تكوين الوصول الآمن ل ZTNA العالمية باستخدام FMC المدار على SCC

المحتويات

المقدمة

يصف هذا المستند كيفية تكوين ZTNA العالمية باستخدام Secure Access و FTD الظاهري الذي تتم إدارته بواسطة FMC الظاهري على الإنترنت.

المتطلبات الأساسية

- يجب نشر مركز إدارة جدران الحماية (FMC) والدفاع عن التهديد باستخدام جدار الحماية (FTD) باستخدام إصدار برنامج 7.7.10 أو إصدار أحدث.
- يجب أن تتم إدارة ميزة الحماية ضد تهديدات جدار الحماية (FTD) من خلال مركز إدارة جدار الحماية (FMC)

- يجب ترخيص برنامج الدفاع عن تهديد جدار الحماية (FTD) باستخدام تشفير (يجب تمكين التشفير القوي مع تمكين ميزة التصدير) ونظام منع الاختراقات (IPS) وتراخيص التهديدات المطلوبة لملفات الأمان.
- يجب إجراء التكوين الأساسي على الدفاع ضد تهديد جدار الحماية (FTD) من مركز إدارة جدار الحماية (FMC) مثل الواجهة والتوجيه وما إلى ذلك.
- يلزم تطبيق تكوين DNS على الجهاز من FMC's لحل FQDN الخاص بالتطبيق
- يلزم أن يكون إصدار Cisco Secure Client هو 5.1.10 وأعلى
- يتم توفير التحكم في سحابة الأمان للعملاء الذين لديهم تطبيقات Firewall و ميزات UZTNA المتكاملة أو Secure Access Micro

المتطلبات

- يجب أن تقوم جميع أجهزة مركز إدارة جدار الحماية الآمن (FMC) بما في ذلك أجهزة CDfmc و Firewall Threat Defense (FTD) بتشغيل الإصدار 7.7.10 من البرنامج أو إصدار أحدث.
- يجب أن تتم إدارة برنامج الدفاع عن تهديد جدار الحماية (FTD) من خلال مركز إدارة جدار الحماية؛ مدير الدفاع عن جدار الحماية (FDM) للمدير المحلي غير مدعوم
- يجب تكوين جميع أجهزة الدفاع عن تهديد جدار الحماية (FTD) للوضع الموجه؛ الوضع الشفاف غير مدعوم.
- الأجهزة المجمعة غير معتمدة.
- أجهزة عالية التوفر (HA) مدعومة؛ يتم عرضها كياناً واحداً.
- Secure Client الإصدار 5.1.10 أو إصدار أحدث

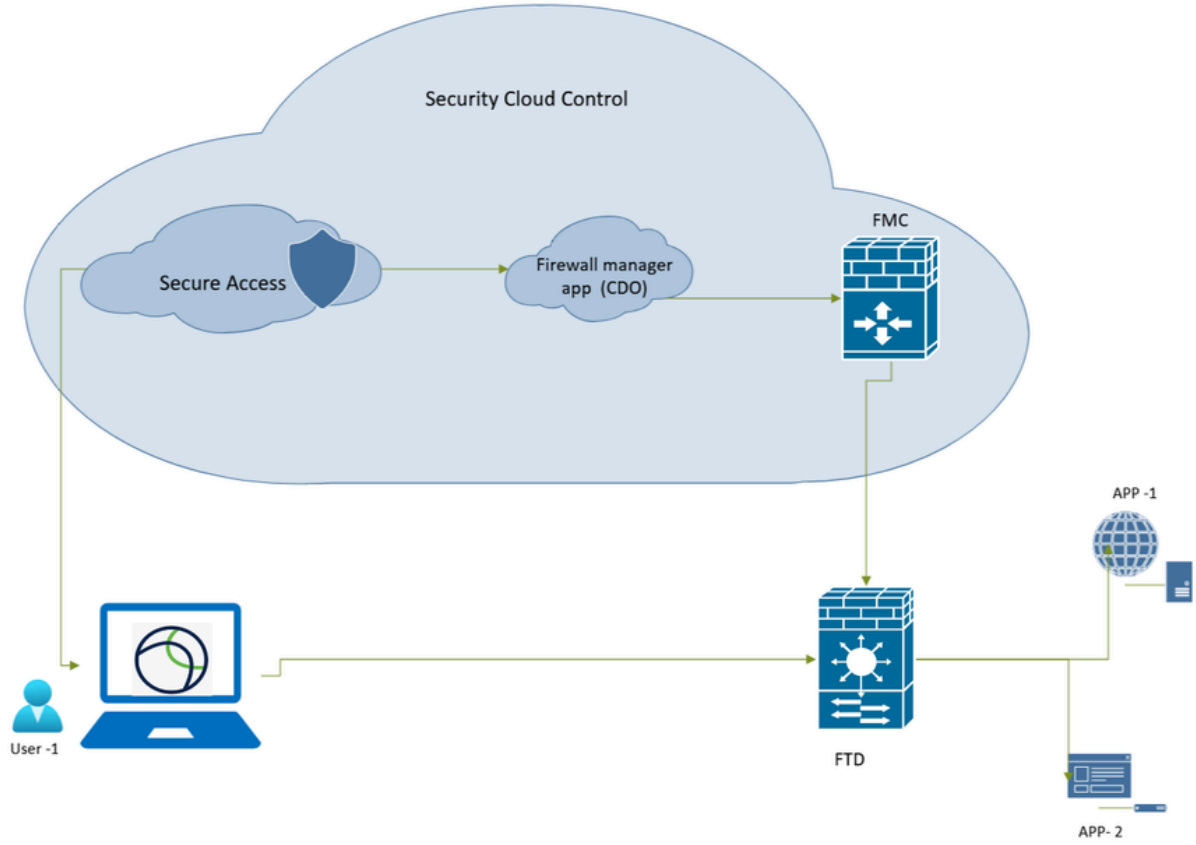
المكونات المستخدمة

تستند المعلومات الواردة في هذا المستند إلى

- التحكم في سحابة الأمان (SCC)
- مركز إدارة جدار الحماية الآمن (FMC)، الإصدار 7.7.10
- Secure Firewall Threat Defense (FTD) virtual -100 الإصدار 7.7.10
- Secure Client لنظام التشغيل Windows الإصدار 5.1.10
- الوصول الآمن

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.

الرسم التخطيطي للشبكة



الوصول الآمن - مخطط الشبكة

معلومات مكيفة

الأجهزة المدعومة

نماذج الدفاع المدعومة ضد تهديد جدار الحماية الآمن:

- FPR 1150
- FPR 3105 و 3110 و 3120 و 3130 و 3140
- FPR4115,4125,4145,4112
- FPR4215,4225,4245
- جهاز الدفاع ضد تهديدات الجدار الناري (FTD) افتراضي مع 16 مركزا من مراكز وحدة المعالجة المركزية (CPU) كحد أدنى

القيود

- مشاركة العنصر
- IPv6 غير مدعوم.
- يتم دعم VRF العمومي فقط.
- لا يتم فرض سياسات ZTNA العالمية على حركة مرور النفق من موقع إلى موقع إلى جهاز .

- الأجهزة المجمعة غير معتمدة.
- لا يتم دعم ملفات FTD التي يتم نشرها كحاويات على سلسلة FirePOWER بسرعة 4 و 9 كيلو

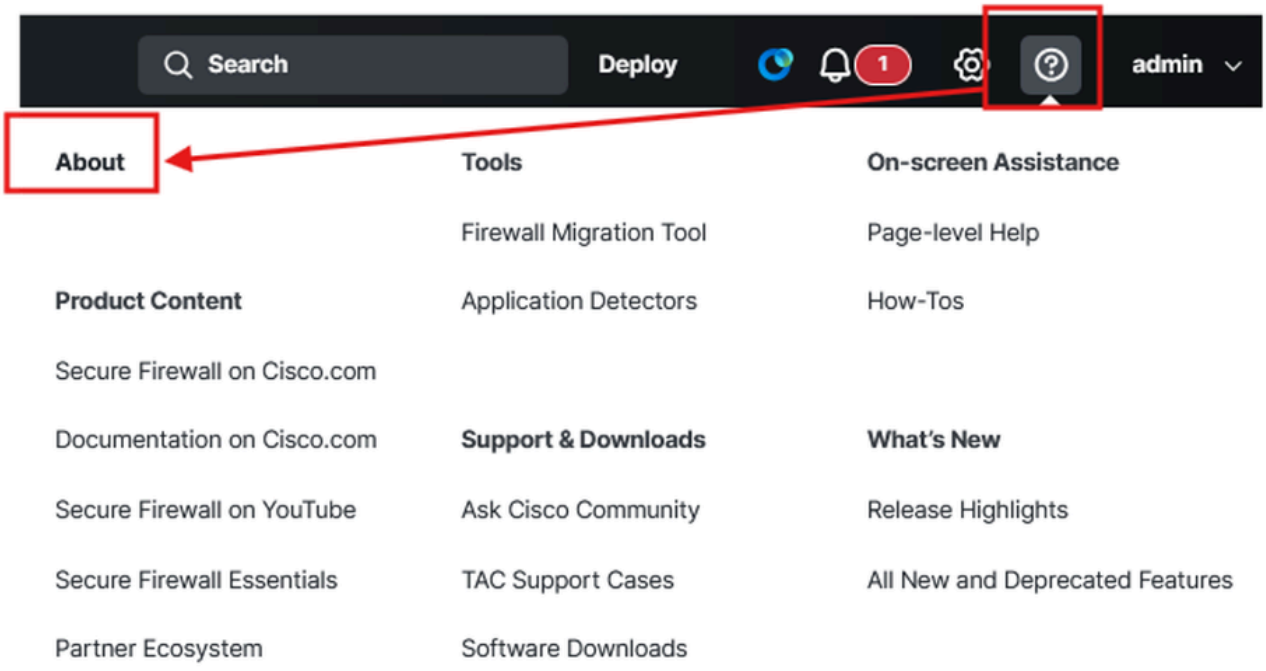
- لا تدعم جلسات ZTNA العامة إطارات Jumbo

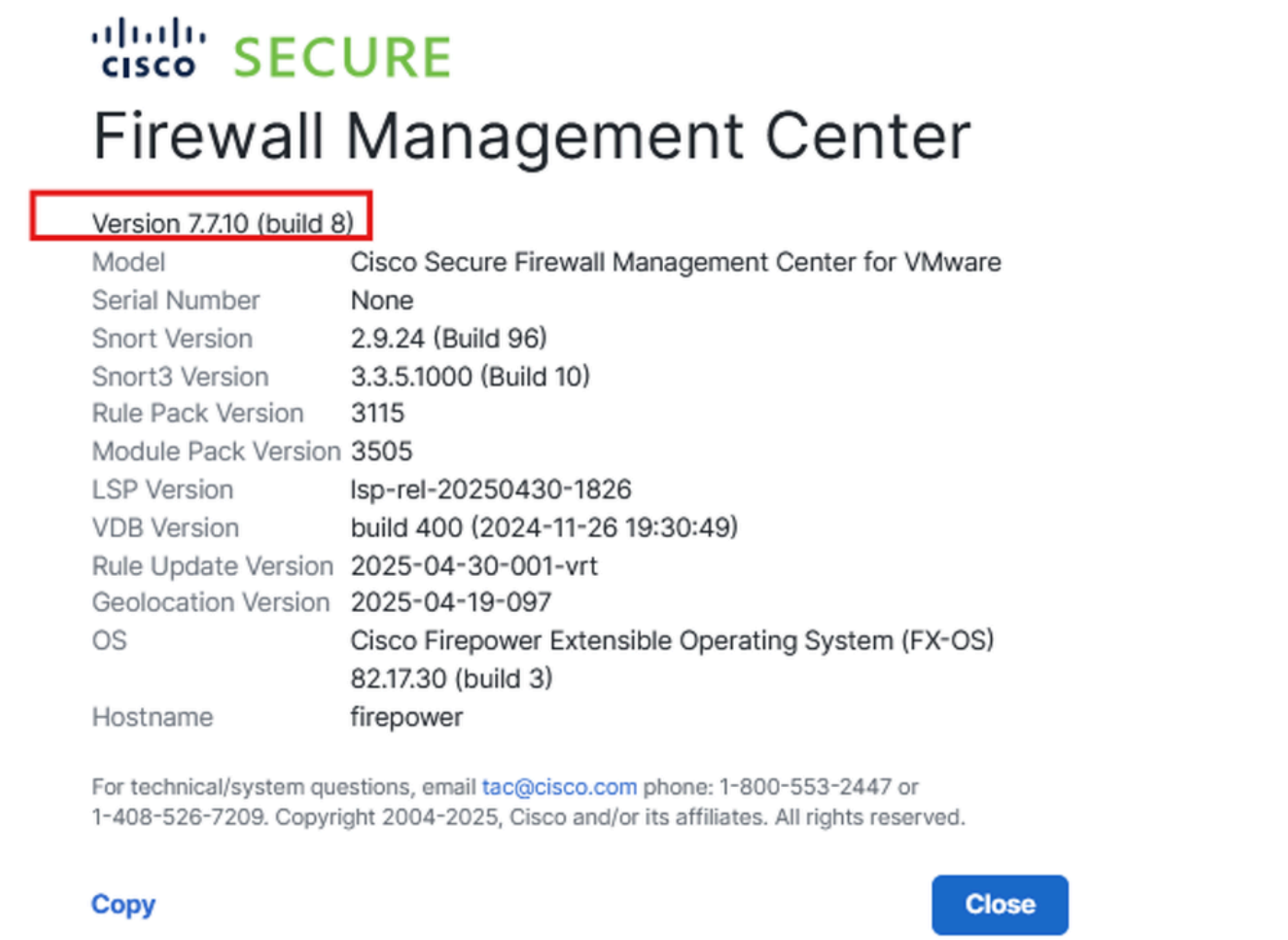
التكوين

التحقق من إصدار FMC

تحقق من تشغيل مركز إدارة جدار الحماية وبرنامج FTD لجدار الحماية على إصدار البرنامج المدعوم ل ZTNA العالمية (يمكن أن يكون 7.7.10 أو أعلى):

