

ACI APIC GUI HTTPS 인증서 구성

목차

[소개](#)

[사전 요구 사항](#)

[요구 사항](#)

[사용되는 구성 요소](#)

[구성](#)

[설정](#)

[1단계. CA 권한 루트 인증서 또는 중간 인증서 가져오기](#)

[2단계. 키 링 만들기](#)

[3단계. 개인 키 및 CSR 생성](#)

[4단계. CSR을 가져와 CA 조직에 보냅니다.](#)

[5단계. 웹에서 서명 인증서 업데이트](#)

[다음을 확인합니다.](#)

[문제 해결](#)

[관련 정보](#)

소개

이 문서에서는 사용자 지정 SSL 및 자체 서명 SSL 인증서의 컨피그레이션에 대해 설명합니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- 디지털 서명 및 디지털 인증서
- CA(Certificate Authority) 조직별 인증서 발급 프로세스

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- APIC(Application Policy Infrastructure Controller)
- 브라우저
- ACI 실행 5.2(8e)

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

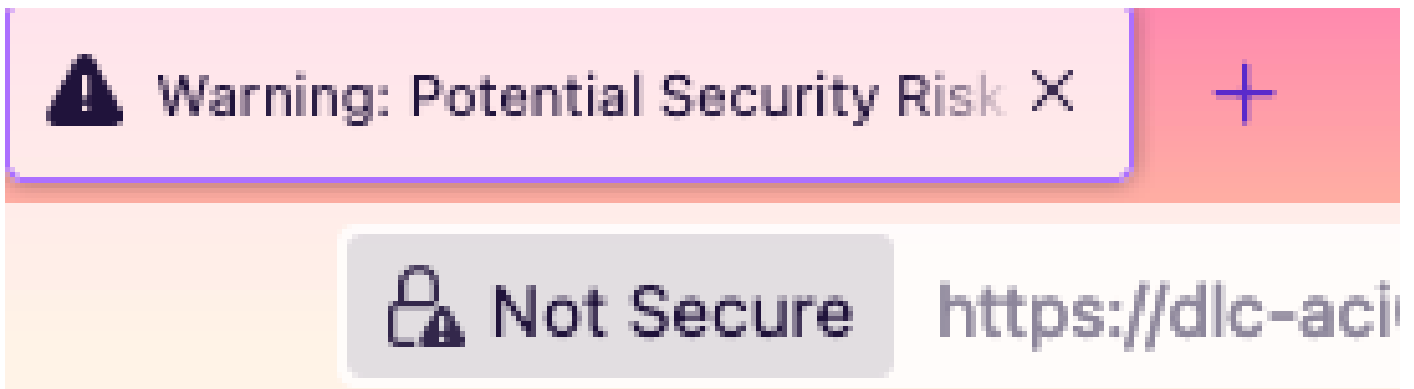
구성

디바이스가 초기화된 후에는 자체 서명 인증서를 HTTPS용 SSL 인증서로 사용합니다. 자체 서명 인증서는 1000일 동안 유효합니다.

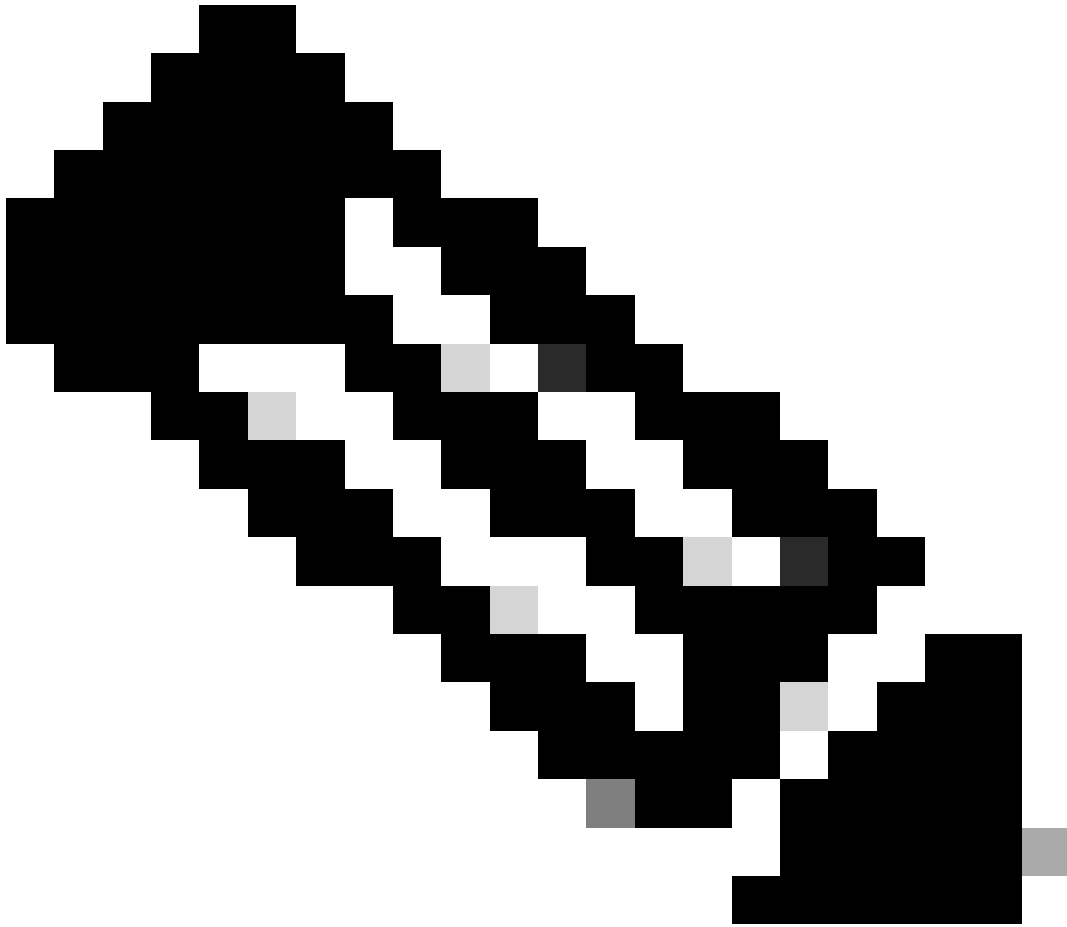
기본적으로 디바이스는 자체 서명 인증서가 만료되기 1개월 전에 자동으로 갱신하고 새 자체 서명 인증서를 생성합니다.

