Configure a senha ou as configurações de complexidade WPA-PSK em um ponto de acesso WAP125 ou WAP581

Objetivo

A segurança de senha aumenta com um aumento na complexidade de senha. É vital que você use senhas longas com uma combinação de letras maiúsculas e minúsculas, números e símbolos para manter uma segurança forte. A complexidade da senha é usada para definir requisitos para senhas a fim diminuir o risco de uma violação de segurança.

O WPA (Wi-Fi Protected Access) é um dos protocolos de segurança usados para redes sem fio. Quando comparada ao protocolo de segurança WEP (Wired Equivalent Privacy), a WPA melhorou os recursos de autenticação e criptografia. Se a WPA estiver configurada no AP, uma chave pré-compartilhada (PSK) WPA será escolhida para autenticar clientes com segurança. Quando a Complexidade WPA-PSK está habilitada, os requisitos de complexidade para a chave usada no processo de autenticação podem ser configurados. Chaves mais complexas fornecem maior segurança.

O objetivo deste documento é mostrar a você como configurar a Complexidade de Senha e as Configurações de Complexidade WPA-PSK em seu ponto de acesso WAP125 ou WAP581.

Dispositivos aplicáveis

- WAP125
- WAP581

Versão de software

- 1.0.0.4 — WAP581
- 1.0.0.5 — WAP125

Configurar a segurança da senha

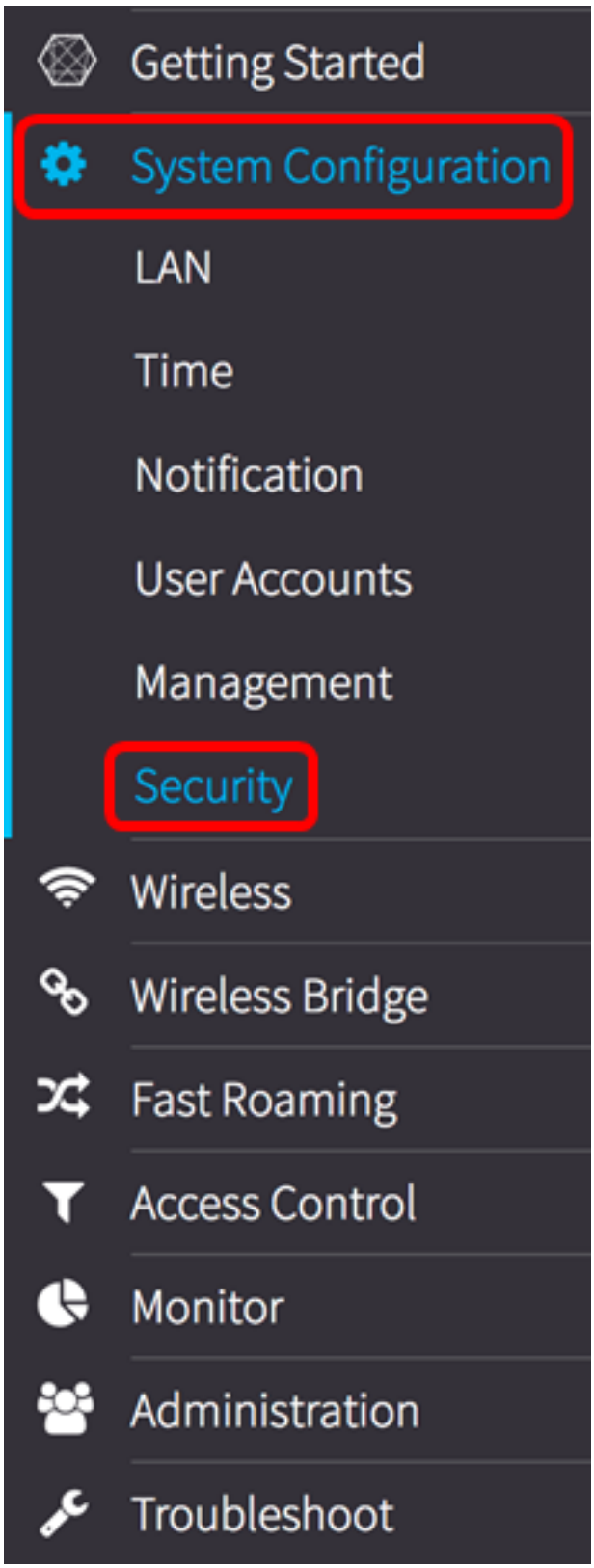
Configurar a complexidade da senha

Etapa 1. Faça login no utilitário baseado na Web do seu WAP. O nome do usuário e a senha padrão são cisco/cisco.

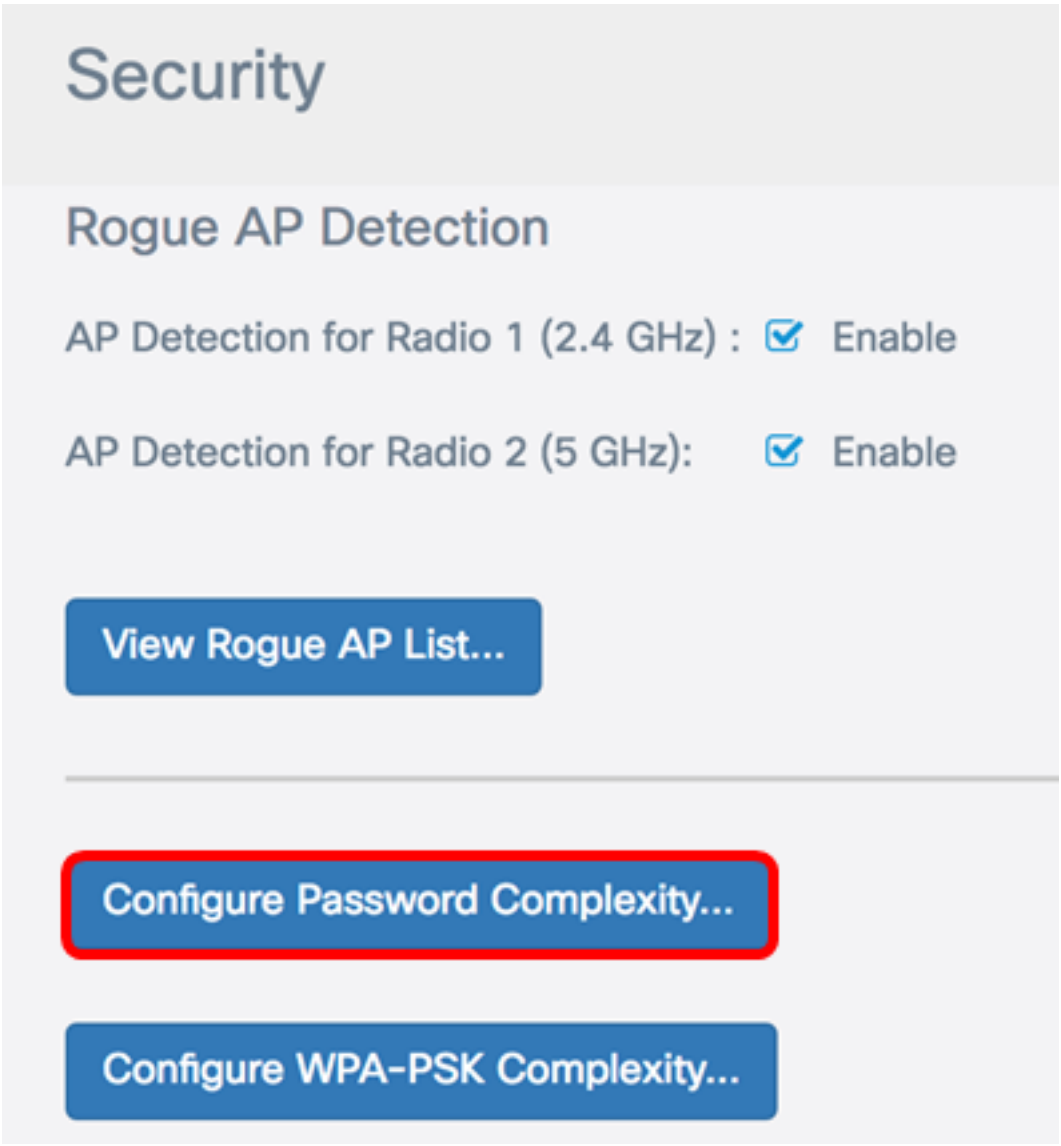
Note: Se você já tiver alterado a senha ou criado uma nova conta, insira suas novas credenciais.

