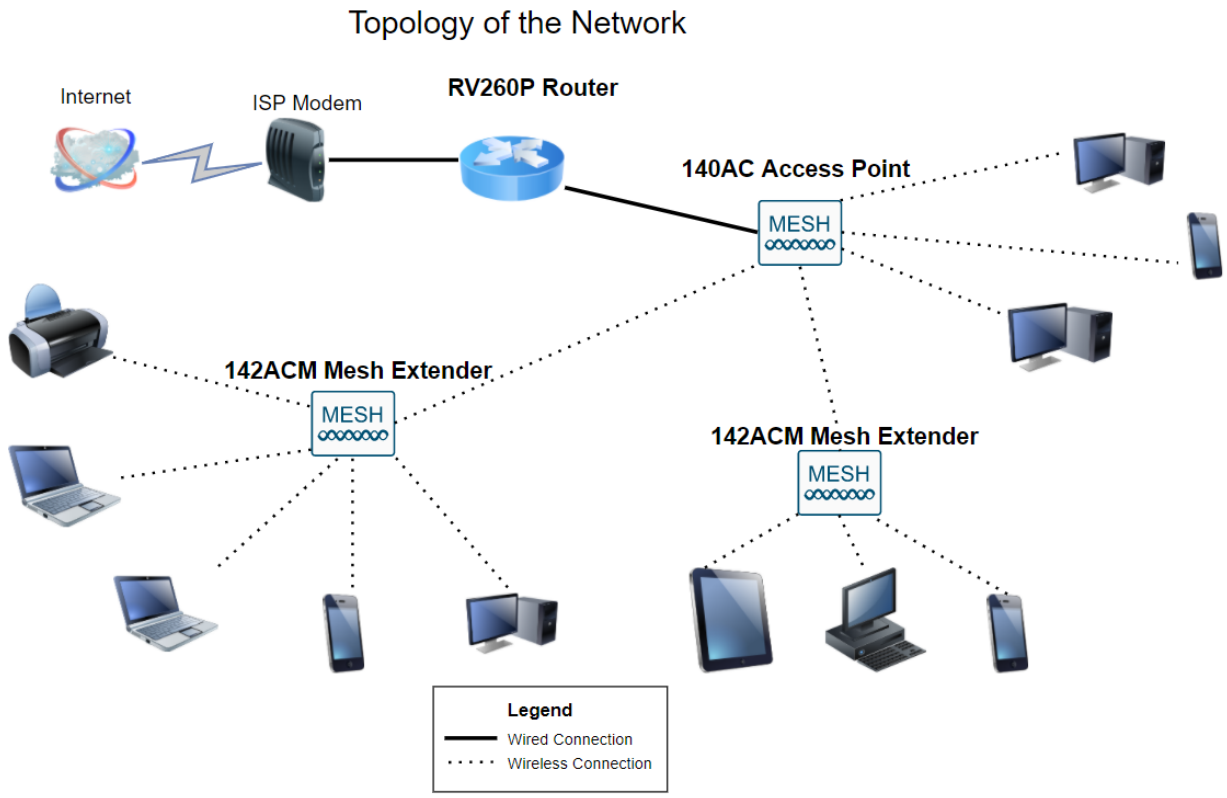
Configuração total da rede: RV260P com Cisco Business Wireless e a IU da Web

Objetivo:

Este guia mostra como configurar uma rede de malha sem fio usando um roteador RV260P, um ponto de acesso CBW140AC e dois extensores de malha CBW142ACM.

Este artigo usa a interface de usuário da Web (UI) para configurar a rede sem fio em malha. Se preferir usar o aplicativo móvel, recomendado para fácil configuração sem fio, clique para ir para o artigo que usa o aplicativo móvel. Se quiser usar a interface de usuário da Web, continue lendo!

Topologia:



Introduction

Aqui está você, pronto para configurar sua nova rede. É um dia emocionante! Neste cenário, estamos usando um roteador RV260P. Este roteador fornece Power over Ethernet (PoE) que permite conectar o CBW140AC ao roteador em vez de um switch. Os extensores de malha CBW140AC e CBW142ACM serão usados para criar uma rede de malha sem fio.

Se você não está familiarizado com alguns dos termos usados neste documento ou deseja obter mais detalhes sobre a rede em malha, consulte os seguintes artigos:

- Negócios da Cisco: Glossário de novos termos
- Bem-vindo à rede em malha sem fio empresarial da Cisco
- Perguntas frequentes (FAQ) para uma rede sem fio empresarial da Cisco

Você está pronto? Vamos lá!

Dispositivos aplicáveis | Versão do software

- RV260P |1.0.0.17
- CBW140AC |10.3.1.0
- CBW142ACM | 10.3.1.0 (é necessário pelo menos um extensor de malha para a rede de malha)

Table Of Contents

Antes de começar

1. Verifique se você tem uma conexão atual com a Internet para configuração.
2. Entre em contato com o ISP para saber as instruções especiais que ele tem ao usar o roteador RV260. Alguns ISPs oferecem gateways com roteadores integrados. Se você tiver um gateway com um roteador integrado, talvez seja necessário desativar o roteador e passar o endereço IP da rede de longa distância (WAN) (o endereço de protocolo de Internet exclusivo que o provedor de Internet atribui à sua conta) e todo o tráfego de rede até o novo roteador.
3. Decida onde colocar o roteador. Se possível, você vai querer uma área aberta. Isso

pode não ser fácil, pois você deve conectar o roteador ao gateway de banda larga (modem) do seu ISP (Provedor de serviços de Internet).

Configurar o roteador RV260P

Um roteador é essencial em uma rede porque roteia pacotes. Permite que um computador se comunique com outros computadores que não estão na mesma rede ou sub-rede. Um roteador acessa uma tabela de roteamento para determinar para onde os pacotes devem ser enviados. A tabela de roteamento lista os endereços de destino. As configurações estáticas e dinâmicas podem ser listadas na tabela de roteamento para levar os pacotes ao seu destino específico.

O RV260P vem com configurações padrão otimizadas para muitas pequenas empresas. No entanto, as suas exigências de rede ou o ISP (Provedor de serviços de Internet) podem exigir que você modifique algumas dessas configurações. Depois de entrar em contato com o ISP para saber quais são os requisitos, você pode fazer alterações usando a interface do usuário da Web (UI).

RV260P pronto para uso

Passo 1

Conecte o cabo Ethernet de uma das portas RV260P LAN (Ethernet) à porta Ethernet no computador. Você precisará de um adaptador se o computador não tiver uma porta Ethernet. O terminal deve estar na mesma sub-rede com fio que o RV260P para executar a configuração inicial.

Passo 2

Não se esqueça de usar o adaptador de alimentação fornecido com o RV260P. O uso de um adaptador de energia diferente pode danificar o RV260P ou fazer com que os dongles USB falhem. Por padrão, a chave liga/desliga está ligada.

Conecte o adaptador de alimentação à porta 12VDC do RV260P, mas ainda não o conecte à alimentação.

Etapa 3

Verifique se o modem está desligado.

Passo 4

Use um cabo Ethernet para conectar o modem a cabo ou DSL à porta WAN no RV260P.

Etapa 5

Conecte a outra extremidade do adaptador RV260P a uma tomada elétrica. Isso ligará o RV260. Reconecte o modem para que ele possa ser ligado também. A luz de alimentação no painel frontal fica verde estável quando o adaptador de energia está conectado corretamente e o RV260P está concluído na inicialização.

Configurar o roteador

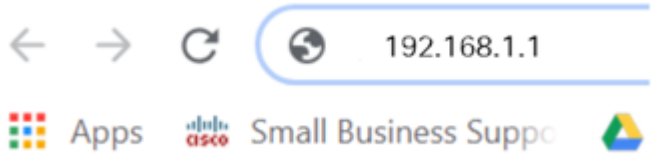
O trabalho preparatório está pronto, agora é hora de fazer algumas configurações! Para iniciar a IU da Web, siga estes passos:

Passo 1

Se seu computador estiver configurado para se tornar um cliente DHCP (Dynamic Host Configuration Protocol), um endereço IP no intervalo 192.168.1.x será atribuído ao PC. O DHCP automatiza o processo de atribuição de endereços IP, máscaras de sub-rede, gateways padrão e outras configurações para computadores. Os computadores devem ser configurados para participar do processo DHCP para obter um endereço. Isso é feito selecionando-se para obter um endereço IP automaticamente nas propriedades do TCP/IP no computador.

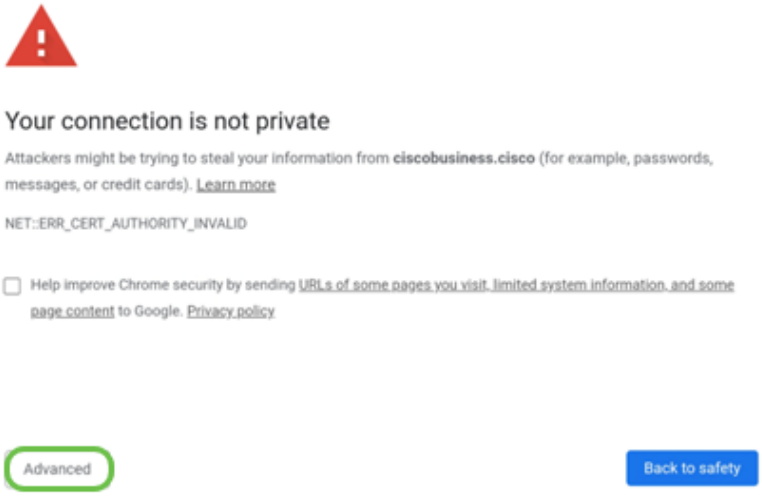
Passo 2

Abra um navegador da Web, como Safari, Internet Explorer ou Firefox. Na barra de endereços, insira o endereço IP padrão do RV260P, que é 192.168.1.1.



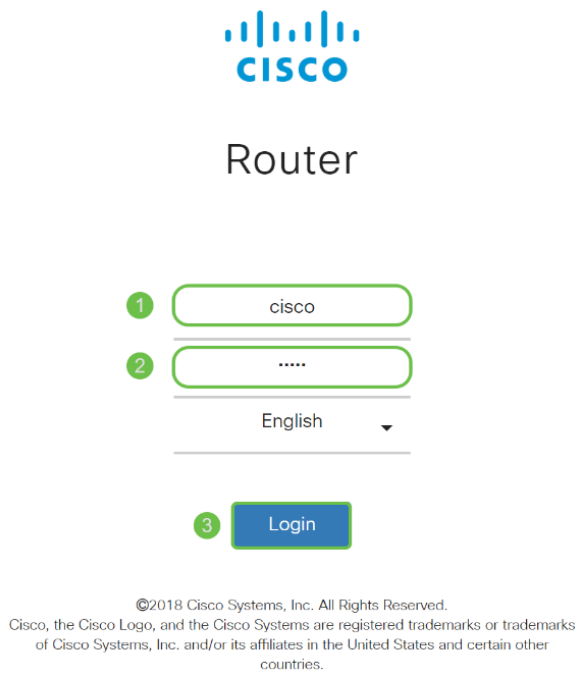
Etapa 3

O navegador pode emitir um aviso de que o site não é confiável. Continue no site. Se você não estiver conectado, vá para Solução de problemas da conexão com a Internet .



Passo 4

Quando a página de entrada for exibida, digite o nome de usuário padrão cisco e a senha padrão *cisco*. O nome de usuário e a senha diferenciam maiúsculas e minúsculas.



Etapa 5

Clique em login. A página *Guia de introdução* é exibida. Agora que você confirmou a conexão e fez login no roteador, vá para a seção Configuração inicial deste artigo.

Solução de problemas da conexão com a Internet

Se você estiver lendo isso, provavelmente está tendo problemas para se conectar à Internet ou à IU da Web. Uma dessas soluções deve ajudar.

No SO Windows conectado, você pode testar a conexão de rede abrindo o prompt de comando. Insira ping 192.168.1.1 (o endereço IP padrão do roteador). Se a solicitação expirar, você não poderá se comunicar com o roteador.

Se a conectividade não estiver acontecendo, você pode verificar a solução de problemas nos roteadores RV160 e RV260.

Algumas outras coisas para tentar:

1. Verifique se o navegador da Web não está definido como Trabalhar off-line.
2. Verifique as configurações de conexão de rede local do adaptador Ethernet. O PC deve obter um endereço IP por meio do DHCP. Como alternativa, o PC pode ter um endereço IP estático no intervalo 192.168.1.x com o gateway padrão definido como 192.168.1.1 (o endereço IP padrão do RV260P). Para se conectar, talvez seja necessário modificar as configurações de rede do RV260P. Se estiver usando o Windows 10, verifique as instruções do Windows 10 para modificar as configurações

de rede.

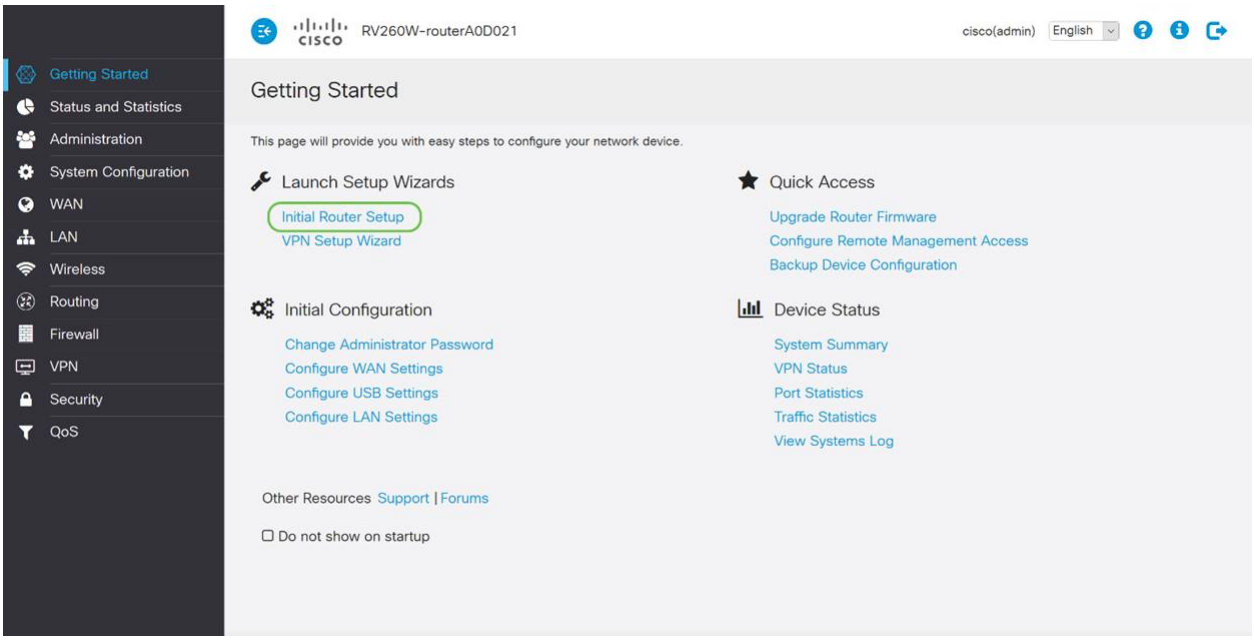
3. Se você tiver um equipamento existente ocupando o endereço IP 192.168.1.1, será necessário resolver esse conflito para que a rede funcione. Mais sobre isso no final desta seção, ou clique aqui para ser levado diretamente.
4. Redefina o modem e o RV260P desligando ambos os dispositivos. Em seguida, ligue o modem e deixe-o ocioso por cerca de 2 minutos. Em seguida, ligue o RV260P. Agora você deve receber um endereço IP WAN.
5. Se você tiver um modem DSL, peça ao ISP para colocar o modem DSL no modo bridge.

Configuração inicial

Recomendamos que você passe pelas etapas do Assistente de configuração inicial listadas nesta seção. Você pode alterar essas configurações a qualquer momento.

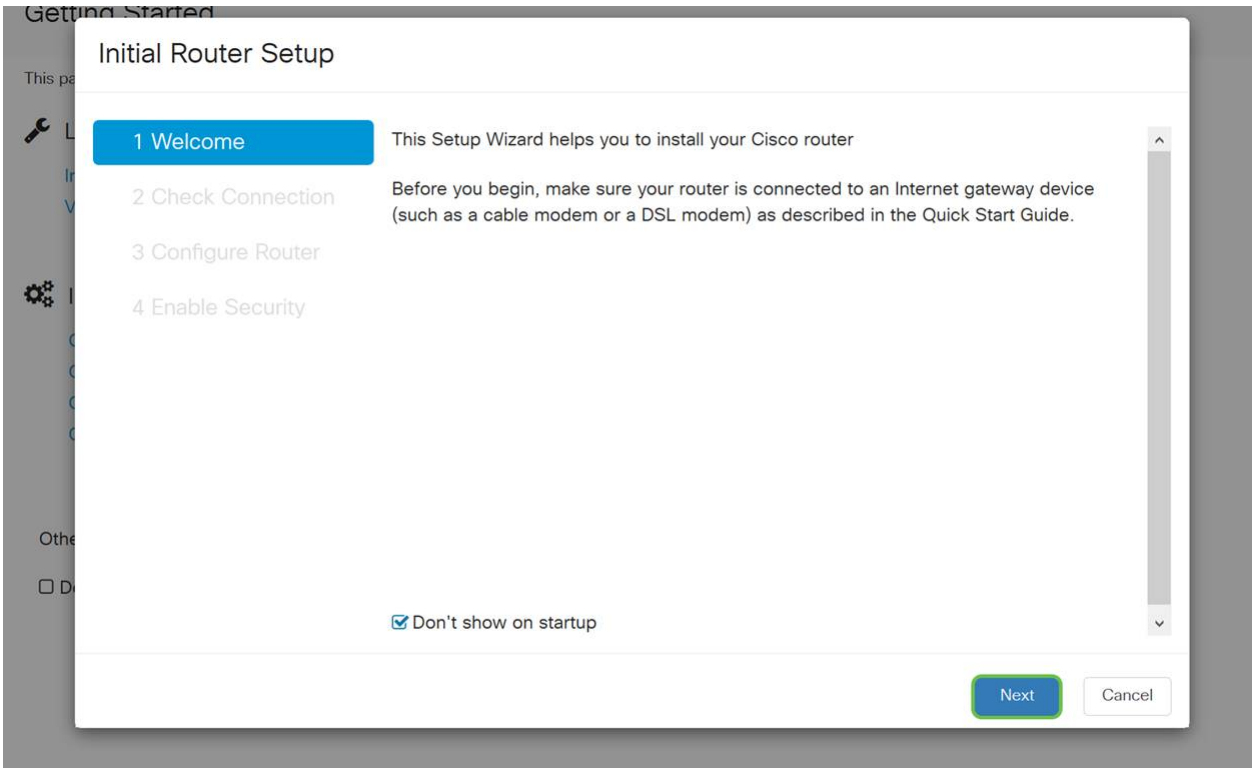
Passo 1

Clique em **Assistente de configuração inicial** na página *Introdução*.



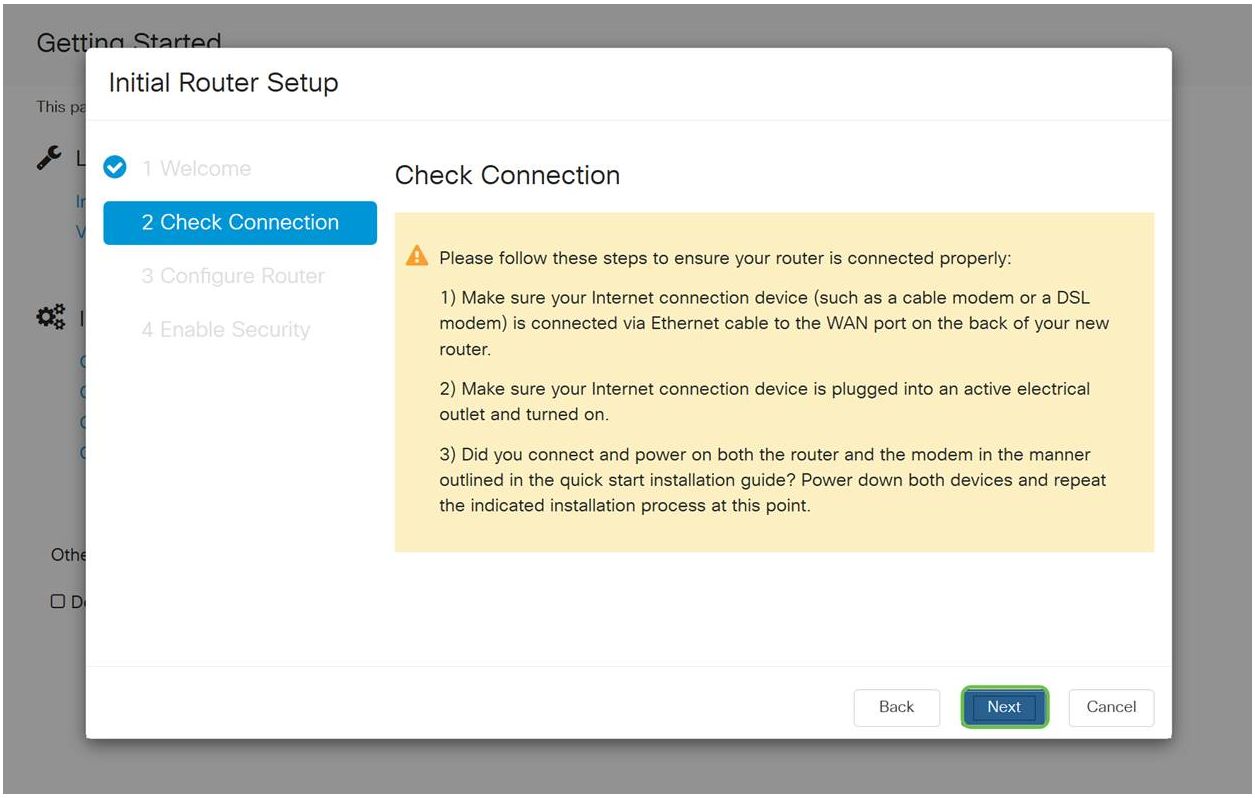
Passo 2

Esta etapa confirma se os cabos estão conectados. Como você já confirmou isso, clique em **Avançar**.



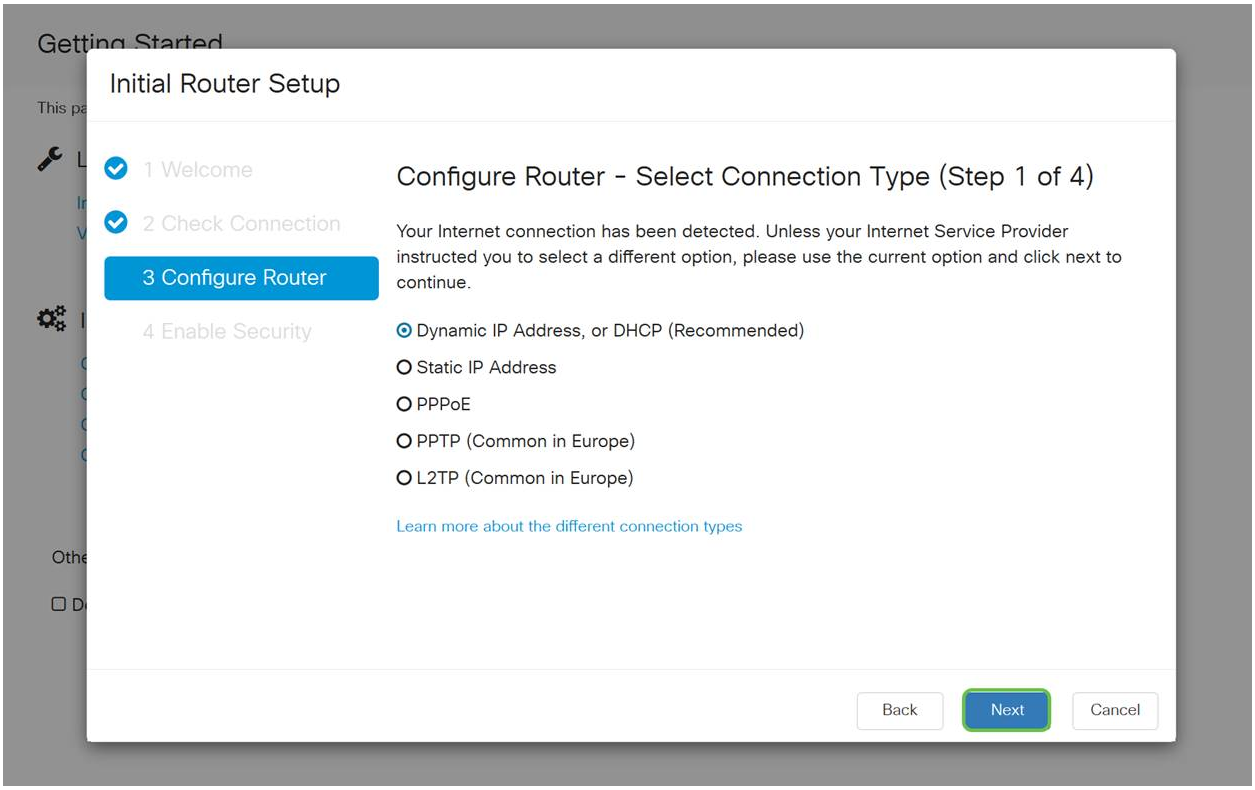
Etapa 3

Esta etapa aborda as etapas básicas para garantir que o roteador esteja conectado. Como você já confirmou isso, clique em **Avançar**.



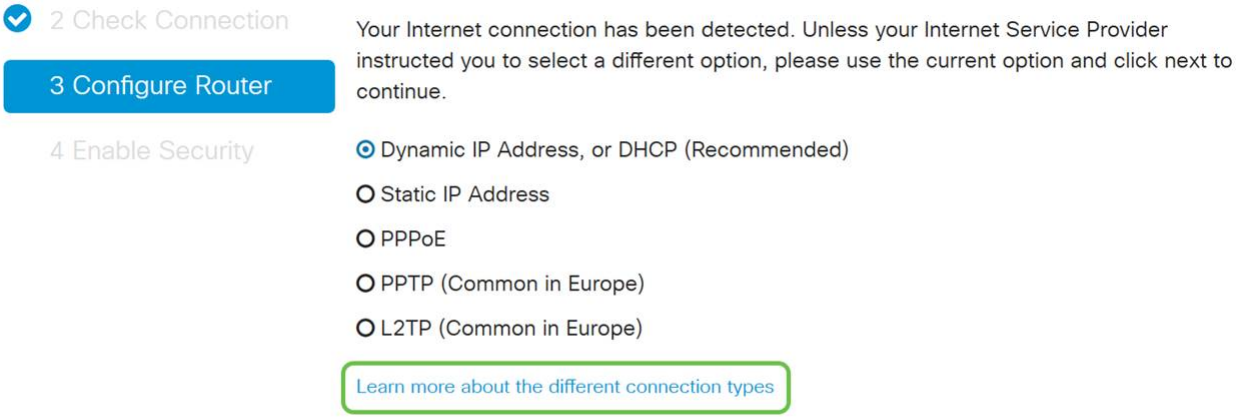
Passo 4

A próxima tela exibe suas opções para atribuir endereços IP ao roteador. Você precisa selecionar DHCP neste cenário. Clique em Next.



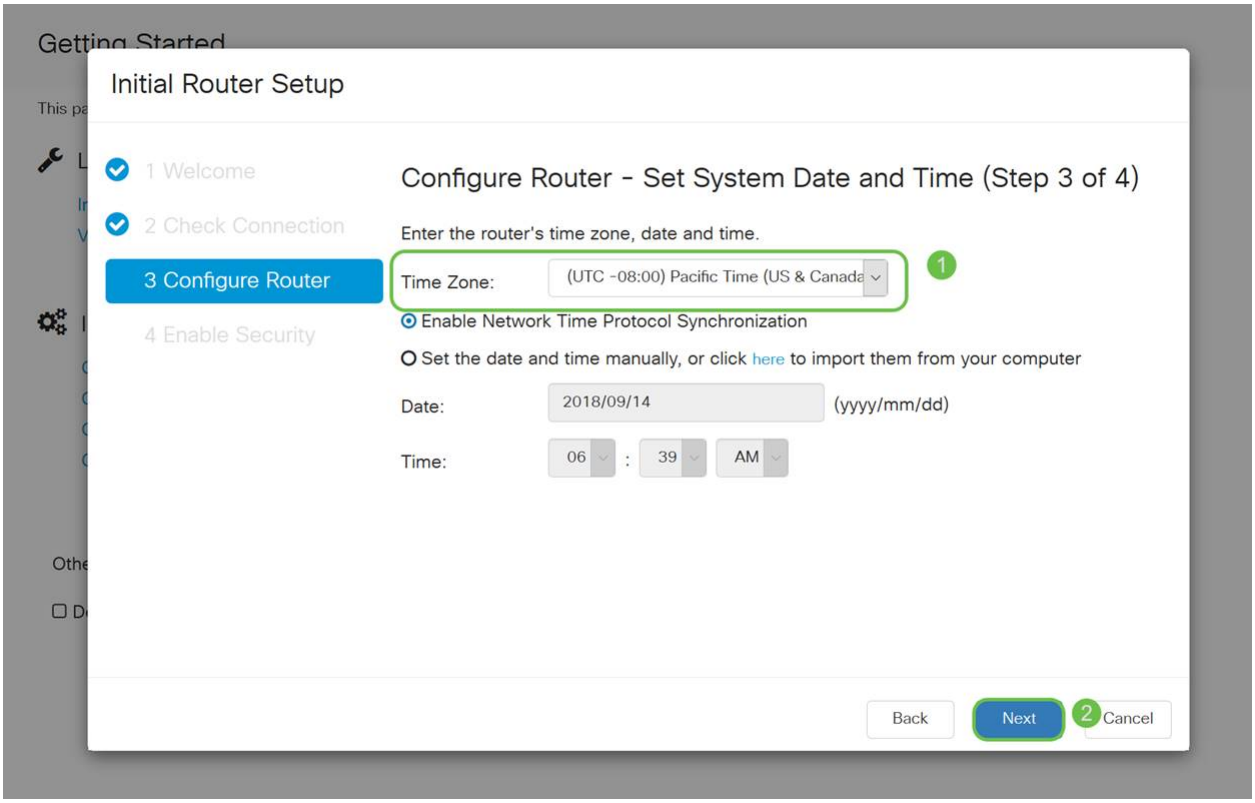
Embora você deva usar o DHCP para essa configuração inicial, você pode selecionar *Saiba mais sobre os diferentes tipos de conexão* na parte inferior da tela como referência futura. Para obter mais detalhes sobre isso, consulte os seguintes artigos:

- Configuração de WAN em dispositivos RV160x e RV260x
- Configurando o roteamento estático no RV160 e RV260



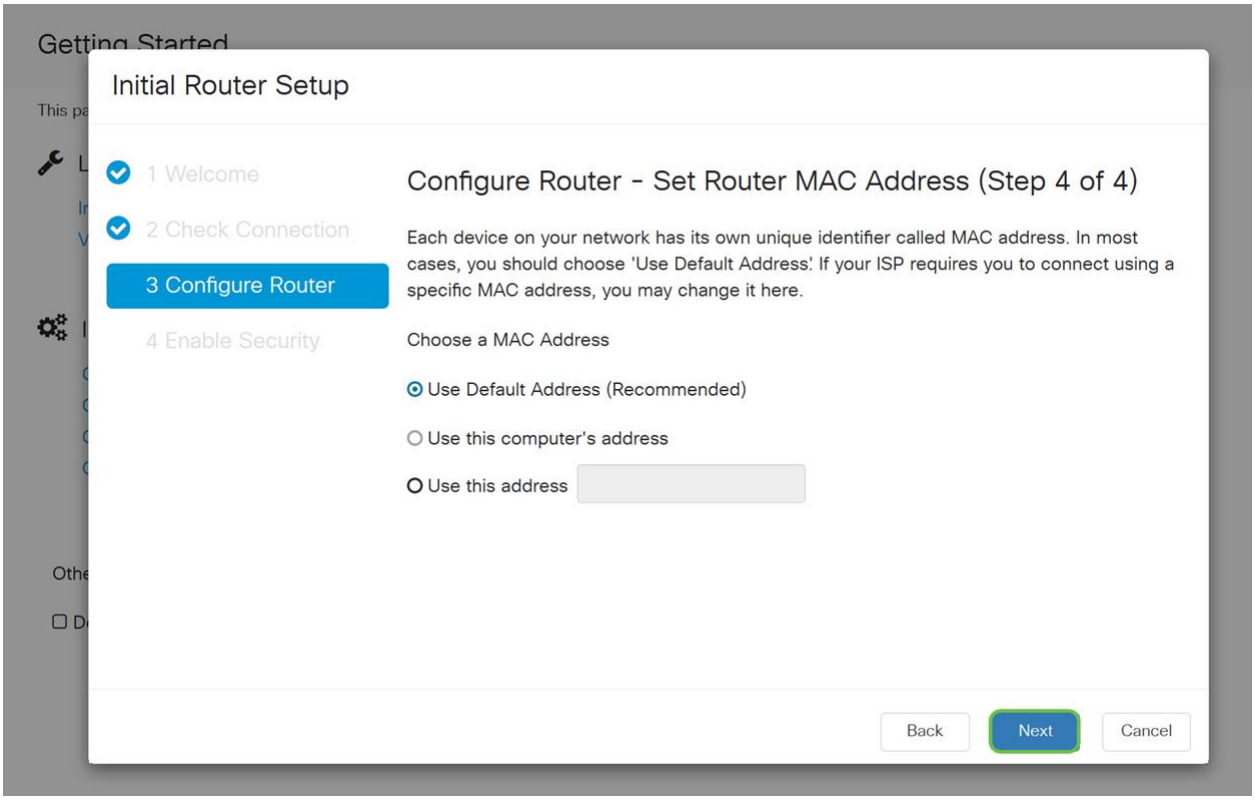
Etapa 5

Aqui, você será solicitado a definir as configurações de hora do roteador. Isso é importante porque permite precisão ao revisar logs ou eventos de solução de problemas. Selecione seu **fuso horário** e clique em **Avançar**.



