تكوين NAM العميل الآمن ل Dot1x باستخدام Windows و ISE 3.2

المحتويات

المقدمة

المتطلبات الأساسية

- المتطلبات
- المكونات المستخدمة

معلومات أساسية

التكوين

- الرسم التخطيطي للشبكة
- التكوينات
  - 1. تنزيل Secure Client NAM (مدير الوصول إلى الشبكة) وتثبيته
  - 2. تنزيل محرر ملف تعريف NAM الآمن وتثبيته.
  - 3. تكوينات افتراضية عامة
  - 4. السيناريو 1: تكوين عميل NAM الآمن لمصادقة مستخدم PEAP (MS-CHAPv2)
  - 5. السيناريو 2: تكوين عميل NAM الآمن لمصادقة EAP-FAST SimultaneousUser والجهاز
  - 6. السيناريو 3: تكوين طلب NAM الآمن لمصادقة شهادة مستخدم EAP TLS
  - 7. قم بتكوين ISR 1100 و ISE للسماح بالمصادقة استنادا إلى السيناريو 1 PEAP MSCHAPv2

التحقق من الصحة

استكشاف الأخطاء وإصلاحها

- المشكلة: لا يستخدم العميل الآمن ملف تعريف NAM.
- المشكلة 2: يجب تجميع السجلات لمزيد من التحليل.
  - 1. تمكين تسجيل NAM الموسع
  - 2 - إعادة طرح المسألة.
  - 3. تجميع حزمة DART الخاصة بالعميل الآمن.

معلومات ذات صلة

المقدمة

يوضح هذا المستند كيفية تكوين وحدة تحليل شبكة العميل الآمنة (NAM) على Windows.

المتطلبات الأساسية

المتطلبات

توصي Cisco بأن تكون لديك معرفة بالمواضيع التالية:

- الفهم الأساسي لما هو متطلب RADIUS
- Dot1x
- خوخ

- PKI

المكونات المستخدمة

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

- تم إنشاء Windows 10 Pro الإصدار 22H2 19045.3930
- ISE 3.2
- برنامج Cisco C1117 Cisco IOS® XE، الإصدار 17.12.02
- Active Directory 2016

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

يوضح هذا المستند كيفية تكوين NAM الخاصة بالعميل الآمن على Windows. يتم إستخدام خيار النشر المسبق و مررت التوصية إلجراء مصادقة dot1x. وتقدم أيضا بعض الأمثلة على كيفية تحقيق ذلك.

في الاتصال الشبكي، يكون الطالب عبارة عن كيان يقع في أحد طرفي مقطع الشبكة المحلية من نقطة إلى نقطة ويسعى إلى التصديق عليه بواسطة مصدق مرتبط بالطرف الآخر من ذلك الرابط.

يستخدم مقياس IEEE 802.1X مصطلح متلقي للإشارة إلى الأجهزة أو البرامج. في التطبيق العملي، الملخص هو تطبيق برمجي مثبت على كمبيوتر المستخدم النهائي.

يقوم المستخدم باستدعاء الطالب وتسليم بيانات الاعتماد لتوصيل الكمبيوتر بالاتصال بشبكة آمنة. في حالة نجاح المصادقة، يسمح المصدق عادة للكمبيوتر بالاتصال بالشبكة.

حول مدير الوصول إلى الشبكة

Network Access Manager (مدير الوصول إلى الشبكة) هو برنامج عميل ويفر شبكة آمنة من الطبقة 2 وفقا لسياساتها.

وتقوم باكتشاف شبكة الوصول المثالية من الطبقة 2 وتحديد هذه الشبكة، كما تقوم بإجراء مصادقة الجهاز للوصول إلى كل من الشبكات السلكية واللاسلكية.

يدير Network Access Manager هوية المستخدم والجهاز وبروتوكولات الوصول إلى الشبكة المطلوبة للوصول الآمن.

ويعمل هذا النظام بذكاء لمنع المستخدمين النهائيين من إجراء إتصالات تخالف السياسات التي يحددها المسؤول.

تم تصميم "مدير الوصول إلى الشبكة" ليكون أحادي المركز، مما يسمح باتصال شبكة واحد فقط في كل مرة.

كما أن التوصيلات السلكية لها أولوية أعلى من التوصيلات اللاسلكية، لذلك إذا كنت موصلا بالشبكة بتوصيل سلكي، يعطل الموجه اللاسلكي بدون عنوان IP.

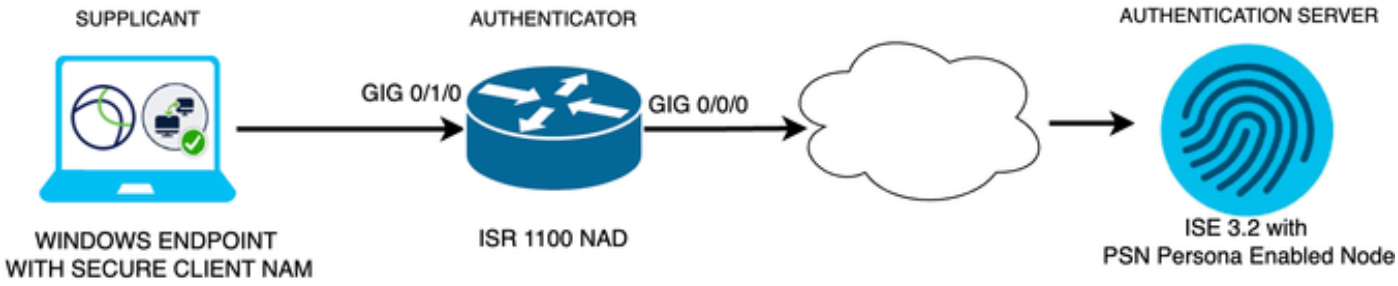
التكوين

الرسم التخطيطي للشبكة

من المهم فهم أنه بالنسبة للمصادقة dot1x، هناك حاجة إلى 3 أجزاء:

1. المطلوب الذي يمكنه القيام dot1x،
2. المصدق المعروف أيضا NAS/NAD الذي يعمل وكيل يغلف حركة مرور dot1x داخل RADIUS،
3. وخادم المصادقة.

في هذا المثال، يتم تثبيت المطالب وتكوينه بطرق مختلفة. وفيما بعد، يظهر سيناريو مع تكوين جهاز الشبكة وخادم المصادقة.



الرسم التخطيطي للشبكة

التكوينات

1. تنزيل Secure Client NAM (مدير الوصول إلى الشبكة) وتثبيته.

2. تنزيل محرر ملف تعريف NAM الآمن وتثبيته.
3. التكوينات الافتراضية العامة
4. السيناريو 1: قم بتكوين طالب NAM الآمن لمصادقة مستخدم PEAP (MS-CHAPv2).
5. السيناريو الثاني: قم بتكوين ملتمس NAM الآمن ل EAP-FAST في نفس الوقت عند تكوين مصادقة المستخدم والجهاز.
6. السيناريو 3 الجزء 1: قم بتكوين طالب NAM الآمن ل EAP-TLS.
7. السيناريو 3 الجزء 2: قم بتكوين العرض التوضيحي NAD و ISE.

1. تنزيل Secure Client NAM (مدير الوصول إلى الشبكة) وتثبيته

تنزيل برامج Cisco

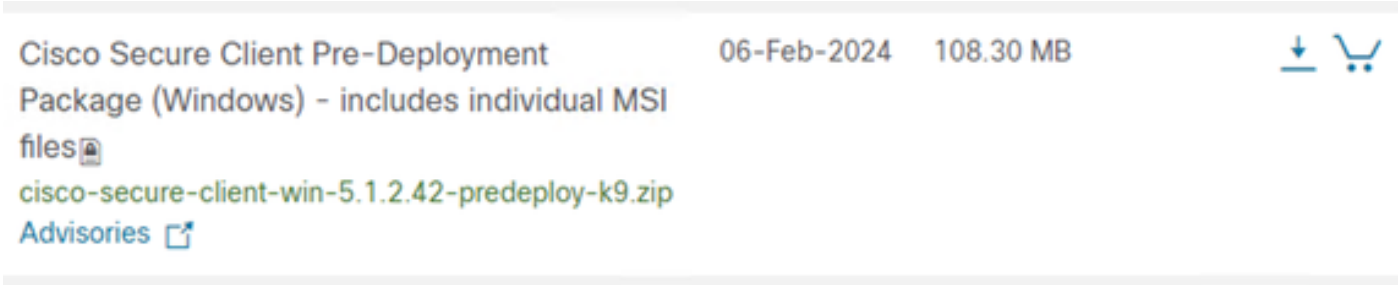
في نوع شريط البحث عن اسم المنتج العميل الآمن 5.

منزل التنزيلات > الأمان > عملاء أمان النقطة الطرفية والشبكة الخاصة الظاهرية (VPN) > عميل آمن (بما في ذلك AnyConnect) > عميل آمن 5 > برنامج عميل AnyConnect VPN.

في مثال التكوين هذا، الإصدار 5.1.2.42 وه المستخدم.

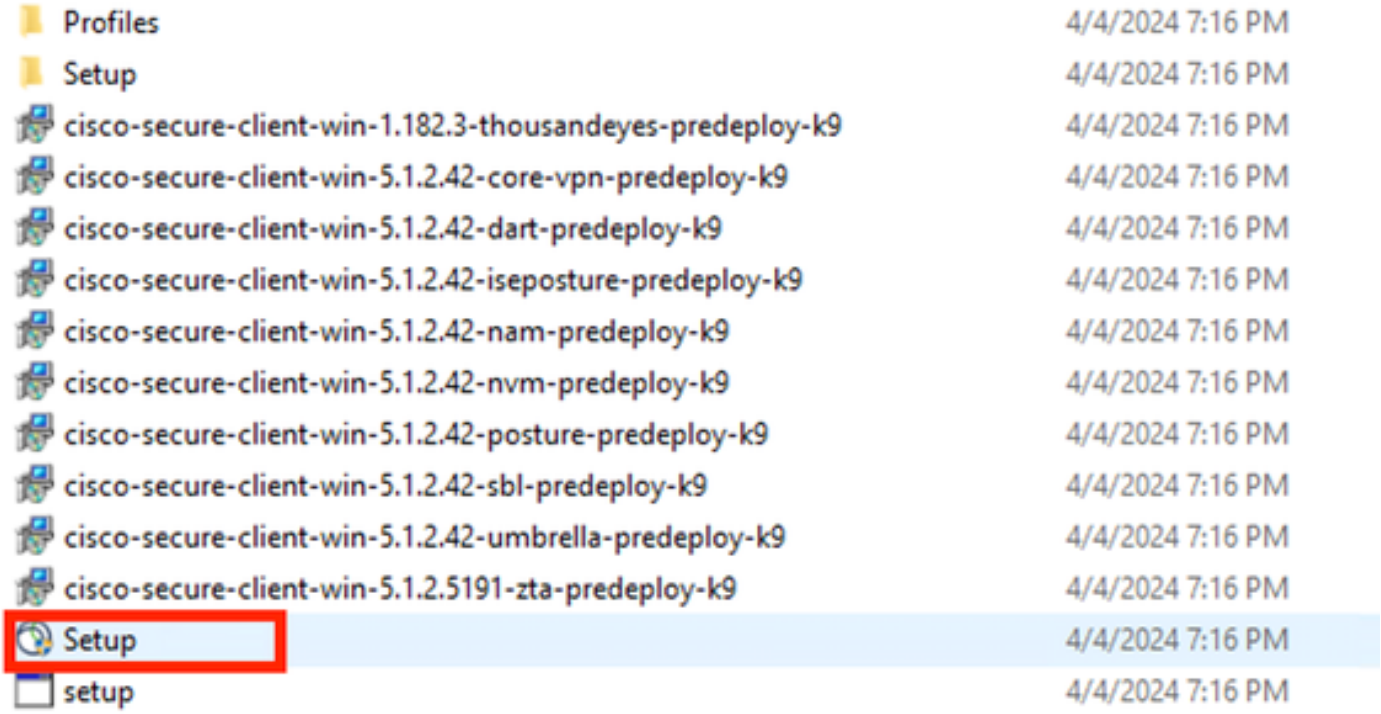
هناك طرق متعددة لنشر "العميل الآمن" على أجهزة Windows؛ من SCCM ومن محرك خدمة الهوية ومن وحدة الاستقبال والبث الخاصة بالشبكة الخاصة الظاهرية (VPN). ومع ذلك، في هذه المقالة، فإن طريقة التثبيت المستخدمة هي طريقة النشر المسبق.

على الصفحة، ابحث عن الملف Cisco Secure Client Headend Deployment Package (في Windows).



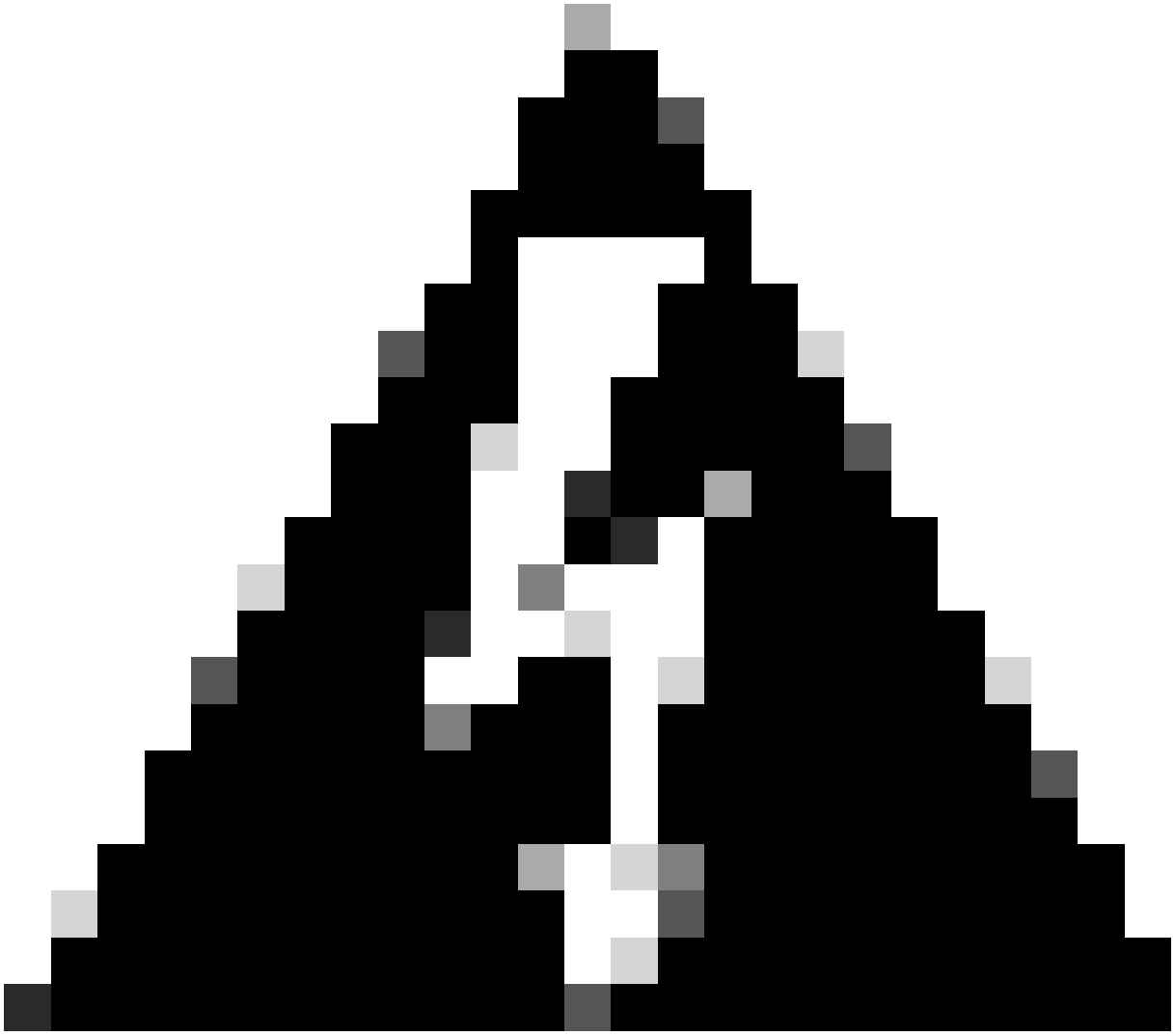
ملف *MSI zip*

بمجرد تنزيلها واستخراجها، انقر فوق الإعداد.

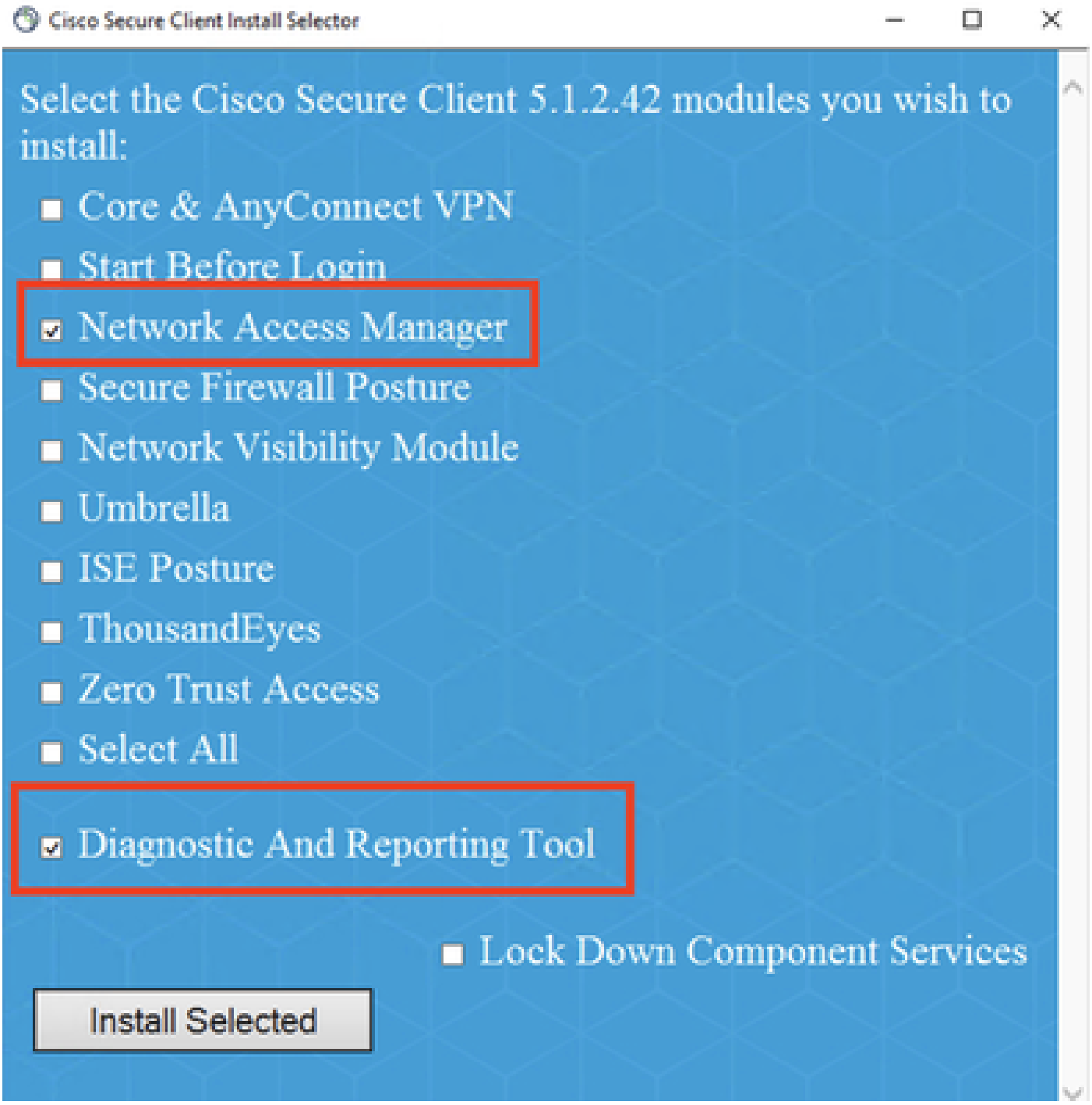


تأمين ملفات العميل

قم بتثبيت مدير الوصول إلى الشبكة والوحدات النمطية لأداة التشخيص وإعداد التقارير.



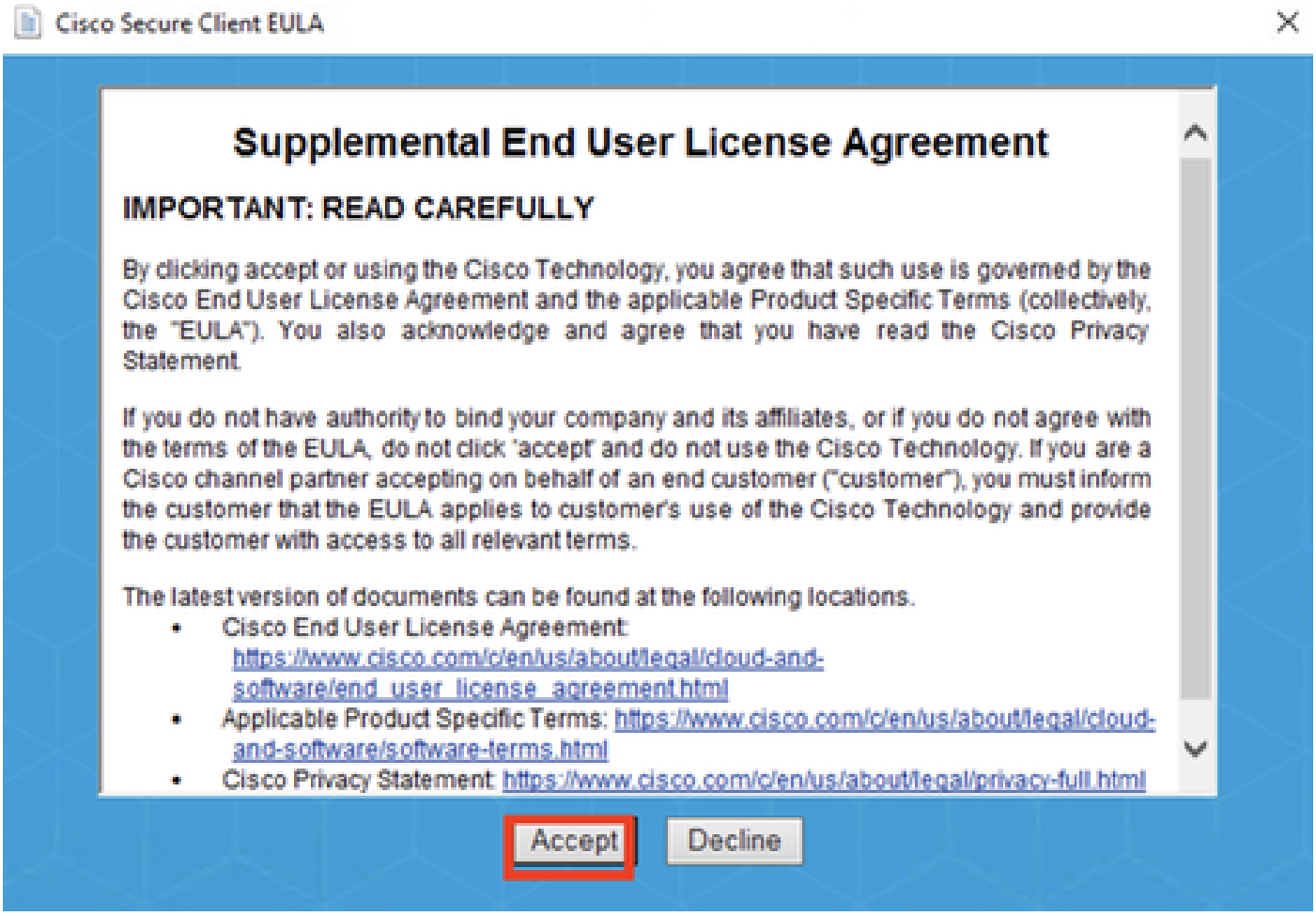
تحذير: إذا كنت تستخدم معالج "العميل الآمن من Cisco"، فسيتم تثبيت وحدة VPN النمطية تلقائيا، وإخفاءها في واجهة المستخدم الرسومية. لا تعمل NAM إذا لم يتم تثبيت وحدة VPN النمطية. إذا كنت تستخدم ملفات MSI الفردية أو طريقة تثبيت مختلفة، فتأكد من تثبيت وحدة VPN النمطية.



أداة تحديد التثبيت

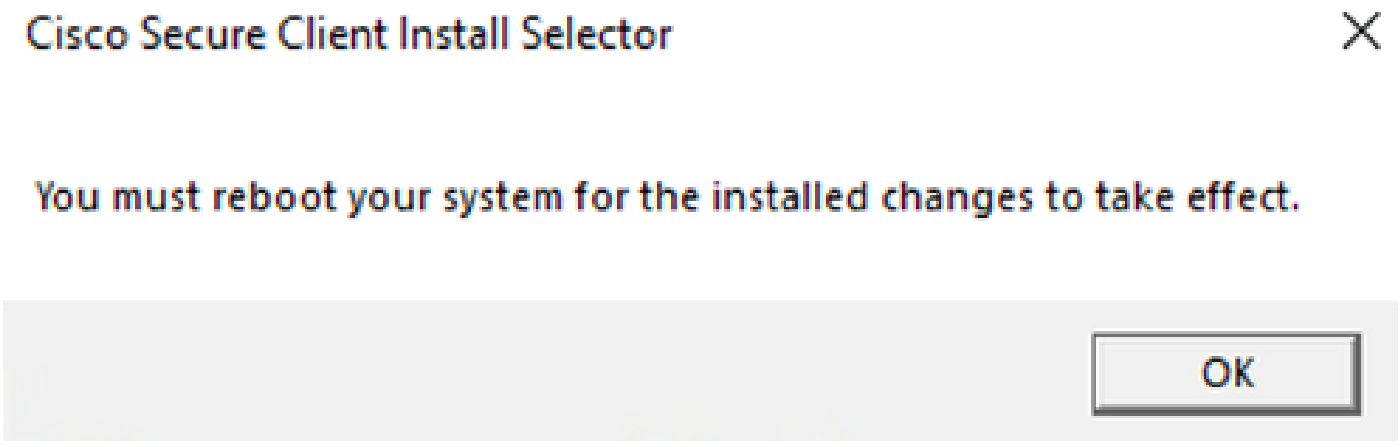
انقر على تثبيت العناصر المحددة.

القبل الإول.



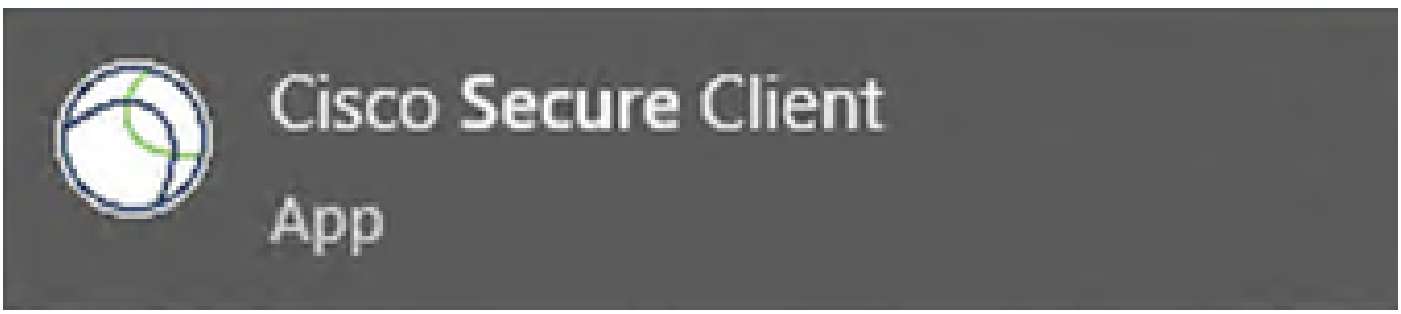
اويال باوندن

يجب إعادة التشغيل بعد تثبيت NAM.



نافذة متطلبات إعادة التشغيل

وبمجرد تثبيته، يمكن العثور عليه وفتحه من شريط Windows Search.

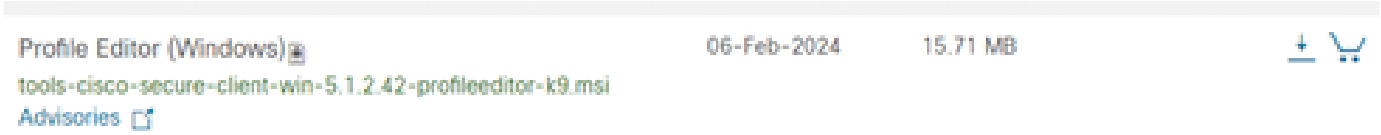


2. تنزيل محرر ملف تعريف NAM الآمن وتثبيته.

مطلوب محرر ملف تعريف مدير الوصول إلى الشبكة من Cisco لتكوين تفضيلات Dot1x.

من نفس الصفحة التي يتم فيها تنزيل Secure Client، يتم العثور على خيار محرر ملف التعريف.

يستخدم هذا المثال الخيار مع الإصدار 5.1.2.42.



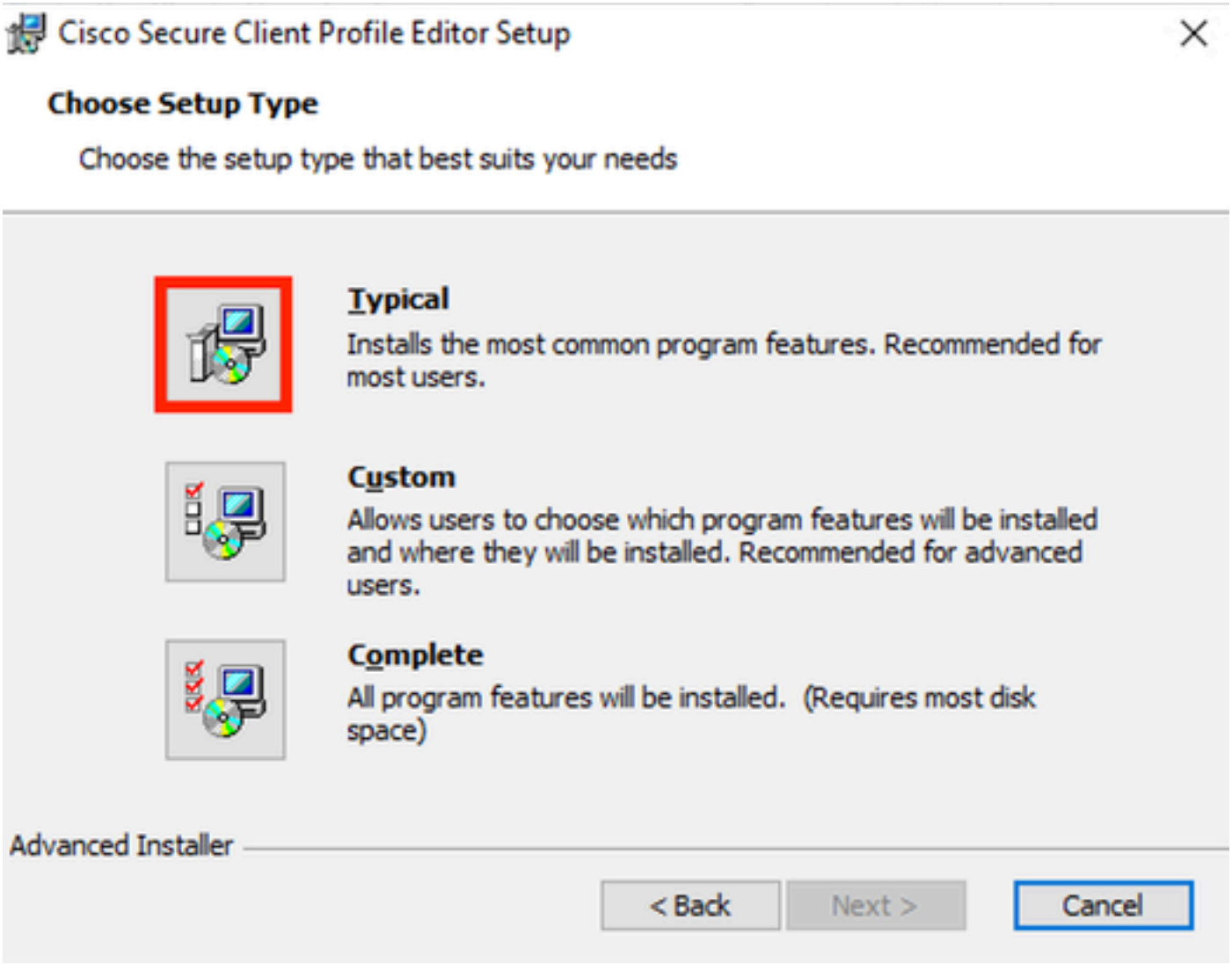
محرر ملف التعريف

بمجرد تنزيله، استمر في التثبيت.

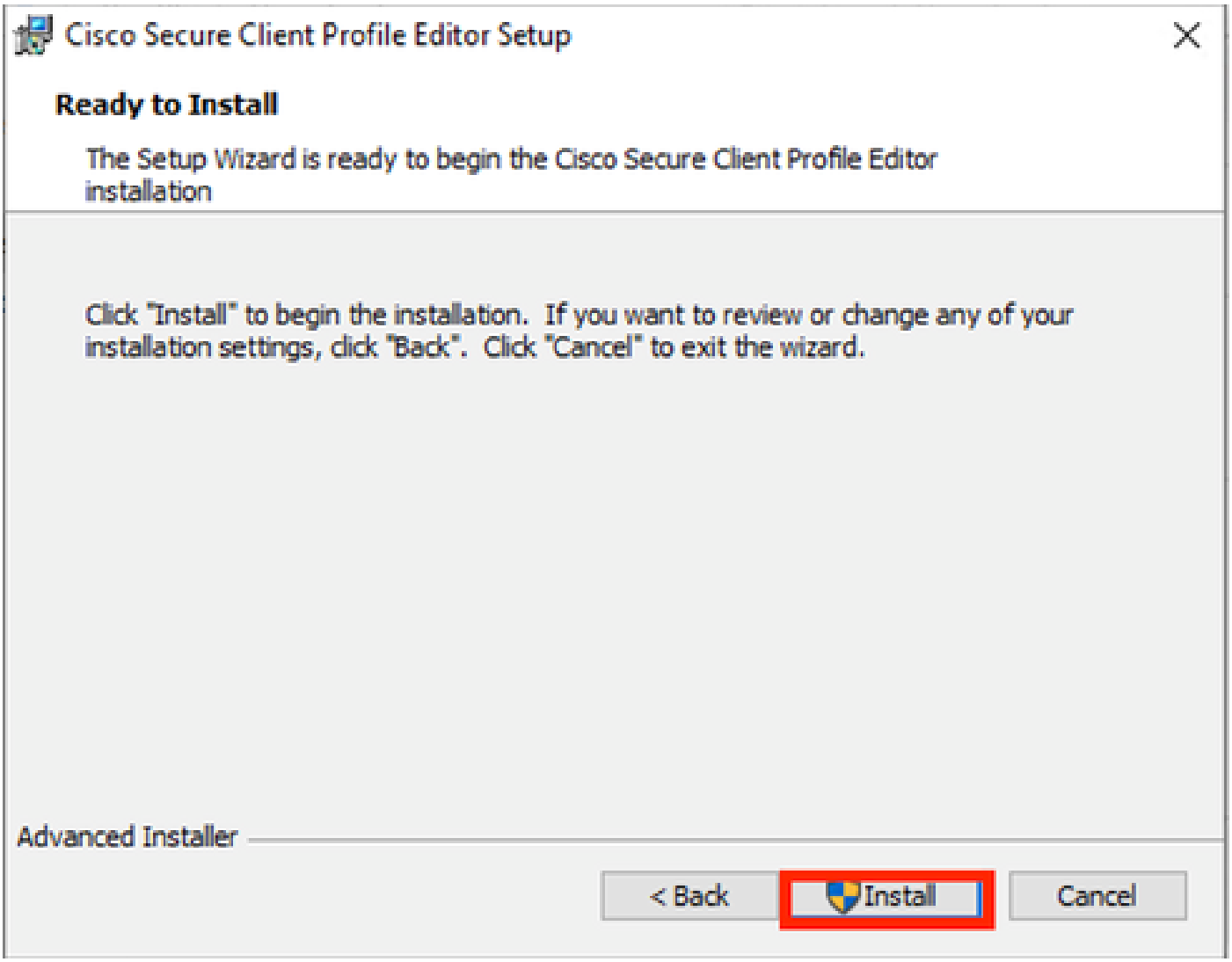
قم بتشغيل ملف msi.

