دمج SNA للتقسيم باستخدام تطبيق سحابة الأمان

المحتويات

المقدمة

المتطلبات الأساسية

المتطلبات

المكونات المستخدمة

التكوين

المشكلات الشائعة وحلولها

المقدمة

يصف هذا المستند تكامل SNA السلس مع Splunk باستخدام Cisco Security Cloud للاستجابة السريعة للحوادث للتهديدات المحددة.

المتطلبات الأساسية

معرفة أساسية بأجهزة Splunk و Cisco.

المتطلبات

لا توجد متطلبات خاصة لهذا المستند.

المكونات المستخدمة

تستند المعلومات الواردة في هذا المستند إلى إصدارات المكونات المادية والبرامج التالية:

مؤسسة Splunk

Secure Network Analytics v7.5.2.

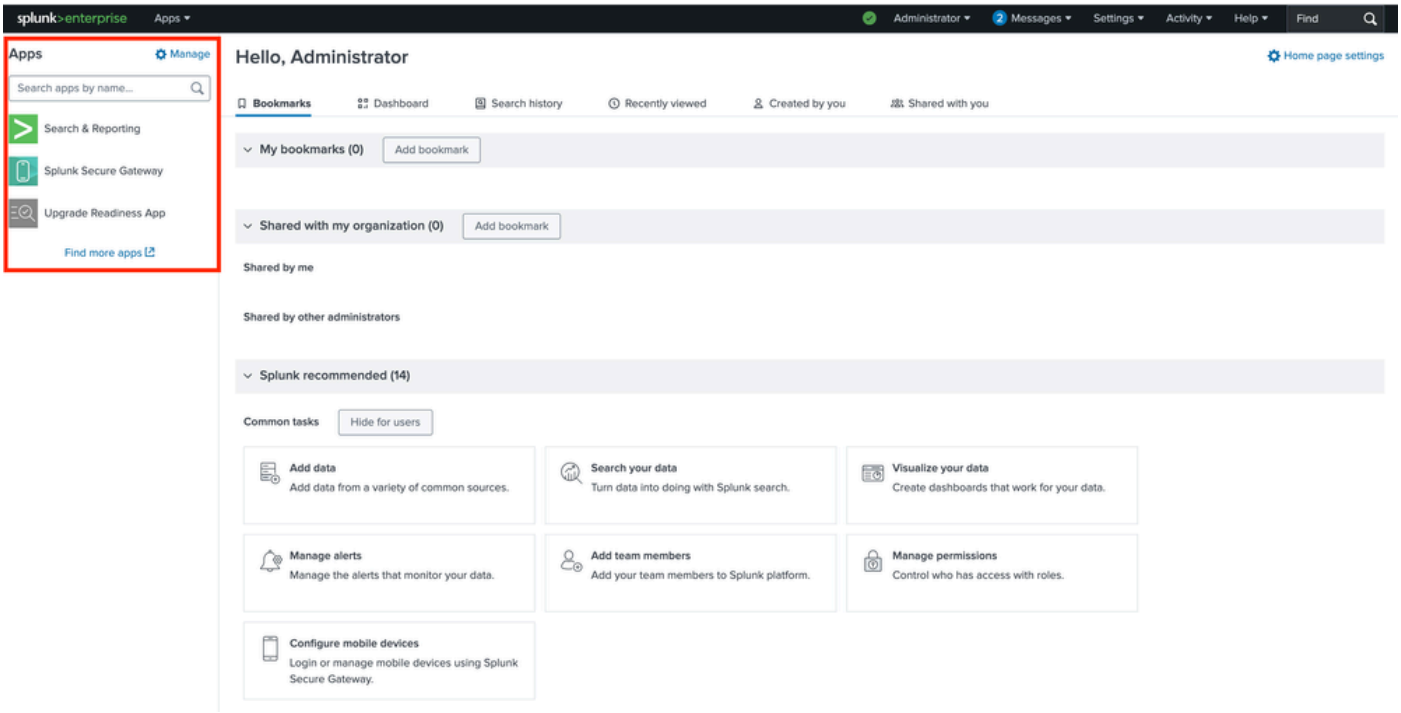
تم إنشاء المعلومات الواردة في هذا المستند من الأجهزة الموجودة في بيئة معملية خاصة. بدأت جميع الأجهزة المُستخدمة في هذا المستند بتكوين ممسوح (افتراضي). إذا كانت شبكتك قيد التشغيل، فتأكد من فهم للتأثير المحتمل لأي أمر.

التكوين

الخطوة 1: قم بالوصول إلى تطبيق Splunk وتثبيت تطبيق Cisco Security Cloud.

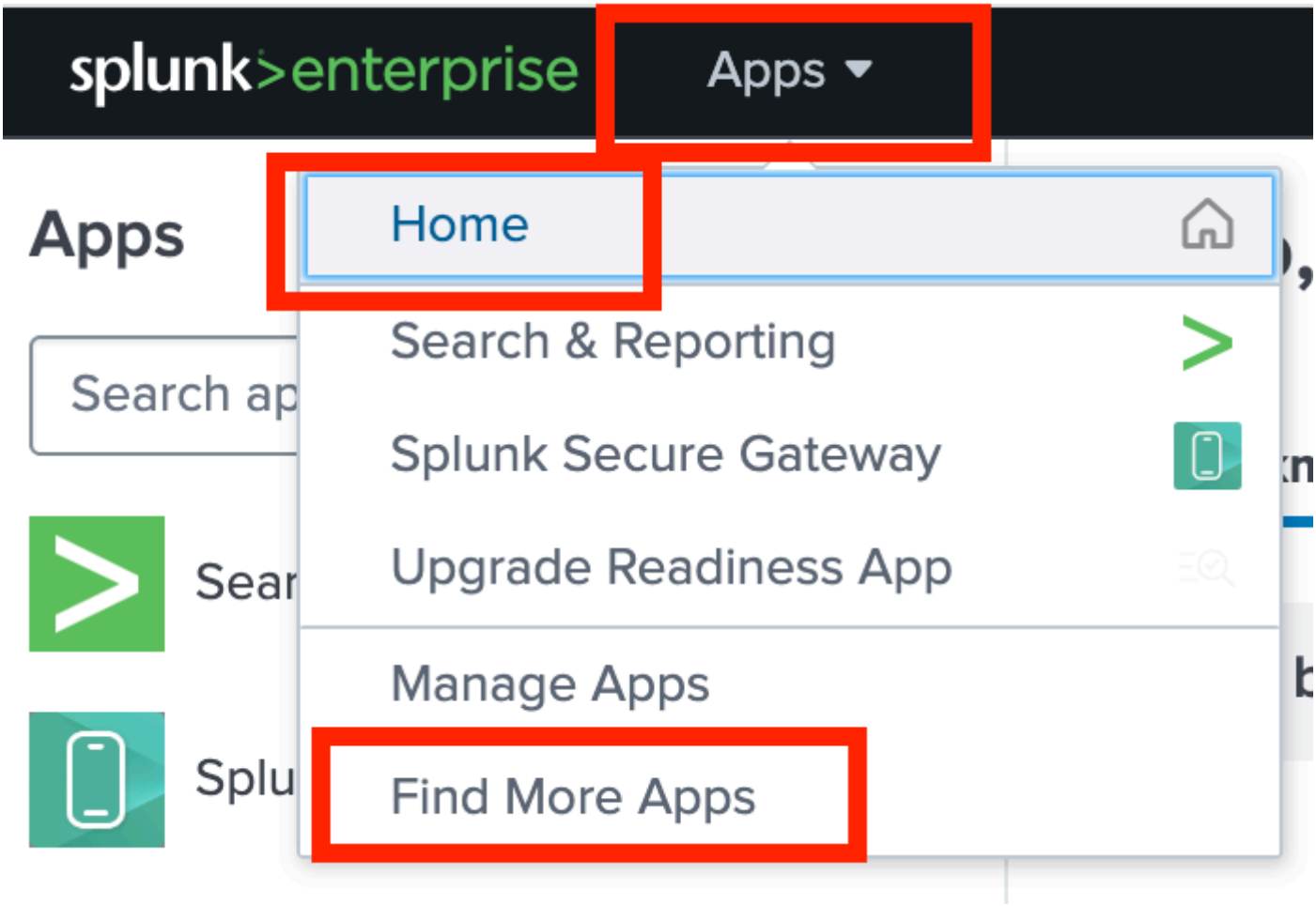
ط. قم بتسجيل الدخول إلى مدخل ويب Splunk باستخدام بيانات اعتماد المسؤول وفي تسجيل الدخول الناجح، يمكن رؤية الصفحة الرئيسية باستخدام قائمة التطبيقات

المثبتة على الجانب الأيسر ضمن قسم "التطبيق":

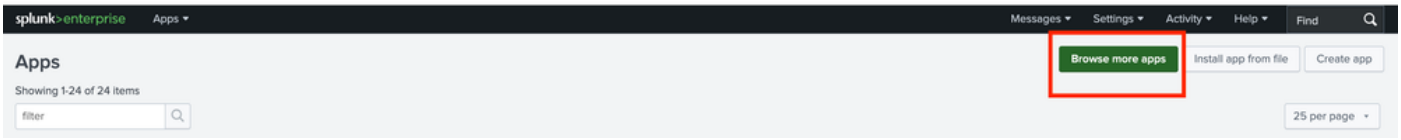


ثانيا. لدمج SNA مع Splunk، يلزم تثبيت تطبيق سحابة أمان Cisco الذي يمكن تحقيقه في أي من الطريقتين المذكورتين:

1. حدد بحث عن المزيد من التطبيقات من القائمة المنسدلة.



