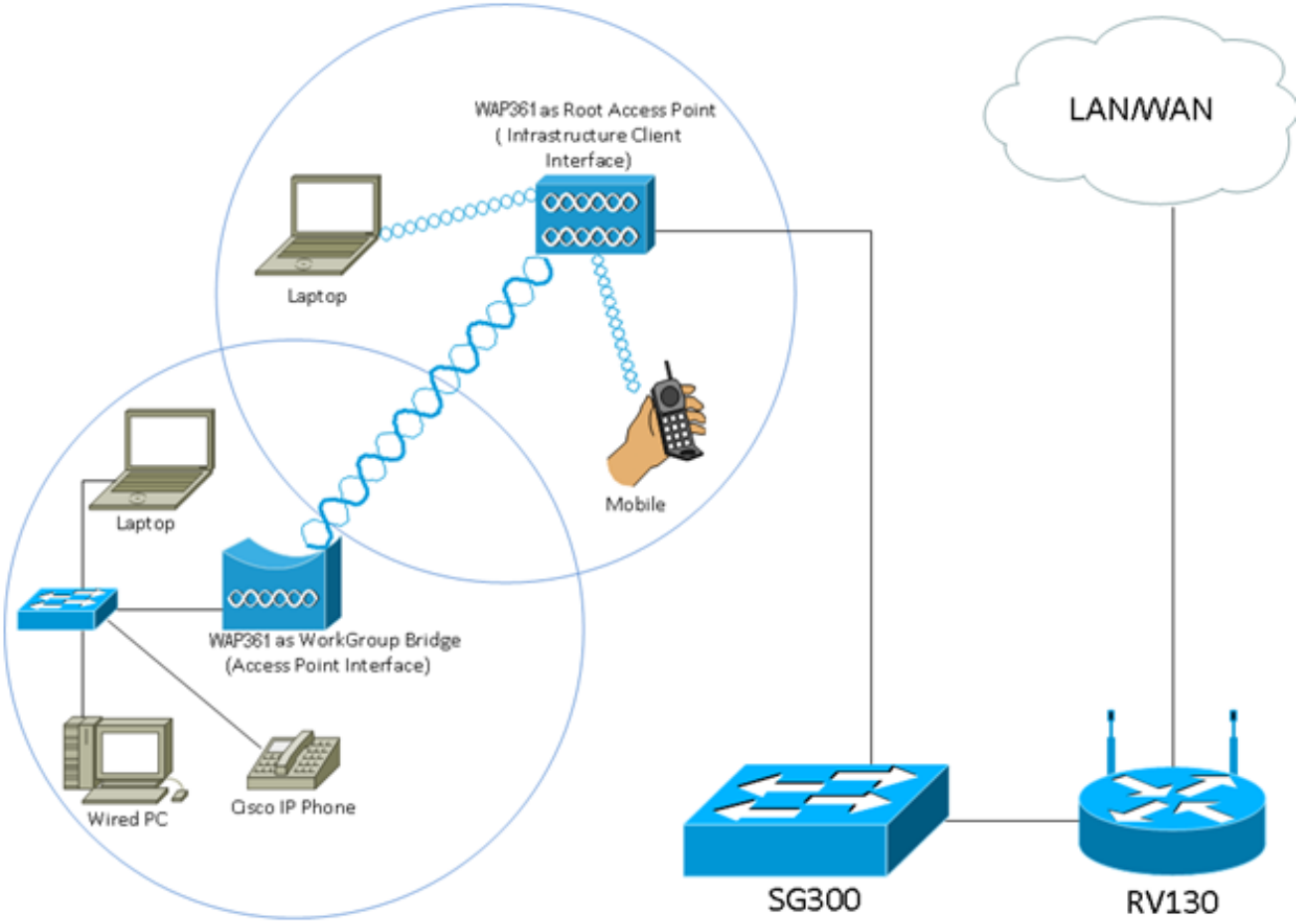
Configurar a ligação de grupo de trabalho em um ponto de acesso sem fio (WAP)

Objetivo

O recurso WorkGroup Bridge permite que o Ponto de Acesso Sem Fio (WAP - Wireless Access Point) faça a ponte do tráfego entre um cliente remoto e a LAN (Local Area Network) sem fio conectada ao Modo de Bridge do Grupo de Trabalho. O dispositivo WAP associado à interface remota é conhecido como uma interface de ponto de acesso, enquanto o dispositivo WAP associado à LAN sem fio é conhecido como uma interface de infraestrutura. A ligação de grupo de trabalho permite que os dispositivos que têm ligações com fios se conectem a uma rede sem fios. O modo de bridge para grupo de trabalho é recomendado como uma alternativa quando o recurso Wireless Distribution System (WDS) não está disponível.



Note: A topologia acima ilustra um exemplo de modelo de ligação de grupo de trabalho. Os dispositivos com fio são ligados a um switch, que se conecta à interface LAN do WAP. O WAP atua como uma interface de ponto de acesso, conecta-se à interface de infraestrutura.

O objetivo deste artigo é mostrar a você como configurar a ponte do grupo de trabalho entre dois WAPs.

Dispositivos aplicáveis

- WAP100 Series

- WAP300 Series
- WAP500 Series

Versão de software

- 1.0.0.17 —WAP571, WAP571E
- 1.0.1.7 — WAP150, WAP361
- 1.0.2.5 — WAP131, WAP351
- 1.0.6.5 — WAP121, WAP321
- 1.2.1.3 — WAP551, WAP561
- 1.3.0.3 — WAP371

