تكوين نفق الجهاز على الوصول الآمن من Cisco

المحتويات

المقدمة

الرسم التخطيطي للشبكة

المتطلبات الأساسية

المتطلبات

المكونات المستخدمة

معلومات أساسية

العمل على Machine Tunnel

القيود

التكوين

التكوين - 1 خطوة: إنشاء مستخدم الجهاز باستخدام machine@sse.com:مستخدم

الخطوة 1 - الإعدادات العامة

الخطوة 2 - شهادة الجهاز

الخطوة 3 - تحويل المسار (النفق المستقل) على جهاز التوجيه

الخطوة 4 - تكوين العميل الآمن من Cisco

الخطوة 5 - التحقق من وجود machine@sse.com User في Cisco Secure Access

الخطوة 6 - إنشاء شهادات CA الموقعة لـ machine@sse.com

الخطوة 7 - استيراد شهادة الجهاز على جهاز الكمبيوتر

الخطوة 8 - اتصال نفق الجهاز

التكوين - 2 خطوة: إنشاء مستخدم باستخدام الجهاز نفق التكوين

الخطوة 5 - تكوين مزامنة AD الداخلية على Cisco Secure Access

الخطوة 6 - تكوين تجميع نفق الثقة الداخلية

الخطوة 7 - إنشاء شهادة نفق الثقة الداخلية

الخطوة 8 - اتصال نفق الجهاز

التكوين - 3 خطوة: إنشاء مستخدم الجهاز باستخدام نفق التكوين

الخطوة 5 - تكوين مزامنة AD المستخدمين على Cisco Secure Access

الخطوة 6 - تكوين تجميع المستخدمين

الخطوة 7 - إنشاء شهادة نفق الثقة الداخلية

الخطوة 8 - اتصال نفق الجهاز

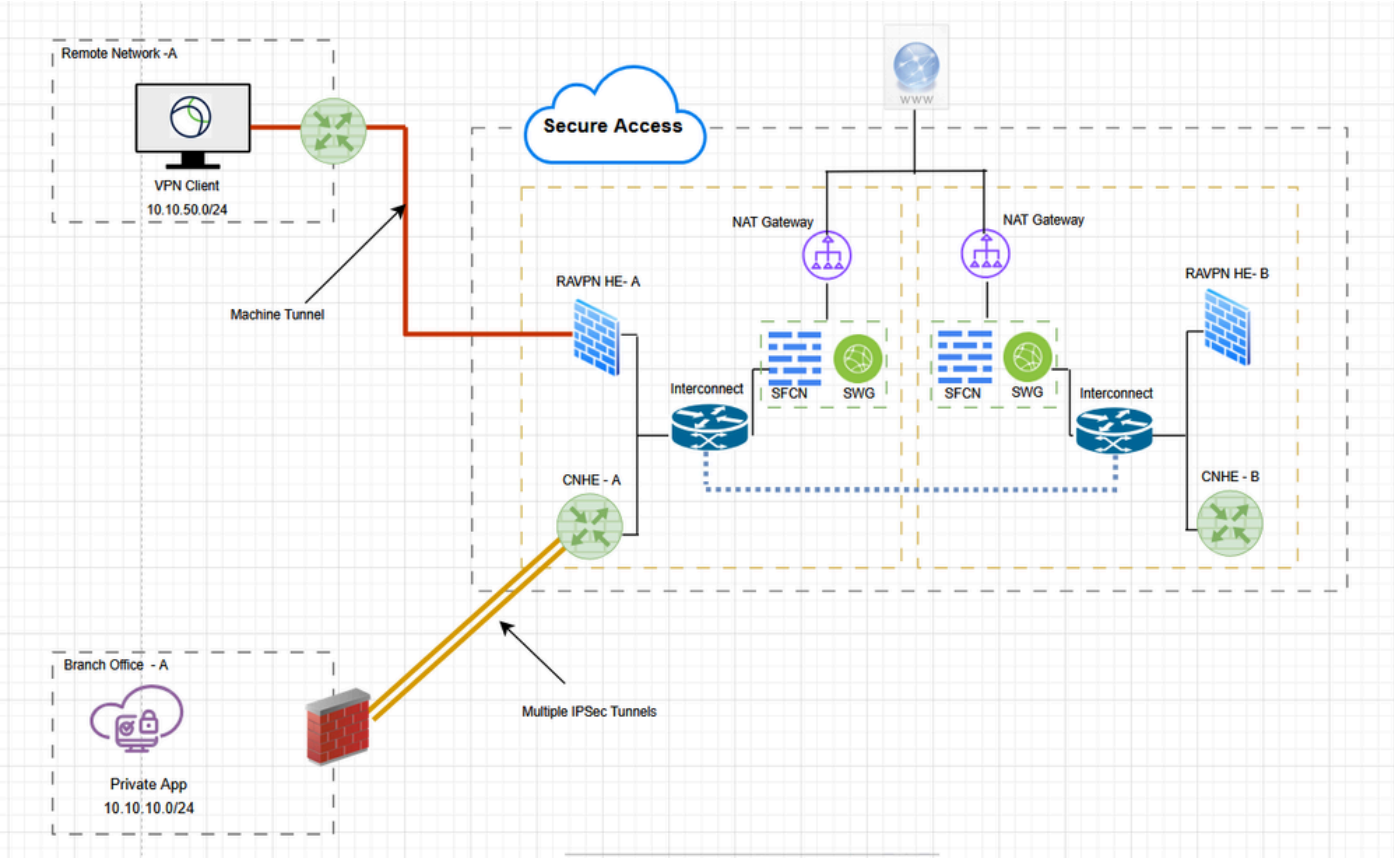
استكشاف الأخطاء وإصلاحها

المقدمة

يوضح هذا المستند كيفية تكوين الوصول الآمن كبوابة شبكة VPN وقبول الاتصالات

من العميل الآمن من خلال نفق جهاز VPN.

الرسم التخطيطي للشبكة



المتطلبات الأساسية

- دور المسؤول الكامل في الوصول الآمن
- مستخدم ip بركة على cisco أمان منفذ
- تكوين ملف تعريف VPN لمستخدم واحد على الأقل على Cisco Secure Access

المتطلبات

يوصى بأن تكون لديك معرفة بالمواضيع التالية:

- OpenSSL
- شهادات عام 509

المكونات المستخدمة

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

- Cisco Secure Access
- Cisco Secure Client 5.1.10
- نظام التشغيل Windows 11
- Windows Server 2019 - CA

تم إنشاء المعلومات الواردة في هذا المستند من الأجهزة الموجودة في بيئة معملية خاصة. إذا كانت شبكتك قيد التشغيل، فتأكد من فهمك للتأثير المحتمل لأي أمر.

معلومات أساسية

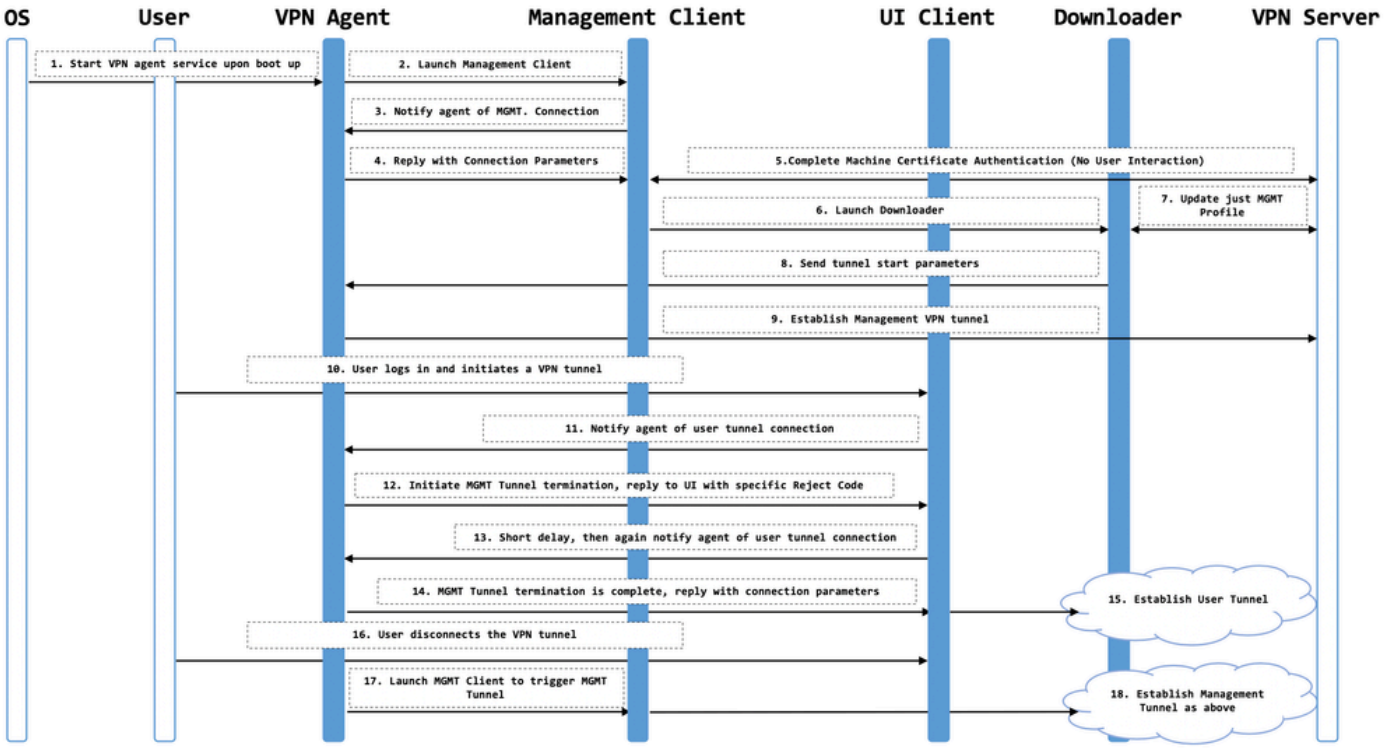
يضمن نفق جاز Secure Access VPN الاتصال بشبكة الشركة كلما تم تشغيل نظام العميل، وليس فقط عند تأسيس اتصال VPN بواسطة المستخدم النهائي. يمكن تنفيذ إدارة الحزم على نطاق النهاية خارج المكتب، وخاصة الأجهزة التي يتم توصيلها بشكل متكرر بواسطة المستخدم، عبر شبكة VPN، بشبكة المكتب. كما تستفيد البرامج النصية لتسجيل الدخول إلى نظام التشغيل Endpoint OS التي تتطلب اتصال شبكة الشركة من هذه الميزة. ولإنشاء هذا النفق بدون تفاعل المستخدم، يتم إستخدام المصادقة المستندة إلى الشهادة.

يتيح نفق جاز الوصول الآمن للمستخدمين إمكانية اتصال Cisco Secure Client دون تدخل المستخدم قبل تسجيل دخول المستخدم. يتم تشغيل نفق جاز الوصول الآمن عندما تكون نقطة النهاية خارج نطاق العمل ويتم فصلها من شبكة VPN بدأها المستخدم. يكون نفق جاز Secure Access VPN شفافا للمستخدم النهائي ويقطع الاتصال تلقائيا عندما يقوم المستخدم بتهيئة VPN.

العمل على Machine Tunnel

يتم بدء تشغيل خدمة عميل VPN الآمن تلقائيا عند تمهيد النظام. يستخدم عميل VPN ميزة نفق الجاز. في حالة تمكين ميزة نفق الجاز، يقوم العميل ببدء تطبيق عميل الإدارة لبدء اتصال نفق الجاز. يستخدم تطبيق عميل الإدارة إدخال المضيف من ملف تعريف VPN لبدء الاتصال. ثم يتم إنشاء نفق VPN الآمن من ملف تعريف VPN لبدء اتصال نفق الجاز. لا يتم إجراء أي تحديث للبرامج أثناء اتصال نفق الجاز لأنه، مع إستثناء واحد: عملاء، مع المفترض أن يكون نفق الجاز شفافا للمستخدم.

يقوم المستخدم ببدء نفق VPN عبر "العميل الآمن"، والذي يقوم بتشغيل إنهاء نفق الجهاز. عند إنهاء النفق الآلي، يستمر إنشاء نفق المستخدم كالمعتاد. يقوم المستخدم بقطع اتصال نفق VPN، والذي يؤدي إلى تشغيل إعادة الإنشاء التلقائية لنفق الجهاز.



القيود

- تفاعل المستخدم غير مدعوم.
- المصادقة المستندة إلى الشهادة من خلال "مخزن الشهادات الآلي" (في Windows) مدعومة فقط.
- يتم فرض فحص شهادة الخادم المقيد.
- الوكيل الخاص غير معتمد.
- الوكيل العام غير معتمد (يتم دعم القيمة الأصلية للوكيل على الأنظمة الأساسية حيث لا يتم إسترداد إعدادات الوكيل الأصلي من المستعرض).
- البرامج النصية لتخصيص العميل الآمن غير مدعومة

التكوين

الطريقة 1 - تكوين نفق الجهاز باستخدام المستخدم: machine@sse.com

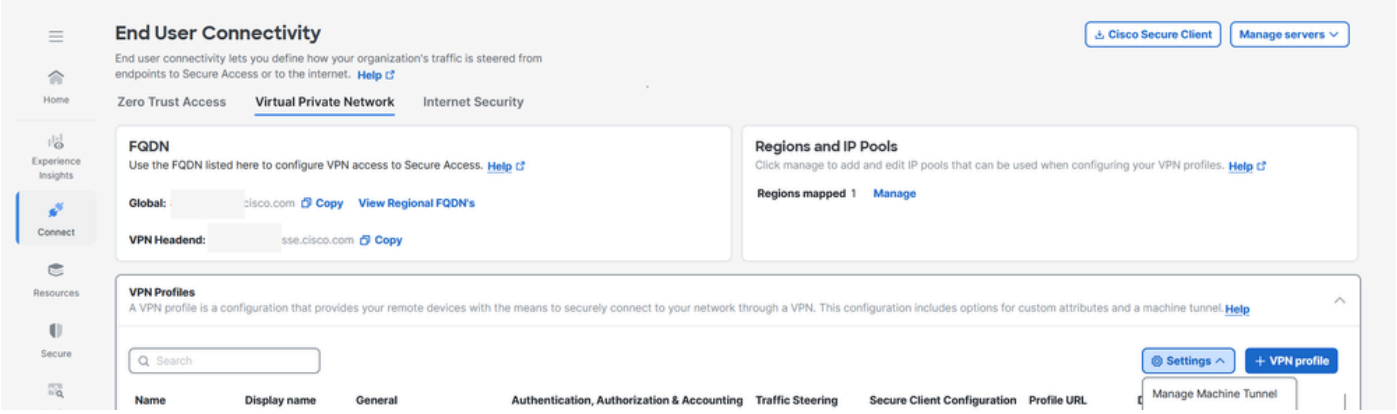
الخطوة 1 - الإعدادات العامة

قم بتكوين الإعدادات العامة، بما في ذلك المجال والبروتوكولات التي يستخدمها نفق الجهاز.