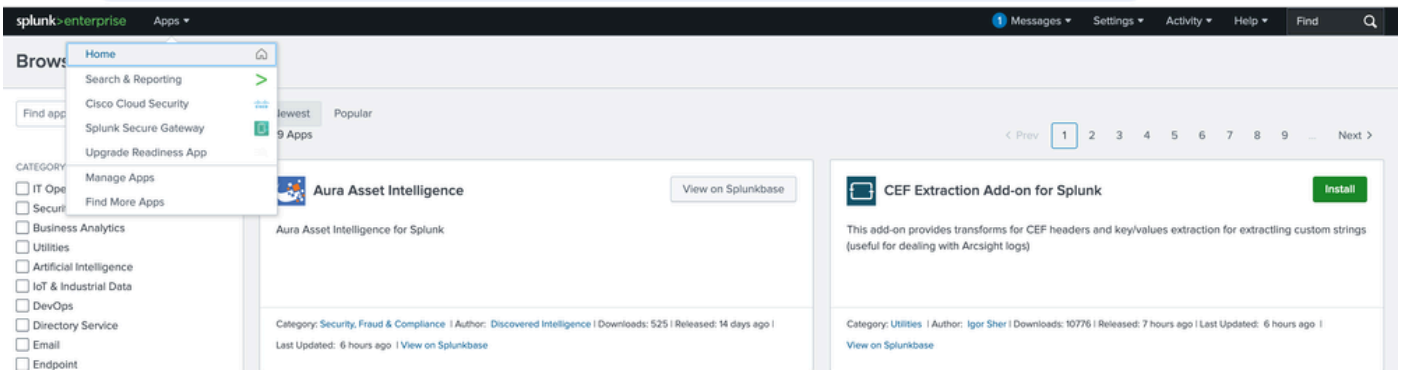
ب. استعرض المزيد من التطبيقات تحت رمز العتاد الخاص بالمدير.



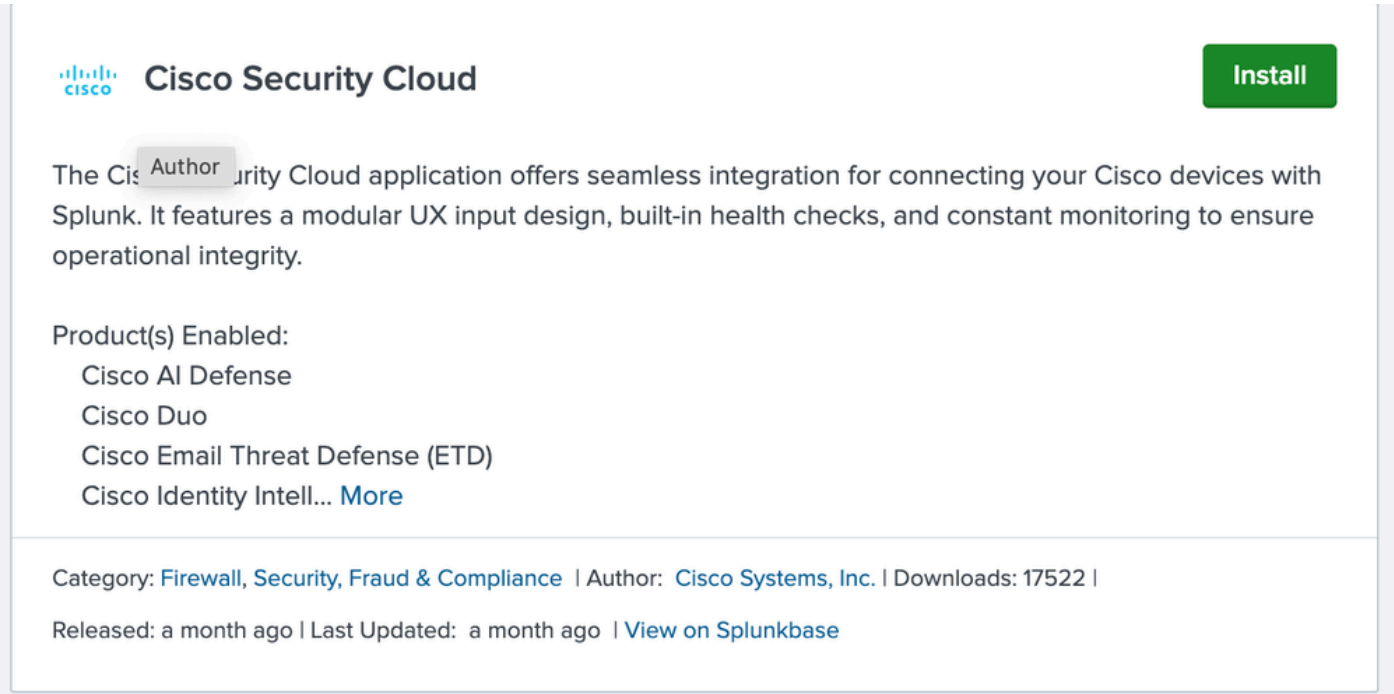
الخطوة 2: تثبيت تطبيق سحابة أمان Cisco.

ط. ابحث عن تطبيق Cisco Security Cloud. الآن، قم بالتمرير لأسفل حتى تجد التطبيق أو ابحث عن سحابة أمان Cisco.

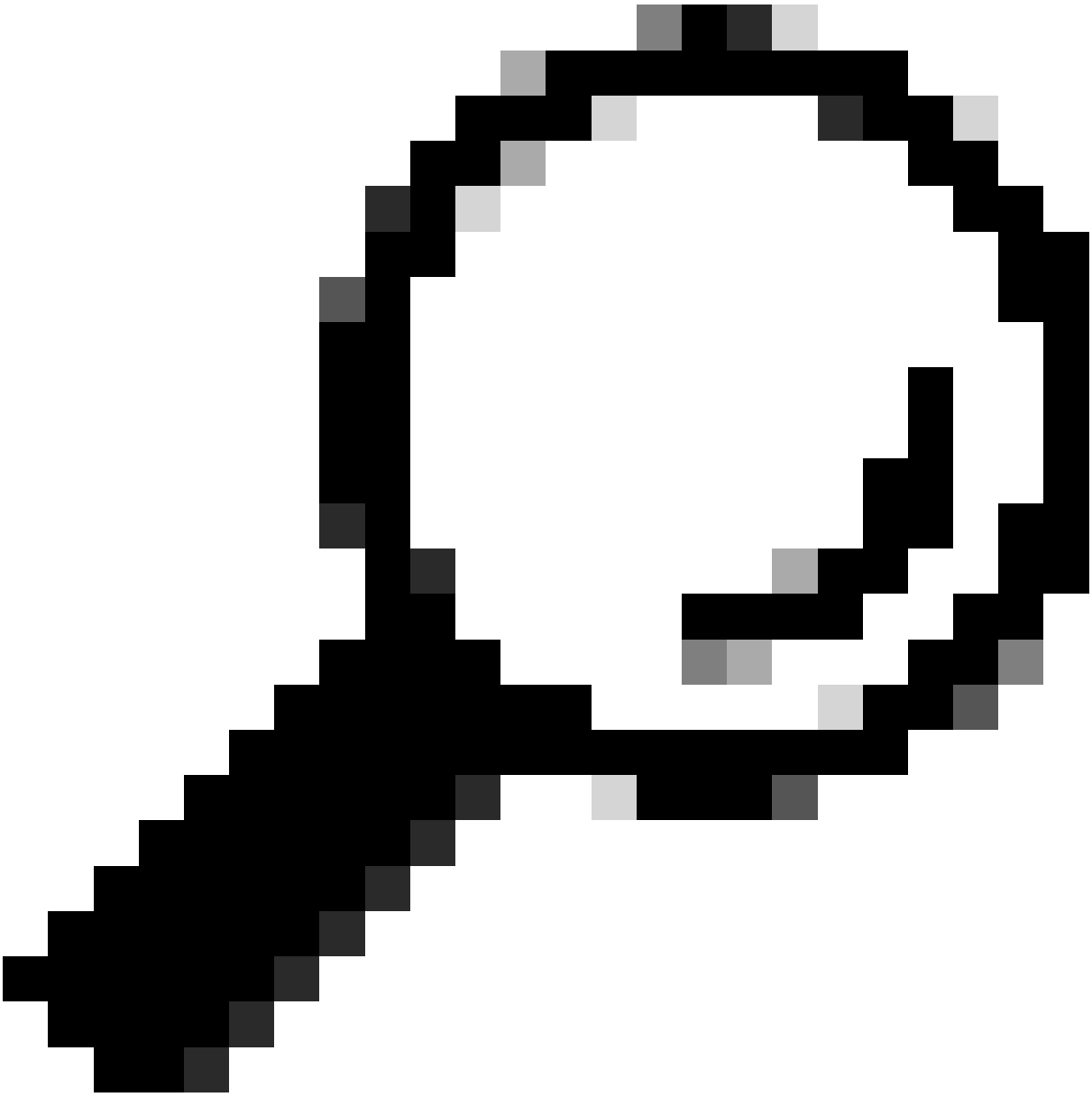
تحذير: لا تختلط مع تطبيق أمان السحابة من Cisco.