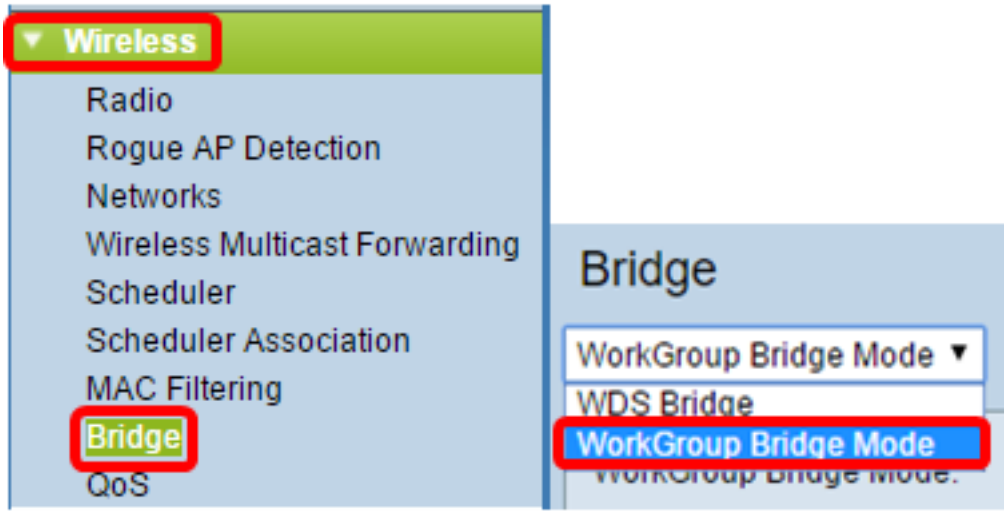
Configurar ligação de grupo de trabalho

Interface do cliente de infraestrutura

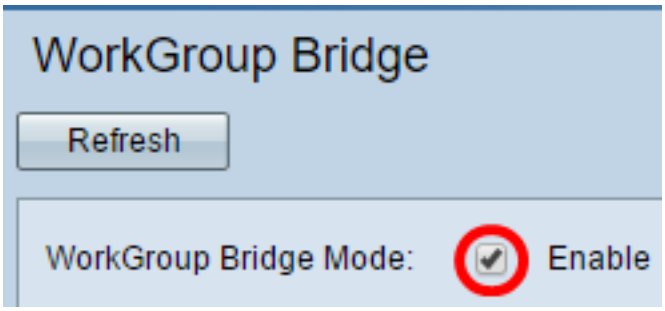
Etapa 1. Faça login no utilitário baseado na Web do WAPe escolha **Wireless > WorkGroup Bridge**.

Note: As opções do menu podem variar dependendo do modelo do dispositivo que você está usando. As imagens abaixo são obtidas do WAP361, a menos que indicado de outra forma.

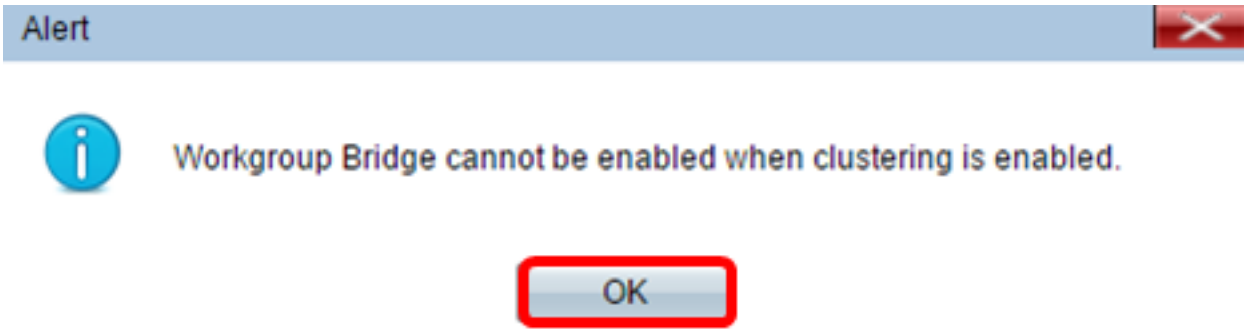
Para WAP571 e WAP571E, escolha **Wireless > Bridge > WorkGroup Bridge Mode**.



Etapa 2. Marque a caixa de seleção **Enable** WorkGroup Bridge Mode.

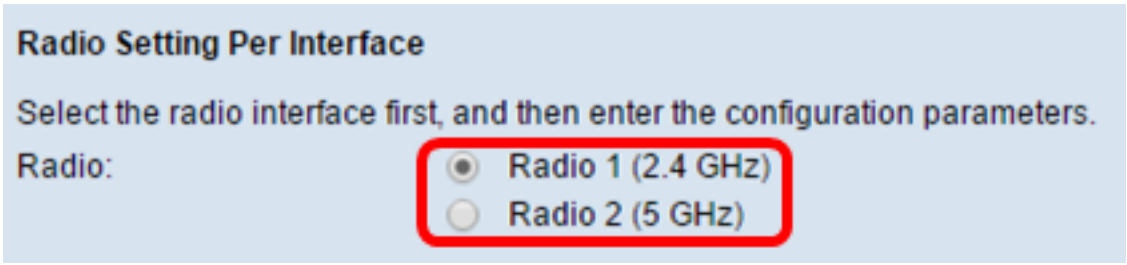


Note: Se o clustering estiver habilitado no WAP, um pop-up notificará você para desativar o clustering para que a ligação do grupo de trabalho funcione. Clique em OK para continuar. Para desabilitar o clustering, escolha **Configuração de ponto único** no painel de navegação e escolha **Pontos de acesso > Desabilitar configuração de ponto único**.



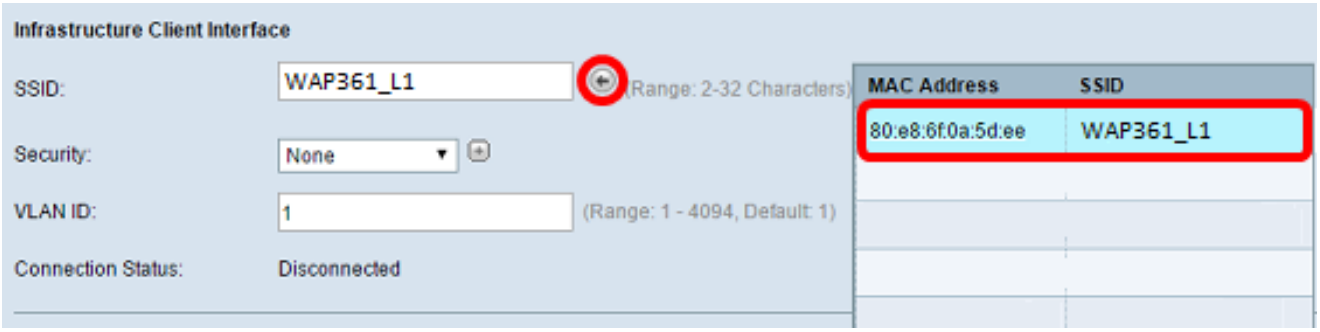
Etapa 3. Clique na interface de rádio para a ligação do grupo de trabalho. Quando você configura um rádio como uma ligação de grupo de trabalho, o outro rádio permanece operacional. As interfaces de rádio correspondem às bandas de radiofreqüência do WAP. O WAP está equipado para transmitir em duas interfaces de rádio diferentes. A definição das configurações de uma interface de rádio não afetará a outra. As opções de interface de rádio podem variar dependendo do modelo WAP. Alguns WAPs mostram o rádio 1 como 2,4 GHz, enquanto outros têm o rádio 2 como 2,4 GHz.

Note: Esta etapa é apenas para os seguintes WAPs com banda dupla: WAP131, WAP150, WAP351, WAP361, WAP371, WAP561, WAP571, WAP571E. Para este exemplo, a opção Radio 1 é escolhida.



