تكوين شهادة HTTPS لواجهة المستخدم الرسومية (GUI) ل ACI

المحتويات

المقدمة

المتطلبات الأساسية

المتطلبات

المكونات المستخدمة

التكوين

التكوينات

الخطوة 1.استيراد الشهادة الجذر أو الشهادة الوسيطة لهيئة CA

الخطوة 2. إنشاء حلقة مفاتيح

الخطوة 3.إنشاء مفتاح خاص وCSR

الخطوة 4. الحصول على CSR وإرساله إلى مؤسسة CA

الخطوة 5.تحديث شهادة التوقيع على الويب

التحقق من الصحة

استكشاف الأخطاء وإصلاحها

معلومات ذات صلة

المقدمة

يصف هذا المستند تكوين شهادات SSL المخصصة و SSL الموقعة ذاتيا.

المتطلبات الأساسية

المتطلبات

توصي Cisco بأن تكون لديك معرفة بالمواضيع التالية:

- التوقيعات الرقمية والشهادات الرقمية
- عملية إصدار الشهادة من قبل هيئة الشهادات (CA)

المكونات المستخدمة

تستند المعلومات الواردة في هذا المستند إلى إصدارات البرامج والمكونات المادية التالية:

- وحدة التحكم الخاصة بتطبيق سياسة البنية الأساسية (APIC)
- المستعرض
- واجهة برمجة التطبيقات (ACI) التي تعمل بنظام التشغيل 5.2 (8e)

تم إنشاء المعلومات الواردة في هذا المستند من الأجهزة الموجودة في بيئة معملية خاصة. بدأت جميع الأجهزة المُستخدمة في هذا المستند بتكوين ممسوح (افتراضي). إذا كانت

شبكتك قيد التشغيل، فتأكد من فهمك للتأثير المحتمل لأي أمر.

التكوين

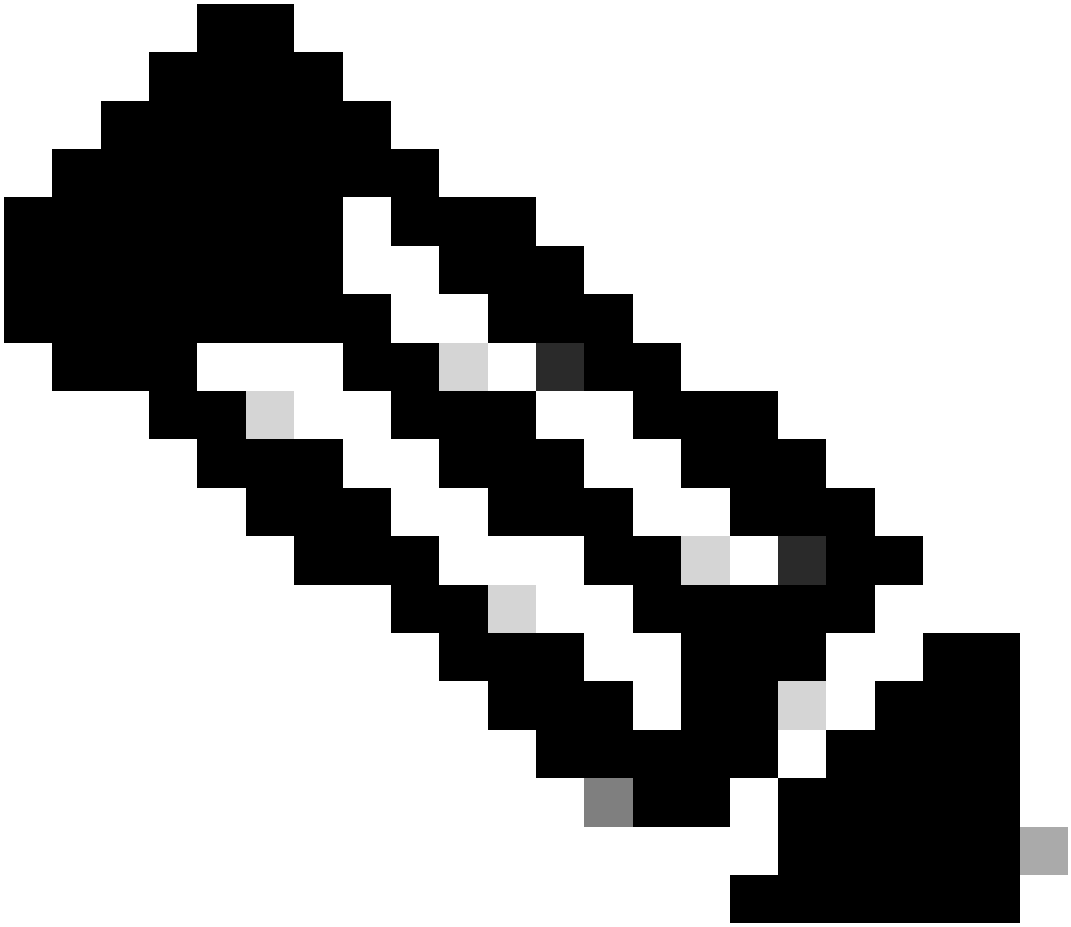
بعد تهيئة الجهاز، يستخدم شهادة التوقيع الذاتي كشهادة SSL ل HTTPS. الشهادة الموقعة ذاتيا صالحة لمدة 1000 يوم.

بشكل افتراضي، يجدد الجهاز تلقائيا ويولد شهادة جديدة موقعة ذاتيا قبل شهر واحد من انتهاء صلاحية الشهادة الموقعة ذاتيا.

التكوينات

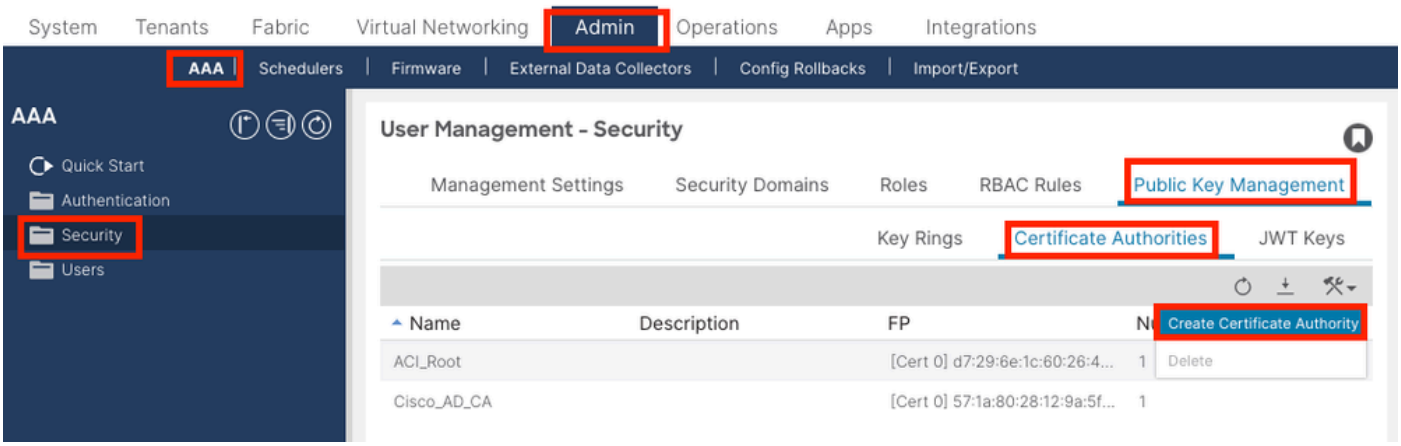
يستخدم الجهاز شهادة موقعة ذاتيا. عند الوصول إلى واجهة المستخدم الرسومية (APIC)، يطلب المستعرض أن الشهادة غير جديرة بالثقة. لحل هذه المشكلة، يستخدم هذا المستند مرجع مصدق ثقة لتوقيع الشهادة.

