تكوين عميل SSL الآمن باستخدام المصادقة المحلية على FTD

المحتويات

المقدمة

يصف هذا المستند كيفية تكوين عميل Cisco الآمن (يتضمن AnyConnect) باستخدام المصادقة المحلية على Cisco FTD التي تتم إدارتها بواسطة Cisco FMC.

المتطلبات الأساسية

المتطلبات

توصي Cisco بأن تكون لديك معرفة بالمواضيع التالية:

- تكوين عميل SSL الآمن من خلال مركز إدارة FirePOWER (FMC)
- تكوين كائنات Firepower من خلال FMC
- شهادات SSL على Firepower

المكونات المستخدمة

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

- Cisco Firepower Threat Defense (FTD)، الإصدار 7.0.0 (Build 94)
- Cisco FMC، الإصدار 7.0.0 (Build 94)
- Cisco Secure Mobility Client 4.10.01075

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.

معلومات أساسية

في هذا المثال، يتم إستخدام طبقة مآخذ التوصيل الآمنة (SSL) لإنشاء الشبكة الخاصة الظاهرية (VPN) بين FTD وعميل Windows 10.

من الإصدار 7.0.0، يدعم برنامج FTD الذي تتم إدارته بواسطة FMC المصادقة المحلية لعملاء Cisco الآمنين. ويمكن تعريف هذه كطريقة مصادقة أساسية أو كطريقة إحتياطية في حالة فشل الطريقة الأساسية. في هذا المثال، يتم تكوين المصادقة المحلية كمصادقة أساسية.

قبل أن يكون إصدار البرنامج هذا Cisco Secure Client Local Authentication على FTD متاحا فقط على Cisco Firepower Device Manager (FDM).

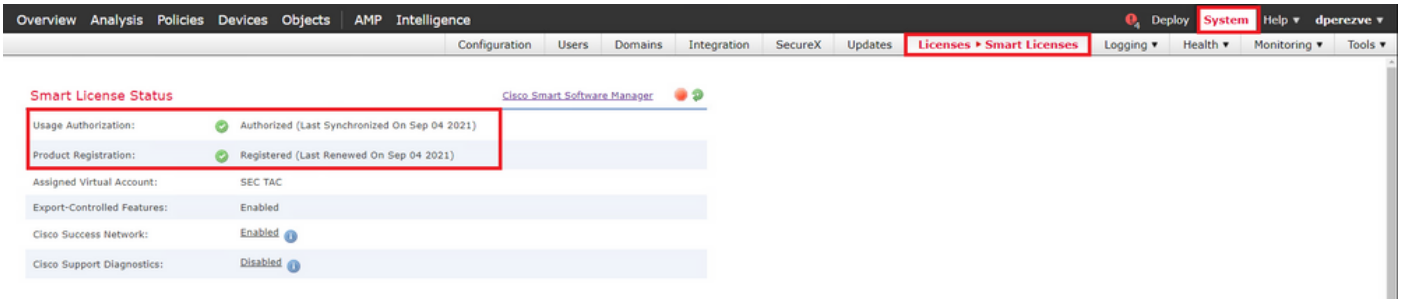
التكوين

التكوينات

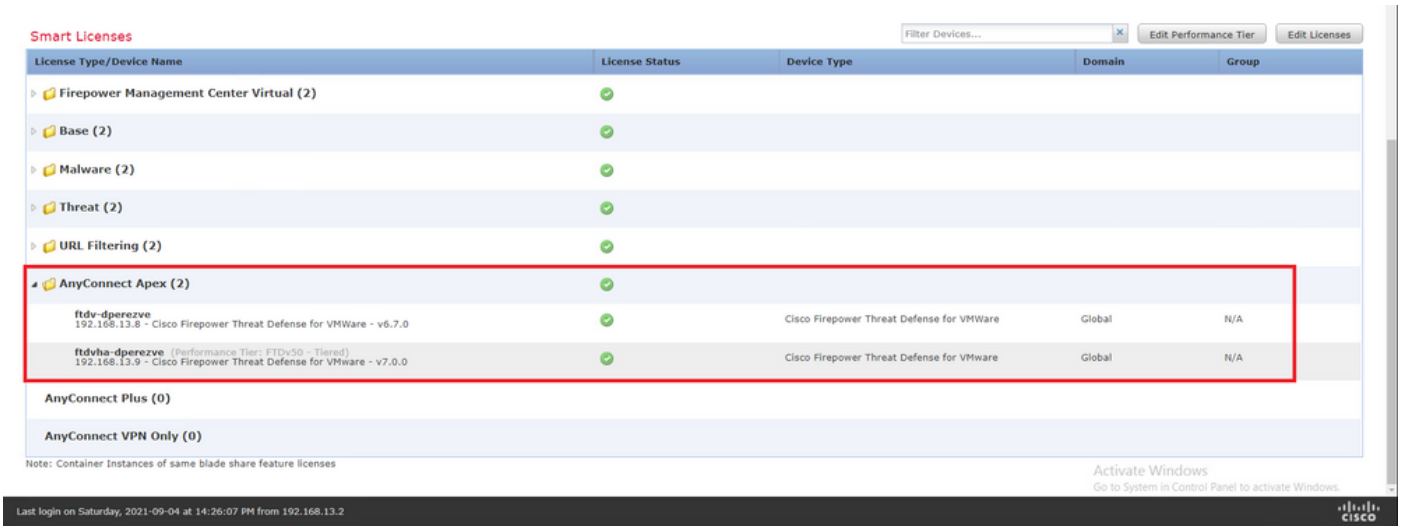
الخطوة 1. التحقق من الترخيص

قبل تكوين Cisco Secure Client، يجب تسجيل FMC، وأن تكون متوافقة مع مدخل الترخيص الذكي. الا يمكنك نشر Cisco Secure Client إذا لم يكن ل FTD ترخيص PLUS أو APEX أو VPN صالح فقط.

انتقل إلى النظام > التراخيص > التراخيص الذكية للتحقق من أن وحدة التحكم في إدارة الإطارات (FMC) مسجلة ومتوافقة مع مدخل الترخيص الذكي.



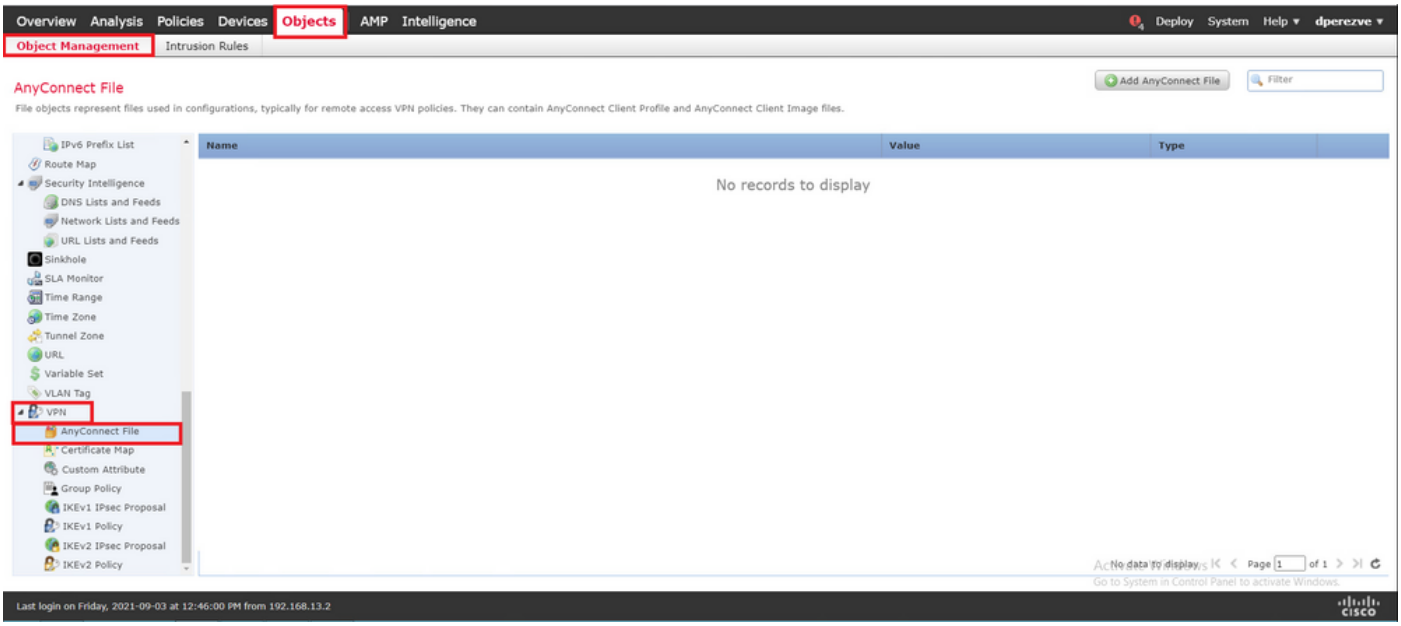
قم بالتمرير لأسفل على نفس الصفحة، في أسفل مخطط التراخيص الذكية يمكنك مشاهدة الأنواع المختلفة من تراخيص عميل Cisco الآمن (AnyConnect) المتوفرة والأجهزة المشتركة في كل منها. التحقق من صحة FTD الموجود قيد التسجيل ضمن أي من هذه الفئات.



