

Configurar certificado HTTPS de GUI de ACI APIC

Contenido

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Configurar](#)

[Configuraciones](#)

[Paso 1. Importar el certificado raíz o el certificado intermedio de la autoridad de la CA](#)

[Paso 2. Crear llavero](#)

[Paso 3. Generar clave privada y CSR](#)

[Paso 4. Obtenga el CSR y envíelo a la organización de la CA](#)

[Paso 5. Actualizar el certificado de firma en Internet](#)

[Verificación](#)

[Troubleshoot](#)

[Información Relacionada](#)

Introducción

Este documento describe la configuración de SSL personalizado y certificados SSL autofirmados.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Firmas y certificados digitales
- Proceso de emisión de certificados por la organización de la autoridad certificadora (CA)

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Controlador de infraestructura de política de aplicación (APIC)
- Navegador
- ACI con 5.2 (8e)

La información que contiene este documento se creó a partir de los dispositivos en un ambiente

de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Configurar

Después de inicializar el dispositivo, utiliza el certificado autofirmado como certificado SSL para HTTPS. El certificado autofirmado es válido durante 1000 días.

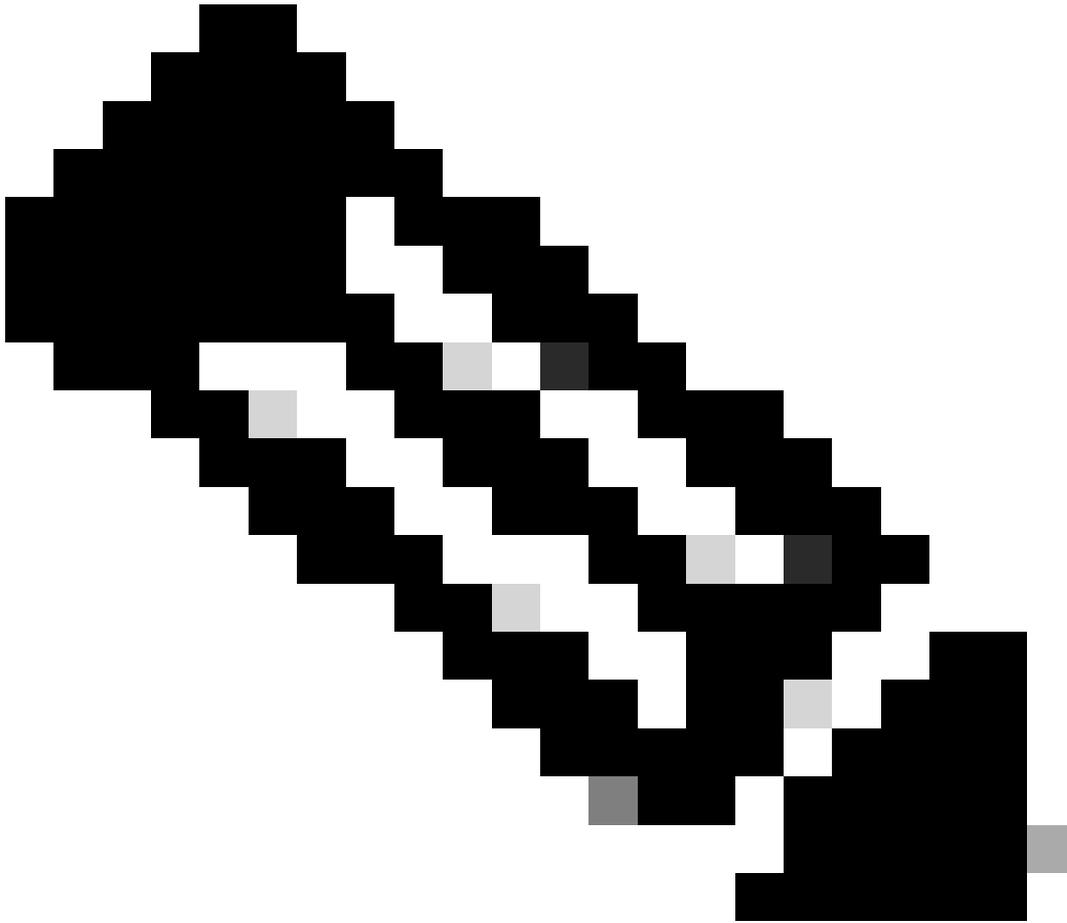
De forma predeterminada, el dispositivo renueva y genera automáticamente un nuevo certificado autofirmado un mes antes de que caduque el certificado autofirmado.

