Configurar o RADIUS no ponto de acesso sem fio comercial da Cisco

Objetivo

O objetivo deste documento é mostrar a você como configurar o RADIUS no Access Point (AP) Cisco Business Wireless (CBW).

Dispositivos aplicáveis | Versão do firmware

- 140AC (Data Sheet) | 10.4.1.0 (Baixe o mais recente)
- 145AC (Data Sheet) | 10.4.1.0 (Baixe o mais recente)
- 240AC (Data Sheet) | 10.4.1.0 (Baixe o mais recente)

Introduction

Se você está procurando configurar o RADIUS em seu AP CBW, você está no lugar certo! Os APs CBW suportam o padrão 802.11ac Wave 2 mais recente para desempenho mais alto, maior acesso e redes de densidade mais alta. Eles proporcionam o melhor desempenho do setor com conexões sem fio altamente seguras e confiáveis, proporcionando uma experiência robusta e móvel ao usuário final.

O RADIUS (Remote Authentication Dial-In User Service) é um mecanismo de autenticação para que os dispositivos se conectem e usem um serviço de rede. É usado para fins de autenticação, autorização e contabilidade centralizadas. Um servidor RADIUS regula o acesso à rede verificando a identidade dos usuários através das credenciais de login inseridas. Por exemplo, uma rede Wi-Fi pública é instalada em um campus universitário. Apenas os alunos que têm a senha podem acessar essas redes. O servidor RADIUS verifica as senhas digitadas pelos usuários e concede ou nega o acesso à rede local sem fio (WLAN), conforme apropriado.

Se você estiver pronto para configurar o RADIUS em seu AP CBW, vamos começar!

Table Of Contents

Configurar o RADIUS no seu AP CBW

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.

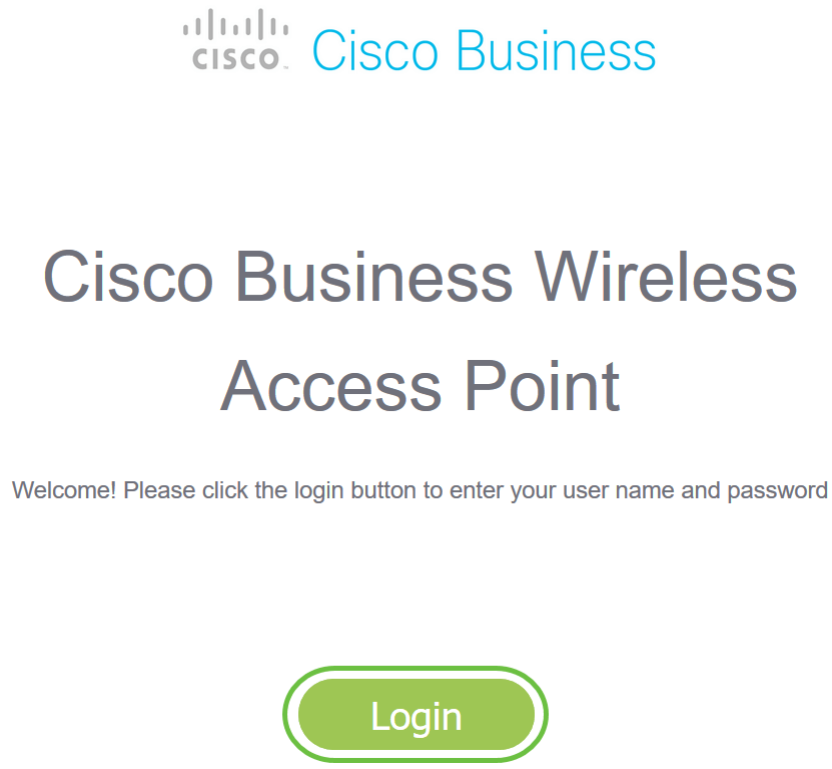
Download do aplicativo iOS Download do aplicativo Android

Perguntas mais freqüentes

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

Passo 1

Faça login no seu AP CBW usando um nome de usuário e uma senha válidos.

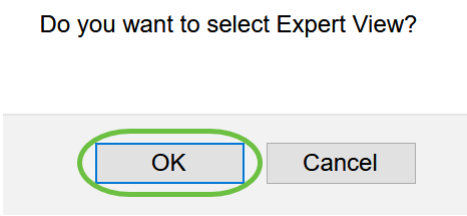


Passo 2

Clique no símbolo de **seta bidirecional** na parte superior da interface do usuário da Web (UI) para

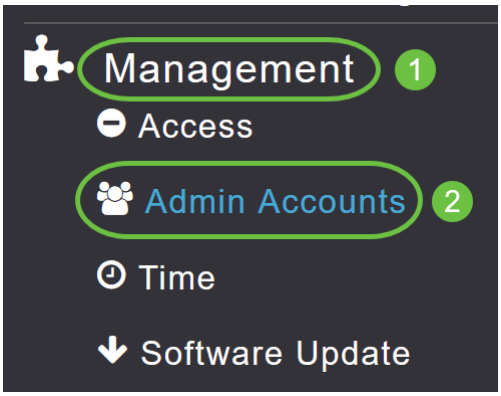
Alternar para o modo de exibição do especialista.

Você verá a seguinte tela pop-up. Clique em **OK** para continuar.



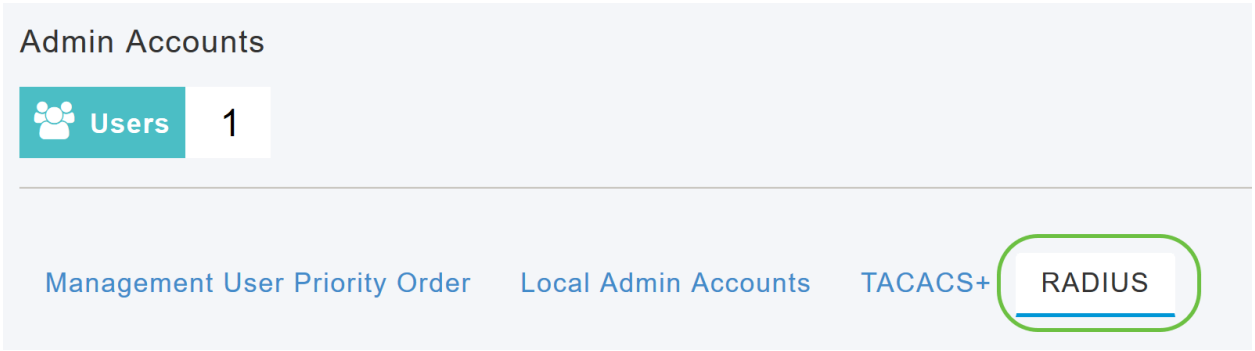
Etapa 3

Navegue até **Gerenciamento > Contas de administração**.



