配置ACI APIC GUI HTTPS證書

目錄

簡介

必要條件

- 需求
- 採用元件

設定

- 組態
  - 步驟1.匯入CA頒發機構根證書或中間證書
  - 步驟2.建立金鑰環
  - 步驟3.生成私鑰和CSR
  - 步驟4.取得CSR並將其傳送到CA組織
  - 步驟5.更新Web上的簽名證書

驗證

疑難排解

相關資訊

簡介

本檔案介紹自訂SSL和自簽名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：

- 應用程式原則基礎架構控制器(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

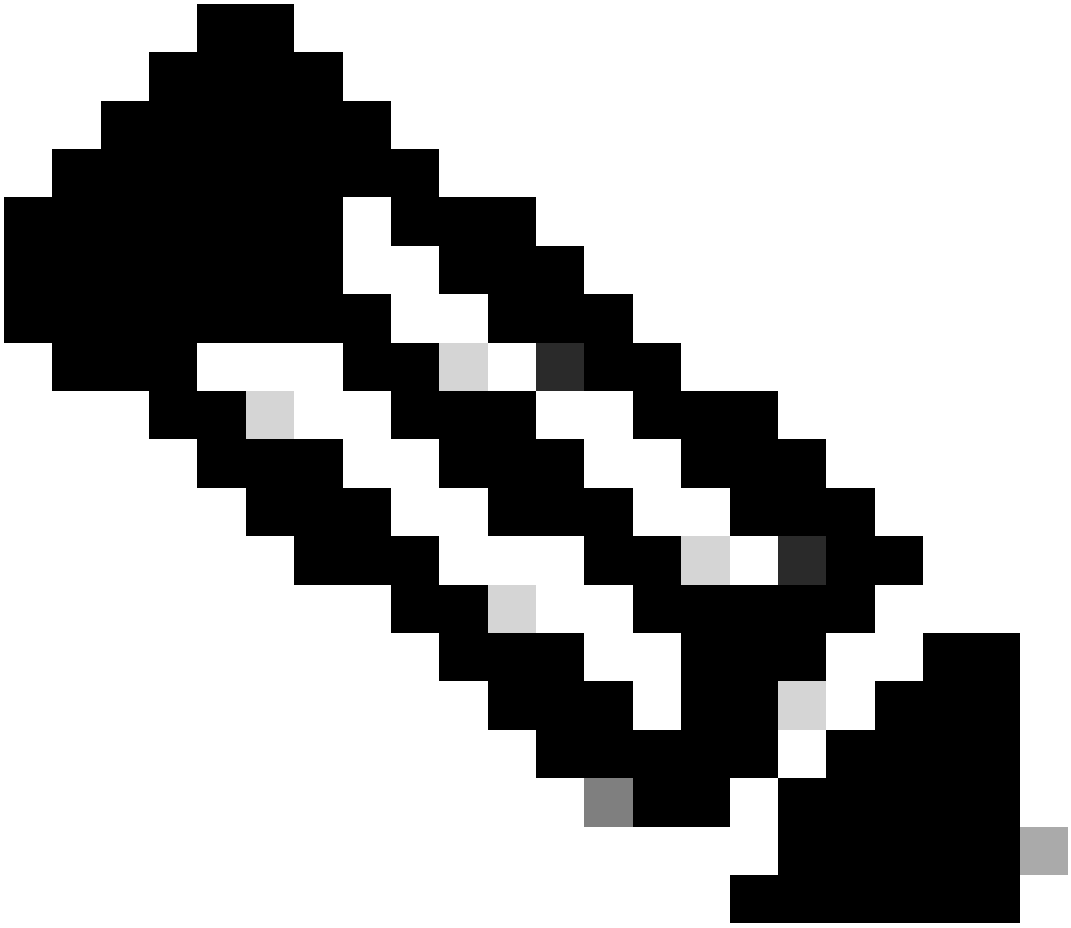
初始化裝置後，它將自簽名證書用作HTTPS的SSL證書。自簽名證書的有效期為1000天。

預設情況下，裝置會在自簽名證書到期前一個月自動續訂並生成新的自簽名證書。

組態

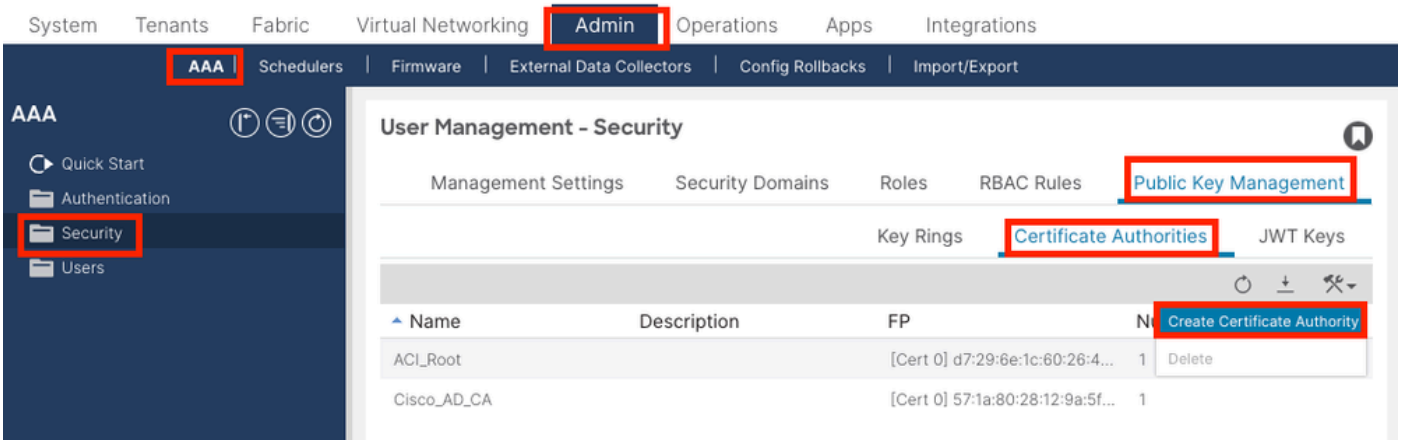
裝置使用自簽名證書。訪問APIC GUI時，瀏覽器提示證書不可信。為了解決此問題，本檔案使用受信任的CA授權單位來簽署憑證。

