تكوين تسجيل الشهادة باستخدام بروتوكول ACME على الدفاع الآمن عن تهديد جدار الحماية الذي تتم إدارته بواسطة FMC

المقدمة

يصف هذا المستند عملية تسجيل شهادة أمان طبقة النقل (TLS) من خلال بروتوكول بيئة إدارة الشهادات المؤتمتة (ACME) على النظام الأساسي Secure Firewall Firepower Threat Defense (FTD).

المتطلبات الأساسية

المتطلبات

cisco يوصي أنك تتلقى معرفة على هذا موضوع:

- عمليات تسجيل الشهادة اليدوية وأساسيات طبقة مآخذ التوصيل الآمنة (SSL).
- مفاهيم المصادقة الأساسية للشبكات الخاصة الظاهرية (VPN) للوصول عن بعد.
- الخبرة مع هيئات التصديق (CAs).

المكونات المستخدمة

- الإصدار 10.0.0-35 من Cisco FTDv.
- Cisco FMC، الإصدار 10.0.0-35.
- خادم جهة منح الشهادة (CA) الذي يدعم بروتوكول ACME.

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.

المتطلبات والحدود

تتضمن المتطلبات الأساسية والقيود الحالية لتسجيل ACME في FTD لجدار الحماية الآمن ما يلي:

- الإصدارات الأحدث. FMC و FTD إصدارات على مدعوم 10.0.0 الإصدار والإصدارات
- لا تسمح ACME بإصدار شهادات حرف البدل؛ يجب أن يحدد كل طلب شهادة اسم مجال محدد.
- يتم تقييد كل نقطة ثقة مسجلة من خلال ACME بواجهة واحدة، لذلك لا يمكن مشاركة الشهادات التي يتم الحصول عليها عبر ACME عبر واجهات متعددة.
- يتم إنشاء أزواج المفاتيح تلقائيا وهي فريدة لكل شهادة مسجلة من خلال ACME، مما يمنع إعادة استخدام المفاتيح ويحسن التأمين.

اعتبارات الخفض

عند الخفض إلى إصدار FTD لجدار الحماية الآمن الذي لا يدعم تسجيل ACME (الإصدار 7.7 أو الأقدم):

- يتم فقد جميع تكوينات TrustPoint ذات الصلة ب ACME المقدمة في الإصدار 10.0.0 أو الأحدث.
- لا يزال الوصول إلى الشهادات المسجلة عبر ACME ممكنا؛ ومع ذلك، فإن مفاتيحها الخاصة تصبح غير مرتبطة بعد أول حفظ وإعادة تشغيل بعد الخفض.

إذا كان الخفض ضروريا، استخدم الحل البديل الموصى به:

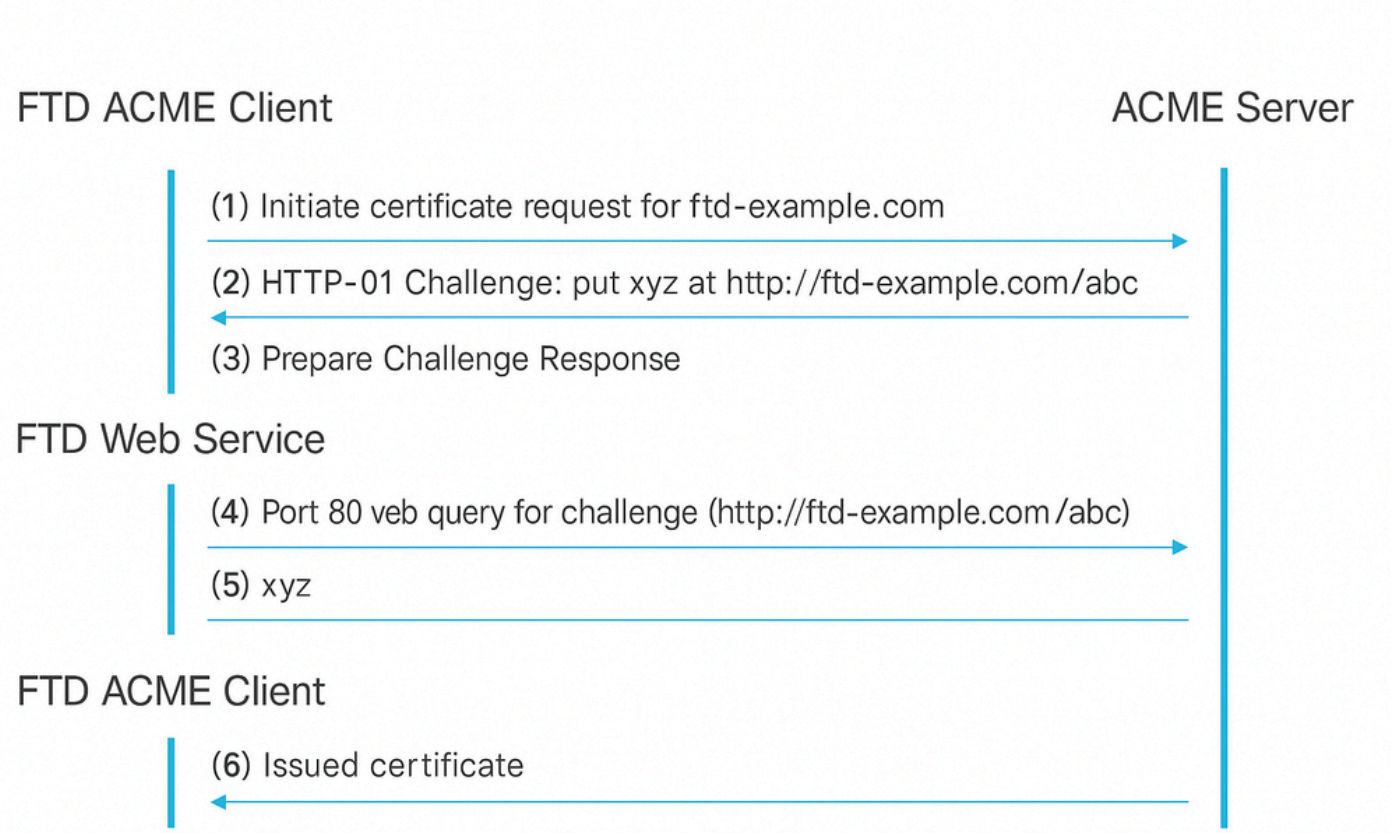
- قبل الخفض، قم بتصدير شهادات ACME بتنسيق PKCS12.
- قبل الخفض، قم بإزالة تكوين ACME TrustPoint.
- بعد الخفض، قم باستيراد شهادة PKCS12. لظل TrustPoint المستوردة صالحة حتى تنتهي صلاحية الشهادة الصادرة عن ACME.

معلومات أساسية

يهدف بروتوكول ACME إلى تبسيط إدارة شهادات TLS للمؤسسات. من خلال برنامج ACME، يمكن للمؤسسات أتمتة المهام المتعلقة باكتساب وتجديد شهادات TLS. هذا ACME، يمكن للمؤسسات أتمتة المهام المتعلقة باكتساب وتجديد شهادات TLS. هذا لأن المرجع المصدق (CA) مثل Let's Encrypt، التي توفر شهادات مجانية ومؤتمتة ويمكن الوصول إليها بشكل عام عبر بروتوكول ACME.يسمى لإصدار شهادات التحقق من صحة المجال (DV). تحقق هذه الشهادات من أن طالب الشهادة له تحكم على المجالات المحددة. يتم التحقق من الصحة عادة من خلال عملية تحقق تستند إلى HTTP، حيث يقوم موقع مقدم الطلب بوضع ملف معين على خادم HTTP يمكن للمرجع المصدق (CA) الوصول إليه عبر هذا الملف. ثم توقف "المرجع المصدق" ب.ه صاخلا بيولا ةداهش رادصإ نم قدصملا عجرملا يدحتلا اذه زايتجإ نكمي .لاجملاب مكحتلا ديكأتل لاجملل DV حاجنب.