Etapa 2. Escolha **Configuração do sistema > Segurança**.

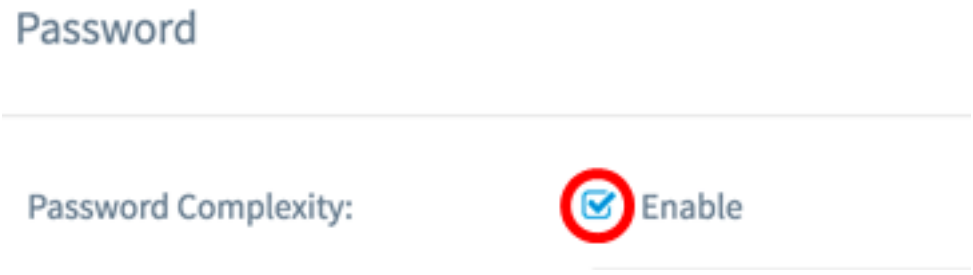
Note: As opções disponíveis podem variar dependendo do modelo exato do dispositivo. Neste exemplo, WAP125 é usado.



Etapa 3. Abaixo da área Detecção de AP não autorizado, clique no botão **Configurar complexidade de senha...**.



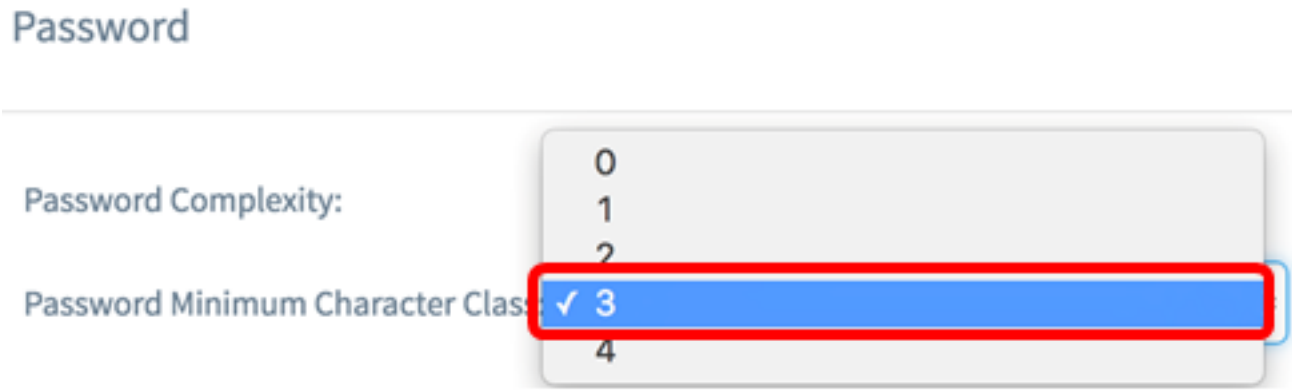
Etapa 4. Marque a caixa de seleção **Enable Password Complexity (Ativar** complexidade da senha) para habilitar as etapas para definir a complexidade da senha. Se esta opção estiver desmarcada, vá para a Etapa 8.



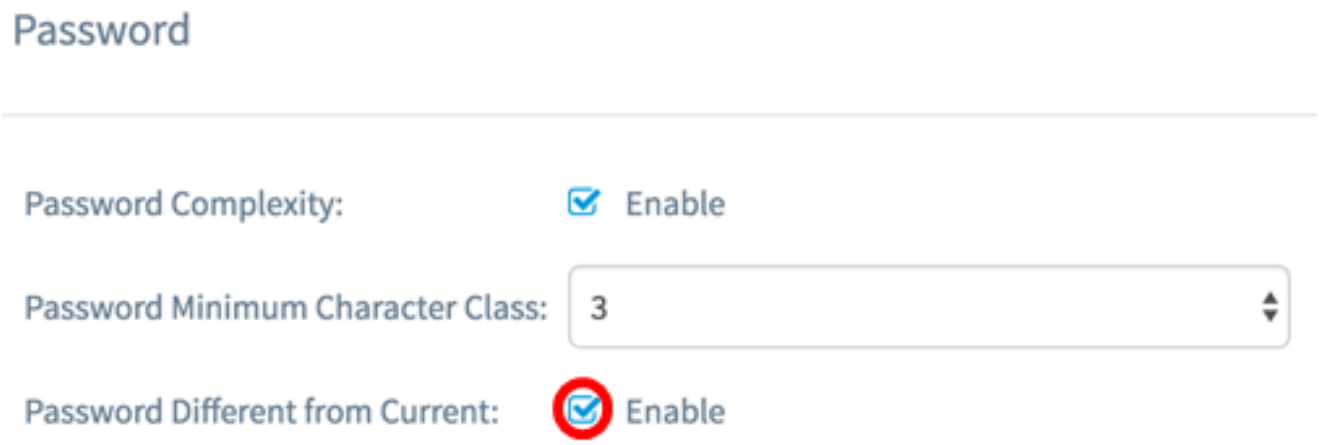
Etapa 5. Escolha um valor na lista suspensa Classe mínima de caracteres da senha. O número inserido representa o número de caracteres mínimo ou máximo das diferentes classes:

- A senha é composta por caracteres maiúsculos (ABCD).
- A senha é composta por caracteres minúsculos (abcd).
- A senha é composta por caracteres numéricos (1234).
- A senha é composta por caracteres especiais (!@#$).

Note: Neste exemplo, 3 é escolhido.

