

Identificazione di client non idonei in una rete wireless aziendale Cisco

Obiettivo

L'obiettivo di questo articolo è quello di mostrare come identificare i punti di accesso (AP) e i client wireless non autorizzati in una rete tradizionale o mesh Cisco Business Wireless (CBW).

Dispositivi interessati | Versione firmware

- 140AC ([Scheda tecnica](#)) | 10.0.1.0 (scarica la versione più recente)
- 141ACM ([scheda tecnica](#)) | 10.0.1.0 ([scarica la versione più recente](#)) - gli estensori vengono utilizzati solo in reti mesh
- 142ACM ([scheda tecnica](#)) | 10.0.1.0 ([scarica la versione più recente](#)) - gli estensori vengono utilizzati solo in reti mesh
- 143ACM ([scheda tecnica](#)) | 10.0.1.0 ([scarica la versione più recente](#)) - gli estensori vengono utilizzati solo in reti mesh
- 145AC ([Scheda tecnica](#)) | 10.0.1.0 (scarica la versione più recente)
- 240AC ([Scheda tecnica](#)) | 10.0.1.0 (scarica la versione più recente)
- 150AX ([data sheet](#)) | 10.3.2.0 (scarica la versione più recente)
- 151AXM ([scheda tecnica](#)) | 10.3.2.0 (scarica la versione più recente)

I dispositivi CBW serie 15x non sono compatibili con i dispositivi CBW serie 14x/240 e la coesistenza sulla stessa LAN non è supportata.

Introduzione

I CBW Access Point (AP) sono basati su 802.11 a/b/g/n/ac (Wave 2), con antenne interne. Possono essere utilizzati come dispositivi standalone tradizionali o come parte di una rete mesh.

In un mondo perfetto, tutti sarebbero rispettosi e onesti quando utilizzano la vostra rete wireless. Sfortunatamente, non viviamo in un mondo perfetto. In qualità di amministratore, il tuo compito è quello di essere consapevole di qualsiasi potenziale problema.

I punti di accesso non autorizzati sono punti di accesso installati in una rete senza l'autorizzazione dell'utente. I client non autorizzati sono tutti i dispositivi rilevati che non appartengono alla società.

Queste connessioni potrebbero essere totalmente innocenti, ma c'è sempre il rischio che questi truffatori tentino di attaccare la rete o di rubare informazioni sensibili. Per continuare, è possibile visualizzare i punti di accesso e i client non autorizzati. Una volta rilevati, questi router non possono essere bloccati tramite l'access point, ma forniscono informazioni per ulteriori indagini.

Gli access point CBW rilevano solo i canali che si stanno usando o i canali che si sovrappongono.


Visualizza punti di accesso non autorizzati

In questa sezione alternata vengono evidenziati i suggerimenti per i principianti.


Login

Accedere all'interfaccia utente Web dell'access point primario. A tale scopo, aprire un browser Web e immettere <https://ciscobusiness.cisco>. È possibile che venga visualizzato un avviso prima di procedere. Immettere le credenziali. È inoltre possibile accedere all'access point primario immettendo [https://\[ipaddress\]](https://[ipaddress]) (dell'access point primario) in un browser Web.

Descrizione comandi

In caso di domande su un campo nell'interfaccia utente, cercare una descrizione comando simile alla seguente: 

Impossibile individuare l'icona Espandi menu principale.

Passare al menu sul lato sinistro dello schermo. Se il pulsante non è visibile, fare clic su questa icona per aprire il menu della barra laterale. 

Cisco Business App

Questi dispositivi dispongono di app complementari che condividono alcune funzionalità di gestione con l'interfaccia utente Web. Non tutte le funzionalità nell'interfaccia utente Web saranno disponibili nell'app.

[Scarica l'app iOS](#) [Scarica l'app per Android](#)

Domande frequenti

Se hai ancora domande a cui non hai risposto, puoi controllare il nostro documento delle domande frequenti. [Domande frequenti](#)

Passaggio 1

Accedere all'interfaccia utente Web dell'access point primario. A tale scopo, aprire un browser Web e immettere <https://ciscobusiness.cisco>. È possibile che venga visualizzato un avviso prima di procedere. Immettere le credenziali.

È inoltre possibile accedere all'access point primario immettendo <https://<indirizzoIP>> (dell'access point primario) in un browser Web.

Se non conosci i termini utilizzati, consulta [Cisco Business: Glossario dei nuovi termini](#).

