使用XDR配置電子郵件通知自動化工作流

目錄

簡介

本文檔介紹如何建立自動工作流程以傳送新事件的電子郵件通知。

必要條件

需求

本文件沒有特定需求。

採用元件

本文件所述內容不限於特定軟體和硬體版本。

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

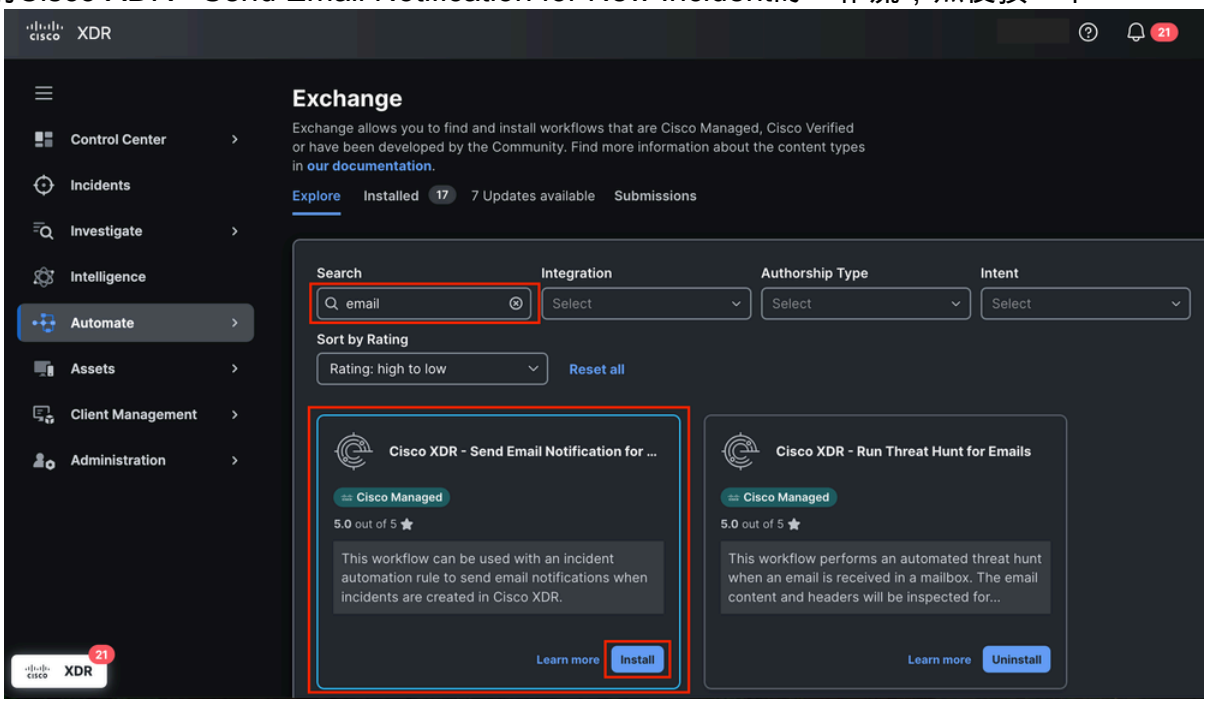
設定

本指南詳細說明了配置和啟用工作流程以在發生事故時自動傳送電子郵件通知所需的步驟。具體步驟詳述如下。

從Cisco XDR Exchange安裝工作流

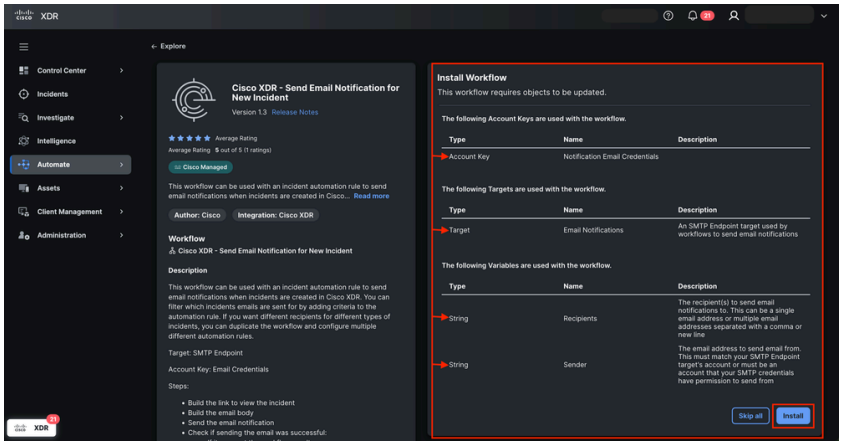
步驟1.安裝終端隔離工作流

1. 登入到Cisco XDR並導航到自動> Exchange。
2. 搜尋名為Cisco XDR - Send Email Notification for New Incident的工作流，然後按一下 Install。



