Identificando clientes invasores em uma rede sem fio empresarial da Cisco

Objetivo

O objetivo deste artigo é mostrar como identificar access points (APs) e clientes sem fio invasores em uma rede tradicional ou em malha Cisco Business Wireless (CBW).

Dispositivos aplicáveis | Versão do firmware

- 140AC (Folha de dados) | 10.0.1.0 (Baixe o mais recente)
- 141ACM (Data Sheet) | 10.0.1.0 (Download mais recente) - extensores são usados apenas em uma rede em malha
- 142ACM (Data Sheet) | 10.0.1.0 (Download mais recente) - extensores são usados apenas em uma rede em malha
- 143ACM (Data Sheet) | 10.0.1.0 (Download mais recente) - extensores são usados apenas em uma rede em malha
- 145AC (Folha de dados) | 10.0.1.0 (Baixe o mais recente)
- 240AC (Folha de dados) | 10.0.1.0 (Baixe o mais recente)
- 150AX (Data Sheet) | 10.3.2.0 (Baixe o mais recente)
- 151AXM (Folha de dados) | 10.3.2.0 (Baixe o mais recente)

Os dispositivos CBW série 15x não são compatíveis com os dispositivos CBW série 14x/240 e a coexistência na mesma LAN não é suportada.

Introduction

Os Access Points (APs) CBW são baseados em 802.11 a/b/g/n/ac (onda 2), com antenas internas. Eles podem ser usados como dispositivos autônomos tradicionais ou como parte de uma rede em malha.

Em um mundo perfeito, todos seriam respeitosos e honestos ao usar sua rede sem fio. Infelizmente, não vivemos em um mundo perfeito. Como administrador, seu trabalho é estar ciente de qualquer problema em potencial.

Os APs invasores são APs que foram instalados em uma rede sem a sua permissão. Clientes invasores são quaisquer outros dispositivos detectados que não pertencem à sua empresa.

Essas conexões podem ser totalmente inocentes, mas há sempre o risco de que esses invasores tentem atacar sua rede ou roubar informações confidenciais. Para se manter informado sobre isso, você pode visualizar os APs invasores e os clientes invasores. Uma vez detectados, esses invasores não podem ser bloqueados pelo AP, mas ele fornece informações para investigar mais.

Os APs CBW detectarão apenas os não autorizados nos canais que você está usando atualmente ou os canais que se sobrepõem.

Visualizar APs invasores

Esta seção alternada destaca dicas para iniciantes.

Fazendo login

Faça login na Interface de usuário da Web (IU) do AP principal. Para fazer isso, abra um navegador da Web e digite https://ciscobusiness.cisco. Você pode receber um aviso antes de continuar. Insira suas credenciais.Você também pode acessar o AP principal inserindo https://[ipaddress] (do AP principal) em um navegador da Web.

Dicas de ferramenta

Se você tiver dúvidas sobre um campo na interface do usuário, verifique se há uma dica de ferramenta que se pareça com a seguinte: 

Problemas ao localizar o ícone Expandir Menu Principal?

Navegue até o menu no lado esquerdo da tela. Se você não vir o botão do menu, clique nesse ícone para abrir o menu da barra lateral. 

Aplicativo empresarial da Cisco

Esses dispositivos têm aplicativos associados que compartilham alguns recursos de gerenciamento com a interface de usuário da Web. Nem todos os recursos na interface de usuário da Web estarão disponíveis no aplicativo.

Baixar Aplicativo iOS Baixar Aplicativo Android

Perguntas mais freqüentes

Se você ainda tiver perguntas não respondidas, verifique nosso documento de perguntas frequentes. FAQ

Passo 1

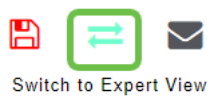
Faça login na Interface de usuário da Web (IU) do AP principal. Para fazer isso, abra um navegador da Web e digite *https://ciscobusiness.cisco*. Você pode receber um aviso antes de continuar. Digite suas credenciais.

Você também pode acessar o AP principal inserindo *https://<ipaddress>* (do AP principal) em um navegador da Web.

