

自適應wIPS ELM配置和部署指南

目錄

[簡介](#)

[必要條件](#)

[需求](#)

[採用元件](#)

[慣例](#)

[ELM wIPS警報流程](#)

[ELM的部署注意事項](#)

[ELM與專用MM](#)

[通道內和通道外效能](#)

[跨WAN連結的ELM](#)

[CleanAir整合](#)

[ELM的功能和優點](#)

[ELM授權](#)

[使用WCS配置ELM](#)

[從WLC進行配置](#)

[在ELM中檢測到的攻擊](#)

[排除ELM故障](#)

[相關資訊](#)

簡介

思科自適應無線入侵防禦系統(wIPS)解決方案新增了增強型本地模式(ELM)功能，允許管理員使用其已部署的接入點(AP)提供全面保護，而無需單獨的重疊網路(圖1)。在ELM之前和傳統自適應wIPS部署中，需要專用監控模式(MM)AP來提供PCI合規性需求或保護，防止未經授權的安全訪問、滲透和攻擊(圖2)。ELM有效地提供同類產品，簡化無線安全實施，同時降低資本支出和運營成本。本文檔僅重點介紹ELM，不會修改任何現有wIPS部署優勢(使用MM AP)。

圖1 — 增強型本地模式接入點部署

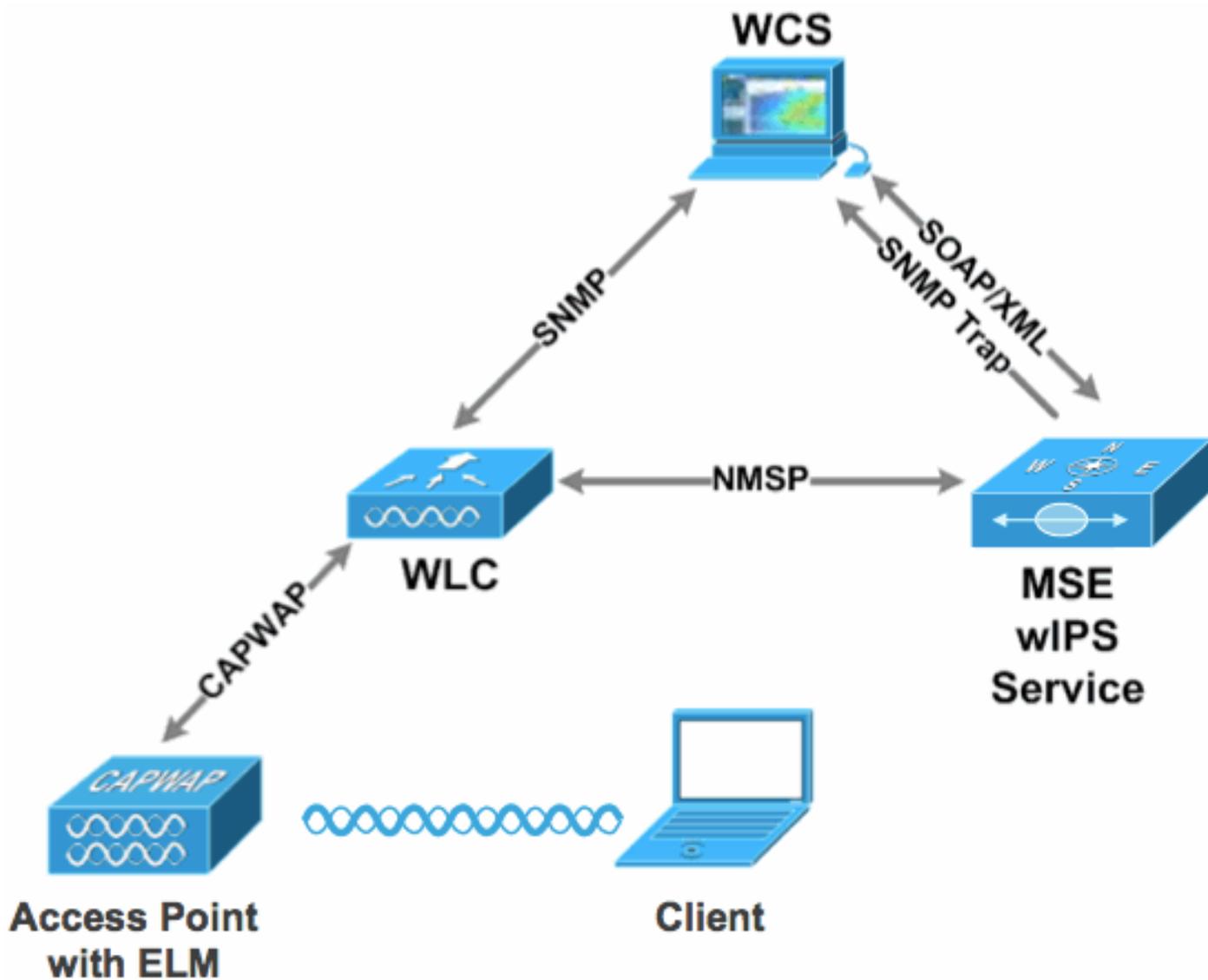
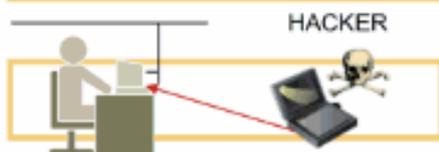


