دمج SecureX واستكشاف أخطاءه وإصلاحها مع جهاز أمان الويب (WSA)

المحتويات

المقدمة

يصف هذا المستند الخطوات المطلوبة لتكامل SecureX مع جهاز أمان الويب (WSA) والتحقق منه واستكشاف أخطاء هذا التكامل وإصلاحها

المتطلبات الأساسية

المتطلبات

توصي Cisco بأن تكون لديك معرفة بالمواضيع التالية:

- جهاز أمان الويب (WSA)
- المحاكاة الافتراضية الاختيارية للصور

المكونات المستخدمة

- جهاز أمان الويب (WSA)
- تبادل خدمات الأمان (SSE)
- بوابة SecureX

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

عناوين URL المطلوبة لكل منطقة ل SecureX

تحقق من أن جهاز WSA لديه إمكانية الوصول إلى عناوين URL على المنفذ 443:

المنطقة الامريكية

- api-sse.cisco.com

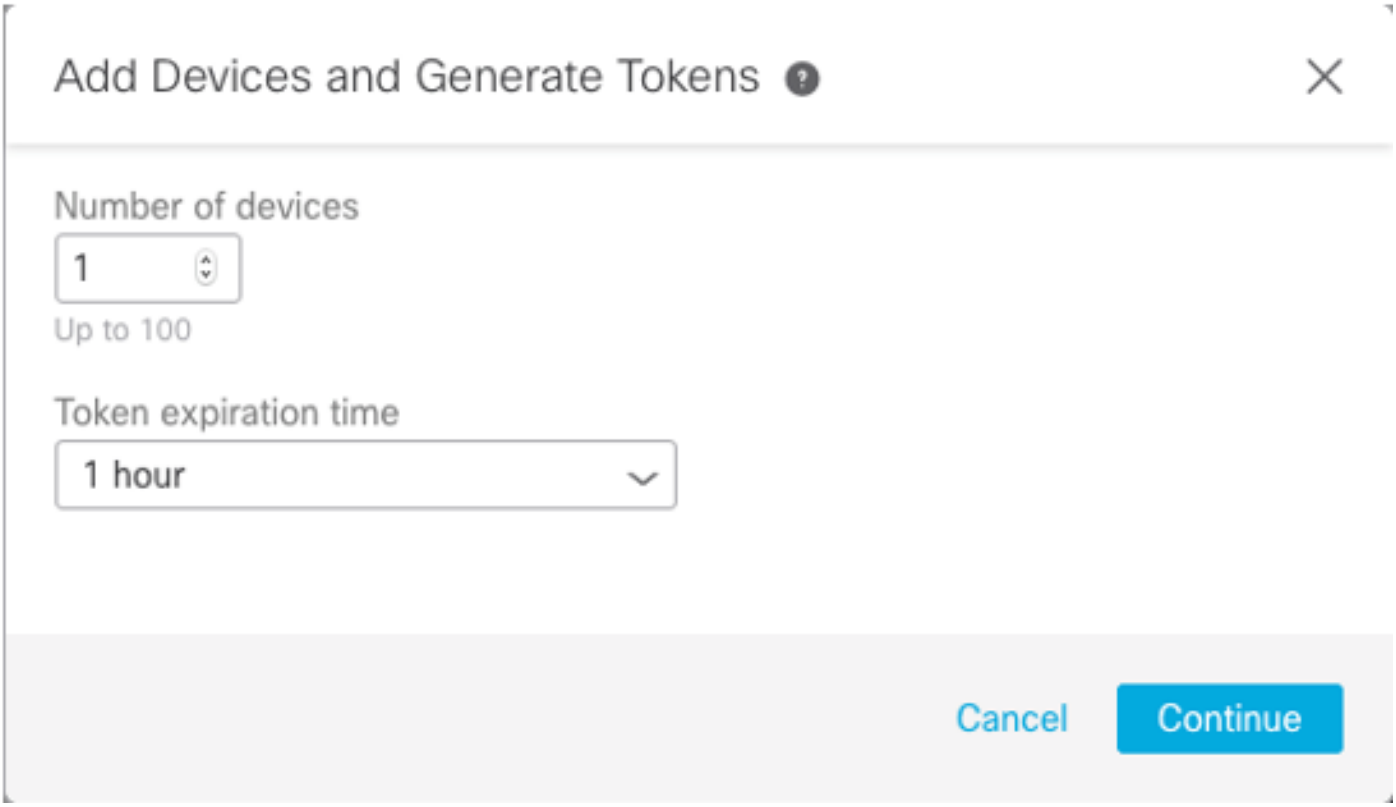
منطقة الاتحاد الأوروبي

- api.eu.sse.itd.cisco.com

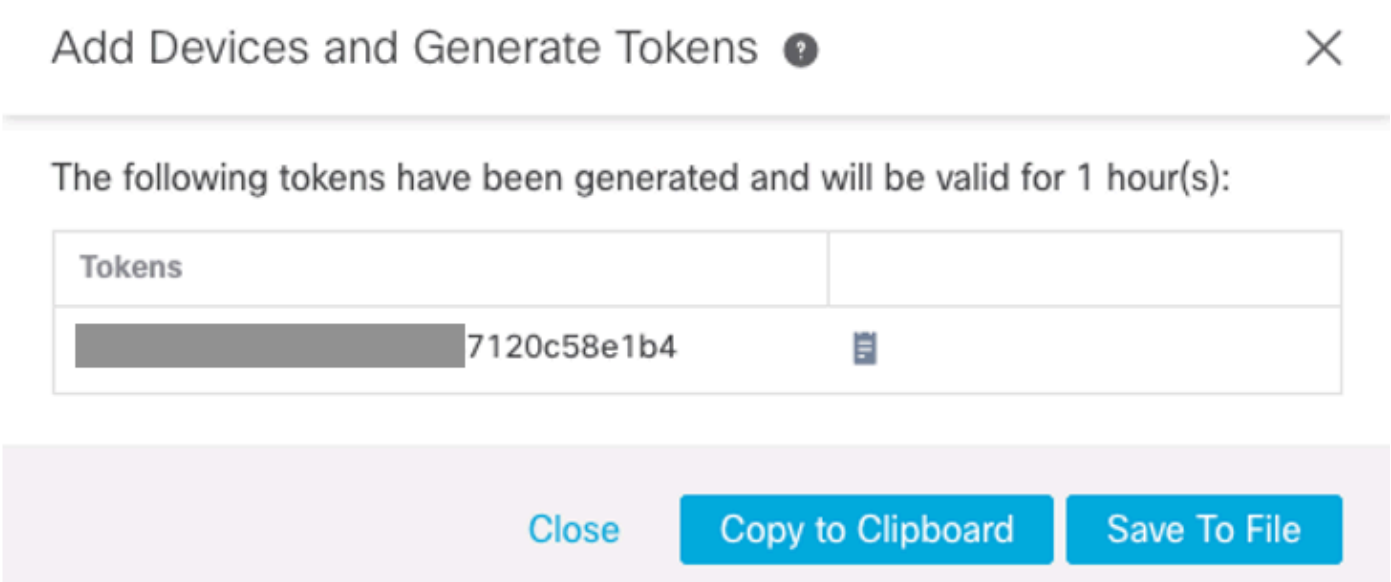
ملاحظة: إذا كان الوصول إلى SecureX باستخدام عنوان URL لآسيا والمحيط الهادئ واليابان والصين (https://visibility.apjc.amp.cisco.com/)، فإن الدمج مع الجهاز غير مدعوم حاليا.

إعداد WSA لتسجيل SSE

1.- على بوابة SSE، انتقل إلى الأجهزة ثم انقر فوق (+) إضافة الأجهزة وإنشاء الرموز المميزة، كما هو موضح في الصورة:



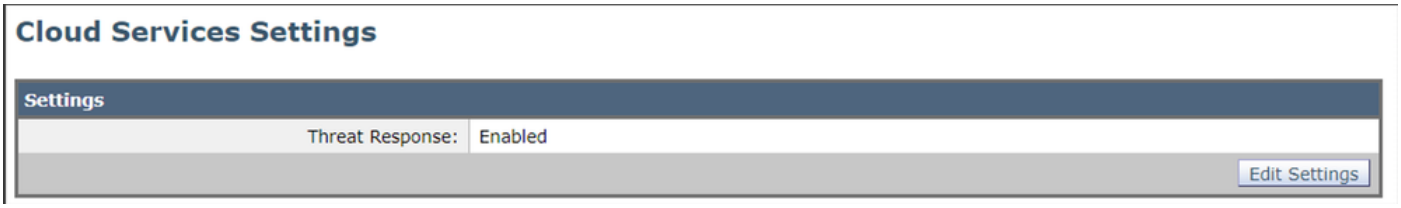
2.- انقر فوق متابعة ويتم إنشاء الرمز المميز ل WSA، كما هو موضح في الصورة.



