Configuração de rede total: RV345P e Cisco Business Wireless usando o aplicativo móvel

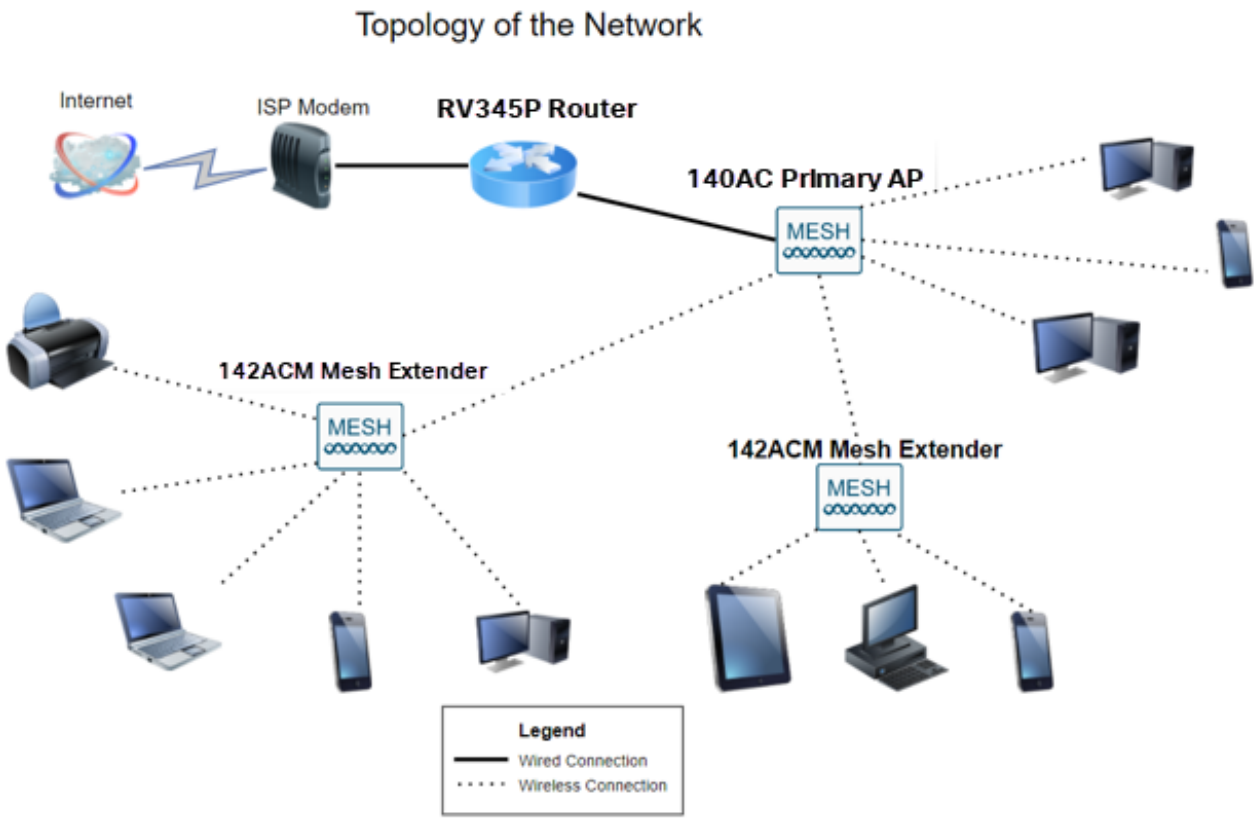
Objetivo

Este guia mostrará como configurar uma rede em malha sem fio usando um roteador RV345P, um ponto de acesso CBW140AC e dois extensores de malha CBW142ACM.

Este artigo usa o aplicativo móvel, que é recomendado para configuração simples na rede sem fio mesh. Se preferir usar a Interface do Usuário da Web (IU) para todas as configurações, clique para ir para o artigo que usa a IU da Web.

Table Of Contents

Topologia



Introdução

Todas as suas pesquisas se juntaram e você comprou seu equipamento da Cisco, que empolgante! Neste cenário, estamos usando um roteador RV345P. 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.

Esse roteador avançado também oferece a opção de recursos adicionais.

1. O controle de aplicativos permite controlar o tráfego. Esse recurso pode ser configurado para permitir tráfego, mas para registrá-lo, bloquear tráfego e registrá-lo ou simplesmente bloquear tráfego.

2. A filtragem da Web é usada para evitar o tráfego da Web para sites da Web inseguros ou inadequados. Não há registro com este recurso.
3. O AnyConnect é uma rede virtual privada (VPN) SSL que está disponível na Cisco. As VPNs permitem que usuários e locais remotos se conectem ao escritório da sua empresa ou data centers, criando um túnel seguro através da Internet.

Se você quiser usar esses recursos, precisará comprar uma licença. Roteadores e licenças são registrados online, que serão abordados neste guia.

Se você não estiver familiarizado com alguns dos termos usados neste documento ou quiser mais detalhes sobre a Rede em Malha, consulte os seguintes artigos:

- Cisco Business: Glossário de novos termos
- Bem-vindo ao Cisco Business Wireless Mesh Networking
- Perguntas frequentes (FAQ) de uma rede sem fio empresarial da Cisco

Dispositivos aplicáveis | Versão de software

- RV345P | 1.0.03.21
- CBW140AC | 10.4.1.0
- CBW142ACM | 10.4.1.0 (pelo menos um extensor de malha é necessário para a rede de malha)

Pré-requisitos

Preparar o roteador

1. Verifique se você tem uma conexão atual com a Internet para a instalação.
2. Entre em contato com o seu ISP (Provedor de serviços de Internet) para descobrir quaisquer instruções especiais que ele tenha ao usar o roteador RV345P. 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 para o seu novo roteador.
3. Decida onde colocar o roteador. Você vai querer uma área aberta, se possível. Isso pode não ser fácil porque você deve conectar o roteador ao gateway de banda larga (modem) de seu ISP (Provedor de serviços de Internet).

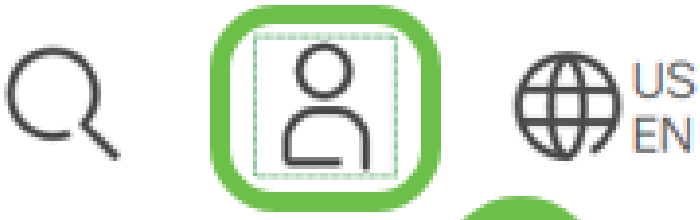
Obtenha uma conta Cisco.com

Agora que você possui equipamentos da Cisco, precisa obter uma conta Cisco.com, às vezes chamada de identificação online do Cisco Connection (ID do CCO). Uma conta não é cobrada.

Se você já tiver uma conta, poderá ir para a próxima seção deste artigo.

Passo 1

Acesse Cisco.com. Clique no ícone de pessoa e em Criar uma conta.



1

Have an account?

- Personalized content
- Your products and support

Log In

Forgot your user ID and/or password?

Manage account

My Cisco

Need an account?

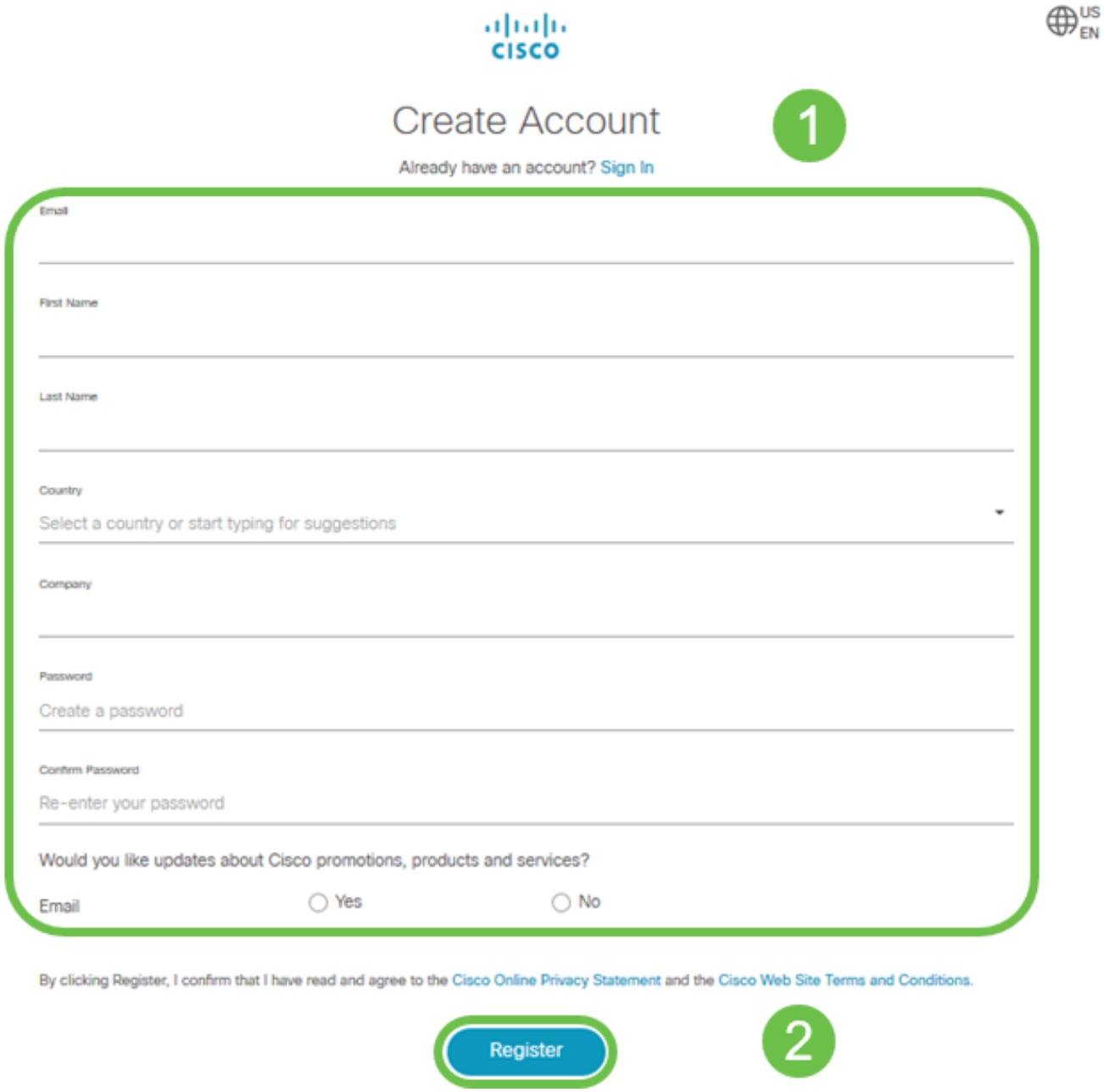
Create an account

2

Help

Passo 2

Insira os detalhes necessários para criar a conta e clique em Register. Siga as instruções para concluir o processo de registro.



Se você tiver algum problema, clique para ir para a página de ajuda Cisco.com Account Registration.

Configurar o roteador RV345P

Um roteador é essencial em uma rede porque roteia pacotes. Ele permite que um computador se comunique com outros computadores que não estejam 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 que os pacotes cheguem ao seu destino específico.

Seu RV345P vem com configurações padrão otimizadas para muitas pequenas empresas. No entanto, suas demandas de rede ou o provedor de serviços de Internet (ISP) podem exigir que você modifique algumas dessas configurações. Depois de entrar em contato com o ISP para obter os requisitos, você pode fazer alterações usando a Interface de Usuário da Web (IU).

Você está pronto? Vamos falar sobre isso!

RV345P pronto para uso

Passo 1

Conecte o cabo Ethernet de uma das portas LAN (Ethernet) RV345P 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 RV345P para executar a configuração inicial.

Passo 2

Certifique-se de usar o adaptador de alimentação fornecido com o RV345P. Usar um adaptador de alimentação diferente pode danificar o RV345P ou fazer com que os dongles USB falhem. O botão liga/desliga está ligado por padrão.

Conecte o adaptador de alimentação à porta 12VDC do RV345P, 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 RV345P.

Etapa 5

Conecte a outra extremidade do adaptador RV345P a uma tomada. Isso ligará o RV345P. Reconecte o modem para que ele também possa ser ligado. A luz de alimentação no painel frontal está verde estável quando o adaptador de alimentação está conectado corretamente e o RV345P concluiu a inicialização.

Configurar o roteador

O trabalho de preparação está concluído, agora é hora de obter algumas configurações!

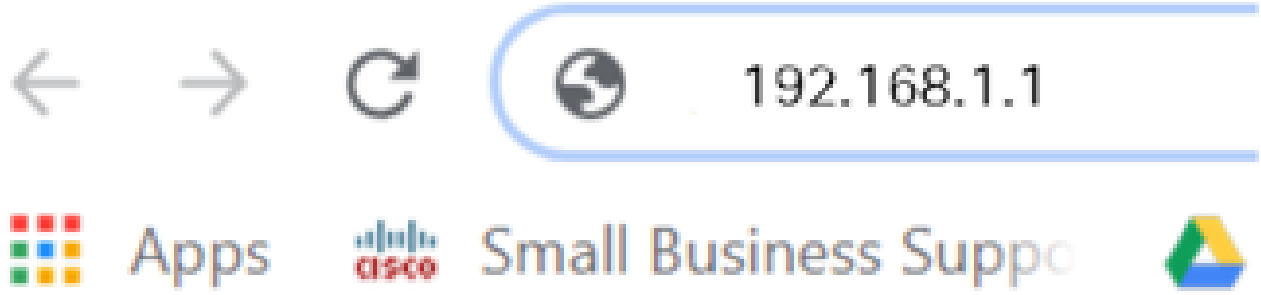
Para iniciar a interface do usuário da Web, siga estas etapas.

Passo 1

Se o seu computador estiver configurado para se tornar um cliente DHCP, 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 aos 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.

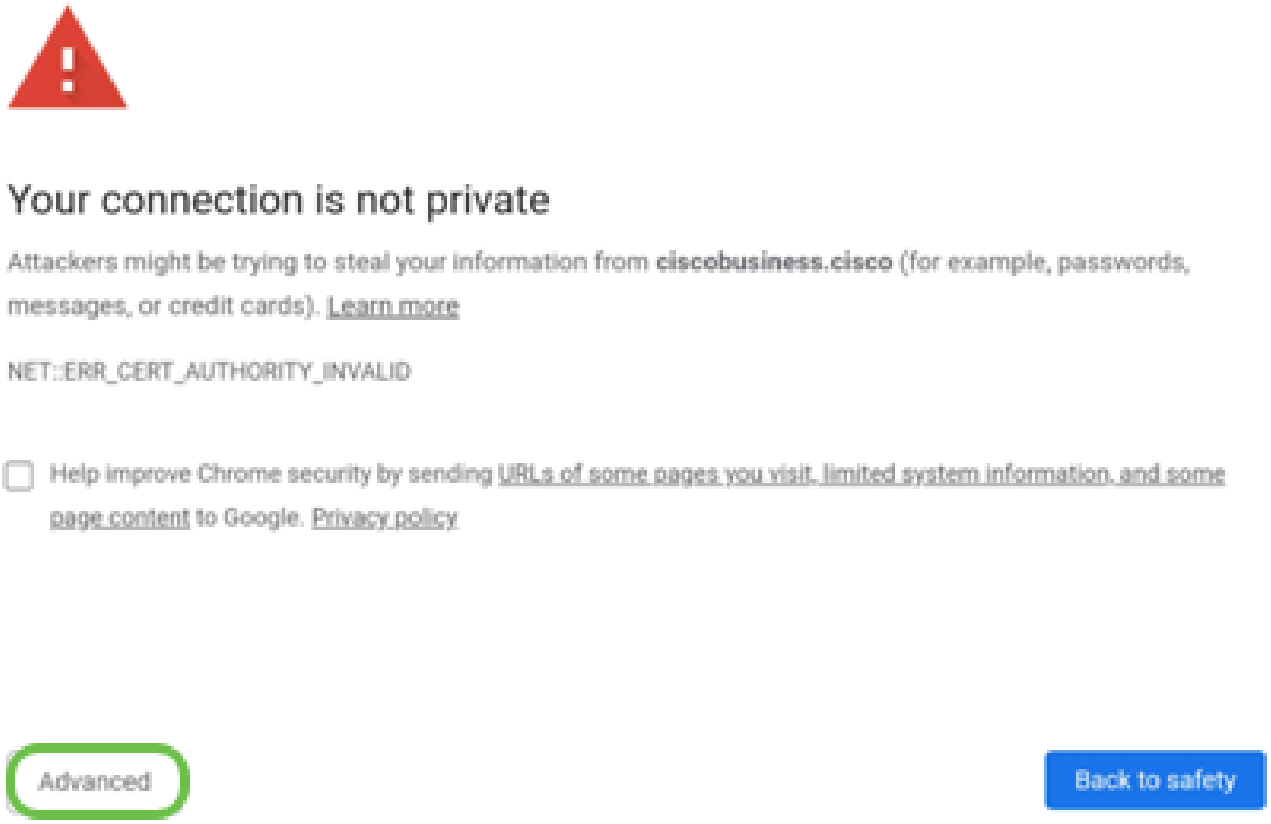
Passo 2

Abra um navegador da Web, como Safari, Internet Explorer ou Firefox. Na barra de endereços, insira o endereço IP padrão do RV345P, 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.

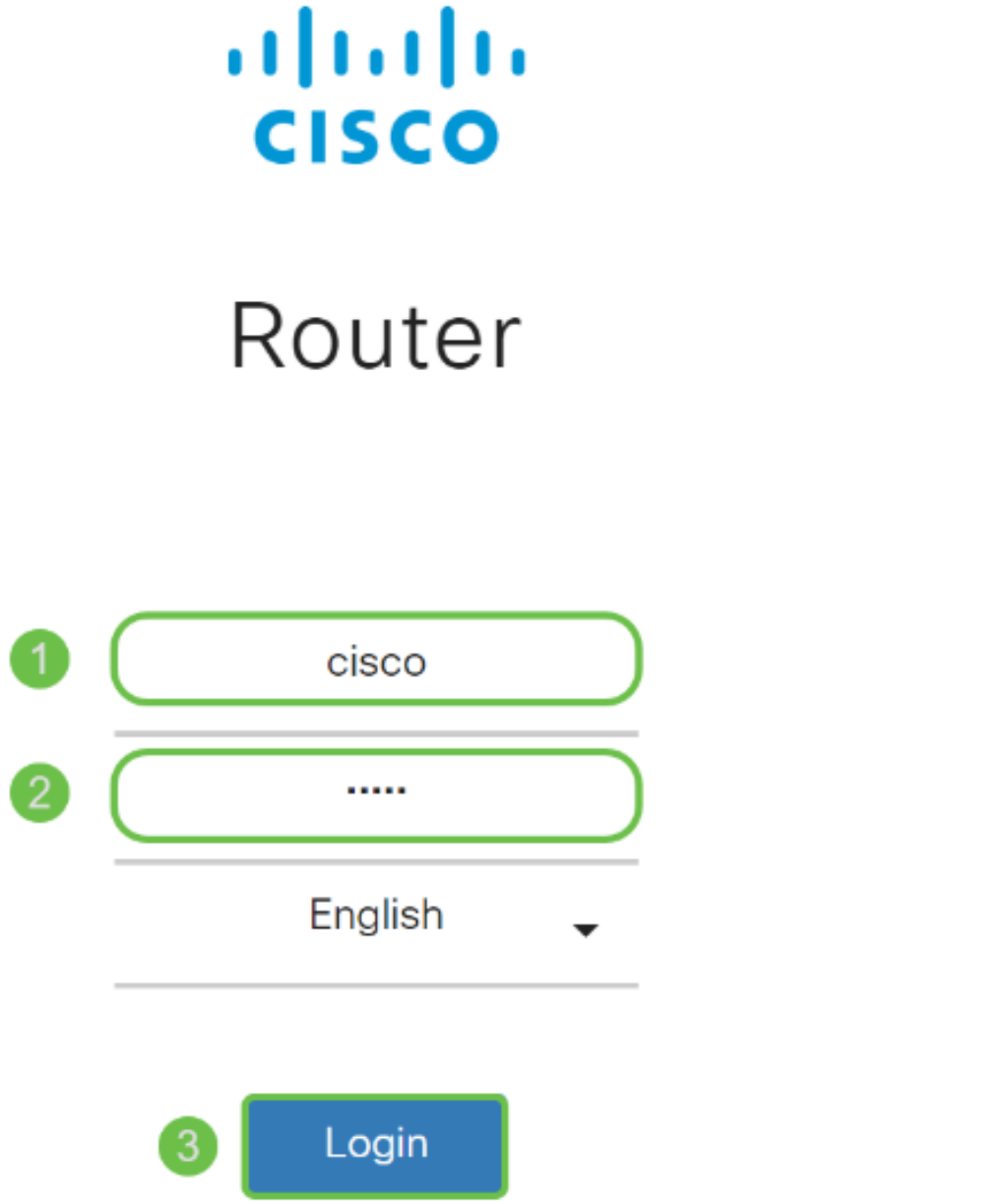


Passo 4

Quando a página de entrada for exibida, insira o nome de usuário padrão cisco e a senha padrão cisco.

Clique em login.

Para obter informações detalhadas, clique em How to access the web-based setup page of Cisco RV340 series VPN routers.



Etapa 5

Clique em login. A página Getting Started é exibida. Se o painel de navegação não estiver aberto, você poderá abri-lo clicando no ícone de menu.

Agora que você confirmou a conexão e fez login no roteador, vá para a seção Configuração inicial deste artigo.

Solucionando problemas da conexão com a Internet

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

No sistema operacional 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 atingir o tempo limite, você não poderá se comunicar com o roteador.

Se a conectividade não estiver acontecendo, consulte este artigo Solução de problemas.

Algumas outras coisas a serem tentadas:

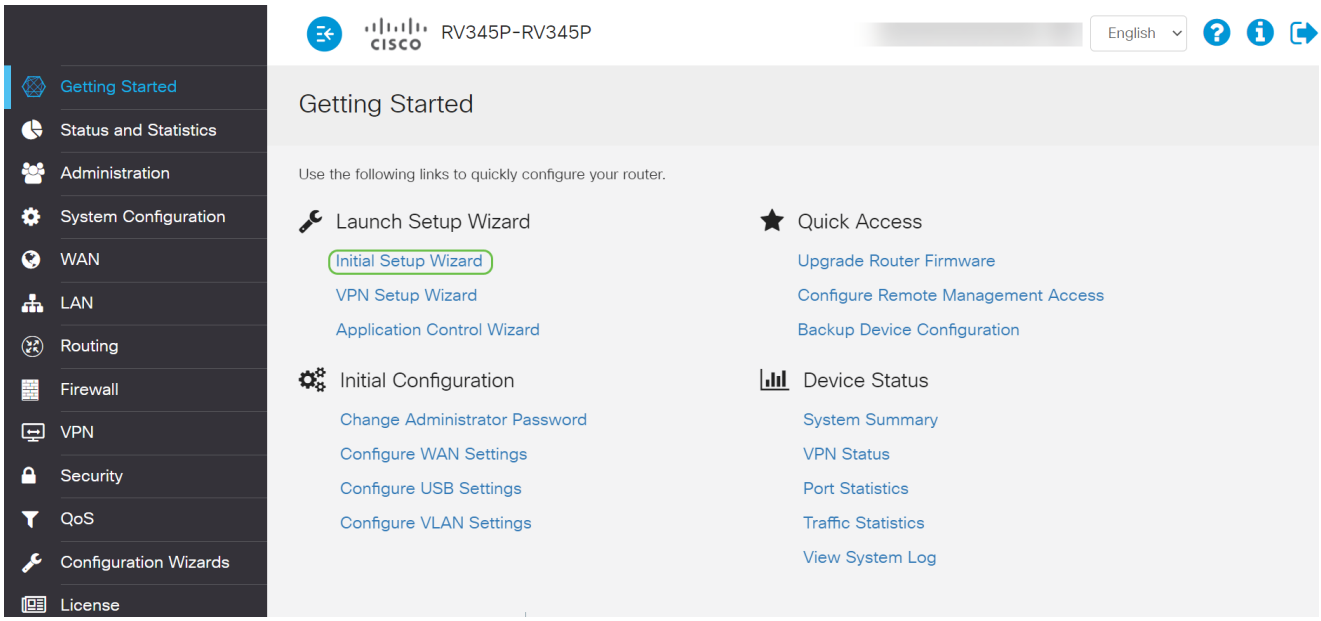
1. Verifique se o seu navegador da Web não está definido como Trabalhar Offline.
2. Verifique as configurações da conexão de rede local do adaptador Ethernet. O PC deve obter um endereço IP por meio de DHCP. Como alternativa, o PC pode ter um endereço IP estático no intervalo 192.168.1.x com o gateway padrão definido como 192.168.1.1 (o endereço IP padrão do RV345P). Para se conectar, pode ser necessário modificar as configurações de rede do RV345P. Se você estiver usando o Windows 10, confira as instruções do Windows 10 para modificar as configurações de rede.
3. Se você tiver equipamentos que ocupam 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. Reinicie o modem e o RV345P desligando ambos os dispositivos. Em seguida, ligue o modem e deixe-o inativo por cerca de 2 minutos. Em seguida, ligue o RV345P. Agora você deve receber um endereço IP de WAN.
5. Se você tiver um modem DSL, peça ao ISP para colocar o modem DSL no modo bridge.

Configuração inicial

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

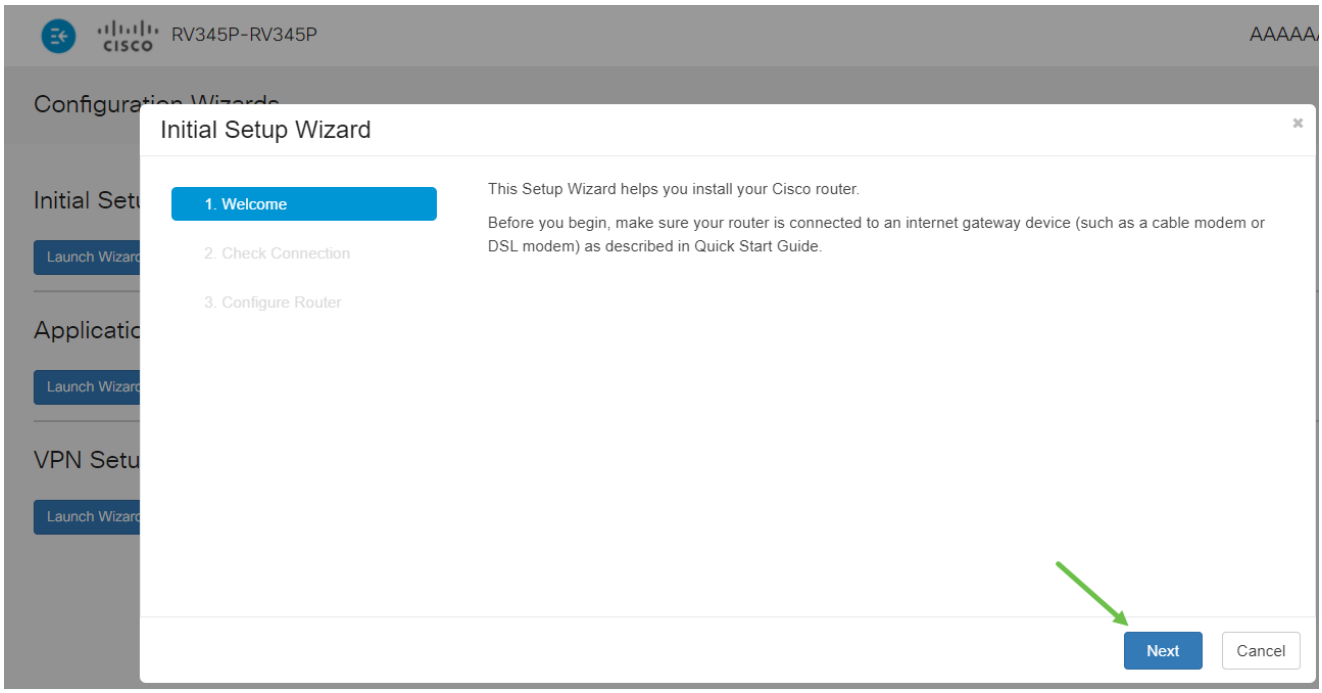
Passo 1

Clique em Initial Setup Wizard na página Getting Started.



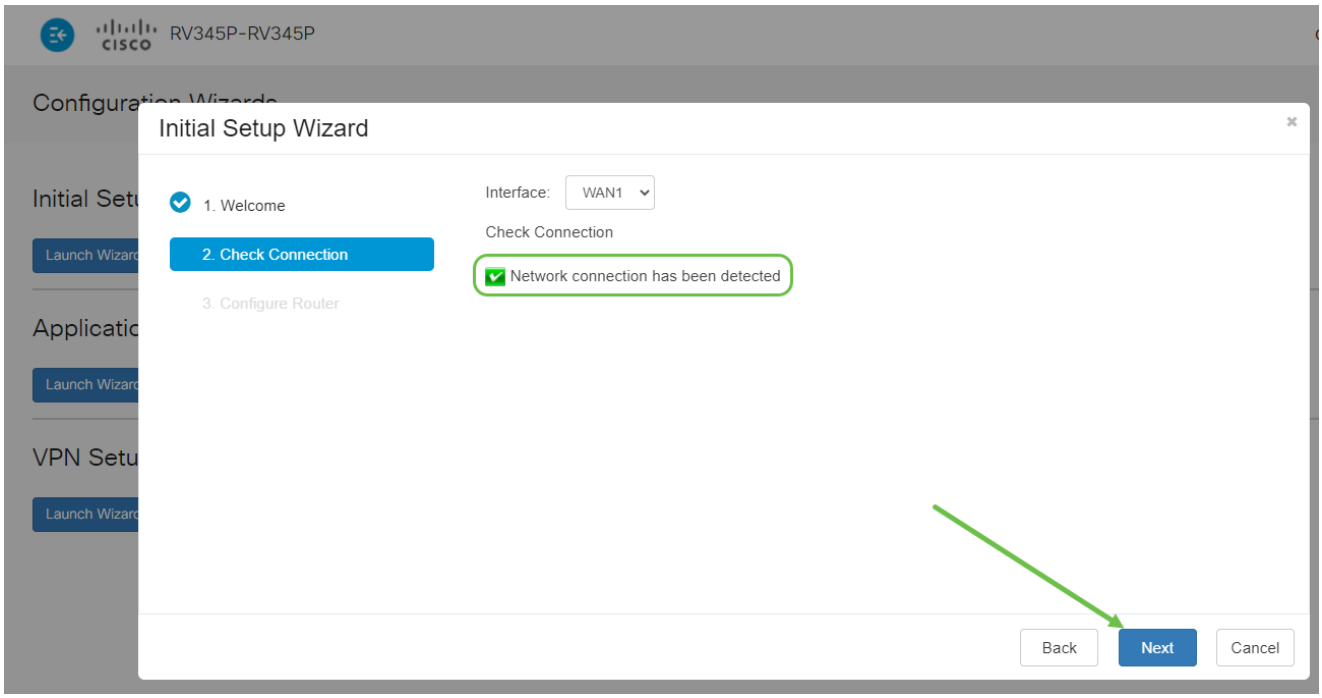
Passo 2

Esta etapa confirma que os cabos estão conectados. Como isso já foi confirmado, clique em Avançar.



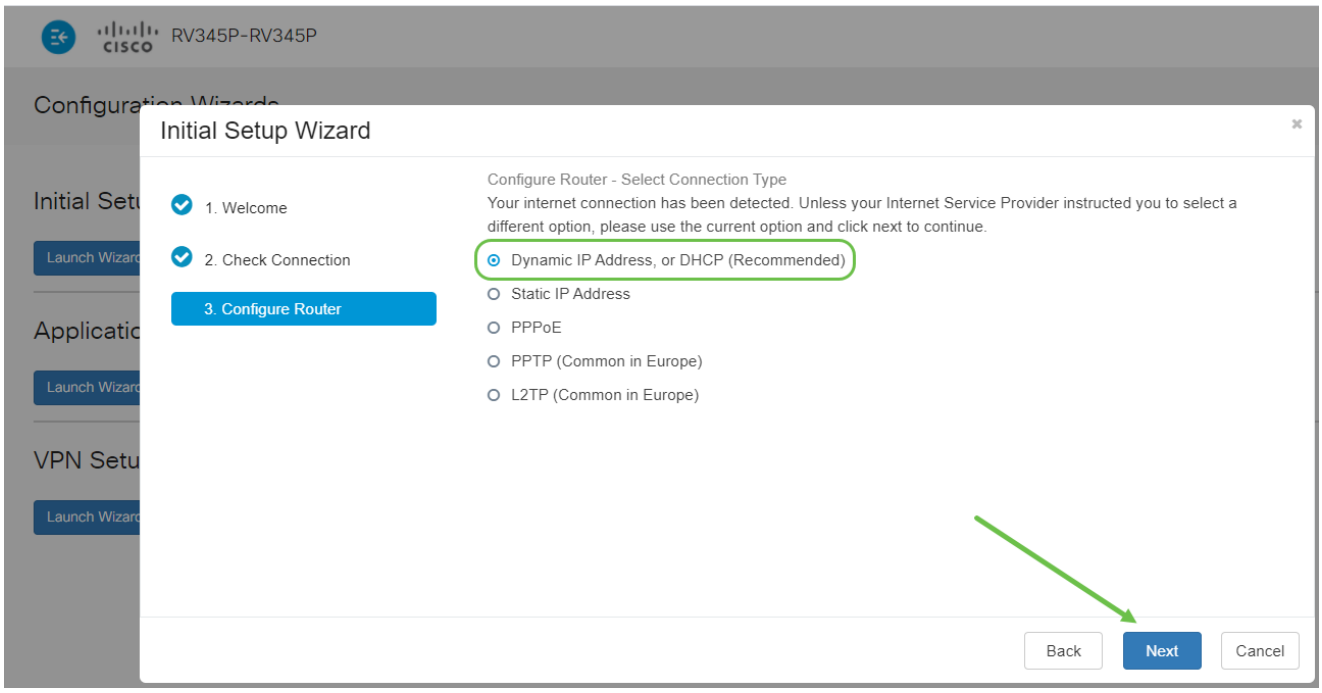
Etapa 3

Esta etapa abrange as etapas básicas para garantir que o roteador esteja conectado. Como isso já foi confirmado, clique em Avançar.



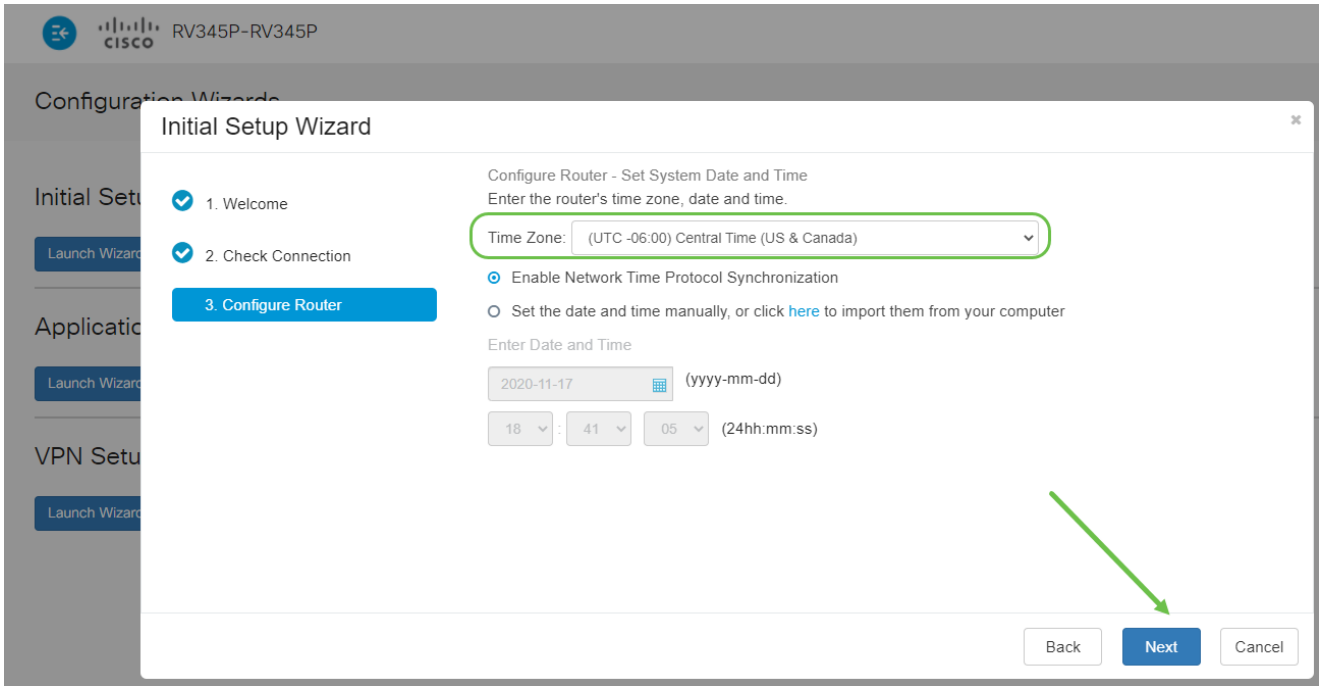
Passo 4

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



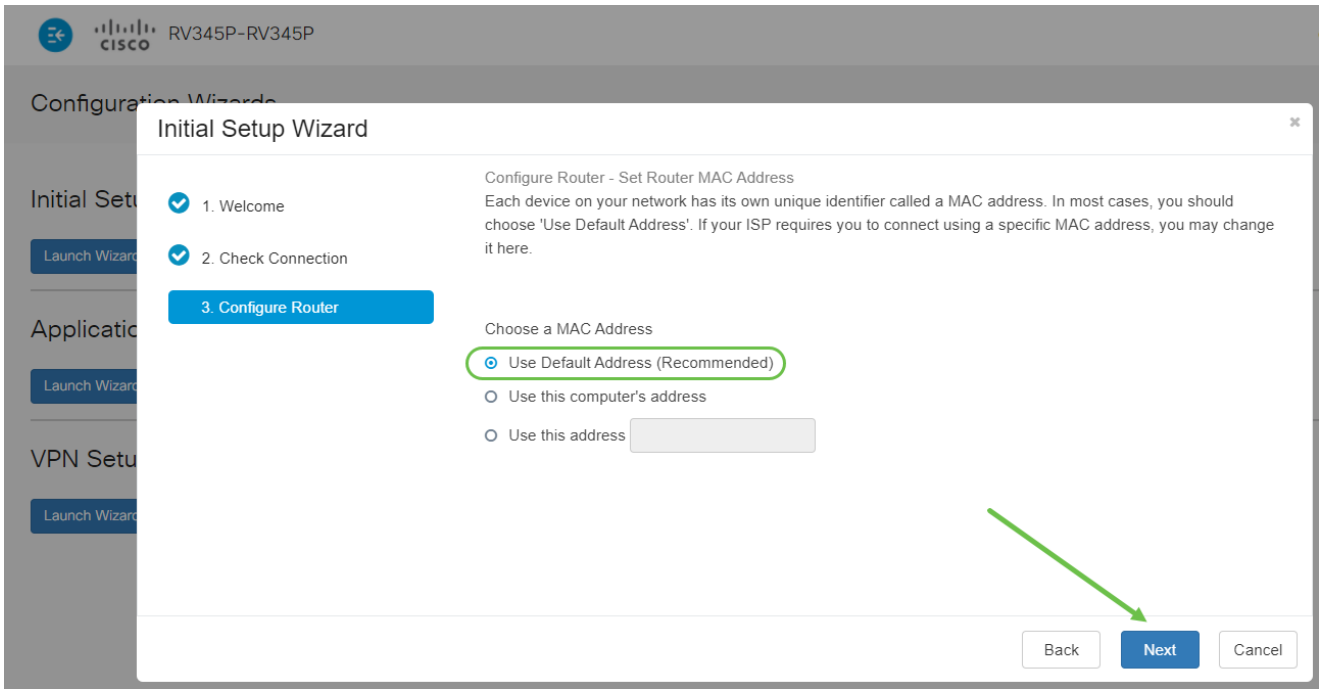
Etapa 5

Você será solicitado a definir as configurações de hora do roteador. Isso é importante porque permite precisão ao revisar logs ou solucionar problemas de eventos. Selecione seu Fuso horário e clique em Avançar.



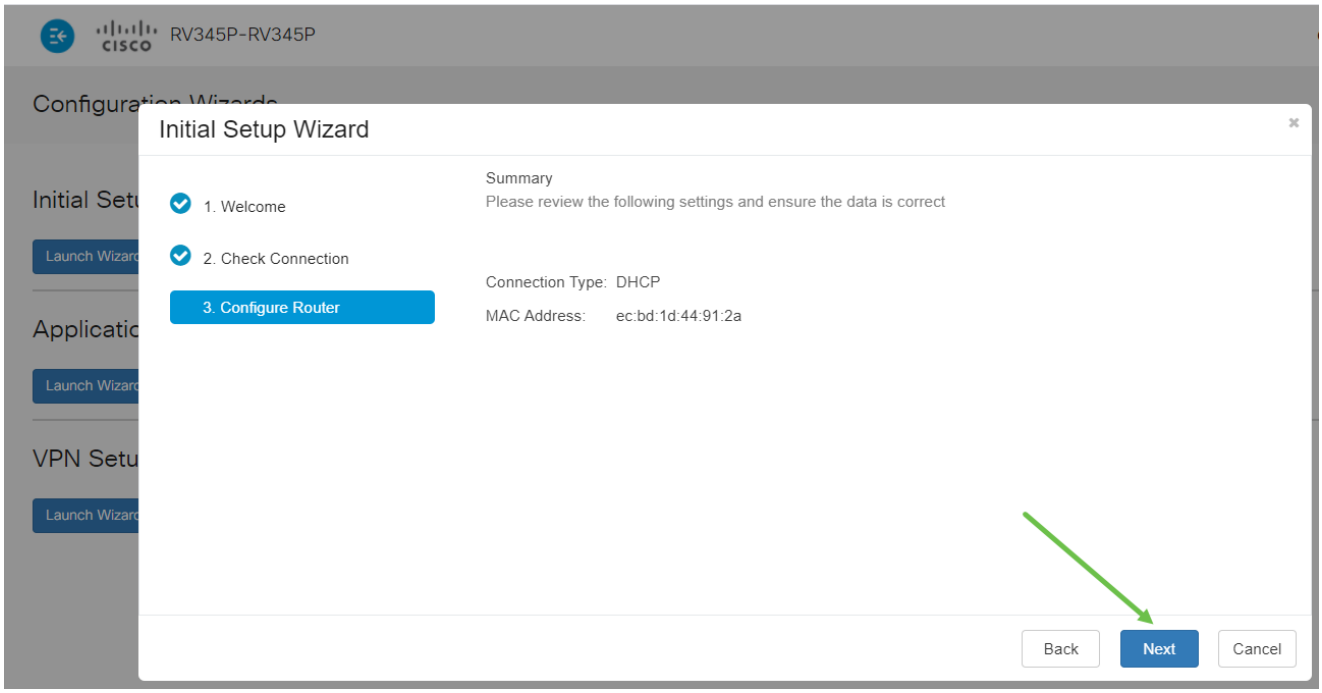
Etapa 6

Você selecionará quais endereços MAC atribuir aos dispositivos. Na maioria das vezes, você usará o endereço padrão. Clique em Next.



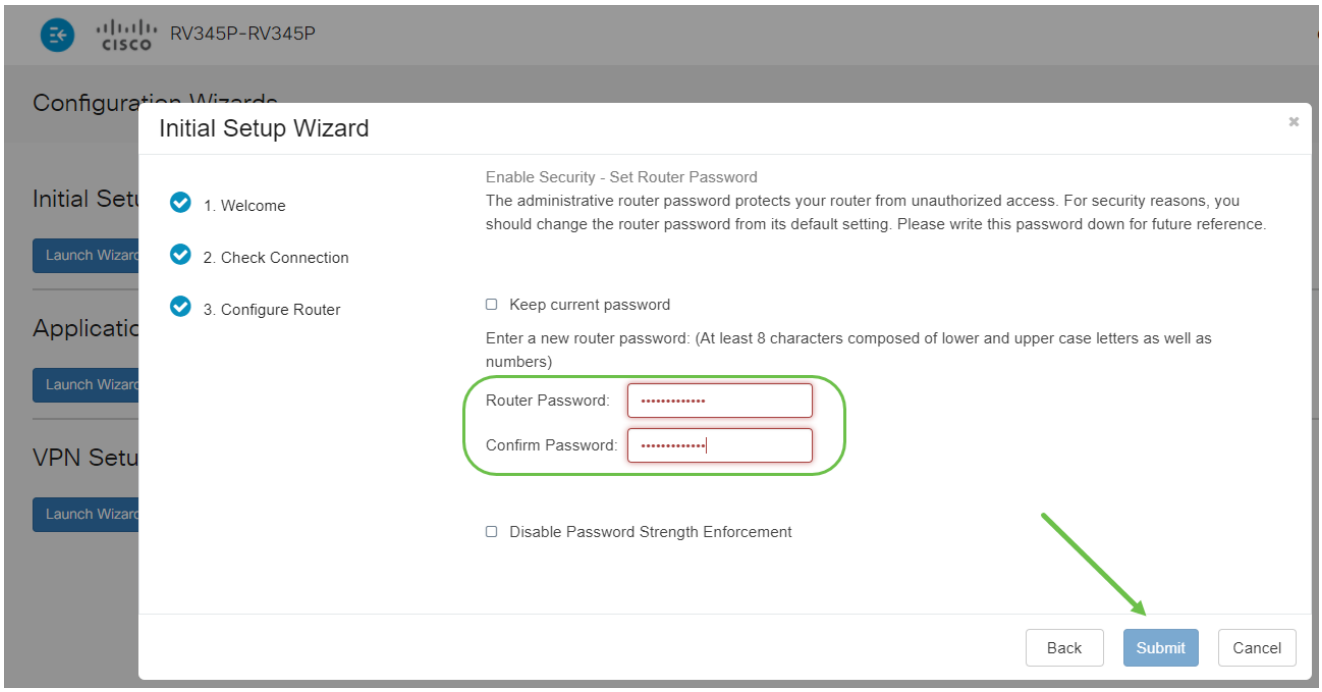
Etapa 7

A página a seguir é um resumo das opções selecionadas. Revise e clique em Avançar se estiver 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 (maiúsculos e minúsculos) e incluir números. Insira uma senha que esteja em conformidade com os requisitos de força. Clique em Next. Anote sua senha para futuros logins.



Não é recomendável selecionar Desabilitar Imposição de Intensidade de Senha. Essa opção permite selecionar uma senha simples como 123, o que seria tão fácil quanto 1-2-3 para os agentes mal-intencionados decifrarem.

Passo 9

Clique no ícone salvar.

Se quiser mais informações sobre essas configurações, você pode ler Configure DHCP WAN Settings on the RV34x Router.

Seu RV345P tem Power over Ethernet (PoE) habilitado por padrão, mas você pode fazer alguns ajustes nele. Se precisar personalizar as configurações, consulte Configurar Power over Ethernet (PoE) no Roteador RV345P.

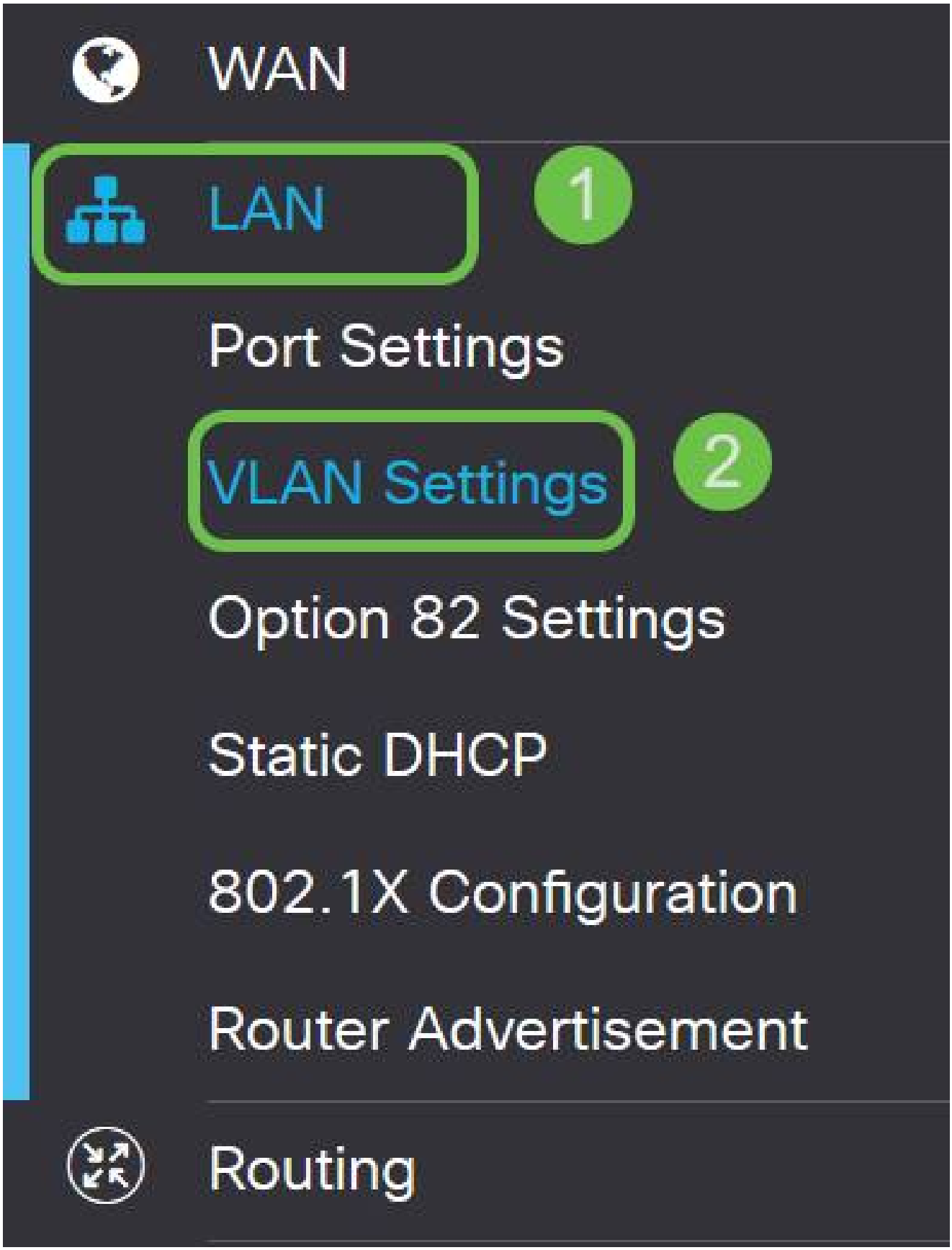
Editar um endereço IP, se necessário (opcional)

Após concluir o Assistente de configuração inicial, você pode definir um endereço IP estático no roteador editando as configurações de VLAN.

Esse processo só é necessário se o endereço IP do roteador precisar ser atribuído a um endereço específico na rede existente. Se não precisar editar um endereço IP, você pode ir para a próxima seção deste artigo.

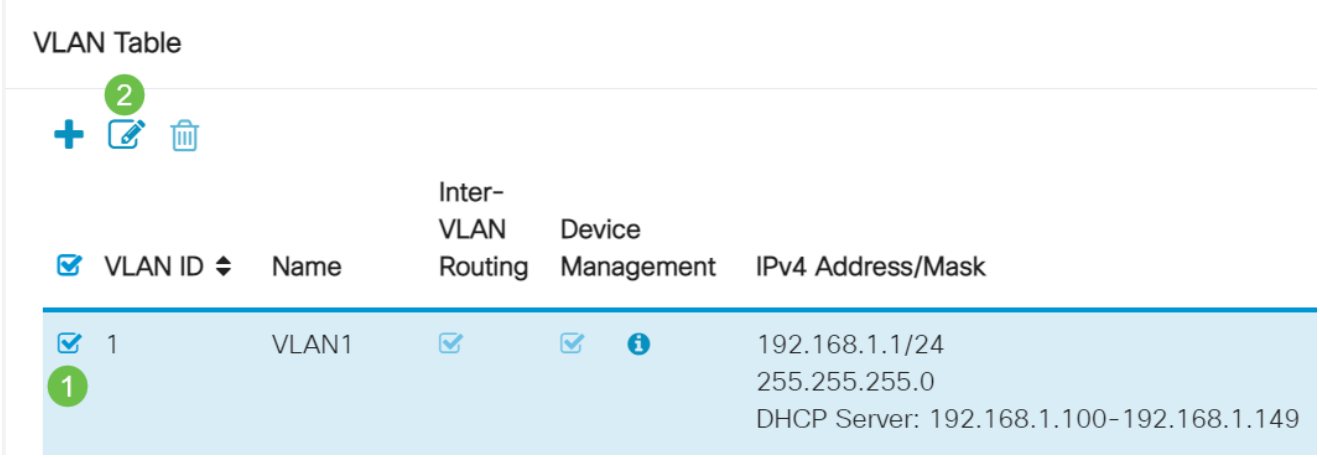
Passo 1

No menu à esquerda, clique em LAN > VLAN Settings.



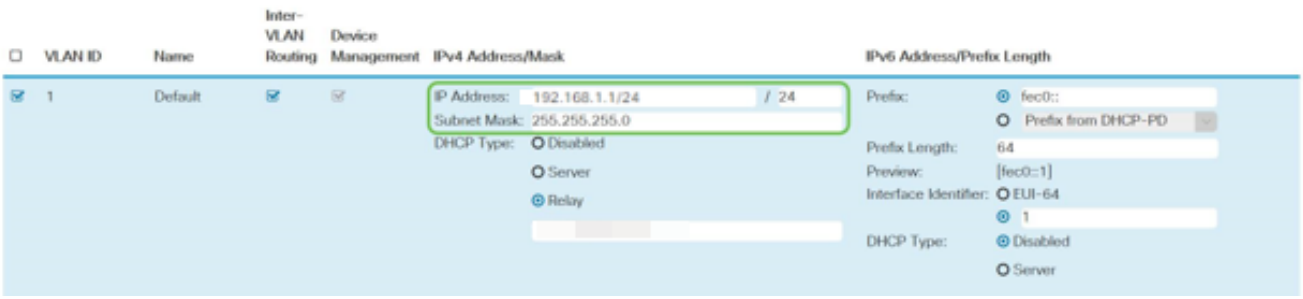
Passo 2

Selecione a VLAN que contém o dispositivo de roteamento e clique no ícone de edição.



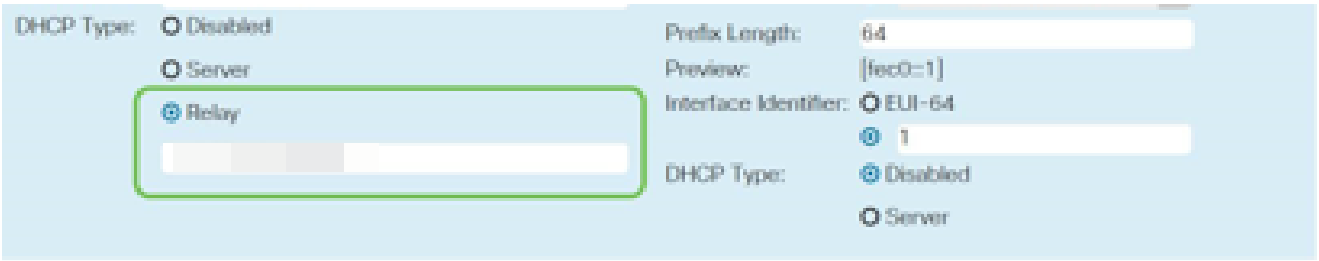
Etapa 3

Insira o endereço IP estático desejado e clique em Apply no canto superior direito.



Etapa 4 (opcional)

Se o roteador não for o servidor/dispositivo DHCP que está 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.

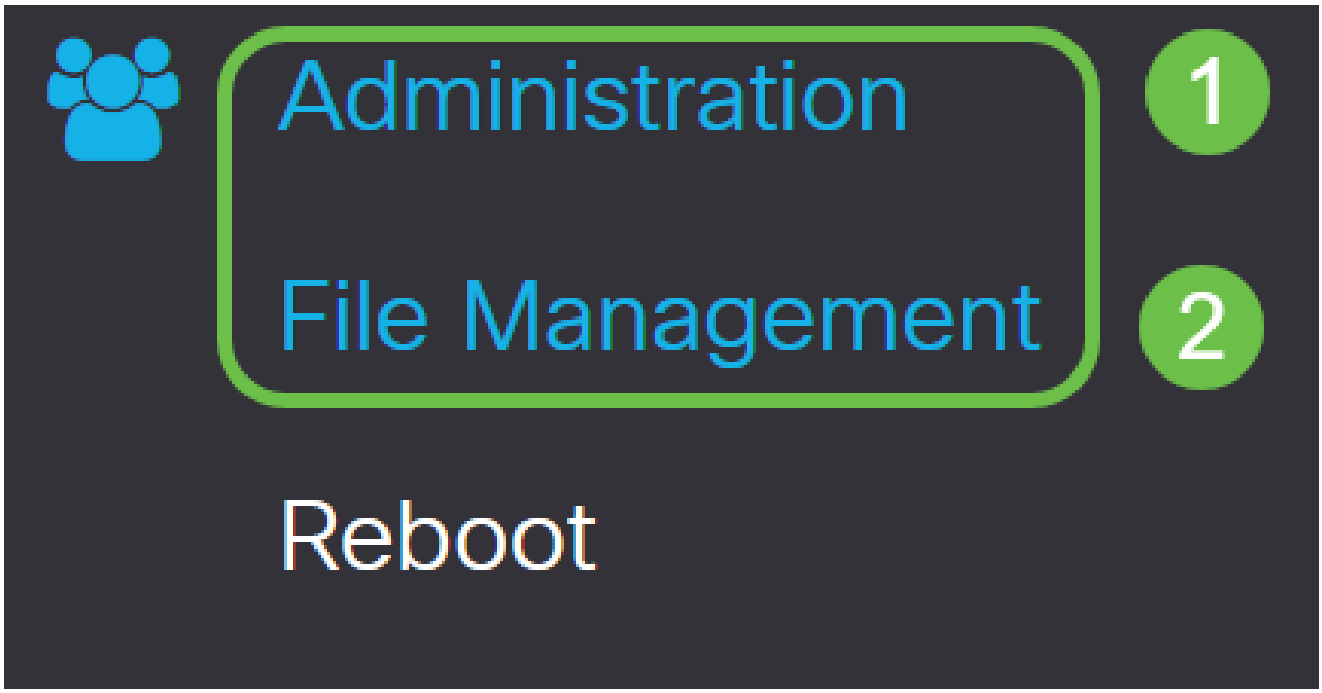


Atualize o firmware se necessário

Essa é uma etapa importante, não ignore-a!

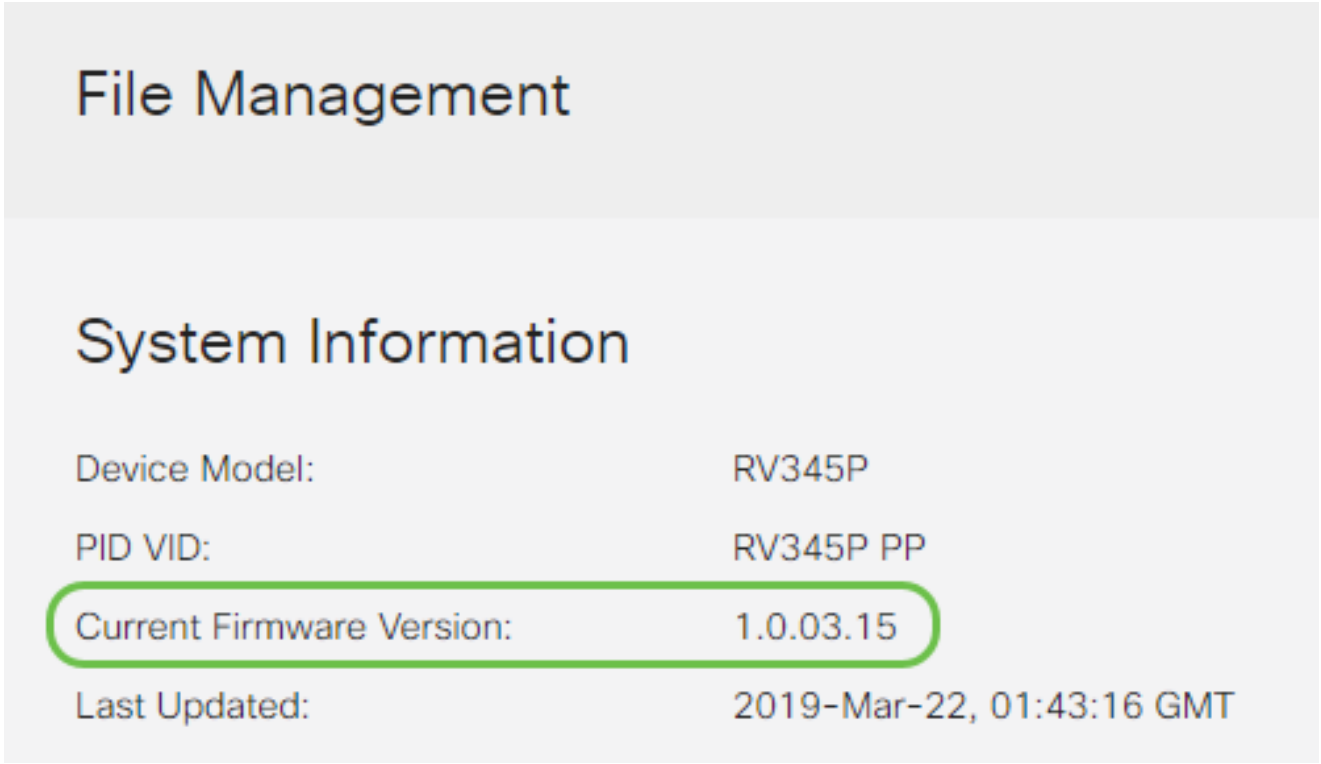
Passo 1

Escolha Administração > Gerenciamento de arquivos.



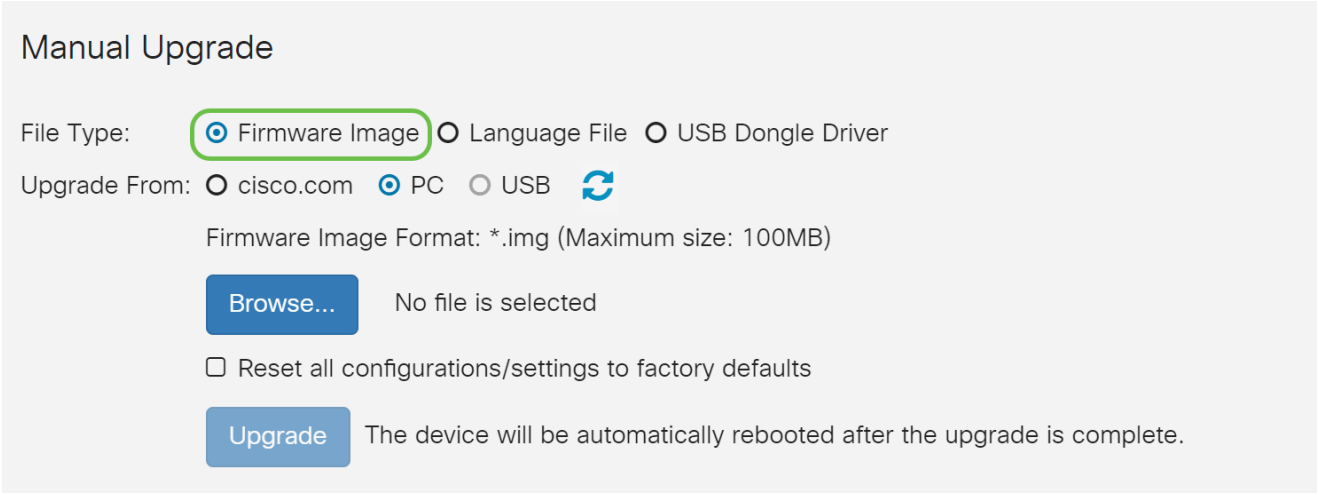
Na área Informações do sistema, as seguintes subáreas descrevem o seguinte:

- Modelo do dispositivo - Exibe o modelo do seu dispositivo.
- PID VID - ID do produto e ID do fornecedor do roteador.
- Versão atual do firmware - Firmware atualmente em execução no dispositivo.
- Versão mais recente disponível em Cisco.com - A 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.



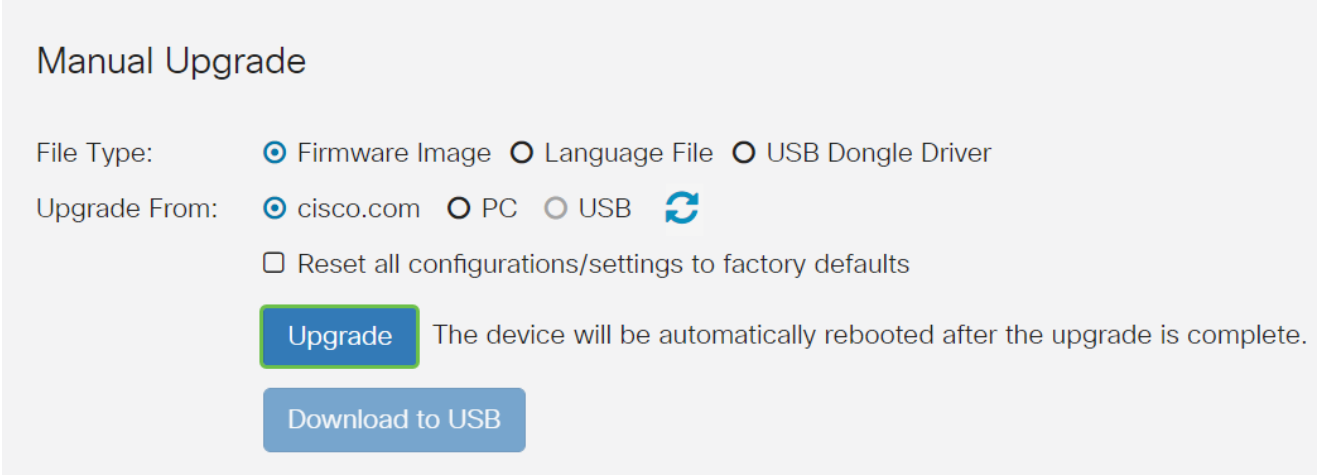
Etapa 3

Na página Manual Upgrade, clique no botão de opção para selecionar cisco.com. Há algumas outras opções para isso, mas essa é a maneira mais fácil de fazer uma atualização. Esse processo instala o arquivo de atualização mais recente diretamente da página da Web Downloads de software da Cisco.

Se o seu dispositivo não estiver conectado à Internet ou estiver sofrendo com desconexões de Internet, você não poderá atualizar de cisco.com. Se isso pertencer a você, opções alternativas podem ser encontradas aqui.

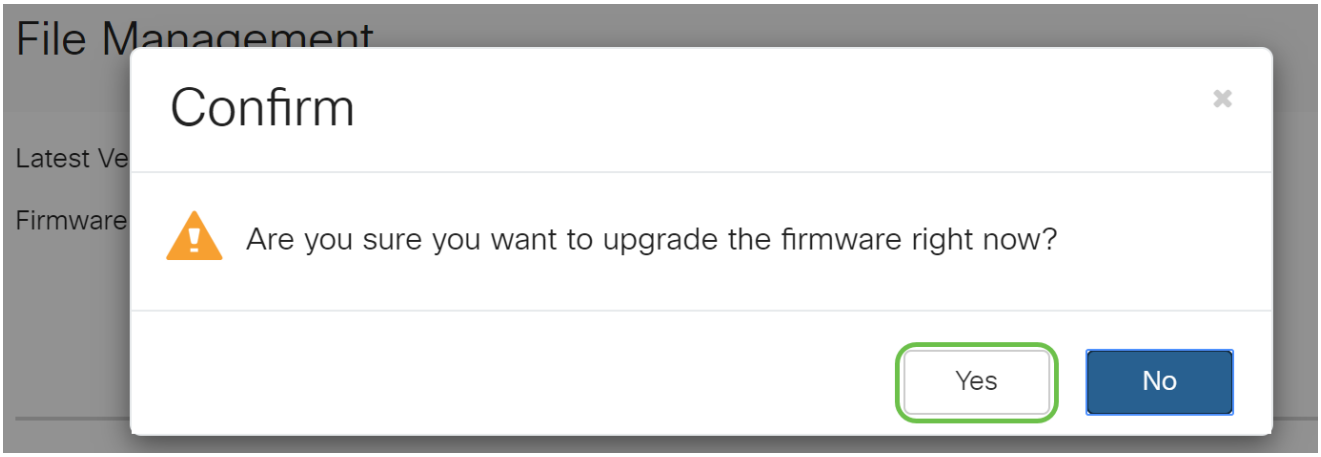
Passo 4

Clique em Upgrade.

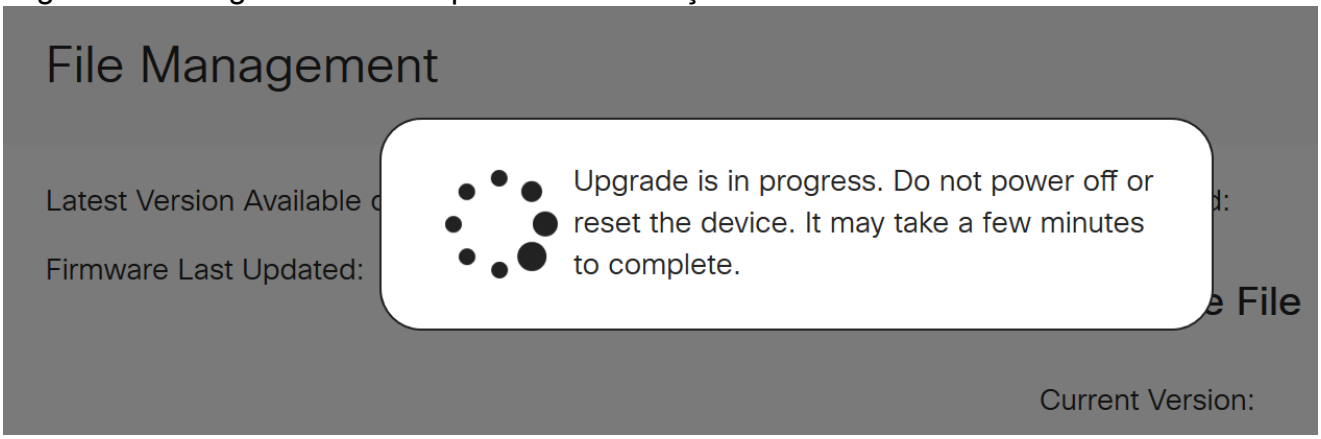


Etapa 5

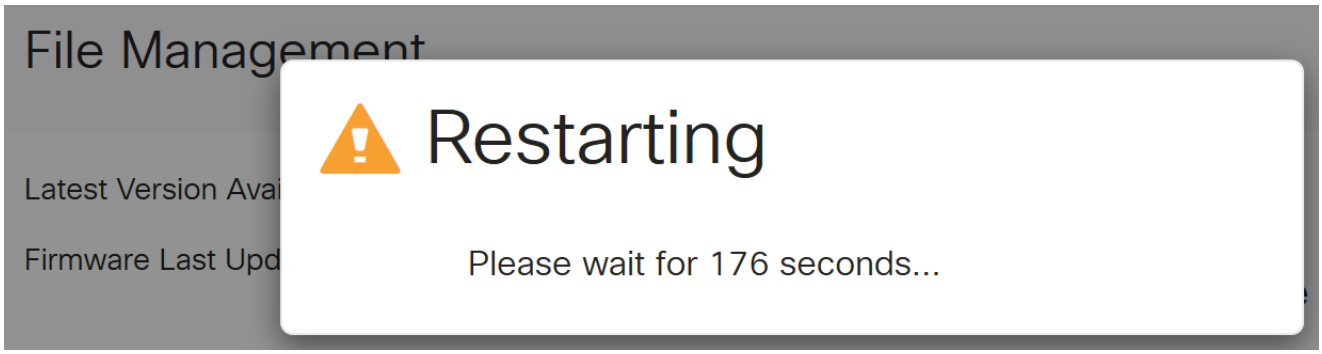
Clique em Sim na janela de confirmação para continuar.



