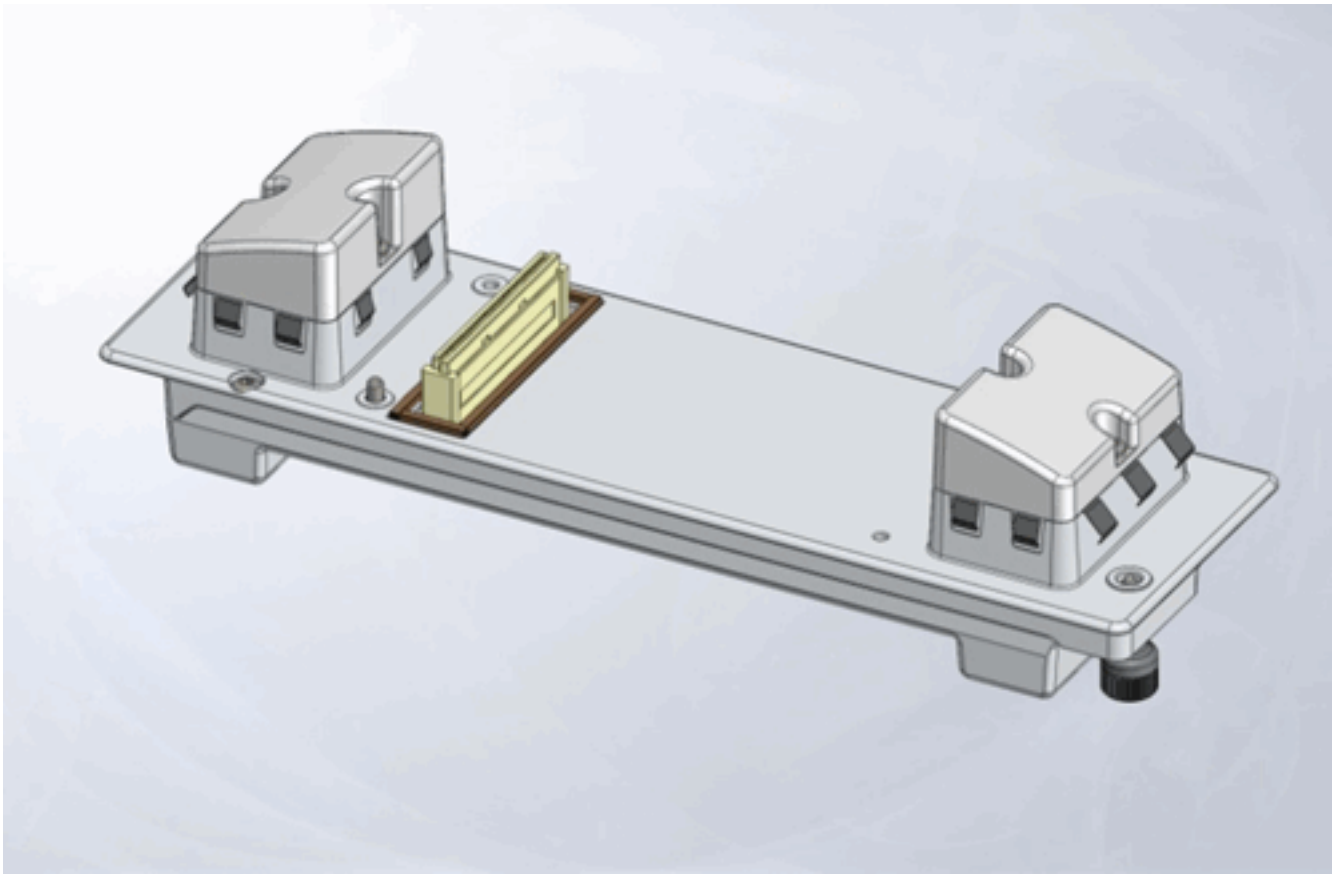
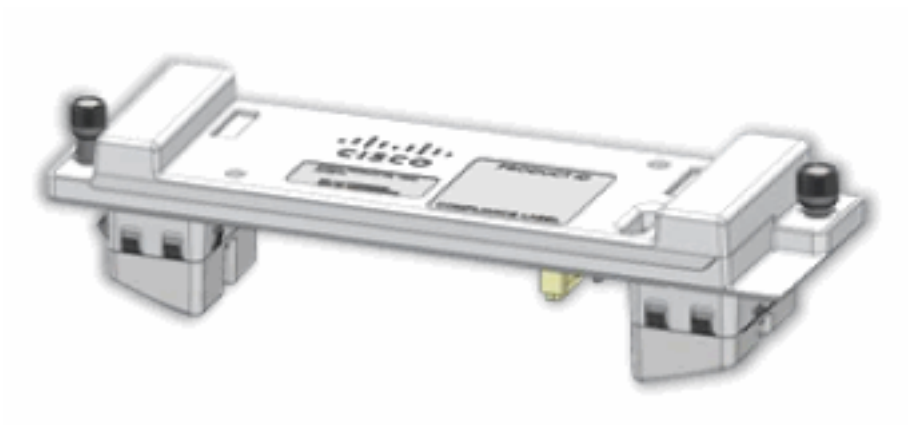
Cisco Aironet无线安全和光谱智能(WSSI)部署指南的AP模块

目录

简介

本文为无线安全和光谱智能的(WSSI) Cisco Aironet接入点模块提供一般配置和部署指导。WSSI是可以插入到模块化访问访问接入点的附加模块(AP)例如Cisco 3600系列AP。





先决条件

要求

本文档没有任何特定的要求。

使用的组件

无线安全和光谱智能模块需要最小编码版本：

- 无线局域网控制器(WLC) –版本7.4.xx.xx或以上
- 接入点(AP) –版本7.4.xx.xx或以上
- 头等基础设施(PI) –版本1.3.xx.xx或以上
- 移动服务引擎(MSE) –版本7.4.xx.xx或以上

规则

有关文档规则的详细信息，请参阅 Cisco 技术提示规则。

产品概述

Cisco无线安全和光谱智能模块，利用Cisco Aironet 3600系列AP的灵活模块设计，提供史无前例，不间断工作的安全扫描和光谱智能。这帮助您避免无线电频率(RF)干扰，以便您获得更加好的覆盖和性能在您的无线网络。

- 24 X 7全面的监视器和缓解aWIPS、CleanAir、上下文感知、恶意检测和无线电资源管理的
- 24 X 7在信道aWIPS威胁保护
- 23倍更多安全和光谱覆盖
- 30%+ CAPEX成本节省与专用的监控模式AP

- 零的联系配置

WSSI现场可升级的模块是卸载所有监听和安全服务从客户端/数据服务无线电到安全监视器模块的一专用的无线电。这不仅允许更加好的客户端性能，而且通过排除对专用的监控模式AP的需要和要求的以太网基础设施降低开销连接那些设备到他们的网络。