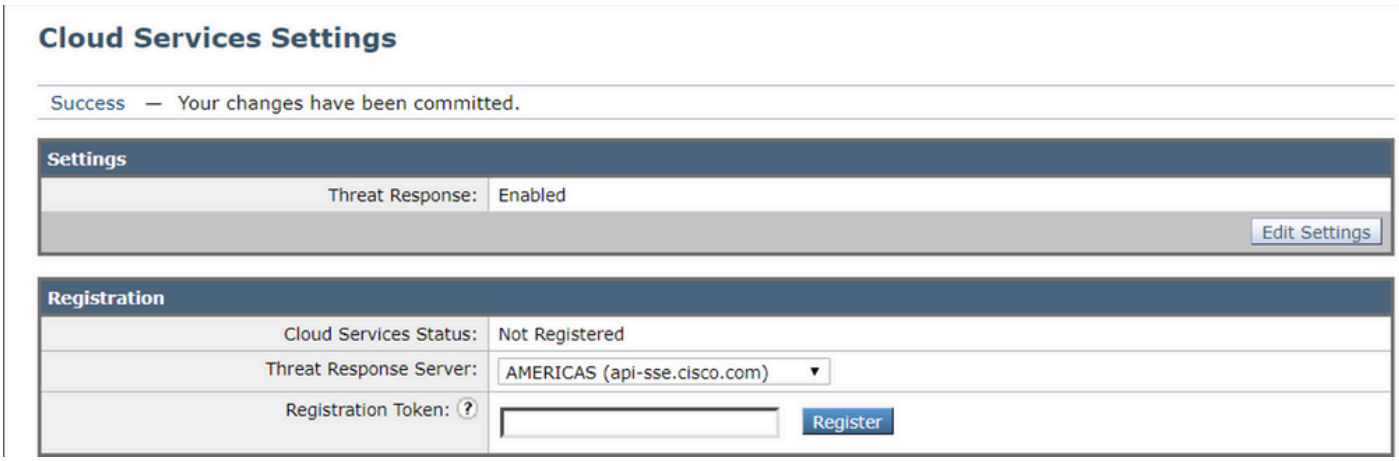
3.- قم بتمكين Ctrobservable في واجهة سطر أوامر WSA (CLI)، تحت ReportIngconfig يمكنك العثور على الخيار لتمكين Ctrobservable، كما هو موضح في الصورة:

```
WSA-[redacted].COM> reportingconfig


hoose the operation you want to perform:
 COUNTERS - Limit counters recorded by the reporting system.
 WEBTRACKINGQUERYTIMEOUT - Timeout value for Webtracking Queries.
 AVERAGEOBJECTSIZE - Average HTTP Object Size used for Bandwidth Savings
alculation.
 WEBEVENTBUCKETING - Enable or Disable web transaction event bucketing.
 CTROBSERVABLE - Enable or Disable CTR observable based indexing.
 CENTRALIZED - Enable/Disable Centralized Reporting for this WSA appliance.
]> ctrobservable

TR observable indexing currently Enabled.
re you sure you want to change the setting? [N]> y


hoose the operation you want to perform:
 COUNTERS - Limit counters recorded by the reporting system.
 WEBTRACKINGQUERYTIMEOUT - Timeout value for Webtracking Queries.
 AVERAGEOBJECTSIZE - Average HTTP Object Size used for Bandwidth Savings Calculation.
 WEBEVENTBUCKETING - Enable or Disable web transaction event bucketing.
 CTROBSERVABLE - Enable or Disable CTR observable based indexing.
 CENTRALIZED - Enable/Disable Centralized Reporting for this WSA appliance.
```

