Gerenciar certificados no FindIT Network Manager

Objetivo

Um certificado digital certifica a propriedade de uma chave pública pelo assunto nomeado do certificado. Isso permite que as partes confiáveis dependam de assinaturas ou asserções feitas pela chave privada que corresponda à chave pública certificada. Após a instalação, o FindIT Network Manager gera um certificado autoassinado para proteger a Web e outras comunicações com o servidor. Você pode optar por substituir este certificado pelo certificado assinado por uma autoridade de certificação (AC) confiável. Para fazer isso, você precisará gerar uma solicitação de assinatura de certificado (CSR) para assinar pela CA.

Você também pode optar por gerar um certificado e a chave privada correspondente completamente independente do Gerenciador. Em caso afirmativo, você pode combinar o certificado e a chave privada em um arquivo de formato PKCS (Public Key Cryptography Standards) #12 antes do upload.

O FindIT Network Manager só suporta certificados de formato .pem. Se você obtiver outros formatos de certificado, precisará converter novamente o formato ou solicitar o certificado de formato .pem da CA.

Este artigo fornece instruções sobre como gerenciar certificados no FindIT Network Manager.

Dispositivos aplicáveis

- FindIT Network Manager

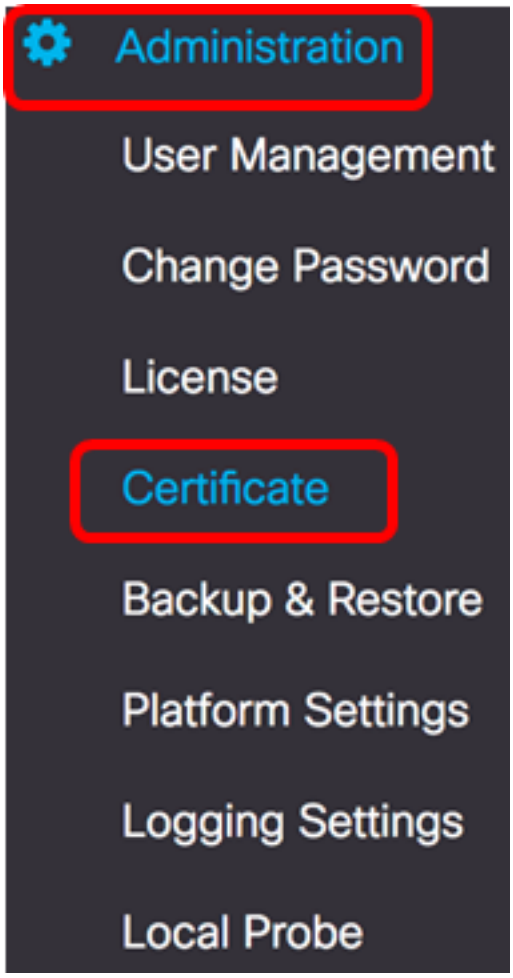
Versão de software

- 1.1

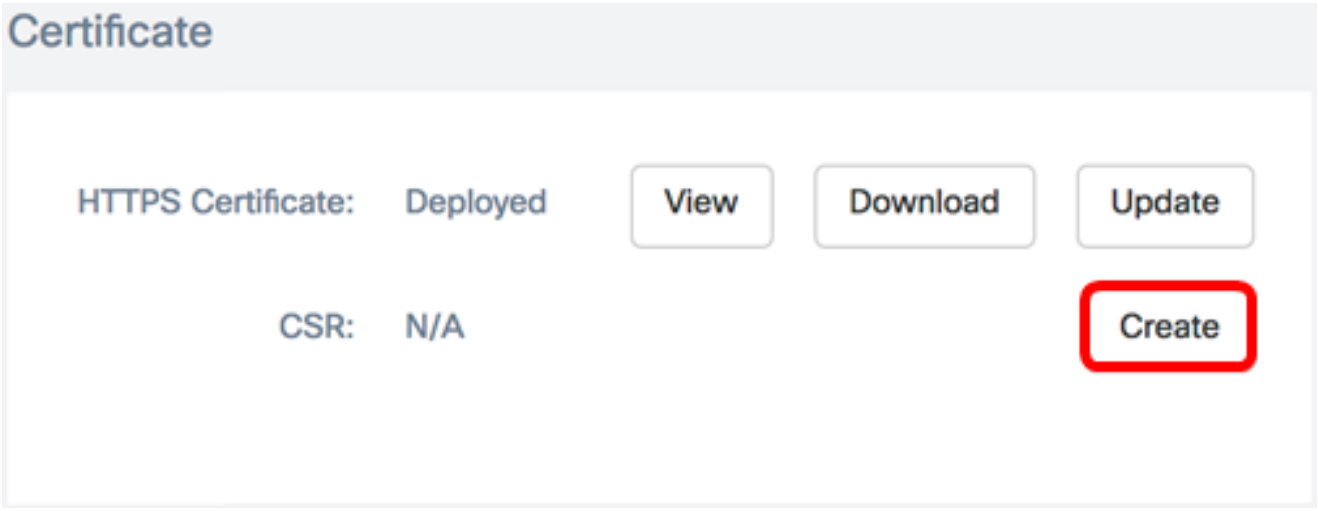
Gerenciar certificados no FindIT Network Manager

Gerar um CSR

Etapa 1. Faça login na GUI de administração do FindIT Network Manager e escolha **Administration > Certificate**.