تتضمن عملية التسجيل الخطوات التالية:

1. بدء طلب الشهادة: يقوم العميل بإرسال طلب شهادة إلى خادم ACME، ويحدد المجال (المجالات) المطلوب الحصول على الشهادة من أجله.
2. تلقي تحدي HTTP-01: يستجيب خادم ACME بتحدي HTTP-01 يحتوي على رمز مميز يجب على العميل إستخدامه لإثبات ملكية المجال.
3. تحضير إستجابة التحدي:
   1. يقوم العميل بإنشاء تفويض مفتاح عن طريق تجميع الرمز المميز من خادم ACME مع مفتاح الحساب الخاص به.
   2. يقوم العميل بتكوين خادم ويب الخاص به لخدمة تفويض المفتاح هذا في مسار مُحدد لـ URL.
4. خادم ACME يستعيد التحدي: يقوم خادم ACME بتنفيذ طلب HTTP GET إلى عنوان URL المتوفر للحصول على تفويض المفتاح.
5. يقوم خادم ACME بالتحقق من الملكية: يقوم الخادم بمقارنة تخويل المفتاح الذي تم إستردادهِ بالقيمة المتوقعة للتحقق من تحكم العميل بالمجال.
6. شهادة الإصدار: عند التحقق من الصحة بنجاح، يصدر خادم ACME شهادة SSL/TLS للعميل.



تدفق مصادقة HTTP-01 لتسجيل ACME.

تتضمن المميزات الرئيسية لاستخدام بروتوكول ACME لتسجيل شهادات TLS على FTD

لجدار الحماية الآمن ما يلي:

- التشغيل التلقائي لإدارة الشهادات: تعمل ميزة التحكم في الوصول للبنية الأساسية (ACME) على تنظيم عملية الحصول على شهادات مجال TLS والاحتفاظ بها لواجهات TLS الخاصة ببرنامج FTD لجدار الحماية الآمن، مما يعمل على تقليل المهام الإدارية اليدوية بشكل كبير.
- التجديد التلقائي للشهادة: ومع وجود نقاط الثقة التي تدعم معيار ACME، يتم تجديد الشهادات تلقائيا مع اقتراب انتهاء صلاحيتها، مما يقلل من الحاجة إلى التدخل الإداري المستمر.
- ضمان الأمان المستمر: يضمن هذا التشغيل التلقائي بقاء الشهادات صالحة دون انقطاع، مما يمنع انتهاء صلاحية الشهادة غير المتوقعة ويحافظ على الاتصالات الآمنة.

تعمل هذه المزايا مجتمعة على تحسين الكفاءة التشغيلية والأمان لعمليات نشر برنامج الإرسال فائق السرعة (FTD) عبر جدار الحماية الآمن.

التكوين

تكوين المتطلبات الأساسية

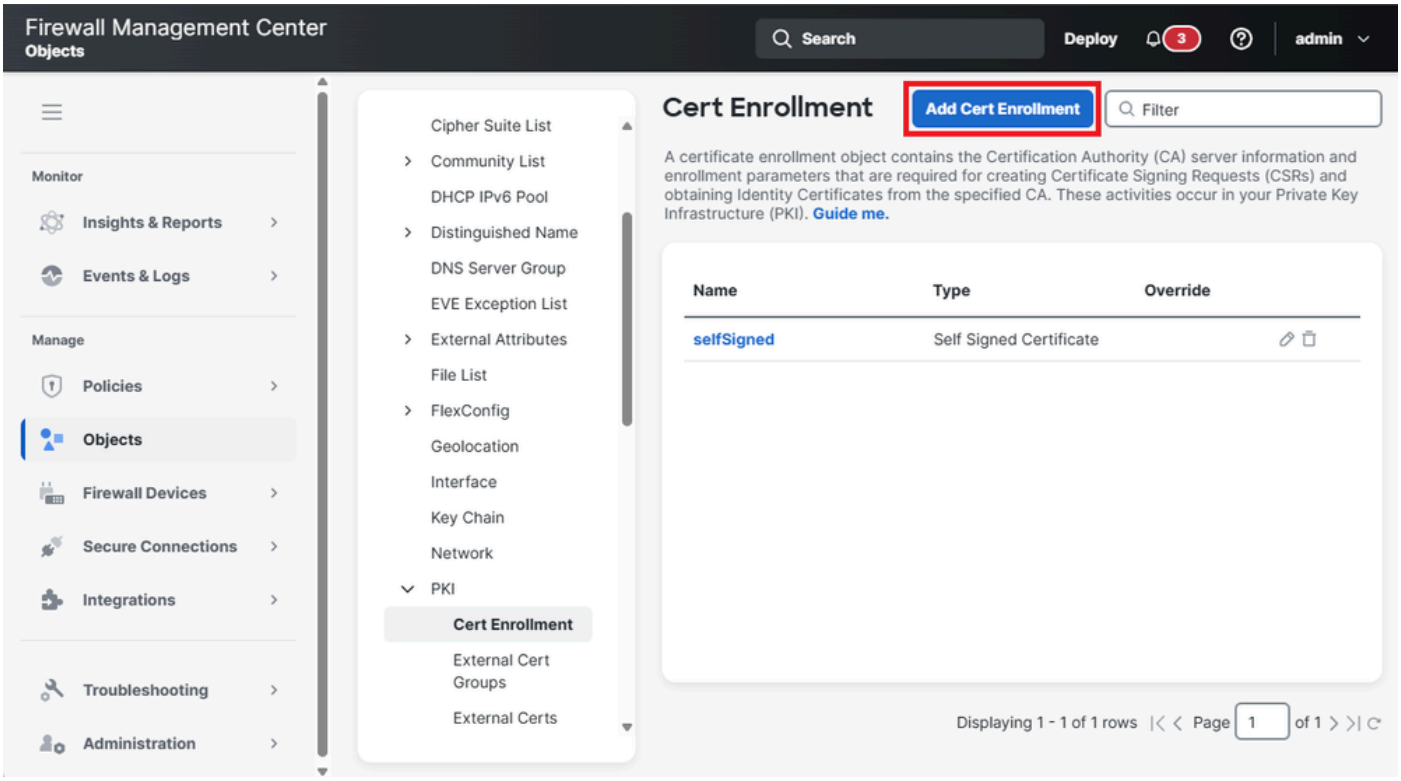
قبل بدء عملية تسجيل ACME، تأكد من استيفاء الشروط التالية:

1. اسم المجال القابل للحل: يجب أن يكون اسم المجال الذي تطلب الشهادة الخاصة به قابلا للحل بواسطة خادم ACME. وهذا يضمن إمكانية قيام الخادم بالتحقق من ملكية المجال.
2. الوصول الآمن إلى جدار الحماية إلى خادم ACME: يجب أن يكون لجدار الحماية الآمن إمكانية الوصول إلى خادم ACME من خلال إحدى الواجهات الخاصة به. لا يلزم أن يتم هذا الوصول عبر الواجهة التي يتم طلب الشهادة من أجلها.
3. التوفر لمنفذ TCP رقم 80: السماح لمنفذ TCP رقم 80 من خادم ACME CA إلى الواجهة المطابقة لاسم المجال. هذا مطلوب أثناء عملية تبادل ACME لإكمال تحدي HTTP-01.

