# Identificatie van schurkenclients in een draadloos Cisco-netwerk voor bedrijven

### Doel

Het doel van dit artikel is om u te tonen hoe u bedrieglijke access points (AP's) en schurkendraadloze clients kunt identificeren in een traditioneel Cisco Business Wireless (CBW) netwerk of een netwerk van netwerken.

## Toepasselijke apparaten | Firmwareversie

- 140AC (gegevensblad) | 10.0.1.0 (Download nieuwste release)
- 141ACM (gegevensblad) | 10.0.1.0 (Download laatste) - verlengers worden alleen gebruikt in een netwerk van mazen
- 1442ACM (gegevensblad) | 10.0.1.0 (Download laatste) - verlengers worden alleen gebruikt in een netwerk van mazen
- 143ACM (gegevensblad) | 10.0.1.0 (Download laatste) - verlengers worden alleen gebruikt in een netwerk van mazen
- 145AC (gegevensblad) | 10.0.1.0 (Download nieuwste release)
- 240AC (gegevensblad) | 10.0.1.0 (Download nieuwste release)
- 150AXE (gegevensblad) | 10.3.2.0 (Download nieuwste release)
- 1551AXM (gegevensblad) | 10.3.2.0 (Download nieuwste release)

CBW 15x Series-apparaten zijn niet compatibel met CBW 14x/240 Series-apparaten en coëxistentie op hetzelfde LAN wordt niet ondersteund.

## Inleiding

CBW Access points (AP's) zijn gebaseerd op 802.11 a/b/g/n/ac (Wave 2), met interne antennes. Ze kunnen worden gebruikt als traditionele standalone apparaten of als deel van een netwerk van mazen.

In een perfecte wereld zou iedereen respectvol en eerlijk zijn wanneer hij je draadloze netwerk gebruikt. Helaas leven we niet in een perfecte wereld. Als beheerder moet u zich bewust zijn van eventuele problemen.

Ruwe AP's zijn AP's die zonder uw toestemming op een netwerk zijn geïnstalleerd. Schurfclients zijn alle andere gedetecteerde apparaten die niet bij uw bedrijf horen.

Deze verbindingen zouden volledig onschuldig kunnen zijn, maar er is altijd een risico dat deze schurken zullen proberen om uw netwerk aan te vallen of gevoelige informatie te stelen. Om bovenop dit te houden, kunt u de bedrieglijke APs en schurkencliënten bekijken. Wanneer deze schurken eenmaal zijn gedetecteerd, kunnen ze niet worden geblokkeerd via het toegangspunt, maar het geeft u wel informatie om verder te onderzoeken.

De CBW AP's detecteren alleen schurken op kanalen die u momenteel gebruikt of kanalen die overlappen.

# Rogue AP's bekijken

Deze omgekeerde sectie benadrukt tips voor beginners.

## Inloggen

Log in op de Web User Interface (UI) van het primaire AP. Open hiervoor een webbrowser en voer https://ciscobusiness.cisco in. U kunt een waarschuwing ontvangen voordat u doorgaat. Voer uw referenties in. U kunt ook toegang krijgen tot de primaire AP door https://[ipaddress] (van de primaire AP) in te voeren in een webbrowser.

## Tips voor tools

Als u vragen hebt over een veld in de gebruikersinterface, controleert u op een knopinfo die er als volgt uitziet:

## Problemen met het lokaliseren van het pictogram van het hoofdmenu uitvouwen?

Navigeer naar het menu aan de linkerkant van het scherm. Als u de menuknop niet ziet, klikt u op dit pictogram om het zijbalkmenu te openen.

## Cisco Business-app

Deze apparaten hebben compacte apps die bepaalde beheerfuncties delen met de web-gebruikersinterface. Niet alle functies in de webgebruikersinterface zijn beschikbaar in de App.

iOS-app downloaden Android-app downloaden

## Veelgestelde vragen

Als u nog steeds onbeantwoorde vragen hebt, kunt u het document met veelgestelde vragen bekijken. FAQ

### Stap 1

Log in op de Web User Interface (UI) van het primaire AP. Open hiervoor een webbrowser en voer *https://ciscobusiness.cisco* in. U kunt een waarschuwing ontvangen voordat u doorgaat. Voer uw referenties in.

