تكامل Cisco Threat Response (CTR) و ESA

المحتويات

المقدمة

يصف هذا المستند عملية دمج الاستجابة للتهديدات من Cisco (CTR) مع جهاز أمان البريد الإلكتروني (ESA) وكيفية التحقق من ذلك من أجل إجراء بعض تحقيقات CTR.

المتطلبات الأساسية

المتطلبات

توصي Cisco بأن تكون لديك معرفة بالمواضيع التالية:

- إستجابة تهديدات الحماية من Cisco
- أجهزة أمان البريد الإلكتروني

المكونات المستخدمة

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

- حساب CTR

- تبادل خدمات الأمان من Cisco
- ESA C100V على برنامج الإصدار 13.0.0-392

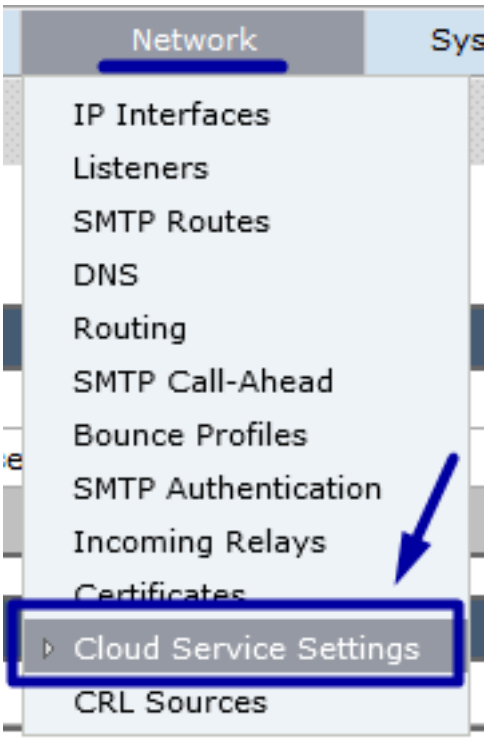
تم إنشاء المعلومات الواردة في هذا المستند من الأجهزة الموجودة في بيئة معملية خاصة. بدأت جميع الأجهزة المُستخدمة في هذا المستند بتكوين ممسوح (افتراضي). إذا كانت شبكتك قيد التشغيل، فتأكد من فهمك للتأثير المحتمل لأي أمر.

التكوين

لتكوين CTR الخاص بالتكامل و ESA، قم بتسجيل الدخول إلى الجهاز الظاهري لأمان البريد الإلكتروني واتبع الخطوات السريعة التالية:

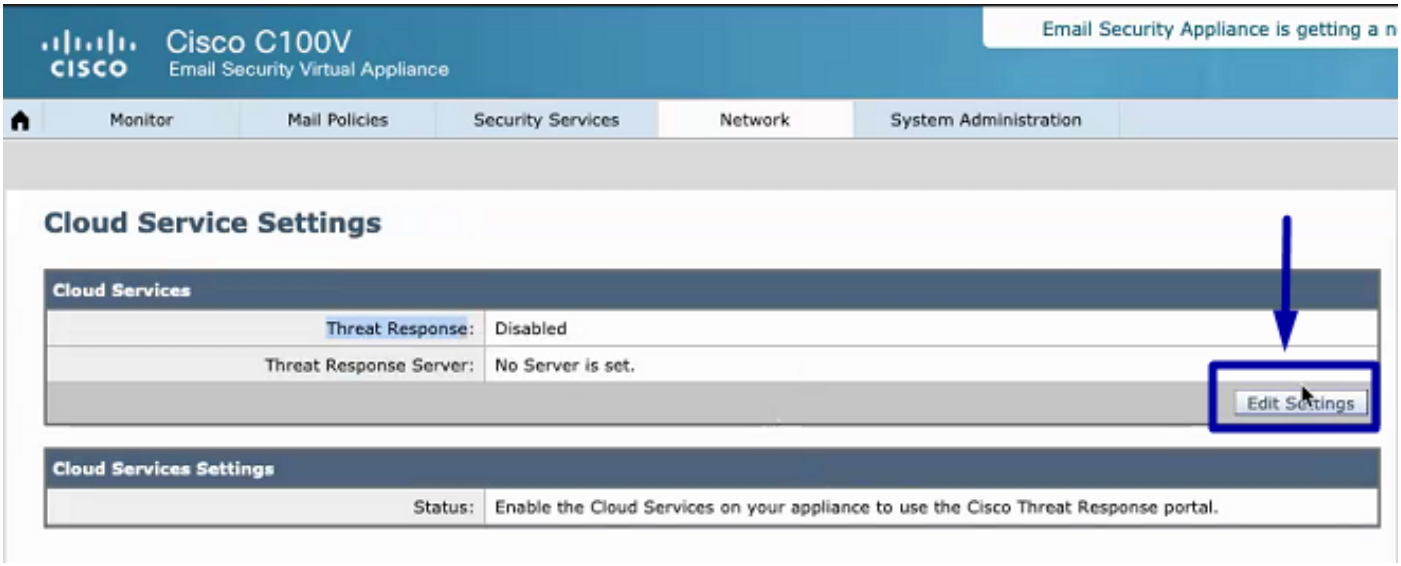
الخطوة 1. انتقل إلى شبكة > إعدادات خدمة السحابة

ما إن في ال ESA، انتقل إلى قائمة السياق شبكة > إعدادات خدمة السحابة، in order to رأيت الحالي تمديد حالة الاستجابة (معطل / ممكن) كما هو موضح في الصورة.