Etapa 2. Na área CSR, clique no botão **Create (Criar)**.



Os valores inseridos no formulário de certificado serão usados para construir o CSR e estarão contidos no certificado assinado que você recebe da CA.

Etapa 3. Insira o endereço IP ou o nome de domínio no campo *Nome de domínio qualificado completo*. Neste exemplo, hostname.cisco.com é usado.

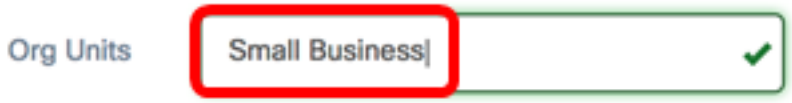
Etapa 4. Insira o código do país no campo *País*. Neste exemplo, US é usado.

Etapa 5. Insira o código de estado no campo *Estado*. Neste exemplo, CA é usado.

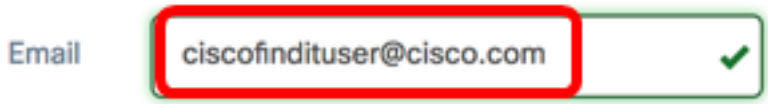
Etapa 6. Digite a cidade no campo *Cidade*. Neste exemplo, é usado Irvine.

Passo 7. Digite o nome da organização no campo *Org*. Neste exemplo, a Cisco é usada.

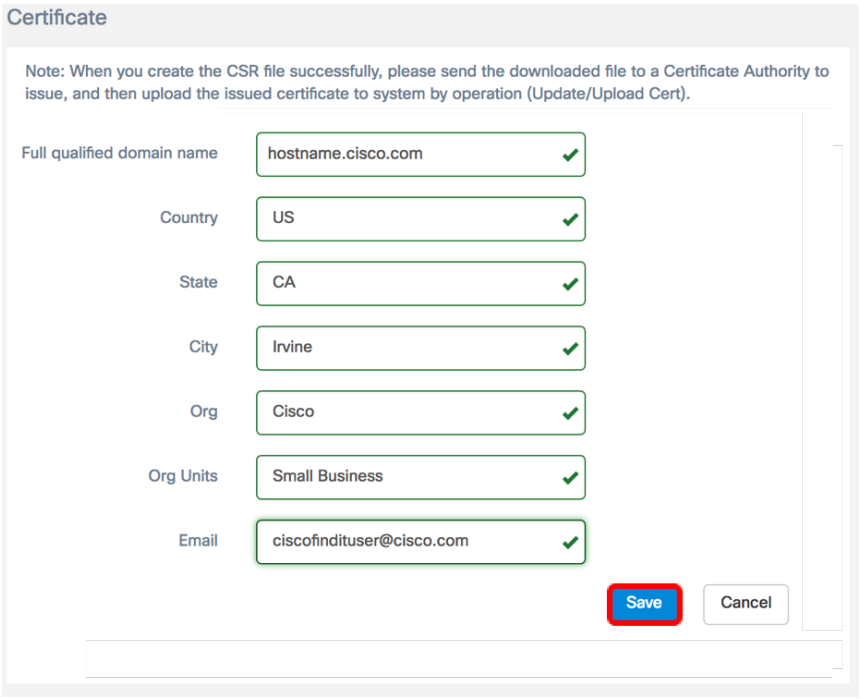
Etapa 8. Insira as unidades da organização no campo *Unidades da organização*. Neste exemplo, Pequenas empresas são usadas.