1. انتقل إلى الاتصال > اتصال المستخدم النهائي > الشبكة الخاصة الظاهرية.

2. انتقل إلى توصيفات VPN وشكل إعدادات نفق الجهاز.

أ. انقر فوق الإعدادات، واختر إدارة نفق الجهاز من القائمة المنسدلة.



---

3. أدخل المجال الافتراضي.

4. تم تعيين خادم DNS المعين من خلال صفحة إدارة المناطق وتجمع IP كخادم افتراضي. يمكنك قبول خادم DNS الافتراضي، أو إختيار خادم DNS آخر من القائمة المنسدلة، أو انقر فوق + إضافة لإضافة زوج خادم DNS جديد. يؤدي تحديد خادم DNS آخر أو إضافة خادم DNS جديد إلى إستبدال هذا الخادم الافتراضي.

5. حدد تجمع IP واحد لكل منطقة من القائمة المنسدلة لتجمعات IP. يجب أن تحتوي ملفات تعريف VPN على تجمع IP واحد على الأقل تم تعيينه في كل منطقة لتكوين صالح.

6. حدد بروتوكول النفق الذي يستخدمه نفق الجهاز هذا:

- TLS/DTLS
- IPSec (IKEv2)

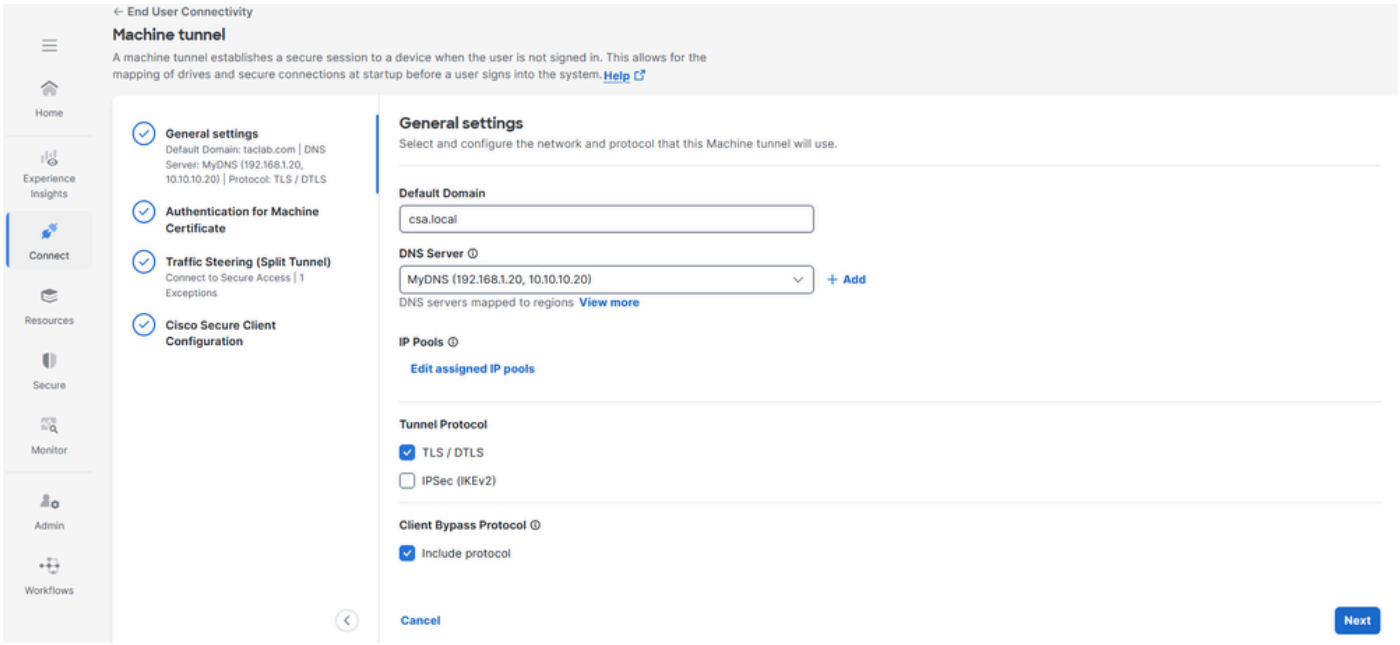
يجب تحديد بروتوكول واحد على الأقل.

7. بشكل إختياري، تحقق من بروتوكول تضمين لإنفاذ بروتوكول تجاوز العميل.

---

1. إذا تم تمكين بروتوكول تجاوز العميل لبروتوكول IP ولم يتم تكوين تجمع عناوين لذلك البروتوكول (بمعنى آخر، لم يتم تعيين عنوان IP لذلك البروتوكول إلى العميل بواسطة ASA)، ال يتم إرسال أي حركة مرور IP باستخدام هذا البروتوكول من خلال نفق VPN. يتم إسقاطها خارج النفق.

2. إذا تم تعطيل بروتوكول تجاوز العميل، ولم يتم تكوين تجمع عناوين لذلك البروتوكول، يقوم العميل بإسقاط جميع حركات مرور البيانات لبروتوكول IP هذا بمجرد إنشاء نفق VPN.



---

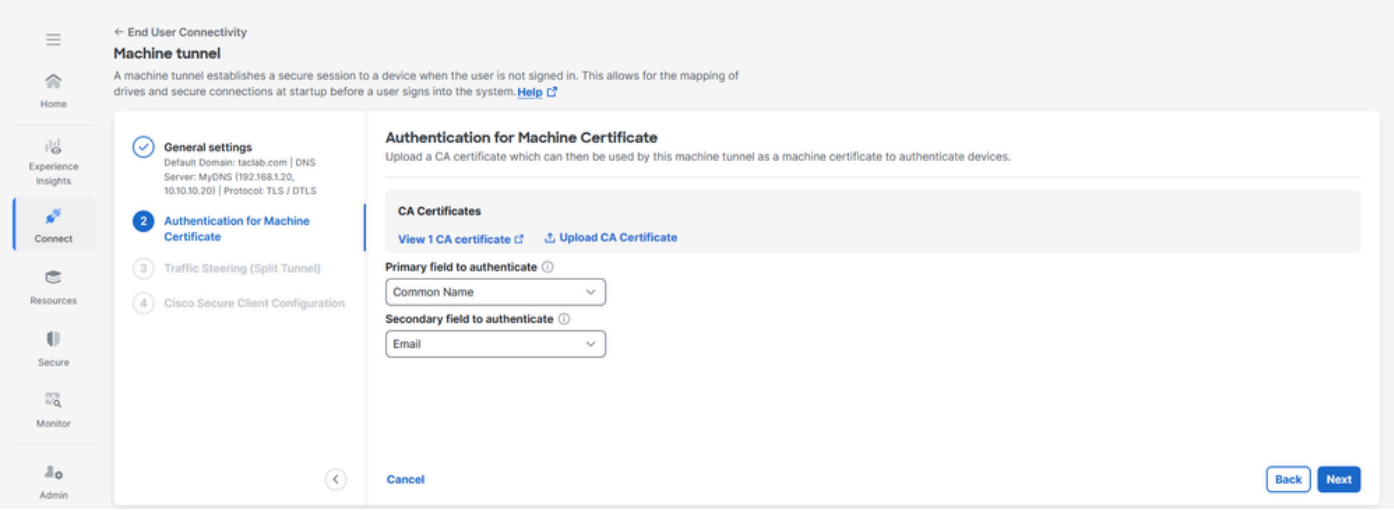
3. انقر فوق التالي

الخطوة 2 - مصادقة شهادة الجهاز

يكون نفق الجهاز شفافا للمستخدم النهائي ويقطع الاتصال تلقائيا عندما يقوم المستخدم بتهيئة جلسة VPN. لإنشاء هذا النفق بدون تفاعل المستخدم، يتم استخدام المصادقة المستندة إلى الشهادة:

1. أختر شهادات المرجع المصدق من القائمة أو انقر على تحميل شهادات المرجع المصدق.

2. حدد حقول المصادقة المستندة إلى الشهادة. لمزيد من المعلومات، راجع حقول المصادقة المستندة إلى الشهادة.



3. انقر فوق التالي

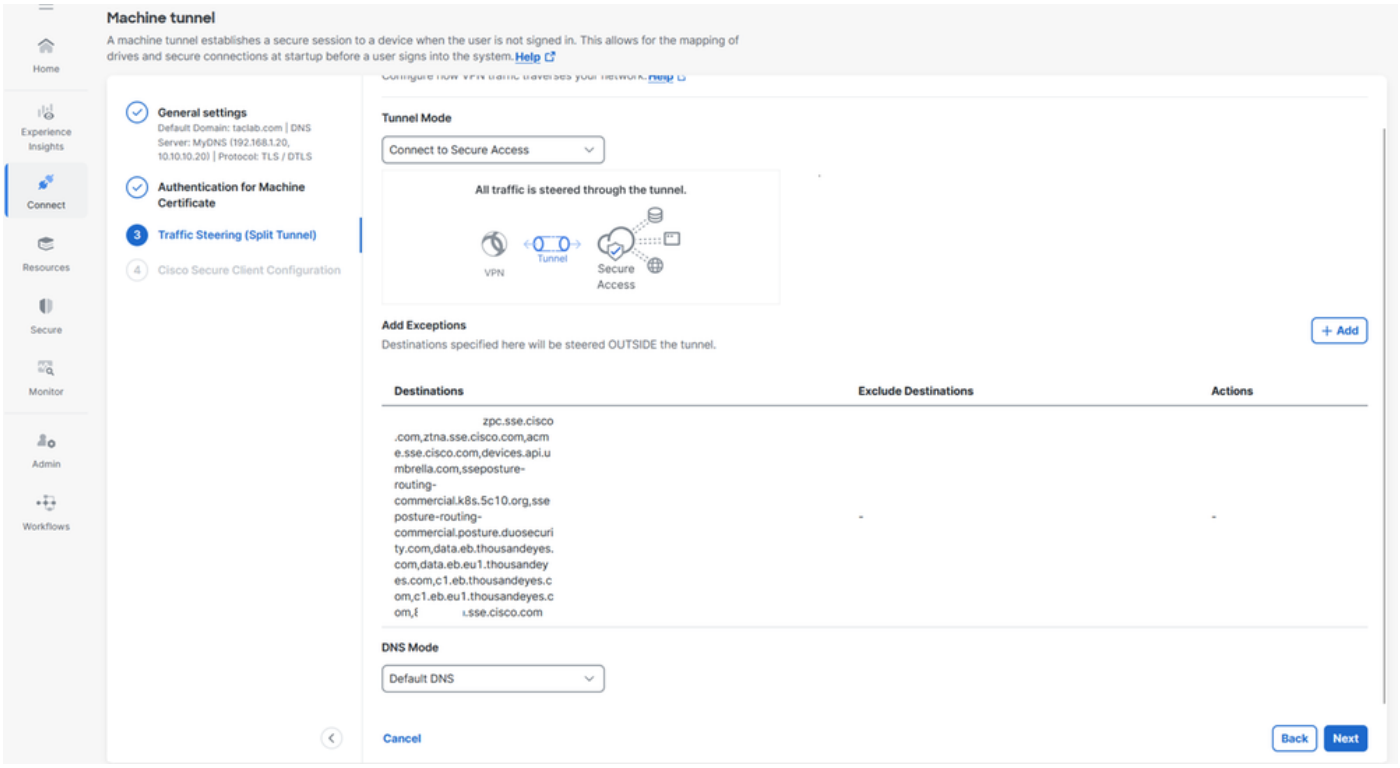
الخطوة 3 - توجيه حركة المرور (النفق المقسم)

باﻟﻨﺴﺒﺔ لتوجيه حركة المرور (النفق المنقسم)، يمكنك تكوين نفق جاز للحفاظ على اتصال نفق كامل للوصول الآمن، أو تكوينه لاستخدام اتصال نفق انقسام لتوجيه حركة المرور من خلال شبكة VPN فقط إذا لزم الأمر. لمزيد من المعلومات، راجع توجيه حركة مرور Machine Tunnel.

1. حدد وضع النفق.

2. وفقا لتحديد وضع النفق، يمكنك إضافة إستثناءات.

3. حدد وضع DNS.

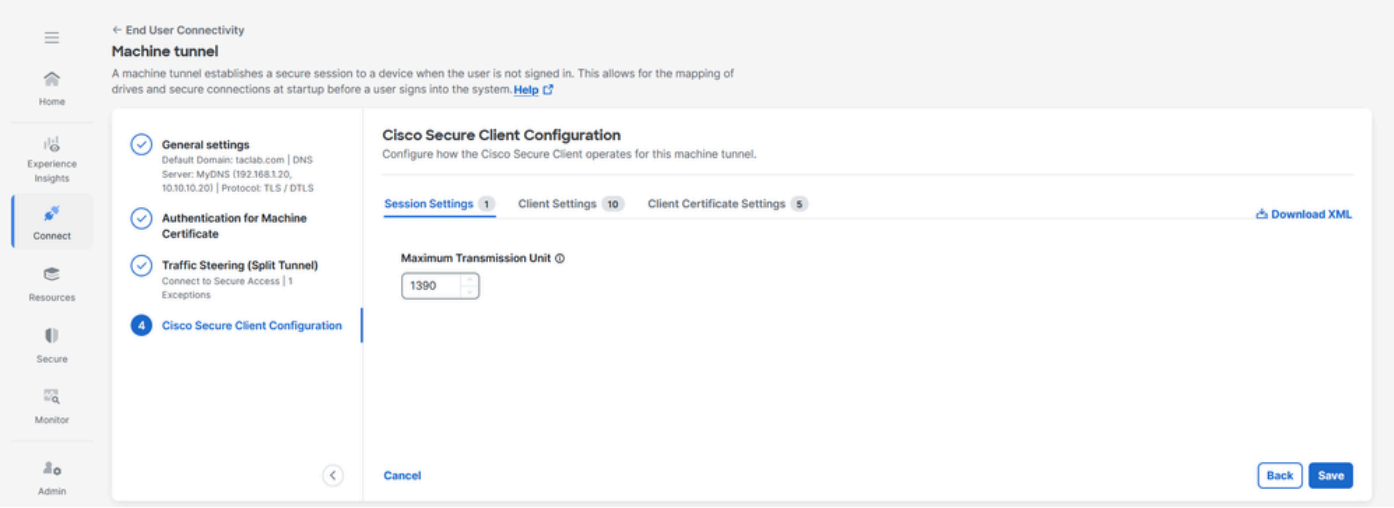


4. انقر فوق التالي.