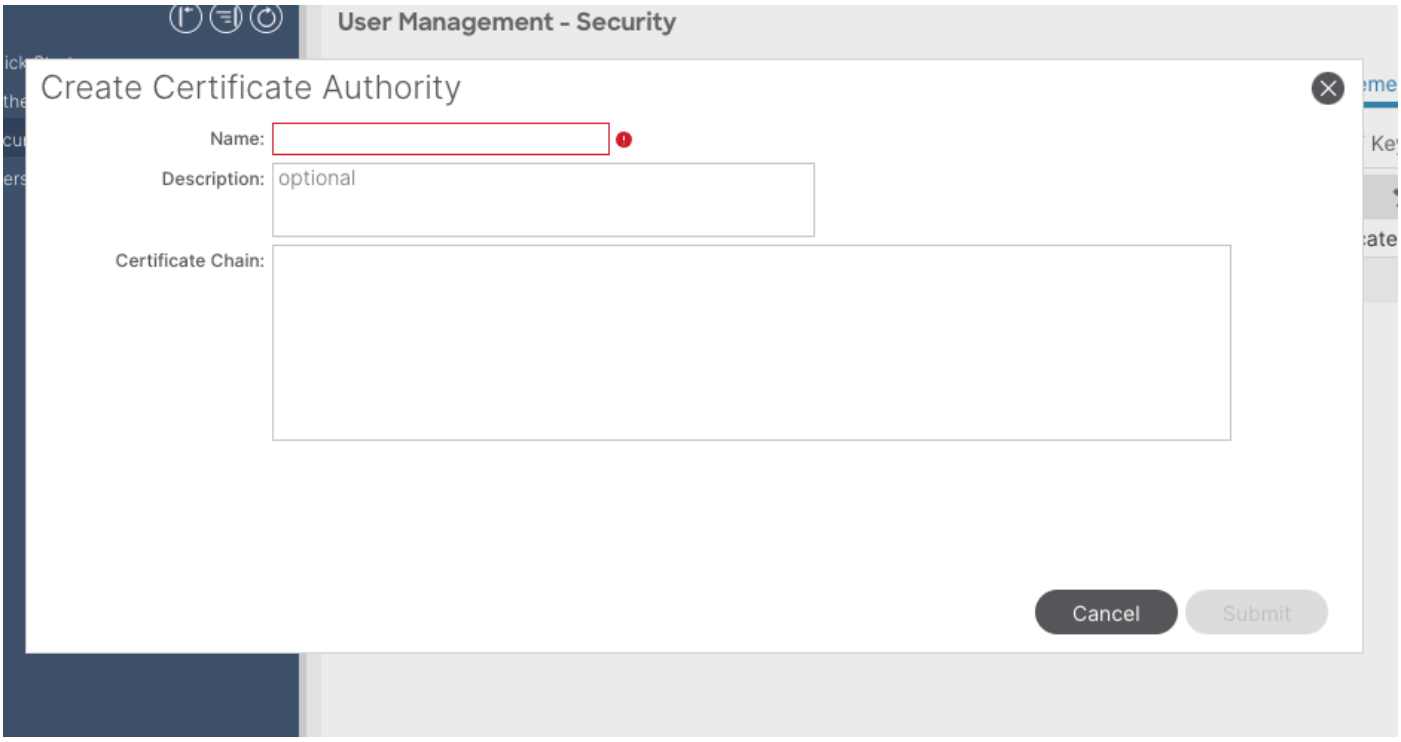
الخطوة 1. إستيراد الشهادة الجذر لهيئة CA أو الشهادة الوسيطة



ملاحظة: إذا كنت تستخدم شهادة جذر المرجع المصدق للتوقيع مباشرة، يمكنك إستيراد شهادة جذر المرجع المصدق فقط. ولكن إذا كنت تستخدم شهادة متوسطة للتوقيع، يجب أن تقوم باستيراد سلسلة الشهادات الكاملة، أي: الشهادة الجذر والشهادات الوسيطة الأقل ثقة.

في شريط القائمة، انتقل إلىAdmin > AAA > Security > Public Key Management > Certificate Authorities.





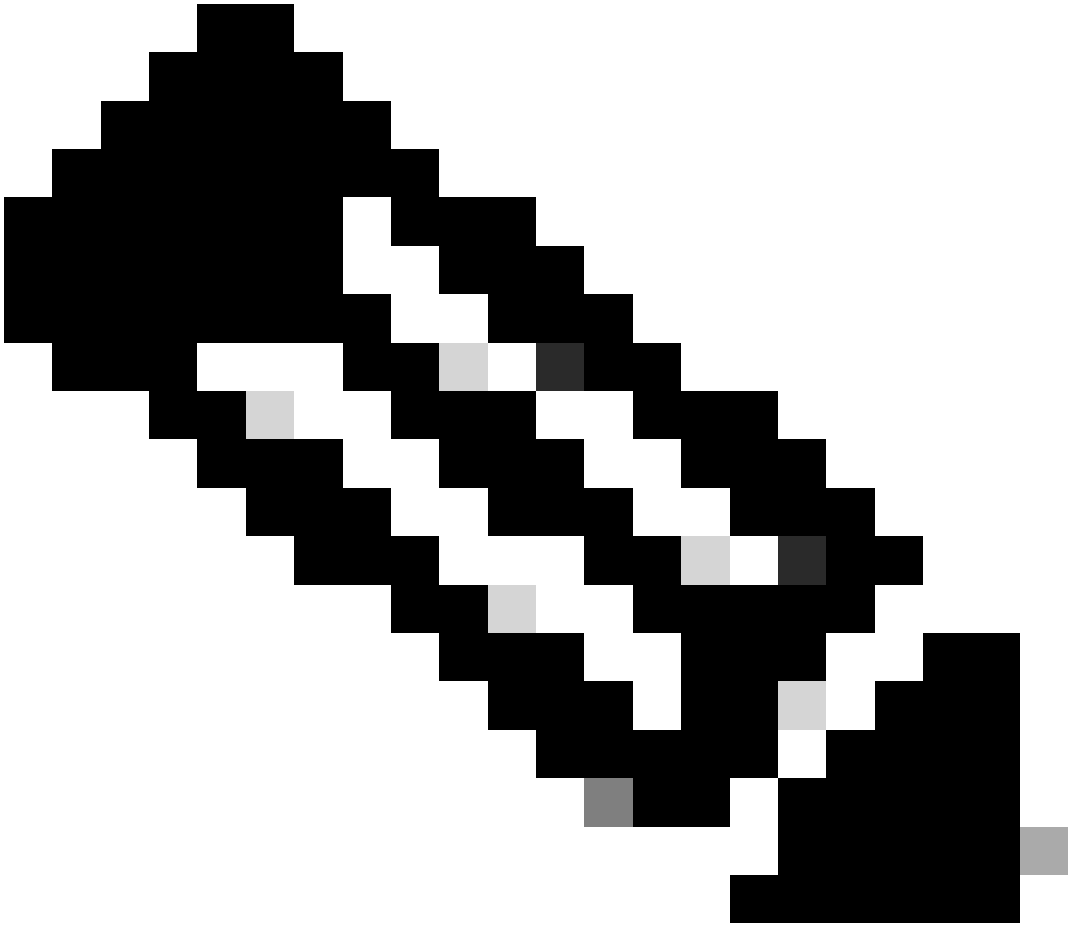
الاسم: مطلوب.

صياغة المحتوى وفقا لقواعد التسمية الخاصة بك. يمكن أن يحتوي_، لكنه لا يمكن أن يحتوي على حروف إنجليزية خاصة، مثل:
, . ; ' " : | + * / = ` ~ ! @ # $ % ^ & ( ) ورموز الفضاء.

الوصف: إختياري.

سلسلة الشهادات: مطلوب.

قم بتعبئة شهادة جذر CA الموثوق بها والشهادة الوسيطة CA.



ملاحظة: يجب أن تتوافق كل شهادة مع تنسيق ثابت.

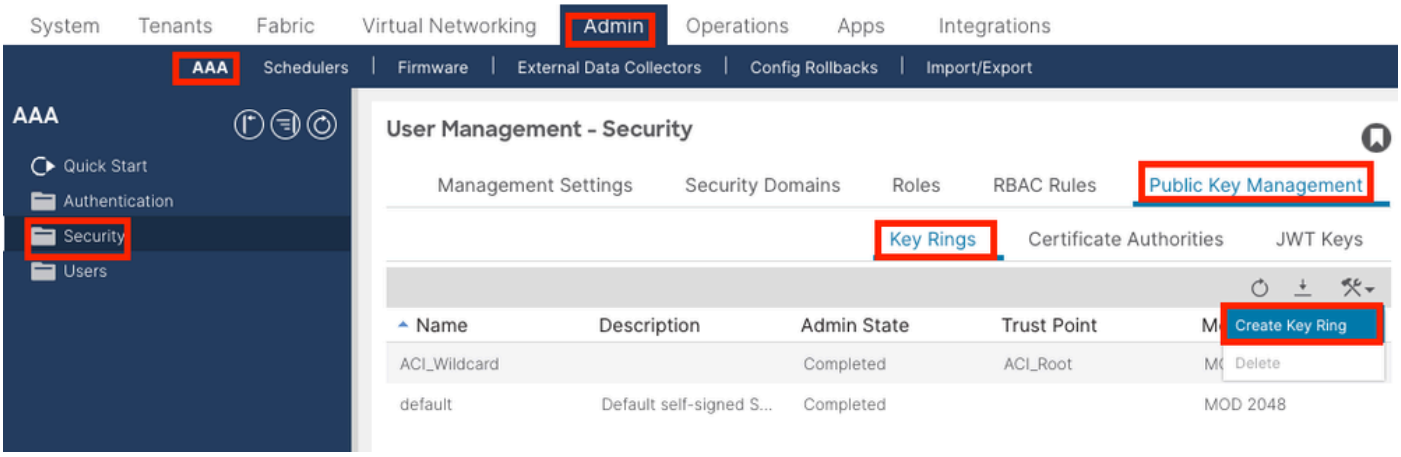
-----BEGIN CERTIFICATE----- INTER-CA-2 CERTIFICATE CONTENT HERE -----END CERTIFICATE----- -----BEGIN CERTIFICATE----- INTER-CA-1 CERTIFICATE CONTENT HERE -----END CERTIFICATE----- -----BEGIN CERTIFICATE----- ROOT-CA CERTIFICATE CONTENT HERE -----END CERTIFICATE-----

