

ACI APIC GUI HTTPS-certificaat configureren

Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Configureren](#)

[Configuraties](#)

[Stap 1. Voer het basiscertificaat van de CA-autoriteit of het tussentijds certificaat in](#)

[Stap 2. Toetsenring maken](#)

[Stap 3. Generate Private Key en CSR](#)

[Stap 4. Haal de MVO en stuur het naar de CA-organisatie](#)

[Stap 5. Update het ondertekeningscertificaat op het web](#)

[Verifiëren](#)

[Problemen oplossen](#)

[Gerelateerde informatie](#)

Inleiding

Dit document beschrijft de configuratie van Aangepaste SSL- en zelfondertekende SSL-certificaten.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Digitale handtekeningen en digitale certificaten
- Procedure voor de afgifte van certificaten door een organisatie van de certificeringsinstantie (CA)

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- Application Policy Infrastructure Controller-controller (APIC)
- Browser
- ACI met 5.2 (8e)

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een

opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

Configureren

Nadat het apparaat is geïntialiseerd, gebruikt het het zelfondertekende certificaat als SSL-certificaat voor HTTPS. Het zelfondertekende certificaat is 1000 dagen geldig.

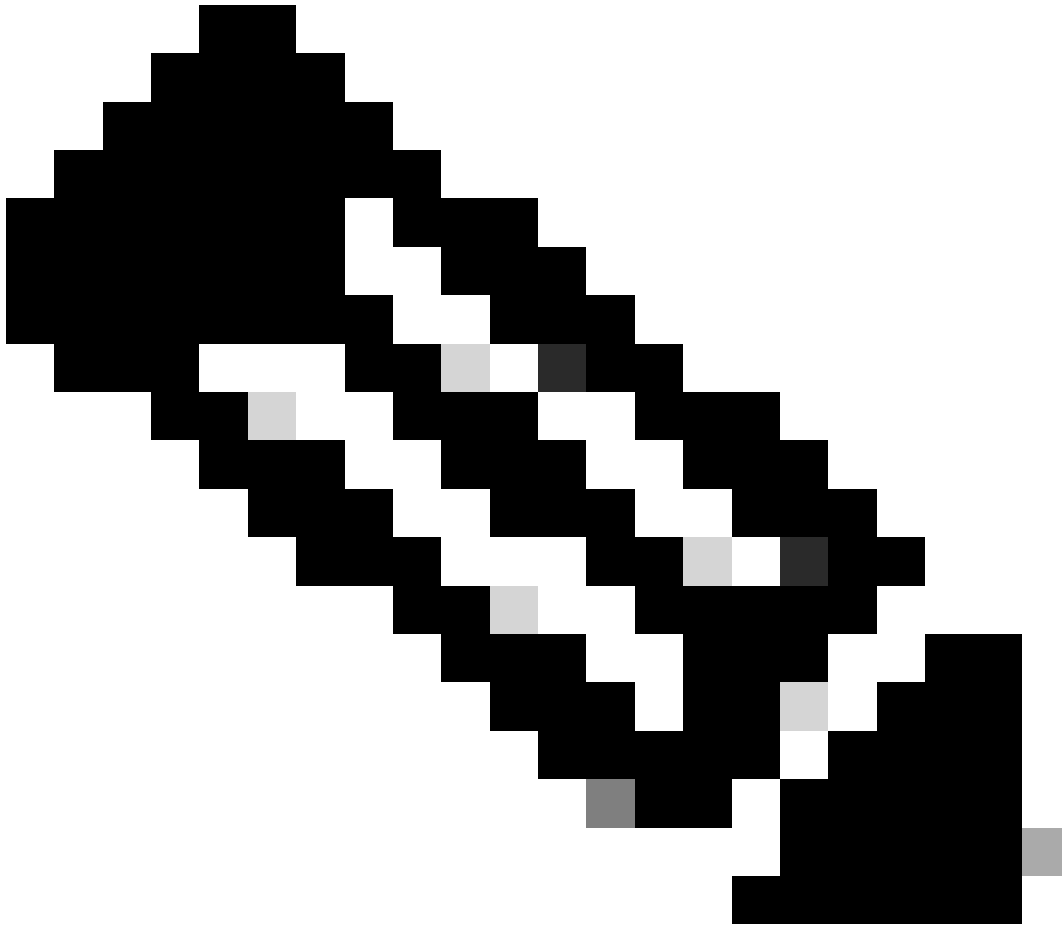
Door gebrek, vernieuwt het apparaat en genereert automatisch een nieuw zelf-ondertekend certificaat één maand voorafgaand aan het verstrijken van het zelf-ondertekende certificaat.

Configuraties

Het apparaat gebruikt een zelfondertekend certificaat. Wanneer het toegang tot van de APIC GUI, vraagt de browser dat het certificaat niet betrouwbaar is. Om dit probleem op te lossen, gebruikt dit document een vertrouwde CA-autoriteit om het certificaat te ondertekenen.



