Regenerar o Certificado Padrão no Modo Gerenciado de Intervisão

Contents

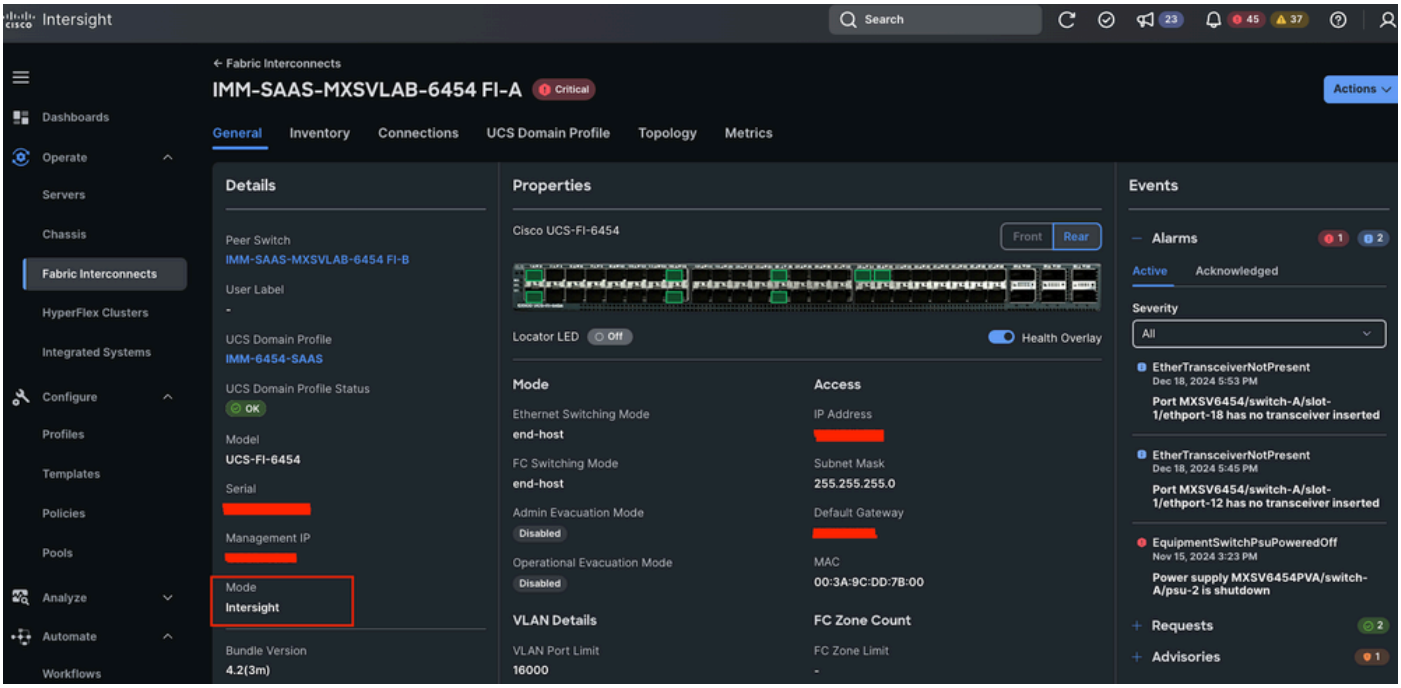
Introdução

Este documento descreve o processo para renovar um certificado autoassinado do Fabric Interconnect em ambientes Intersight (SAAS ou dispositivo).

Pré-requisitos

Requisitos

Domínio do UCS no modo gerenciado Intersight.



Componentes Utilizados

- Interconexão de estrutura 6454
- Versão: 4.2 (3m)

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Gerar certificado autoassinado

A Cisco recomenda o uso de certificados assinados pela CA para acessar o dispositivo, já que os navegadores modernos podem restringir o acesso se os certificados assinados automaticamente forem usados. O Intersight Virtual Appliance permite gerar um certificado autoassinado para estender sua validade se o certificado fornecido pela Cisco expirar.