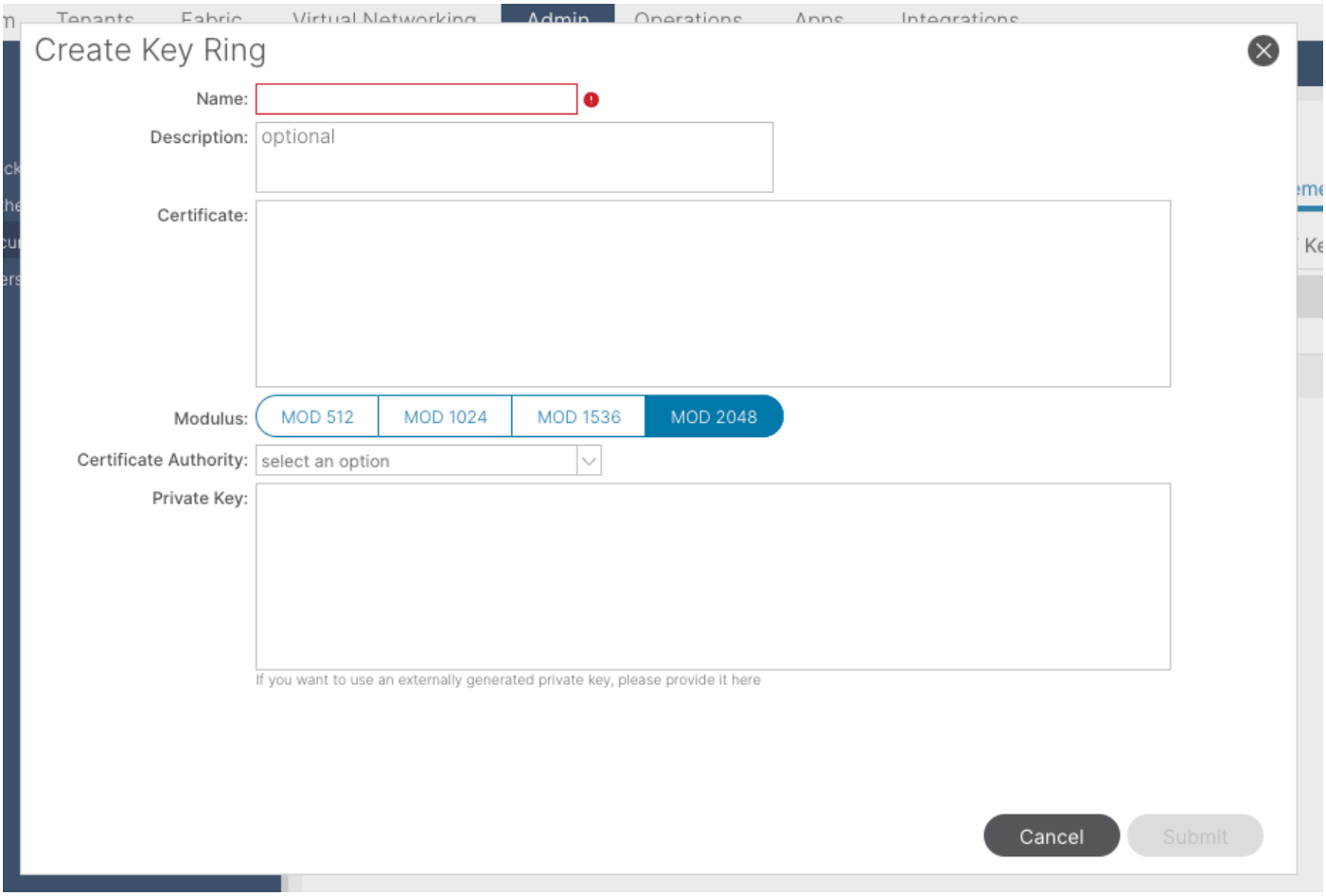
---

انقر فوق الزر إرسال.

الخطوة 2. إنشاء حلقة مفاتيح

في شريط القائمة، انتقل إلىAdmin > AAA > Security > Public Key Management > Key Rings.





الاسم:مطلوب (أدخل اسما).

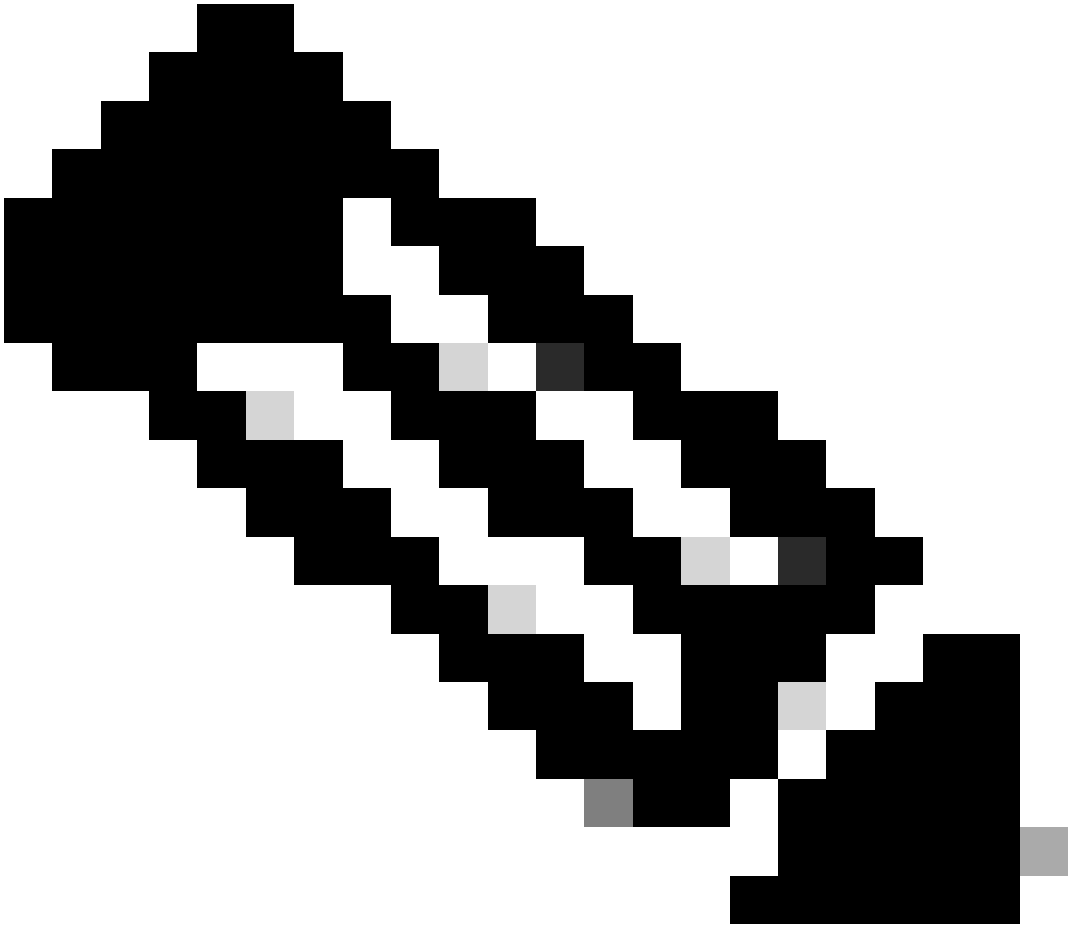
الترخيص:ال تضيف أي محتوى إذا قمت بإنشاء طلب توقيع شهادة (CSR) باستخدام Cisco APIC من خلال حلقة المفاتيح. بدلا من ذلك، قم بإضافة محتوى الشهادة الموقعة إذا كان لديك بالفعل محتوى موقع من قبل CA من الخطوات السابقة عن طريق إنشاء مفتاح خاص و CSR خارج Cisco APIC.

المعامل: مطلوب (انقر زر الخيار للحصول على قوة المفتاح المطلوبة).

مرجع الشهادة: مطلوب. من القائمة المنسدلة، أختر مرجع الشهادة الذي أنشأته مسبقا.

