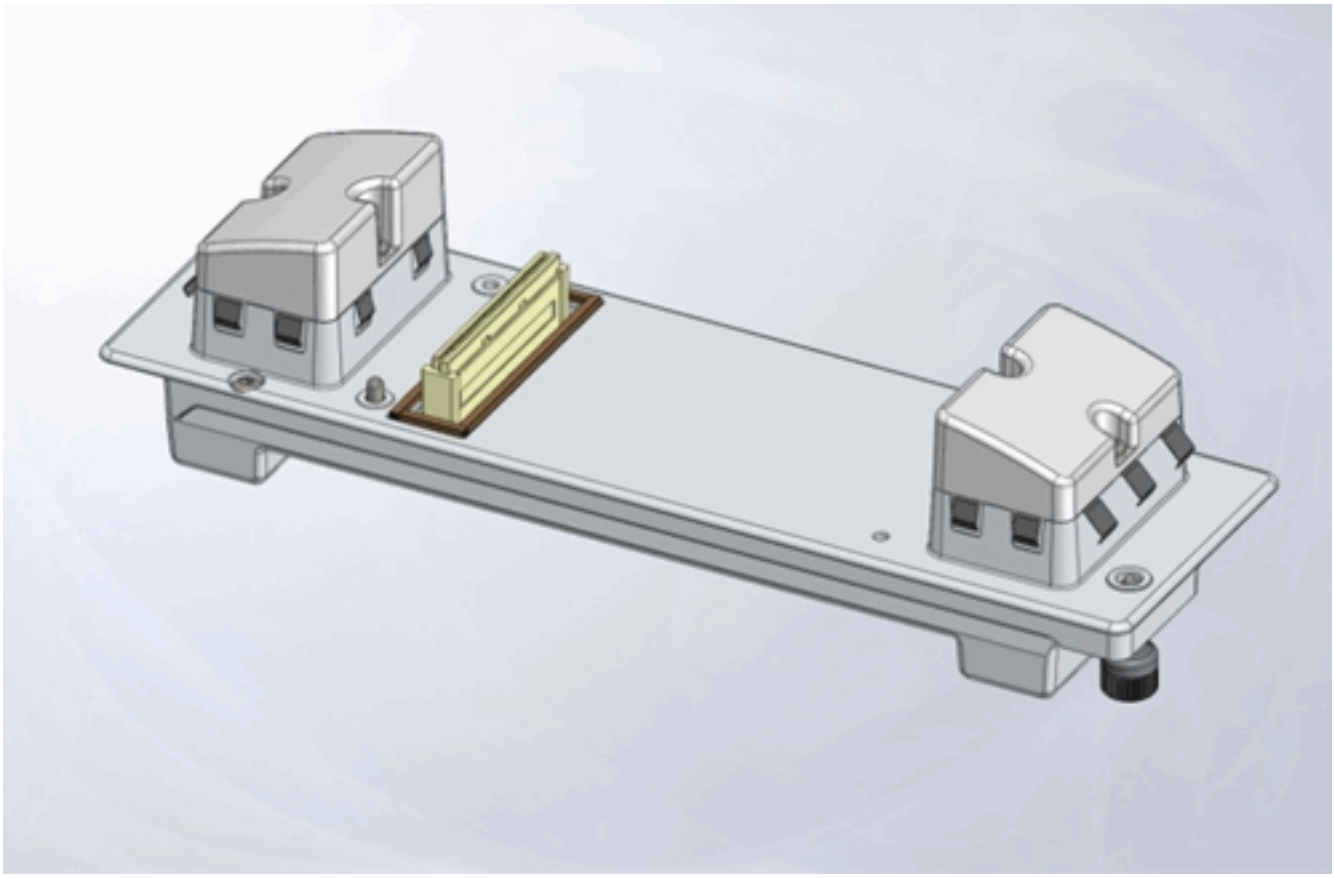
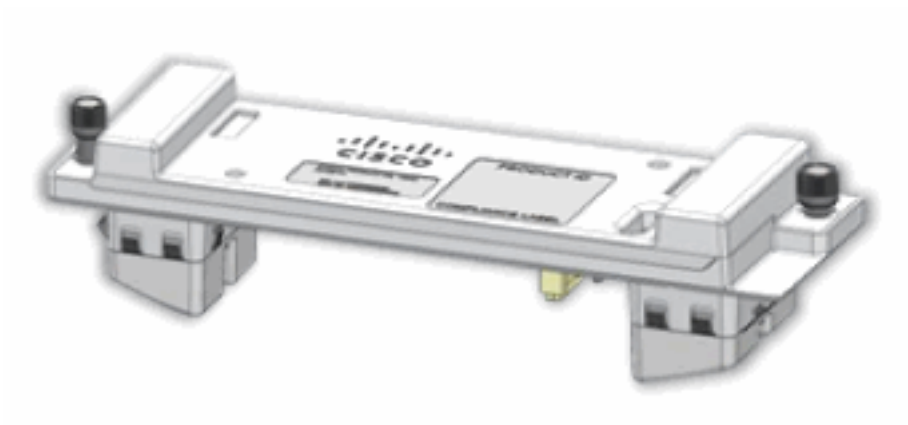
Implementierungsleitfaden für das Cisco Aironet AP-Modul für Wireless Security and Spectrum Intelligence (WSSI)

Inhalt

Einführung

Dieses Dokument enthält allgemeine Richtlinien für die Konfiguration und Bereitstellung des Cisco Aironet Access Point Module for Wireless Security and Spectrum Intelligence (WSSI). Das WSSI ist ein Zusatzmodul, das in modulare Access Points (APs) wie den Cisco AP der Serie 3600 eingesetzt werden kann.





Voraussetzungen

Anforderungen

Für dieses Dokument bestehen keine speziellen Anforderungen.

Verwendete Komponenten

Das Modul Wireless Security and Spectrum Intelligence benötigt die Mindestcodeversionen:

- Wireless LAN Controller (WLC) - Version 7.4.xx.xx oder höher
- Access Point (AP) - Version 7.4.xx.xx oder höher
- Prime Infrastructure (PI) - Version 1.3.xx.xx oder höher
- Mobility Services Engine (MSE) - Version 7.4.xx.xx oder höher

Konventionen

Weitere Informationen zu Dokumentkonventionen finden Sie unter Cisco Technical Tips Conventions (Technische Tipps zu Konventionen von Cisco).

Produktübersicht

Das Cisco Wireless Security and Spectrum Intelligence-Modul bietet dank des flexiblen modularen Designs des Cisco Aironet Access Points der Serie 3600 beispiellose, stets verfügbare Sicherheits-Scans und Spektrumerkennung. Auf diese Weise können Funkstörungen vermieden werden, die eine bessere Abdeckung und Leistung in Ihrem Wireless-Netzwerk ermöglichen.

- Rund-um-die-Uhr-Vollspektrum-Überwachung und -Eindämmung für aWIPS, CleanAir, Kontextsensitivität, Erkennung nicht autorisierter APs und Radio Resource Management
- 24 x 7 On-Channel-Schutz vor aWIPS-Bedrohungen

- 23-fache Sicherheit und Spektrumandeckung
- Kosteneinsparungen von über 30 % bei den Investitionskosten im Vergleich zum AP mit dediziertem Überwachungsmodus
- Konfiguration ohne Benutzereingriff

Das vor Ort aufrüstbare WSSI-Modul ist eine dedizierte Funkeinheit, die alle Überwachungs- und Sicherheitsservices vom Client-/Daten-Funkmodul an das Sicherheitsüberwachungsmodul auslagert. Dies ermöglicht nicht nur eine bessere Client-Leistung, sondern senkt auch die Kosten, da dedizierte Überwachungsmodus-APs und die Ethernet-Infrastruktur für die Verbindung dieser Geräte mit dem Netzwerk entfallen.

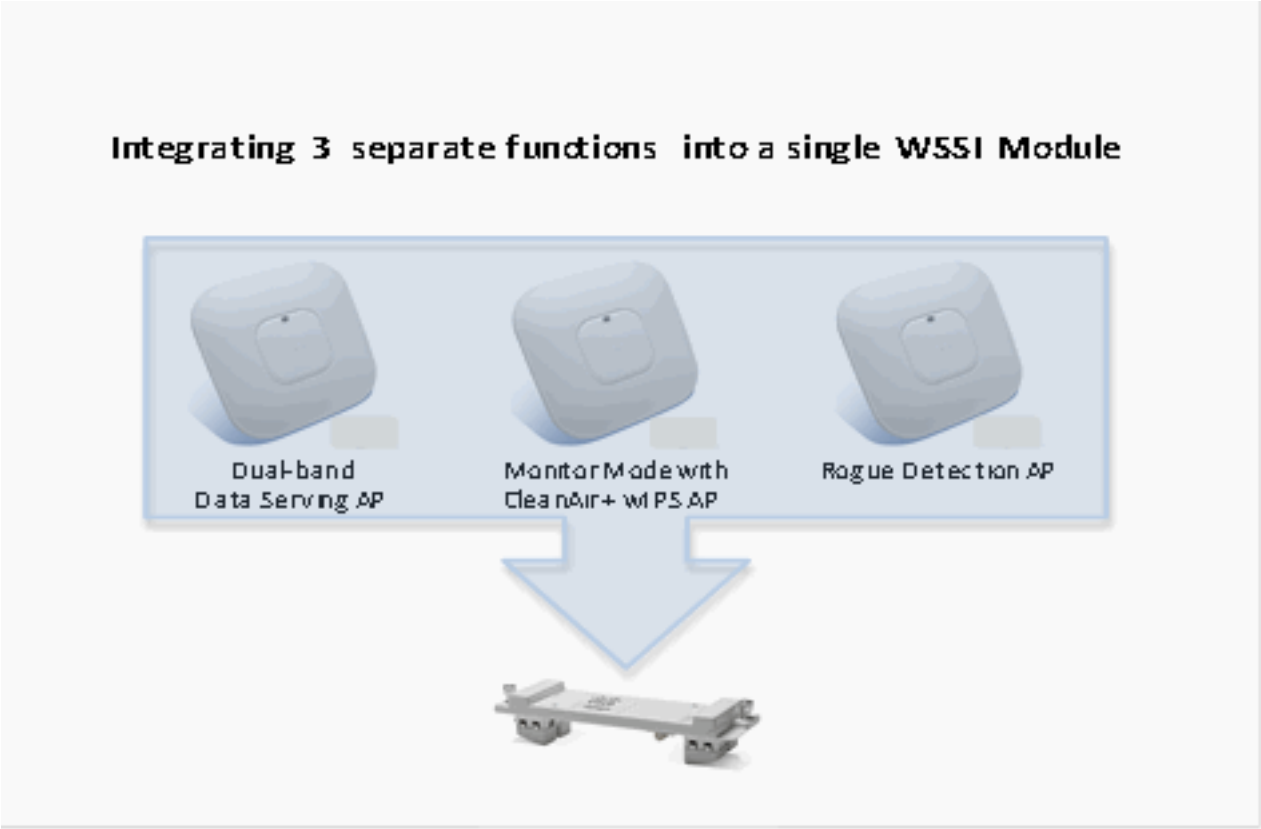
Zusammen ermöglichen die APs der Serie 3600 und das WSSI-Modul die gleichzeitige Bereitstellung hochmoderner Sicherheits- und Spektrumanalysefunktionen für Wi-Fi-Clients auf allen Kanälen, sowohl im 2,4-GHz- als auch im 5-GHz-Frequenzband.