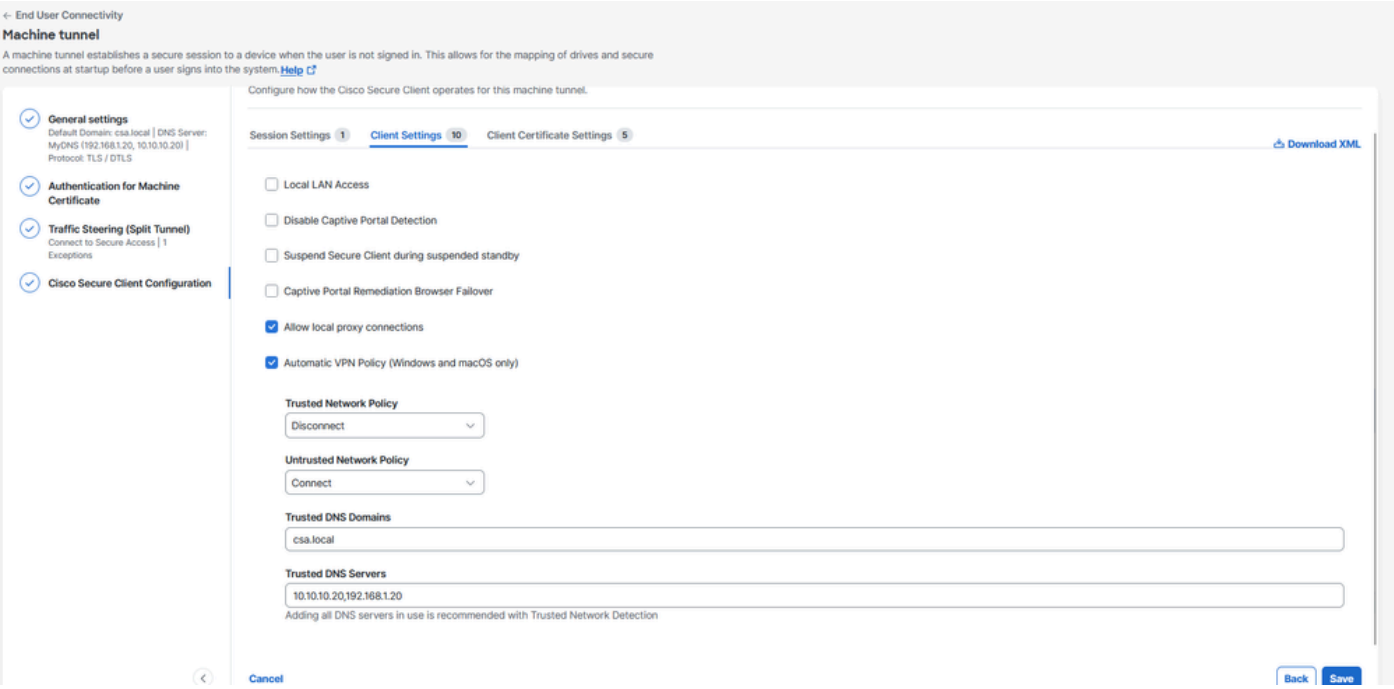
الخطوة 4 - تكوين العميل الآمن من Cisco

يمكنك تعديل مجموعة فرعية من إعدادات Cisco Secure Client استنادا إلى إحتياجات نفق جهاز VPN معين. لمزيد من المعلومات، ارجع إلى: تكوين العميل الآمن.

1. تحقق من وحدة الإرسال القصوى، وهي أكبر حجم للحزمة التي يمكن إرسالها في نفق VPN دون تجزئة.



2. إعدادات العميل، ارجع إلى إعدادات عميل Machine Tunnel للحصول على مزيد من المعلومات.



---

3. إعدادات شهادة العميل، حدد الخيارات وفقا لذلك:

أ. تجاوز مخزن شهادات Windows: يسمح للمسؤول بتوجيه "العميل الآمن" لاستخدام الشهادات في مخزن شهادات "جهاز Windows (النظام المحلي)" لمصادقة شهادة العميل.

ب. تحديد الشهادة تلقائيا: عند تكوين مصادقة شهادات متعددة على البوابة الآمنة.

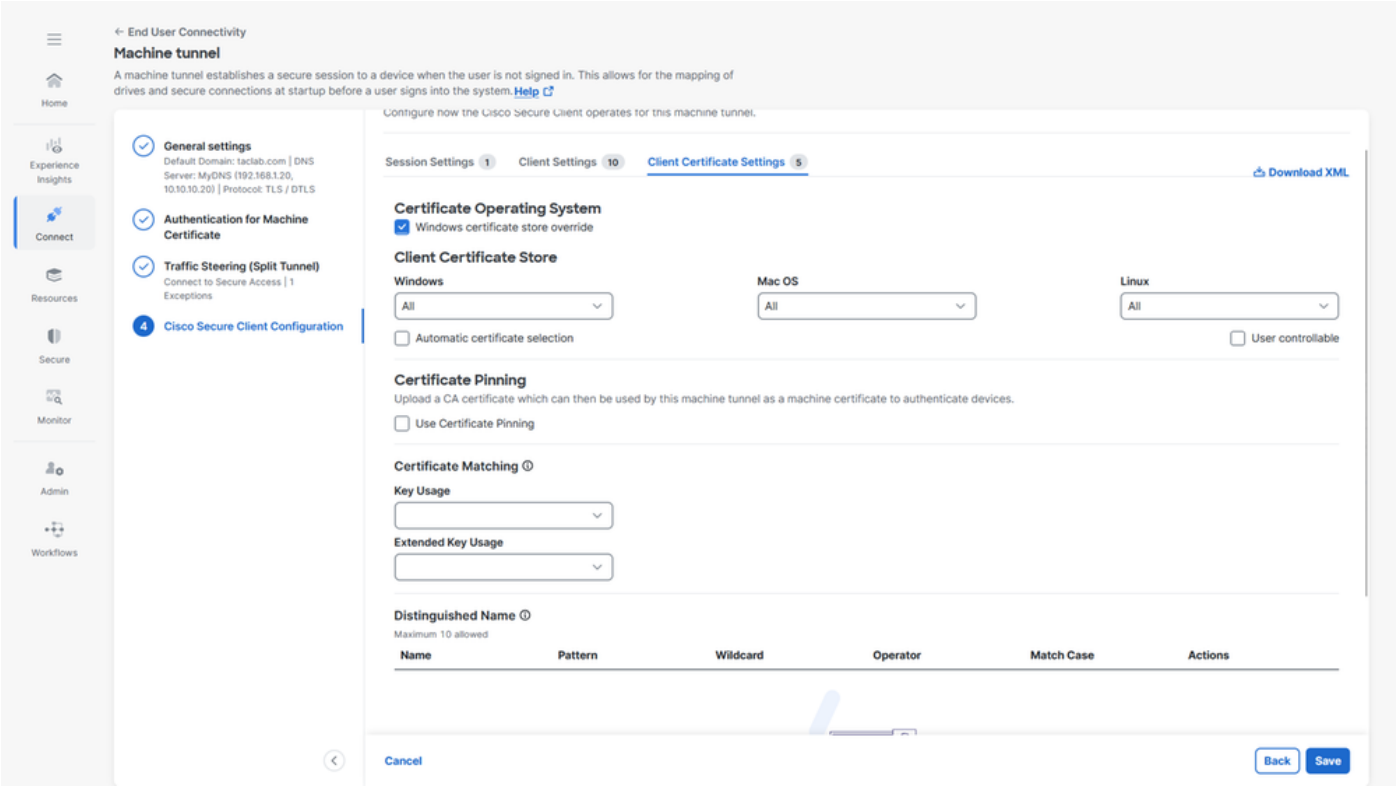
ج. تثبيت الشهادة: شهادة المرجع المصدق المستخدمة من قبل نفق الجهاز كشهادة جهاز للمصادقة على الأجهزة.

د. مطابقة الشهادة: في حالة عدم تحديد معايير مطابقة الشهادة، يقوم Cisco Secure Client بتطبيق قواعد مطابقة الشهادة:

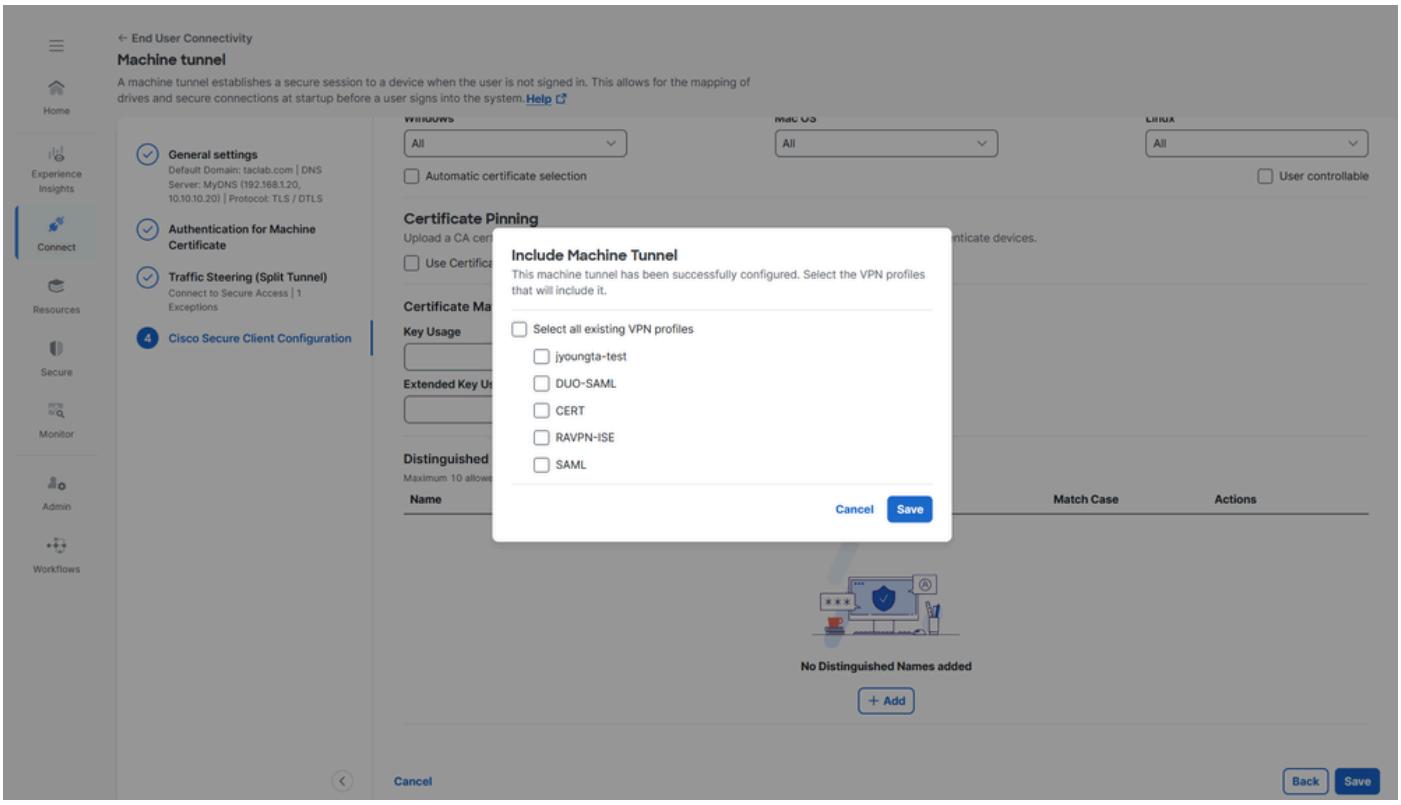
ط. إستخدام المفتاح: Digital_Signature

ثانياً. إستخدام المفتاح الموسع: مصادقة العميل

هـ. الاسم المميز: يحدد الأسماء المميزة (DNs) لمعايير المطابقة الدقيقة عند إختيار شهادات العميل المقبولة. عند إضافة أسماء مميزة متعددة، يتم التحقق من كل شهادة مقابل كل الإدخالات، ويجب أن تتطابق جميعها.

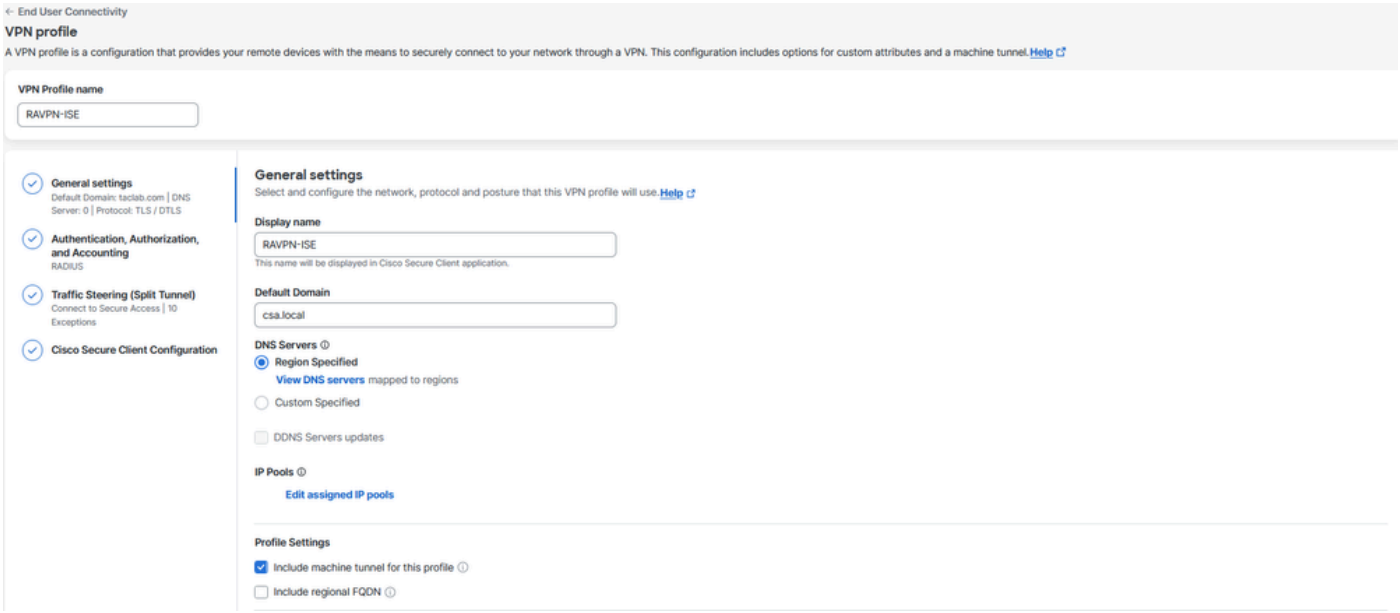


4. قم بتعيين ملف تعريف Machine Tunnel إلى ملف تعريف VPN للمستخدم، انقر فوق حفظ وهناك خيار لتحديد ملفات تعريف VPN للمستخدم.