الخطوة 2. انقر على تحرير الإعدادات

حتى الآن أعجزت ميزة الاستجابة للتمديدات في ESA، in order to مكنت السمة، طقطقت على تحرير الإعدادات كما هو موضح في الصورة:



الخطوة 3. حدد خانة الاختيار تمكين وخادم الاستجابة للتهديدات

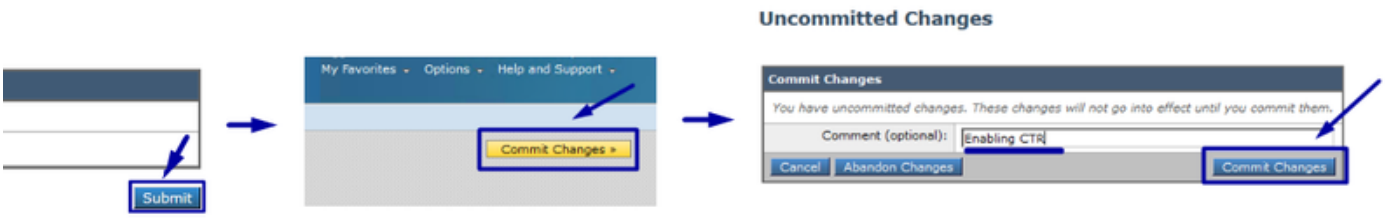
حدد خانة الاختيار "تمكين"، ثم أختر "خادم الاستجابة للتهديدات"، الرجاء مراجعة الصورة أدناه:

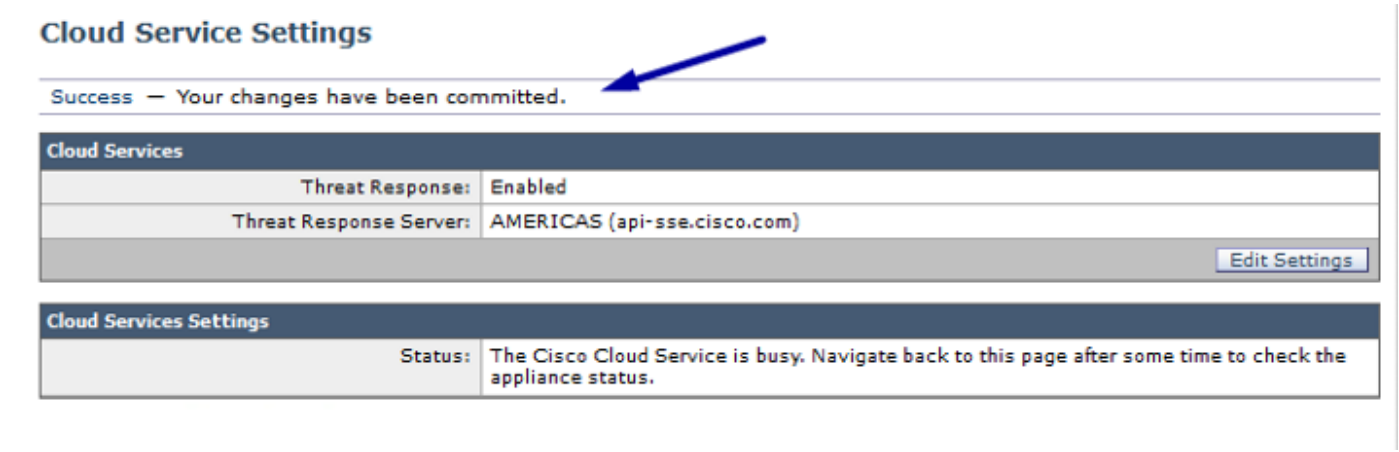
ملاحظة: يكون التحديد الافتراضي لعنوان URL الخاص بخادم الاستجابة للتهديدات هو AMERICAS (api-sse.cisco.com). بالنسبة للشركات الأوروبية، انقر فوق القائمة المنسدلة واختر أوروبا (api.eu.sse.itd.cisco.com)

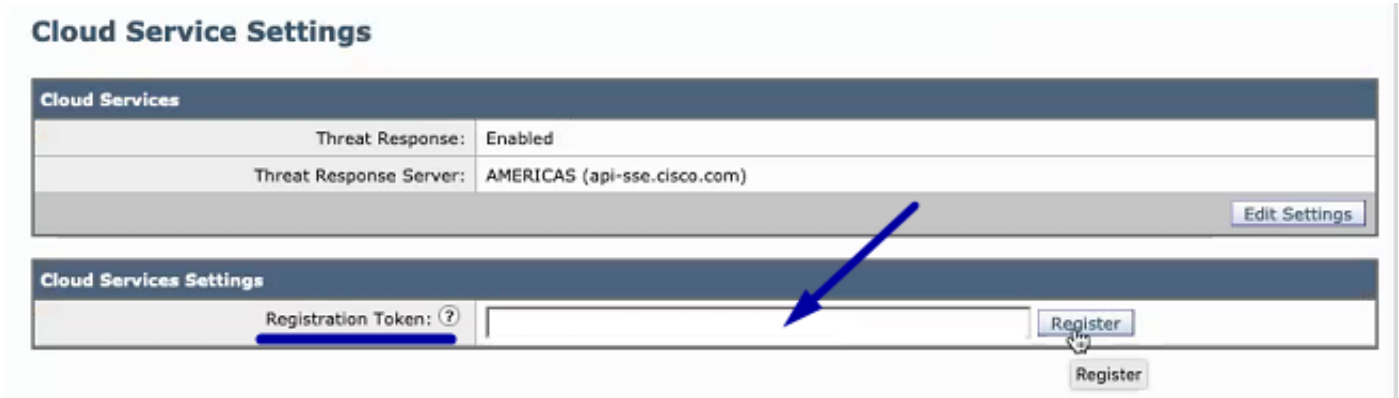
الخطوة 4. إرسال التغييرات وتنفيذها

يلزم إرسال التغييرات وتنفيذها، من أجل حفظ أي تغيير وتطبيقه. الآن إذا تم تحديث واجهة ESA، فيتم طلب رمز تسجيل مميز لتسجيل التسجيل الكامل، كما هو موضح في الصورة أدناه.

ملاحظة: يمكنك مشاهدة رسالة نجاح: تم تنفيذ التغييرات التي أجريتها.