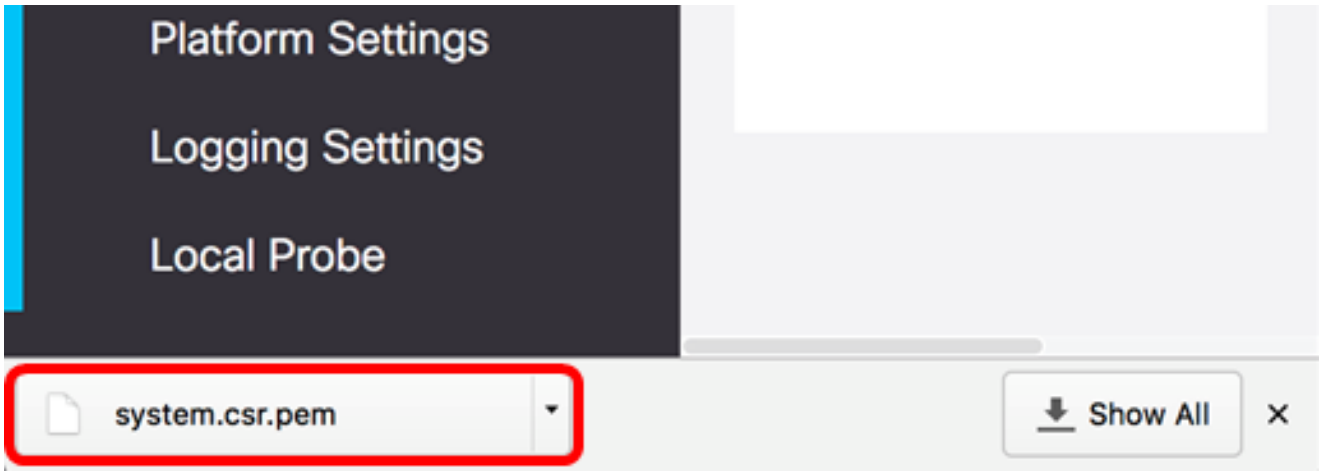
Etapa 9. Digite seu endereço de e-mail no campo *Email*. Neste exemplo, ciscofindituser@cisco.com é inserido.



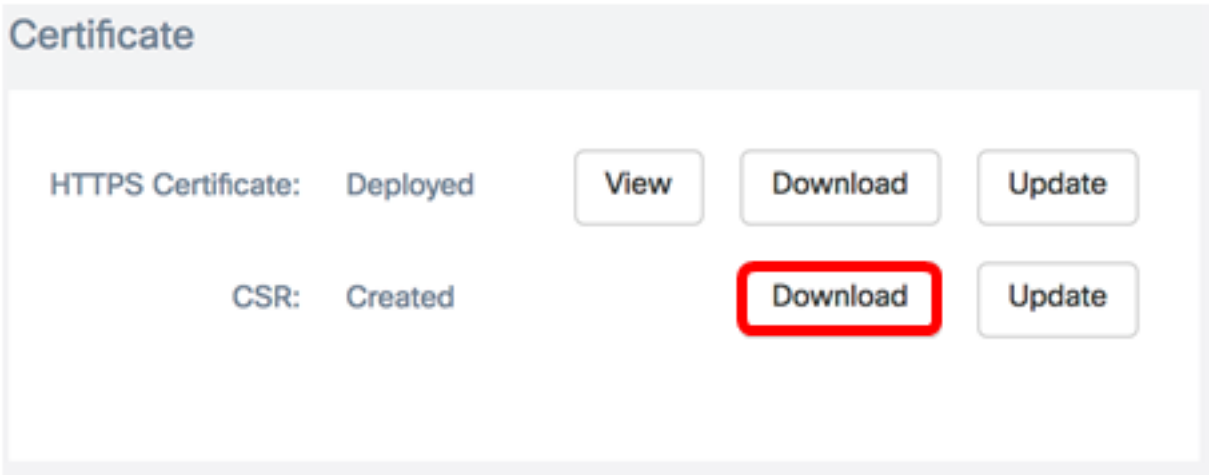
Etapa 10. Click **Save**.



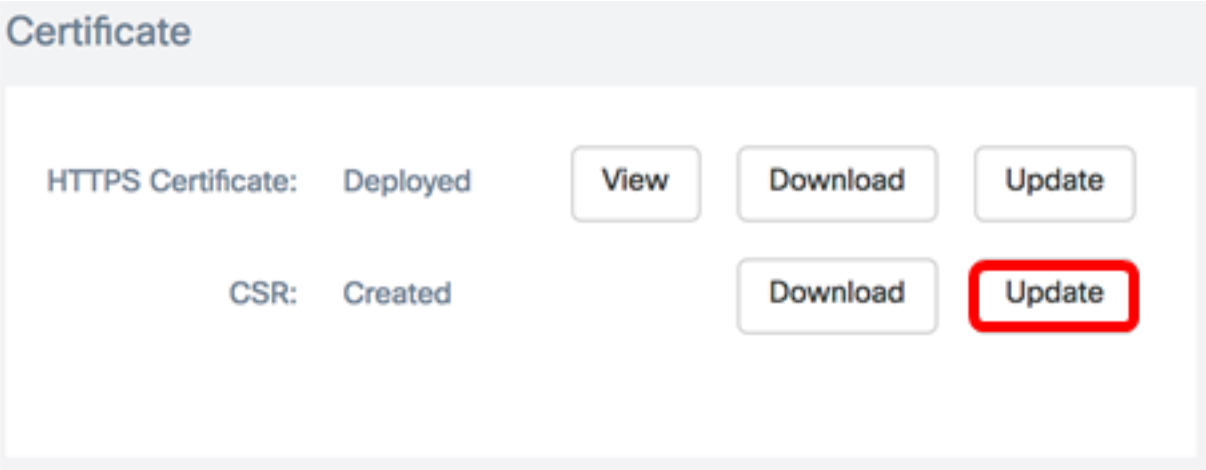
O arquivo CSR será baixado automaticamente em seu computador. Neste exemplo, o arquivo system.csr.pem é gerado.