圖2 — 主要的無線安全威脅

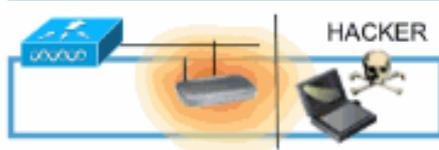
On-Wire Attacks

Ad-hoc Wireless Bridge



Client-to-client backdoor access

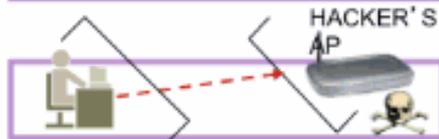
Rogue Access Points



Backdoor network access

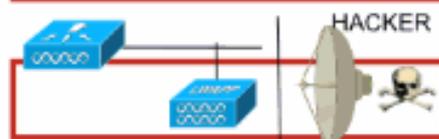
Over-the-Air Attacks

Evil Twin/Honeytrap AP



Connection to malicious AP

Reconnaissance



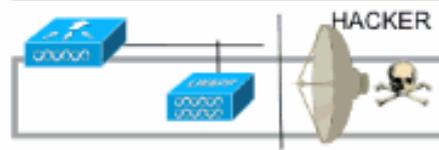
Seeking network vulnerabilities

Denial of Service



Service disruption

Cracking Tools



Sniffing and eavesdropping

必要條件

需求

本文件沒有特定需求。

採用元件

ELM必需元件和最低代碼版本

- 無線LAN控制器(WLC)- 7.0.116.xx版或更高版本
- AP - 7.0.116.xx版或更高版本
- 無線控制系統(WCS)- 7.0.172.xx版或更高版本
- 移動服務引擎 — 7.0.201.xx版或更高版本

支援WLC平台

WLC5508、WLC4400、WLC 2106、WLC2504、WiSM-1和WiSM-2WLC平台支援ELM。

支援AP

11n AP支援ELM，包括3500、1250、1260、1040和1140。

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路正在作用，請確保您已瞭解任何指令可能造成的影響。

慣例

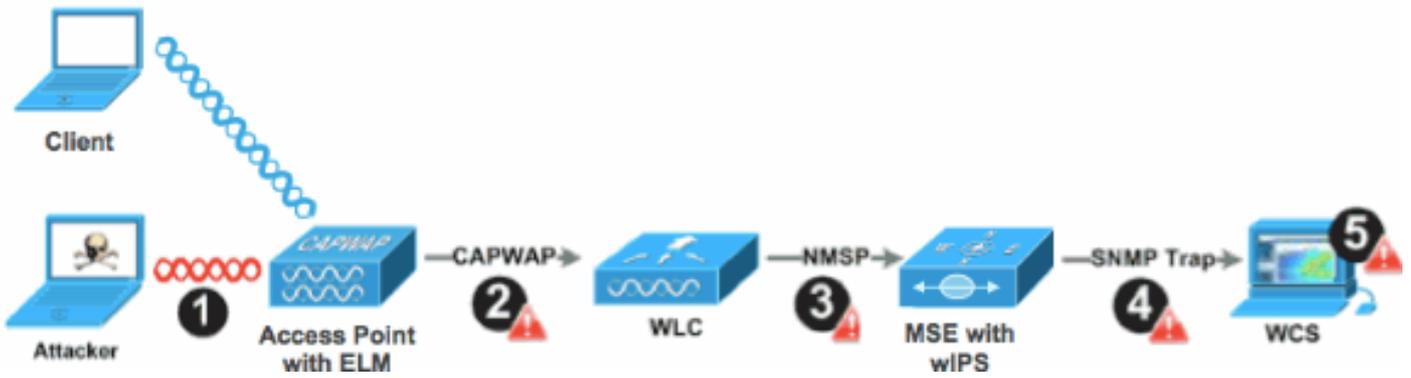
如需文件慣例的詳細資訊，請參閱[思科技術提示慣例](#)。

ELM wIPS警報流程

只有當攻擊發生在受信任的基礎設施AP上時，攻擊才相關。ELM AP將檢測並與控制器通訊，並與MSE關聯以便通過WCS管理進行報告。[圖3](#)從管理員的角度提供了警報流程：

1. 對基礎設施裝置（「受信任」AP）發起的攻擊
2. 在通過CAPWAP與WLC通訊的ELM AP上檢測到
3. 通過NMSP透明地傳遞給MSE
4. 在MSE上登入wIPS資料庫通過SNMP陷阱傳送到WCS
5. 在WCS顯示

