

Configure ACI APIC GUI HTTPS Certificate

Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Components Used](#)

[Configure](#)

[Configurations](#)

[Step 1.Import the CA Authority Root Certificate or Intermediate Certificate](#)

[Step 2. Create Key Ring](#)

[Step 3.Generate Private Key andCSR](#)

[Step 4. Get the CSR and Send it to the CA Organization](#)

[Step 5.Update the Signing Certificate on the Web](#)

[Verify](#)

[Troubleshoot](#)

[Related Information](#)

Introduction

This document describes the configuration of Custom SSL and Self-signed SSL Certificates.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- Digital signatures and digital certificates
- Certificate issuance process by Certificate Authority (CA) organization

Components Used

The information in this document is based on these software and hardware versions:

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

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Configure

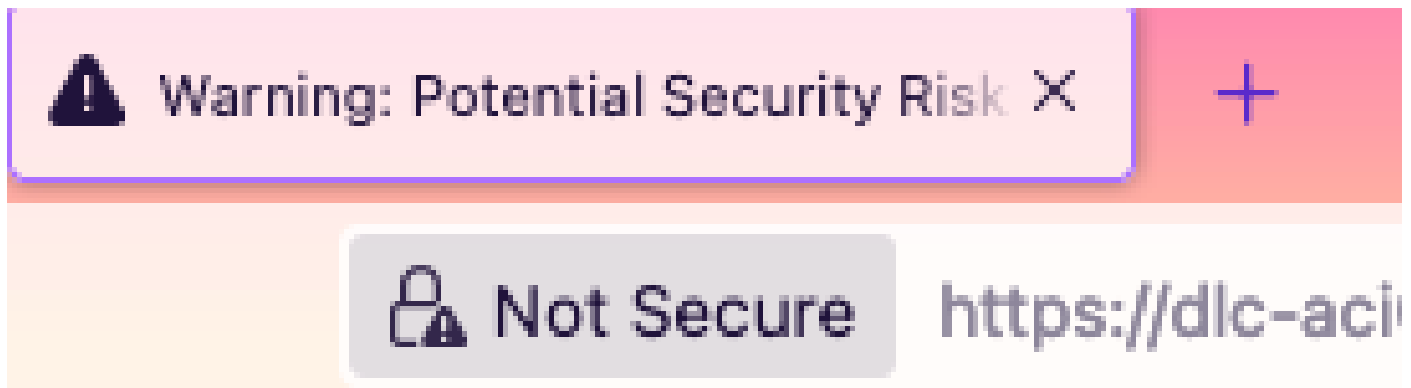
After the device is initialized, it uses the self-signed certificate as the SSL certificate for HTTPS. The self-

signed certificate is valid for 1000 days.

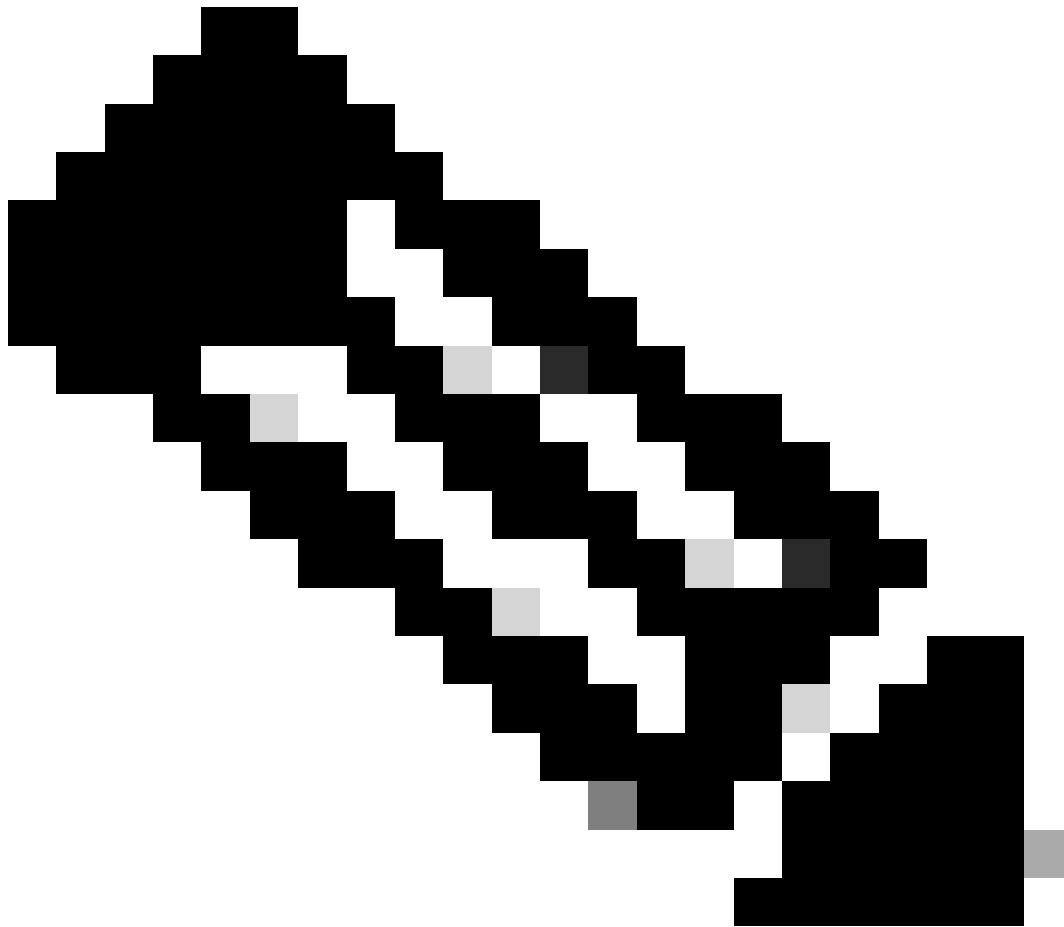
By default, the device automatically renews and generates a new self-signed certificate one month prior to the expiration of the self-signed certificate.