Stap 1. Voer het basiscertificaat van de CA-autoriteit of tussentijds certificaat in



Opmerking: als u het CA-basiscertificaat gebruikt voor direct ondertekenen, kunt u het CA-basiscertificaat gewoon importeren. Maar als u een tussentijds certificaat gebruikt voor het ondertekenen, moet u de volledige certificaatketen importeren, dat wil zeggen: het basiscertificaat en de minder betrouwbare tussenliggende certificaten.

Navigeer in de menubalk naar Admin > AAA > Security > Public Key Management > Certificate Authorities.

The screenshot shows the Cisco ICM interface. The top navigation bar includes 'System', 'Tenants', 'Fabric', 'Virtual Networking', 'Admin', 'Operations', 'Apps', and 'Integrations'. The 'Admin' tab is selected. Below it, a sub-menu shows 'AAA', 'Schedulers', 'Firmware', 'External Data Collectors', 'Config Rollbacks', and 'Import/Export'. The 'AAA' sub-menu is expanded, showing 'Quick Start', 'Authentication', 'Security', and 'Users'. The 'Security' folder is selected. The main content area is titled 'User Management - Security' and contains tabs for 'Management Settings', 'Security Domains', 'Roles', 'RBAC Rules', 'Public Key Management', 'Key Rings', 'Certificate Authorities', and 'JWT Keys'. The 'Certificate Authorities' tab is selected. Below the tabs is a table with columns for 'Name', 'Description', 'FP', and 'N'. The table contains two entries: 'ACI_Root' and 'Cisco_AD_CA'. A 'Create Certificate Authority' button is visible in the bottom right corner of the table area.

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

User Management - Security

Create Certificate Authority

Name: !

Description: optional

Certificate Chain:

Cancel Submit

Naam: **Vereist.**

Formuleer de inhoud volgens uw naamgevingsregels. Het kan speciale Engelse tekens bevatten_, maar het kan geen speciale Engelse tekens bevatten zoals:

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

Beschrijving: **Optioneel.**

Certificeringsketen: **verplicht.**

Vul het vertrouwde basiscertificaat van CA en tussenliggend certificaat van CA in.



