

# Configuratie- en implementatiegids voor adaptieve IPS ELM

## Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Conventies](#)

[ELM met IPS-alarmstroom](#)

[Implementatieoverwegingen voor ELM](#)

[ELM vs speciale MM](#)

[On-Channel en Off-Channel prestaties](#)

[ELM via WAN-links](#)

[Integratie met CleanAir](#)

[ELM-functies en -voordelen](#)

[ELM-licentiëring](#)

[ELM configureren met WCS](#)

[Configuratie vanuit WLC](#)

[Aanvallen gedetecteerd in ELM](#)

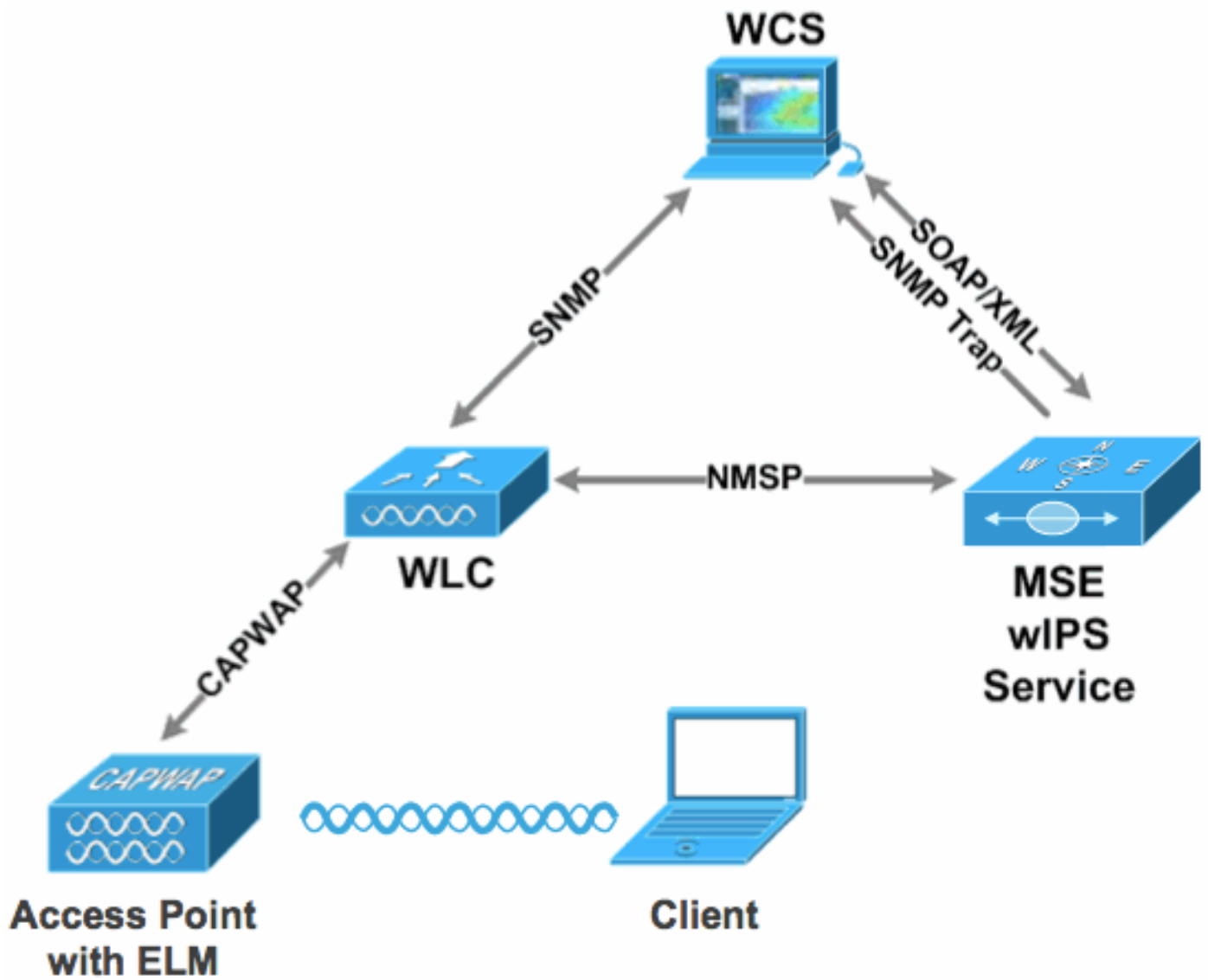
[Probleemoplossing ELM](#)

[Gerelateerde informatie](#)