نافذة إعداد محرر ملف التعريف

أستخدم خيار الإعداد النموذجي.

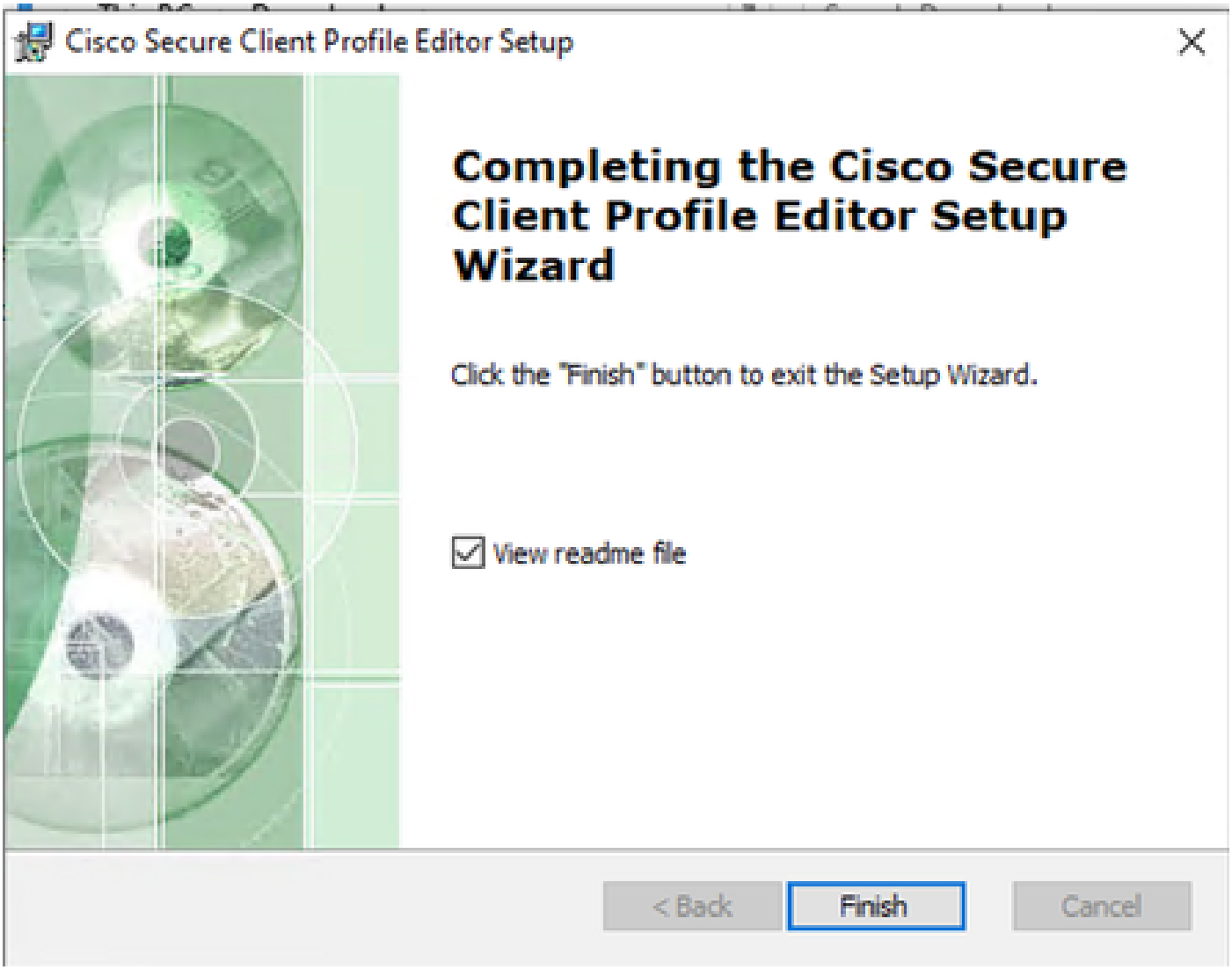


إعداد محرر ملف التعريف



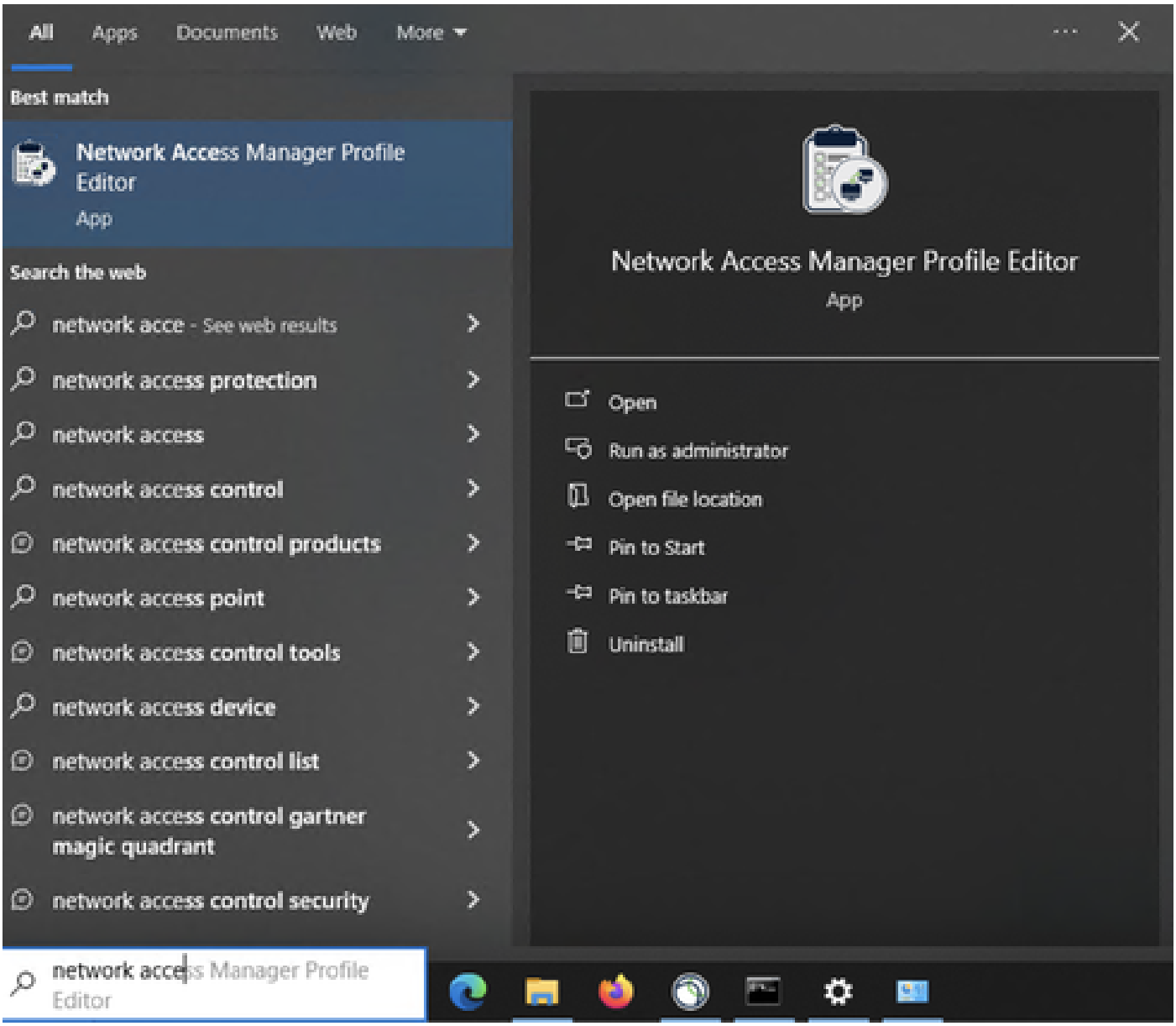
إطار التثبيت

انقر فوق إنهاء.



نهاية إعداد محرر ملف التعريف

افتح محرر ملف تعريف مدير الوصول إلى الشبكة من شريط البحث بمجرد تثبيته.



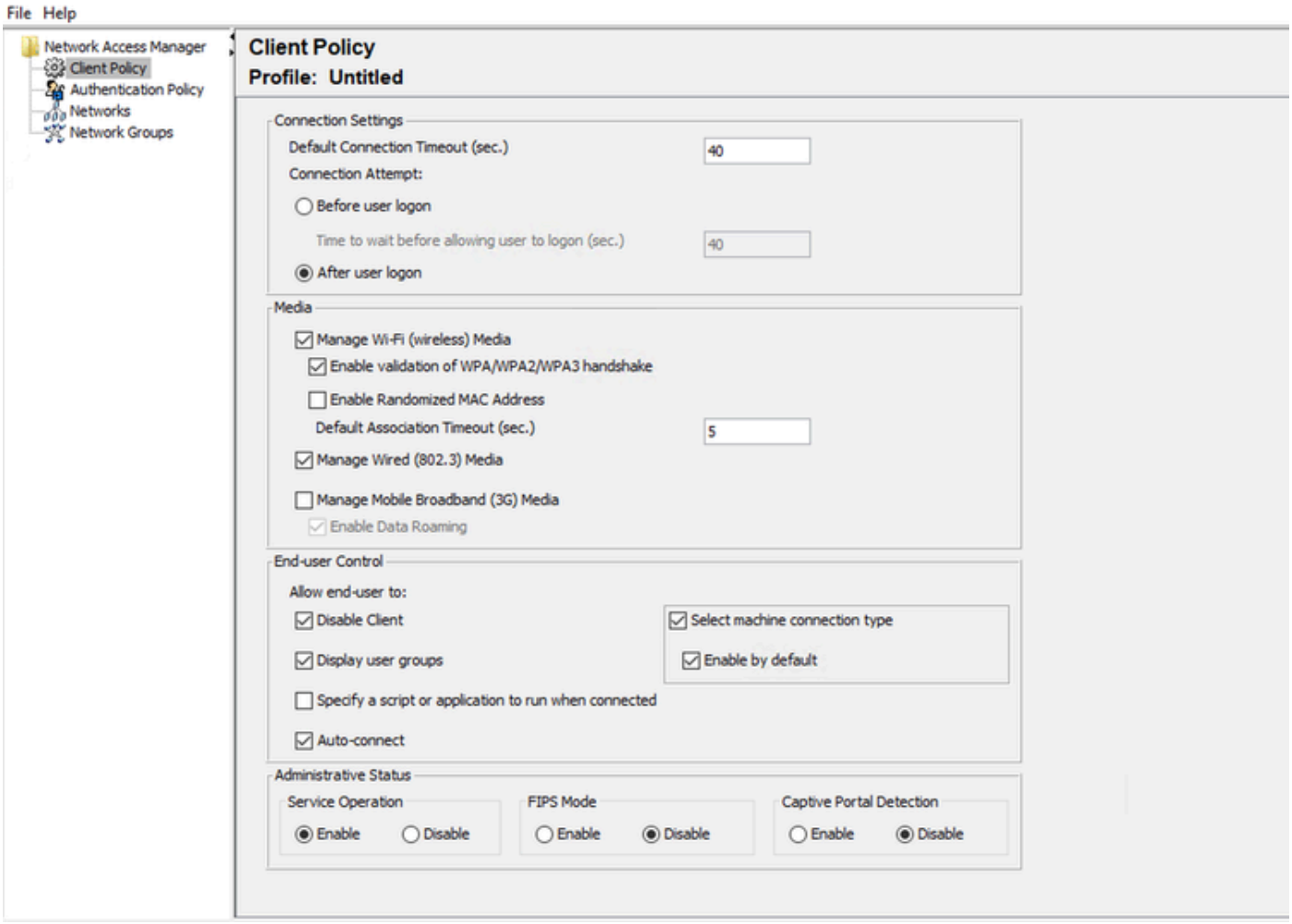
محرر ملف التعريف ل NAM على شريط البحث

اكتمل تثبيت مدير الوصول إلى الشبكة ومحرر ملف التعريف.

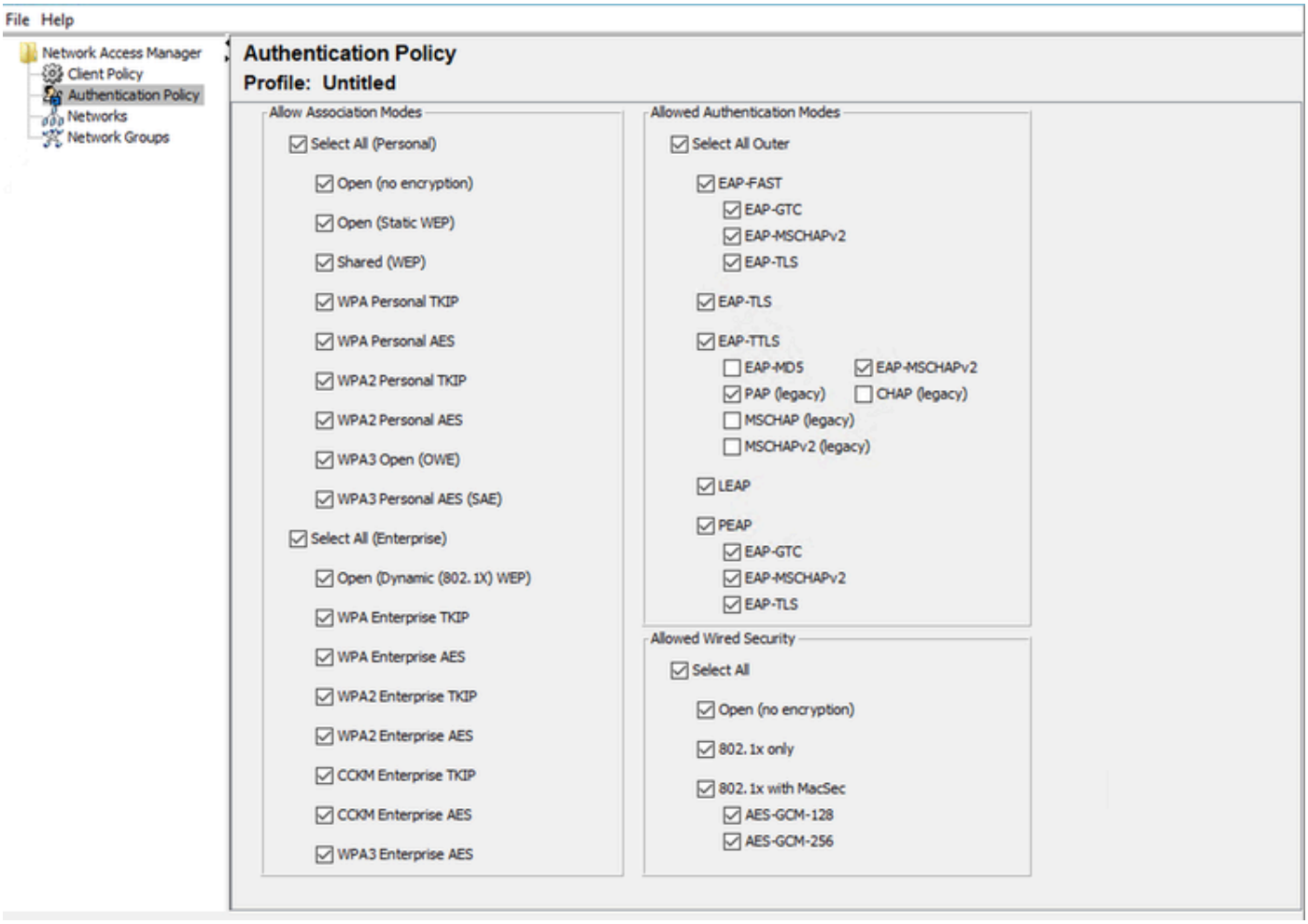
3. تكوينات افتراضية عامة

تحتوي كافة السيناريوهات المقدمة في هذه المقالة على تكوينات ل:

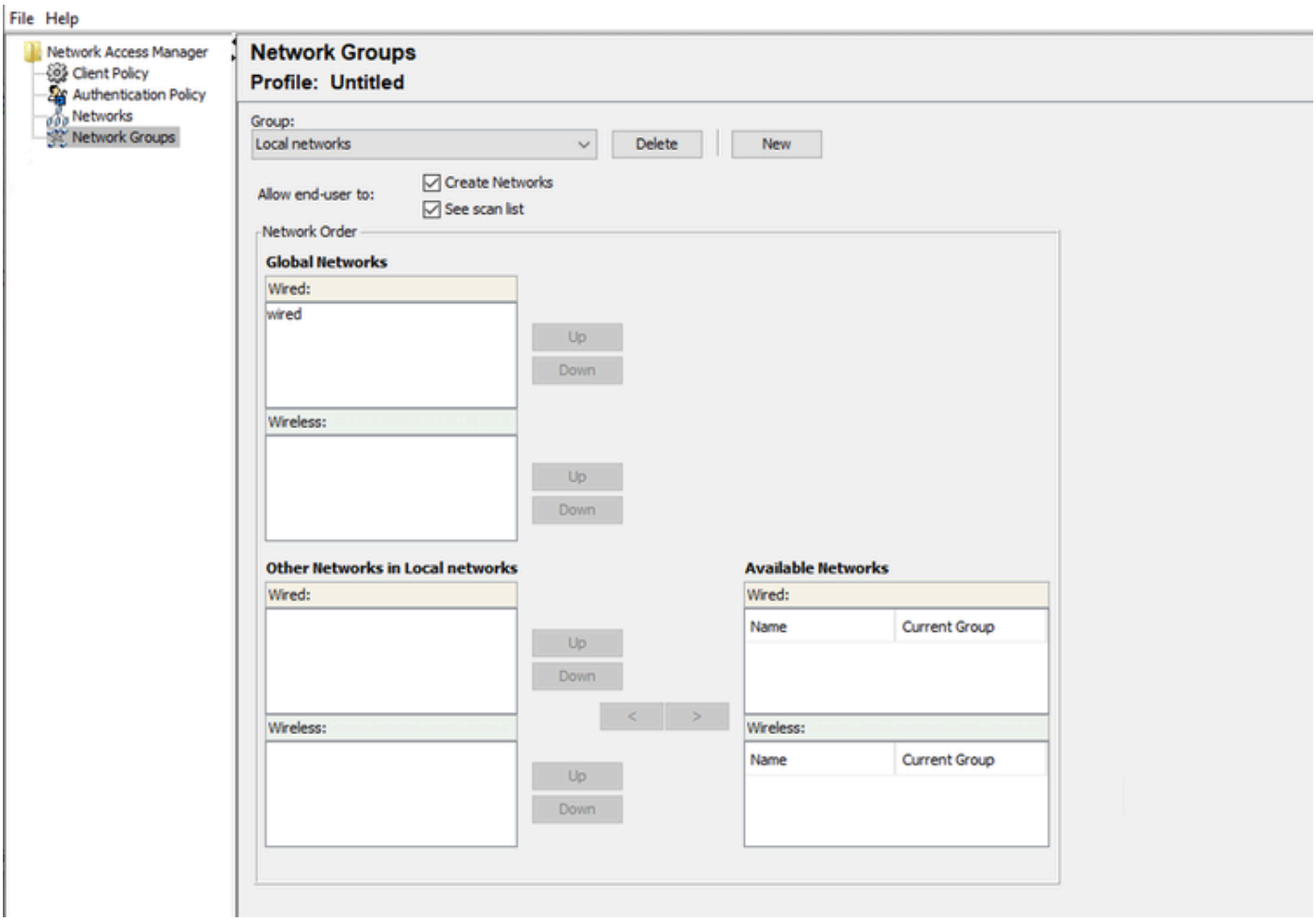
- نهج العميل
- نهج المصادقة
- مجموعات الشبكات



نهج عميل محرر ملف تعريف *NAM*



سياسة مصادقة محرر ملف تعريف *NAM*



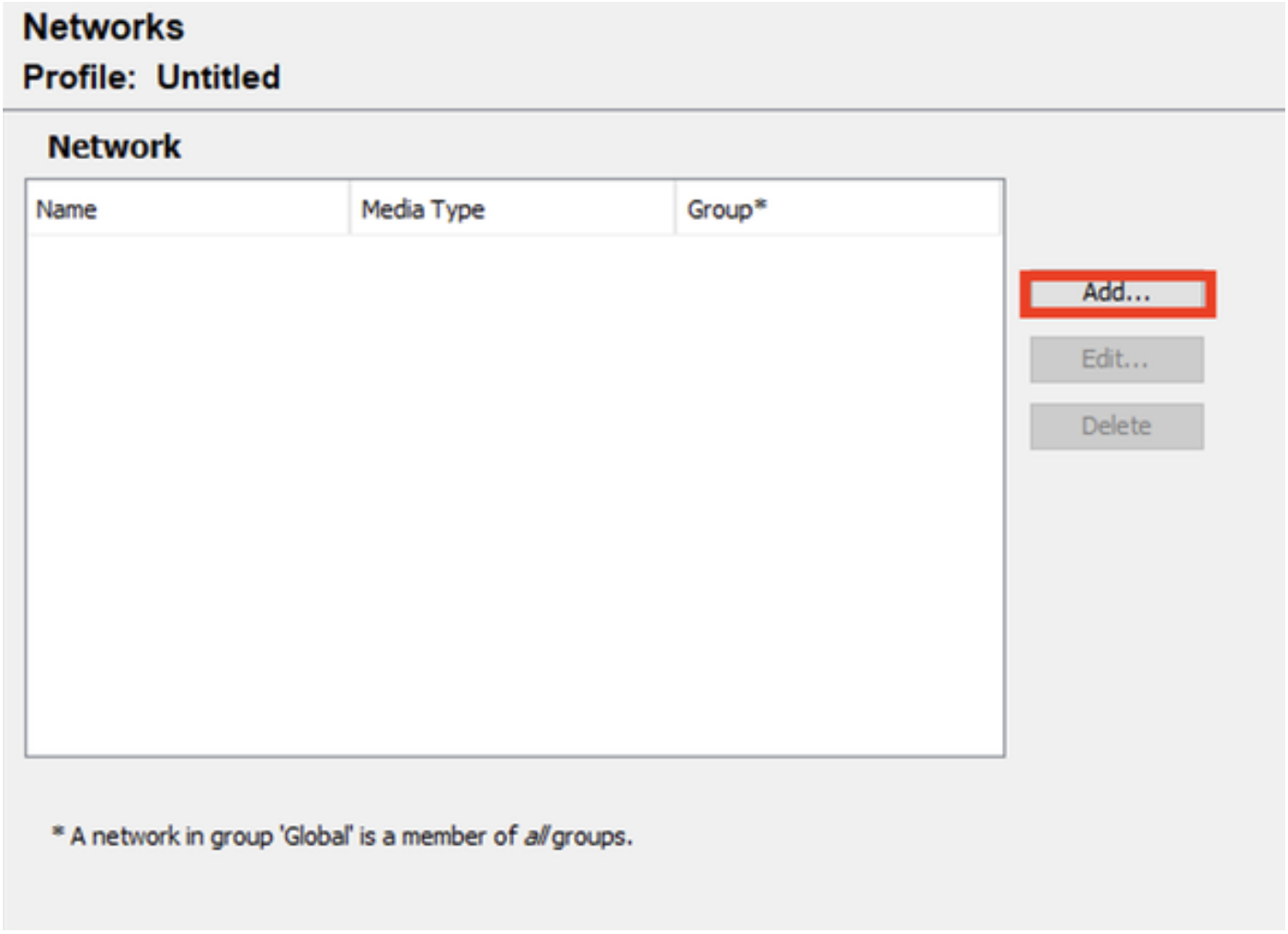
علامة تبويب مجموعات الشبكة

4. السيناريو 1: تكوين عميل NAM الآمن لمصادقة مستخدم PEAP (MS-CHAPv2)

انتقل إلى قسم الشبكات.

يمكن حذف ملف تعريف الشبكة الافتراضي.

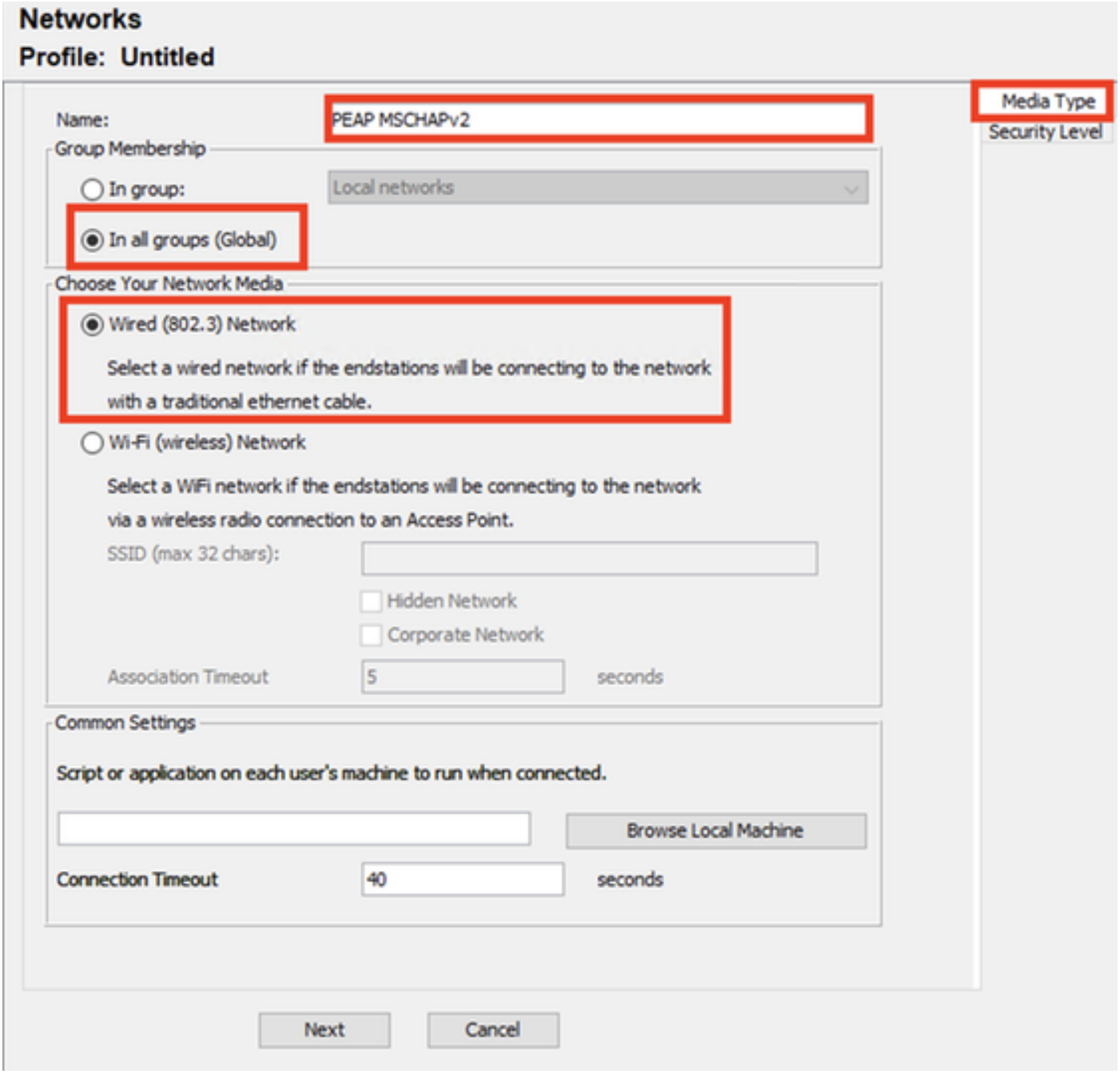
انقر فوق إضافة (Add).



إنشاء ملف تعريف الشبكة

قم بتسمية ملف تعريف الشبكة.

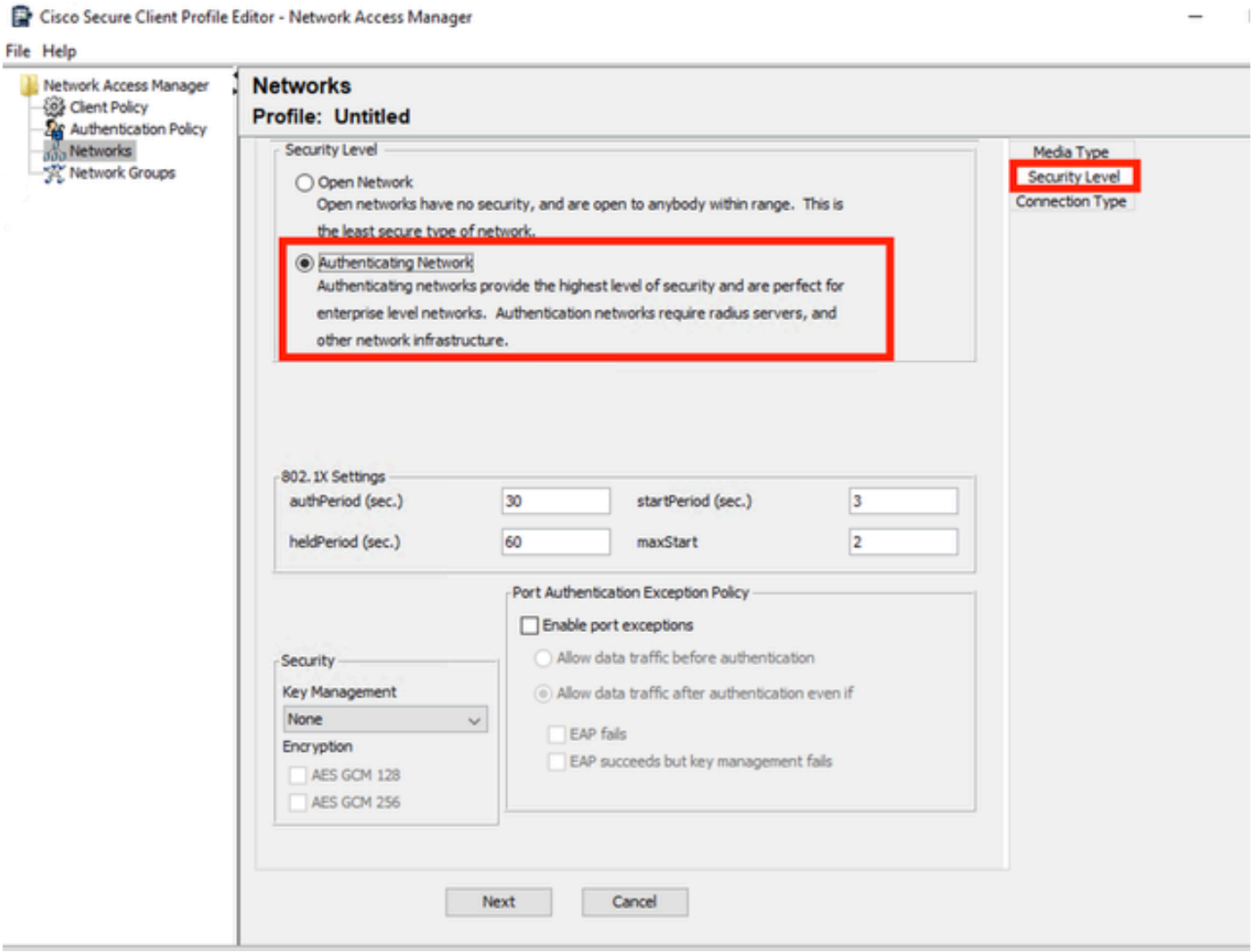
حدد عمومي ل عضوية المجموعة. حدد وسائط الشبكة السلكية.



قسم نوع وسائط ملف تعريف الشبكة

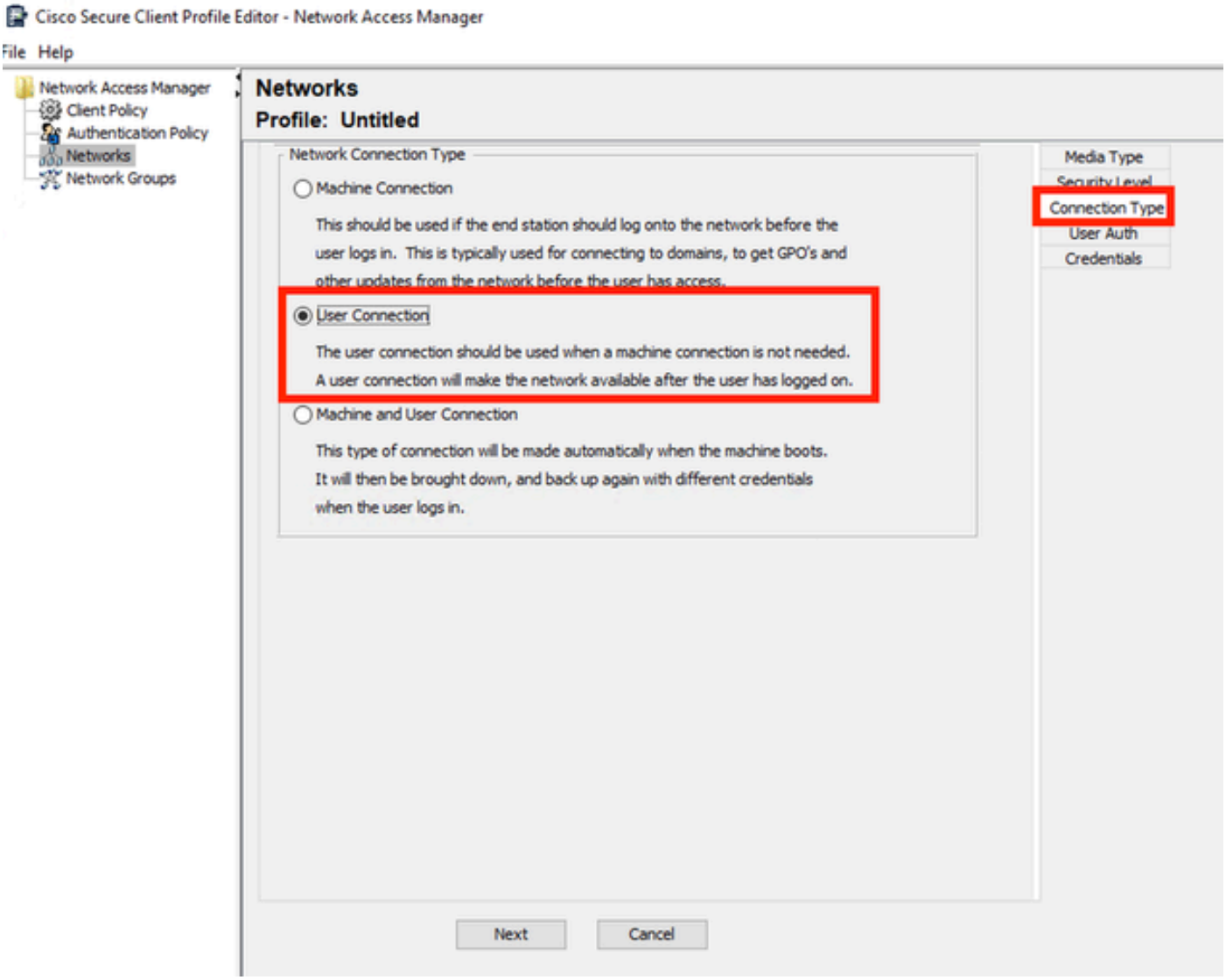
انقر فوق Next (التالي).

