# دليل أفضل الممارسات للحماية المتقدمة من البرامج الضارة (AMP) على أمان البريد الإلكتروني من Cisco

## المحتويات



## المقدمة

الحماية المتقدمة من البرامج الضارة (AMP) هي حل شامل يتيح اكتشاف البرامج الضارة وحظرها والتحليل المستمر والتنبيه بأثر رجعي. تتيح الاستفادة من AMP مع أمان البريد الإلكتروني من Cisco إمكانية حماية فائقة عبر سلسلة الهجمات المستمرة - قبل هجوم وخلاله وبعده بنهج موفر للتكلفة وسهل النشر للدفاع عن البرامج الضارة المتقدمة.

يغطي مستند أفضل الممارسات هذا الميزات الأساسية لـ AMP على جهاز أمان البريد الإلكتروني من Cisco (ESA) كما هو مدرج أدناه:

- **File Reputation** - يلتقط بصمة إصبع لكل ملف أثناء إجتيازه ESA وإرساله إلى شبكة الذكاء القائمة على سحابة AMP من أجل إصدار حكم على السمعة. بافتراض هذه النتائج، يمكن حظر الملفات الضارة تلقائيا وتطبيق سياسة معرفة من قبل المسؤول.
- **تحليل الملف** - يوفر القدرة على تحليل الملفات غير المعروفة التي تجتاز ESA. تعمل بيئة وضع الحماية الآمنة للغاية على تمكين AMP من الحصول على تفاصيل دقيقة حول سلوك الملف ودمج هذه البيانات مع التحليل البشري والجهاز التفصيلي لتحديد مستوى تهديد الملف. ثم يتم تغذية هذا المصير النهائي بشبكة الذكاء المستندة إلى سحابة AMP ويتم إستخدامه لتحديث مجموعة بيانات سحابة AMP وتوسيعها بشكل ديناميكي من أجل الحماية المحسنة.
- **الإصلاح التلقائي لصندوق البريد (MAR)** - يقوم Microsoft Office 365 و Exchange 2013/2016 بأتمتة إزالة رسائل البريد الإلكتروني باستخدام الملفات التي تصبح ضارة بعد نقطة التفتيش الأولية. يؤدي ذلك إلى توفير ساعات عمل المسؤولين والمساعدة على إحتواء تأثير التهديد.
- **Cisco AMP Unity** - هي القدرة التي تسمح للمؤسسة بتسجيل الجهاز الذي يمكنها من AMP، بما في ذلك ESA باستخدام اشتراك AMP في AMP لوحدة تحكم نقاط النهاية. ومع هذا التكامل، يمكن رؤية أمان البريد الإلكتروني من Cisco والاستعلام عنه لعمليات مراقبة العينات بنفس الطريقة التي يقدم بها AMP لنقاط النهاية وحدة التحكم

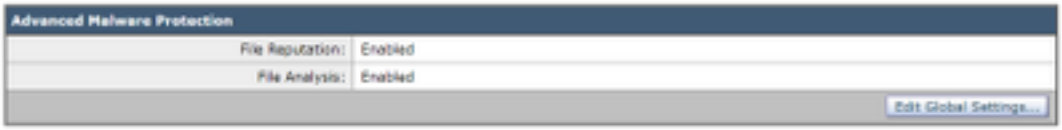
بالفعل لنقاط النهاية ويسمح بربط بيانات نشر الملفات عبر جميع متجهات التهديد في واجهة مستخدم واحدة.
- **الاستجابة للتهديدات من Cisco** - هي منصة تزامن تجمع المعلومات المتعلقة بالأمان من مصادر Cisco والجهات الخارجية في وحدة تحكم واحدة سهلة التحقيق والاستجابة. وذلك من خلال تصميم قابل لإضافة وحدات أخرى يعمل كإطار عمل للتكامل فيما يتعلق بسجلات الأحداث والمعلومات الاستخباراتية حول التهديدات. وتسمح الوحدات النمطية بالترابط السريع للبيانات من خلال بناء رسوم بيانية للعلاقة تمكن بدورها فرق الأمن من الحصول على رؤية واضحة للهجوم، وكذلك إتخاذ إجراءات إستجابة فعالة على وجه السرعة.