Configuraciones

El dispositivo utiliza un certificado autofirmado. Al acceder a la GUI de APIC, el navegador le indica que el certificado no es de confianza. Para resolver este problema, este documento utiliza una autoridad de CA de confianza para firmar el certificado.



Paso 1. Importar el certificado raíz o el certificado intermedio de la autoridad de la CA



Nota: si está utilizando el certificado raíz de la CA para firmar directamente, puede importar el certificado raíz de la CA. Pero si está utilizando un certificado intermedio para la firma, debe importar la cadena de certificados completa, es decir: el certificado raíz y los certificados intermedios menos fiables.

En la barra de menús, desplácese hasta 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 'Admin' menu item is highlighted in red. The 'AAA' menu item is also highlighted in red. The 'Security' menu item is highlighted in red. The 'Public Key Management' menu item is highlighted in red. The 'Certificate Authorities' menu item is highlighted in red. The 'Create Certificate Authority' button is highlighted in red.

Name	Description	FP	N	Actions
ACI_Root		[Cert 0] d7:29:6e:1c:60:26:4...	1	Delete
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

Nombre: **obligatorio**.

Formule el contenido según sus reglas de denominación. Puede contener `_`, pero no puede contener caracteres especiales en inglés, como: `, . ; ' " : | + * / = ` ~ ! @ # $ % ^ & ()` y espacios.

Descripción: **Opcional**.

Cadena de certificación: **obligatorio**.

Especifique el certificado raíz de la CA de confianza y el certificado intermedio de la CA.



Nota: Cada certificado debe ajustarse a un formato fijo.

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

Haga clic en el botón **Submit**.

Paso 2. Crear llavero

En la barra de menús, desplácese hasta Admin > AAA > Security > Public Key Management > Key Rings.

The screenshot shows the Cisco APIC Admin console. The top navigation bar includes System, Tenants, Fabric, Virtual Networking, Admin, Operations, Apps, and Integrations. The Admin menu is expanded, showing AAA, Schedulers, Firmware, External Data Collectors, Config Rollbacks, and Import/Export. The AAA menu is further expanded to show Authentication, Security, and Users. The Security menu is selected, leading to the 'User Management - Security' page. This page has tabs for Management Settings, Security Domains, Roles, RBAC Rules, Public Key Management, Certificate Authorities, and JWT Keys. The 'Public Key Management' tab is active, and the 'Key Rings' sub-tab is selected. A table lists existing key rings with columns for Name, Description, Admin State, Trust Point, and Modulus. A 'Create Key Ring' button is visible in the top right of the table area.

The 'Create Key Ring' dialog box is shown. It contains the following fields and options:

- Name:** A text input field with a red border and a red error icon.
- Description:** A text input field with the value 'optional'.
- Certificate:** A large text area for pasting certificate content.
- Modulus:** A set of radio buttons with options: MOD 512, MOD 1024, MOD 1536, and MOD 2048. The MOD 2048 option is selected.
- Certificate Authority:** A dropdown menu with the text 'select an option'.
- Private Key:** A large text area for pasting private key content.

Below the Private Key field, there is a note: "If you want to use an externally generated private key, please provide it here". At the bottom right, there are 'Cancel' and 'Submit' buttons.

Nombre:**obligatorio** (introduzca un nombre).