Etapa 11. (Opcional) Na área CSR, o status será atualizado de N/A para Criado. Para baixar o CSR criado, clique no botão **Download**.



Etapa 12. (Opcional) Para atualizar o CSR criado, clique no botão **Atualizar** e retorne à Etapa 3.

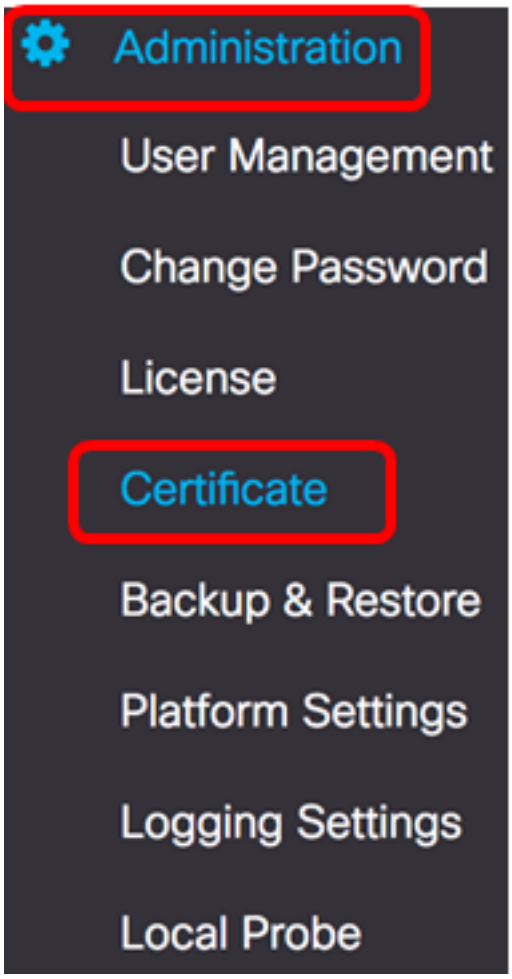


Agora você deve ter gerado com êxito um CSR no FindIT Network Manager. Agora você pode enviar o arquivo CSR baixado para a CA.

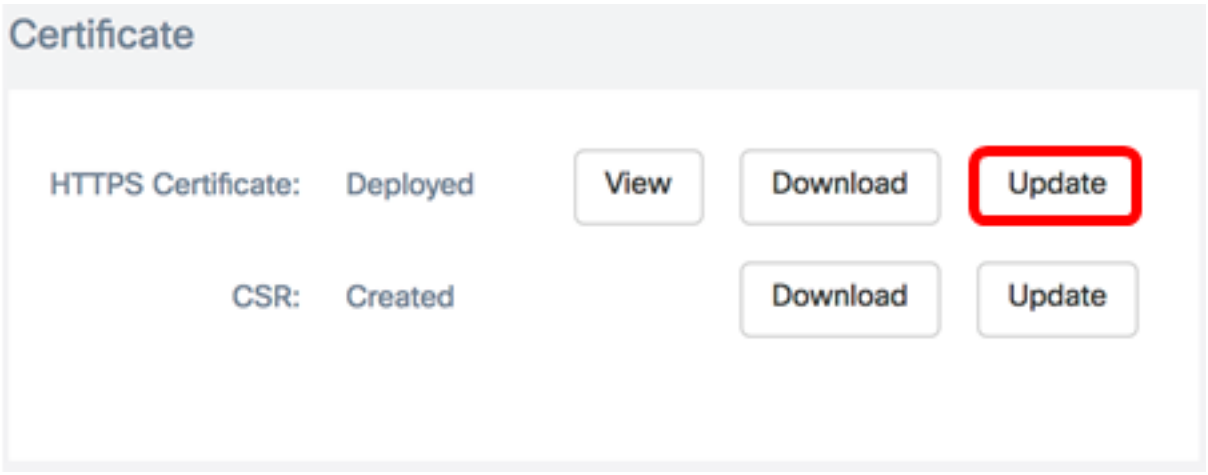
Carregar um certificado assinado da CA

Depois de receber o CSR assinado da CA, você pode agora carregá-lo para o gerente.

