Recurso de chave pré-compartilhada pessoal no ponto de acesso CBW

Objetivo

Este artigo explicará o recurso de chave pré-compartilhada (PSK) pessoal no firmware do ponto de acesso (AP) Cisco Business Wireless (CBW) versão 10.6.1.0.

Dispositivos aplicáveis | Versão do software

- Access point Cisco Business Wireless 140AC | 10.6.1.0 (Baixe o mais recente)
- Access point Cisco Business Wireless 145AC | 10.6.1.0 (Baixe o mais recente)
- Access point Cisco Business Wireless 240AC | 10.6.1.0 (Baixe o mais recente)

Introduction

Se você tiver equipamento CBW na rede, poderá usar o recurso PSK pessoal no firmware versão 10.6.1.0!

A PSK pessoal, também conhecida como PSK individual (iPSK), é uma característica que permite ao administrador emitir chaves pré-partilhadas exclusivas para dispositivos individuais para a mesma WPA2 (Wi-Fi Protected Access II). A PSK exclusiva está vinculada ao endereço MAC do dispositivo. Isso não é suportado em WLANs onde a política WPA3 está habilitada.

Este recurso autentica o cliente usando um servidor RADIUS. Geralmente, ele é destinado ao uso por dispositivos da IoT e por laptops e dispositivos móveis fornecidos pela empresa.

Table Of Contents

Prerequisites

- Verifique se você atualizou o firmware do AP CBW para 10.6.1.0. Clique em se quiser obter instruções passo a passo sobre como atualizar o firmware.
- Você precisará de um servidor RADIUS no qual a PSK pessoal e o endereço MAC do dispositivo precisem ser configurados.
- Este recurso CBW é suportado com três servidores RADIUS diferentes - FreeRADIUS, NPS da Microsoft e ISE da Cisco. A configuração varia dependendo do servidor

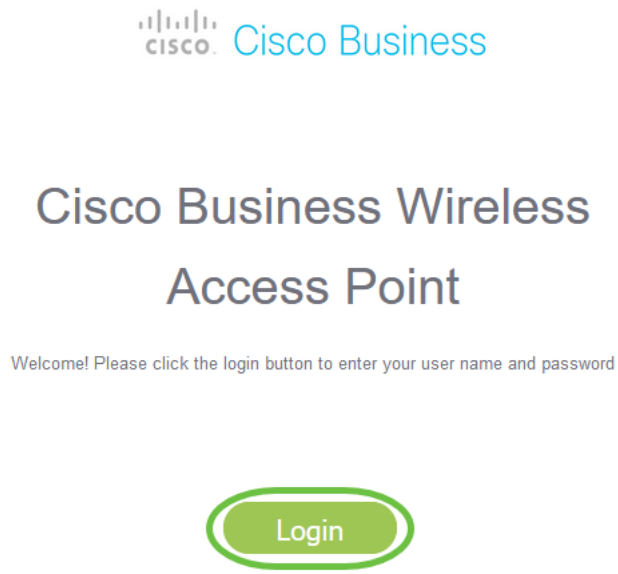
RADIUS usado.

Definir configurações de RADIUS CBW

Para definir as configurações de RADIUS no AP CBW, siga as etapas.

Passo 1

Faça login na interface de usuário da Web (UI) do AP CBW.

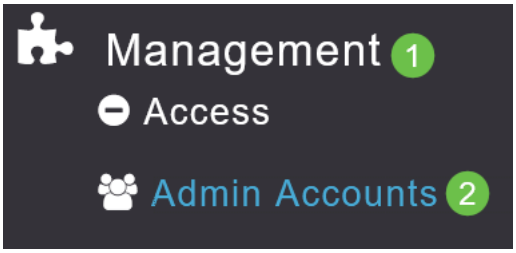


Passo 2

Clique no símbolo de **seta bidirecional** para alternar para a visualização do especialista.

