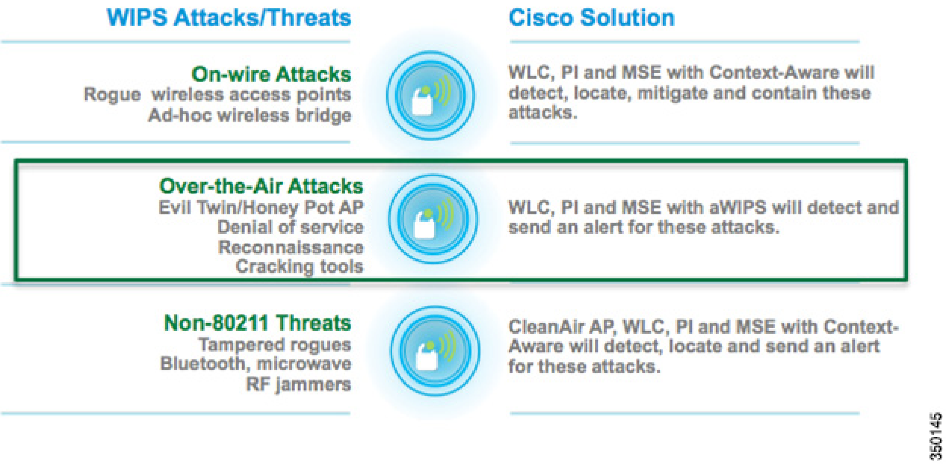
Cisco Adaptive wIPS Deployment Guide, Cisco Unified Wireless Network Version 7.4

First Published: Month Day, Year-<required>
Last Updated: Month Day, Year-<optional, only required when a document is revised>

Cisco wIPS Solution Overview

Cisco wIPS solution offers flexible and scalable, 24x7x365-based full time wireless security solution to meet each customer's needs. This document will cover the wIPS security solutions that are provided as part of Cisco Unified Wireless Solution. Depending on your deployment, there is a solution to meet your security needs, starting with the base Wireless LAN Controller (WLC), followed by the WLC and MSE, and finally the WLC, MSE, and CleanAir enabled access points. These three solutions are compared below.



WIPS Attacks/Threats	Cisco Solution
On-wire Attacks Rogue wireless access points Ad-hoc wireless bridge	WLC, PI and MSE with Context-Aware will detect, locate, mitigate and contain these attacks.
Over-the-Air Attacks Evil Twin/Honey Pot AP Denial of service Reconnaissance Cracking tools	WLC, PI and MSE with aWIPS will detect and send an alert for these attacks.
Non-80211 Threats Tampered rogues Bluetooth, microwave RF jammers	CleanAir AP, WLC, PI and MSE with Context-Aware will detect, locate and send an alert for these attacks.

Cisco Systems, Inc.
www.cisco.com

On-wire Attacks

An Access Point in wIPS-optimized mode will perform rogue threat assessment and mitigation using the same logic as current Cisco Unified Wireless Network implementations. This allows a wIPS access point to scan, detect and contain rogue access points and ad-hoc networks. Once discovered, this information regarding rogue wireless devices is reported to PI where rogue alarm aggregation takes place. However, with this functionality comes the caveat that if a containment attack is launched using a wIPS mode access point, its ability to perform methodical attack-focused channel scanning is interrupted for the duration of the containment.

Feature	BaseWIPS (WLC)	Adaptive WIPS (WLC and MSE)	Adaptive WIPS (WLC, MSE, and CleanAir Access Points)
Rogue access point and ad hoc rogue detection, classification, location tracking, and containment	Yes	Yes	Yes
Rogue access point switch port tracing and disabling	Yes	Yes	Yes
Management frame impersonation detection	Yes	Yes	Yes
Rogue containment when WAN is down	Yes	Yes	Yes
Internal and external rogue access point detection and containment times	Yes	Yes	Yes

Over-the-Air Attacks

Cisco Adaptive Wireless IPS embeds complete wireless threat detection and mitigation into the wireless network infrastructure to deliver the industry’s most comprehensive, accurate and operationally cost-effective wireless security solution. Below are the Over-the-Air attacks that are detected by the Cisco Adaptive wIPS solution.

Feature	BaseWIPS (WLC)	Adaptive WIPS (WLC and MSE)	Adaptive WIPS (WLC, MSE, and CleanAir Access Points)
Smartphone tethering detection and containment	Yes	Yes	Yes
Location tracking and containment for DoS attacker and non-authorized device that is trying to associate internal access point	Yes	Yes	Yes

Feature	BaseWIPS (WLC)	Adaptive WIPS (WLC and MSE)	Adaptive WIPS (WLC, MSE, and CleanAir Access Points)
Wired Equivalent Privacy (WEP) cracking detection	Yes	Yes	Yes
MAC spoofing rogue's detection and containment	Yes	Yes	Yes
Auto MAC learning	Yes	Yes	Yes
Internet connection sharing (ICS) detection	Yes	Yes	Yes
Enterprise-level alarm/event correlation	Yes	Yes	Yes
Attack signature threshold customization	Yes	Yes	Yes
Off-channel rogue detection and location, integrated into infrastructure	Yes	Yes	Yes
DoS signature updates	No	Yes	Yes
Wireless intrusion signature updates	No	Yes	Yes
Attack forensics (all signatures)	No	Yes	Yes

Non-802.11 Threats

Cisco CleanAir® technology is an effective tool to monitor and manage your network's RF conditions. The Cisco MSE extends those capabilities. The figure below shows the advantages of deploying CleanAir enable Access points with a Cisco Adaptive wIPS solution.

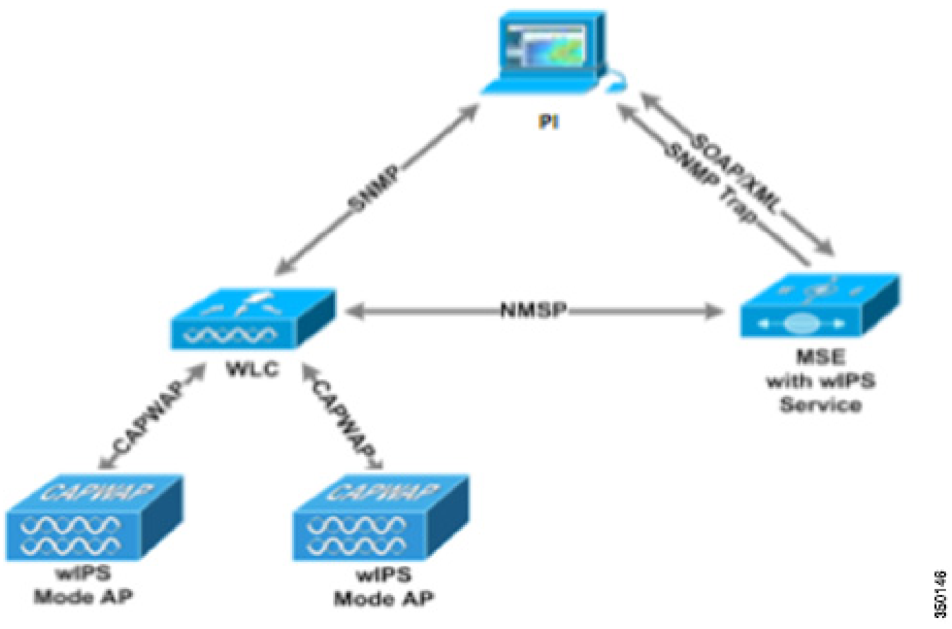
Feature	BaseWIPS (WLC)	Adaptive WIPS (WLC and MSE)	Adaptive WIPS (WLC, MSE, and CleanAir Access Points)
Non-Wi-Fi transmitter detection and location	No	No	Yes
Non-Wi-Fi bridge detection and location	No	No	Yes
Non-Wi-Fi access point detection and location	No	No	Yes
Layer 1 DoS attack location and detection	No	No	Yes

Cisco Adaptive wIPS Introduction

While the complete Cisco wIPS solution is included in the introduction, this document will focus on all aspects of the Over-the-Air wIPS detection. This document will go into detail on:

- Adaptive wIPS components / architecture
- The wIPS deployment modes
- Off-channel vs. On-channel wIPS scanning
- wIPS communication protocols
- wIPS Configuration and Profile Management
- wIPS Alarm Flow
- Deployment Considerations
- Forensics
- Licensing and Support
- A Step by Step Configuration Guide

Cisco Adaptive wIPS System Architecture



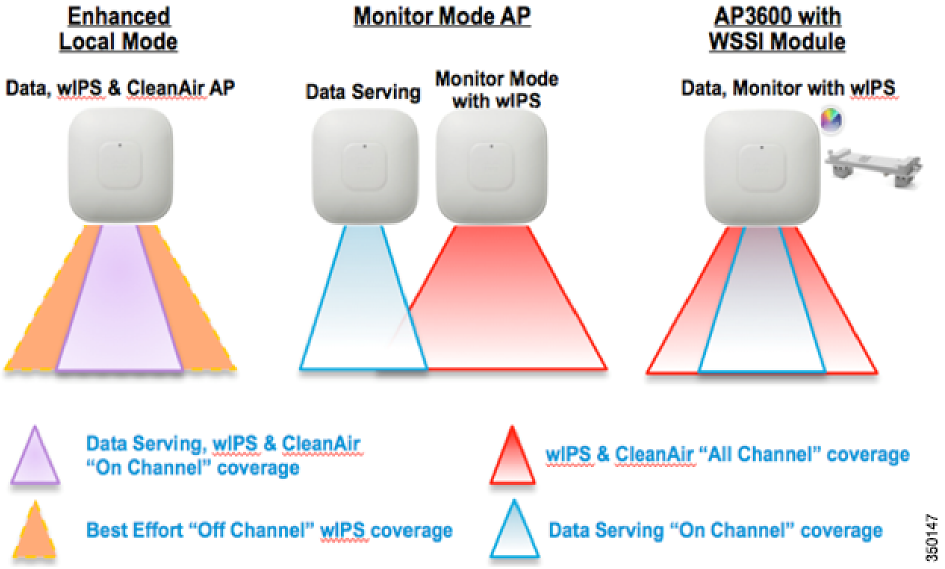
This document will address the wIPS solution for Over-the-Air Attacks. Cisco's Adaptive Wireless Intrusion Prevention System (wIPS) is made up of a number of components that work together to provide a unified security monitoring solution. In addition to the WLAN Controllers, Access Points and Prime Infrastructure components that currently comprise Cisco's Unified Wireless Networking solution; the wIPS portion introduces two additional components. These additional hardware components include Access Points in wIPS mode and the Mobility Services Engine running the wIPS service software.

Component Functions in an Adaptive Wireless IPS Deployment

- wIPS Mode Access Point – A wIPS mode access point is any access point in Monitor Mode, Enhanced Local Mode, or with the WSSI module.   This term will be used to group access points capable of wIPS.
- wIPS Monitor Mode Access Point(s) – Provides constant channel scanning with attack detection and forensics (packet capture) capabilities.
- Local Mode Access Point(s) – Provides wireless service to clients in addition to limited time-sliced attacker scanning.
- Enhanced Local Mode Access Point(s) – Like Local Mode, provides wireless service to client, but when scanning off-channel, the radio dwells on the channel for an extended period of time, allowing enhanced attack detection
- Wireless Security and Spectrum Intelligence (WSSI) Module – This is an add-on module to the Cisco Aironet 3600 Series Access Point, which offloads the constant channel scanning with attack detection and forensics capabilities to the module, freeing up the serving radios for clients
- Mobility Services Engine (running wIPS Service) – The central point of alarm aggregation from all controllers and their respective wIPS Monitor Mode Access Points. Alarm information and forensic files are stored on the system for archival purposes.
- Wireless LAN Controller(s) – Forwards attack information from wIPS Monitor Mode Access Points to the MSE and distributes configuration parameters to APs.
- Prime Infrastructure – Provides the administrator the means to configure the wIPS Service on the MSE, push wIPS configurations to the controller and set Access Points into wIPS Monitor mode. It is also used for viewing wIPS alarms, forensics, reporting and accessing the attack encyclopedia.

wIPS Deployment Modes

Beginning with the 7.4 release, Cisco Adaptive Wireless IPS has three options for wIPS mode access points. To better understand the differences between the wIPS mode access points, lets discuss each mode.


Enhanced Local Mode
Monitor Mode AP
AP3600 with WSSI Module
Data, wIPS & CleanAir AP
Data Serving
Monitor Mode with wIPS
Data, Monitor with wIPS
Data Serving, wIPS & CleanAir "On Channel" coverage
wIPS & CleanAir "All Channel" coverage
Best Effort "Off Channel" wIPS coverage
Data Serving "On Channel" coverage
350147

Enhanced Local Mode (ELM)

Enhanced local mode (ELM) provides wIPS detection “on-channel”, which means attackers will be detected on the channel that is serving clients. For all other channels, ELM provides best effort wIPS detection. This means that every frame the radio would go “off-channel” for a short period of time. While “off-channel”, if an attack occurs while that channel is scanned, the attack will be detected.

An example of enhanced local mode on an AP3600, the 2.4GHz radio is operating on channel 6. The AP will constantly monitor channel 6, any attacks on channel 6 will be detected and reported. If an attacker attacks channel 11, while the AP is scanning channel 11 “off-channel”, the attack will be detected.

The features of ELM are:

- Adds wIPS security scanning for 7x24 on channel scanning (2.4GHz and 5 GHz), with best effort off channel support
- The access point is additionally serving clients and with the G2 Series of Access Points enables CleanAir spectrum analysis on channel (2.4GHz and 5GHz)
- Adaptive wIPS scanning in data serving local and flexconnect APs
- Protection without requiring a separate overlay network
- Supports PCI compliance for the wireless LANs
- Full 802.11 and non-802.11 attack detection
- Adds forensics and reporting capabilities
- Flexibility to set integrated or dedicated MM APs
- Pre-processing at APs minimize data backhaul (that is, works over very low bandwidth links)
- Low impact on the serving data

Monitor Mode

Monitor Mode provides wIPS detection “off-channel”, which means the access point will dwell on each channel for an extend period of time, this allows the AP to detect attacks on all channels. The 2.4GHz radio will scan all 2.4GHz channels, while the 5GHz channel scans all 5GHz channels. An additional access point would need to be installed for client access.

Some of the features of Monitor Mode are:

- The Monitor Mode Access Point (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 Access Points enable 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

A Cisco 3600 series Access point with the WSSI module uses a combination of “on-channel” and “off-channel”. This means that the AP3600 2.4GHz and 5GHz will scan the channel that they are serving clients and the WSSI module would operate in monitor mode and scan all channels.

Some of the features of the WSSI Module are:

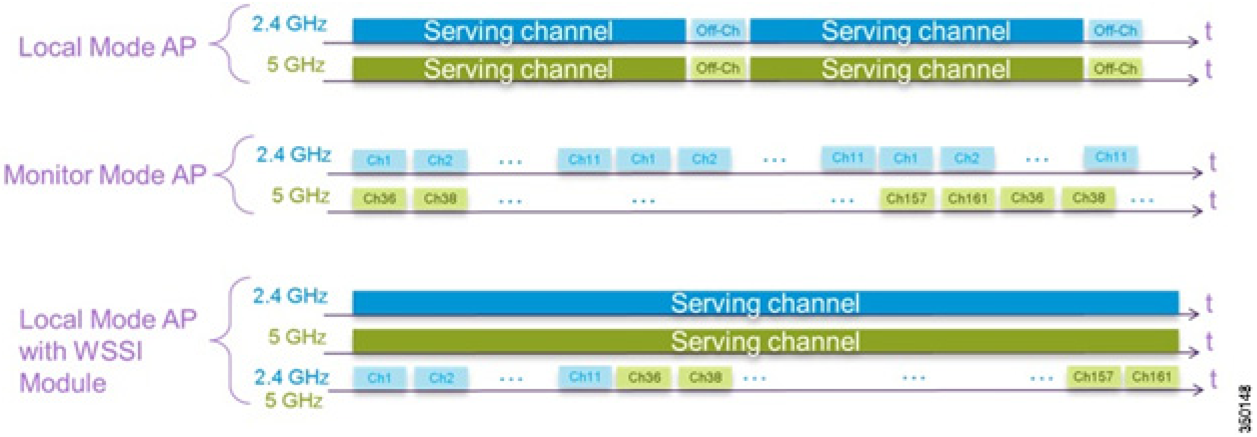
- The industry’s first Access Point enabling the ability to simultaneously “Serve clients, wIPS security scan and analyze the spectrum using CleanAir Technology”

- Dedicated 2.4GHz and 5GHz radio with its own antennas enabling 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

On-Channel vs. Off-Channel Scanning per wIPS Mode

The figure below explains the radio's behavior. When a radio is on its serving channel it is considered "on-channel", when the radio is scanning other channels, it is considered "off-channel".