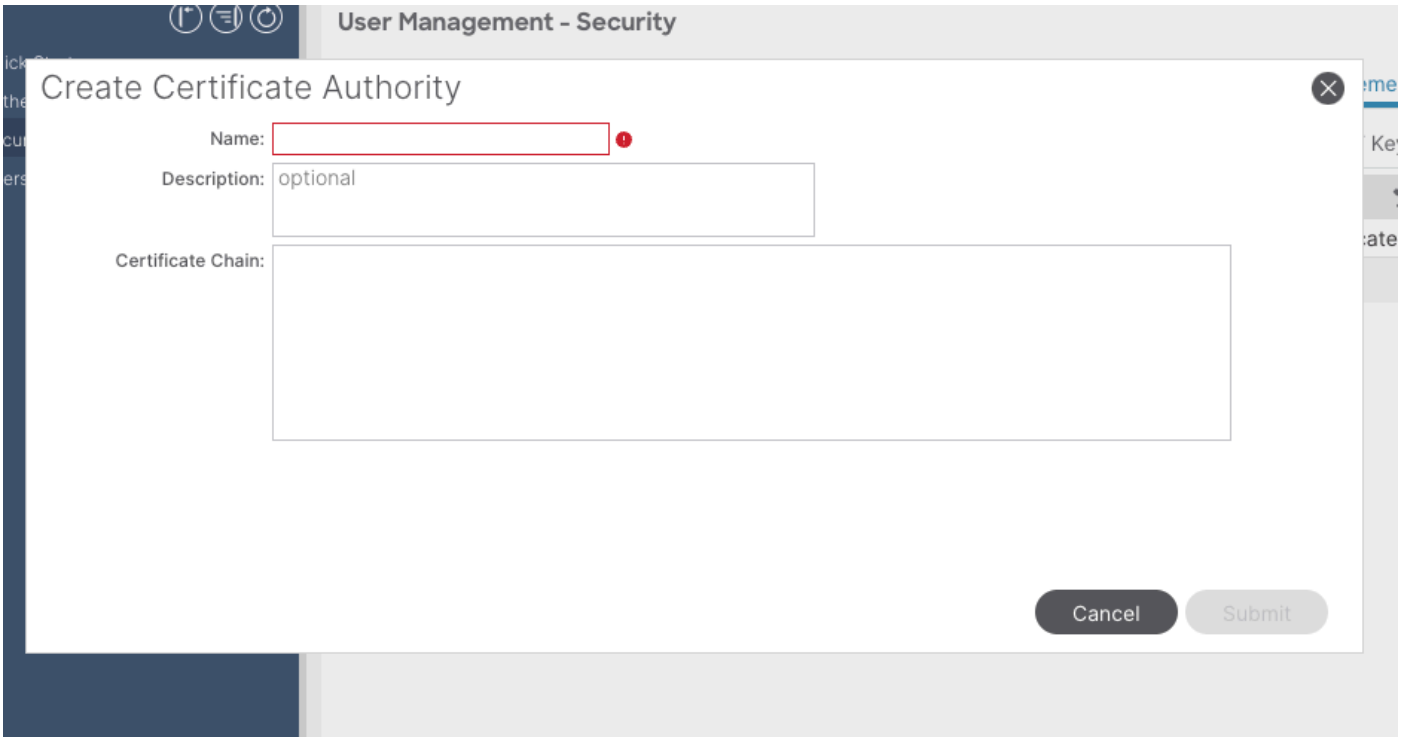
步驟1.匯入CA頒發機構根證書或中間證書



附註：如果您使用CA根證書直接進行簽名，則只需匯入CA根證書。但是，如果您使用中間證書進行簽名，則必須匯入完整的證書鏈，即：根證書和不太受信任的中間證書。

在選單欄中，導航至Admin > AAA > Security > Public Key Management > Certificate Authorities。