Configurations

The device uses a self-signed certificate. When accessing the APIC GUI, the browser prompts that the certificate is not trustworthy. In order to solve this problem, this document uses a trusted CA authority in order to sign the certificate.



Step 1. Import the CA Authority Root Certificate or Intermediate Certificate



Note: If you are using the CA root certificate for signing directly, you can just import the CA root certificate. But if you are using an intermediate certificate for signing, you must import the complete certificate chain, that is: the root certificate and the less trusted intermediate certificates.

On the menu bar, navigate to Admin > AAA > Security > Public Key Management > Certificate Authorities.

The screenshot shows the Cisco ACI User Management - Security interface. The navigation path is highlighted: Admin > AAA > Security > Public Key Management > Certificate Authorities. The 'Create Certificate Authority' button is also highlighted.

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

Create Certificate Authority

Name: !

Description: optional

Certificate Chain:

Cancel Submit

Name: **Required.**

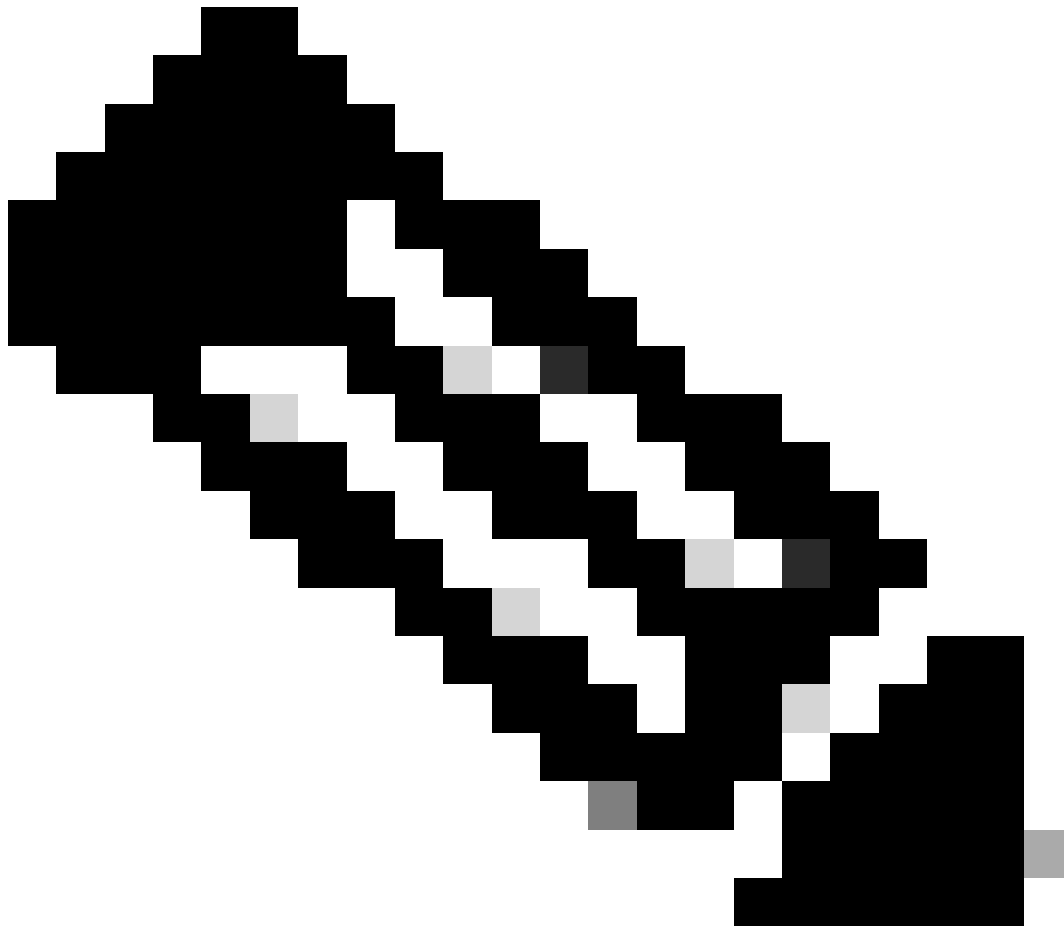
Formulate the content according to your naming rules. It can contain `_`, but it cannot contain special English characters, such as:

`, . ; ' " : | + * / = ` ~ ! @ # $ % ^ & ()` and space characters.

