Configurar a tarefa do serviço HTTP/HTTPS em um Access point WAP125 ou WAP581

Objetivo

O protocolo de transferência de hipertexto seguro (HTTPS) é um protocolo transfer que seja mais seguro do que o HTTP. O Access point pode ser controlado através do HTTP e das conexões de HTTPS quando os server HTTP/HTTPS são configurados. Alguns navegadores da Web usam o HTTP quando outro usarem o HTTPS. Um Access point deve ter um certificado válido do Secure Socket Layer (SSL) para usar serviços HTTPS.

Por que nós precisamos de configurar a tarefa do serviço HTTP/HTTPS?

Esta característica é útil manter para fora anfitriões desonestos de alcançar a utilidade com base na Web. Usando o Access Control List do Gerenciamento, permite que você especifique até os endereços IP de Um ou Mais Servidores Cisco ICM NT 10, os cinco para o IPv4 e os cinco para que o IPv6 tenha o acesso à utilidade com base na Web.

O objetivo deste documento é mostrar-lhe como fortificar sua rede que mostra por você como configurar a tarefa do serviço HTTP/HTTPS no WAP125.

Dispositivos aplicáveis

- WAP125
- WAP581

Versão de software

- 1.0.0.4 — WAP581
- 1.0.0.5 — WAP125

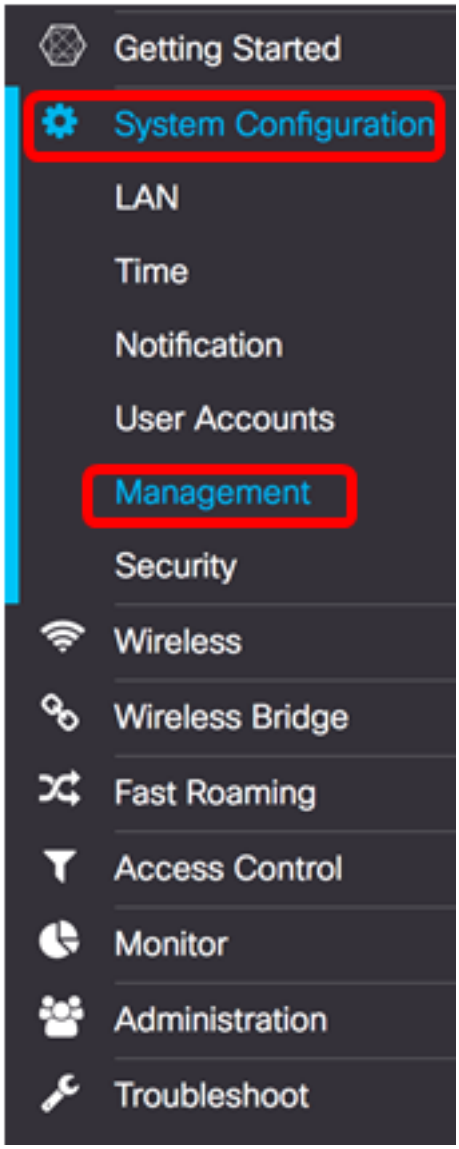
Recolha a informação da sustentação

Etapa 1. Entre à utilidade com base na Web de seu WAP. O nome de usuário padrão e a senha são Cisco/Cisco.

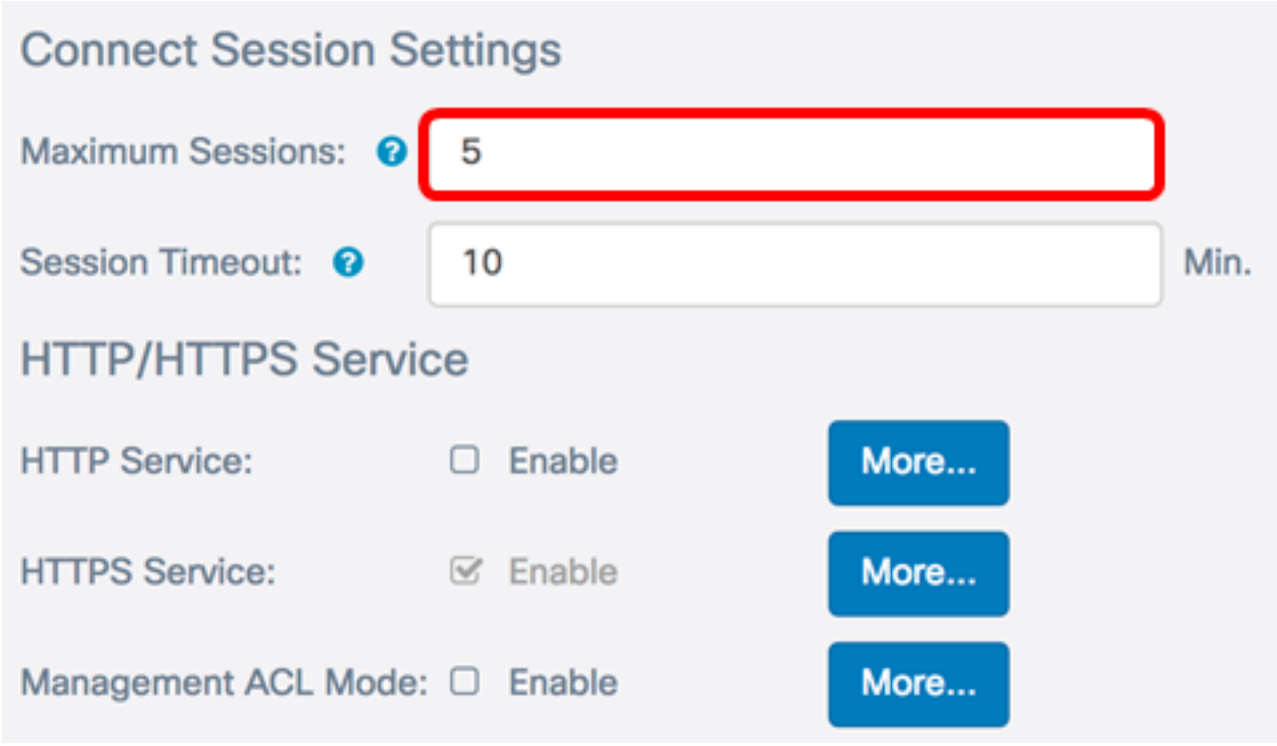
Nota: Se você tem mudado a senha ou tem criado já uma conta nova, incorpore suas credenciais novas pelo contrário.

Etapa 2. Escolha a **configuração de sistema > o Gerenciamento**.

Nota: As opções disponíveis podem variar segundo o modelo exato de seu dispositivo. Neste exemplo, WAP125 é usado.