An AP in local mode is mostly "on-channel", making it difficult to detect attackers "off-channel". A monitor mode AP is always "off-channel", but cannot server clients, the WSSI module provides a great combination of both.



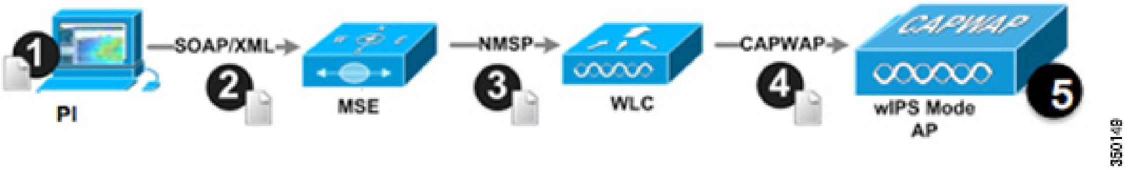
wIPS Communication Protocols

To provide communication between each system component, a number of protocols are utilized:

- CAPWAP (Control and Provisioning of Wireless Access Points) – This protocol is utilized for communication between Access Points and controllers. It provides a bi-directional tunnel in which alarm information is shuttled to the controller and configuration information is pushed to the Access Point. CAPWAP control messages are DTLS encrypted and CAPWAP data has the option to be DTLS encrypted
- NMSP (Network Mobility Services Protocol) – The protocol used for communication between Wireless LAN Controllers and the Mobility Services Engine. In the case of a wIPS Deployment, this protocol provides a pathway for alarm information to be aggregated from controllers to the MSE and for wIPS configuration information to be pushed to the controller. This protocol is encrypted.
  - Controller TCP Port: 16113
- SOAP/XML (Simple Object Access Protocol) - The method of communication between the MSE and PI. This protocol is used to distribute configuration parameters to the wIPS service running on the MSE.
  - oMSE TCP Port: 443
- SNMP (Simple Network Management Protocol) – This protocol is used to forward wIPS alarm information from the Mobility Services Engine to the Prime Infrastructure. It is also utilized to communicate rogue access point information from the Wireless LAN Controller to the Prime Infrastructure.

wIPS Configuration and Profile Management

Configuration of wIPS Profiles follows a chained hierarchy starting with PI, which is used for profile viewing and modification. The actual profiles are stored within the wIPS service running on the MSE. From the wIPS Service on the MSE, profiles are propagated to specific controllers, which in turn communicate this profile transparently to wIPS Mode Access Points associated to that perspective controller. When a configuration change to a wIPS profile is made at PI and applied to a set of Mobility Services Engine(s) and Controller(s), the following steps occur to put the change in place:



1. The configuration profile is modified on PI and versioning information is updated.
2. An XML-based profile is pushed to the wIPS Engine running on the MSE. This update occurs via the SOAP/XML protocol.
3. The wIPS Engine on the MSE will update each controller associated with that profile by pushing out the configuration profile via NMSP.

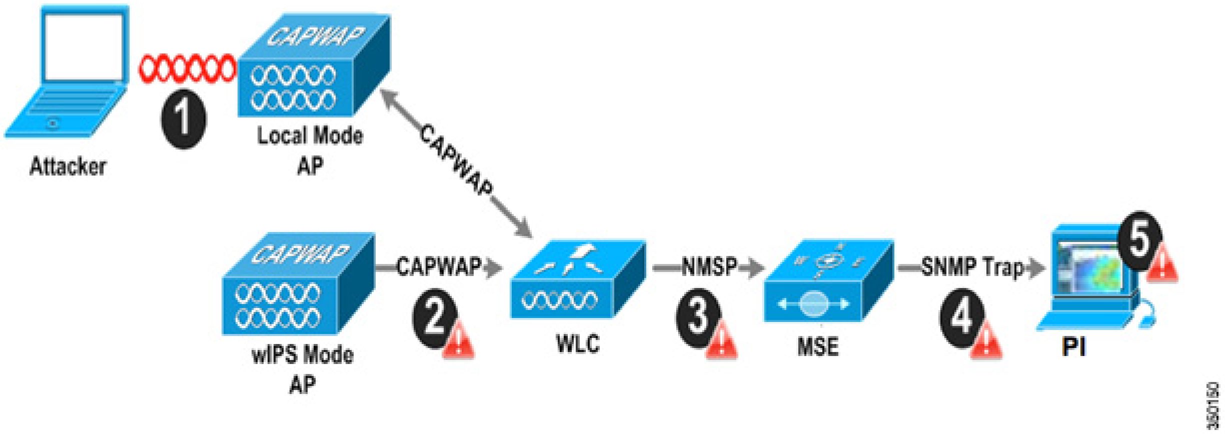
Note A controller is associated to a single configuration profile, which will be utilized for all wIPS mode Access Points joined to that controller. As such, all wIPS Mode APs connected to a controller will share the same wIPS configuration.

4. The Wireless LAN Controller receives the updated wIPS profile, stores it into NVRAM (replacing any previous revision of the profile) and propagates the updated profile to its associated wIPS Access Points via CAPWAP control messages.
5. A wIPS Mode Access Point receives the updated profile from the controller and applies the modifications to its wIPS software engine.

It should be noted that a Mobility Services Engine can only be configured from one Prime Infrastructure. This is essentially a 1:1 relationship meaning that a Mobility Services Engine, once associated to a particular PI, cannot be added to another PI.

wIPS Alarm Flow

The Adaptive wIPS system follows a linear chain of communication to propagate attack information obtained from scanning the airwaves to the console of the Prime Infrastructure.



1. In order for an alarm to be triggered on the Cisco Adaptive wIPS system, an attack must be launched against a legitimate Access Point or Client. Legitimate Access Points and clients are discovered automatically in a Cisco Unified Wireless Network by 'trusting' devices broadcasting the same 'RF-Group' name. In this configuration, the system dynamically maintains a list of local-mode Access Points and their associated clients. The system can also be configured to 'trust' devices by SSID using the SSID Groups feature. Only attacks, which are considered harmful to the WLAN infrastructure, are propagated upwards to the rest of the system.
2. Once an attack has been identified by the wIPS Mode Access Point engine, an alarm update is sent to the Wireless LAN Controller and is encapsulated inside the CAPWAP control tunnel.
3. The Wireless LAN Controller will transparently forward the alarm update from the Access Point to the wIPS Service running on the Mobility Services Engine. The protocol used for this communication is NMSP.

4. Once received by the wIPS Service on the Mobility Services Engine, the alarm update will be added to the alarm database for archival and attack tracking. An SNMP trap is forwarded to the Prime Infrastructure containing the attack information. If multiple alarm updates are received referencing the same attack (for example, if multiple Access Points hear the same attack) only one SNMP trap will be sent to PI.
5. The SNMP trap containing the alarm information is received and displayed by PI.

Deployment Considerations:

Required Components

The basic system components for a Cisco Adaptive wIPS system include:

- Access Points in wIPS Monitor Mode, in enhanced local mode, or with a wireless security and spectrum intelligence module
- Wireless LAN Controller(s)
- A Mobility Services Engine running the wIPS Service
- A Prime Infrastructure

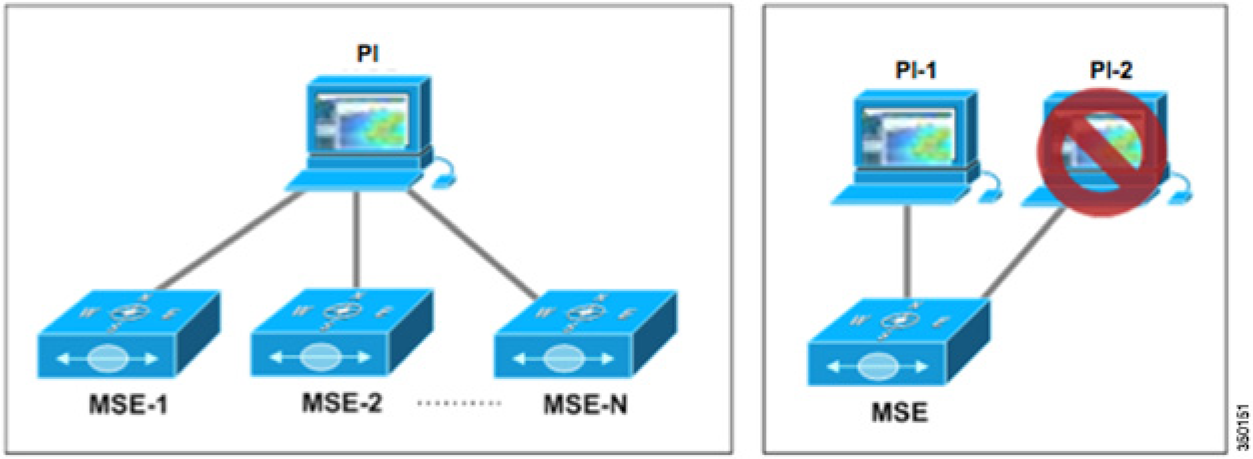
The minimum code versions required for an Adaptive wIPS system:

- Available with Cisco Mobility Services Engine Software Release 5.2.xxx or later
- Requires 5.2.xxx or later on Cisco Wireless Control System
- Requires 5.2.xxx or later on Cisco wireless LAN controllers
- Release 5.2 and later wireless IPS functionality requires Monitor Mode (that is, non-client-serving) access points
- Release 7.1.xxx and later wireless IPS functionality requires Enhanced Local Mode (that is, client-serving) access points

The minimum code versions required for the Wireless Security and Spectrum Intelligence Module:

- Wireless LAN Controller(s) – Version 7.4.XX or greater
- Cisco Prime Infrastructure– Version 1.3.XX or greater
- Mobility Services Engine – Version 7.4.XX or greater

System Scalability



A Mobility Services Engine can be managed only by one Prime Infrastructure, which has design implications when scaling the network. It is possible to have multiple Mobility Services Engines managed by a single Prime Infrastructure.

Use the following scalability facts when designing a system:

- PI can support a maximum of 15,000 Access Points on a high-end server. This limit of 15,000 includes both client-serving Access Points and Access Points in wIPS Monitor Mode. wIPS and Data APs can be intermixed at a variety of ratios to reach the upper limit of 15000 Access Points per PI. These ratios are dependent on environmental RF conditions, density of the existing WLAN installation and the required level of security monitoring.
- Each wIPS mode has a different recommended deployment density. For Enhanced local mode, we recommend a density of 1:1, meaning that every AP should be in enhanced local mode. For Monitor Mode APs we recommend a density of 1:5 and for the AP3600 with the WSSI module, we recommend 2:5. This is shown in the table below.

Recommendations to support 15K Access Points in Various wIPS modes

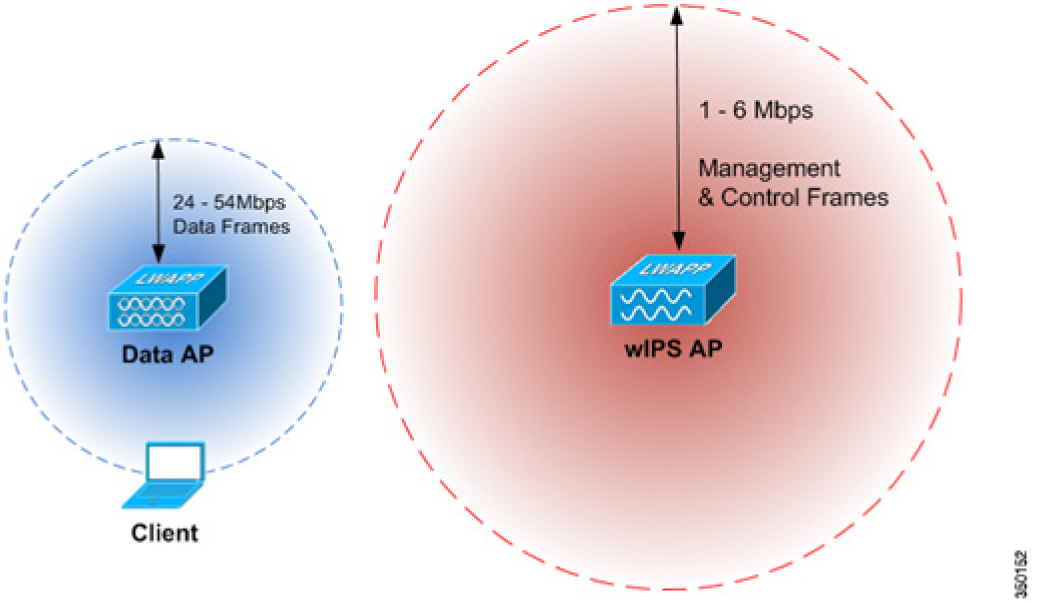
	1:1 Ratio	1:5 Ratio	2:5 Ratio
wIPS MM APs		3000	
Local Mode Data APs		12000	9000
ELM APs	15000		
AP3600 + WSSI			6000
Total (PI Limited)	15000	15000	15000

Note Only Monitor Mode wIPS requires separate Access points for data.

- A Wireless LAN Controller can support running local mode, monitor mode, enhanced local mode, and local/flex connect mode with the WSSI module all concurrently. Each access point uses an AP license.

How Many wIPS Access Points do I need?

Before deploying an Adaptive wIPS system, it's important to consider that the communications range of an access point's cell is less than the actual range at which frames may be received and decoded. The reason for this discrepancy is that an Access Point's communication range is limited by the weakest link – which in typical deployments is the WLAN client. Given that the output power of a WLAN client is intrinsically less than the Access Point's maximum, the range of the cell is restricted to the client's abilities. In addition, it is recommended practice to run Access Points at less than full power to build RF redundancy and load balancing into the wireless network. These aforementioned fact combined with the superior receive sensitivity of Cisco's Access Points allows the Adaptive wIPS system to be deployed with less access point density than the client serving infrastructure while still providing pervasive monitoring.



As depicted in the above diagram, a wIPS deployment is based on hearing 802.11 management and control frames which are used by a majority of attacks to cause harm. This is in contrast to a data Access Points deployment which is surveyed to provide higher throughput data rates anywhere from 24Mbps to 54Mbps.

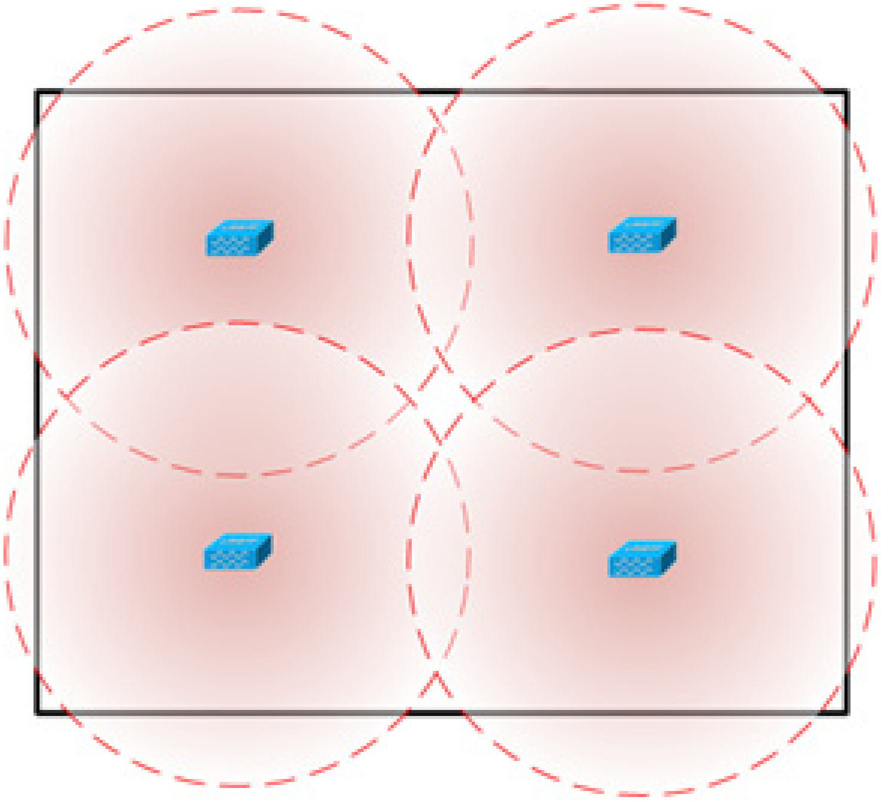
There are numerous factors that go into deciding exactly the number of wIPS Access Points that are required for a specific environment. Given that each prospective deployment's security requirements and environmental conditions are different, there is no hard and fast rule that will address the needs of every deployment but a few generalized guidelines must be taken into account.

The main factors, which affect the number of wIPS Access Points required, are as follows.