- انقر فوق?(الزاوية العلوية اليمنى) وانقر فوق About



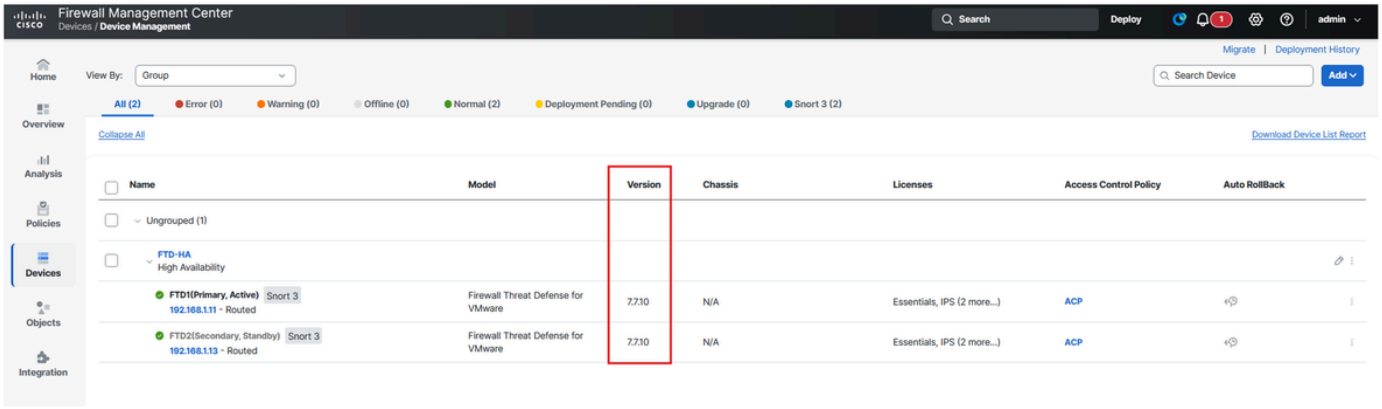


مركز إدارة جدار الحماية الآمن - إصدار البرامج

التحقق من إصدار FTD

انتقل إلى واجهة مستخدم FMC:

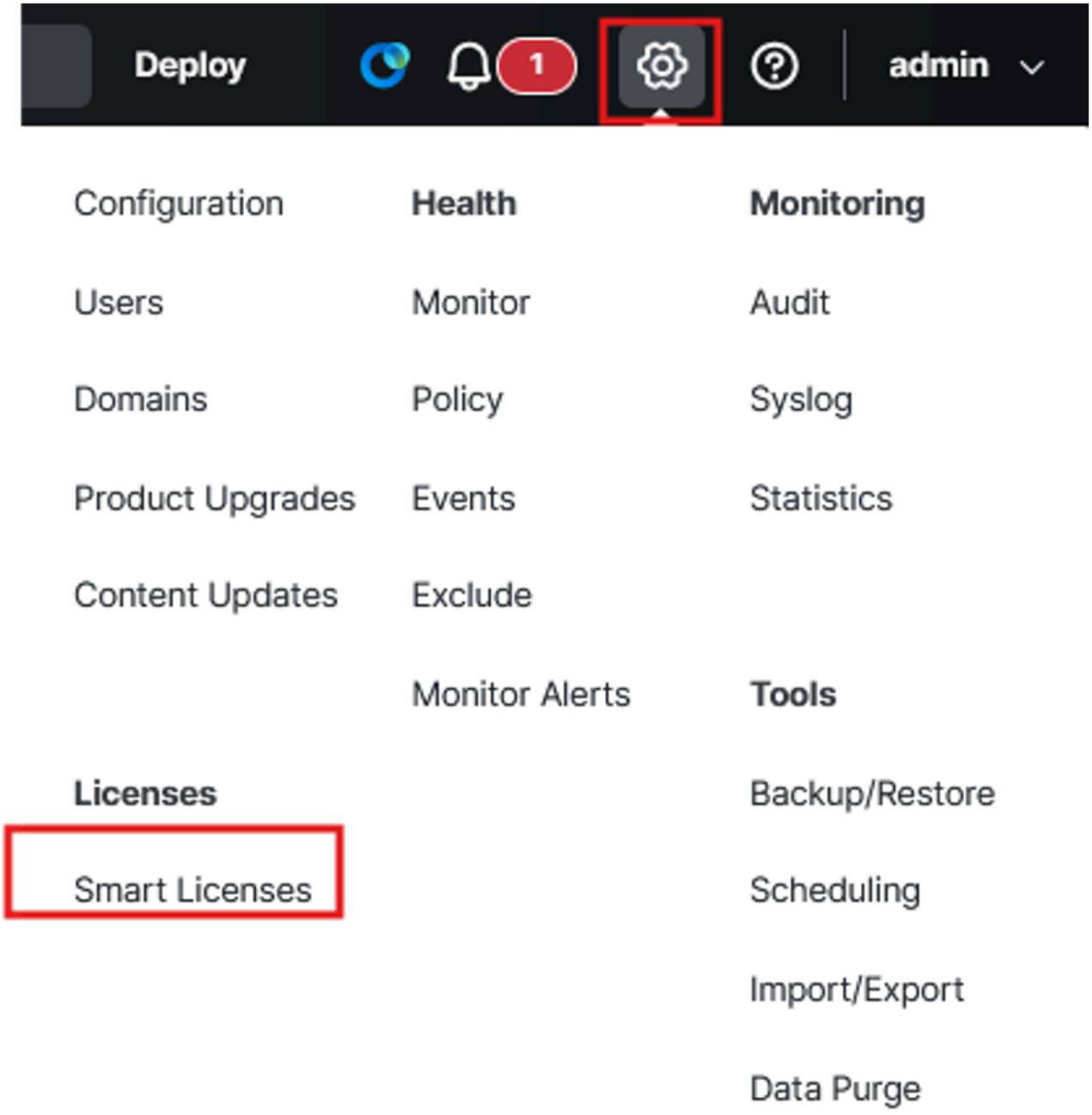
- انقر فوقDevices> Device Management

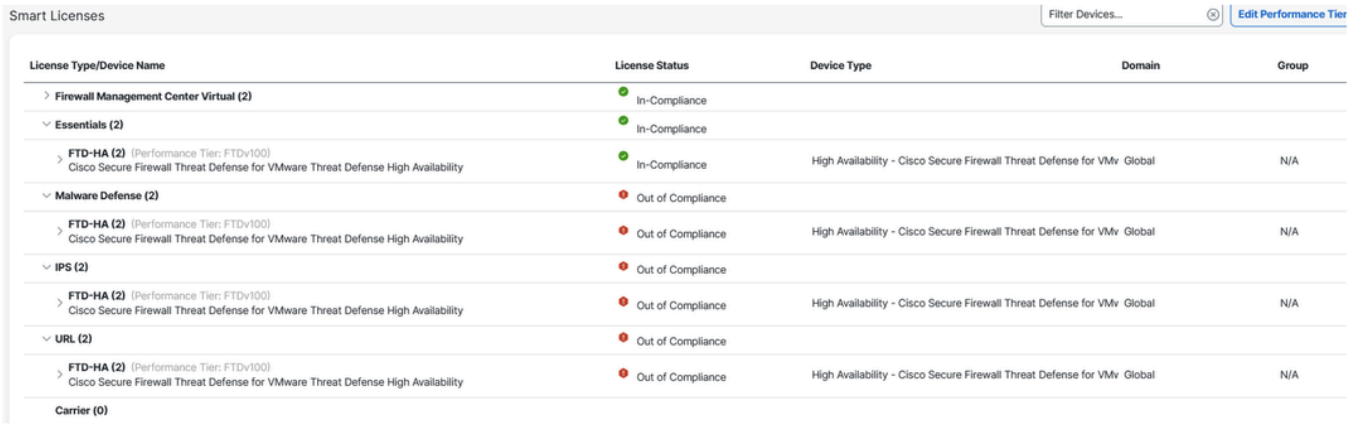


الدفاع الآمن ضد تهديد جدار الحماية - إصدار البرامج

التحقق من ترخيص FTD

- انقر فوقSetting Icon> Licenses> Smart Licenses





الدفاع الآمن ضد التهديد باستخدام جدار الحماية - تراخيص ذكية

التحقق من إعدادات النظام الأساسي DNS التي تم تكوينها بشكل صحيح

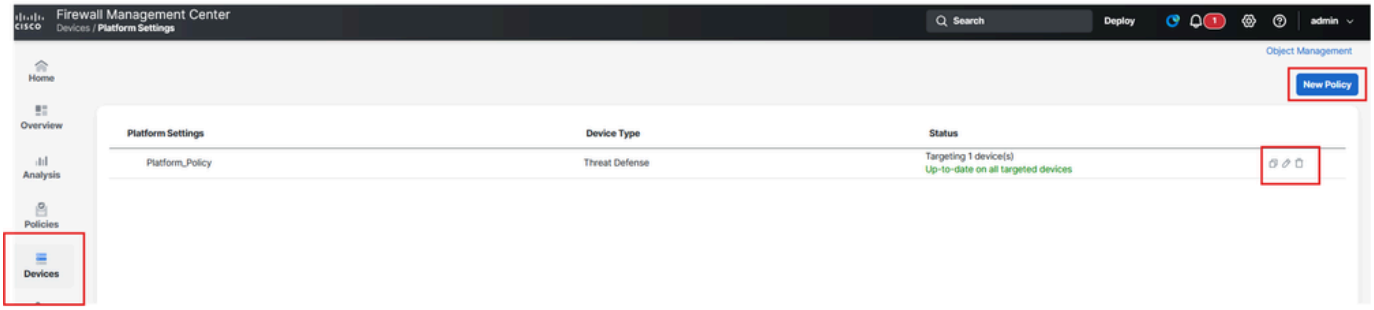
التسجيل إلى FTD عبر CLI:

- قم بتشغيل الأمر للتحقق من تكوين DNS:

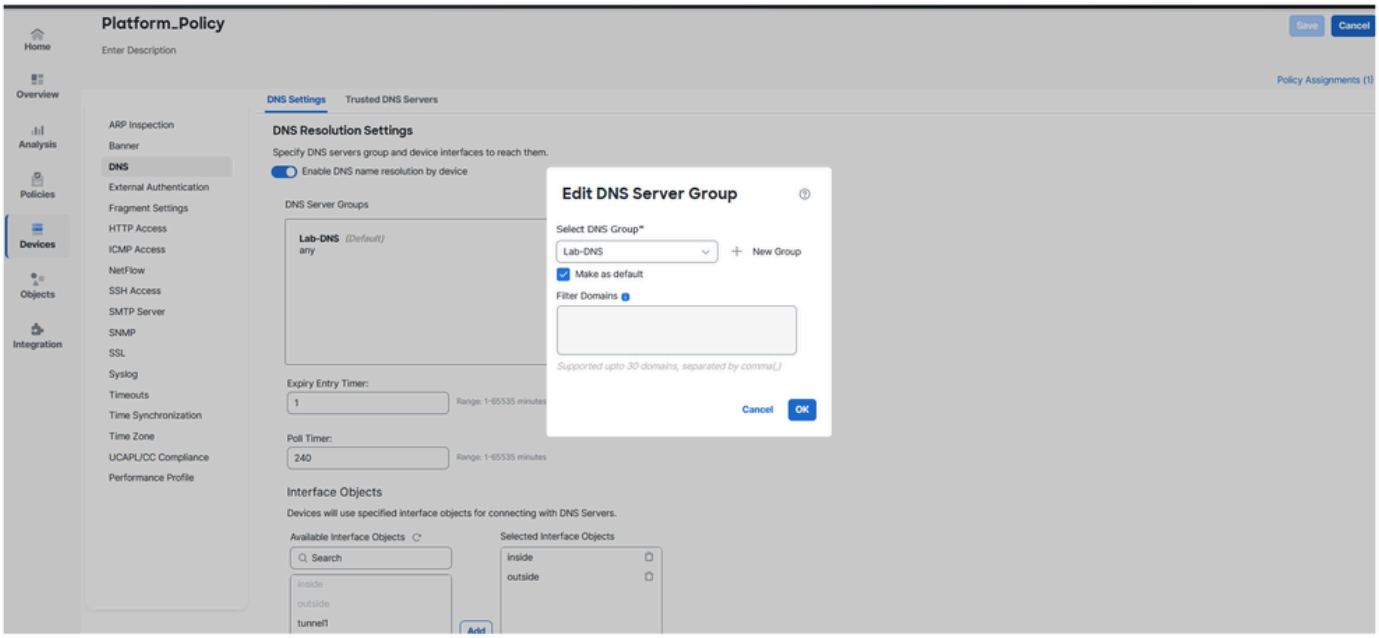
```
show run dns
```

في FMC:

- انقر فوقDevices>Platform Settings، أو قم بتحرير أو إنشاء سياسة جديدة



الدفاع الآمن ضد تهديد جدار الحماية - سياسة النظام الأساسي



الدفاع الآمن عن تهديد جدار الحماية - تكوين DNS

تحقق من خلال واجهة سطر أوامر (CLI) خاصة ب FTD أنه يمكنك إختبار اتصال عنوان IP الخاص و FQDN (إذا كنت ترغب في الوصول إلى PR باستخدام FQDN الخاص به).

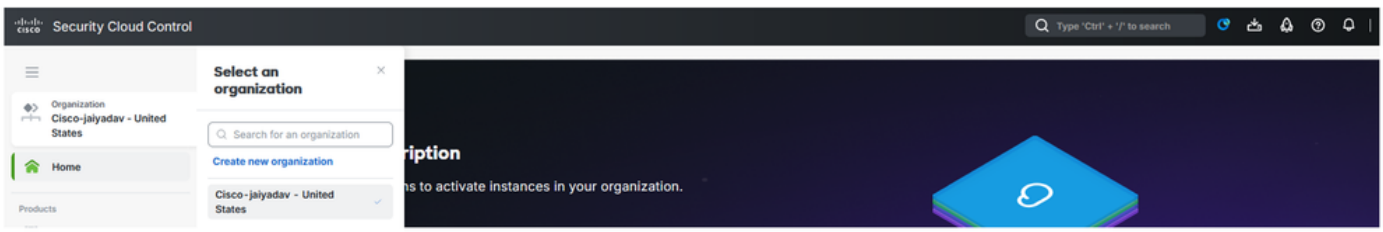
```
dns-group Lab-DNS
ftd1# ping ise.taclab.com
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.10.10.50, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
ftd1#
```

إنشاء مستأجر عنصر تحكم سحابة أمان على CDO

ملاحظة: إذا كان لديك بالفعل مستأجر SCC تم تكوينه، فلن يكون عليك إنشاء مستأجر جديد.

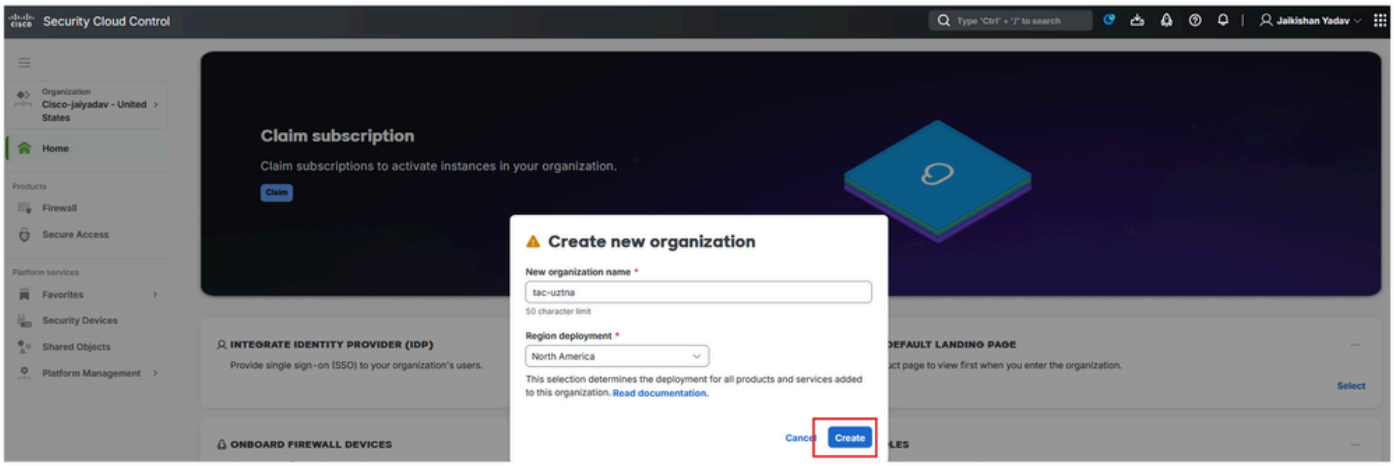
انتقل إلى التحكم في سحابة الأمان:

- انقر فوقOrganization> Create new organization



التحكم في السحابة الآمنة - المؤسسة

- انقر فوق Create



التحكم في السحابة الآمنة - إنشاء المؤسسة

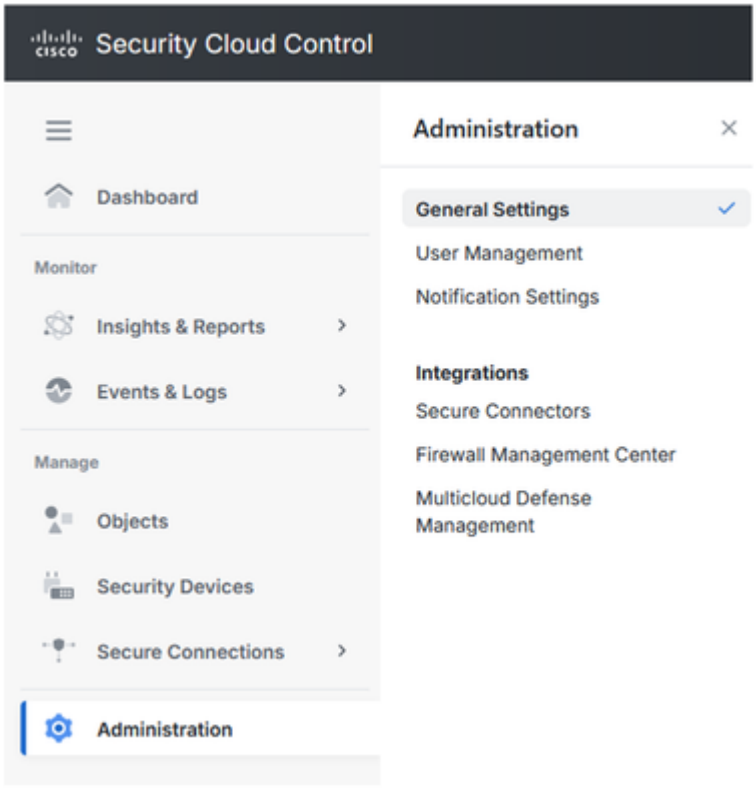
بمجرد إنشاء مستأجر SCC، قم بتجميع معلومات المستأجر لتمكين Firewall و Secure Access Microapp وتمكين uZTNA.

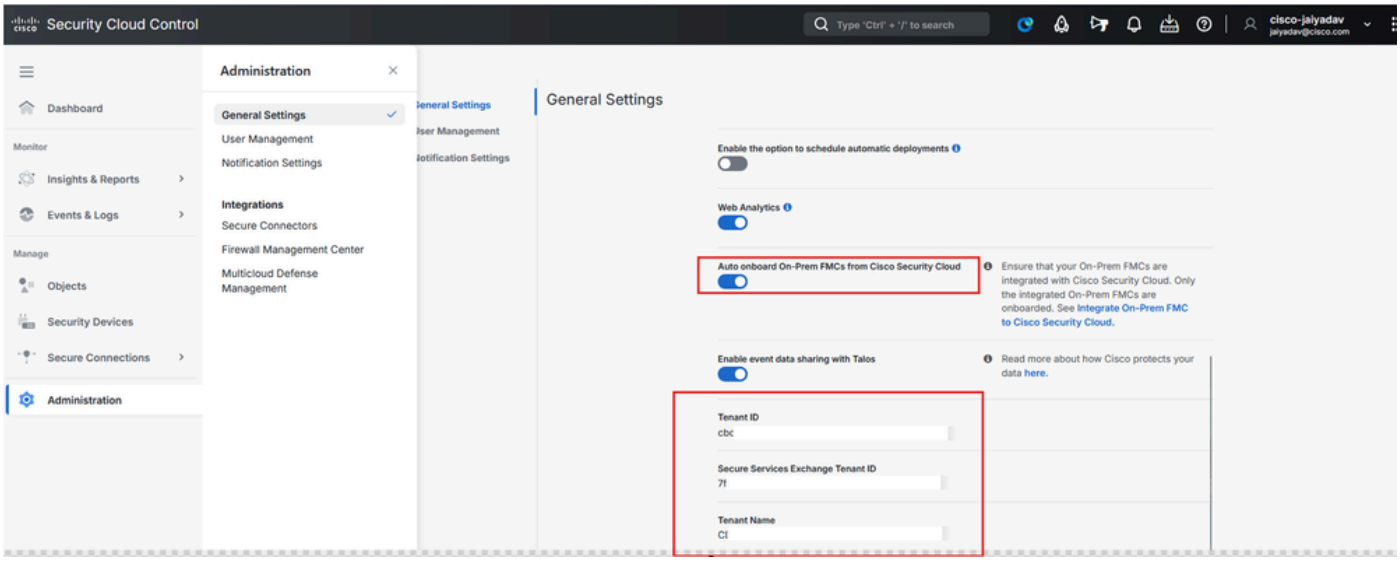
التأكد من تكوين الإعدادات العامة لجدار حماية SCC

انتقل إلى CDO/SCC:

- انقر فوقAdministration> General Settings
- تأكد من تمكينAuto onboard On-Prem FMCs from Cisco Security Cloudالخيار.

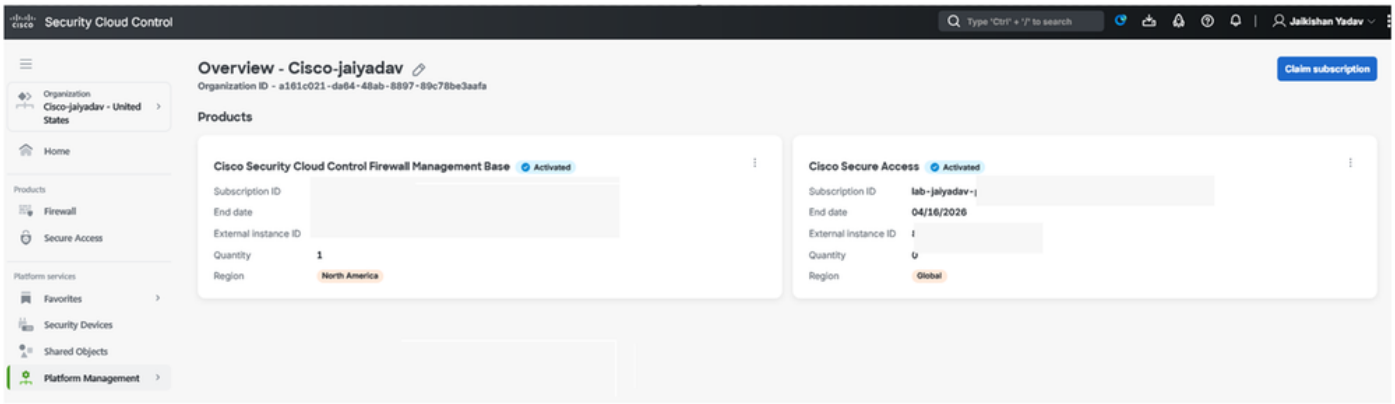
ملاحظة: يجب أن يكون للمستخدم الذي يحاول الوصول إلى Secure Access MicroAppSecure Accessوأدوار Security Cloud Control المسؤول.





