تكوين تطبيق أمان السحابة ل IBM QRadar

المحتويات

المقدمة

يصف هذا المستند كيفية تكوين تطبيق أمان السحابة من Cisco باستخدام IBM QRadar لتحليل السجل.

نظرة عامة

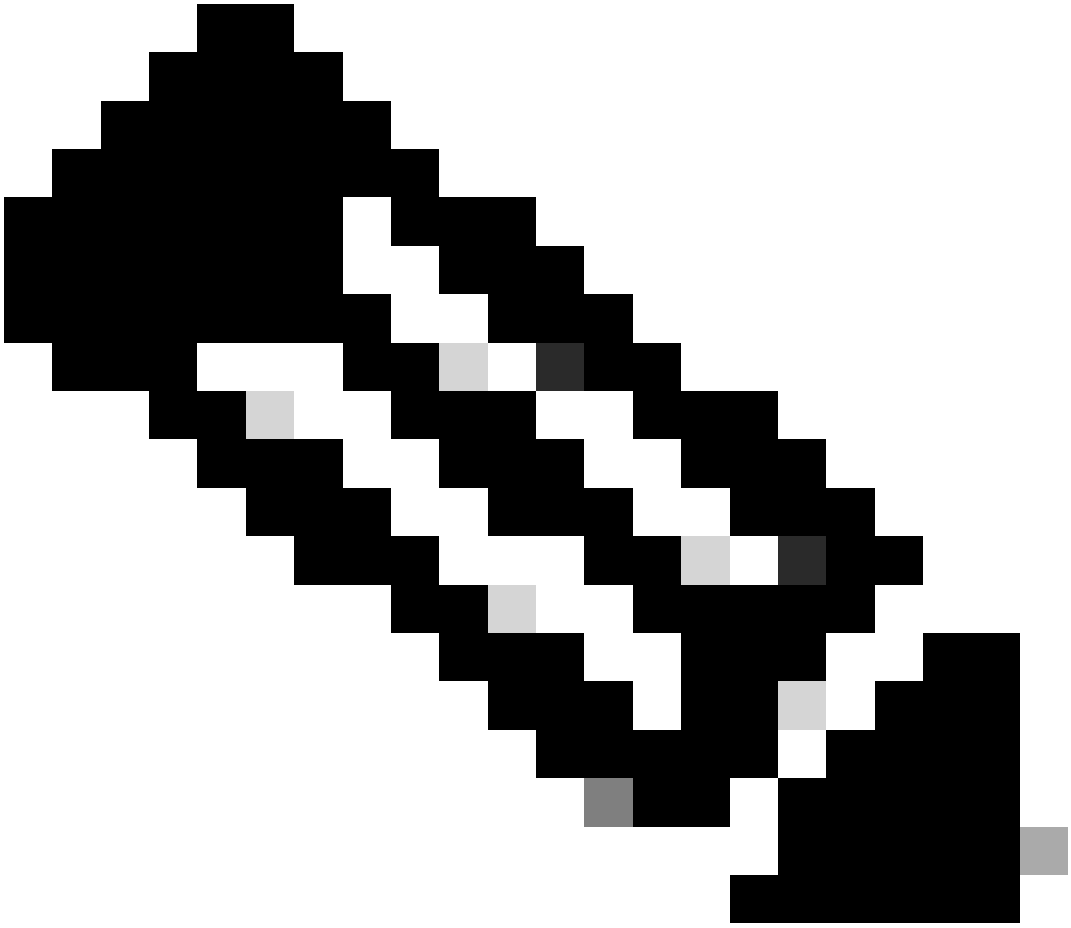
QRadar من IBM هو SIEM شائع لتحليل السجل. وهو يوفر واجهة قوية لتحليل مجموعات كبيرة من البيانات، مثل السجلات المقدمة من Cisco Umbrella لحركة مرور DNS في مؤسستك. يوفر تطبيق أمان السحابة ل IBM QRadar رؤية من منتجات أمان متعددة (التحقيق والإنذار و CloudLock) ويدمجها مع QRadar. كما تساعد هذه الأداة المستخدم على أتمتة الأمان واحتواء التهديدات بشكل أسرع ومباشر من خلال تطبيق QRadar.

عند إعداد تطبيق أمان السحابة من Cisco ل QRadar، فإنه يدمج جميع البيانات من منصة أمان السحابة من Cisco ويسمح لك بعرض البيانات في شكل رسومي في وحدة تحكم QRadar. من التطبيق، يستطيع المحللون:

- التحقيق في المجالات وعناوين IP وعناوين البريد الإلكتروني
- حظر المجالات وإلغاء حظرها (الإنذار)
- عرض معلومات جميع حوادث الشبكة.

يوضح هذا المقال الطريقة الأساسية لإعداد QRadar وتشغيله حتى يتمكن من سحب السجلات من دلو S3 واستهلاكها.

المتطلبات



ملاحظة: يجب أن يأتي دعم QRadar من IBM، لأن Cisco غير قادرة على دعم الأجهزة أو البرامج التابعة لجهات خارجية مباشرة. في حالة أي مشكلات تتعلق بتوصيل لوحة معلومات Umbrella الخاصة بك بحزمة S3، يمكننا توفير الدعم. كما يمكن العثور على الكثير من المعلومات التي تم العثور عليها هنا على موقع IBM على الويب: https://www.ibm.com/support/knowledgecenter/SS42VS_DSM/c_dsm_guide_microsoft_Cisco_Umb

متطلبات Cisco Umbrella

يفترض هذا المستند أنه قد تم تكوين دلو Amazon AWS S3 في Umbrella (الإعدادات > إدارة السجل) وهو يظهر اللون الأخضر مع تحميل السجلات الحديثة.

للحصول على مزيد من المعلومات حول كيفية تكوين هذه الميزة، يمكنك القراءة هنا: إدارة سجلاتك.

