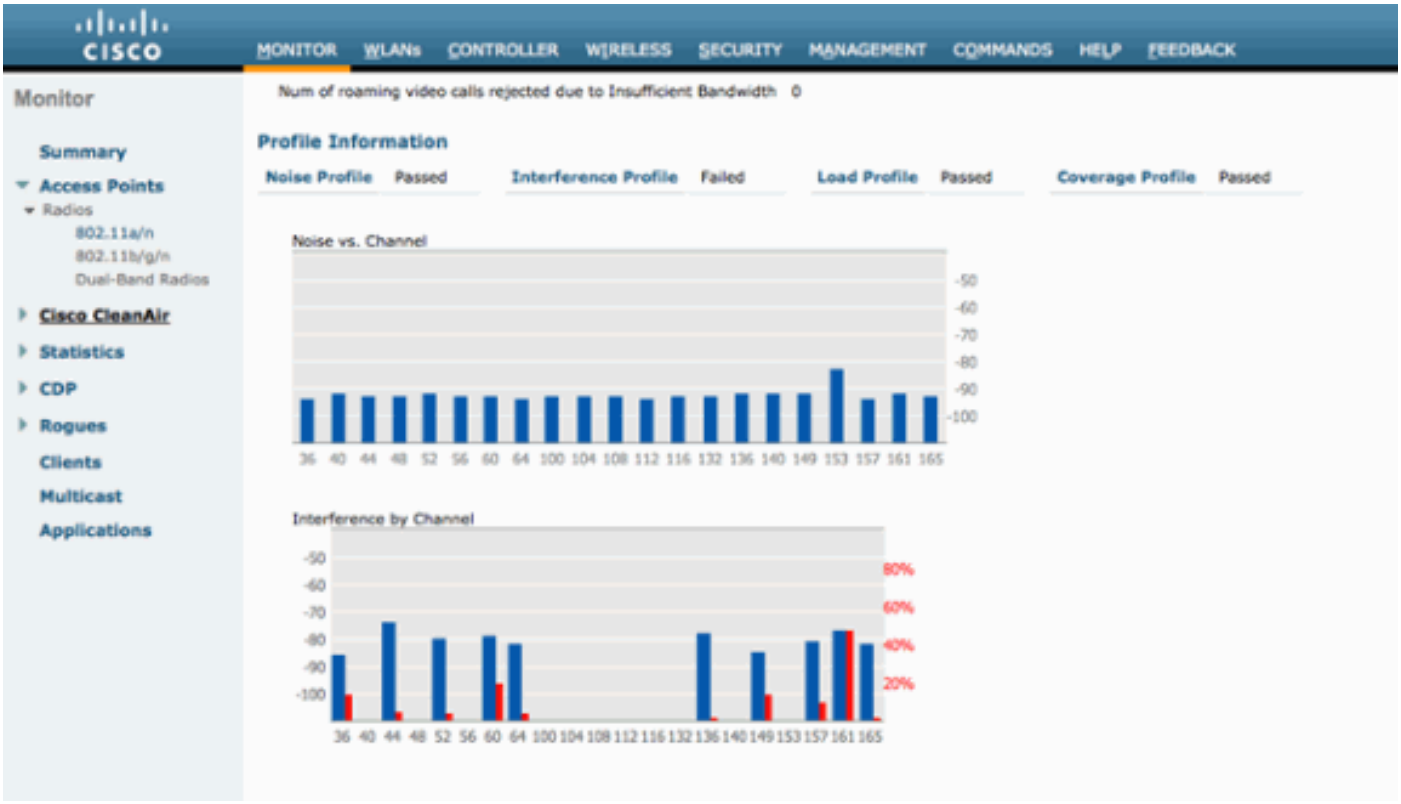
L'access point serie 3600 con un modulo WSSI installato supera i 15,4 watt (802.3af). L'access point richiede (802.3at - PoE+), Enhanced PoE, un alimentatore CA locale o l'iniettore Cisco PoE (AIR-PWRINJ4).