설정

디바이스는 자체 서명 인증서를 사용합니다. APIC GUI에 액세스할 때 브라우저에서 인증서를 신뢰할 수 없다는 프롬프트를 표시합니다. 이 문제를 해결하기 위해 이 문서에서는 신뢰할 수 있는 CA 기관을 사용하여 인증서를 서명합니다.



1단계. CA 권한 루트 인증서 또는 중간 인증서 가져오기



참고: 직접 서명하기 위해 CA 루트 인증서를 사용하는 경우 CA 루트 인증서를 가져오기만 하면 됩니다. 그러나 서명을 위해 중간 인증서를 사용하는 경우 전체 인증서 체인, 즉 루트 인증서 및 덜 신뢰할 수 있는 중간 인증서를 가져와야 합니다.

메뉴 모음에서 **로** Admin > AAA > Security > Public Key Management > Certificate Authorities 이동합니다.

The screenshot shows the Cisco ISE Admin interface. 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 expanded to show Management Settings, Security Domains, Roles, RBAC Rules, **Public Key Management**, Key Rings, **Certificate Authorities**, and JWT Keys. The Certificate Authorities menu is expanded to show a table of certificate authorities and a **Create Certificate Authority** button.

Name	Description	FP	N	
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

이름: 필수.

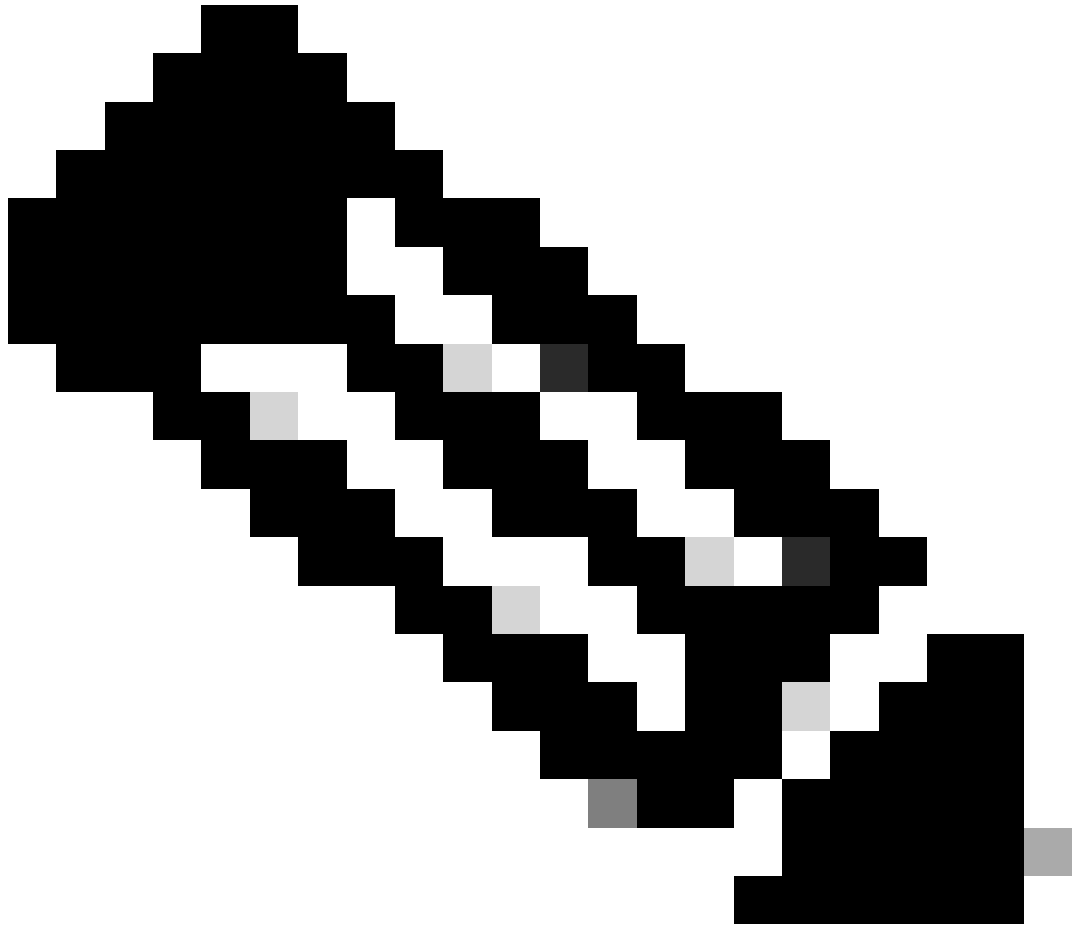
명명 규칙에 따라 내용을 공식화합니다. 예는 다음과 같은 특수 영어 문자를 포함할 수 없습니다.

, . ; ' " : | + * / = ` ~ ! @ # \$ % ^ & () 및 공백 문자입니다.

설명: 선택 사항입니다.

인증 체인: 필수.

신뢰할 수 있는 CA 루트 인증서 및 CA 중간 인증서를 입력합니다.



