

# Configurar Certificado para Servidores Gerenciados pela Intersight

## Contents

---

[Introdução](#)

[Pré-requisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Informações de Apoio](#)

[Configurar](#)

[Criar o arquivo de configuração \(.cnf\)](#)

[Gerar uma chave privada \(.key\)](#)

[Gerar CSR](#)

[Gerar o arquivo de certificado](#)

[Criar a Política de Gerenciamento de Certificados na Intersight](#)

[Adicionar a Diretiva a um Perfil de Servidor](#)

[Troubleshooting](#)

---

## Introdução

Este documento descreve o processo para gerar uma CSR (Certificate Signed Request, solicitação assinada por certificado) para criar certificados personalizados para servidores gerenciados pela Intersight.

## Pré-requisitos

### Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Intersight
- Certificados de terceiros
- OpenSSL

### Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- Interconexão em malha Cisco UCS 6454, firmware 4.2(1m)
- Servidor blade UCSB-B200-M5, firmware 4.2(1c)
- Software como serviço (SaaS) da Intersight

- Computador MAC com OpenSSL 1.1.1k

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.

## Informações de Apoio

No Modo Gerenciado de Interceptação, a política de Gerenciamento de Certificado permite que você especifique os detalhes do par de certificado e chave privada para um certificado externo e anexe a política aos servidores. Você pode carregar e usar o mesmo certificado externo e par de chaves privadas para vários Servidores Gerenciados Intersight.

## Configurar

Este documento usa o OpenSSL para gerar os arquivos necessários para obter a cadeia de certificados e o par de chaves privadas.

|          |  |
|----------|--|
| Etapa 1. | Crie o <code>.cnf</code> arquivo que tem todos os detalhes do certificado (deve incluir os endereços IP para a conexão IMC aos servidores).  |
| Etapa 2. | Crie a chave privada e o <code>.csr</code> arquivos por meio do OpenSSL.   |
| Etapa 3. | Envie o arquivo CSR a uma CA para assinar o certificado. Se sua organização gerar seus próprios certificados autoassinados, você poderá usar o arquivo CSR para gerar um certificado autoassinado. |
| Etapa 4. | Crie a Política de Gerenciamento de Certificados na Intersight e cole as cadeias de pares de Certificado e Chave Privada.  |

### Criar o arquivo de configuração (`.cnf`)

Use um editor de arquivos para criar o arquivo de configuração com a extensão `.cnf`. Preencha as configurações com base nos detalhes da sua organização.

```
<#root>
```

```
[ req ]
default_bits =
```

```
2048
```

distinguished\_name =  
req\_distinguished\_name

req\_extensions =  
req\_ext

prompt =  
no

[ req\_distinguished\_name ]  
countryName =  
US

stateOrProvinceName =  
California

localityName =  
San Jose

organizationName =  
Cisco Systems

commonName =  
esxi01

[ req\_ext ]  
subjectAltName =  
@alt\_names


[alt\_names]  
DNS.1 =  
10.31.123.60

IP.1 =  
10.31.123.32

IP.2 =  
10.31.123.34

IP.3 =  
10.31.123.35

---

 Cuidado: use os Nomes alternativos do assunto para especificar nomes de host ou endereços IP adicionais para seus servidores. Não configurá-lo ou excluí-lo do certificado carregado pode fazer com que os navegadores bloqueiem o acesso à interface do Cisco IMC.

---

## Gerar uma chave privada (.key)

Uso `openssl genrsa` para gerar uma nova chave.

```
<#root>
```

```
Test-Laptop$
```

```
openssl genrsa -out cert.key 2048
```

Verifique o arquivo chamado `cert.key` é criado por meio da `ls -la` comando.

```
<#root>
```

```
Test-Laptop$
```

```
ls -la | grep cert.key
```

```
-rw----- 1 user staff 1675 Dec 13 21:59 cert.key
```

## Gerar CSR

Uso `openssl req -new` para solicitar uma `.csr` usando a chave privada e `.cnf` arquivos criados anteriormente.

```
<#root>
```

```
Test-Laptop$
```

```
openssl req -new -key cert.key -out cert.csr -config cert.cnf
```


Uso `ls -la` a fim de verificar a `cert.csr` é criado.

```
<#root>
```

```
Test-Laptop$
```

```
ls -la | grep .csr
```

```
-rw-r--r-- 1 user staff 1090 Dec 13 21:53 cert.csr
```

 Observação: se sua organização usar uma CA (Autoridade de Certificação), você poderá enviar este CSR para que o certificado seja assinado por sua CA.