U hebt ook toegang tot het primaire toegangspunt door *https://<ipaddress>* (van het primaire toegangspunt) in te voeren in een webbrowser.

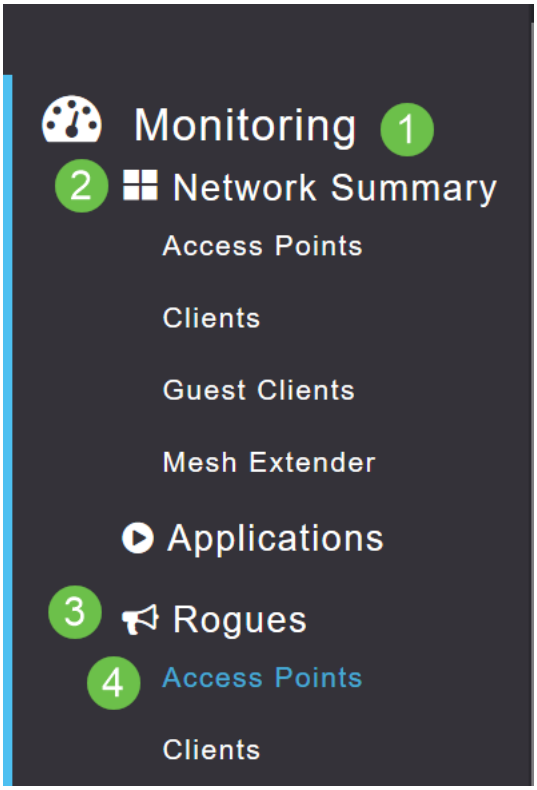
Als u niet bekend bent met de gebruikte termen, kunt u Cisco Business: Glossary of New Terms bekijken.

### Stap 2

Om deze configuraties te maken, moet u in *Expert View* zijn. Klik op het **pijlpictogram** in het rechterbovenmenu van de Web UI naar switch naar *Expert View*.

