Definir as configurações de segurança sem fio em um WAP

Introduction

A configuração da segurança sem fio em seu WAP (Wireless Access Point, ponto de acesso sem fio) é altamente essencial para proteger sua rede sem fio de invasores que podem comprometer a privacidade de seus dispositivos sem fio, bem como a transmissão de dados pela rede sem fio. Você pode configurar a segurança sem fio em sua rede sem fio configurando o Filtro MAC, o Acesso Protegido Wi-Fi (WPA/WPA2) Pessoal e a WPA/WPA2 Empresarial.

A filtragem MAC é usada para filtrar os clientes sem fio para acessar a rede usando seus endereços MAC. Uma lista de clientes será configurada para permitir ou bloquear os endereços na lista para acessar a rede, dependendo de sua preferência. Para saber mais sobre a filtragem de MAC, clique aqui.

WPA/WPA2 Personal e WPA/WPA2 Enterprise são protocolos de segurança usados para proteger a privacidade ao criptografar os dados transmitidos pela rede sem fio. WPA/WPA2 é compatível com os padrões IEEE 802.11E e 802.11i. Comparado ao protocolo de segurança WEP (Wired Equivalent Privacy), a WPA/WPA2 melhorou os recursos de autenticação e criptografia.

A WPA/WPA2 Personal é para uso doméstico e a WPA/WPA2 Enterprise é para rede em escala empresarial. A WPA/WPA2 Enterprise oferece maior segurança e controle centralizado sobre a rede em comparação com a WPA/WPA2 Personal.

Neste cenário, a segurança sem fio será configurada no WAP para proteger a rede de invasores usando as configurações WPA/WPA2 Personal e Enterprise.

Objetivo

O objetivo deste artigo é mostrar a você como configurar os protocolos de segurança WPA/WPA2 Personal e Enterprise para melhorar a segurança e a privacidade da sua rede sem fio.

Note: Este artigo pressupõe que um SSID (Service Set Identifier, Identificador do conjunto de serviços) ou uma WLAN (Wireless Local Area Network, Rede local sem fio) já foram criados em seu WAP.

Dispositivos aplicáveis

- WAP100 Series
- WAP300 Series
- WAP500 Series

Versão de software

- 1.0.2.14 - WAP131, WAP351

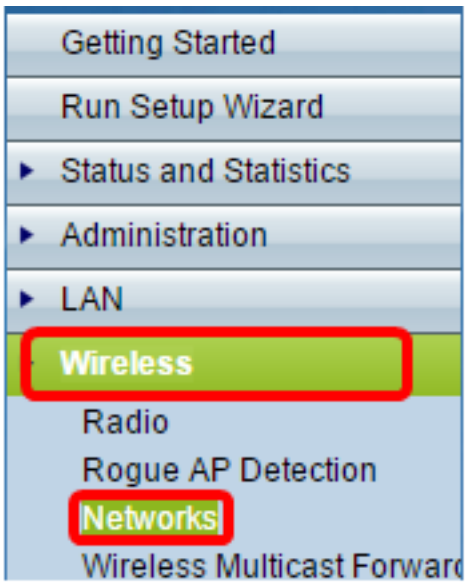
- 1.0.6.5 - WAP121, WAP321
- 1.3.0.4 - WAP371
- 1.1.0.7 - WAP150, WAP361
- 1.2.1.5 - WAP551, WAP561
- 1.0.1.11 - WAP571, WAP571E

Definir configurações de segurança sem fio

Configurar WPA/WPA2 Personal

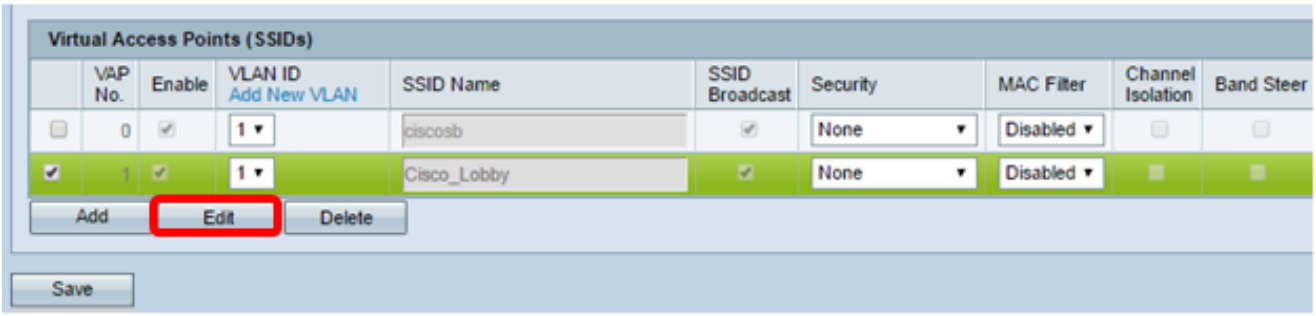
Etapa 1. Efetue login no utilitário baseado na Web do seu ponto de acesso e escolha **Wireless > Networks**.