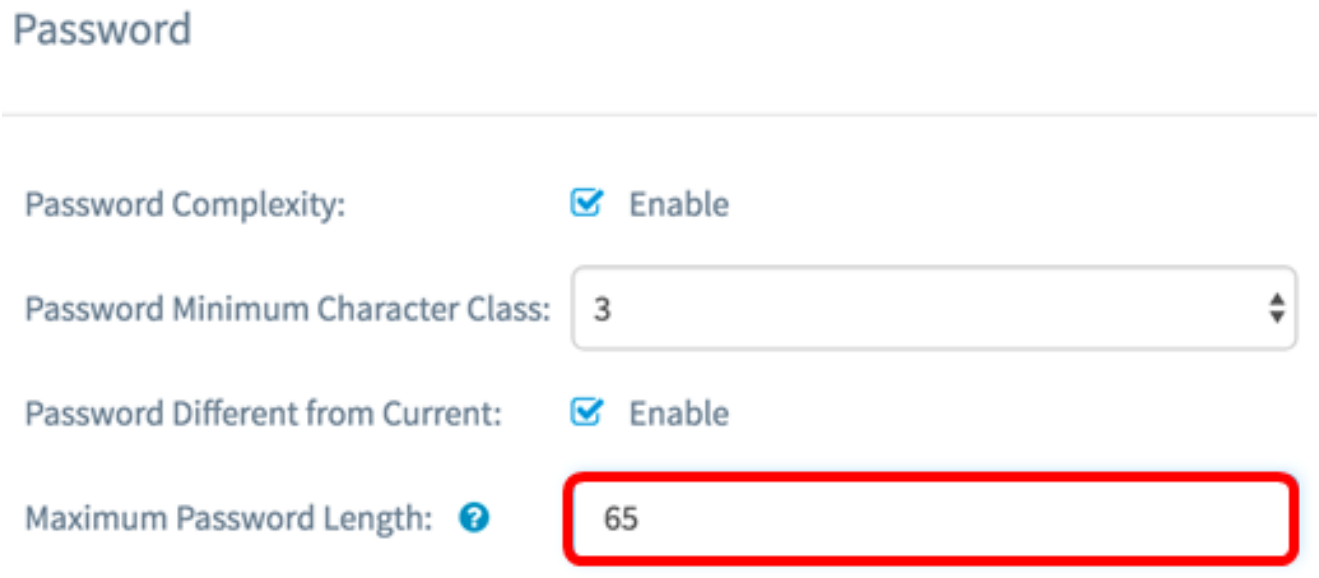


Etapa 6. Marque a caixa de seleção **Enable** Password Different from Current (Ativar senha diferente do atual) para permitir que os usuários atualizem sua senha quando ela expirar. Se esta opção for deixada desmarcada, os usuários ainda poderão digitar novamente a mesma senha quando ela expirar.



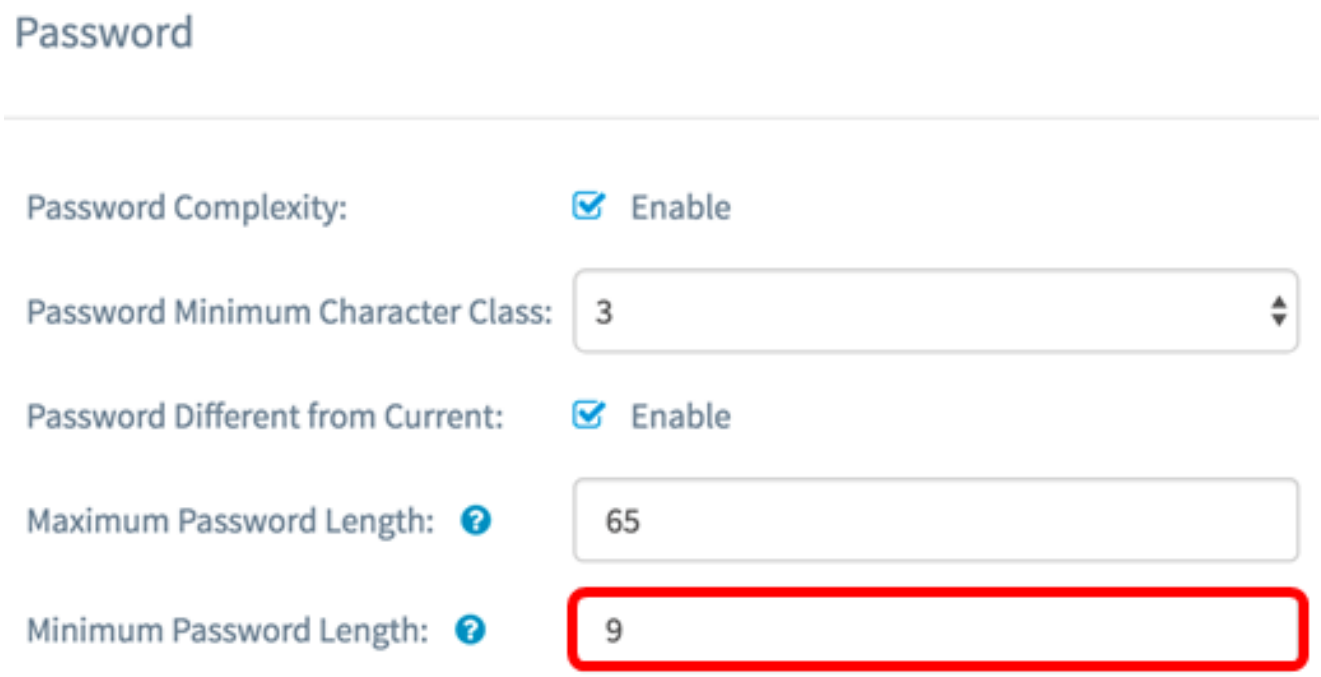
Passo 7. No campo *Tamanho máximo da senha*, insira um valor de 64 a 127 para definir o número de caracteres e o comprimento da senha. O padrão é 64.

Note: Neste exemplo, 65 é usado.

