

Identification des clients indésirables dans un réseau sans fil professionnel Cisco

Objectif

L'objectif de cet article est de vous montrer comment identifier les points d'accès (AP) et les clients sans fil indésirables dans un réseau traditionnel ou maillé Cisco Business Wireless (CBW).

Périphériques pertinents | Version du micrologiciel

- 140 CA ([fiche technique](#)) | 10.0.1.0 ([Télécharger la dernière version](#))
- 141ACM ([fiche technique](#)) | 10.0.1.0 ([Télécharger la dernière version](#)) - les extendeurs sont uniquement utilisés dans un réseau maillé
- 142ACM ([fiche technique](#)) | 10.0.1.0 ([Télécharger la dernière version](#)) - les extendeurs sont uniquement utilisés dans un réseau maillé
- 143ACM ([fiche technique](#)) | 10.0.1.0 ([Télécharger la dernière version](#)) - les extendeurs sont uniquement utilisés dans un réseau maillé
- 145AC ([fiche technique](#)) | 10.0.1.0 ([Télécharger la dernière version](#))
- 240AC ([fiche technique](#)) | 10.0.1.0 ([Télécharger la dernière version](#))
- 150AX ([fiche technique](#)) | 10.3.2.0 ([Télécharger la dernière version](#))
- 151AXM ([fiche technique](#)) | 10.3.2.0 ([Télécharger la dernière version](#))

Les périphériques CBW 15x ne sont pas compatibles avec les périphériques CBW 14x/240 et la coexistence sur le même réseau local n'est pas prise en charge.

Introduction

Les points d'accès CBW sont basés sur la norme 802.11 a/b/g/n/ac (phase 2), avec des antennes internes. Ils peuvent être utilisés en tant que périphériques autonomes traditionnels ou dans le cadre d'un réseau maillé.

Dans un monde parfait, tout le monde serait respectueux et honnête lors de l'utilisation de votre réseau sans fil. Malheureusement, nous ne vivons pas dans un monde parfait. En tant qu'administrateur, votre travail consiste à être conscient de tout problème potentiel.

Les points d'accès non autorisés sont des points d'accès qui ont été installés sur un réseau sans votre autorisation. Les clients indésirables sont tous les autres périphériques détectés qui n'appartiennent pas à votre société.

Ces connexions peuvent être totalement inoffensives, mais il existe toujours un risque que ces pirates tentent d'attaquer votre réseau ou de voler des informations sensibles. Pour garder le dessus, vous pouvez afficher les points d'accès et les clients indésirables. Une fois détectés, ces indésirables ne peuvent pas être bloqués par l'intermédiaire du point d'accès, mais ils vous donnent des informations pour approfondir vos recherches.

Les points d'accès CBW détectent uniquement les routeurs sur les canaux que vous utilisez actuellement ou les canaux qui se chevauchent.


Afficher les points d'accès indésirables

Cette section à bascule présente des conseils pour les débutants.


Connexion en cours

Connectez-vous à l'interface utilisateur Web du point d'accès principal. Pour ce faire, ouvrez un navigateur Web et entrez <https://ciscobusiness.cisco>. Vous pouvez recevoir un avertissement avant de continuer. Entrez vos informations d'identification. Vous pouvez également accéder au point d'accès principal en entrant [https://\[adresse IP\]](https://[adresse IP]) (du point d'accès principal) dans un navigateur Web.

Conseils sur les outils

Si vous avez des questions sur un champ de l'interface utilisateur, recherchez une info-bulle semblable à celle-ci : 

Vous ne trouvez pas l'icône Développer le menu principal ?

Accédez au menu situé à gauche de l'écran. Si vous ne voyez pas le bouton de menu, cliquez sur cette icône pour ouvrir le menu de la barre latérale. 

Application professionnelle Cisco

Ces périphériques sont accompagnés d'applications qui partagent certaines fonctions de gestion avec l'interface utilisateur Web. Toutes les fonctionnalités de l'interface utilisateur Web ne seront pas disponibles dans l'application.