Description: **Optional.**

Certification Chain: **Required.**

Fill in the trusted CA root certificate and CA intermediate certificate.



Note: Each certificate must conform to a fixed format.

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

Click the **Submit** button.

Step 2. Create Key Ring

On the menu bar, navigate to 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' (highlighted), 'Operations', 'Apps', and 'Integrations'. The left sidebar shows 'AAA' with sub-items 'Quick Start', 'Authentication', 'Security' (highlighted), and 'Users'. The main content area is titled 'User Management - Security' and includes tabs for 'Management Settings', 'Security Domains', 'Roles', 'RBAC Rules', and 'Public Key Management' (highlighted). Under 'Public Key Management', there are sub-tabs for 'Key Rings' (highlighted), 'Certificate Authorities', and 'JWT Keys'. A table lists existing key rings with columns for Name, Description, Admin State, Trust Point, and Modulus. A 'Create Key Ring' button is highlighted in the top right of the table.

Name	Description	Admin State	Trust Point	Modulus
ACL_Wildcard		Completed	ACL_Root	MOD 2048
default	Default self-signed S...	Completed		MOD 2048

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

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

At the bottom of the dialog, there is a note: 'If you want to use an externally generated private key, please provide it here'. The dialog has 'Cancel' and 'Submit' buttons at the bottom right.

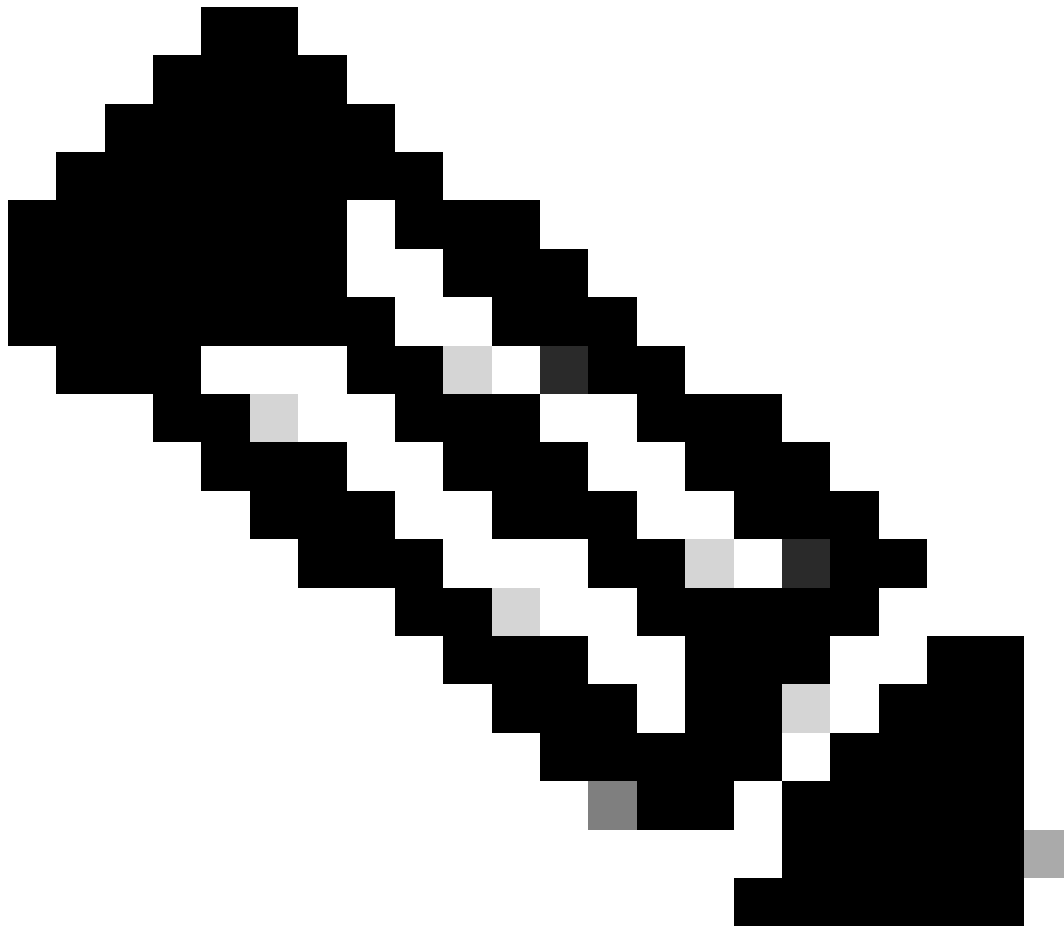
Name: **Required** (enter a name).