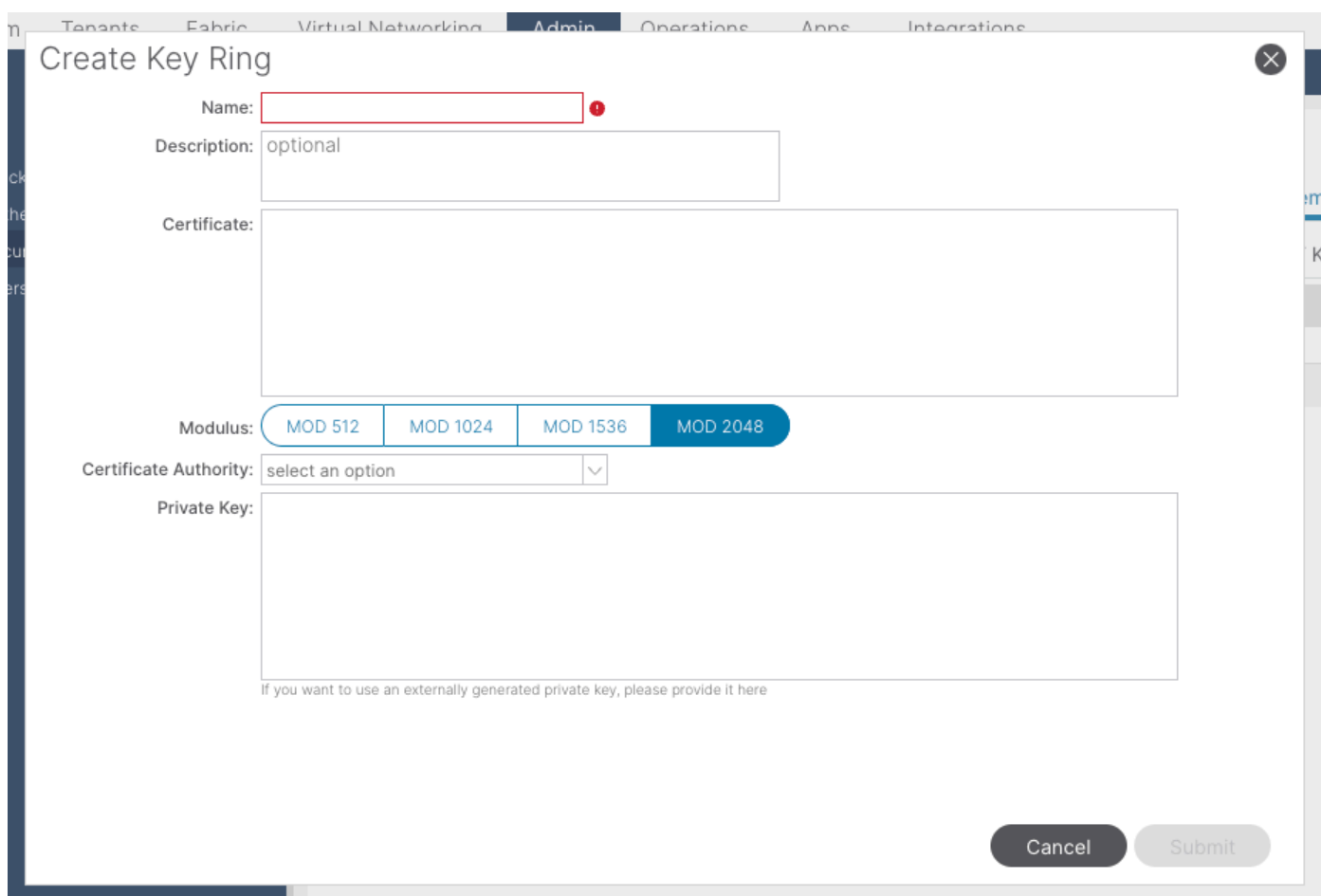
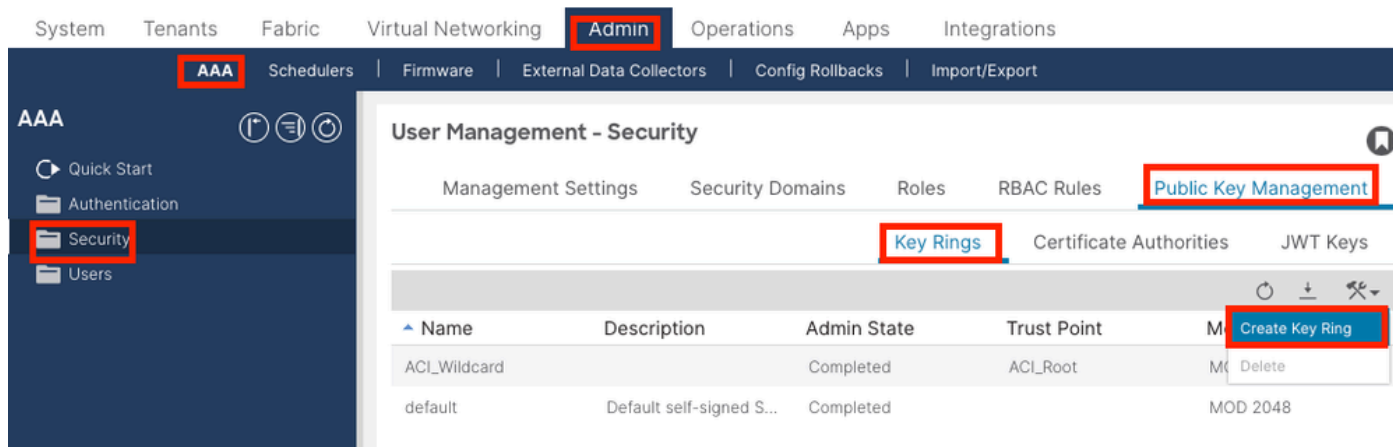
Noot: Elk certificaat moet een uniform model hebben.

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

Klik op de knop **Verzenden**.

Stap 2. Toetsenring maken

Navigeer in de menubalk naar Admin > AAA > Security > Public Key Management > Key Rings.



Naam: Vereist (geef een naam op).