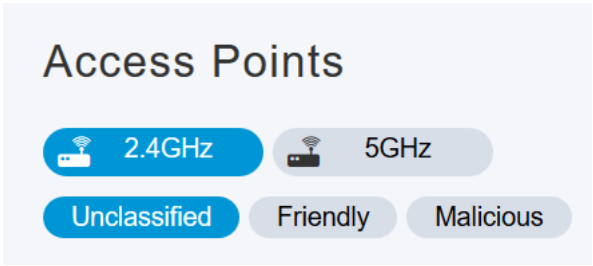
### Stap 3

Navigeer naar **Monitoring > Netwerkoverzicht > Rogues > Access points.**



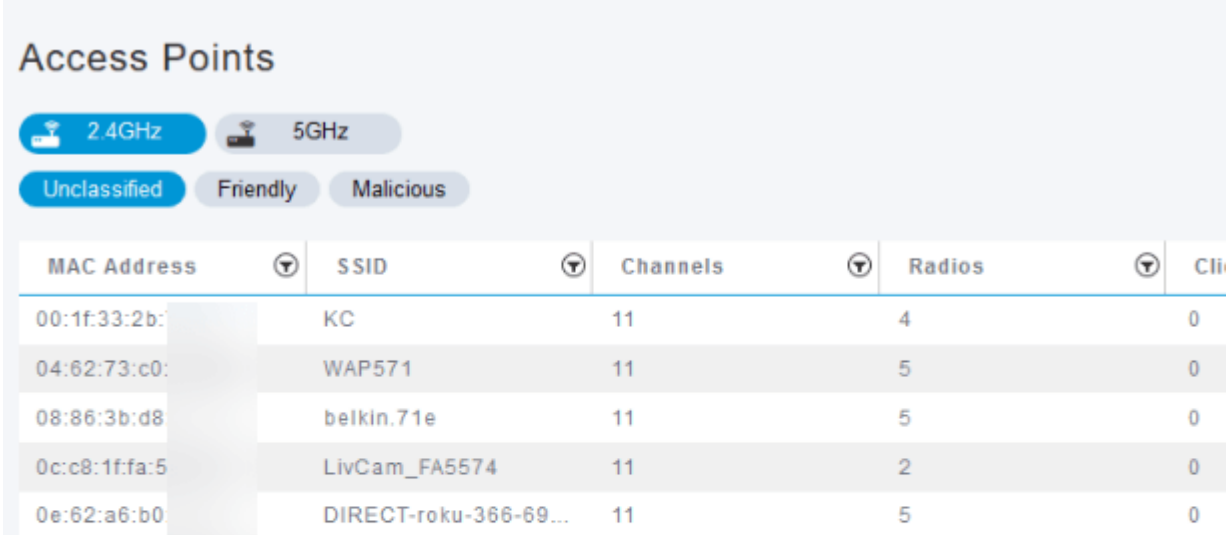

### Stap 4

Nadat deze pagina is geopend, kunt u 2,4 GHz of 5 GHz selecteren door op het tabblad te klikken. Standaard worden alle frauduleuze AP's aangeduid als Niet geclassificeerd. AP verandert niet de etiketten voor de schurkenAPs, dat is iets u manueel zou doen.



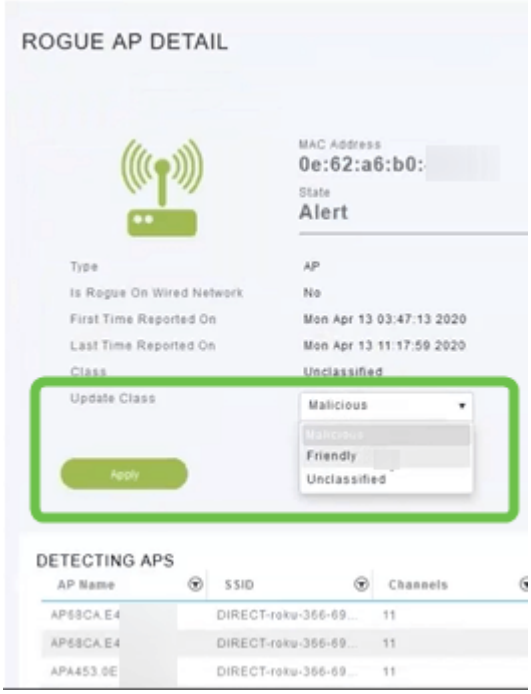

### Stap 5

De frauduleuze AP's worden vermeld, kunt u op een van hen klikken om verder te onderzoeken.



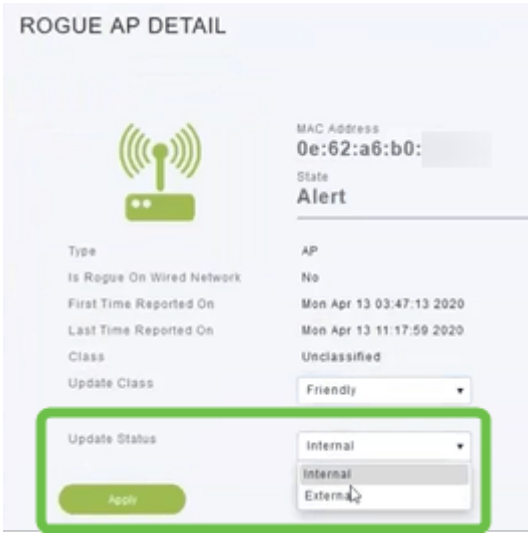
### Stap 6 (optioneel)

Als u een van de AP's wilt classificeren als *vriendelijk* of *kwaadaardig*, kunt u een van beide opties selecteren in het vervolgkeuzemenu onder *Update Class*. U zou dit kunnen willen doen zodat wanneer u in de toekomst kijkt naar Niet-geclassificeerde access points, u niet hoeft te sorteren door een volledige lijst. Klik op **Toepassen** als u klaar bent.




### Stap 7 (optioneel)

Als u een AP wilt labelen als *Intern* (in netwerk) of *Extern* (mogelijk een naburig bedrijf) kunt u dat doen onder de sectie *Update Status*. Klik op **Toepassen** als u klaar bent.