## [Inleiding](#)

De Cisco Adaptieve Wireless Inbraakpreventiesysteem (IPS) oplossing voegt de functie Enhanced Local Mode (ELM) toe, waarmee beheerders hun geïmplementeerde access points (AP's) kunnen gebruiken om uitgebreide bescherming te bieden zonder dat er een afzonderlijk overlay-netwerk nodig is ([afbeelding 1](#)). Voorafgaand aan ELM en in de traditionele adaptieve IPS-implementatie, zijn er speciale AP's in de monitormodus (MM) nodig om PCI-nalevingsbehoeften te bieden of bescherming te bieden tegen onbevoegde toegang tot beveiliging, penetratie en aanvallen ([afbeelding 2](#)). ELM biedt effectief een vergelijkbaar aanbod dat de implementatie van draadloze beveiliging vergemakkelijkt en de kosten van CapEx en OpEx verlaagt. Dit document concentreert zich alleen op ELM en wijzigt geen bestaande IPS-implementatievoordelen met MPLS.

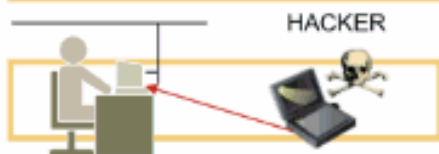
**Afbeelding 1 - Uitgebreide implementatie van Local Mode AP**



Afbeelding 2 - Belangrijkste bedreigingen voor draadloze beveiliging

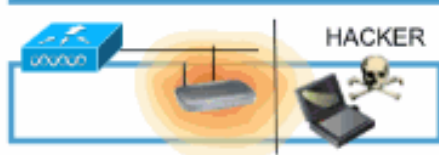
### On-Wire Attacks

#### Ad-hoc Wireless Bridge



Client-to-client backdoor access

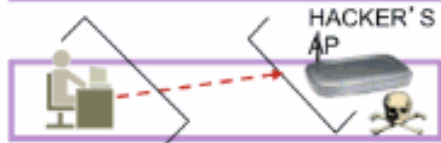
#### Rogue Access Points



Backdoor network access

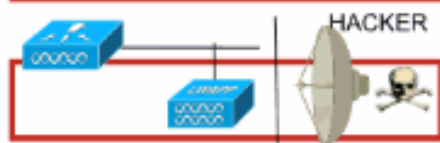
### Over-the-Air Attacks

#### Evil Twin/Honeypot AP



Connection to malicious AP

#### Reconnaissance



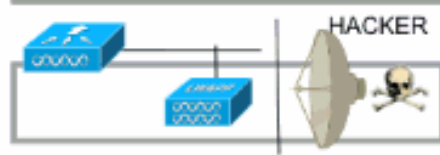
Seeking network vulnerabilities

#### Denial of Service



Service disruption

#### Cracking Tools



Sniffing and eavesdropping

[Voorwaarden](#)

[Vereisten](#)

Er zijn geen specifieke vereisten van toepassing op dit document.

## Gebruikte componenten

### **ELM Vereiste componenten en minimumcode versies**

- Draadloze LAN-controller (WLC) - versie 7.0.16.xx of hoger
- APs - versie 7.0.16.xx of hoger
- Wireless Control System (WCS) - versie 7.0.172.xx of hoger
- Mobility Services Engine - versie 7.0.201.xx of hoger

### **Ondersteunende WLC-platforms**

ELM wordt ondersteund op WLC508-, WLC4400-, WLC 2106-, WLC2504-, WiSM-1- en WiSM-2WLC-platforms.

### **Ondersteunende APs**

ELM wordt ondersteund op 11n AP's waaronder 3500, 1250, 1260, 1040 en 1140.

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u de potentiële impact van elke opdracht begrijpen.