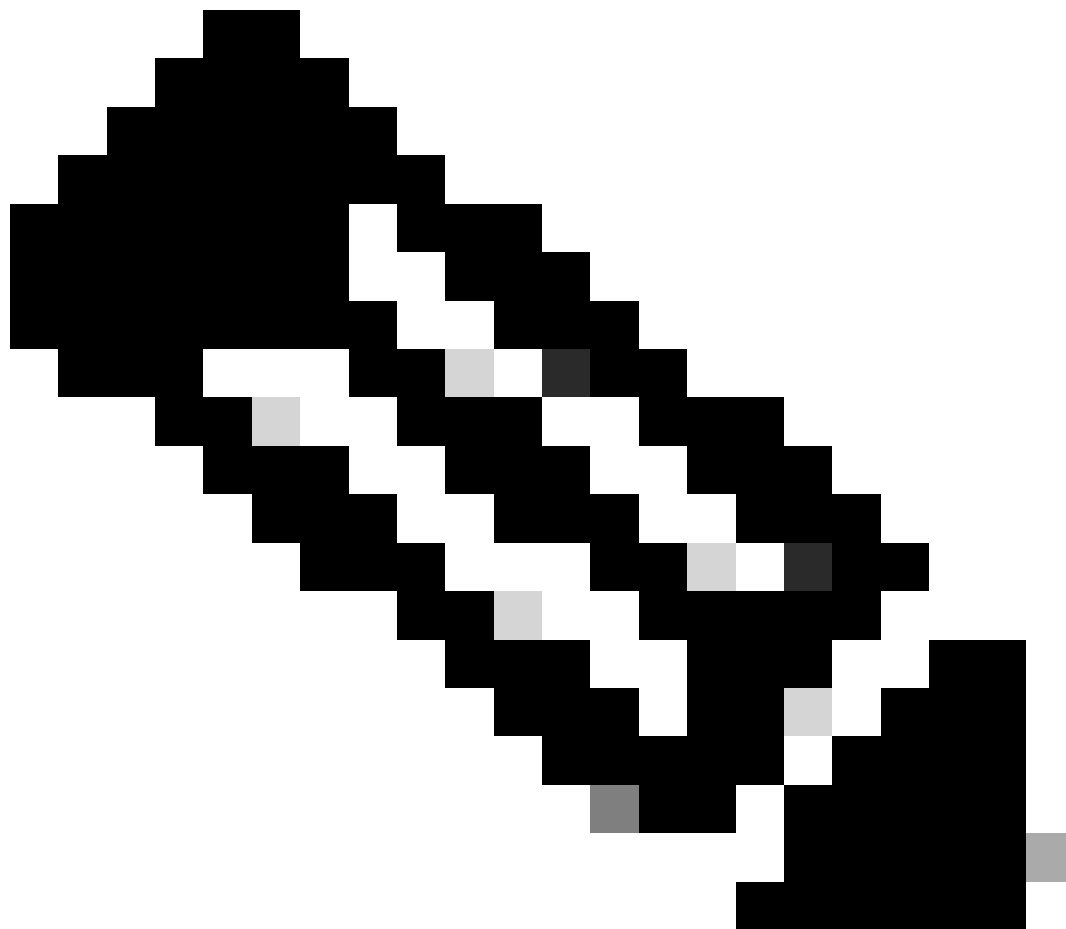
Certificaat: voeg geen inhoud toe als u een certificaatondertekeningsverzoek (CSR) genereert met Cisco APIC via de sleutelring. U kunt ook de ondertekende certificaatinhoud toevoegen als u er al een hebt die door de CA is ondertekend uit de vorige stappen door een persoonlijke sleutel en een CSR buiten Cisco APIC te genereren.

Modulus: Vereist (klik op het keuzerondje voor de gewenste toetssterkte).

Certificaatautoriteit: verplicht. Kies in de vervolgkeuzelijst de certificeringsinstantie die u eerder hebt gemaakt.

Private Key: voeg geen inhoud toe als u een CRS genereert met de Cisco APIC via de sleutelring. U kunt ook de persoonlijke sleutel toevoegen

die wordt gebruikt om de CSR te genereren voor het ondertekende certificaat dat u hebt ingevoerd.