Passo 4

Para adicionar os servidores RADIUS, clique na guia **RADIUS**.

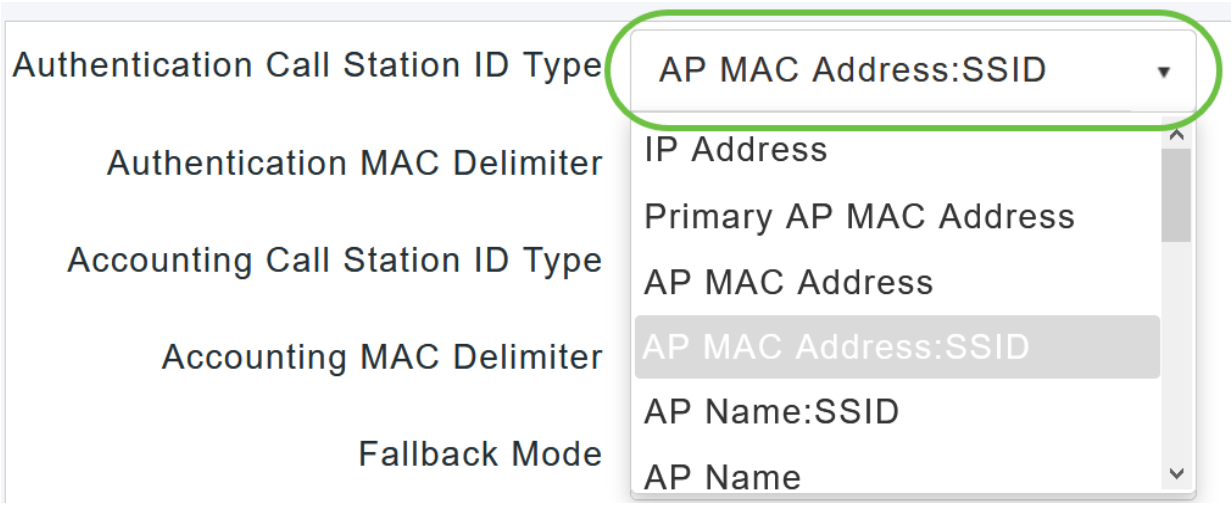


Etapa 5

Na lista suspensa *Authentication Call Station ID Type*, escolha a opção que é enviada ao servidor RADIUS na mensagem Access-Request. As seguintes operações estão disponíveis:

- *IP Address*

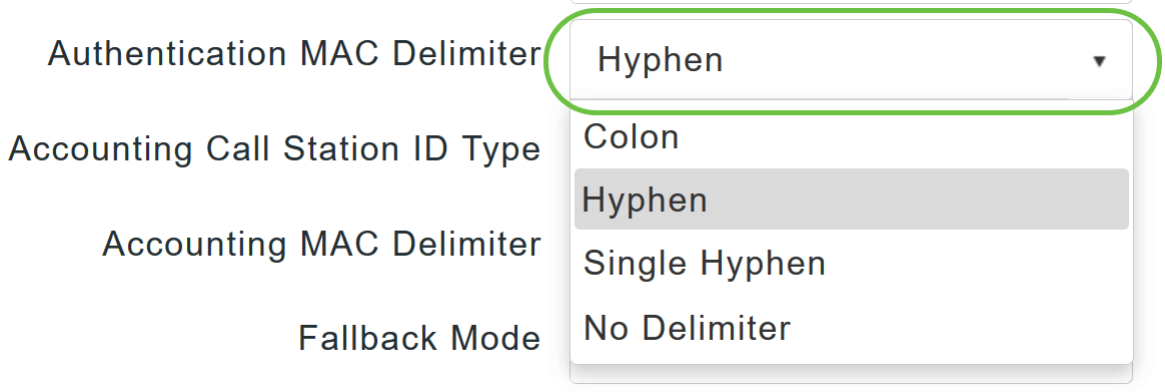
- *Endereço MAC do AP primário*
- *Endereço MAC do AP*
- *Endereço MAC do AP:SSID*
- *Nome do AP:SSID*
- *Nome do AP*
- *Grupo AP*
- *Grupo Flex*
- *Local do AP*
- *ID da VLAN*
- *Endereço MAC Ethernet do AP*
- *Endereço MAC Ethernet do AP:SSID*
- *Endereço do rótulo do AP*
- *Endereço do rótulo do AP:SSID*
- *AP MAC:SSID AP Group*
- *AP Eth MAC:SSID AP Group*



Etapa 6

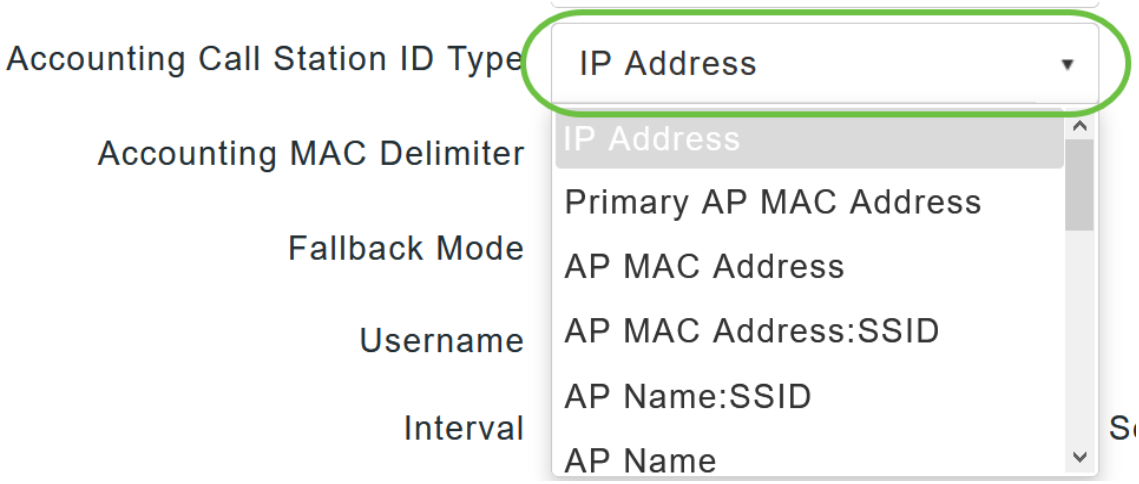
Selecione o *Authentication MAC Delimiter* na lista suspensa. As opções são:

- *Colon*
- *Hífen*
- *hífen único*
- *Sem Delimitador*



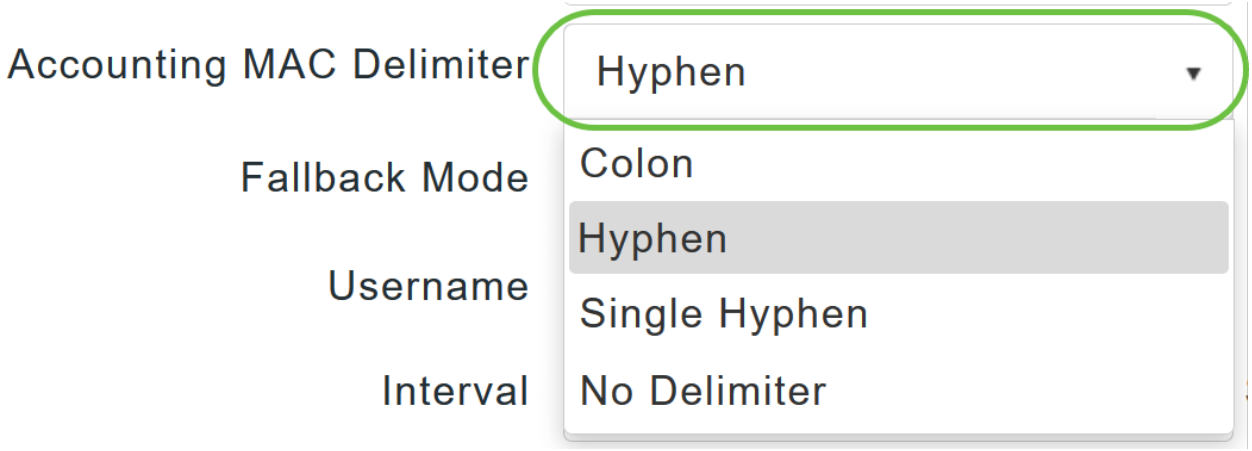
Etapa 7

Escolha o *Tipo de ID da Estação de Chamada Contábil* na lista suspensa.



Passo 8

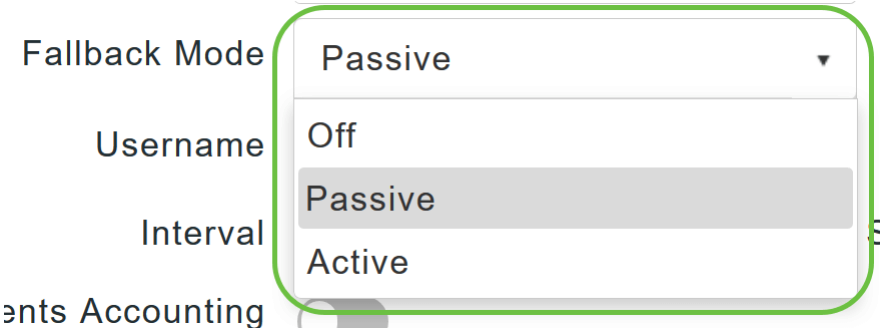
Escolha o *Delimitador MAC de Contabilidade* na lista suspensa.



Passo 9

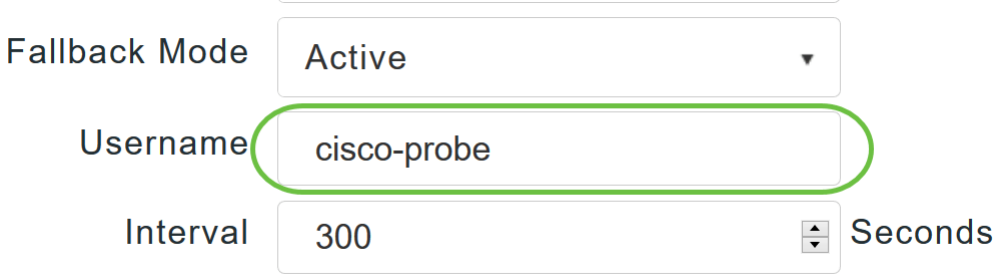
Especifique o *Modo de Fallback* do servidor RADIUS na lista suspensa. Pode ser um dos seguintes:

- *Desativado* - Desativa o fallback do servidor RADIUS. Este é o valor padrão.
- *Passivo* - Faz com que o AP primário reverta para um servidor com uma prioridade mais baixa dos servidores de backup disponíveis sem usar mensagens de sondagem externas. O AP primário ignora todos os servidores inativos por um período e tenta novamente mais tarde quando uma mensagem RADIUS precisa ser enviada.
- *Ativo* - Faz com que o AP principal seja revertido para um servidor com uma prioridade mais baixa dos servidores de backup disponíveis usando mensagens de sondagem RADIUS para determinar proativamente se um servidor marcado como inativo está novamente on-line. O AP primário ignora todos os servidores inativos para todas as solicitações RADIUS ativas. Quando o servidor primário recebe uma resposta do servidor ACS recuperado, o servidor RADIUS de fallback ativo não envia mais mensagens de sondagem ao servidor que solicita a autenticação de sondagem ativa.



Passo 10

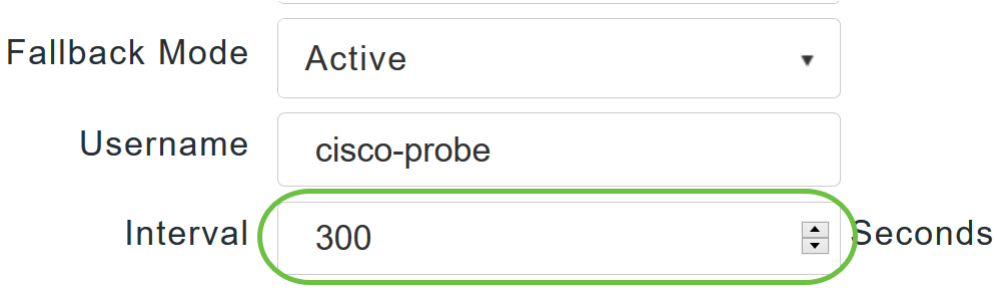
Se você habilitou o *modo Fallback Ativo*, insira o nome a ser enviado nos testadores de servidor inativos no campo *Nome de usuário*.



Você pode digitar até 16 caracteres alfanuméricos. O valor padrão é **cisco-probe**.

Passo 11

Se você habilitou o *modo Fallback Ativo*, insira o valor do intervalo de sondagem (em segundos) no campo Intervalo. O intervalo serve como tempo inativo no modo passivo e intervalo de sondagem no modo ativo.