Note: Na imagem abaixo, o utilitário baseado na Web do WAP361 é usado como exemplo. As opções de menu podem variar dependendo do modelo do dispositivo.

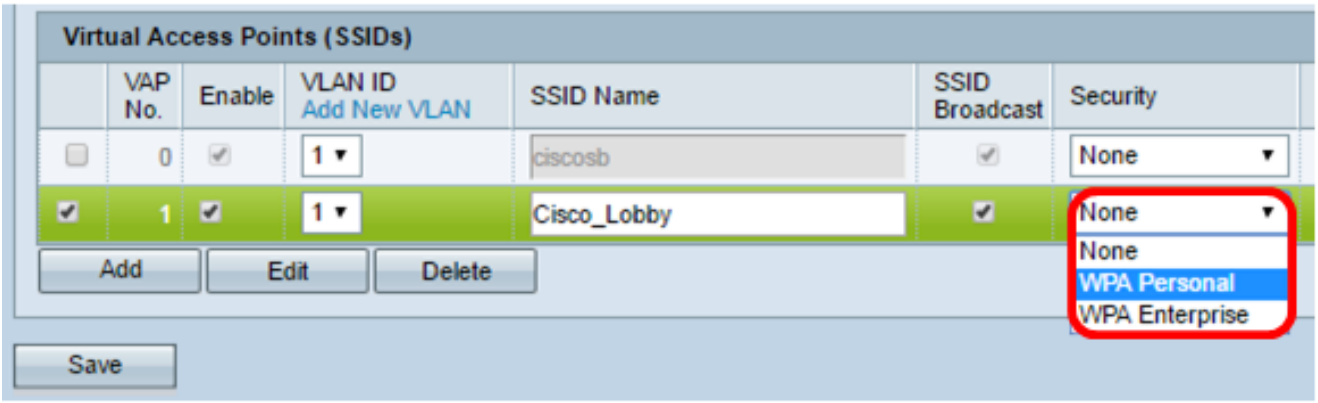


Etapa 2. Na área de Pontos de acesso virtuais (SSIDs), marque a caixa de seleção do SSID que deseja configurar e clique em **Editar**.

Note: Neste exemplo, VAP1 é escolhido.



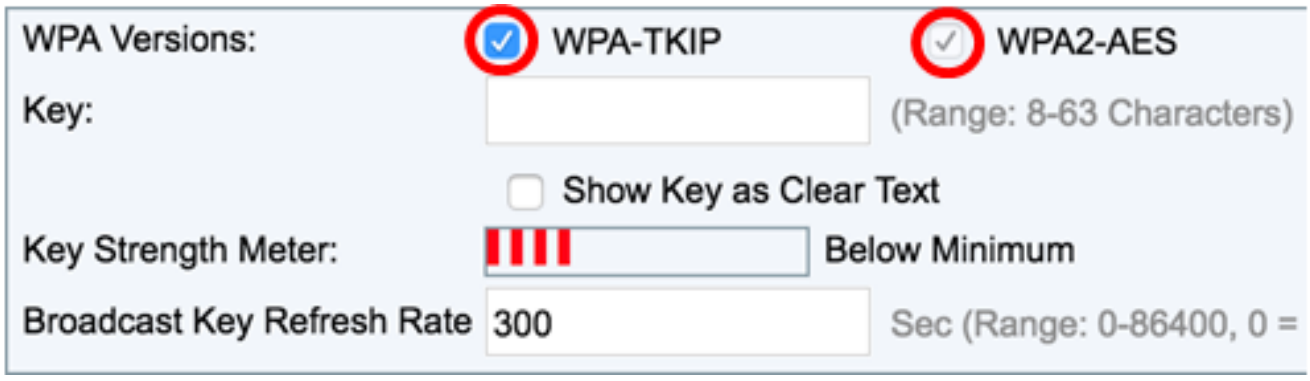
Etapa 3. Clique em **WPA Personal** na lista suspensa Segurança.



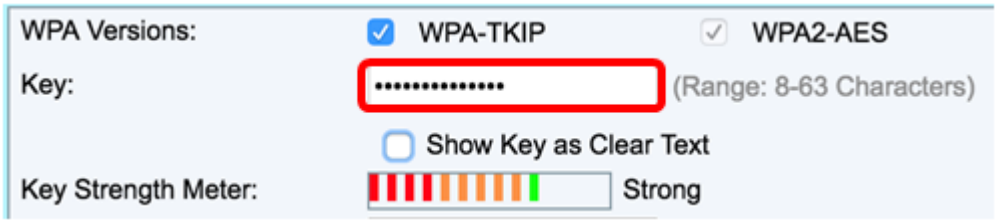
Etapa 4. Escolha a versão WPA (WPA-TKIP ou WPA2-AES) marcando a caixa de seleção. Dois podem ser escolhidos de uma só vez.

