Controle Certificados na gerente de rede de FindIT

Objetivo

Um certificado digital certifica a posse de uma chave pública pelo assunto Nomeado do certificado. Isto permite que os partidos de confiança dependam em cima das assinaturas ou das afirmações feitas pela chave privada que corresponde à chave pública que é certificada. Em cima da instalação, a gerente de rede de FindIT gerencie um certificado auto-assinado para fixar a Web e a outra comunicação com o server. Você pode escolher substituir este certificado com esse assinado por um Certificate Authority (CA) confiado. Para fazer isto, você precisará de gerar uma solicitação de assinatura de certificado (CSR) para assinar por CA.

Você pode igualmente escolher gerar um certificado e a chave privada correspondente completamente independentes do gerente. Em caso afirmativo, você pode combinar o certificado e a chave privada em um erro de arquivo #12 dos padrões da criptografia de chave pública (PKCS) antes da transferência de arquivo pela rede.

A gerente de rede de FindIT apoia somente Certificados do formato do .pem. Se você obtém outros formatos do certificado, você precisa de converter outra vez o formato ou o pedido para o certificado do formato do .pem de CA.

Este artigo fornece instruções em como controlar Certificados na gerente de rede de FindIT.

Dispositivos aplicáveis

- Gerente de rede de FindIT

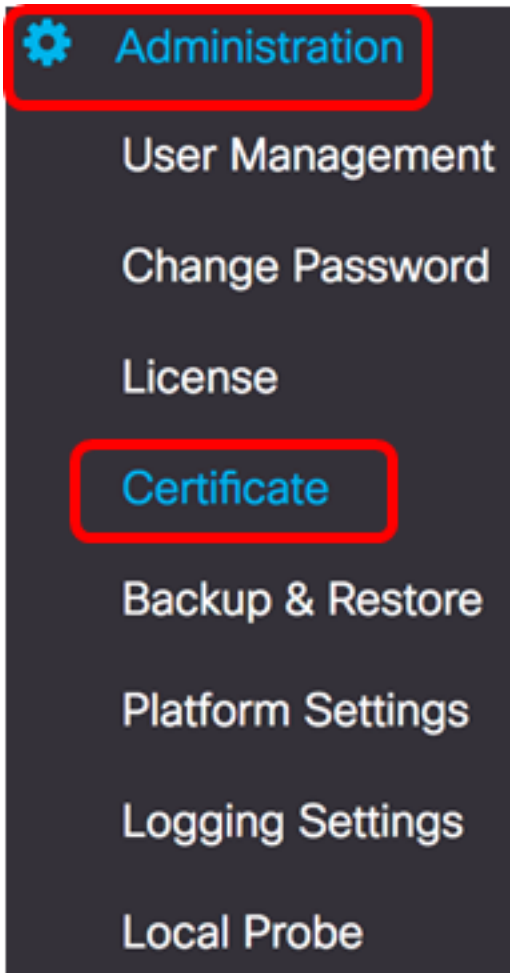
Versão de software

- 1.1

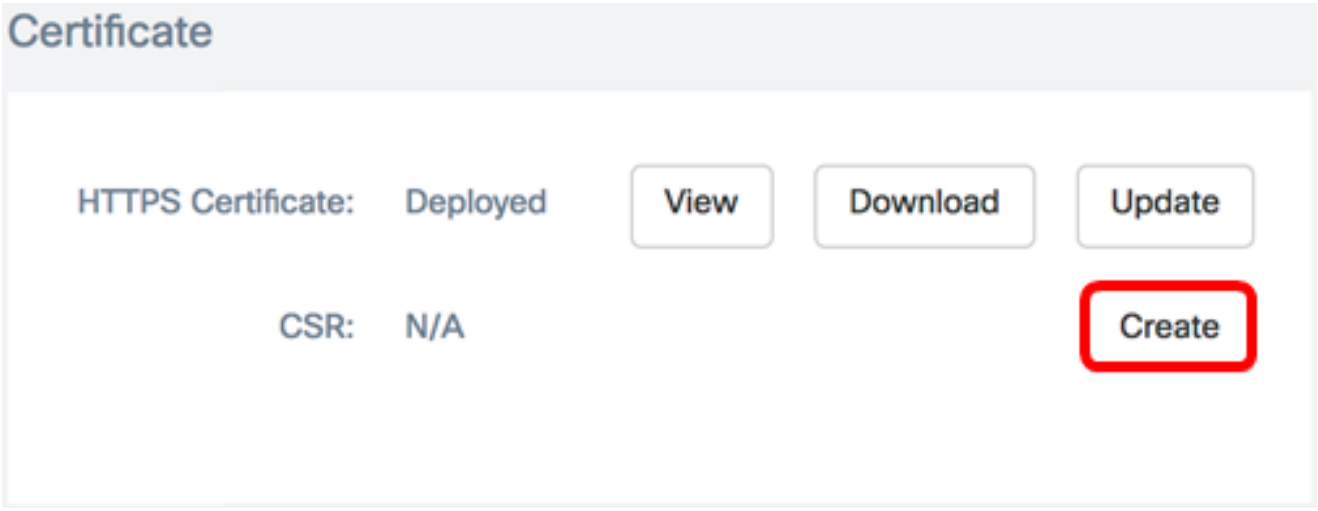
Controle Certificados na gerente de rede de FindIT

Gerencia um CSR

Etapa 1. O início de uma sessão à administração GUI de sua gerente de rede de FindIT escolhe então a **administração > o certificado**.