Ao gerar um novo certificado autoassinado, o certificado SSL existente é substituído, possivelmente fazendo seu logout da sessão atual do navegador. Se você não estiver desconectado, atualize o navegador para aplicar o novo certificado. Para confirmar a atualização, clique no ícone de cadeado ou aviso ao lado da URL na barra de endereços do navegador. Após a atualização, você será direcionado para a página Settings **>** Certificates sem precisar fazer login novamente.

A interface do usuário do console do dispositivo usa um certificado autoassinado com o nome comum (CN) definido como switch. Este certificado é gerado na primeira vez que o Interconector de estrutura (FI) é ligado e configurado. O certificado autoassinado é válido por 365 dias, o que significa que qualquer FI com mais de um ano de validade tem um certificado expirado.

Alguns clientes usam ferramentas de monitoramento automatizadas para filtrar o IP ou o nome do host do dispositivo por HTTPS e validar a data de validade do certificado. Quando o certificado expira, essas ferramentas podem disparar alarmes, levando a equipes de observação e segurança a sinalizá-lo como um possível problema.

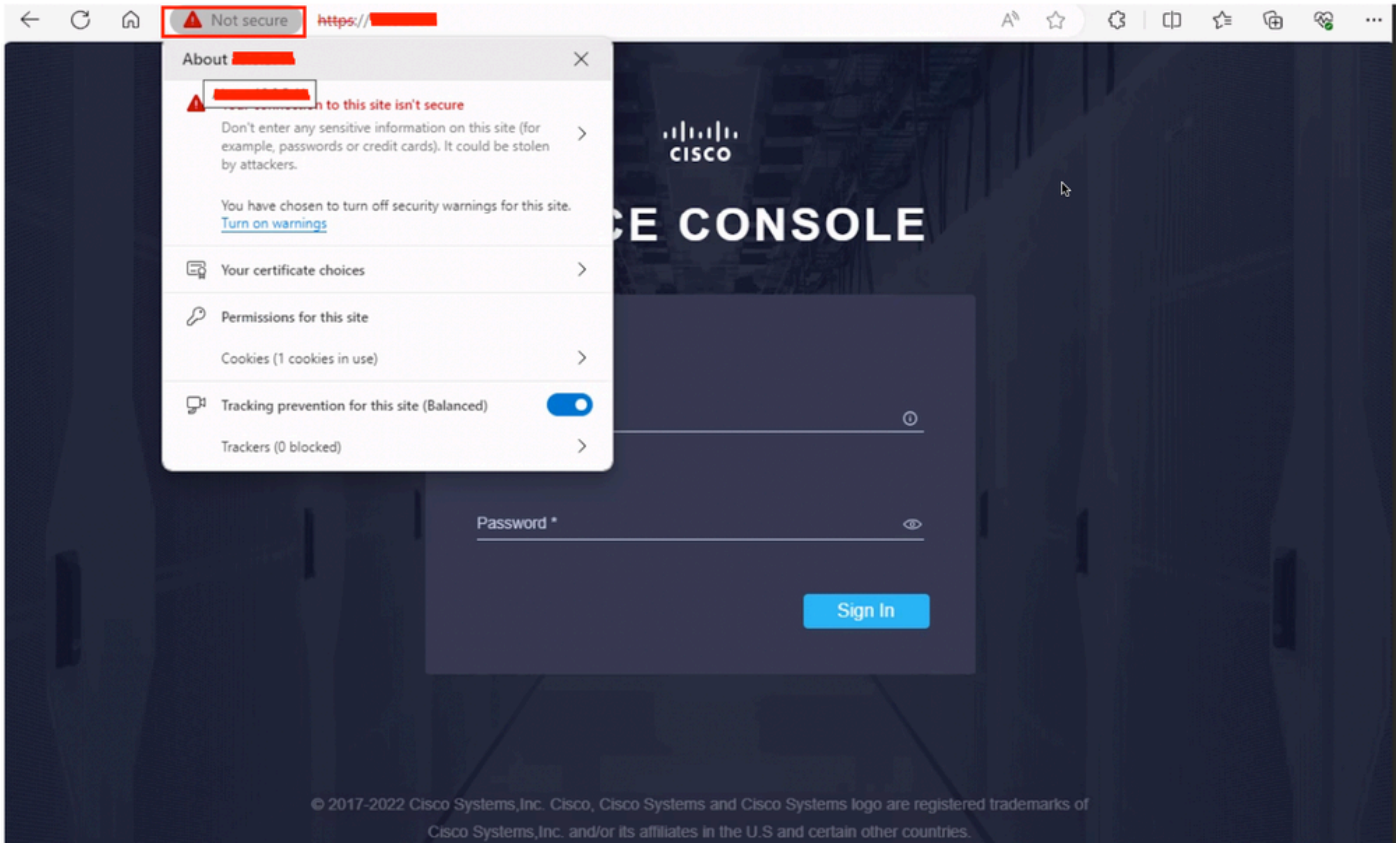
Além disso, como o certificado é autoassinado, os navegadores da Web exibem um aviso Não seguro. Esse aviso também poderá ser exibido se o certificado tiver expirado, o que poderá causar mais problemas de segurança.