حدد مصادقة الشبكة واستخدم الافتراضي لباقي الخيارات في قسم مستوى الأمان.



مستوى أمان توصيف الشبكة

انقر على التالي لمتابعة إستخدام قسم نوع الاتصال.

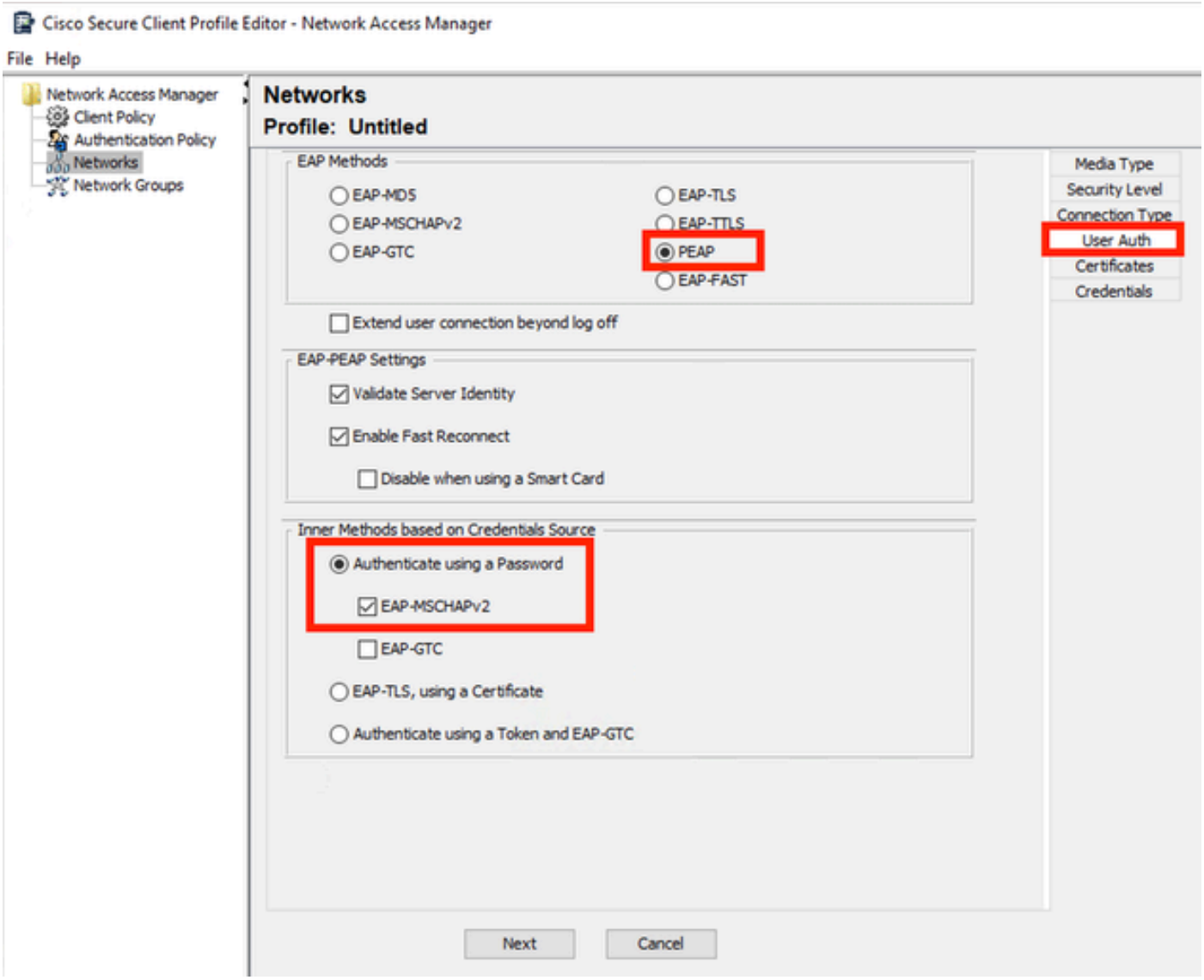


نوع اتصال ملف تعريف الشبكة

حدد نوع اتصال المستخدم.

انقر على التالي لمتابعة قسم مصادقة المستخدم المتوفر الآن.

حدد PEAP كطريقة EAP العامة.



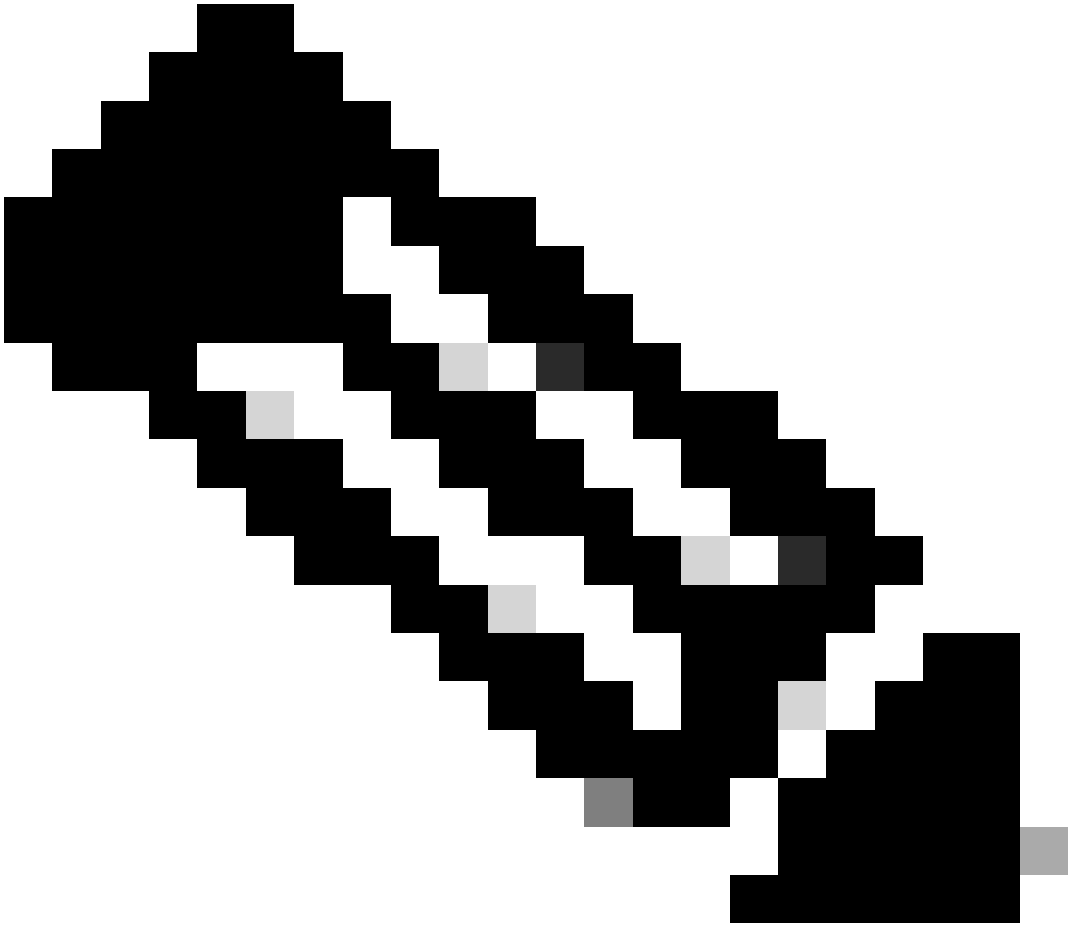
مصادقة مستخدم ملف تعريف الشبكة

ال تغير القيم الافتراضية في إعدادات EAP-PEAP.

تابع مع قسم ألأساليب الداخلية المستندة إلى مصدر بيانات الاعتماد.

من ألأساليب الداخلية المتعددة الموجودة ل EAP PEAP، حدد المصادقة باستخدام كلمة مرور وحدد EAP-MSCHAPv2.

انقر على التالي للاستمرار إلى قسم الشهادة.

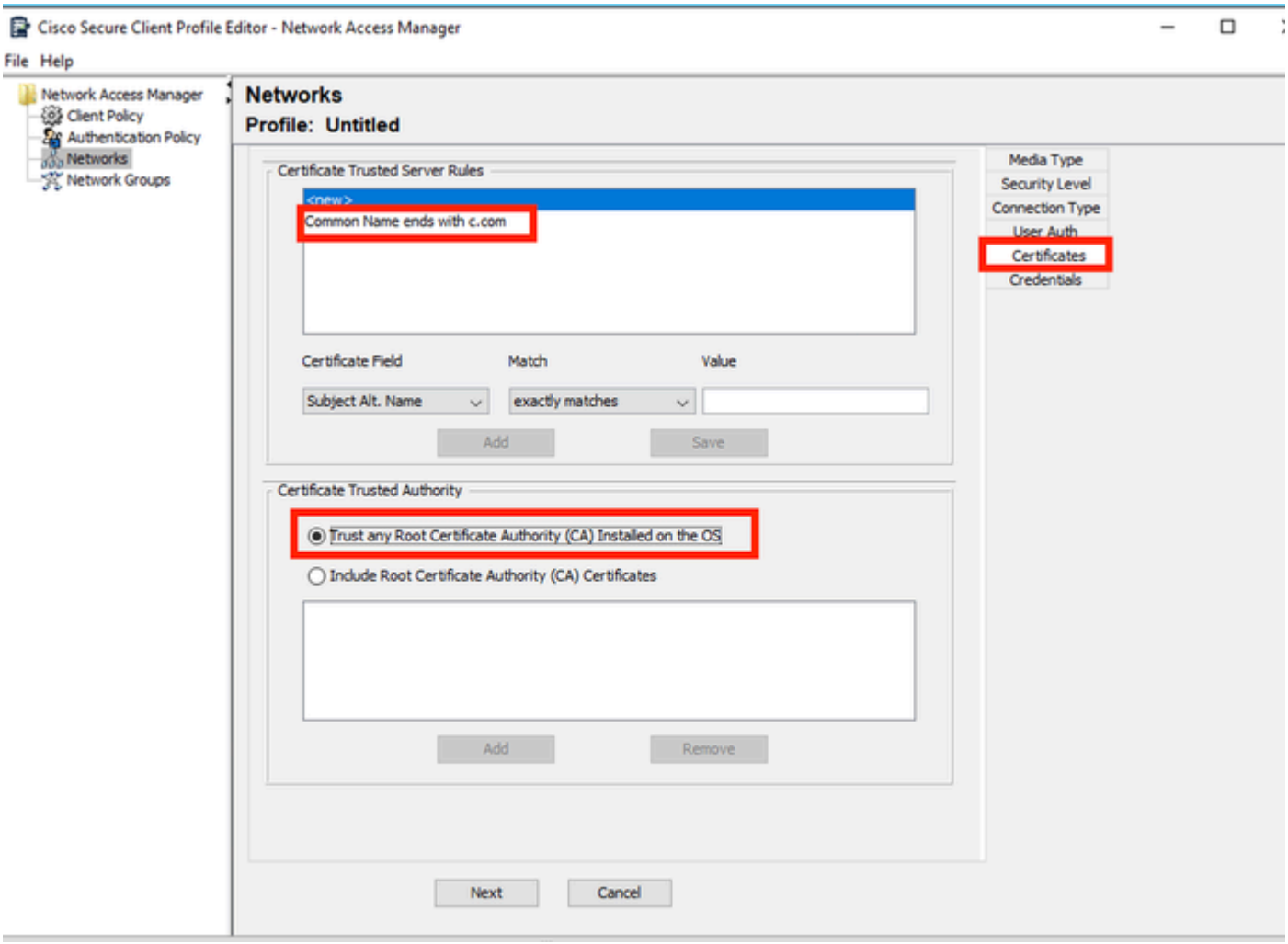


> ملاحظة: يتم عرض قسم الشهادة لأنه قد تم تحديد الخيار التحقق من معرف الخادم في إعدادات EAP-PEAP. بالنسبة إلى EAP PEAP، فإنها تقوم بعملية التضمين باستخدام شهادة الخادم.

في قسم الشهادات، في قواعد خادم الشهادة الموثوق به، يتم إستخدام القاعدة نهاية الاسم الشائع ب c.com.

يشير هذا القسم من التكوين إلى الشهادة التي يستخدمها الخادم أثناء تدفق EAP PEAP.

إذا تم إستخدام محرك خدمة الهوية (ISE) على بيئتك، فيمكنك إستخدام الاسم الشائع لشهادة EAP لعقدة خادم النهج.

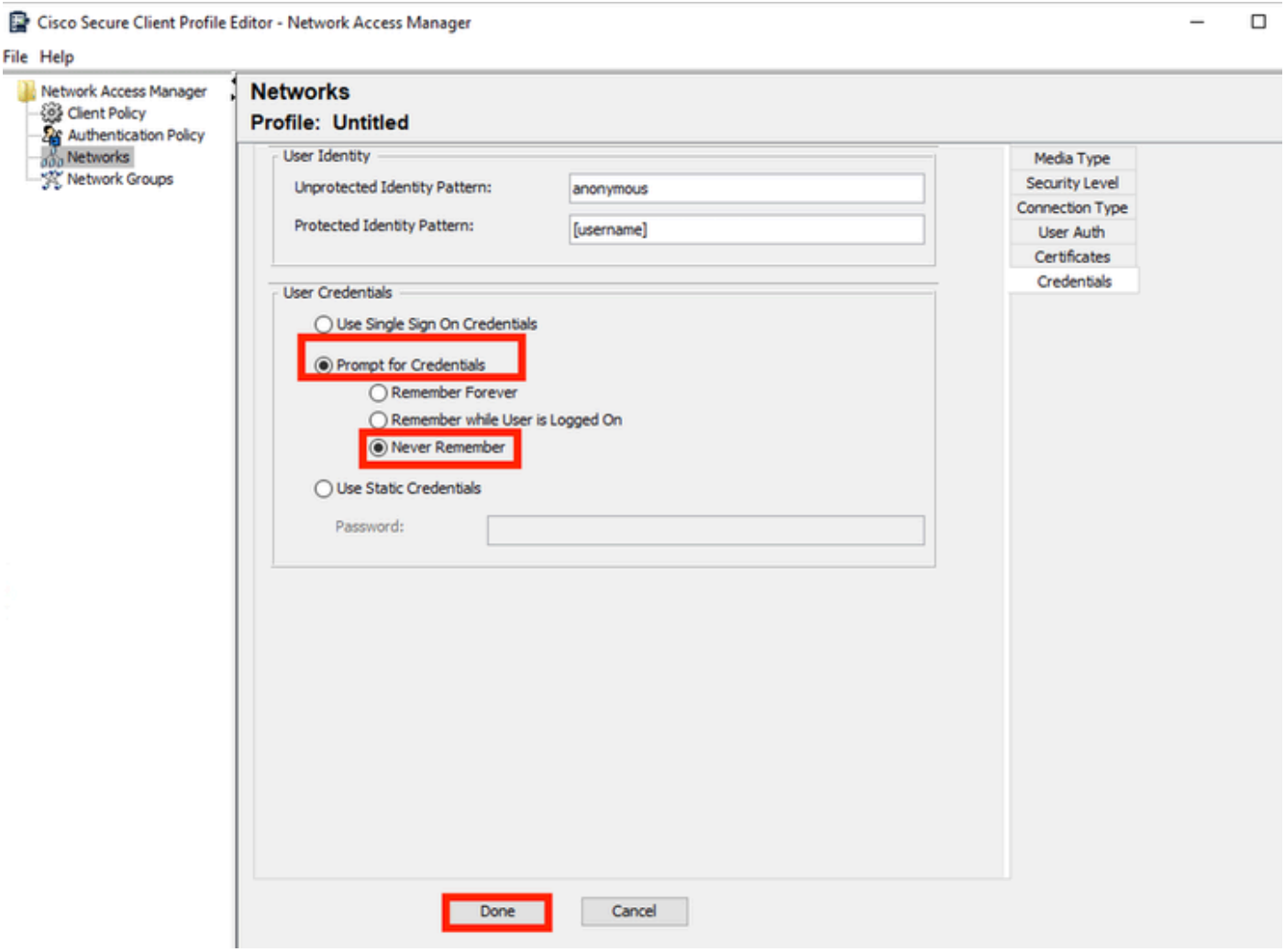


قسم شهادة توصيف الشبكة

يمكن تحديد خياريين في مرجع مصدق ثقة للشهادة. لهذا السيناريو، بدلا من إضافة شهادة مرجع مصدق معينة توقع شهادة RADIUS EAP، يتم إستخدام الخيار "ثقة أي مرجع مصدق جذر (CA) مثبت على نظام التشغيل.

مع هذا الخيار يثق جهاز Windows في أي شهادة EAP موقعة من قبل جهة متضمنة في إدارة ترخيص برنامج تقييم المستخدمين — المستخدم الحالي > مراجع التصديق الجذر الموثوق فيها > الشهادات.

انقر فوق Next (التالي).



قسم بيانات اعتماد ملف تعريف الشبكة

في قسم بيانات الاعتماد يتم تغيير قسم بيانات اعتماد المستخدم فقط.

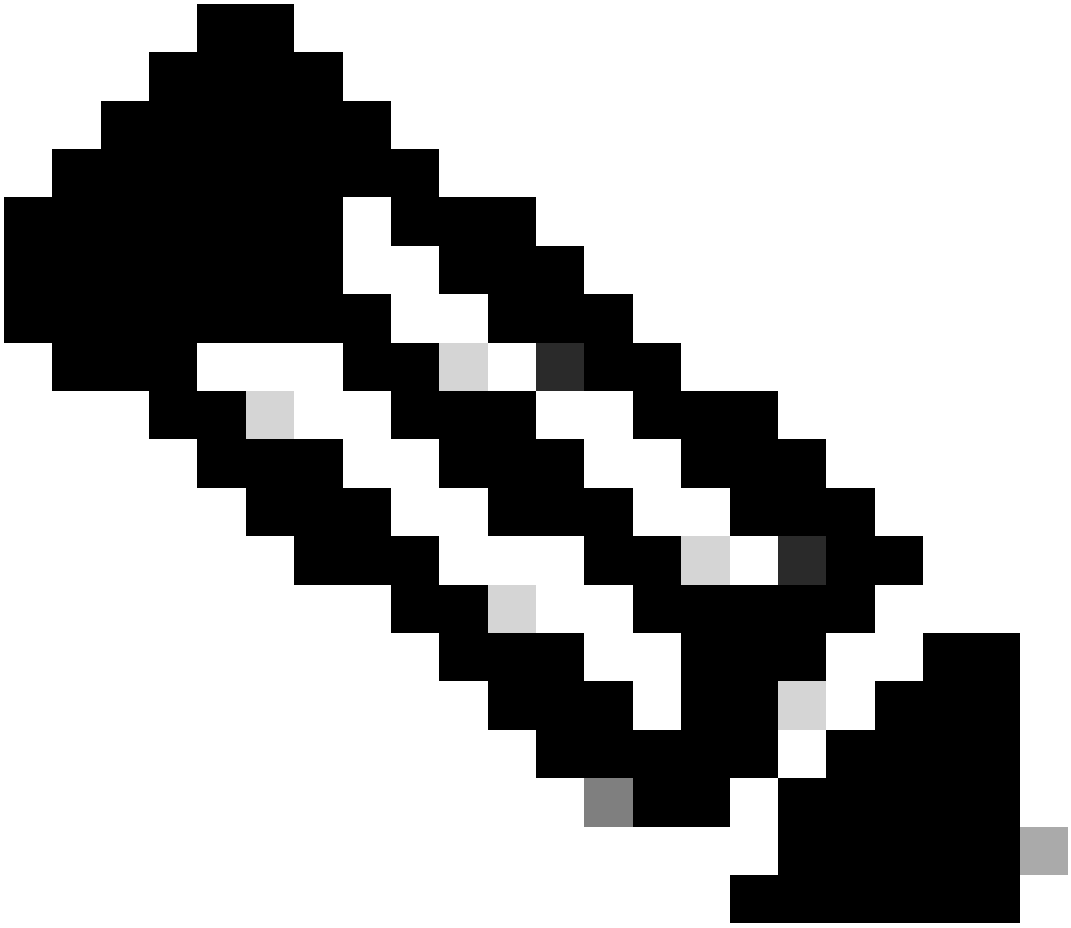
يتم تحديد الخيار مطالبة ببيانات الاعتماد > عدم التذكر أبدا، لذلك في كل مصادقة، يجب على المستخدم الذي يقوم بإجراء المصادقة إدخال بيانات الاعتماد الخاصة به.

طقطقة تم.

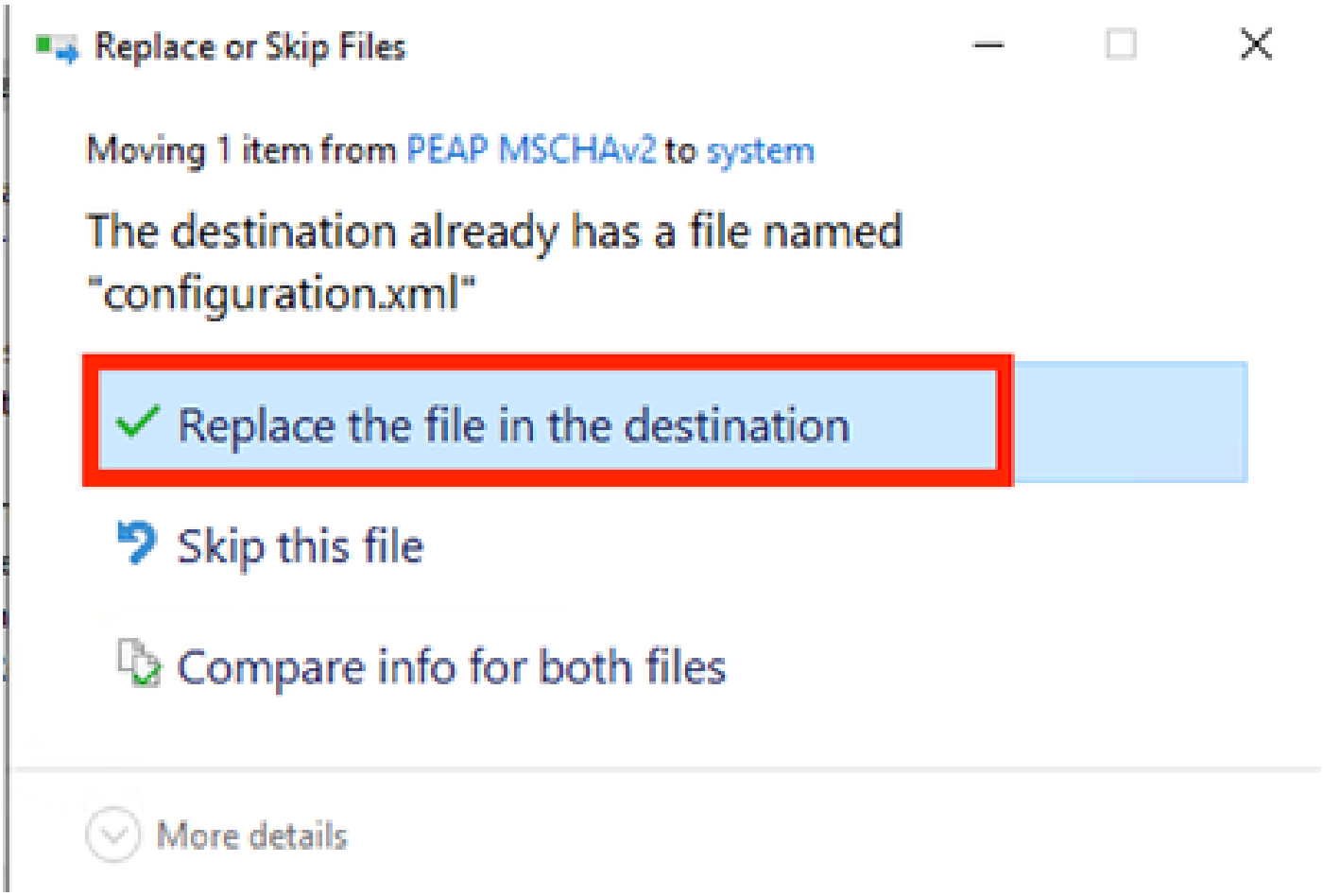
احفظ ملف تعريف Secure Client Network Access Manager، مثل configuration.xml باستخدام خيار ملف > حفظ باسم.

لجعل "إدارة الوصول إلى شبكة العميل الآمنة" تستخدم ملف التعريف الذي تم إنشاؤه للتو، استبدل ملف configuration.xml في الدليل التالي بالدليل الجديد:

C:\ProgramData\Cisco\CiscoSecure Client\Network Access Manager\System



ملاحظة: يجب تسمية الملف configuration.xml، وإلا فلن يعمل.

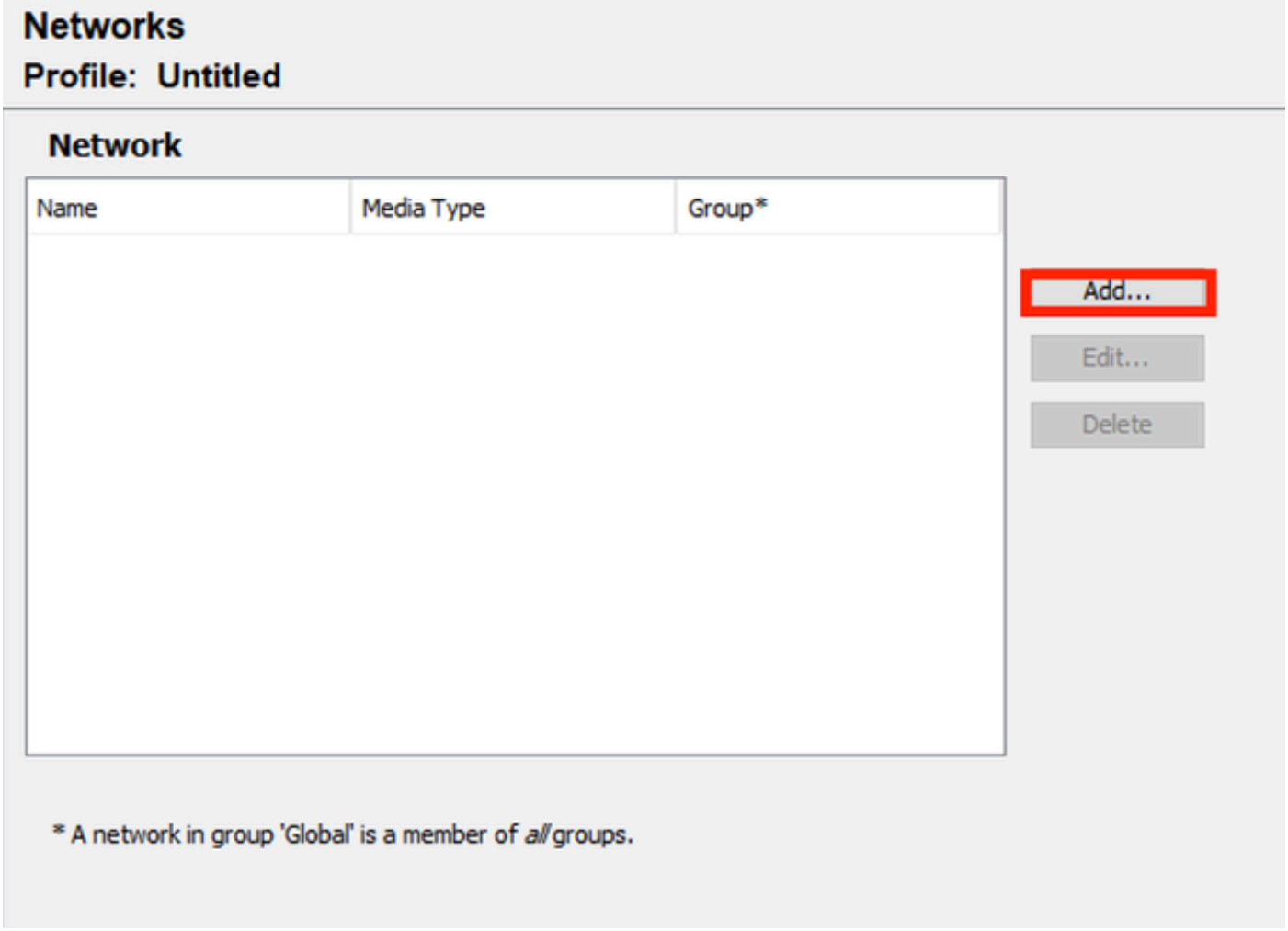


إستبدال مقطع الملف

5. السيناريو 2: تكوين عميل NAM الآمن لمصادقة EAP-FAST المتزامنة للمستخدم والجهاز

افتح محرر ملف تعريف NAM وانتقل إلى قسم الشبكات.

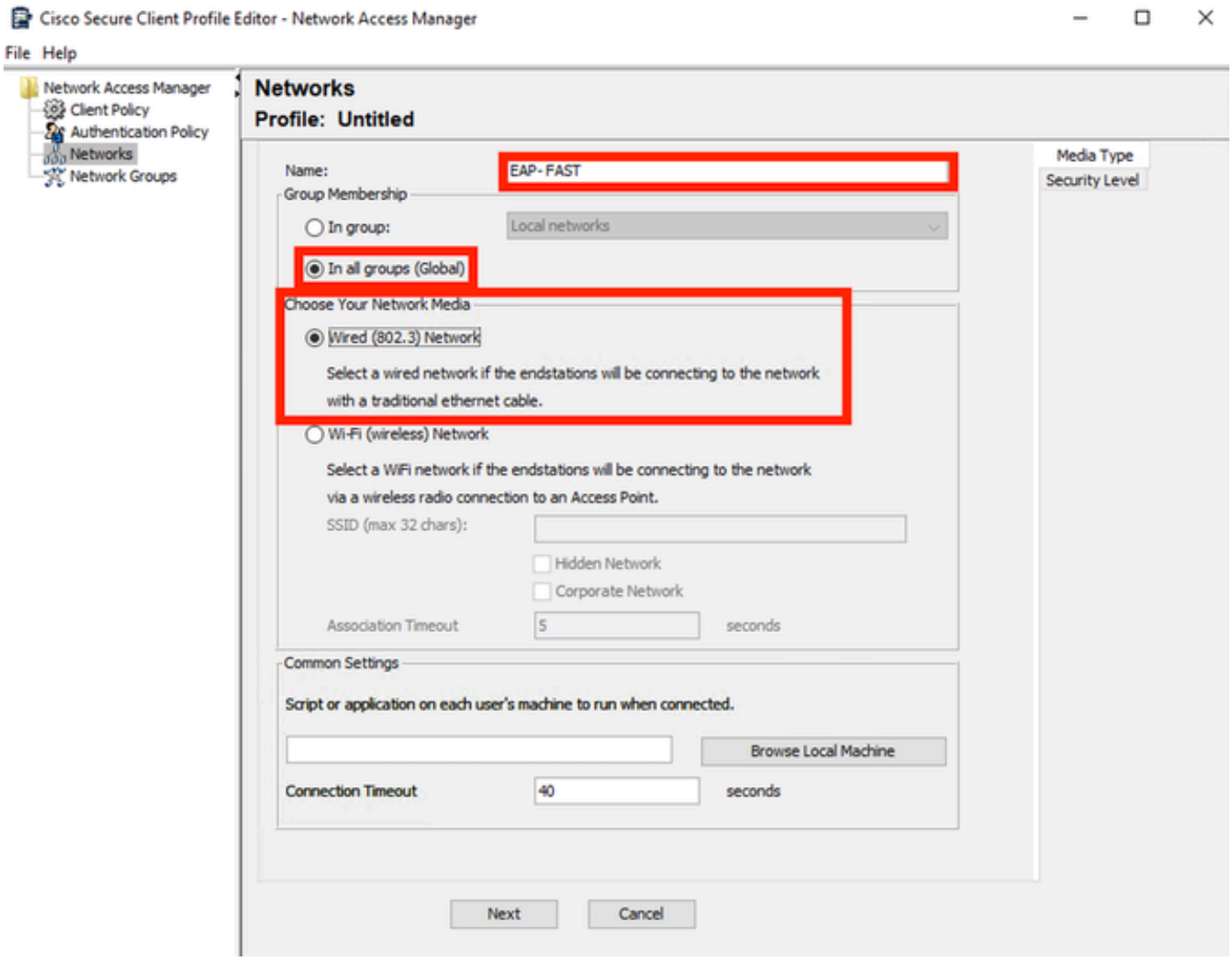
انقر فوق إضافة (Add).



عالمة تبويب شبكة محرر ملف تعريف NAM

أدخل اسما في توصيف الشبكة.

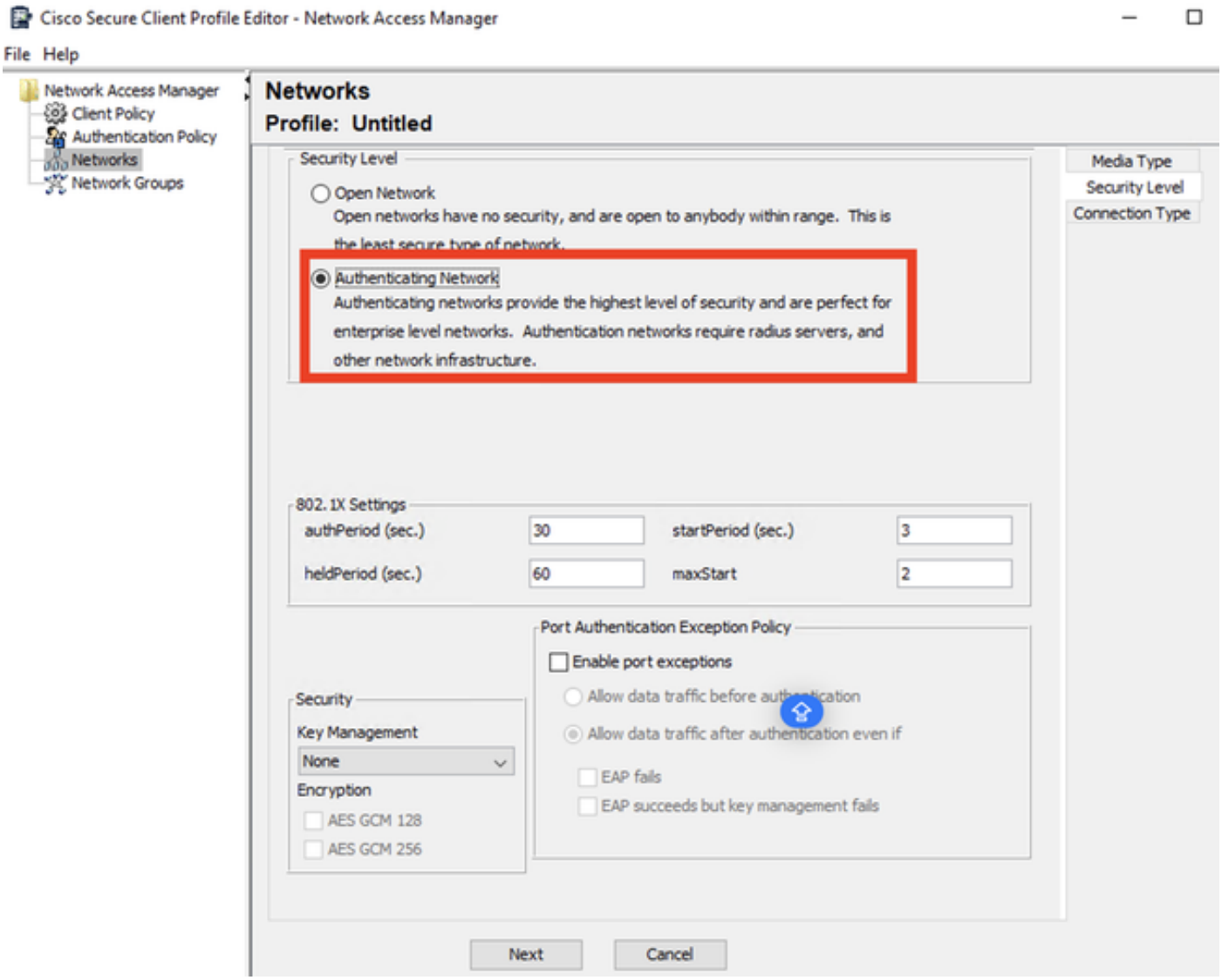
حدد عمومي ل عضوية المجموعة. تحديد وسائط الشبكة السلكية.