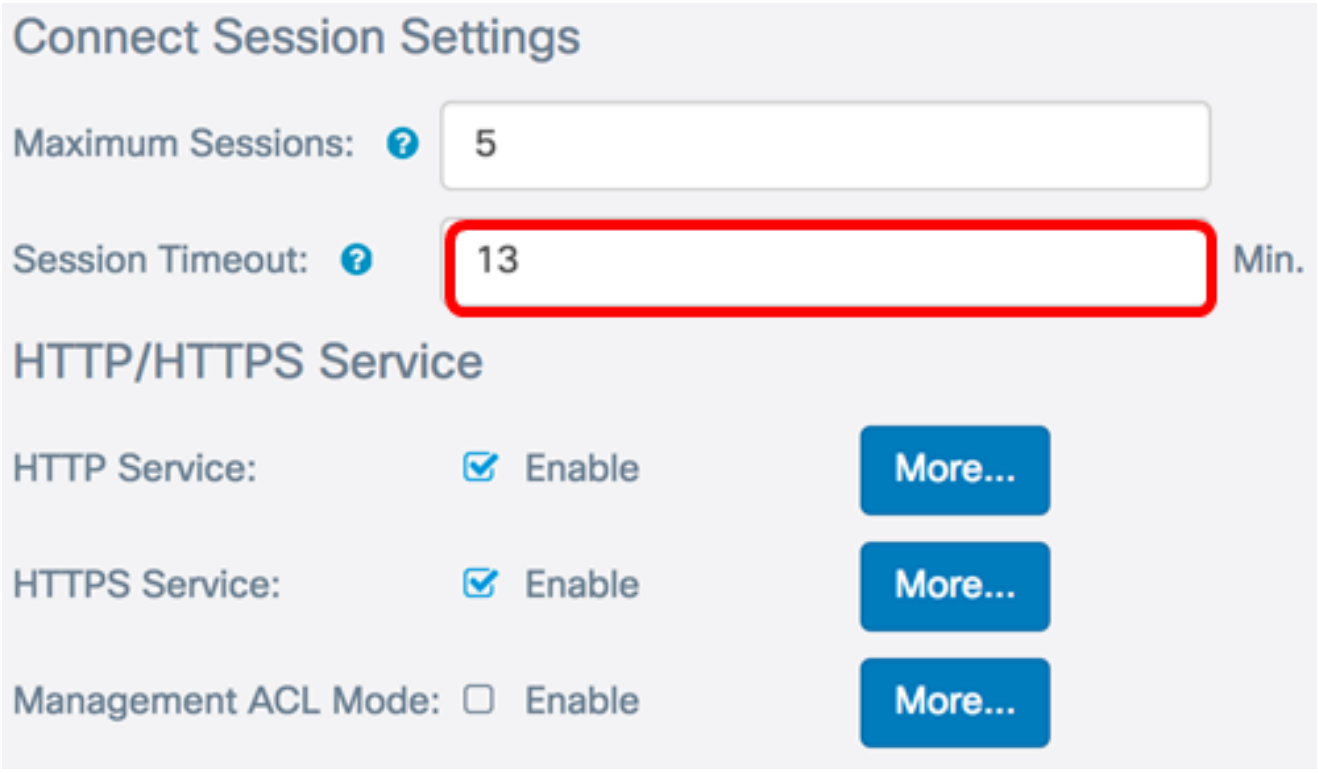


Etapa 3. *Nas sessões máxima* coloque conectam abaixo configurações de sessão, incorporam um valor de 1 ao 10 para ajustar o número máximo de sessões da web simultâneas. Uma sessão é criada cada vez que um usuário entra ao dispositivo. Se a sessão máxima é alcançada então o usuário seguinte que tenta entrar no dispositivo com serviço HTTP ou HTTPS está rejeitado. O padrão é 5.



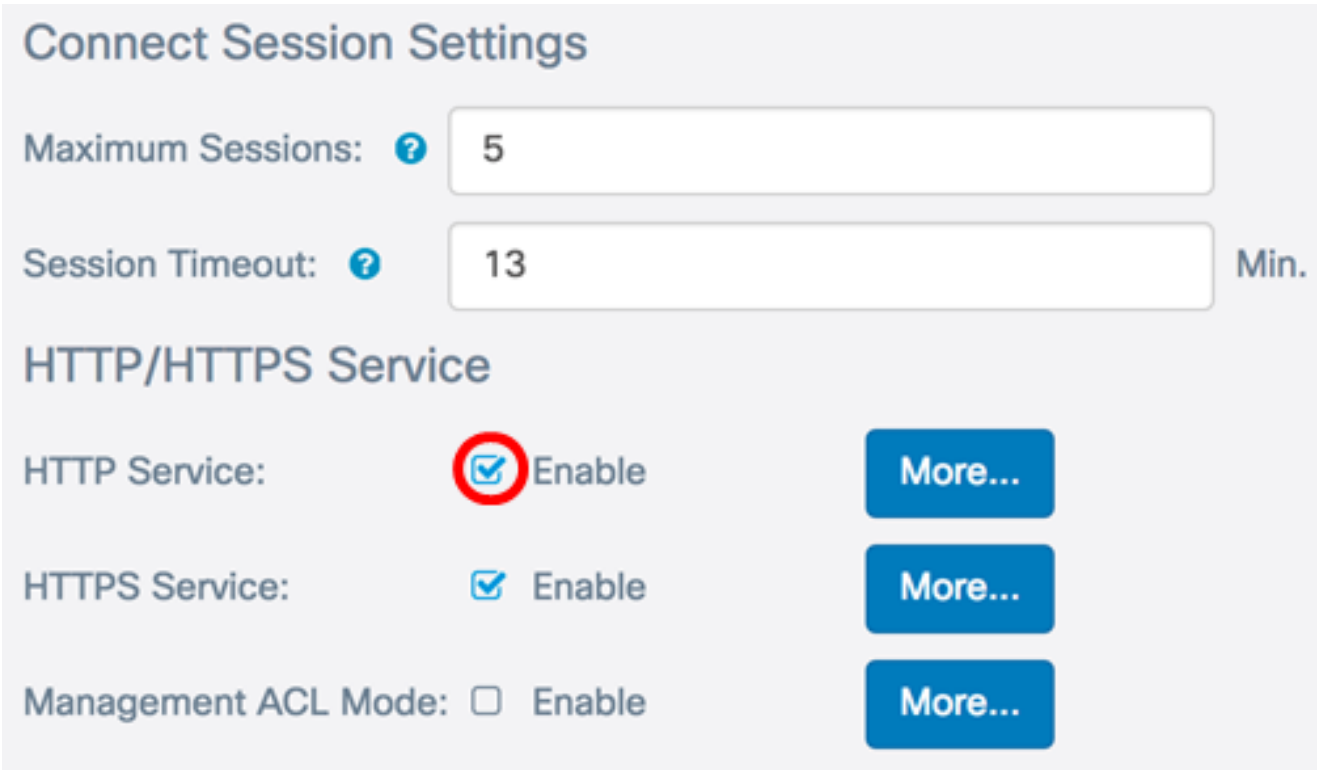
Etapa 4. No campo do *timeout de sessão*, incorpore um valor entre 2 e 60 minutos para ajustar a hora onde a sessão da web pode permanecer inativa. O valor padrão é os minutos 10.

Nota: Neste exemplo, 13 são usados.

