AMP لتكامل نقاط النهاية مع Splunk

المحتويات

المقدمة

يصف هذا المستند عملية التكامل بين "الحماية المتقدمة من البرامج الضارة" (AMP) وتقسيم الشبكة.

ساهم في ذلك أوريليل إيسالس وييوفنتينو مايسايس، تحرير خوريخ نافاريت، مهندس Cisco TAC.

المتطلبات الأساسية

المتطلبات

cisco يوصي أن يتلقى أنت المعرفة من:

- AMP لنقاط النهاية
- واجهة برمجة التطبيقات (API)
- شظية
- مستخدم المسؤول على Splunk

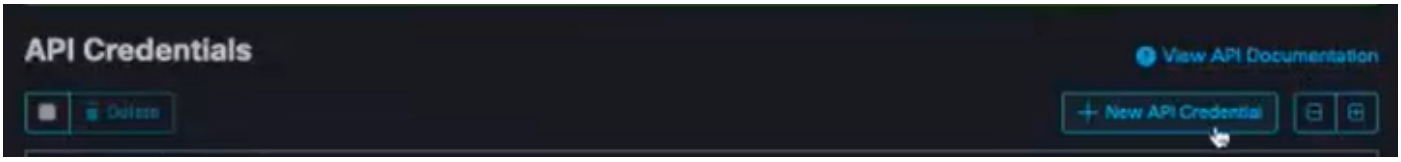
المكونات المستخدمة

- الحماية المتقدمة (AMP) من البرامج السحابية العامة
- مثيل النقسام

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

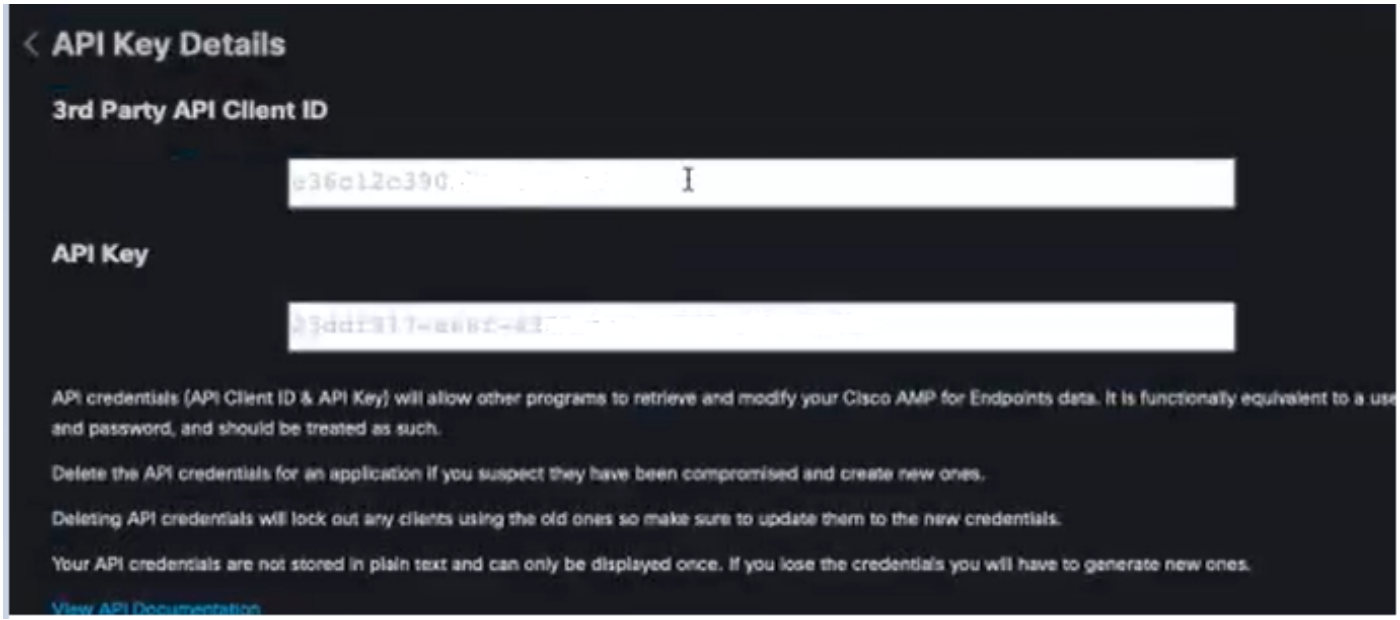
الخطوة 1. انتقل إلى وحدة تحكم AMP (https://console.amp.cisco.com) وانتقل إلى **Accounts>مسوغات API**، حيث يمكنك إنشاء تدفقات الأحداث.