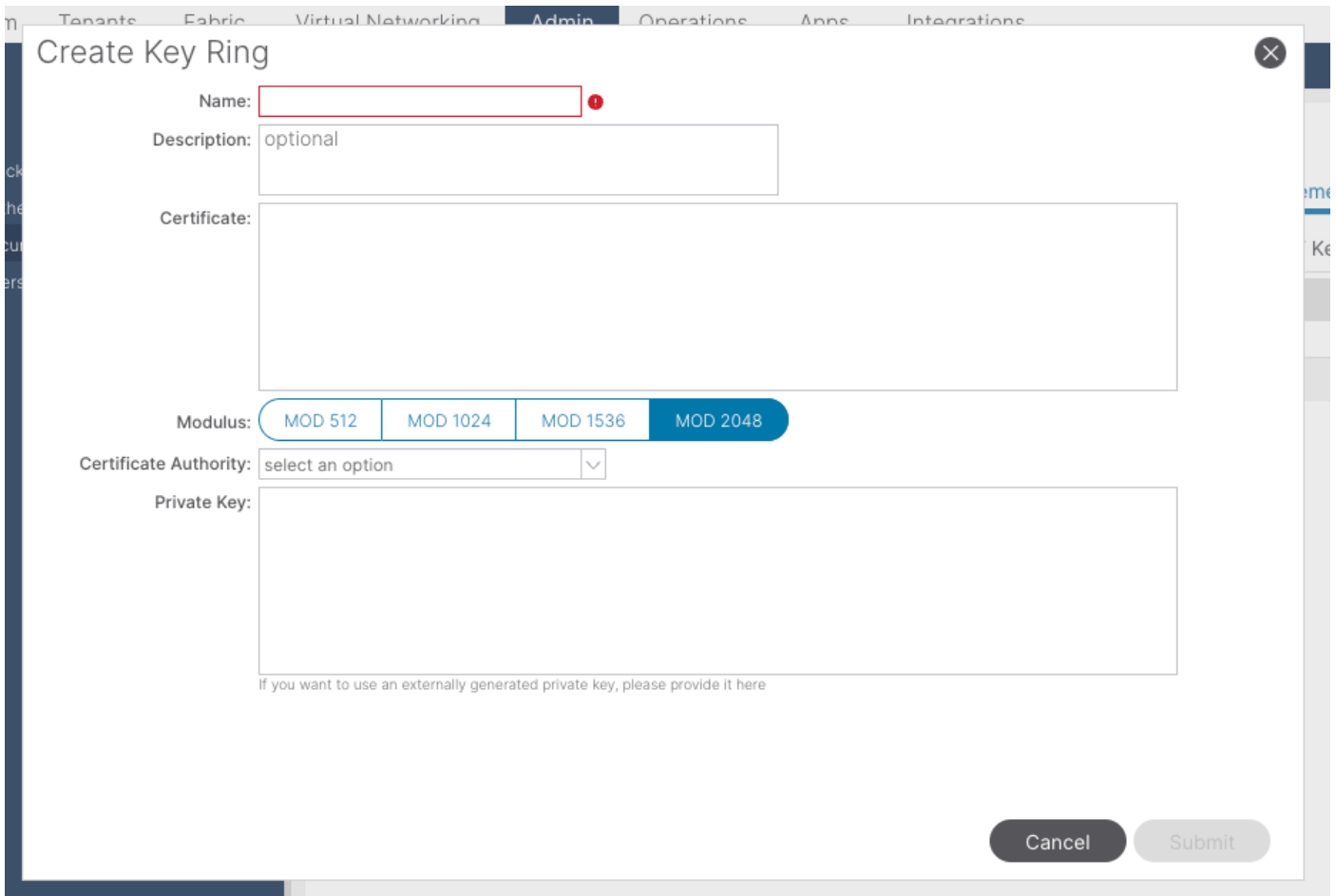
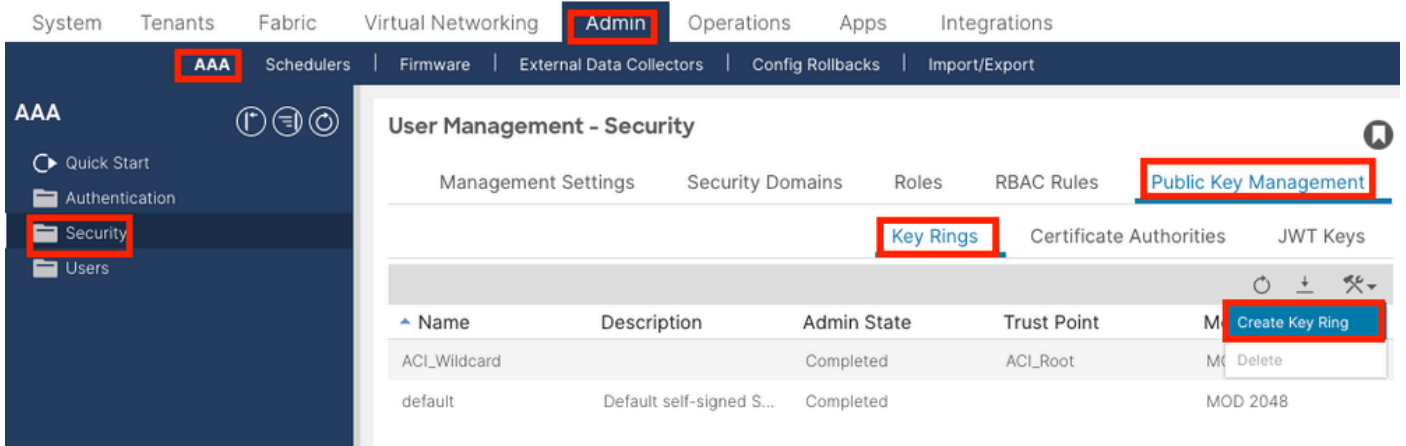
참고: 각 인증서는 고정된 형식을 준수해야 합니다.

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

Submit(제출) 버튼을 클릭합니다.

2단계. 키 링 만들기

메뉴 모음에서 로 Admin > AAA > Security > Public Key Management > Key Rings 이동합니다.



이름: 필수(이름 입력)