Para evitar esses problemas, é recomendável renovar ou substituir o certificado proativamente.

Problema/Sintoma

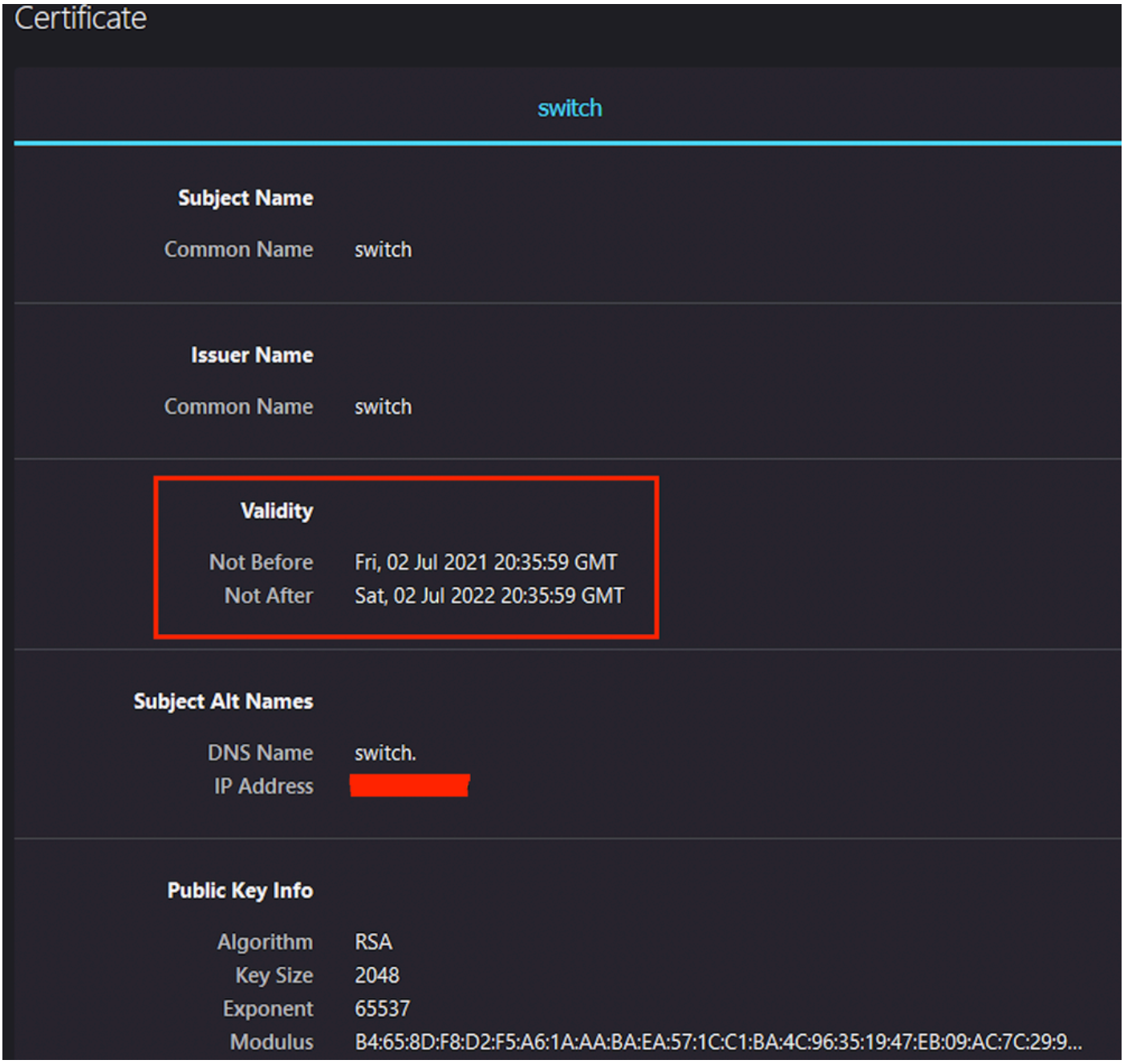
Você vê que o site não é seguro quando acessa o console do dispositivo.