الخطوة 2. من أجل تنفيذ هذا التكامل، ضع علامة على خانة الاختيار **قراءة وكتابة** كما هو موضح أدناه:

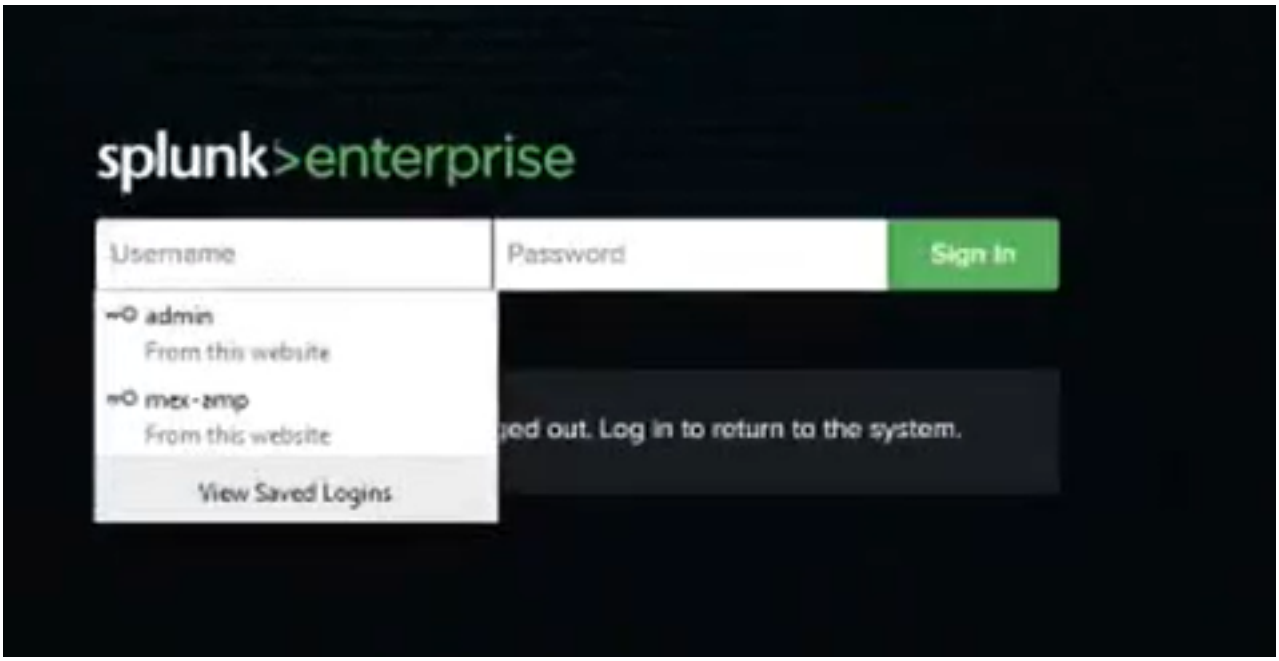
ملاحظة: إذا كنت ترغب في جمع مزيد من المعلومات حول الأحداث، فحدد مربع **سطر الأوامر enable**"، للحصول على سجلات التدقيق التي تم إنشاؤها من مستودع الملفات، حدد مربع **السماح بوصول واجهة برمجة التطبيقات (API) إلى مستودع الملفات**.

الخطوة 3. بمجرد إنشاء تدفق الأحداث، سيتم عرض معرف عميل واجهة برمجة التطبيقات (API) ومفتاح واجهة برمجة التطبيقات (API) المطلوب على Splunk.