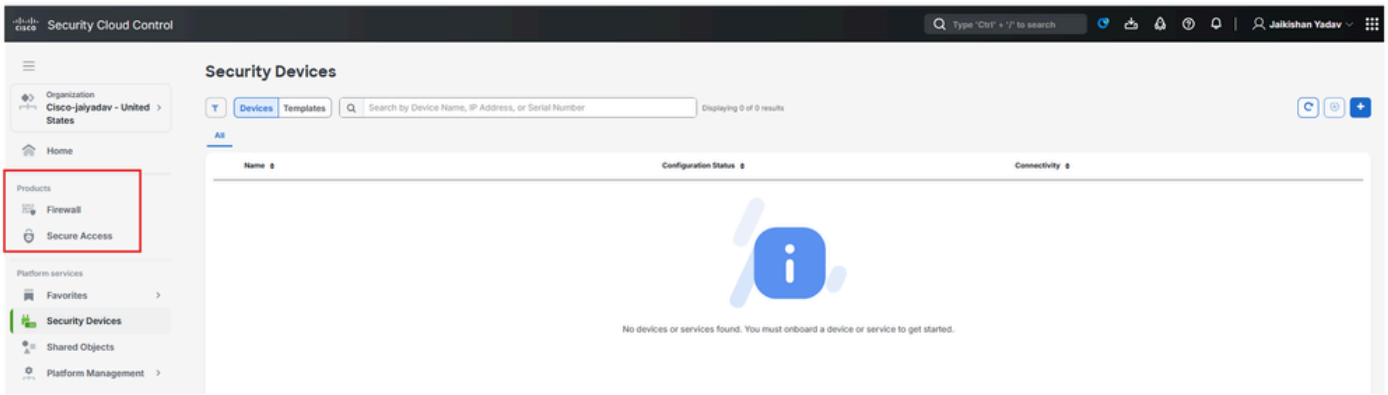
التحكم في السحابة الآمنة - تفاصيل المؤسسة

التحقق من تكامل قاعدة إدارة جدار حماية التحكم في الوصول الآمن ومستأجر الوصول الآمن



التحكم في السحابة الآمنة - تنشيط الوصول الآمن

بمجرد اكتمال الخطوة [إنشاء مستأجر التحكم في سحابة الأمان على CDO](#) و[إنشاء مستأجر التحكم في سحابة الأمان على CDO](#)، يمكنك حينئذ رؤية تطبيقات Firewall و Secure Access micro على لوحة معلومات SCC:



التحكم الآمن في السحابة - تطبيقات Micro

إنشاء شهادة CA موقعة ذاتيًا لتمديدات جدار الحماية (FTD)

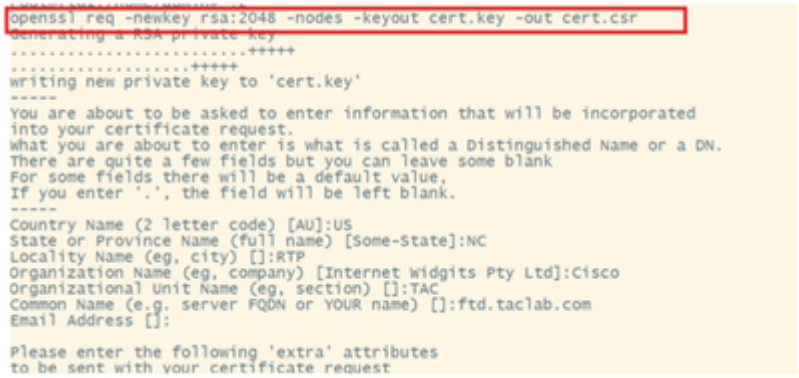
ملاحظة: يمكنك أيضا استخدام شهادات FTD ذاتية التوقيع (راجع قسم إنشاء شهادات CA الداخلية والداخلية ذاتية التوقيع). يجب أن يكون Cerficiate بتنسيق PKCS12 ويجب أن يكون موجودا في مخزن أجهزة المستخدم تحت مرجع مصدق مركزي موثوق به.

لإنشاء شهادة موقعة من CA باستخدام FTD في ميزة إنشاء OpenSSL:

- الاتصال إلى FTD
- أمر تشغيلexpert

- إنشاء CSR والمفاتيح باستخدام OpenSSL
  - أمر OpenSSL:

```
openssl req -newkey rsa:2048 -nodes -keyout cert.key -out cert.csr
```



طلب توقيع الشهادة

- انسخ CSR واحصل على شهادة CA موقعة
- أستخدم الشهادة والمفتاح الموقع من قبل FTD CA وقم بتحويل الشهادة إلى تنسيق PKCS12
    - أمر OpenSSL:

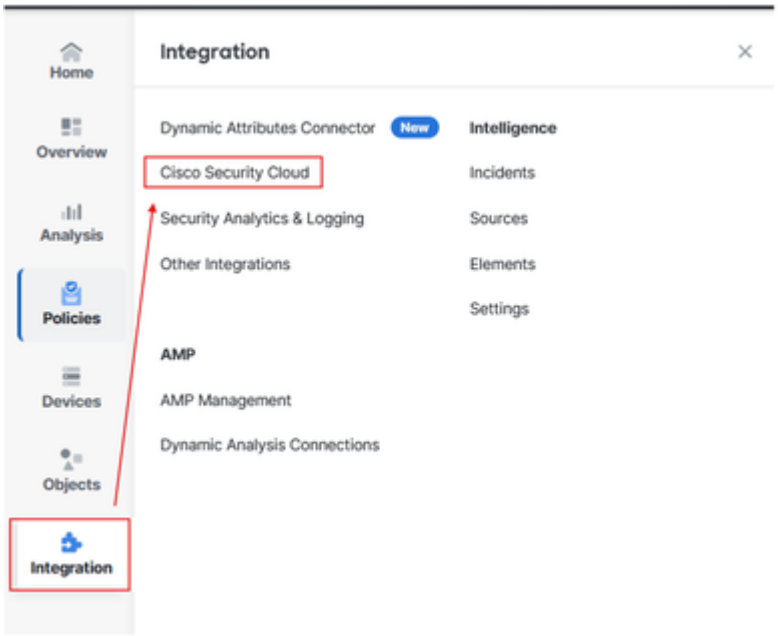
```
openssl pkcs12 -export -out ftdcert.p12 -in cert.crt -inkey cert.key
```

- تصدير الشهادة باستخدام SCP أو أداة أخرى.

مركز إدارة جدار الحماية المضمن على اللوحة للتحكم في سحابة الأمان

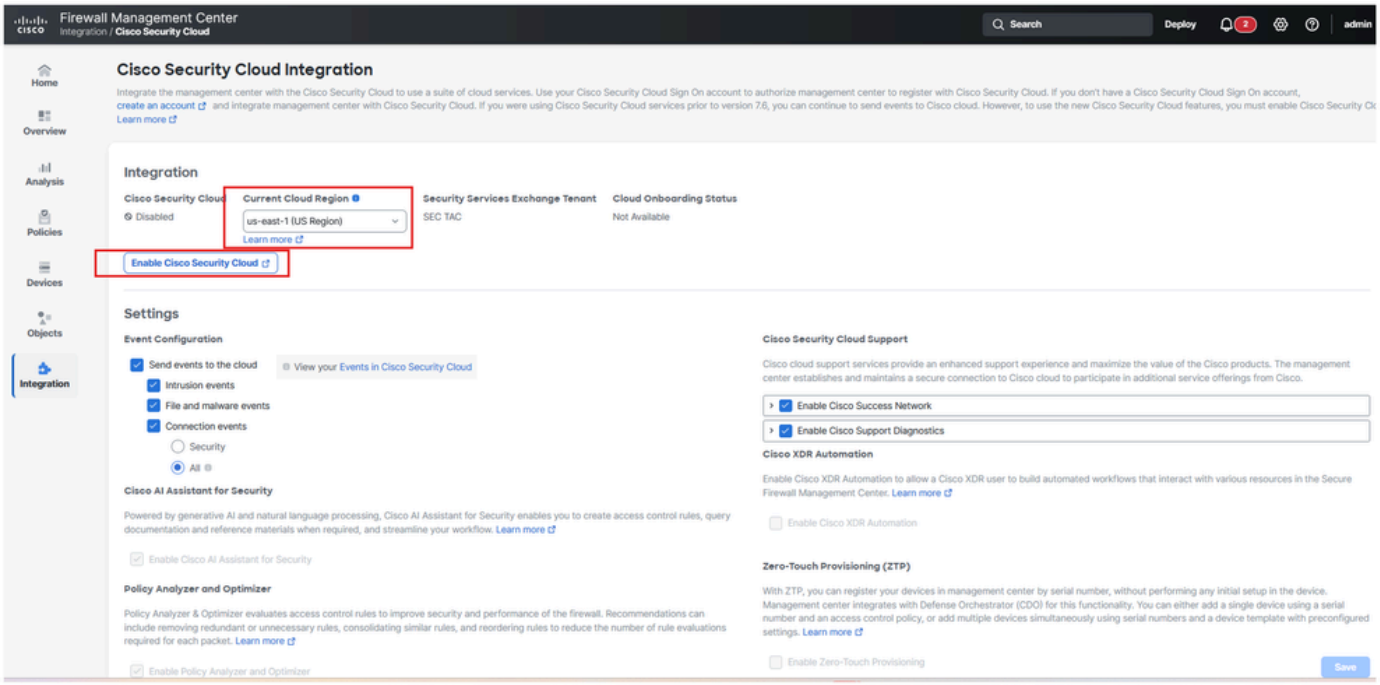
انتقل إلى FMC:

- انقر فوقIntegration> Cisco Security Cloud



دمج مركز إدارة جدار الحماية و SCC

- أختر منطقة السحابة ثم انقر فوق Enable Cisco Security Cloud

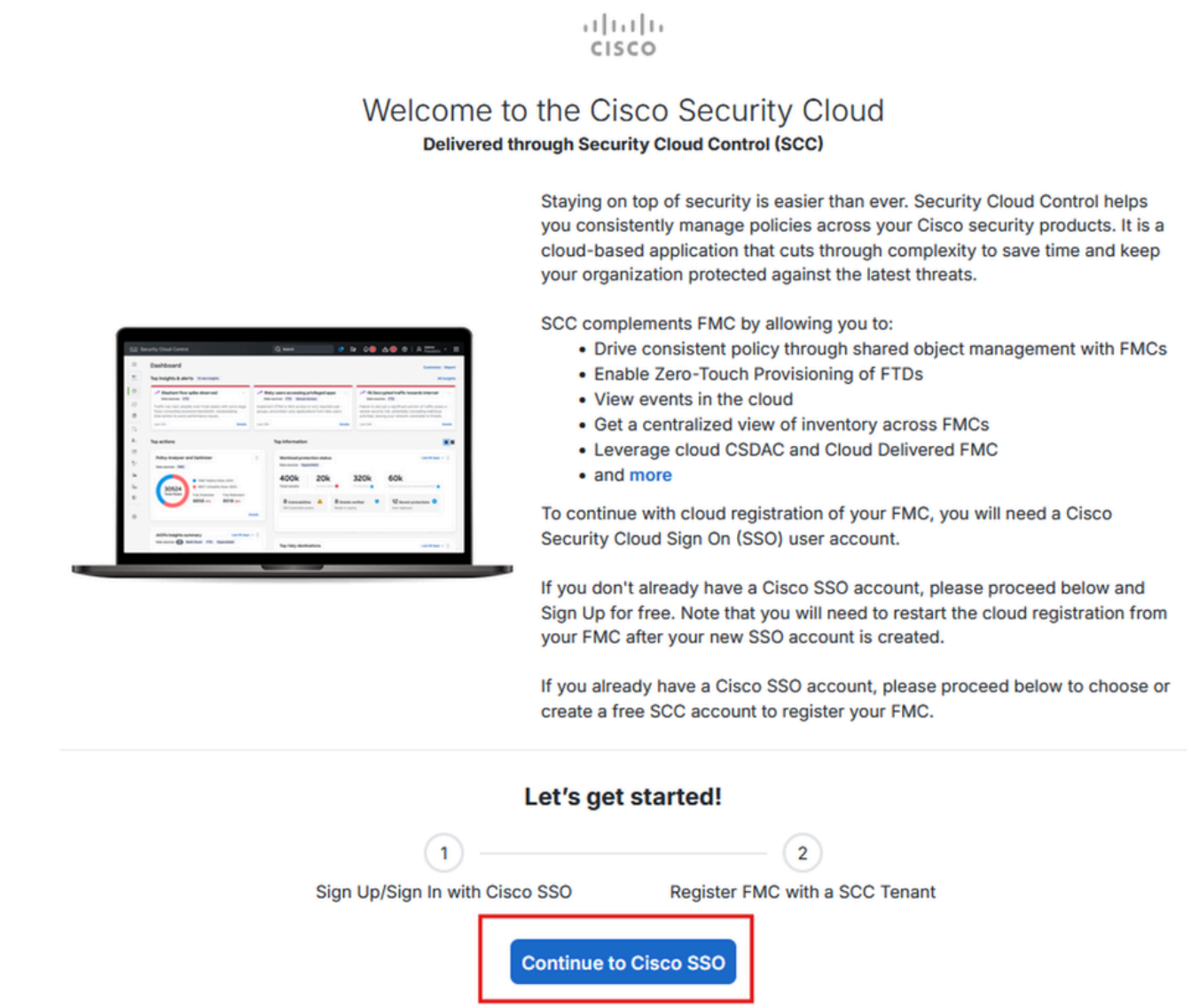


إمكانية الانضمام إلى مركز إدارة جدار الحماية ل SCC

سيفتح علامة تبويب مستعرض جديدة، في علامة التبويب الجديدة:

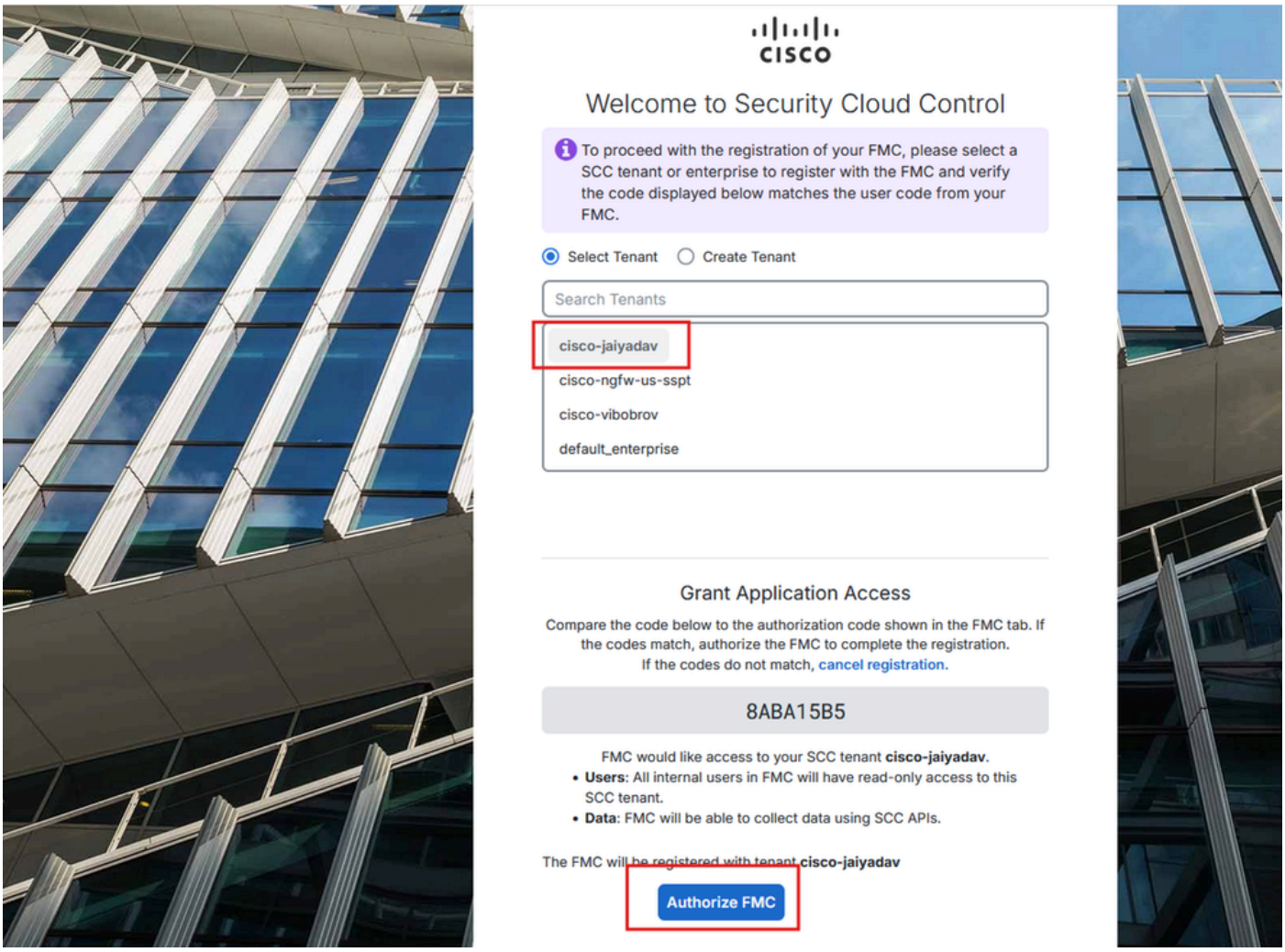
- انقر فوق Continue to Cisco SSO

ملاحظة: تأكد من أنك خارج SCC وليس لديك أي علامات تبويب أخرى مفتوحة.



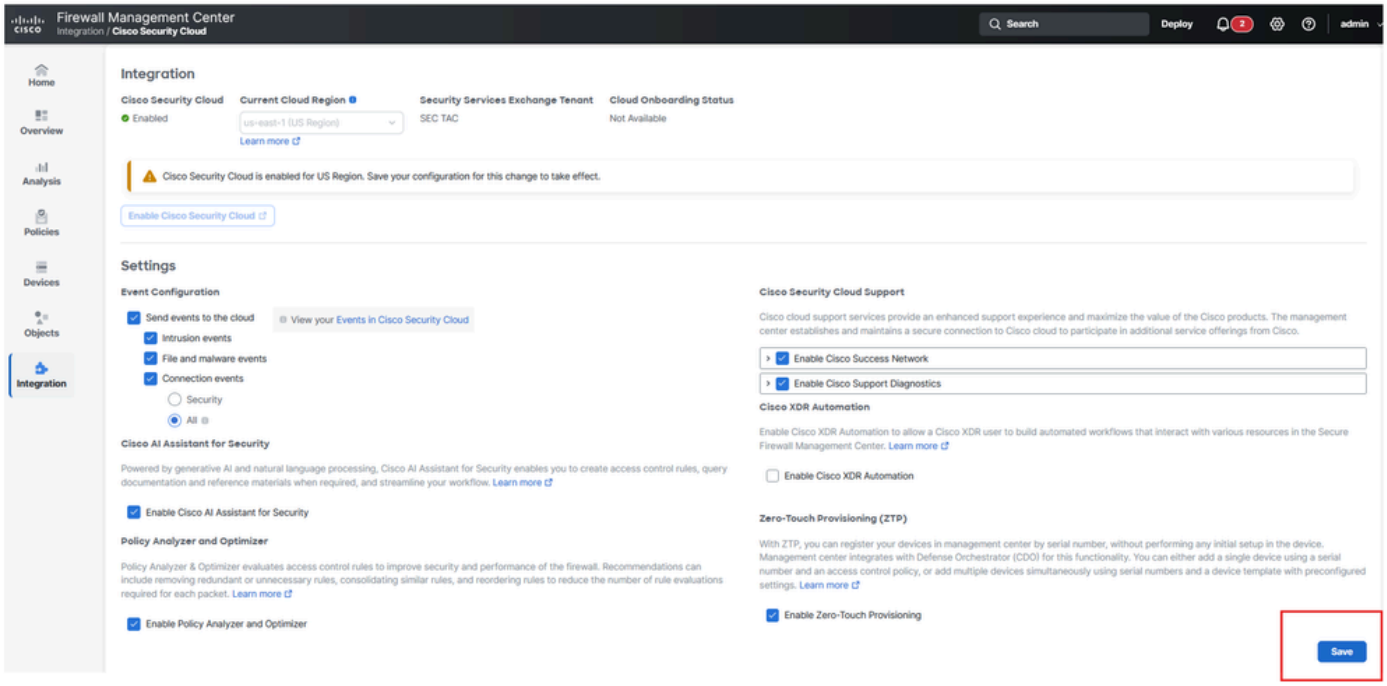
إمكانية الانضمام إلى مركز إدارة جدار الحماية ل SCC

- أختر مستأجر SCC وانقر فوق Authorize FMC



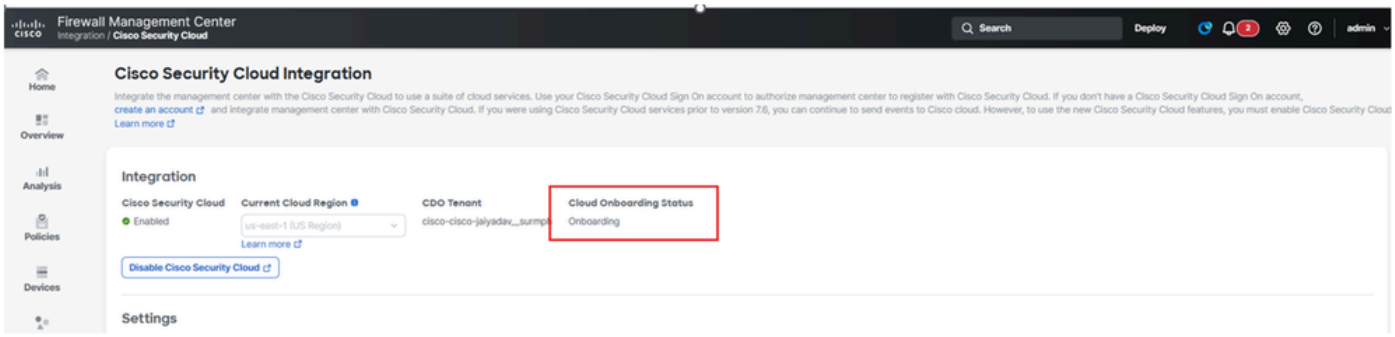
إمكانية الانضمام إلى مركز إدارة جدار الحماية ل SCC

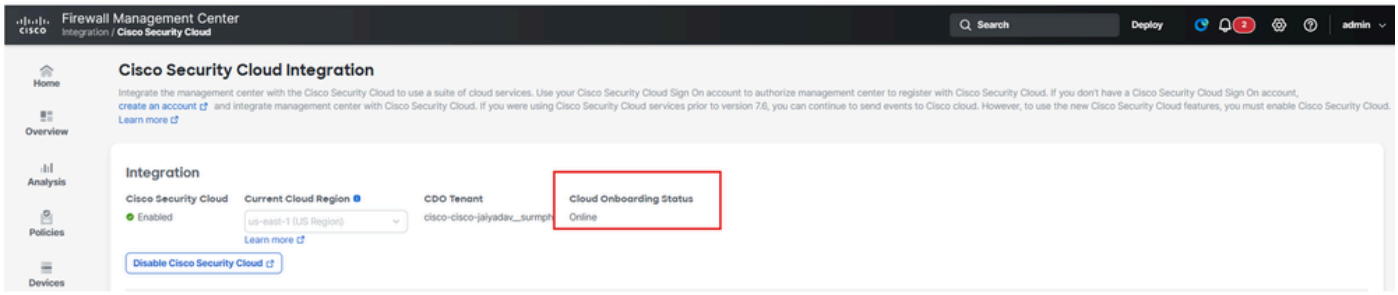
- انقر فوق Save



إمكانية الانضمام إلى مركز إدارة جدار الحماية ل SCC

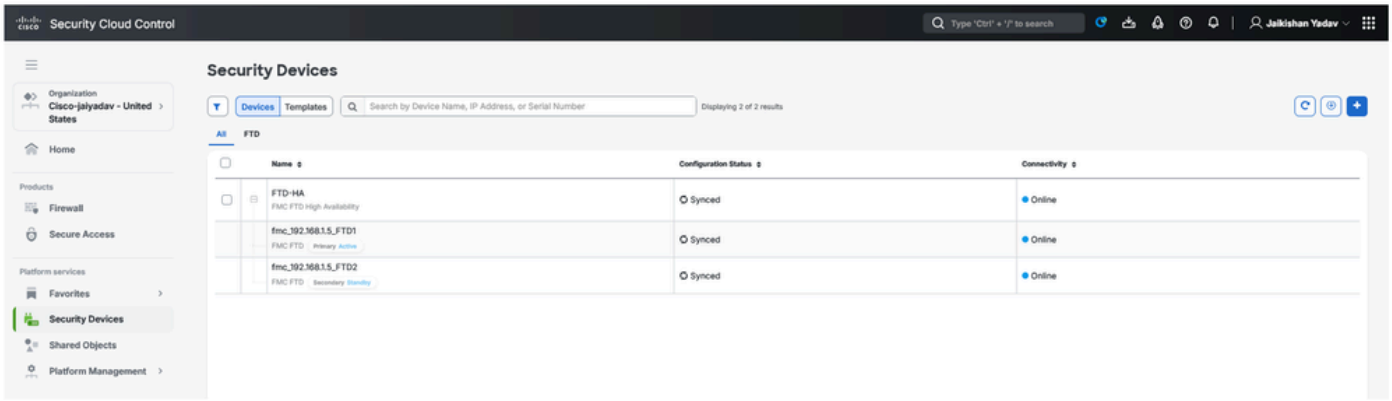
يجب أن تتغيرCloud Onboarding Statusحالة من **Not Available** إلىOnboardingذلك الحينOnline.





