Configuração de porta com RLANs em uma rede CBW

Objetivo

O objetivo deste artigo é criar uma rede RLAN (Remote Local Area Network, rede local remota) e atribuir portas e grupos de pontos de acesso em um AP (Primary Access Point, ponto de acesso primário) Cisco Business Wireless (CBW).

Dispositivos aplicáveis | Versão do software

- 145AC (Data Sheet) | 10.4.1.0 (Baixe o mais recente)
- 240AC (Data Sheet) | 10.4.1.0 (Baixe o mais recente)

Introduction

Os APs CBW são baseados em 802.11 a/b/g/n/ac (onda 2), com antenas internas. Esses APs suportam o mais recente padrão 802.11ac Wave 2 para desempenho mais alto, maior acesso e redes de maior densidade.

Os APs 145AC e 240AC mencionados neste artigo têm a capacidade de ser usados em uma rede tradicional ou em malha. Este artigo usa o equipamento para uma rede sem fio tradicional.

Se você quiser aprender os conceitos básicos de rede em malha, consulte a Cisco Business: Bem-vindo à rede de malha sem fio.

Se preferir fazer a configuração de porta em uma rede em malha, leia Configurar portas Ethernet do Cisco Business Wireless Access Point no Modo Mesh.

Em uma rede sem fio tradicional, uma RLAN é usada para autenticar clientes com fio usando o AP principal. Depois que o cliente com fio ingressa com êxito no AP primário, as portas LAN comutam o tráfego entre os modos de comutação central ou local. O tráfego do cliente com fio é tratado como tráfego de cliente sem fio.

A RLAN envia a solicitação de autenticação para autenticar o cliente com fio. A autenticação do cliente com fio em uma RLAN é semelhante ao cliente sem fio autenticado central.

Se você só precisa de uma rede local virtual (VLAN), não é necessário configurar uma RLAN. Uma RLAN vem no AP por padrão, VLAN 1 nativa. Ele tem segurança aberta e todas as portas são atribuídas a este RLAN por padrão.

Se você não está familiarizado com os termos usados, confira o Cisco Business: Glossário de Novos Termos.

As RLANs não funcionam em uma rede em malha. A malha não está habilitada por padrão, portanto, a menos que você tenha previamente o AP em execução no modo de malha, você está definido para ir.

Configuration Steps

Esta seção alternada destaca dicas para iniciantes.

Login

Efetue login na Interface de usuário da Web (UI) do AP primário. Para 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 primário digitando https://[ipaddress] (Endereço principal do AP) em um navegador da Web.

Dicas de ferramenta

Se você tiver dúvidas sobre um campo na interface do usuário, procure 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 o botão de menu não aparecer, clique nesse ícone para abrir o menu da barra lateral. 

Cisco Business App

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

Download do aplicativo iOS Download do aplicativo Android

Perguntas mais freqüentes

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

Passo 1

Ligue o access point se ele ainda não estiver ligado. Verifique o status das luzes indicadoras. Quando a luz do LED estiver piscando em verde, vá para a próxima etapa.

A inicialização do access point levará de 8 a 10 minutos. O LED piscará em verde em vários padrões, alternando rapidamente entre verde, vermelho e âmbar antes de ficar verde novamente. Pode haver pequenas variações na intensidade e matiz dos LEDs.

Passo 2

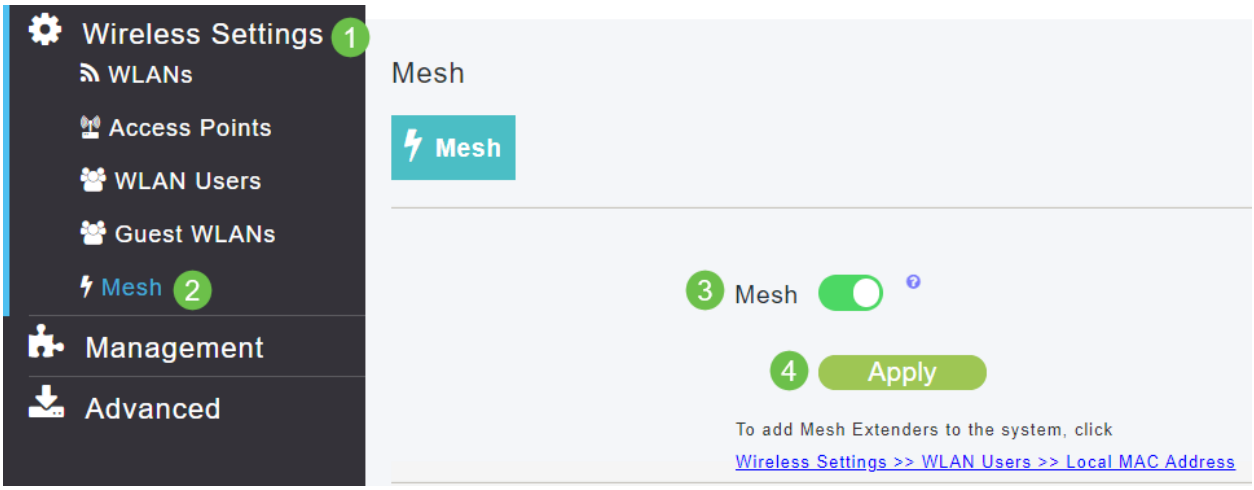
Efetue login na Interface de usuário da Web (UI) do AP primário. Abra um navegador da Web e digite https://ciscobusiness.cisco Você pode receber um aviso antes de continuar. Digite suas credenciais.