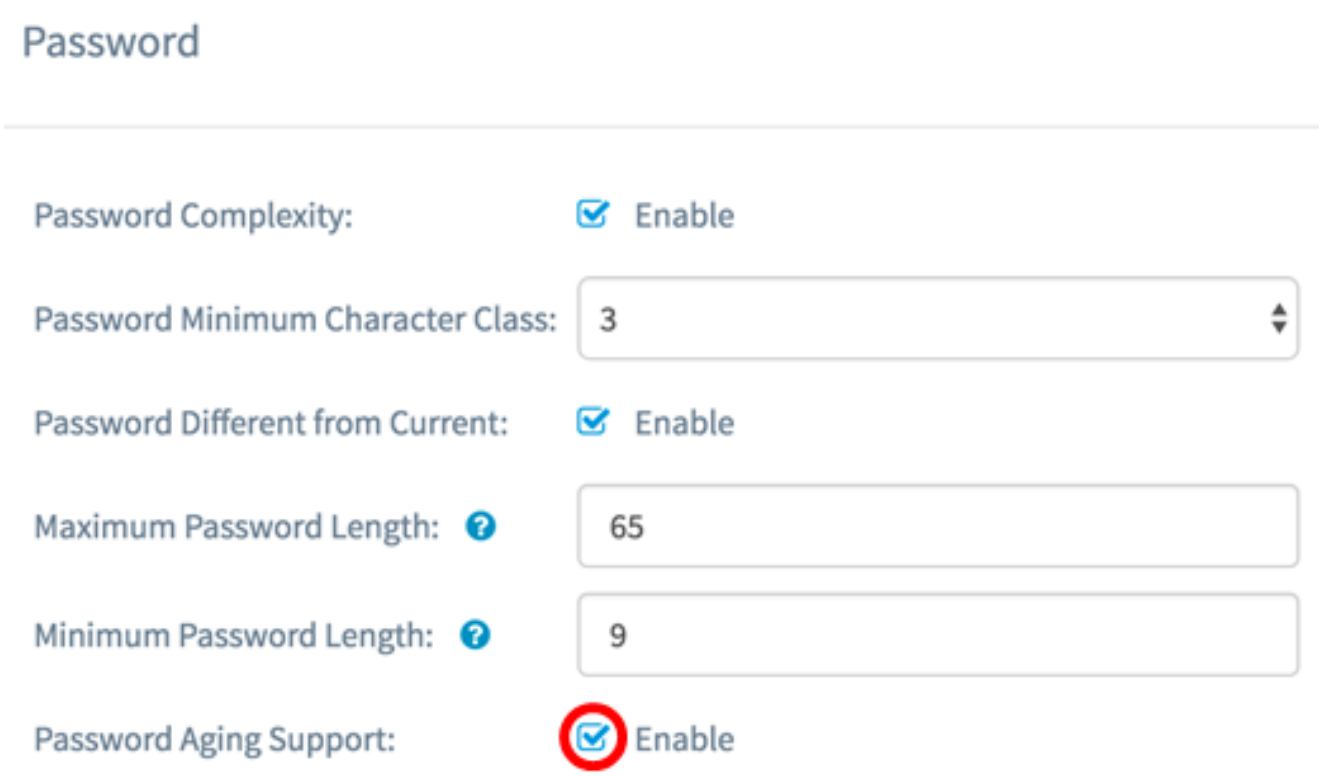


Etapa 8. No campo *Tamanho mínimo da senha*, insira um valor de 0 a 32 para definir o número mínimo necessário de caracteres para a senha. O padrão é 8.

Note: Neste exemplo, o comprimento mínimo da senha é 9.

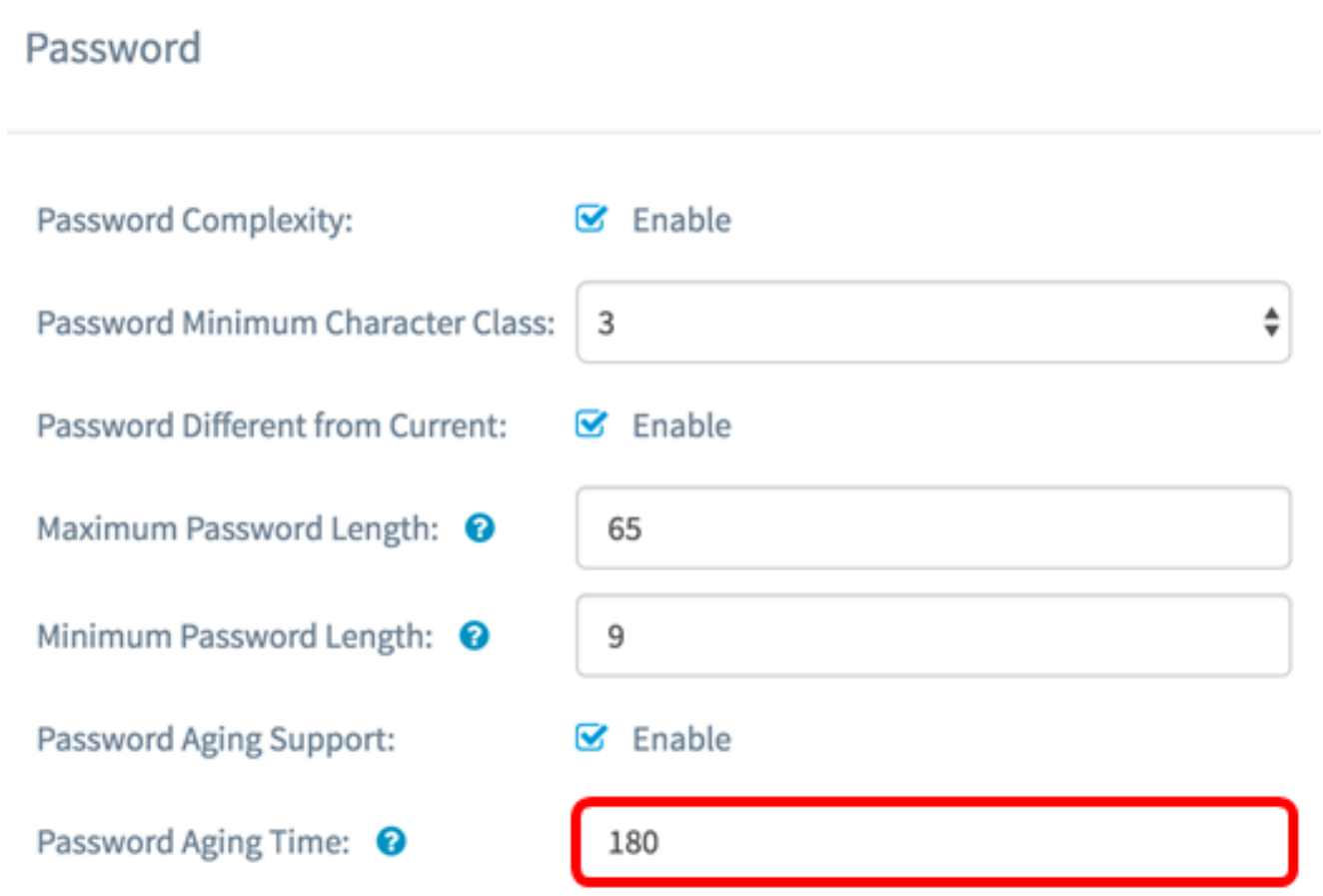


Etapa 9. Marque a caixa de seleção **Habilitar** Suporte ao vencimento de senha para permitir que as senhas expirem. Se isso estiver habilitado, vá para a próxima etapa, caso contrário, vá para .