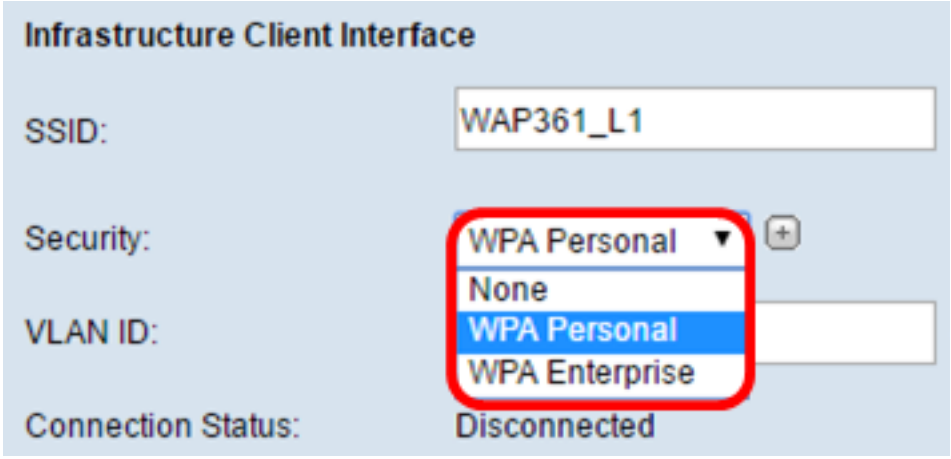
Etapa 4. Insira o nome do SSID (Service Set Identifier, Identificador do conjunto de serviços) no campo *SSID* ou clique no botão de seta ao lado do campo para procurar vizinhos. Isso serve como a conexão entre o dispositivo e o cliente remoto. Você pode digitar de 2 a 32 caracteres para o SSID do cliente de infraestrutura.

Note: É importante habilitar a detecção de AP não autorizado. Para saber mais sobre como habilitar o recurso, clique aqui. Para este exemplo, o botão de seta é clicado para escolher WAP361_L1 como o SSID da interface do cliente de infraestrutura.



Etapa 5. Na área Interface do cliente de infraestrutura, escolha o tipo de segurança para autenticar como uma estação cliente no dispositivo WAP de upstream na lista suspensa Segurança. As opções são:

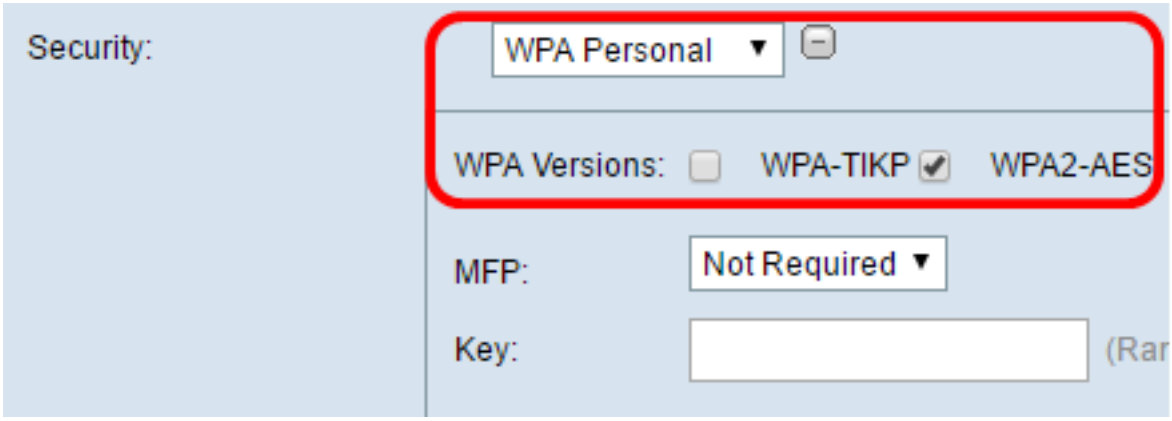
- Nenhum — Aberto ou sem segurança. Esse é o padrão. Se isso for escolhido, vá para a Etapa 18.
- WPA Personal — A WPA Personal pode suportar chaves com 8 a 63 caracteres. A WPA2 é recomendada porque tem um padrão de criptografia mais potente. Vá para a Etapa 6 para configurar.
- WPA Enterprise — A WPA Enterprise é mais avançada que a WPA Personal e é a segurança recomendada para autenticação. Usa o PEAP (Protected Extensible Authentication Protocol) e o TLS (Transport Layer Security). Vá para a Etapa 9 para configurar. Esse tipo de segurança é frequentemente usado em um ambiente de escritório e precisa de um servidor RADIUS (Remote Authentication Dial-In User Service) configurado. Clique aqui para saber mais sobre os servidores RADIUS.



Note: Neste exemplo, a WPA Personal é escolhida.

Etapa 6. Clique no botão **+** e marque a caixa de seleção WPA-TKIP ou WPA2-AES para determinar que tipo de criptografia WPA a interface do cliente de infraestrutura usará.

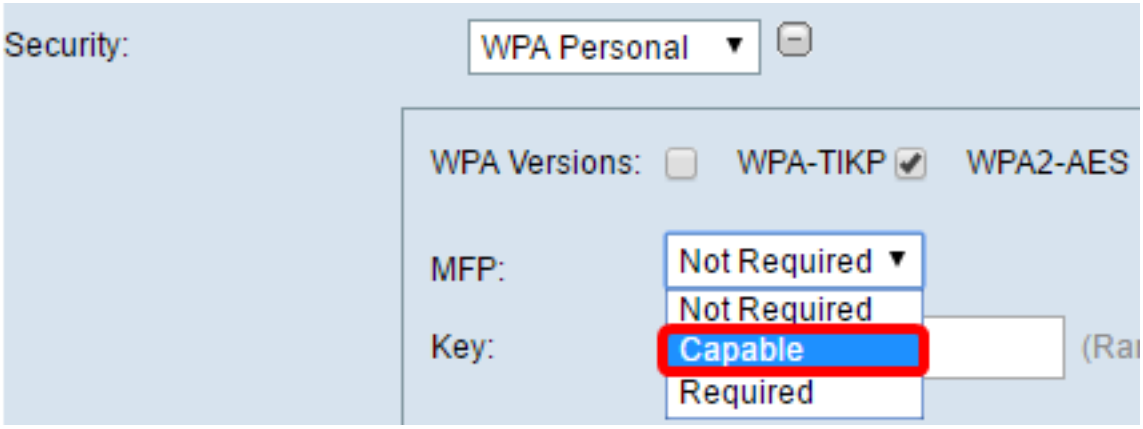
Note: Se todos os seus equipamentos sem fio oferecerem suporte a WPA2, defina a segurança do cliente da infraestrutura como WPA2-AES. O método de criptografia é RC4 para WPA e AES (Advanced Encryption Standard) para WPA2. A WPA2 é recomendada porque tem um padrão de criptografia mais potente. Para este exemplo, WPA2-AES é usado.



