配置ACI APIC GUI HTTPS證書

目錄

簡介

本檔案介紹自訂SSL和自簽SSL憑證的組態。

必要條件

需求

思科建議您瞭解以下主題：

- 數位簽章和數位證書
- 證書頒發機構(CA)組織的證書頒發過程

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- 應用策略基礎設施控制器(APIC)
- 瀏覽器
- 運行5.2 (8e)的ACI

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

設定

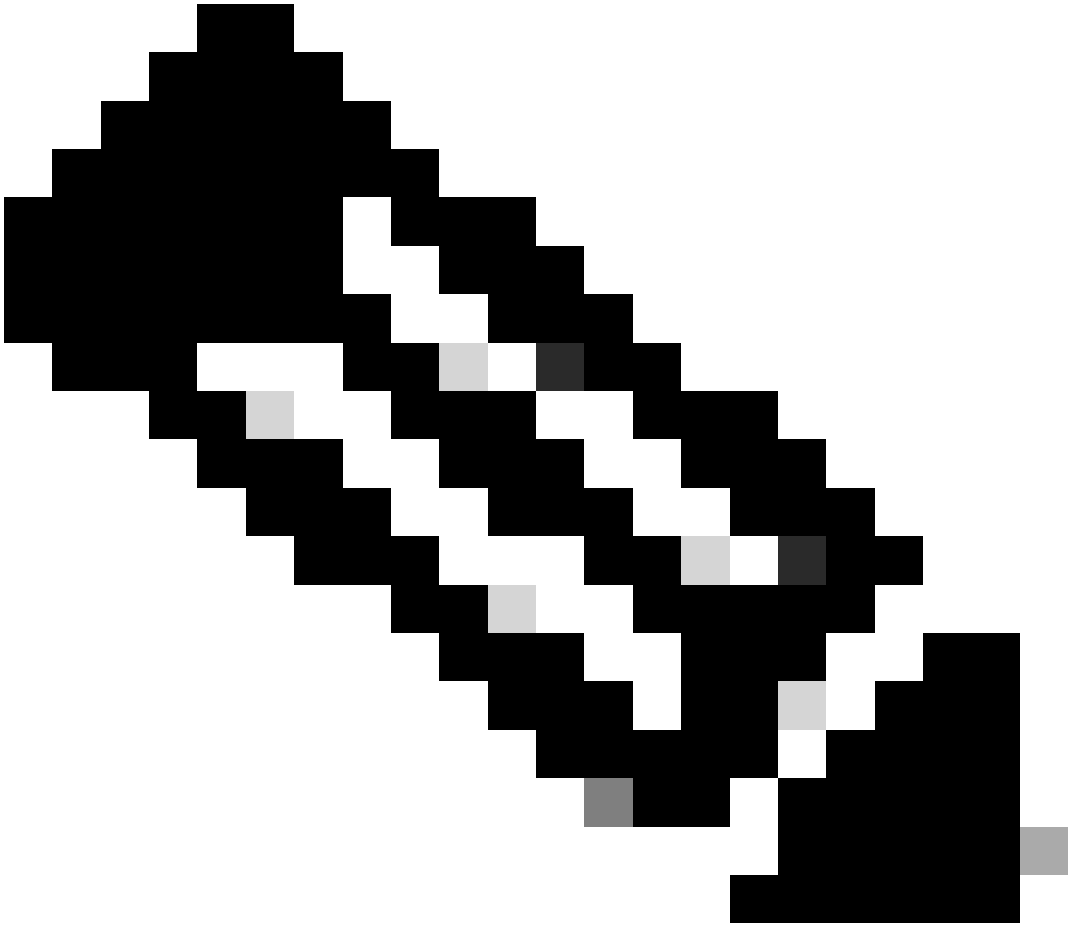
裝置初始化後，它將自簽名證書用作HTTPS的SSL證書。自簽名證書的有效期為1000天。

預設情況下，裝置會在自簽名證書到期前一個月自動更新並生成新的自簽名證書。

組態

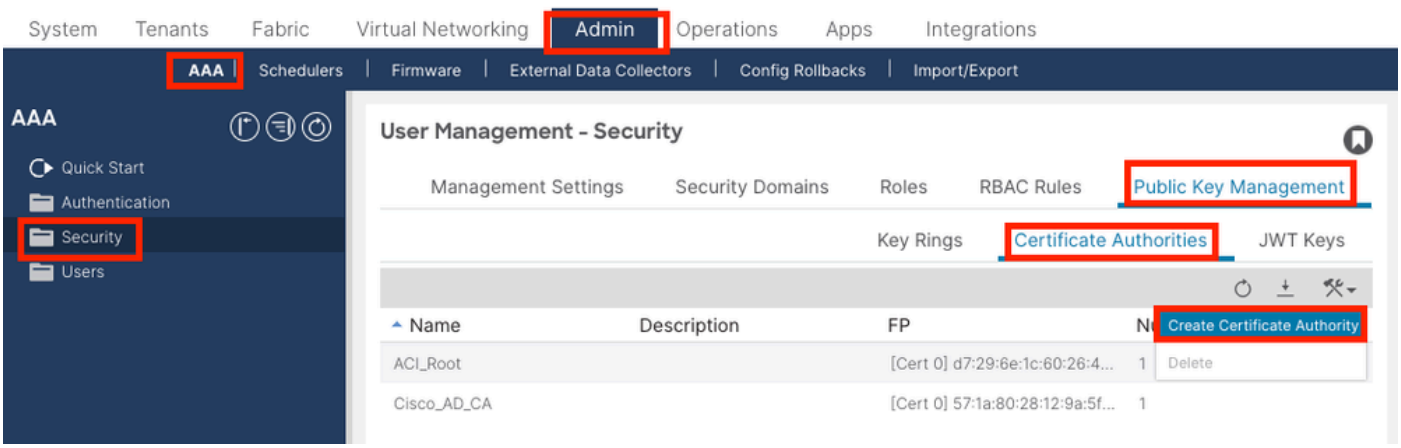
裝置使用自簽名證書。訪問APIC GUI時，瀏覽器會提示證書不可信。為了解決此問題，本文檔使用受信任的CA授權對證書進行簽名。