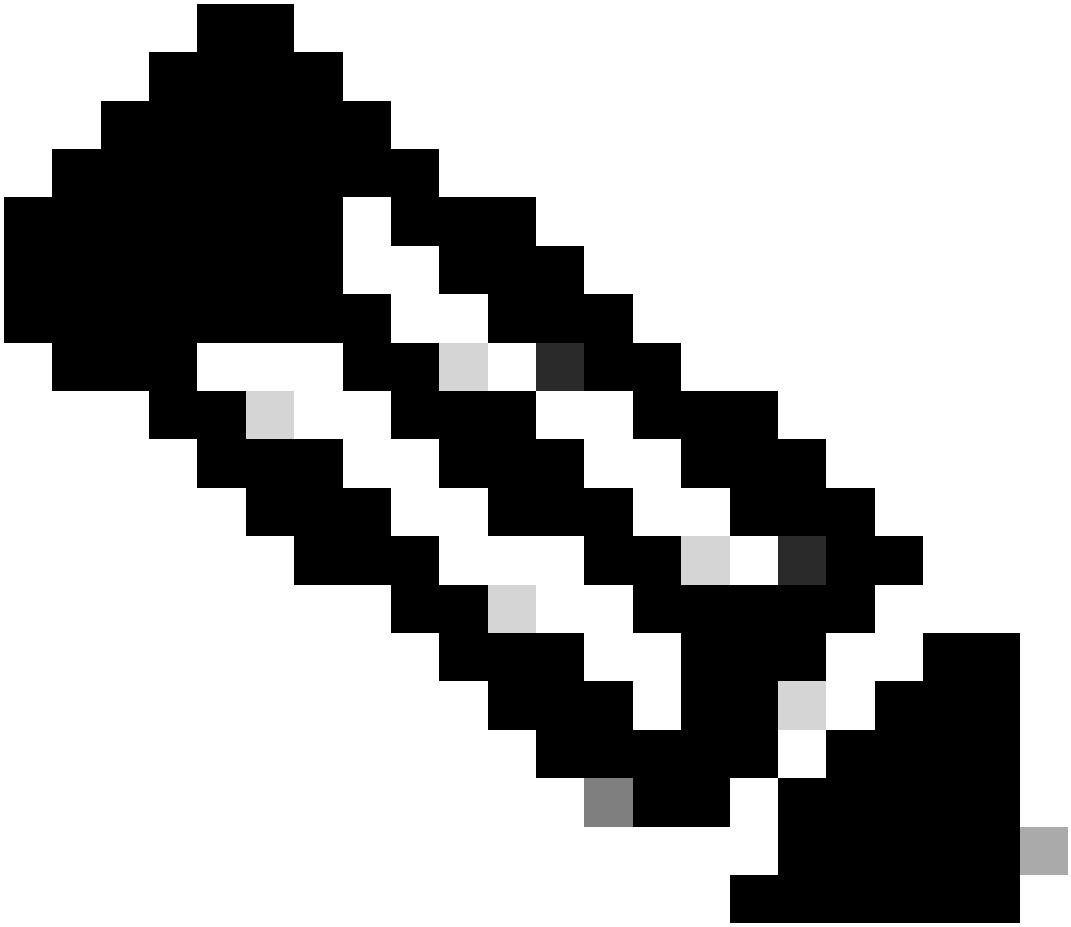
名稱：必需。

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。

認證鏈：必需。

填寫受信任的CA根證書和CA中間證書。



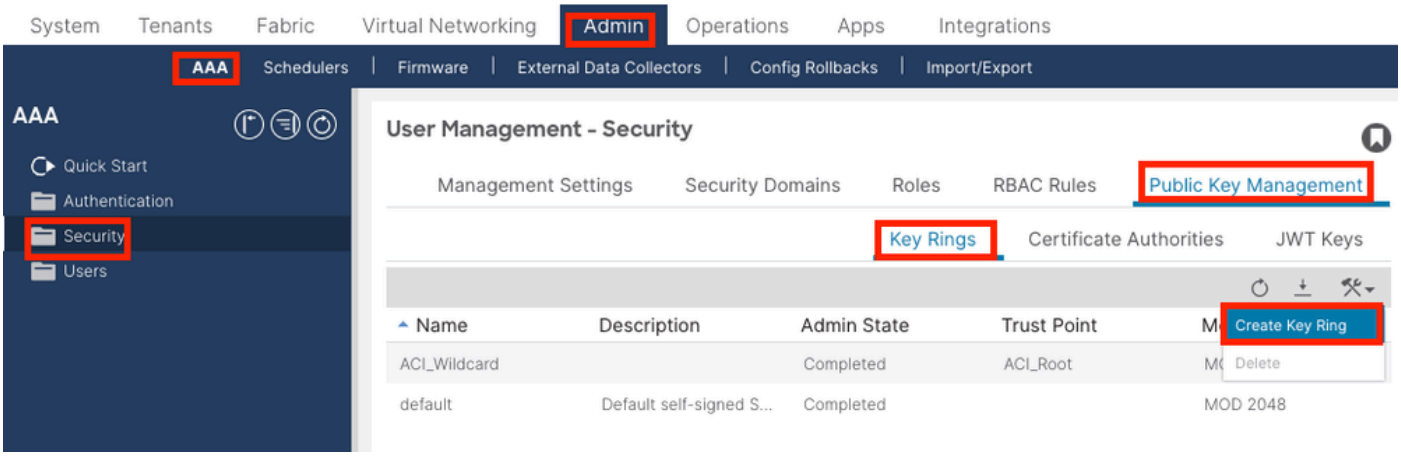
附註：每個證書必須符合固定格式。

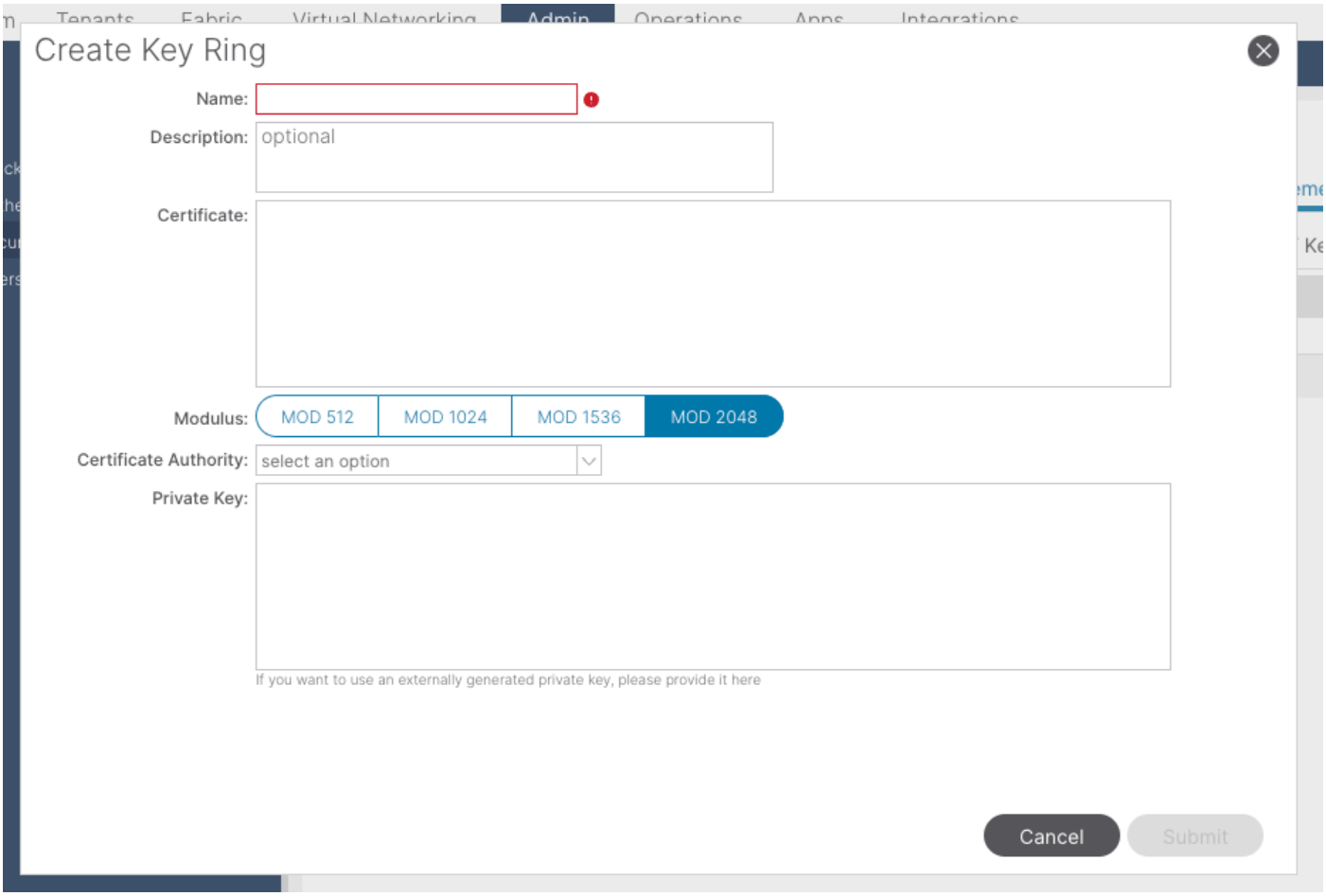
-----BEGIN CERTIFICATE----- INTER-CA-2 CERTIFICATE CONTENT HERE -----END CERTIFICATE----- -----BEGIN CERTIFICATE----- INTER-CA-1 CERTIFICATE CONTENT HERE -----END CERTIFICATE----- -----BEGIN CERTIFICATE----- ROOT-CA CERTIFICATE CONTENT HERE -----END CERTIFICATE-----

按一下Submit按鈕。

步驟2.建立金鑰環

在選單欄中，導航至Admin > AAA > Security > Public Key Management > Key Rings。





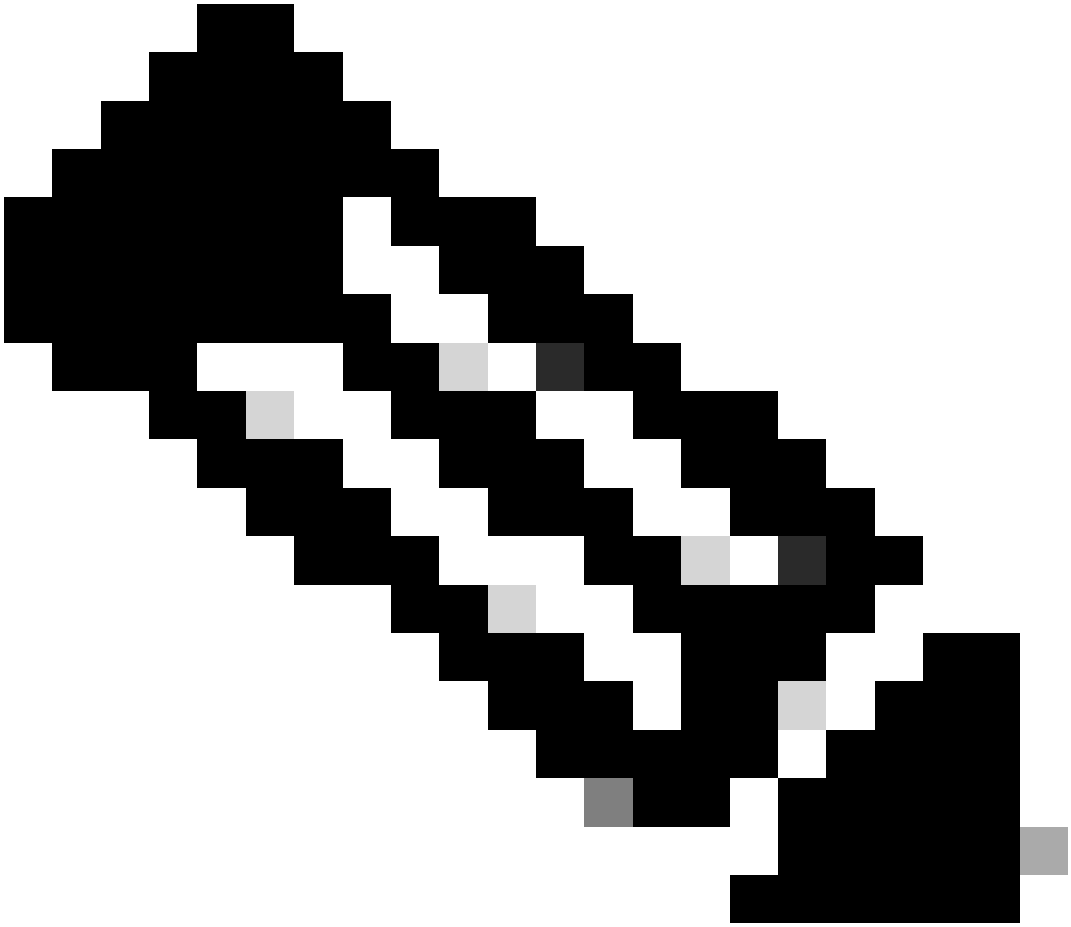
名稱：必需（輸入名稱）。

證書：如果您通過金鑰環使用思科APIC生成證書簽名請求(CSR)，請不要添加任何內容。或者，如果您已經擁有由CA在前面的步驟中簽名的證書內容，請透過在Cisco APIC之外產生私鑰和CSR來新增簽名的證書內容。