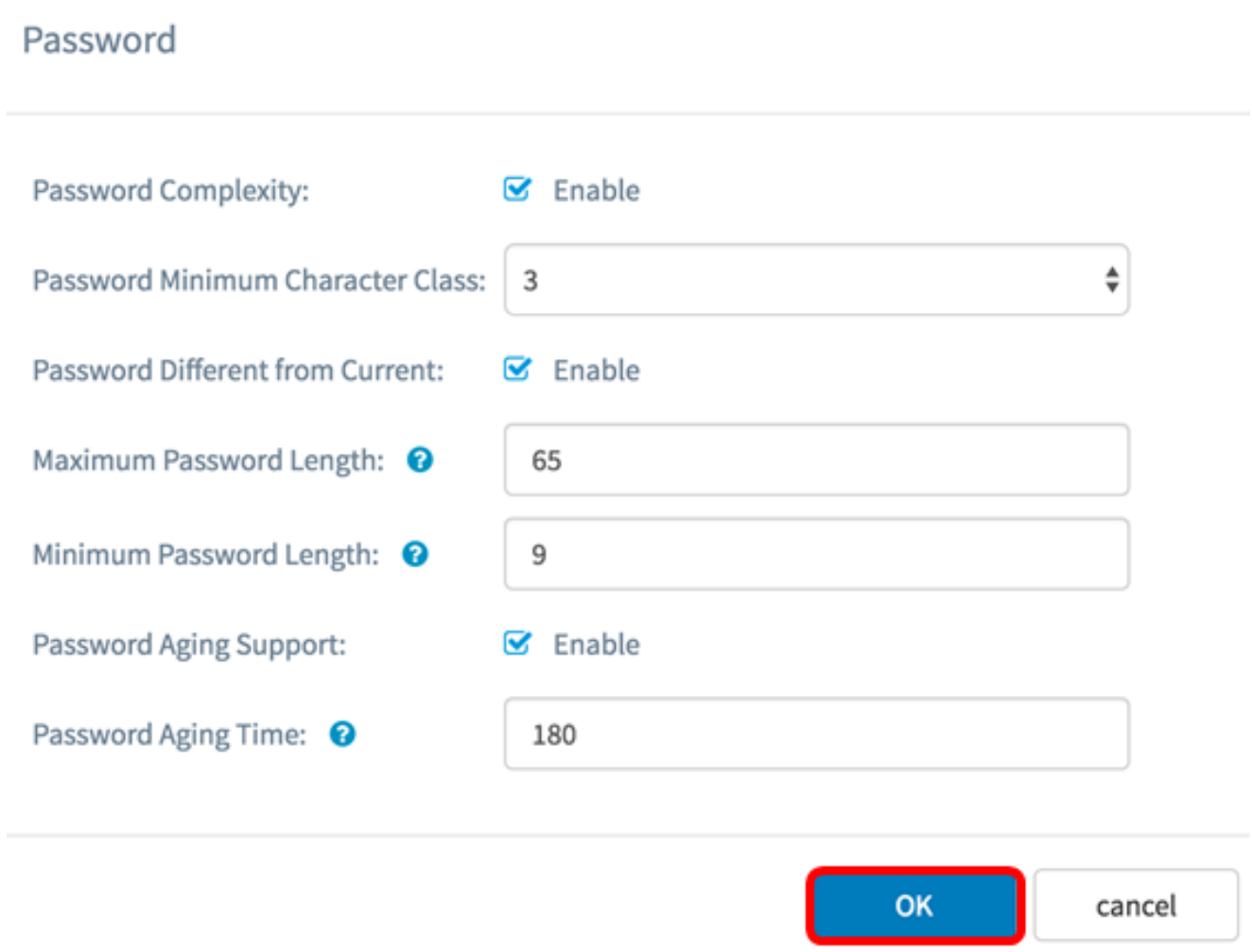


Etapa 10. No campo *Password Aging Time*, insira um valor entre 1 e 365 para definir o número de dias antes da expiração de uma senha recém-criada. O padrão é 180 dias.

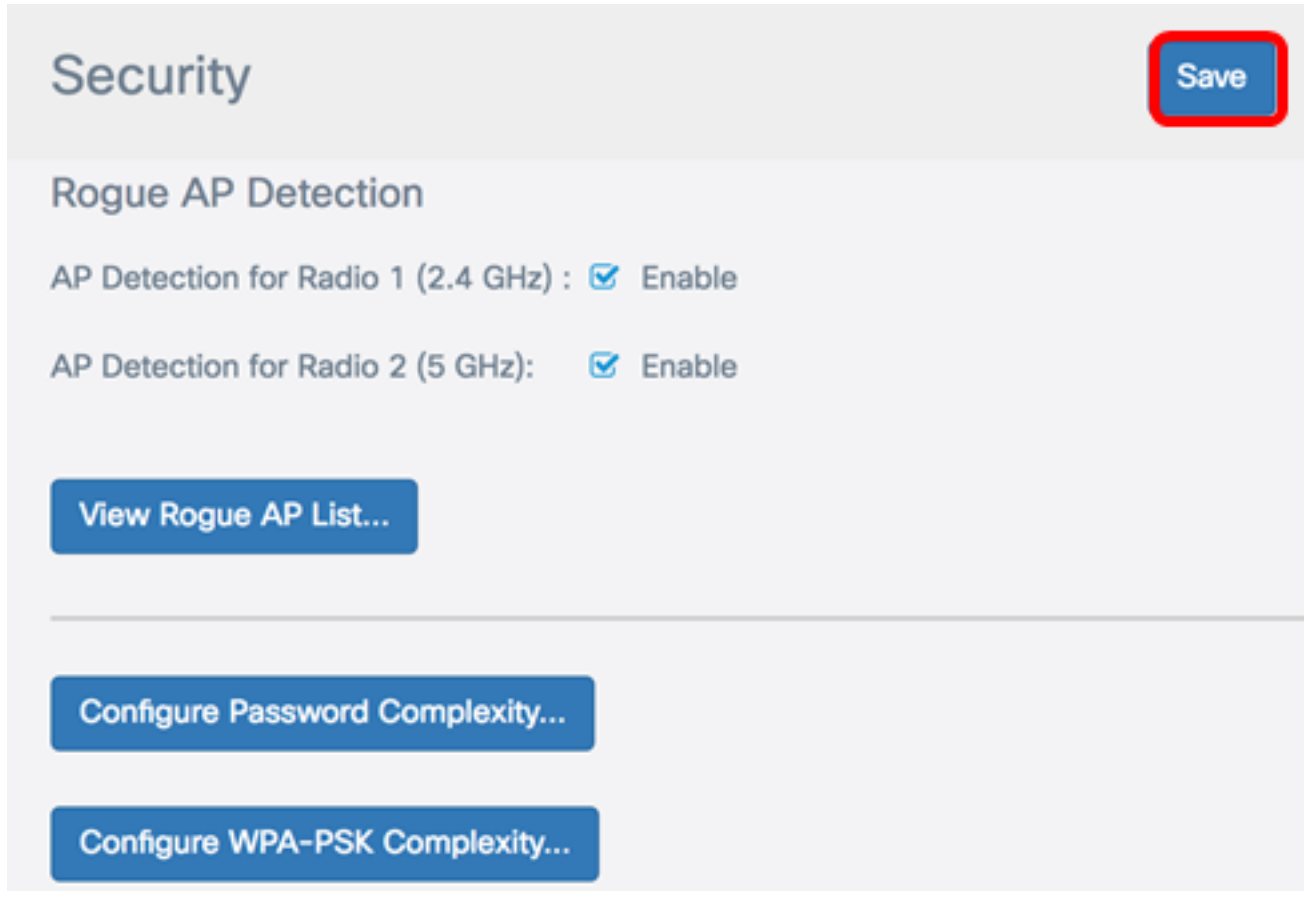
Note: Neste exemplo, 180 é usado.



