تكوين مصادقة ThreatGrid RADIUS عبر DTLS لمدخل وحدة التحكم و OPadmin

المحتويات

المقدمة

يصف هذا المستند ميزة مصادقة طلب المصادقة عن بعد في خدمة المستخدم (RADIUS) التي تم تقديمها في الإصدار 2.10 من ThreatGrid (TG). وهو يسمح للمستخدمين بتسجيل الدخول إلى مدخل الإدارة وبوابة وحدة التحكم مع بيانات الاعتماد المخزنة في خادم المصادقة والتفويض والمحاسبة (AAA).

في هذا المستند، تجد الخطوات الضرورية لتكوين الميزة.

المتطلبات الأساسية

المتطلبات

- ThreatGrid الإصدار 2.10 أو أعلى
- خادم AAA الذي يدعم مصادقة RADIUS عبر DTLS (draft-ietf-radext-dtls-04)

المكونات المستخدمة

- جهاز ThreatGrid 2.10
- Identity Services Engine (ISE)، الإصدار 2.7

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 مباشرة، فتأكد من فهمك للتأثير المحتمل لأي أمر.

التكوين

يقدم هذا القسم إرشادات تفصيلية حول كيفية تكوين جهاز ThreatGrid وميزة ISE لميزة مصادقة RADIUS.

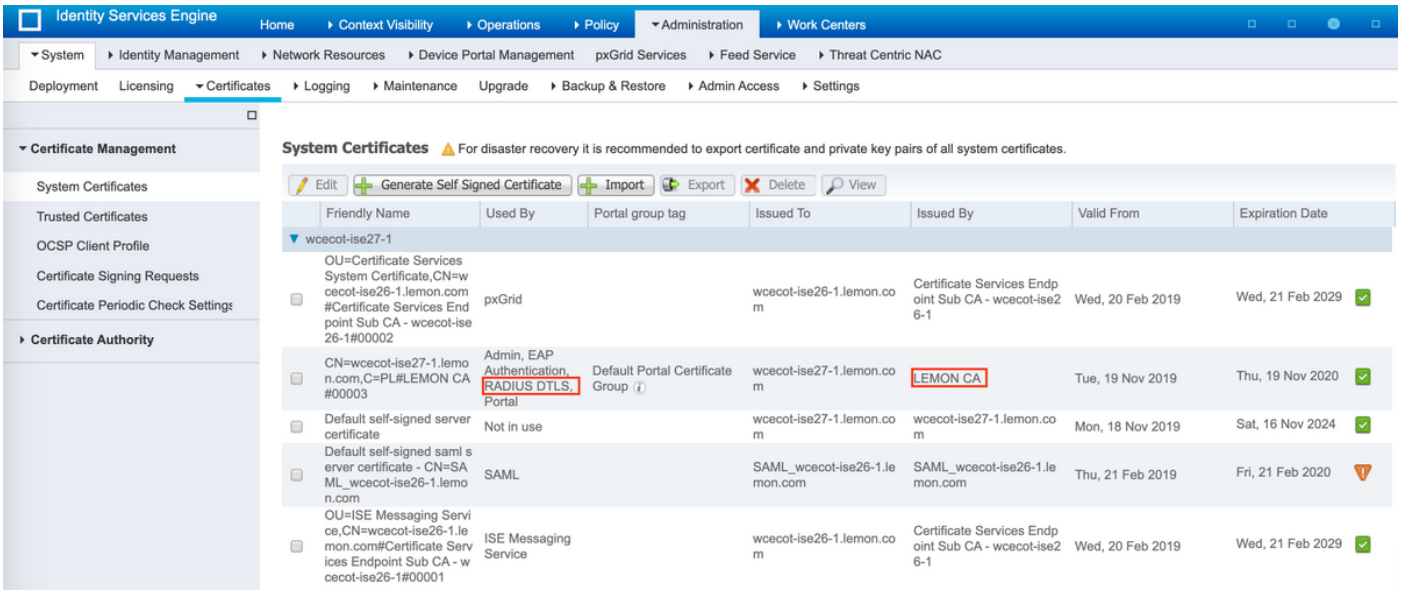
ملاحظة: من أجل تكوين المصادقة، تأكد من السماح بالاتصال على المنفذ UDP 2083

بين واجهة ThreatGrid الظيفة وعقدة خدمة سياسة ISE (PSN).