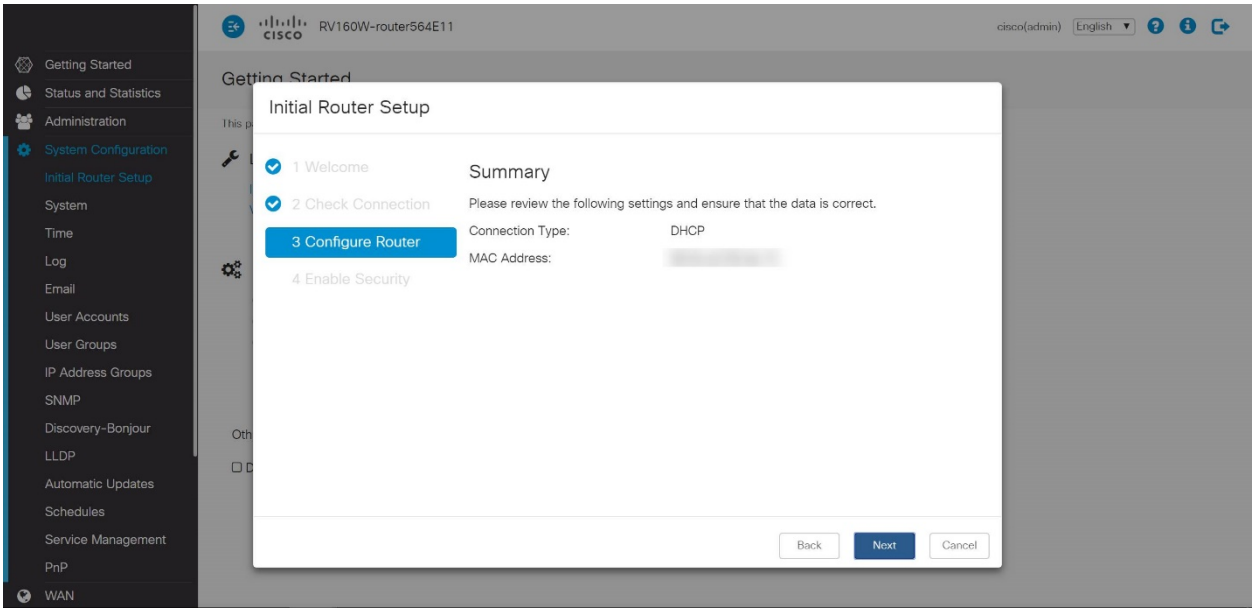
Etapa 6

Nessa tela, você selecionará os endereços MAC a serem atribuídos aos dispositivos. Com mais frequência, você usará o endereço padrão. Clique em Next.



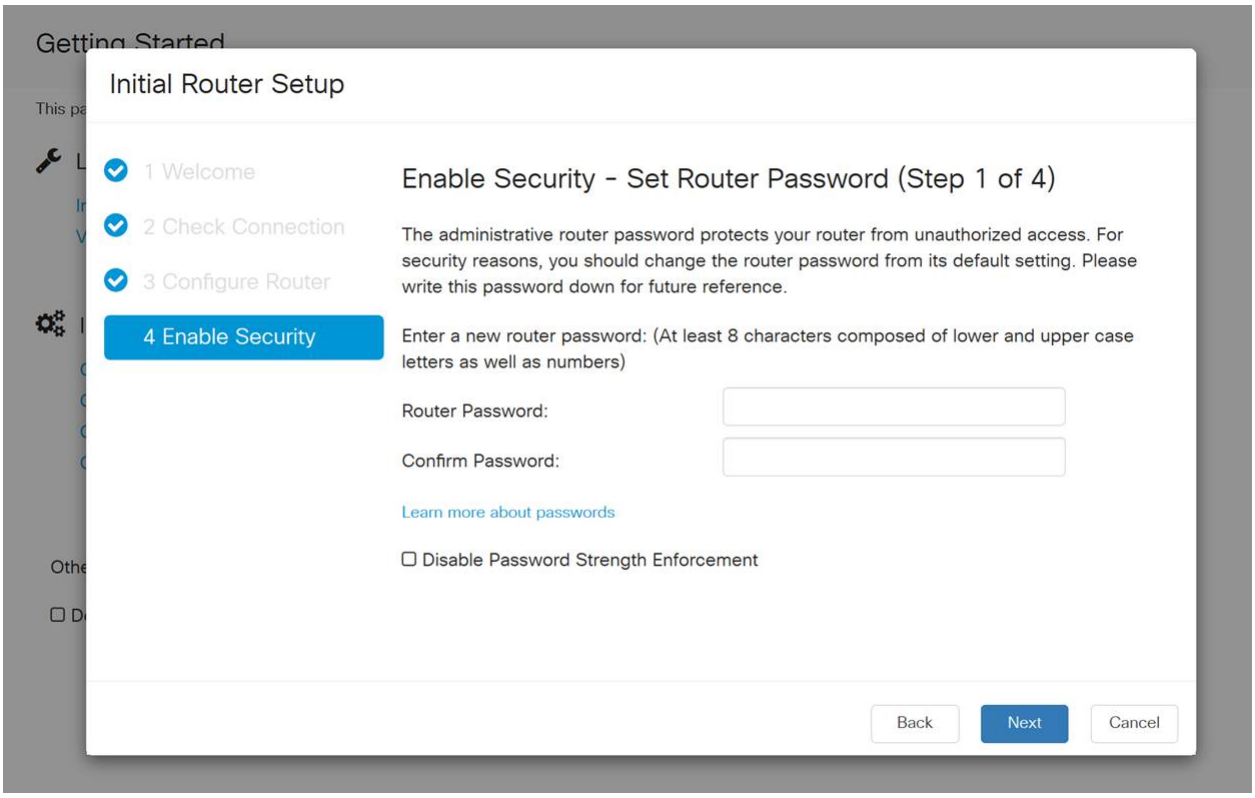
Etapa 7

A página a seguir é um resumo das opções selecionadas. Revise e clique em **Next (Avançar)** se satisfeito.



Passo 8

Na próxima etapa, você selecionará uma senha para usar ao fazer login no roteador. O padrão para senhas é conter pelo menos 8 caracteres (maiúsculas e minúsculas) e inclui números. **Digite uma senha** que esteja em conformidade com os requisitos de força. Clique em Next. Anote sua senha para logins futuros.



Não é recomendável selecionar Desativar *imposição de força da senha*. Essa opção permite que você selecione uma senha tão simples quanto 123, o que seria tão fácil quanto 1-2-3 para agentes mal-intencionados quebrarem.

Passo 9

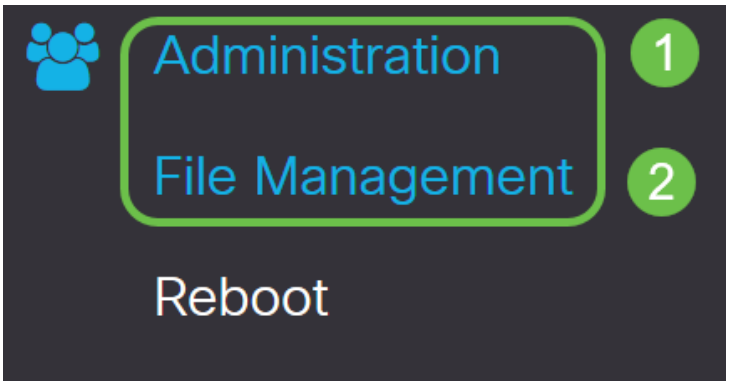
Clique no **ícone salvar**.

Atualize o firmware, se necessário

Esta é uma seção importante, não pule!

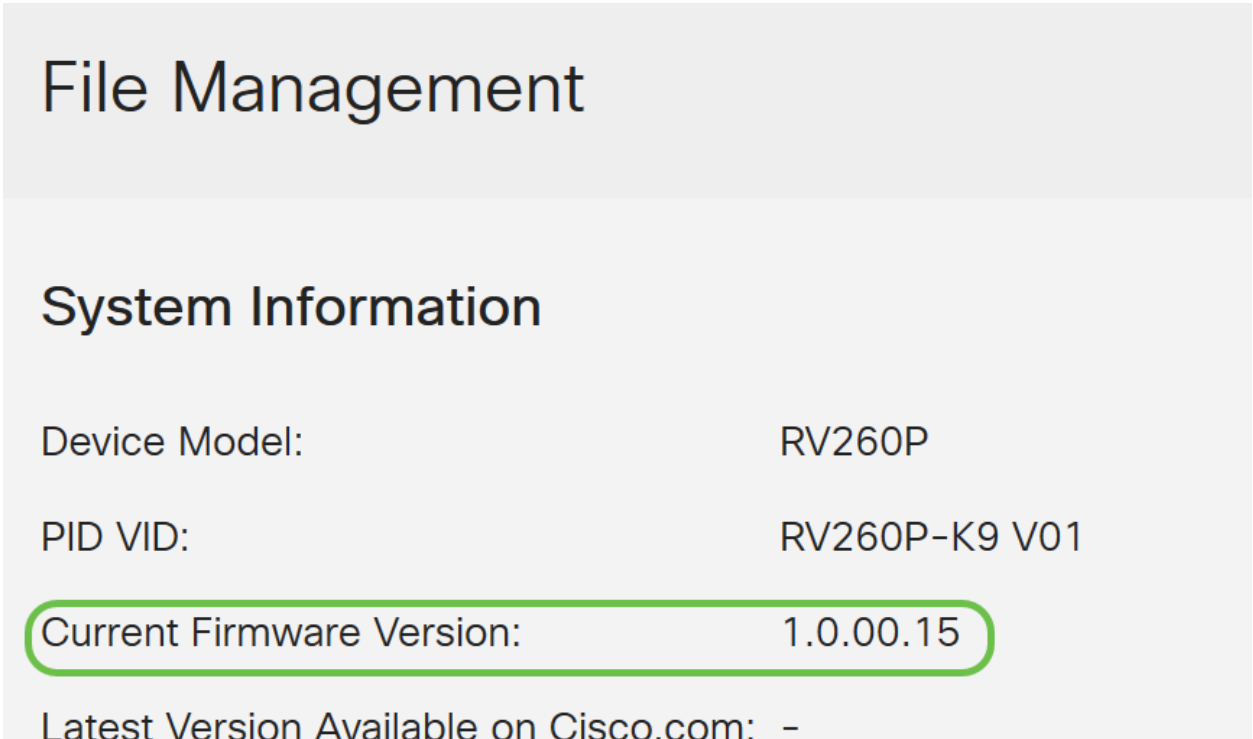
Passo 1

Escolha **Administration > File Management**.



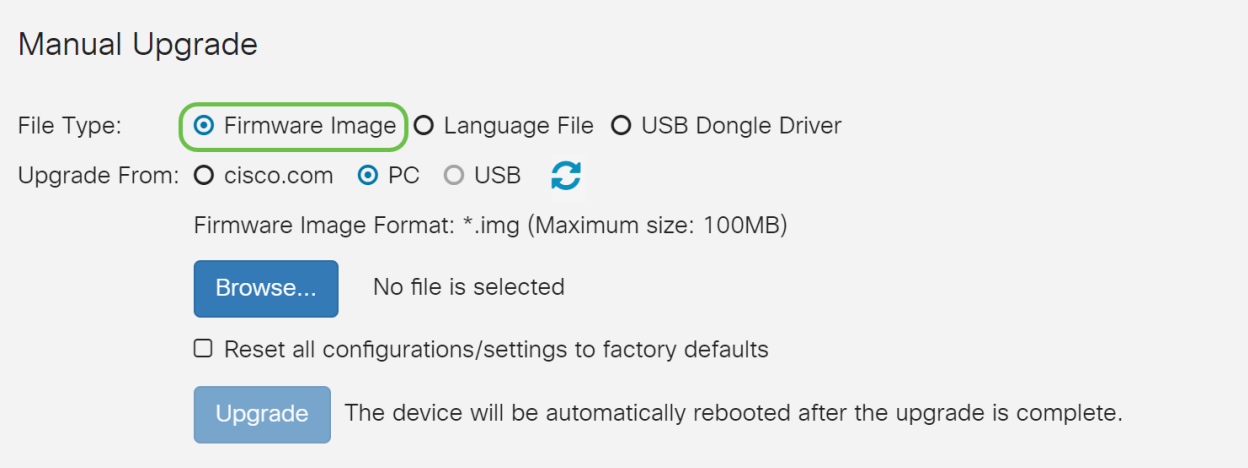
Na área *Informações do Sistema*, as seguintes subáreas descrevem o seguinte:

- Modelo do dispositivo - Exibe o modelo do dispositivo.
- PID VID - ID do produto e ID do fornecedor do roteador.
- Versão atual do firmware - Firmware que está sendo executado no momento no dispositivo.
- Versão mais recente disponível no Cisco.com - Versão mais recente do software disponível no site da Cisco.
- Última atualização do firmware - Data e hora da última atualização do firmware feita no roteador.



Passo 2

Na seção *Atualização manual*, clique no botão de opção **Imagem do firmware** para *Tipo de arquivo*.



Etapa 3

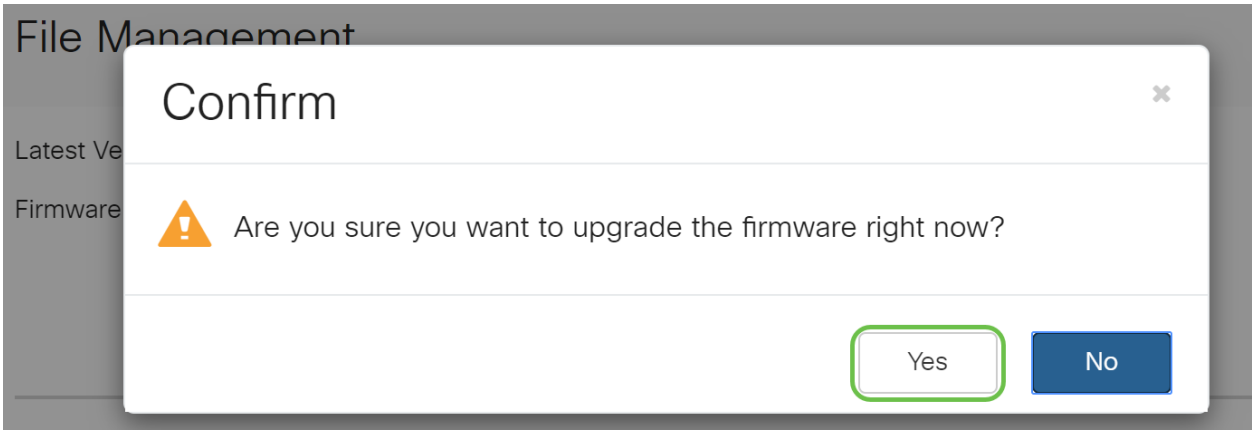
Na página *Atualização manual*, clique em um botão de opção para selecionar cisco.com. Há outras opções para isso, mas essa é a maneira mais fácil de fazer uma atualização. Este processo instala o arquivo de atualização mais recente diretamente da página da Web Downloads de software da Cisco.

Passo 4

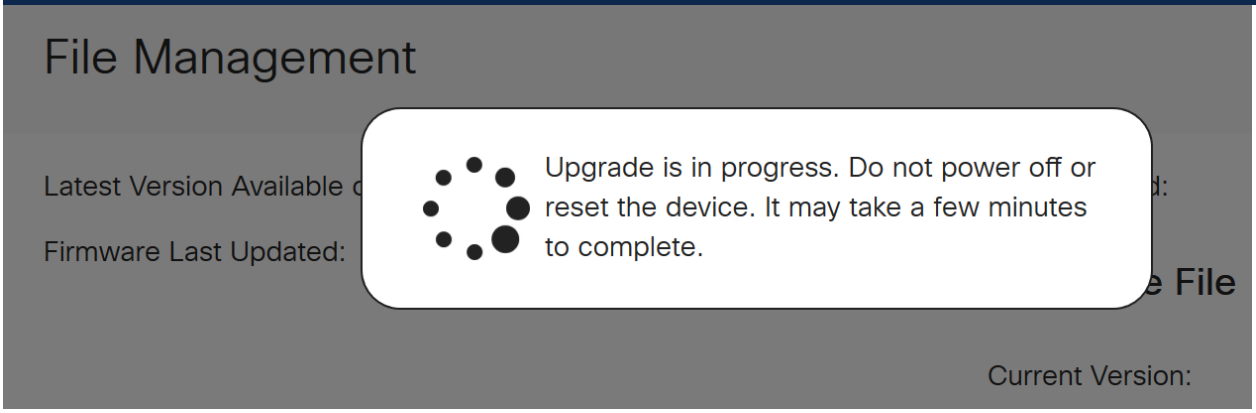
Clique em **Atualizar**.

Etapa 5

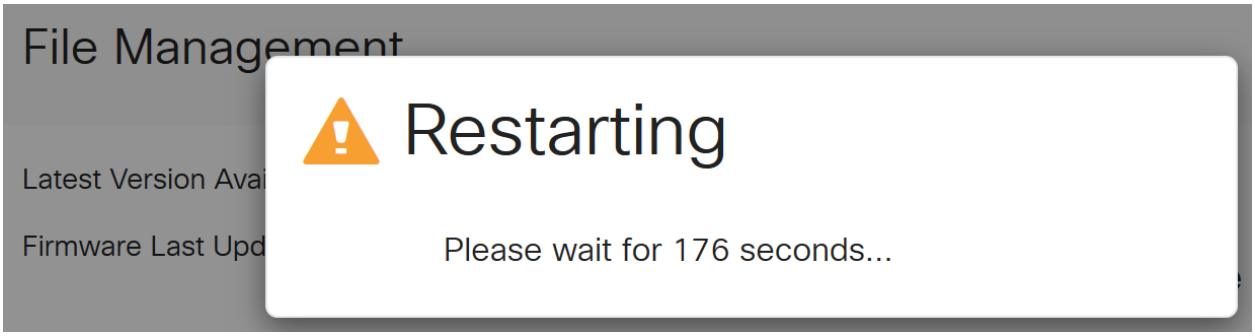
Clique em **Sim** na janela de confirmação para continuar.



O processo de atualização precisa ser executado sem interrupção. Você receberá a seguinte mensagem na tela enquanto a atualização estiver em andamento.

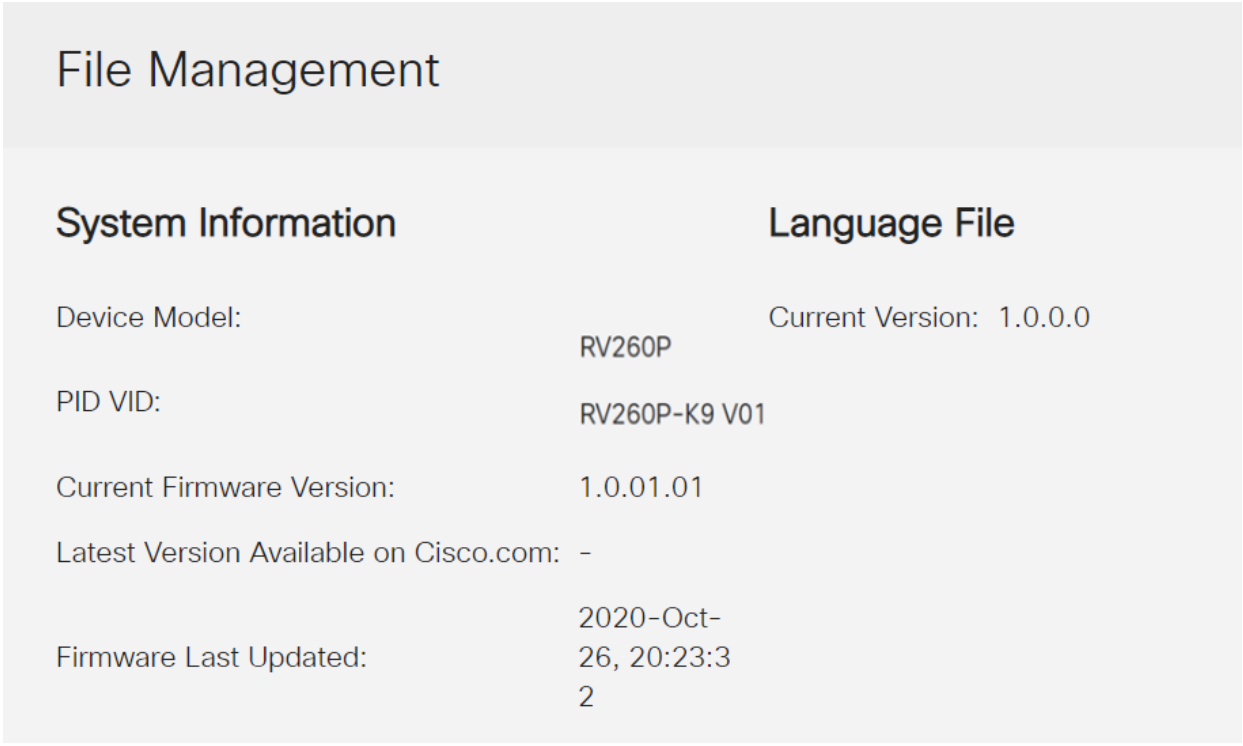


Quando a atualização for concluída, uma janela de notificação será exibida para informá-lo de que o roteador será *reinicializado* com uma contagem regressiva do tempo estimado para a conclusão do processo. Depois disso, você será desconectado.



Etapa 6

Efetue login novamente no utilitário baseado na Web para verificar se o firmware do roteador foi atualizado e vá até *System Information (Informações do sistema)*. A área *Versão atual do firmware* deve agora exibir a versão atualizada do firmware.



Parabéns, suas configurações básicas no roteador estão completas! Você tem algumas opções de configuração avançando.

Recomendo que você continue navegando pelo artigo para saber mais sobre essas opções e se elas se aplicam a você. Se preferir, você pode clicar em qualquer um dos hiperlinks para ir para uma seção.

- Configurar VLANs (opcional)
- Editar endereço IP (opcional)
- Adicionar endereços IP estáticos (opcional)
- Estou pronto para configurar a parte da rede sem fio em malha!

Configurar VLANs (opcional)

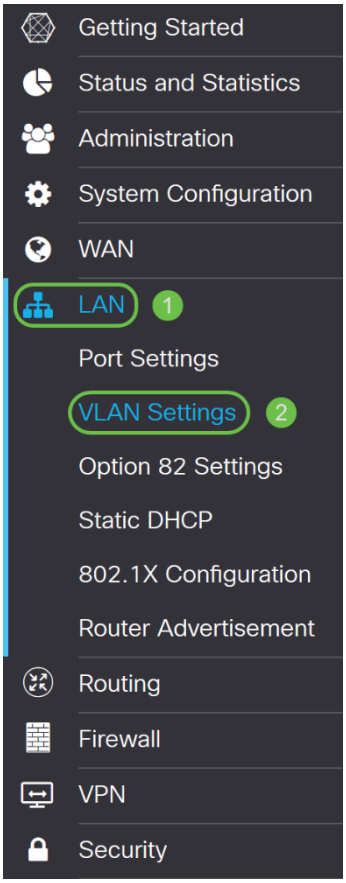
Uma rede local virtual (VLAN) permite segmentar logicamente uma rede de área local (LAN) em diferentes domínios de transmissão. Nos cenários em que dados confidenciais podem ser transmitidos em uma rede, as VLANs podem ser criadas para

aumentar a segurança, designando uma transmissão para uma VLAN específica. As VLANs também podem ser usadas para melhorar o desempenho, reduzindo a necessidade de enviar broadcasts e multicasts para destinos desnecessários. Você pode criar uma VLAN, mas isso não tem efeito até que a VLAN seja conectada a pelo menos uma porta, manual ou dinamicamente. As portas devem sempre pertencer a uma ou mais VLANs.

Se não quiser criar VLANs, você pode ir para a próxima seção.

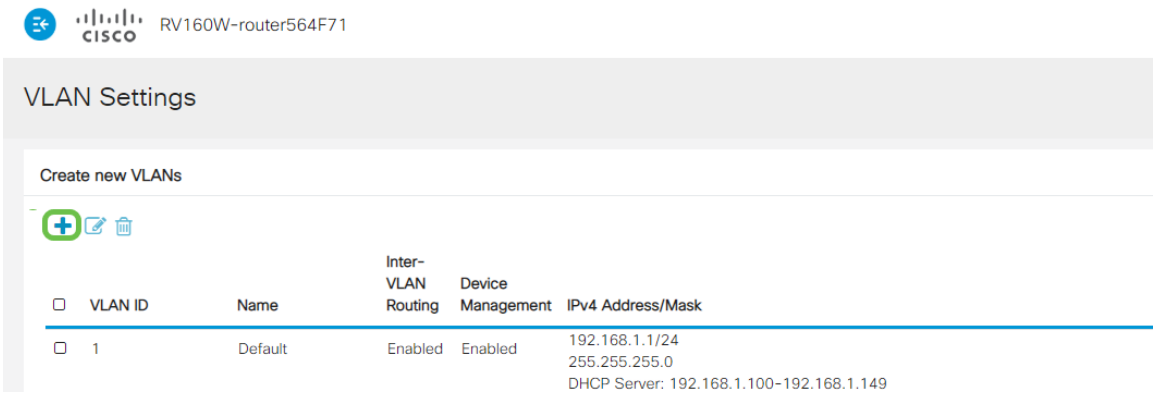
Passo 1

Navegue até **LAN > VLAN Settings**.



Passo 2

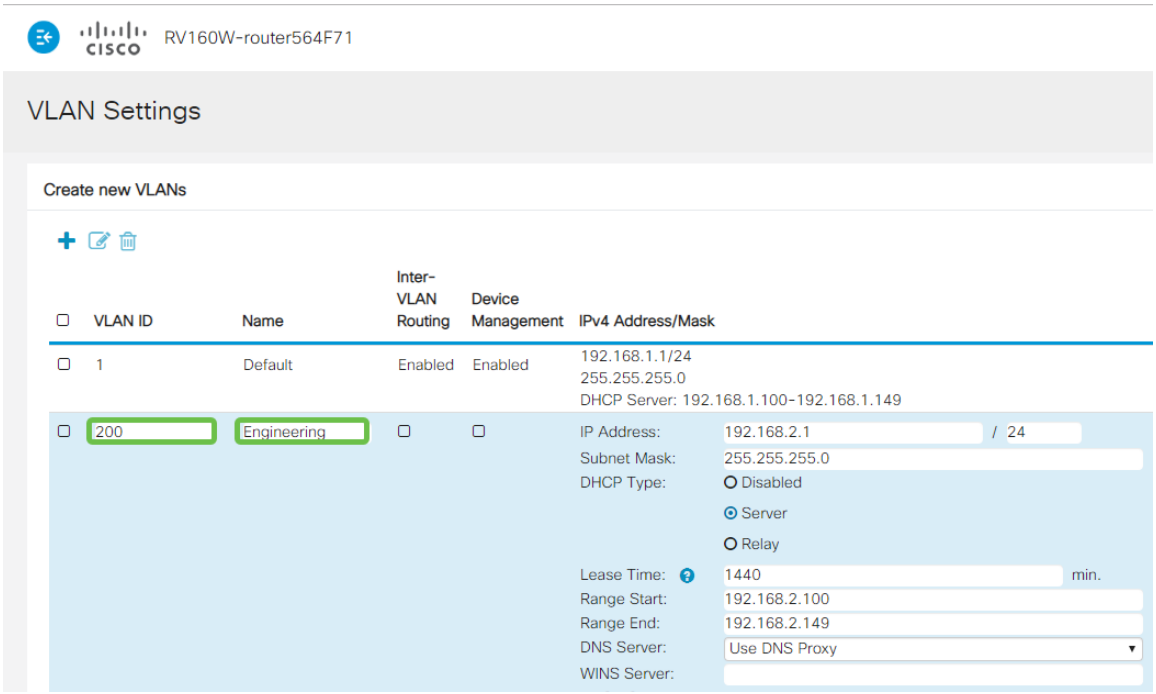
Clique em **Adicionar** para criar uma nova VLAN.



Etapa 3

Digite o *ID da VLAN* que deseja criar e um *Nome* para ele. O intervalo de *ID* da *VLAN* é de 1 a 4093.

Entramos em **200** como nossa *ID de VLAN* e **Engenharia** como *Nome* para a VLAN.