Certificate: **do not add** any content if you generate a Certificate Signing Request (CSR) using the Cisco APIC through the key ring. Alternatively, add the signed certificate content if you already have one that was signed by the CA from the previous steps by generating a private key and CSR outside of the Cisco APIC.

Modulus: **Required** (click the radio button for the desired key strength).

Certificate Authority: **Required**. From the drop-down list, choose the certificate authority that you created earlier.

Private Key: **do not add** any content if you generate a CSR using the Cisco APIC through the key ring. Alternatively, add the private key used to generate the CSR for the signed certificate that you entered.



Note: If you do not want to use the system-generated private key and CSR and use a custom private key and certificate, you only need to fill in four items: Name, Certificate, Certificate Authority, and Private Key. After submitting you only need to perform the last step, Step 5.

Click the **Submit** button.

Step 3. Generate Private Key and CSR

On the menu bar, navigate to Admin > AAA > Security > Public Key Management > Key Rings.

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

AAA Schedulers Firmware External Data Collectors Config Rollbacks Import/Export

AAA

- Quick Start
- Authentication
- Security**
- Users

User Management - Security

Management Settings Security Domains Roles RBAC Rules **Public Key Management**

Key Rings Certificate Authorities JWT Keys

Name	Description	Admin State	Trust Point	Modulus
default	Default self-signed SSL Certi...	Completed		MOD 2048
Cisco_test		Started	Cisco	MOD 2048
Cisco_SSL		Completed	Cisco	MOD 2048
ACI_Wildcard_0		Started	ACI_Root_Copy	MOD 2048
ACI_Wildcard		Completed	ACI_Root	MOD 2048

Context menu for Cisco_test:

- Delete
- Create Certificate Request**
- Save as ...
- Post ...
- Share
- Open In Object Store Browser

Create Certificate Request

Subject:

Alternate Subject Name:

Eg:- DNS:server1.example.com,DNS:server2.example.com

Locality:

State:

Country:

Organization Name:

Organization Unit Name:

Email:

Password:

Confirm Password:

Cancel Submit

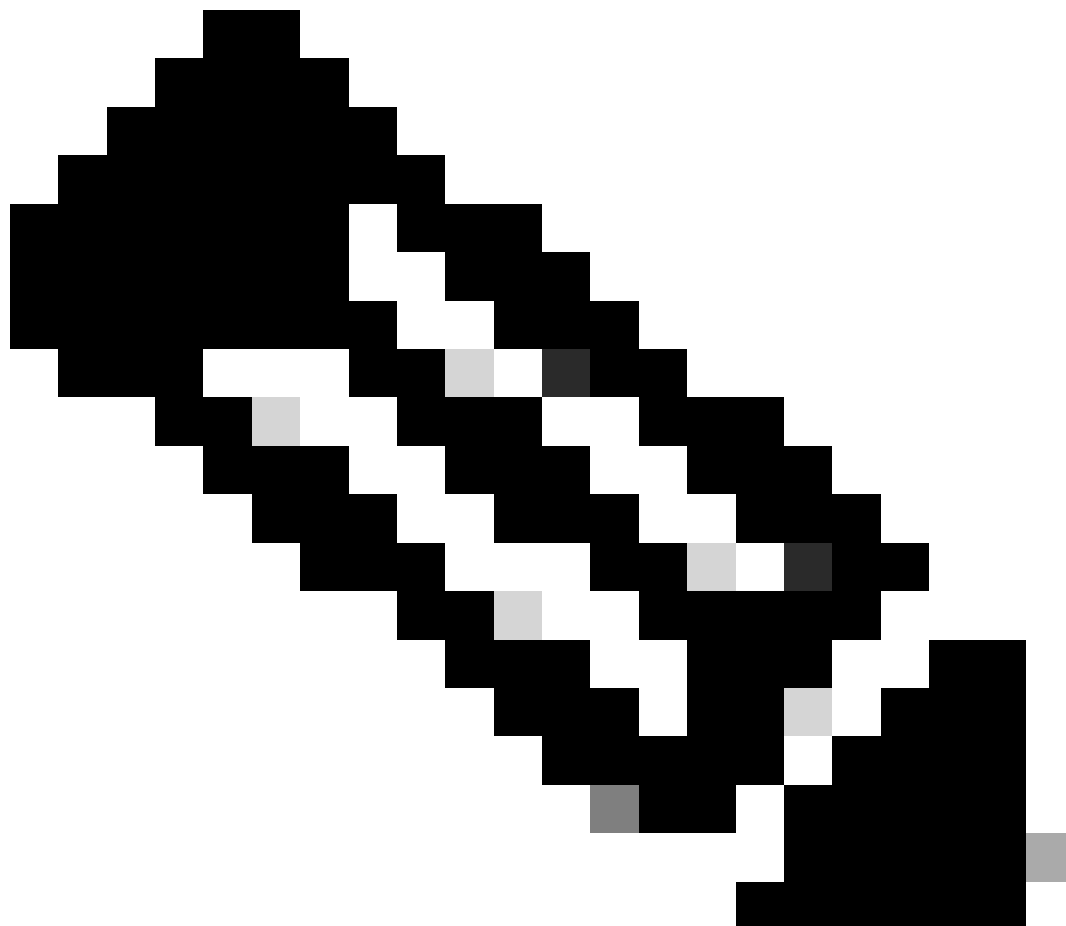
Subject: **Required.** Enter the common name (CN) of the CSR.