قسم نوع الوسائط

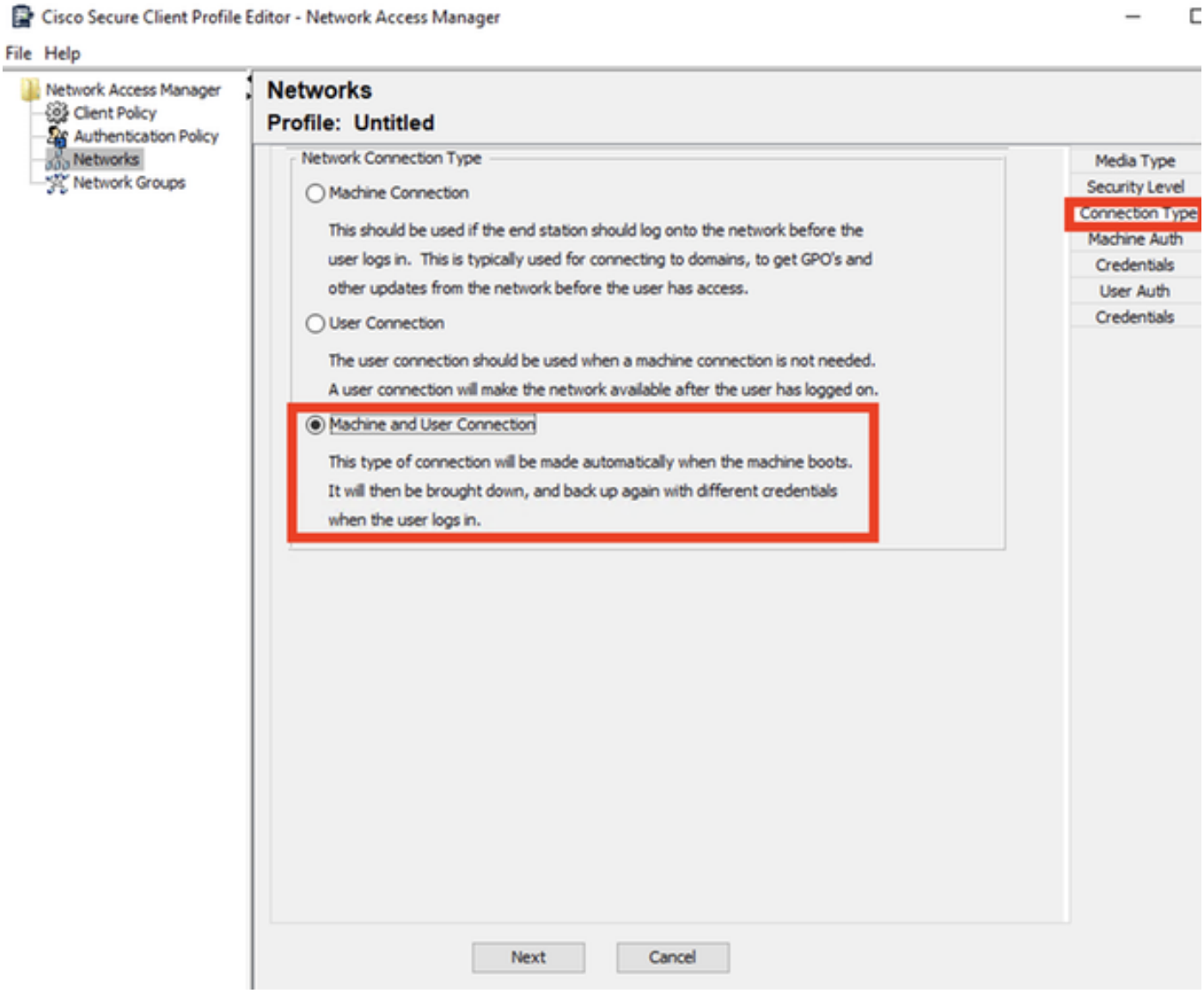
انقر فوق Next (التالي).

حدد مصادقة الشبكة والتغيير القيم الافتراضية لبقية الخيارات في هذا القسم.



قسم محرر ملف تعريف مستوى الأمان

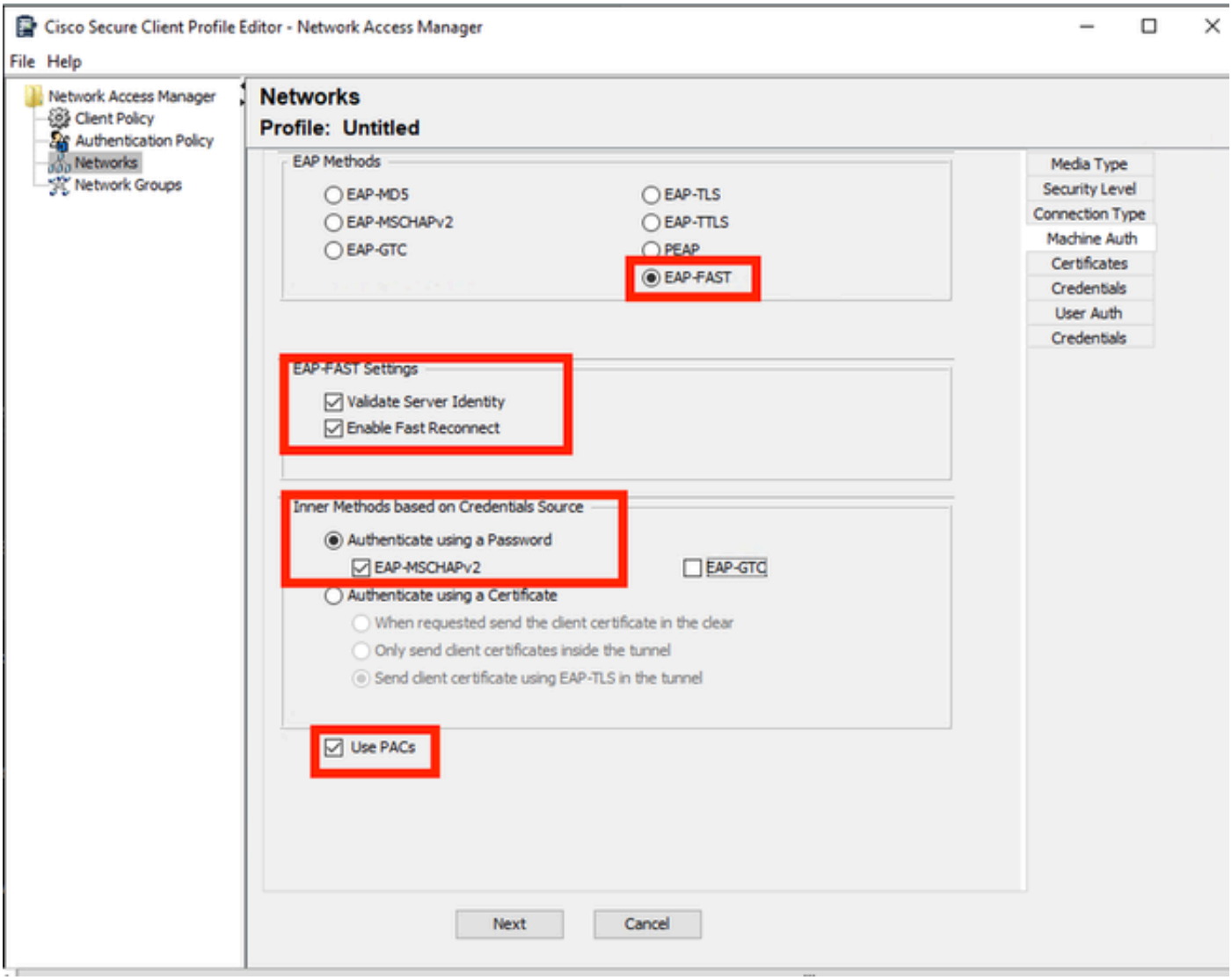
انقر على التالي لمتابعة إستخدام قسم نوع الاتصال.



قسم نوع الاتصال

قم بتكوين مصادقة المستخدم والآلة في آن واحد من خلال تحديد الخيار الثالث.

انقر فوق Next (التالي).



قسم مصادقة الآلة

في قسم مصادقة الجهاز، حدد EAP-FAST كطريقة EAP. لا تغير قيم EAP FAST Settings الافتراضية.

بالنسبة للطرق الداخلية المستندة إلى مصدر بيانات الاعتماد، حدد قسم المصادقة باستخدام كلمة المرور وEAP-MSCHAPv2 باعتباره الطريقة.

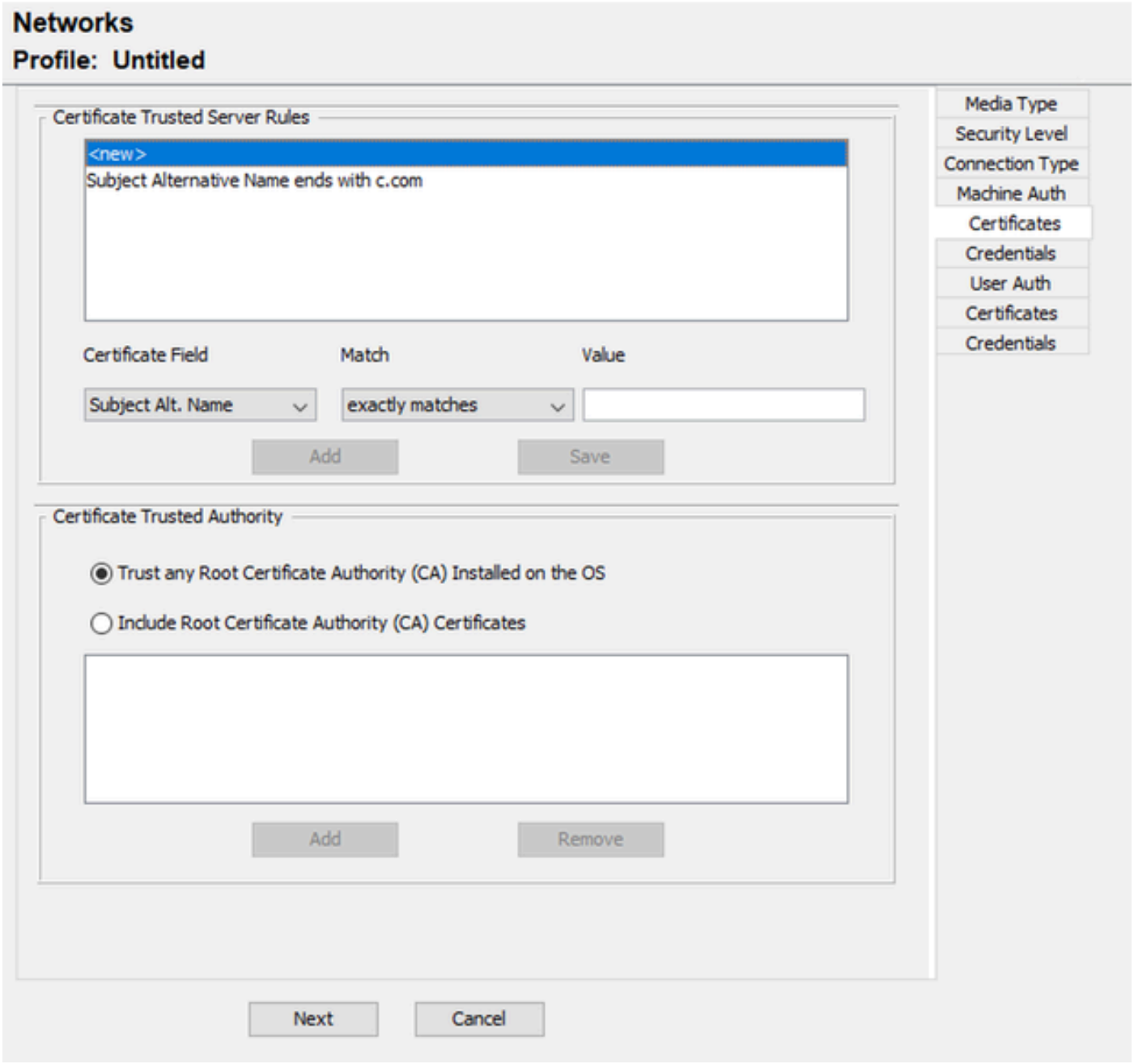
ثم حدد خيار إستخدام مسوغات الوصول المحمي (PACs).

انقر فوق Next (التالي).

في قسم الشهادات، في قواعد خادم الشهادة الموثوق به ينتهي الاسم الشائع للقاعدة ب c.com.

يشير هذا القسم إلى الشهادة التي يستخدمها الخادم أثناء تدفق EAP PEAP.

في حالة إستخدام محرك خدمة الهوية (ISE) على بيئتك، يمكن إستخدام الاسم الشائع لشهادة EAP لعقدة خادم النهج.

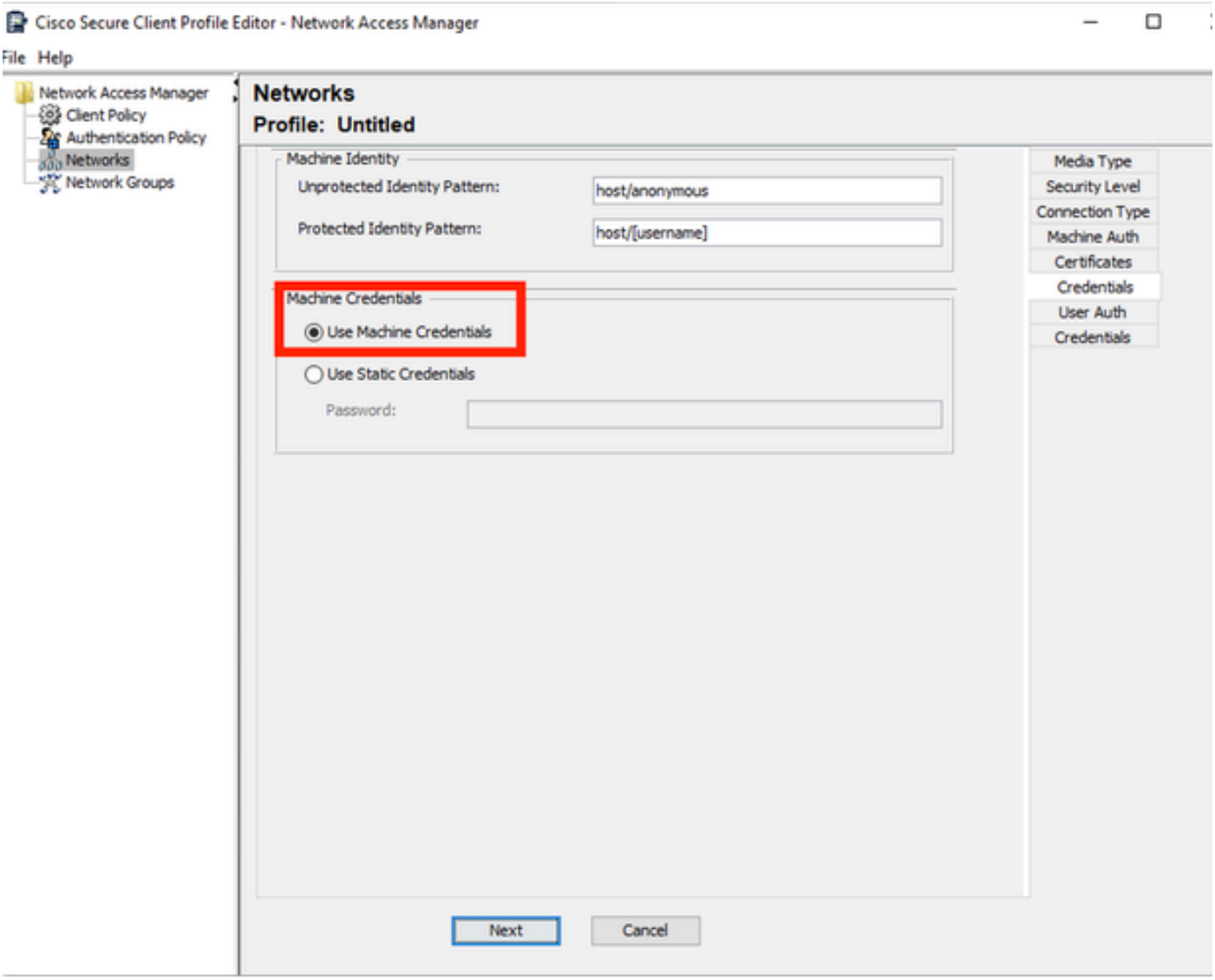


قسم الثقة بشهادة خادم المصادقة الآلية

يمكن تحديد خيارين في المرجع المصدق عليه. لهذا السيناريو، بدلا من إضافة شهادة مرجع مصدق محددة موقعة على شهادة RADIUS EAP، أستخدم الخيار ثقة في أي مرجع مصدق جذري (CA) مثبت على نظام التشغيل.

باستخدام هذا الخيار، يثق Windows في أي شهادة EAP موقعة من قبل لجنة خبراء متضمنة في برنامج إدارة شهادة المستخدم (المستخدم الحالي > مراجع التصديق الجذر الموثوق فيها > الشهادات).

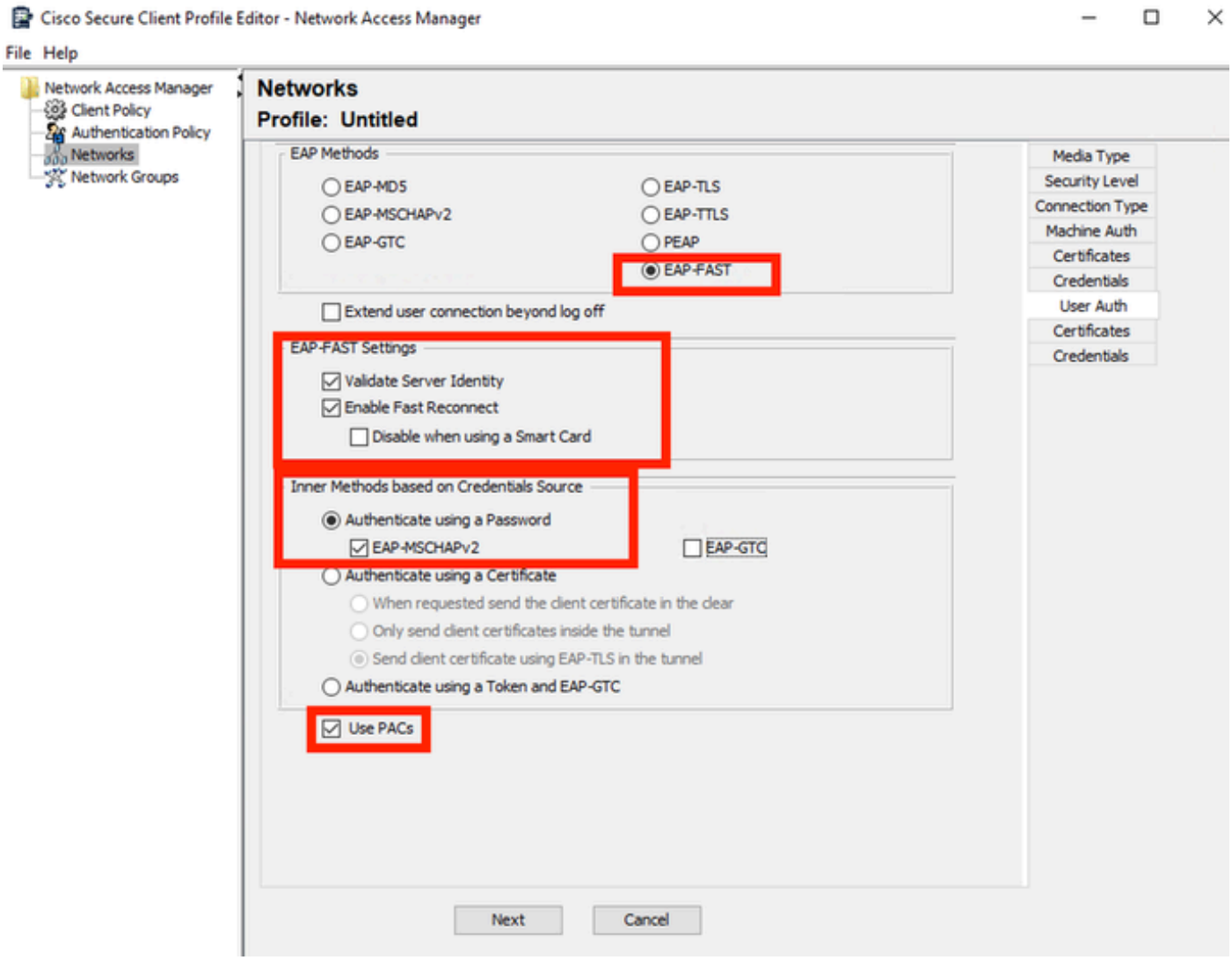
انقر فوق Next (التالي).



قسم بيانات اعتماد مصادقة *Mahine*

حدد إستخدام مسوغات الجهاز في قسم مسوغات الجهاز.

انقر فوق Next (التالي).



قسم مصادقة المستخدم

بالنسبة إلى مصادقة المستخدم، حدد EAP-FAST كطريقة EAP.

ال تغير القيم الافتراضية في قسم إعدادات EAP-FAST.

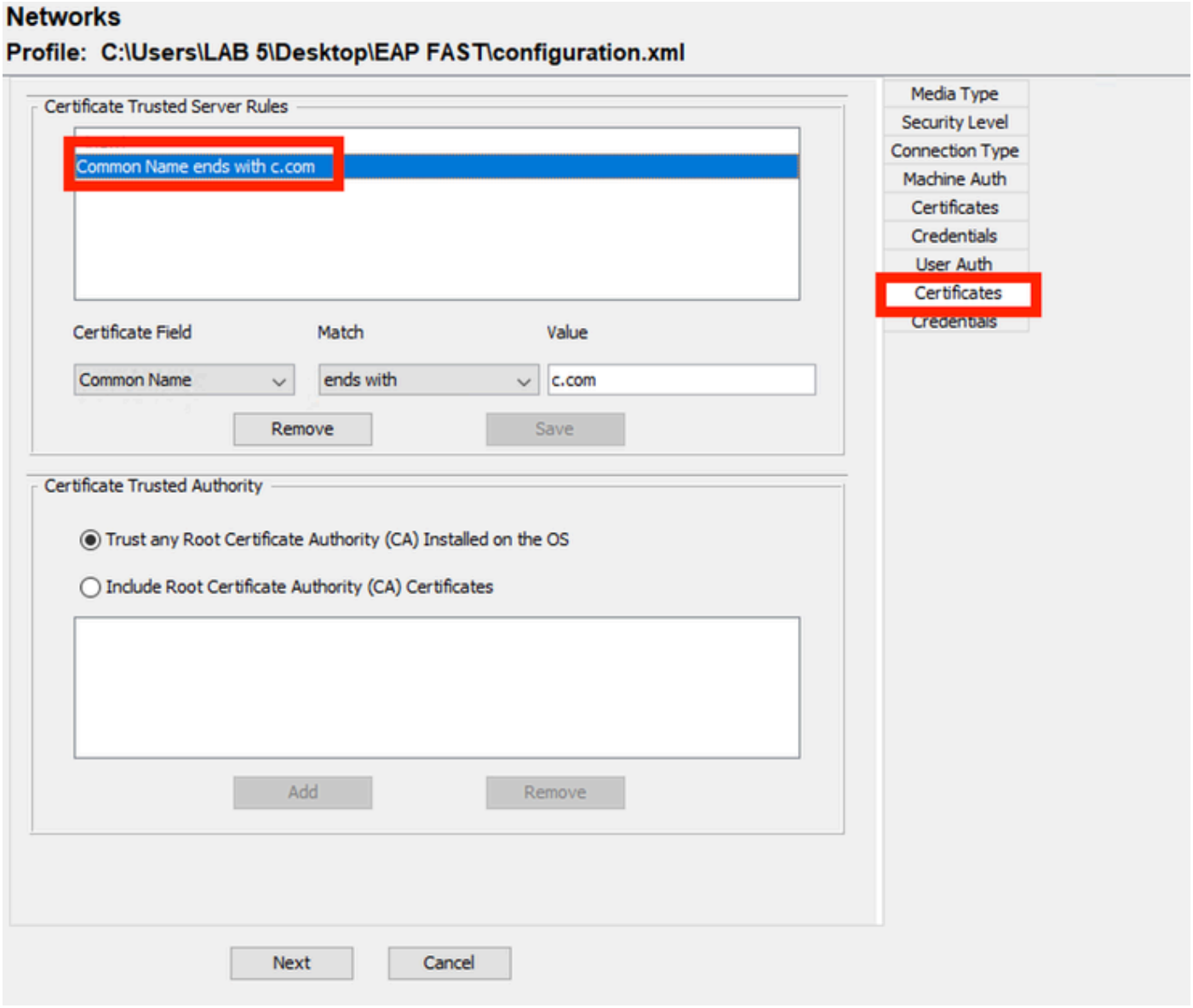
بالنسبة للأسلوب الداخلي المستند إلى قسم مصدر بيانات الاعتماد، حدد المصادقة باستخدام كلمة مرور وEAP-MSCHAPv2 كطريقة.

حدد إستخدام مسوغات الوصول المحمي (PACs).

انقر فوق Next (التالي).

في قسم الشهادات، في قواعد خادم الشهادة الموثوق به، تنتهي القاعدة باسم عام ب c.com.

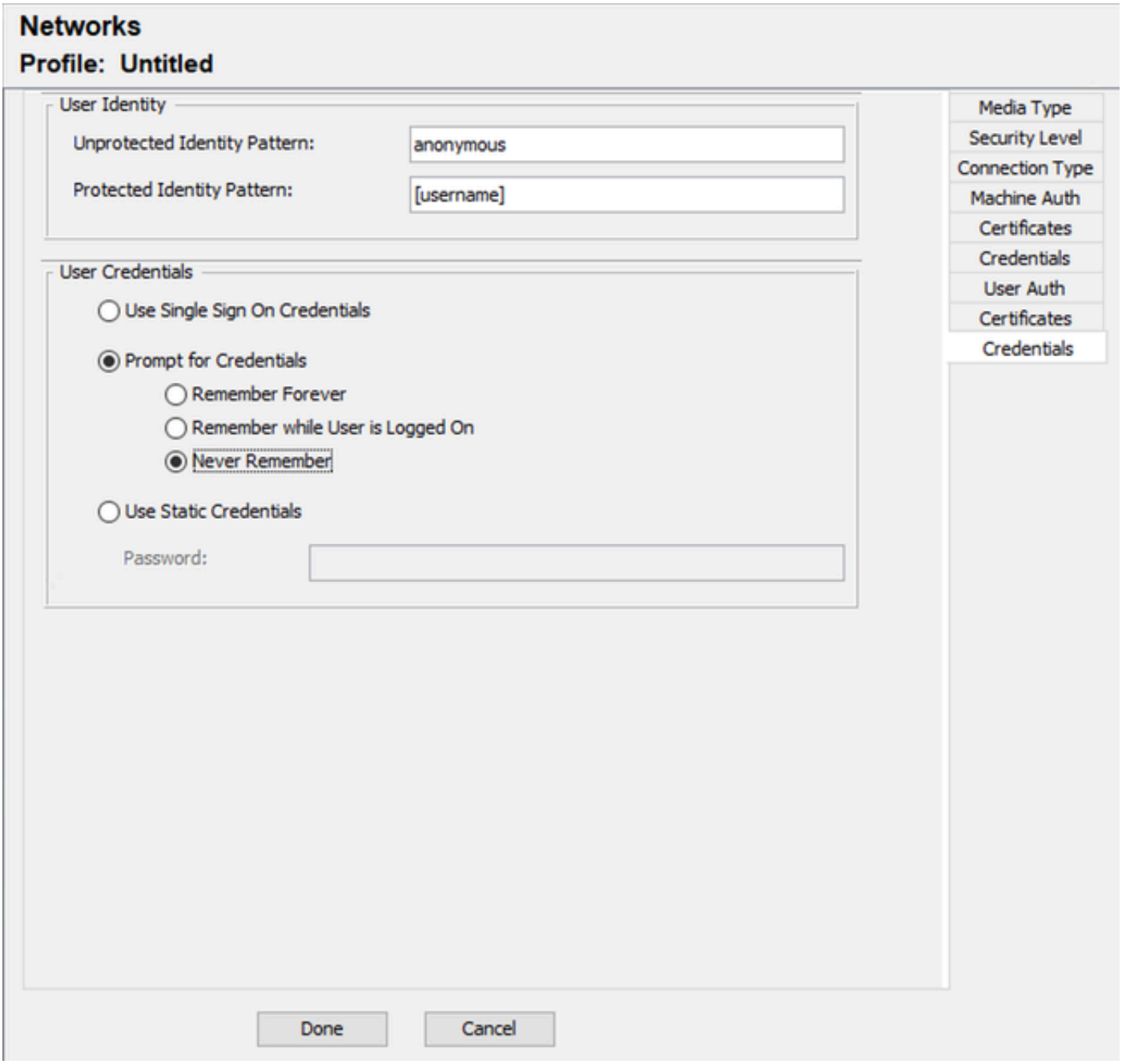
وهذه التكوينات هي للشهادة التي يستخدمها الخادم أثناء تدفق EAP PEAP. إذا تم إستخدام ISE في بيئتك، يمكن إستخدام الاسم الشائع لشهادة EAP الخاصة بعقدة خادم النهج.



قسم الثقة في شهادة خادم مصادقة المستخدم

يمكن تحديد خيارين في المرجع المصدق. لهذا السيناريو بدلا من إضافة شهادة مرجع مصدق محددة موقعة على شهادة RADIUS EAP، يتم إستخدام الخيار ثقة أي مرجع مصدق جذر (CA) مثبت على نظام التشغيل.

انقر فوق Next (التالي).



بيانات اعتماد مصادقة المستخدم

في قسم المسوغات، يتم تغيير قسم مسوغات المستخدم فقط.

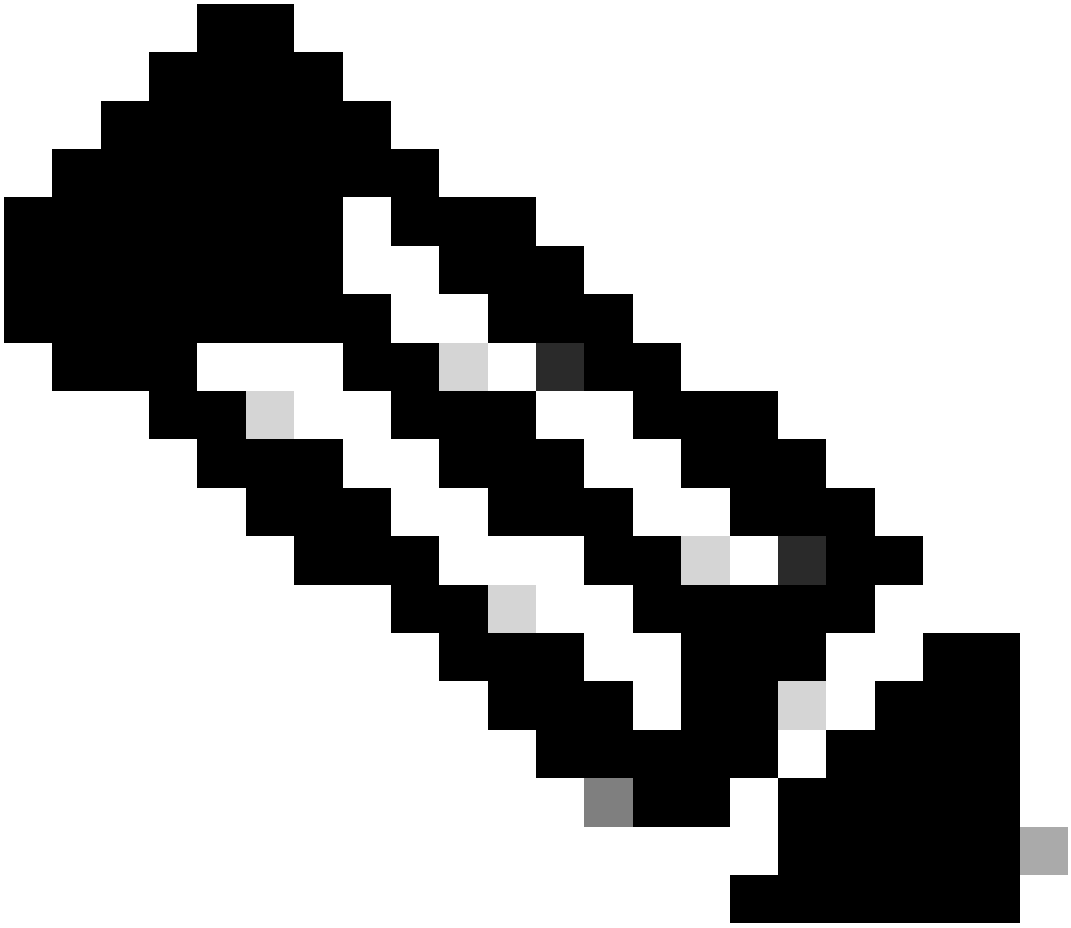
تم تحديد الخيار رسالة حث بيانات الاعتماد > عدم التذكر. لذلك في كل مصادقة، يجب أن تدخل مصادقة المستخدم بيانات الاعتماد الخاصة بهم.

انقر فوق الزر تم".

حدد ملف > حفظ باسم ثم احفظ ملف تعريف Secure Client Network Access Manager باسم Configuration.xml.