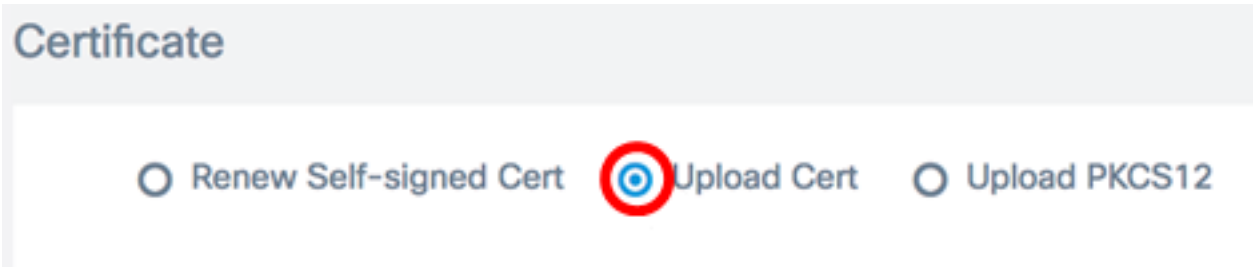
Etapa 1. Faça login na GUI de administração do FindIT Network Manager e escolha **Administration > Certificate**.



Etapa 2. Na área Certificado HTTPS, clique no botão **Atualizar**.

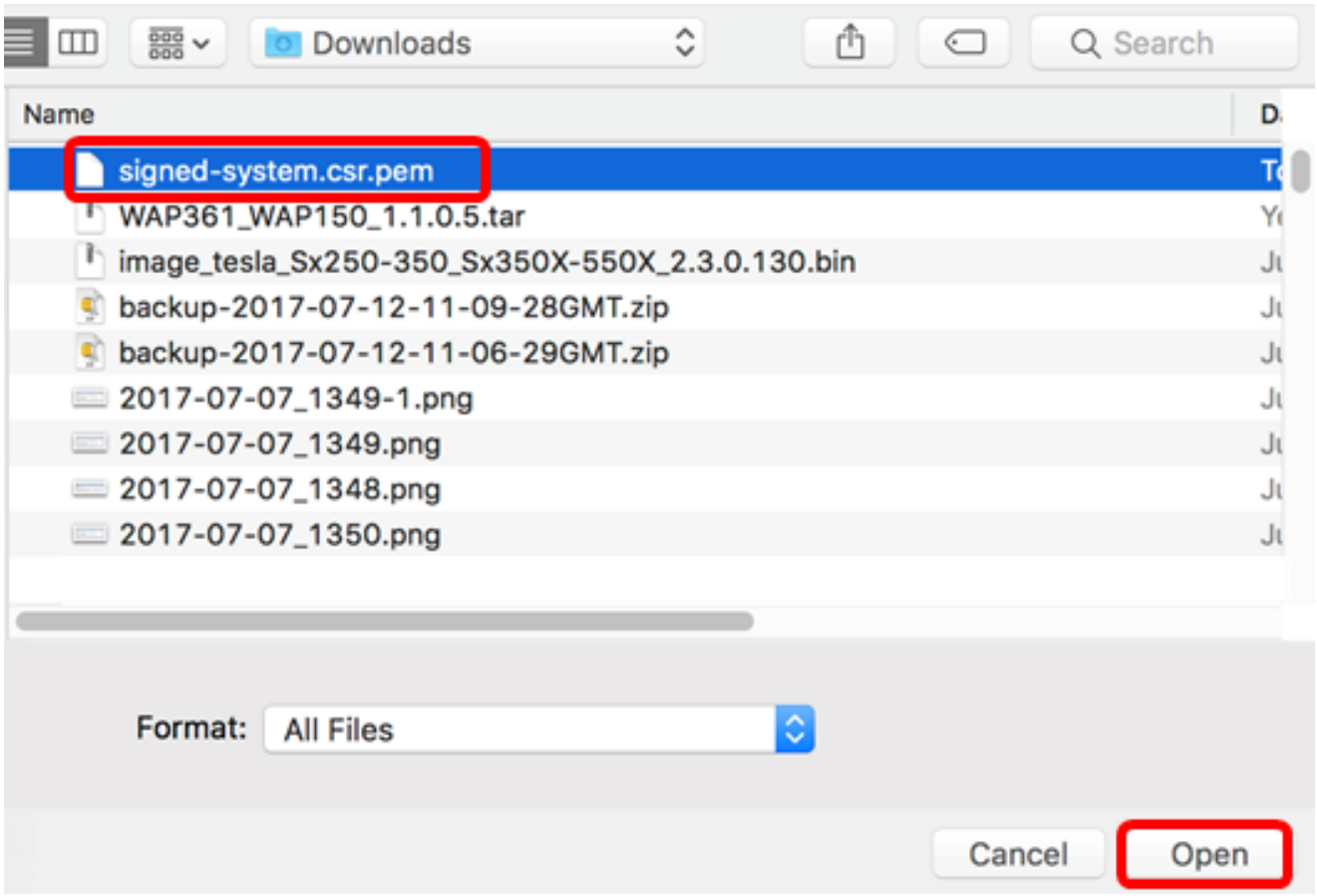


Etapa 3. Clique no botão de opção **UploadCert**.