Etapa 2. Na área CSR, clique o **botão Create**.



Os valores incorporados ao formulário do certificado serão usados para construir o CSR, e contidos no certificado assinado que você recebe de CA.

Etapa 3. Incorpore o endereço IP de Um ou Mais Servidores Cisco ICM NT ou o Domain Name ao campo de *nome de domínio qualificado completo*. Neste exemplo, hostname.cisco.com é usado.

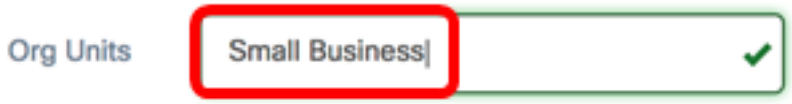
Etapa 4. Dê entrada ao código de país no campo do *país*. Neste exemplo, os E.U. são usados.

Etapa 5. Dê entrada ao código do estado no *campo de estado*. Neste exemplo, CA é usado.

Etapa 6. Entre na cidade no campo da *cidade*. Neste exemplo, Irvine é usado.

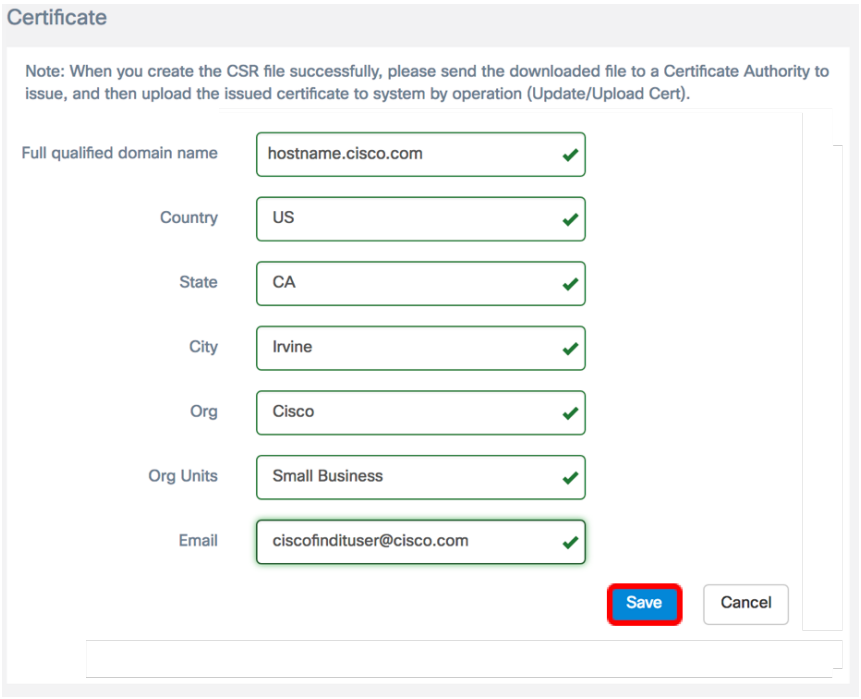
Etapa 7. Dê entrada com o nome de organização no campo do *org*. Neste exemplo, Cisco é usado.

Etapa 8. Incorpore as unidades da organização ao campo das *unidades do org*. Neste exemplo, a empresa de pequeno porte é usada.