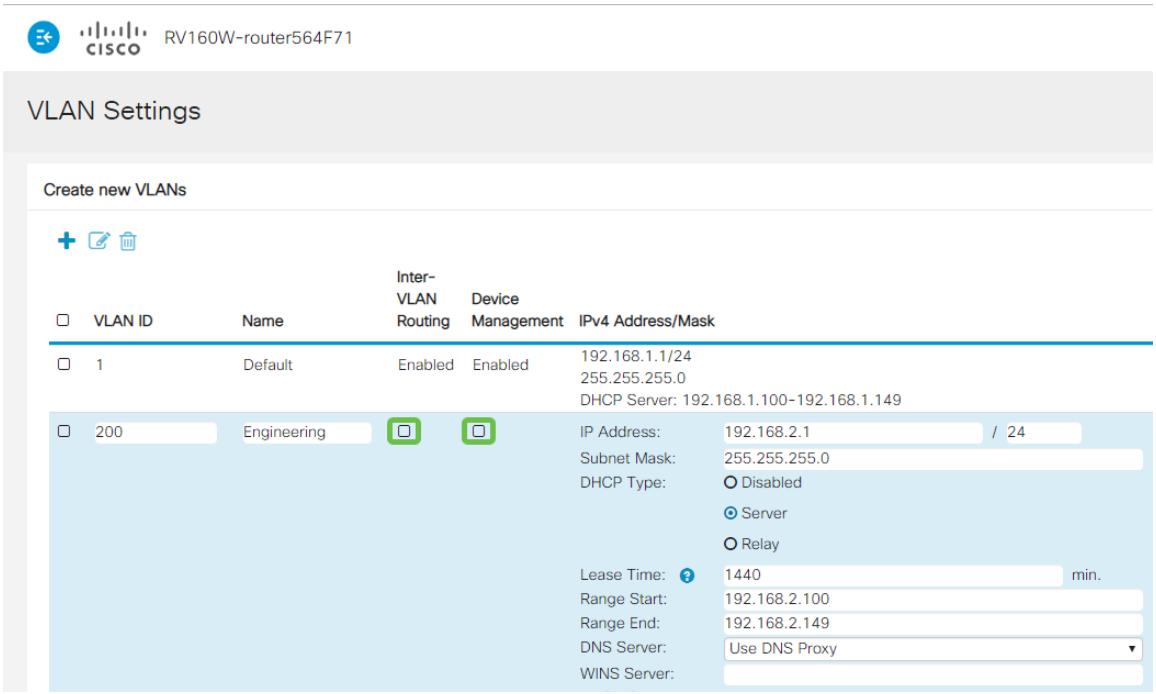
Passo 4

Desmarque a caixa *Enabled (Habilitado)* para *Inter-VLAN Routing* e *Device Management*, se desejado.

O roteamento entre VLANs é usado para rotear pacotes de uma VLAN para outra VLAN. Em geral, isso não é recomendado para redes de convidados, pois você vai querer isolar os usuários convidados, deixando as VLANs menos seguras. Às vezes, pode ser necessário que as VLANs façam o roteamento entre si. Se for esse o caso, verifique o Roteamento entre VLANs em um roteador RV34x com restrições de ACL direcionadas para configurar o tráfego específico que você permite entre VLANs.

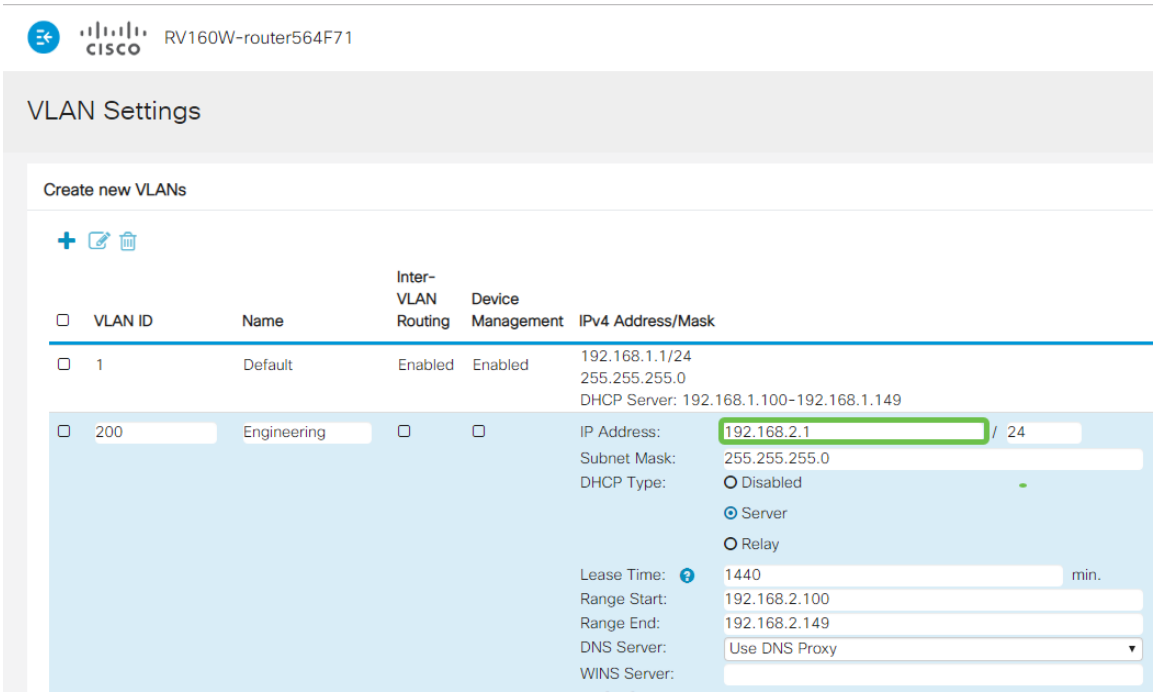
O Gerenciamento de dispositivos é o software que permite usar o navegador para fazer login na IU da Web do RV260P, a partir da VLAN, e gerenciar o RV260P. Isso também deve ser desativado em redes de Convidados.

Neste exemplo, não habilitamos o *roteamento entre VLANs* ou o *gerenciamento de dispositivos* para manter a VLAN mais segura.



Etapa 5

O endereço IPv4 privado será preenchido automaticamente no campo *Endereço IP*. Você pode ajustar isso se escolher. Neste exemplo, a sub-rede tem endereços IP 192.168.2.100-192.168.2.149 disponíveis para DHCP. 192.168.2.1-192.168.2.99 e 192.168.2.150-192.168.2.254 estão disponíveis para endereços IP estáticos.

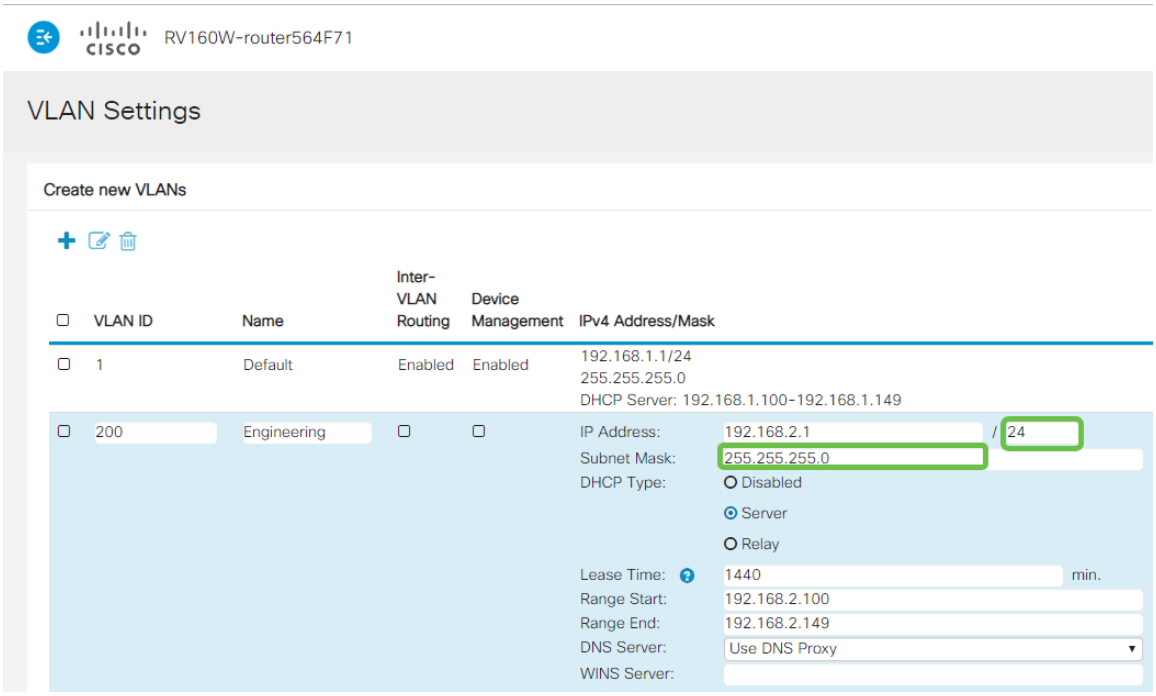


Etapa 6

A máscara de sub-rede em *Máscara de sub-rede* será preenchida automaticamente. Se você fizer alterações, o campo será automaticamente ajustado.

Para esta demonstração, deixaremos a *Máscara de sub-rede* como **255.255.255.0** ou

/24.



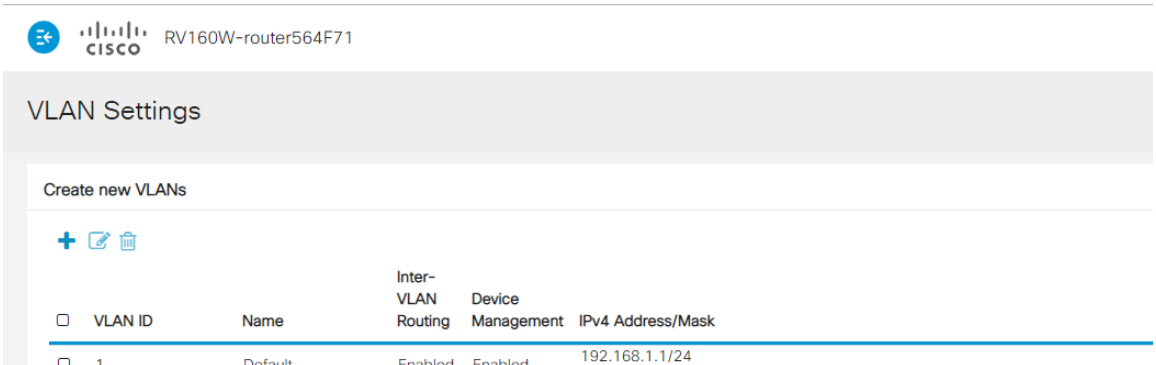
Etapa 7

Selecione um *tipo de protocolo DHCP*. As seguintes opções são:

Disabled (Desabilitado) - Desabilita o servidor DHCP IPv4 na VLAN. Isso é recomendado em um ambiente de teste. Nesse cenário, todos os endereços IP precisariam ser configurados manualmente e toda a comunicação seria interna.

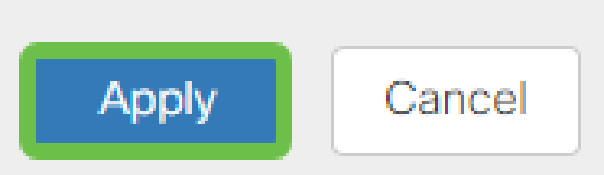
Server - Esta é a opção mais usada.

- Tempo de concessão - Insira um valor de tempo de 5 a 43.200 minutos. O padrão é 1440 minutos (igual a 24 horas).
- Intervalo Início e Intervalo Final - Insira o intervalo de início e fim dos endereços IP que podem ser atribuídos dinamicamente.
- Servidor DNS - Selecione para usar o servidor DNS como proxy ou do ISP na lista suspensa.
- WINS Server - Insira o nome do servidor WINS.
- Opções de DHCP:
    - Opção 66 - Insira o endereço IP do servidor TFTP.
    - Opção 150 - Insira o endereço IP de uma lista de servidores TFTP.
    - Opção 67 - Insira o nome do arquivo de configuração.
- Relay - Insira o endereço IPv4 do servidor DHCP remoto para configurar o agente de retransmissão DHCP. Essa é uma configuração mais avançada.



Passo 8

Clique em **Apply** para criar a nova VLAN.



Atribuir VLANs às portas

16 VLANs podem ser configuradas no RV260, com uma VLAN para a rede de longa distância (WAN). As VLANs que não estão em uma porta devem ser *excluídas*. Isso mantém o tráfego nessa porta exclusivamente para as VLAN/VLANs especificamente atribuídas pelo usuário. É considerada uma boa prática.

As portas podem ser definidas como uma porta de acesso ou uma porta de tronco:

- Porta de acesso - uma VLAN atribuída. Os quadros não marcados são passados.
- Porta de tronco - Pode transportar mais de uma VLAN. 802.1q. O entroncamento permite que uma VLAN nativa seja desmarcada. As VLANs que você não deseja no tronco devem ser excluídas.

Uma VLAN atribuiu sua própria porta:

- Considerada uma porta de acesso.
- A VLAN atribuída a esta porta deve ser rotulada como Não rotulada.
- Todas as outras VLANs devem ser rotuladas como Excluídas para essa porta.

Duas ou mais VLANs que compartilham uma porta:

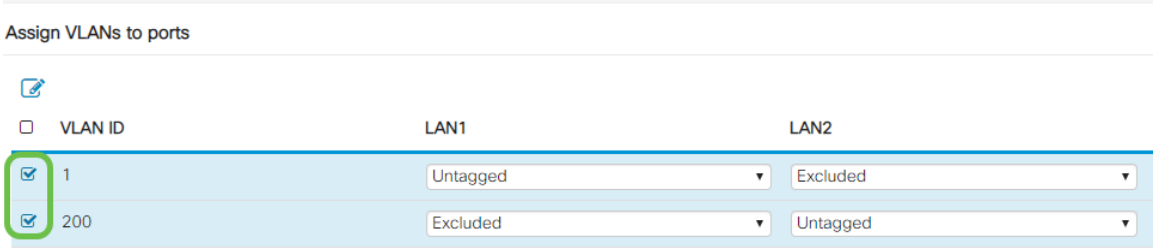
- Considerada uma porta de tronco.
- Uma das VLANs pode ser rotulada como Não rotulada.
- O restante das VLANs que fazem parte da porta de tronco deve ser rotulado como Marcado.
- As VLANs que não fazem parte da Porta de Tronco devem ser rotuladas Excluídas para essa porta.

Observação: neste exemplo, não há troncos.

Passo 9

Selecione as *IDs de VLAN* a serem editadas. Clique em Editar.

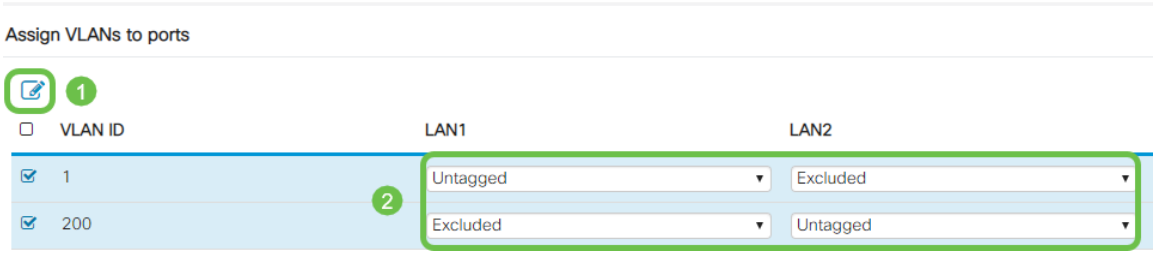
Neste exemplo, selecionamos *VLAN 1* e *VLAN 200*.



Passo 10

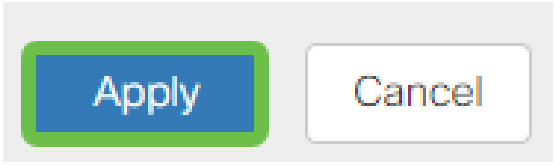
Clique em **Editar** para atribuir uma VLAN a uma porta LAN e especifique cada configuração como *Marcada*, *Não Marcada* ou *Excluída*.

Neste exemplo, em LAN1, atribuímos a VLAN 1 como **Não Marcada** e a VLAN 200 como **Excluída**. Para LAN2, atribuímos a VLAN 1 como **excluída** e a VLAN 200 como **não rotulada**.



Passo 11

Clique em **Apply** para salvar a configuração.



Agora você deve ter criado com êxito uma nova VLAN e configurado VLANs para portas no RV260. Repita o processo para criar as outras VLANs. Por exemplo, a VLAN300 seria criada para o Marketing com uma sub-rede de 192.168.3.x e a VLAN400 seria criada para o Accounting com uma sub-rede de 192.168.4.x.

Isso é o básico das VLANs. Clique no hiperlink para saber mais sobre as Melhores práticas de VLAN e as Dicas de segurança para os Cisco Business Routers.

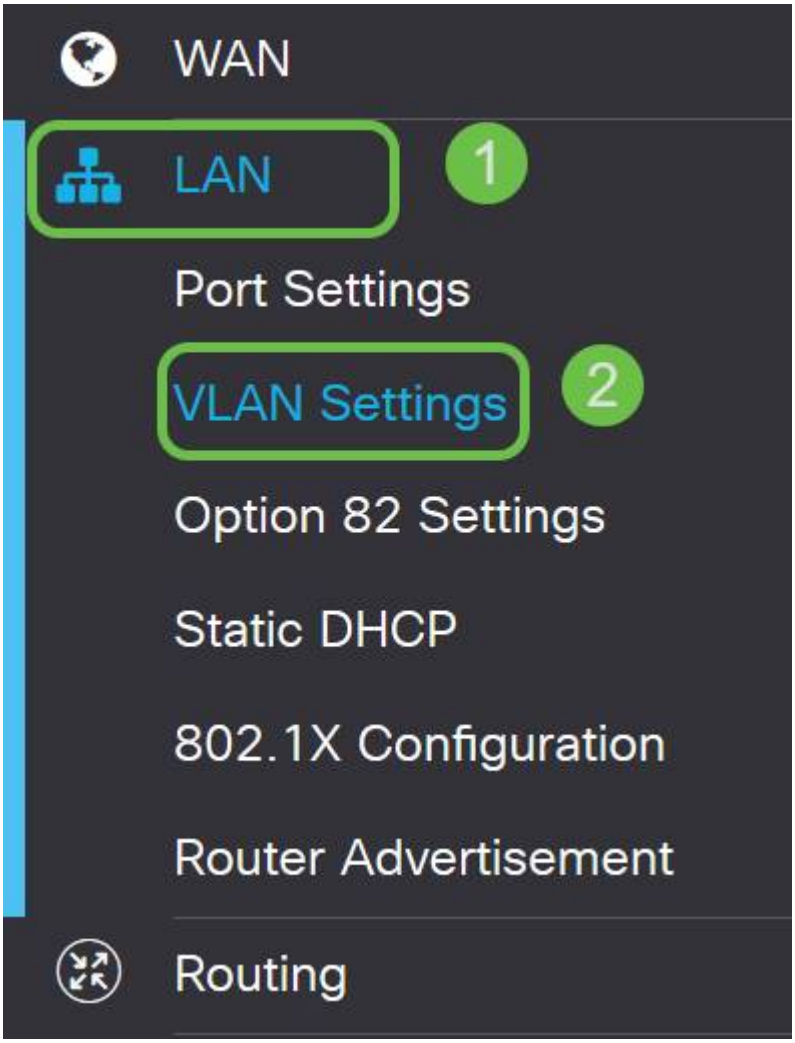
Editar um endereço IP (opcional)

Após concluir o *Assistente de configuração inicial*, você pode definir um endereço IP estático no roteador editando as configurações da VLAN. Ignore a reexecução do assistente de configuração inicial. Para executar essa alteração, siga as etapas abaixo.

Se não precisar editar um endereço IP, você pode ir para a próxima seção deste artigo.

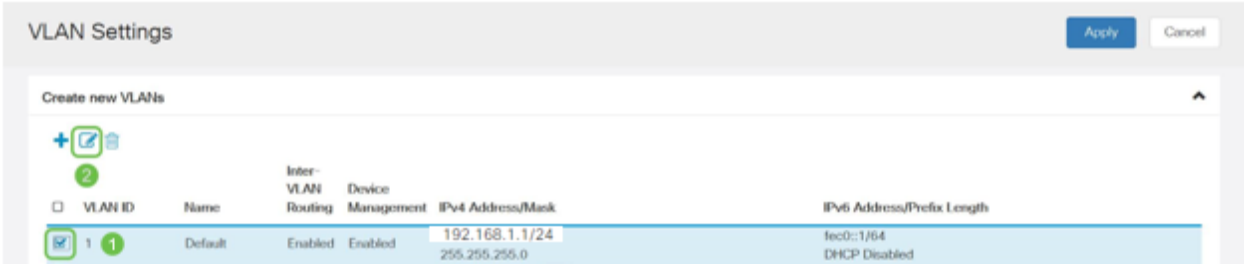
Passo 1

Na barra de menus à esquerda, clique em **LAN > VLAN Settings**.



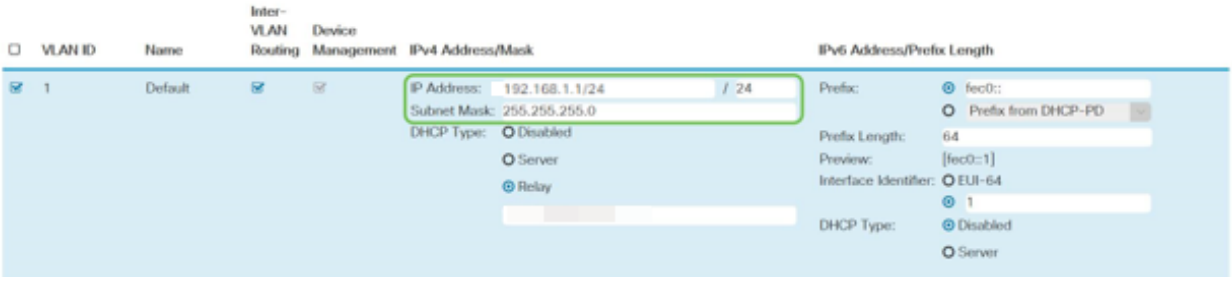
Passo 2

Em seguida, selecione a **VLAN** que contém seu dispositivo de roteamento e clique no **ícone de edição**.



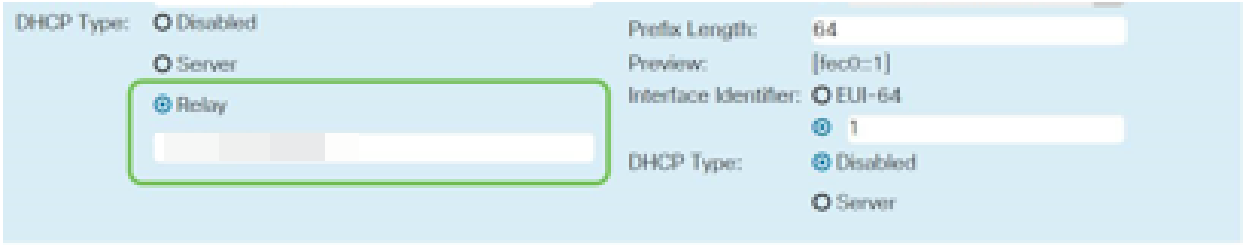
Etapa 3

Insira o **endereço IP estático** desejado e clique em **Apply (Aplicar)** no canto superior direito.



Etapa 4 (Opcional)

Se o roteador não for o servidor/dispositivo DHCP atribuindo endereços IP, você poderá usar o recurso de Retransmissão DHCP para direcionar solicitações DHCP a um endereço IP específico. O endereço IP provavelmente será o roteador conectado à WAN/Internet.



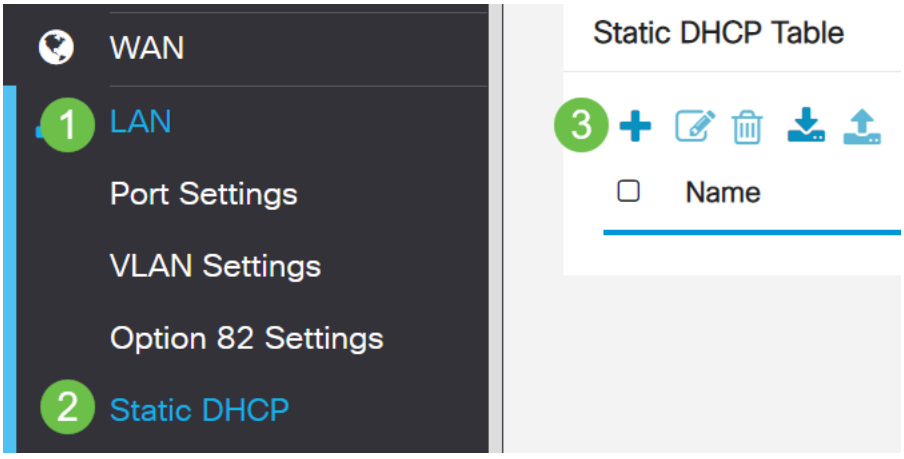
Adicionar um IP estático

Se você quiser que um determinado dispositivo esteja acessível a outras VLANs, você pode dar a esse dispositivo um endereço IP local estático e criar uma regra de acesso para torná-lo acessível. Isso só funciona se o roteamento entre VLANs estiver ativado. Há outras situações em que um IP estático pode ser útil. Para obter mais informações sobre como configurar endereços IP estáticos, consulte Práticas recomendadas para configurar endereços IP estáticos no hardware comercial da Cisco.

Se não precisar adicionar um endereço IP estático, você pode ir para a próxima seção deste artigo para configurar os Pontos de acesso.

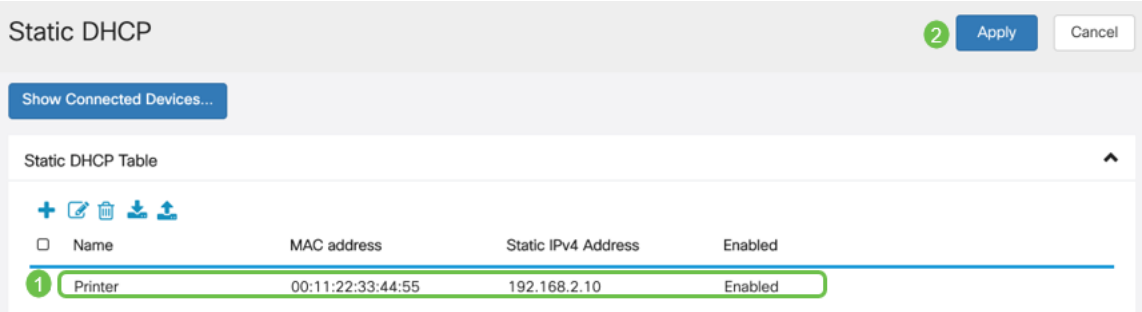
Passo 1

Navegue até **LAN > DHCP estático.** Clique no **ícone de mais**.



Passo 2

Adicione as informações **DHCP estático** para o dispositivo. Neste exemplo, o dispositivo é uma impressora.



Parabéns, você concluiu a configuração do roteador RV260P. Agora, configuraremos seus dispositivos sem fio comerciais da Cisco.

Configurar o CBW140AC

CBW140AC pronto para uso

Comece conectando um cabo Ethernet da porta PoE no CBW140AC a uma porta PoE no RV260P. As primeiras 4 portas no RV260P podem fornecer PoE, para que qualquer uma delas possa ser usada.

Verifique o status das luzes indicadoras. O ponto de acesso levará cerca de 10 minutos para ser inicializado. 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 da cor do LED e na tonalidade de unidade para unidade. Quando a luz do LED estiver piscando em verde, vá para a próxima etapa.

A porta de uplink Ethernet PoE no AP primário SÓ pode ser usada para fornecer um uplink para a LAN e NÃO para se conectar a qualquer outro dispositivo de extensor de malha ou com capacidade primária.

Se o seu ponto de acesso não for novo, verifique se ele está redefinido para as configurações padrão de fábrica do SSID *Cisco Business-Setup* para aparecer em suas opções Wi-Fi. Para obter ajuda com isso, consulte Como reinicializar e redefinir as configurações padrão de fábrica nos roteadores RV260.

Configurar o ponto de acesso sem fio principal 140AC na interface do usuário da Web

Você pode configurar o ponto de acesso usando o aplicativo móvel ou a interface de usuário da Web. Este artigo usa a interface de usuário da Web para configuração, que oferece mais opções para configuração, mas é um pouco mais complicada. Se quiser usar o aplicativo móvel para as próximas seções, clique para acessar as instruções do aplicativo móvel.

Se tiver problemas para se conectar, consulte a seção Dicas de solução de problemas

sem fio deste artigo.

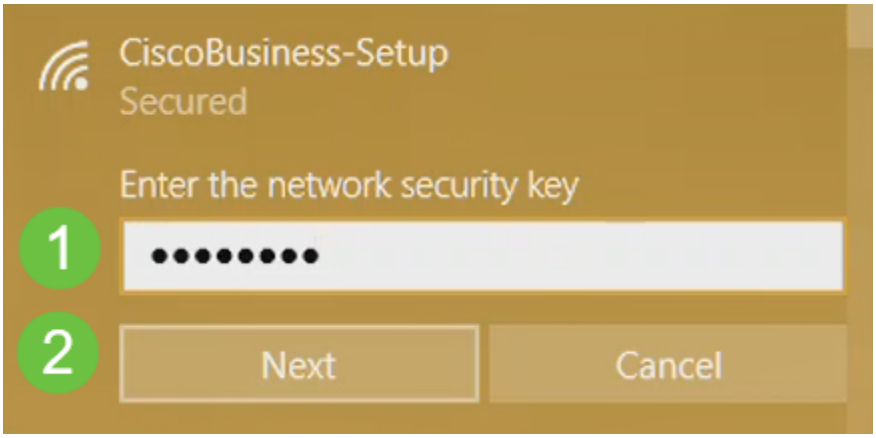
Passo 1

No PC, clique no **ícone Wi-Fi** e escolha rede sem fio *Cisco Business-Setup*. Clique em Conectar.

Se o seu ponto de acesso não for novo, verifique se ele está redefinido para as configurações padrão de fábrica do SSID *Cisco Business-Setup* para aparecer em suas opções Wi-Fi.

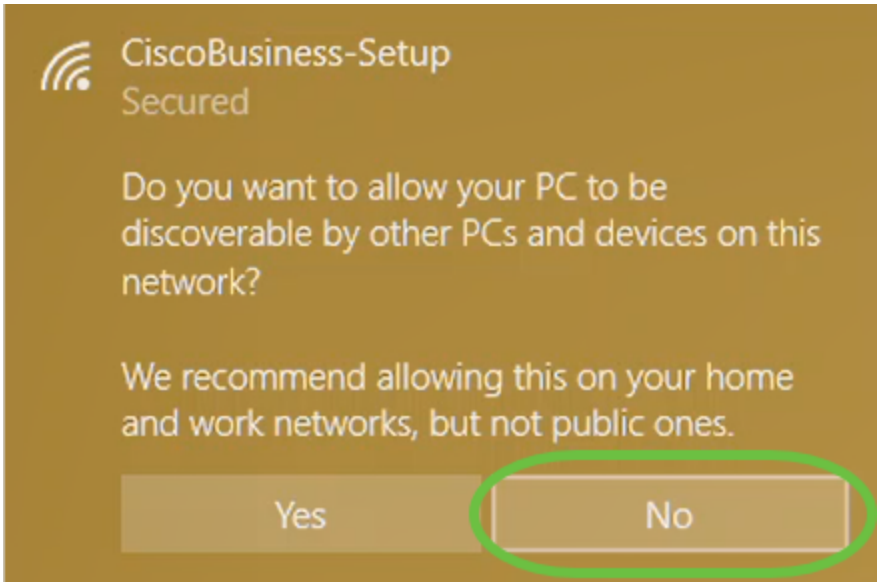
Passo 2

Insira a senha **cisco123** e clique em **Avançar**.