التكوين

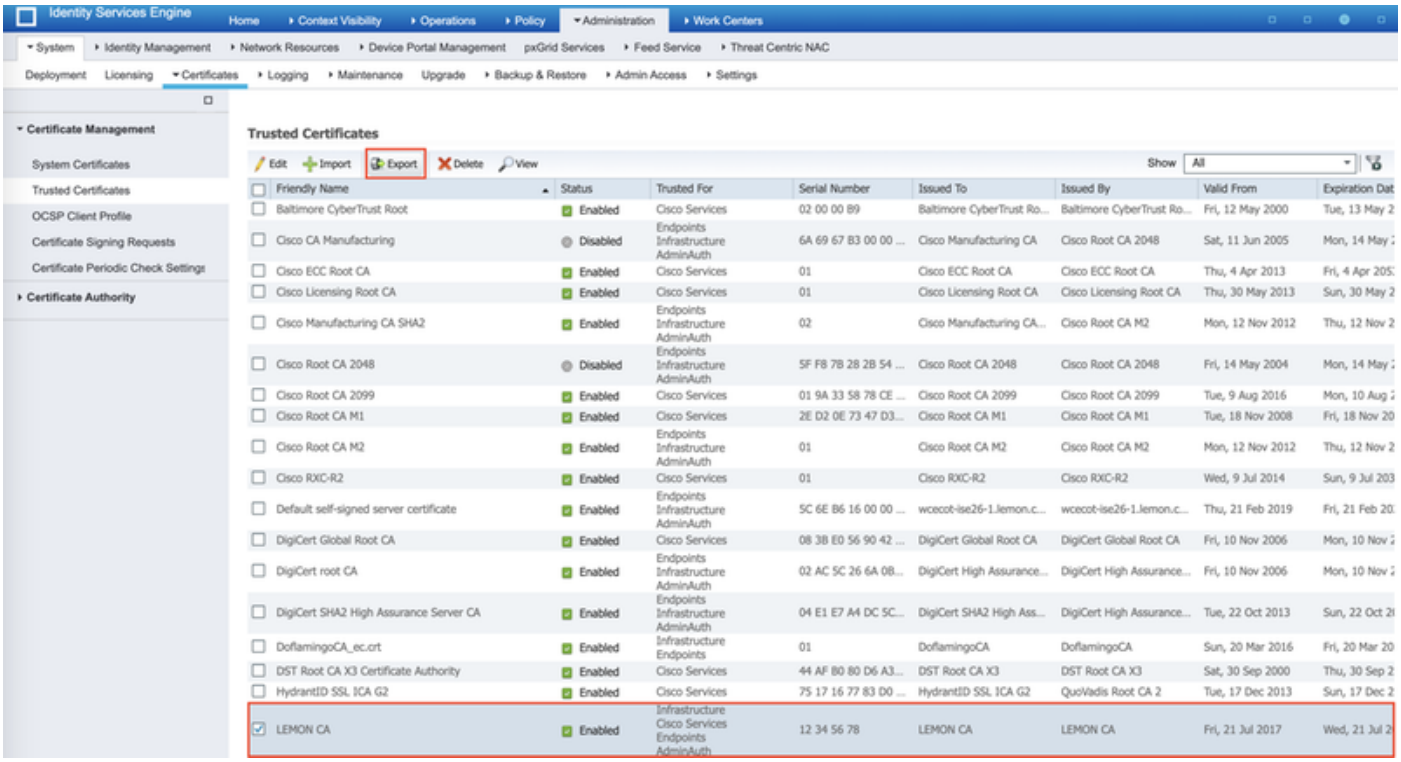
الخطوة 1. إعداد شهادة ThreatGrid للمصادقة.

يستخدم RADIUS عبر DTLS مصادقة الشهادات المتبادلة مما يعني أن شهادة المرجع المصدق (CA) من ISE مطلوبة. تحقق أولا من شهادة RADIUS DTLS الموقعة من CA:



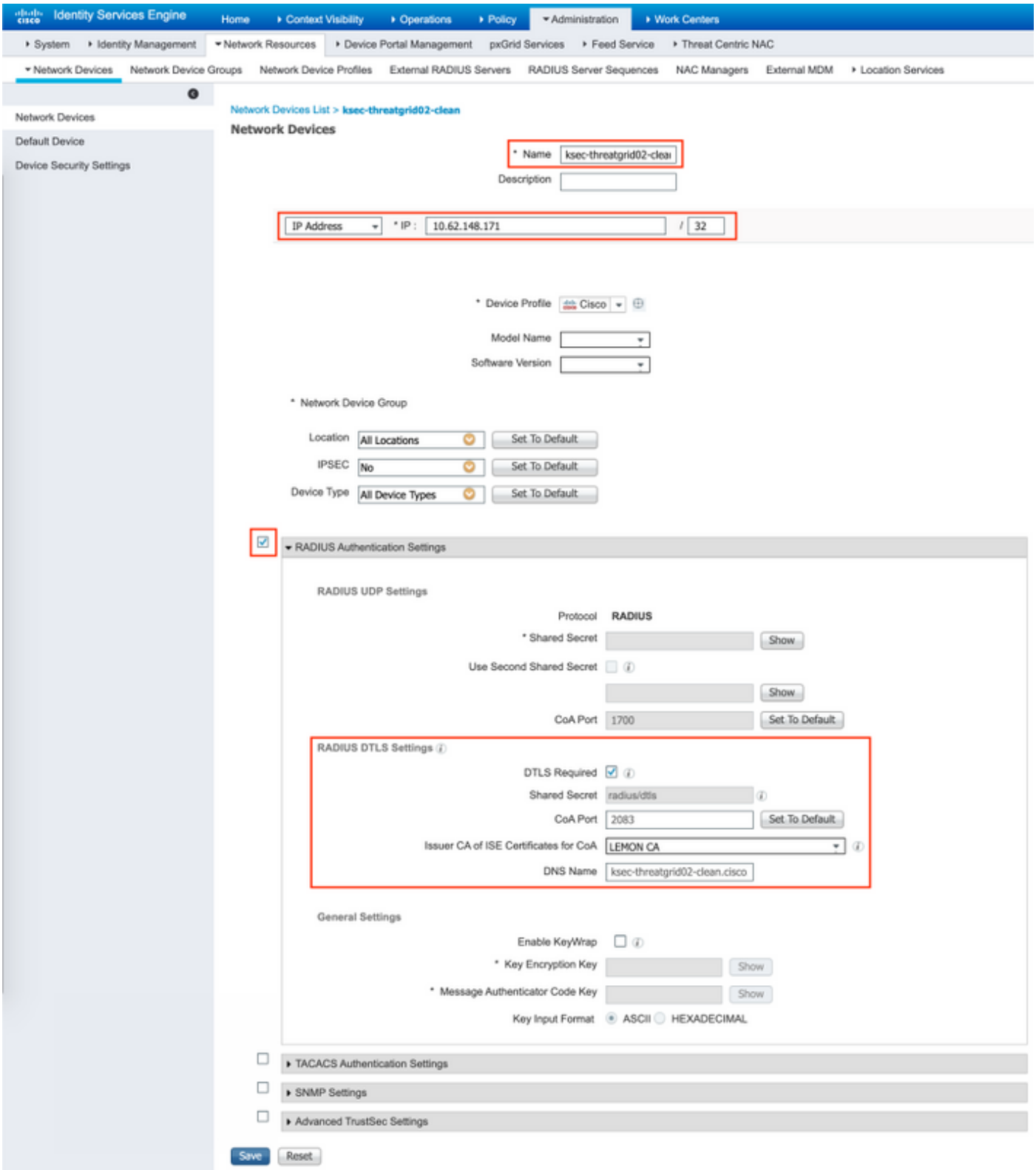
الخطوة 2. تصدير شهادة المرجع المصدق من ISE.

