تكوين سير العمل التلقائي لإعلامات البريد الإلكتروني باستخدام XDR.

المحتويات

المقدمة

يوضح هذا المستند كيفية إنشاء سير عمل مؤتمت لإرسال إعلام عبر البريد الإلكتروني حول حادث جديد.

المتطلبات الأساسية

المتطلبات

لا توجد متطلبات خاصة لهذا المستند.

المكونات المستخدمة

لا يقتصر هذا المستند على إصدارات برامج ومكونات مادية معينة.

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.

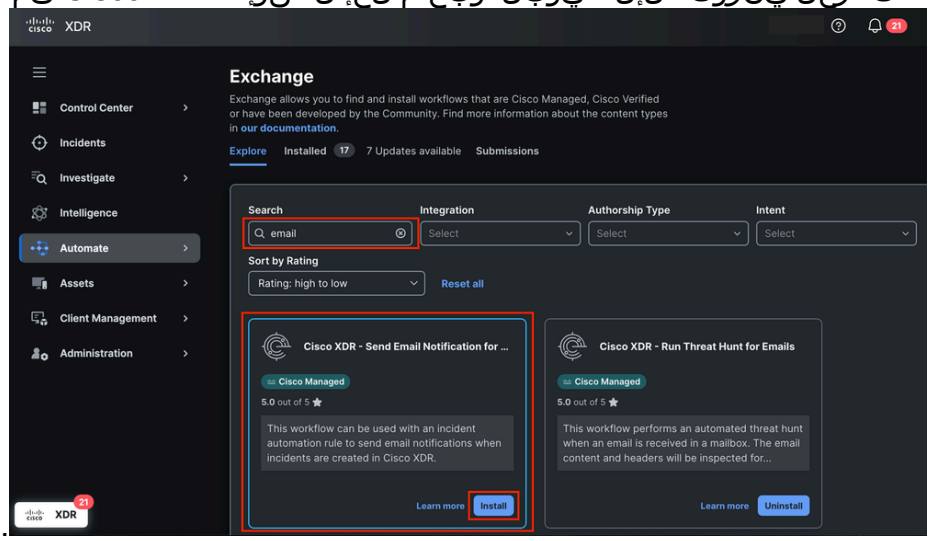
التكوين

يوضح هذا الدليل بالتفصيل الخطوات اللازمة لتكوين سير عمل وتنشيطه لإرسال إعلام بالبريد الإلكتروني تلقائيا عند وقوع حادث. وترد تفاصيل هذه الخطوات على النحو التالي.

تثبيت سير العمل من Cisco XDR Exchange

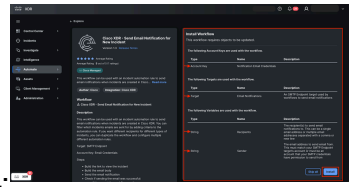
الخطوة 1. تثبيت سير عمل عزل نقاط النهاية

1. قم بتسجيل الدخول إلى Cisco XDR وانتقل إلى أتمتة > Exchange.
2. ابحث عن سير العمل المسمى Cisco XDR - إرسال إعلام عبر البريد الإلكتروني لحوادث جديدة وانقر فوق تثبيت.