Você também pode acessá-lo inserindo o endereço IP do AP primário em um navegador da Web.

Etapa 3

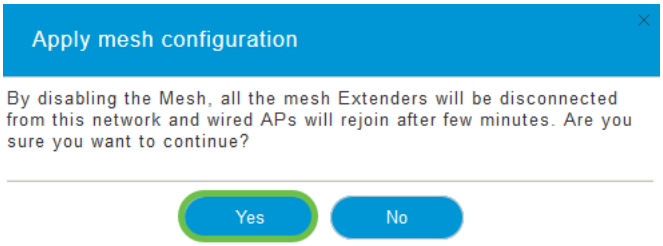
O AP não pode estar no modo mesh para que um RLAN funcione. Para desativar o modo mesh,

navegue até **Wireless Settings > Mesh**. Selecione para desligar a malha. Se o seu AP for novo ou você souber que o modo mesh não está ativado, você poderá passar para a Etapa 7.



Passo 4

Confirme se você deseja desativar o modo de malha clicando em **Sim**.

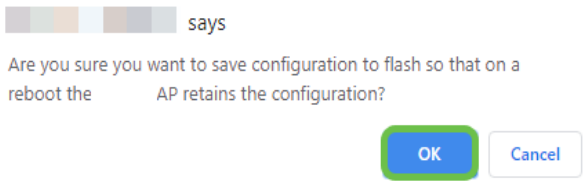


Etapa 5

Certifique-se de salvar suas configurações clicando no **ícone Salvar** no painel superior direito da tela da IU da Web.

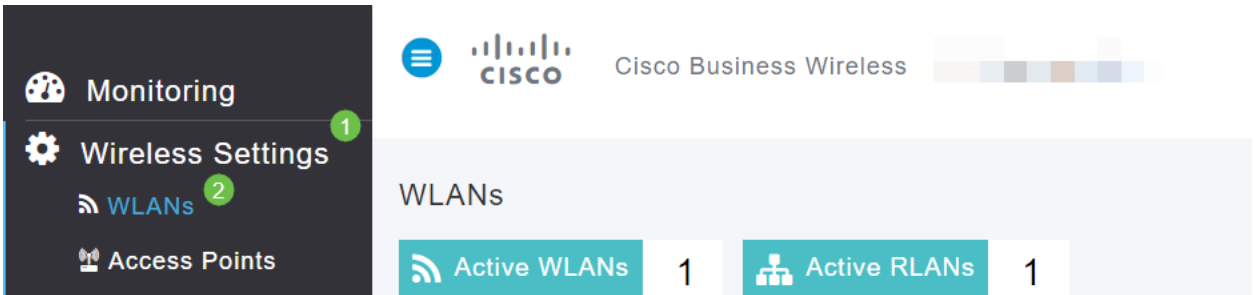
Etapa 6

Confirme a opção Salvar clicando em **OK**. O AP será reinicializado. Isso levará de 8 a 10 minutos para ser concluído.



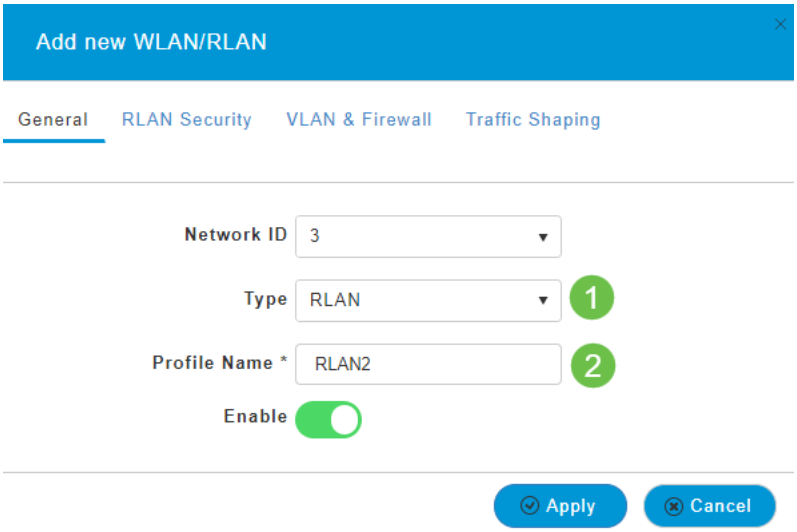
Etapa 7

Uma RLAN pode ser criada navegando para **Wireless Settings > WLANs**. Em seguida, selecione **Add new WLAN/RLAN**.



Passo 8

Selecione **RLAN**. Crie um nome para o perfil.