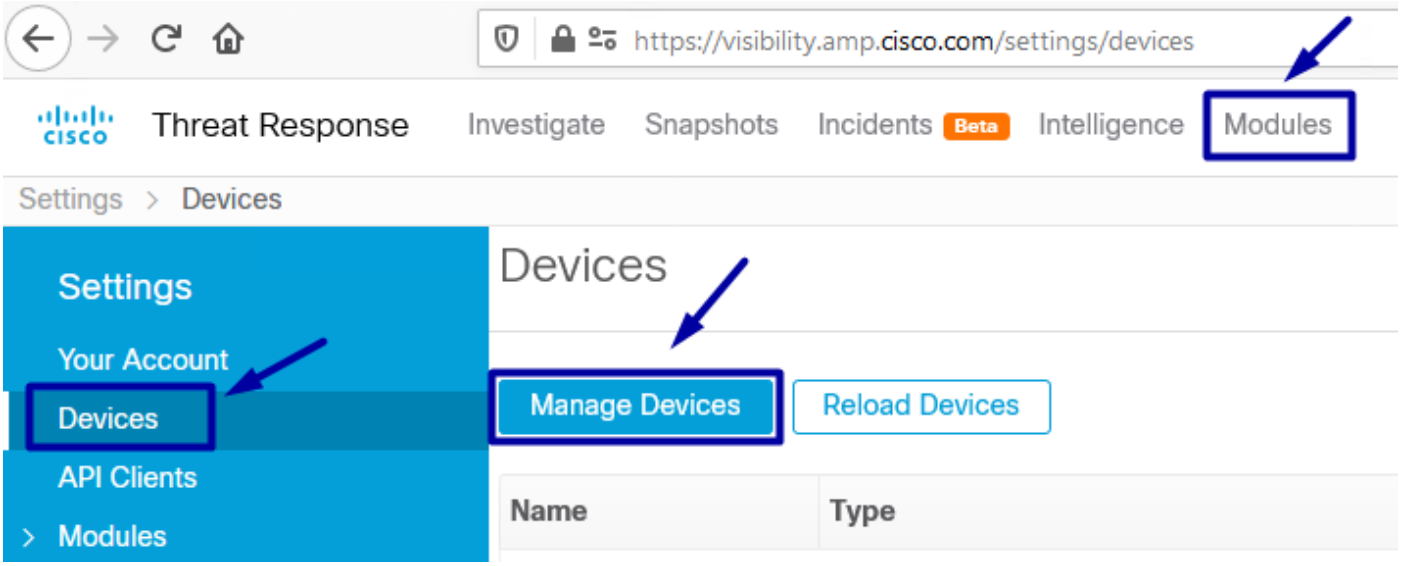




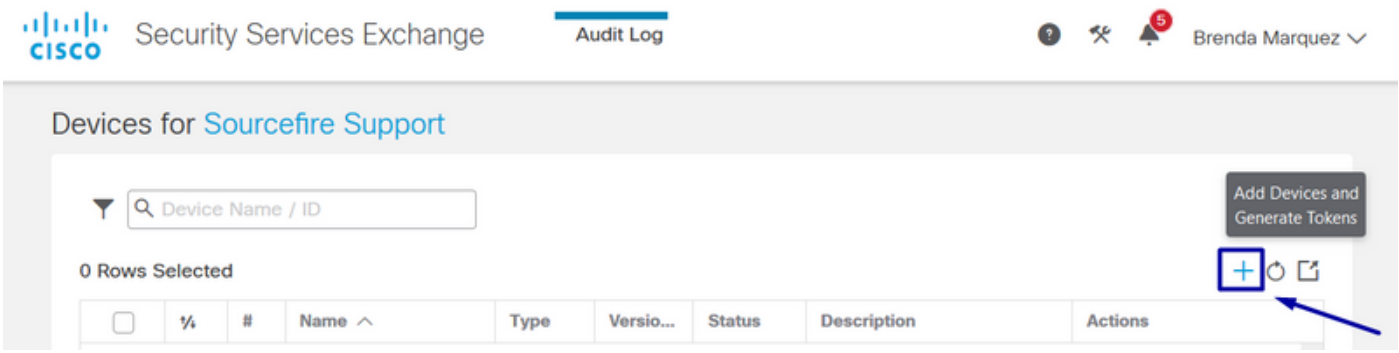


الخطوة 5. تسجيل الدخول إلى بوابة CTR وإنشاء رمز التسجيل المطلوب في ESA

1.- بمجرد أن تدخل إلى بوابة CTR، انتقل إلى وحدات > أجهزة > إدارة الأجهزة، الرجاء مشاهدة الصورة التالية.

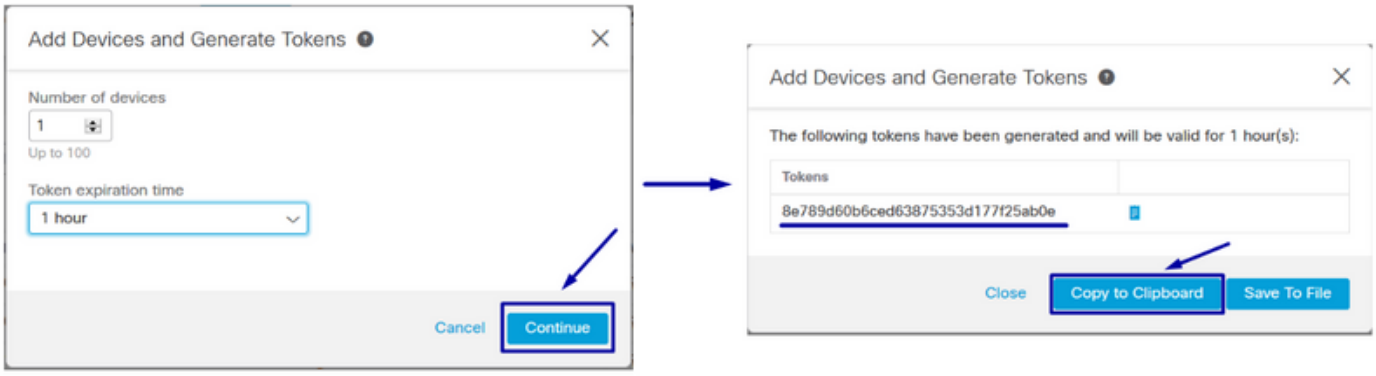


2.- تقوم إدارة إرتباط الأجهزة بإعادة توجيهك إلى تبادل خدمات الأمان (SSE)، بمجرد وصولك إلى هناك، انقر فوق الرمز إضافة أجهزة وإنشاء العلامات المميزة كما هو موضح في الصورة.