مفتاح خاص:ال تقم بإضافة أي محتوى إذا قمت بإنشاء CSR باستخدام Cisco APICمن خلال حلقة المفاتيح. بدلا من ذلك، أضف المفتاح الخاص المستخدم لإنشاء CSR للشهادة

الموقعة التي أدخلتها.

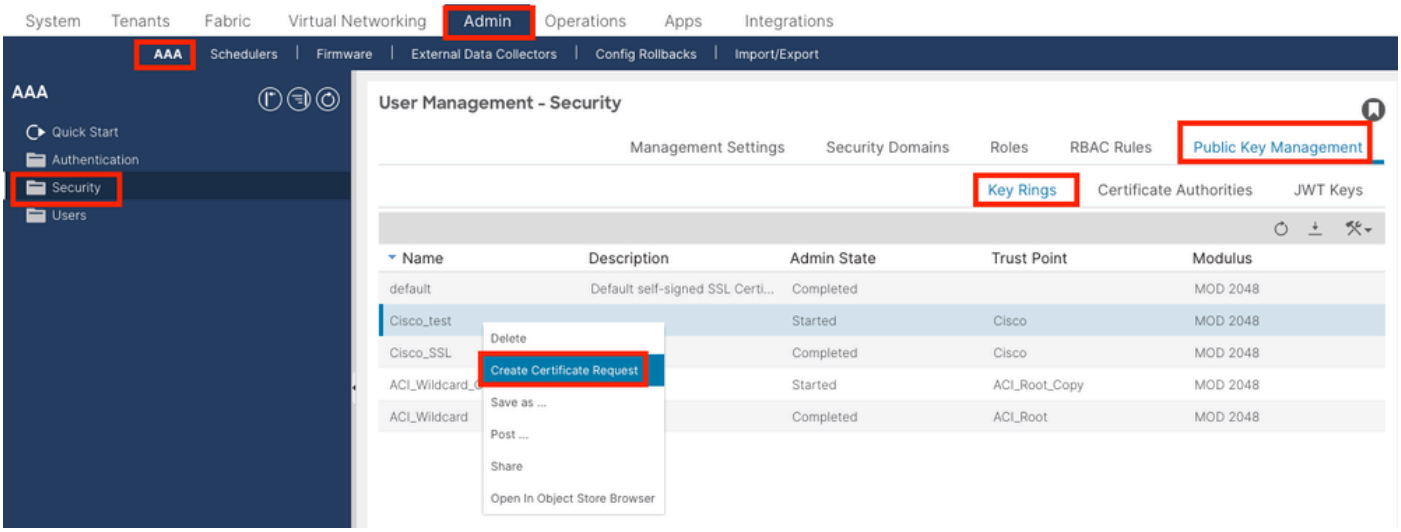


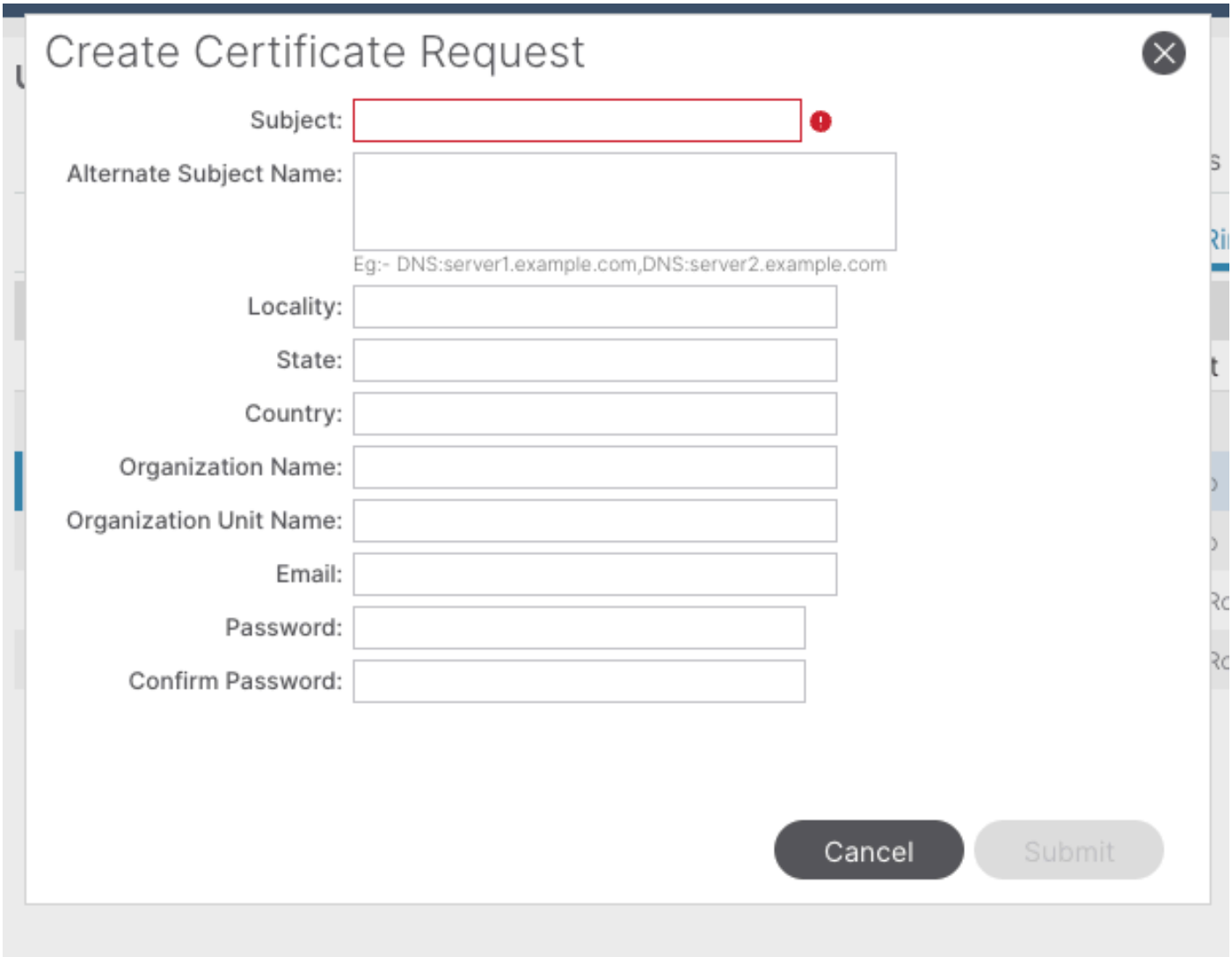
ملاحظة: إذا كنت لا تريد إستخدام المفتاح الخاص المنشأ من قبل النظام و CSR واستخدام مفتاح خاص وشهادة مخصصة، تحتاج فقط إلى تعبئة أربعة عناصر: الاسم والشهادة وسلطة الشهادة والمفتاح الخاص. بعد الإرسال، يجب عليك فقط تنفيذ الخطوة الأخيرة، الخطوة 5.

انقر فوق الزر إرسال.

الخطوة 3. إنشاء مفتاح خاص و CSR

في شريط القائمة، انتقل إلىAdmin > AAA > Security > Public Key Management > Key Rings.