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

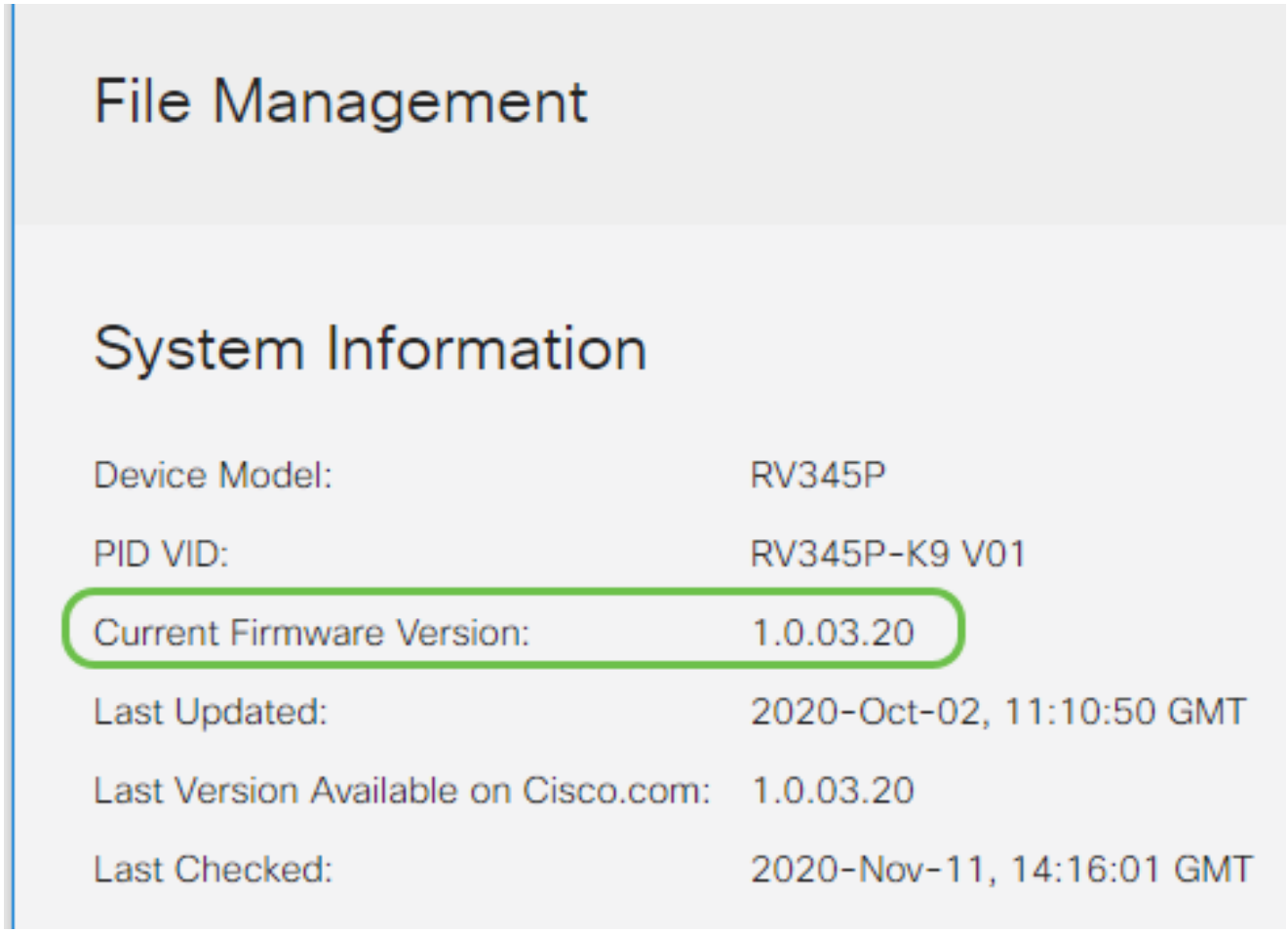


Após a conclusão da atualização, uma janela de notificação será exibida para informá-lo de que o roteador será reinicializado com uma contagem regressiva do tempo estimado para a conclusão do processo. Depois disso, você será desconectado.



Etapa 6

Efetue login novamente no utilitário baseado na Web para verificar se o firmware do roteador foi atualizado. Role até System Information. A área Versão atual do firmware deve agora exibir a versão atualizada do firmware.



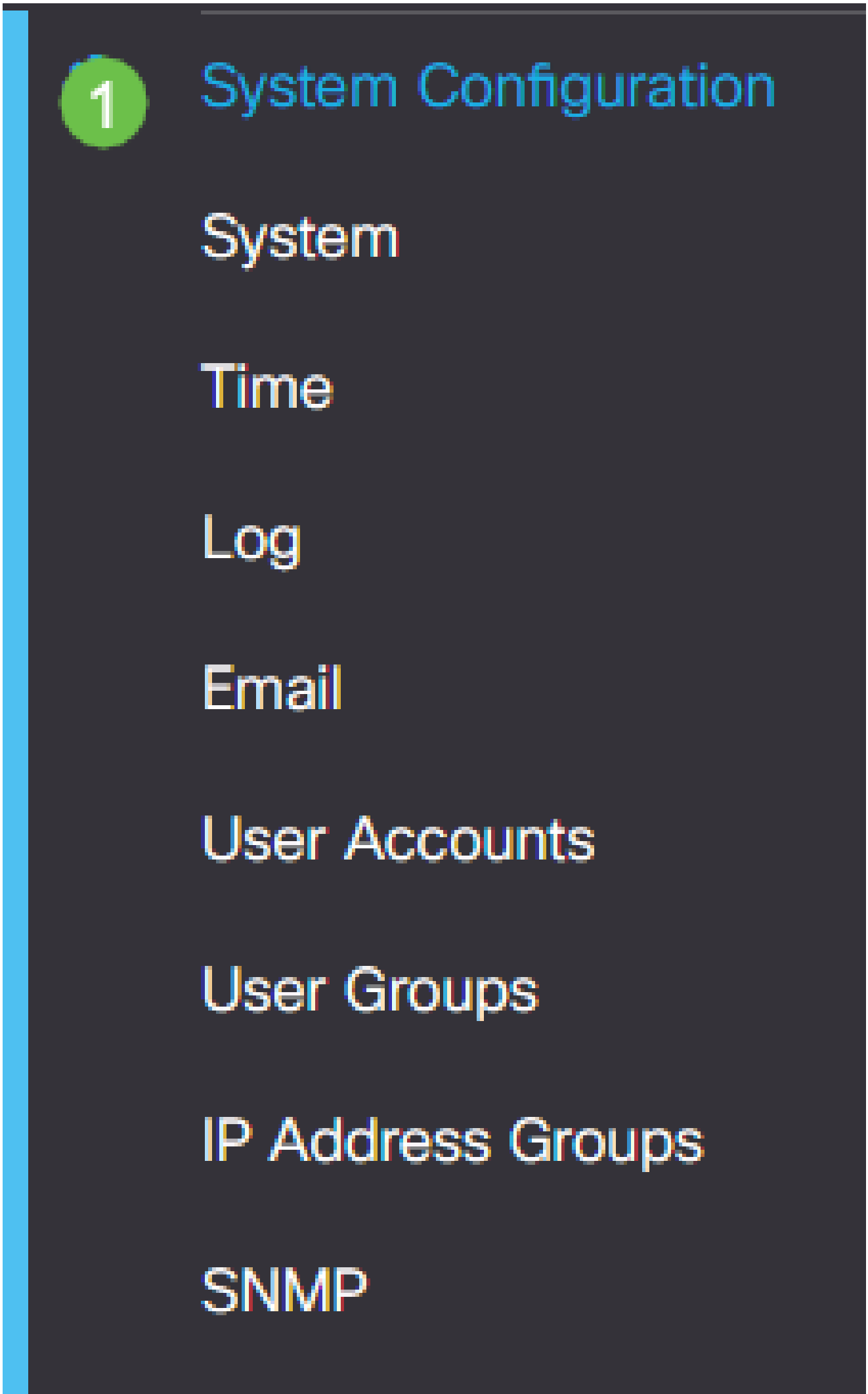
Configure as atualizações automáticas no roteador série RV345P

Como as atualizações são muito importantes e você é uma pessoa ocupada, faz sentido configurar as atualizações automáticas daqui em diante!

Passo 1

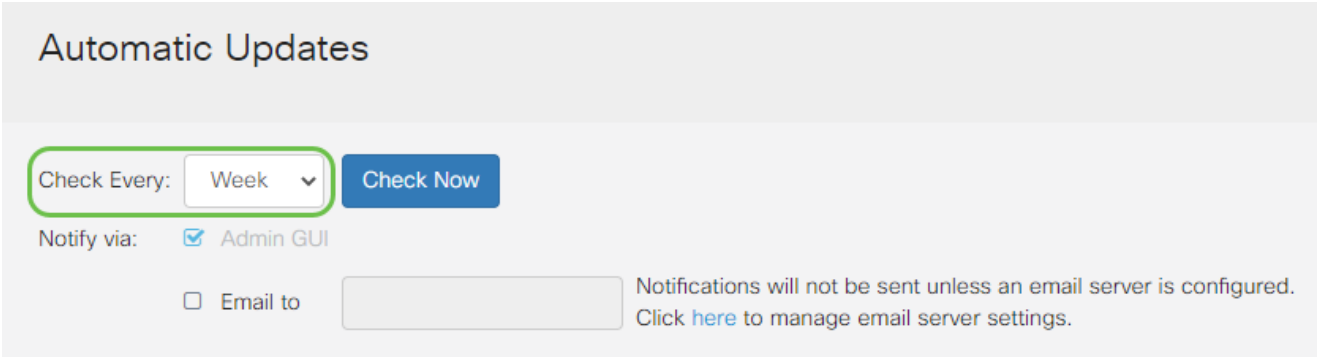
Efetue login no utilitário baseado na Web e escolha System Configuration > Automatic

Updates.


1
System Configuration
System
Time
Log
Email
User Accounts
User Groups
IP Address Groups
SNMP

Passo 2

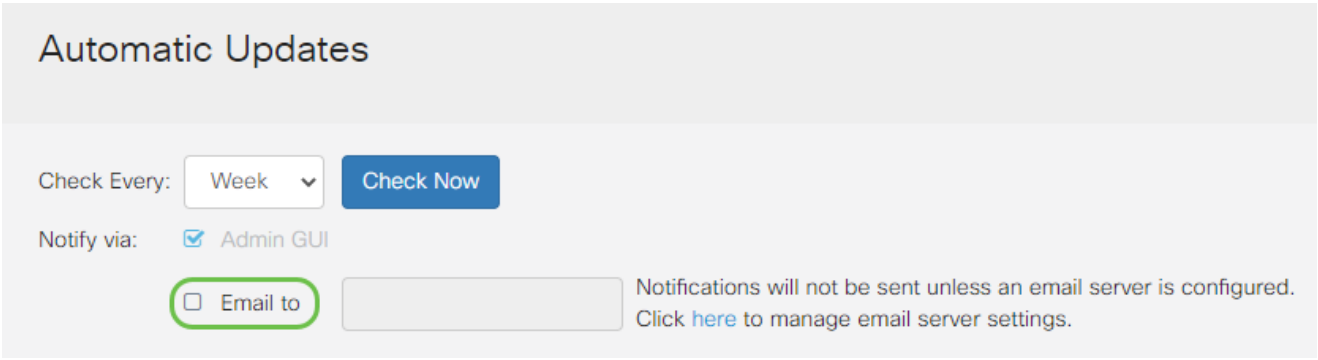
Na lista suspensa Verificar a cada, escolha com que frequência o roteador deve verificar se há atualizações.



Etapa 3

Na área Notify via, marque a caixa de seleção Email to para receber atualizações por e-mail. A caixa de seleção Admin GUI é ativada por padrão e não pode ser desativada. Uma notificação será exibida na configuração baseada na Web assim que uma atualização estiver disponível.

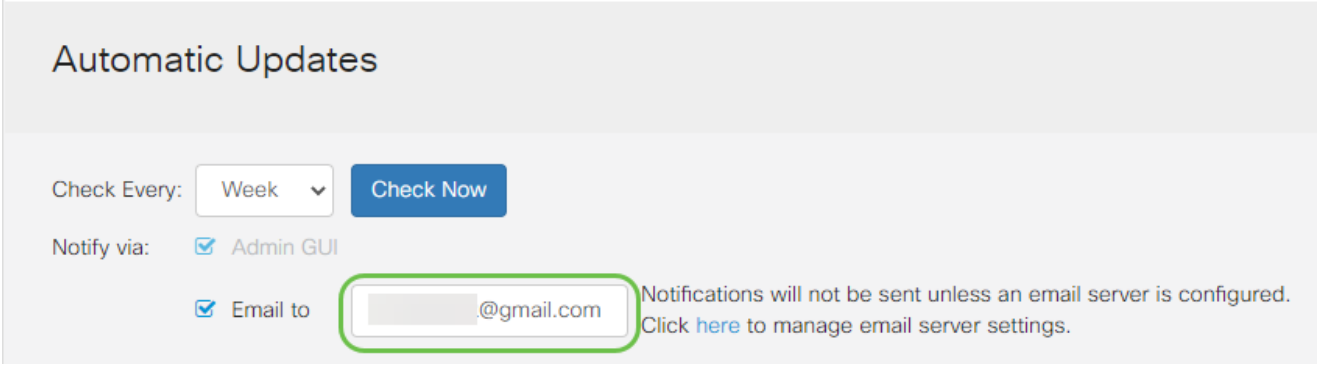
Se quiser definir as configurações do servidor de e-mail, clique aqui para saber como.



Passo 4

Insira um endereço de e-mail no campo Email to address (Endereço de e-mail).

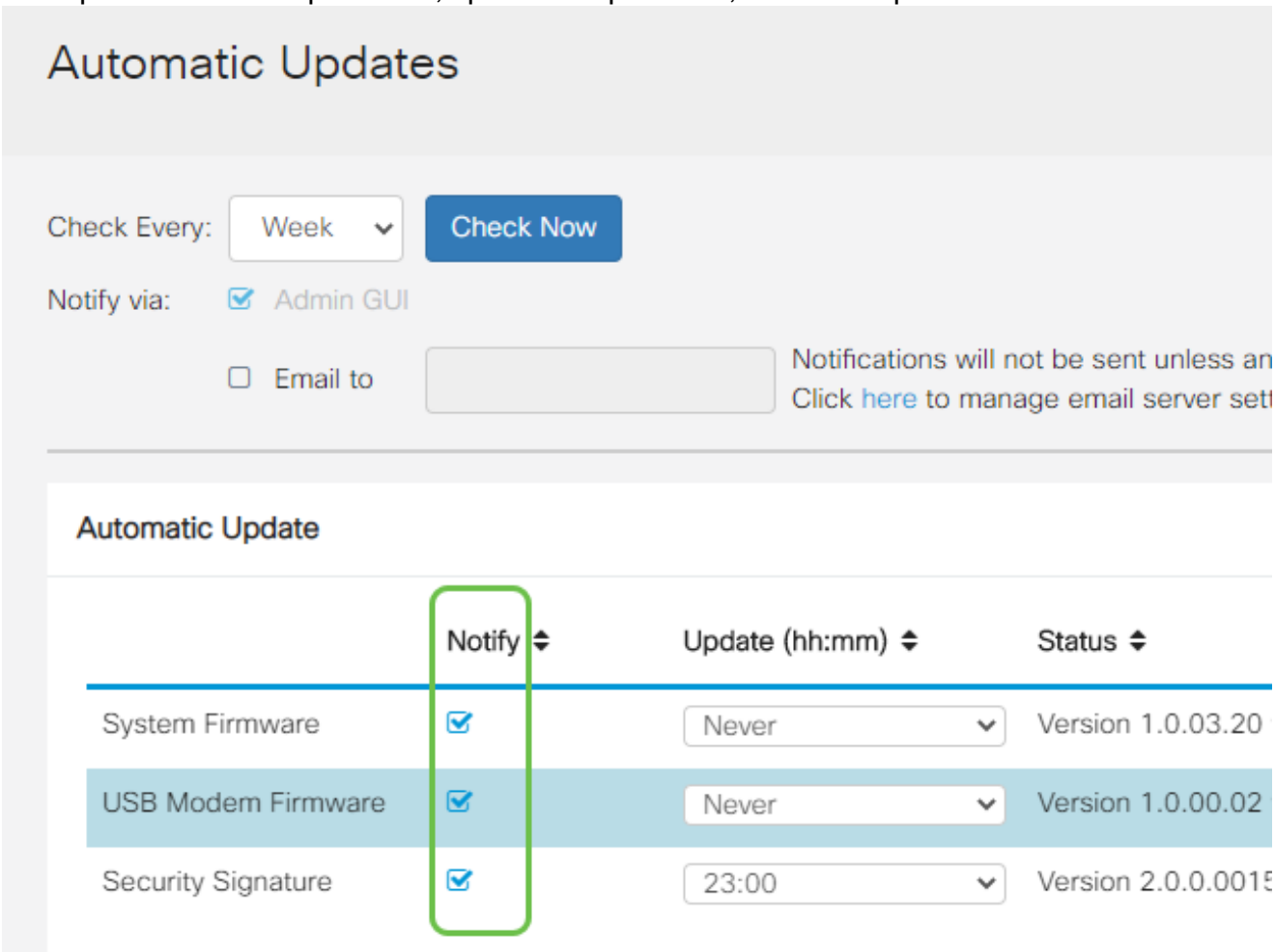
É altamente recomendável usar uma conta de e-mail separada em vez de usar seu e-mail pessoal para manter a privacidade.



Etapa 5

Na área Atualização automática, marque as caixas de seleção Notificar do tipo de atualização sobre a qual você deseja ser notificado. As opções são:

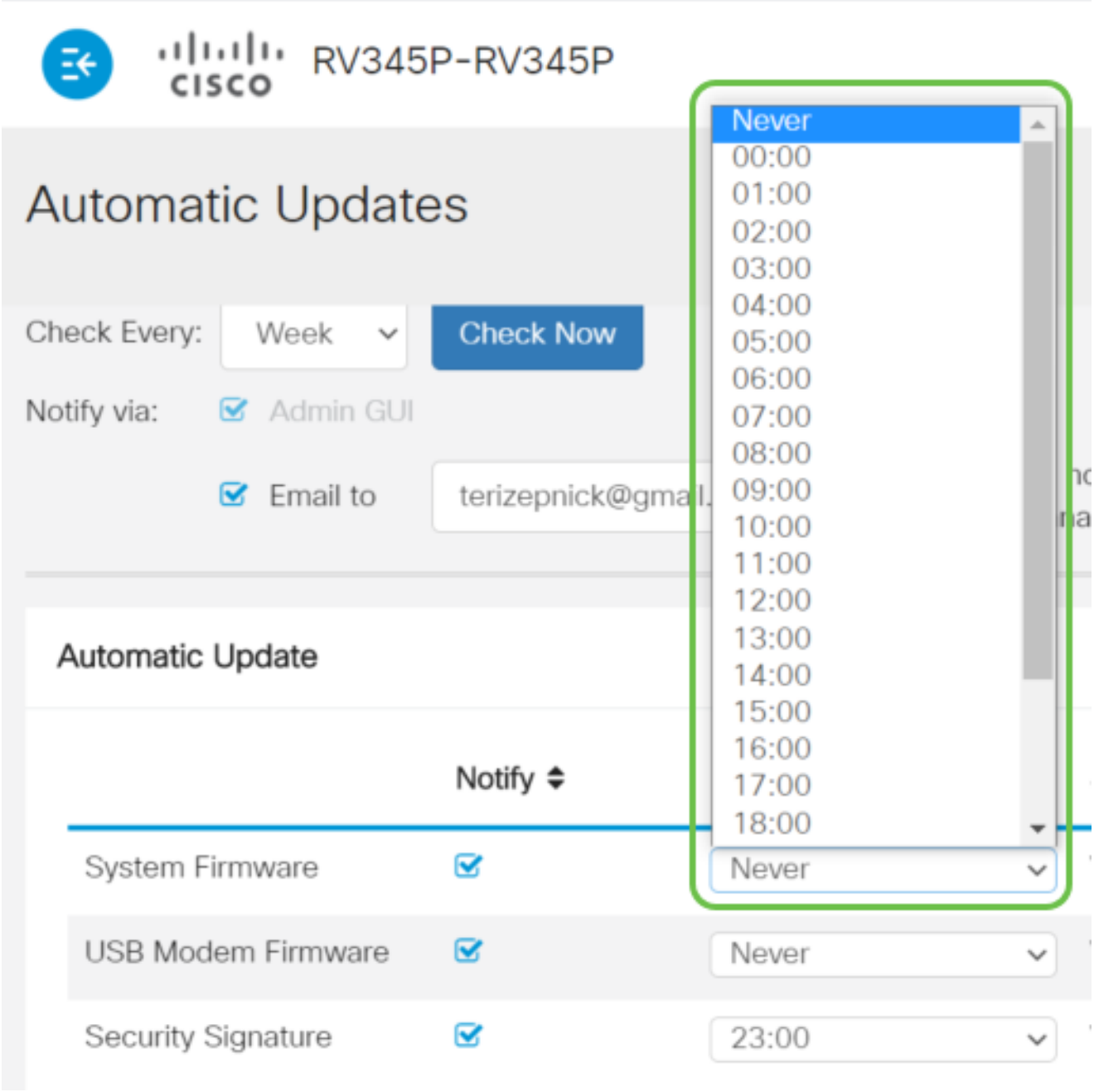
- Firmware do sistema — O principal programa de controle do dispositivo.
- Firmware do modem USB — O programa ou driver de controle da porta USB.
- Assinatura de segurança — Ela conterá assinaturas para o Controle de aplicativos para identificar aplicativos, tipos de dispositivos, sistemas operacionais etc.



Etapa 6

Na lista suspensa Atualização automática, escolha uma hora do dia em que deseja que a

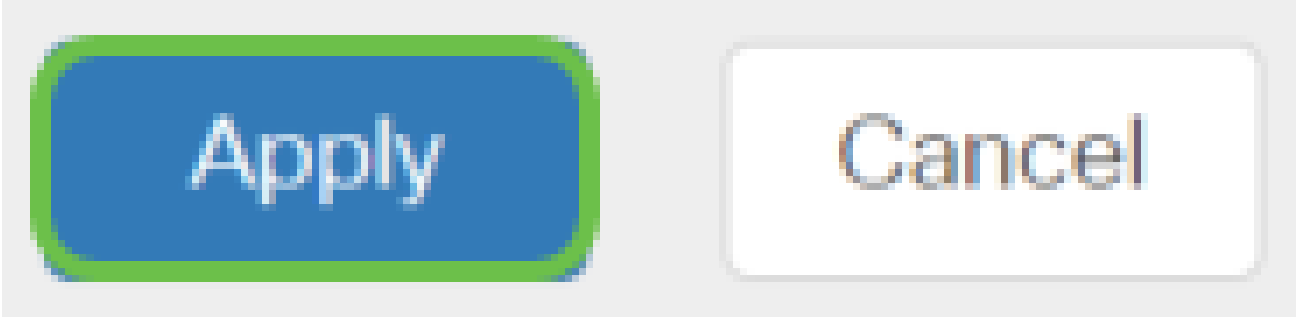
atualização automática seja feita. Algumas opções podem variar de acordo com o tipo de atualização escolhido. A assinatura de segurança é a única opção a ter uma atualização imediata. É recomendável definir uma hora para o fechamento do escritório, para que o serviço não seja interrompido em um momento inconveniente.



O status exibe a versão atualmente em execução do firmware ou a assinatura de segurança.

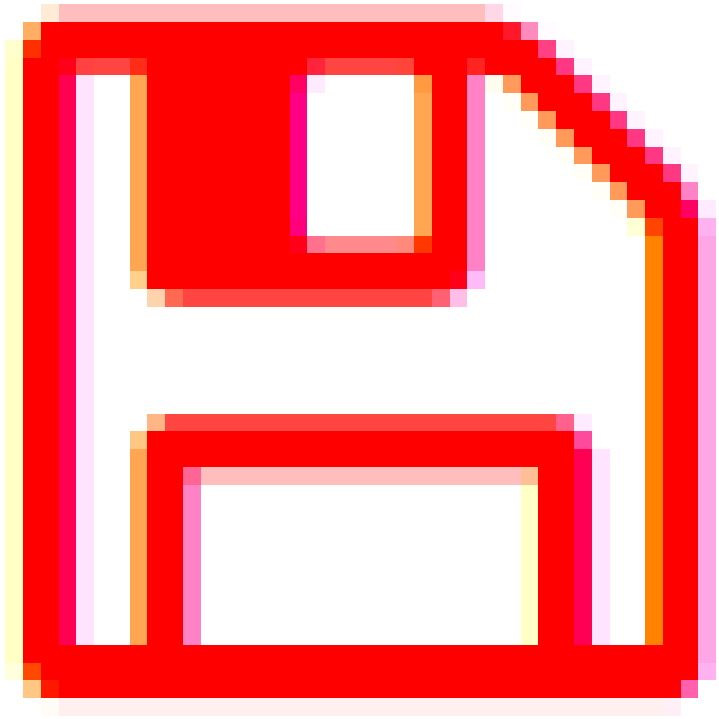
Etapa 7

Clique em Apply.



Passo 8

Para salvar a configuração permanentemente, vá para a página Copiar/Salvar configuração ou clique no ícone salvar na parte superior da página.



Incrível, suas configurações básicas no roteador estão completas! Agora você tem algumas opções de configuração para explorar.

Opções de segurança

É claro que você deseja que sua rede esteja segura. Existem algumas opções simples, como ter uma senha complexa, mas se você quiser tomar medidas para uma rede ainda mais segura, consulte esta seção sobre segurança.

Licença de segurança RV (opcional)

Este recurso de licença de segurança RV protege a sua rede contra ataques da Internet:

- Sistema de prevenção contra invasões (IPS): inspeciona pacotes, registros e/ou bloqueia uma ampla gama de ataques à rede. Ele oferece maior disponibilidade de rede, remediação mais rápida e proteção abrangente contra ameaças.
- Antivírus: proteção contra vírus verificando os aplicativos em busca de vários protocolos, como HTTP, FTP, anexos SMTP de e-mail, anexos POP3 de e-mail e anexos IMAP de e-mail passando pelo roteador.
- Segurança da Web: permite a eficiência e a segurança dos negócios enquanto se conecta à Internet, permite políticas de acesso à Internet para dispositivos finais e aplicativos da Internet para ajudar a garantir desempenho e segurança. Ele é baseado em nuvem e contém mais de 80 categorias com mais de 450 milhões de domínios classificados.
- Identificação de aplicativos: identifique e atribua políticas a aplicativos da Internet. 500 aplicativos exclusivos são identificados automaticamente.
- Identificação do cliente: identifica e categoriza clientes dinamicamente. A capacidade de atribuir políticas com base na categoria do dispositivo final e no sistema operacional.

A Licença RV Security oferece filtragem da Web. A filtragem da Web é um recurso que permite gerenciar o acesso a sites inadequados. Ele pode filtrar as solicitações de acesso à Web de um cliente para determinar se permite ou nega esse site.

Os recursos de segurança licenciados podem ser testados gratuitamente por 90 dias. Se desejar continuar usando os recursos de segurança avançados no roteador após o período de avaliação, você deverá adquirir e ativar uma licença.

Outra opção de segurança é o Cisco Umbrella. Clique aqui para ir para a seção Umbrella.

Se você não quiser nenhuma licença de segurança, clique para ir para a seção VPN deste documento.

Introdução às Smart Accounts

Para adquirir a Licença RV Security, você precisa de uma Smart Account.

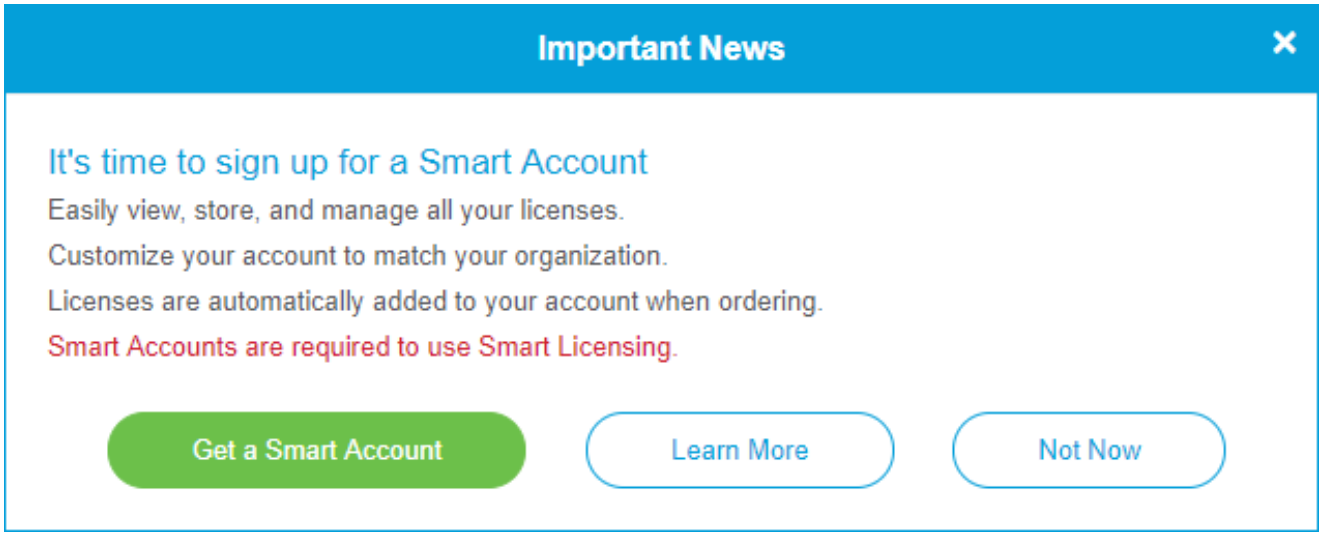
Ao autorizar a ativação desta Smart Account, você concorda que está autorizado a criar contas e gerenciar direitos de produtos e serviços, contratos de licença e acesso de usuário a contas em nome da sua organização. Os Parceiros da Cisco não podem autorizar a criação de contas em nome dos clientes.

A criação de uma nova Smart Account é um evento único e o gerenciamento a partir desse

ponto é fornecido pela ferramenta.

Crie uma Smart Account

Ao acessar sua conta geral da Cisco usando sua conta Cisco.com, ou ID do CCO (a que você criou no início deste documento), você pode ser recebido por uma mensagem para criar uma Smart Account.



Se você ainda não viu esse pop-up, clique para ir para a página de criação de Smart Account. Talvez seja necessário fazer login com suas credenciais de conta Cisco.com.

Para obter mais detalhes sobre as etapas envolvidas na solicitação de sua Smart Account, clique aqui.

Não deixe de anotar o nome da sua conta junto com outros detalhes de registro.

Dica rápida: se for necessário inserir um domínio e você não tiver um, digite seu endereço de e-mail no formato name@domain.com. Os domínios comuns são gmail, yahoo, etc., dependendo da sua empresa ou provedor.

É muito importante que você tenha uma Conta Cisco.com (ID do CCO) e uma Conta inteligente da Cisco antes de adquirir a Licença de segurança RV.

Comprar Licença de Segurança RV

Você deve comprar uma licença de seu distribuidor ou parceiro da Cisco. Para localizar um parceiro da Cisco, clique aqui.

A tabela abaixo exibe o número da peça da licença.

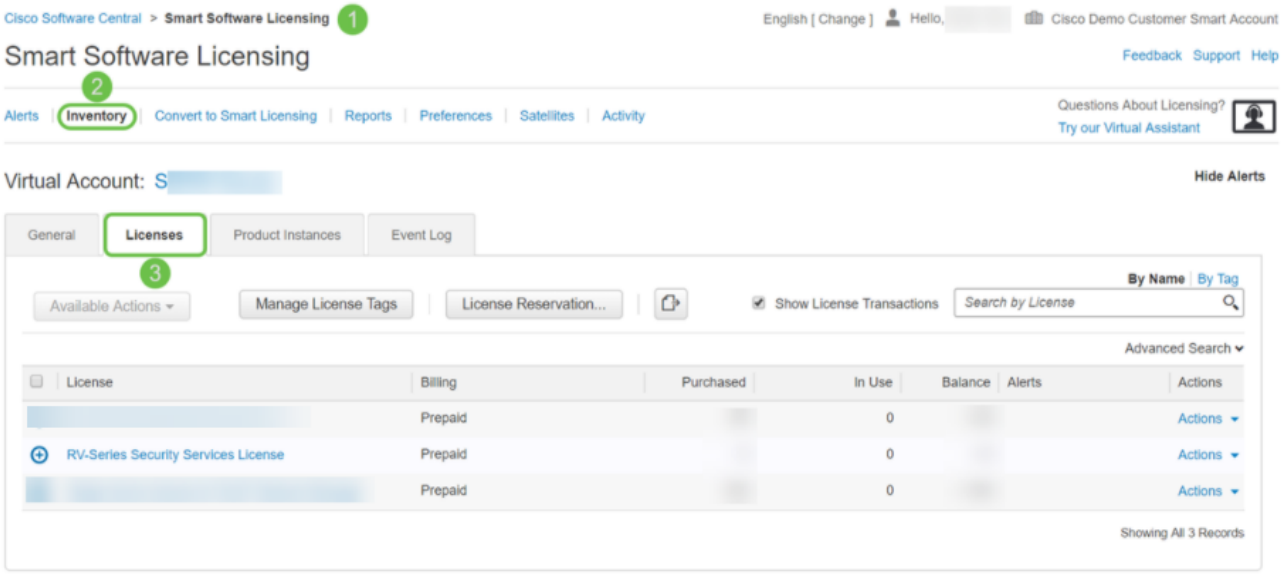
Tipo	ID do produto	Descrição
Licença de segurança RV	LS-RV34X-SEC-1YR=	Segurança RV: 1 ano: Filtro dinâmico da Web, visibilidade de aplicativos, identificação e estatísticas de clientes, antivírus de

Tipo	ID do produto	Descrição
		gateway e IPS de sistema de prevenção contra invasões.

A chave de licença não é inserida diretamente no roteador, mas será atribuída à sua Conta inteligente da Cisco depois que você solicitar a licença. O tempo necessário para que a licença apareça em sua conta depende de quando o parceiro aceita o pedido e quando o revendedor vincula as licenças à sua conta, que geralmente é de 24 a 48 horas.

Confirmar se a licença está na Smart Account

Navegue até a página da sua conta Smart License e clique em Página Smart Software License > Inventory > Licenses.

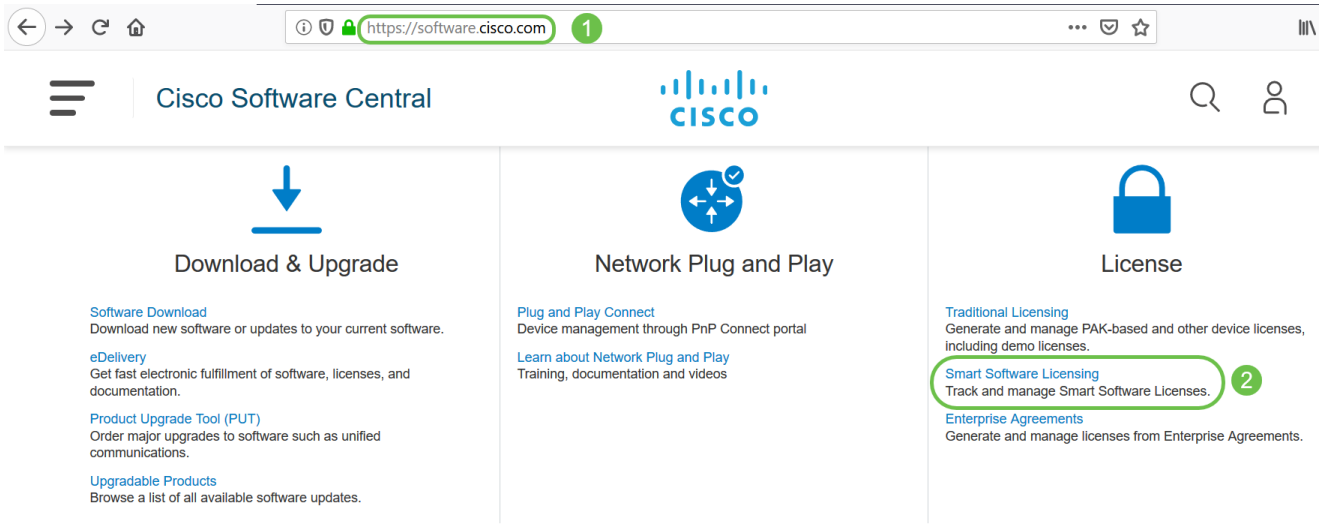


Se você não vir sua licença em sua Smart Account, entre em contato com seu parceiro da Cisco.

Configure a licença de segurança RV no roteador série RV345P

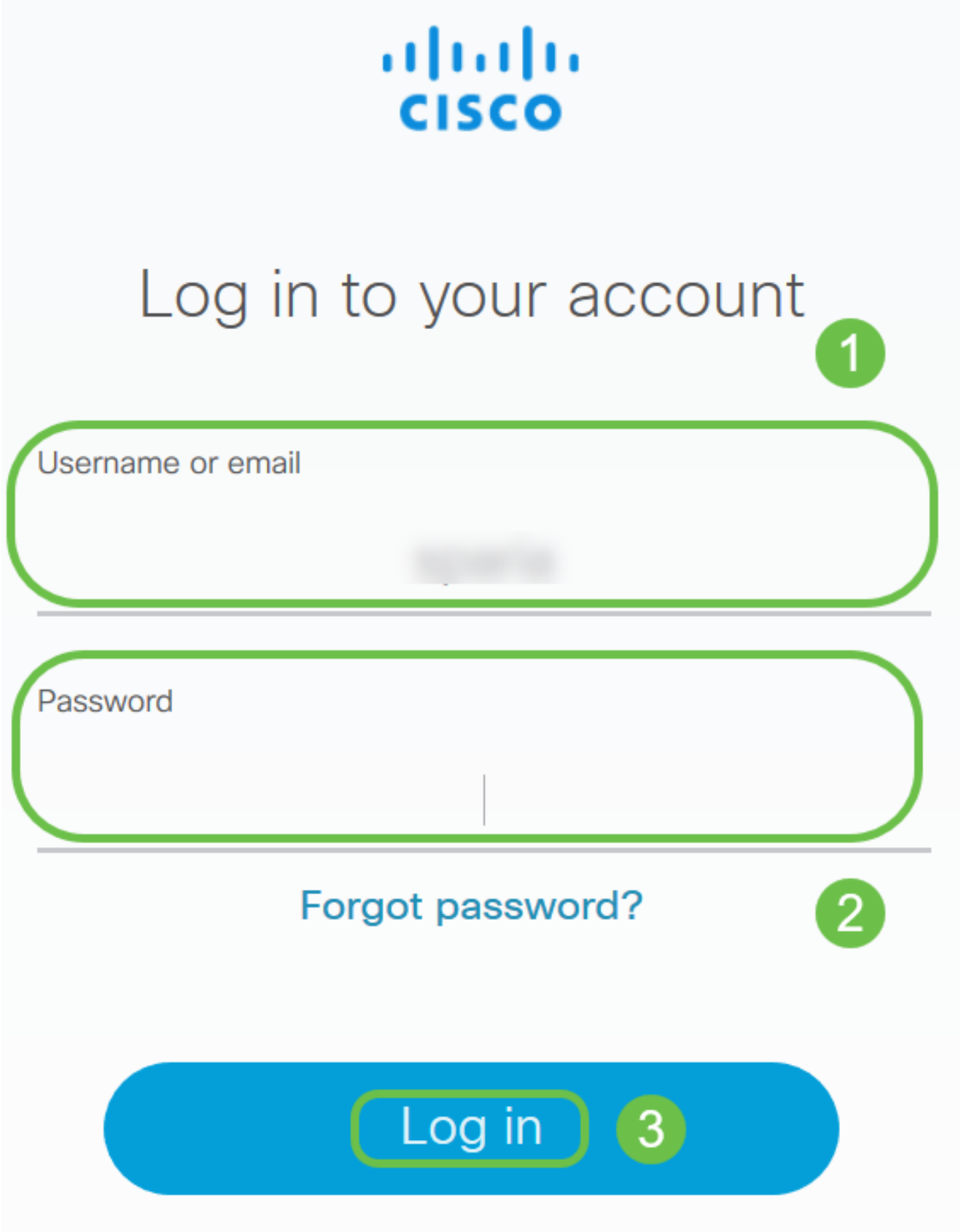
Passo 1

Acesse o Cisco Software e navegue até Smart Software Licensing.



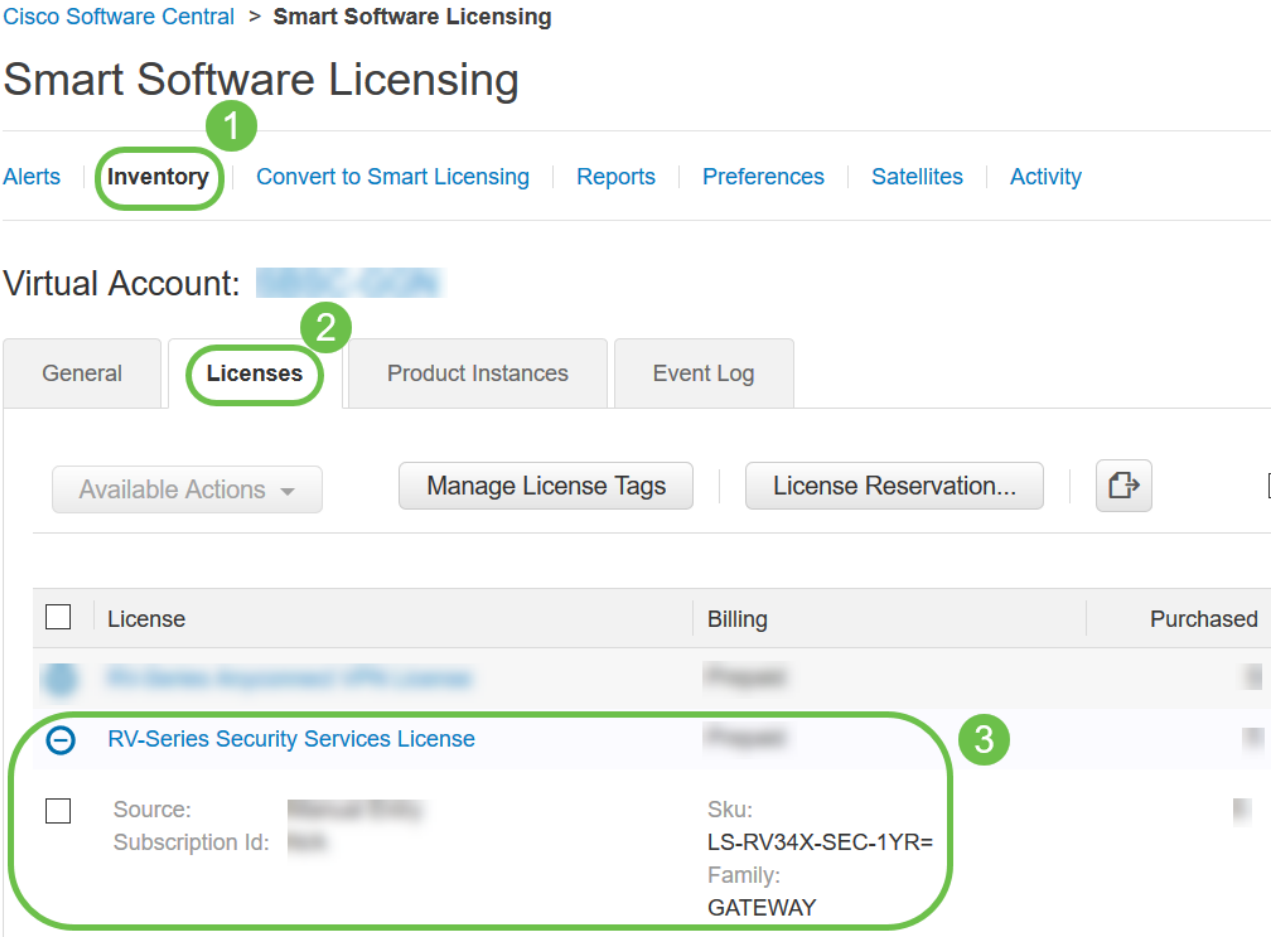
Passo 2

Insira seu nome de usuário ou e-mail e senha para fazer login em sua Smart Account. Clique em Log in.



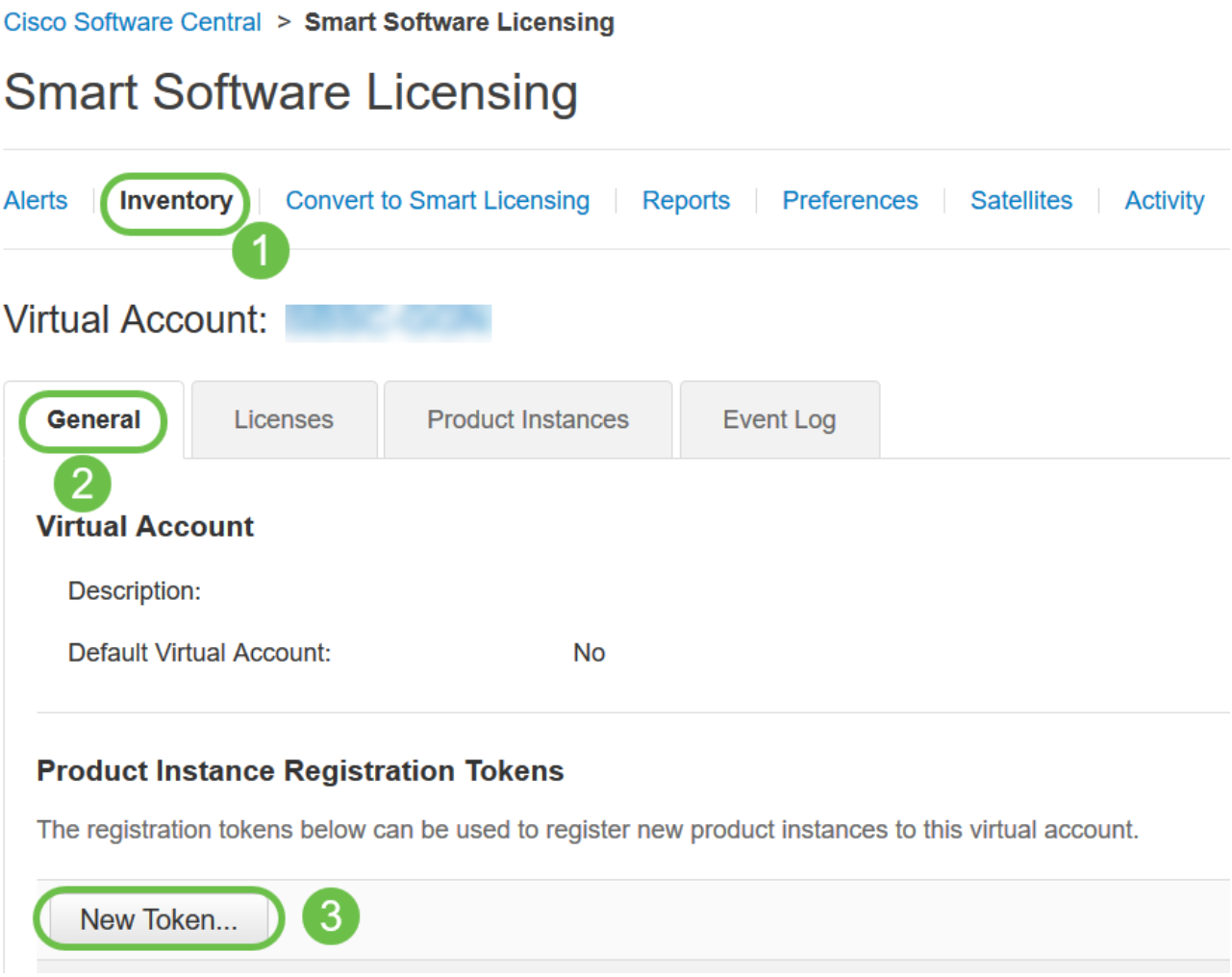
Etapa 3

Navegue para Inventory > Licenses e verifique se a licença de serviços de segurança RV-Series está listada em sua Smart Account. Se você não encontrar a licença listada, entre em contato com seu parceiro da Cisco.



Passo 4

Navegue até Inventário > Geral. Em Product Instance Registration Tokens, clique em New Token.



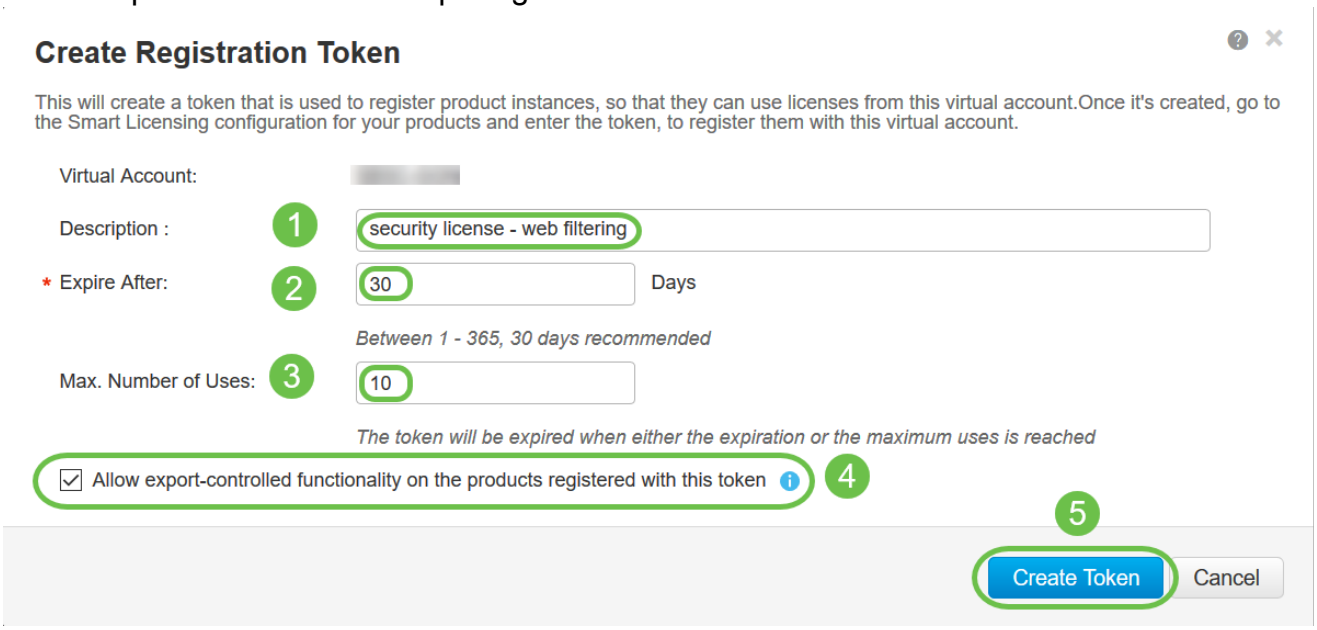
Etapa 5

A janela Create Registration Token (Criar token de registro) será exibida. A área Virtual Account exibe a Virtual Account sob a qual o token de registro será criado. Na página Create Registration Token, faça o seguinte:

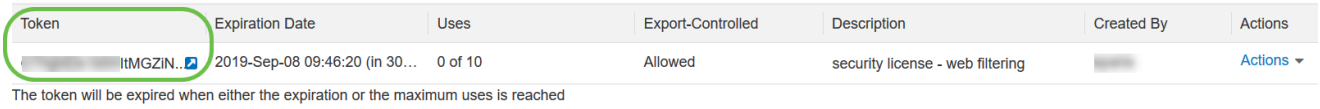
- No campo Descrição, insira uma descrição exclusiva para o token. Neste exemplo, a licença de segurança - filtragem da Web é inserida.
- No campo Expirar após, insira um valor entre 1 e 365 dias. A Cisco recomenda o valor 30 dias para esse campo; no entanto, você pode editar o valor de acordo com suas necessidades.
- No campo Max. Número de Usos insira um valor para definir o número de vezes que você deseja usar esse token. O token expirará quando a quantidade de dias ou o número máximo de usos for atingido.
- Marque a caixa de seleção Permitir funcionalidade de exportação controlada nos produtos registrados com este token para habilitar a funcionalidade de exportação controlada para tokens de uma instância de produto em sua conta virtual. Desmarque a caixa de seleção se não quiser permitir que a funcionalidade de exportação controlada seja disponibilizada para uso com este token. Use essa opção apenas se estiver em conformidade com a funcionalidade de exportação controlada. Alguns recursos de exportação controlada são restritos pelo Departamento de Comércio dos

Estados Unidos. Esses recursos são restritos para produtos registrados usando esse token quando você desmarca a caixa de seleção. Qualquer violação é sujeita a penalidades e encargos administrativos.

- Clique em Create Token para gerar o token.

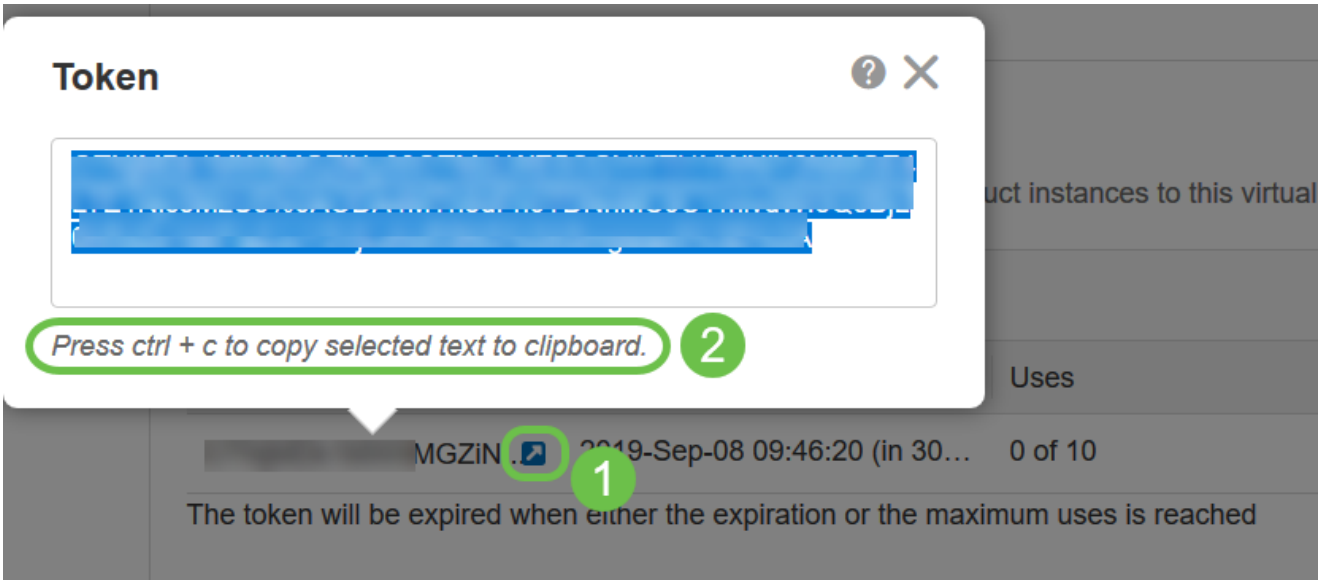


Agora você gerou com êxito um token de registro de instância de produto.



Etapa 6

Clique no ícone de seta na coluna Token, para copiar o token para a área de transferência, pressione ctrl + c no teclado.

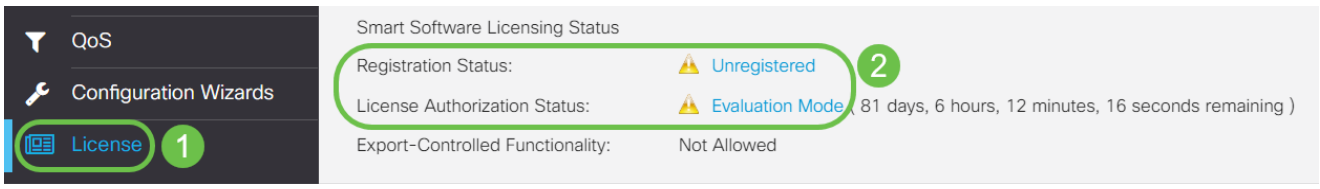


Etapa 7 (opcional)

Clique no menu suspenso Actions, escolha Copy para copiar o token para a área de transferência ou Download... para baixar uma cópia do arquivo de texto do token do qual você pode copiar.

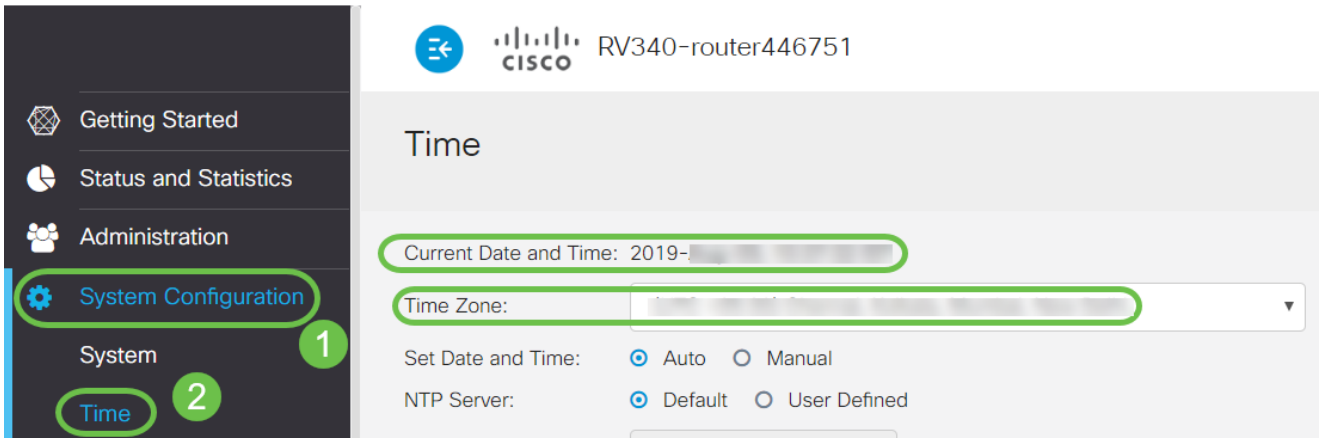
Passo 8

Navegue até License e verifique se o Registration Status está sendo mostrado como Unregistered e License Authorization Status está sendo mostrado como Evaluation Mode.



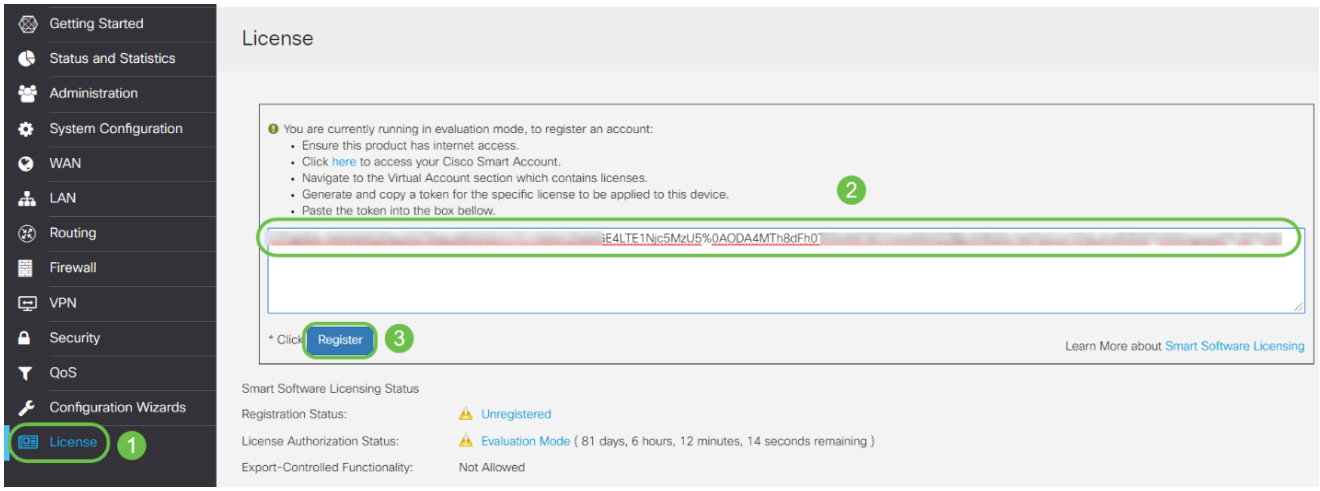
Passo 9

Navegue para System Configuration > Time e verifique se a Current Date and Time e o Time Zone estão refletindo corretamente de acordo com o seu fuso horário.



Passo 10

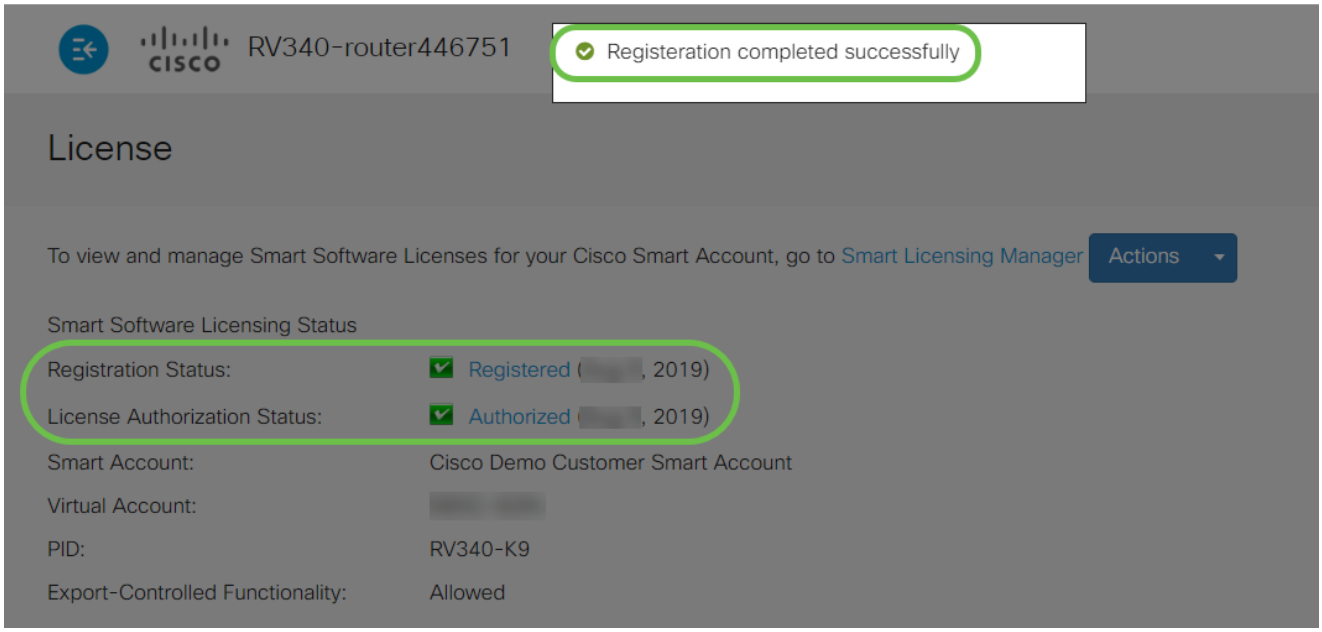
Navegue até License. Cole o token copiado na etapa 6 na caixa de texto sob a guia License selecionando ctrl + v no teclado. Clique em Registrar.



O registro pode levar alguns minutos. Não saia da página quando o roteador tentar entrar em contato com o servidor de licenças.

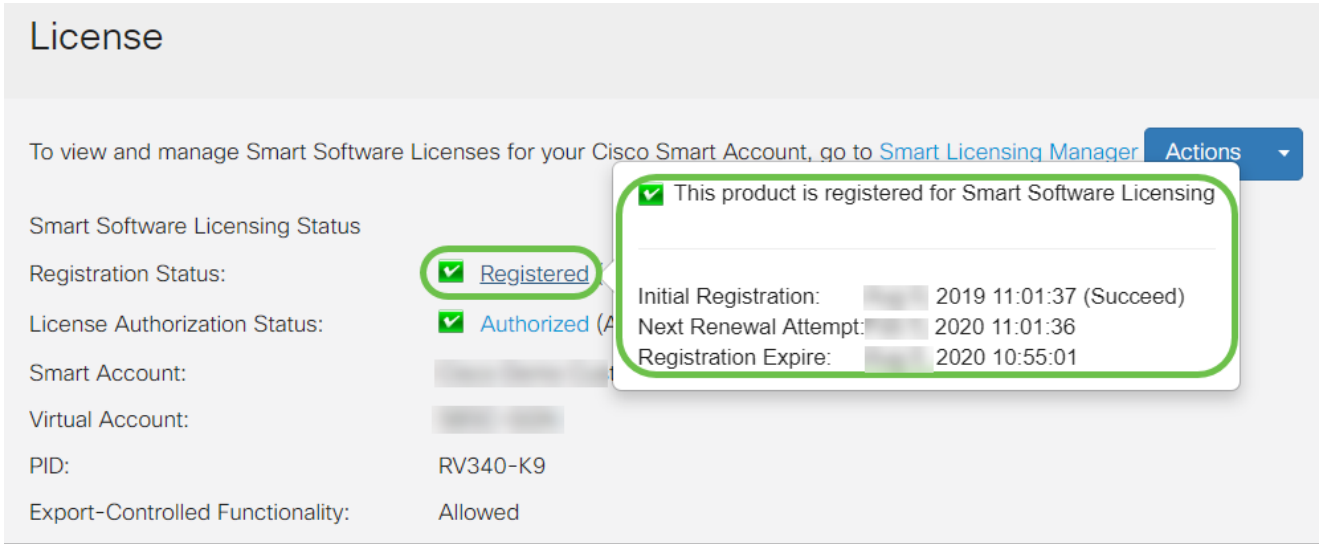
Passo 11

Agora você deve ter registrado e autorizado com êxito seu roteador série RV345P com uma Smart License. Você receberá uma notificação na tela Registro concluído com êxito. Além disso, você poderá ver que o Status de registro está sendo mostrado como Registered e Status de autorização de licença está sendo mostrado como Authorized.



Etapa 12 (opcional)

Para exibir mais detalhes do Status de registro da licença, passe o ponteiro sobre o status Registered. Uma mensagem de diálogo é exibida com as seguintes informações:

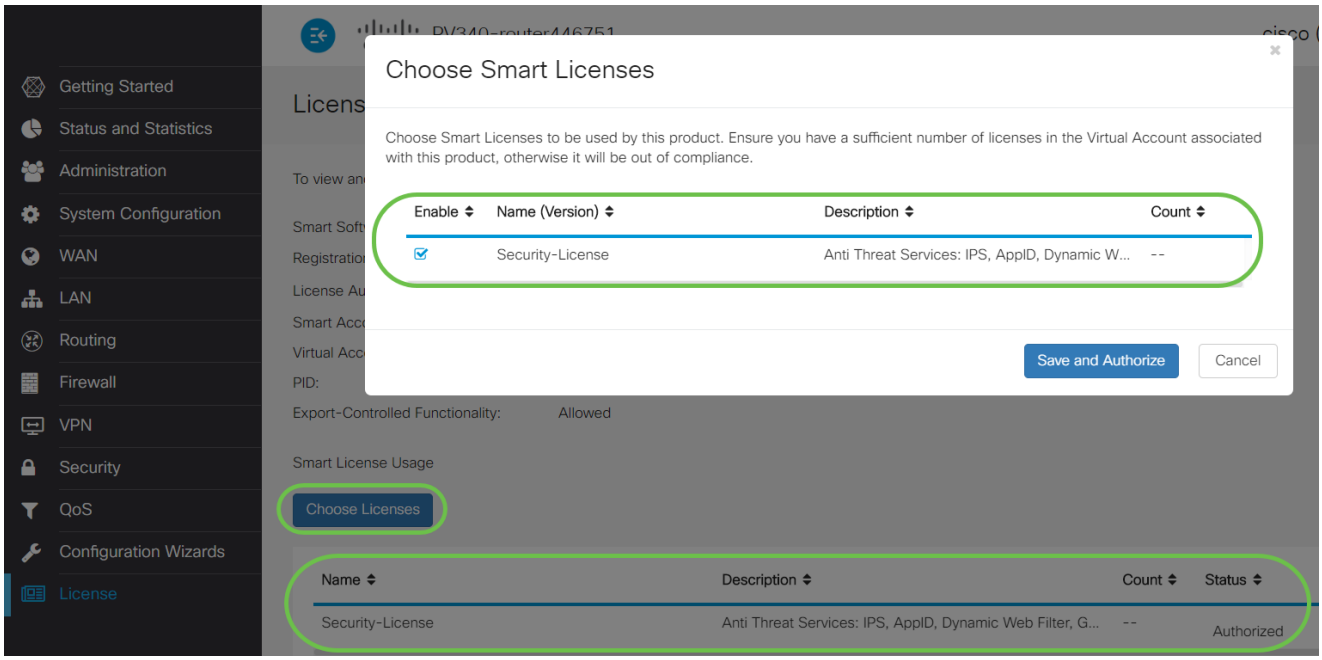


- Registro inicial — Esta área indica a data e a hora em que a licença foi registrada.
- Próxima tentativa de renovação — Esta área indica a data e a hora em que o roteador tentará renovar a licença.
- Registration Expire (Expiração do registro) — Esta área indica a data e a hora de expiração do registro.

Passo 13

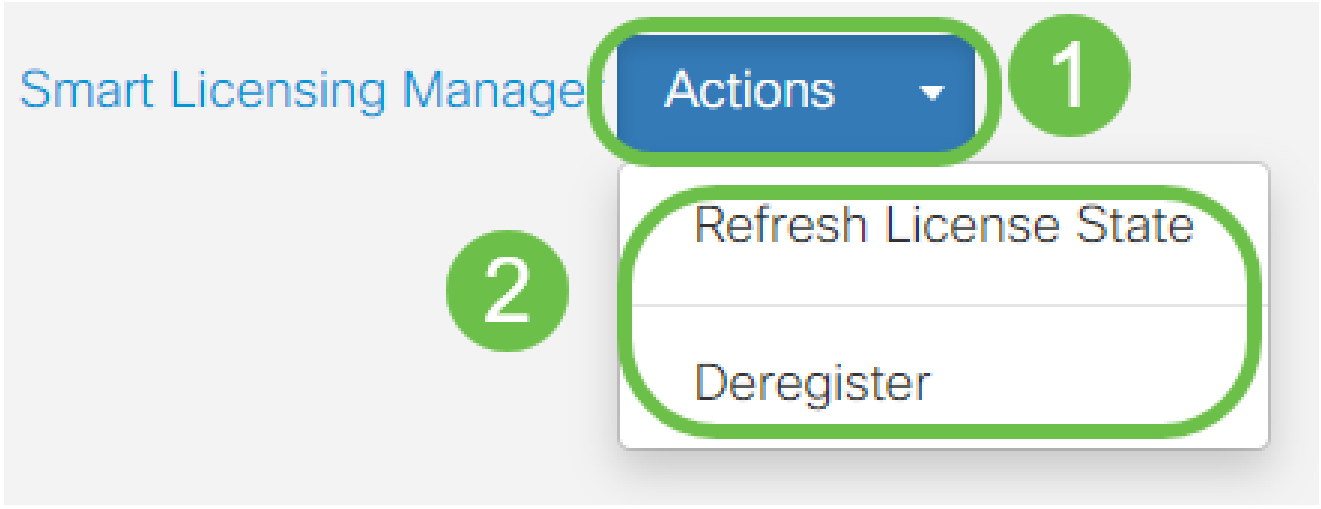
Na página License, verifique se o status Security-License está exibindo Authorized. Você também pode clicar no botão Escolher licença para verificar se a Licença de segurança está habilitada.

Se tiver algum problema nesta etapa, talvez seja necessário reinicializar o roteador.



Etapa 14 (opcional)

Para Atualizar o estado da licença ou Cancelar o registro da licença do roteador, clique no menu suspenso Ações do Gerenciador de Smart Licensinge selecione um item de ação.



Agora que você tem sua licença no roteador, é necessário concluir as etapas na próxima seção.