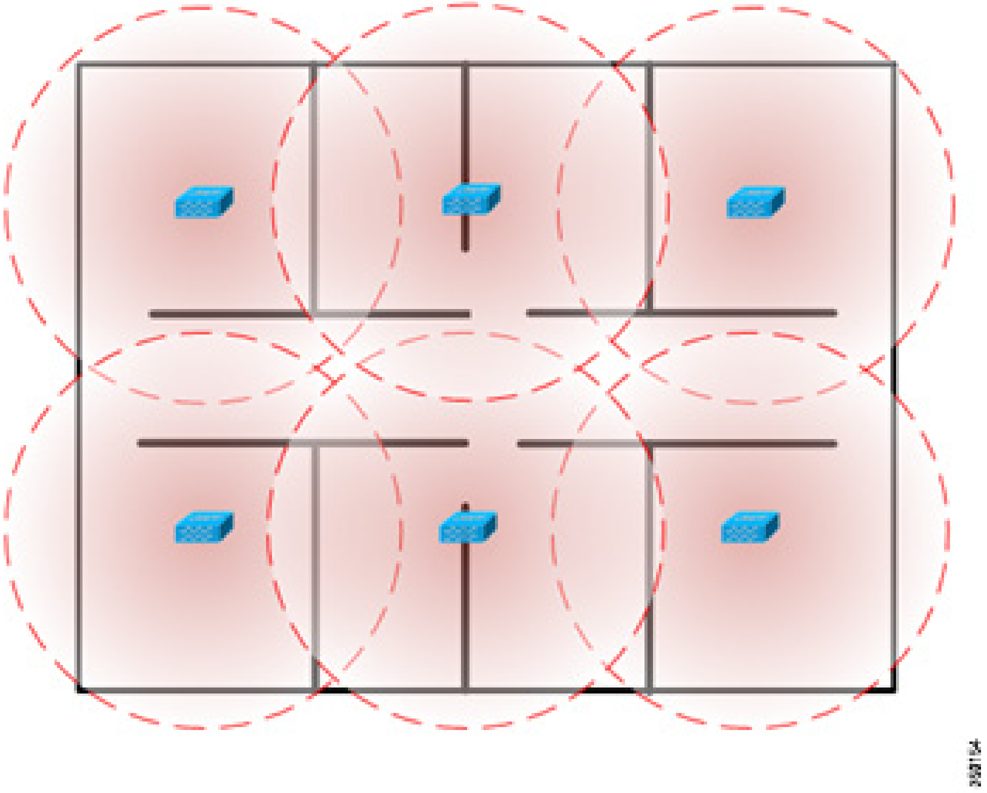
Deployment Conditions

Deployment-specific environmental conditions such as floor layout and building materials. Given that wireless signal propagation is heavily dependent on the type of material the signal must pass through, an office environment with numerous walls will require more sensors than an empty warehouse. This factor is similar to pre-existing knowledge as to how data-serving Access Points are deployed. The more obstacles in the environment which cause RF signal attenuation, the denser the deployment of wIPS Access Points will need to be.

In the below diagram, an open indoor environment is depicted where wIPS Access Points are deployed with the ability to 'listen' for attacks for a long distance given that there are no walls to disrupt or weaken a wireless signal.



In sharp contrast, the diagram below depicts an indoor environment with numerous heavy walls, which cause signal attenuation. In this case, more wIPS Access Points will need to be deployed to ensure that attacks are picked up.



Frequency Band(s) Monitored

The radio frequency propagation characteristics of the 2.4GHz and 5GHz bands vary as a result of the wavelength differences between the two. Put simply, 2.4GHz wireless signals (802.11b/g/n) travel a further distance than 5GHz (802.11a/n). In order to accurately compute the number of wIPS access points needed for a prospective installation, one must consider what frequency bands must be monitored in the wIPS deployment.

Monitor Range per wIPS AP (2.4GHz)		
Data Rate	Walled Indoor	Open Indoor
6Mbps @ -86dBm	~ 35,000 sqft	~ 85,000 sqft
6Mbps @ -86dBm	~ 10,668 sqm	~ 25,908 sqm

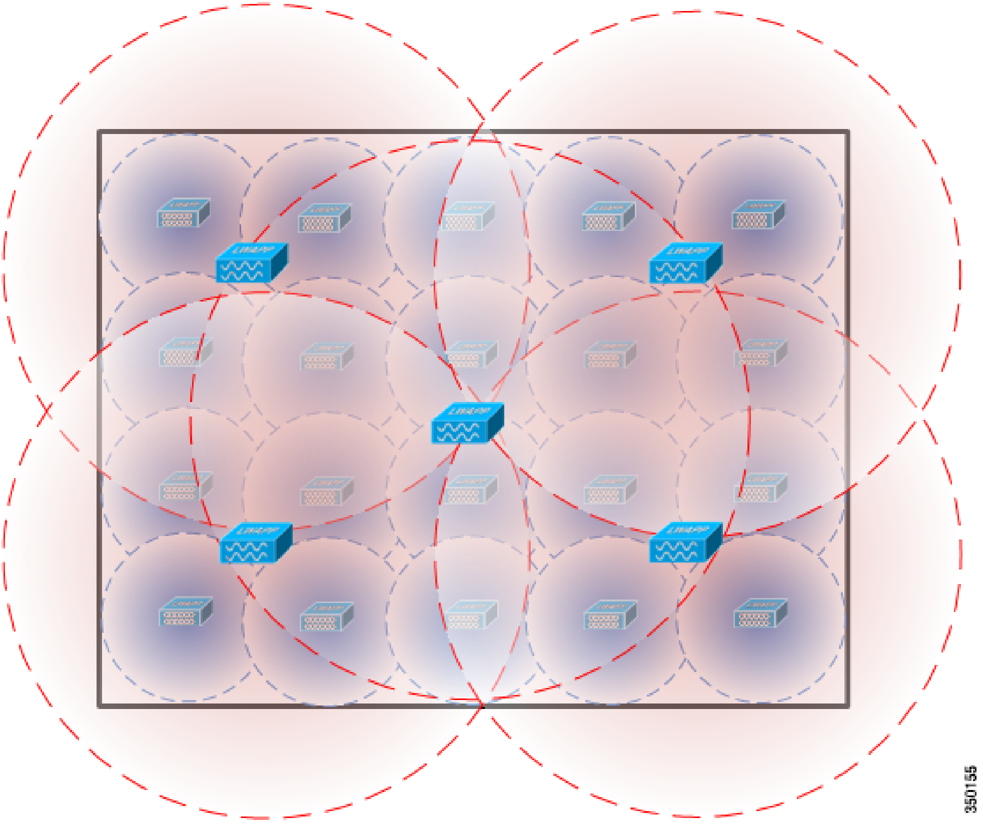
Monitor Range per wIPS AP (5GHz)		
Data Rate	Walled Indoor	Open Indoor
6Mbps @ -86dBm	~ 15,000 sqft	~ 85,000 sqft
6Mbps @ -86dBm	~ 4,572 sqm	~ 25,908 sqm

The above charts outline the circular square footage than can be covered by a single wIPS mode Access Point in each frequency band and each type of environment. These metrics can provide a baseline as how many wIPS Access Points are needed to cover a specific floor area. These charts were created using MatLab simulation software assuming an attacking device outputting 15dBm of transmit power. The receive sensitivity used this calculation represents the lowest common denominator between Cisco's line of Access Points that support wIPS.

Location of wIPS Access Points

The physical deployment of wIPS Mode Access Points is based on the end goal of providing pervasive monitoring across the entire WLAN infrastructure. To this end, wIPS mode APs are placed using two general guidelines. First, deploy wIPS access points around the periphery of your physical location to ensure adequate monitoring of attacks being launched from outside the building. This does not mean that wIPS mode Access Points should be deployed in the physical extremities of the building but instead they should be appropriately positioned to provide detection coverage to the extremities. Second, deploy wIPS access points throughout the center of the building to ensure complete detection of attacks launched from within the physical building.

The physical mounting location of a wIPS Access Point should be based on the same best practices used when mounting data serving Access Points. Following these conventions, it's important that wIPS Access Point antennas are not hidden behind heavy building materials or placed above drop ceilings. In the case that an Access Point is mounted above the ceiling, specific external antennas should be used to bring antenna leads into the same physical space that will be monitored.



In the above deployment example, four wIPS Access Points are deployed around the edges of the building to provide security monitoring around the periphery of the physical building. In addition, a wIPS Access Point is deployed in the center of the building to provide security-monitoring coverage inside the building.

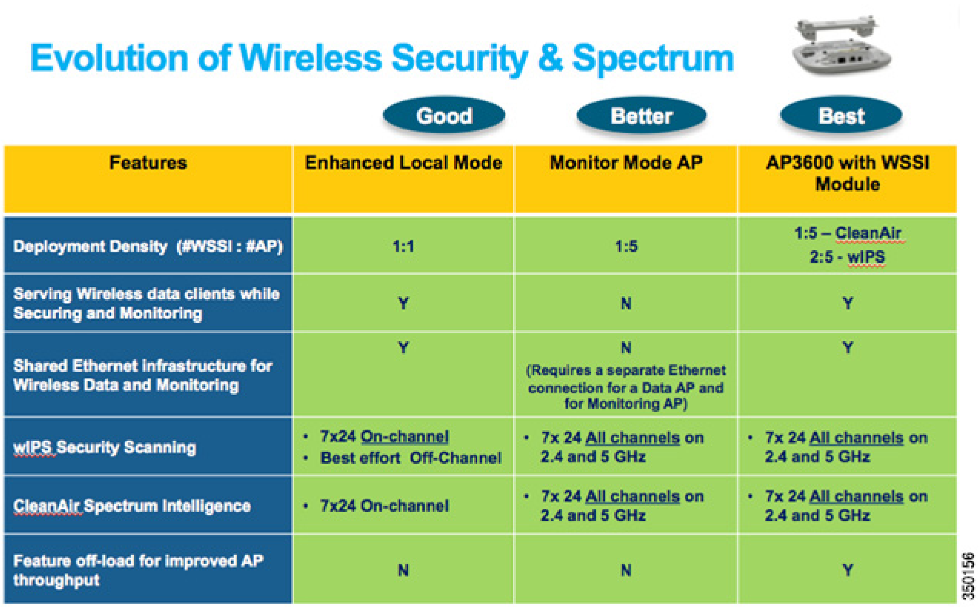
Access Point Density Recommendations

As stated above, the square footage of access point coverage can be measured based on frequency and environment, but with the newer wIPS modes, other factors also contribute to wIPS access point density recommendations. All access point modes can monitor the same distance, but due to the reasons below, it is recommended to deploy each mode with a different density.

wIPS Enhanced local mode Access Point are geared towards serving clients. For enhanced local mode deployments, it is recommended for every access point be put in enhanced local mode.

For monitor mode access points, we recommend that a ratio of 1:5 local mode to monitor mode access points.

Finally for the WSSI module, there is a single radio monitoring all channels on both the 2.4GHz and 5GHz band.   Since radio has additional channels to scan, it is recommended that the WSSI module be deployed with a 2:5 density to speed up detection time.



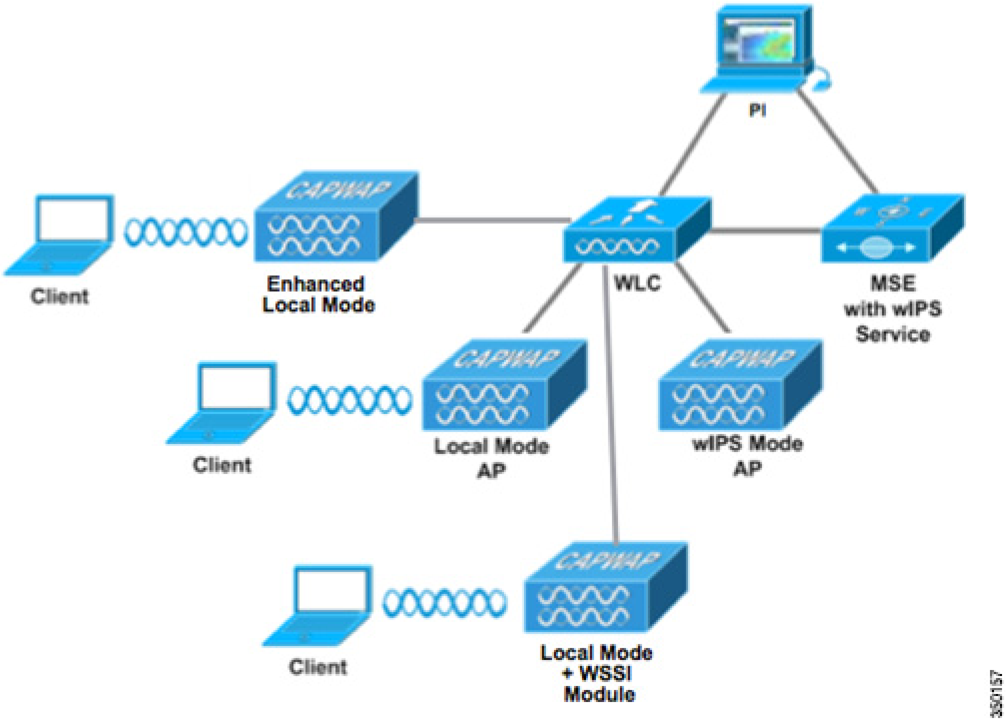
Evolution of Wireless Security & Spectrum

	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

350156

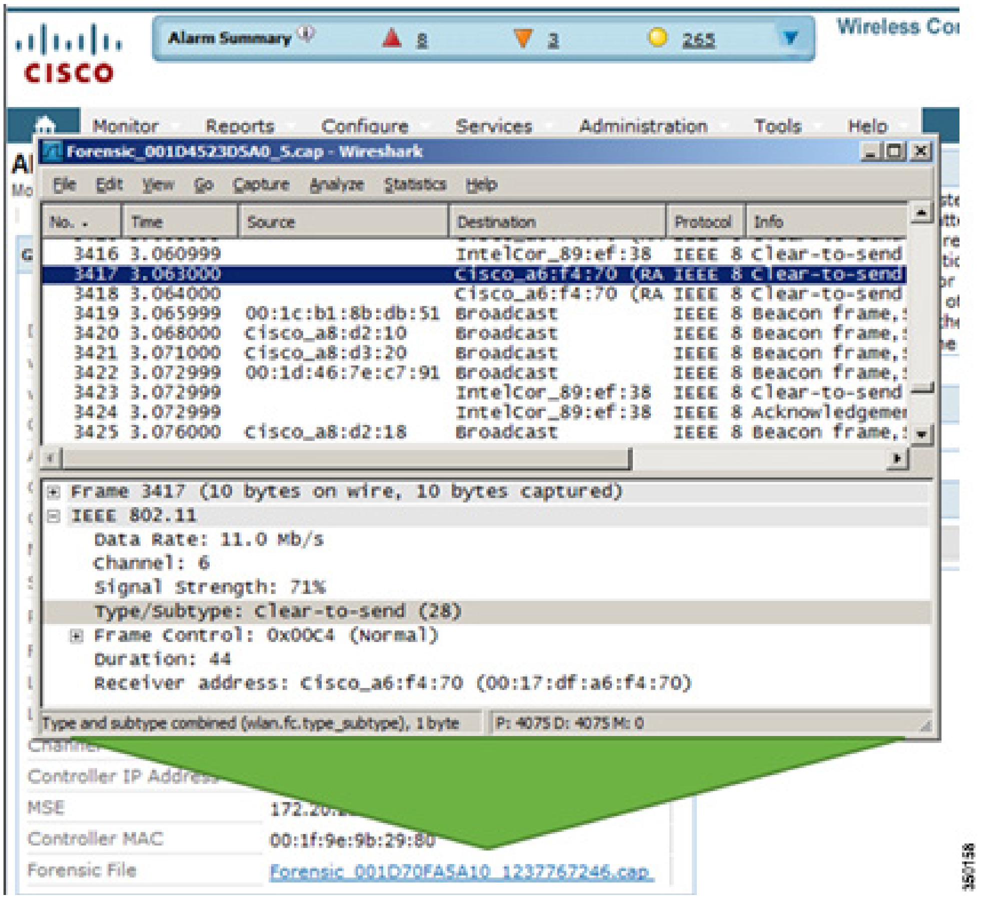
wIPS Integrated in a Cisco Unified Wireless Network

An integrated wIPS deployment is a system design in which non-wIPS Mode Access Points and wIPS Mode Access Points are intermixed on the same controller(s) and managed by the same Prime Infrastructure. This can be any combination of local mode, flex connect mode, enhanced local mode, monitor mode, and 3600 series Access points with the WSSI module. Overlaying wIPS protection and data shares many of the components including controllers and Prime Infrastructure thus reducing duplicate infrastructure costs.