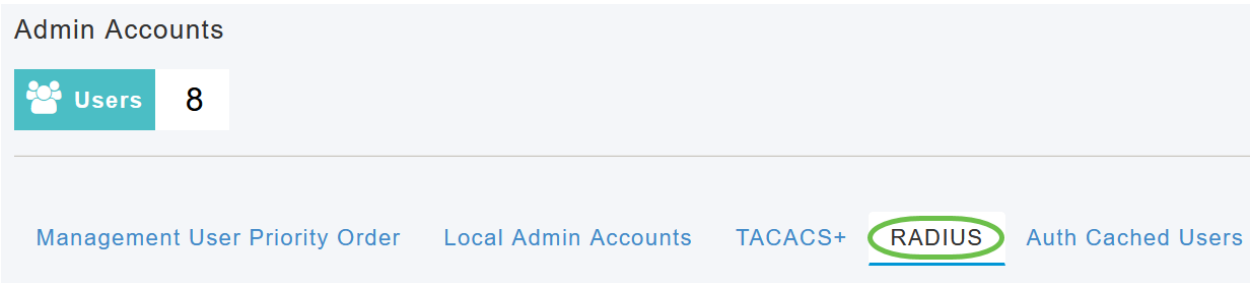
Etapa 3

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



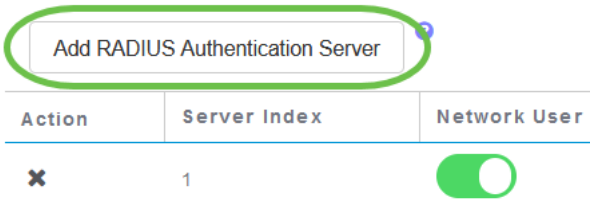
Passo 4

Selecione a guia **RADIUS**.



Etapa 5

Clique em **Adicionar servidor de autenticação RADIUS**.

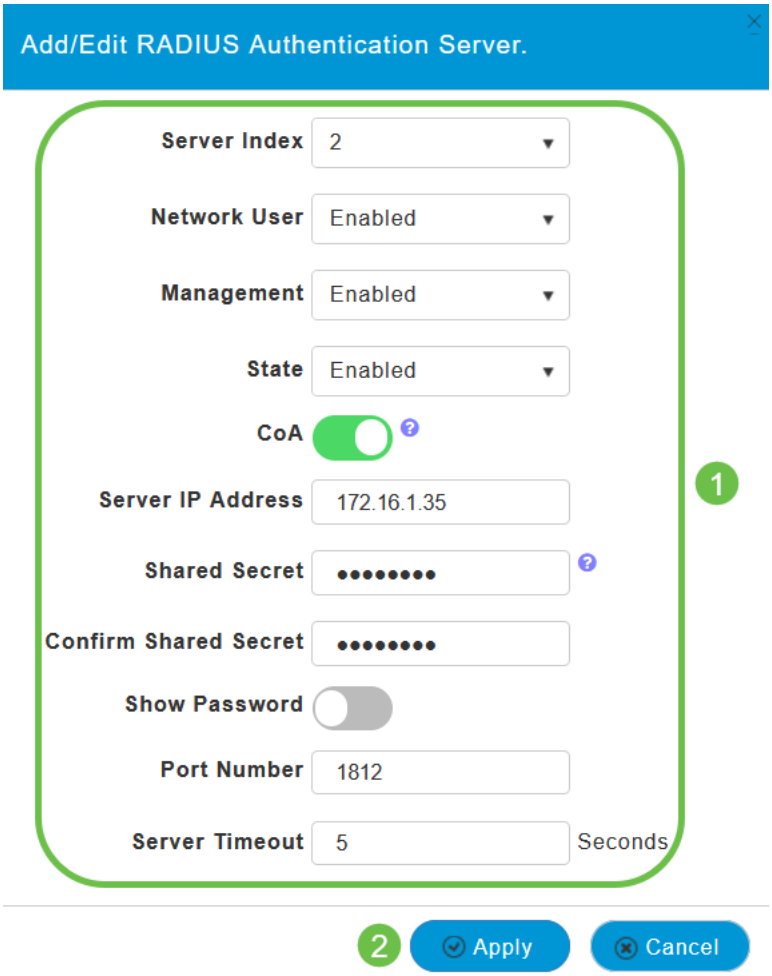


Etapa 6

Configure o seguinte:

- *Índice do servidor* - Selecione de 1 a 6
- *Network User* - Ative o estado. Por padrão, Habilitado
- *Management* - Enable the state (Gerenciamento - Habilitar o estado). Por padrão, Habilitado
- *State* - Enable the state (Estado). Por padrão, Habilitado
- *CoA* - Certifique-se de que a cobrança de autoridade (CoA) esteja habilitada.
- *Server IP Address (Endereço IP do servidor)* - Insira o endereço IPv4 do servidor RADIUS
- *Shared Secret* - (Segredo compartilhado) Insira a chave secreta compartilhada
- *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.



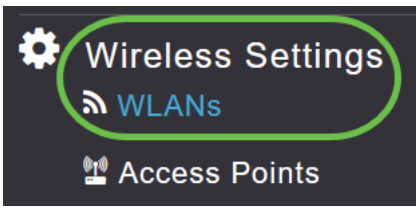
Configurar as definições da WLAN

Crie uma WLAN como uma WLAN padrão segura para WPA2 pessoal.

A chave pré-compartilhada não será usada para os dispositivos PSK pessoais. Isso só seria usado para dispositivos que NÃO são autenticados no servidor RADIUS. Você precisaria adicionar os endereços MAC de QUALQUER dispositivo que se conectará a esta WLAN à lista de permissões deste dispositivo.

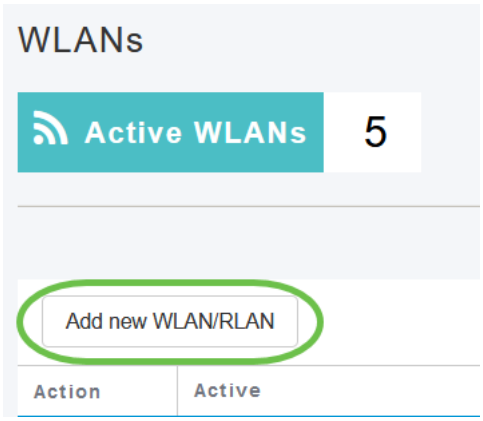
Passo 1

Navegue até **Wireless Settings > WLANs**.