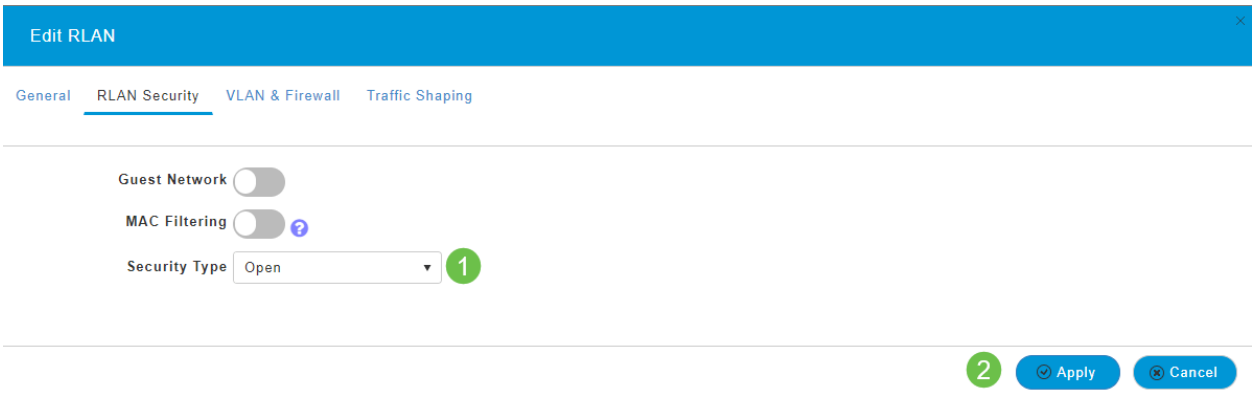


Etapa 9 (Usando a segurança aberta)

Na guia *RLAN Security*. Em *Security Type*, você pode selecionar *Open* ou *802.1X*.

Neste exemplo, o *Tipo de Segurança* foi deixado como padrão.

Clique em Apply. Isso ativará automaticamente essa RLAN de segurança aberta. Vá para a Etapa 11.



Etapa 10a (Usando a segurança 802.1X)

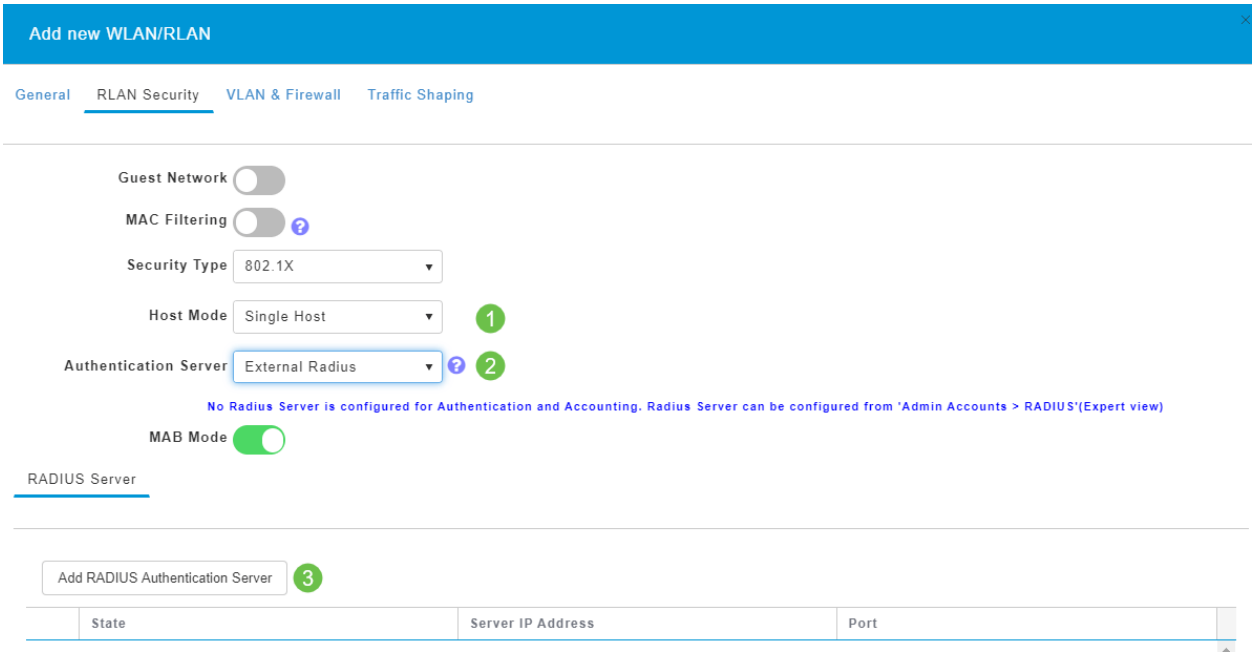
Para configurar o Radius Externo, você deve ter um Servidor Radius configurado em *Contas Administrativas* em *RADIUS* no *Expert View*. Clique no **ícone de seta** no menu superior direito da interface do usuário da Web para alternar para *Expert View*. Para obter detalhes sobre como configurar um servidor RADIUS, consulte Radius

Etapa 10b (Usando a segurança 802.1X)

Se você escolher 802.1X para o Tipo de segurança, mais opções deverão ser selecionadas. Você precisa selecionar o seguinte:

- *Modo de host - Host único* ou *multihost*

- *Servidor de autenticação - Radius externo* ou *AP*
- *Modo MAB - Habilitado* ou *Desabilitado.* Para adicionar endereços MAC, siga as instruções na próxima etapa.