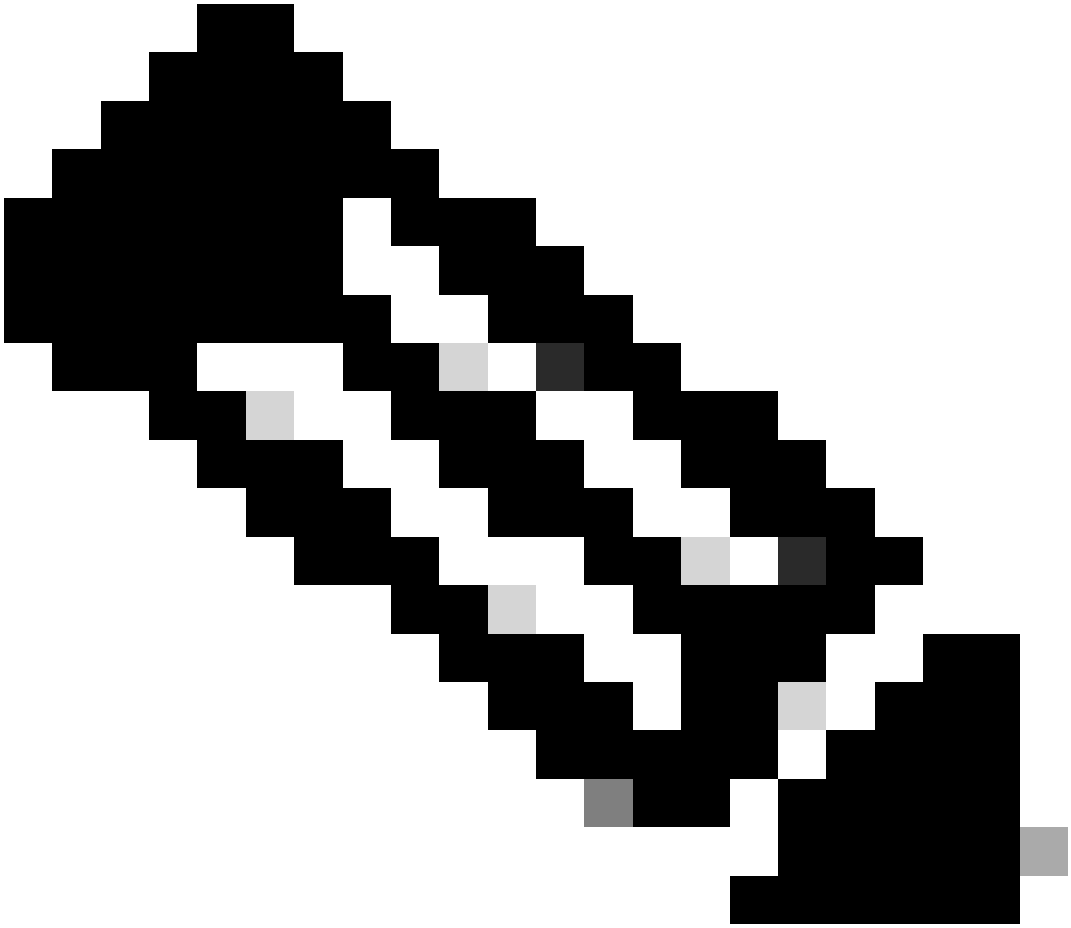


الموضوع: مطلوب. أدخل الاسم الشائع (CN) ل CSR.

يمكنك إدخال اسم المجال المؤهل بالكامل (FQDN) من Cisco APICs باستخدام حرف بدل، ولكن في شهادة حديثة، يوصى بشكل عام بإدخال اسم يمكن تعريفه للشهادة وإدخال FQDN لجميع Cisco APICs في حقل اسم الموضوع البديل (المعروف أيضا باسم SAN - اسم الموضوع البديل) لأن العديد من المستعرضات الحديثة تتوقع FQDN في حقل SAN.

اسم الموضوع البديل: مطلوب. أدخل FQDN لكافة APICs من Cisco، مثلDNS:apic1.example.com,DNS:apic2.example.com,DNS:apic3.example.comأوDNS:*example.com.

بدلا من ذلك، إذا كنت تريد أن تتطابق شبكة التخزين (SAN) مع عنوان IP، فأدخل عنواني IP الخاصة بواجهات برمجة التطبيقات (APIC) Cisco مع التنسيق: IP:192.168.1.1.



ملاحظة: يمكنك إستخدام أسماء خادم اسم المجال (DNS) أو عنواني IPv4 أو مزيج من الاثنين في هذا الحقل. عنواني IPv6 غير مدعومة.

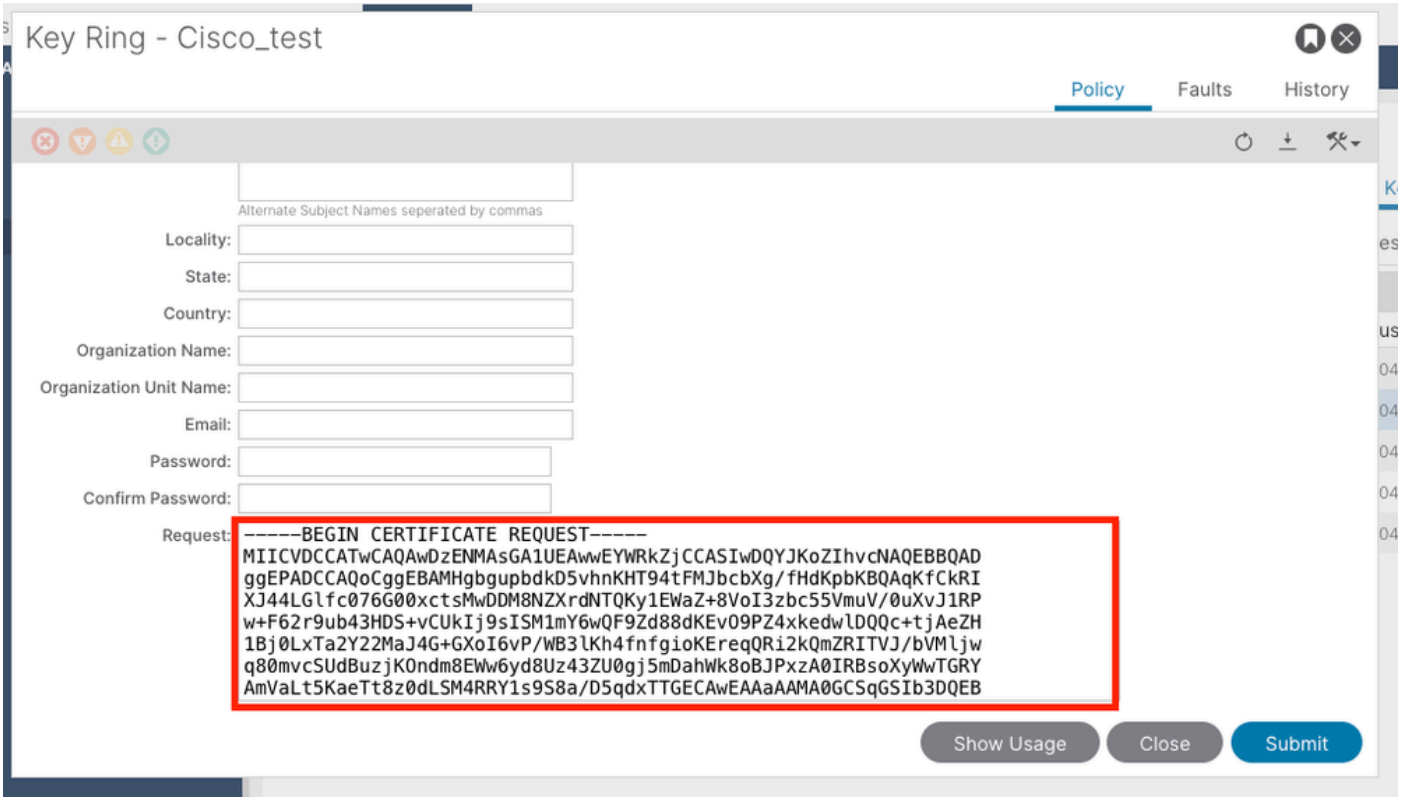
املأ الحقول المتبقية طبقا لمتطلبات مؤسسة CA التي تقوم بتطبيقها لإصدار الشهادة.

انقر فوق الزر إرسال.

الخطوة 4. الحصول على CSR وإرساله إلى مؤسسة CA

في شريط القائمة، انتقل إلىAdmin > AAA > Security > Public Key Management > Key Rings.

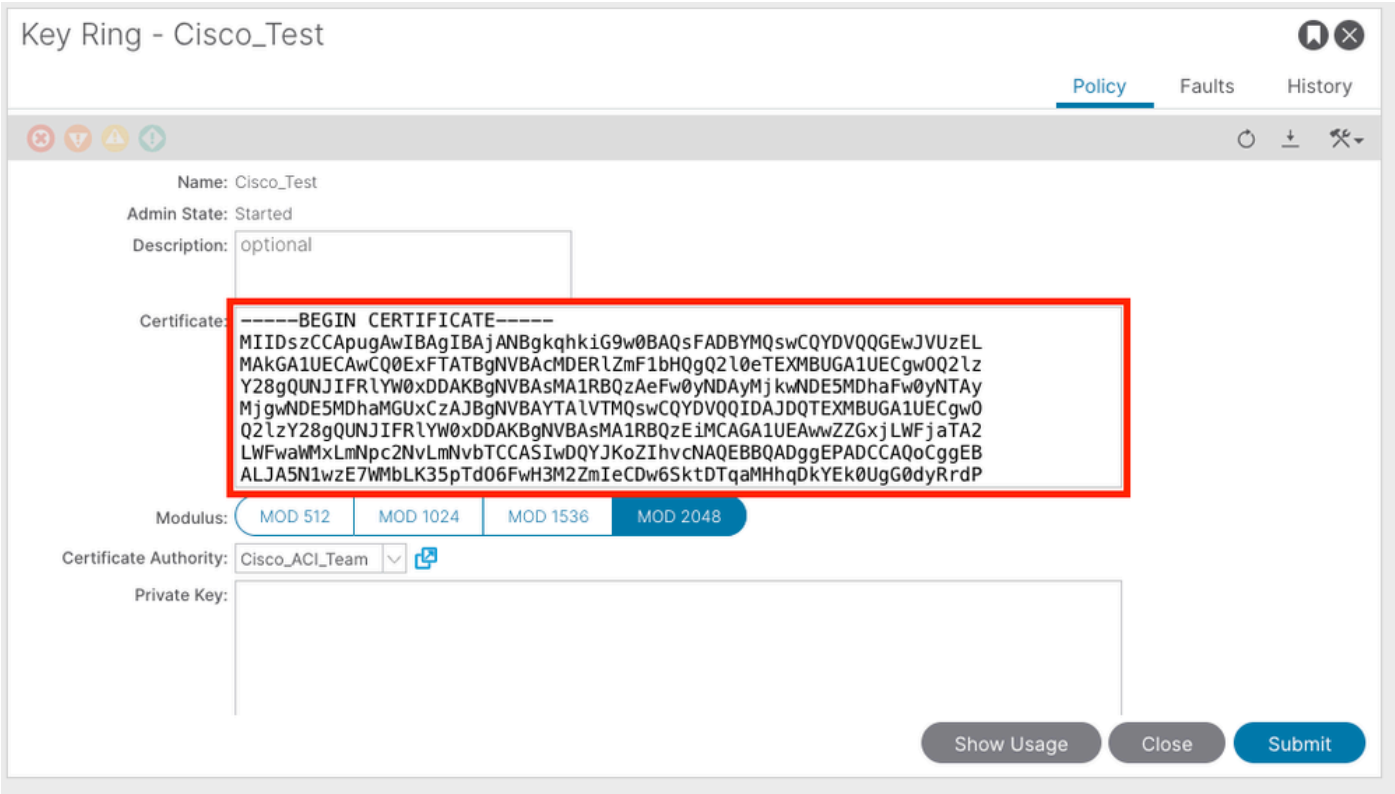
انقر نقرا مزدوجا فوق اسم حلقة المفاتيح والعثور على خيار الطلب. المحتوى الموجود في الطلب هو CSR.

