

Configurar o certificado HTTPS da GUI do APIC da ACI

Contents

[Introdução](#)

[Pré-requisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Configurar](#)

[Configurações](#)

[Etapa 1. Importar o Certificado Raiz ou Certificado Intermediário da Autoridade de Certificação](#)

[Etapa 2. Criar Toque de Tecla](#)

[Etapa 3. Gerar chave privada e CSR](#)

[Etapa 4. Obtenha o CSR e envie-o para a organização da CA](#)

[Etapa 5. Atualizar o certificado de autenticação na Web](#)

[Verificar](#)

[Troubleshooting](#)

[Informações Relacionadas](#)

Introdução

Este documento descreve a configuração de certificados SSL personalizados e SSL autoassinados.

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Assinaturas e certificados digitais
- Processo de emissão de certificado pela organização da Autoridade de Certificação (CA)

Componentes Utilizados

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

- Application Policy Infrastructure Controller (APIC)
- Navegador
- ACI executando 5.2 (8e)

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.

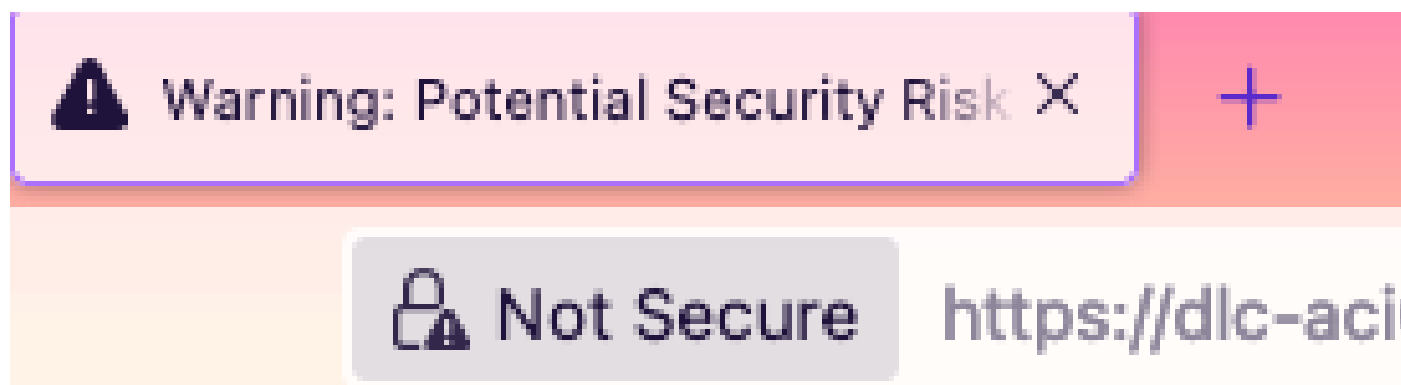
Configurar

Após a inicialização do dispositivo, ele usa o certificado autoassinado como o certificado SSL para HTTPS. O certificado autoassinado é válido por 1000 dias.

Por padrão, o dispositivo renova automaticamente e gera um novo certificado autoassinado um mês antes da expiração do certificado autoassinado.

Configurações

O dispositivo usa um certificado autoassinado. Ao acessar a GUI do APIC, o navegador avisa que o certificado não é confiável. Para resolver esse problema, este documento usa uma autoridade CA confiável para assinar o certificado.



Etapa 1. Importar o Certificado Raiz ou Certificado Intermediário da Autoridade de Certificação



Observação: se você estiver usando o certificado raiz de CA para assinar diretamente, poderá apenas importar o certificado raiz de CA. Mas se estiver usando um certificado intermediário para assinatura, você deverá importar a cadeia completa de certificados, ou seja: o certificado raiz e os certificados intermediários menos confiáveis.

Na barra de menus, navegue até Admin > AAA > Security > Public Key Management > Certificate Authorities.

The screenshot shows the Cisco ICM GUI navigation path: System > Tenants > Fabric > Virtual Networking > Admin > AAA > Security > Public Key Management > Certificate Authorities. The 'AAA' menu item is highlighted in the top navigation bar, and the 'Security' folder is highlighted in the left sidebar. In the main content area, the 'Public Key Management' tab is selected, and the 'Certificate Authorities' sub-tab is active. A table lists existing Certificate Authorities, and a 'Create Certificate Authority' button is visible.

Name	Description	FP	N
ACI_Root		[Cert 0] d7:29:6e:1c:60:26:4...	1
Cisco_AD_CA		[Cert 0] 57:1a:80:28:12:9a:5f...	1

The screenshot shows a web application window titled "User Management - Security". A modal dialog box titled "Create Certificate Authority" is open. It contains three input fields: "Name" (with a red border and a red error icon), "Description" (with the text "optional" inside), and "Certificate Chain" (empty). At the bottom right of the dialog are "Cancel" and "Submit" buttons.

Nome: **Obrigatório.**

Formule o conteúdo de acordo com suas regras de nomenclatura. Ele pode conter _, mas não caracteres especiais do inglês, como: , . ; ' " : | + * / = ` ~ ! @ # \$ % ^ & () e espaços.

Descrição: **Opcional.**

Cadeia de Certificação: **Obrigatório.**

Preencha o certificado raiz de CA confiável e o certificado intermediário de CA.