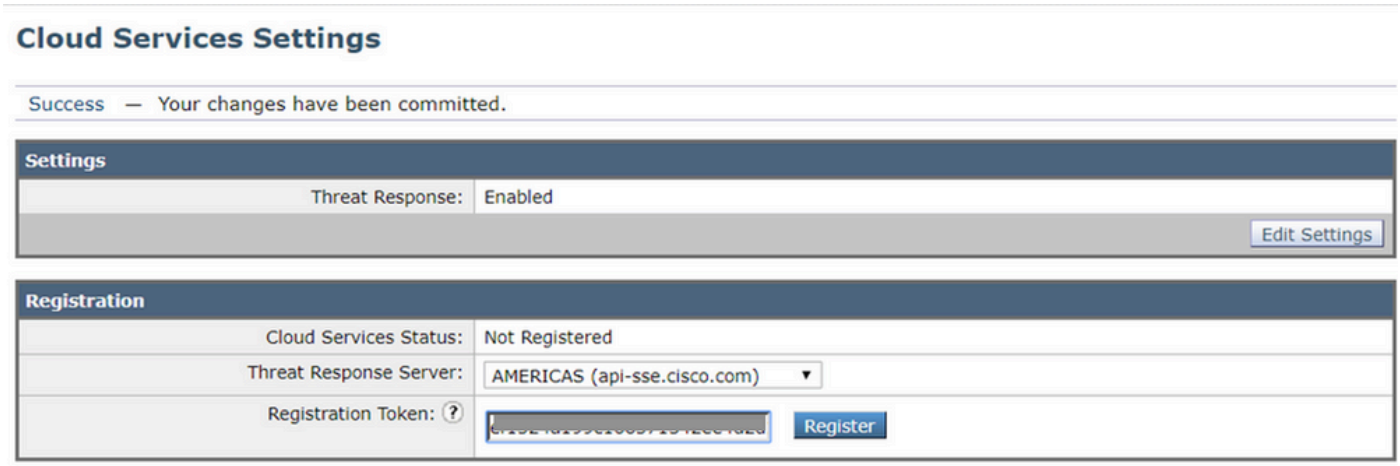
4.- تمكين بوابة السحابة الخاصة بتبادل خدمات الأمان (SSE) والتنقل إلى الشبكة >إعدادات خدمات السحابة > تحرير الإعدادات، انقر فوق تمكين وإرسال ، كما هو موضح في الصورة:



5.- حدد السحابة التي تريد الاتصال بها:

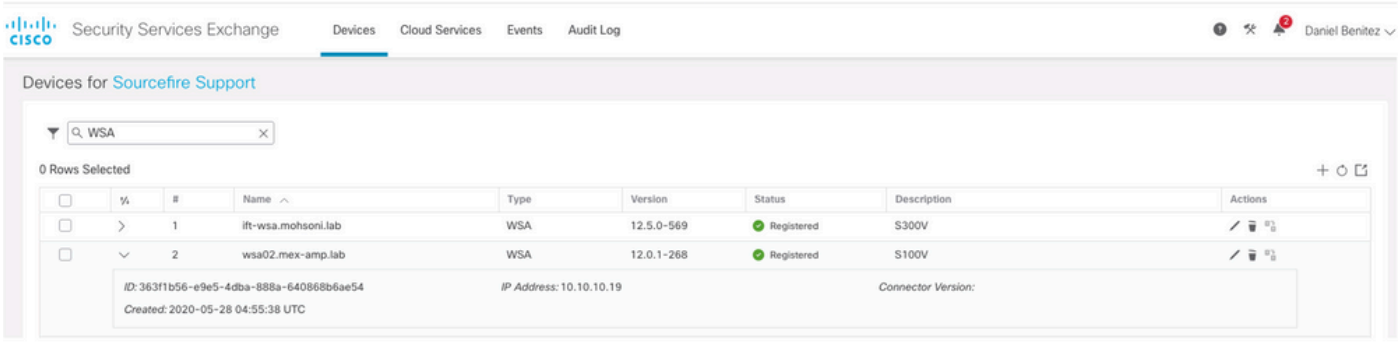


6.- أدخل الرمز المميز الذي أنشأته على SEE (تأكد من إستخدام الرمز المميز قبل وقت انتهاء الصلاحية):