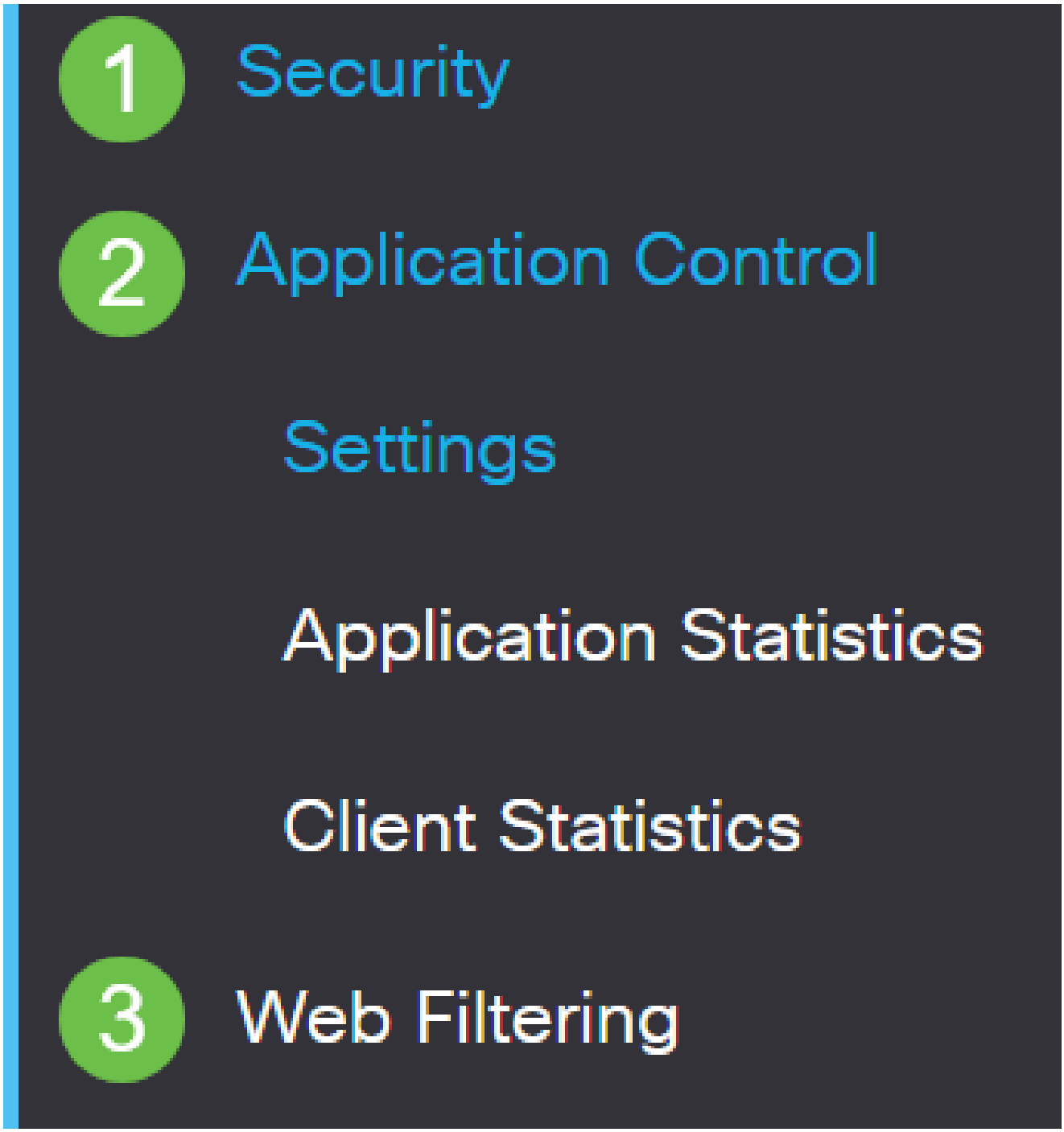
Filtragem da Web no roteador RV345P

Você tem 90 dias após a ativação para usar a filtragem da Web gratuitamente. Após a avaliação gratuita, se desejar continuar usando esse recurso, você precisará comprar uma licença. Clique para voltar para essa seção.

Passo 1

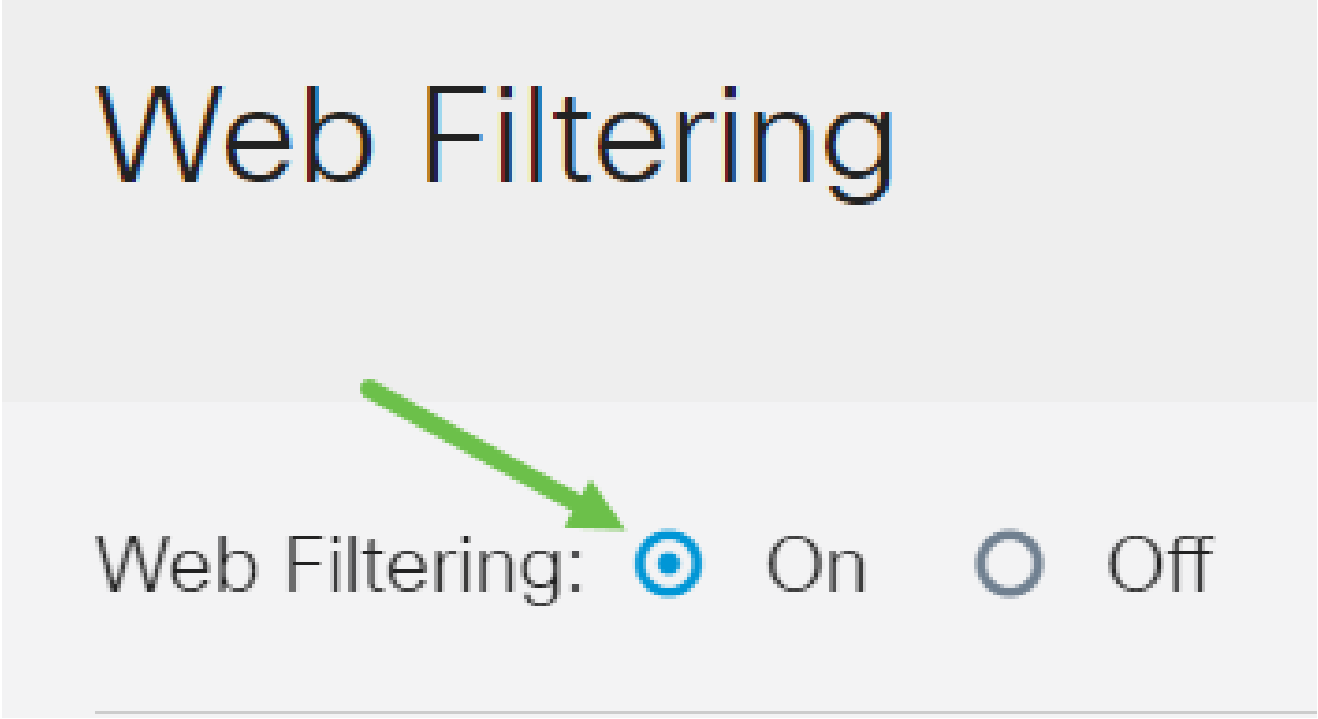
Efetue login no utilitário baseado na Web e escolha Security > Application Control > Web

Filtering.



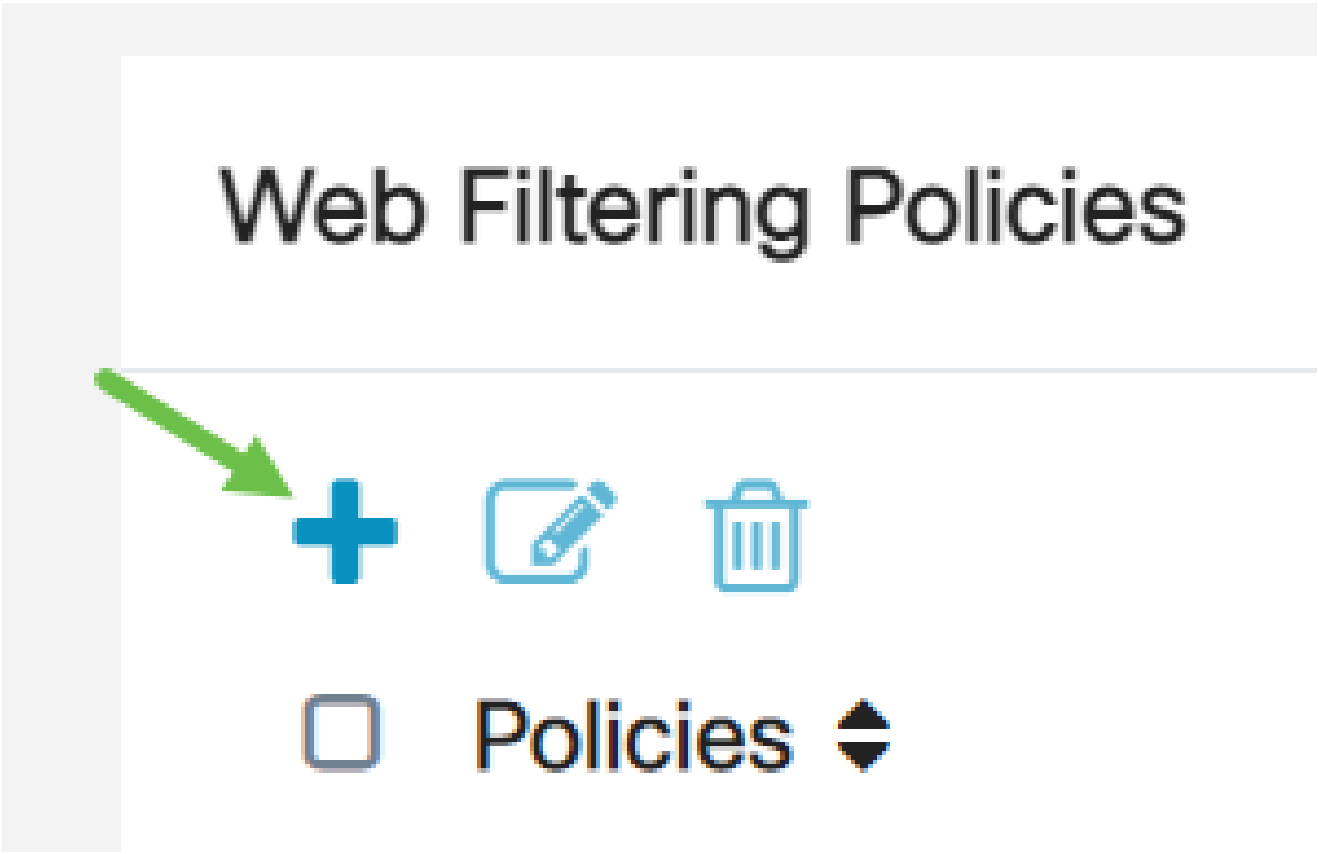
Passo 2

Selecione o botão de opção On.



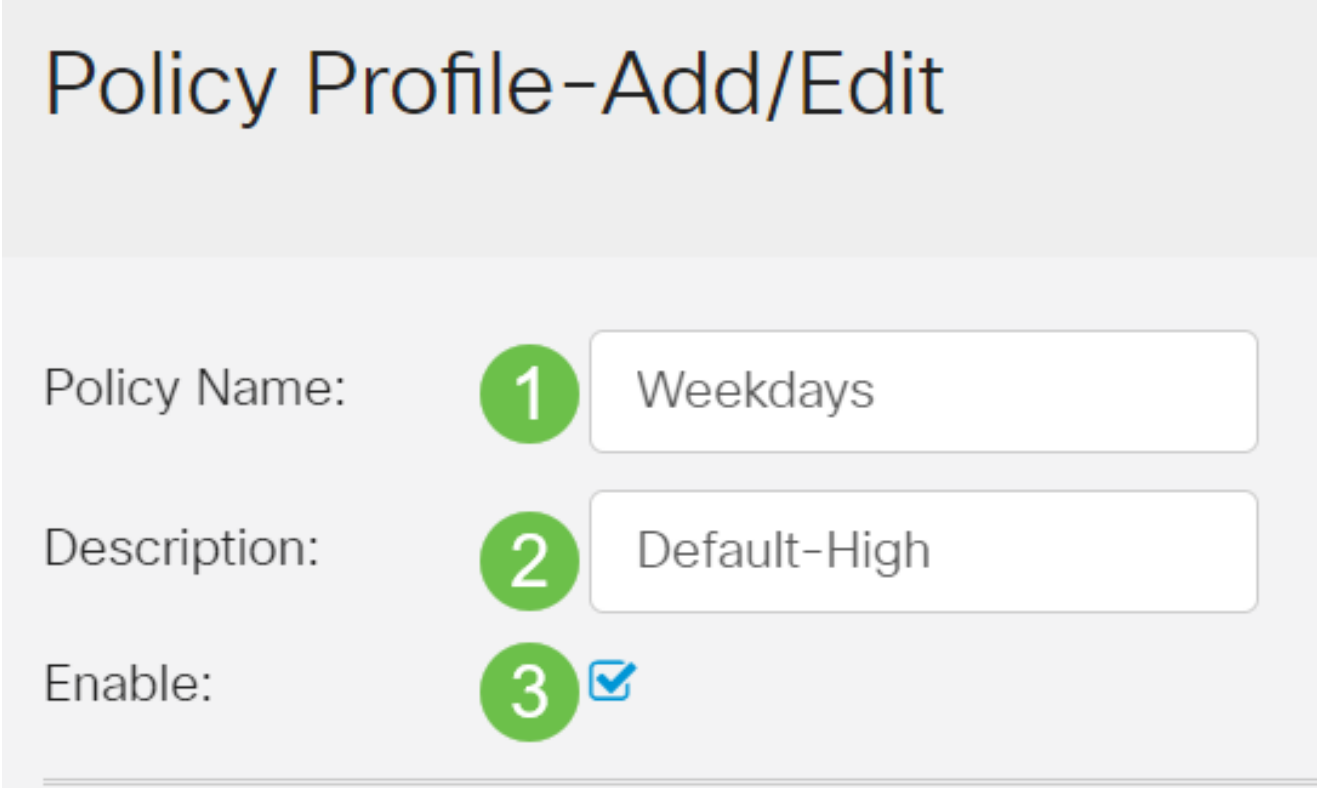
Etapa 3

Clique no ícone adicionar.



Passo 4

Insira um Nome da política, Descrição e a caixa de seleção Habilitar.



Se a Filtragem de conteúdo estiver habilitada no roteador, uma notificação será exibida para informá-lo de que a Filtragem de conteúdo foi desabilitada e que os dois recursos não podem ser habilitados simultaneamente. Clique em Apply para continuar com a configuração.

Etapa 5

Marque a caixa de seleção Web Reputation para habilitar a filtragem com base em um índice de reputação da Web.

O conteúdo será filtrado de acordo com a notoriedade de um site ou URL com base em um índice de reputação da Web. Se a pontuação cair abaixo de 40, o site será bloqueado. Para ler mais sobre a tecnologia de reputação na Web, clique aqui para obter mais detalhes.

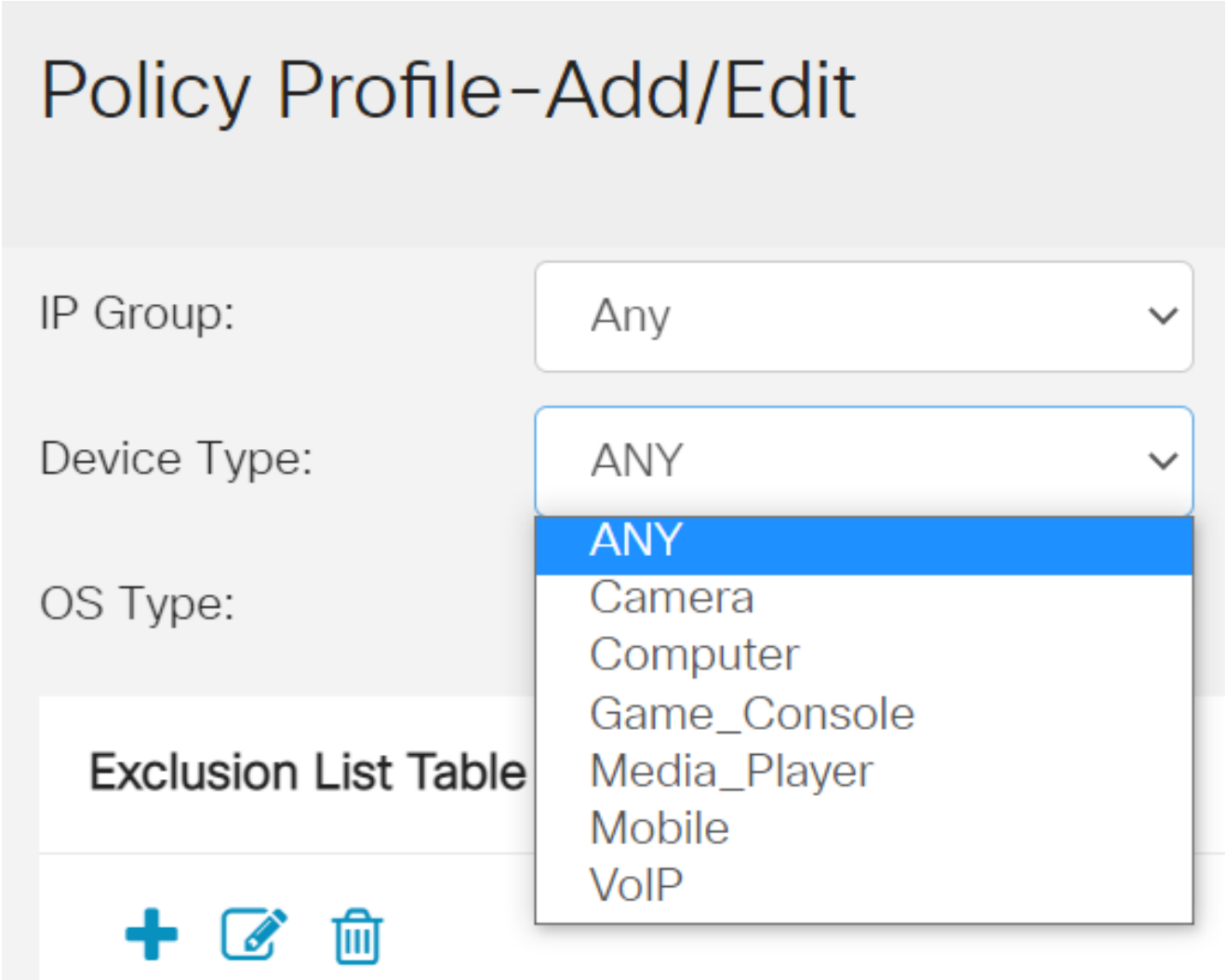
Etapa 6

Na lista suspensa Device Type, selecione a origem/o destino dos pacotes a serem filtrados. É possível escolher apenas uma opção por vez. As opções são:

- ANY (QUALQUER UM) — Escolha essa opção para aplicar a política a qualquer dispositivo.
- Câmera — Escolha essa opção para aplicar a diretiva às câmeras (como câmeras de

segurança IP).

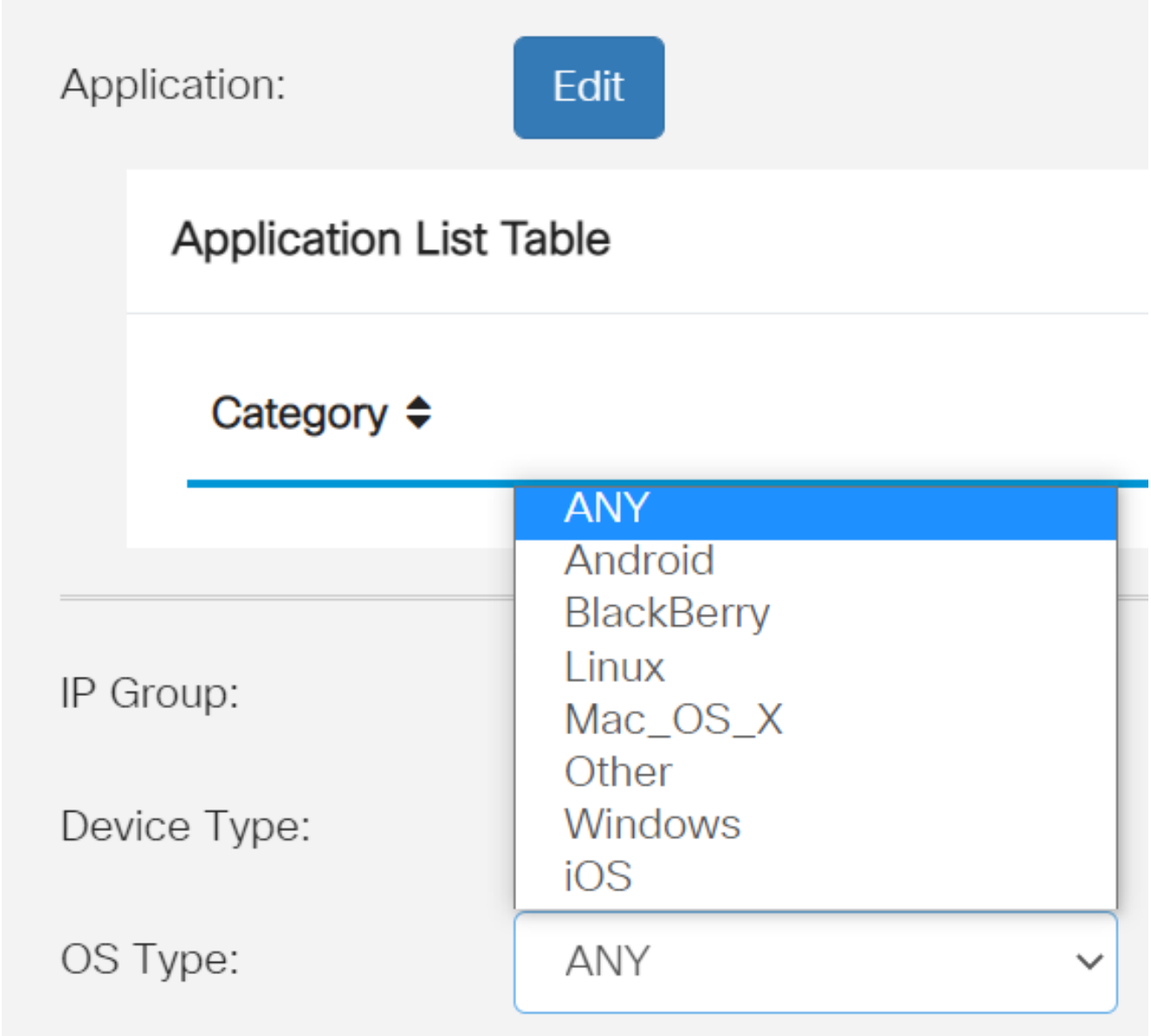
- Computador — Escolha esta opção para aplicar a regra a computadores.
- Game_Console — Escolha esta opção para aplicar a diretiva aos consoles de jogos.
- Media_Player — Escolha essa opção para aplicar a política a Media Players.
- Móvel — Escolha esta opção para aplicar a política a dispositivos móveis.
- VoIP — Escolha esta opção para aplicar a política aos dispositivos de Voz sobre Protocolo de Internet.



Etapa 7

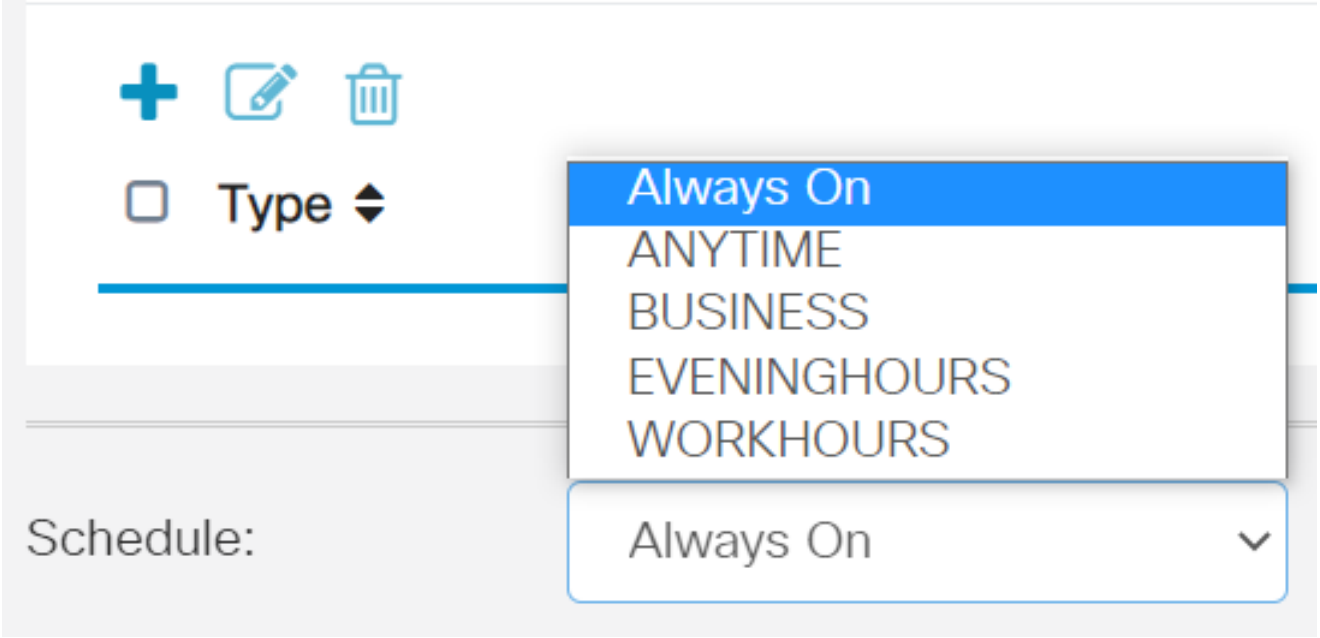
Na lista suspensa Tipo de sistema operacional, escolha um sistema operacional ao qual a diretiva deve ser aplicável. É possível escolher apenas uma opção por vez. As opções são:

- ANY — Aplica a política a qualquer tipo de SO. Esse é o padrão.
- Android — Aplica a política somente ao sistema operacional Android.
- BlackBerry — Aplica a política somente ao sistema operacional Blackberry.
- Linux — Aplica a política somente ao sistema operacional Linux.
- Mac_OS_X — Aplica a política somente ao Mac OS.
- Outro — Aplica a política a um SO que não está listado.
- Windows — Aplica a política ao sistema operacional Windows.
- iOS — Aplica a política somente ao iOS OS.



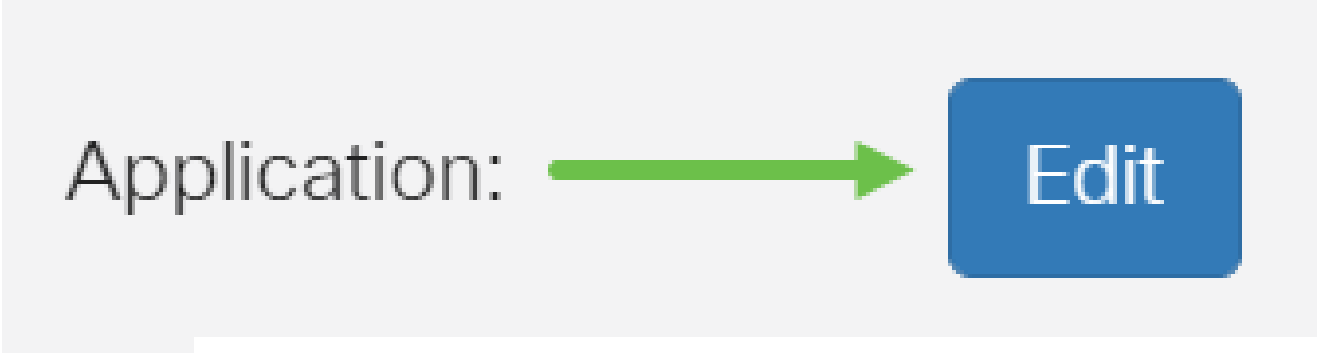
Passo 8

Role para baixo até a seção Schedule e selecione a opção que melhor atenda às suas necessidades.



Passo 9

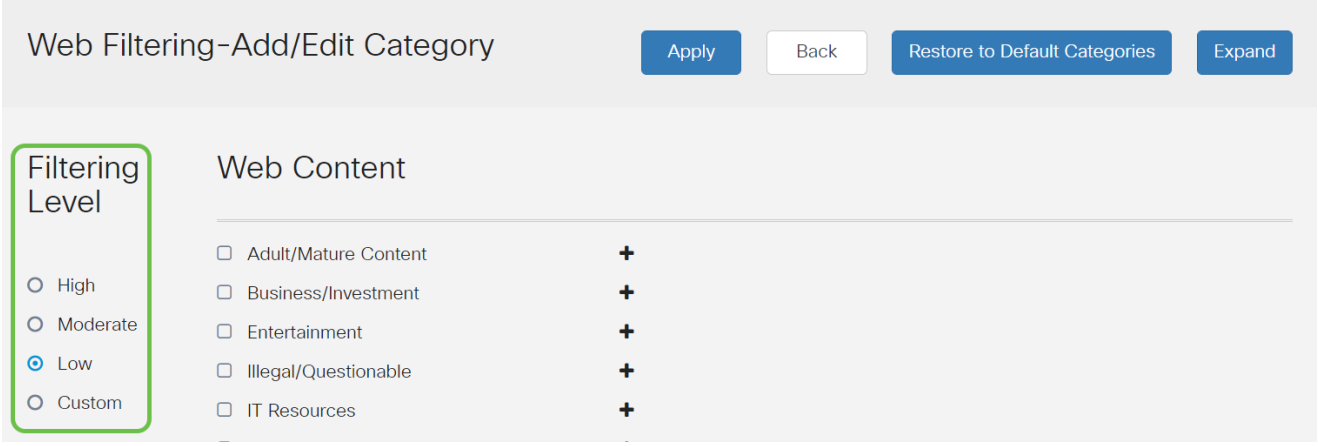
Clique no ícone de edição.



Passo 10

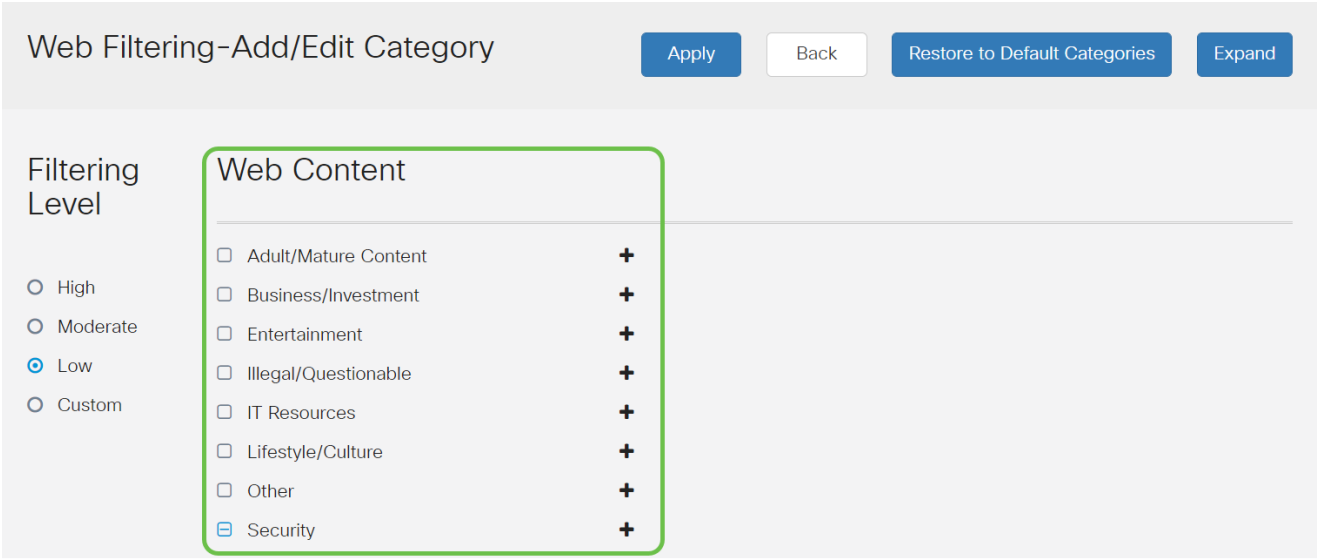
Na coluna Filtering Level (Nível de filtragem), clique em um botão de opção para definir rapidamente a extensão de filtragem que melhor se adapta às políticas de rede. As opções são High (Alta), Moderate (Moderada), Low (Baixa) e Custom (Personalizada). Clique em qualquer um dos níveis de filtragem abaixo para conhecer as subcategorias predefinidas específicas filtradas para cada uma das categorias de conteúdo da Web ativadas. Os filtros predefinidos não podem ser mais alterados e ficam esmaecidos.

- Low — Essa é a opção padrão. A segurança é ativada com essa opção.
- Moderada — Conteúdo adulto/maduro, Ilegal/Questionável e Segurança são ativados com essa opção.
- Alta — Conteúdo adulto/maduro, Negócios/Investimentos, Ilegal/Questionável, Recursos de TI e Segurança são ativados com essa opção.
- Personalizado — Nenhum padrão é definido para permitir filtros definidos pelo usuário.



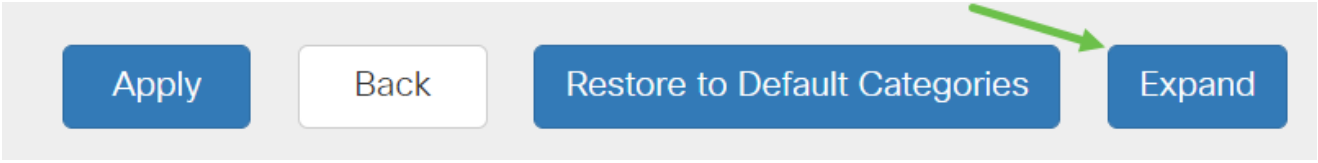
Passo 11

Insira o conteúdo da Web que deseja filtrar. Clique no ícone de adição se quiser mais detalhes sobre uma seção.



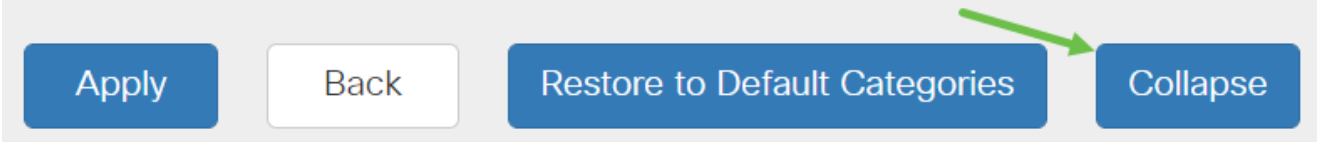
Etapa 12 (opcional)

Para exibir todas as subcategorias e descrições de Conteúdo da Web, você pode clicar no botão Expandir.



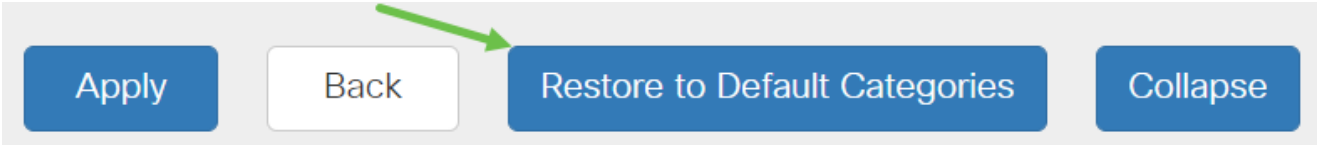
Etapa 13 (opcional)

Clique em Recolher para recolher as subcategorias e descrições.



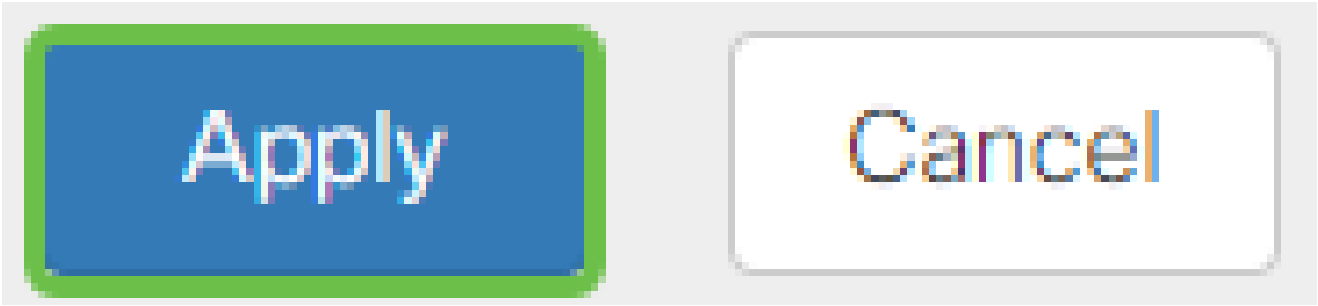
Etapa 14 (opcional)

Para retornar às categorias padrão, clique em Restaurar categorias padrão.



Etapa 15

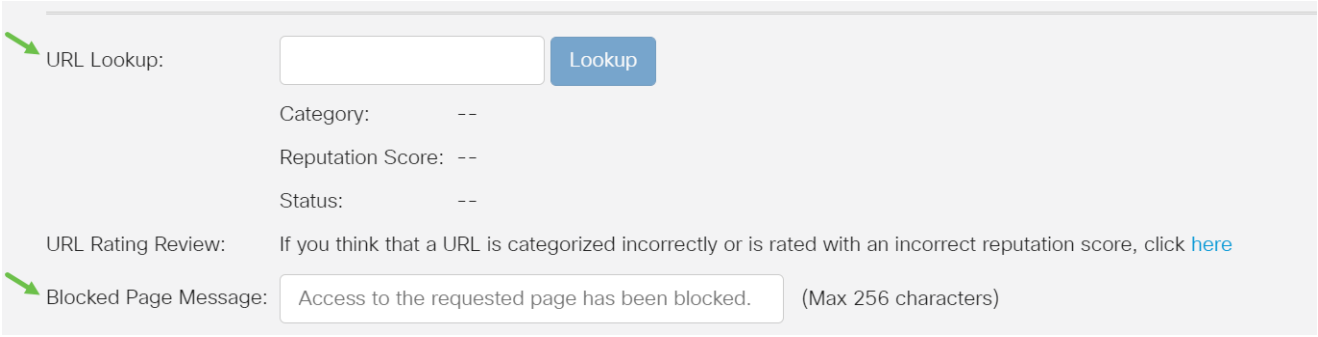
Clique em Apply para salvar a configuração e retornar à página Filter para continuar a configuração.



Na tabela Lista de aplicativos, as subcategorias correspondentes com base no nível de filtragem escolhido preencherão a tabela.

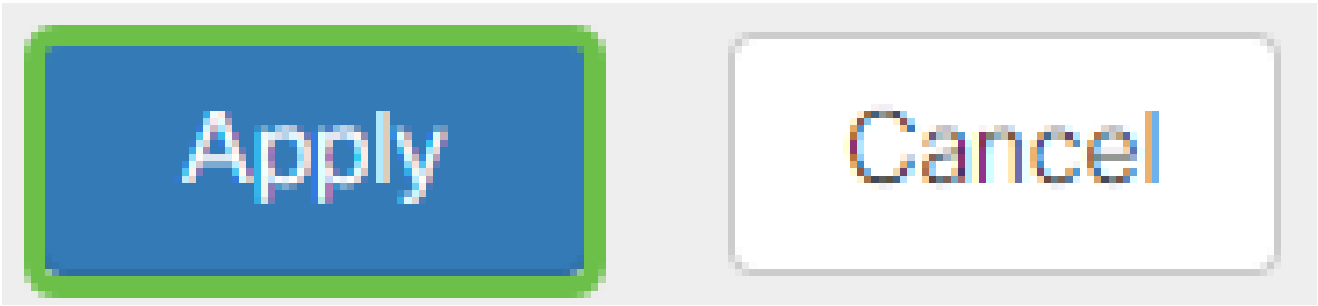
Etapa 16 (opcional)

Outras opções incluem a Pesquisa de URL e a mensagem que mostra quando uma página solicitada foi bloqueada.



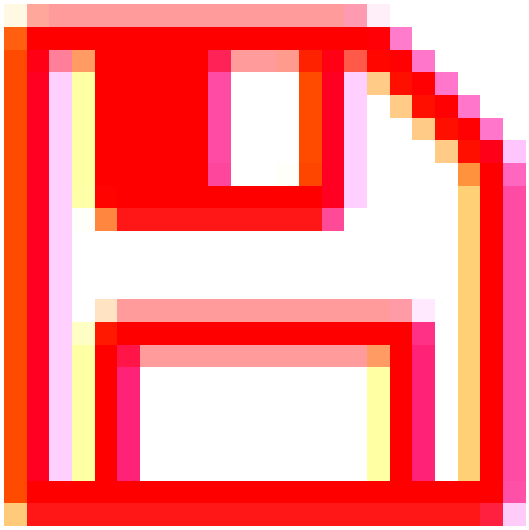
Etapa 17 (opcional)

Clique em Apply.



Etapa 18

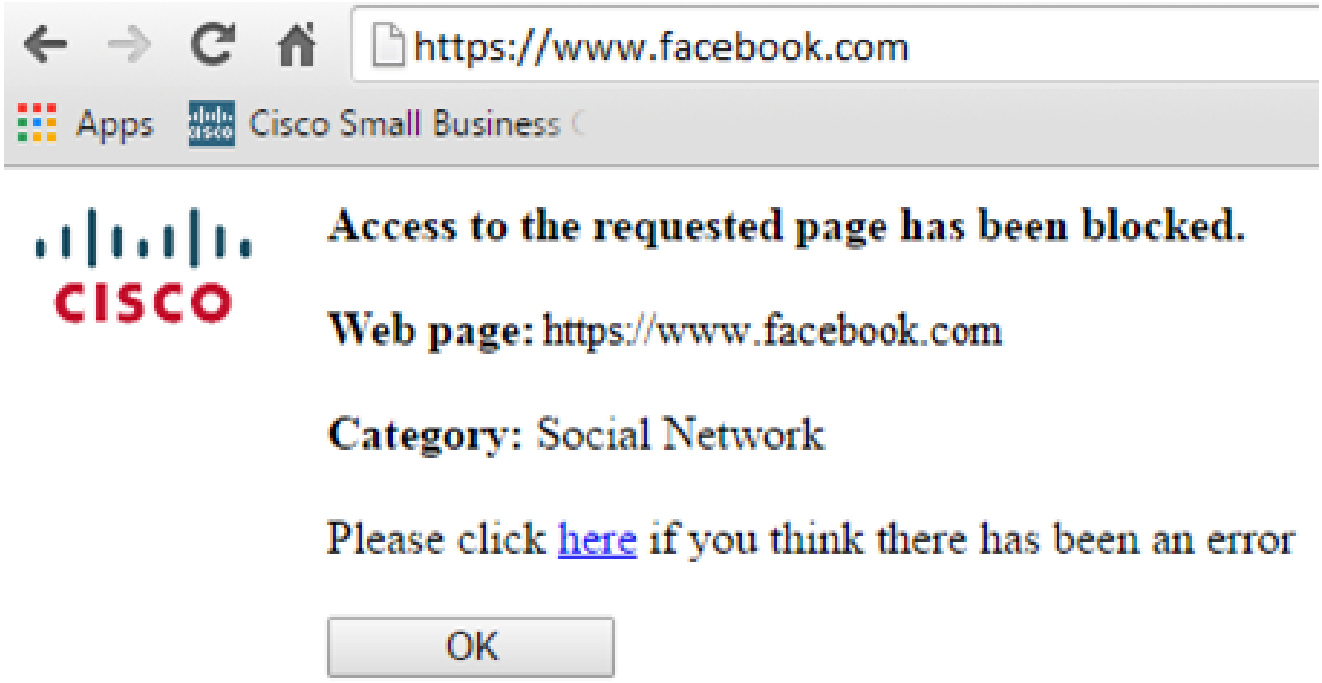
Para salvar a configuração permanentemente, vá para a página Copiar/salvar configuração ou clique no ícone salvar na parte superior da página.



Etapa 19 (opcional)

Para verificar se um site ou URL foi filtrado ou bloqueado, abra um navegador da Web ou abra uma nova guia no navegador. Digite o nome de domínio que você bloqueou ou que filtrou para ser bloqueado ou negado.

Neste exemplo, usamos www.facebook.com.



Agora você deve ter configurado com êxito a filtragem da Web no roteador RV345P. Como você está usando a Licença RV Security para filtragem da Web, provavelmente não precisará do Umbrella. Se você também quiser o Umbrella, clique aqui. Se você tiver segurança suficiente, clique para ir para a próxima seção.

Troubleshooting

Se você comprou uma licença, mas ela não está aparecendo em sua conta virtual, há duas opções:

1. Entre em contato com o revendedor para solicitar que ele faça a transferência.
2. Fale conosco e entraremos em contato com o revendedor.

O ideal seria que você não precisasse fazer isso, mas se você chegar a esse cruzamento, teremos o prazer de ajudar! Para tornar o processo o mais conveniente possível, você precisará das credenciais da tabela acima, bem como das descritas abaixo.

Informações necessárias	Localizando as informações
Fatura de licença	Ele deve ser enviado por e-mail a você após a conclusão da compra das licenças.
Número do pedido de vendas da Cisco	Talvez seja necessário voltar ao revendedor para obter isso.
Captura de tela da página	Capturar um screenshot captura o conteúdo de sua tela para

Informações necessárias	Localizando as informações
de licença da sua Conta inteligente	compartilhamento com nossa equipe. Se você não está familiarizado com capturas de tela, você pode usar os métodos abaixo.

Capturas de tela

Uma vez que você tenha um token, ou se estiver solucionando problemas, é recomendável que você faça uma captura de tela para capturar o conteúdo de sua tela.

Dadas as diferenças no procedimento necessário para capturar uma captura de tela, veja abaixo os links específicos para o seu sistema operacional.

- Windows
- MAC
- iPhone/iPad
- Android

Licença de filial Umbrella RV (opcional)

A Umbrella é uma plataforma de segurança de nuvem simples, mas muito eficaz, da Cisco.

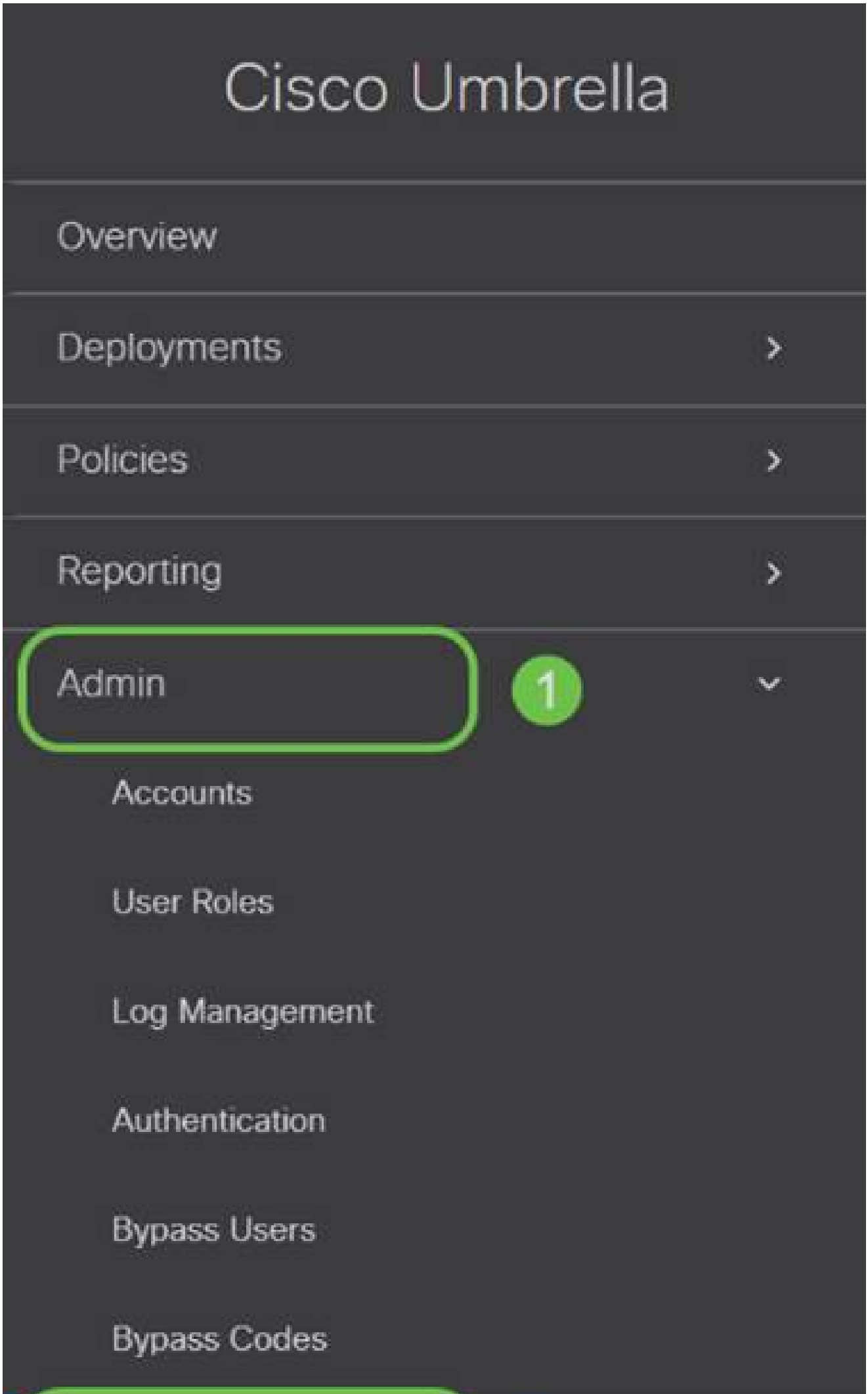
A Umbrella opera na nuvem e executa muitos serviços relacionados à segurança. Da ameaça emergente à investigação pós-evento. O Umbrella detecta e evita ataques em todas as portas e protocolos.

O Umbrella usa o DNS como seu principal vetor de defesa. Quando os usuários inserem uma URL na barra do navegador e pressionam Enter, o Umbrella participa da transferência. Essa URL passa para o resolvedor DNS da Umbrella e, se um aviso de segurança estiver associado ao domínio, a solicitação será bloqueada. Essa telemetria transfere dados e é analisada em microssegundos, praticamente sem latência. Os dados de telemetria usam logs e instrumentos para rastrear bilhões de solicitações de DNS em todo o mundo. Quando esses dados estão difundidos, correlacioná-los em todo o mundo permite uma resposta rápida aos ataques no início. Consulte a política de privacidade da Cisco aqui para obter mais informações: política completa, versão resumida. Pense nos dados de telemetria como dados derivados de ferramentas e registros.

Visite o Cisco Umbrella para saber mais e criar uma conta. Se tiver algum problema, verifique a documentação aqui e as opções de suporte do Umbrella.

Passo 1

Depois de fazer login na sua conta Umbrella, na tela Dashboard, clique em Admin > API Keys.

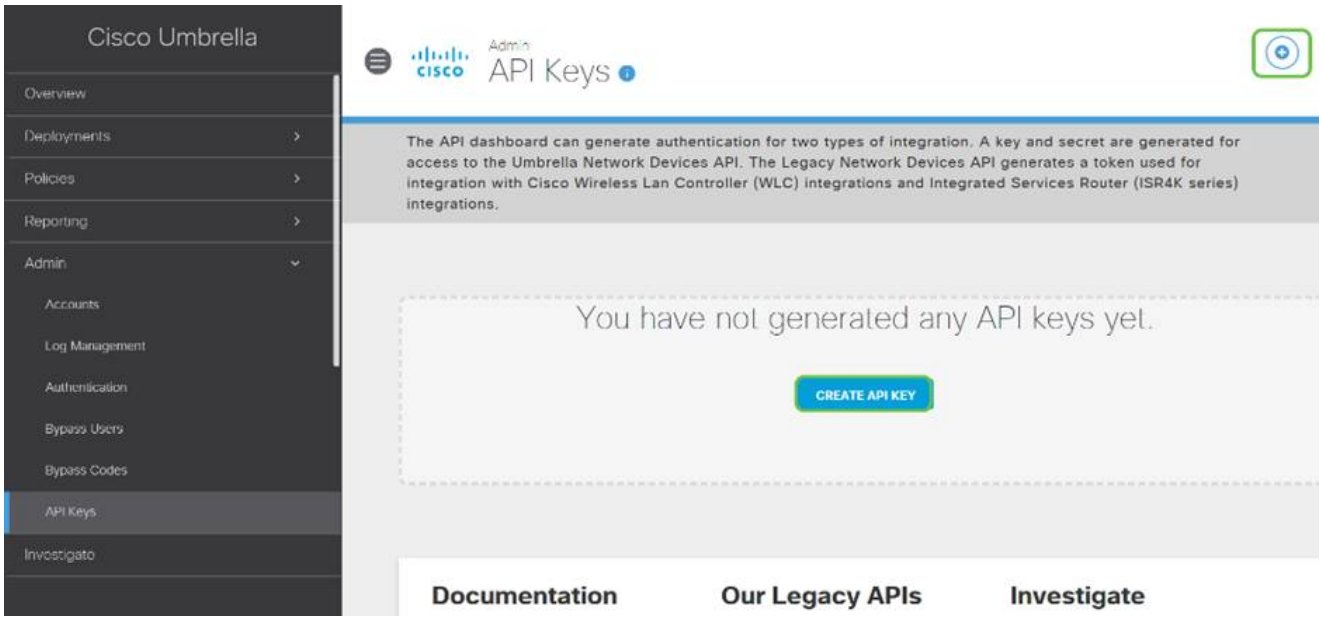

Cisco Umbrella
Overview
Deployments
Policies
Reporting
Admin
1
Accounts
User Roles
Log Management
Authentication
Bypass Users
Bypass Codes

Anatomia da tela de chaves de API (com chave de API pré-existente)

1. Adicionar chave de API - Inicia a criação de uma nova chave para uso com a API Umbrella.
2. Informações adicionais - desliza para baixo/para cima com um explicador para esta tela.
3. Compartimento Token - Contém todas as chaves e tokens criados por esta conta. (Preenche quando uma chave é criada)
4. Documentos de suporte - Links para a documentação no site do Umbrella referente aos tópicos em cada seção.

Passo 2

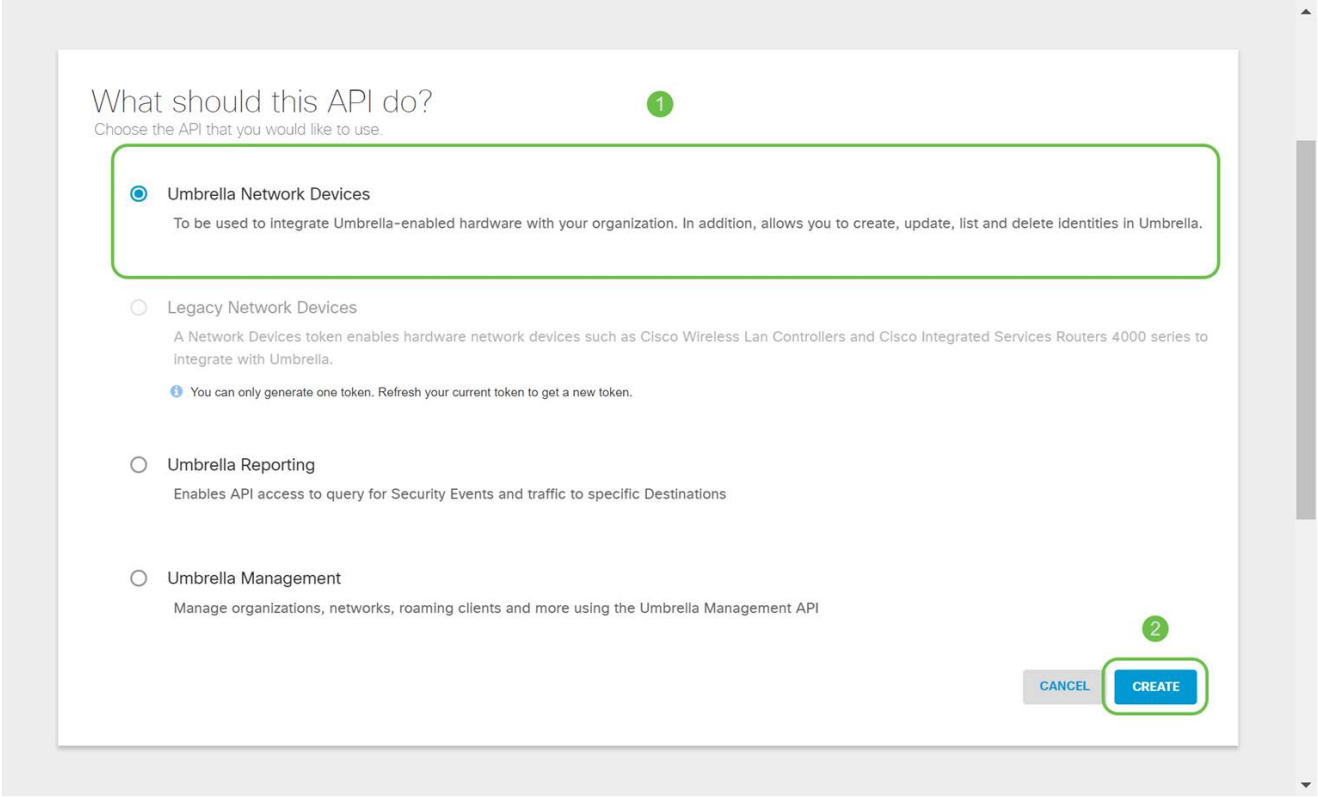
Clique no botão Add API Key no canto superior direito ou clique no botão Create API Key. Ambos funcionam da mesma forma.



A captura de tela acima seria semelhante ao que você veria abrindo este menu pela primeira vez.

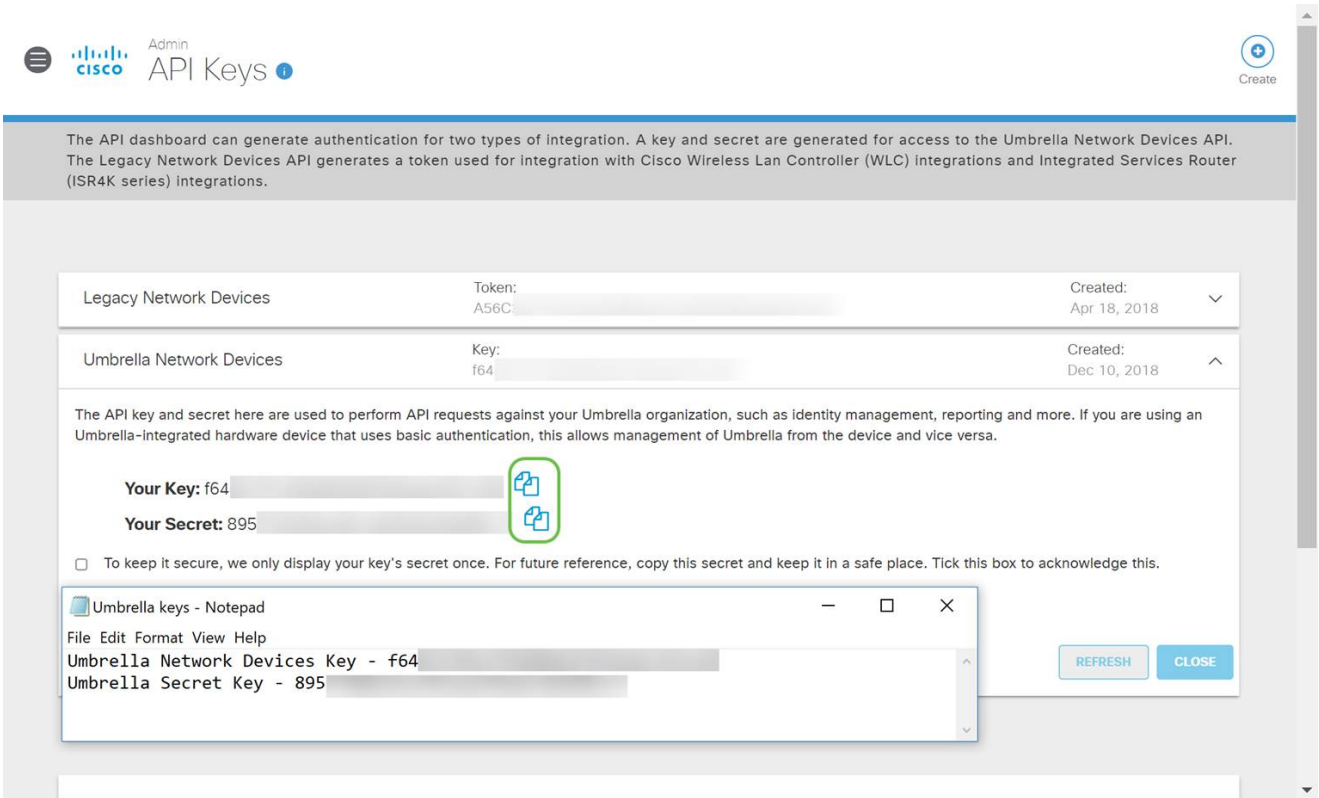
Etapa 3

Selecione Umbrella Network Devices e clique no botão Create.



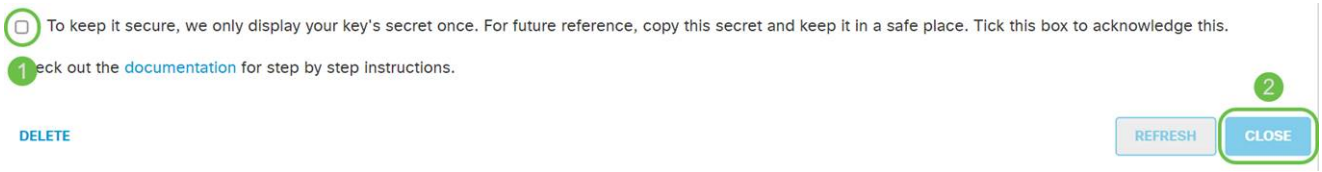
Passo 4

Abra um editor de texto, como o notepad, e clique no ícone de cópia à direita da API e da Chave secreta da API. Uma notificação pop-up confirmará que a chave foi copiada para a área de transferência. Cole seu segredo e a chave de API no documento, rotulando-os para referência futura. Nesse caso, seu rótulo é "Umbrella network devices key". Em seguida, salve o arquivo de texto em um local seguro e de fácil acesso posteriormente.



Etapa 5

Depois de ter copiado a chave e a chave secreta para um local seguro, na tela Umbrella API, clique na caixa de seleção para confirmar a exibição temporária da chave secreta e, em seguida, clique no botão Fechar.



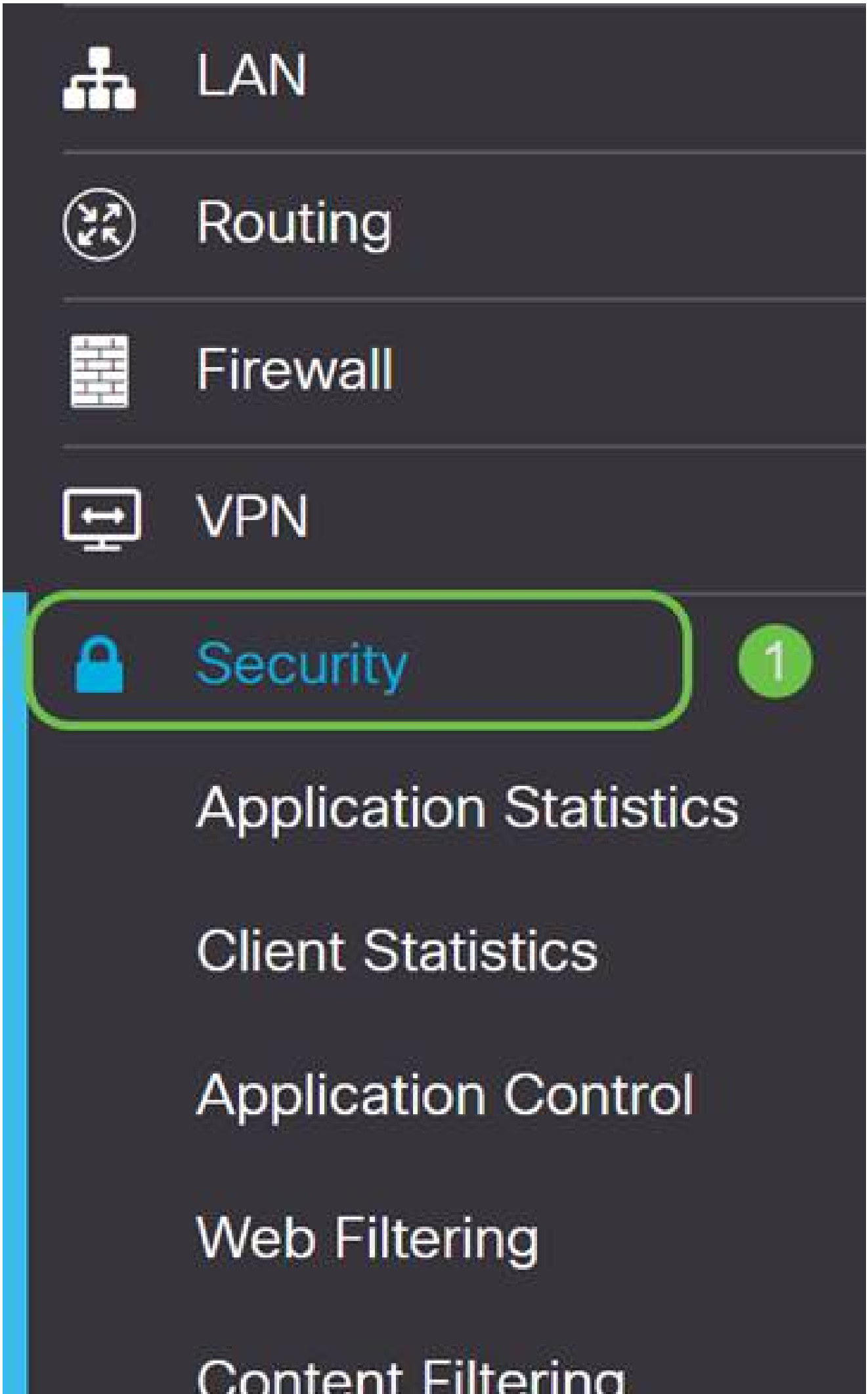
Se você perder ou acidentalmente excluir a chave secreta, não haverá nenhuma função ou número de suporte para ligar para recuperar essa chave. Se perder, você precisará excluir a chave e autorizar novamente a nova chave de API com cada dispositivo que deseja proteger com o Umbrella.

Configurando o Umbrella em seu RV345P

Agora que criamos chaves de API no Umbrella, você pode pegar essas chaves e instalá-las no RV345P.

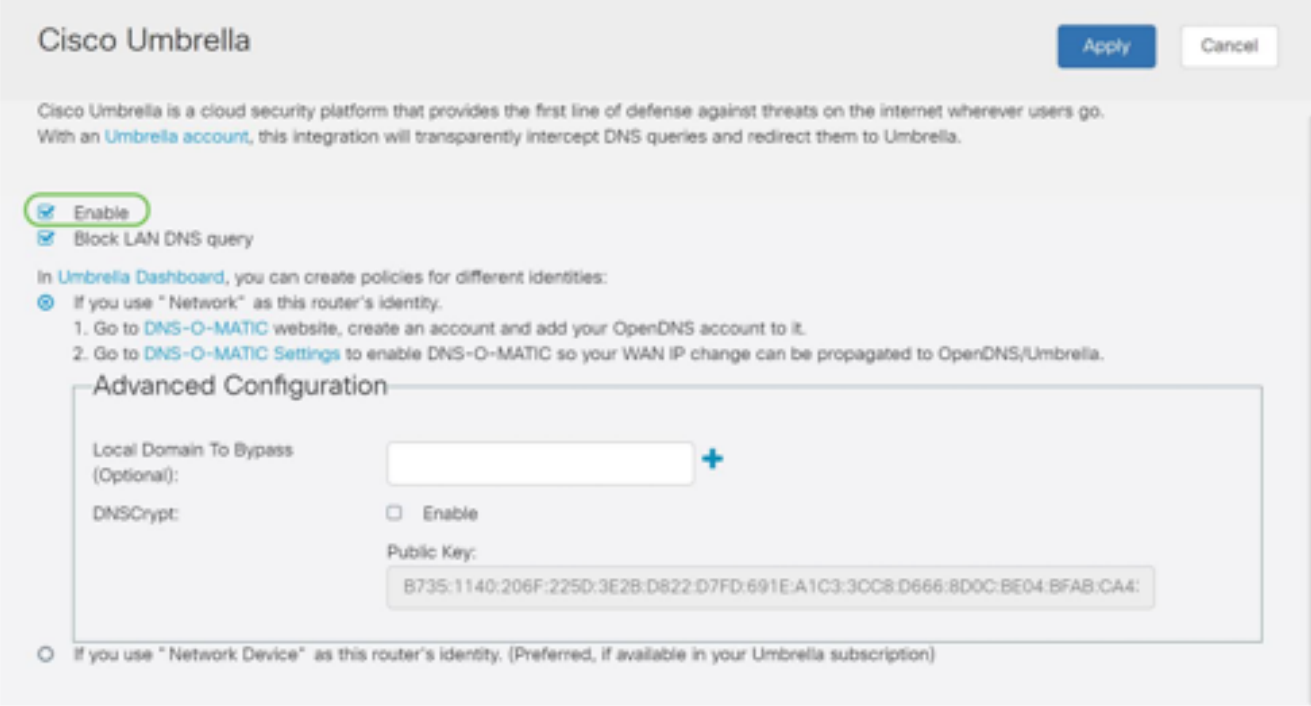
Passo 1

Depois de iniciar sessão no roteador RV345P, clique em Security > Umbrella no menu da barra lateral.


LAN
Routing
Firewall
VPN
Security
1
Application Statistics
Client Statistics
Application Control
Web Filtering
Content Filtering

Passo 2

A tela da API do Umbrella tem uma variedade de opções, comece a ativar o Umbrella clicando na caixa de seleção Habilitar.

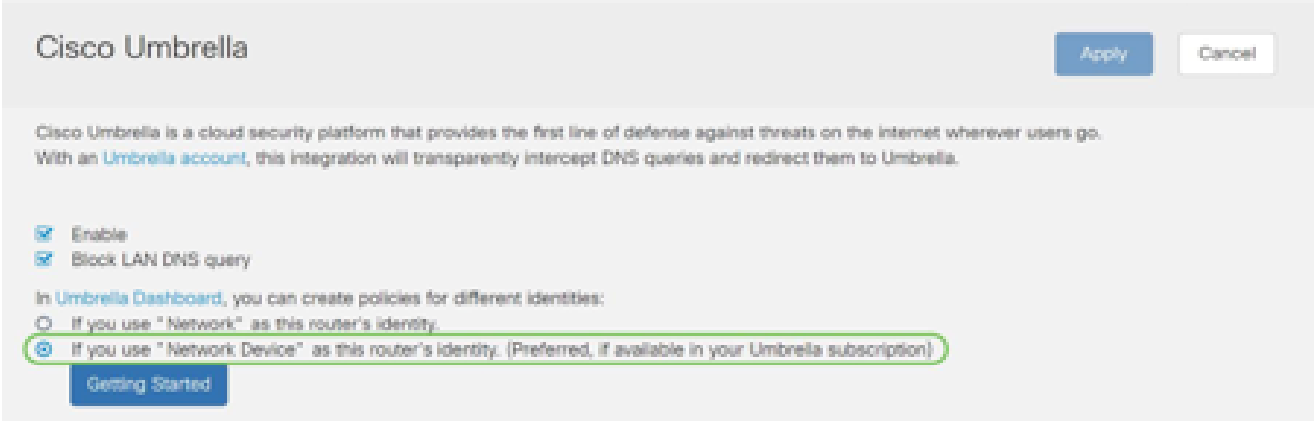


Etapa 3 (opcional)

Por padrão, a caixa Block LAN DNS Queries está selecionada. Esse recurso limpo cria automaticamente listas de controle de acesso no roteador, o que impedirá que o tráfego DNS saia para a Internet. Este recurso força todas as solicitações de tradução de domínio a serem direcionadas através do RV345P e é uma boa ideia para a maioria dos usuários.