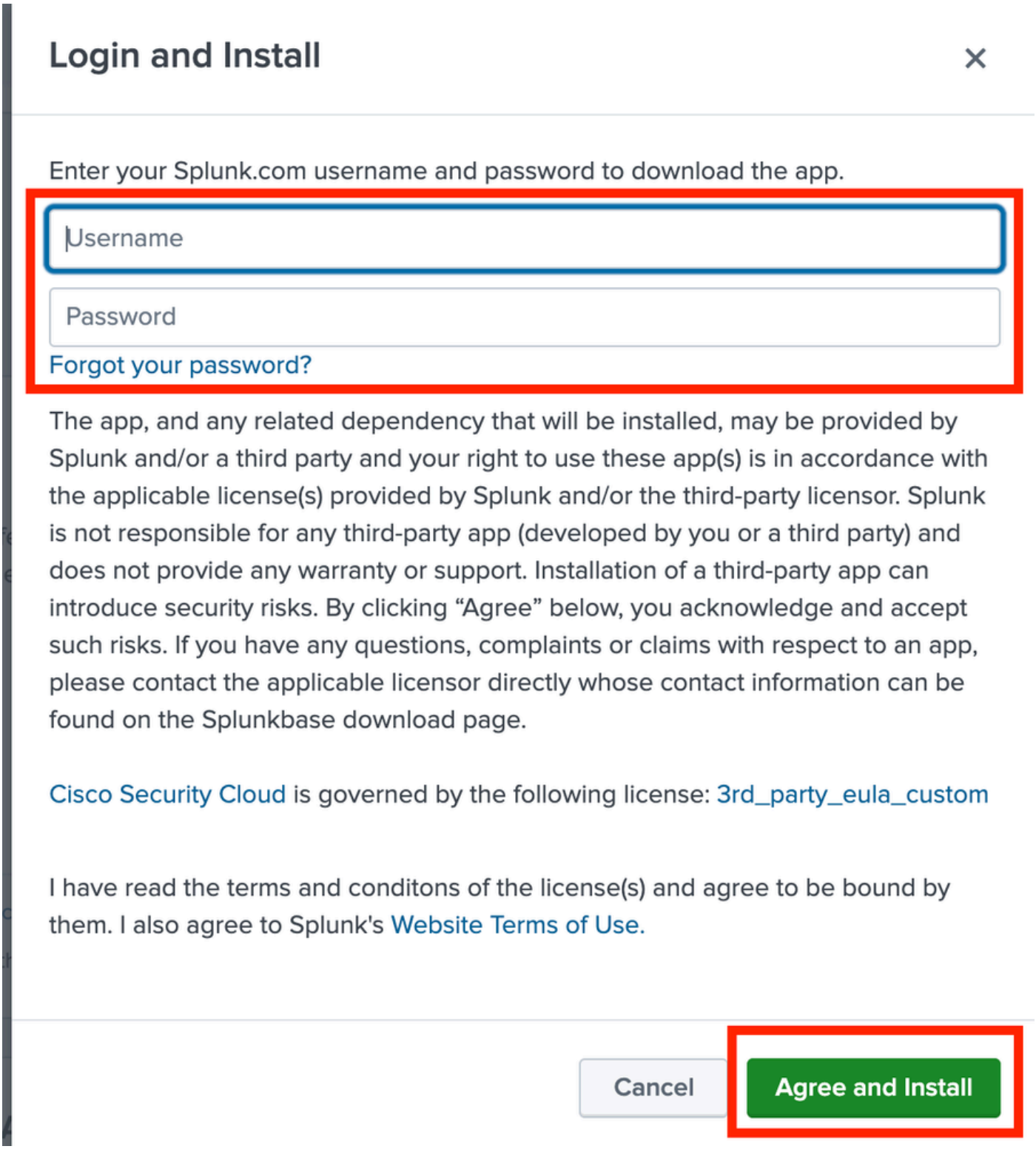
ثانياً. قم بتثبيت التطبيق بالنقر فوق الزر تثبيت.



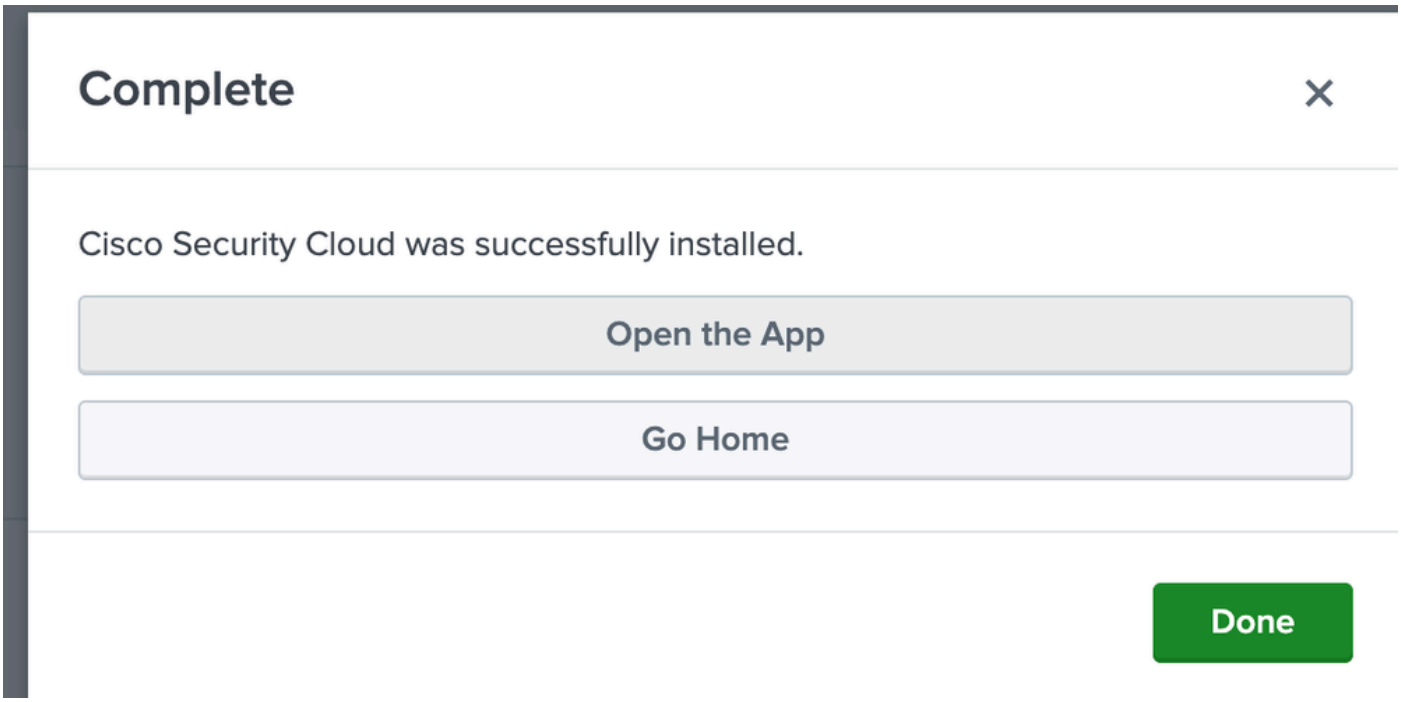
ثالثا. تظهر اللحظة التي تنقر فيها على زر التثبيت نافذة تطلب بيانات اعتماد حساب Splunk قبل تثبيت التطبيق. قم بتوفير بيانات الاعتماد وانقر فوق موافقة وتثبيت للمتابعة.



