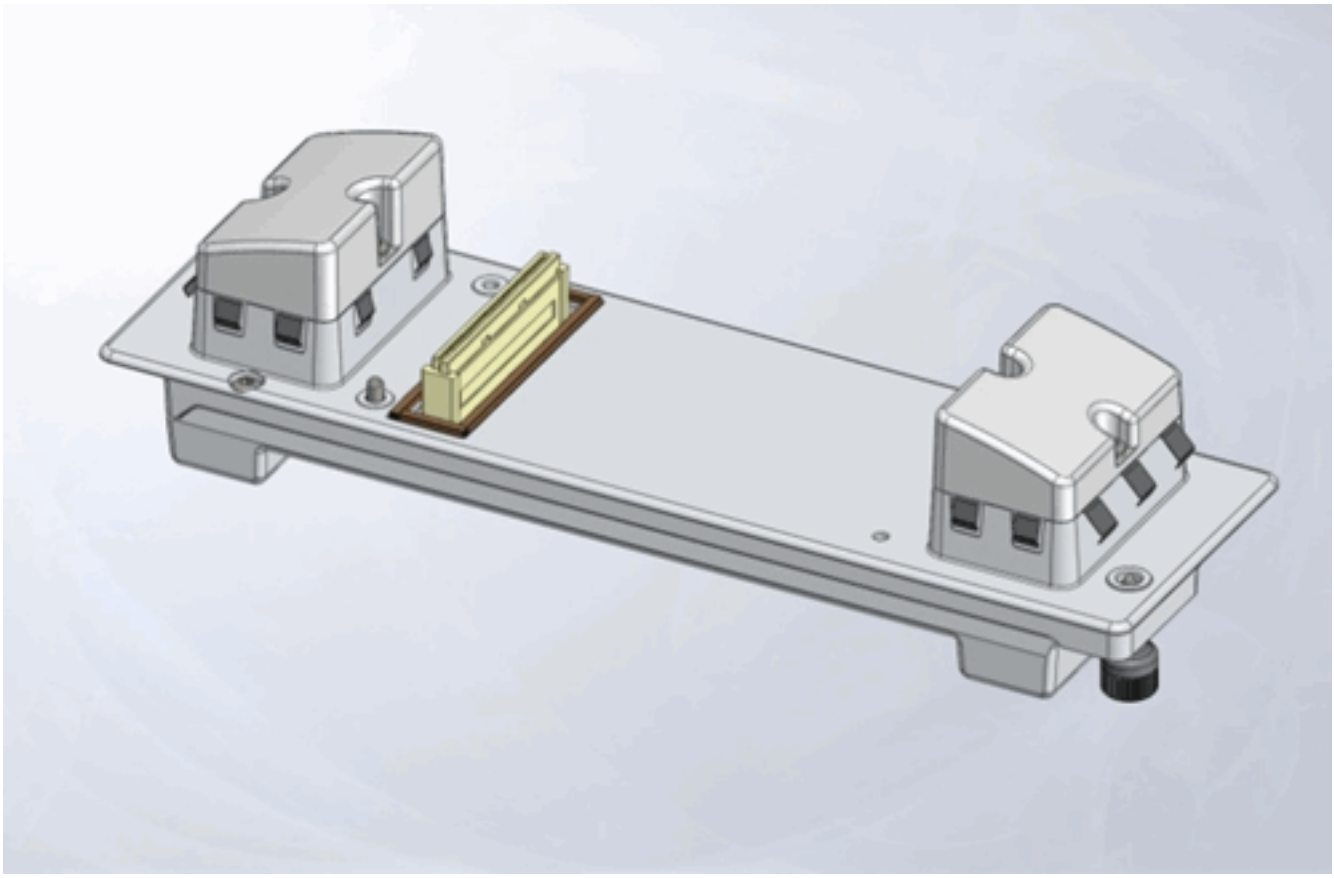
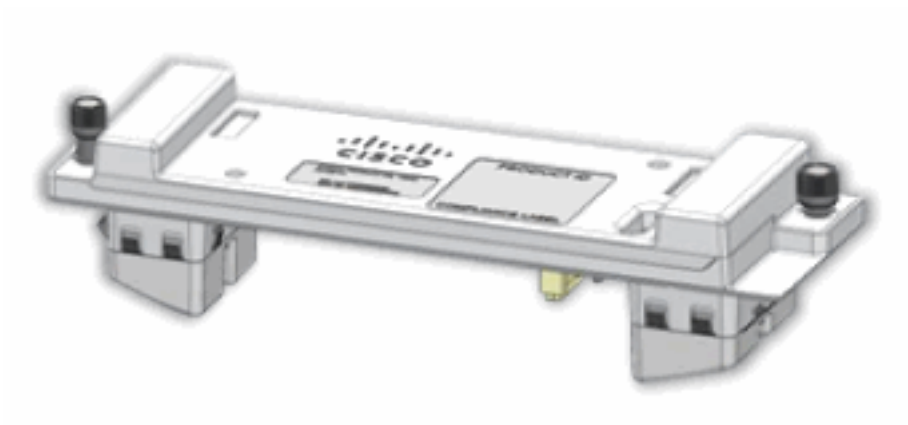
適用於WSSI的Aironet AP模組部署指南

目錄

簡介

本文檔提供了適用於無線安全和頻譜智慧(WSSI)的Cisco Aironet接入點模組的一般配置和部署指南。 WSSI是一個附加模組，可以插入模組化接入點(AP)，例如Cisco 3600系列AP。





必要條件

需求

本文件沒有特定需求。

採用元件

無線安全和頻譜智慧模組需要最低代碼版本：

- 無線LAN控制器(WLC) — 版本7.4.xx.xx或更高版本
- 接入點(AP) — 版本7.4.xx.xx或更高版本
- Prime基礎架構(PI) — 版本1.3.xx.xx或更高版本
- 行動化服務引擎(MSE) — 版本7.4.xx.xx或更高版本

慣例

如需文件慣例的詳細資訊，請參閱思科技術提示慣例。

產品概觀

思科無線安全和頻譜智慧模組利用Cisco Aironet 3600系列AP靈活的模組化設計，可提供前所未有的始終線上安全掃描和頻譜智慧。這有助於您避免射頻(RF)干擾，從而獲得更好的無線網路覆蓋範圍和效能。

- 適用於aWIPS、CleanAir、情景感知、欺詐檢測和無線電資源管理的24x7全頻譜監控和緩解
- 24 x 7通道內aWIPS威脅防護
- 安全性和頻譜覆蓋範圍提高23倍
- 與專用監控模式AP相比，CAPEX成本節約超過30%

- 零接觸配置

WSSI現場可升級模組是一個專用無線電，可將所有監控和安全服務從客戶端/資料服務無線電轉移到安全監控模組。這不僅可以實現更好的客戶端效能，而且還可以通過消除將這些裝置連線到其網路所需的專用監控模式AP和乙太網基礎設施的需求而降低成本。