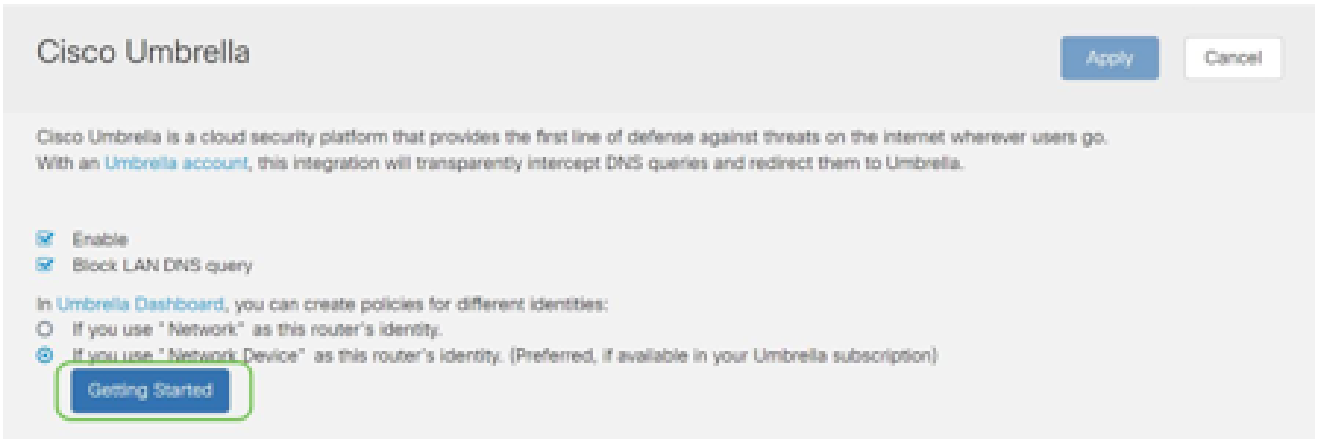
Passo 4

A próxima etapa é executada de duas maneiras diferentes. Ambos dependem da configuração da sua rede. Se usar um serviço como DynDNS ou NoIP, você deixará o esquema de nomenclatura padrão de "Rede". Você precisará fazer login nessas contas para garantir que o Umbrella faça interface com esses serviços, pois ele oferece proteção. Para nossos propósitos, estamos confiando em "Dispositivo de rede", então clicamos no botão de opção inferior.



Etapa 5

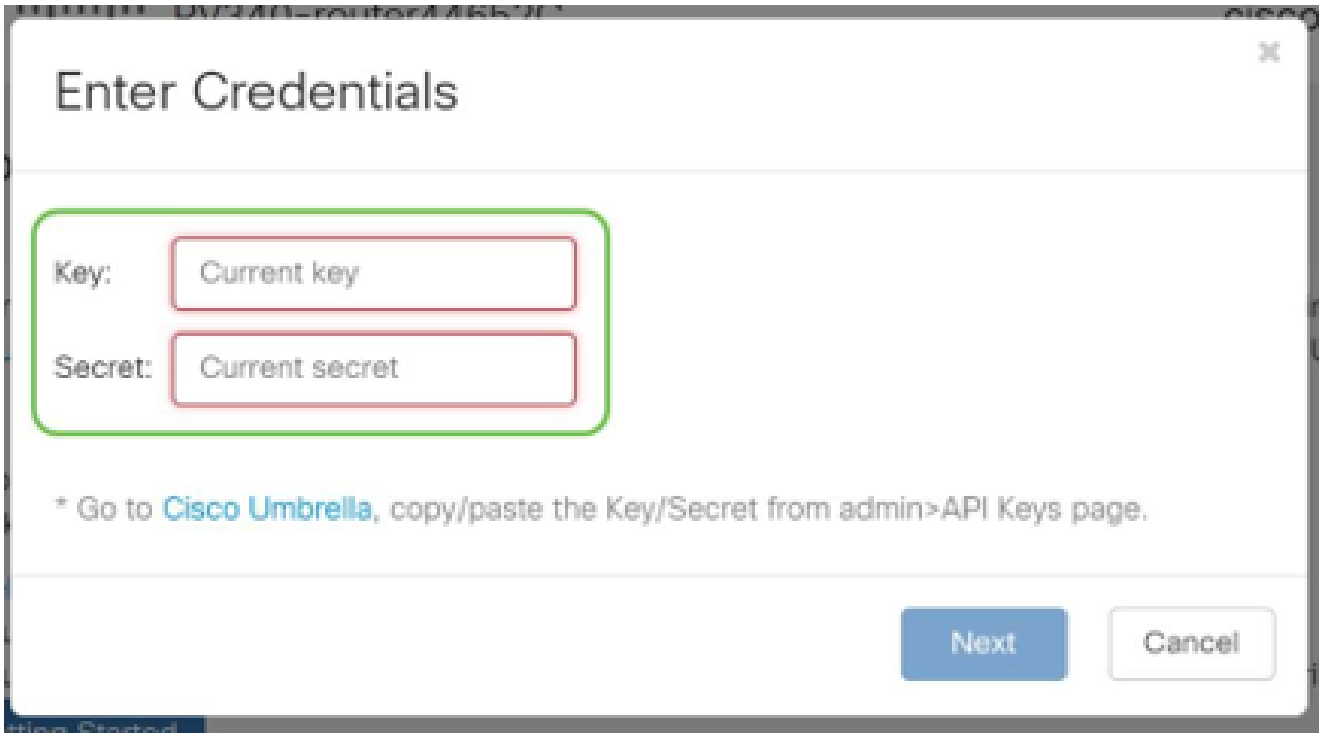
Clique em Getting Started.



Etapa 6

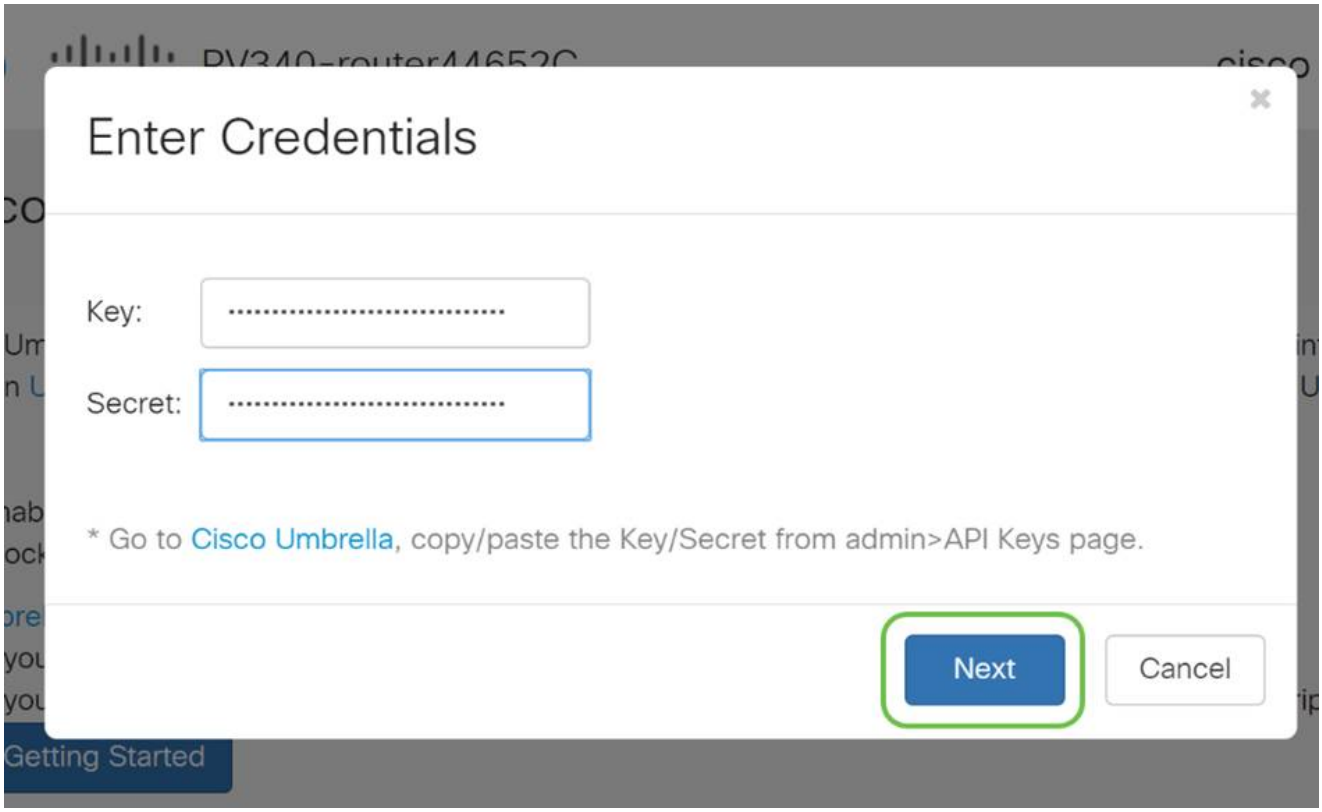
Insira a chave de API e a chave secreta nas caixas de texto.

Falar duas vezes para que saiba que é importante! Se você perder ou acidentalmente excluir a chave secreta, não haverá nenhuma função ou número de suporte para ligar para recuperar essa chave. Mantenha segredo e seguro. Se perder, você precisará excluir a chave e autorizar novamente a nova chave de API com cada dispositivo que deseja proteger com o Umbrella.



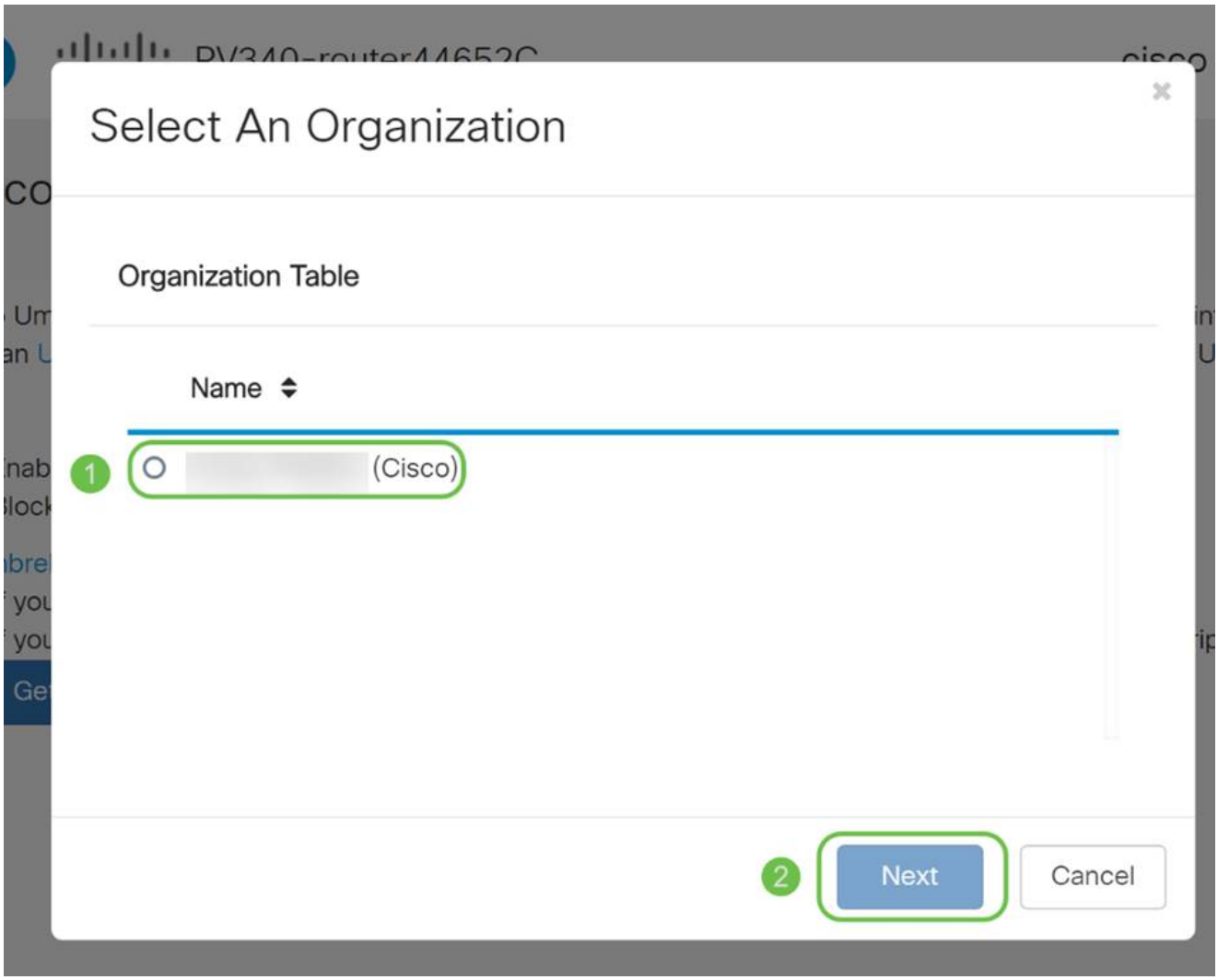
Etapa 7

Depois de inserir a API e a chave secreta, clique no botão Next.



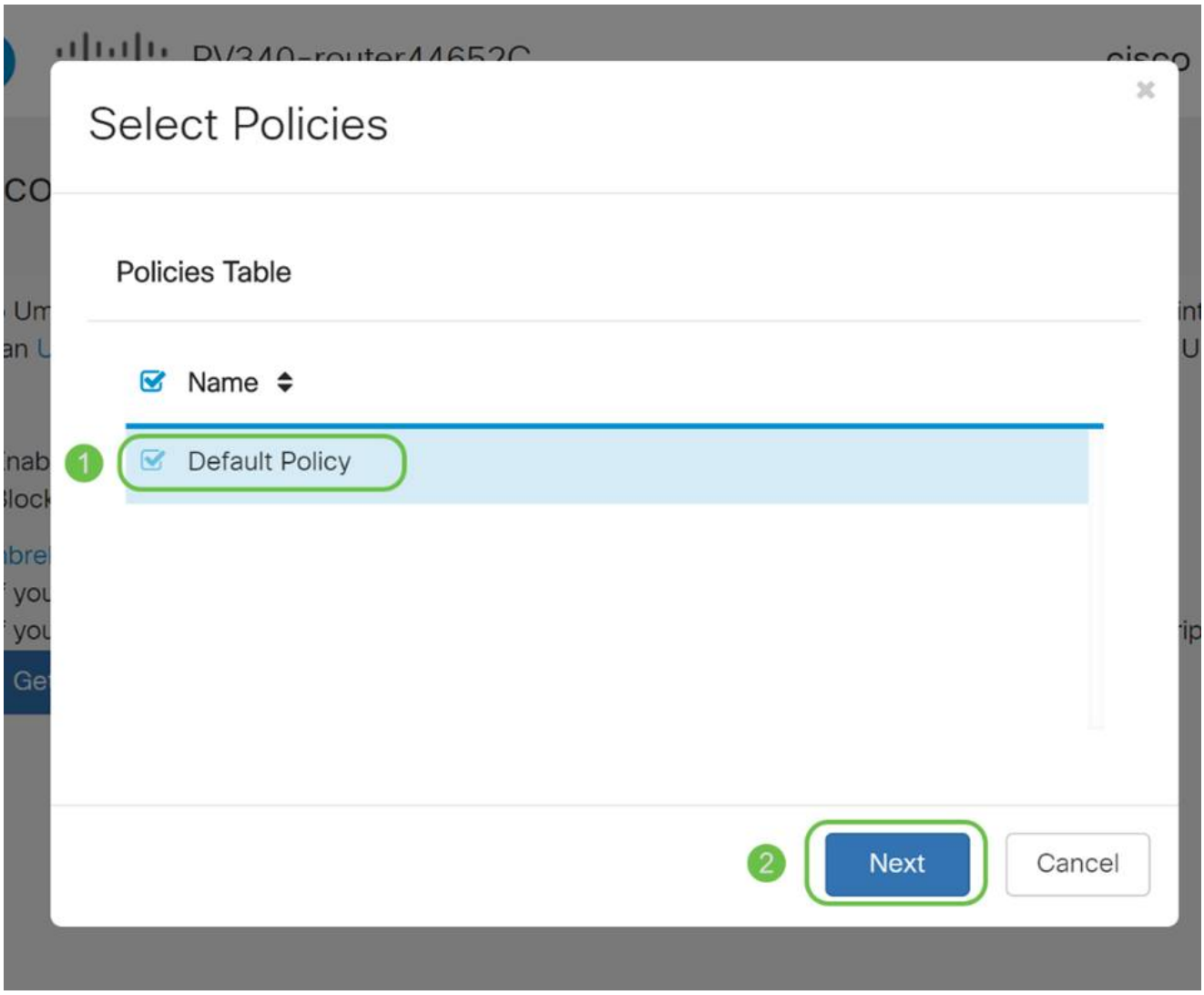
Passo 8

Na próxima tela, selecione a organização que deseja associar ao roteador. Clique em Next.



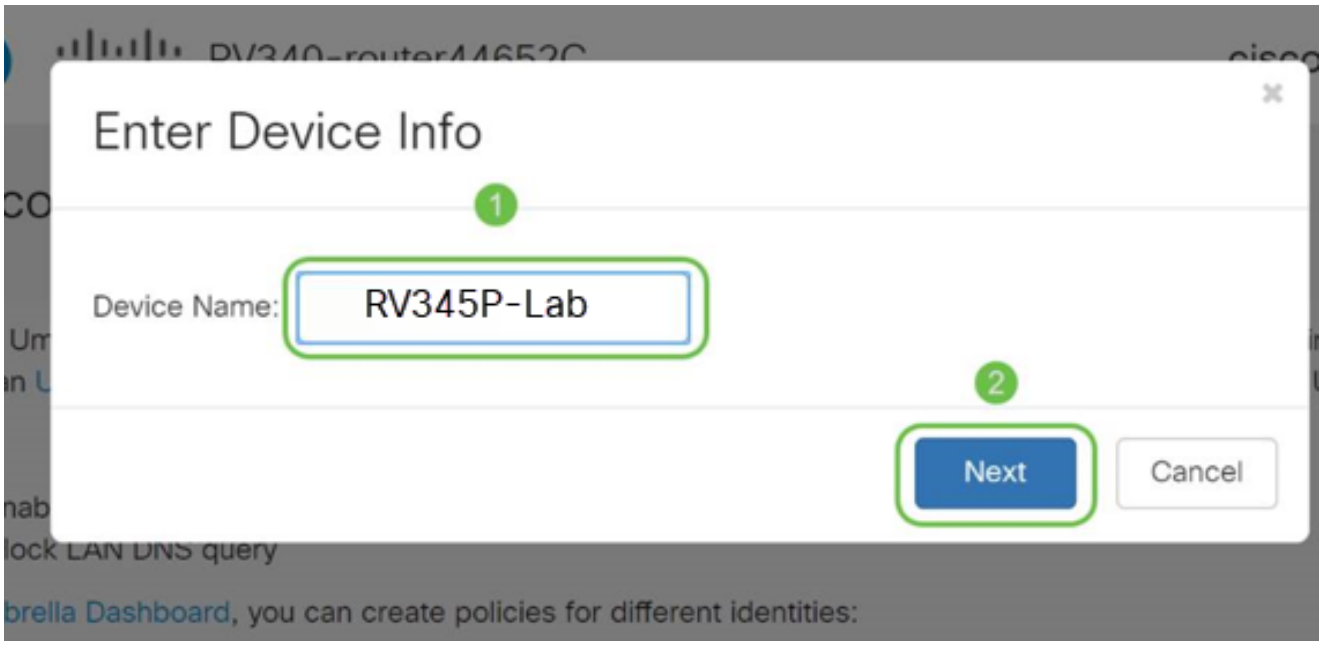
Passo 9

Selecione a diretiva a ser aplicada ao tráfego roteado pelo RV345P. Para a maioria dos usuários, a política padrão fornecerá cobertura suficiente.



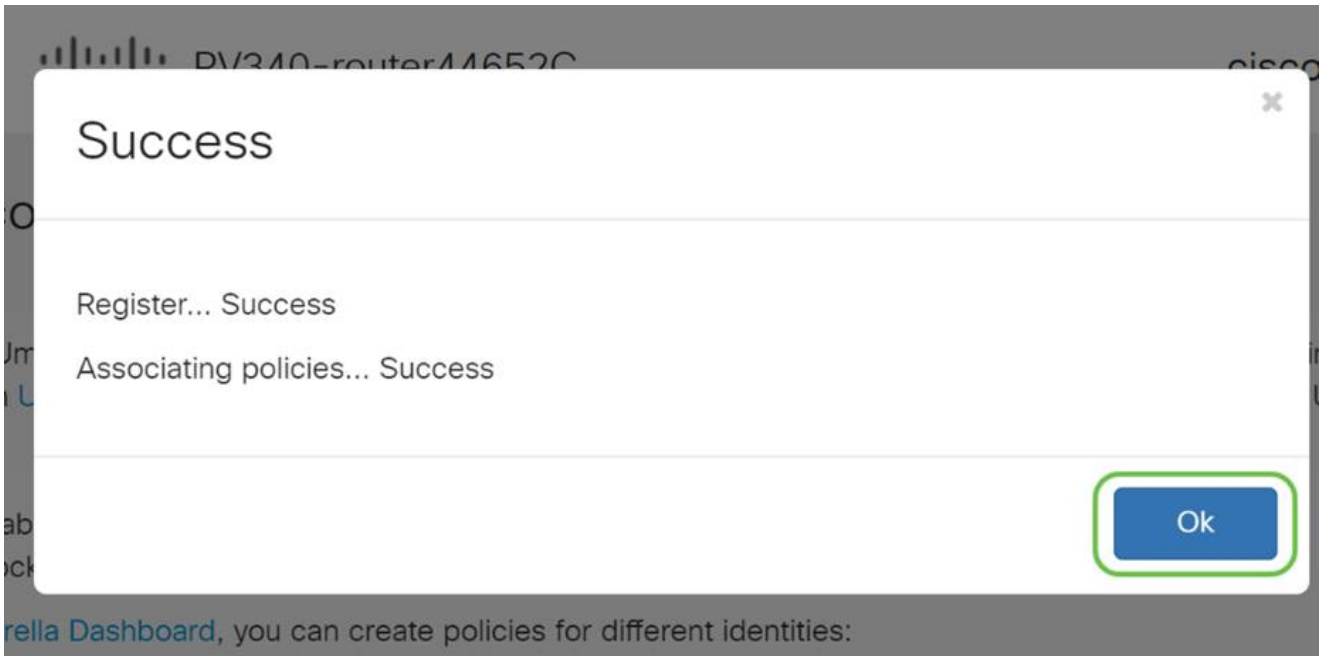
Passo 10

Atribua um nome ao dispositivo para que ele possa ser designado nos relatórios do Umbrella. Em nossa configuração, nós o denominamos RV345P-Lab.



Passo 11

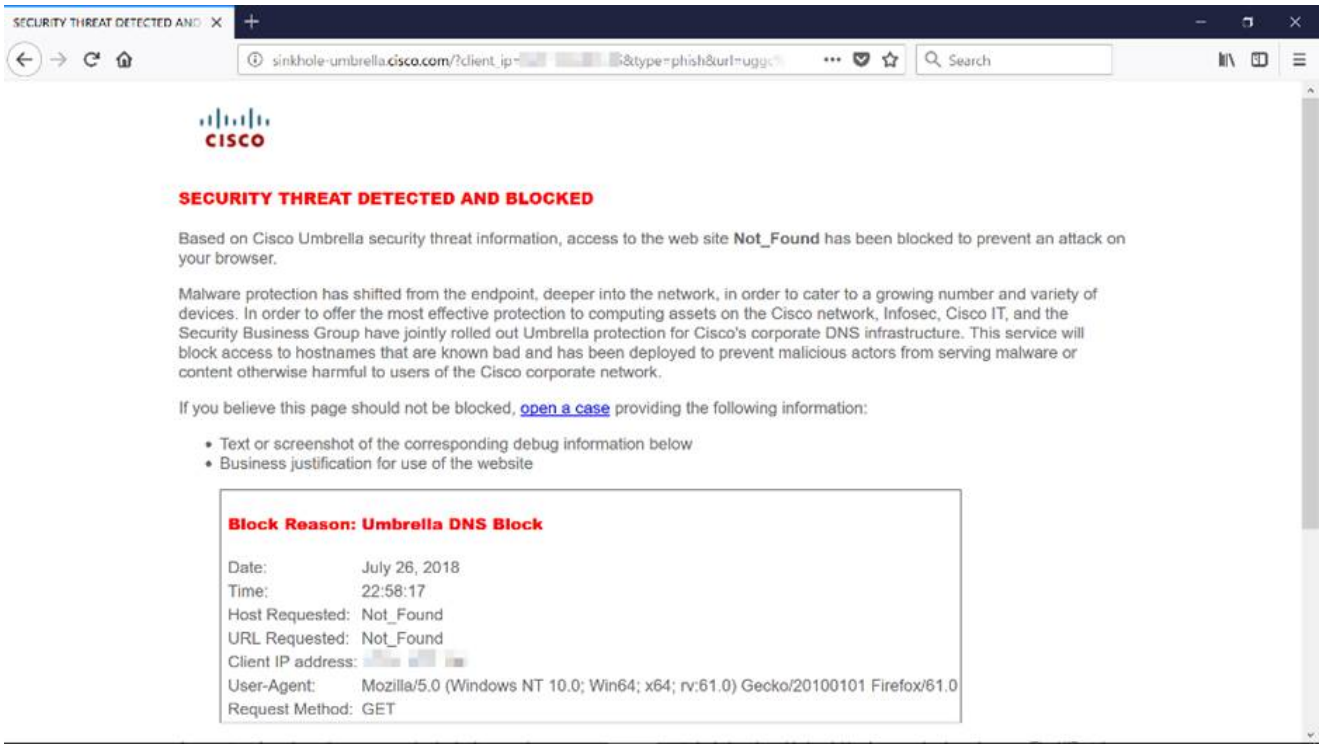
A próxima tela validará as configurações escolhidas e fornecerá uma atualização quando associada com êxito. Click OK.



Confirmação

Parabéns, agora você está protegido pelo Cisco Umbrella. Ou você está? Vamos ter certeza, verificando duas vezes com um exemplo ao vivo, que a Cisco criou um site dedicado a determinar isso tão rapidamente quanto a página é carregada. Clique aqui ou digite https://InternetBadGuys.com na barra do navegador.

Se o Umbrella estiver configurado corretamente, você será recebido por uma tela semelhante a esta.



Outras opções de segurança

Você está preocupado que alguém possa tentar acessar a rede sem autorização desconectando um cabo Ethernet de um dispositivo de rede e conectando-se a ele? Nesse caso, é importante registrar uma lista de hosts permitidos para se conectar diretamente ao roteador com seus respectivos endereços IP e MAC. As instruções podem ser encontradas no artigo Configure IP Source Guard no RV34x Series Router.

Opções de VPN

Uma conexão VPN (Virtual Private Network) permite que os usuários acessem, enviem e recebam dados de e para uma rede privada por meio da passagem por uma rede pública ou compartilhada, como a Internet, mas ainda garantindo uma conexão segura a uma infraestrutura de rede subjacente para proteger a rede privada e seus recursos.

Um túnel VPN estabelece uma rede privada que pode enviar dados com segurança usando criptografia e autenticação. Os escritórios corporativos usam principalmente a conexão VPN, já que ela é útil e necessária para permitir que seus funcionários tenham acesso à sua rede privada, mesmo que estejam fora do escritório.

A VPN permite que um host remoto atue como se estivesse localizado na mesma rede local. O roteador suporta até 50 túneis. Uma conexão VPN pode ser configurada entre o roteador e um endpoint depois que o roteador tiver sido configurado para conexão com a Internet. O cliente VPN depende inteiramente das configurações do roteador VPN para poder estabelecer uma conexão.

Se não tiver certeza de qual VPN melhor atende às suas necessidades, consulte Visão geral e práticas recomendadas da Cisco Business VPN.

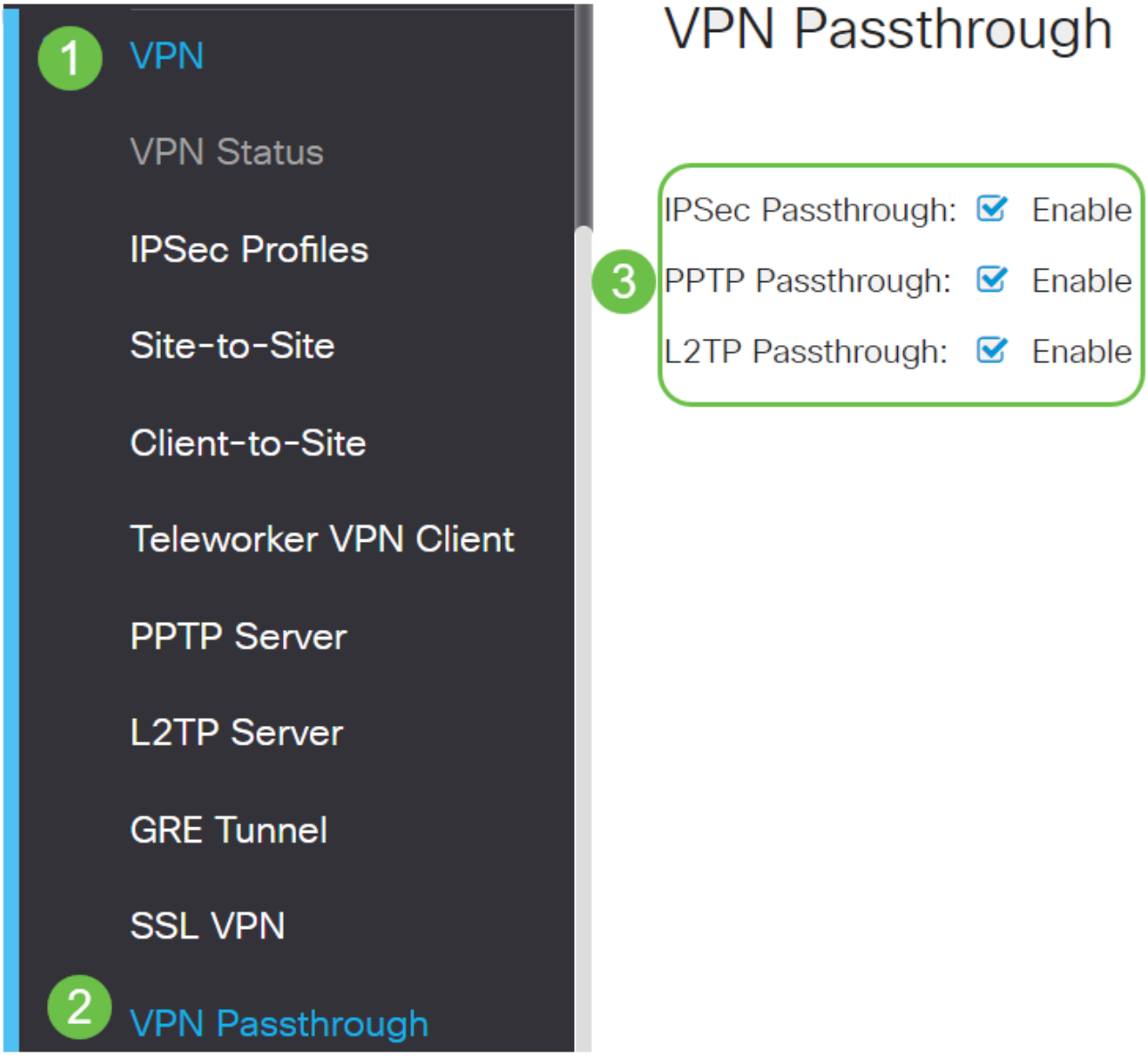
O AnyConnect VPN é o único produto com suporte ao Cisco VPN listado neste guia de configuração. Produtos de terceiros que não são da Cisco, incluindo TheGreenBow e Shrew Soft, não são suportados pela Cisco. Eles são incluídos estritamente para fins de orientação. Se precisar de suporte além do artigo, entre em contato com o terceiro para obter suporte.

Se não estiver planejando configurar uma VPN, você pode clicar para ir para a próxima seção.

Passagem de VPN

Geralmente, cada roteador suporta a conversão de endereços de rede (NAT) para conservar endereços IP quando você quiser suportar vários clientes com a mesma conexão de Internet. No entanto, o protocolo PPTP (Point-to-Point Tunneling Protocol) e a VPN IPsec (Internet Protocol Security) não suportam NAT. É aqui que entra a passagem VPN. Uma Passagem de VPN é um recurso que permite que o tráfego de VPN gerado de clientes VPN conectados a este roteador passe por este roteador e se conecte a um ponto final de VPN. O VPN Passthrough permite que o PPTP e o IPsec VPN passem apenas para a Internet, que é iniciada de um cliente VPN e, em seguida, acessem o gateway de VPN remoto. Esse recurso é comumente encontrado em roteadores domésticos que suportam NAT.

Por padrão, a passagem IPsec, PPTP e L2TP está habilitada. Se quiser exibir ou ajustar essas configurações, selecione VPN > VPN Passthrough. Visualize ou ajuste conforme necessário.



VPN AnyConnect

Há várias vantagens em usar o Cisco AnyConnect:

1. Conectividade segura e persistente
2. Segurança persistente e aplicação de políticas
3. Implantável a partir do Adaptive Security Appliance (ASA) ou de Sistemas de Implantação de Software Corporativo
4. Personalizável e traduzível
5. Fácil configuração
6. Suporta IPsec e SSL (Secure Sockets Layer)
7. Suporta o protocolo Internet Key Exchange versão 2.0 (IKEv2.0)

Configurar o AnyConnect SSL VPN no RV345P

Passo 1

Acesse o utilitário baseado na Web do roteador e escolha VPN > SSL VPN.

VPN 1

VPN Status

IPSec Profiles

Site-to-Site

Client-to-Site

Teleworker VPN Client

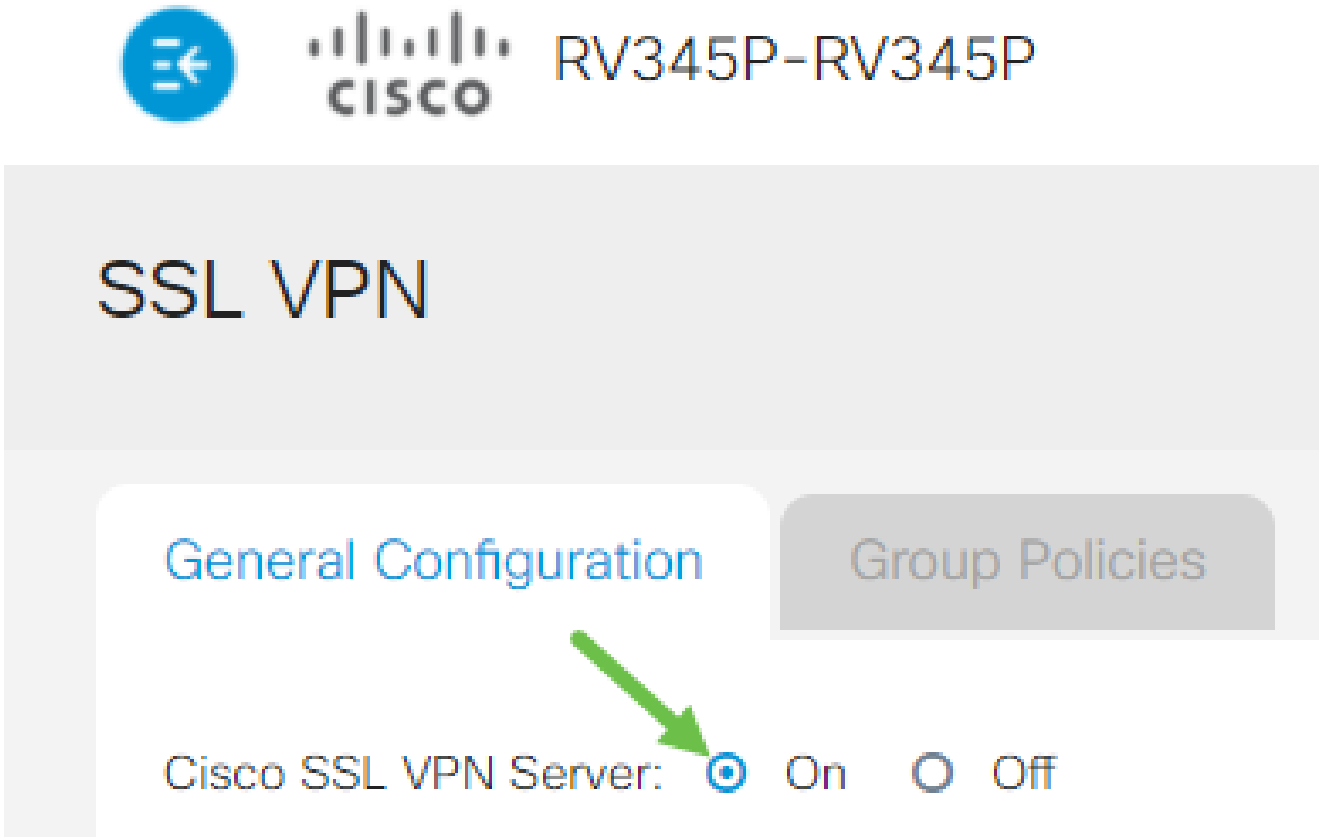
PPTP Server

L2TP Server

GRE Tunnel

Passo 2

Clique no botão de opção On para habilitar o Cisco SSL VPN Server.



Configurações de Gateway Obrigatórias

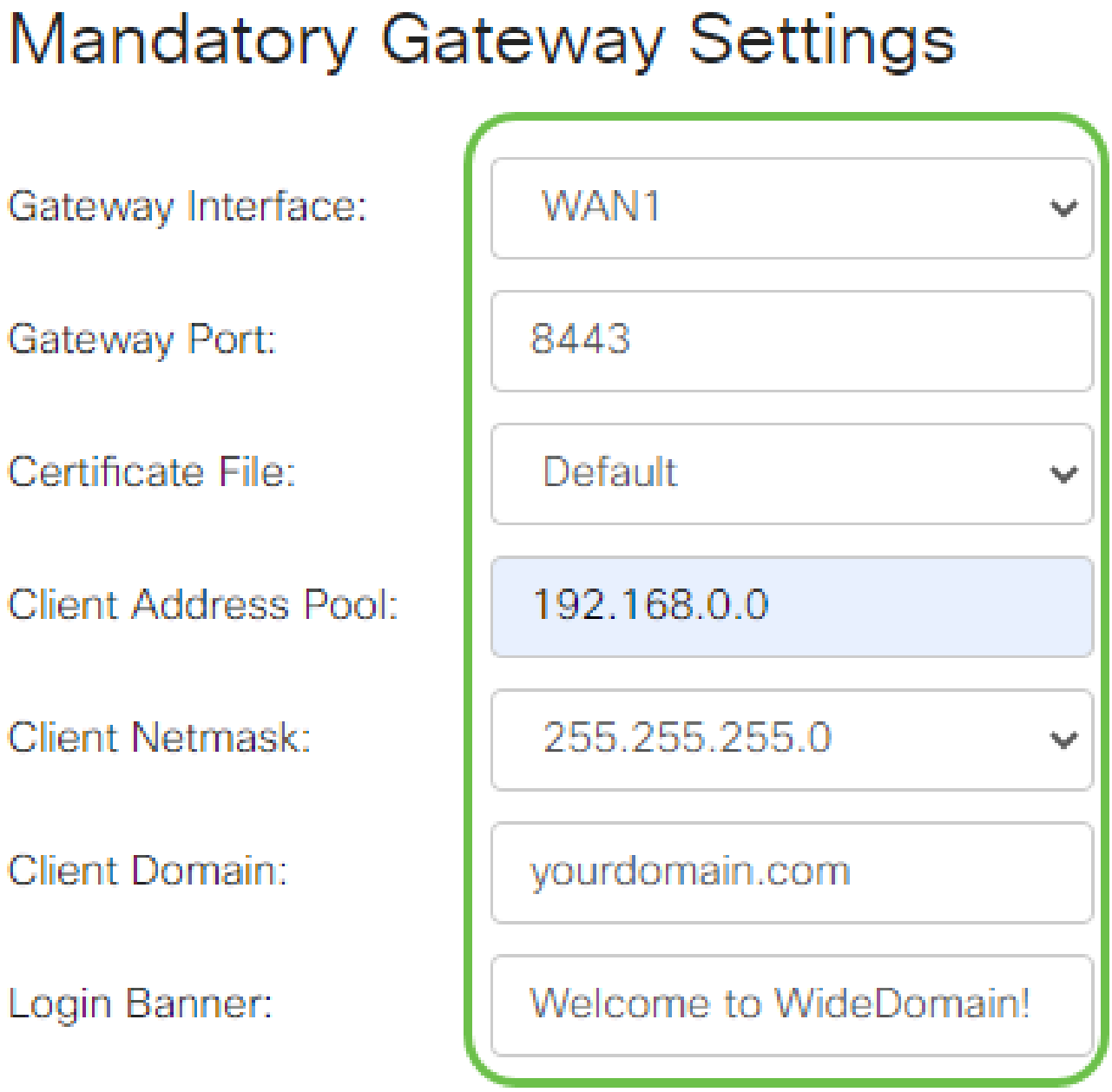
Passo 1

As seguintes definições de configuração são obrigatórias:

1. Escolha a Interface do gateway na lista suspensa. Esta será a porta que será usada para passar o tráfego através dos Túneis VPN SSL. As opções incluem: WAN1, WAN2, USB1, USB2
2. Insira o número da porta usada para o gateway VPN SSL no campo Gateway Port (Porta do gateway) que varia de 1 a 65535.
3. Escolha o Arquivo de certificado na lista suspensa. Este certificado autentica os usuários que tentam acessar o recurso de rede através dos túneis VPN SSL. A lista suspensa contém um certificado padrão e os certificados que são importados.
4. Insira o endereço IP do pool de endereços do cliente no campo Client Address Pool. Este pool será o intervalo de endereços IP que serão alocados para clientes VPN remotos.

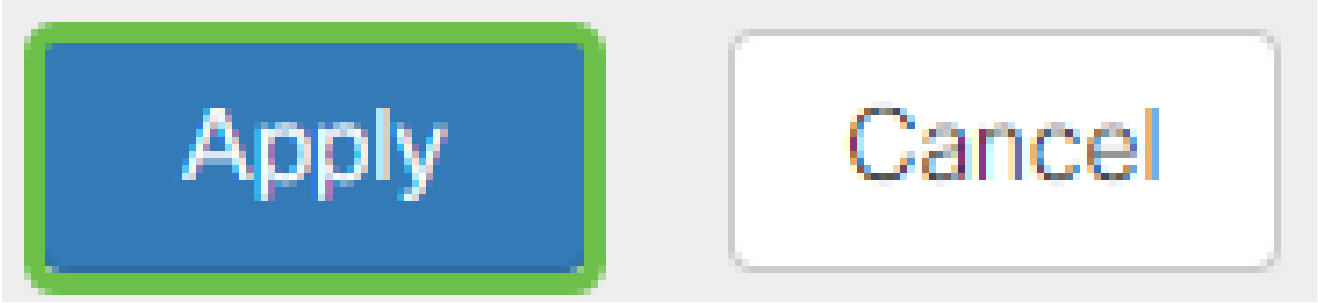
   Verifique se o intervalo de endereços IP não se sobrepõe a nenhum dos endereços IP na rede local.

5. Escolha a Máscara de rede do cliente na lista suspensa.
6. Digite o nome de domínio do cliente no campo Domínio do cliente. Este será o nome de domínio que deve ser enviado aos clientes VPN SSL.
7. Insira o texto que apareceria como um banner de login no campo Banner de login. Este será o banner que será exibido toda vez que um cliente fizer login.



Passo 2

Clique em Apply.

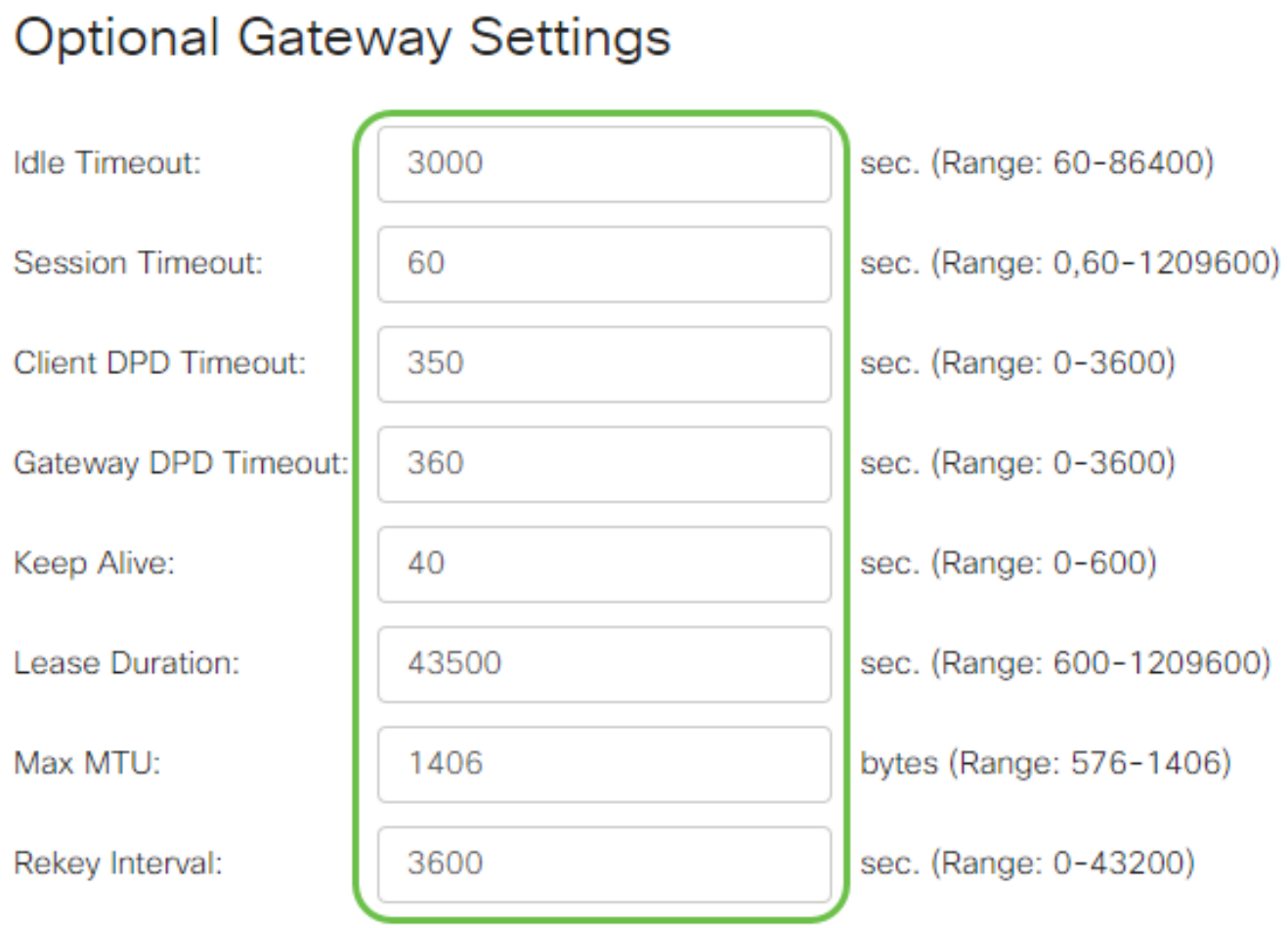


Configurações opcionais do gateway

Passo 1

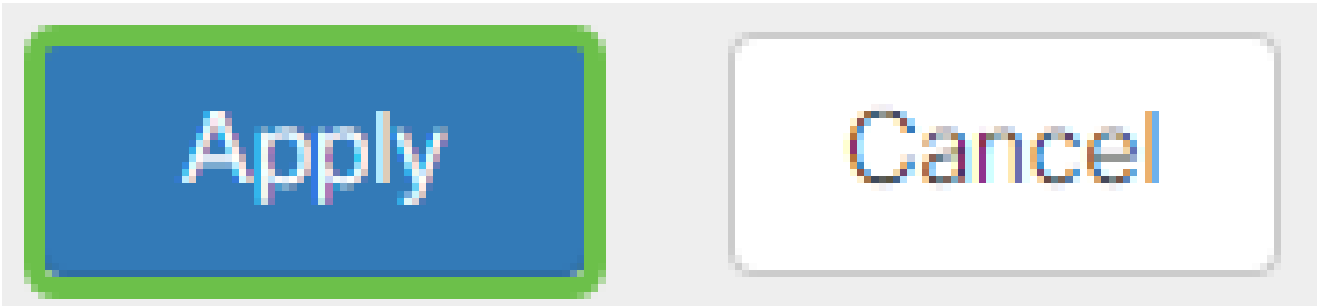
As seguintes definições de configuração são opcionais:

1. Insira um valor em segundos para o intervalo de tempo limite ocioso de 60 a 86400. Esta será a duração de tempo durante a qual a sessão VPN SSL poderá permanecer ociosa.
2. Insira um valor em segundos no campo Tempo limite da sessão. Este é o tempo que leva para que a sessão do Transmission Control Protocol (TCP) ou do User Datagram Protocol (UDP) expire após o tempo ocioso especificado. O intervalo é de 60 a 1209600.
3. Insira um valor em segundos no campo ClientDPD Timeout, variando de 0 a 3600. Esse valor especifica o envio periódico de mensagens HELLO/ACK para verificar o status do túnel VPN. Esse recurso deve ser habilitado em ambas as extremidades do túnel VPN.
4. Insira um valor em segundos no campo GatewayDPD Timeout, variando de 0 a 3600. Esse valor especifica o envio periódico de mensagens HELLO/ACK para verificar o status do túnel VPN. Esse recurso deve ser habilitado em ambas as extremidades do túnel VPN.
5. Insira um valor em segundos no campo Keep Alive variando de 0 a 600. Esse recurso garante que o roteador esteja sempre conectado à Internet. Ele tentará restabelecer a conexão VPN se ela for descartada.
6. Insira um valor em segundos para a duração do túnel a ser conectado no campo Lease Duration. O intervalo é de 600 a 1209600.
7. Insira o tamanho do pacote em bytes que pode ser enviado pela rede. O intervalo é de 576 a 1406.
8. Insira o tempo do intervalo de retransmissão no campo Rekey Interval. O recurso Rechavear permite que as chaves SSL renegociem após o estabelecimento da sessão. O intervalo é de 0 a 43200.



Passo 2

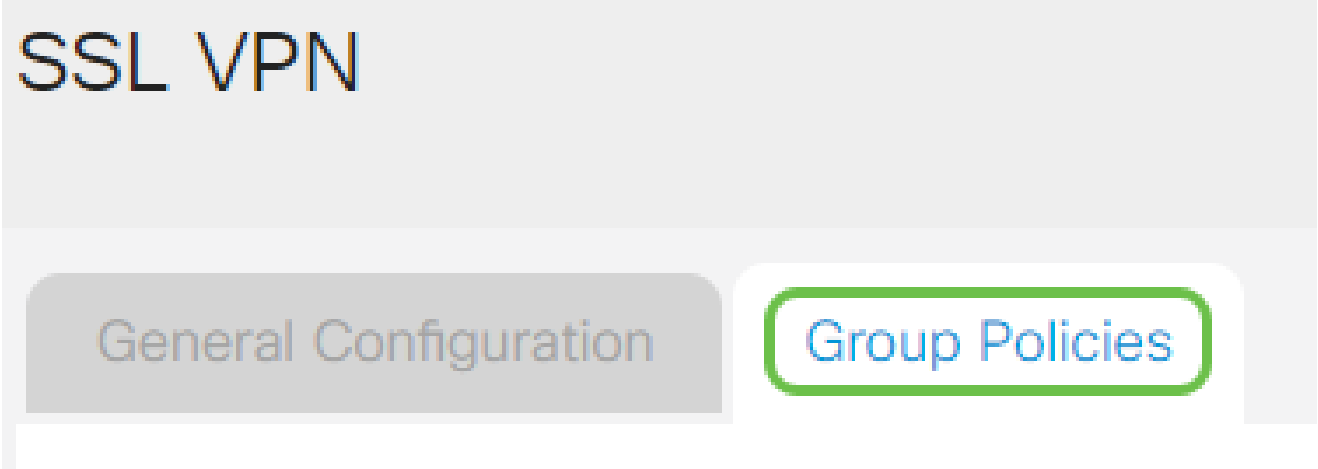
Clique em Apply.



Configurar Políticas de Grupo

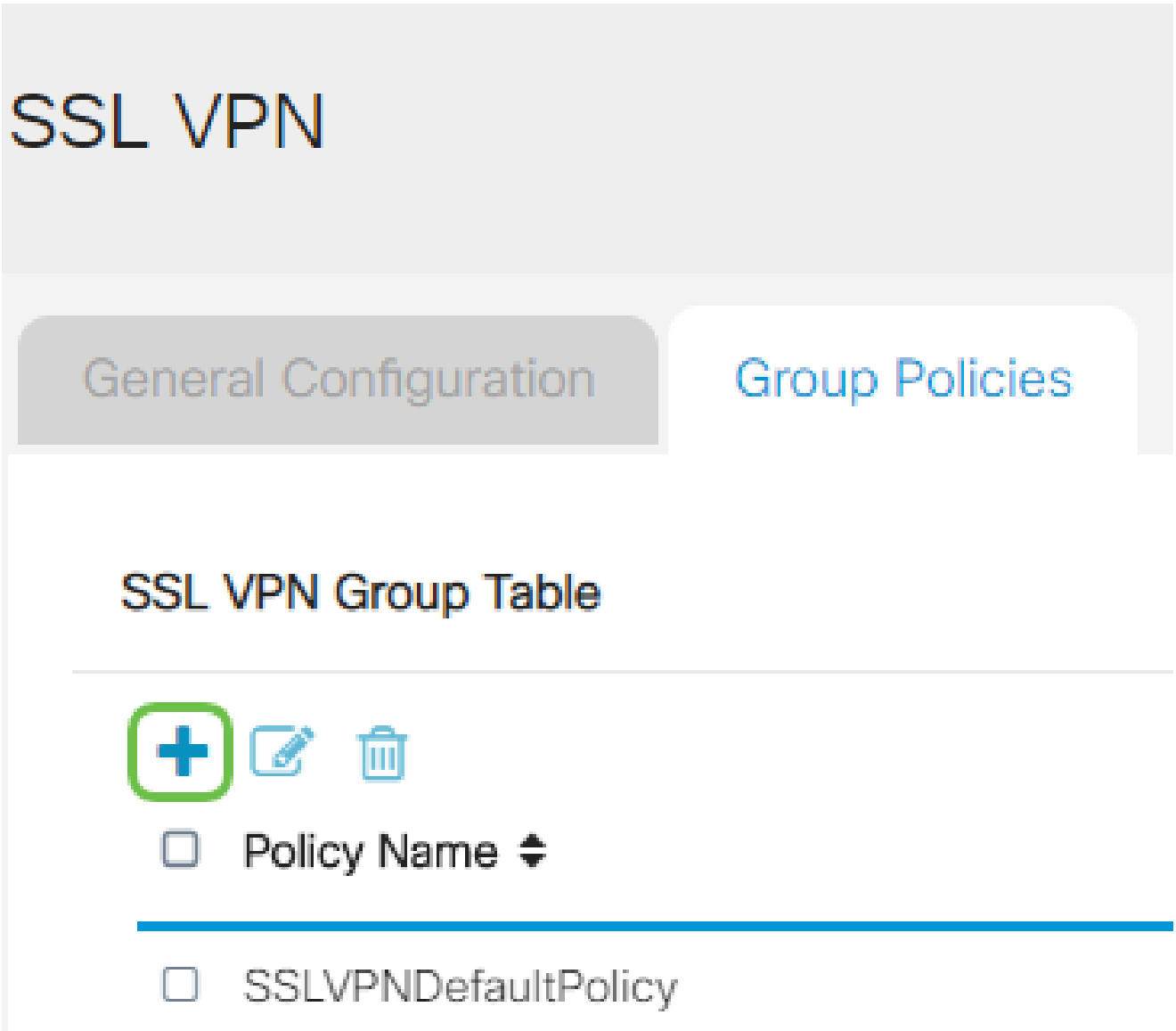
Passo 1

Clique na guia Group Policies.



Passo 2

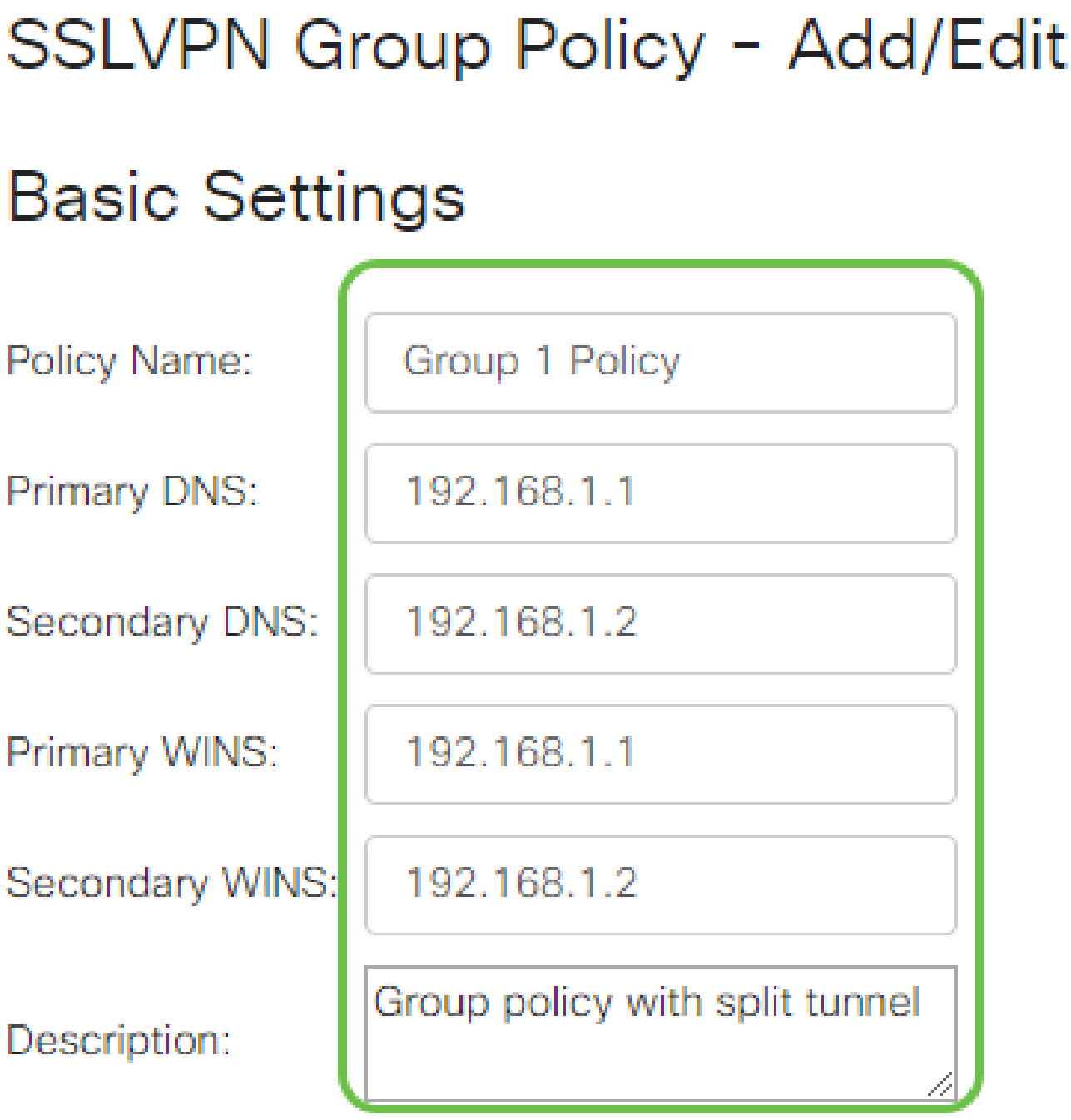
Clique no ícone add na tabela de grupos VPN SSL para adicionar uma política de grupo.



A tabela Grupo de VPN SSL mostrará a lista de políticas de grupo no dispositivo. Você também pode editar a primeira política de grupo na lista, que se chama SSLVPNDefaultPolicy. Esta é a política padrão fornecida pelo dispositivo.

Etapa 3

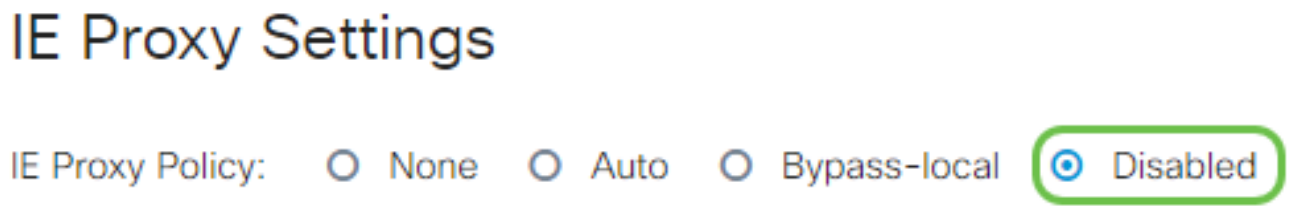
1. Insira o nome da política de sua preferência no campo Policy Name.
2. Insira o endereço IP do DNS primário no campo fornecido. Por padrão, esse endereço IP já é fornecido.
3. (Opcional) Insira o endereço IP do DNS secundário no campo fornecido. Isso servirá como backup em caso de falha do DNS primário.
4. (Opcional) Digite o endereço IP do WINS primário no campo fornecido.
5. (Opcional) Insira o endereço IP do WINS secundário no campo fornecido.
6. (Opcional) Digite uma descrição da política no campo Description.



Etapa 4 (opcional)

Clique em um botão de opção para escolher IE Proxy Policy (Diretiva de proxy do IE) para ativar as configurações de proxy do Microsoft Internet Explorer (MSIE) para estabelecer o túnel VPN. As opções são:

- Nenhum - Permite que o navegador não use configurações de proxy.
- Automático - Permite que o navegador detecte automaticamente as configurações de proxy.
- Bypass-local - Permite que o navegador ignore as configurações de proxy definidas no usuário remoto.
- Desabilitado - Desabilita as configurações de proxy MSIE.



Etapa 5 (opcional)

Na área Split Tunneling Settings, marque a caixa de seleção Enable Split Tunneling para permitir que o tráfego destinado à Internet seja enviado sem criptografia diretamente para a Internet. O Encapsulamento Completo envia todo o tráfego para o dispositivo final, onde é então roteado para os recursos de destino, eliminando a rede corporativa do caminho para o acesso à Web.

Etapa 6 (opcional)

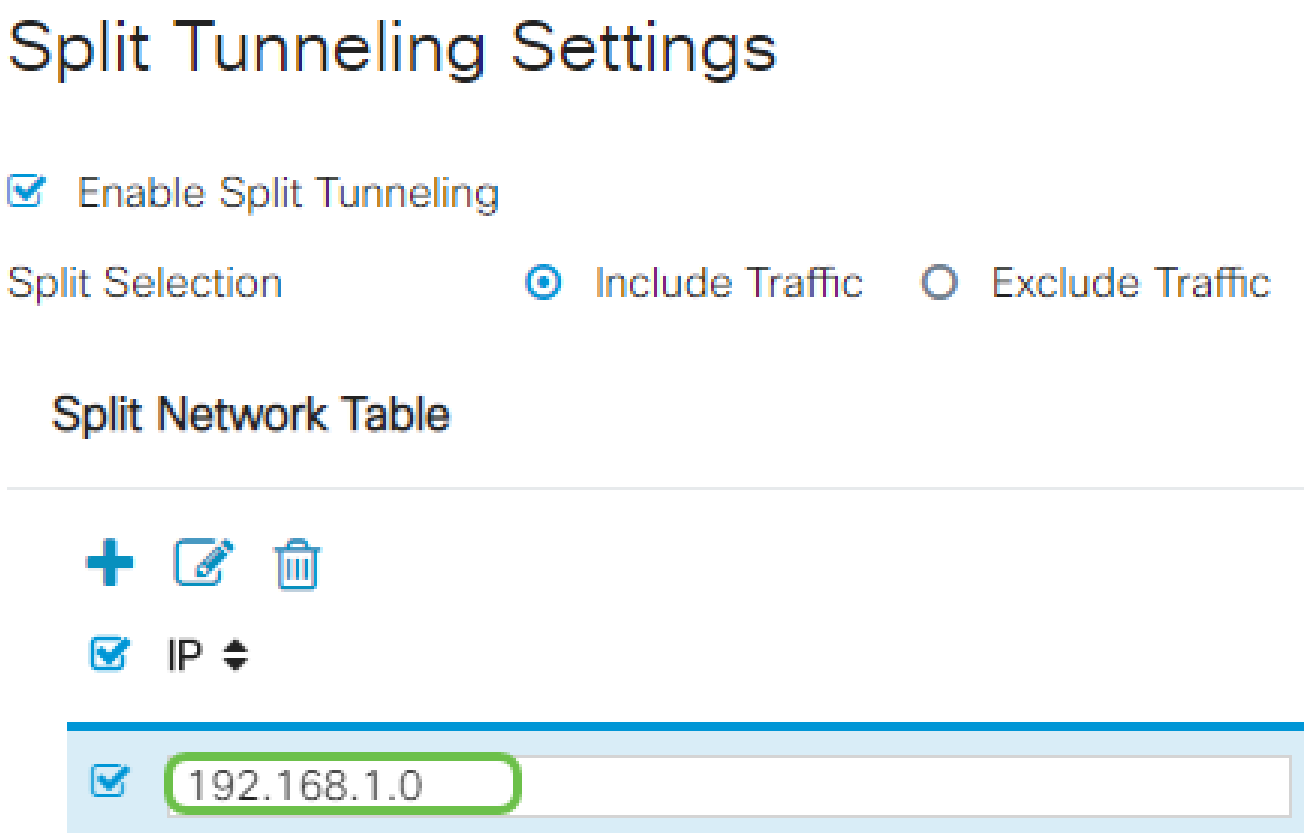
Clique em um botão de opção para escolher se deseja incluir ou excluir tráfego ao aplicar o tunelamento dividido.

Etapa 7

Na tabela Dividir rede, clique no ícone adicionar para adicionar uma exceção Dividir rede.

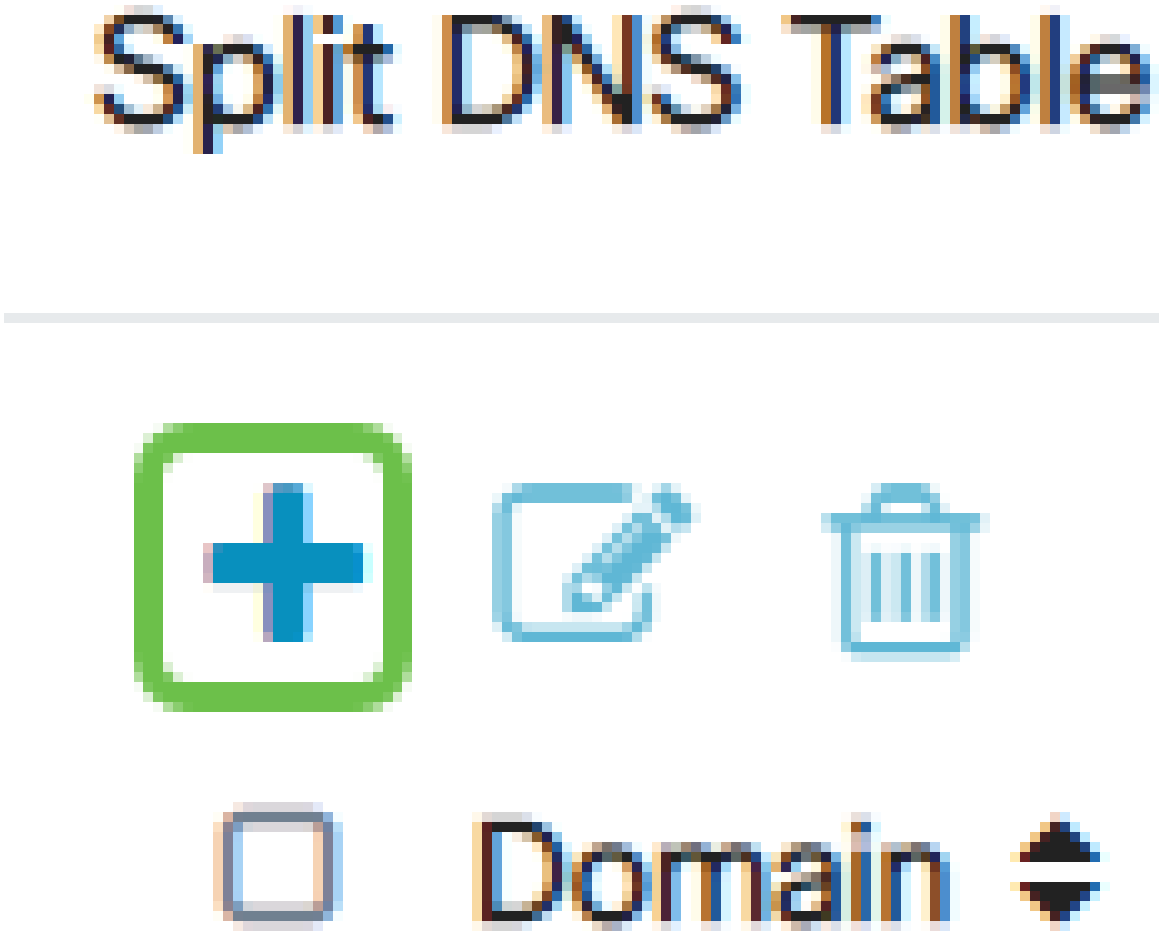
Passo 8

Insira o endereço IP da rede no campo fornecido.



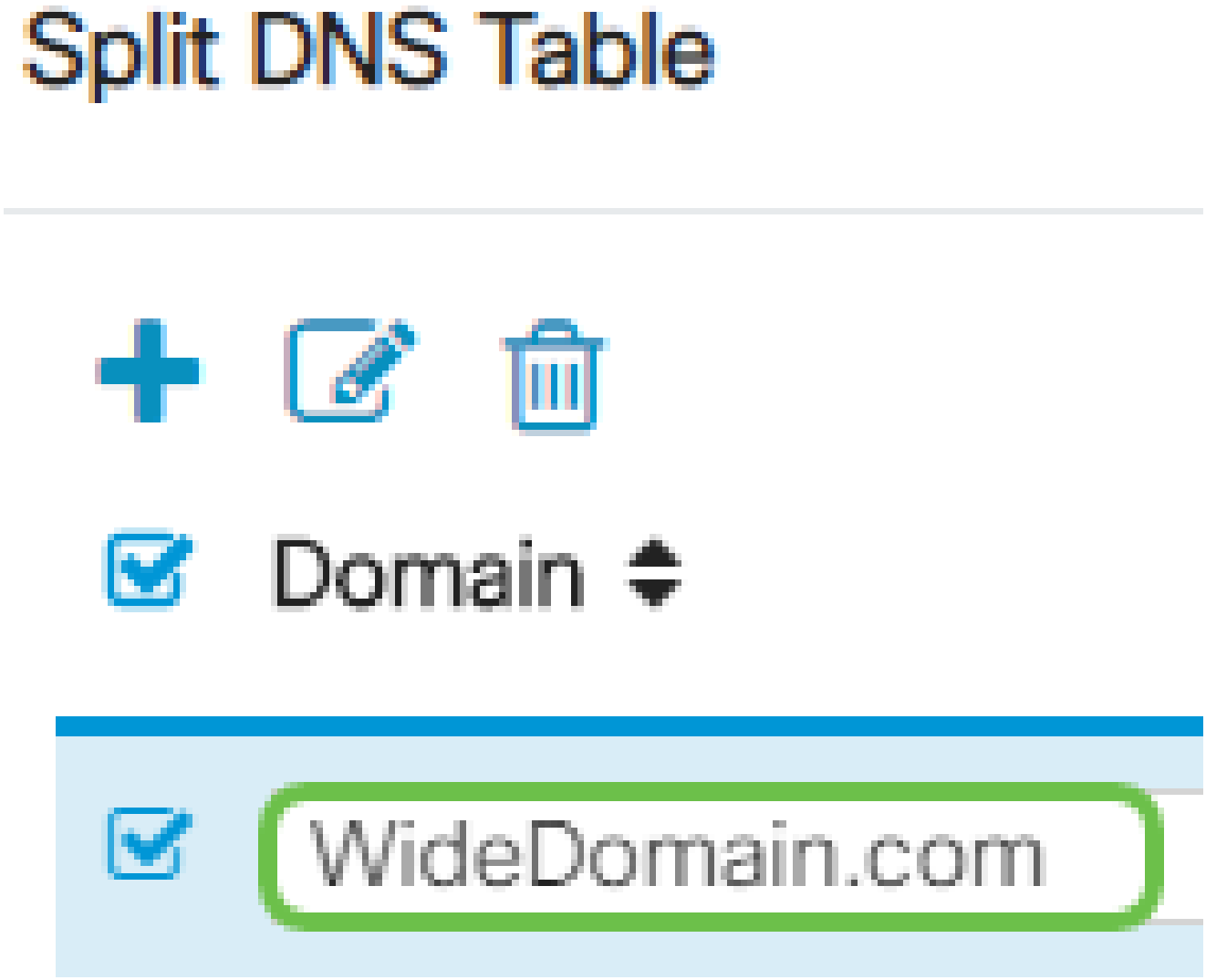
Passo 9

Na Tabela DNS dividida, clique no ícone adicionar para adicionar uma exceção DNS dividida.