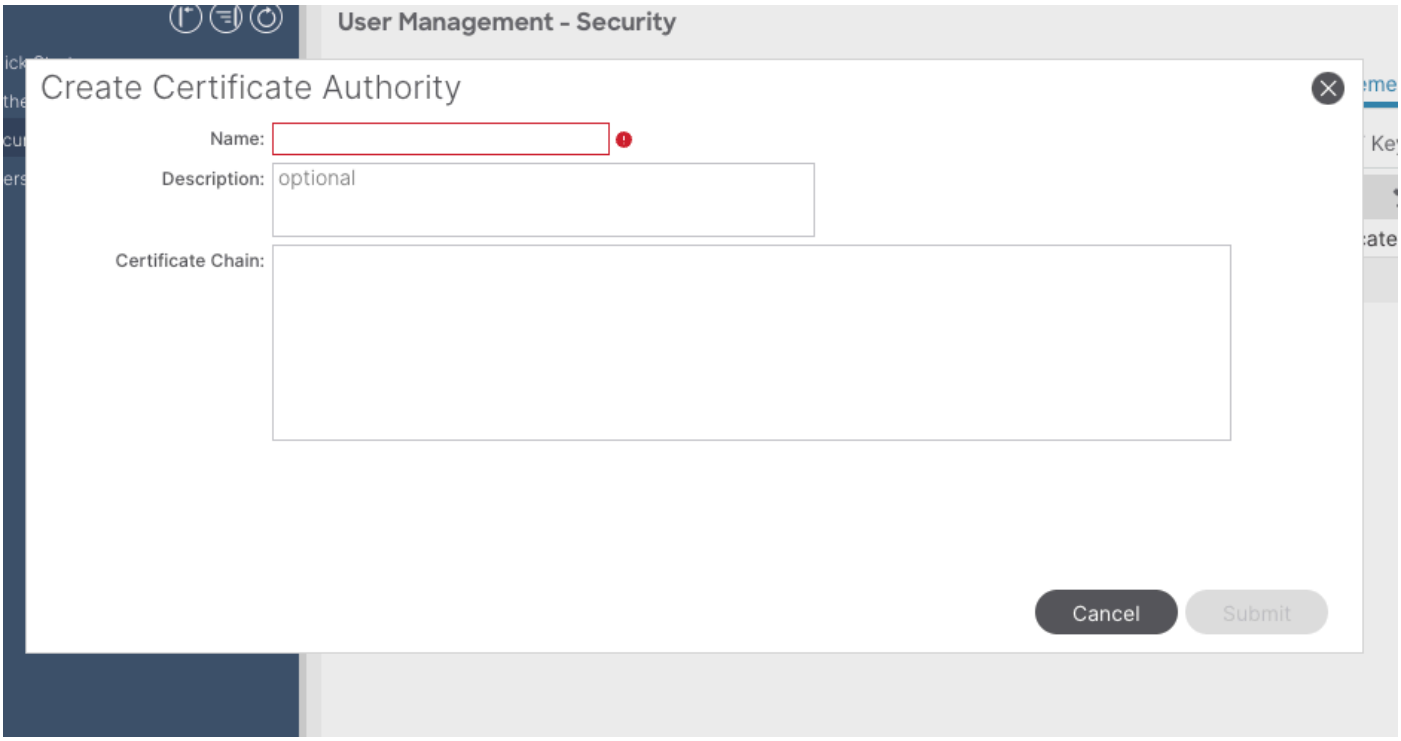
步驟 1. 導入CA機構根證書或中間證書



注意：如果直接使用CA根證書進行簽名，則只需導入CA根證書即可。但是，如果使用中間證書進行簽名，則必須導入完整的證書鏈，即：根證書和不太受信任的中間證書。

在選單欄上，導航到Admin > AAA > Security > Public Key Management > Certificate Authorities。





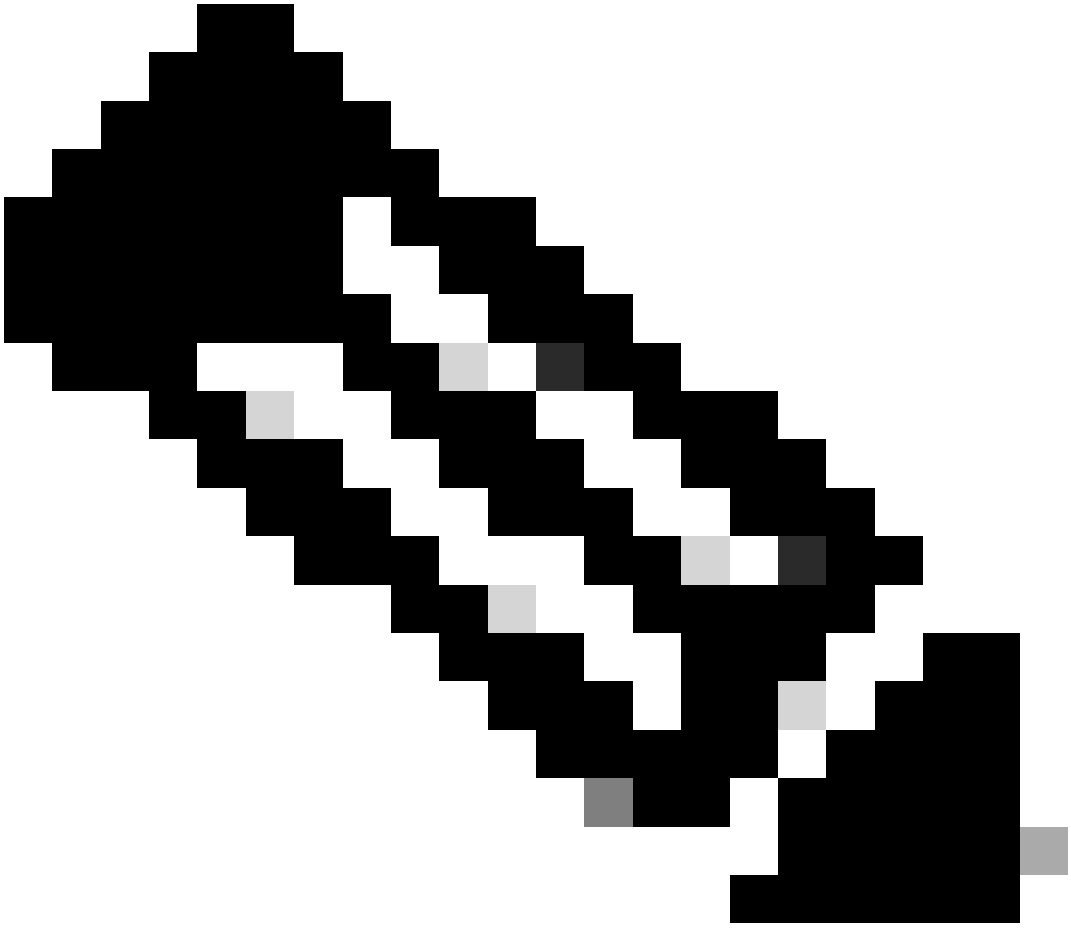
名稱：**必要**。

根據命名規則制定內容。它可以包含_，但不能包含特殊英文字元，例如：
, . ; ' " : | + * / = ` ~ ! @ # $ % ^ & ( ) 和空格字元。