Forensics

Cisco's Adaptive wIPS system provides the ability to capture attack forensics for further investigation and troubleshooting purposes. At a base level, the forensics capability is a toggle-based packet capture facility, which provides the ability to log and retrieve a set of wireless frames. This feature is enabled on a per attack basis from within the wIPS profile configuration of PI.



```
No. -  Time      Source             Destination          Protocol Info
 3416 3.060999                      Intelcor_89:ef:38    IEEE 8 Clear-to-send
 3417 3.063000                      Cisco_a6:f4:70 (RA   IEEE 8 Clear-to-send
 3418 3.064000                      Cisco_a6:f4:70 (RA   IEEE 8 Clear-to-send
 3419 3.065999 00:1c:b1:8b:db:51    Broadcast            IEEE 8 Beacon frame,:
 3420 3.068000 Cisco_a8:d2:10       Broadcast            IEEE 8 Beacon frame,:
 3421 3.071000 Cisco_a8:d3:20       Broadcast            IEEE 8 Beacon frame,:
 3422 3.072999 00:1d:46:7e:c7:91    Broadcast            IEEE 8 Beacon frame,:
 3423 3.072999                      Intelcor_89:ef:38    IEEE 8 Clear-to-send
 3424 3.072999                      Intelcor_89:ef:38    IEEE 8 Acknowledgemei
 3425 3.076000 Cisco_a8:d2:18       Broadcast            IEEE 8 Beacon frame,:
```

```
⊞ Frame 3417 (10 bytes on wire, 10 bytes captured)
⊟ IEEE 802.11
    Data Rate: 11.0 Mb/s
    Channel: 6
    Signal Strength: 71%
    Type/Subtype: Clear-to-send (28)
  ⊞ Frame Control: 0x00C4 (Normal)
    Duration: 44
    Receiver address: Cisco_a6:f4:70 (00:17:df:a6:f4:70)
Type and subtype combined (wlan.fc.type_subtype), 1 byte    P: 4075 D: 4075 M: 0
```

Channe
Controller IP Address
MSE 172.20.
Controller MAC 00:1f:9e:9b:29:80
Forensic File Forensic_001D70FA5A10_1237767246.cap

Once enabled, the forensics feature is triggered once a specific attack alarm is seen over the airwaves. The forensic file will be created based on the packets contained within the buffer of the wIPS Mode AP that triggered the original alarm. This file is transferred to the Wireless LAN Controller via CAPWAP, which then forwards the forensic file via NMSP to the wIPS Service running on the Mobility Services Engine. The file is stored within the forensic archive on the MSE until the user configured disk space limit for forensics is reached. By default this limit is 20Gigabytes, which when reached will cause the oldest forensic files to be removed. Access to the forensic file can be obtained by opening the alarm on the Prime Infrastructure, which contains a hyperlink to the forensic file. The files are stored as a '.CAP' file format which can be opened by either WildPacket's Omnipeek, AirMagnet WiFi Analyzer, Wireshark or any other packet capture program which supports this format. Wireshark is available at http://www.wireshark.org.

Note The forensics capability of the wIPS system should be used sparingly and then disabled after the desired information is captured. The reason for this recommendation is the intensive load it places on the Access Point as well as the interruption in scheduled channel scanning this capability requires. A wIPS Access Point cannot be simultaneously performing channel scanning at the same instance it is producing a forensic file. While the forensic file is being dumped, channel scanning will be delayed for a maximum of 5 seconds.

Licensing and Ordering Information

Cisco Adaptive wIPS is a licensed software feature set on the Cisco Mobility Services Engine. The table below shows the license levels available for Adaptive wIPS

Table 1 Cisco Adaptive wIPS Software Licenses

License SKUs	Description
L-WIPS-MM-1AP	License for 1 monitor mode access point
L-WIPS-MM-100AP	License for 100 monitor mode access points
L-WIPS-MM-1000AP	License for 1000 monitor mode access points
L-WIPS-ELM-1AP	License for 1 enhanced local mode access point
L-WIPS-ELM-100AP	License for 100 enhanced local mode access points
L-WIPS-ELM-1000AP	License for 1000 enhanced local mode access points

Note The WSSI module will use a L-WIPS-MM license

Ordering Support

For MSE hardware appliance orders, Cisco SMARTnet® Service includes both hardware and license support. Select the appropriate level of hardware support under the Cisco SMARTnet Service program for the Cisco MSE hardware appliances. Use the following SKU:

- CON-SNT-MSE3355

For MSE Virtual Appliance orders, use the following SKU for both software and license support:

- CON-SAU-LMSE7K

Adaptive wIPS Configuration

Mobility Services Engine Setup

To setup the mobility services engine:

Step 1 Login:

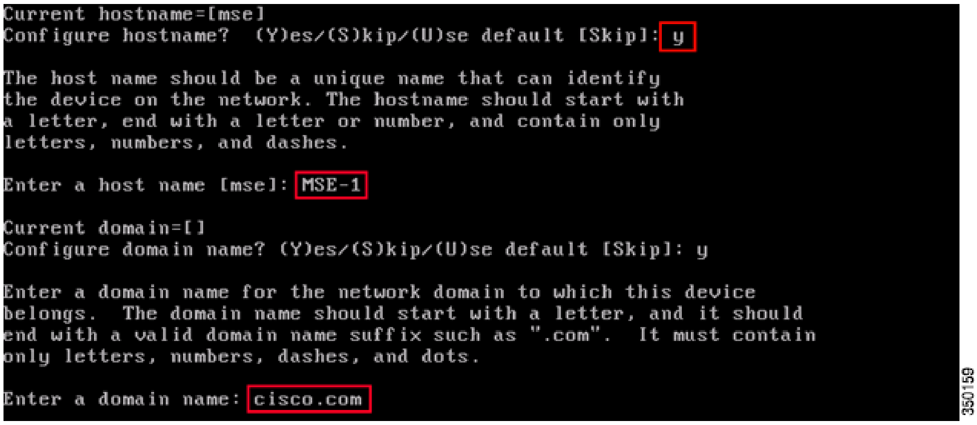
Login with the following credentials: **root/password**

Step 2 Start the Setup Process:

Upon the initial boot up, the MSE will prompt the administrator to launch the setup script. Enter **yes** to this prompt.

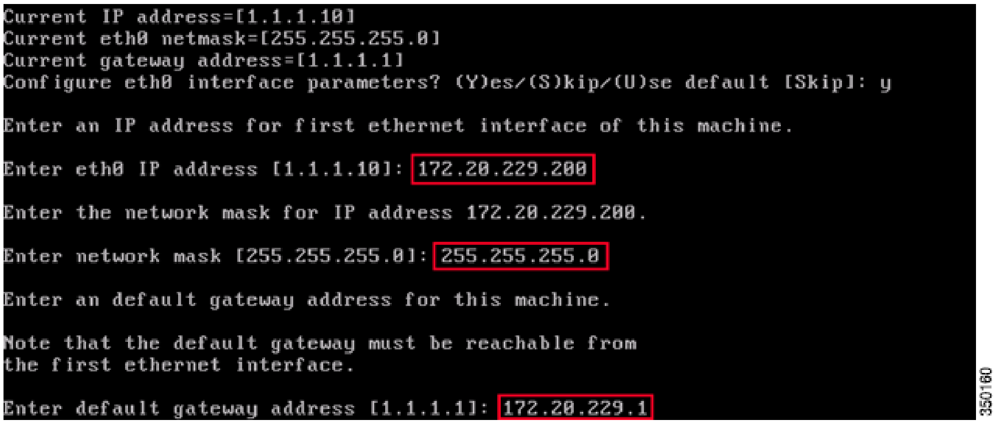
Note If the MSE does not prompt for setup, enter the following command: **`/opt/mse/setup/setup.sh`**

Step 3 Configure Hostname and DNS Domain Name:



```
Current hostname=[mse]
Configure hostname?  (Y)es/(S)kip/(U)se default [Skip]: y

The host name should be a unique name that can identify
the device on the network. The hostname should start with
a letter, end with a letter or number, and contain only
letters, numbers, and dashes.

Enter a host name [mse]: MSE-1

Current domain=[]
Configure domain name? (Y)es/(S)kip/(U)se default [Skip]: y

Enter a domain name for the network domain to which this device
belongs.  The domain name should start with a letter, and it should
end with a valid domain name suffix such as ".com".  It must contain
only letters, numbers, dashes, and dots.

Enter a domain name: cisco.com
```

Step 4 Configure Ethernet Interface Parameters:

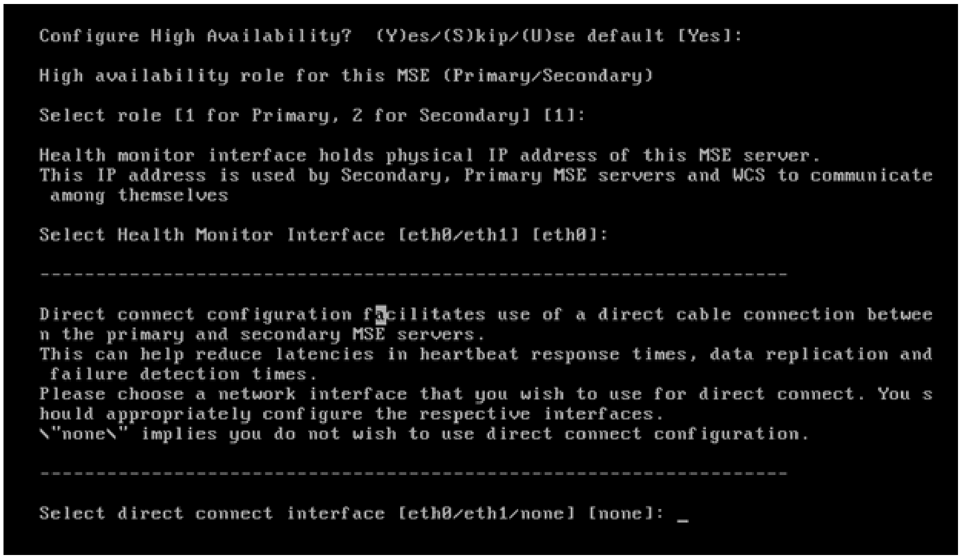


```
Current IP address=[1.1.1.10]
Current eth0 netmask=[255.255.255.0]
Current gateway address=[1.1.1.1]
Configure eth0 interface parameters? (Y)es/(S)kip/(U)se default [Skip]: y

Enter an IP address for first ethernet interface of this machine.

Enter eth0 IP address [1.1.1.10]: 172.20.229.200

Enter the network mask for IP address 172.20.229.200.

Enter network mask [255.255.255.0]: 255.255.255.0

Enter an default gateway address for this machine.

Note that the default gateway must be reachable from
the first ethernet interface.

Enter default gateway address [1.1.1.1]: 172.20.229.1
```

When prompted for **eth1** interface parameters, enter ‘Skip’ to proceed to the next step as a second NIC is not required for operation.

Note The address configured must provide IP connectivity to the perspective Wireless LAN controller(s) and PI Management system used with this appliance.

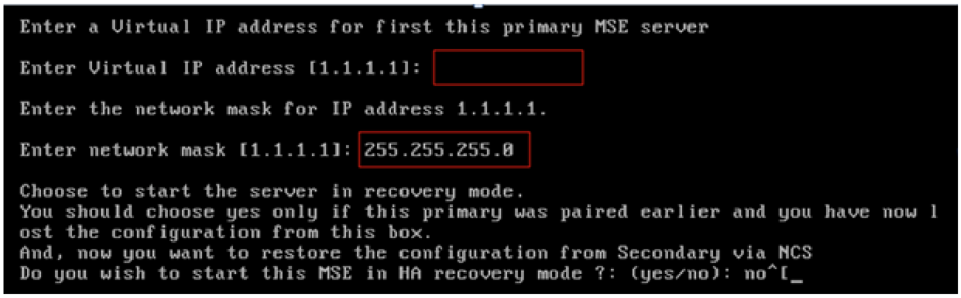
Step 5 Configure High Availability (Optional):



```
Configure High Availability?  (Y)es/(S)kip/(U)se default [Yes]:

High availability role for this MSE (Primary/Secondary)

Select role [1 for Primary, 2 for Secondary] [1]:

Health monitor interface holds physical IP address of this MSE server.
This IP address is used by Secondary, Primary MSE servers and WCS to communicate
 among themselves

Select Health Monitor Interface [eth0/eth1] [eth0]:

-------------------------------------------------------------------

Direct connect configuration facilitates use of a direct cable connection betwee
n the primary and secondary MSE servers.
This can help reduce latencies in heartbeat response times, data replication and
 failure detection times.
Please choose a network interface that you wish to use for direct connect. You s
hould appropriately configure the respective interfaces.
\"none\" implies you do not wish to use direct connect configuration.

-------------------------------------------------------------------

Select direct connect interface [eth0/eth1/none] [none]: _
```

350161

Enabled High Availability, then select the role of the MSE. Then select the Ethernet port that will be actively monitored by a secondary MSE server. If there is a direct connection, the Ethernet port must be given.



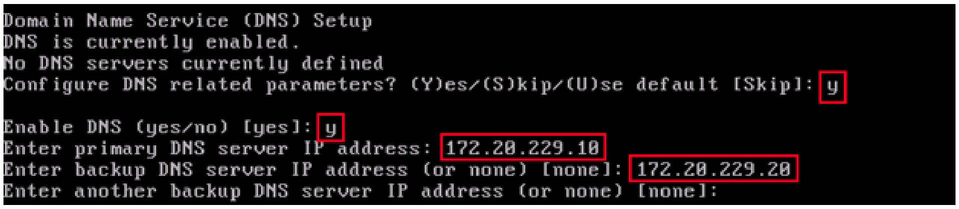
```
Enter a Virtual IP address for first this primary MSE server

Enter Virtual IP address [1.1.1.1]:

Enter the network mask for IP address 1.1.1.1.

Enter network mask [1.1.1.1]: 255.255.255.0

Choose to start the server in recovery mode.
You should choose yes only if this primary was paired earlier and you have now l
ost the configuration from this box.
And, now you want to restore the configuration from Secondary via NCS
Do you wish to start this MSE in HA recovery mode ?: (yes/no): no^[_
```

350162

Now provide a Virtual IP address for this HA pair. Once a Virtual IP address is given, you can being the HA exchange by starting HA Recovery mode.

Step 6 Enter DNS Server(s) Information:

Only one DNS server is required for successful domain resolution, enter backup servers for resiliency.

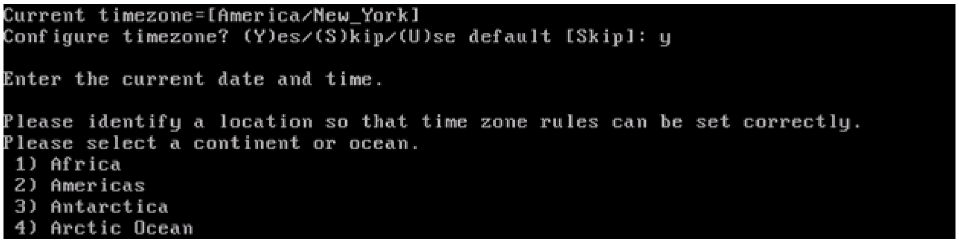


```
Domain Name Service (DNS) Setup
DNS is currently enabled.
No DNS servers currently defined
Configure DNS related parameters? (Y)es/(S)kip/(U)se default [Skip]: y

Enable DNS (yes/no) [yes]: y
Enter primary DNS server IP address: 172.20.229.10
Enter backup DNS server IP address (or none) [none]: 172.20.229.20
Enter another backup DNS server IP address (or none) [none]:
```

350163

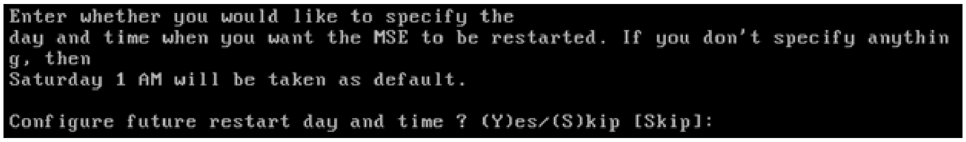
Step 7 Configure Time Zone:

If the default time zone of New York is not applicable to your environment, browse through the location menus to set it correctly.



```
Current timezone=[America/New_York]
Configure timezone? (Y)es/(S)kip/(U)se default [Skip]: y

Enter the current date and time.

Please identify a location so that time zone rules can be set correctly.
Please select a continent or ocean.
 1) Africa
 2) Americas
 3) Antarctica
 4) Arctic Ocean
```

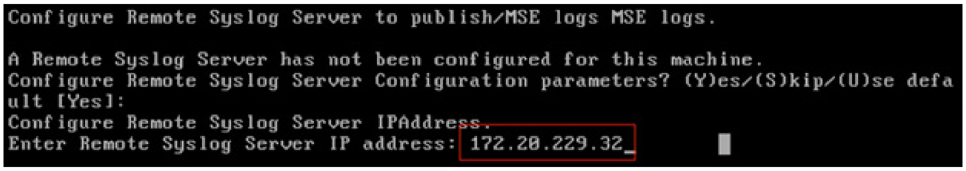
Step 8 Assign a time to restart the MSE (This step is optional):



```
Enter whether you would like to specify the
day and time when you want the MSE to be restarted. If you don't specify anythin
g, then
Saturday 1 AM will be taken as default.

Configure future restart day and time ? (Y)es/(S)kip [Skip]:
```

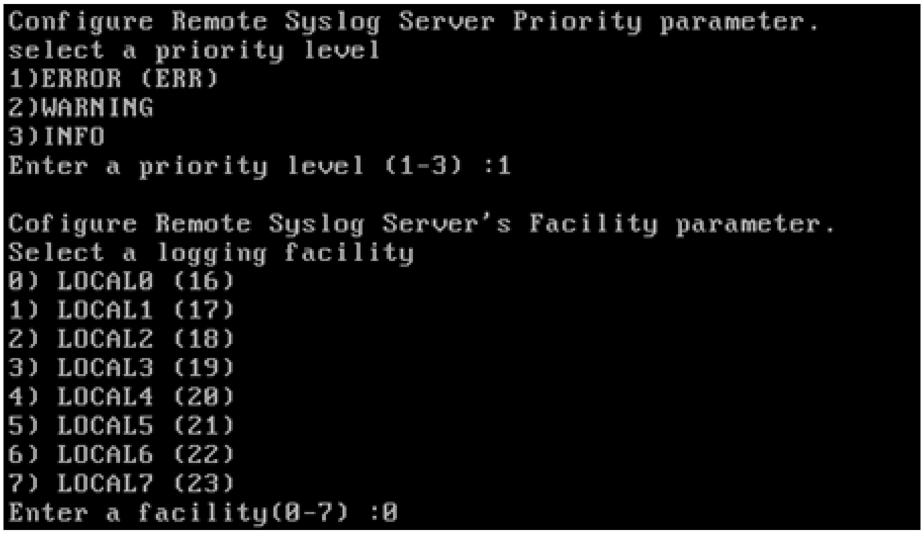
This can be skipped.