圖3 — 威脅檢測和警報流程



ELM的部署注意事項

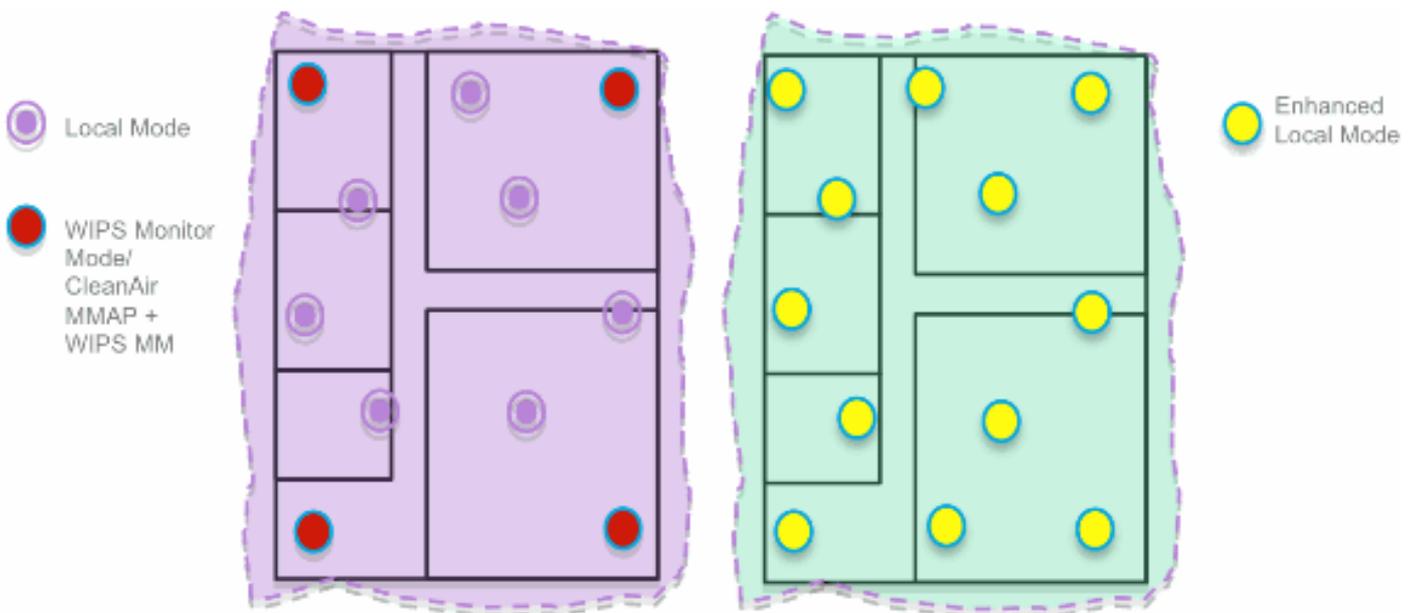
思科建議，當考慮網路重疊和/或成本時，通過在網路上的每個AP上啟用ELM來滿足大多數客戶的安全需求。ELM主要功能可在不降低資料、語音和影片客戶端及服務效能的情況下有效應對通道攻擊。

ELM與專用MM

圖4提供了wIPS MM AP標準部署與ELM標準部署之間的常規對比。綜上所述，這兩種模式的典型覆蓋範圍都表明：

- 專用wIPS MM AP通常覆蓋15,000-35,000平方英尺
- 客戶端服務的AP通常覆蓋面積在3,000-5,000平方英尺

圖4 - MM與所有ELM AP的重疊



在傳統的自適應wIPS部署中，思科建議每5個本地模式AP配置1 MM的AP，此比例也可能因網路設計和專家指導的最佳覆蓋範圍而異。通過考慮ELM，管理員只需為所有現有AP啟用ELM軟體功能，從而在保持效能的同時有效地將MM wIPS操作新增到本地資料服務模式AP。

通道內和通道外效能

MM AP利用無線電100%的時間掃描所有通道，因為它不為任何WLAN客戶端提供服務。ELM的主要功能可在不降低資料、語音和影片客戶端及服務效能的情況下，有效應對通道內攻擊。主要區別在於本地模式變化的脫離通道掃描；根據活動情況，脫離通道掃描提供最小停留時間，以收集足夠的可用於分類和確定攻擊的資訊。例如，與關聯的語音客戶端有關，其中AP的RRM掃描會延遲，直到取消關聯語音客戶端，以確保服務不受影響。出於此考慮，非通道期間ELM檢測被認為是盡最大努力。在所有、國家/地區或DCA通道上運行的相鄰ELM AP提高了有效性，因此建議在每個本地模式AP上啟用ELM，以獲得最大保護覆蓋範圍。如果要求在所有通道上全時進行專用掃描，則建議部署MM AP。

以下要點回顧本地模式和MM AP的差異：

- 本地模式AP — 為WLAN客戶端提供分時離通道掃描，每個通道監聽50毫秒，並為所有/國家/地區/DCA通道提供可配置的掃描。
- 監控模式AP — 不為WLAN客戶端提供服務（僅專門用於掃描），偵聽每個通道上的1.2秒，並掃描所有通道。

跨WAN連結的ELM

思科已做出巨大努力，以便在各種挑戰性場景中最佳化功能，例如跨低頻寬WAN鏈路部署ELM AP。ELM功能包括確定AP上的攻擊特徵碼的預處理，並經過最佳化以適用於慢速鏈路。作為最佳實踐，建議測試和測量基準，以驗證通過WAN使用ELM的效能。