說明：**可選**。

憑證鏈結：**必要**。

填寫受信任的CA根證書和CA中間證書。



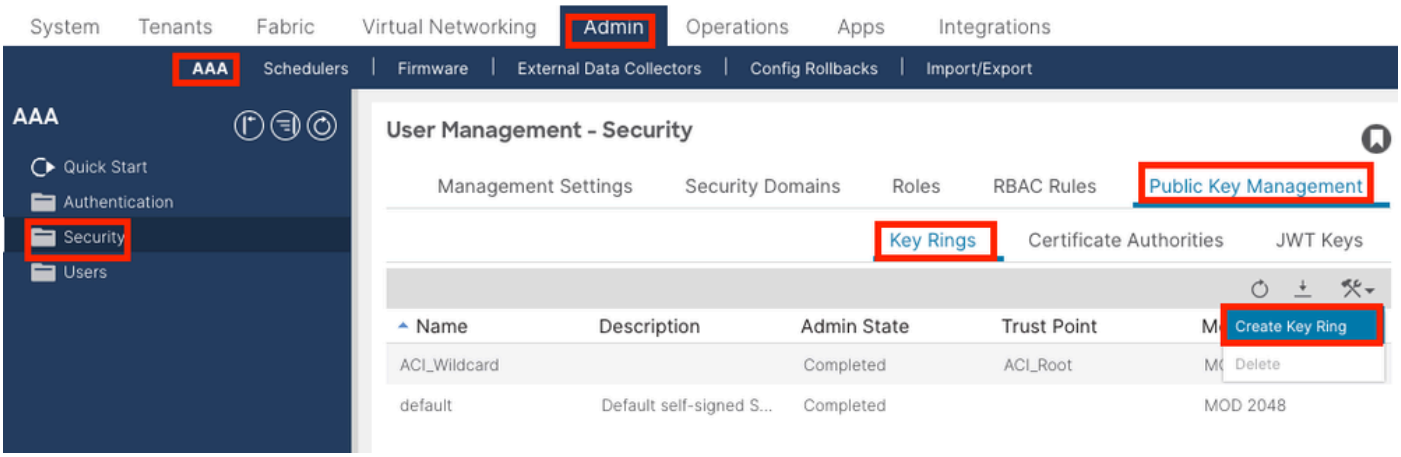
注意：每個證書都必須符合固定格式。

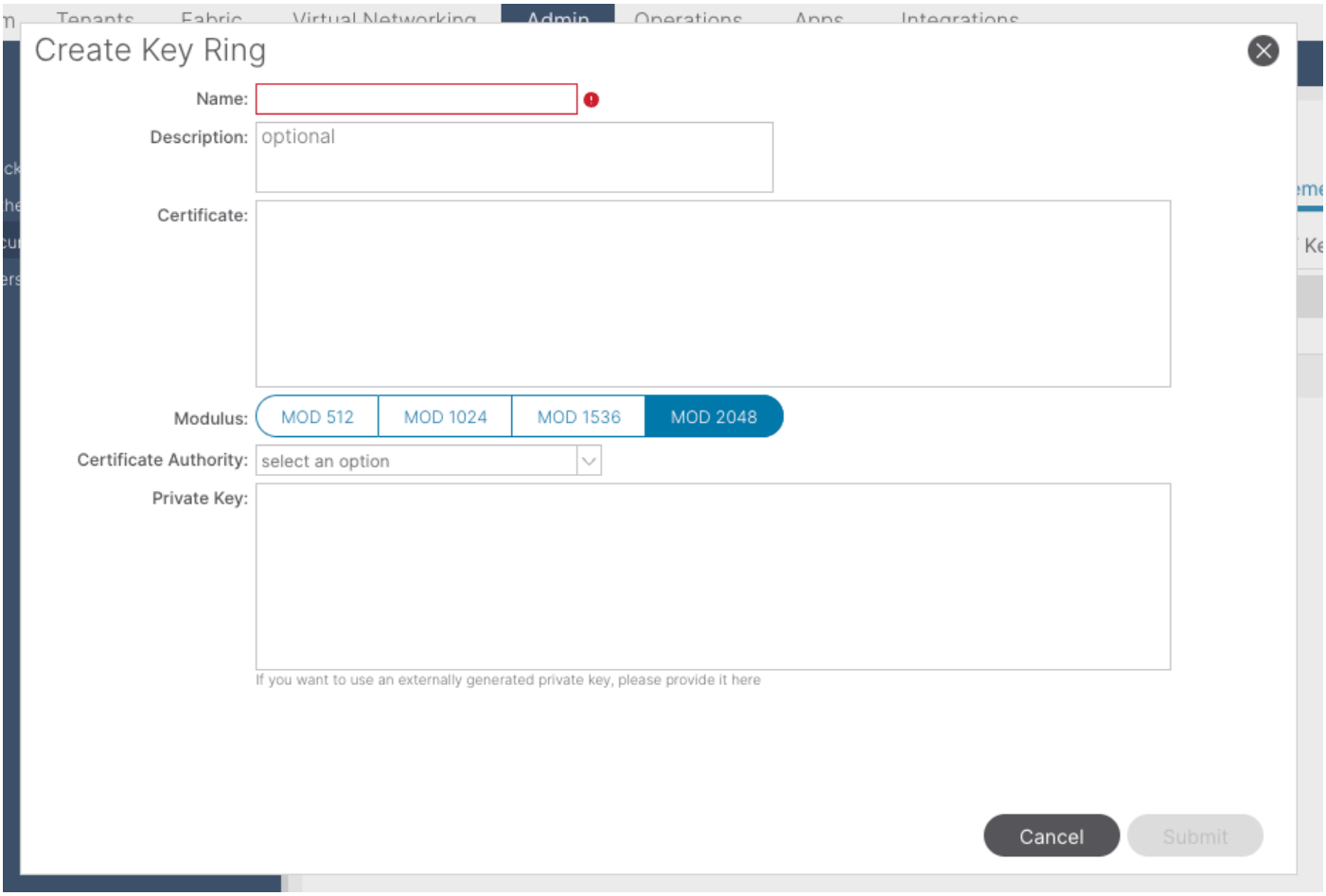
-----BEGIN CERTIFICATE----- INTER-CA-2 CERTIFICATE CONTENT HERE -----END CERTIFICATE----- -----BEGIN CERTIFICATE----- INTER-CA-1 CERTIFICATE CONTENT HERE -----END CERTIFICATE----- -----BEGIN CERTIFICATE----- ROOT-CA CERTIFICATE CONTENT HERE -----END CERTIFICATE-----

按一下**Submit**按鈕。

步驟 2.建立金鑰環

在選單欄上，導航到Admin > AAA > Security > Public Key Management > Key Rings。





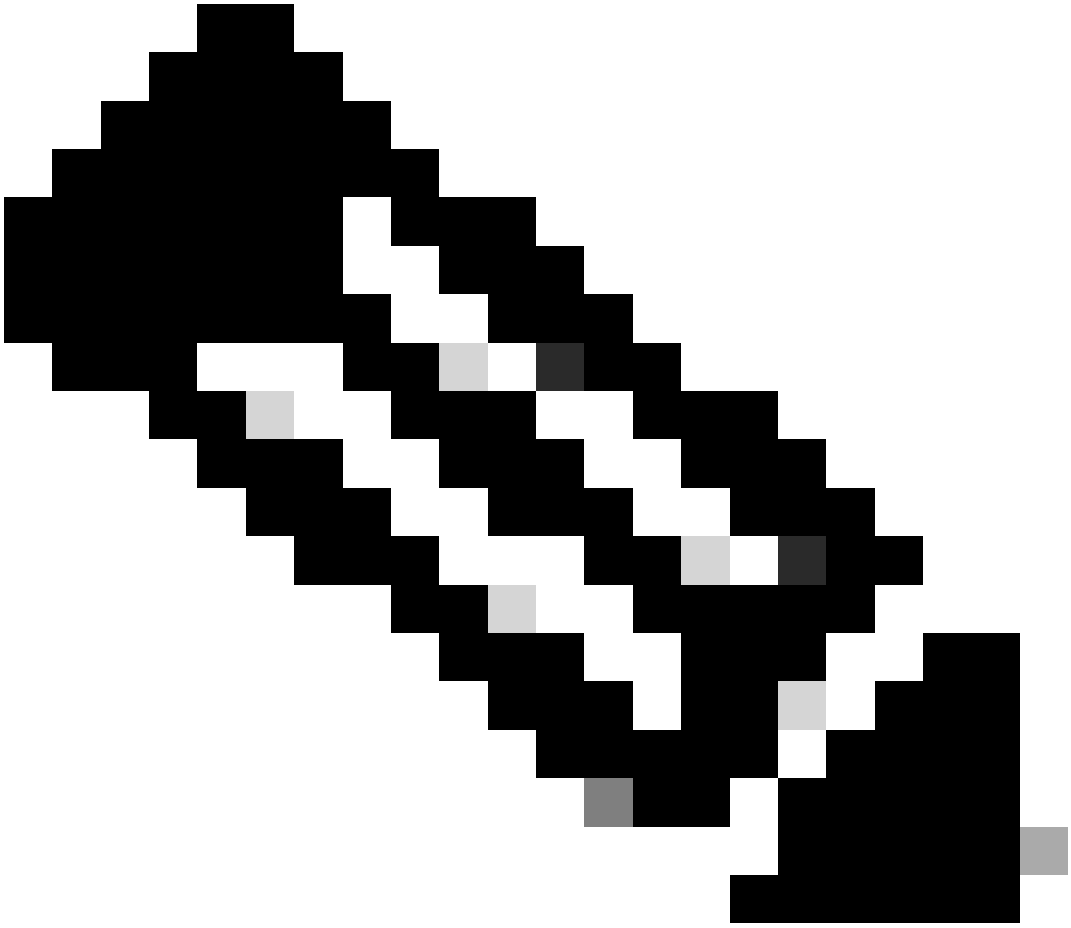
名稱：**必要**（輸入名稱）。

證書：如果使用思科APIC透過金鑰環生成證書簽名請求(CSR)，**請勿增加**任何內容。或者，如果您已經有CA在前面的步驟中簽署的證書內容，請在思科APIC外部生成私鑰和CSR，以增加簽署的證書內容。