Etapa 11. Click **OK**. Você será levado de volta para a página principal de configuração de segurança.



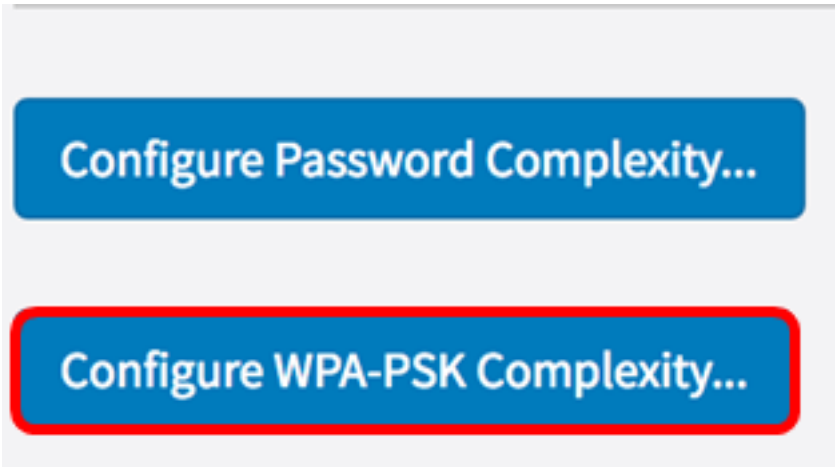
Etapa 12. Clique no botão **Salvar** para salvar as configurações definidas.



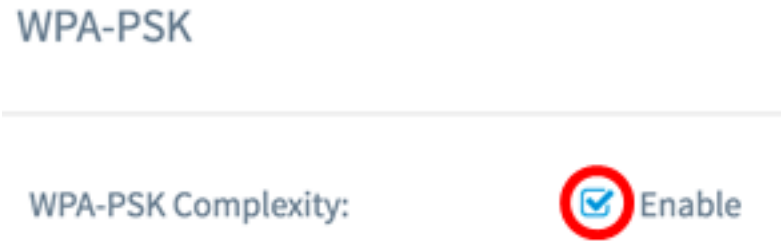
Agora você deve ter configurado com êxito as configurações de segurança de Complexidade de Senha em seu WAP.

Configurar a complexidade WPA-PSK

Etapa 1. Clique no botão **Configure WPA-PSK Complexity (Configurar complexidade WPA-PSK)**.



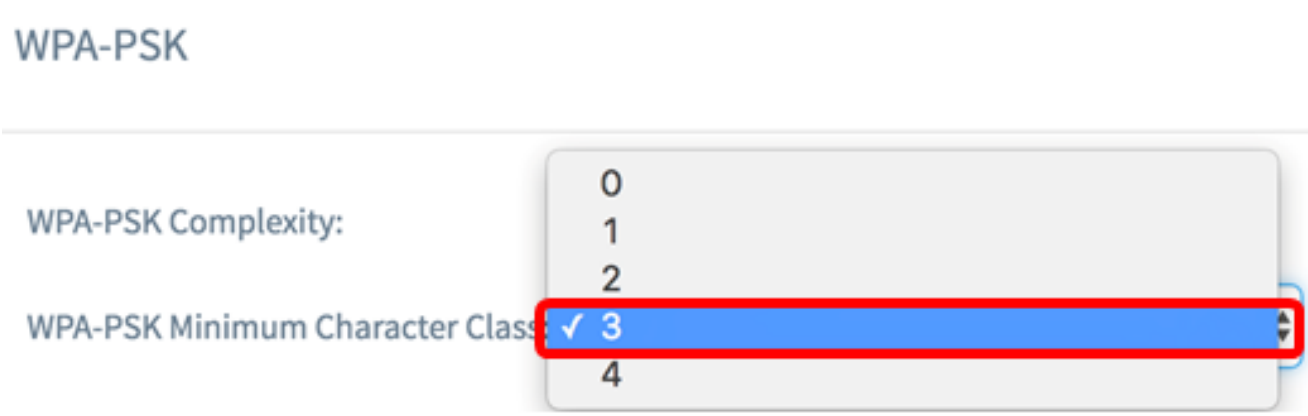
Etapa 2. Marque a caixa de seleção **Enable** WPA-PSK Complexity (Ativar complexidade WPA-PSK) para habilitar as etapas para definir a complexidade da senha.



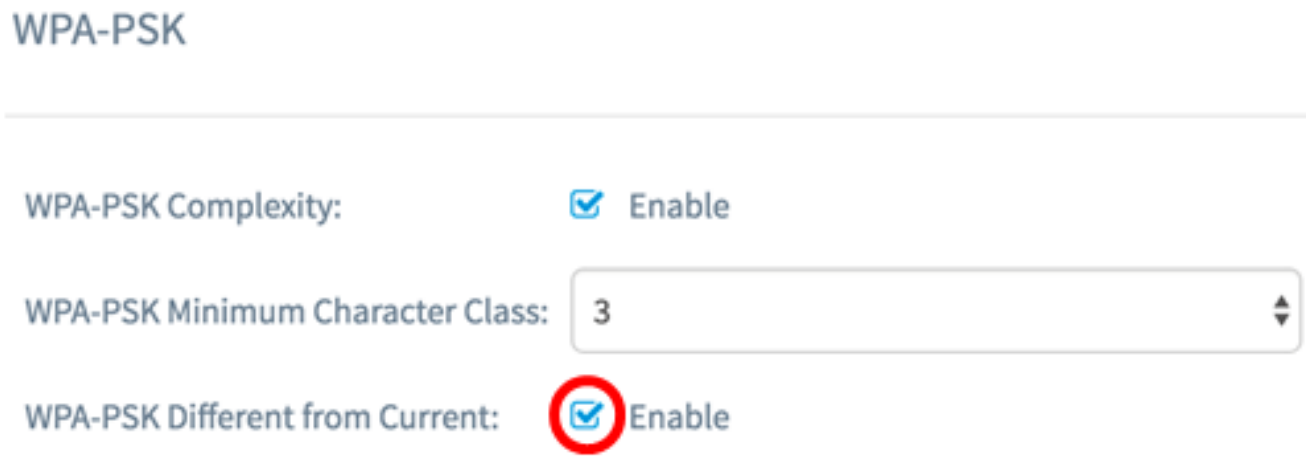
Etapa 3. Escolha um valor na lista suspensa Classe de caractere mínimo WPA-PSK. O número inserido representa o número de caracteres mínimo ou máximo das diferentes classes:

- A senha é composta por caracteres maiúsculos (ABCD).
- A senha é composta por caracteres minúsculos (abcd).
- A senha é composta por caracteres numéricos (1234).
- A senha é composta por caracteres especiais (!@#$).