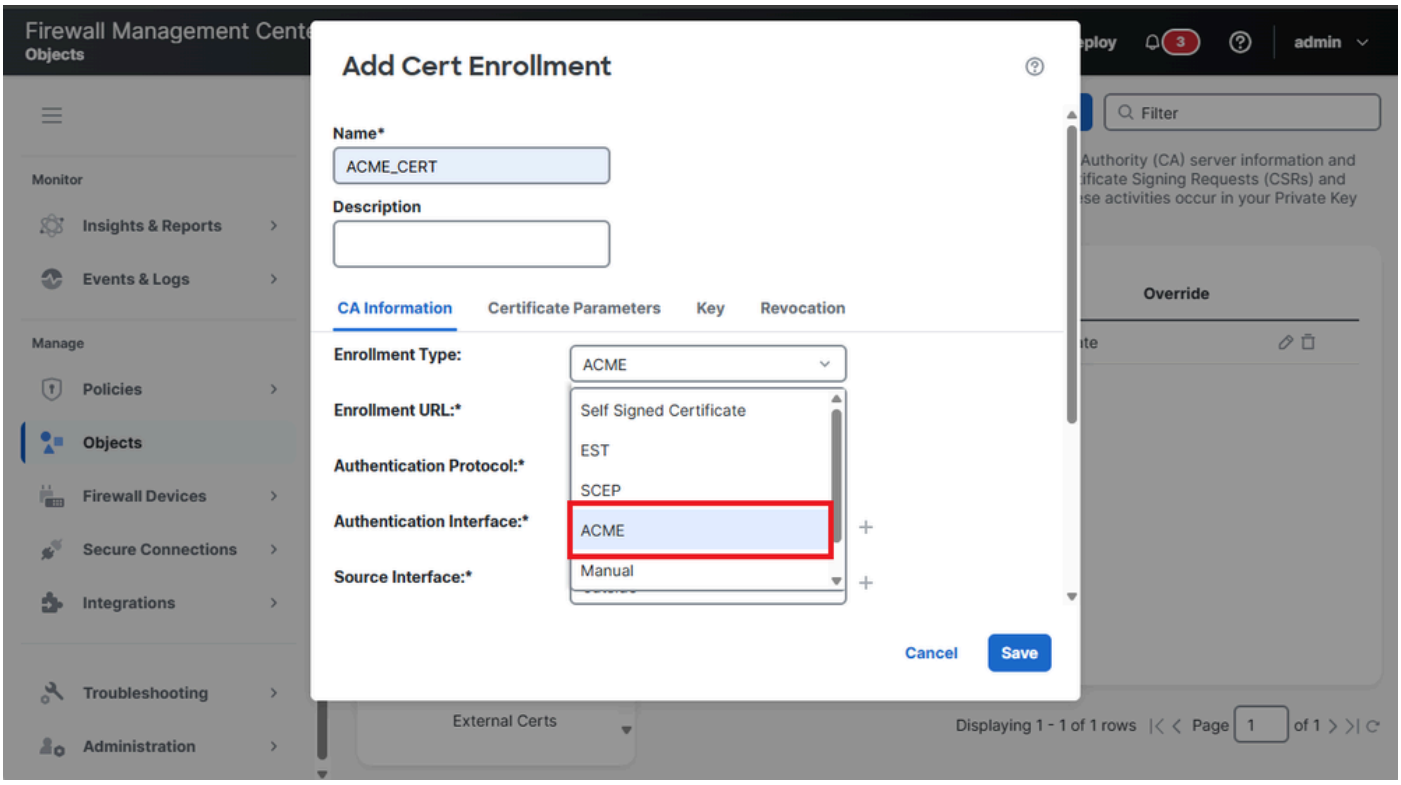
ملاحظة: أثناء الفترة التي يكون فيها المنفذ 80 مفتوحا، يمكن الوصول إلى بيانات تحدي ACME فقط.

إنشاء كائن تسجيل شهادة ACME

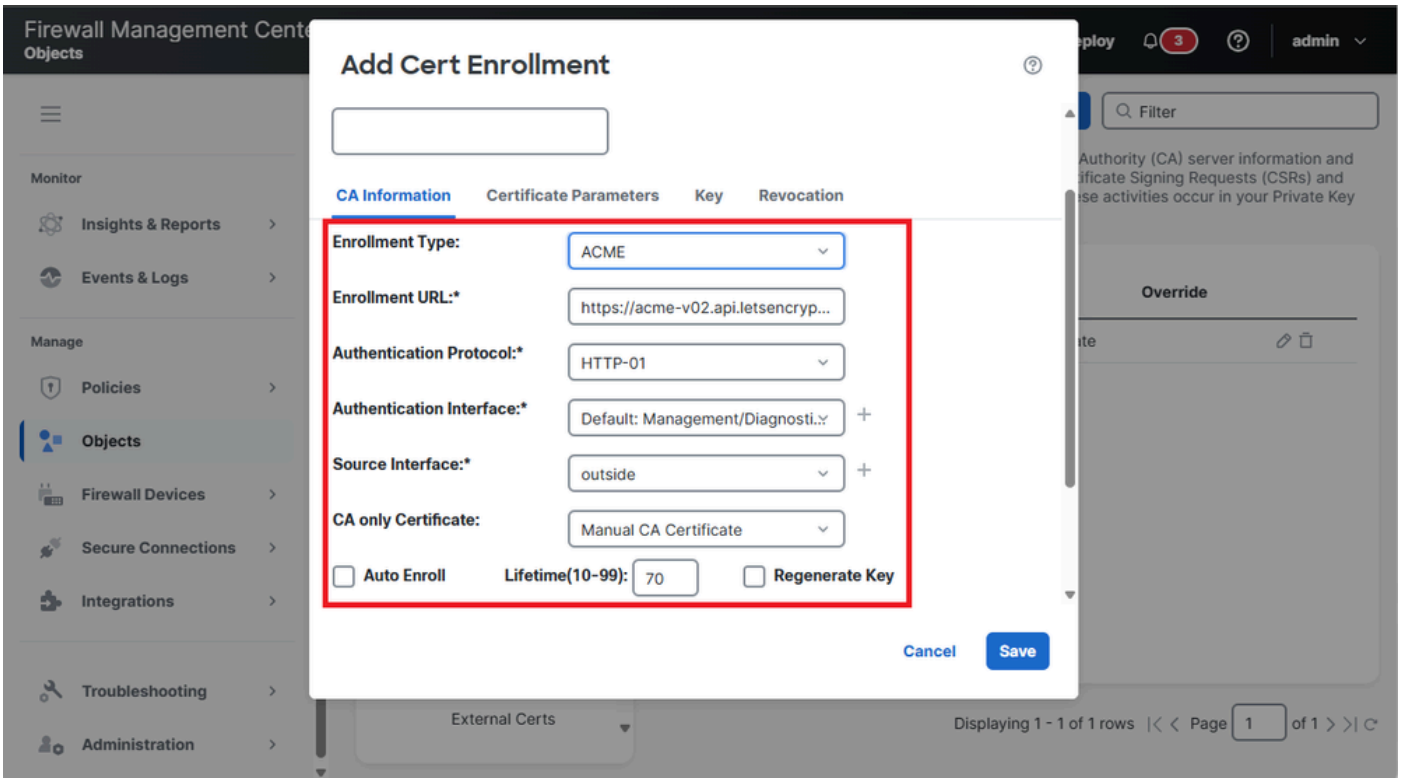
1. انتقل إلى الكائنات > PKI > تسجيل CERT وانقر فوق إضافة تسجيل CERT لبدء عملية التكوين.



2. يتم سرد خيار تسجيل ACME في القائمة المنسدلة مع طرق التسجيل الأخرى. حدد ACME من القائمة المنسدلة نوع التسجيل للمتابعة.



3. يتم عرض خيارات تكوين معلمات الشهادة، وإكمال الحقول بالمعلومات المناسبة.