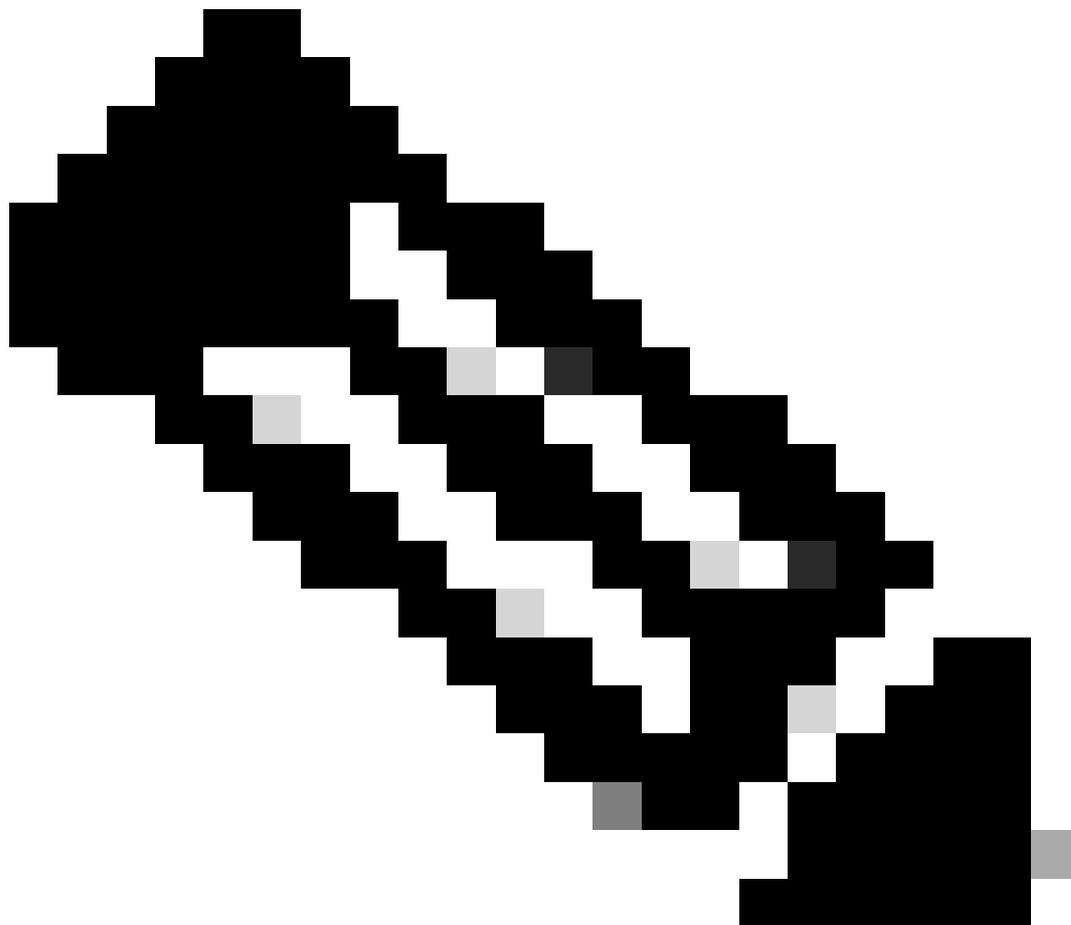
Certificado:**no agregue** ningún contenido si genera una solicitud de firma de certificado (CSR) mediante Cisco APIC a través del anillo de claves. Como alternativa, agregue el contenido del certificado firmado si ya tiene uno firmado por la CA de los pasos anteriores mediante la generación de una clave privada y CSR fuera de Cisco APIC.

Módulo: **obligatorio** (haga clic en el botón de opción de la intensidad de tecla deseada).

Autoridad de certificación: **obligatorio**. En la lista desplegable, elija la entidad emisora de certificados que creó anteriormente.

Clave privada:**no agregue** ningún contenido si genera una CSR mediante el Cisco APIC a través del anillo de claves. También puede agregar la

clave privada utilizada para generar la CSR del certificado firmado que ha especificado.