متطلبات IBM Security QRadar SIEM

يلزم أن يكون للمستخدم حقوق إدارية في جهاز (أجهزة) QRadar والتكوين في Amazon S3

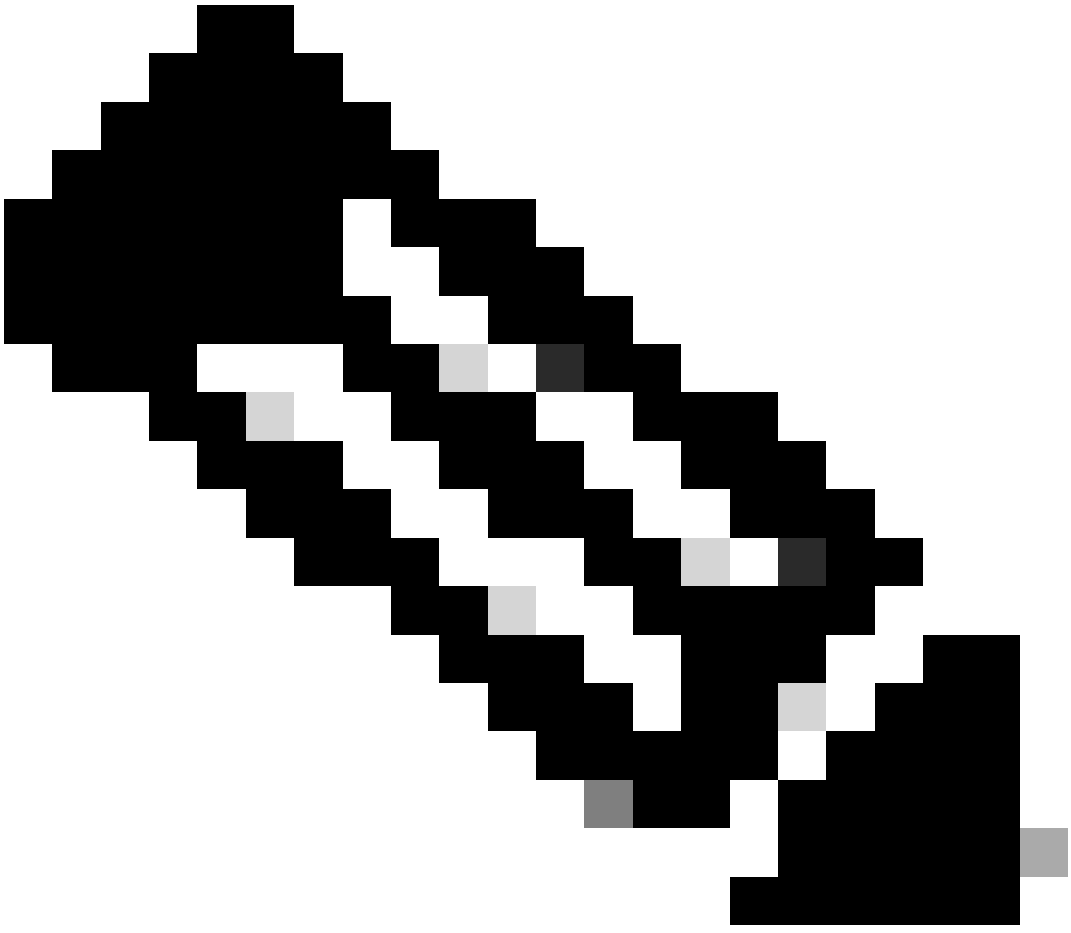
ولوحة معلومات المظلة، وتفترض هذه التعليمات أن مسؤول QRadar على دراية بإنشاء ملفات LSX (ملحق مصدر السجل).

الرجاء العلم بأن تطبيق أمان السحابة Cisco v1.0.3 يعمل فقط حتى IBM QRadar 7.2.8. يعمل الإصدار الجديد، v1.0.6، مع الإصدار الحالي QRadar من 7.4.2 والإصدارات الأحدث.

تثبيت تطبيق أمان السحابة ل IBM QRadar

1. تنزيل تطبيق أمان السحابة من Cisco وتثبيته ل IBM QRadar الموجود هنا: Cisco Cloud Security App v1.0.3 (ل IBM QRadar v7.2.8) أو Cisco Cloud Security App v1.0.6 (ل IBM QRadar v7.4.8).
2. بعد التثبيت، قم بنشر التغييرات في QRadar.

تكوين تطبيق أمان السحابة من Cisco: إضافة مصدر سجل



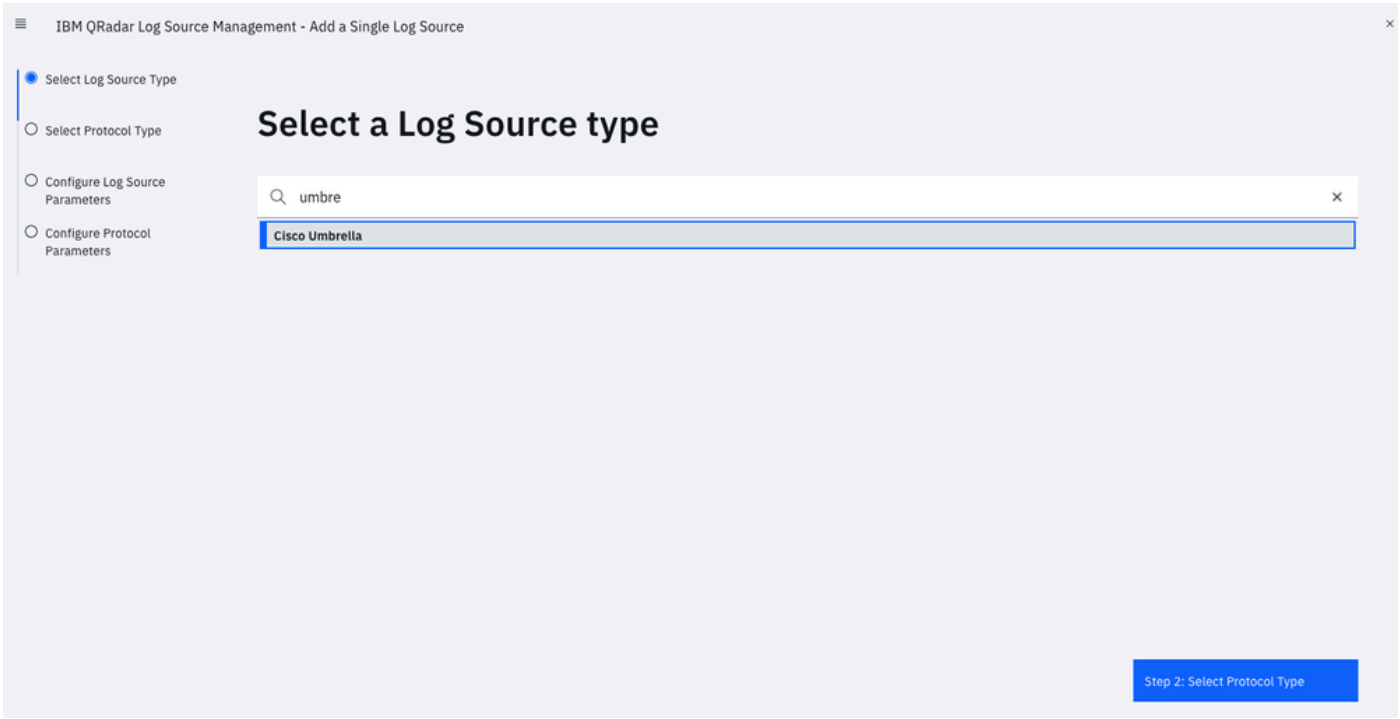
ملاحظة: أنت يستطيع رأيت آخر سجل في S3 مثل تدقيق وجدار حماية، غير أن هم ال يساند. قم فقط بإعداد الثلاثة المذكورة هنا. ينتج عن أي محاولات لتكوين هذه

السجلات الأخرى فشل.