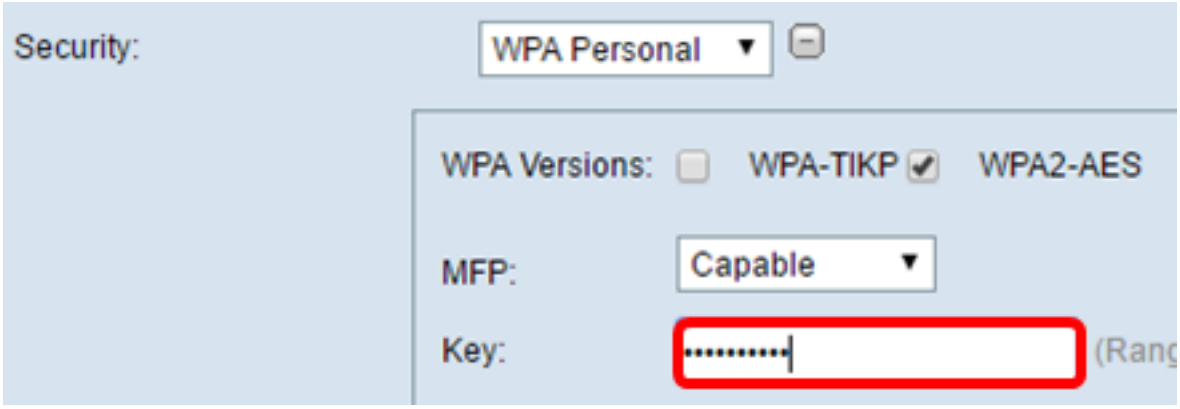
Passo 7. (Opcional) Se você marcou o WPA2-AES na Etapa 6, escolha uma opção na lista suspensa Proteção de Quadro de Gerenciamento (MFP) se deseja que o WAP exija quadros protegidos ou não. Para saber mais sobre o MFP, clique aqui. As opções são:

- Não obrigatório — Desativa o suporte ao cliente para MFP.
- Capable (Capaz) — Permite que clientes compatíveis com MFP e que não suportam MFP entrem na rede. Essa é a configuração MFP padrão no WAP.
- Obrigatório — Os clientes podem se associar somente se o MFP for negociado. Se os dispositivos não oferecerem suporte a MFP, eles não poderão ingressar na rede.

Note: Para este exemplo, Capable é escolhido.



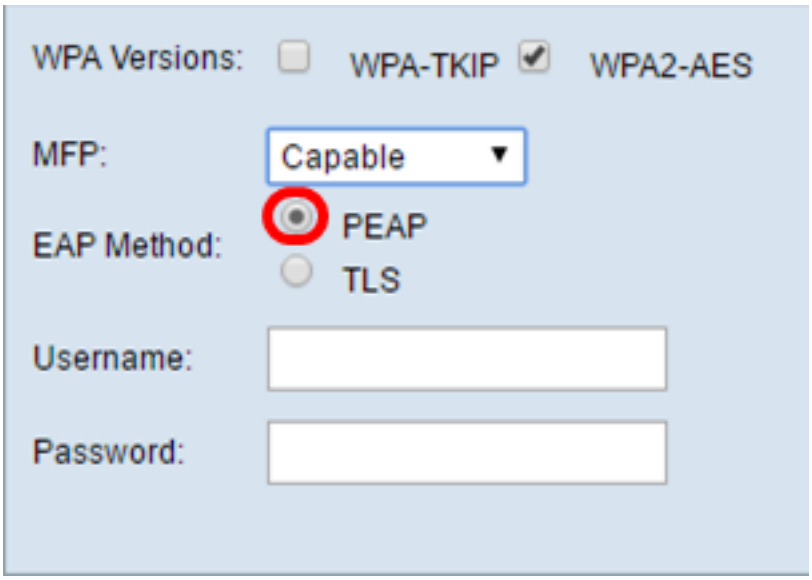
Etapa 8. Insira a chave de criptografia WPA no campo *Key (Chave)*. A chave deve ter de 8 a 63 caracteres. É uma combinação de letras, números e caracteres especiais. É a senha usada ao conectar-se à rede sem fio pela primeira vez. Então, vá para a Etapa 18.



Etapa 9. Se você escolheu WPA Enterprise na Etapa 5, clique em um botão de opção para o Método EAP.

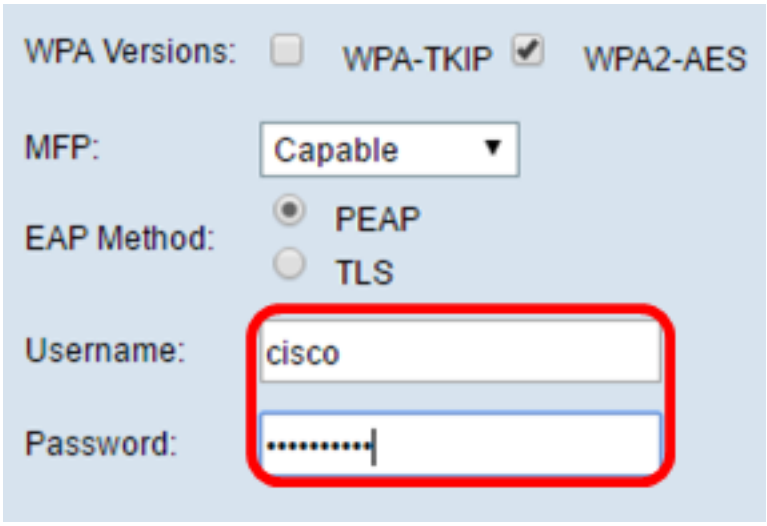
As opções disponíveis são definidas da seguinte forma:

- PEAP — Este protocolo fornece a cada usuário sem fio nomes de usuário e senhas individuais WAP que suportam padrões de criptografia AES. Como o PEAP é um método de segurança baseado em senha, a segurança Wi-Fi baseia-se nas credenciais do dispositivo do cliente. O PEAP pode representar um risco de segurança potencialmente grave se você tiver senhas fracas ou clientes não protegidos. Ele depende do TLS, mas evita a instalação de certificados digitais em todos os clientes. Em vez disso, ele fornece autenticação através de um nome de usuário e senha.
- TLS — O TLS exige que cada usuário tenha um certificado adicional para ter acesso. O TLS é mais seguro se você tiver os servidores adicionais e a infraestrutura necessária para autenticar usuários na sua rede.



Note: Para este exemplo, PEAP é escolhido.