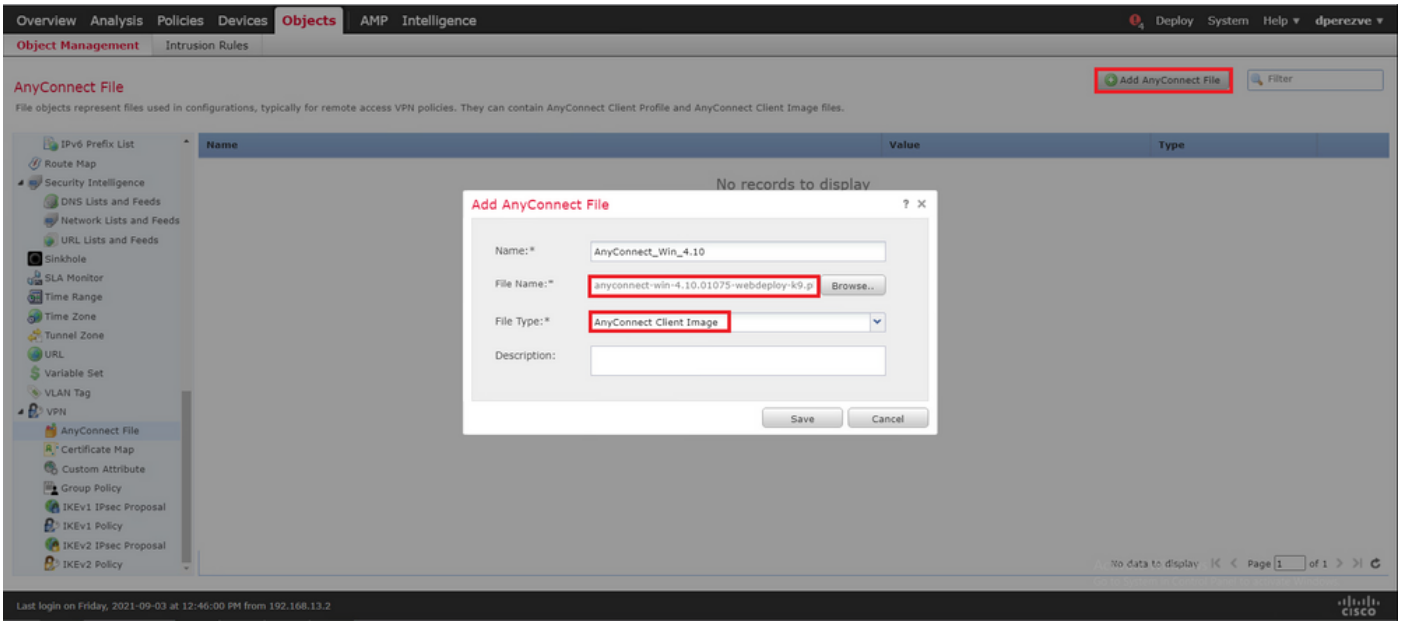
الخطوة 2. تحميل حزمة Cisco Secure Client إلى FMC

قم بتنزيل حزمة نشر وحدة الاستقبال والبث الخاصة ب Cisco Secure Client (AnyConnect) ل Windows من cisco.com.

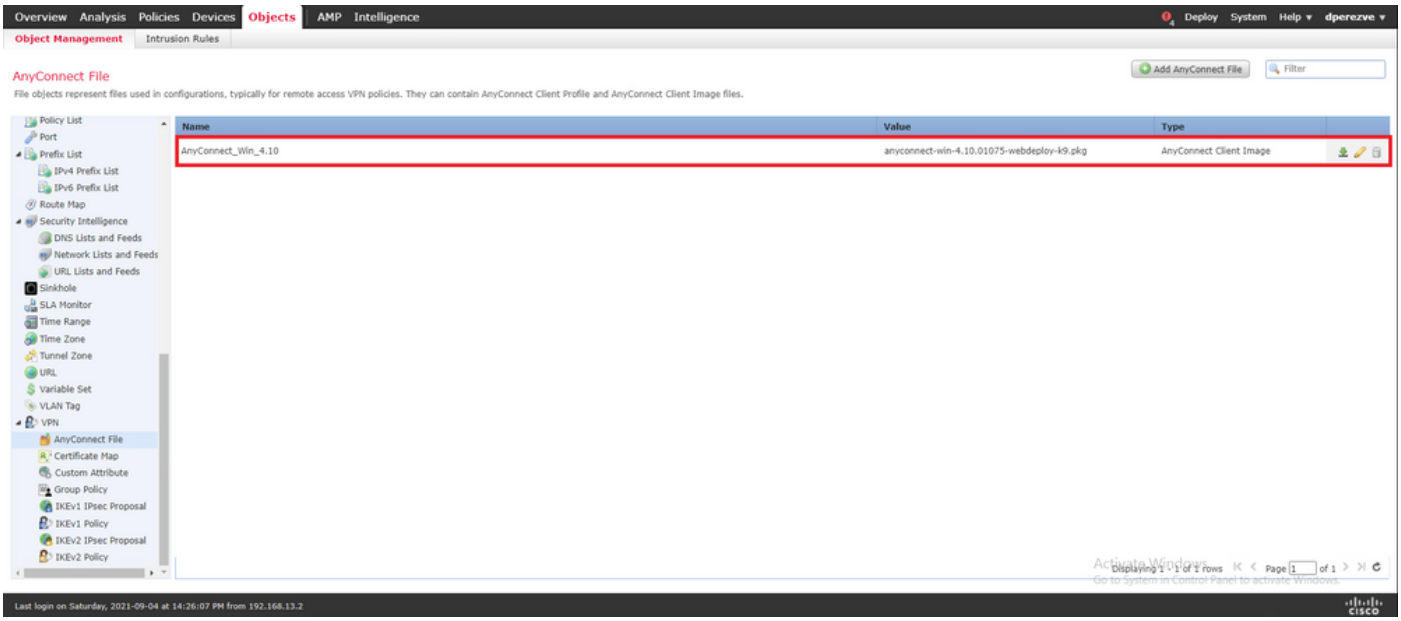
لتحميل صورة عميل Cisco الآمن، انتقل إلى الكائنات > إدارة الكائنات واختر ملف عميل Cisco الآمن ضمن فئة VPN في جدول المحتويات.



أختر الزر إضافة ملف AnyConnect. في نافذة إضافة ملف عميل AnyConnect الآمن، قم بتعيين اسم للكائن، ثم أختر إستعراض. لاختيار حزمة عميل Cisco الآمن وأخيرا أختر صورة عميل AnyConnect كنوع الملف في القائمة المنسدلة.



أختر الزر حفظ. يجب إضافة الكائن إلى قائمة الكائنات.



