

配置ACI APIC GUI HTTPS证书

目录

[简介](#)

[先决条件](#)

[要求](#)

[使用的组件](#)

[配置](#)

[配置](#)

[第1步：导入CA机构根证书或中间证书](#)

[第二步：创建密钥环](#)

[第3步：生成私钥和CSR](#)

[第四步：获取CSR并将其发送到CA组织](#)

[第5步：在Web上更新签名证书](#)

[验证](#)

[故障排除](#)

[相关信息](#)

简介

本文档介绍自定义SSL证书和自签名SSL证书的配置。

先决条件

要求

Cisco 建议您了解以下主题：

- 数字签名和数字证书
- 证书颁发机构(CA)组织的证书颁发过程

使用的组件

本文档中的信息基于以下软件和硬件版本：

- 应用策略基础设施控制器 (APIC)
- 浏览器
- 运行5.2 (8e)的ACI

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

配置

设备初始化后，它将自签名证书用作HTTPS的SSL证书。自签名证书的有效期为1000天。

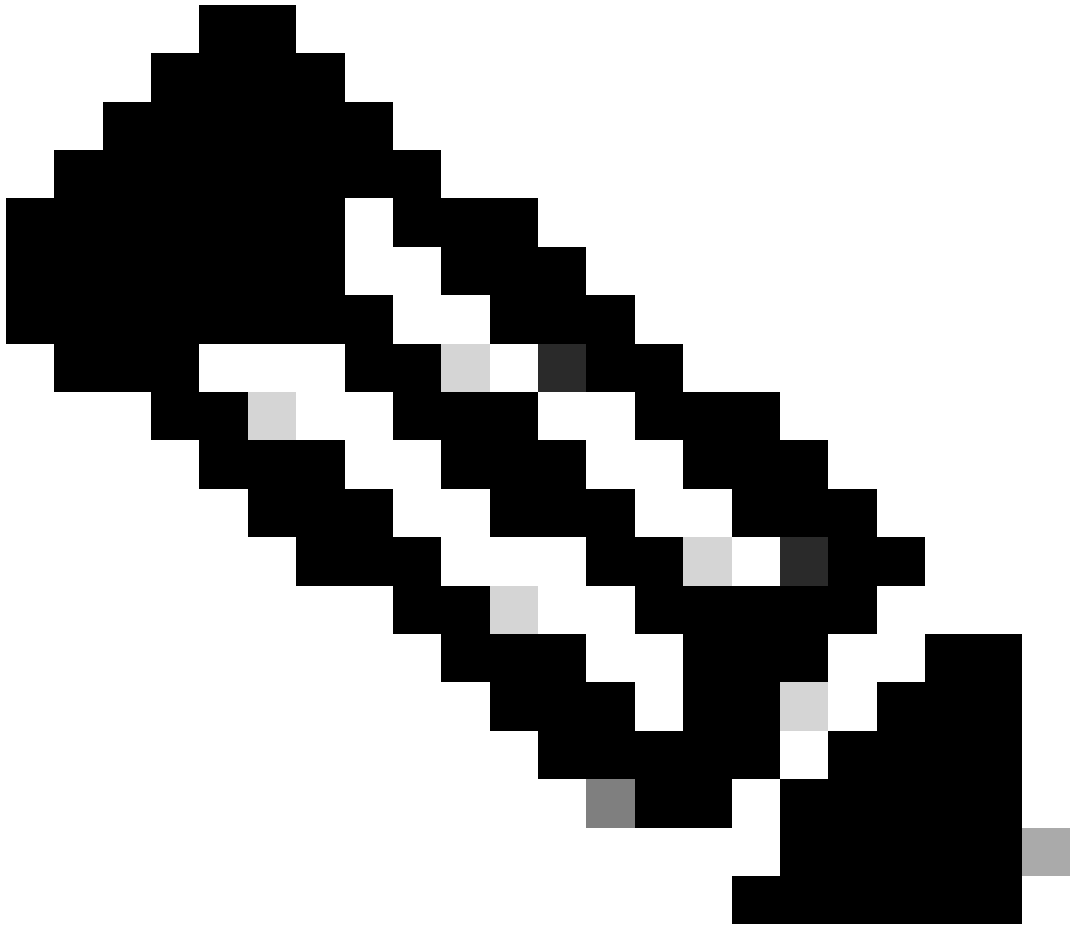
默认情况下，设备会在自签名证书到期前一个月自动续订并生成新的自签名证书。

配置

设备使用自签名证书。访问APIC GUI时，浏览器会提示证书不可信。为了解决此问题，本文档使用受信任的CA颁发机构对证书进行签名。



步骤1: 导入CA颁发机构根证书或中间证书



注意：如果使用CA根证书直接签名，则只需导入CA根证书。但是，如果您使用中间证书进行签名，则必须导入完整的证书链，即：根证书和不太受信任的中间证书。

在菜单栏上，导航到Admin > AAA > Security > Public Key Management > Certificate Authorities。

The screenshot shows the Cisco ACI management interface. The top navigation bar includes System, Tenants, Fabric, Virtual Networking, Admin (highlighted with a red box), Operations, Apps, and Integrations. Below this, a secondary bar contains AAA (highlighted with a red box), Schedulers, Firmware, External Data Collectors, Config Rollbacks, and Import/Export. The left sidebar shows the AAA menu with sub-items: Quick Start, Authentication, Security (highlighted with a red box), and Users. The main content area is titled 'User Management - Security' and contains several tabs: Management Settings, Security Domains, Roles, RBAC Rules, Public Key Management (highlighted with a red box), Key Rings, Certificate Authorities (highlighted with a red box), and JWT Keys. Under the Certificate Authorities tab, there is a table with columns for Name, Description, FP, and a 'Create Certificate Authority' button (highlighted with a red box). The table contains two entries: ACI_Root and Cisco_AD_CA.

| Name | Description | FP | |
|-------------|-------------|----------------------------------|---|
| 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 |

User Management - Security

Create Certificate Authority

Name: !

