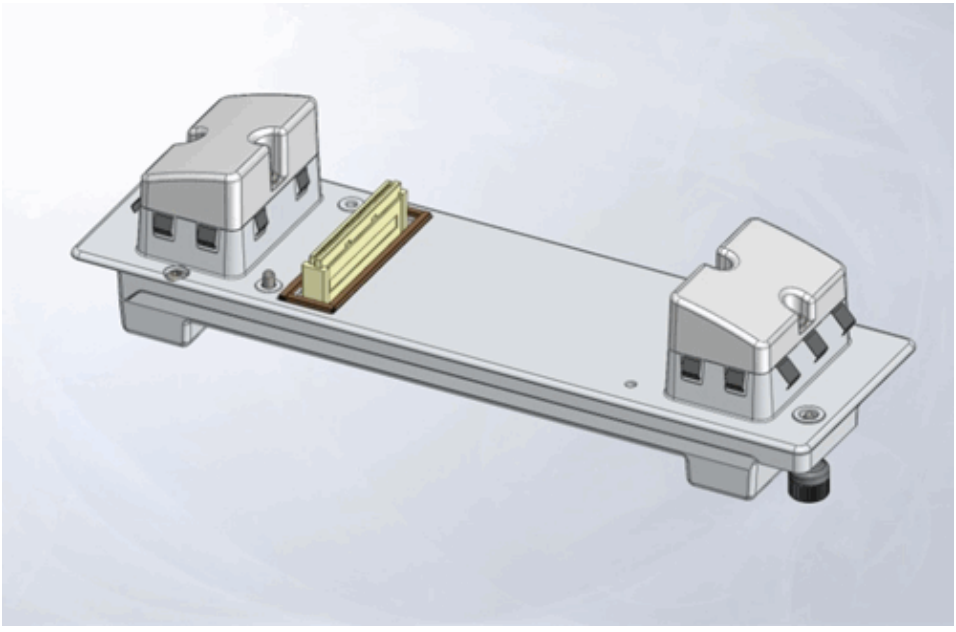
Aironet Access Point Module for Wireless Security and Spectrum Intelligence

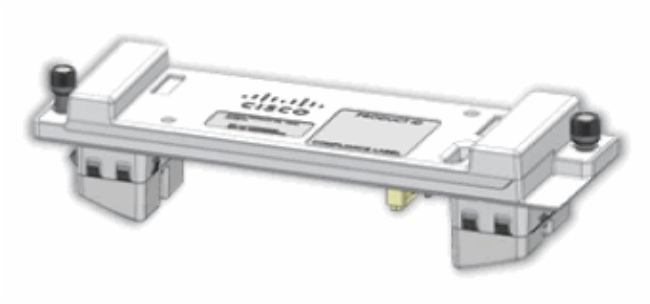
Document ID: 115612

Contents

Introduction

This document provides general configuration and deployment guidelines for the Cisco Aironet Access Point Module for Wireless Security and Spectrum Intelligence (WSSI). The WSSI is an add−on module that can be inserted into modular access points (APs) such as the Cisco 3600 series AP.





Prerequisites

Requirements

There are no specific requirements for this document.

Components Used

The Wireless Security and Spectrum Intelligence module needs the minimum code versions:

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

Conventions

Refer to Cisco Technical Tips Conventions for more information on document conventions.

Product Overview

The Cisco Wireless Security and Spectrum Intelligence module, taking advantage of the flexible modular design of the Cisco Aironet 3600 Series AP, delivers unprecedented, always−on security scanning and spectrum intelligence. This helps you avoid radio frequency (RF) interference so that you get better coverage and performance on your wireless network.

- 24 x 7 full spectrum monitor and mitigation for aWIPS, CleanAir, Context Awareness, Rogue Detection and Radio Resource Management
- 24 x 7 on−channel aWIPS threat protection
- 23 times more security and spectrum coverage
- 30%+ CAPEX cost savings versus dedicated monitor mode AP
- Zero touch configuration

The WSSI field−upgradeable module is a dedicated radio that off−loads all monitoring and security services from the client/data serving radios to the security monitor module. This not only allows for better client performance, but also reduces costs by eliminating the need for dedicated Monitor Mode APs and the Ethernet infrastructure required to connect those devices into their network.

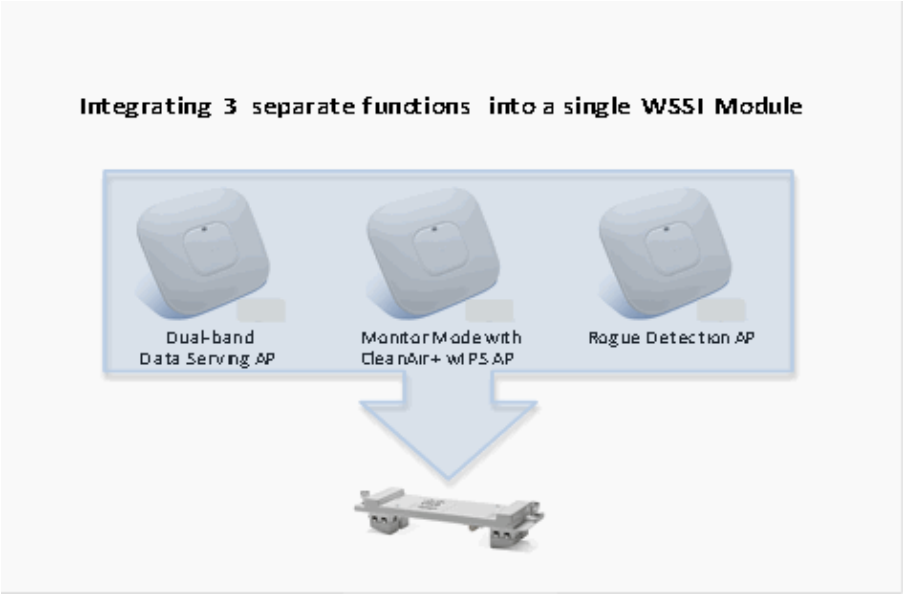
Together, the 3600 Series APs and WSSI module enable you to concurrently provide state−of−the−art security and spectrum analysis functions for Wi−Fi clients on all channels, in both the 2.4−GHz and 5−GHz bands.