Note: Para acessar o console do dispositivo, você precisa do endereço IP do Interconector de estrutura.



Erro de certificado

Ao clicar nas informações do certificado, você verá a data de expiração da certificação.



Data de vencimento do certificado

Regenerar o certificado

Para renovar o certificado padrão no Intersight, é necessário reiniciar o console do dispositivo ou reiniciar o Fabric Interconnect (não recomendado).

Use estas etapas para regenerar manualmente o certificado padrão no Intersight:

1. Abra uma sessão SSH usando o endereço IP de uma interconexão de estrutura.
2. Execute o comando:

```
UCS# generate-self-signed-certificate
```

Se o certificado tiver sido gerado com êxito, você verá:

```
hostname is IMM-FI6454
Successfully generated the self-signed-certificates
Successfully restarted the web-server
```

Para verificar o certificado real e confirmá-lo como alterado, use este comando:

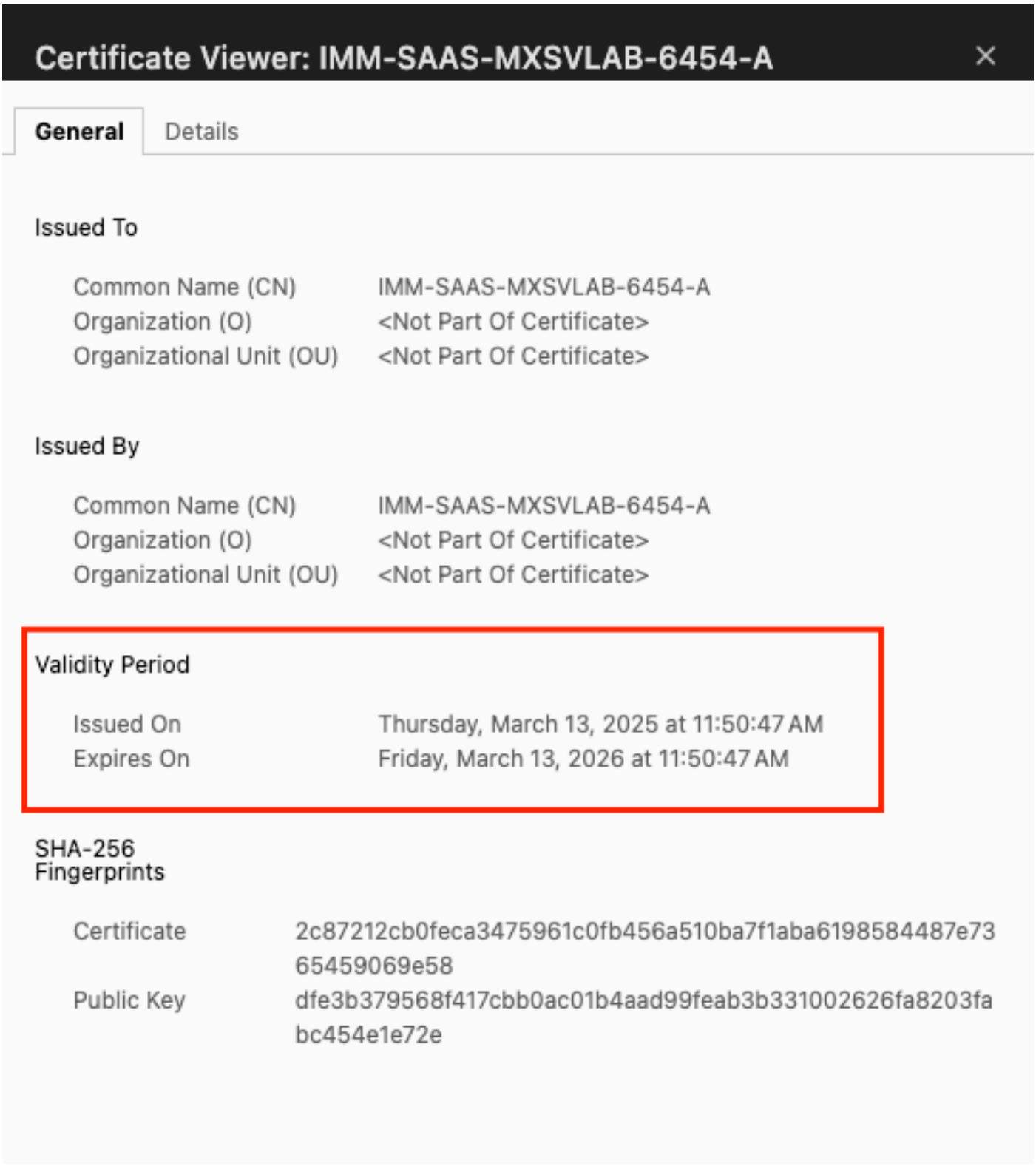
```
UCS# show self-signed-certificate
```