Description: optional

Certificate Chain:

Cancel Submit

名称：必填。

根据命名规则制定内容。它可包含_，但不能包含特殊英语字符，例如：
.,;':"|+*/=\`~!@#% ^&() 和空格字符。

说明：可选。

认证链：必填。

填写受信任CA根证书和CA中间证书。



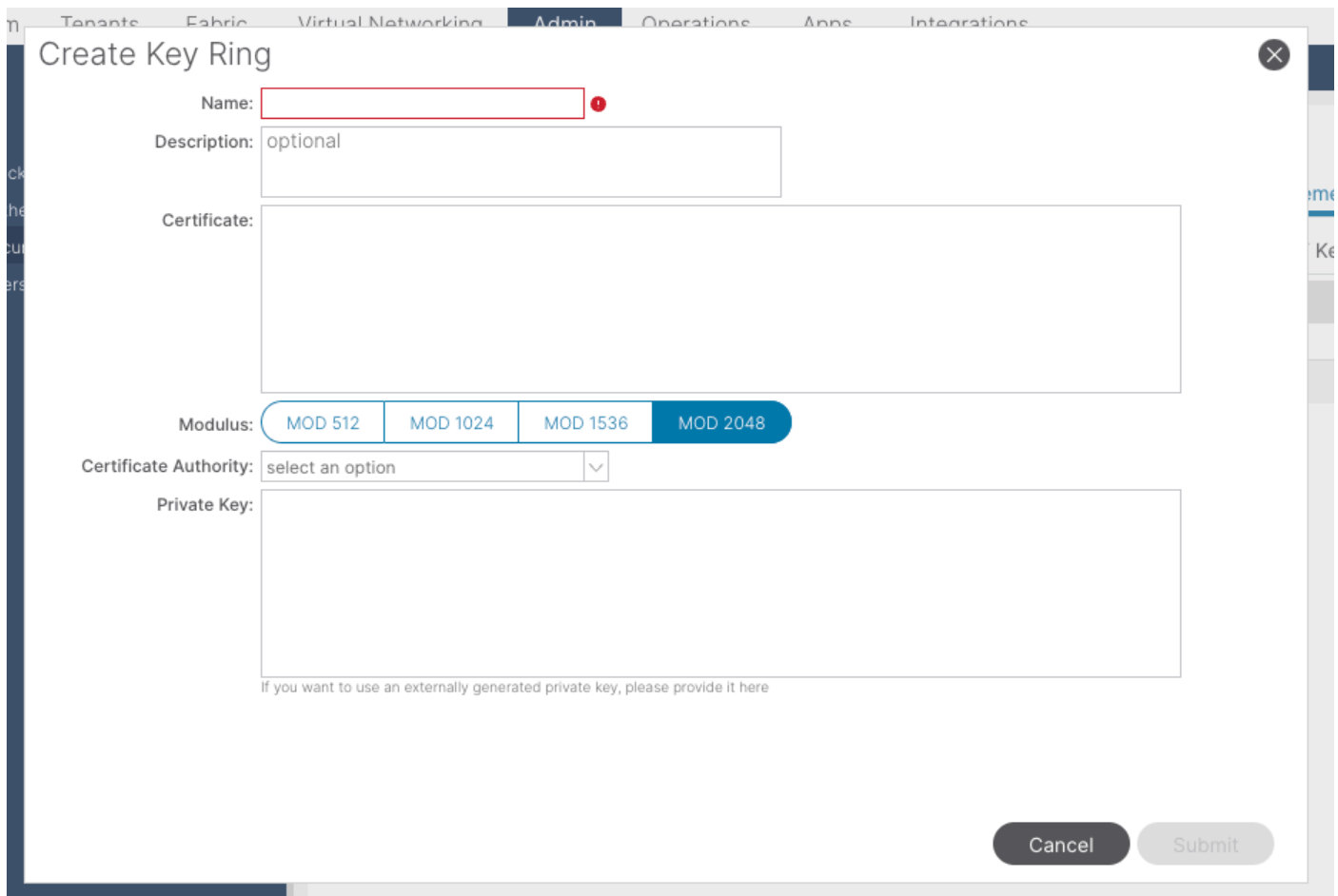
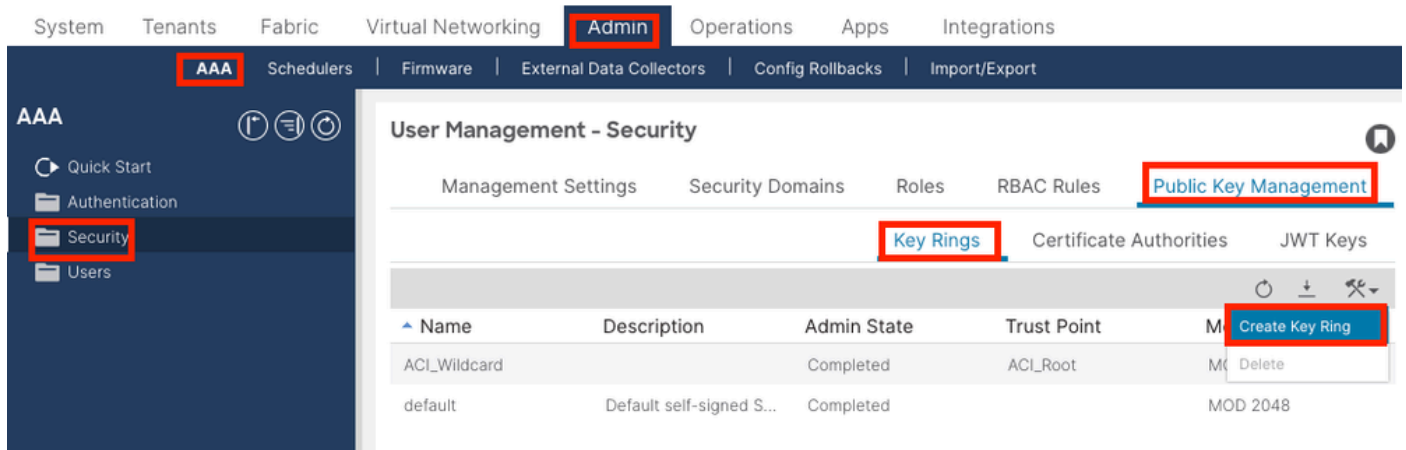
注意：每个证书都必须符合固定格式。

```
-----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-----
```