CleanAir整合

ELM功能高度補充了CleanAir運營，其效能和優勢與部署MM AP相似，並具有以下現有CleanAir頻譜感知優勢：

- 專用矽級RF智慧
- 頻譜感知、自我修復和自我最佳化
- 非標準通道威脅和干擾檢測和緩解
- 非Wi-Fi檢測，例如藍芽、微波、無繩電話等。
- 檢測和定位RF層DOS攻擊（例如RF干擾器）

ELM的功能和優點

- 資料服務本地和H-REAP中的自適應wIPS掃描
- 無需單獨的重疊網路的保護
- 可供現有wIPS客戶免費下載軟體

- 支援無線區域網的PCI合規性
- 完整的802.11和非802.11攻擊檢測
- 增加調查分析和報告功能
- 與現有的CUWM和WLAN管理整合
- 靈活設定整合或專用MM AP
- AP的預處理，可最大程度地減少資料回傳（即，在極低頻寬鏈路上工作）
- 對服務資料的影響較小

ELM授權

ELM wIPS在訂購中增加了一個新許可證：

- AIR-LM-WIPS-xx - Cisco ELM wIPS許可證
- AIR-WIPS-AP-xx - Cisco無線wIPS許可證

其他ELM許可說明：

- 如果已安裝wIPS MM AP許可證SKU，則這些許可證也可以用於ELM AP。
- wIPS許可證和ELM許可證一起計入wIPS引擎的平台許可證限制；3310上分別為2000個AP，335x上分別為3000個AP。
- 評估許可證包括10個wIPS接入點和10個ELM接入點，有效期最長為60天。在ELM之前，評估許可證最多允許20個wIPS MM AP。必須滿足支援ELM的軟體版本的最低要求。

使用WCS配置ELM

圖5 — 使用WCS配置ELM

AP Name	Ethernet MAC	IP Address	Radio	Map Location	Controller	Client Count	Admin Status	AP Mode
<input type="checkbox"/> demo-AP3502i-S	00:22:90:e3:37:dc	10.10.20.103	802.11b/g/n	System Campus > BuildingS1 > 1st Floor	10.10.10.5	0	Enabled	Local
<input type="checkbox"/> demo-AP3502i-S	00:22:90:e3:37:dc	10.10.20.103	802.11a/b	System Campus > BuildingS1 > 1st Floor	10.10.10.5	0	Enabled	Local
<input type="checkbox"/> demo-AP1260	f8:66:f2:ab:1f:96	10.10.20.113	802.11b/g/n	System Campus > BuildingS1 > 1st Floor	10.10.10.5	0	Enabled	Local
<input type="checkbox"/> demo-AP1260	f8:66:f2:ab:1f:96	10.10.20.113	802.11a/b	System Campus > BuildingS1 > 1st Floor	10.10.10.5	0	Enabled	Local
<input type="checkbox"/> demo-AP3502i-J	04:7d:4f:3a:ed:48	10.10.20.105	802.11b/g/n	System Campus > BuildingS1 > 1st Floor	10.10.10.5	0	Enabled	Local
<input type="checkbox"/> demo-AP3502i-J	04:7d:4f:3a:ed:48	10.10.20.105	802.11a/b	System Campus > BuildingS1 > 1st Floor	10.10.10.5	0	Enabled	Local
<input type="checkbox"/> demo-AP3502i-MM	04:7d:4f:3a:06:62	10.10.20.114	802.11b/g/n	System Campus > BuildingS1 > 1st Floor	Not Associated	0	Enabled	H-REAP
<input type="checkbox"/> demo-AP3502i-MM	04:7d:4f:3a:06:62	10.10.20.114	802.11a/b	System Campus > BuildingS1 > 1st Floor	Not Associated	1	Enabled	H-REAP
<input type="checkbox"/> demo-AP1142n	00:22:90:90:99:ef	10.10.20.111	802.11b/g/n	System Campus > BuildingS1 > 1st Floor	Not Associated	0	Enabled	H-REAP
<input type="checkbox"/> demo-AP1142n	00:22:90:90:99:ef	10.10.20.111	802.11a/b	System Campus > BuildingS1 > 1st Floor	Not Associated	0	Enabled	H-REAP
<input type="checkbox"/> demo-AP1262N-FR	f8:66:f2:67:68:93	10.10.20.102	802.11b/g/n	System Campus > BuildingS1 > 1st Floor	10.10.10.5	0	Enabled	H-REAP
<input type="checkbox"/> demo-AP1262N-FR	f8:66:f2:67:68:93	10.10.20.102	802.11a/b	System Campus > BuildingS1 > 1st Floor	10.10.10.5	0	Enabled	H-REAP

1. 在WCS中，在啟用「增強型wIPS引擎」之前禁用AP的802.11b/g和802.11a無線電。

注意：將斷開所有關聯客戶端的連線，並且在啟用無線電之前不會加入。

2. 配置一個AP，或者對多個輕量AP使用WCS配置模板。請參見圖6。

圖6 — 啟用增強型wIPS引擎(ELM)子模式

Access Point Detail : demo-AP3502i-S
Configure > Access Points > Access Point Detail