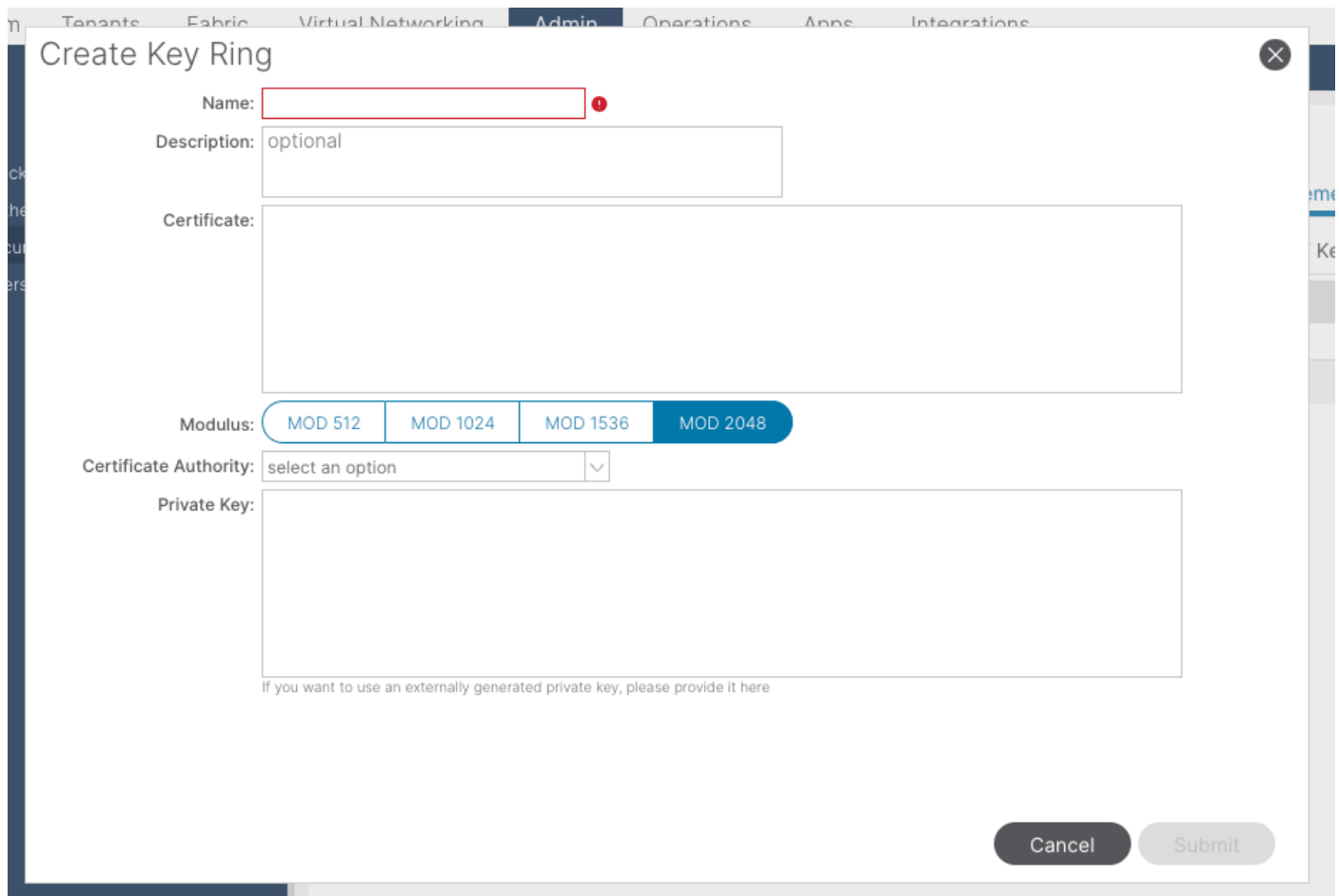
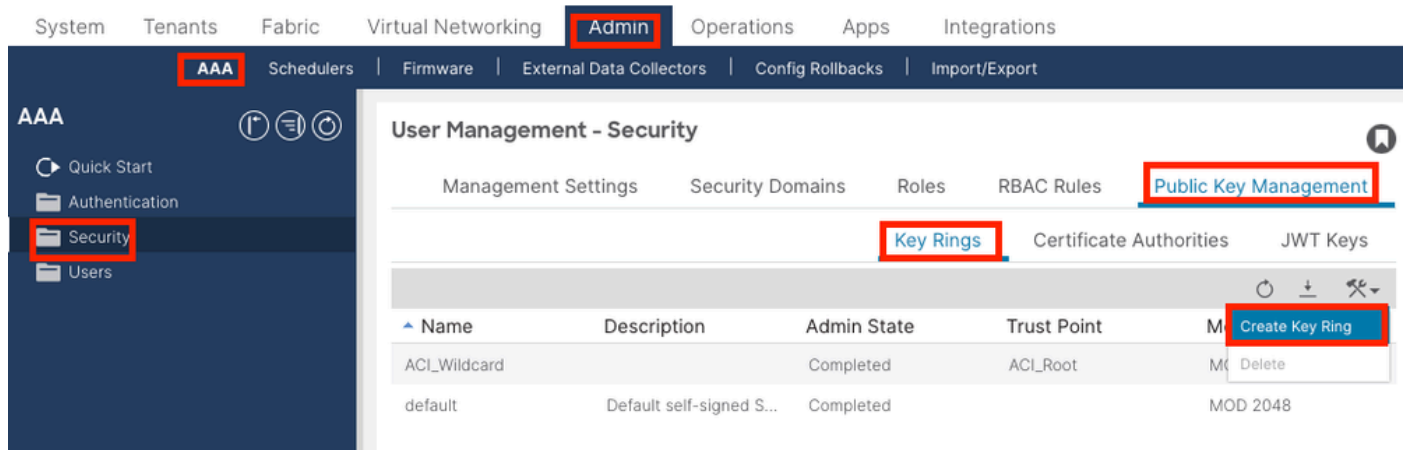
Observação: cada certificado deve estar em conformidade com um formato fixo.

```
-----BEGIN CERTIFICATE----- INTER-CA-2 CERTIFICATE CONTENT HERE -----END CERTIFICATE----- -----BEGIN  
CERTIFICATE----- INTER-CA-1 CERTIFICATE CONTENT HERE -----END CERTIFICATE----- -----BEGIN CERTIFICATE---  
-- ROOT-CA CERTIFICATE CONTENT HERE -----END CERTIFICATE-----
```

