تكوين تغيير التفويض في Catalyst 1300 باستخدام واجهة مستخدم الويب

الهدف

الهدف من هذا مادة أن يبدي أنت كيف أن يشكل تغير التفويض (CoA) في مادة حفازة 1300 مفتاح يستعمل ال web مستعمل قارن (UI).

إصدار البرامج والأجهزة القابلة للتطبيق

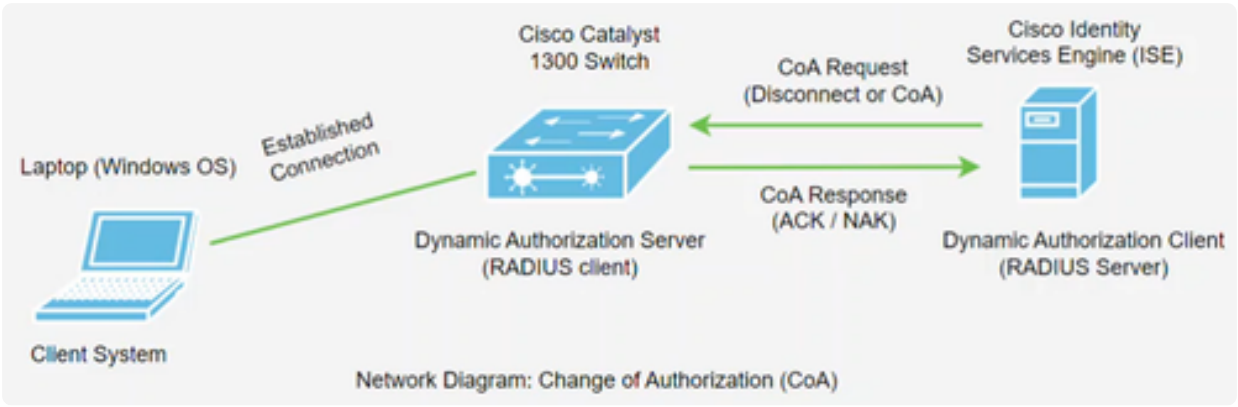
- المحولات Catalyst 1300 switches | 4.1.6.53

المقدمة

تغيير التفويض (CoA) هو امتداد لبروتوكول RADIUS، يسمح لك بتغيير خصائص المصادقة والتخويل والمحاسبة (AAA) أو dot1x جلسة عمل المستخدم بعد مصادقته. عند تغيير سياسة لمستخدم أو مجموعة في AAA، يمكن للمسؤولين إرسال حزم RADIUS CoA من خادم AAA، مثل محرك خدمات الهوية (ISE) من Cisco، لإعادة تهيئة المصادقة وتطبيق السياسة الجديدة.

محرك خدمات الهوية من Cisco (ISE) عبارة عن محرك متكامل المميزات للتحكم في الوصول وإنفاذ السياسات قائمة على الشبكة. وهو يوفر تحليلات الأمان وإنفاذه وخدمات RADIUS و TACACS وتوزيع السياسات وغير ذلك. Cisco ISE هو عميل التفويض الديناميكي CoA الوحيد المدعوم للمحولات Catalyst 1300 switches. راجع دليل مسؤول ISE للحصول على مزيد من المعلومات.

تتطلب هذه المميزة الاتصال بين عميل التفويض الديناميكي (خادم RADIUS) وخادم التفويض الديناميكي (محول Catalyst). كما هو موضح في الرسم التخطيطي للشبكة أدناه، يرسل خادم التخويل الديناميكي رسالة قطع اتصال أو CoA إلى خادم التخويل الديناميكي ويوفر المحول إستجابة.



تمت إضافة دعم CoA إلى محولات Catalyst 1300 في الإصدار 4.1.3.36 من البرنامج الثابت. ويتضمن ذلك دعم فصل المستخدمين وتغيير الأذون القابلة للتطبيق على جلسة عمل المستخدم. يدعم الجهاز إجراءات CoA التالية:

- قطع اتصال جلسة العمل
- تعطيل الأمر host port CoA
- أمر Bounce host port CoA
- إعادة مصادقة أمر CoA للمضيف

لتكوين CoA باستخدام واجهة سطر الأوامر (CLI)، ارجع إلى تكوين تفويض تغيير في محول Catalyst 1300 switch باستخدام CLI (واجهة سطر الأوامر).

جدول المحتويات

- تكوين عميل Catalyst 1300 RADIUS على ISE
- التكوينات في المحول Catalyst 1300 Switch
- عملية التعاون

تكوين عميل Catalyst 1300 RADIUS على ISE

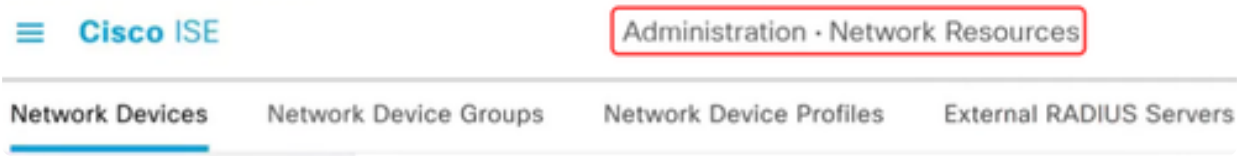
في هذا المثال، يتم إستخدام الإصدار 3.2 من Cisco ISE Server. للحصول على نظرة عامة على ISE، راجع صفحة منتج محرك خدمات الهوية من Cisco.

> **Note:**
> يتم دعم CoA على الإصدار 2.7 من ISE والإصدارات الأحدث.

بعد نشر خادم Cisco ISE، سجل الدخول للوصول إلى واجهة مستخدم الويب.

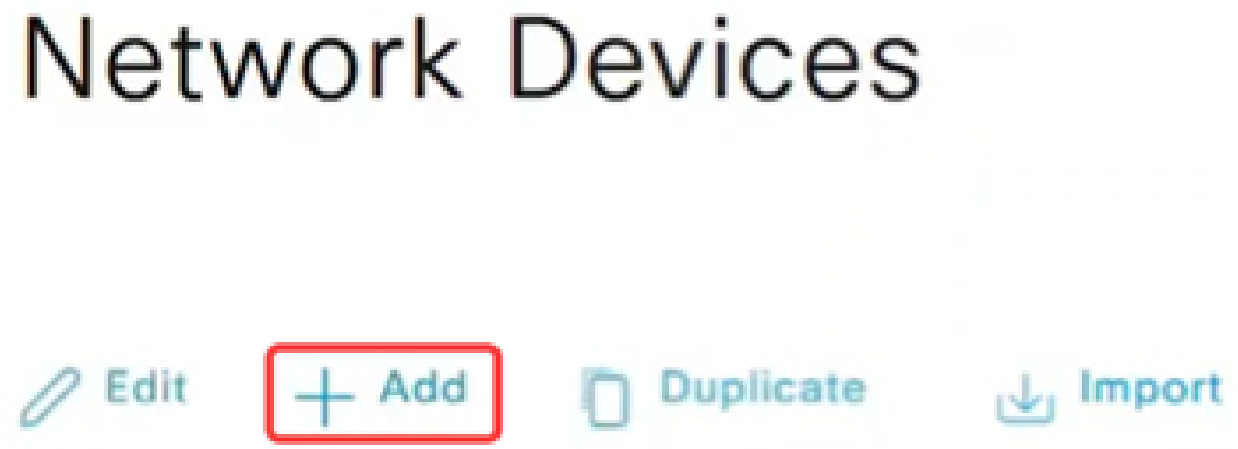
الخطوة 1

لإضافة أجهزة شبكة، انتقل إلى قائمة إدارة > موارد الشبكة.



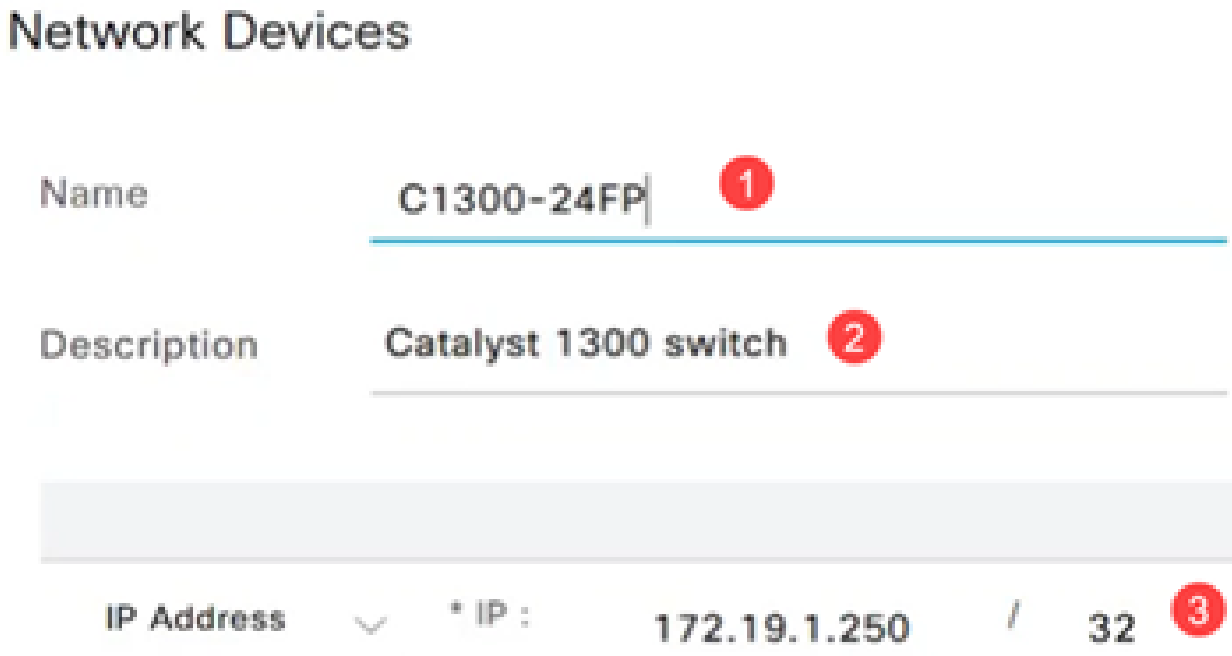
الخطوة 2

انقر فوق الزر +إضافة .



الخطوة 3

دخلت الإسم، الوصف، وعنوان من المادة حفازة مفتاح.