[Télécharger l'application iOS](#) [Télécharger l'application Android](#)

Forum aux questions

Si vous avez encore des questions sans réponse, vous pouvez consulter notre Forum Aux Questions. [Forum aux questions](#)

Étape 1

Connectez-vous à l'interface utilisateur Web du point d'accès principal. Pour ce faire, ouvrez un navigateur Web et entrez <https://ciscobusiness.cisco>. Vous pouvez recevoir un avertissement avant de continuer. Entrez dans vos informations d'identification.

Vous pouvez également accéder au point d'accès principal en entrant <https://<ipaddress>> (du point d'accès principal) dans un navigateur Web.

Si vous n'êtes pas familier avec les termes utilisés, consultez [Cisco Business : Glossaire des nouveaux termes](#).

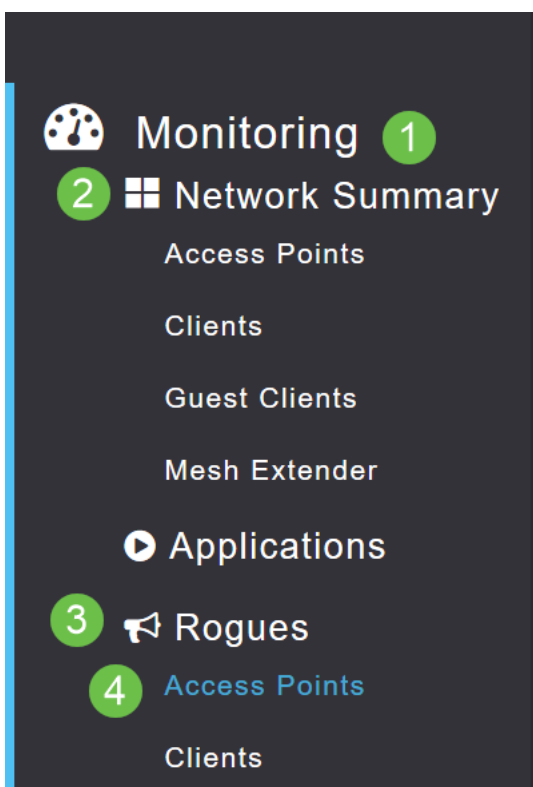
Étape 2

Pour effectuer ces configurations, vous devez vous trouver dans *Expert View*. Cliquez sur l'icône en forme de **flèche** dans le menu supérieur droit de l'interface utilisateur Web pour passer à *Expert View*.



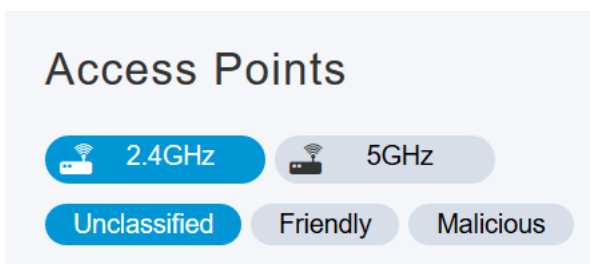
Étape 3

Accédez à **Monitoring > Network Summary > Rogues > Access Points**.



Étape 4

Une fois cette page ouverte, vous pouvez choisir de voir 2,4 GHz ou 5 GHz en cliquant sur l'onglet. Par défaut, tous les points d'accès non autorisés sont étiquetés Non classifié. L'AP ne change pas les étiquettes pour les AP indésirables, c'est quelque chose que vous feriez manuellement.



Étape 5

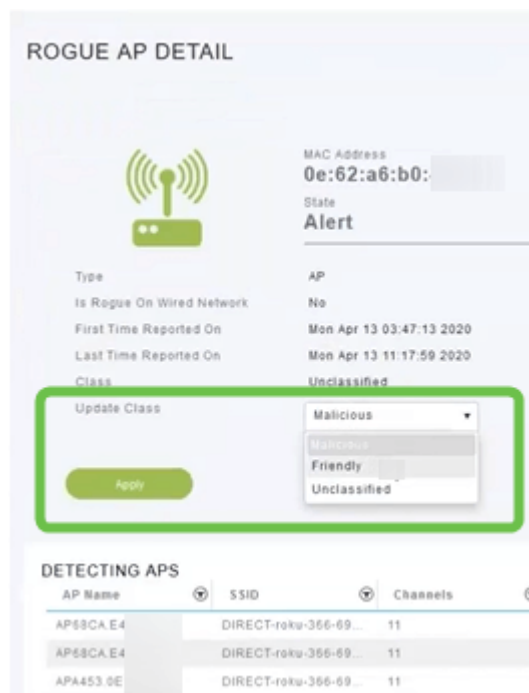
Les points d'accès indésirables sont répertoriés, vous pouvez cliquer sur l'un d'entre eux pour examiner plus en détail.