- WPA-TKIP — Ferramenta de Integridade da Chave Temporal de Acesso Protegido Wi-Fi. A rede tem algumas estações clientes que suportam apenas o protocolo de segurança WPA e TKIP original. Observe que a escolha somente de WPA-TKIP para access point não é permitida de acordo com o requisito mais recente da Wi-Fi Alliance.
- WPA2-AES — Wi-Fi Protected Access-Advanced Encryption Standard. Todas as estações clientes na rede suportam protocolo de criptografia/segurança WPA2 e AES-CCMP. Esta versão WPA fornece a melhor segurança de acordo com o padrão IEEE 802.11i. De acordo com o requisito mais recente da Wi-Fi Alliance, o WAP tem de suportar este modo o tempo todo.

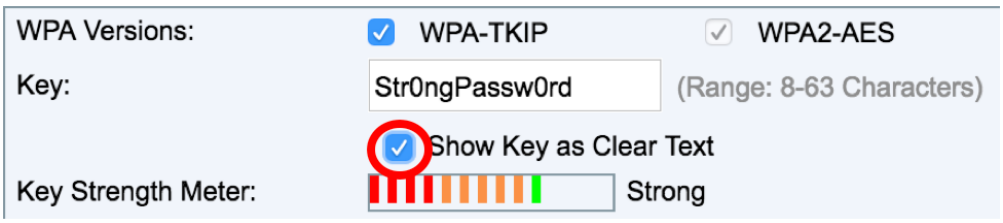
Note: Para este exemplo, ambas as caixas de seleção estão marcadas.



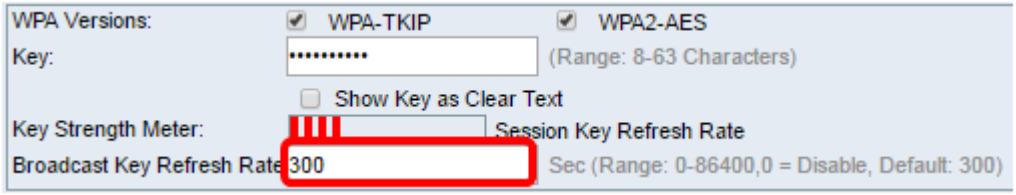
Etapa 5. Crie uma senha com 8 a 63 caracteres e insira-a no campo *Key (Chave)*.



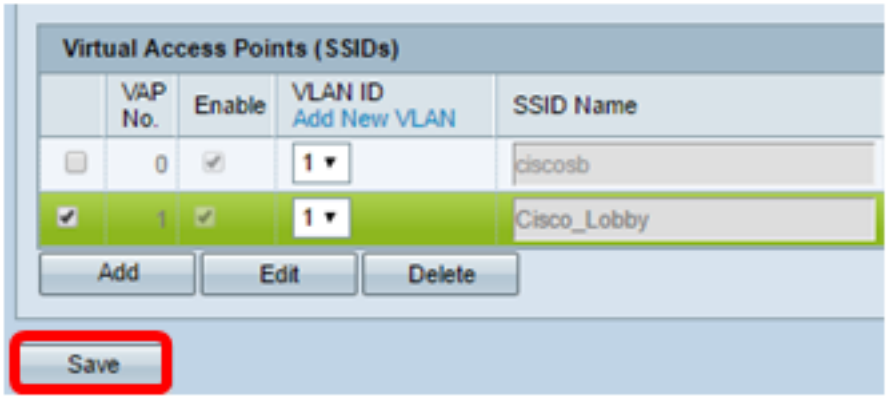
Note: Você pode marcar a caixa **Show Key as Clear Text** para mostrar a senha criada.



Etapa 6. (Opcional) No campo *Taxa de Atualização da Chave de Broadcast*, insira um valor ou o intervalo no qual a chave de broadcast (grupo) é atualizada para clientes associados a esse VAP. O padrão é 300 segundos e o intervalo válido é de 0 a 86400 segundos. Um valor 0 indica que a chave de broadcast não está atualizada.



Passo 7. Click Save.

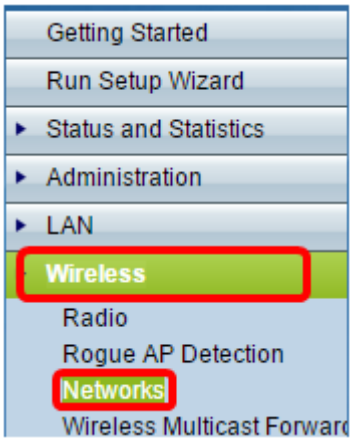


Agora você configurou a WPA Personal em seu WAP.

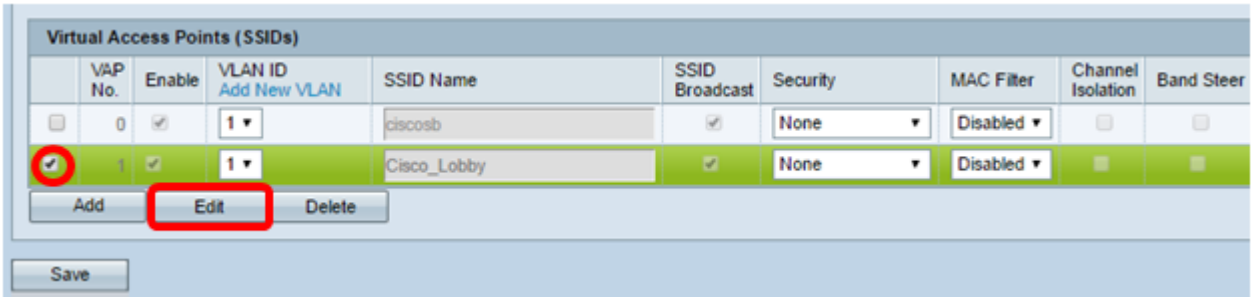
Configurar WPA/WPA2 Enterprise

Etapa 1. Faça login no utilitário baseado na Web do seu ponto de acesso e escolha **Wireless > Networks**.