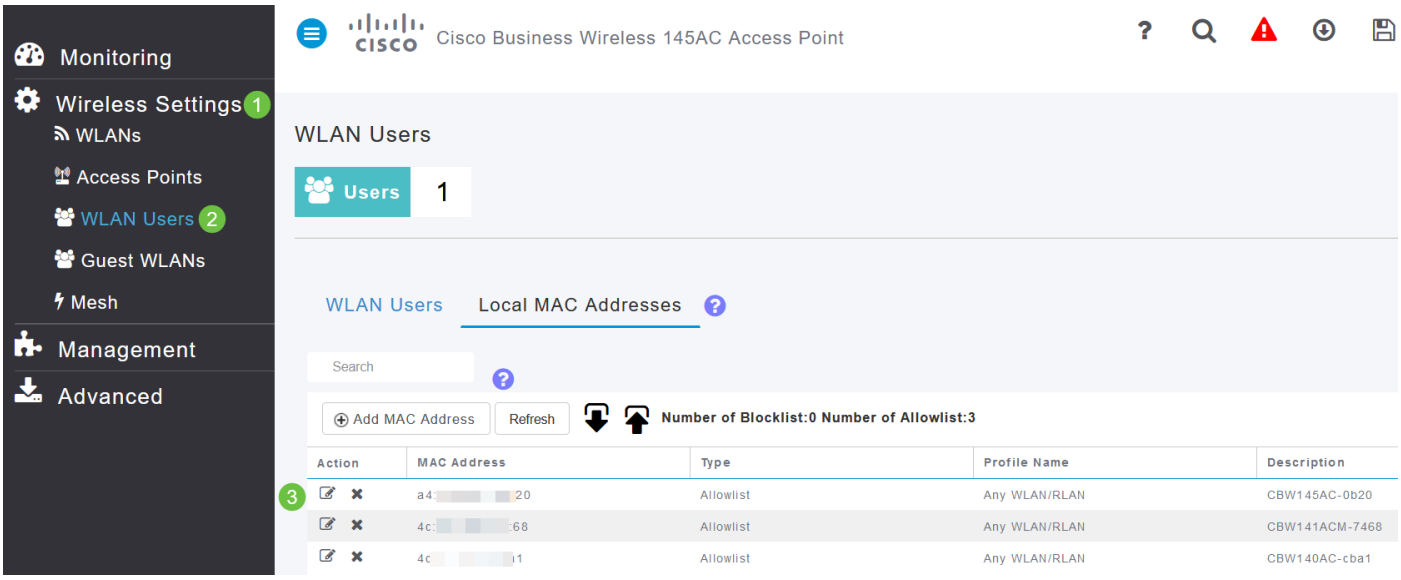


Etapa 11 (Opcional)

O modo MAC Authentication Bypass (MAB) significa que se você tiver um endereço MAC listado em WLAN Users (Usuários da WLAN), o dispositivo não precisará se autenticar. Os endereços MAC listados podem ignorar a autenticação para receber acesso automático à rede ou negado automaticamente. Isso seria útil em um caso em que um telefone IP é conectado a uma porta PoE em um switch.

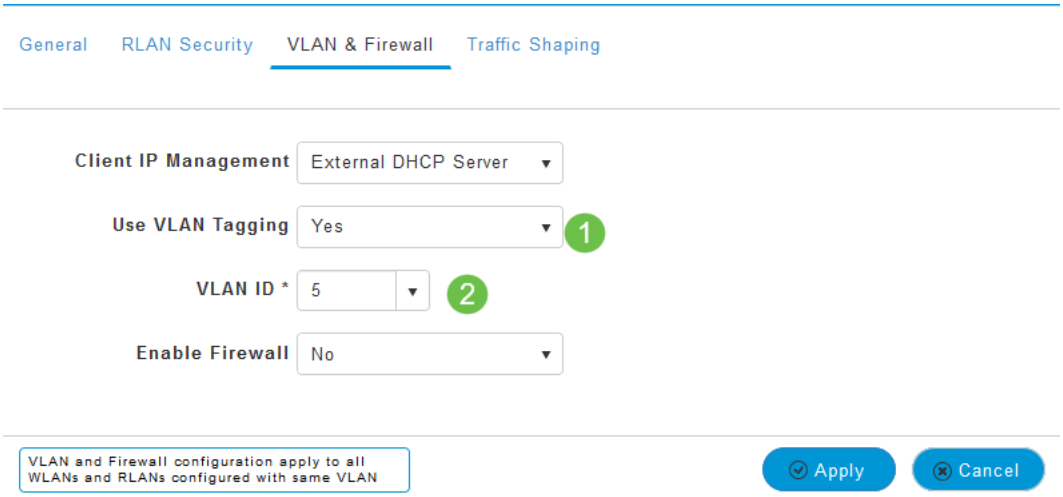
Você pode rotular cada endereço MAC de duas maneiras:

1. *Permitido listado* - O dispositivo recebe acesso automático.
2. *Bloqueado* - O acesso ao dispositivo será automaticamente negado.