## Conventies

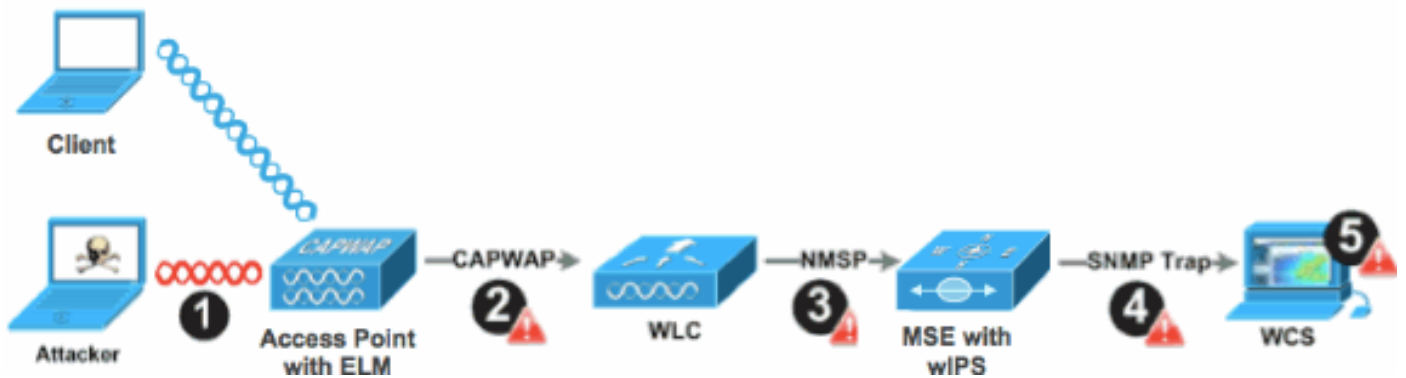
Raadpleeg [Cisco Technical Tips Conventions \(Conventies voor technische tips van Cisco\) voor meer informatie over documentconventies.](#)

## ELM met IPS-alarmstroom

Aanvallen zijn alleen relevant wanneer ze optreden op vertrouwde infrastructuur-AP's. De ELM AP's detecteren en communiceren met de controller en correleren met de MSE voor rapportage met WCS-beheer. [Figuur 3](#) verstrekt de alarmstroom vanuit het standpunt van een beheerder:

1. Aanval gestart tegen een infrastructuurapparaat ("vertrouwde" AP)
2. Gedetecteerd op ELM AP gecommuniceerd via CAPWAP naar WLC
3. Doorgegeven aan MSE via NMSP
4. Inloggen in wIPS Database op MSE verzonden naar WCS via SNMP-trap
5. Weergegeven op WCS

### **Afbeelding 3 - Dreigingsdetectie en alarmstroom**



## Implementatieoverwegingen voor ELM

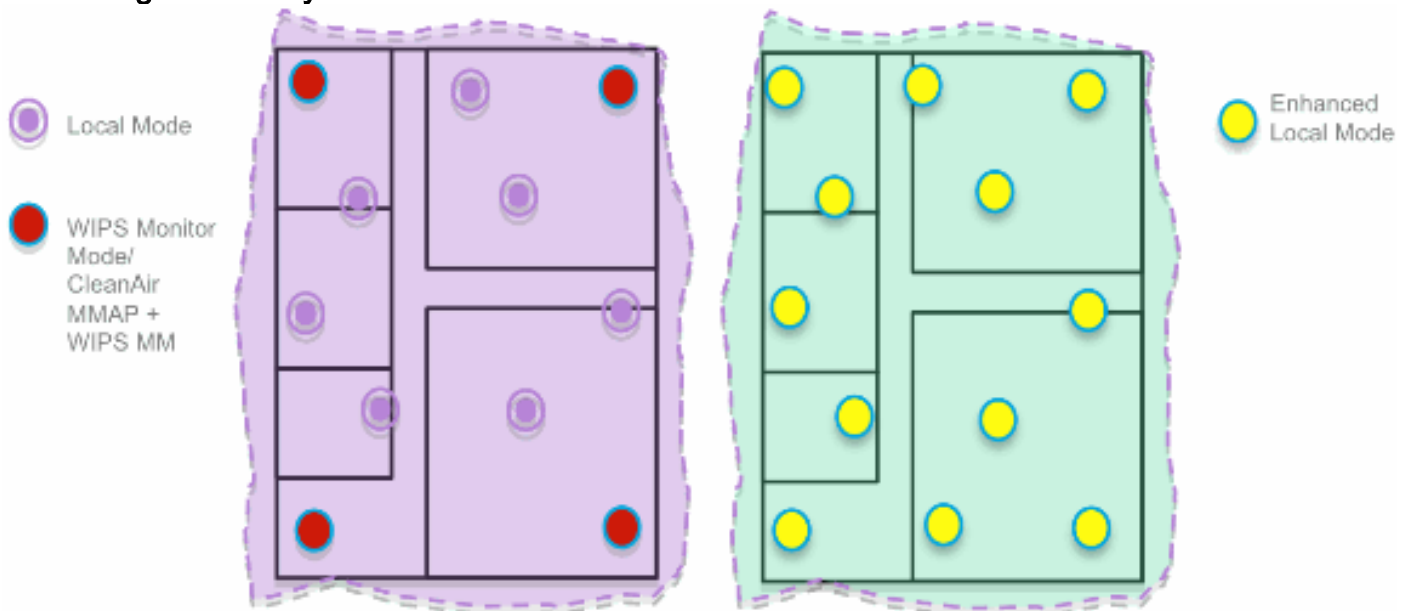
Cisco raadt aan om, door ELM op elke AP op het netwerk in te schakelen, aan de meeste beveiligingsbehoeften van klanten te voldoen wanneer een netwerkoverlay en/of kosten onderdeel van de overweging zijn. De primaire functie van ELM werkt effectief voor on-channel aanvallen, zonder enige afbreuk te doen aan de prestaties op data-, spraak- en videoclients, en services.