Passo 10

Insira o nome de domínio no campo fornecido e clique em Aplicar.



O roteador vem com 2 licenças de servidor AnyConnect por padrão. Isso significa que, uma vez que você tenha licenças de cliente AnyConnect, você pode estabelecer 2 túneis VPN simultaneamente com qualquer outro roteador da série RV340.

Resumindo, o roteador RV345P não precisa de uma licença, mas todos os clientes precisarão de uma. As licenças de cliente AnyConnect permitem que clientes móveis e de desktop acessem a rede VPN remotamente.

A próxima seção detalha como obter licenças para seus clientes.

Cliente AnyConnect Mobility

Um cliente VPN é um software instalado e executado em um computador que deseja se conectar à rede remota. Esse software cliente deve ser configurado com a mesma configuração do servidor VPN, como o endereço IP e as informações de autenticação. Essas informações de autenticação incluem o nome de usuário e a chave pré-compartilhada que será usada para criptografar os dados. Dependendo da localização física das redes a serem conectadas, um cliente VPN também pode ser um dispositivo de hardware. Isso

geralmente acontece se a conexão VPN for usada para conectar duas redes que estão em locais separados.

O Cisco AnyConnect Secure Mobility Client é um aplicativo de software para conexão com uma VPN que funciona em vários sistemas operacionais e configurações de hardware. Esse aplicativo de software possibilita que os recursos remotos de outra rede se tornem acessíveis como se o usuário estivesse diretamente conectado à sua rede, mas de forma segura.

Depois que o roteador é registrado e configurado com o AnyConnect, o cliente pode instalar licenças no roteador a partir do seu pool disponível de licenças que você compra, que é detalhado na próxima seção.

Comprar licença

Você deve comprar uma licença de seu distribuidor ou parceiro da Cisco. Ao solicitar uma licença, você deve fornecer sua ID de Conta inteligente da Cisco ou ID de domínio no formato name@domain.com.

Se você não tiver um distribuidor ou parceiro da Cisco, localize um aqui.

No momento em que este documento foi escrito, as SKUs de produto a seguir podem ser usadas para adquirir licenças adicionais em pacotes de 25. Observe que há outras opções para as licenças de cliente do AnyConnect, conforme descrito no Guia de pedidos do Cisco AnyConnect. No entanto, a ID do produto listada seria o requisito mínimo para funcionalidade total.

Observe que a SKU de produto de licença de cliente do AnyConnect listada primeiro, fornece licenças para um período de 1 ano e exige uma compra mínima de 25 licenças. Outras SKUs de produto aplicáveis aos roteadores da série RV340 também estão disponíveis com níveis de assinatura variáveis, como a seguir:

- LS-AC-PLS-1Y-S1 — licença de cliente Cisco AnyConnect Plus de 1 ano
- LS-AC-PLS-3Y-S1 — licença de cliente Cisco AnyConnect Plus de 3 anos
- LS-AC-PLS-5Y-S1 — licença de cliente Cisco AnyConnect Plus de 5 anos
- LS-AC-PLS-P-25-S — licença de cliente perpétuo Cisco AnyConnect Plus com 25 pacotes
- LS-AC-PLS-P-50-S — pacote com 50 licenças perpétuas do Cisco AnyConnect Plus

Informações do cliente

Quando o cliente configurar um dos itens a seguir, você deverá enviar a eles estes links:

- Windows: AnyConnect em um computador Windows
- Mac: instale o AnyConnect no Mac.
- Ubuntu Desktop: instalação e uso do AnyConnect no Ubuntu Desktop
- Se você tiver problemas, vá para Coletar informações para solução básica de problemas sobre erros do Cisco AnyConnect Secure Mobility Client.

Verificar a conectividade do AnyConnect VPN

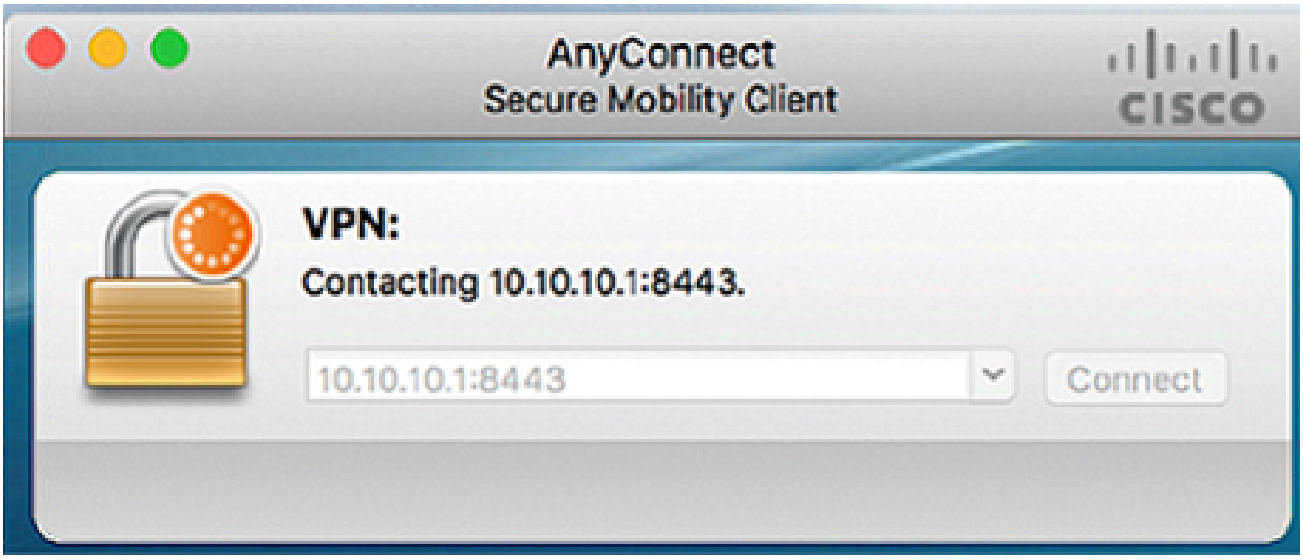
Passo 1

Clique no ícone AnyConnect Secure Mobility Client.

Passo 2

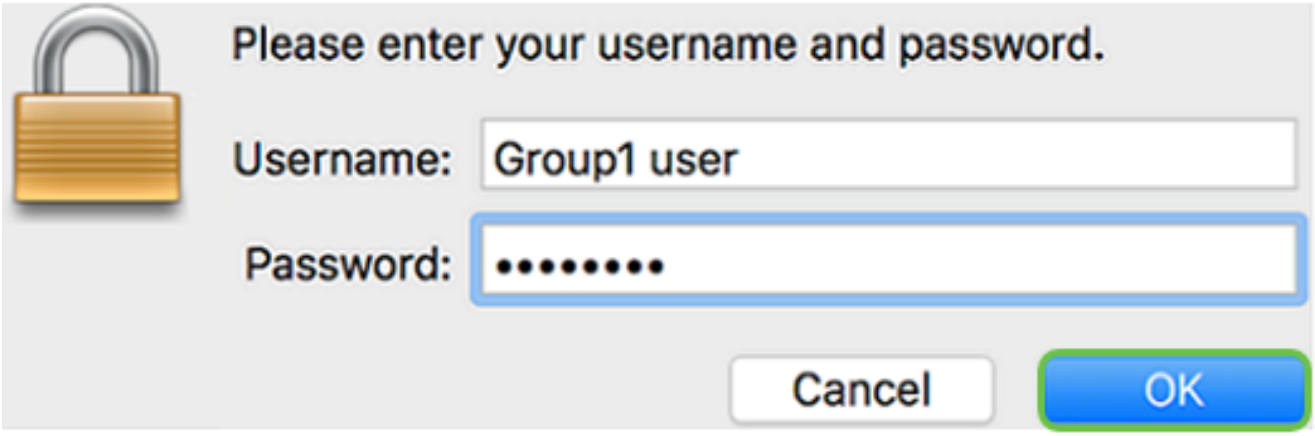
Na janela AnyConnect Secure Mobility Client, insira o endereço IP do gateway e o número da porta do gateway separados por dois-pontos (:) e clique em Connect.

O software agora mostrará que está entrando em contato com a rede remota.



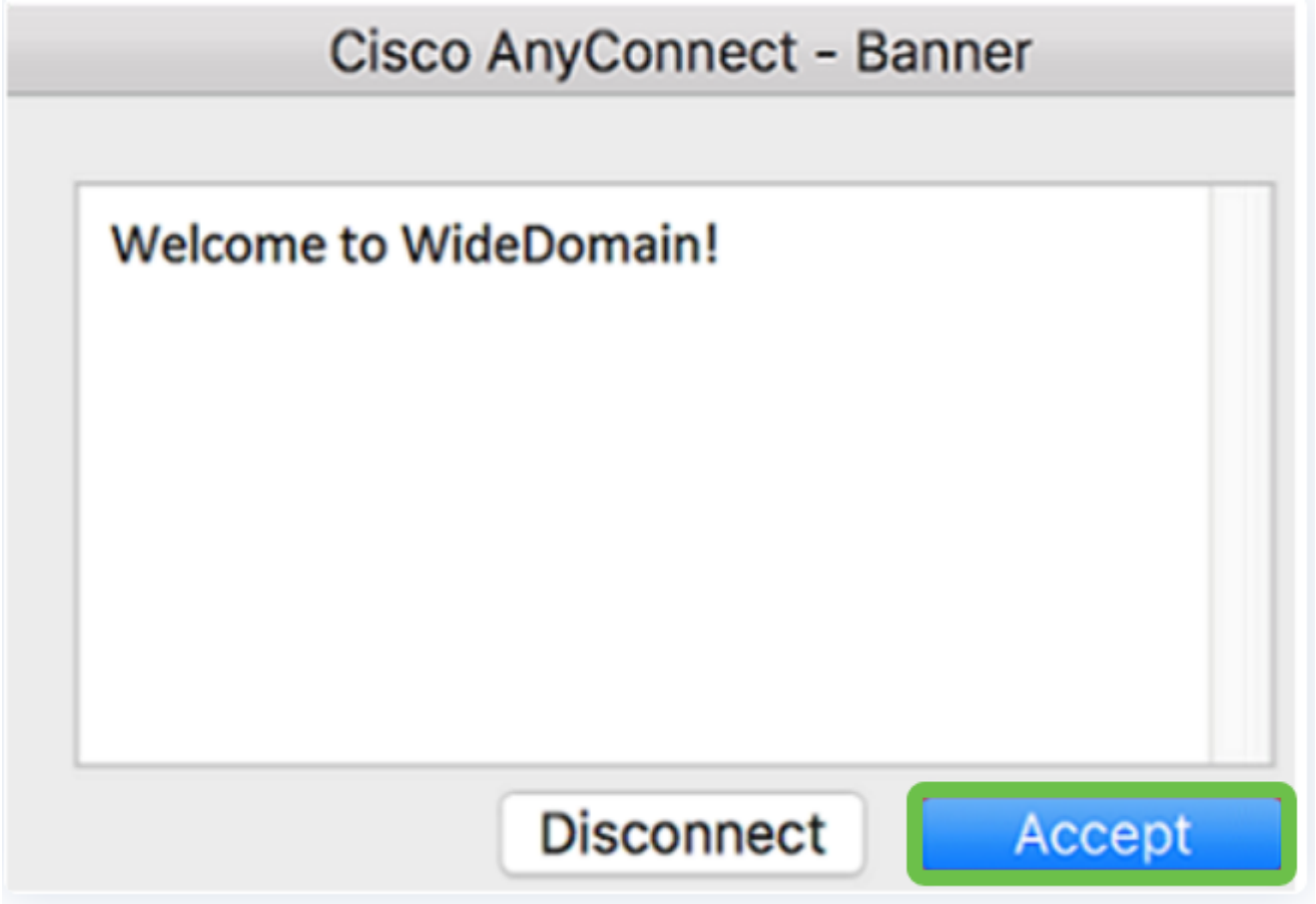
Etapa 3

Insira o nome de usuário e a senha do servidor nos respectivos campos e clique em OK.

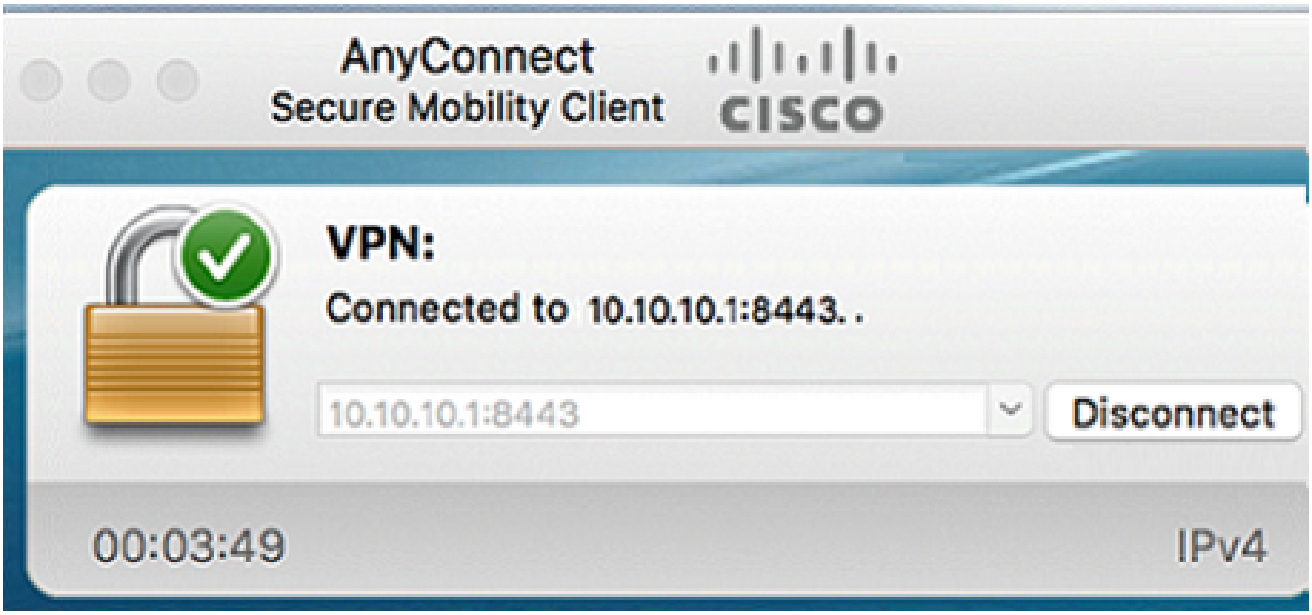


Passo 4

Assim que a conexão for estabelecida, o banner de login será exibido. Clique em Aceitar.



A janela do AnyConnect deve indicar agora a conexão VPN bem-sucedida com a rede.



Se você estiver usando o AnyConnect VPN, poderá ignorar outras opções de VPN e passar para a próxima seção.

Shrew Soft VPN

Uma VPN IPsec permite que você obtenha recursos remotos com segurança, estabelecendo um túnel criptografado na Internet. Os roteadores da série RV34X funcionam

como servidores VPN IPsec e suportam o cliente Shrew Soft VPN. Esta seção mostrará como configurar seu roteador e o Shrew Soft Client para proteger uma conexão a uma VPN.

A Cisco não oferece suporte a Shrew Soft. Este exemplo é fornecido apenas para fins de demonstração. Se você tiver problemas com a Shrew Soft, entre em contato com ela para obter suporte.

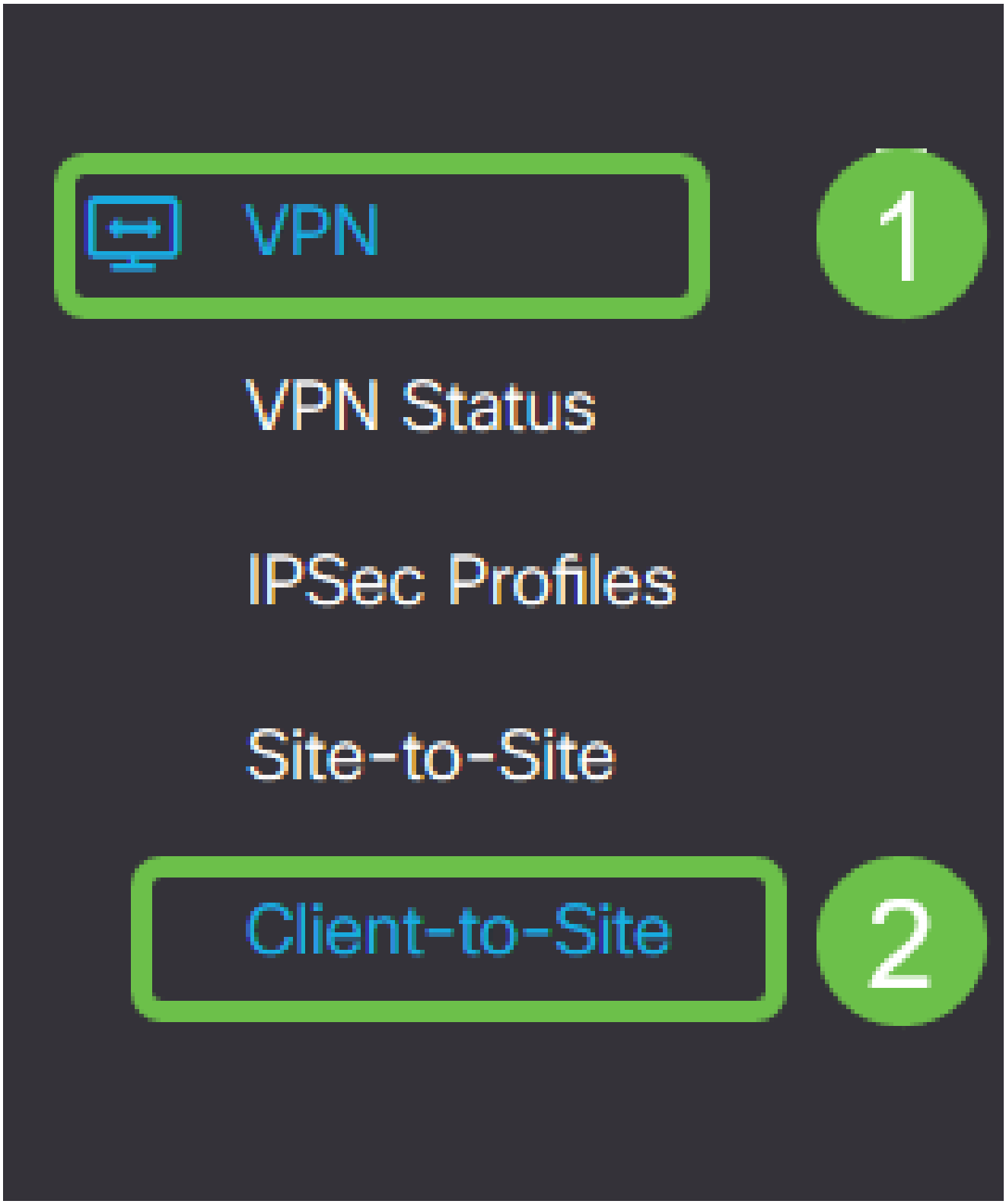
Você pode baixar a versão mais recente do software cliente Shrew Soft VPN aqui: https://www.shrew.net/download/vpn

Configurar o Shrew Soft no Roteador da Série RV345P

Começaremos configurando a VPN Cliente a Site no RV345P.

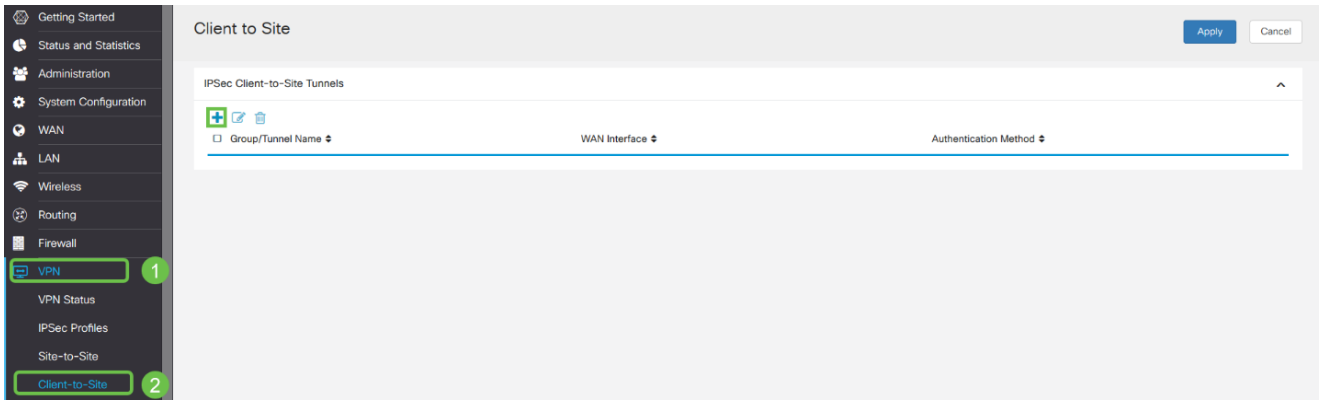
Passo 1

Navegue até VPN > Client-to-Site.



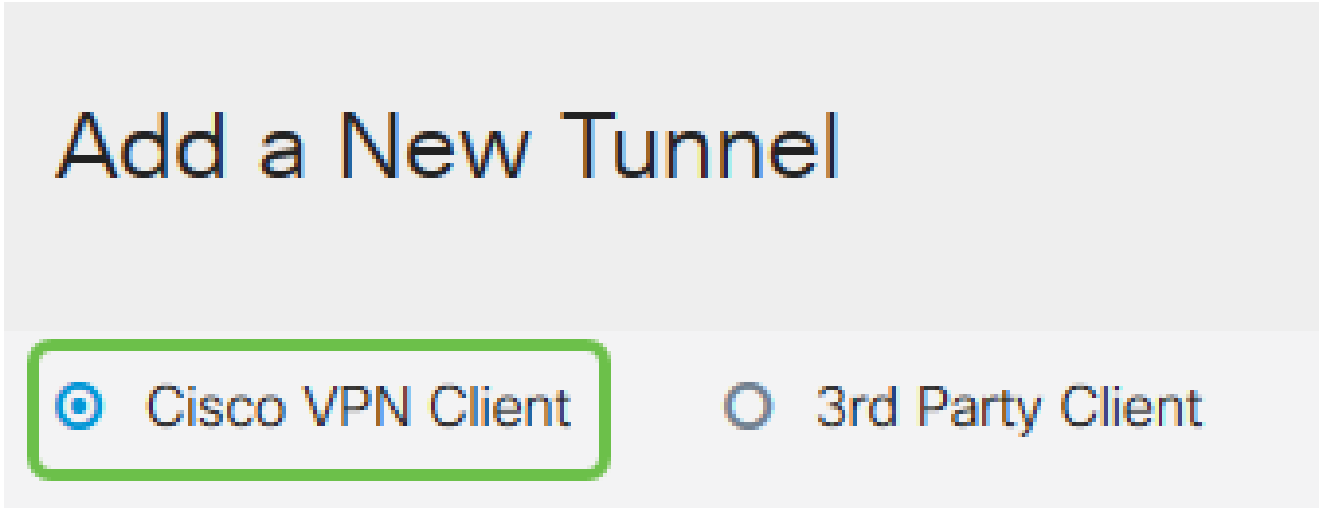
Passo 2

Adicione um perfil de VPN de cliente para site.



Etapa 3

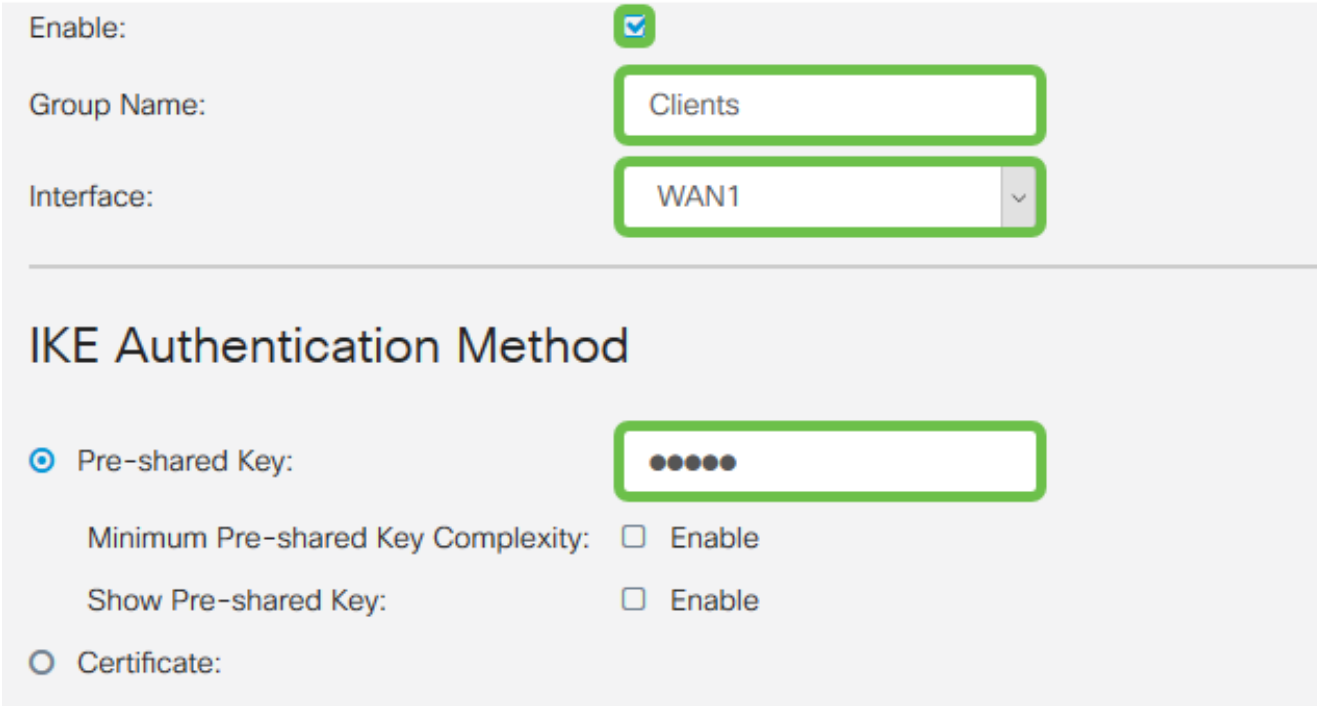
Selecione a opção Cisco VPN Client.



Passo 4

Marque a caixa Enable para ativar o Perfil de cliente VPN. Também configuraremos o Nome do grupo, selecionaremos a interface WAN e digitaremos uma Chave pré-compartilhada.

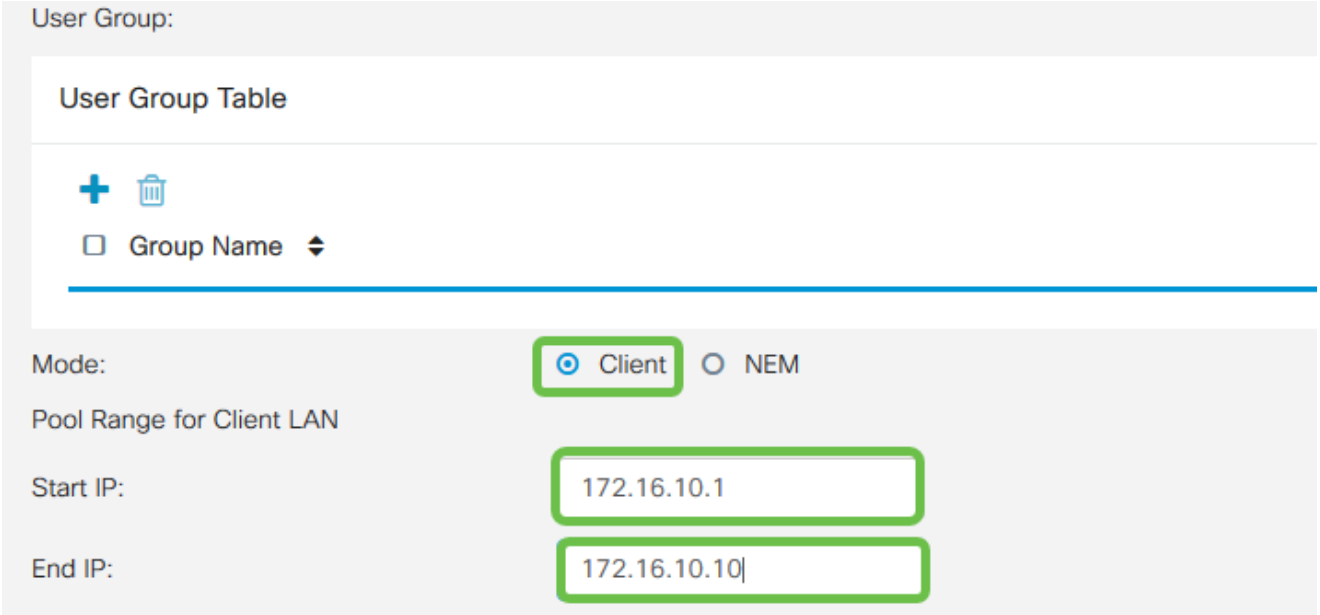
Observe o Nome do grupo e a Chave pré-compartilhada, pois eles serão usados mais tarde ao configurar o cliente.



Etapa 5

Por enquanto, deixe a Tabela de grupos de usuários em branco. Isso é para o grupo de usuários no roteador, mas ainda não o configuramos. Verifique se Mode está definido como Client. Digite o Intervalo do Pool para a LAN do Cliente. Usaremos de 172.16.10.1 a 172.16.10.10.

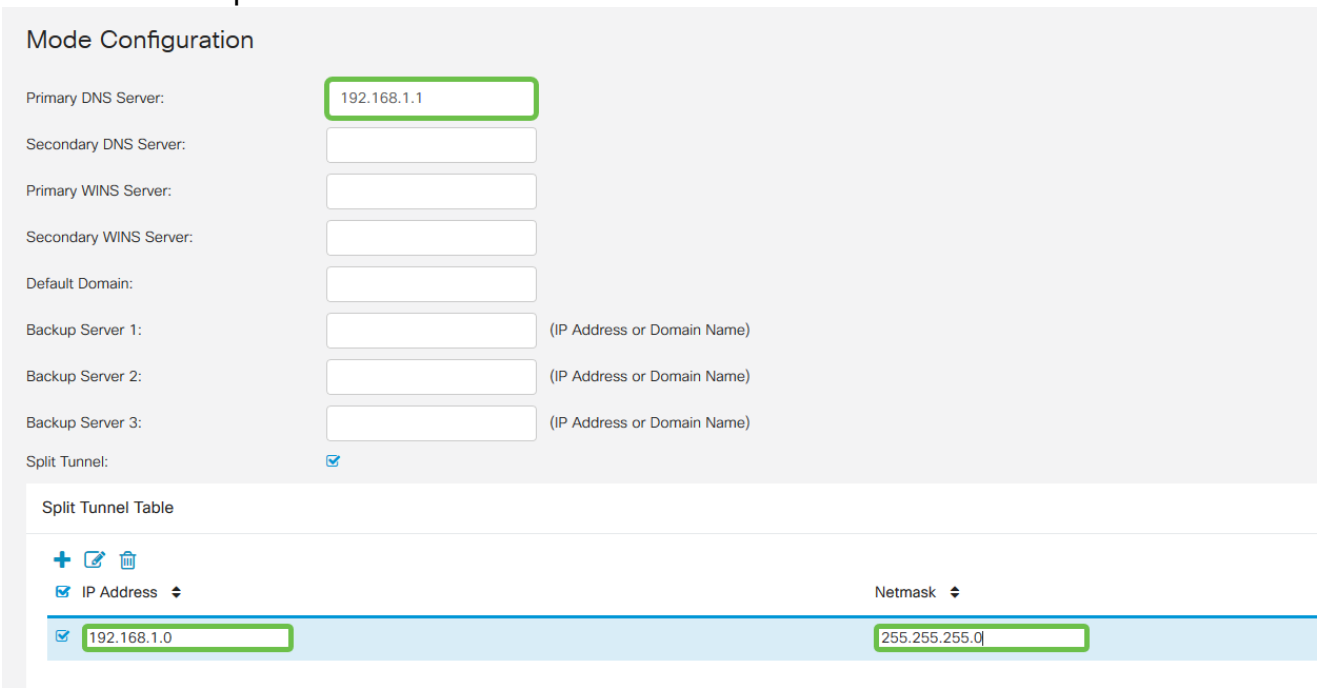
O Intervalo de Pool deve usar uma sub-rede exclusiva que não seja usada em nenhum outro lugar da rede.



Etapa 6

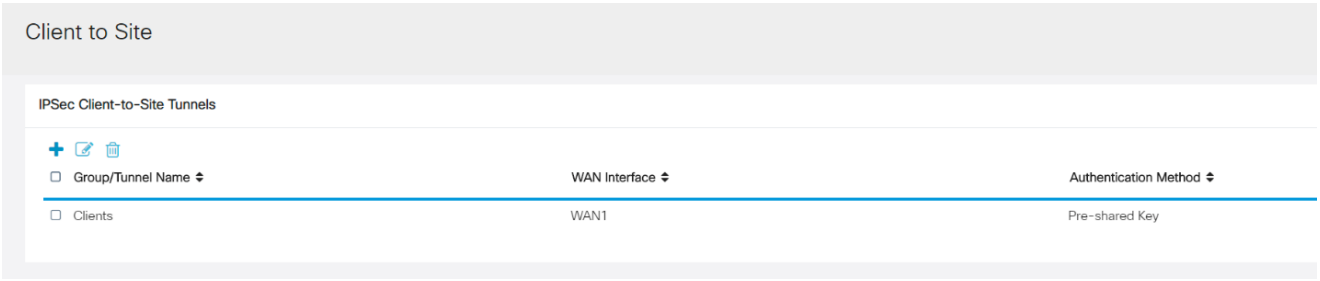
Aqui é onde definimos as configurações de configuração do modo. Aqui estão as configurações que usaremos:

- Servidor DNS primário: se tiver um servidor DNS interno ou quiser usar um servidor DNS externo, você pode inseri-lo aqui. Caso contrário, o padrão é definido como o endereço IP da LAN RV345P. Usaremos o padrão em nosso exemplo.
- Split Tunnel: Marque para habilitar o Split Tunneling. Isso é usado para especificar qual tráfego passará pelo túnel VPN. Usaremos o Split Tunnel em nosso exemplo.
- Split Tunnel Table: insira as redes às quais o cliente VPN deve ter acesso pela VPN. Este exemplo usa a rede LAN RV345P.



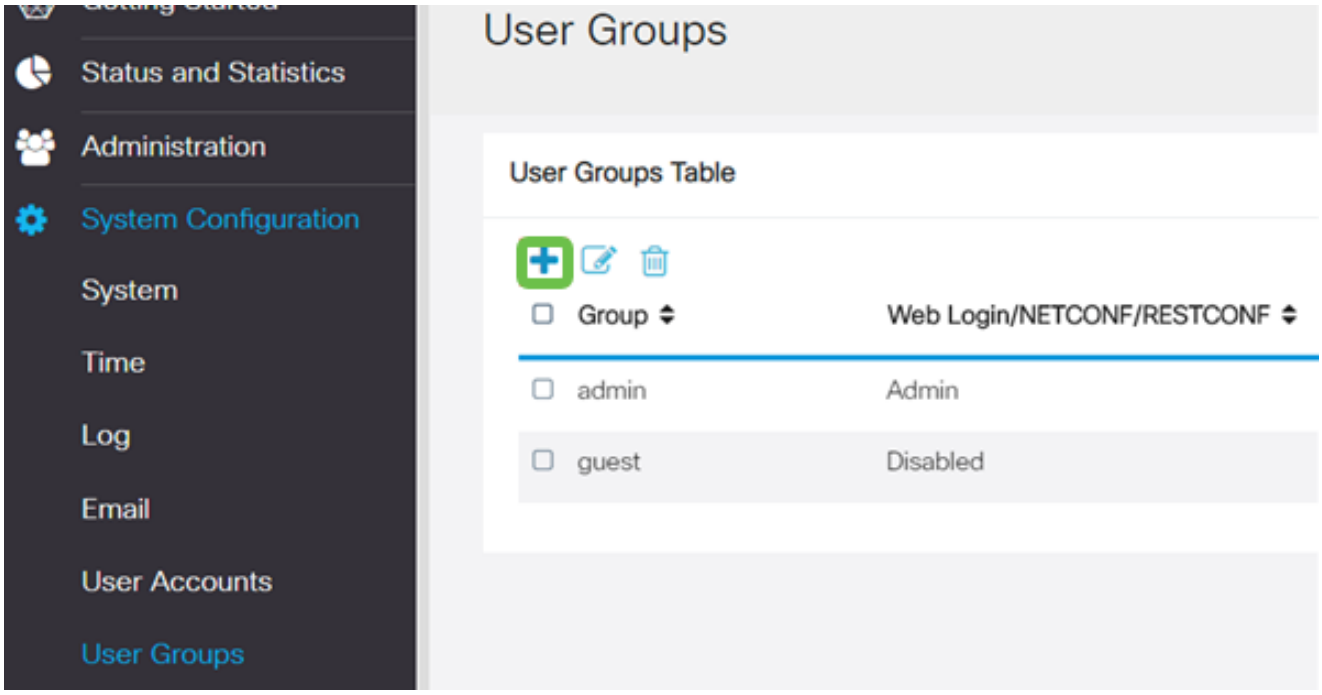
Etapa 7

Após clicar em Save, podemos ver o perfil na lista IPsec Client-to-Site Groups.



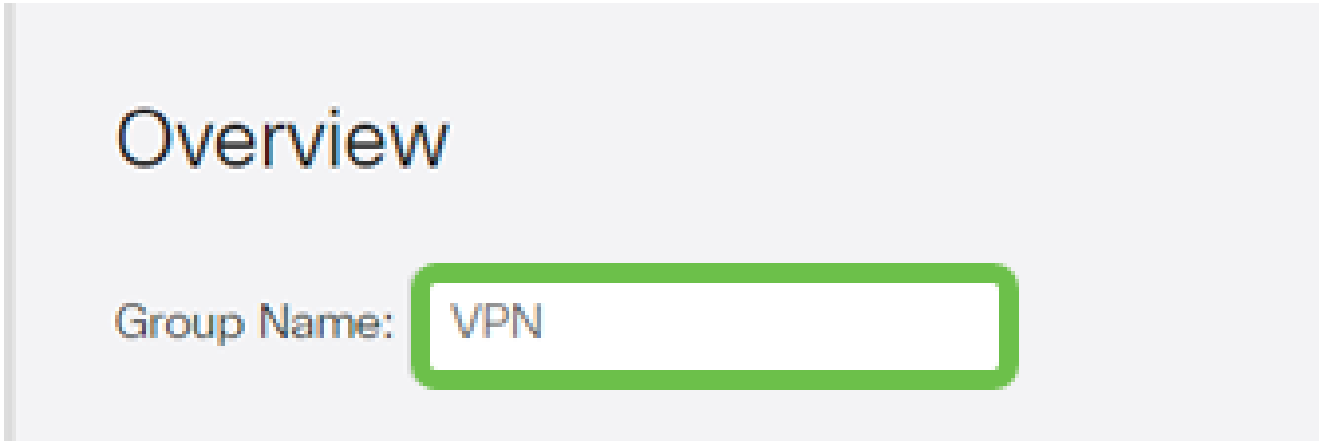
Passo 8

Configure um Grupo de Usuários para usar na Autenticação de usuários de clientes VPN. Em System Configuration > User Groups, clique no ícone de mais para adicionar um grupo de usuários.



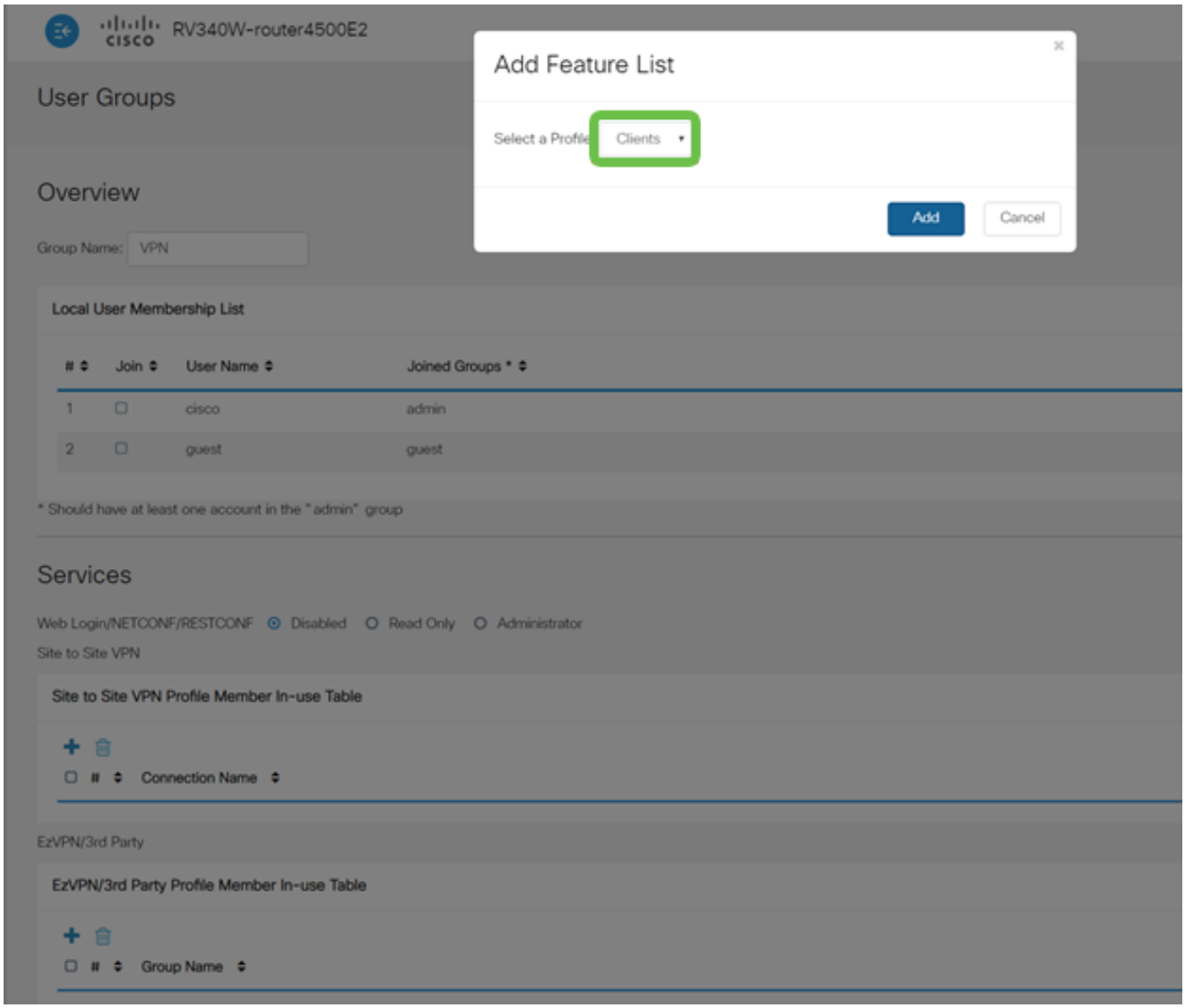
Passo 9

Insira um nome de grupo.



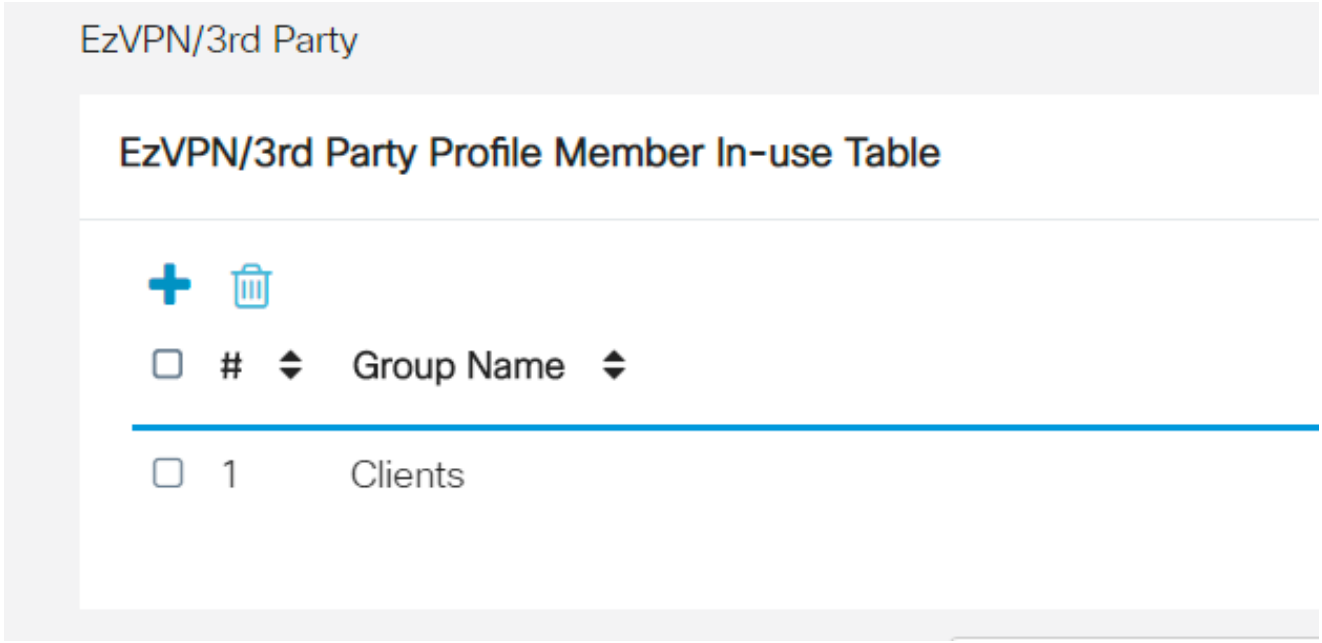
Passo 10

Em Services > EzVPN/3rd Party, clique em Add para vincular este grupo de usuários ao perfil Client-to-Site que foi configurado anteriormente.



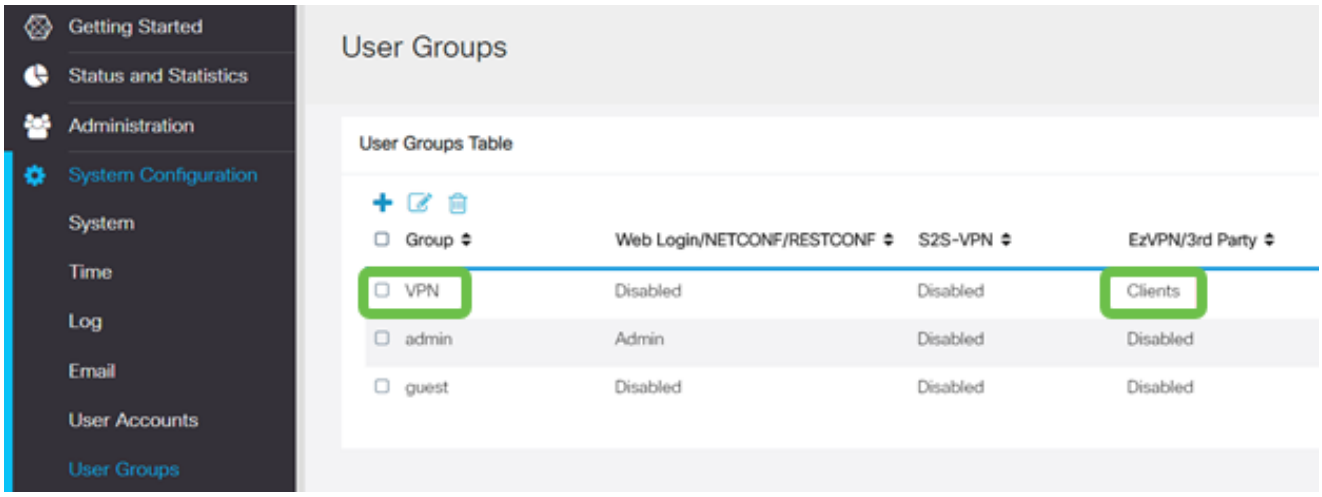
Passo 11

Agora você deve ver o nome do grupo de cliente para site na lista para EzVPN/terceiros.



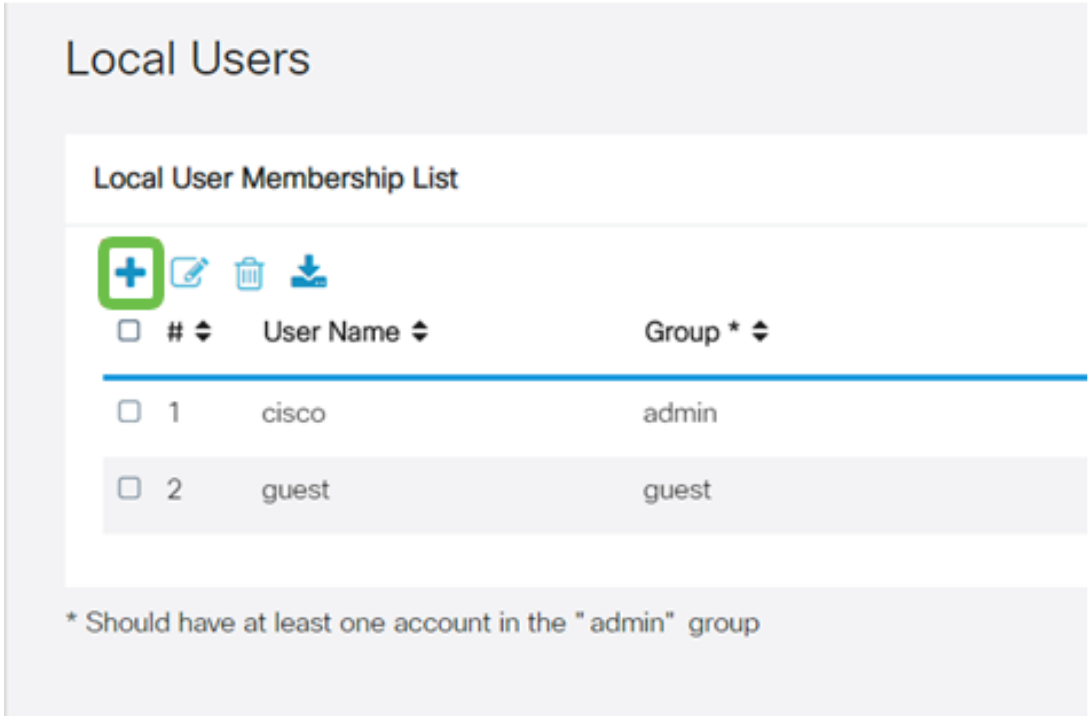
Etapa 12

Depois de aplicar a configuração do grupo de usuários, você a verá na lista Grupos de usuários e ela mostrará o novo grupo de usuários que será usado com o perfil de cliente para site criado anteriormente.



Passo 13

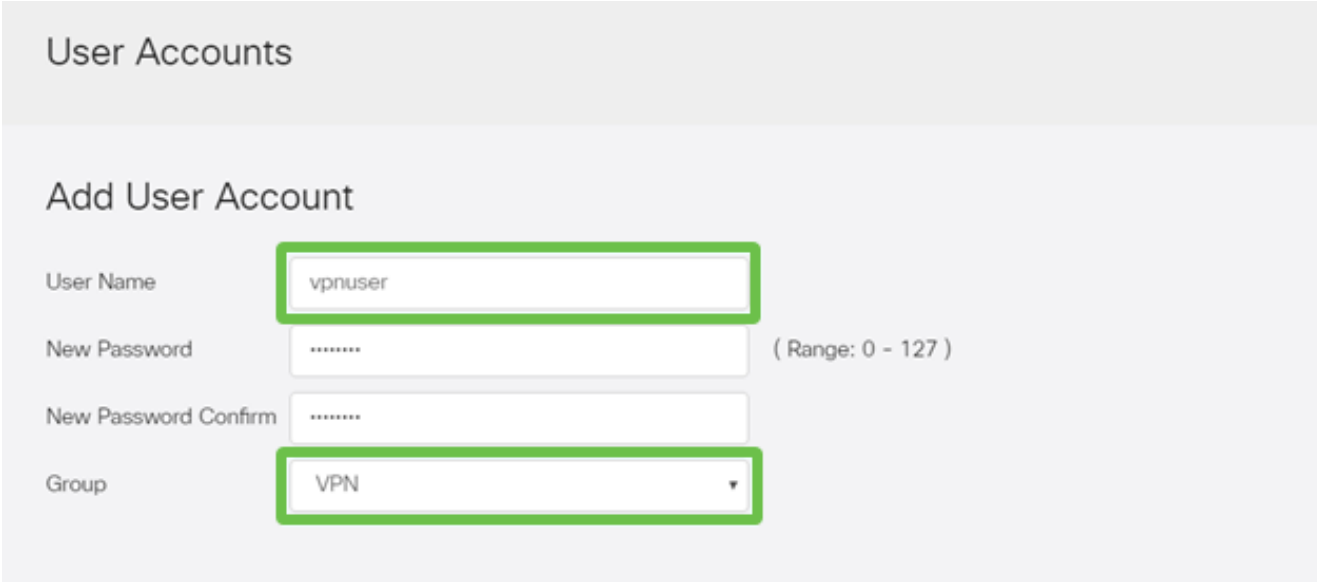
Configure um novo usuário em System Configuration > User Accounts. Clique no ícone de adição para criar um novo usuário.



Passo 14

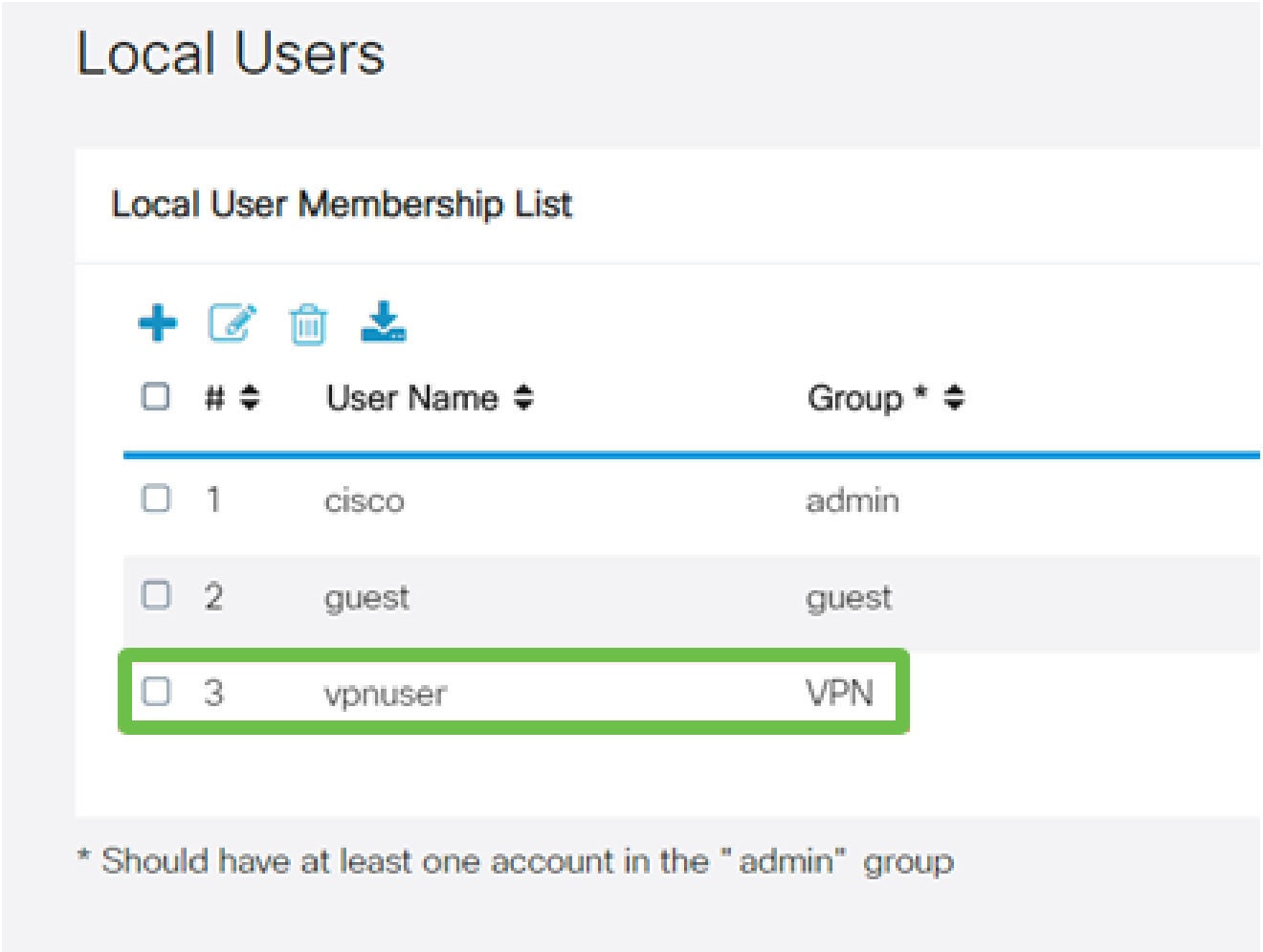
Insira o novo Nome de usuário junto com a Nova senha. Verifique se o Grupo está definido

como o novo Grupo de usuários que você acabou de configurar. Clique em Apply quando terminar.



Etapa 15

O novo Usuário aparecerá na lista de Usuários Locais.



Isso conclui a configuração no RV345P Series Router. Em seguida, você configurará o

cliente Shrew Soft VPN.

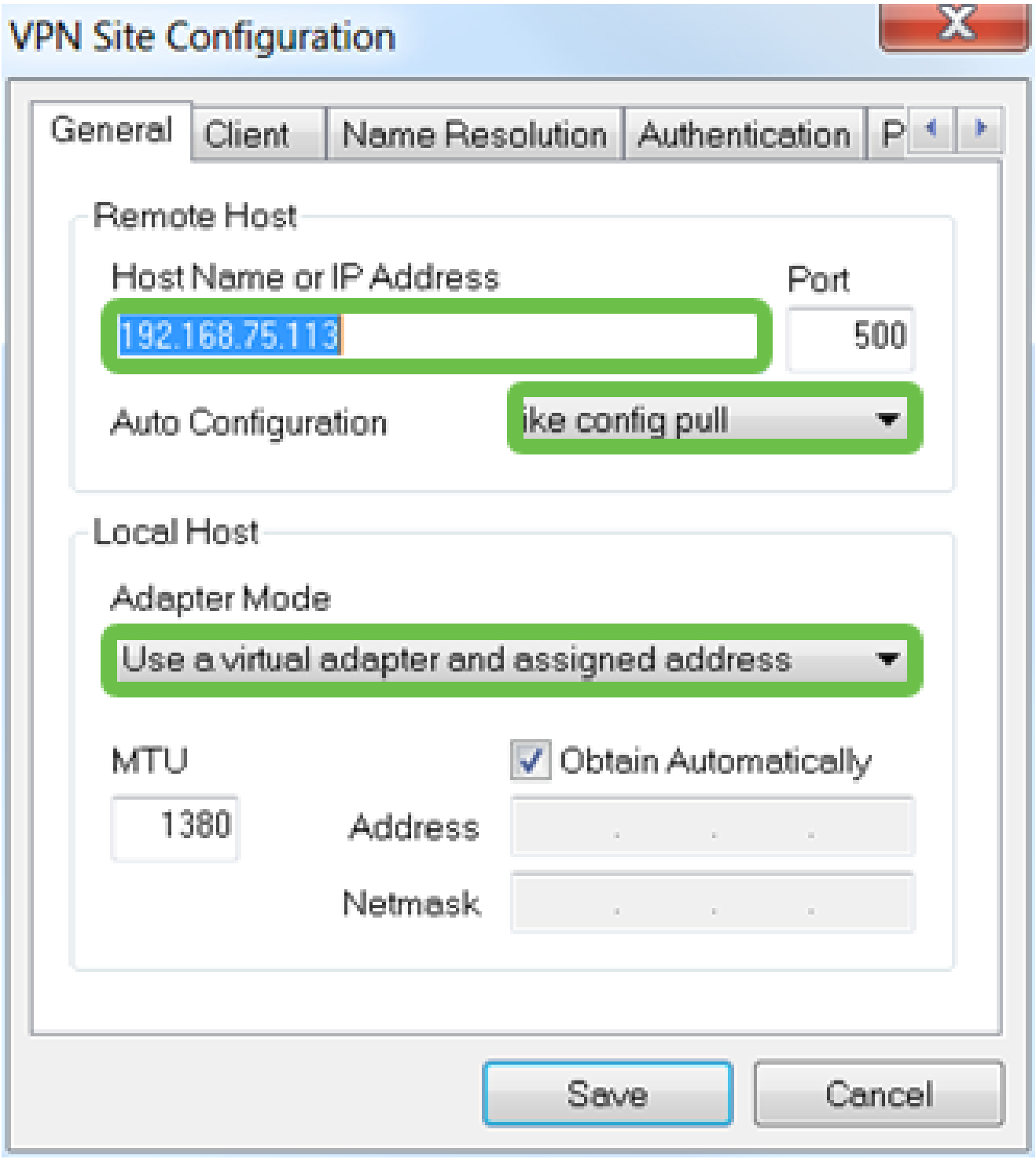
Configurar o cliente Shrew Soft VPN

Execute as seguintes etapas.

Passo 1

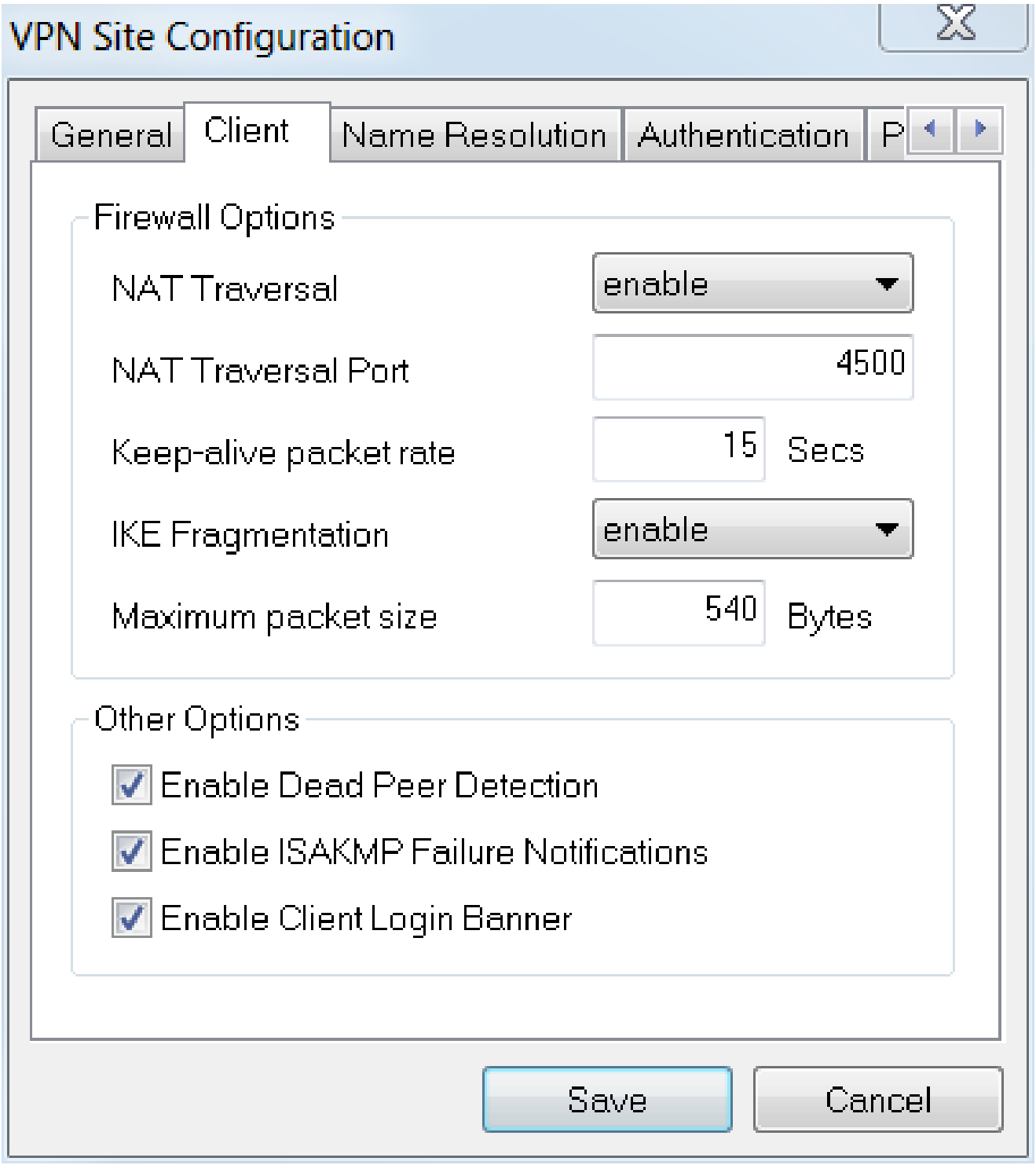
Abra o Shrew Soft VPN Access Manager e clique em Add para adicionar um perfil. Na janela VPN Site Configuration exibida, configure a guia General:

- Nome de host ou endereço IP: use o endereço IP da WAN (ou o nome de host do RV345P)
- Configuração automática: selecione ike config pull
- Modo de adaptador: selecione Usar um adaptador virtual e o endereço atribuído



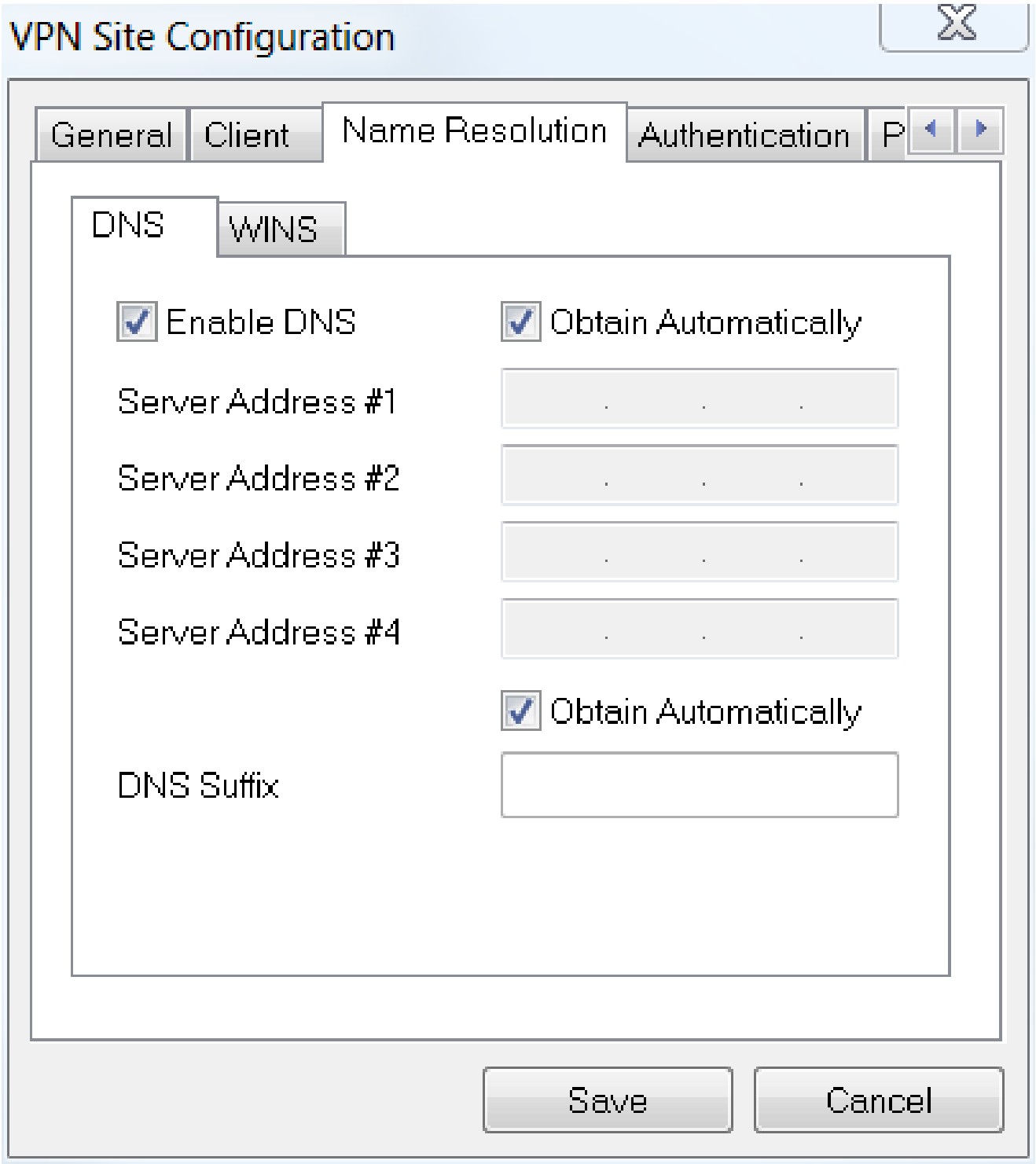
Passo 2

Configure a guia Client. Neste exemplo, mantivemos as configurações padrão.



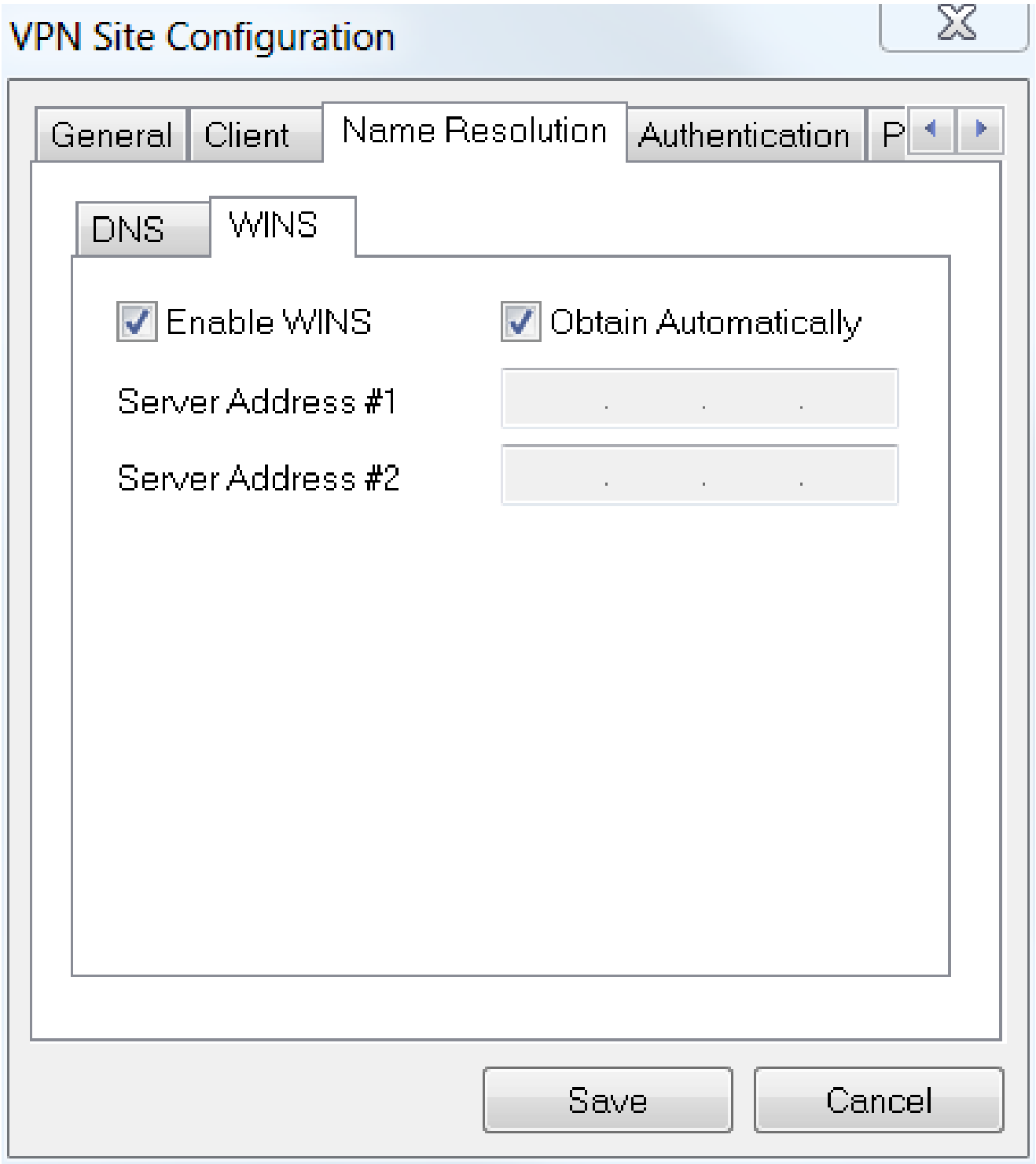
Etapa 3

Em Name Resolution > DNS, marque a caixa Enable DNS e deixe marcadas as caixas Obtain Automatically.