Clique no botão **Submit**.

Etapa 2. Criar Toque de Tecla

Na barra de menus, navegue até Admin > AAA > Security > Public Key Management > Key Rings.



Nome: **Obrigatório** (insira um nome).

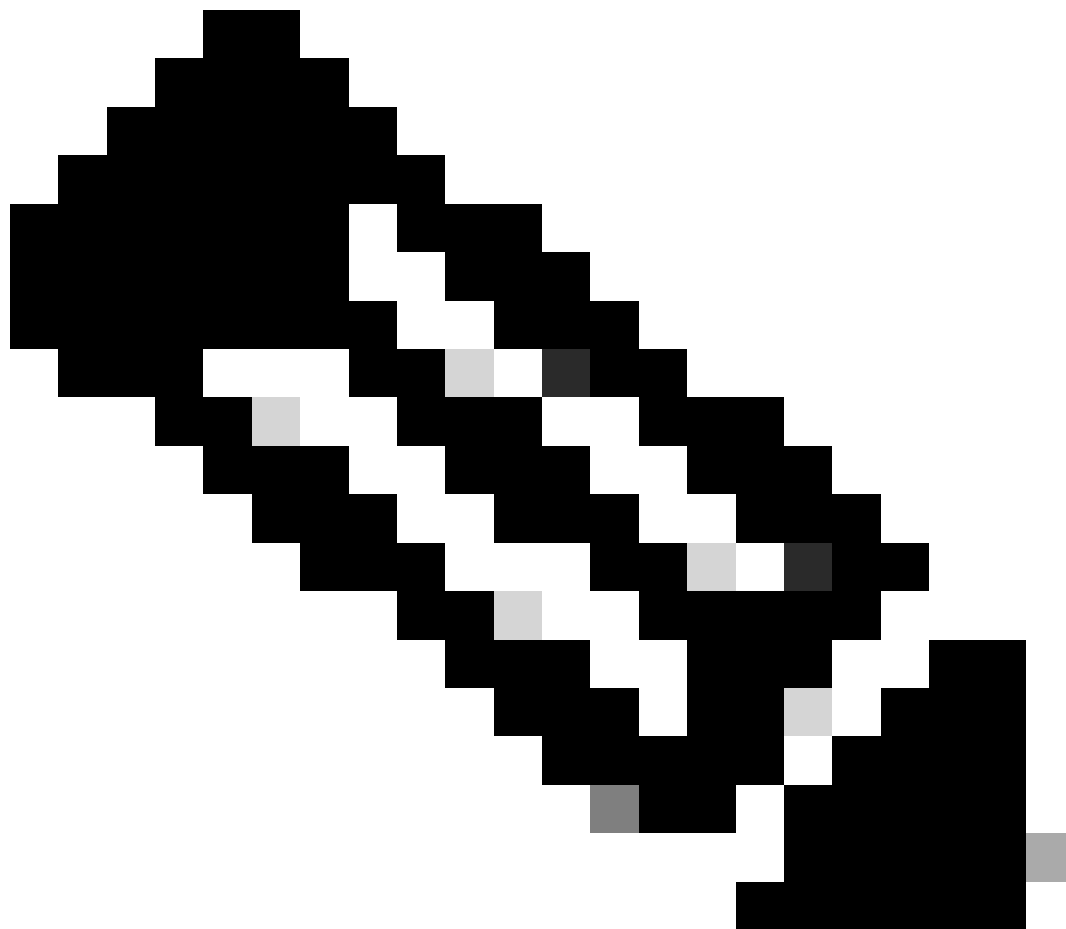
Certificado: **não adicione** nenhum conteúdo se você gerar uma CSR (Certificate Signing Request, solicitação de assinatura de certificado) usando o Cisco APIC através do toque de chave. Como alternativa, adicione o conteúdo do certificado assinado se você já tiver um assinado pela CA nas etapas anteriores, gerando uma chave privada e CSR fora do Cisco APIC.