3.- انقر فوق "متابعة" لإنشاء الرمز المميز، بمجرد إنشاء الرمز المميز، انقر فوق "نسخ إلى الحافظة"، كما هو موضح في الصورة.

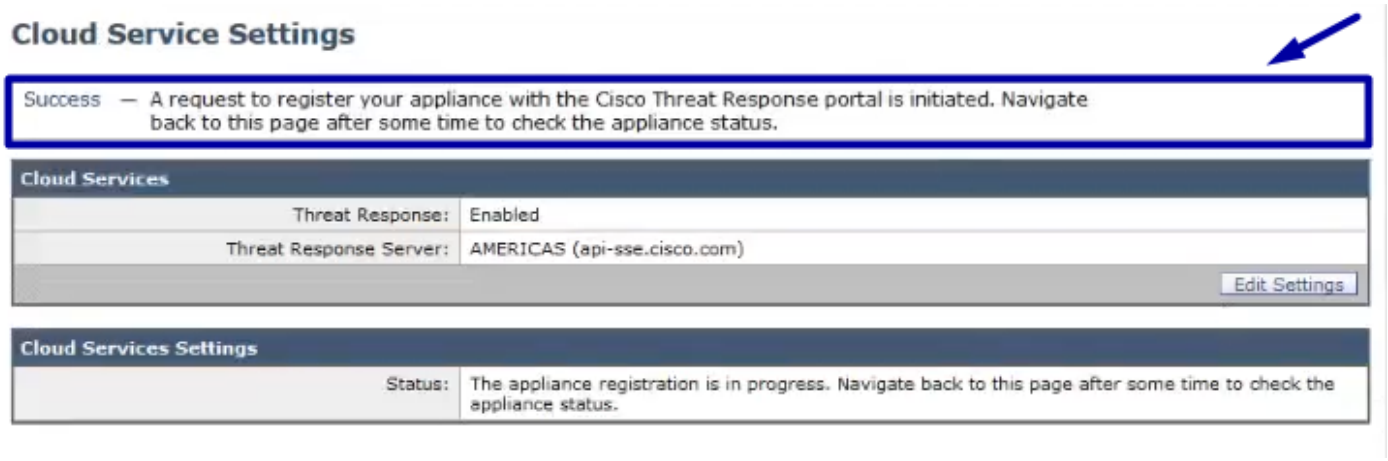
تلميح: يمكنك تحديد عدد الأجهزة التي تريد إضافتها (من 1 وما يصل إلى 100) وتحديد وقت انتهاء صلاحية الرمز المميز (1 ساعة و 2 ساعات و 4 ساعات و 6 ساعات و 8 ساعات و 12 ساعة و 01 يوم و 02 يوم و 03 أيام و 04 أيام و 05 أيام).



الخطوة 6. الصق رمز التسجيل (الذي تم إنشاؤه من مدخل CTR) في ESA

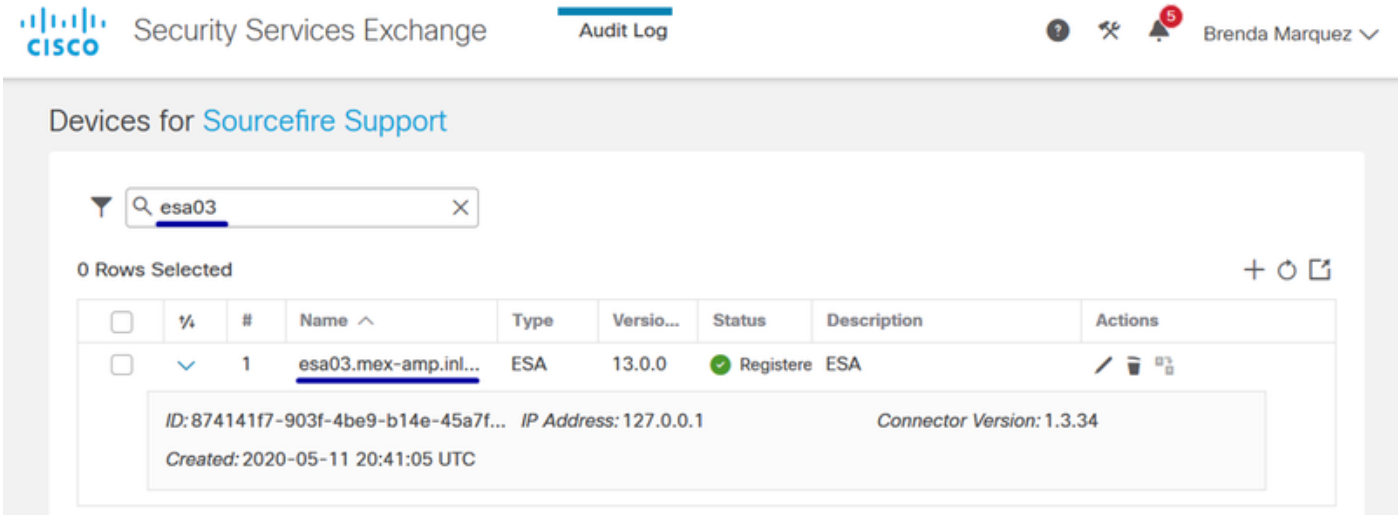
بمجرد إنشاء الرمز المميز للتسجيل، الصقه في قسم "إعدادات خدمات السحابة" في ESA، كالصورة أدناه.

ملاحظة: يمكنك مشاهدة رسالة نجاح: تم بدء طلب تسجيل الجهاز الخاص بك في بوابة الاستجابة لتهديدات Cisco. انتقل مرة أخرى إلى هذه الصفحة بعد مرور بعض الوقت للتحقق من حالة الجهاز.