انتقل إلى **إدارة > نظام > شهادات > إدارة شهادات > شهادات موثوق بها**، حدد مكان المرجع المصدق، حدد **تصدير** كما هو موضح في الصورة، ثم احفظ الشهادة على القرص لوقت لاحق:



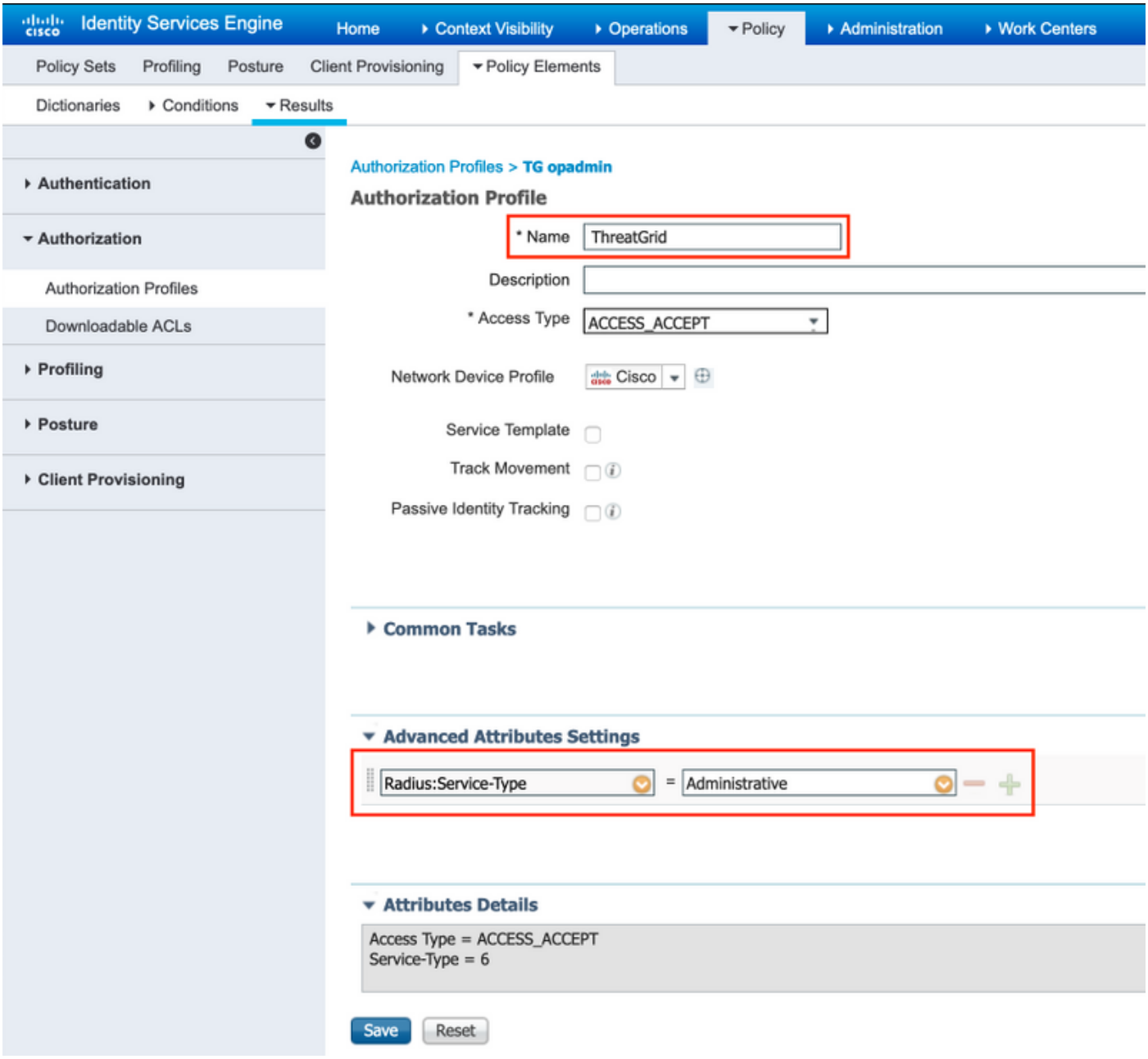
الخطوة 3. إضافة ThreatGrid كجهاز وصول إلى الشبكة.

انتقل إلى **إدارة > موارد الشبكة > أجهزة الشبكة > إضافة** لإنشاء إدخال جديد لـ TG وأدخل **الاسم**، **عنوان IP** للواجهة النظيفة وحدد **DTLS المطلوب** كما هو موضح في الصورة. انقر فوق **حفظ**" في الأسفل:



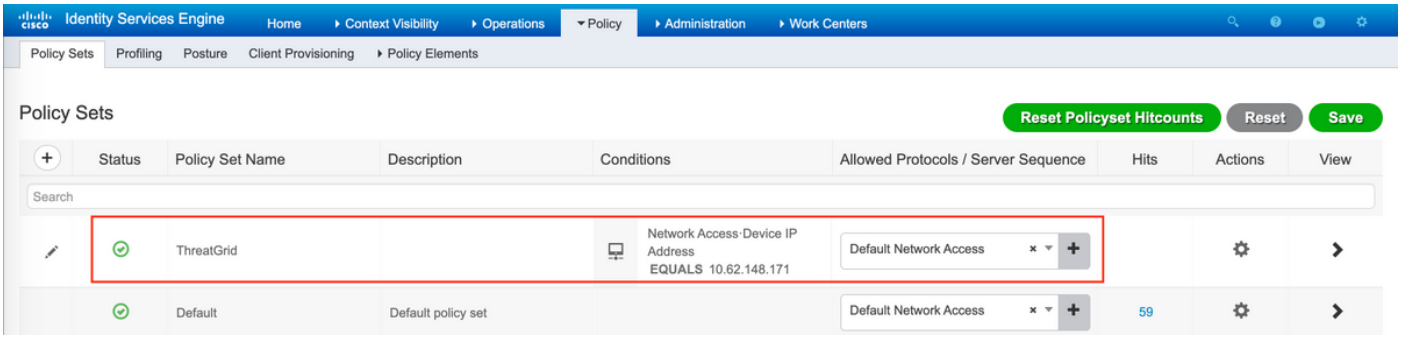
الخطوة 4. إنشاء ملف تعريف تخويل لنهج التخويل.