You can enter the fully qualified domain name (FQDN) of the Cisco APICs using a wildcard, but in a modern certificate, it is generally recommended that you enter an identifiable name of the certificate and enter the FQDN of all Cisco APICs in the Alternate Subject Name field (also known as the SAN – Subject Alternative Name) because many modern browsers expect the FQDN in the SAN field.

Alternate Subject Name: **Required.** Enter the FQDN of all Cisco APICs, such as

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

Alternatively, if you want SAN to match an IP address, enter the IP addresses of Cisco APICs with the format: IP:192.168.1.1.



Note: You can use Domain Name Server (DNS) names, IPv4 addresses, or a mixture of both in this field. IPv6 addresses are not supported.

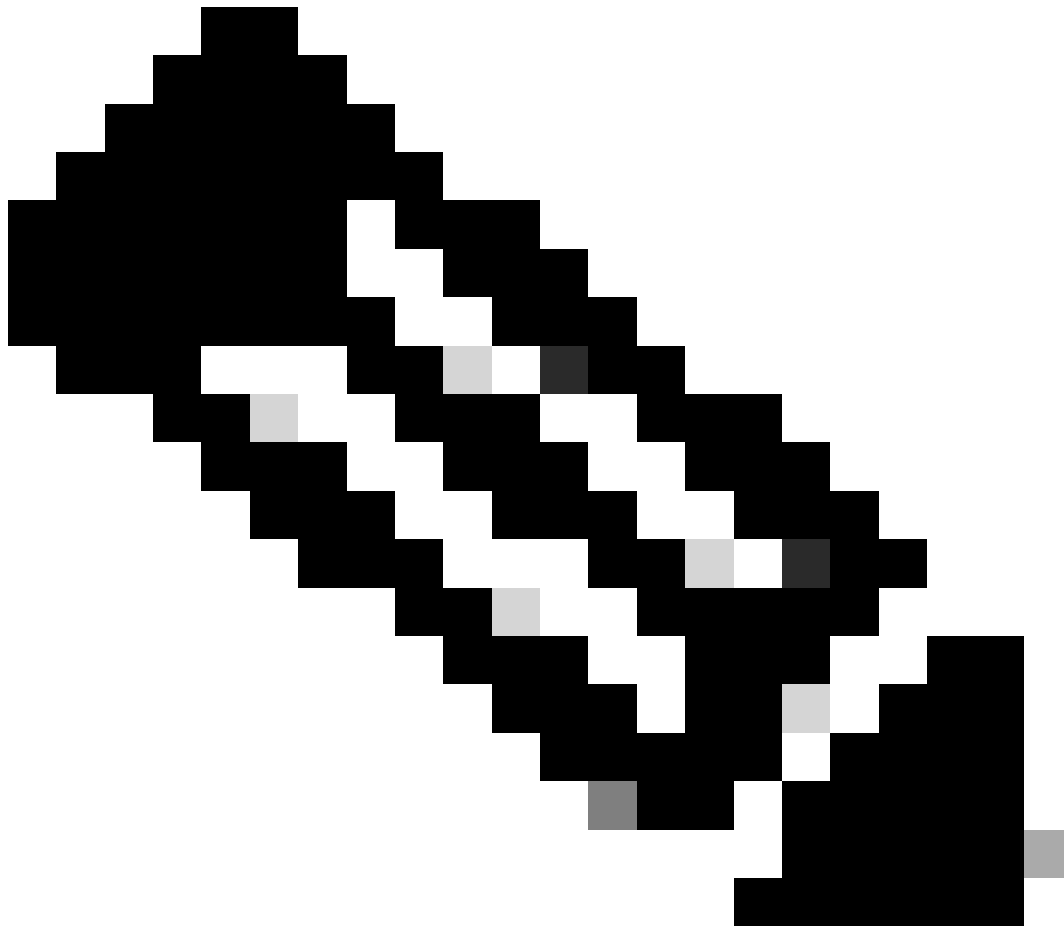
Fill in the remaining fields according to the requirements of the CA organization you are applying in order to issue the certificate.