Etapa 3

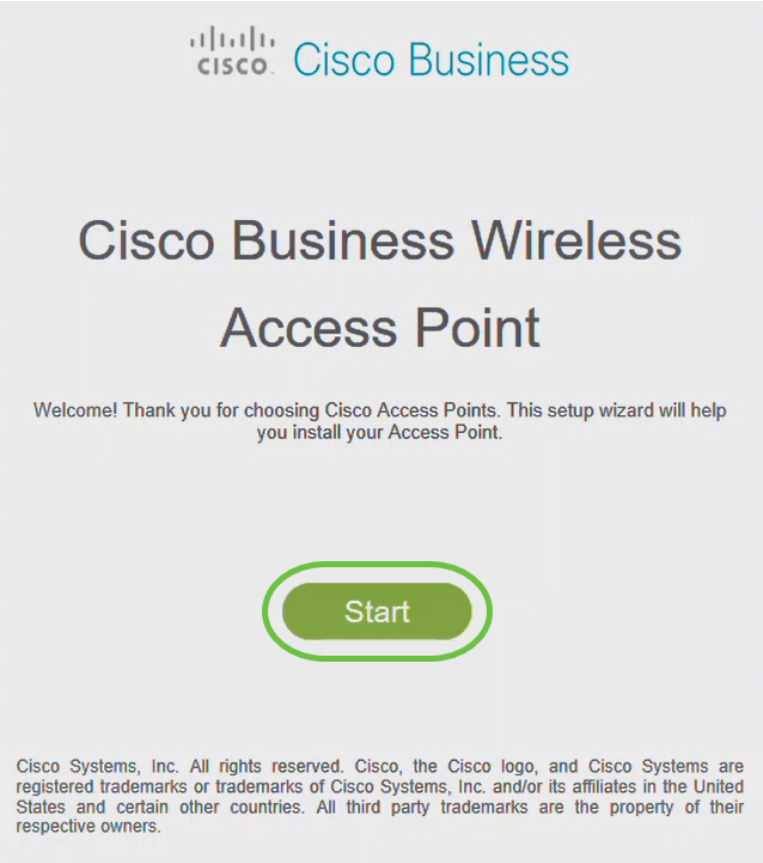
Você receberá a seguinte tela. Como você pode configurar apenas um dispositivo por vez, clique em **Não**.



Apenas um dispositivo pode ser conectado ao SSID *Cisco Business-Setup*. Se um segundo dispositivo tentar se conectar, ele não poderá. Se você não puder se conectar ao SSID e tiver validado a senha, talvez outro dispositivo tenha feito a conexão. Reinicie o AP e tente novamente.

Passo 4

Depois de conectado, o navegador da Web deve redirecionar automaticamente para o assistente de configuração do AP CBW. Caso contrário, abra um navegador da Web, como Internet Explorer, Firefox, Chrome ou Safari. Na barra de endereços, digite **http://ciscobusiness.cisco** e pressione **Enter**. Clique em **Iniciar** na página da Web.



Se você não vir a página da Web, aguarde mais alguns minutos ou recarregue a página. Após essa configuração inicial, você usará https://ciscobusiness.cisco para fazer login. Se o seu navegador da Web for preenchido automaticamente com *http://*, você precisará digitar manualmente *https://* para obter acesso.

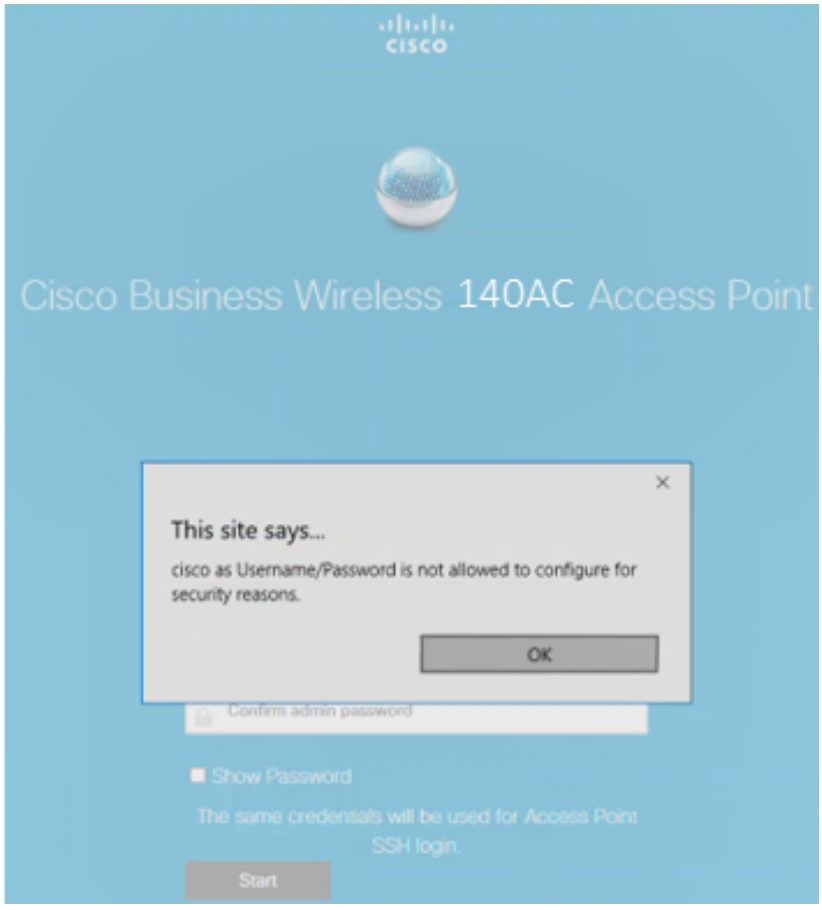
Etapa 5

Crie uma *conta admin* inserindo o seguinte:

- Nome de usuário do administrador (máximo de 24 caracteres)
- Senha do administrador
- Confirmar senha do administrador

Você pode escolher mostrar a senha marcando a caixa de seleção ao lado de *Mostrar senha*. Clique em Iniciar.

Não use *cisco* ou suas variações nos campos nome de usuário ou senha. Em caso afirmativo, você receberá uma mensagem de erro, conforme mostrado abaixo.

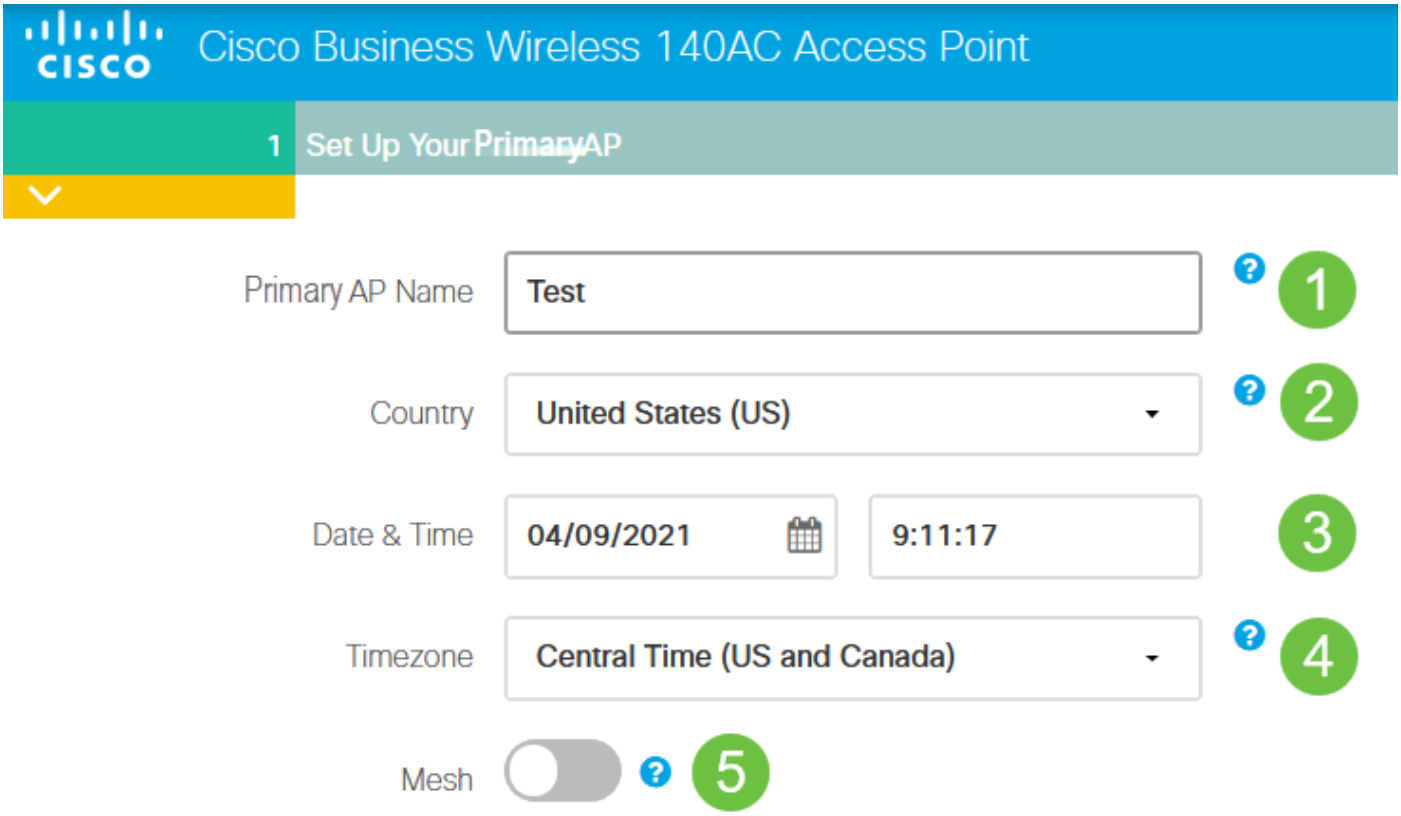


Etapa 6

Configure seu AP primário inserindo o seguinte:

- Nome do AP principal
- País

- Data e hora
- Fuso horário
- Malha



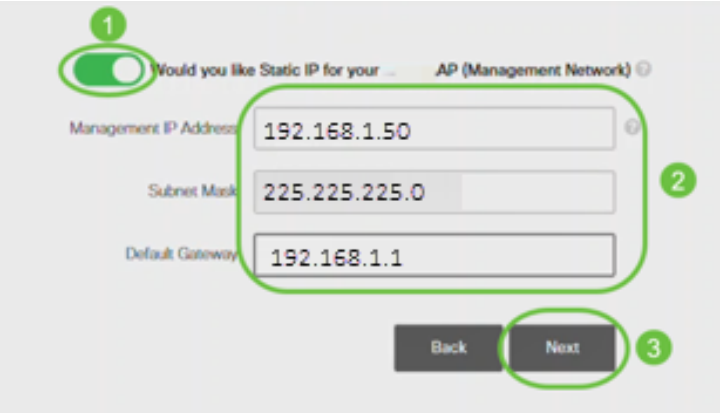
A malha deve ser habilitada somente se você planeja criar uma rede em malha. Por padrão, ele é desativado.

Etapa 7

(Opcional) Você pode habilitar o *IP estático para seu* CBW140AC para fins de gerenciamento. Caso contrário, a interface obtém um endereço IP do servidor DHCP. Para configurar o IP estático, insira o seguinte:

- Endereço IP de gerenciamento
- Máscara de sub-rede
- Gateway padrão

Clique em Next.



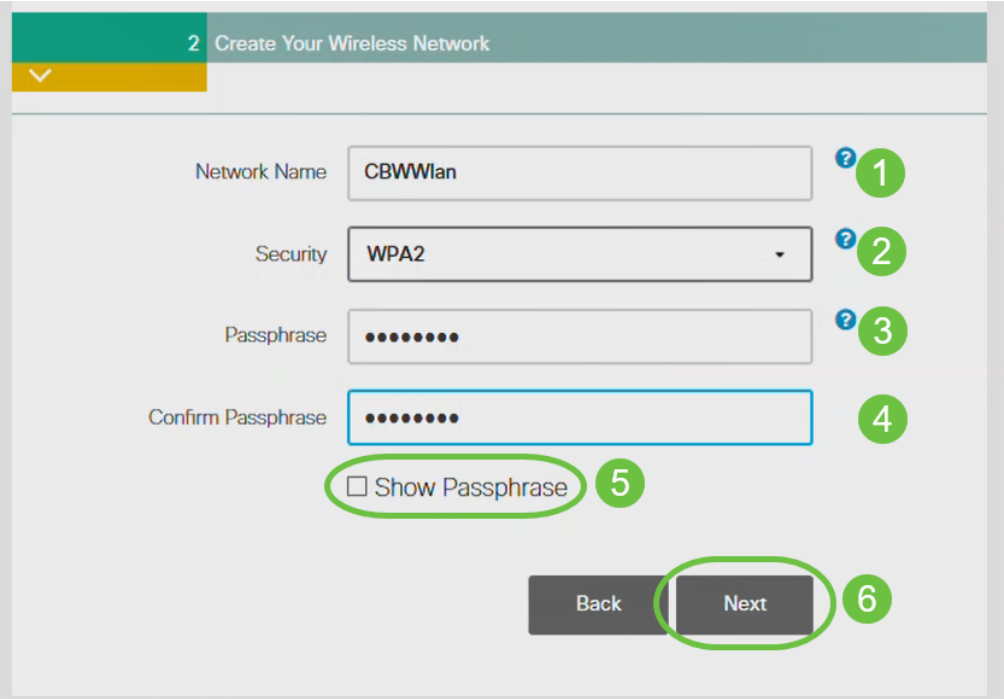
Por padrão, essa opção está desativada.

Passo 8

Crie suas redes sem fio inserindo o seguinte:

- Nome da rede
- Escolher segurança
- Senha
- Confirmar senha
- (Opcional) Marque a caixa de seleção para Mostrar senha.

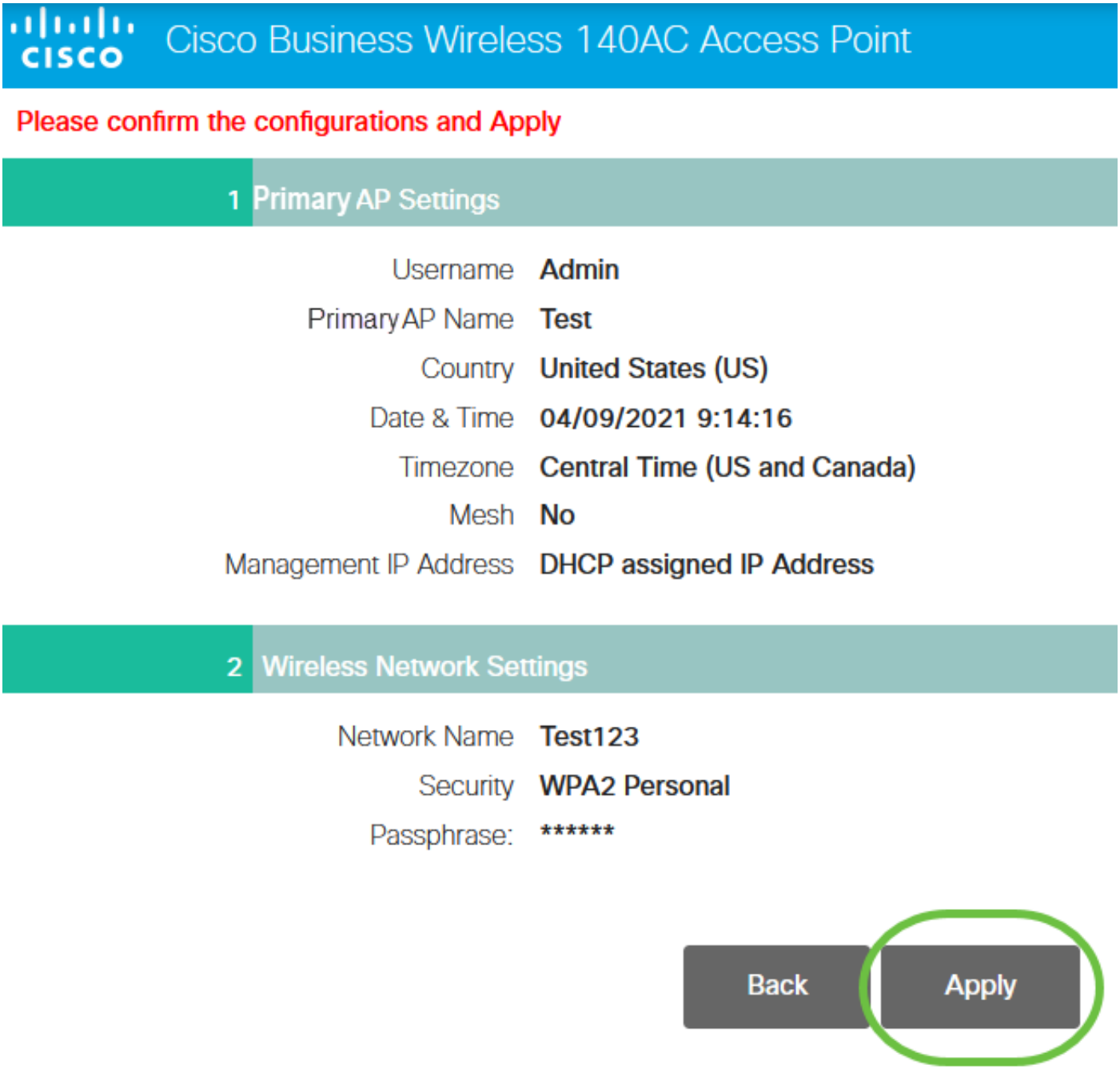
Clique em Next.



O WPA (Wi-Fi Protected Access) versão 2 (WPA2) é o padrão atual para segurança Wi-Fi.

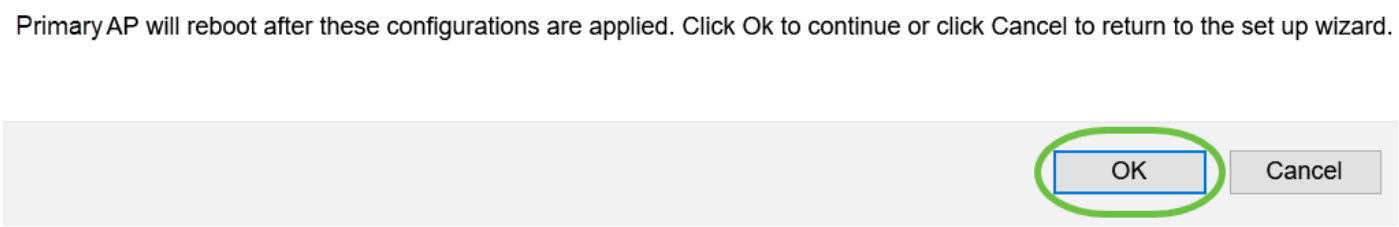
Passo 9

Confirme as configurações e clique em **Aplicar**.

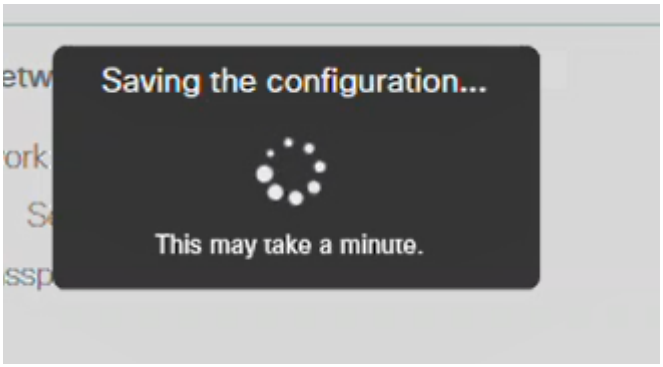


Passo 10

Clique em **OK** para aplicar as configurações.



Você verá a tela a seguir enquanto as configurações estiverem sendo salvas e o sistema for reinicializado. Isso pode levar 10 minutos.

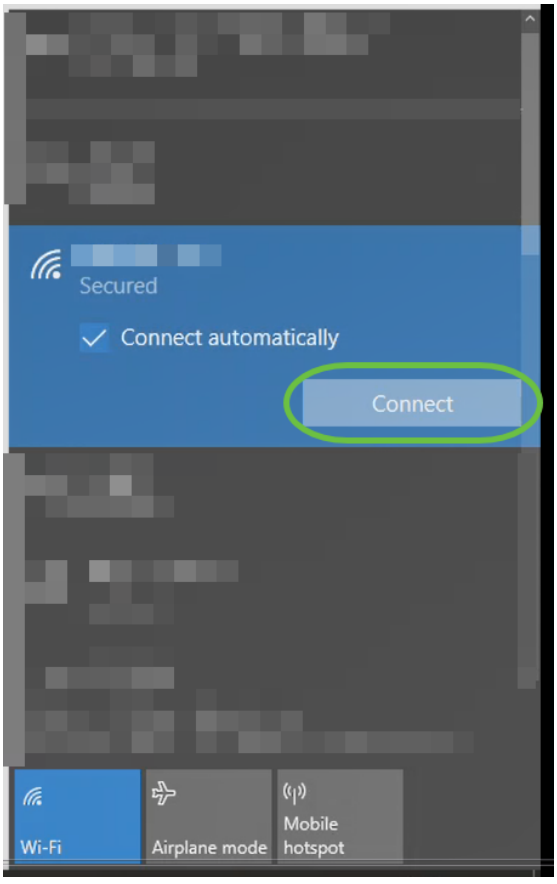


Durante a reinicialização, o LED no ponto de acesso passará por vários padrões de cores. Quando o LED estiver piscando em verde, vá para a próxima etapa. Se o LED não ultrapassar o padrão vermelho piscante, isso indica que não há servidor DHCP em sua rede. Verifique se o AP está conectado a um switch ou roteador com um servidor DHCP.

Passo 11

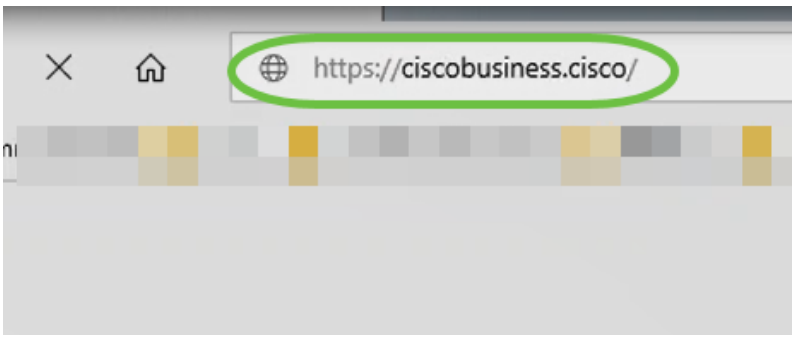
Vá para as opções sem fio do PC e escolha a rede que você configurou. Clique em Conectar.

O SSID *Cisco Business-Setup* desaparecerá após a reinicialização.



Etapa 12

Abra um navegador da Web e digite *https://[endereço IP do AP CBW]*. Como alternativa, você pode digitar *https://ciscobusiness.cisco* na barra de endereços e pressionar Enter.



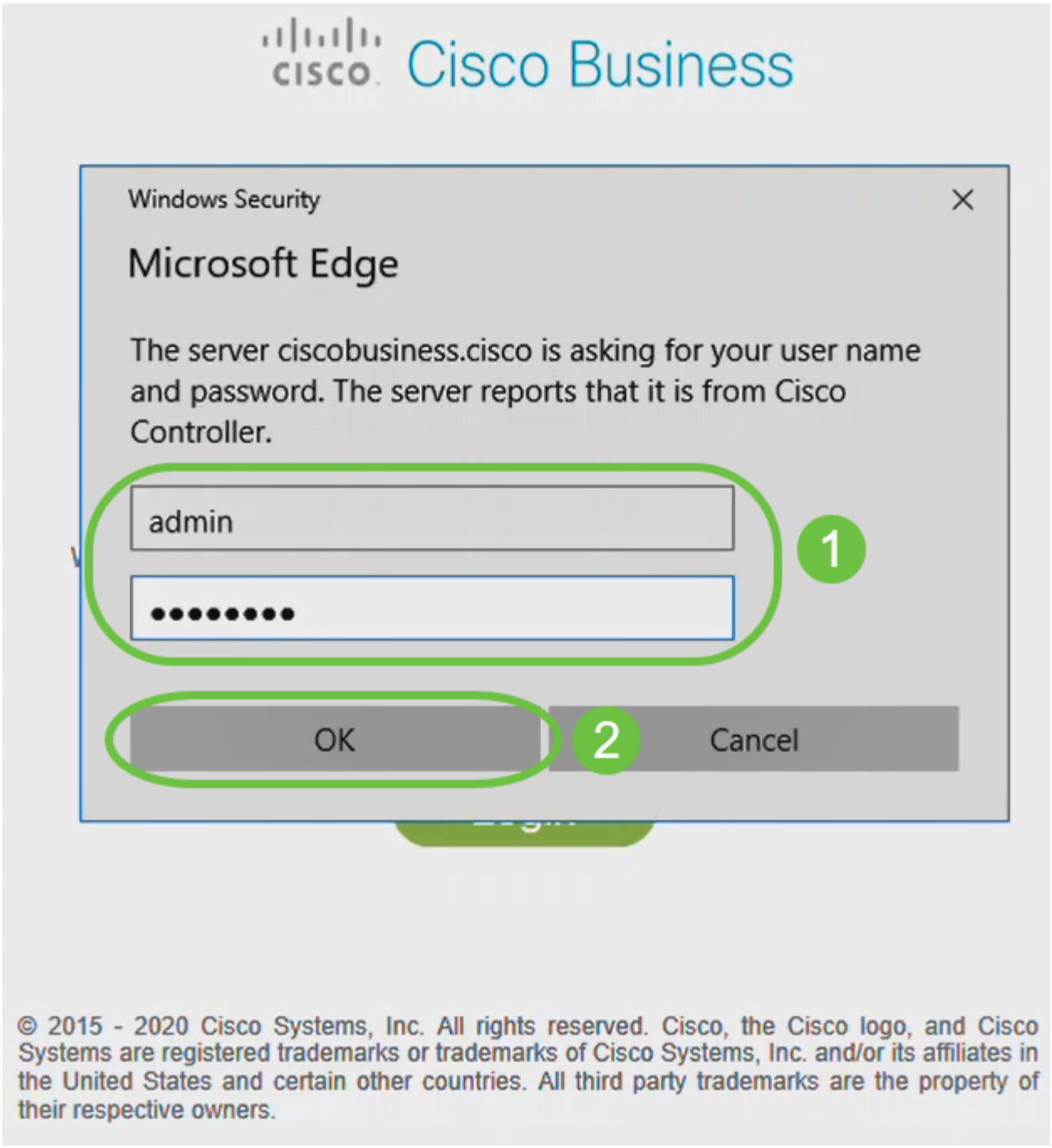
Certifique-se de digitar *https* e não *http* nesta etapa.

Passo 13

Clique em login.

Passo 14

Faça login usando as credenciais configuradas. Click OK.



Etapa 15

Você poderá acessar a página da IU da Web do AP.

Dicas para solução de problemas sem fio

Se tiver problemas, dê uma olhada nas seguintes dicas:

- Verifique se o SSID (Service Set Identifier, Identificador do conjunto de serviços) correto está selecionado. Este é o nome que você criou para a rede sem fio.
- Desconecte qualquer VPN do aplicativo móvel ou de um laptop. Você pode até estar conectado a uma VPN que o seu provedor de serviços móveis usa e que você talvez nem saiba. Por exemplo, um telefone Android (Pixel 3) com Google Fi como provedor de serviços, há uma VPN integrada que se conecta automaticamente sem notificação. Isso precisaria ser desabilitado para encontrar o AP primário.
- Efetue login no AP primário com https://<endereço IP do AP primário>.
- Depois de fazer a configuração inicial, certifique-se de que https:// is esteja sendo usado para fazer login no *ciscobusiness.cisco* ou inserindo o endereço IP no navegador da Web. Dependendo das suas configurações, o computador pode ter sido preenchido automaticamente com http:// since, que é o que você usou na primeira vez em que se conectou.
- Para ajudar com problemas relacionados ao acesso à interface do usuário da Web ou problemas do navegador durante o uso do AP, no navegador da Web (neste caso, Firefox), clique no menu Abrir, vá para Ajuda > Informações de solução de problemas e clique em Atualizar Firefox.

Configure os extensores de malha CBW142ACM usando a interface de usuário da Web

Você está na parte inicial da configuração dessa rede, basta adicionar seus extensores de malha!

Passo 1

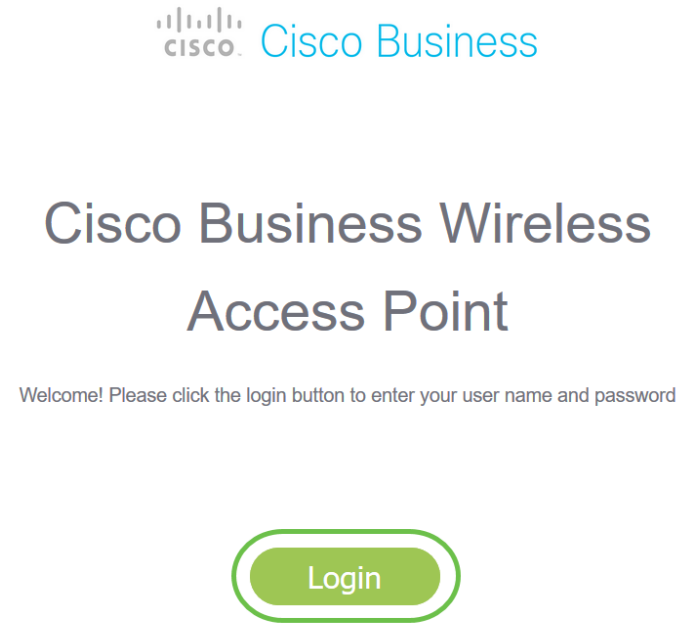
Conecte os dois extensores de malha na parede nos locais selecionados. Anote o endereço MAC de cada extensor de malha.

Passo 2

Aguarde cerca de 10 minutos até que o Mesh Extenders seja inicializado.