General

AP Name: demo-AP3502i-S [Requirements](#)

Ethernet MAC: 00:22:90:e3:37:dc

Base Radio MAC: 00:22:90:90:99:ef

Country Code: US

IP Address: 10.10.20.103

Admin Status: Enable

AP Static IP: Enable

AP Mode: Local

Enhanced wIPS Engine: Enable

AP Failover Priority: Low

Registered Controller: 10.10.10.5

Primary Controller Name: wlc

Access Point Detail : demo-AP1142n
Configure > Access Points > Access Point Detail

H-REAP settings cannot be changed when AP is enabled.

General

AP Name: demo-AP1142n [Requirements](#)

Ethernet MAC: 00:22:90:90:99:ef

Base Radio MAC: 00:22:90:93:4a:50

Country Code: US

IP Address: 10.10.20.101

Admin Status: Enable

AP Static IP: Enable

AP Mode: H-REAP

Enhanced wIPS Engine: Enable

AP Failover Priority: Medium

Registered Controller: 10.10.10.5

Primary Controller Name: wlc

3. 選擇Enhanced wIPS Engine，然後按一下Save。

a. 啟用增強型wIPS引擎不會導致AP重新啟動。

b. 支援H-REAP；啟用與本地模式AP相同的方法。

注意：如果啟用了此AP的其中一個無線電，WCS將忽略配置並引發圖7中的錯誤。

圖7 — 啟用ELM之前禁用AP無線電的WCS提醒

The page at https://172.20.227.169 says:



Please make sure all the radios are disabled.

OK

- 通過觀察AP模式從「Local or H-REAP」更改為Local/wIPS或H-REAP/wIPS，可以驗證配置是否成功。請參見圖8。

圖8 - WCS顯示AP模式以包括wIPS與本地和/或H-REAP

	AP Name	Ethernet MAC	IP	Admin Status	AP Mode
<input type="checkbox"/>	demo-AP3502i-S	00:22:90:e3:37:dc	10	Enabled	Local/wIPS
<input type="checkbox"/>	demo-AP3502i-S	00:22:90:e3:37:dc	10	Enabled	Local/wIPS
<input type="checkbox"/>	demo-AP1260	f8:66:f2:ab:1f:96	10	Enabled	Local/wIPS
<input type="checkbox"/>	demo-AP1260	f8:66:f2:ab:1f:96	10	Enabled	Local/wIPS
<input type="checkbox"/>	demo-AP3502i-J	c4:7d:4f:3a:ed:48	10	Enabled	Local/wIPS
<input type="checkbox"/>	demo-AP3502i-J	c4:7d:4f:3a:ed:48	10	Enabled	Local/wIPS
<input type="checkbox"/>	demo-AP3502i-MM	c4:7d:4f:3a:06:62	10	Enabled	H-REAP/wIPS
<input type="checkbox"/>	demo-AP3502i-MM	c4:7d:4f:3a:06:62	10	Enabled	H-REAP/wIPS
<input type="checkbox"/>	demo-AP1142n	00:22:90:90:99:6f	10	Enabled	H-REAP/wIPS
<input type="checkbox"/>	demo-AP1142n	00:22:90:90:99:6f	10	Enabled	H-REAP/wIPS
<input type="checkbox"/>	demo-AP1262N-FB	f8:66:f2:67:68:93	10	Enabled	H-REAP/wIPS
<input type="checkbox"/>	demo-AP1262N-FB	f8:66:f2:67:68:93	10	Enabled	H-REAP/wIPS

