تكوين مصادقة شهادة العميل الآمنة على FTD المدارة من قبل FMC

المحتويات

المقدمة

المتطلبات الأساسية

المتطلبات

المكونات المستخدمة

التكوين

الرسم التخطيطي للشبكة

التكوينات

إنشاء/استيراد شهادة تستخدم لمصادقة الخادم

إضافة شهادة مرجع مصدق ثقة/داخلية

تكوين تجمع العناوين لمستخدمي VPN

تحميل صور العميل الآمنة

إنشاء ملف تعريف XML وتحميله

تكوين VPN للوصول عن بعد

التحقق من الصحة

استكشاف الأخطاء وإصلاحها

المقدمة

يصف هذا المستند تكوين شبكة VPN للوصول عن بعد على الدفاع عن تهديد FirePOWER (FTD) المدار من قبل مركز إدارة FirePOWER (FMC) بمصادقة الشهادة.

المتطلبات الأساسية

المتطلبات

توصي Cisco بأن تكون لديك معرفة بالمواضيع التالية:

- تسجيل الشهادة اليدوي وأساسيات طبقة مآخذ التوصيل الآمنة (SSL)
- FMC
- معرفة المصادقة الأساسية لشبكة VPN للوصول عن بعد
- المرجع المصدق التابع لجهة خارجية (CA) مثل Entrust و Geotrust و GoDaddy و Thawte و VeriSign

المكونات المستخدمة

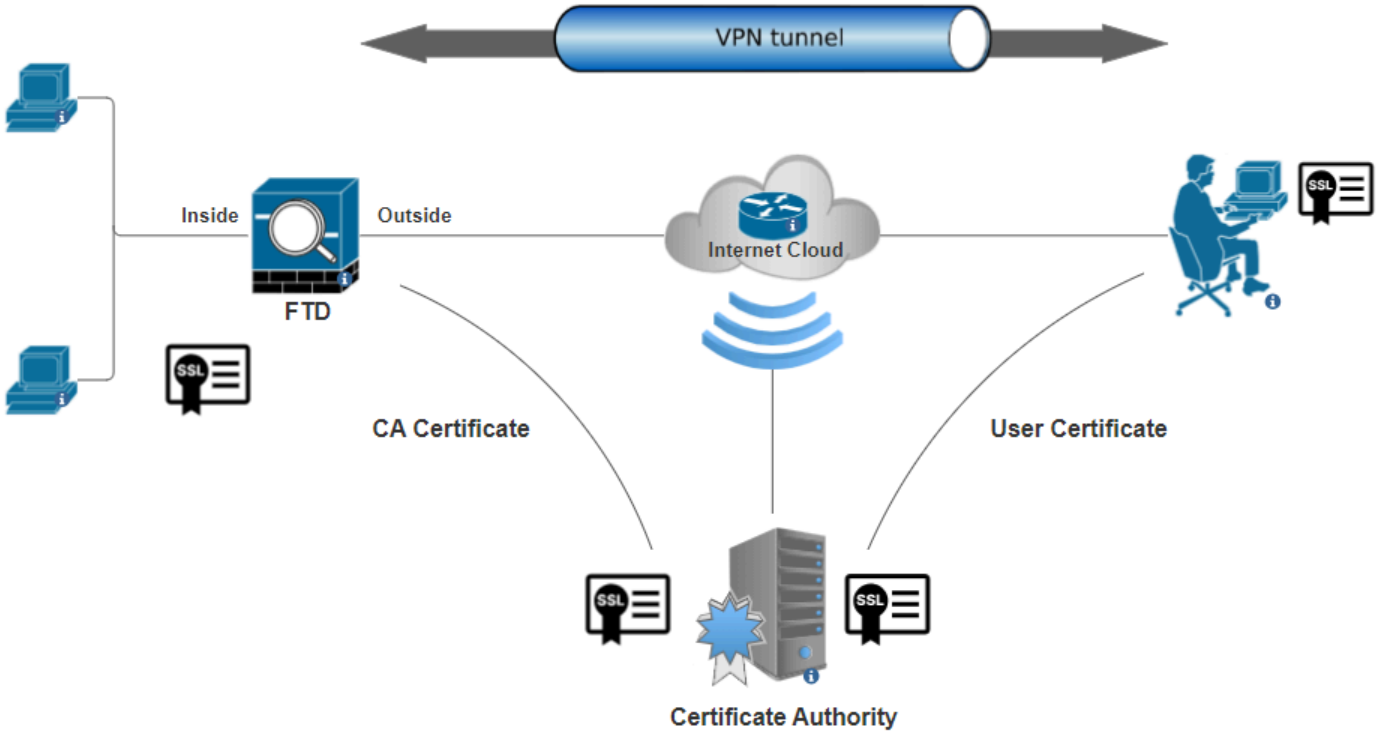
تستند المعلومات الواردة في هذا المستند إلى إصدارات البرامج التالية:

- الدفاع الآمن ضد تهديد FirePOWER، الإصدار 7.4.1
- FMC، الإصدار 7.4.1
- Secure Client الإصدار 5.0.05040
- Microsoft Windows Server 2019 كخادم CA