Click the **Submit** button.

Step 4. Get the CSR and Send it to the CA Organization

On the menu bar, navigate to Admin > AAA > Security > Public Key Management > Key Rings.

Double-click your create **Key Ring** name and find the **Request** option. The content in the Request is the CSR.



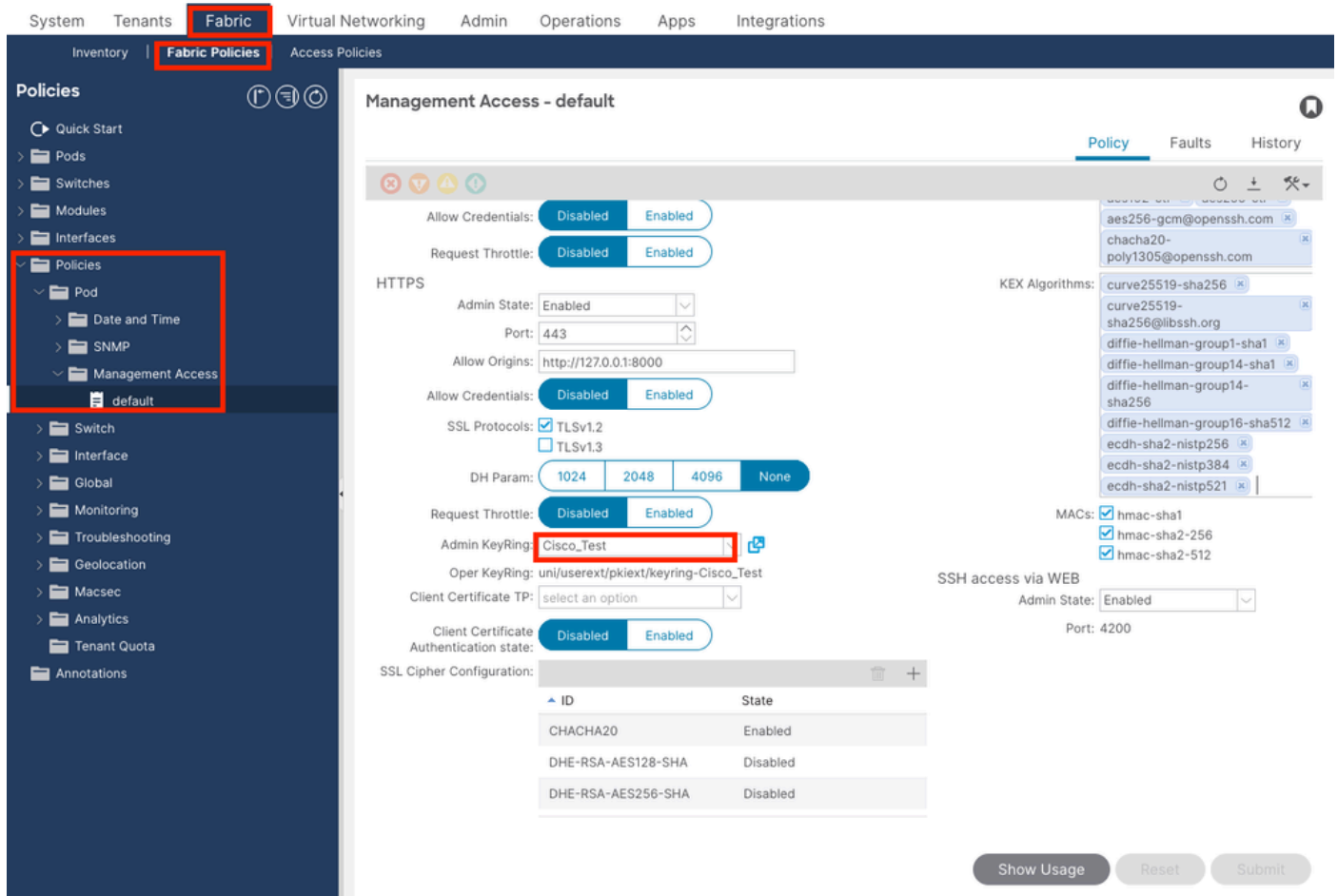
Note: Each certificate must conform to a fixed format.

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

Click the **Submit** button.

Step 5. Update the Signing Certificate on the Web

On the menu bar, navigate to Fabric > Fabric Policies > Policies > Pod > Management Access > Default.