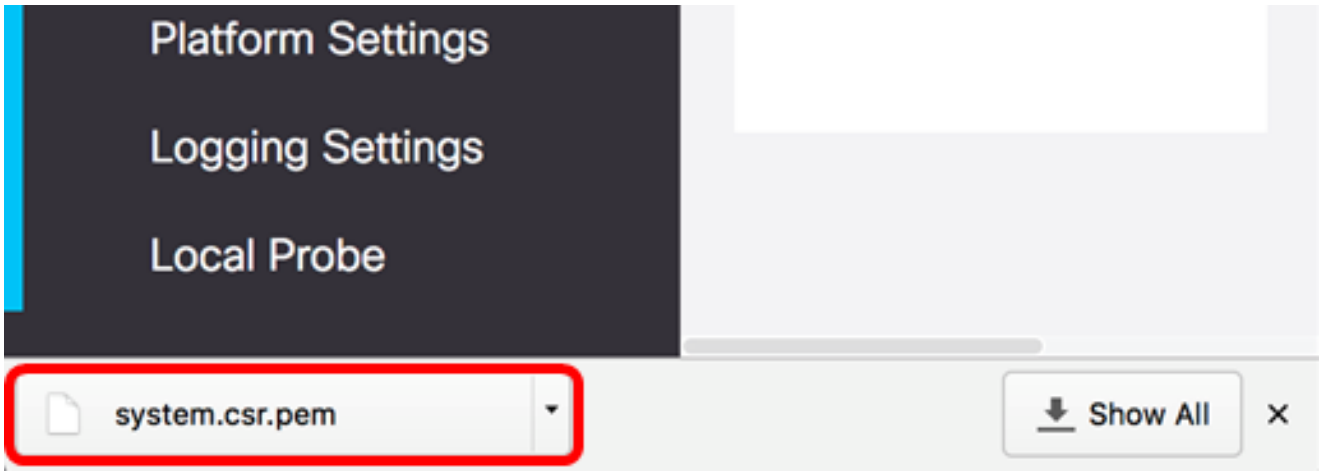


Etapa 9. Incorpore seu endereço email ao campo do *email*. Neste exemplo, ciscofinduser@cisco.com é entrado.

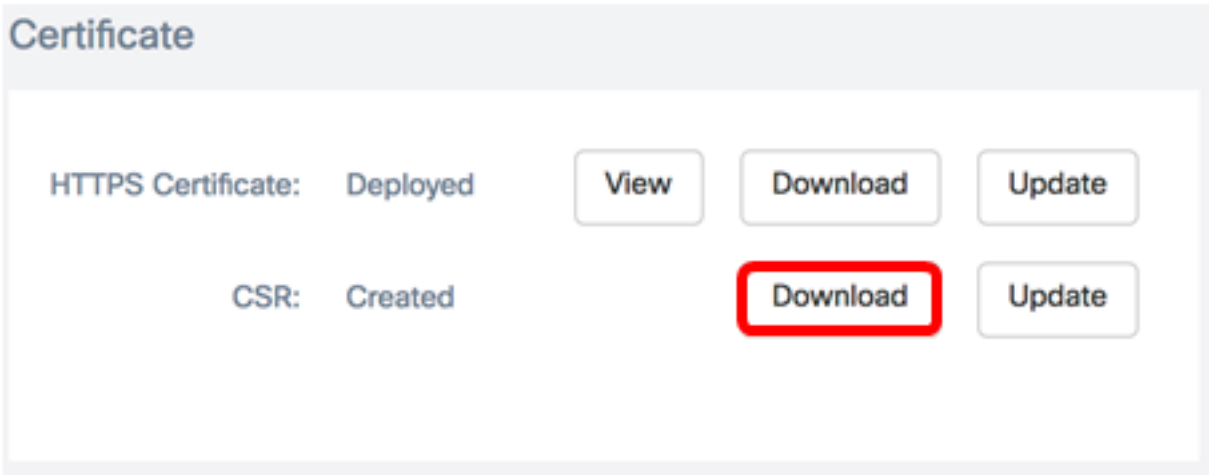
Etapa 10. **Salvaguarda do** clique.



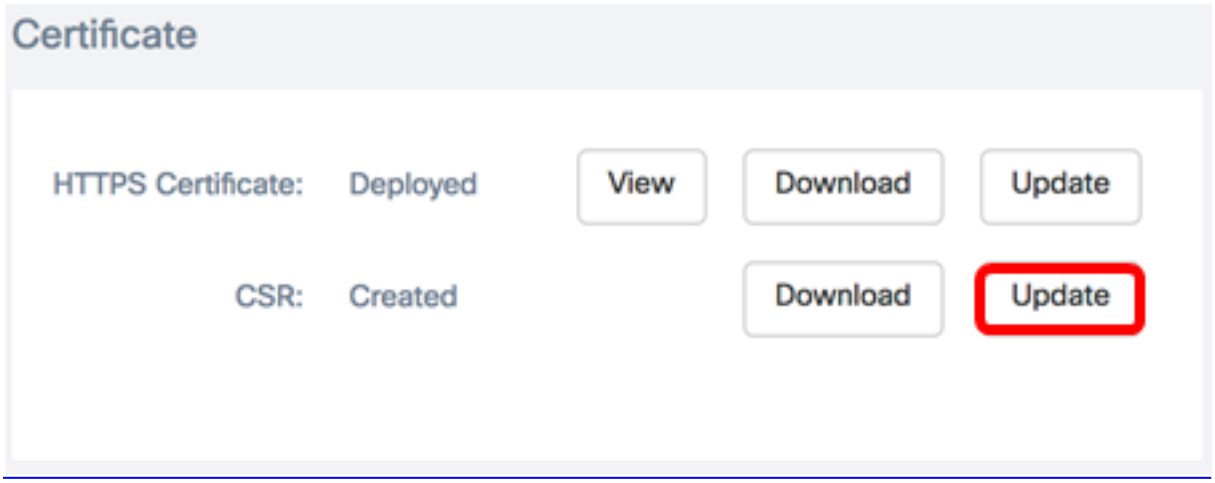
O arquivo CSR será transferido automaticamente a seu computador. Neste exemplo, o arquivo system.csr.pem é gerado.