Step 9 Configure a Remote Syslog Server:



```
Configure Remote Syslog Server to publish/MSE logs MSE logs.

A Remote Syslog Server has not been configured for this machine.
Configure Remote Syslog Server Configuration parameters? (Y)es/(S)kip/(U)se defa
ult [Yes]:
Configure Remote Syslog Server IPAddress.
Enter Remote Syslog Server IP address: 172.20.229.32_
```

Configure the IP address of your remote Syslog Server.

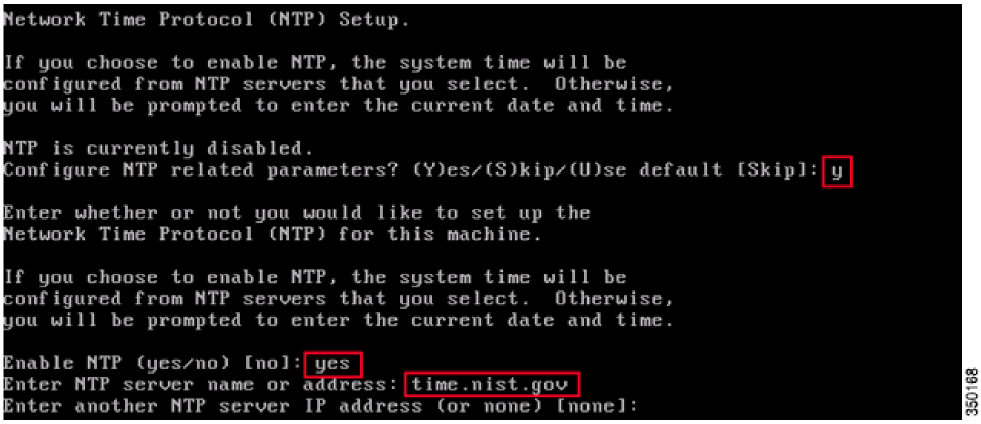


```
Configure Remote Syslog Server Priority parameter.
select a priority level
1)ERROR (ERR)
2)WARNING
3)INFO
Enter a priority level (1-3) :1

Cofigure Remote Syslog Server's Facility parameter.
Select a logging facility
0) LOCAL0 (16)
1) LOCAL1 (17)
2) LOCAL2 (18)
3) LOCAL3 (19)
4) LOCAL4 (20)
5) LOCAL5 (21)
6) LOCAL6 (22)
7) LOCAL7 (23)
Enter a facility(0-7) :0
```

Then provide the log message priority level and facility.

Step 10 Configure NTP or System Time:

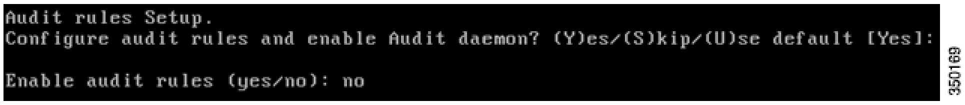
NTP is optional but ensures your system maintains an accurate system time. If you select **No** you will be prompted to set the current time for the system.



```
Network Time Protocol (NTP) Setup.

If you choose to enable NTP, the system time will be
configured from NTP servers that you select.  Otherwise,
you will be prompted to enter the current date and time.

NTP is currently disabled.
Configure NTP related parameters? (Y)es/(S)kip/(U)se default [Skip]: y

Enter whether or not you would like to set up the
Network Time Protocol (NTP) for this machine.

If you choose to enable NTP, the system time will be
configured from NTP servers that you select.  Otherwise,
you will be prompted to enter the current date and time.

Enable NTP (yes/no) [no]: yes
Enter NTP server name or address: time.nist.gov
Enter another NTP server IP address (or none) [none]:
```

Note It is imperative that the correct time be set on the Mobility Services Engine, Wireless LAN Controller and PI Management System. This can be achieved by pointing all three systems to the same NTP server and ensuring they have the correct time zones configured.

Step 11 Configure Audit Rules (Optional):

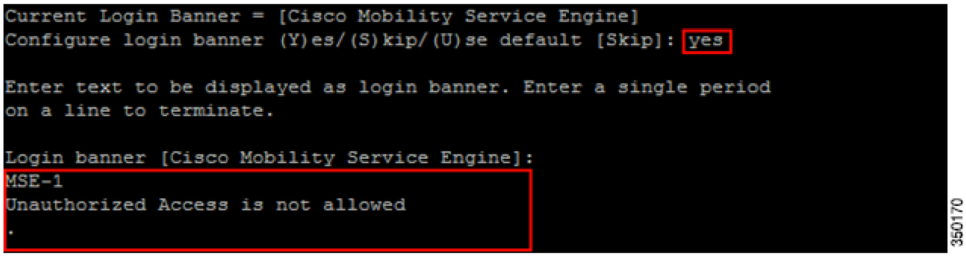


```
Audit rules Setup.
Configure audit rules and enable Audit daemon? (Y)es/(S)kip/(U)se default [Yes]:

Enable audit rules (yes/no): no
```

This allows the user to configure an audit daemon. This step can be skipped.

Step 12 Set Login Banner:

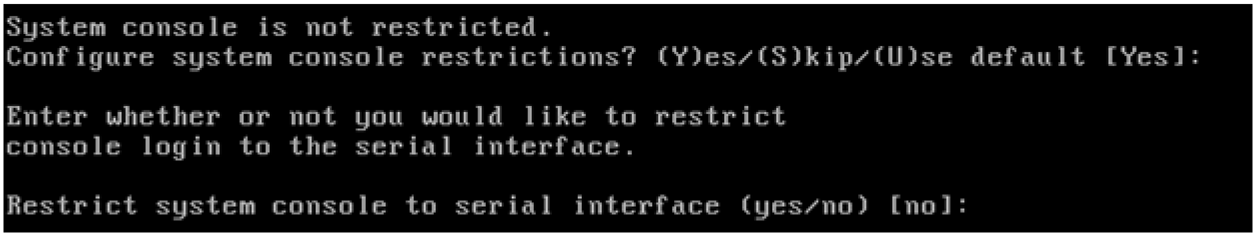
A login banner is used to inform users of the system's use and present a warning to keep unauthorized users from accessing the system. Since the login banner may be a multi-line message, a single period (.) ends the message and proceeds to the next step.



```
Current Login Banner = [Cisco Mobility Service Engine]
Configure login banner (Y)es/(S)kip/(U)se default [Skip]: yes

Enter text to be displayed as login banner. Enter a single period
on a line to terminate.

Login banner [Cisco Mobility Service Engine]:
MSE-1
Unauthorized Access is not allowed
.
```

Step 13 Enable local console root login:

This parameter is used to enable/disable local console access to the system. This should be enabled so local troubleshooting can occur.

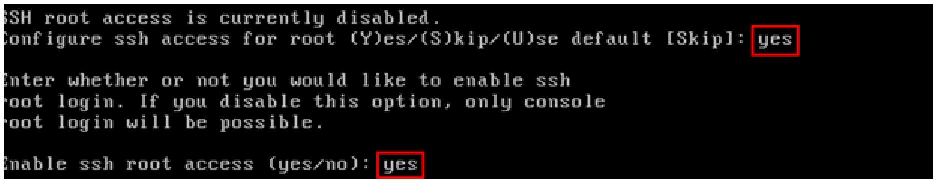


```
System console is not restricted.
Configure system console restrictions? (Y)es/(S)kip/(U)se default [Yes]:

Enter whether or not you would like to restrict
console login to the serial interface.

Restrict system console to serial interface (yes/no) [no]:
```

350171

Step 14 Enable SSH (Secure Shell) root login (Optional):

This parameter is used to enable/disable remote console access to the system. This should be enabled so remote troubleshooting can occur however corporate security policies may mandate disabling this option.

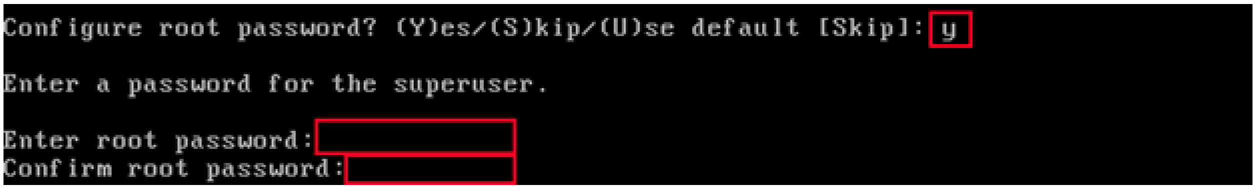


```
SH root access is currently disabled.
onfigure ssh access for root (Y)es/(S)kip/(U)se default [Skip]: yes

nter whether or not you would like to enable ssh
oot login. If you disable this option, only console
oot login will be possible.

nable ssh root access (yes/no): yes
```

350172

Step 15 Change the root password:

This step is critical in ensuring system security, be sure to pick a strong password consisting of letters and numbers with no dictionary words. The minimum password length is 8 characters.

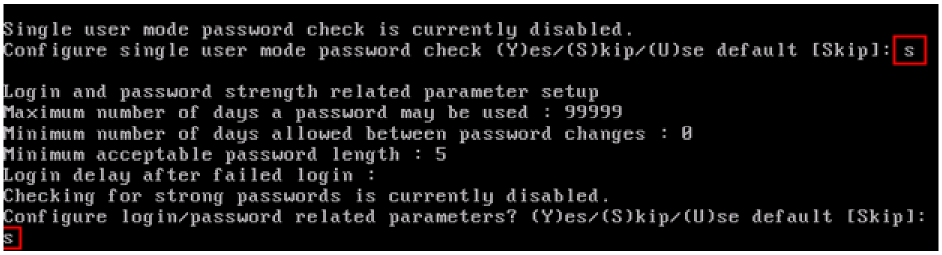


```
Configure root password? (Y)es/(S)kip/(U)se default [Skip]: y

Enter a password for the superuser.

Enter root password:
Confirm root password:
```

350173

Step 16 Configure single user mode and password strength:

These configuration parameters are not required and the default setting is to skip them by entering 's'.

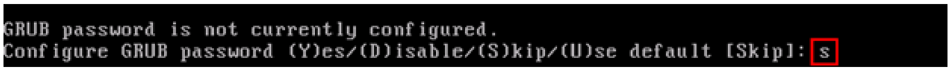


```
Single user mode password check is currently disabled.
Configure single user mode password check (Y)es/(S)kip/(U)se default [Skip]: s

Login and password strength related parameter setup
Maximum number of days a password may be used : 99999
Minimum number of days allowed between password changes : 0
Minimum acceptable password length : 5
Login delay after failed login :
Checking for strong passwords is currently disabled.
Configure login/password related parameters? (Y)es/(S)kip/(U)se default [Skip]:
s
```

350174

Step 17 Configure a GRUB password:

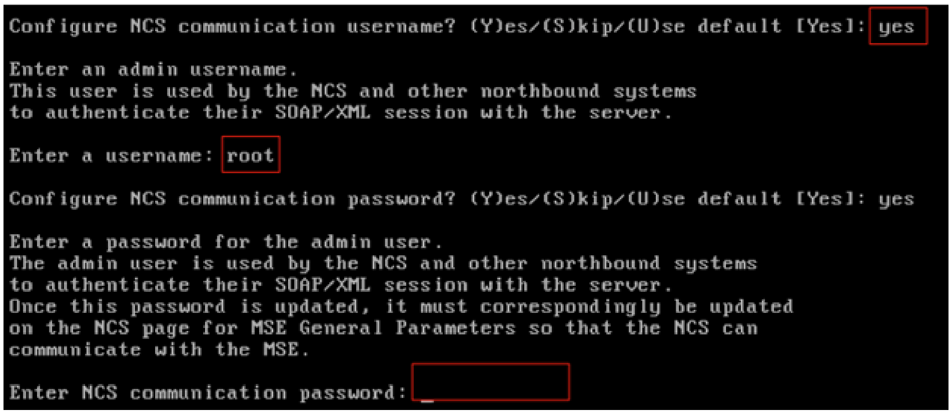
This configuration parameter is not required and the default setting is to skip it by entering 's'. (This step is optional).



```
GRUB password is not currently configured.
Configure GRUB password (Y)es/(D)isable/(S)kip/(U)se default [Skip]: s
```

350175

Step 18 Configure a Prime Infrastruction communication password:



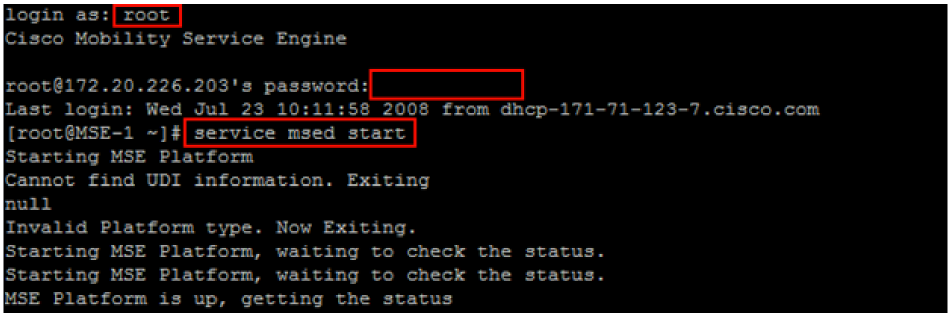
```
Configure NCS communication username? (Y)es/(S)kip/(U)se default [Yes]: yes

Enter an admin username.
This user is used by the NCS and other northbound systems
to authenticate their SOAP/XML session with the server.

Enter a username: root

Configure NCS communication password? (Y)es/(S)kip/(U)se default [Yes]: yes

Enter a password for the admin user.
The admin user is used by the NCS and other northbound systems
to authenticate their SOAP/XML session with the server.
Once this password is updated, it must correspondingly be updated
on the NCS page for MSE General Parameters so that the NCS can
communicate with the MSE.

Enter NCS communication password: _
```

Step 19 Save Changes and Reboot:

Once the setup script has completed, **save your changes when prompted**. After saving, **follow the prompts to reboot** the MSE as well to ensure all settings are applied successfully.