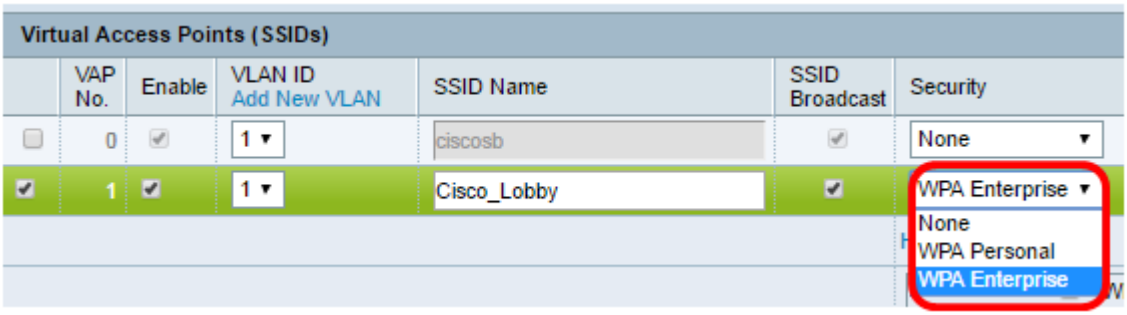
Note: Na imagem abaixo, o utilitário baseado na Web do WAP361 é usado como exemplo.



Etapa 2. Na área de Pontos de acesso virtuais (SSIDs), verifique o SSID que deseja configurar e clique no botão **Editar** abaixo dele.



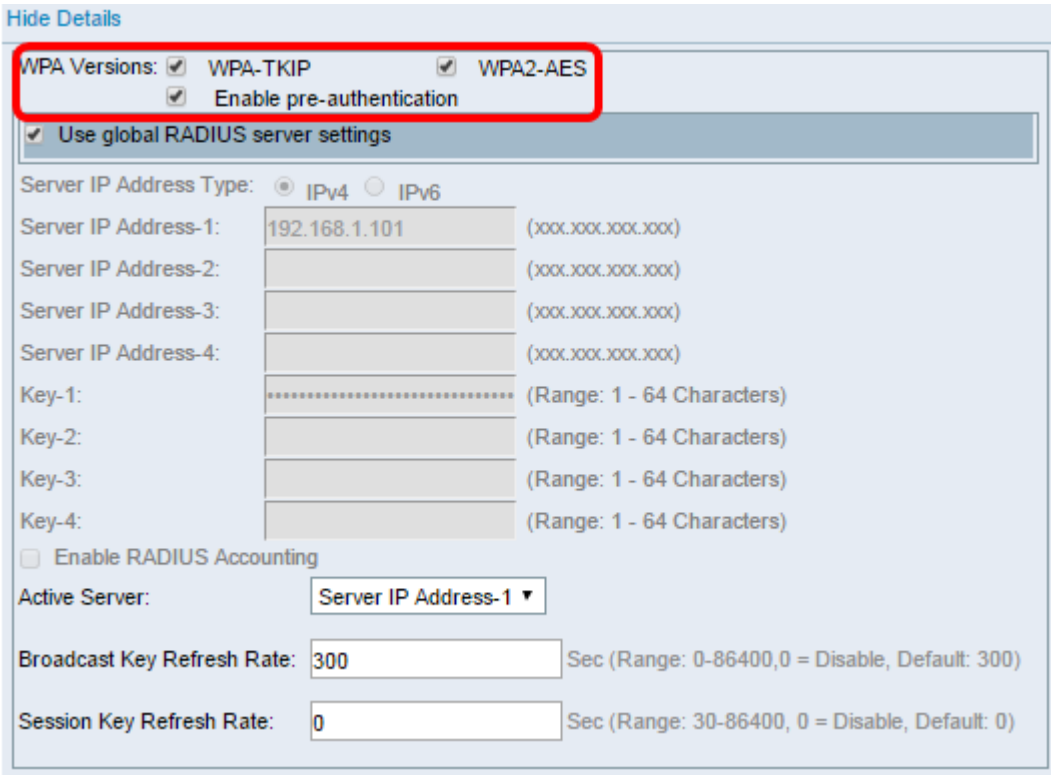
Etapa 3. Escolha **WPA Enterprise** na lista suspensa Segurança.