# التحقق من مفاتيح الميزة

- على ESA، انتقل إلى **إدارة النظام>مفاتيح الميزات**
- ابحث عن مفاتيح ميزة "سمعة الملف" و"تحليل الملفات" وتأكد من أن الحالات **نشطة**

# تمكين الحماية المتقدمة من البرامج الضارة

- على ESA، انتقل إلى **خدمات الأمان>الحماية المتقدمة من البرامج الضارة - سمعة الملف وتحليله**
- انقر على زر **تمكين** في الإعدادات العامة **للحماية المتقدمة من البرامج الضارة**:




- **قم بإكمال** تغييراتك.

## تخصيص الإعدادات العامة للحماية المتقدمة من البرامج الضارة (AMP)

- تم تمكين AMP الآن، انقر فوق **تحرير الإعدادات العمومية** لتخصيص الإعدادات العمومية.
- سيتم تحديث قائمة ملحقات الملفات تلقائيا من وقت لآخر، لذا يرجى دائما زيارة هذه الإعداد والتأكد من تحديد كافة ملحقات الملفات:

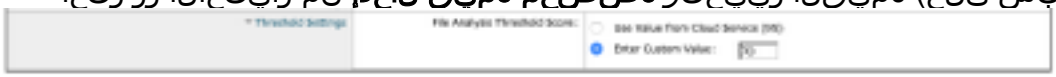

- توسيع **الإعدادات المتقدمة لسمعة الملف**
- التحديد الافتراضي لخادم سمعة الملف هو **أمريكا (cloud-sa.amp.cisco.com)**
- انقر فوق القائمة المنسدلة واختر أقرب خوادم سمعة الملفات (خاصة لعملاء APJC وعملاء أوروبا):

- توسيع **الإعدادات المتقدمة لتحليل الملف**
- التحديد الافتراضي ل URL خادم تحليل الملفات هو **AMERICAS** (https://panacea.threatgrid.com)
- انقر فوق القائمة المنسدلة واختر أقرب خوادم File Reputation (خاصة للعملاء الأوروبيين):

## إعداد حد تحليل الملف

(إختياري) يسمح لك بتعيين حد الحد الأقصى لدرجة تحليل الملفات المقبولة. يتم عرض الملفات التي يتم حظرها بناء على إعدادات الحد الفاصل كحد مخصص في قسم "ملفات تهديدات البرامج الضارة" الواردة في "تقرير الحماية المتقدمة من البرامج الضارة".

- في صفحة إعداد AMP العمومي، قم بتوسيع إعدادات **العتبة**.
- القيمة الافتراضية من خدمة السحابة هي **95**.
- أختر زر الاختيار من **إدخال قيمة مخصصة** وتغيير القيمة (على سبيل المثال، 70):

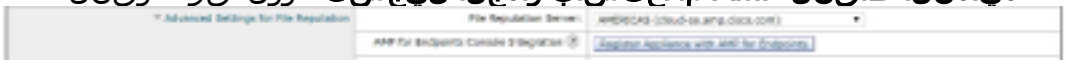


- انقر فوق **إرسال وتنفيذ** التغييرات الخاصة بك

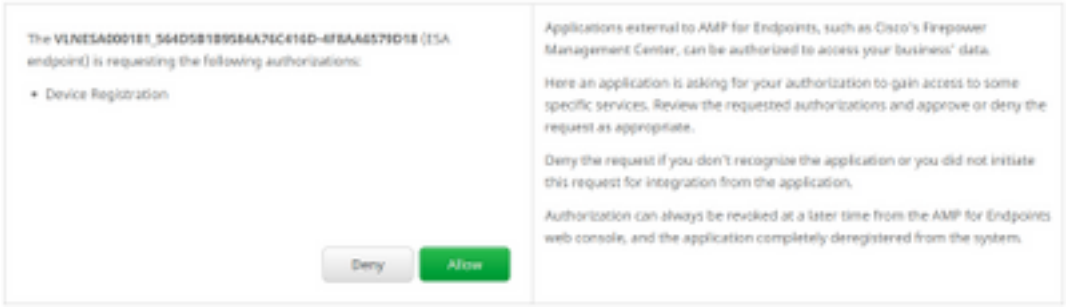
## دمج ESA مع AMP لوحدة التحكم في نقاط النهاية

(فقط لـ AMP لنقاط النهاية Customer) يمكن إنشاء قائمة حظر ملفات مخصصة موحدة (أو قائمة السماح بالملفات) من خلال AMP لوحدة التحكم في نقاط النهاية، كما يمكن توزيع إستراتيجية الاحتواء بسلاسة تامة عبر بنية الأمان، بما في ذلك ESA.