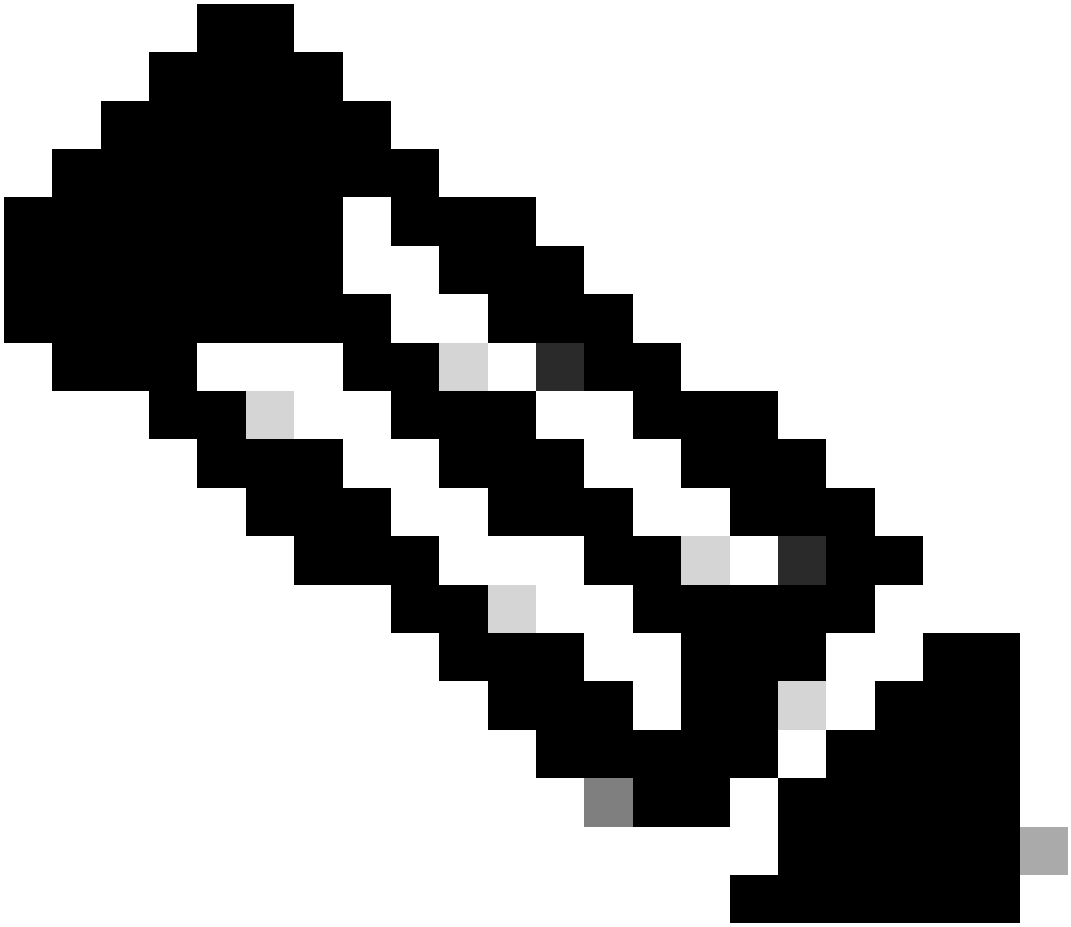


انسخ كافة محتويات الطلب وأرسله إلى المرجع المصدق.

يستخدم CA مفتاحه الخاص لإجراء التحقق من التوقيع على CSR الخاص بك.

وبعد الحصول على الشهادة الموقعة من المرجع المصدق، ينسخ الشهادة إلى الشهادة.





ملاحظة: يجب أن تتوافق كل شهادة مع تنسيق ثابت.

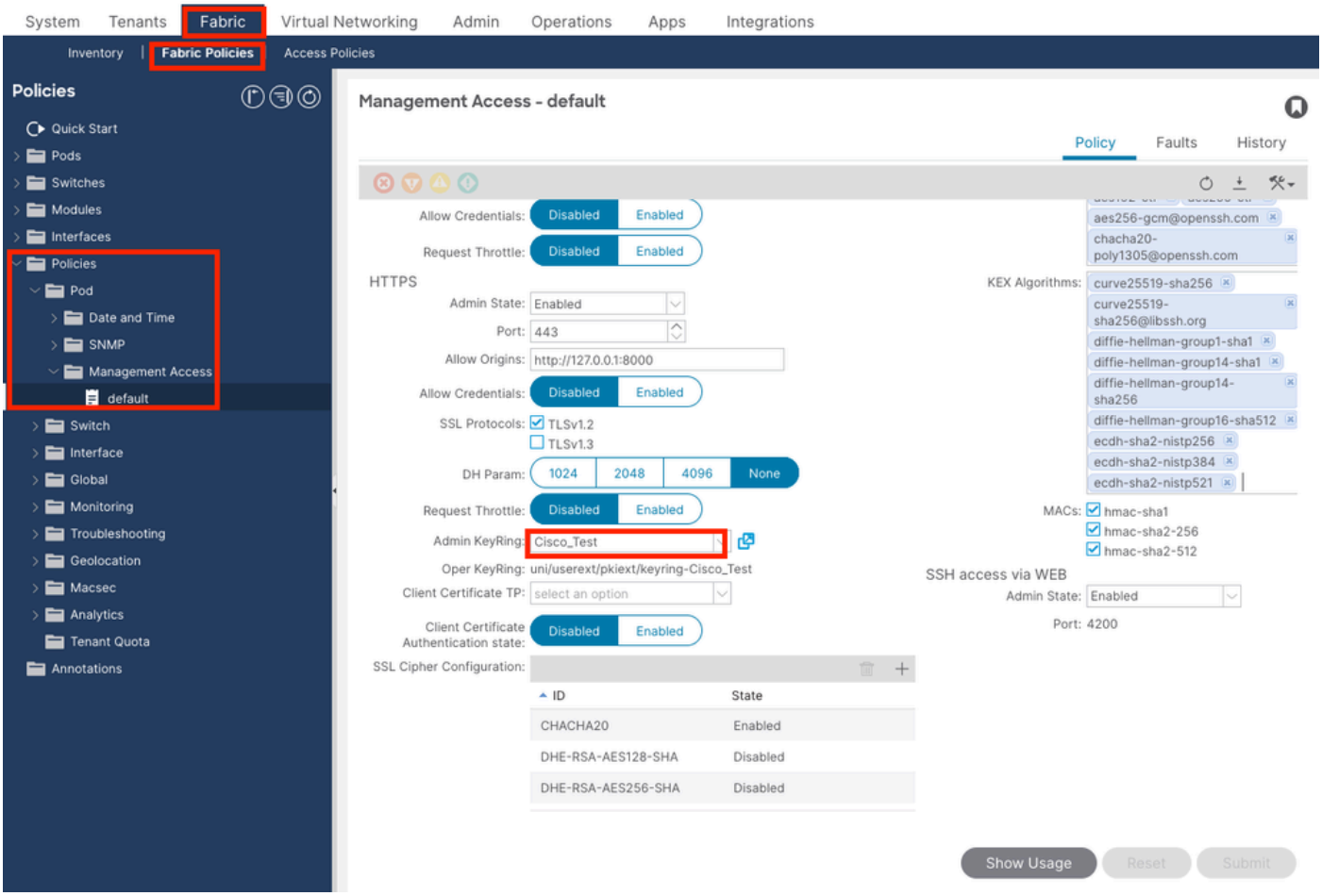
-----BEGIN CERTIFICATE----- CERTIFICATE CONTENT HERE -----END CERTIFICATE-----

---

انقر فوق الزر إرسال.