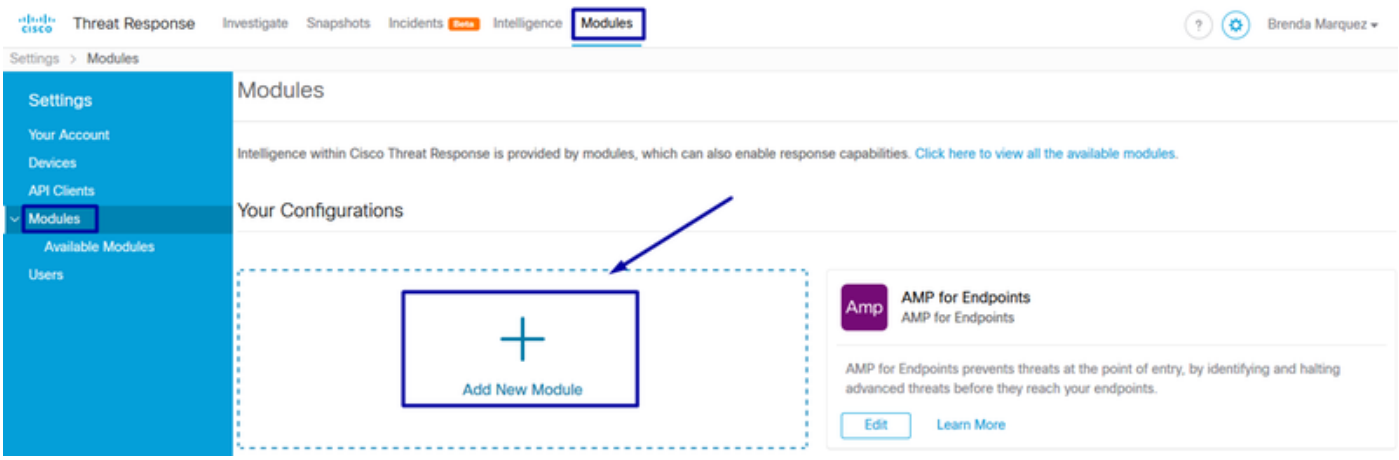
الخطوة 7. التحقق من وجود جهاز ESA في بوابة SSE

يمكنك الانتقال إلى بوابة SSE (CTR > وحدات > أجهزة > إدارة الأجهزة)، وفي علامة التبويب بحث بحث ابحث ابحث في جهاز ESA، كما هو موضح في الصورة.