Etapa 11. (opcional) na área CSR, o estado será atualizada do N/A ao criado. Para transferir o CSR criado, clique o botão da **transferência**.



Etapa 12. (Opcional) para atualizar o CSR criado, clique o **botão Update Button** a seguir retorne a etapa 3.

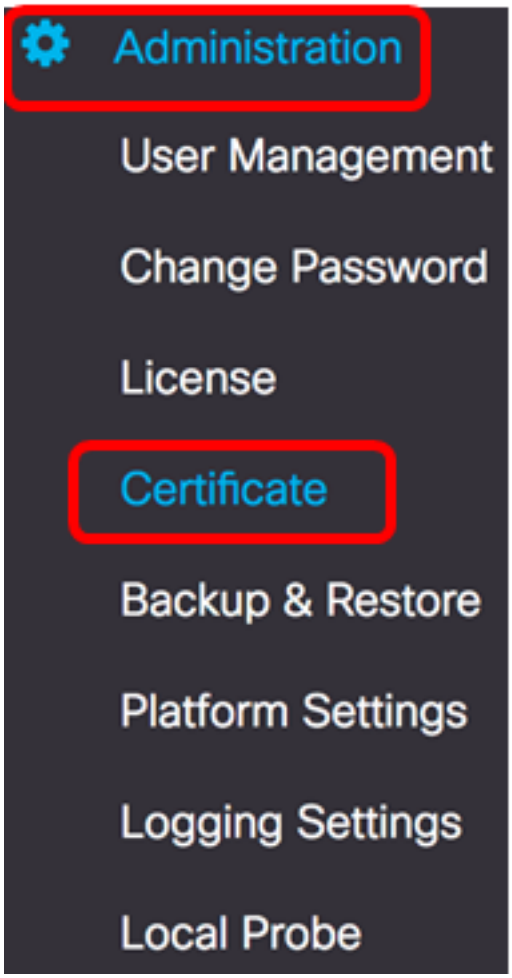


Você deve agora com sucesso ter gerado um CSR em sua gerente de rede de FindIT. Você pode agora enviar o arquivo transferido CSR a CA.

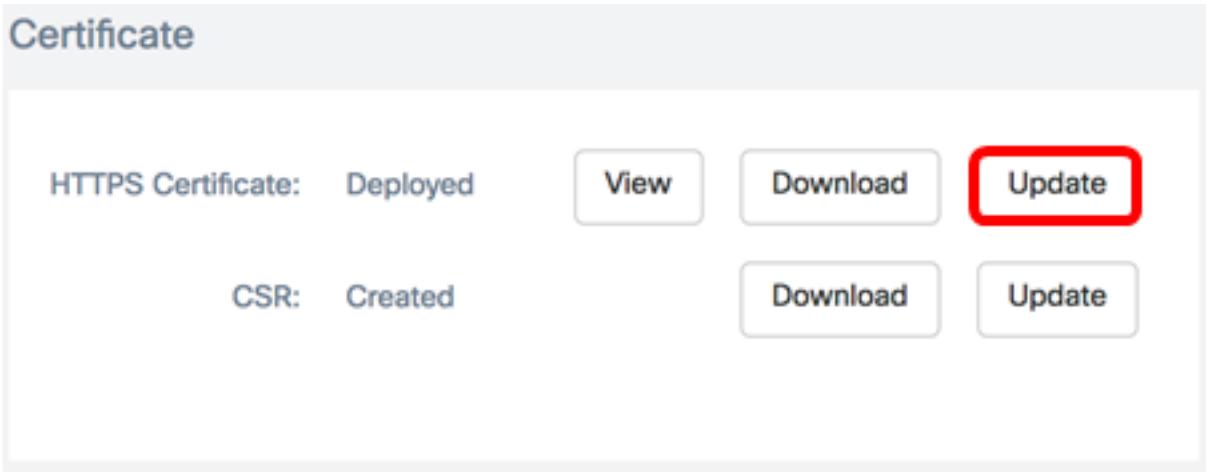
Transfira arquivos pela rede um certificado assinado de CA

Uma vez que você recebe o CSR assinado de CA, você pode agora transferi-lo arquivos pela rede ao gerente.