模數：必需（按一下所需鍵強度的單選按鈕）。

證書頒發機構： 必需。從下拉選單中，選擇您之前建立的證書頒發機構。

私鑰：如果您使用思科APIC通過金鑰環生成了CSR，則不新增任何內容。或者，為輸入的簽名證書新增用於生成CSR的私鑰。

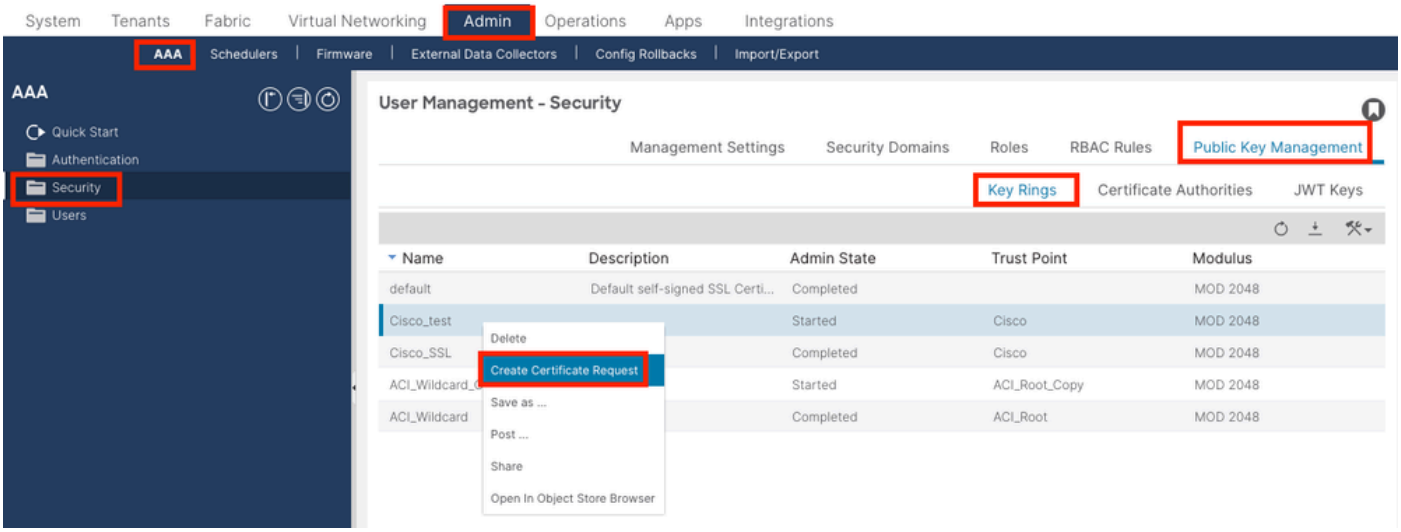


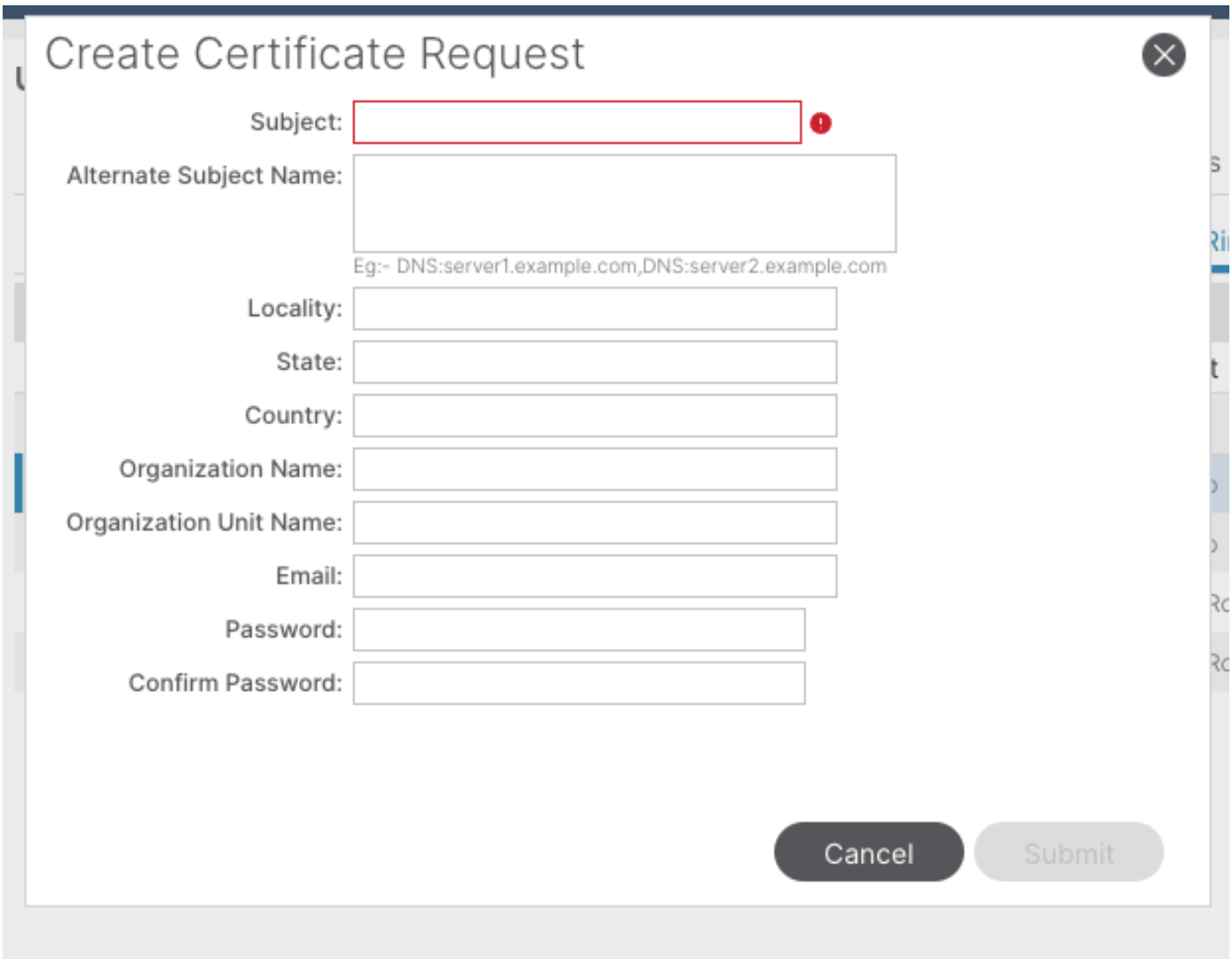
附註：如果您不想使用系統生成的私鑰和CSR，並且不想使用自定義私鑰和證書，則只需填寫以下四個專案：名稱、證書、證書頒發機構和私鑰。提交後，您只需執行最後一步即步驟5。