Módulo: **Obrigatório** (clique no botão de opção para obter a intensidade de chave desejada).

Autoridade de Certificação: **Obrigatória**. Na lista suspensa, escolha a autoridade de certificação criada anteriormente.

Chave privada: **não adicione** nenhum conteúdo se você gerar um CSR usando o Cisco APIC através do toque de chave. Como alternativa,

adicione a chave privada usada para gerar o CSR para o certificado assinado que você inseriu.

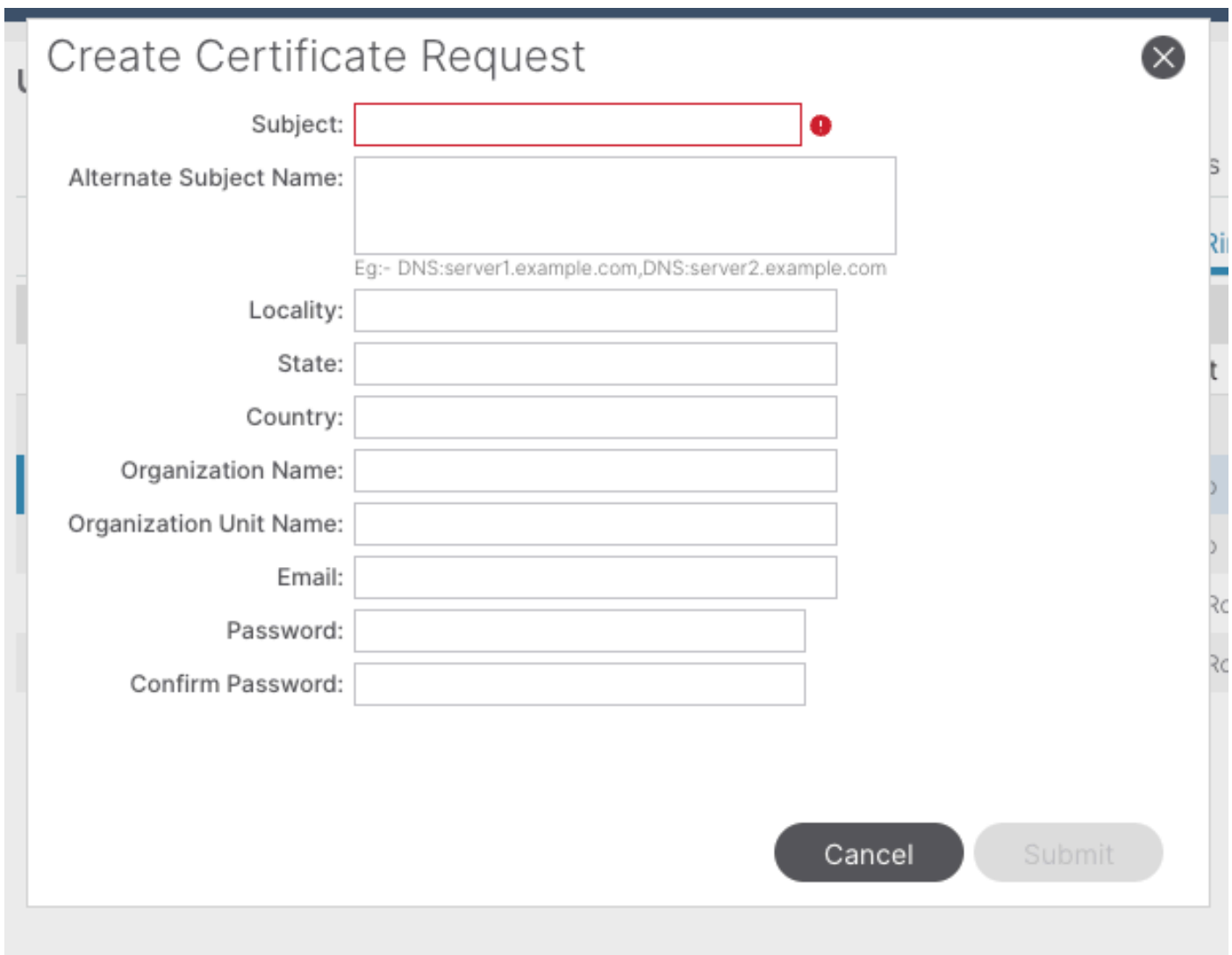
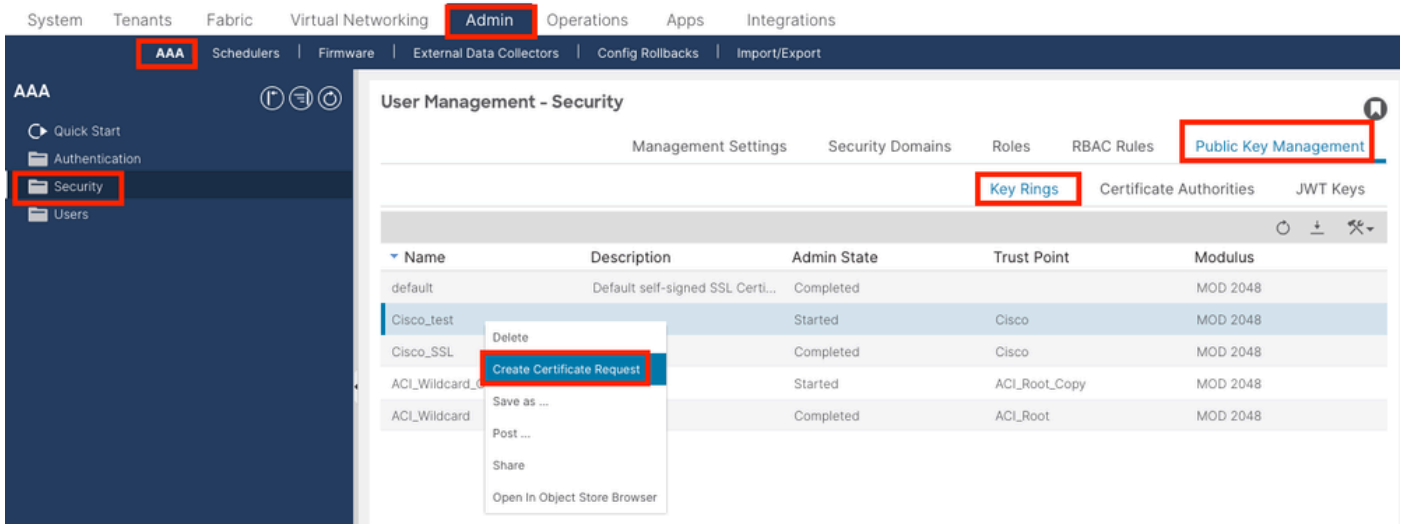