Once deployed, the module is constantly scanning all channels to help ensure the most secure and robust wireless experience available in the industry.

Advantages of WSSI Mode

Enhanced Local Mode (ELM):

- Reduces network costs and operations. By integrating the WSSI module into the 3600 series, you can replace up to three separate devices. This provides three separate functions into a single, multi−purpose 3600 Series AP.

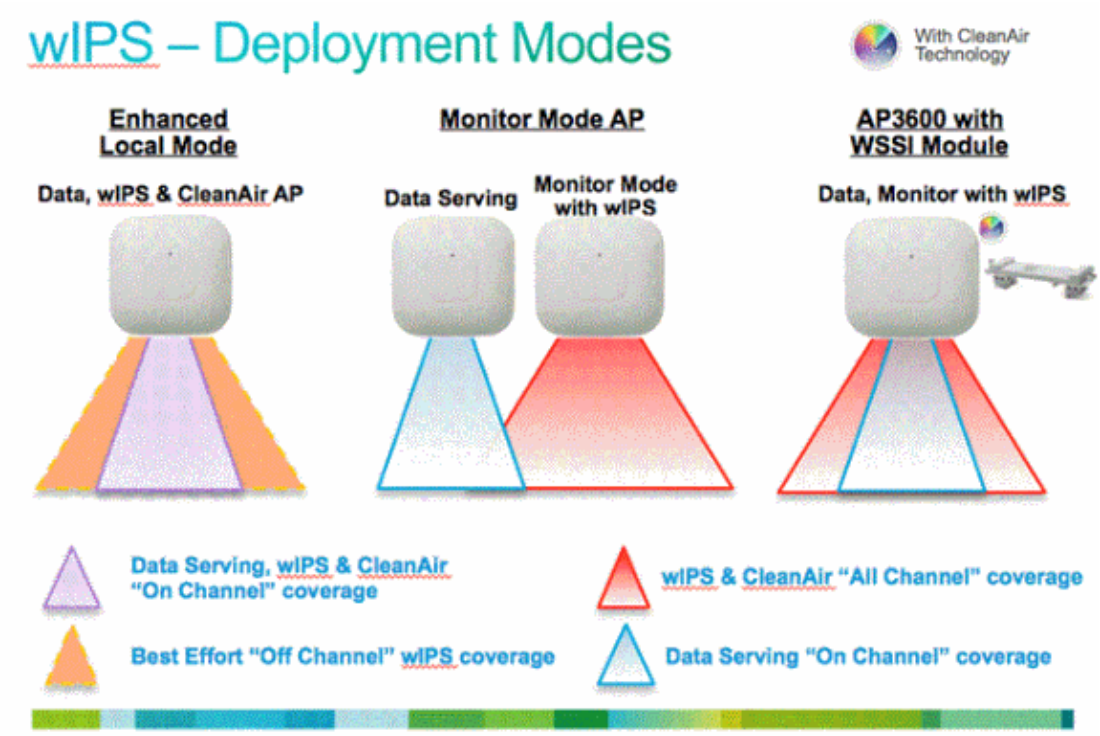


- Customers can now leverage a single Ethernet connection (cable and port) into their wired network, in place of what would typically require up to three separate Ethernet cables and an access port into their wired network. This significantly reduces their CAPEX.
- By integrating all these features to a single AP, customers simplify the day−to−day management and monitoring of their wireless infrastructure and network with a greatly reduced number of APs. The WSSI module appears to the WLC and management systems as an additional radio supporting 802.11b/g/a/n client devices (2.4 and 5 GHz) within the specific 3600 Series AP.
- *Zero Touch Configuration*, Install, Power−up and Go. There is absolutely no configuration required to enable the WSSI Module to be up and running, and immediately monitoring and securing your wireless network. The WSSI module is inserted and secured to any 3600 Series AP. When the AP is

powered back up the module is initialized along with the other radios in the AP and immediately begins monitoring all channels on both 2.4 and 5 GHz for any potential security threats and sources of interference.

- Adaptive wIPS provides accurate and efficient threat detection on all channels from over−the−air attacks, rogue APs, and ad hoc connections, as well as the ability to classify, notify, mitigate and report for constant monitoring and proactive management. Works in conjunction with the Cisco Mobility Services Engine (MSE).

ELM:



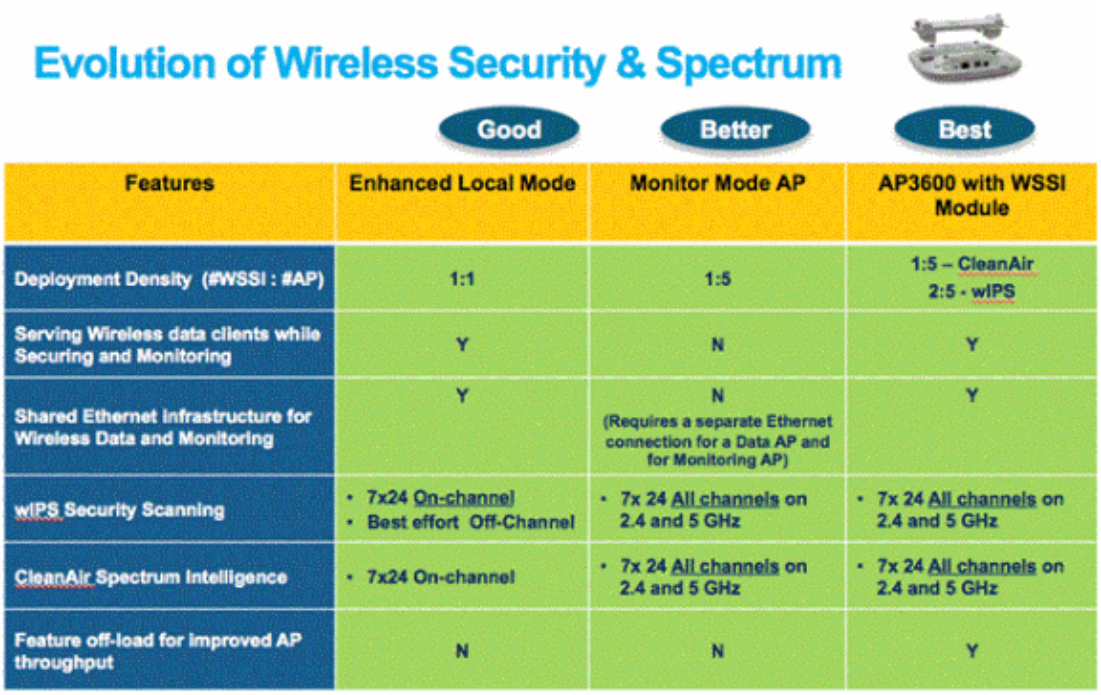
- Adds wIPS security scanning for 7x24 on channel scanning (2.4GHz and 5 GHz), with best effort off channel support.
- The AP is additionally serving clients and with the G2 Series of APs, enables CleanAir spectrum analysis on channels (2.4GHz and 5GHz).