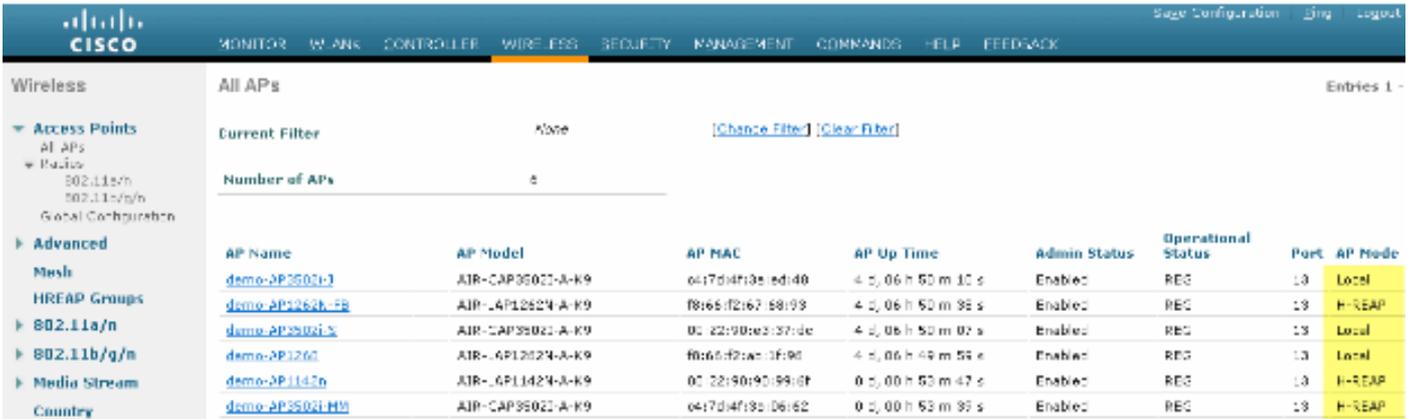
- 啟用在步驟1中禁用的無線電。

6. 建立wIPS設定檔並將其推送到控制器，以便完成組態。

注意：有關wIPS的完整配置資訊，請參閱[Cisco自適應wIPS部署指南](#)。

從WLC進行配置

圖9 — 使用WLC配置ELM

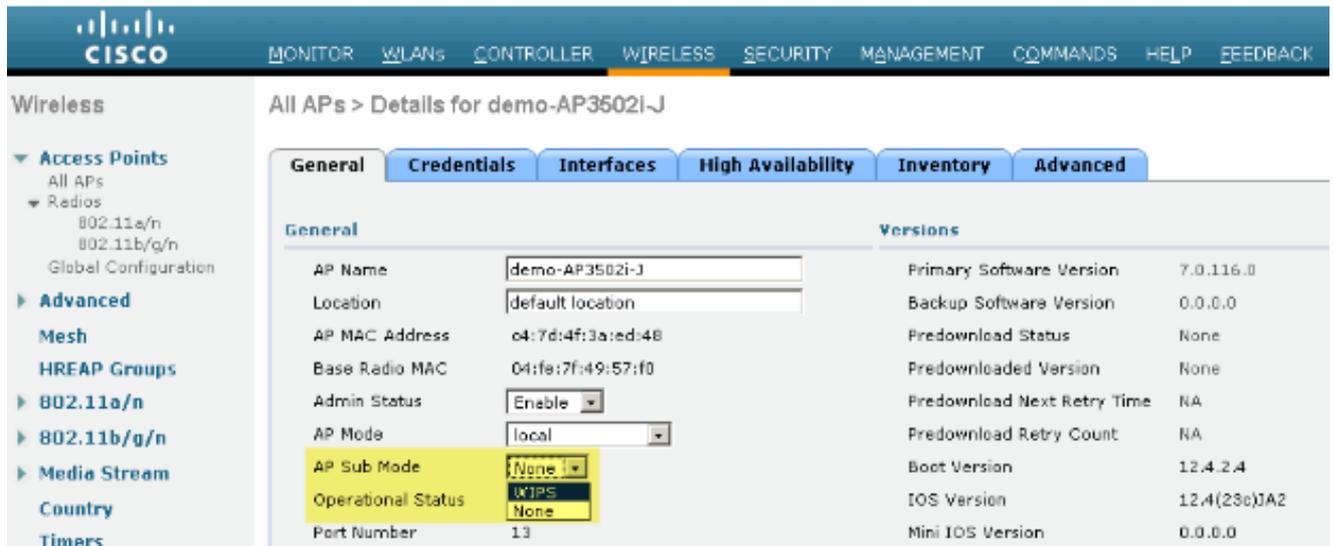


The screenshot shows the Cisco WLC 'Wireless' page. The 'All APs' section is active, displaying a table of APs. The table has columns for AP Name, AP Model, AP MAC, AP Up Time, Admin Status, Operational Status, Port, and AP Mode. The AP Mode column shows 'Local' for most APs, with one highlighted in yellow.

AP Name	AP Model	AP MAC	AP Up Time	Admin Status	Operational Status	Port	AP Mode
demo-AP3502i-J	AIR-CAP3502i-A-K9	047d4f13e-ed48	4 d, 06 h 50 m 10 s	Enabled	REC	13	Local
demo-AP1262b-EB	AIR-CT1262b-A-K9	f866f2167-68f93	4 d, 06 h 50 m 35 s	Enabled	REC	13	H-REAP
demo-AP3502i-S	AIR-CAP3502i-A-K9	0c-22-90e2-371de	4 d, 06 h 50 m 07 s	Enabled	REC	13	Local
demo-AP1260	AIR-CT1262b-A-K9	f866f2167-68f93	4 d, 06 h 49 m 54 s	Enabled	REC	13	Local
demo-AP1145n	AIR-CT1142n-A-K9	0c-22-90e2-371de	0 d, 00 h 53 m 47 s	Enabled	REC	13	H-REAP
demo-AP3502i-HV	AIR-CAP3502i-A-K9	047d4f13e-d6162	0 d, 00 h 53 m 35 s	Enabled	REC	13	H-REAP

1. 從Wireless頁籤中選擇AP。

圖10 - WLC將AP子模式更改為包含wIPS ELM



The screenshot shows the 'All APs > Details for demo-AP3502i-J' configuration page. The 'General' tab is selected. The 'AP Sub Mode' dropdown menu is open, showing 'None', 'wIPS', and 'None' as options. The 'wIPS' option is highlighted in yellow.