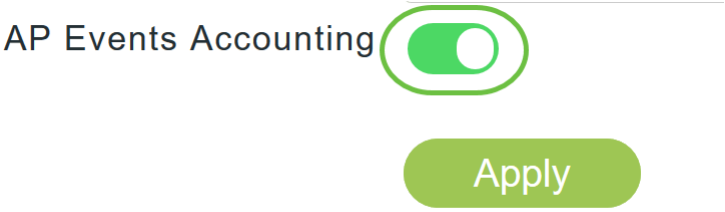


O intervalo válido é de 180 a 3600 segundos, e o valor padrão é **300** segundos.

Etapa 12

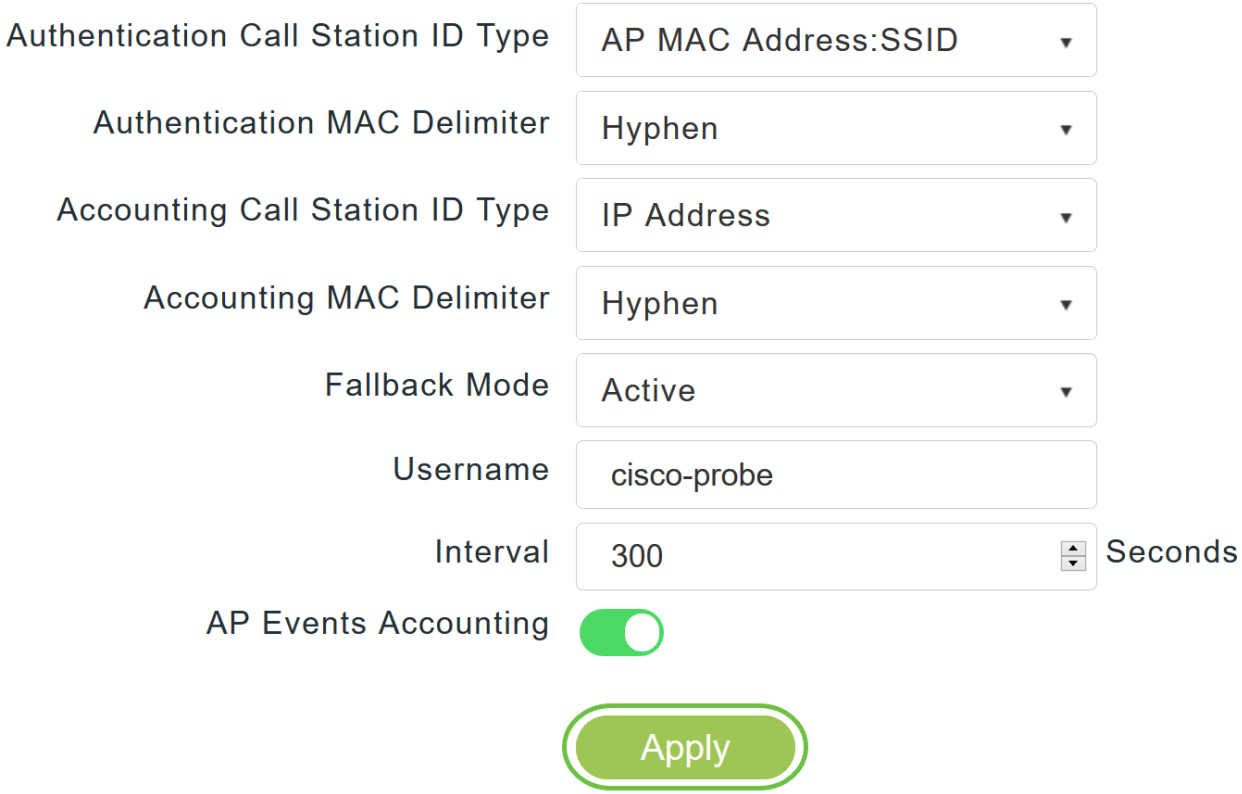
Habilite o botão deslizante *Contabilidade de Eventos de AP* para ativar o envio de solicitações de contabilização para o servidor RADIUS.

Durante problemas de rede, os APs se juntam/desligam do AP principal. Habilitar essa opção garante que esses eventos sejam monitorados e que as solicitações de contabilização sejam enviadas ao servidor RADIUS para ajudar a detectar os problemas de rede.



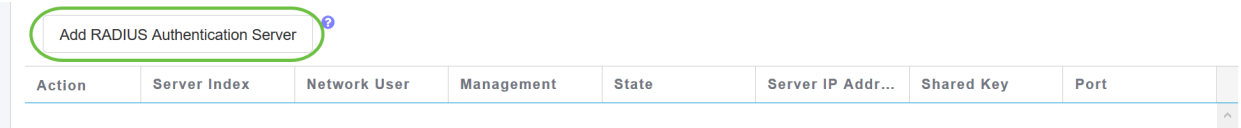
Passo 13

Clique em Apply.



Passo 14

Para configurar o servidor de autenticação RADIUS, clique em **Adicionar servidor de autenticação RADIUS**.