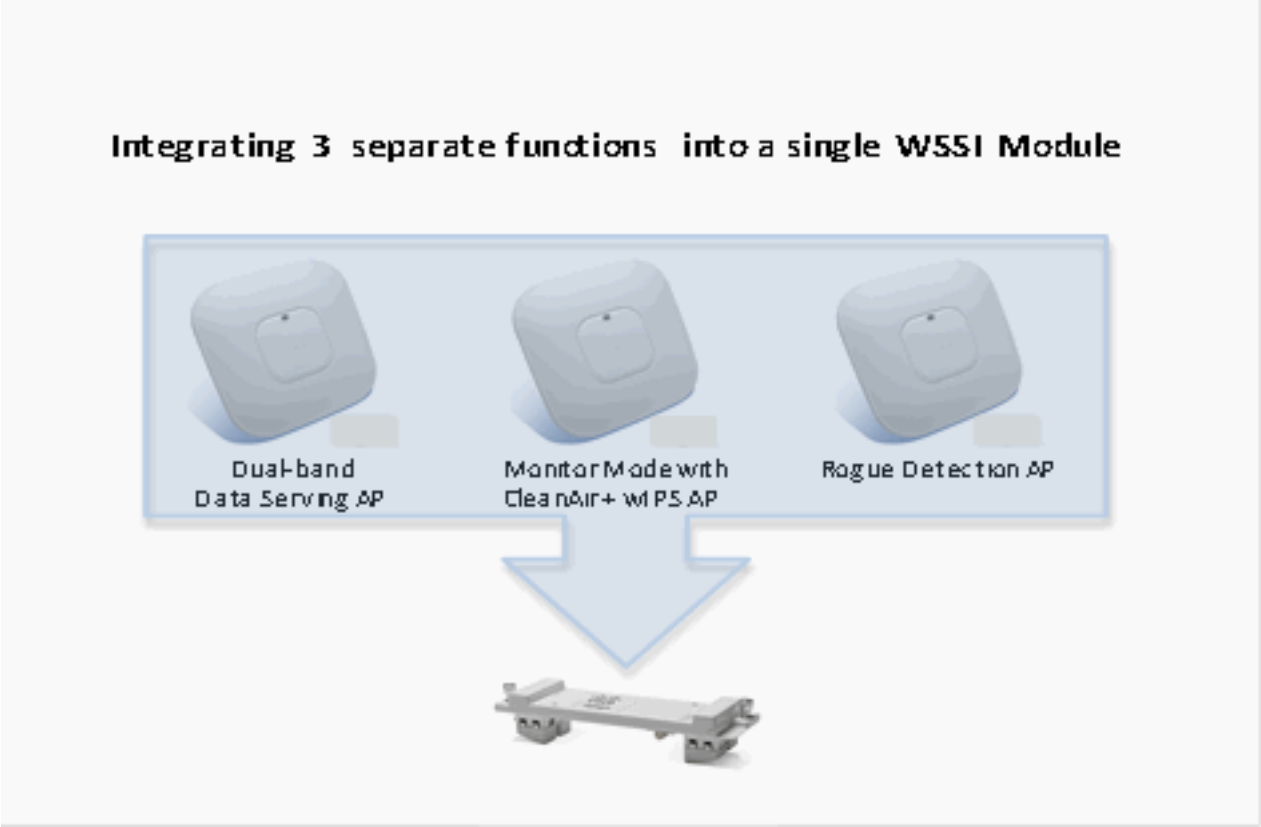
同时， 3600系列AP和WSSI模块enable (event)同時提供科技目前进步水平安全和频谱分析的您为wi-fi所有信道的客户端作用，在2.4 GHz和5 GHz波段。

一旦部署，模块经常扫描所有信道帮助保证在行业的多数安全和稳健无线体验联机。

WSSI模式优点

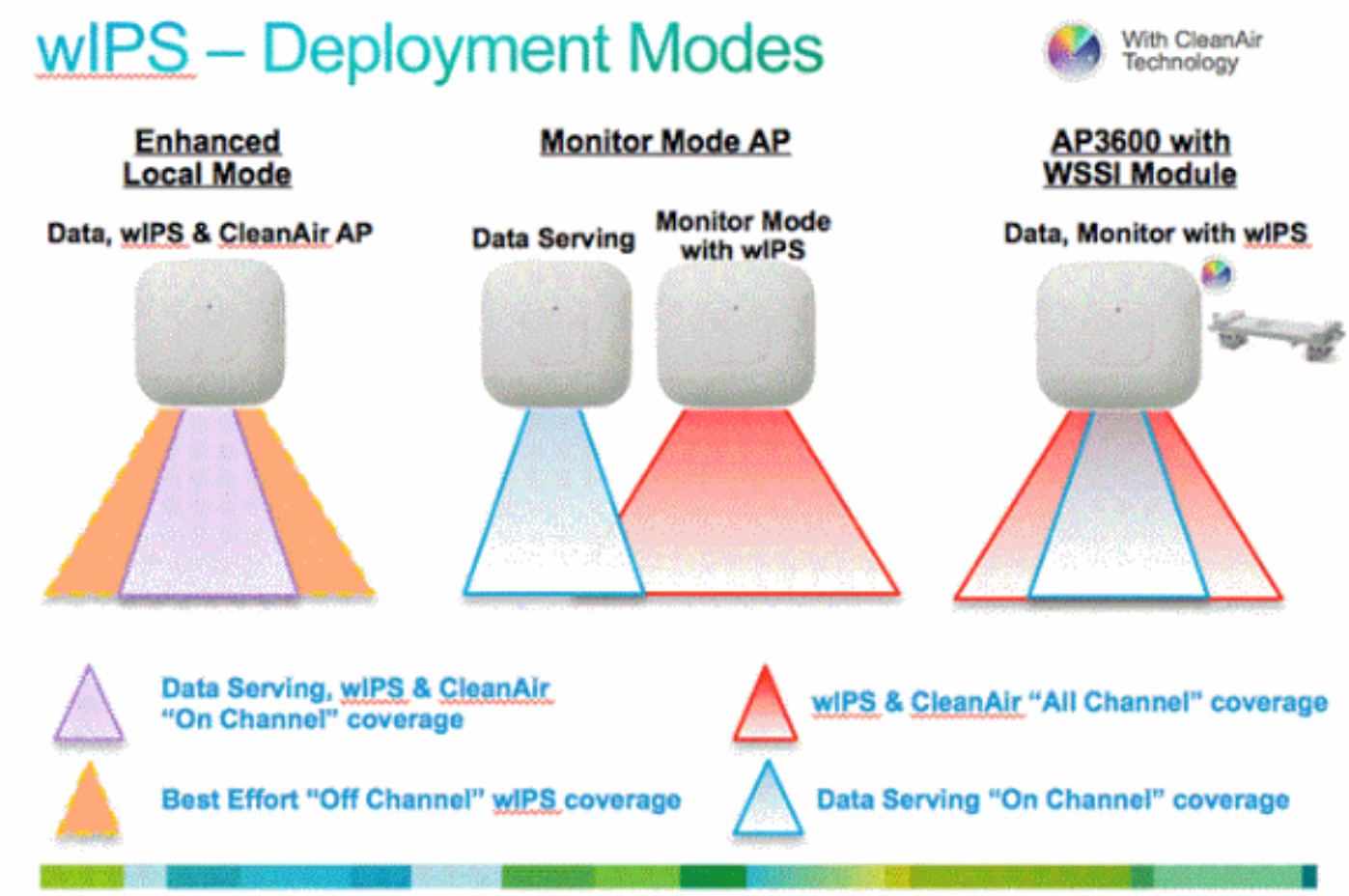
改进的本地传送方式(榆木) ：

- 减少网络成本和操作。通过集成WSSI模块到3600系列里，您能替换三个独立设备。这提供三个独立的功能到单个，多用途3600系列AP。



- 客户能当前有效利用单个以太网连接(电缆和端口)到他们的有线网络，在什么位置将典型地要求三种独立的以太网电缆和接入端口到他们的有线网络。这极大减少他们的CAPEX。
- 通过集成对单个AP的所有这些功能，客户简化每日管理和监控他们的无线结构和网络与一非常地减少的AP数。WSSI模块出现到WLC和管理系统作为其他无线电支持的802.11b/g/a/n客户端设备(2.4和5 GHz)在特定3600系列AP内。
- *零的联系配置*，安装，通电和是。没有绝对要求的配置使WSSI模块是正在运行和立即监控并且保护您的无线网络。WSSI模块插入并且绑到所有3600系列AP上。当AP是电源备份时模块与在AP的其他无线电一起初始化和立即开始监控在2.4和5 GHz的所有信道所有潜在的安全威胁和干扰源的。
- 可适应在所有信道的wIPS提供准确和高效威胁检测从通过空气攻击、恶意AP和临时连接，以及能力分类，为不变监听和主动管理通知，缓和并且报告。与Cisco Mobility服务引擎(MSE)一道工作。

榆木：



- 添加wIPS 7x24的安全扫描在信道扫描(2.4GHz和5 GHz)，与尽力信道支持。
- AP另外服务客户端和有G2系列的AP，启用在信道的CleanAir频谱分析(2.4GHz和5GHz)。

监控模式：

- 监控模式AP (MMAP)在监控模式投入运行并且有所有信道选项添加wIPS安全扫描(2.4GHz和5GHz)。
- G2系列AP启用在所有信道的CleanAir频谱分析(2.4GHz和5GHz)。
- MMAPs不服务客户端。