Observação: se você não quiser usar a chave privada e o CSR gerados pelo sistema e usar uma chave privada e um certificado personalizados, basta preencher quatro itens: Nome, Certificado, Autoridade de Certificação e Chave Privada. Depois de enviar, você só precisa executar a última etapa, Etapa 5.

Clique no botão **Submit**.

Etapa 3. Gerar Chave Privada e CSR

Na barra de menus, navegue até Admin > AAA > Security > Public Key Management > Key Rings.

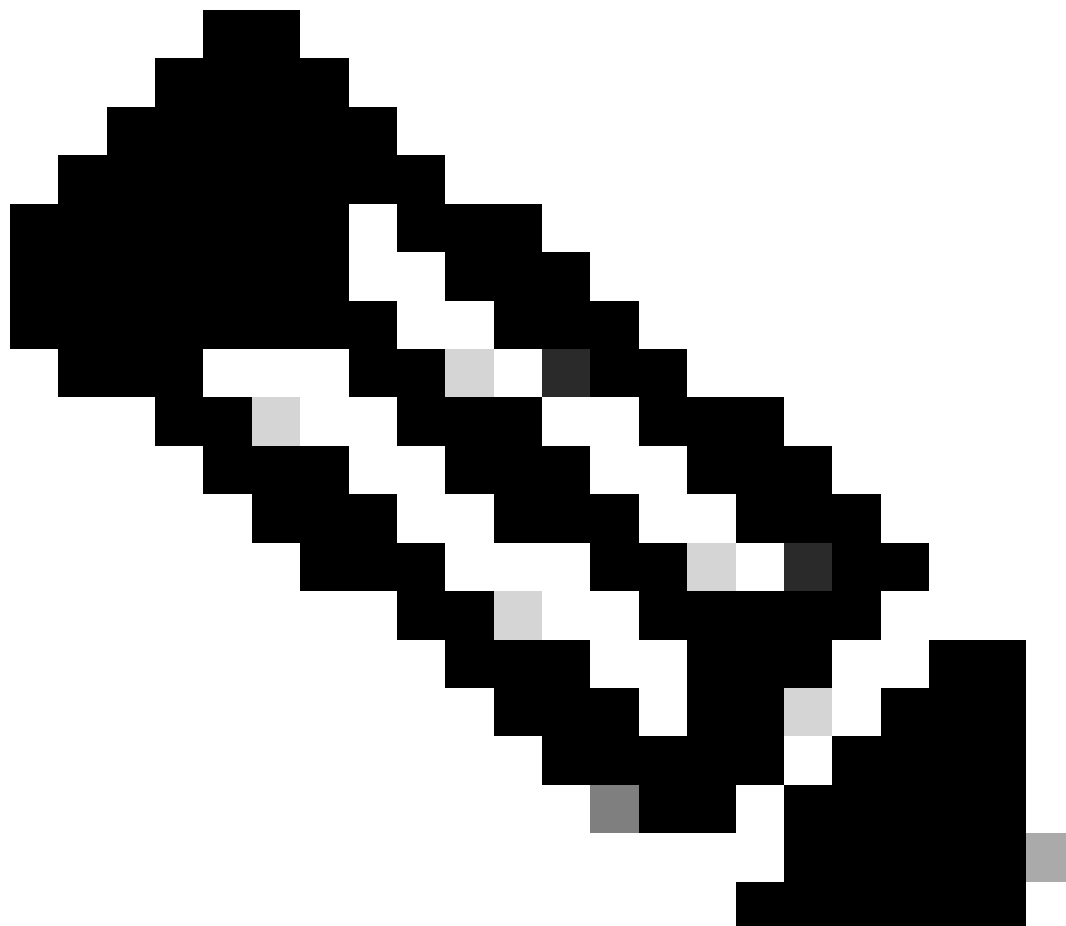


Assunto: **Obrigatório.** Insira o CN (nome comum) do CSR.