The screenshot shows the 'Access Points' table with the following columns and data:

MAC Address	SSID	Channels	Radios	Clients
00:1f:33:2b:...	KC	11	4	0
04:62:73:c0:...	WAP571	11	5	0
08:86:3b:d8:...	belkin.71e	11	5	0

Étape 6 (facultative)

Si vous voulez classer l'un des AP comme *Amical* ou *Malicious*, vous pouvez sélectionner l'une ou l'autre option dans le menu déroulant sous *Update Class*. Vous pouvez faire cela de sorte que lorsque vous examinerez les points d'accès non classifiés à l'avenir, vous n'aurez pas à trier une liste entière. Assurez-vous de cliquer sur **Apply** lorsque vous avez terminé.



The screenshot shows the 'ROGUE AP DETAIL' page. The 'Update Class' dropdown menu is open, showing three options: 'Malicious', 'Friendly', and 'Unclassified'. The 'Apply' button is highlighted with a green box.

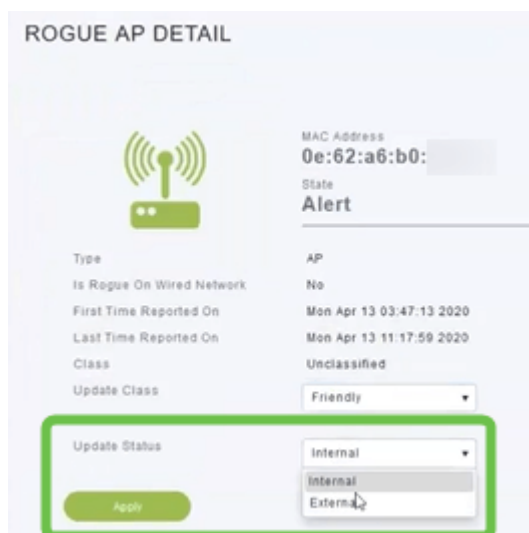
MAC Address: 0e:62:a6:b0:
State: Alert

Type: AP
Is Rogue On Wired Network: No
First Time Reported On: Mon Apr 13 03:47:13 2020
Last Time Reported On: Mon Apr 13 11:17:59 2020
Class: Unclassified

AP Name	SSID	Channels
AP68CA E4	DIRECT-roku-366-69...	11
AP68CA E4	DIRECT-roku-366-69...	11
APA453 0E	DIRECT-roku-366-69...	11

Étape 7 (facultative)

Si vous voulez étiqueter un AP comme *Interne* (dans le réseau) ou *Externe* (peut-être une compagnie voisine) vous pouvez le faire sous la section *Update Status*. Cliquez sur **Apply** lorsque vous avez terminé.



The screenshot shows the 'ROGUE AP DETAIL' page. The 'Update Status' dropdown menu is open, showing three options: 'Internal', 'Internal', and 'External'. The 'Apply' button is highlighted with a green box.

MAC Address: 0e:62:a6:b0:
State: Alert

Type: AP
Is Rogue On Wired Network: No
First Time Reported On: Mon Apr 13 03:47:13 2020
Last Time Reported On: Mon Apr 13 11:17:59 2020
Class: Unclassified

Update Class: Friendly

Update Status: Internal

Afficher les clients indésirables

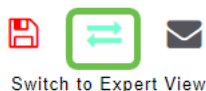
Étape 1

Connectez-vous à l'interface utilisateur Web du point d'accès principal. Pour ce faire, ouvrez un navigateur Web et entrez <https://ciscobusiness.cisco>. Vous pouvez recevoir un avertissement avant de continuer. Entrez dans vos informations d'identification.