AP3600用WSSI模块：无线安全和光谱的演变

- 使用CleanAir技术，实现同时客户端服务、wIPS安全扫描和频谱分析的行业的第一AP。
- 启用7x24所有无线信道扫描在2.4GHz和5GHz波段的专用的2.4GHz和5GHz无线电用其自己的天线。
- 单个以太网基础设施提供简化操作以少量设备管理并且优化AP3600无线结构和以太网有线基础架构的投资回报。

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

- 思科CleanAir技术：提供积极，高速的光谱情报抵抗性能问题由于无线干扰。检查并且分类能量模式的行业的第一个科技目前进步水平RF分析技术(签名)设备能极大影响无线网络的质量。
- 高级无线电资源管理(RRM) ：简化的，先进的RF管理，自动地适应根据信息的无线网络环境接收从思科CleanAir技术。一旦干扰物识别， RRM能移动客户端设备向远离干扰的信道和调节传输电源移动远离干扰源。对用户的此提供更加好的RF质量。
- 恶意检测：检测并且报告背后网络访问和访问对无线客户端。
- 位置和上下文感知：提供实时感知和能力跟踪无线终端。

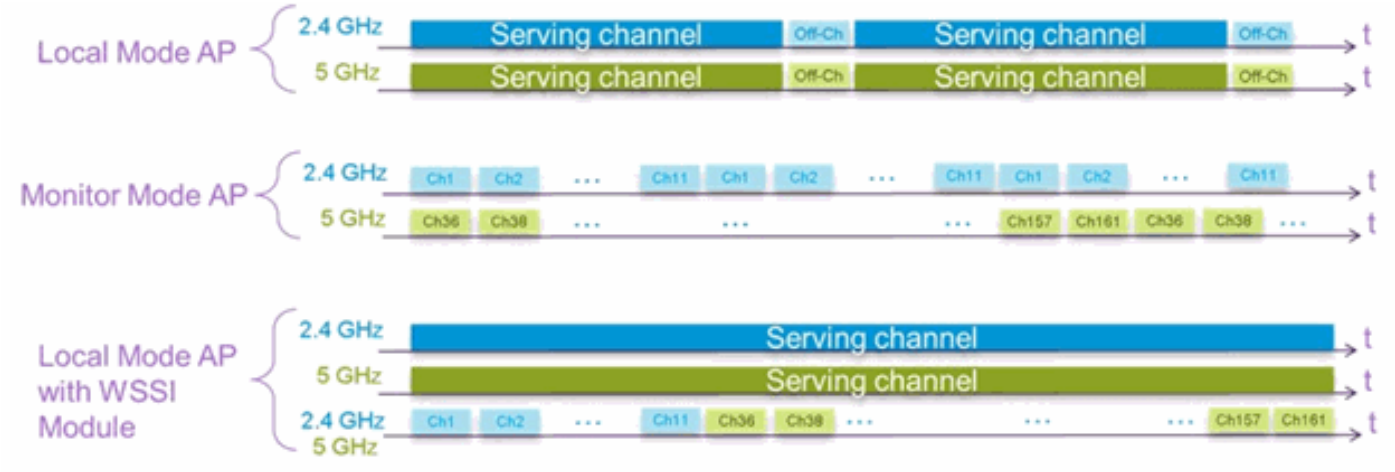
使用这些功能， Cisco无线安全和光谱智能模块，与Cisco 3600系列AP一起，为您的集群用户和数据提供安全的多数和可能坚固企业级的无线网络。

在信道与脱离信道使用WSSI模块

本地传送方式AP为CleanAir干扰物和wIPs攻击者在信道扫描。这意味着仅AP扫瞄信道服务。与2.4GHz无线电服务信道1和5GHz无线电服务信道64，仅提供保护的本地传送方式AP在信道1和64。

MMAP为CleanAir干扰物和wIPs攻击者脱离信道扫描。这意味着AP扫描所有信道。2.4GHz无线电扫描所有2.4GHz信道，并且5GHz信道扫描所有5GHz信道。

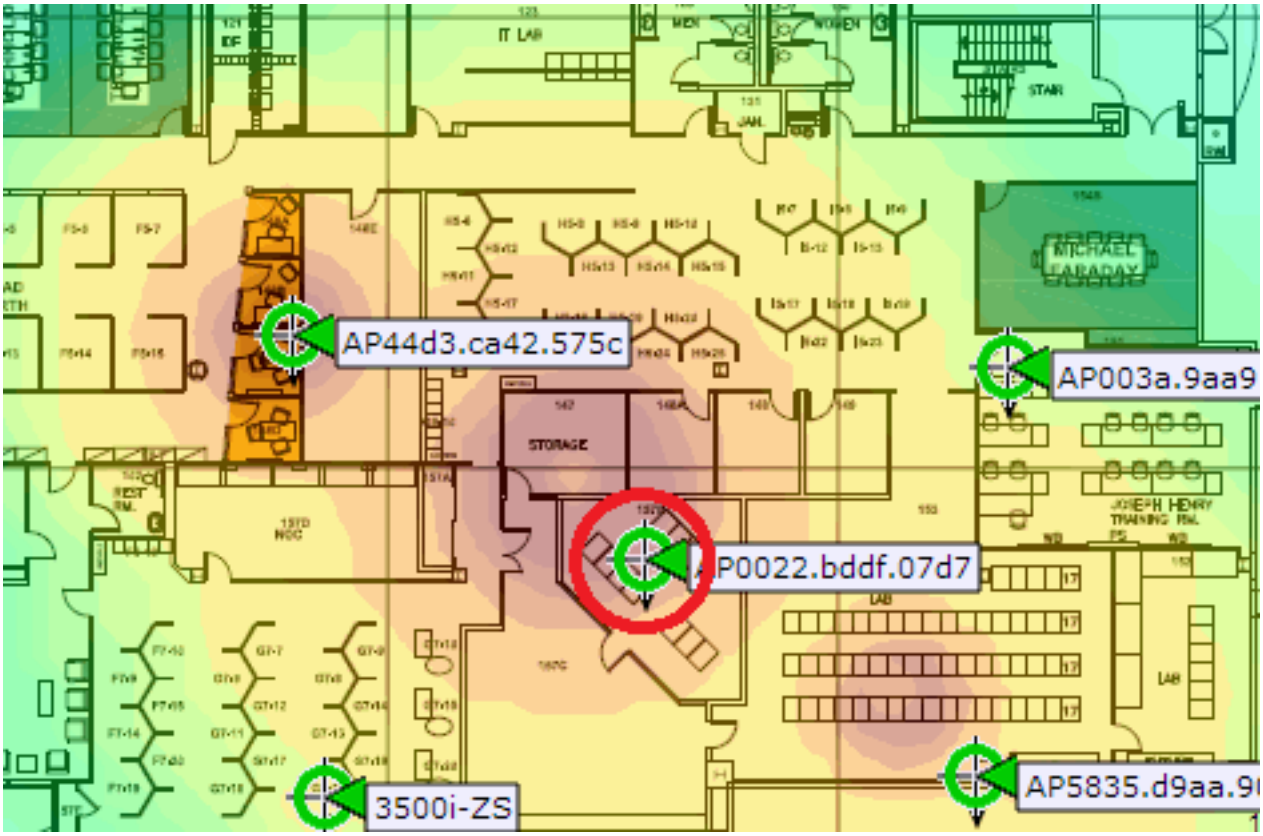
Cisco 3600系列AP使用在信道和脱离信道的组合。2.4GHz和5GHz无线电扫描在信道，并且WSSI模块扫描脱离信道，循环在所有2.4GHz和5GHz信道之间。