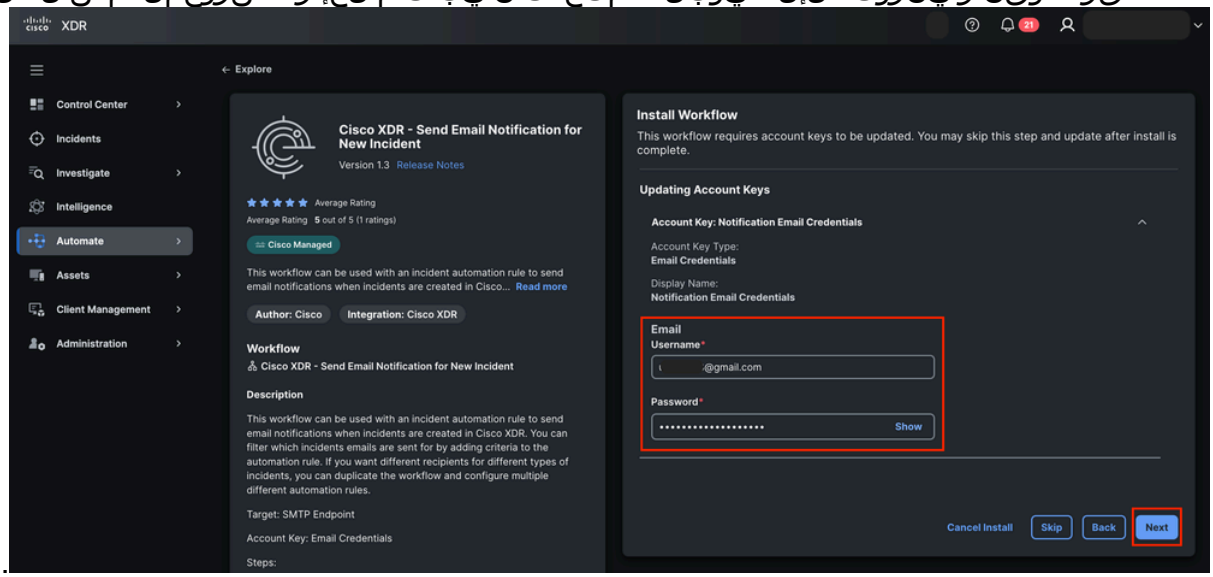
إرسال سير عمل إخطار البريد الإلكتروني من Exchange

3. تحقق من المعلومات اللازمة لتكوين سير العمل بشكل صحيح.



نظرة عامة على سير عمل إخطار الإرسال عبر البريد الإلكتروني

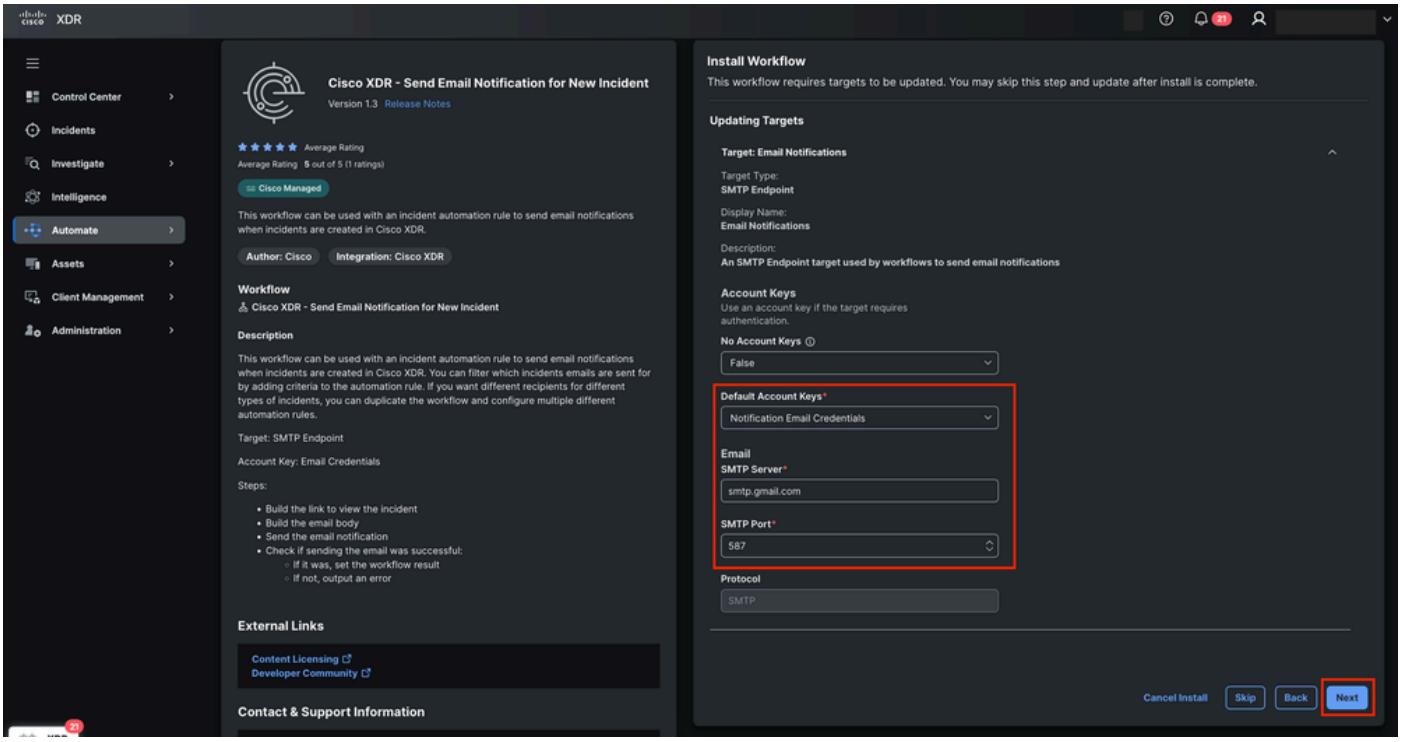
4. تعبئة مفاتيح الحسابباستخدام بيانات اعتماد البريد الإلكتروني لتعيين المرسل. الاسم المعروض هو إعلامات بيانات اعتماد البريد الإلكتروني وانقر فوق التالي.