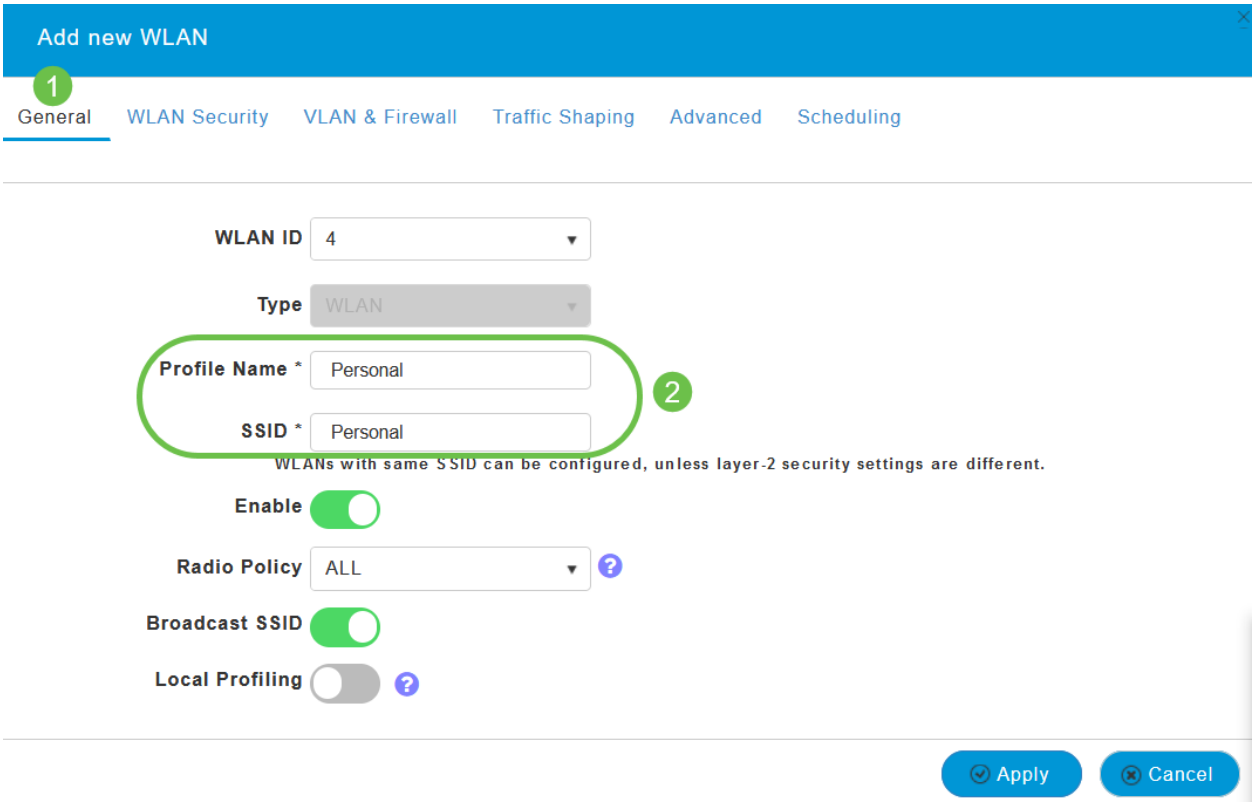
Passo 2

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



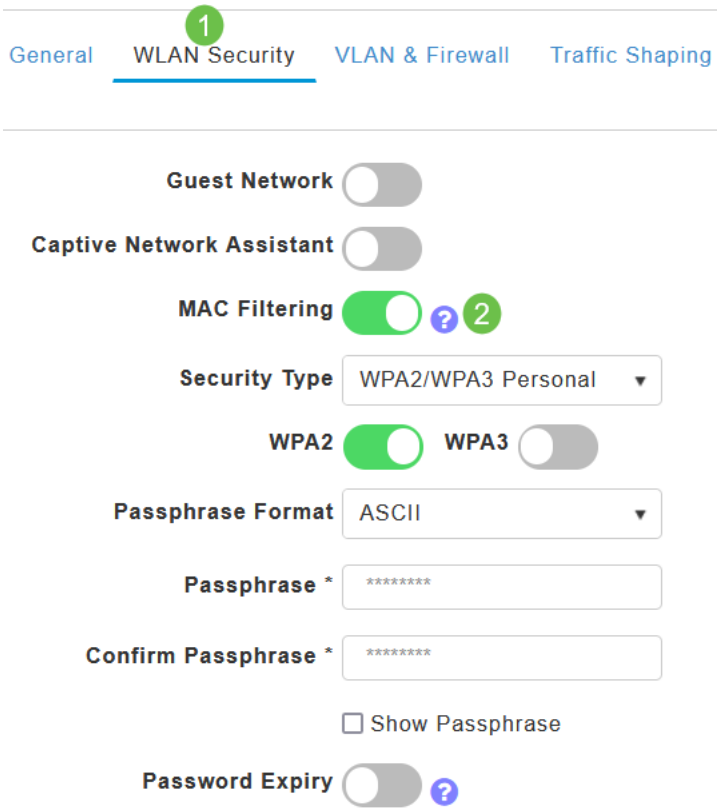
Etapa 3

Na guia *Geral*, insira um *Nome de perfil* para a WLAN.