模數：**必要**（按一下所需按鍵強度的圓鈕）。

證書頒發機構：**必需**。 從下拉選單中，選擇之前建立的證書頒發機構。

私鑰：如果使用思科APIC透過金鑰環生成CSR，**請勿增加**任何內容。或者，為您輸入的簽名證書增加用於生成CSR的私鑰。

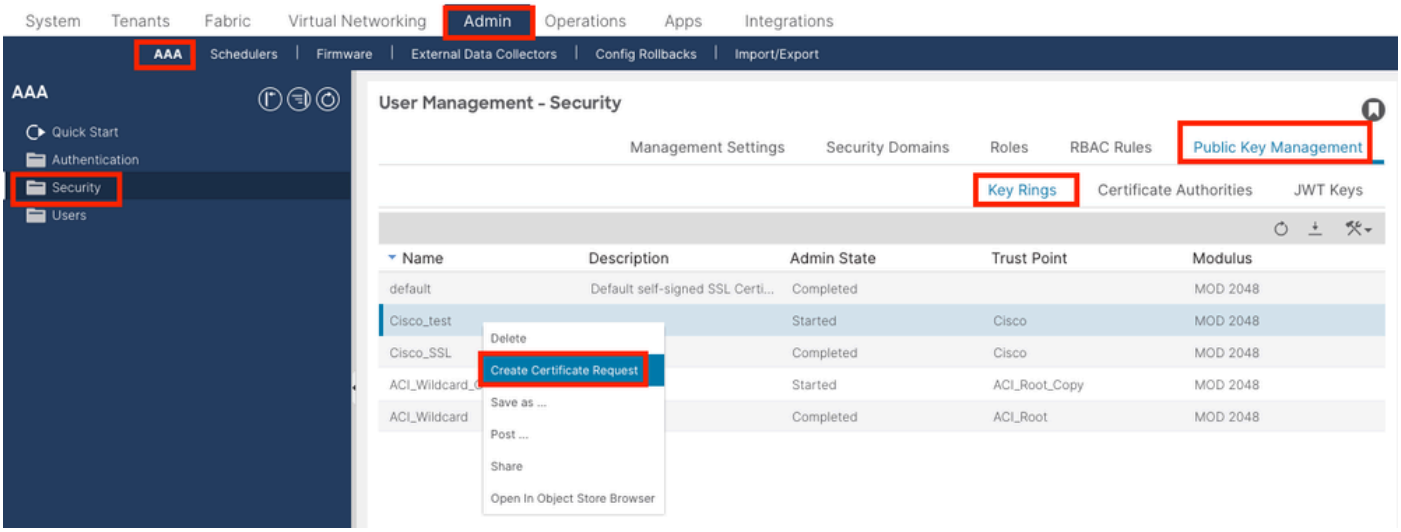


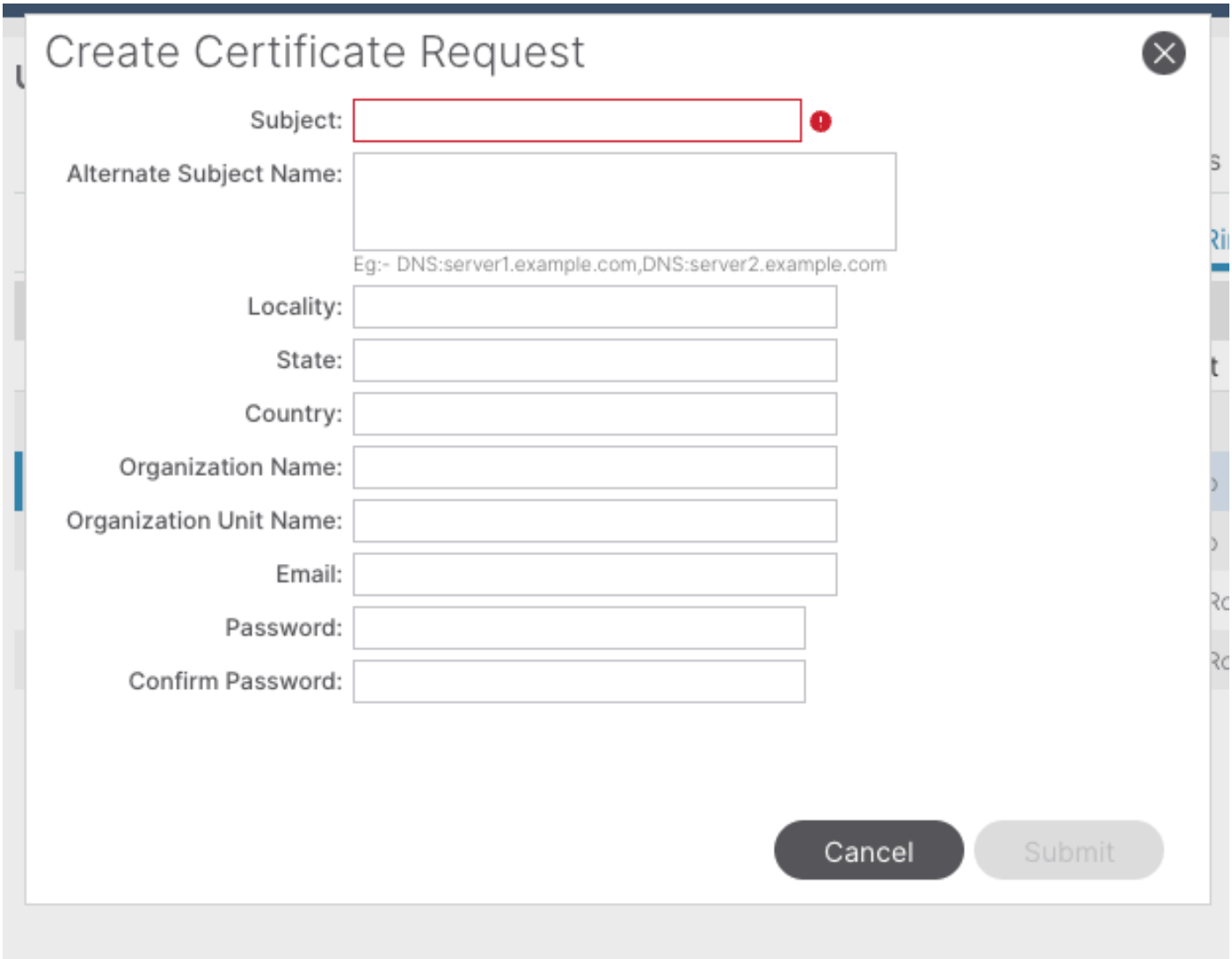
附註：如果您不想使用系統產生的私密金鑰和CSR，並使用自訂私密金鑰和憑證，只需要填寫四個專案：名稱、憑證、憑證授權單位和私密金鑰。 提交後，您只需執行最後一個步驟，即步驟5。