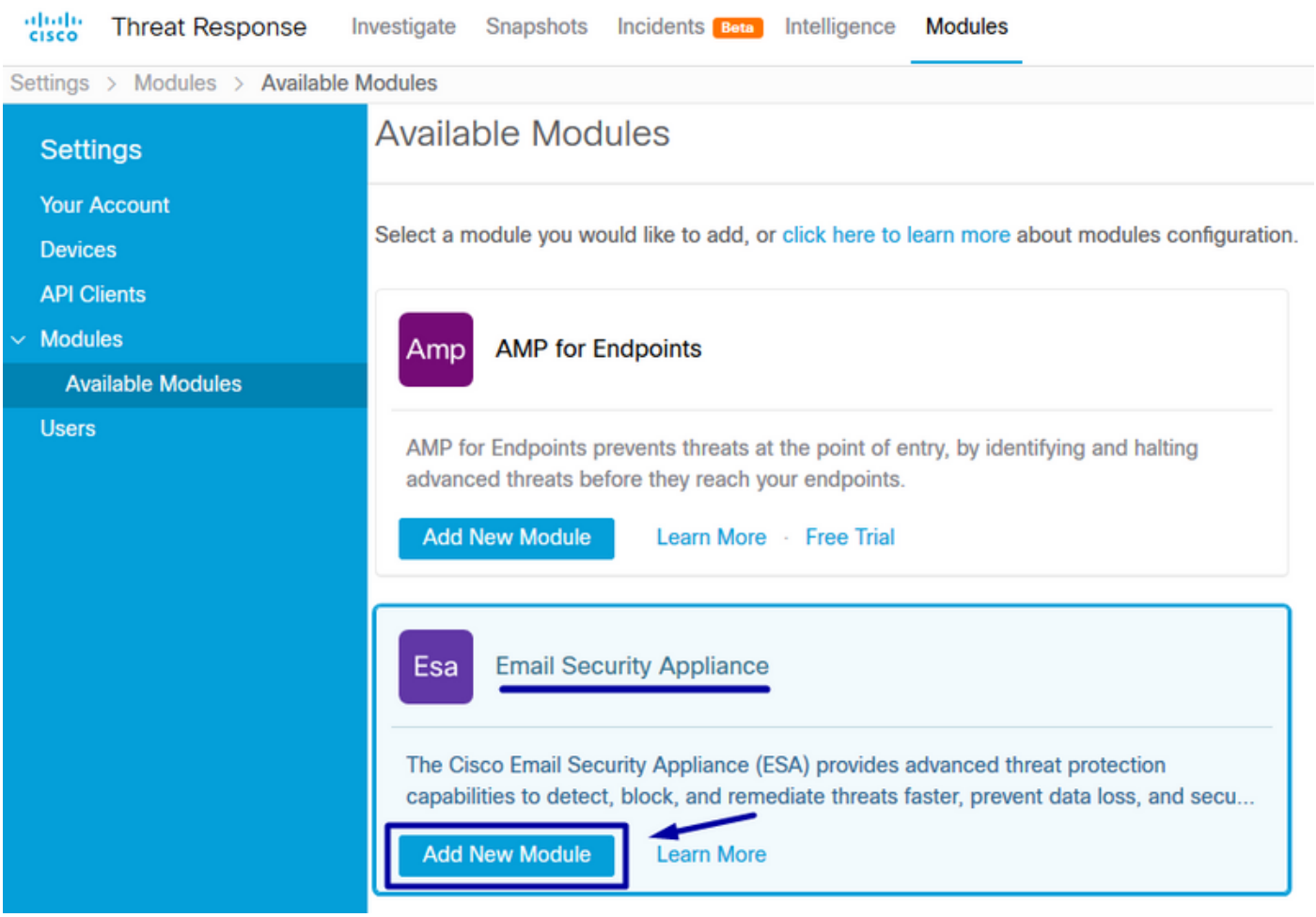


الخطوة 8. انتقل إلى بوابة CTR وأضف وحدة ESA جديدة

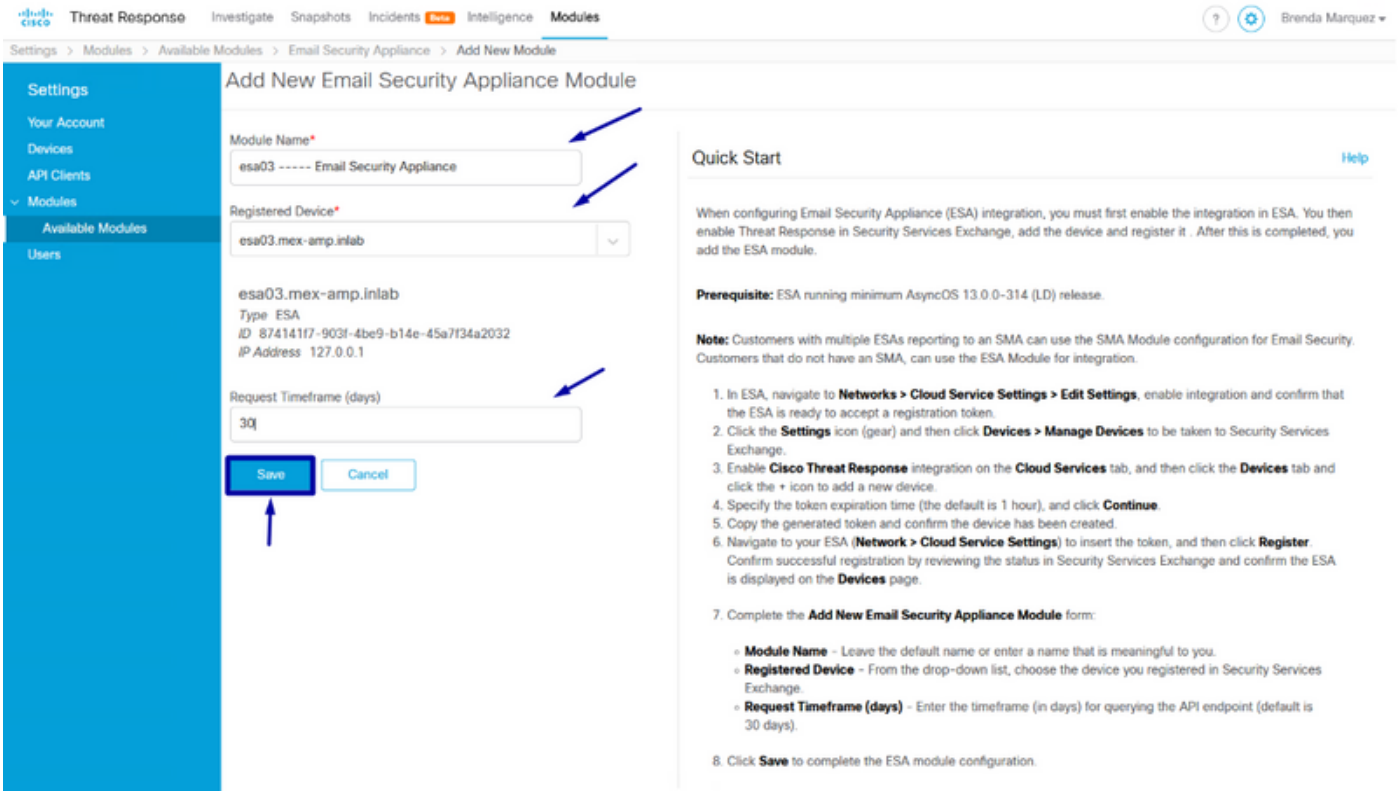
1.- بمجرد أن تكون في بوابة CTR، انتقل إلى الوحدات النمطية > إضافة وحدة نمطية جديدة، كما هو موضح في الصورة.



2.- أختر نوع الوحدة النمطية، في هذه الحالة، تكون الوحدة النمطية عبارة عن وحدة Email Security Appliance كالصورة أدناه.

