SecureX مع الحماية المتقدمة من البرامج الضارة (AMP) دليل دمج نقاط النهاية

المحتويات

المقدمة

يصف هذا المستند العملية المطلوبة لدمج Cisco SecureX والتحقق منه مع Cisco Advanced Ware Protection (AMP) لنقاط النهاية.

ساهم به يارالدين سانشيز وأوريبيل توريس، تحرير خورخي نافاريت، مهندسو مركز المساعدة الفنية التابع لشركة Cisco.

المتطلبات الأساسية

المتطلبات

توصي Cisco بأن تكون لديك معرفة بالمواضيع التالية:

- الحماية المتقدمة لنقاط النهاية من البرامج الضارة من Cisco
- التنقل الأساسي في وحدة تحكم SecureX
- المحاكاة الافتراضية الاختيارية للصور

المكونات المستخدمة

- AMP لوحدة تحكم نقاط النهاية، الإصدار 5.4.20200804
- AMP لحساب مسؤول نقاط النهاية
- SecureX Console، الإصدار 1.54
- حساب مسؤول SecureX

- Microsoft Edge الإصدار 84.0.522.52

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.

معلومات أساسية

الحماية المتقدمة من البرامج الضارة (AMP) من Cisco لنقاط النهاية هي جزء أساسي من منصة أمان نقاط النهاية ويتم نشرها كأداة وقائية وتحقيقية تدعم وظائف الكشف و/أو الاستجابة لأجهزة Windows و/أو MacOS و Linux و Android و iOS، وتوفر وحدة AMP لنقاط النهاية 5 تجانبات.

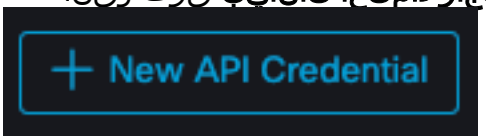
- **التنازلات التي تم اكتشافها بواسطة AMP:** مجموعة من المقاييس تلخص التنازلات التي تم اكتشافها بواسطة AMP
- **ملخص أجهزة الكمبيوتر AMP:** مجموعة من المقاييس تلخص حالة أجهزة الكمبيوتر AMP
- **ملخص AMP:** مجموعة من المقاييس تلخص اكتشاف AMP والاستجابة له
- **AMP Quarantines:** مجموعة من القياسات التي تلخص AMP Quarantines حسب الوقت
- **تكتيكات Miter ATT&CK التي تم كشفها بواسطة AMP:** مجموعة من المقاييس تلخص تكتيكات Miter ATT&CK التي تم كشفها بواسطة AMP

التكوين

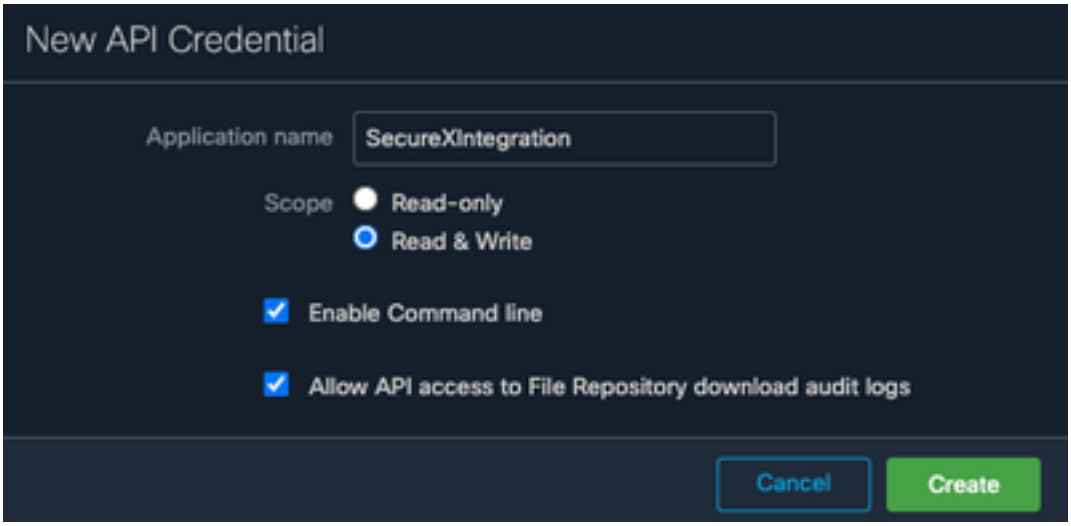
إنشاء بيانات اعتماد API في وحدة تحكم AMP

في وحدة تحكم AMP، يتم إنشاء بيانات اعتماد API جديدة.