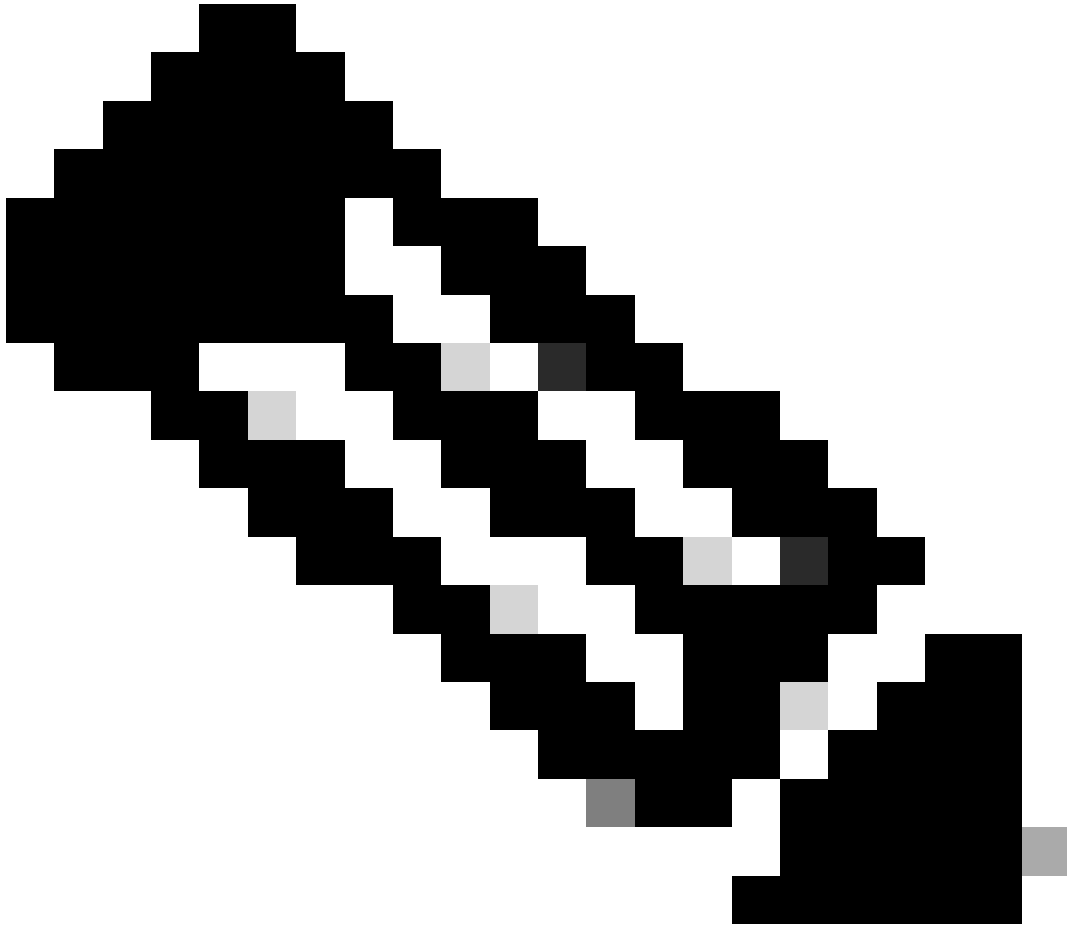
인증서: 키 링을 통해 Cisco APIC을 사용하여 CSR(Certificate Signing Request)을 생성하는 경우 콘텐츠를 추가하지 마십시오. 또는, 이전 단계에서 CA가 Cisco APIC 외부에서 개인 키 및 CSR을 생성하여 서명한 인증서 콘텐츠가 이미 있는 경우, 서명한 인증서 콘텐츠를 추가합니다.

모듈러스: 필수(원하는 키 강도를 보려면 라디오 버튼을 클릭).

인증 기관: 필수. 드롭다운 목록에서 이전에 생성한 인증 기관을 선택합니다.

Private Key(개인 키): 키 링을 통해 Cisco APIC을 사용하여 CSR을 생성하는 경우 콘텐츠를 추가하지 마십시오. 또는, 입력한 서명된

인증서에 대한 CSR을 생성하는 데 사용되는 개인 키를 추가합니다.

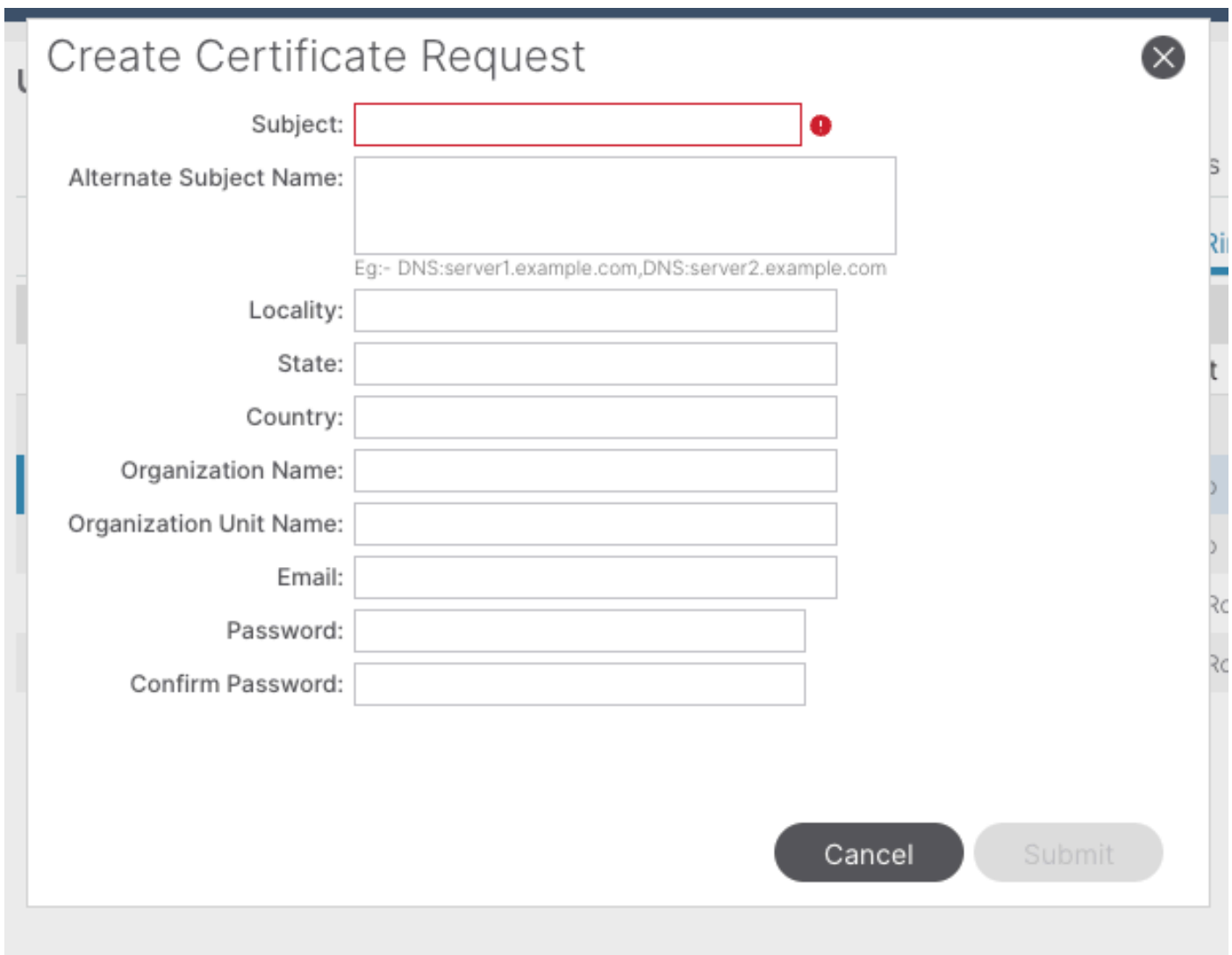
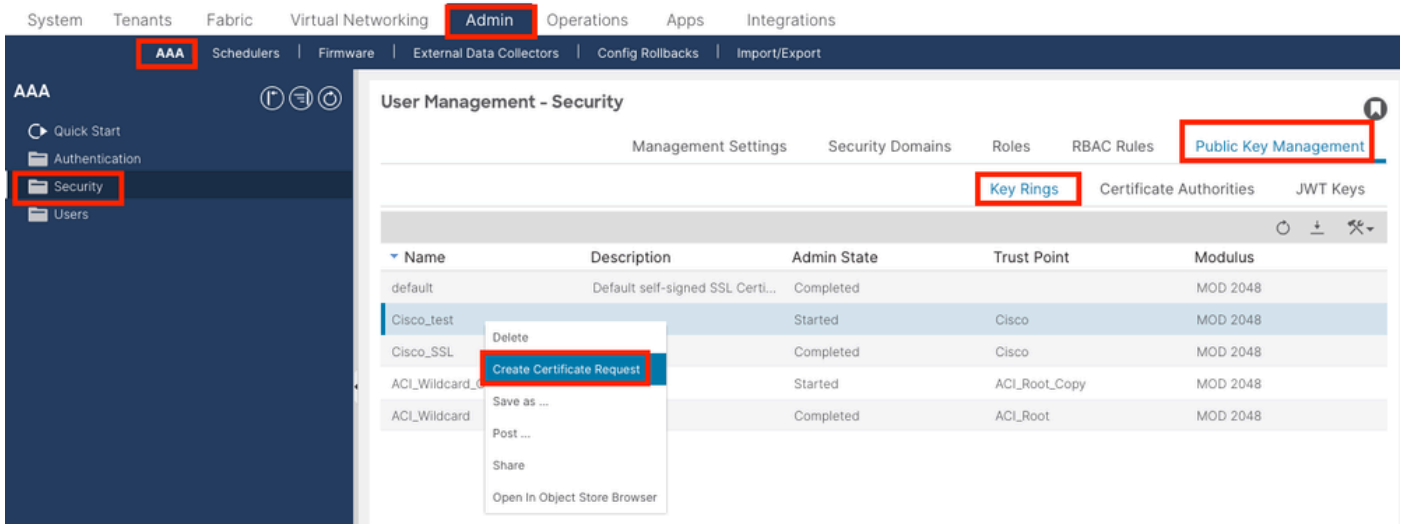