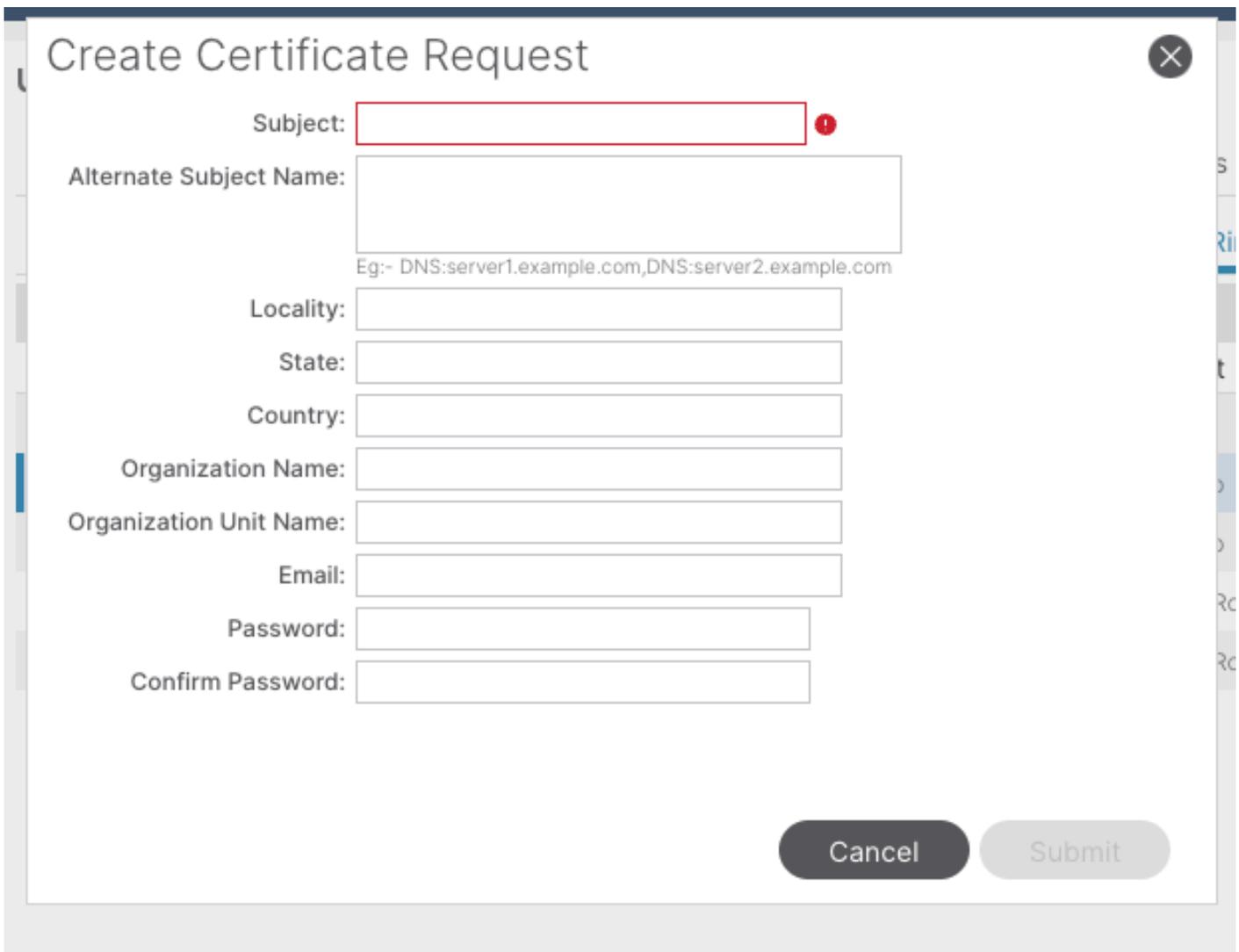
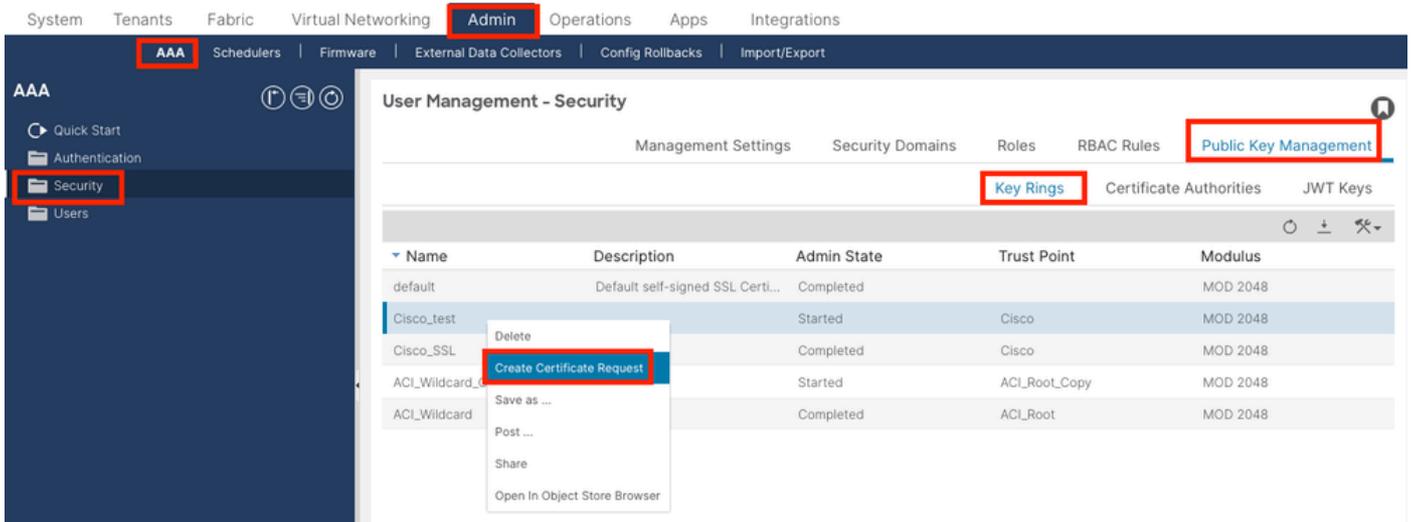


Nota: Si no desea utilizar la clave privada generada por el sistema y CSR, así como una clave privada y un certificado personalizados, sólo debe rellenar cuatro campos: Nombre, Certificado, Autoridad certificadora y Clave privada. Después de enviar, solo tiene que realizar el último paso, el paso 5.