## ELM vs speciale MM

[Afbeelding 4](#) biedt een algemeen contrast tussen de standaardimplementaties van IPS MM AP's en ELM. In het overzicht van de verschillende modi wordt het volgende voorgesteld:

- Speciale IPS M400 access point beslaat doorgaans 15.000-35.000 vierkante voet
- Clientserverende AP bedekt doorgaans vanaf 3.000-5.000 vierkante voet

**Afbeelding 4 - Overlay van MM vs Alle ELM AP's**



In de traditionele adaptieve IPS-implementatie raadt Cisco een verhouding van 1 MM AP aan op elke 5 lokale mode AP's, die ook kunnen variëren op basis van netwerkontwerp en deskundige begeleiding voor de beste dekking. Door ELM te overwegen, laat de beheerder eenvoudig de ELM softwarefunctie voor alle bestaande AP's toe, effectief toevoegend de verrichtingen van MwIPS aan lokale gegeven-dienende wijze AP terwijl het handhaven van prestaties.

## On-Channel en Off-Channel prestaties

Een MM AP gebruikt 100% van de tijd van de radio voor het scannen van alle kanalen, aangezien het geen WLAN-clients bedient. De primaire functie voor ELM werkt effectief voor on-channel-aanvallen, zonder enige afbreuk te doen aan de prestaties op data-, spraak- en videoclients en -diensten. Het belangrijkste verschil is in de lokale modus variërend off-channel scannen; afhankelijk van de activiteit, off-channel scannen biedt minimale verblijftijd om genoeg informatie te verzamelen om te classificeren en te bepalen aanval. Een voorbeeld kan met stemcliënten zijn die worden geassocieerd en waar het scannen van RRM van AP wordt uitgesteld tot de stemcliënt wordt losgekoppeld om ervoor te zorgen de dienst niet wordt beïnvloed. Voor deze overweging, wordt de opsporing ELM tijdens off-channel beschouwd als beste inspanning. De naburige ELM AP's die op alle, land of DCA-kanalen werken, verhogen de effectiviteit, vandaar de aanbeveling om ELM op elke lokale modus AP in te schakelen voor maximale beschermingsdekking. Als het nodig is om op alle kanalen fulltime speciaal te scannen, is het raadzaam om APM's te implementeren.

In deze punten worden verschillen tussen lokale modi en MMA-toegangspunten beoordeeld:

- Local Mode AP - Serveer WLAN-clients met tijdsnijden off-channel scannen, luistert naar 50 ms op elk kanaal en beschikt over configureerbare scanning voor alle / land / DCA-kanalen.
- AP van de Modus van de monitor - dient geen WLAN cliënten, gewijd aan het scannen slechts, luistert op 1.2s op elk kanaal, en scant alle kanalen.

## ELM via WAN-links

Cisco heeft zich grote inspanningen getroost om functies in uitdagende scenario's te optimaliseren, zoals het implementeren van ELM AP's via WAN-koppelingen met lage bandbreedte. De ELM-functie maakt voorbereiding nodig bij het bepalen van aanvalshandtekeningen op het toegangspunt en is geoptimaliseerd om langzame koppelingen te verwerken. Als best practices wordt aanbevolen om de basislijn te testen en meten om de prestaties met ELM via WAN te valideren.

## Integratie met CleanAir

De ELM-functie vult CleanAir-operaties in hoge mate aan met vergelijkbare prestaties en voordelen voor de inzet van MAP's met deze bestaande CleanAir-spectrumbewuste voordelen:

- Speciale siliconenniveau RF-intelligentie
- Spectrumbewust, zelfherstellend en zelfoptimaliserend
- Niet-standaard kanaaldreiging en interferentiedetectie en -beperking
- Niet-Wi-Fi detectie zoals Bluetooth, magnetron, draadloze telefoons, enz.
- Detecteer en lokaliseer RF-laag DOS-aanvallen zoals RF-jammers

## ELM-functies en -voordelen

- Adaptieve IPS-scanning in gegevens voor lokale toegangspunten en toegangspunten met H-REAP
- Bescherming zonder dat er een afzonderlijk overlay-netwerk nodig is
- Verkrijgbaar als gratis SW-download voor bestaande IPS-klanten
- Ondersteunt naleving van PCI voor draadloze LAN's