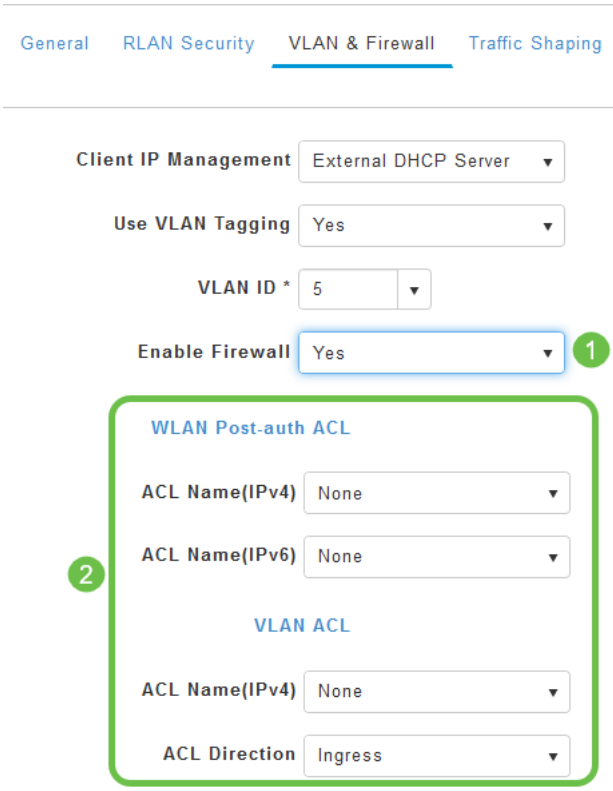
Etapa 12

Na guia *VLAN e firewall*, você pode selecionar Usar *marcação de VLAN* e selecionar um número de *ID de VLAN*.



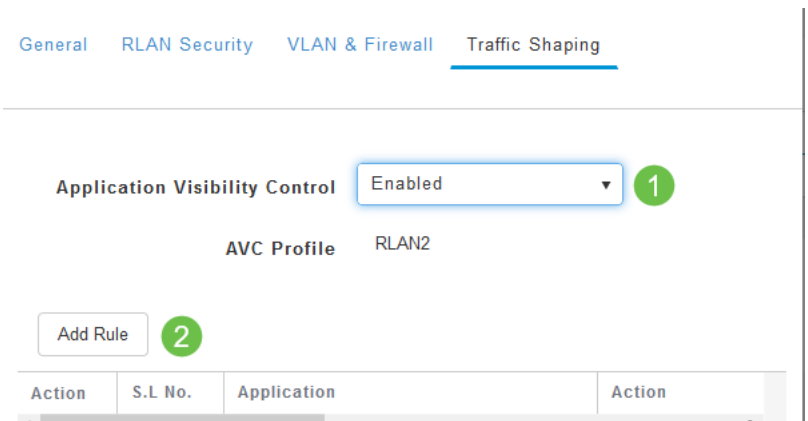
Etapa 13 (Opcional)

Você pode selecionar **Ativar firewall** se quiser configurar *Listas de controle de acesso (ACLs)* que permitem permitir ou rejeitar o acesso para endereços IP ou VLANs específicos. Isso é usado se alguém estiver conectado ao dispositivo de porta de rede para se conectar à rede.



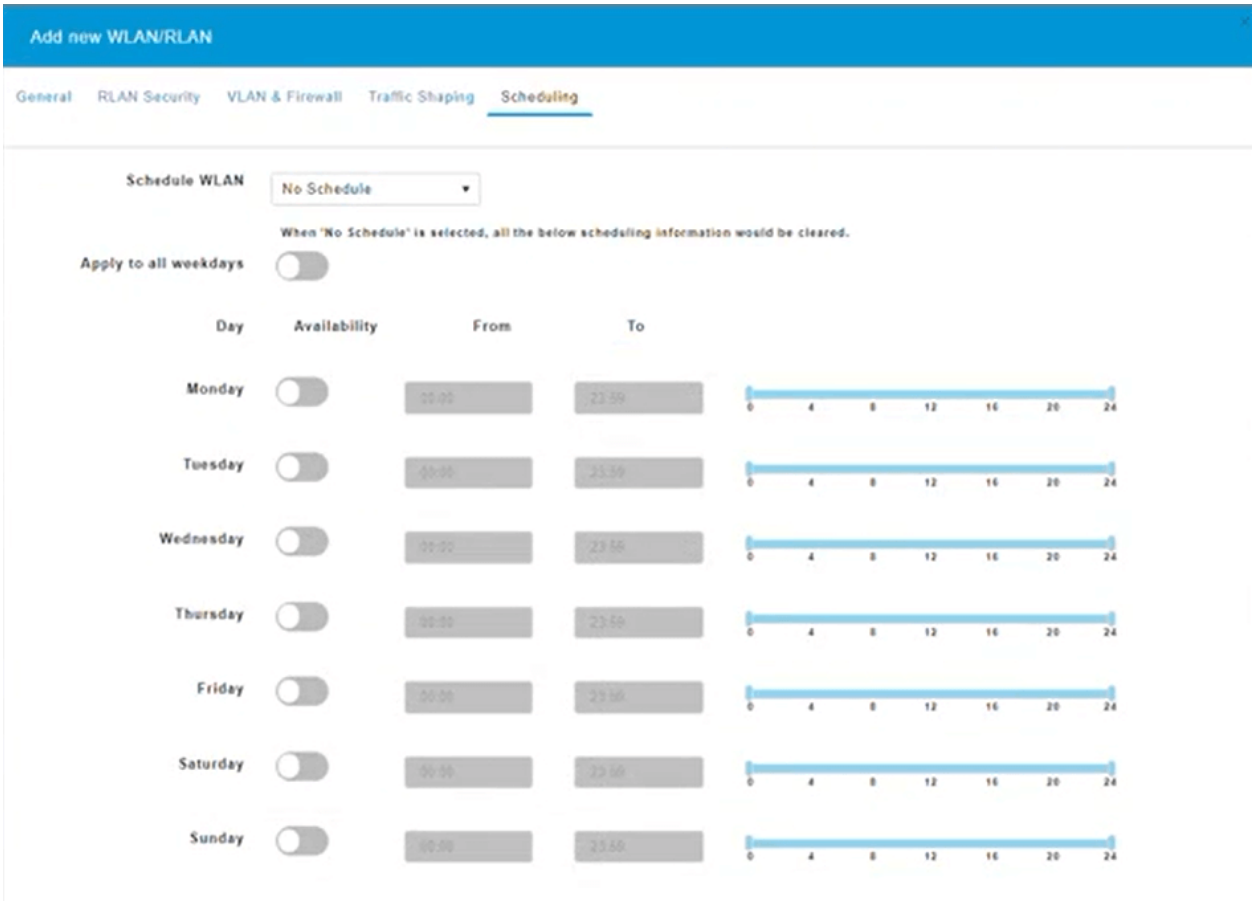
Etapa 14 (Opcional)