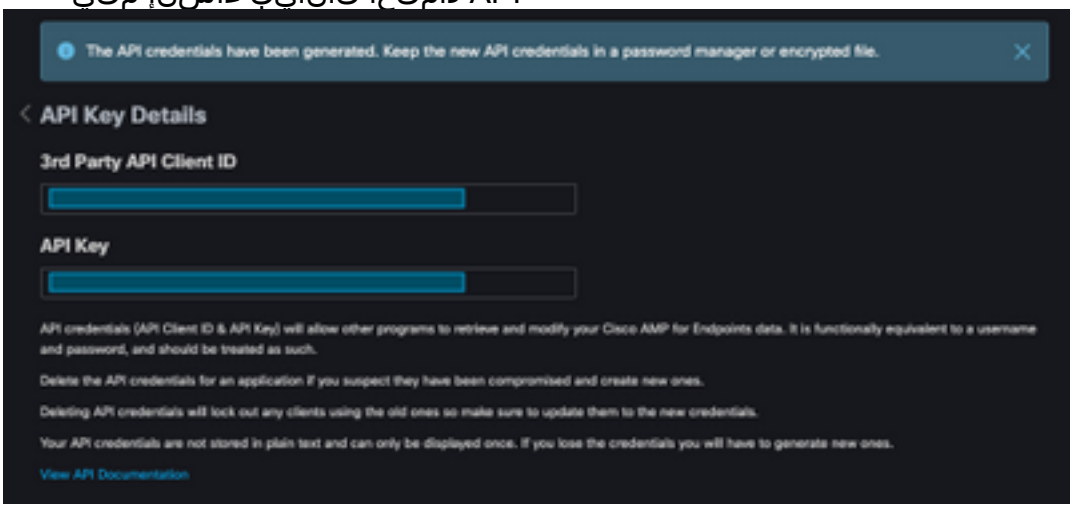
- تسجيل الدخول إلى وحدة تحكم AMP بامتيازات المسؤول
- في وحدة تحكم AMP، انتقل إلى **الحسابات > بيانات اعتماد واجهة برمجة التطبيقات (API)**
- انقر فوق **بيانات اعتماد واجهة برمجة تطبيقات جديدة**



- قم بتسمية التطبيق
- حدد **قراءة وكتابة**
- تدقيق **تمكين سطر الأوامر والسماح بوصول API إلى سجلات تدقيق تنزيل مستودع الملفات**
- انقر فوق **إنشاء**