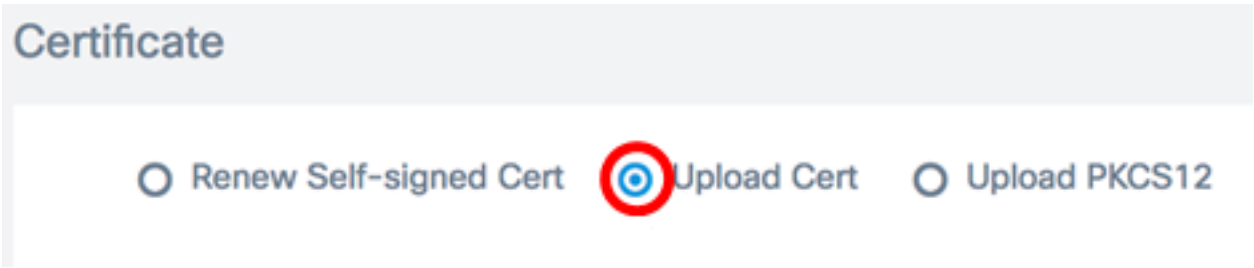
Etapa 1. O início de uma sessão à administração GUI de sua gerente de rede de FindIT escolhe então a **administração > o certificado**.



Etapa 2. Na área do certificado HTTPS, clique o **botão Update Button**.

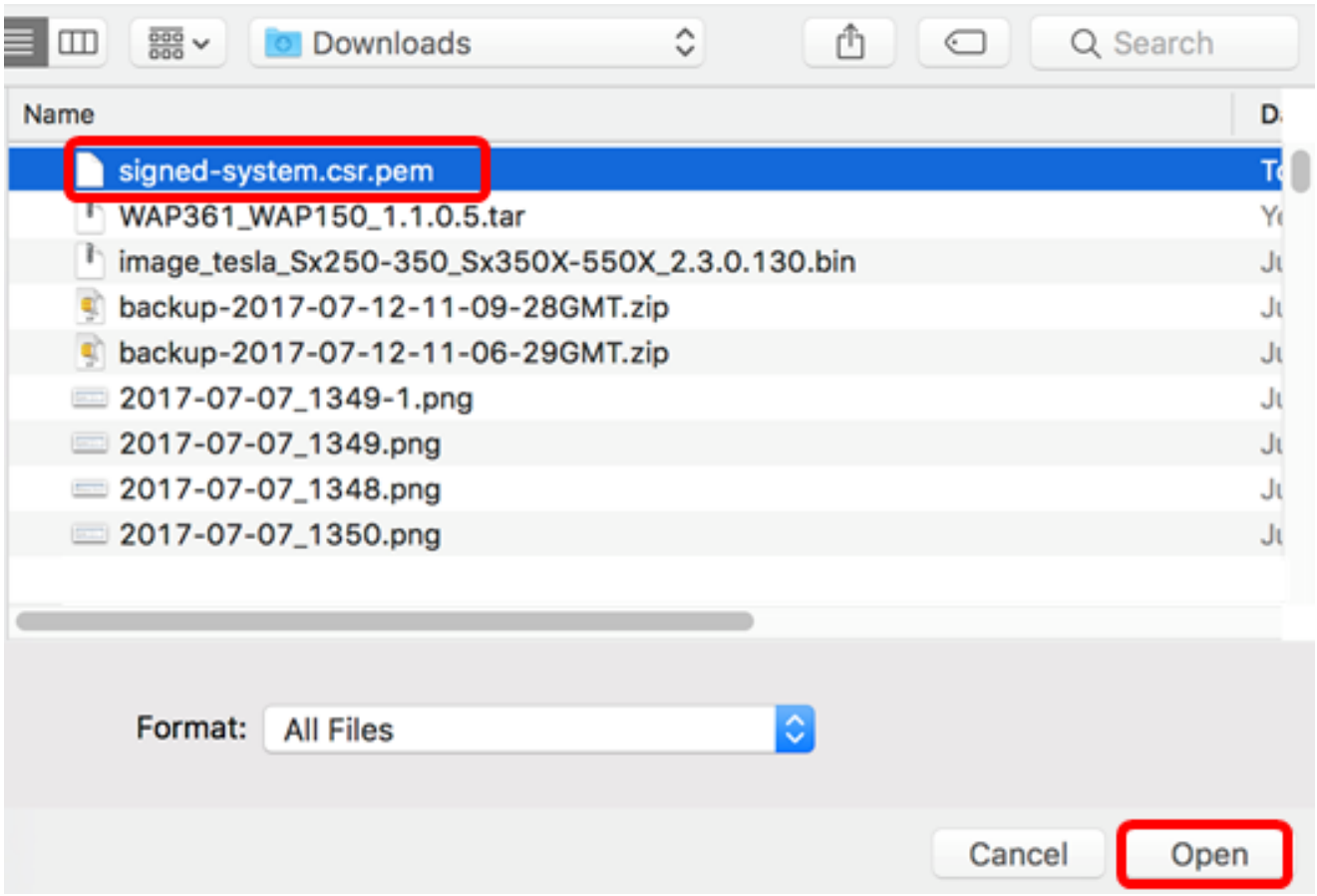


Etapa 3. Clique o botão de rádio de **UploadCert**.