- Volledige aanvalsdetectie van 802.11 en niet-802.11
- Voegt forensische wetenschap en rapportagemogelijkheden toe
- Geïntegreerd met bestaand CUWM- en WLAN-beheer
- Flexibiliteit voor het instellen van geïntegreerde of speciale APM's
- Voorbewerking bij AP's minimaliseert de backhaul van gegevens (dat wil zeggen, werkt via zeer lage bandbreedte links)
- Lage impact op de serveergegevens

## ELM-licentiëring

ELM-wIPS voegt een nieuwe licentie toe aan het bestellen:

- AIR-LM-WIPS-xx - Cisco ELM IPS-licentie
- AIR-WIPS-AP-xx - Cisco draadloze IPS-licentie

Aanvullende ELM-licentienota's:

- Als er al een of meer SKU's voor IPS MM AP-licenties zijn geïnstalleerd, kunnen deze licenties ook worden gebruikt voor ELM AP's.
- wIPS-licenties en ELM-licenties tellen samen voor de limieten van de platformlicentie voor wIPS-engine; 2000 AP's op respectievelijk 3310 en 3000 AP's op 335x.
- De evaluatielicentie omvat 10 AP's voor wIPS en 10 voor ELM voor een periode van maximaal 60 dagen. Voorafgaand aan ELM, stond de evaluatielicentie tot 20 IPS MM AP's toe. Er moet worden voldaan aan de minimumeis van softwareversies die ELM ondersteunen.

## ELM configureren met WCS

Afbeelding 5 - Gebruik WCS om ELM te configureren

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/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	802.11b/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/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	802.11b/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/n	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/n	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/n	System Campus > BuildingS1 > 1st floor	Not Associated	0	Enabled	H-REAP
<input type="checkbox"/> demo-AP1262N-FB	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-FB	f8:66:f2:67:68:93	10.10.20.102	802.11a/n	System Campus > BuildingS1 > 1st floor	10.10.10.5	0	Enabled	H-REAP

1. Schakel vanuit WCS zowel de 802.11b/g- als 802.11a-radio's van het AP uit voordat "Enhanced IPS Engine" wordt ingeschakeld. **Opmerking:** alle bijbehorende clients worden losgekoppeld en worden pas lid als de radio is ingeschakeld.
2. Configureer één AP of gebruik een WCS-configuratiesjabloon voor meerdere lichtgewicht AP's. Zie [afbeelding 6](#). **Afbeelding 6 - Uitgebreide submodus van IPS Engine (ELM) inschakelen**

### Access Point Detail : demo-AP3502i-S

Configure > [Access Points](#) > Access Point Detail

#### General

AP Name	demo-AP3502i-S	<a href="#">Requirements</a>
Ethernet MAC	00:22:90:e3:37:dc	
Base Radio MAC	00:22:8d:d1:71:10	
Country Code	US	
IP Address	10.10.20.103	
Admin Status	<input checked="" type="checkbox"/> Enable	
AP Static IP	<input type="checkbox"/> Enable	
AP Mode	Local	
Enhanced wIPS Engine	<input checked="" type="checkbox"/> Enable	
AP Failover Priority	Low	
Registered Controller	10.10.10.5	
Primary Controller Name	wlc	

### Access Point Detail : demo-AP1142n

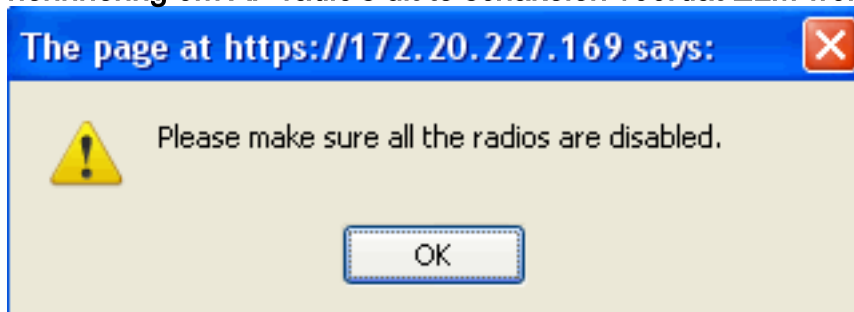
Configure > [Access Points](#) > Access Point Detail

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

#### General

AP Name	demo-AP1142n	<a href="#">Requirements</a>
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	<input checked="" type="checkbox"/> Enable	
AP Static IP	<input type="checkbox"/> Enable	
AP Mode	H-REAP	
Enhanced wIPS Engine	<input checked="" type="checkbox"/> Enable	
AP Failover Priority	Medium	
Registered Controller	10.10.10.5	
Primary Controller Name	wlc	