Note:

- La funzionalità PoE avanzata è stata creata da Cisco ed è un precursore di 802.3at PoE+. Fornisce fino a 20 W di potenza.
- PoE+ può fornire fino a 30 W di potenza.

Gestione delle risorse radio sul modulo WSSI

Il modulo WSSI esegue tutte le misurazioni RRM sia sulla banda a 2,4 GHz che su quella a 5 GHz. Le misurazioni vengono visualizzate nella GUI del WLC in Monitor > Access Point > 802.11a/n > AP_NAME > Dettagli o Monitor > Access Point > 802.11b/g/n > AP_NAME > Dettagli.



CleanAir sul modulo WSSI

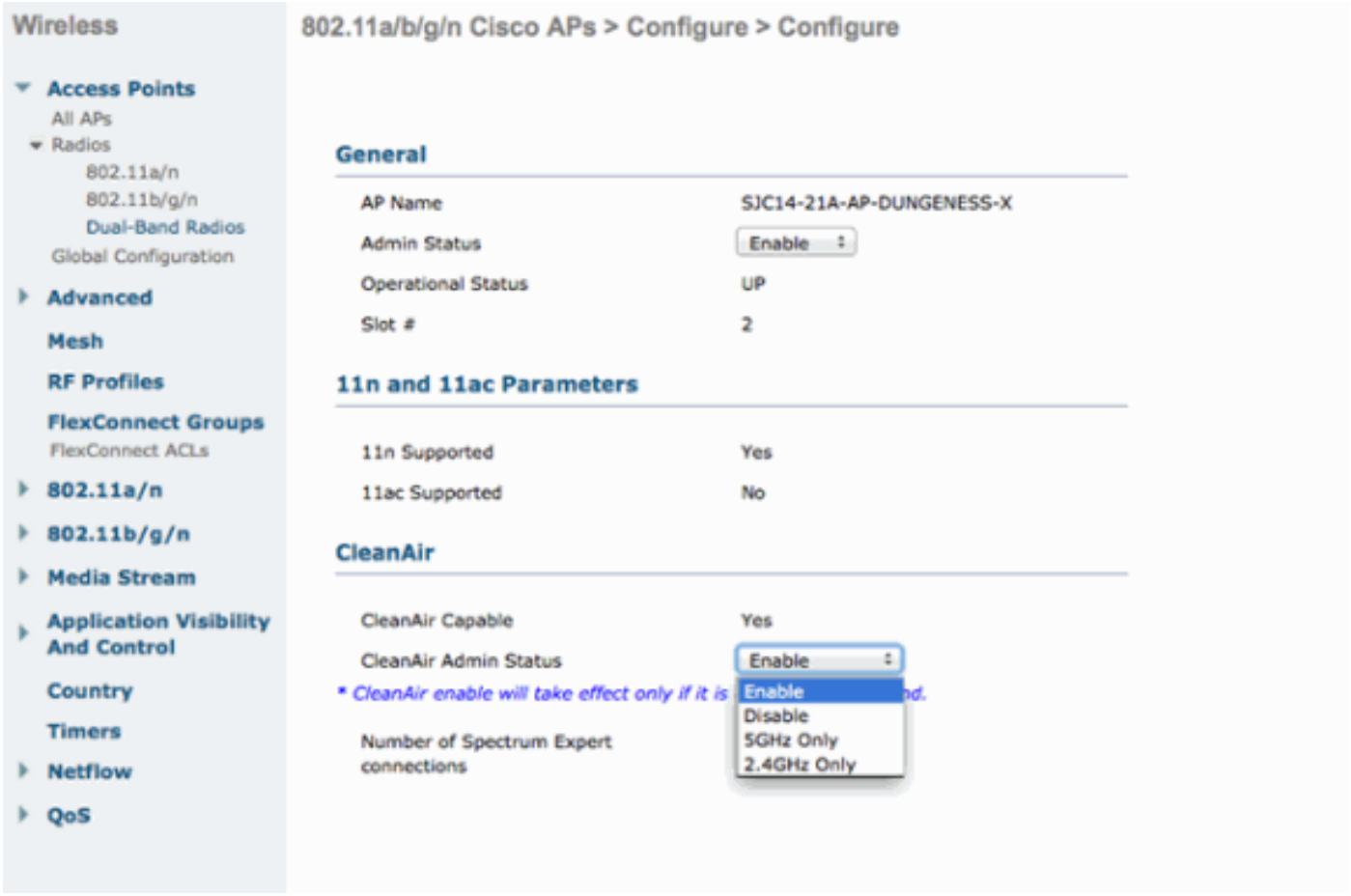
Il modulo WSSI rileva interferenze CleanAir con la stessa precisione di un MMAP. Cisco consiglia di distribuire il modulo WSSI con una densità di 1:5, in cui deve essere presente un modulo WSSI ogni 5 AP. Si tratta della stessa densità consigliata per un MMAP.