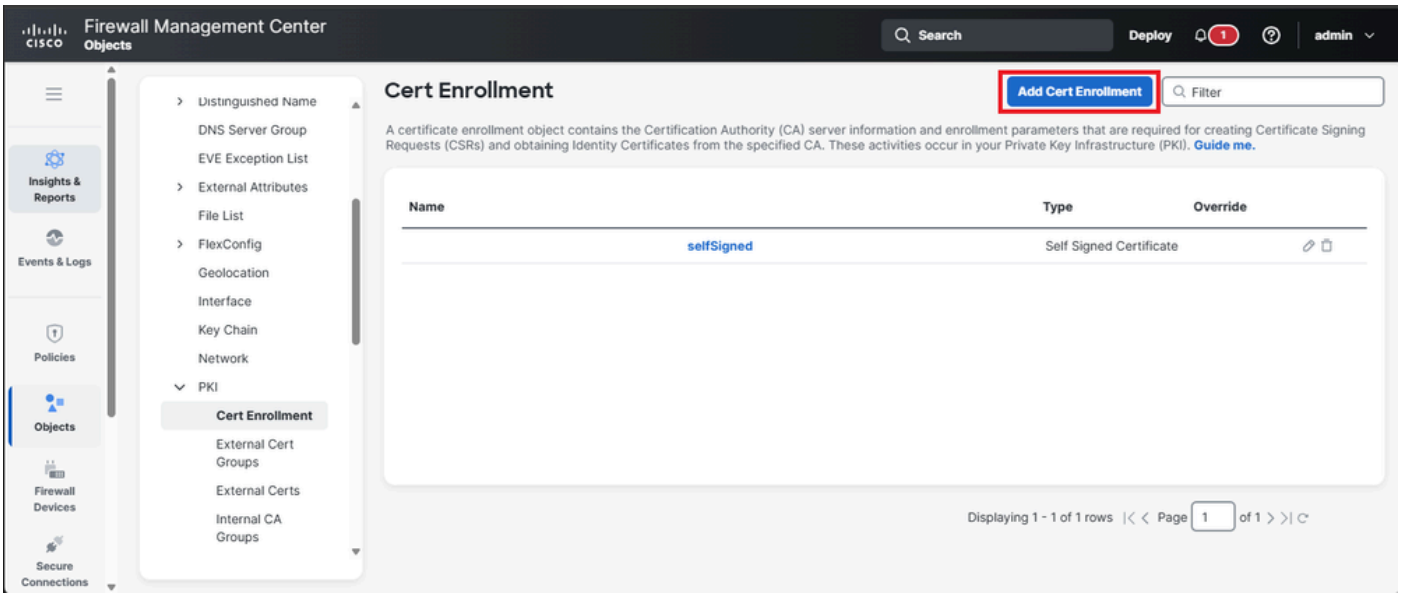


- عنوان URL للتسجيل: هذا هو عنوان خادم ACME (مثل Let'Encrypt) المستخدم لطلب الشهادات واسترجاعها.
- بروتوكول المصادقة: يحدد هذا الأسلوب المستخدم للتحقق من ملكية المجال. والبروتوكول المدعوم لتحديات ACME هو HTTP-01.
- واجهة المصادقة: واجهة الشبكة على جهاز FTD الذي يستقبل تحدي HTTP-01 من خادم ACME.
- شهادة CA فقط: يجب إختيار شهادة من مرجع مصدق (CA) للثقة في خادم ACME.

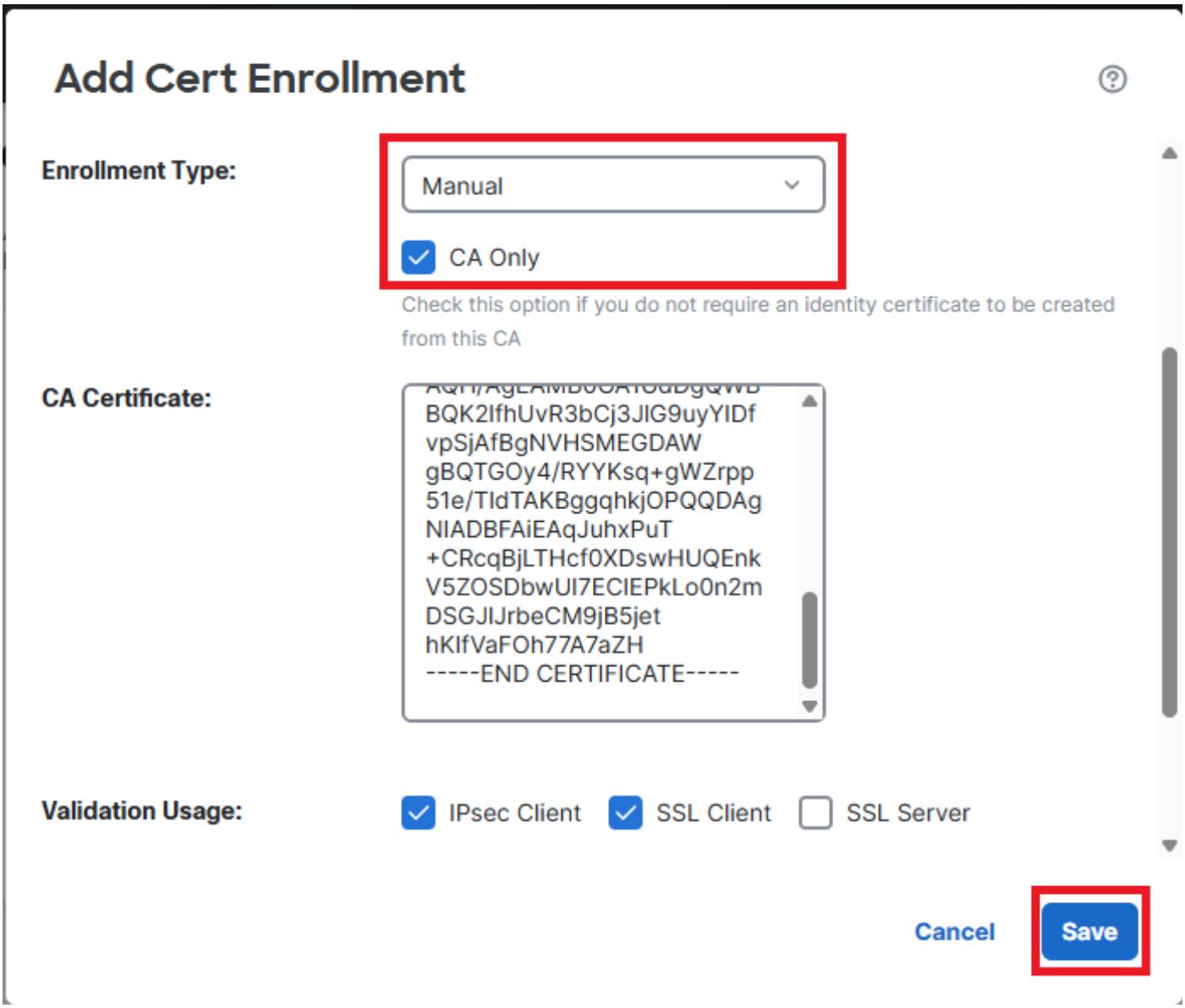
ملاحظة: بشكل افتراضي، يشير إلى عنوان URL الخاص بخدمة التشفير العامة: https://acme-v02.api.letsencrypt.org/directory.

---

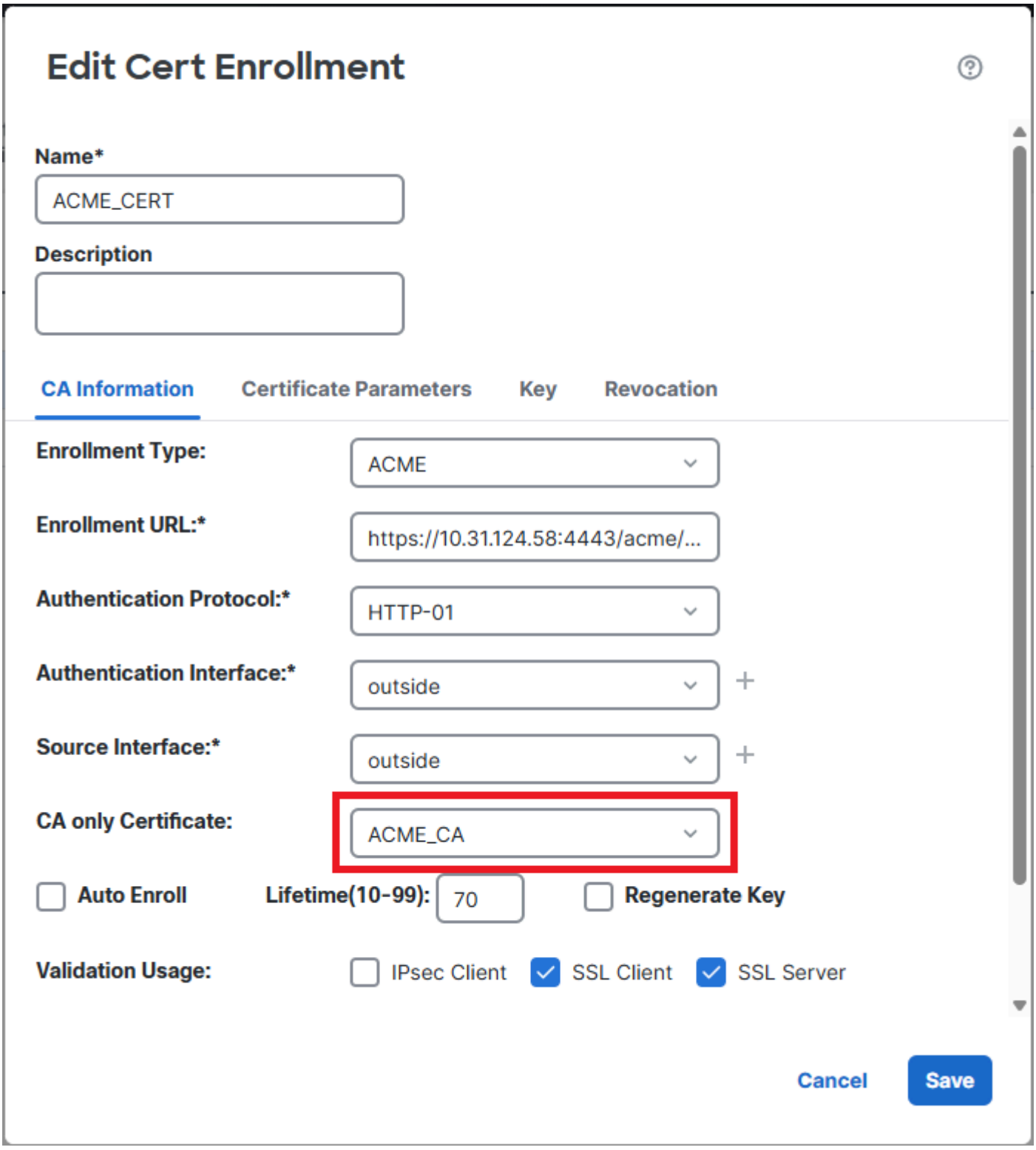
4. إذا كنت تستخدم خادم ACME غير معروف جيدا، فأنت بحاجة إلى إضافة شهادة CA لخادم ACME. انتقل إلى الكائنات > تسجيل الاقتران وانقر فوق الزر إضافة تسجيل الاقتران.