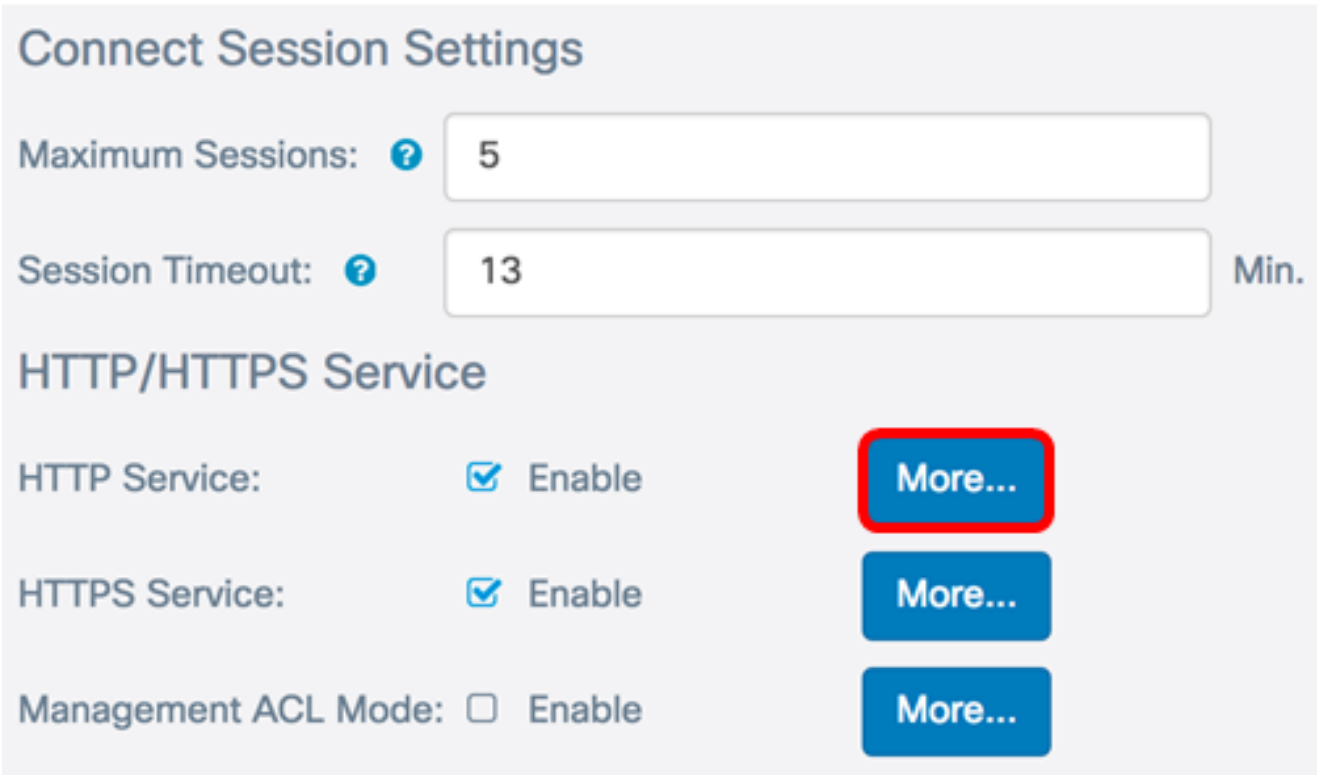


Serviço HTTP

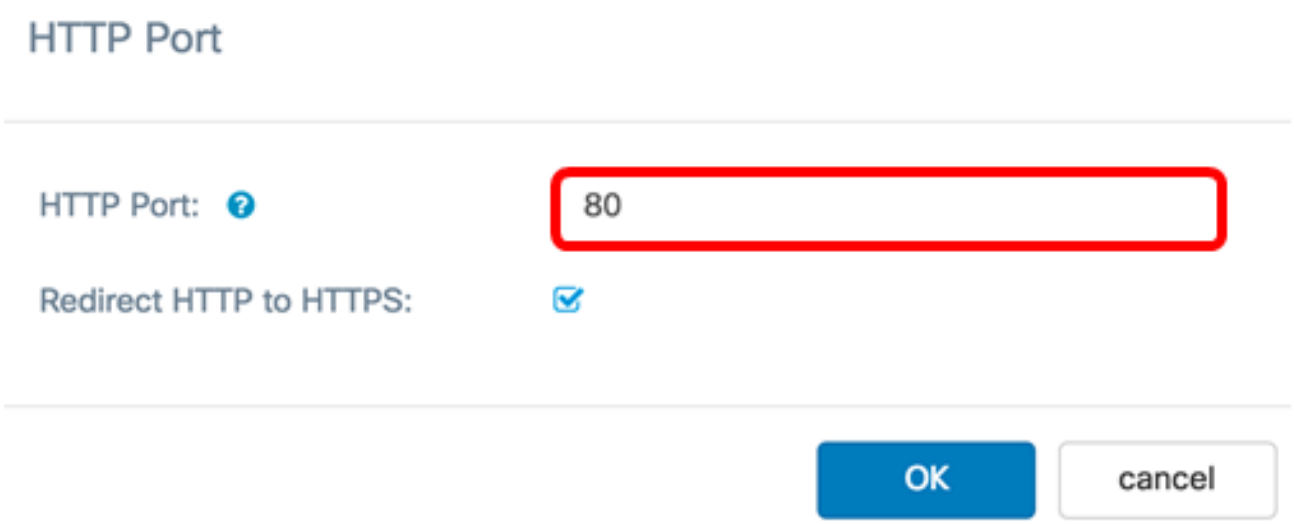
Etapa 5. Verifique a caixa de verificação do serviço da **possibilidade** HTTP para permitir que as sessões da web sejam conectadas com o HTTP.



Clique (opcional) de etapa 6. **mais** para ver mais opções e para configurar um número de porta.