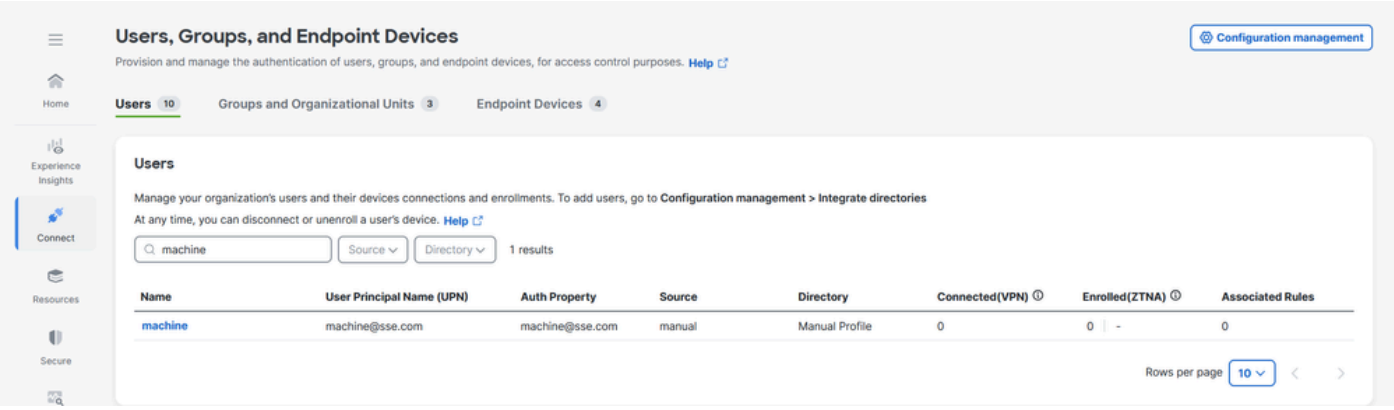
5. انقر فوق حفظ.

6. تحقق مما إذا كان ملف تعريف Machine Tunnel ملحقا بملف تعريف VPN للمستخدم.



الخطوة 5 - التحقق من وجود مستخدم machine@sse.com في Cisco Secure Access

1. انتقل إلى الاتصال > المستخدمون والمجموعات وأجهزة نقاط النهاية > المستخدمون.



---

2. إذا لم يكن المستخدم machine@sse.com موجودا، قم باالستيراد يدويا. لمزيد من المعلومات، راجع: استيراد المستخدمين والمجموعات اليدوية

الخطوة 6 - إنشاء شهادة موقعة من المرجع المصدق ل machine@sse.com

1. إنشاء طلب توقيع شهادة:

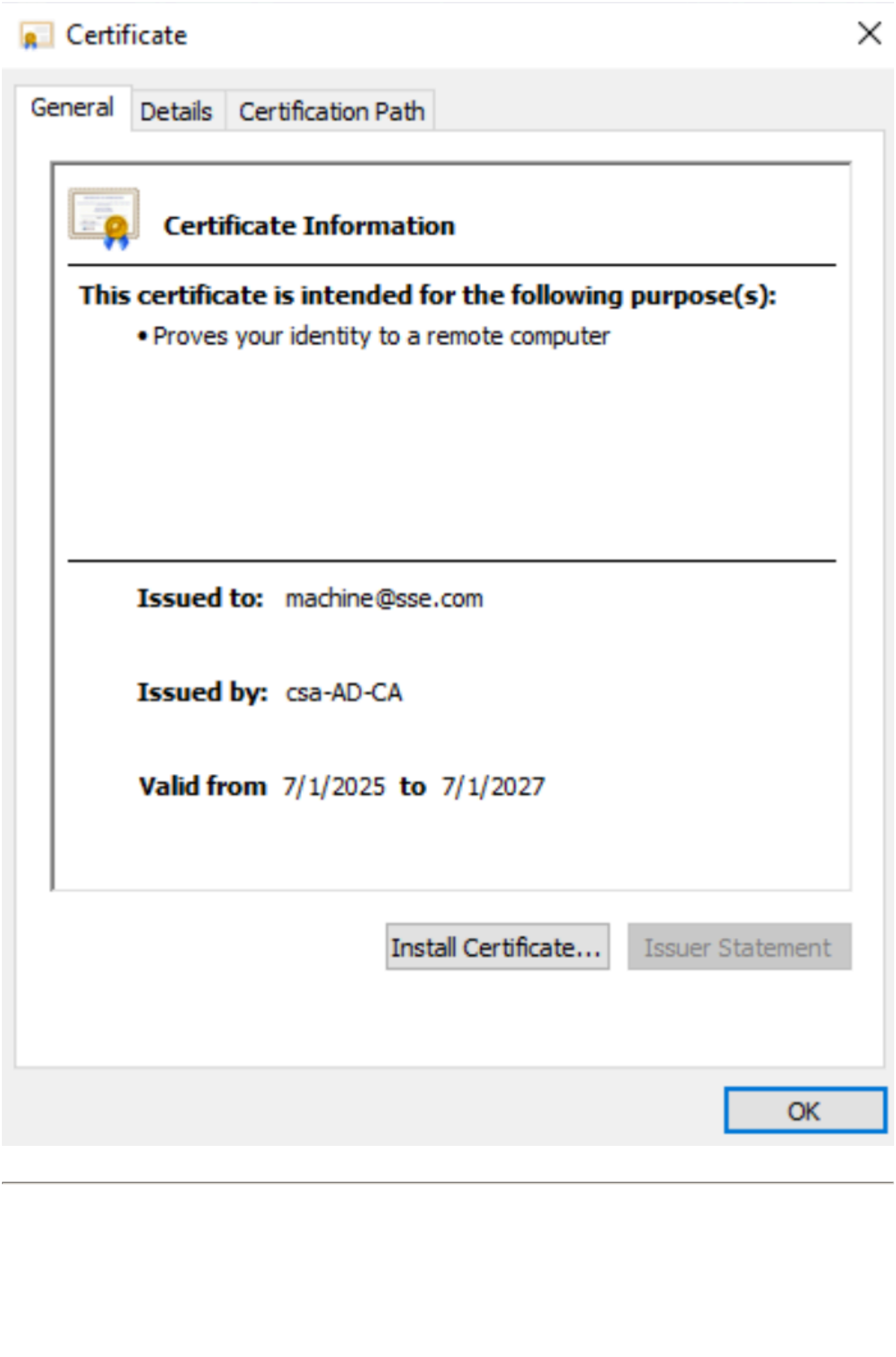
أ. يمكنك إستخدام أي برنامج مولد CSR عبر الإنترنت أو واجهة سطر أوامر (CLI) OpenSSL.

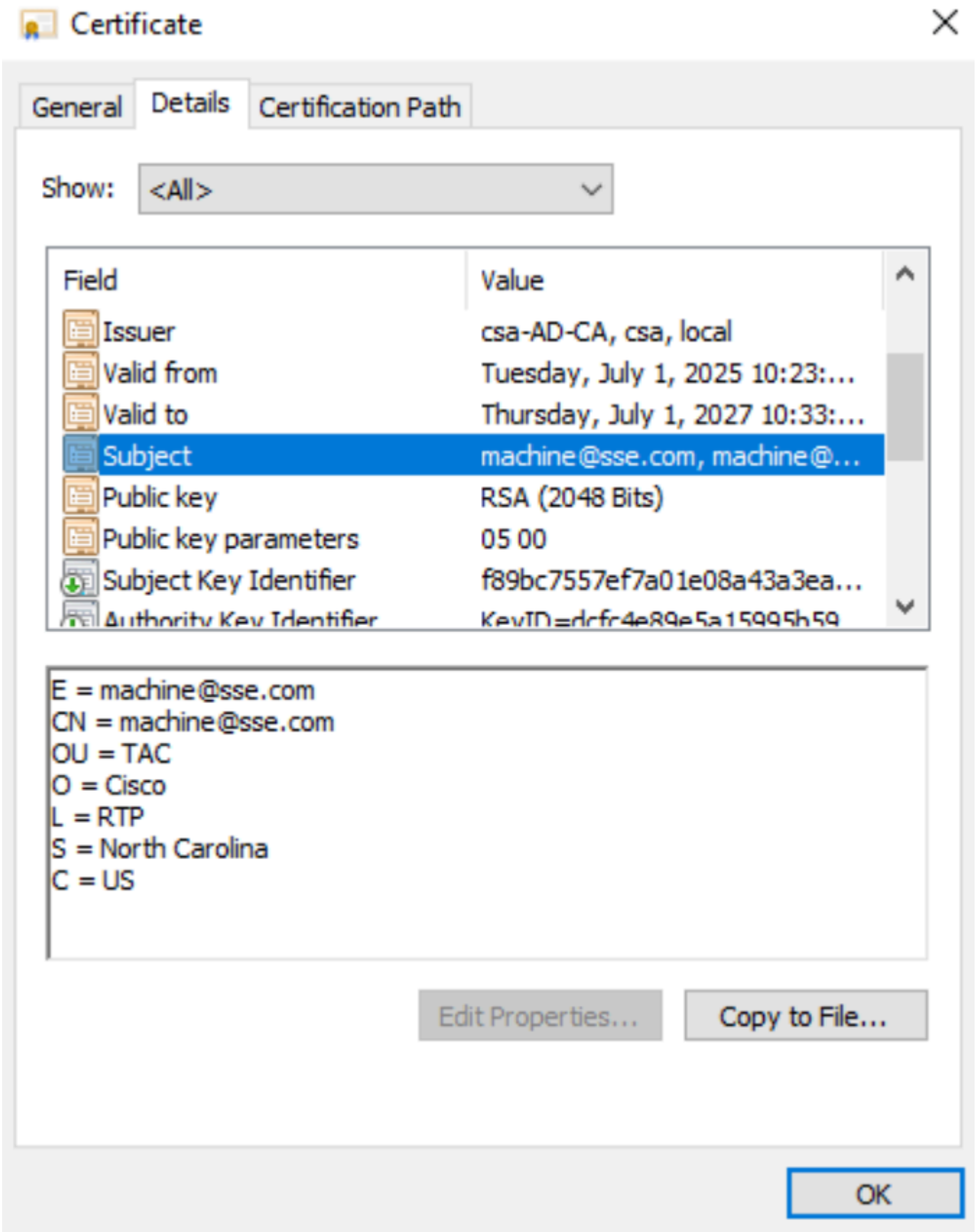
openssl req -new key rsa:2048 -node -keyout cert.key -out cert.csr

```
root@ftd1:/home/admin# openssl req -newkey rsa:2048 -nodes -keyout cert.key -out cert.csr
Generating a RSA private key
.....................................................................................+++++
.....................................................................+++++
writing new private key to 'cert.key'
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:US
State or Province Name (full name) [Some-State]:North Carolina
Locality Name (eg, city) []:RTP
Organization Name (eg, company) [Internet Widgits Pty Ltd]:TAC
Organizational Unit Name (eg, section) []:CiscoTAC
Common Name (e.g. server FQDN or YOUR name) []:machine@sse.com
Email Address []:machine@sse.com

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
```

2. انسخ CSR وإنشاء شهادة جهاز.


Certificate
General
Details
Certification Path
Certificate Information
This certificate is intended for the following purpose(s):
• Proves your identity to a remote computer
Issued to: machine@sse.com
Issued by: csa-AD-CA
Valid from 7/1/2025 to 7/1/2027
Install Certificate...
Issuer Statement
OK



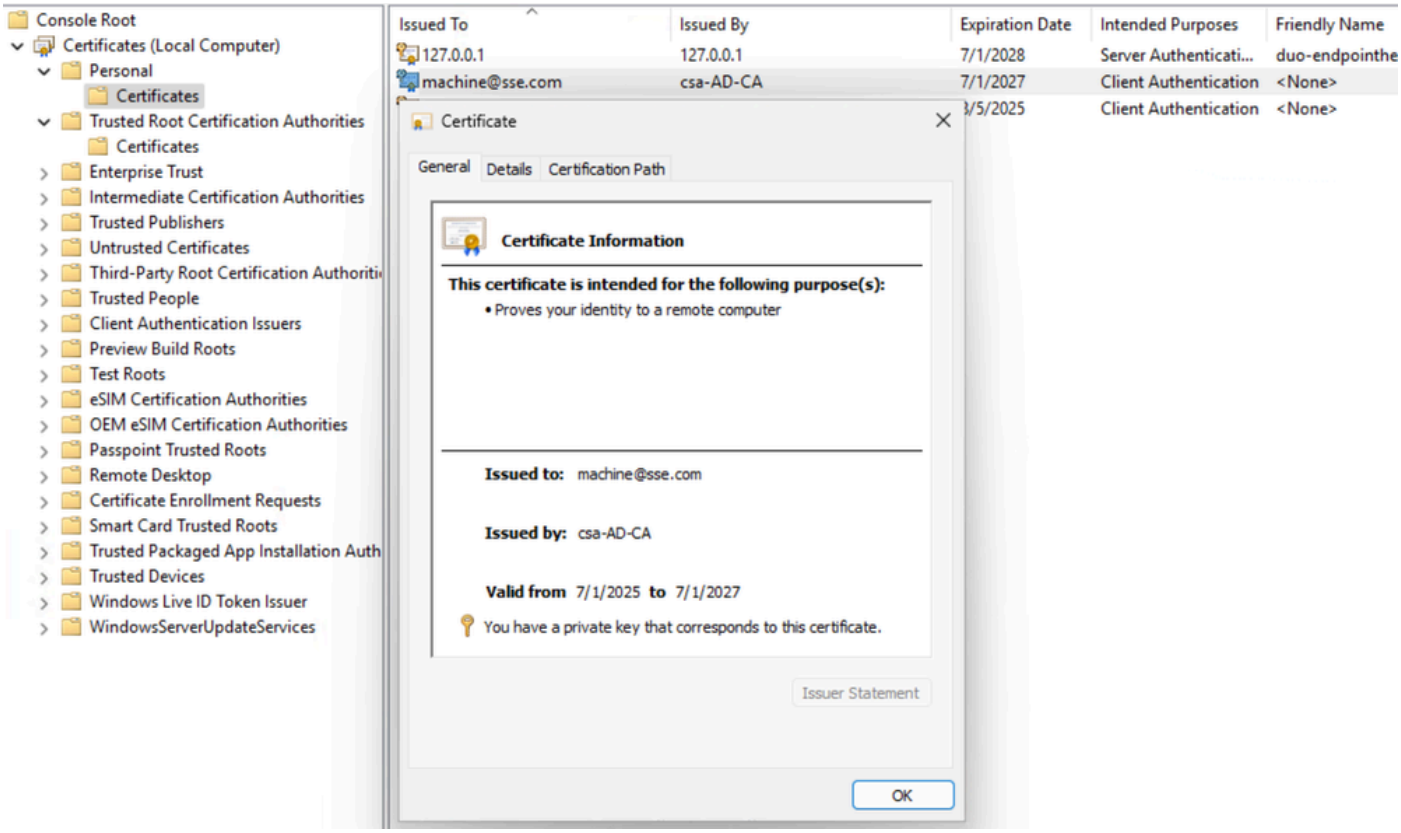
3. تحويل شهادة الجهاز إلى تنسيق PKCS12 باستخدام المفتاح والشهادة المولدة في الخطوات السابقة (الخطوة 1 والخطوة 2) على التوالي:

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

```
root@ftd1:/home/admin# openssl pkcs12 -export -out Machine.p12 -in machine.crt -inkey cert.key
Enter Export Password:
Verifying - Enter Export Password:
root@ftd1:/home/admin#
```

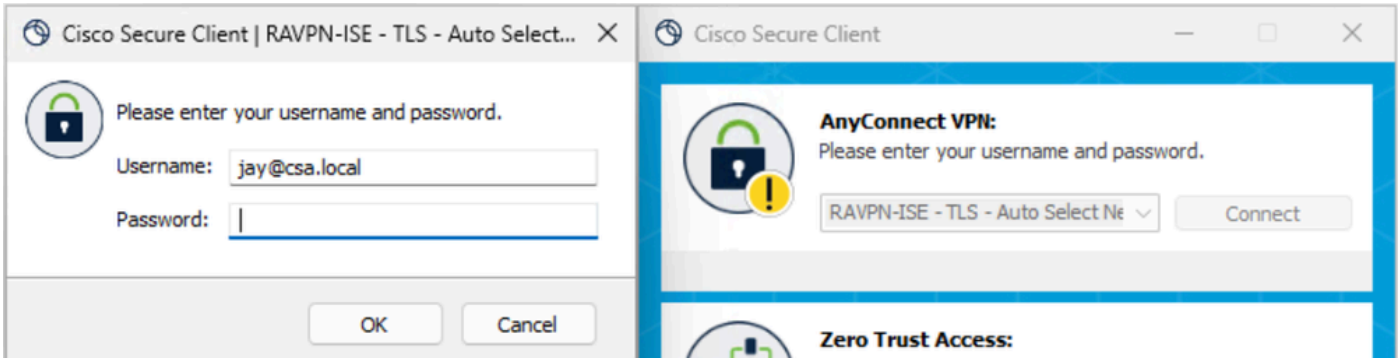
الخطوة 7 - إستيراد شهادة الجهاز على جهاز إختبار

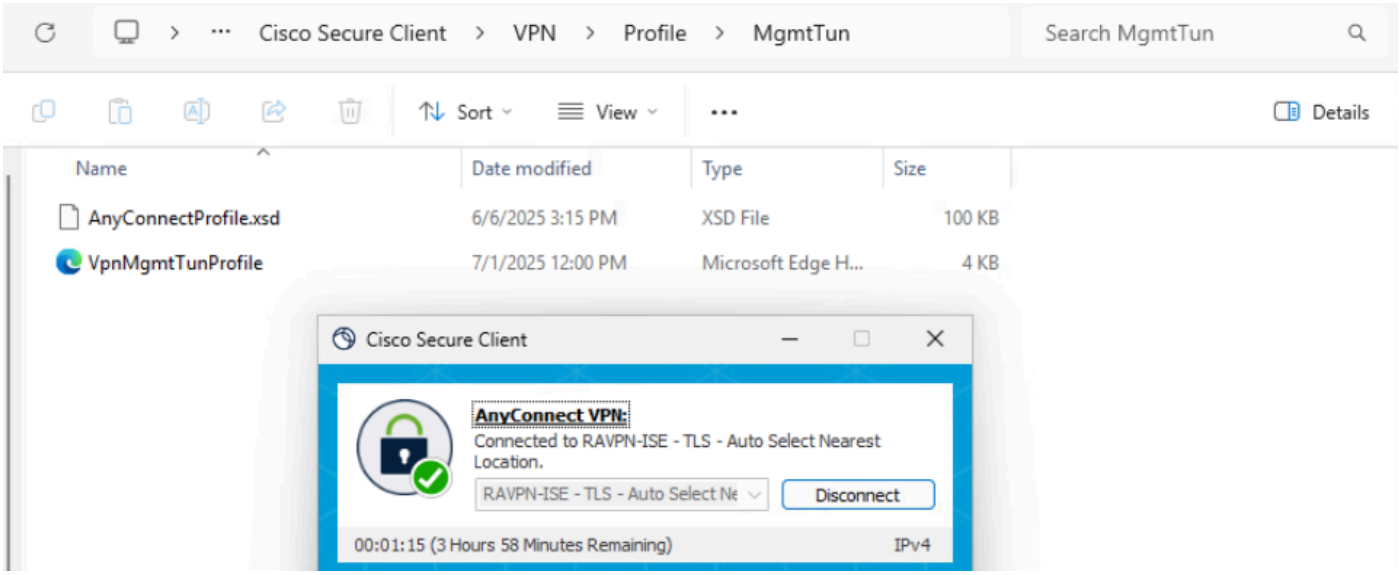
1. إستيراد شهادة جهاز PKCS12 تحت مخزن محلي أو مخزن أجهزة:



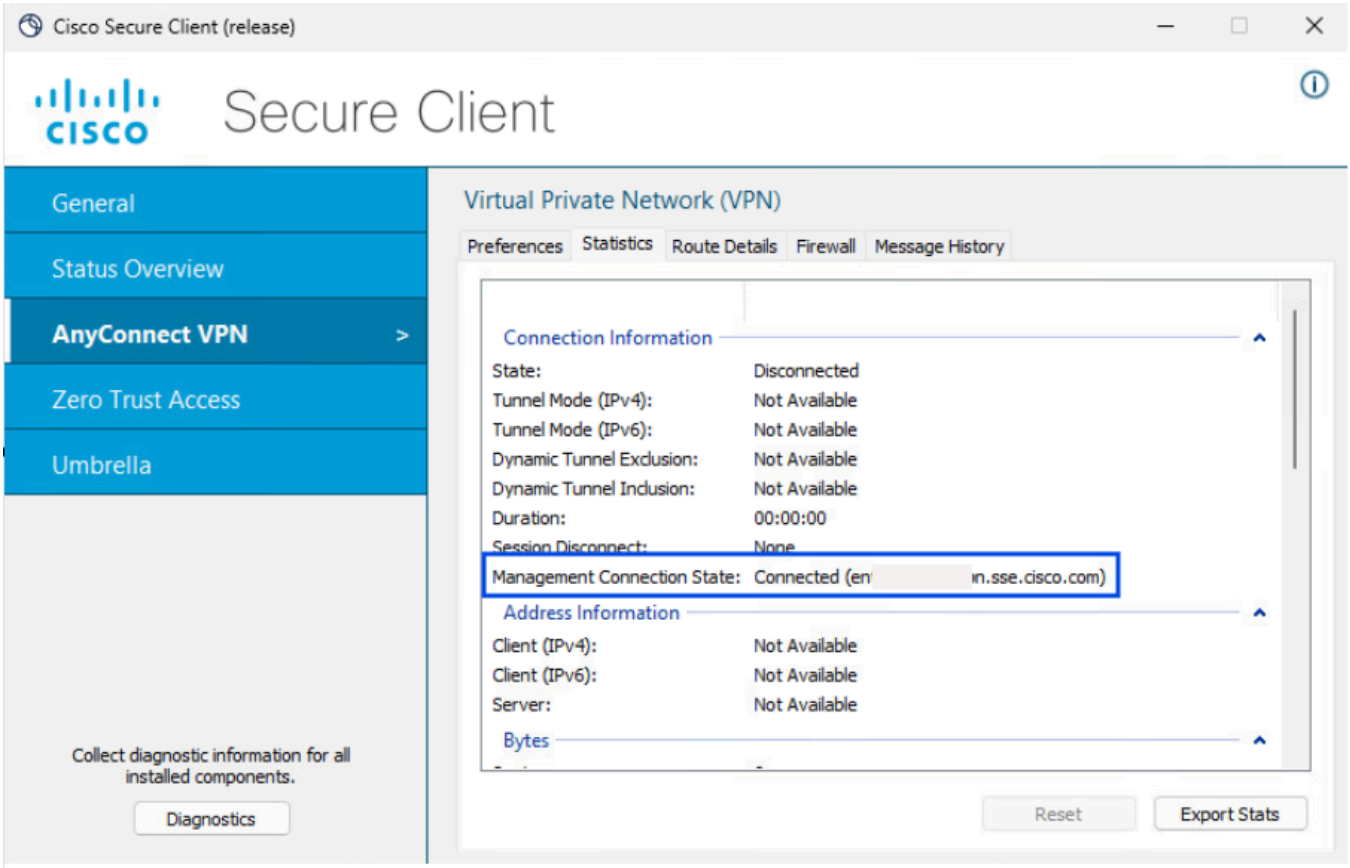
الخطوة 8 - الاتصال بنفق الجهاز

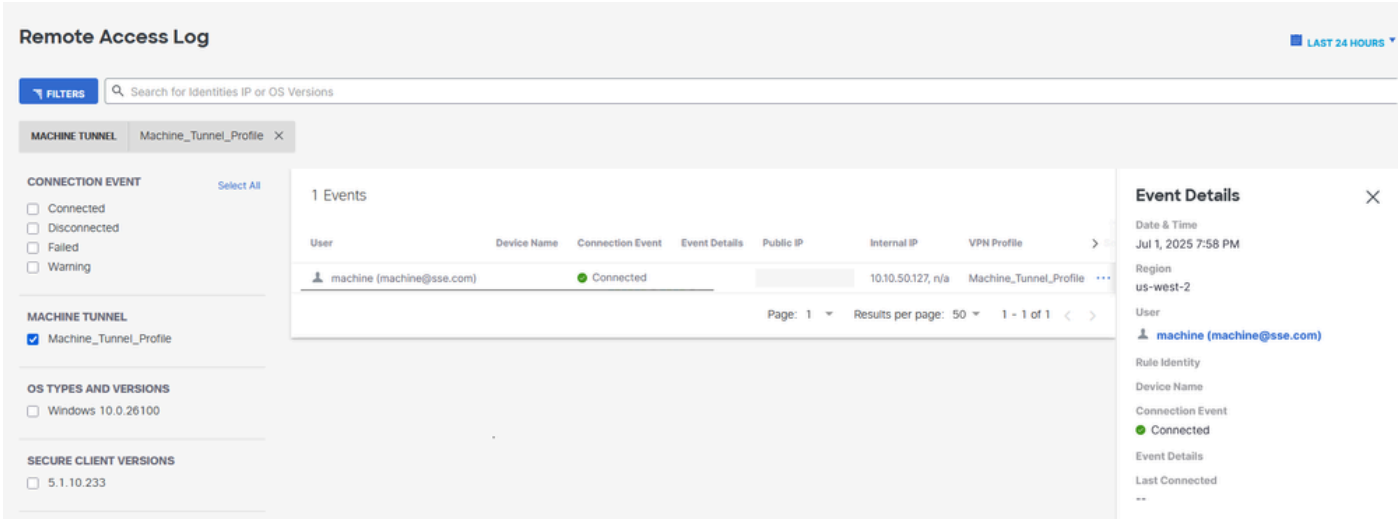
1. اتصل ب "نفق المستخدم"، يؤدي هذا إلى تشغيل ملف تعريف xml للجهاز المراد تنزيله.





2. التحقق من اتصال النفق الآلي:





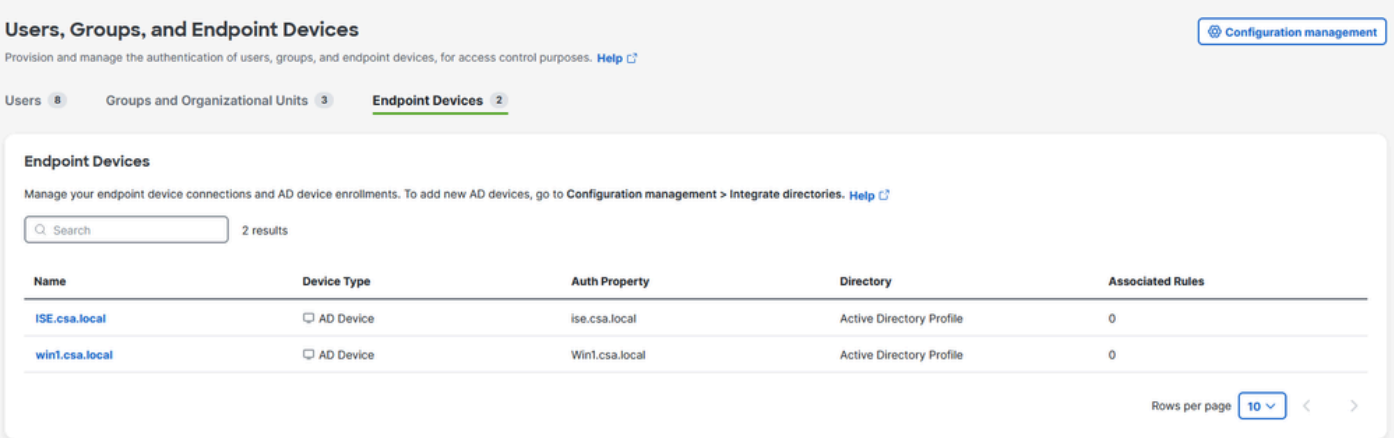
الطريقة 2 - تكوين نفق الجهاز باستخدام شهادة نقطة النهاية

في هذه الحالة لمصادقة الحقل الأساسي، أختر حقل الشهادة الذي يحتوي على اسم الجهاز (اسم الكمبيوتر). يستخدم Secure Access اسم الجهاز كمعرف نفق الجهاز. يجب أن يتطابق تنسيق اسم الكمبيوتر مع تنسيق معرف الجهاز المختار.

انتقل من الخطوة 1 إلى الخطوة 4 لتكوين نفق الجهاز.