单击Submit按钮。

第二步：创建密钥环

在菜单栏上，导航到Admin > AAA > Security > Public Key Management > Key Rings。



名称：必填（输入名称）。

证书：如果使用思科APIC通过密钥环生成证书签名请求(CSR)，请勿添加任何内容。或者，如果您已经有CA在前面的步骤中签名的证书内容，则可通过在思科APIC之外生成私钥和CSR来添加签名证书内容。

模数：必填（点击所需密钥强度的单选按钮）。

证书颁发机构：必需。从下拉列表中，选择之前创建的证书颁发机构。

私钥：如果使用思科APIC通过密钥环生成CSR，请勿添加任何内容。或者，添加用于为您输入的签名证书生成CSR的私钥。

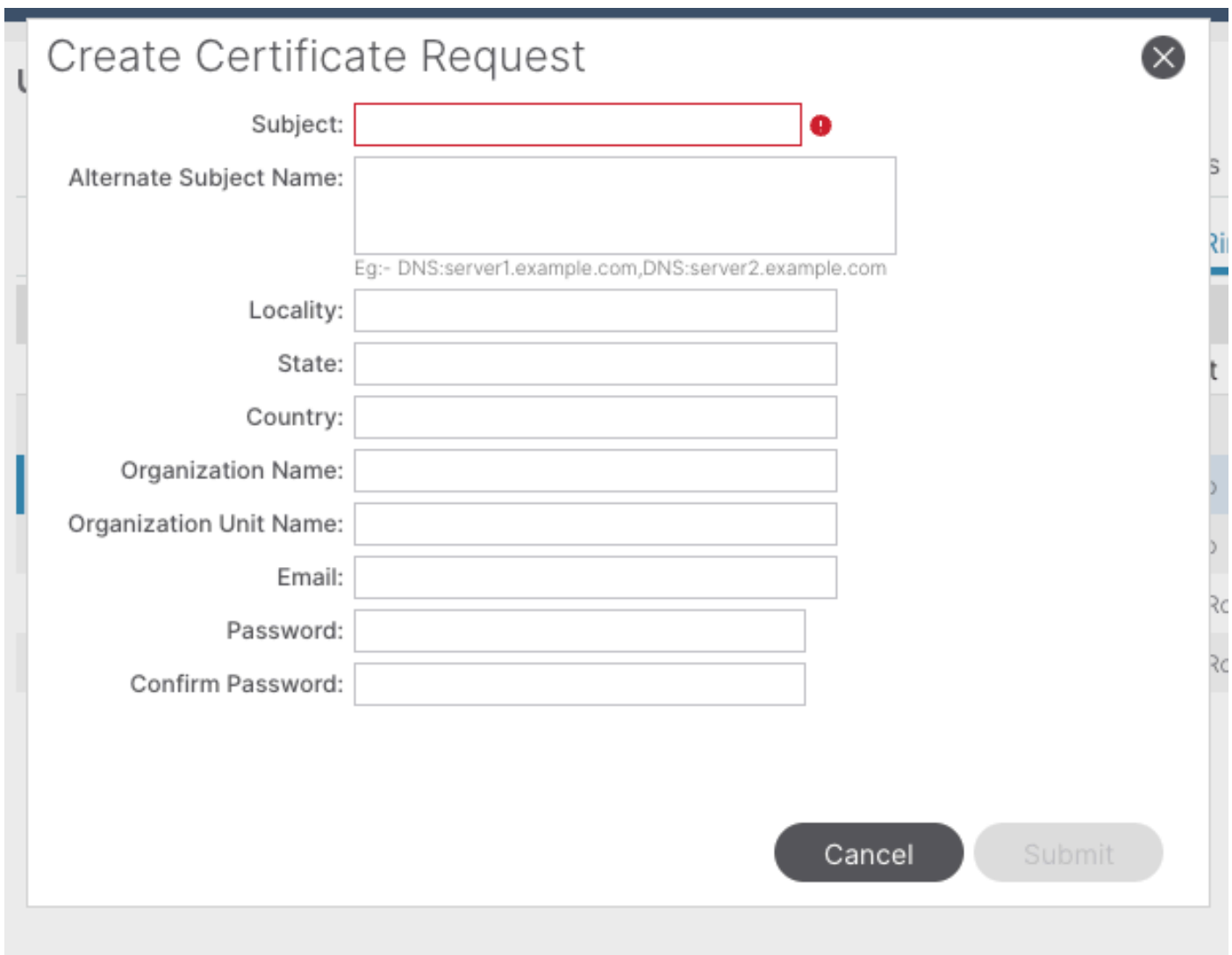
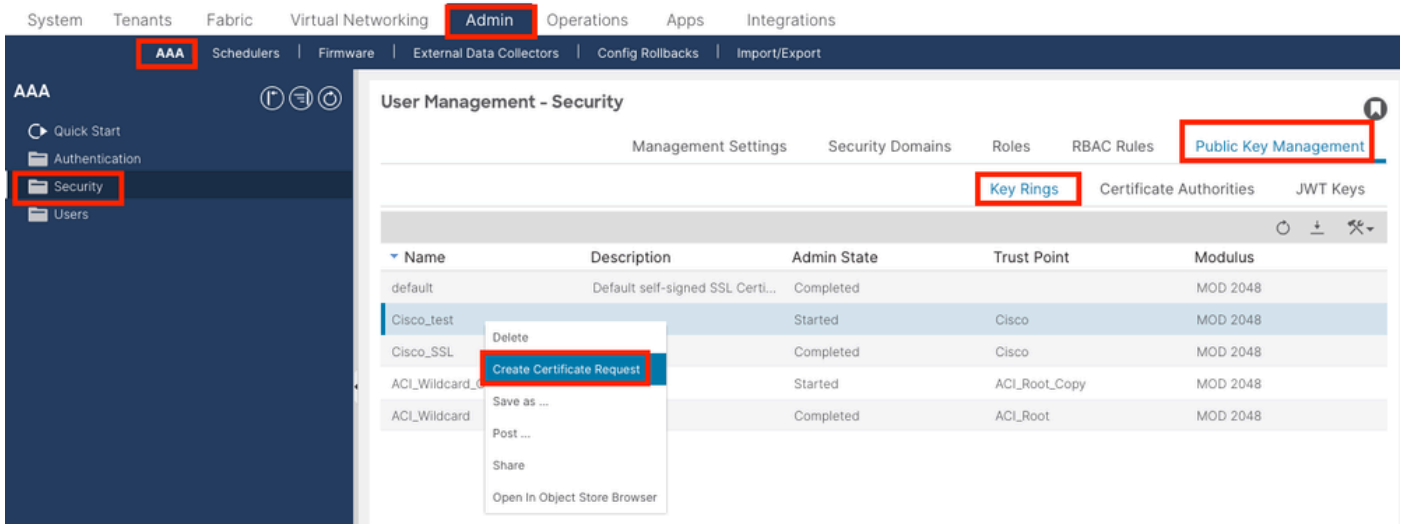