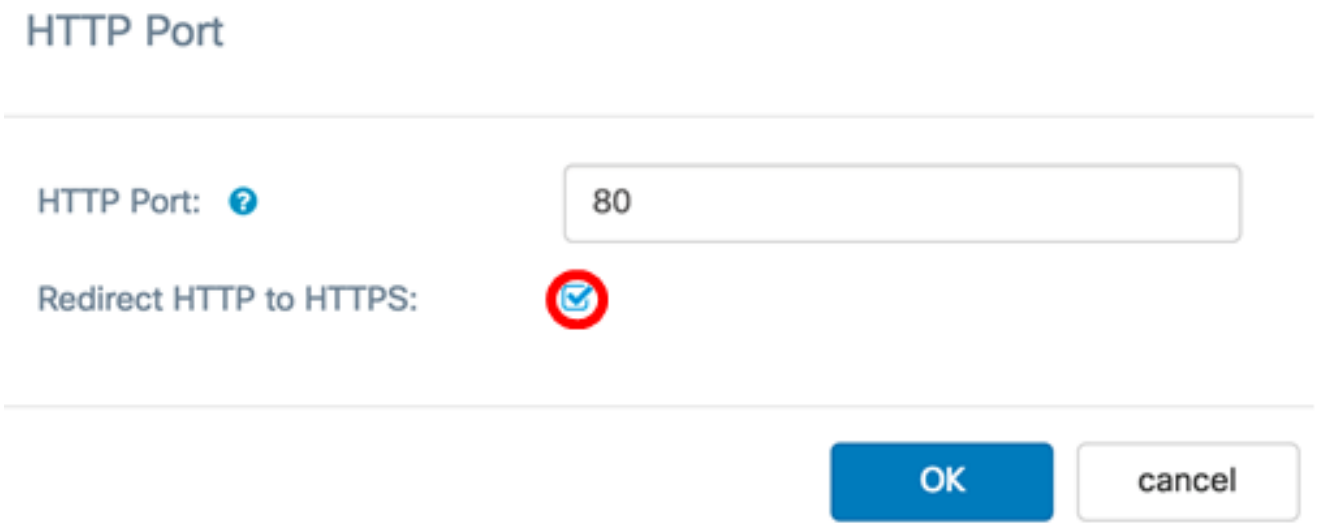


Passo 7. No campo de *porta de HTTP*, incorpore um número de porta lógica para usar-se para conexões de HTTP. O valor de porta varia desde 1025 a 65535. A porta bem conhecida do padrão para conexões de HTTP é 80.

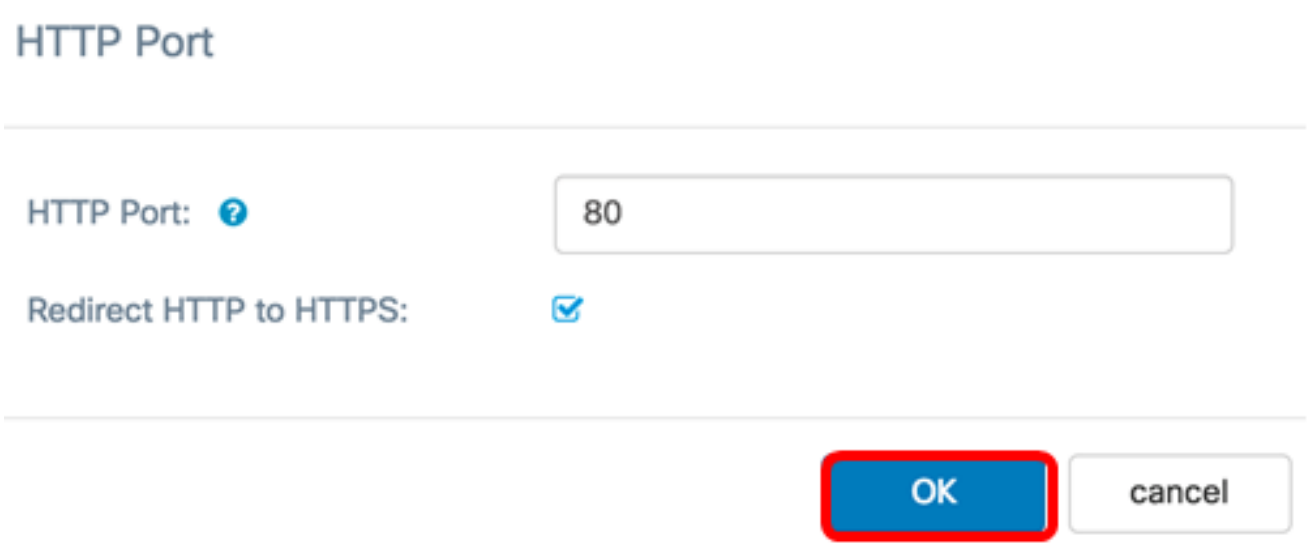


Verificação (opcional) de etapa 8. a **reorientação HTTP à caixa de verificação HTTPS** para permitir que o navegador reoriente-o a um protocolo mais seguro, HTTPS em cima de estabelecer uma sessão da web.

Nota: Esta opção está somente disponível se a caixa de verificação do serviço HTTP é desabilitada em etapa 4. Neste exemplo, esta opção é verificada.



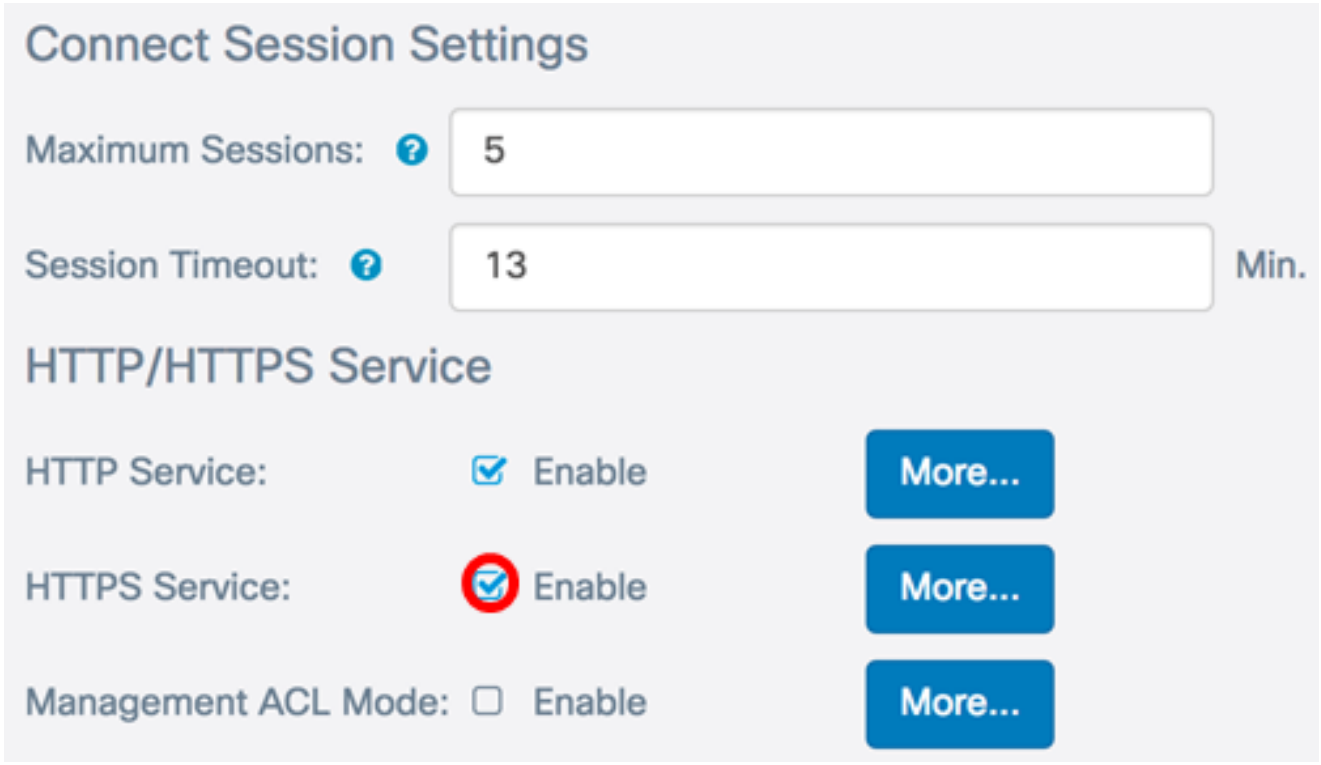
Etapa 9. Clique a **APROVAÇÃO** para retornar à página do Gerenciamento e para continuar com a configuração.