참고: 시스템 생성 개인 키 및 CSR을 사용하지 않고 사용자 지정 개인 키 및 인증서를 사용하려면 이름, 인증서, 인증 기관 및 개인 키의 4개 항목만 작성하면 됩니다. 제출 후에는 마지막 단계인 5단계만 수행하면 됩니다.

Submit(제출) 버튼을 클릭합니다.

3단계. 개인 키 및 CSR 생성

메뉴 모음에서 로 Admin > AAA > Security > Public Key Management > Key Rings 이동합니다.



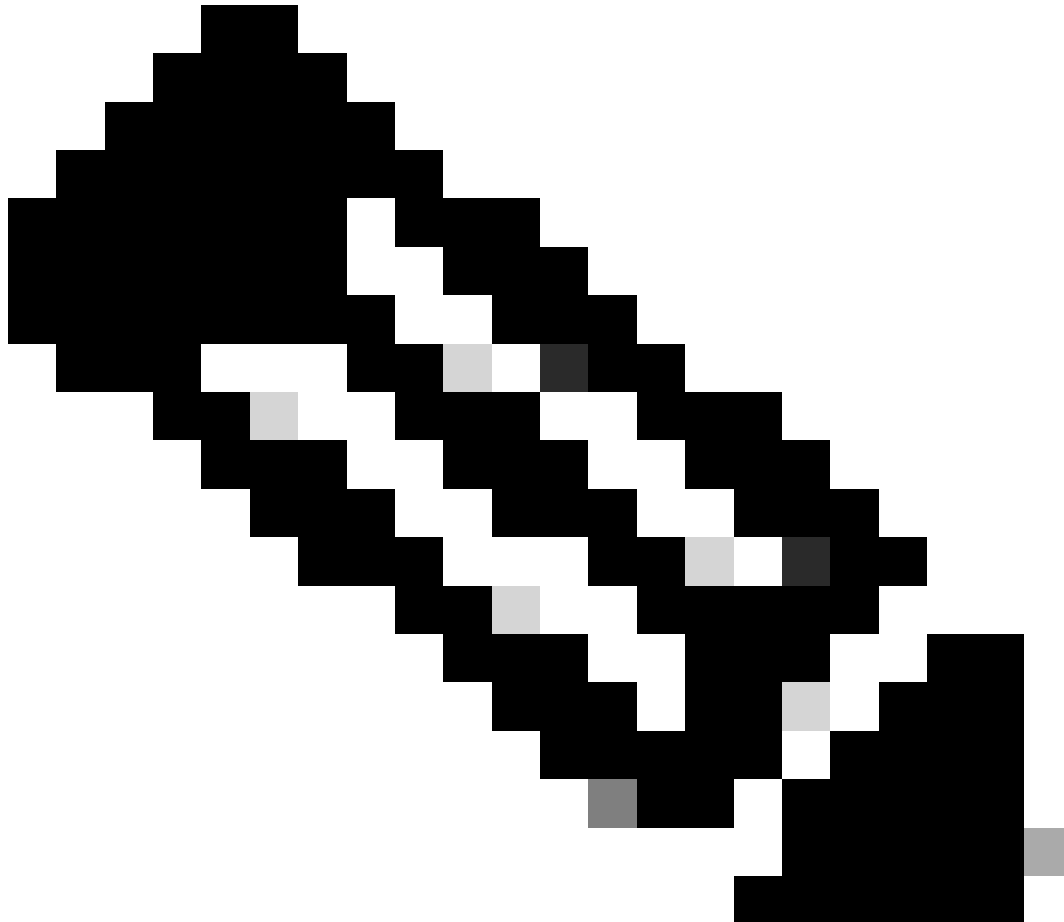
제목: 필수. CSR의 CN(Common Name)을 입력합니다.

와일드카드를 사용하여 Cisco APIC의 FQDN(Fully Qualified Domain Name)을 입력할 수 있지만, 많은 최신 브라우저에서는 SAN 필드에 FQDN을 기대하므로 최신 인증서에서는 일반적으로 인증서의 식별 가능한 이름을 입력하고 Alternate Subject Name 필드(SAN-Subject Alternative Name이라고도 함)에 모든 Cisco APIC의 FQDN을 입력하는 것이 좋습니다.