- يتم إنشاء بيانات اعتماد API

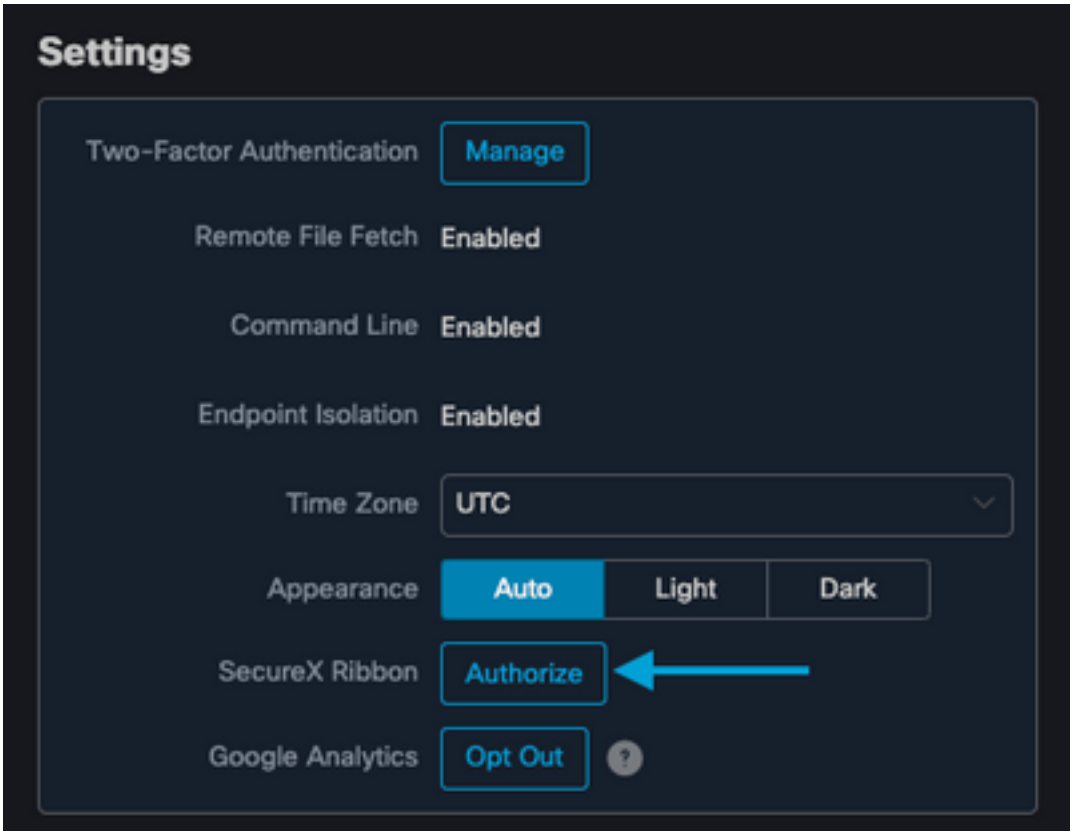


ملاحظة: هذه المعلومات متوفرة فقط في هذا الإطار، احفظ بيانات الاعتماد الخاصة بك في ملف نسخ إحتياطي.