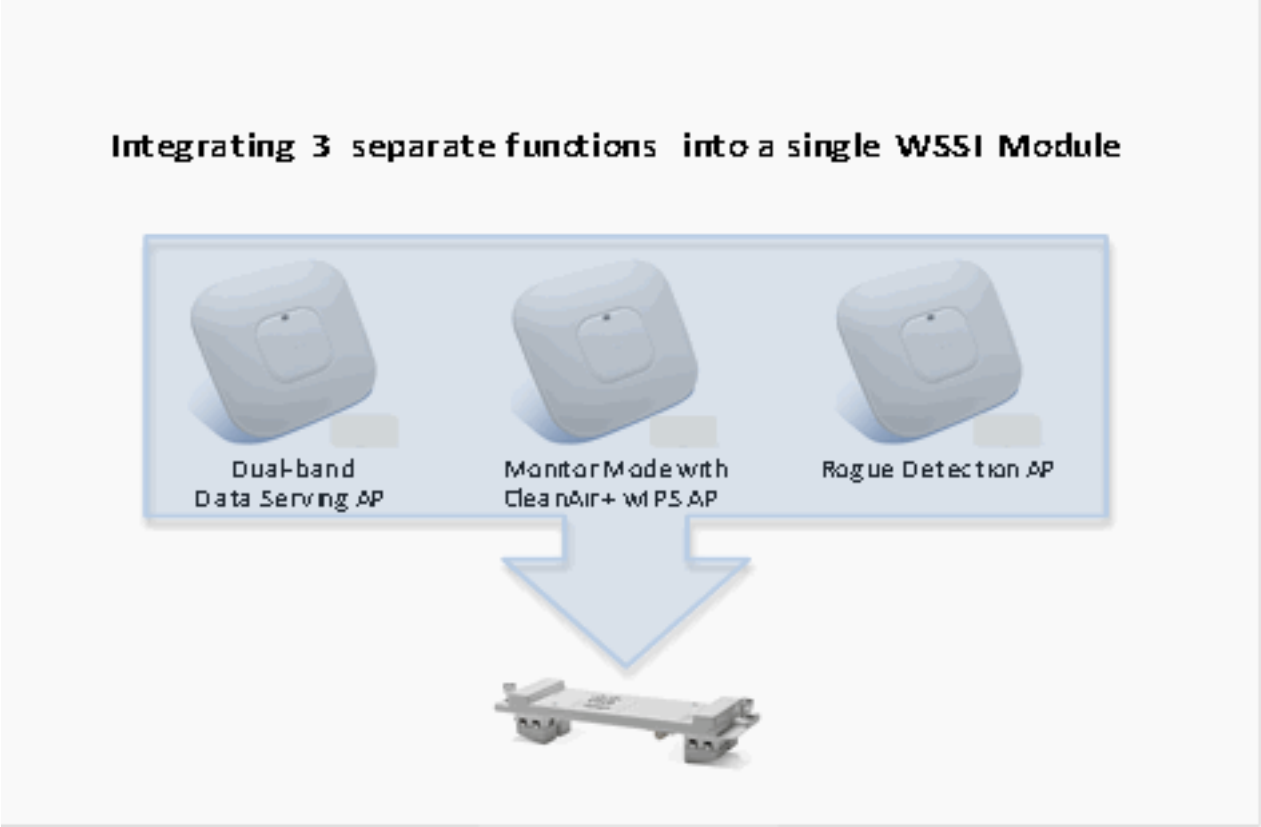
3600系列AP和WSSI模組可讓您同時為所有通道上的Wi-Fi客戶端（2.4 GHz和5 GHz頻段）提供一流的安全性和頻譜分析功能。

部署後，該模組將持續掃描所有通道，以幫助確保業內提供最安全和最強大的無線體驗。

WSSI模式的優點

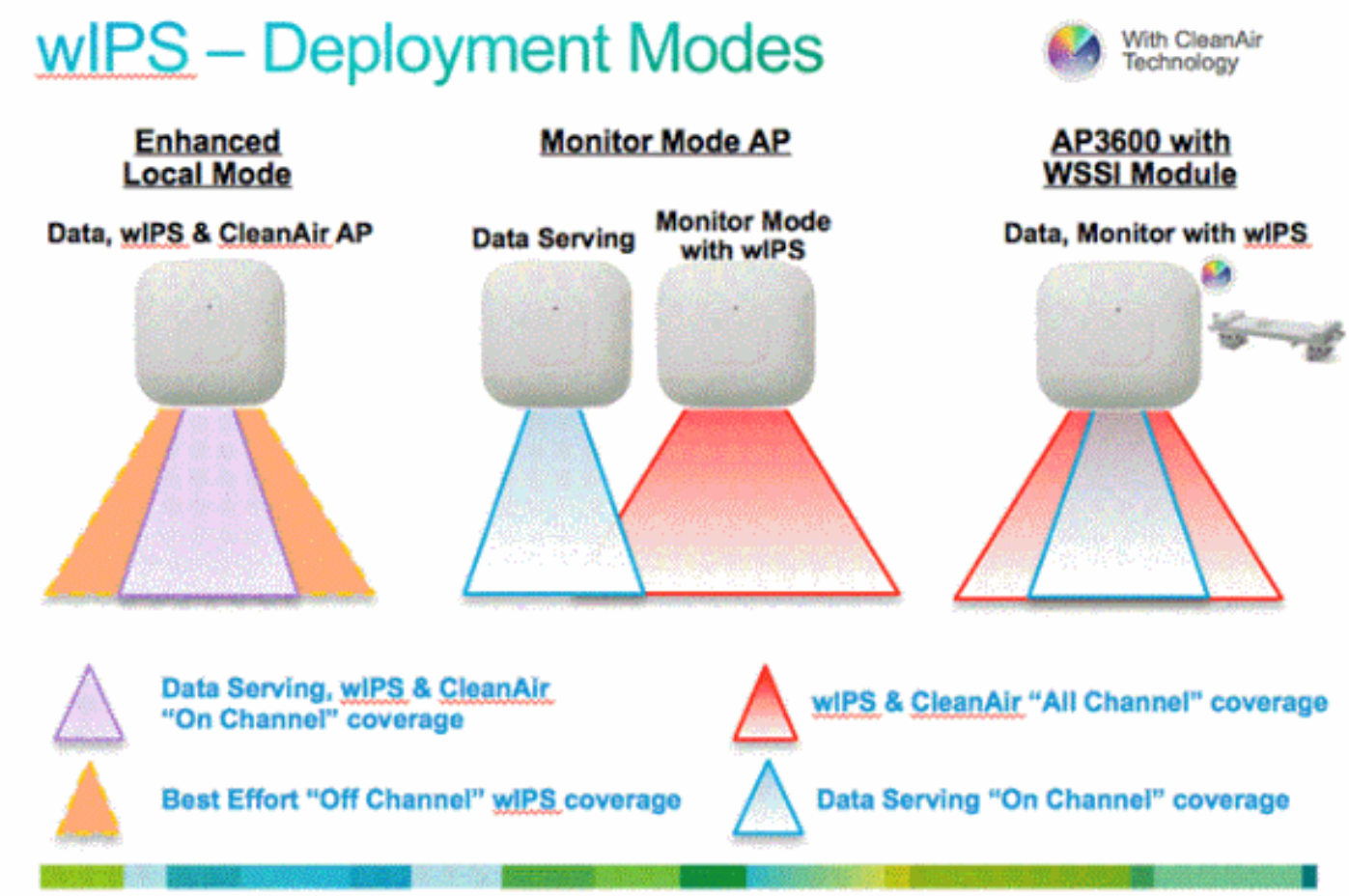
增強型區域模式(ELM):

- 降低網路成本和運營。通過將WSSI模組整合到3600系列中，您可以替換最多三個獨立的裝置。這可以將三個獨立的功能整合到一個多用途的3600系列AP中。



- 現在，客戶可以利用單個乙太網連線（電纜和埠）連線到其有線網路，以取代通常需要多達三根單獨的乙太網電纜和連線到其有線網路的接入埠的情況。這大大降低了他們的資本支出。
- 通過將所有這些功能整合到單個AP，客戶可通過大大減少的AP數簡化其無線基礎設施和網路的日常管理和監控。WSSI模組在WLC和管理系統中顯示為支援特定3600系列AP中的802.11b/g/a/n客戶端裝置（2.4和5 GHz）的附加無線電。
- *零接觸配*置、安裝、啟動和啟動。WSSI模組完全不需要配置即可啟動和運行，並且可以立即監控和保護無線網路。WSSI模組插入並固定到任何3600系列AP。當AP重新通電後，模組將與AP中的其他無線電一起初始化，並立即開始監控2.4和5 GHz上的所有通道，以發現任何潛在的安全威脅和干擾源。
- 自適應wIPS可在來自空中攻擊、惡意AP和臨時連線的所有通道上提供準確、高效的威脅檢測，並且能夠分類、通知、緩解和報告以進行持續監控和主動管理。可與思科行動服務引擎(MSE)配合使用。

ELM:



- 在通道掃描（2.4GHz和5 GHz）中新增針對7x24的wIPS安全掃描，最大程度減少通道支援。
- AP為客戶端提供額外服務，並使用G2系列AP在通道（2.4GHz和5GHz）上啟用CleanAir頻譜分析。

監控模式：

- 監控模式AP(MMAP)專用於在監控模式下運行，可選擇新增對所有通道（2.4GHz和5GHz）的wIPS安全掃描。
- G2系列AP在所有通道（2.4GHz和5GHz）上啟用CleanAir頻譜分析。
- MMAP不為客戶端提供服務。