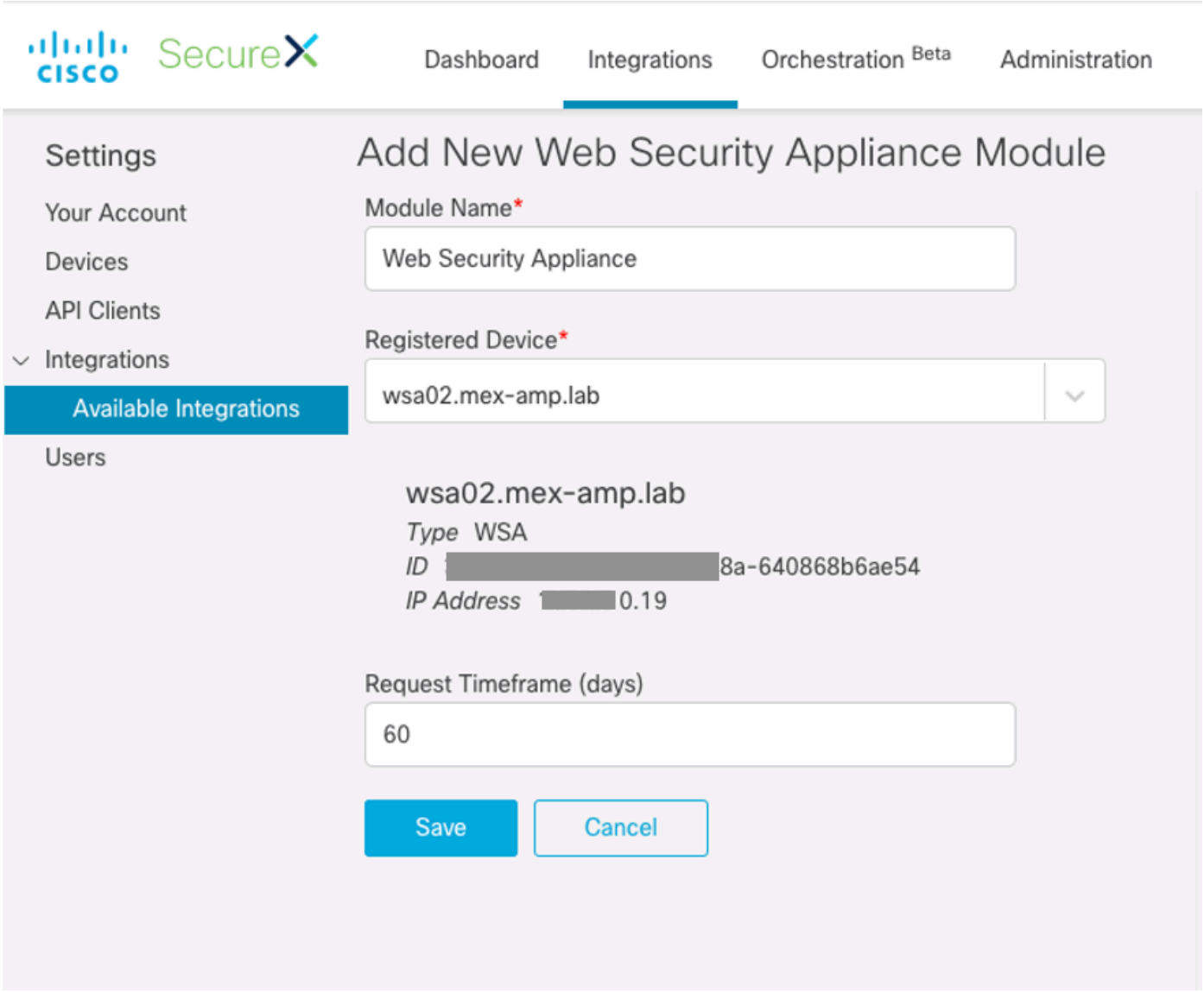
7.- بمجرد تسجيل الرمز المميز، ستري رسالة تشير إلى تسجيل الجهاز بنجاح

8.- بعد ذلك، ترى الجهاز المسجل على بوابة SSE:

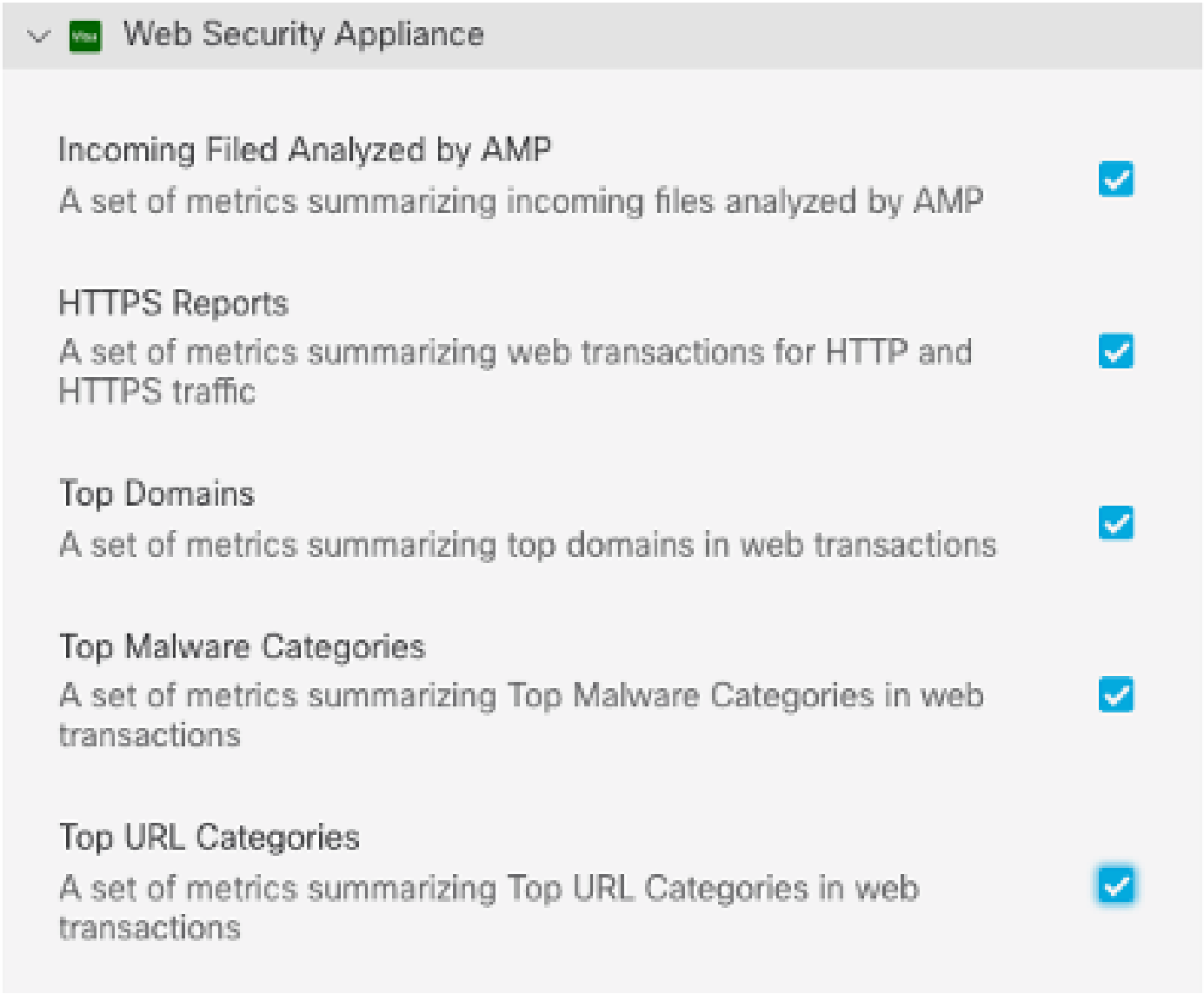


دمج الجهاز لديك مع SecureX

الخطوة 1. لدمج WSA مع SecureX، انتقل إلى عمليات التكامل>إضافة وحدة نمطية جديدة وحدد جهاز أمان الويب، ثم حدد جهازك، وقم بإعداد الإطار الزمني للطلب، ثم انقر فوق حفظ، كما هو موضح في الصورة.