الخطوة 5. تحديث شهادة التوقيع على الويب

في شريط القائمة، انتقل إلىFabric > Fabric Policies > Policies > Pod > Management Access > Default.



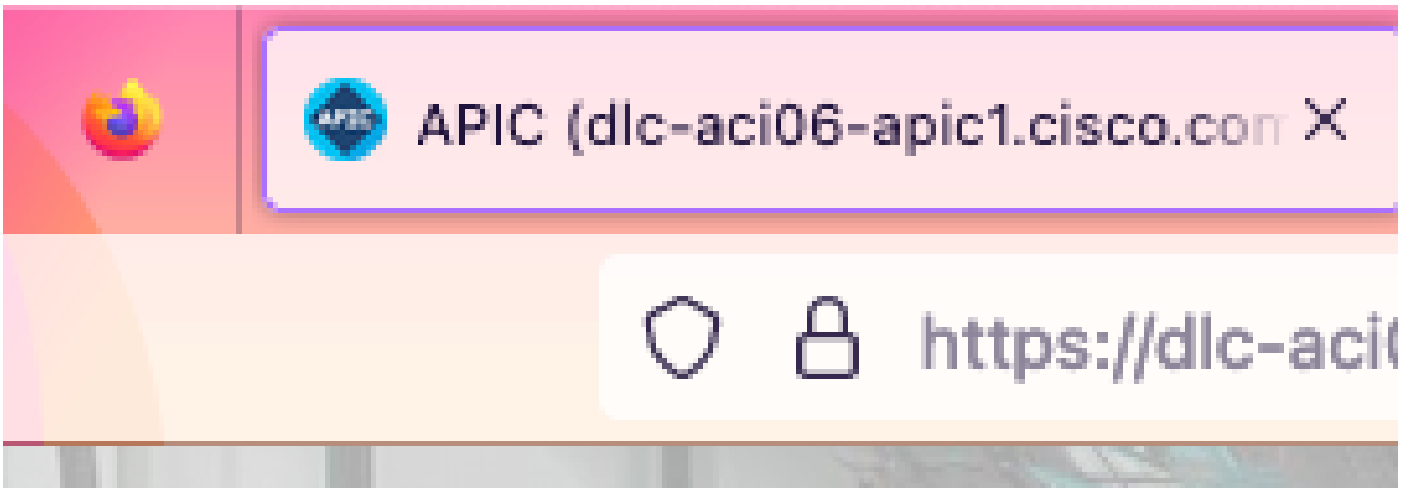
في القائمة المنسدلة Admin KeyRing، أختر KeyRing المطلوب.

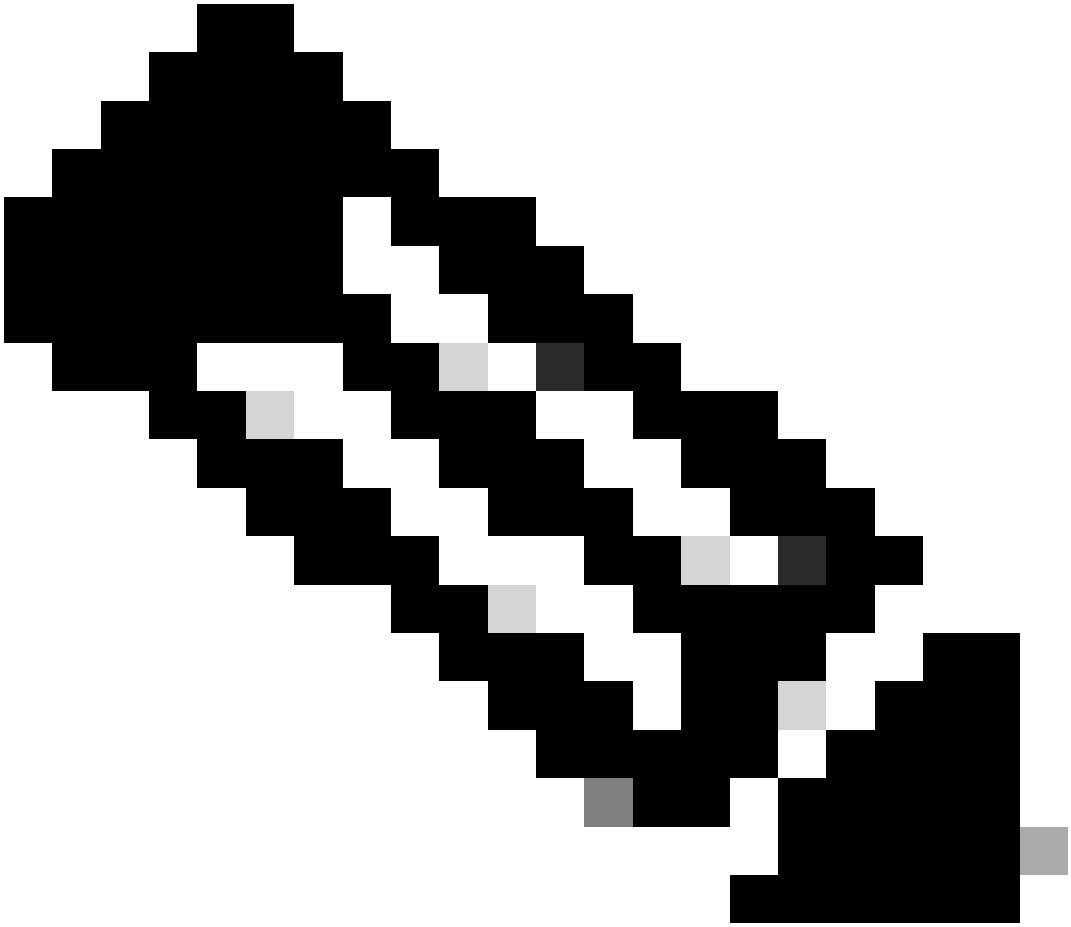
انقر فوق الزر إرسال.

بعد النقر فوق "إرسال"، يحدث خطأ لأسباب تتعلق بالشهادة. تحديث مع الشهادة الجديدة.

التحقق من الصحة

بعد الوصول إلى واجهة المستخدم الرسومية APIC، تستخدم APIC الشهادة الموقعة من CA للاتصال. عرض معلومات الشهادة في المستعرض للتحقق منها.