General	Credentials	Interfaces	High Availability	Inventory	Advanced
General		Versions			
AP Name	demo-AP3502i-J	Primary Software Version	7.0.116.0		
Location	default location	Backup Software Version	0.0.0.0		
AP MAC Address	04:7d:4f:3a:ed:48	Predownload Status	None		
Base Radio MAC	04:fe:7f:49:57:f0	Predownload Version	None		
Admin Status	Enable	Predownload Next Retry Time	NA		
AP Mode	local	Predownload Retry Count	NA		
AP Sub Mode	wIPS	Boot Version	12.4.2.4		
Operational Status	None	IOS Version	12.4(23c)JA2		
Port Number	13	Mini IOS Version	0.0.0.0		

2. 在「AP Sub Mode」下拉選單中，選擇wIPS(圖10)。

3. 應用，然後儲存配置。

注意：要使ELM功能正常工作，需要wIPS許可的MSE和WCS。僅從WLC更改AP子模式不會啟用ELM。

在ELM中檢測到的攻擊

表1 - wIPS簽名支援清單

檢測到的攻擊	ELM	MM
針對AP的DoS攻擊		
關聯泛洪	Y	Y
關聯表溢位	Y	Y
身份驗證泛洪	Y	Y
EAPOL-Start攻擊	Y	Y
PS-Poll泛洪	Y	Y
探測請求泛洪	否	Y
未經驗證的關聯	Y	Y
針對基礎設施的DoS攻擊		
CTS泛洪	否	Y
昆士蘭工業大學開發	否	Y
RF干擾	Y	Y
RTS泛洪	否	Y
虛擬運營商攻擊	否	Y
DoS攻擊工作站		
Authentication-failure攻擊	Y	Y
阻止ACK泛洪	否	Y
De-Auth廣播泛洪	Y	Y
De-Auth flood	Y	Y
Dis-Assoc廣播泛洪	Y	Y
Dis-Assoc泛洪	Y	Y
EAPOL-Logoff攻擊	Y	Y
FATA-Jack工具	Y	Y
過早的EAP失敗	Y	Y
EAP未成熟成功	Y	Y
安全滲透攻擊		
檢測到ASLEAP工具	Y	Y
Airsnarf攻擊	否	Y
ChopChop攻擊	Y	Y
由WLAN安全異常引起的零日攻擊	否	Y
由裝置安全異常引起的零日攻擊	否	Y
AP的裝置探測	Y	Y

對EAP方法的字典攻擊	Y	Y
針對802.1x身份驗證的EAP攻擊	Y	Y
檢測到虛假AP	Y	Y
檢測到假冒DHCP伺服器	否	Y
檢測到快速WEP裂紋工具	Y	Y
分段攻擊	Y	Y
檢測到Honeypot AP	Y	Y
檢測到Hotspotter工具	否	Y
廣播幀不正確	否	Y
檢測到格式錯誤的802.11資料包	Y	Y
中間襲擊者	Y	Y
檢測到Netstumbler	Y	Y
檢測到Netstumbler受害者	Y	Y
檢測到PSPF違規	Y	Y
檢測到軟接入點或主機AP	Y	Y
檢測到偽裝MAC地址	Y	Y
檢測到可疑的課後流量	Y	Y
按供應商清單進行未經授權的關聯	否	Y
檢測到未經授權的關聯	Y	Y
已檢測到Wellenreiter	Y	Y