採用WSSI模組的AP3600:無線安全和頻譜的發展

- 業界首個AP，使用CleanAir技術促進同時客戶端服務、wIPS安全掃描和頻譜分析。
- 具有自己的天線的專用2.4GHz和5GHz無線電，可對2.4GHz和5GHz頻段中的所有無線通道進行7x24掃描。
- 單個乙太網基礎設施通過更少的裝置提供簡化的操作，從而管理AP3600無線基礎設施和乙太網有線基礎設施並最佳化投資回報。

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

- Cisco CleanAir技術：提供主動的高速頻譜智慧以應對無線干擾導致的效能問題。業內首項最先進的RF分析技術，用於檢查和分類對無線網路品質有重大影響的裝置的能量模式（簽名）。
- 無線電資源管理(RRM):簡化的高級RF管理，可根據從Cisco CleanAir技術收到的資訊自動適應無線網路環境。一旦識別出干擾源，RRM能夠將客戶端裝置移動到遠離干擾的通道上，並調整傳輸功率以遠離干擾源。這為使用者提供了更好的射頻品質。
- 欺詐檢測：檢測並報告後門網路訪問和對無線客戶端的訪問。
- 位置和情景感知：提供即時感知和跟蹤無線端點的能力。

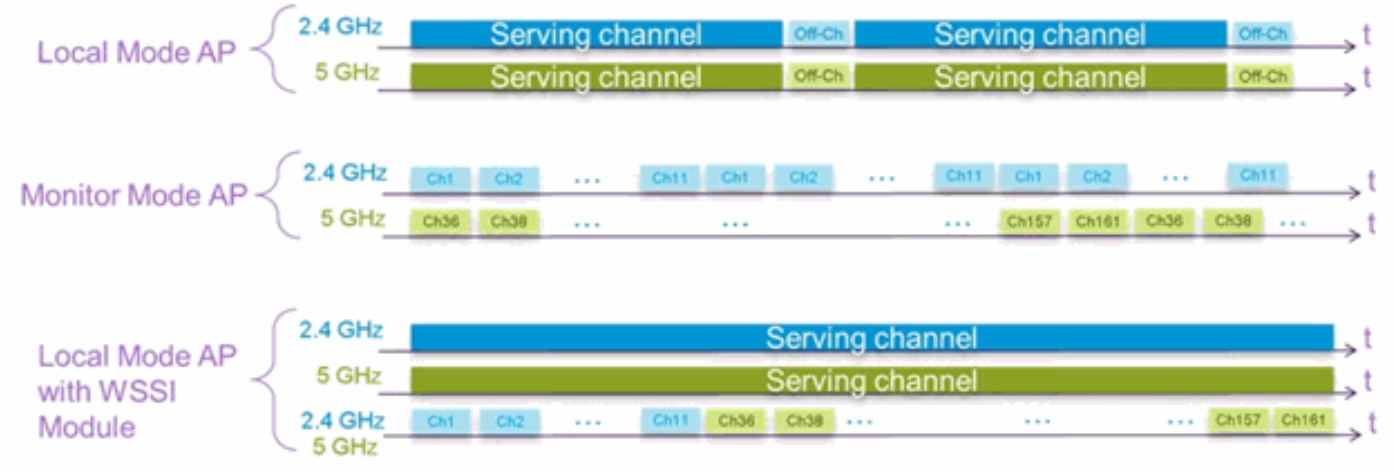
藉助這些功能，思科無線安全和頻譜智慧模組以及Cisco 3600系列AP可為您的企業使用者和資料提供最安全、最強大的企業級無線網路。

使用WSSI模組的通道內與通道外

本地模式AP在通道上掃描CleanAir干擾程式和wIP攻擊程式。這表示AP僅掃描其服務的通道。具有2.4GHz無線電服務通道1和5GHz無線電服務通道64的本地模式AP僅在通道1和64上提供保護。

MMAP會掃描通道外的CleanAir干擾程式和wIP攻擊程式。這表示AP掃描所有通道。2.4GHz無線電掃描所有2.4GHz通道，5GHz通道掃描所有5GHz通道。

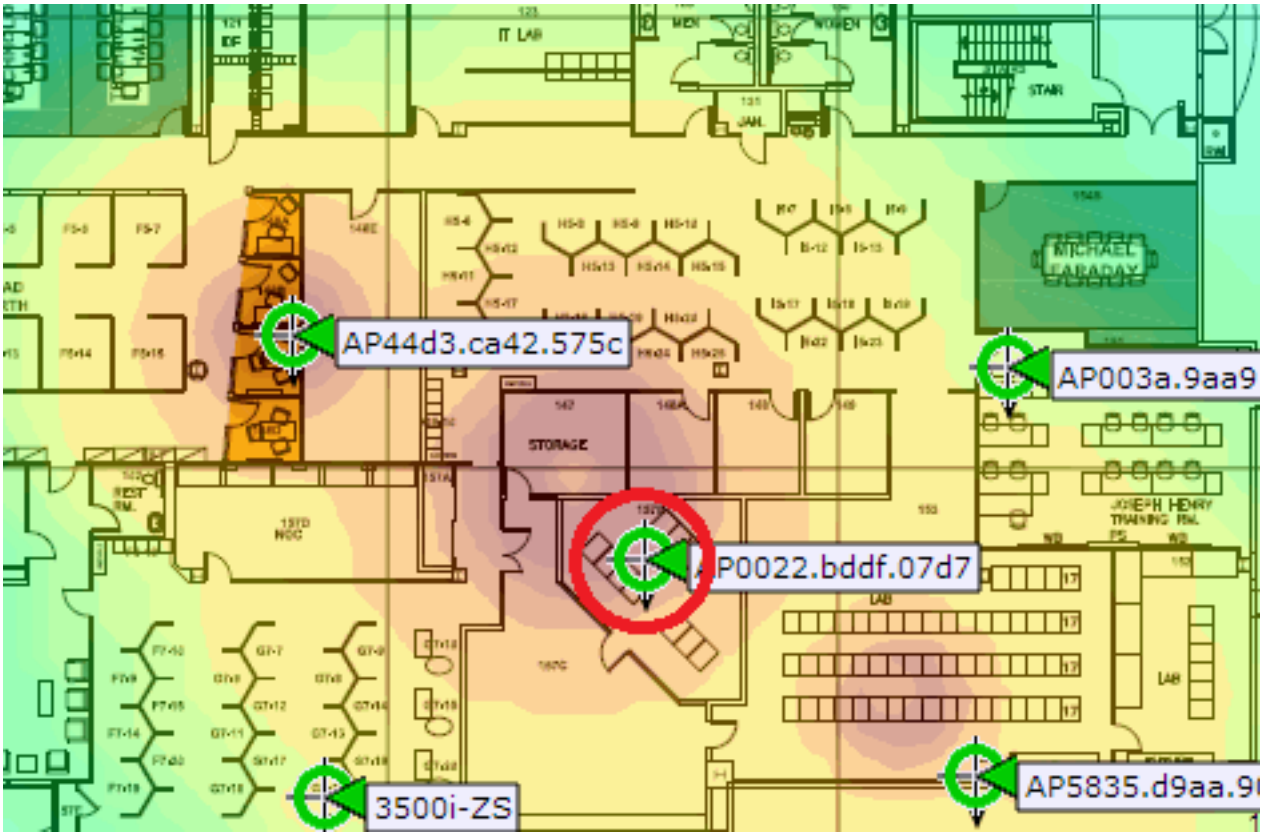
Cisco 3600系列AP使用通道內和通道外的組合。2.4GHz和5GHz射頻掃描在通道上，WSSI模組掃描在通道外，在所有2.4GHz和5GHz通道之間循環。