الخطوة 5 - تكوين موصل AD لاستيراد نقاط النهاية على Cisco Secure Access

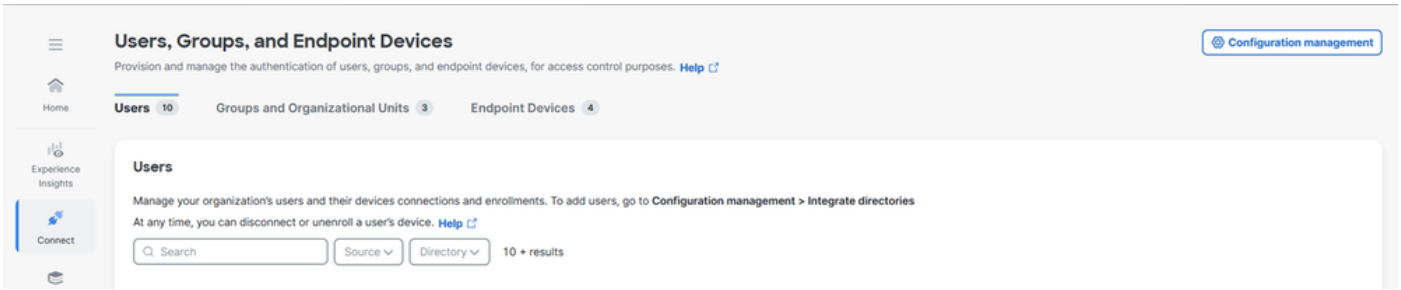
لمزيد من المعلومات، ارجع إلى: تكامل Active Directory على الخادم.



الخطوة 6 - تكوين مصادقة أجهزة نقاط النهاية

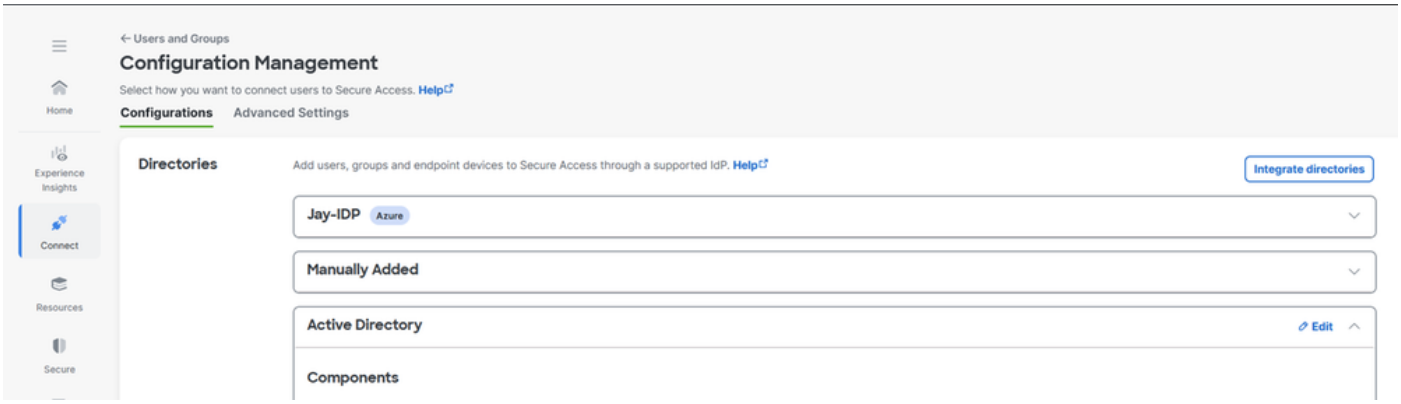
1. انتقل إلى الاتصال > المستخدمون والمجموعات وأجهزة نقاط النهاية.

2. انقر فوق إدارة التكوين.

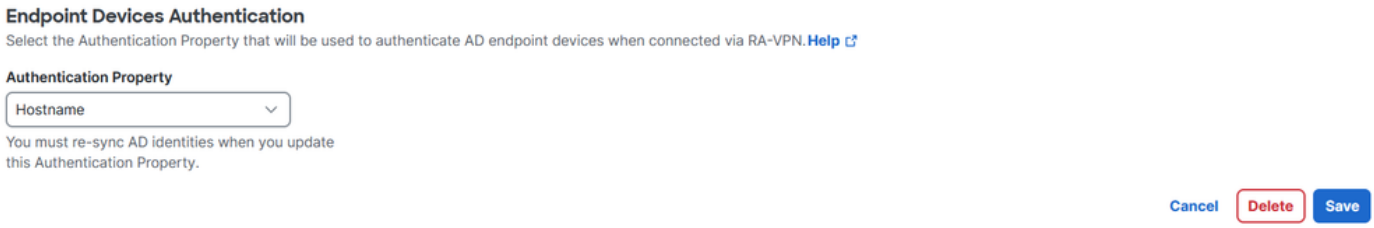


---

3. تحت التكوينات، انقر فوق تحرير Active Directory.



4. تعيين خاصية مصادقة أجهزة نقطة النهاية إلى اسم المضيف.



5. انقر فوق حفظ خدمات موصل AD وإعادة تشغيلها على الخوادم التي تم تثبيتها بها

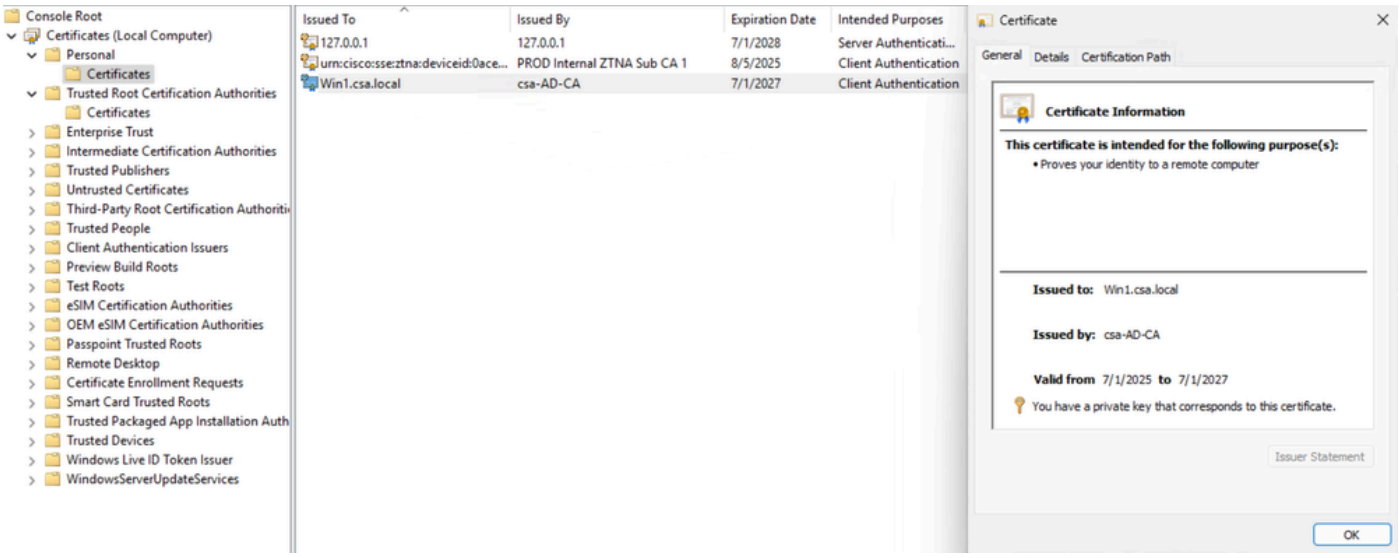
الخطوة 7 - إنشاء واستيراد شهادة نقطة النهاية

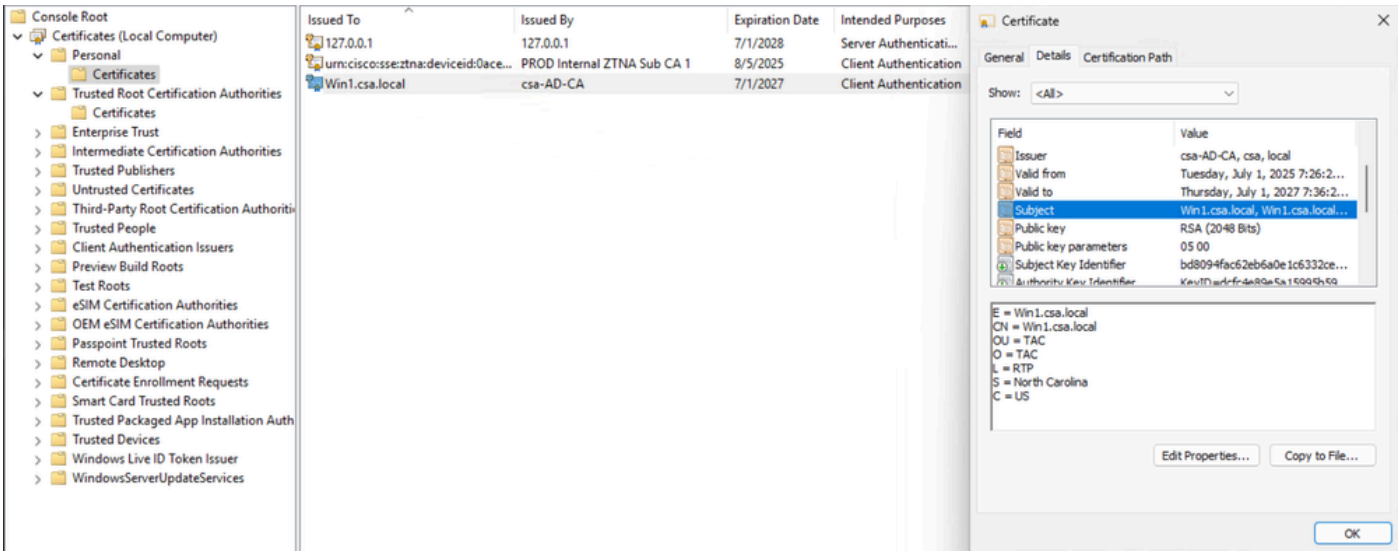
1. إنشاء CSR أو فتح مولد CSR أو أداة OpenSSL.

2. إنشاء شهادة نقطة نهاية من المرجع المصدق.

3. تحويل ملف .cert إلى تنسيق PKCS12.

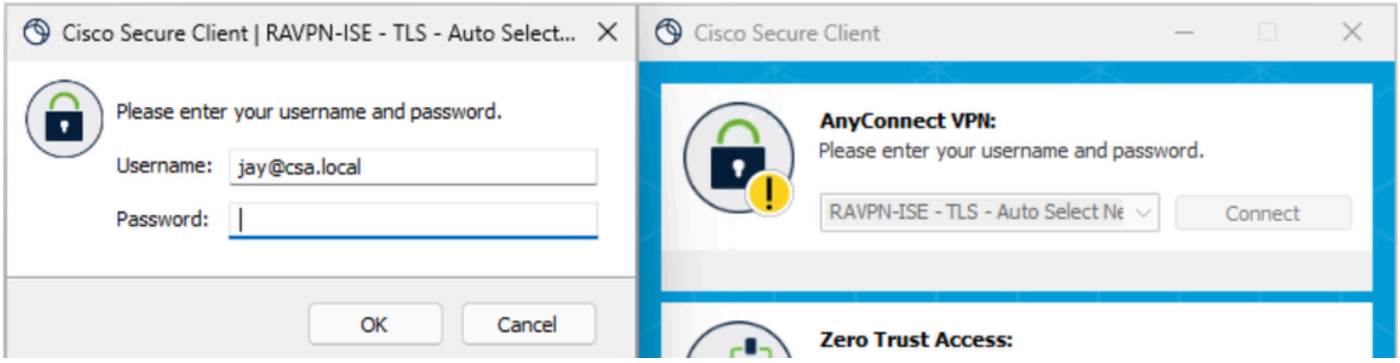
4. إستيراد شهادة PKCS12 في مخزن شهادات نقطة النهاية.