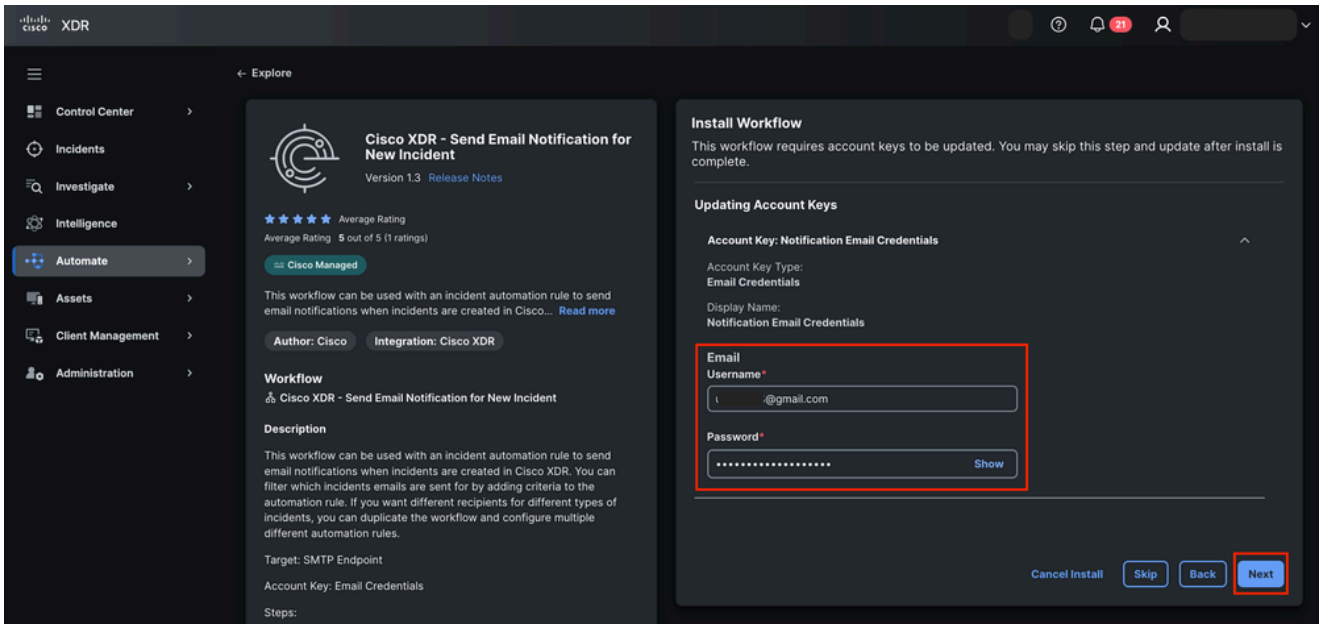
從Exchange傳送電子郵件通知工作流

3. 檢查正確配置工作流所需的資訊。