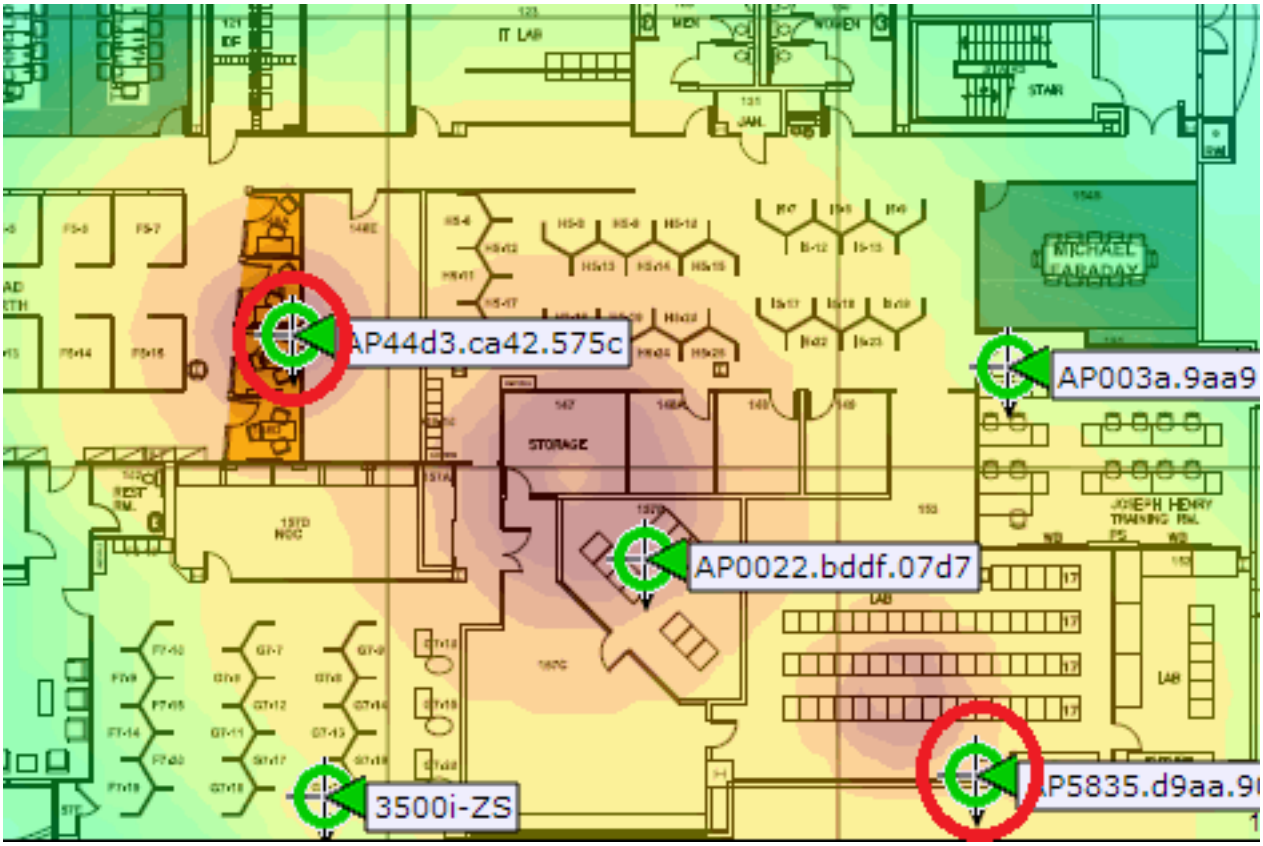
WSSI模組的建議部署密度

在傳統的監控AP部署中，思科建議每5個本地模式AP配置1個MMAP。這取決於網路設計和專家指導，以確定最佳覆蓋範圍。對於WSSI模組，根據功能提供不同的部署建議，以實現與MMAP的覆蓋奇偶校驗。

對於CleanAir，建議為每5個本地或Flexconnect AP部署1個WSSI模組。此1:5部署提供與啟用CleanAir的MMAP相同的效能，但仍允許AP為客戶端提供服務。建議對執行CleanAir的WSSI模組進行以下部署：



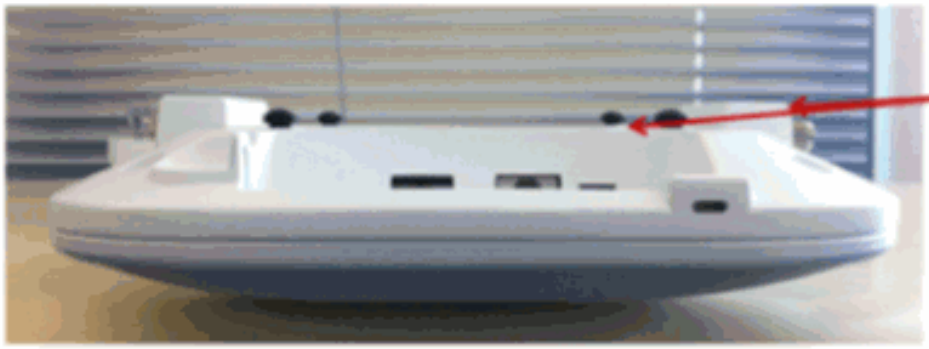
對於wIPS保護，建議為每5個本地或FlexConnect AP部署2個WSSI模組。通道外攻擊的wIPS檢測時間約為MMAP的兩倍。因此，需要2:5的部署才能提供wIPS檢測奇偶校驗。對於執行wIPS保護的WSSI模組，推薦部署如下：