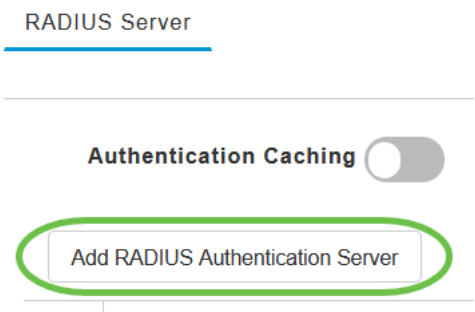
Passo 4

Navegue até a guia **WLAN Security** e ative a **Filtragem MAC** deslizando a alternância.



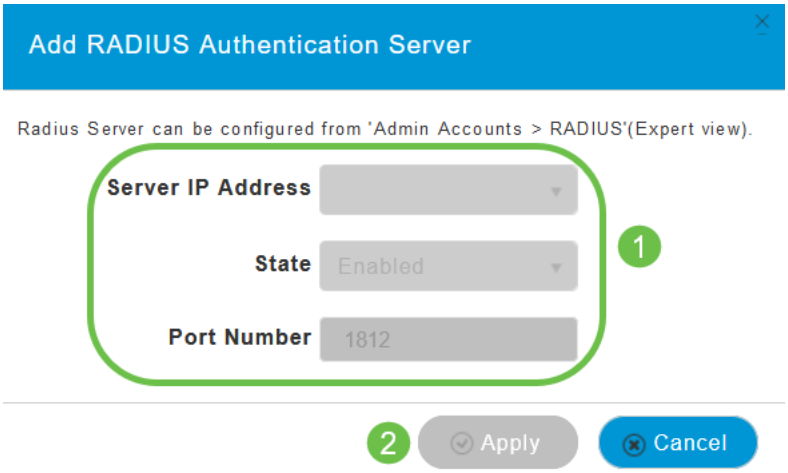
Etapa 5

Clique em **Add RADIUS Authentication Server** para adicionar o servidor RADIUS configurado na seção anterior para fornecer autenticação para esta WLAN.



Etapa 6

Uma janela pop-up será exibida. Insira o *Server IP Address (Endereço IP do servidor), State (Estado) e Port Number (Número da porta)*. Clique em Apply.

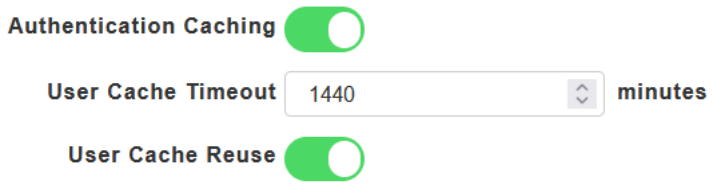


Etapa 7

(Opcional)

Habilitar *Cache de Autenticação*. Quando você habilita essa opção, os campos a seguir são exibidos.

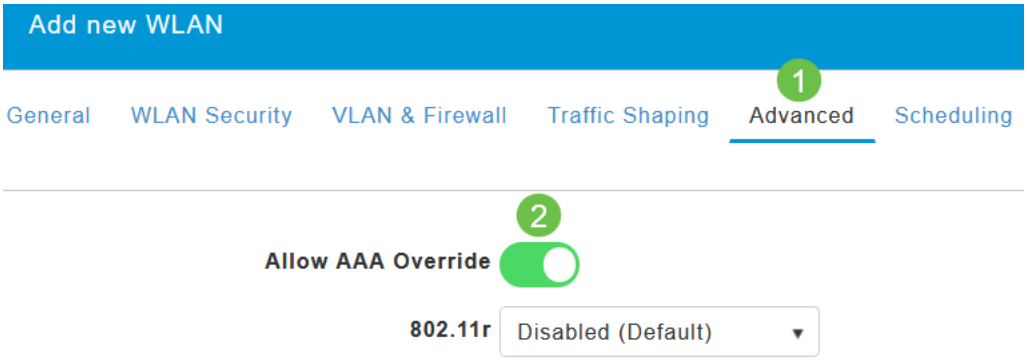
- *User Cache Timeout* - Especifica o período em que a credencial autenticada no cache expira.
- *User Cache Reuse* - Use as informações de cache de credenciais antes do tempo limite do cache. Por padrão, esta
está desabilitado.