انتقل إلى **السياسة > عناصر السياسة > النتائج > التخويل > توصيفات التخويل** وانقر على **إضافة**. أدخل **الاسم** وحدد **إعدادات الخصائص المتقدمة** كما هو موضح في الصورة وانقر **حفظ**:



الخطوة 5. إنشاء سياسة مصادقة.

انتقل إلى **السياسة > مجموعات السياسات** وانقر فوق **+**". أدخل **اسم** مجموعة النهج وقم بتعيين الشرط إلى **NAD IP Address**، المعين إلى واجهة TG النظيفة، انقر فوق **حفظ** كما هو موضح في الصورة:



الخطوة 6. إنشاء سياسة تخويل.

انقر فوق **>**" للانتقال إلى نهج التخويل، وقم بتوسيع نهج التخويل، وانقر فوق **+**"، ثم قم

بالتكوين كما هو موضح في الصورة، بعد الانتهاء انقر فوق **حفظ**:

تلميح: يمكنك إنشاء قاعدة تفويض واحدة لكافة المستخدمين الذين تطابق كل الشرطين والمسؤول وواجهة المستخدم.

الخطوة 7. إنشاء شهادة هوية ل ThreatGrid.

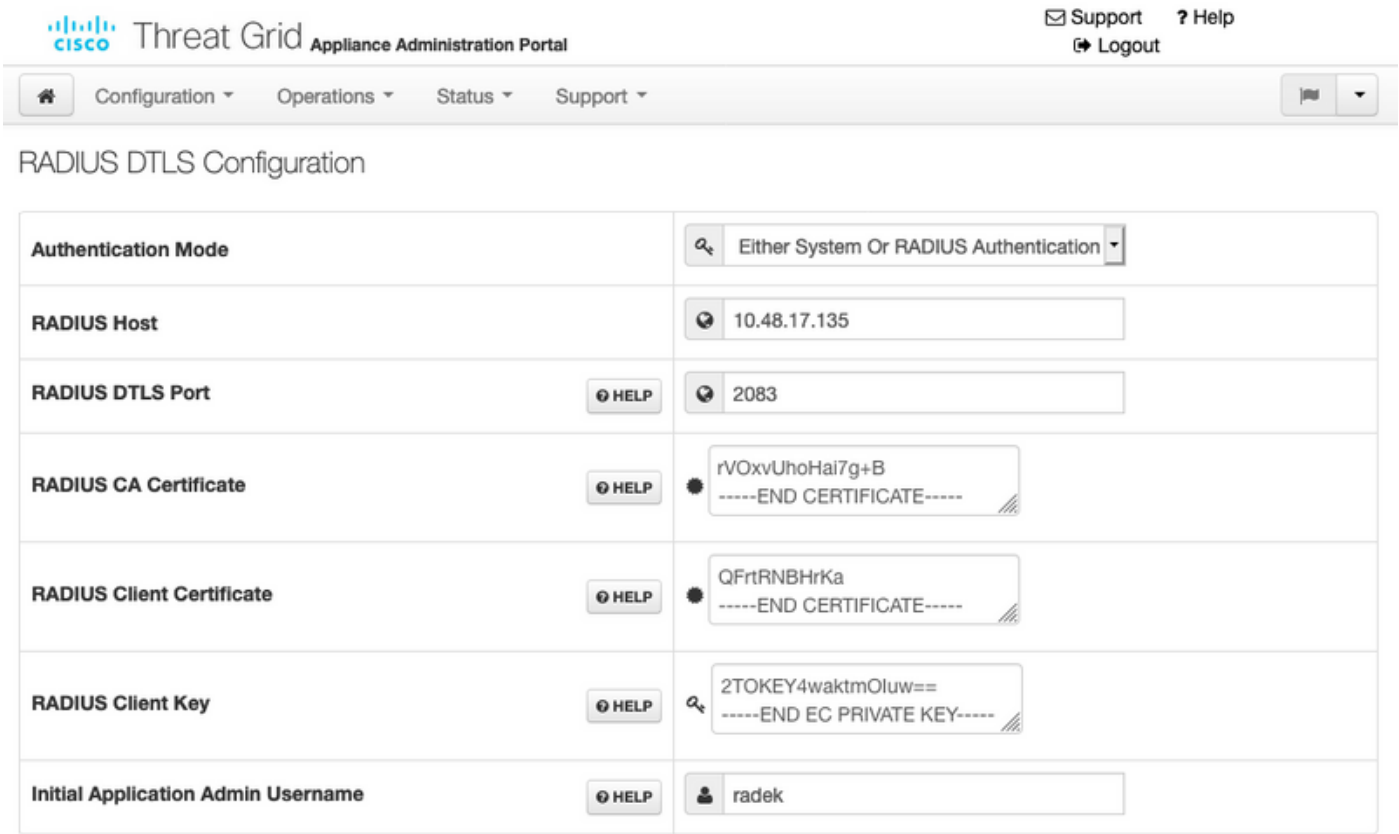
يجب أن تستند شهادة عميل ThreatGrid إلى مفتاح المنحنى البيضاوي:

```
openssl ecparam -name secp521r1 -genkey -out private-ec-key.pem
```

يجب أن يتم التوقيع عليها من قبل هيئة النزاهة التي يثق بها ISE. تحقق من *استيراد الشهادات الجذر إلى* صفحة *مخزن الشهادات الموثوق بها* للحصول على مزيد من المعلومات حول كيفية إضافة شهادة مرجع مصدق إلى مخزن شهادات ISE الموثوق به.

الخطوة 8. تكوين ThreatGrid لاستخدام RADIUS.