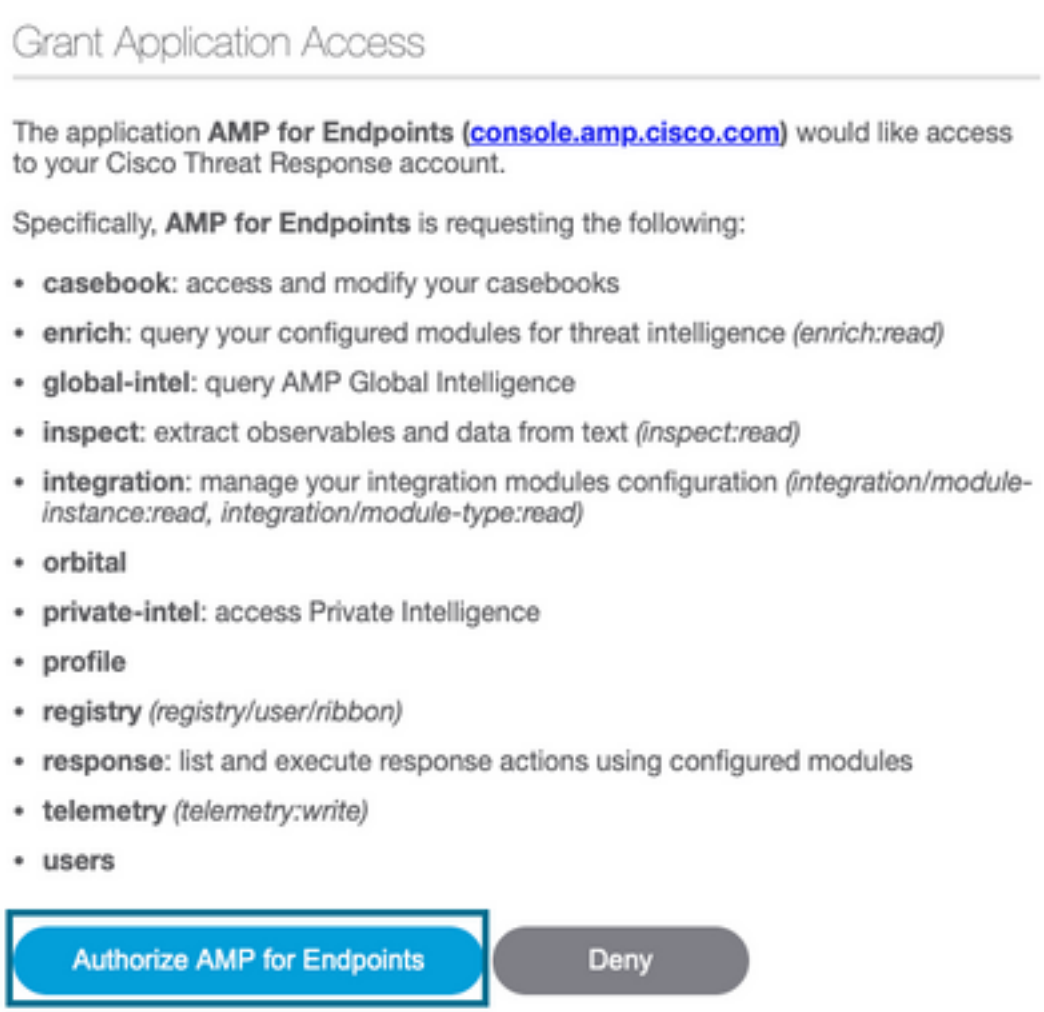
تمكين شريط SecureX في وحدة تحكم AMP

يعتبر برنامج SecureX وحدة تحكم مركزية ومجموعة موزعة من القدرات التي تعمل على توحيد إمكانية الرؤية وتمكين التشغيل التلقائي وتسريع عمليات سير العمل الخاصة باالستجابة للحوادث وتحسين عملية البحث عن التهديدات. يتم تقديم هذه الإمكانات الموزعة في شكل تطبيقات (تطبيقات) وأدوات في شريط SecureX، ويمكن تمكين شريط SecureX في وحدة تحكم AMP.

- تسجيل الدخول إلى SecureX
- على وحدة التحكم AMP
- انتقل إلى **الحسابات** > **المستخدمون** > انقر فوق **المستخدم**
- في **الإعدادات** انقر فوق **تخويل** شريط SecureX

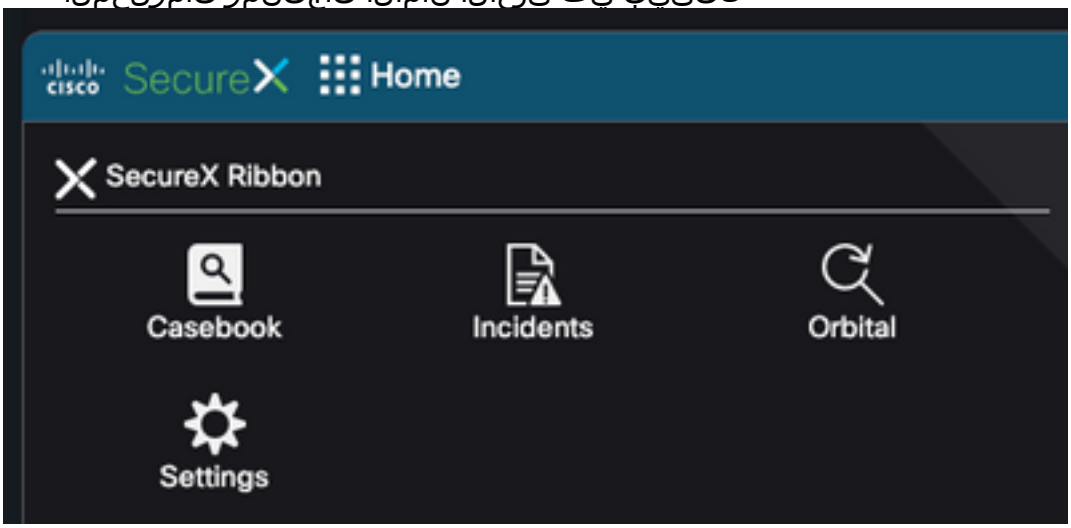


- تتم إعادة توجيهك إلى إستجابة تهديد SecureX
- انقر فوق **تخويل AMP لنقاط النهاية**