لجعل Secure Client Network Access Manager يستخدم ملف التعريف الذي تم إنشاؤه للتو، استبدل ملف configuration.xml في الدليل التالي بالدليل الجديد:

C:\ProgramData\Cisco\CiscoSecure Client\Network Access Manager\System

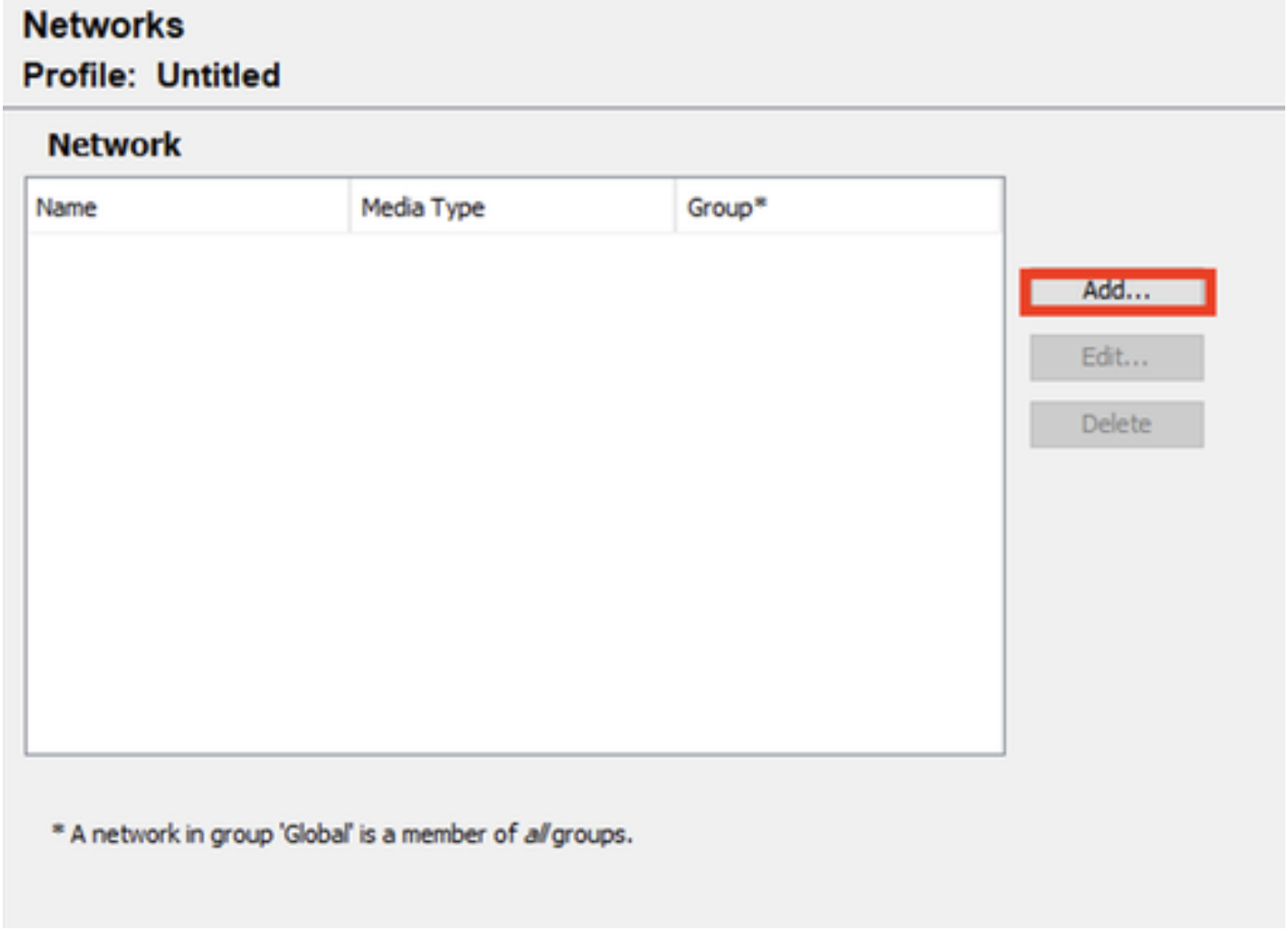


ملاحظة: يجب تسمية الملف configuration.xml، وإلا فلن يعمل.

6. السيناريو 3: تكوين طالب NAM الآمن لمصادقة شهادة مستخدم EAP TLS

افتح محرر ملف تعريف NAM وانتقل إلى قسم الشبكات.

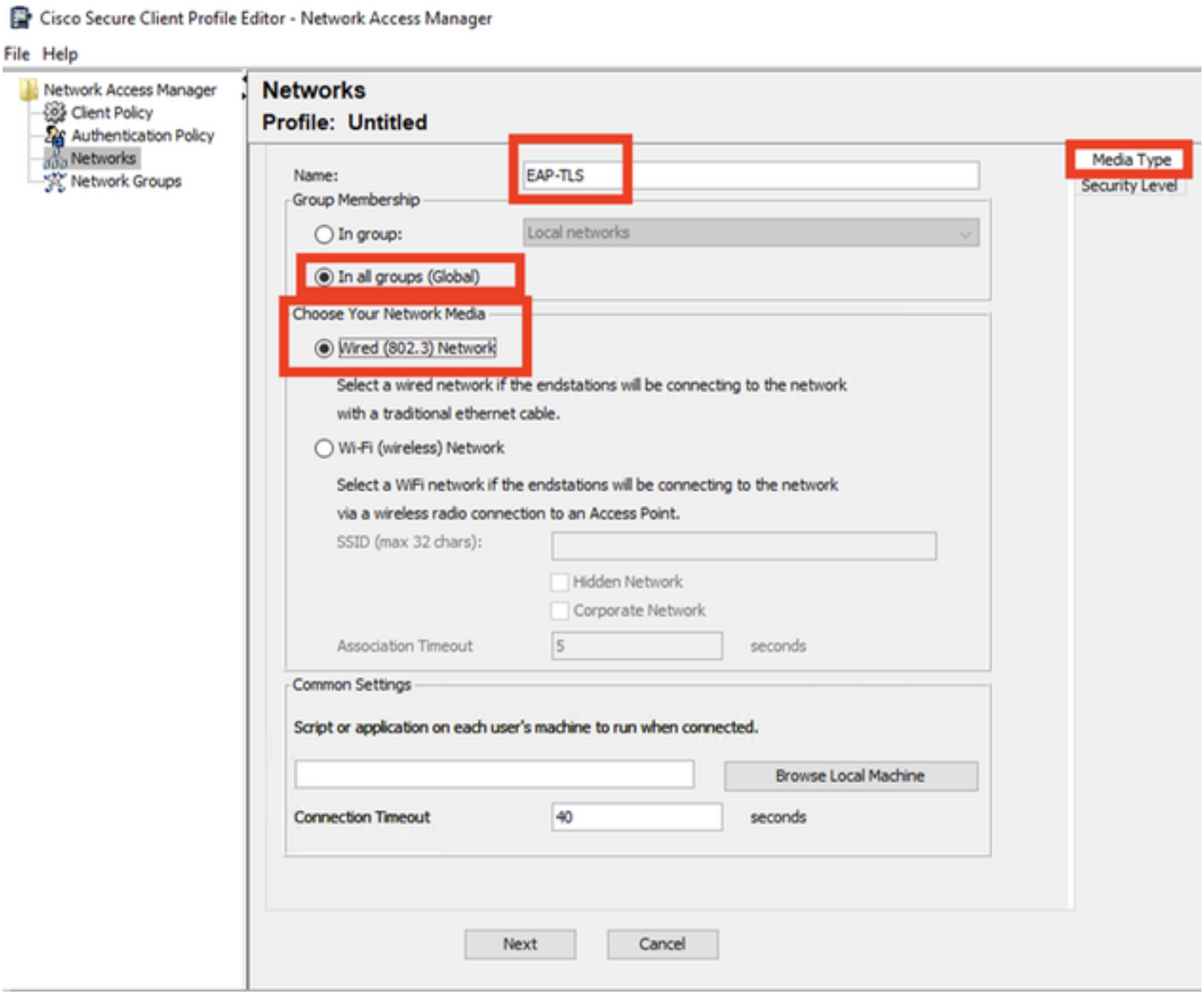
انقر فوق إضافة (Add).



قسم إنشاء الشبكة

قم بتسمية ملف تعريف الشبكة، وفي هذه الحالة يكون المسمى مع بروتوكول EAP المستخدم لهذا السيناريو.

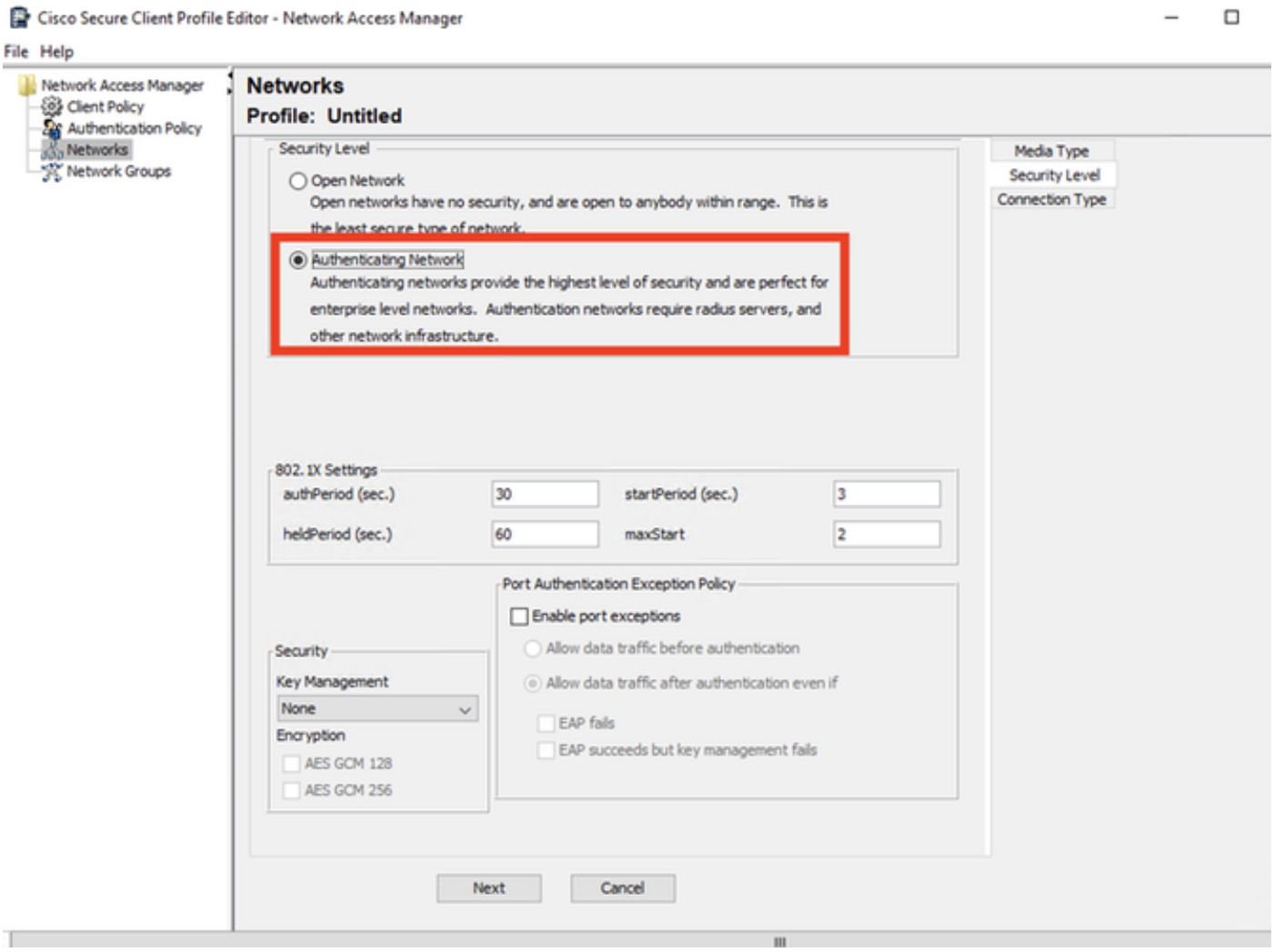
حدد عمومي ل عضوية المجموعة. وسائط الشبكة السلكية.



قسم نوع الوسائط

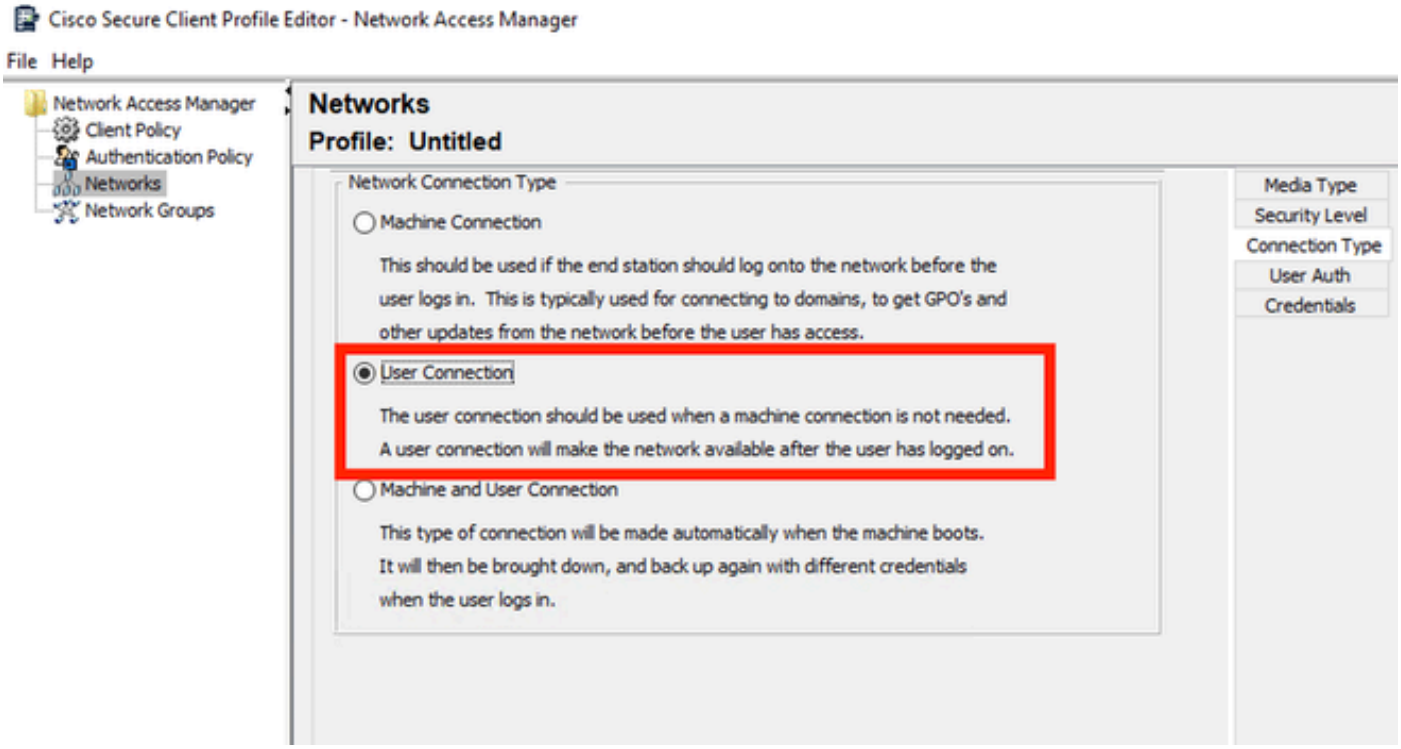
انقر فوق Next (التالي).

حدد مصادقة الشبكة والا تغير القيم الافتراضية لبقية الخيارات في قسم مستوى الأمان.



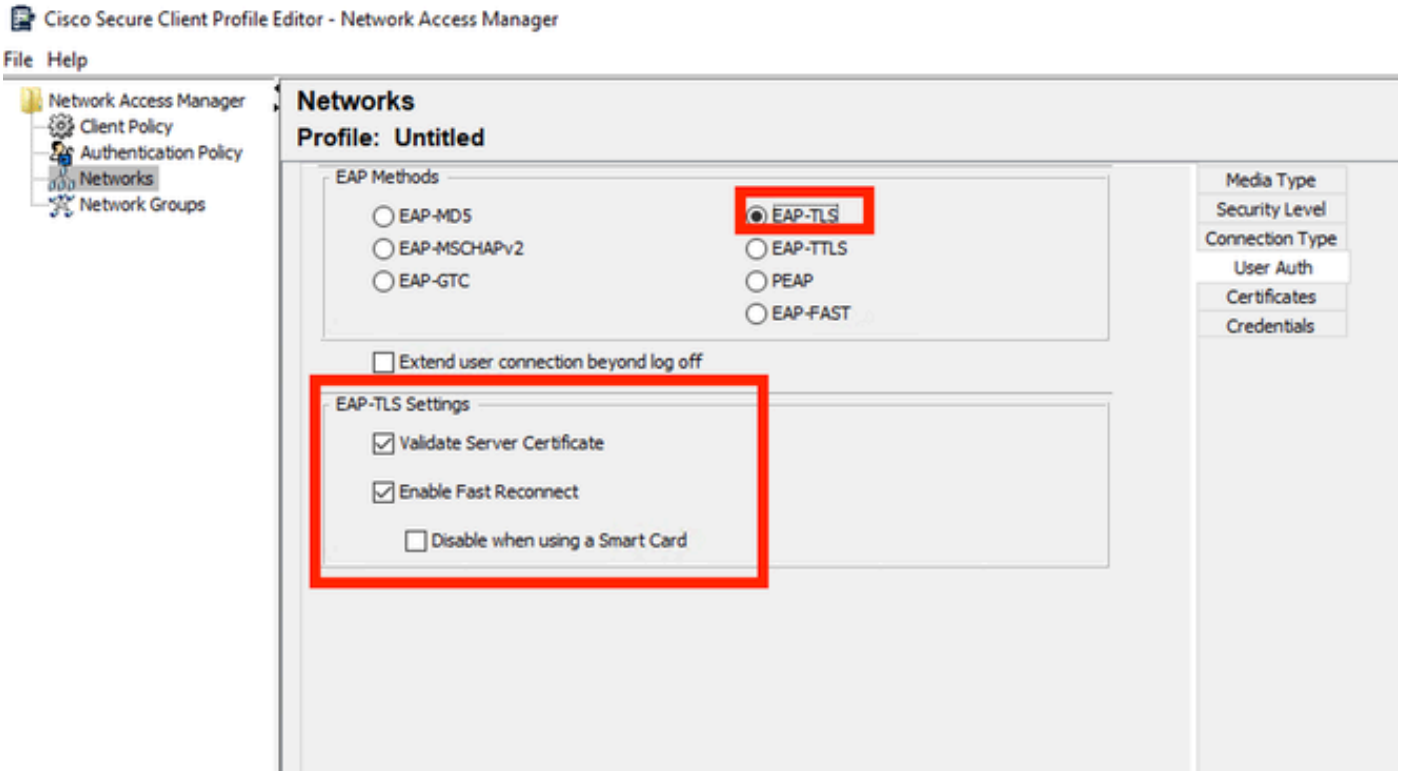
مستوى الأمان

هذا السيناريو لمصادقة المستخدم باستخدام شهادة. ولهذا السبب يتم إستخدام خيار اتصال المستخدم.



نوع الاتصال

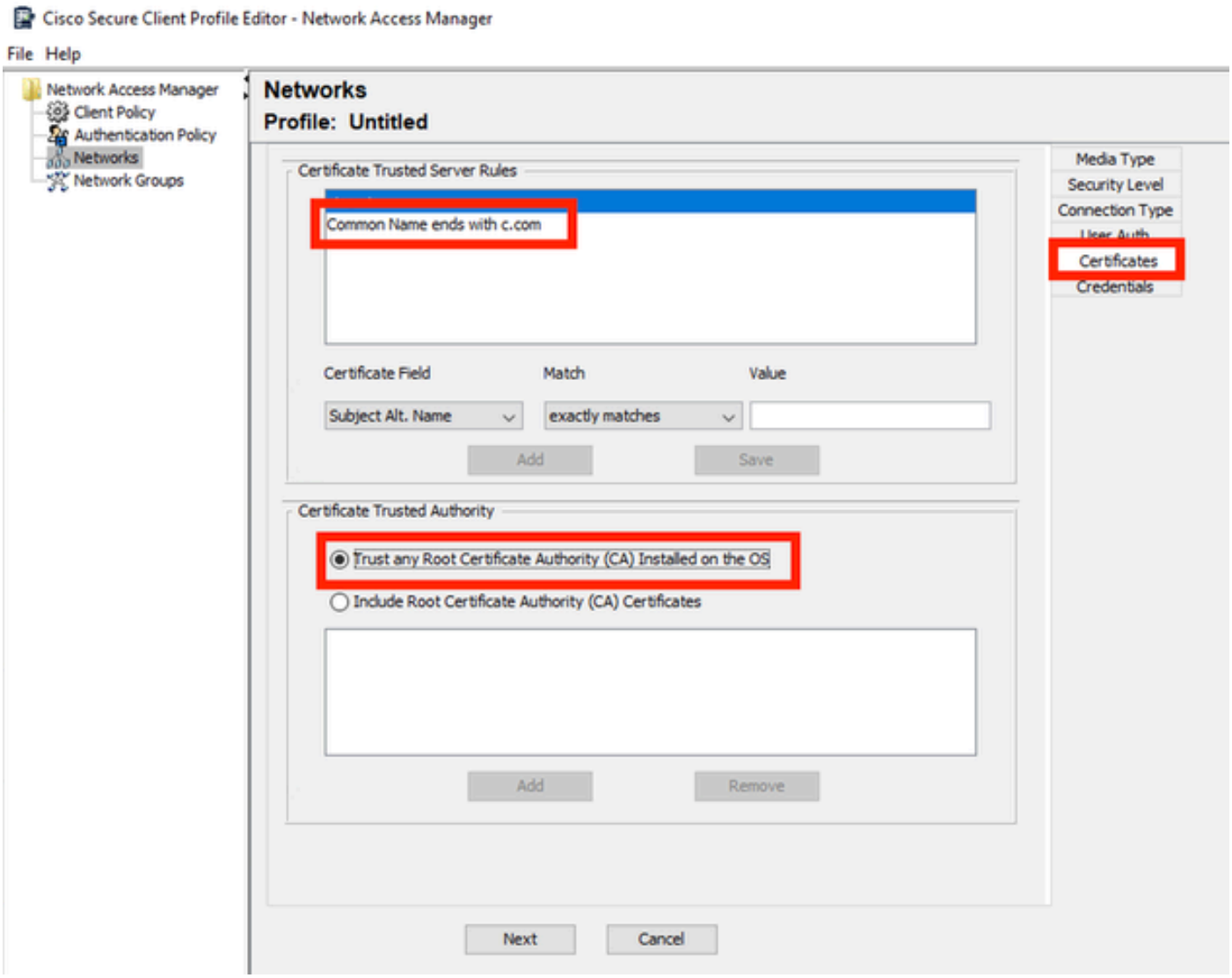
قم بتكوين EAP-TLS كطريقة EAP. لا تغير القيم الافتراضية في قسم إعدادات EAP-TLS.



قسم مصادقة المستخدم

بالنسبة لقسم الشهادات، قم بإنشاء قاعدة تطابق شهادة AAA EAP-TLS. إذا كنت تستخدم ISE، ابحث عن هذه القاعدة في قسم إدارة > نظام > شهادات.

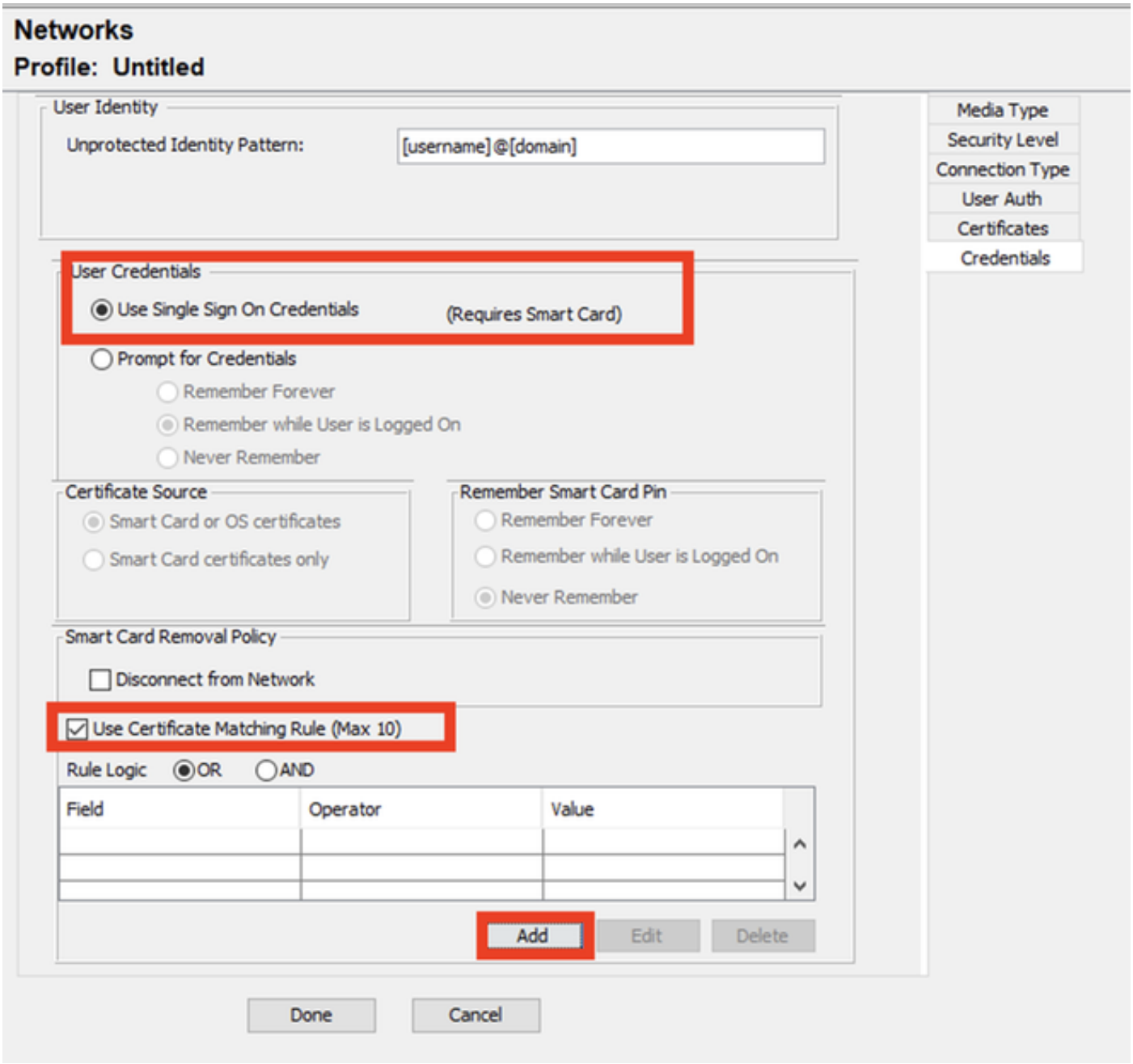
بالنسبة لقسم المرجع الموثوق به للشهادات، حدد الثقة بأي مرجع مصدق جذر (CA) مثبت على نظام التشغيل.



إعدادات الثقة بشهادة خادم مصادقة المستخدم

انقر فوق Next (التالي).

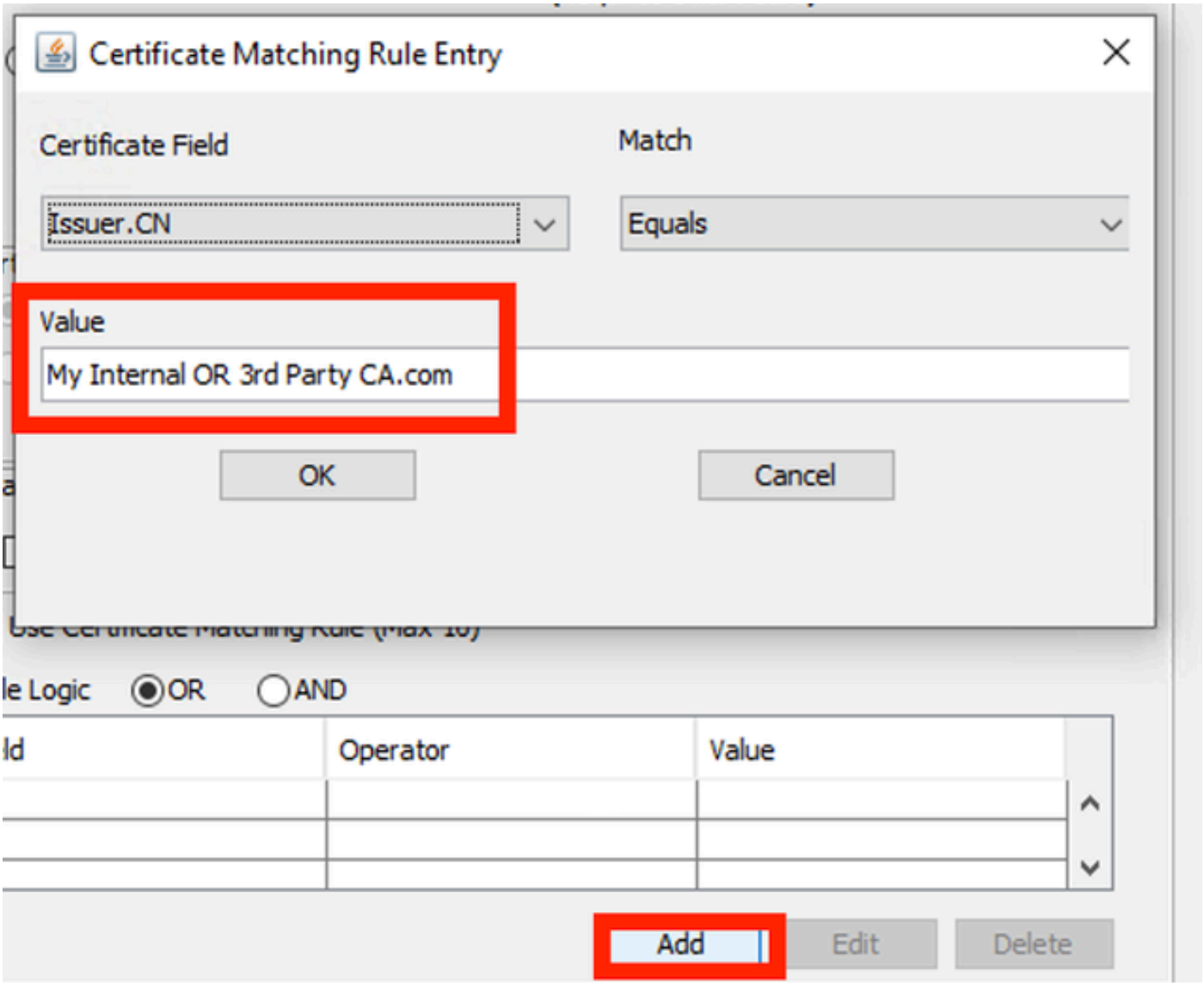
في قسم مسوغات المستخدم، ال تغير القيم الافتراضية في الجزء الأول.



قسم بيانات اعتماد مصادقة المستخدم

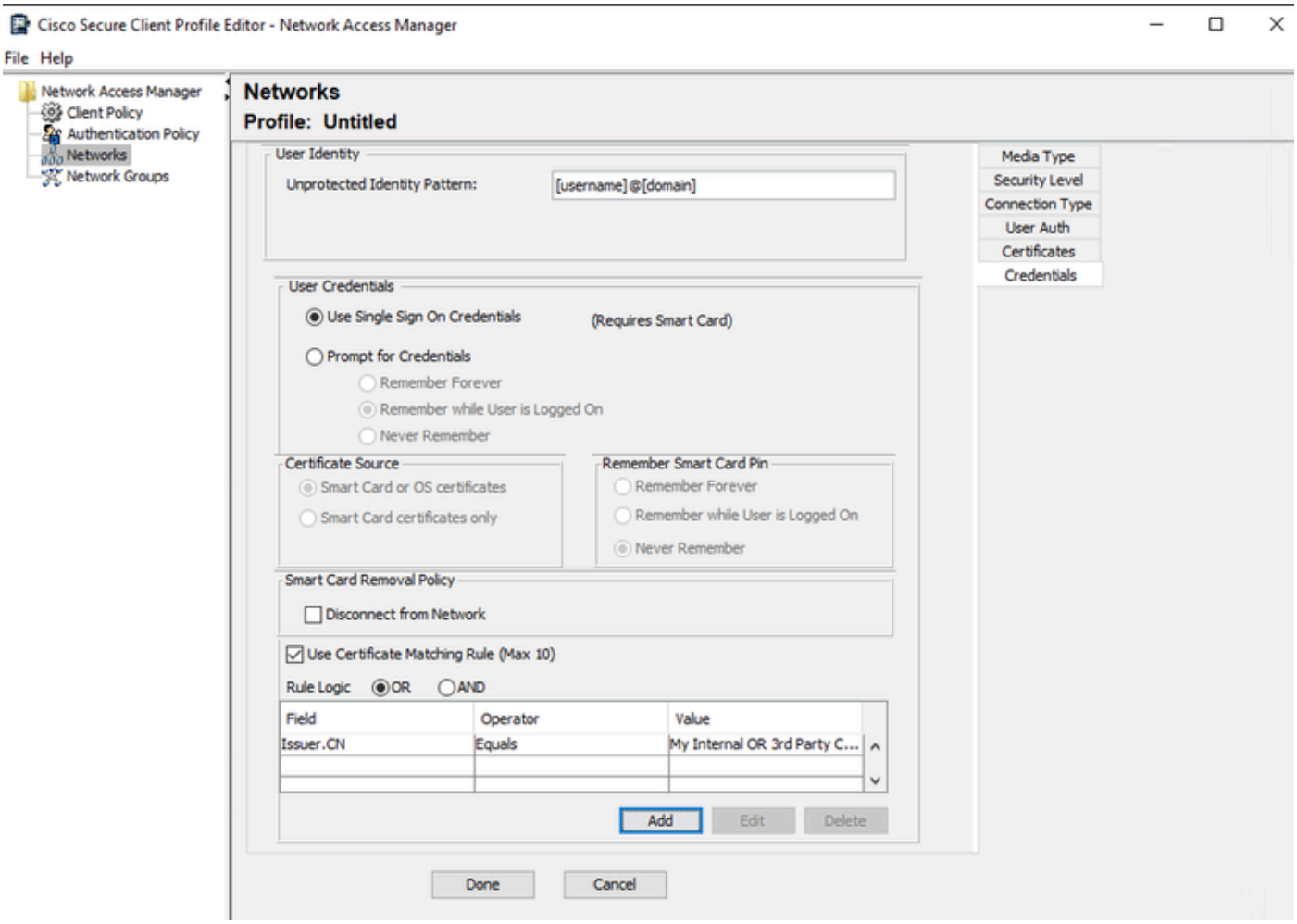
من المهم تكوين قاعدة تطابق شهادة الهوية التي يرسلها المستخدم أثناء عملية EAP TLS. للقيام بذلك، انقر فوق خانة الاختيار المجاورة لاستخدام قاعدة التحويل البرمجي للشهادات (الحد الأقصى 10).

انقر فوق إضافة (Add).



ةداهشلا ةقباطم ةدعاق ةذفان

إستبدال القيمة بسلسلة CA.com الداخلية أو الخاصة بجهة خارجية ب CN لشهادة المستخدم.



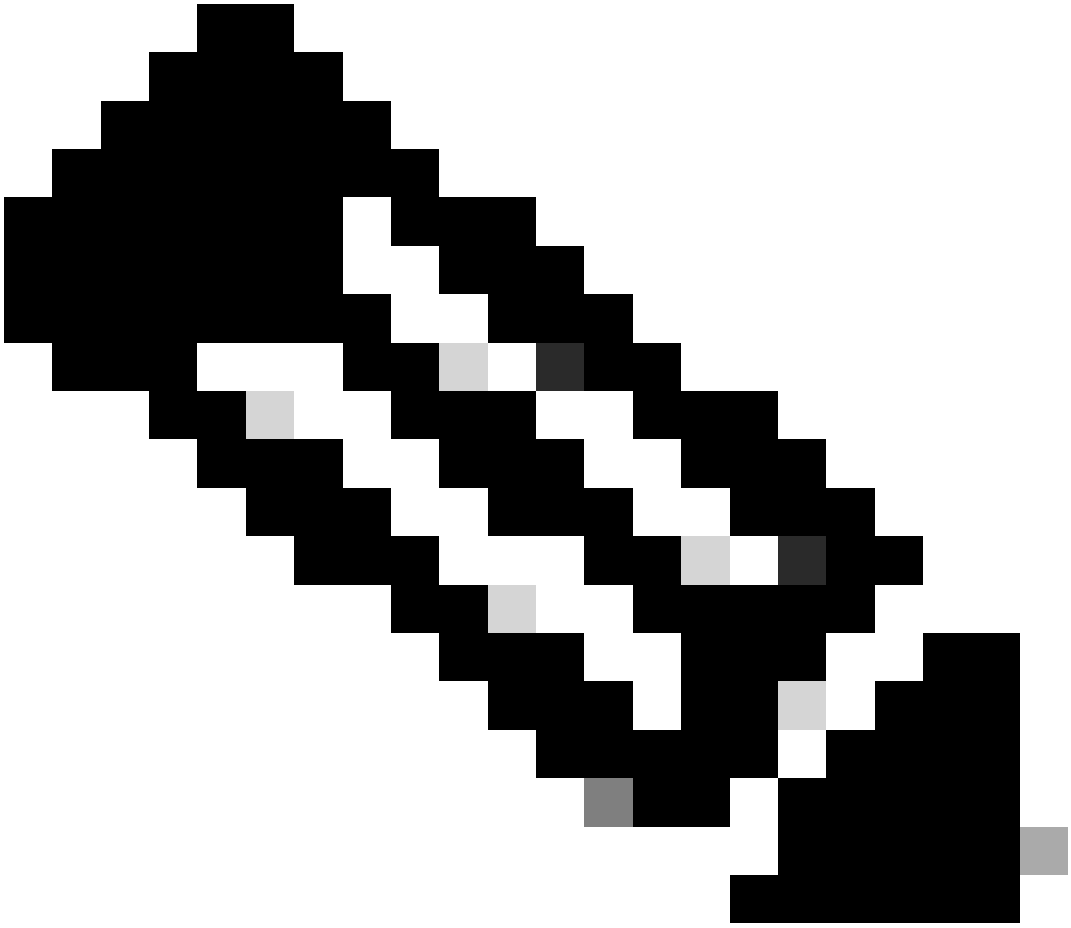
قسم بيانات اعتماد شهادة مصادقة المستخدم

انقر فوق تم لإنهاء التكوين.