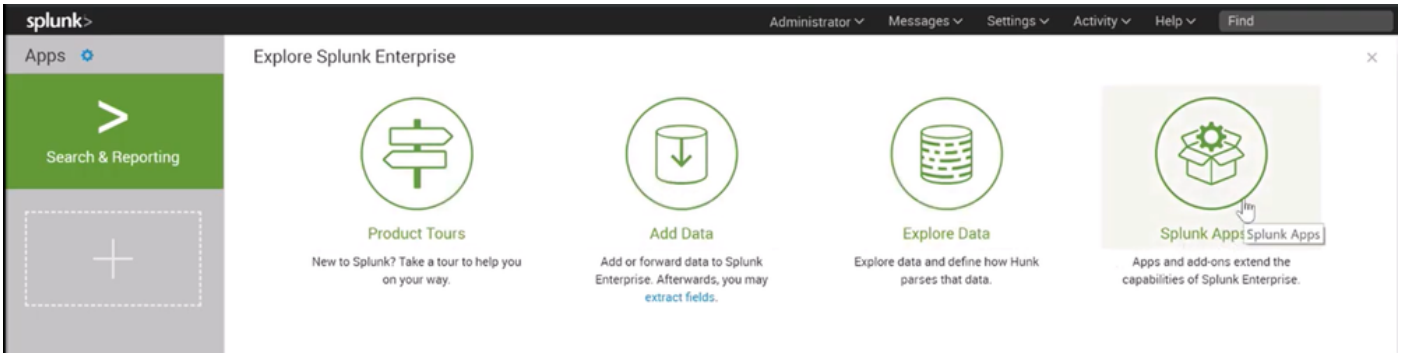


تحذير: لا يمكن إسترداد هذه المعلومات بأية وسيلة، في حالة الخسارة، يجب إنشاء مفتاح واجهة برمجة تطبيقات جديد.

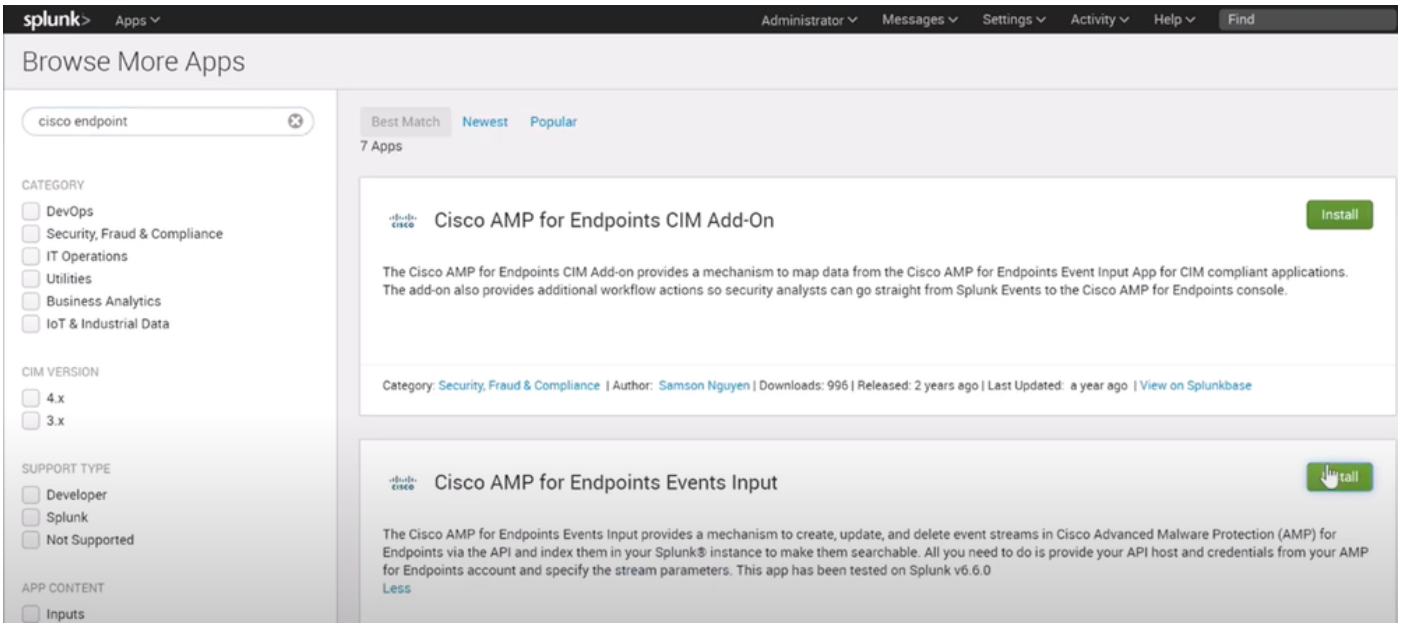
الخطوة 4. من أجل تكامل Splunk مع AMP لنقاط النهاية، تأكد من وجود **مسؤول** الحساب على Splunk.



الخطوة 5. بمجرد تسجيل الدخول إلى Splunk، انتقل إلى تنزيل AMP من تطبيقات Splunk.