按一下Submit按鈕。

步驟3.產生私鑰和CSR

在選單欄中，導航至Admin > AAA > Security > Public Key Management > Key Rings。





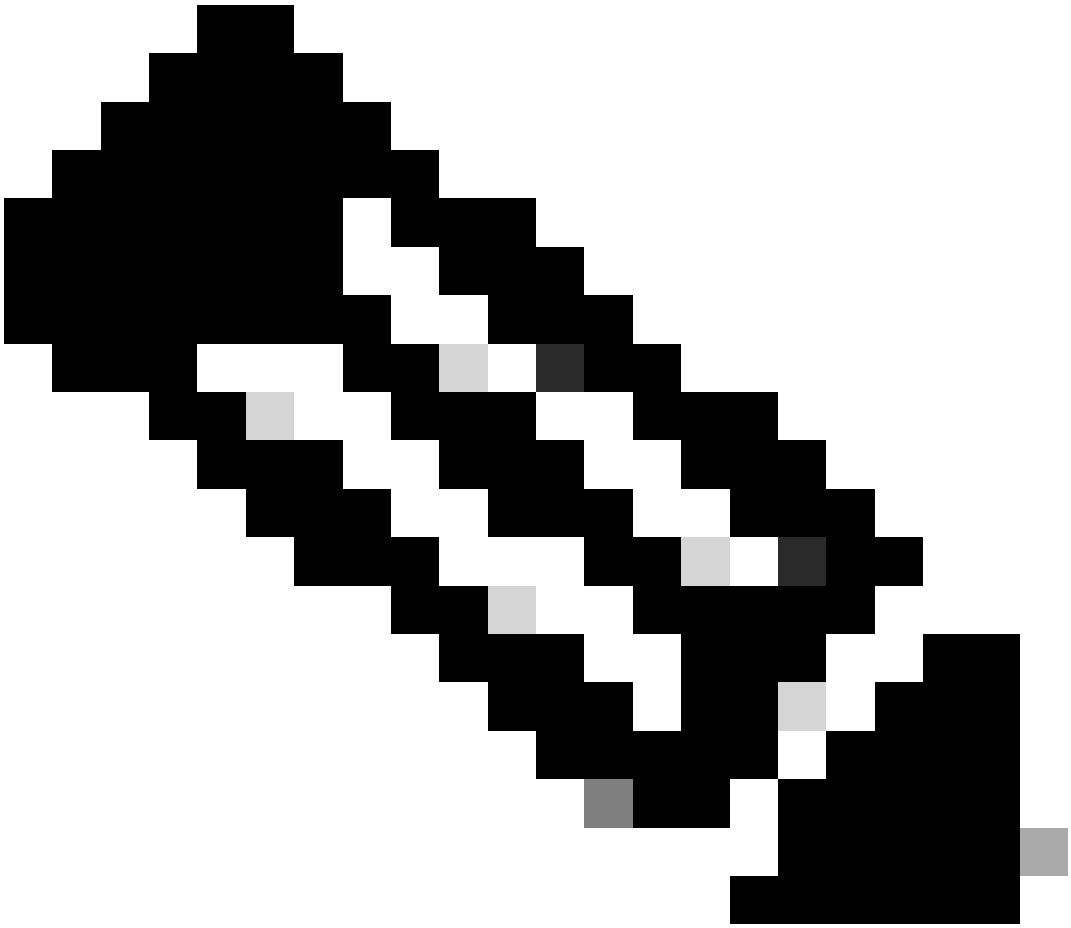
主題：必需。輸入CSR的公用名稱(CN)。

可以使用萬用字元輸入Cisco 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識別名稱，並在Alternate Subject Name欄位中輸入所有Cisco APIC的FQDN(也稱為SAN — 使用者替代名稱)，因為許多現代瀏覽器都期望SAN欄位中的FQDN。

備用使用者名稱：必需。輸入所有思科APIC的

FQDN，DNS:apic1.example.com,DNS:apic2.example.com,DNS:apic3.example.comDNS:*example.com。

或者，如果您希望SAN與IP地址匹配，請按以下格式輸入Cisco APIC的IP地址：IP:192.168.1.1.