Quando il modulo WSSI è abilitato senza modalità secondaria, il modulo analizza sia la banda a 2,4 GHz che la banda a 5 GHz. Il modulo risiede su ciascun canale per 1,2 sec e cerca gli interferenti CleanAir.

CleanAir può essere abilitato solo su 2,4 GHz, solo su 5 GHz e su 2,4 GHz e 5 GHz. Questa opzione è selezionabile dalla CLI del WLC o dalla GUI. Di seguito è riportato un esempio di configurazione di CleanAir sulla CLI del WLC:

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

La stessa configurazione può essere applicata sulla GUI tramite Wireless > Radio dual-band > Configura. Di seguito è riportato un esempio:



Per verificare che l'interferente CleanAir sia stato rilevato dal modulo WSSI, usare il comando **show cleanair interferers** dalla console 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 stessa configurazione può essere applicata sulla GUI tramite Wireless > Radio dual-band > Configura. Di seguito è riportato un esempio:

Gli interferenti di CleanAir vengono segnalati nella GUI del WLC. Gli interferenti vengono visualizzati PER BAND. Ciò significa che gli interferenze rilevati sul modulo WSSI sulla banda dei 5 GHz vengono visualizzati in Monitor > 802.11a/n > Interference Devices (Monitor > 802.11a/n > Dispositivi di interferenza).