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

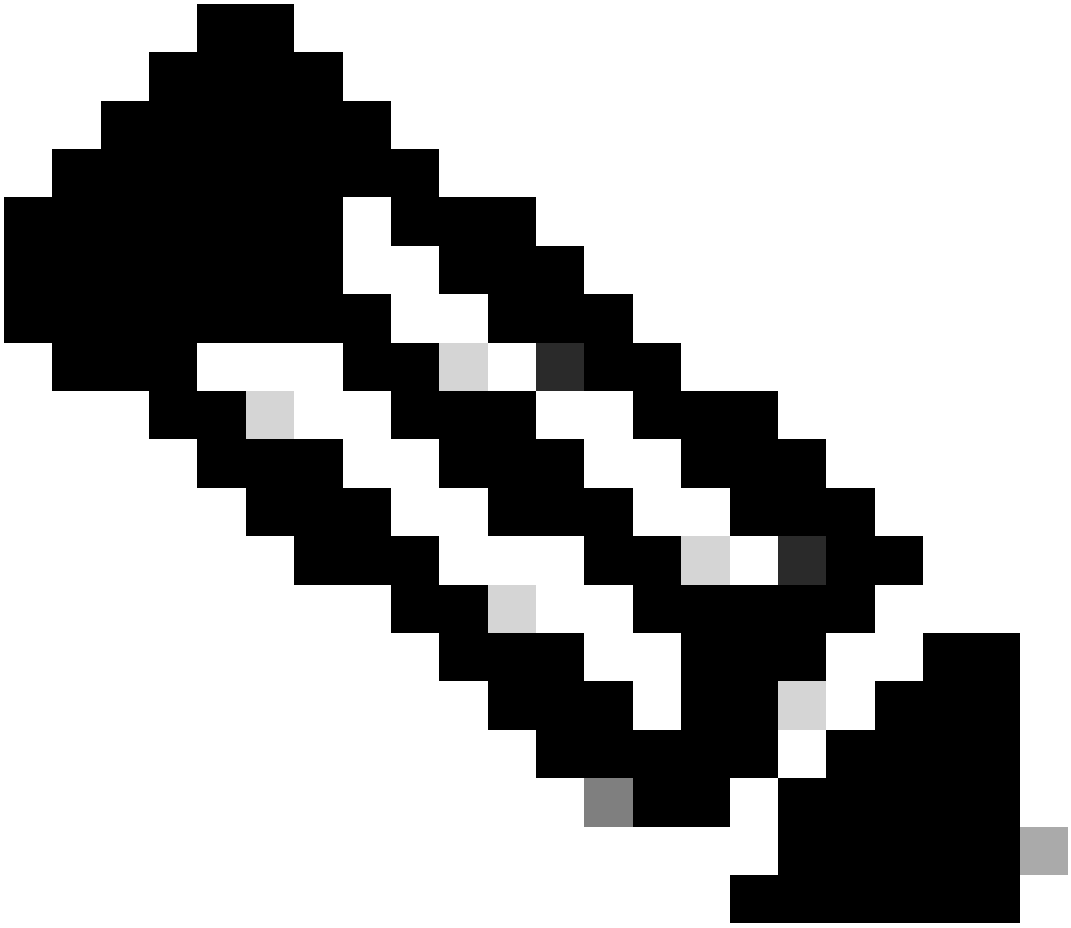
الرسم التخطيطي للشبكة



الرسم التخطيطي للشبكة

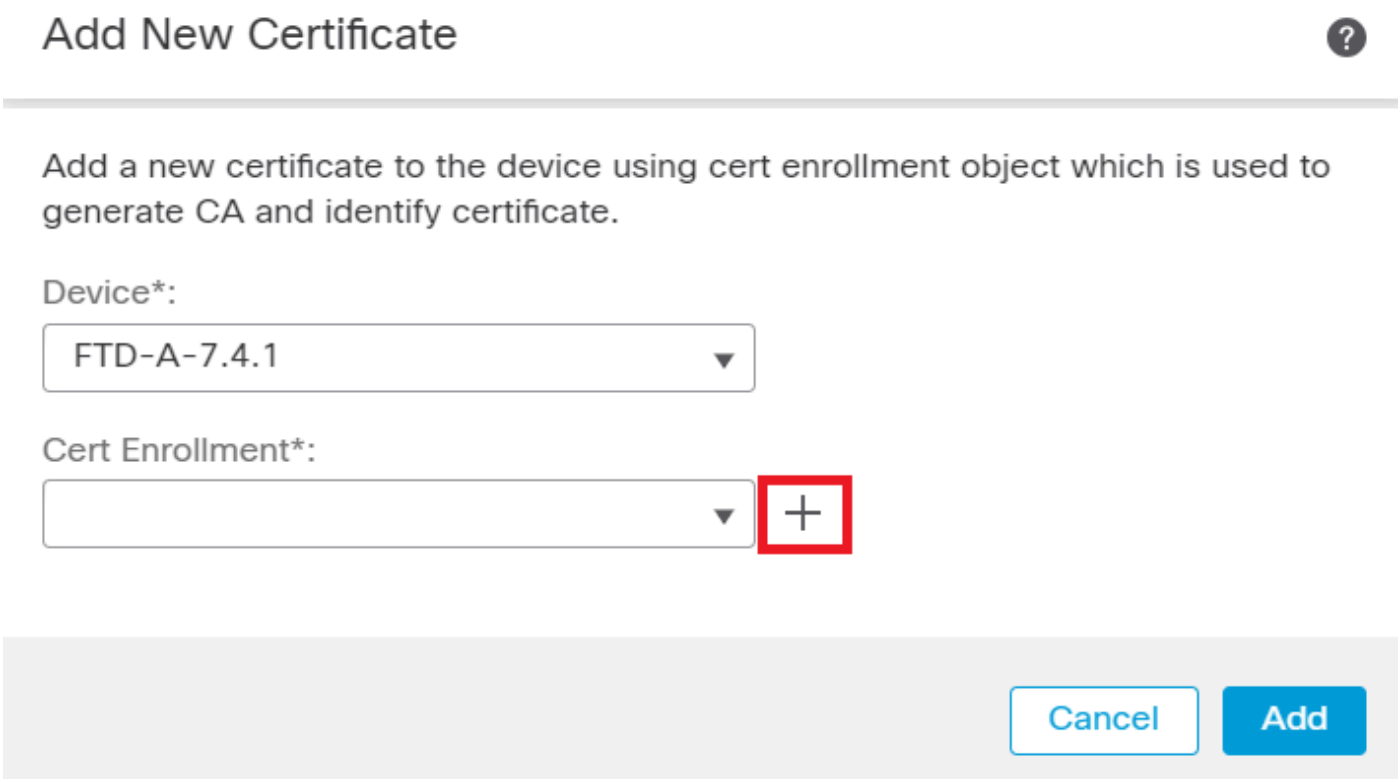
التكوينات

إنشاء/إستيراد شهادة تستخدم لمصادقة الخادم



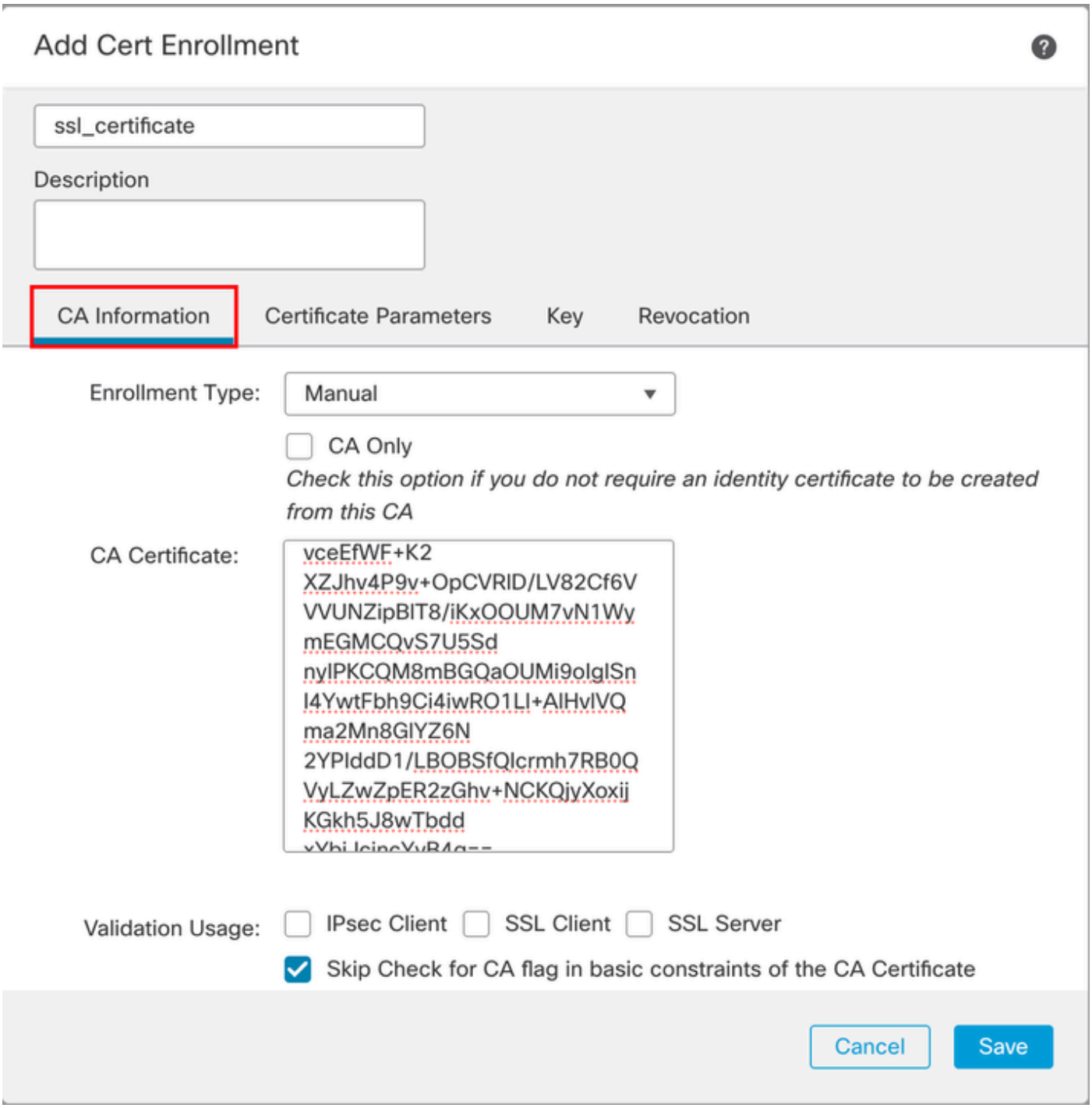
ملاحظة: في FMC، هناك حاجة إلى شهادة المرجع المصدق (CA) قبل أن تتمكن من إنشاء CSR. إذا تم إنشاء CSR من مصدر خارجي (OpenSSL أو جهة خارجية)، فإن الأسلوب اليدوي يفشل ويجب إستخدام تنسيق شهادة PKCS12.

الخطوة 1. انتقل إلىDevices > CertificatesوانقرAdd. أختر الجهاز وانقر فوق علامة الجمع (+) ضمن تسجيل الاقتران.



إضافة تسجيل الشهادة

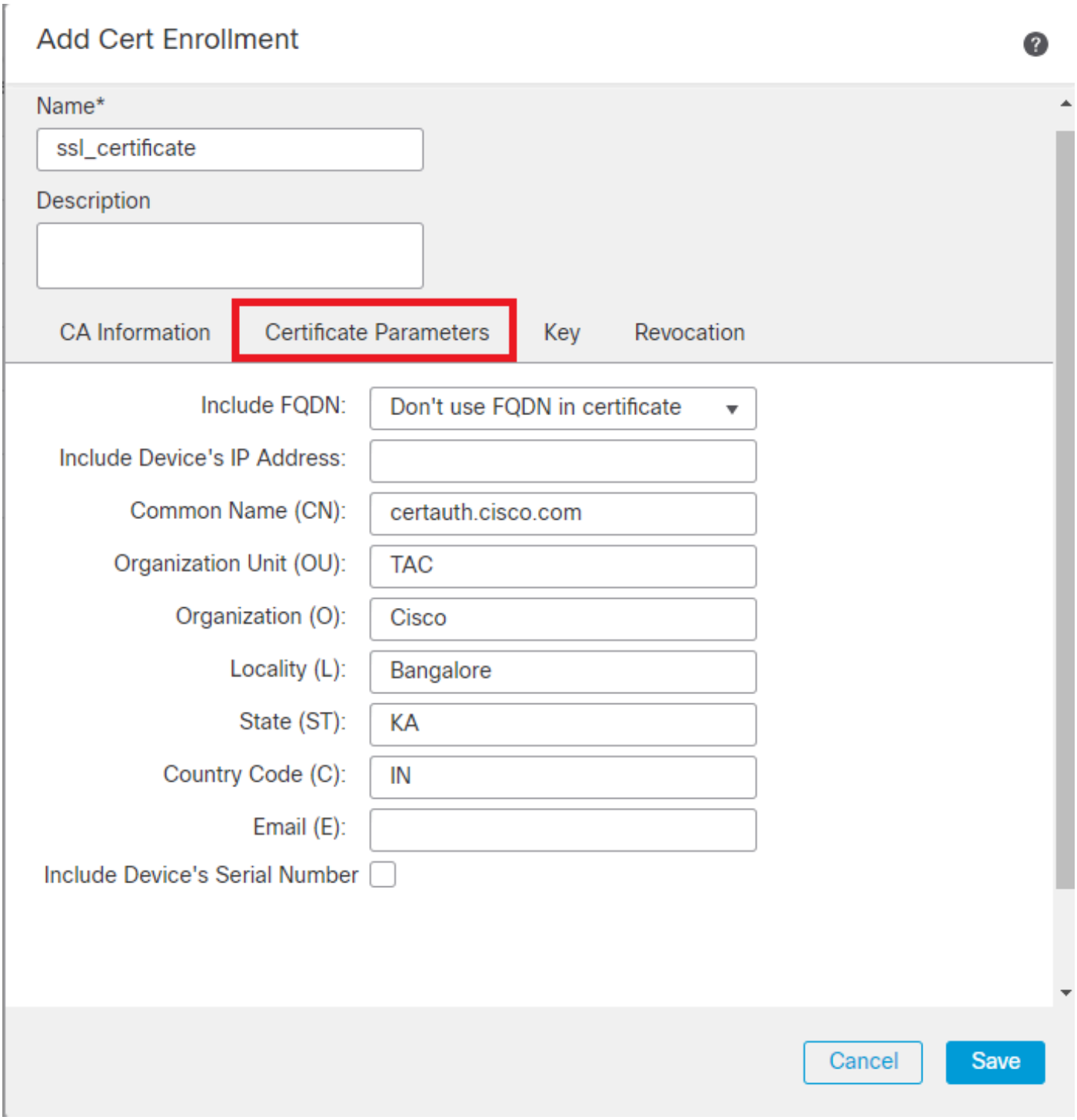
الخطوة 2. تحتCA Information، أختر نوع التسجيل كManualوالصق شهادة CA المستخدمة لتوقيع CSR.