تلميح: قم بتوفير بيانات الاعتماد التي يتم إستخدامها للوصول إلى مدخل Splunk، وليس بيانات اعتماد المسؤول المستخدمة لتطبيق Splunk Enterprise أثناء تسجيل الدخول.

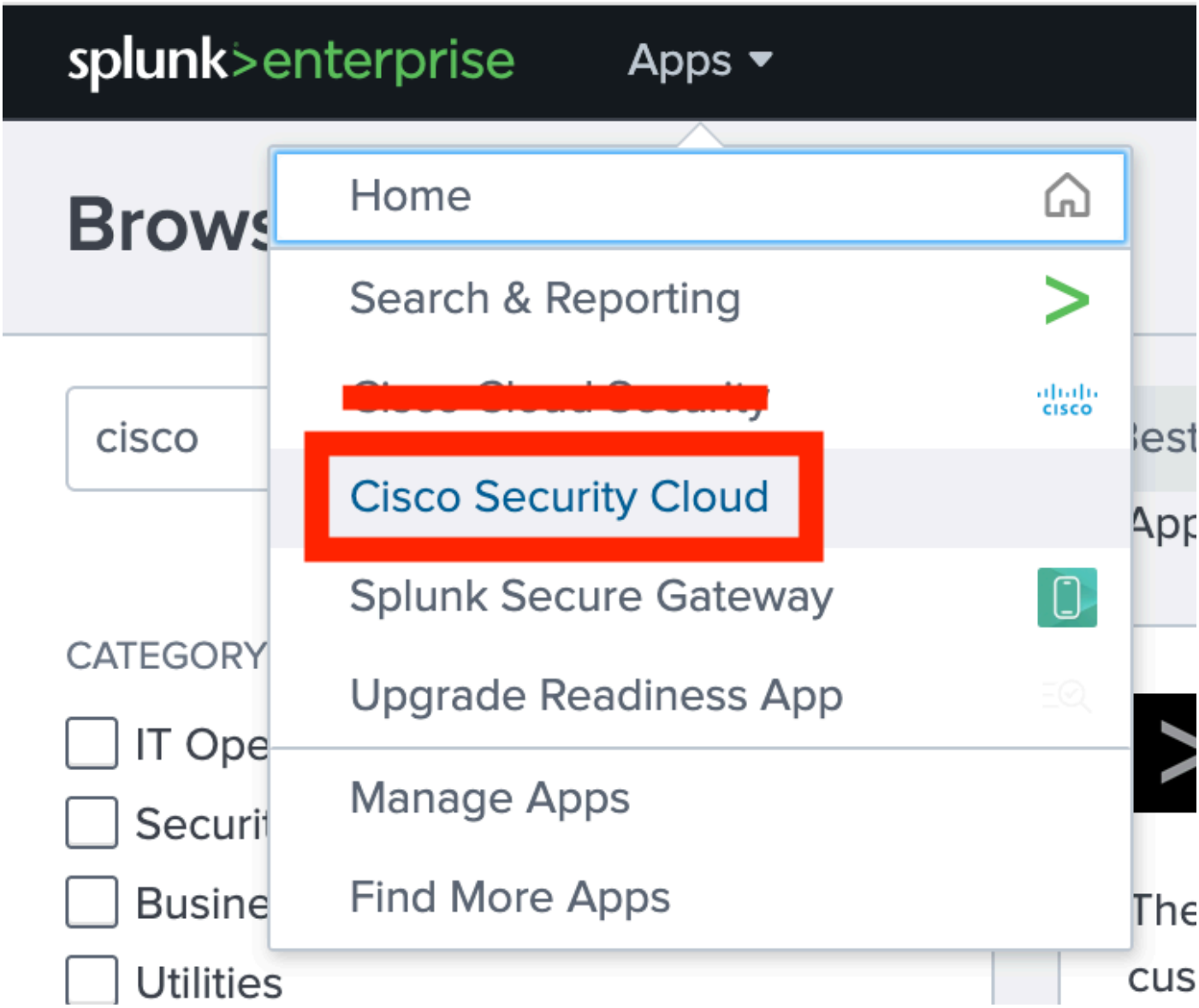


رابع. تظهر رسالة حول التثبيت الناجح للتطبيق كما هو موضح. طقطقة تم.

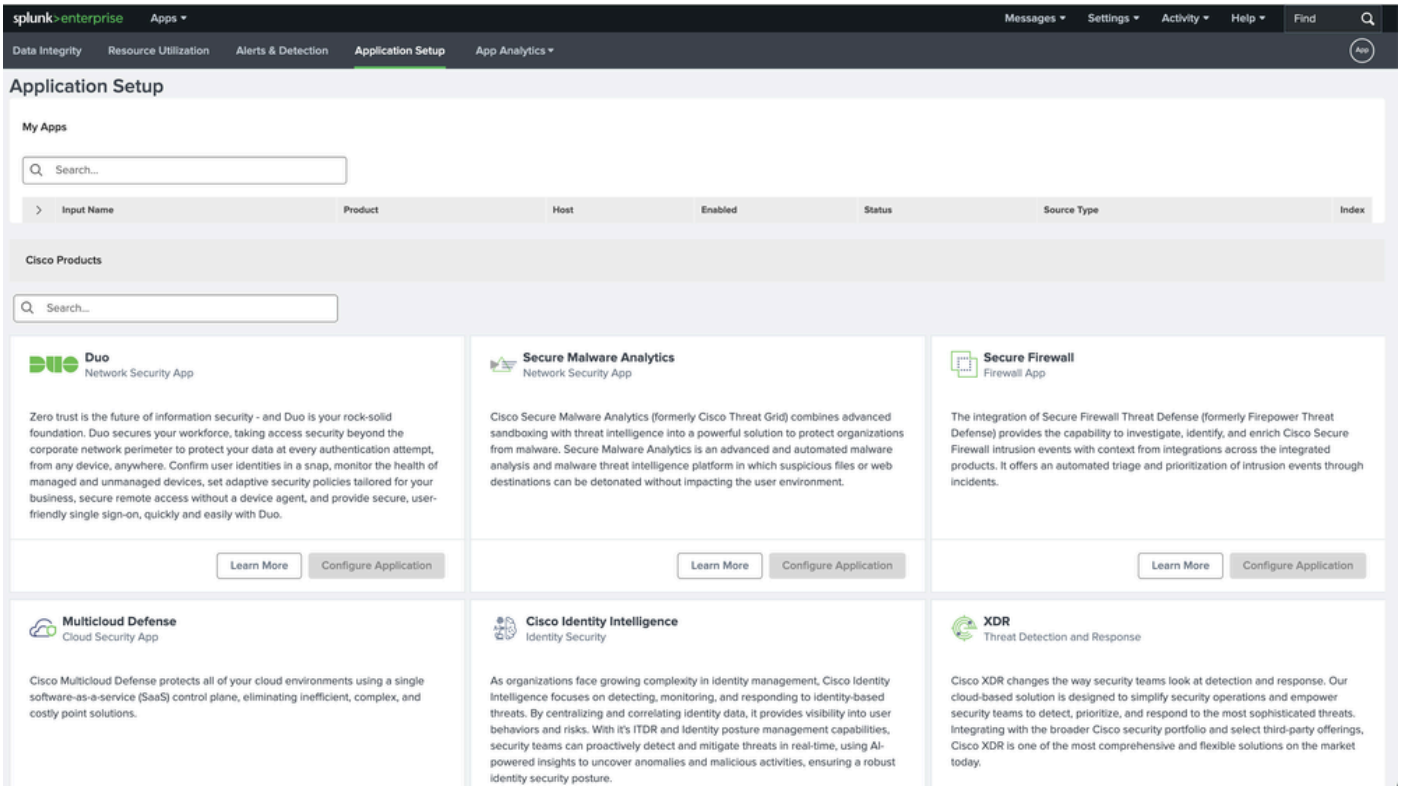


الخطوة 3: التحقق من تثبيت تطبيق سحابة أمان Cisco.