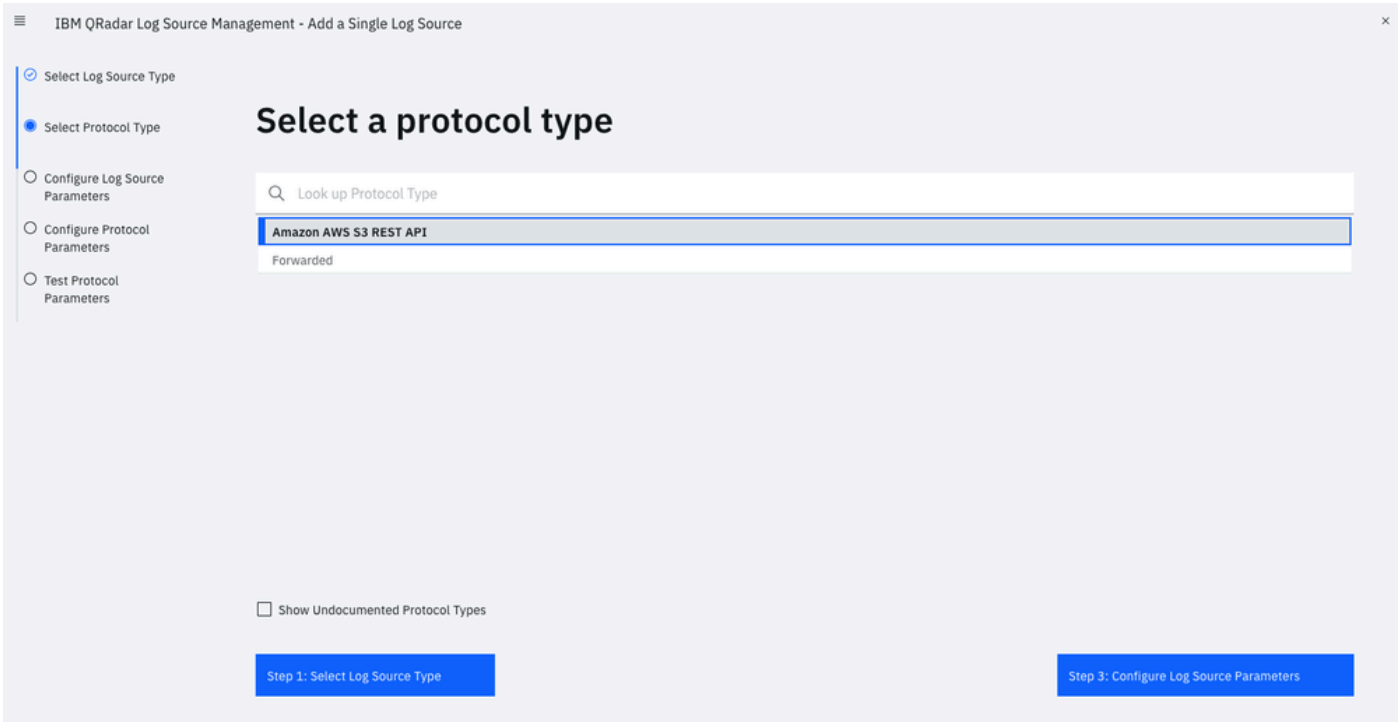
لإضافة مصدر سجل، انقر فوق علامة التبويب Admin في شريط التنقل QRadar، وانتقل لأسفل وانقر فوق إدارة مصدر سجل QRadar، ثم انقر فوق الزر +مصدر سجل جديد:

- سجل اسم المصدر (يجب أن تتطابق أسماء الإدخال تمامًا كما هو مدرج):
  - سجلات DNS من Cisco: cisco_umbrella_dns_log
  - سجلات Cisco Umbrella IP: cisco_umbrella_ip_log
  - سجلات وكيل Cisco Umbrella: cisco_umbrella_proxy_log
- تنسيق الحدث: Cisco Umbrella CSV
- نوع مصدر السجل: Cisco Umbrella
- تكوين البروتوكول: Amazon AWS S3 REST API
- نموذج الملف: .*؟\.csv\.gz
- سجل مصدر المادة: Cisco Umbrella_ext **
- الرجاء تحديد أي مجموعات تريد أن يكون مصدر السجل هذا عضوا فيها: cisco_umbrella_logsource_group

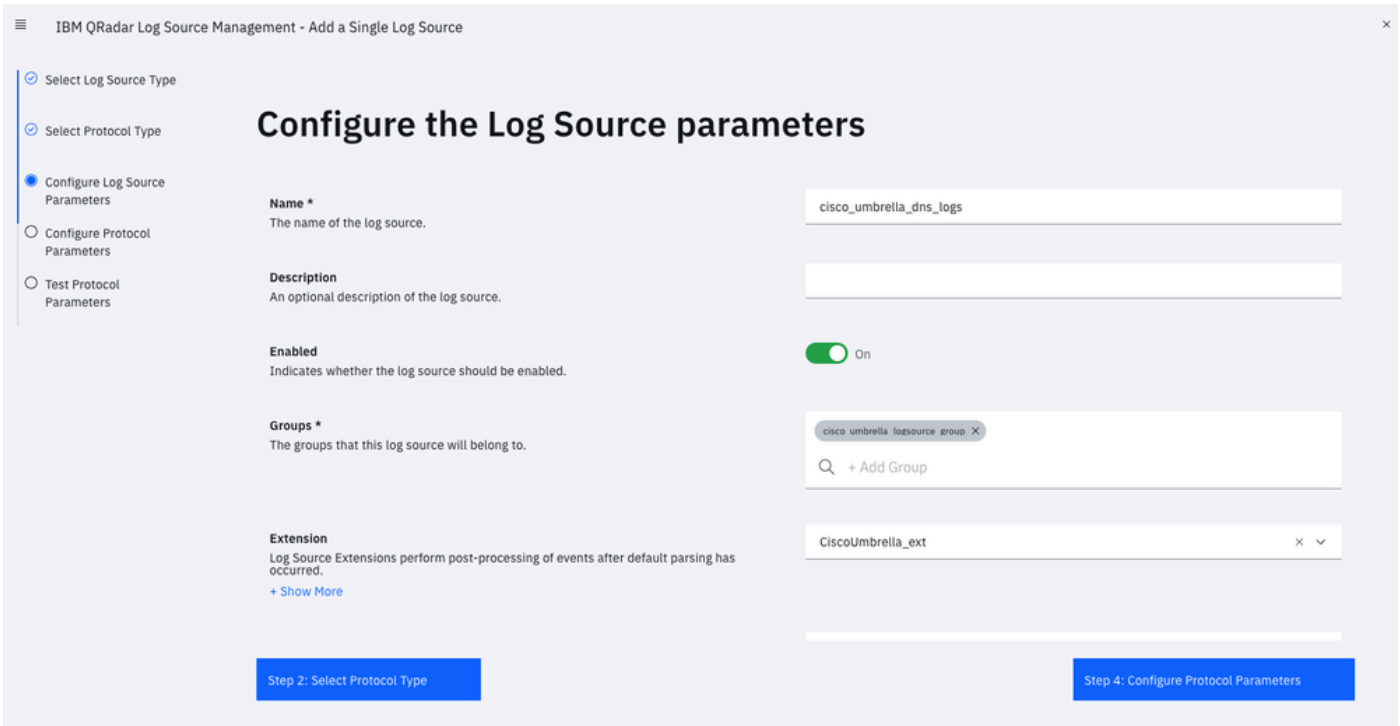
انتقل إلى معالج إضافة مصدر سجل واحد:



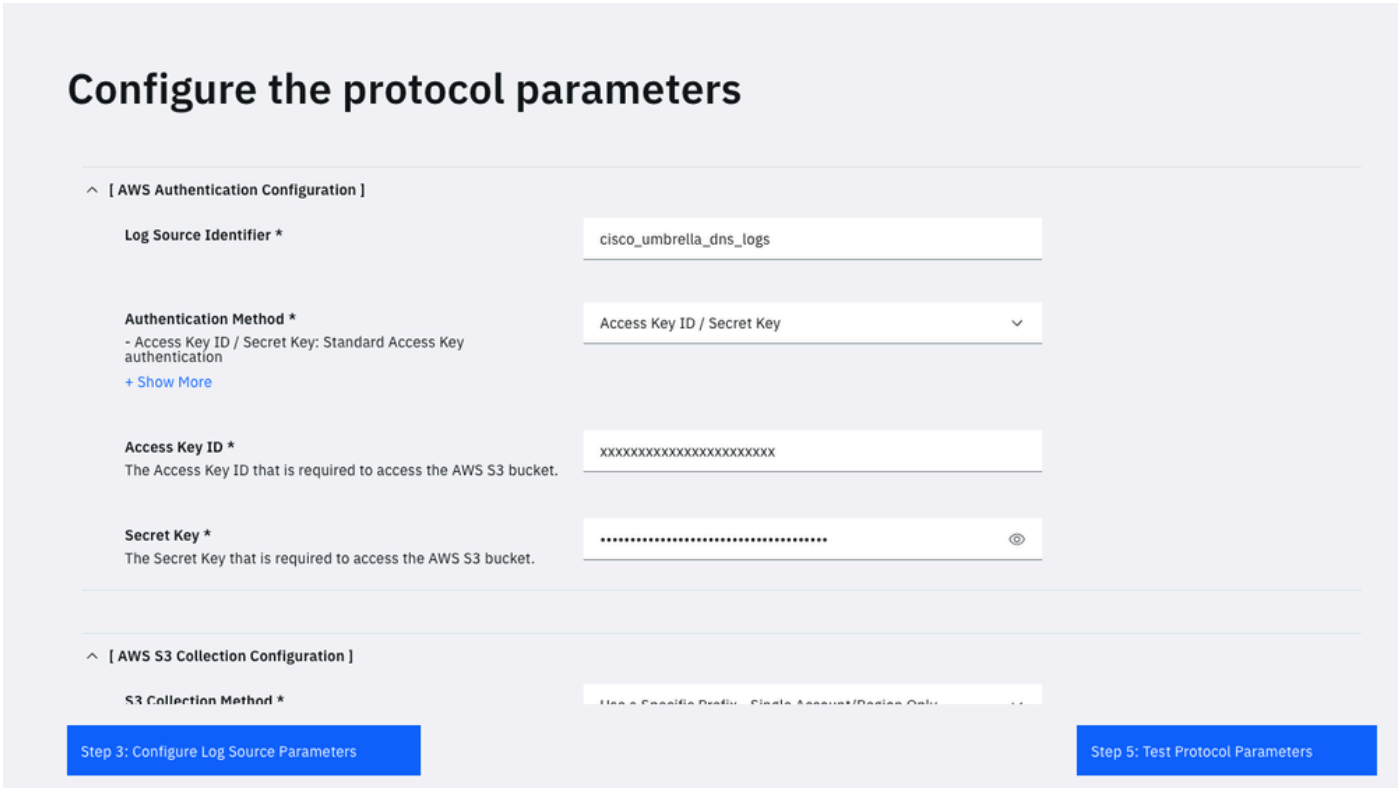
4404306773524



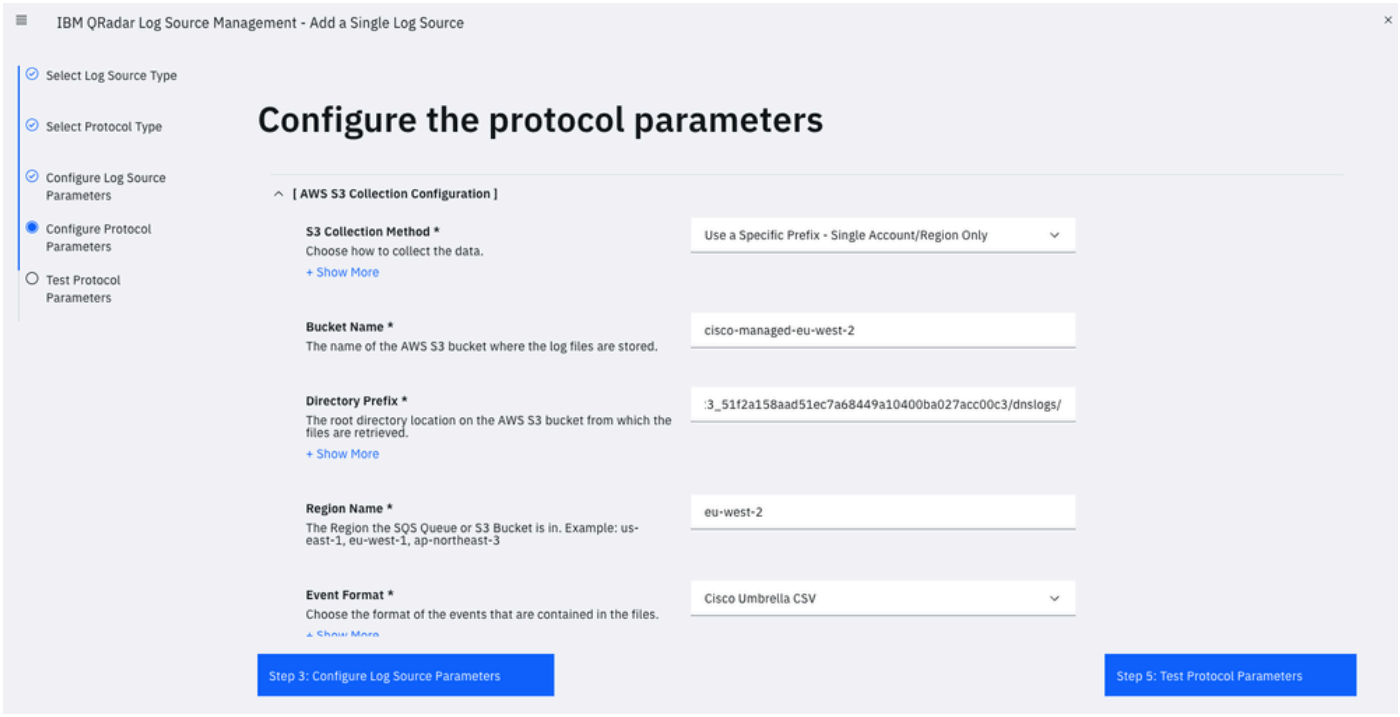
4404306773268



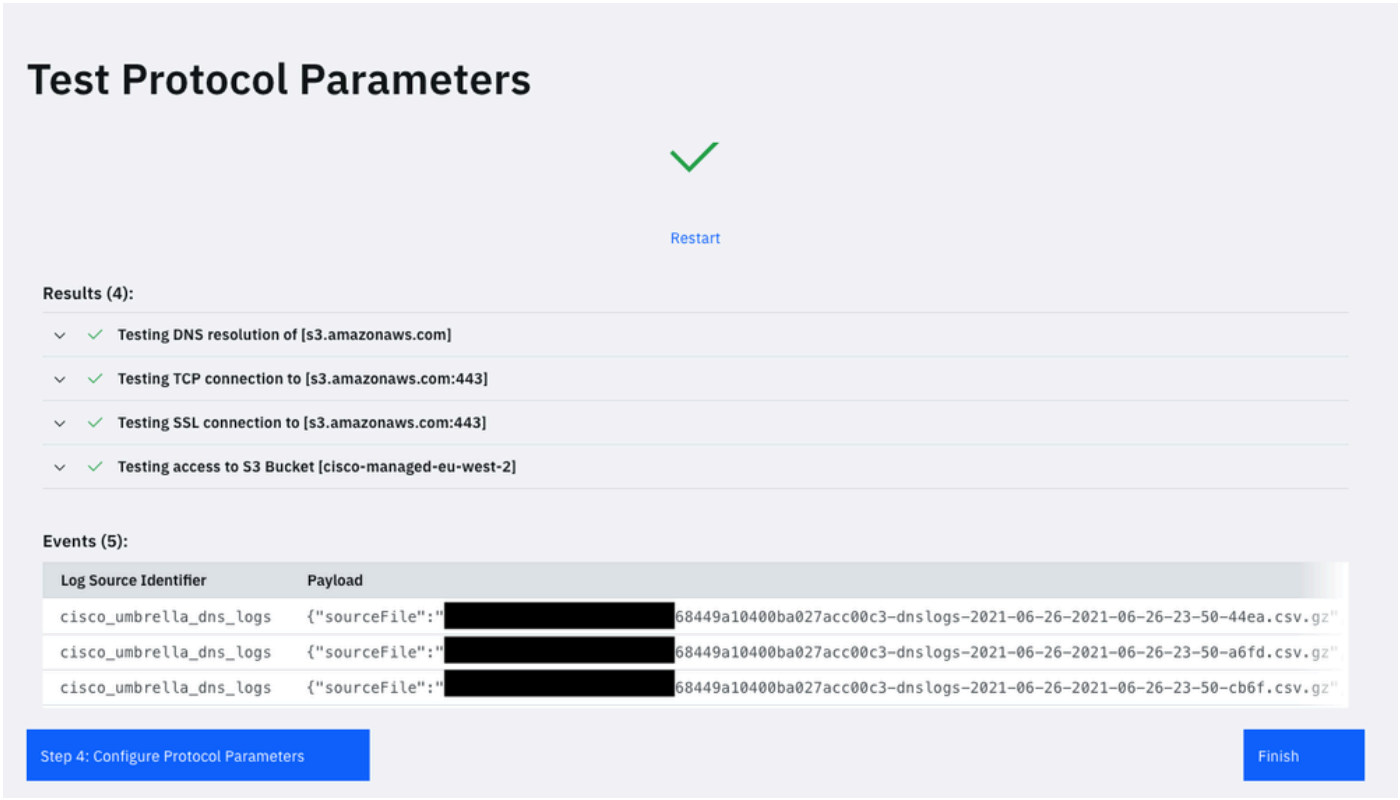
4404313505300



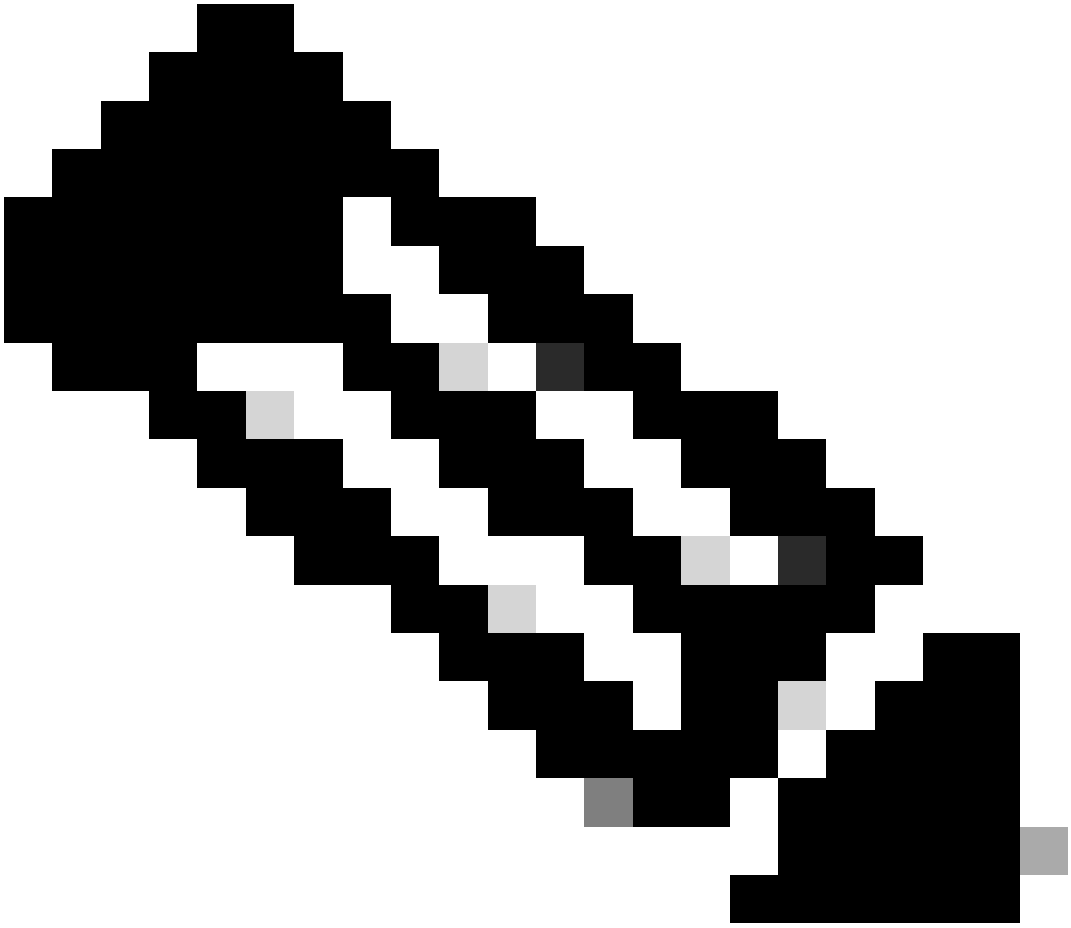
4404306774164



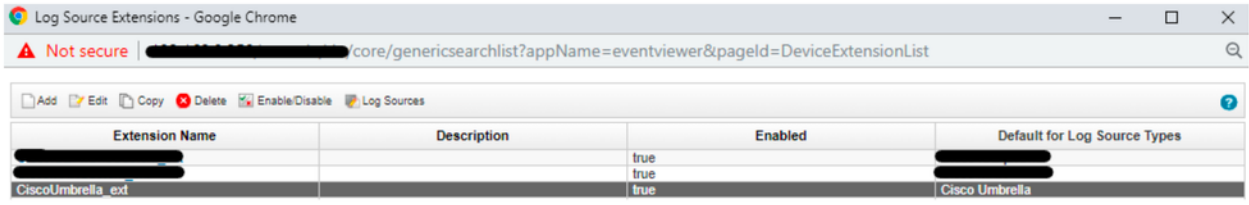
4404306897556



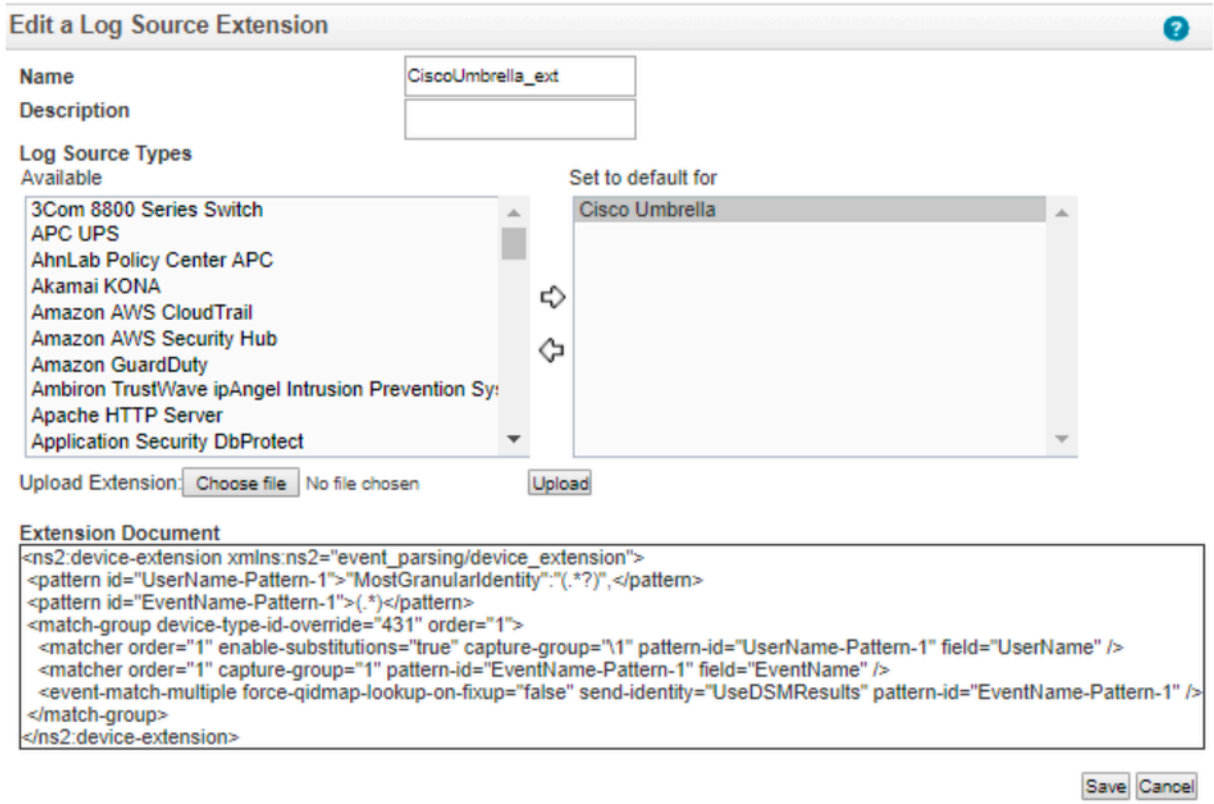
4404306881812