Na guia *Traffic Shaping*, você pode configurar a modelagem de tráfego ativando o **Application Visibility Control**. Isso define a priorização do tráfego.



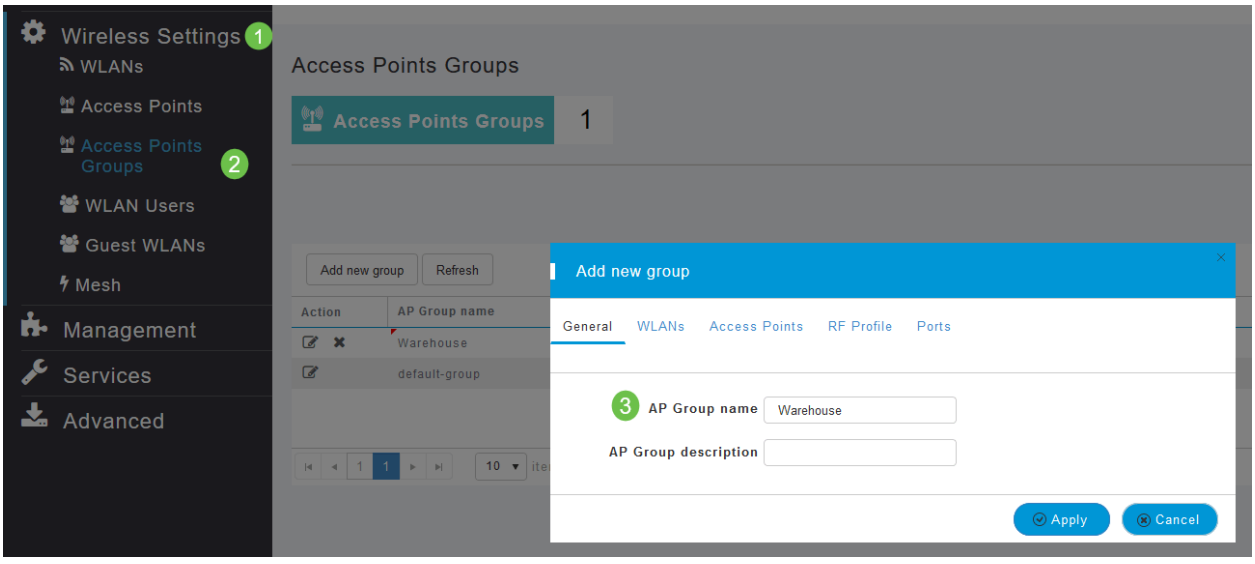
Etapa 15 (Opcional)

Na guia *Programação*, você pode selecionar uma programação. Isso define as horas em que a porta terá a capacidade de ser conectada à rede.



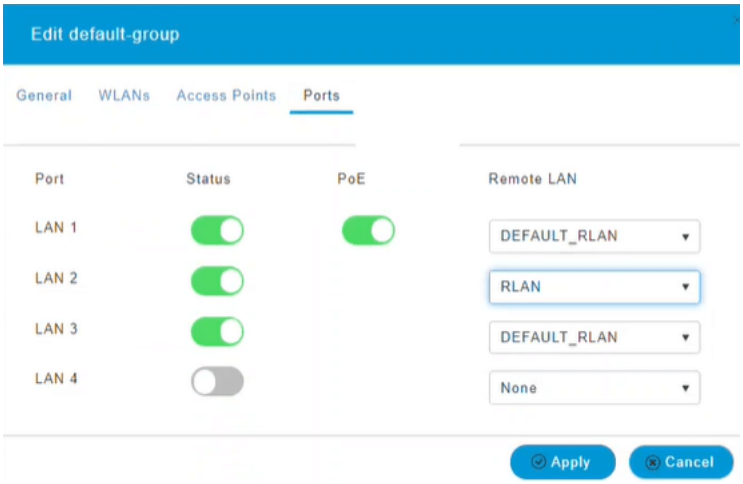
Etapa 16 (Opcional)

Agora que a RLAN foi criada, você pode navegar para **Configurações sem fio > Grupos de pontos de acesso**. É aqui que você pode adicionar ou editar grupos. Para visualizar esta tela, você precisa estar no *Expert View*, que você selecionou na Etapa 10a.