حالة الانضمام إلى مركز إدارة جدار الحماية

- انتقل إلى SCC وتحقق من حالة FTD ضمنPlatform Services> Security Devices

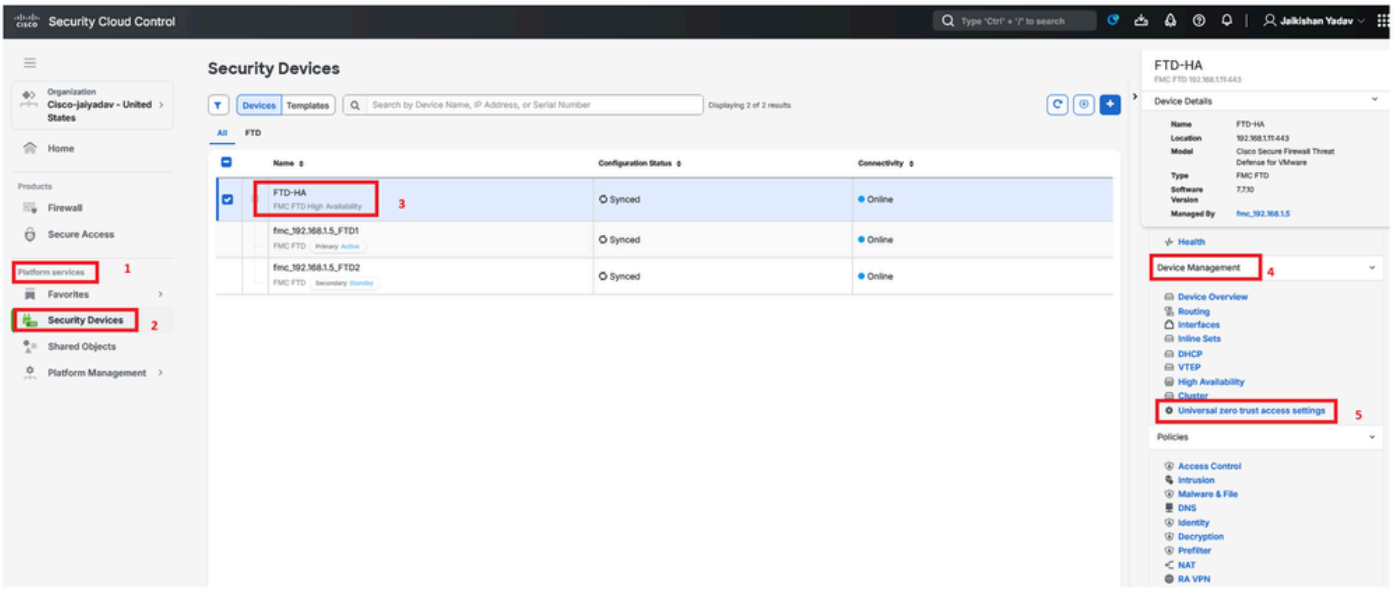


حالة الحماية ضد تهديد جدار الحماية الآمن على SCC

تسجيل الإعدادات العالمية للوصول إلى شبكة Zero Trust (uZTNA) على FTD

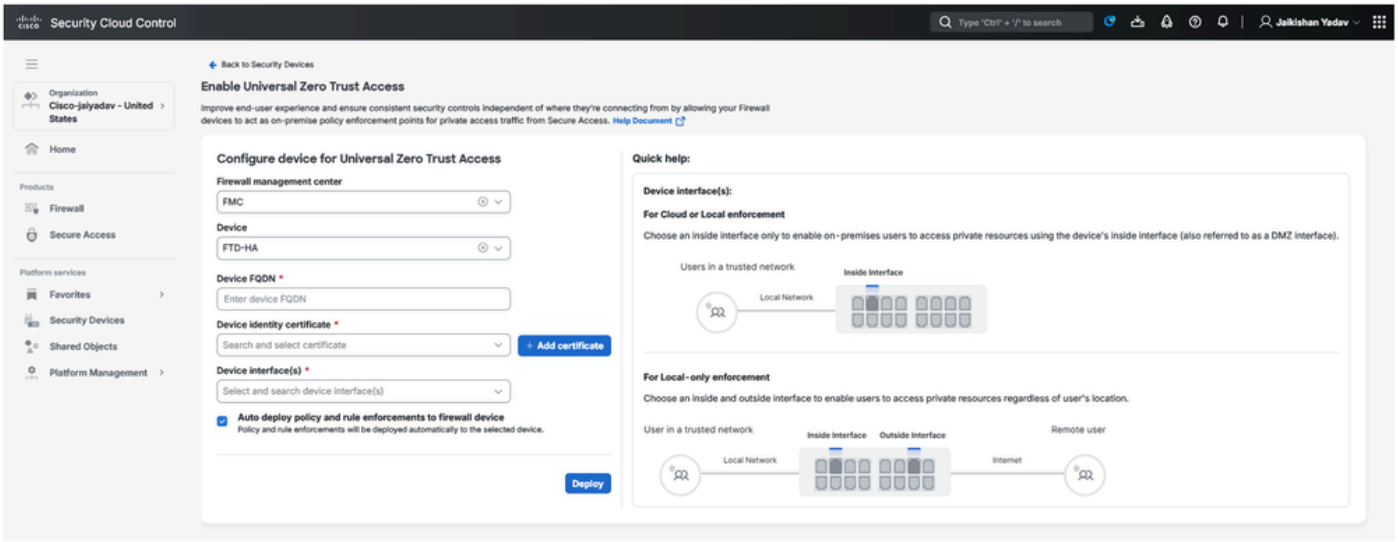
انتقل إلى SCC:

- انقر فوقPlatform Services> **Security Devices** > **FTD** > **Device Management** > Universal Zero Trust Network Access

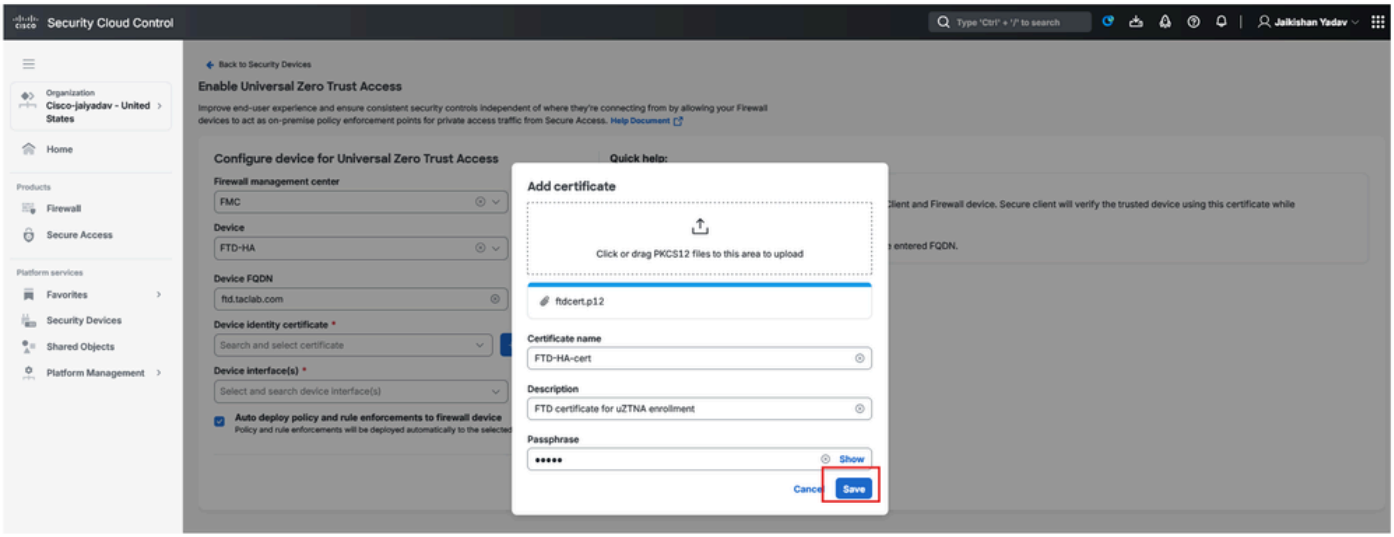


الدفاع الآمن ضد تهديد جدار الحماية - تكوين ZTNA الغالمي

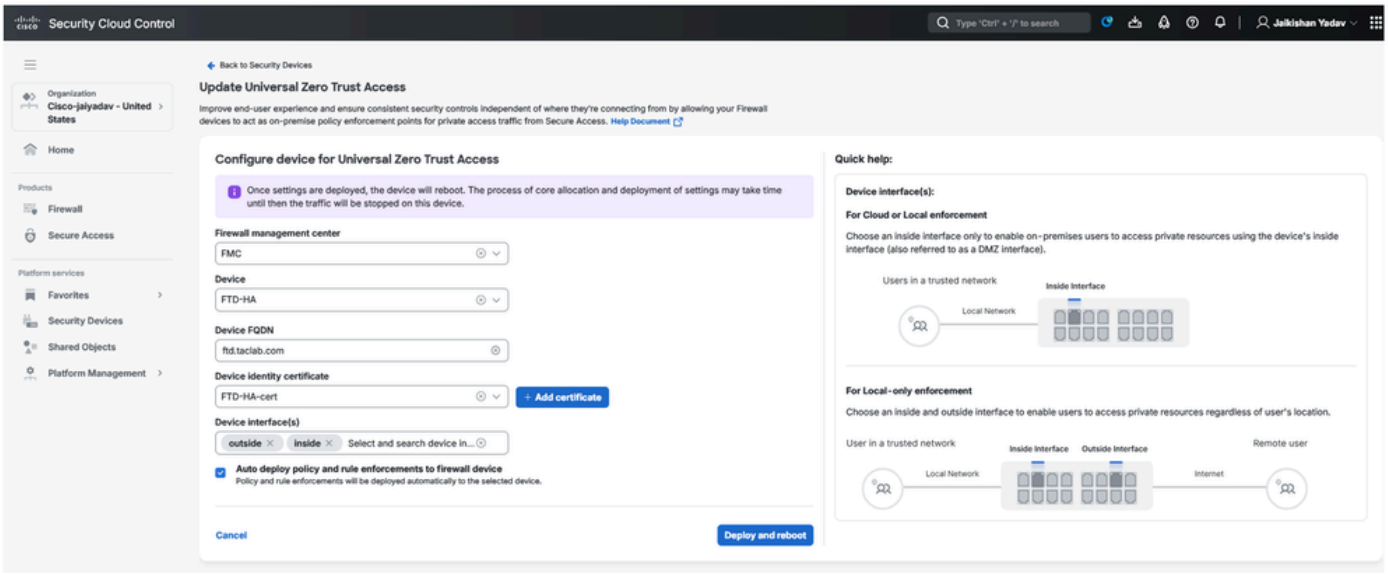
- المأ المعلومات وتحميل شهادة FTD التي تم إنشاؤها في الشهادة الموقعة الخاصة بإنشاء تهديد جدار الحماية (FTD)