Se você não estiver familiarizado com os termos usados, consulte Cisco Business: Glossário de novos termos.

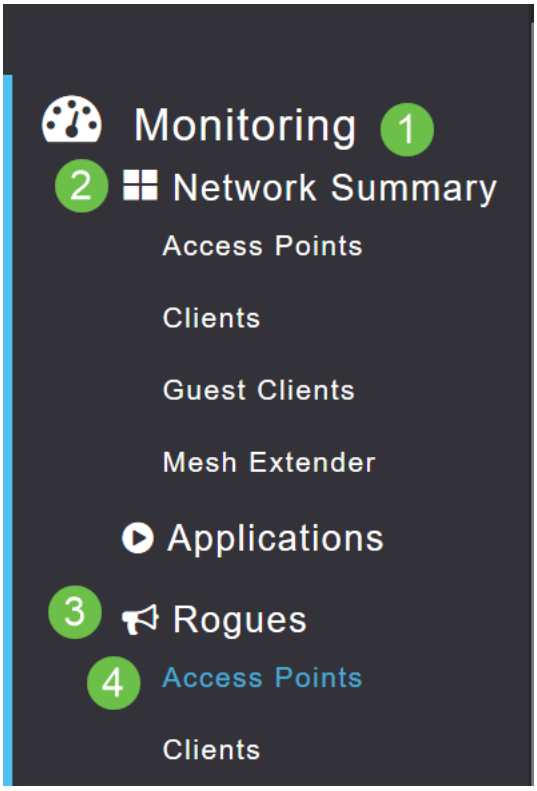
Passo 2

Para fazer essas configurações, você precisa estar na *Expert View*. Clique no **ícone de seta** no menu superior direito da interface do usuário da Web para alternar para *Expert View*.