Per verificare che l'interferente CleanAir sia stato rilevato dal modulo WSSI, usare il comando **show cleanair interferers** dalla console 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
```

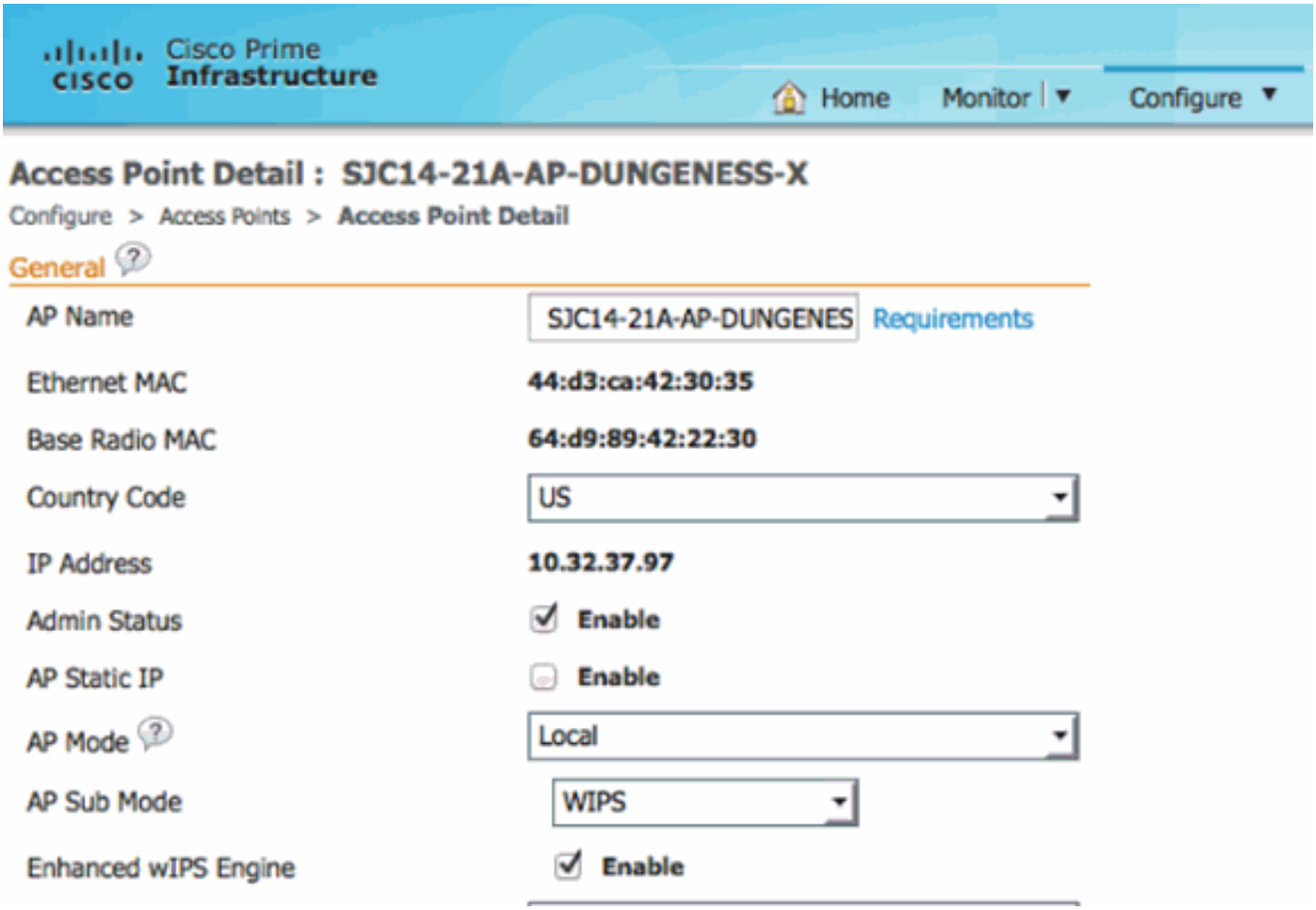
wIPS sul modulo WSSI

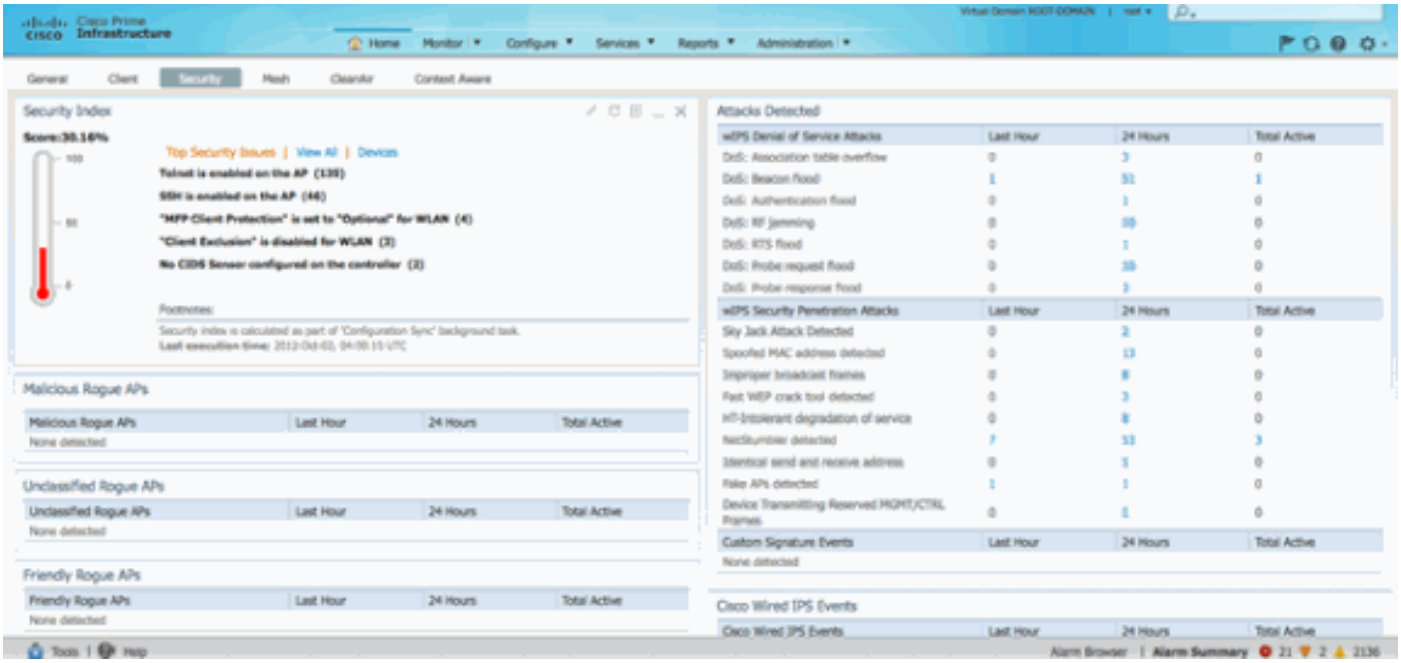
Il modulo WSSI rileva gli hacker wIPS con quasi la stessa precisione di un MMAP. Per i punti di accesso wireless, Cisco consiglia di distribuire il modulo WSSI con un rapporto di 2:5 tra i punti di accesso. Ciò significa che per ogni 5 access point, due devono contenere il modulo WSSI.

Èpossibile configurare due modalità wIPS:

- Modalità secondaria wIPS: consente il rilevamento degli attacchi wIPS e la scansione di tutti i canali per 1.2s. Questa modalità consente al punto di accesso di acquisire ancora tutti i report RRM oltre ai rilevamenti wIPS.
- Modalità wIPS avanzata: abilita il rilevamento degli attacchi wIPS e analizza tutti i canali per 250 ms. Il tempo di permanenza del canale ridotto consente al modulo di sicurezza di rilevare gli aggressori più rapidamente.

Dalla pagina Prime Infrastructure (PI), selezionare Configure > Access Point > AP_NAME. Il modulo WSSI può essere configurato in modalità secondaria wIPS o wIPS + supporto Enhanced wIPS Engine. È possibile eseguire il push anche di questo elemento come parte di un modello di configurazione AP.





Gli attacchi wIPS vengono visualizzati in Prime Infrastructure dalla scheda Home > Security.

La PI mostra una vista a livello di rete, ma è possibile visualizzare l'attacco a un AP3600 con un modulo WSSI usando il comando **show capwap am alarm_NUM** dalla console AP.

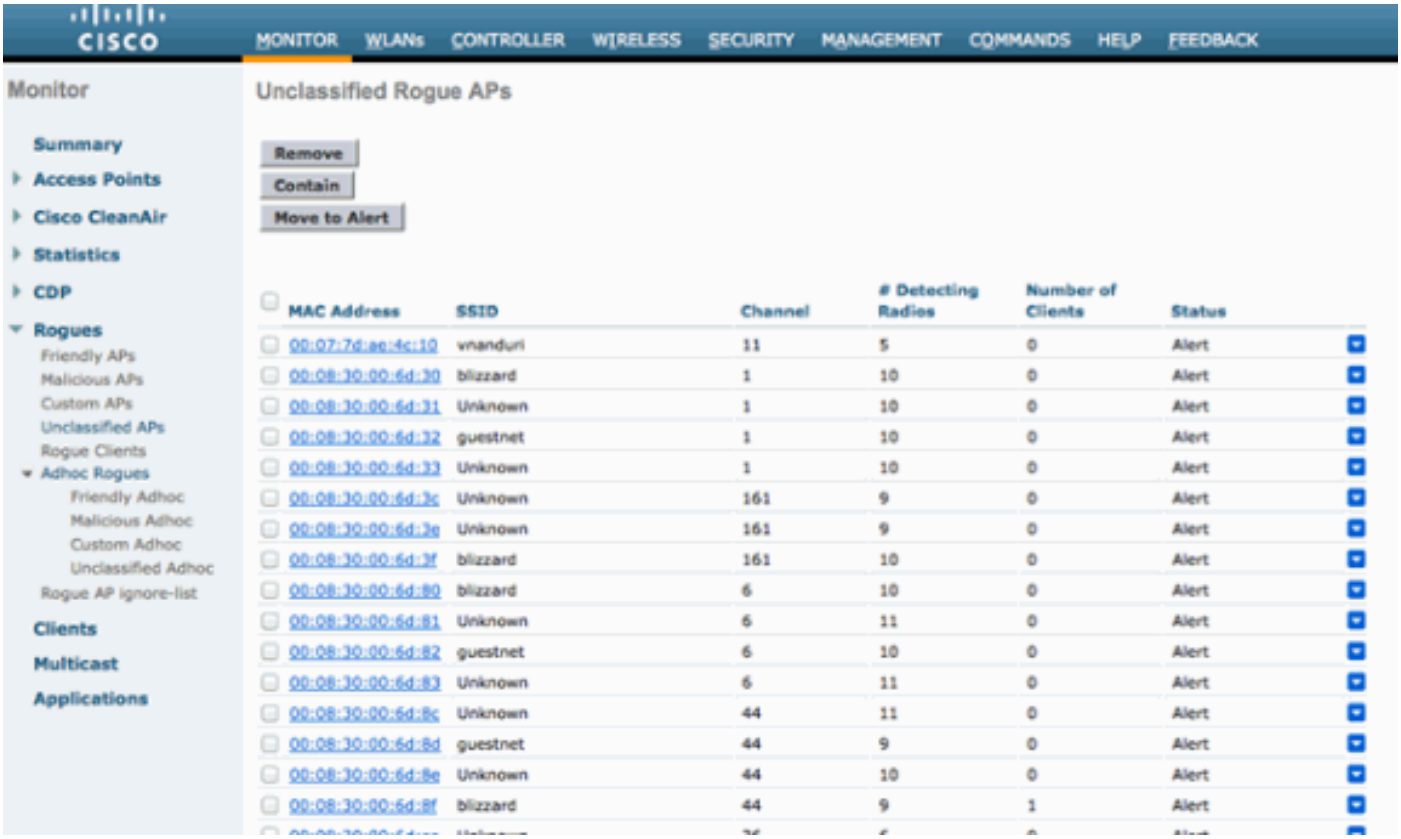
Ad esempio, alarm 52 è un flusso di autenticazione Denial of Service. Per verificare se l'attacco è stato rilevato sul modulo WSSI, usare il comando **show capwap am alarm 52**:

```
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
```

Rogue Detect sul modulo WSSI

Il modulo WSSI rileva access point non autorizzati con la stessa precisione di un MMAP. Un elenco di access point anomali viene visualizzato sia nel WLC che nel PI.

Questo è l'elenco dei Rogue AP non classificati dall'interfaccia utente del WLC. Gli access point non autorizzati possono essere visualizzati nell'interfaccia utente grafica del WLC in Monitor > Rogues.



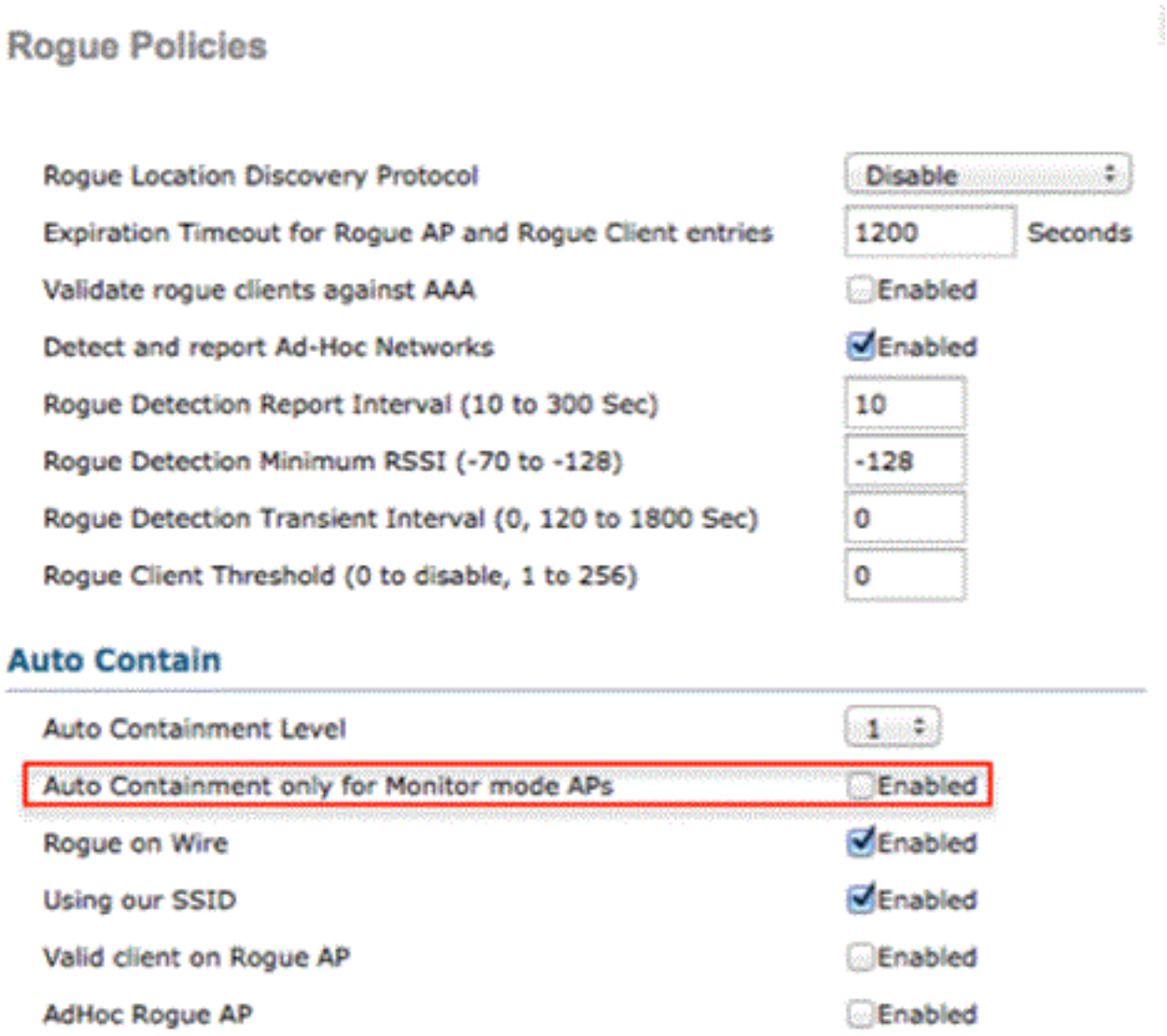
Èpossibile verificare che il modulo WSSI che utilizza la console AP abbia rilevato un punto di accesso non autorizzato. Dalla console, immettere il comando **show capwap rm rogue ap d2 all**. In questo modo vengono visualizzati tutti gli access point non autorizzati rilevati nella radio del modulo WSSI.