附註：在此欄位中可以使用域名伺服器(DNS)名稱、IPv4地址或兩者的組合。不支援IPv6地址。

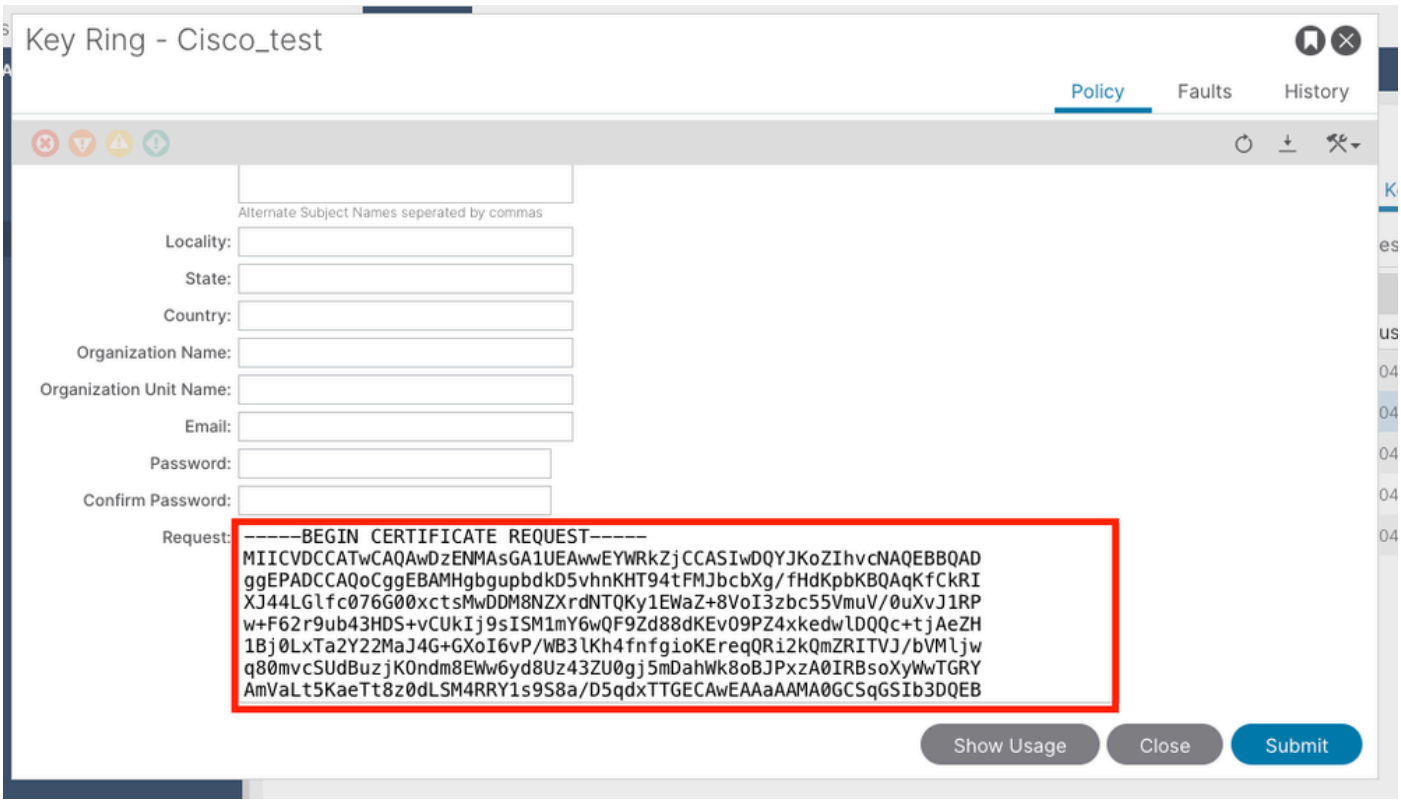
根據您正在申請的CA組織的要求填寫剩餘欄位，以便頒發證書。

按一下Submit按鈕。

步驟4.取得CSR並將其傳送到CA組織

在選單欄中，導航至Admin > AAA > Security > Public Key Management > Key Rings。

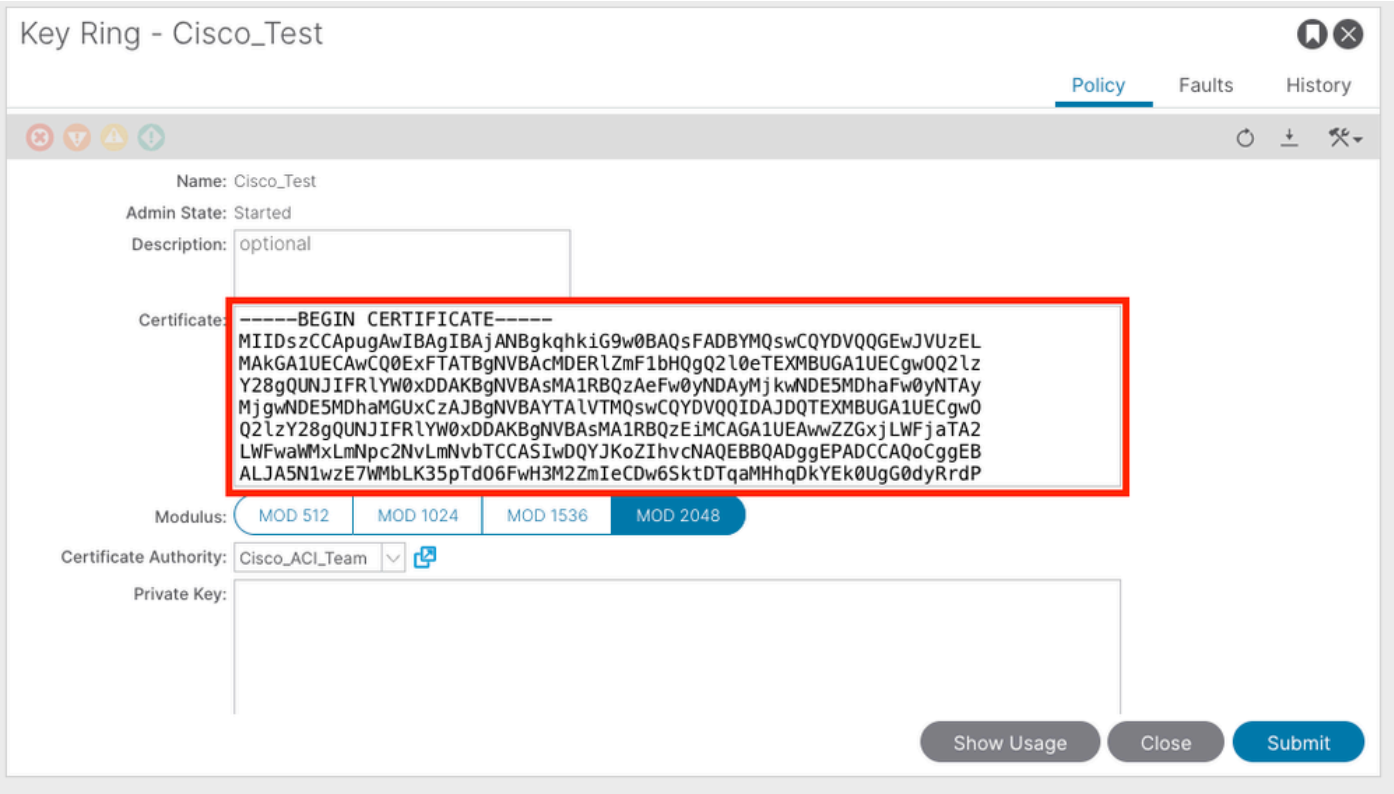
按兩下您的建立金鑰環名並找到請求選項。請求中的內容是CSR。