帶WSSI模組的Cisco 3600 AP利用通道內和通道外掃描，在為客戶端提供服務時提供行業領先的解決方案。

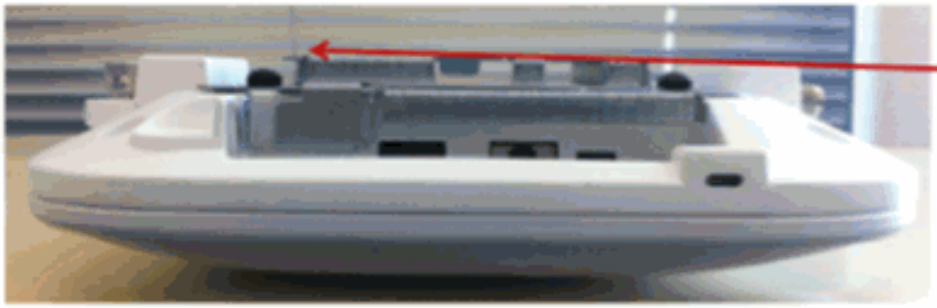
安裝WSSI模組

AP3600 - WSSI Module



Monitor Module installed can have a slight rise

Bracket-1 would be slightly below rise

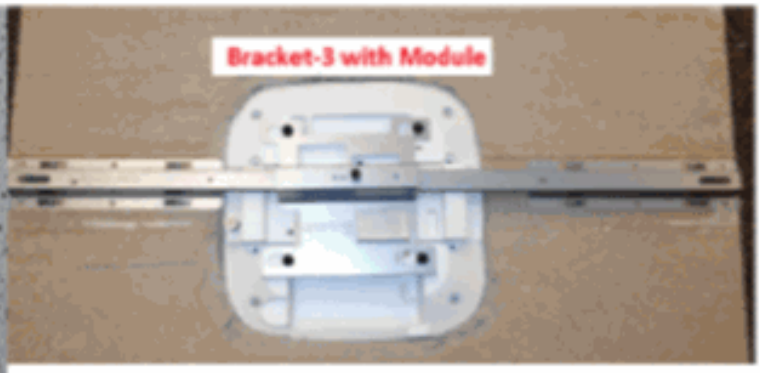


Monitor Module is Flush when Bracket-2 is used

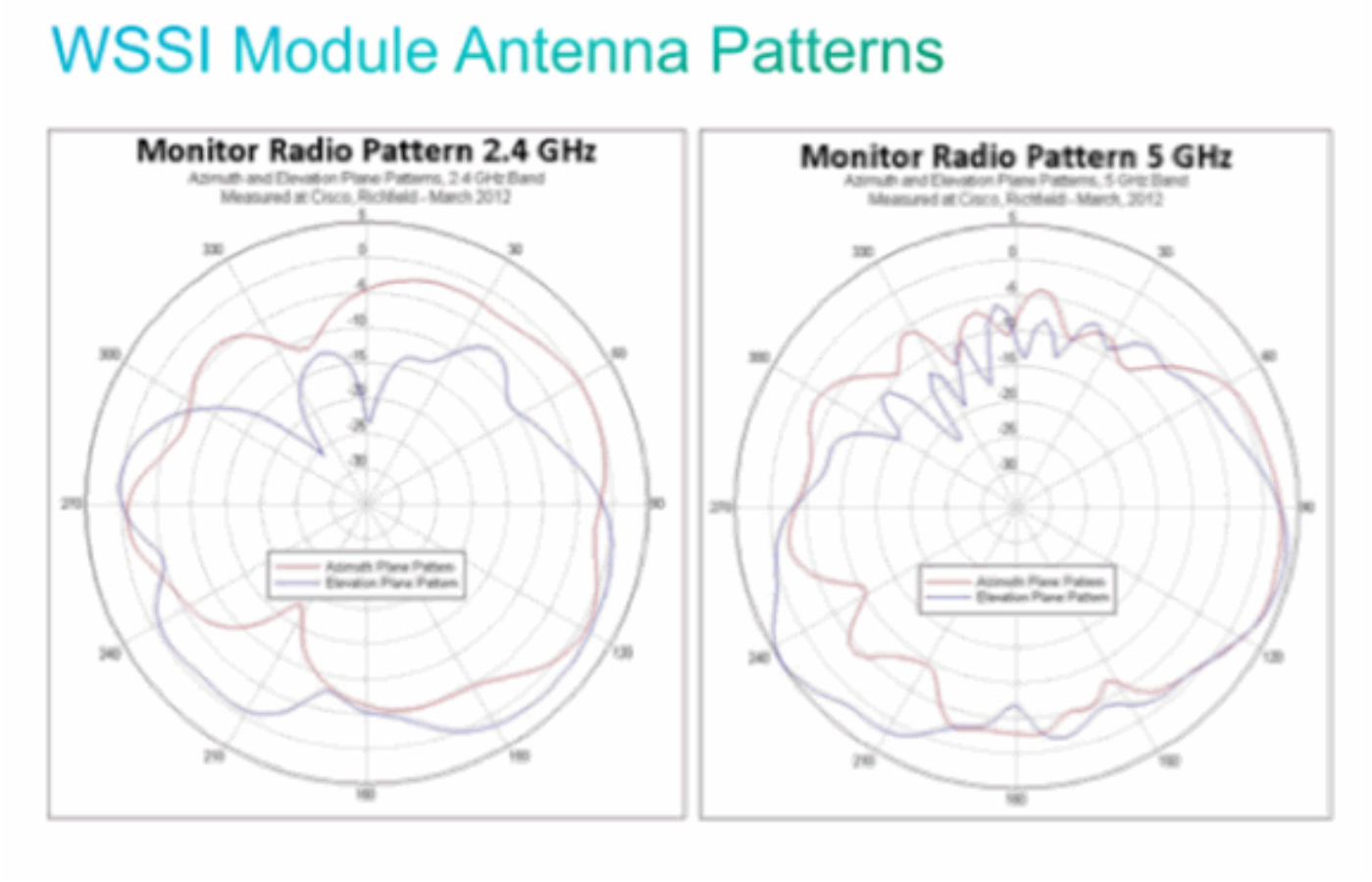
Recommend Customers use Mounting Bracket-2 or Bracket-3
Existing Bracket-1 may work on some ceilings but not on hard surfaces

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



AP3600 WSSI模組的配置

不需要為WSSI模組進行配置。模組使用其0x4（僅接收）0個Tx天線x 4個Rx天線自動掃描兩個頻段上的所有通道。

請注意，WSSI模組僅在本地模式或FlexConnect模式下配置的AP3600上處於活動狀態。WSSI模組在所有其他模式下均被禁用。

WSSI模組的電源要求

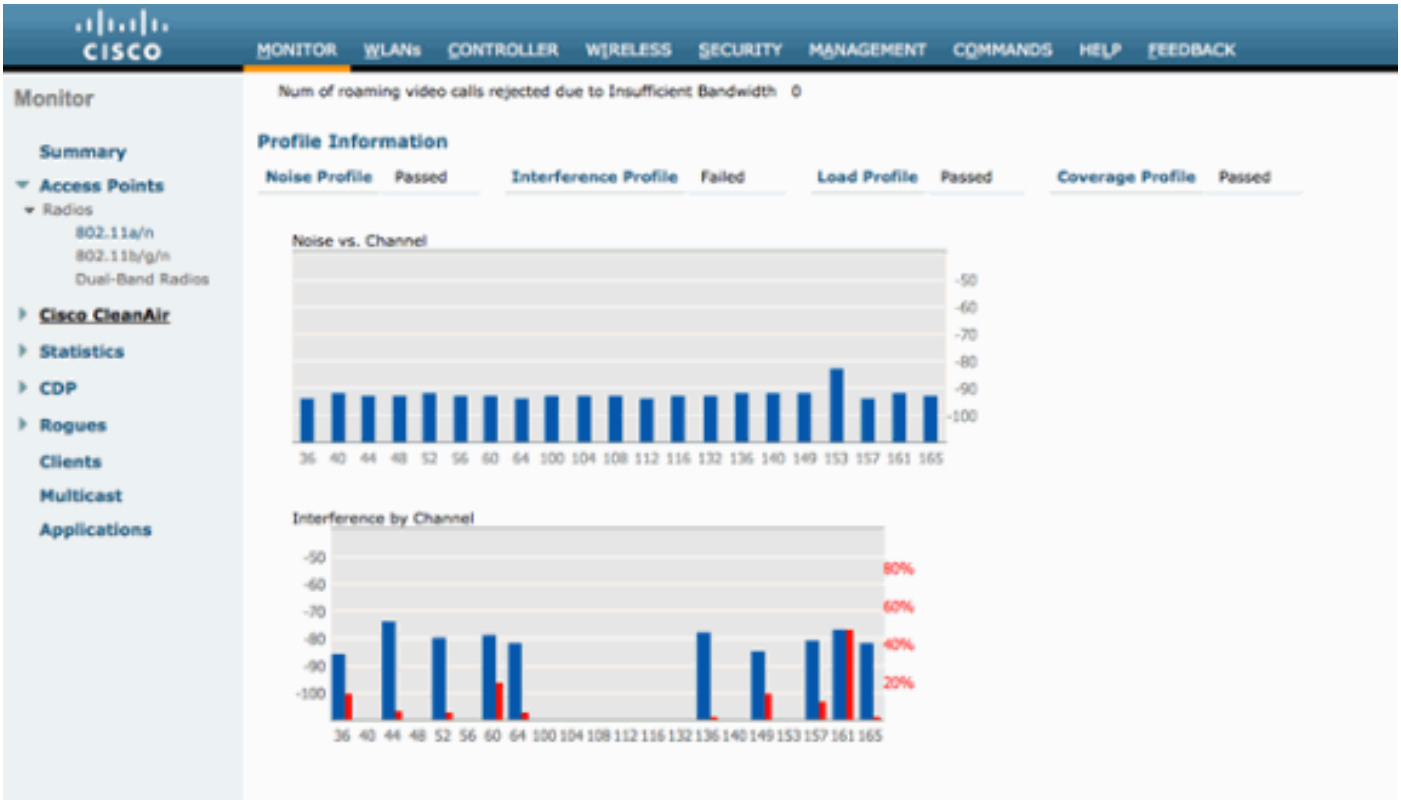
安裝了WSSI模組的AP3600超過15.4瓦(802.3af)。 AP需要(802.3at - PoE+)、增強型PoE、本地交流電源或Cisco PoE饋電器(AIR-PWRINJ4)。

附註：

- 增強型PoE由思科建立，是802.3at PoE+的先驅。它提供高達20W的功率。
- PoE+可提供高達30W的功率。

WSSI模組上的無線電資源管理

WSSI模組在2.4GHz和5GHz頻帶上執行所有RRM測量。測量結果顯示在WLC GUI中的「監控」(Monitor)>「接入點」(Access Points)>「802.11a/n」(802.11a/n)>「AP_NAME」(AP_NAME)>「詳細資訊」(Details)或「監控」(Monitor)>「接入點」(Access Points)>「802.11b/g/n」(802.11b/g/n)>「AP_NAME」(AP_AP)>「詳細資訊」(Details)下。