Step 20 Start the MSE Service:

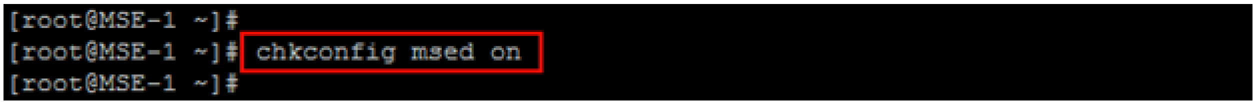
Login to the MSE using the username **root** and password previously configured in **step 13.** Execute the command **`service msed start`** to start the MSE service.



```
login as: root
Cisco Mobility Service Engine

root@172.20.226.203's password:
Last login: Wed Jul 23 10:11:58 2008 from dhcp-171-71-123-7.cisco.com
[root@MSE-1 ~]# service msed start
Starting MSE Platform
Cannot find UDI information. Exiting
null
Invalid Platform type. Now Exiting.
Starting MSE Platform, waiting to check the status.
Starting MSE Platform, waiting to check the status.
MSE Platform is up, getting the status
```

Step 21 Enable the MSE Service to Start at Bootup:

Execute the command: **`chkconfig msed on`**



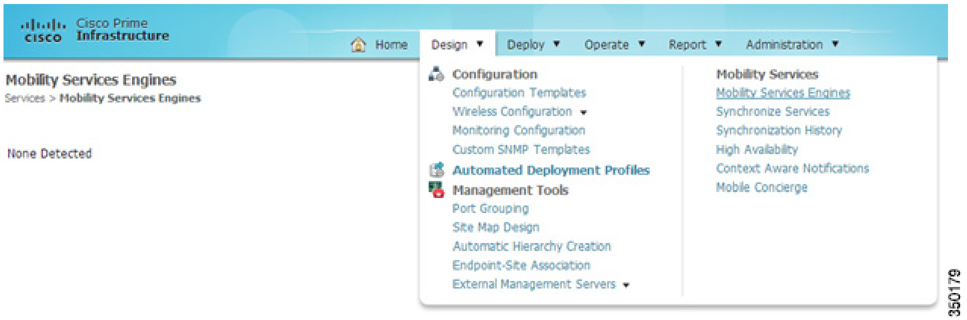
```
[root@MSE-1 ~]#
[root@MSE-1 ~]# chkconfig msed on
[root@MSE-1 ~]#
```

Adding the MSE to PI

To add MSE to PI:

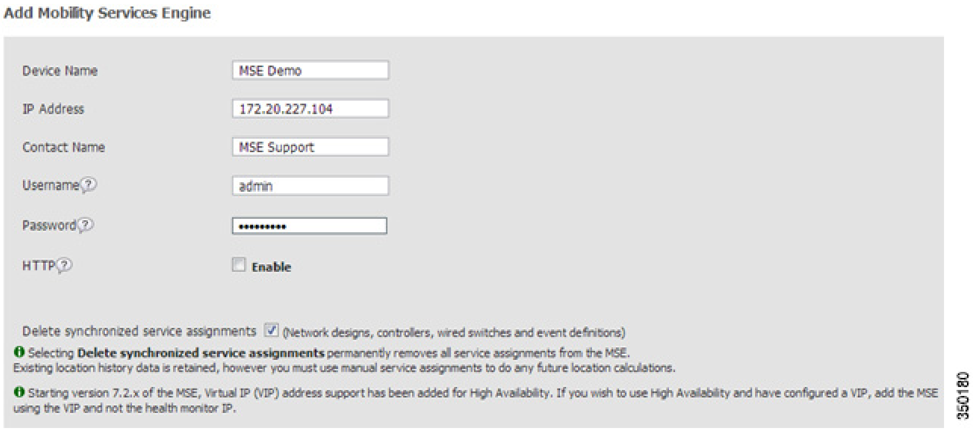
Step 1 Navigate to the Mobility Services Configuration Page:

Login to PI and click **Mobility Services Engine** from the **Design** drop-down menu.



Step 2 Add the Mobility Services Engine to PI:

From the drop down on the right hand side, select **Add Mobility Services Engine** and click **Go**


Add Mobility Services Engine

Device Name	MSE Demo
IP Address	172.20.227.104
Contact Name	MSE Support
Username	admin
Password	••••••••••
HTTP	□ Enable

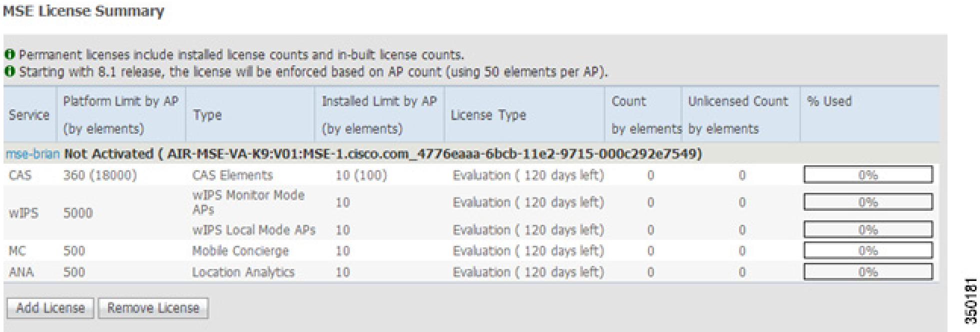
Delete synchronized service assignments ☑ (Network designs, controllers, wired switches and event definitions)

Selecting **Delete synchronized service assignments** permanently removes all service assignments from the MSE.
Existing location history data is retained, however you must use manual service assignments to do any future location calculations.

Starting version 7.2.x of the MSE, Virtual IP (VIP) address support has been added for High Availability. If you wish to use High Availability and have configured a VIP, add the MSE using the VIP and not the health monitor IP.

Enter a unique device name for the MSE, the IP address previously configured during the MSE setup, a contact name for support and the **PI Communication Password** configured during the MSE setup. Do not change the username from the default of **admin**.

Step 3 Add MSE License:

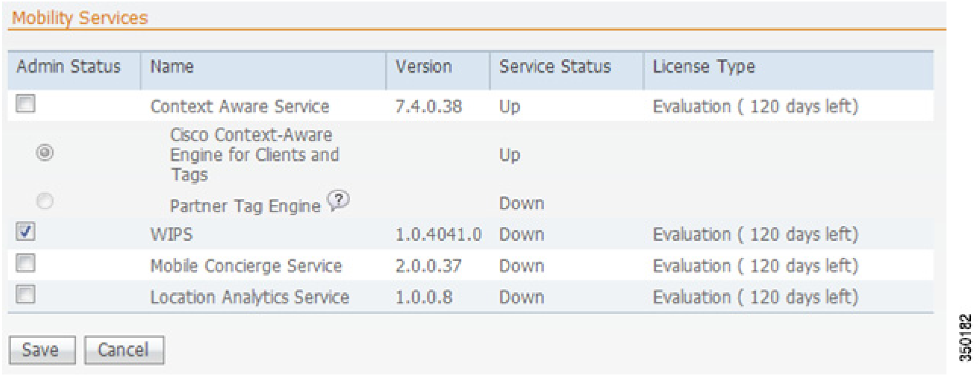

MSE License Summary

Permanent licenses include installed license counts and in-built license counts.
Starting with 8.1 release, the license will be enforced based on AP count (using 50 elements per AP).

Service	Platform Limit by AP (by elements)	Type	Installed Limit by AP (by elements)	License Type	Count by elements	Unlicensed Count by elements	% Used
mse-brian Not Activated (AIR-MSE-VA-K9:V01:MSE-1.cisco.com_4776eaaa-6bcb-11e2-9715-000c292e7549)							
CAS	360 (18000)	CAS Elements	10 (100)	Evaluation (120 days left)	0	0	0%
wIPS	5000	wIPS Monitor Mode APs	10	Evaluation (120 days left)	0	0	0%
		wIPS Local Mode APs	10	Evaluation (120 days left)	0	0	0%
MC	500	Mobile Concierge	10	Evaluation (120 days left)	0	0	0%
ANA	500	Location Analytics	10	Evaluation (120 days left)	0	0	0%

Add your MSE license here.

Step 4 Select the WIPS Service to run on the MSE:

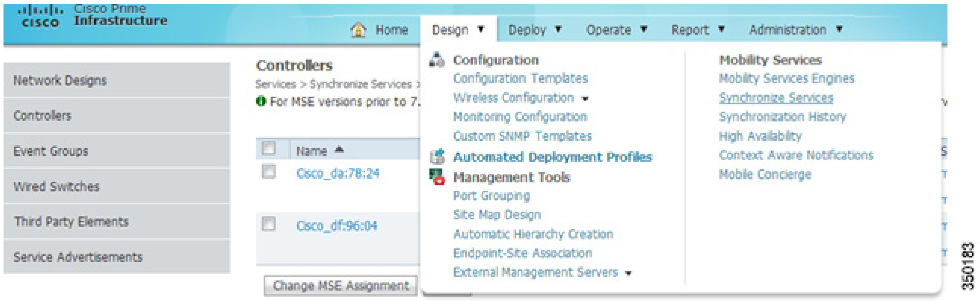


Mobility Services

Admin Status	Name	Version	Service Status	License Type
□	Context Aware Service	7.4.0.38	Up	Evaluation (120 days left)
●	Cisco Context-Aware Engine for Clients and Tags		Up	
○	Partner Tag Engine ?		Down	
☑	WIPS	1.0.4041.0	Down	Evaluation (120 days left)
□	Mobile Concierge Service	2.0.0.37	Down	Evaluation (120 days left)
□	Location Analytics Service	1.0.0.8	Down	Evaluation (120 days left)

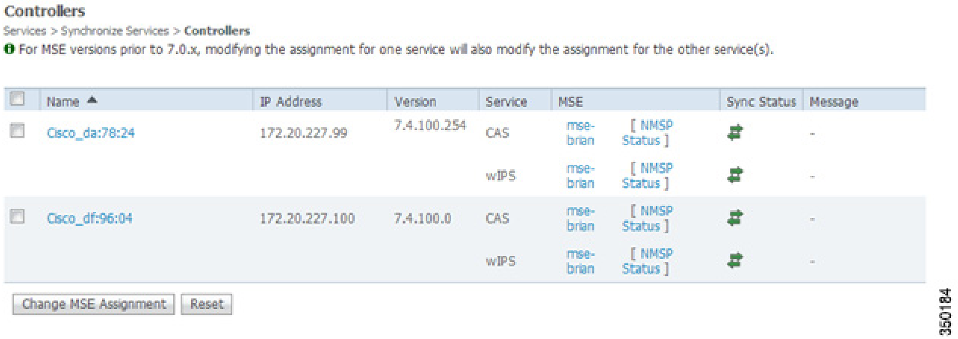
Step 5 Synchronize:

From the **Design** drop-down menu, select **Synchronize Services**



Step 6 Select Controllers to Synchronize:

Select the Controllers tab, to see a list of controllers. Once the desired controllers are selected, press the **Change MSE Assignment** button.



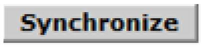
Controllers

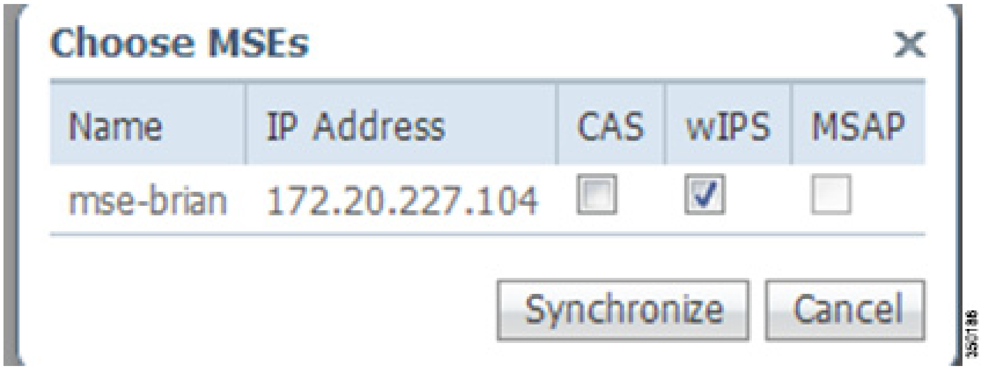
Services > Synchronize Services > **Controllers**

For MSE versions prior to 7.0.x, modifying the assignment for one service will also modify the assignment for the other service(s).

□	Name ▲	IP Address	Version	Service	MSE		Sync Status	Message
□	Cisco_da:78:24	172.20.227.99	7.4.100.254	CAS	mse-brian	[NMSP Status]	⇄	-
				wIPS	mse-brian	[NMSP Status]	⇄	-
□	Cisco_df:96:04	172.20.227.100	7.4.100.0	CAS	mse-brian	[NMSP Status]	⇄	-
				wIPS	mse-brian	[NMSP Status]	⇄	-

A popup will be displayed with a list of controllers to synchronize the MSE with. Select the desired features for synchronization and click.





Choose MSEs

Name	IP Address	CAS	wIPS	MSAP
mse-brian	172.20.227.104	□	☑	□

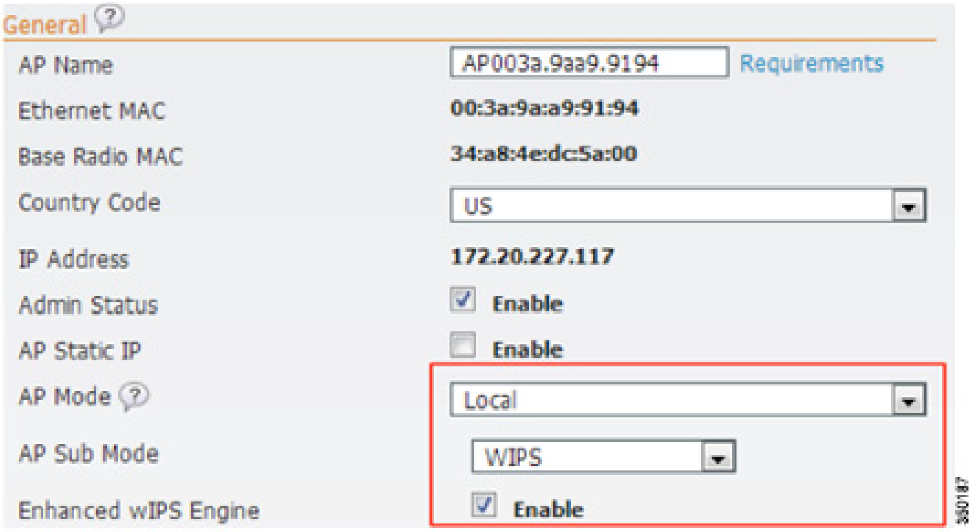
Configuring Access Points for Enhanced Local Mode

Any local mode indoor access point can be configured in enhanced local mode.

To configure access points for enhanced local mode:

Step 1 Configure the Access Point for Enhanced Local Mode:

a. Enter the Access Point configuration menu in PI via **Operate > Device Group > Device Type > Unified AP** and click on the Access Point's name, then **Configuration.**



General

AP Name	AP003a.9aa9.9194
Ethernet MAC	00:3a:9a:a9:91:94
Base Radio MAC	34:a8:4e:dc:5a:00
Country Code	US
IP Address	172.20.227.117
Admin Status	☑ Enable
AP Static IP	□ Enable
AP Mode	Local
AP Sub Mode	WIPS
Enhanced wIPS Engine	☑ Enable

b. Change **AP Mode** to **Local**

c. Enable **Enhanced WIPS Engine**

d. Change **AP Sub Mode** to **WIPS**

e. Click **Save** at the bottom of the page.

f. Click **OK** when prompted to reboot the Access Point.

Repeat this for each Access Point that has been configured into Enhanced Local Mode.

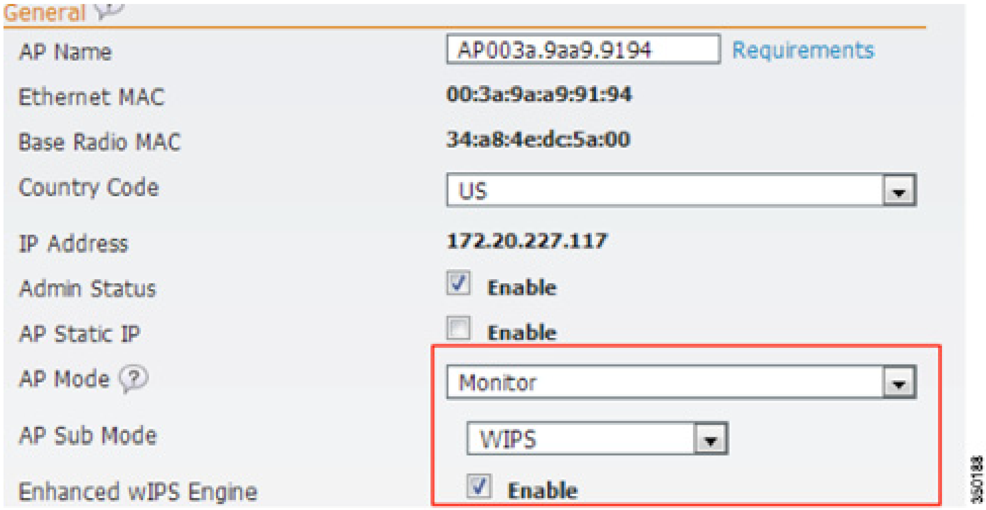
Configuring Access Points for wIPS Monitor Mode

Any indoor access point can be configured in wIPS monitor mode.