按一下**Submit**按鈕。

步驟 3. 生成私鑰和CSR

在選單欄上，導航到Admin > AAA > Security > Public Key Management > Key Rings。



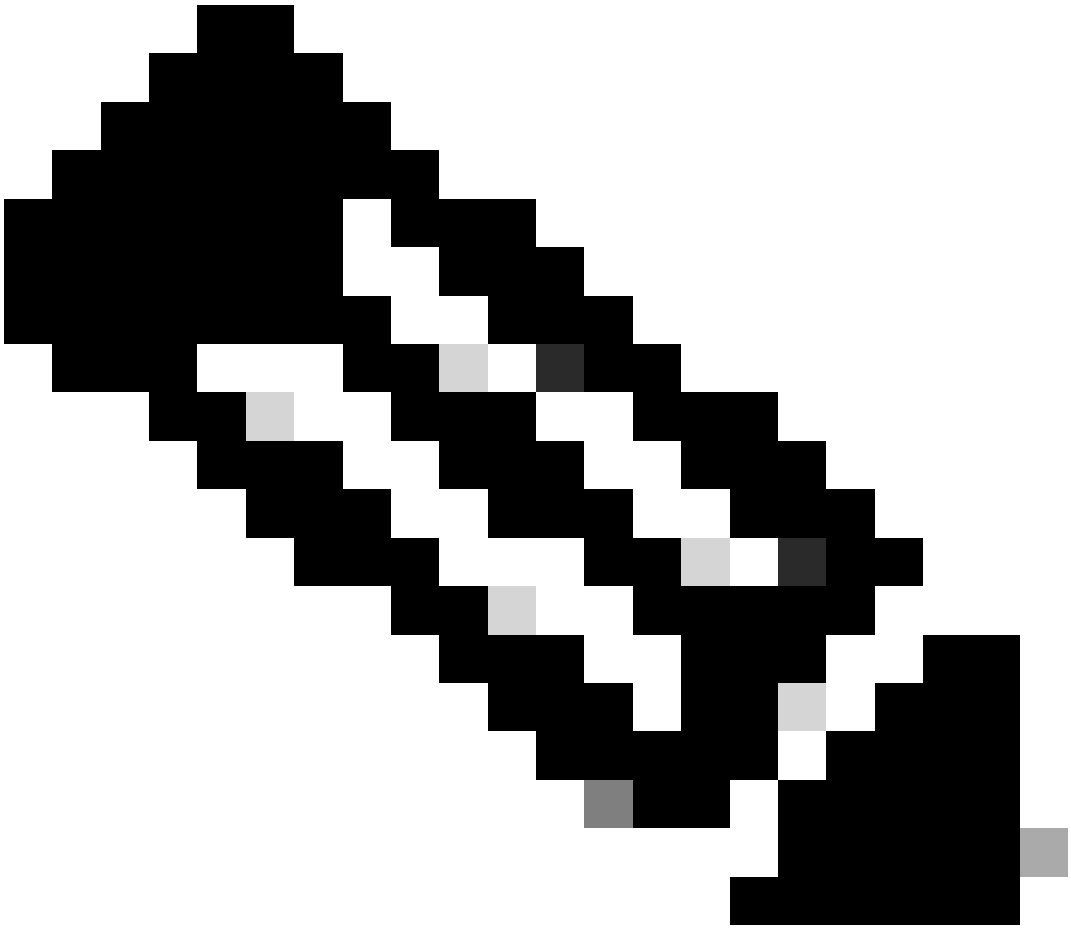


主旨：**必要**。輸入CSR的一般名稱(CN)。

您可以使用萬用字元輸入思科 APIC的完全限定域名(FQDN)，但在現代證書中，通常建議輸入證書的可辨識名稱，並在備用主體名稱欄位中輸入所有思科APIC的FQDN(也稱為SAN - 備用主體名稱)，因為許多現代瀏覽器都期望SAN欄位中包含FQDN。

替代使用者名稱：**必要**。 **輸入**allCisco APIC的FQDN，例如DNS:apic1.example.com,DNS:apic2.example.com,DNS:apic3.example.com或DNS:*example.com。

或者，如果您希望SAN匹配IP地址，請以下列格式輸入Cisco APIC的IP地址：IP:192.168.1.1。



注意：您可以在此欄位中使用網域名稱伺服器(DNS)名稱、IPv4位址或兩者兼有。不支援IPv6地址。

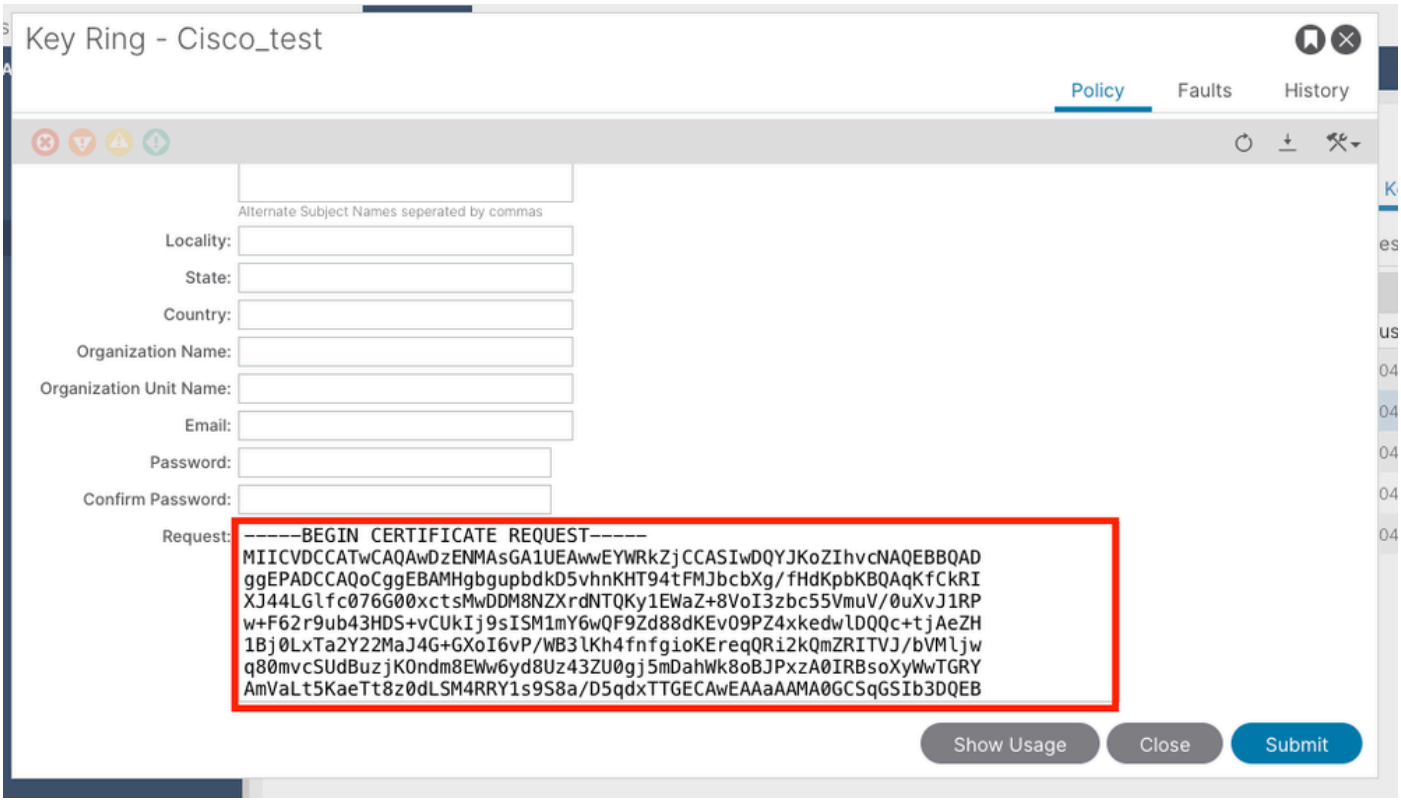
根據您為頒發證書而申請的CA組織的要求填寫其餘欄位。

按一下**Submit**按鈕。

步驟 4.獲取CSR並將其傳送到CA組織

在選單欄上，導航到Admin > AAA > Security > Public Key Management > Key Rings。

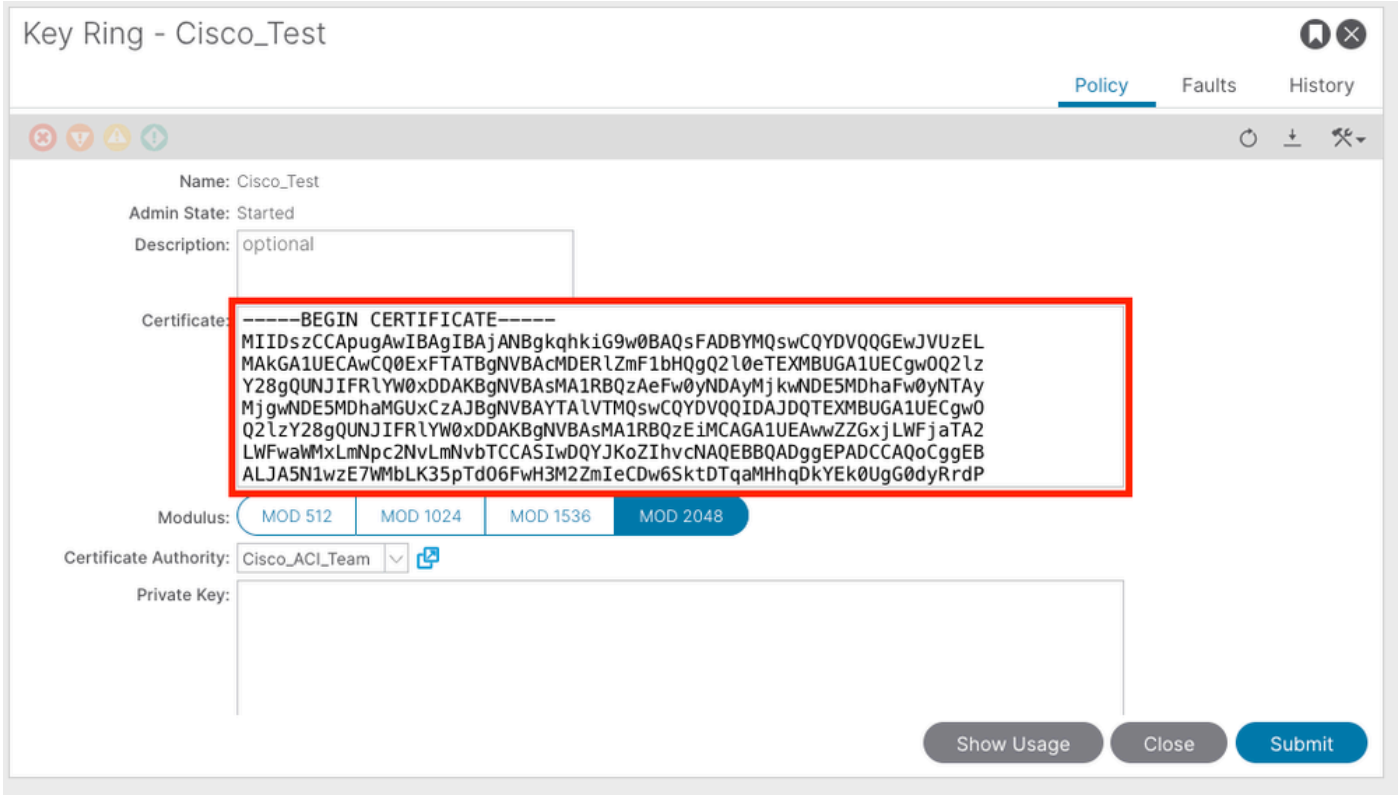
按兩下您的create **Key Ring**名稱並找到**Request**選項。 請求中的內容是CSR。