ملاحظة: إذا لم يتم تعيين "ملحق مصدر السجل" على "CiscoUmbrella_ext"، الرجاء إختيار اسم مصدر السجل من القائمة:



360071157752



360071326791

هنا مثال على ما يبدو على دلو مدار من Cisco:

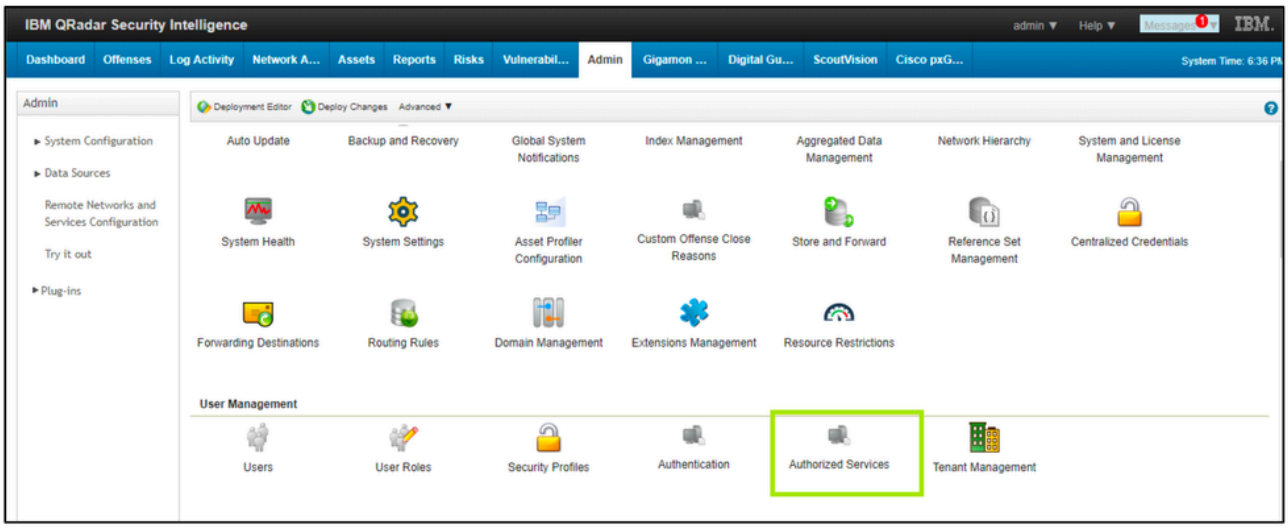
```
Bucket name: cisco-managed-us-west-1
ACCESS_KEY_ID: xxxxxxxxxxxxxx
SECRET_ACCESS_KEY: xxxxxxxxxxxxxx
Region: us-west-1
Your Directory Prefix is the key part of this. This is the customers folder,
followed by the appropriate log folder.
For example: xxxxxxx_cfa37bd906xxxxxx3aff94e205db7bxxxxxxx/dnslogs
```

انتقل مرة أخرى إلى إعدادات تطبيق أمان السحابة من Cisco وقم بتعيين معدل تحديث اللوحة بالساعات إلى قيمة أدنى مقدارها "1" لعرض البيانات في الرسومات البيانية.