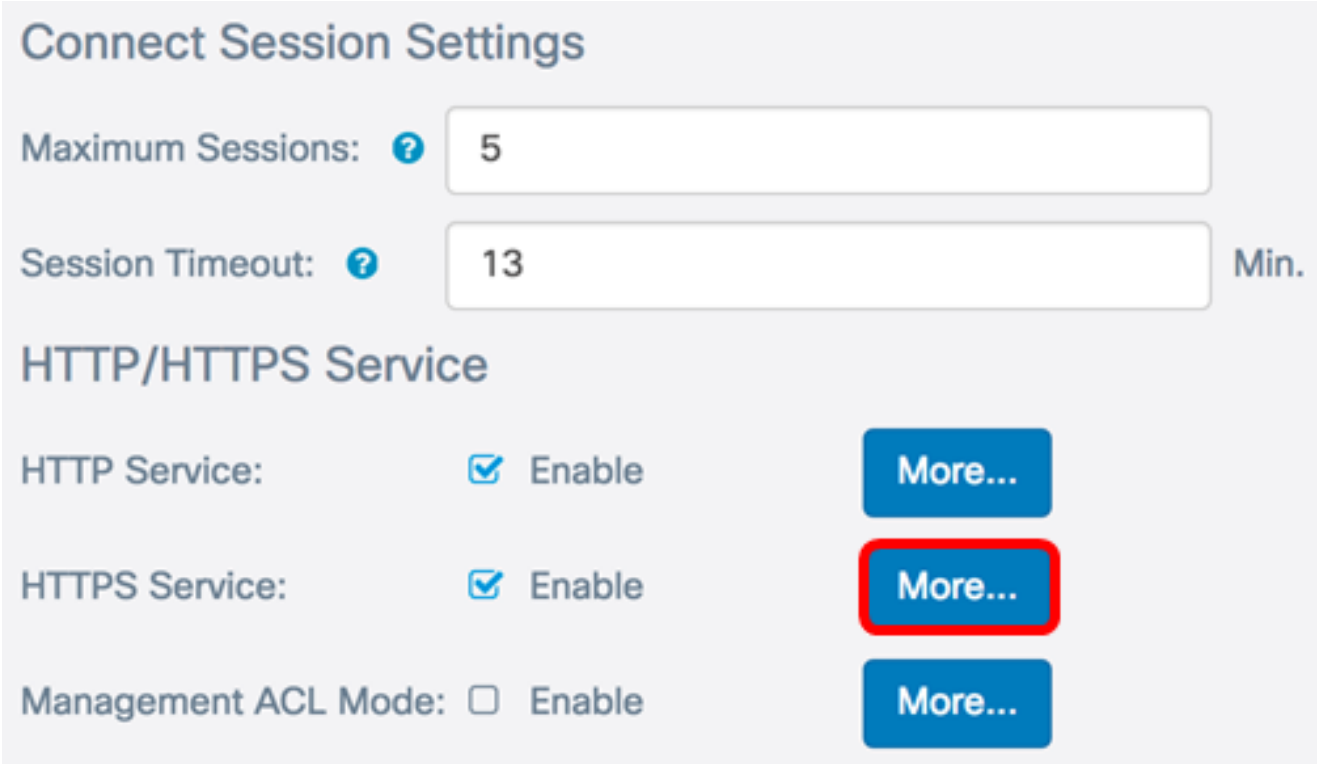
O HTTPS presta serviços de manutenção

Etapa 10. Verifique a caixa de verificação do serviço da **possibilidade** HTTPS para permitir que as sessões da web sejam estabelecidas com um protocolo fixado, HTTPS. Esta opção é permitida à revelia.

Nota: Se esta opção é desabilitada, todas as conexões existentes que usam o HTTPS estão desligadas.



Etapa 11. Clique **mais** para definir uma porta a ser usada pelo HTTPS e para escolher as versões do Transport Layer Security a ser usadas no HTTPS.

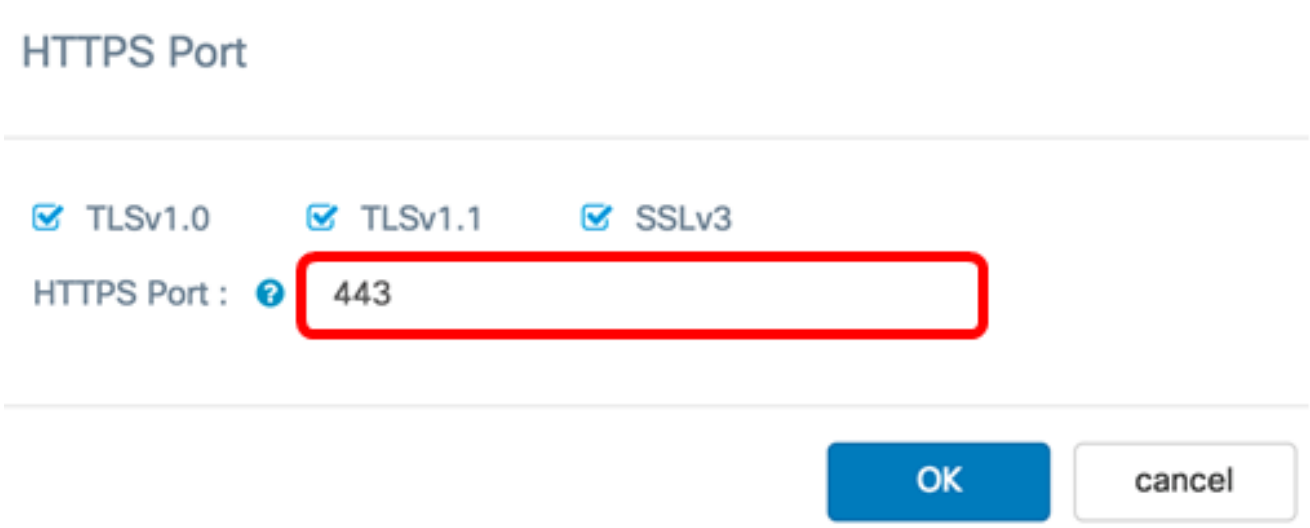


Etapa 12. Sob a área de porta HTTPS, verifique as caixas de seleção dos seguintes protocolos de segurança que são usados sobre o HTTPS:

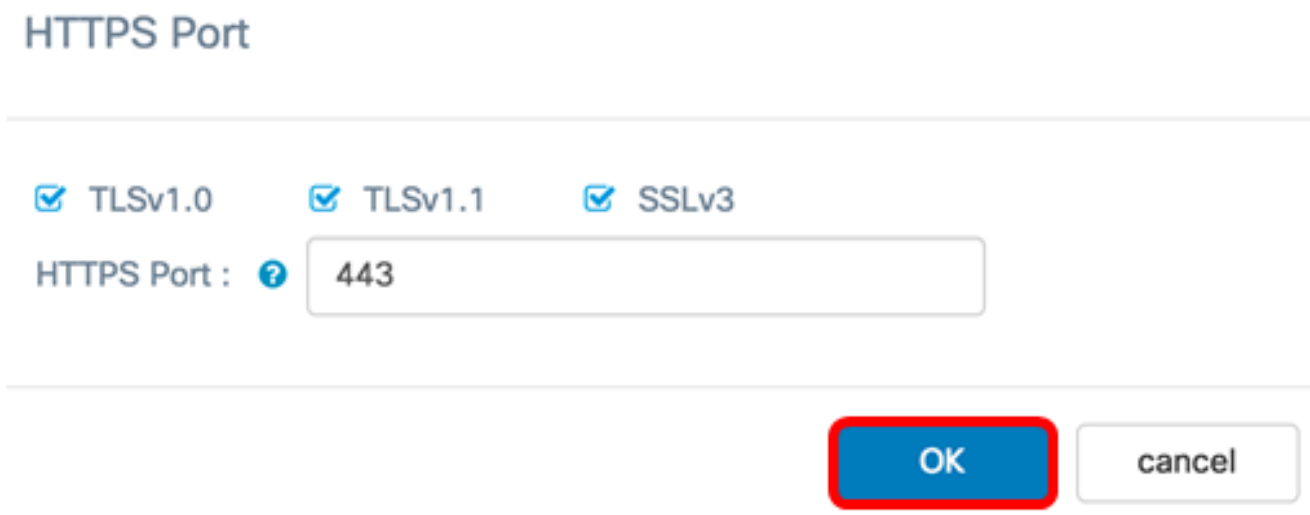
- TLSv1.0 — A versão 1 do Transport Layer Security (TLSv1) é um protocolo criptograficamente que forneça a Segurança e a integridade de dados para uma comunicação sobre o Internet.
- TLSv1.1 — Uma versão melhorada da primeira versão do TSLv1, melhora a segurança de dados e a integridade para uma comunicação.
- SSLv3 — A versão 3 fixada da camada de soquete (SSLv3) é um protocolo que seja usado sobre o HTTPS para estabelecer sessões e uma comunicação fixadas sobre o Internet.

Nota: Neste exemplo, todas as caixas de seleção são verificadas.

Etapa 13. No campo de *porta HTTPS*, incorpore um número de porta lógica para usar-se para conexões de HTTPS. A porta bem conhecida do padrão é 443.

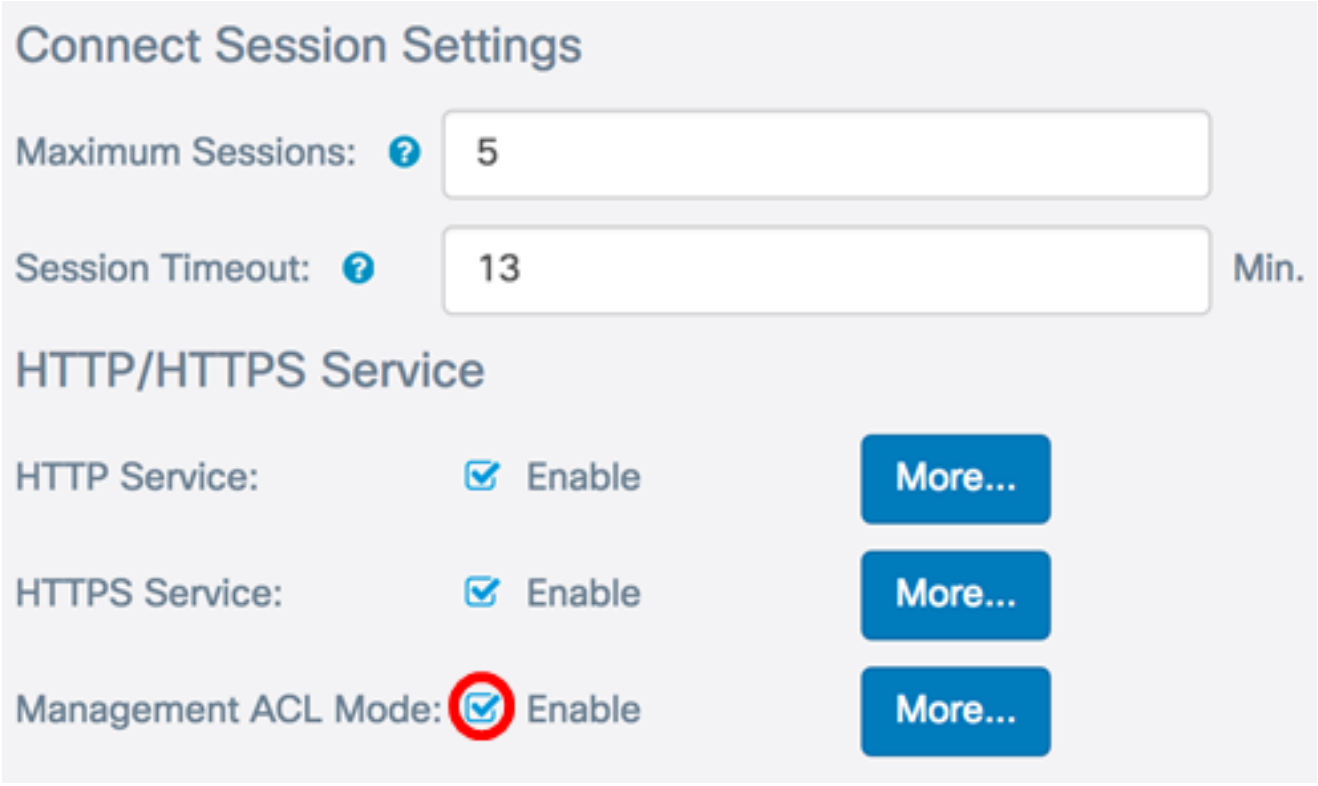


Etapa 14. Clique em OK para continuar.