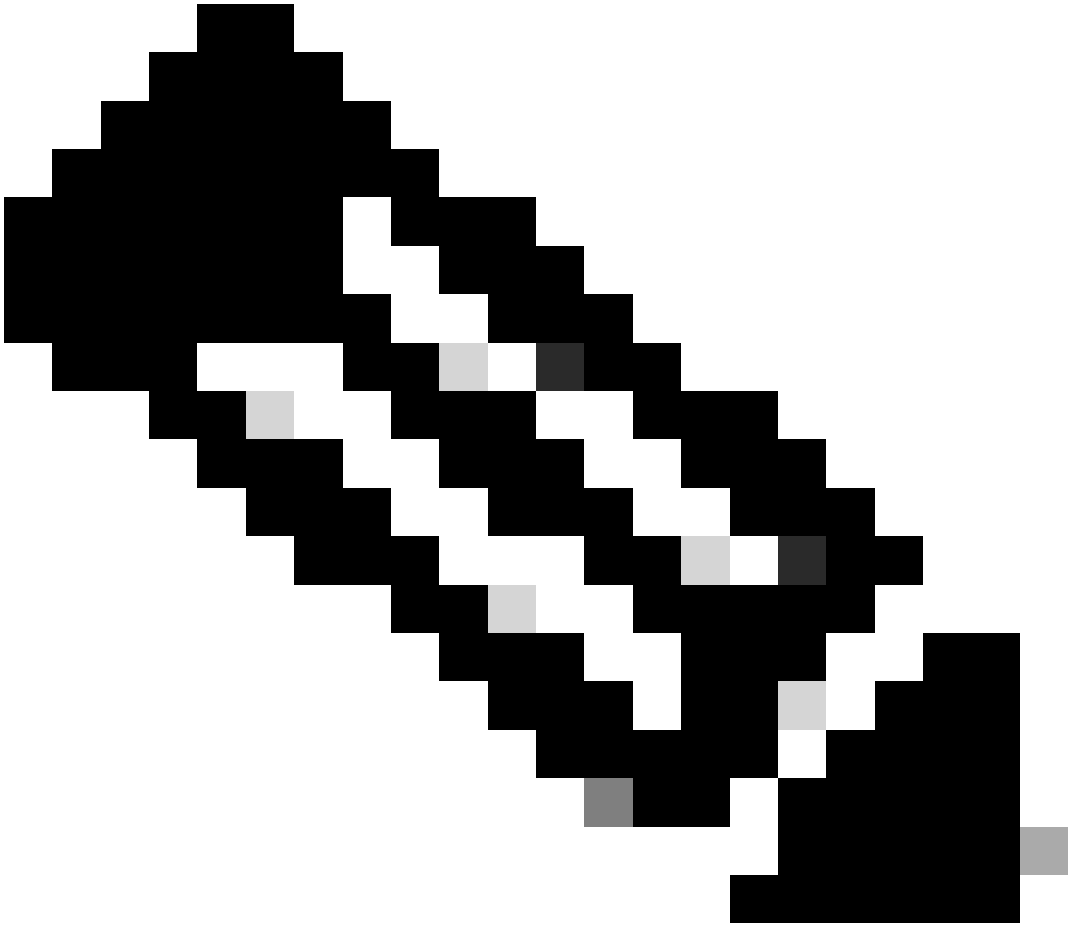


複製請求的所有內容並將其傳送到您的CA。

CA使用其私鑰對CSR執行簽名驗證。

從CA取得簽署的憑證後，它會將該憑證複製到憑證。





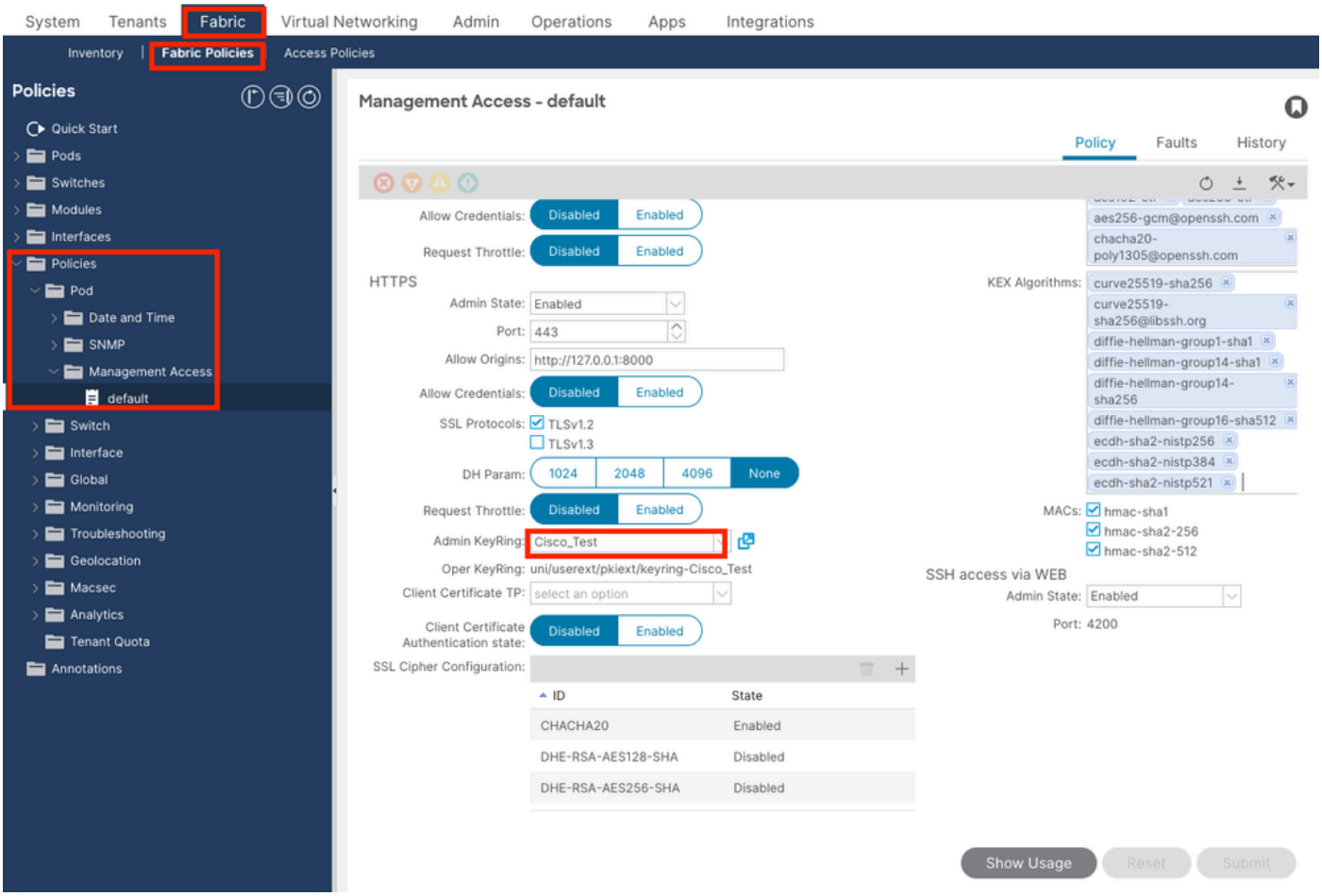
注意：每個證書都必須符合固定格式。

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

按一下**Submit**按鈕。

步驟 5. 在Web上更新簽署憑證

在選單欄上，導航到Fabric > Fabric Policies > Policies > Pod > Management Access > Default。