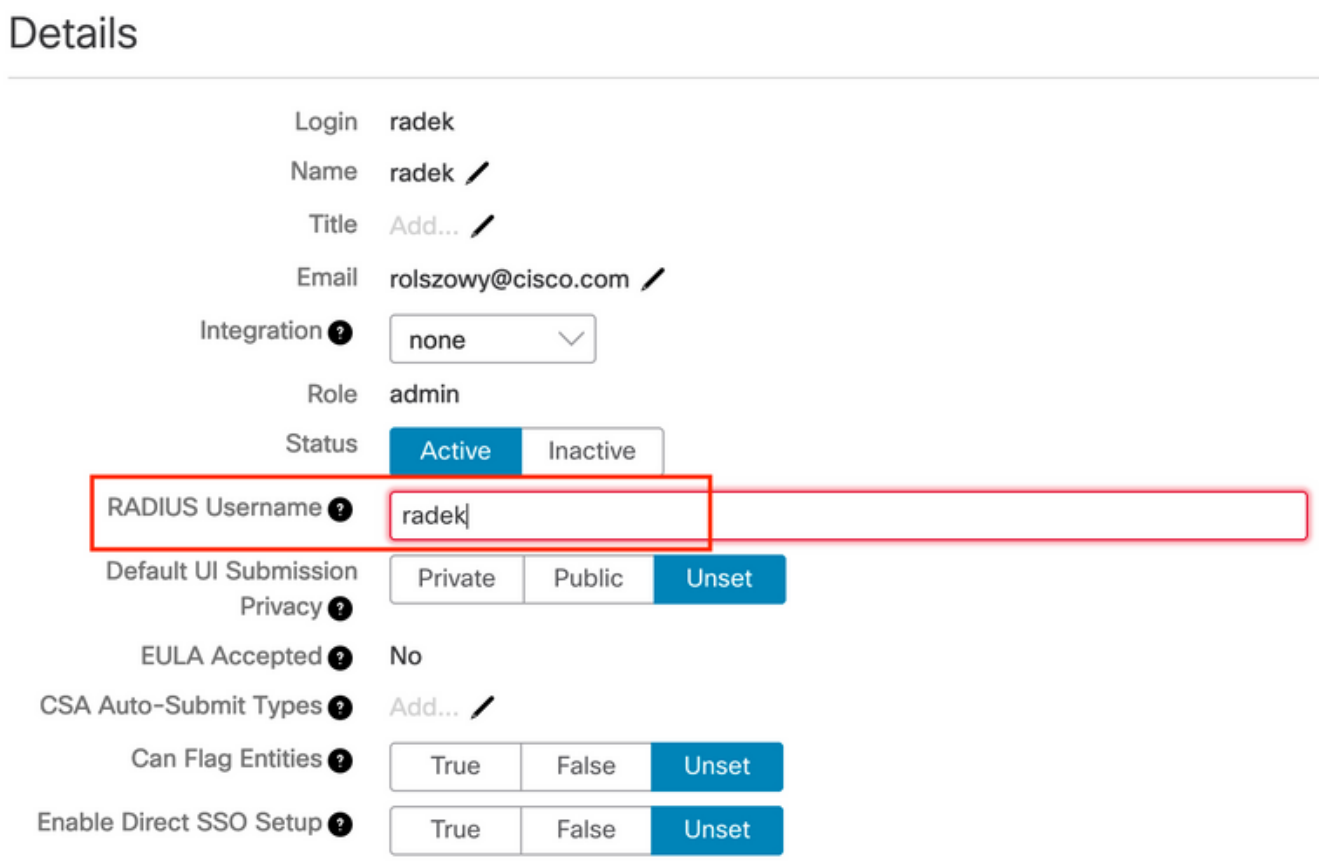
قم بتسجيل الدخول إلى مدخل المسؤول، انتقل إلى **التكوين>RADIUS**. في شهادة RADIUS CA الصق محتوى ملف PEM الذي يتم تجميعه من ISE، في الشهادة المنسقة PEM الخاصة بالصق شهادة العميل والمستلمة من CA وفي محتوى لصق مفتاح العميل الخاص بملف private-ec-key.pem من الخطوة السابقة كما هو موضح في الصورة. طقطقة **حفظ**:



ملاحظة: يجب إعادة تكوين جهاز TG بعد حفظ إعدادات RADIUS.

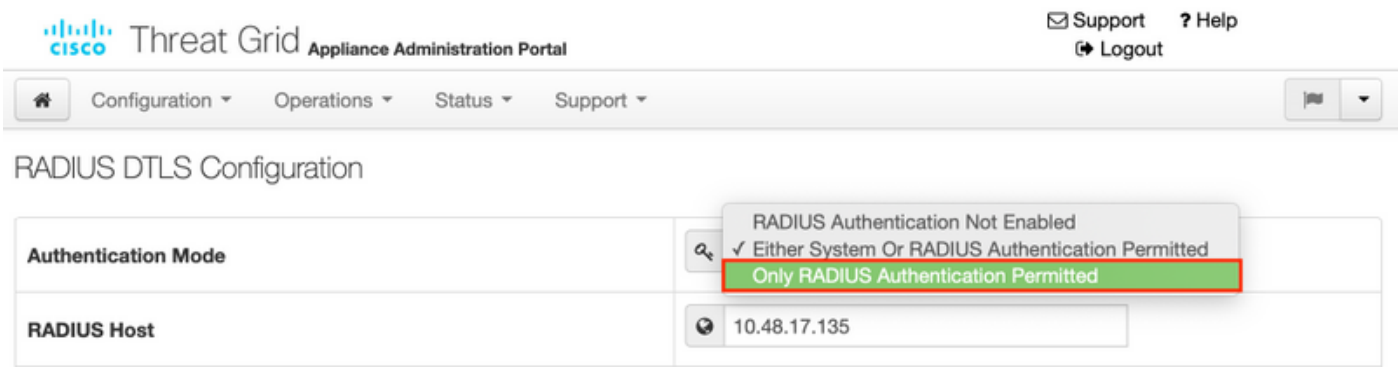
الخطوة 9. إضافة اسم مستخدم RADIUS لمستخدمي وحدة التحكم.