대체 주체 이름: 필수. 모든 Cisco APIC의 FQDN을 입력합니다(예: 또는

DNS:apic1.example.com,DNS:apic2.example.com,DNS:apic3.example.com)DNS:*example.com.

또는 SAN이 IP 주소와 일치하도록 하려면 Cisco APIC의 IP 주소를 IP:192.168.1.1 형식으로 입력합니다.



참고: 이 필드에서는 DNS(Domain Name Server) 이름, IPv4 주소 또는 이 둘의 혼합을 사용할 수 있습니다. IPv6 주소는 지원되지 않습니다.

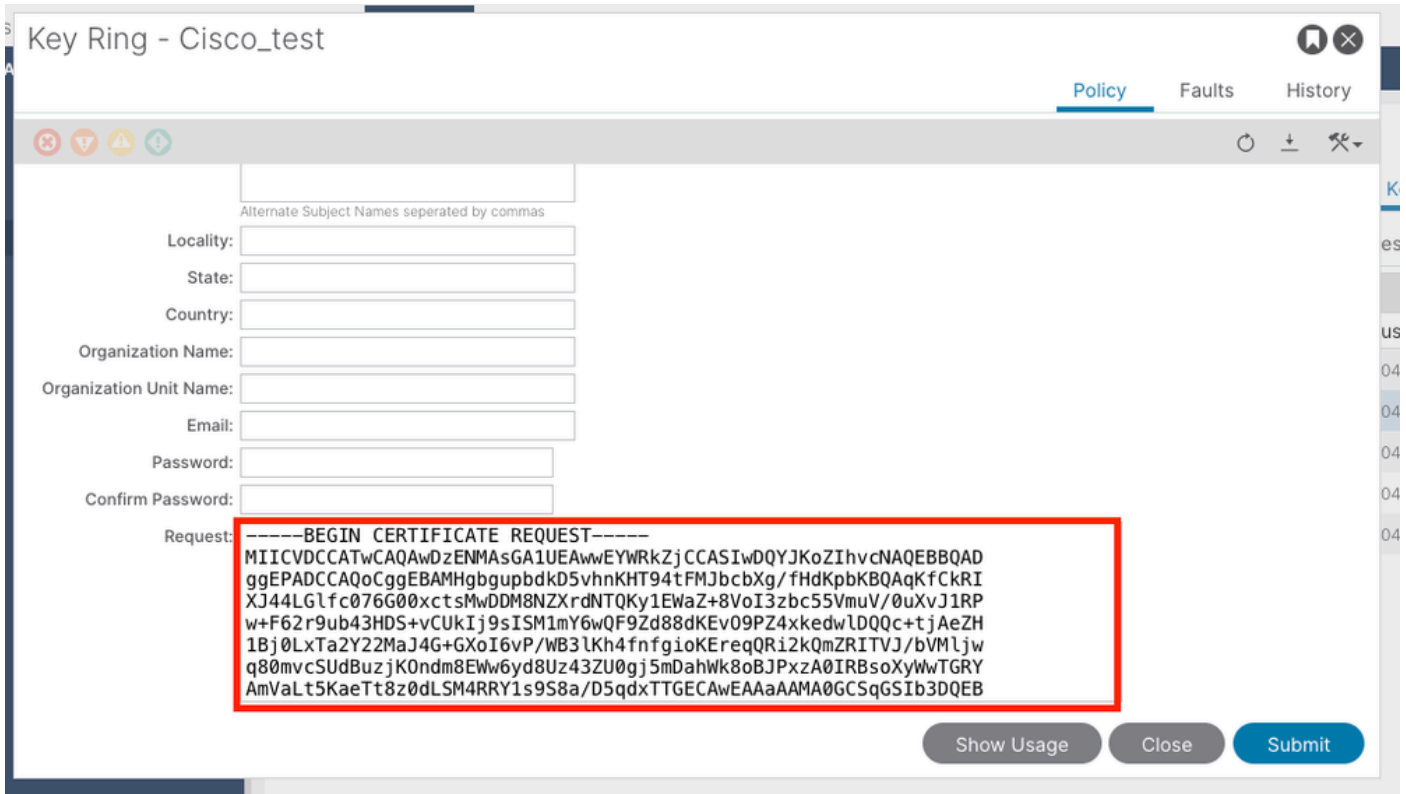
인증서를 발급하기 위해 신청하려는 CA 조직의 요구 사항에 따라 나머지 필드를 입력합니다.

Submit(제출) 버튼을 클릭합니다.

4단계. CSR을 가져와 CA 조직에 보냅니다.

메뉴 모음에서 로 Admin > AAA > Security > Public Key Management > Key Rings 이동합니다.

생성 키 링 이름을 두 번 클릭하고 요청 옵션을 찾습니다. 요청의 내용은 CSR입니다.



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

```
-----BEGIN CERTIFICATE REQUEST-----  
MIICVDCCATwCAQAwDzENMAsGA1UEAwEYWRkZjCCASIwDQYJKoZIhvcNAQEBBQAD  
ggEPADCCAQoCggEBAMHgbgubdkD5vhnKHT94tFMJbcbXg/fHdKpbKBQAgKfCKRI  
XJ44LGLfc076G00xctSMwDDM8NZXrdNTQKy1Ewaz+8VoI3zbc55VmuV/0uXvJ1RP  
w+F62r9ub43HDS+vCUkIj9sISM1mY6wQF9Zd88dKEv09PZ4xkedwLDQc+tjAeZH  
1Bj0LxTa2Y22MaJ4G+GXoI6vP/WB3lKh4fnfgioKEreqQR12kQmZRITVJ/bVMljw  
q80mvcSUDBuzjK0ndm8EWw6yd8Uz43ZU0gj5mDahWk8oBJPxzA0IRBsoXyWwTGRY  
AmValt5KaeTt8z0dLSM4RRY1s9S8a/D5qdxTTGECAwEAaAAMA0GCSqGSIb3DQEBA
```

요청의 모든 내용을 복사하여 CA에 보냅니다.

CA는 CSR에서 서명 확인을 수행하기 위해 개인 키를 사용합니다.

CA에서 서명된 인증서를 얻은 후 인증서를 인증서에 복사합니다.