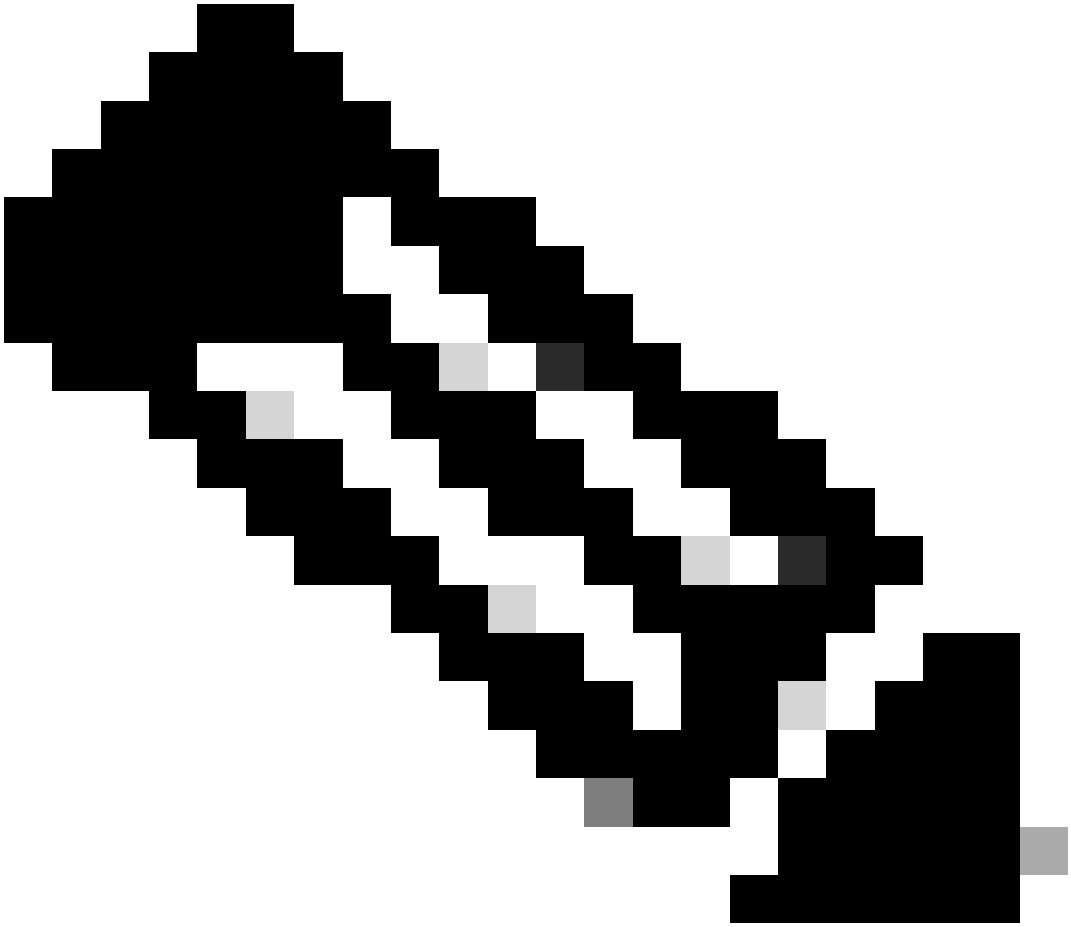


複製請求的所有內容並將其傳送給您的CA。

CA使用其私鑰對CSR執行簽名驗證。

從CA取得簽名的憑證後，會將憑證複製到憑證。





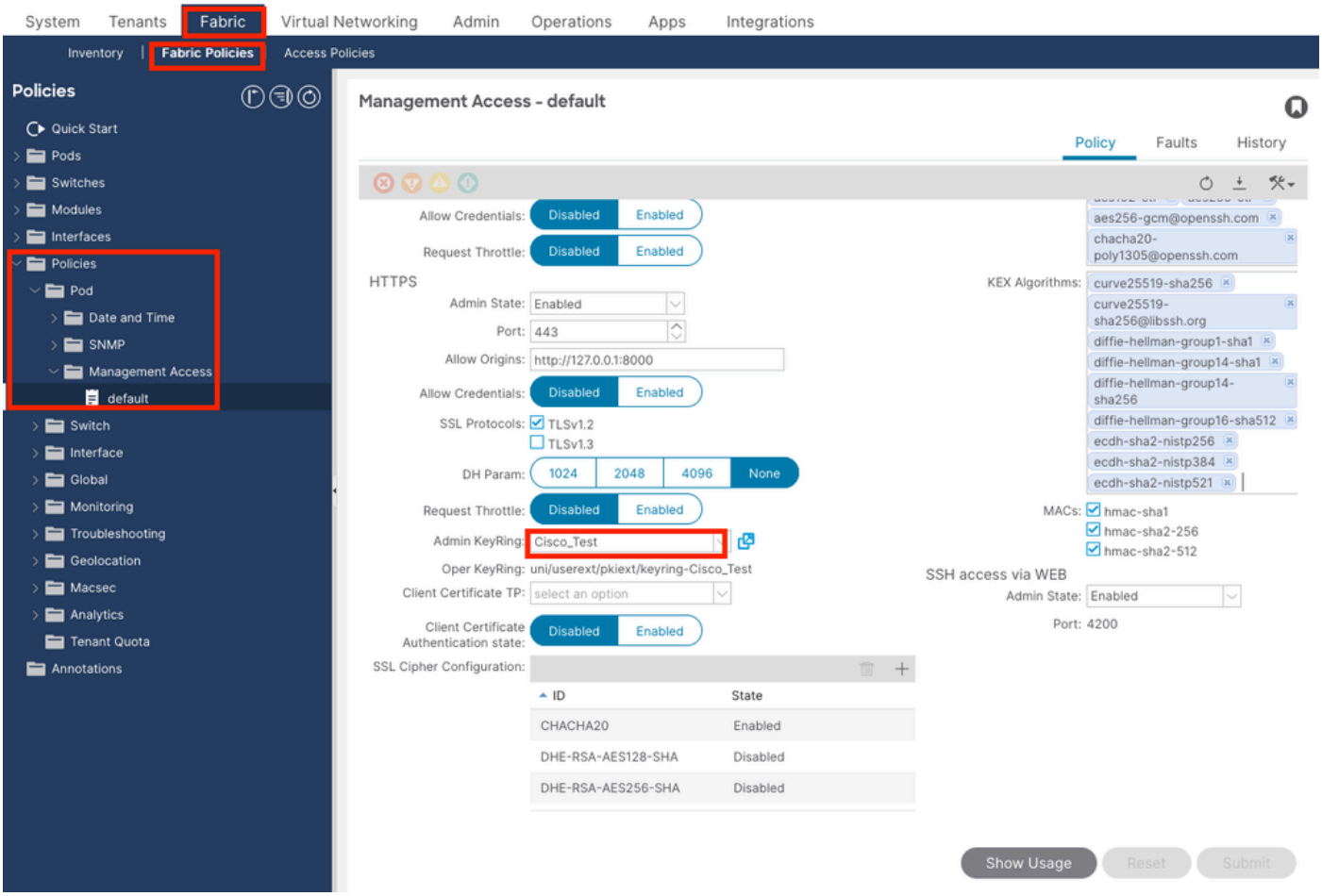
附註：每個證書必須符合固定格式。

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

按一下Submit按鈕。

步驟5.更新Web上的簽名證書

在選單欄中，導航至Fabric > Fabric Policies > Policies > Pod > Management Access > Default。