Nach der Bereitstellung scannt das Modul ständig alle Kanäle, um sicherzustellen, dass die Wireless-Umgebung die höchste Sicherheit und Zuverlässigkeit bietet, die es in der Branche bietet.

Vorteile des WSSI-Modus

Enhanced Local Mode (ELM):

- Senkung von Netzwerkkosten und -betrieb Durch die Integration des WSSI-Moduls in die Serie 3600 können Sie bis zu drei separate Geräte ersetzen. Dies bietet drei separate Funktionen in einem einzigen, vielseitig einsetzbaren AP der Serie 3600.

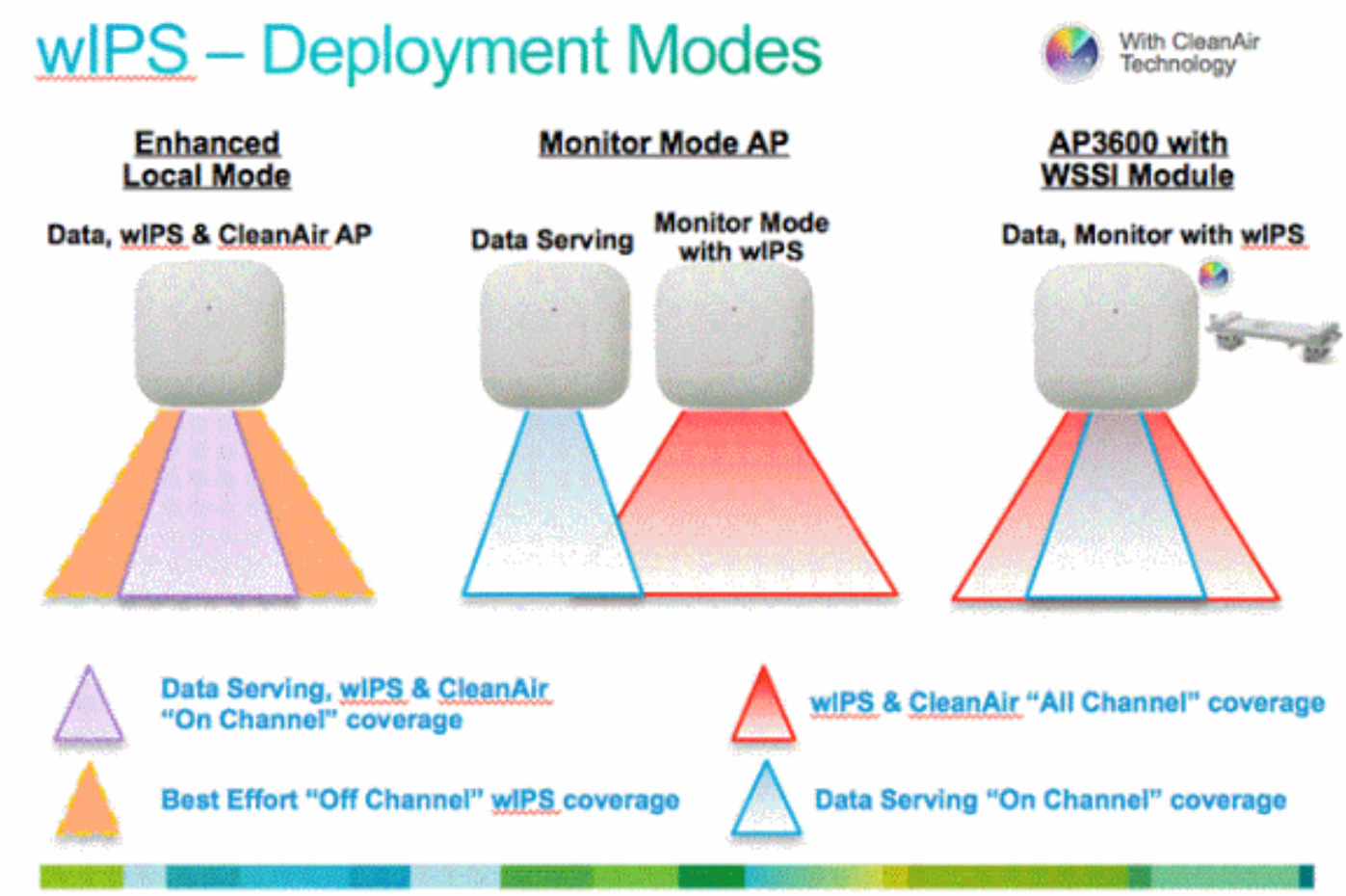


- Kunden können nun eine einzelne Ethernet-Verbindung (Kabel und Port) in ihr kabelgebundenes Netzwerk nutzen, anstatt bis zu drei separate Ethernet-Kabel und einen Access Port in ihr kabelgebundenes Netzwerk einzubinden. Dadurch werden die

Investitionskosten deutlich gesenkt.

- Durch die Integration all dieser Funktionen in einen einzigen Access Point können Kunden die alltägliche Verwaltung und Überwachung ihrer Wireless-Infrastruktur und ihres Netzwerks mit einer deutlich geringeren Anzahl von Access Points vereinfachen. Das WSSI-Modul wird dem WLC und den Managementsystemen als zusätzliches Funkmodul angezeigt, das 802.11b/g/a/n-Client-Geräte (2,4 und 5 GHz) innerhalb des AP der Serie 3600 unterstützt.
- *Konfiguration*, Installation, Hochfahren und Starten ohne Benutzereingriff Es ist absolut keine Konfiguration erforderlich, um die Einrichtung und den Betrieb des WSSI-Moduls sowie die sofortige Überwachung und Sicherung Ihres Wireless-Netzwerks zu ermöglichen. Das WSSI-Modul wird in einen beliebigen Access Point der Serie 3600 eingesteckt und gesichert. Wenn der Access Point wieder eingeschaltet wird, wird das Modul zusammen mit den anderen Funkmodulen im Access Point initialisiert und beginnt sofort mit der Überwachung aller Kanäle sowohl im 2,4-GHz- als auch im 5-GHz-Frequenzbereich auf potenzielle Sicherheitsbedrohungen und Störungsquellen.
- Das adaptive wIPS ermöglicht eine präzise und effiziente Erkennung von Sicherheitsrisiken auf allen Kanälen, von Over-the-Air-Angriffen, nicht autorisierten APs und Ad-hoc-Verbindungen bis hin zur Klassifizierung, Benachrichtigung, Eindämmung und Berichterstellung für eine kontinuierliche Überwachung und proaktives Management. Arbeitet mit der Cisco Mobility Services Engine (MSE) zusammen.

ELM:



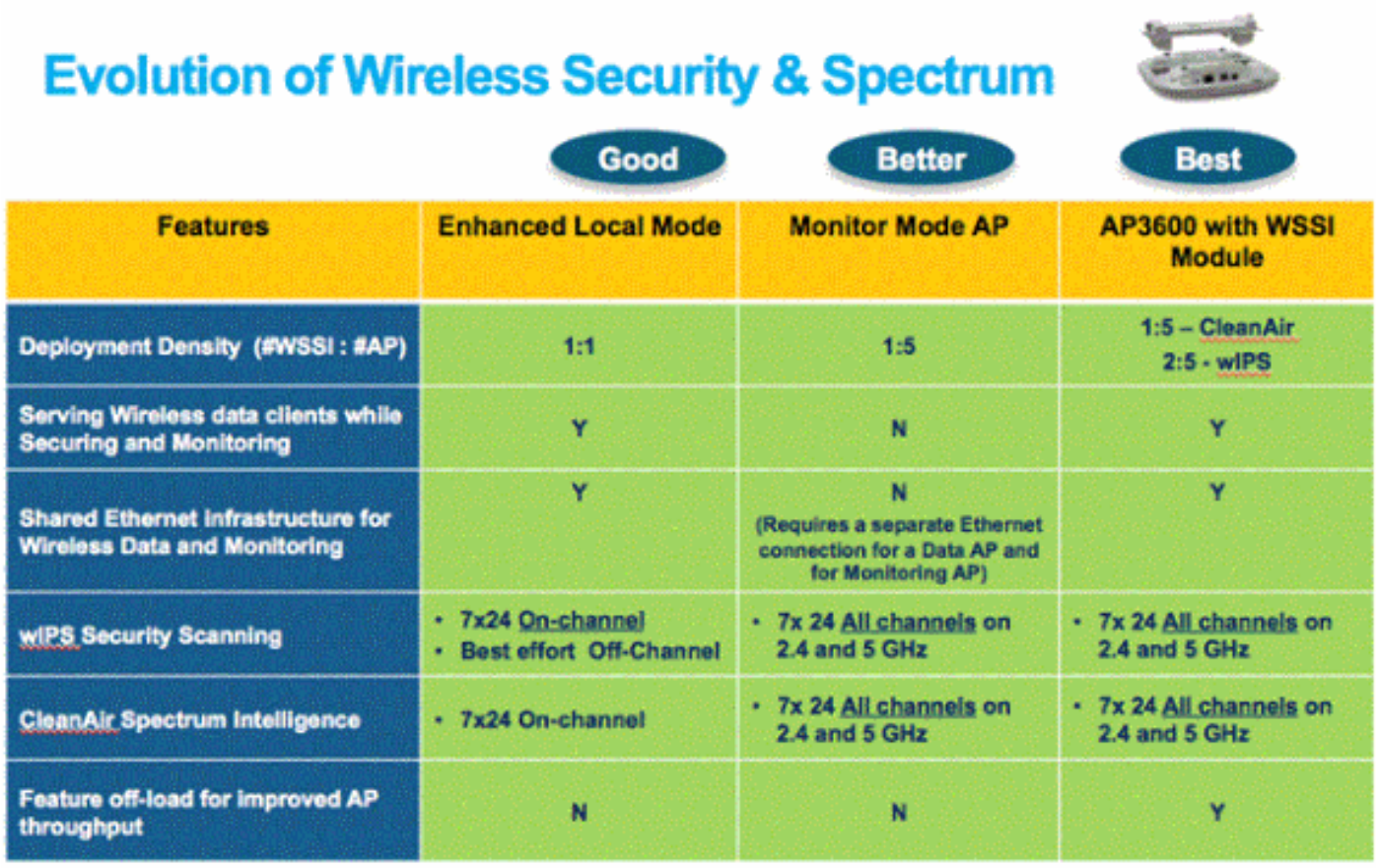
- Bietet bei Kanalabtastung (2,4 GHz und 5 GHz) wIPS-Sicherheitsscans für 7x24 mit bestmöglicher Kanalunterstützung.
- Der Access Point ist darüber hinaus für Clients ausgelegt und ermöglicht mit den Access Points der G2-Serie die CleanAir-Spektrumanalyse auf Kanälen (2,4 GHz und 5 GHz).

Überwachungsmodus:

- Der Überwachungsmodus-AP (MMAP) ist für den Betrieb im Überwachungsmodus vorgesehen und kann wIPS-Sicherheitsscans aller Kanäle (2,4 GHz und 5 GHz) hinzufügen.
- Die Access Points der G2-Serie ermöglichen die Analyse des CleanAir-Spektrums auf allen Kanälen (2,4 GHz und 5 GHz).
- MMAPs dienen Clients nicht.

AP3600 mit WSSI-Modul: Die Entwicklung von Wireless-Sicherheit und -Spektrum

- Der branchenweit erste Access Point, der gleichzeitige Client-Services, wIPS-Sicherheitsscans und Spektrumanalysen mithilfe der CleanAir-Technologie ermöglicht.
- Dedizierte 2,4-GHz- und 5-GHz-Funkmodule mit eigenen Antennen ermöglichen das 7x24-Scannen aller Wireless-Kanäle im 2,4-GHz- und 5-GHz-Frequenzbereich.
- Eine einzige Ethernet-Infrastruktur bietet einen vereinfachten Betrieb mit weniger Geräten für die Verwaltung und einen optimierten Return on Investment der AP3600-Wireless-Infrastruktur und der kabelgebundenen Ethernet-Infrastruktur.



- Cisco CleanAir-Technologie: bietet proaktive, hochgeschwindigkeits-Spektrumintelligenz, um Leistungsprobleme aufgrund von Funkstörungen zu bekämpfen. Die branchenweit erste hochmoderne Funkanalysetechnologie, die die Energiemuster (Signaturen) von Geräten überprüft und klassifiziert, die die Qualität eines Wireless-Netzwerks erheblich beeinträchtigen können.
- Radio Resource Management (RRM): Vereinfachte, erweiterte HF-Verwaltung, automatische Anpassung an die Wireless-Netzwerkumgebung auf der Grundlage der von der Cisco CleanAir-Technologie erhaltenen Informationen. Sobald Störungsquellen identifiziert wurden, kann das RRM Client-Geräte von den Interferenzen weg zu den Kanälen bewegen und die Übertragungsleistung so anpassen, dass sie sich von der Störungsquelle entfernen. Dadurch

wird die Funkqualität für den Benutzer verbessert.
- Erkennung nicht autorisierter APs: erkennt und meldet den Backdoor-Netzwerkzugriff und den Zugriff auf Wireless-Clients.
- Standort- und Kontextsensitivität: bietet Echtzeit-Erkennungsfunktionen und die Möglichkeit, Wireless-Endgeräte zu verfolgen.

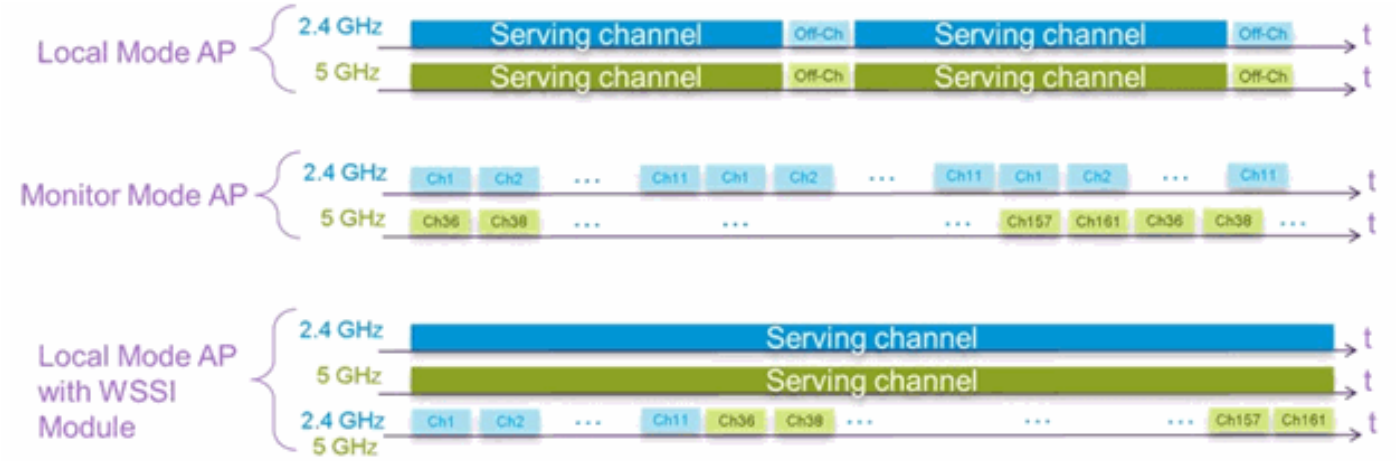
Mit diesen Funktionen bietet das Cisco Wireless Security and Spectrum Intelligence-Modul zusammen mit dem Cisco AP der Serie 3600 das sicherste und robuste drahtlose Netzwerk der Enterprise-Klasse, das für Benutzer und Daten in Ihrem Unternehmen möglich ist.

On-Channel vs. Off-Channel mit dem WSSI-Modul

Ein AP im lokalen Modus scannt im Kanal nach CleanAir-Störungsquellen und wIP-Angreifern. Dies bedeutet, dass der Access Point nur den Kanal durchsucht, für den er zuständig ist. Ein AP im lokalen Modus mit einem 2,4-GHz-Funkmodul für Kanal 1 und 5-GHz-Funkmodule für Kanal 64 bietet nur Schutz für die Kanäle 1 und 64.

Ein MMAP sucht außerhalb des Kanals nach CleanAir-Störungsquellen und wIP-Angreifern. Das bedeutet, der Access Point scannt alle Kanäle. Das 2,4-GHz-Funkmodul scannt alle 2,4-GHz-Kanäle, und der 5-GHz-Kanal scannt alle 5-GHz-Kanäle.