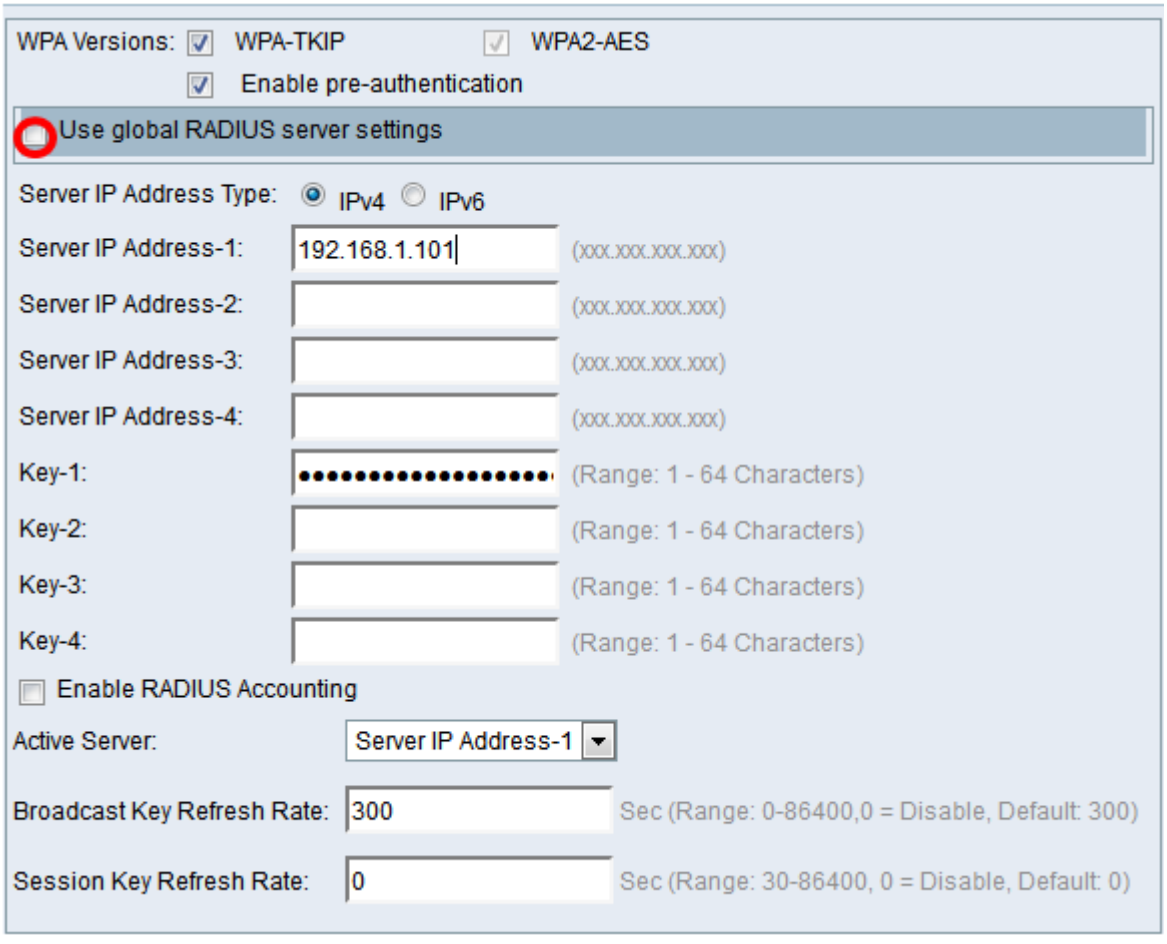
Etapa 4. Escolha a versão WPA (WPA-TKIP, WPA2-AES e Ativar pré-autenticação).

- Ativar pré-autenticação — Se escolher somente WPA2-AES ou WPA-TKIP e WPA2-AES como a versão WPA, você poderá ativar a pré-autenticação para os clientes WPA2-AES. Marque essa opção se desejar que os clientes sem fio WPA2 enviem os pacotes de pré-autenticação. As informações de pré-autenticação são retransmitidas do dispositivo WAP que o cliente está usando no momento para o dispositivo WAP de destino. Ativar esse recurso pode ajudar a acelerar a autenticação de clientes móveis que se conectam a vários pontos de acesso (AP).

Note: Esta opção não se aplica se você selecionou WPA-TKIP para versões WPA porque a WPA original não oferece suporte a esse recurso.