- يوجد الشريط في الجزء السفلي من الصفحة ولا يزال موجودا أثناء التنقل بين لوحة

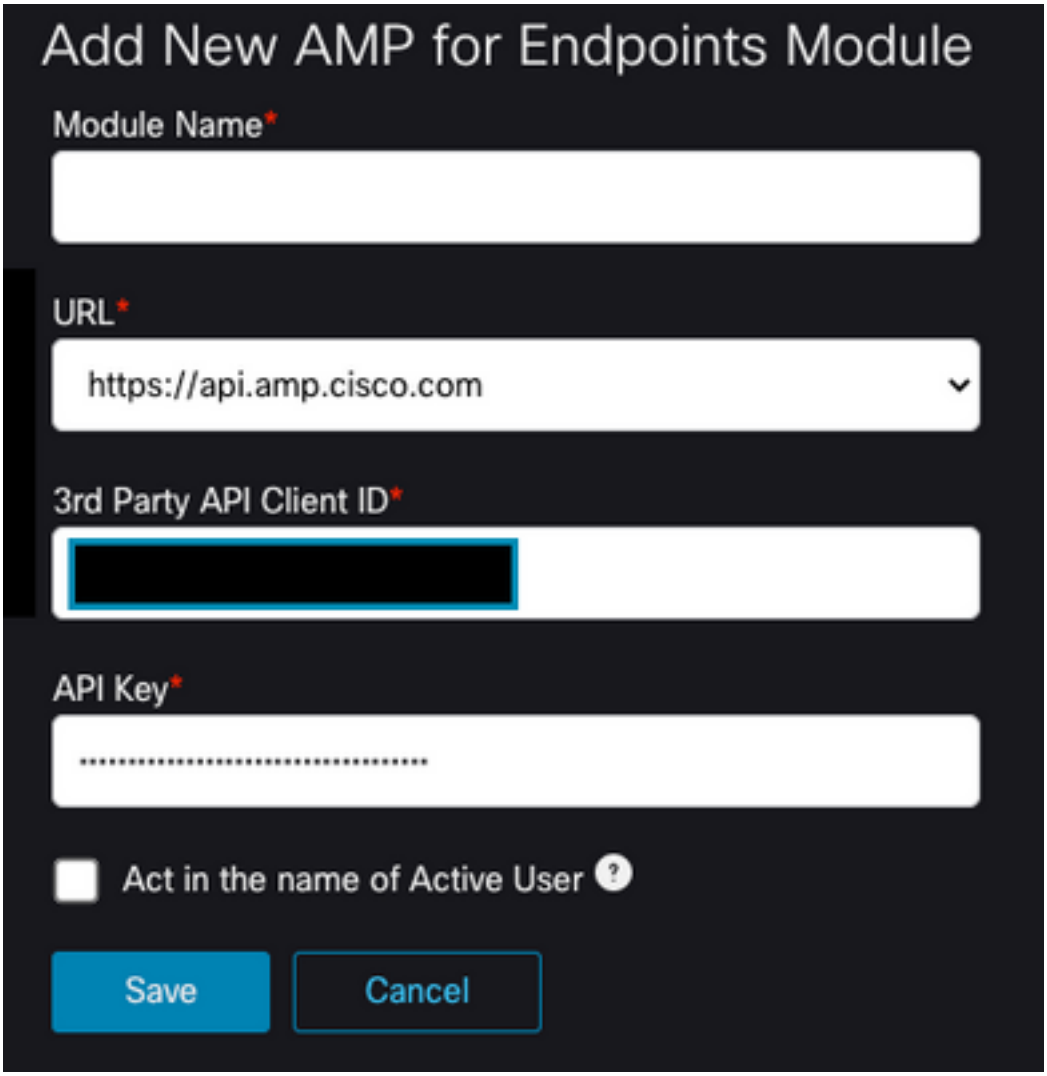
المعلومات ومنتجات الأمان الأخرى في بيئتك



دمج الوحدة النمطية AMP لنقاط النهاية في SecureX

تسمح لك الوحدة النمطية AMP for Endpoints بالتحري عن الملفات المتعددة ذات السياق وتحديدها من عمليات التكامل عبر منتجات الأمان. يوفر معلومات تفصيلية حول نقاط النهاية والأجهزة المتأثرة، بما في ذلك عناوين IP ونظام التشغيل ومعرف AMP GUID.