لتسجيل الدخول إلى مدخل وحدة التحكم، يجب إضافة سمة اسم مستخدم RADIUS إلى المستخدم الخاص كما هو موضح في الصورة:



الخطوة 10. تمكين مصادقة RADIUS فقط.

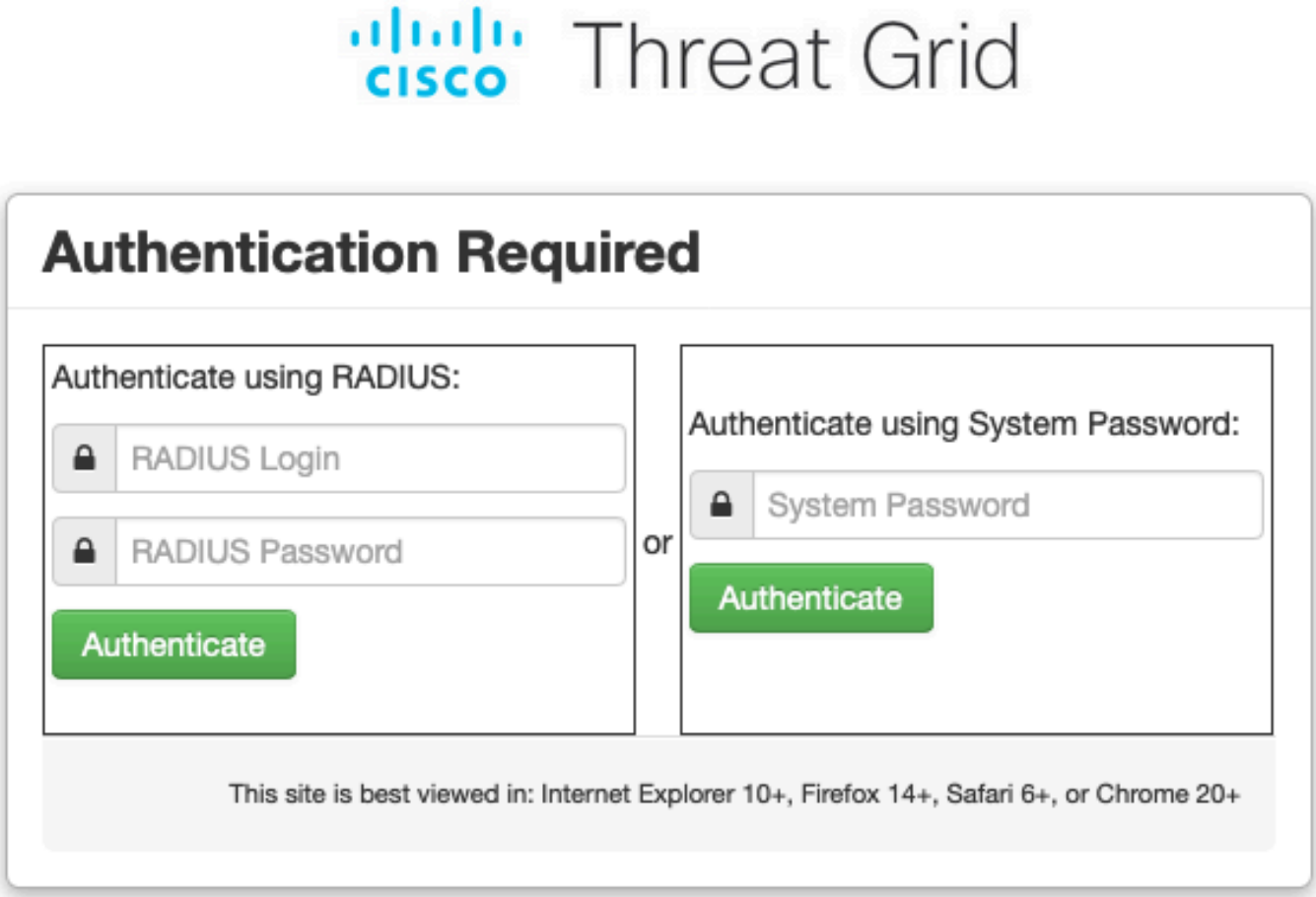
بعد تسجيل الدخول الناجح إلى مدخل المسؤول، يظهر خيار جديد، والذي يعطل مصادقة النظام المحلي تمامًا ويترك فقط مصادقة مستندة إلى RADIUS.