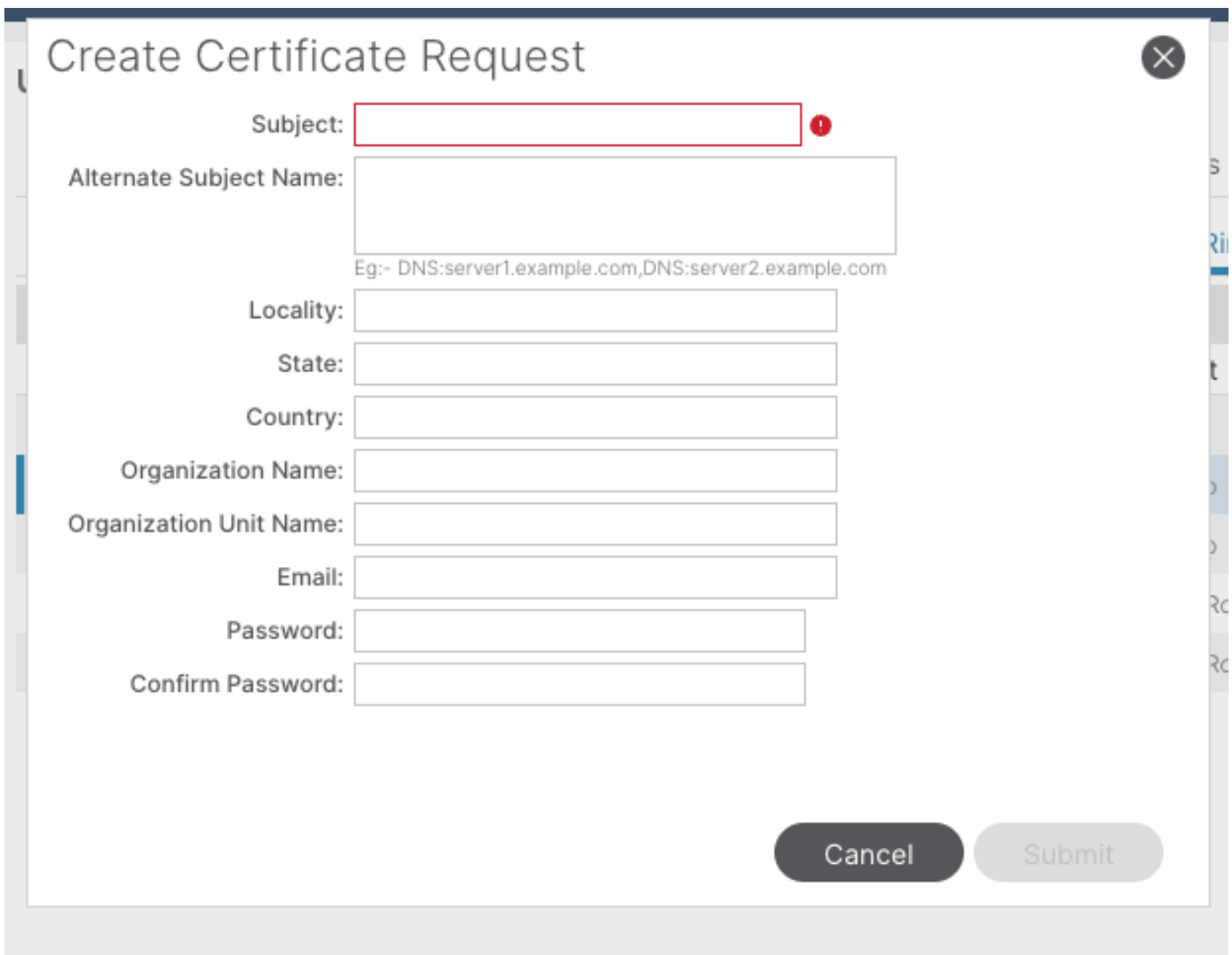
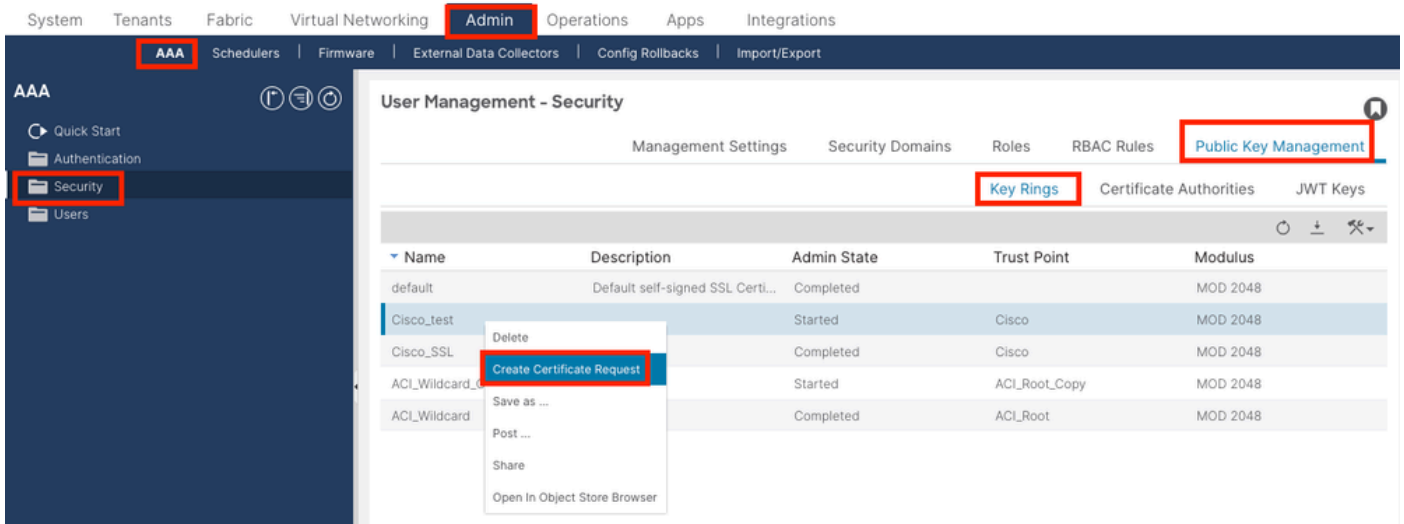


Opmerking: Als u de door het systeem gegenereerde privé-sleutel en MVO niet wilt gebruiken en een aangepaste privé-sleutel en certificaat wilt gebruiken, hoeft u alleen maar vier items in te vullen: Naam, Certificaat, Certificaatautoriteit en Privé-sleutel. Na het indienen hoeft u alleen de laatste stap, Stap 5, uit te voeren.

Klik op de knop **Verzenden**.

Stap 3. Private sleutel en MVO genereren

Navigeer in de menubalk naar Admin > AAA > Security > Public Key Management > Key Rings.