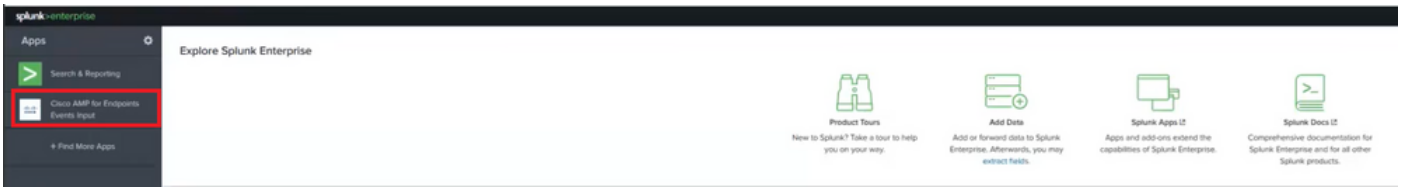


الخطوة 6. ابحث عن نقطة نهاية Cisco على مستعرض "التطبيق" وقم بتثبيتها (Cisco AMP for Endpoints Events Input).

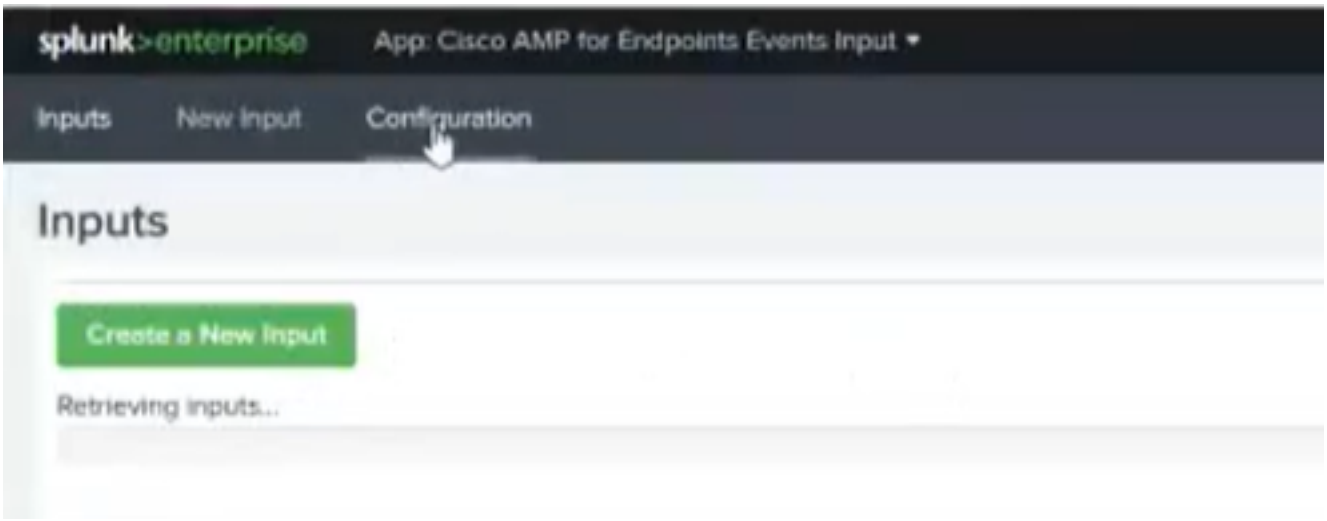


الخطوة 7. مطلوب إعادة تشغيل جلسة العمل لإكمال التثبيت على Splunk.