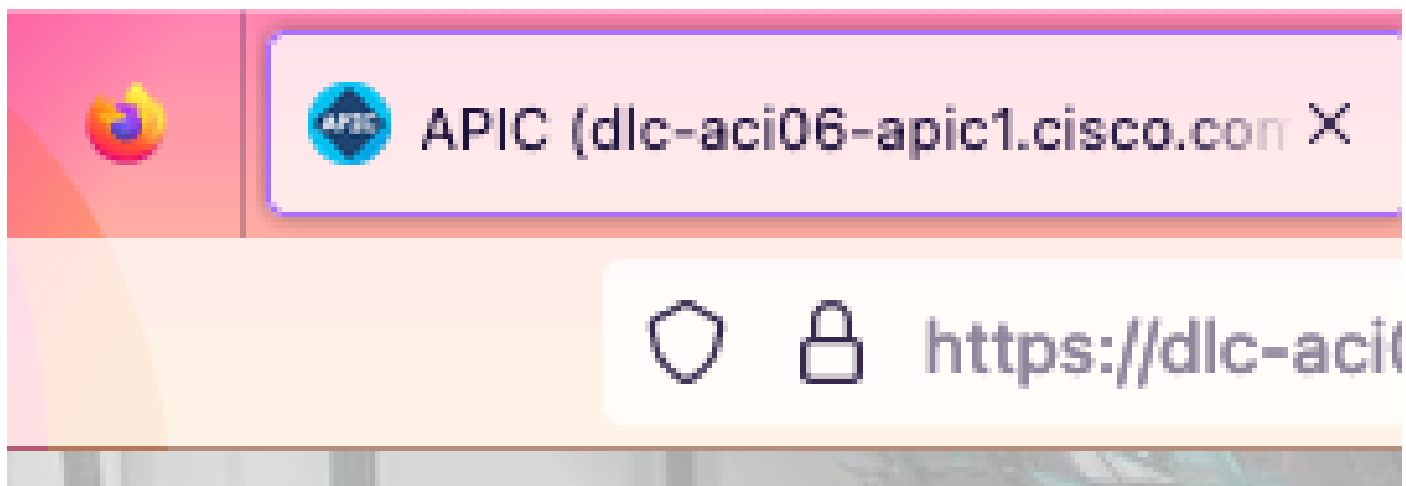
in the **Admin KeyRing** drop-down list, choose the desired KeyRing.

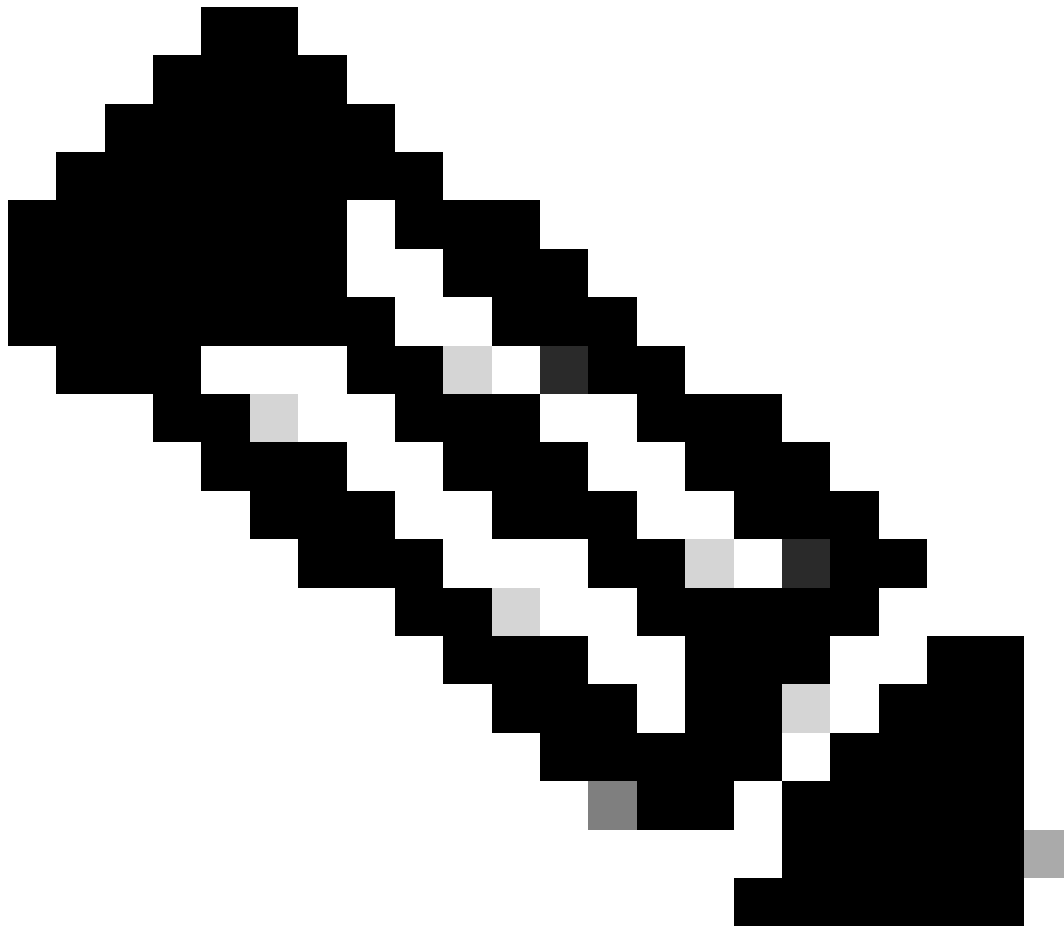
Click the **Submit** button.