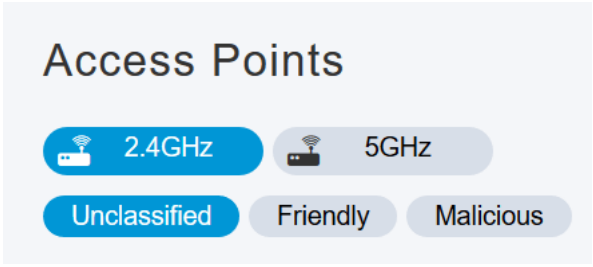
Etapa 3

Navegue até **Monitoring > Network Summary > Rogues > Access Points.**



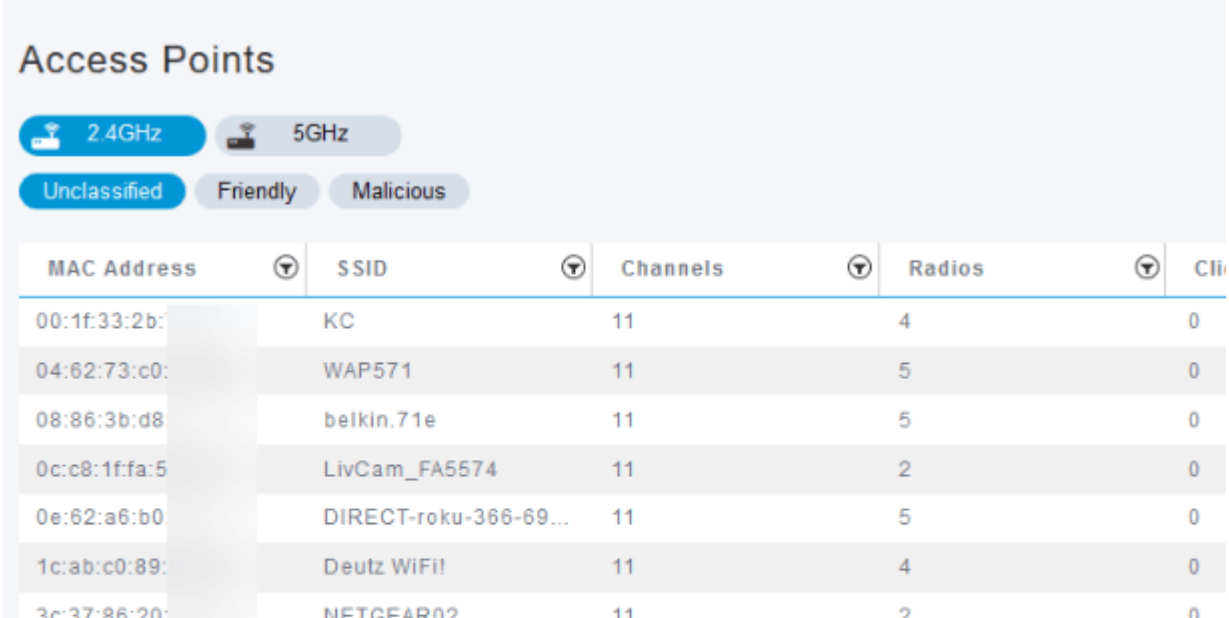
Passo 4

Quando esta página for aberta, você poderá selecionar 2,4 GHz ou 5 GHz clicando na guia. Por padrão, todos os APs invasores são rotulados como Não classificado. O AP não altera os rótulos dos APs invasores, isso é algo que você faria manualmente.



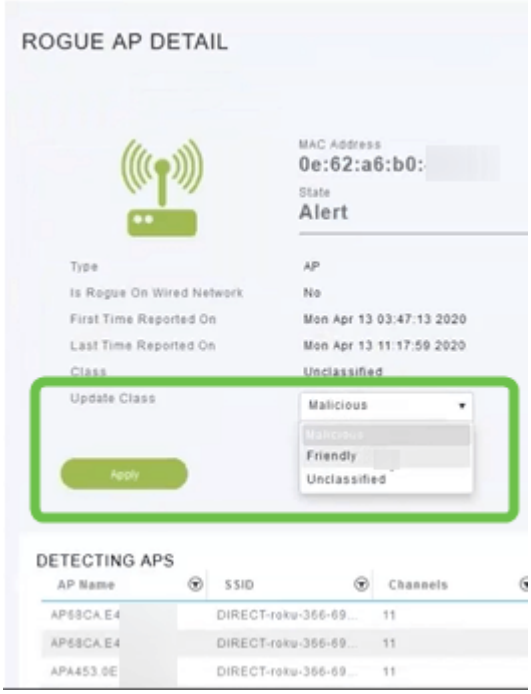
Etapa 5

Os APs invasores estão listados, você pode clicar em qualquer um deles para investigar mais.



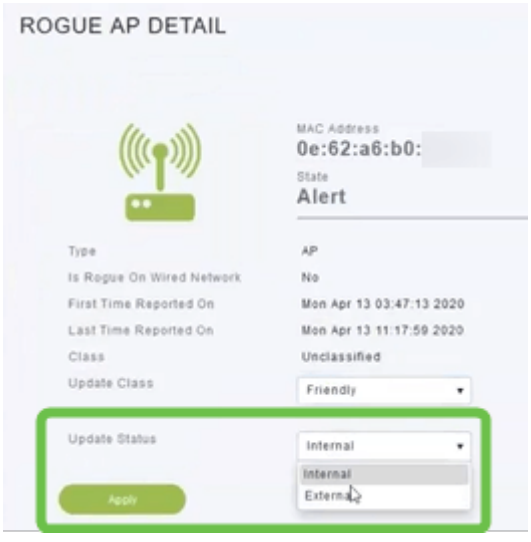
Etapa 6 (opcional)

Se quiser classificar qualquer um dos AP como *Amigável* ou *Mal-intencionado*, você pode selecionar qualquer opção no menu suspenso em *Atualizar classe*. Você pode querer fazer isso para que, ao olhar para Pontos de acesso não classificados no futuro, você não tenha que classificar por uma lista inteira. Certifique-se de clicar em **Aplicar** ao terminar.



Etapa 7 (opcional)

Se você quiser rotular um AP como *Interno* (na rede) ou *Externo* (possivelmente uma empresa vizinha), você pode fazer isso na seção *Atualizar Status*. Clique em **Aplicar** quando terminar.