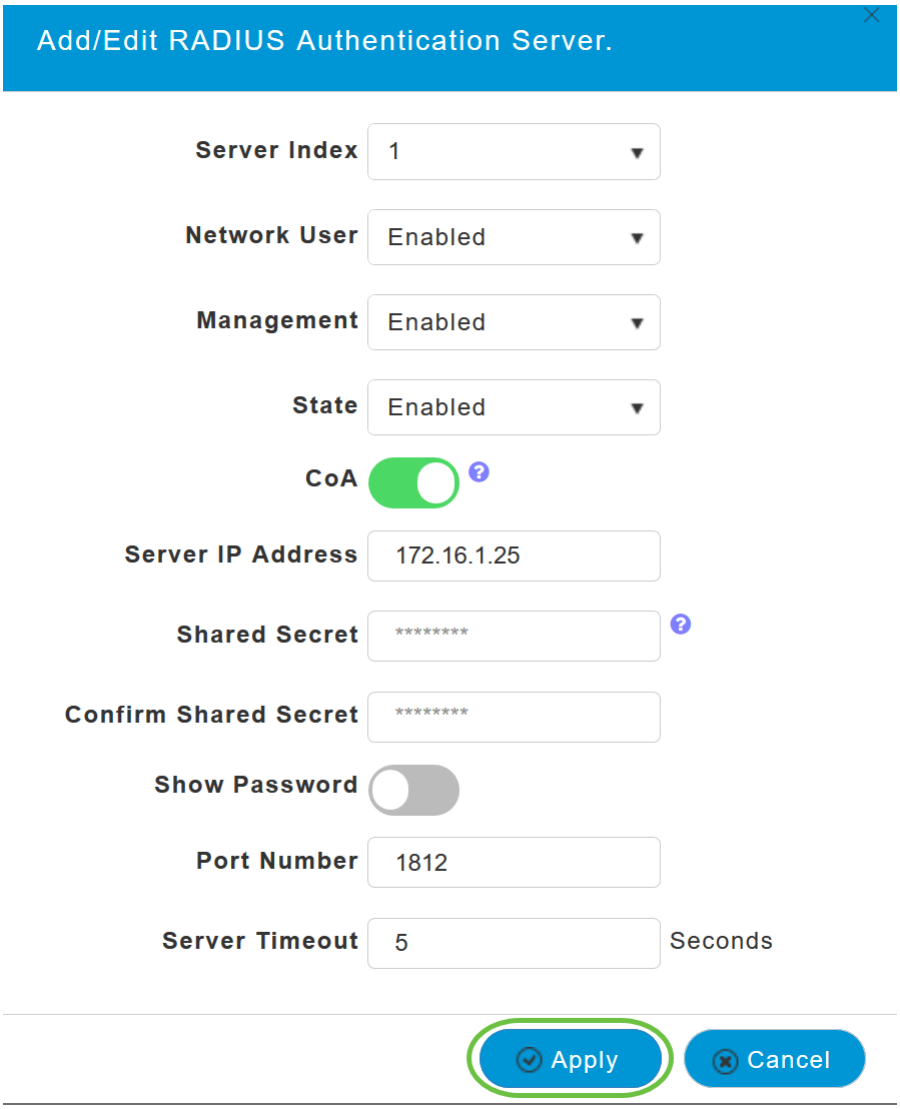
Etapa 15

Na janela pop-up *Add/Edit RADIUS Authentication*, configure o seguinte:

- *Índice do servidor* - Selecione de 1 a 6
- *Network User* - Ative o estado. Por padrão, esta opção está Ativada
- *Management* - Enable the state (Gerenciamento - Habilitar o estado). Por padrão, esta opção está Ativada
- *State* - Enable the state (Estado). Por padrão, esta opção está Ativada
- *CoA* - Você pode optar por habilitar essa opção movendo o botão do controle deslizante

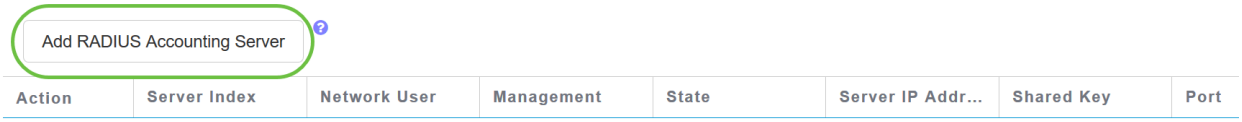
- *Server IP Address (Endereço IP do servidor)* - Insira o endereço IPv4 do servidor RADIUS
- *Shared Secret* - Insira o segredo compartilhado
- *Port Number* - (Número da porta) Insira o número da porta que está sendo usada para se comunicar com o servidor RADIUS.
- *Server Timeout* - Insira o tempo limite do servidor

Clique em Apply.



Passo 16

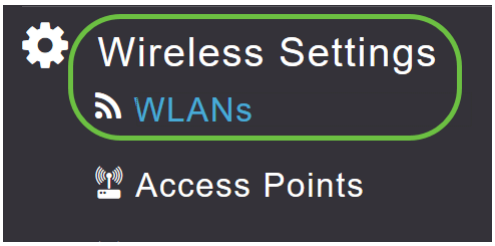
Para Adicionar o *Servidor de Contabilidade RADIUS*, siga as mesmas etapas da Etapa 15, pois a página contém campos semelhantes.



Configurar WLAN

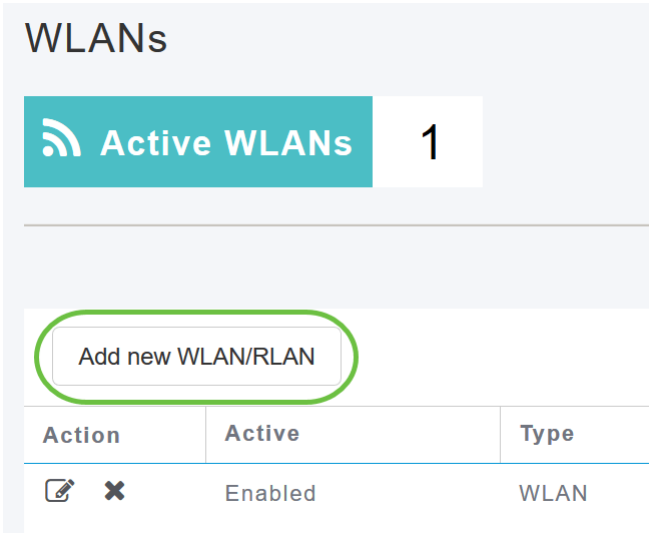
Passo 1

Para configurar a WLAN que irá processar a autenticação WPA2 com RADIUS, navegue para **Wireless settings > WLAN**.