注意：新增CleanAir還將啟用對非802.11攻擊的檢測。

圖11 - WCS wIPS配置檔案檢視

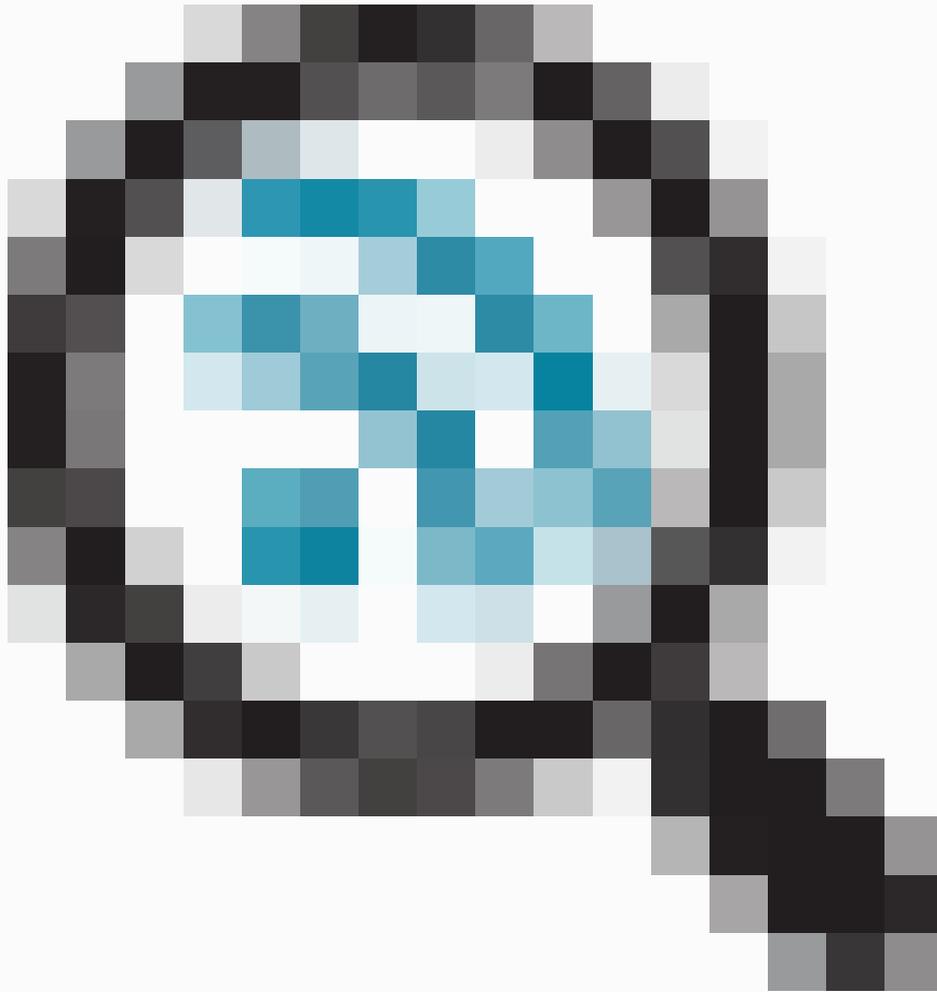
Profile Configuration

Configure > [wIPS Profiles](#) > wips-elm > **Profile Configuration**

Select Policy

- DoS: Block ACK flood 
- DoS: De-Auth broadcast flood
- DoS: De-Auth flood
- DoS: Dis-Assoc broadcast flood
- DoS: Dis-Assoc flood
- DoS: EAPOL-Logoff attack
- DoS: FATA-Jack tool
- DoS: Premature EAP-Failure
- DoS: Premature EAP-Success
- wIPS - Security Penetration
 - ASLEAP tool detected
 - Airsnarf attack 

Available only in Monitor Mode



在圖11中，從WCS配置wIPS配置檔案，該圖示表示只有在AP位於MM中時才會檢測到攻擊，而只有在ELM中時才會檢測到攻擊。

排除ELM故障

查看以下項目：

- 確保配置了NTP。
- 確保MSE時間設定採用UTC。
- 如果裝置組不工作，請將重疊配置檔案SSID與Any一起使用。重新啟動AP。
- 確保配置了許可（當前ELM AP使用KAM許可證）
- 如果wIPS配置檔案更改過於頻繁，請再次同步MSE控制器。確保配置檔案在WLC上處於活動狀態。
- 使用MSE CLI確保WLC是MSE的一部分：
 1. 通過SSH或telnet連線到您的MSE。

2. Execute `/opt/mse/wips/bin/wips_cli` — 此控制檯可用於訪問以下命令，以收集有關自適應wIPS系統狀態的資訊。
3. `show wlc all` - wIPS主控台內部問題。此命令用於驗證與MSE上的wIPS服務進行主動通訊的控制器。請參見圖12。

圖12 - MSE CLI使用MSE wIPS服務驗證WLC是否處於活動狀態

```
<#root>
wIPS>
show wlc all
```

WLC MAC	Profile	Profile
Status	IP	
Onx Status	Status	
00:21:55:06:F2:80	WCS-Default	Policy
active on controller	172.20.226.197	
Active		

- 確保使用MSE CLI在MSE上檢測到警報。
 - `show alarm list` - wIPS控制檯內問題。此命令用於列出wIPS服務資料庫中當前包含的警報。金鑰欄位是分配給特定警報的唯一雜湊金鑰。Type欄位是警報的型別。圖13中的此圖表顯示了警報ID清單和說明：

圖13 - MSE CLI `show alarm list`命令

```
<#root>
wIPS>
show alarm list
```

Key	Type	Src MAC	Active	First Time
LastTime				
89	89	00:00:00:00:00:00		2008/09/04
18:19:26	2008/09/07	02:16:58	1	
65631	95	00:00:00:00:00:00		2008/09/04
17:18:31	2008/09/04	17:18:31	0	
1989183	99	00:1A:1E:80:5C:40		2008/09/04
18:19:44	2008/09/04	18:19:44	0	

First Time和Last Time欄位表示檢測到警報的時間戳；這些時間戳以UTC時間儲存。如

果當前檢測到警報，則「活動」欄位會突出顯示。

- 清除MSE資料庫。
 - 如果遇到MSE資料庫已損壞或者沒有其他故障排除方法可用的情況，最好清除資料庫並重新開始。

圖14 - MSE Services命令

1. /etc/init.d/msed stop
2. Remove the database using the command 'rm /opt/mse/locserver/db/linux/server-eng.db'
3. /etc/init.d/msed start

相關資訊

- [思科無線LAN控制器組態設定指南7.0.116.0版](#)
- [思科無線控制系統配置指南7.0.172.0版](#)
- [技術支援與文件 - Cisco Systems](#)

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。