注意：如果不想使用系统生成的私钥和CSR并使用自定义私钥和证书，则只需填写四个项目：名称、证书、证书颁发机构和私钥。提交后，您只需执行最后一个步骤，即步骤5。

单击Submit按钮。

第三步：生成私钥和CSR

在菜单栏上，导航到Admin > AAA > Security > Public Key Management > Key Rings。

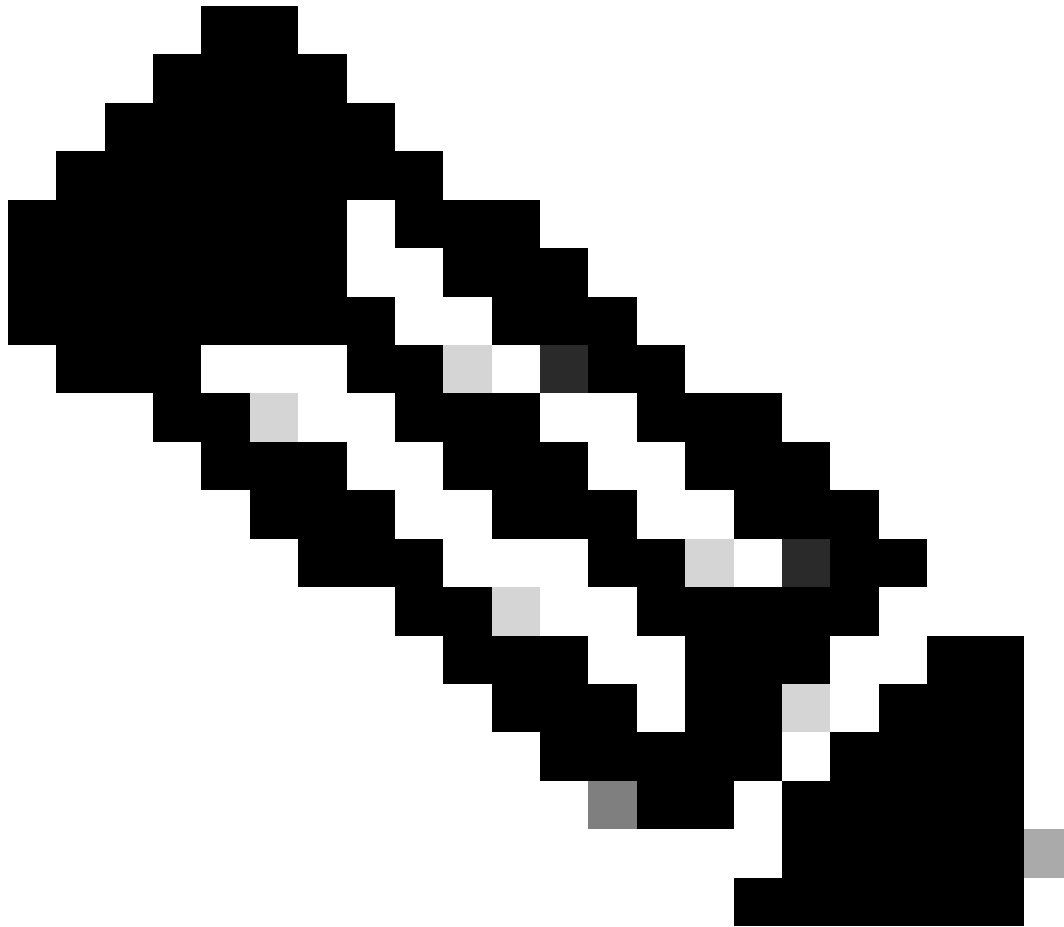


主题：必需。输入CSR的公用名称(CN)。

可以使用通配符输入思科 APIC的完全限定域名(FQDN)，但在现代证书中，通常建议输入证书的可识别名称并在备用主题名称字段中输入所有思科 APIC的FQDN(也称为SAN - 主题备用名称)，因为许多现代浏览器期望SAN字段中包含FQDN。

备用主题名称：必填。输入allCisco APIC的FQDN，例如DNS:apic1.example.com,DNS:apic2.example.com,DNS:apic3.example.com或DNS:*example.com。