Passo 4

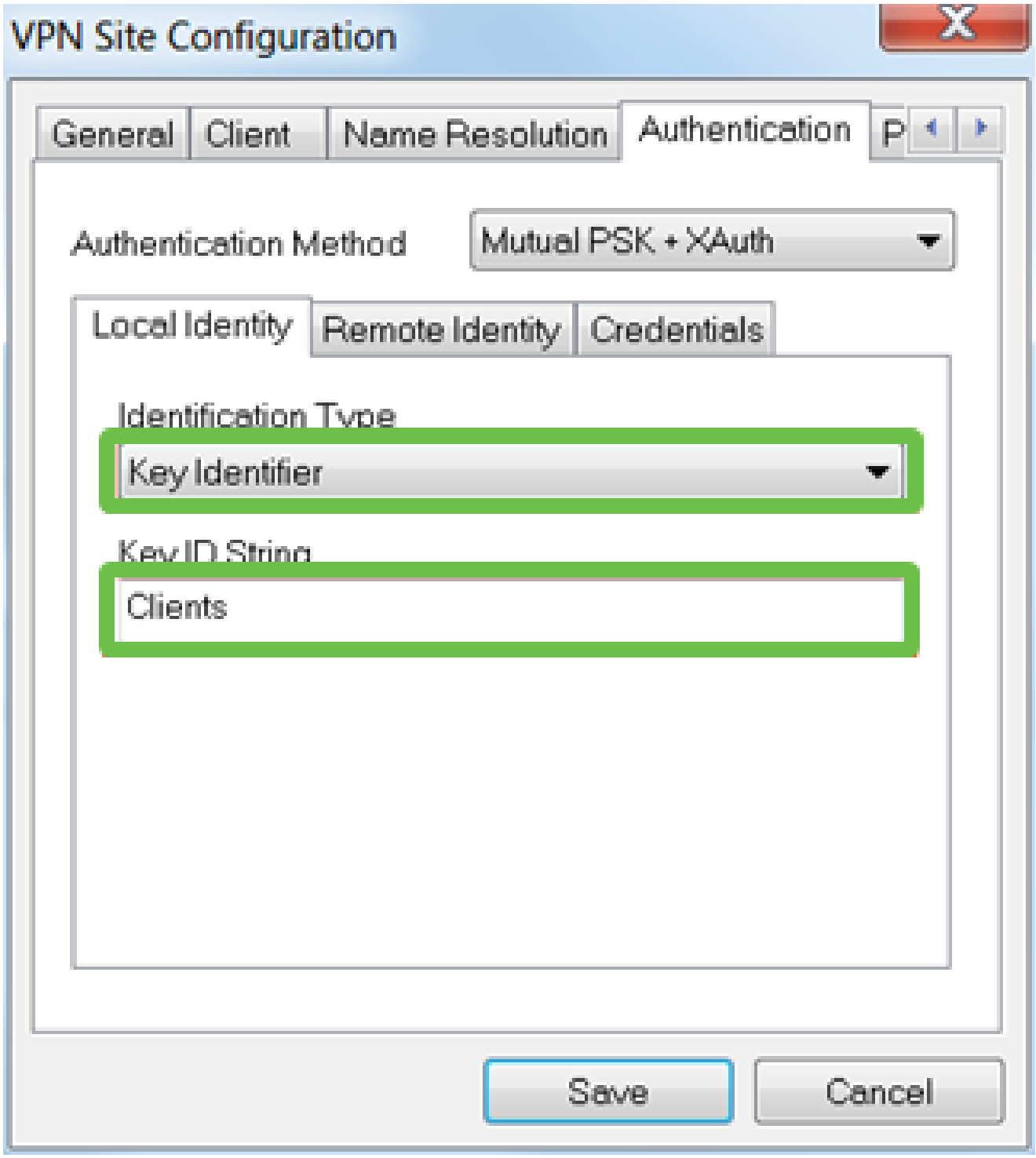
Na guia Resolução de nomes > WINS, marque a caixa Ativar WINS e deixe a caixa Obter automaticamente marcada.



Etapa 5

Clique em Authentication > Local Identity.

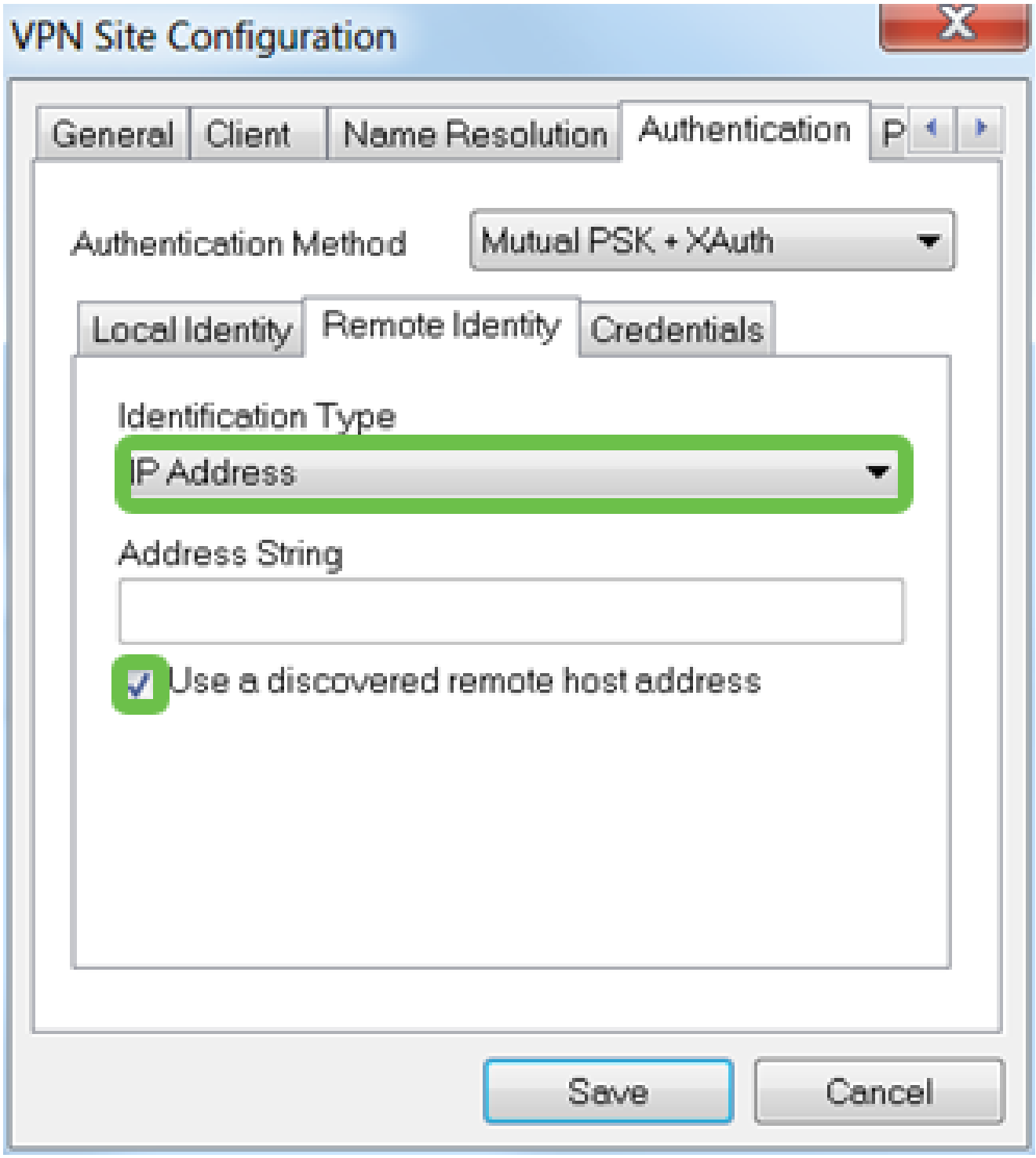
- Tipo de Identificação: Selecionar Identificador de Chave
- String de ID da chave: digite o nome do grupo que foi configurado no RV345P



Etapa 6

Em Authentication > Remote Identity. Neste exemplo, mantivemos as configurações padrão.

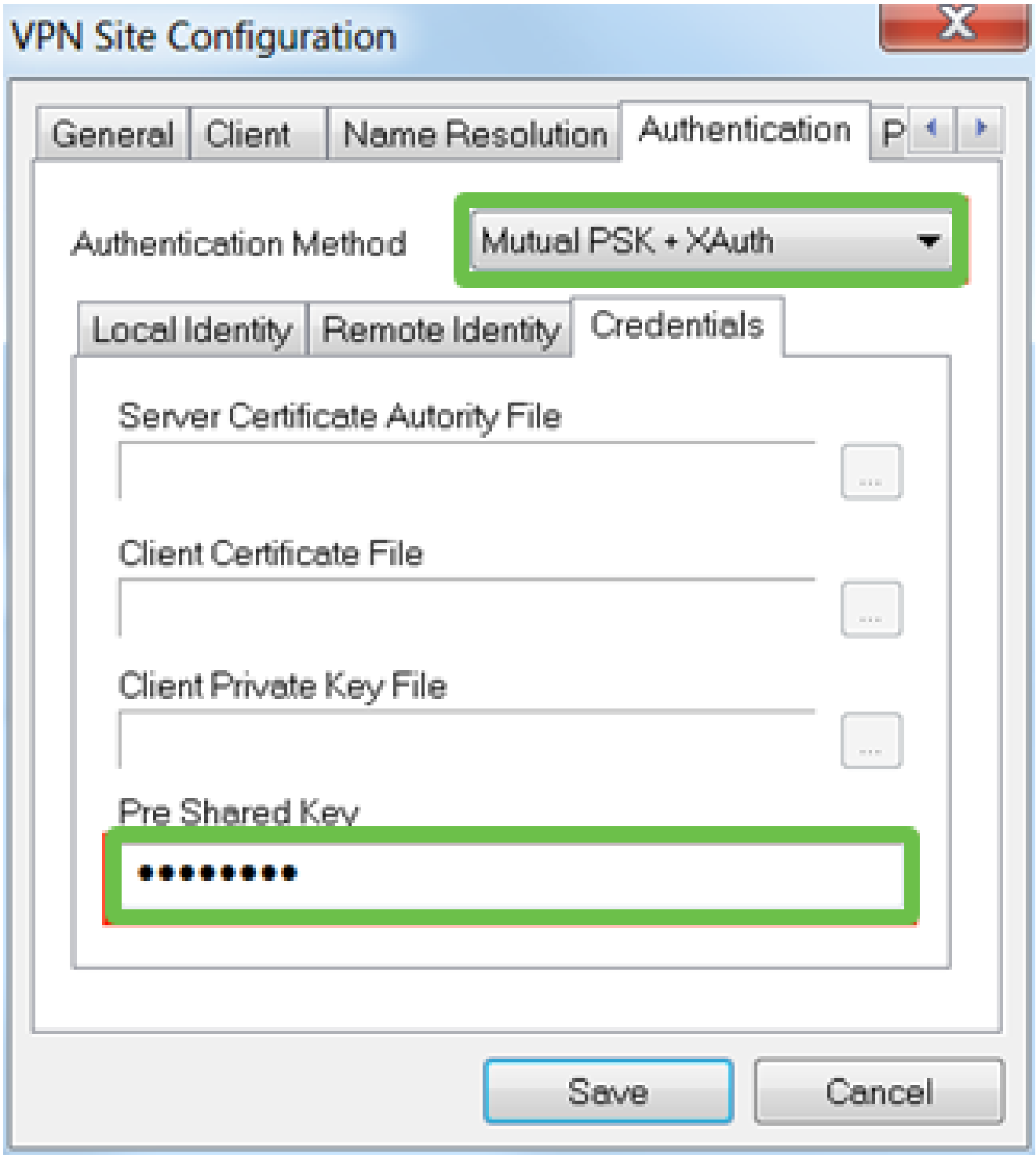
- Tipo de identificação: endereço IP
- Cadeia de caracteres de endereço: <blank>
- Usar uma caixa de endereço de host remoto descoberto: Marcada



Etapa 7

Em Authentication > Credentials, configure o seguinte:

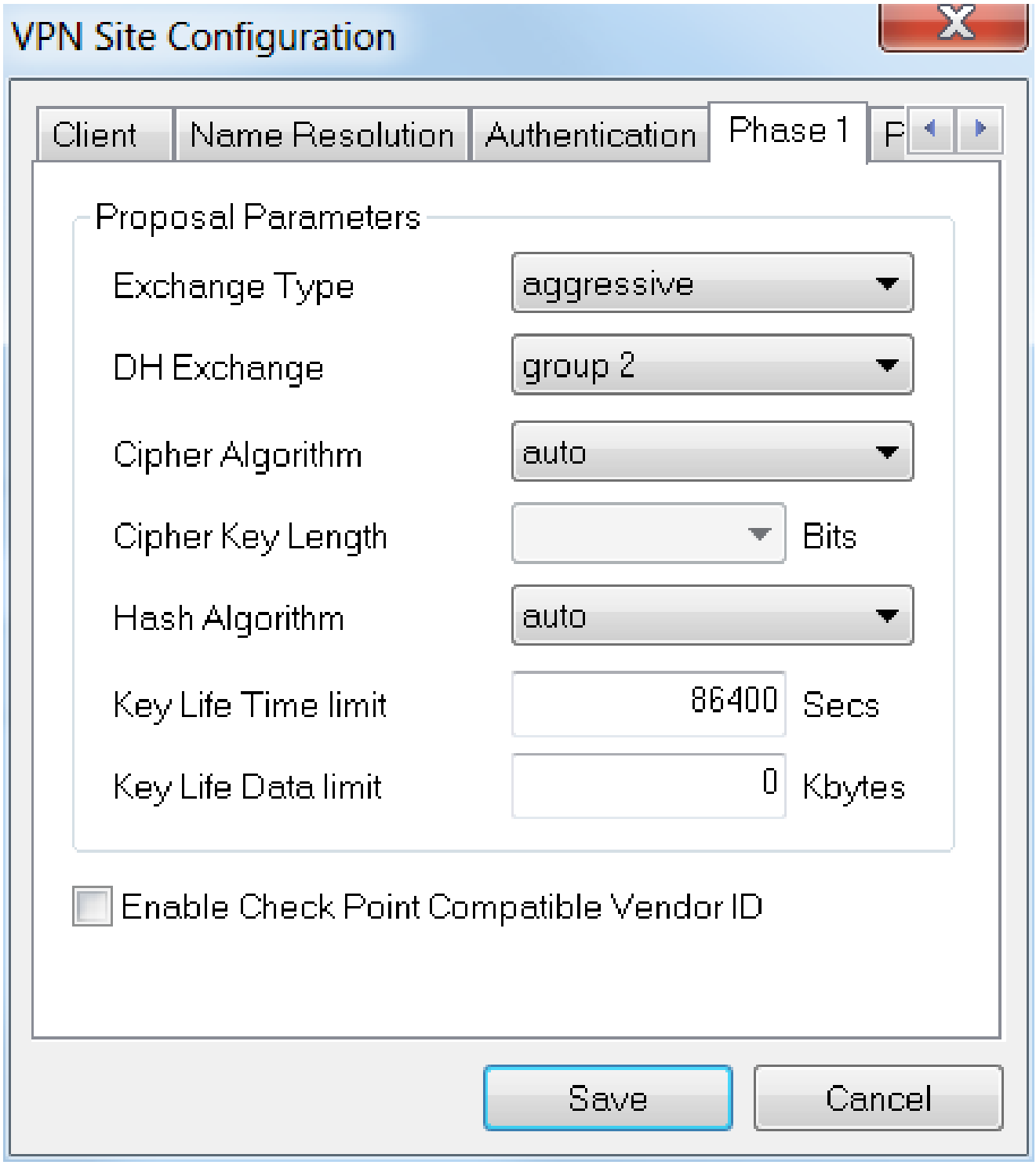
- Método de autenticação: selecionar PSK mútua + XAuth
- Chave pré-compartilhada: insira a chave pré-compartilhada configurada no perfil do cliente RV345P



Passo 8

Para a guia Fase 1. Neste exemplo, as configurações padrão foram mantidas:

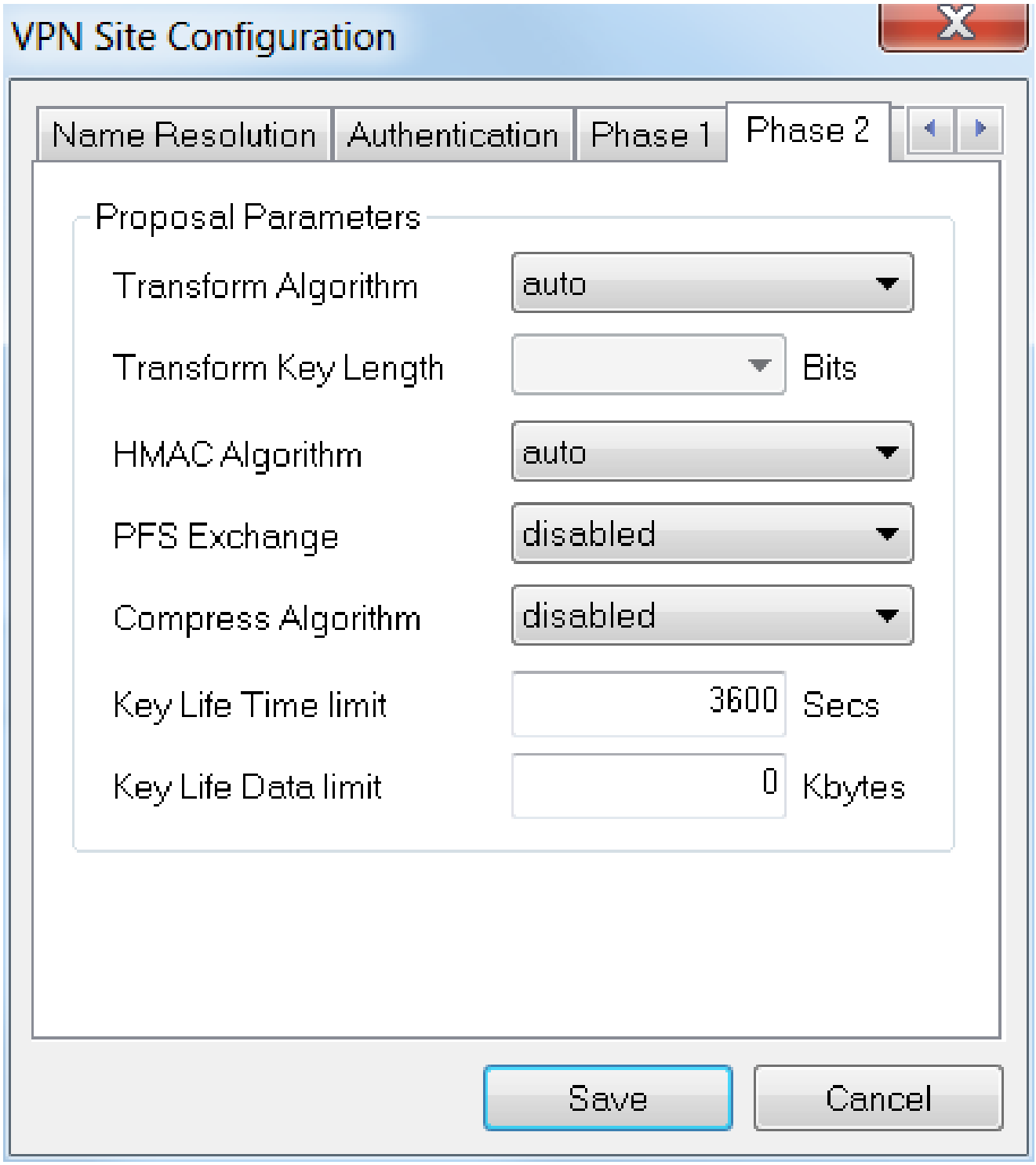
- Tipo de Intercâmbio: Agressivo
- DH Exchange: grupo 2
- Algoritmo de codificação: Automático
- Algoritmo de hash: Automático



Passo 9

Neste exemplo, os padrões para a guia Fase 2 foram mantidos iguais.

- Transformar algoritmo: automático
- Algoritmo HMAC: Automático
- Troca de PFS: Desabilitada
- Algoritmo de compactação: Desabilitado

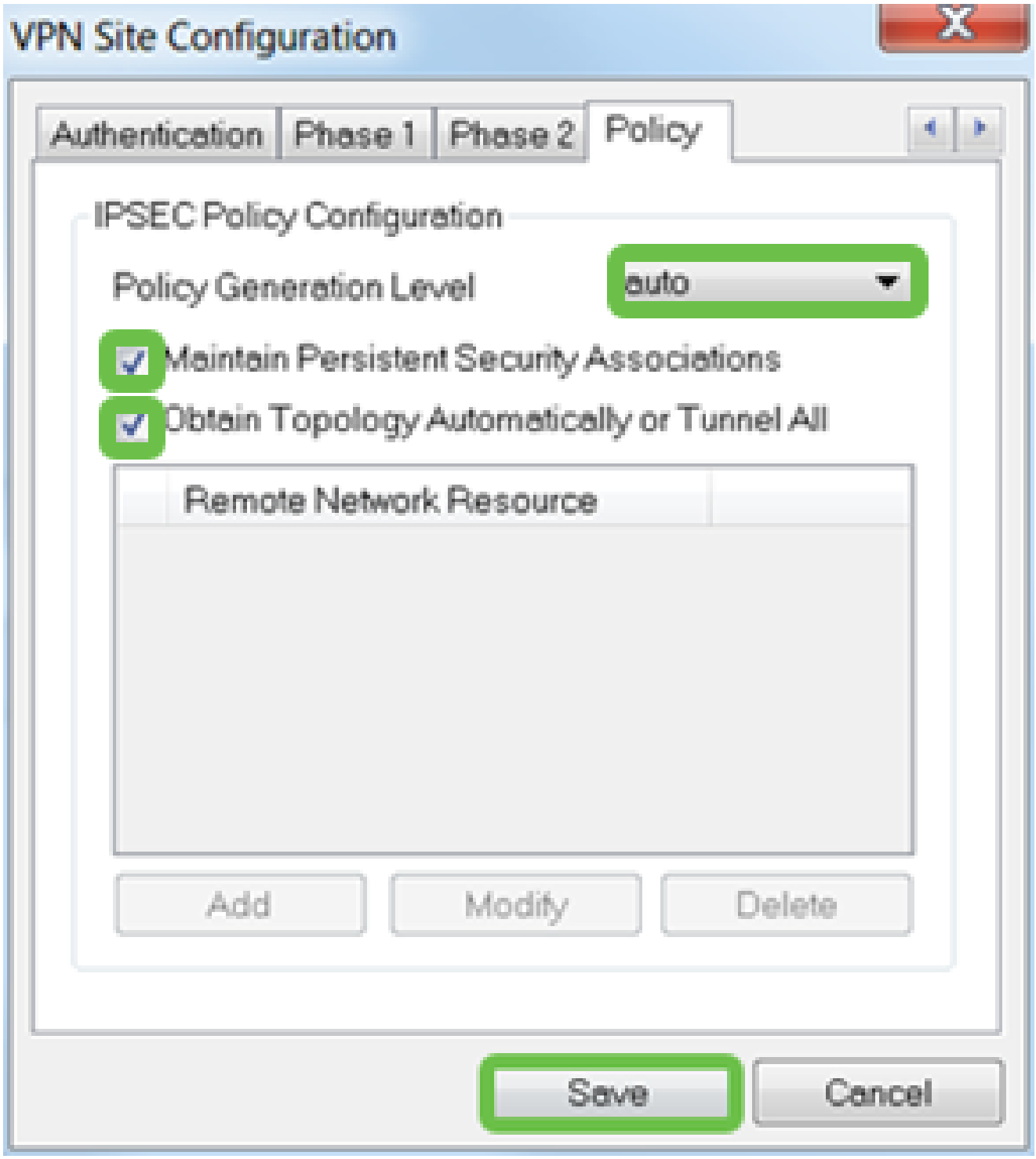


Passo 10

Para o exemplo da guia Política, usamos as seguintes configurações:

- Nível de geração de política: Automático
- Manter Associações De Segurança Persistentes: Marcada
- Obter a topologia automaticamente ou criar um túnel para todos: Verificado

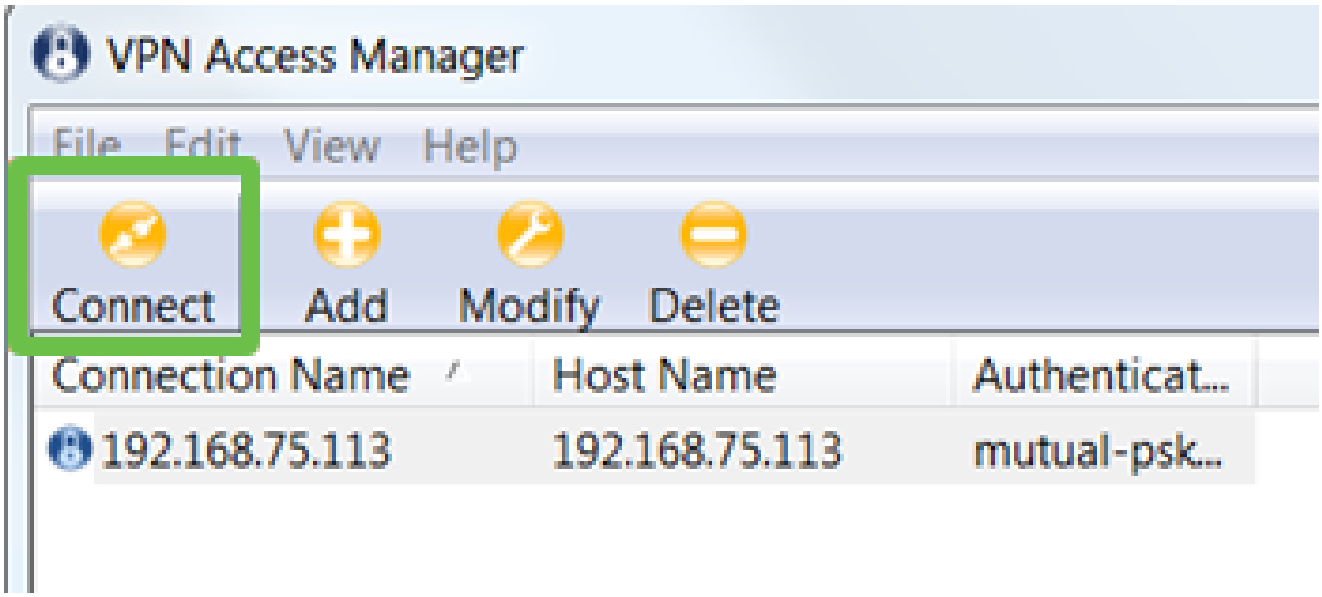
Como configuramos o Split-Tunneling no RV345P, não precisamos configurá-lo aqui.



Ao concluir, clique em Save (Salvar).

Passo 11

Agora você está pronto para testar a conexão. No VPN Access Manager, realce o perfil de conexão e clique no botão Connect.

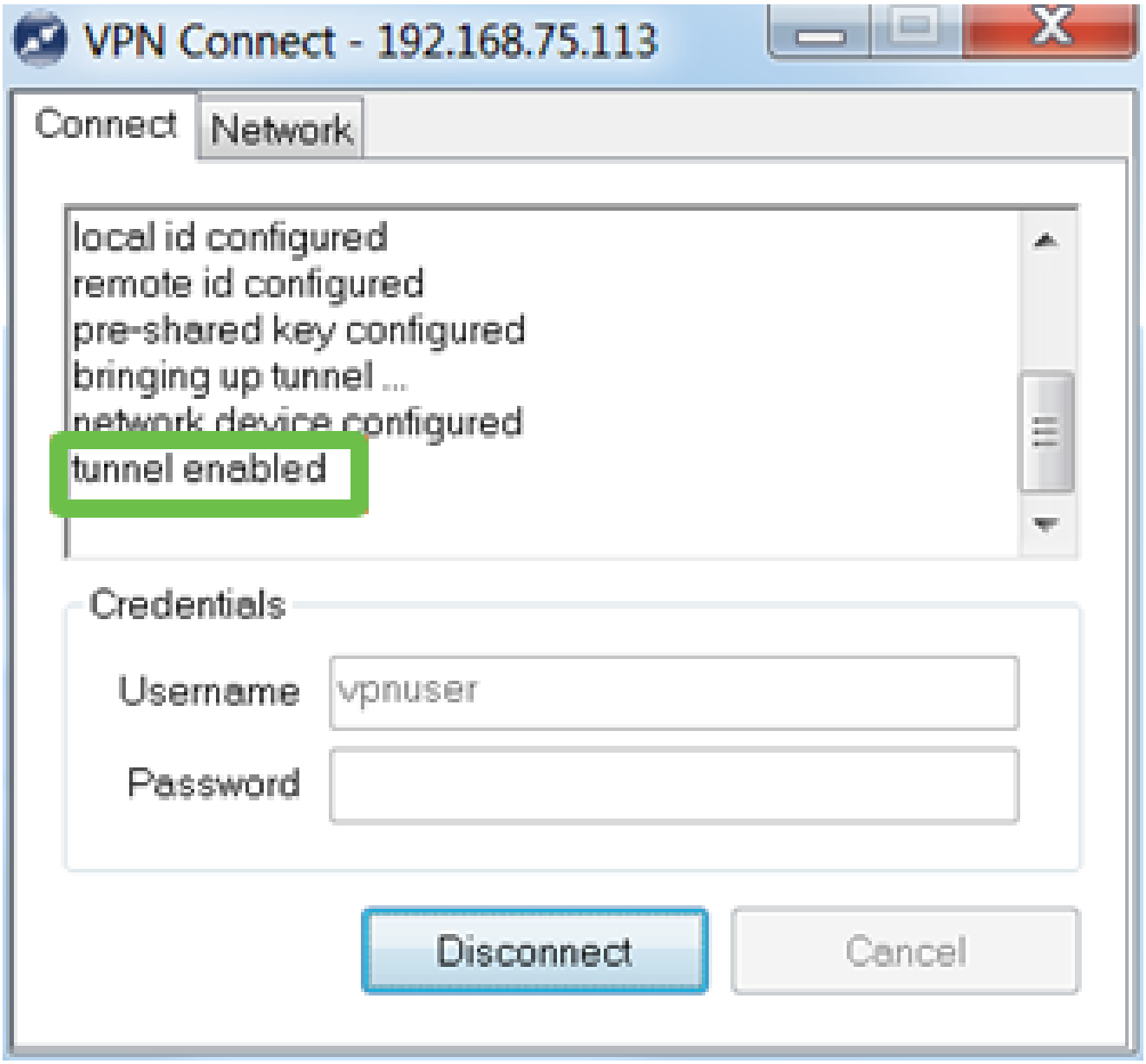


Etapa 12

Na janela VPN Connect que aparece, digite o Username e Password usando as credenciais da User Account que você criou no RV345P (etapas 13 e 14). Ao terminar, clique em Connect.

Passo 13

Verifique se o túnel está conectado. Você deve ver tunnel enabled.



A Shrew Soft foi usada como exemplo nesta configuração. Como a Shrew Soft não é um produto da Cisco, entre em contato com terceiros se precisar de assistência técnica.

Outras opções de VPN

Há outras opções para usar uma VPN. Clique nos seguintes links para obter mais informações:

- Use o cliente VPN GreenBow para se conectar com o roteador série RV34x
- Configurar um cliente VPN para trabalhadores à distância no roteador série RV34x
- Configurar um servidor PPTP (Point-to-Point Tunneling Protocol) no roteador série Rv34x
- Configurar um Perfil de Segurança de Protocolo Internet (IPsec) em um Roteador da Série RV34x
- Definir as configurações L2TP WAN no roteador RV34x
- Configuração da VPN Site a Site no RV34x

Configurações suplementares no roteador RV345P

Configurar VLANs (Opcional)

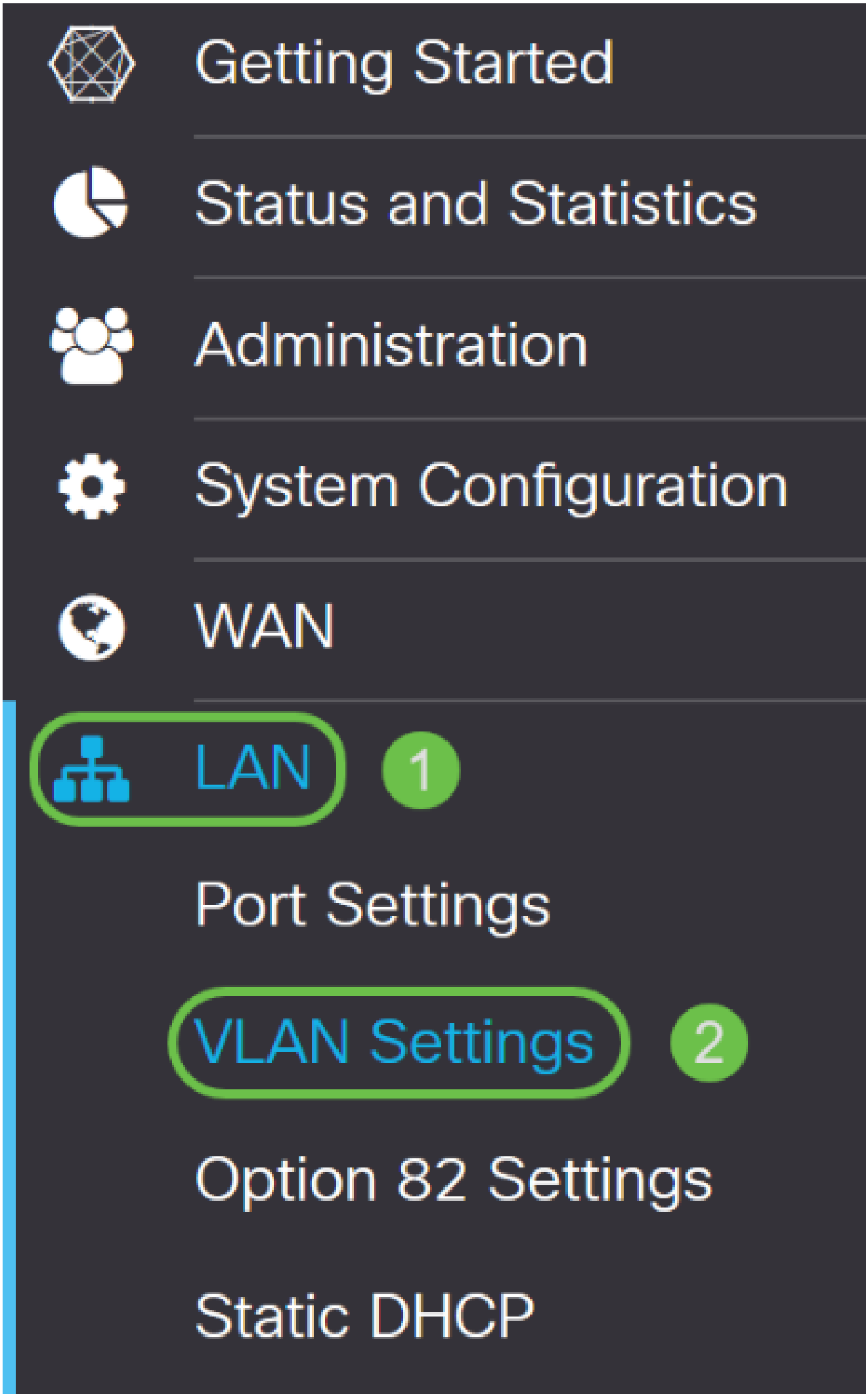
Uma rede local virtual (VLAN) permite segmentar logicamente uma rede de área local (LAN) em diferentes domínios de transmissão. Nos cenários em que dados confidenciais podem ser transmitidos em uma rede, as VLANs podem ser criadas para aumentar a segurança, designando uma transmissão para uma VLAN específica. 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, seja manual ou dinamicamente. As portas devem sempre pertencer a uma ou mais VLANs.

Consulte Práticas Recomendadas de VLAN e Dicas de Segurança para obter orientações adicionais.

Se não quiser criar VLANs, vá para a próxima seção.

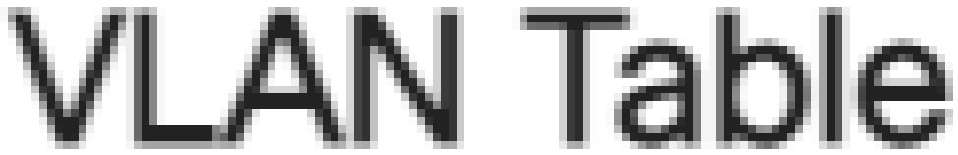
Passo 1

Navegue até LAN > VLAN Settings.


Getting Started
Status and Statistics
Administration
System Configuration
WAN
LAN
1
Port Settings
VLAN Settings
2
Option 82 Settings
Static DHCP

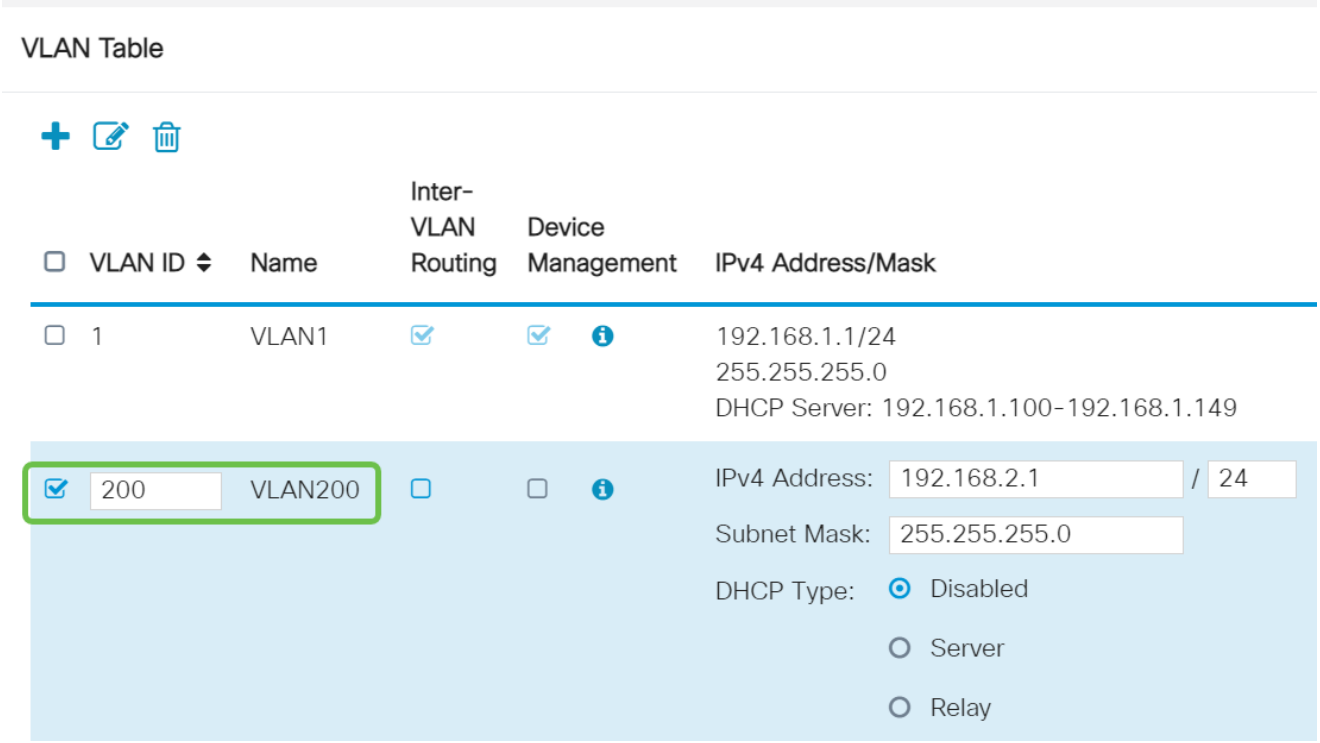
Passo 2

Clique no ícone add para criar uma nova VLAN.



Etapa 3

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



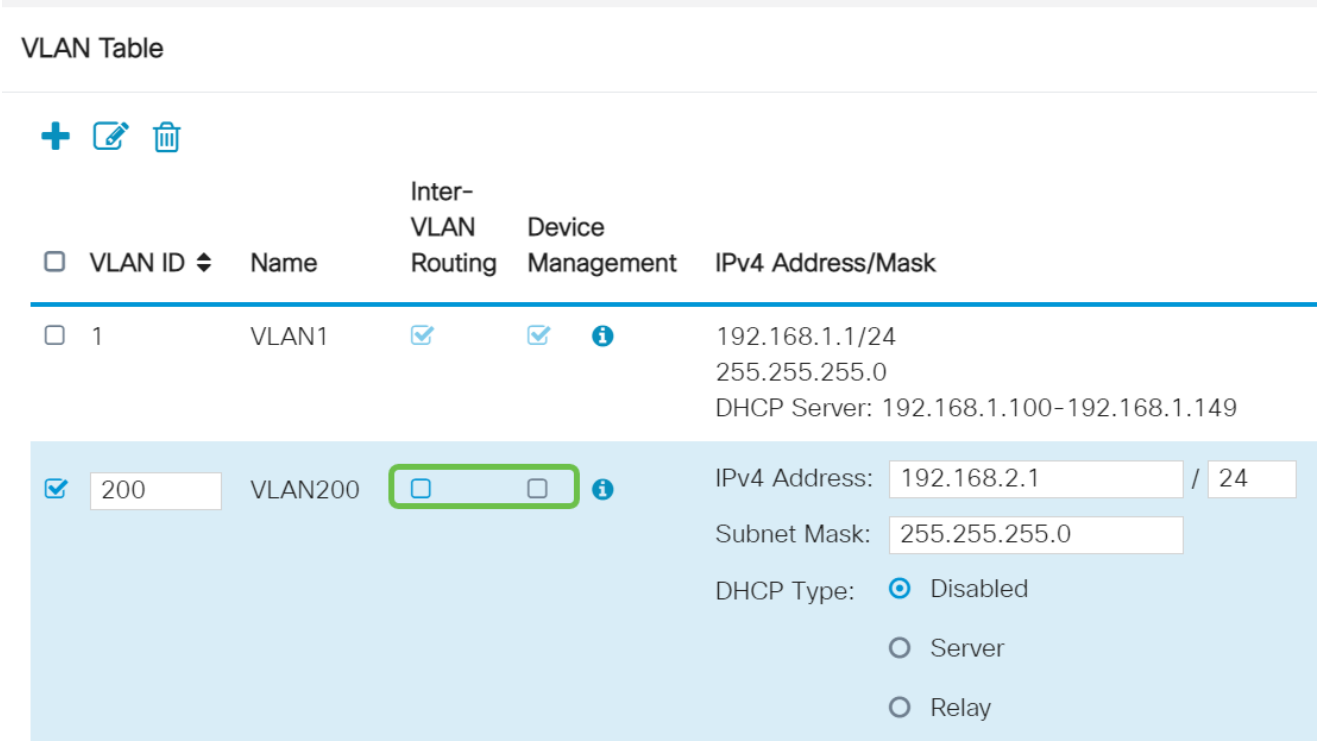
Passo 4

Desmarque a caixa Enabled para Inter-VLAN Routing e Device Management se desejar. 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 desejará isolar os usuários convidados, pois isso deixa as VLANs menos seguras. Há momentos em que pode ser necessário que as VLANs façam o roteamento entre si. Se esse for o caso, verifique Inter-VLAN Routing em um roteador RV34x com restrições de ACL direcionada para configurar o tráfego específico permitido entre VLANs.

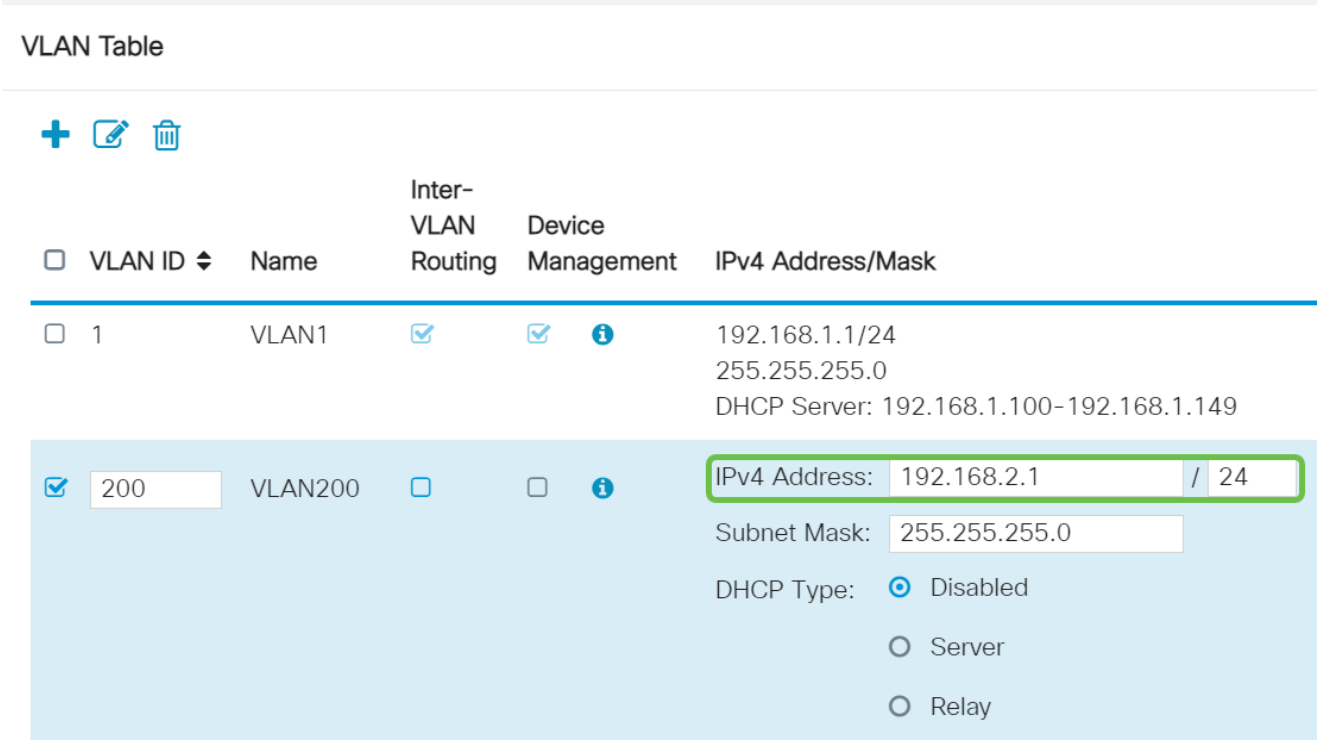
O Gerenciamento de dispositivos é o software que permite usar seu navegador para fazer login na interface de usuário da Web do RV345P, a partir da VLAN, e gerenciar o RV345P. Isso também deve ser desativado em redes de convidado.

Neste exemplo, não habilitamos o Roteamento entre VLANs ou o Gerenciamento de dispositivos para manter a VLAN mais segura.



Etapa 5

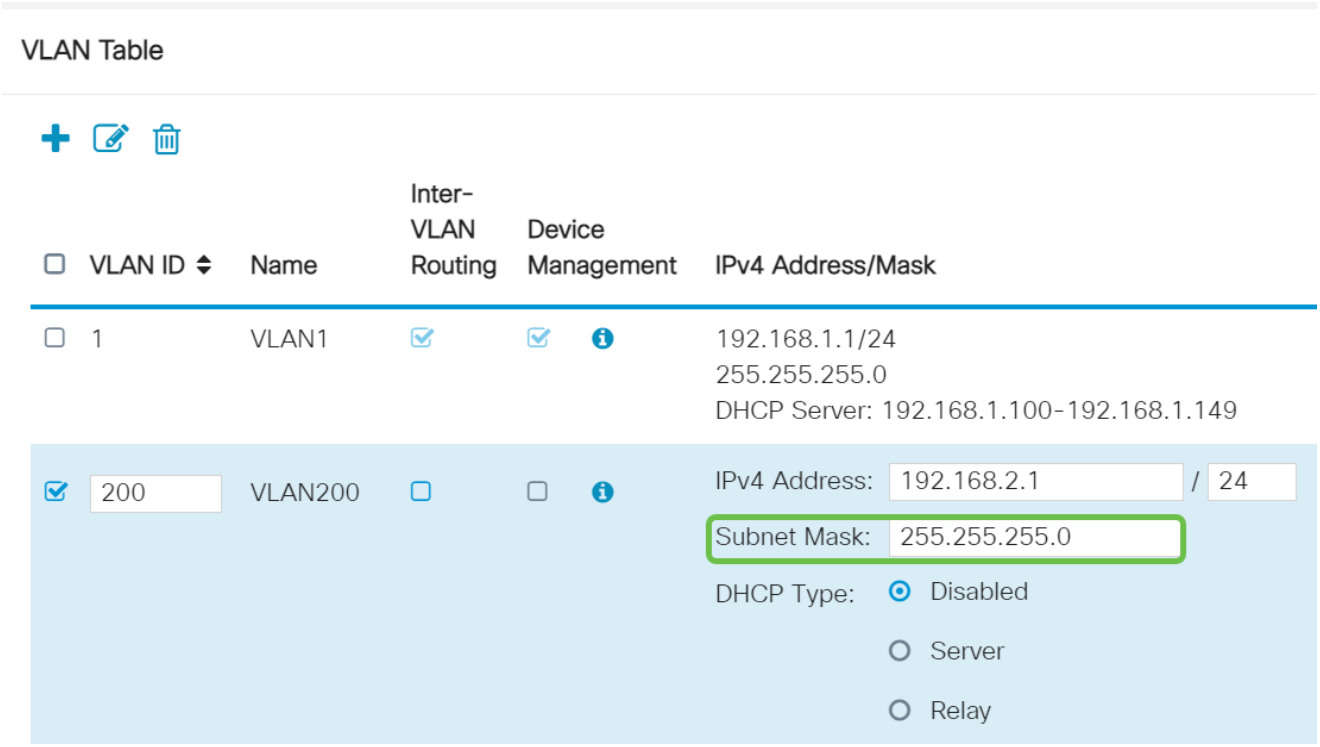
O endereço IPv4 privado será preenchido automaticamente no campo Endereço IP. Você pode ajustar isso se quiser. Neste exemplo, a sub-rede tem endereços IP 192.168.2.100-192.168.2.149 disponíveis para DHCP. 192.168.2.1-192.168.2.99 e 192.168.2.150-192.168.2.254 estão disponíveis para endereços IP estáticos.



Etapa 6

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

Para esta demonstração, deixaremos a máscara de sub-rede como 255.255.255.0 ou /24.



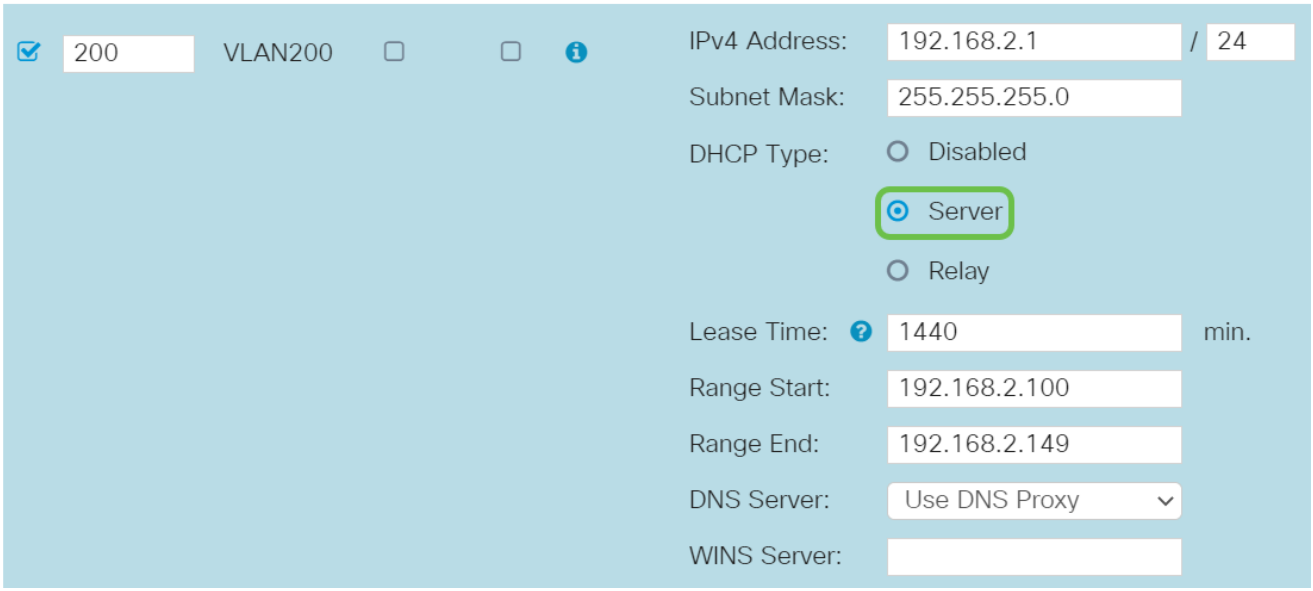
Etapa 7

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

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.

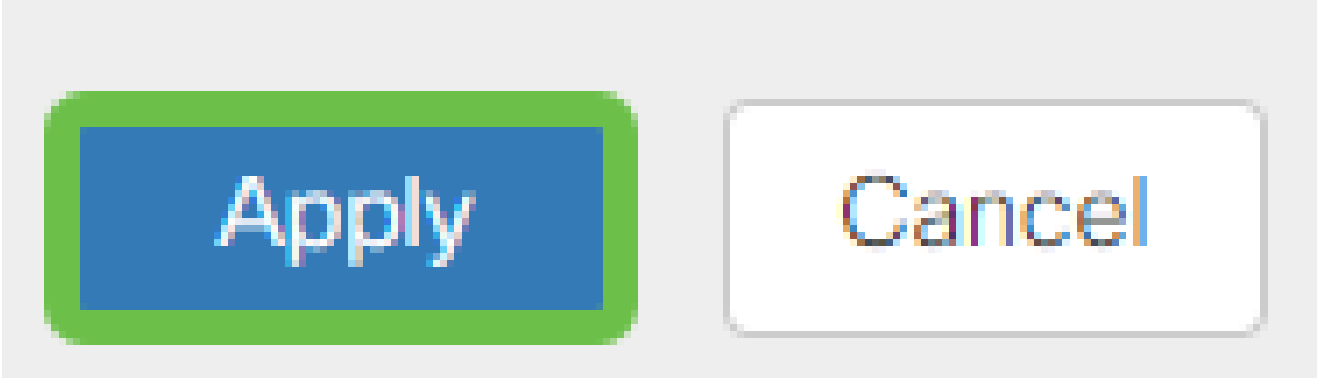
Servidor - Esta é a opção mais usada.

- Lease Time - (Tempo de concessão) Insira um valor de tempo de 5 a 43.200 minutos. O padrão é 1440 minutos (igual a 24 horas).
- Range Start and Range End - (Início do intervalo e fim do intervalo) Insira o início e o fim do intervalo dos endereços IP que podem ser atribuídos dinamicamente.
- Servidor DNS - Selecione para usar o servidor DNS como proxy ou ISP na lista suspensa.
- Servidor WINS - Insira o nome do servidor WINS.
- Opções DHCP:
  - Opção 6 - Digite o endereço IP do servidor TFTP.
  - Opção 150 - Digite o endereço IP de uma lista de servidores TFTP.
  - Opção 67 - Inserir o nome do arquivo de configuração.
- Relay - insira o endereço IPv4 do servidor DHCP remoto para configurar o agente de retransmissão DHCP. Esta é uma configuração mais avançada.



Passo 8

Clique em Apply para criar a nova VLAN.



Atribuir VLANs às portas (opcional)

16 VLANs podem ser configuradas no RV345P, 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 VLANs/VLANs que o usuário especificamente atribuiu. É considerada uma melhor prática.

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

- Porta de acesso - atribuída uma VLAN. Quadros não marcados são passados.
- Porta de tronco - Pode transportar mais de uma VLAN. O entroncamento 802.1q 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 essa porta deve ser rotulada como Não rotulada.

- Todas as outras VLANs devem ser rotuladas como Excluded (Excluído) dessa porta.

Duas ou mais VLANs que compartilham uma porta:

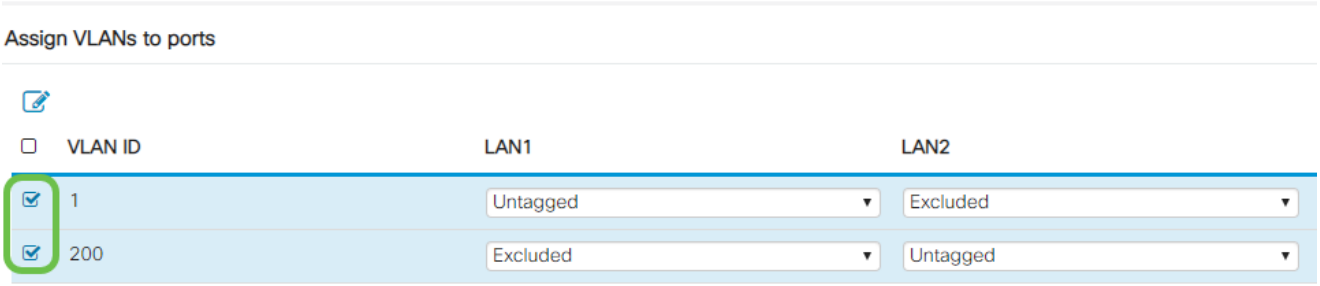
- Considerada uma porta de tronco.
- Uma das VLANs pode ser rotulada como Untagged.
- O restante das VLANs que fazem parte da porta do tronco deve ser rotulado como Tagged.
- As VLANs que não fazem parte da porta do tronco devem ser rotuladas como Excluded para essa porta.

Neste exemplo, não há troncos.

Passo 1

Selecione as IDs de VLAN a serem editadas.

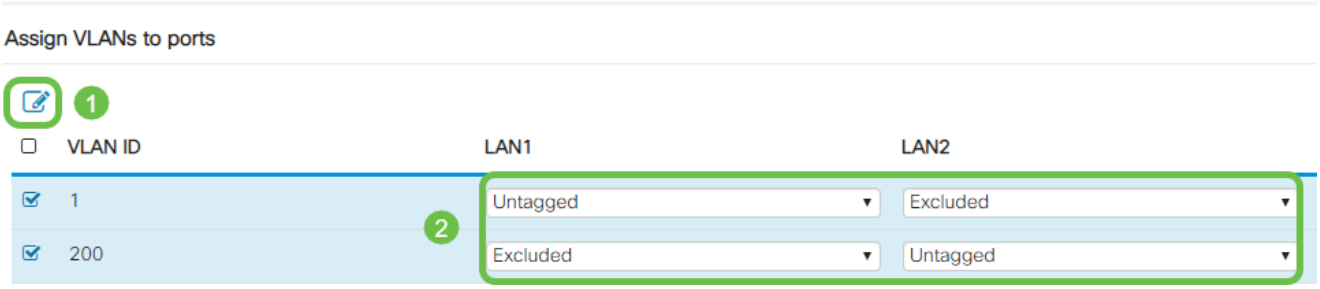
Neste exemplo, selecionamos VLAN 1 e VLAN 200.



Passo 2

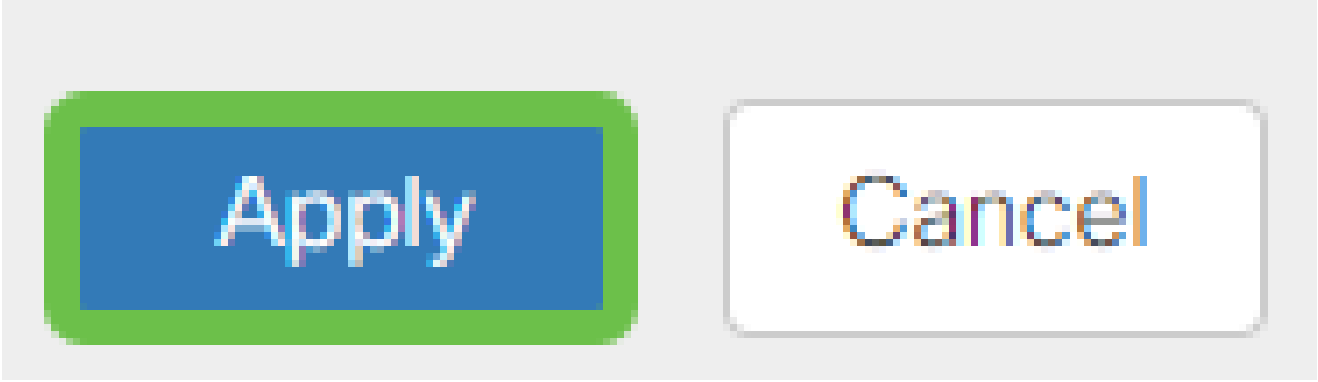
Clique em Edit para atribuir uma VLAN a uma porta LAN e especifique cada configuração como Tagged, Untagged ou Excluded.

Neste exemplo, em LAN1, atribuímos VLAN 1 como Não Marcado e VLAN 200 como Excluído. Para LAN2, atribuímos VLAN 1 como Excluded e VLAN 200 como Untagged.



Etapa 3

Clique em Apply para salvar a configuração.



Agora você deve ter criado com êxito uma nova VLAN e configurado VLANs para portas no RV345P. Repita o processo para criar as outras VLANs. Por exemplo, VLAN300 seria criada para Marketing com uma sub-rede de 192.168.3.x e VLAN400 seria criada para Contabilidade com uma sub-rede de 192.168.4.x.

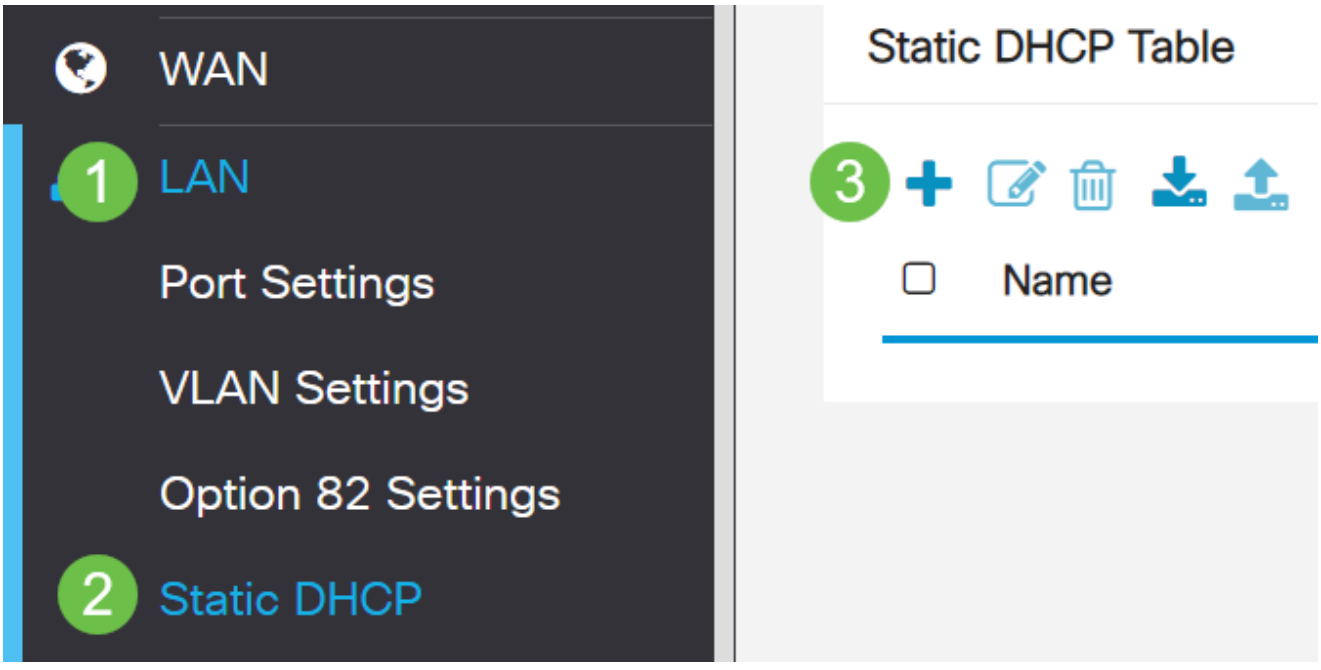
Adicionar um IP estático (opcional)

Se 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 a definição de endereços IP estáticos, consulte Melhores práticas para a definição de 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.

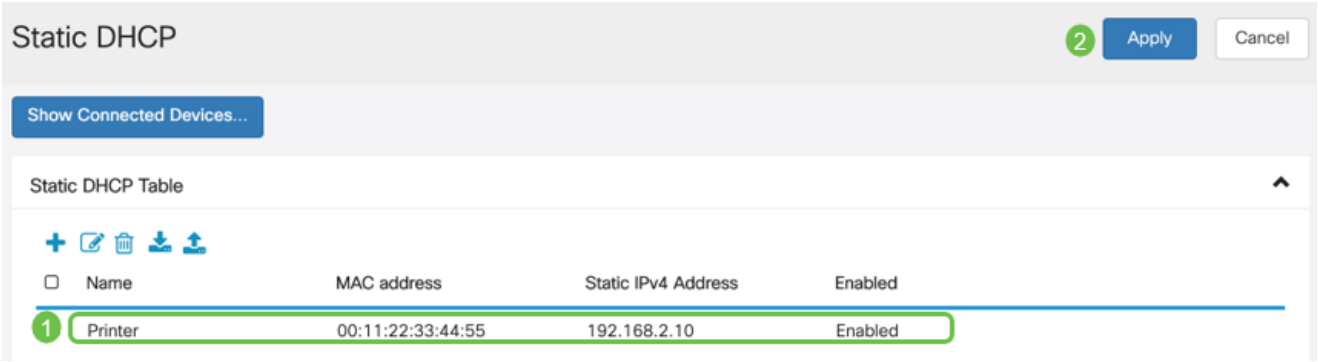
Passo 1

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



Passo 2

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



Gerenciamento de certificados (opcional)

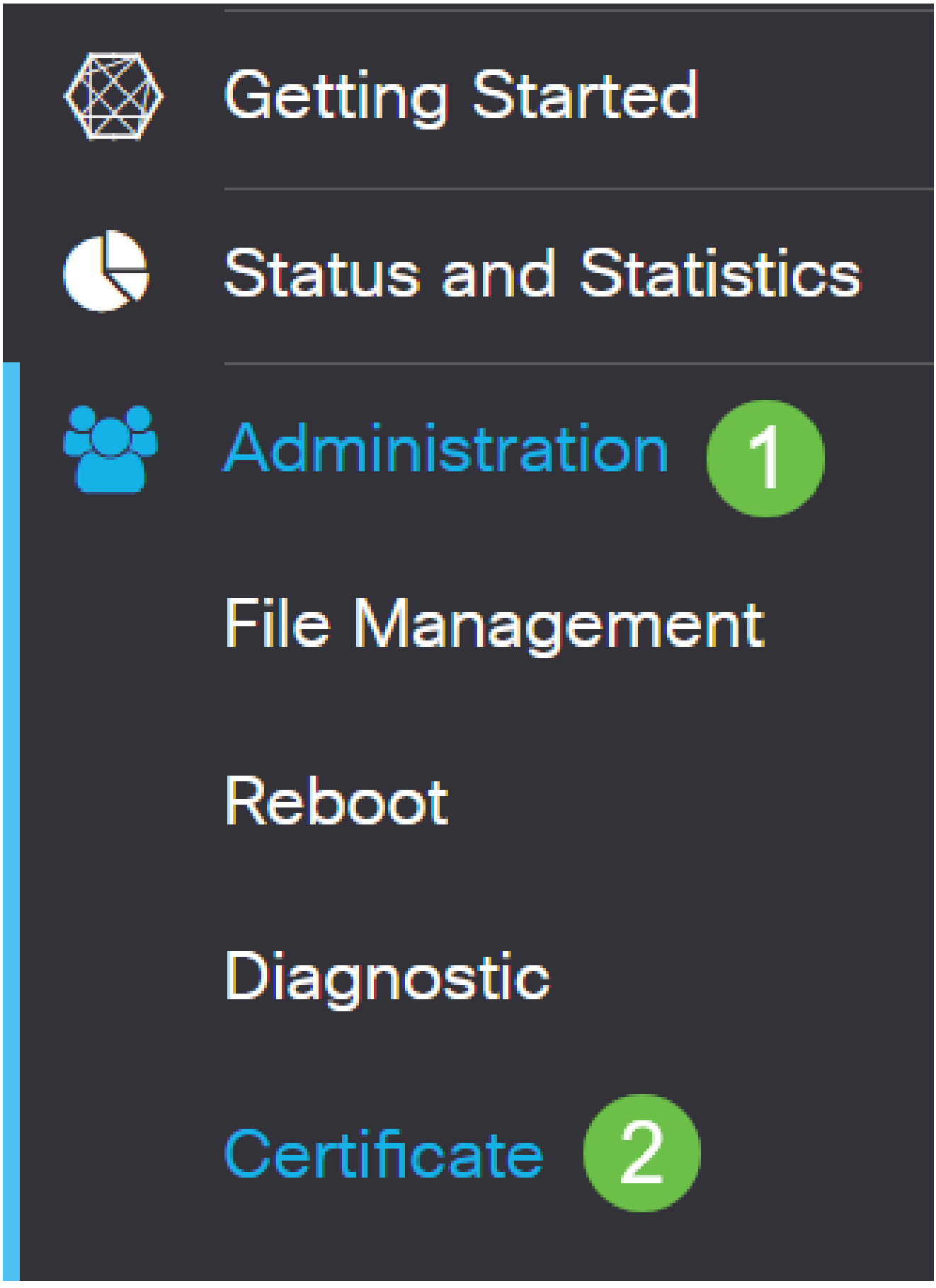
Um certificado digital certifica a propriedade de uma chave pública pela entidade nomeada do certificado. Isso permite que as partes confiáveis dependam de assinaturas ou afirmações feitas pela chave privada que corresponde à chave pública certificada. Um roteador pode gerar um certificado autoassinado, um certificado criado por um administrador de rede. Ele também pode enviar solicitações às Autoridades de Certificação (CA) para solicitar um certificado de identidade digital. É importante ter certificados legítimos de aplicativos de terceiros.

Uma Autoridade de Certificação (CA) é usada para autenticação. Os certificados podem ser adquiridos em qualquer número de sites de terceiros. É uma maneira oficial de provar que seu site é seguro. Essencialmente, a CA é uma fonte confiável que verifica se você é uma empresa legítima e se é confiável. Dependendo das suas necessidades, um certificado com um custo mínimo. Você é submetido a check-out pela CA e, depois que a CA verificar suas informações, ela emitirá o certificado para você. Este certificado pode ser baixado como um arquivo no seu computador. Em seguida, você pode ir para o roteador (ou servidor VPN) e carregá-lo lá.

Gerar CSR/certificado

Passo 1

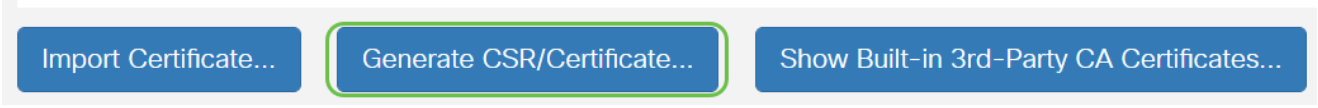
Efetue login no utilitário baseado na Web do roteador e escolha Administration > Certificate.



Passo 2

Clique em Gerar CSR/Certificado. Você será direcionado para a página Gerar

CSR/Certificado.