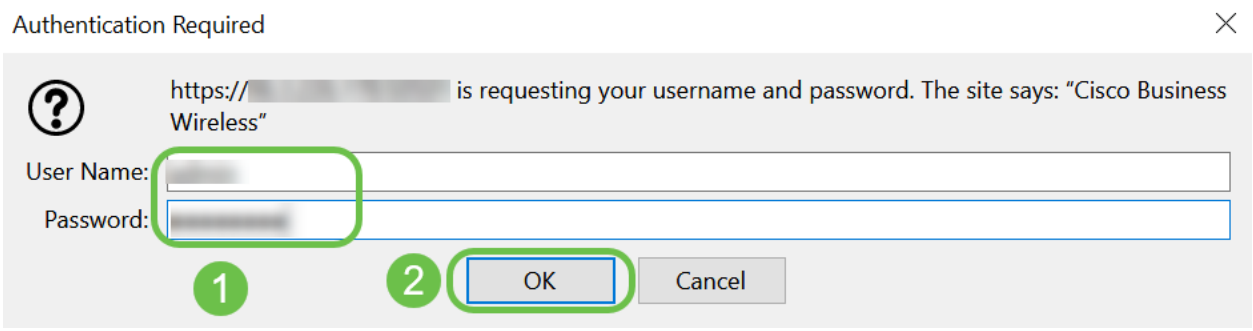
Etapa 3

Insira o endereço IP dos pontos de acesso primários (APs) no navegador da Web. Clique em **Login** para acessar o AP primário.



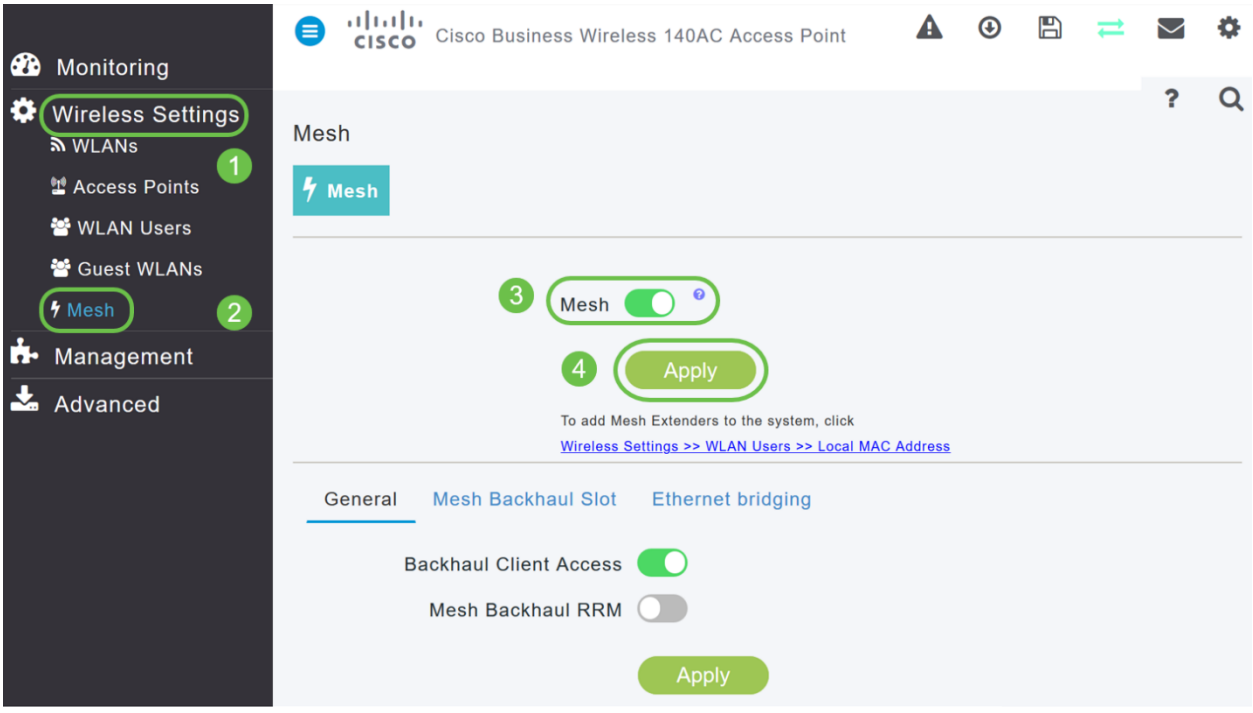
Passo 4

Insira suas credenciais *de Nome de usuário* e *Senha* para acessar o AP primário. Click OK.



Etapa 5

Navegue até **Wireless Settings > Mesh**. Verifique se a *malha* está ativada. Clique em Apply.

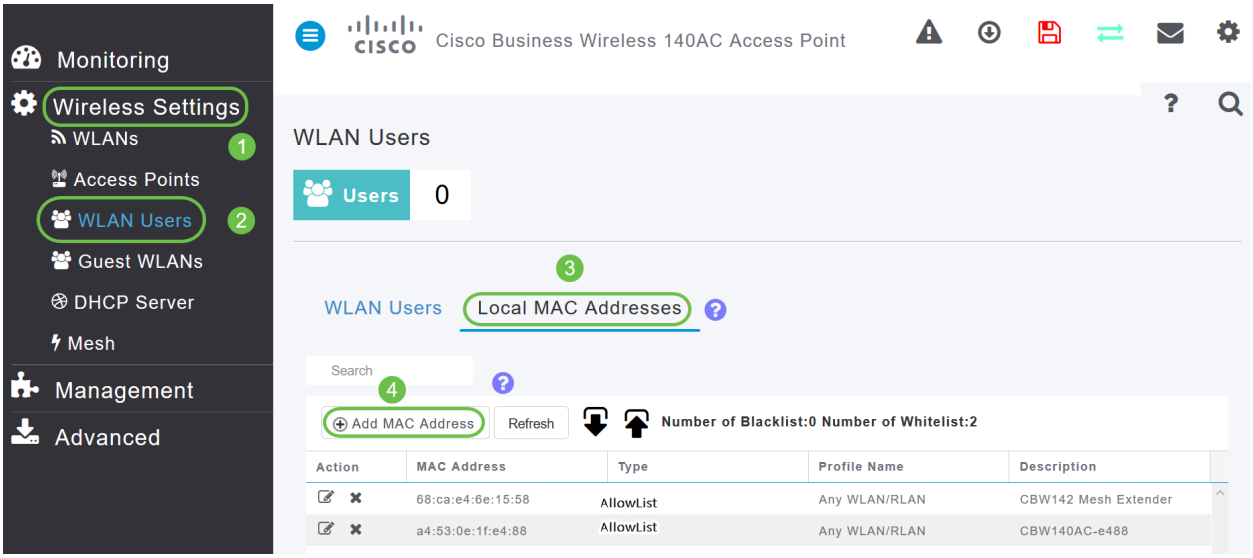


Etapa 6

Se Mesh ainda não estiver habilitada, o WAP pode precisar executar uma reinicialização. Uma janela pop-up será exibida para fazer uma reinicialização. Confirme. Isso levará cerca de 10 minutos. Durante uma reinicialização, 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 da cor do LED e na tonalidade de unidade para unidade.

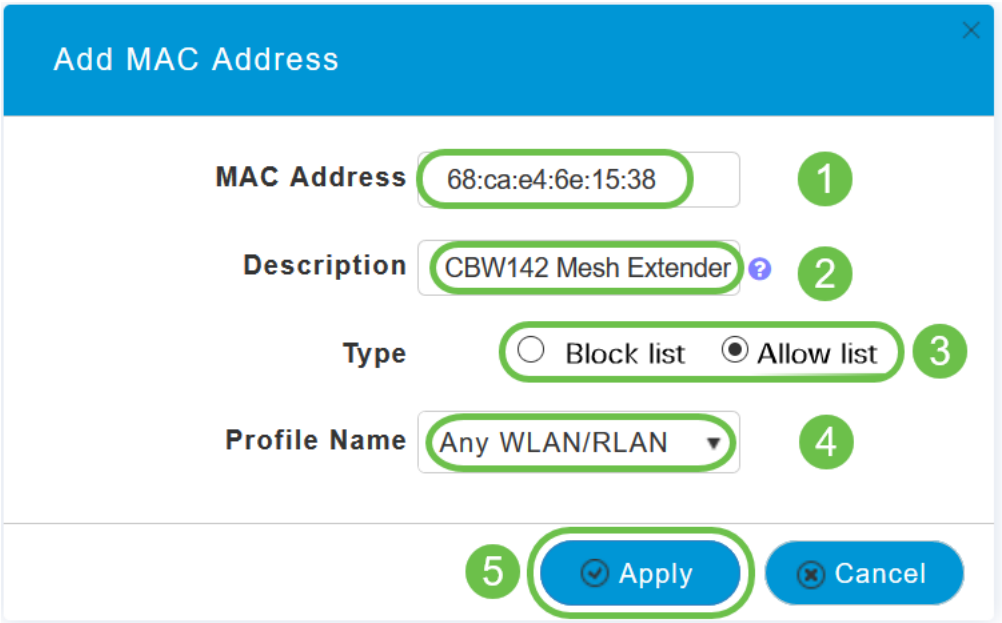
Etapa 7

Navegue até **Wireless Settings > WLAN Users > Local MAC Addresses**. Clique em **Adicionar endereço MAC**.



Passo 8

Insira o endereço MAC e a descrição do extensor de malha. Selecione a lista *Tipo* como Permitir. Selecione o *nome do perfil* no menu suspenso. Clique em Apply.



Passo 9

Certifique-se de salvar todas as configurações pressionando o **ícone salvar** no painel superior direito da tela.

Repita para cada extensor de malha.

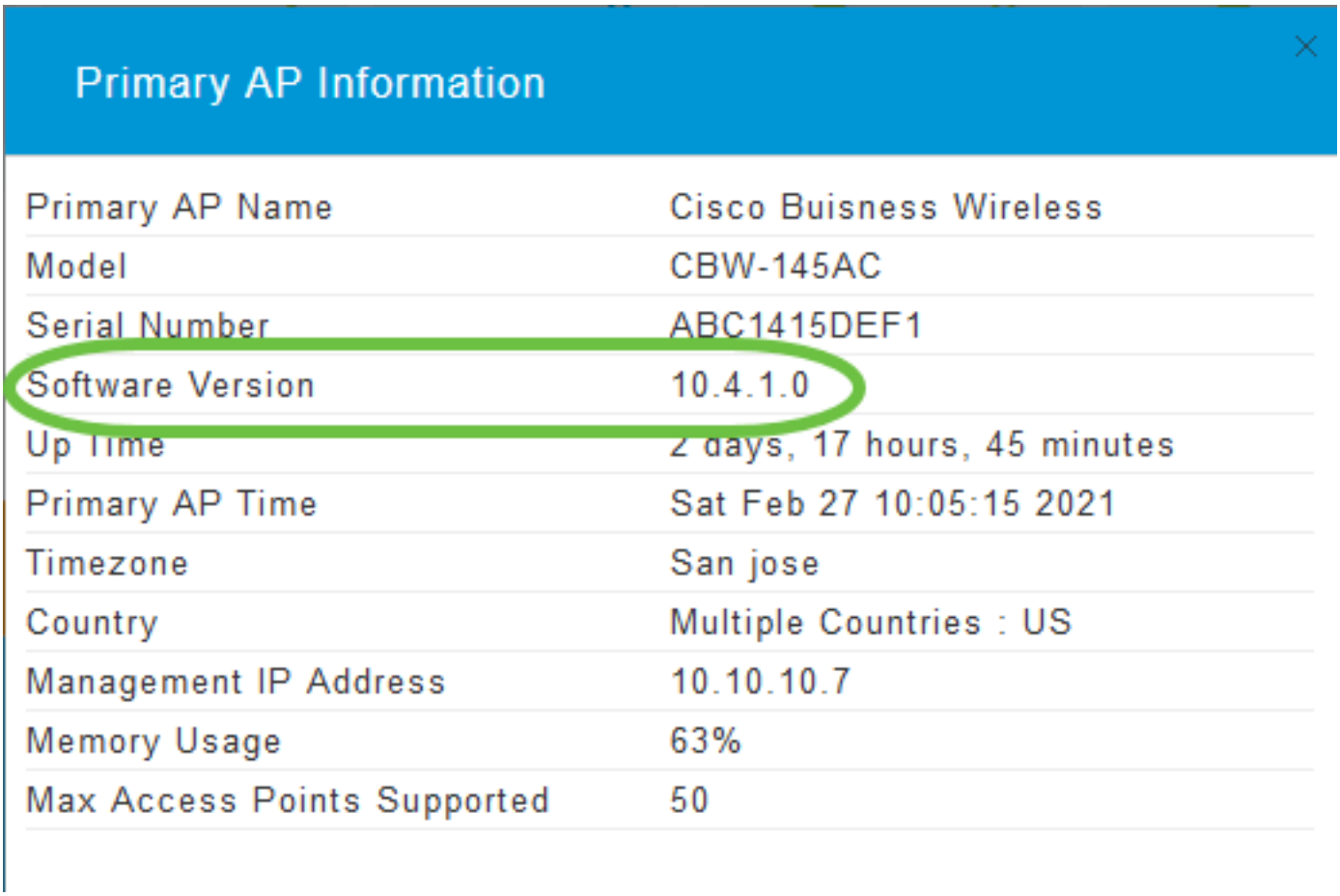
Verificar e atualizar o software usando a interface de usuário da Web

Não ignore esta etapa importante! Há algumas maneiras de atualizar o software, mas as etapas listadas abaixo são recomendadas como as mais fáceis de executar quando você usa a IU da Web.

Para exibir e atualizar a versão atual do software do seu AP primário, execute as seguintes etapas.

Passo 1

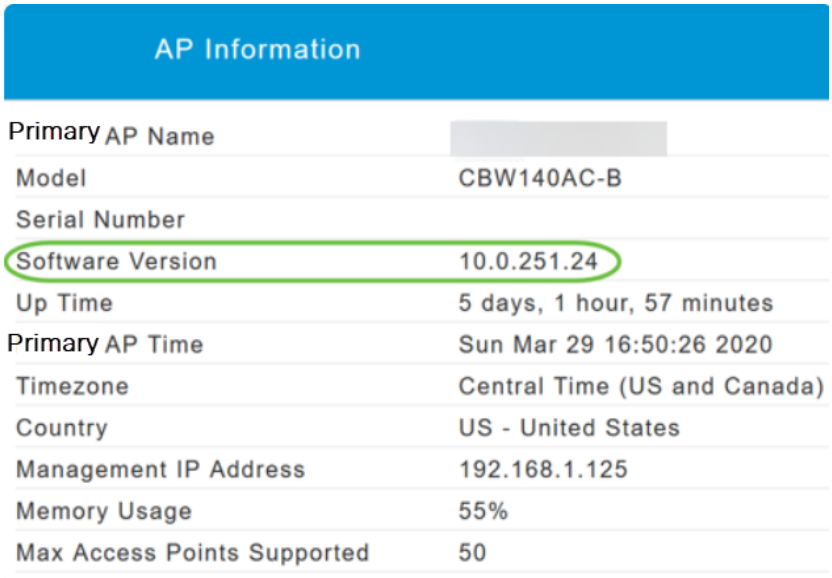
Clique no **ícone da engrenagem** no canto superior direito da interface da Web e clique em **Primary AP Information (Informações principais do AP)**.



Passo 2

Compare a versão que está sendo executada com a versão de software mais recente.

Feche a janela quando souber se precisa atualizar o software.

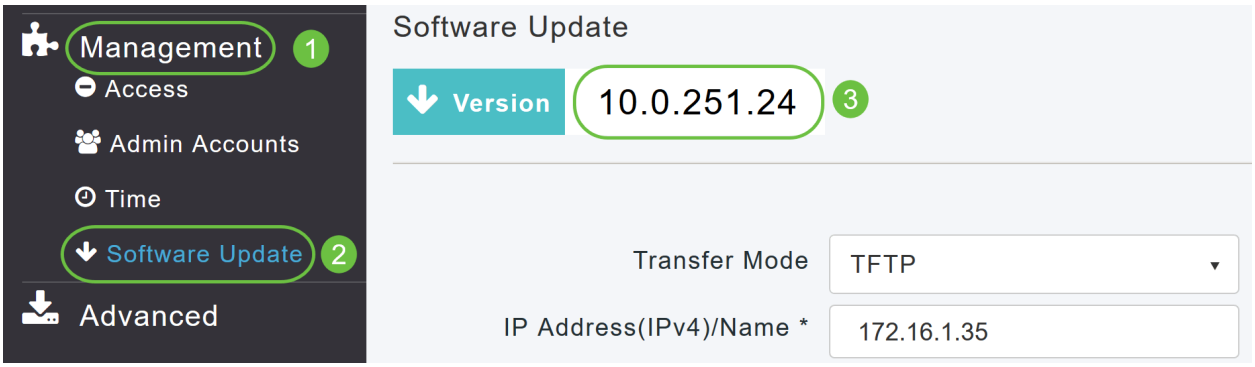


Se estiver executando a versão mais recente do software, você poderá ir para a seção Criar WLANs.

Etapa 3

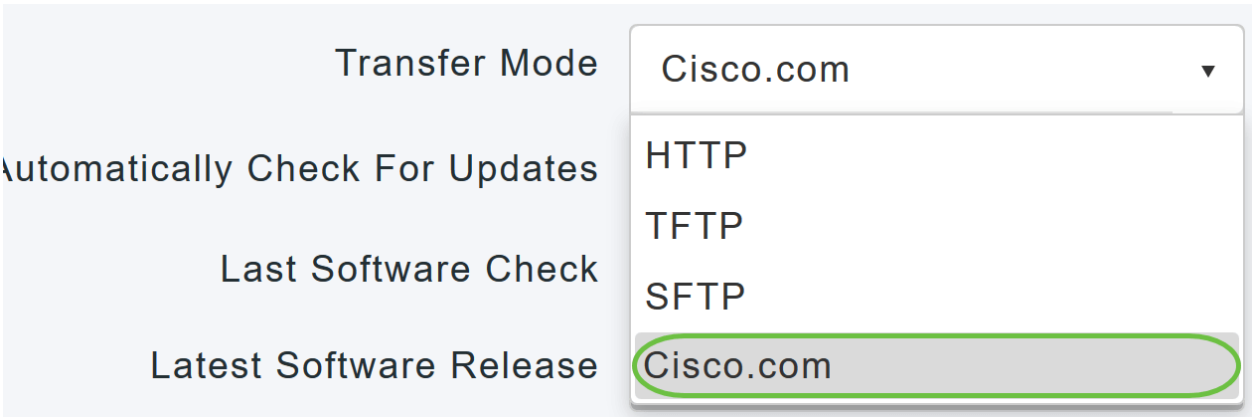
Escolha **Management > Software Update** no menu.

A janela *Software Update* é exibida com o número de versão do software atual listado na parte superior.



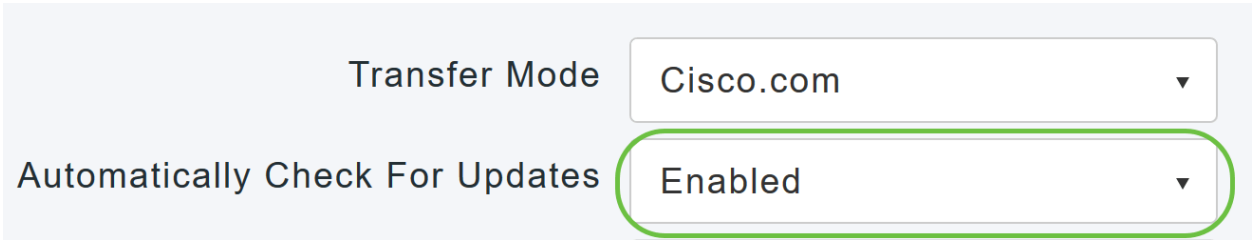
Você pode atualizar o software de AP CBW e as configurações atuais no AP primário não serão excluídas.

Na lista suspensa *Modo de transferência*, escolha **Cisco.com**.



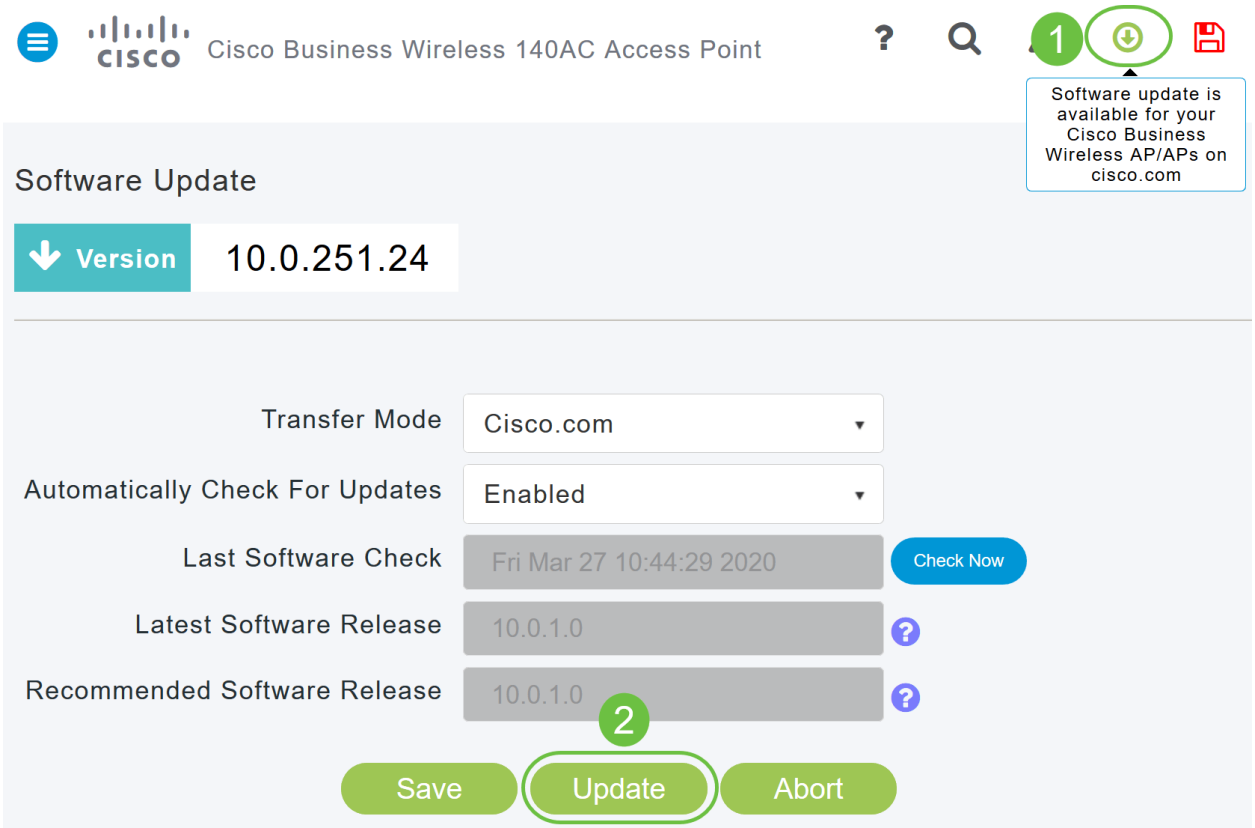
Passo 4

Para definir o AP primário para verificar automaticamente as atualizações de software, escolha **Enabled (Habilitado)** na lista suspensa *Automatically Check for Updates (Verificar automaticamente as atualizações)*. Iss está habilitado por padrão.



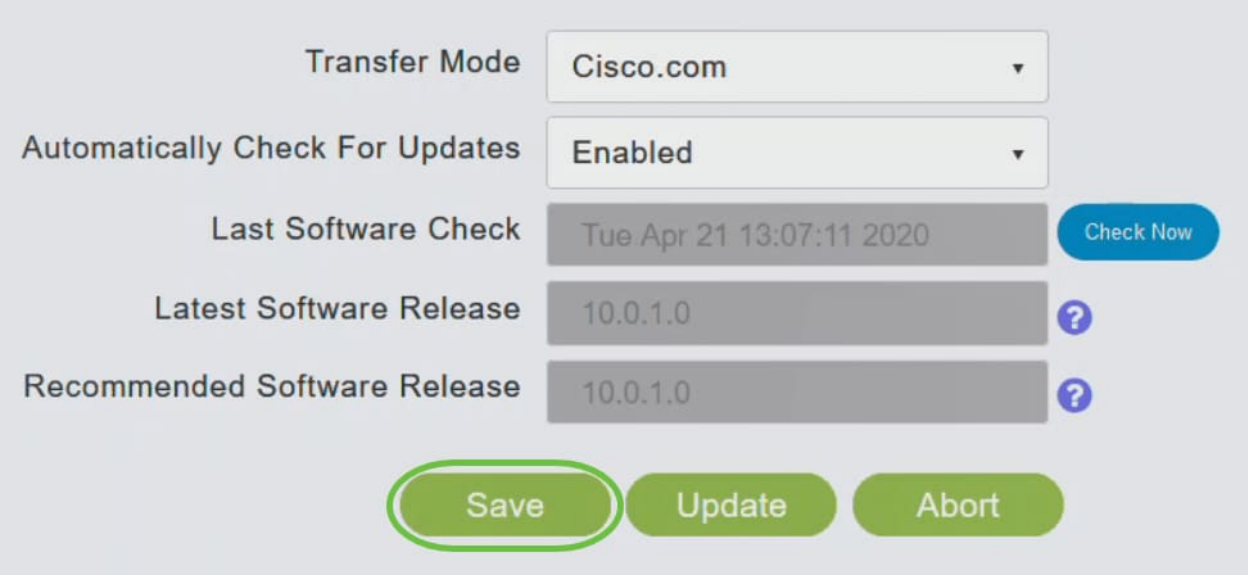
Quando uma verificação de software é feita e se uma atualização de software mais recente ou recomendada está disponível no Cisco.com, então:

- O **ícone de alerta de atualização de software** no canto superior direito da IU da Web estará verde (ou cinza). Clicar no ícone o levará à página Atualização de software.
- O botão Update (Atualizar) na parte inferior da página *Software Update (Atualização de software)* está ativado.

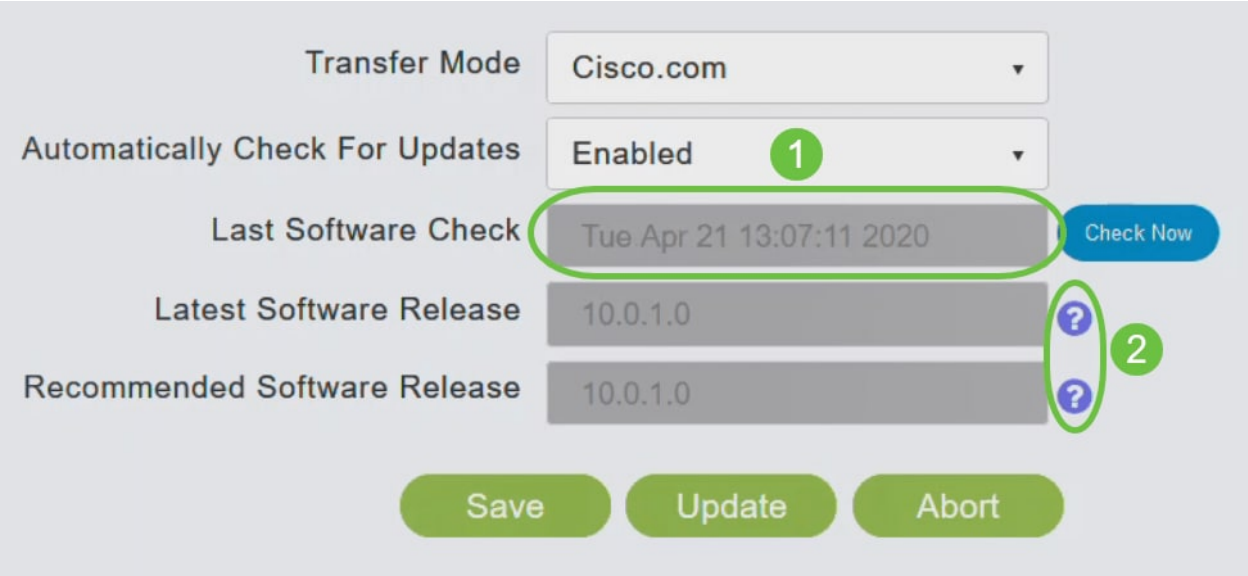


Etapa 5

Click Save. Isso salva as entradas ou alterações feitas em ambos os *modos de transferência* e *verifica automaticamente se há atualizações*.

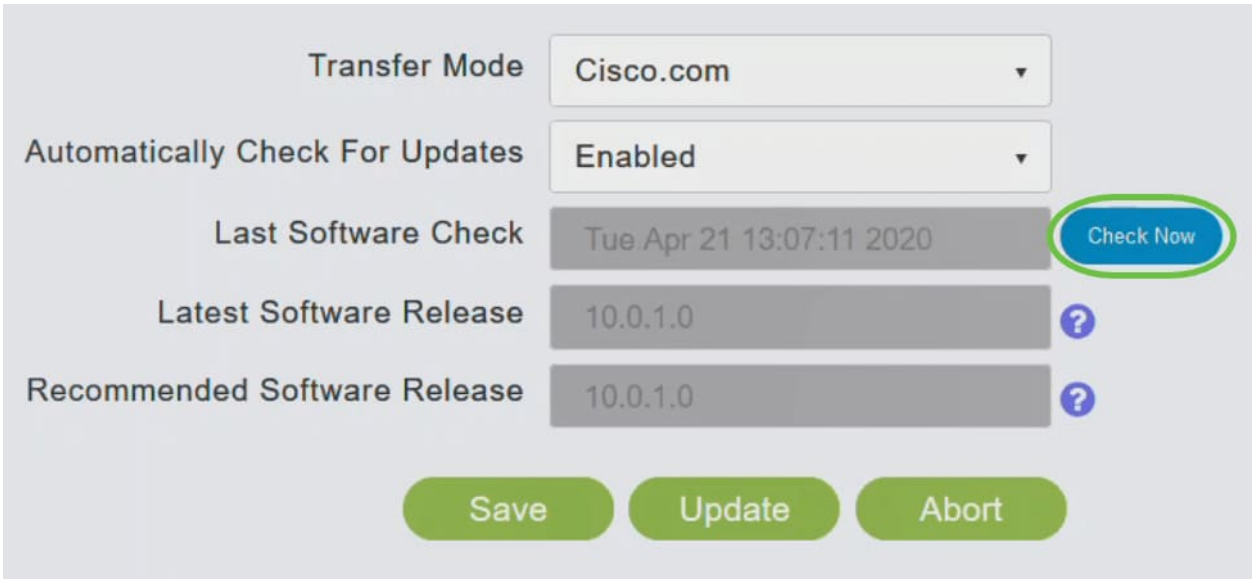


O campo *Última verificação de software* exibe o carimbo de data e hora da última verificação automática ou manual de software. Você pode ver as notas das versões exibidas clicando no **ícone de ponto de interrogação** ao lado.