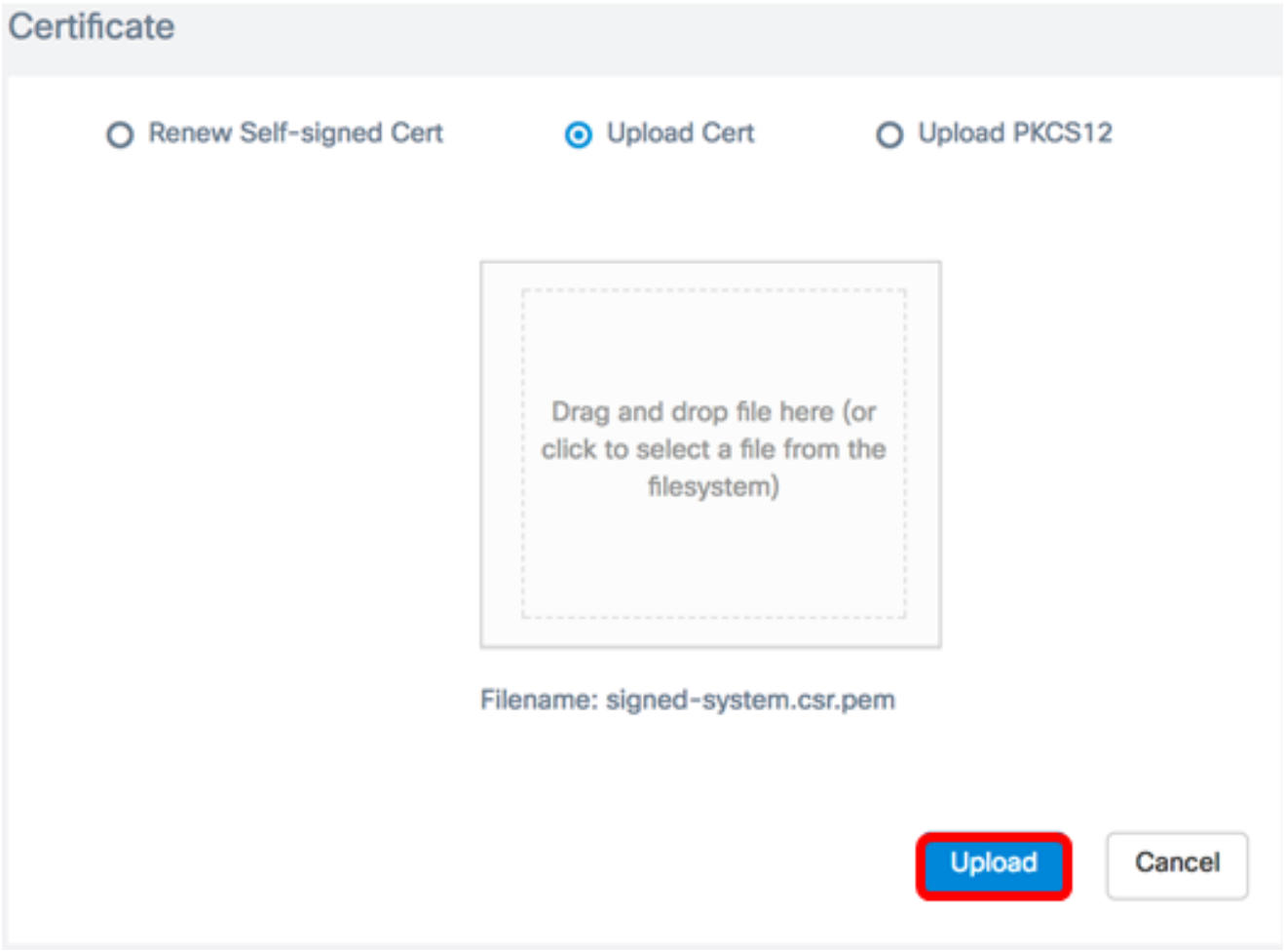
Note: Como alternativa, você pode carregar um certificado com a chave privada associada no formato PKCS#12 escolhendo o botão de opção **Upload PKCS12**. A senha para desbloquear o arquivo deve ser especificada no campo *Senha* fornecido.

Etapa 4. Solte o certificado assinado na área de destino ou clique na área de destino para navegar pelo sistema de arquivos e clique em **Abrir**. O arquivo deve estar no formato .pem.



Note: Neste exemplo, signed-system.csr.pem é usado.