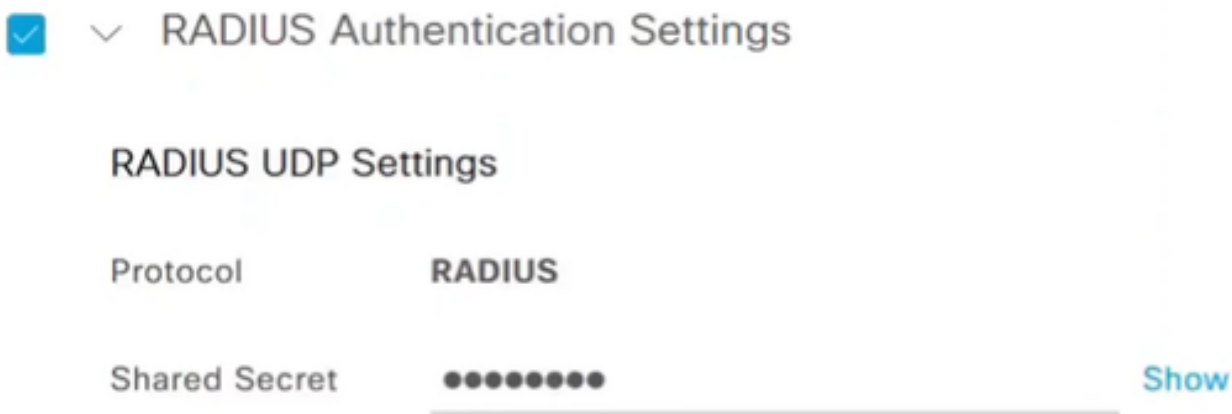


الخطوة 4

من القائمة المنسدلة ملف تعريف الجهاز، حدد Cisco.

الخطوة 5

قم بتكوين إعدادات مصادقة RADIUS بإدخال السر المشترك.

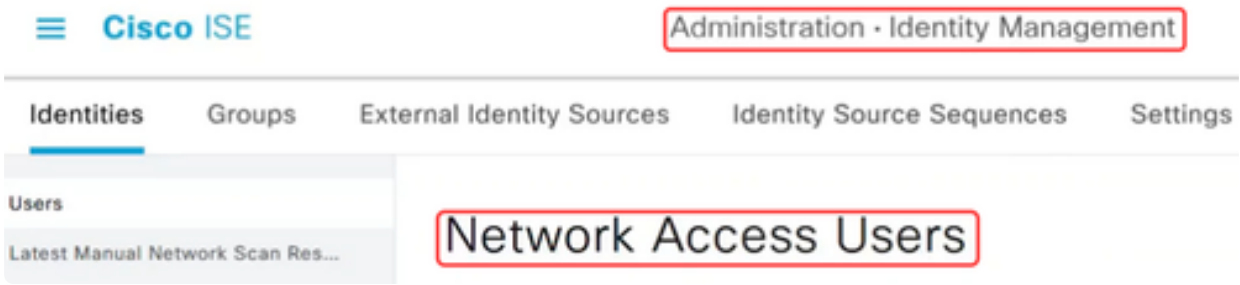


الخطوة 6

دخلت الـ coA ميناء رقم. المنفذ الافتراضي هو 1700.

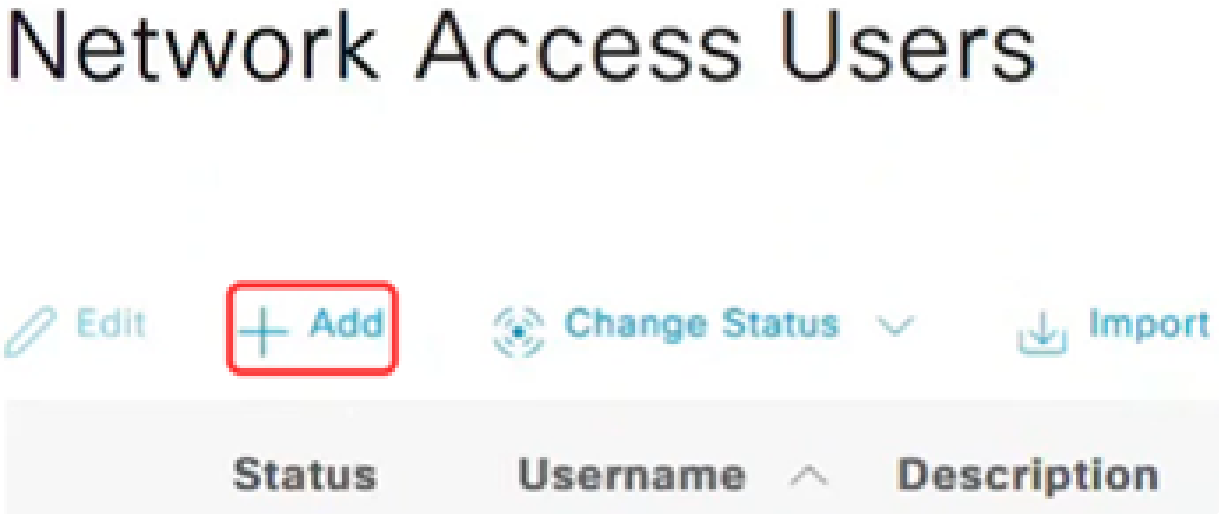
الخطوة 7

بعد ذلك، انتقل إلى إدارة > إدارة الهوية وحدد مستخدمي الوصول إلى الشبكة.



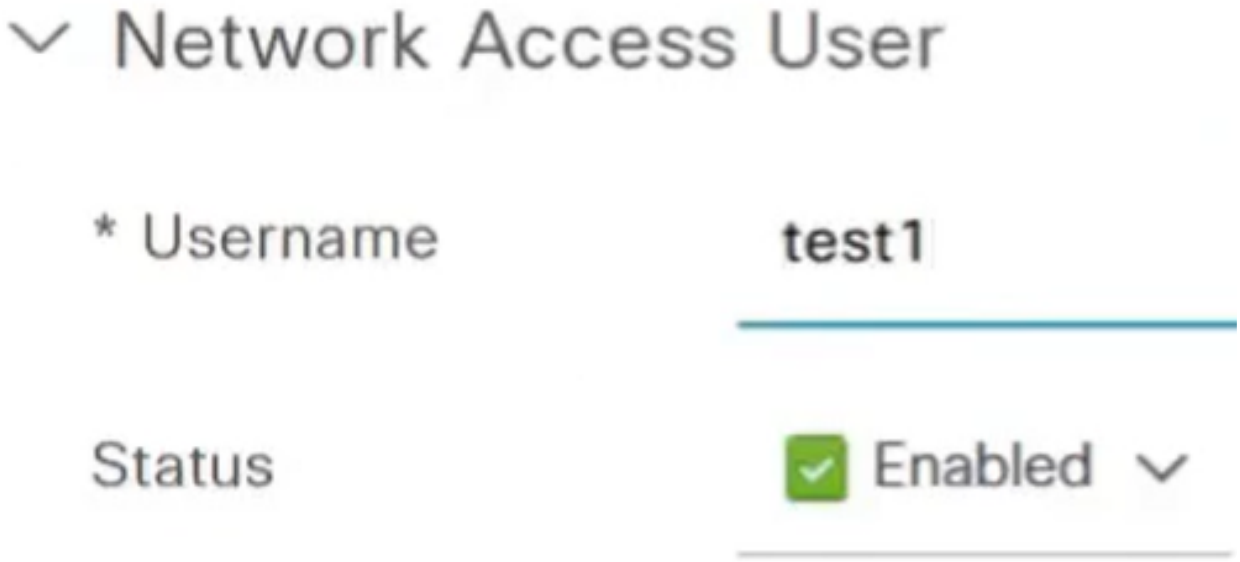
الخطوة 8

لتعريف اسم المستخدم وكلمة المرور، انقر على رمز +إضافة.



الخطوة 9

أدخل اسم المستخدم وكلمة المرور وانقر فوق حفظ في أسفل الصفحة.



التكوينات في المحول Catalyst 1300 Switch

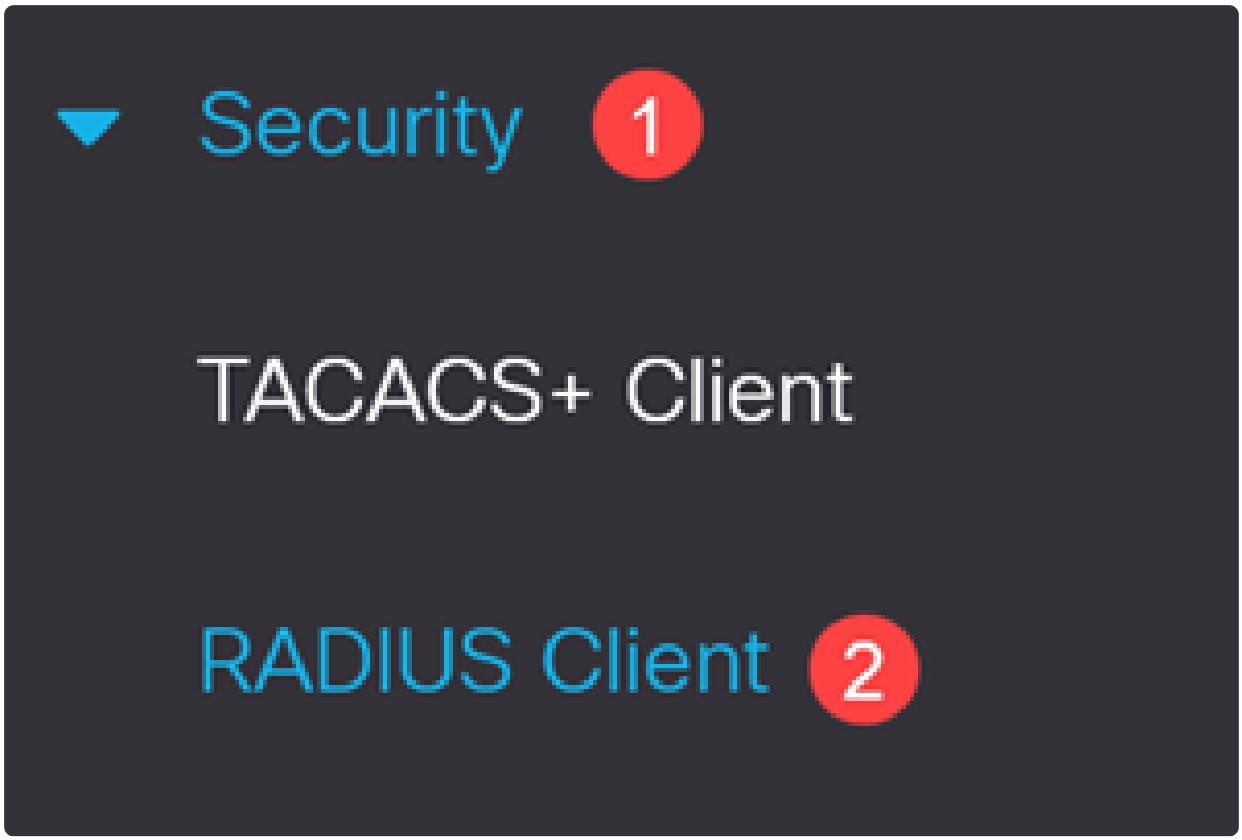
الخطوة 1

قم بتسجيل الدخول إلى المحول Catalyst 1300 switch وحدد الوضع المتقدم. في هذا المثال، يتم إستخدام C1300-24FP-4X.