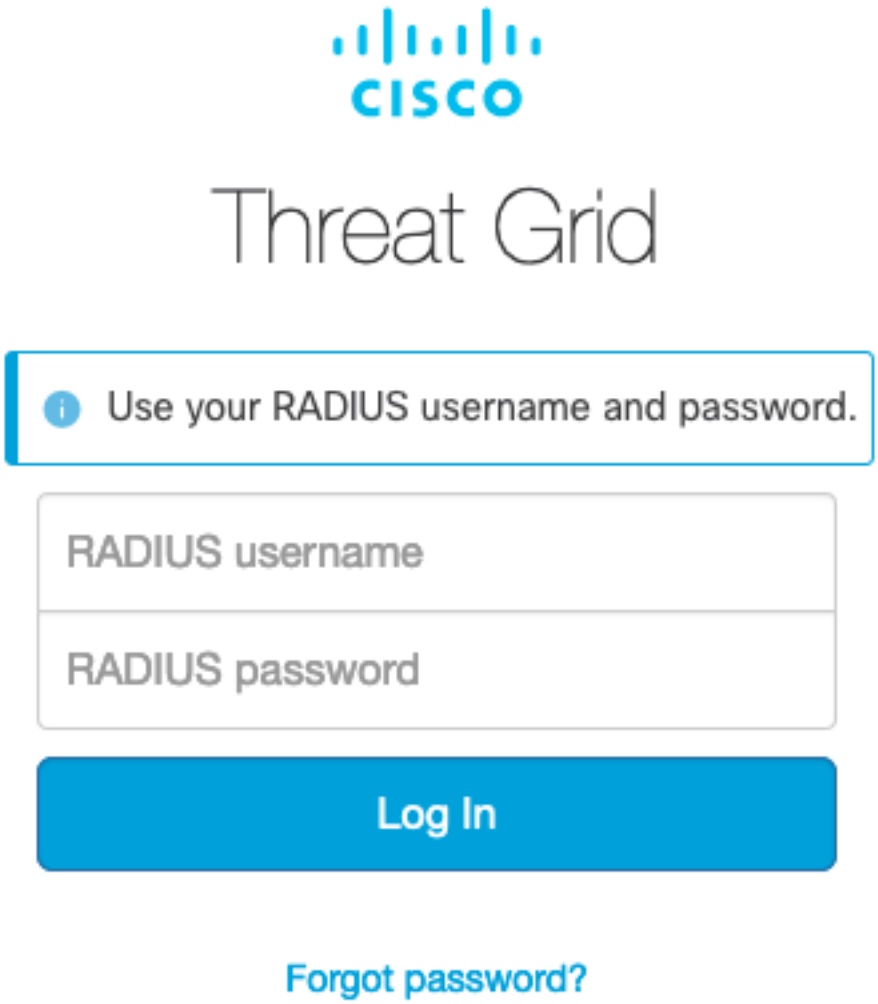


التحقق من الصحة

بعد إعادة تكوين TG، قم بتسجيل الخروج، والآن يدوي تسجيل الدخول إلى الصفحات كما هو

الحال في مدخل الصور والمسؤول ووحدة التحكم على التوالي:



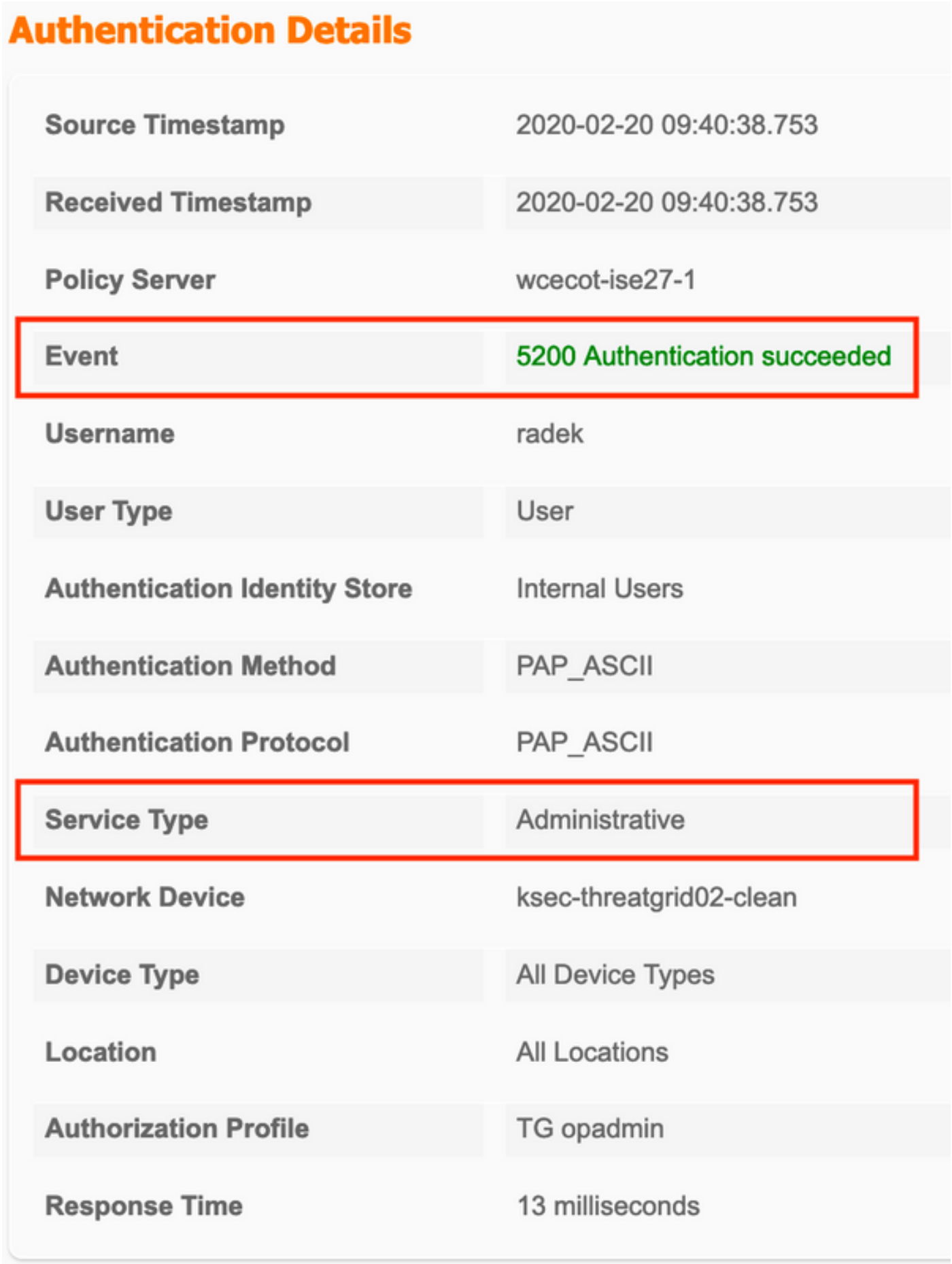


استكشاف الأخطاء وإصلاحها

هناك ثلاثة مكونات يمكن أن تسبب مشاكل: ISE واتصال الشبكة و ThreatGrid.