حدد ملف > حفظ باسم لحفظ ملف تعريف Secure Client Network Access Manager باسم configuration.xml.

لجعل Secure Client Network Access Manager يستخدم ملف التعريف الذي تم إنشاؤه للتو، استبدل ملف configuration.xml في الدليل التالي بالدليل الجديد:

C:\ProgramData\Cisco\CiscoSecure Client\Network Access Manager\System



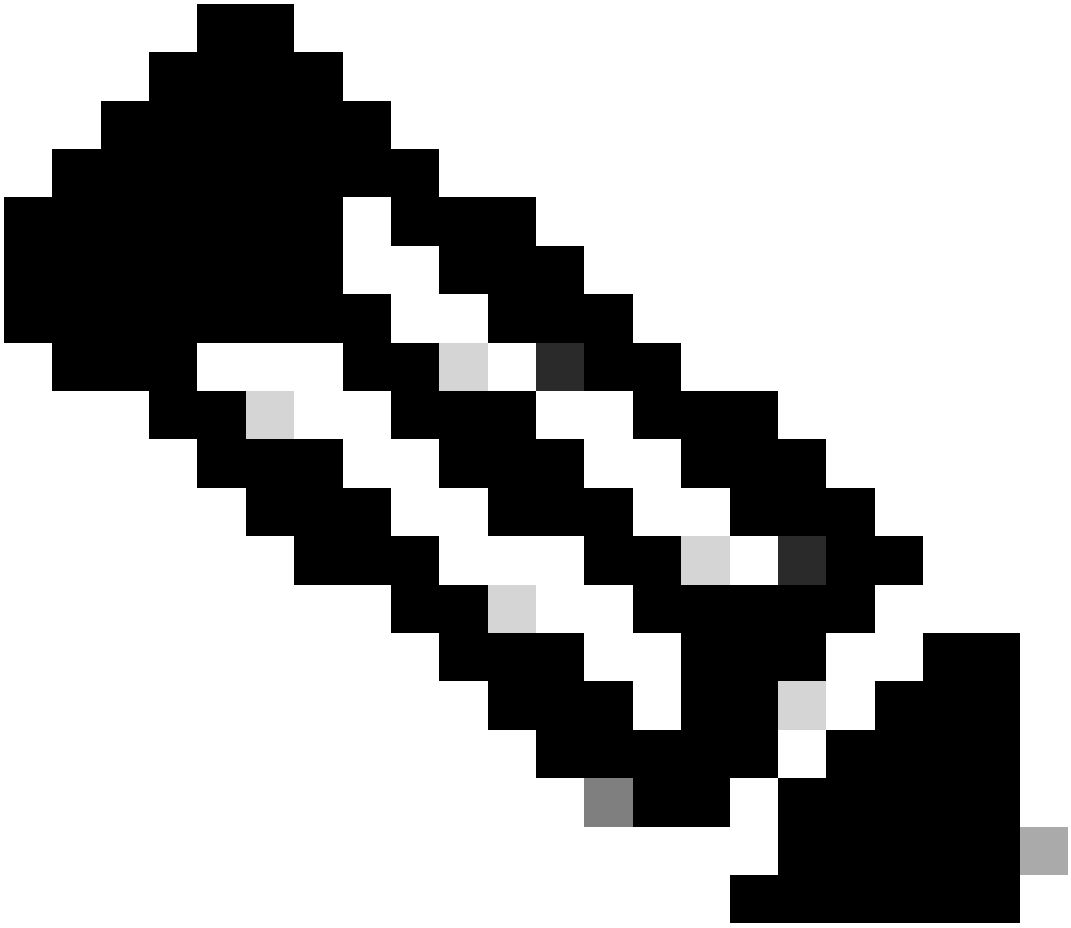
ملاحظة: يجب تسمية الملف configuration.xml، وإلا فلن يعمل.

---

7. قم بتكوين ISR 1100 و ISE للسماح بالمصادقة استنادا إلى السيناريو 1 PEAP MSCHAPv2

قم بتكوين الموجه ISR 1100 Router.

يغطي هذا القسم التكوين الأساسي الذي يجب على NAD جعله dot1x يعمل.



ملاحظة: لنشر ISE متعدد العقد، أشر إلى أي عقدة تم تمكين Policy Server Node Persona لها. يمكن التحقق من هذا بالانتقال إلى ISE في الإدارة > النظام > عامة التبويب النشر.

```
aaa new-model
aaa session-id common
!
aaa authentication dot1x default group ISE-CLUSTER
aaa authorization network default group ISE-CLUSTER
aaa accounting system default start-stop group ISE-CLUSTER
aaa accounting dot1x default start-stop group ISE-CLUSTER
!
aaa server radius dynamic-author
 client A.B.C.D server-key  <Your shared secret>
!
!
radius server  ISE-PSN-1
 address ipv4 A.B.C.D auth-port 1645 acct-port 1646
 timeout 15
 key <Your shared secret>
```

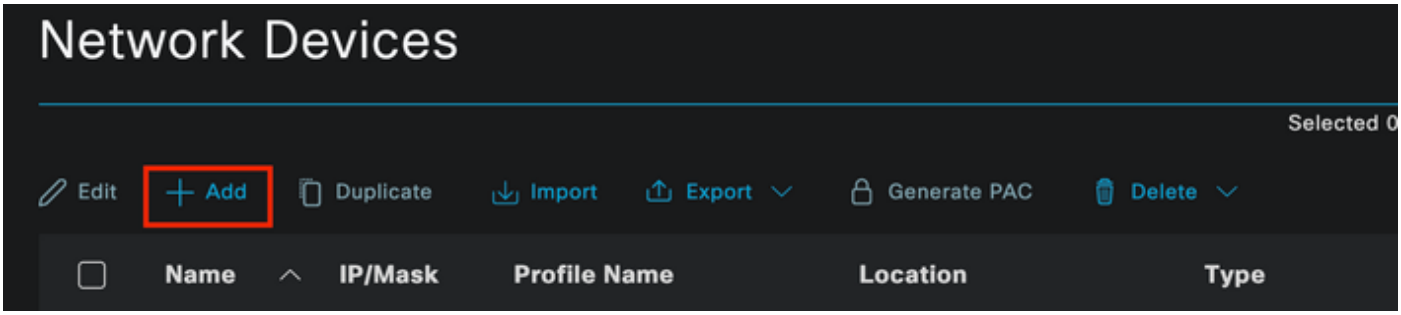
```
!
!
aaa group server radius ISE-CLUSTER
 server name ISE-PSN-1
!
interface GigabitEthernet0/1/0
 description "Endpoint that supports dot1x"
 switchport access vlan 15
 switchport mode access
 authentication host-mode multi-auth
 authentication order dot1x mab
 authentication priority dot1x mab
 authentication port-control auto
 dot1x pae authenticator
 spanning-tree portfast
```

تكوين Identity Service Engine 3.2.

قم بتكوين جهاز الشبكة.

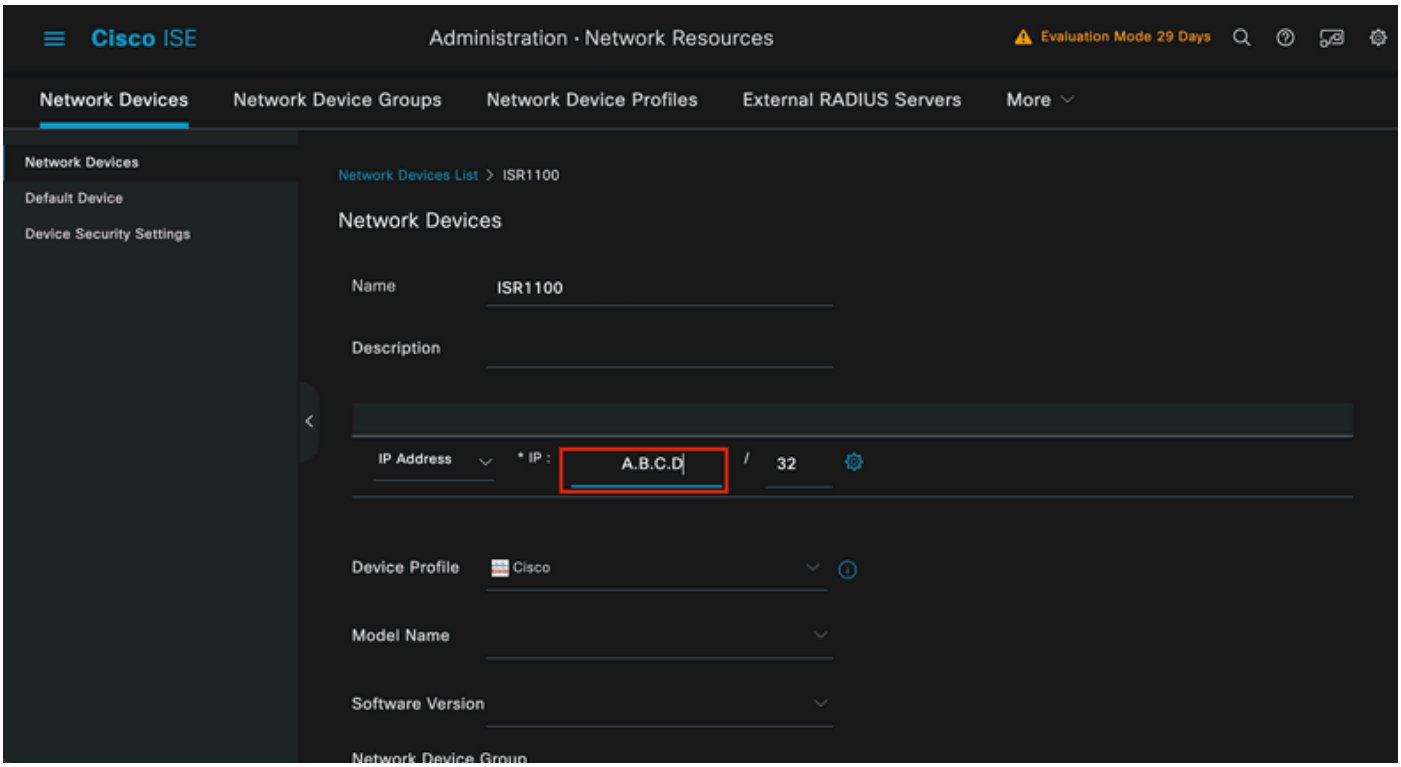
أضف ISR NAD إلى إدارة ISE > موارد الشبكة > أجهزة الشبكة.

انقر فوق إضافة (Add).



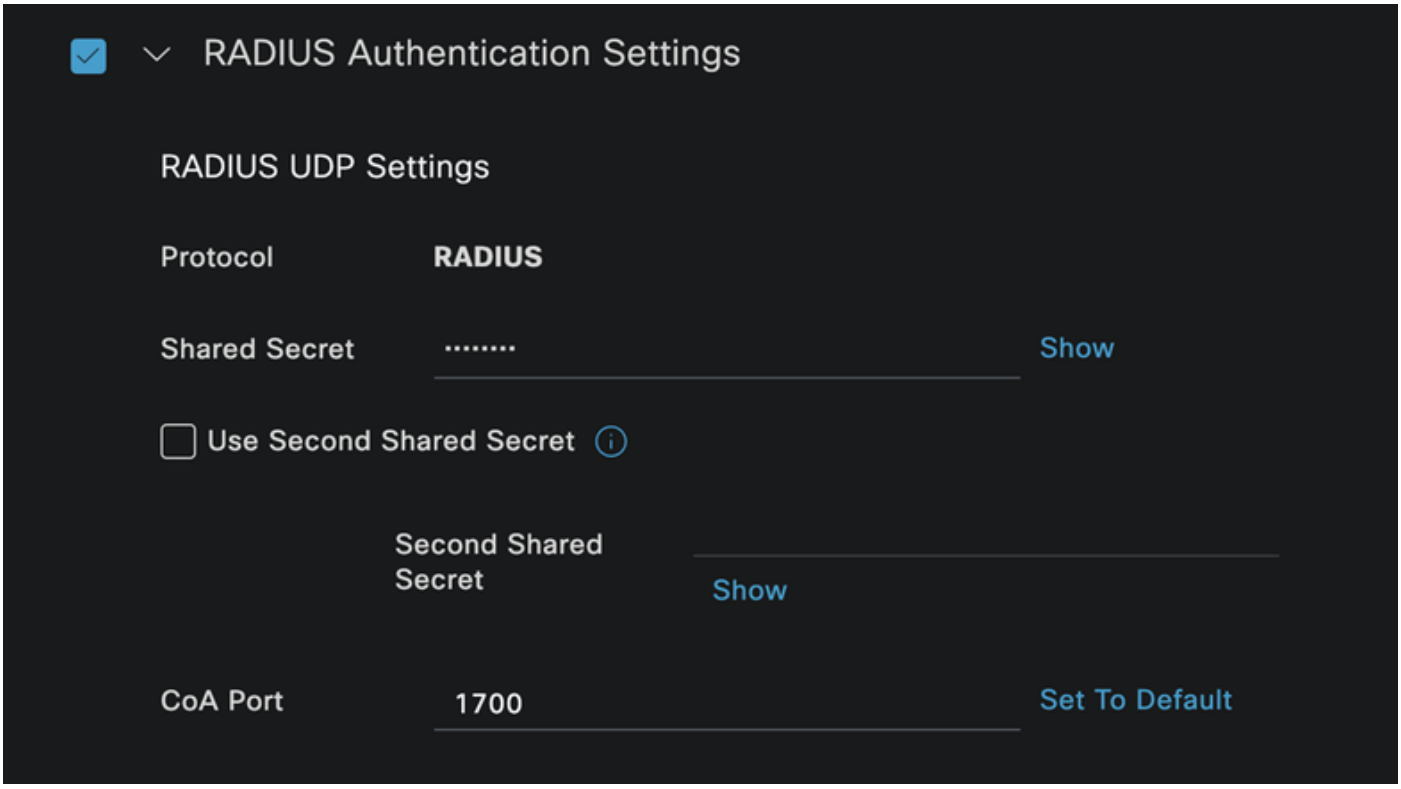
قسم جهاز الشبكة

قم بتعيين اسم إلى NAD الذي تقوم بإنشائه. إضافة IP لجهاز الشبكة.



إنشاء جهاز الشبكة

في أسفل نفس الصفحة أضف نفس السر المشترك الذي أستخدمته في تكوين جهاز الشبكة.



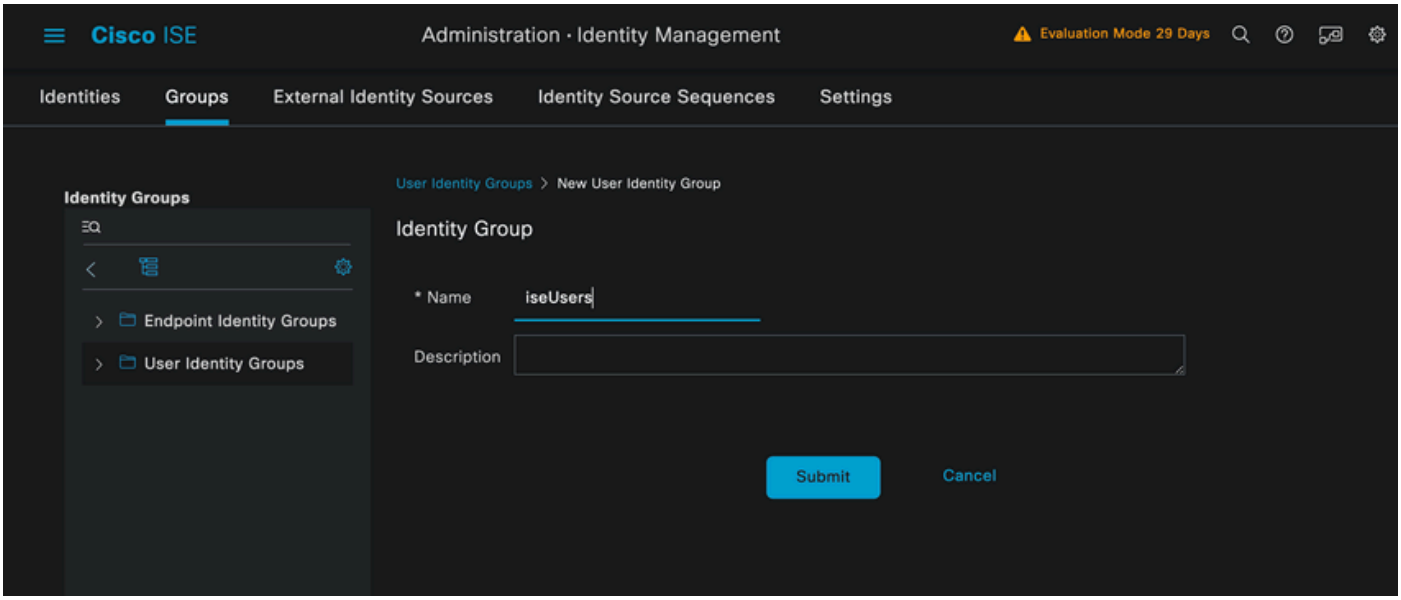
إعدادات *RADIUS* لجهاز الشبكة

قم بحفظ التغييرات.

قم بتكوين الهوية التي يتم إستخدامها لمصادقة نقطة النهاية.

يتم إستخدام مصادقة ISE المحلية. ال يتم شرح مصادقة ISE الخارجية في هذه المقالة.

انتقل إلى علامة التبويب إدارة > إدارة الهوية > مجموعات" وقم بإنشاء المجموعة التي يعد المستخدم جزءا منها. مجموعة الهوية التي تم إنشاؤها لهذا العرض التوضيحي هي ISEusers.

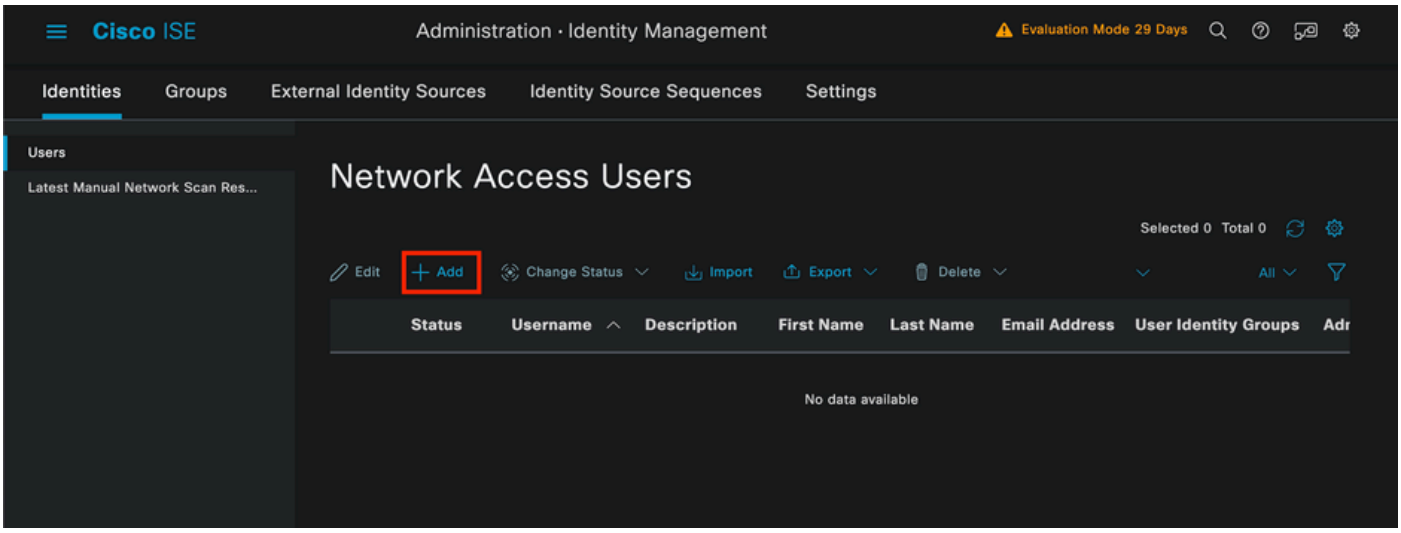


إنشاء مجموعة الهوية

انقر فوق إرسال.

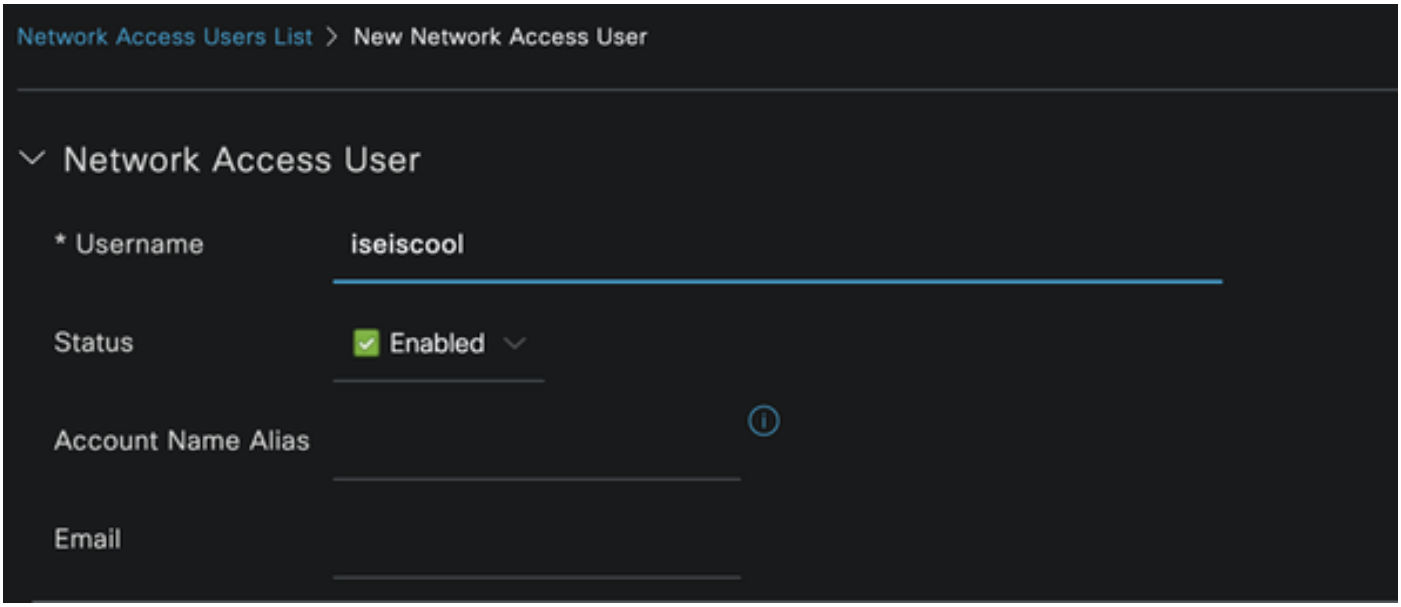
انتقل إلى الإدارة > إدارة الهوية > تبويب الهوية.

انقر فوق إضافة (Add).



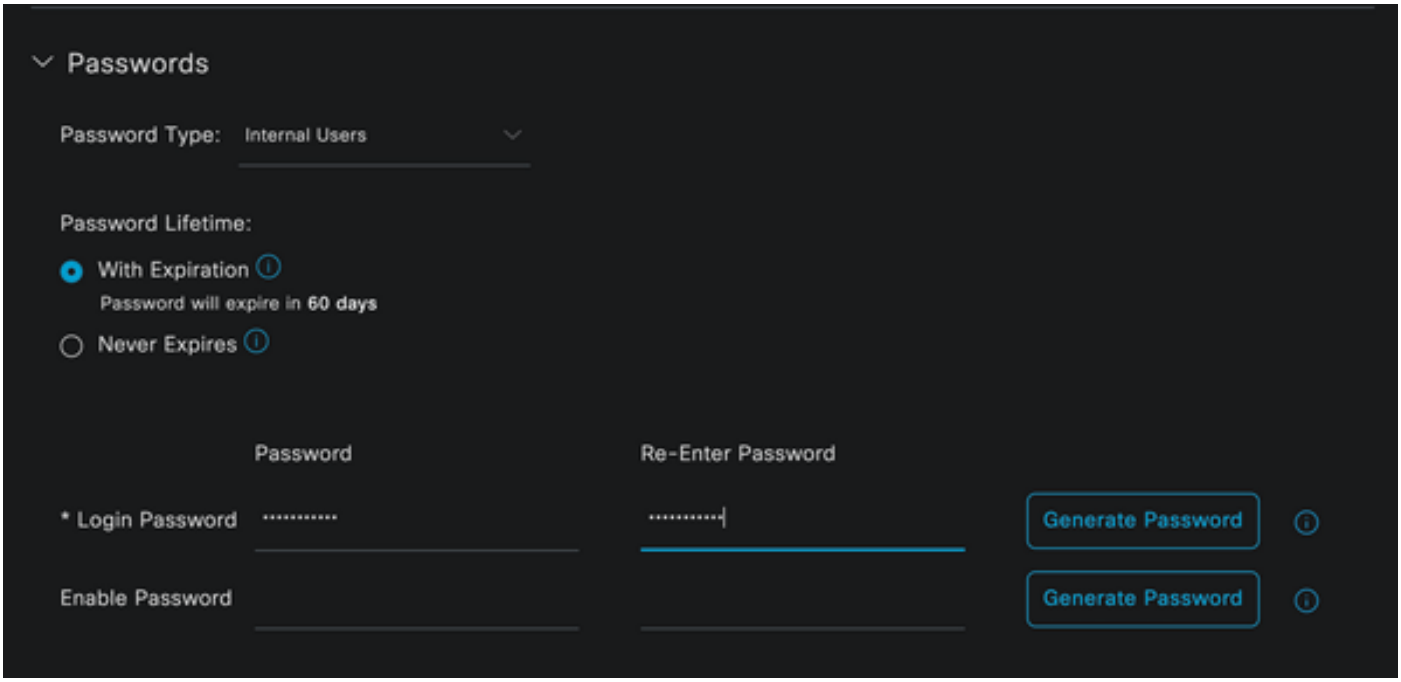
قسم مستخدمي الوصول إلى الشبكة

كجزء من الحقول الإلزامية، يدأ باسم المستخدم. يتم إستخدام اسم المستخدم iseiscool في هذا المثال.



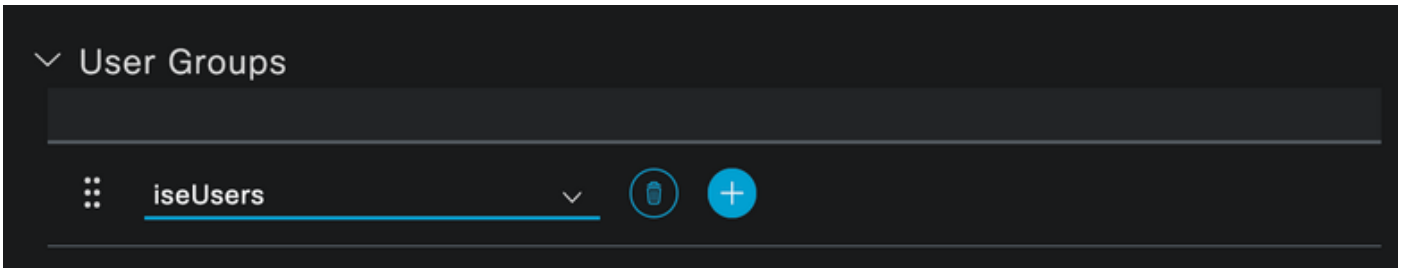
إنشاء مستخدم الوصول إلى الشبكة

قم بتعيين كلمة مرور للمستخدم. يتم إستخدام VainillaISE97.



قسم كلمة مرور إنشاء المستخدم

قم بتعيين المستخدم إلى مجموعة IseUsers.

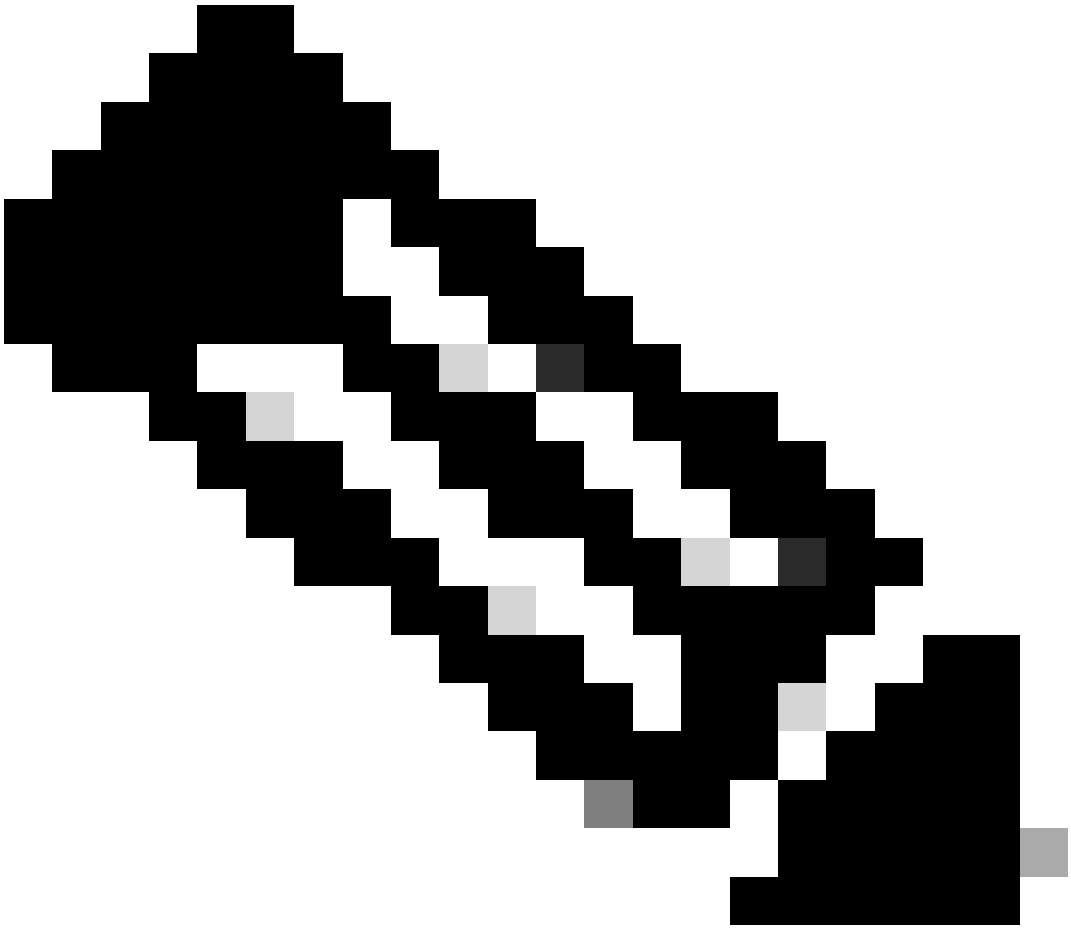


تعيين مجموعة المستخدمين

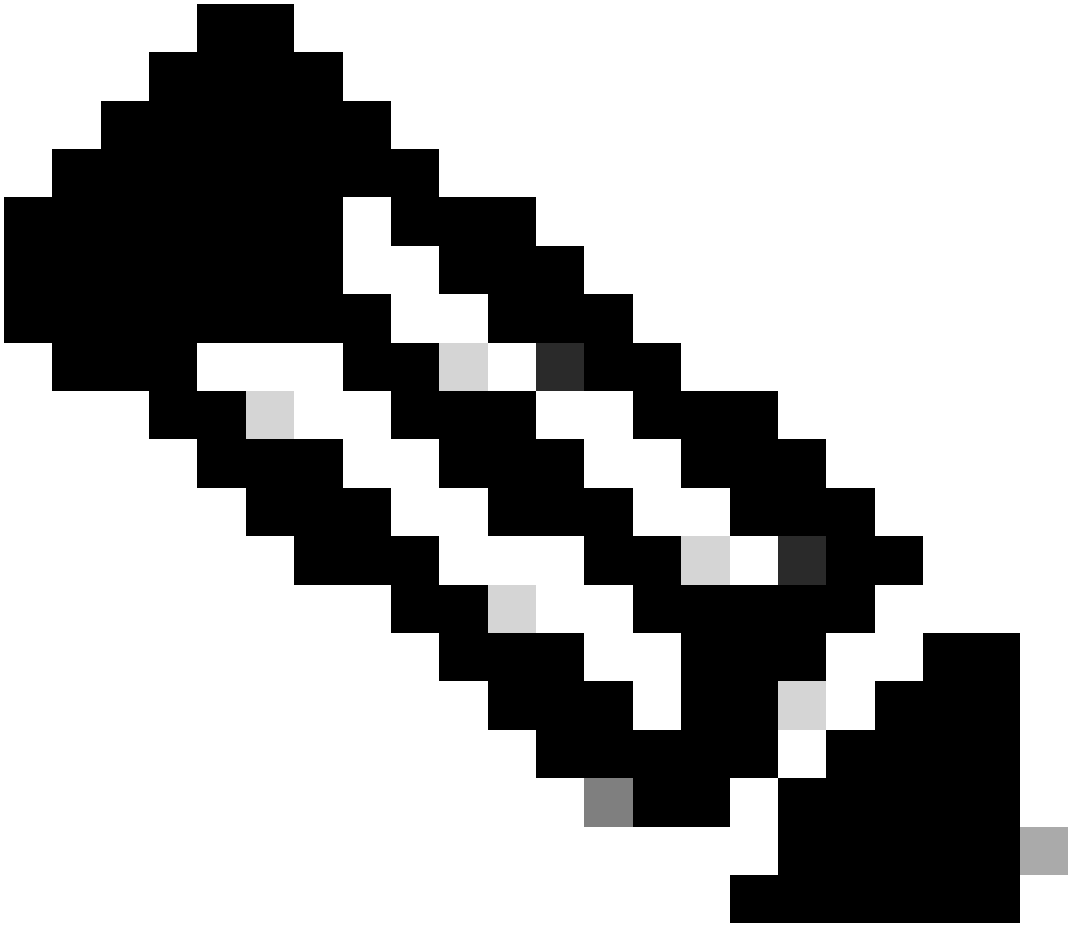
قم بتكوين مجموعة النهج.

انتقل إلى قائمة ISE > السياسة > مجموعات السياسات.