Monitor Mode:

- The Monitor Mode AP (MMAP) is dedicated to operate in Monitor Mode and has the option to add wIPS security scanning of all channels (2.4GHz and 5GHz).
- The G2 Series of APs enables CleanAir spectrum analysis on all channels (2.4GHz and 5GHz).
- MMAPs do not serve clients.

AP3600 with WSSI Module: The Evolution of Wireless Security and Spectrum

- The industry s first AP that facilitates simultaneous client service, wIPS security scanning and spectrum analysis using CleanAir Technology.
- Dedicated 2.4GHz and 5GHz radio with its own antennas that enables 7x24 scanning of all wireless channels in the 2.4GHz and 5GHz bands.
- A single Ethernet infrastructure provides simplified operation with fewer devices to manage and optimized return on investment of the AP3600 wireless infrastructure and the Ethernet wired infrastructure.



- Cisco CleanAir Technology: provides proactive, high−speed spectrum intelligence to combat performance problems due to wireless interference. The industry s first state−of−the−art RF analysis technology that inspects and classifies the energy patterns (signatures) of devices that can significantly impact the quality of a wireless network.
- Radio Resource Management (RRM): simplified, advanced RF management, automatically adapts to the wireless network environment based on the information received from Cisco CleanAir Technology. Once interferers are identified, RRM is able to move client devices to channels away from the interference and adjust the transit power to move away from the source of interference. This provides better RF quality to the user.
- Rogue Detection: detects and reports backdoor network access and access to wireless clients.
- Location and Context awareness: provides real−time awareness and the ability to track wireless endpoint.

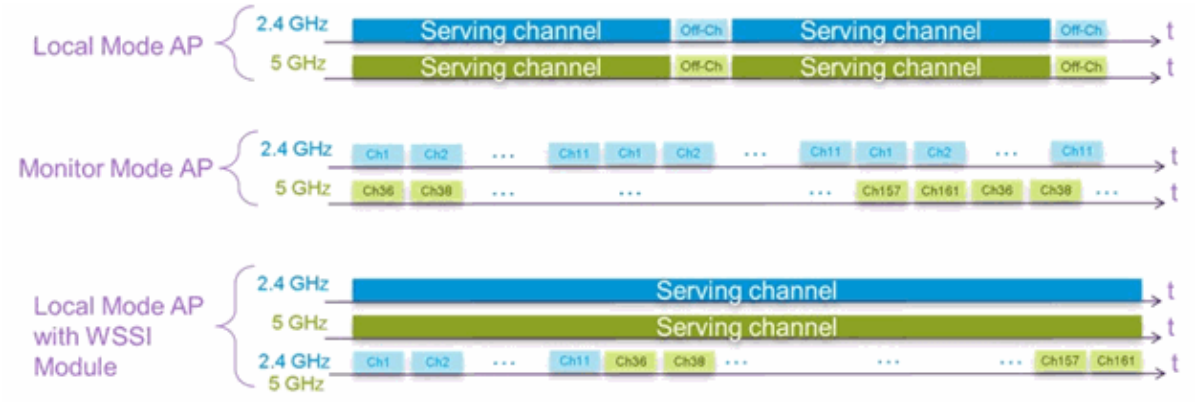
With these features, the Cisco Wireless Security and Spectrum Intelligence module, along with the Cisco 3600 series AP, provides the most secure and robust enterprise class wireless network possible for your corporate users and data.

On−channel vs. Off−channel using the WSSI Module

A local mode AP scans for CleanAir interferers and wIPs attackers on−channel. This means the AP only scans the channel that it is serving. A local mode AP with a 2.4GHz radio serving channel 1 and 5GHz radio serving channel 64, only provides protection on channels 1 and 64.

A MMAP scans for CleanAir interferers and wIPs attackers off−channel. This means the AP scans all channels. The 2.4GHz radio scans all 2.4GHz channels and the 5GHz channel scans all 5GHz channels.

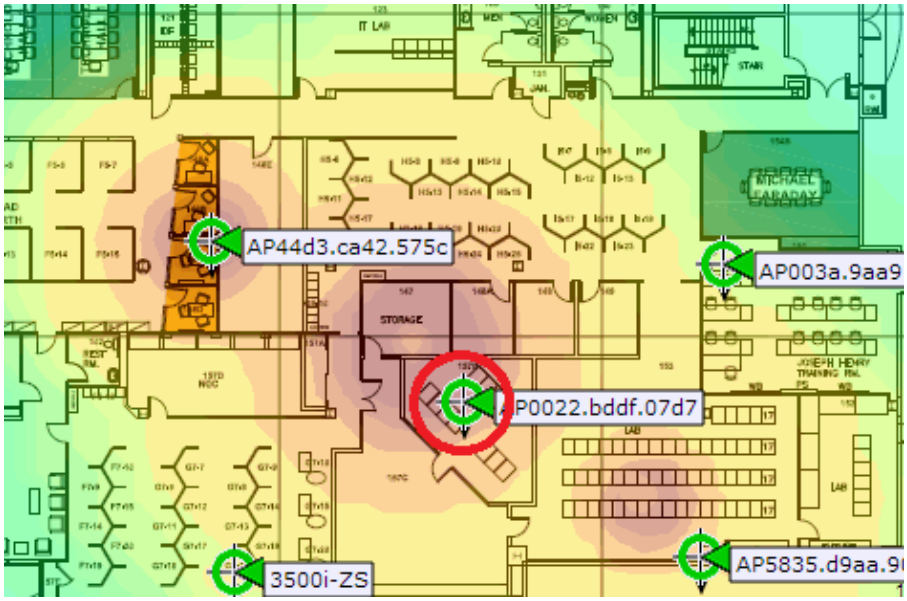
A Cisco 3600 series AP uses a combination of on−channel and off−channel. The 2.4GHz and 5GHz radios scan on−channel and the WSSI module scans off−channel, cycling between all 2.4GHz and 5GHz channels.