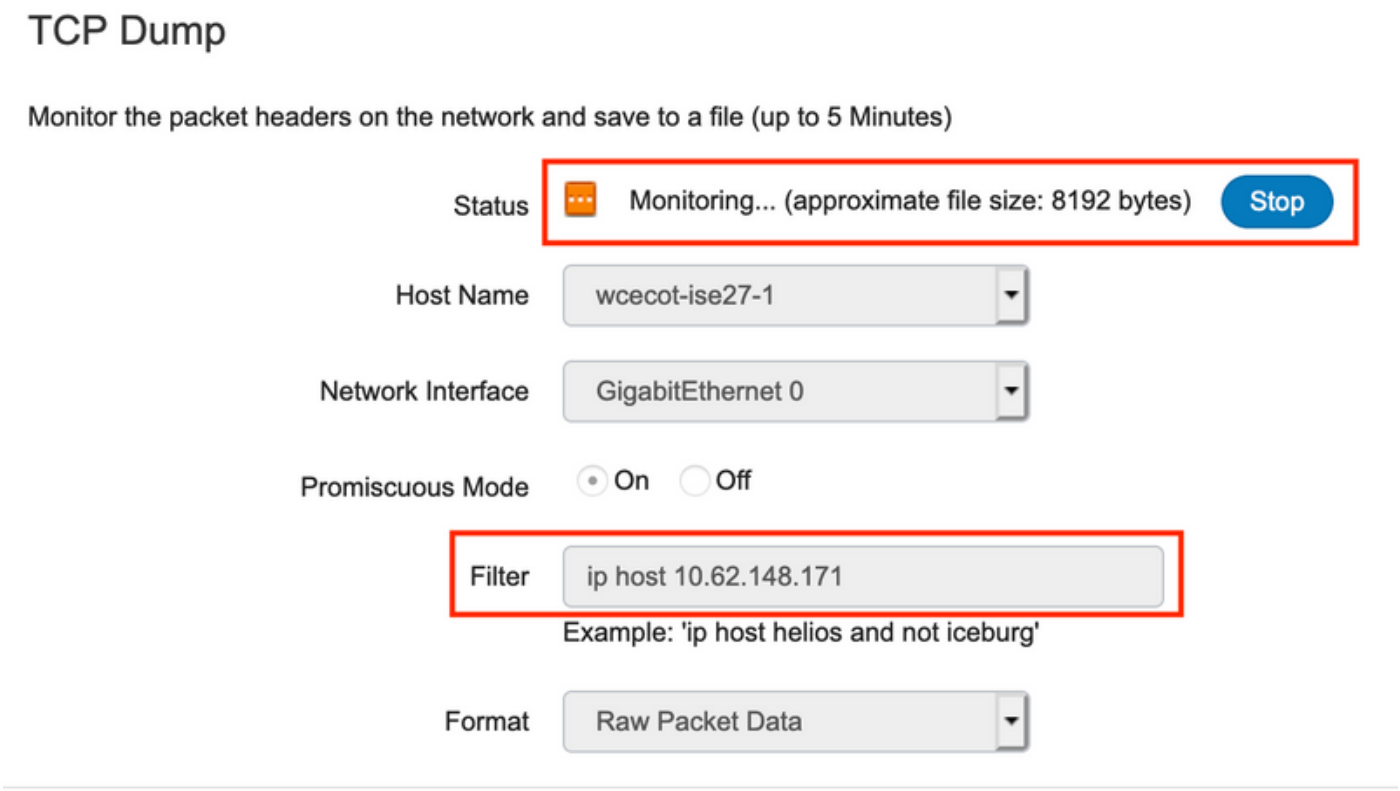
- في ISE، تأكد من أنها ترجع ServiceType=Administrative إلى طلبات مصادقة ThreatGrid. انتقل إلى **العمليات>RADIUS>السجلات المباشرة** على ISE وحدد التفاصيل:

Time	Status	Details	Repeat ...	Identity	Authentication Policy	Authorization Policy	Authorizati...	Network Device
×				Identity	ThreatGrid ×	Authorization Policy	Authorization	Network Device
Feb 20, 2020 09:40:38.753 AM	✓			radek	ThreatGrid >> Default	ThreatGrid >> ThreatGrid Admin	TG opadmin	ksec-threatgrid02-clean
Feb 20, 2020 09:40:18.260 AM	✓			radek	ThreatGrid >> Default	ThreatGrid >> ThreatGrid Console	TG console	ksec-threatgrid02-clean



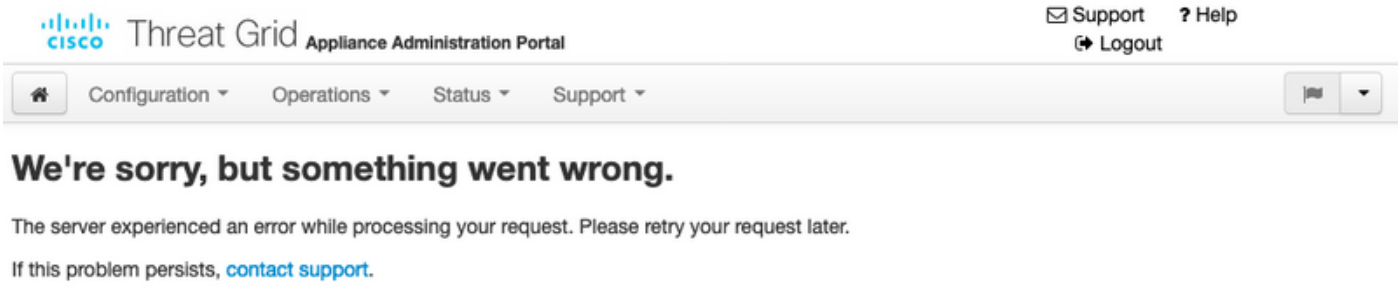
- إذا لم تكن ترى هذه الطلبات، فعليك التقاط حزمة على ISE. انتقل إلى **العمليات>تشخيص>أدوات** التشخيص **TCP**، ووفر حقل IP في عامل التصفية الخاص بواجهة **التنظيف الخاصة** ب TG، **انقر فوق** بدء **وحاول تسجيل**

الدخول إلى ThreatGrid:



يجب أن ترى عدد وحدات البايت التي تمت زيادتها. افتح ملف PCAP في Wireshark للحصول على مزيد من المعلومات.

- إذا رأيت الخطأ "أنسف، ولكن حدث خطأ ما" بعد النقر فوق "حفظ في ThreatGrid" والصفحة تبدو كما يلي:



وهذا يعني أنك على الأرجح قد أستخدمت مفتاح RSA لشهادة العميل. يجب إستخدام مفتاح ECC مع المعلمات المحددة في الخطوة 7.

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).