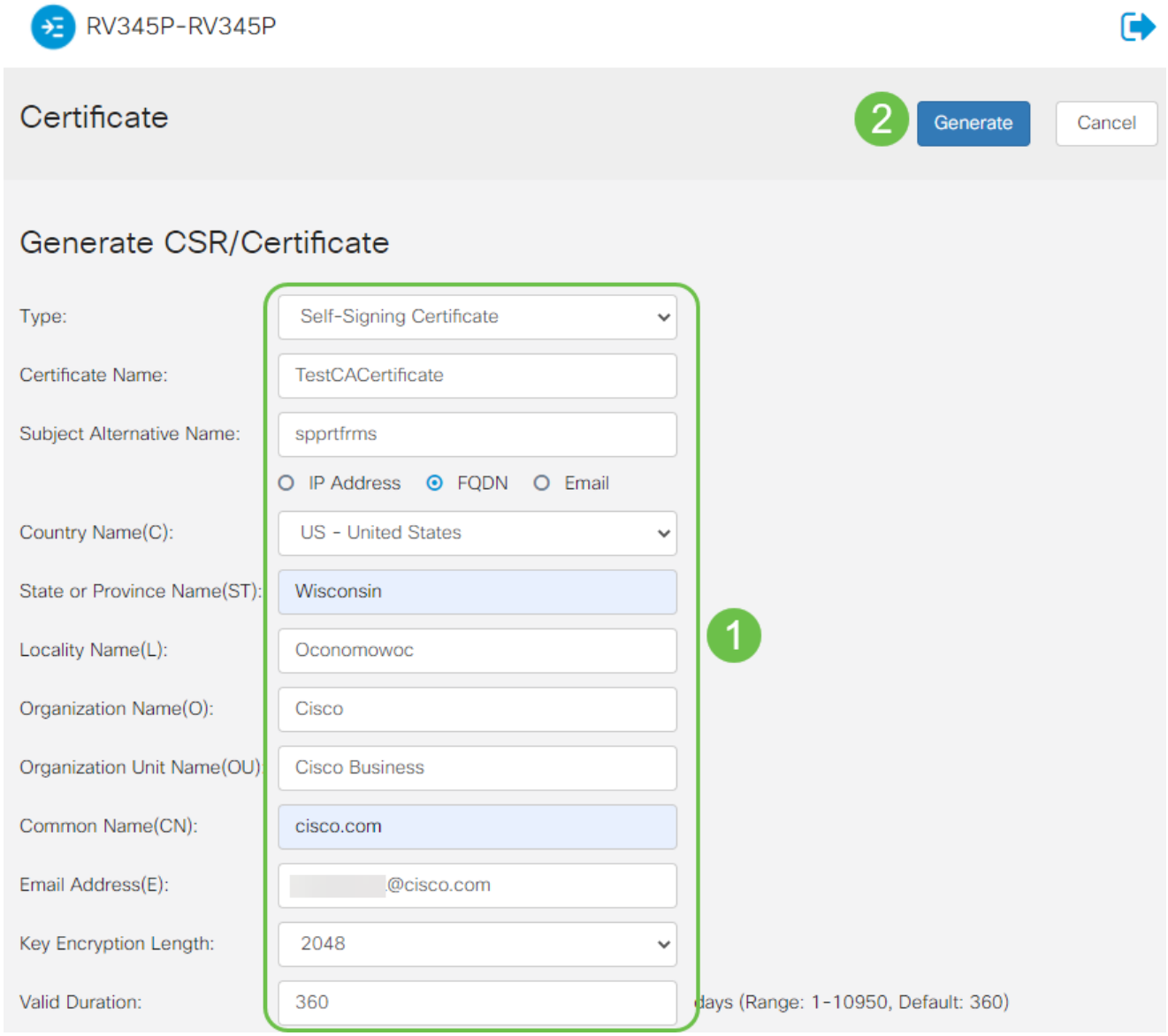
Etapa 3

Preencha as caixas com o seguinte:

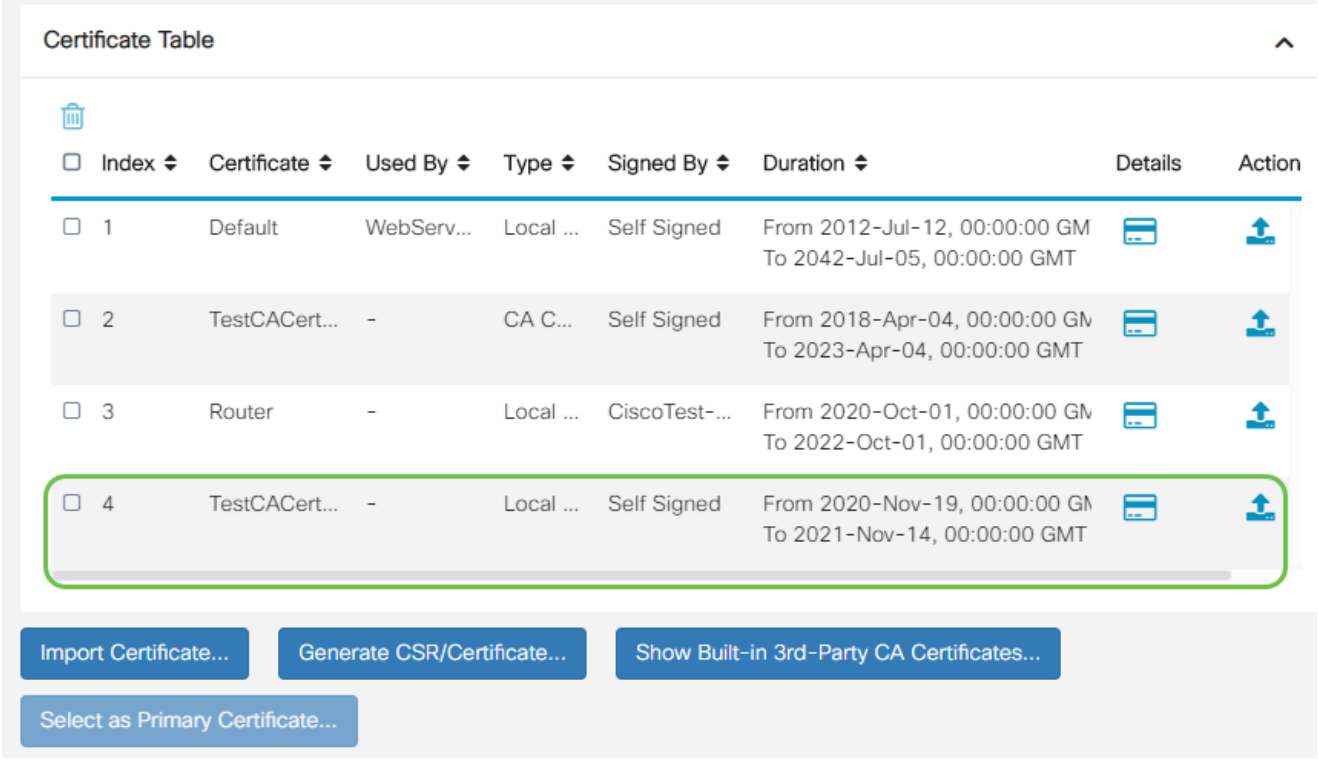
- Escolha o tipo de certificado apropriado
  - Certificado de Autosassinatura — Este é um certificado SSL (Secure Socket Layer) assinado por seu próprio criador. Este certificado é menos confiável, pois não pode ser cancelado se a chave privada for comprometida de alguma forma por um invasor.
  - Solicitação de assinatura certificada — Esta é uma infraestrutura de chave pública (PKI) que é enviada à autoridade de certificação para solicitar um certificado de identidade digital. É mais seguro do que autoassinado, pois a chave privada é mantida em segredo.
- Insira um nome para o certificado no campo Nome do certificado para identificar a solicitação. Este campo não pode estar em branco nem conter espaços e caracteres especiais.
- (Opcional) Na área Nome alternativo do assunto, clique em um botão de opção. As opções são:
  - Endereço IP — Insira um endereço IP (Internet Protocol)
  - FQDN — Inserir um Nome de Domínio Totalmente Qualificado (FQDN)
  - E-mail — Insira um endereço de e-mail
- No campo Nome Alternativo do Assunto, insira o FQDN.
- Na lista suspensa Nome do país, escolha o nome do país no qual sua empresa está legalmente registrada.
- Insira um nome ou abreviação do estado, província, região ou território onde sua organização está localizada no campo Nome do estado ou província (ST).
- Informe um nome da localidade ou cidade em que sua organização está registrada ou localizada no campo Nome da Localidade.
- Insira um nome sob o qual sua empresa está legalmente registrada. Se você estiver se inscrevendo como uma pequena empresa ou proprietário único, insira o nome do solicitante do certificado no campo Nome da organização. Caracteres especiais não podem ser usados.
- Informe um nome no campo Nome da Unidade da Organização para diferenciar as divisões dentro de uma organização.
- Insira um nome no campo Nome comum. Esse nome deve ser o nome de domínio totalmente qualificado do site para o qual você usa o certificado.
- Insira o endereço de email da pessoa que deseja gerar o certificado.
- Na lista suspensa Key Encryption Length, escolha um comprimento de chave. As opções são 512, 1024 e 2048. Quanto maior o comprimento da chave, mais seguro o certificado.
- No campo Valid Duration (Duração válida), insira o número de dias em que o

certificado será válido. O padrão é 360.

- Clique em Gerar.



O certificado gerado deve aparecer agora na Tabela de Certificados.

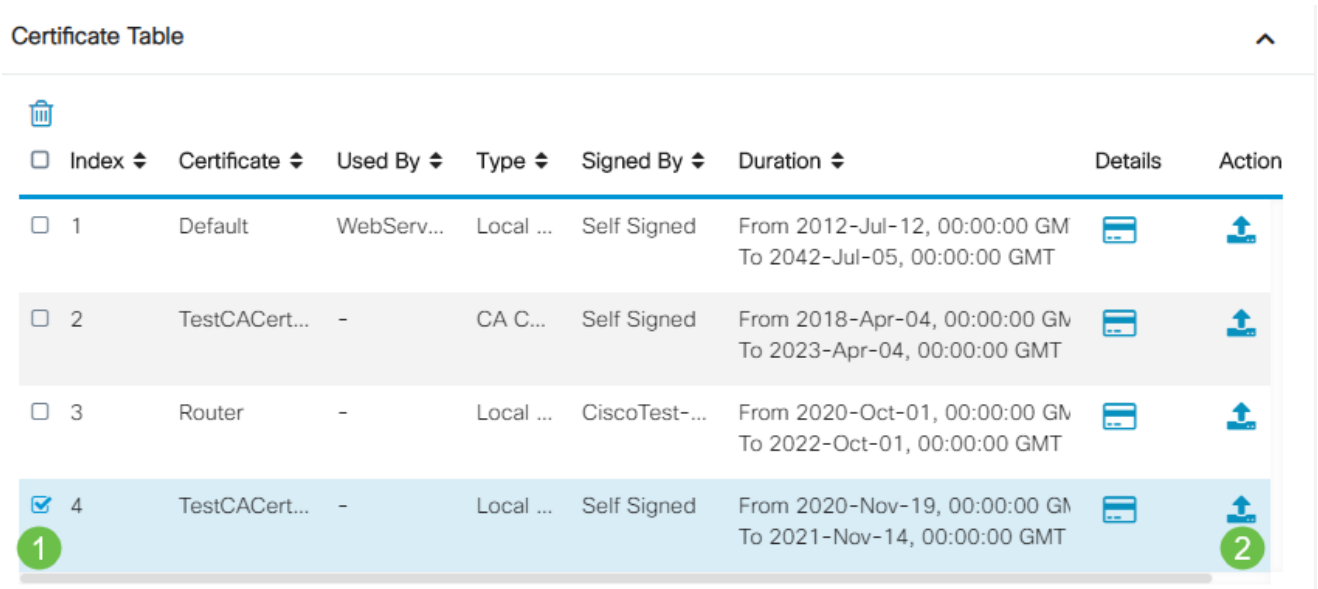


Agora você deve ter criado com êxito um certificado no roteador RV345P.

Exportar um certificado

Passo 1

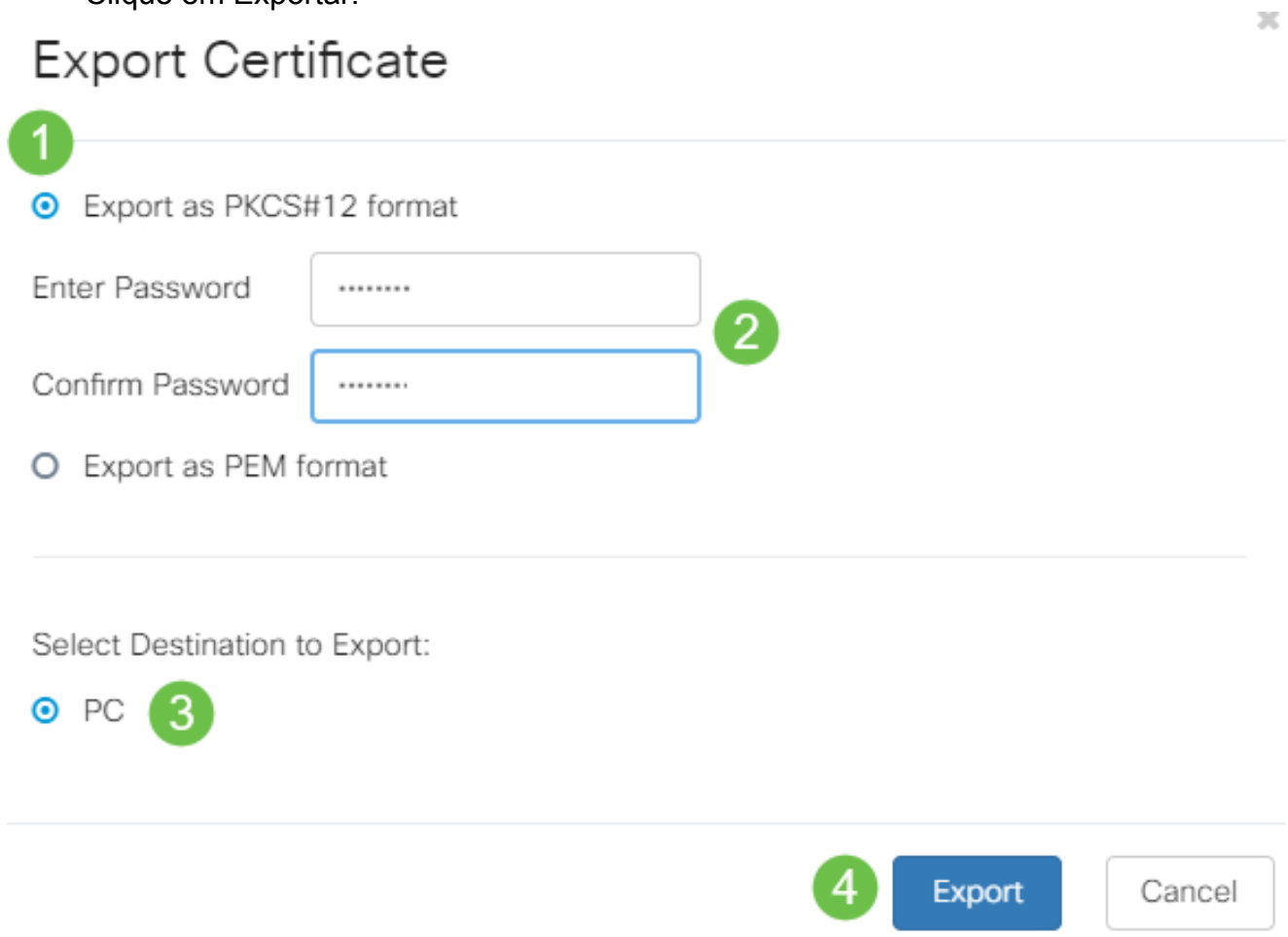
Na Tabela de Certificados, marque a caixa de seleção do certificado que deseja exportar e clique no ícone de exportação.



Passo 2

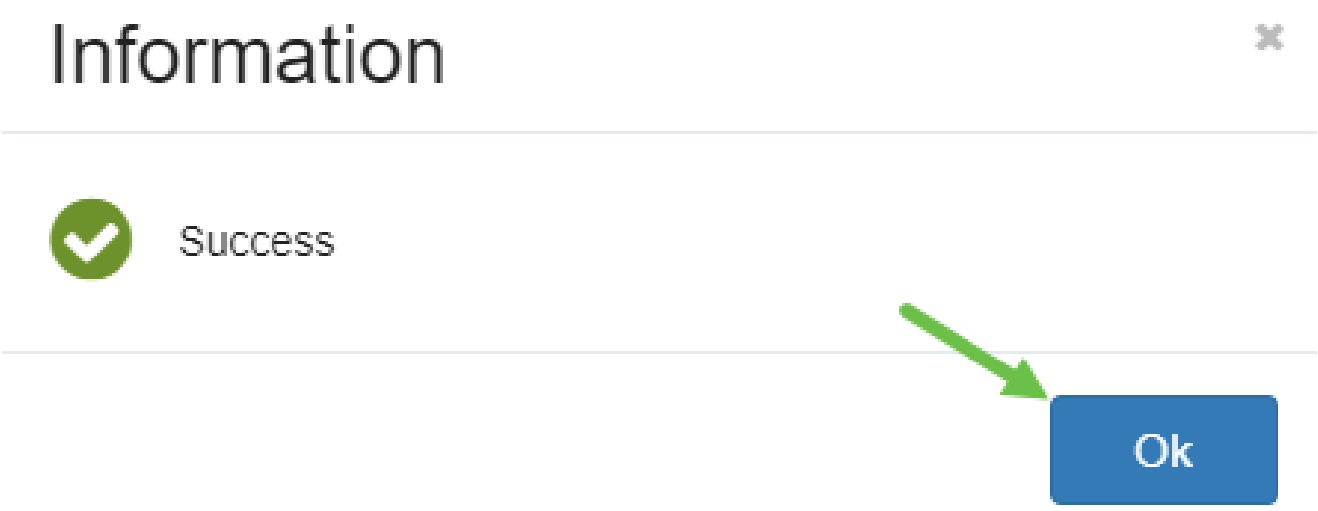
- Clique em um formato para exportar o certificado. As opções são:
  - PKCS #12 — O PKCS (Public Key Cryptography Standards) #12 é um certificado

exportado que vem com uma extensão .p12. Uma senha será necessária para criptografar o arquivo e protegê-lo quando ele for exportado, importado e excluído.
    - PEM — O Privacy Enhanced Mail (PEM) é frequentemente usado para servidores da Web devido à sua capacidade de serem facilmente traduzidos em dados legíveis por meio de um editor de texto simples, como o bloco de notas.
- Se você escolher PEM, basta clicar em Exportar.
- Digite uma senha para proteger o arquivo a ser exportado no campo Digitar senha.
- Insira novamente a senha no campo Confirmar senha.
- Na área Selecionar destino, o PC foi escolhido e é a única opção disponível no momento.
- Clique em Exportar.



Etapa 3

Uma mensagem indicando o sucesso do download será exibida abaixo do botão Download. O download de um arquivo será iniciado em seu navegador. Click OK.

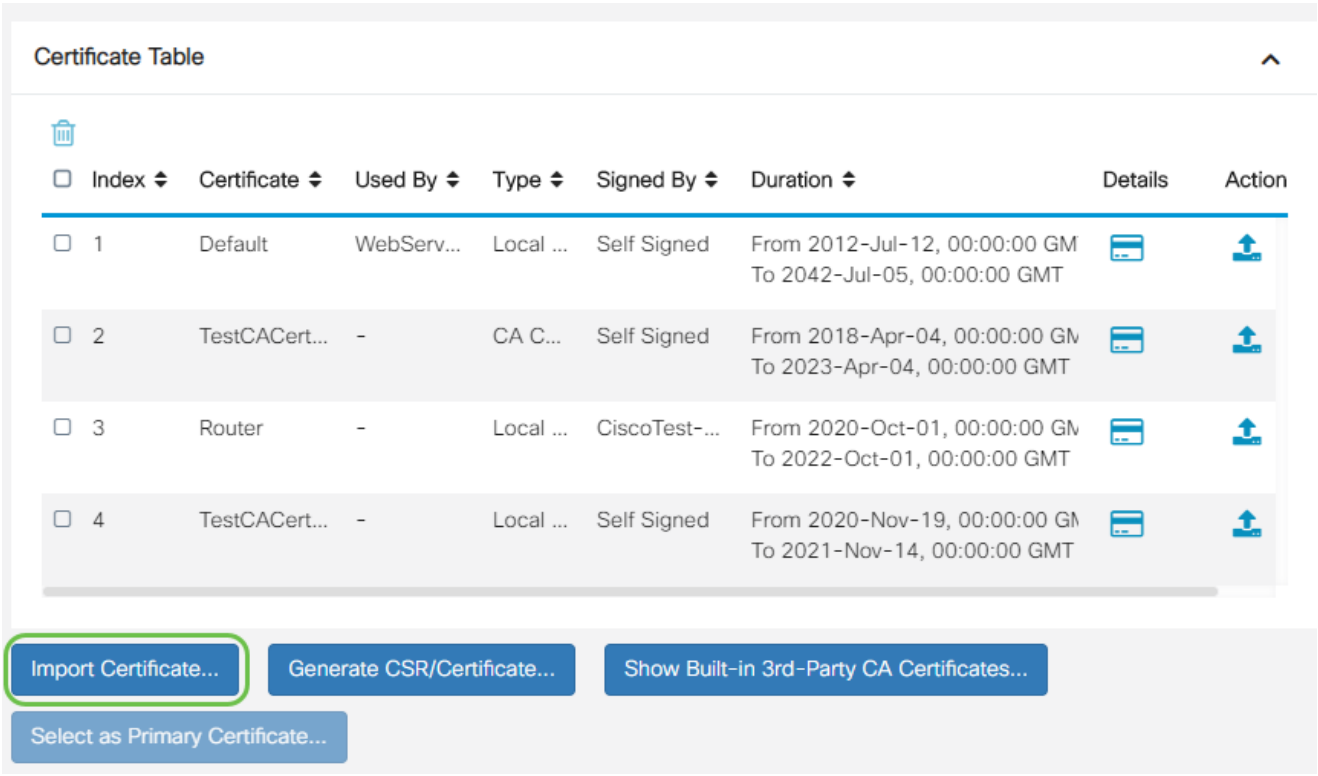


Agora você deve ter exportado com êxito um certificado no RV345P Series Router.

Importar um certificado

Passo 1

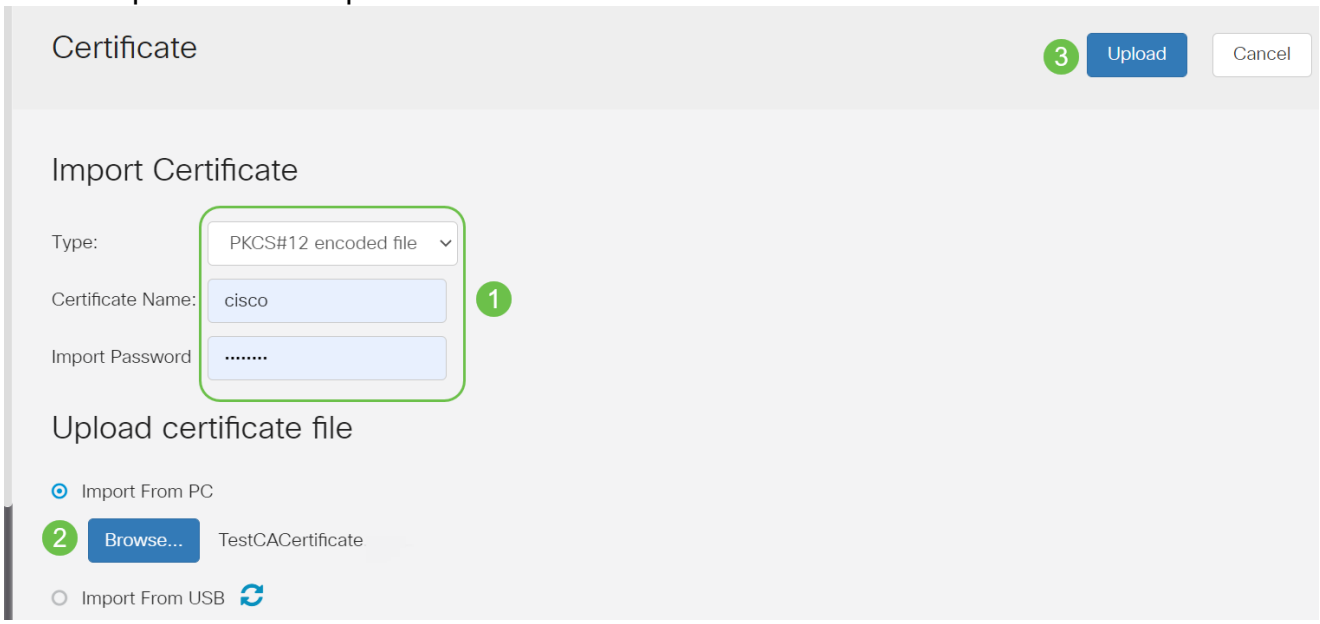
Clique em Importar certificado....



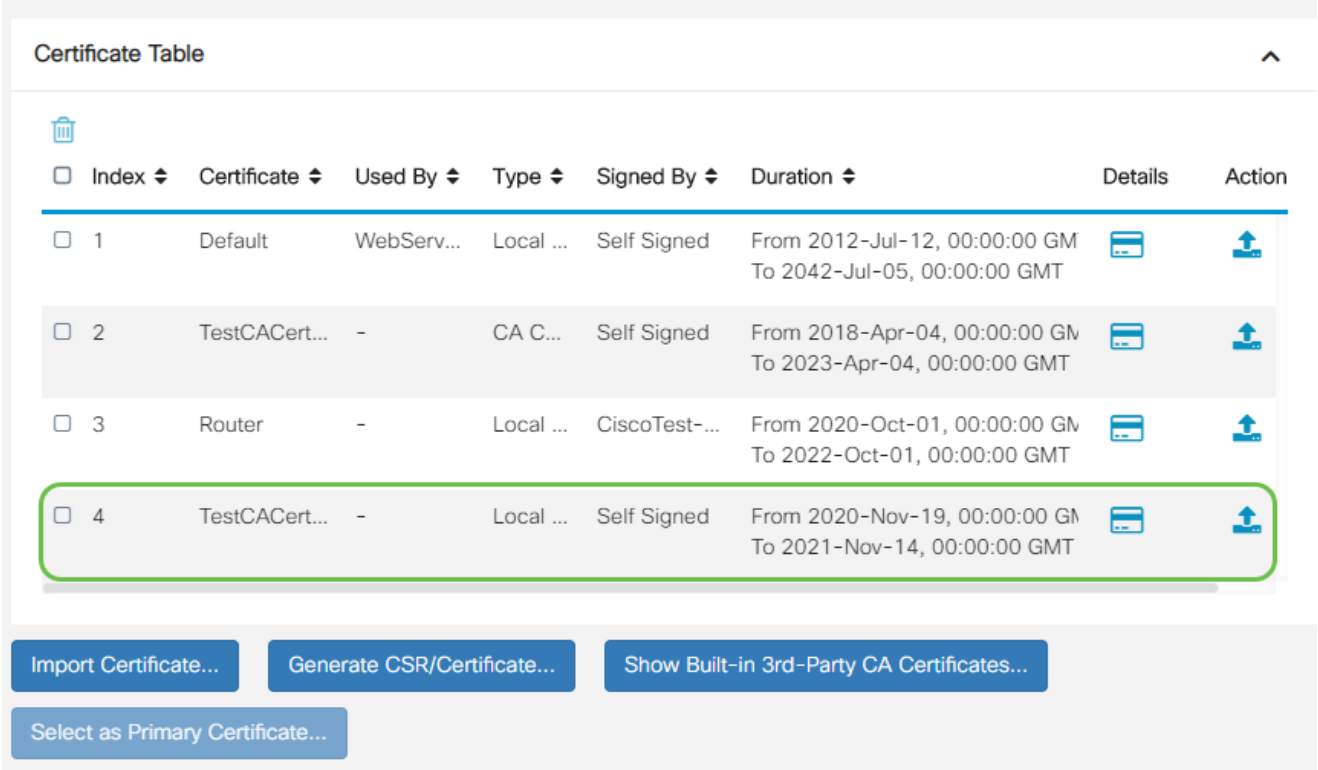
Passo 2

- Escolha o tipo de certificado a ser importado na lista suspensa. As opções são:
  - Certificado local — Um certificado gerado no roteador.
  - Certificado de CA — Um certificado certificado certificado por uma autoridade terceira confiável que confirmou que as informações contidas no certificado são

precisas.
    - Arquivo PKCS #12 Codificado — #12 PKCS (Public Key Cryptography Standards) é um formato de armazenamento de um certificado de servidor.
- Insira um nome para o certificado no campo Nome do certificado.
- Se o #12 PKCS tiver sido escolhido, insira uma senha para o arquivo no campo Import Password (Importar senha). Caso contrário, vá para o passo 3.
- Clique em uma origem para importar o certificado. As opções são:
    - Importar do PC
    - Importar do USB
- Se o roteador não detectar uma unidade USB, a opção Importar de USB ficará acinzentada.
- Se você escolheu Import From USB (Importar do USB) e seu USB não estiver sendo reconhecido pelo roteador, clique em Refresh (Atualizar).
- Clique no botão Choose File (Escolher arquivo) e escolha o arquivo apropriado.
- Clique em Fazer upload.



Assim que obtiver êxito, você será automaticamente direcionado à página Certificado principal. A tabela de certificados será preenchida com o certificado importado recentemente.



Agora você deve ter importado com êxito um certificado em seu roteador RV345P.

Configure uma rede móvel usando um dongle e um roteador série RV345P (opcional)

Talvez você queira configurar uma rede móvel de backup usando um dongle e seu roteador RV345P. Se esse for o caso, você deverá ler Configure a Mobile Network Using a Dongle and an RV34x Series Router.

Parabéns, você concluiu a configuração de seu roteador RV345P! Agora você configurará seus dispositivos sem fio Cisco Business.

Configurar a rede em malha sem fio

CBW140AC pronto para uso

Comece conectando um cabo Ethernet da porta PoE no CBW140AC a uma porta PoE no RV345P. Metade das portas no RV345P pode fornecer PoE, portanto, qualquer uma delas pode ser usada.

Verifique o status das luzes indicadoras. O ponto de acesso levará cerca de 10 minutos para inicializar. O LED piscará em verde em vários padrões, alternando rapidamente entre verde, vermelho e âmbar antes de ficar verde novamente. Pode haver pequenas variações na intensidade e matiz da cor do LED de uma unidade para outra. Quando a luz do LED estiver piscando em verde, continue com a próxima etapa.

A porta de uplink Ethernet PoE no AP de Aplicativo Móvel SÓ pode ser usada para fornecer

um uplink para a LAN e NÃO para se conectar a qualquer outro aplicativo móvel com capacidade ou dispositivos de extensor de malha.

Se o seu ponto de acesso não for novo, pronto para uso, certifique-se de que ele esteja redefinido para as configurações padrão de fábrica para que o SSID CiscoBusiness-Setup apareça em suas opções de Wi-Fi. Para obter ajuda com isso, consulte Como reinicializar e redefinir para as configurações padrão de fábrica em roteadores RV345x.

Configurar o ponto de acesso sem fio do aplicativo móvel 140AC

Nesta seção, você usará o aplicativo móvel para configurar o ponto de acesso sem fio do aplicativo móvel.

Tenha em mente que o aplicativo tem atualizações frequentes e a aparência/layout pode mudar com o tempo.

Na parte traseira do 140AC, conecte o cabo fornecido com o AP ao PoE amarelo e conecte o 140 AC. Conecte a outra extremidade a uma das portas LAN RV345P.

Se você tiver problemas para se conectar, consulte a seção Dicas de solução de problemas para conexões sem fio deste artigo.

Passo 1

Baixe o Cisco Business Wireless App disponível no Google Play ou na Apple App Store em seu dispositivo móvel. Você precisará de um dos seguintes sistemas operacionais:

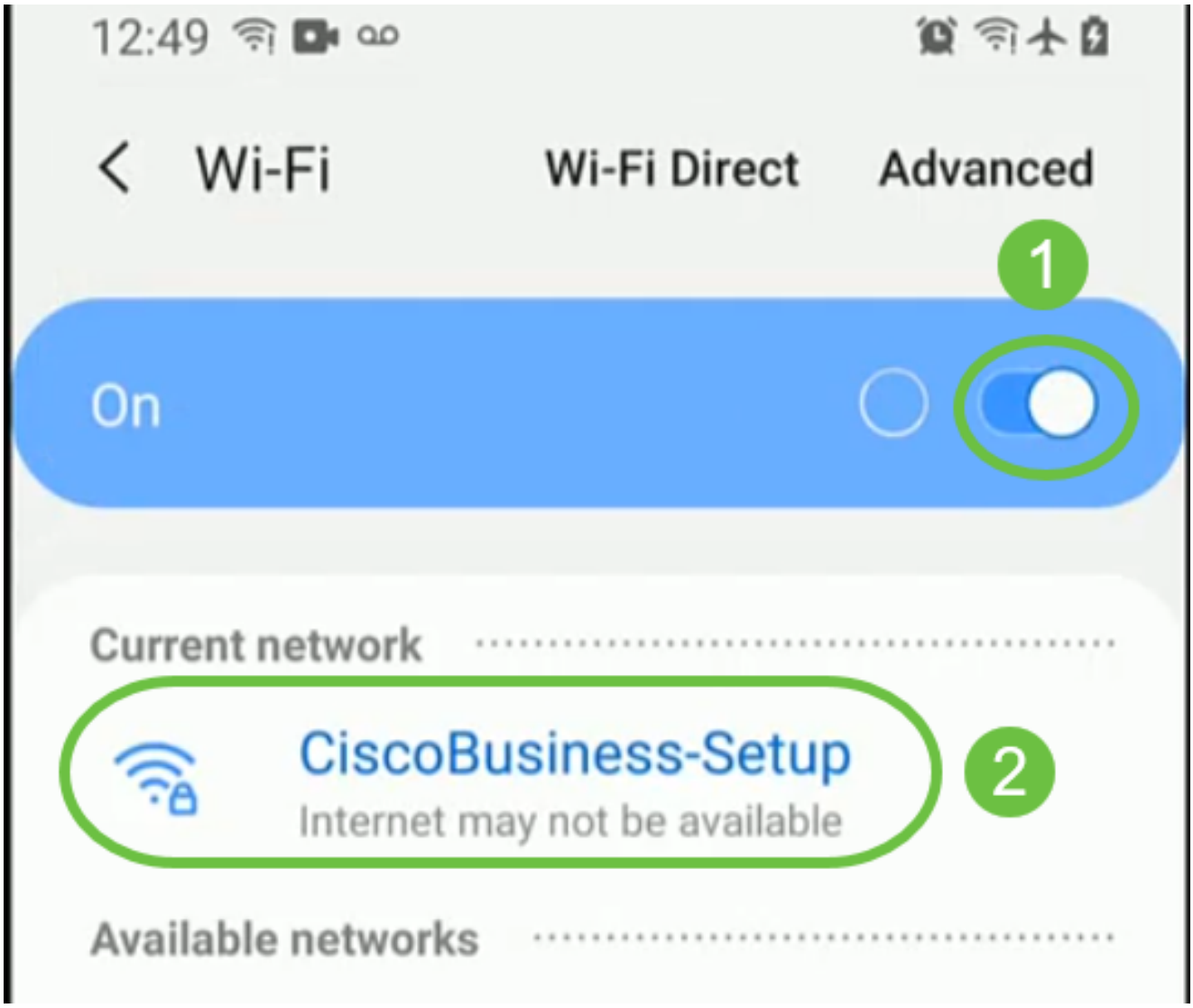
- Android versão 5.0 ou superior
- iOS versão 8.0 ou superior

Passo 2

Abra o Cisco Business Application em seu dispositivo móvel.

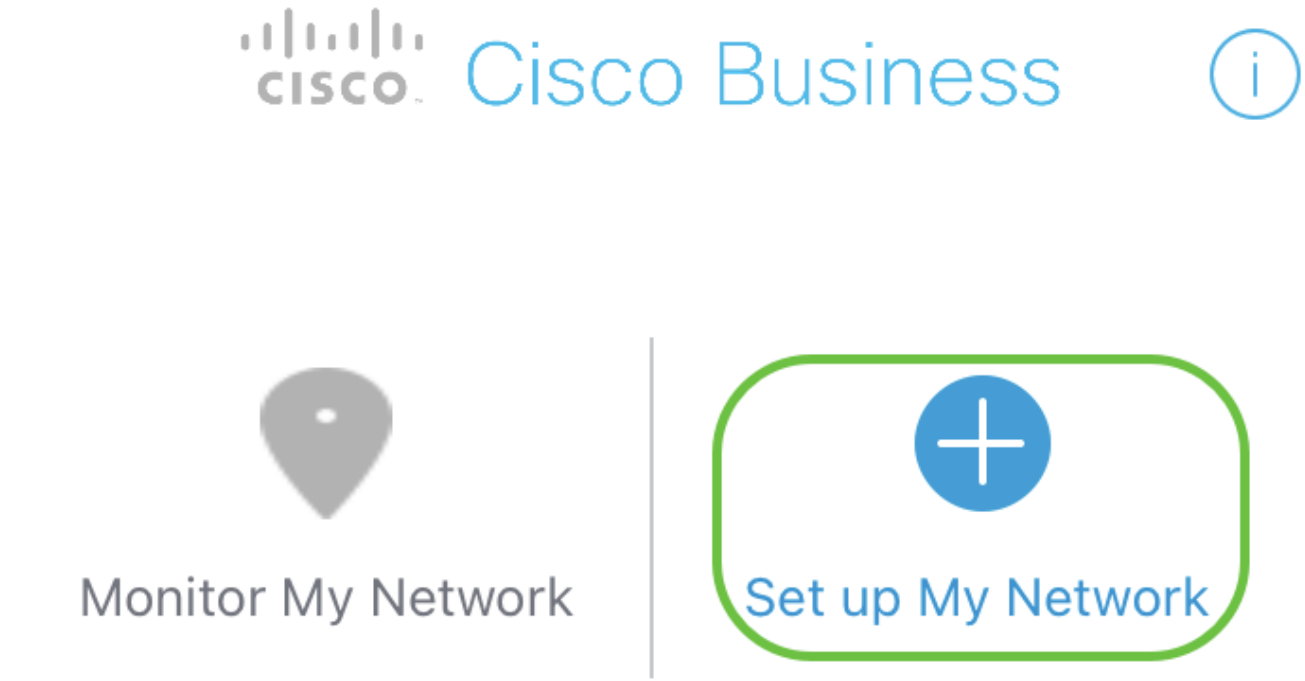
Etapa 3

Conecte-se à rede sem fio CiscoBusiness-Setup em seu dispositivo móvel. A senha é cisco123.



Passo 4

O aplicativo detecta automaticamente a rede móvel. Selecione Configurar minha rede.

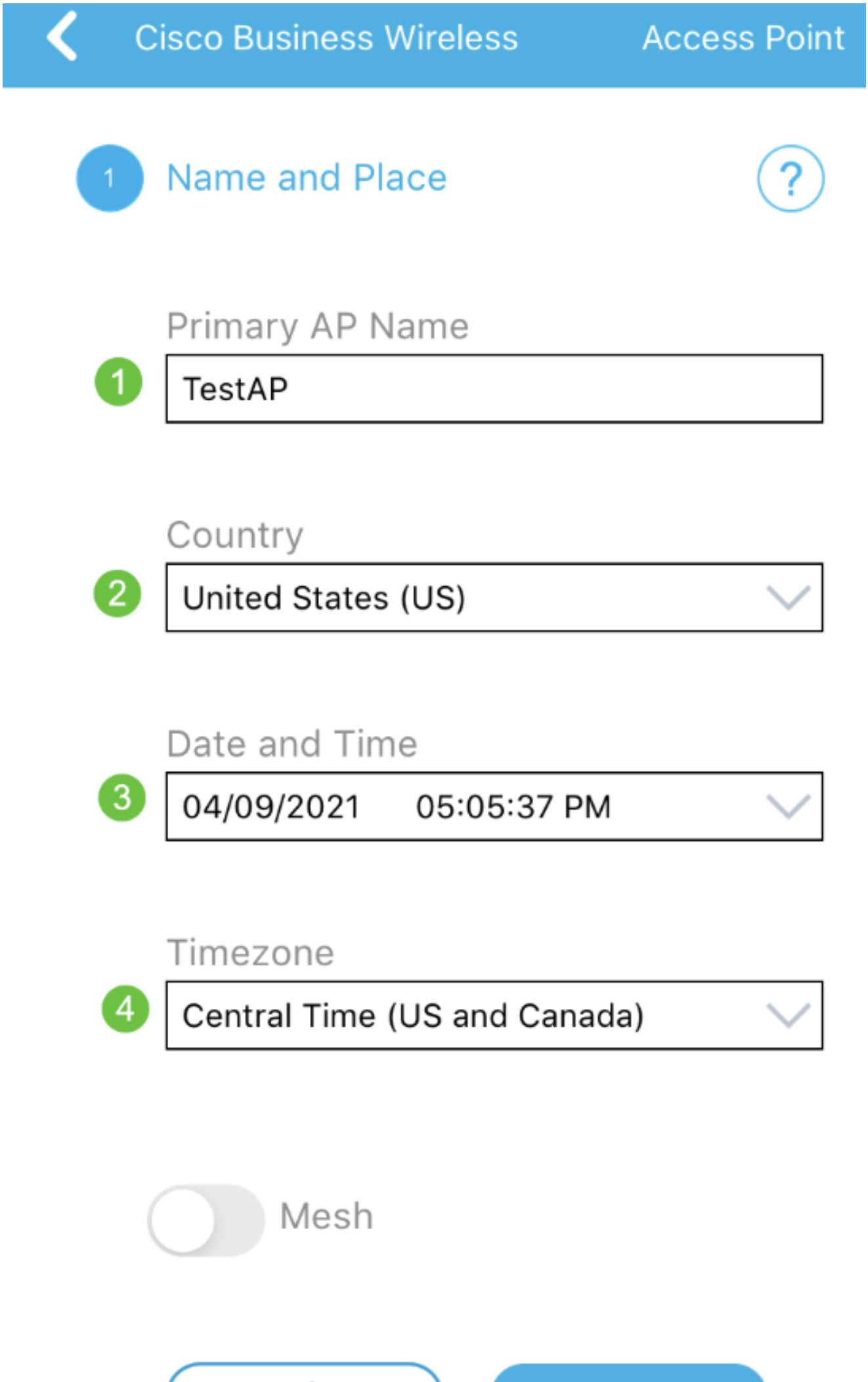


Etapa 5

Para configurar a rede, insira o seguinte:

- Criar nome de usuário do administrador
- Criar senha de administrador
- Confirme a senha do administrador digitando-a novamente
- (Opcional) Marque a caixa de seleção para Mostrar senha.

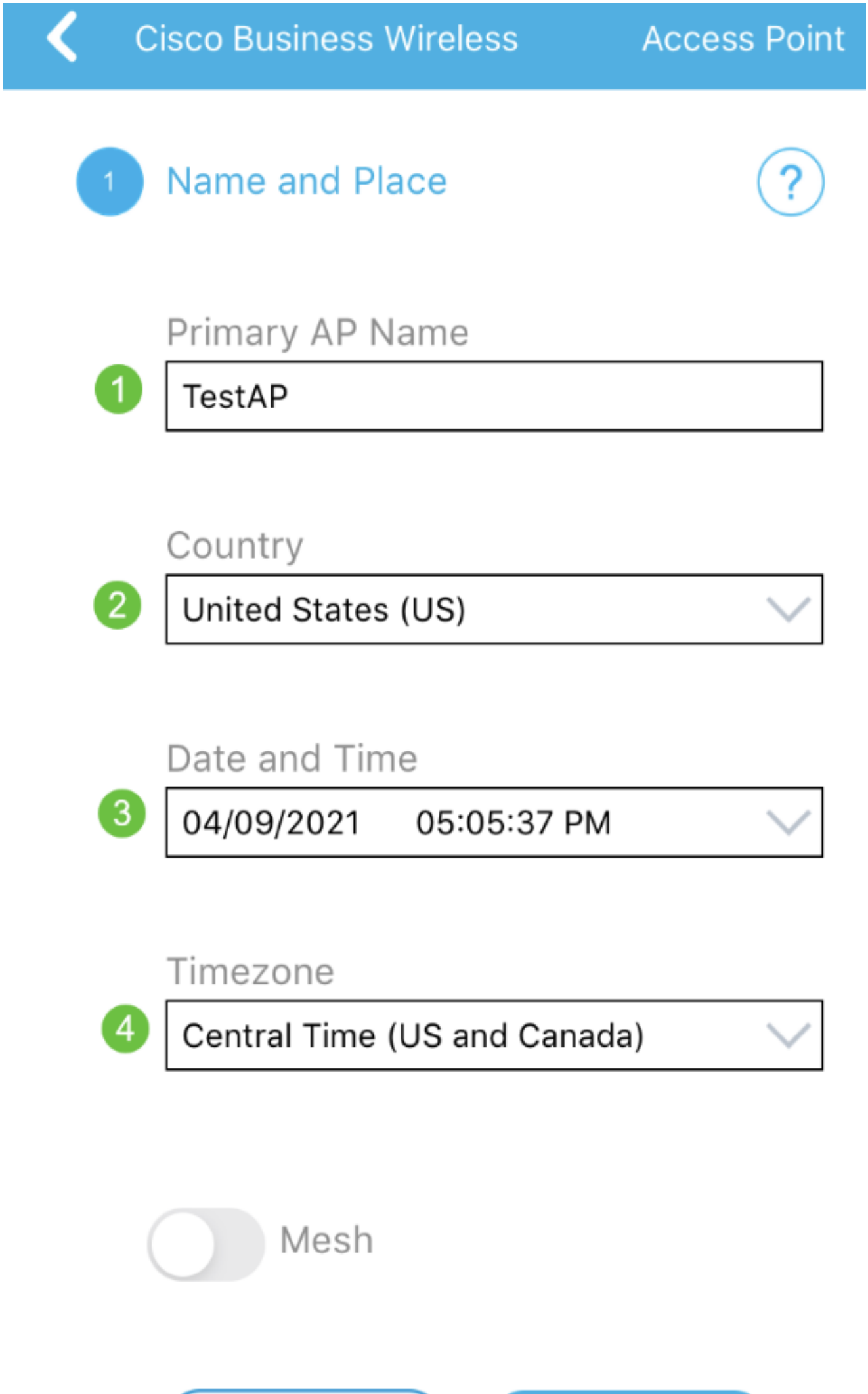
Selecione Comece agora.


Cisco Business Wireless
Access Point
1
Name and Place
?
Primary AP Name
1
TestAP
Country
2
United States (US)
Date and Time
3
04/09/2021 05:05:37 PM
Timezone
4
Central Time (US and Canada)
Mesh

Etapa 6

Para configurar Nome e local, insira com precisão as informações a seguir. Se você inserir informações conflitantes, isso poderá levar a um comportamento imprevisível.

- Nome do AP do aplicativo móvel para sua rede sem fio.
- País
- Data
- Tempo
- Fuso horário


Cisco Business Wireless
Access Point
1
Name and Place
Primary AP Name
1
TestAP
Country
2
United States (US)
Date and Time
3
04/09/2021 05:05:37 PM
Timezone
4
Central Time (US and Canada)
Mesh

Etapa 7

Ative o botão de alternância para Mesh. Clique em Next.

1 Name and Place

Primary AP Name

TestAP

Country

United States (US)

Date and Time

04/09/2021 05:05:37 PM

Timezone

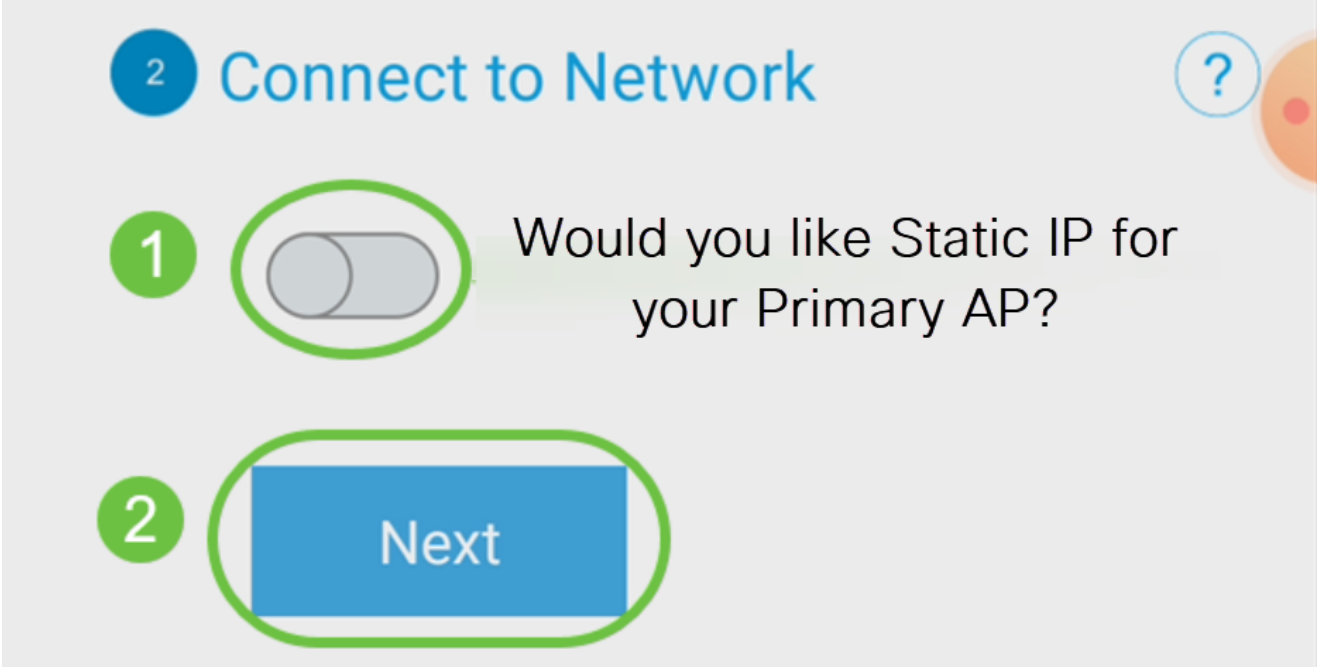
Central Time (US and Canada)

1

Mesh

Passo 8

(Opcional) Você pode optar por habilitar o IP estático para seu AP de aplicativo móvel para fins de gerenciamento. Caso contrário, o servidor DHCP atribuirá um endereço IP. Se você não quiser configurar o IP estático para seu ponto de acesso, clique em Avançar.

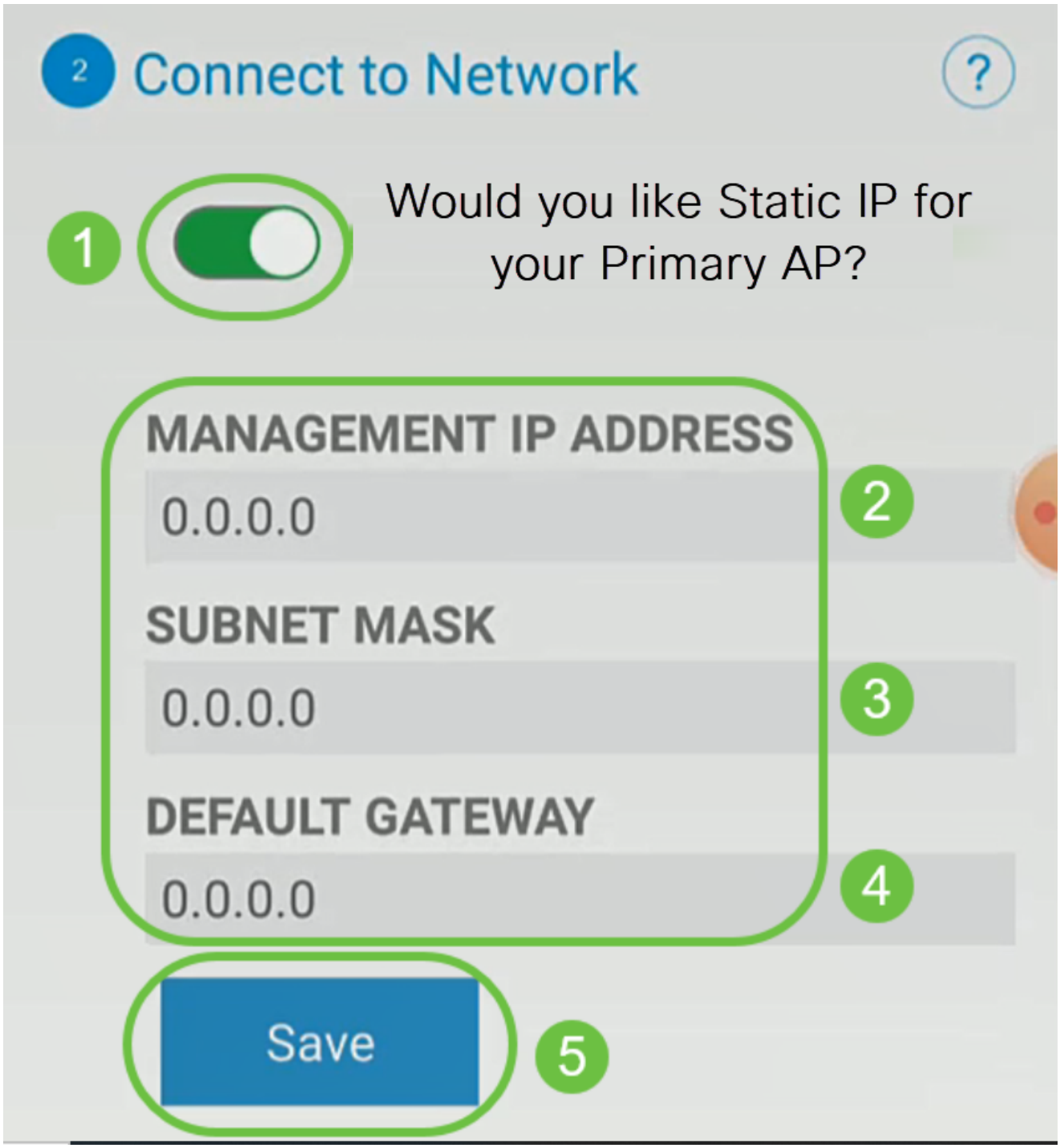


Como alternativa, para conectar-se à rede:

Selecione Static IP (IP estático) para seu aplicativo móvel AP. Por padrão, essa opção está desativada.

- Insira o endereço IP de gerenciamento
- Máscara de sub-rede
- Gateway padrão

Click Save.

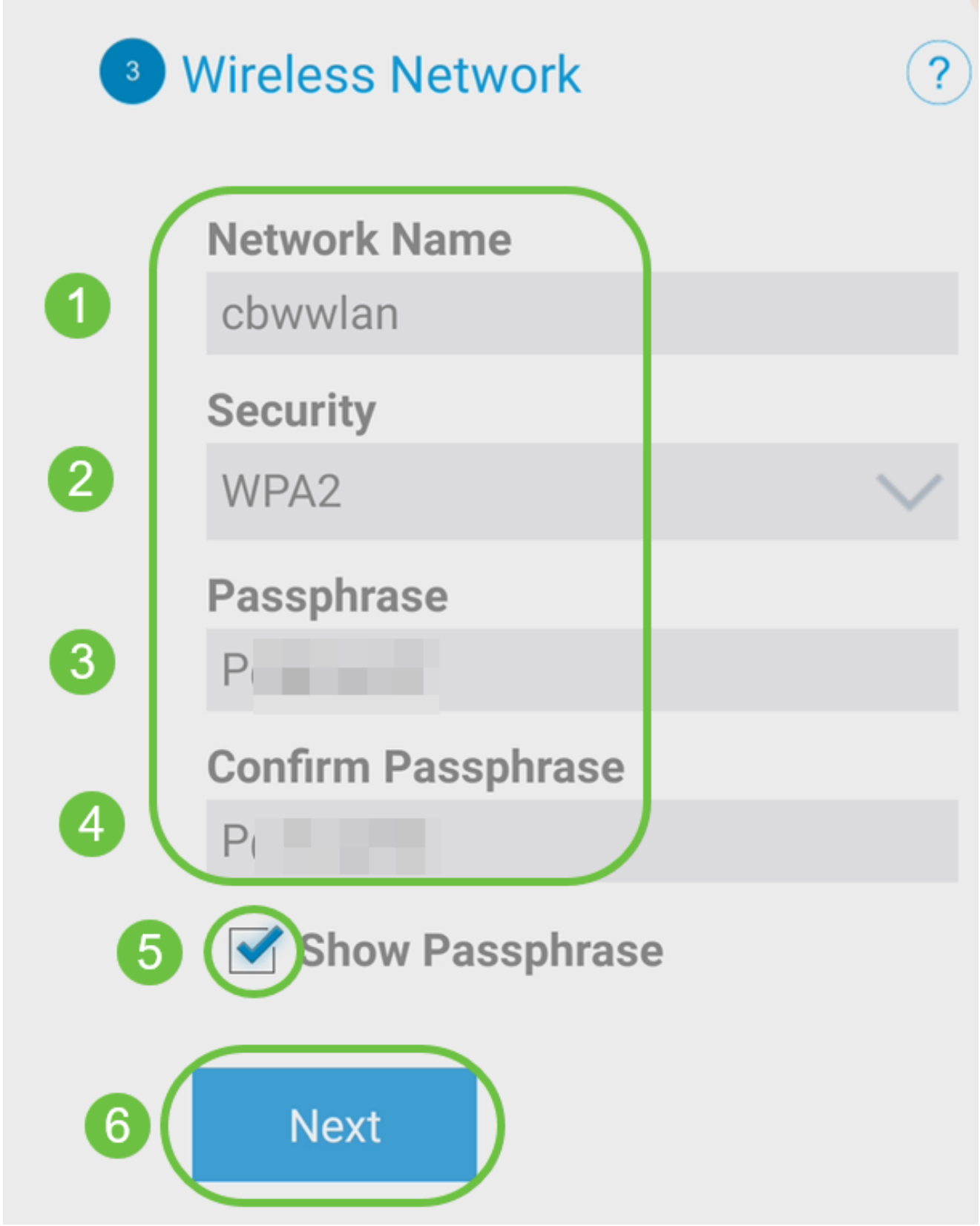


Passo 9

Configure a rede sem fio digitando o seguinte:

- Nome da rede/SSID
- Security
- Senha
- Confirmar senha
- (Opcional) Marque Mostrar senha

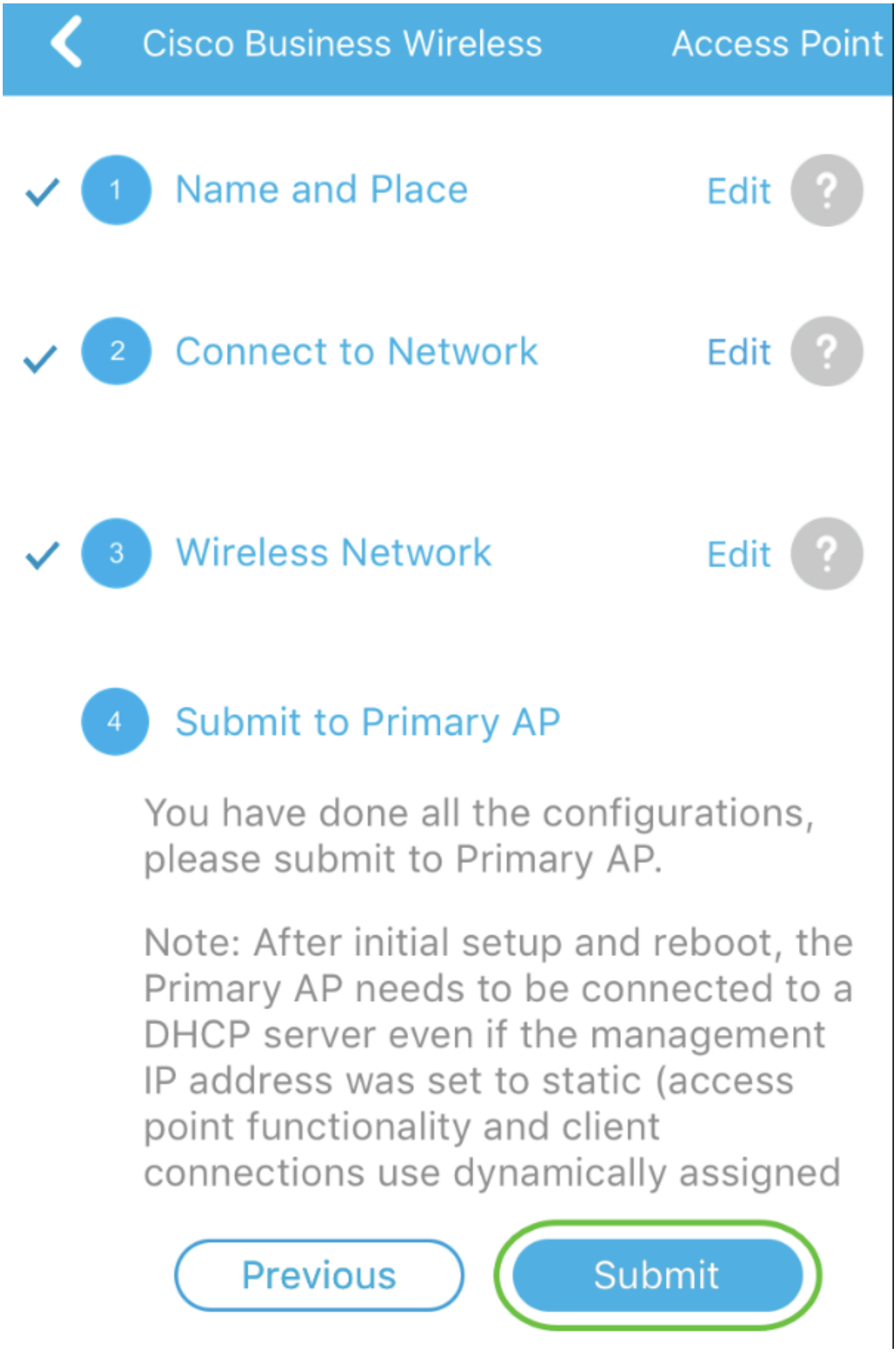
Clique em Next.



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

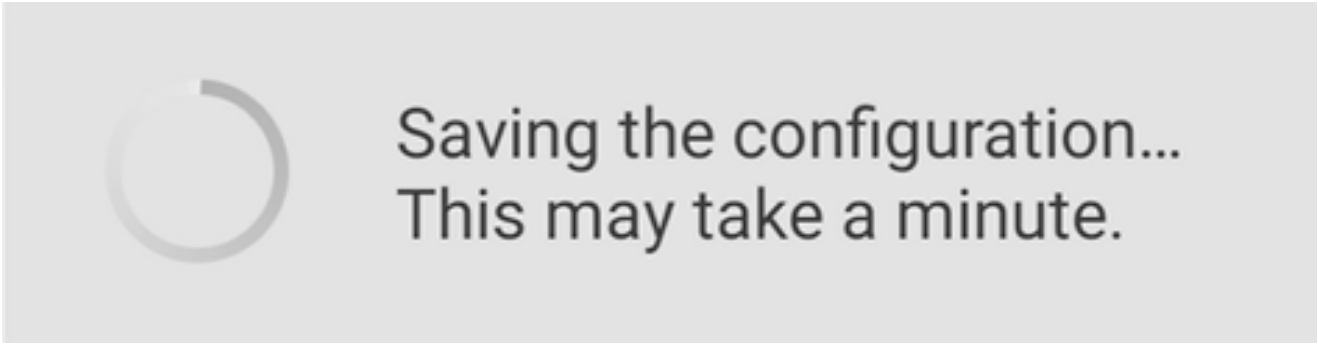
Passo 10

Para confirmar as configurações na tela Submit to Mobile Application AP, clique em Submit.


Cisco Business Wireless
Access Point
1
Name and Place
Edit
2
Connect to Network
Edit
3
Wireless Network
Edit
4
Submit to Primary AP
You have done all the configurations, please submit to Primary AP.
Note: After initial setup and reboot, the Primary AP needs to be connected to a DHCP server even if the management IP address was set to static (access point functionality and client connections use dynamically assigned
Previous
Submit

Passo 11

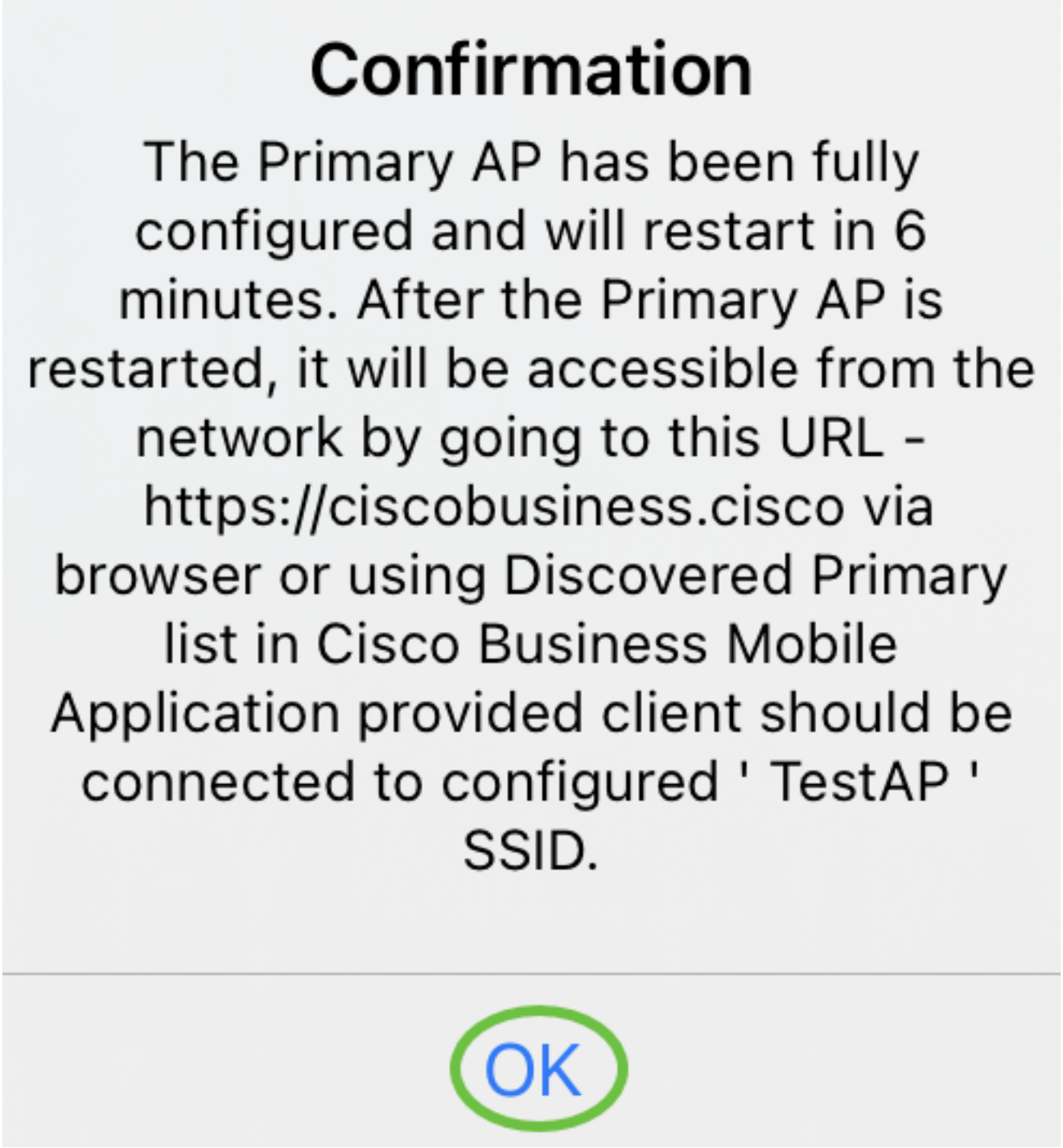
Aguarde até que a reinicialização seja concluída.



A reinicialização pode levar até 10 minutos. Durante uma reinicialização, o LED no access point passará por vários padrões de cores. Quando o LED estiver piscando em verde, vá para a próxima etapa. Se o LED não passar pelo padrão de vermelho piscando, isso indica que não há nenhum servidor DHCP em sua rede. Assegure-se de que o AP esteja conectado a um switch ou a um roteador com um servidor DHCP.

Etapa 12

Você verá a seguinte tela Confirmation. Click OK.



Passo 13

Feche o aplicativo, conecte-se à rede sem fio recém-criada e reinicie-a para concluir com êxito a primeira parte da rede sem fio.

Dicas de solução de problemas sem fio

Se tiver algum problema, confira as seguintes dicas:

- Verifique se o Service Set Identifier (SSID) correto está selecionado. Esse é o nome que você criou para a rede sem fio.
- Desconecte qualquer VPN para o aplicativo móvel ou em um laptop. Você pode até

estar conectado a uma VPN que o seu provedor de serviços móveis usa e que talvez você nem saiba. Por exemplo, um telefone Android (Pixel 3) com Google Fi como provedor de serviços, tem uma VPN integrada que se conecta automaticamente sem notificação. Isso precisaria ser desabilitado para encontrar o AP do aplicativo móvel.
- Faça login no AP de aplicativo móvel com https://<endereço IP do AP de aplicativo móvel>.
- Depois de fazer a configuração inicial, certifique-se de que https:// is esteja sendo usado, esteja você fazendo login em ciscobusiness.cisco ou inserindo o endereço IP no seu navegador da Web. Dependendo de 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 (Firefox neste caso) clique no menu Abrir, vá para Ajuda > Informações de solução de problemas e clique em Atualizar Firefox.

Configurar os extensores de malha CBW142ACM

Você está no trecho inicial da configuração desta rede, você só precisa adicionar seus extensores de malha!

Faça login no aplicativo Cisco Business em seu dispositivo móvel.

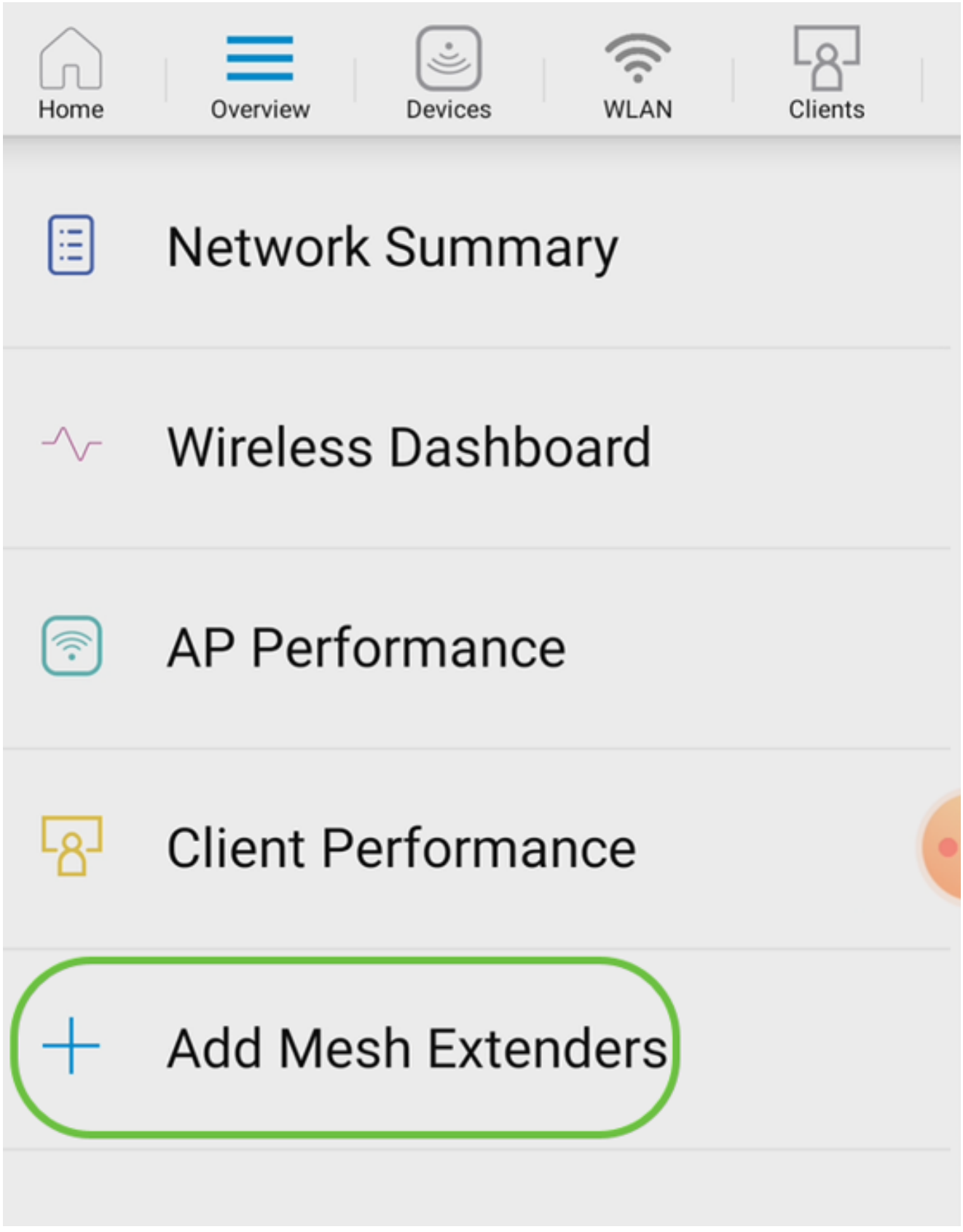
Passo 1

Navegue até Devices. Verifique se a malha está habilitada.