Name: Cisco_Test

Admin State: Started

Description: optional

Certificate:

```
-----BEGIN CERTIFICATE-----  
MIIDszCCApugAwIBAgIBAgjANBgqhkiG9w0BAQsFADBYMQswCQYDVQQGEwJVUzEL  
MAKGA1UECAwCQ0EFTATBgNVBACMDERlZmF1bHQgQ2l0eTEEXMBUGA1UECgw0Q2Lz  
Y28gQUNJIFRlYW0xDDAKBgNVBAsMA1RBQzAeFw0yNDYyMjE5MDU5MDhaFw0yNTAy  
MjE5MDU5MDhaMGUxCzAJBgNVBAYTAlVMTQswCQYDVQQIDAJDQTEEXMBUGA1UECgw0  
Q2LzY28gQUNJIFRlYW0xDDAKBgNVBAsMA1RBQzEiMCAGA1UEAwwZZGxjLWFlaTA2  
LWFWaWxLmNpc2NvLmNvbTCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEB  
ALJA5N1wzE7WmBk35pTd06FwH3M2ZmIeCDw6SktDTqaMHhqDkYEK0UgG0dyRrdP
```

Modulus: MOD 512 MOD 1024 MOD 1536 MOD 2048

Certificate Authority: Cisco_ACL_Team

Private Key:

Show Usage Close Submit



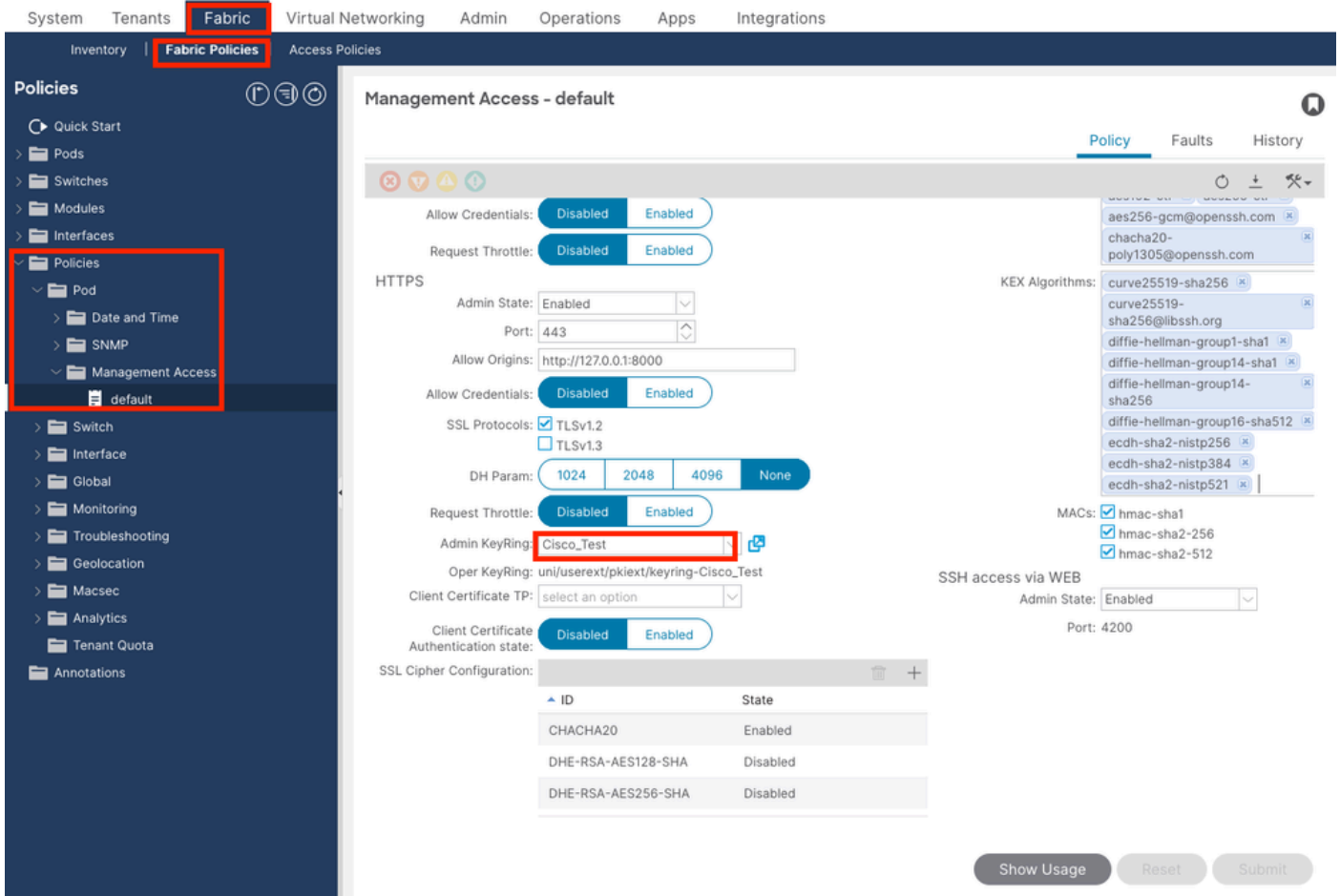
참고: 각 인증서는 고정된 형식을 준수해야 합니다.

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

Submit(제출) 버튼을 클릭합니다.

5단계. 웹에서 서명 인증서 업데이트

메뉴 모음에서 로 Fabric > Fabric Policies > Policies > Pod > Management Access > Default 이동합니다.