## Rogue-clients bekijken

### Stap 1

Meld u aan bij de Web UI van het primaire toegangspunt. Open hiervoor een webbrowser en voer *https://ciscobusiness.cisco* in. U kunt een waarschuwing ontvangen voordat u doorgaat. Voer uw referenties in.

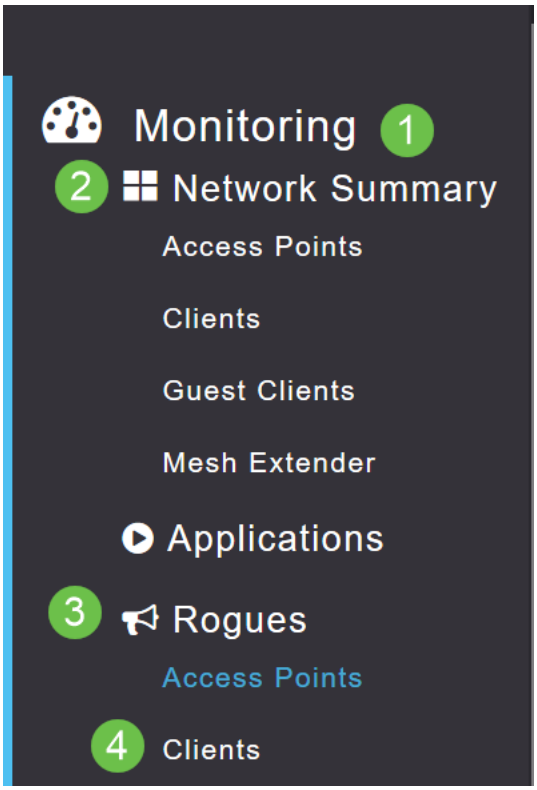
U hebt ook toegang tot het primaire toegangspunt door *https://<ipaddress>* (van het primaire toegangspunt) in te voeren in een webbrowser. Voor sommige acties kunt u de Cisco Business Mobile-app gebruiken.

### Stap 2

Om deze configuraties te maken, moet u in *Expert View* zijn. Klik op het **pijlpictogram** in het rechterbovenmenu van de Web UI naar switch naar *Expert View*. Kijk voor meer informatie over het instellen van een RADIUS-server in Radius

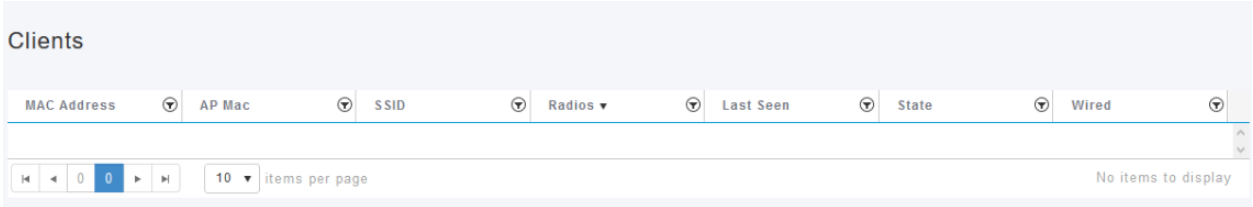

### Stap 3

Navigeer naar **Monitoring > Netwerkoverzicht > Rogues > Clients.**




### Stap 4

Als er schurkencliënten zijn, zullen zij vermeld worden. In dit voorbeeld, zijn geen schurkencliënten ontdekt.




## Conclusie

Nu heb je de mogelijkheid om schurken in je netwerk te zien. Als je veel schurken ziet op een kanaal dat je gebruikt, kun je het kanaal wijzigen. Er zijn overwegingen om in gedachten te

houden, dus controleer het artikel over het wijzigen van RF-kanaal (link indien beschikbaar).

Veelgestelde vragen Straal Firmware-upgrade LAN's Toepassingsprofilering Clientprofilering Primaire AP-tools Umbrella WLAN-gebruikers Vastlegging Traffic Shaping Rogues Inmengers Configuratiebeheer Netwerkmodus voor poortconfiguratie Welkom bij CBW Mesh Networks Gastnetwerk met e-mailverificatie en RADIUS-accounting Probleemoplossing Een Draytek router met CBW gebruiken

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.