> Note:
> تمت إضافة دعم CoA إلى محولات Catalyst 1300 في إصدار البرنامج الثابت 4.1.3.36.

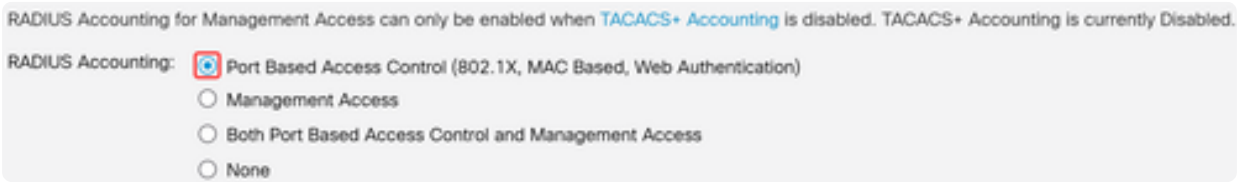
الخطوة 2

انتقل إلى الأمان > عميل RADIUS في جزء التنقل.



الخطوة 3

تعيين محاسبة RADIUS على التحكم في الوصول المستند إلى المنفذ.



الخطوة 4

لإضافة خادم ISE، قم بالتمرير إلى جدول RADIUS وانقر فوق أيقونة زائد.

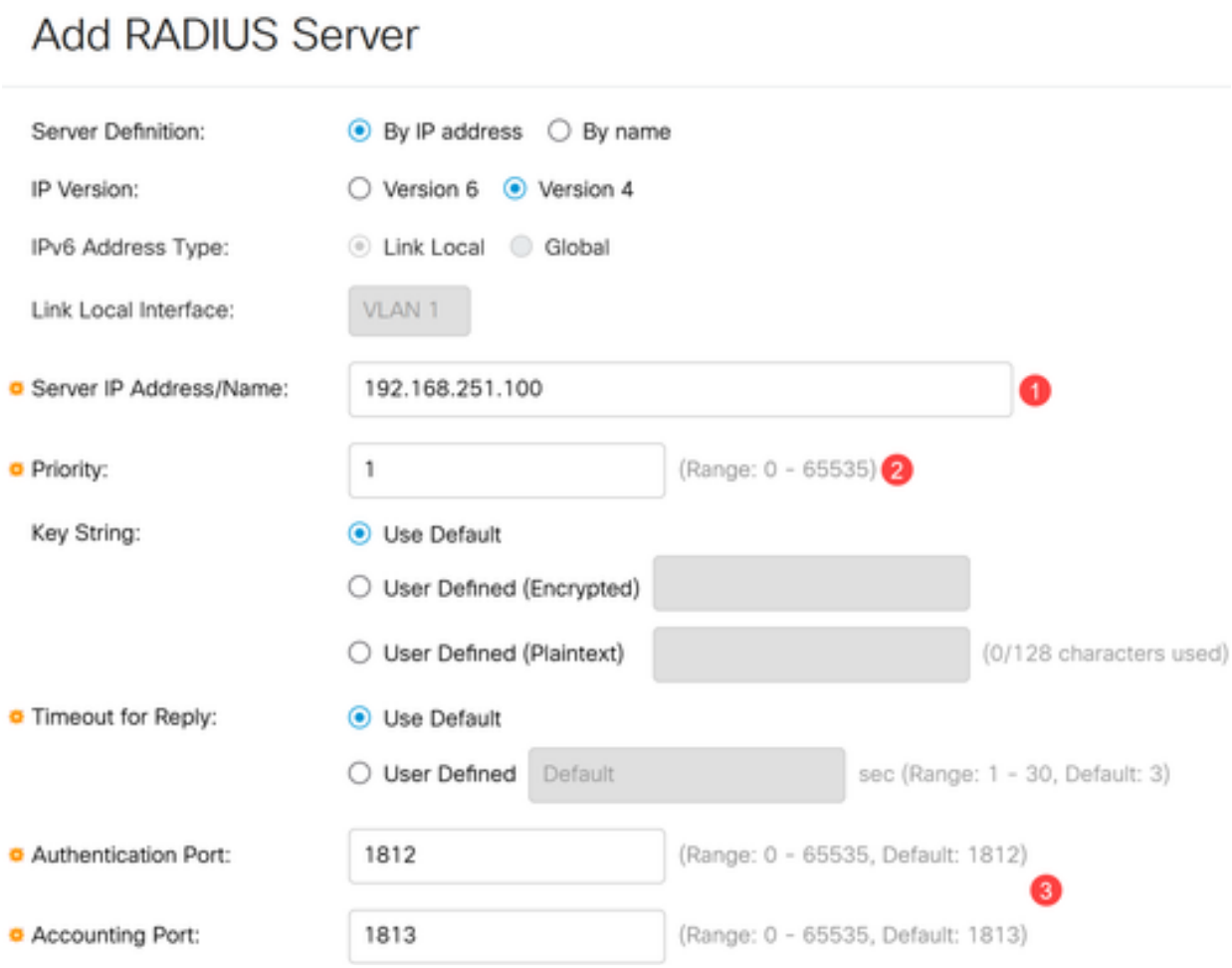
الخطوة 5

قم بتكوين إعدادات خادم RADIUS.

- حدد تعريف الخادم. في هذا المثال، يتم تحديد حسب عنوان IP. أدخل عنوان IP في حقل عنوان/اسم IP للخادم.
- تعيين أولوية RADIUS.
- تم تعيين منافذ المصادقة والمحاسبة على الوضع الافتراضي.

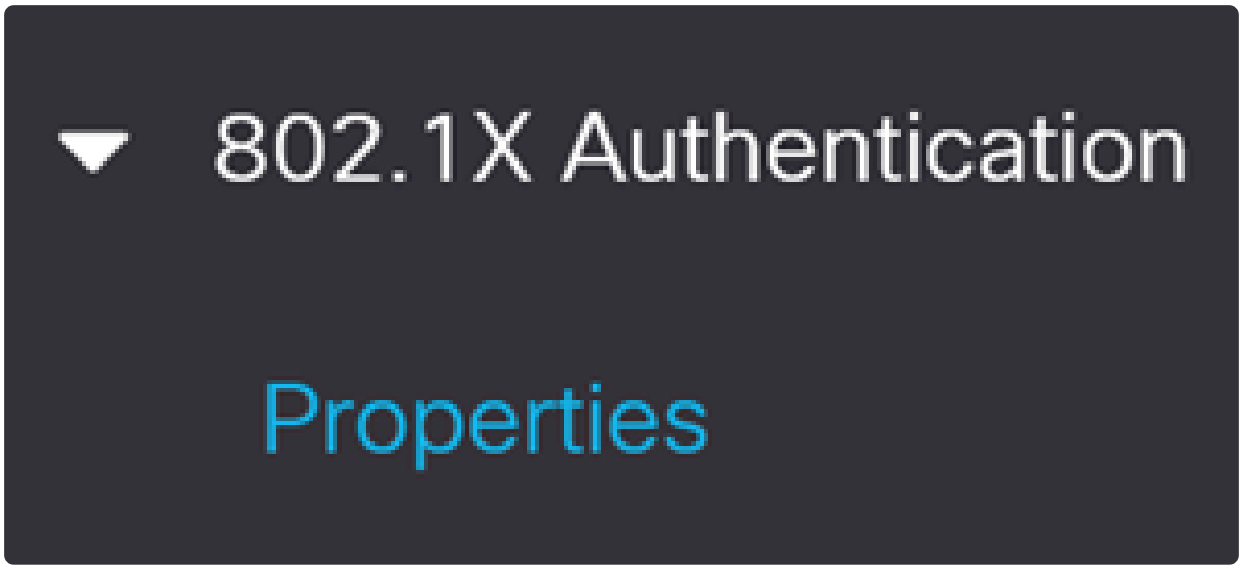
- نوع الاستخدام هو 802.1x.

انقر فوق تطبيق.



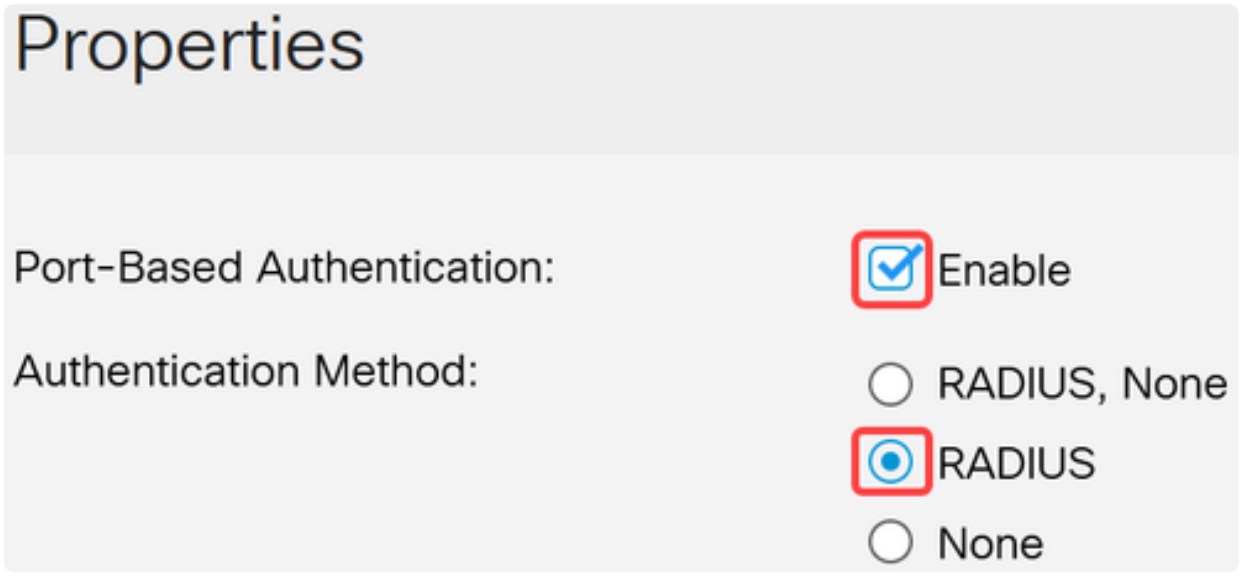
الخطوة 6

لتكوين مصادقة 802.1x، انتقل إلى التأمين > مصادقة 802.1X > قائمة خصائص.