WSSI模組上的CleanAir

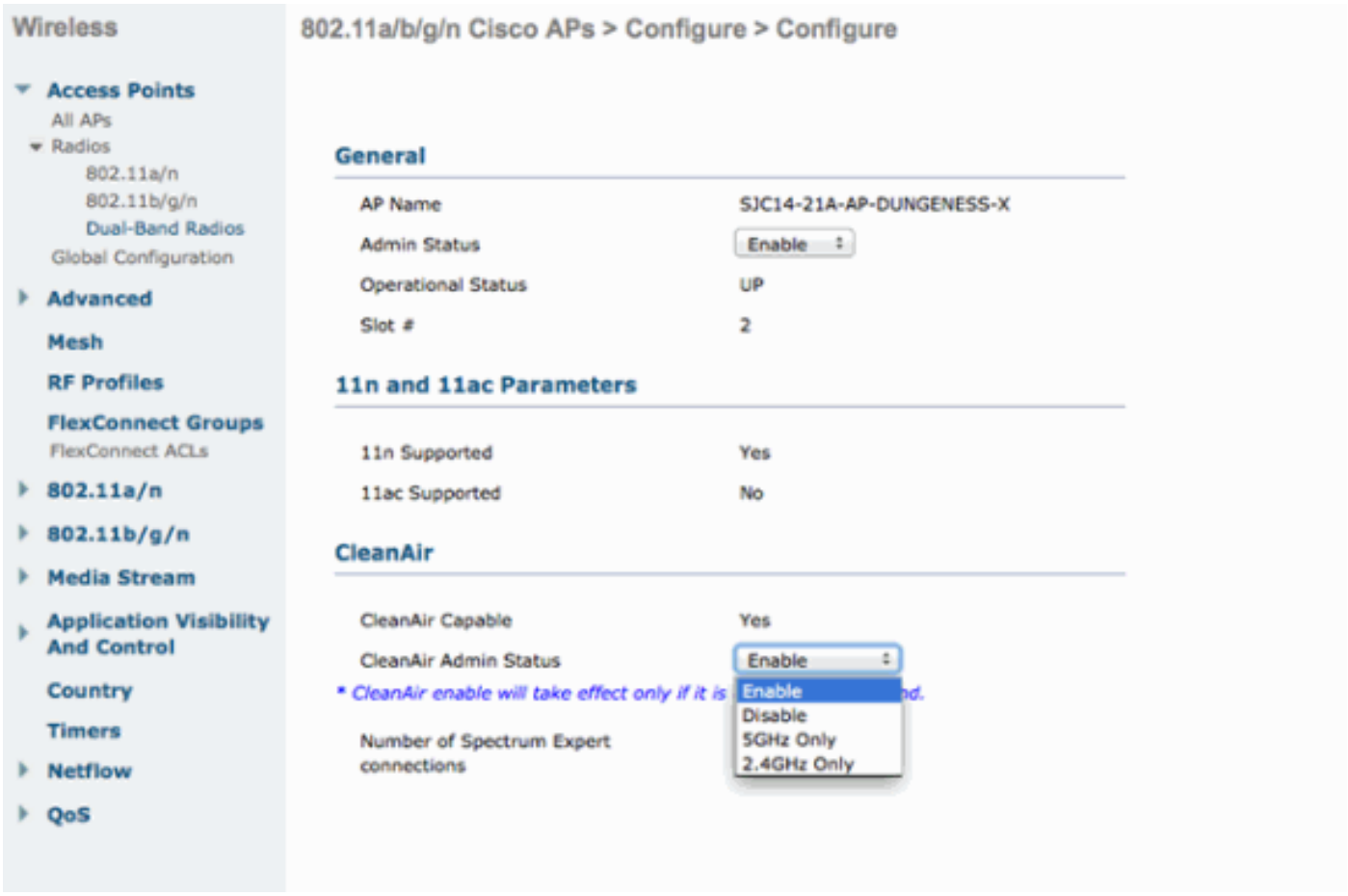
WSSI模組以與MMAP相同的精度檢測CleanAir干擾源。思科建議以1:5的密度部署WSSI模組，其中每5個AP必須有1個WSSI模組。此密度與MMAP的建議密度相同。

當啟用無子模式的WSSI模組時，模組會掃描2.4GHz和5GHz頻段。該模組在每個通道上保留1.2秒並掃描CleanAir干擾源。

CleanAir僅在2.4GHz、5GHz以及2.4GHz和5GHz上啟用。可從WLC CLI或GUI選擇此選項。以下是在WLC CLI上設定CleanAir的範例：

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

通過Wireless > Dual-Band Radiations > Configure可在GUI上應用相同的配置。以下是範例：



要驗證WSSI模組是否檢測到CleanAir干擾程式，請從AP控制檯發出**show cleanair interferers**命令：

```
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
```

通過Wireless > Dual-Band Radiations > Configure可在GUI上應用相同的配置。以下是範例：

WLC GUI上報告CleanAir干擾。每個頻段顯示干擾源。這意味著在5GHz頻段的WSSI模組上檢測到的干擾將顯示在Monitor > 802.11a/n > Interference Devices下。

若要驗證WSSI模組是否檢測到CleanAir干擾程式，請從AP控制檯發出**show cleanair interferers**:

```
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
```