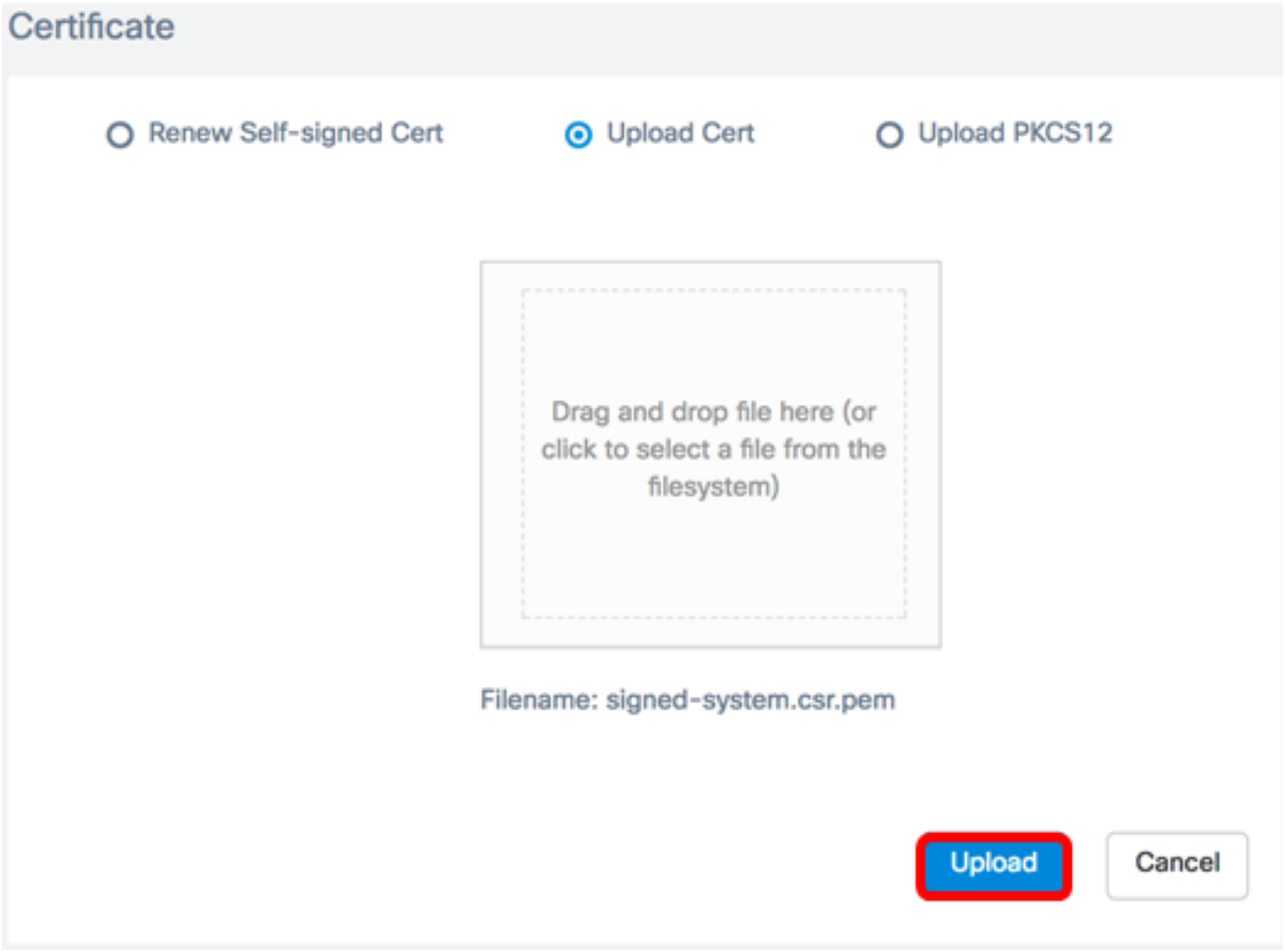
Nota: Alternativamente, você pode transferir arquivos pela rede um certificado com a chave privada associada no formato do PKCS-12 escolhendo o botão de rádio do **PKCS12 da transferência de arquivo pela rede**. A senha para destravar o arquivo deve ser especificada no campo de *senha* fornecido.

Etapa 4. Deixe cair o certificado assinado na área de alvo, ou clique a área de alvo para consultar o sistema de arquivos a seguir clique **aberto**. O arquivo deve estar no formato do .pem.