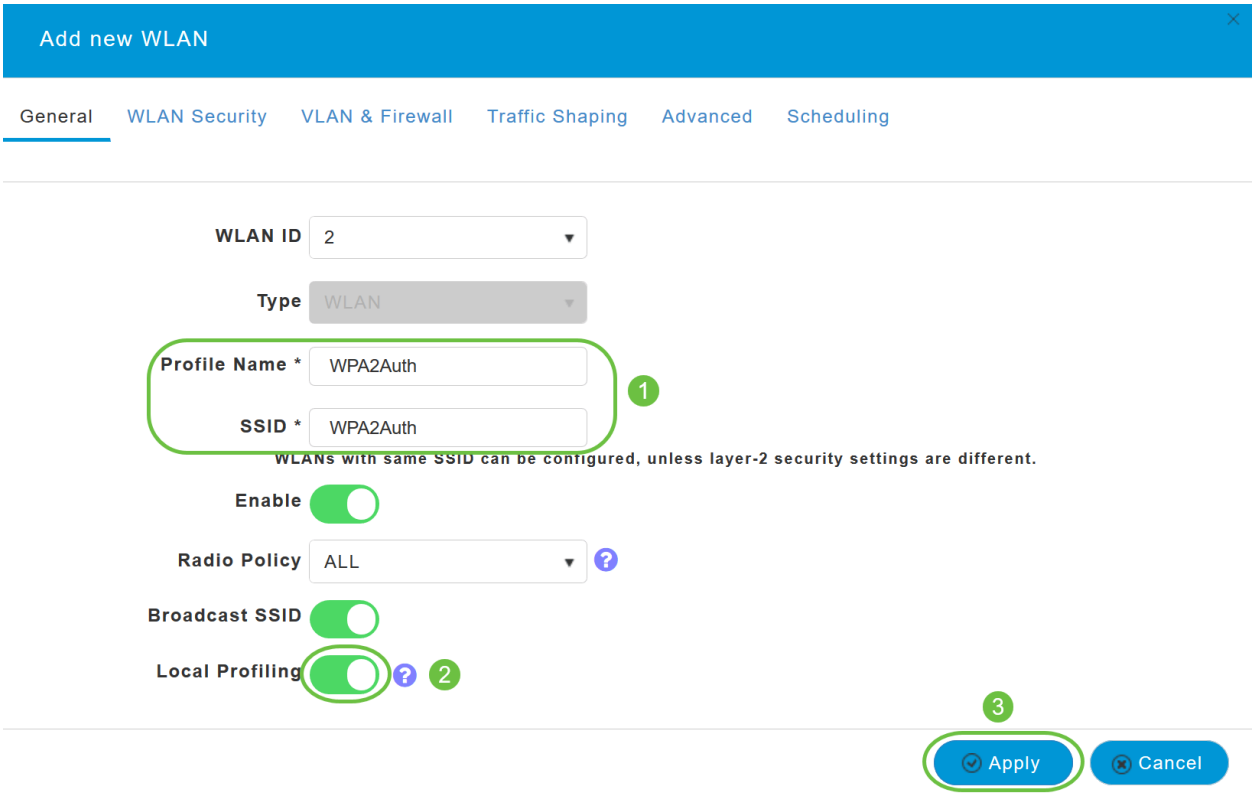
Passo 2

Clique em **Adicionar nova WLAN/RLAN**.



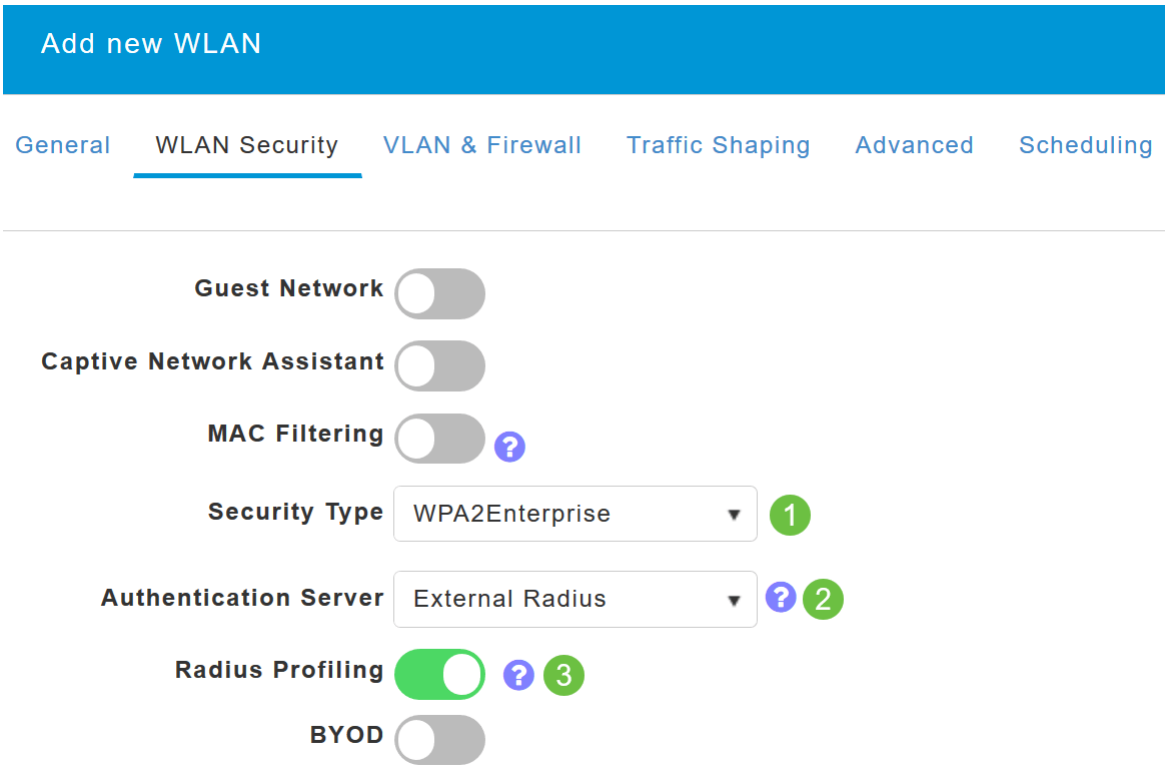
Etapa 3

Na guia *Geral*, digite o *Nome do perfil*. O campo *SSID* será preenchido automaticamente. Você pode optar por ativar o *perfil local*. Clique em Apply.



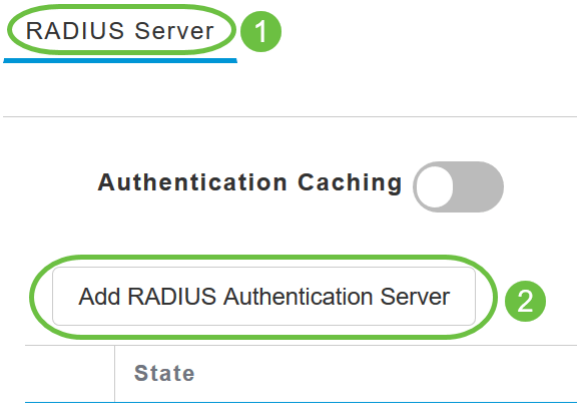
Passo 4

Navegue até a guia *WLAN Security*. No menu suspenso *Security Type*, escolha **WPA2Enterprise**. Selecione **External Radius** como o *Authentication Server*. Você pode optar por habilitar a *criação de perfis de raios*.



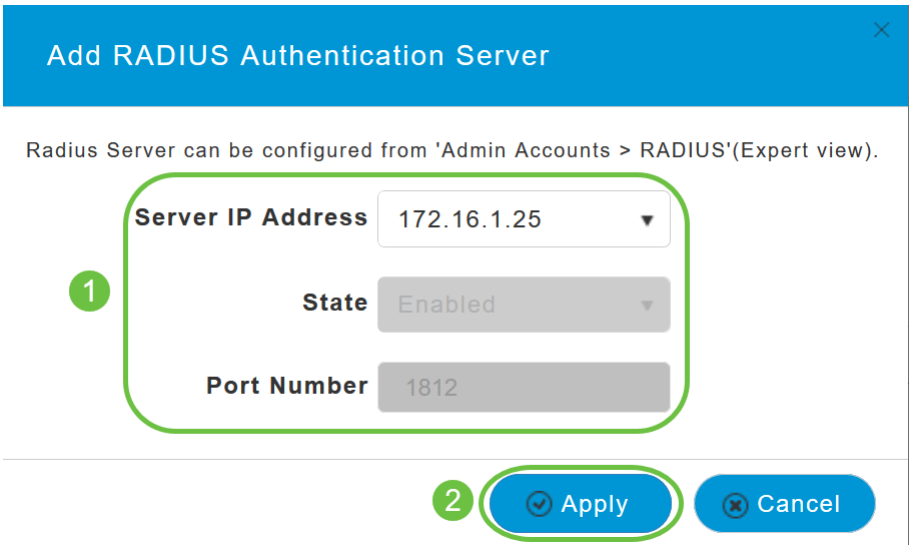
Etapa 5

Navegue até a seção *Servidor RADIUS*. Clique em **Adicionar servidor de autenticação RADIUS**.