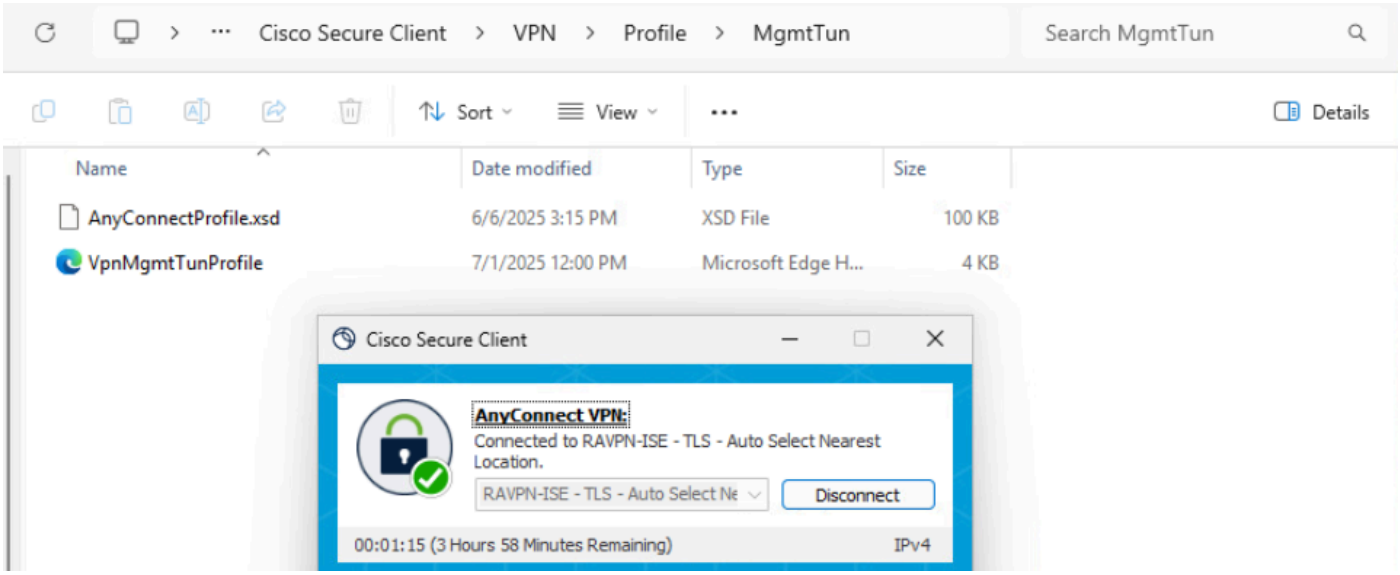




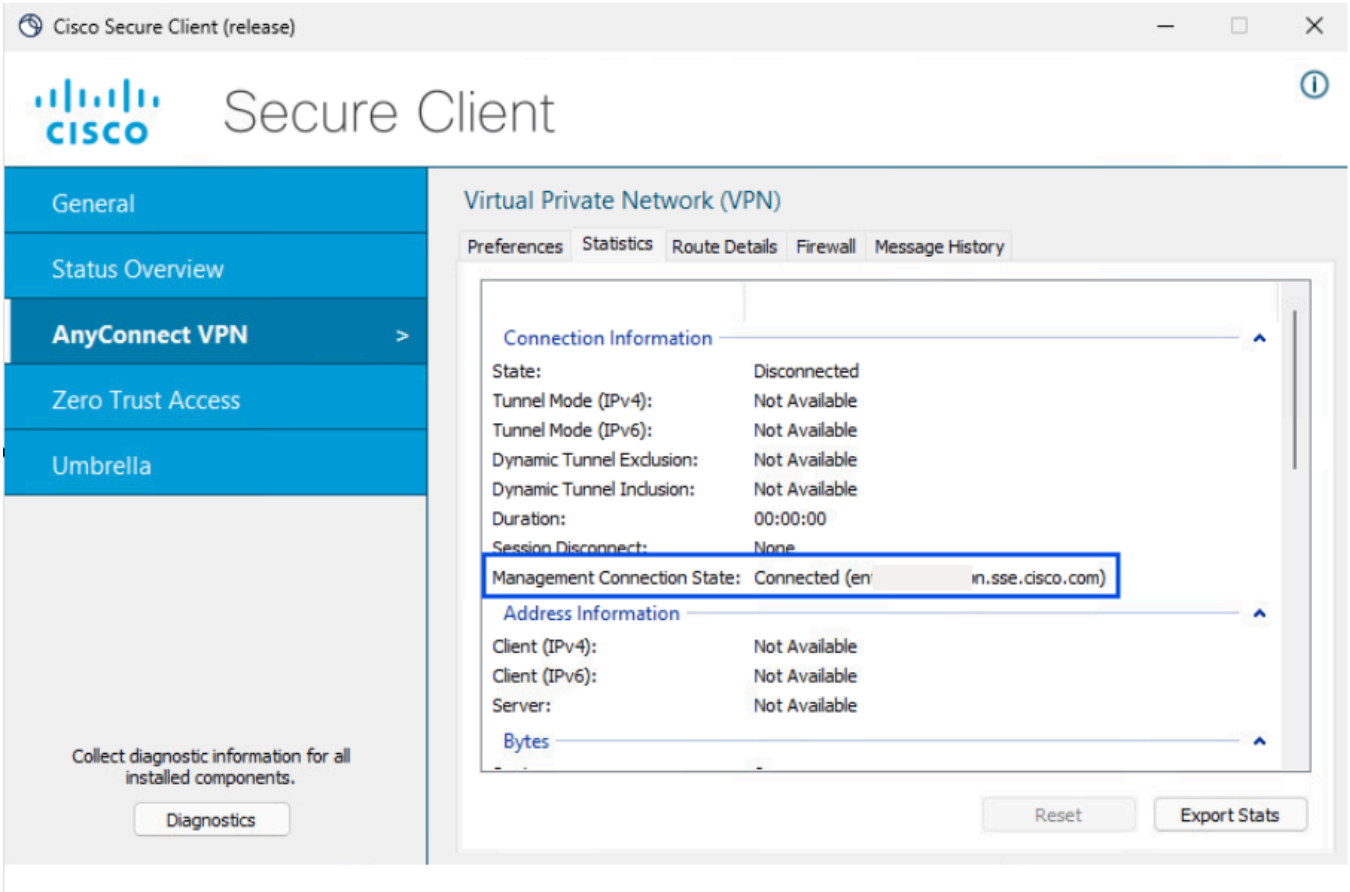
الخطوة 8 - الاتصال بنفق الجهاز

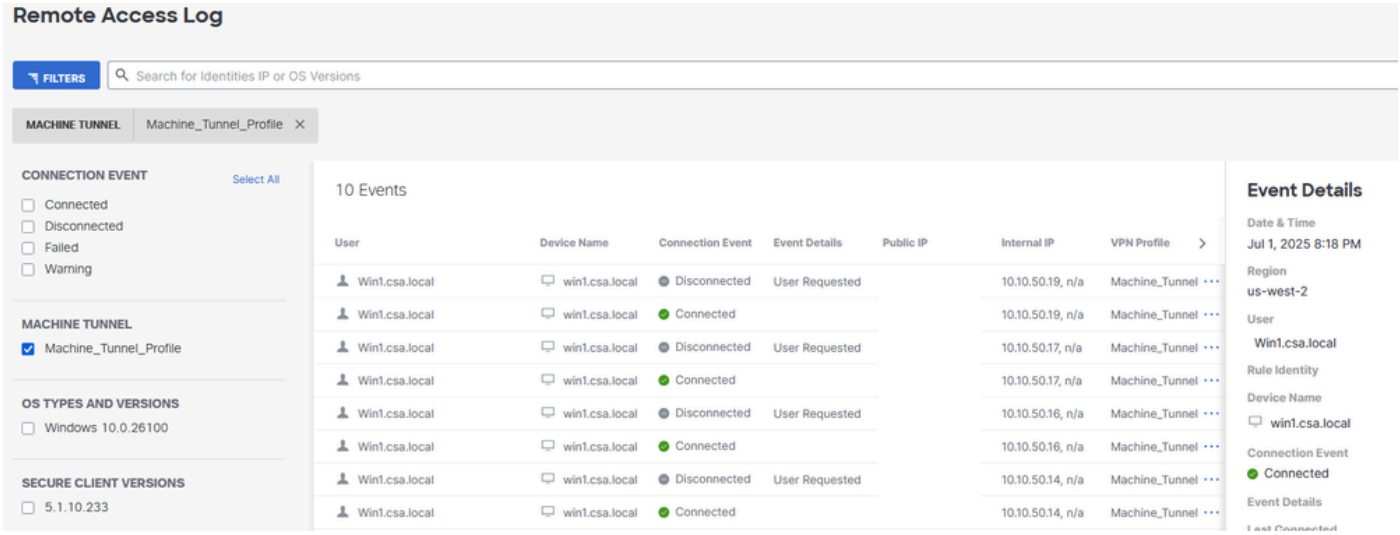
1. اتصل ب User Tunnel، ويقوم بتشغيل تنزيل ملف تعريف xml الخاص بنفق الجهاز.





2. التحقق من اتصال النفق الآلي:





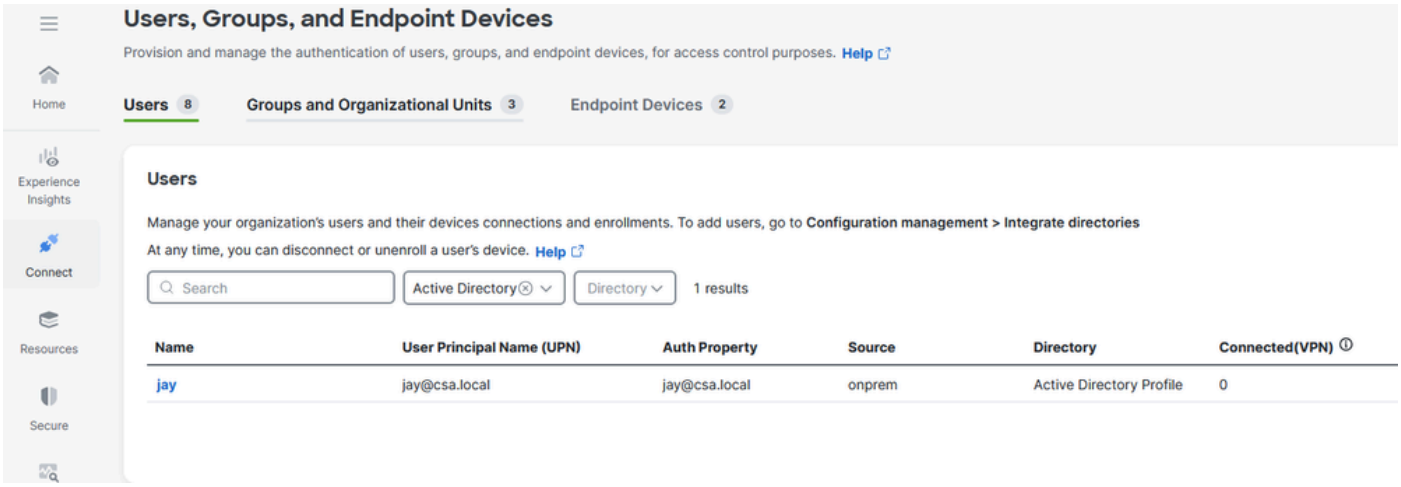
الطريقة 3 - تكوين نفق الجهاز باستخدام شهادة المستخدم

في هذه الحالة لمصادقة الحقل الأساسي، أختر حقل الشهادة الذي يحتوي على بريد المستخدم الإلكتروني أو UPN. يستخدم Secure Access البريد الإلكتروني أو UPN كمعرف نفق الجهاز. يجب أن يتطابق تنسيق البريد الإلكتروني أو UPN مع تنسيق معرف الجهاز المختار

انتقل من خلال الخطوات 1 إلى الخطوة 4 لتكوين نفق الجهاز.

الخطوة 5 - تكوين موصل AD لاستيراد المستخدمين على Cisco Secure Access

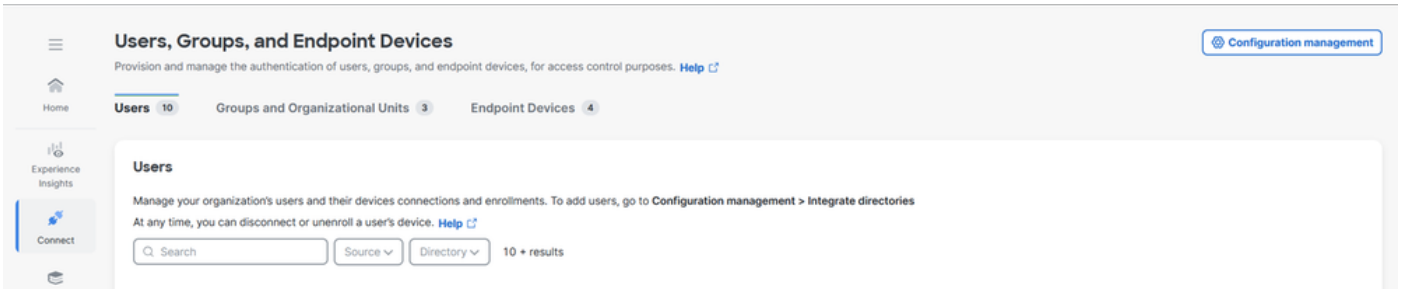
لمزيد من المعلومات، ارجع إلى: تكامل Active Directory على الخادم.



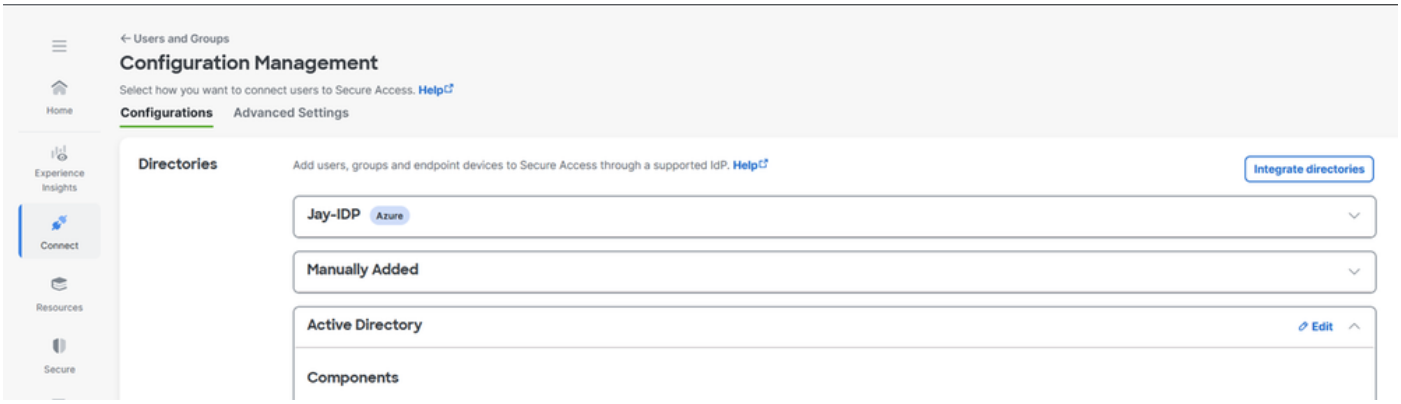
الخطوة 6 - تكوين مصادقة المستخدمين

1. انتقل إلى الاتصال > المستخدمون والمجموعات وأجهزة نقاط النهاية.

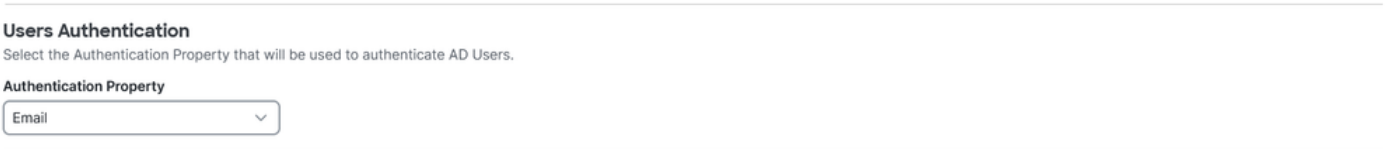
2. انقر فوق إدارة التكوين.



3. تحت التكوينات، انقر فوق تحرير Active Directory.



4. تعيين خاصية مصادقة المستخدمين على البريد الإلكتروني.



5. انقر فوق حفظ وإعادة تشغيل خدمات موصل AD على الخوادم التي تم تثبيتها بها.