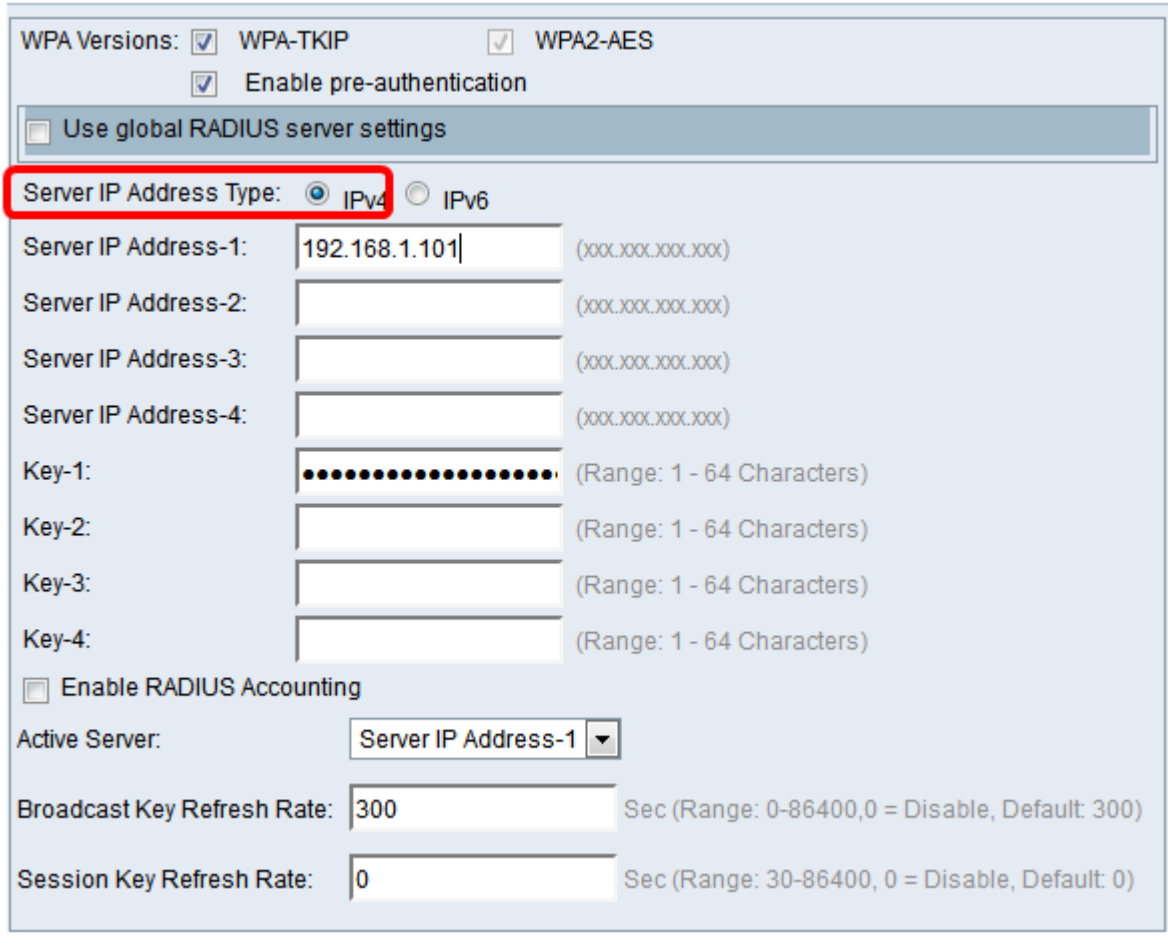


Etapa 5. (Opcional) Desmarque a caixa de seleção **Usar configurações globais do servidor RADIUS** para editar as configurações.



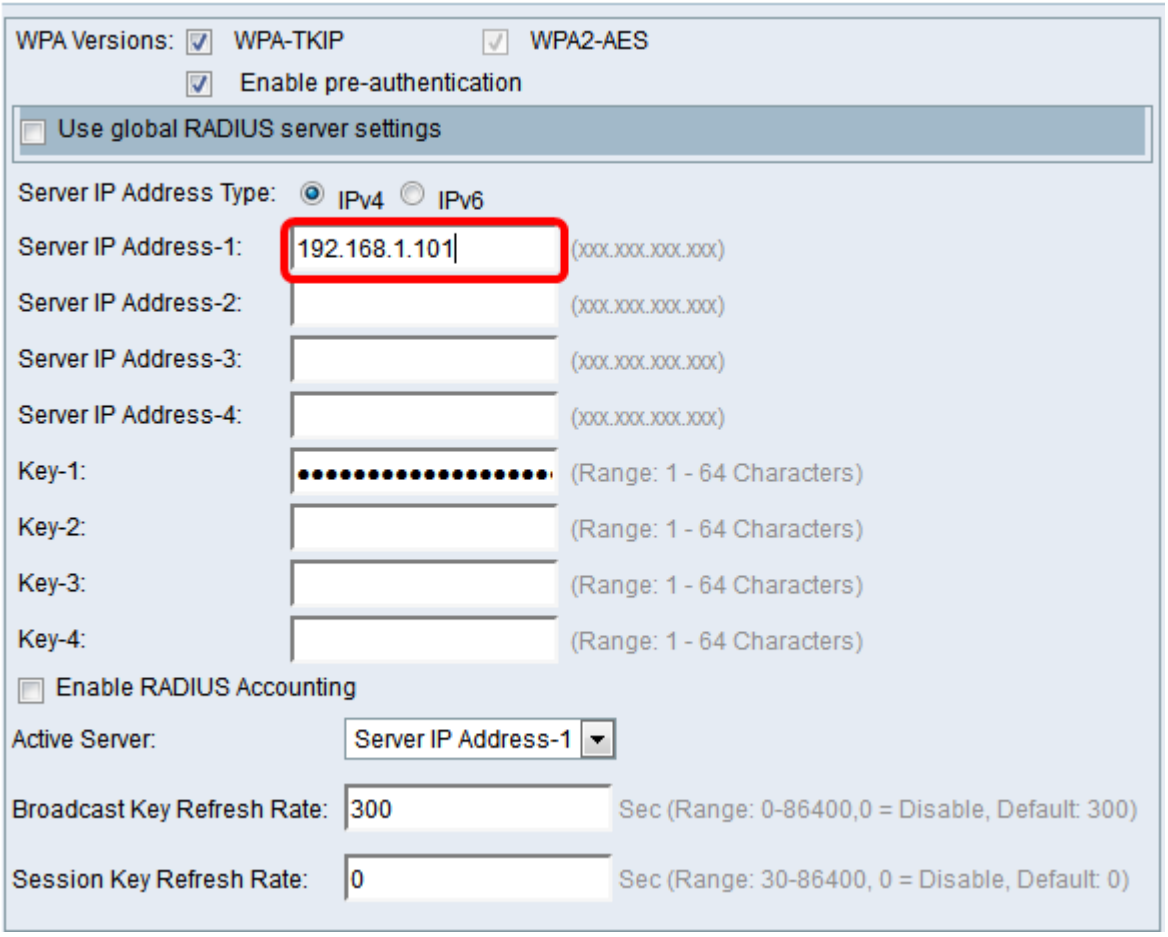
Etapa 6. (Opcional) Clique no botão de opção para o **Server IP Address Type** correto.