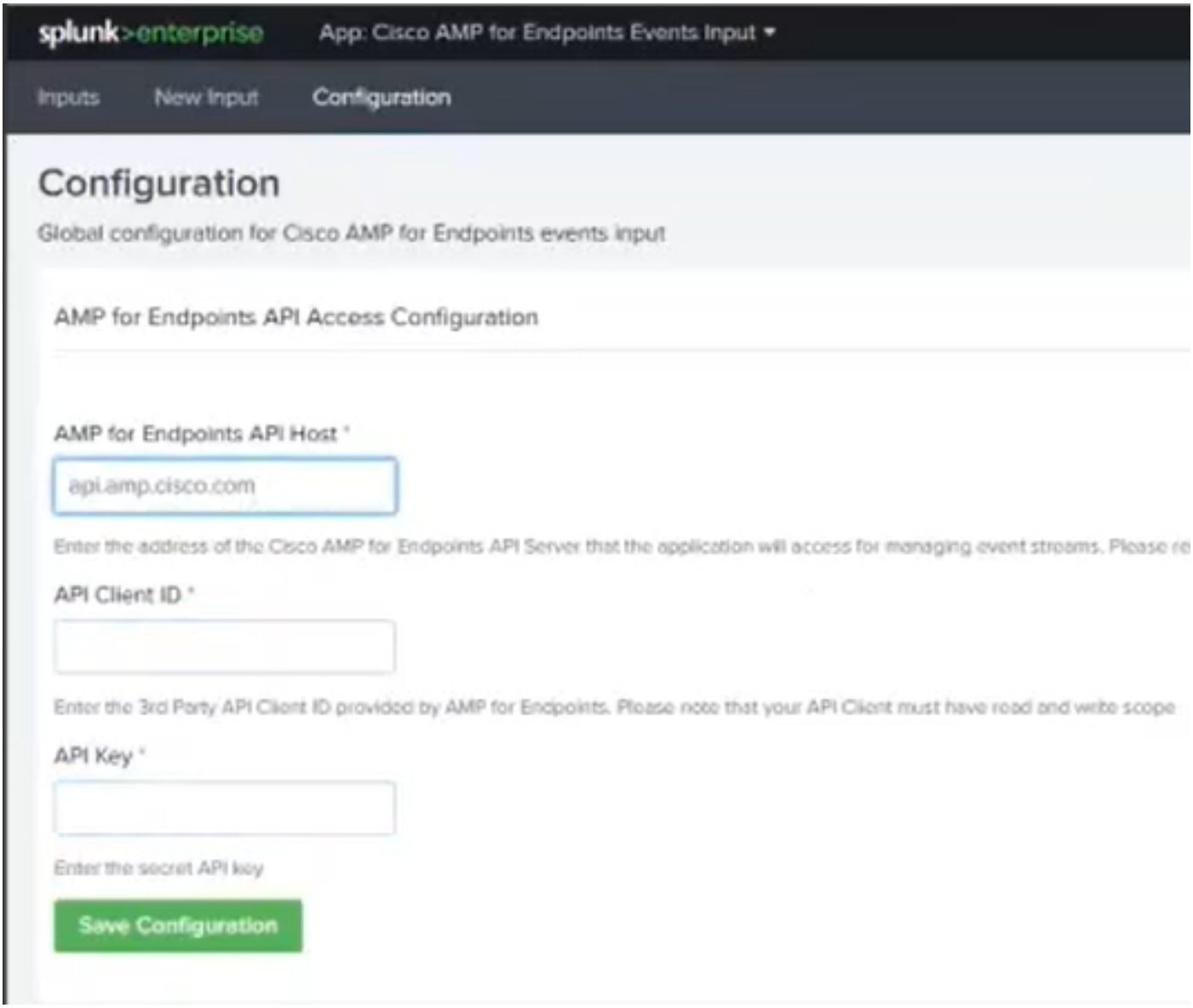
الخطوة 8. بمجرد تسجيل الدخول أسفل Splunk، انقر فوق **Cisco AMP للحصول على نقاط النهاية** على الجانب الأيسر من الشاشة.



الخطوة 9. انقر فوق تسمية **التكوين** في أعلى الشاشة.



الخطوة 10. اكتب بيانات اعتماد واجهة برمجة التطبيقات (API) التي تم إنشاؤها مسبقا من وحدة تحكم AMP.