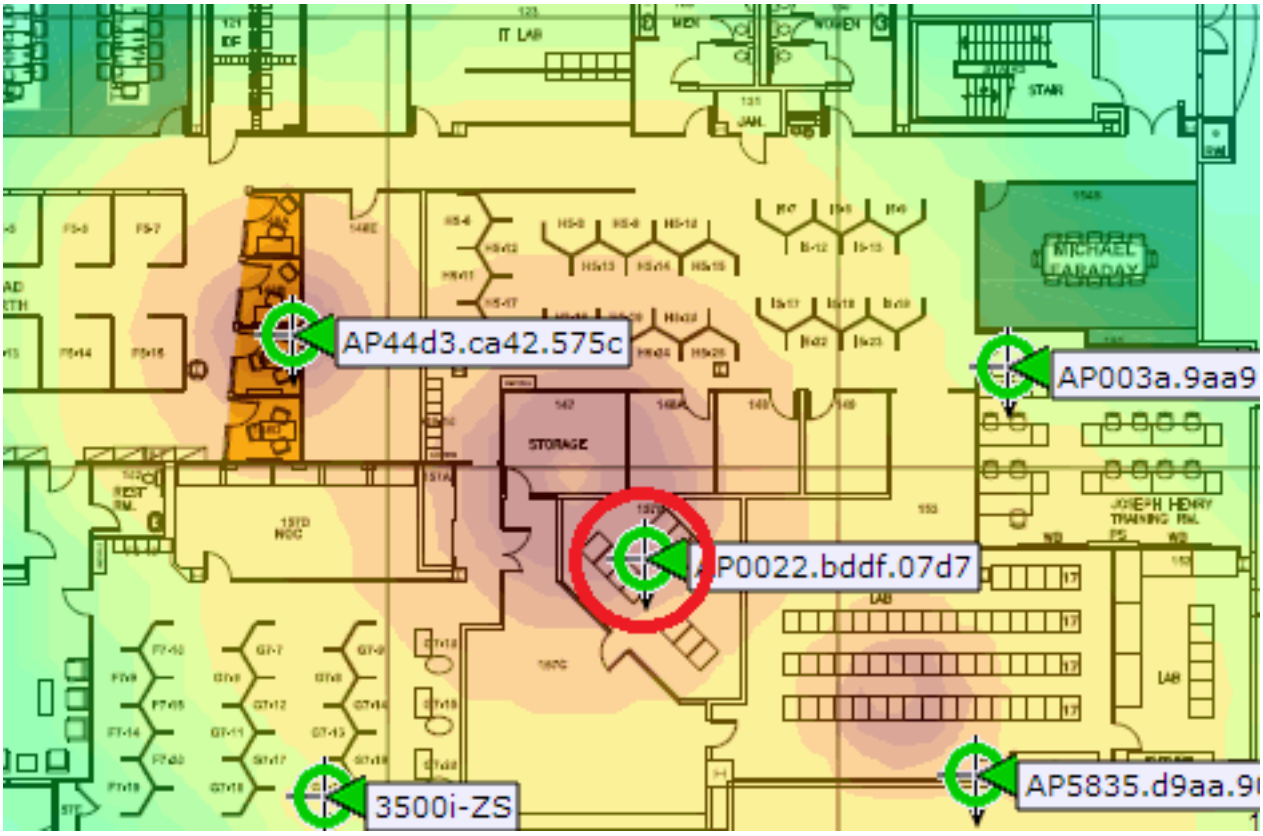
Ein Cisco AP der Serie 3600 verwendet eine Kombination aus einem Kanal und einem Kanal. Die 2,4-GHz- und 5-GHz-Funkmodule scannen auf dem Kanal, und das WSSI-Modul scannt den Kanal von einem Kanal zum anderen, und zwar zwischen allen 2,4-GHz- und 5-GHz-Kanälen.



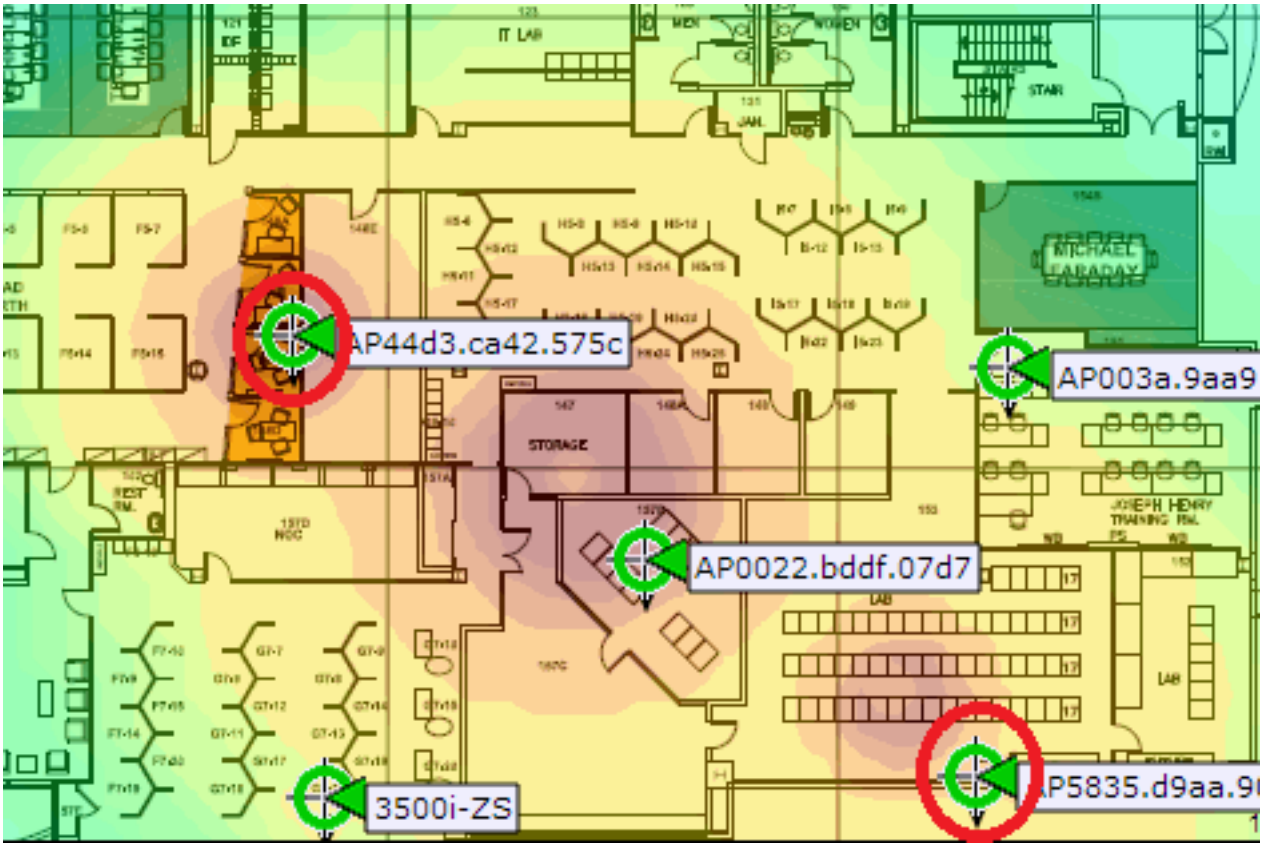
Empfohlene Bereitstellungsdichte für das WSSI-Modul

Bei der herkömmlichen Monitor-AP-Bereitstellung empfiehlt Cisco ein Verhältnis von 1 MMAP zu 5 APs im lokalen Modus. Dies kann je nach Netzwerkdesign und fachkundiger Unterstützung für eine optimale Abdeckung variieren. Beim WSSI-Modul gibt es verschiedene Bereitstellungsempfehlungen, die auf der Funktionalität basieren, um eine Abdeckungsvergleich mit einem MMAP zu erreichen.

Für CleanAir wird die Bereitstellung eines WSSI-Moduls für jeweils fünf lokale oder Flexconnect-APs empfohlen. Diese 1:5-Bereitstellung bietet die gleiche Leistung wie ein CleanAir-aktiviertes MMAP, ermöglicht jedoch dennoch die Bedienung der Clients durch den AP. Dies ist eine empfohlene Bereitstellung für ein WSSI-Modul, das CleanAir ausführt:

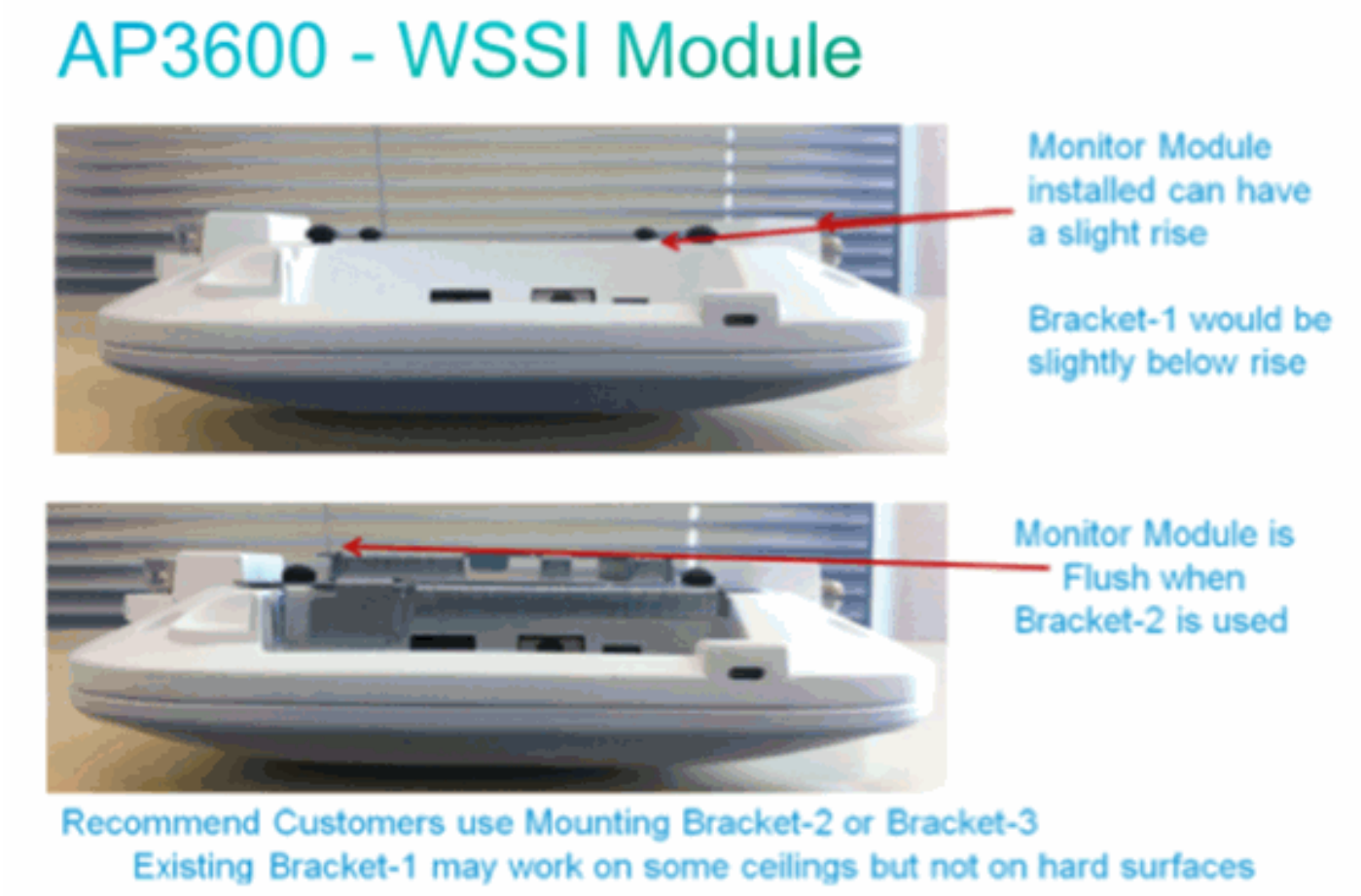


Für den wIPS-Schutz wird die Bereitstellung von 2 WSSI-Modulen für jeweils 5 lokale oder FlexConnect-APs empfohlen. Die wIPS-Erkennungszeit für einen Off-Channel-Angriff beträgt etwa das Zweifache eines MMAP. Daher ist eine 2:5-Bereitstellung erforderlich, um wIPS-Erkennungsparität bereitzustellen. Dies ist die empfohlene Bereitstellung für ein WSSI-Modul mit wIPS-Schutz:



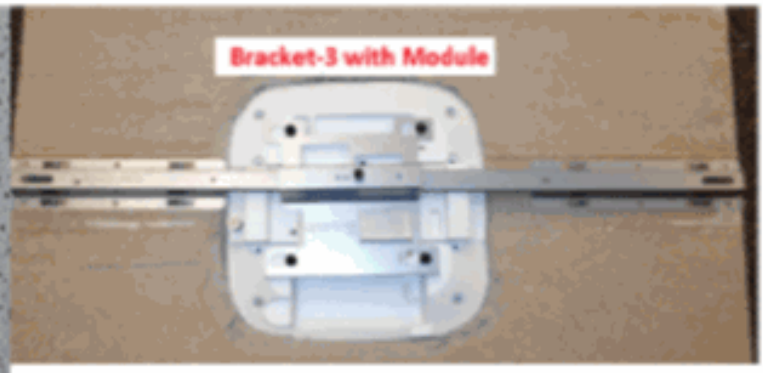
Der Cisco Access Point der Serie 3600 mit einem WSSI-Modul nutzt sowohl das On-Channel- als auch das Off-Channel-Scanning, um eine branchenführende Lösung für Clients bereitzustellen.

[Installieren des WSSI-Moduls]



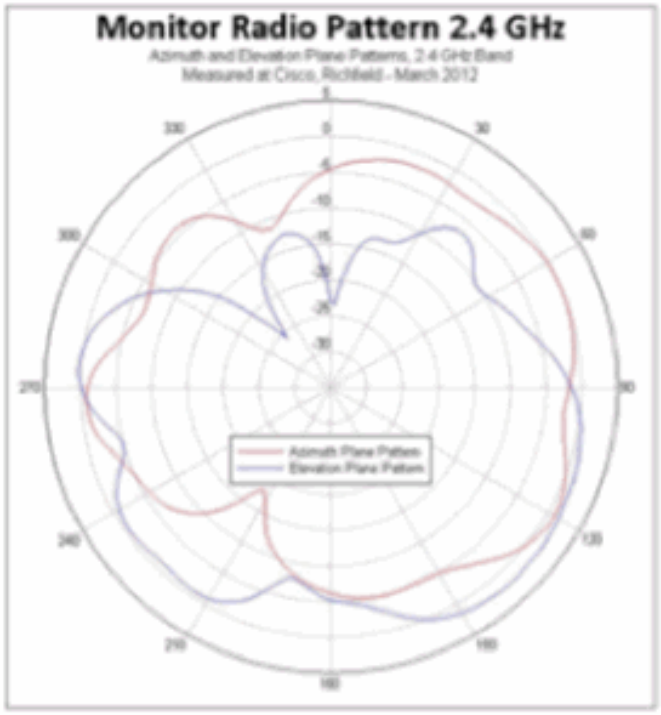
AP3600 with WSSI Module and Bracket-3

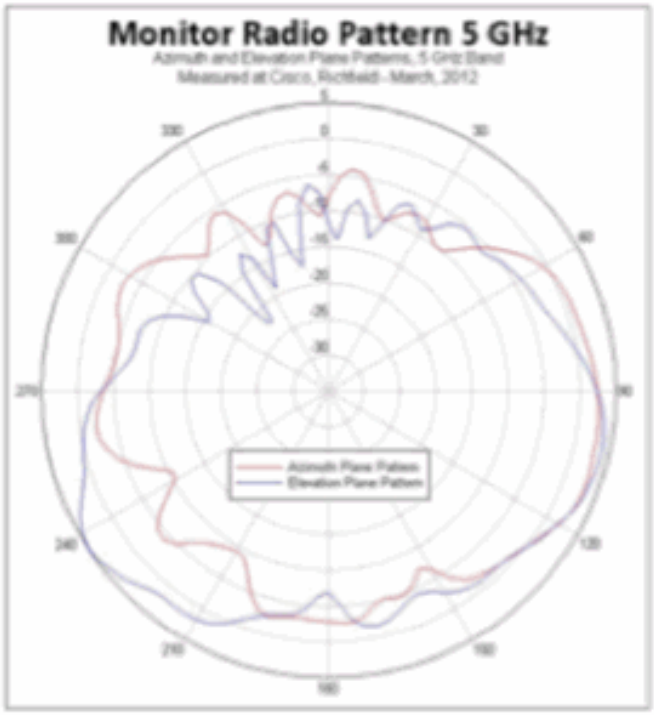
Elegant in-tile flush mount



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





Konfiguration für das AP3600 WSSI-Modul

Für das WSSI-Modul ist keine Konfiguration erforderlich. Das Modul scannt automatisch alle Kanäle auf beiden Bändern mit seinen 0x4-Antennen (nur Empfangsantennen) 0 Tx x 4 Rx Antennen.

Beachten Sie, dass das WSSI-Modul nur auf AP3600-Geräten aktiv ist, die entweder im lokalen Modus oder im FlexConnect-Modus konfiguriert sind. Das WSSI-Modul ist in allen anderen Modi deaktiviert.

Leistungsanforderung für das WSSI-Modul

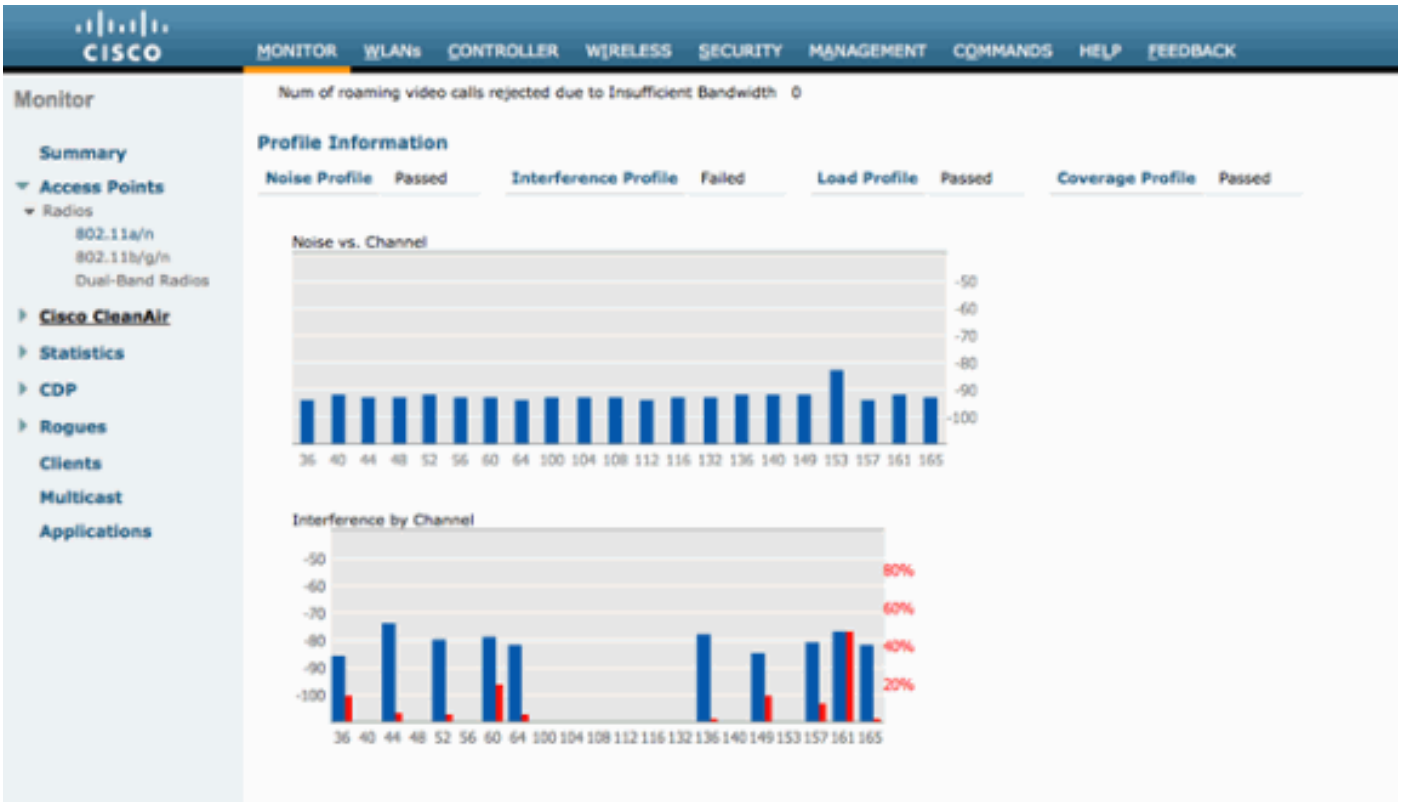
Der AP3600 mit installiertem WSSI-Modul überschreitet 15,4 Watt (802.3af). Der Access Point benötigt entweder (802.3at - PoE+), Enhanced PoE, ein lokales Netzteil oder den Cisco PoE Injector (AIR-PWRINJ4).