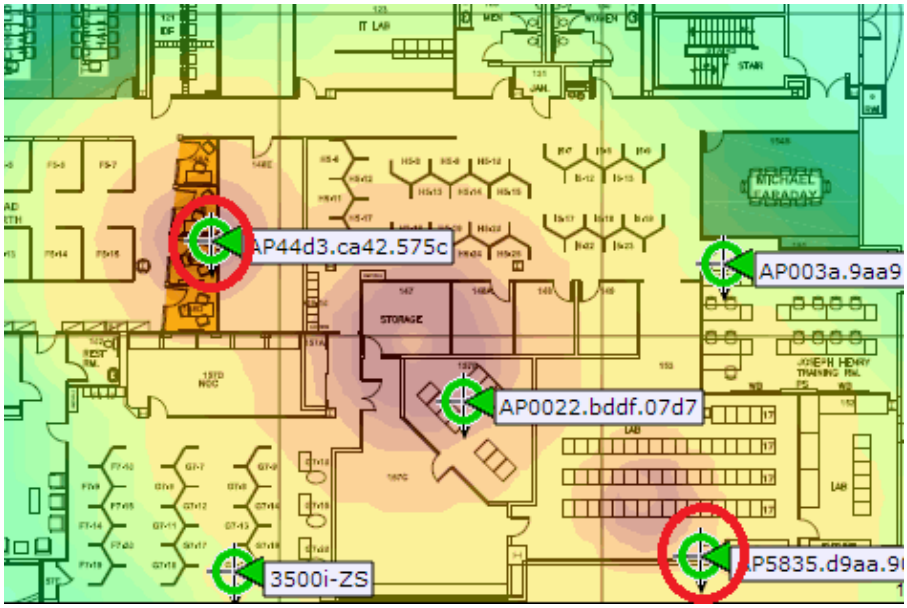
Suggested Deployment Density for the WSSI Module

In traditional Monitor AP deployment, Cisco recommends a ratio of 1 MMAP to every 5 local mode APs. This can vary based on network design and expert guidance for best coverage. With the WSSI module, there are different deployment recommendations based on functionality to achieve coverage parity with a MMAP.

For CleanAir, it is recommended to deploy 1 WSSI module for every 5 local or Flexconnect APs. This 1:5 deployment offers the same performance as a CleanAir enabled MMAP, but still allows the AP to serve clients. This is a recommended deployment for a WSSI module performing CleanAir:



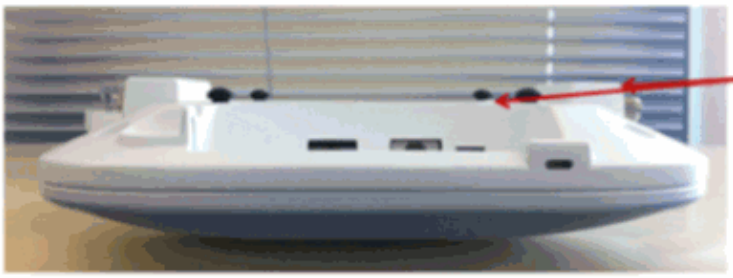
For wIPS protection, it is recommended to deploy 2 WSSI modules for every 5 local or FlexConnect APs. The wIPS detection time for an off−channel attack is about two times that of a MMAP. Therefore, a 2:5 deployment is required to provide wIPS detection parity. This is the recommended deployment for a WSSI module performing wIPS protection:



The Cisco 3600 AP with a WSSI module utilizes both on−channel and off−channel scanning to provide an industry leading solution while serving clients.