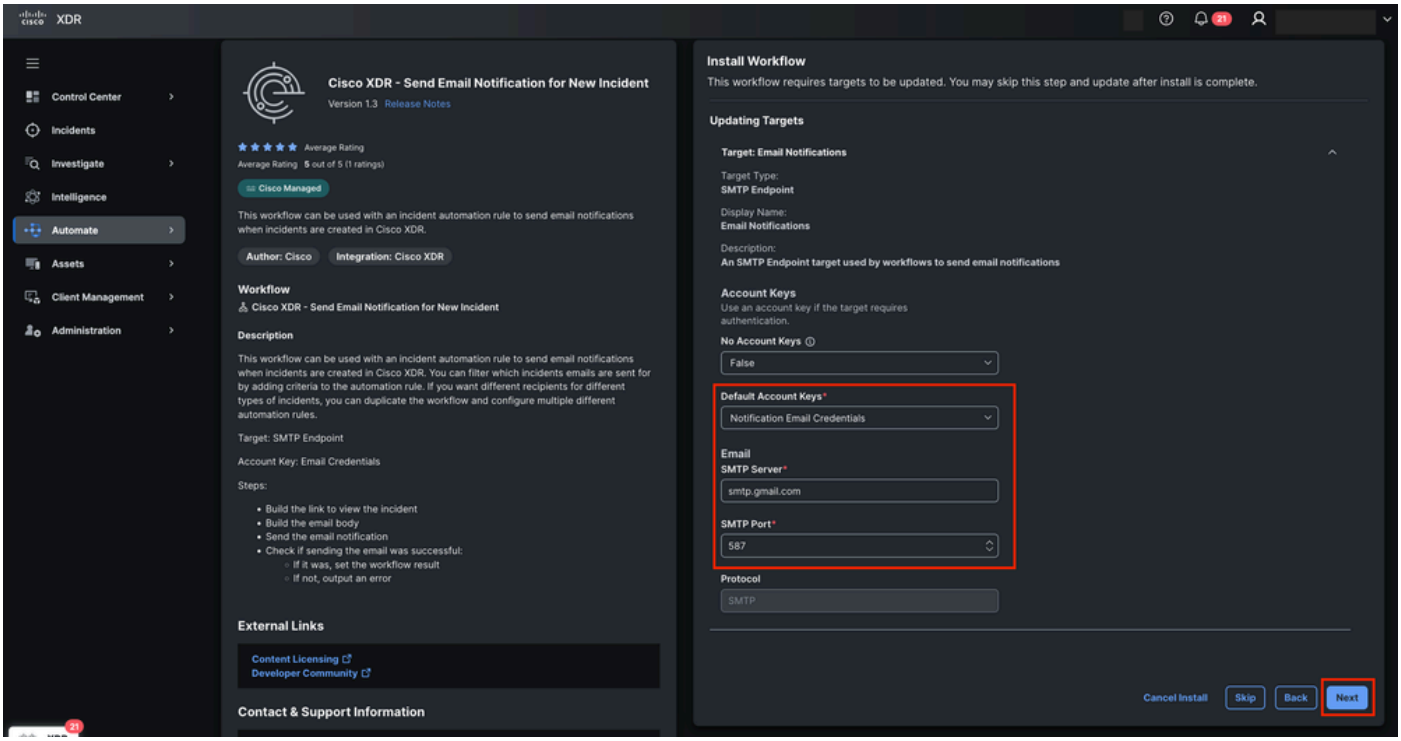
傳送電子郵件通知工作流概述

4. 填寫帳戶金鑰使用電子郵件憑據設定發件人。顯示的名稱是「通知電子郵件憑證」，然後按一下 下一頁.