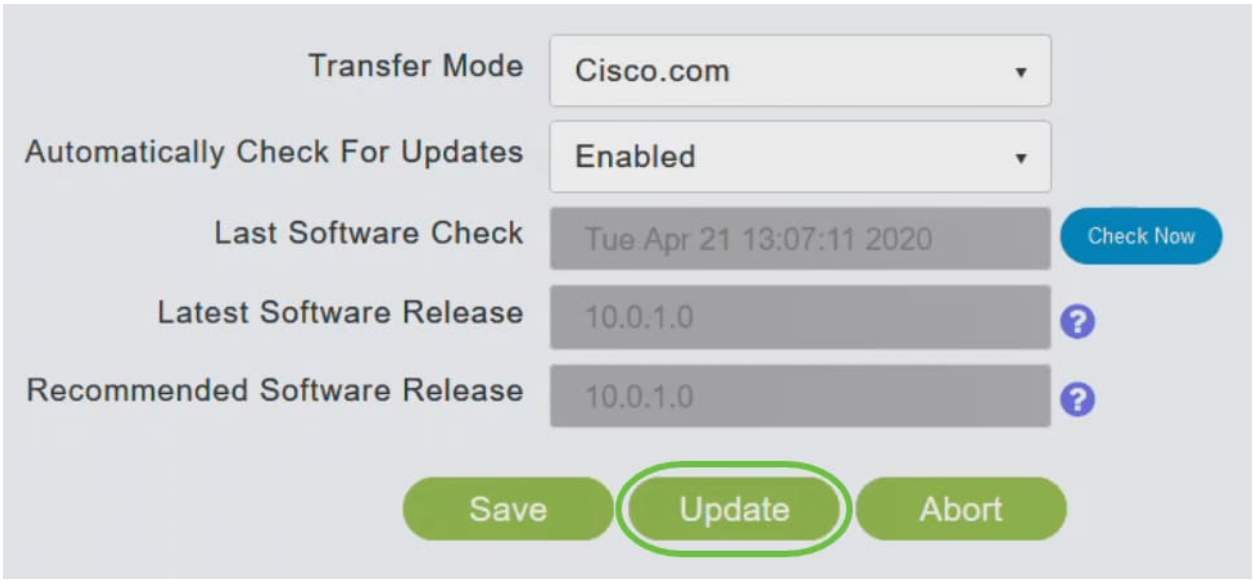
Etapa 6

Você pode executar manualmente uma verificação de software a qualquer momento clicando em *Verificar agora*.



Etapa 7

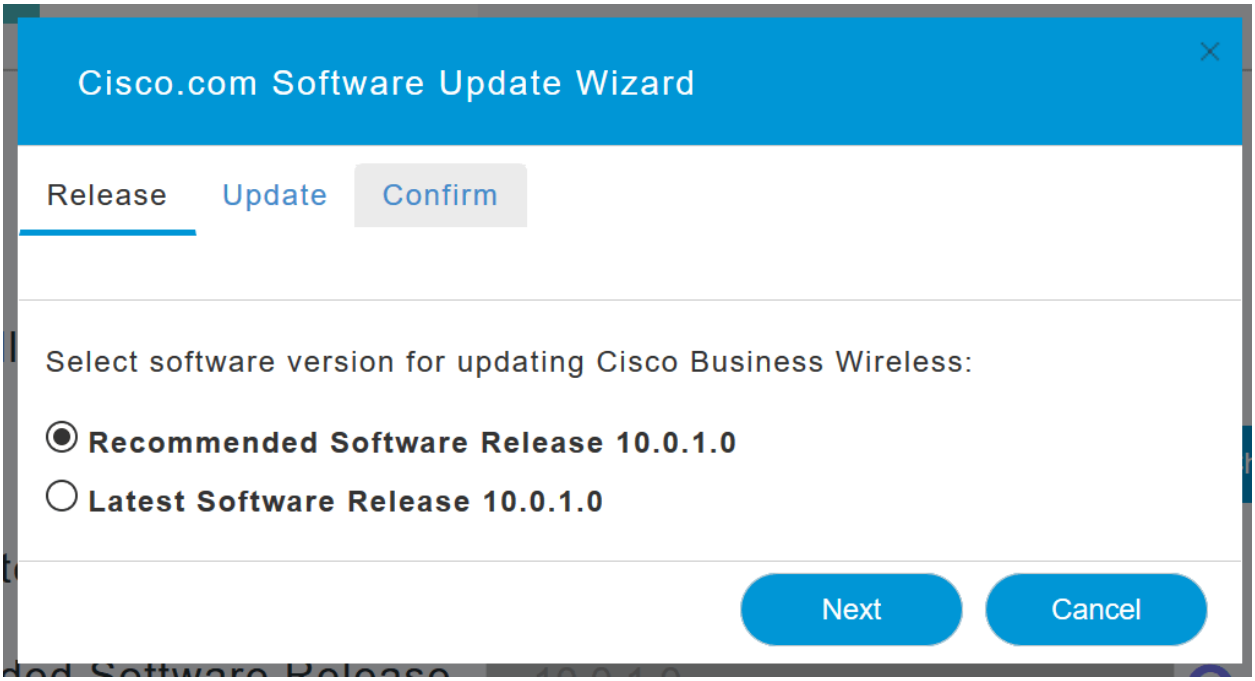
Para continuar com a atualização do software, clique em **Atualizar**.



O *Assistente de atualização de software* é exibido. O assistente exibe as três guias a seguir em sequência:

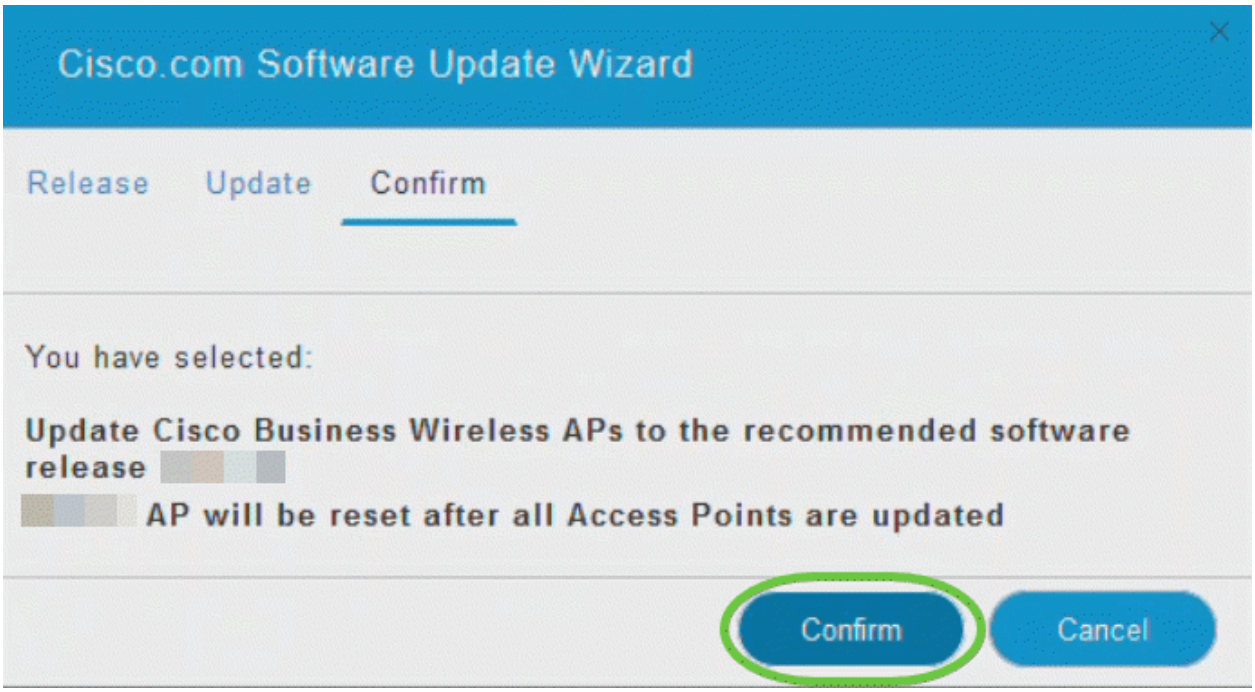
- Guia Versão - Especifique se deseja atualizar para a versão de software recomendada ou para a versão de software mais recente.
- Guia Atualizar - Especifique quando os APs devem ser redefinidos. Você pode optar por fazê-lo imediatamente ou agendá-lo para um horário posterior. Para configurar o AP primário para reinicializar automaticamente após a conclusão do pré-download da imagem, marque a caixa de seleção Reiniciar automaticamente.
- Confirmar guia - Confirme suas seleções.

Siga as instruções do assistente. Você pode voltar para qualquer guia a qualquer momento antes de clicar em *Confirmar*.



Passo 8

Clique em **Confirmar**.

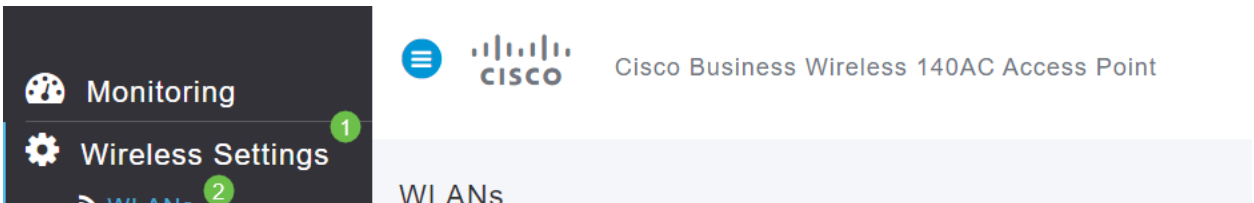


Criar WLANs na IU da Web

Esta seção permite criar redes locais sem fio (WLANs).

Passo 1

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



Passo 2

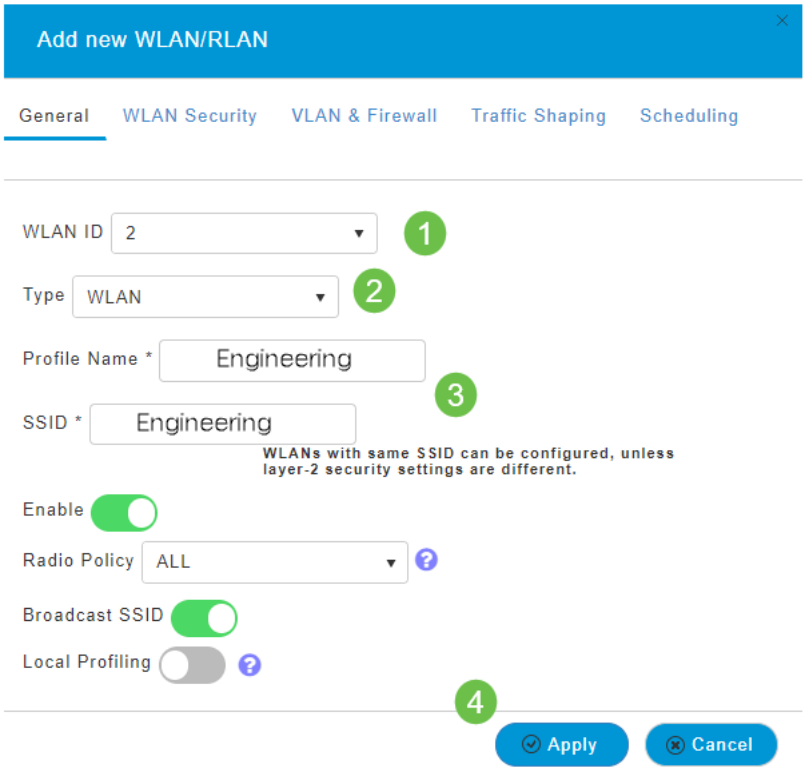
Na guia *Geral*, insira as seguintes informações:

- ID da WLAN - Selecione um número para a WLAN
- Tipo - Selecionar **WLAN**
- Nome do perfil - Ao inserir um nome, o SSID será preenchido automaticamente com o mesmo nome. O nome deve ser exclusivo e não deve exceder 31 caracteres.

Os campos a seguir foram deixados como padrão neste exemplo, mas as explicações são listadas caso você queira configurá-los de forma diferente.

- SSID - O nome do perfil também atua como SSID. Você pode alterar isso se desejar. O nome deve ser exclusivo e não deve exceder 31 caracteres.
- Habilitar - Deve ser deixado habilitado para que a WLAN funcione.
- Política de rádio - Normalmente, você gostaria de deixar isso como **tudo** para que os clientes de 2,4 GHz e 5 GHz possam acessar a rede.
- SSID de transmissão - normalmente, você deseja que o SSID seja descoberto, portanto, deixe-o como Ativado.
- Criação de perfil local - Deseja habilitar essa opção apenas para exibir o sistema operacional que está sendo executado no cliente ou para ver o nome do usuário.

Clique em Apply.



Etapa 3

Você será direcionado para a guia *WLAN Security*.

Neste exemplo, as seguintes opções foram deixadas como padrão:

- A rede do convidado, o Captive Network Assistant e a filtragem de MAC foram deixados desabilitados. Os detalhes da configuração de uma rede de convidado estão detalhados na próxima seção.
- WPA2 Personal - Wi-Fi Protected Access 2 com PSK (Pre-shared Key, Formato de senha de chave pré-compartilhada) - ASCII. Esta opção significa Wi-Fi Protected Access 2 com chave pré-compartilhada (PSK).

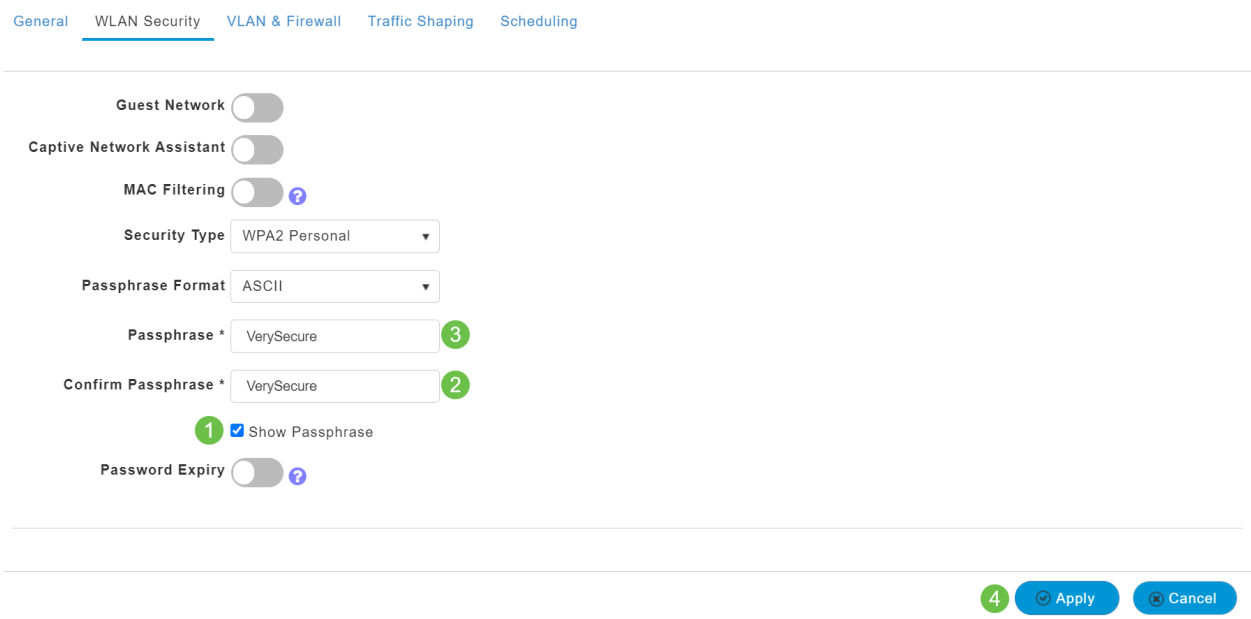
WPA2 Personal é um método usado para proteger sua rede com o uso de uma autenticação PSK. A PSK é configurada separadamente no AP primário, na política de segurança da WLAN e no cliente. A WPA2 Personal não depende de um servidor de autenticação na sua rede.

- Formato de Senha - **ASCII é deixado como padrão.**

Os seguintes campos foram inseridos neste cenário:

- Show Passphrase - (Mostrar senha) clique na caixa de seleção para ver a senha inserida.
- Passphrase - (Senha) Insira um nome para a senha (senha).
- Confirmar senha - Insira a senha novamente para confirmá-la.

Clique em Apply. Isso ativará automaticamente a nova WLAN.

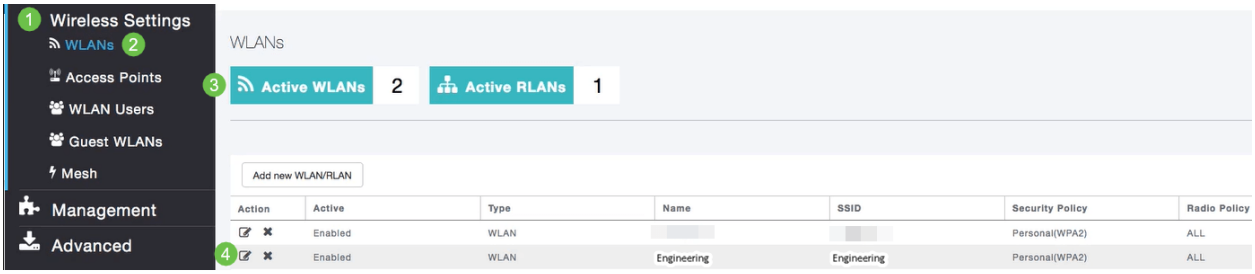


Passo 4

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

Etapa 5

Para ver a WLAN que você criou, selecione **Wireless Settings > WLANs**. Você verá o número de WLANs ativas elevado a 2 e a nova WLAN será exibida.



Repita essas etapas para outras WLANs que você deseja criar.

Configurações sem fio opcionais

Agora você tem todas as configurações básicas definidas e estão prontas para serem implementadas. Você tem algumas opções, então sinta-se à vontade para ir para qualquer uma das seguintes seções:

- Crie uma WLAN de Convidado usando a IU da Web (Opcional)
- Criação de perfis de aplicativos (opcional)
- Criação de perfis de clientes (opcional)
- Estou pronto para concluir isso e começar a usar minha rede!

Crie uma WLAN de Convidado usando a IU da Web (Opcional)

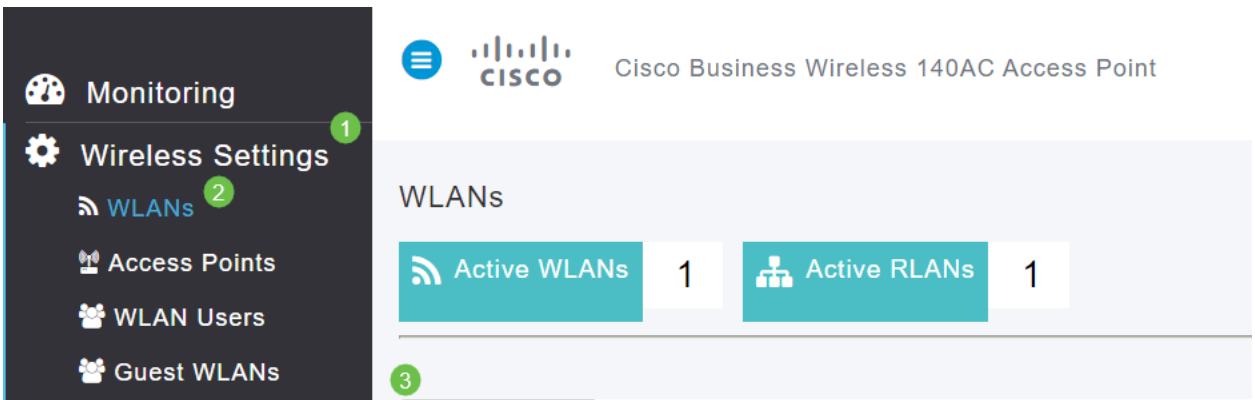
Uma WLAN de convidado fornece acesso de convidado à sua rede Cisco Business Wireless.

Passo 1

Efetue login na IU da Web do AP primário. Abra um navegador da Web e digite www.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.

Passo 2

Uma rede local sem fio (WLAN) pode ser criada navegando para **Wireless Settings > WLANs**. Em seguida, selecione **Add new WLAN/RLAN**.



Etapa 3

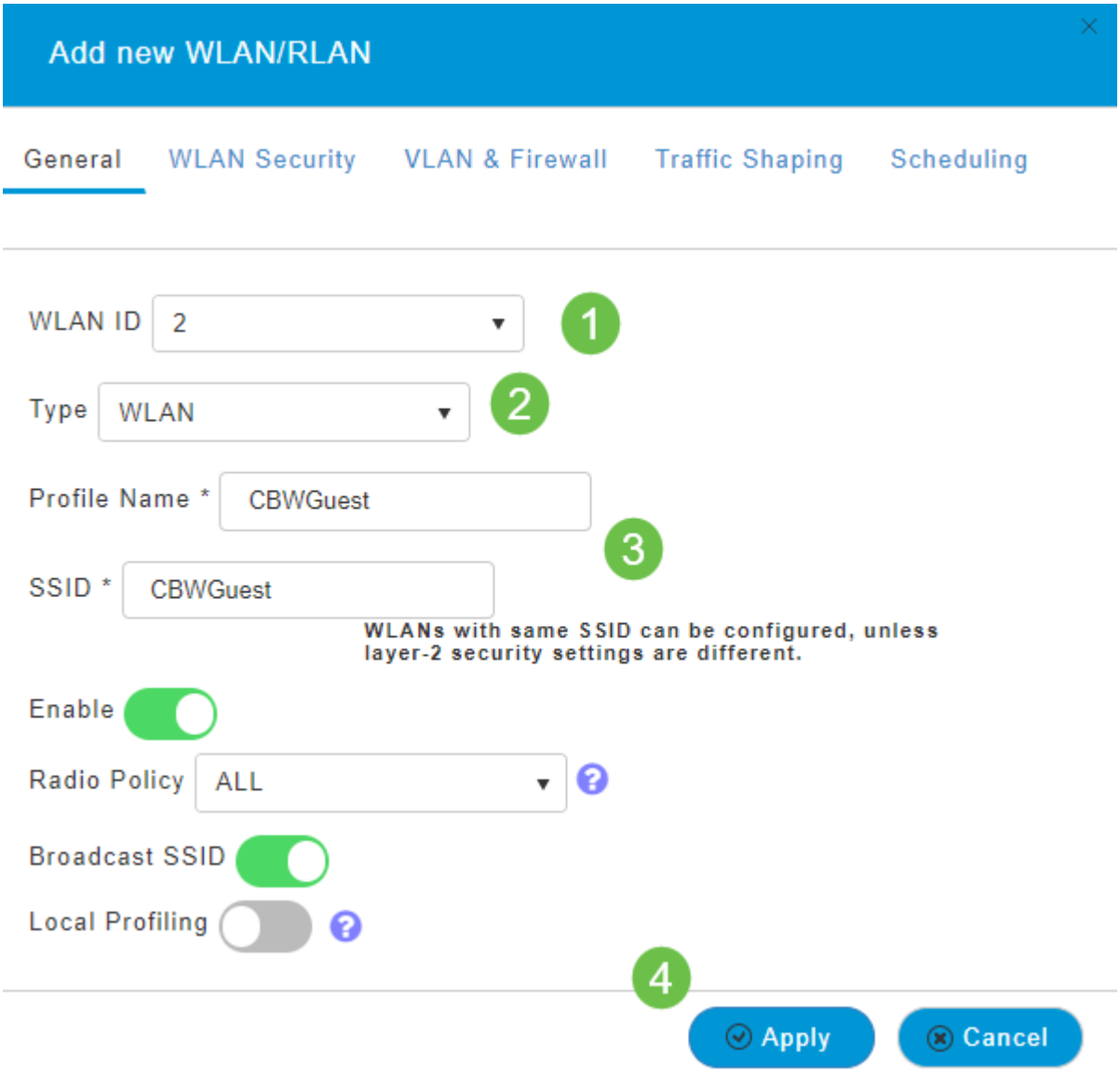
Na guia *Geral*, insira as seguintes informações:

WLAN ID - Selecione um número para a WLAN
Tipo - Selecionar **WLAN**
Nome do perfil - Quando você digita um nome, o SSID será preenchido automaticamente com o mesmo nome. O nome deve ser exclusivo e não deve exceder 31 caracteres.

Os campos a seguir foram deixados como padrão neste exemplo, mas as explicações são listadas caso você queira configurá-los de forma diferente.

SSID - O nome do perfil também atua como SSID. Você pode alterar isso se desejar. O nome deve ser exclusivo e não deve exceder 31 caracteres.
Habilitar - Deve ser deixado habilitado para que a WLAN funcione.
Política de rádio - Normalmente, você gostaria de deixar isso como **tudo** para que os clientes de 2,4 GHz e 5 GHz possam acessar a rede.
SSID de transmissão - Normalmente, você deseja que o SSID seja descoberto, portanto, deixe-o como Ativado.
Criação de perfil local - Só pretende ativar esta opção para ver o sistema operacional que está a ser executado no cliente ou para ver o nome de utilizador.

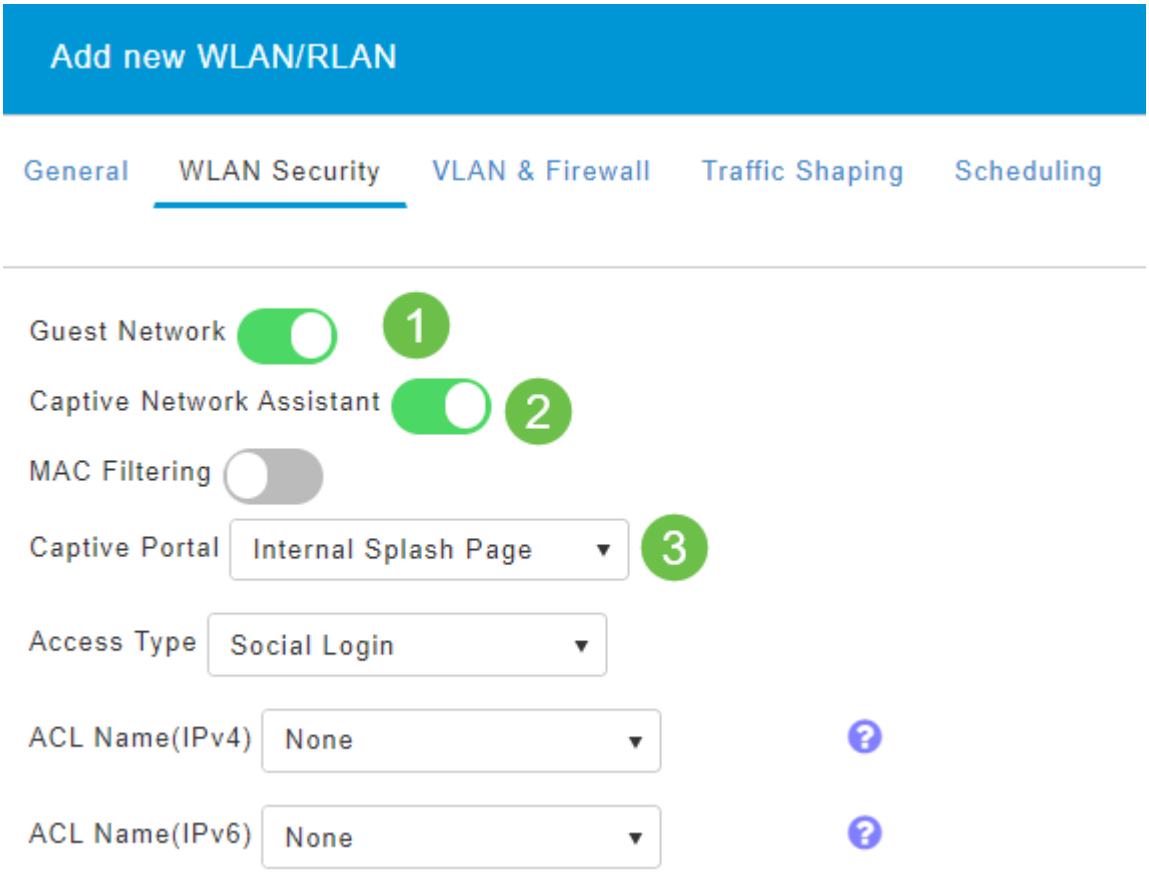
Clique em Apply.



Passo 4

Você será direcionado para a guia *WLAN Security*. Neste exemplo, as seguintes opções foram selecionadas.

- Rede de convidado - Habilitar
- Captive Network Assistant - Se você usa o Mac ou o IOS, provavelmente deseja habilitá-lo. Este recurso detecta a presença de um portal cativo enviando uma solicitação da Web ao conectar-se a uma rede sem fio. Esta solicitação é direcionada a um URL (Uniform Resource Locator) para modelos de iPhone e, se uma resposta for recebida, o acesso à Internet é considerado disponível e nenhuma outra interação é necessária. Se nenhuma resposta for recebida, o acesso à Internet será bloqueado pelo portal cativo e o Captive Network Assistant (CNA) da Apple iniciará automaticamente o pseudo-navegador para solicitar o login do portal em uma janela controlada. O CNA pode quebrar ao redirecionar para um portal cativo do Identity Services Engine (ISE). O AP primário impede que este pseudo-navegador apareça.
- Portal cativo - Esse campo fica visível somente quando a opção Rede de convidado está ativada. Isso é usado para especificar o tipo de portal da Web que pode ser usado para fins de autenticação. Selecione Página inicial interna para usar a autenticação padrão baseada no portal da Web da Cisco. Escolha External Splash Page se você tiver autenticação de portal cativo, usando um servidor Web fora da sua rede. Além disso, especifique a URL do servidor no campo URL do site.



Neste exemplo, a WLAN de convidado com um tipo de acesso de login social habilitado será criada. Quando o usuário se conectar a esta WLAN de convidado, ela será redirecionada para a página de login padrão da Cisco, onde poderá encontrar os botões de login do Google e do Facebook. O usuário pode fazer login usando sua conta Google ou Facebook para obter acesso à Internet.

Etapa 5

Nessa mesma guia, selecione um *Tipo de acesso* no menu suspenso. Neste exemplo, *Login Social* foi selecionado. Essa é a opção que permite que os convidados usem suas credenciais do Google ou Facebook para autenticar e obter acesso à rede.

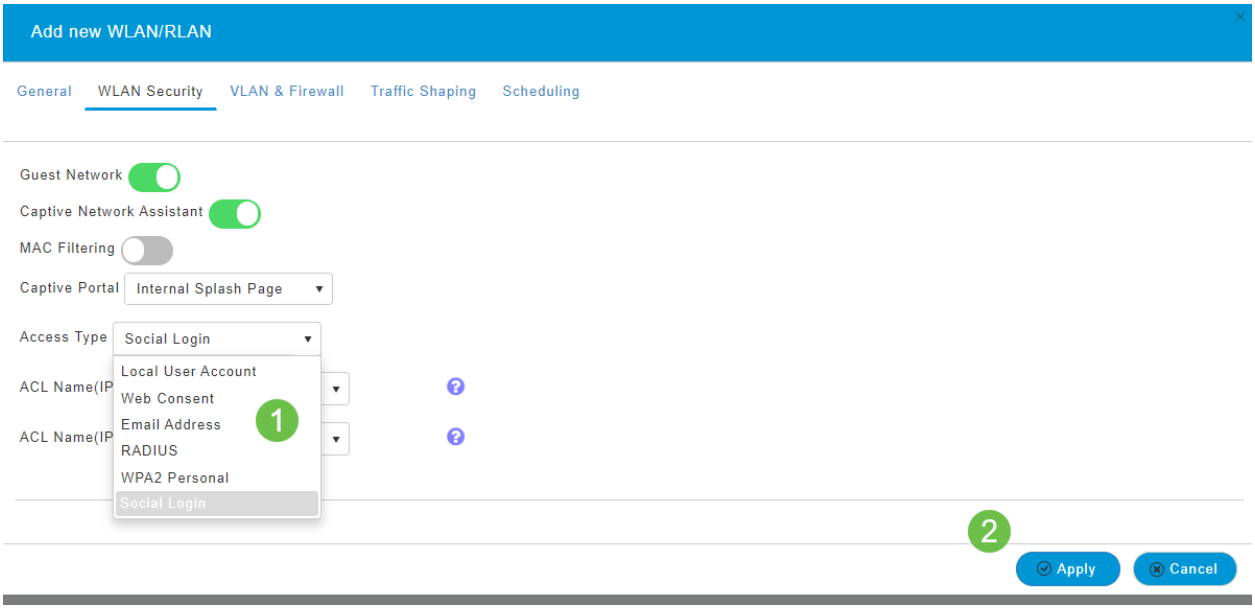
Outras opções para *Tipo de acesso* incluem:

Conta de usuário local - A opção padrão. Escolha esta opção para autenticar convidados usando o nome de usuário e a senha que você pode especificar para usuários convidados desta WLAN, em **Configurações sem fio > Usuários de WLAN**. Este é um exemplo da página inicial interna padrão.