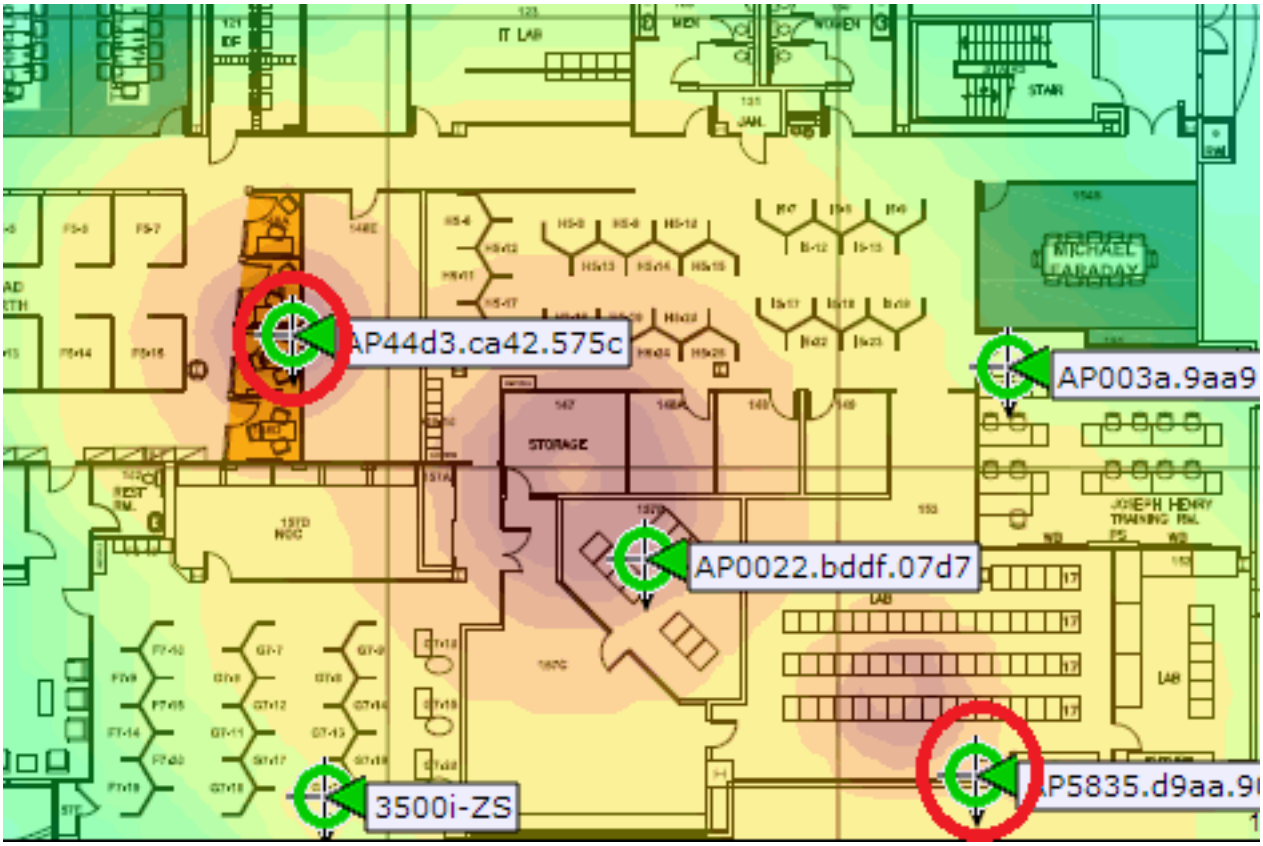
建议的WSSI模块的部署密度

在传统箴言报AP部署，思科推荐1个MMAP比与每5本地传送方式AP。这能变化基于最好的覆盖的网络设计和专家指导。使用WSSI模块，有根据功能的不同的部署推荐达到与MMAP的覆盖奇偶校验。

对于CleanAir，推荐部署每5本地或Flexconnect的AP 1个WSSI模块。此1:5部署提供性能和CleanAir启用的MMAP一样，但是仍然允许AP为客户端服务。这是WSSI的模块执行的CleanAir一推荐的部署：



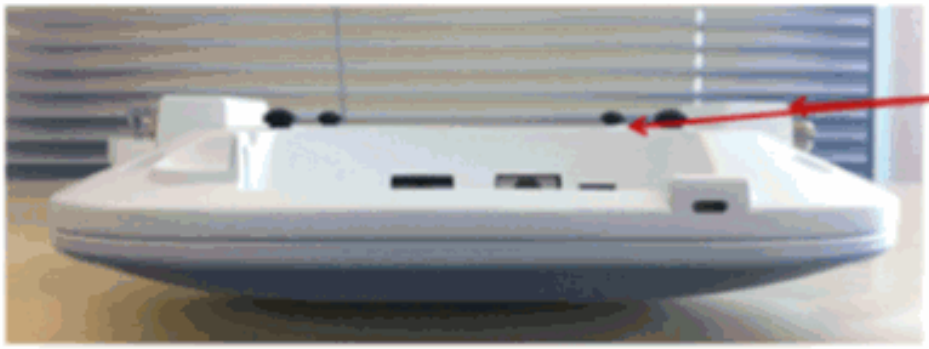
对于wIPS保护，推荐部署每5本地或FlexConnect的AP 2个WSSI模块。脱离信道攻击的wIPS检测时间是大约MMAP的两次。所以， 2:5部署要求提供wIPS检测奇偶校验。这是WSSI模块执行的wIPS保护的推荐的部署：