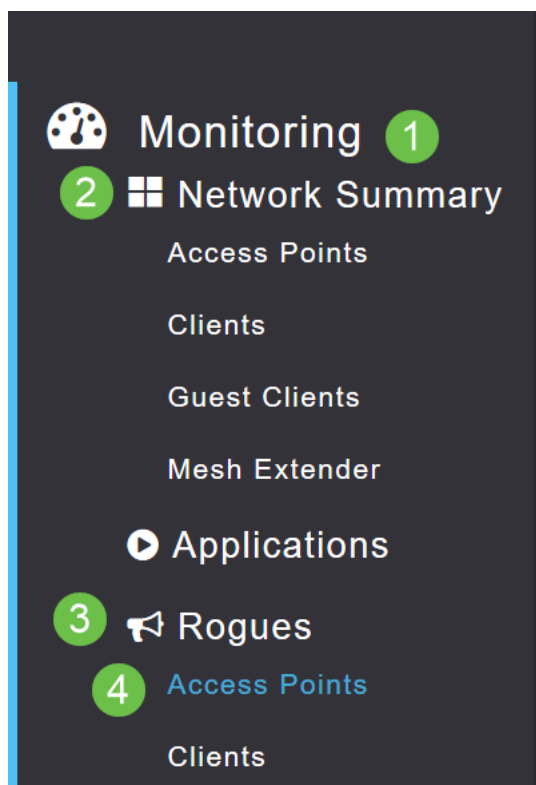
Passaggio 2

Per eseguire queste configurazioni, è necessario che sia attiva la *visualizzazione Esperti*. Fare clic sull'**icona a forma di freccia** nel menu in alto a destra dell'interfaccia utente Web per passare alla *visualizzazione avanzata*.



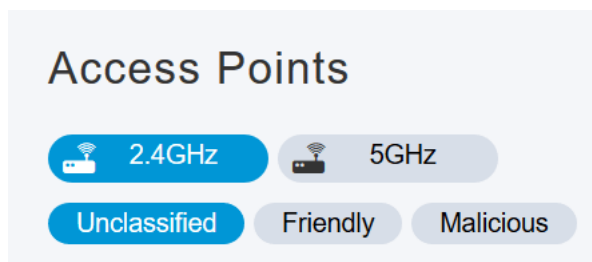
Passaggio 3

Passare a **Monitoraggio > Sintetico rete > Canali > Access point.**



Passaggio 4

Una volta aperta questa pagina, è possibile scegliere di visualizzare 2.4 GHz o 5 GHz facendo clic sulla scheda. Per impostazione predefinita, tutti i punti di accesso non autorizzati sono contrassegnati come Non classificato. Il punto di accesso non modifica le etichette dei punti di accesso non autorizzati, come si farebbe manualmente.



Passaggio 5

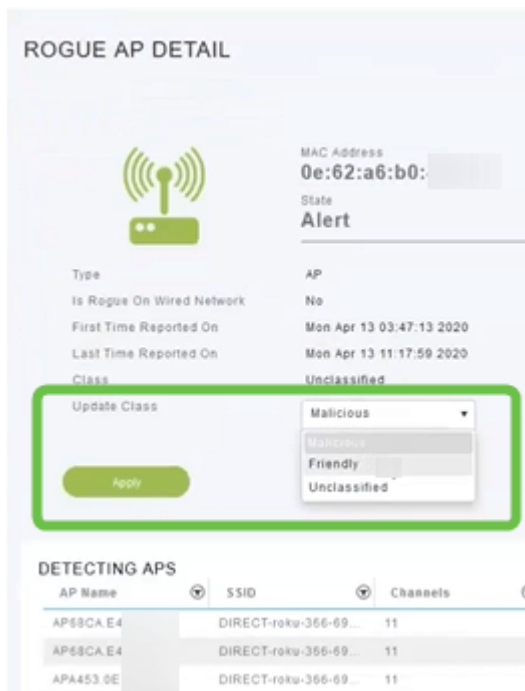
I punti di accesso non autorizzati sono elencati, è possibile fare clic su uno qualsiasi di essi per indagare ulteriormente.

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

MAC Address	SSID	Channels	Radios	Cli
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
0c:c8:1f:fa:5...	LivCam_FA5574	11	2	0
0e:62:a6:b0:...	DIRECT-roku-366-69...	11	5	0

Passaggio 6 (facoltativo)

Se si desidera classificare uno degli access point come *Friendly* o *Malicious* (Dannoso), è possibile selezionare una delle opzioni dal menu a discesa in *Aggiorna classe*. È consigliabile eseguire questa operazione in modo che in futuro, quando si esamineranno i punti di accesso non classificati, non sarà necessario ordinare l'intero elenco. Al termine, fare clic su **Apply** (Applica).

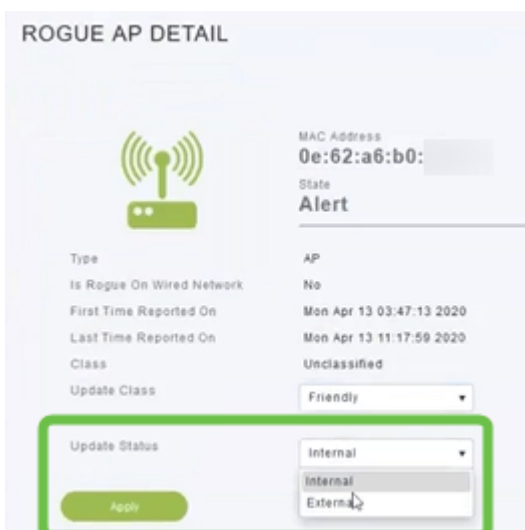


The screenshot shows the 'ROGUE AP DETAIL' page. The MAC Address is 0e:62:a6:b0 and the State is Alert. The 'Update Class' dropdown menu is open, showing options: Malicious, Friendly, and Unclassified. The 'Apply' button is highlighted with a green box.