Vous pouvez également accéder au point d'accès principal en entrant `https://<ipaddress>` (du point d'accès principal) dans un navigateur Web. Pour certaines actions, vous pouvez utiliser l'application Cisco Business Mobile.

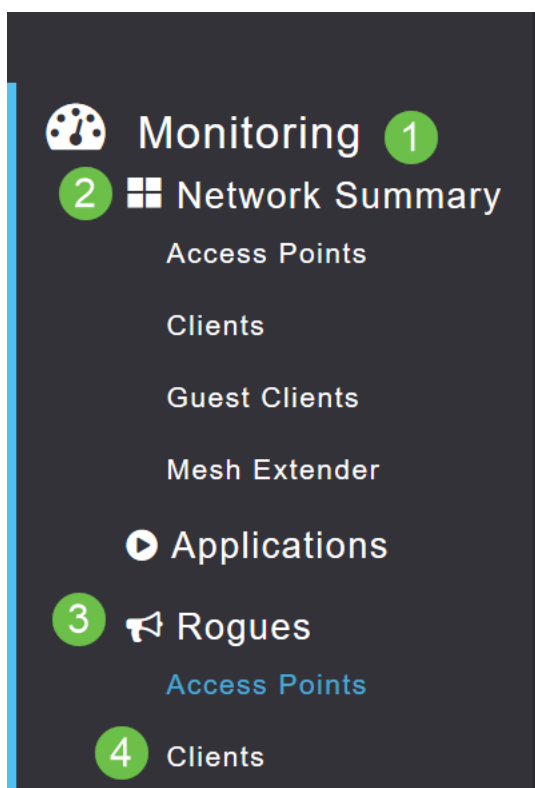
Étape 2

Pour effectuer ces configurations, vous devez vous trouver dans *Expert View*. Cliquez sur l'icône en forme de **flèche** dans le menu supérieur droit de l'interface utilisateur Web pour passer à *Expert View*. Pour plus d'informations sur la configuration d'un serveur RADIUS, consultez [Radius](#)



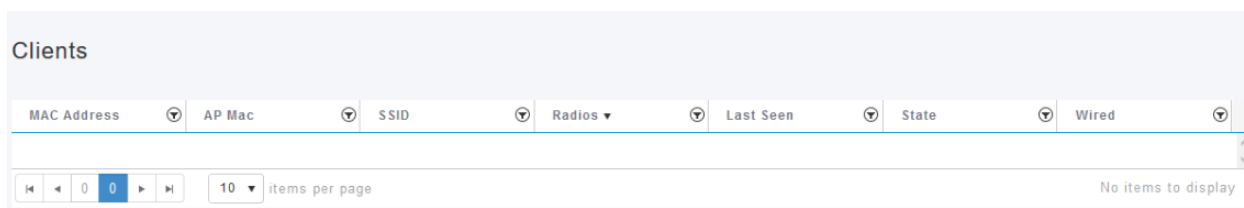
Étape 3

Accédez à **Monitoring > Network Summary > Rogues > Clients**.



Étape 4

S'il y a des clients indésirables, ils seront répertoriés. Dans cet exemple, aucun client non autorisé n'a été détecté.



Conclusion

Vous avez désormais la possibilité de détecter les routeurs sur votre réseau. Si vous voyez beaucoup d'éléments indésirables sur un canal que vous utilisez, vous pouvez changer de canal.

Il y a des considérations à garder à l'esprit, donc consultez l'article de changement de canal RF (lien si disponible).

[Forum aux questions](#) [RADIUS](#) [Mise à niveau du micrologiciel](#) [RLAN](#) [Profilage des applications](#) [Profilage client](#) [Outils du point d'accès principal](#) [Umbrella](#) [Utilisateurs WLAN](#) [Journalisation](#) [Modélisation du trafic](#) [Hors-La-Loi](#) [Brouilleurs](#) [Gestion de la configuration](#) [Mode de maillage de configuration de port](#) [Bienvenue dans CBW](#) [Mesh Networking](#) [Réseau invité utilisant l'authentification de la messagerie et la comptabilité RADIUS](#) [Dépannage](#) [Utilisation d'un routeur Draytek avec CBW](#)

À propos de cette traduction

Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.