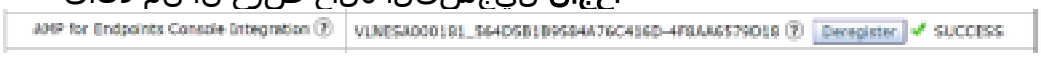
- في صفحة إعداد AMP العمومي، قم بتوسيع **الإعدادات المتقدمة لسمعة الملف**
- النقر فوق الزر - **تسجيل الجهاز باستخدام AMP لنقاط النهاية**:



- انقر فوق **موافق** لإعادة التوجيه إلى موقع وحدة تحكم AMP لنقاط النهاية لإكمال التسجيل.
- تسجيل الدخول إلى AMP لوحدة تحكم نقاط النهاية باستخدام بيانات اعتماد المستخدم الخاصة بك
- طقطقة **يسمح** يخول ال ESA تسجيل:




- توقوم وحدة التحكم AMP for Endpoints تلقائيا بتحويل الصفحة إلى ESA.
- تأكد من أن عرض حالة التسجيل **ناجح**:

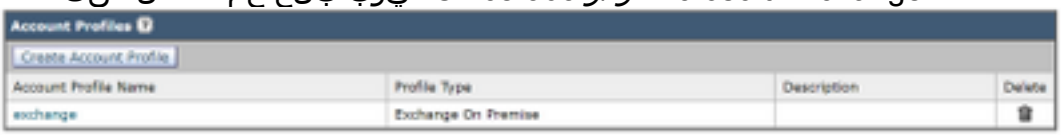



- انقر فوق **إرسال وتنفيذ** التغييرات الخاصة بك

## تمكين الإصلاح التلقائي لعلبة البريد (MAR)

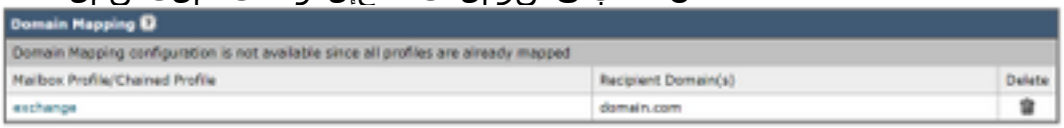
إذا كانت لديك علب بريد O365 أو Microsoft Exchange 2013/2016، فستسمح ميزة الإصلاح التلقائي لعلبة البريد (MAR) باتخاذ الإجراء عند تغيير الحكم على سمعة الملف من نظيف/غير معروف إلى ضار.

- انتقل إلى **إدارة النظام >إعدادات الحساب**
- ضمن **ملف تعريف الحساب**، انقر فوق **إنشاء ملف تعريف الحساب** لإنشاء ملف تعريف اتصال API مع علب بريد Office 365 و/أو Microsoft Exchange:




- انقر فوق **إرسال وتنفيذ** التغييرات الخاصة بك

- (إختياري) يعد ملف التعريف المرتبط مجموعة من ملفات التعريف، ولا تقم بتكوين ملف التعريف المتسلسل إلا عندما تكون الحسابات التي سيتم الوصول إليها موجودة عبر مستأجرين مختلفين من أنواع مختلفة من عمليات النشر.
- انقر فوق **إنشاء** زر **تعيين مجال** لتعيين ملف تعريف الحساب الخاص بك مع مجال المستلم. تظهر الإعدادات الموصى بها أدناه:



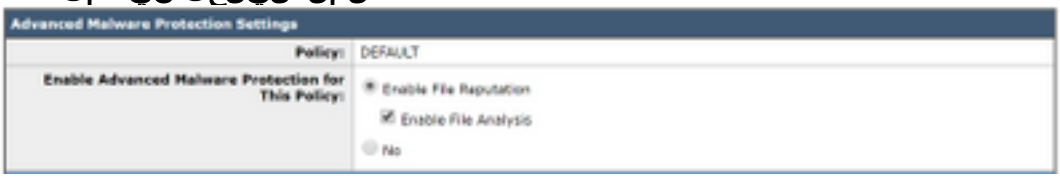

- انقر فوق **إرسال وتنفيذ** التغييرات الخاصة بك

## تكوين الحماية المتقدمة من البرامج الضارة (AMP) في نهج البريد

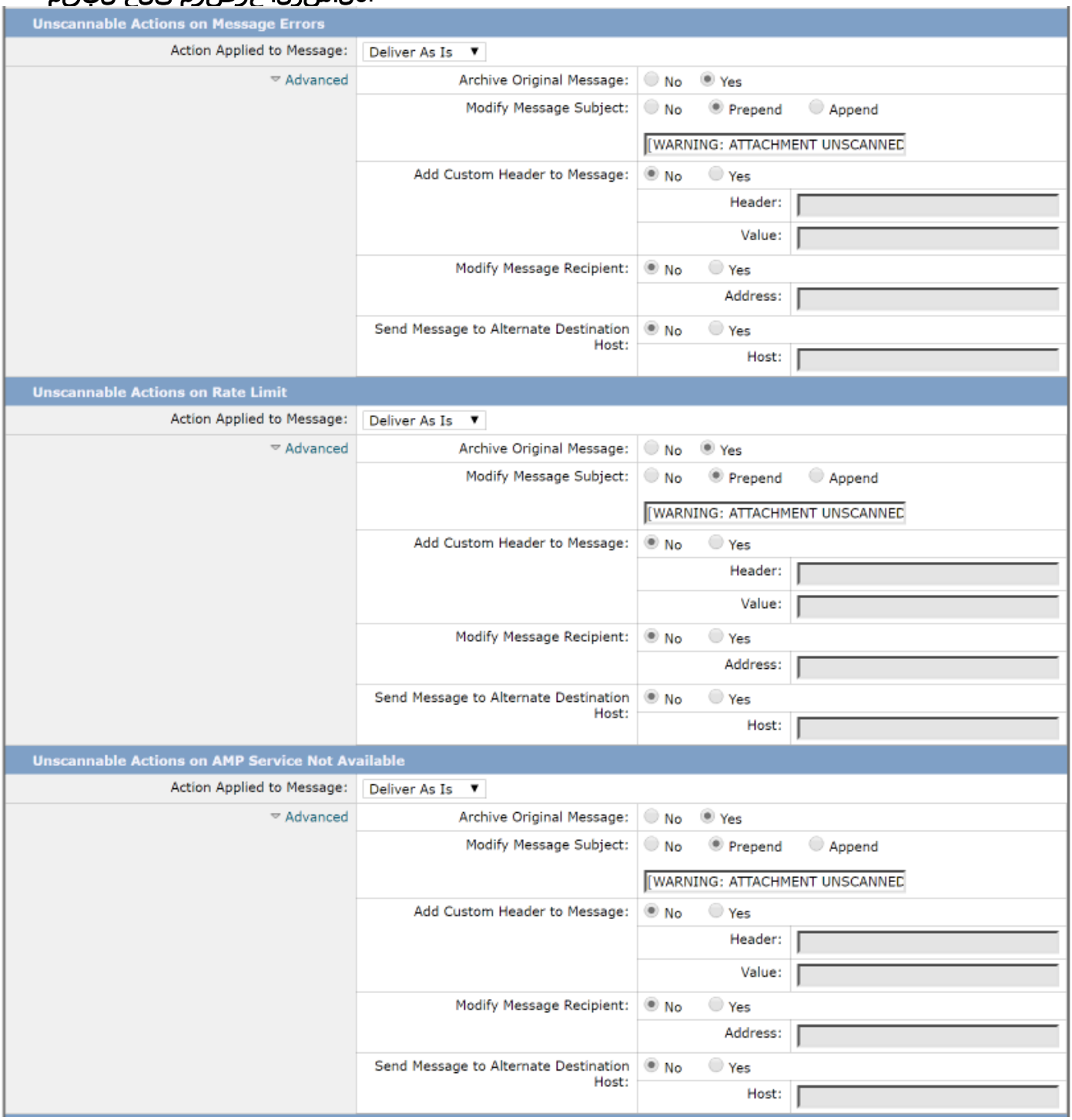
بمجرد تكوين AMP و MAR بشكل عام، يمكنك الآن تمكين الخدمات من نهج البريد.