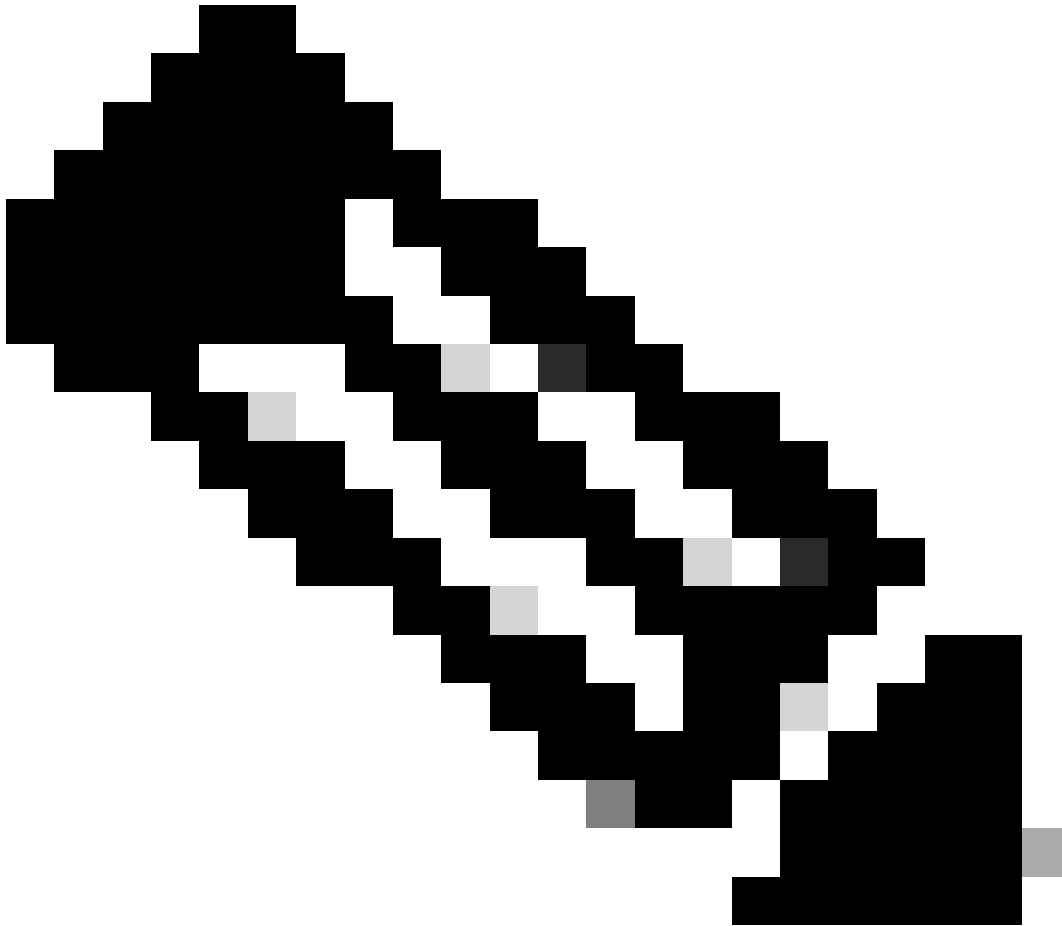


Onderwerp: **verplicht**. Vermeld de algemene naam (GN) van de MVO.

U kunt de volledig gekwalificeerde domeinnaam (FQDN) van Cisco APICs invoeren met behulp van een jokerteken, maar in een modern certificaat wordt het over het algemeen aanbevolen dat u een identificeerbare naam van het certificaat invoert en de FQDN van alle Cisco APICs invoert in het veld Alternatieve onderwerpnaam (ook bekend als de SAN - Alternatieve naam), omdat veel moderne browsers de FQDN verwachten in het SAN-veld.

Alternatieve onderwerpnaam: **verplicht**. Voer de FQDN in van alle Cisco APIC's, zoals
DNS:apic1.example.com,DNS:apic2.example.com,DNS:apic3.example.com of DNS:*example.com.

Als u wilt dat een SAN overeenstemt met een IP-adres, specificeert u de IP-adressen van Cisco APIC's in de volgende indeling: IP:192.168.1.1.



Opmerking: u kunt in dit veld domeinnaamsservernamen (DNS), IPv4-adressen of een combinatie van beide gebruiken. IPv6-adressen worden niet ondersteund.