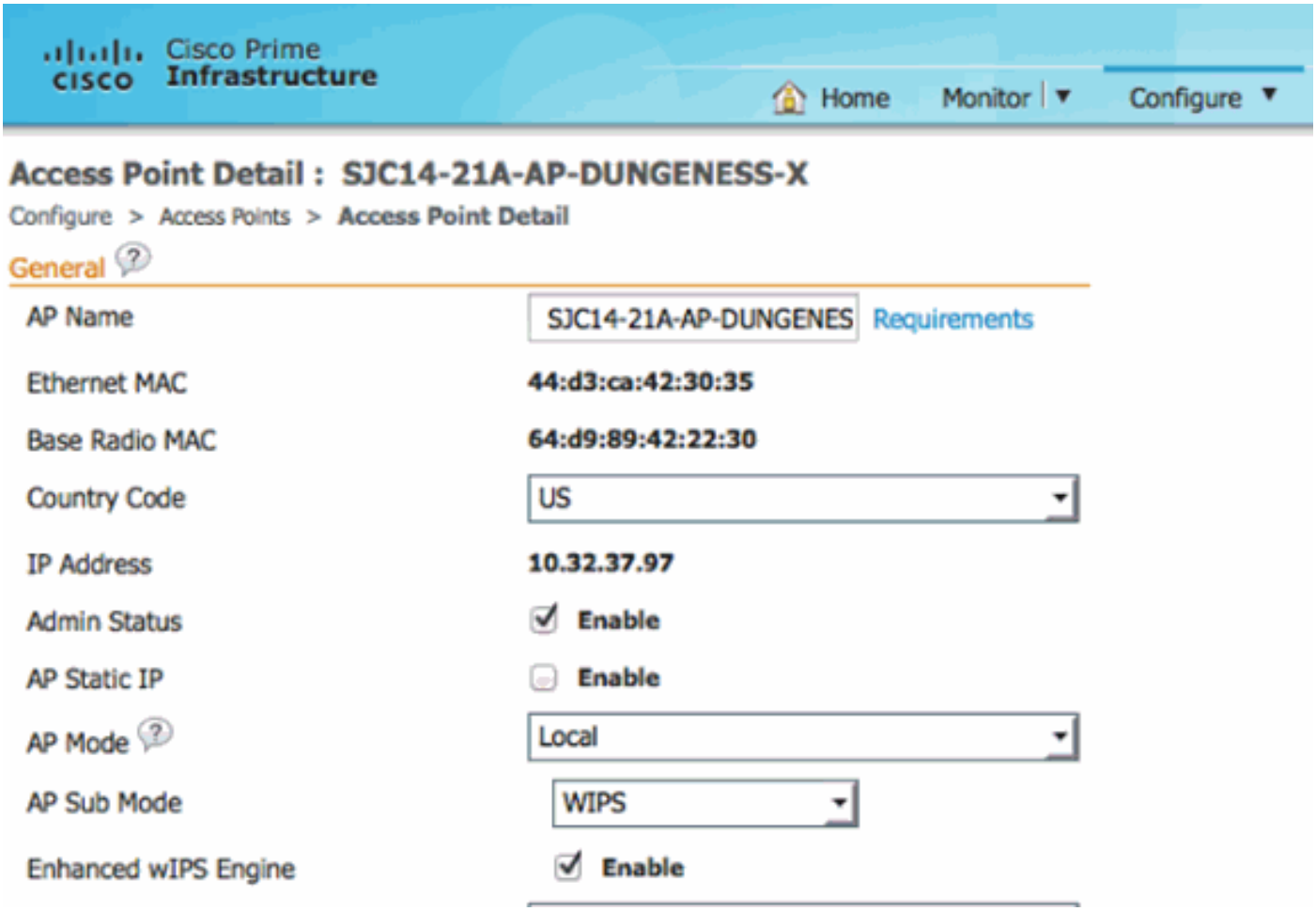
wssi模組上的wIPS

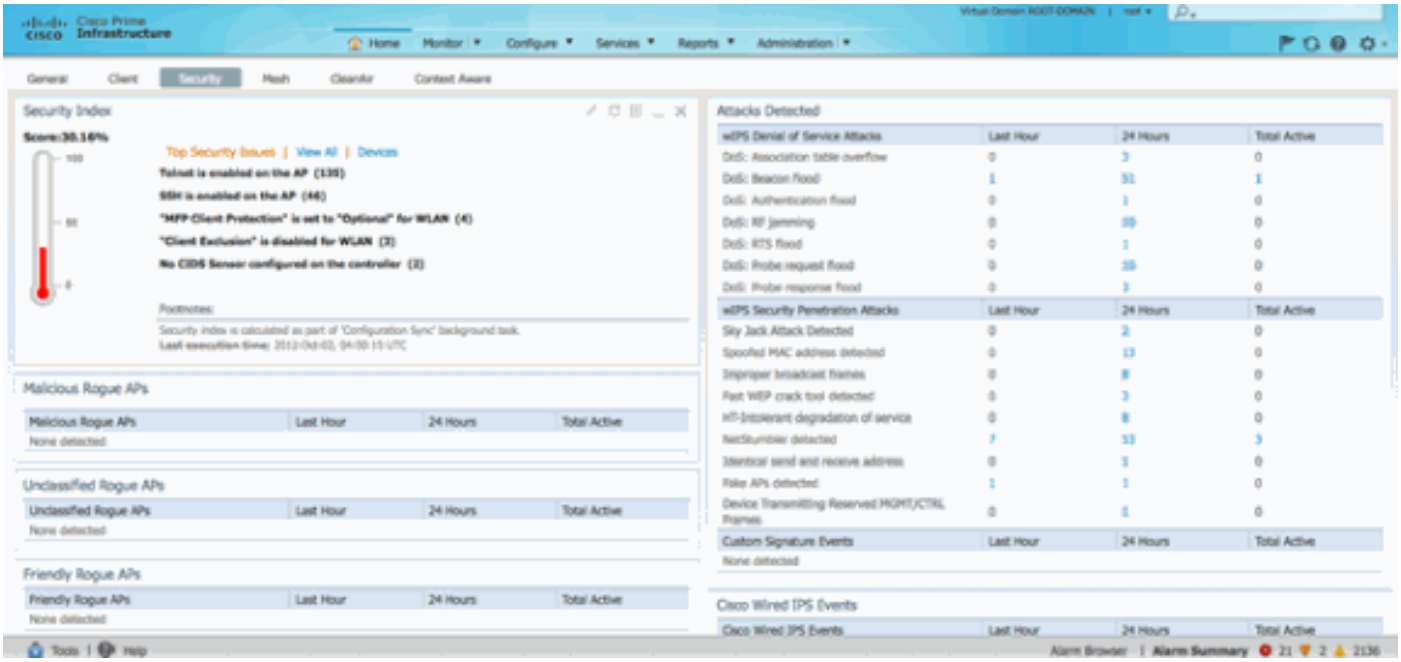
WSSI模組檢測wIPS攻擊者的準確度幾乎與MMAP相同。對於wIPS，思科建議在AP之間以2:5的比例部署WSSI模組。這意味著每5個AP中，必須有2個AP包含WSSI模組。

可以配置兩種wIPS模式：

- wIPS子模式 — 啟用wIPS攻擊檢測並掃描1.2s的所有通道。除了wIPS檢測外，此模式還允許AP捕獲所有RRM報告。
- 增強型wIPS模式 — 啟用wIPS攻擊檢測並掃描所有通道250毫秒。通道停留時間越短，安全模組檢測攻擊者的速度就越快。

從Prime Infrastructure(PI)頁面，轉至Configure > Access Points > AP_NAME。WSSI模組可配置為wIPS子模式或wIPS子模式+增強型wIPS引擎支援。這也可以作為AP配置模板的一部分推送。





wIPS攻擊顯示在Prime Infrastructure的Home > Security頁籤中。

PI顯示網路級檢視，但您可以從AP控制檯發出**show capwap am alarm ALARM_NUM**命令，顯示對具有WSSI模組的AP3600的攻擊。

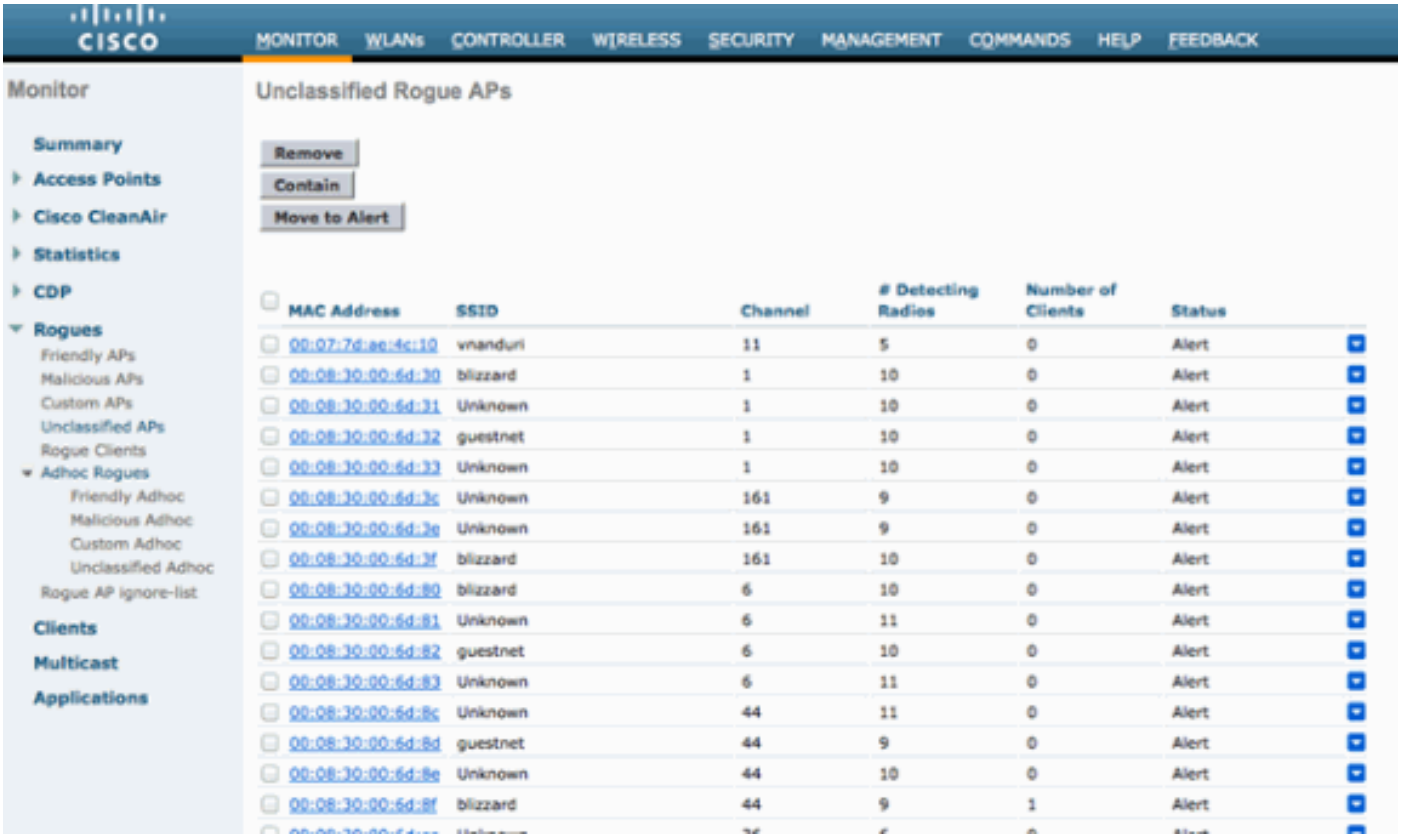
例如，警報52是拒絕服務、身份驗證泛洪。若要檢視是否在WSSI模組上檢測到該攻擊，請發出**show capwap am alarm 52**命令：

```
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
```