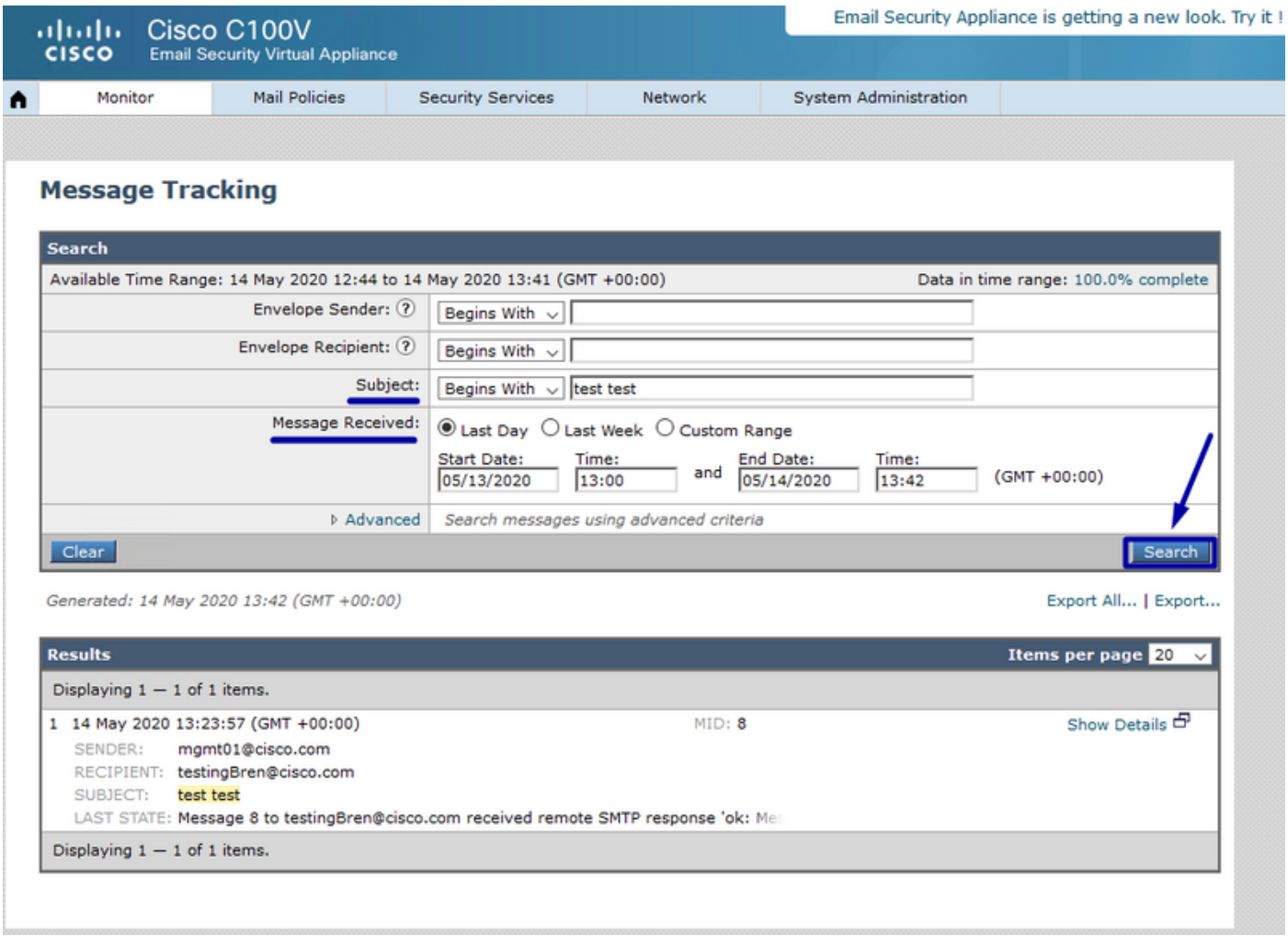


3.- أدخل الحقول: اسم الوحدة النمطية، الجهاز المسجل (حدد الجهاز المسجل سابقا) والإطار الزمني للطلب (بالأيام)، والحظ، كما هو موضح في الصورة.

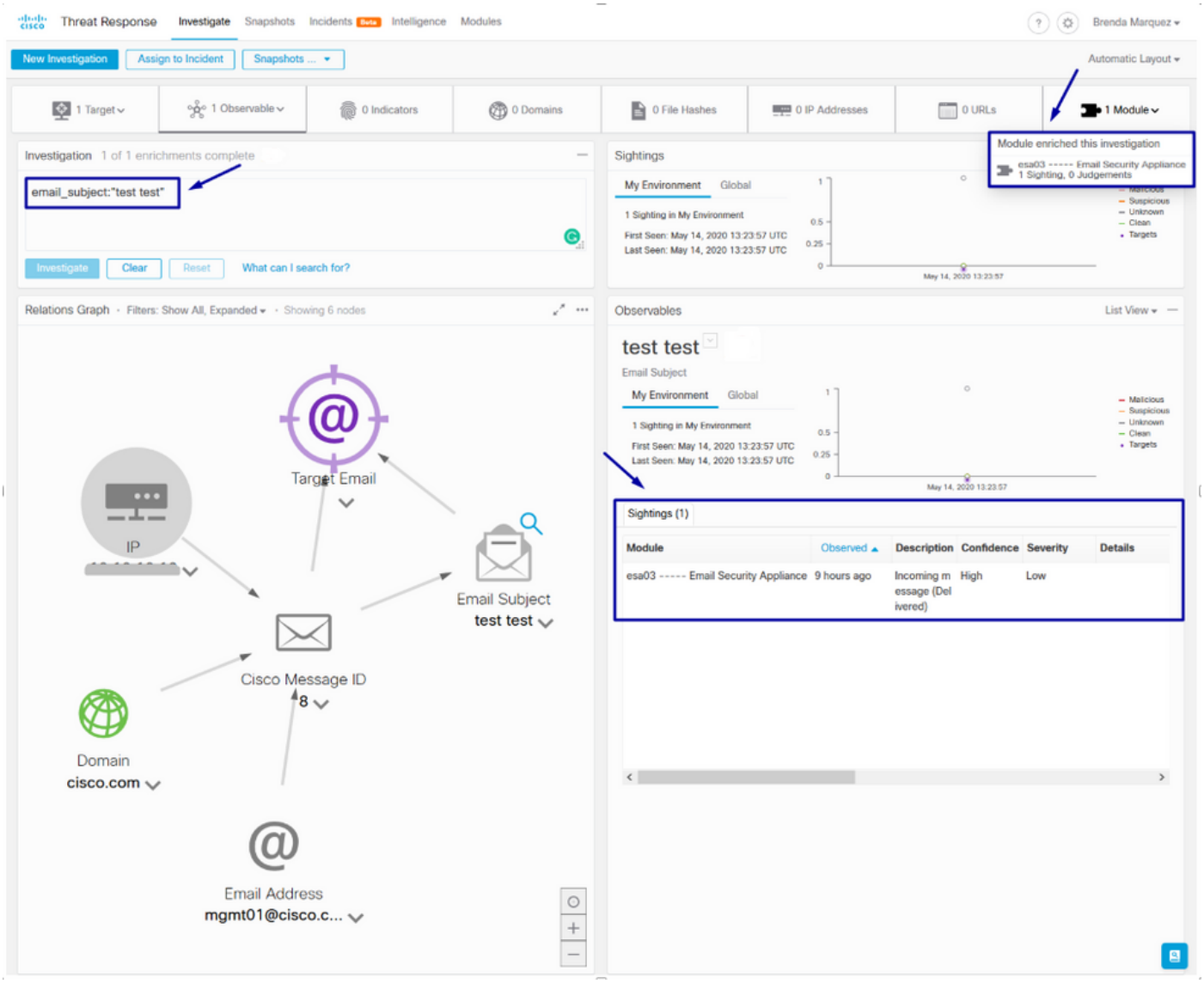


التحقق من الصحة

من أجل التحقق من تكامل CTR و ESA، يمكنك إرسال بريد إلكتروني للاختبار، والذي يمكنك أيضا رؤيته من ESA الخاص بك، والتصفح إلى الشاشة > تعقب الرسائل، والبحث عن بريد الاختبار الإلكتروني. في هذه الحالة، قمت بالترشيح باستخدام موضوع البريد الإلكتروني كصورة أدناه.