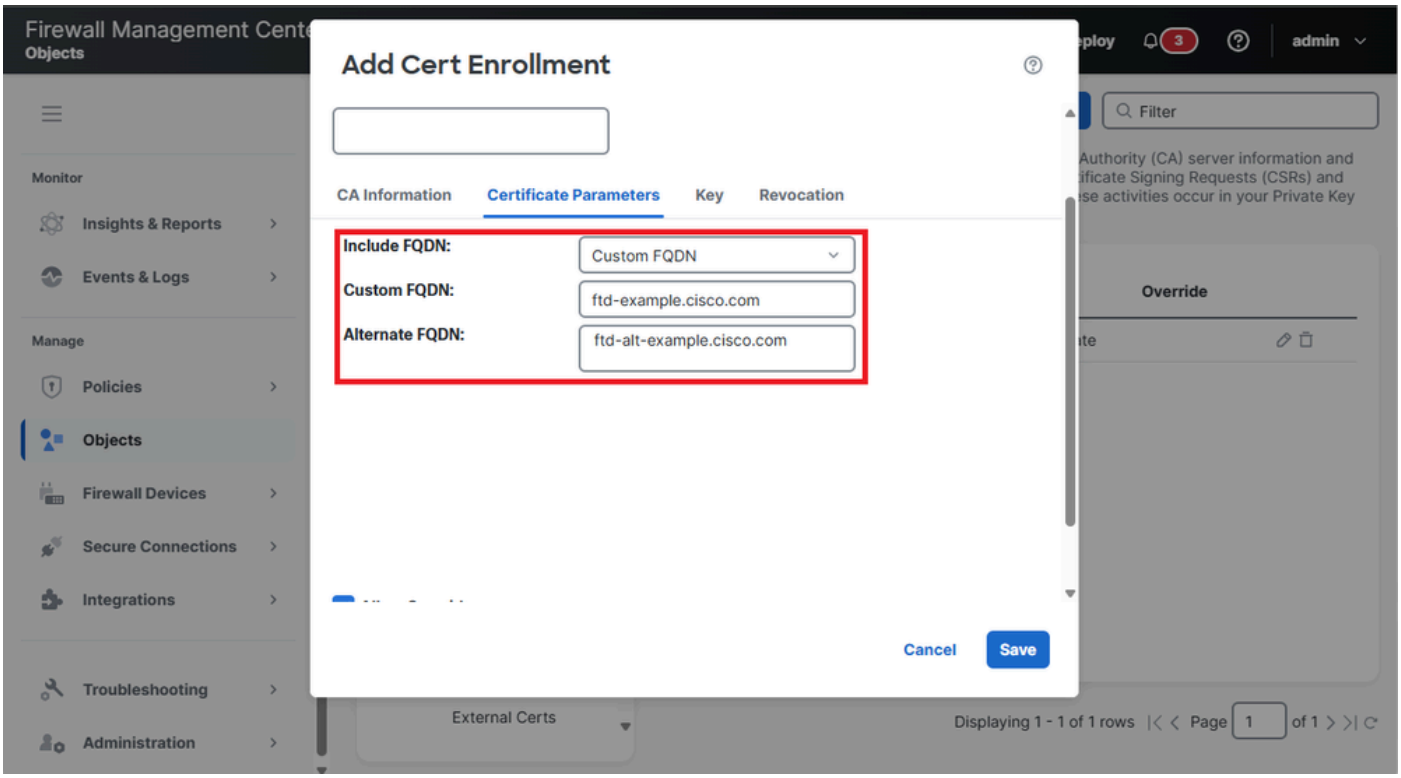
- قم بتسمية TrustPoint وحدد نوع التسجيل ك Manual. بعد ذلك، تحقق من الخيار CA فقط. أخيرا، الصق شهادة ACME Server CA وانقر فوق حفظ.



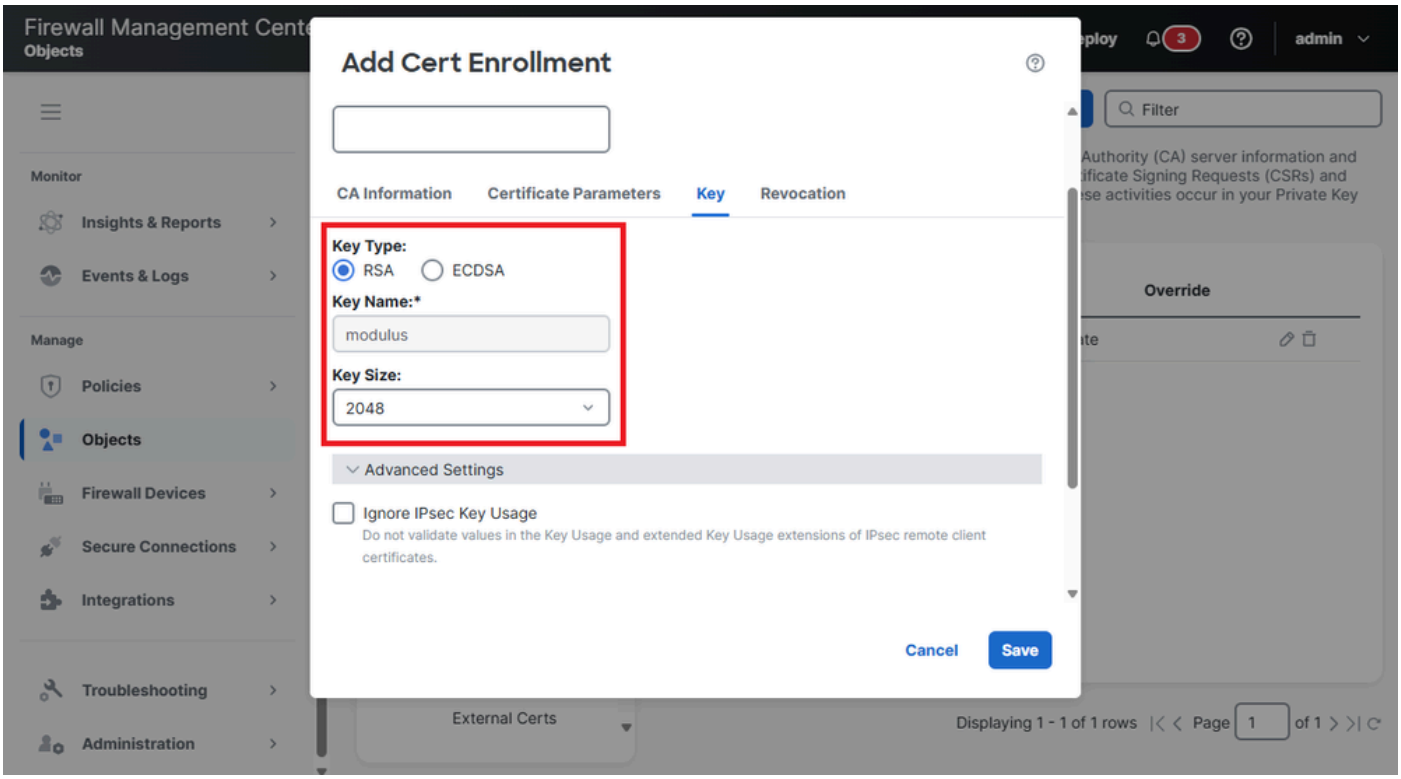
- أخيرا، حدد TrustPoint الخاص بخادم ACME CA في قسم ترخيص CA فقط.