إنشاء رمز المصادقة المميز

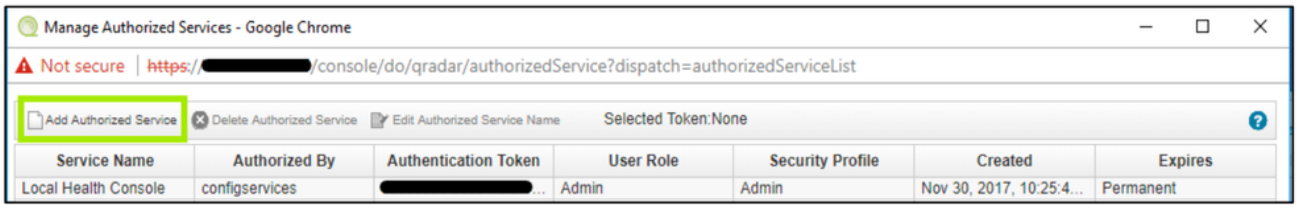
يحتاج المسؤول إلى إنشاء رمز مميز للخدمة لإضافته إلى تطبيق أمان Cisco الخاص بك. كأفضل ممارسة، تمت إعادة إنشاء رمز الخدمة المميز المعتمد كل 90 يوما:

1. تسجيل الدخول إلى QRadar > علامة التبويب "المسؤول" > الخدمات المعتمدة.



360071965571

2. إضافة الخدمات المعتمدة.

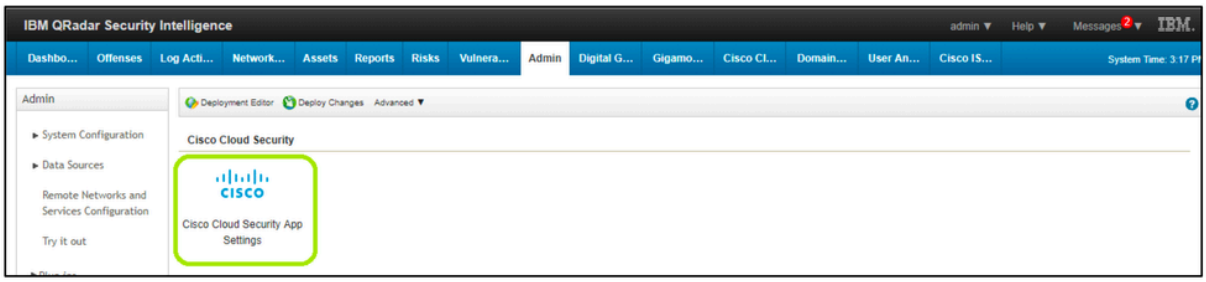


360071965551

3. أدخل التفاصيل وقم بإنشاء رمز مصادقة مميز.
4. بعد إنشاء الرمز المميز، انقر فوق "نشر التغييرات".

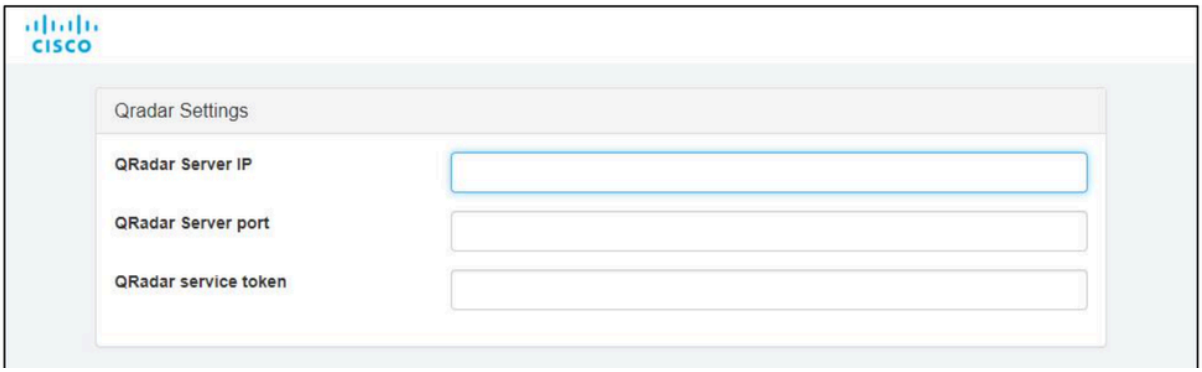
تكوين تطبيق أمان السحابة من Cisco

1. من علامة التبويب Admin في شريط التنقل QRadar، قم بالتمرير إلى أسفل وفتح إعدادات تطبيق أمان سحابة Cisco.



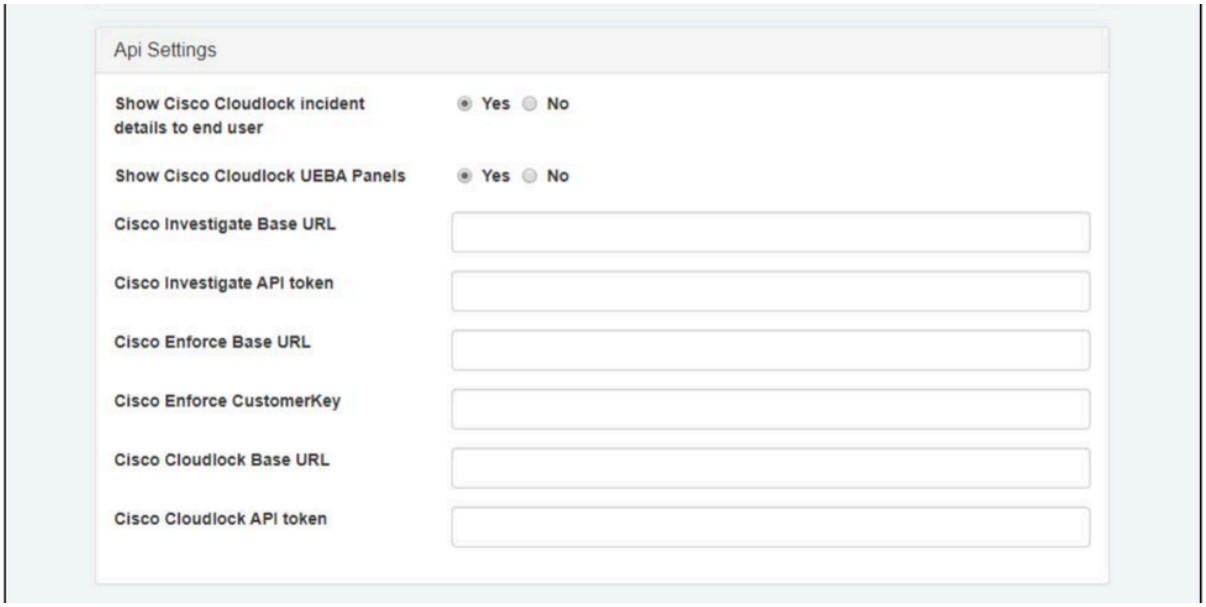
360071754732

2. أدخل رمز المصادقة المميز الذي تم إنشاؤه في الخطوة السابقة.