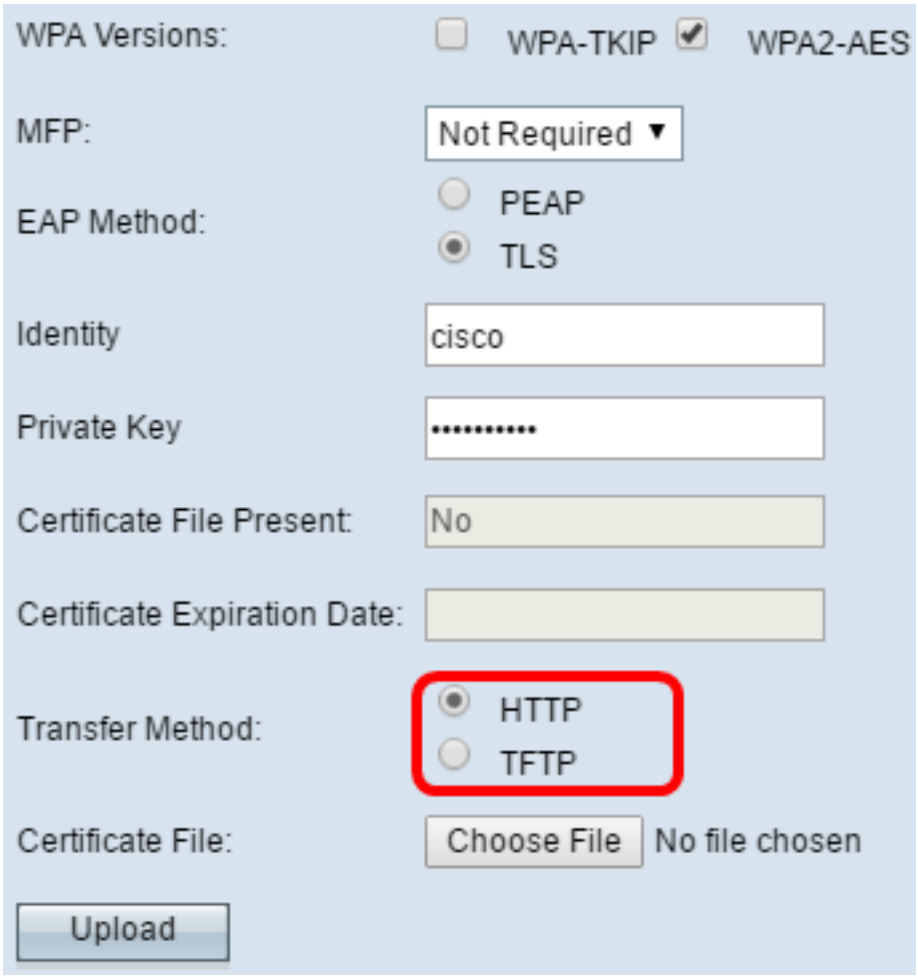
Etapa 10. Insira o nome de usuário e a senha do cliente de infraestrutura nos campos *Nome de usuário* e *Senha*. Essas são as informações de login usadas para conectar-se à interface do cliente da infraestrutura; consulte a interface do seu cliente de infraestrutura para encontrar essas informações. Então, vá para a Etapa 18.



Etapa 11. Se você clicou em TLS na Etapa 9, insira a identidade e a chave privada do cliente de infraestrutura nos campos *Identidade* e *Chave Privada*.

Etapa 12. Na área do método de transferência, clique em um botão de opção das seguintes opções:

- TFTP — O TFTP (Trivial File Transfer Protocol) é uma versão simplificada e não segura do FTP. É usado principalmente para distribuir software ou autenticar dispositivos entre redes corporativas. Se você clicou em TFTP, vá para a Etapa 15.
- HTTP — O HTTP (Hypertext Transfer Protocol) fornece uma estrutura de autenticação de desafio-resposta simples que pode ser usada por um cliente para fornecer a estrutura de autenticação.

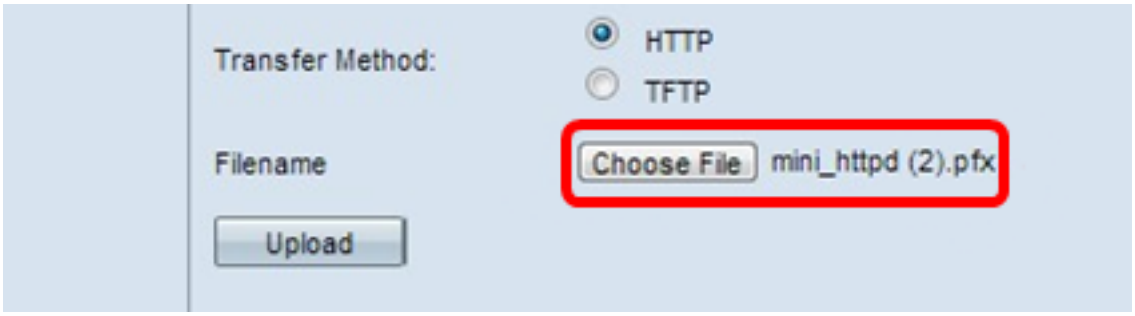


Observação: se um arquivo de certificado já estiver presente no WAP, os campos *Arquivo de certificado presente* e *Data de expiração do certificado* já serão preenchidos com as informações relevantes. Caso contrário, estarão em branco.

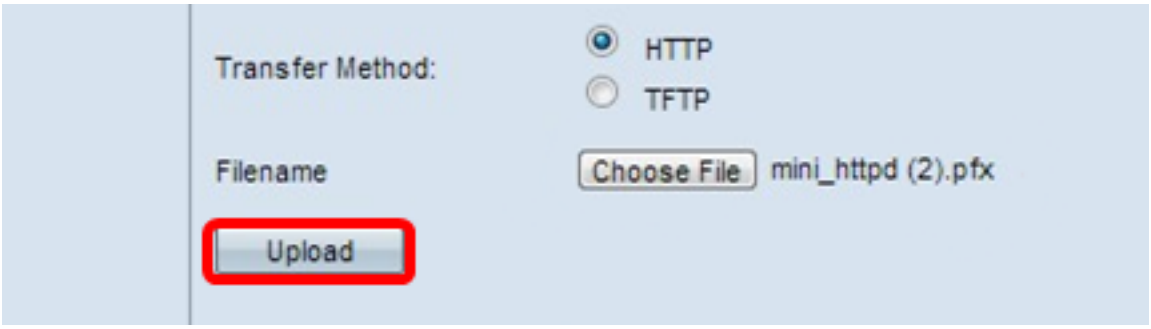
HTTP

Etapa 13. Clique no botão **Escolher arquivo** para localizar e selecionar um arquivo de certificado. O arquivo deve ter a extensão de arquivo de certificado adequada (como .pem ou .pfx); caso contrário, o arquivo não será aceito.