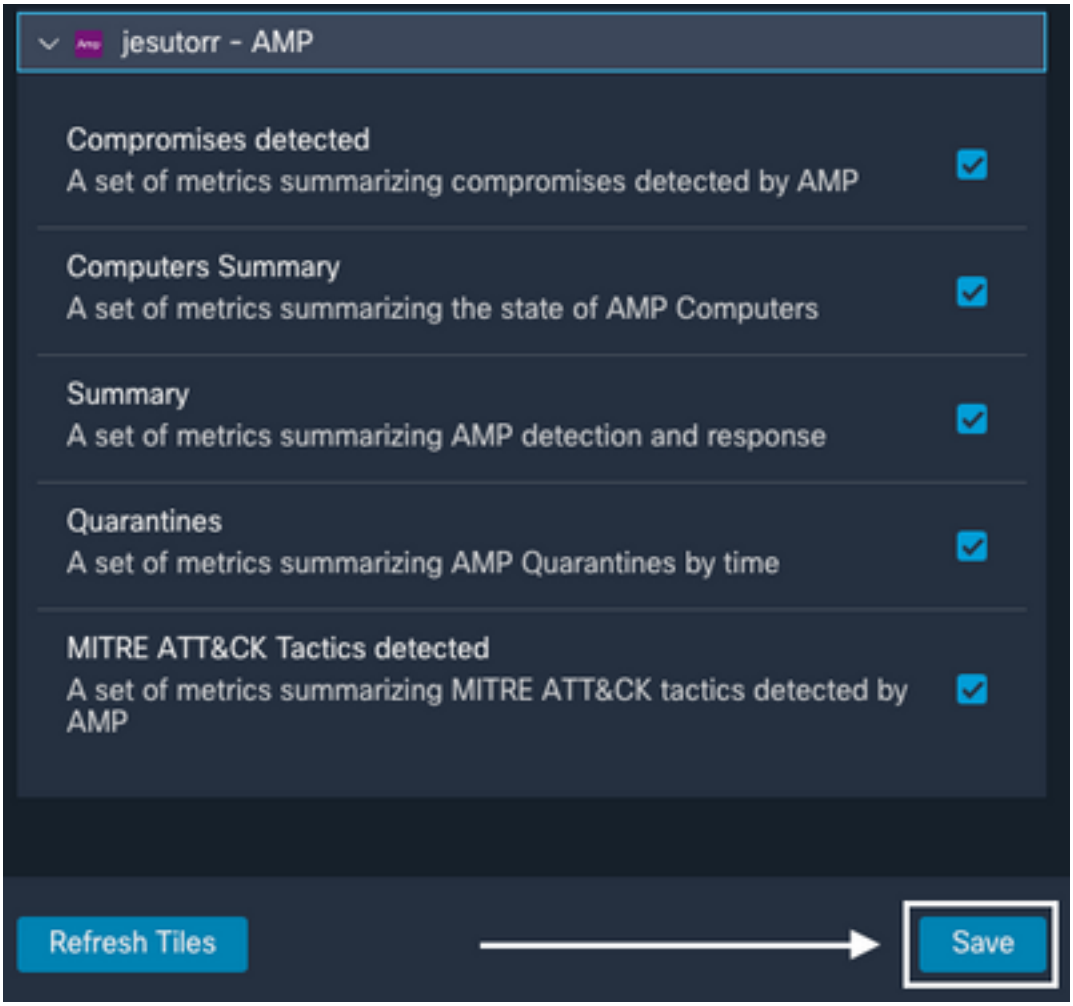
- في وحدة تحكم SecureX، انتقل إلى **عمليات التكامل>انقر فوق إضافة وحدة نمطية جديدة**
- انتقيت **AMP لنهاية نقطة** وحدة نمطية وطقطقة **يضيف وحدة نمطية جديدة**
- تسمية الوحدة النمطية
- تحديد سحابة AMP
- يتم إدخال بيانات اعتماد واجهة برمجة التطبيقات (API) التي تم تجميعها مسبقا تحت **معرف عميل واجهة برمجة التطبيقات (API)** من **الطرف الثالث ومفتاح واجهة برمجة التطبيقات (API)**