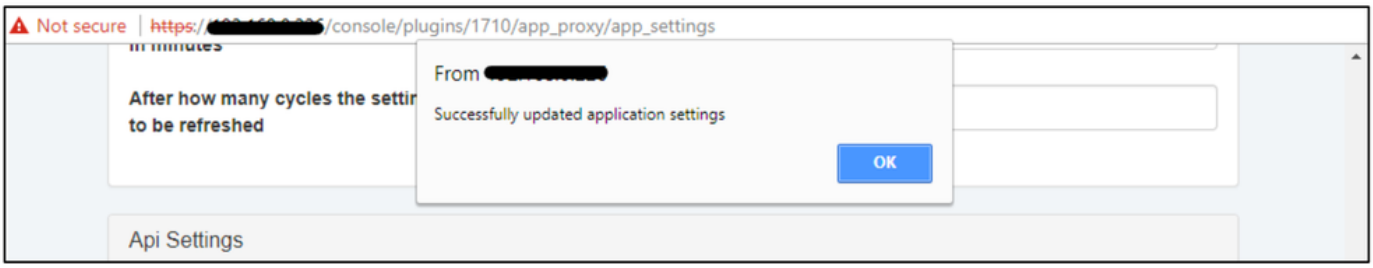
360072462992

3. حرر إعدادات API كما يلي:
   - تحقق من عنوان URL الأساسي من Cisco: https://investigate.api.umbrella.com/
   - تحقق Cisco من رمز API المميز: إنشاء من خلال لوحة معلومات Umbrella -> التحقيق -> مفاتيح API -> إنشاء رمز مميز جديد؛ لمزيد من المعلومات، راجع https://docs.umbrella.com/deployment-umbrella/docs/create-investigate-api-key
   - فرض عنوان URL الأساسي من Cisco: https://s-platform.api.opendns.com/1.0/
   - فرض مفتاح العميل من Cisco: إنشاء من خلال لوحة المعلومات Umbrella -> مكونات النهج -> عمليات التكامل -> إضافة؛ لمزيد من المعلومات، راجع https://docs.umbrella.com/umbrella-user-guide/docs/set-up-custom-integrations
   - عنوان URL لقاعدة CloudLock من Cisco: https://{YourCloudlockAPIServer}/API/V2 (على سبيل المثال، https://api-demo.cloudlock.com/api/v2/. الرجاء تأكيد عنوان URL الخاص بقاعدة Cloudlock المعروف باسم URL API Enterprise Cloudlock عن طريق إرسال بريد إلكتروني إلى support@cloudlock.com.)
   - الرمز المميز لواجهة برمجة التطبيقات Cisco Cloudlock: إنشاء عبر Cloudlock -> إنشاء؛ لمزيد من المعلومات، راجع https://developer.cisco.com/docs/cloud-security/cloudlock-api-getting-started/#authentication



360072703611

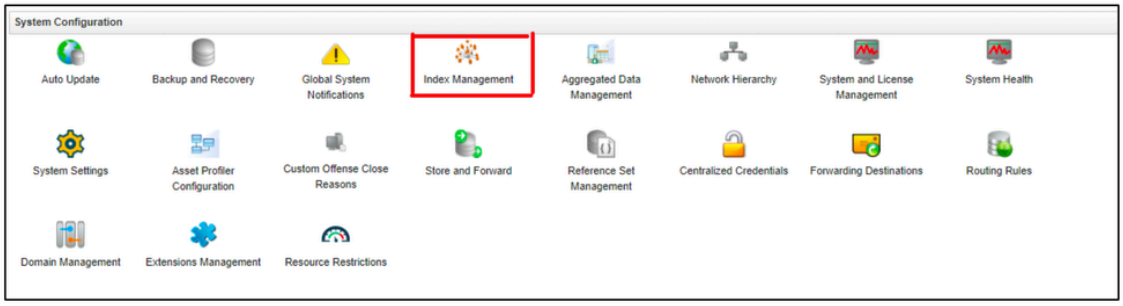
تشير القائمة المنبثقة إلى أنه تم تحديث إعدادات التطبيق بنجاح.



360071986151

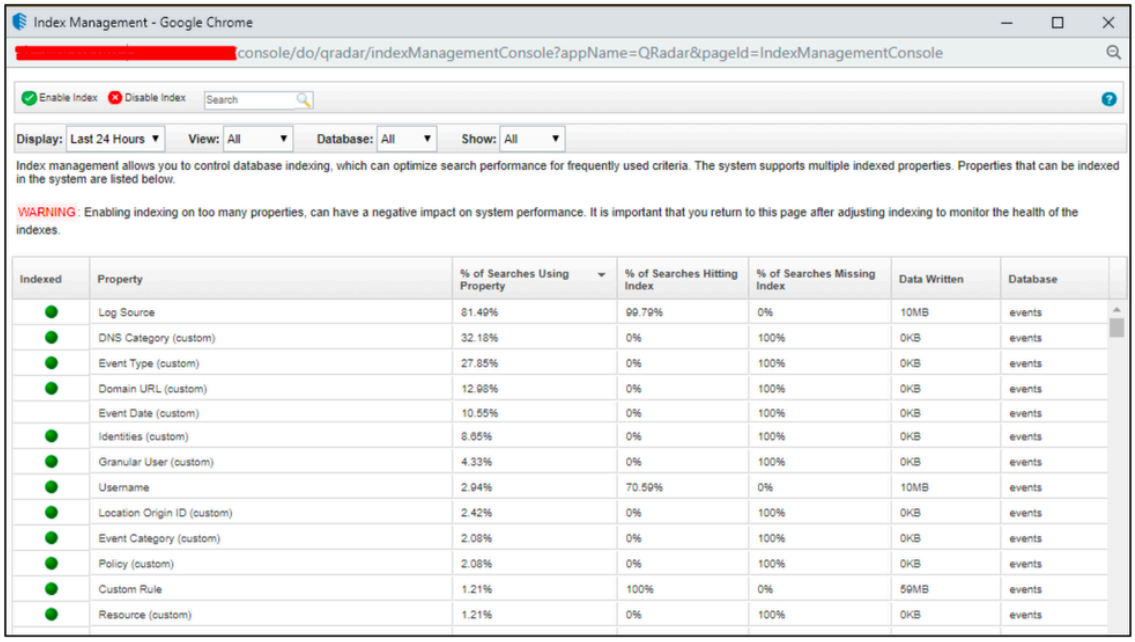
الفهرسة في QRadar

1. انتقل إلى علامة التبويب Admin، ثم انقر فوق إدارة الفهرس.



360071780112

2. فهرسة CEPs Packaged مع التطبيق.



360071988811

هذه هي وحدات CEP الموصى بها التي يجب فهرستها:

1. مصدر السجل
2. فئة DNS
3. نوع الحدث
4. عنوان URL للمجال
5. الهويات
6. مستخدم متعدد المستويات
7. Username
8. معرف أصل الموقع
9. فئة الحدث
10. السياسة
11. مورد

الآن أنت جاهز لاستخدام QRadar لبدء أنشطة مراقبة تفاصيل Cisco Umbrella، و Investigate، و CloudLock. يمكن العثور على مزيد من الإرشادات حول كيفية التنقل عبر QRadar هنا: التنقل عبر تطبيق أمان السحابة من Cisco.

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).