مفاتيح الحساب لسير العمل

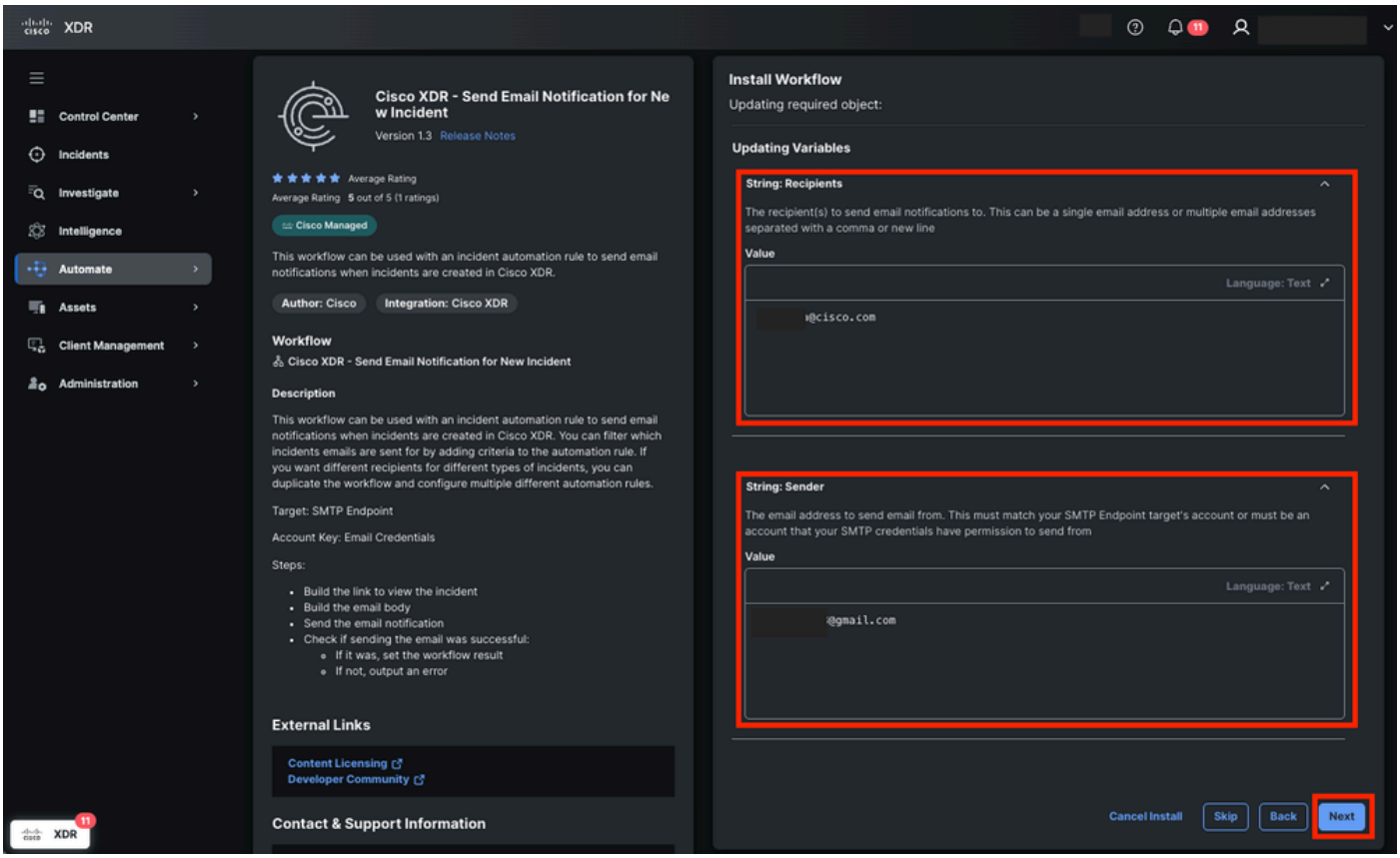
5. تكوين المعلومات الهدف باستخدام:

- مفاتيح الحساب: بيانات اعتماد الإعلام بالبريد الإلكتروني
- البريد الإلكتروني
  - خادم SMTP: smtp.gmail.com
  - منفذ SMTP: 587



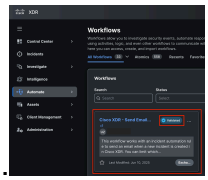
التكوين الهدف لسير العمل

1. انقر فوق Next (التالي).
2. تحديث المتغير ل:
   - متلقيي
   - المرسل



تعيين متغيرات لسير العمل

8. انقر فوق التالي.



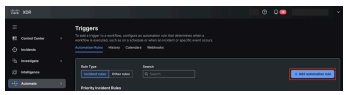
9. انتقل إلى أتمتة > عمليات سير العمل للتحقق من حالة التحقق من الصحة.

حالة التحقق من صحة سير العمل

إنشاء قاعدة أتمتة

الخطوة 2. تكوين قاعدة أتمتة

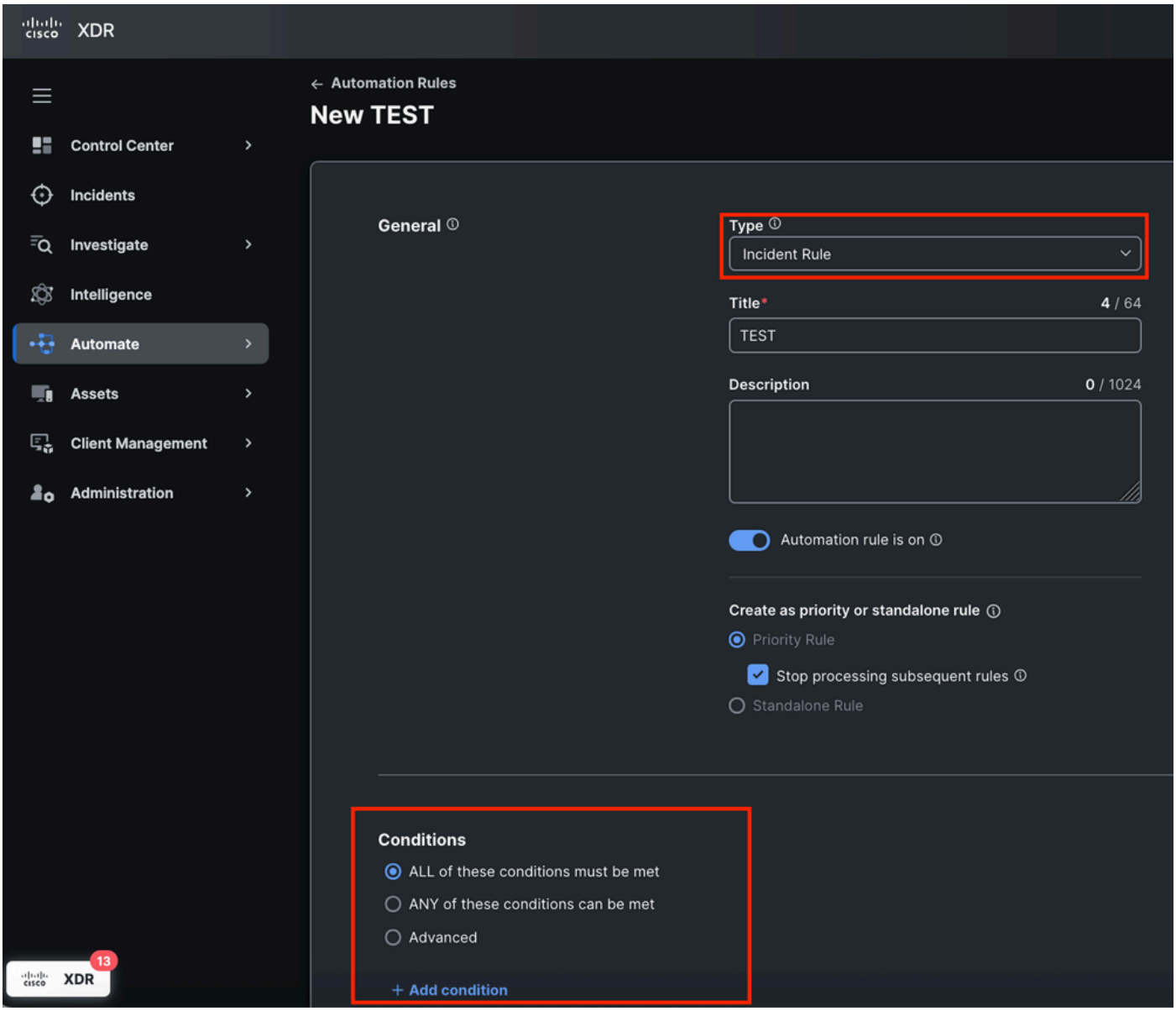
1. انتقل إلى قسم الأتمتة > المشغلات.



2. إنشاء قاعدة جديدة. انقر فوق إضافة قاعدة أتمتة وتعيين اسم.

إضافة قاعدة أتمتة من المشغلات

3. حدد نوع قاعدة الحادث وحدد شروط المشغل. يمكنك المتابعة دون الحاجة إلى إضافة حالة قاعدة، والتي تضمن أن أي حدث ينشط هذه القاعدة. قم بتخصيص الظروف إذا لزم الأمر.



نوع قاعدة الأتمتة وشروطها

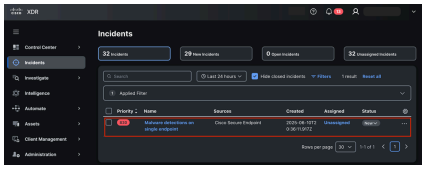
4. تطبيق قاعدة التشغيل التلقائي على Cisco XDR - إرسال إعلام عبر البريد الإلكتروني لسير عمل حادث جديد قمت بتثبيته مسبقا. تعيين متغيرات المستلمين والمرسل. 

تطبيق قاعدة الأتمتة على سير العمل وتعيين متغيرات

5. قم بحفظ القاعدة.

التحقق من وظيفة سير العمل

الخطوة 3. التحقق من تنفيذ سير العمل

1. قم بإنشاء حادث يتوافق مع شروط القاعدة أو انتظر حدوثه. 

تم اكتشاف حادث جديد في Cisco XDR

2. انقر فوق الحدث ثم اعرض تفاصيل الحدث.

Malware detections on single endpoint

Priority 830 Status New

Reported by
Cisco XDR Analytics

on 2025-06-10T20:36:11.917Z

Unassigned

MITRE

Priority score breakdown

830

83	10
Detection Risk	Asset Value at Risk

Sources

Cisco Secure Endpoint

View Incident Detail

يتم إنشاء اسم الحادث الأولي بناء على الكشف الأول؛ ومع ذلك، يمكن أن تتغير إذا حدثت اكتشافات إضافية أو أدت المعلومات الجديدة إلى إثراء الحادث.

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).