Você pode inserir o nome de domínio totalmente qualificado (FQDN) dos APICs da Cisco usando um curinga, mas em um certificado moderno, geralmente é recomendável que você insira um nome identificável do certificado e insira o FQDN de todos os APICs da Cisco no campo Nome de assunto alternativo (também conhecido como SAN - Nome alternativo do assunto) porque muitos navegadores modernos esperam o FQDN no campo SAN.

Nome Alternativo do Assunto: **Obrigatório. Insira o FQDN de todos os APICs da Cisco, como**
DNS:apic1.example.com,DNS:apic2.example.com,DNS:apic3.example.com ou DNS:*example.com.

Como alternativa, se desejar que a SAN corresponda a um endereço IP, insira os endereços IP dos APICs da Cisco com o formato:
IP:192.168.1.1.



Observação: você pode usar nomes DNS (Domain Name Server), endereços IPv4 ou uma combinação de ambos nesse campo. Não há suporte para endereços IPv6.

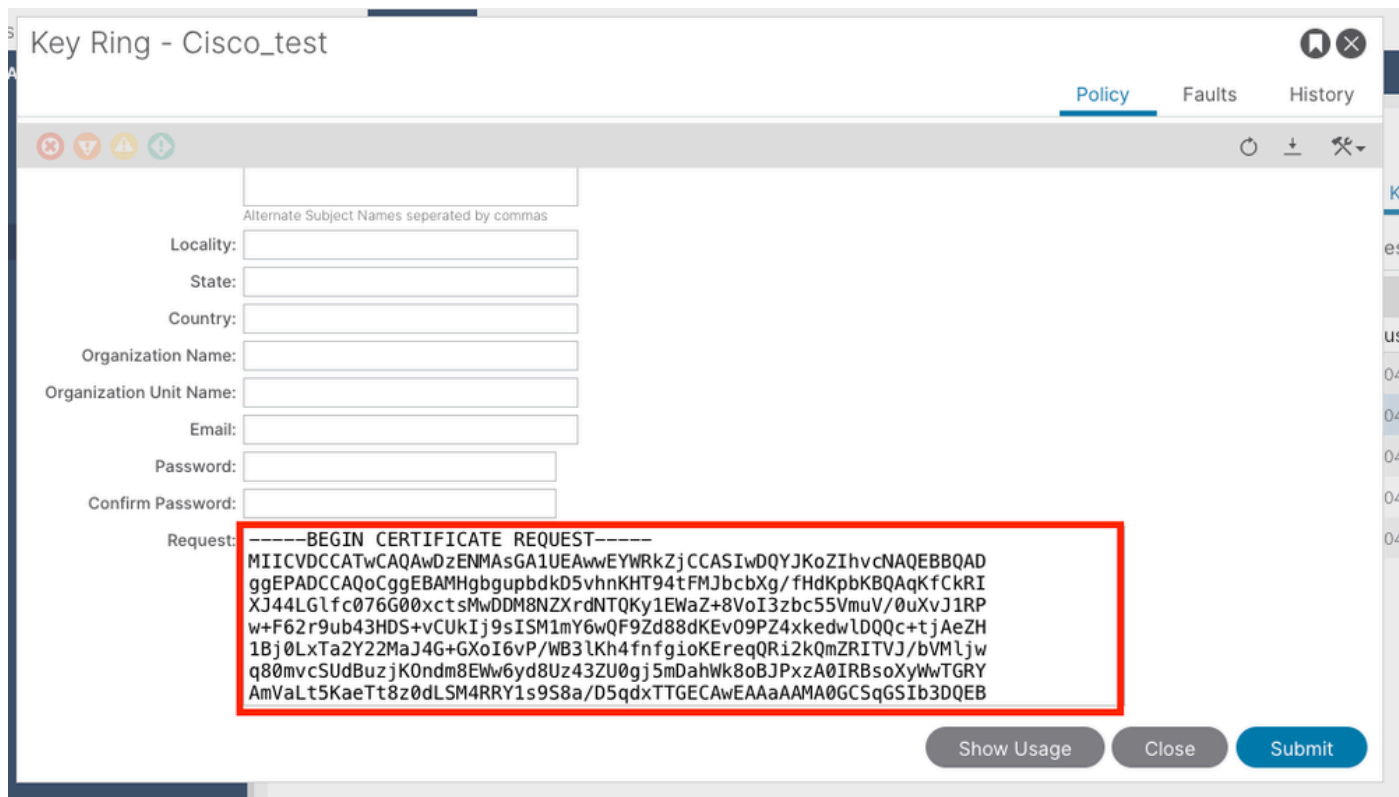
Preencha os campos restantes de acordo com os requisitos da organização de CA que você está solicitando para emitir o certificado.

Clique no botão **Submit**.

Etapa 4. Obtenha o CSR e envie-o para a organização da CA

Na barra de menus, navegue até Admin > AAA > Security > Public Key Management > Key Rings.