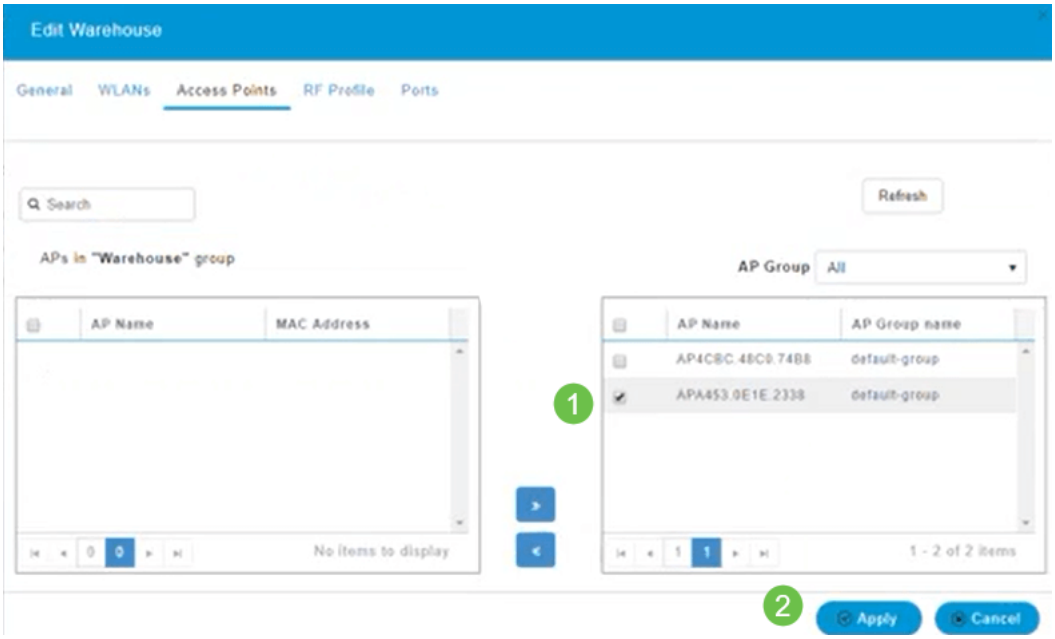
Etapa 17

Na guia *Portas*, você pode atribuir as Portas no AP a LANs remotas específicas.



Etapa 18

Na guia *Pontos de Acesso*, você precisa atribuir um ponto de acesso específico a esse Grupo de Pontos de Acesso. Clique em Apply.



Etapa 19

Selecione **Sim** para confirmar.

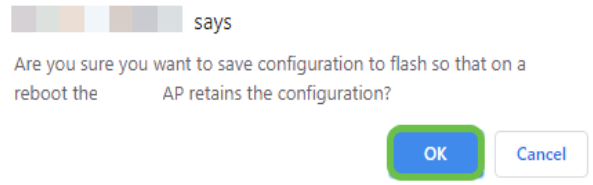
Etapa 20

Certifique-se de salvar suas configurações clicando no **ícone Salvar** no painel superior direito da tela da IU da Web.

Etapa 21

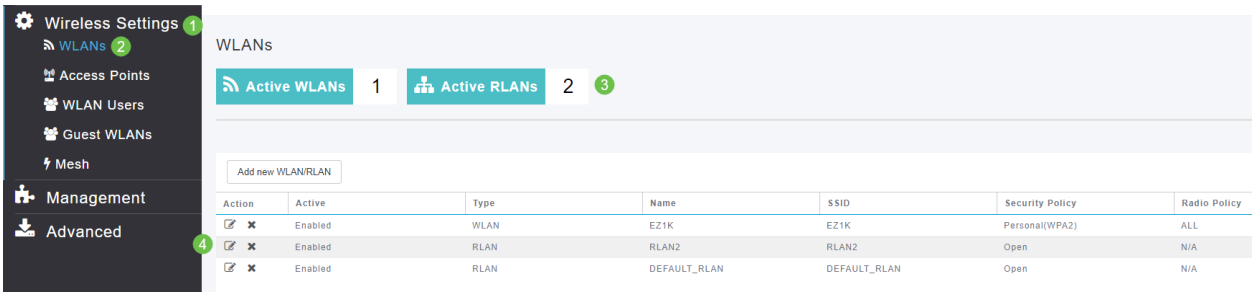
Confirme a opção Salvar clicando em **OK**. O AP será reinicializado. Isso levará de 8 a 10 minutos

para ser concluído.



Exibir o RLAN

Para ver a RLAN que você criou, selecione **Wireless Settings > WLANs**. Você verá o número de RLANs ativas aumentadas para 2 e a nova RLAN será listada.

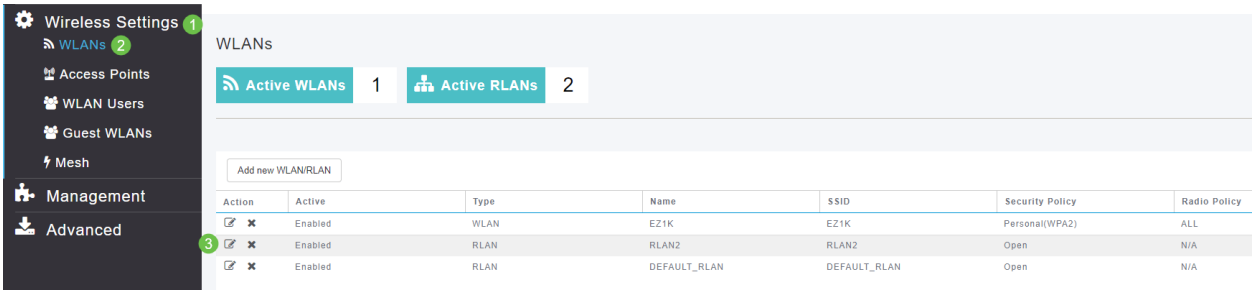


Edite o RLAN

Quando você clicou em **Apply** no final da configuração do RLAN, o RLAN foi ativado automaticamente. Se você precisar desabilitar o RLAN ou fazer outras alterações, siga estas etapas simples abaixo.