Saída de exemplo:

```
-----BEGIN CERTIFICATE-----
MIIC+DCCAeCgAwIBAgICBnowDQYJKoZIhvcNAQELBQAwIjEgMB4GA1UEAxMXSU1N
LVNBQVMtTVhTVkxBQi02NDU0LUEwHhcNMjUwMzEyMjI1MTM4WhcNMjYwMzEyMjI1
MTM4WjAiMSAwHgYDVQQDExdJTU0tU0FBUy1NWFNWTEFCLTY0NTQtQTCCASIwDQYJ
KoZIhvcNAQEBBQADggEPADCCAQoCggEBAK+Q9oAU2rHxtV5stg9vfCeKQ+9+n5Ke
oz6IKOeEDufeRcBYepaJlEhffvdLp/uOh/NnyphT4mVLiJxh6dTTIhW58G8LaGNV
hIRtNAX984eLCs1nSG3o3tzJ3+e5t04G6klAcj43HiKY+oRCEs+oiUsQlYpBjHoy
FGxMT8wpnNMIg59mKVTuUeC4r6ACnyy1CRNp8qD8Rf4lIBU/jTI/jPdzE2//9rAo
G85qhZ46vIOdLu1jv/ySszQkATFA15KHFETnyTkptdlJH8mcO33edJ1Xq9plebMp
dtn18zj+2qxQq8ErZ6doFdkOuyuq3N6QOdbfdefKKuiFvkCGv4GwRG8CAwEAAaM4
MDYwDgYDVR0PAQH/BAQDAgKkMBMGA1UdJQQMMAoGCCsGAQUFBwMBMA8GA1UdEQQI
MAaHBH8AAAEwDQYJKoZIhvcNAQELBQADggEBAFn+v4ehwLFi/mcHWA4ld03JBkvI
RIlbFPHjOykzmAN8E1XoJlLciCxA3gHUzPP6lT+2VpeAXAoWzIlgUlm2GwPzZbCQ
nz2v7NpGHchaXAEi756IMmCm2IJ2jOuS9p9v3AAX3gLUp43SeCQN+C2nNOcZgmZr
/K1CoNkIUXdVI8nxEDCMFPezL1SXdNa2c4AB699teolCNc65tnnNDjsxkLkL7bTx
P5euETVi5CizQQpjcZzXEMHv3XdvXtkzyAATjRmvUS8lxyXxiisMjMl7f8zXkLnG
n7ZKR746BXgXufmSOzITtbpvgI9+6PnauoWOh3EH7rGmJyZnn5L62/oaoy4=
-----END CERTIFICATE-----
```

Note: Se você verificar o certificado antes da renovação, certifique-se de que ele seja alterado após o processo de renovação.

Finalmente, o certificado deve ter esta aparência:



Validação de certificado

Informações Relacionadas

[Certificados no Intersight Virtual Appliance](#)

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.