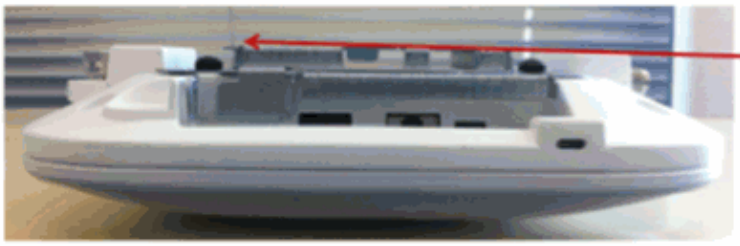
Installing the WSSI Module

AP3600 - WSSI Module



Monitor Module installed can have a slight rise

Bracket-1 would be slightly below rise

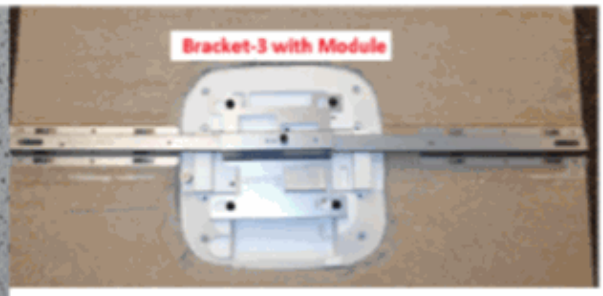


Monitor Module is Flush when Bracket-2 is used

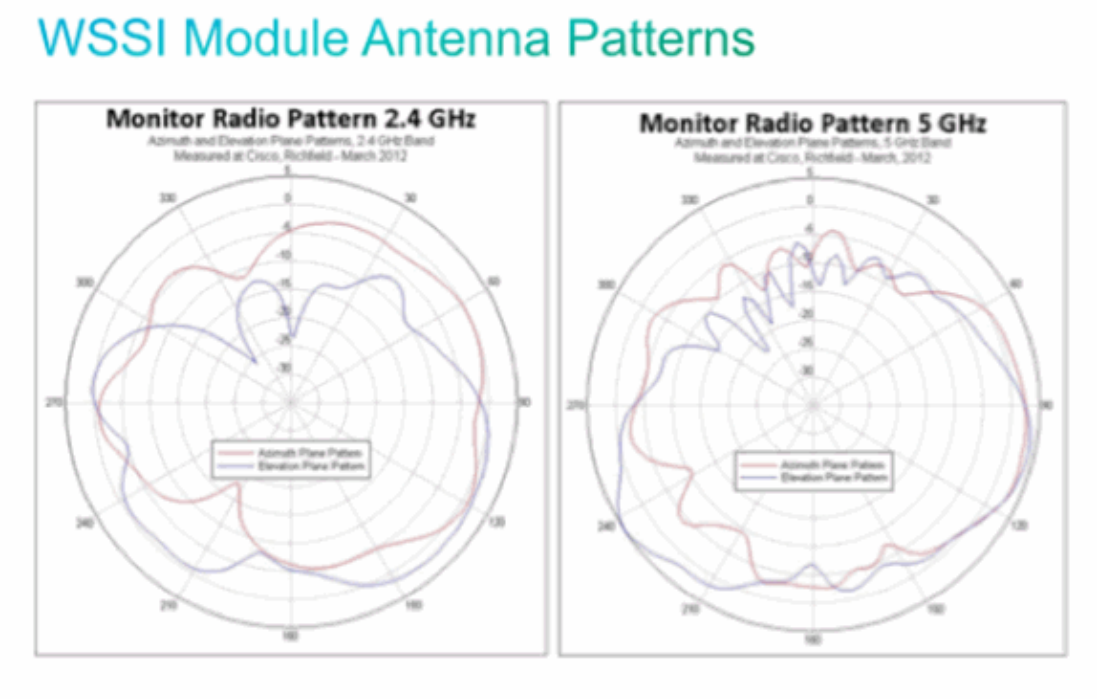
Recommend Customers use Mounting Bracket-2 or Bracket-3
Existing Bracket-1 may work on some ceilings but not on hard surfaces

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



Configuration for the AP3600 WSSI Module

There is no configuration for the WSSI module needed. The module automatically scans all channels on both bands using its 0x4 (receive only) 0 Tx Antennas x 4 Rx Antennas.

Note that the WSSI module is only active on AP3600s configured in either Local Mode or FlexConnect Mode. The WSSI module is disabled in all other modes.

Power Requirement for the WSSI Module

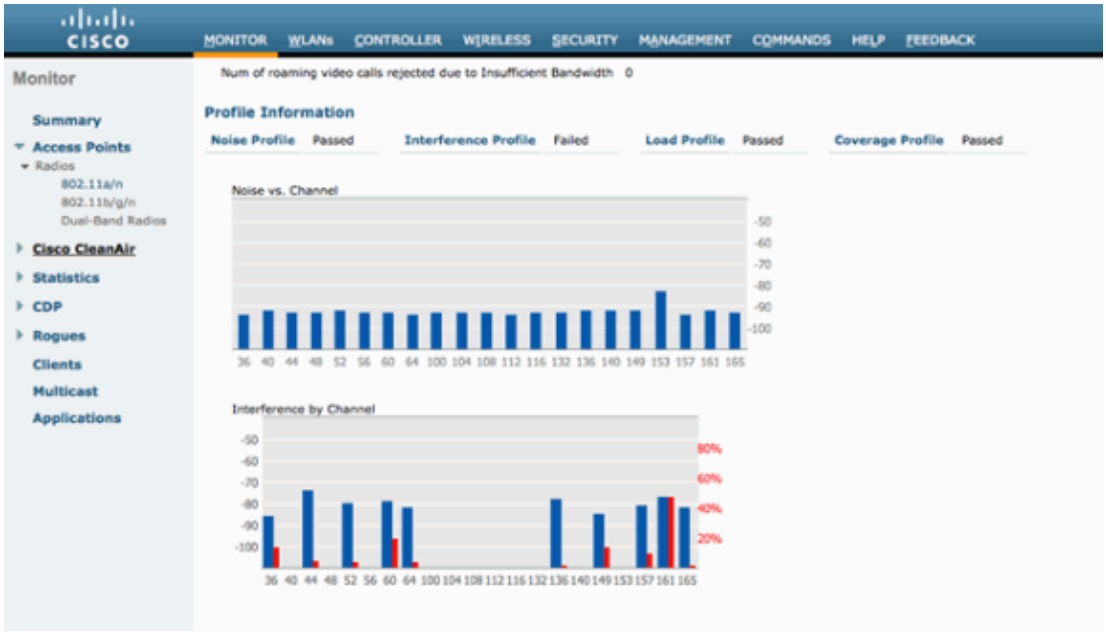
The AP3600 with a WSSI module installed exceeds 15.4 Watts (802.3af). The AP requires either (802.3at − PoE+), Enhanced PoE, a local AC power supply, or the Cisco PoE injector (AIR−PWRINJ4).

Notes:

- Enhanced PoE was created by Cisco and is a forerunner to 802.3at PoE+. It provides up to 20W of power.
- PoE+ can deliver up to 30W of power.

Radio Resource Management on the WSSI Module

The WSSI module takes all RRM measurements on both the 2.4GHz band and 5GHz band. The measurements are displayed in the WLC GUI under either Monitor > Access Points > 802.11a/n > AP_NAME > Details or Monitor > Access Points > 802.11b/g/n > AP_NAME > Details.