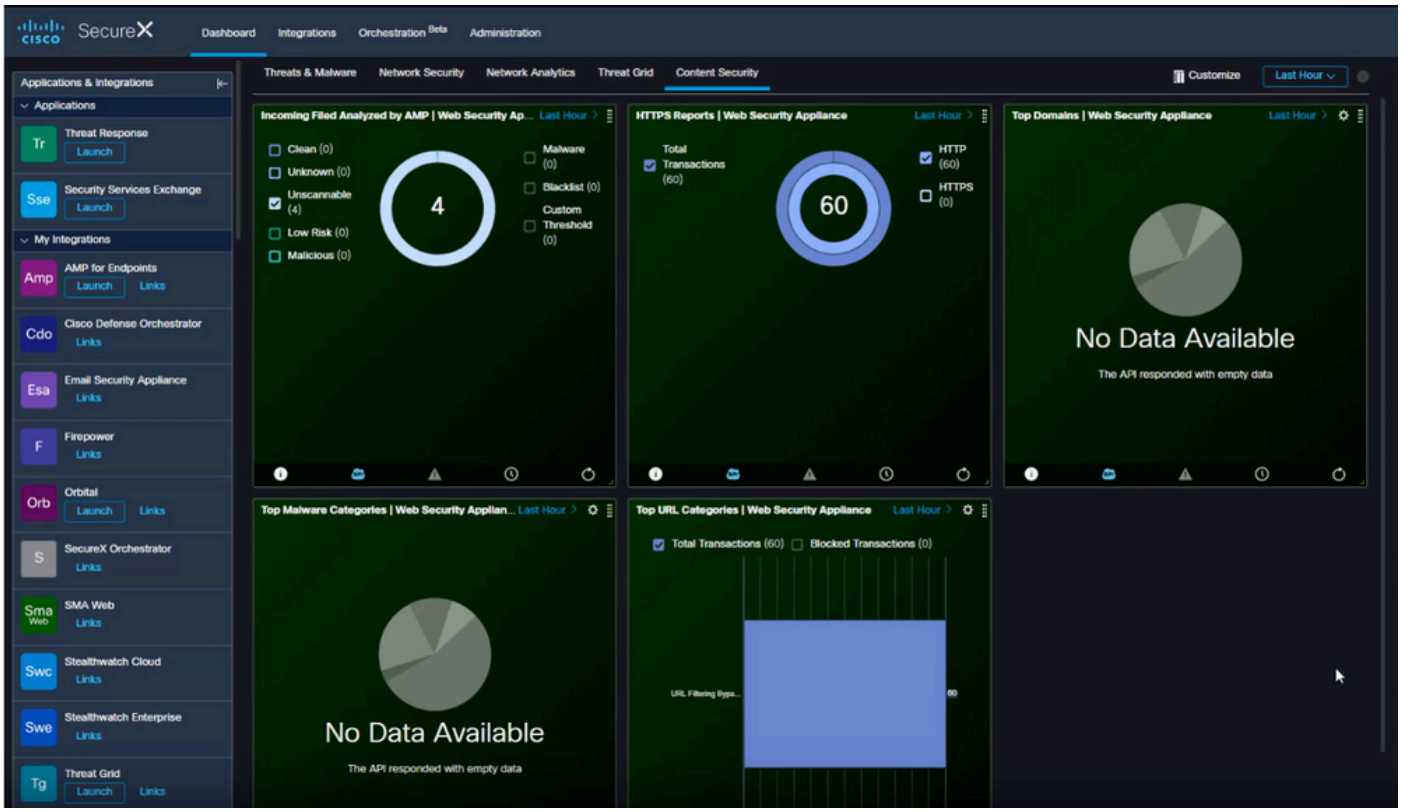


الخطوة 2. لإنشاء لوحة المعلومات الخاصة بك، انقر فوق أيقونة + لوحة معلومات جديدة، حدد اسما وتجانبا تريد إستخدامهما للوحة المعلومات.



التحقق من الصحة

بعد إجراء التكامل يمكنك مشاهدة معلومات لوحة المعلومات التي تم نشرها في نموذج SSE، يمكنك النقر فوق أي من التهديدات التي تم الكشف عنها وتم تشغيل بوابة SSE مع عامل تصفية نوع الحدث عليها.