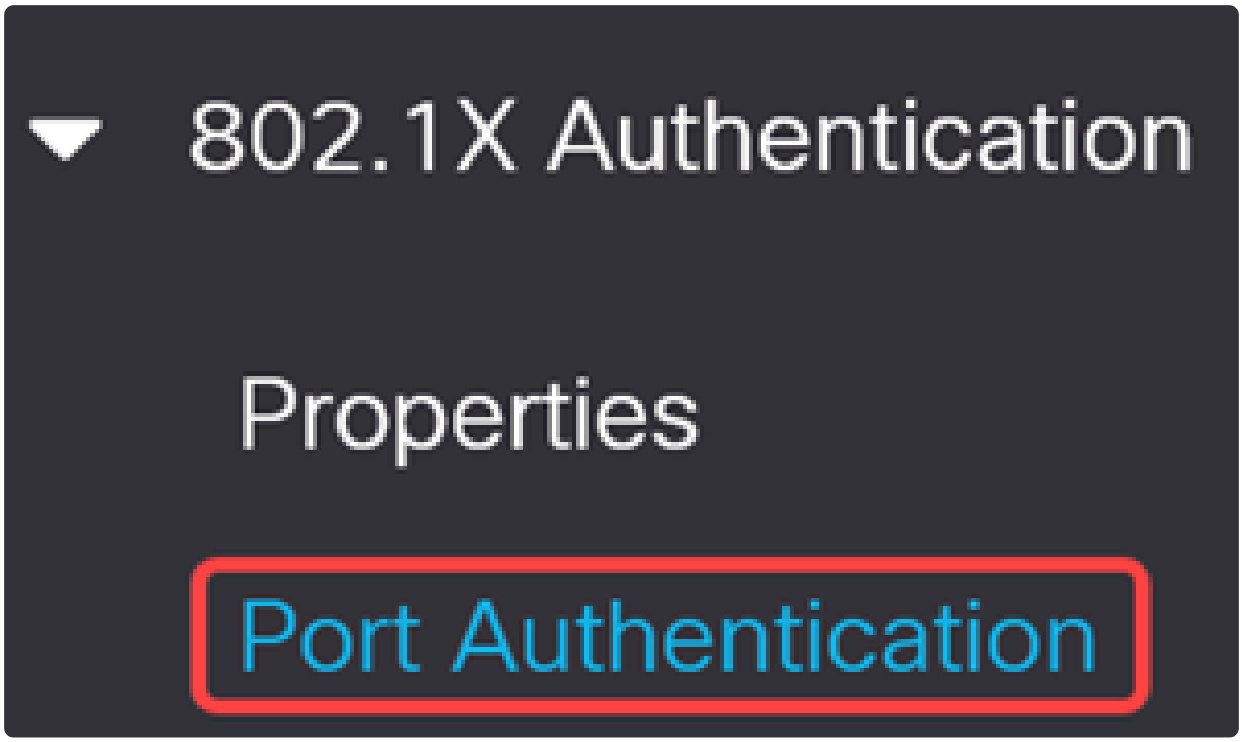
الخطوة 7

تأكد من تمكين المصادقة المستندة إلى المنفذ، وتم تعيين أسلوب المصادقة على RADIUS.



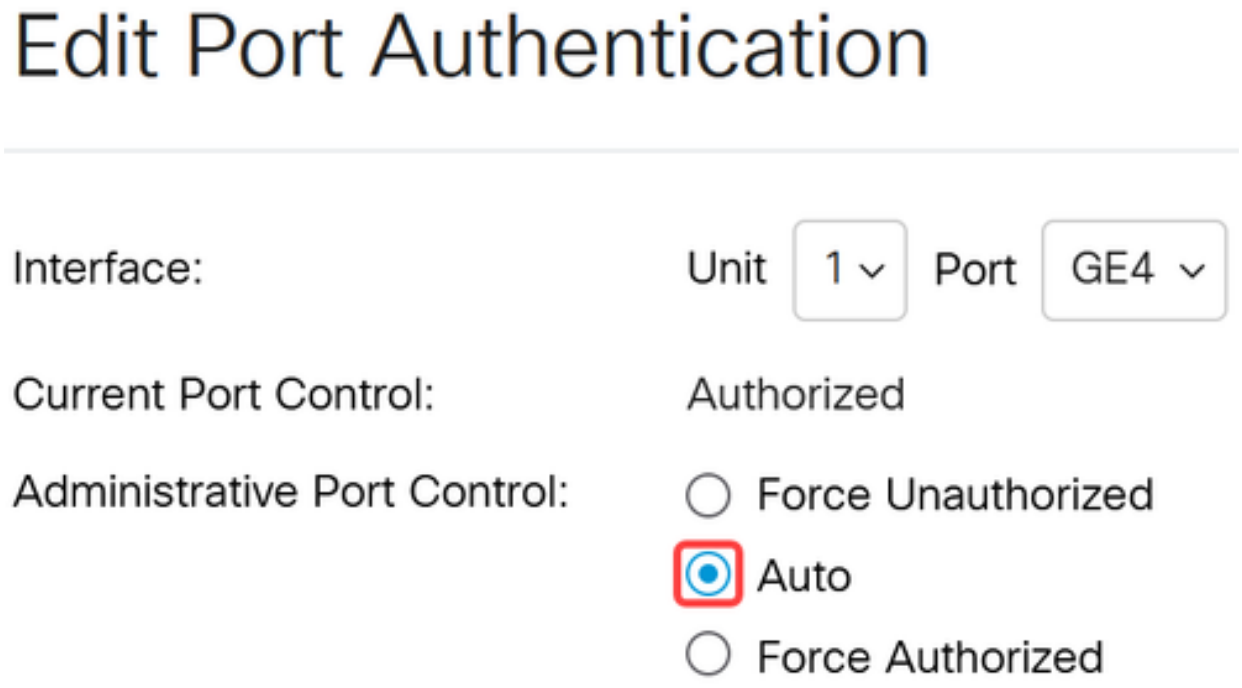
الخطوة 8

انتقل إلى قائمة مصادقة المنفذ، وحدد المنفذ المطلوب، وانقر تحرير.



الخطوة 9

للتحكم في المنفذ الإداري، حدد خيار تلقائي الذي سيحول المنفذ بين الحالة المصرح بها وغير المصرح بها استنادا إلى إستجابة RADIUS.

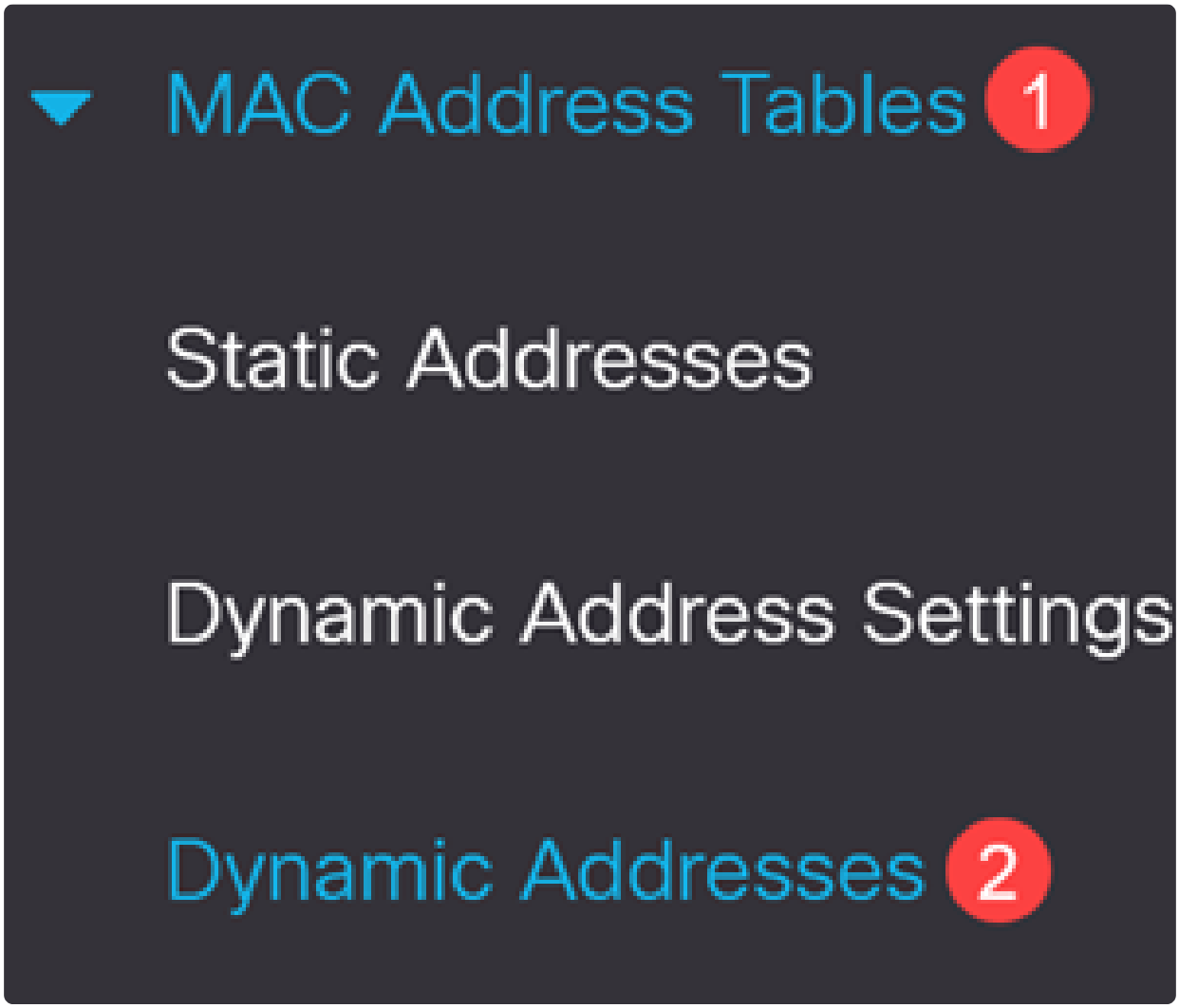


الخطوة 10

قم بتمكين المصادقة المستندة إلى معيار 802.1x وانقر فوق تطبيق.