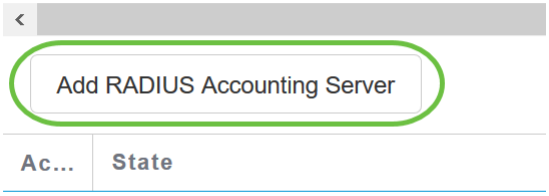
Etapa 6

Verifique os detalhes do RADIUS Authentication Server que você configurou e clique em **Apply**.



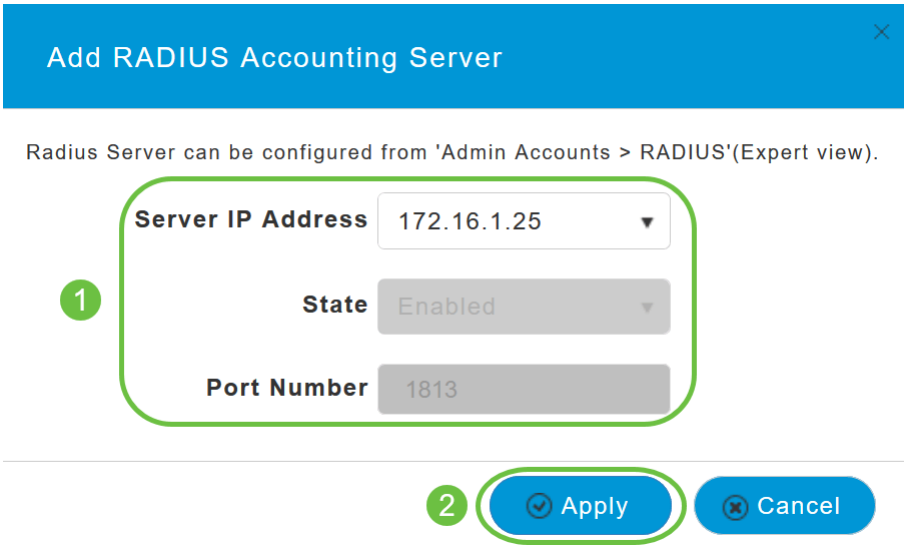
Etapa 7

Clique em **Add RADIUS Accounting Server**.



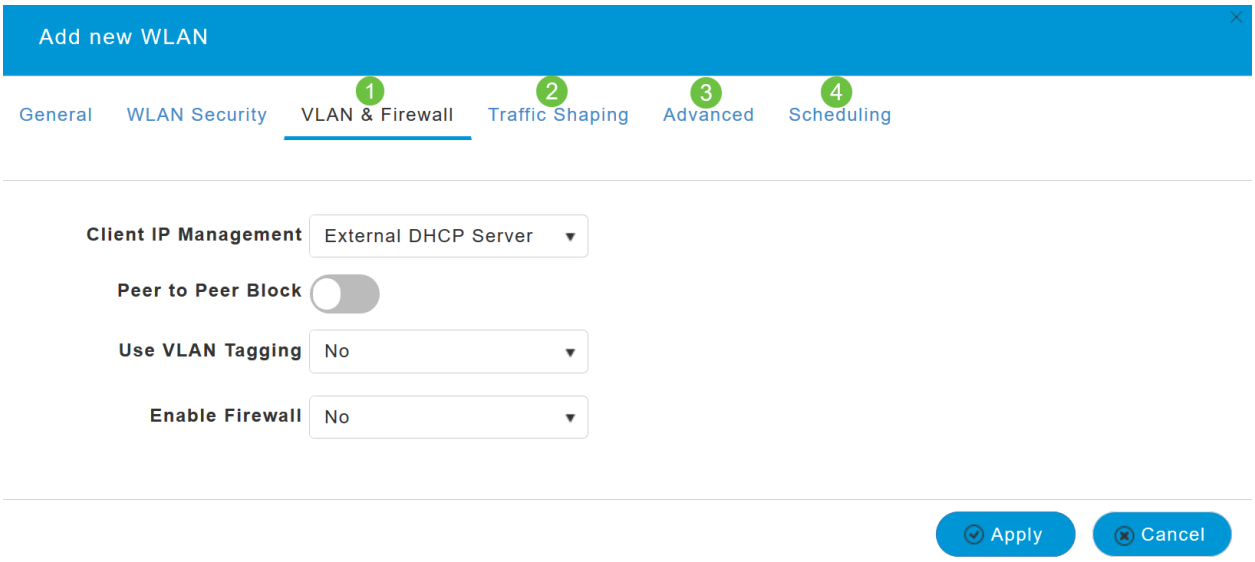
Passo 8

Verifique os detalhes do RADIUS Accounting Server que você configurou e clique em **Apply**.



Passo 9

Navegue até *VLAN & Firewall*, *Traffic Shaping*, *Advanced* e *Scheduling* guias para definir as configurações com base nas preferências de rede. Clique em Apply.