Se este recurso estiver ativado, um cliente que já foi autenticado neste servidor não precisará passar dados para o servidor RADIUS quando se reconectar a esta WLAN nas próximas 24 horas.

Passo 8

Navegue até a guia Avançado. Habilite **Permitir substituição de AAA** deslizando a alternância.

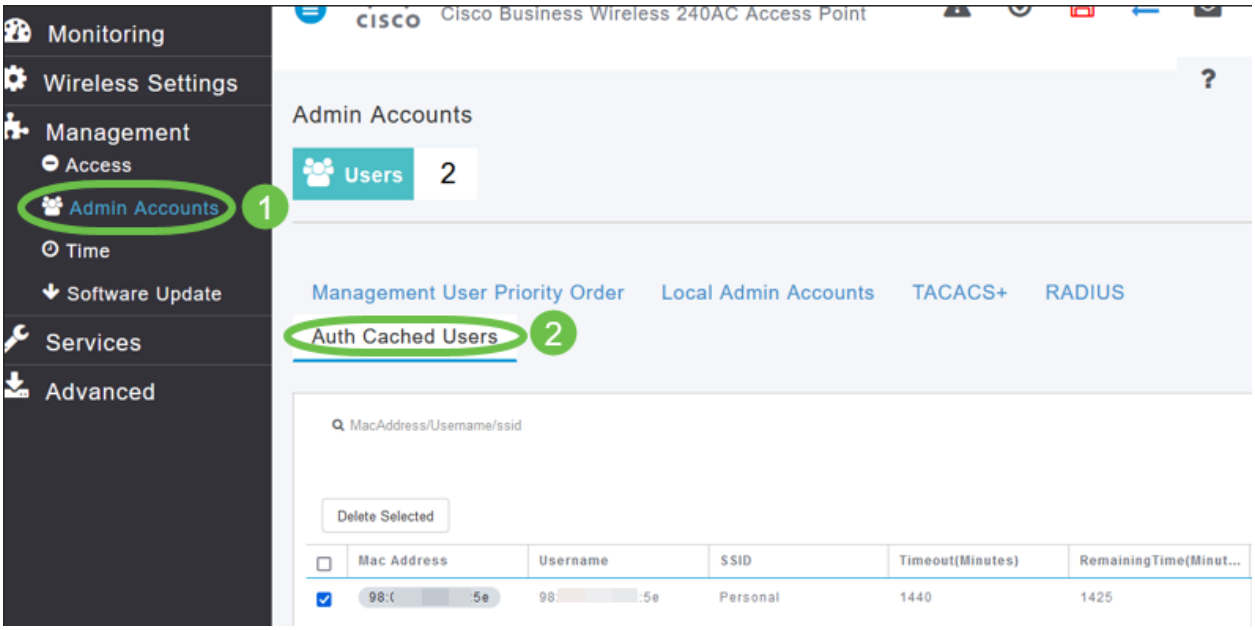


A guia *Avançado* ficará visível somente se você estiver no *Expert View*.

Próximas etapas

Depois de definir as configurações no AP CBW e configurar o servidor RADIUS, você poderá conectar o dispositivo. Insira a PSK personalizada configurada para esse endereço MAC e ela ingressará na rede.

Se tiver configurado o cache de autenticação, você poderá ver os dispositivos que ingressaram na WLAN acessando a guia *Auth Cached Users* em *Admin Accounts*. Se necessário, isso pode ser excluído.



Conclusão

Aqui está! Agora você pode aproveitar os benefícios do recurso PSK pessoal em seu AP CBW.