الخطوة 11

أنت تحتاج الـ mac عنوان للجهاز على الميناء. سيتم تطبيق عملية CoA على ISE على عنوان MAC هذا. في هذا المثال، هو المنفذ 9. للحصول عليه، انتقل إلى جداول عناوين MAC > العناوين الديناميكية.

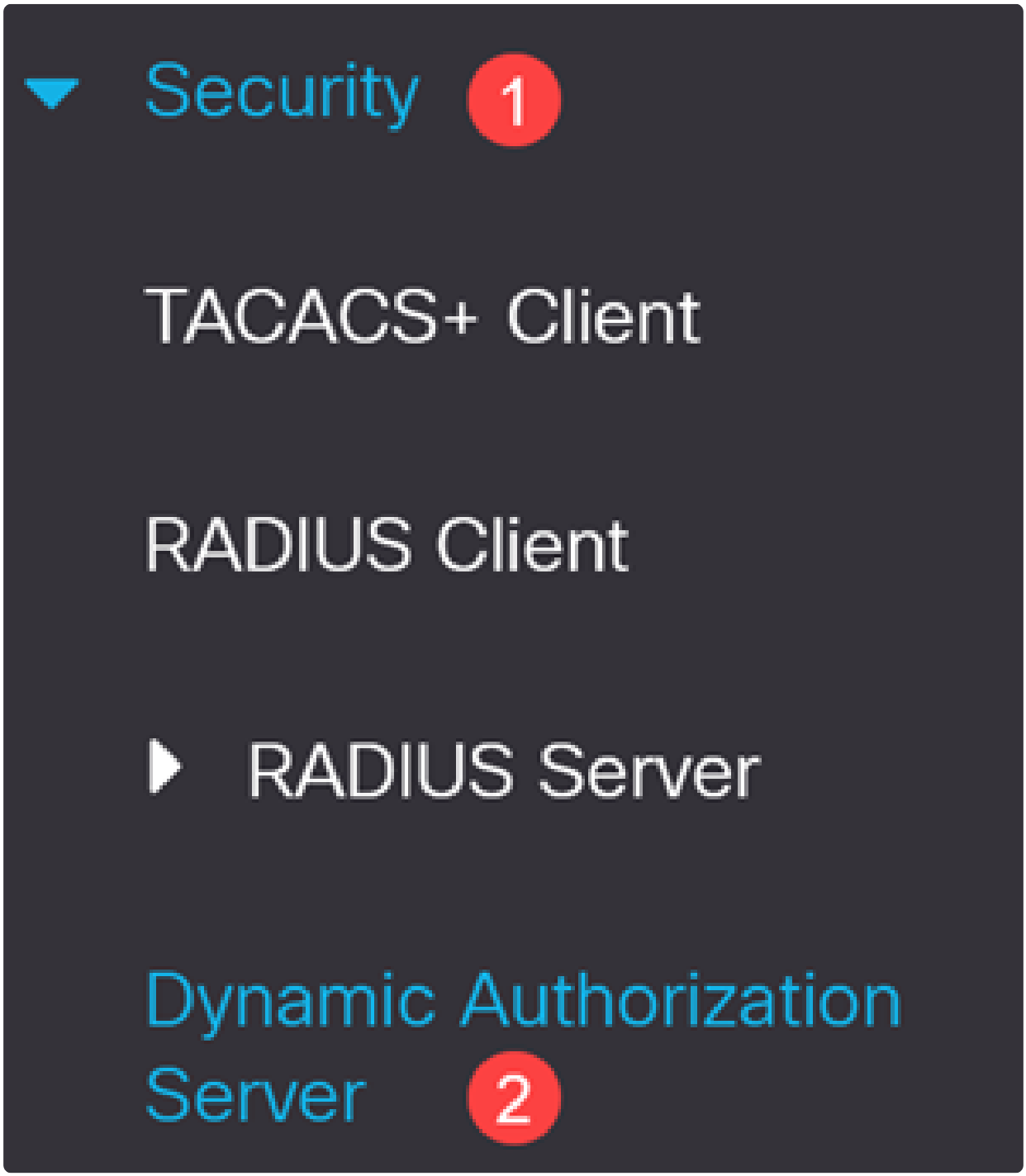


الخطوة 12

قم بالتمرير لأسفل إلى المنفذ ولاحظ عنوان MAC.

الخطوة 13

انتقل إلى الأمان > خادم التفويض الديناميكي.

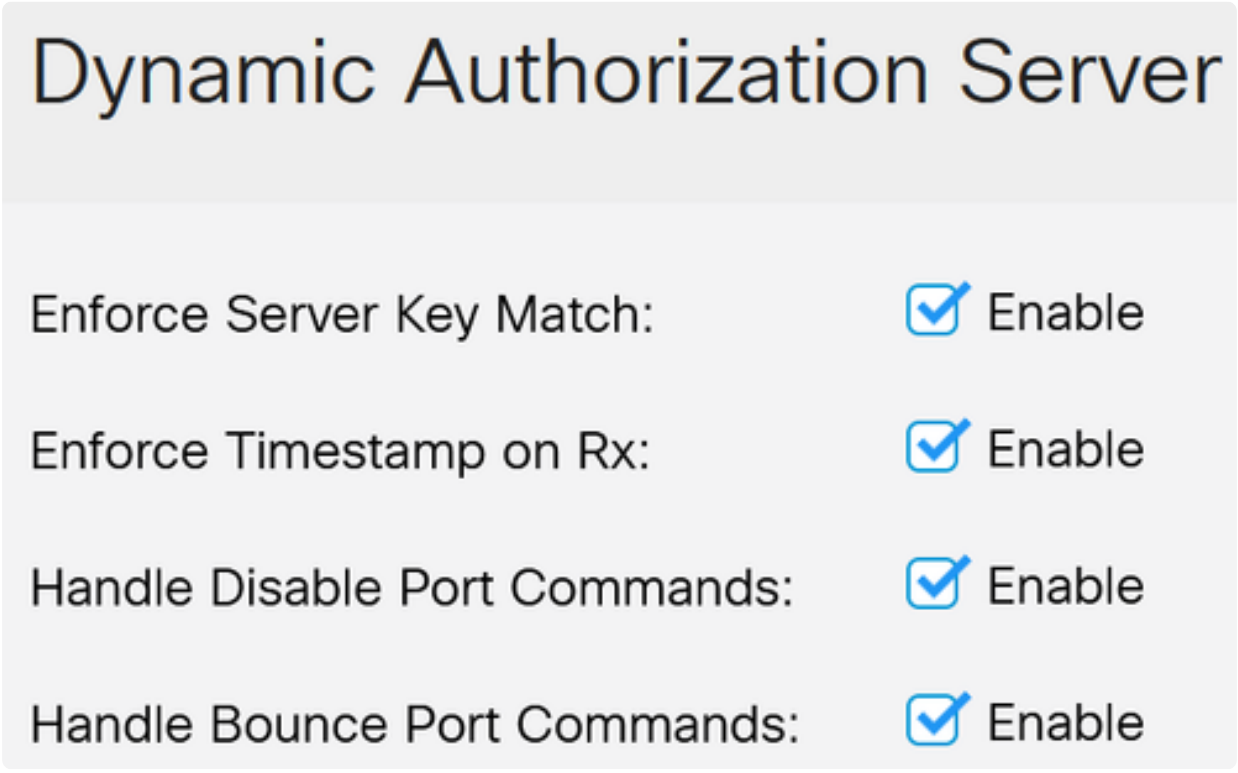


الخطوة 14

تمكين ما يلي:

- فرض تطابق مفتاح الخادم

- فرض الطابع الزمني على Rx
- معالجة تعطيل أوامر المنفذ
- معالجة أوامر منفذ القفزات

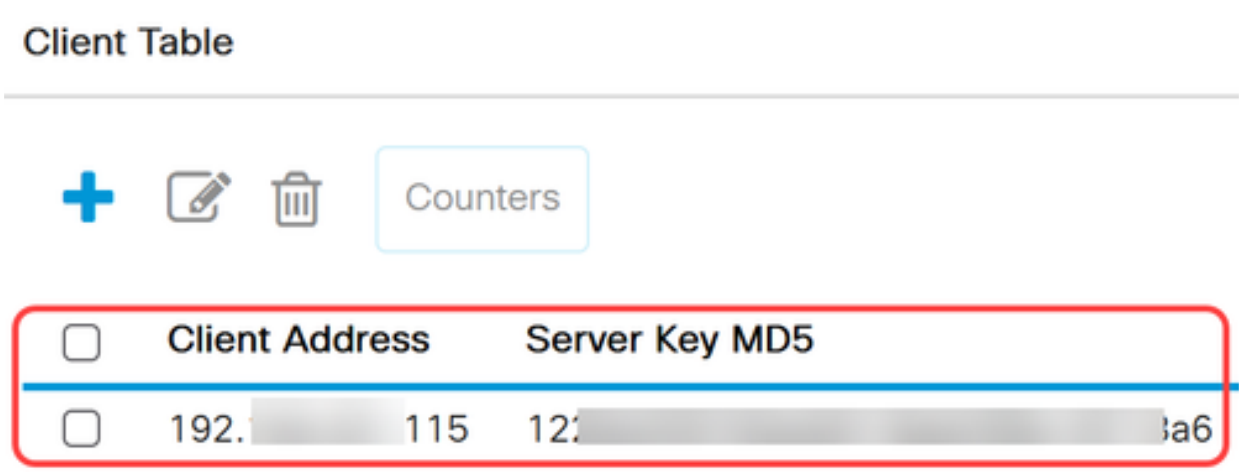


الخطوة 15

أترك منفذ UDP عند القيمة الافتراضية 1700.