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

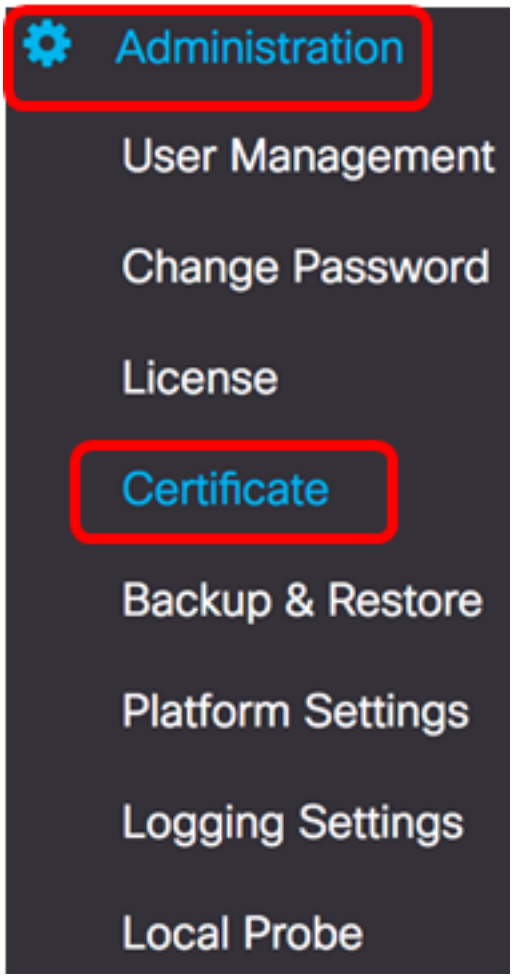
Etapa 5. **Transferência de arquivo pela rede do** clique.



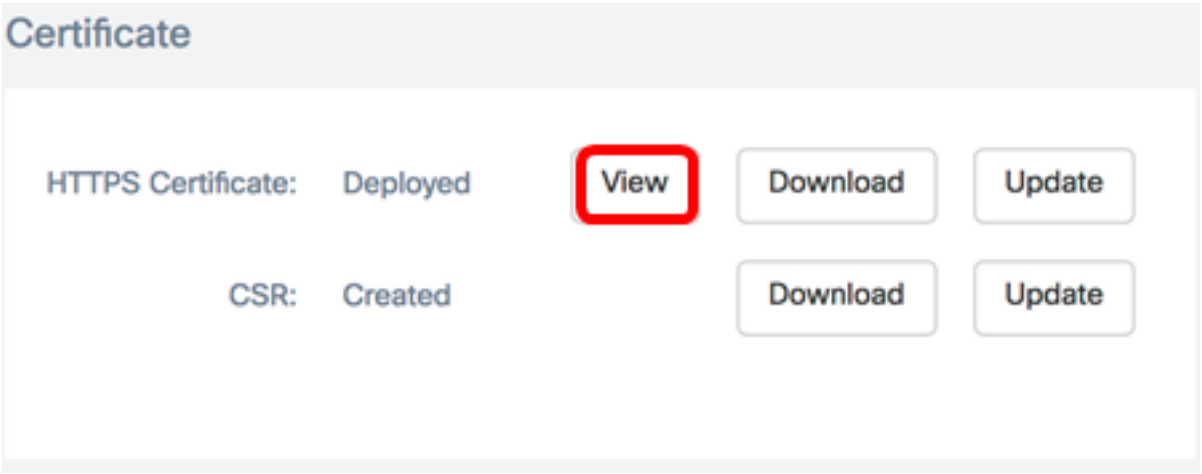
Você deve agora com sucesso ter transferido arquivos pela rede um certificado assinado à gerente de rede de FindIT.