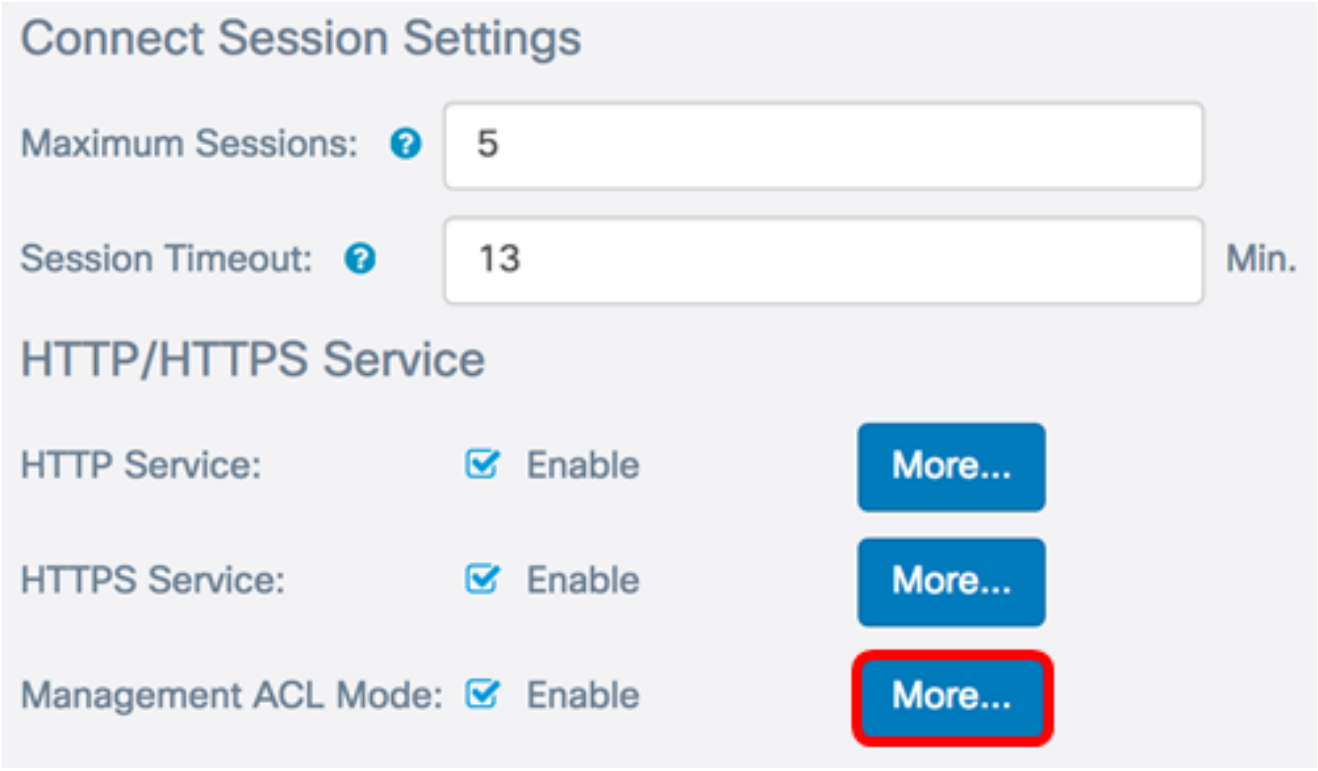


Modo do Gerenciamento ACL

Etapa 15. Verifique a caixa de verificação do modo da **possibilidade** ACL para especificar um Access Control List (ACL) dos endereços IP de Um ou Mais Servidores Cisco ICM NT que são permitidos para alcançar a utilidade com base na Web. Se esta característica é desabilitada, a seguir esta concede o acesso à utilidade com base na Web.



Etapa 16. Clique **mais** para especificar uma lista de endereços do IPv4 e do IPv6 permitidos para alcançar a utilidade com base na Web.

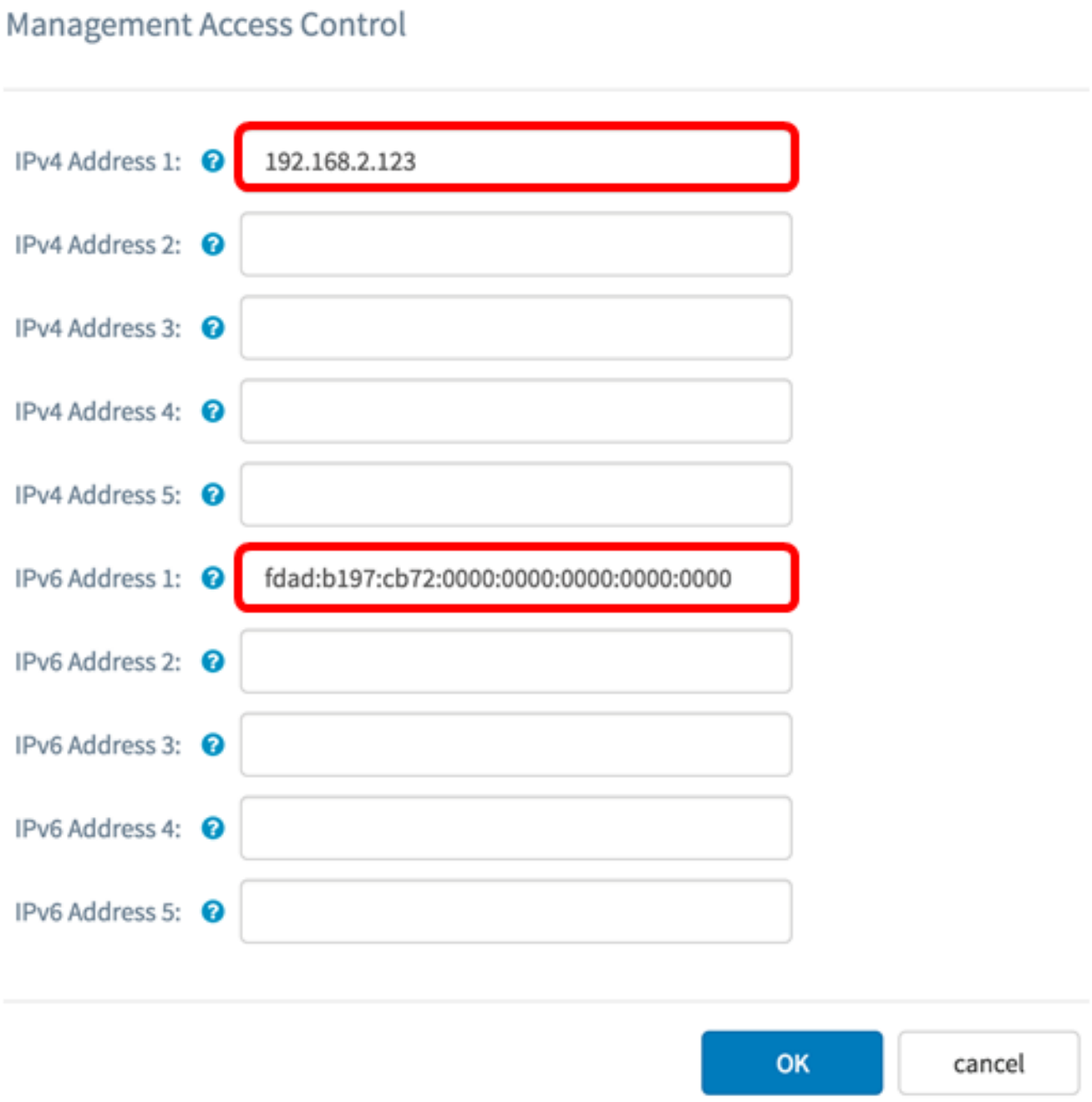


Etapa 17. *No endereço do IPv4* e nos *campos de endereço do IPv6*, incorpore os endereços IP de Um ou Mais Servidores Cisco ICM NT administrativos aos formatos respectivos que serão concedidos o acesso à utilidade com base na Web.