Cisco3600 AP用WSSI模块使用在信道和脱离信道扫描提供行业一流的解决方案，当服务客户端时。

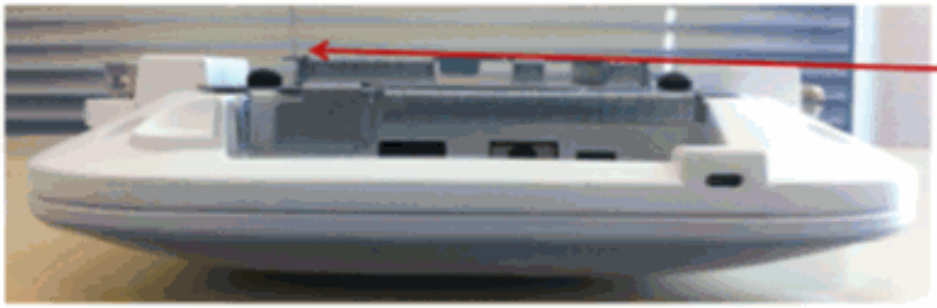
安装WSSI模块

AP3600 - WSSI Module



Monitor Module installed can have a slight rise

Bracket-1 would be slightly below rise

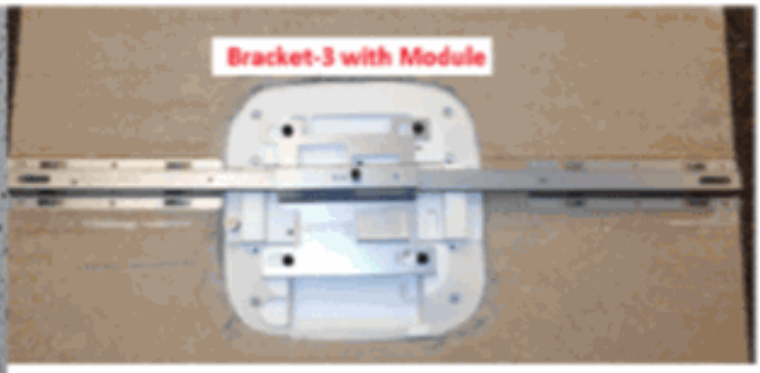


Monitor Module is Flush when Bracket-2 is used

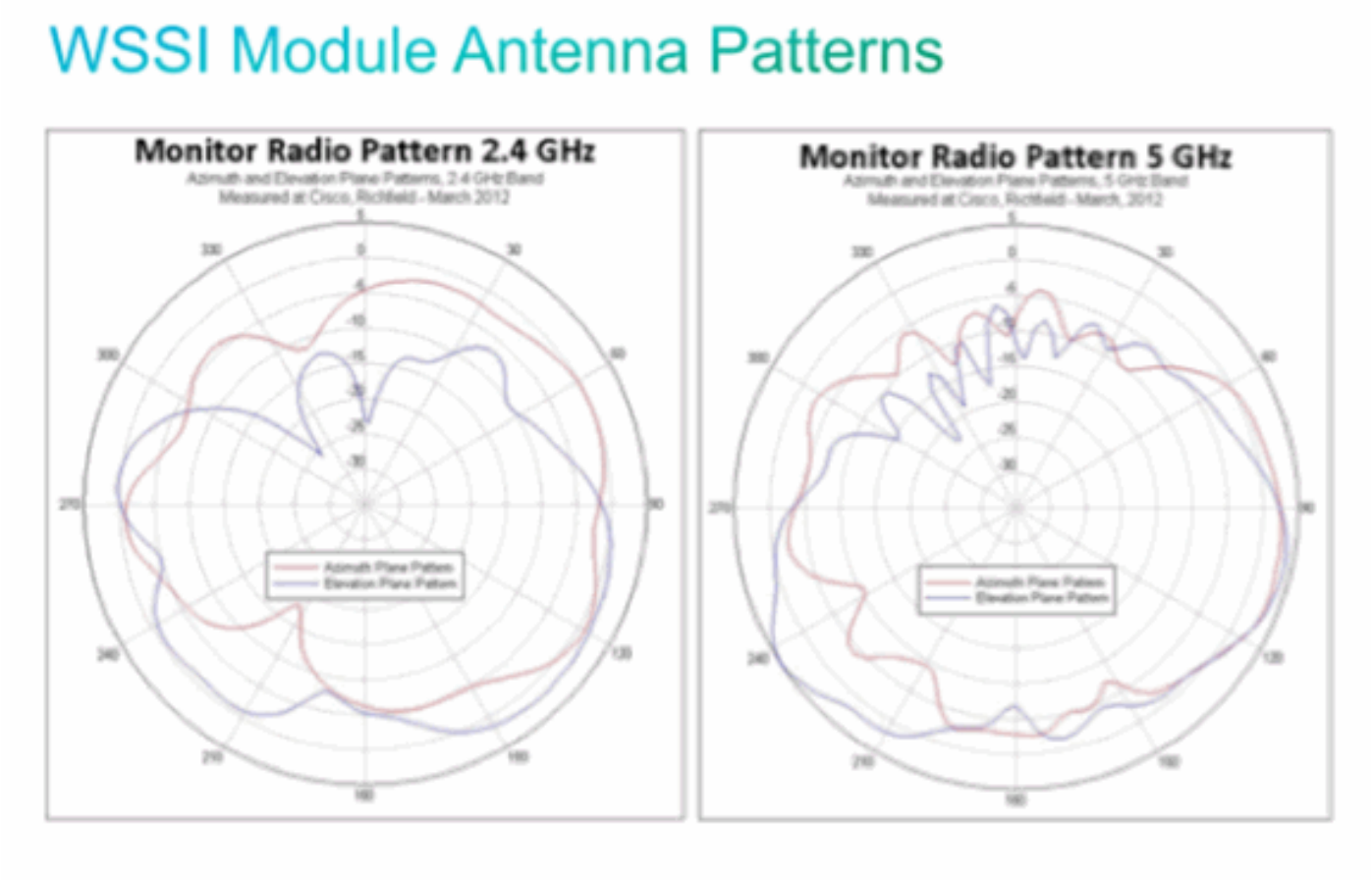
Recommend Customers use Mounting Bracket-2 or Bracket-3
Existing Bracket-1 may work on some ceilings but not on hard surfaces

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模块的配置

没有需要的WSSI模块的配置。模块自动地扫描在两个波段的所有信道使用其0x4 (只接收) 0 Tx天线 x 4 Rx天线。

注意WSSI模块只是活跃的在本地传送方式或FlexConnect模式配置的AP3600s。WSSI模块在其他模式禁用。

WSSI模块的功率要求

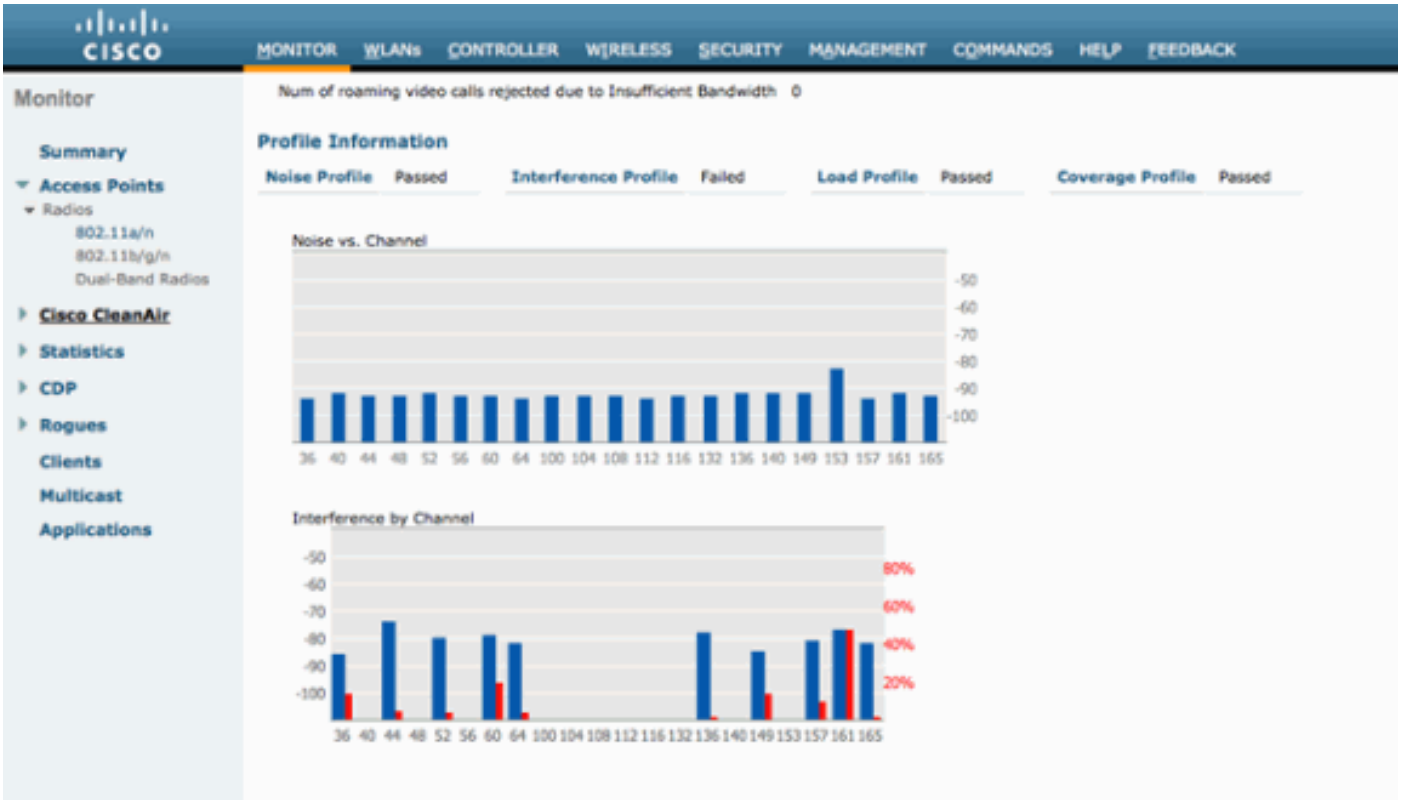
AP3600用安装的WSSI模块超出15.4瓦特(802.3af)。AP要求二者之一(802.3at - PoE+)，增强版柏吾，一个本地AC电源或者思科柏吾注射器(AIR-PWRINJ4)。

注意：

- 增强版柏吾由思科创建并且是先行者对802.3at PoE+。它提供至电源20W。
- PoE+能传送至电源30W。

在WSSI模块的无线电资源管理

WSSI模块采取在2.4GHz波段和5GHz的所有RRM评定波段。评定在监视器>接入点> 802.11a/n > AP_NAME >详细信息或者监视器>接入点> 802.11b/g/n > AP_NAME >详细信息下的WLC GUI显示。