Note: Para este exemplo, o IPv4 é escolhido.



Passo 7. Insira o endereço IP do servidor RADIUS no campo *Server IP Address (Endereço IP do servidor)*.

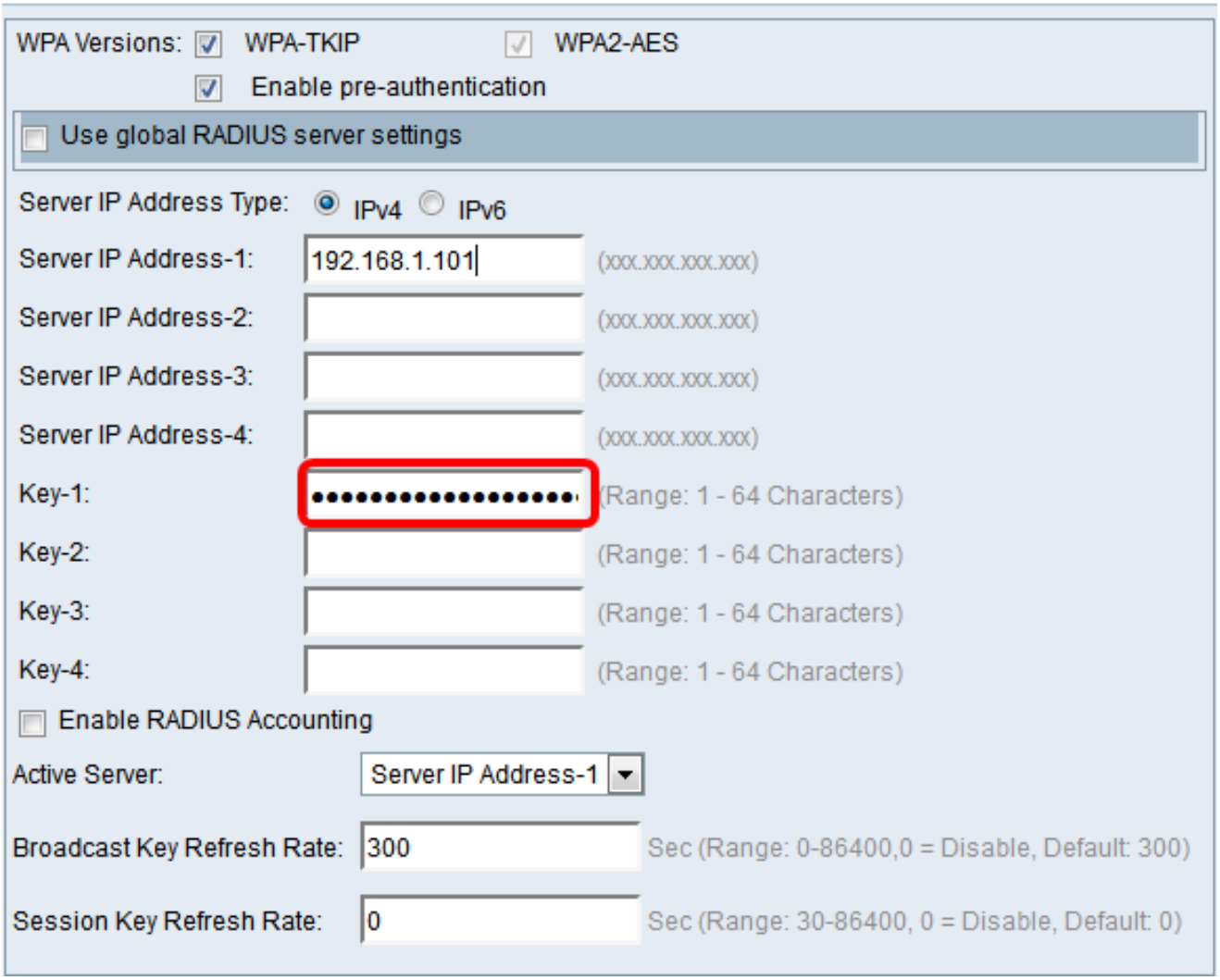
Note: Para este exemplo, 192.168.1.101 é usado.