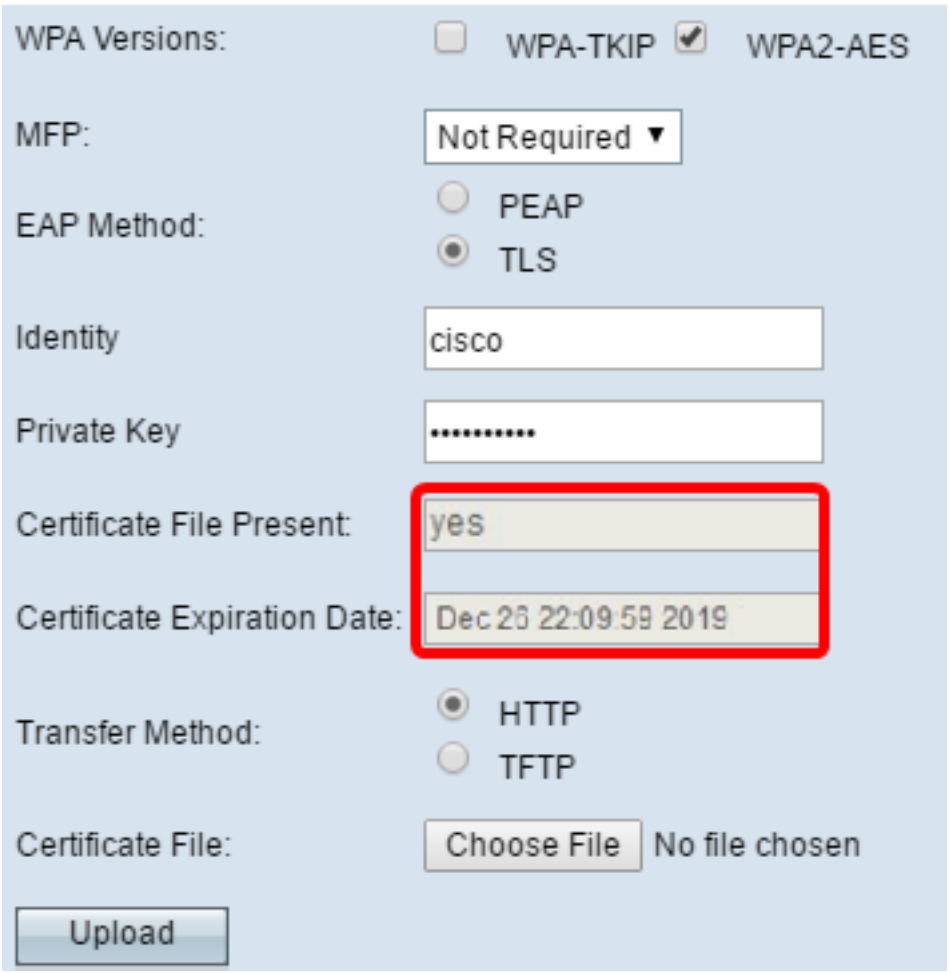
Note: Neste exemplo, mini_httpd(2).pfx é escolhido.



Etapa 14. Clique em **Carregar** para carregar o arquivo de certificado selecionado. Vá para a Etapa 18.



Os campos *Arquivo de certificado presente* e *Data de expiração do certificado* serão atualizados automaticamente.



TFTP

Etapa 15. Se você clicou em TFTP na Etapa 12, insira o nome do arquivo de certificado no campo *Nome do arquivo*.

Note: Neste exemplo, mini_httpd.pem é usado.

Etapa 16. Insira o endereço do servidor TFTP no campo *Endereço IPv4 do servidor TFTP*.

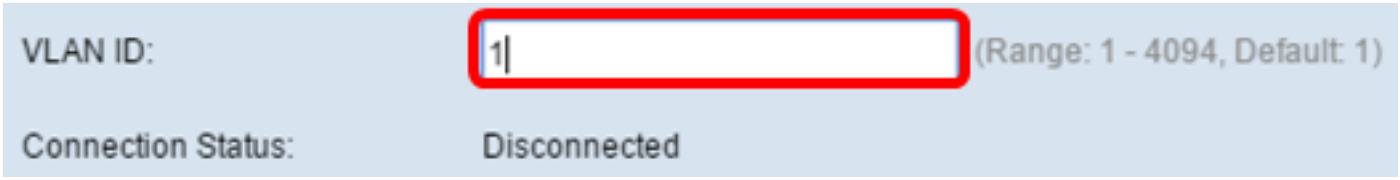
Note: Neste exemplo. 192.168.1.20 é usado como o endereço do servidor TFTP.

Etapa 17. Clique no botão **Carregar** para carregar o arquivo de certificado especificado.

Os campos *Arquivo de certificado presente* e *Data de expiração do certificado* serão atualizados automaticamente.

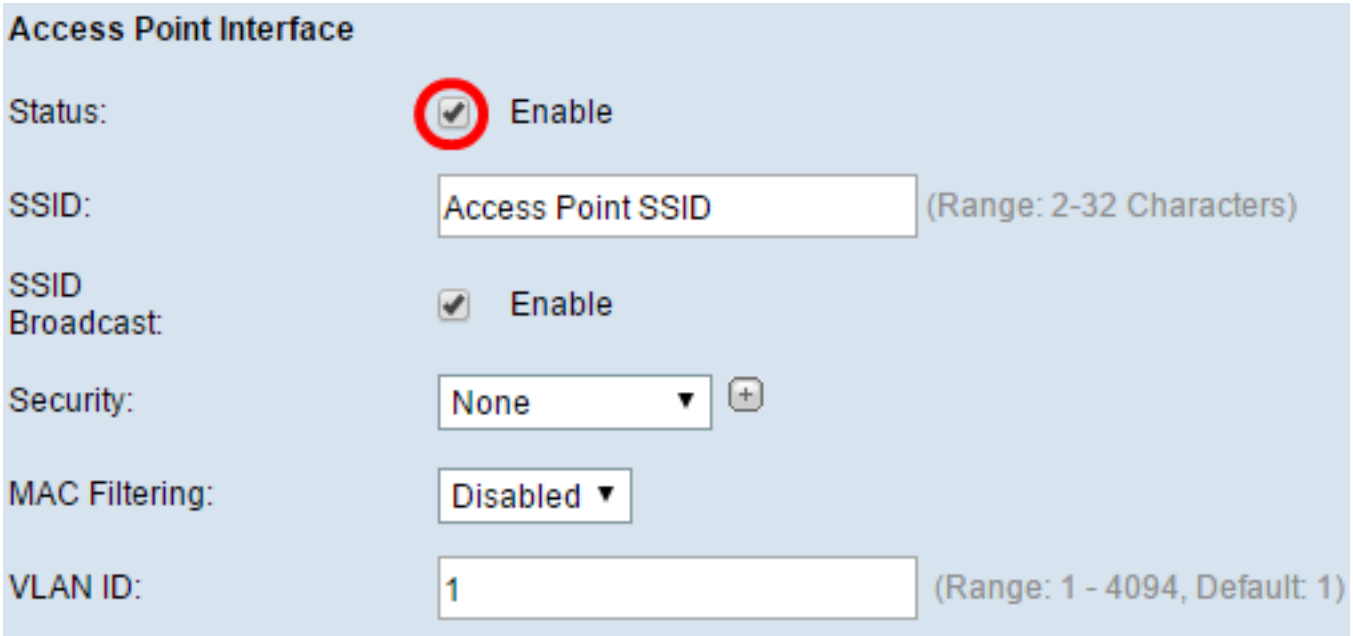
Etapa 18. Digite a ID da VLAN para a interface do cliente de infraestrutura. O padrão é 1.

Note: Para este exemplo, o ID de VLAN padrão é usado.