5. انتقل إلى معلمات الشهادة، وحدد خيار FQDN المخصص في مربع تضمين FQDN، وقم بتعبئة حقلي FQDN المخصص وFQDN البديل مع FQDN الأساسي وأي أسماء مجالات بديلة لتضمينها في الشهادة.



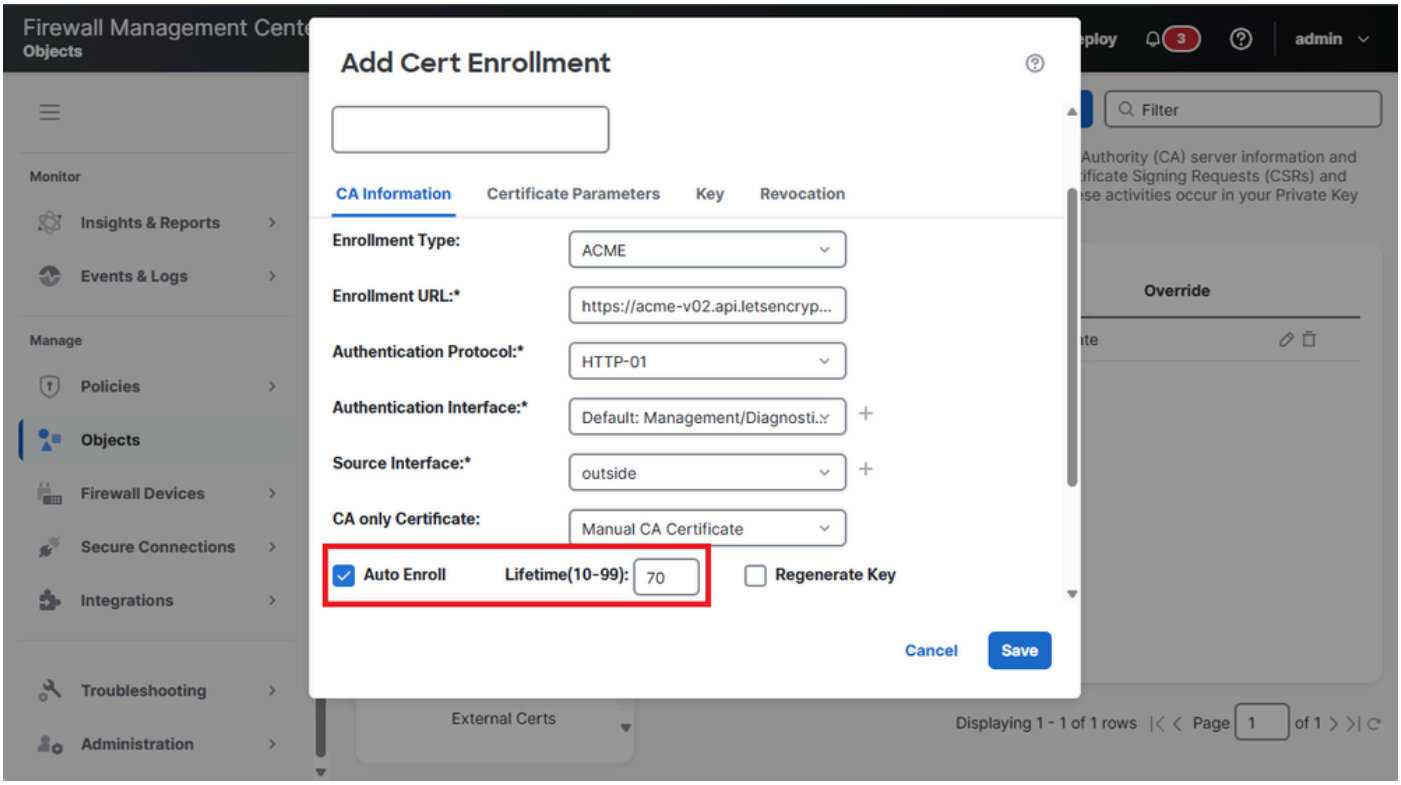
6. انتقل إلى المفتاح لتعديل إعدادات نوع المفتاح وحجم المفتاح.



7. (إختياري) قم بتمكين التسجيل التلقائي لشهادة الهوية.

حدد خانة الاختيار Auto Registration وحدد النسبة المئوية لفترة بقاء التسجيل التلقائي.

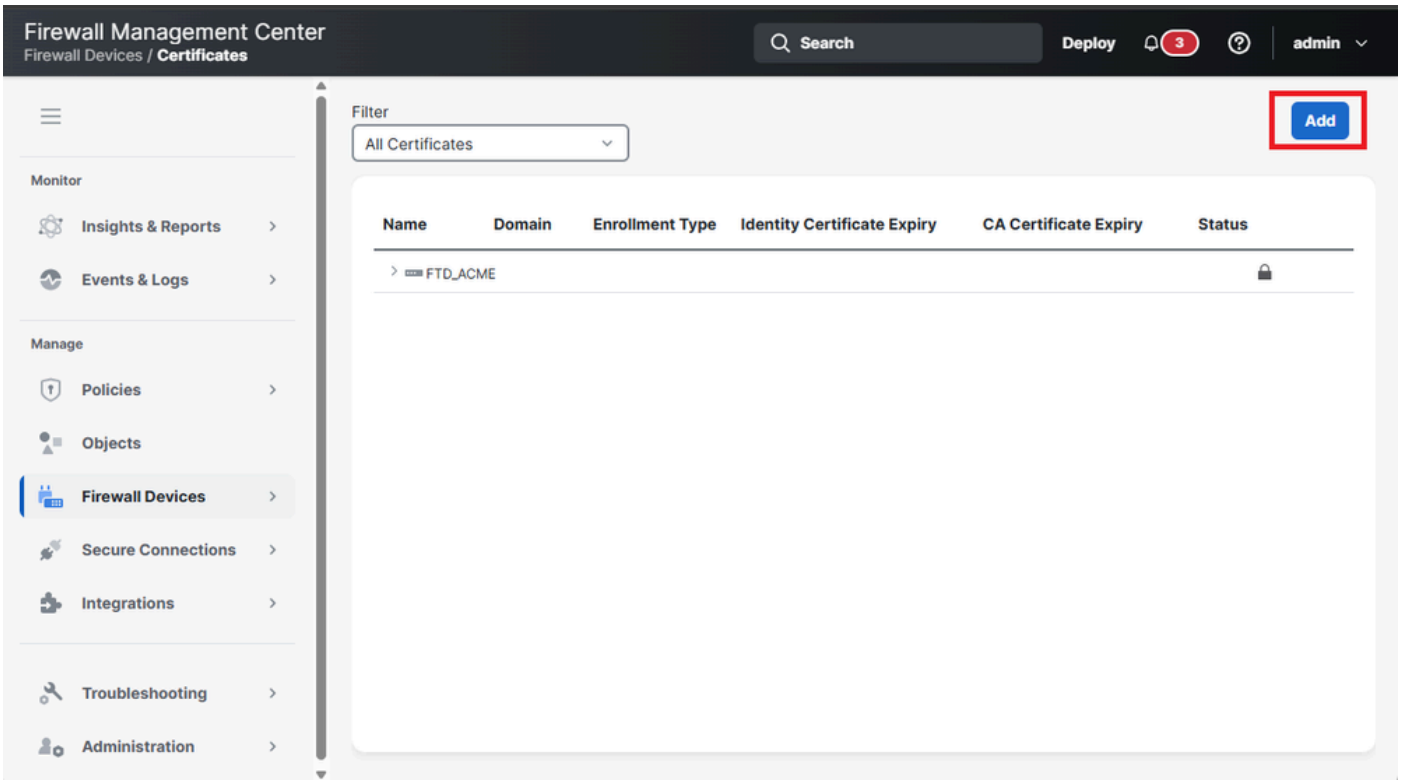
تضمن هذه الميزة تجديد الشهادة تلقائيا قبل انتهاء صلاحيتها. تحدد النسبة المئوية الفترة التي تسبق انتهاء صلاحية الشهادة التي تبدأ فيها عملية التجديد. على سبيل المثال، إذا تم تعيينها على 80٪، تبدأ عملية التجديد عندما تصل الشهادة إلى 80٪ من فترة صلاحيتها.