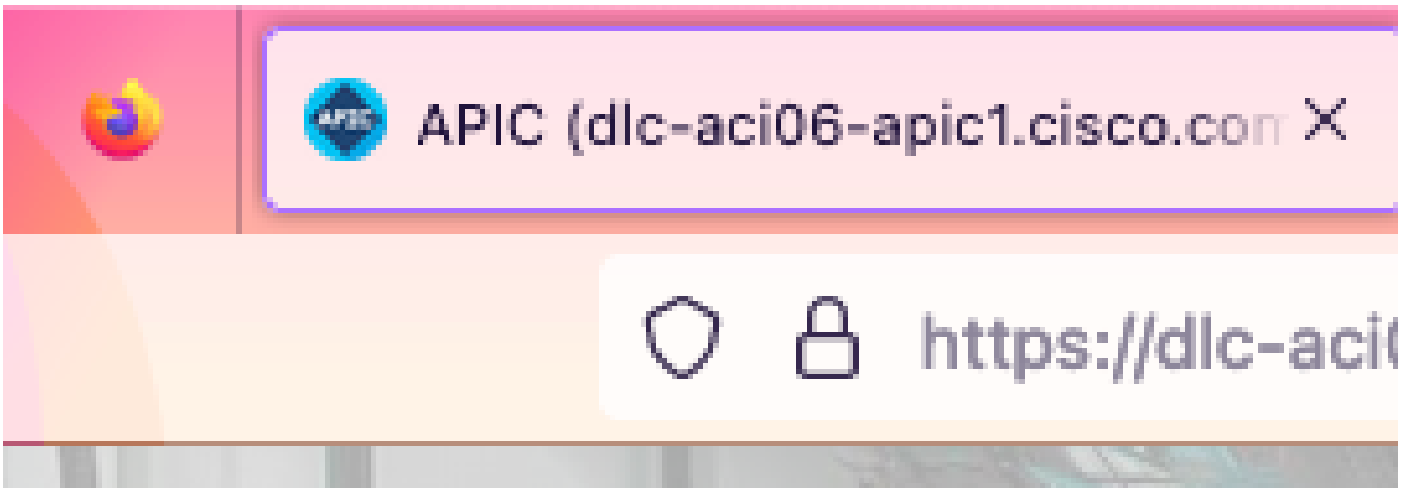
在**Admin KeyRing**下拉選單中，選擇所需的KeyRing。

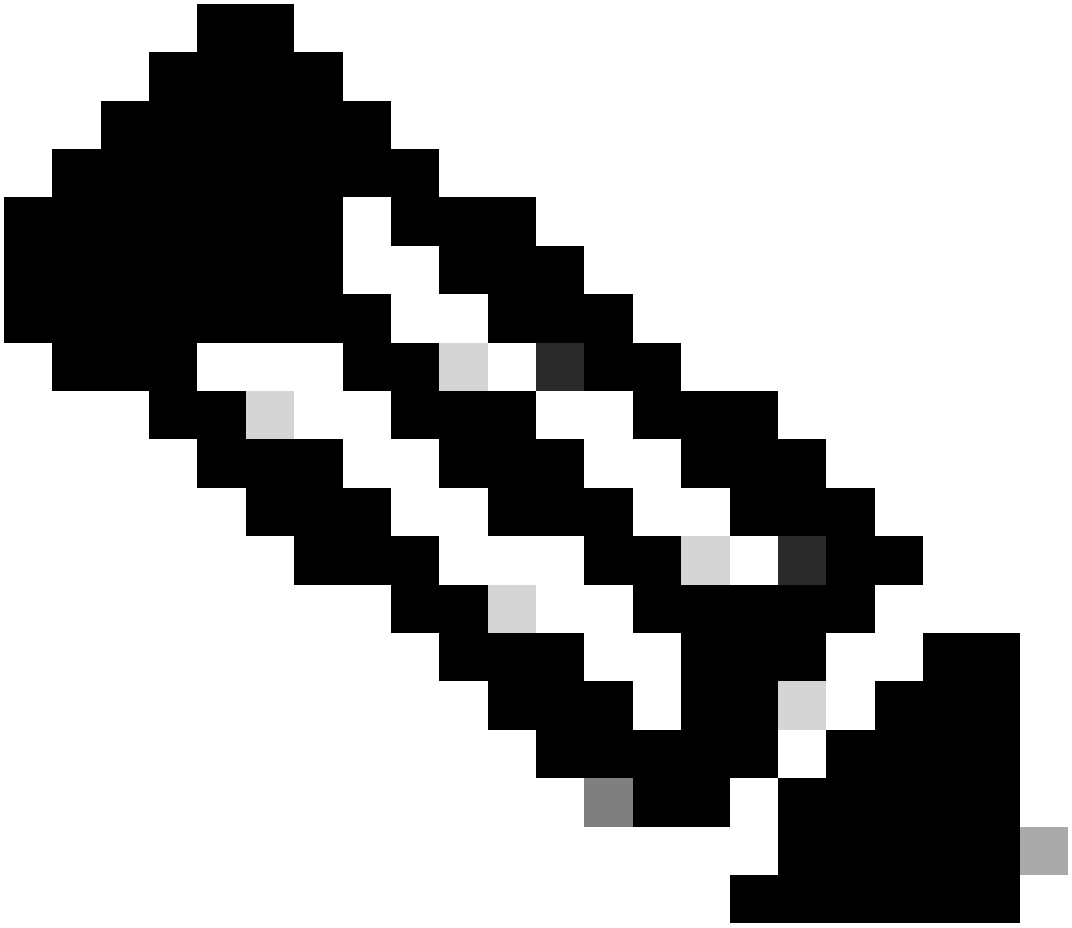
按一下**Submit**按鈕。

按一下「提交」後，由於憑證原因而發生錯誤。使用新憑證重新整理。

驗證

訪問APIC GUI後，APIC使用CA簽名的證書進行通訊。在瀏覽器中檢視憑證資訊以驗證它。

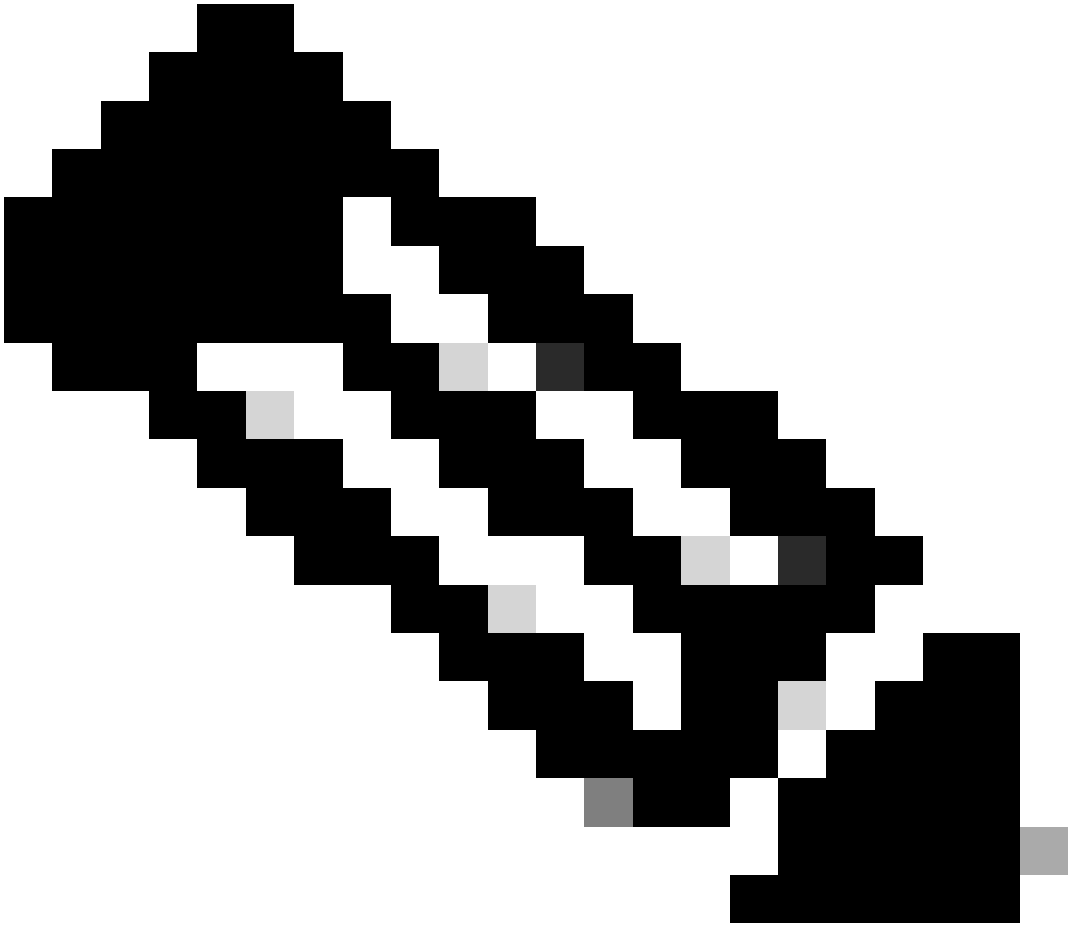




注意：在不同的瀏覽器中檢視HTTPS證書的方法不完全相同。有關特定方法，請參閱瀏覽器的使用手冊。

疑難排解

如果瀏覽器仍然提示APIC GUI不受信任，請在瀏覽器中驗證GUI的證書是否與金鑰環中提交的證書一致。
您需要信任在您的電腦或瀏覽器中頒發證書的**CA根證書**。