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

Passaggio 7 (facoltativo)

Se si desidera etichettare un punto di accesso come *Interno* (in rete) o *Esterno* (possibilmente una società vicina), è possibile farlo nella sezione *Aggiorna stato*. Al termine, fare clic su **Apply** (Applica).



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

Visualizza client non autorizzati

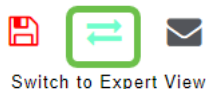
Passaggio 1

Accedere all'interfaccia utente Web dell'access point primario. A tale scopo, aprire un browser Web e immettere <https://ciscobusiness.cisco>. È possibile che venga visualizzato un avviso prima di procedere. Immettere le credenziali.

È inoltre possibile accedere all'access point primario immettendo `https://<indirizzoIP>` (dell'access point primario) in un browser Web. Per alcune azioni, puoi utilizzare l'app Cisco Business Mobile.

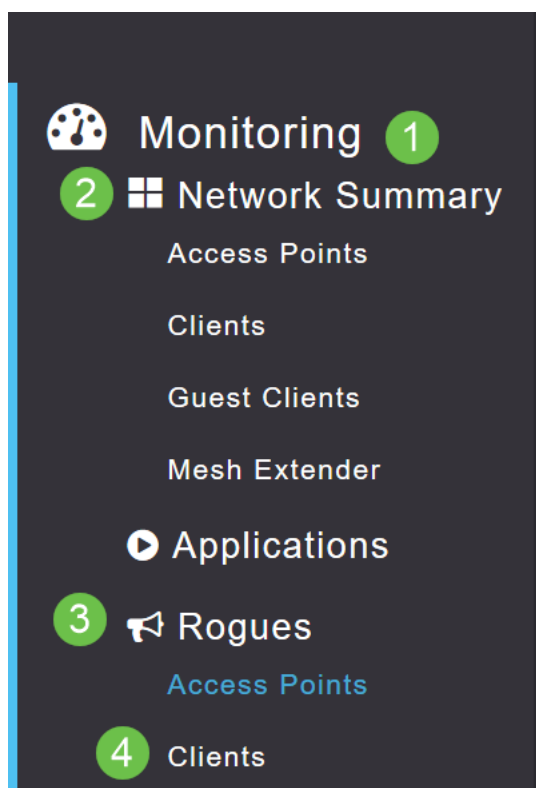
Passaggio 2

Per eseguire queste configurazioni, è necessario che sia attiva la *visualizzazione Esperti*. Fare clic sull'icona a forma di freccia nel menu in alto a destra dell'interfaccia utente Web per passare alla *visualizzazione avanzata*. Per ulteriori informazioni sulla configurazione di un server RADIUS, consultare [Radius](#)



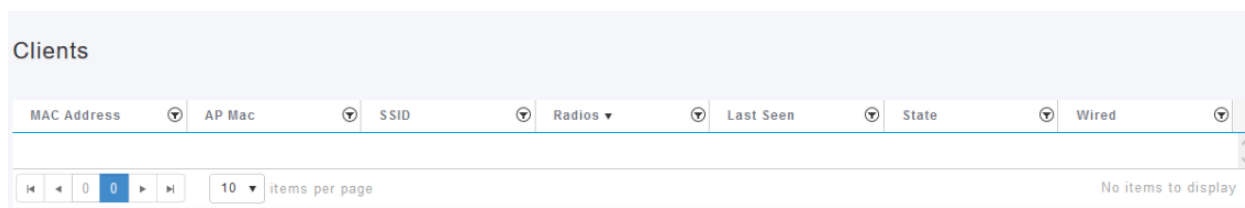
Passaggio 3

Passare a **Monitoraggio > Riepilogo rete > Rogues > Client**.



Passaggio 4

Se ci sono dei clienti canaglia, saranno elencati. Nell'esempio non è stato rilevato alcun client non autorizzato.



Conclusioni

Ora puoi vedere i tizi nella tua rete. Se su un canale in uso vengono visualizzati molti errori, è possibile cambiare canale. È opportuno tenere presenti alcune considerazioni, quindi consultare

l'articolo [Modifica canale RF](#) (collegamento se disponibile).

[Domande frequenti](#) [Raggio](#) [Aggiornamento del firmware](#) [RLAN](#) [Creazione profilo applicazione](#)
[Creazione profilo client](#) [Strumenti AP primari](#) [Umbrella](#) [Utenti WLAN](#) [Registrazione](#) [Traffic Shaping](#)
[Nemici Interferenti](#) [Gestione della configurazione](#) [Port Configuration](#) [Mesh Mode](#) [Benvenuti nella](#)
[sezione CBW](#) [Mesh Networking](#) [Rete guest con autenticazione e-mail e accounting](#) [RADIUS](#)
[Risoluzione dei problemi](#) [Uso di un router Draytek con CBW](#)

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l'accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).