3. Kies **Uitgebreide IPS Engine** en klik op **Opslaan**. Als u Enhanced IPS Engine inschakelt, wordt het AP niet opnieuw opgestart. H-REAP wordt ondersteund. Schakel de lokale modus van het toegangspunt in. **Opmerking:** als een van de radio's van dit AP is ingeschakeld, zal WCS de configuratie negeren en de fout in [afbeelding 7](#) overslaan. **Afbeelding 7 - WCS-herinnering om AP-radio's uit te schakelen voordat ELM wordt ingeschakeld**



4. Het succes van de configuratie kan worden geverifieerd door de verandering in de AP-modus te observeren van "Local or H-REAP" op **Local/wIPS** of **H-REAP/wIPS**. Zie [afbeelding 8](#). **Afbeelding 8 - De WCS-weergavemodus voor weergave van het toegangspunt om WIPS met lokaal netwerk en/of H-REAP op te nemen**

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

- Schakel de radio's in die in Stap 1 zijn uitgeschakeld.
- Maak het wIPS-profiel en druk het naar de controller zodat de configuratie kan worden voltooid. **N.B.:** Raadpleeg de [Cisco Adaptieve IPS-implementatiegids voor volledige configuratie-informatie over wIPS](#).

## [Configuratie vanuit WLC](#)

Afbeelding 9 - Configureer ELM met WLC

Cisco							
MONITOR W-LAN CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK							
Wireless							
All APs							
Current Filter		None		[Change Filter] [Clear Filter]			
Number of APs		8					
AP Name	AP Model	AP MAC	AP Up Time	Admin Status	Operational Status	Port	AP Mode
<a href="#">demo-AP3502i-J</a>	AIR-CAP3502i-A-K9	04:7d:4f:3a:ed:48	4 d, 06 h 50 m 10 s	Enabled	REC	13	Local
<a href="#">demo-AP1262N-FB</a>	AIR-CT5524-A-K9	f8:66:f2:67:68:93	4 d, 06 h 50 m 35 s	Enabled	REC	13	H-REAP
<a href="#">demo-AP3502i-S</a>	AIR-CAP3502i-A-K9	00:22:90:e3:37:dc	4 d, 06 h 50 m 02 s	Enabled	REC	13	Local
<a href="#">demo-AP1260</a>	AIR-CT5524-A-K9	f8:66:f2:ab:1f:96	4 d, 06 h 49 m 59 s	Enabled	REC	13	Local
<a href="#">demo-AP1142n</a>	AIR-CT5524-A-K9	00:22:90:90:99:6f	0 d, 00 h 50 m 47 s	Enabled	REC	13	H-REAP
<a href="#">demo-AP3502i-MM</a>	AIR-CAP3502i-A-K9	04:7d:4f:3a:06:62	0 d, 00 h 53 m 35 s	Enabled	REC	13	H-REAP

- Kies een AP in het tabblad Draadloos. Afbeelding 10 - WLC-submodus voor verandering van



## AP, inclusief WiPS ELM

The screenshot shows the Cisco WLC configuration interface for an AP named 'demo-AP3502I-J'. The 'General' tab is active, displaying various configuration parameters. The 'AP Sub Mode' dropdown menu is highlighted, showing 'WIPS' as the selected option. The 'Versions' section on the right provides details about the software and boot versions.

2. Kies in het vervolgkeuzemenu AP Sub Mode IPS ([afbeelding 10](#)).
3. Pas de configuratie toe en sla deze op.

**Opmerking:** voor de ELM-functionaliteit zijn MSE en WCS vereist bij WIPS-licenties. Als u de submodus van het toegangspunt wijzigt van alleen WLC, wordt ELM niet ingeschakeld.