## Gerar o arquivo de certificado

Gerar o .cer arquivo com formato de código x509.

```
<#root>
```

```
Test-Laptop$
```

```
openssl x509 -in cert.csr -out certificate.cer -req -signkey cert.key -days 4000
```

Uso `ls -la` a fim de verificar a `certificate.cer` é criado.

```
<#root>
```

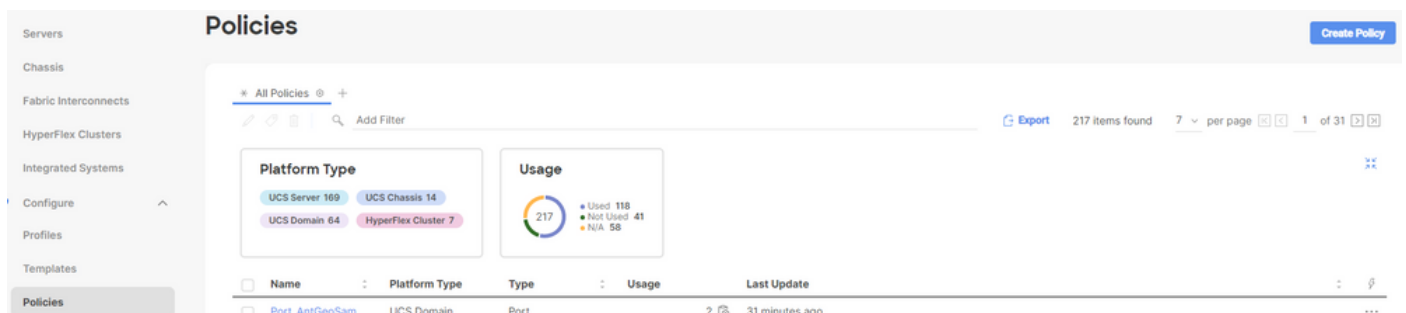
```
Test-Laptop$
```

```
ls -la | grep certificate.cer
```

```
-rw-r--r-- 1 user staff 1090 Dec 13 21:54 certificate.cer
```

## Criar a Política de Gerenciamento de Certificados na Intersight

Faça login na sua conta da Intersight, navegue até [Infrastructure Service](#), clique no botão [Policies](#) e clique em [Create Policy](#).



| Name           | Platform Type | Type | Usage | Last Update    |
|----------------|---------------|------|-------|----------------|
| Port_AntGeoSam | UCS Domain    | Port | 2     | 31 minutes ago |

Filtrar por servidor UCS e escolher [Certificate Management](#).

# Create

## Filters

### Platform Type

- All
- UCS Server
- UCS Domain
- UCS Chassis
- HyperFlex Cluster
- Kubernetes Cluster

Search

- Adapter Configuration
- Add-ons
- Auto Support
- Backup Configuration
- BIOS
- Boot Order
- Certificate Management
- Container Runtime
- FC Zone
- Fibre Channel Adapter
- Fibre Channel Network
- Fibre Channel QoS
- Flow Control
- HTTP Proxy
- Http Proxy Policy
- IMC Access
- Local User
- Multicast Policy
- Network CIDR
- Network Configuration
- Network Connectivity
- Node IP Ranges
- Node OS Configuration
- NTP
- SNMP
- SSH
- Storage
- Storage Configuration
- Switch Control
- Syslog
- System QoS
- Thermal

Use o `cat` para copiar o conteúdo do certificado (`certificate.cert` arquivo) e o arquivo de chave (`cert.key` arquivo) e cole-os na Política de gerenciamento de certificados no Intersight.