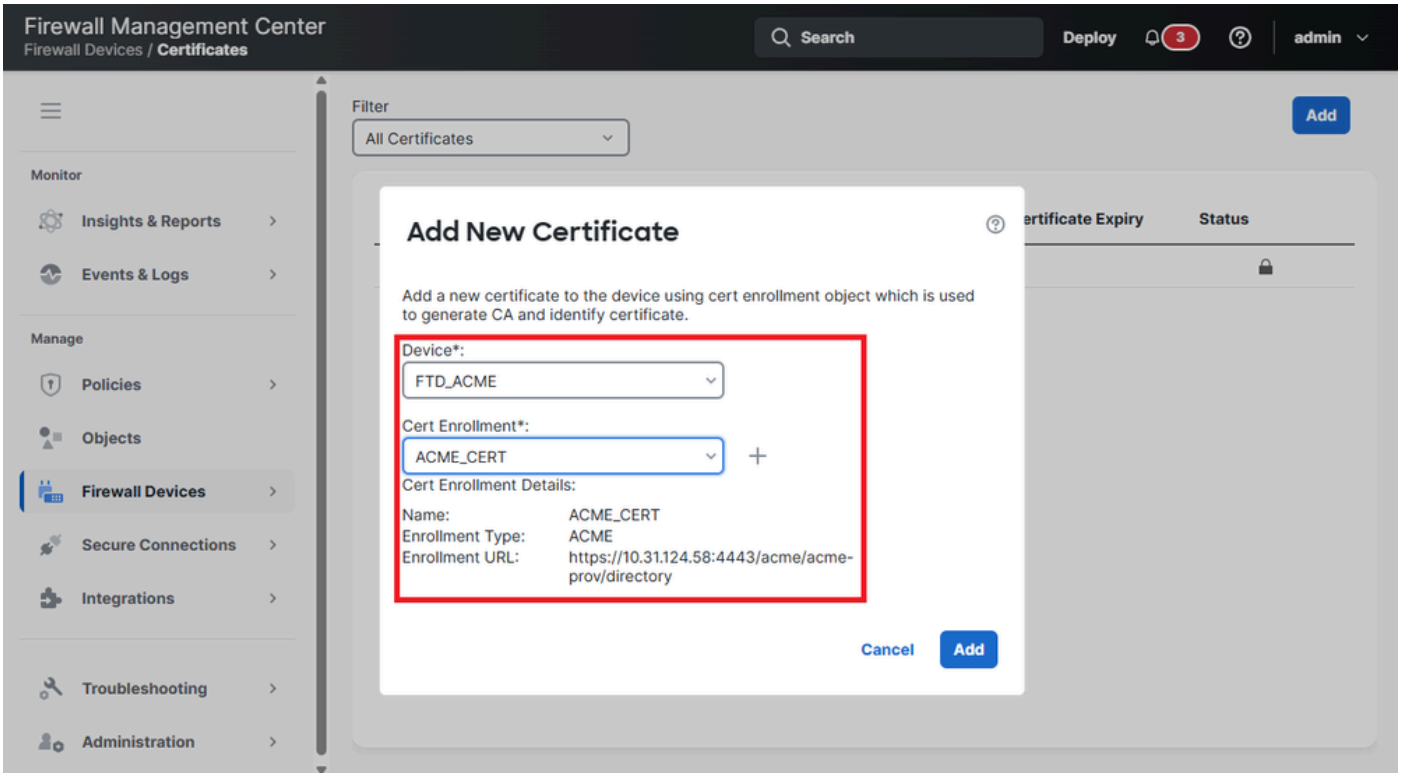
8. انقر فوق حفظ.

تسجيل شهادة ACME على الجهاز

1.انتقل إلى أجهزة جدار الحماية > الشهادات وانقر فوق الزر إضافة لتسجيل شهادة جديدة.

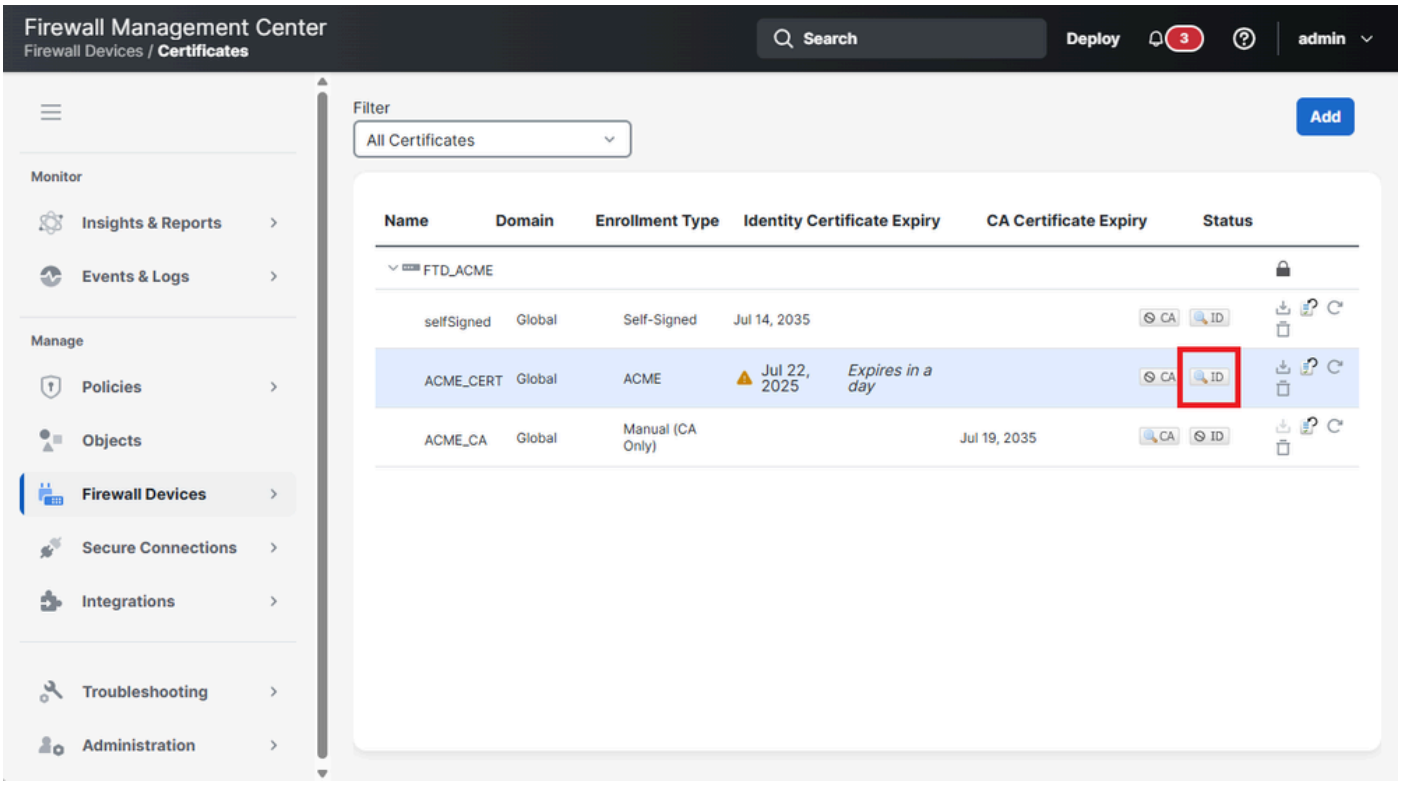


2. حدد جهاز FTD من القائمة المنسدلة الجهاز وكائن الشهادة الذي تم إنشاؤه مسبقا في تسجيل المنتج.