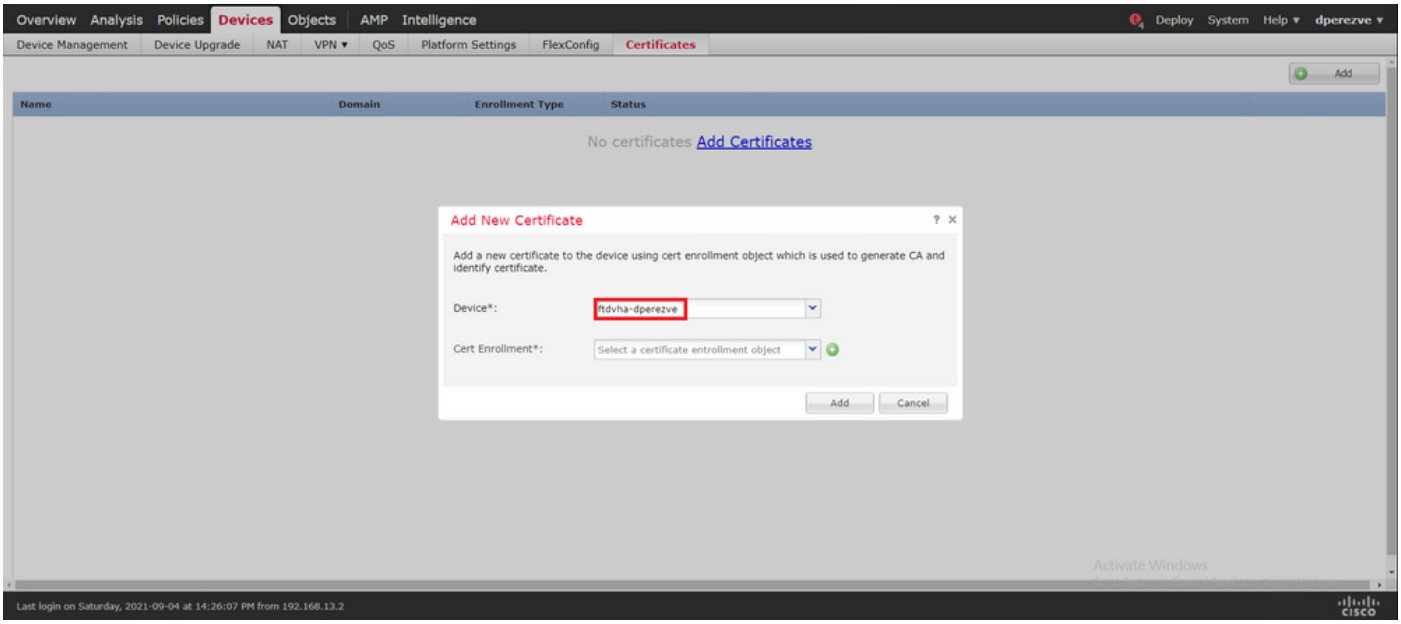
الخطوة 3. إنشاء شهادة موقعة ذاتيا

يتطلب SSL Cisco Secure Client (AnyConnect) وجود شهادة واحدة صالحة ليتم إستخدامها في مصافحة SSL بين وحدة الاستقبال والبث الخاصة بشبكة VPN والعميل.

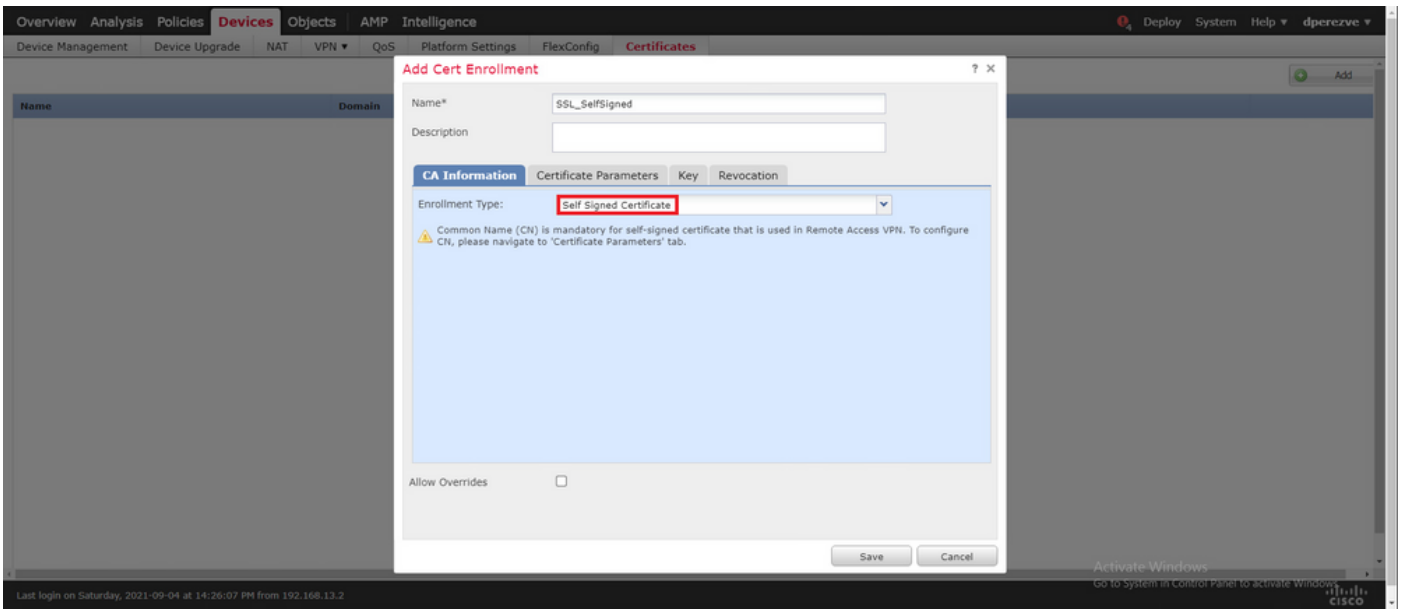
ملاحظة: في هذا المثال، يتم إنشاء شهادة موقعة ذاتيا لهذا الغرض. ومع ذلك، فإلى جانب الشهادات الموقعة ذاتيا، من الممكن تحميل شهادة موقعة إما من هيئة شهادة داخلية أو من مرجع مصدق معروف أيضا.

لإنشاء الشهادة الموقعة ذاتيا، انتقل إلى الأجهزة > الشهادات.

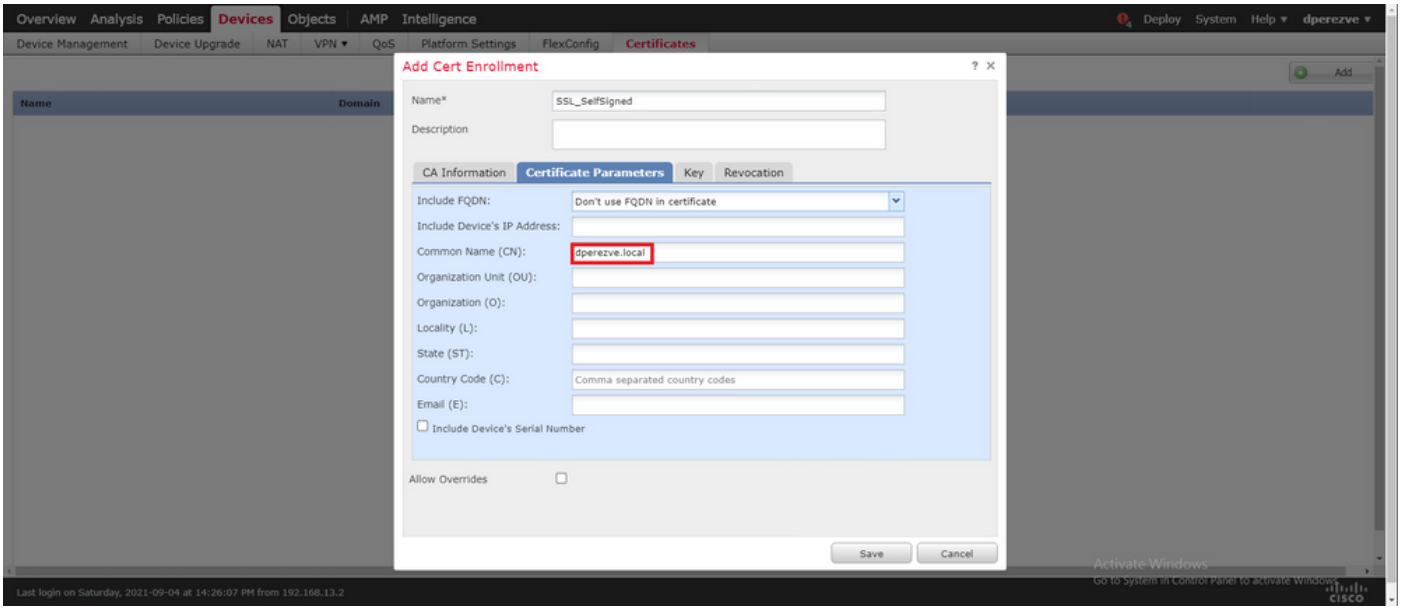
أختر الزر إضافة. ثم أختر FTD الموجود حاليا في القائمة المنسدلة الجهاز في نافذة إضافة شهادة جديدة.



أختر زر إضافة تسجيل الوصول (أخضر + رمز) لإنشاء كائن تسجيل جديد. قم الآن، في نافذة إضافة تسجيل دخول للعنصر، بتعييني اسم للكائن واختر شهادة موقعة ذاتيا في القائمة المنسدلة نوع التسجيل.



أخيرا، بالنسبة للشهادات الموقعة ذاتيا، يكون إلزاميا أن يكون هناك اسم مشترك (CN). انتقل إلى علامة تبويب معلمات الشهادات لتحديد CN.