انقر فوق خيار Apps المنسدل، والآن يمكن مشاهدة التطبيق في القائمة بعد التثبيت الناجح:



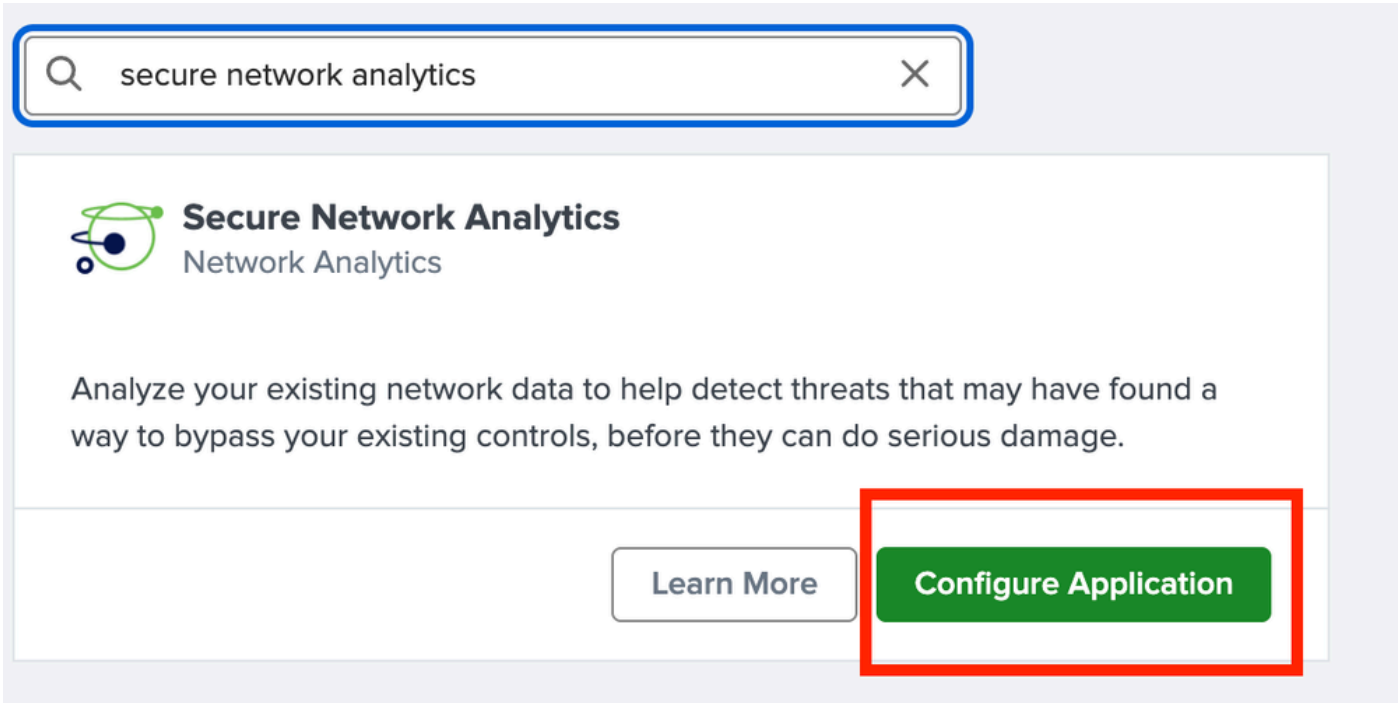
ii. حدد سحابة أمان Cisco بالنقر عليها. يمكنك الحصول على إعادة التوجيه إلى صفحة إعداد التطبيق حيث يمكن العثور على جميع منتجات أمان سحابة Cisco المتاحة.



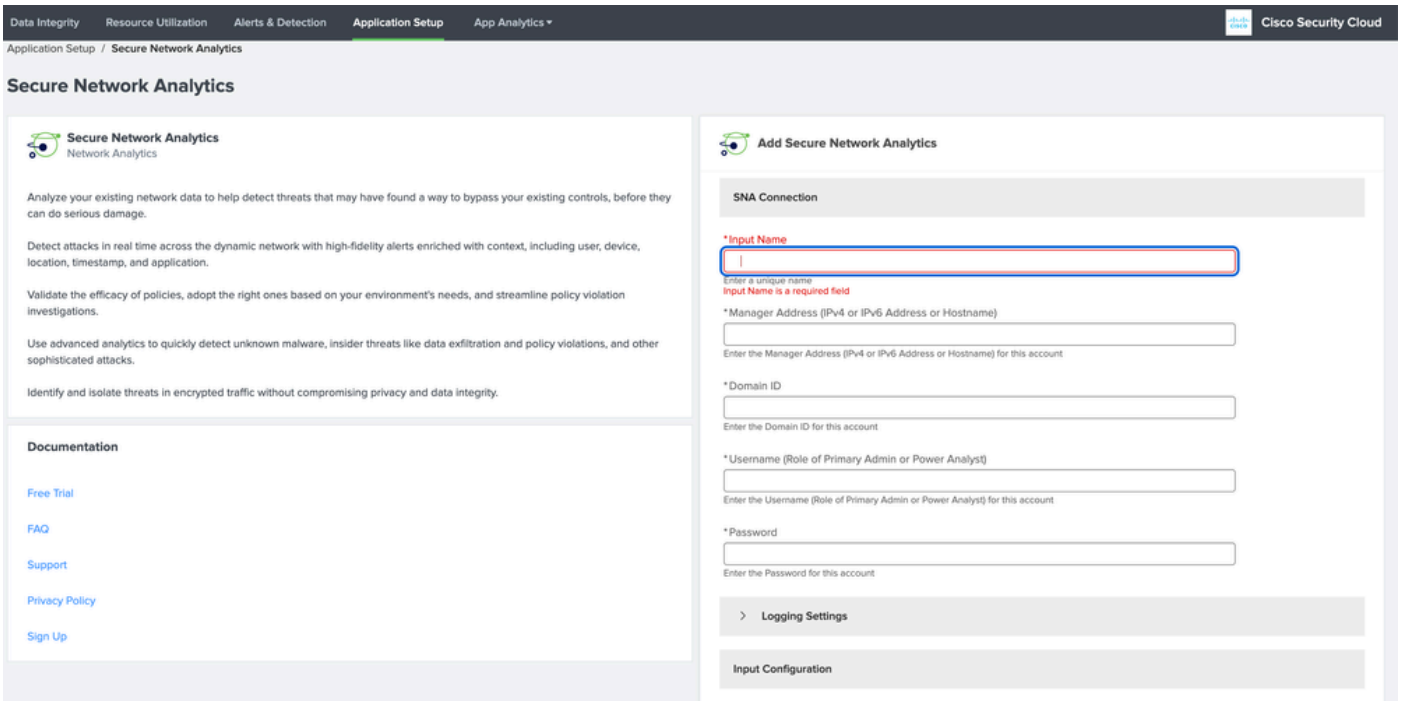
الخطوة 4: التكامل مع تحليلات الشبكة الآمنة (SNA).

الهدف من هذا المستند هو إبراز خطوات التثبيت الخاصة ب Splunk باستخدام تحليلات الشبكة الآمنة (SNA) التي تمت الإشارة إليها أكثر.

i. ابحث عن تحليلات الشبكة الآمنة وعندما تظهر، يرجى تحديد تكوين التطبيق:

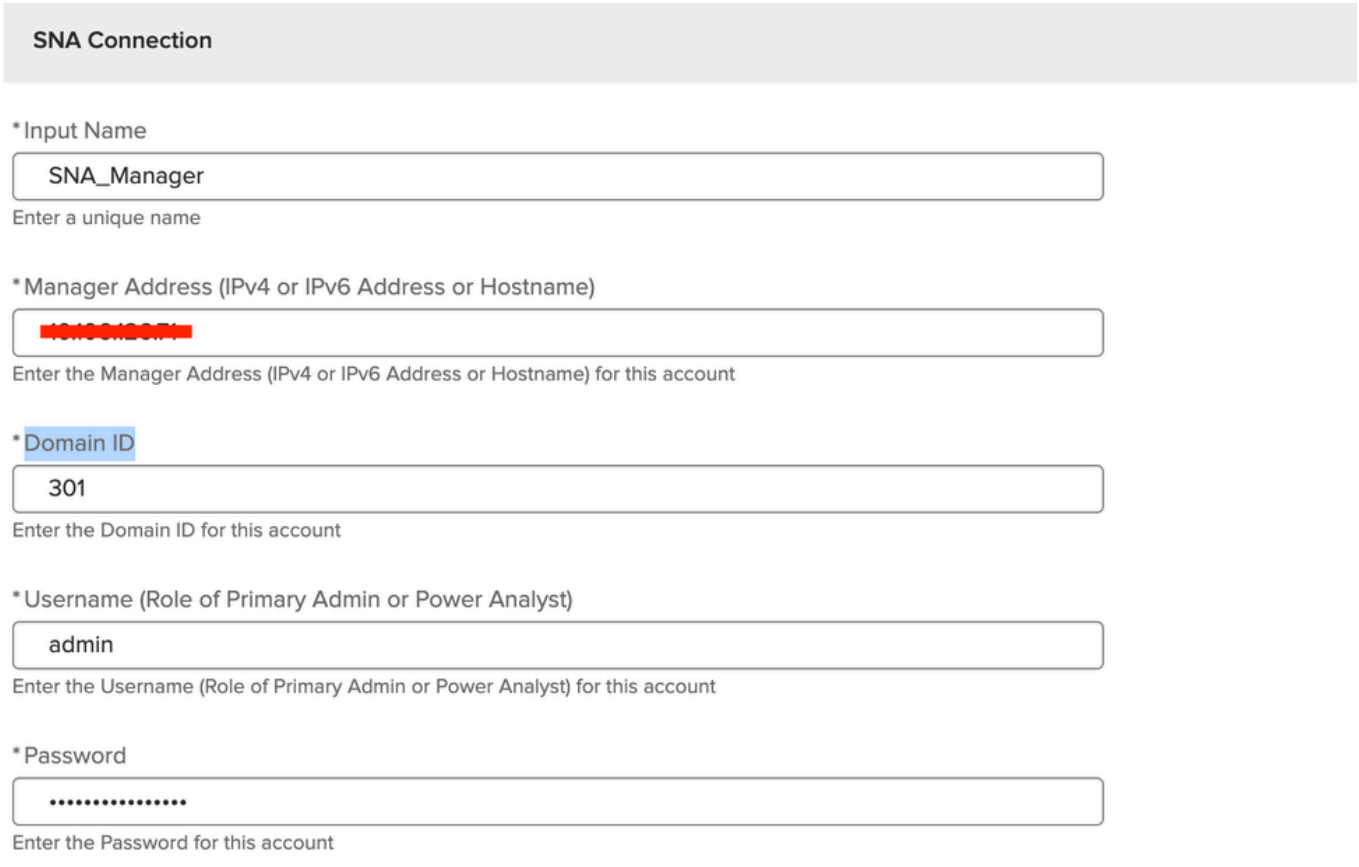


ثانياً. عند تحديد خيار التكوين، صفحة التكوين الخاصة بالتفاصيل لإضافة عمليات التشغيل.

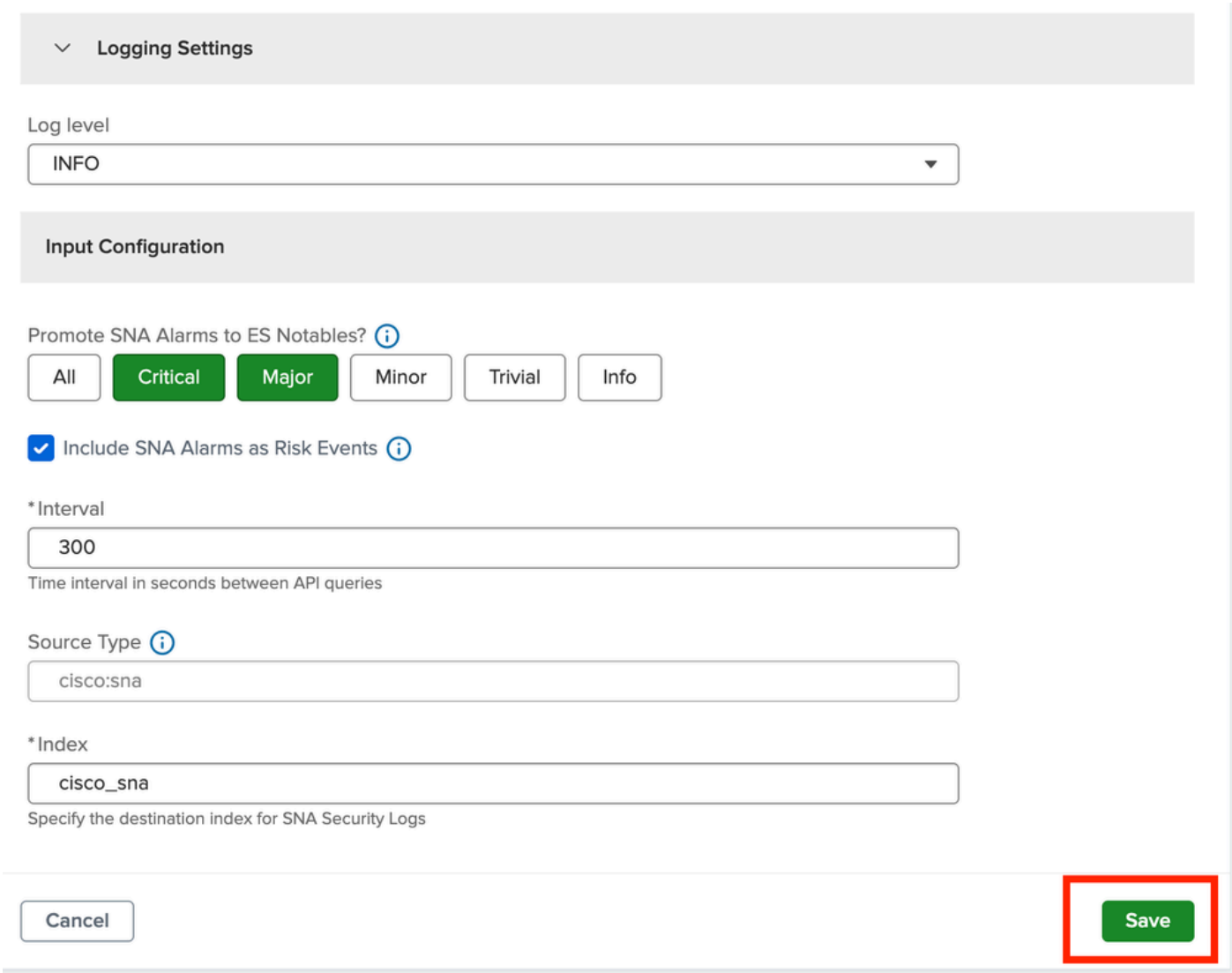


ثالثا. املأ جميع التفاصيل الإلزامية كما هو مذكور لتفاصيل اتصال SNA:

1. اسم الإدخال: أي اسم فريد ل SNA
2. عنوان المدير (عنوان IPv4 أو عنوان IPv6 أو اسم المضيف): إدارة IP الخاصة بمدير SNA الأساسي
3. معرف المجال: أدخل القيمة مقابل domain_id (على سبيل المثال، 301)
4. Username: اسم المستخدم الخاص بالمدير الأساسي (على سبيل المثال admin)
5. كلمة المرور: كلمة المرور الخاصة بمستخدم المدير الأساسي



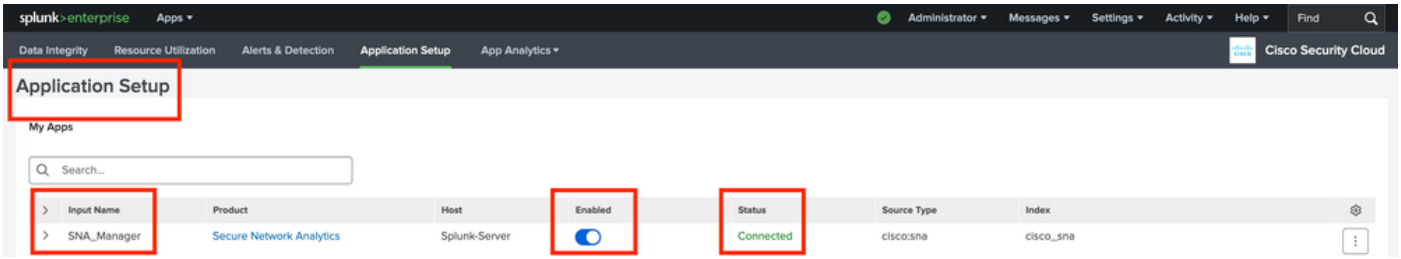
رابعا. أترك الإعدادات المتبقية عند قيمها الافتراضية أو قم بتعديلها حسب الحاجة، ثم انقر حفظ. تظهر رسالة ناجحة على الشاشة بعد الاكتمال.