إضافة معلومات المرجع المصدق

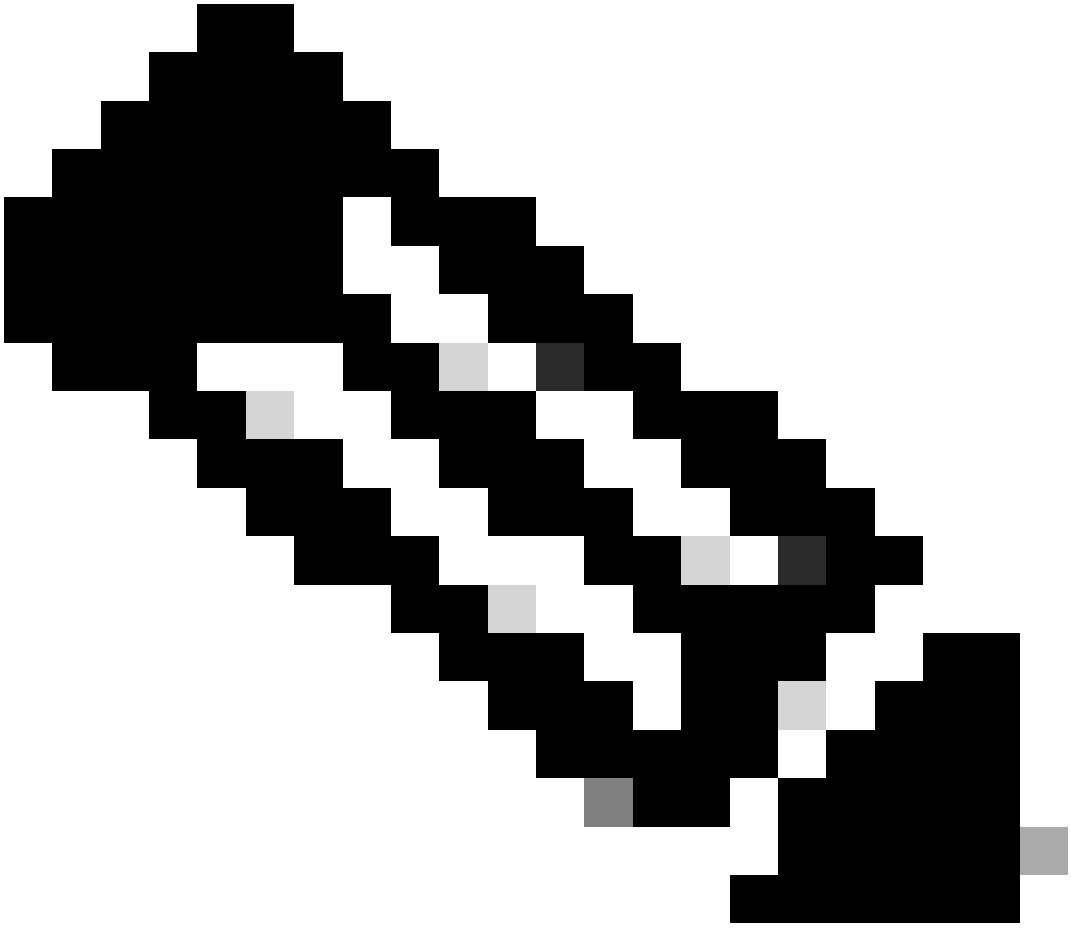
الخطوة 3. أختر Skip Check for CA flag in basic constraints of the CA Certificate as shown in the earlier image.

الخطوة 4. تحتCertificate Parameters، املأ تفاصيل اسم الموضوع.

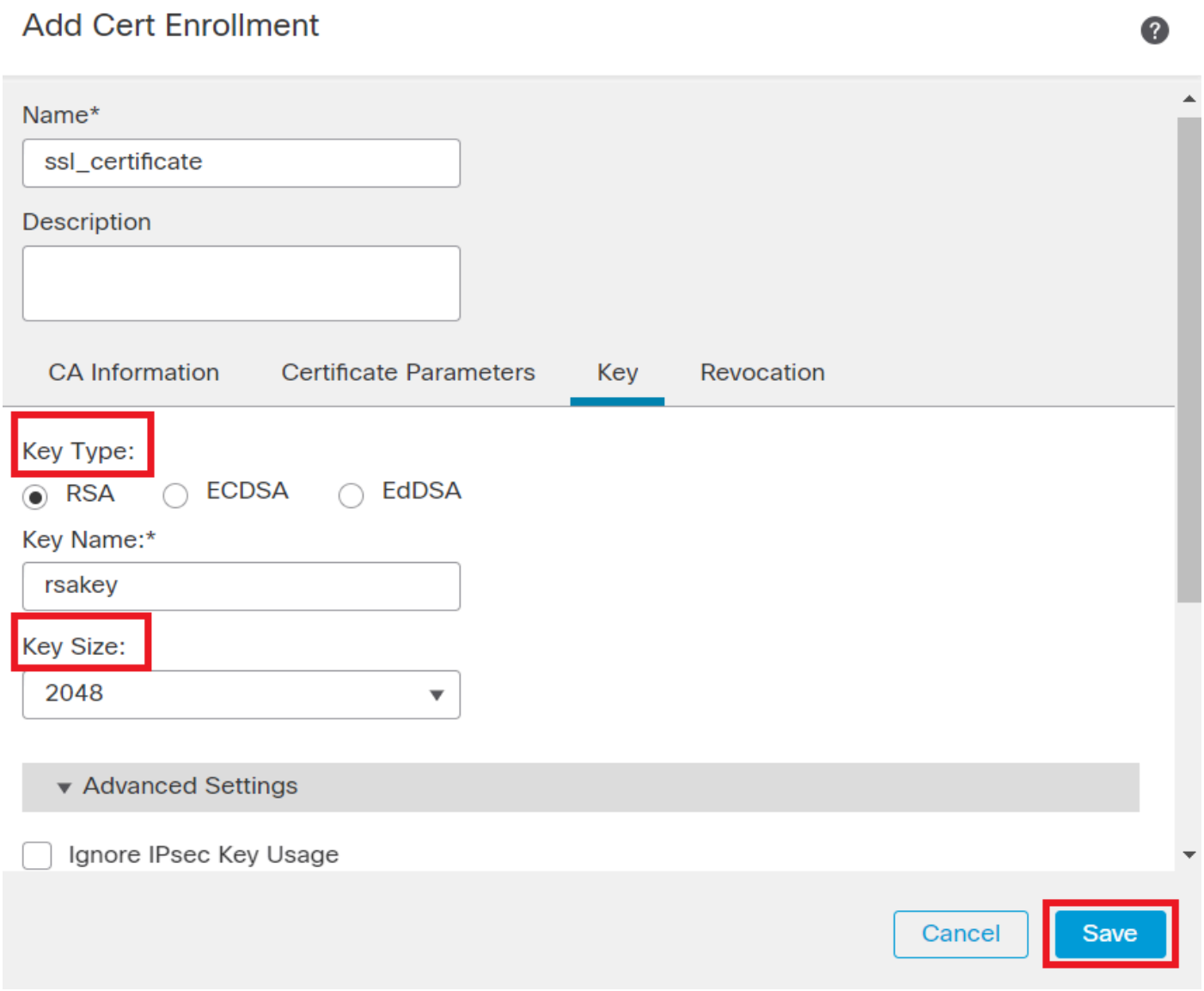


إضافة معلمات شهادة

الخطوة 5. تحتKeyأختر نوع المفتاح ك RSA مع اسم وحجم مفتاح. انقر فوقSave.