Você pode personalizar isso navegando para **Wireless Settings > Guest WLANs**. A partir daqui, você pode inserir um *Título da página* e uma *mensagem da página*. Clique em Apply. Clique em **Visualizar**.

Consentimento da Web - Permite que os convidados acessem a WLAN após a aceitação dos termos e condições exibidos. Os usuários convidados podem acessar a WLAN sem digitar um nome de usuário e uma senha.
Endereço de e-mail - Os usuários convidados precisarão inserir seu endereço de e-mail para acessar a rede.
RADIUS - Use isso com um servidor de autenticação externo.
WPA2 Personal - Wi-Fi Protected Access 2 com chave pré-compartilhada (PSK)

Clique em Apply.



Etapa 6

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

Agora, você criou uma rede de convidado disponível em sua rede CBW. Seus convidados vão gostar da conveniência.

Criação de perfil de aplicativo usando a interface de usuário da Web (opcional)

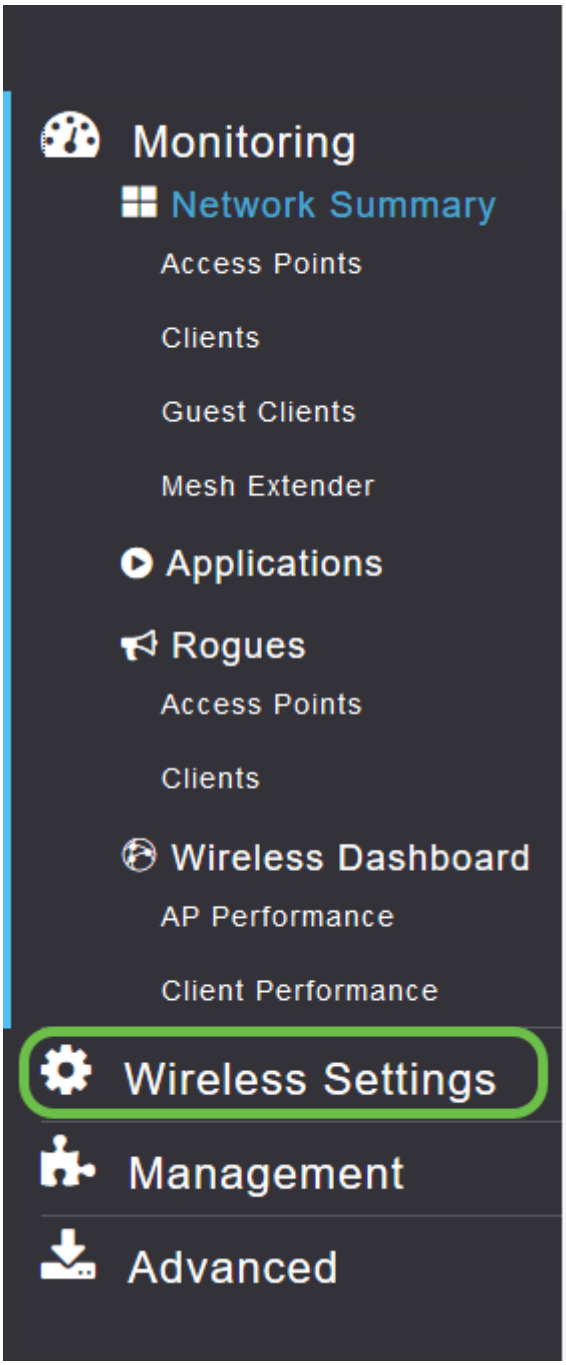
A criação de perfis é um subconjunto de recursos que permite a aplicação de políticas organizacionais. Ele permite que você combine e priorize os tipos de tráfego. Como regras tomam decisões sobre como classificar ou descartar o tráfego. O sistema Cisco Business Mesh Wireless apresenta perfil de cliente e aplicativo. O ato de acessar uma rede como usuário começa com muitas trocas de informações, entre elas o tipo de tráfego. A política interrompe o fluxo de tráfego para direcionar o caminho, como um fluxograma. Outros tipos de recursos de política incluem: acesso de convidado, listas de controle de acesso e QoS.

Passo 1

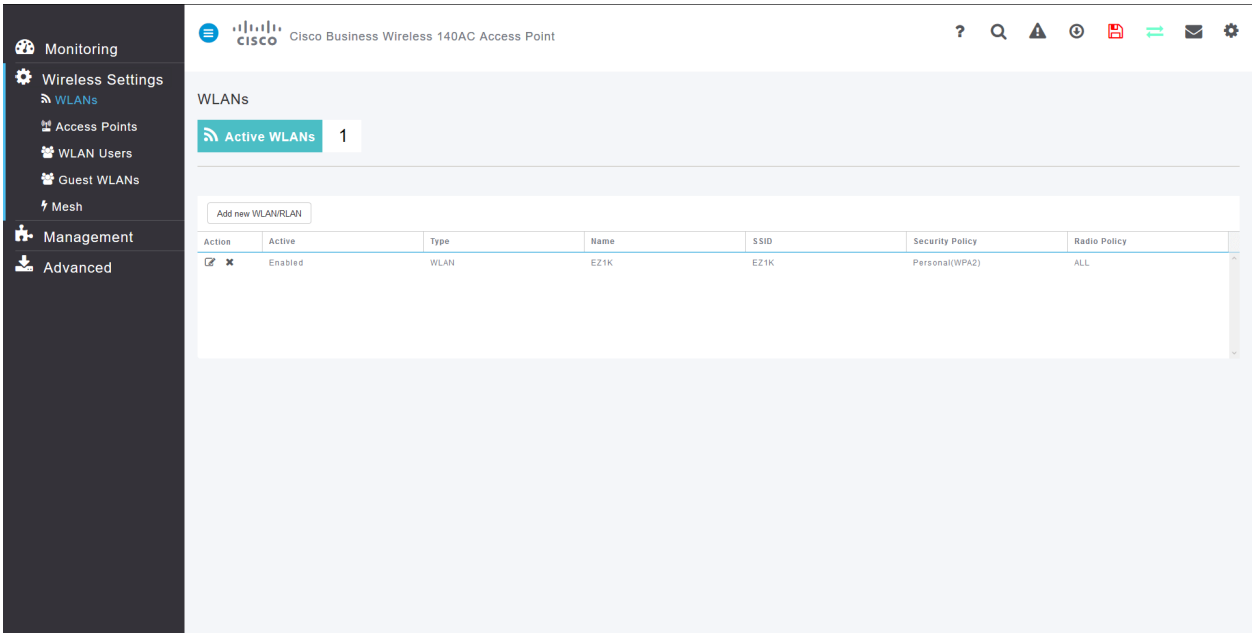
Navegue até o menu no lado esquerdo da tela se não vir a barra de menus à esquerda.

Passo 2

O menu Monitoramento é carregado por padrão ao entrar no dispositivo. Você precisará clicar em **Wireless Settings (Configurações sem fio)**.

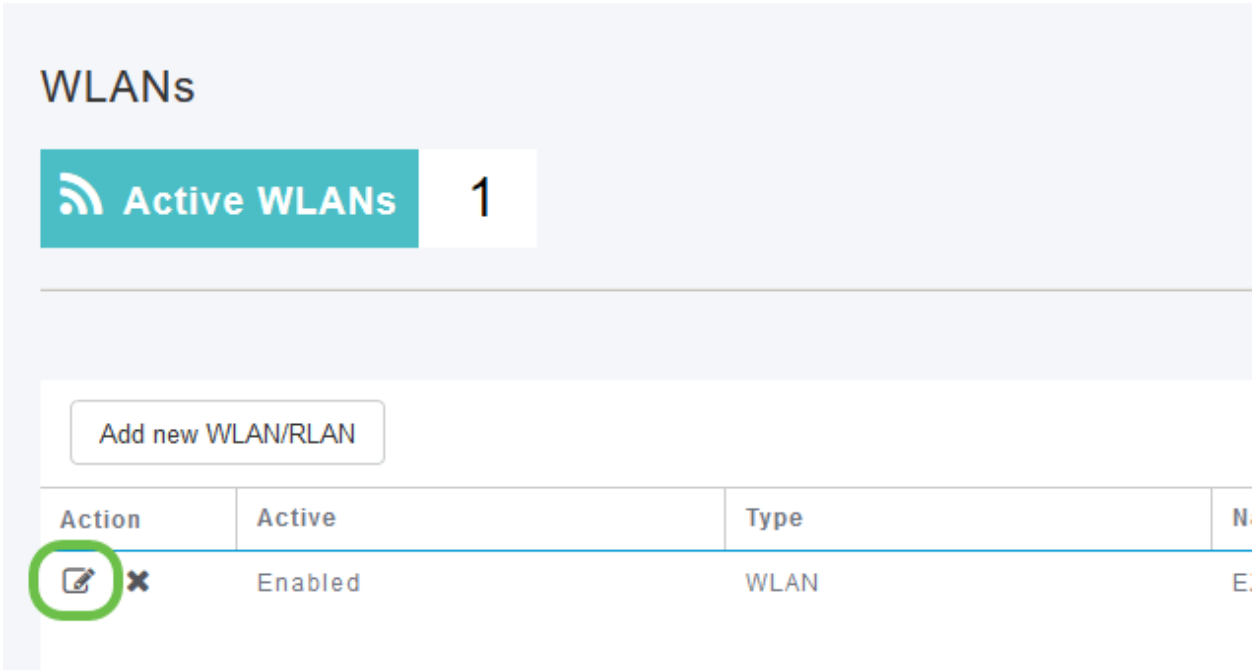


A imagem abaixo é semelhante à exibida quando você clica no link Configurações sem fio.

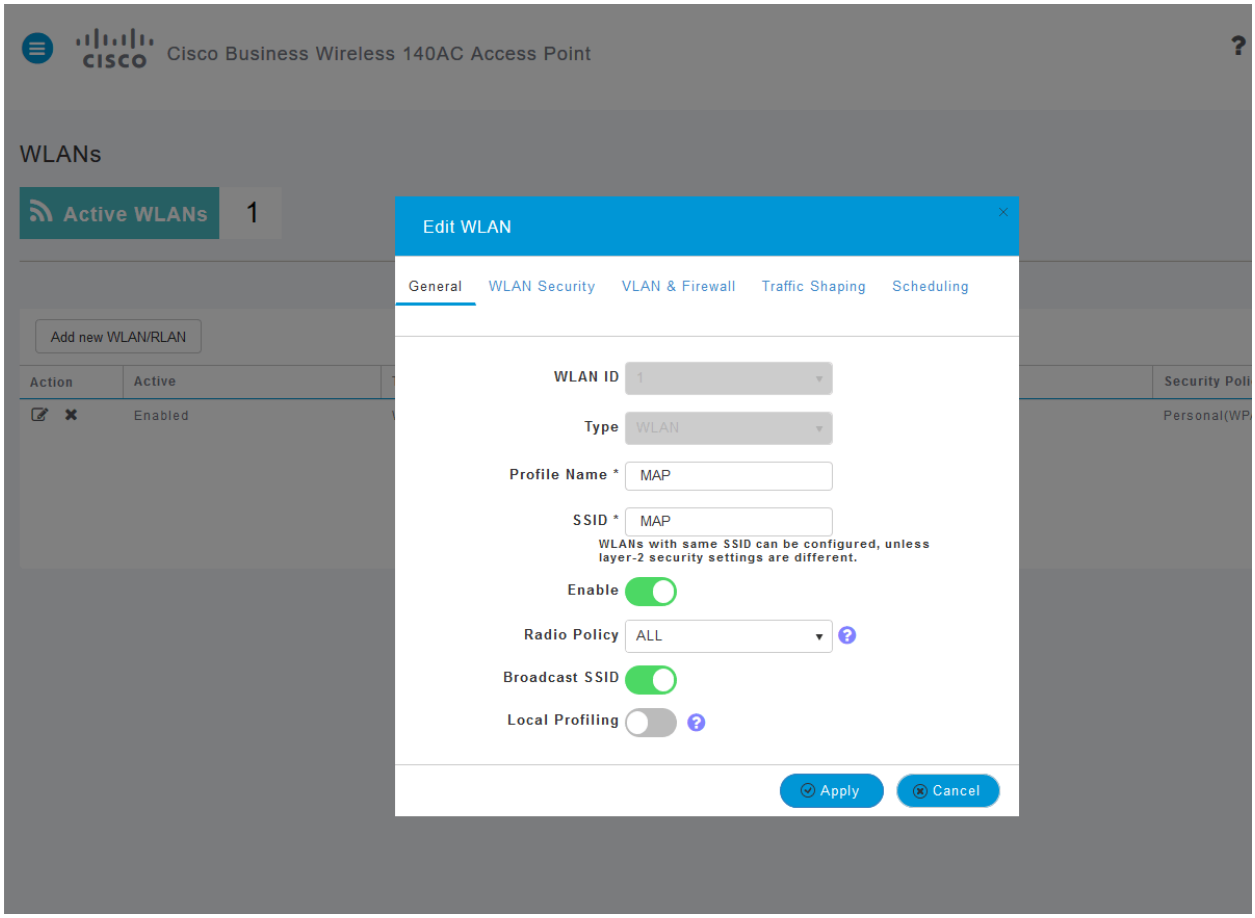


Etapa 3

Clique no **ícone de edição** à esquerda da rede local wireless na qual você deseja habilitar o aplicativo.

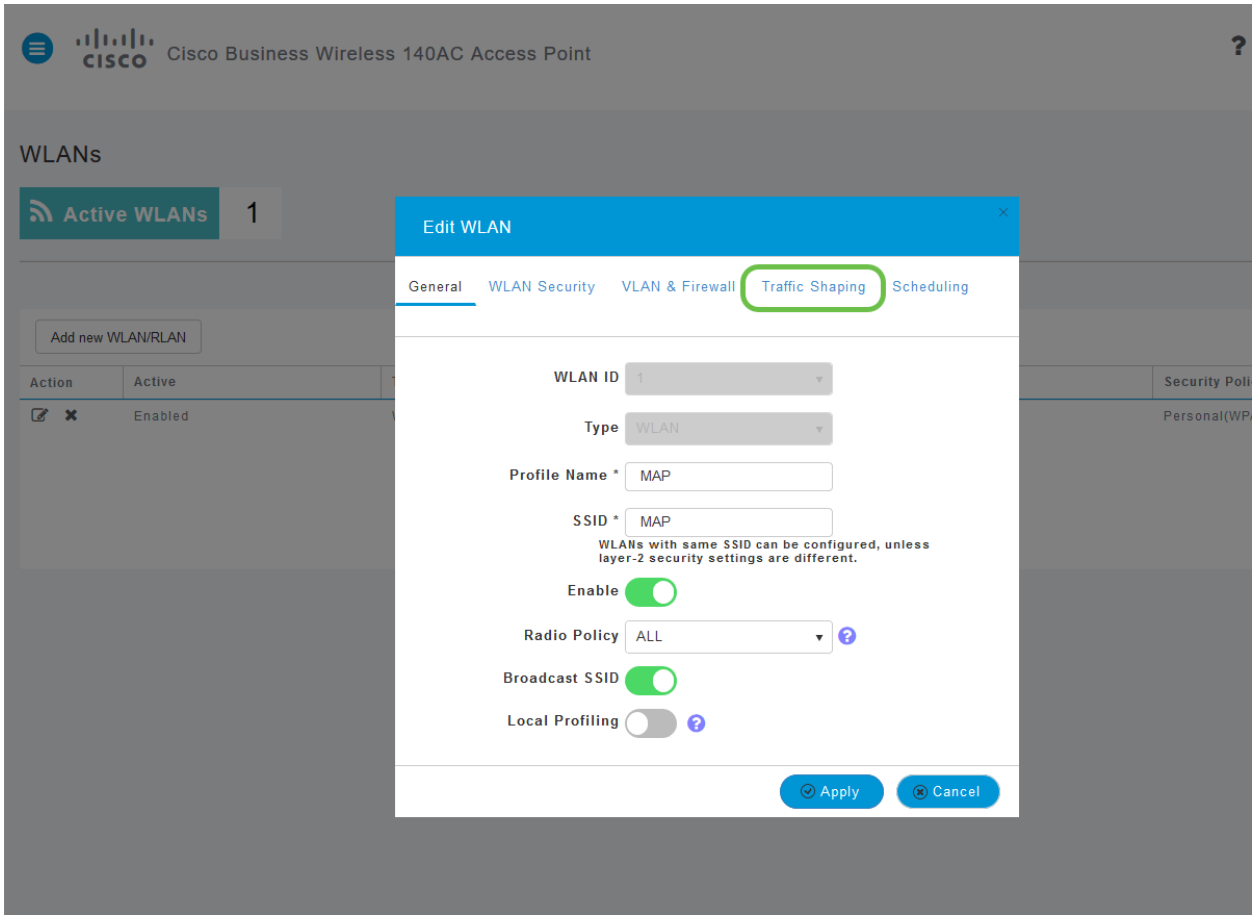


Como você adicionou a WLAN recentemente, sua página *Editar WLAN* pode ser semelhante à seguinte:

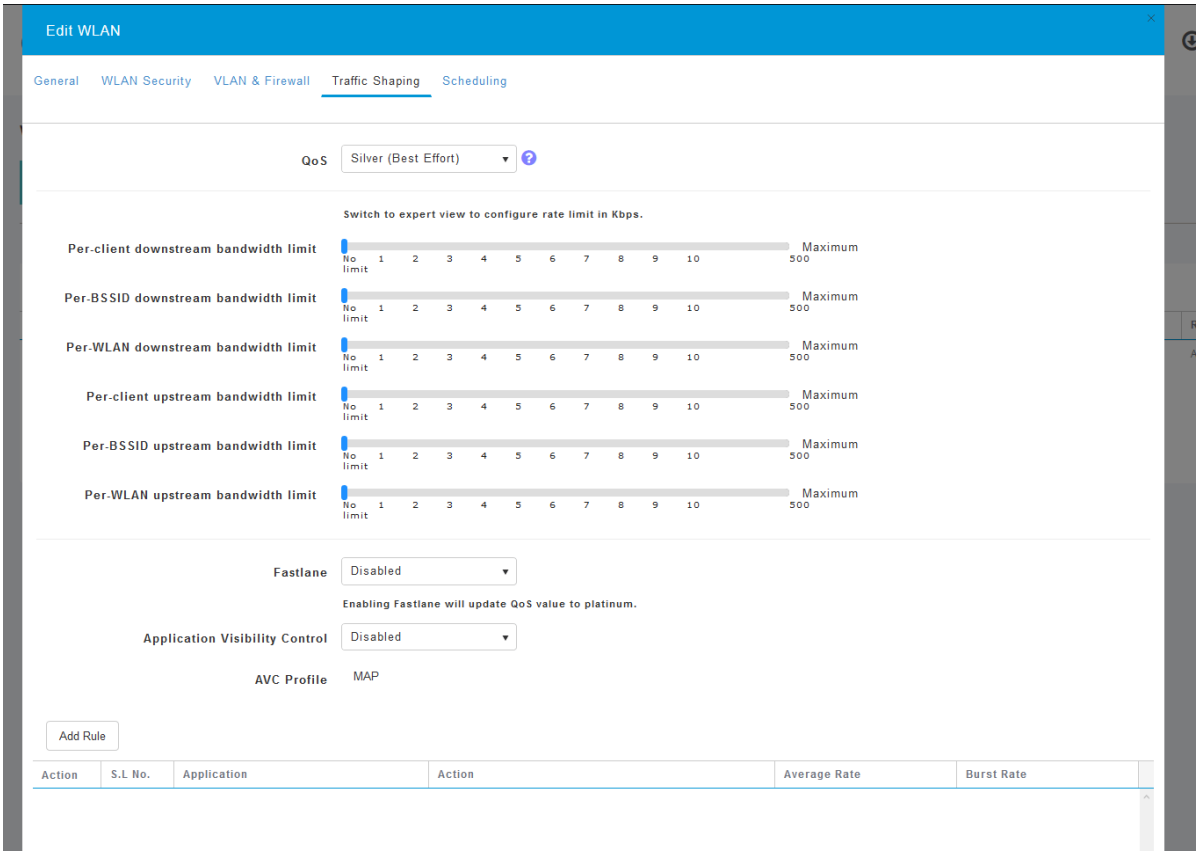


Passo 4

Navegue até a guia **Traffic Shaping (Modelagem de Tráfego)** clicando nela.

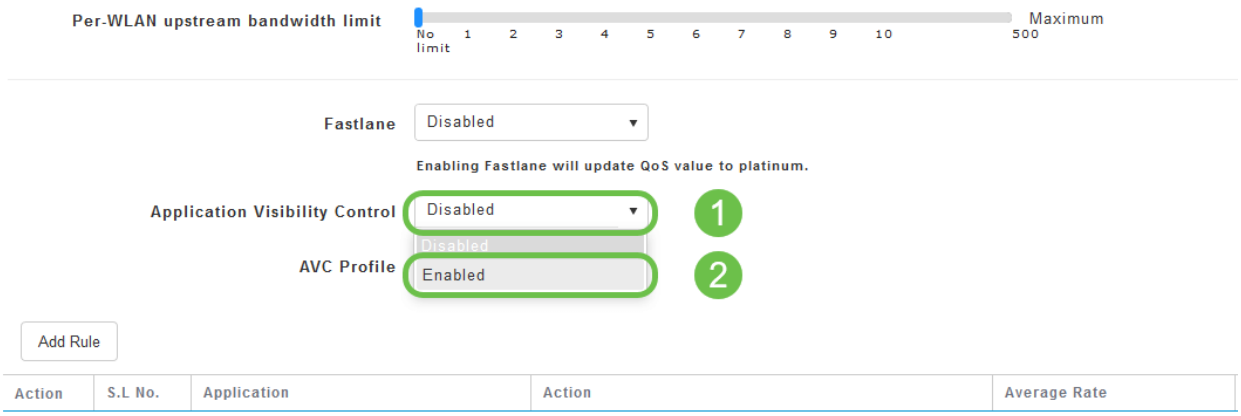


Sua tela pode ser exibida da seguinte maneira:



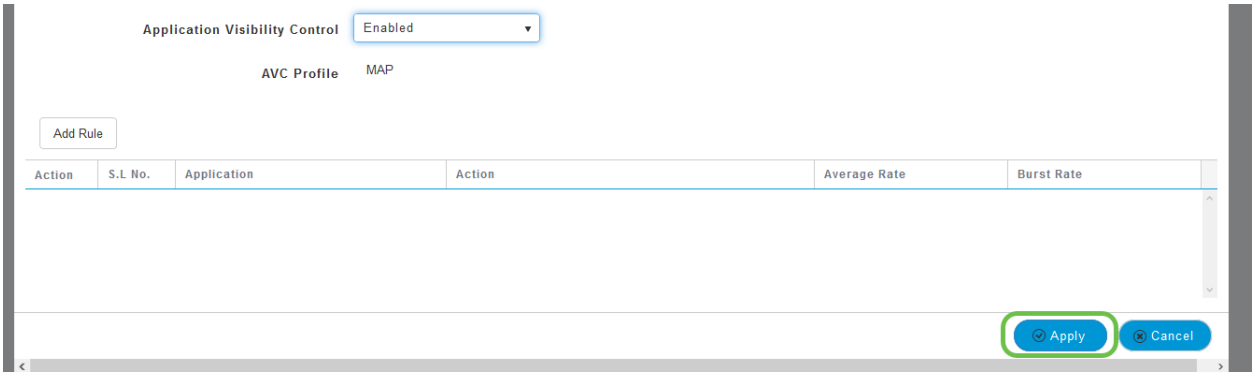
Etapa 5

Na parte inferior da página, você encontrará o recurso *Controle de visibilidade do aplicativo*. Por padrão, isso é desativado. Clique no menu suspenso e selecione **Enabled (Habilitado)**.



Etapa 6

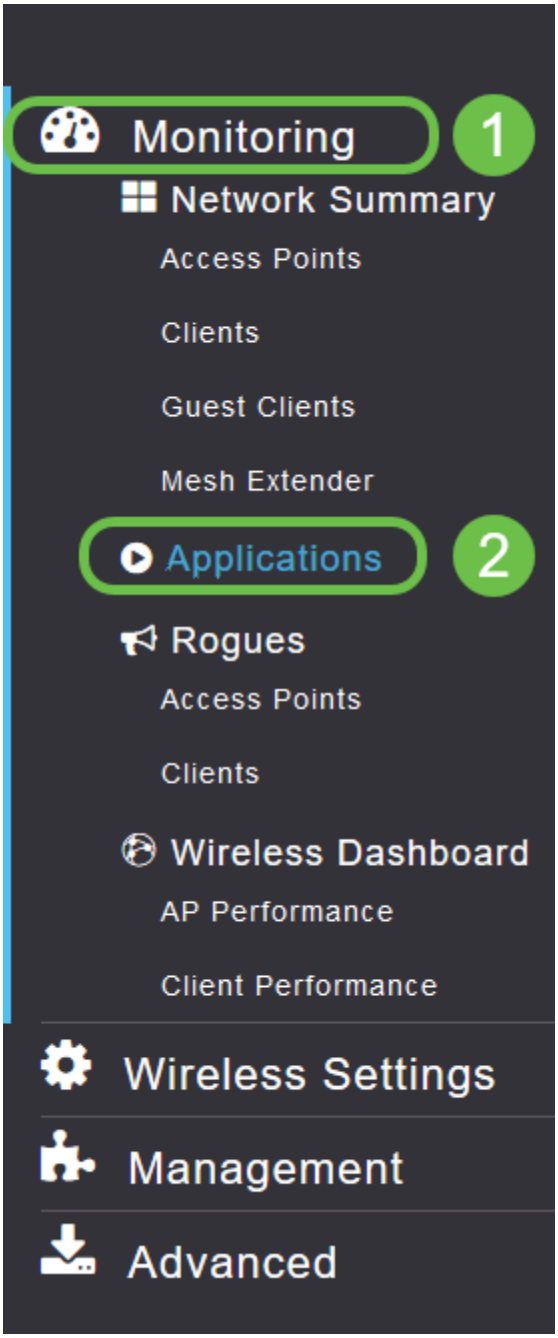
Clique no botão **Aplicar**.



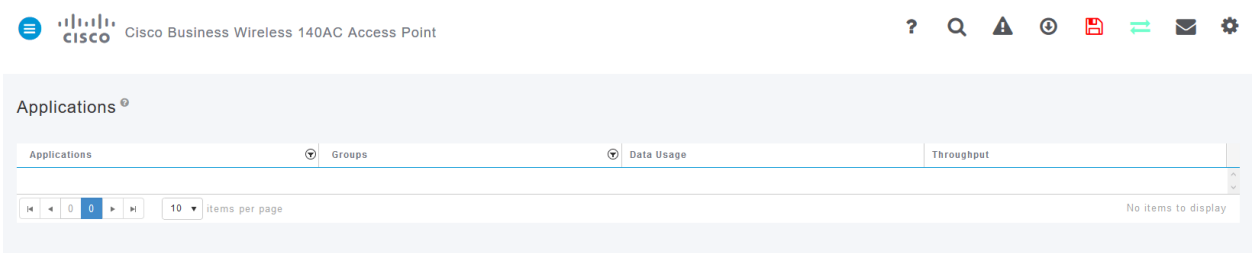
Essa configuração deve ser ativada, caso contrário, o recurso não funcionará.

Etapa 7

Clique no botão Cancelar para fechar o submenu WLAN. Em seguida, clique no menu **Monitoramento** na barra de menus à esquerda. Depois de conseguir, clique no item de menu **Aplicativos**.



Se você não tiver tráfego para nenhuma origem, sua página ficará em branco, como mostrado abaixo.



Esta página exibirá as seguintes informações:

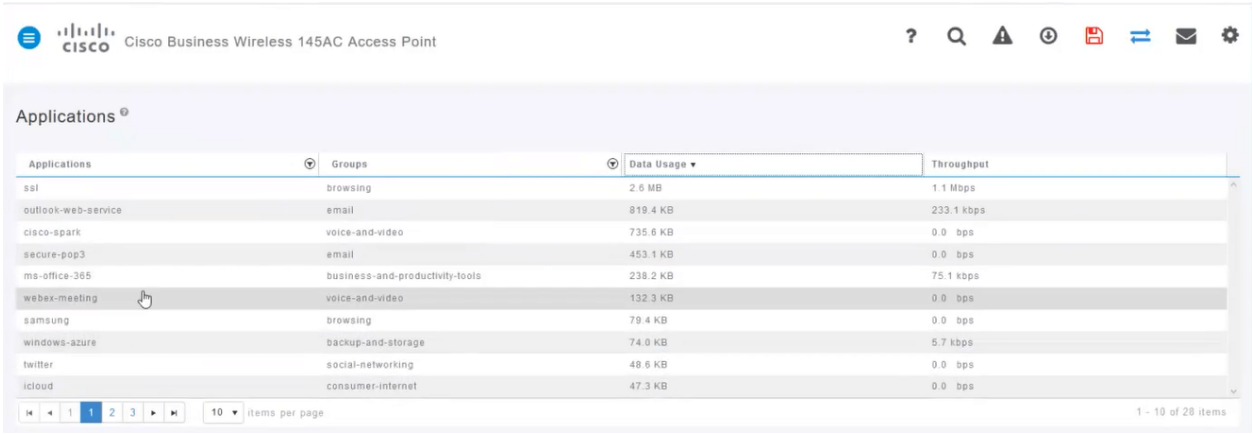
- Aplicativo - inclui vários tipos diferentes
- Grupos - Indica o tipo de grupo de aplicativos para facilitar a classificação
- Uso de dados - A quantidade de dados usada por este serviço como um todo
- Produtividade - A quantidade de largura de banda usada pelo aplicativo

Você pode clicar nas guias para classificar do maior para o menor, o que pode ajudar a identificar os maiores consumidores de recursos de rede.