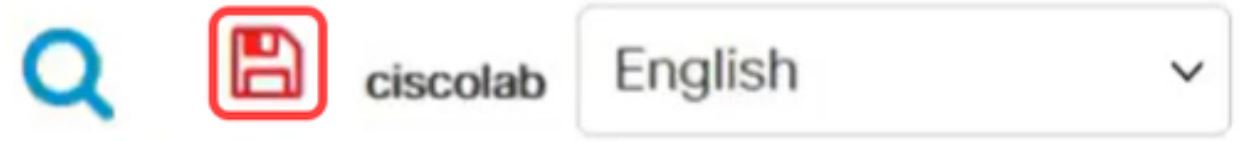
الخطوة 16

ضمن جدول العملاء، تأكد من إضافة خادم ISE باستخدام مفتاح الخادم الصحيح.
انقر فوق تطبيق.



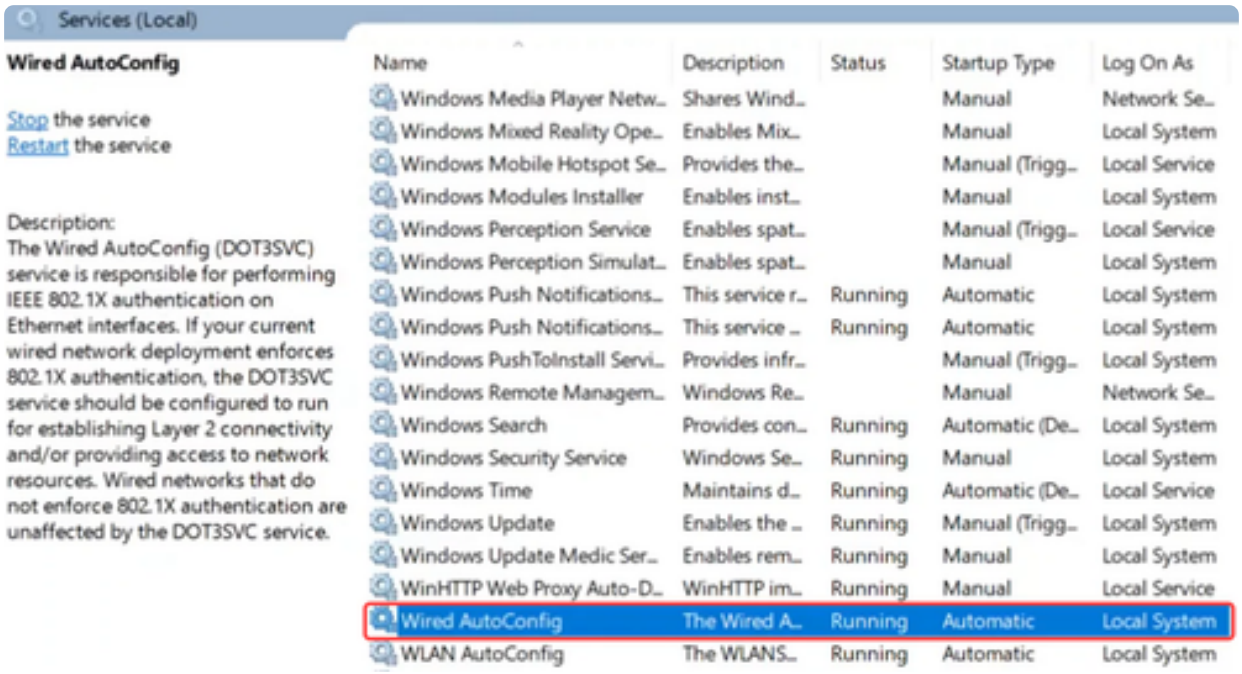
الخطوة 17

انقر أيقونة حفظ الوامض الأحمر لحفظ التكوينات.



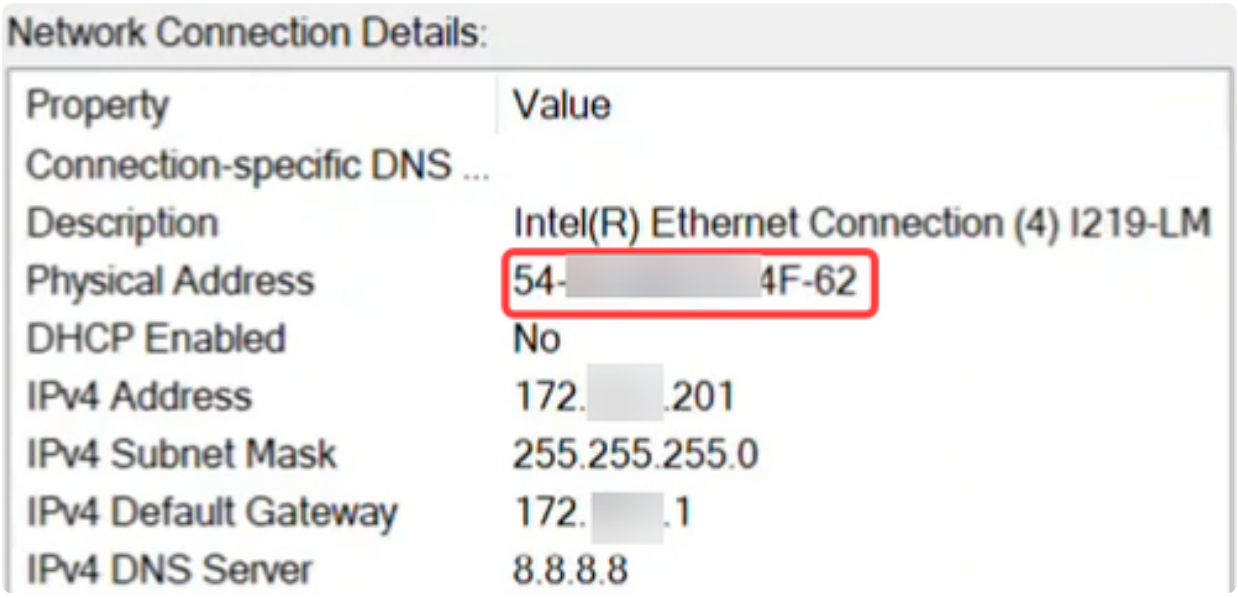
الخطوة 18

على الكمبيوتر المحمول العميل المتصل بالمنفذ 9، تحقق من تمكين خدمة التكوين التلقائي السلكية لمصادقة 802.1 X.



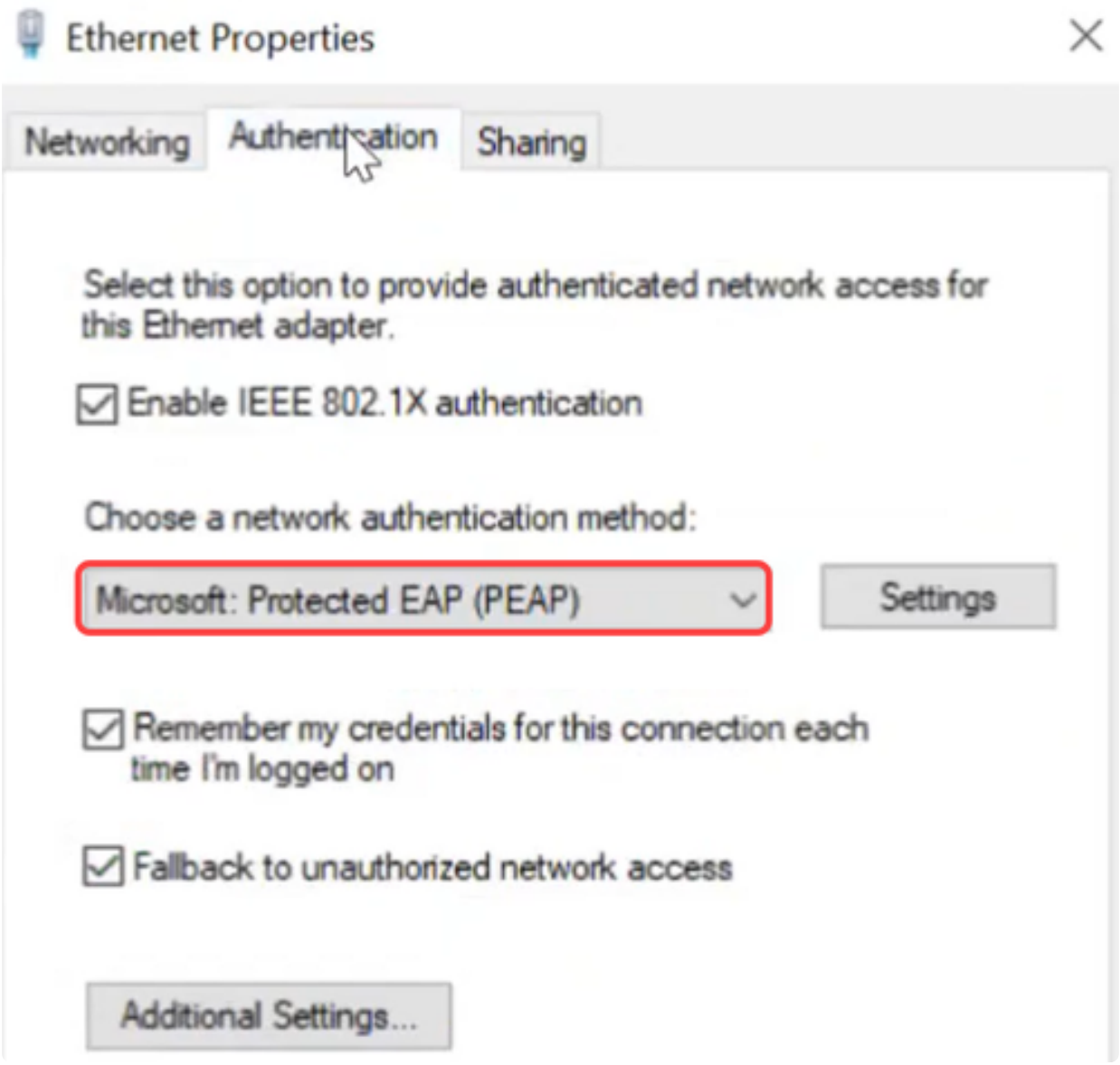
الخطوة 19

في إعدادات محول الإيثرنت، تحقق من تطابق عنوان MAC.



الخطوة 20

انقر فوق الزر خصائص ضمن إعدادات إيثرنت وتحت علامة التبويب المصادقة، تأكد من تمكين خانات الاختيار. تأكد أيضا من أن أسلوب المصادقة هو EAP محمي (PEAP).