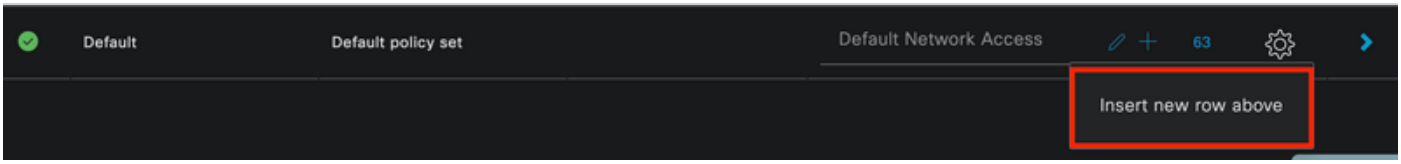
يمكن إستخدام مجموعة النهج الافتراضية. ومع ذلك، يتم إنشاء واحد يسمى Wired لهذا المثال.



ملاحظة: تساعد عملية تصنيف مجموعات السياسات وتمييزها عند أستكشاف الأخطاء وإصلاحها،

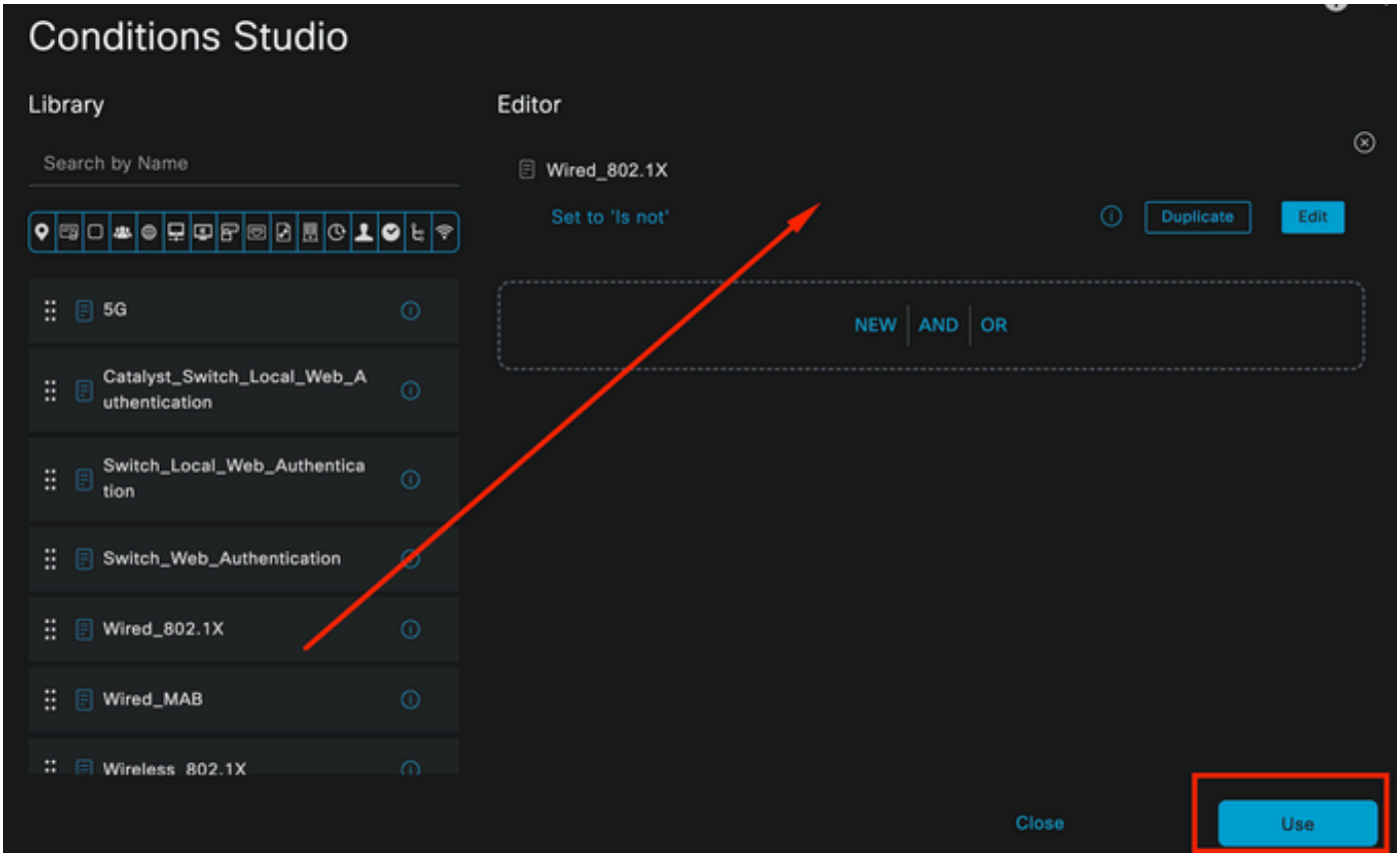


ملاحظة: إذا لم تكن أيقونة إضافة أو زائد مرئية، يمكن نقر أيقونة العتاد لأي مجموعة نهج، ثم حدد إدراج صف جديد أعلاه.



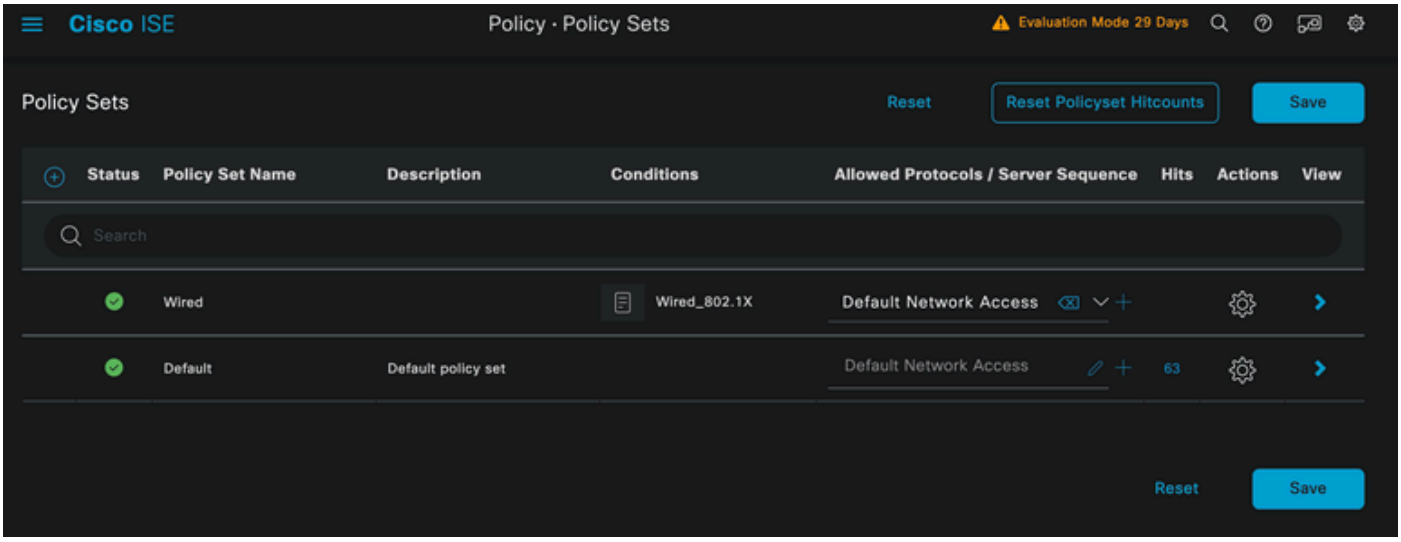
خيارات أيقونة الترس

الشرط المستخدم هو Wired 8021x. اسحبه ثم انقر فوق إستخدام.



أستوديو شروط سياسة المصادقة

حدد الوصول الافتراضي للشبكة في قسم البروتوكولات المسموح بها.

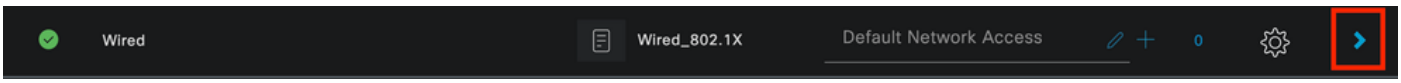


طريقة عرض عامة لمجموعات النهج

انقر فوق حفظ.

2.د. قم بتكوين سياسات المصادقة والتفويض.

انقر فوق أيقونة >.



مجموعة السياسات السلكية

قم بتوسيع قسم نهج المصادقة.

انقر على أيقونة +.

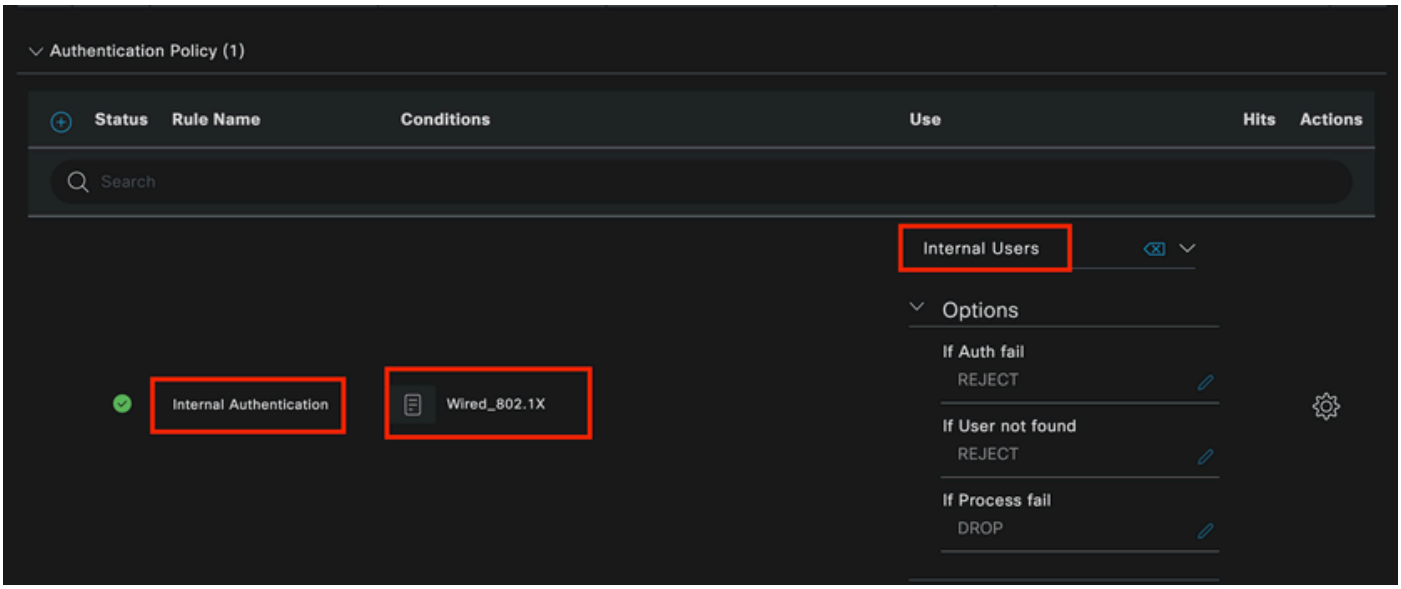
نهج المصادقة

قم بتعيين اسم لنهج المصادقة. يتم إستخدام المصادقة الداخلية في هذا المثال.

انقر فوق أيقونة + في عمود الشروط لنهج المصادقة الجديد هذا.

يتم إستخدام الشرط Wired Dot1x الذي تم تكوينه مسبقا.

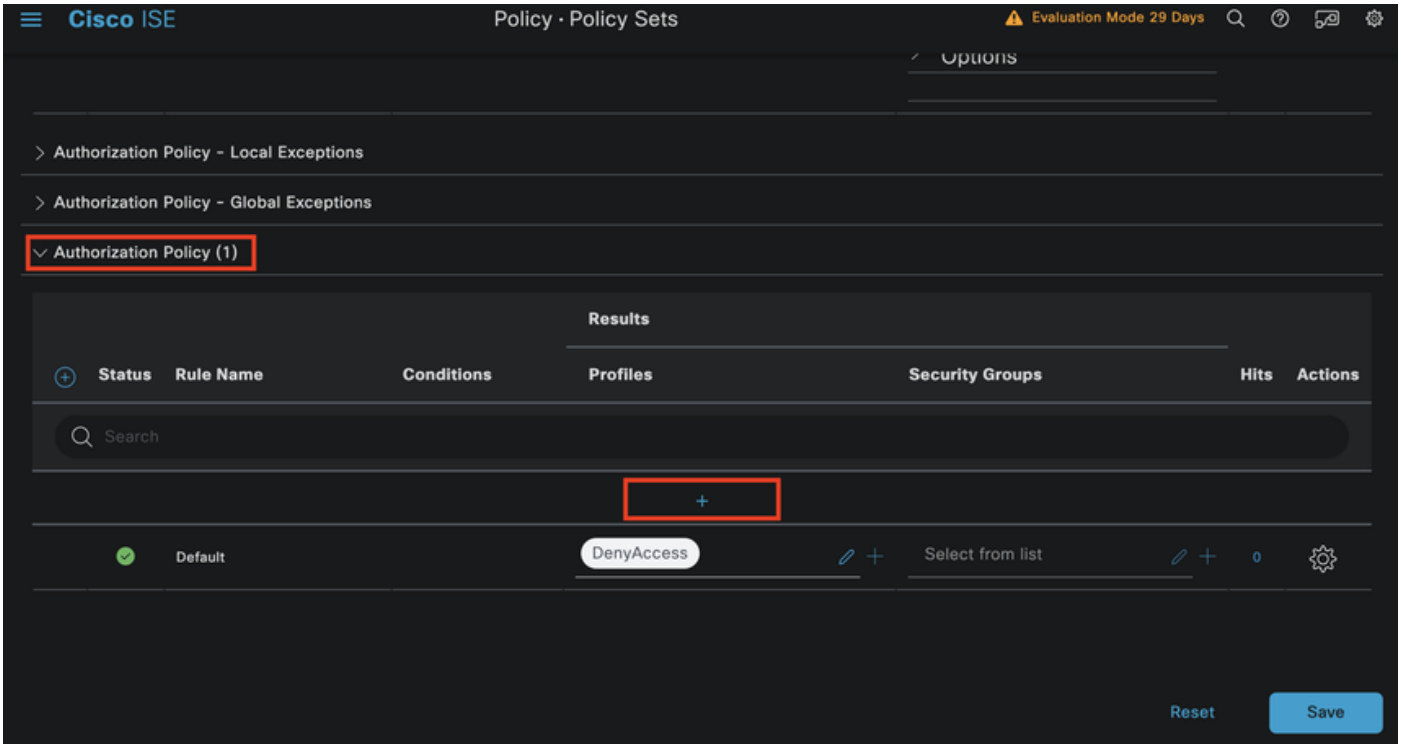
أخيرا، في عمود إستخدام حدد المستخدمين الداخليين.



نهج المصادقة

نهج التخويل.

يقع قسم نهج التخويل في أسفل الصفحة. قم بتمديده وانقر فوق أيقونة +.



سياسة التخويل

قم بتسمية نهج التفويض الذي تم إنشاؤه مؤخرا. في مثال التكوين هذا، يتم إستخدام اسم مستخدمي ISE الداخليين.

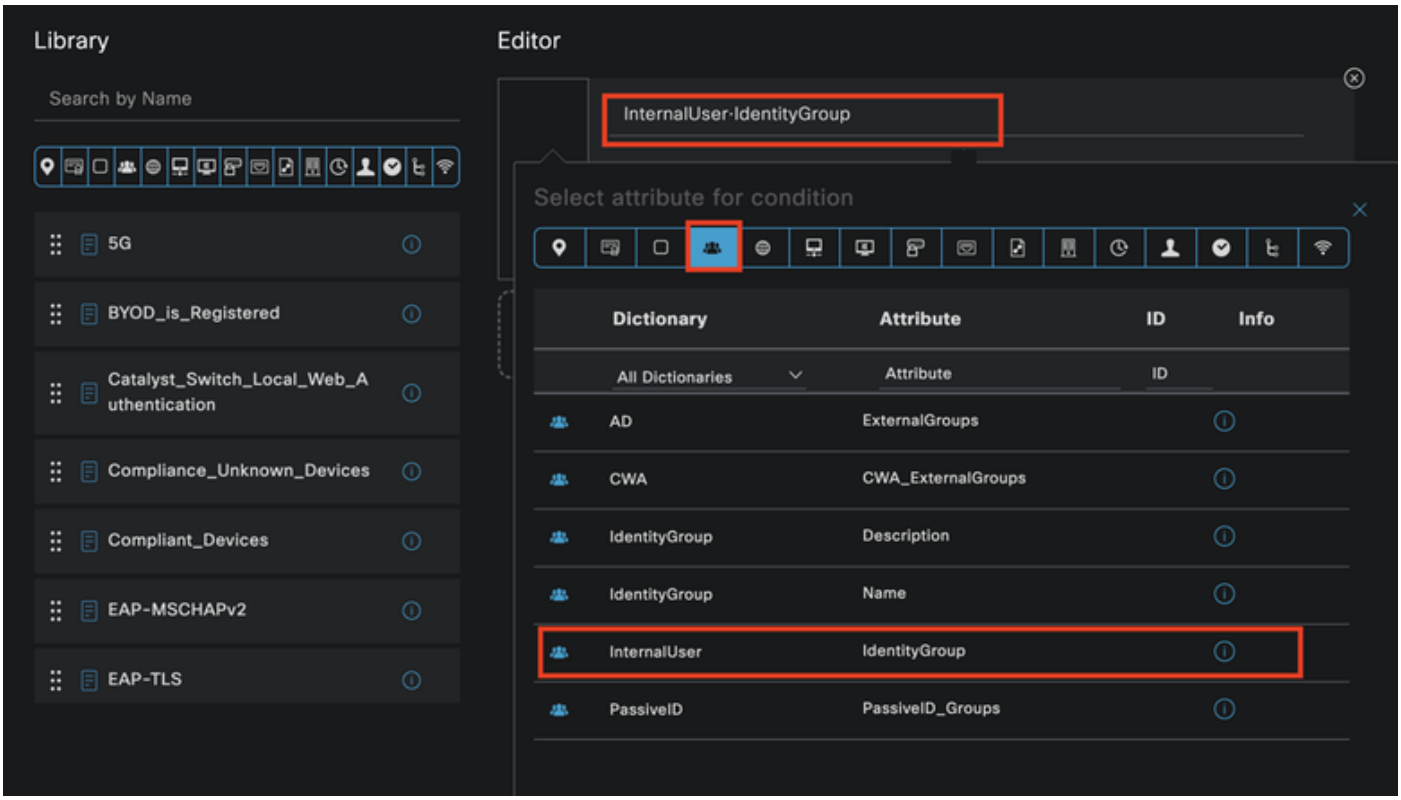
لإنشاء شرط لنهج التخويل هذا، انقر فوق أيقونة + في العمود شروط.

يتم إستخدام المجموعة IseUsers.

انقر فوق قسم السمة.

حدد أيقونة IdentityGroup.

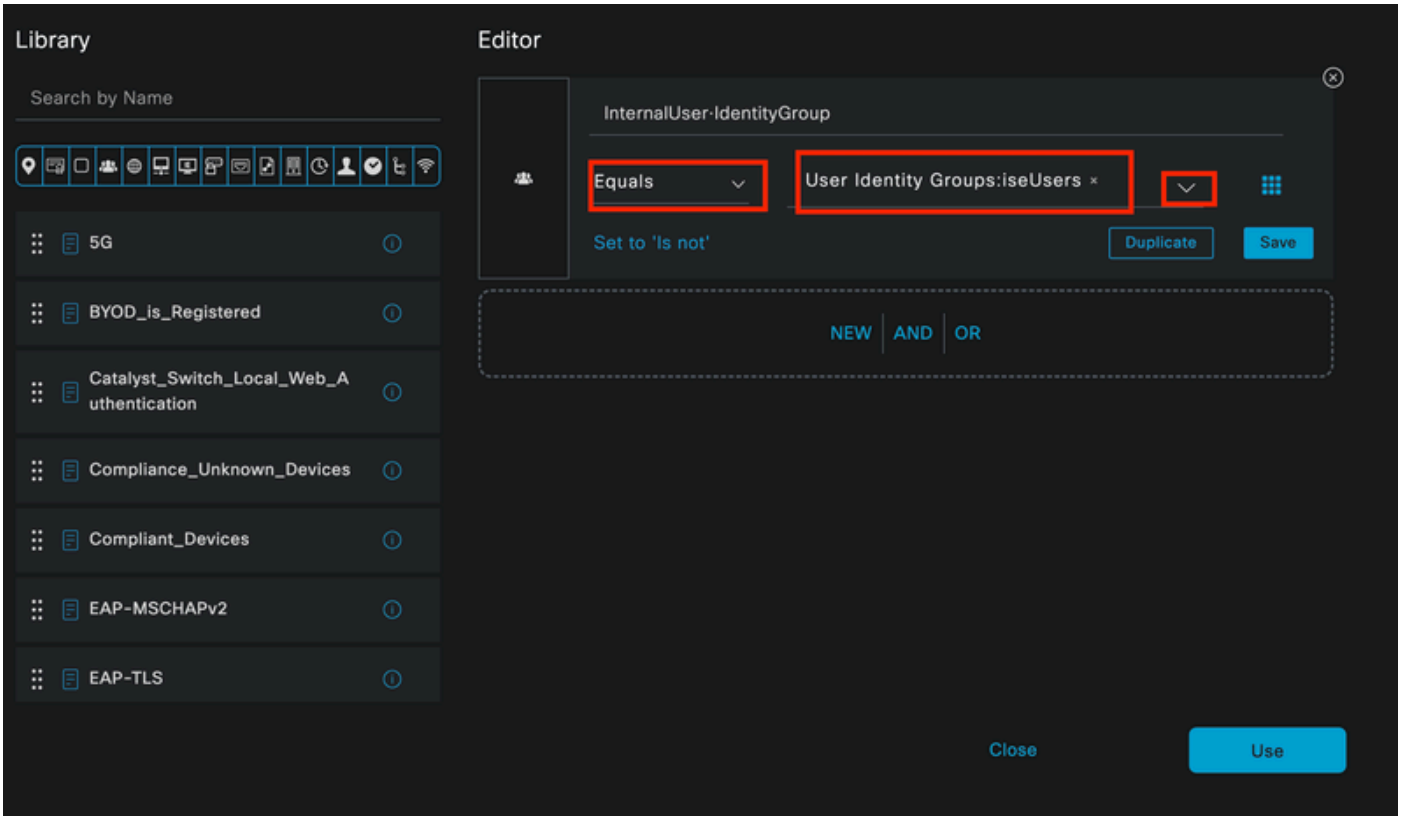
من القاموس حدد قاموس InternalUser الذي يأتي مع سمة IdentityGroup.



إنشاء الشرط

حدد المشغل يساوي.

من مجموعات هوية المستخدم، حدد IseUsers للمجموعة.

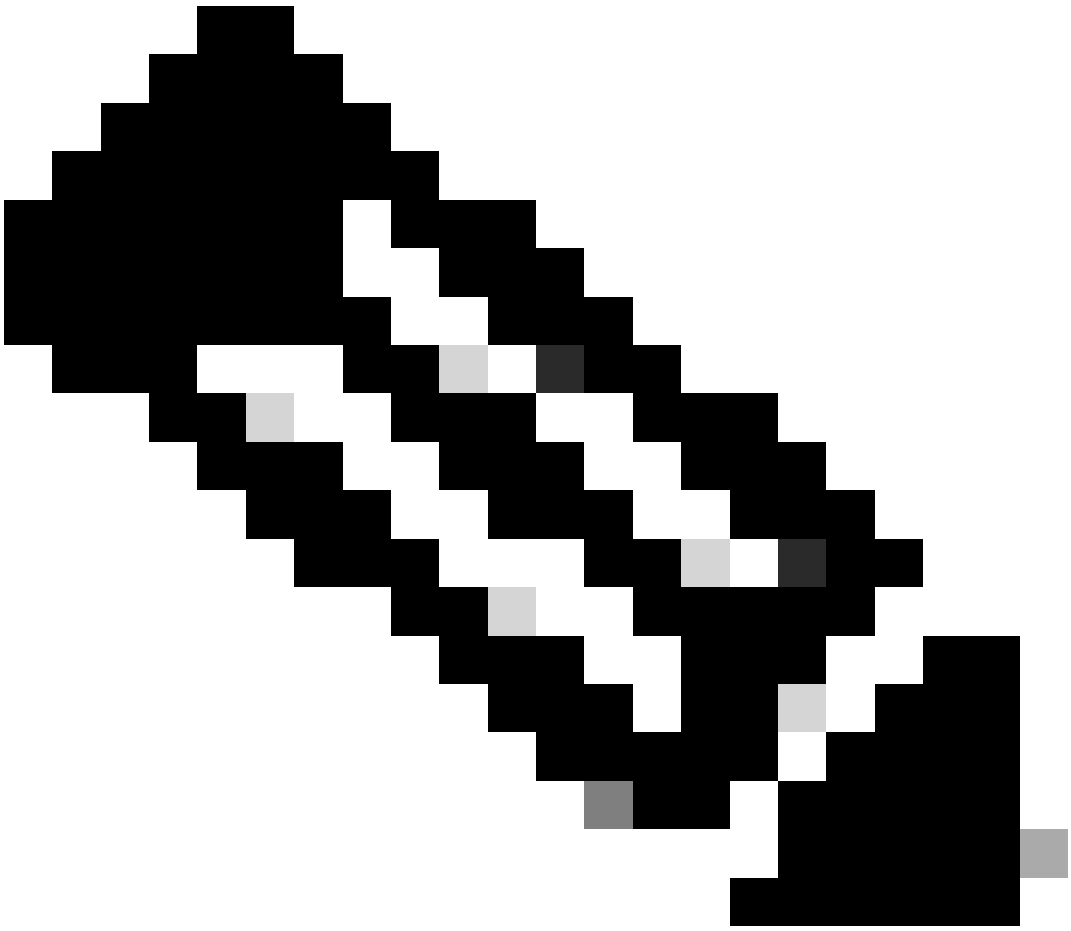


إنشاء الشرط

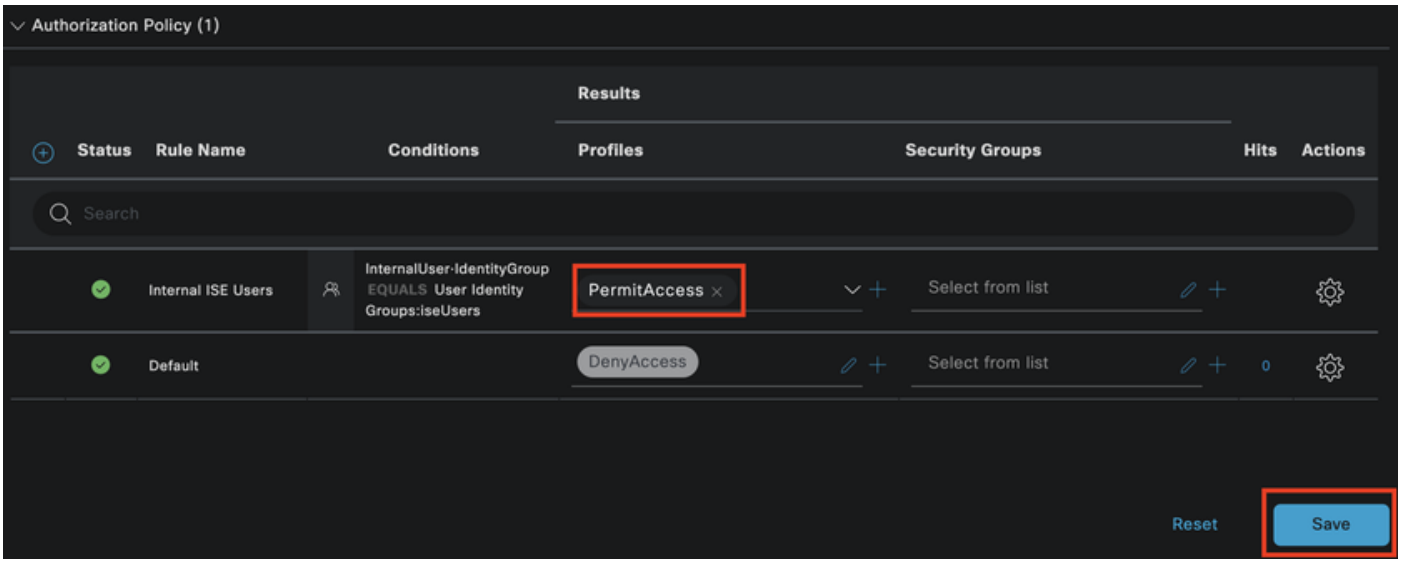
طقطقة إستعمال.

إضافة ملف تعريف تخويل النتيجة.

يتم إستخدام تصريح الوصول إلى ملف التعريف الذي تم تكوينه مسبقا.



ملاحظة: الرجاء ملاحظة أن عمليات المصادقة الواردة إلى ISE التي تؤثر على مجموعة النهج Wired Dot1x هذه التي ليست جزءا من ISEUsers لمجموعة هوية المستخدمين، تصل إلى نهج التخويل الافتراضي، والذي ينتج عنه DenyAccess.



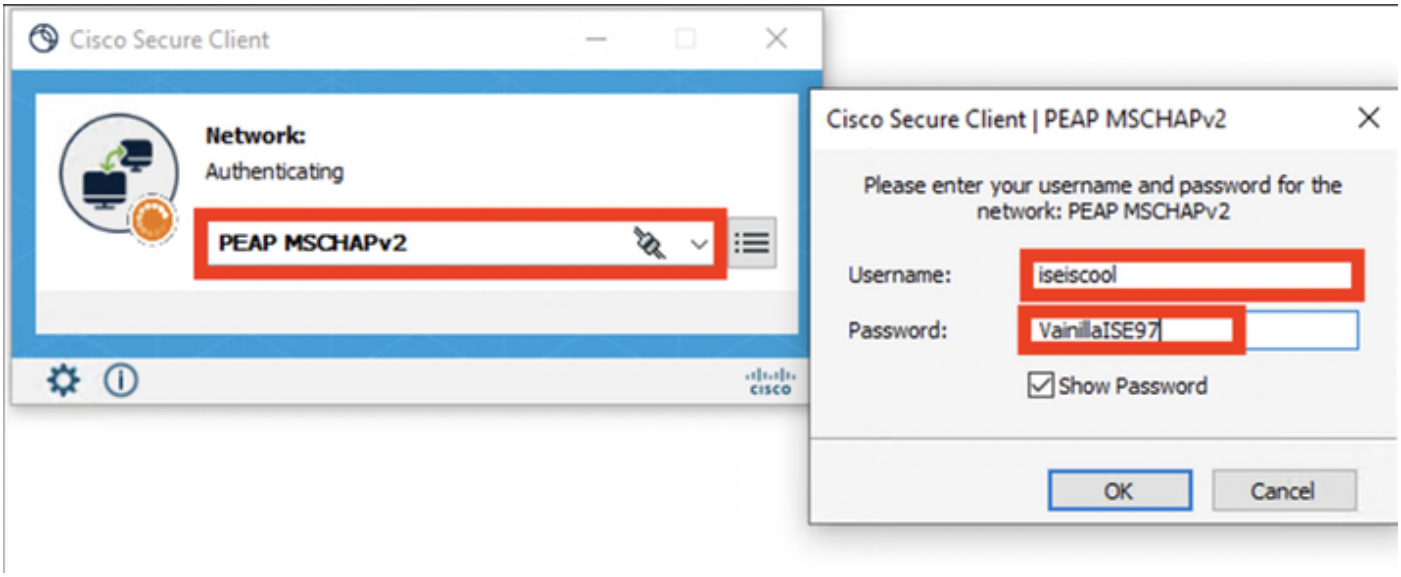
سياسة التخويل

انقر فوق حفظ.

التحقق من الصحة

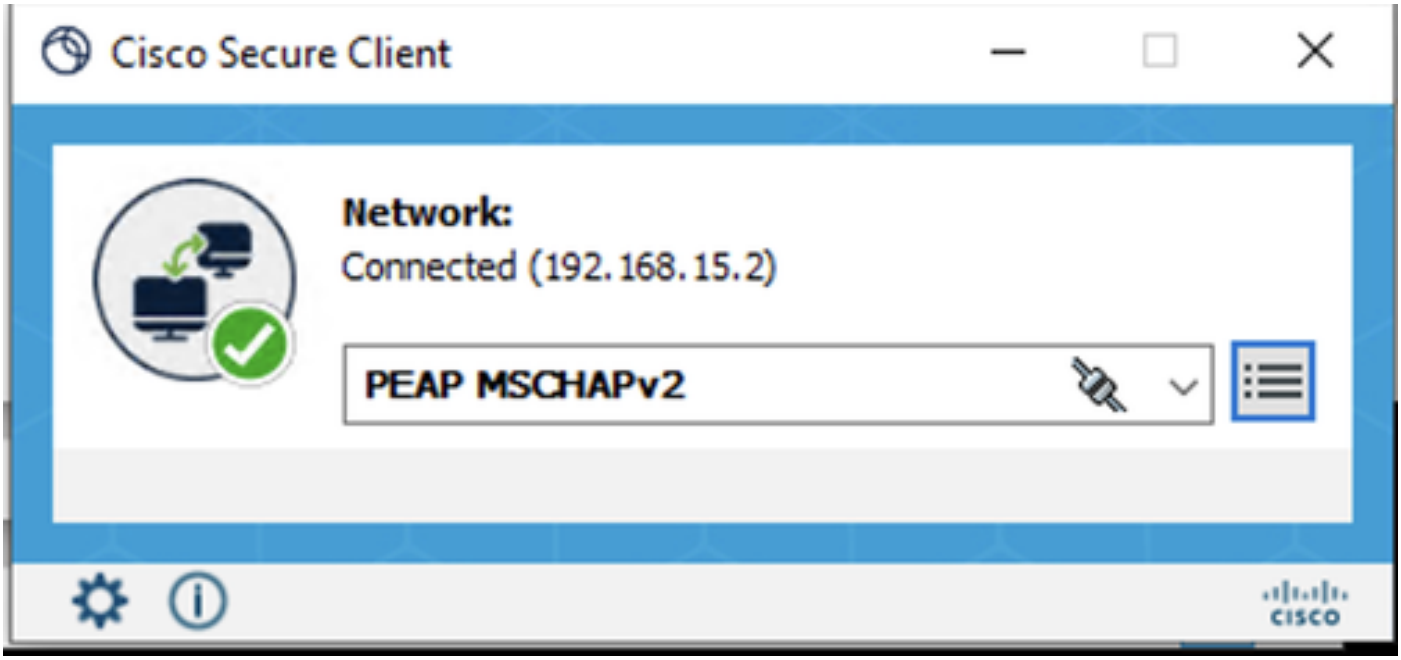
يطلب العميل الآمن فور انتهاء التكوين بيانات الاعتماد، ويحدد إستخدام ملف تعريف PEAP MSCHAPv2.

يتم إدخال بيانات الاعتماد التي تم إنشاؤها مسبقا.



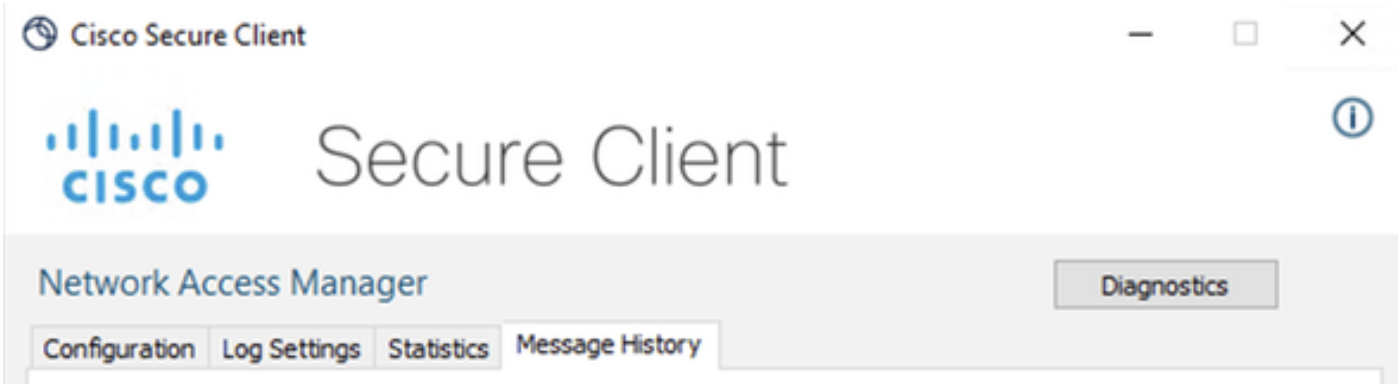
Secure Client NAM

إذا تمت مصادقة نقطة النهاية بشكل صحيح، تظهر NAM أنها متصلة.