- انتقل إلى **نهج البريد > نهج البريد الوارد**
- تخصيص إعدادات **الحماية المتقدمة من البرامج الضارة** لنهج البريد الوارد بالنقر فوق

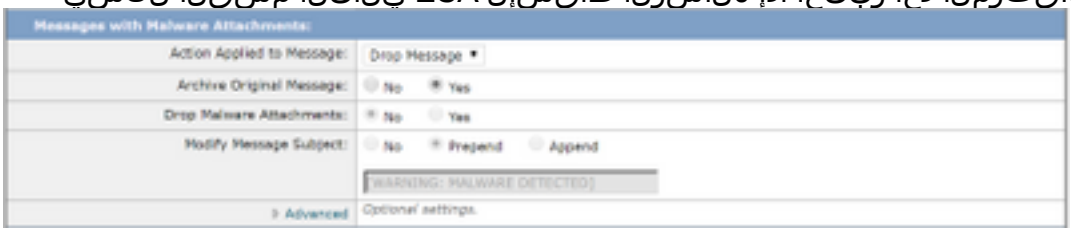
الارتباط الأزرق تحت **الحماية المتقدمة من البرامج الضارة** للنهج الذي تريد تخصيصه.
- لأغراض وثيقة أفضل ممارسة هذه، انقر زر الخيار التالي **لتمكين سمعة الملف** وحدد **تمكين تحليل الملف**:



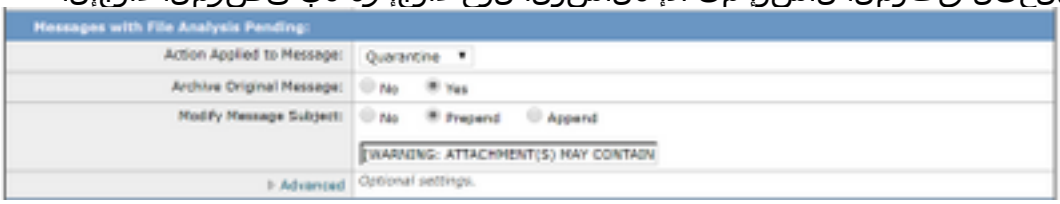

- يوصى **بتضمين رأس X مع نتيجة AMP في رسالة**.
- تتيح لك الأقسام الثلاثة التالية تحديد الإجراء الذي يجب على ESA تنفيذه إذا كان المرفق غير قابل للمسح الضوئي بسبب أخطاء الرسائل أو الحد الأقصى للمعدل أو إذا لم تكن خدمة AMP متوفرة. الإجراء الموصى به هو **تسليم الوضع كما هو** مع **نص تحذيري مقبل على موضوع الرسالة**:



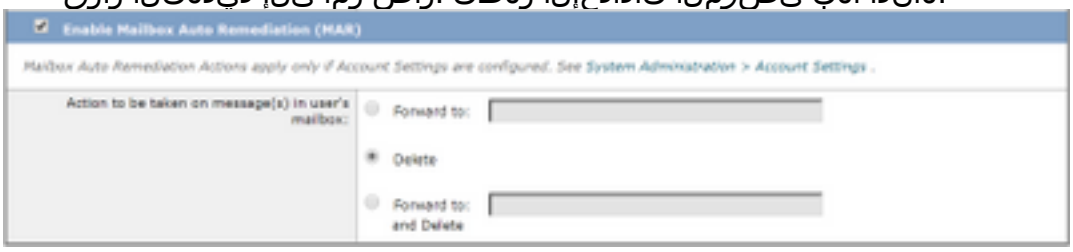
- يشكل القسم التالي ESA لإسقاط الرسالة إذا اعتبر أحد المرفقات ضارا:




- الإجراء الموصى به هو إجراء عزل الرسالة إذا تم إرسال المرفق لتحليل الملف:




- (لسياسة البريد الوارد فقط) قم بتكوين الإجراءات التصحيحية التي سيتم تنفيذها على الرسالة التي يتم تسليمها إلى المستخدمين النهائيين عندما يتغير قرار التهديد إلى أمر ضار. تظهر الإعدادات الموصى بها أدناه:

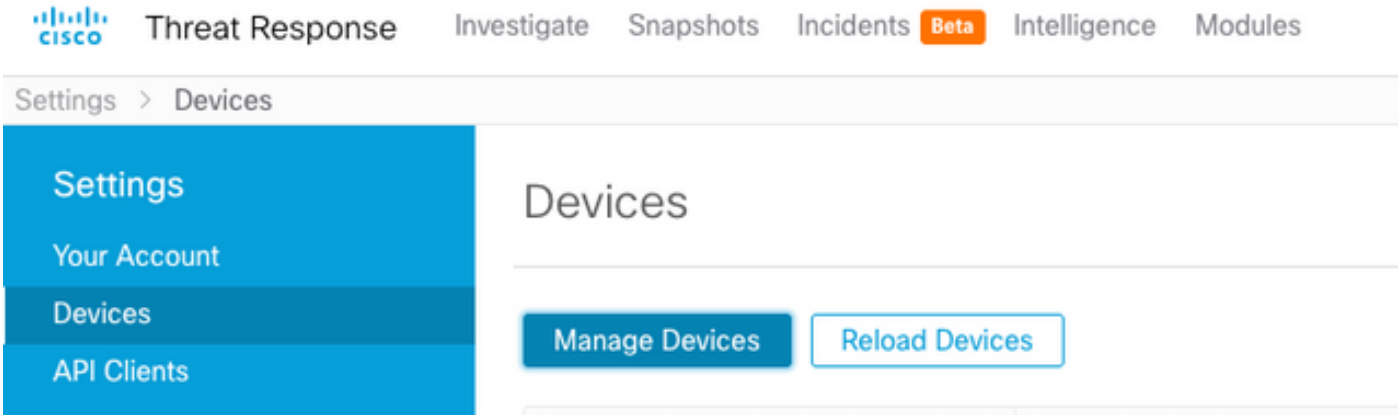



- انقر فوق **إرسال وتنفيذ** التغييرات الخاصة بك

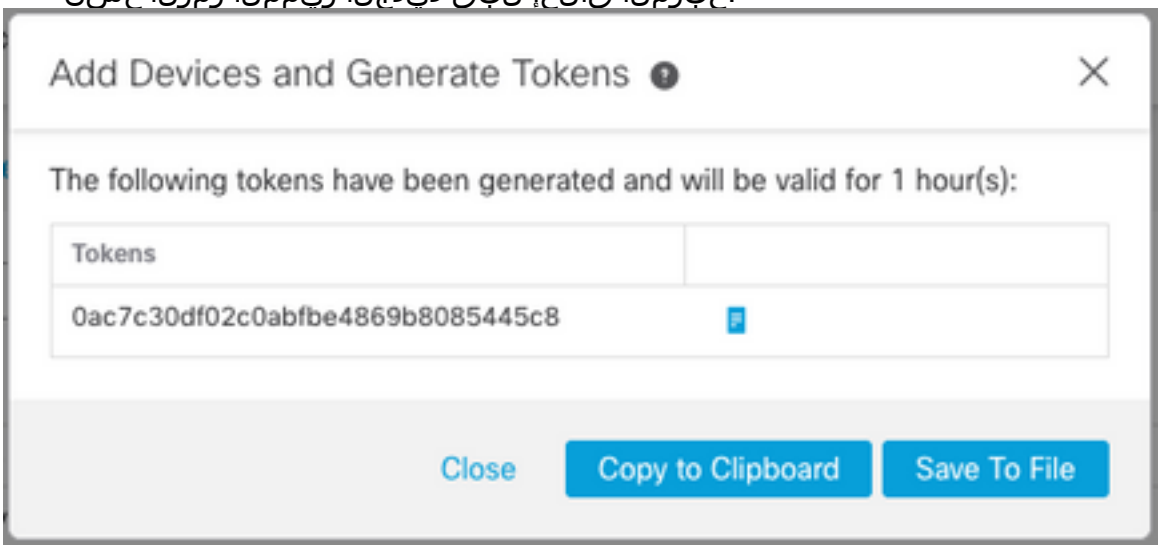
## دمج SMA مع الاستجابة للتهديدات من Cisco (CTR)

يتطلب دمج وحدة البريد الإلكتروني ل SMA إستخدام تبادل خدمات الأمان (SSE) عبر CTR. يسمح SSE ل SMA بالتسجيل مع Exchange وتوفر إذن صريح لاستجابة تهديدات Cisco للوصول إلى الأجهزة المسجلة. تتضمن العملية ربط SMA الخاص بك ب SSE عبر رمز مميز يتم إنشاؤه عندما تكون مستعد لربطه.