Haga clic en el botón **Submit**.

Paso 3. Generar clave privada y CSR

En la barra de menús, desplácese hasta Admin > AAA > Security > Public Key Management > Key Rings.

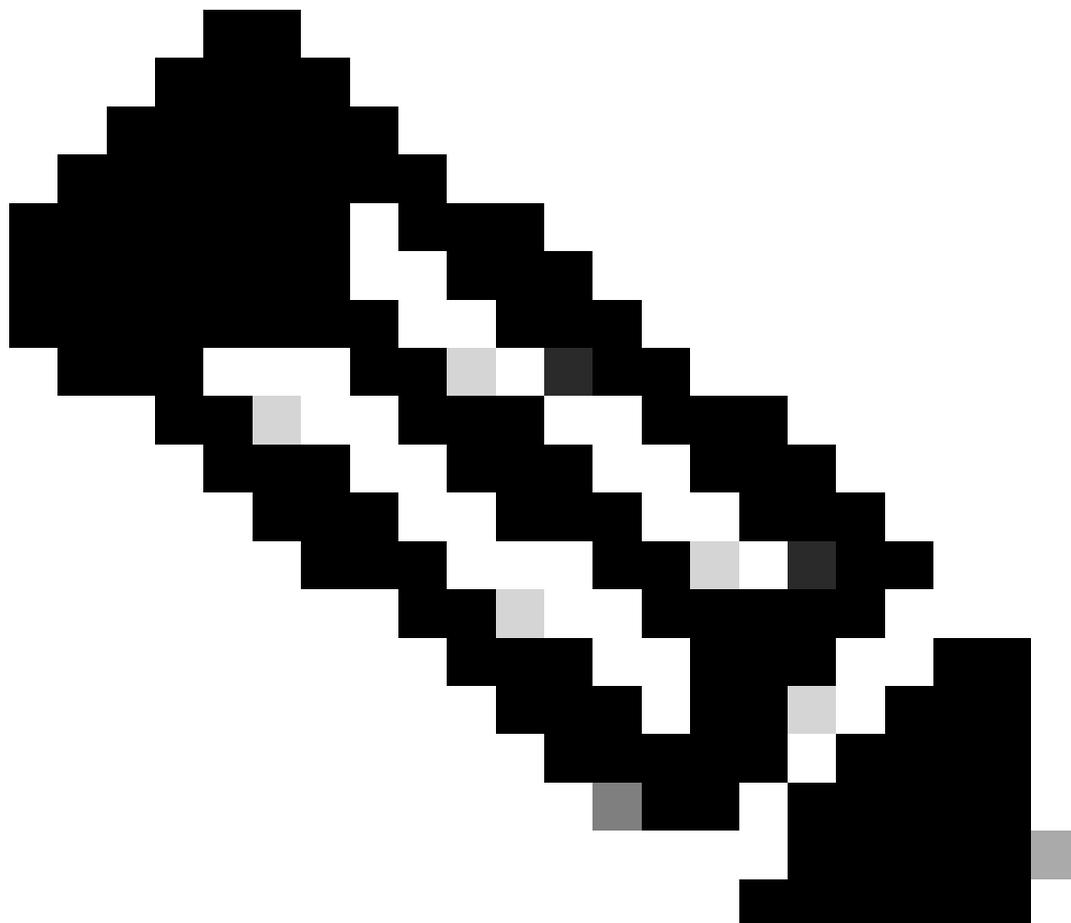


Asunto: **Obligatorio.** Introduzca el nombre común (CN) del CSR.

Puede introducir el nombre de dominio completo (FQDN) de los Cisco APIC mediante un comodín, pero en un certificado moderno, se recomienda generalmente que introduzca un nombre identificable del certificado e introduzca el FQDN de todos los Cisco APIC en el campo Nombre de asunto alternativo (también conocido como SAN - Nombre alternativo de asunto) porque muchos exploradores modernos esperan el FQDN en el campo SAN.