CleanAir on the WSSI Module

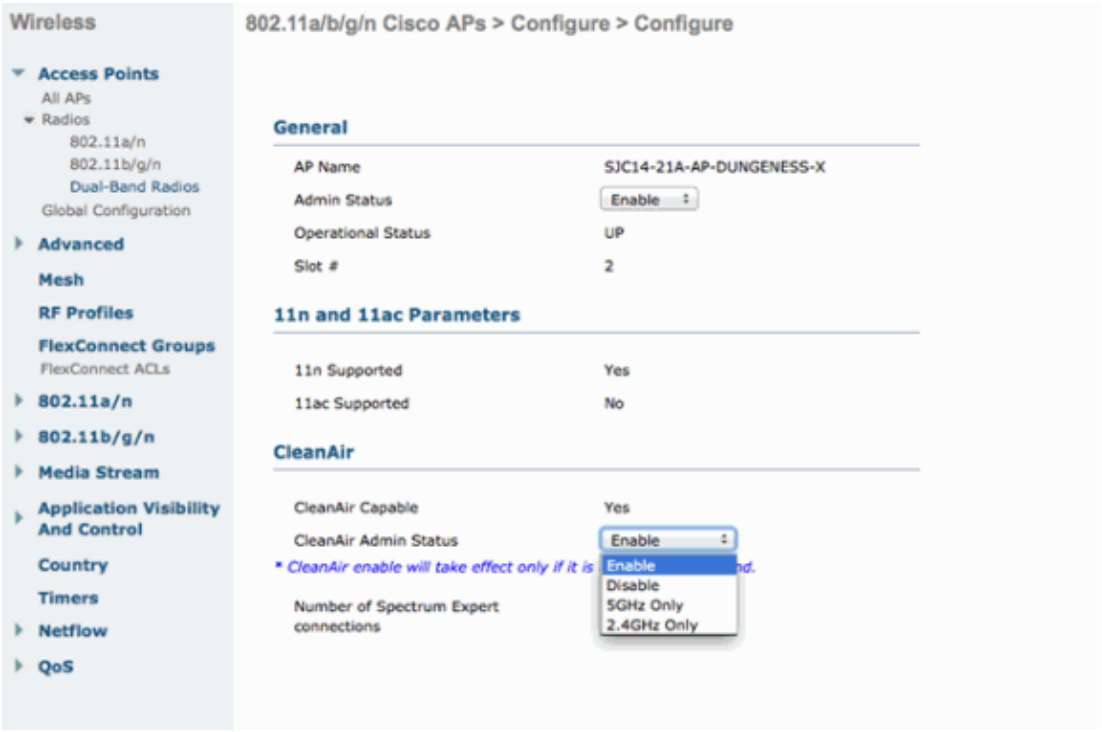
The WSSI module detects CleanAir interferers with the same precision as a MMAP. Cisco recommends that the WSSI module be deployed with a density of 1:5, where there must be 1 WSSI module for every 5 APs. This is the same recommended density as for a MMAP.

When the WSSI module is enabled with no sub−mode, the module scans both the 2.4GHz band and 5GHz band. The module dwells on each channel for 1.2secs and scans for CleanAir interferers.

CleanAir can be enabled on 2.4GHz only, 5GHz only, and both 2.4GHz and 5GHz. This is selectable from either the WLC CLI or GUI. Here is an example of configuring CleanAir on the WLC CLI:

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

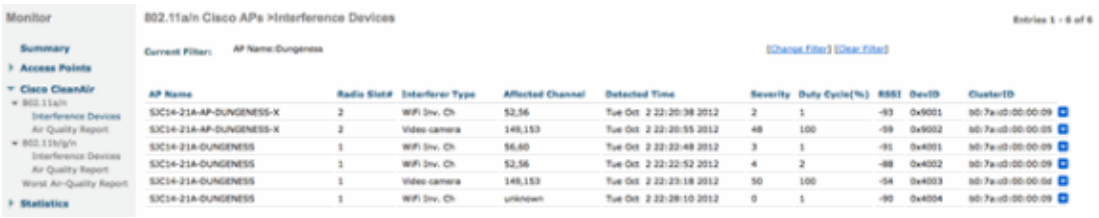
The same configuration can be applied on the GUI via Wireless > Dual−Band Radios > Configure. Here is an example of this:



In order to verify that the CleanAir interferer was detected by the WSSI module, issue the **show cleanair interferers** command from the AP console:

```
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
```

The same configuration can be applied on the GUI via Wireless > Dual−Band Radios > Configure. Here is an example:



The CleanAir interferers are reported at the WLC GUI. Interferers are displayed PER BAND. This means interferers detected on the WSSI module on the 5GHz band are displayed under Monitor > 802.11a/n > Interference Devices.

In order to verify that the CleanAir interferer was detected by the WSSI module, issue the **show cleanair interferers** from the AP console:

```
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
```