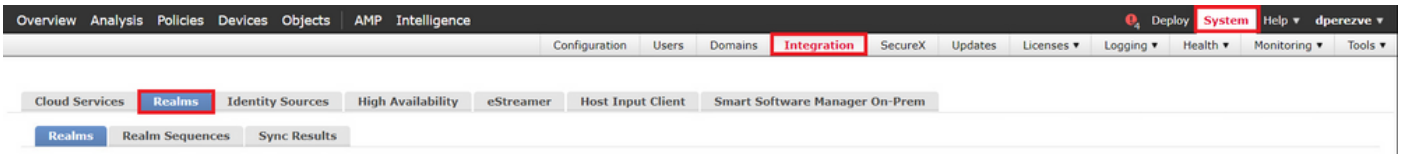


أختر أزرار حفظ وإضافة. بعد بضع ثوان، يجب إضافة الشهادة الجديدة إلى قائمة الشهادات.

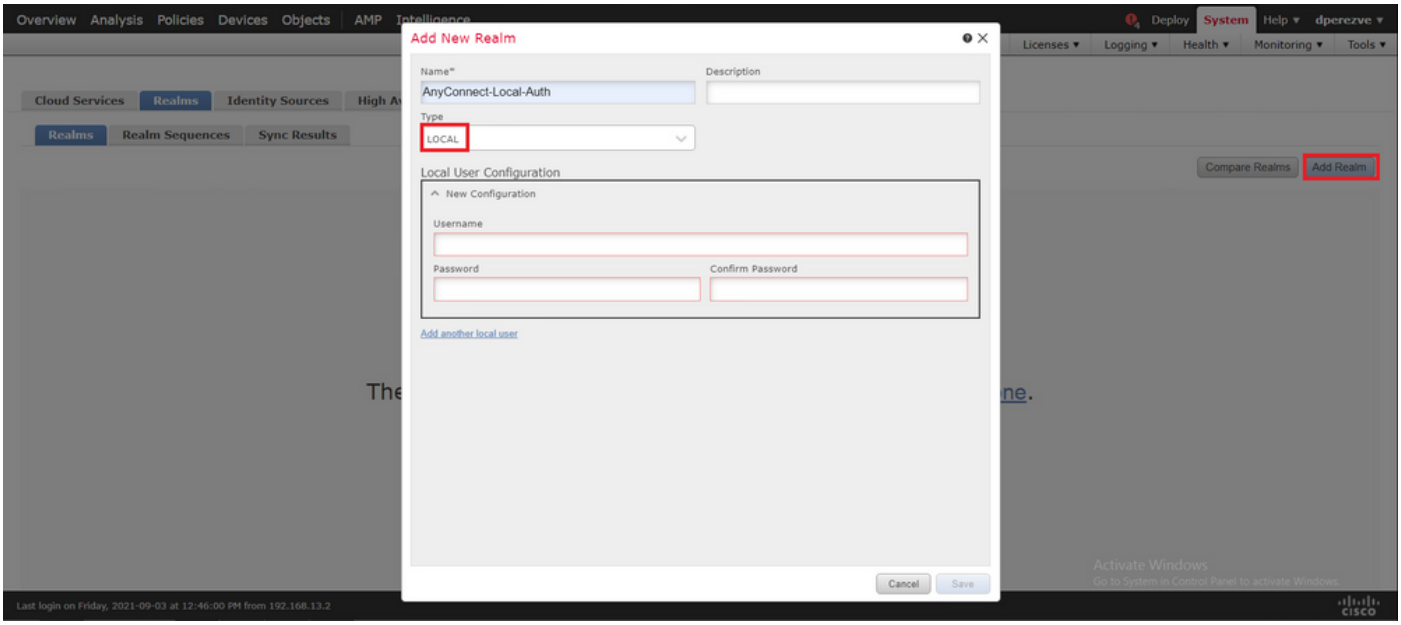
الخطوة 4. إنشاء نطاق محلي على FMC

يتم تخزين قاعدة بيانات المستخدم المحلي وكلمات المرور المقابلة في نطاق محلي.

لإنشاء المجال المحلي، انتقل إلى نظام > تكامل > ريمز.

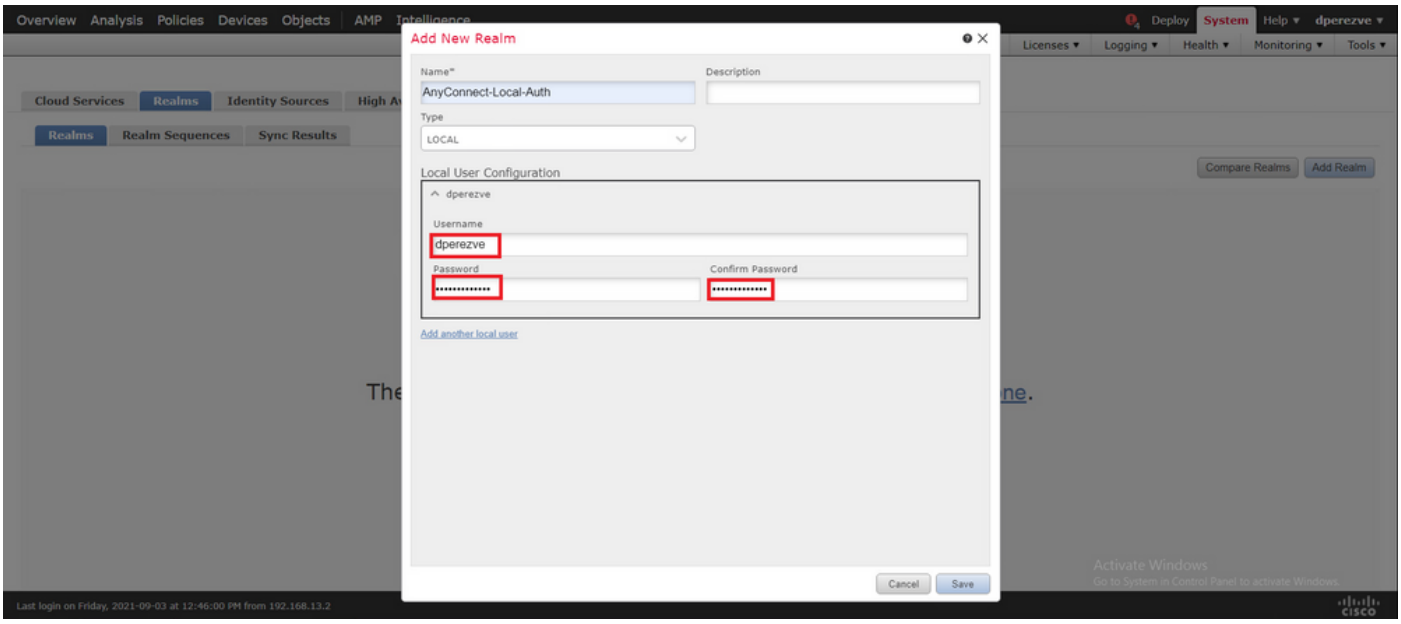


أختر زر إضافة حيز. في نافذة إضافة حيز جديد، قم بتعيين اسم واختر خيار محلي في القائمة المنسدلة النوع.

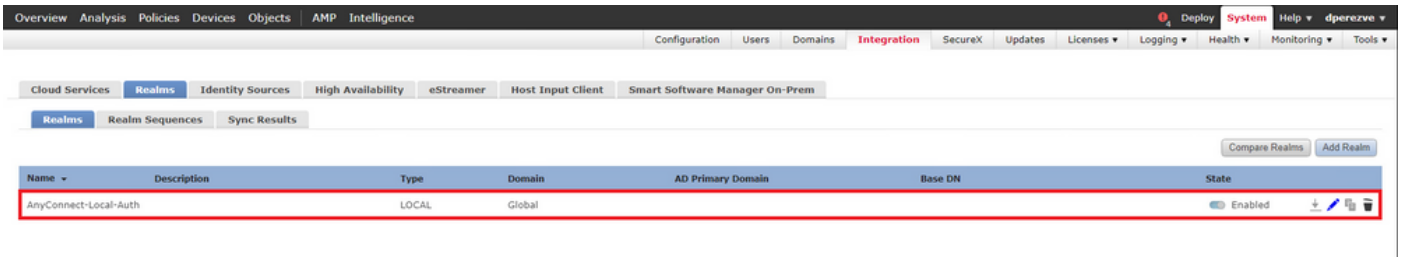


يتم إنشاء حسابات المستخدمين وكلمات المرور في قسم تكوين المستخدم المحلي.

ملاحظة: يجب أن يكون لكلمات المرور حرف حرف حرف كبير واحد على الأقل وحرف حرف حرف صغير ورقم واحد وحرف خاص واحد.

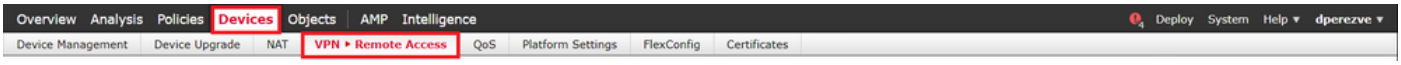


يجب إضافة حفظ التغييرات والحيز الجديد إلى قائمة القيم الموجودة.