## Aanvallen gedetecteerd in ELM

Tabel 1 - Ondersteuningsmatrix voor IPS-handtekeningen

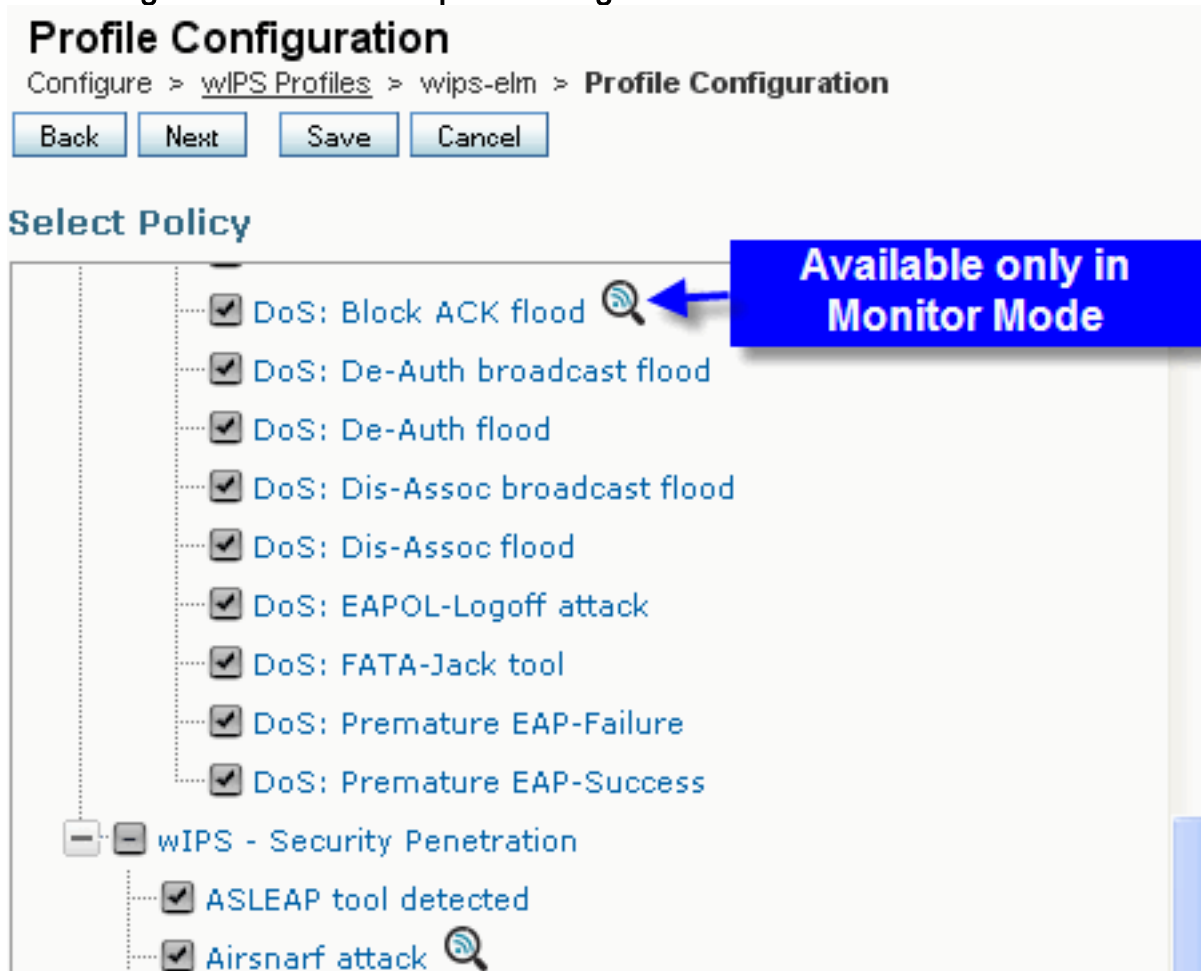
Aanvallen gedetecteerd	ELM	MM
<b>VoS-aanval op access point</b>		
Associatieraad overstroming	Y	Y
Associatietabeloverloop	Y	Y
Verificatievloed	Y	Y
EAPOL-Start aanval	Y	Y
PS-Poll-overstroming	Y	Y
Overstroming van sonde-verzoek	N	Y
Niet-geverifieerde associatie	Y	Y
<b>Aanval van gegevensbeschermingsautoriteiten op infrastructuur</b>		
CTS-overstroming	N	Y
Gebruik van de Queensland University of Technology	N	Y
RF-blokking	Y	Y
RTS-overstroming	N	Y
Virtual Carrier-aanval	N	Y
<b>DoS-aanval op station</b>		
Aanval op verificatiefouten	Y	Y
Blokkeer ACK-overstroming	N	Y
De-Auth uitzendvloed	Y	Y