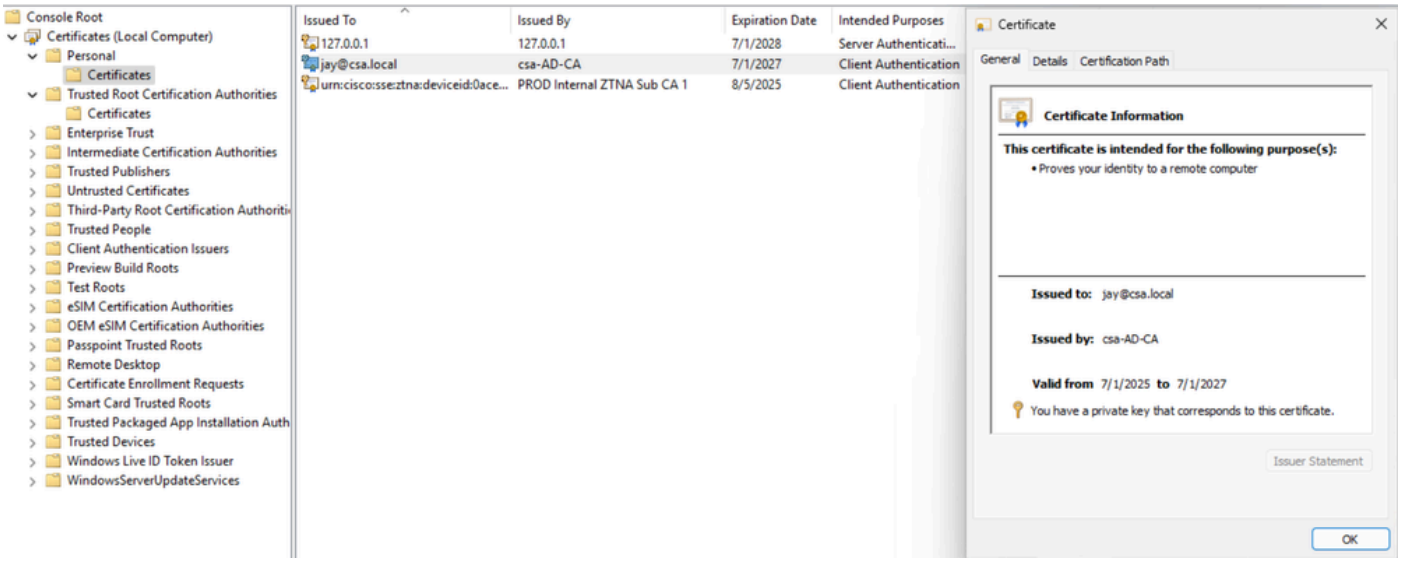
الخطوة 7 - إنشاء واستيراد شهادة نقطة النهاية

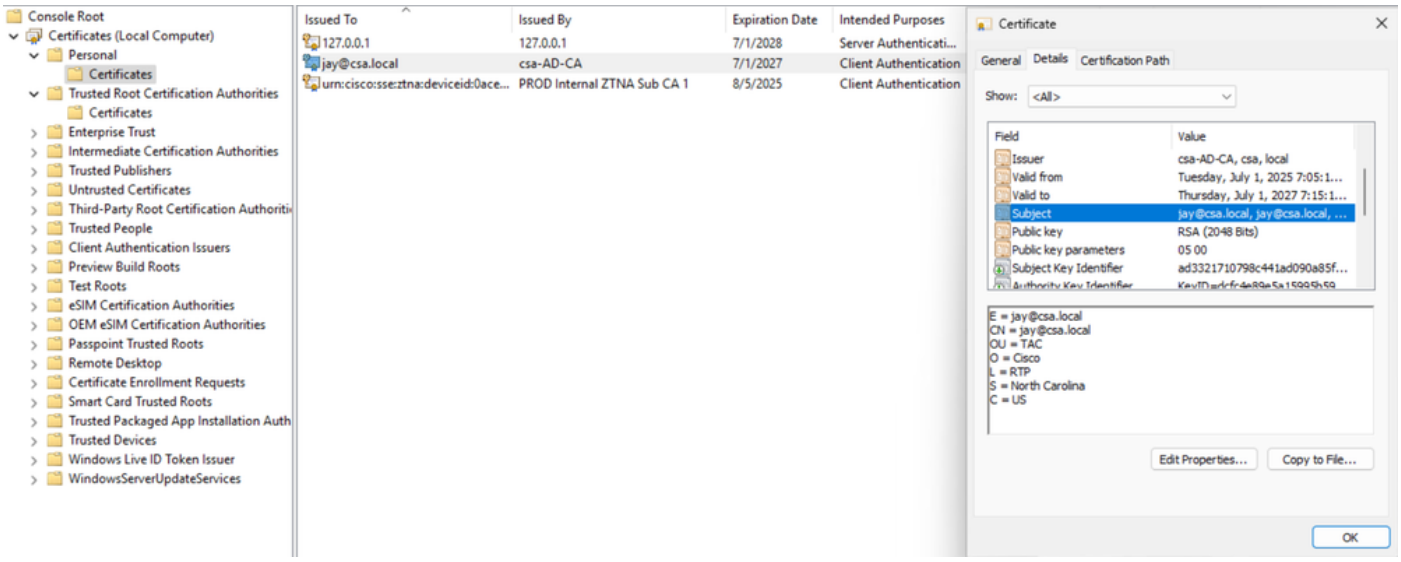
1. قم بإنشاء CSR أو فتح مولد CSR أو أداة OpenSSL.

2. إنشاء شهادة نقطة نهاية من CA.

3. تحويل ملف .cert إلى تنسيق PKCS12.

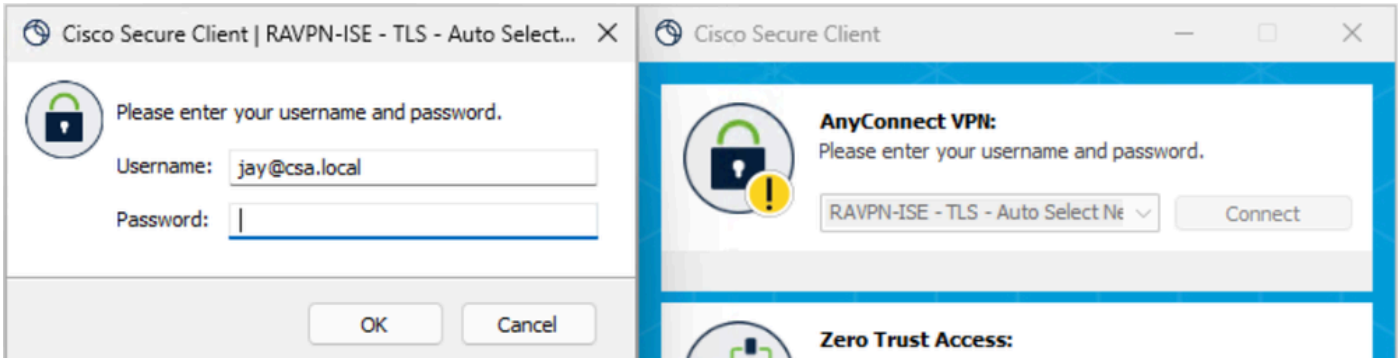
4. إستيراد شهادة PKCS12 في مخزن شهادات نقطة النهاية.

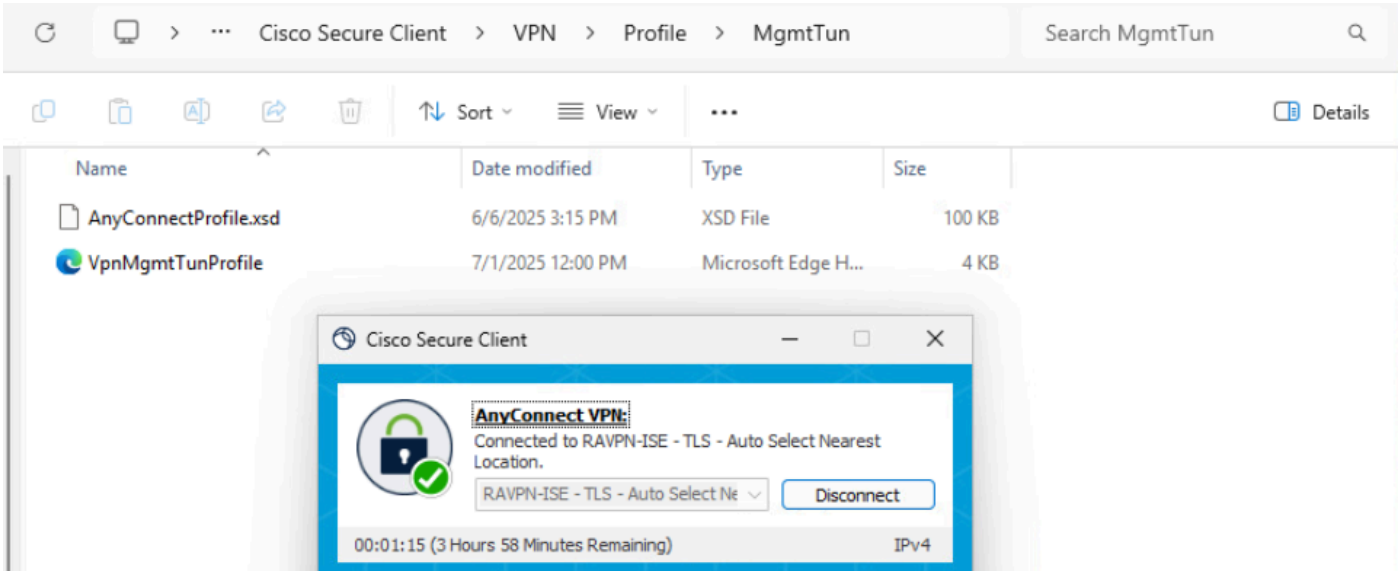




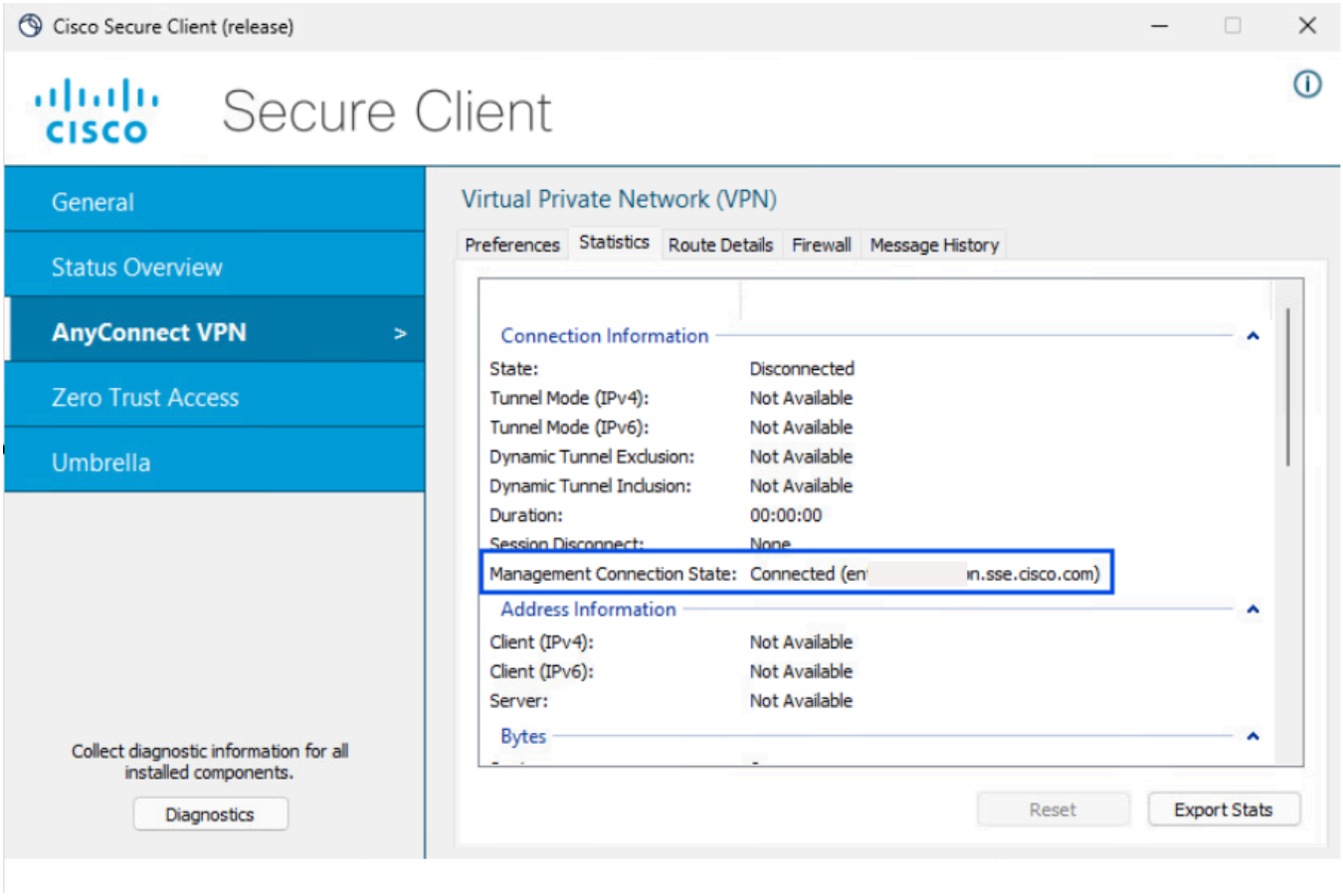
الخطوة 8 - الاتصال بنفق الجهاز

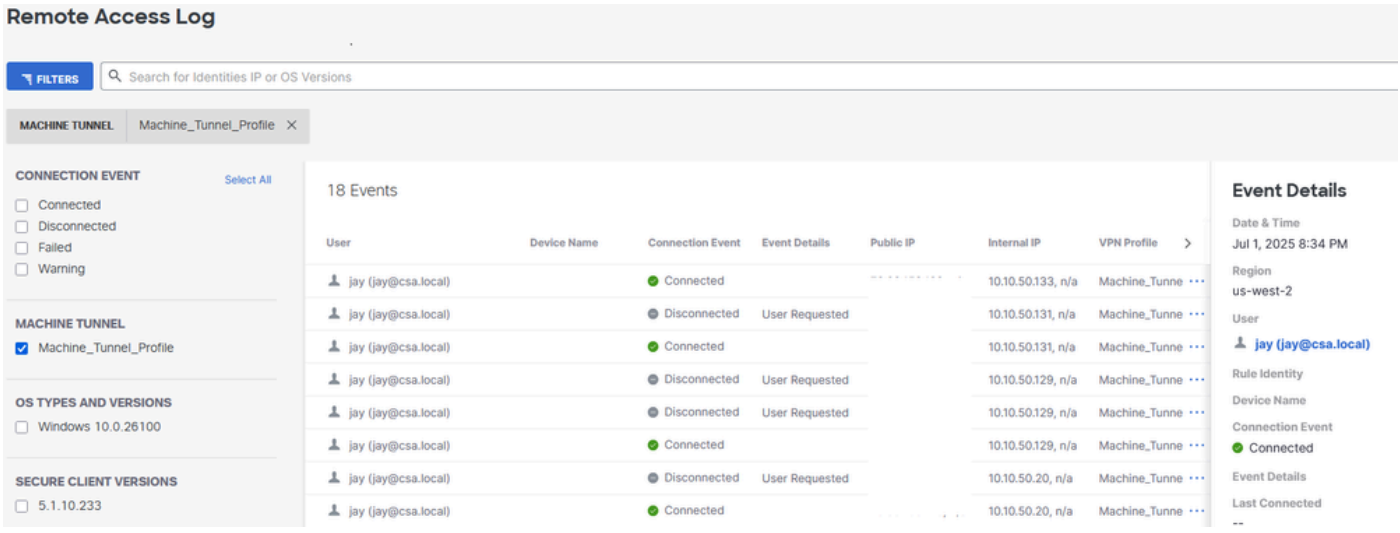
1. اتصل ب User Tunnel، ويقوم بتشغيل تنزيل ملف تعريف xml الخاص بنفق الجهاز.





2. التحقق من اتصال النفق الآلي:





استكشاف الأخطاء وإصلاحها

استخرج حزمة DART وافتح سجلات AnyConnectVPN وحلل رسائل الخطأ:

DARTBundle_0603_1656.zip\Cisco Secure Client\AnyConnect VPN\Log

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).