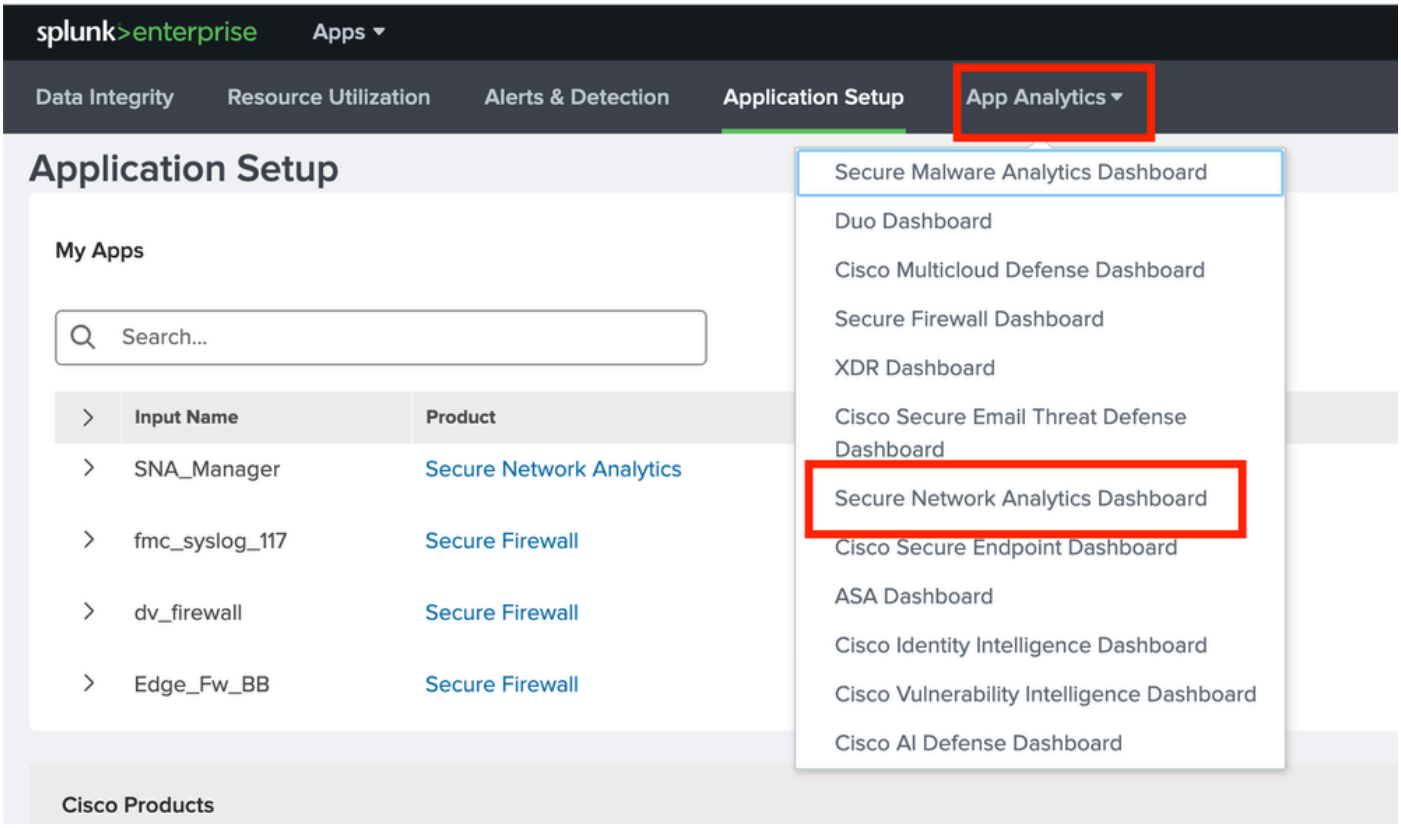
الخطوة 5: التأكد من التكامل.

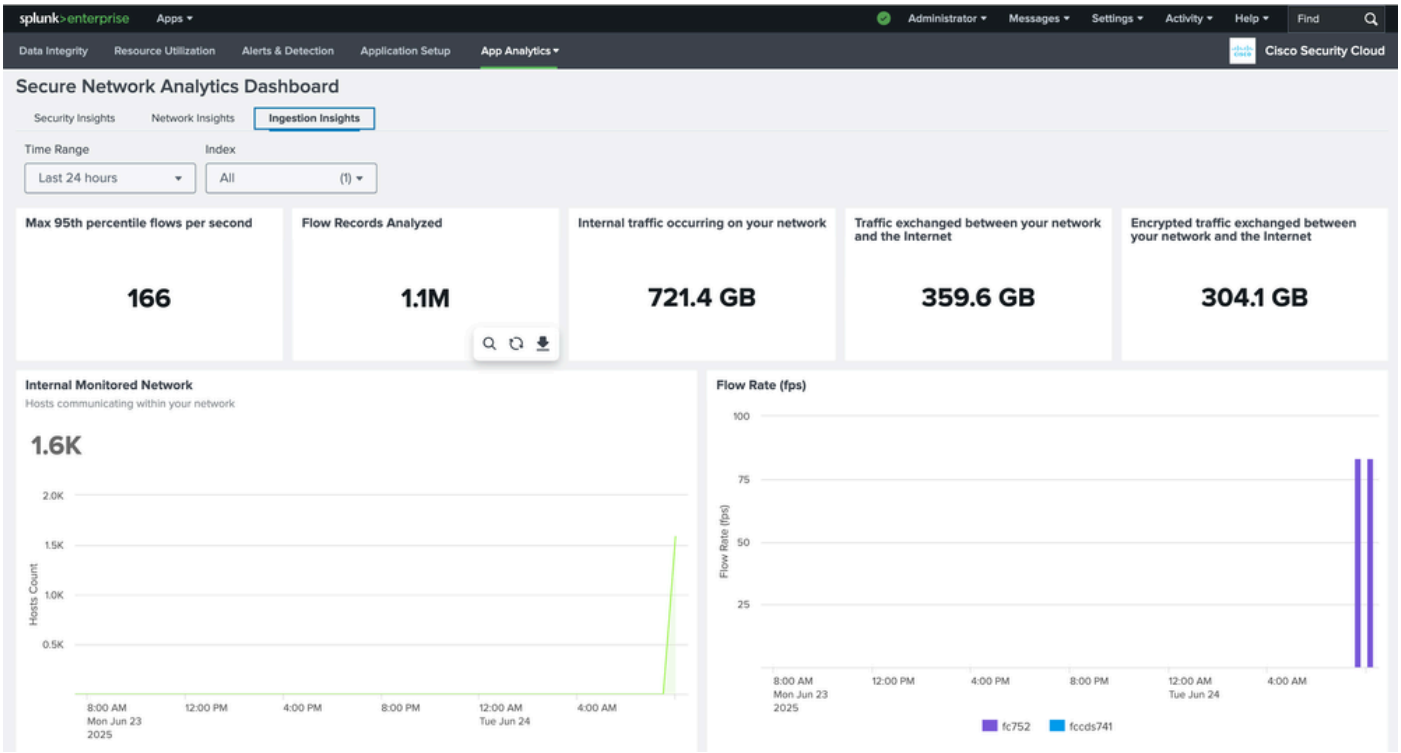
هذه خطوة مهمة حيث تحتاج إلى التحقق مما إذا كان التكامل الذي تم تنفيذه في الخطوة السابقة تم بنجاح أم لا.

ط. يجب أن تكون حالة الاتصال الخاصة بالإدخال متصلة في علامة التبويب إعداد التطبيق بشكل افتراضي على أنه ممكن للاسم الأيمن في حقل الإدخال.



II. حدد لوحة معلومات تحليلات الشبكة الآمنة من القائمة المنسدلة، وتبدأ الإحصائيات في النهاية في الانعكاس على لوحة المعلومات.