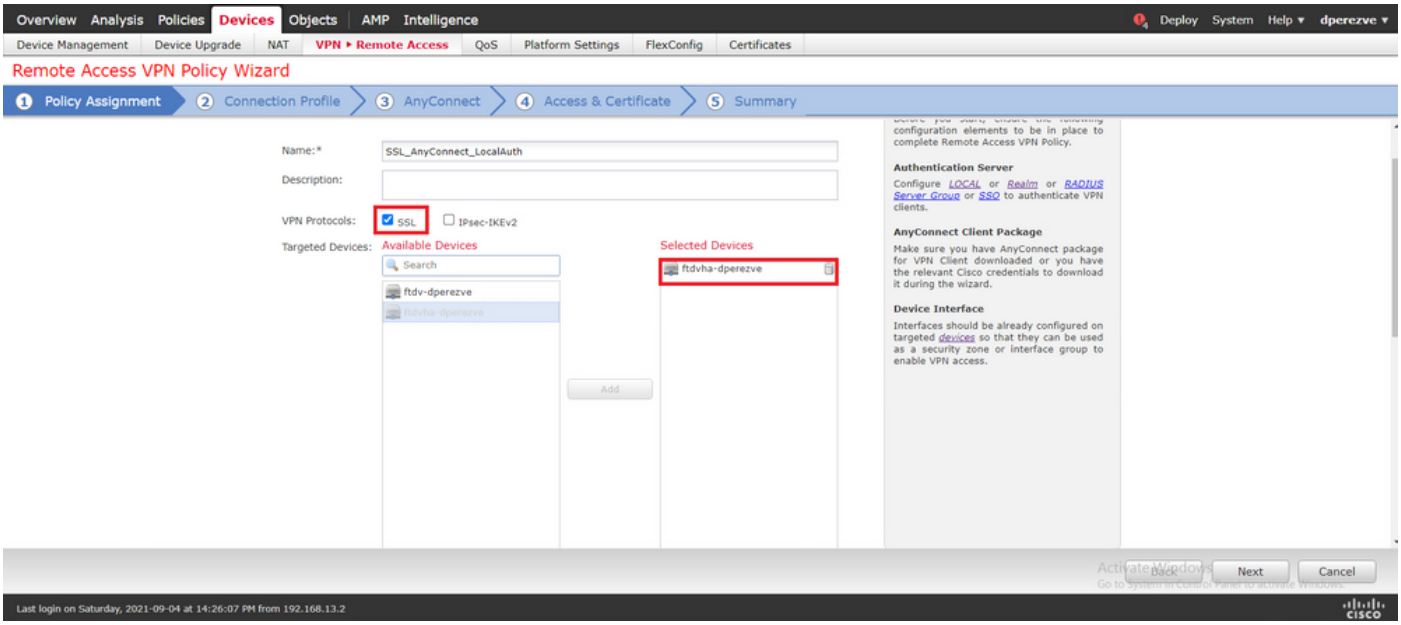


الخطوة 5. تكوين SSL Cisco Secure Client

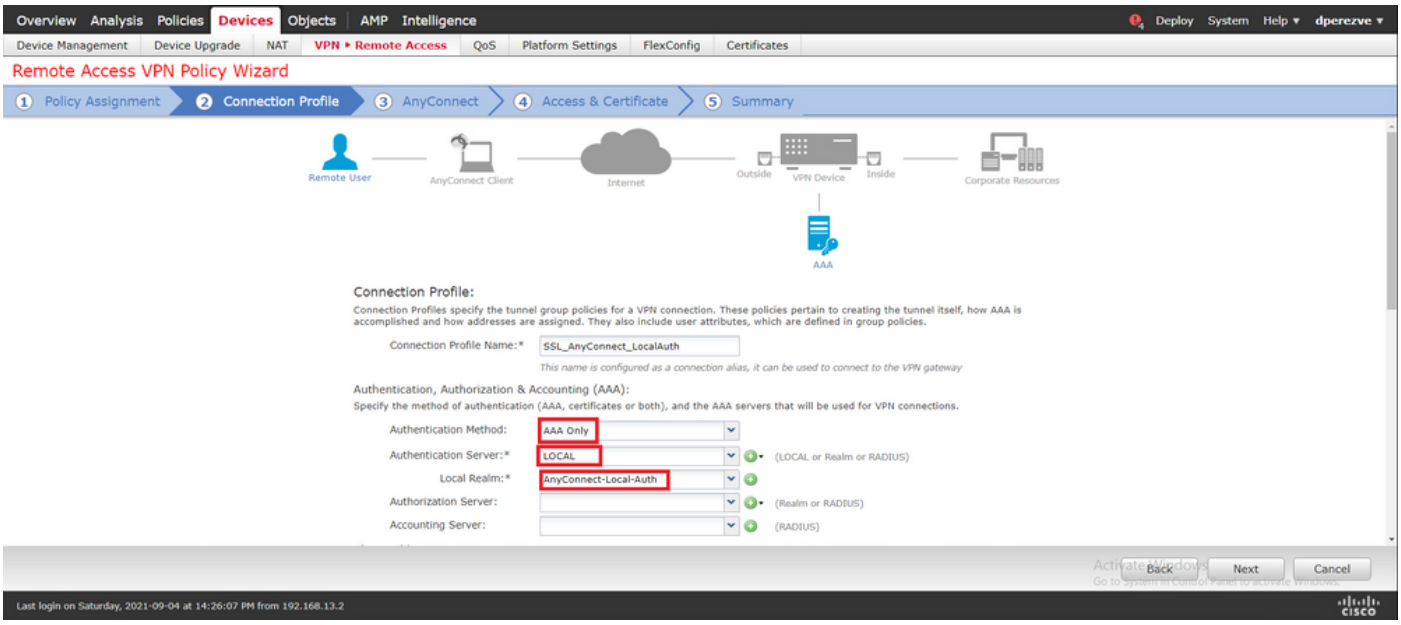
لتكوين SSL Cisco Secure Client، انتقل إلى الأجهزة > VPN > الوصول عن بعد.



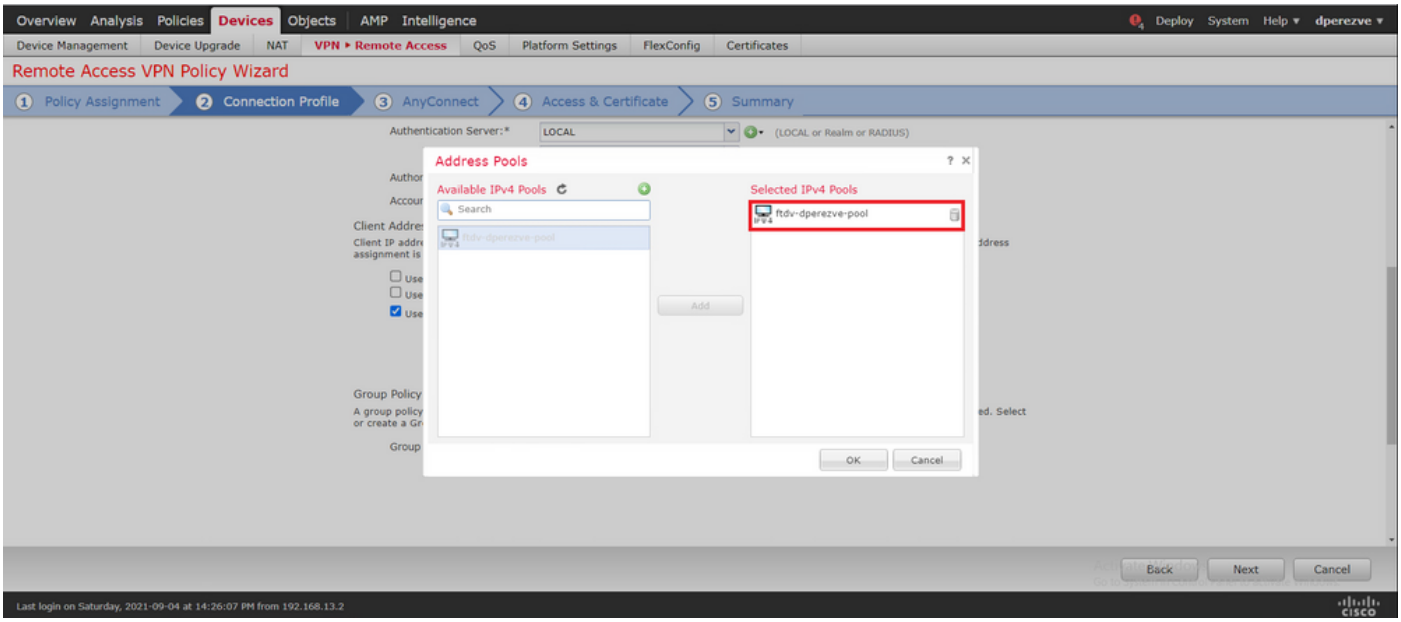
أخترت يضيف زر in order to خلقت جديد VPN سياسة. قم بتحديد اسم لملف تعريف الاتصال، ثم حدد خانة إختيار SSL، ثم أختر FTD الموجود كجهاز مستهدف. يجب تكوين كل شيء في قسم تعيين النهج في معالج نهج VPN للوصول عن بعد.