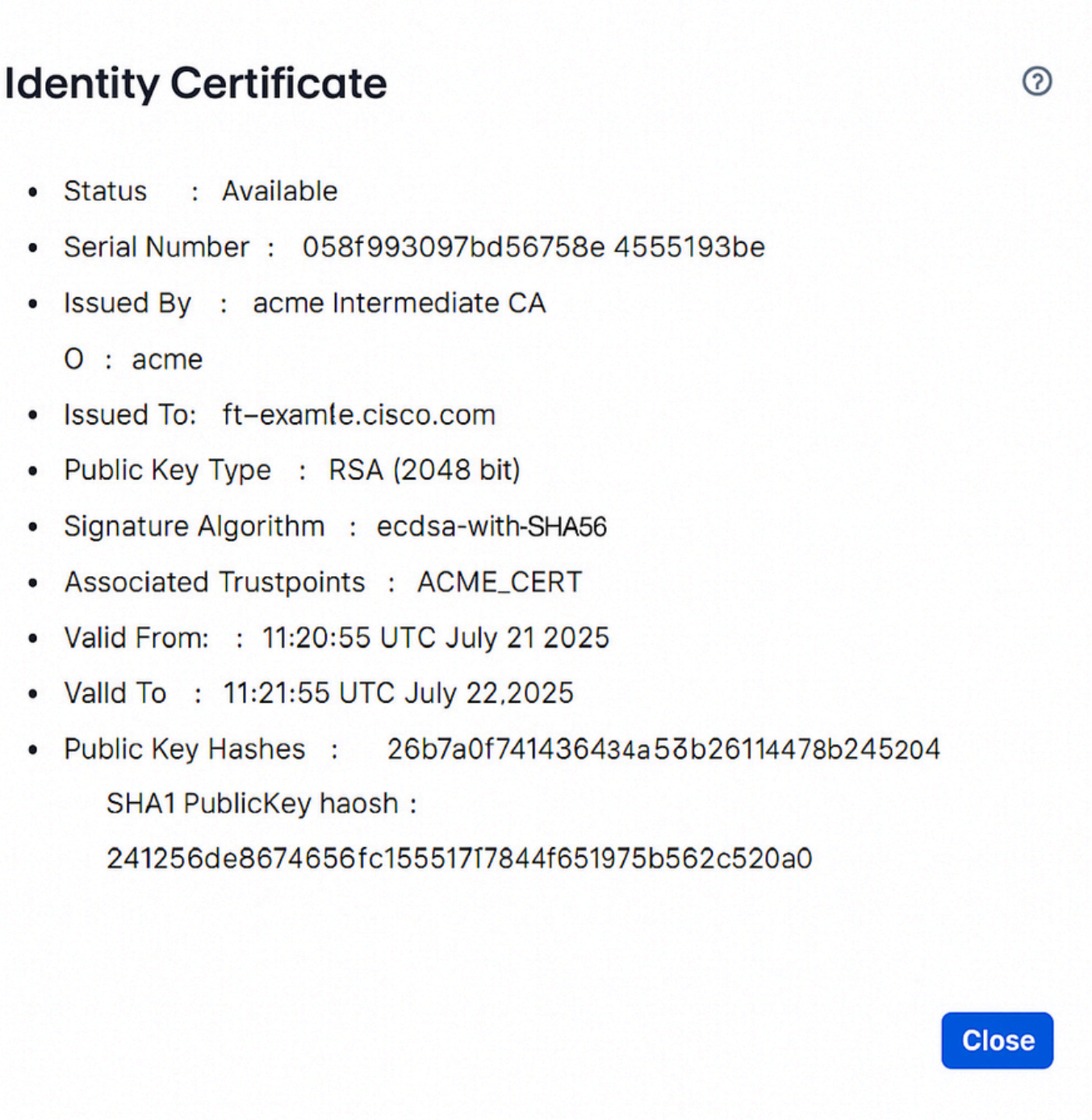


3. انقر فوق إضافة.

4. بمجرد اكتمال النشر، يعرض عمود الحالة زر شهادة المعرف.



5. تحقق من صحة معلومات شهادة المعرف بالنقر على زر المعرف.



التحقق من الصحة

عرض الشهادة المثبتة في FTD

تأكد من أن الشهادة مسجلة في الأمر.show crypto ca certificates <trust point name>.

```
<#root>

firepower#
```

```
show crypto ca certificates
```

```
ACME_CERT
```

```
Certificate
Status: Available
Certificate Serial Number: 058f993097bd56758e44554194a953be
Certificate Usage: General Purpose
Public Key Type: RSA (2048 bits)
Signature Algorithm: ecdsa-with-SHA256
Issuer Name:
CN=acme Intermediate CA
O=acme
Subject Name:
CN=ftd-example.cisco.com
Validity Date:
start date: 11:20:55 UTC Jul 21 2025
end date: 11:21:55 UTC Jul 22 2025
Storage: immediate
Associated Trustpoints: ACME_CERT
Public Key Hashes:
SHA1 PublicKey hash: 26b7a0f7414364a45b246114478bb74f432520c4
SHA1 PublicKeyInfo hash: 24125d6e8674566c1551784f651975b562c520a
```

أحداث Syslog

هناك syslogs جديدة في FTD لجدار الحماية الآمن لالتقاط الأحداث المتعلقة بتسجيل ACME: باستخدام بروتوكول الشهادة

- 717067: يوفر معلومات عن متى يبدأ تسجيل شهادة ACME.

```
%FTD-5-717067: Starting ACME certificate enrollment for the trustpoint <private_acme> with CA <ca-acme.e
```

- 717068: يوفر معلومات عن وقت نجاح تسجيل شهادة ACME.

```
%FTD-5-717068: ACME Certificate enrollment succeeded for trustpoint <private_acme> with CA <ca-acme.exa
```

- 717069: يوفر معلومات حول وقت فشل تسجيل ACME.

```
%FTD-3-717069: ACME Certificate enrollment failed for trustpoint <private_acme>
```

- 717070: توفر معلومات متعلقة بزوج المفاتيح لتسجيل الشهادة أو تجديد الشهادة.

```
%FTD-5-717070: Keypair <Auto.private_acme> in the trustpoint <private_acme> is regenerated for <manual>
```

استكشاف الأخطاء وإصلاحها

إذا فشل تسجيل شهادة ACME، فقم بالتفكير في الخطوات التالية لتعريف المشكلة وحلها:

- تحقق من الاتصال بالخادم: تأكد من أن جدار الحماية الآمن لديه اتصال شبكة بخادم ACME. تحقق من عدم وجود مشاكل في الشبكة أو قواعد جدار الحماية التي تمنع الاتصال.
- تأكد من أن اسم مجال جدار الحماية الآمن قابل للحل: تأكد من أن اسم المجال الذي تم تكوينه على جدار الحماية الآمن FTD قابل للحل بواسطة خادم ACME. يعد هذا التحقق من الصحة أمرا بالغ الأهمية للخادم للتحقق من صحة الطلب.
- تأكيد ملكية المجال: تحقق من أن كافة أسماء المجالات المحددة في TrustPoint مملوكة ملكية صحيحة للجدار الآمن FTD. وهذا يضمن أن خادم ACME يمكنه التحقق من ملكية المجال.

أوامر استكشاف الأخطاء وإصلاحها

للحصول على معلومات إضافية، قم بتجميع مخرجات أوامر تصحيح الأخطاء التالية:

- debug crypto ca acme <1-255>
- debug crypto ca <1-14>

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).