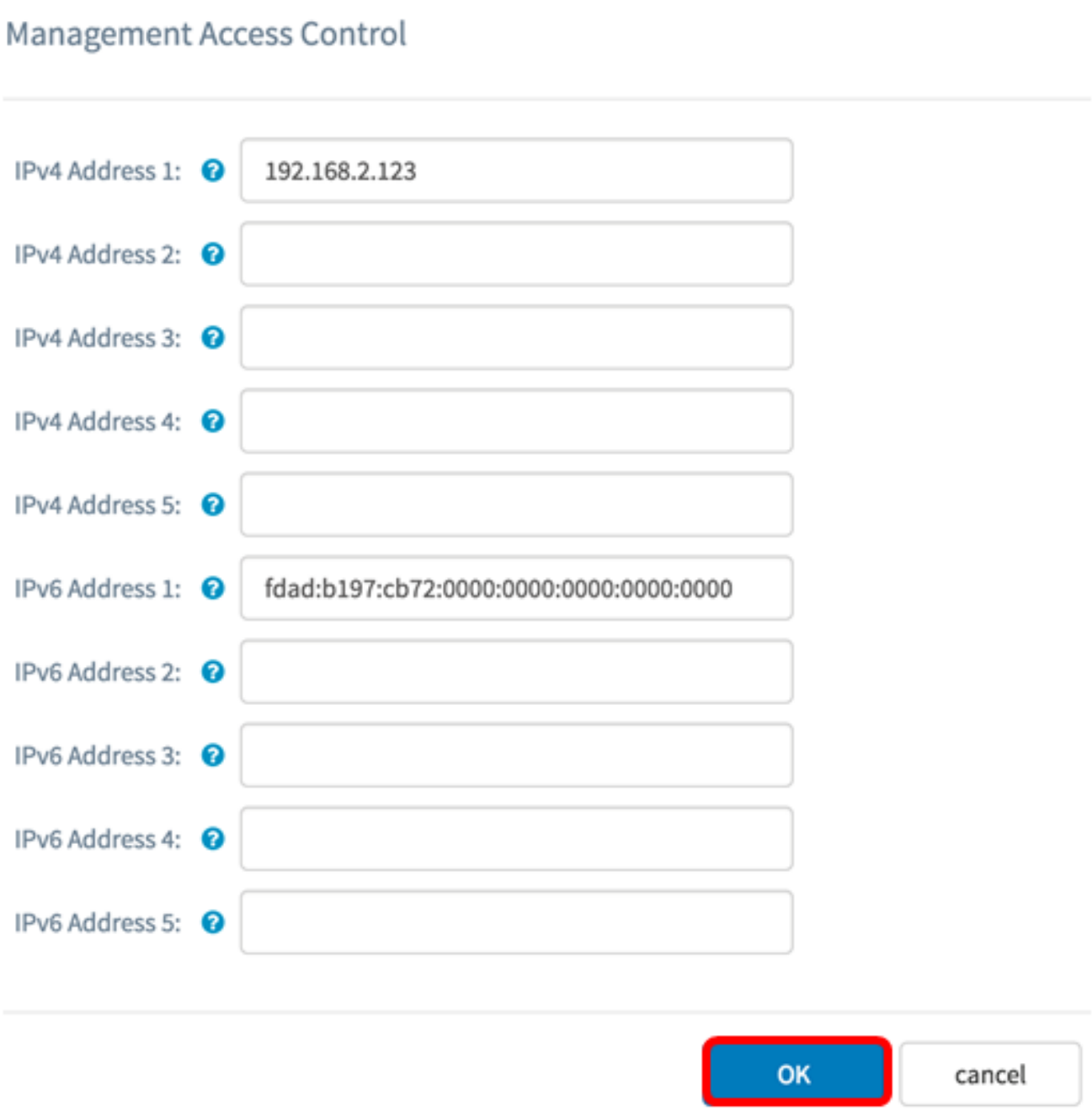
Dica: Atribua endereços IP estáticos aos endereços IP de Um ou Mais Servidores Cisco ICM NT administrativos.

Nota: Neste exemplo, 192.168.2.123 é usado enquanto o endereço do IPv4 e o fdad:b197:cb72:0000:0000:0000:0000:0000 administrativos são usados como o endereço

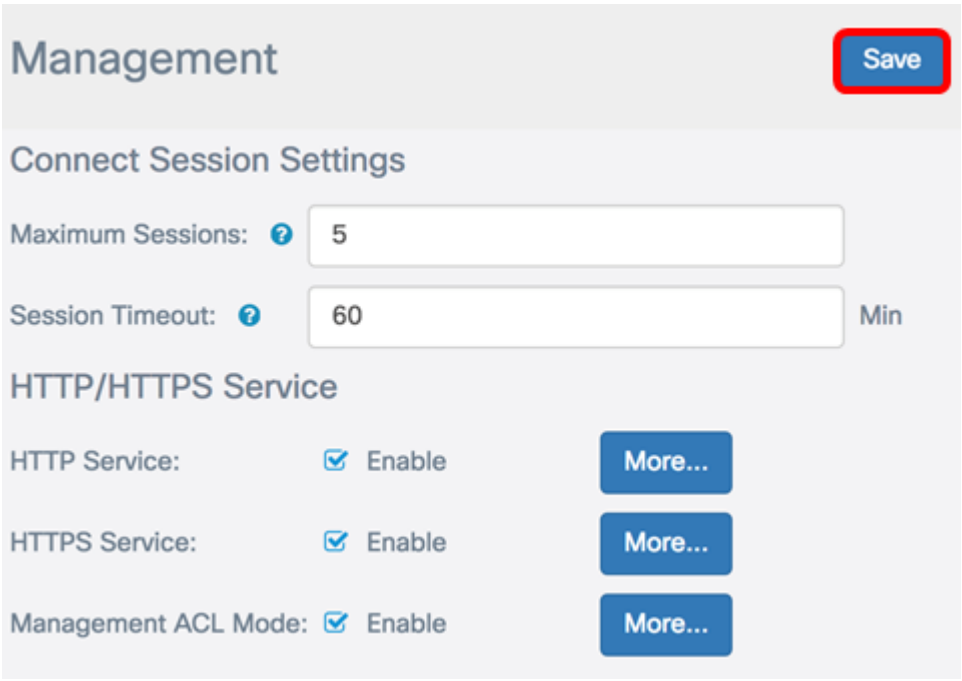
administrativo do IPv6.



Etapa 18. Clique em **OK**.



Etapa 19. **Botão Save Button do** clique para salvar os ajustes configurados.



Você deve agora com sucesso ter configurado a tarefa do serviço HTTP/HTTPS em seu Access point WAP125 ou WAP581.