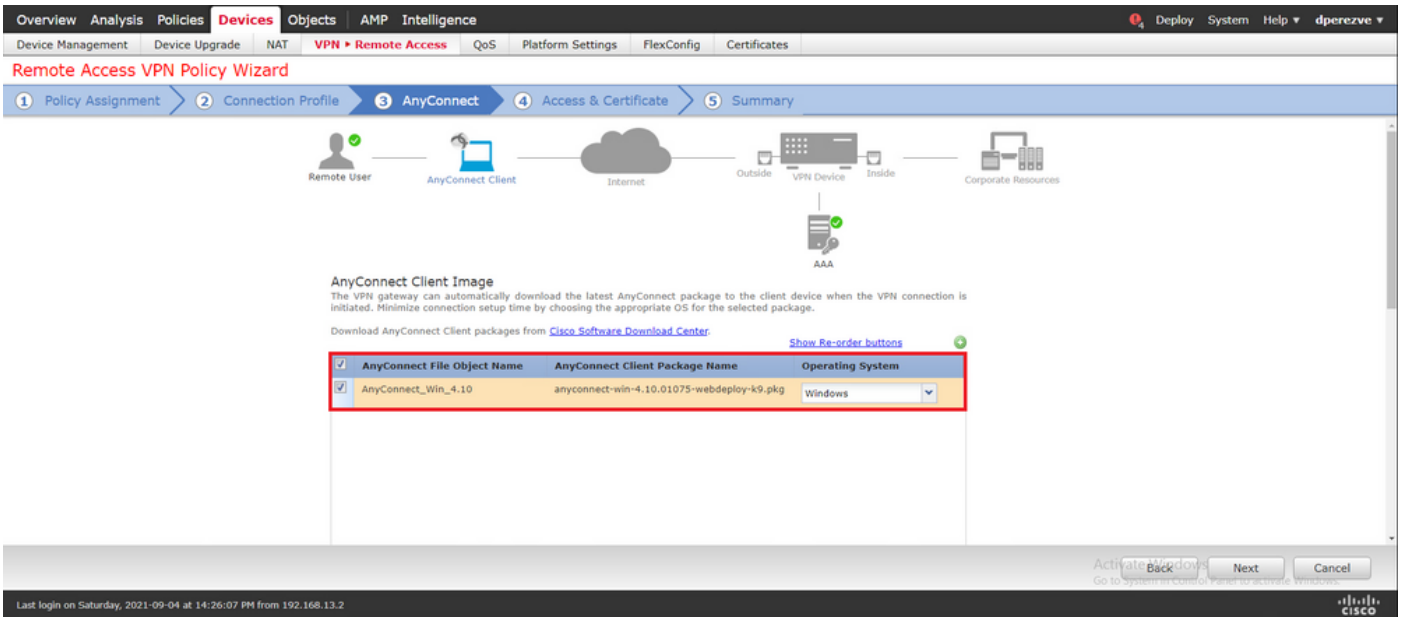
أختر التالي للتنقل إلى تكوين ملف تعريف الاتصال. قم بتعريف اسم لتوصيف التوصيل واختر AAA فقط كطريقة مصادقة. ثم، في القائمة المنسدلة خادم المصادقة، أختر محلي، وأخيرا، أختر النطاق المحلي الذي تم إنشاؤه في الخطوة 4 في القائمة المنسدلة النطاق المحلي.



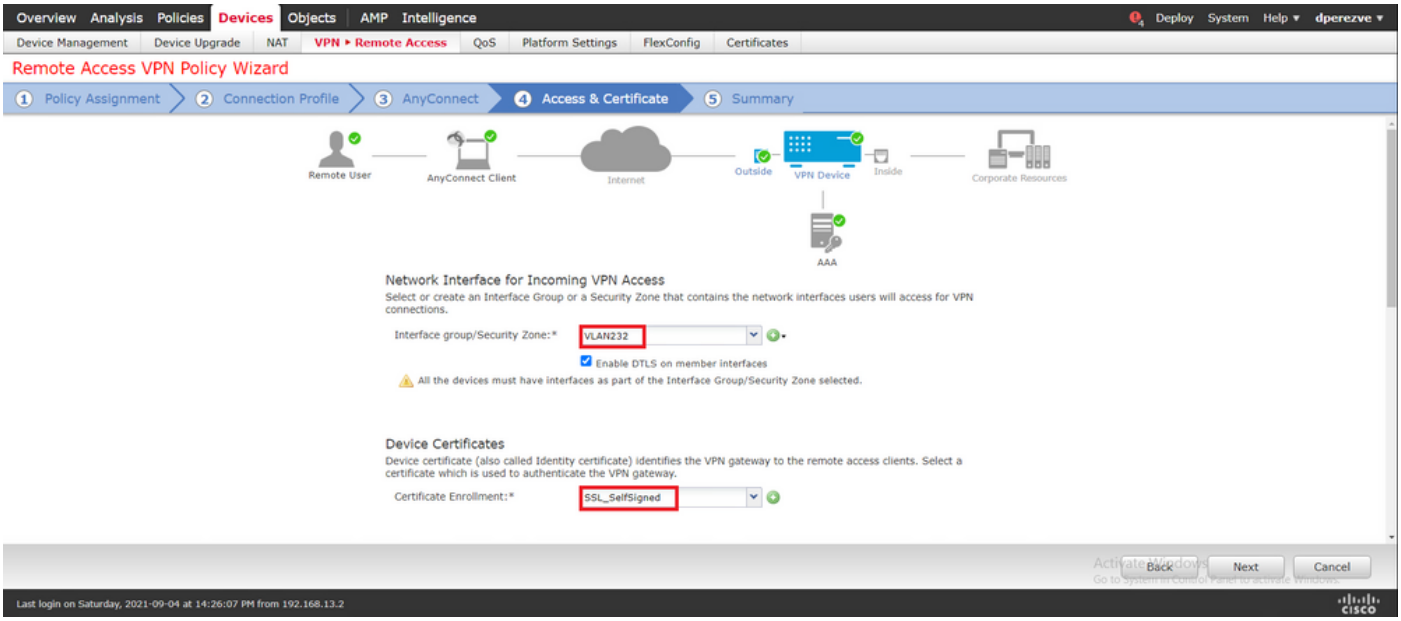
قم بالتمرير إلى أسفل على نفس الصفحة، ثم أختر أيقونة القلم الرصاص في قسم تجمع عناوين IPv4 لتحديد تجمع IP المستخدم من قبل عملاء Cisco الآمن.



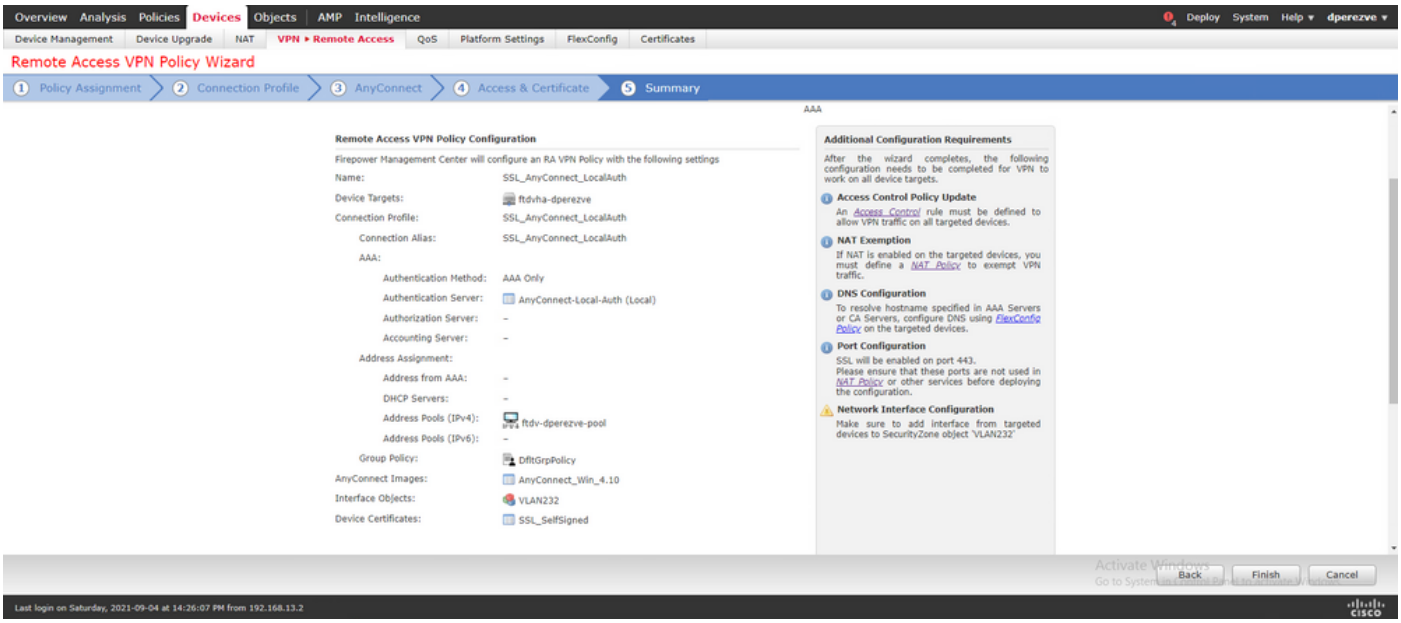
أخترت بعد ذلك in order to نقلت إلى AnyConnect قسم. الآن، أختر صورة عميل Cisco الآمن التي تم تحميلها في الخطوة 2.