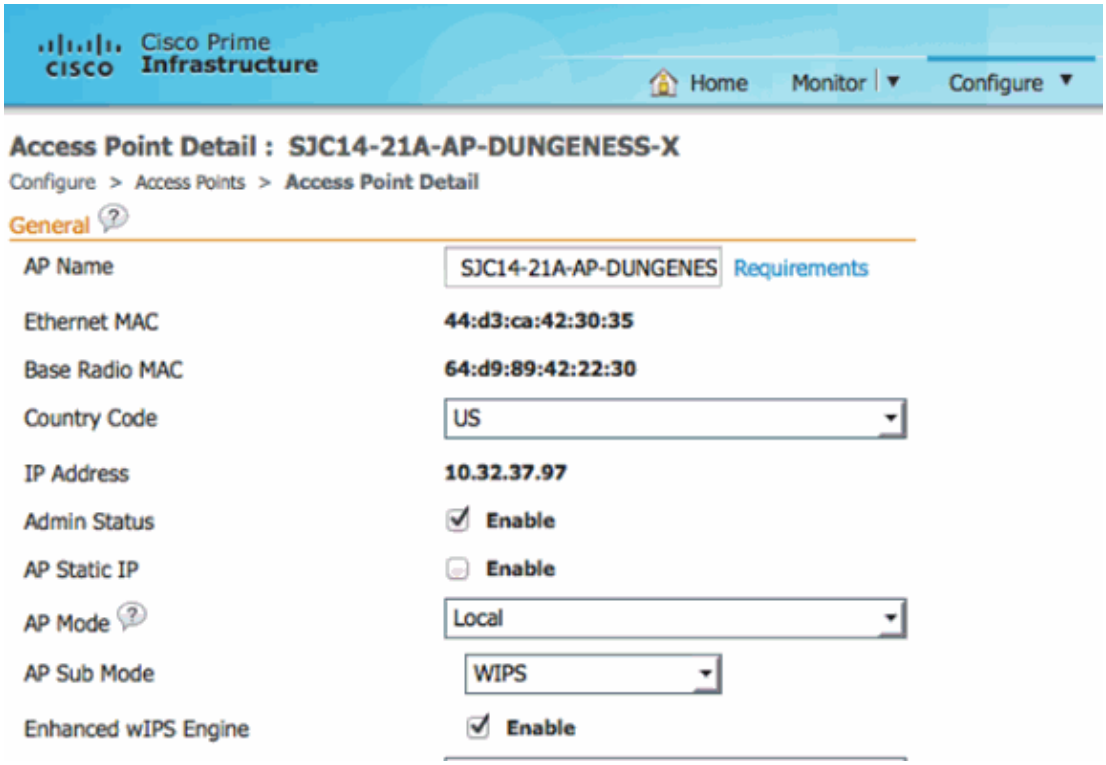
wIPS on the WSSI Module

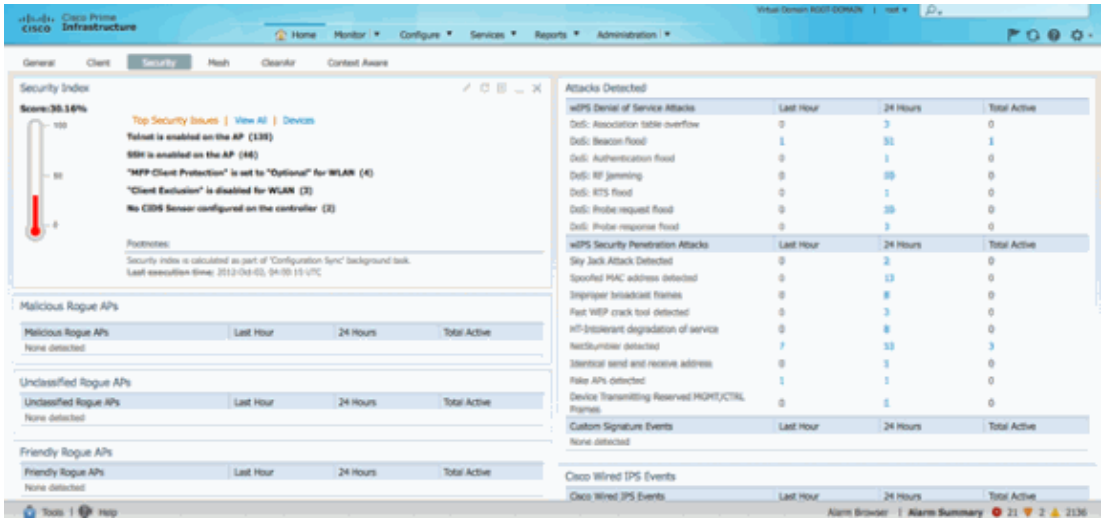
The WSSI module detects wIPS attackers with nearly the same precision as a MMAP. For wIPS, Cisco recommends deploying the WSSI module with a 2:5 ratio among APs. This means for every 5 APs, two of the APs must contain the WSSI module.

There are two wIPS modes that can be configured:

- wIPS submode − Enables wIPS attack detection and scans all channels for 1.2s. This mode allows the AP to still capture all RRM reports in addition to wIPS detections.
- Enhanced wIPS mode − Enable wIPS attack detection and scans all channels for 250ms. The smaller channel dwell time allows the security module to detect attackers quicker.

From the Prime Infrastructure (PI) page, go to Configure > Acesss Points > AP_NAME. The WSSI module can be configured to either wIPS submode or wIPS submode + Enhanced wIPS Engine Support. This can also be pushed as part of an AP configuration template.





The wIPS attacks are displayed at the Prime Infrastructure from the Home > Security tab.

The PI displays a network−level view, but you can display the attack on an AP3600 with a WSSI module by issuing the **show capwap am alarm ALARM_NUM** command from the AP console.