Visualizar clientes invasores

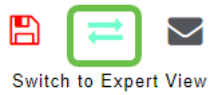
Passo 1

Faça login na interface do usuário da Web do AP principal. Para fazer isso, abra um navegador da Web e digite *https://ciscobusiness.cisco*. Você pode receber um aviso antes de continuar. Digite suas credenciais.

Você também pode acessar o AP principal inserindo *https://<ipaddress>* (do AP principal) em um navegador da Web. Para algumas ações, você pode usar o aplicativo Cisco Business Mobile.

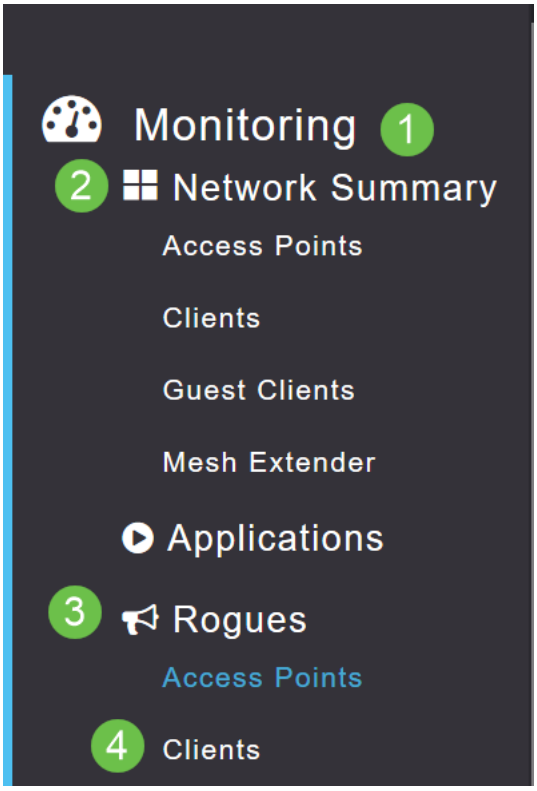
Passo 2

Para fazer essas configurações, você precisa estar na *Expert View*. Clique no **ícone de seta** no menu superior direito da interface do usuário da Web para alternar para *Expert View*. Para obter detalhes sobre como configurar um servidor RADIUS, consulte Radius



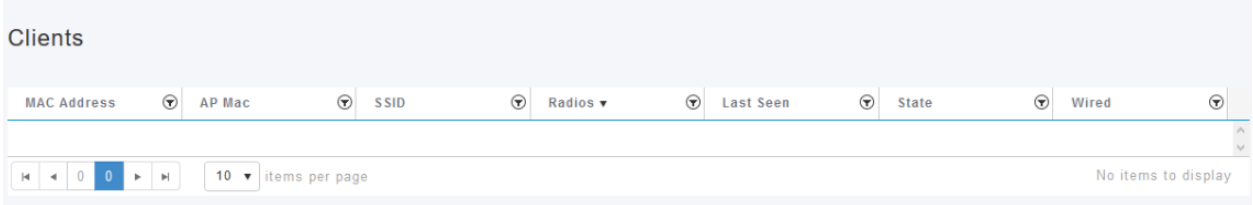
Etapa 3

Navegue até **Monitoring > Network Summary > Rogues > Clients.**



Passo 4

Se houver clientes invasores, eles serão listados. Neste exemplo, nenhum cliente invasor foi detectado.



Conclusão

Agora você pode ver invasores na sua rede. Se você vir muitos invasores em um canal que está usando, poderá alterar o canal. Há considerações a serem lembradas, portanto, consulte o artigo change RF channel (alterar canal RF) (link quando disponível).

Perguntas mais freqüentes Radius Upgrade de firmware RLANS Criação de perfil de aplicativo Criação de perfil do cliente Ferramentas principais de AP Umbrella Usuários de WLAN Registro Modelagem de tráfego Invasores Interferentes Gerenciamento de configuração Modo de malha de configuração de porta Bem-vindo ao CBW Mesh Networking Rede de convidado usando autenticação de e-mail e tarifação RADIUS Troubleshooting Usando um roteador Draytek com CBW

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.