الخطوة 21

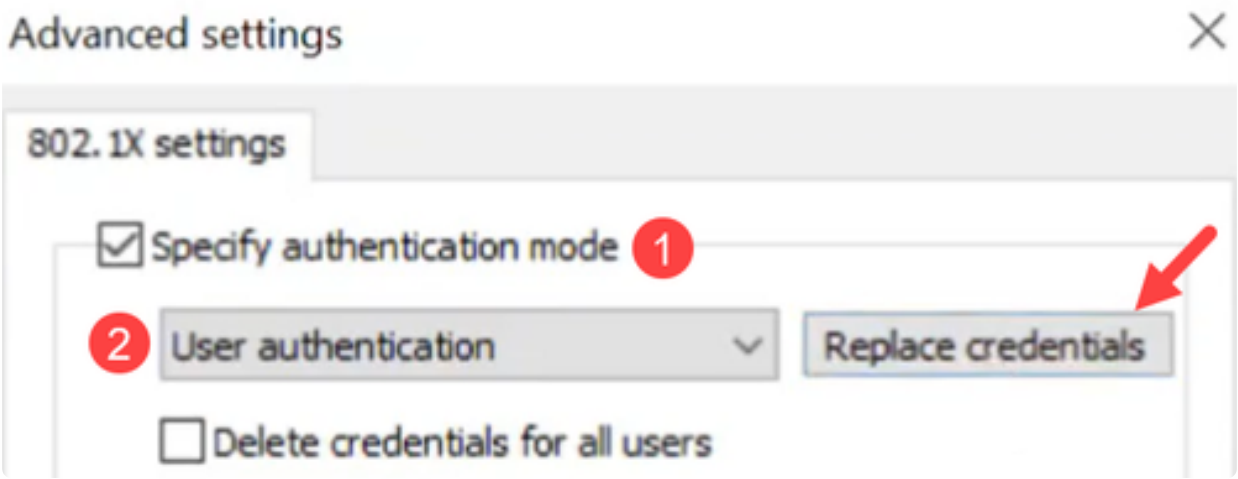
انقر فوق الزر إعدادات للتأكد من أن خانة الاختيار المجاورة للتحقق من هوية الخادم عن طريق التحقق من صحة الشهادة غير محددة.

الخطوة 22

يجب تحديد تمكين مربع إعادة الاتصال السريع.

الخطوة 23

ضمن الإعدادات الإضافية، تأكد من تمكين تحديد وضع المصادقة وتحديد مصادقة المستخدم من القائمة المنسدلة. يمكنك حفظ بيانات الاعتماد التي تم إنشاؤها على ISE أو إستبدالها باستخدام الزر إستبدال بيانات الاعتماد.



عملية التعاون

قبل بدء عملية CoA، قم بتمكين التقاط الحزمة على المحول.

الخطوة 1

على PuTTY، قم بتسجيل الدخول إلى محول Catalyst وحدد حجم المخزن المؤقت ووضع

الالتقاط باستخدام الأمر monitor capture cap1 buffer size 20 circular.

الخطوة 2

قم بتعيين مستوى التحكم على حد سواء باستخدام الأمر monitor capture cap1 control-plane كما.

الخطوة 3

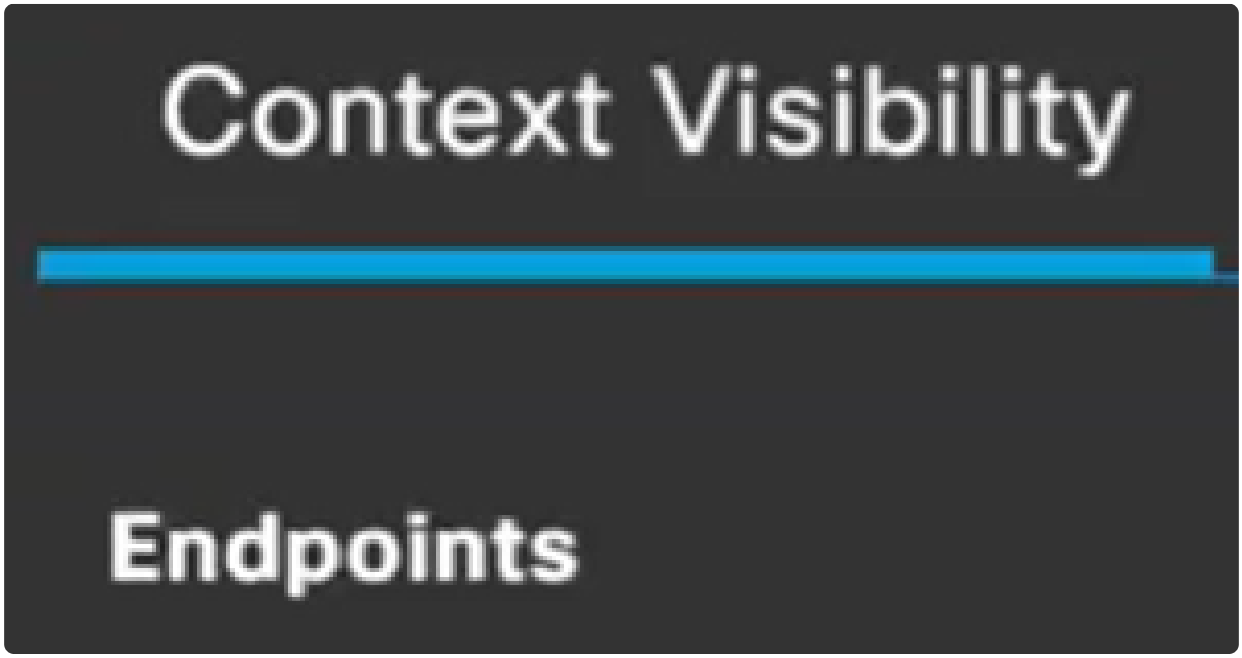
أدخل معايير المطابقة كأي. الأمر ل هذا سيكون مدرب التقاط cap1 يطابق أي.

الخطوة 4

بدء التقاط الحزمة.

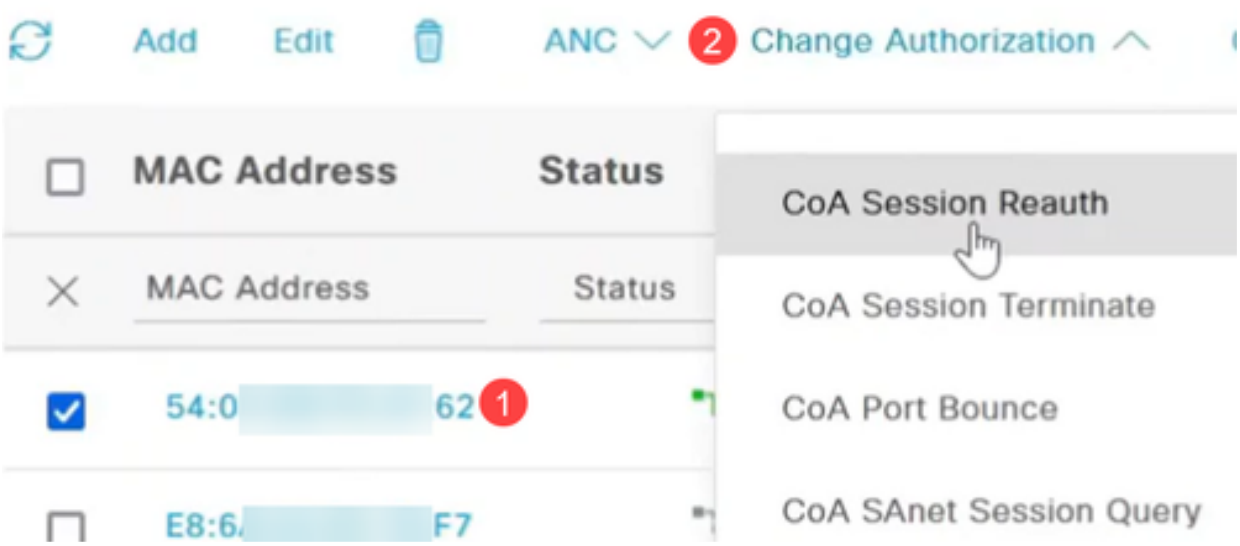
الخطوة 5

على واجهة ISE، انتقل إلى خيار نقاط النهاية ضمن إمكانية رؤية السياق.



الخطوة 6

أختر عنوان MAC وحدد عملية CoA من القائمة المنسدلة تغيير التفويض. في هذا المثال، يتم تحديد مرجع جلسة عمل CoA. هذا يجبر reauthentication على الميناء ب يرسل CoA رطب مع reauthentication أمر.



الخطوة 7

ارجع إلى وحدة PuTTY الطرفية للتحقق من نجاح عملية CoA.

```
Started capture point : capl
Cat1300-1#04-Jul-2024 20:49:45 %SEC-W-COAREAUTHSESSN: 802.1x re-authentication initiated for host 5
4:    62 by CoA Request "reauthenticate"
```

الخطوة 8

إذا قمت بتحديد إنهاء جلسة عمل CoA، فسيرسل طلب قطع اتصال باستخدام أمر إنهاء استناد إلى طلب إداري.

```
Cat1300-1#04-Jul-2024 20:50:02 %SEC-W-PORTUNAUTHORIZED: Port gi1/0/9 is unAuthorized
04-Jul-2024 20:50:02 %SEC-W-COADISCSESSN: 802.1x session for host 54:    :62 on interface gi
1/0/9 has been terminated by Disconnect-Request. Authenticator state on the Interface will be re-in
itialized
04-Jul-2024 20:50:02 %SEC-I-PORTAUTHORIZED: Port gi1/0/9 is Authorized
```

الخطوة 9

يرسل خيار CoA وثبة أيسر ربط طلب CoA مع قارن مضيف ميناء أمر، يعجز ويعيد يمكن المينا عل المفتاح. يستمر محول الشبكة دون اتصال لمدة 10 ثوان ويصبح غير مصرح به. ستتم العودة عبر الإنترنت، وستصبح معتمدة ويمكن إعادة توجيه الحزم.

```
Cat1300-1#04-Jul-2024 20:50:21 %SEC-W-COABNCEPORT: Interface gi1/0/9 suspended for 10 seconds by Co
A Request "bounce host port" for host 54:          :62
04-Jul-2024 20:50:21 %LINK-W-Down:  gi1/0/9
04-Jul-2024 20:50:34 %LINK-I-Up:  gi1/0/9
04-Jul-2024 20:50:34 %SEC-W-PORTUNAUTHORIZED: Port gi1/0/9 is unAuthorized
04-Jul-2024 20:50:36 %LINK-W-Down:  gi1/0/9
04-Jul-2024 20:50:39 %LINK-I-Up:  gi1/0/9
04-Jul-2024 20:50:39 %SEC-I-PORTAUTHORIZED: Port gi1/0/9 is Authorized

Cat1300-1#04-Jul-2024 20:50:45 %STP-W-PORTSTATUS: gi1/0/9: STP status Forwarding
```