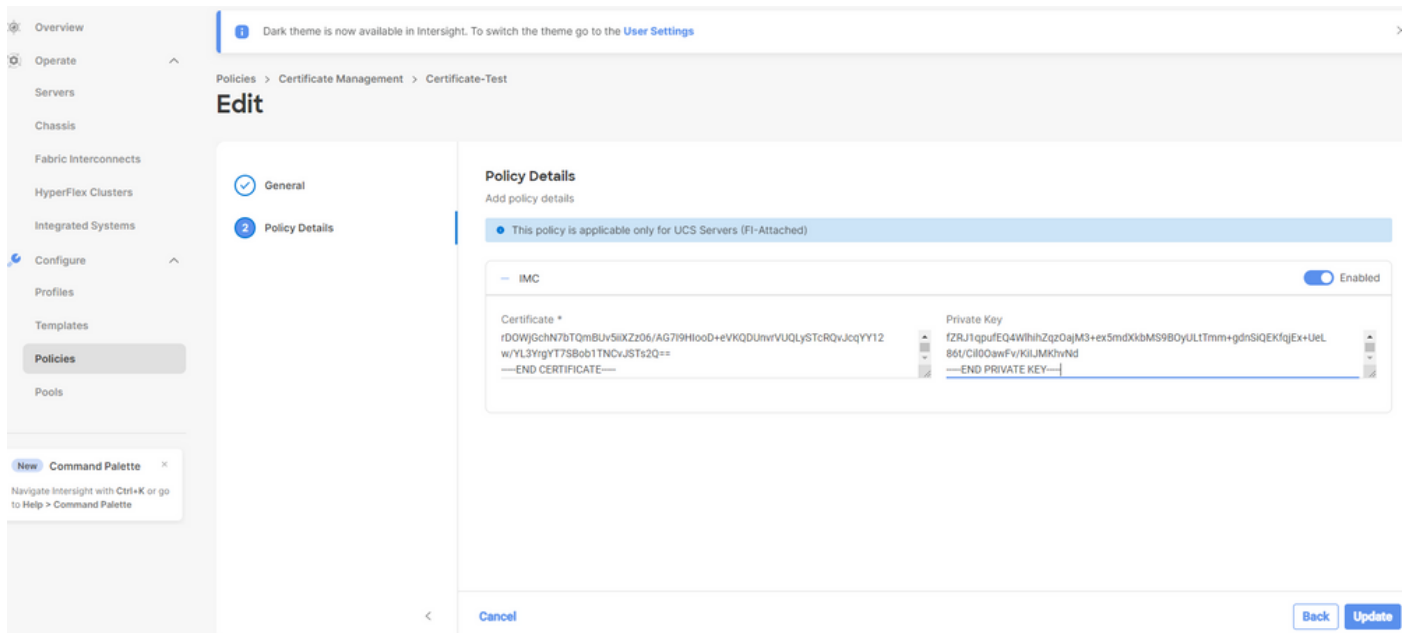
```
<#root>
```

```
Test-Laptop$
```

```
cat certificate.cert
```

```
Test-Laptop$
```

```
cat cert.key
```



Verifique se a política foi criada sem erros.

# Policies



Successfully created policy Certificate-TAC



## Adicionar a Diretiva a um Perfil de Servidor

Navegue até a página [Profiles](#) e modifique um perfil de servidor ou crie um novo perfil e anexe políticas adicionais, se necessário. Este exemplo modifica um perfil de serviço. Clique em [edit](#) e continue, anexe a política e implante o perfil do servidor.

**Management Configuration**  
Create or select existing Management policies that you want to associate with this profile.

|                        |         |
|------------------------|---------|
| Certificate Management |         |
| IMC Access             | KVM-IMM |
| IPMI Over LAN          |         |
| Local User             |         |
| Serial Over LAN        |         |
| SNMP                   |         |
| Syslog                 |         |
| Virtual KVM            | KVM_IMM |

## Troubleshooting

Se você precisar verificar as informações em um certificado, CSR ou chave privada, use os comandos OpenSSL conforme mencionado.

Para verificar os detalhes de CSR:

```
<#root>
```

```
Test-Laptop$
```

```
openssl req -text -noout -verify -in cert.csr
```

Para verificar os detalhes do certificado:

```
<#root>
```

```
Test-Laptop$
```

```
openssl x509 -in cert.cer -text -noout
```

## 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.