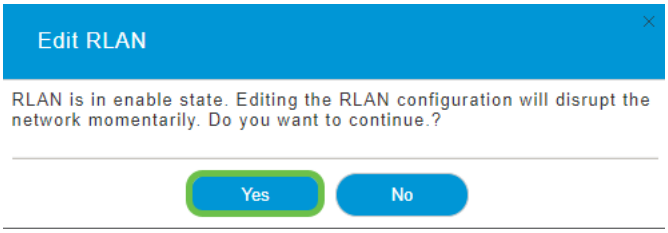
Passo 1

Selecione **Wireless Settings > WLANs**. Clique no **ícone de edição**.



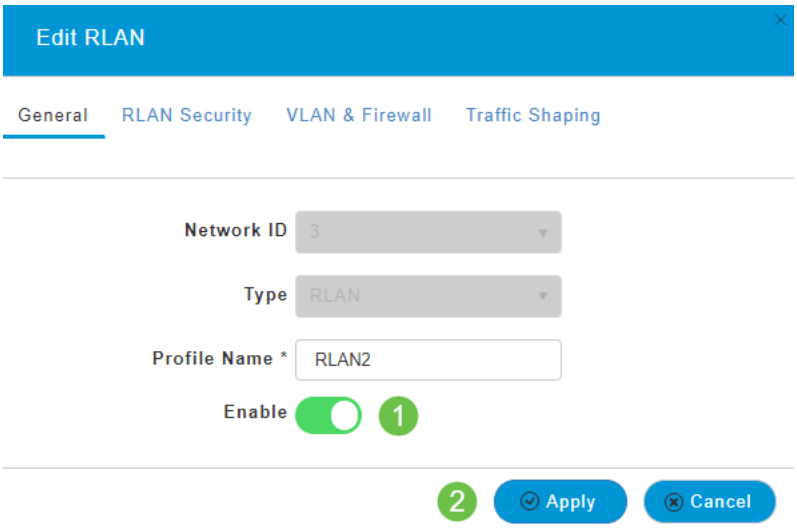
Passo 2

Você receberá um pop-up notificando que a edição do RLAN interromperá a rede em um momento. Confirme se deseja continuar clicando em **Sim**.



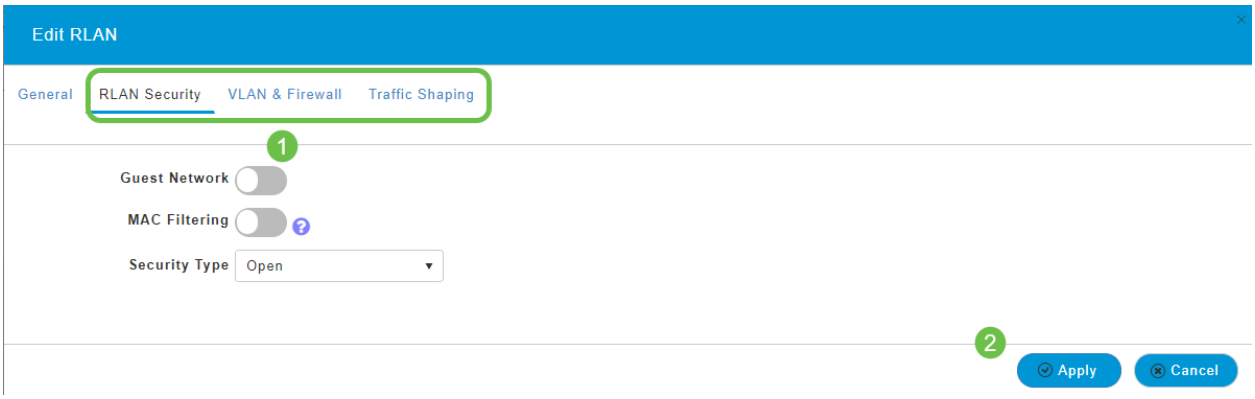
Etapa 3 (Ativar/Desativar)

Na janela **Editar WLAN/RLAN**, em **Geral**, selecione ***Habilitado*** ou ***Desabilitado*** para habilitar/desabilitar a RLAN. Clique em Apply.



Etapa 4 (Edição de outras configurações)

Navegue até as guias *RLAN Security*, *VLAN & Firewall* ou *Traffic Shaping* se precisar alterar as configurações. Clique em **Aplicar** depois de fazer alterações.



Etapa 5

Certifique-se de salvar suas configurações clicando no **ícone Salvar** no painel superior direito da tela da IU da Web.

Conclusão

Agora você criou uma RLAN na sua rede CBW. Aproveite e sinta-se à vontade para adicionar mais se ele se adequar às suas necessidades.

Perguntas mais freqüentes Radius Upgrade de firmware RLANs Criação de perfis de aplicativos Criação de perfil do cliente Principais ferramentas AP Umbrella Usuários de WLAN Registro Modelagem de tráfego Rogues Interferidores Gerenciamento de configuração Modo de malha de configuração de porta Bem-vindo à rede em malha CBW Rede de convidado usando autenticação de e-mail e relatório RADIUS Troubleshooting Usando um roteador Draytek com CBW