Nombre de asunto alternativo: **obligatorio**. Introduzca el FQDN de todos los Cisco APIC, como
DNS:apic1.example.com,DNS:apic2.example.com,DNS:apic3.example.com o DNS:*example.com.

Como alternativa, si desea que la SAN coincida con una dirección IP, introduzca las direcciones IP de Cisco APIC con el formato:
IP:192.168.1.1.



Nota: En este campo puede utilizar nombres de servidor de nombres de dominio (DNS), direcciones IPv4 o una combinación de ambos. No se admiten direcciones IPv6.

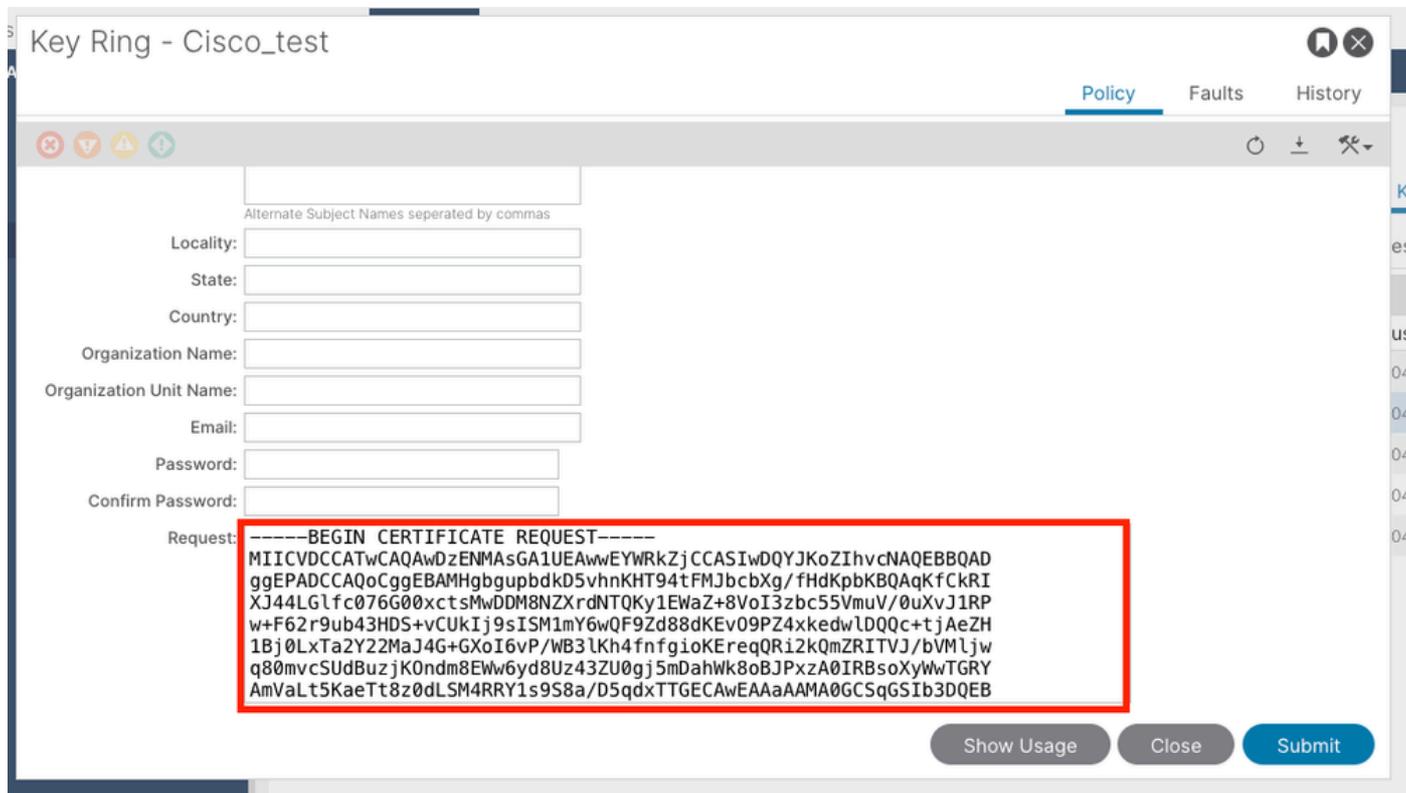
Rellene los campos restantes de acuerdo con los requisitos de la organización de CA que esté solicitando para emitir el certificado.