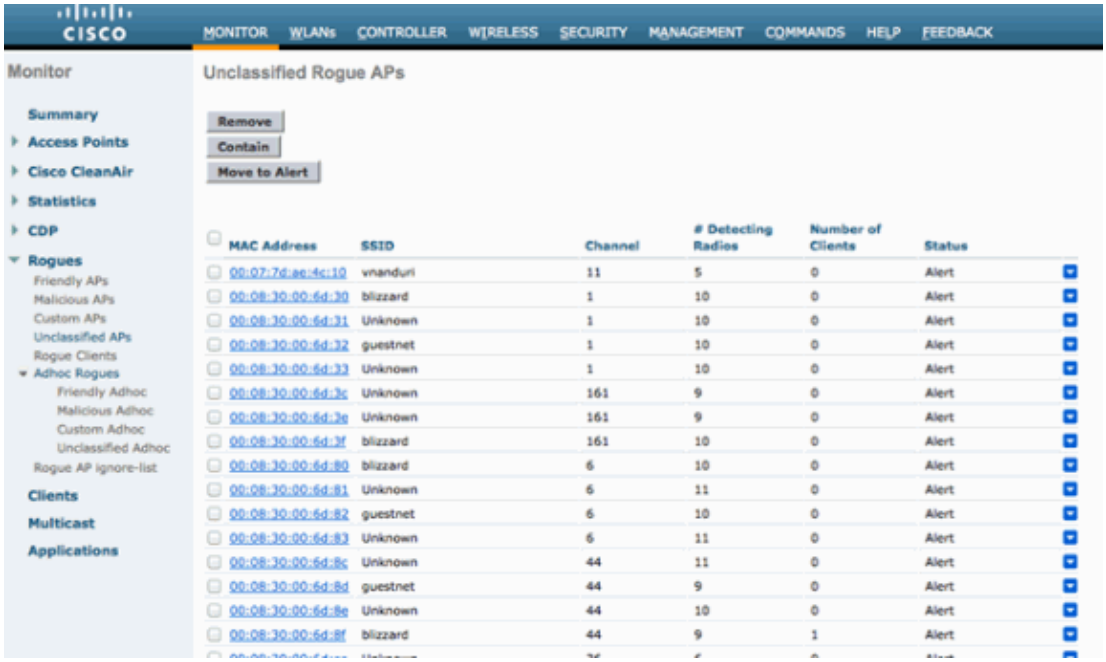
For example, alarm 52 is a Denial of Service, authentication flood. In order to see if that attack was detected on the WSSI module, issue the **show capwap am alarm 52** command:

```
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 on the WSSI Module

The WSSI module detects rogue APs with the same precision as a MMAP. A list of rogue APs is displayed in both the WLC and PI.

This is the list of Unclassified Rogue APs from the WLC GUI. Rogue APs can be viewed in the WLC GUI under Monitor > Rogues.



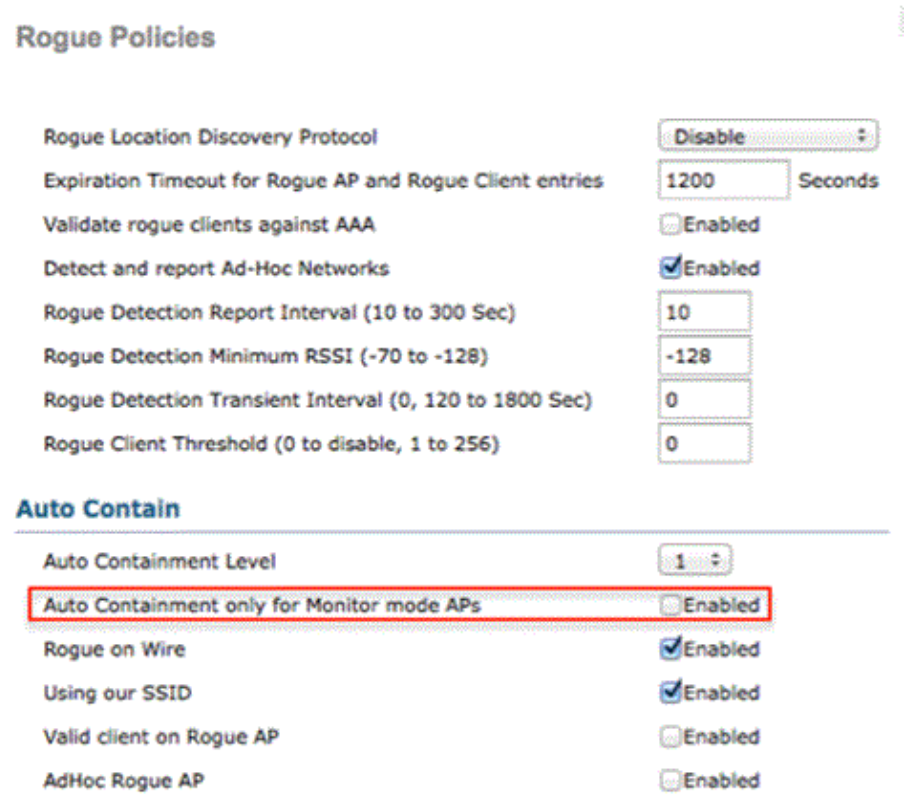
You can verify that the WSSI module using the AP console detected a Rogue AP. From the console, enter the **show capwap rm rogue ap d2 all** command. This displays all Rogue APs seen at the WSSI Module Radio.

```
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
```

Rogue Containment using the WSSI Module

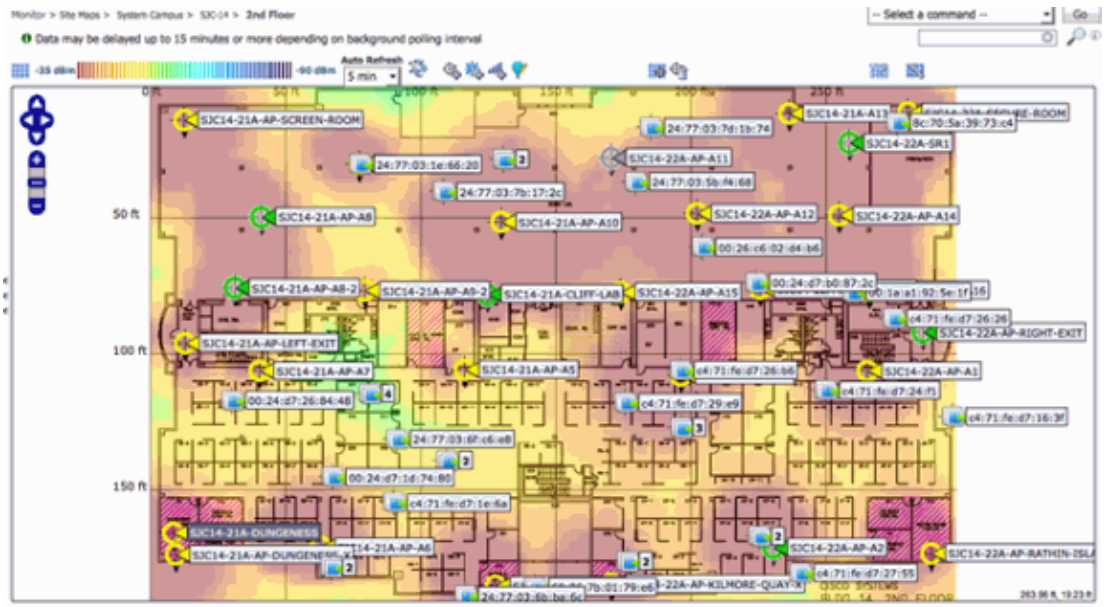
The WSSI module is a 0x4 module (receive antennas only), meaning that rogue containment will be performed on the 2.4GHz or 5GHz radio. In order to configure the WSSI to automatically contain rogue APs, you must ensure that in the WLC GUI under Security > Wireless Protection Policies > Rogue Policies > General that **Auto Containment only for Monitor mode APs** is not enabled (see the next screenshot). All

other check−boxes can be enabled.



Context Aware−Location on the WSSI Module

When connected with a Cisco MSE, the WSSI module provides Context Aware Location data with the same accuracy as a MMAP.



WSSI Module Licensing

The WSSI module uses wIPS monitor mode licenses.

Related Information

- **Technical Support & Documentation − Cisco Systems**

Updated: Jan 15, 2013 Document ID: 115612