```
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
```

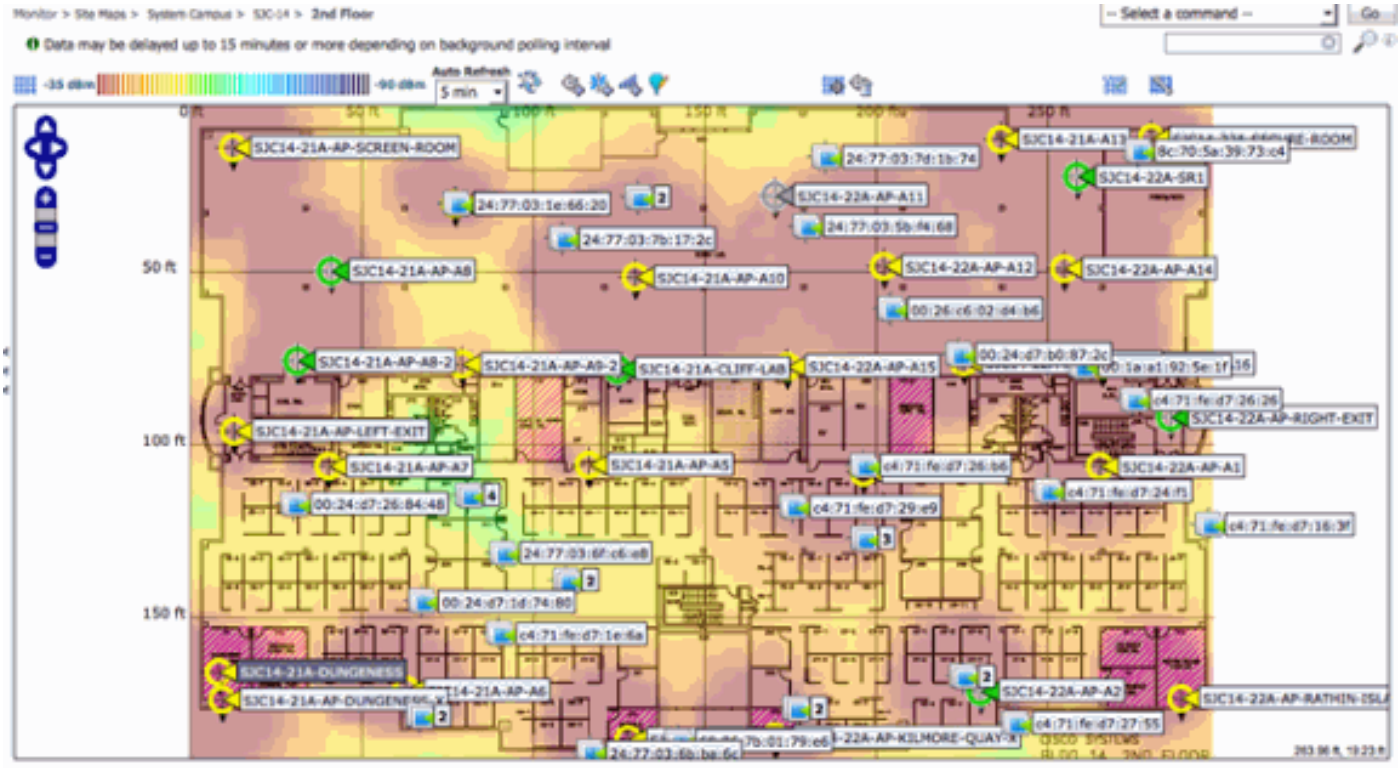
Contenimento Rogue tramite il modulo WSSI

Il modulo WSSI è un modulo 0x4 (solo antenne riceventi), il che significa che il contenimento rogue verrà eseguito sulla radio a 2,4 GHz o 5 GHz. Per configurare il WSSI in modo che contenga automaticamente i punti di accesso non autorizzati, accertarsi che nell'interfaccia utente del WLC in Security > Wireless Protection Policies > Rogue Policies > General (Policy non autorizzati) il **contenimento automatico solo per i punti di accesso in modalità Monitor** non sia abilitato (vedere la schermata successiva). È possibile attivare tutte le altre caselle di controllo.



Posizione sensibile al contesto nel modulo WSSI

Quando collegato a un Cisco MSE, il modulo WSSI fornisce i dati di tipo Context-Aware-Location con la stessa accuratezza di un MMAP.



Licenze modulo WSSI

Il modulo WSSI utilizza licenze in modalità di monitoraggio wIPS.

Informazioni correlate

- Documentazione e supporto tecnico – Cisco Systems