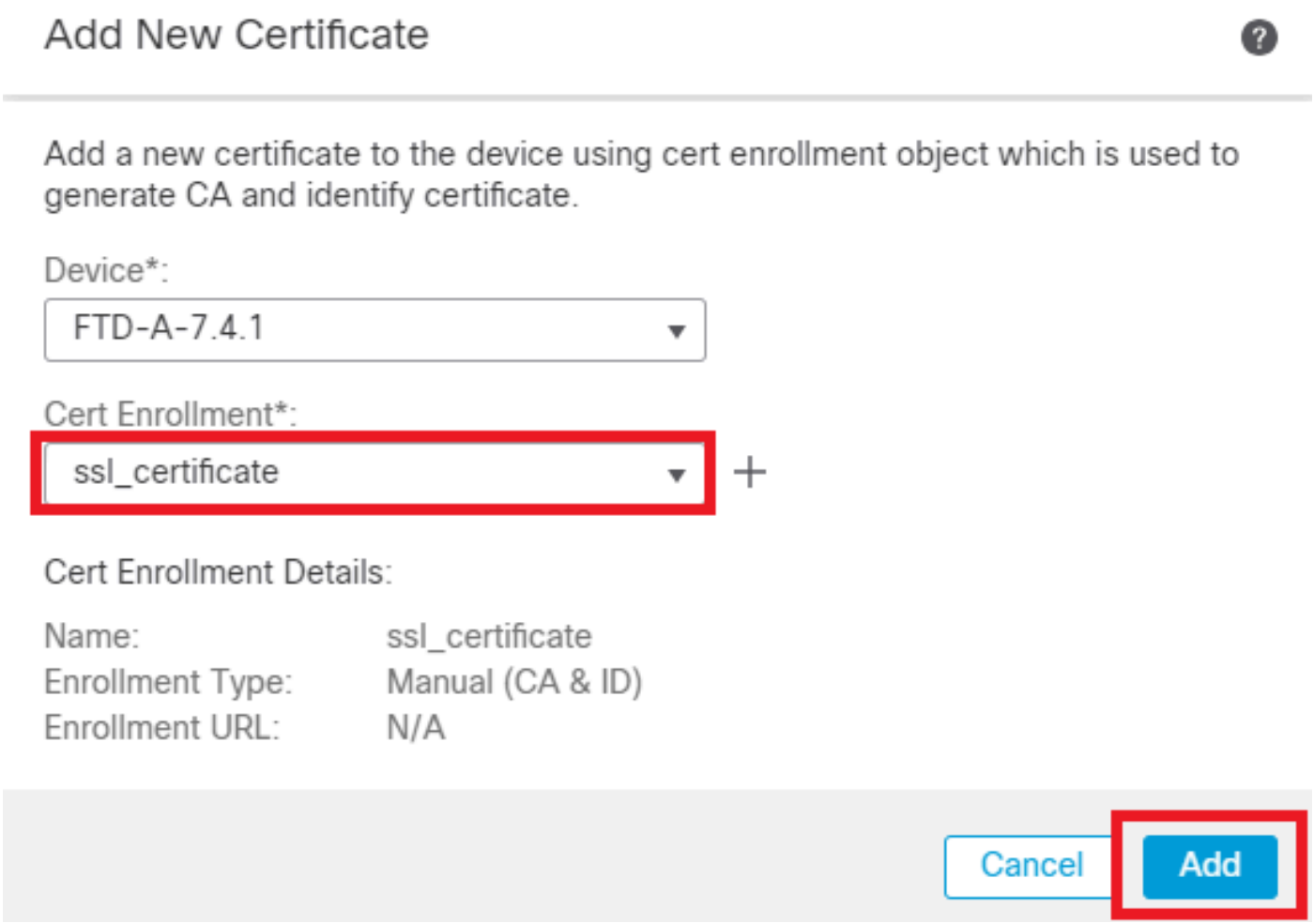


ملاحظة: بالنسبة لنوع مفتاح RSA، يكون الحد الأدنى لحجم المفتاح 2048 بت.



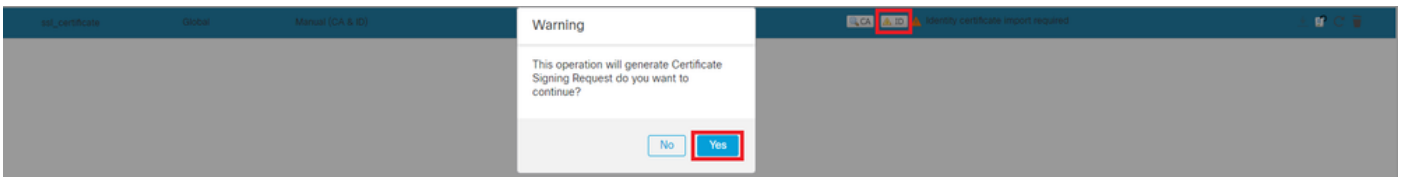
إضافة مفتاح RSA

الخطوة 6. تحتCert Enrollment، أختر نقطة الثقة من القائمة المنسدلة التي تم إنشاؤها للتو وانقر فوقAdd.



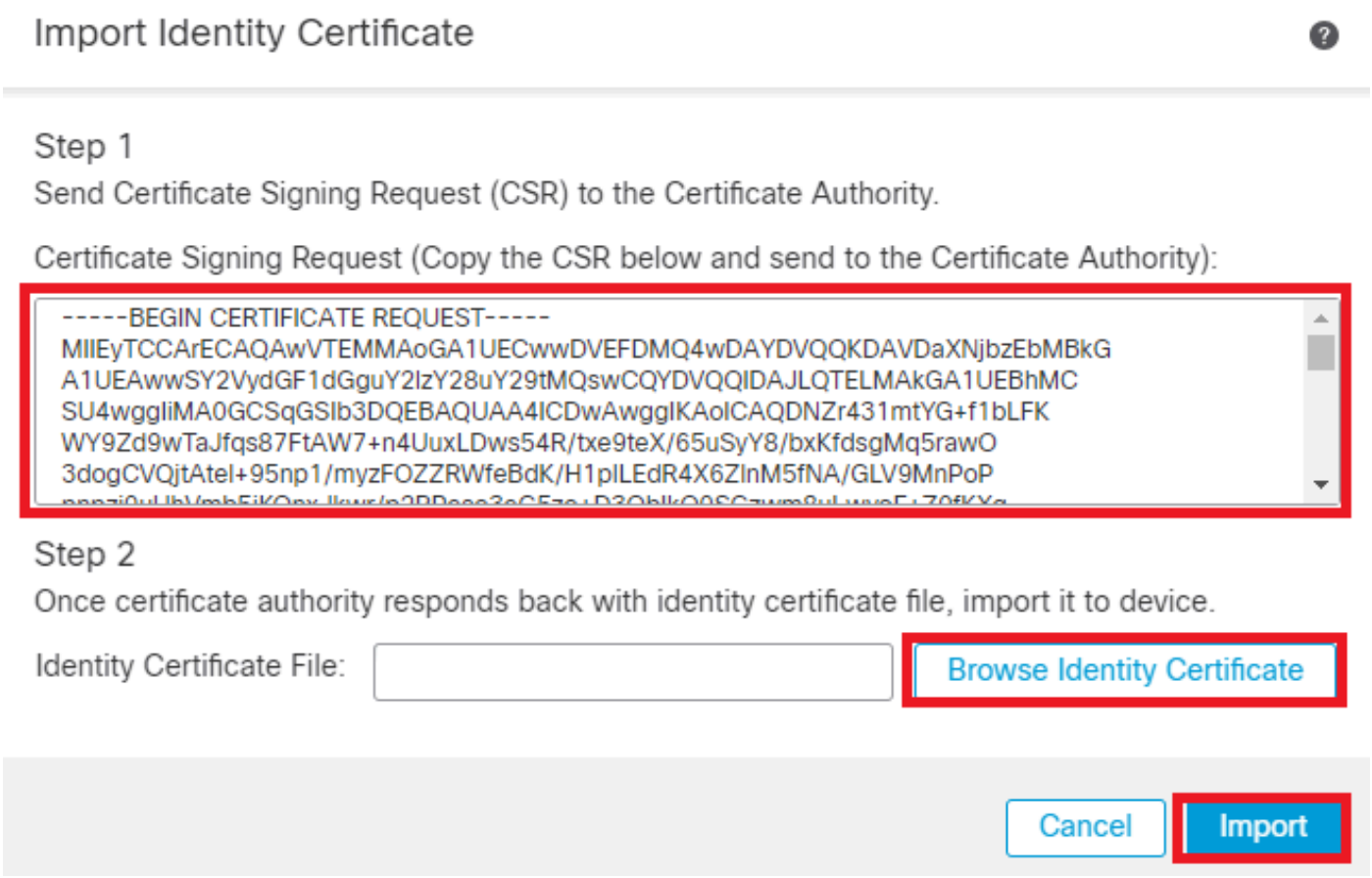
إضافة شهادة جديدة

الخطوة 7. انقر فوق معرف، ثم انقر فوقYesمطالبة أخرى لإنشاء CSR.