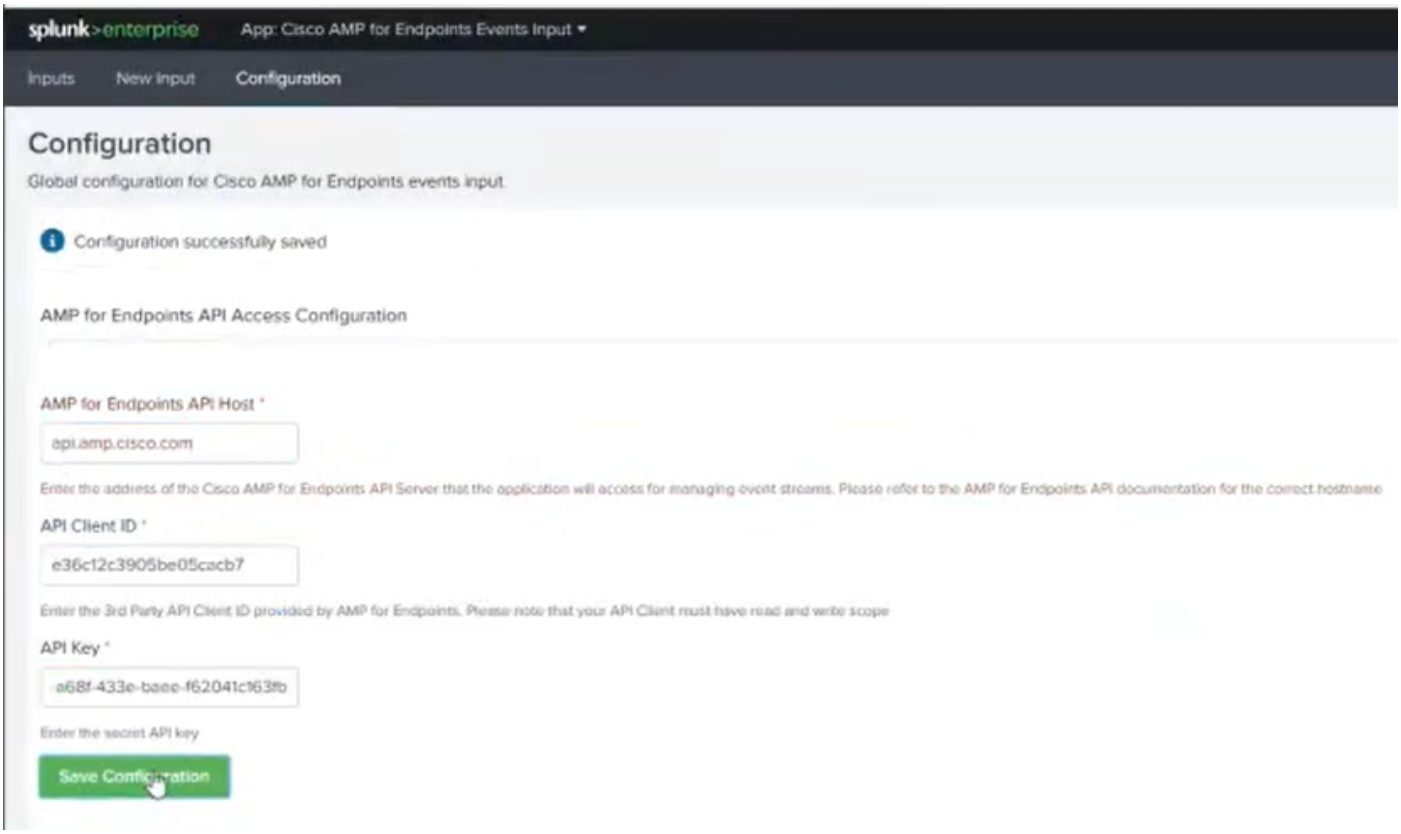


ملاحظة: قد تكون نقطة مضيف API مختلفة استنادا إلى مركز بيانات السحابة الذي تشير إليه مؤسستك على:

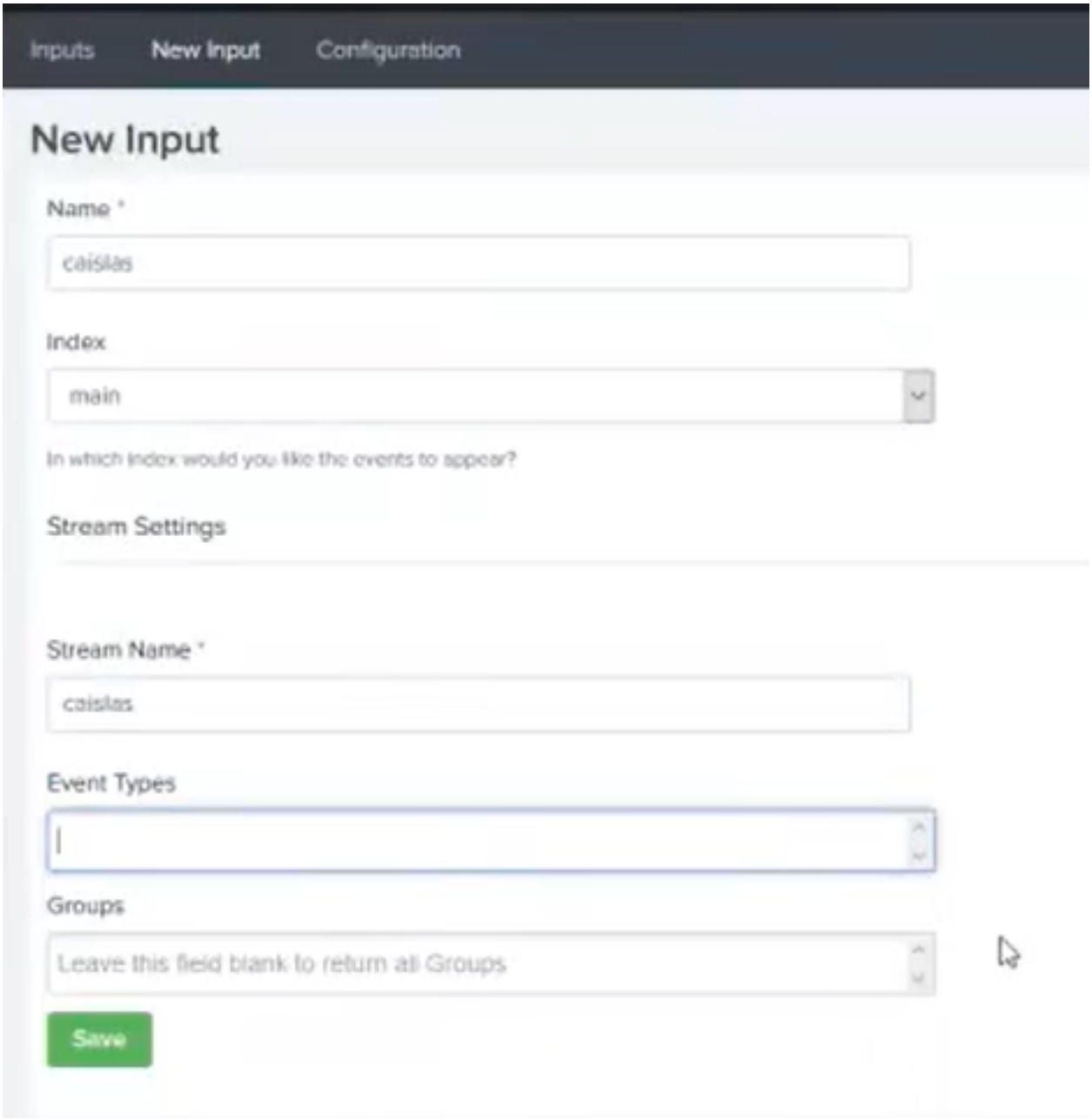
أمريكا الشمالية: api.amp.cisco.com
أوروبا: api.eu.amp.cisco.com