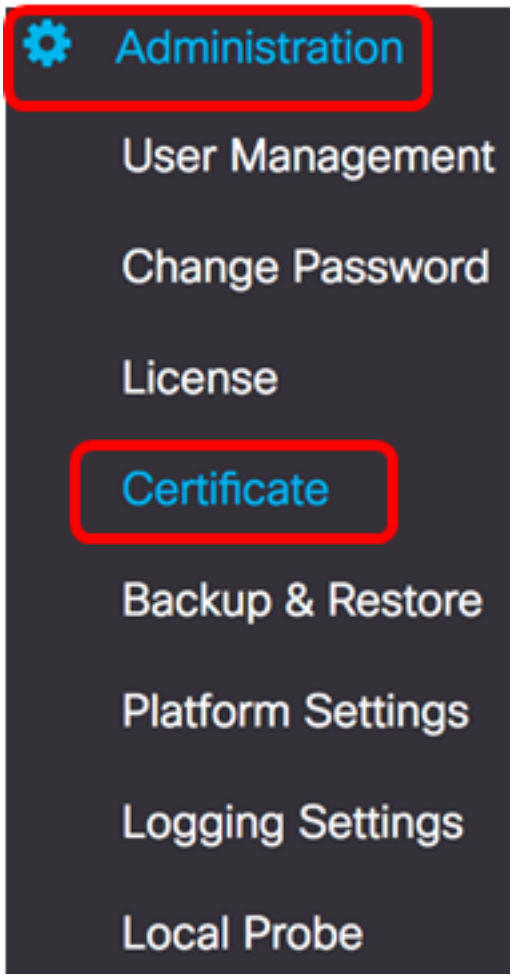
Etapa 5. Clique em **Fazer upload**.



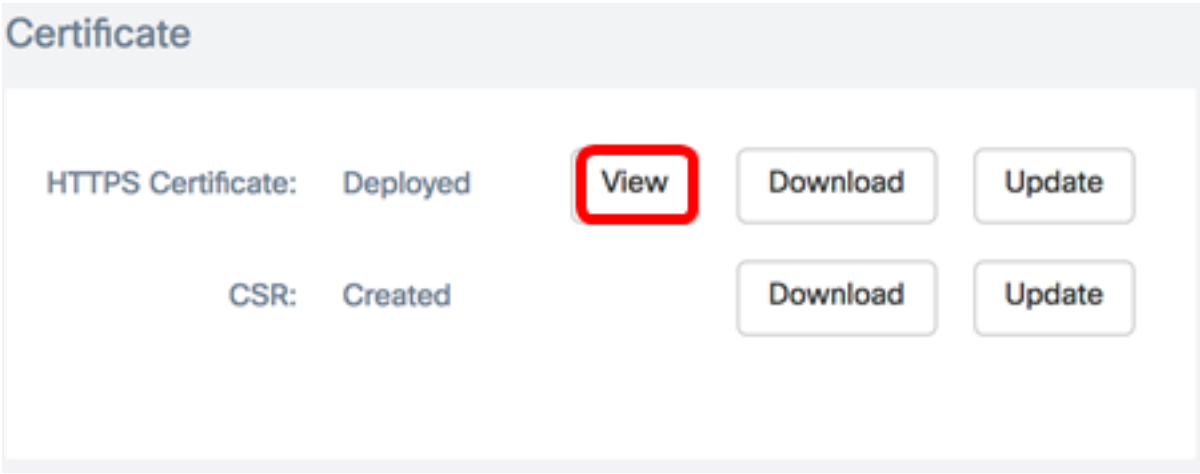
Agora você deve ter carregado com êxito um certificado assinado no FindIT Network Manager.