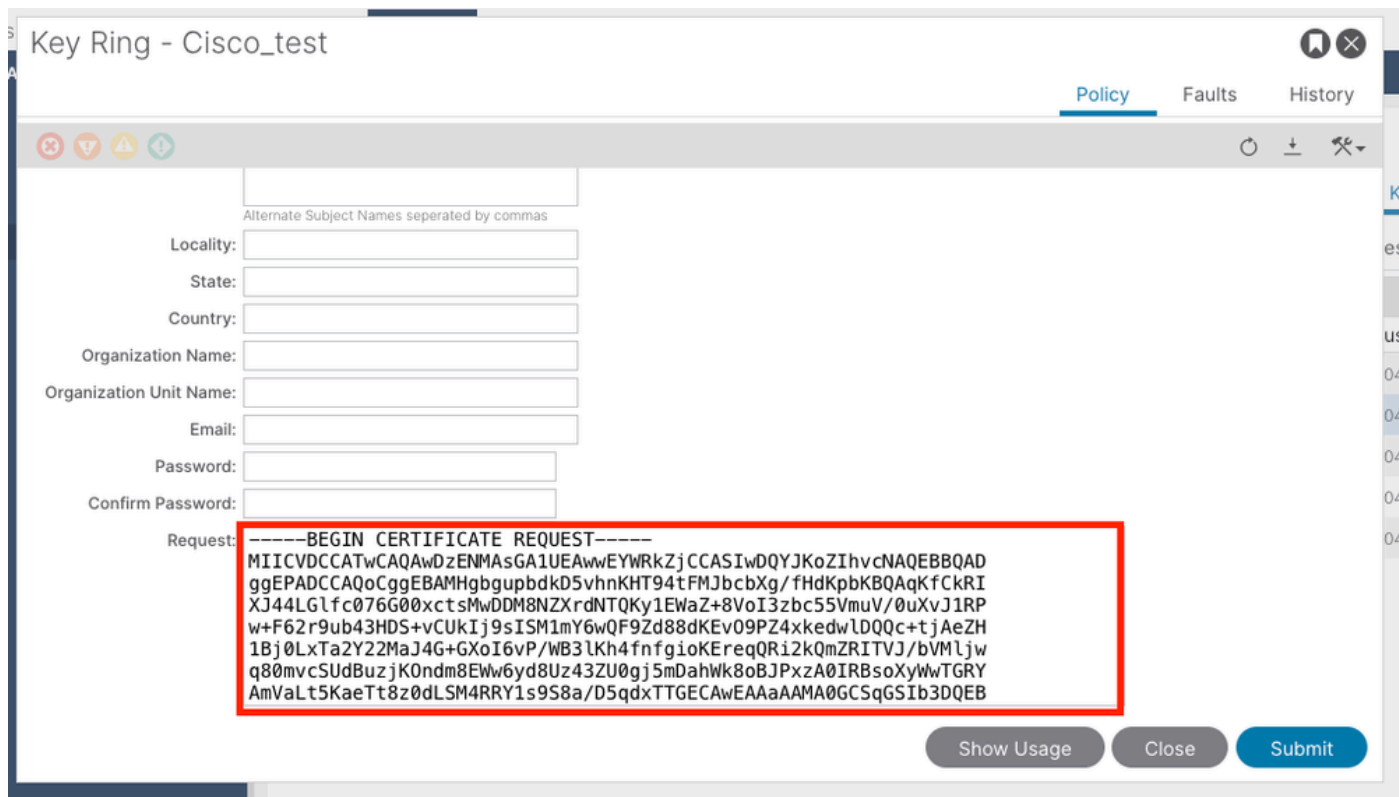
Vul de overige velden in volgens de vereisten van de CA-organisatie die u wenst te verkrijgen om het certificaat af te geven.

Klik op de knop **Verzenden**.

Stap 4. Haal de MVO en stuur het naar de CA-organisatie

Navigeer in de menubalk naar Admin > AAA > Security > Public Key Management > Key Rings.

Dubbelklik op uw **Key Ring**-naam maken en vind de optie **Aanvragen**. De inhoud van het verzoek is de MVO.



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-----
MIICVDCCAAwDzENMAAsGA1UEAwEYWRkZjCCASIwDQYJKoZIhvcNAQEBBQAD
ggEPADCCAQoCggEBAMHgbgubdkD5vhnKHT94tFMJbcXg/fHdKpbKBQAqfCKRI
XJ44LGLfc076G00xctsmwDDM8NZXrdNTQKy1EwaZ+8VoI3zbc55VmuV/0uXvJ1RP
w+F62r9ub43HDS+vCUkIj9sISM1mY6wQF9Zd88dKEv09PZ4xkedwLDQqc+tjAeZH
1Bj0LxTa2Y22MaJ4G+GXoI6vP/WB3lKh4fnfgioKEreqQR12kQmZRITVJ/bVMljw
q80mvcSUDBuzjK0ndm8EWw6yd8Uz43ZU0gj5mDahWk8oBJPxzA0IRBsoXyWwTGRY
AmValt5KaeTt8z0dLSM4RRY1s9S8a/D5qdxTTGECAwEAAsAAAMA0GCSqSgsIb3DQEB

Show Usage | Close | Submit

Kopieer alle inhoud van het verzoek en stuur het naar uw CA.

De CA gebruikt zijn persoonlijke sleutel om handtekeningverificatie uit te voeren op uw CSR.

Na het verkrijgen van het ondertekende certificaat van de CA, kopieert zij het certificaat naar het certificaat.



Name: Cisco_Test

Admin State: Started

Description: optional

Certificate:

```
-----BEGIN CERTIFICATE-----  
MIIDszCCApugAwIBAgIBAgjANBgqhkiG9w0BAQsFADBYMQswCQYDVQGEwJVUzEL  
MAKGA1UECAwCQ0EFTATBgNVBACMDERlZmF1bHQgQ2l0eTEEXMBUGA1UECgw0Q2Lz  
Y28gQUNJIFRlYW0xDDAKBgNVBAsMA1RBQzAeFw0yNDYyMjE5MDU5MDhaFw0yNTAy  
MjE5MDU5MDhaMGUxCzAJBgNVBAYTAlVMTQswCQYDVQQLIDQTEEXMBUGA1UECgw0  
Q2LzY28gQUNJIFRlYW0xDDAKBgNVBAsMA1RBQzEiMCAGA1UEAwwZZGxjLWFlaTA2  
LWFWaWxLmNpc2NvLmNvbTCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEB  
ALJA5N1wzE7WmBk35pTd06FwH3M2ZmIeCDw6SktDTqaMHhqDkYEK0UgG0dyRrdP
```

Modulus: MOD 512 MOD 1024 MOD 1536 MOD 2048

Certificate Authority: Cisco_ACL_Team

Private Key:

Show Usage Close Submit



Noot: Elk certificaat moet een uniform model hebben.