الدفاع الآمن ضد تهديد جدار الحماية - تكوين ZTNA الغالمي



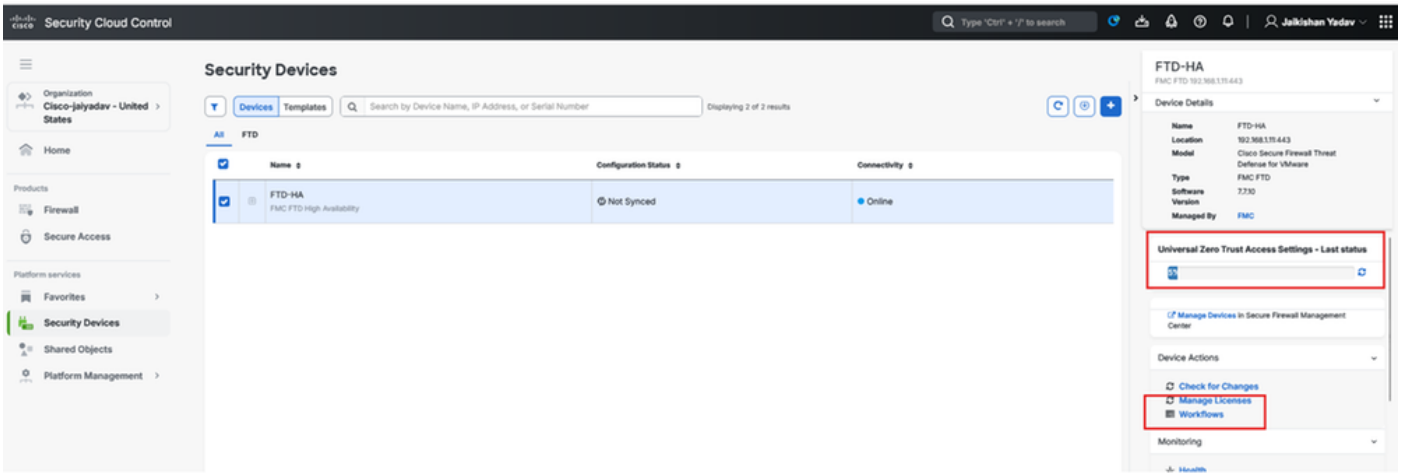
الدفاع الآمن ضد تهديد جدار الحماية - تكوين ZTNA العالمي



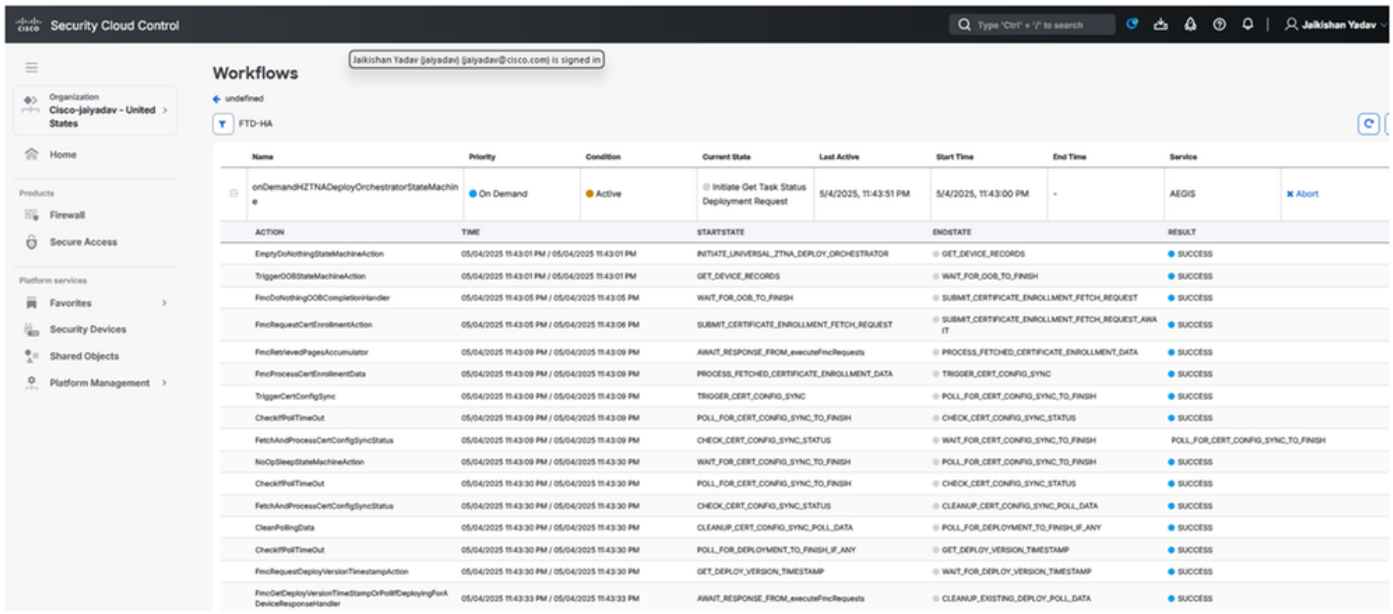
الدفاع الآمن ضد تهديد جدار الحماية - تكوين ZTNA العالمي

ملاحظة: عند تمكين uZTNA على FTD HA، سيتم نشر التغييرات وإعادة تشغيل كل من وحدات الدفاع عن تهديد جدار الحماية (FTD) في نفس الوقت. تأكد من جدولة إطار صيانة مناسب.

- انقر فوقWorkflowللتحقق من السجلات

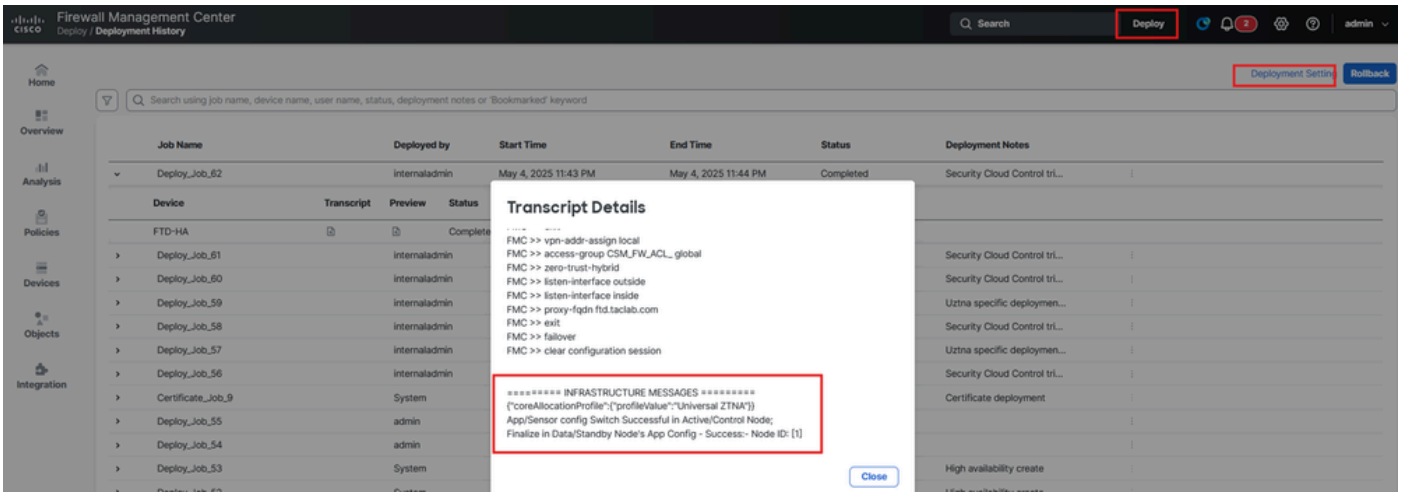


الدفاع الآمن عن تهديد جدار الحماية - حالة تكوين ZTNA العالمية



سير عمل التحكم في سحابة الأمان

تحت تفاصيل النص الإنكليزي يمكنك أن ترىPolicy Deployment Statusوتتغير FMC.



مركز إدارة جدار الحماية الآمن - حالة نشر السياسة

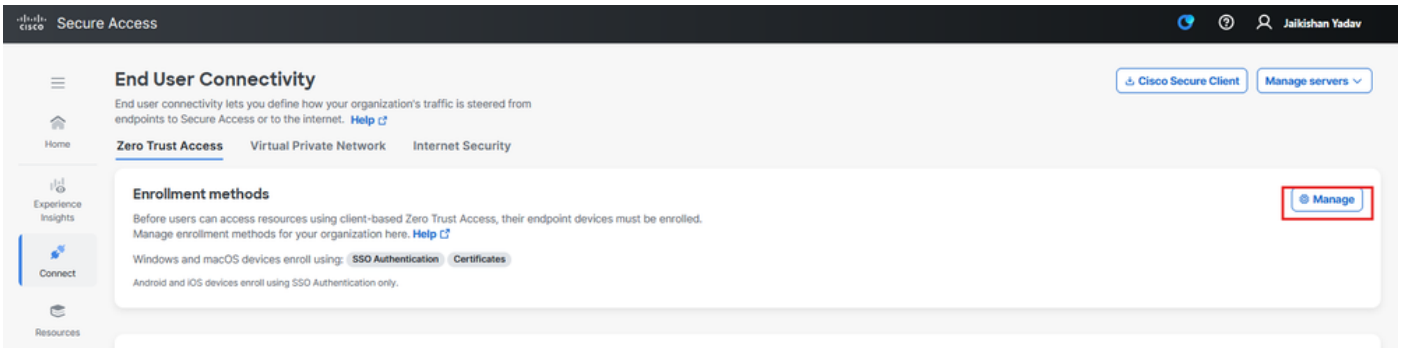
تسجيل العميل باستخدام uZTNA

تكوين الوصول الآمن

ملاحظة: يمكنك إستخدام تسجيل ZTA المستند إلى شهادة أو SSO. الروابط، هي خطوات تسجيل ZTA المستند إلى الشهادة

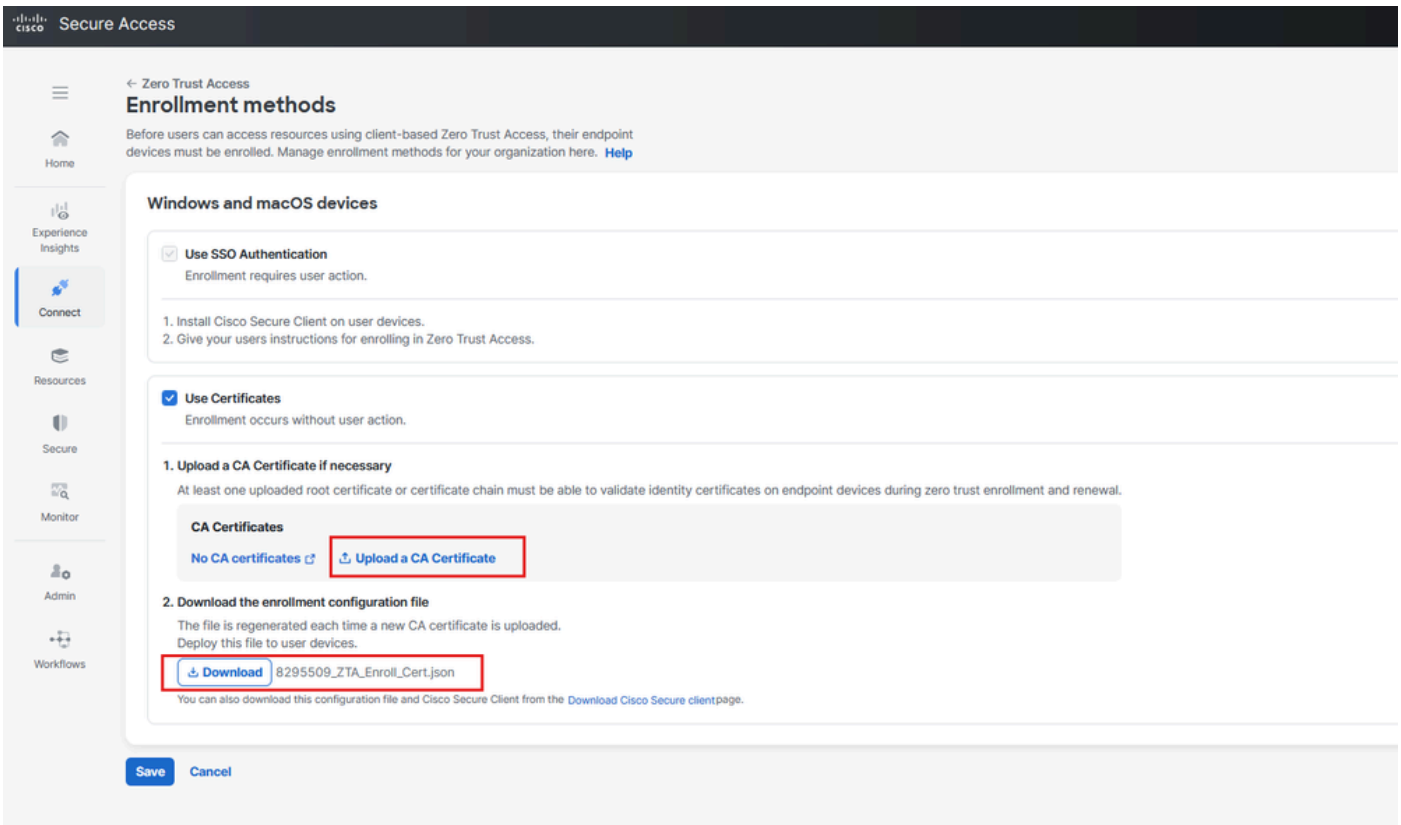
انتقل إلى لوحة معلومات الوصول الآمن:

- انقر فوق **Connect** > **End User Connectivity** > Zero Trust Access
- انقر فوق Manage



الوصول الآمن - تسجيل شهادة ZTA

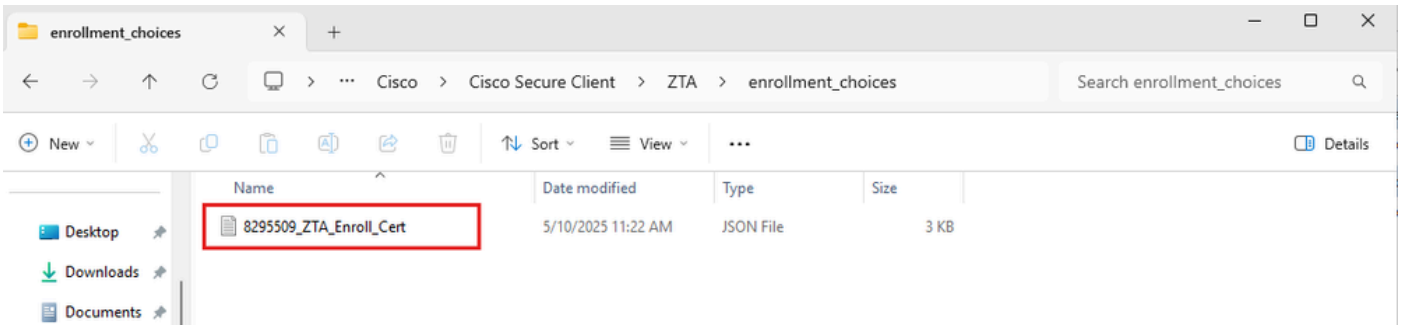
- تحميل شهادة المرجع المصدق الجذر وتنزيل ملف تكوين التسجيل



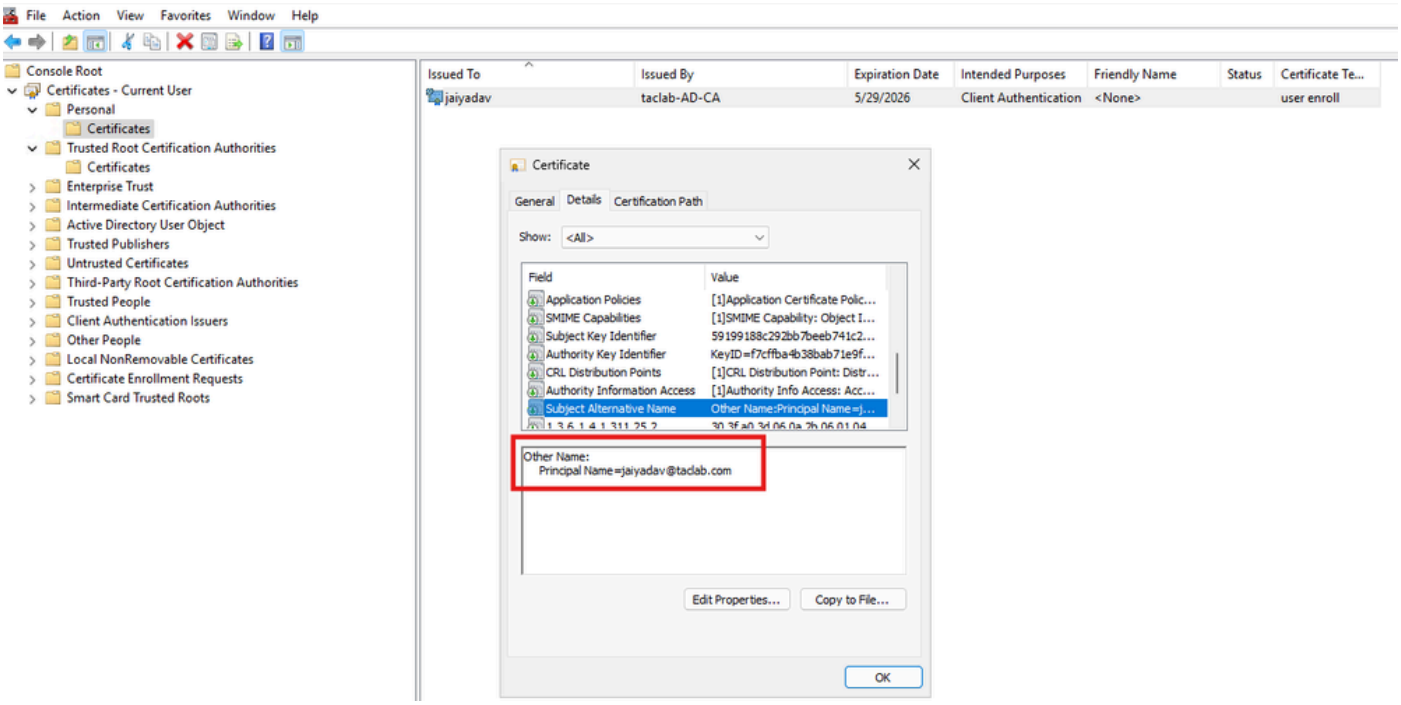
- انقر فوق Save

تكوين العميل

نسخ ملف تكوين التسجيل إلى C:\ProgramData\Cisco\Cisco Secure Client\ZTA\enrollment_choices

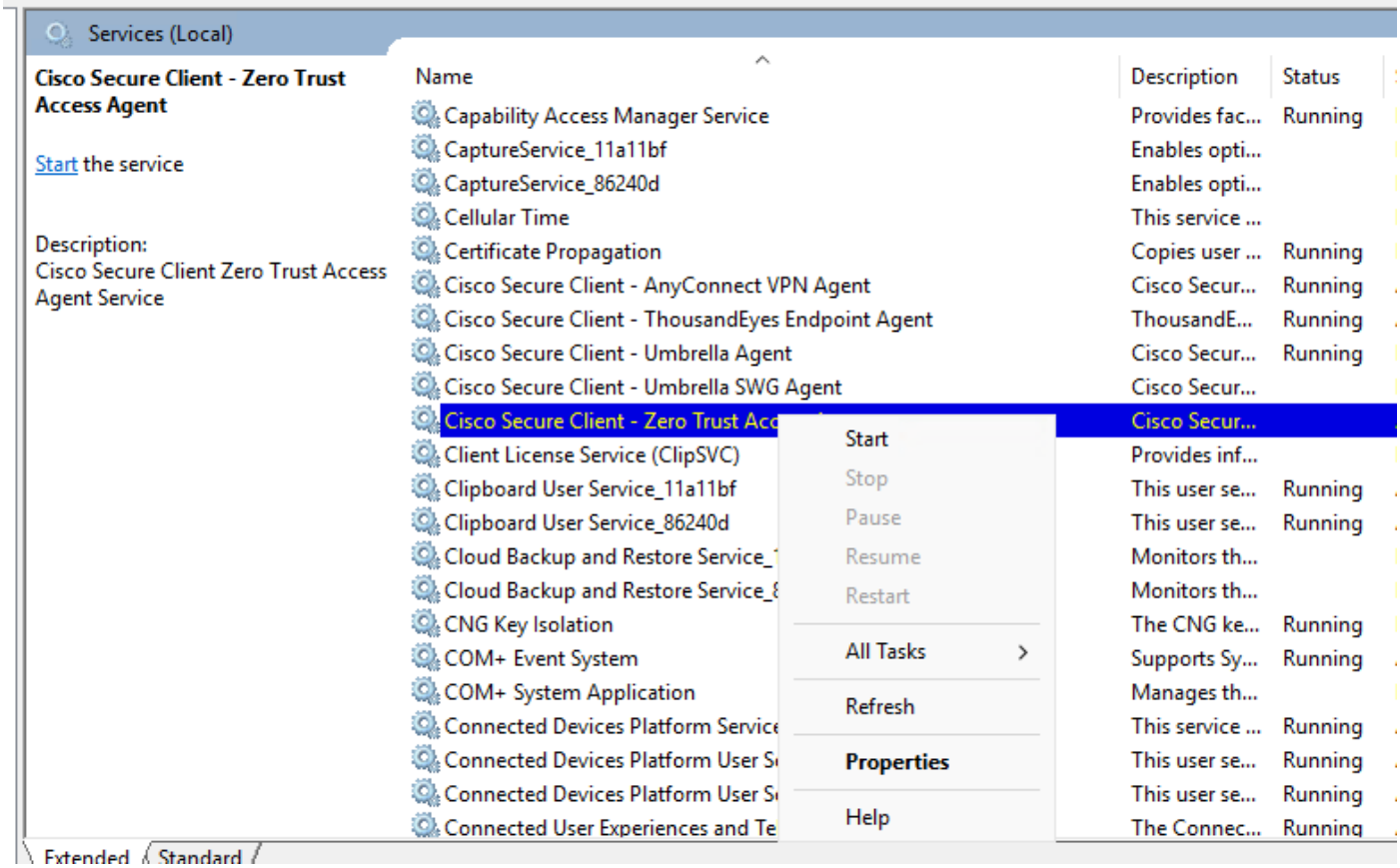


- إنشاء Client Certficiate، الذي يجب أن يحتوي على UPN في SAN Filed



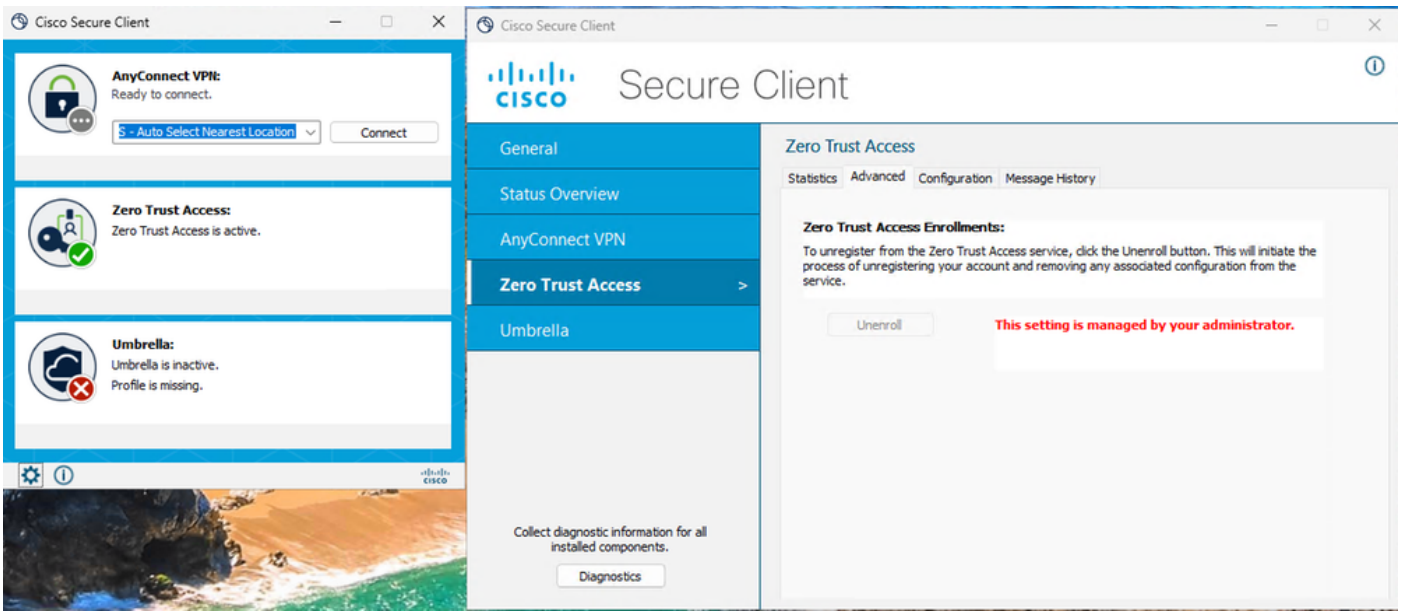
تثبيت الشهادة

- بدء/إعادة تشغيل Cisco Secure Client - Zero Trust Access Agent



خدمات Windows

- حالة وحدة ZTA النمطية



الوصول الآمن - حالة تسجيل شهادة ZTA

التحقق من الصحة

أستخدم الأمر التالي للتحقق من تكوين uZTNA على حماية تهديد جدار الحماية (FTD):

```
show allocate-core profile
show running-config universal-zero-trust
```

معلومات ذات صلة

- الدعم الفني والتنزيلات من Cisco
- مركز تعليمات الوصول الآمن من Cisco
- دليل تصميم Cisco SASE

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).