After clicking submit, an error occurs due to certificate reasons. Refresh with the new certificate.

Verify

After accessing the APIC GUI, APIC uses the CA-signed certificate to communicate. View the certificate information in the browser in order to verify it.



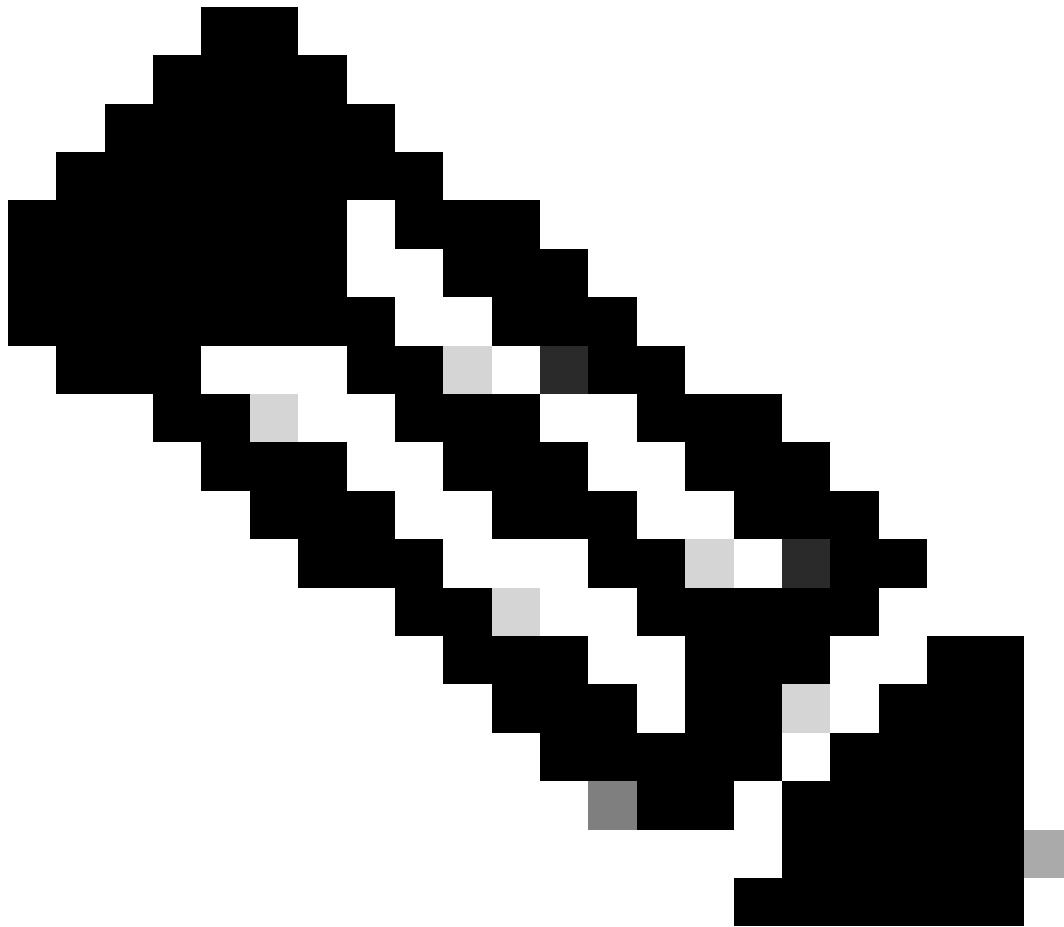


Note: The methods of viewing HTTPS certificates in different browsers are not exactly the same. For specific methods, refer to the user guide of your browser.

Troubleshoot

If the browser still prompts that the APIC GUI is untrusted, verify in the browser whether the certificate of the GUI is consistent with the one submitted in the Keyring.

You need to trust the **CA root certificate** that issued the certificate on your computer or browser.



Note: The Google Chrome browser must verify the **SAN** of the certificate in order to trust this certificate.

In APICs that use self-signed certificates, certificate expiration warnings can appear in rare cases.

Find the certificate in Keyring, use the certificate parsing tool in order to parse the certificate, and compare it with the certificate used in the browser.

If the certificate in the keyring is renewed, create a new Management Access Policy and apply it.

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 Port
	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

If the certificate in Keyring is not automatically renewed, contact Cisco TAC for more assistance.

Related Information

- [Cisco APIC Security Configuration Guide, Release 5.2\(x\)](#)
- [Cisco Technical Support & Downloads](#)