Esse recurso é muito potente para gerenciar os recursos da WLAN em um nível granular. Abaixo estão alguns dos grupos e tipos de aplicativos mais comuns. É provável que sua lista inclua muito mais, incluindo os seguintes grupos e exemplos:

- Navegação
  - EX: Cliente específico, SSL
- E-mail
  - EX: Outlook, Secure-pop3
- Voz e vídeo
  - EX: WebEx, Cisco Spark,
- Ferramentas de negócios e produtividade
  - EX: Microsoft Office 365,
- Backup e armazenamento
  - EX: Windows-Azure,
- Consumidor-Internet
  - iCloud, Google Drive
- Redes sociais
  - EX: Twitter, Facebook
- Atualizações de software
  - EX: Google-Play, IOS
- Mensagens instantâneas
  - EX: Suspensões, mensagens

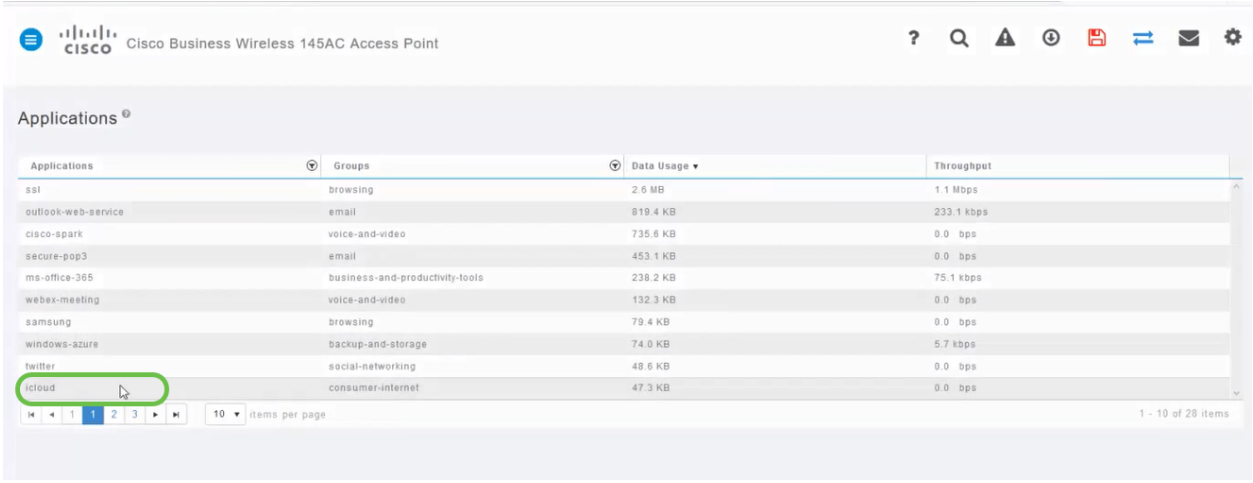
Aqui é mostrado um exemplo de como a página será quando preenchida.



Cada cabeçalho de tabela pode ser clicado para classificação, o que é especialmente útil para os campos *Uso de Dados* e *Rendimento*.

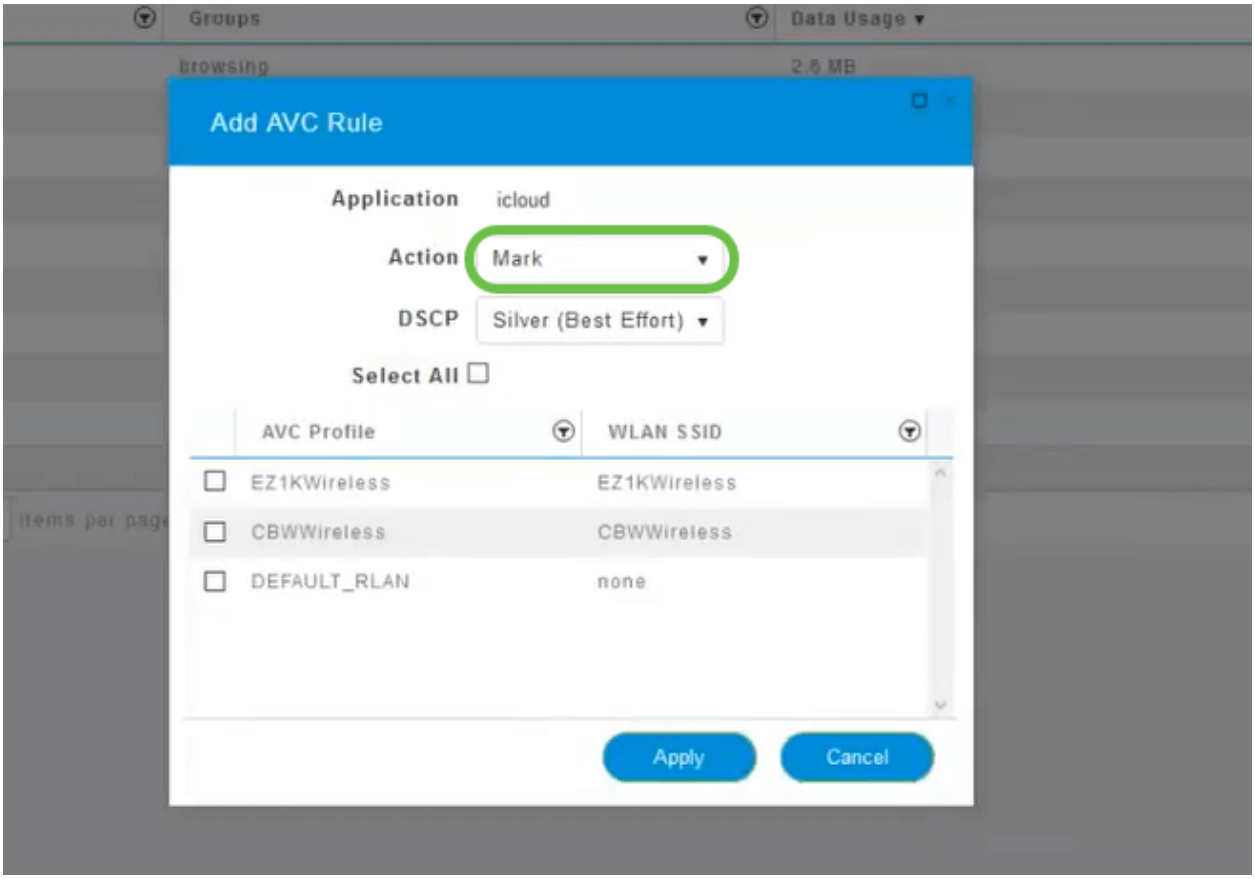
Passo 8

Clique na linha do tipo de tráfego que deseja gerenciar.



Passo 9

Clique na caixa suspensa **Ação** para selecionar como você tratará esse tipo de tráfego.



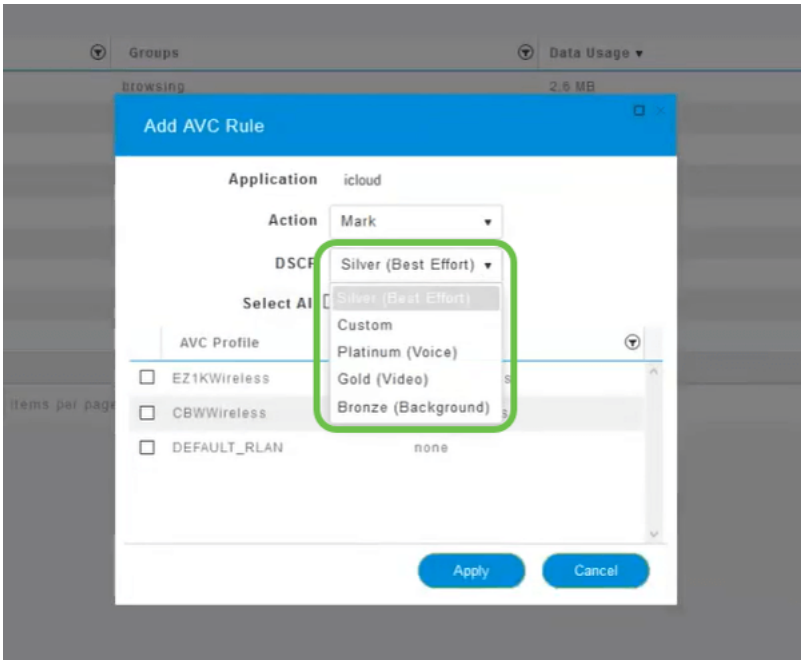
Para este exemplo, estamos deixando esta opção em *Mark*.

Ação a tomar no tráfego

- Marcar - Coloca o tipo de tráfego em um dos três níveis do Differentiated Services Code Point (DSCP) - governando quantos recursos estão disponíveis para o tipo de aplicativo
- Drop - Não faça nada além de descartar o tráfego
- Limite de taxa - Permite definir a taxa média, a taxa de burst em Kbps

Passo 10

Clique na caixa suspensa no campo **DSCP** para selecionar uma das opções a seguir.



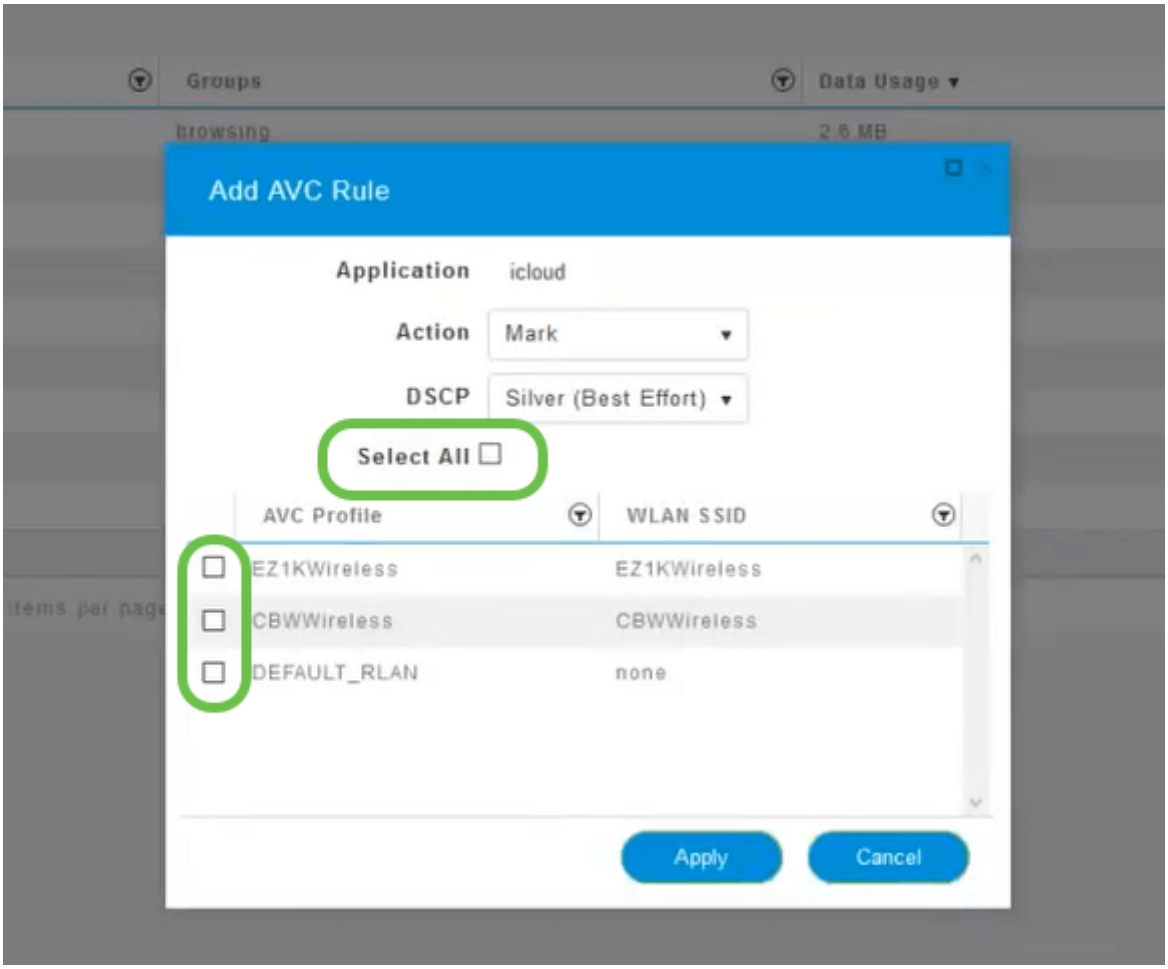
Abaixo estão as opções de DSCP para o tráfego a ser marcado. Essas opções mudam de menos recursos para mais recursos disponíveis para o tipo de tráfego que você está editando.

- Bronze (fundo) - Menos
- Prata (melhor esforço)
- Gold (vídeo)
- Mais Platinum (Voz)
- Personalizado - Conjunto de usuários

Como uma convenção da Web, o tráfego migrou para a navegação SSL, o que impede que você veja o que está dentro dos pacotes à medida que eles se movem de sua rede para a WAN. Como tal, uma grande maioria do tráfego da Web usará SSL. A definição de tráfego SSL para uma prioridade mais baixa pode afetar sua experiência de navegação.

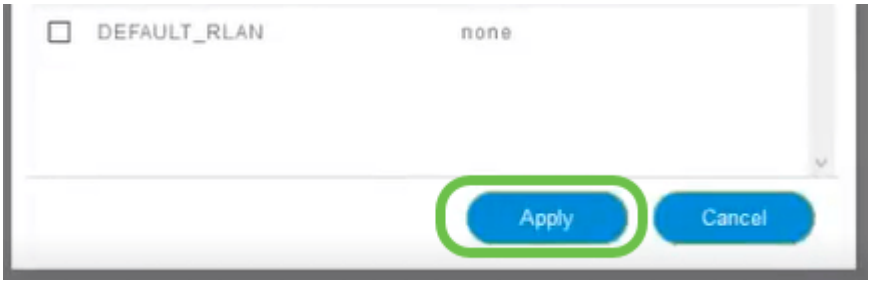
Passo 11

Agora selecione o SSID individual que você deseja que esta diretiva execute ou clique em **Selecionar tudo**.



Etapa 12

Agora clique em **Aplicar** para iniciar esta diretiva.



Dois casos em que tal se poderia aplicar:

- Convidados/usuários transmitindo uma grande quantidade de tráfego, impedindo que o tráfego de missão crítica passe. Você pode aumentar a prioridade de Voz, diminuir a prioridade do tráfego Netflix para melhorar as coisas.
- O download de grandes atualizações de software durante o horário comercial pode ser despriorizado ou a taxa é limitada.

Você conseguiu! A criação de perfis de aplicativos é uma ferramenta muito poderosa que também pode ser ativada com a ativação do perfil do cliente, como detalhado na próxima seção.

Criação de perfil do cliente usando a interface de usuário da Web (opcional)

Ao se conectarem a uma rede, os dispositivos trocam informações de perfil do cliente. Por padrão, o *perfil do cliente* está desabilitado. Essas informações podem incluir:

- Nome do host - ou o nome do dispositivo
- Sistema operacional - o software principal do dispositivo
- Versão do SO - A iteração do software aplicável

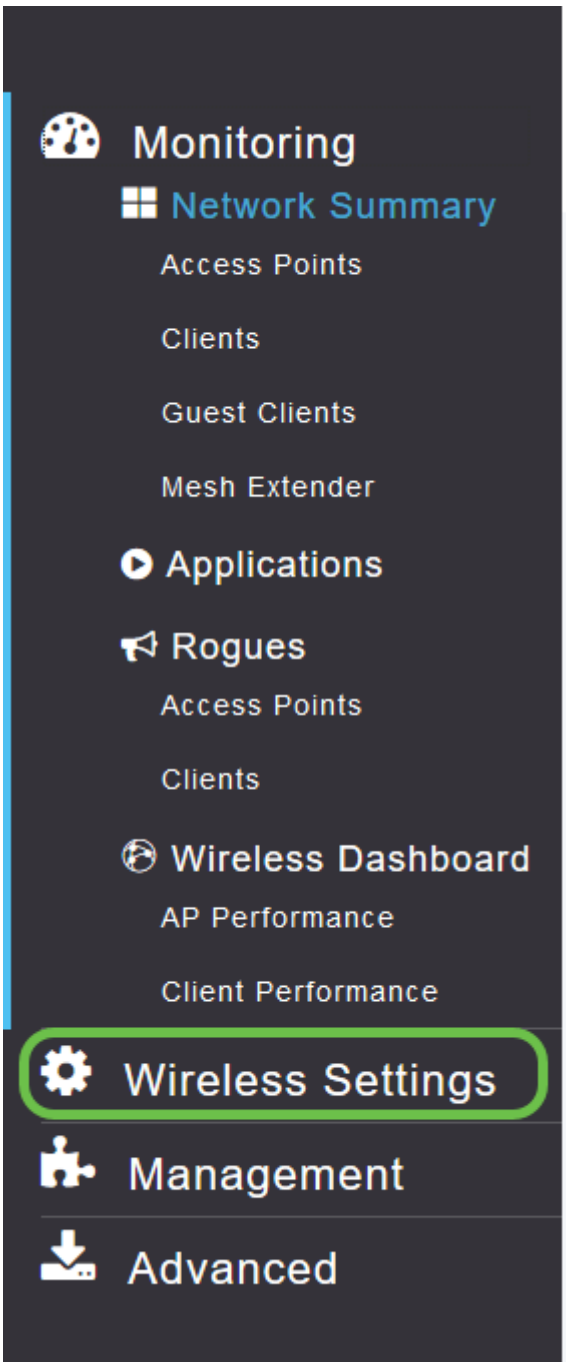
As estatísticas sobre esses clientes incluem a quantidade de dados usados e o throughput.

O rastreamento de perfis de clientes permite maior controle sobre a rede local sem fio. Ou você pode usá-lo como uma função de outro recurso. Como usar tipos de dispositivos de limitação de aplicativos que não transportam dados de missão crítica para sua empresa.

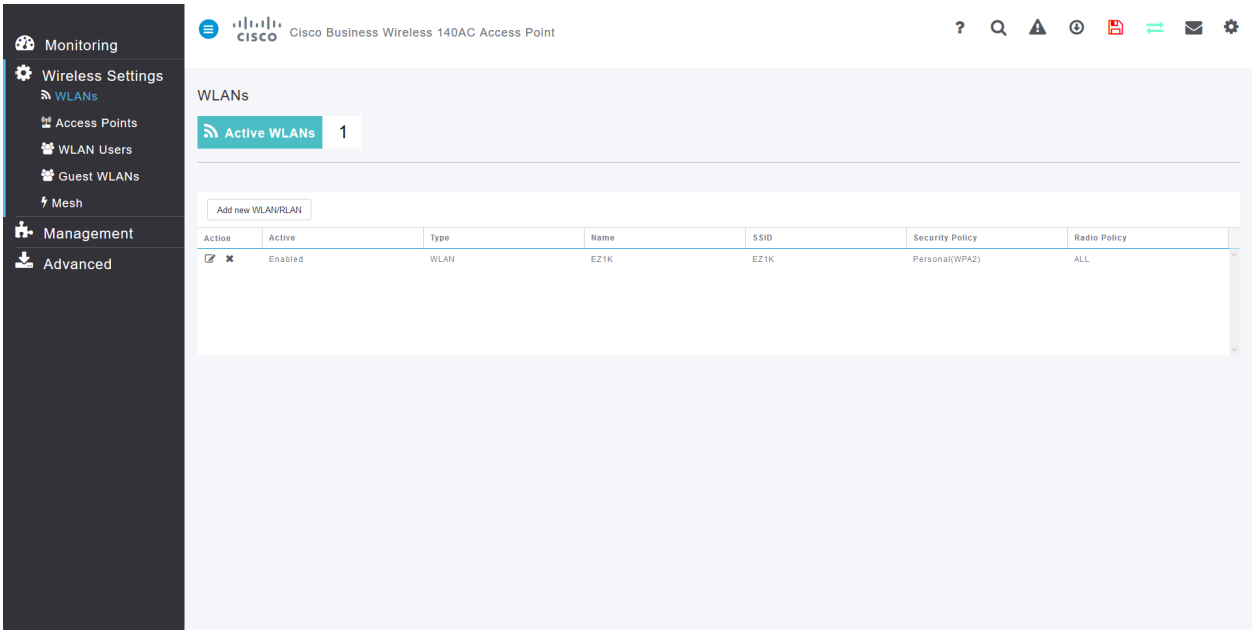
Depois de ativada, os detalhes do cliente para a sua rede podem ser encontrados na seção Monitoramento da interface do usuário da Web.

Passo 1

Clique em **Configurações sem fio**.

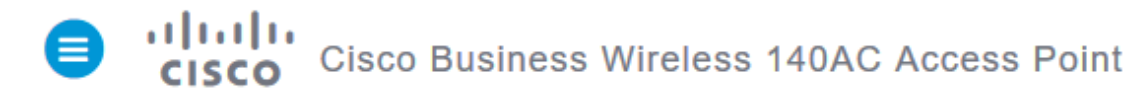


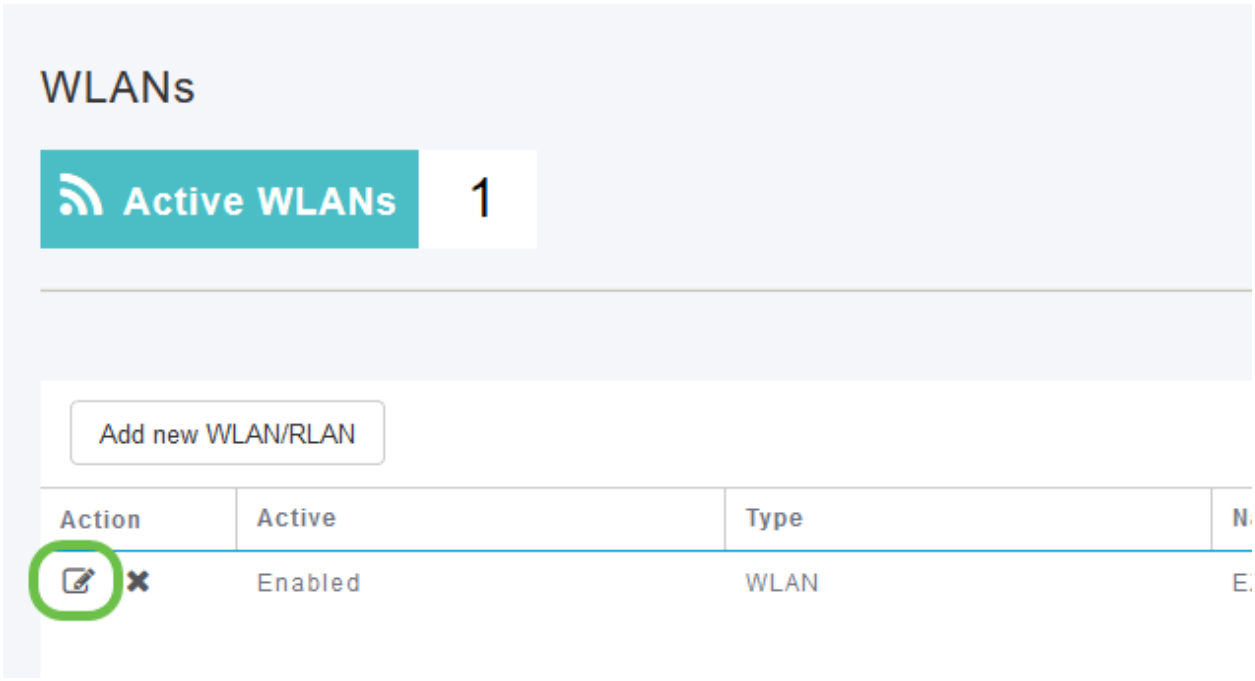
A imagem abaixo é semelhante à que você verá quando clicar no link Wireless Settings (Configurações sem fio):



Passo 2

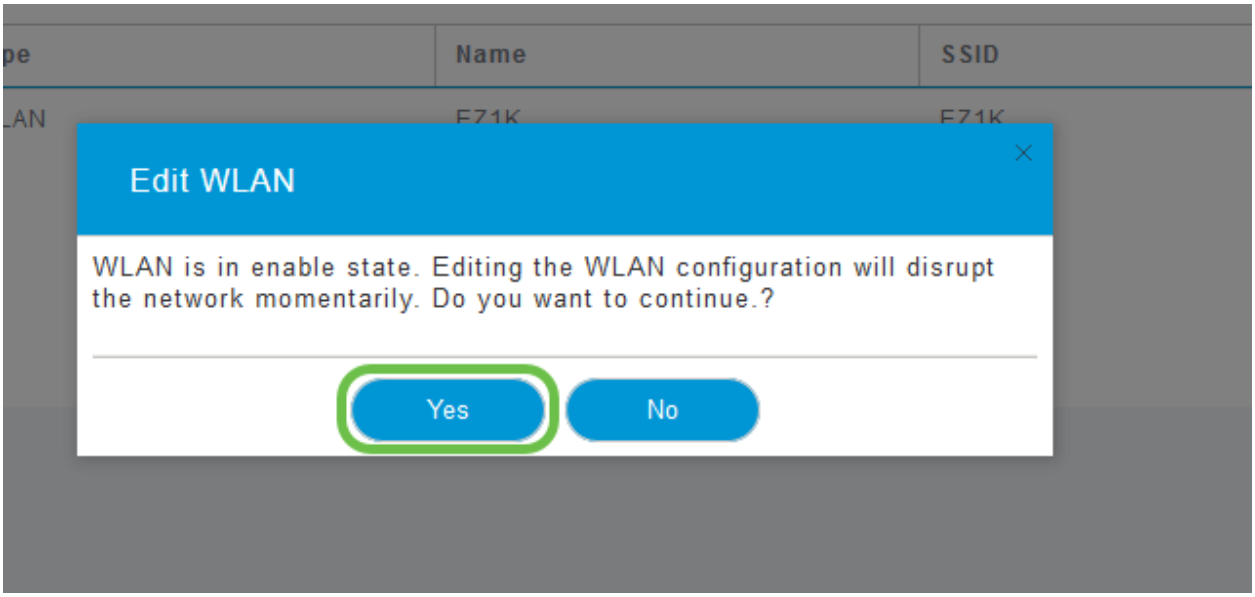
Decida qual WLAN você deseja usar para o aplicativo e clique no **ícone de edição** à esquerda dele.





Etapa 3

Um menu pop-up pode ser exibido de maneira semelhante ao abaixo. Esta mensagem importante pode afetar temporariamente o serviço na rede. Clique em **Sim** para prosseguir.

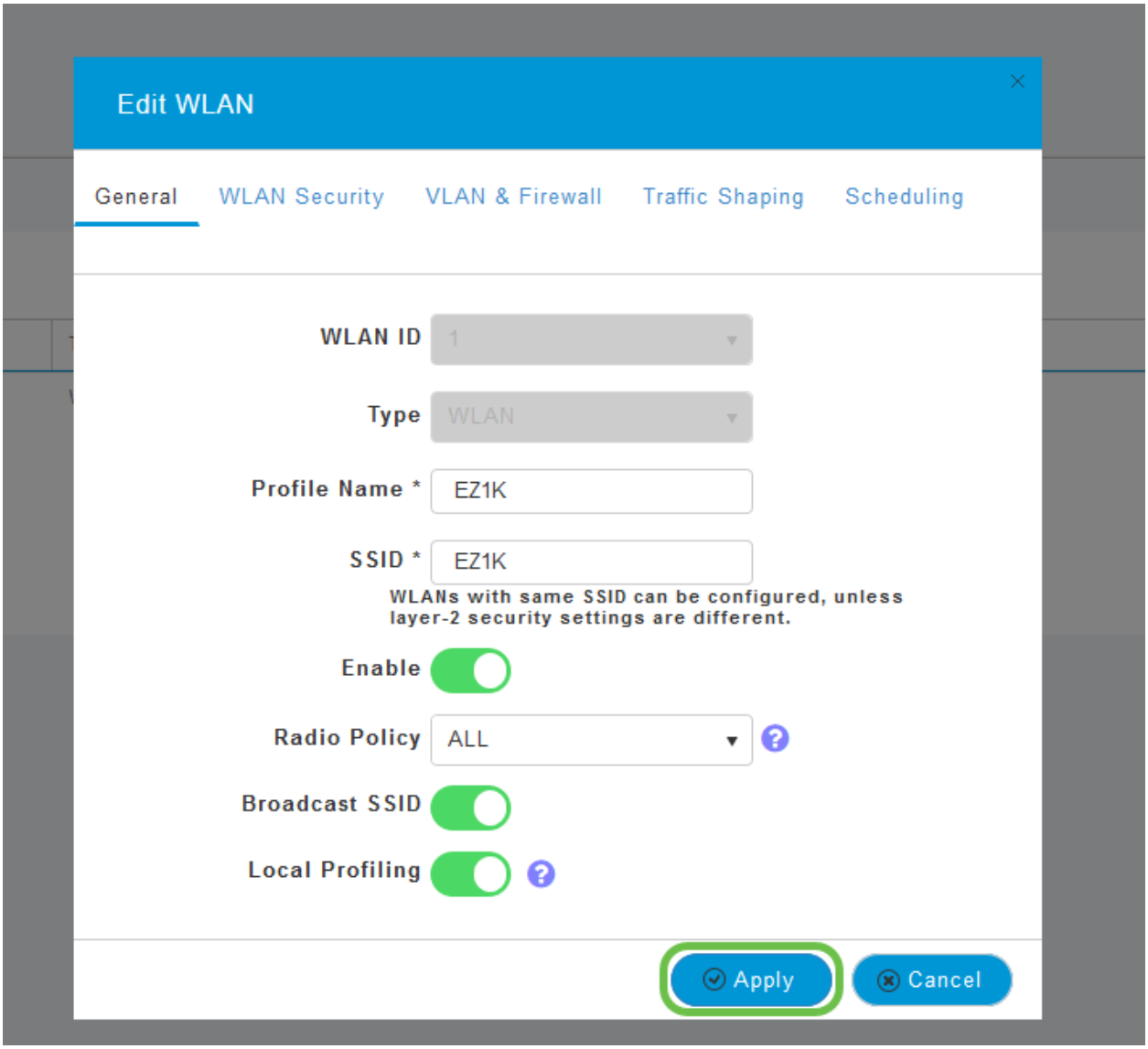


Passo 4

Alterna a criação de perfis de clientes clicando no botão de alternância **Local Profiles**.

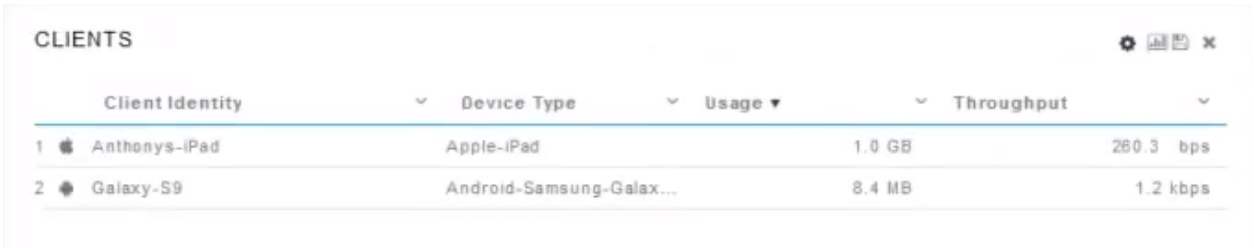
Etapa 5

Clique em Apply.



Etapa 6

Clique no item de menu da seção **Monitoramento** no lado esquerdo. Você verá que os dados do cliente começam a aparecer no Painel da guia *Monitoramento*.



Conclusão

Agora você concluiu a configuração da sua rede segura. Que grande sensação, agora preciso de um minuto para comemorar e depois começar a trabalhar!

Queremos o melhor para nossos clientes, portanto, se você tiver comentários ou sugestões sobre este tópico, envie um e-mail para a equipe de conteúdo da Cisco.

Para ler outros artigos e documentação, consulte as páginas de suporte do seu hardware:

- Roteador VPN Cisco RV260P com PoE
- Access point Cisco Business 140AC
- Extensor de malha Cisco Business 142ACM