To configure access points for wIPS monitor mode:

Step 1 Configure the Access Point for Monitor Mode:

a. Enter the Access Point configuration menu in PI via **Operate>Device Group> Device Type> Unified AP** and click on the Access Point's name, then **Configuration**



General

AP Name	AP003a.9aa9.9194 Requirements
Ethernet MAC	00:3a:9a:a9:91:94
Base Radio MAC	34:a8:4e:dc:5a:00
Country Code	US
IP Address	172.20.227.117
Admin Status	☑ Enable
AP Static IP	□ Enable
AP Mode	Monitor
AP Sub Mode	WIPS
Enhanced wIPS Engine	☑ Enable

b. Change **AP Mode** to **Monitor**

c. Enable **Enhanced WIPS Engine**

d. Change **Monitor Mode Optimization** to **WIPS**

e. Click **Save** at the bottom of the page

f. Click **OK** when prompted to reboot the Access Point.

Repeat this for each Access Point that has been configured into wIPS Monitor Mode.

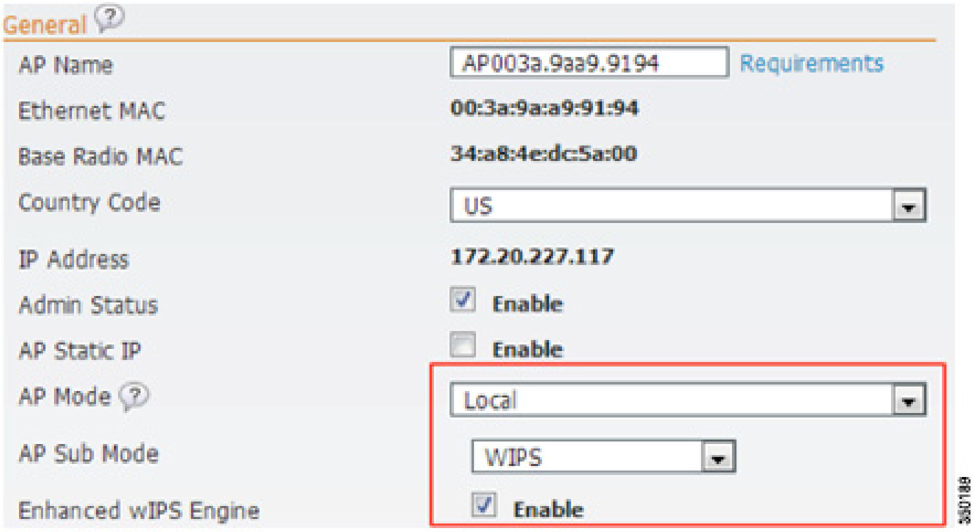
Configuring Access Points for AP3600 Local mode plus the WSSI Module

This mode is only available for a 3600 series Access Point with a WSSI module installed.

To configure access points for AP3600 local mode plus the WSSI module:

Step 1 Configure the Access Point for Local Mode:

Enter the Access Point configuration menu in PI via **Operate > Device Group > Device Type > Unified AP** and click on the Access Point's name, then **Configuration.**



General

AP Name	AP003a.9aa9.9194 Requirements
Ethernet MAC	00:3a:9a:a9:91:94
Base Radio MAC	34:a8:4e:dc:5a:00
Country Code	US
IP Address	172.20.227.117
Admin Status	☑ Enable
AP Static IP	☐ Enable
AP Mode	Local
AP Sub Mode	WIPS
Enhanced wIPS Engine	☑ Enable

350189

a. Change **AP Mode** to **Local**

b. Enable **Enhanced WIPS Engine**

c. Change **AP Sub Mode** to **WIPS**

d. Click **Save** at the bottom of the page.

e. Click **OK** when prompted to reboot the Access Point.

f. Repeat this for each Access Point that has been configured into Local Mode.

Configuring wIPS Profiles

By default, the MSE and corresponding wIPS Access Points inherit the default wIPS profile from PI. This profile comes pre-tuned with a majority of attack alarms enabled by default and will monitor attacks against Access Points within the same RF-Group as the wIPS Access Points. In this manner, the system comes pre-setup to monitor attacks against a deployment model that utilizes an integrated solution in which both the WLAN infrastructure and wIPS Access Points are intermixed on the same controller.

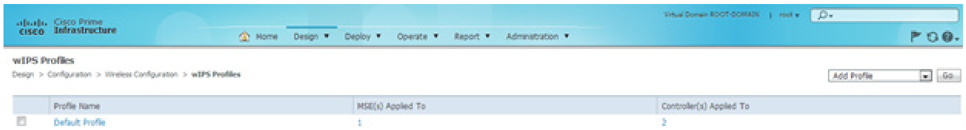
Note Some of the steps below are marked as Overlay-Only and are only to be undertaken when deploying the Adaptive wIPS solution to monitor an existing WLAN Infrastructure such as an autonomous or completely separate controller-based WLAN.

To configure wIPS profiles:

Step 1 Navigate to wIPS Profiles:

From the top-level PI menu, click **Design > Configuration > Wireless Configuration > wIPS Profiles**

Step 2 Create a new Profile:



Cisco Prime Infrastructure

Home | Design ▾ | Deploy ▾ | Operate ▾ | Report ▾ | Administration ▾

Virtual Domain ROOT-DOMAIN | root ▾

wIPS Profiles

Design > Configuration > Wireless Configuration > wIPS Profiles

Add Profile ▾ Go

	Profile Name	MSE(s) Applied To	Controller(s) Applied To
□	Default Profile	1	2

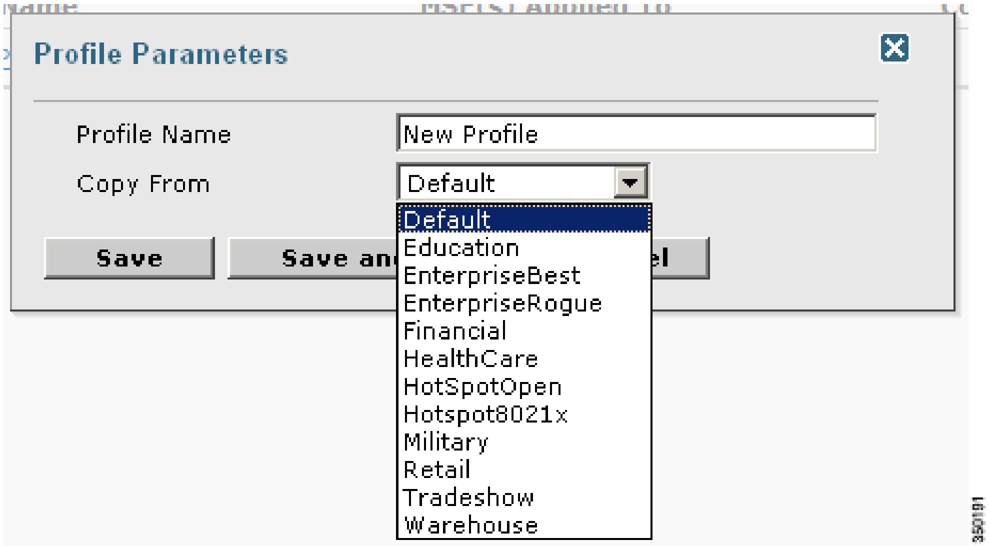
350190

Click **Profile List** on the left hand side.

Select **Add Profile** from the upper right-hand drop down menu.

Step 3 Select a profile template:

Cisco's Adaptive wIPS system comes with a pre-defined set of profile templates of which customers can use as a starting place to create their own custom profiles. Each one is tailored to a specific vertical and varies in regards to which specific alarms are enabled.



Profile Parameters

Profile Name: New Profile

Copy From: Default ▾

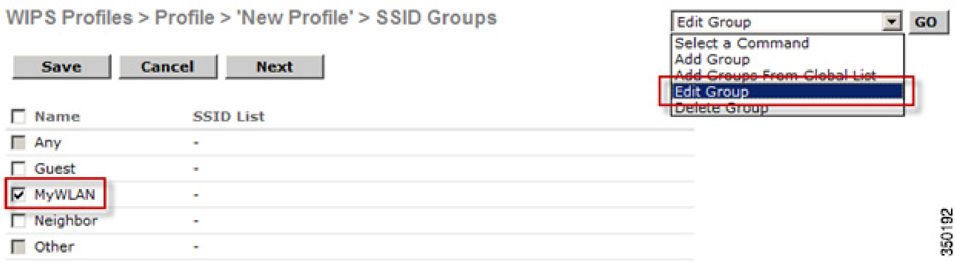
350191

After selecting a profile and providing a name, click **Save** and **Edit**

Step 4 Configure the SSIDs to Monitor (Optional):

By default, the system monitors attacks launched against the local Wireless LAN Infrastructure (as defined by APs which have the same 'RF Group' name). If the system should also be required to monitor attacks against another network, such as when deployed in an overlay deployment model, the SSID groups feature must be utilized.

If this step is not required, simply click **Next**.



WIPS Profiles > Profile > 'New Profile' > SSID Groups

Edit Group ▾ GO

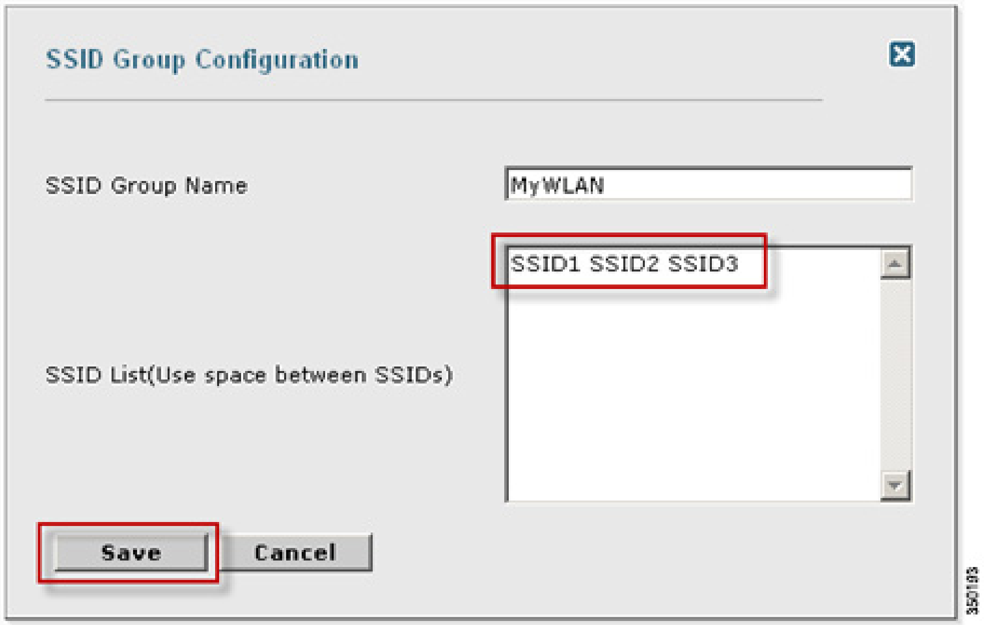
	Name	SSID List
□	Any	-
□	Guest	-
☑	MyWLAN	-
□	Neighbor	-
□	Other	-

350192

Check the box next to **MyWLAN** and select **Edit Group** from the drop down in the upper right hand corner then click **Go**.

Step 5 Enter SSIDs to Monitor (Optional):

Once again, this step is only required if the system is to be utilized to monitor attacks against a different WLAN infrastructure which is typical of an overlay deployment model.



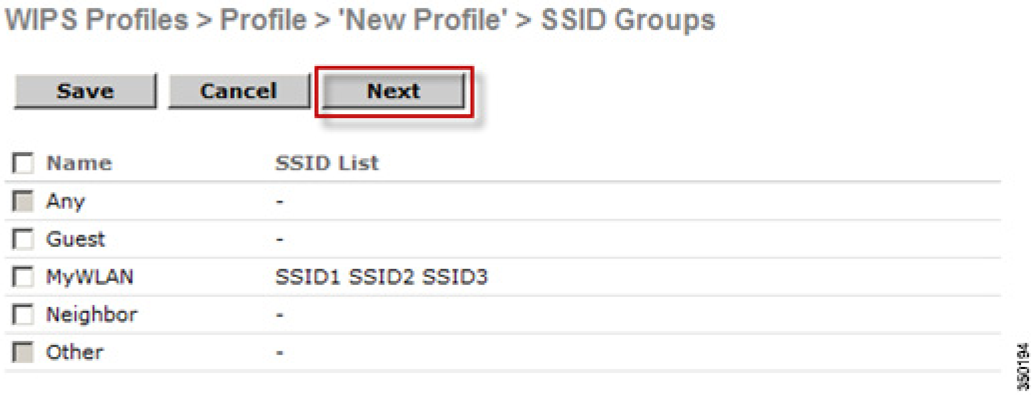
SSID Group Configuration

SSID Group Name: MyWLAN

SSID List(Use space between SSIDs): SSID1 SSID2 SSID3

Enter the SSID(s) (separated by a single space if there are more than one) and click **Save**

The SSID Groups page will now look like the following screen shot, confirming the SSID(s) were added successfully.



WIPS Profiles > Profile > 'New Profile' > SSID Groups

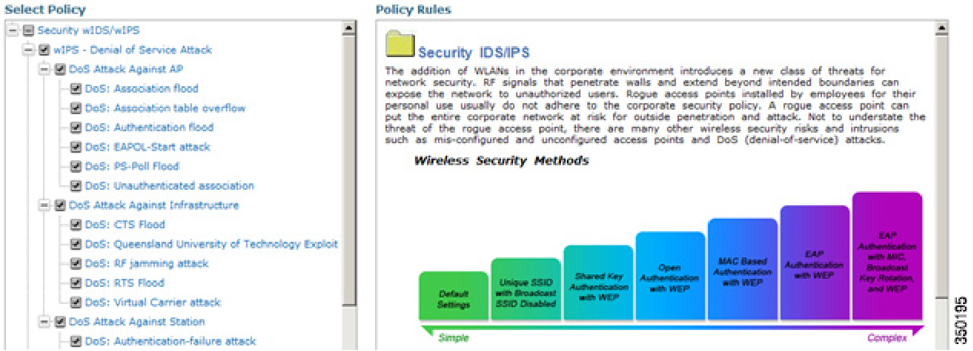
	Name	SSID List
□	Any	-
□	Guest	-
□	MyWLAN	SSID1 SSID2 SSID3
□	Neighbor	-
□	Other	-

Click **Next**

Step 6 Edit the Profile:

This configuration screen allows specific attacks to be enabled or disabled. It also permits the administrator to drill down to specific alarms and edit their specific thresholds or even turn on forensics.

To enable or disable alarms, simply click the box next to the specific alarm in question.



Select Policy

- ⊟ Security wIDS/wIPS
  - ⊟ ☑ wIPS - Denial of Service Attack
    - ⊟ ☑ DoS Attack Against AP
      - ☑ DoS: Association flood
      - ☑ DoS: Association table overflow
      - ☑ DoS: Authentication flood
      - ☑ DoS: EAPOL-Start attack
      - ☑ DoS: PS-Poll Flood
      - ☑ DoS: Unauthenticated association
    - ⊟ ☑ DoS Attack Against Infrastructure
      - ☑ DoS: CTS Flood
      - ☑ DoS: Queensland University of Technology Exploit
      - ☑ DoS: RF jamming attack
      - ☑ DoS: RTS Flood
      - ☑ DoS: Virtual Carrier attack
    - ⊟ ☑ DoS Attack Against Station
      - ☑ DoS: Authentication-failure attack

Policy Rules

Security IDS/IPS

The addition of WLANs in the corporate environment introduces a new class of threats for network security. RF signals that penetrate walls and extend beyond intended boundaries can expose the network to unauthorized users. Rogue access points installed by employees for their personal use usually do not adhere to the corporate security policy. A rogue access point can put the entire corporate network at risk for outside penetration and attack. Not to understate the threat of the rogue access point, there are many other wireless security risks and intrusions such as mis-configured and unconfigured access points and DoS (denial-of-service) attacks.

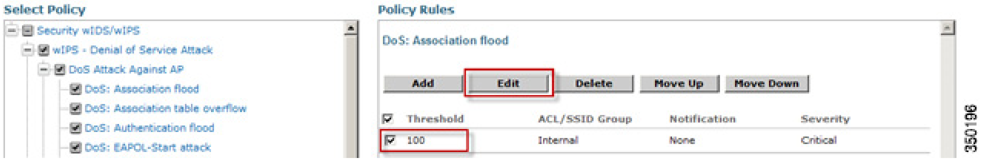
Wireless Security Methods

Default Settings
Unique SSID with Broadcast SSID Disabled
Shared Key Authentication with WEP
Open Authentication with WEP
MAC Based Authentication with WEP
EAP Authentication with WEP
EAP Authentication with MIC, Broadcast Key Rotation, and WEP
Simple
Complex
350195

To edit the policy parameters, click on an alarm, which modifies the right hand frame to represent the point configuration of that attack.