Hinweise:

- Enhanced PoE wurde von Cisco erstellt und ist ein Vorläufer von 802.3at PoE+. Sie bietet eine Leistung von bis zu 20 W.
- PoE+ kann bis zu 30 W Leistung bereitstellen.

Radio Resource Management auf dem WSSI-Modul

Das WSSI-Modul nimmt alle RRM-Messungen sowohl im 2,4-GHz- als auch im 5-GHz-Band vor. Die Messwerte werden in der WLC-GUI entweder unter Monitor > Access Points > 802.11a/n > AP_NAME > Details oder unter Monitor > Access Points > 802.11b/g/n > AP_NAME > Details angezeigt.



CleanAir auf dem WSSI-Modul

Das WSSI-Modul erkennt CleanAir-Interferenzen mit der gleichen Genauigkeit wie ein MMAP. Cisco empfiehlt die Bereitstellung des WSSI-Moduls mit einer Dichte von 1:5, wobei für jeweils 5 APs ein WSSI-Modul erforderlich ist. Dies ist die gleiche empfohlene Dichte wie bei einem MMAP.

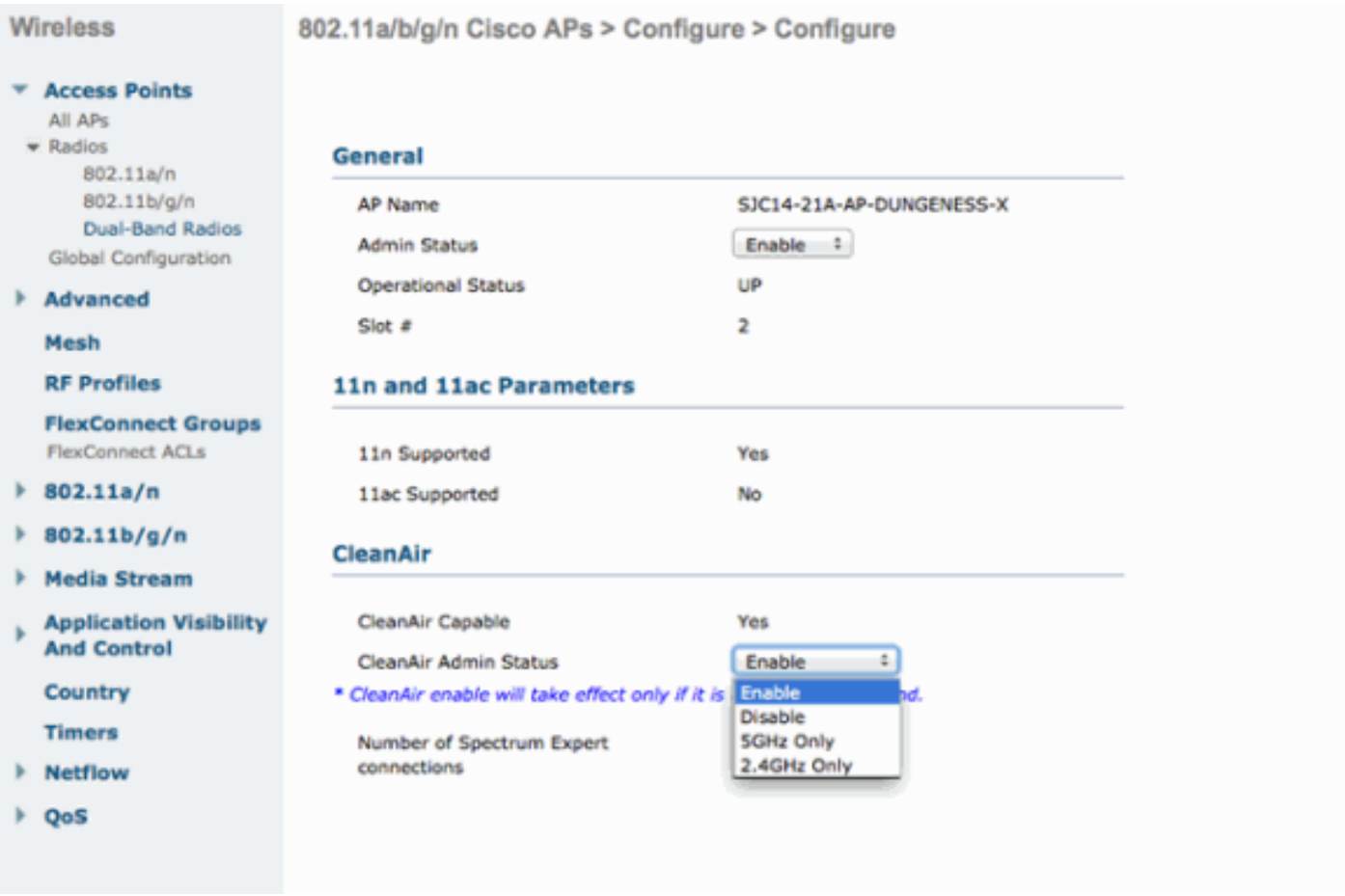
Wenn das WSSI-Modul ohne Submodus aktiviert ist, scannt das Modul sowohl das 2,4-GHz- als

auch das 5-GHz-Band. Das Modul hält sich 1,2 Sekunden lang an jedem Kanal und scannt nach CleanAir-Störungsquellen.

CleanAir kann nur für 2,4 GHz, 5 GHz und 2,4 GHz und 5 GHz aktiviert werden. Diese Option kann entweder über die WLC-CLI oder die GUI ausgewählt werden. Im Folgenden finden Sie ein Beispiel für die Konfiguration von CleanAir in der WLC-CLI:

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

Dieselbe Konfiguration kann über Wireless > Dual-Band Radios > Configure auf die GUI angewendet werden. Hier ein Beispiel:



Führen Sie den Befehl **show cleanair interferers** von der AP-Konsole aus, um zu überprüfen, ob der CleanAir-Interferer vom WSSI-Modul erkannt wurde:

```
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
```

Dieselbe Konfiguration kann über Wireless > Dual-Band Radios > Configure auf die GUI angewendet werden. Hier ein Beispiel:

Die CleanAir-Störungsquellen werden in der WLC-GUI gemeldet. Interferer werden PER BAND angezeigt. Dies bedeutet, dass auf dem WSSI-Modul im 5-GHz-Band erkannte Interferenzen unter Monitor > 802.11a/n > Interference Devices angezeigt werden.

Führen Sie die folgenden **show cleanair-Interferer** von der AP-Konsole aus, um zu überprüfen, ob der CleanAir-Interferer vom WSSI-Modul erkannt wurde:

```
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
```