استكشاف الأخطاء وإصلاحها

التحقق من تسجيل الجهاز من CLI

الخطوة 1. قم بتشغيل الأمر curl في الجهة الخلفية للتحقق من حالة الاتصال. ابحث عن حقل الحالة تحت التبادل من الإخراج المتوافق مع الحقول مثل FQDN(اسم المجال المؤهل بالكامل)، التسجيل. الجهاز المسجل في الحالة المسجلة:

<#root>

/usr/local/bin/curl -XGET -v

http://localhost:8823/v1/contexts/default

```
  "exchange": [
                    {
                     "type": "registration",

"status": "Enrolled"

,
                     "name": "",
                     "description": "Device has been enrolled."
```

الخطوة 2. من هذا الإخراج، يمكنك أيضا التحقق من الاستعلامات التي تم إجراؤها من الموصل:

```
type": "administration",
         "statistics": {
            "transactionsProcessed": 20,
           "failedTransactions": 0,
           "lastFailedTransaction": "0001-01-01T00:00:00Z",
            "requestFetchFailures": 0,
            "responseUploadFailures": 0,
            "commandsProcessed": 20,
            "commandsFailed": 0,
            "lastFailedCommand": "0001-01-01T00:00:00Z"
```

الخطوة 3. يمكنك أيضا التحقق من نبضات القلب التي تم عملها من الموصل إلى SSE (5 دقائق بشكل افتراضي):

```
refresh": {
              "registration": {
                "timestamp": "2010-06-29T03:51:45Z",
                "timeTaken": 1.387869786,
                "successCount": 6,
                "failureCount": 0
```

الخطوة 4. للتحقق من سجلات الموصل على WSA، يلزمك التنقل إلى:

<#root>

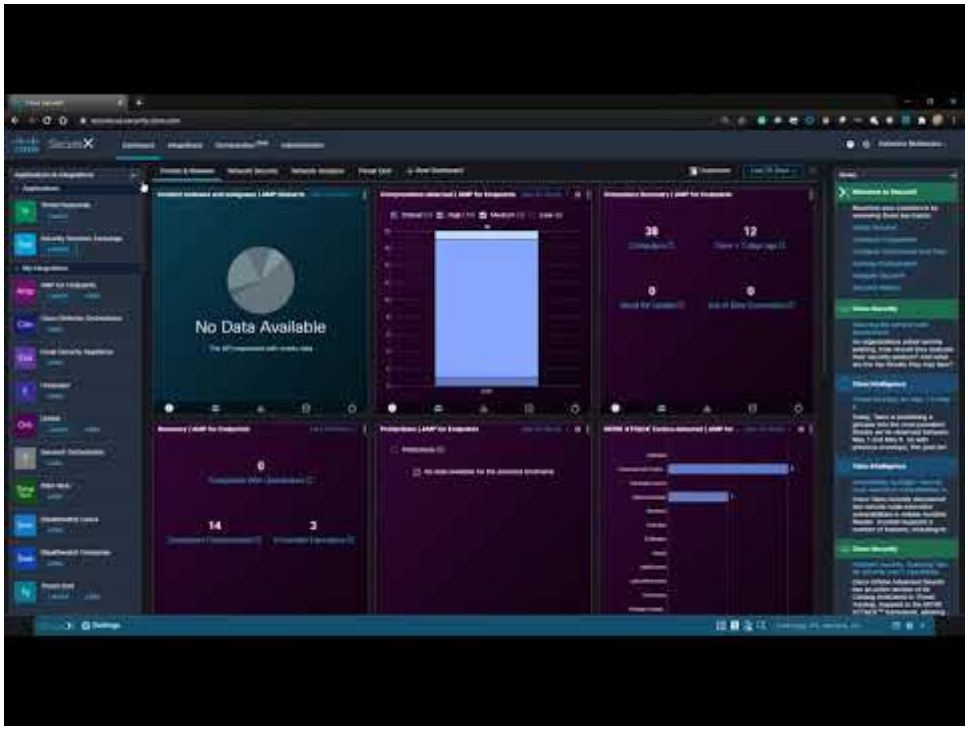
/data/pub/sse_connectord_logs/sse_connectord_log.current

المعلومات التي يمكن العثور عليها في sse_connectord_log.current

- حركة التسجيل مع SSE
- سجلات استعلام الإثراء
- سجلات إلغاء التسجيل في بوابة SSE

الفيديو

يمكنك العثور على المعلومات الواردة في هذا المستند في هذا الفيديو


No Data Available
38
12
0
0
0
14
3

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).