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

Klik op de knop **Verzenden**.

Stap 5. Werk het ondertekeningscertificaat bij op het web

Navigeer in de menubalk naar 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:

SSH Cipher Configuration:

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

Show Usage Reset Submit

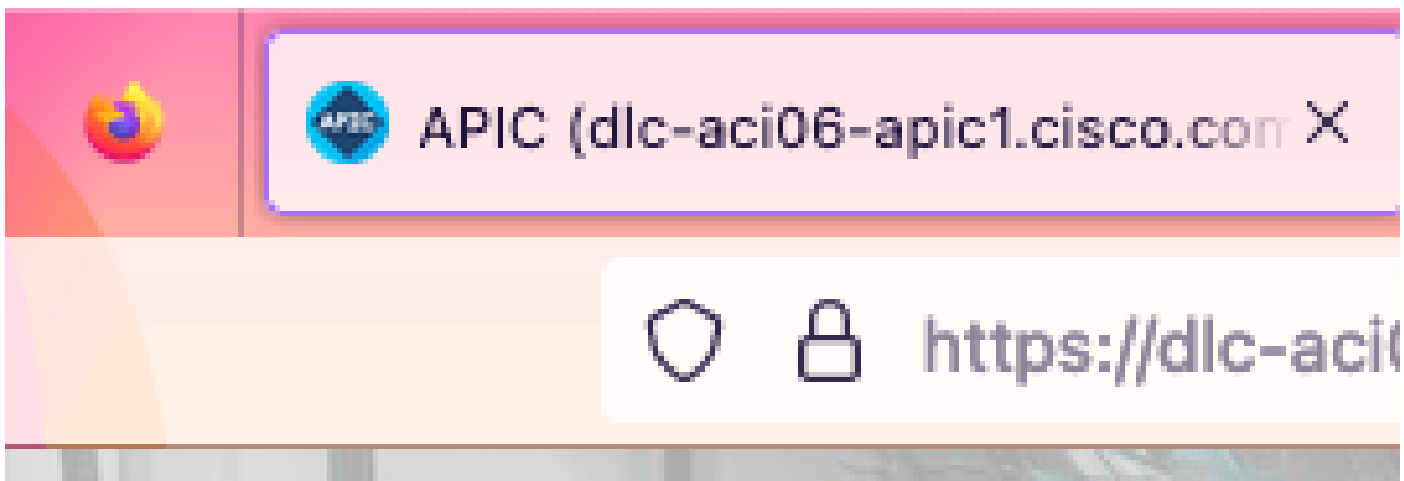
Kies in de vervolgkeuzelijst **Admin KeyRing** de gewenste KeyRing.

Klik op de knop **Verzenden**.

Nadat u op Verzenden hebt geklikt, treedt er een fout op vanwege certificeringsredenen. Verfris met het nieuwe certificaat.

Verifiëren

Na toegang tot de APIC GUI, gebruikt APIC het CA-ondertekende certificaat om te communiceren. Bekijk de certificaatinformatie in de browser om het te verifiëren.





Opmerking: de methoden voor het bekijken van HTTPS-certificaten in verschillende browsers zijn niet precies hetzelfde. Raadpleeg voor specifieke methoden de gebruikershandleiding van uw browser.

Problemen oplossen

Als de browser nog steeds vraagt dat de APIC GUI niet vertrouwd is, controleert u in de browser of het certificaat van de GUI consistent is met het certificaat dat in de Keyring is ingediend.

U moet vertrouwen op het **CA-basiscertificaat** dat het certificaat op uw computer of browser heeft afgegeven.



Opmerking: De Google Chrome-browser moet het **SAN** van het certificaat verifiëren om dit certificaat te vertrouwen.

In APIC's die zelfondertekende certificaten gebruiken, kunnen in zeldzame gevallen verloopwaarschuwingen voor certificaten worden weergegeven.

Vind het certificaat in Keyring, gebruik het certificaat parsing tool om het certificaat te parseren, en vergelijk het met het certificaat gebruikt in de browser.

Als het certificaat in de sleutelring wordt vernieuwd, creëer een nieuw Beleid van de Toegang van het Beheer en pas het toe.

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
- 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

Als het certificaat in Keyring niet automatisch wordt verlengd, neem dan contact op met Cisco TAC voor meer assistentie.

Gerelateerde informatie

- [Cisco APIC-configuratiehandleiding voor beveiliging, release 5.2\(x\)](#)
- [Cisco Technical Support en downloads](#)

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document ([link](#)) te raadplegen.