Note: Neste exemplo, 3 é escolhido.

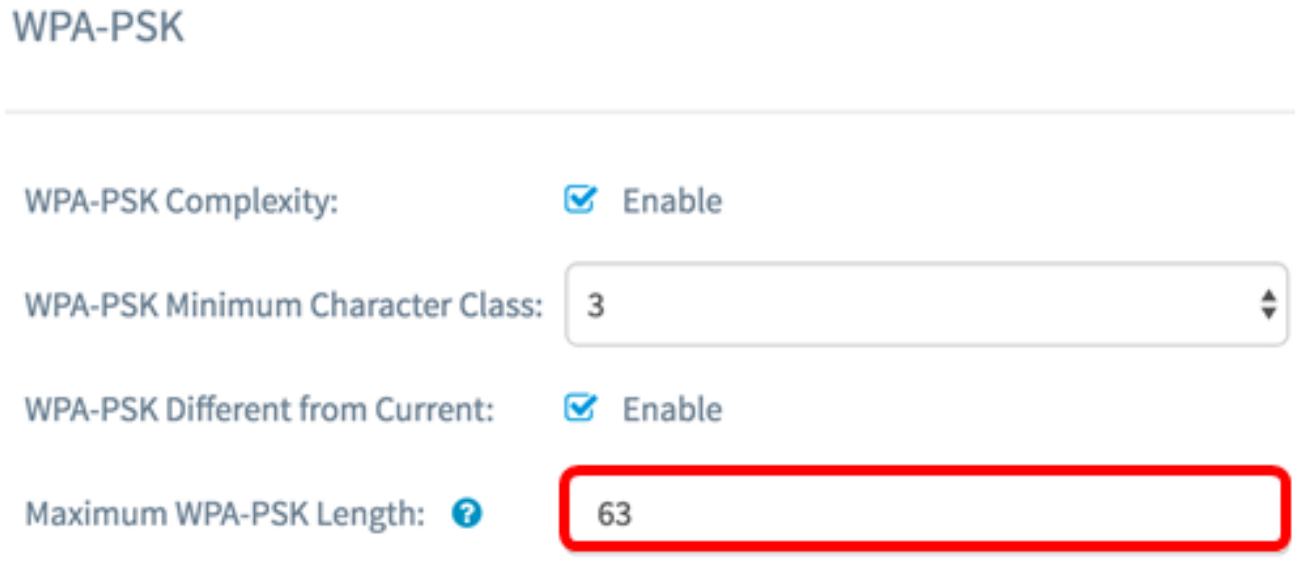


Etapa 4. Marque a caixa de seleção **Enable** WPA-PSK Different from Current (Ativar WPA-PSK diferente de Atual) para permitir que os usuários atualizem sua senha quando ela expirar. Se esta opção for deixada desmarcada, os usuários ainda poderão digitar novamente a mesma senha quando ela expirar.



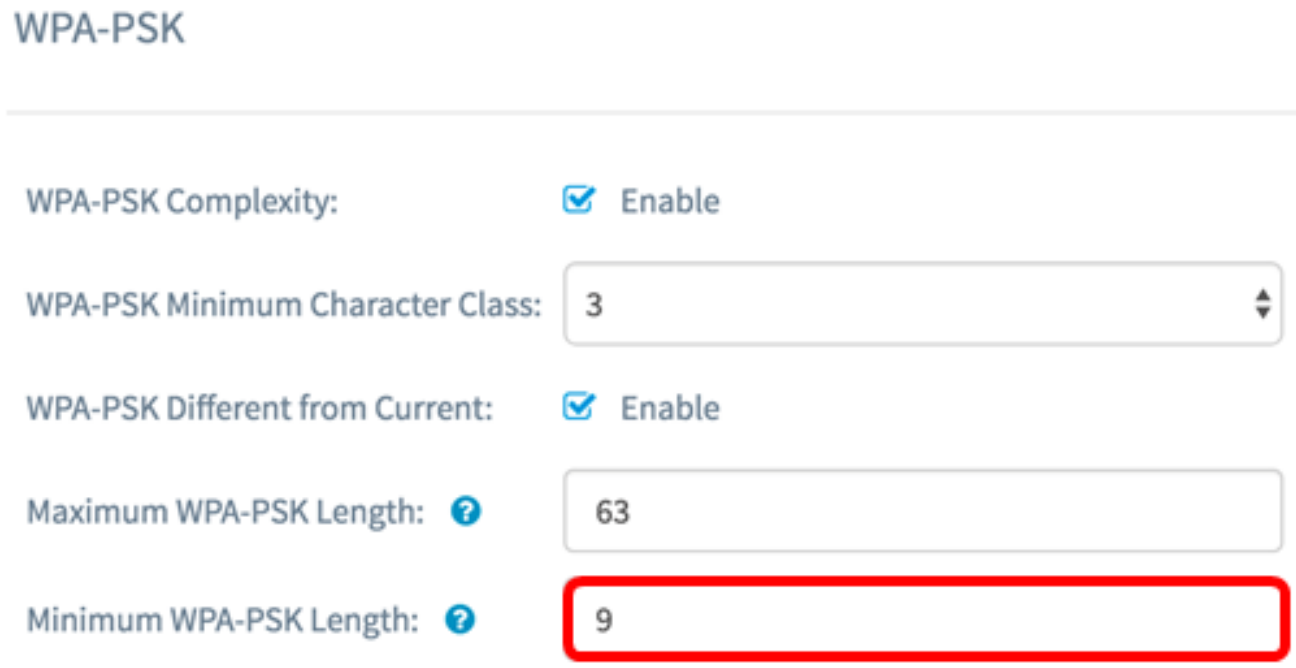
Etapa 5. No campo *WPA-PSK Length*, insira um valor de 32 a 63 para definir o número de caracteres e o comprimento da senha. O padrão é 63.

Note: Neste exemplo, 63 é usado.