الآن، من بوابة CTR، يمكنك إجراء تحقيق، والتصفح للتحقيق، واستخدام بعض ملاحظات البريد الإلكتروني، كما هو موضح في الصورة.



تلميح: يمكنك إستخدام نفس الصيغة لنقاط مالحظة البريد الإلكتروني الأخرى كما يلي في الصورة.

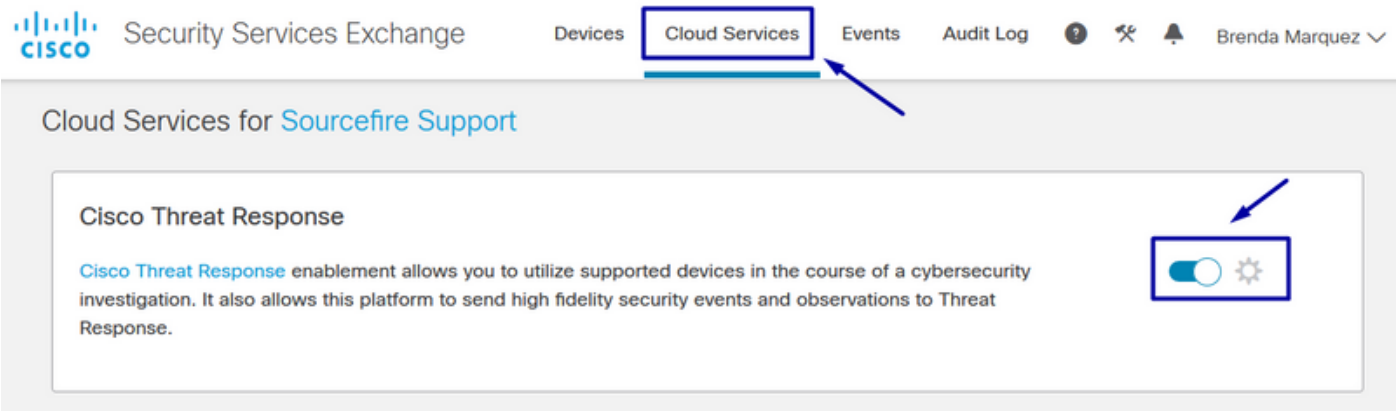
IP address	ip:"4.2.2.2"	Email subject	email_subject:"Invoice Due"
Domain	domain:"cisco.com"	Cisco Message ID (MID)	cisco_mid:"12345"
Sender email address	email:"noreply@cisco.com"	SHA256 filehash	sha256:"sha256filehash"
Email message header	email_messageid:"123-abc-456@cisco.com"	Email attachment file name	file_name:"invoice.pdf"

استكشاف الأخطاء وإصلاحها

إذا كنت أحد عمالء CES أو إذا قمت بإدارة أجهزة ESA الخاصة بك عبر SMA، فيمكنك االتصال بالاستجابة للتهديدات فقط عبر SMA. الرجاء التأكد من تشغيل SMA الخاص بك ل AsyncOS 12.5 أو أعلى. إذا لم تقم بإدارة ESA الخاص بك باستخدام SMA وقمت بدمج ESA مباشرة، فتأكد من أنه في الإصدار 13.0 من AsyncOS أو إصدار أعلى.

جهاز ESA غير ظاهر في بوابة CTR

إذا لم يتم عرض جهاز ESA الخاص بك في الجهاز المسجل المنسدل أثناء إضافة الوحدة النمطية ESA في بوابة CTR، فيرجى التأكد من تمكين CTR في SSE، وفي انتقال CTR إلى الوحدات النمطية > الأجهزة > إدارة الأجهزة، ثم في بوابة SSE انتقل إلى خدمات السحابة وتمكين CTR، كما هو موضح أدناه:



لا يظهر تحقيق لجنة التحقيق بيانات من وكالة الفضاء الأوروبية

يرجى التأكد مما يلي:

- بناء جملة التحقيق صحيح، تظهر بيانات البريد الإلكتروني التي تمت ملاحظتها أعلاه في قسم التحقق.
- لقد قمت باختيار "خادم أو شبكة الاستجابة للتهديدات" المناسبة (بين الأمريكتين/أوروبا).

لا يطلب ESA الرمز المميز للتسجيل

يرجى التأكد من تنفيذ التغييرات، عندما يتم تمكين "الاستجابة للتهديدات"، وإلا فلن يتم تطبيق التغييرات على قسم "الاستجابة للتهديدات" في ESA.

فشل التسجيل بسبب رمز مميز غير صالح أو منتهي الصلاحية

الرجاء التأكد من إنشاء الرمز المميز من السحابة الصحيحة:

إذا كنت تستخدم سحابة أوروبا (EU) ل ESA، قم بإنشاء الرمز المميز من: https://admin.eu.sse.itd.cisco.com/

إذا كنت تستخدم سحابة (NAM) الخاصة ب ESA، قم بإنشاء الرمز المميز من: https://admin.sse.itd.cisco.com/

تذكر أيضا أن الرمز المميز للتسجيل لديه وقت انتهاء صلاحية (حدد الوقت الأكثر ملاءمة لإكمال التكامل في الوقت المناسب).

معلومات ذات صلة

- يمكنك العثور على المعلومات الواردة في هذا المقال في فيديو الاستجابة لتهديدات Cisco وتكامل ESA.
- الدعم التقني والمستندات - Cisco Systems

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).