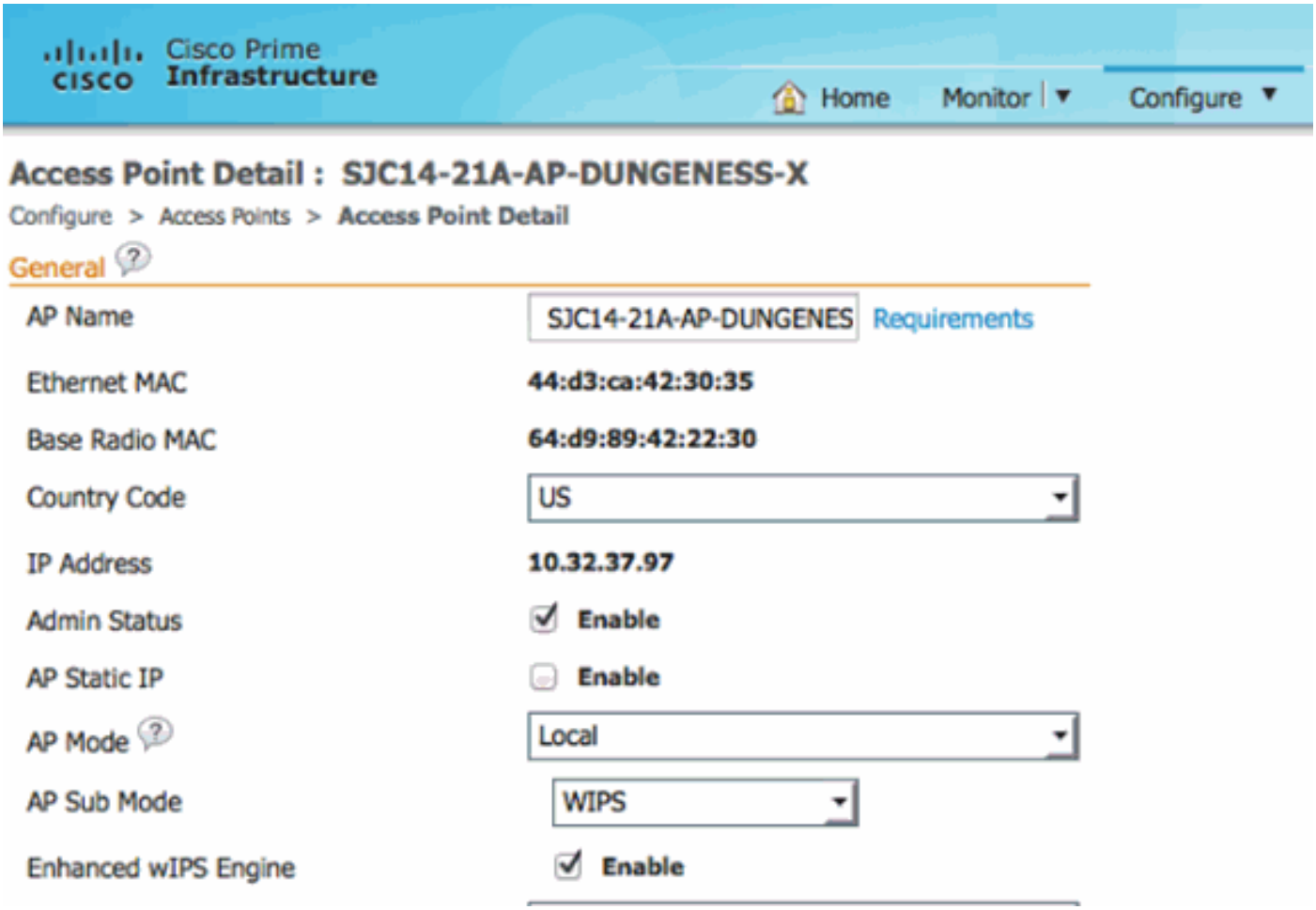
wIPS auf dem WSSI-Modul

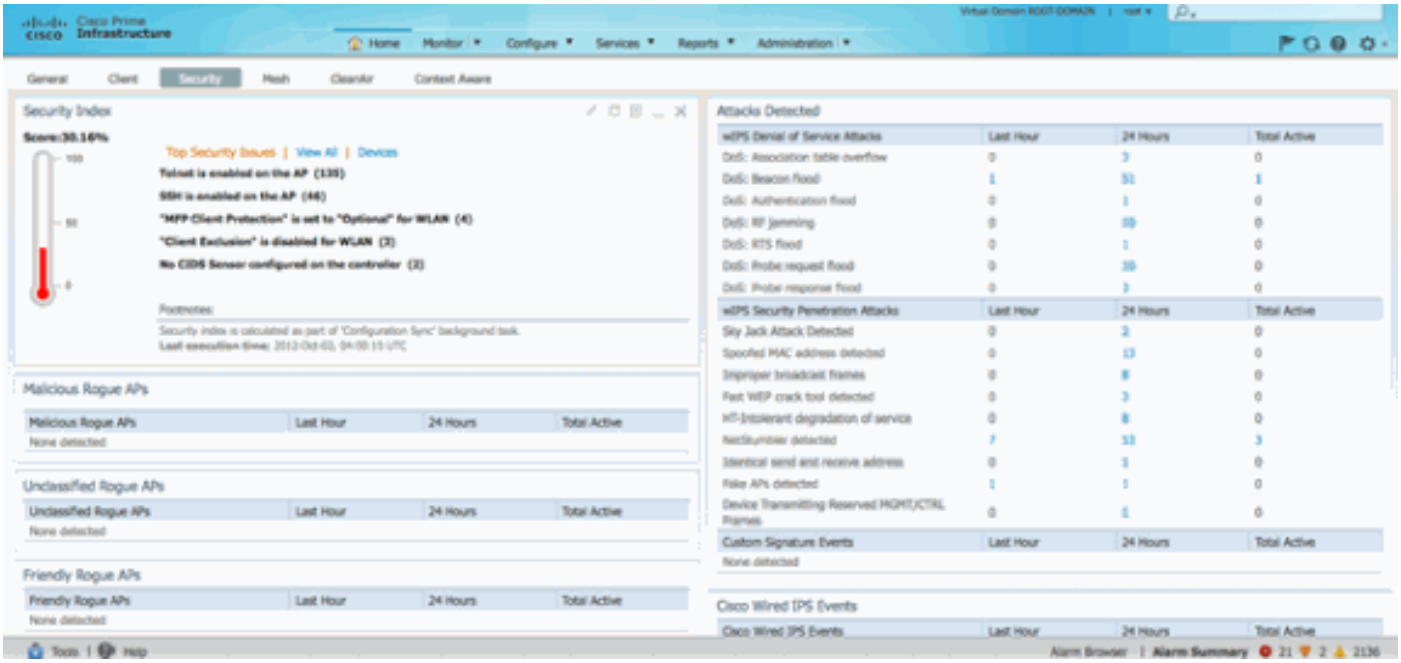
Das WSSI-Modul erkennt wIPS-Angreifer mit nahezu derselben Genauigkeit wie ein MMAP. Für wIPS empfiehlt Cisco die Bereitstellung des WSSI-Moduls mit einem Verhältnis von 2:5 zwischen den APs. Das bedeutet, dass für jeden 5 Access Point zwei Access Points das WSSI-Modul enthalten müssen.

Es gibt zwei wIPS-Modi, die konfiguriert werden können:

- wIPS-Submodus - Ermöglicht die Erkennung von wIPS-Angriffen und scannt alle Kanäle auf 1,2 s. Dieser Modus ermöglicht es dem Access Point, zusätzlich zur wIPS-Erkennung noch alle RM-Berichte zu erfassen.
- Erweiterter wIPS-Modus - Ermöglicht die Erkennung von wIPS-Angriffen und scannt alle Kanäle für einen Zeitraum von 250 ms. Die kleinere Kanalverweilzeit ermöglicht dem Sicherheitsmodul, Angreifer schneller zu erkennen.

Gehen Sie auf der Seite Prime Infrastructure (PI) zu Configure > Access Points > AP_NAME. Das WSSI-Modul kann entweder für den wIPS-Submodus oder den wIPS-Submodus + die Unterstützung für die erweiterte wIPS-Engine konfiguriert werden. Dies kann auch als Teil einer Access Point-Konfigurationsvorlage weitergegeben werden.





Die wIPS-Angriffe werden in der Prime-Infrastruktur auf der Registerkarte Home > Security (Startseite > Sicherheit) angezeigt.

Der PI zeigt eine Ansicht auf Netzwerkebene an, aber Sie können den Angriff auf einen AP3600 mit einem WSSI-Modul anzeigen, indem Sie den Befehl **show capwap am alarm ALARM_NUM** von der AP-Konsole ausgeben.

Beispielsweise ist alarm 52 eine Denial of Service-, Authentifizierungs-Flood. Führen Sie den Befehl **show capwap am alarm 52 aus**, um zu überprüfen, ob dieser Angriff auf dem WSSI-Modul

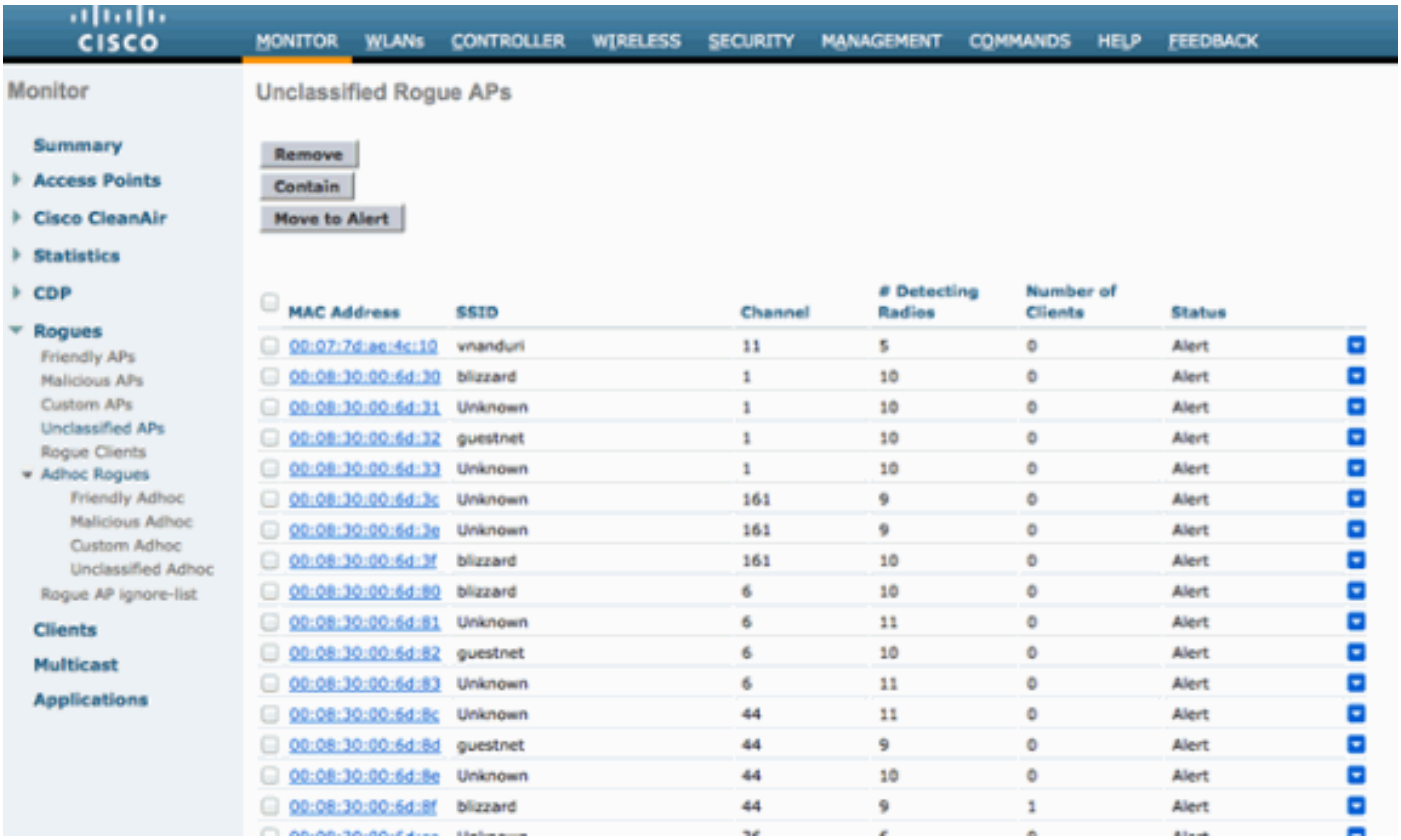
erkannt wurde:

```
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
```

Erkennung nicht autorisierter APs auf dem WSSI-Modul

Das WSSI-Modul erkennt nicht autorisierte APs mit der gleichen Genauigkeit wie ein MMAP. Eine Liste nicht autorisierter APs wird sowohl im WLC als auch im PI angezeigt.