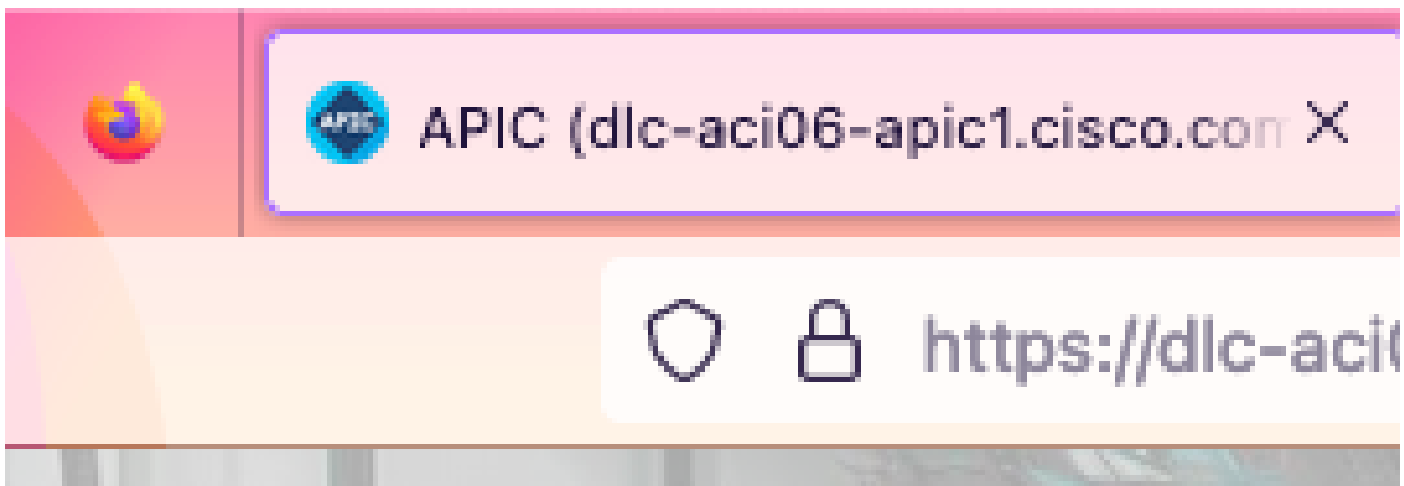
admin **KeyRing**(관리자 키링) 드롭다운 목록에서 원하는 키링을 선택합니다.

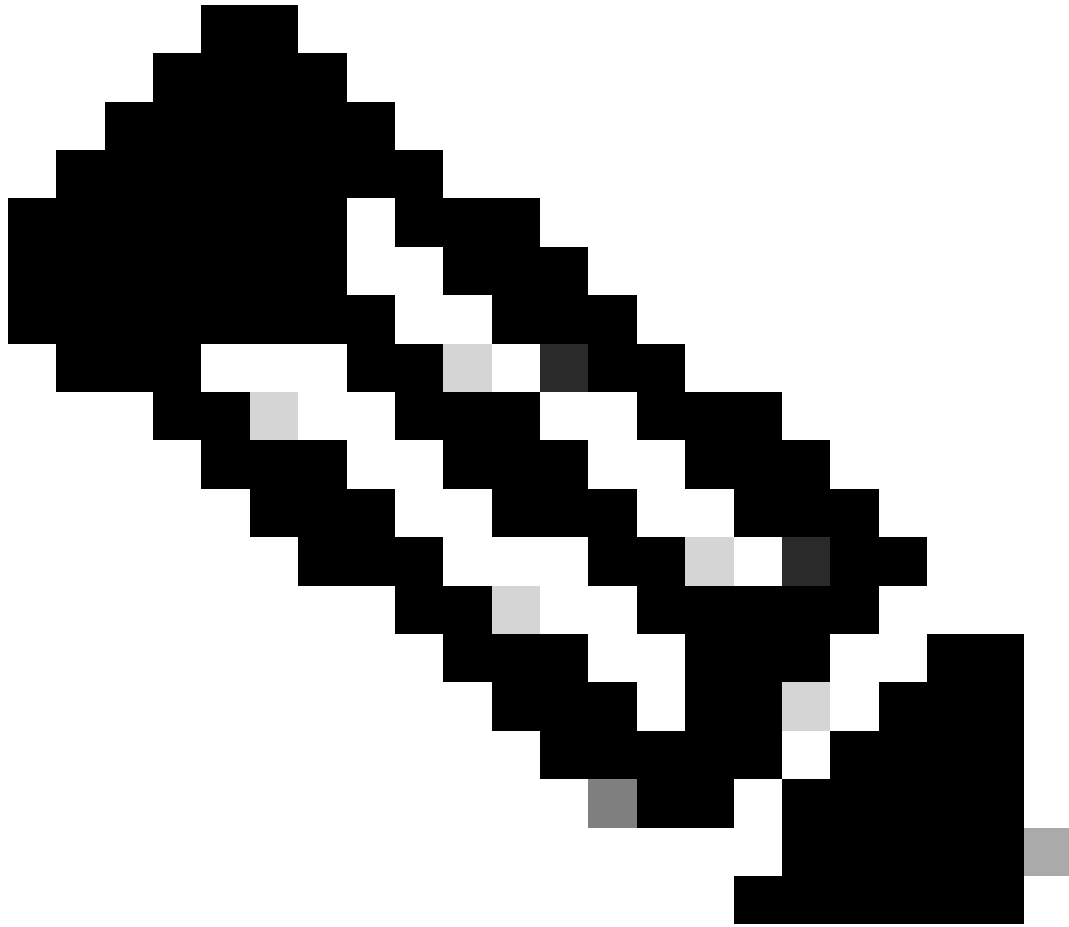
Submit(제출) 버튼을 클릭합니다.

Submit(제출)을 클릭하면 인증서 사유로 인해 오류가 발생합니다. 새 인증서로 새로 고칩니다.

다음을 확인합니다.

APIC GUI에 액세스한 후 APIC는 CA 서명 인증서를 사용하여 통신합니다. 브라우저에서 인증서 정보를 보고 확인합니다.





참고: 다른 브라우저에서 HTTPS 인증서를 보는 방법은 완전히 동일하지 않습니다. 특정 방법은 브라우저의 사용 설명서를 참조하십시오.

문제 해결

APIC GUI를 신뢰할 수 없다는 메시지가 브라우저에 계속 표시되면 브라우저에서 GUI의 인증서가 Keyring에서 제출한 인증서와 일치하는지 확인합니다.

컴퓨터 또는 브라우저에서 인증서를 발급한 CA 루트 인증서를 신뢰해야 합니다.



참고: 이 인증서를 신뢰하려면 Google Chrome 브라우저에서 인증서의 SAN을 확인해야 합니다.

자체 서명 인증서를 사용하는 APIC에서는 드물게 인증서 만료 경고가 나타날 수 있습니다.

Keyring에서 인증서를 찾고, 인증서를 구문 분석하기 위해 certificate parsing tool을 사용하여 브라우저에서 사용되는 인증서와 비교합니다.

키링의 인증서가 갱신되는 경우 새 관리 액세스 정책을 생성하고 적용합니다.

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

키링의 인증서가 자동으로 갱신되지 않을 경우 Cisco TAC에 자세한 내용을 문의하십시오.

관련 정보

- [Cisco APIC 보안 컨피그레이션 가이드, 릴리스 5.2\(x\)](#)
- [Cisco 기술 지원 및 다운로드](#)

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.