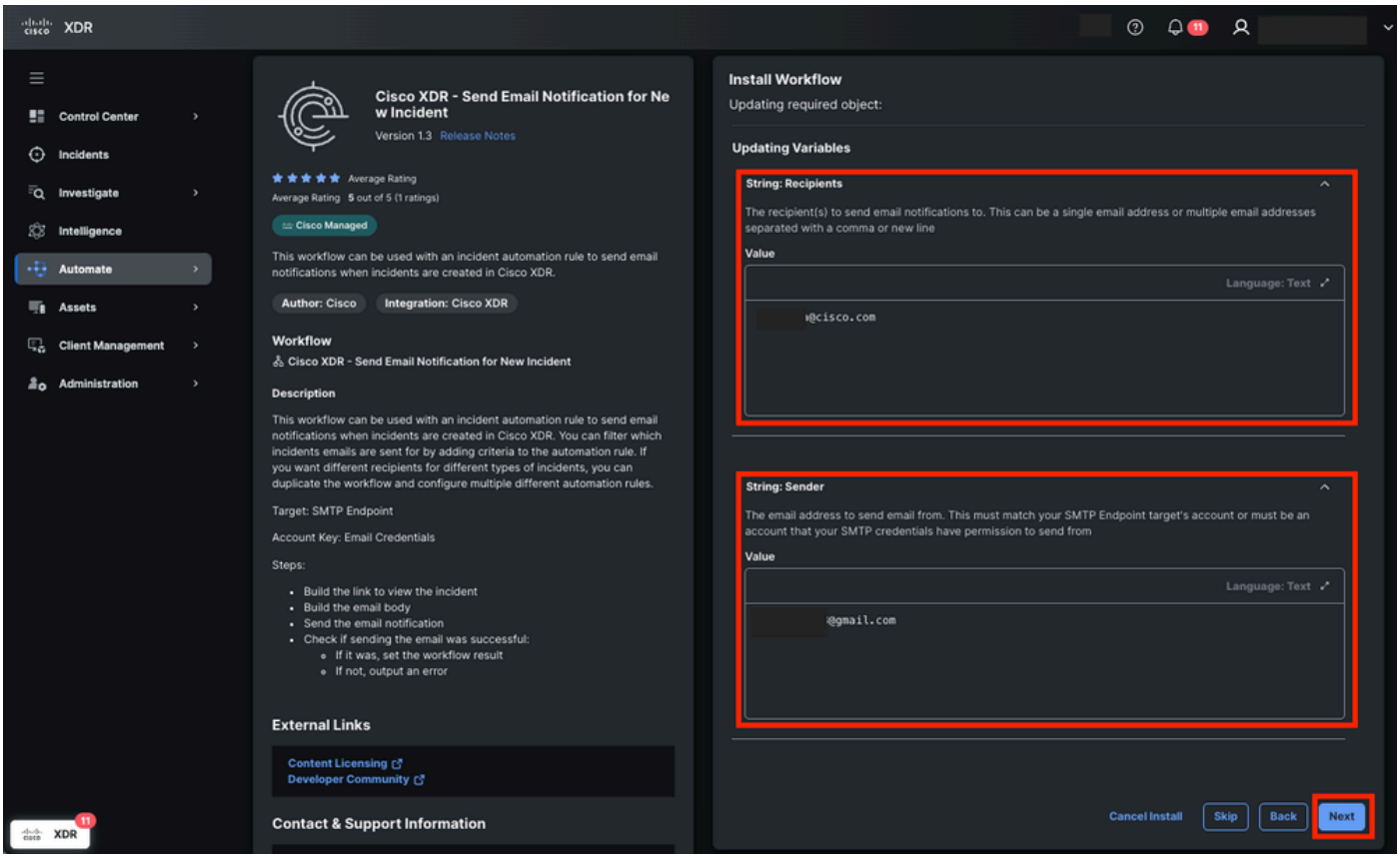
工作流的帳戶金鑰

5. 使用以下命令配置目標資訊：
    - 帳戶金鑰：通知電子郵件憑據
    - 電子郵件
        - SMTP伺服器：smtp.gmail.com
        - SMTP埠：587