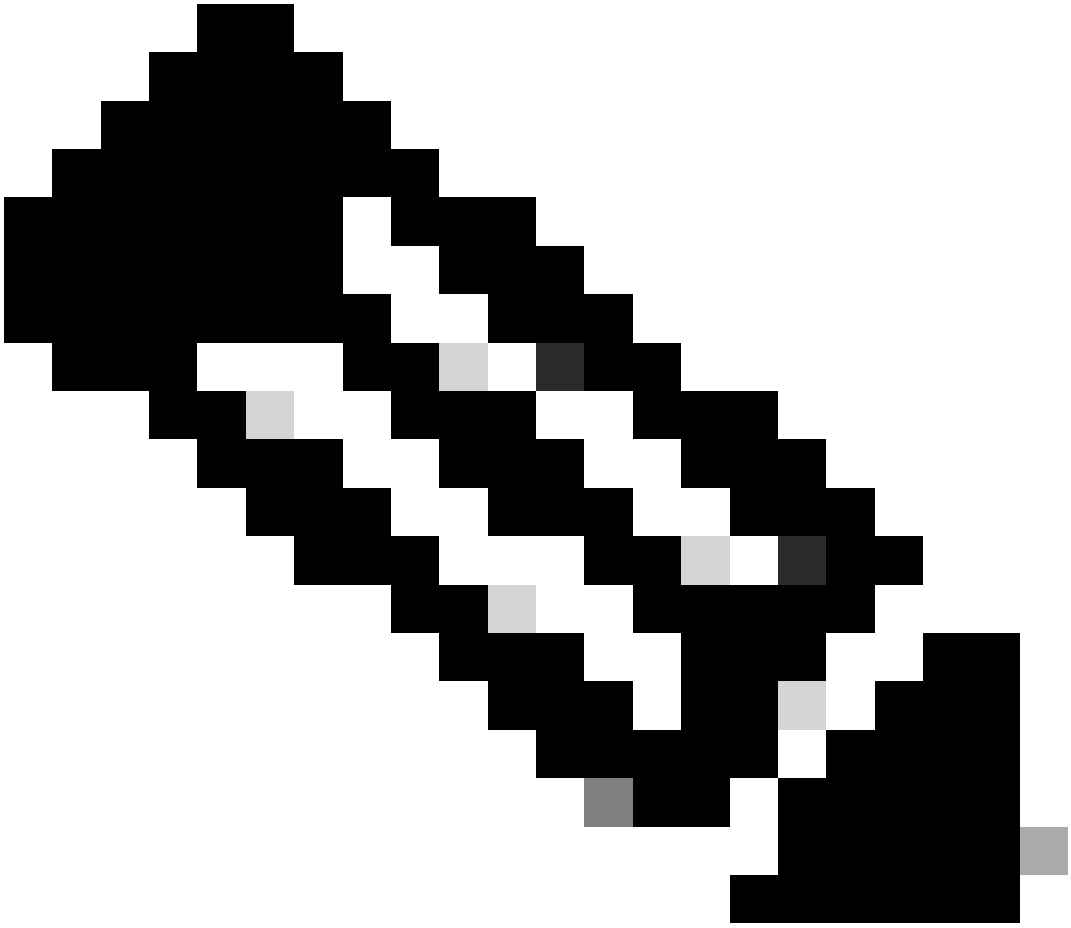


إنشاء CSR

الخطوة 8. انسخ CSR واحصل على توقيعه من قبل المرجع المصدق. بمجرد إصدار شهادة الهوية من قبل CA، قم باستيرادها بالنقرBrowse Identity Certificateوالنقر فوقImport.



استيراد شهادة المعرف



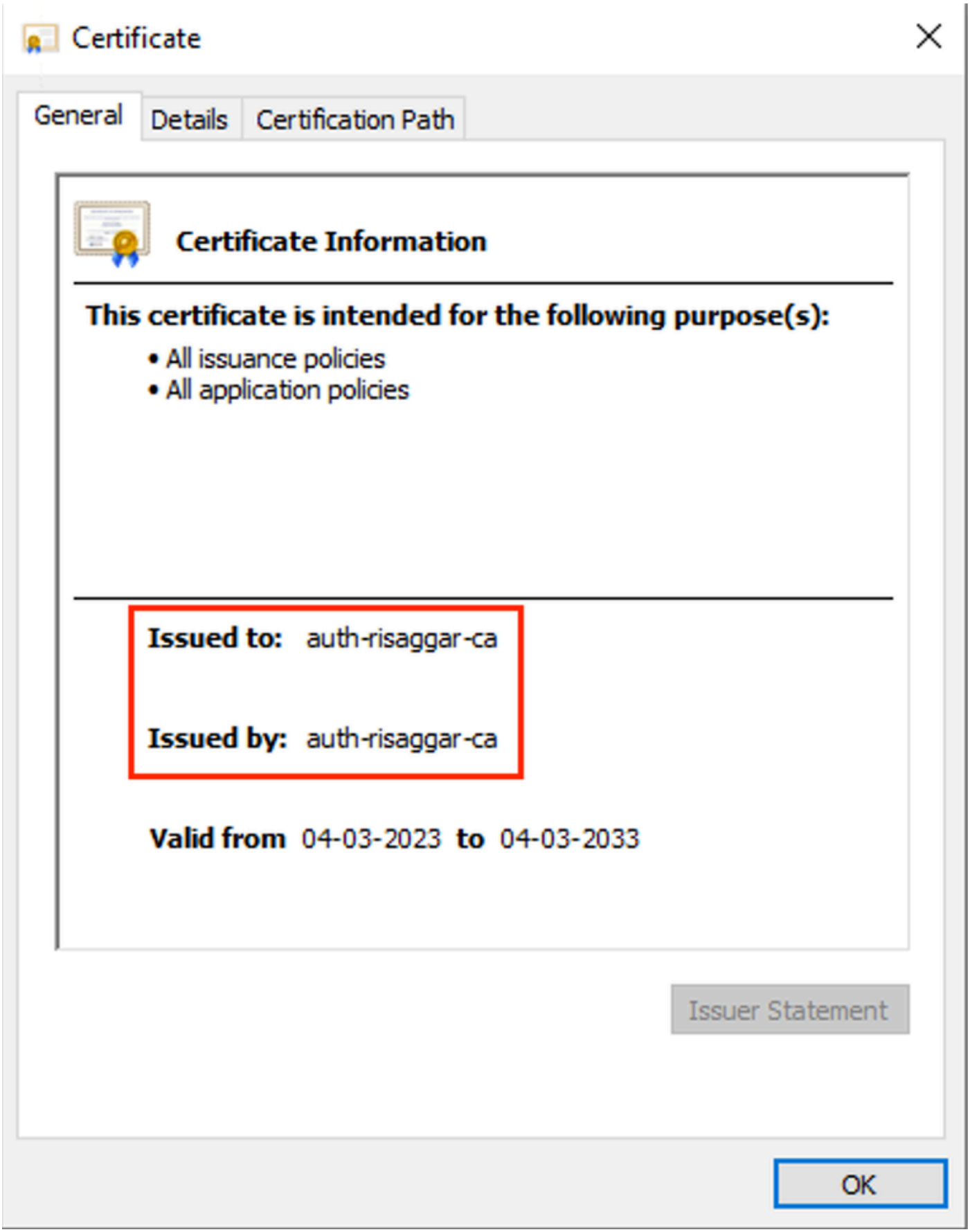
ملاحظة: إذا استغرق إصدار شهادة المعرف وقتا، يمكنك تكرار الخطوة 7. فيما بعد. سيؤدي ذلك إلى إنشاء CSR نفسه ويمكنك إستيراد شهادة المعرف.

إضافة شهادة مرجع مصدق ثقة/داخلية

الخطوة 1. انتقل إلىDevices > Certificatesوانقر فوقAdd.

أختر الجهاز وانقر فوق علامة الجمع (+) ضمن تسجيل القارات.

هنا، تستخدم Auth-risaggar-ca من أجل إصدار شهادات الهوية/المستخدم.

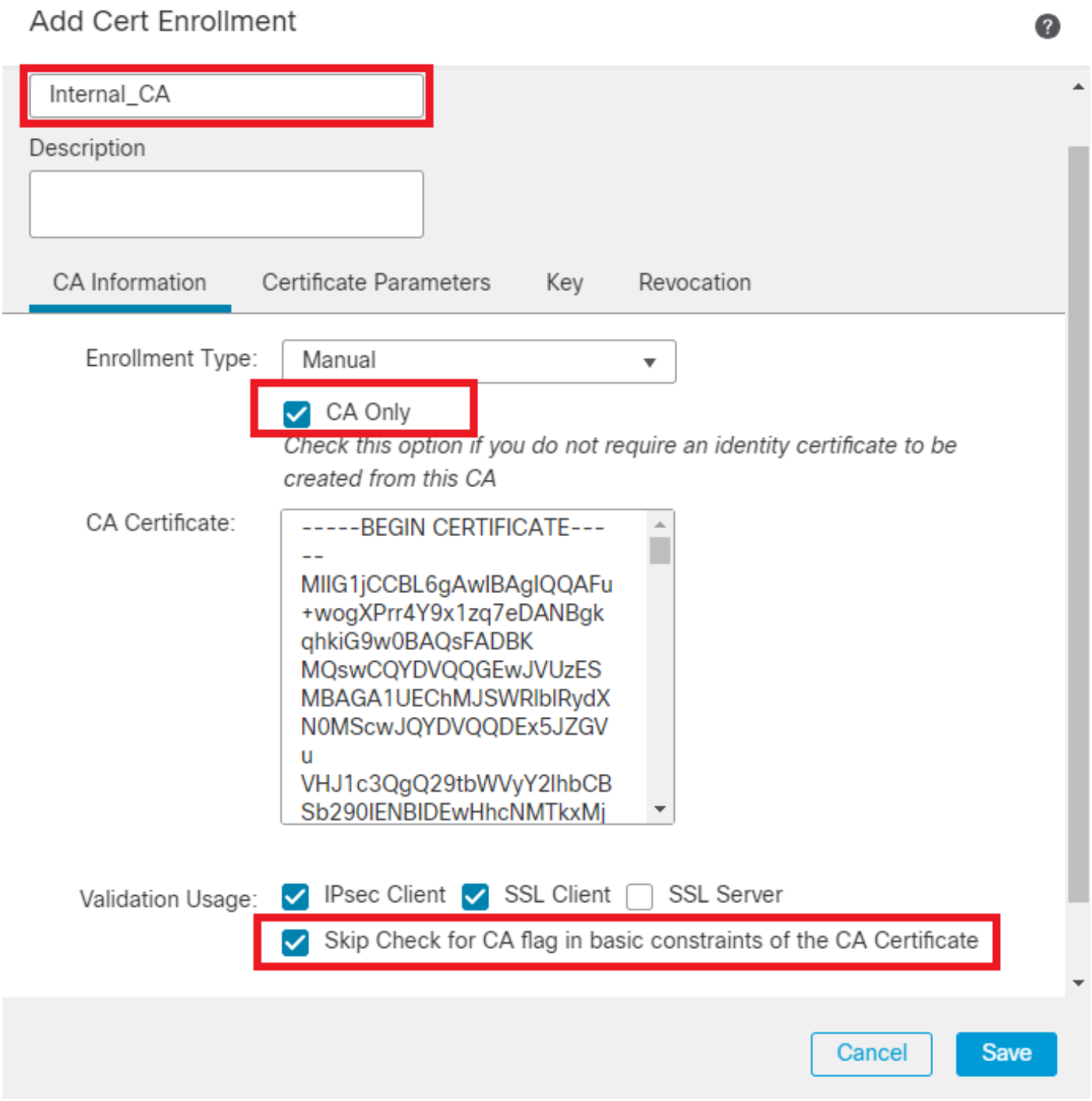


اك-راغاسيرثوأيدان

الخطوة 2. أدخل اسم TrustPoint واخترManualكنوع تسجيل أسفلCA information.