WSSI模組上的欺詐檢測

WSSI模組檢測無管理AP的準確度與MMAP相同。WLC和PI中均會顯示惡意AP清單。

這是WLC GUI中的未分類欺詐AP清單。可在WLC GUI的Monitor > Rogues下檢視惡意AP。

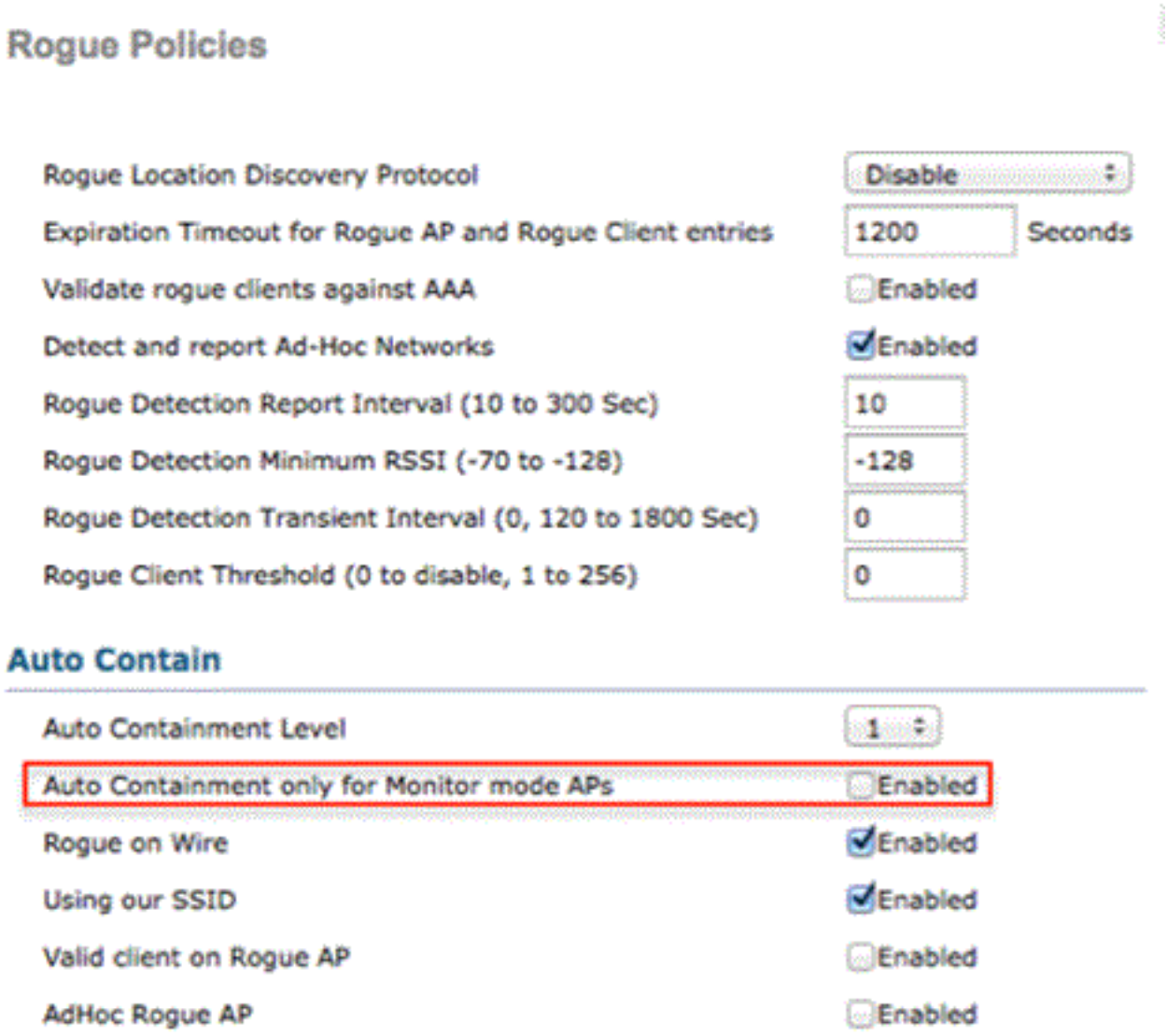


您可以使用AP控制檯驗證WSSI模組是否檢測到無管理AP。在控制檯中，輸入**show capwap rm rogue ap d2 all**命令。這將顯示在WSSI模組無線電中看到的所有欺詐AP。

```
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
```

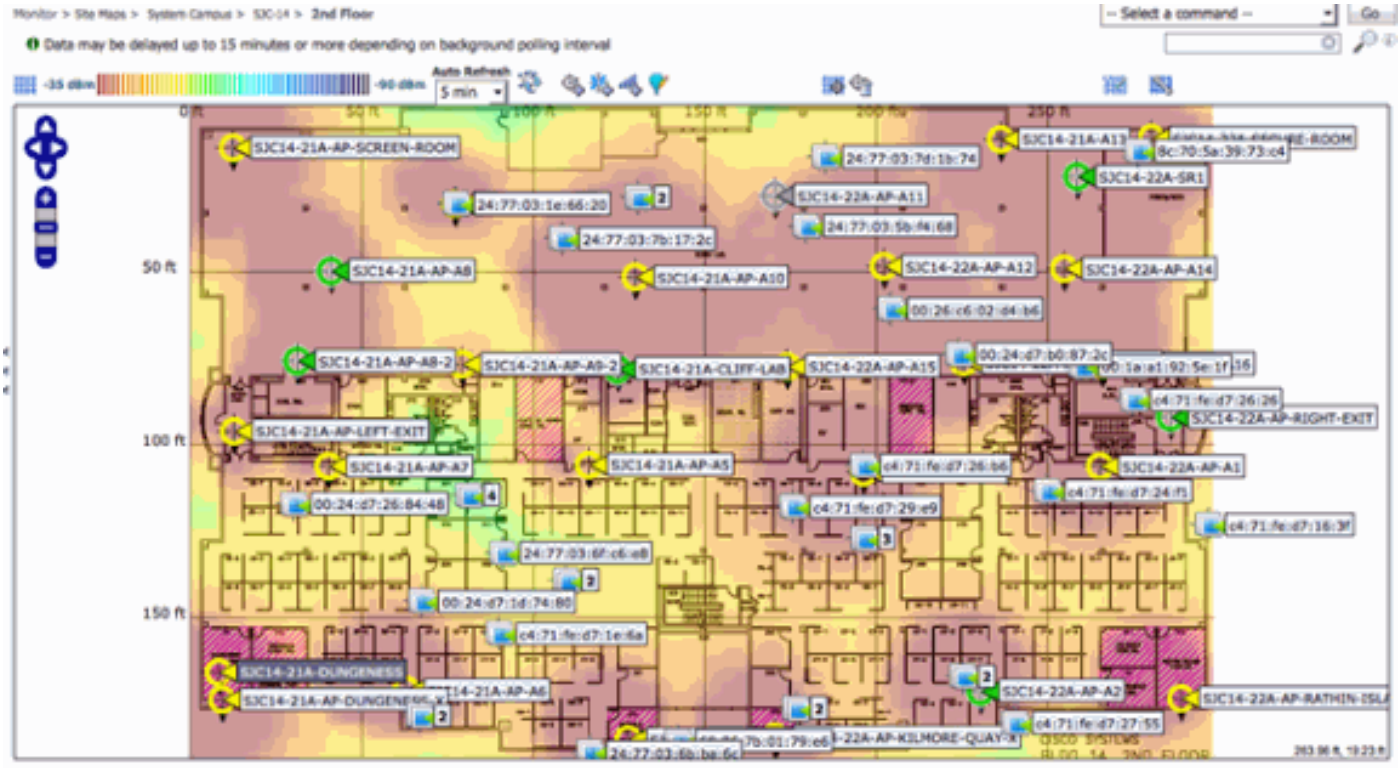
使用WSSI模組的欺詐控制

WSSI模組是0x4模組（僅接收天線），這意味著將對2.4GHz或5GHz無線電執行欺詐遏制操作。為了將WSSI配置為自動包含惡意AP，您必須確保在WLC GUI中的Security > Wireless Protection Policies > Rogue Policies > General下，未啟用**Auto Containing only for Monitor mode AP**（請參見下一個螢幕快照）。 可以啟用所有其他覈取方塊。



WSSI模組上的情景感知位置

當與Cisco MSE連線時，WSSI模組可提供與MMAP相同的準確度環境感知位置資料。



WSSI模組授權

WSSI模組使用wIPS監控模式許可證。

相關資訊

- 技術支援與文件 - Cisco Systems