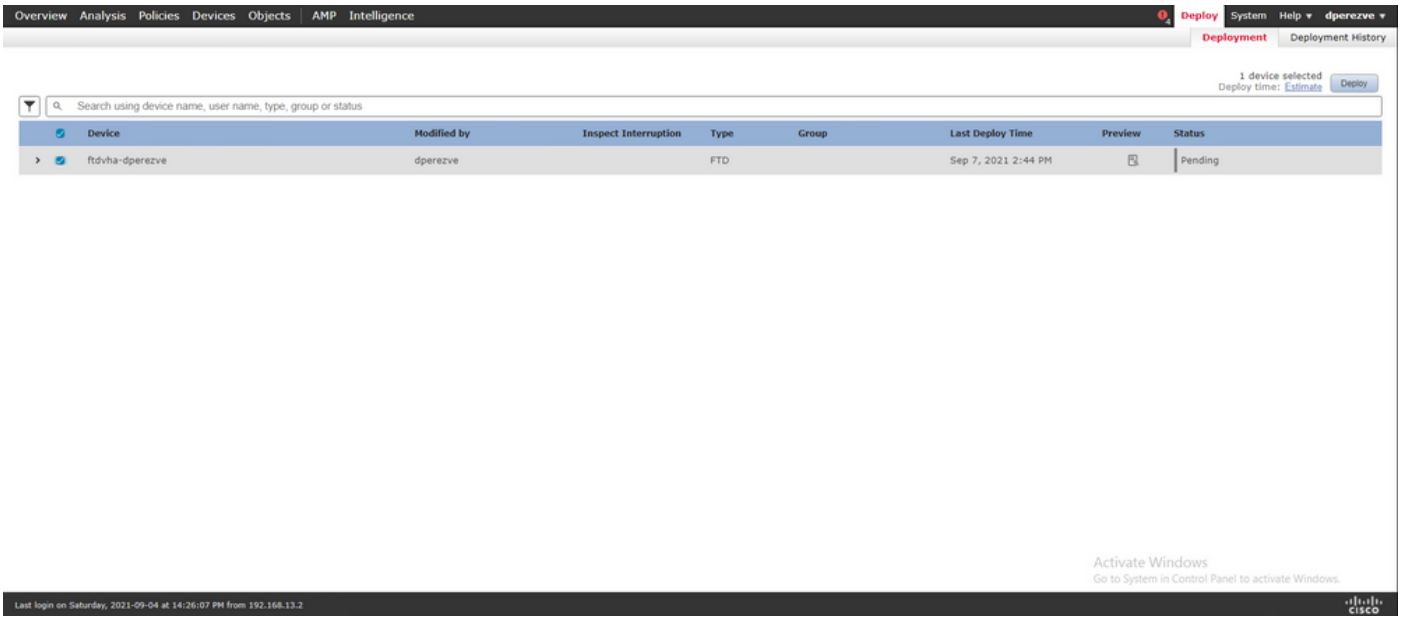
أختر التالي للتنقل إلى قسم الوصول والشهادة. في القائمة المنسدلة مجموعة الواجهة/منطقة الأمان ، أختر الواجهة التي يلزم تمكين Cisco Secure Client (AnyConnect) فيها. ثم، في القائمة المنسدلة تسجيل الشهادة، أختر الشهادة التي تم إنشاؤها في الخطوة 3.



أخيرا، أخترت بعد ذلك in order to رأيت خلاصة من ال cisco يأمن زبون تشكيل.

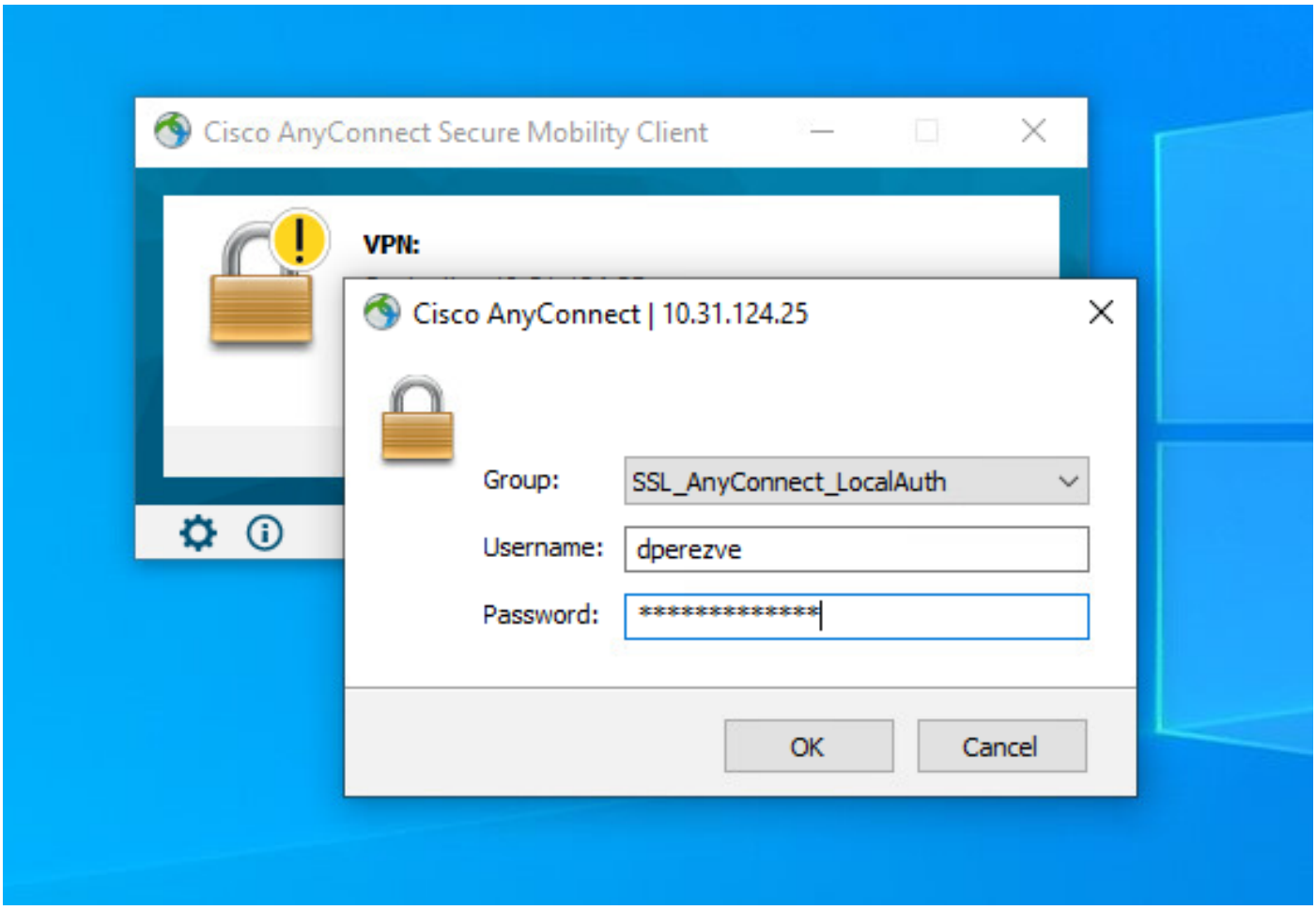


إذا كانت جميع الإعدادات صحيحة، أختر إنهاء ونشر التغييرات على FTD.