或者，如果希望SAN匹配IP地址，请输入思科APIC的IP地址，格式为：IP:192.168.1.1。



注意：可以在此字段中使用域名服务器(DNS)名称、IPv4地址或二者的组合。不支持IPv6地址。

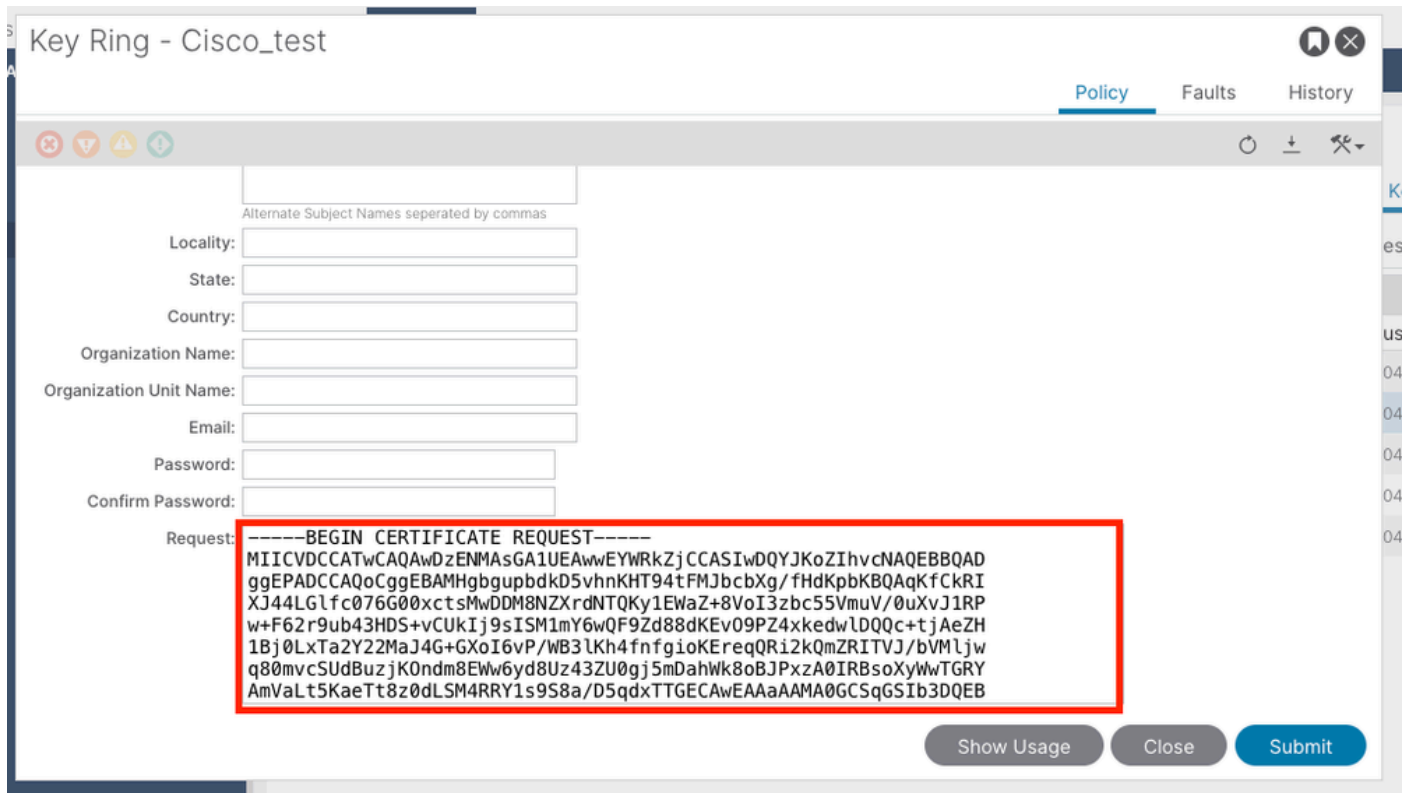
根据您正在申请的CA组织的要求填写其余字段，以便颁发证书。

单击Submit按钮。

第四步：获取CSR并将其发送到CA组织

在菜单栏上，导航到Admin > AAA > Security > Public Key Management > Key Rings。

双击您的create **Key Ring**名称并找到**Request**选项。请求中的内容是CSR。



Key Ring - Cisco_test

Policy | Faults | History

Alternate Subject Names separated by commas

Locality:

State:

Country:

Organization Name:

Organization Unit Name:

Email:

Password:

Confirm Password:

Request:

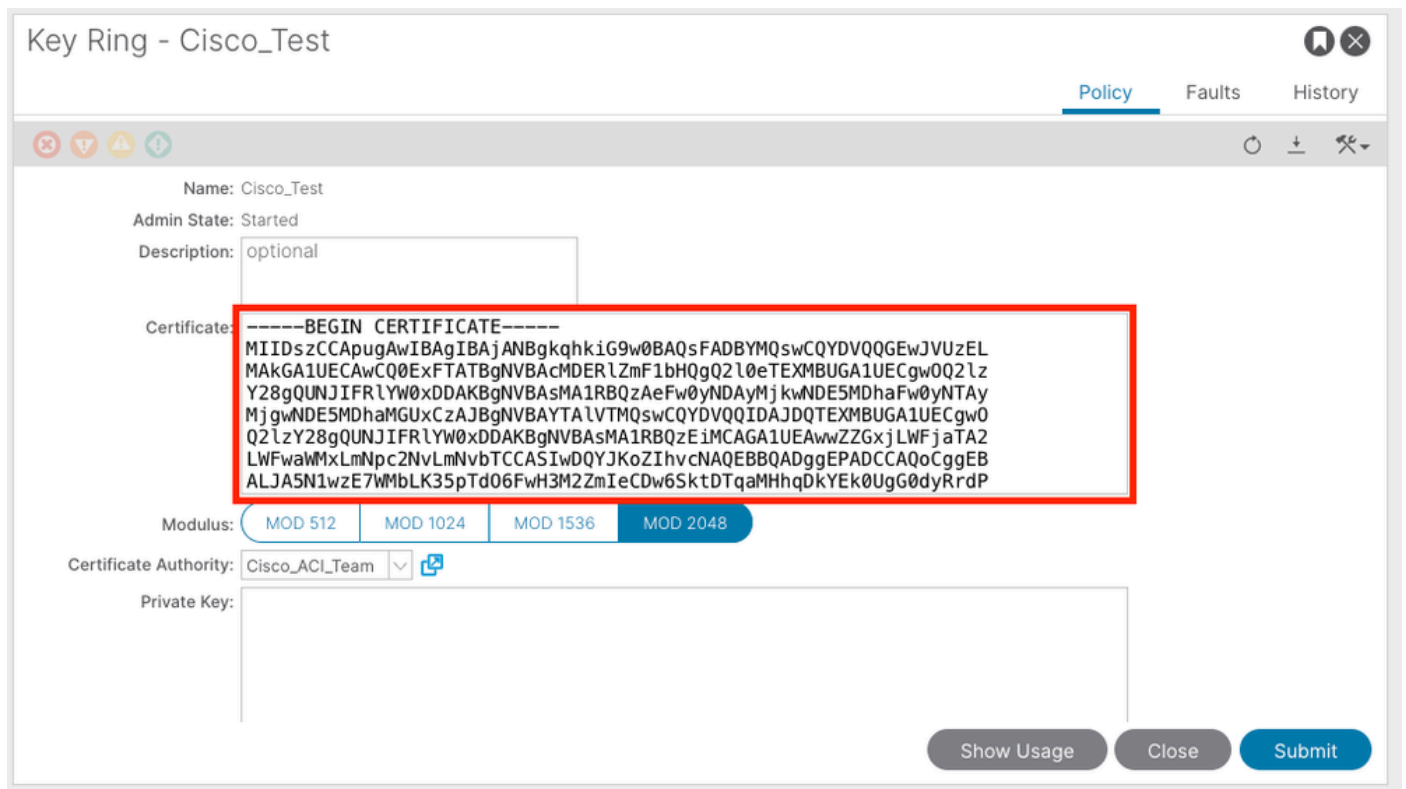
```
-----BEGIN CERTIFICATE REQUEST-----
MIICVDCCATwCAQAwDzENMAsgA1UEAwEYWRkZjCCASIwDQYJKoZIhvcNAQEBBQAD
ggEPADCCAQoCggEBAMHgbgubdkD5vhnKHT94tFMJbcXg/fHdKpbKBQAqKfCkRI
XJ44LGlfC076G00xctSMwDDM8NZrdNTQKy1EWaZ+8VoI3zbc55VmuV/0uXvJ1RP
w+F62r9ub43HDS+vCUkIj9sISM1mY6wQF9Zd88dKEv09PZ4xkedwLDQqc+tjAeZH
1Bj0LxTa2Y22MaJ4G+GXoI6vP/WB3lKh4fnfgioKEreqQRi2kQmZRITVJ/bVMljw
q80mvcSudBuzjK0ndm8EwW6yd8Uz43ZU0gj5mDahWk8oBJPxxA0IRBsoXyWwTGRY
AmVaLt5KaeTt8z0dLSM4RRY1s9S8a/D5qdxTTGECawEAAaAAMA0GCSqGSIB3DQEB
```

Show Usage | Close | Submit

复制请求的所有内容并将其发送到CA。

CA使用其私钥对CSR执行签名验证。

从CA获取签名证书后，它会将该证书复制到证书中。



Key Ring - Cisco_Test

Policy | Faults | History

Name: Cisco_Test

Admin State: Started

Description: optional

Certificate:

```
-----BEGIN CERTIFICATE-----
MIIDSzCCApuGAWIBAgIBAJANBgkqhkiG9w0BAQsFADBMYswCQYDVQQGEwJVUzEL
MAKGA1UECAwCQ0ExFTATBgNVBACMDERlZmF1bH0gQ2l0eTEwMDU0MjE0MjE0
Y28gQUNJIFRlYW0xDDAKBgNVBAsMA1RBQzAeFw0yNDYyMjE0MjE0MjE0MjE0
MjE0MjE0MjE0MjE0MjE0MjE0MjE0MjE0MjE0MjE0MjE0MjE0MjE0MjE0MjE0
Q2l0eTEwMDU0MjE0MjE0MjE0MjE0MjE0MjE0MjE0MjE0MjE0MjE0MjE0MjE0
LWFwaWxLmNpc2NvLmNvbTCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEB
ALJA5N1wzE7WmbLK35pTd06FwH3M2ZmIeCDw6SktdTqaMHhqDkYek0UgG0dyRrDP
```

Modulus: MOD 512 | MOD 1024 | MOD 1536 | MOD 2048

Certificate Authority: Cisco_ACI_Team

Private Key:

Show Usage | Close | Submit



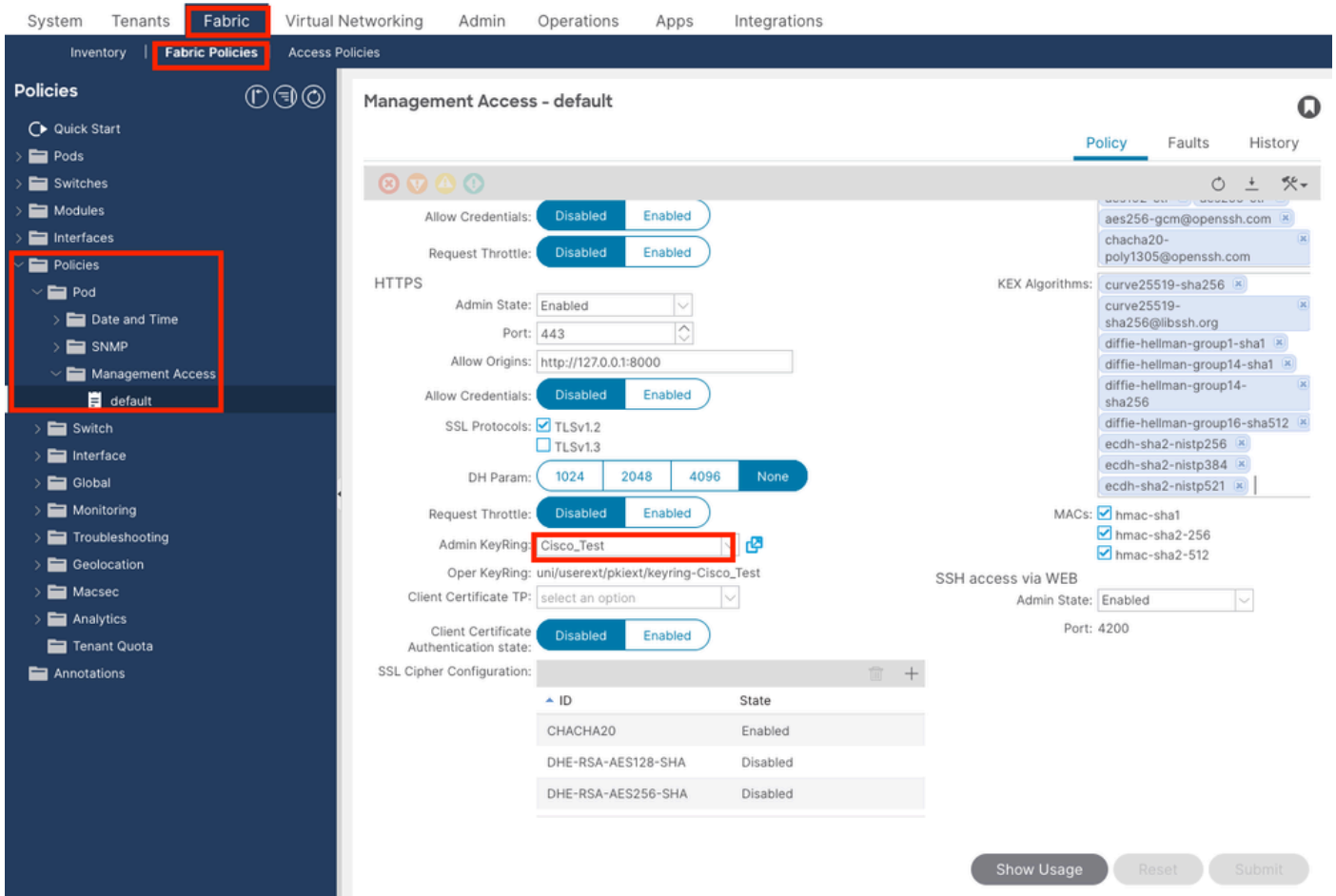
注意：每个证书都必须符合固定格式。

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

单击Submit按钮。

第五步：在Web上更新签名证书

在菜单栏上，导航到Fabric > Fabric Policies > Policies > Pod > Management Access > Default。