الخطوة 10

سيؤدي إنهاء جلسة عمل CoA مع توقف المنفذ إلى إنهاء الجلسة الحالية وإرجاع المنفذ لمدة 10 ثوان ليصبح غير مصرح به. ثم تعود مرة أخرى إلى الإنترنت، وتصبح مصرح بها، ويمكنها إعادة توجيه الحزم.

```
Cat1300-1#04-Jul-2024 20:51:04 %SEC-W-COABNCEPORT: Interface gi1/0/9 suspended for 10 seconds by Co
A Request "bounce host port" for host 54:          :62
04-Jul-2024 20:51:04 %LINK-W-Down:  gi1/0/9
04-Jul-2024 20:51:22 %LINK-I-Up:  gi1/0/9
04-Jul-2024 20:51:22 %SEC-W-PORTUNAUTHORIZED: Port gi1/0/9 is unAuthorized
04-Jul-2024 20:51:22 %SEC-I-PORTAUTHORIZED: Port gi1/0/9 is Authorized
04-Jul-2024 20:51:29 %STP-W-PORTSTATUS: gi1/0/9: STP status Forwarding
```

الخطوة 11

سيقوم إنهاء جلسة عمل CoA مع إيقاف تشغيل المنفذ بإنهاء الجلسة وإغلاق المنفذ إدارياً.

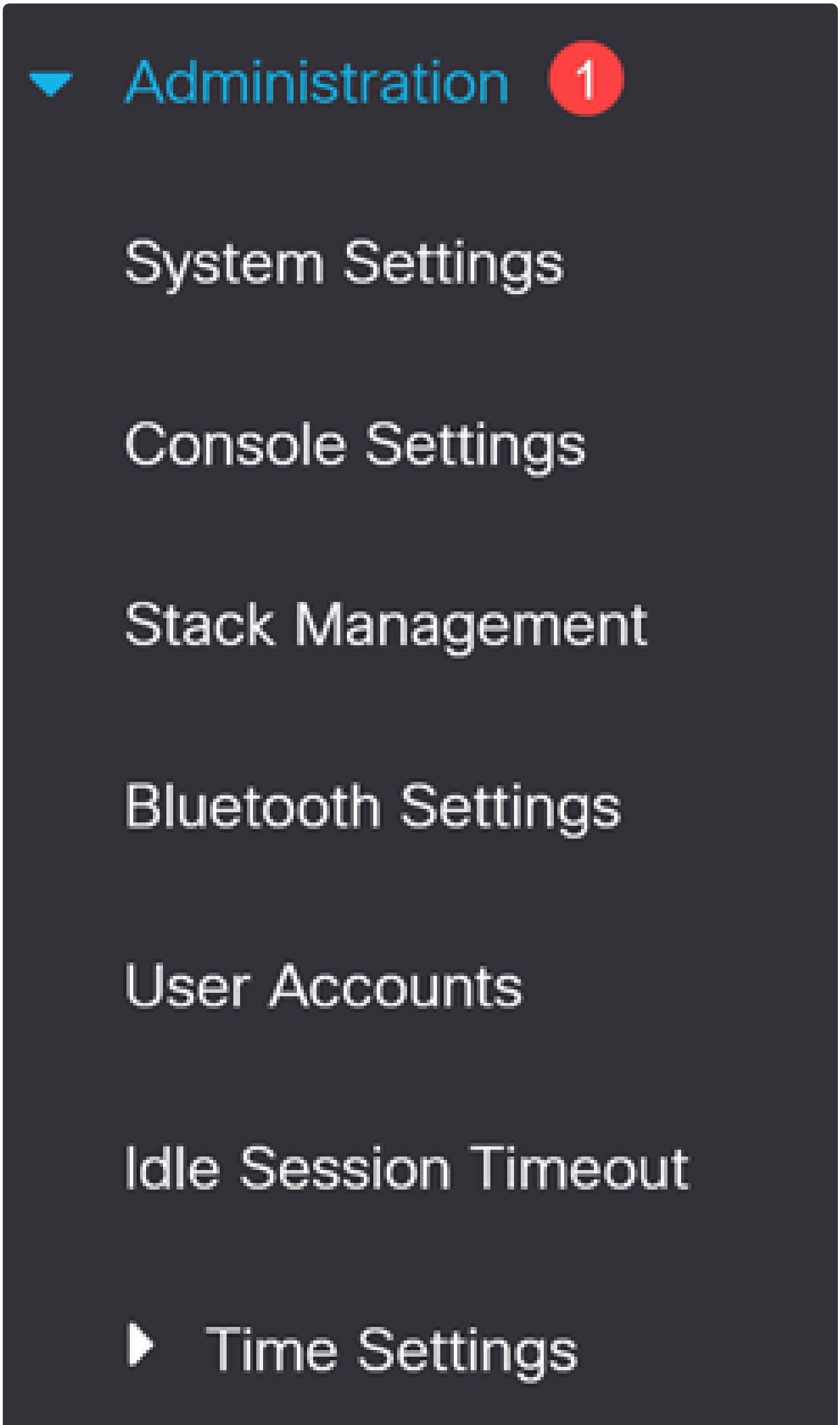
```
Cat1300-1#04-Jul-2024 20:51:47 %SEC-W-COADISPORT: Interface gi1/0/9 suspended by CoA Request "disab
le host port" for host 54:          :62
04-Jul-2024 20:51:47 %LINK-W-Down:  gi1/0/9
```

الخطوة 12

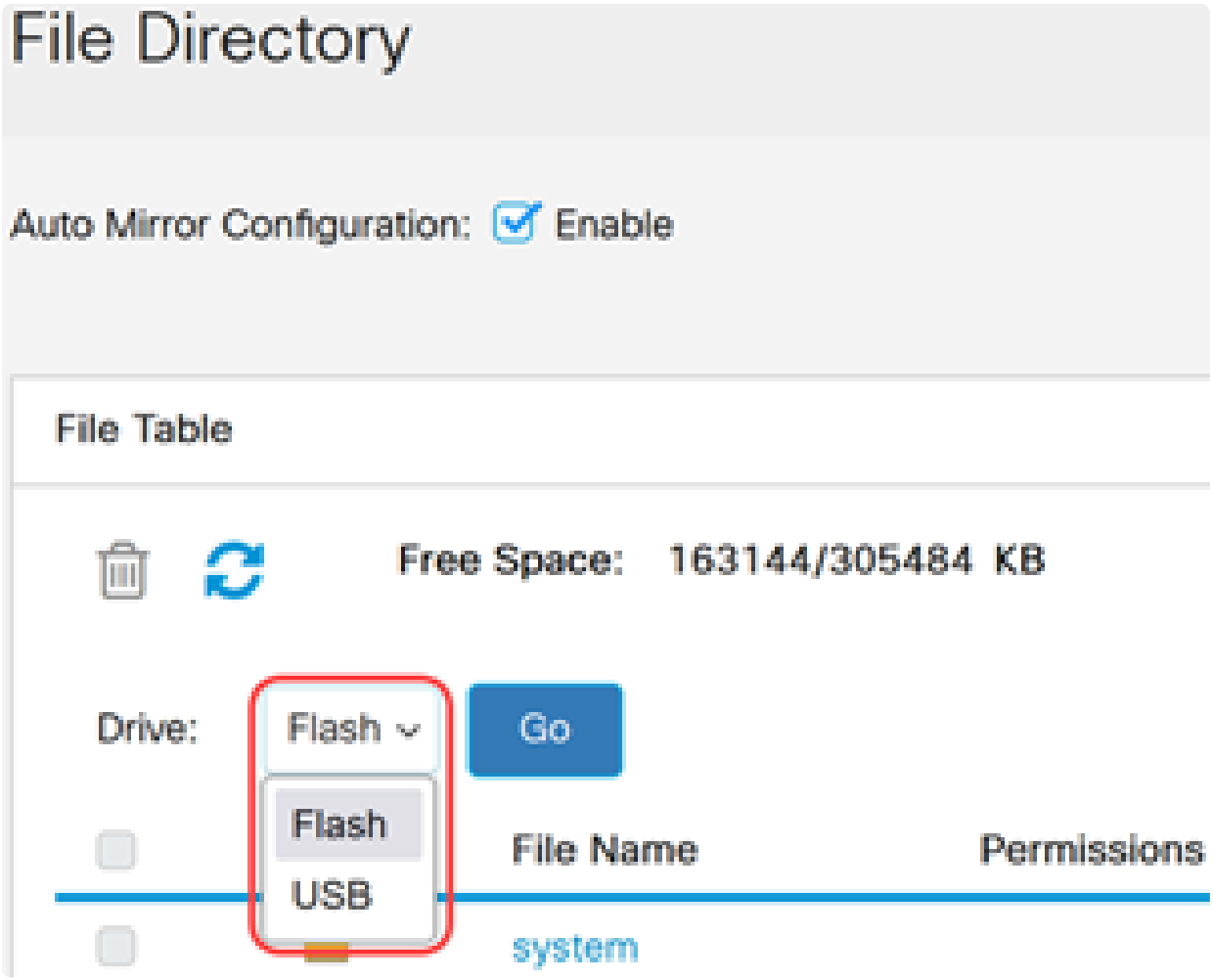
لإيقاف التقاط الحزمة، أستخدم الأمر monitor capture cap1 stop.

الخطوة 13

لنسخ الملفات، انتقل إلى إدارة > إدارة الملفات > دليل الملفات.


Administration
1
System Settings
Console Settings
Stack Management
Bluetooth Settings
User Accounts
Idle Session Timeout
Time Settings

يتوفر الأمر Flash الافتراضي. وبدلا من ذلك، يمكنك تحديد USB من القائمة المنسدلة محرك الأقراص.



القرار

الآن أنت تعرف كل حول ISE وكيف أن يشكل CoA في المادة حفازة 1300 sery مفتاح.

لمزيد من المعلومات، راجع الفيديو أدناه.

شاهد مقطع فيديو يتعلق بهذه المقالة...

انقر هنا لعرض Tech Talks (المحادثات التقنية) الأخيرة 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).