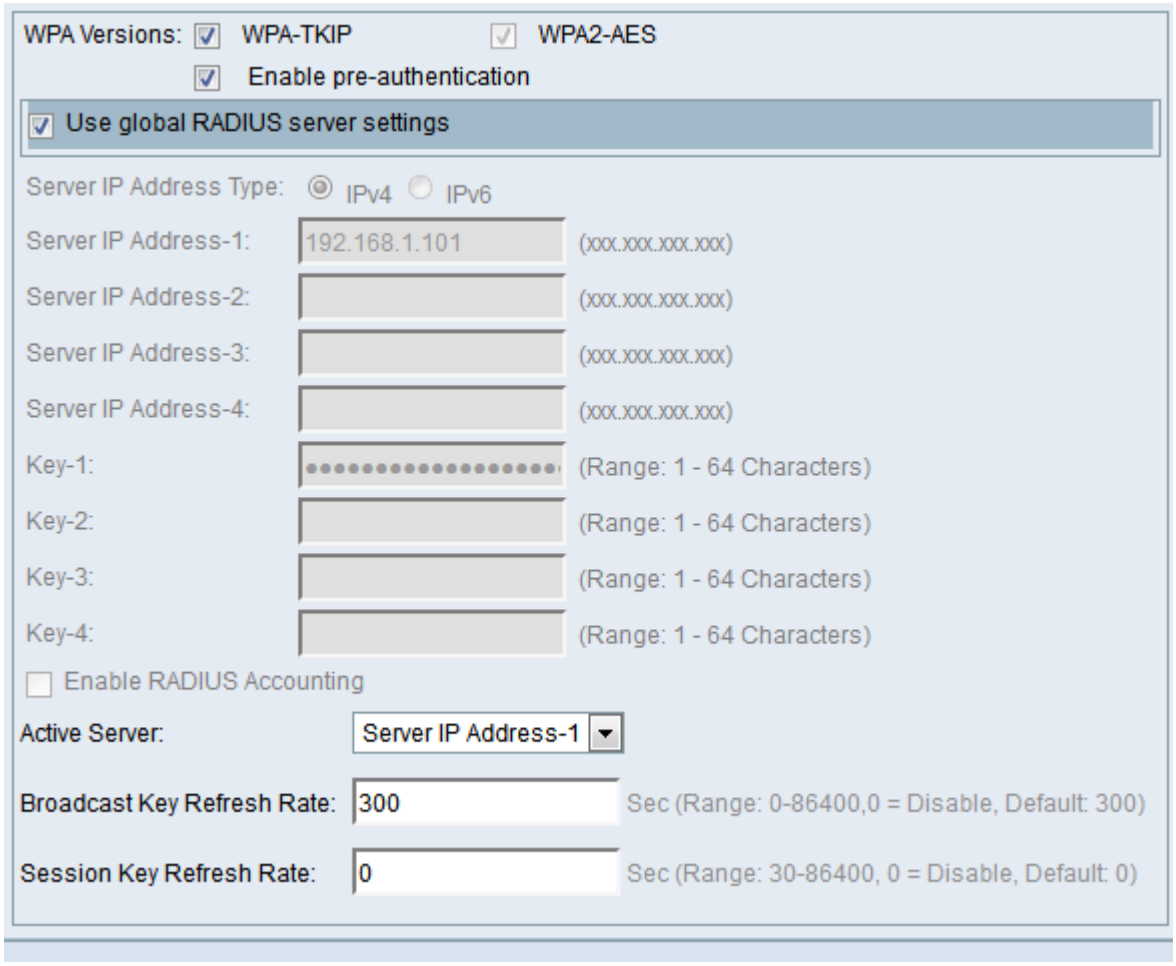
Etapa 8. No campo *Key*, insira a chave de senha correspondente ao servidor RADIUS que o WAP usa para autenticar no servidor RADIUS. Você pode usar de 1 a 64 caracteres alfanuméricos e especiais padrão.

Note: As chaves diferenciam maiúsculas de minúsculas e devem corresponder à chave configurada no servidor RADIUS.

Etapa 9. (Opcional) Repita as Etapas 7 a 8 para cada servidor RADIUS na rede com o qual você deseja que o WAP se comunique.



Etapa 10. (Opcional) Marque a caixa de seleção **EnableRADIUS Accounting** para habilitar o rastreamento e a medição dos recursos que um usuário consumiu (hora do sistema, a quantidade de dados transmitidos). Habilitar esse recurso permitirá a contabilização de RADIUS para os servidores principal e de backup.



Etapa 11. Clique em Save.

Agora você configurou com êxito a segurança WPA/WPA2 Enterprise em seu WAP.