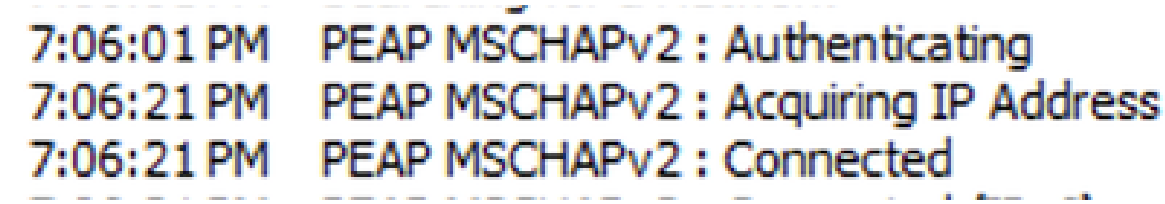


Secure Client NAM

بالنقر فوق رمز المعلومات والتنقل إلى قسم محفوظات الرسائل، يتم عرض تفاصيل كل خطوة قامت بها NAM.



تأمين محفوظات رسائل العميل



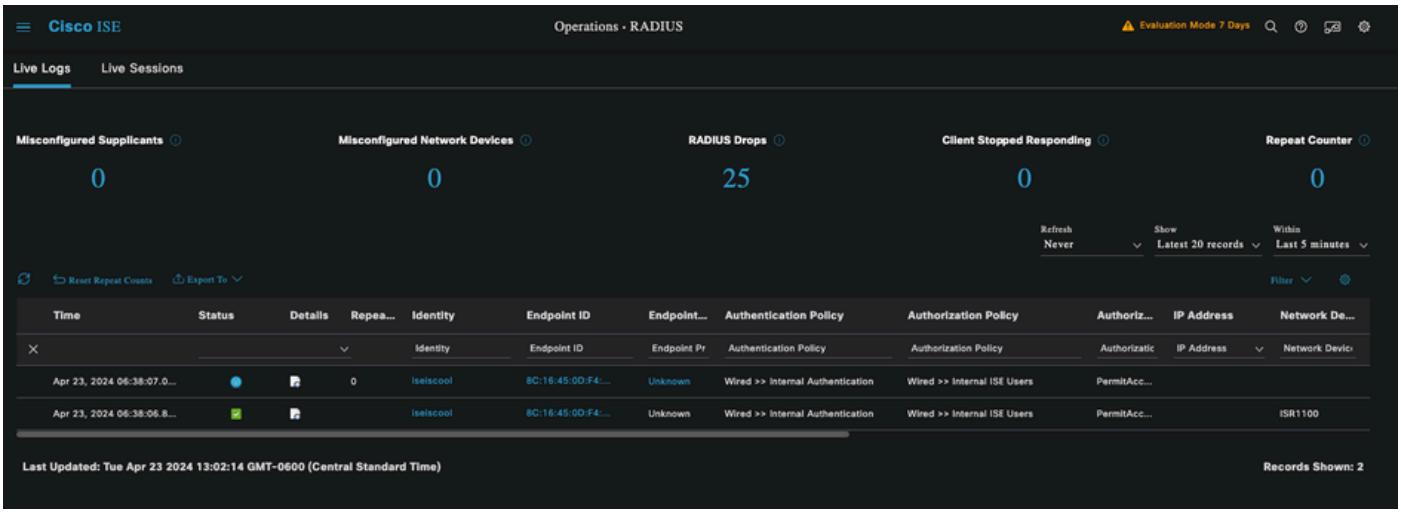
تأمين محفوظات رسائل العميل

من ISE انتقل إلى العمليات > Radius LiveLog للاطلاع على تفاصيل المصادقة. كما هو موضح في الصورة التالية، يتم عرض اسم المستخدم الذي تم إستخدامه.

تفاصيل أخرى مثل:

- الطابع الزمني.
- عنوان MAC.
- مجموعة النهج المستخدمة.
- نهج المصادقة.

- نهج التخويل.
- معلومات أخرى ذات صلة.



سجلات *ISE RADIUS Live*

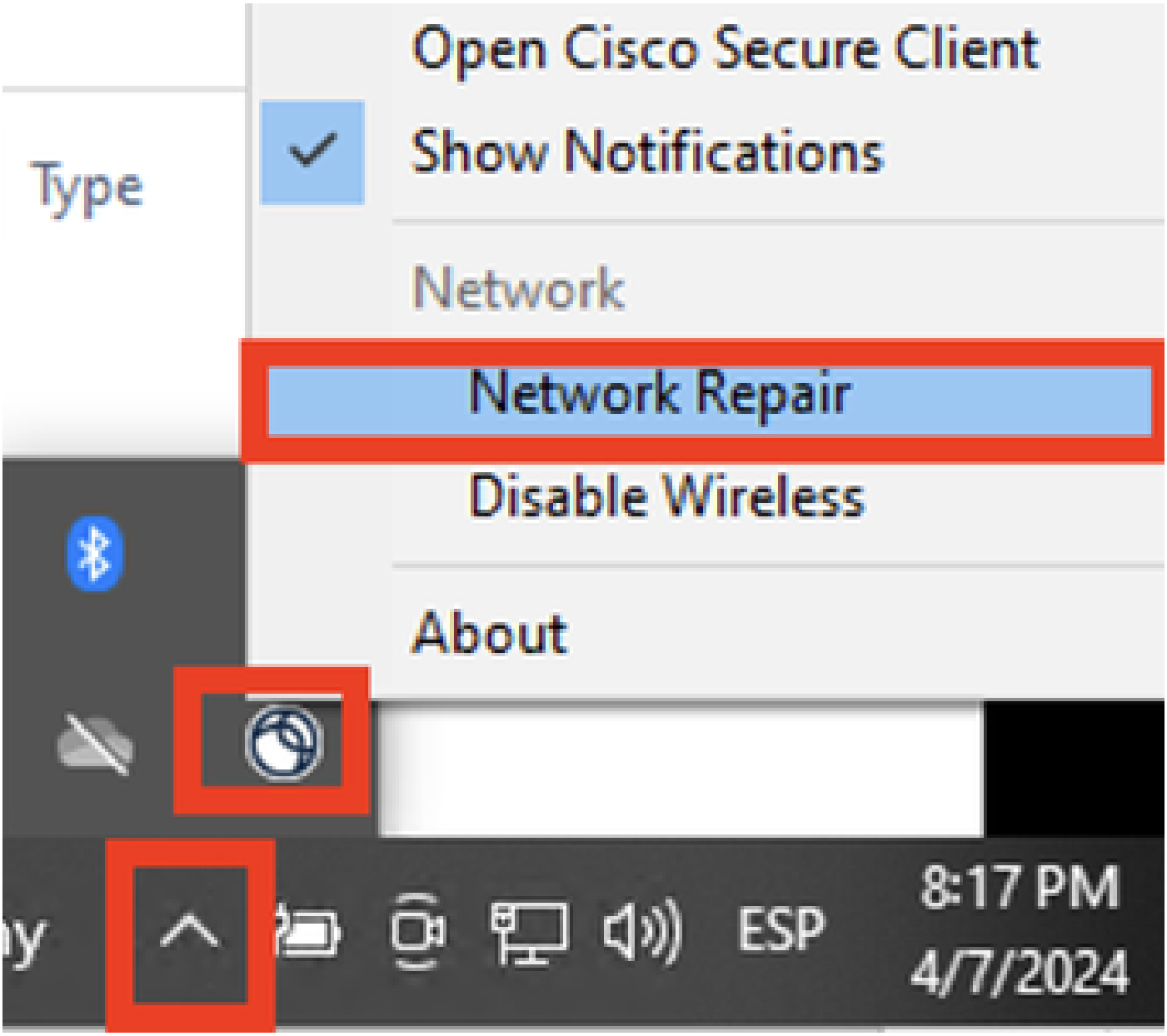
ونظرا لأنك ترى أنها تحقق السياسات الصحيحة، والنتيجة هي حالة مصادقة ناجحة، فإنها تستنتج أن التكوين صحيح.

استكشاف الأخطاء وإصلاحها

المشكلة: لا يستخدم العميل الآمن ملف تعريف NAM.

إذا لم تستخدم NAM التوصيف الجديد الذي تم إنشاؤه في محرر ملف التعريف، فاستخدم خيار إصلاح الشبكة لعميل آمن.

يمكنك العثور على هذا الخيار من خلال التنقل إلى شريط Windows > النقر فوق رمز Circumflex > النقر بزر الماوس الأيمن فوق رمز "العميل الآمن" > انقر فوق "إصلاح الشبكة".



قسم إصلاح الشبكة

المشكلة 2: يجب تجميع السجلات لمزيد من التحليل.

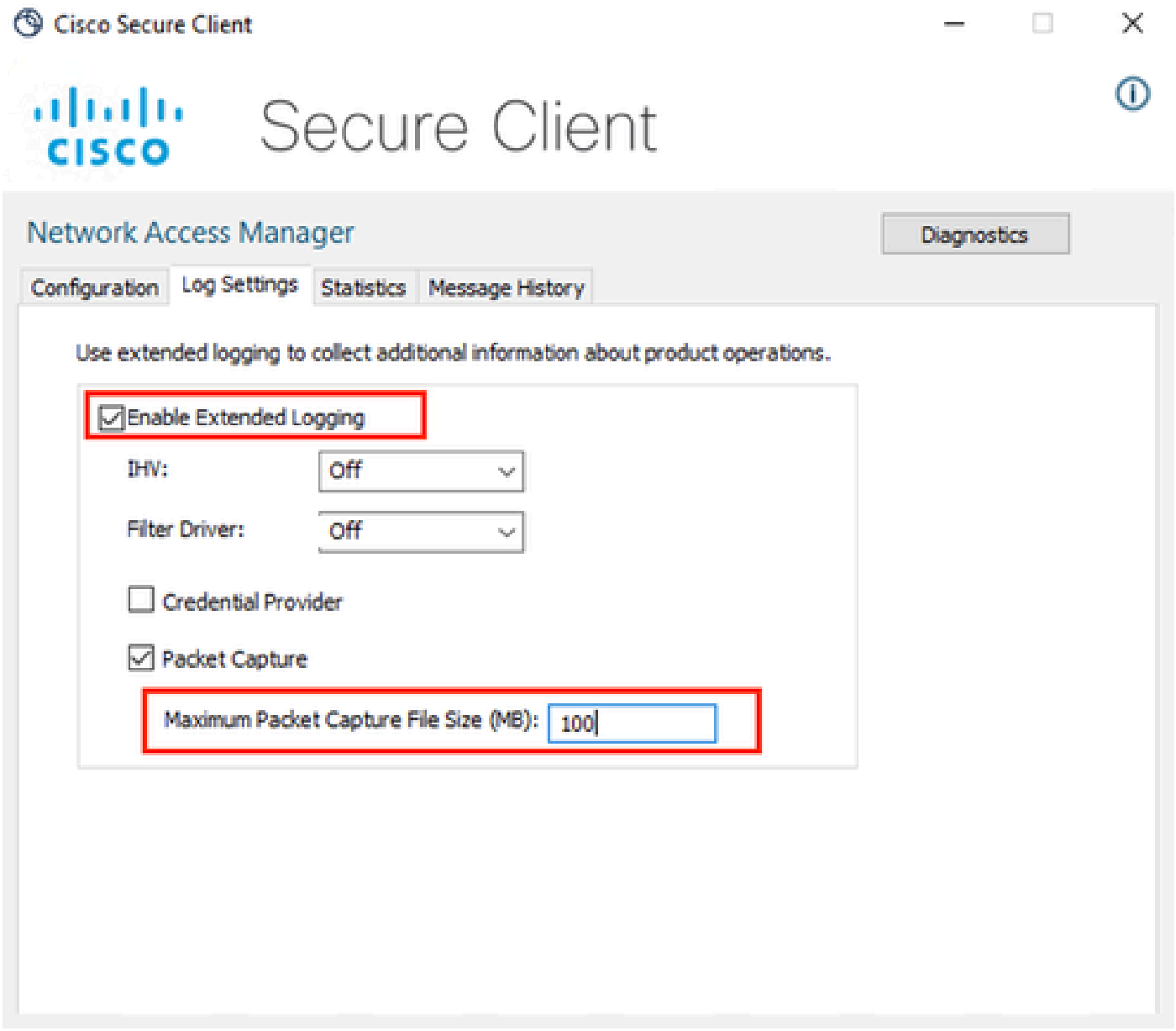
1. تمكين تسجيل NAM الموسع

افتح NAM، وانقر أيقونة الترس.

واجهة NAM

انتقل إلى علامة التبويب إعدادات السجل. حدد خانة الاختيار تمكين التسجيل الموسع.

قم بتعيين حجم ملف التقاط الحزمة على 100 ميجابت.



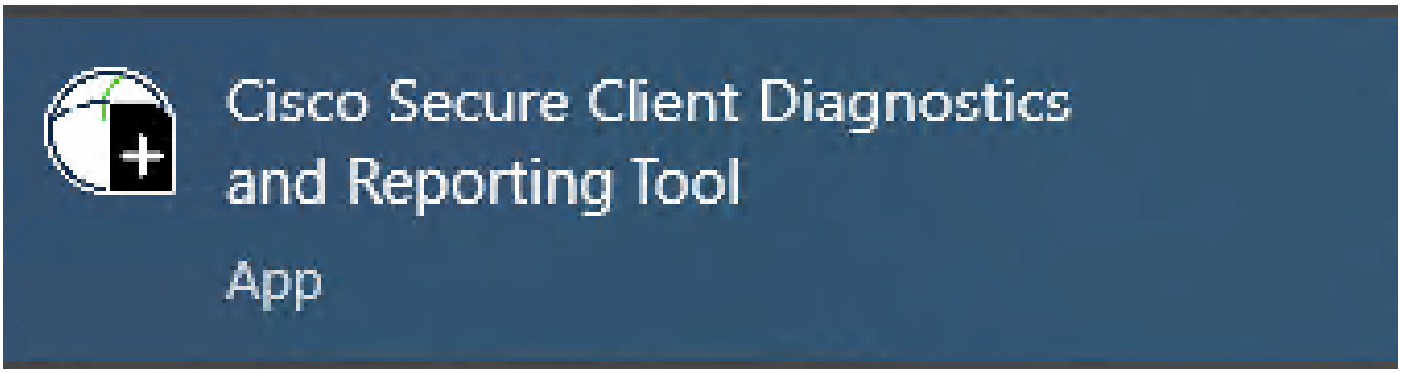
إعدادات سجل NAM الآمن للعميل

2 - إعادة طرح المسألة.

بمجرد تمكين التسجيل الموسع، يتم إعادة إنتاج المشكلة عدة مرات لضمان إنشاء السجلات وقبض حركة المرور.

3. تجميع حزمة DART الخاصة بالعميل الآمن.

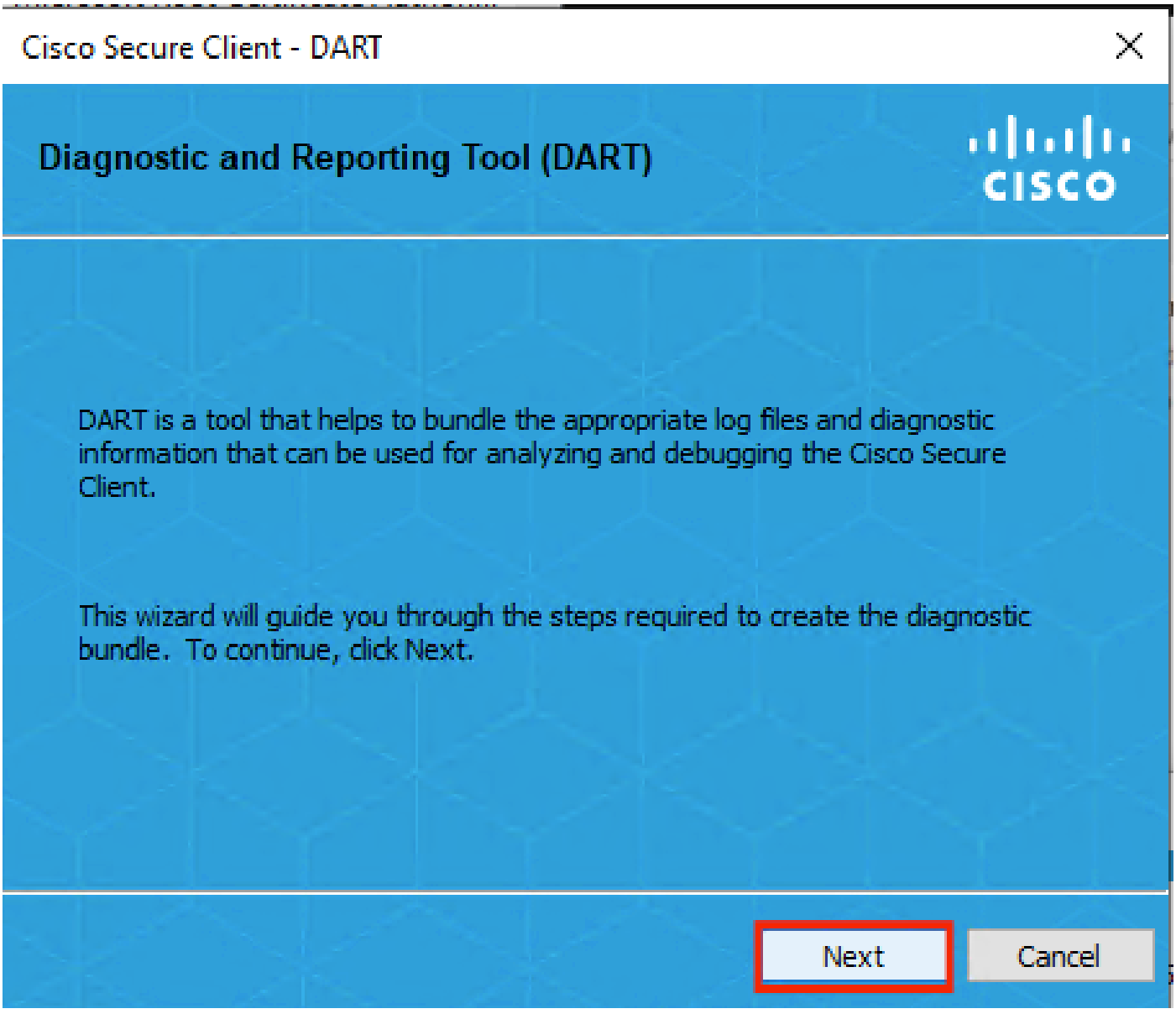
من Windows، انتقل إلى شريط البحث والنوع، أداة Cisco Secure Client Diagnostics and Reporting Tool.



وحدة DART

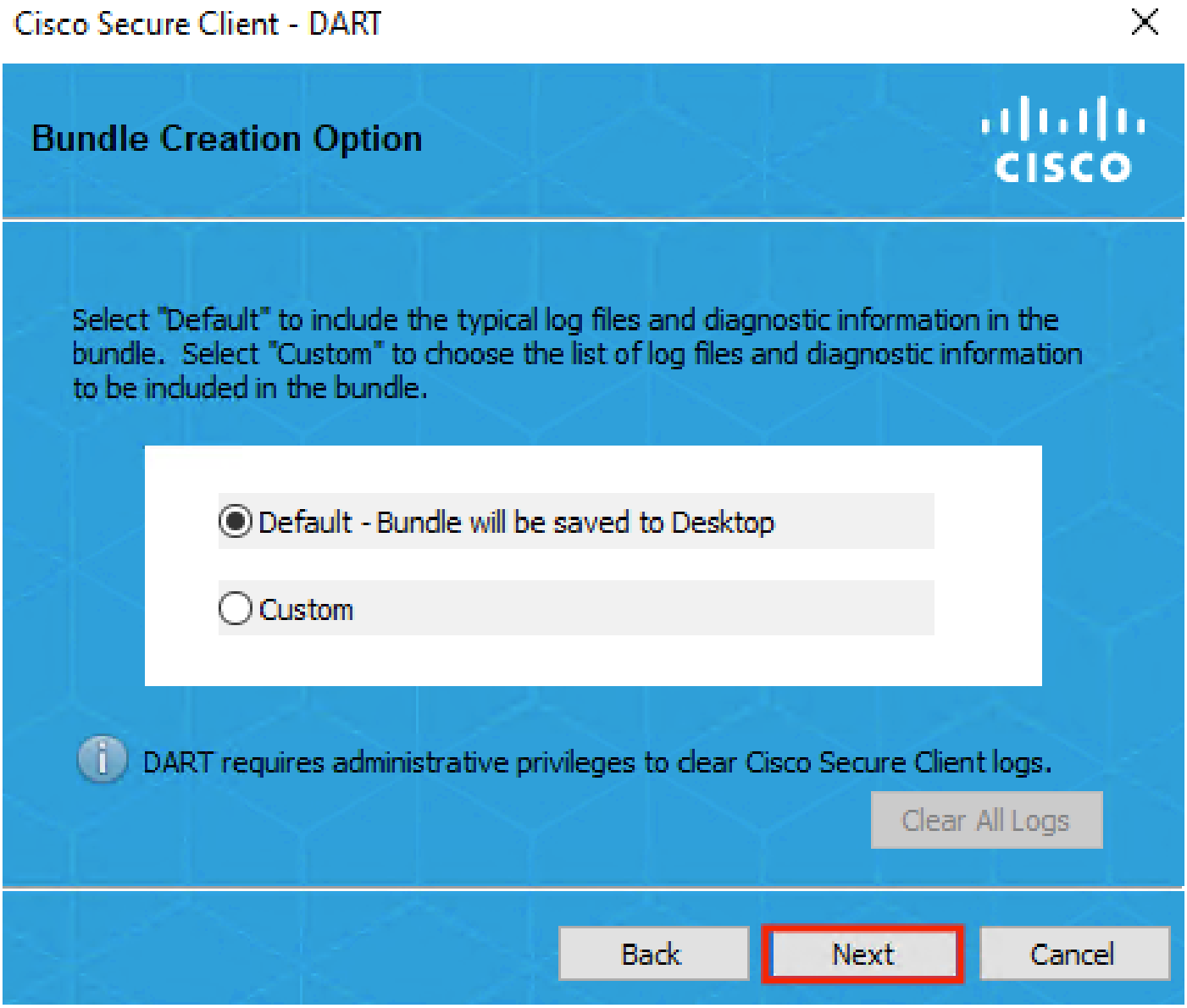
أثناء عملية التثبيت، قمت أيضا بتثبيت هذه الوحدة النمطية. وهو أداة تساعد أثناء عملية أستكشاف الأخطاء وإصلاحها من خلال تجميع السجلات ومعلومات جلسة dot1x ذات الصلة.

طقطقت بعد ذلك في أول نافذة.



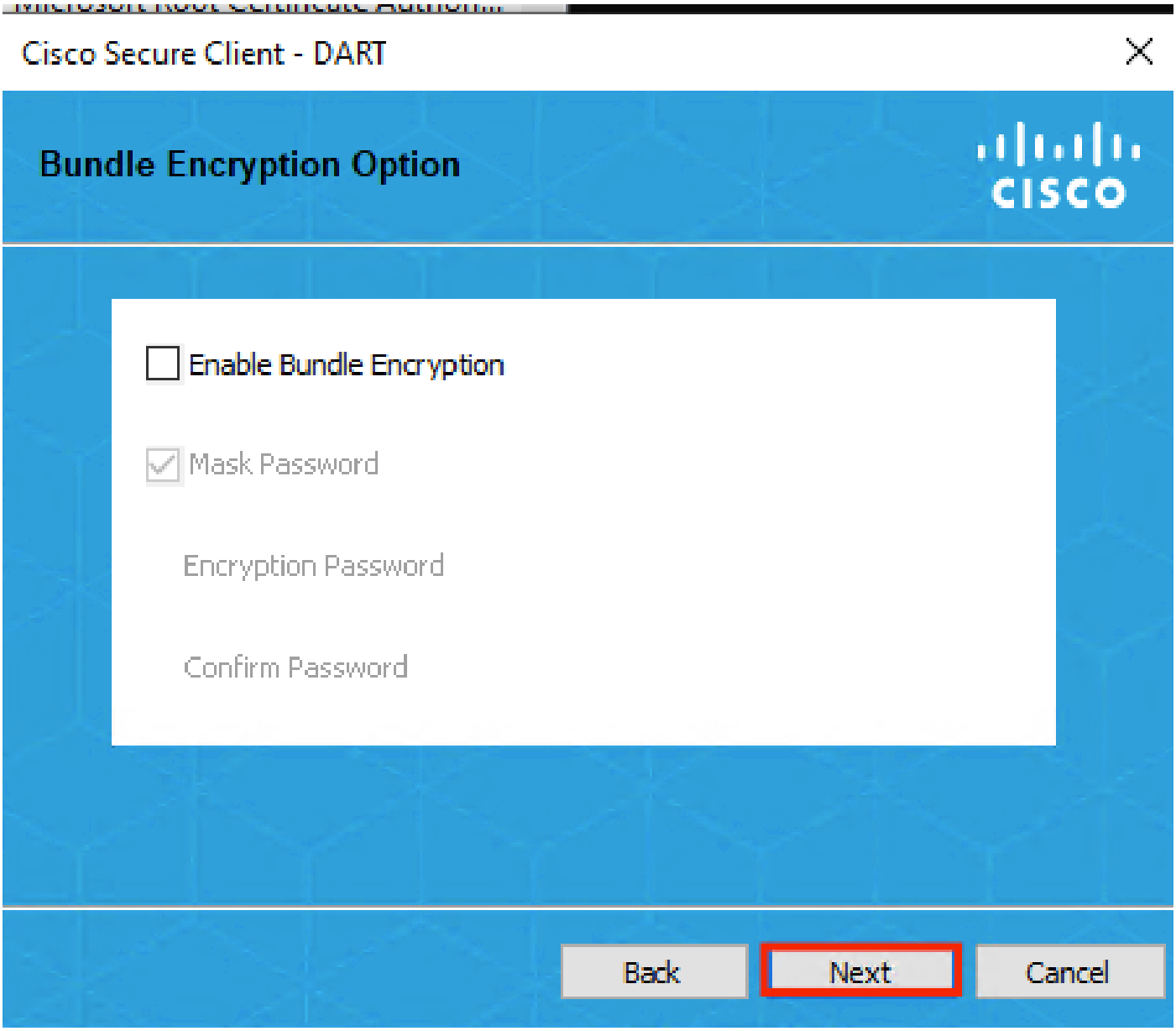
وحدة DART

انقر مرة أخرى فوق التالي، لذلك يمكن حفظ حزمة السجل على سطح المكتب.



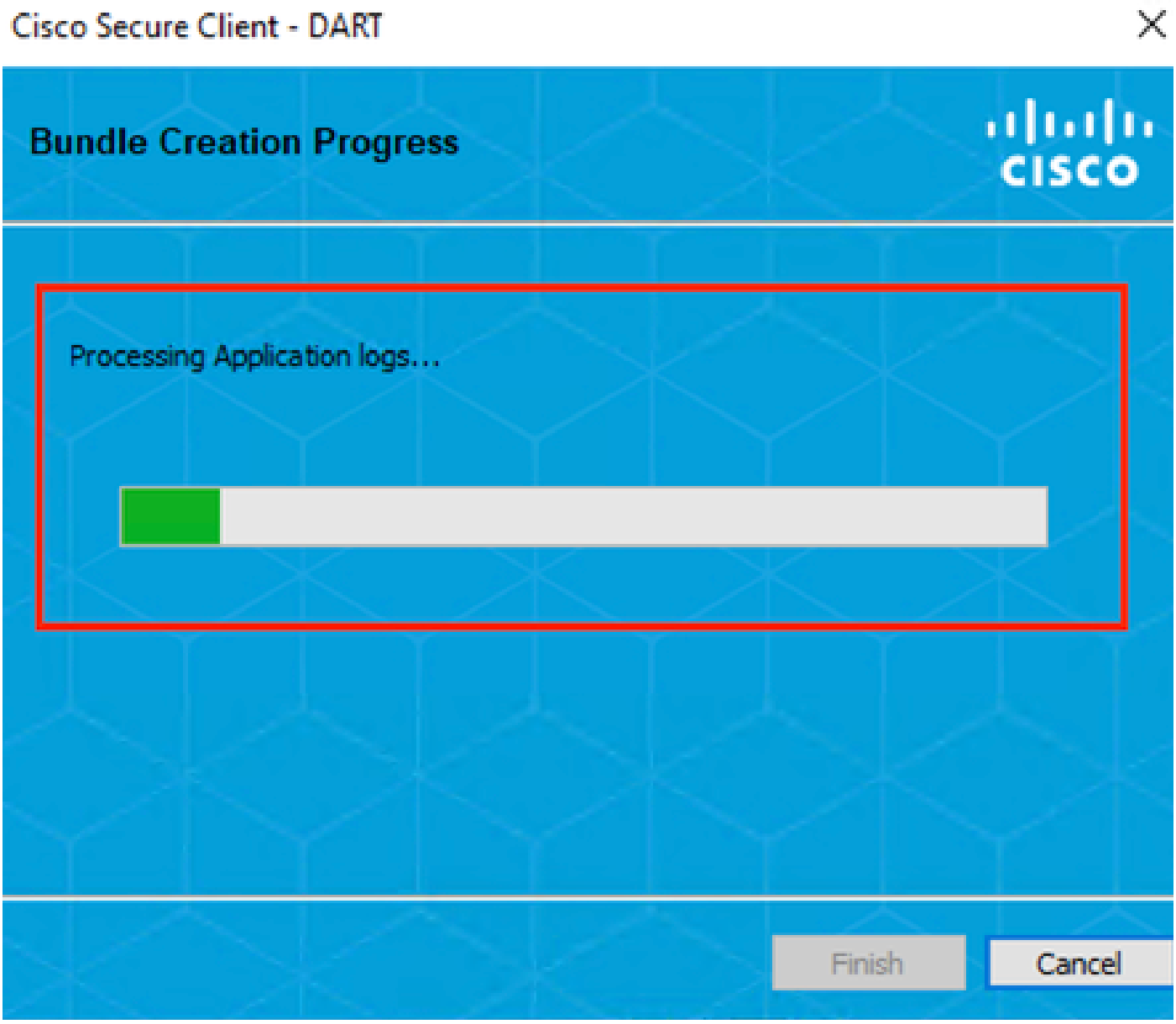
وحدة DART

إن أمكن فحصت ال checkbox enable حزمة تشفير.



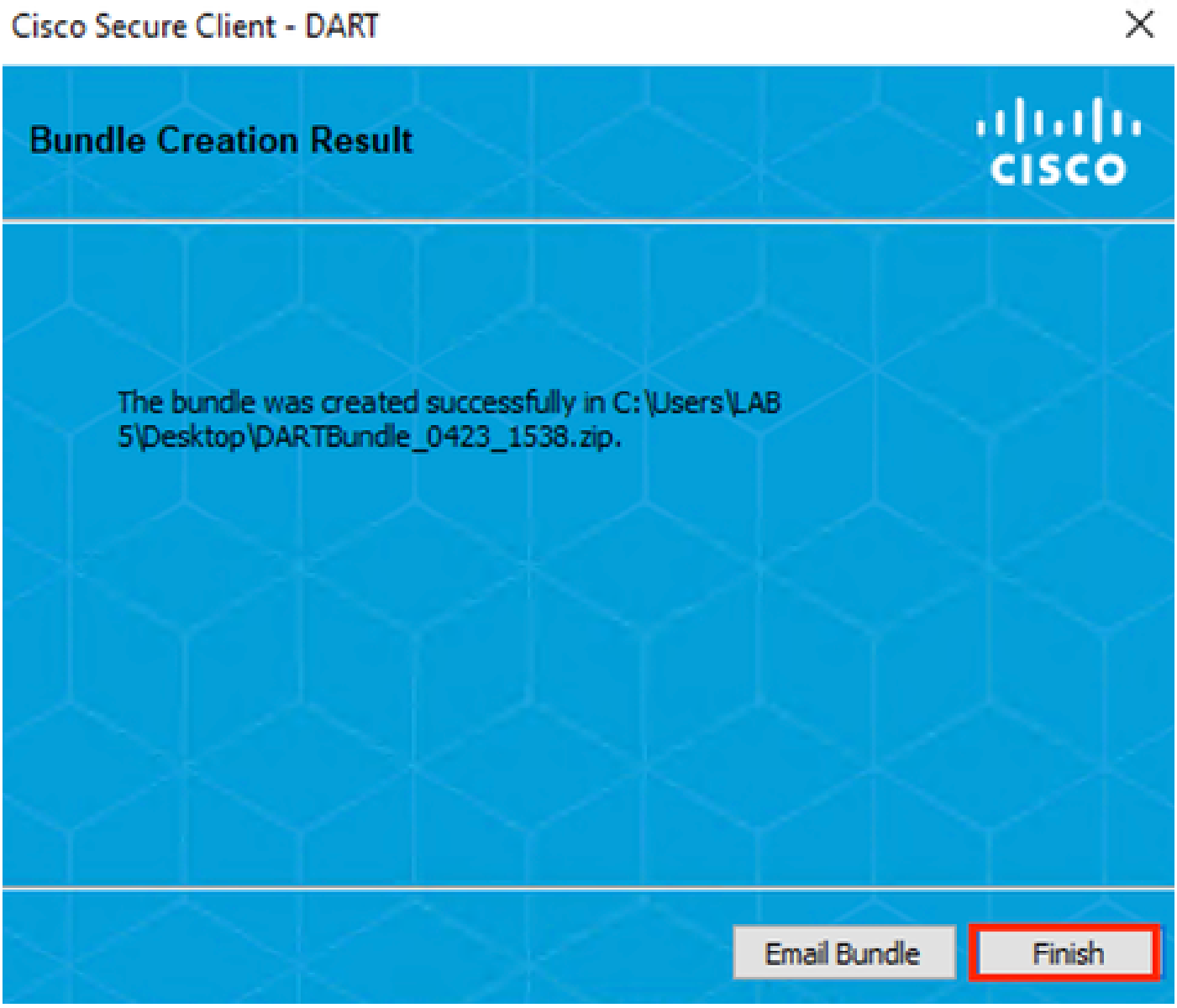
وحدة DART

تبدأ مجموعة سجلات DART.



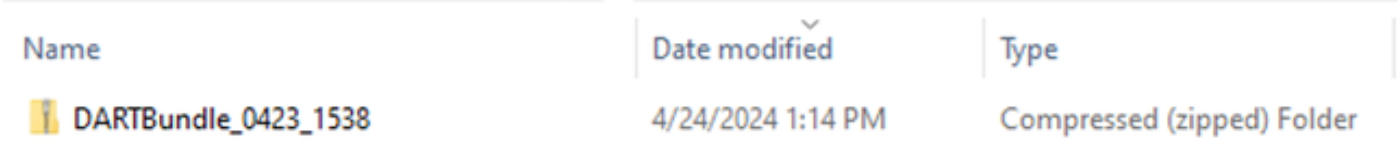
مجموعة سجل DART

قد يستغرق الأمر 10 دقائق أو أكثر حتى تنتهي العملية.



نتيجة إنشاء حزمة DART

يمكن العثور على ملف نتائج DART في دليل سطح المكتب.



ملف نتائج DART

معلومات ذات صلة

- الدعم الفني والتنزيلات من Cisco

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).