Step 7 Editing Policy Rules:

Once a specific alarm is selected, the policy rules associated to that alarm can be modified.



Select Policy

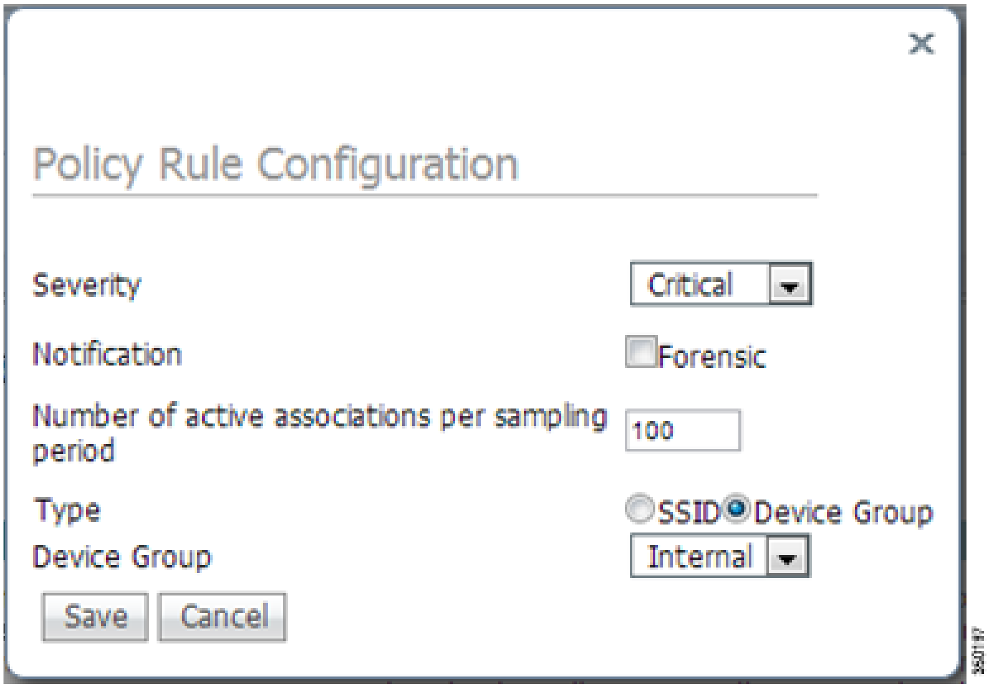
- ⊟ Security wIDS/wIPS
  - ⊟ ☑ wIPS - Denial of Service Attack
    - ⊟ ☑ DoS Attack Against AP
      - ☑ DoS: Association flood
      - ☑ DoS: Association table overflow
      - ☑ DoS: Authentication flood
      - ☑ DoS: EAPOL-Start attack

Policy Rules

DoS: Association flood

☑	Threshold	ACL/SSID Group	Notification	Severity
☑	100	Internal	None	Critical

To edit a policy rule, check the box next to the rule and click **Edit**



Policy Rule Configuration

Severity: Critical

Notification: □ Forensic

Number of active associations per sampling period: 100

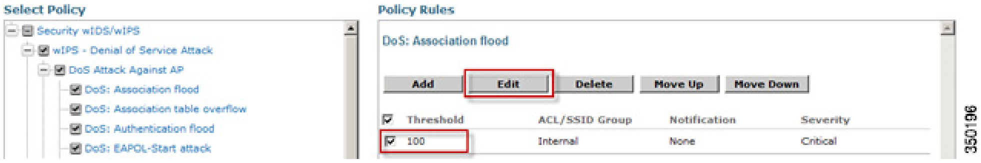
Type: ○ SSID ● Device Group

Device Group: Internal

The policy rule window allows the severity of the alarm to be modified in addition to a number of other parameters. The notification item is a check box which defines whether forensic (packet captures) are taken for this particular alarm. There is also a specific threshold for this alarm, which in this case is defined as the number of active associations but this is different for every alarm. Next, the type parameter defines what WLAN infrastructure the system will monitor attacks against. By default this is configured to **Device Group** and **Internal** which specifies all APs in the same 'RF Group' name as the wIPS APs. Changing the type to **SSID** allows the system to monitor a separate network, which is typical of an overlay deployment and this configuration is discussed below.

Step 8 Add Policy Rules (Optional):

Editing a policy rule would typically only be needed in an overlay deployment where the system is to be configured to monitor another WLAN infrastructure by SSID.



Select Policy

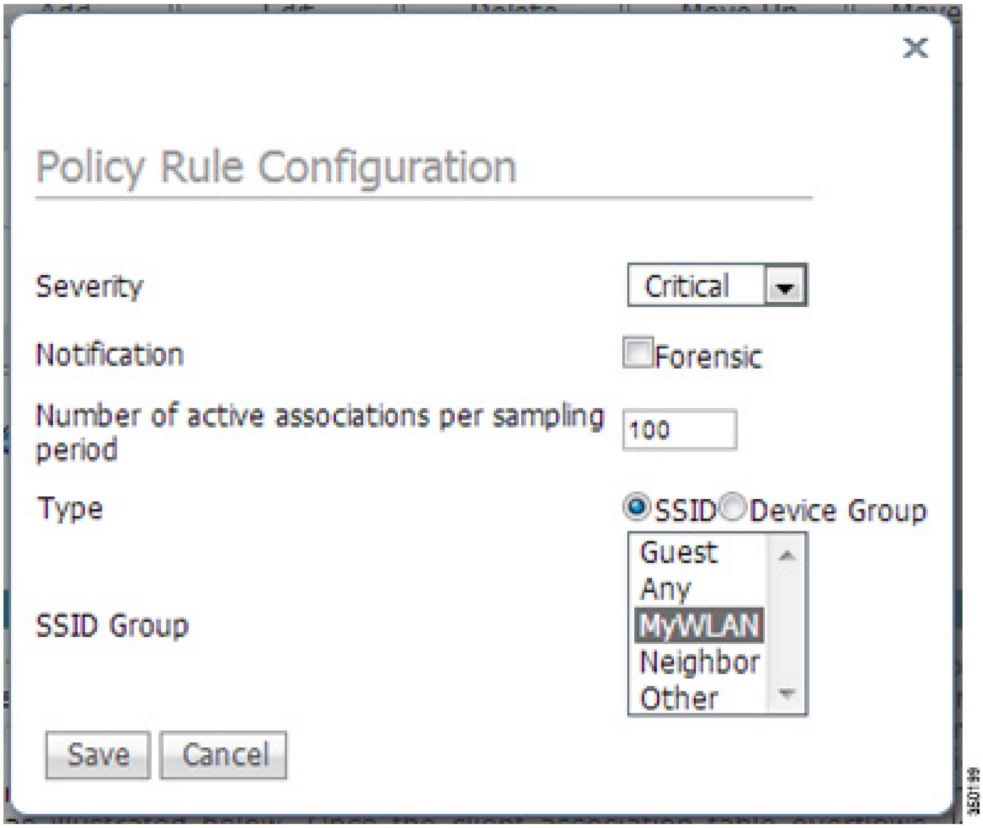
- ⊟ ▣ Security wIDS/wIPS
  - ⊟ ☑ wIPS - Denial of Service Attack
    - ⊟ ☑ DoS Attack Against AP
      - ☑ DoS: Association flood
      - ☑ DoS: Association table overflow
      - ☑ DoS: Authentication flood
      - ☑ DoS: EAPOL-Start attack

Policy Rules

DoS: Association flood

☑	Threshold	ACL/SSID Group	Notification	Severity
☑	100	Internal	None	Critical

To add a policy rule, click **Add**



Policy Rule Configuration

Severity: Critical

Notification: □ Forensic

Number of active associations per sampling period: 100

Type: ● SSID ○ Device Group

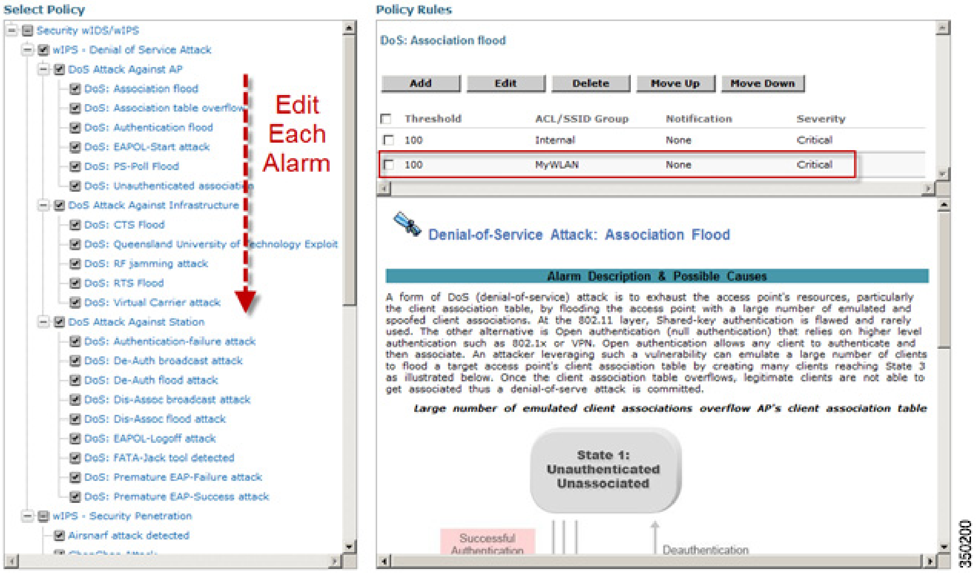
SSID Group: Guest, Any, MyWLAN, Neighbor, Other

The policy rule window allows the severity of the alarm to be modified in addition to a number of other parameters. The notification item is a check box which defines whether forensic (packet captures) are taken for this particular alarm. There is also a specific threshold for this alarm, which in this case is defined as the number of active associations but this is different for every alarm. Next, the type parameter defines what SSIDs the system will monitor. If the type is changed to 'Device Group' then the system will monitor attacks only against APs in the same 'RF Group'. In the case that 'SSID' is selected, then the system can be utilized to monitor attacks against a separate WLAN infrastructure as defined by the SSID Groups earlier in the setup.

After any changes have been made, click **Save**

Step 9 Configuring Additional Policy Rules (Optional):

If the system is to be configured to monitor another WLAN infrastructure by SSID, then changes will need to be made for each and every policy rule to monitor by SSID. A policy rule will need to created under each separate alarm which defines the system to monitor attacks against the SSID Group created earlier.


Select Policy
Security wIDS/wIPS
wIPS - Denial of Service Attack
DoS Attack Against AP
DoS: Association flood
DoS: Association table overflow
DoS: Authentication flood
DoS: EAPOL-Start attack
DoS: PS-Poll Flood
DoS: Unauthenticated association
DoS Attack Against Infrastructure
DoS: CTS Flood
DoS: Queensland University of Technology Exploit
DoS: RF jamming attack
DoS: RTS Flood
DoS: Virtual Carrier attack
DoS Attack Against Station
DoS: Authentication-failure attack
DoS: De-Auth broadcast attack
DoS: De-Auth flood attack
DoS: Dis-Assoc broadcast attack
DoS: Dis-Assoc flood attack
DoS: EAPOL-Logoff attack
DoS: FATA-Jack tool detected
DoS: Premature EAP-Failure attack
DoS: Premature EAP-Success attack
wIPS - Security Penetration
Airsnarf attack detected
Edit
Each
Alarm
Policy Rules
DoS: Association flood
Add
Edit
Delete
Move Up
Move Down
State 1:
Unauthenticated
Unassociated
Successful
Authentication
Deauthentication
350200

□	Threshold	ACL/SSID Group	Notification	Severity
□	100	Internal	None	Critical
□	100	MyWLAN	None	Critical

Denial-of-Service Attack: Association Flood

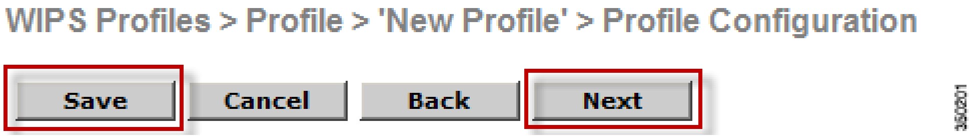
Alarm Description & Possible Causes

A form of DoS (denial-of-service) attack is to exhaust the access point's resources, particularly the client association table, by flooding the access point with a large number of emulated and spoofed client associations. At the 802.11 layer, Shared-key authentication is flawed and rarely used. The other alternative is Open authentication (null authentication) that relies on higher level authentication such as 802.1x or VPN. Open authentication allows any client to authenticate and then associate. An attacker leveraging such a vulnerability can emulate a large number of clients to flood a target access point's client association table by creating many clients reaching State 3 as illustrated below. Once the client association table overflows, legitimate clients are not able to get associated thus a denial-of-serve attack is committed.

Large number of emulated client associations overflow AP's client association table

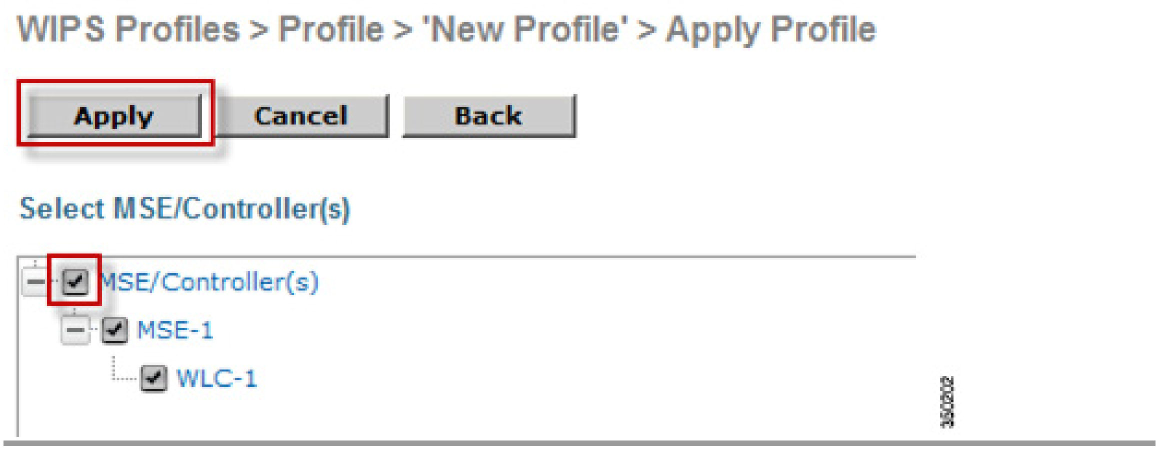
Step 10 Save the Profile:

After any changes are made, click **Save** to save the profile on Prime Infrastructure and then click **Next** when done.


WIPS Profiles > Profile > 'New Profile' > Profile Configuration
Save
Cancel
Back
Next
350201

Step 11 Apply the Profile:

Select the MSE/Controller combinations to apply the profile to and then click **Apply**.



WIPS Profiles > Profile > 'New Profile' > Apply Profile

Select MSE/Controller(s)

- ☑ MSE/Controller(s)
  - ☑ MSE-1
    - ☑ WLC-1

Disabling Controller-based IDS

Once the Adaptive wIPS system has been pervasively installed across the entire area to be monitored, it is recommended that Cisco's traditional Wireless LAN Controller IDS be disabled. Executing this step prevents duplicate alerts being triggered on both the Adaptive wIPS and existing IDS systems.

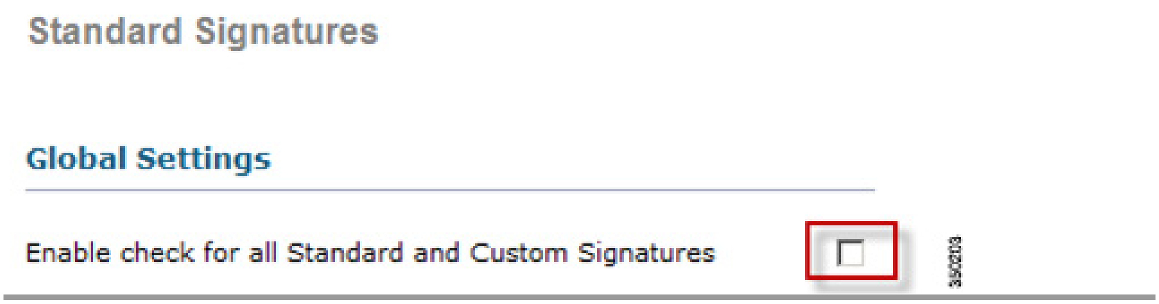
To disable controller-based IDS:

Step 1 Login to the Controller(s).

Step 2 Click on the **Security** tab from the top-level controller menu.

Step 3 On the left hand-side, click **Wireless Protection Policies > Standard Signatures**

Step 4 Uncheck the standard signatures as depicted in the below screenshot.



Standard Signatures

Global Settings

Enable check for all Standard and Custom Signatures □