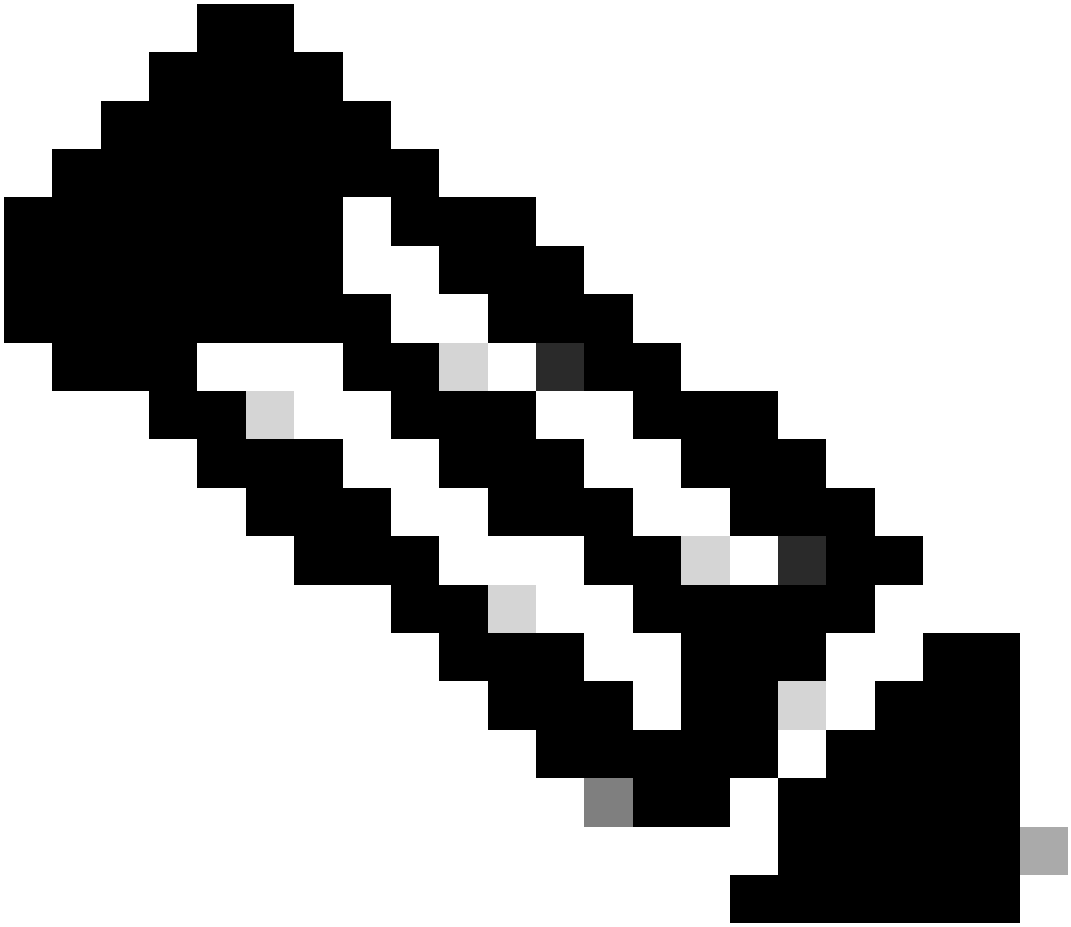




ملاحظة: طرق عرض شهادات HTTPS في مستعرضات مختلفة ليست متطابقة تمامًا. لطرق محددة، ارجع إلى دليل المستخدم الخاص بالمستعرض لديك.

استكشاف الأخطاء وإصلاحها

إذا استمر المستعرض في المطالبة بأن واجهة المستخدم الرسومية (GUI) الخاصة بواجهة برمجة التطبيقات (APIC) غير موثوق بها، فتحقق في المستعرض مما إذا كانت شهادة واجهة المستخدم الرسومية (GUI) متوافقة مع الشهادة المقدمة في حلقة المفاتيح.
يجب أن تثق في شهادة جذر المرجع المصدق التي أصدرت الشهادة على الكمبيوتر أو المستعرض.

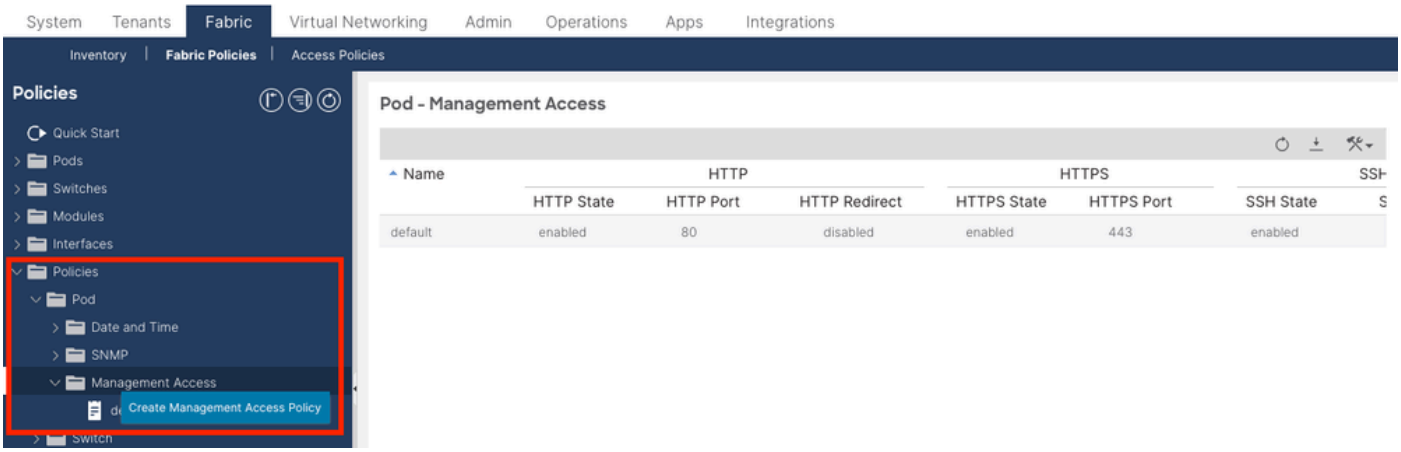


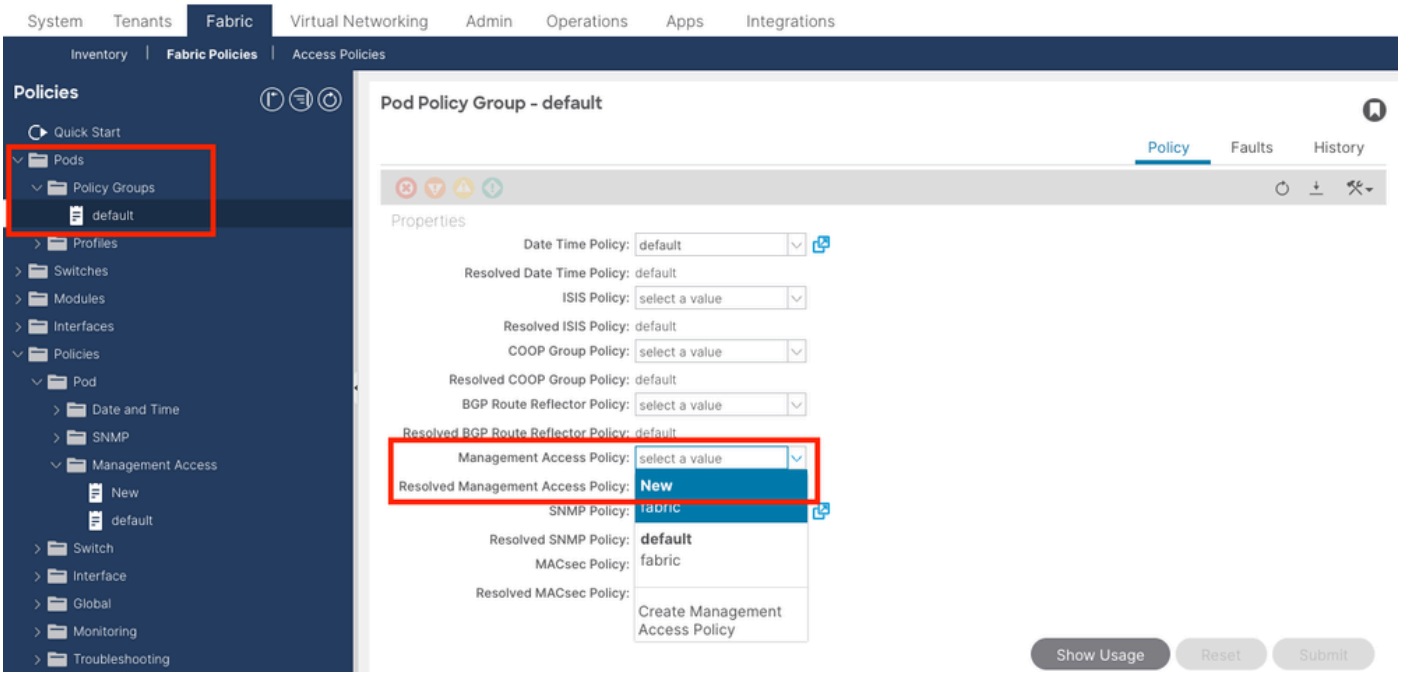
ملاحظة: يجب أن يقوم متصفح Google Chrome بالتحقق من SAN للشهادة للثقة بهذه الشهادة.

في APICs التي تستخدم شهادات موقعة ذاتيا، يمكن أن تظهر تحذيرات انتهاء صلاحية الشهادة في حالات نادرة.

ابحث عن الشهادة في KeyRing، واستخدم أداة تحليل الشهادة لتحليل الشهادة، وقارنها مع الشهادة المستخدمة في المتصفح.

في حالة تجديد الشهادة الموجودة في حلقة المفاتيح، قم بإنشاء نهج وصول جديد للإدارة وتطبيقه.





إن لم يتم تجديد الشهادة في KeyRing تلقائيا، اتصل ب cisco TAC للحصول على مزيد من المساعدة.

معلومات ذات صلة

- دليل تكوين أمان واجهة برمجة التطبيقات من Cisco، الإصدار 5.2(x)
- الدعم الفني والتنزيلات من Cisco

حول هذه الترجمة

ترجمت Cisco هذا المستند باستخدام مجموعة من التقنيات الآلية والبشرية لتقديم محتوى دعم للمستخدمين في جميع أنحاء العالم بلغتهم الخاصة. يُرجى ملاحظة أن أفضل ترجمة آلية لن تكون دقيقة كما هو الحال مع الترجمة الاحترافية التي يقدمها مترجم محترف. تخلي Cisco Systems مسئوليتها عن دقة هذه الترجمات وتُوصي بالرجوع دائماً إلى المستند الإنجليزي الأصلي (الرابط متوفر).