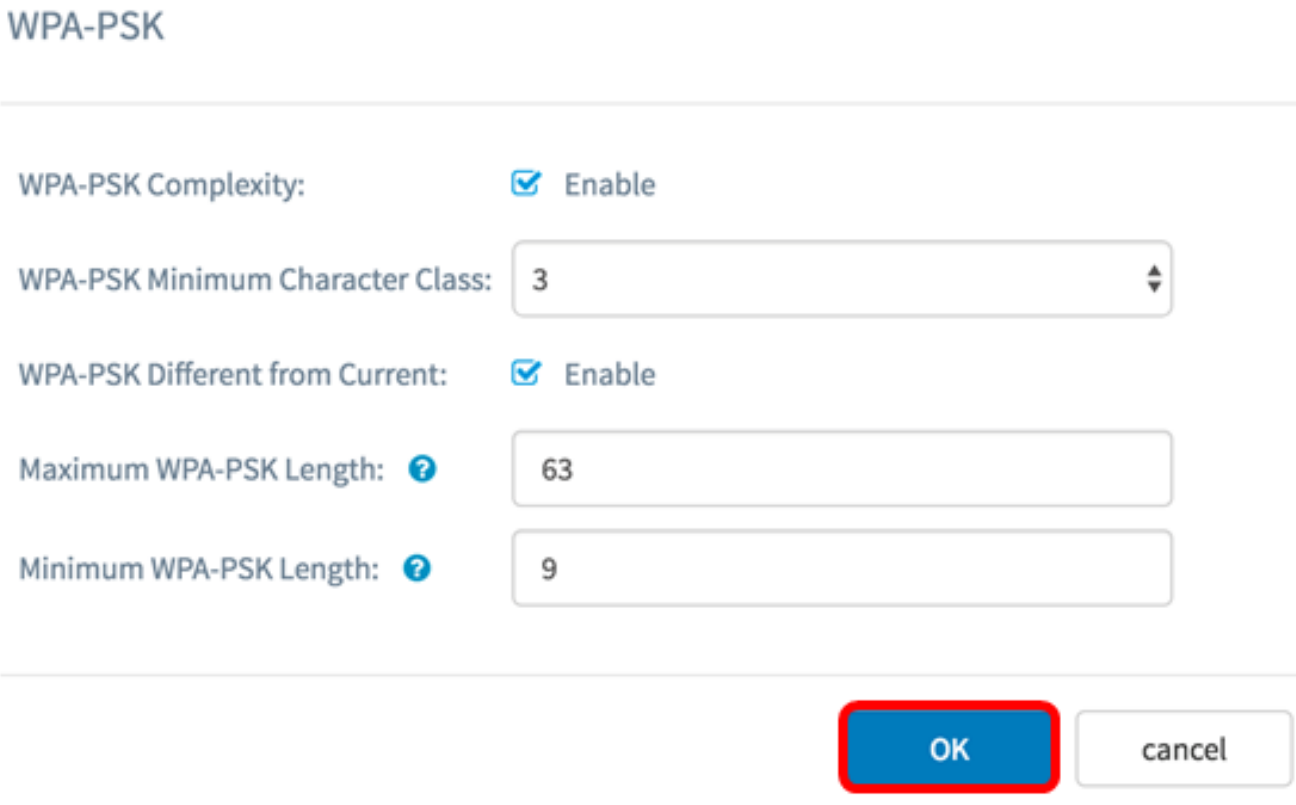


Etapa 6. No campo *Minimum WPA-PSK Length*, insira um valor de 0 a 32 para definir o número mínimo necessário de caracteres para a senha. O padrão é 8.

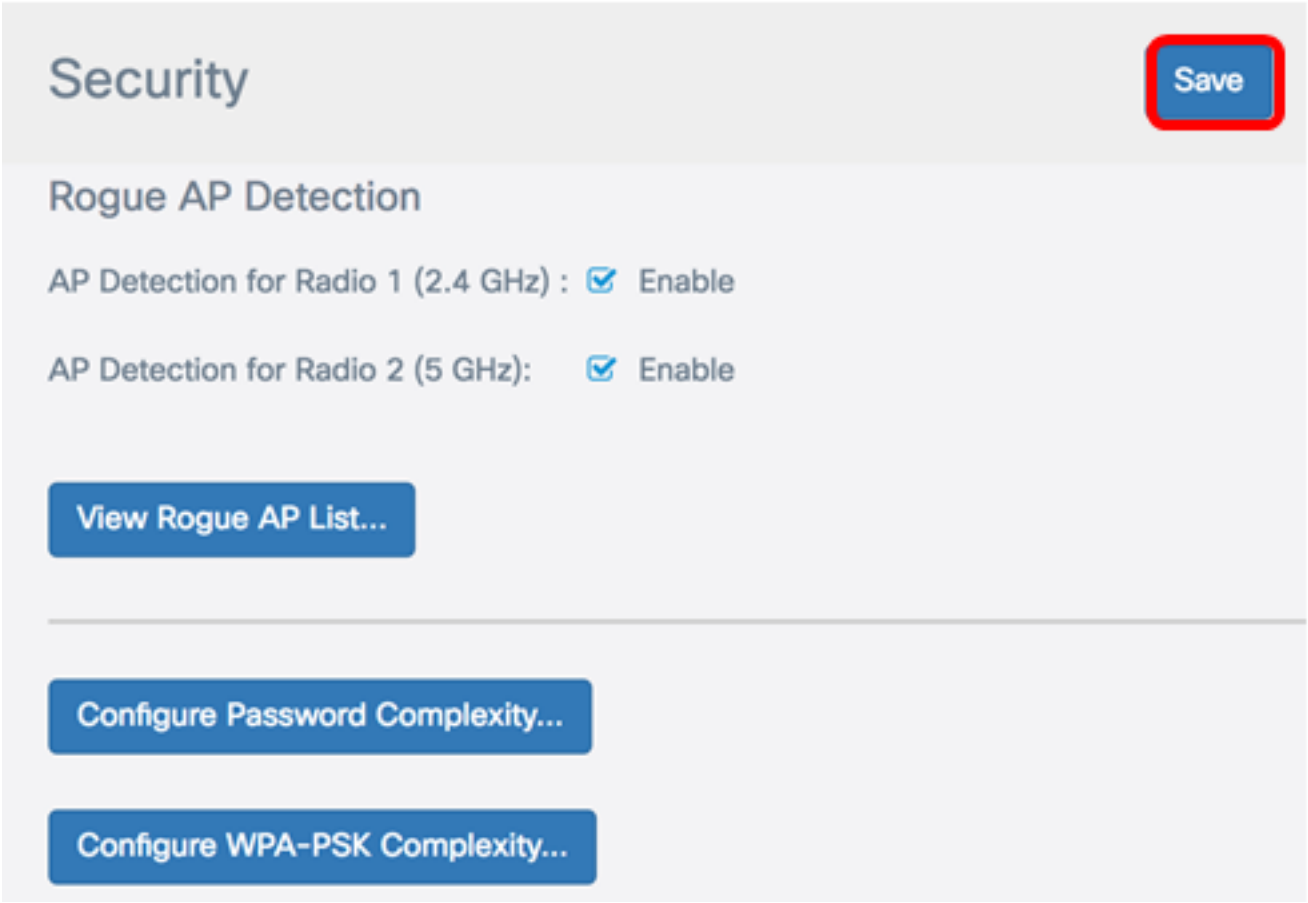
Note: Neste exemplo, o comprimento mínimo da senha é 9.



Passo 7. Click **OK**. Você será levado de volta para a página principal de configuração de segurança.



Etapa 8. Clique no botão **Salvar** para salvar as configurações definidas.



Agora você deve ter configurado com êxito as configurações de segurança de Complexidade WPA-PSK em seu WAP.