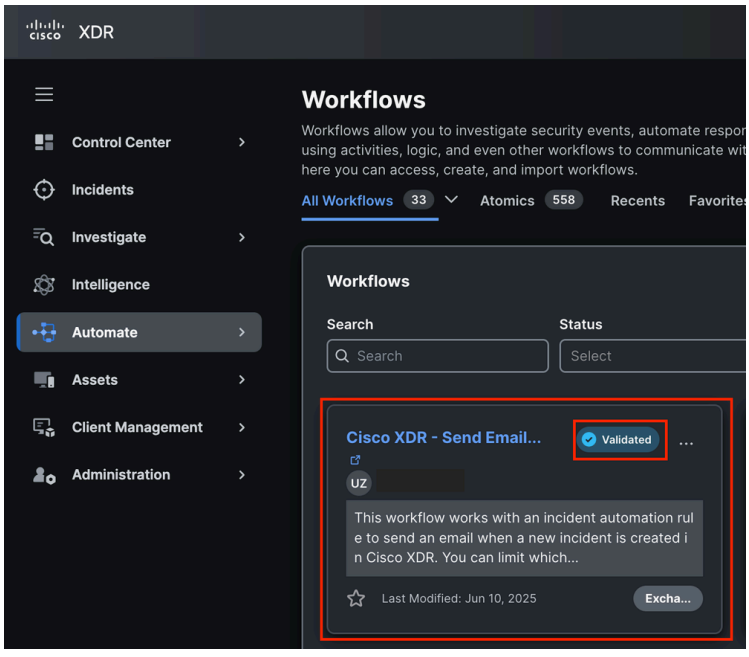
工作流程的目標配置

1. 按「Next」（下一步）。
2. 更新以下項的變數：
    - 收件人
    - 發件人



為工作流分配變數

8.按一下「下一步」。



9.定位至自動>工作流以檢查「已驗證」狀態。

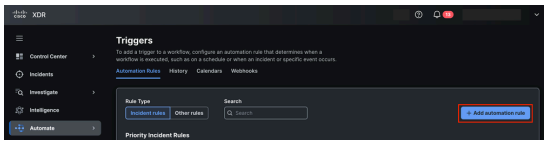
工作流驗證狀態

建立自動化規則

步驟2.配置自動化規則

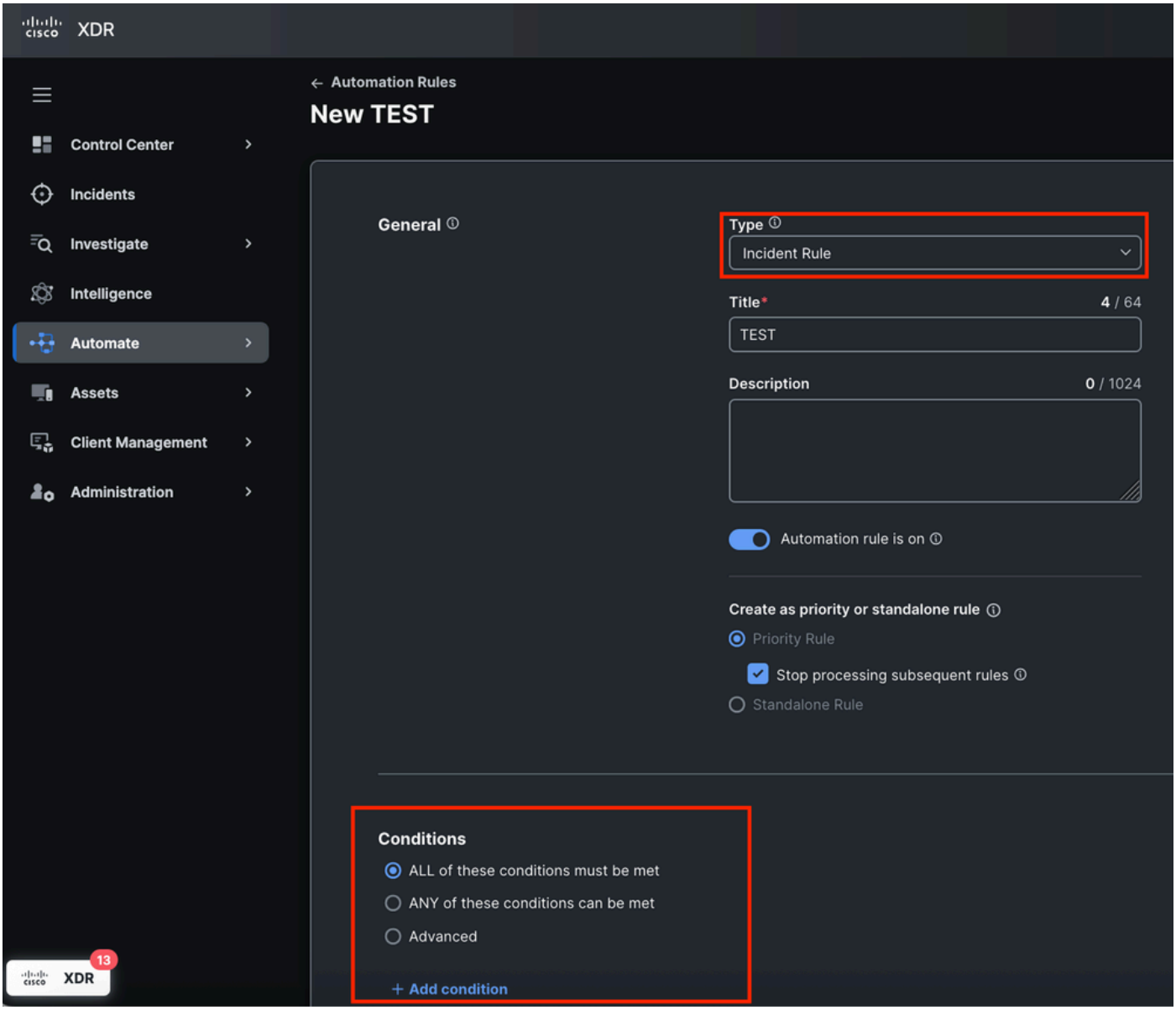
1. 導航到Automation > Triggers部分。

2. 建立新規則。按一下Add automation rule並分配名稱。



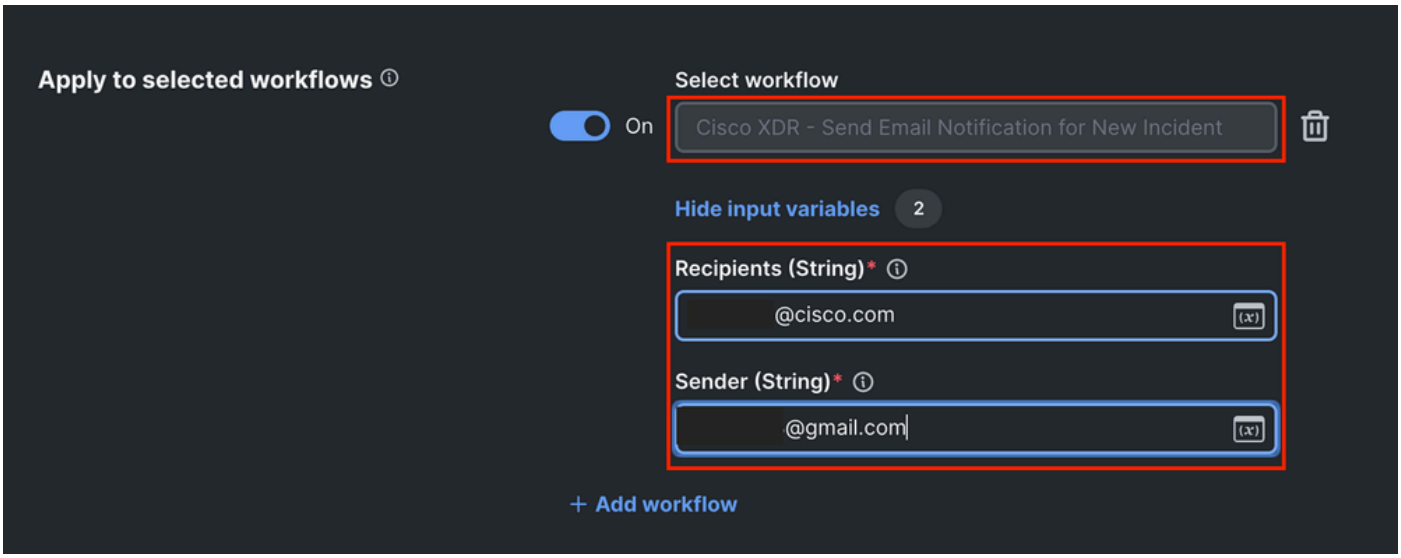
從觸發器新增自動化規則

3. 選擇Incident Rule型別並定義觸發條件。您可以繼續操作，而無需新增規則條件，這樣可確保任何突發事件均啟用此規則。如有必要，自定義條件。