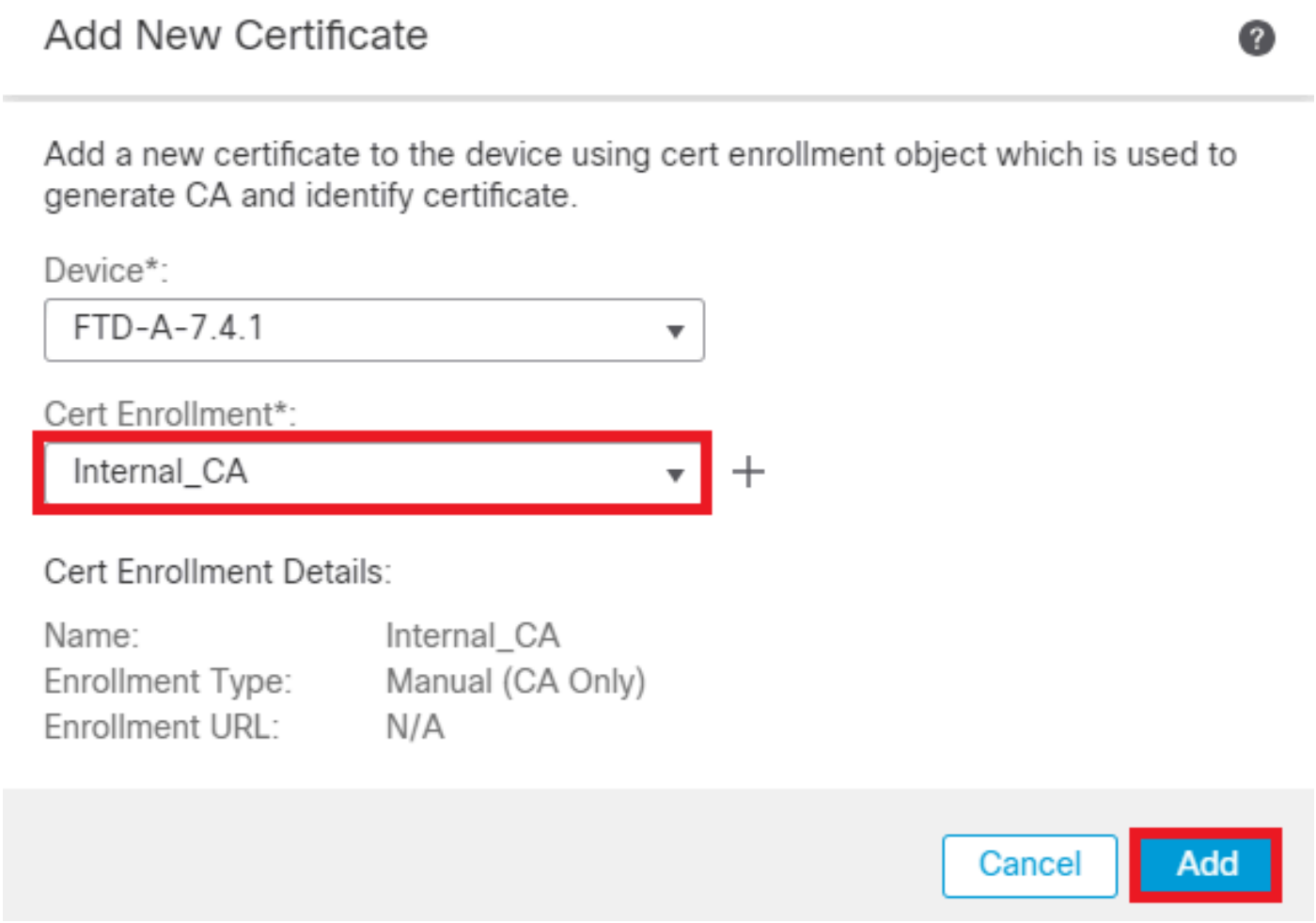
الخطوة 3. تحققCA Only من شهادة المرجع المصدق (CA) الموثوق بها/الداخلية ولصقها بتنسيق PEM.

الخطوة 4. تحقق **Skip Check for CA flag in basic constraints of the CA Certificate** وانقرSave.



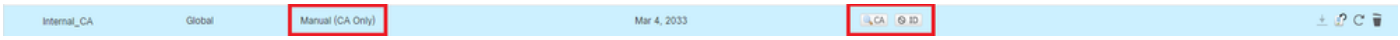
إضافة TrustPoint

الخطوة 5. تحتCert Enrollment، أختر نقطة الثقة من القائمة المنسدلة التي تم إنشاؤها للتو وانقر فوقAdd.



إضافة مرجع مصدق داخلي

الخطوة 6. يتم عرض الشهادة التي تمت إضافتها مسبقا على النحو التالي:

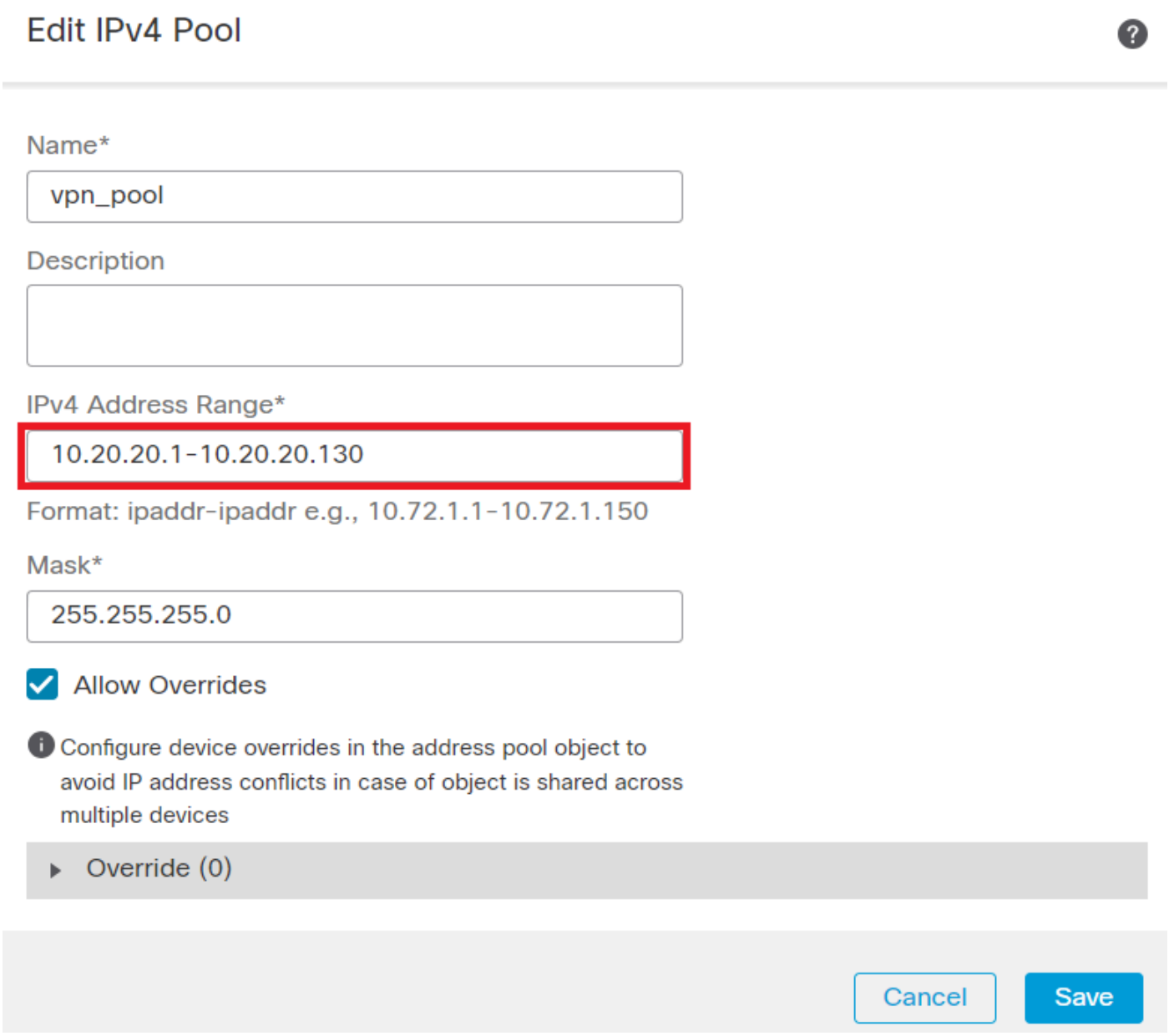


الشهادة المضافة

تكوين تجمع العناوين لمستخدمي VPN

الخطوة 1. انتقل إلىObjects > Object Management > Address Pools > IPv4 Pools.

يدخل خطوة 2. الإسم وعنوان IPv4 مدى مع قناع.