Gerenciar certificado atual

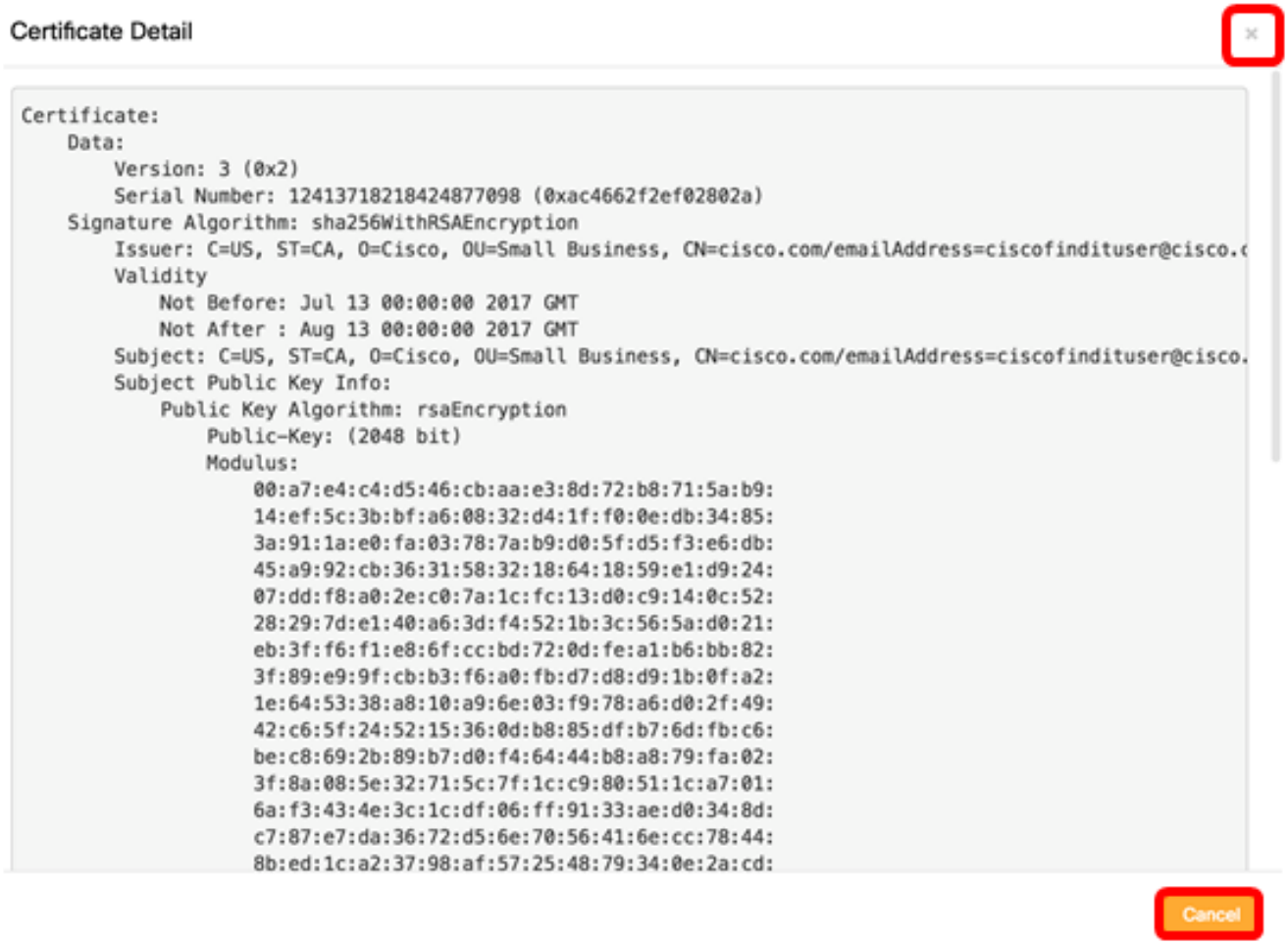
Etapa 1. Faça login na GUI de administração do FindIT Network Manager e escolha **Administration > Certificate**.



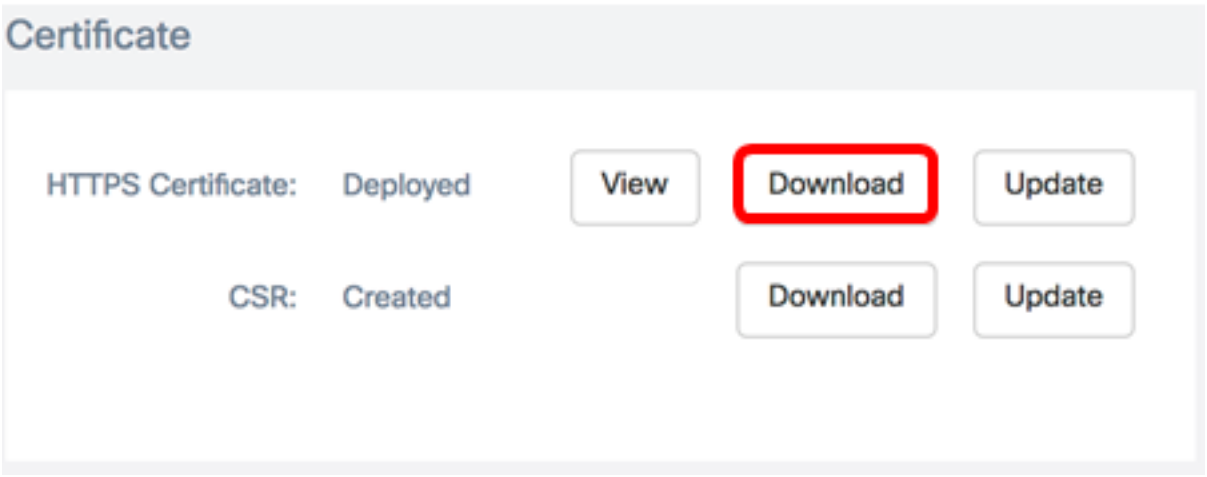
Etapa 2. Na área Certificado HTTPS, clique no botão **Exibir**.



Etapa 3. O certificado atual será exibido em formato de texto simples em uma nova janela do navegador. Clique no botão **x** ou **Cancel** para fechar a janela.



Etapa 4. (Opcional) Para baixar uma cópia do certificado atual, clique no botão **Download** na área Certificado HTTPS.



Agora você deve ter gerenciado com êxito o certificado atual no FindIT Network Manager.