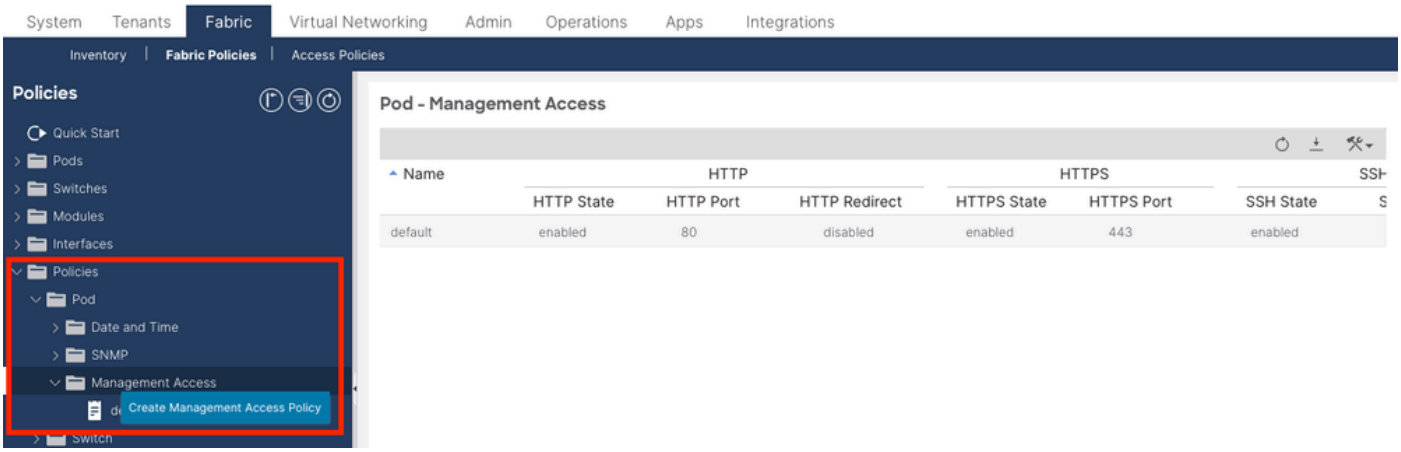


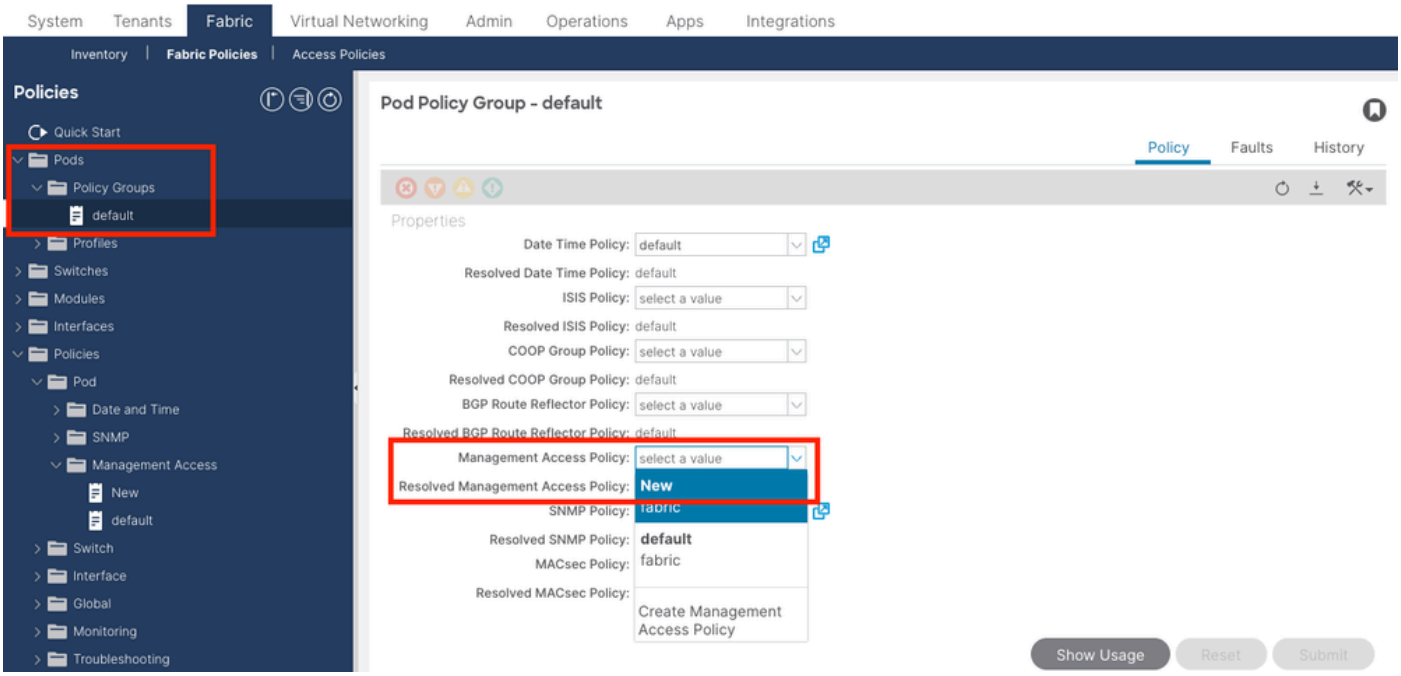
注意：Google Chrome瀏覽器必須驗證證書的**SAN**，才能信任此證書。

在使用自簽名證書的APIC中，證書到期警告在極少數情況下出現。

在Keyring中查詢證書，使用證書解析工具來解析證書，並將其與瀏覽器中使用的證書進行比較。

如果金鑰環中的證書已更新，請建立新的管理訪問策略並應用該策略。





如果Keyring中的證書沒有自動更新，請與Cisco TAC聯絡以獲取更多幫助。

相關資訊

- 思科APIC安全配置指南5.2(x)版
- 思科技術支援與下載

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。