إضافة تجمع IPv4

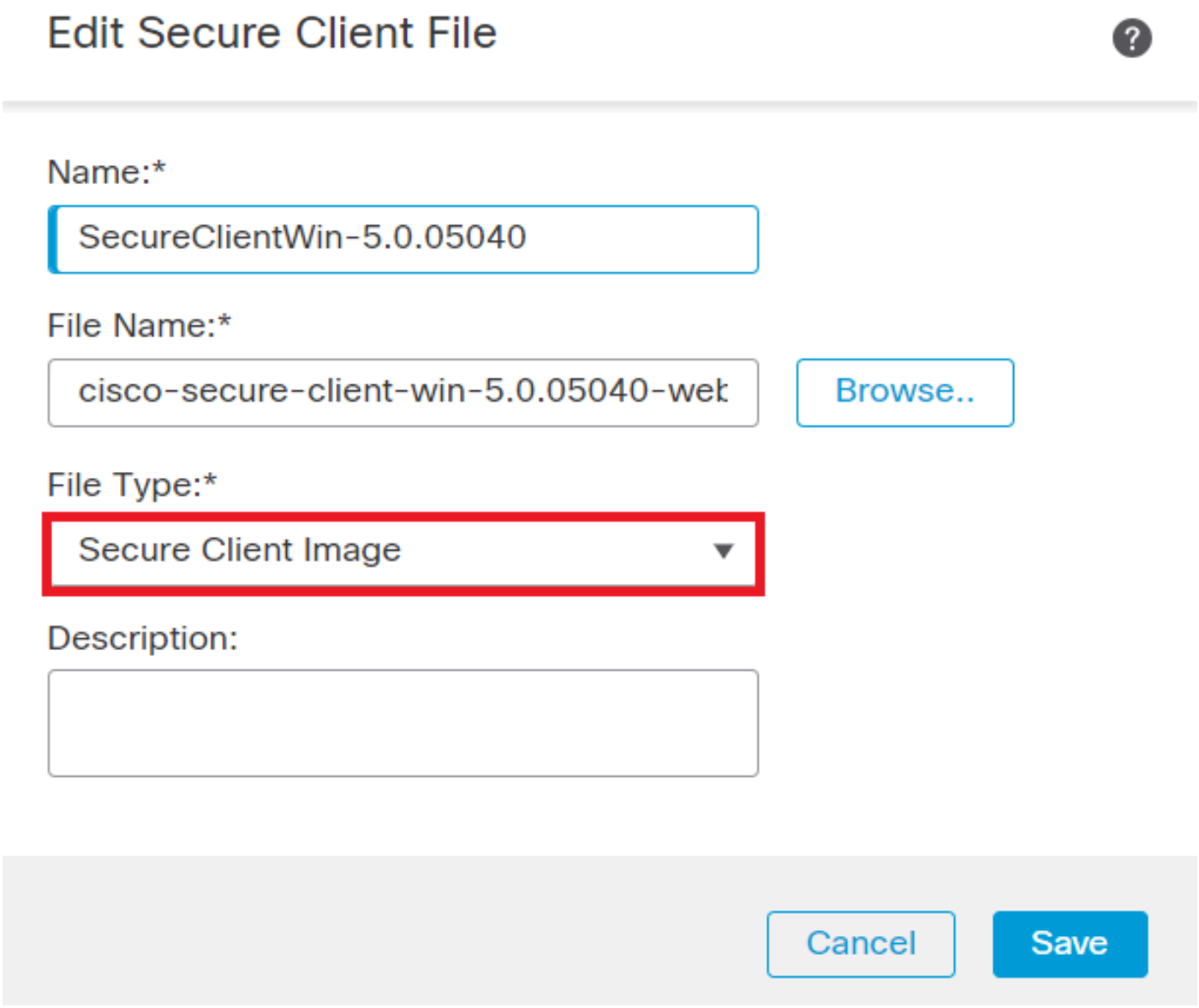
تحميل صور العميل الآمنة

الخطوة 1. تنزيل WebDeployment صور العميل الآمنة وفقا لنظام التشغيل من موقع برامج Cisco.

الخطوة 2. انتقل إلىObjects > Object Management > VPN > Secure Client File > Add Secure Client File.

يدخل خطوة 3. الإسم واختار Secure Client مبرد من القرص.

الخطوة 4. أختر نوع الملف باسمSecure Client Imageوانقر فوقSave.



إضافة صورة عميل آمنة

إنشاء ملف تعريف XML وتحميله

الخطوة 1. تنزيل العميلProfile Editorالآمن وتثبيته من موقع برامج Cisco.

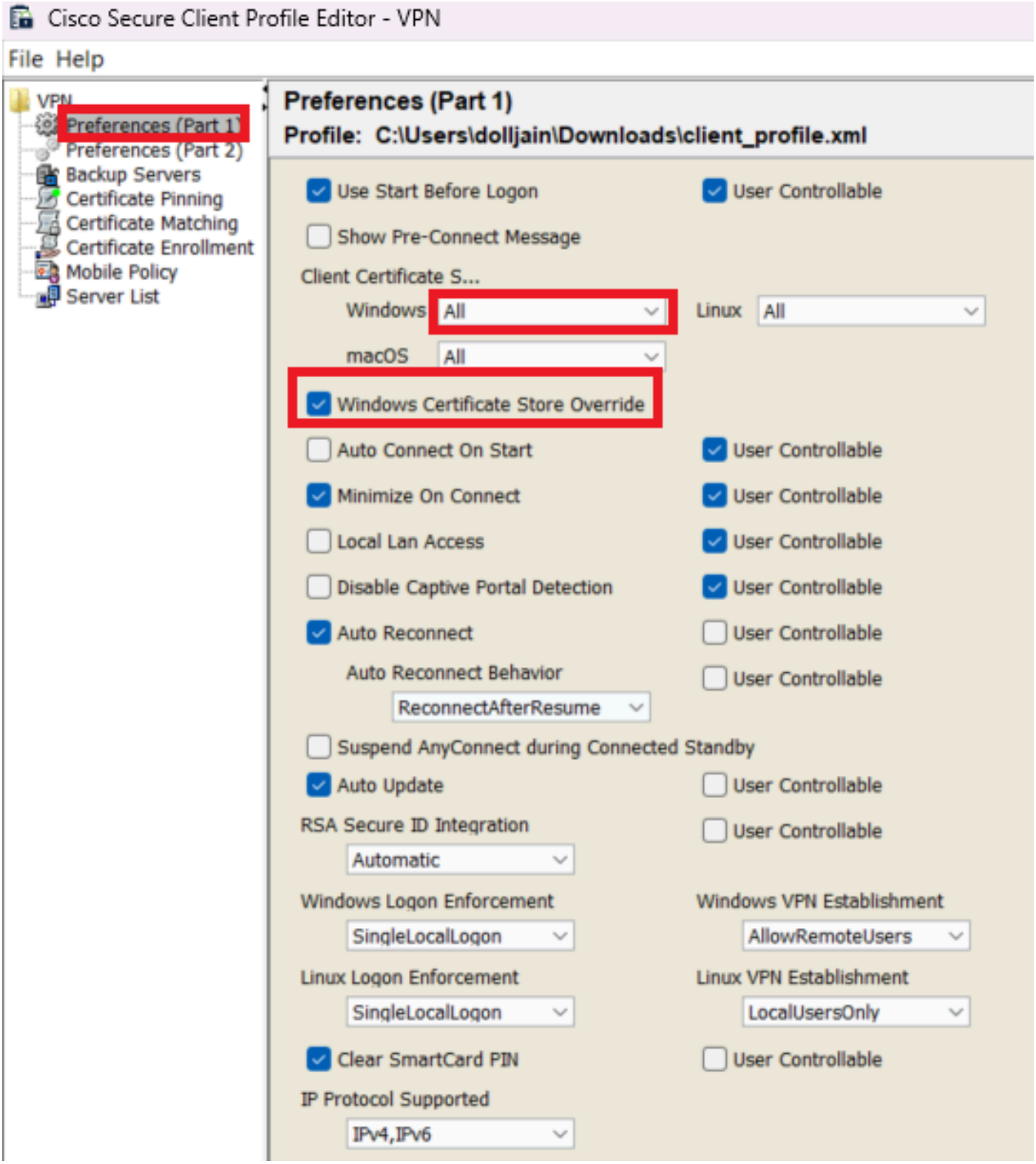
الخطوة 2. قم بإنشاء ملف تعريف جديد واخترAllمن القائمة المنسدلة لتحديد شهادة العميل. وهو يتحكم بشكل رئيسي في مخزن (مخازن) الشهادات التي يمكن لـ "العميل الآمن" استخدامها لتخزين الشهادات وقراءتها.

خياران آخران متاحان هما:

1. الجهاز - تم تقييد Secure Client للبحث عن الشهادة في مخزن شهادات الجهاز المحلي لـ Windows.
2. المستخدم - تم تقييد العميل الآمن للبحث عن الشهادة في مخزن شهادات مستخدم Windows المحلي.

تعيين تجاوز مخزن الشهاداتTrue.