Interface do ponto de acesso

Etapa 1. Marque a caixa de seleção **Enable** Status para habilitar o Bridging na interface do ponto de acesso.

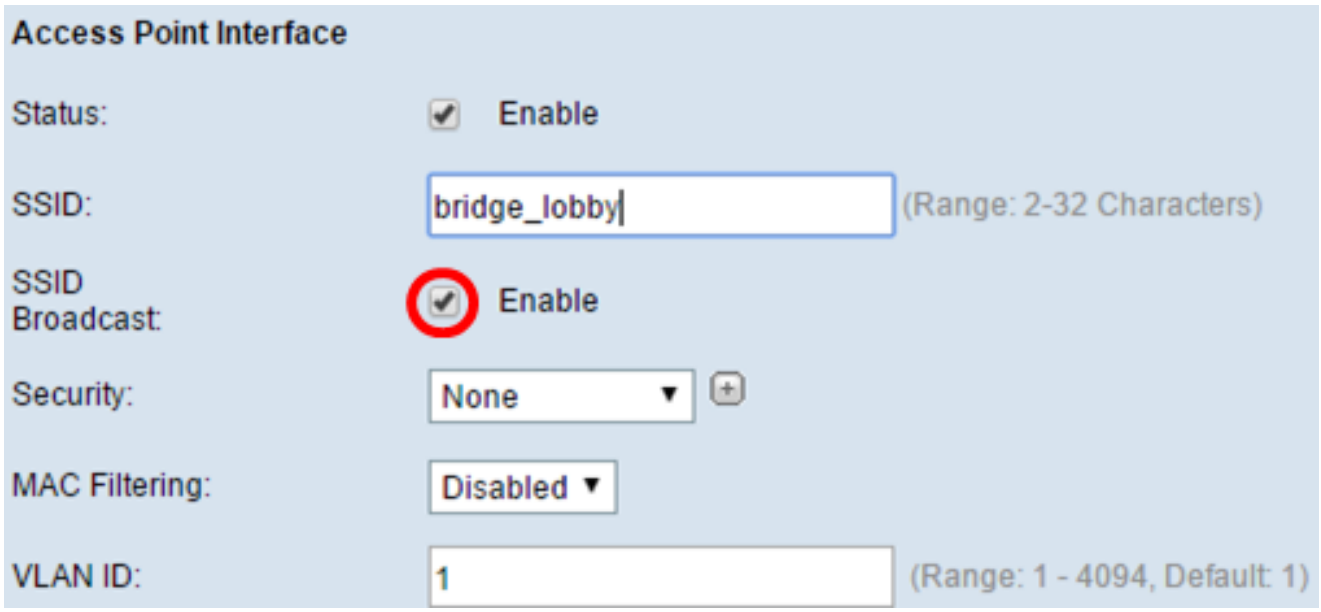


Etapa 2. Digite o SSID do ponto de acesso no campo *SSID*. O comprimento do SSID deve

estar entre 2 e 32 caracteres. O padrão é Access Point SSID.

Note: Para este exemplo, o SSID usado é bridge_lobby.

Etapa 3. (Opcional) Se você não quiser transmitir o SSID, desmarque a caixa de seleção **Habilitar** transmissão de SSID. Ao fazê-lo, o ponto de acesso ficará invisível aos que procuram pontos de acesso sem fios; ele só pode ser conectado por alguém que já conhece o SSID. SSID Broadcast (Transmissão de SSID) está ativado por padrão.

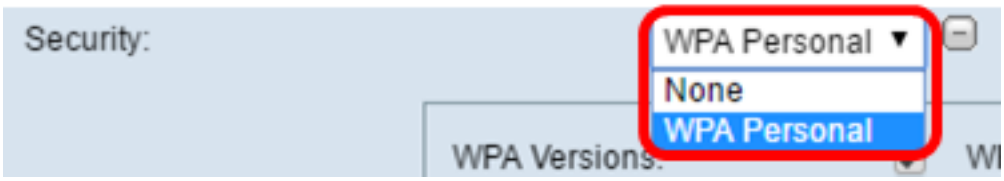


Etapa 4. Escolha o tipo de segurança para autenticar estações clientes downstream para o WAP na lista suspensa Segurança.

As opções disponíveis são definidas da seguinte forma:

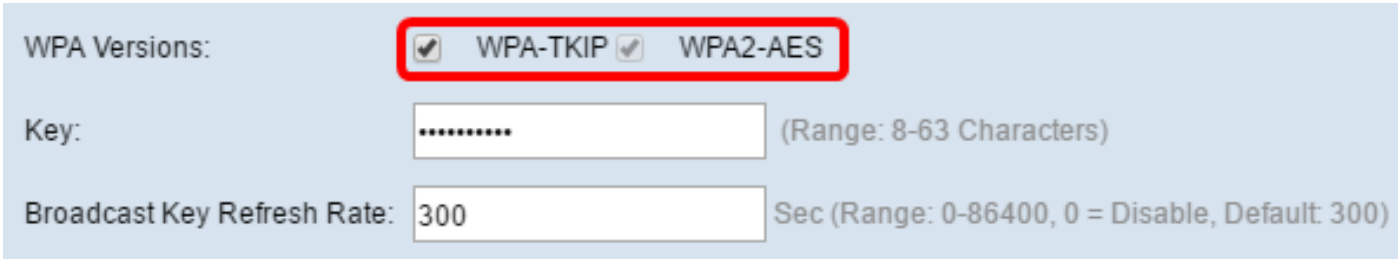
- Nenhum — Aberto ou sem segurança. Este é o valor padrão. Vá para a Etapa 10 se você escolher esta opção.
- WPA Personal — A WPA (Wi-Fi Protected Access) Personal pode suportar chaves com 8 a 63 caracteres. O método de criptografia é TKIP ou Counter Cipher Mode com Block Chaining Message Authentication Code Protocol (CCMP). A WPA2 com CCMP é recomendada porque

tem um padrão de criptografia mais potente, o AES (Advanced Encryption Standard), em comparação com o TKIP (Temporal Key Integrity Protocol) que usa apenas um padrão RC4 de 64 bits.

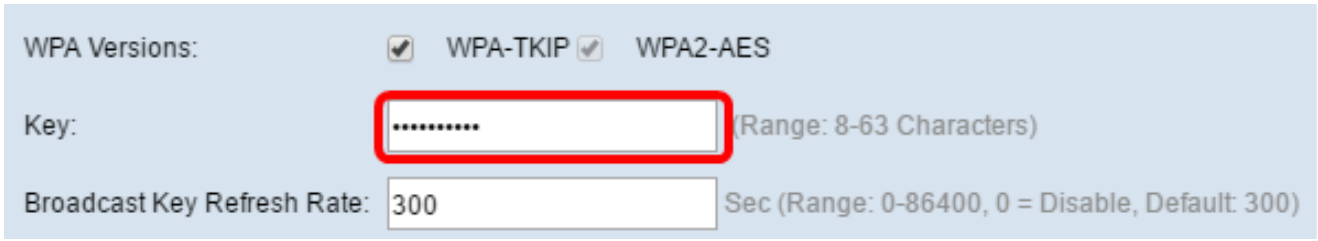


Etapa 5. Marque a caixa de seleção **WPA-TKIP** ou **WPA2-AES** para determinar que tipo de criptografia WPA a interface do ponto de acesso usará. Por padrão, eles são ativados.