Name	Clients	Usage
APA453.0E1E.2338*	0	0 Bytes
AP4CBC.48C0.74B8	0	0 Bytes
APA453.0E22.0A70	0	0 Bytes
AP68CA.E46E.1650	0	2 MB
AP68CA.E470.0500	0	11 MB

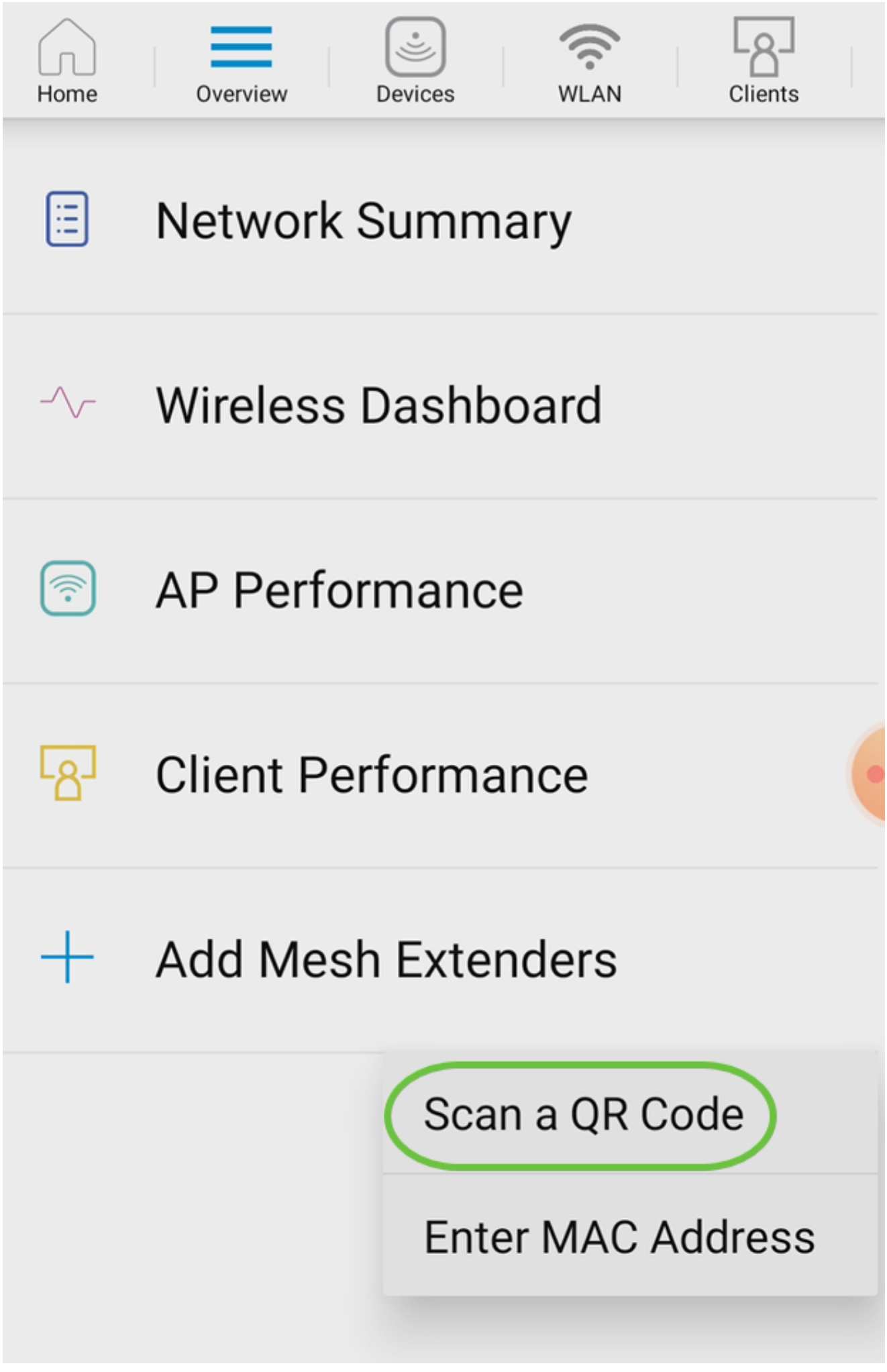
Passo 2

Você deve inserir o endereço MAC de todos os extensores de malha que deseja usar na rede em malha com o AP de aplicativo móvel. Para adicionar o endereço MAC, clique em Add Mesh Extenders no menu.



Etapa 3

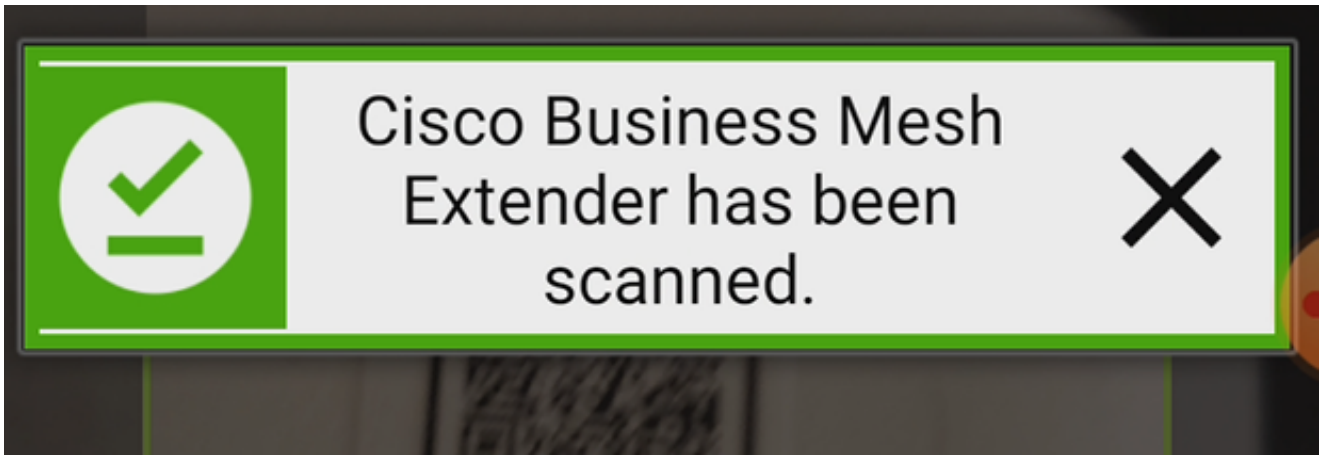
Você pode adicionar o endereço MAC examinando um código QR ou inserindo manualmente o endereço MAC. Neste exemplo, Digitalizar um código QR está selecionado.


Home
Overview
Devices
WLAN
Clients
Network Summary
Wireless Dashboard
AP Performance
Client Performance
Add Mesh Extenders
Scan a QR Code
Enter MAC Address

Passo 4

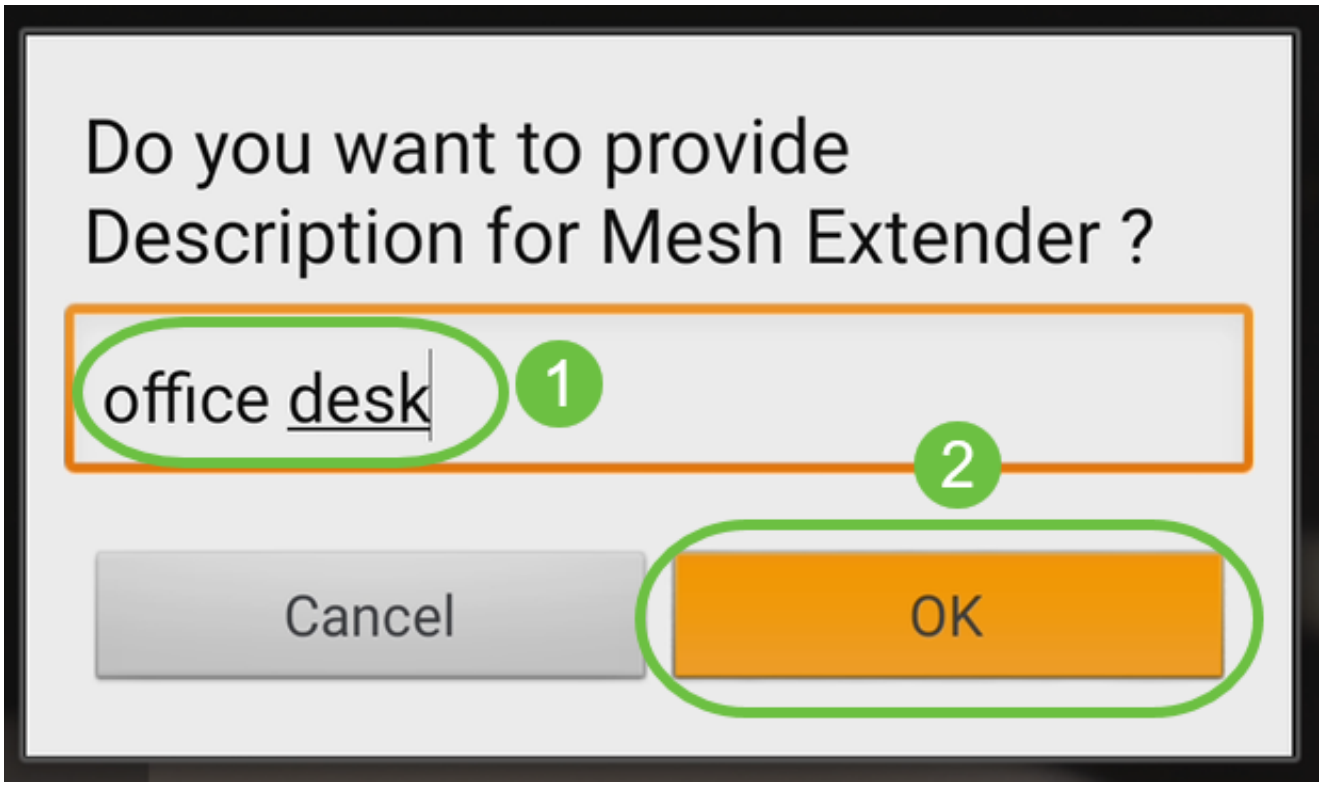
Um leitor de código QR aparecerá para digitalizar o código QR.

Você verá a tela a seguir depois que o código QR do extensor de malha tiver sido digitalizado.



Etapa 5 (opcional)

Se preferir, insira uma Descrição para o Extensor de Malha. Click OK.



Etapa 6

Revise o Resumo e clique em Enviar.

Summary

Almost done. The following Mesh Extenders will be added to your site. If you are done adding Mesh Extenders, click submit.

Mesh Extenders To Be Added

Scanned MAC Address

A4 0 office desk

Etapa 7

Clique em Add More Mesh Extenders para adicionar outros extensores de malha à sua rede. Quando todos os extensores de malha tiverem sido adicionados, clique em Concluído.

Done! Your Mesh Extender has been added

Good News! You've successfully added your Mesh Extender

Mesh Extender Status

A4 0 SUCCESS

What's Next ?

Add More Mesh Extenders

Repita o procedimento para cada extensor de malha.

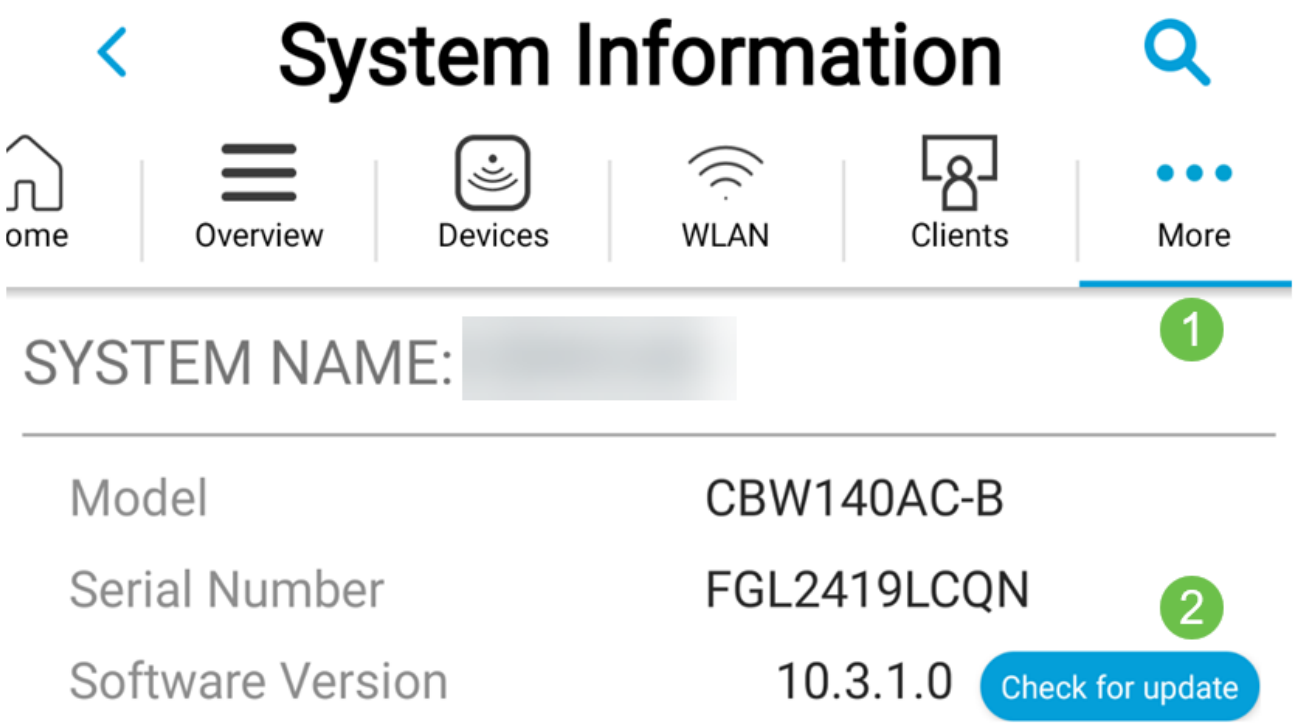
Agora você tem as configurações básicas prontas para serem implementadas. Antes de prosseguir, verifique e atualize o software, se necessário.

Verificar e atualizar software no aplicativo móvel

A atualização do software é extremamente importante, portanto, não ignore esta parte!

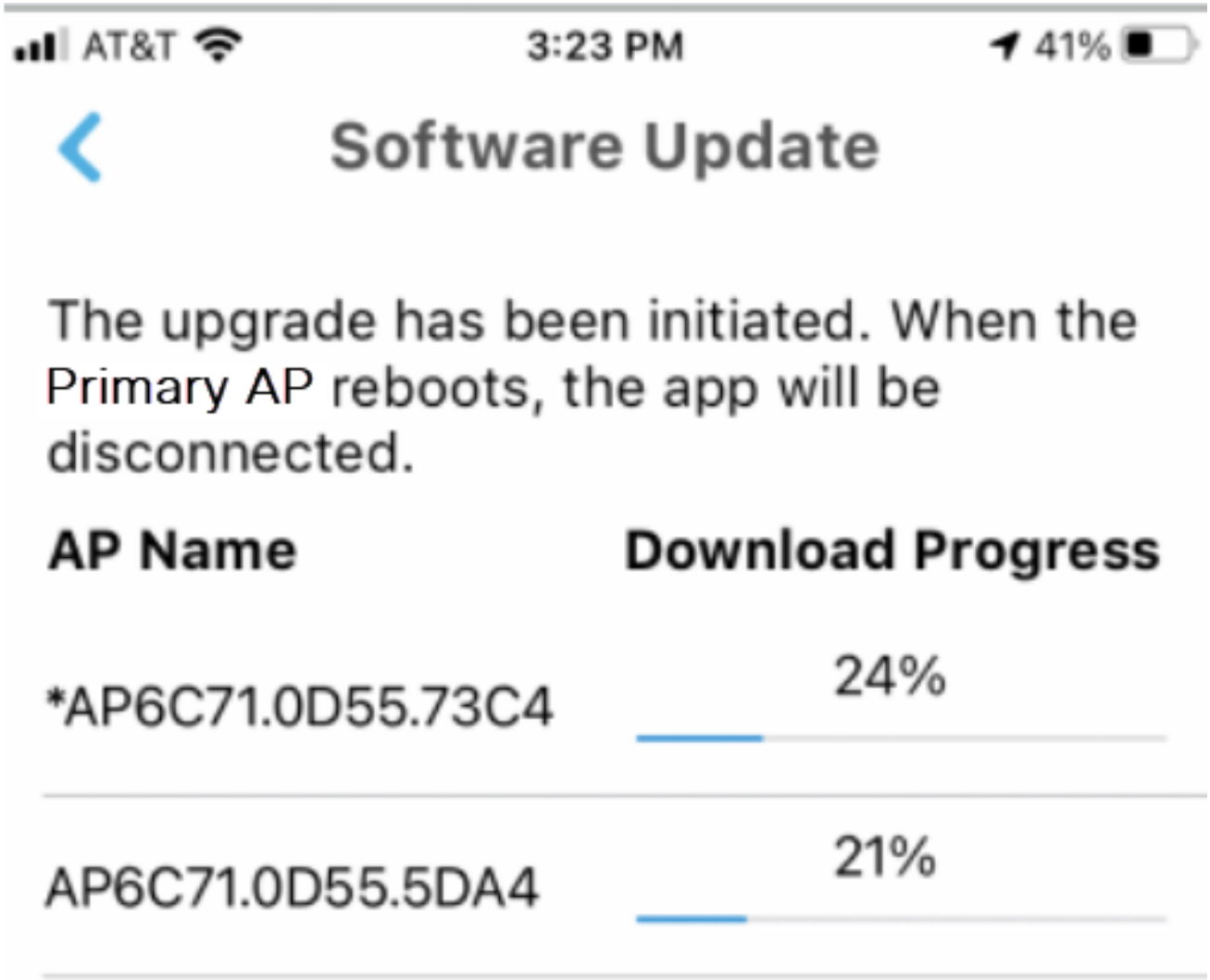
Passo 1

Em seu aplicativo móvel, na guia More, clique no botão Check for update. Siga os avisos para atualizar o software para a versão mais recente.



Passo 2

Você verá o progresso do download à medida que ele for carregado.


AT&T
3:23 PM
41%
Software Update
The upgrade has been initiated. When the Primary AP reboots, the app will be disconnected.
AP Name
Download Progress
*AP6C71.0D55.73C4
24%
AP6C71.0D55.5DA4
21%

Etapa 3

Uma confirmação pop-up o notificará da conclusão da atualização do software. Click OK.

Criar WLANs usando o aplicativo móvel

Esta seção permite criar Redes Locais Sem Fio (WLANs).

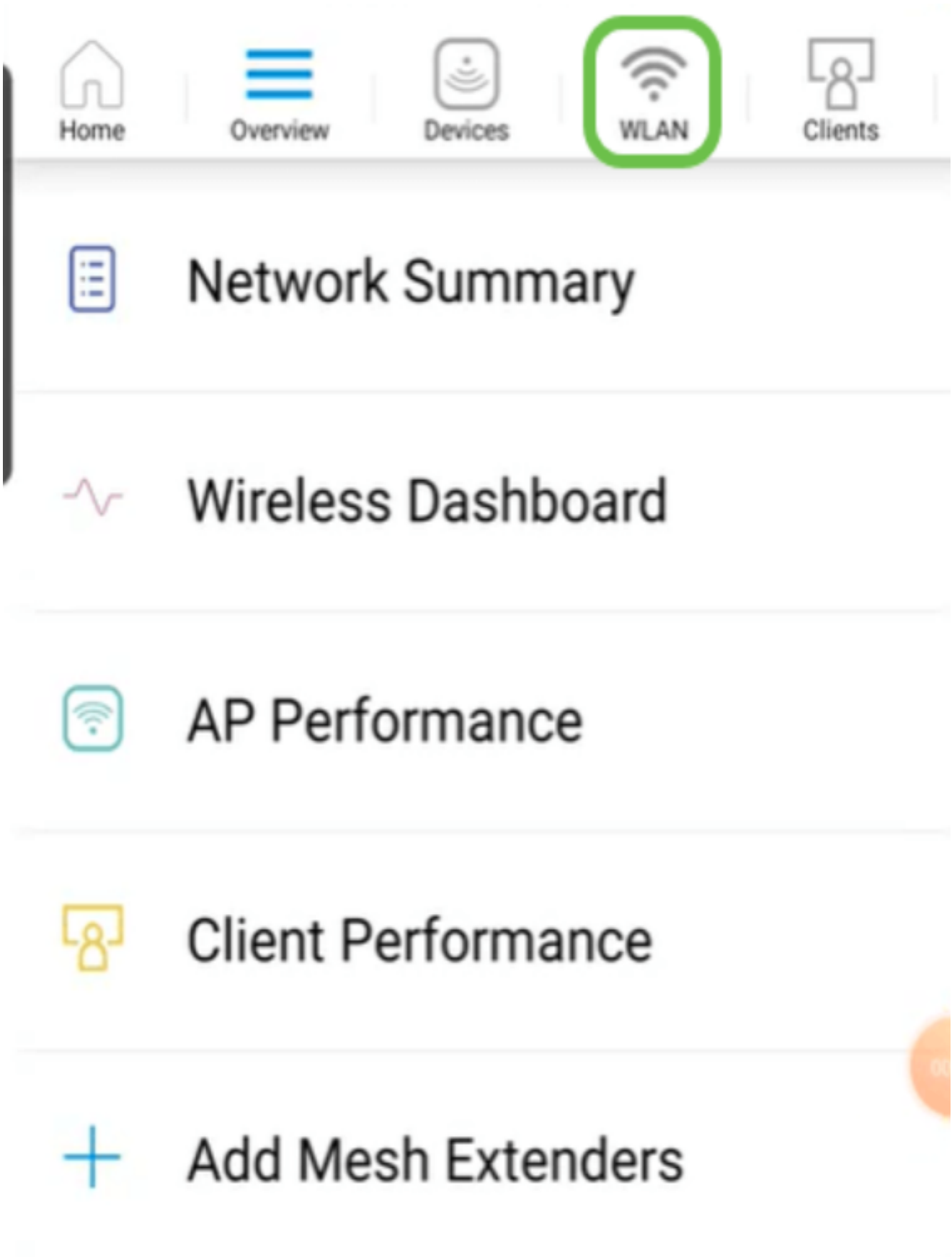
Passo 1

Abra o aplicativo sem fio Cisco Business.

Passo 2

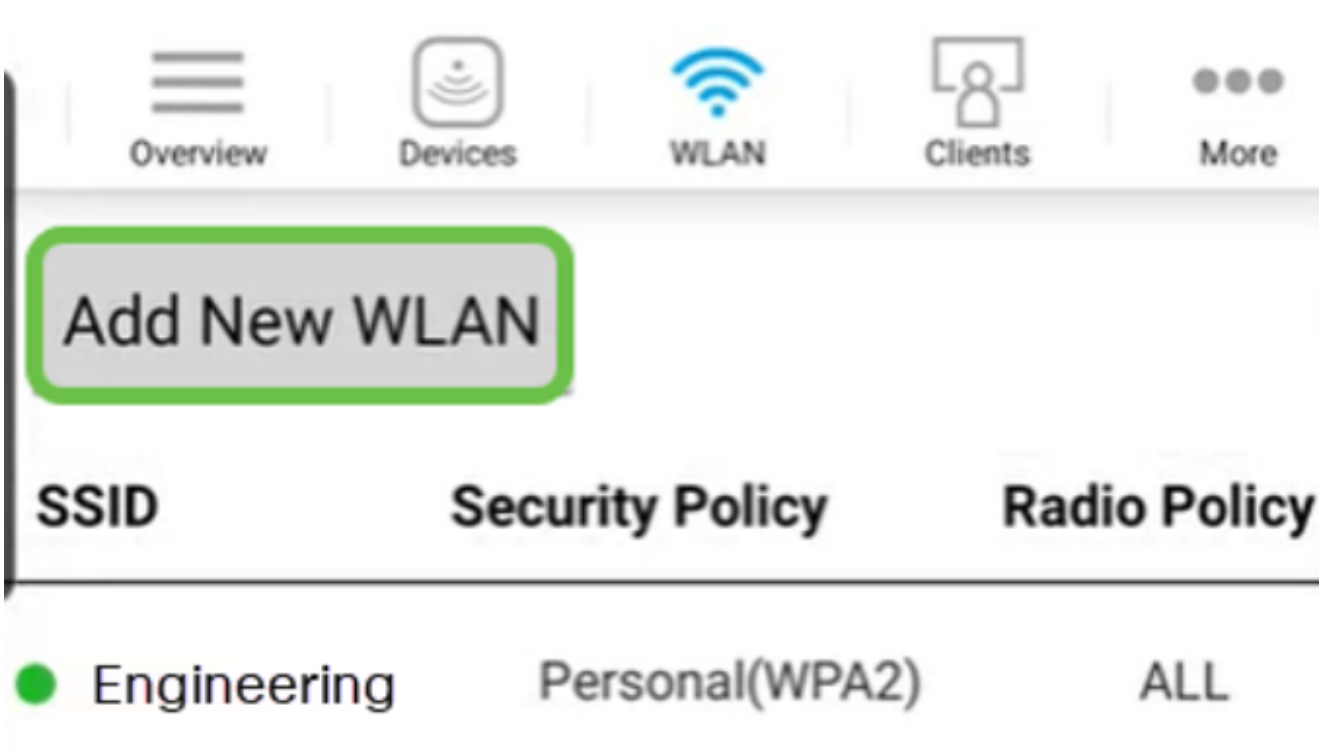
Conecte-se à sua rede sem fio Cisco Business no seu dispositivo móvel. Faça login no

aplicativo. Clique no ícone WLAN na parte superior da página.



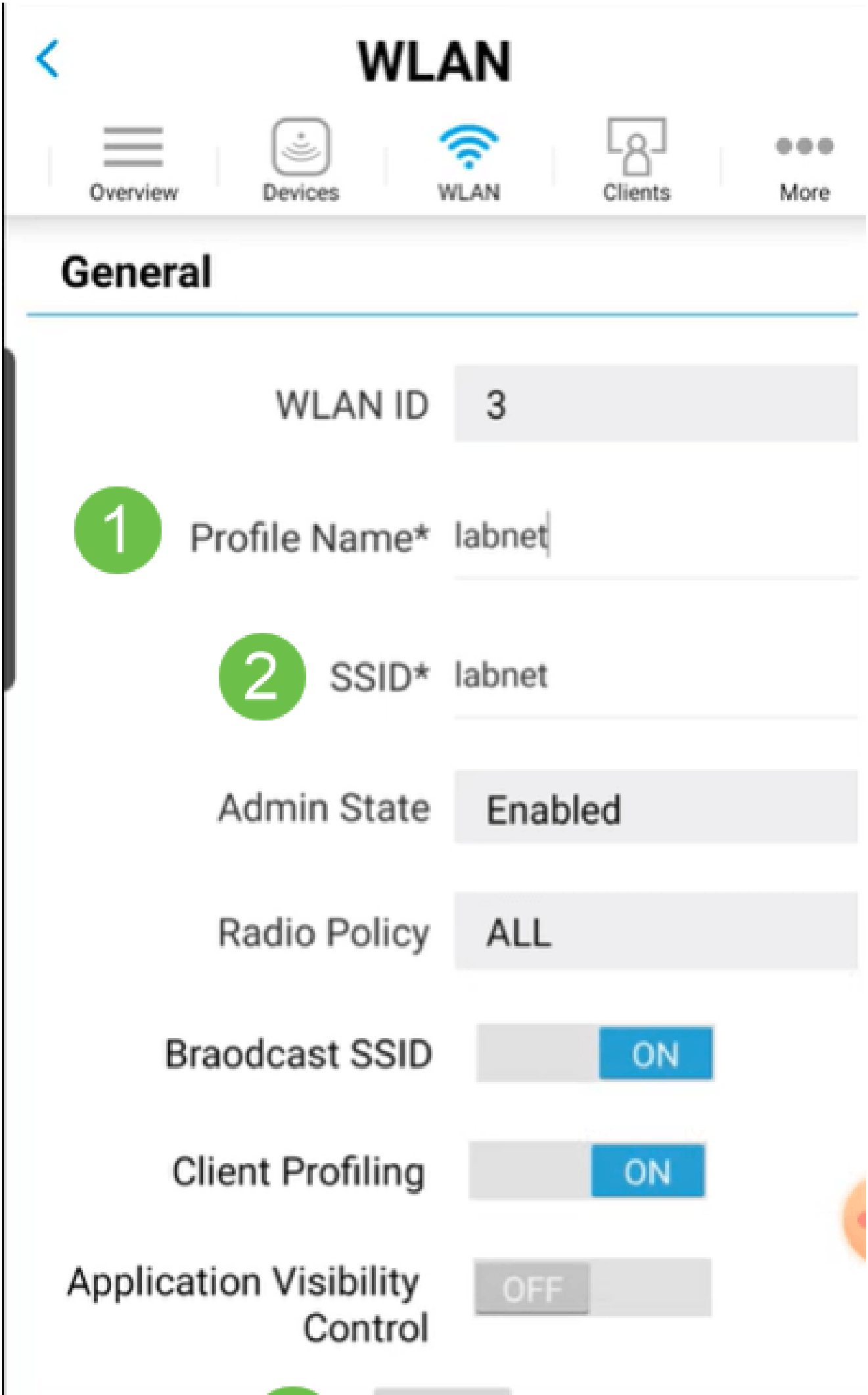
Etapa 3

A tela Add New WLAN é aberta. Você verá as WLANs existentes. Selecione Add New WLAN.



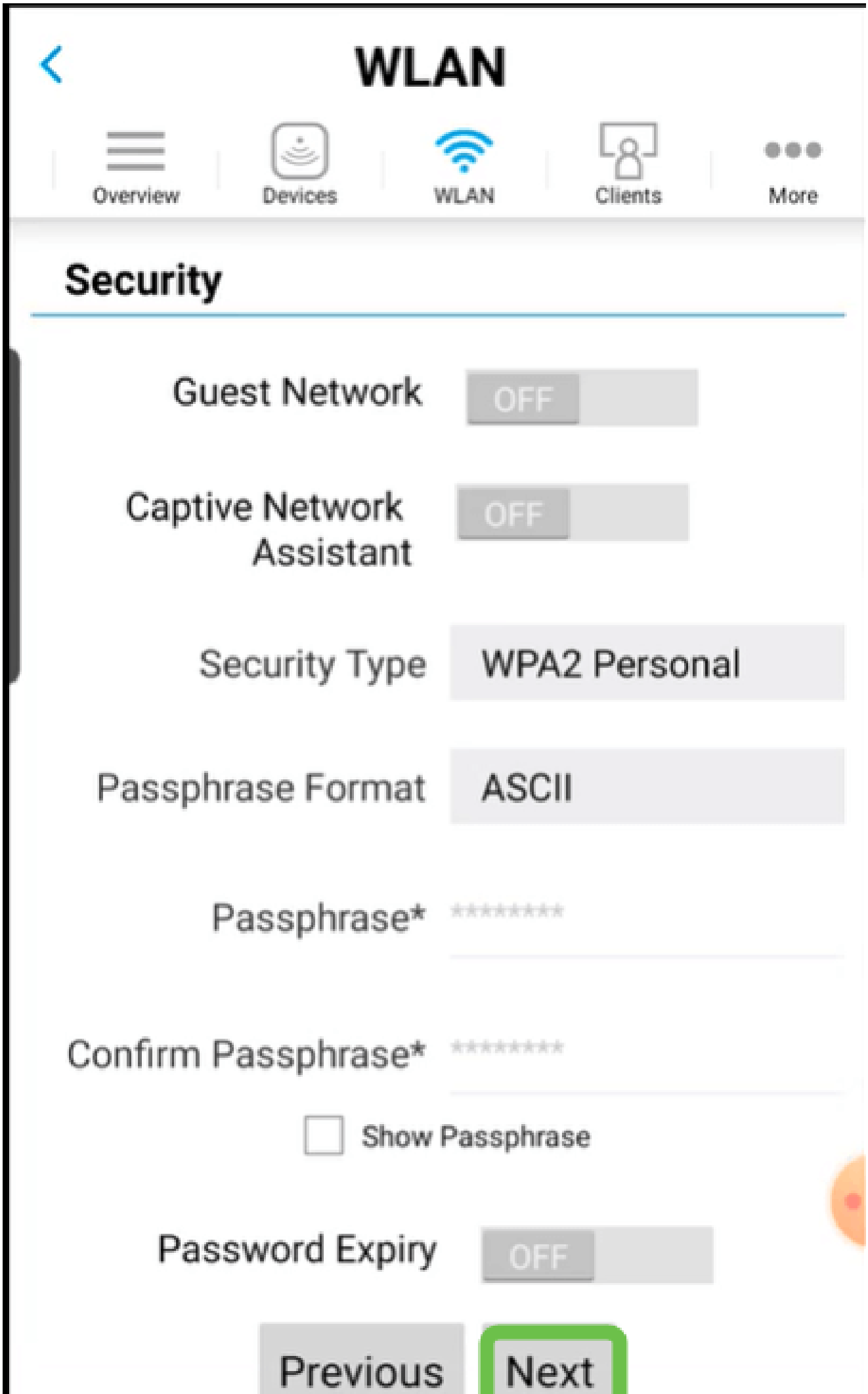
Passo 4

Insira um Profile Name e SSID. Preencha o restante dos campos ou deixe as configurações padrão. Se você ativou o Application Visibility Control, outras configurações serão explicadas na Etapa 6. Clique em Next.


WLAN
Overview
Devices
WLAN
Clients
More
General
WLAN ID
3
1
Profile Name*
labnet
2
SSID*
labnet
Admin State
Enabled
Radio Policy
ALL
Braodcast SSID
ON
Client Profiling
ON
Application Visibility Control
OFF

Etapa 5 (opcional)

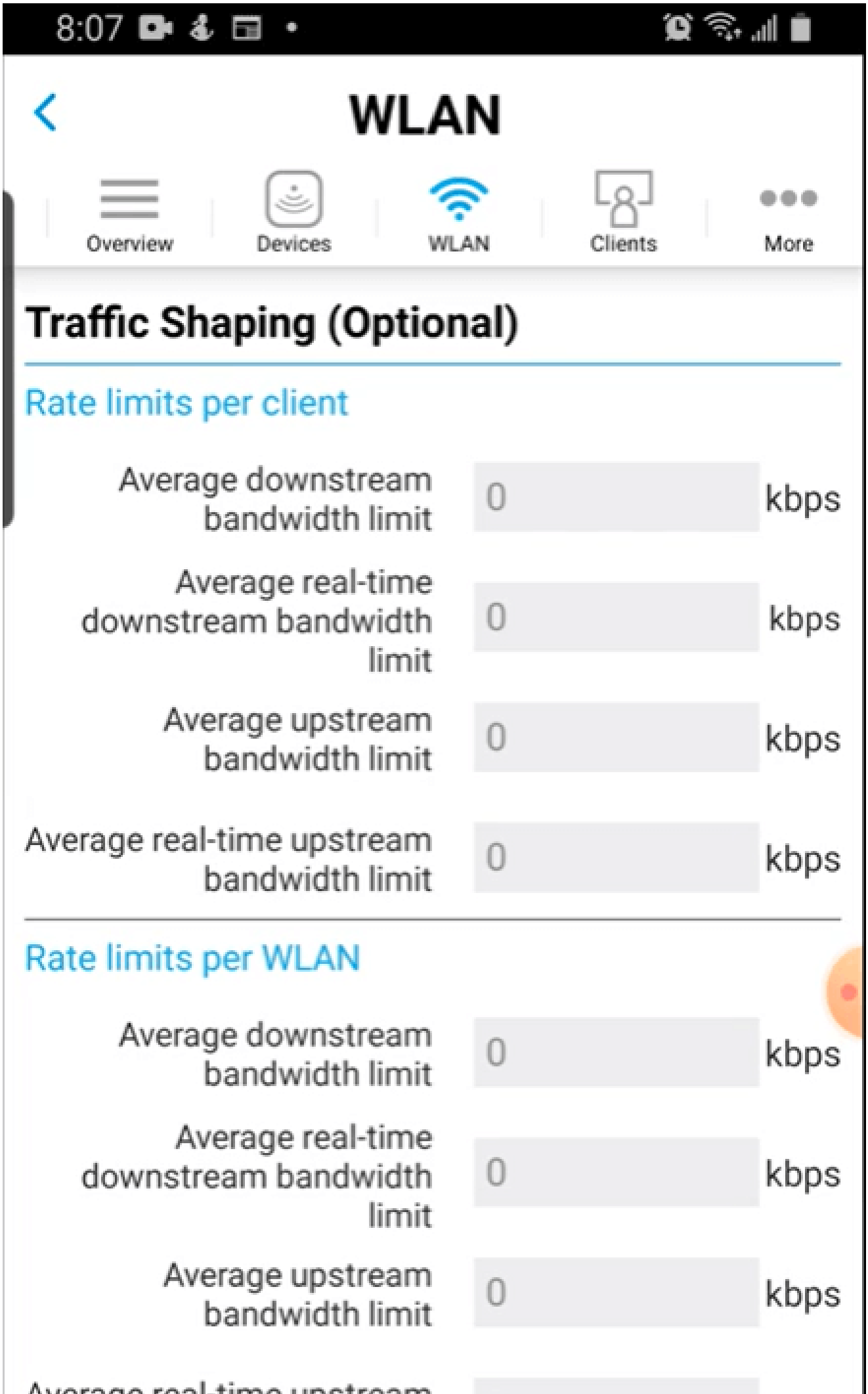
Se você habilitou o Application Visibility Control na etapa 4, poderá definir outras configurações, incluindo uma Guest Network, Os detalhes para isso podem ser encontrados na próxima seção. O Captive Network Assistant, o tipo de segurança, a senha e a expiração de senha também podem ser adicionados aqui. Depois de adicionar todas as configurações, clique em Avançar.


WLAN
Overview
Devices
WLAN
Clients
More
Security
Guest Network
OFF
Captive Network Assistant
OFF
Security Type
WPA2 Personal
Passphrase Format
ASCII
Passphrase*
Confirm Passphrase*
Show Passphrase
Password Expiry
OFF
Previous
Next

Ao usar o aplicativo móvel, as únicas opções para Tipo de segurança são Abrir ou WPA2 Personal. Para obter opções mais avançadas, faça login na interface do usuário da Web do AP de aplicativo móvel.

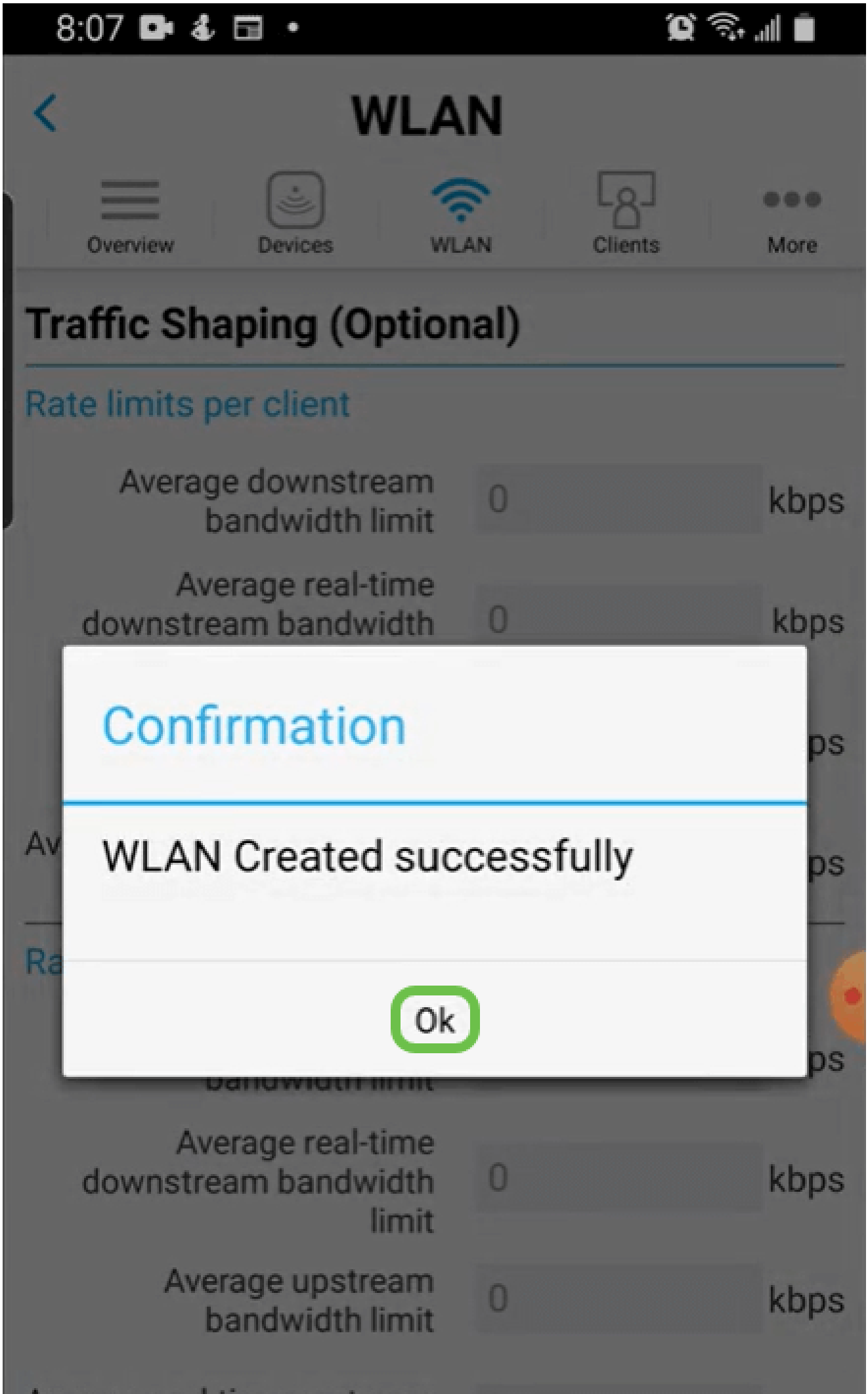
Etapa 6 (opcional)

Esta tela fornece as opções para modelagem de tráfego. Neste exemplo, nenhuma modelagem de tráfego foi configurada. Clique em Submit.


8:07
WLAN
Overview
Devices
WLAN
Clients
More
Traffic Shaping (Optional)
Rate limits per client
Average downstream bandwidth limit
0
kbps
Average real-time downstream bandwidth limit
0
kbps
Average upstream bandwidth limit
0
kbps
Average real-time upstream bandwidth limit
0
kbps
Rate limits per WLAN
Average downstream bandwidth limit
0
kbps
Average real-time downstream bandwidth limit
0
kbps
Average upstream bandwidth limit
0
kbps

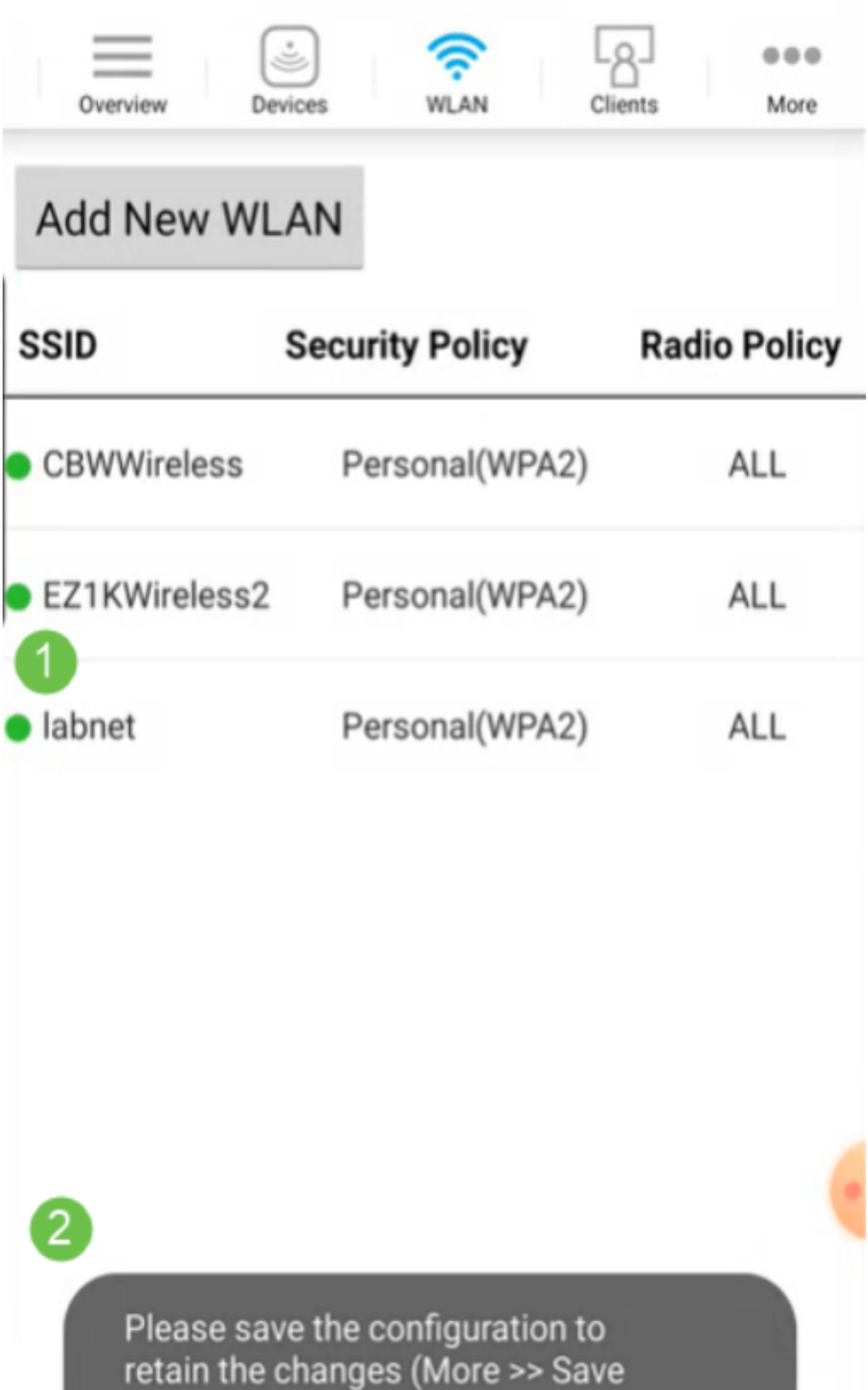
Etapa 7

Você verá um pop-up de confirmação. Click OK.


8:07
WLAN
Overview
Devices
WLAN
Clients
More
Traffic Shaping (Optional)
Rate limits per client
Average downstream bandwidth limit
0
kbps
Average real-time downstream bandwidth
0
kbps
Confirmation
WLAN Created successfully
Ok
Average real-time downstream bandwidth limit
0
kbps
Average upstream bandwidth limit
0
kbps

Passo 8

Você verá a Nova WLAN adicionada à rede, bem como um lembrete para salvar a configuração.


Overview
Devices
WLAN
Clients
More
Add New WLAN
SSID
Security Policy
Radio Policy
CBWWireless
Personal(WPA2)
ALL
EZ1KWireless2
Personal(WPA2)
ALL
1
labnet
Personal(WPA2)
ALL
2
Please save the configuration to
retain the changes (More >> Save

Passo 9

Salve sua configuração clicando na guia More e, em seguida, selecione Save Configuration no menu suspenso.

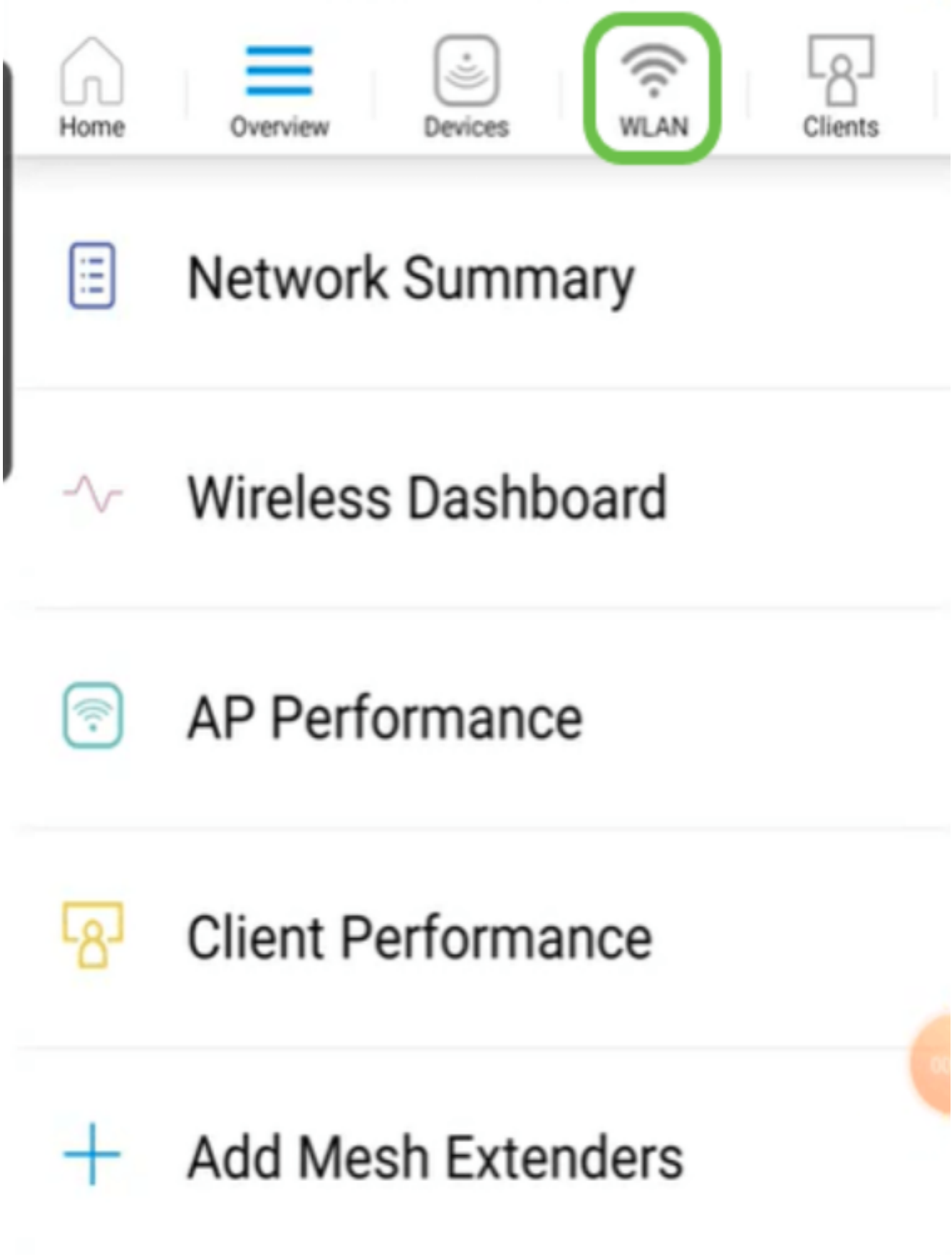
Crie uma Guest WLAN usando o aplicativo móvel

Passo 1

Conecte-se à sua rede sem fio Cisco Business em seu dispositivo móvel. Faça login no aplicativo.

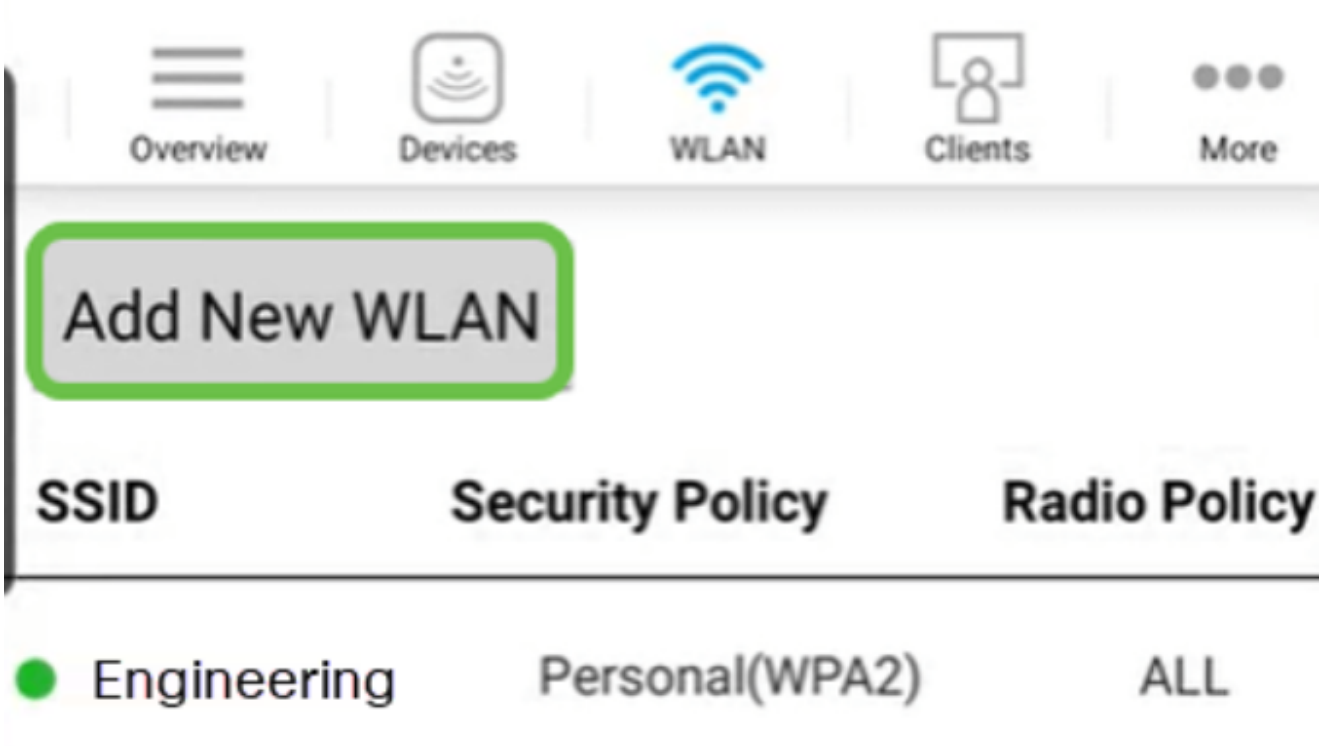
Passo 2

Clique no ícone WLAN na parte superior da página.



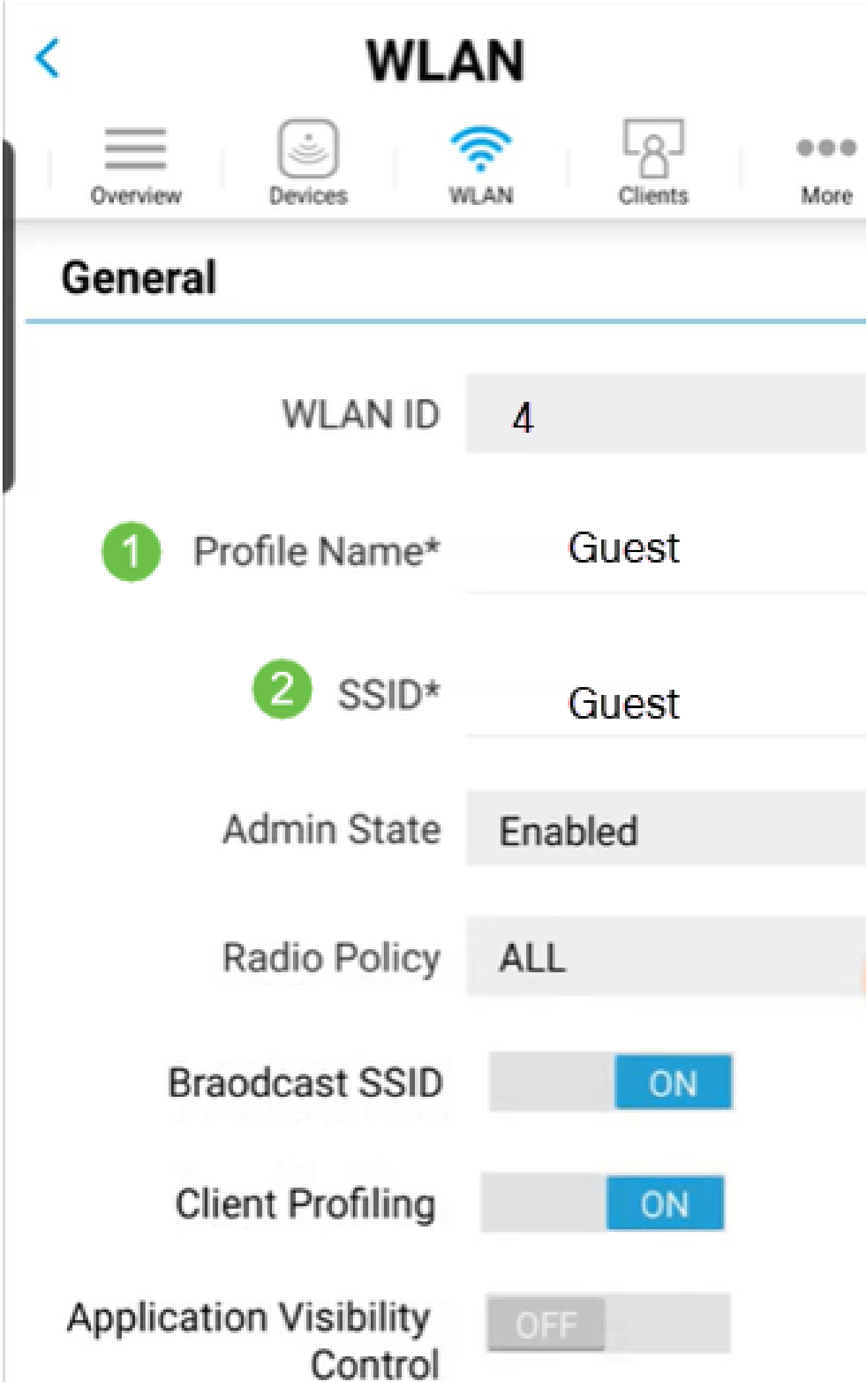
Etapa 3

A tela Add New WLAN é aberta. Você verá todas as WLANs existentes. Selecione Add New WLAN.



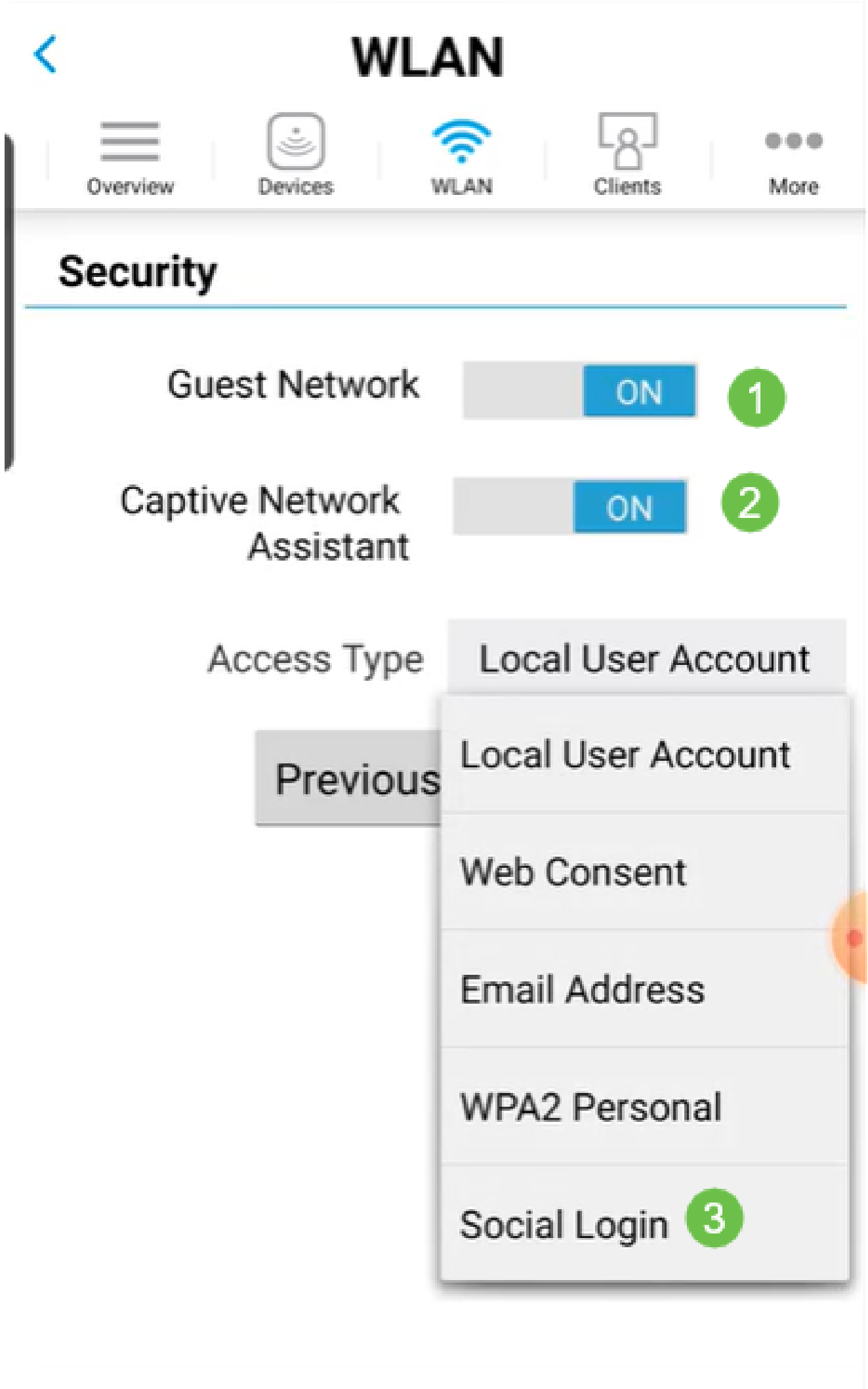
Passo 4

Insira um Profile Name e SSID. Preencha o restante dos campos ou deixe as configurações padrão. Clique em Next.


WLAN
Overview
Devices
WLAN
Clients
More
General
WLAN ID
4
1
Profile Name*
Guest
2
SSID*
Guest
Admin State
Enabled
Radio Policy
ALL
Braodcast SSID
ON
Client Profiling
ON
Application Visibility Control
OFF

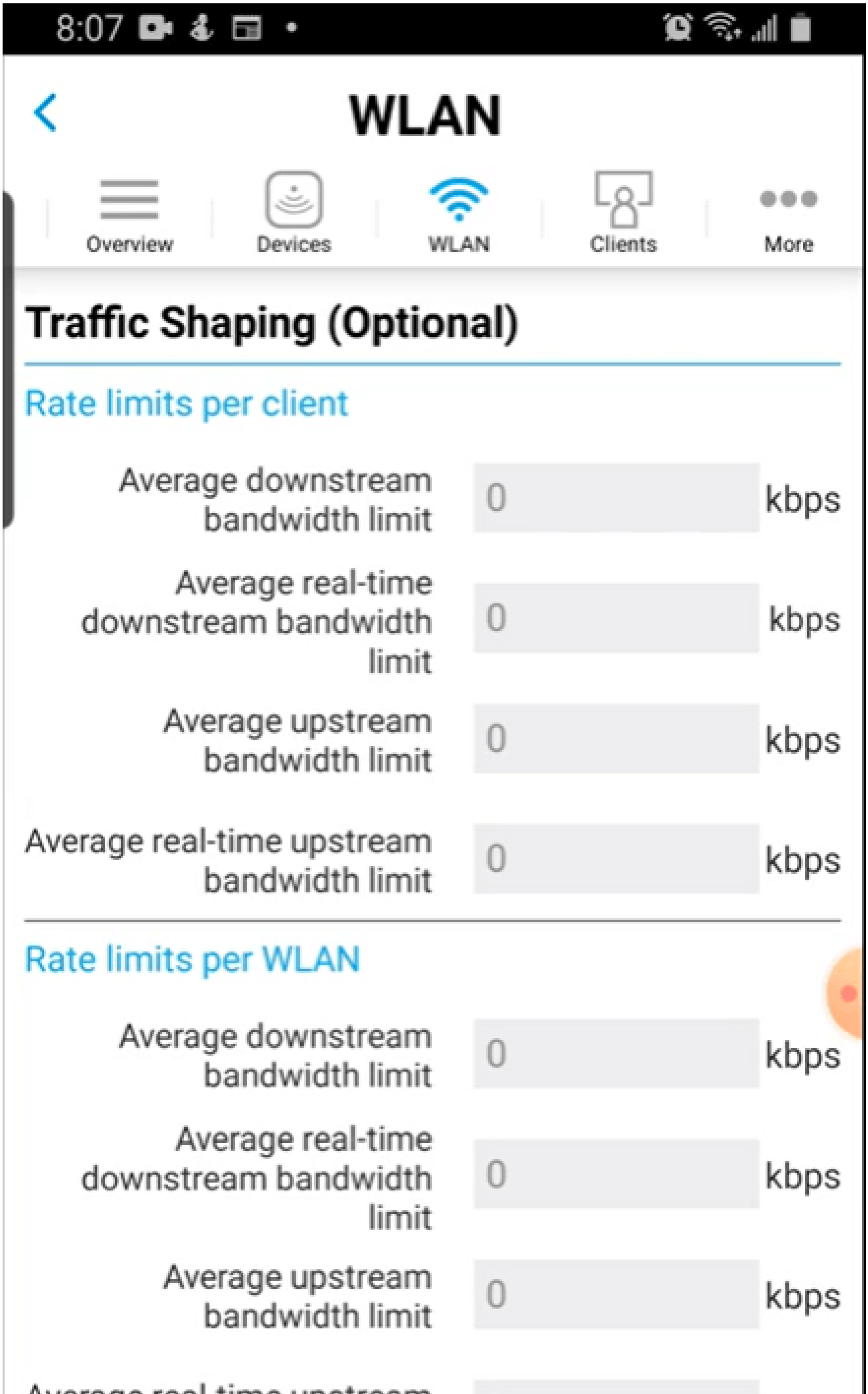
Etapa 5

Ative a rede de convidado. Neste exemplo, o Captive Network Assistant também está ativado, mas isso é opcional. Você tem opções para Tipo de acesso. Nesse caso, Social Login é selecionado.


WLAN
Overview
Devices
WLAN
Clients
More
Security
Guest Network
ON
1
Captive Network Assistant
ON
2
Access Type
Local User Account
Previous
Local User Account
Web Consent
Email Address
WPA2 Personal
Social Login
3

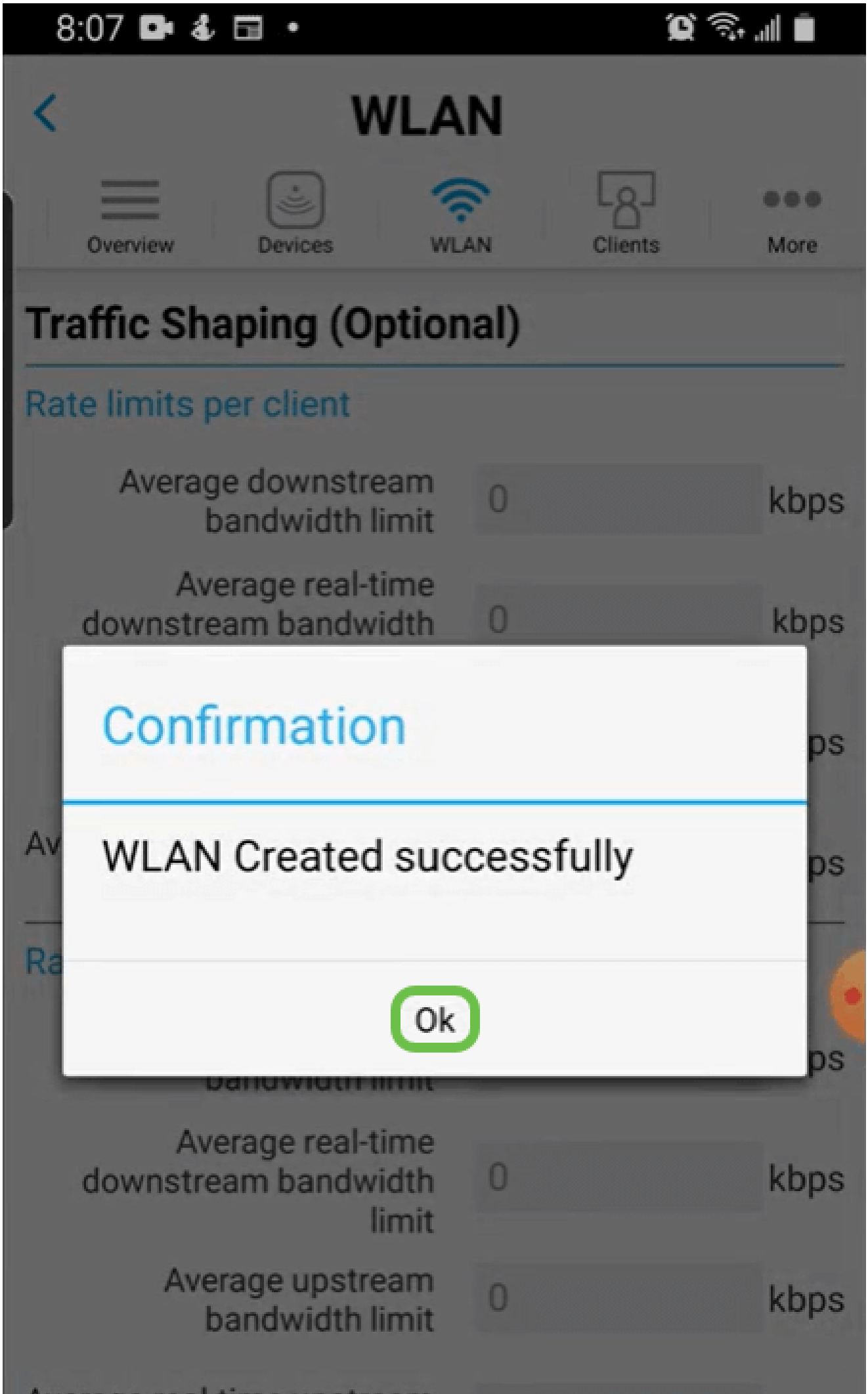
Etapa 6

Esta tela fornece as opções para modelagem de tráfego (opcional). Neste exemplo, nenhuma modelagem de tráfego foi configurada. Clique em Submit.


8:07
WLAN
Overview
Devices
WLAN
Clients
More
Traffic Shaping (Optional)
Rate limits per client
Average downstream bandwidth limit
0
kbps
Average real-time downstream bandwidth limit
0
kbps
Average upstream bandwidth limit
0
kbps
Average real-time upstream bandwidth limit
0
kbps
Rate limits per WLAN
Average downstream bandwidth limit
0
kbps
Average real-time downstream bandwidth limit
0
kbps
Average upstream bandwidth limit
0
kbps

Etapa 7

Você verá um pop-up de confirmação. Click OK.


8:07
WLAN
Overview
Devices
WLAN
Clients
More
Traffic Shaping (Optional)
Rate limits per client
Average downstream bandwidth limit
0
kbps
Average real-time downstream bandwidth
0
kbps
Confirmation
WLAN Created successfully
Ok
Average real-time downstream bandwidth limit
0
kbps
Average upstream bandwidth limit
0
kbps

Passo 8

Salve sua configuração clicando na guia More e, em seguida, selecione Save Configuration no menu suspenso.

Conclusão

Agora você tem uma configuração completa para sua rede. Tire um minuto para comemorar e depois comece a trabalhar!

Se quiser adicionar a Criação de perfil de aplicativos ou a Criação de perfil de cliente à sua rede de malha sem fio, use a Interface de usuário da Web (UI). Clique para configurar esses recursos.

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

Se quiser ler outros artigos e documentação, confira as páginas de suporte do seu hardware:

- Roteador VPN Cisco RV345P com PoE
- Access point Cisco Business 140AC
- Extensor em malha Cisco Business 142ACM

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

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

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