在WSSI模块的CleanAir

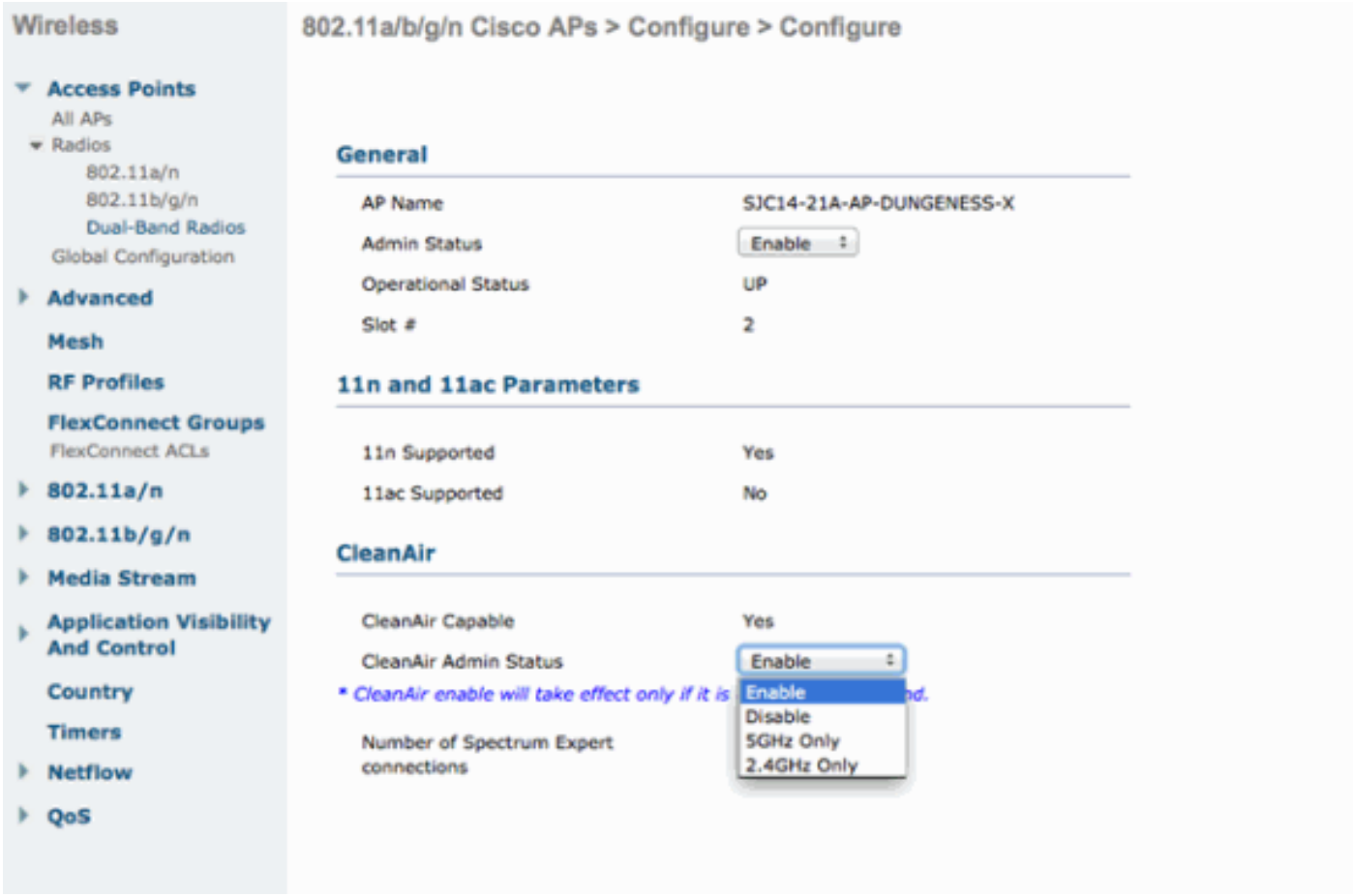
WSSI模块检测有精确度的CleanAir干扰物和MMAP一样。思科建议WSSI模块配置有一个密度1:5，其中必须有每5的AP 1个WSSI模块。这是推荐的密度和一样MMAP的。

当WSSI模块启用没有从属方式时，模块扫描2.4GHz波段和5GHz波段。模块在1.2secs的每个信道居住并且为CleanAir干扰物扫描。

CleanAir在仅仅2.4GHz， 5GHz可以启用，和2.4GHz和5GHz。这从WLC CLI或GUI是可选择的。这是配置在WLC CLI的CleanAir示例：

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

相同的配置在GUI可以应用通过无线>双波段无线电>配置。这是此的示例：



为了验证CleanAir干扰物由WSSI模块检测，请发出从AP控制台的**显示cleanair干扰物**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
```

相同的配置在GUI可以应用通过无线>双波段无线电>配置。示例如下：

CleanAir干扰物报告在WLC GUI。干扰物每波段显示。这意味着在5GHz波段的WSSI模块检测的干扰物显示在监视器>下802.11a/n >干扰设备。

为了验证CleanAir干扰物由WSSI模块检测，请发出从AP控制台的**显示cleanair干扰物**：