Controle o certificado atual

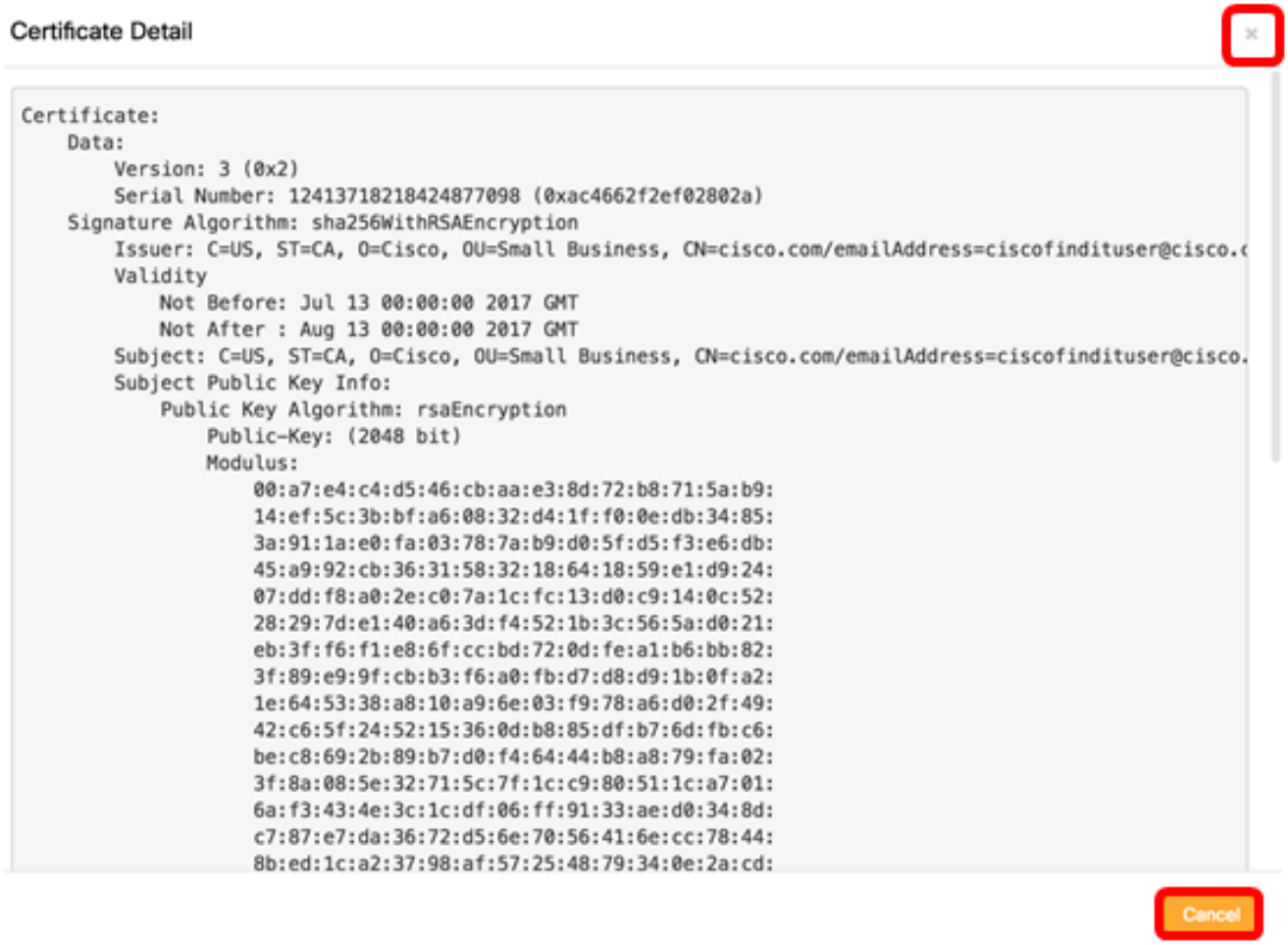
Etapa 1. O início de uma sessão à administração GUI de sua gerente de rede de FindIT escolhe então a **administração > o certificado**.



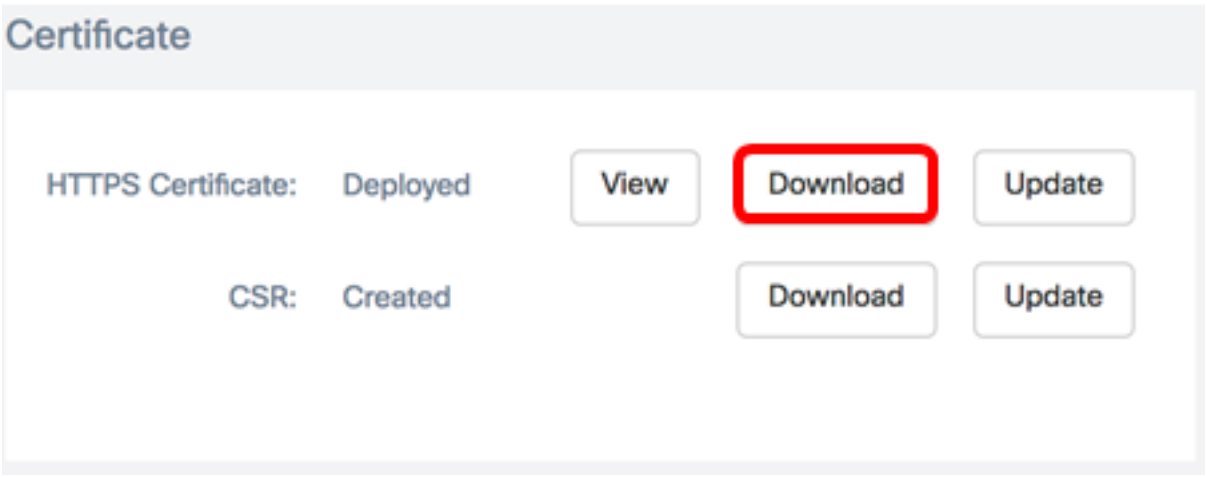
Etapa 2. Na área do certificado HTTPS, clique o **botão View Button**.



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



Etapa 4. (opcional) para transferir uma cópia do certificado atual, clica o botão da **transferência na** área do certificado HTTPS.



Você deve agora com sucesso ter controlado o certificado atual em sua gerente de rede de FindIT.