المركز: api.apjc.amp.cisco.com

الخطوة 11. قم بتضمين بيانات اعتماد واجهة برمجة التطبيقات (API) وحفظها على وحدة تحكم Splunk لربطها مع AMP.

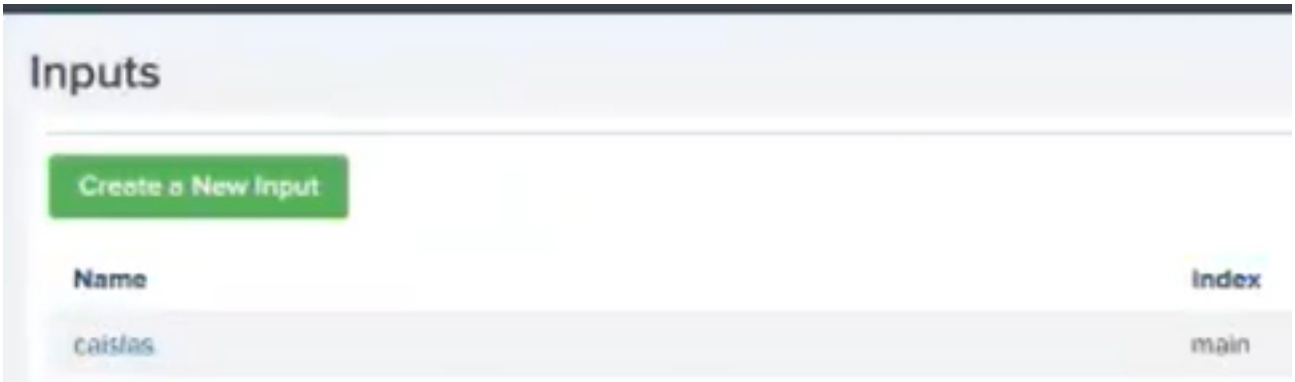


الخطوة 12. ارجع إلى **Input** لإنشاء دفق الحدث.



ملاحظة: إذا كنت تريد الحصول على كافة الأحداث الخاصة بكافة المجموعات من AMP، فاترك حقلي **أنواع الأحداث والمجموعات** فارغة.