自動化規則型別和條件

4.將自動化規則應用於之前安裝的Cisco XDR - Send Email Notification for New Incident工作流程。設定收件人和發件人變數。

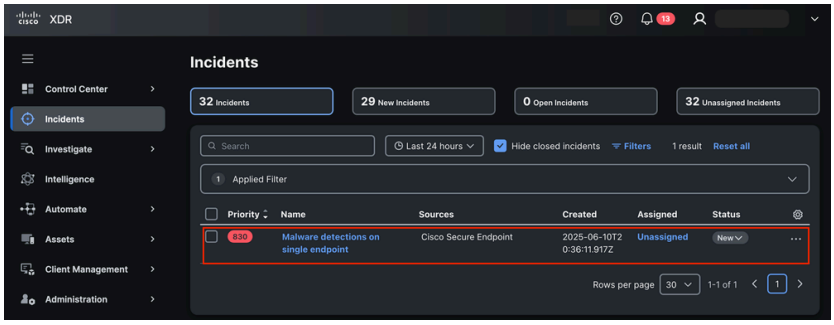


將自動化規則應用於工作流並分配變數

5.儲存規則。

驗證工作流功能

步驟3.驗證工作流執行



1. 生成或等待符合規則條件的事件。

檢測到Cisco XDR中的新事件

2. 按一下Incident，然後按一下View Incident Detail。

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

基於第一次檢測生成初始事件名稱；但是，如果發生其他檢測或新資訊豐富了事件，則情況可能會發生變化。

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。