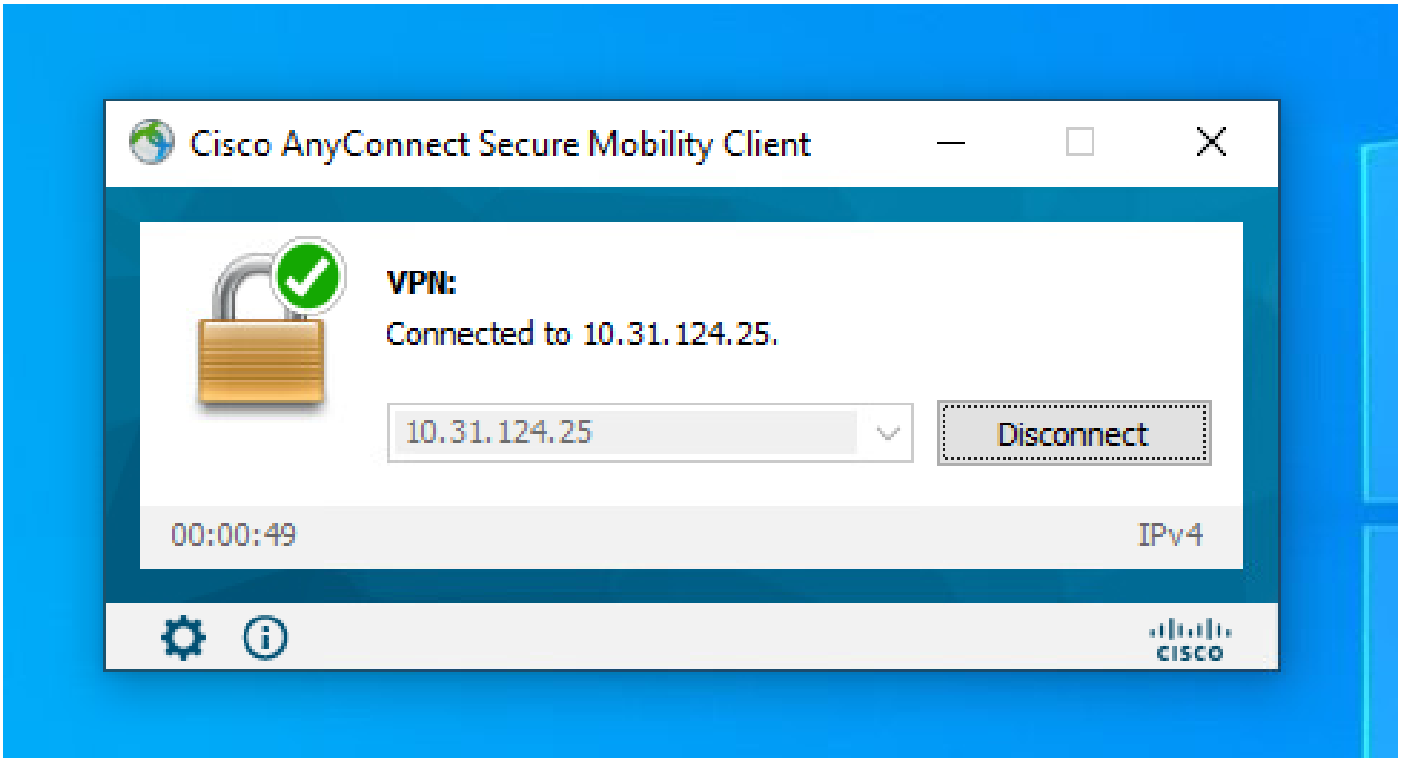


التحقق من الصحة

بمجرد نجاح النشر، ابدأ اتصال Cisco AnyConnect Secure Mobility Client من عميل Windows إلى FTD. يجب أن يكون اسم المستخدم وكلمة المرور المستخدمين في مطالبة المصادقة هما نفس الشيء الذي تم إنشاؤه في الخطوة 4.



بمجرد اعتماد بيانات الاعتماد من قبل FTD، يجب أن يعرض تطبيق Cisco AnyConnect Secure Mobility Client حالة الاتصال.



من FTD يمكنك تشغيل الأمر show vpn-sessionDB anyConnect لعرض جلسات عمل العميل

الآمنة من Cisco النشطة حاليا على جدار الحماية.

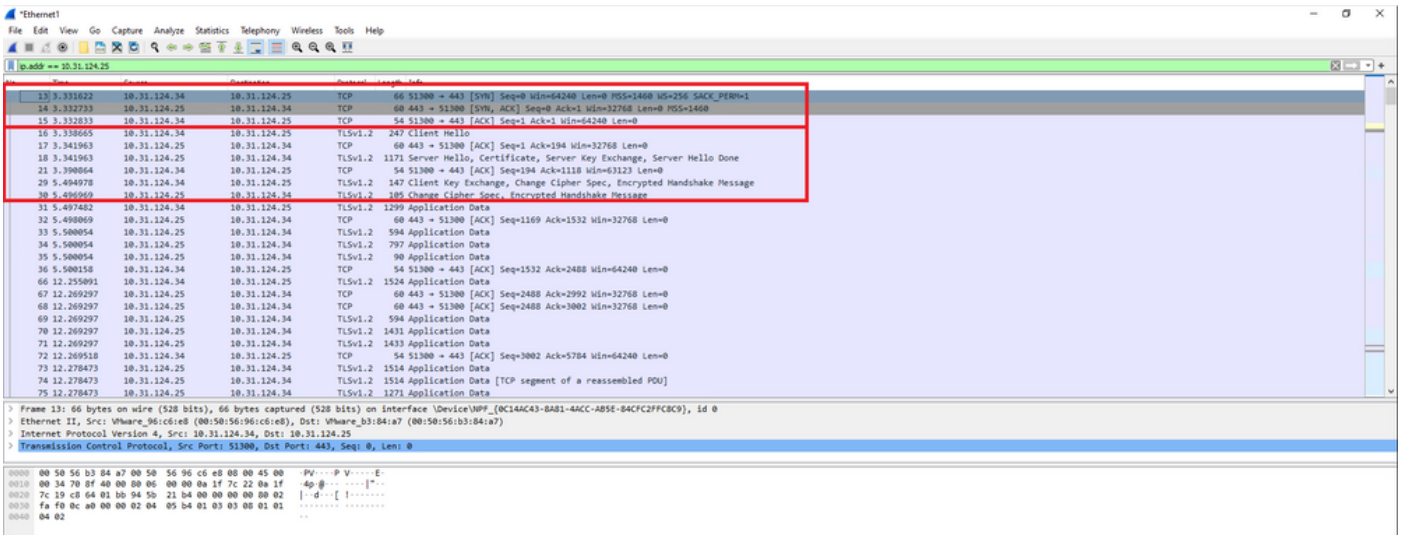
```
firepower# show vpn-sessiondb anyconnect

Session Type: AnyConnect

Username     : dperezve               Index        : 8
Assigned IP  : 172.16.13.1            Public IP    : 10.31.124.34
Protocol     : AnyConnect-Parent SSL-Tunnel DTLS-Tunnel
License      : AnyConnect Premium
Encryption   : AnyConnect-Parent: (1)none  SSL-Tunnel: (1)AES-GCM-256  DTLS-Tunnel: (1)AES-GCM-256
Hashing      : AnyConnect-Parent: (1)none  SSL-Tunnel: (1)SHA384  DTLS-Tunnel: (1)SHA384
Bytes Tx     : 15756                  Bytes Rx     : 14606
Group Policy : DfltGrpPolicy
Tunnel Group : SSL_AnyConnect_LocalAuth
Login Time   : 21:42:33 UTC Tue Sep 7 2021
Duration     : 0h:00m:30s
Inactivity   : 0h:00m:00s
VLAN Mapping : N/A                    VLAN         : none
Audt Sess ID : 0000000000080006137dcc9
Security Grp : none                   Tunnel Zone  : 0
```

استكشاف الأخطاء وإصلاحها

قم بتشغيل الأمر debug webVPN AnyConnect 255 على FTD لترى تدفق اتصال SSL على FTD.

```
firepower# debug webvpn anyconnect 255
```

بالإضافة إلى تصحيح أخطاء العميل الآمن من Cisco، يمكن مالحظة تدفق الاتصال مع التقاط حزمة TCP أيضا. هذا مثال على اتصال ناجح، يتم إكمال ثالث عمليات مصافحة دورية بين عميل Windows و FTD، يتبعها مصافحة SSL تستخدم للموافقة على عمليات التشفير.



بعد عمليات تأكيد الاتصال بالبروتوكول، يجب أن يقوم FTD بالتحقق من صحة بيانات الاعتماد باستخدام المعلومات المخزنة في النطاق المحلي.

تجمع حزمة DART واتصل ب Cisco TAC لمزيد من البحث.

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).