De-Auth-overstroming	Y	Y
Dis-Assoc uitzendingsoverstroming	Y	Y
Dis-Assoc-overstroming	Y	Y
EAPOL-afsluitaanval	Y	Y
FATA-Jack-gereedschap	Y	Y
Voortijdig EAP-Falen	Y	Y
Voortijdig EAP-succes	Y	Y
<b>Beveiligingsaanvallen</b>		
ASLEAP-gereedschap gedetecteerd	Y	Y
Aironarf-aanval	N	Y
ChopChop aanval	Y	Y
Day-Zero aanval door WLAN-beveiligingsanomalie	N	Y
Day-Zero aanval door anomalie in apparaatbeveiliging	N	Y
Apparaatcontrole voor AP's	Y	Y
Woordenboekaanval op EAP-methoden	Y	Y
EAP-aanval tegen 802.1x-verificatie	Y	Y
Fake AP's gedetecteerd	Y	Y
Fake DHCP-server gedetecteerd	N	Y
FAST WEP-cracktool gedetecteerd	Y	Y
Fragmentation attack	Y	Y
Honeypot AP gedetecteerd	Y	Y
Hotspotter-gereedschap gedetecteerd	N	Y
Onjuiste broadcast-frames	N	Y
Misvormde 802.11 pakketten gedetecteerd	Y	Y
Man in de middelste aanval	Y	Y
Netstumbler gedetecteerd	Y	Y
slachtoffer Netstumbler gedetecteerd	Y	Y
PSPF-overschrijding gedetecteerd	Y	Y
Zachte AP of host AP gedetecteerd	Y	Y
Spoofed MAC-adres gedetecteerd	Y	Y
Verdachte na-urenverkeer	Y	Y

gedetecteerd		
Niet-geautoriseerde associatie op leverancierslijst	N	Y
Onbevoegde associatie gedetecteerd	Y	Y
Wellenreiter gevonden	Y	Y

**Opmerking:** als u CleanAir toevoegt, kunt u ook niet-802.11-aanvallen detecteren.

Afbeelding 11 - WCS met IPS-profielweergave



In [afbeelding 11](#), configureer het wIPS-profiel vanuit WCS, geeft het  pictogram aan dat de aanval alleen gedetecteerd zal worden wanneer AP in MM is, terwijl alleen de beste inspanning wanneer in ELM.

## Probleemoplossing ELM

Controleer de volgende items:

- Zorg ervoor dat NTP is geconfigureerd.
- Controleer of de MSE-tijdsinstelling in UTC is.
- Als de apparaatgroep niet werkt, gebruikt u overlay-profiel SSID met Any. Start het toegangspunt opnieuw op.
- Zorg ervoor dat de licenties zijn geconfigureerd (momenteel gebruiken ELM AP's KAM-licenties)

- Als de IPS-profielen te vaak worden gewijzigd, synchroniseer de MSE-controller opnieuw. Zorg ervoor dat het profiel actief is op WLC.
- Zorg ervoor dat WLC deel uitmaakt van MSE met MSE CLI's:SSH of telnet aan uw MSE.`Execute/opt/mse/wips/bin/wips_cli` - Deze console kan worden gebruikt voor toegang tot de volgende opdrachten om informatie te verzamelen over de status van het adaptieve WIPS-systeem.`wlc all tonen` - Problemen binnen de IPS-console. Deze opdracht wordt gebruikt om de controllers te verifiëren die actief communiceren met de IPS-service op de MSE. Zie figuur 12.**Afbeelding 12 - MSE CLI-verificatie van WLC actief met MSE IPS-services**

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

```

- Zorg ervoor dat de alarmen op MSE worden gedetecteerd met behulp van MSE CLI's.`alarmlijst tonen` - Problemen binnen de IPS-console. Deze opdracht wordt gebruikt om een lijst te maken van de alarmen die momenteel in de IPS-servicedatabank aanwezig zijn. Het sleutelveld is de unieke hash sleutel die is toegewezen aan het specifieke alarm. Het veld Type is het type alarm. Deze grafiek in Figuur 13 toont een lijst van alarm IDs en beschrijvingen:**Afbeelding 13 - MSE CLI toont alarmlijst Opdracht**

wIPS>`show alarm list`

```

Key           Type  Src MAC
LastTime           Active           First Time
-----
-----
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

```

De velden Eerste en Laatste keer geven de tijdstempels aan wanneer het alarm werd gedetecteerd; deze worden in UTC-tijd opgeslagen. Het actieve veld markeert als het alarm momenteel is gedetecteerd.

- Schakel de MSE-database uit. Als u een situatie tegenkomt waarin de MSE-database beschadigd is, of geen andere probleemoplossingsmethoden zullen werken, is het misschien het beste om de database te wissen en opnieuw te beginnen.**Afbeelding 14 - Opdracht MSE services**

```

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

```

## Gerelateerde informatie

- [Configuratiehandleiding voor Cisco draadloze LAN-controllers, release 7.0.16.0](#)
- [Cisco-configuratiehandleiding voor draadloos controlesysteem, release 7.0.172.0](#)
- [Technische ondersteuning en documentatie – Cisco Systems](#)

## Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document ([link](#)) te raadplegen.