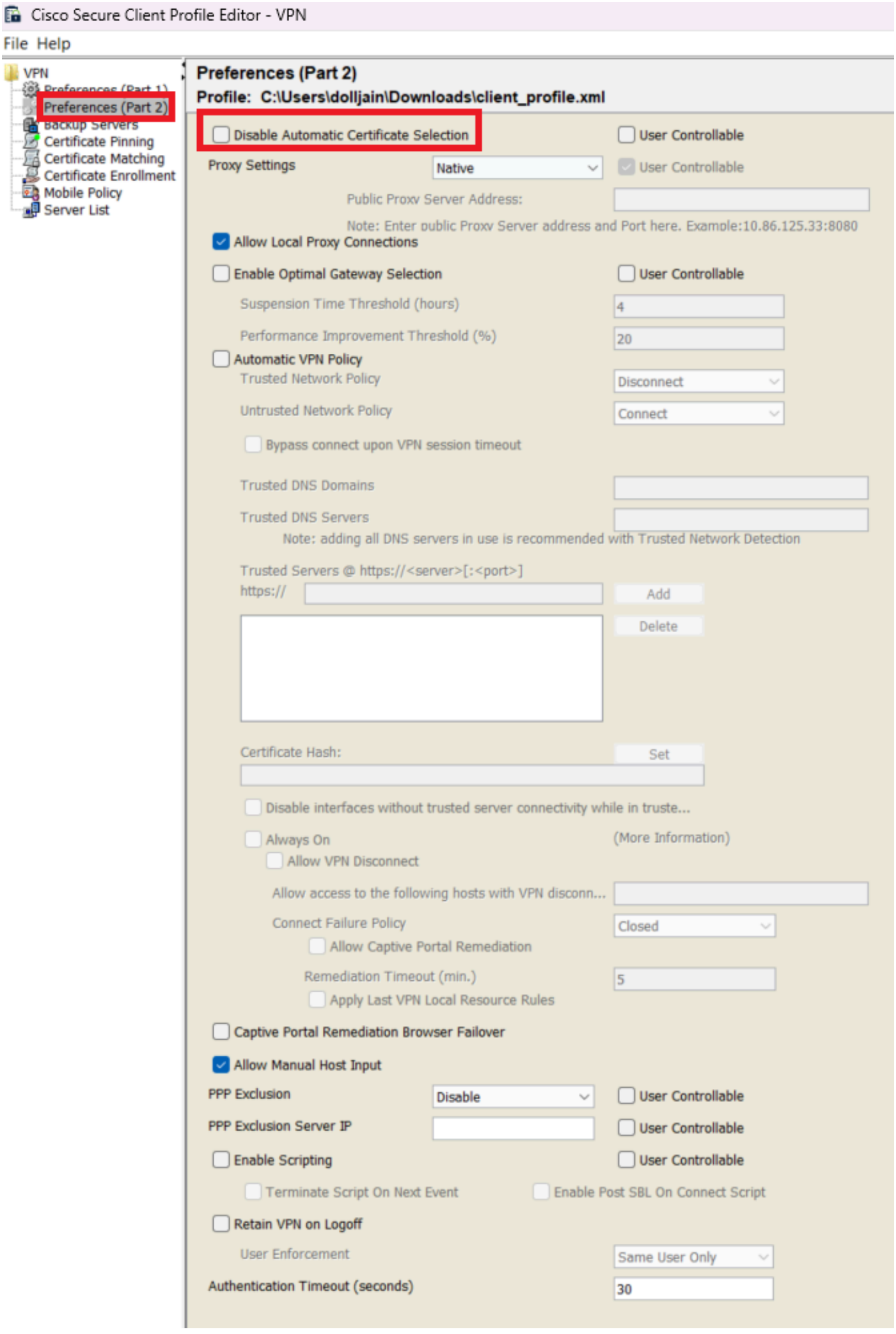
وهذا يسمح للمستخدم بتوجيه "العميل الآمن" لاستخدام الشهادات الموجودة في مخزن الشهادات الخاص بجهاز Windows (النظام المحلي) لمصادقة شهادة العميل. ينطبق "تجاوز مخزن الشهادات" على SSL فقط، حيث يتم بدء الاتصال، بشكل افتراضي، بواسطة عملية واجهة المستخدم. عند إستخدام IPSec/IKEv2، لا تنطبق هذه الميزة الموجودة في ملف تعريف العميل الآمن.

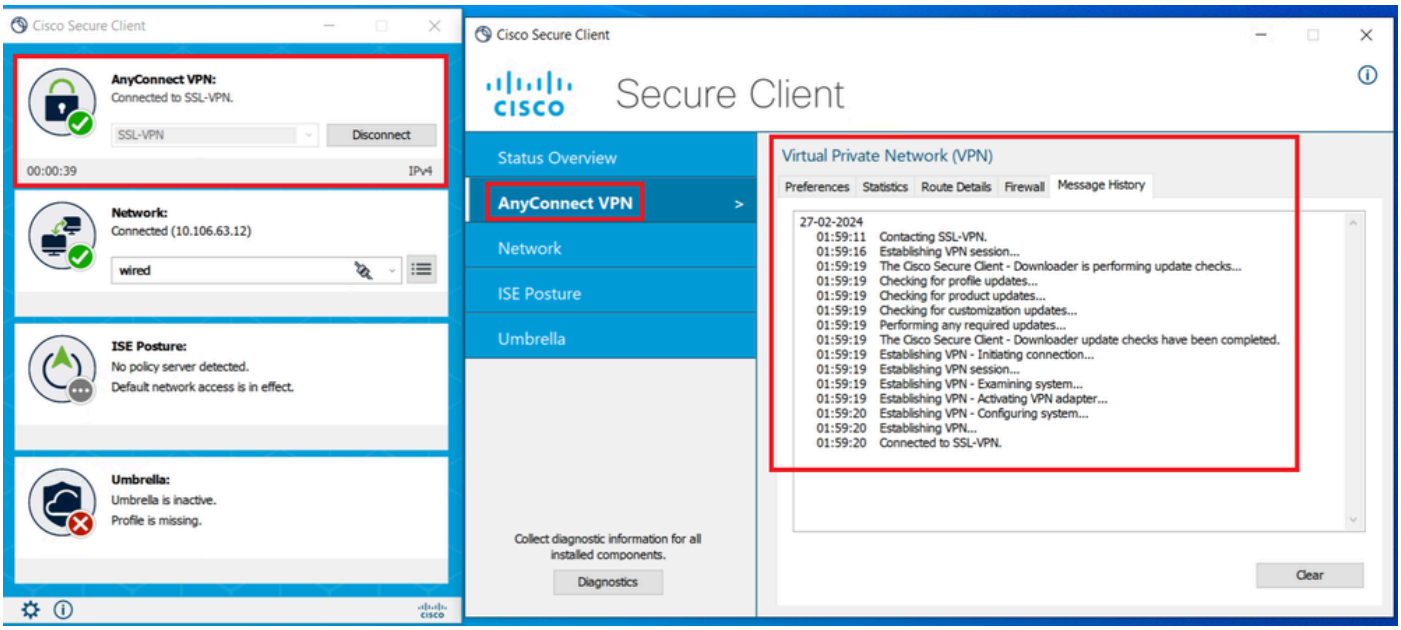


إضافة تفضيلات (الجزء 1)

الخطوة 3. (إختياري) قمDisable Automatic Certificate Selectionبإلغاء تحديد الأمر لأنه يجنب الإيعاز

للمستخدم باختيار شهادة المصادقة.


Cisco Secure Client Profile Editor - VPN
File Help
VPN
Preferences (Part 1)
Preferences (Part 2)
Backup Servers
Certificate Pinning
Certificate Matching
Certificate Enrollment
Mobile Policy
Server List
Preferences (Part 2)
Profile: C:\Users\dolljain\Downloads\client_profile.xml
Disable Automatic Certificate Selection
User Controllable
Proxy Settings
Native
User Controllable
Public Proxy Server Address:
Note: Enter public Proxy Server address and Port here. Example:10.86.125.33:8080
Allow Local Proxy Connections
Enable Optimal Gateway Selection
User Controllable
Suspension Time Threshold (hours)
4
Performance Improvement Threshold (%)
20
Automatic VPN Policy
Trusted Network Policy
Disconnect
Untrusted Network Policy
Connect
Bypass connect upon VPN session timeout
Trusted DNS Domains
Trusted DNS Servers
Note: adding all DNS servers in use is recommended with Trusted Network Detection
Trusted Servers @ https://<server>[:<port>]
https://
Add
Delete
Certificate Hash:
Set
Disable interfaces without trusted server connectivity while in truste...
Always On
(More Information)
Allow VPN Disconnect
Allow access to the following hosts with VPN disconn...
Connect Failure Policy
Closed
Allow Captive Portal Remediation
Remediation Timeout (min.)
5
Apply Last VPN Local Resource Rules
Captive Portal Remediation Browser Failover
Allow Manual Host Input
PPP Exclusion
Disable
User Controllable
PPP Exclusion Server IP
User Controllable
Enable Scripting
User Controllable
Terminate Script On Next Event
Enable Post SBL On Connect Script
Retain VPN on Logoff
User Enforcement
Same User Only
Authentication Timeout (seconds)
30



اتصال عميل آمن ناجح

3. تشغيلshow vpn-sessiondb anyconnectلتأكيد تفاصيل الاتصال للمستخدم النشط ضمن مجموعة النفق المستخدمة.

```
firepower# show vpn-sessiondb anyconnect

Session Type: AnyConnect

Username     : dolljain.cisco.com     Index        : 8
Assigned IP  : 10.20.20.1             Public IP    : 72.163.X.X
Protocol     : AnyConnect-Parent SSL-Tunnel
License      : AnyConnect Premium
Encryption   : AnyConnect-Parent: (1)none  SSL-Tunnel: (1)AES-GCM-128
Hashing      : AnyConnect-Parent: (1)none  SSL-Tunnel: (1)SHA256
Bytes Tx     : 14402                  Bytes Rx     : 9652
Group Policy : DfltGrpPolicy          Tunnel Group : RAVPN-CertAuth
Login Time   : 08:32:22 UTC Mon Mar 18 2024
Duration     : 0h:03m:59s
Inactivity   : 0h:00m:00s
VLAN Mapping : N/A                    VLAN         : none
Audt Sess ID : 0ac5de050000800065f7fc16
Security Grp : none                   Tunnel Zone  : 0
```

استكشاف الأخطاء وإصلاحها

يوفر هذا القسم معلومات يمكنك إستخدامها لاستكشاف أخطاء التكوين وإصلاحها.

1. يمكن تشغيل تصحيح الأخطاء من واجهة سطر الأوامر التشخيصية ل FTD:

```
debug crypto ca 14
debug webvpn anyconnect 255
debug crypto ike-common 255
```

2. راجع اذه الدليل للتعرف عىل املشاكل املشتركة.

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 دائمًا إلى المستند الإنجليزي الأصلي (الرابط متوفر).