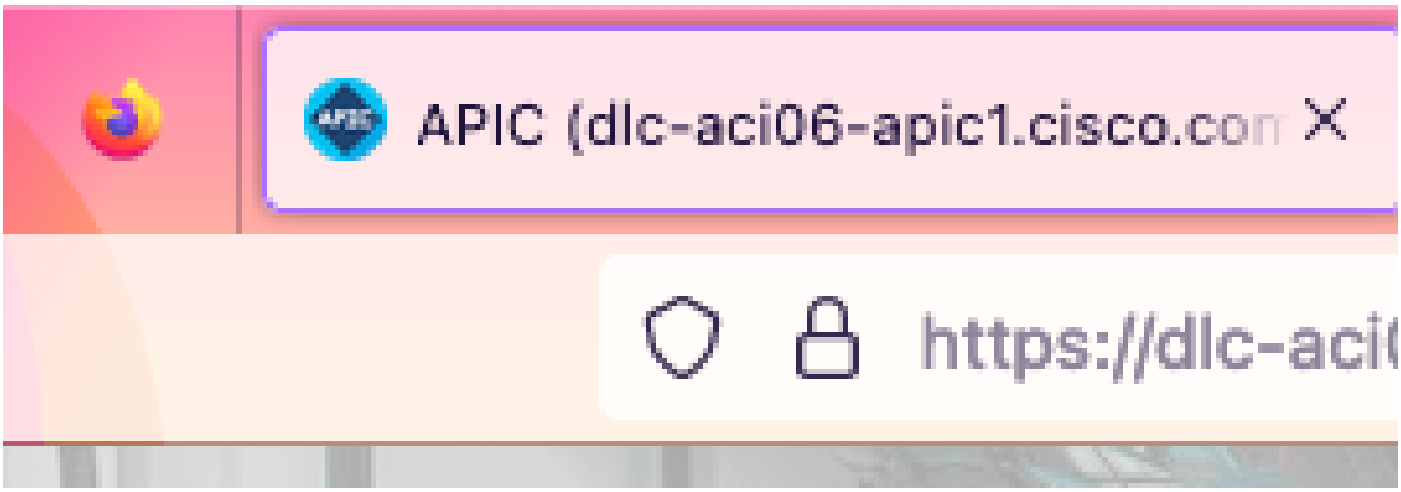
在Admin KeyRing下拉選單中，選擇所需的KeyRing。

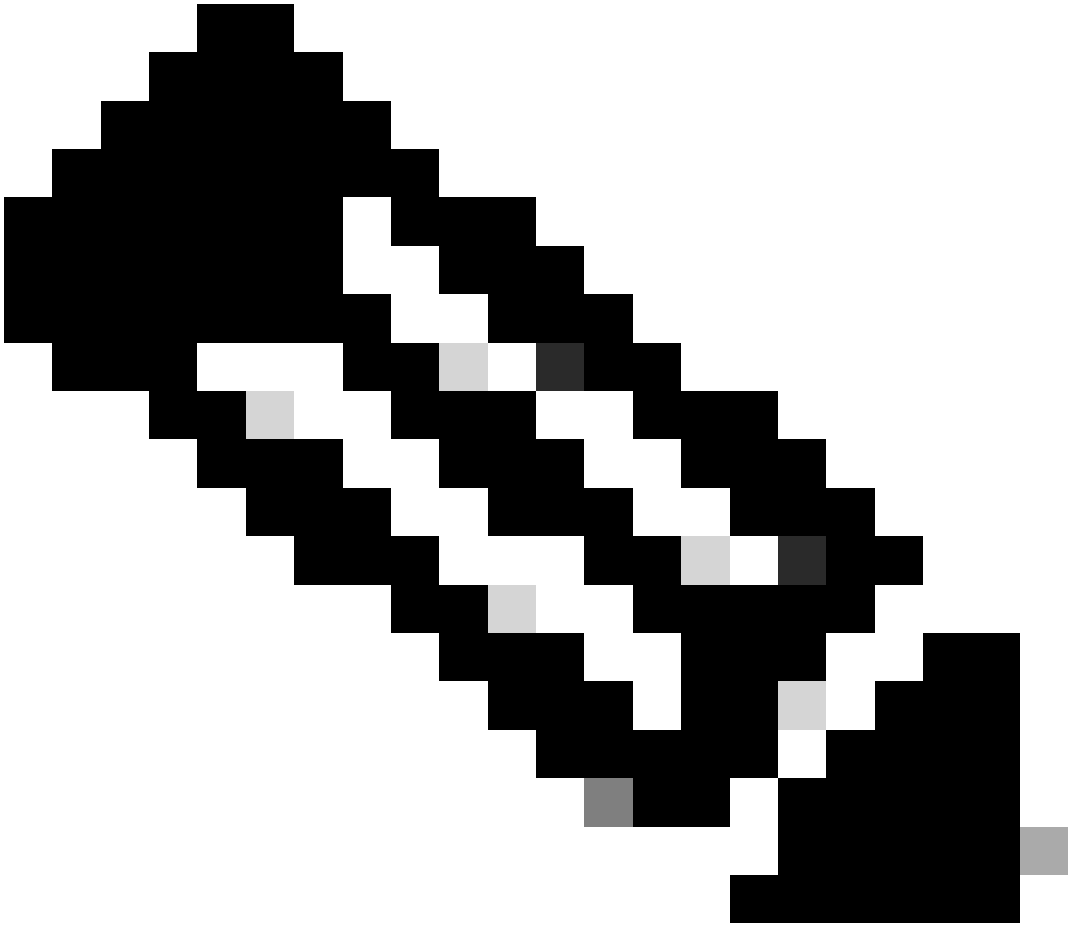
按一下Submit按鈕。

按一下提交後，由於證書原因會出現錯誤。使用新證書刷新。

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便進行驗證。

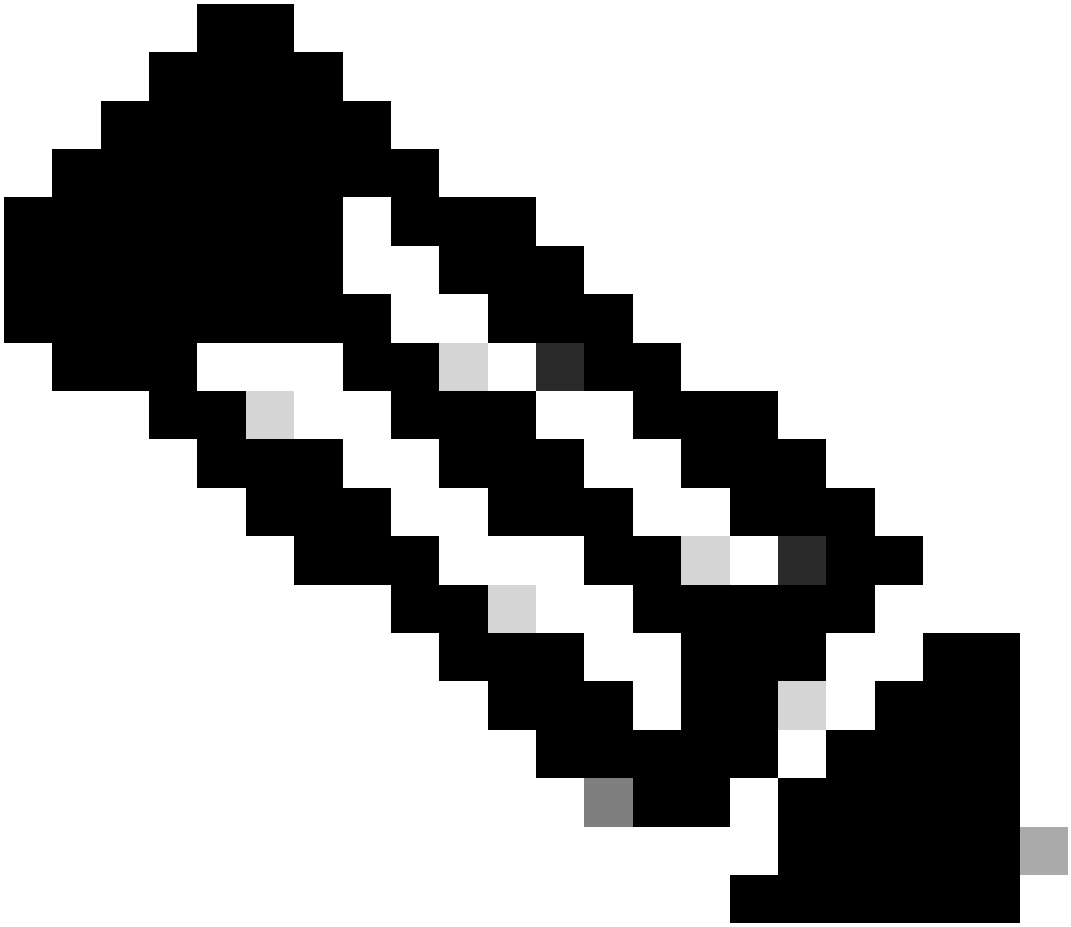




附註：在不同的瀏覽器中檢視HTTPS證書的方法並不完全相同。有關特定方法，請參閱瀏覽器的使用手冊。

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。
您需要信任在計算機或瀏覽器上頒發證書的CA根證書。

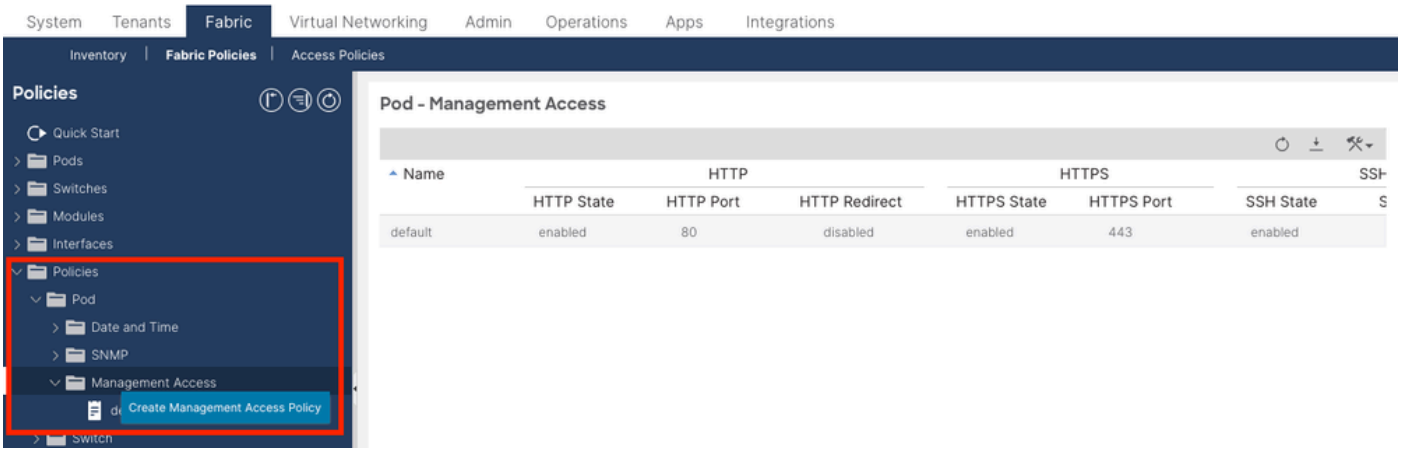


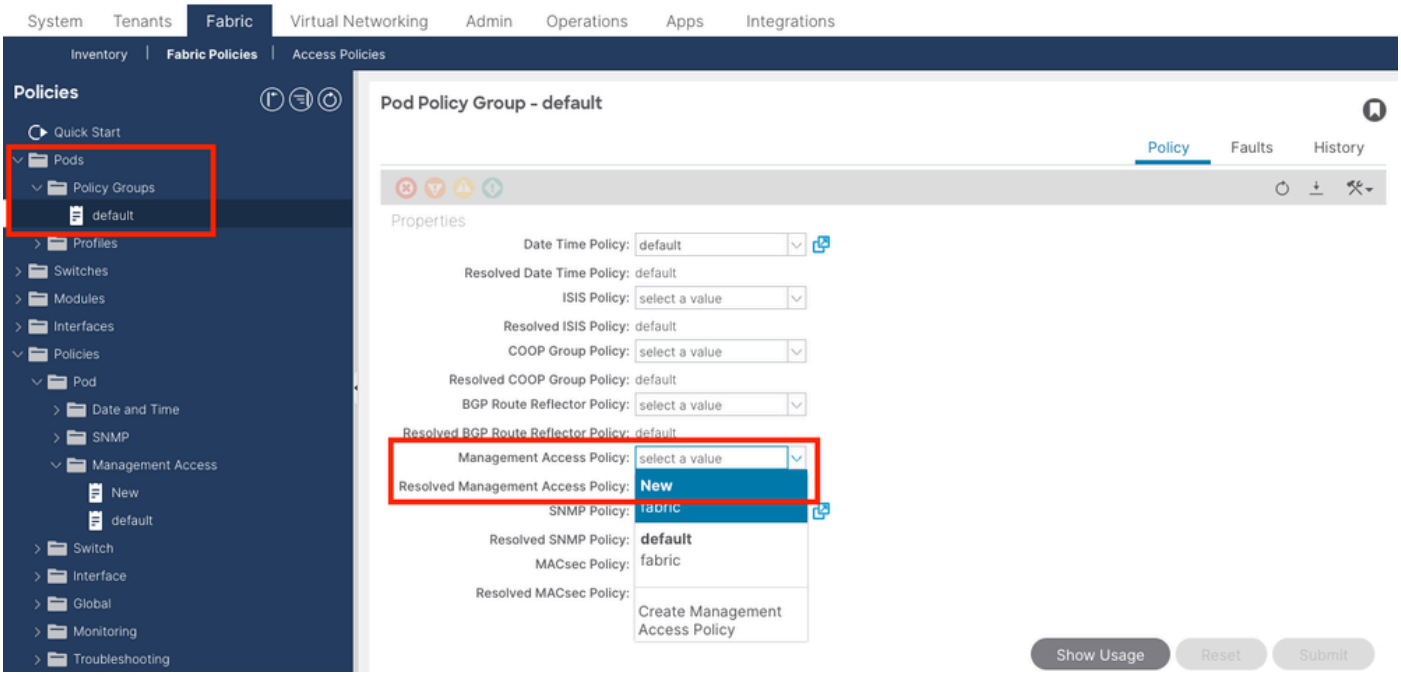
附註：Google Chrome瀏覽器必須驗證憑證的SAN，才能信任此憑證。

在使用自簽名證書的APIC中，證書過期警告可能在極少數情況下出現。

在Keyring中查詢證書，使用證書分析工具來分析證書，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續訂，請建立新的管理訪問策略並應用該策略。





如果未自動續訂金鑰環中的證書，請聯絡Cisco TAC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）。