```
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
```

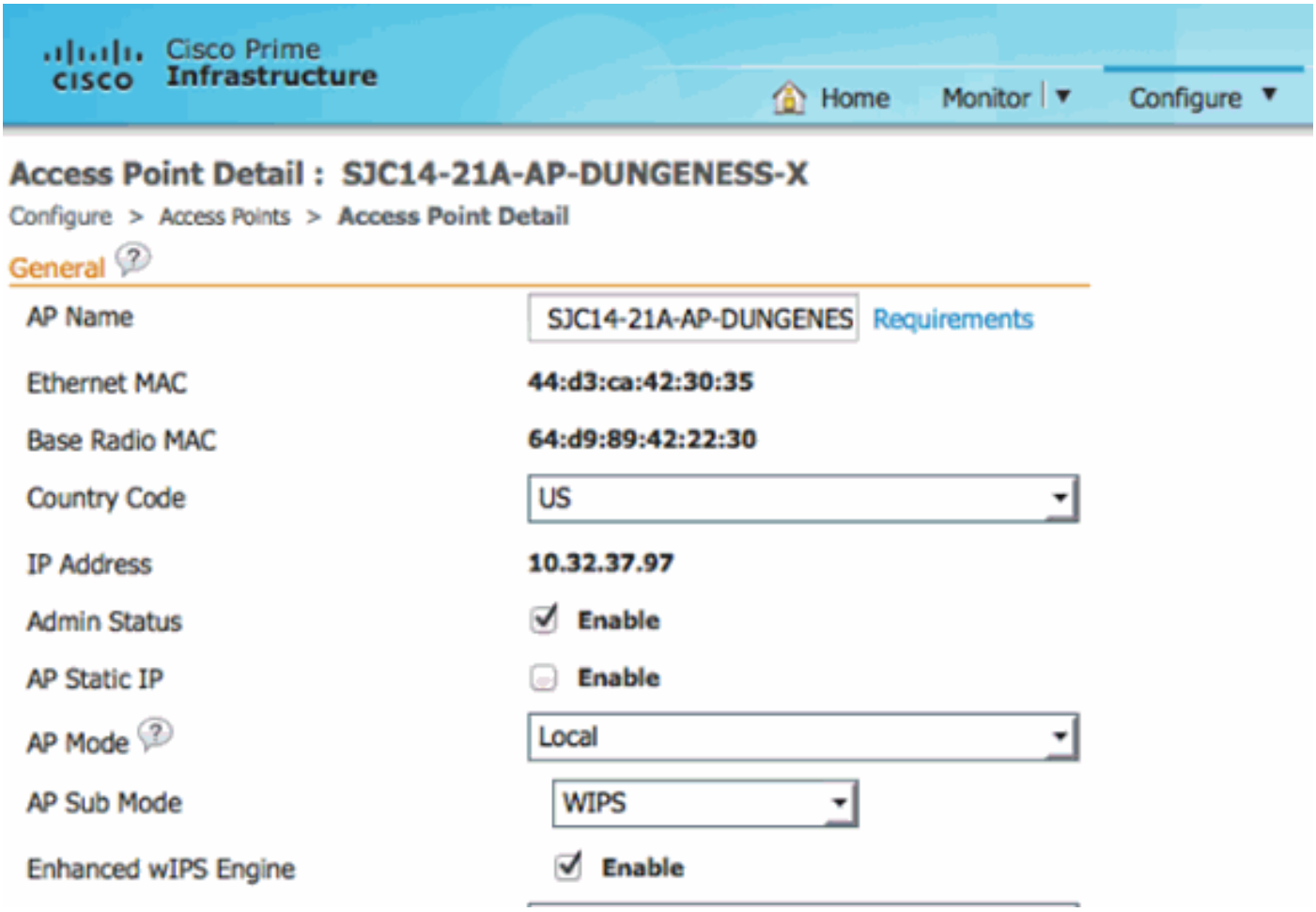
在WSSI模块的wIPS

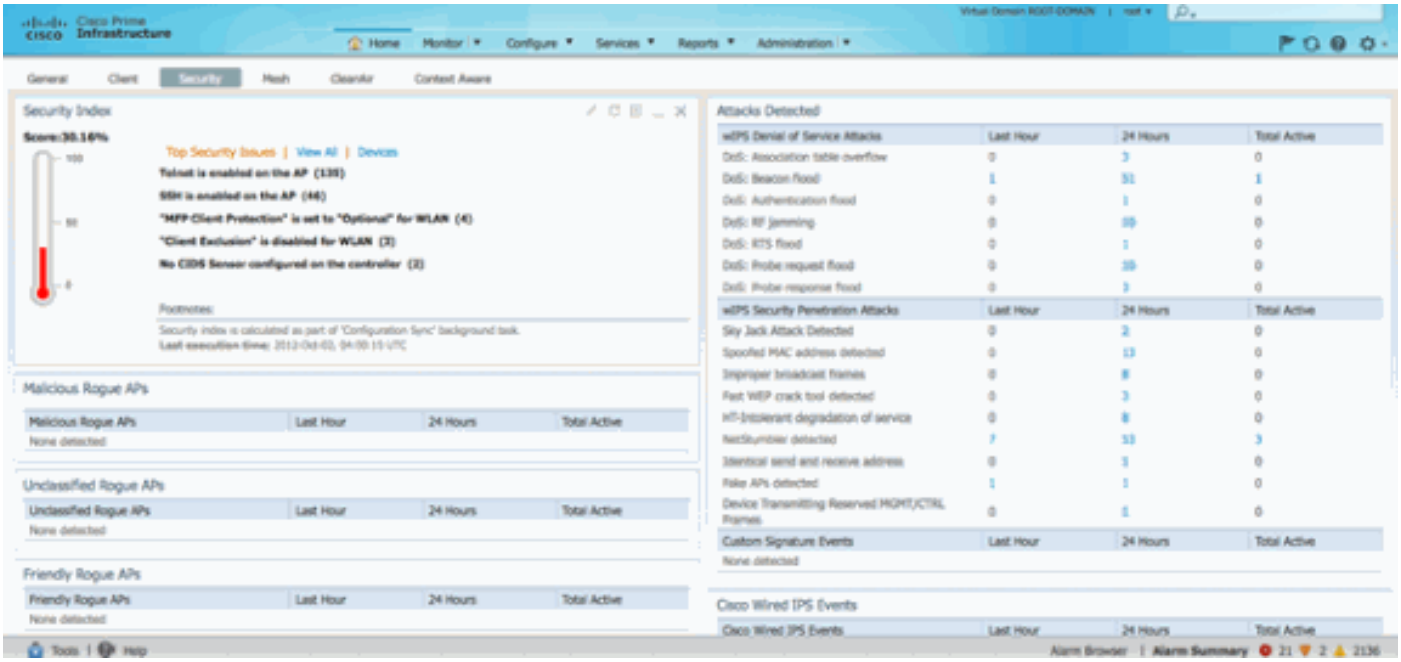
WSSI模块接近检测与精确度的wIPS攻击者和MMAP一样。对于wIPS，思科推荐部署WSSI模块以在AP中的一个2:5比率。这为每5 AP意味着，两AP必须包含WSSI模块。

有可以配置的两个wIPS模式：

- wIPS从属方式-启动wIPS攻击检测并且扫描1.2s的所有信道。除wIPS检测之外，此模式允许AP仍然捕获所有RRM报告。
- 增强版wIPS模式-启动wIPS攻击检测并且扫描250ms的所有信道。更加小的信道停留时间允许安全模块检测更加快速的攻击者。

从头等基础设施(PI)页，去配置> Acesss指向> AP_NAME。WSSI模块可以配置到wIPS从属方式或wIPS从属方式+增强版wIPS引擎支持。作为AP配置模板一部分，这可能也推送。





wIPS攻击显示在从家庭> Security选项卡的头等基础设施。

PI显示网络级视图，但是您能通过发出从AP控制台的**显示capwap上午报警ALARM_NUM**命令显示在AP3600的攻击用WSSI模块。

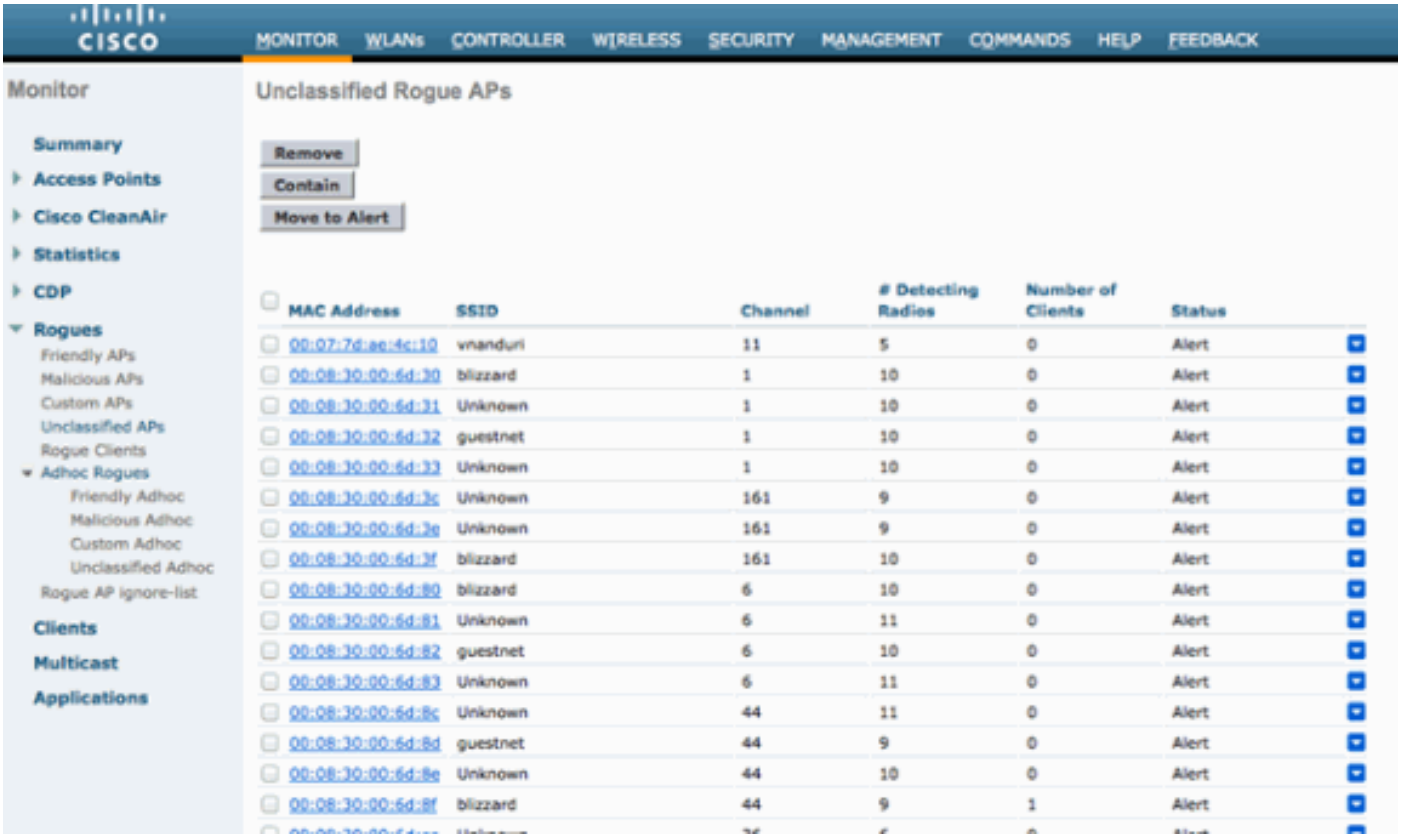
例如，报警52是拒绝服务，验证充斥。为了看到该攻击是否检测在WSSI模块，请发出**显示capwap上午报警52**命令：