Clique duas vezes no nome de **Key Ring** de criação e localize a opção **Request**. O conteúdo na Solicitação é o CSR.



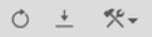
The screenshot shows the 'Key Ring - Cisco_test' configuration page. The 'Request' field is highlighted with a red box and contains the following CSR text:

```
-----BEGIN CERTIFICATE REQUEST-----  
MIICVDCCATwCAQAwDzENMAsgA1UEAwEYWRkZjCCASIwDQYJKoZIhvcNAQEBBQAD  
ggEPADCCAQoCggEBAMHgbgubdkD5vhnKHT94tFMJbcbXg/fHdKpbKBQAgKfCKRI  
XJ44LGLfc076G00xctSmwDDM8NZXrdNTQKy1Ewaz+8VoI3zbc55VmuV/0uXvJ1RP  
w+F62r9ub43HDS+vCUKIj9sISM1mY6wQF9Zd88dKEv09PZ4xkedwLDQqc+tjAeZH  
1Bj0LxTa2Y22MaJ4G+GxoI6vP/WB3lKh4fnfgioKEreqQR12kQmZRITVJ/bVMljw  
q80mvcSUDBuzjK0ndm8EWw6yd8Uz43ZU0gj5mDahWk8oBJPxzA0IRBsoXyWwTGRY  
AmVaLt5KaeTt8z0dLSM4RRY1s9S8a/D5qdxTTGECAwEAAaAAMA0GCSqGSIb3DQEBA
```

Copie todo o conteúdo da solicitação e envie-a para sua autoridade de certificação.

A autoridade de certificação usa sua chave privada para executar a verificação de assinatura no seu CSR.

Depois de obter o certificado assinado da CA, ele copia o certificado para o Certificado.



Name: Cisco_Test

Admin State: Started

Description: optional

Certificate:

```
-----BEGIN CERTIFICATE-----  
MIIDSzCCApugAwIBAgIBAgjANBgqhkiG9w0BAQsFADBYMQswCQYDVQGEwJVUzEL  
MAKGA1UECAwCQ0EFTATBgNVBACMDERlZmF1bHQgQ2l0eTEEXMBUGA1UECgw0Q2Lz  
Y28gQUNJIFRlYW0xDDAKBgNVBAsMA1RBQzAeFw0yNDYyMjE5MDU5MDhaFw0yNTAy  
MjE5MDU5MDhaMGUxCzAJBgNVBAYTAlVMTQswCQYDVQQLIDQTEEXMBUGA1UECgw0  
Q2LzY28gQUNJIFRlYW0xDDAKBgNVBAsMA1RBQzEiMCAGA1UEAwwZZGxjLWFlaTA2  
LWFwawMxLmNpc2NvLmNvbTCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEB  
ALJA5N1wzE7WmBk35pTd06FwH3M2ZmIeCDw6SktDTqaMHhqDkYEK0UgG0dyRrdP
```

Modulus: MOD 512 MOD 1024 MOD 1536 MOD 2048

Certificate Authority: Cisco_ACL_Team

Private Key:

Show Usage Close Submit



Observação: cada certificado deve estar em conformidade com um formato fixo.

-----BEGIN CERTIFICATE----- CERTIFICATE CONTENT HERE -----END CERTIFICATE-----

Clique no botão **Submit**.

Etapa 5. Atualizar o Certificado de Autenticação na Web

Na barra de menus, navegue até Fabric > Fabric Policies > Policies > Pod > Management Access > Default.

System Tenants **Fabric** Virtual Networking Admin Operations Apps Integrations

Inventory **Fabric Policies** Access Policies

Policies

- Quick Start
- Pods
- Switches
- Modules
- Interfaces
- Policies**
 - Pod
 - Date and Time
 - SNMP
 - Management Access
 - default**
 - Switch
 - Interface
 - Global
 - Monitoring
 - Troubleshooting
 - Geolocation
 - Macsec
 - Analytics
 - Tenant Quota
 - Annotations

Management Access - default

Policy Faults History

Allow Credentials: Disabled Enabled

Request Throttle: Disabled Enabled

HTTPS

Admin State:

Port:

Allow Origins:

Allow Credentials: Disabled Enabled

SSL Protocols: TLSv1.2 TLSv1.3

DH Param:

Request Throttle: Disabled Enabled

Admin KeyRing:

Oper KeyRing: uni/userext/pkiext/keyring-Cisco_Test

Client Certificate TP:

Client Certificate Authentication state: Disabled Enabled

SSH access via WEB

Admin State:

Port:

MACS: hmac-sha1 hmac-sha2-256 hmac-sha2-512

KEX Algorithms:

SSL Cipher Configuration:

ID	State
CHACHA20	Enabled
DHE-RSA-AES128-SHA	Disabled
DHE-RSA-AES256-SHA	Disabled