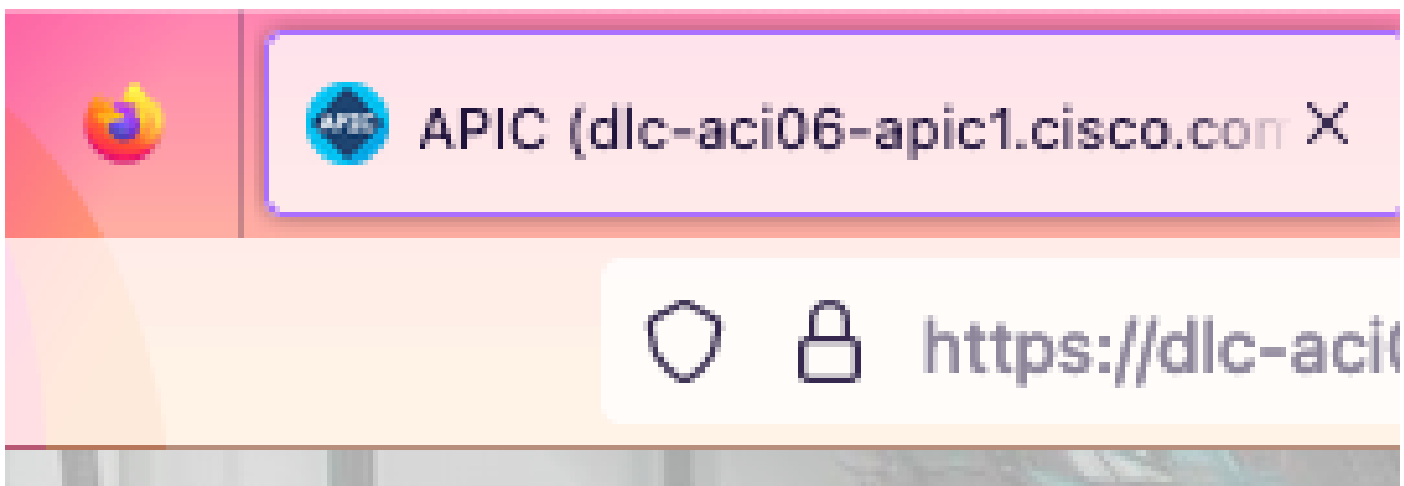
在Admin KeyRing下拉列表中，选择所需的KeyRing。

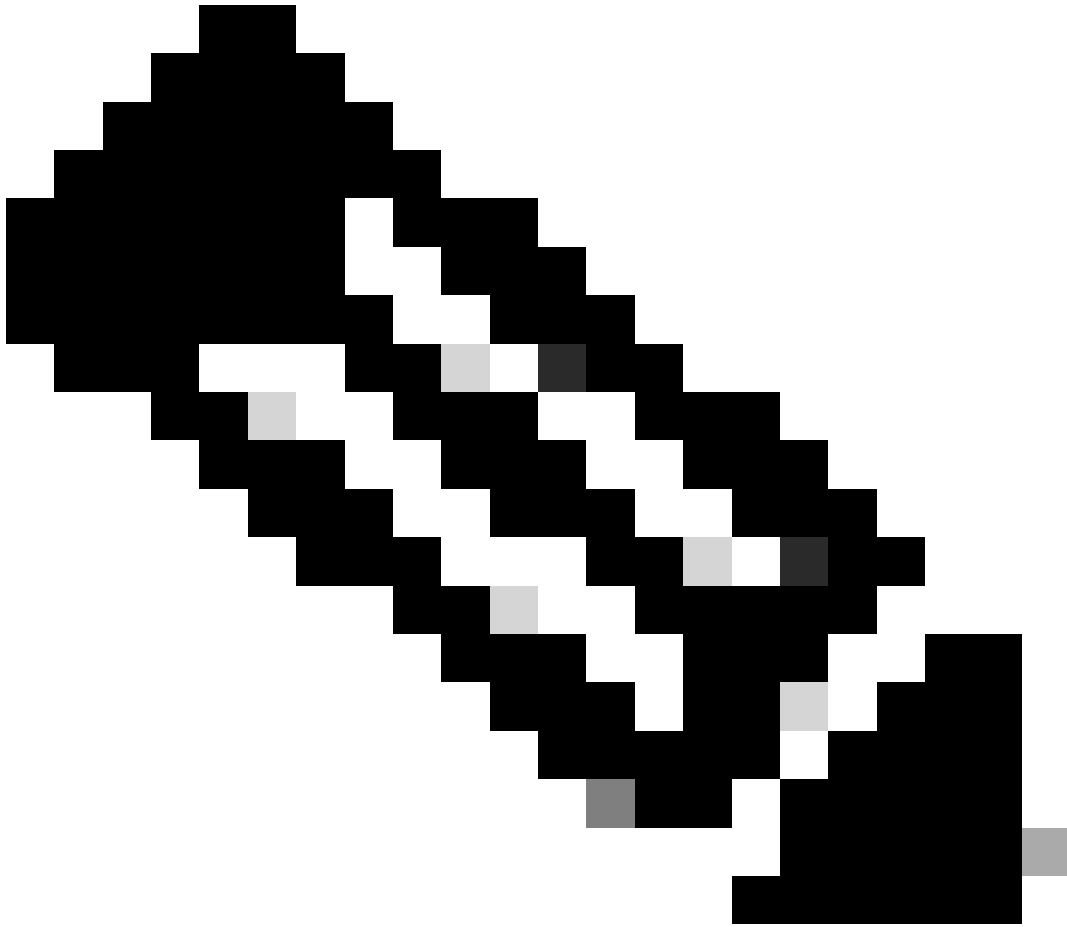
单击Submit按钮。

点击提交后，由于证书原因会出现错误。使用新证书刷新。

验证

访问APIC GUI后，APIC使用CA签名的证书进行通信。在浏览器中查看证书信息以对其进行验证。



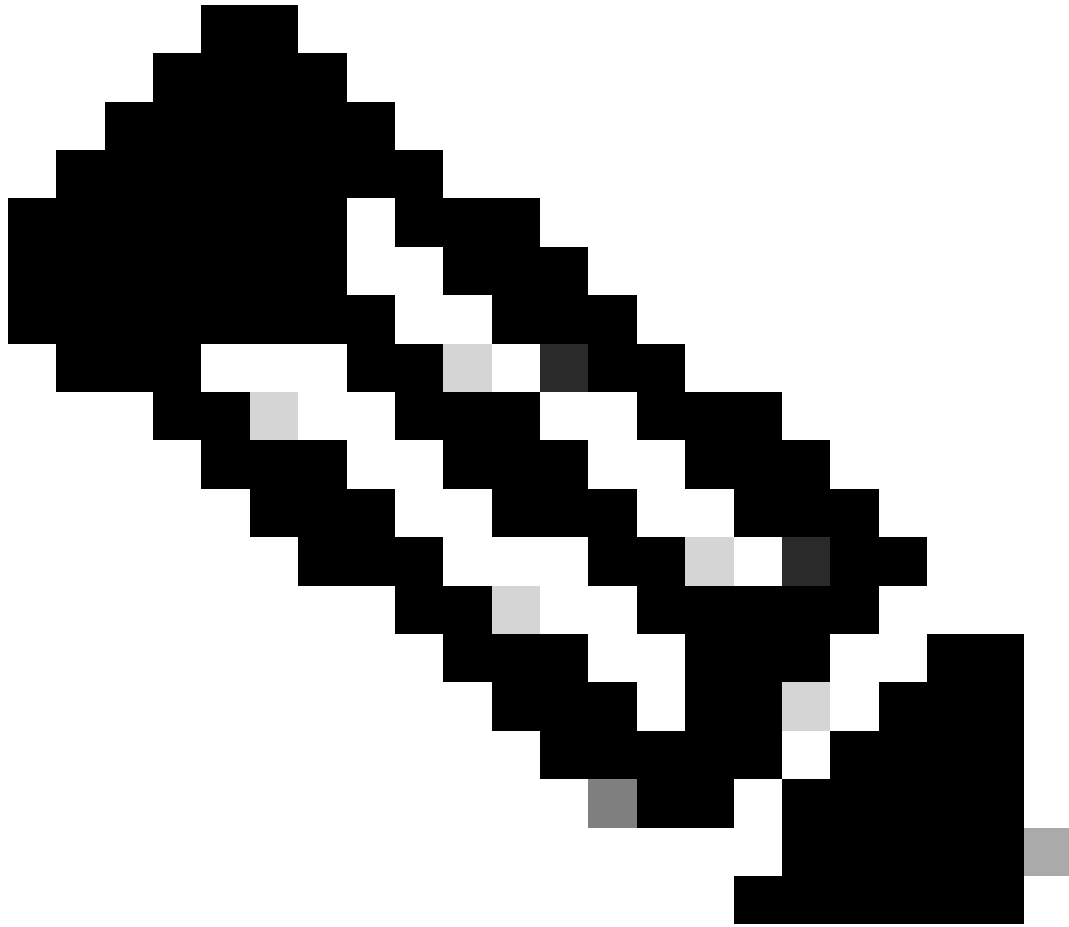


注意：在不同的浏览器中查看HTTPS证书的方法并不完全相同。有关特定方法，请参阅浏览器的用户指南。

故障排除

如果浏览器仍然提示APIC GUI不受信任，请在浏览器中验证GUI的证书是否与密钥环中提交的证书一致。

您需要信任在计算机或浏览器上颁发证书的CA根证书。



注意：Google Chrome浏览器必须验证证书的SAN才能信任此证书。

在使用自签名证书的APIC中，证书过期警告在极少数情况下会出现。

在Keyring中查找证书，使用证书解析工具来解析证书，然后将其与浏览器中使用的证书进行比较。

如果密钥环中的证书已续订，请创建新的管理访问策略并应用该策略。

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

如果Keyring中的证书未自动续订，请联系思科TAC获取更多帮助。

相关信息

- [思科APIC安全配置指南5.2\(x\)版](#)
- [思科技术支持和下载](#)

关于此翻译

思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。