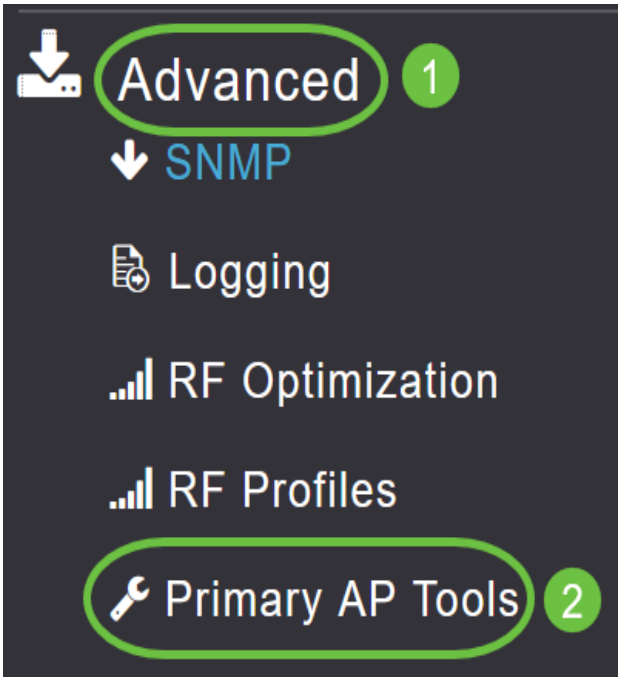


Verificação

Para testar a autenticação RADIUS, faça o seguinte:

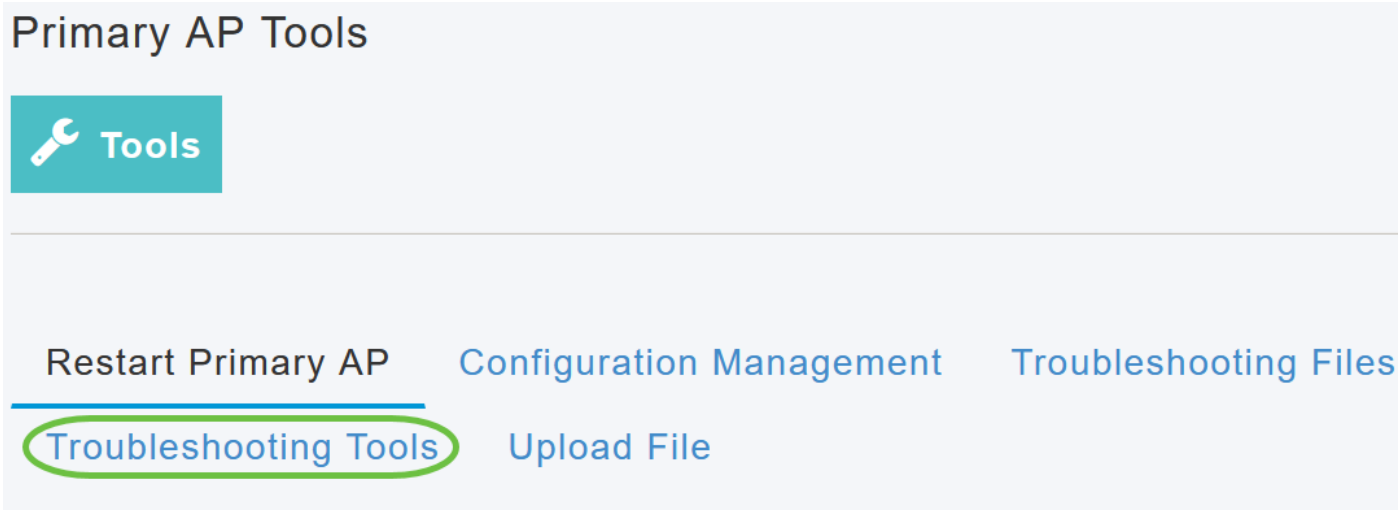
Passo 1

Navegue até **Avançado > Ferramentas AP primárias**.



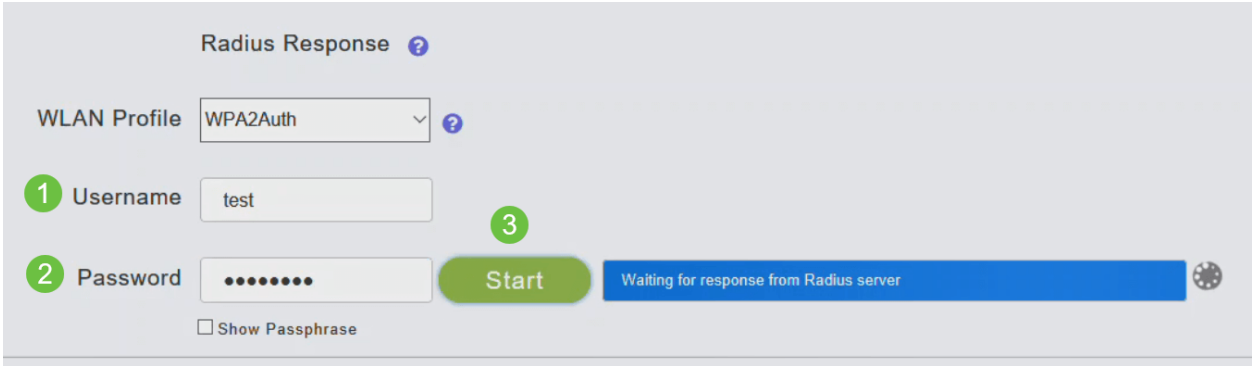
Passo 2

Clique em **Ferramentas de solução de problemas**.



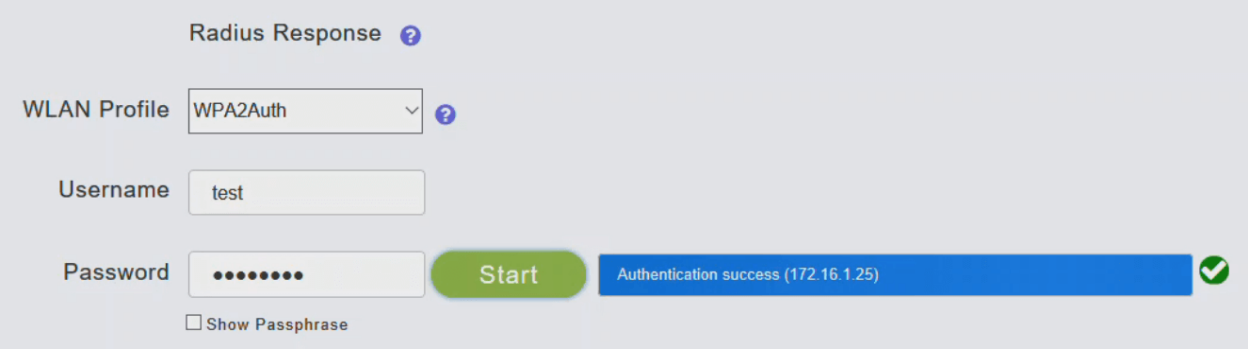
Etapa 3

Na seção *Resposta ao RADIUS*, digite o *Nome de usuário* e a *Senha* do perfil WLAN que você configurou anteriormente e clique em **Iniciar**.



Passo 4

Quando a verificação for concluída com êxito, você verá a seguinte notificação na tela.



Conclusão

Pronto. Agora você aprendeu as etapas para configurar o RADIUS no seu AP CBW. Para obter configurações mais avançadas, consulte o *Guia de administração do Cisco Business Wireless Access Point.*

Perguntas mais freqüentes 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