- على بوابة CTR (https://visibility.amp.cisco.com)، قم بتسجيل الدخول باستخدام بيانات اعتماد المستخدم الخاصة بك.
- يستخدم CTR وحدة نمطية للتكامل مع منتجات الأمان الأخرى من Cisco بما في ذلك ESA. انقر فوق علامة التبويب **الوحدات النمطية**.
- أختر **الأجهزة** وانقر فوق **إدارة الأجهزة:**

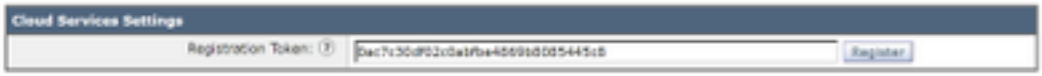


- سيقوم CTR بتحويل الصفحة إلى SSE محورا.
- انقر فوق أيقونة + لإنشاء رمز مميز جديد وانقر فوق **متابعة**.
- نسخ الرمز المميز الجديد قبل إغلاق المربع:

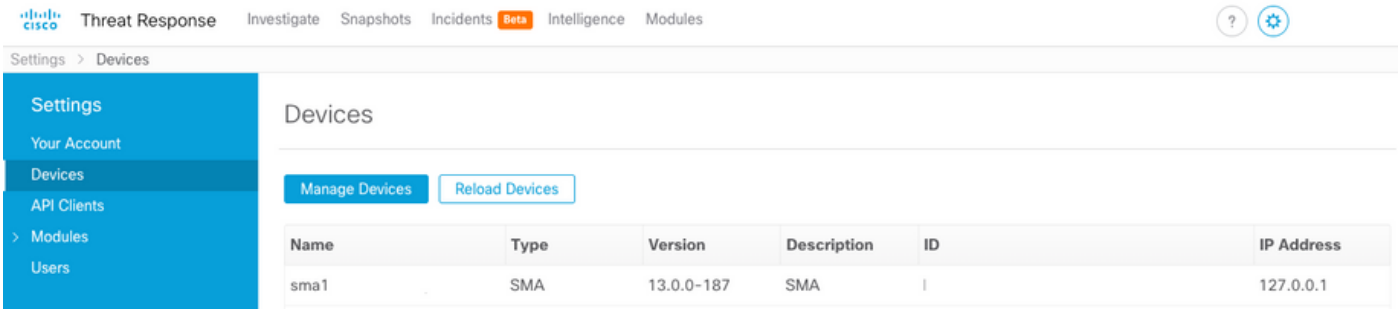



- في SMA، انتقل إلى علامة التبويب **أجهزة الإدارة > الشبكة > إعدادات خدمة السحابة**
- انقر فوق **تحرير الإعداد** وتأكد من **تمكين** خيار الاستجابة للتهديدات.
- يكون التحديد الافتراضي لعنوان URL الخاص بخادم الاستجابة للتهديدات هو **AMERICAS (api-sse.cisco.com)**. بالنسبة للعملاء الأوروبيين، انقر فوق القائمة المنسدلة واختر **أوروبا (api.eu.sse.itd.cisco.com)**:


- انقر فوق **إرسال** و**تنفيذ** التغييرات الخاصة بك
- الصق مفتاح الرمز المميز (الذي أنشأته من مدخل CTR) في إعداد خدمات السحابة وانقر فوق **تسجيل**:




- سيستغرق إكمال عملية التسجيل بعض الوقت، الرجاء الانتقال مرة أخرى إلى هذه الصفحة بعد بضع دقائق للتحقق من الحالة مرة أخرى.
- ارجع إلى **CTR > Modules > Device** وانقر فوق الزر **إعادة تحميل الجهاز** للتأكد من ظهور SMA في القائمة:




# القرار

يهدف هذا المستند إلى وصف تكوينات الممارسات الافتراضية أو الأفضل لـ Cisco Advanced Malware Protection (AMP) في جهاز أمان البريد الإلكتروني. تتوفر معظم هذه الإعدادات على كل من سياسات البريد الإلكتروني الواردة والصادرة، كما يوصى بالتكوين والتصفية في كلا الاتجاهين.

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).