```
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
```

歹徒在WSSI模块检测

WSSI模块检测与精确度的恶意AP和MMAP一样。恶意AP列表在WLC和PI显示。

这是未保密的歹徒AP列表从WLC GUI的。恶意AP在监视器>歹徒下的WLC GUI可以查看。

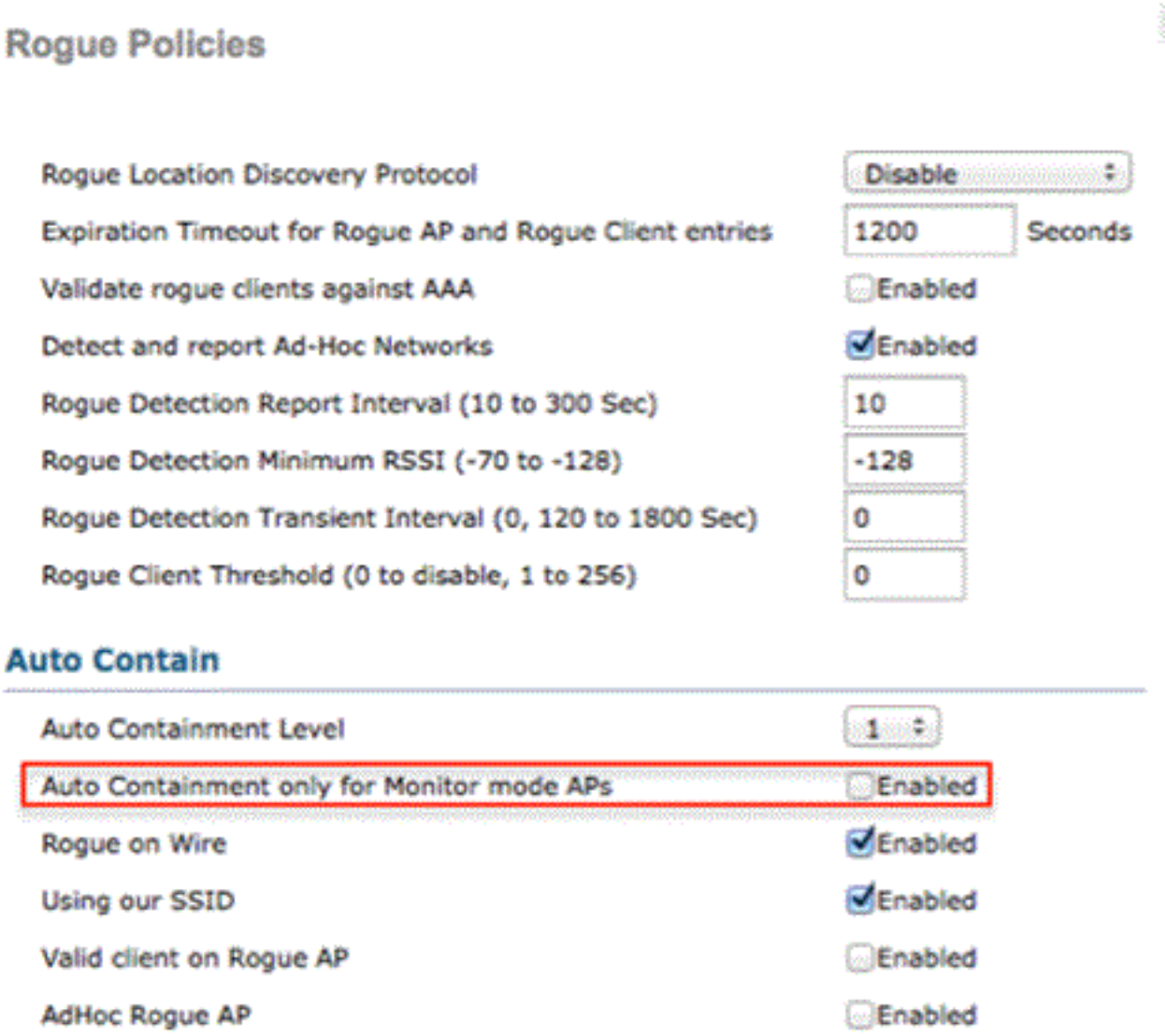


您能验证WSSI模块使用AP控制台检测非法AP。从控制台，请输入**all命令显示capwap rm的歹徒ap d2**。这显示所有恶意AP被看到在WSSI模块无线电。

```
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
```

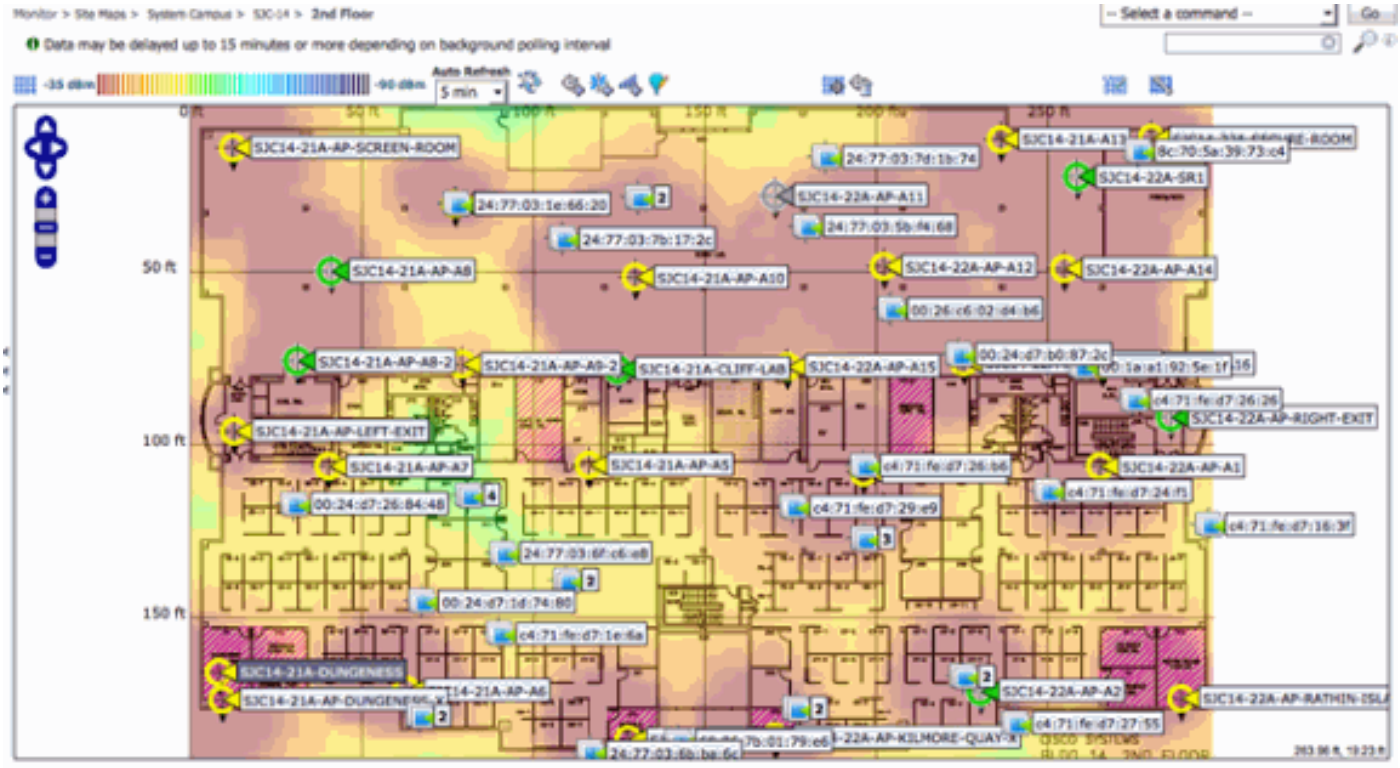
恶意遏制使用WSSI模块

WSSI模块是0x4模块(仅接收天线)，含义歹徒遏制在2.4GHz或5GHz无线电将执行。为了配置WSSI自动地包含恶意AP，您必须保证在安全下的WLC GUI >无线保护策略>欺诈策略>General**自动仅遏制监控模式的AP没有**启用(请参阅下张屏幕画面)。其他复选框可以启用。



WSSI模块的上下文意识位置

当连接与思科MSE， WSSI模块提供上下文意识–与准确性的位置数据和MMAP一样。



WSSI模块许可授权

WSSI模块使用wIPS监控模式许可证。

相关信息

- 技术支持和文档 - Cisco Systems