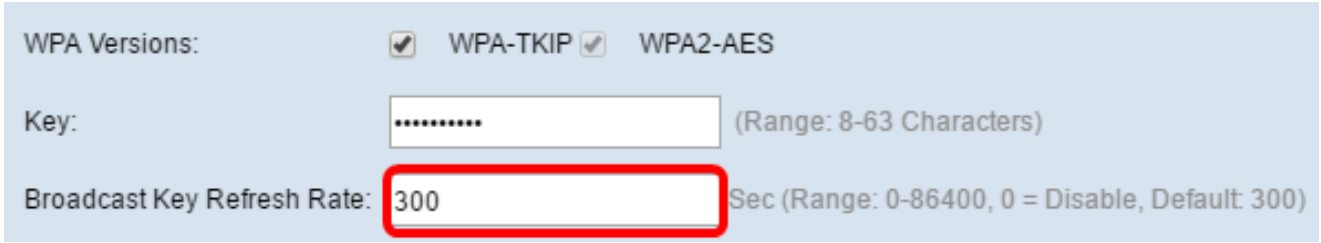
Note: Se todos os seus equipamentos sem fio oferecerem suporte a WPA2, defina a segurança do cliente da infraestrutura como WPA2-AES. O método de criptografia é RC4 para WPA e AES (Advanced Encryption Standard) para WPA2. A WPA2 é recomendada porque tem um padrão de criptografia mais potente. Para este exemplo, WPA2-AES é usado.



Etapa 6. Digite a chave WPA compartilhada no campo *Key*. A chave deve ter de 8 a 63 caracteres e pode incluir caracteres alfanuméricos, letras maiúsculas e minúsculas e caracteres especiais.



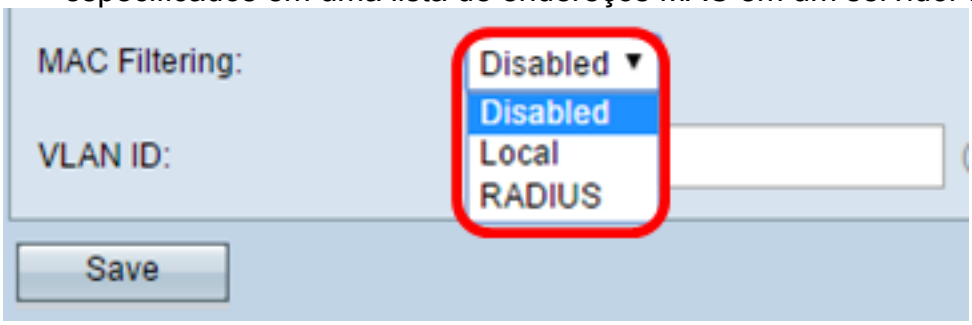
Passo 7. Insira a taxa no campo *Broadcast Key Refresh Rate (Taxa de atualização da chave de transmissão)*. A taxa de atualização da chave de broadcast especifica o intervalo no qual a chave de segurança é atualizada para clientes associados a este ponto de acesso. A taxa deve estar entre 0 e 86400, com um valor 0 desabilitando o recurso. O padrão é 300.



Etapa 8. Escolha o tipo de filtragem MAC que deseja configurar para a interface do ponto de acesso na lista suspensa Filtragem MAC. Quando habilitados, os usuários recebem ou negam acesso ao WAP com base no endereço MAC do cliente que usam.

As opções disponíveis são definidas da seguinte forma:

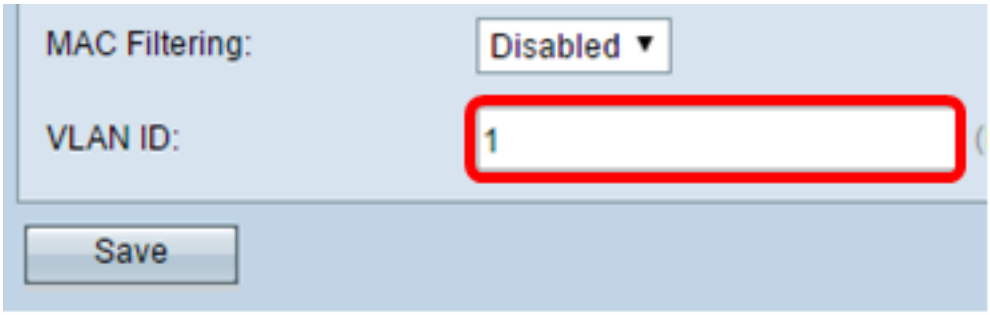
- Desabilitado — Todos os clientes podem acessar a rede upstream. Este é o valor padrão.
- Local — O conjunto de clientes que podem acessar a rede upstream é restrito aos clientes especificados em uma lista de endereços MAC definidos localmente.
- RADIUS — O conjunto de clientes que podem acessar a rede upstream é restrito aos clientes especificados em uma lista de endereços MAC em um servidor RADIUS.



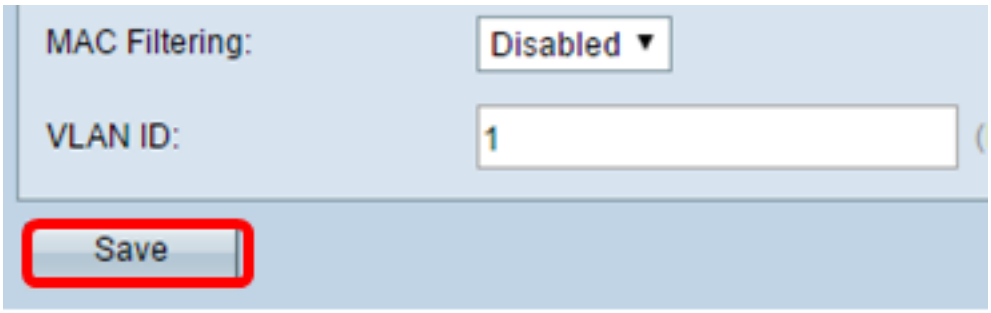
Note: Para este exemplo, Desabilitado é escolhido.

Etapa 9. Digite o ID da VLAN no campo *VLAN ID* para a interface do ponto de acesso.

Observação: para permitir o bridging de pacotes, a configuração da VLAN para a interface do ponto de acesso e a interface com fio deve corresponder à da interface do cliente de infraestrutura.



Etapa 10. Clique em **Salvar** para salvar suas alterações.



Agora você deve ter configurado com êxito uma ligação de grupo de trabalho em um ponto de acesso sem fio.