Dies ist die Liste nicht klassifizierter nicht autorisierter APs aus der WLC-GUI. Nicht autorisierte APs können in der WLC-GUI unter Monitor > Rogues angezeigt werden.



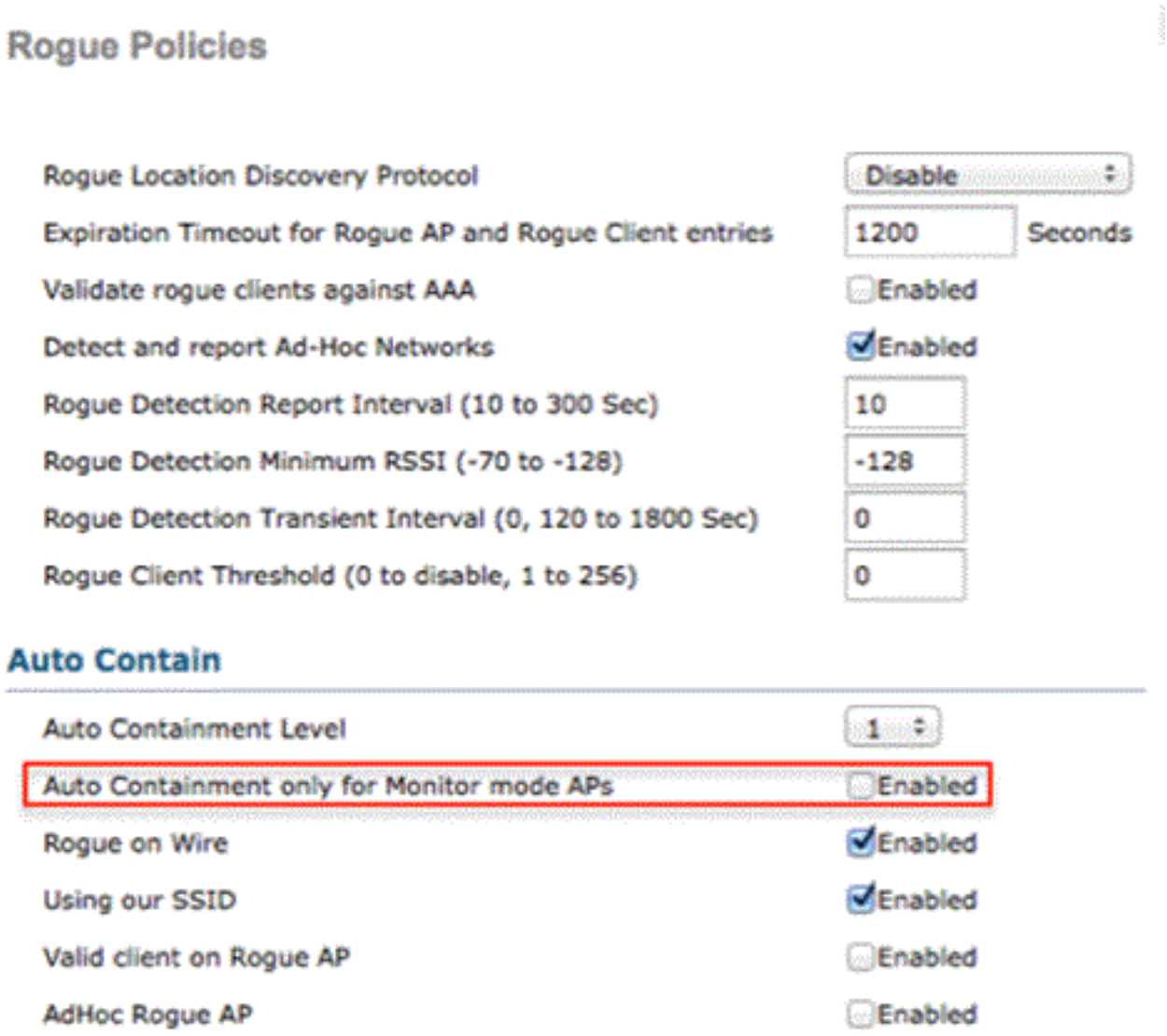
Sie können überprüfen, ob das WSSI-Modul mit der AP-Konsole einen nicht autorisierten Access Point erkannt hat. Geben Sie in der Konsole den Befehl **show capwap rm rogue ap d2 all** ein. Es werden alle nicht autorisierten APs angezeigt, die im WSSI-Modulradio angezeigt werden.

```
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
```

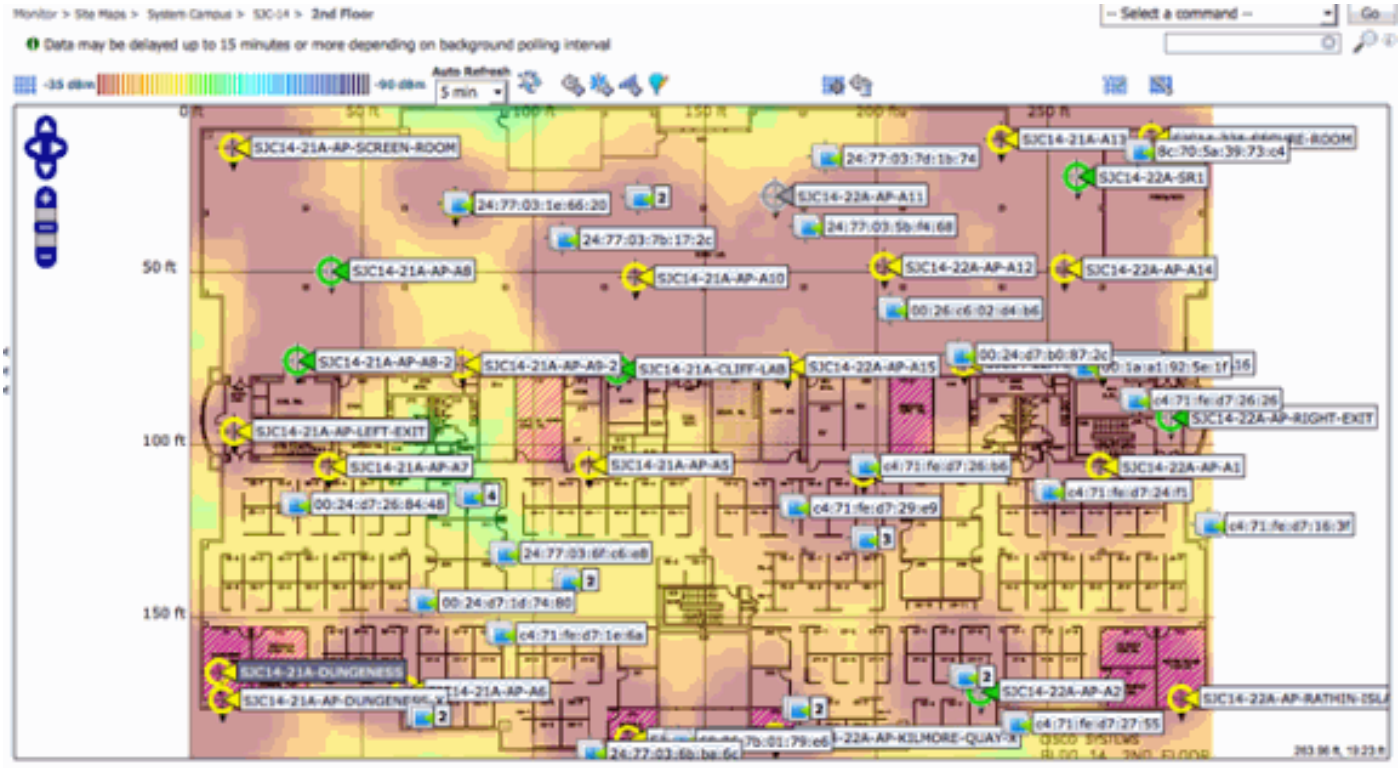
Nicht autorisierte Containment mit dem WSSI-Modul

Das WSSI-Modul ist ein 0x4-Modul (nur Empfangsantennen), d. h., auf dem 2,4-GHz- oder 5-GHz-Funkmodul wird eine unberechtigte Eingrenzung durchgeführt. Damit das WSSI automatisch nicht autorisierte APs enthalten kann, müssen Sie sicherstellen, dass in der WLC-GUI unter Sicherheit > Wireless Protection Policies > Rogue Policies > General (Sicherheit > Wireless-Schutzrichtlinien > Richtlinien für nicht autorisierte Zugriffe) sichergestellt ist, dass **die automatische Eindämmung nur für APs im Überwachungsmodus** nicht aktiviert ist (siehe nächster Screenshot). Alle anderen Kontrollkästchen können aktiviert werden.



Kontextsensitiver Standort auf dem WSSI-Modul

Wenn das WSSI-Modul mit einer Cisco MSE verbunden ist, stellt es kontextsensitive Standortdaten mit derselben Genauigkeit wie ein MMAP bereit.



WSSI-Modullizenzierung

Das WSSI-Modul verwendet Lizenzen für den wIPS-Überwachungsmodus.

Zugehörige Informationen

- Technischer Support und Dokumentation - Cisco Systems