Show Usage Reset Submit

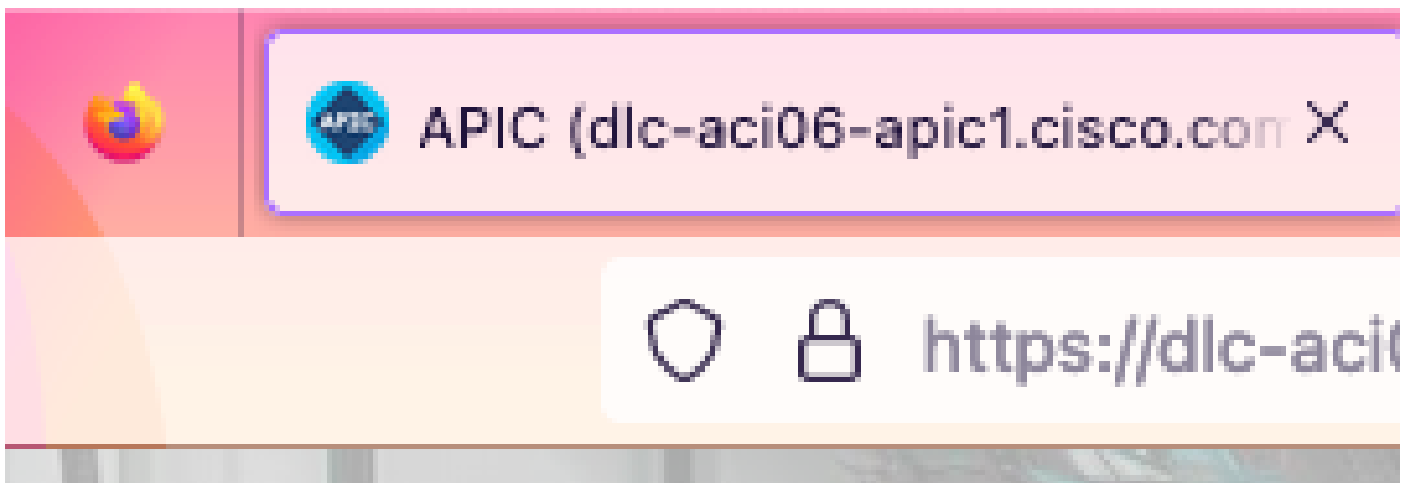
na lista suspensa **Admin KeyRing**, escolha o KeyRing desejado.

Clique no botão **Submit**.

Após clicar em enviar, ocorre um erro devido a motivos de certificado. Atualizar com o novo certificado.

Verificar

Depois de acessar a GUI do APIC, o APIC usa o certificado assinado pela CA para se comunicar. Exiba as informações do certificado no navegador para verificá-las.





Observação: os métodos de exibição de certificados HTTPS em navegadores diferentes não são exatamente os mesmos. Para obter os métodos específicos, consulte o guia do usuário do seu navegador.

Troubleshooting

Se o navegador ainda perguntar que a GUI do APIC não é confiável, verifique no navegador se o certificado da GUI é consistente com o enviado no Keyring.

Você precisa confiar no **certificado raiz da autoridade de certificação** que emitiu o certificado no seu computador ou navegador.



Observação: o navegador Google Chrome deve verificar a **SAN do certificado para confiar nesse certificado.**

Em APICs que usam certificados autoassinados, avisos de expiração de certificado podem aparecer em raros casos.

Localize o certificado no Keyring, use a ferramenta de análise de certificado para analisar o certificado e compare-o com o certificado usado no navegador.

Se o certificado no chaveiro for renovado, crie uma nova Política de Acesso de Gerenciamento e aplique-a.

System Tenants **Fabric** Virtual Networking Admin Operations Apps Integrations

Inventory | **Fabric Policies** | Access Policies

Policies

- Quick Start
- Pods
- Switches
- Modules
- Interfaces
- Policies**
 - Pod
 - Date and Time
 - SNMP
 - Management Access
 - Create Management Access Policy**
 - Switch

Pod - Management Access

Name	HTTP			HTTPS		SSH State	SSH State
	HTTP State	HTTP Port	HTTP Redirect	HTTPS State	HTTPS Port		
default	enabled	80	disabled	enabled	443	enabled	

System Tenants **Fabric** Virtual Networking Admin Operations Apps Integrations

Inventory | **Fabric Policies** | Access Policies

Policies

- Quick Start
- Pods**
 - Policy Groups**
 - default**
 - Profiles
 - Switches
 - Modules
 - Interfaces
 - Policies
 - Pod
 - Date and Time
 - SNMP
 - Management Access
 - New
 - default
 - Switch
 - Interface
 - Global
 - Monitoring
 - Troubleshooting

Pod Policy Group - default

Policy | Faults | History

Properties

Date Time Policy: default

Resolved Date Time Policy: default

ISIS Policy: select a value

Resolved ISIS Policy: default

COOP Group Policy: select a value

Resolved COOP Group Policy: default

BGP Route Reflector Policy: select a value

Resolved BGP Route Reflector Policy: default

Management Access Policy: select a value

Resolved Management Access Policy: New

SNMP Policy: fabric

Resolved SNMP Policy: default

MACsec Policy: fabric

Resolved MACsec Policy: fabric

Create Management Access Policy

Show Usage | Reset | Submit

Se o certificado no Keyring não for renovado automaticamente, entre em contato com o TAC da Cisco para obter mais assistência.

Informações Relacionadas

- [Guia de configuração de segurança do Cisco APIC, versão 5.2\(x\)](#)
- [Suporte técnico e downloads da Cisco](#)

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.