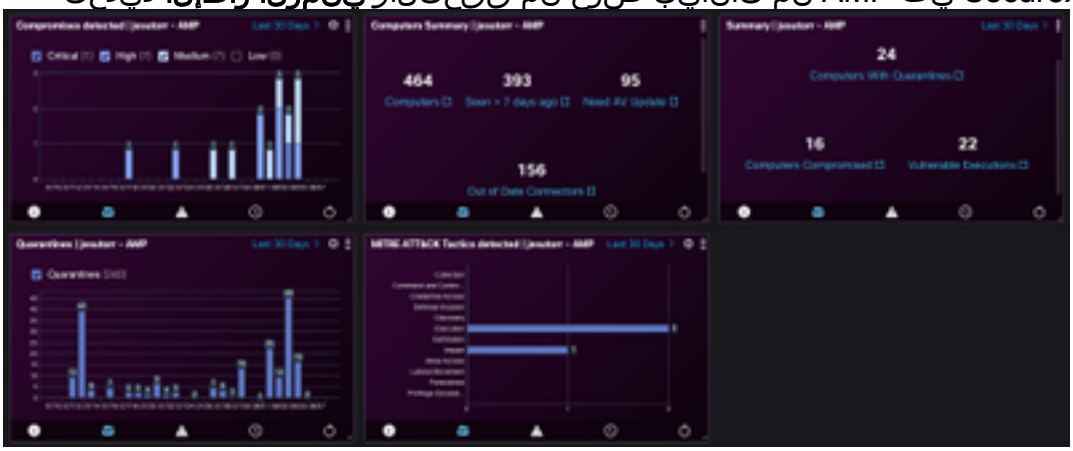
التحقق من الصحة

تحقق من عرض المعلومات من وحدة تحكم AMP في لوحة معلومات SecureX.

- انتقل على SecureX إلى **لوحة المعلومات**
- انقر فوق **لوحة معلومات جديدة** واسمها
- تحديد الوحدة النمطية AMP التي تم إنشاؤها مسبقا
- حدد المربعات، حيث يتم إضافة كل المربعات لهذا الدليل
- طقطقة **حفظ**



- تحديد **الإطار الزمني** والتحقق من عرض بيانات من AMP في SecureX



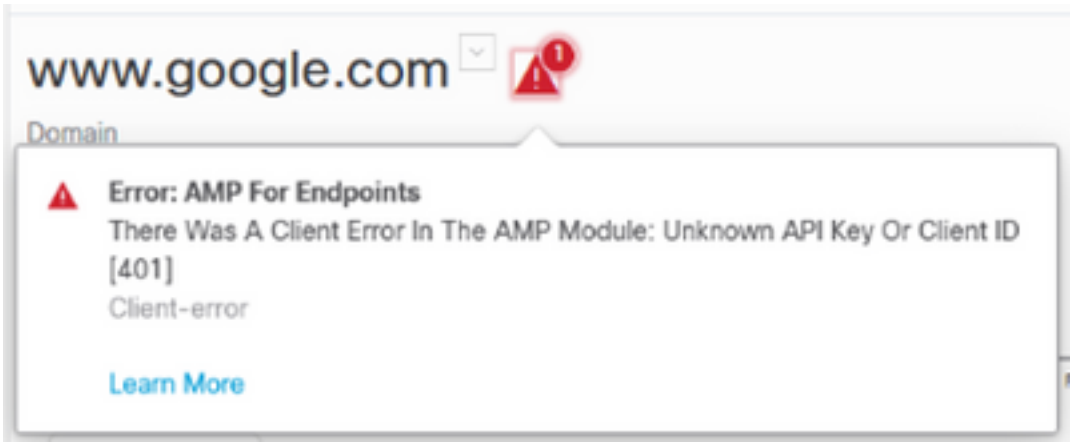
استكشاف الأخطاء وإصلاحها

عميل API ليس لديه حق الوصول للكتابة [403]

يتطلب SecureX - AMP لتكامل نقاط النهاية **AMP للقراءة والكتابة** واجهات برمجة التطبيقات (API) لنقاط النهاية، إن لم يكن كذلك، يتم عرض رسالة خطأ كما هو موضح في الصورة.

خطأ: مفتاح API غير معروف أو معرف العميل [401]

إذا كانت واجهات برمجة التطبيقات غير صالحة إذا تم إجراء تحقيق في "إستجابة تهديد SecureX" كما هو موضح في الصورة.



تحقق من صحة بيانات اعتماد API أو وجودها في وحدة تحكم AMP، إذا لم تكن صحيحة، فحاول مع بيانات اعتماد جديدة.

إذا كنت لا تزال تواجه مشكلات بعد مراجعة المعلومات الواردة أعلاه، فالرجاء الاتصال بفريق الدعم.

دليل الفيديو

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).