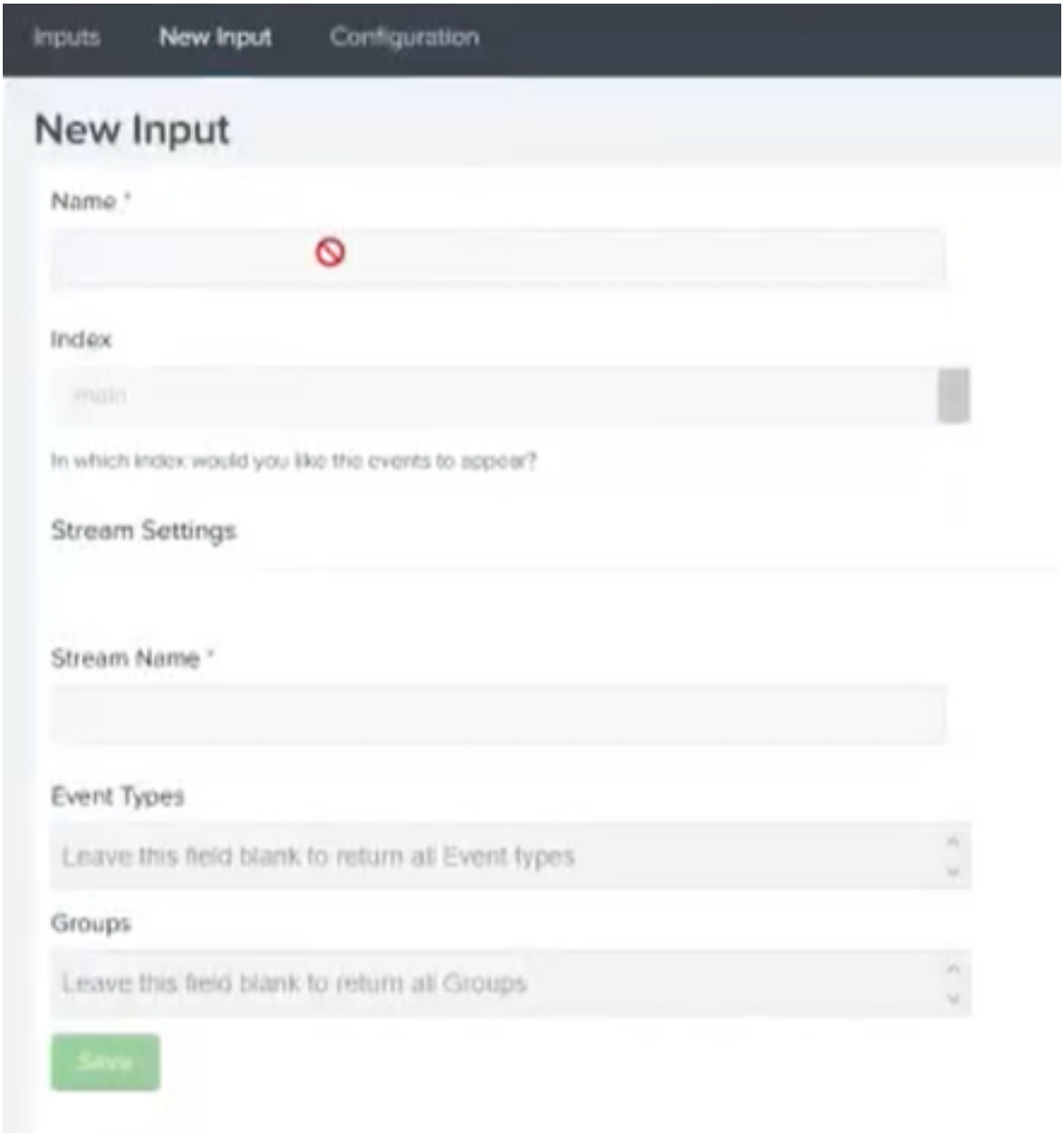
الخطوة 13. تأكد من أن الإدخال الخاص بك تم إنشاؤه بنجاح.



ملاحظة: يرجى مراعاة أن هذا الدمج غير مدعوم رسميا

استكشاف الأخطاء وإصلاحها

إذا تم تصنيف كافة الحقول أثناء إنشاء دفق حدث، قد يرجع ذلك إلى بعض الأسباب أدناه:



1. مشاكل الاتصال: تأكد من قدرة مثيل Splunk على الاتصال بمضيف API
2. مضيف واجهة برمجة التطبيقات (API): تأكد من أن مضيف واجهة برمجة التطبيقات الذي تم تكوينه في الخطوة 10 يتوافق مع مؤسسة AMP الخاصة بك، وذلك استنادا إلى موقع نقاط شركتك على.
3. بيانات اعتماد API: تأكد من تطابق مفتاح API ومعرف العميل مع تلك التي تم تكوينها في الخطوة 3.
4. تدفقات الأحداث: تأكد من أن لديك أقل من 4 تدفقات أحداث تم تكوينها.

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).