Haga clic en el botón **Submit**.

Paso 4. Obtenga el CSR y envíelo a la organización de la CA

En la barra de menús, desplácese hasta Admin > AAA > Security > Public Key Management > Key Rings.

Haga doble clic en el nombre del **Key Ring** y busque la opción **Request**. El contenido de la solicitud es el CSR.



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

```
-----BEGIN CERTIFICATE REQUEST-----
MIICVDCCATwCAQAwDzENMAsgA1UEAwEYWRkZjCCASIwDQYJKoZIhvcNAQEBBQAD
ggEPADCCAQoCggEBAMHgbgubdkD5vhnKHT94tFMJbcbXg/fHdKpbKBQAgfCKRI
XJ44LGlfC076G00xctSmwDDM8NZXrdNTQKy1Ewaz+8VoI3zbc55VmuV/0uXvJ1RP
w+F62r9ub43HDS+vCUkIj9sISM1mY6wQF9Zd88dKEv09PZ4xkedwLDQ0c+tjAeZH
1Bj0LxTa2Y22MaJ4G+GXoI6vP/WB3lKh4fnfgioKEreqQR12kQmZRITVJ/bVMljw
q80mvcSUDBuzjK0ndm8EWw6yd8Uz43ZU0gj5mDahWk8oBJPxzA0IRBsoXyWwTGRY
AmValt5KaeTt8z0dLSM4RRY1s9S8a/D5qdxTTGECAwEAAaAAMA0GCSqGSIb3DQEBA
```

Copie todo el contenido de la solicitud y envíela a la CA.

La CA utiliza su clave privada para realizar la verificación de firma en su CSR.

Después de obtener el certificado firmado de la CA, copia el certificado en el certificado.



Name: Cisco_Test

Admin State: Started

Description: optional

Certificate:

```
-----BEGIN CERTIFICATE-----  
MIIDSzCCApugAwIBAgIBAgjANBgqhkiG9w0BAQsFADBVMQswCQYDVQGEwJVUzEL  
MAKGA1UECAwCQ0EFTATBgNVBACMDERlZmF1bHQgQ2l0eTEEXMBUGA1UECgw0Q2Lz  
Y28gQUNJIFRlYW0xDDAKBgNVBAsMA1RBQzAeFw0yNDYyMjE5MDU5MDhaFw0yNTAy  
MjE5MDU5MDhaMGUCzAJBGVBAYTAjVMTQswCQYDVQQLIDQTEEXMBUGA1UECgw0  
Q2LzY28gQUNJIFRlYW0xDDAKBgNVBAsMA1RBQzEiMCAGA1UEAwwZZGxjLWFlaTA2  
LWFwawMxLmNpc2NvLmNvbTCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEB  
ALJA5N1wzE7WmBk35pTd06FwH3M2ZmIeCDw6SktDTqaMHhqDkYEK0UgG0dyRrdP
```

Modulus: MOD 512 MOD 1024 MOD 1536 MOD 2048

Certificate Authority: Cisco_ACL_Team

Private Key:

Show Usage Close Submit



Nota: Cada certificado debe ajustarse a un formato fijo.

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

Haga clic en el botón **Submit**.

Paso 5. Actualizar el certificado de firma en Internet

En la barra de menús, desplácese hasta Fabric > Fabric Policies > Políticas > Pod > Management Access > Default.

The screenshot shows the APIC GUI configuration for the 'Management Access - default' policy. The 'Fabric' tab is selected, and the 'Fabric Policies' section is expanded. The 'Management Access' policy is selected, and the 'Admin KeyRing' is set to 'Cisco_Test'. The 'Submit' button is highlighted.

Configuration details for 'Management Access - default':

- Allow Credentials: Disabled
- Request Throttle: Disabled
- HTTPS:
 - Admin State: Enabled
 - Port: 443
 - Allow Origins: http://127.0.0.1:8000
 - Allow Credentials: Disabled
 - SSL Protocols: TLSv1.2, TLSv1.3
 - DH Param: 1024, 2048, 4096, None
 - Request Throttle: Disabled
 - Admin KeyRing: Cisco_Test
 - Oper KeyRing: uni/userext/pkiext/keyring-Cisco_Test
 - Client Certificate TP: select an option
 - Client Certificate Authentication state: Disabled
- SSH access via WEB:
 - Admin State: Enabled
 - Port: 4200
- MACs: hmac-sha1, hmac-sha2-256, hmac-sha2-512
- KEX Algorithms: curve25519-sha256, curve25519-sha256@libssh.org, diffie-hellman-group1-sha1, diffie-hellman-group14-sha1, diffie-hellman-group14-sha256, diffie-hellman-group16-sha512, ecdh-sha2-nistp256, ecdh-sha2-nistp384, ecdh-sha2-nistp521
- SSL Cipher Configuration:

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

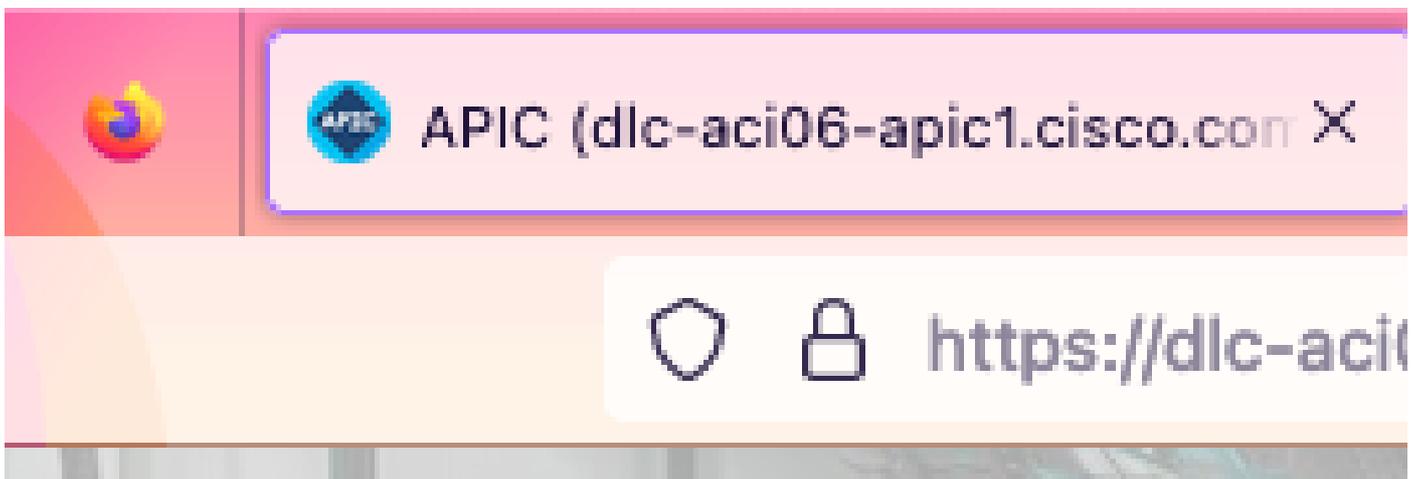
en la lista desplegable **Admin KeyRing**, elija el KeyRing que desee.

Haga clic en el botón **Submit**.

Después de hacer clic en Enviar, se produce un error por motivos de certificado. Actualice con el nuevo certificado.

Verificación

Después de acceder a la GUI de APIC, APIC utiliza el certificado firmado por la CA para comunicarse. Vea la información del certificado en el navegador para verificarla.





Nota: Los métodos para ver certificados HTTPS en diferentes navegadores no son exactamente iguales. Para obtener información sobre métodos específicos, consulte la guía del usuario del navegador.

Troubleshoot

Si el explorador sigue solicitando que la GUI de APIC no es fiable, compruebe en el explorador si el certificado de la GUI es coherente con el enviado en el anillo de claves.

Debe confiar en el **certificado raíz de CA** que emitió el certificado en su equipo o explorador.



Nota: El navegador de Google Chrome debe verificar la **SAN** del certificado para confiar en este certificado.

En los APIC que utilizan certificados autofirmados, pueden aparecer advertencias de expiración de certificados en casos excepcionales.

Busque el certificado en Keyring, utilice la herramienta de análisis de certificados para analizar el certificado y compárelo con el certificado utilizado en el navegador.

Si se renueva el certificado del anillo de claves, cree una nueva directiva de acceso a la administración y aplíquela.

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
	HTTP State	HTTP Port	HTTP Redirect	HTTPS State	HTTPS Port		
default	enabled	80	disabled	enabled	443	enabled	S

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

Si el certificado en el llavero no se renueva automáticamente, comuníquese con el TAC de Cisco para obtener más ayuda.

Información Relacionada

- [Guía de configuración de seguridad de Cisco APIC, versión 5.2\(x\)](#)
- [Soporte técnico y descargas de Cisco](#)

Acerca de esta traducción

Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).