الأسئلة المتداولة

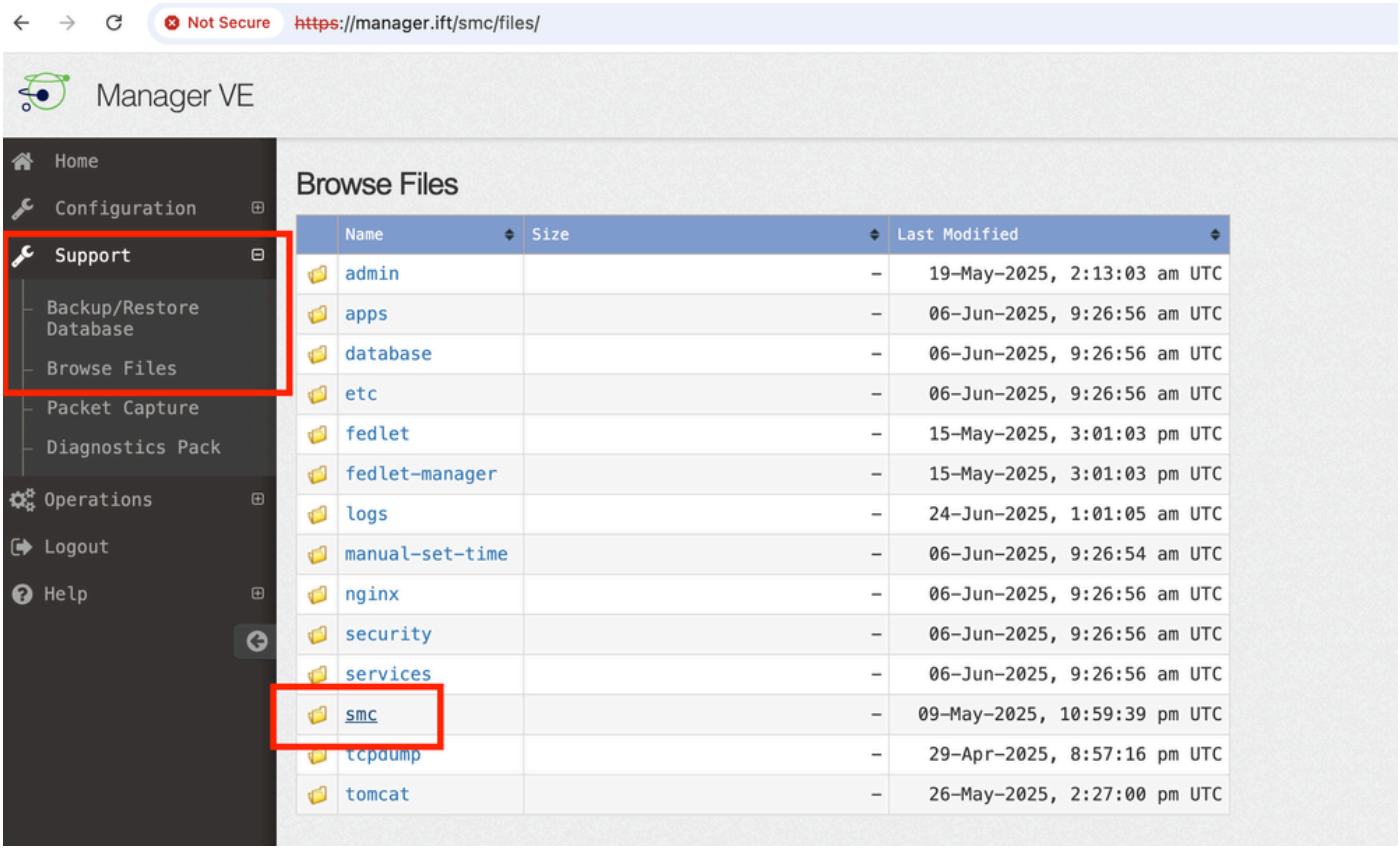
أين يمكن العثور على معرف المجال لإدارة SNA؟

الإجابة:

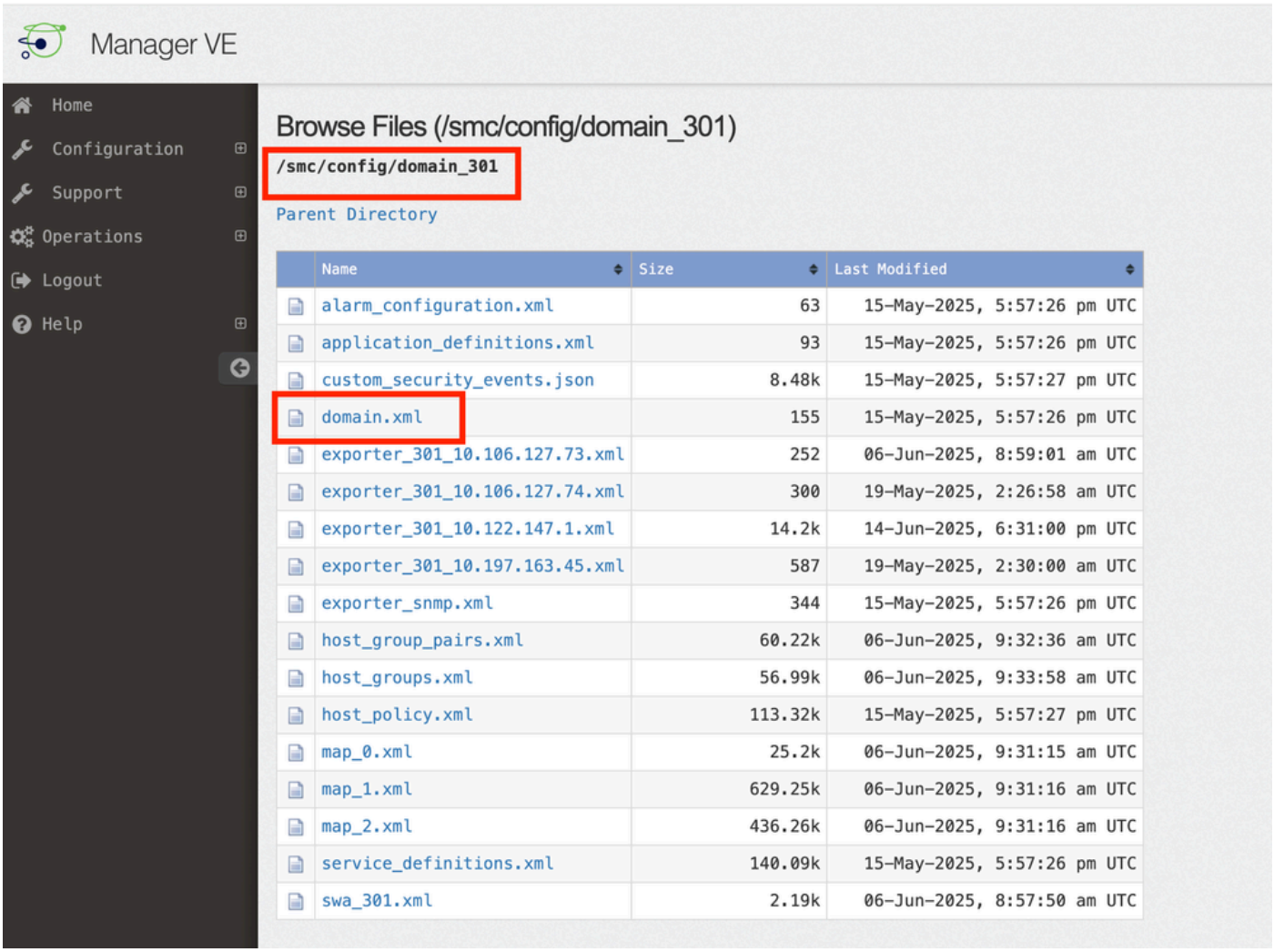
ط. قم بتسجيل الدخول إلى مدير SNA الأساسي وإعادة التوجيه إلى صفحة إدارة الأجهزة أو

عنوان URL لفهرس IP لدارة الوصول.

ثانيا. استعرض مجلد SMC ضمن قسم الدعم.



ثالثا. افتح ملف domain.xml الموفر في domain_xxx folder تحت المجلد config.


Manager VE
Home
Configuration
Support
Operations
Logout
Help
Browse Files (/smc/config/domain_301)
/smc/config/domain_301
Parent Directory
Name
Size
Last Modified
alarm_configuration.xml 63 15-May-2025, 5:57:26 pm UTC
application_definitions.xml 93 15-May-2025, 5:57:26 pm UTC
custom_security_events.json 8.48k 15-May-2025, 5:57:27 pm UTC
domain.xml 155 15-May-2025, 5:57:26 pm UTC
exporter_301_10.106.127.73.xml 252 06-Jun-2025, 8:59:01 am UTC
exporter_301_10.106.127.74.xml 300 19-May-2025, 2:26:58 am UTC
exporter_301_10.122.147.1.xml 14.2k 14-Jun-2025, 6:31:00 pm UTC
exporter_301_10.197.163.45.xml 587 19-May-2025, 2:30:00 am UTC
exporter_snmp.xml 344 15-May-2025, 5:57:26 pm UTC
host_group_pairs.xml 60.22k 06-Jun-2025, 9:32:36 am UTC
host_groups.xml 56.99k 06-Jun-2025, 9:33:58 am UTC
host_policy.xml 113.32k 15-May-2025, 5:57:27 pm UTC
map_0.xml 25.2k 06-Jun-2025, 9:31:15 am UTC
map_1.xml 629.25k 06-Jun-2025, 9:31:16 am UTC
map_2.xml 436.26k 06-Jun-2025, 9:31:16 am UTC
service_definitions.xml 140.09k 15-May-2025, 5:57:26 pm UTC
swa_301.xml 2.19k 06-Jun-2025, 8:57:50 am UTC

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).