

使用Cisco XDR配置終端隔離自動化 workflow

目錄

[簡介](#)

[必要條件](#)

[需求](#)

[採用元件](#)

[設定](#)

[思科安全端點中的初始配置](#)

[步驟 1.1: 在策略中啟用隔離功能](#)

[驗證與思科安全終端的整合](#)

[步驟 2.1: 驗證整合](#)

[從Cisco XDR Exchange安裝 workflow](#)

[步驟 3.1: 安裝終端隔離 workflow](#)

[建立自動化規則](#)

[步驟 4.1: 配置自動化規則](#)

[驗證 workflow 功能](#)

[步驟 5.1: 驗證 workflow 執行](#)

[步驟 5.2: 確認端點隔離](#)

[常見問題](#)

[未從思科安全端點啟用隔離功能](#)

簡介

本文描述如何建立自動化 workflow 以隔離新事件的終結點。

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。

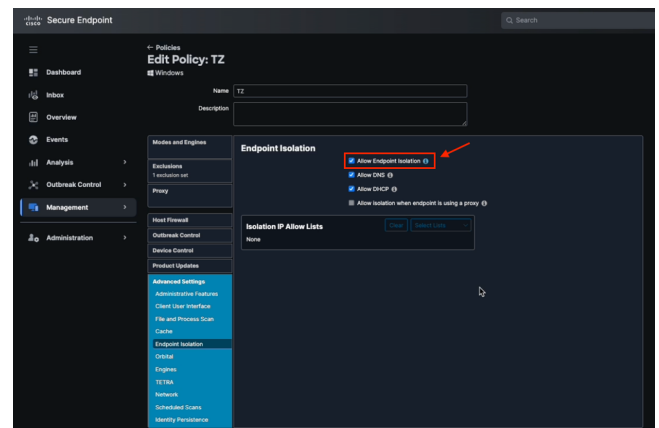
設定

本指南詳細說明了配置和啟用工作流程以在發生事件時自動隔離端點所需的步驟。整合通過思科安全終端和工作流程自動化功能執行。這些步驟概述如下。

思科安全端點中的初始配置

步驟 1.1:在策略中啟用隔離功能

1. 登入到思科安全終端門戶。
2. 導航到管理>策略部分。
3. 選擇應用於要隔離的端點的策略。



4. 確保在策略設定中啟用了Device Isolation選項。

允許從安全端點策略隔離端點

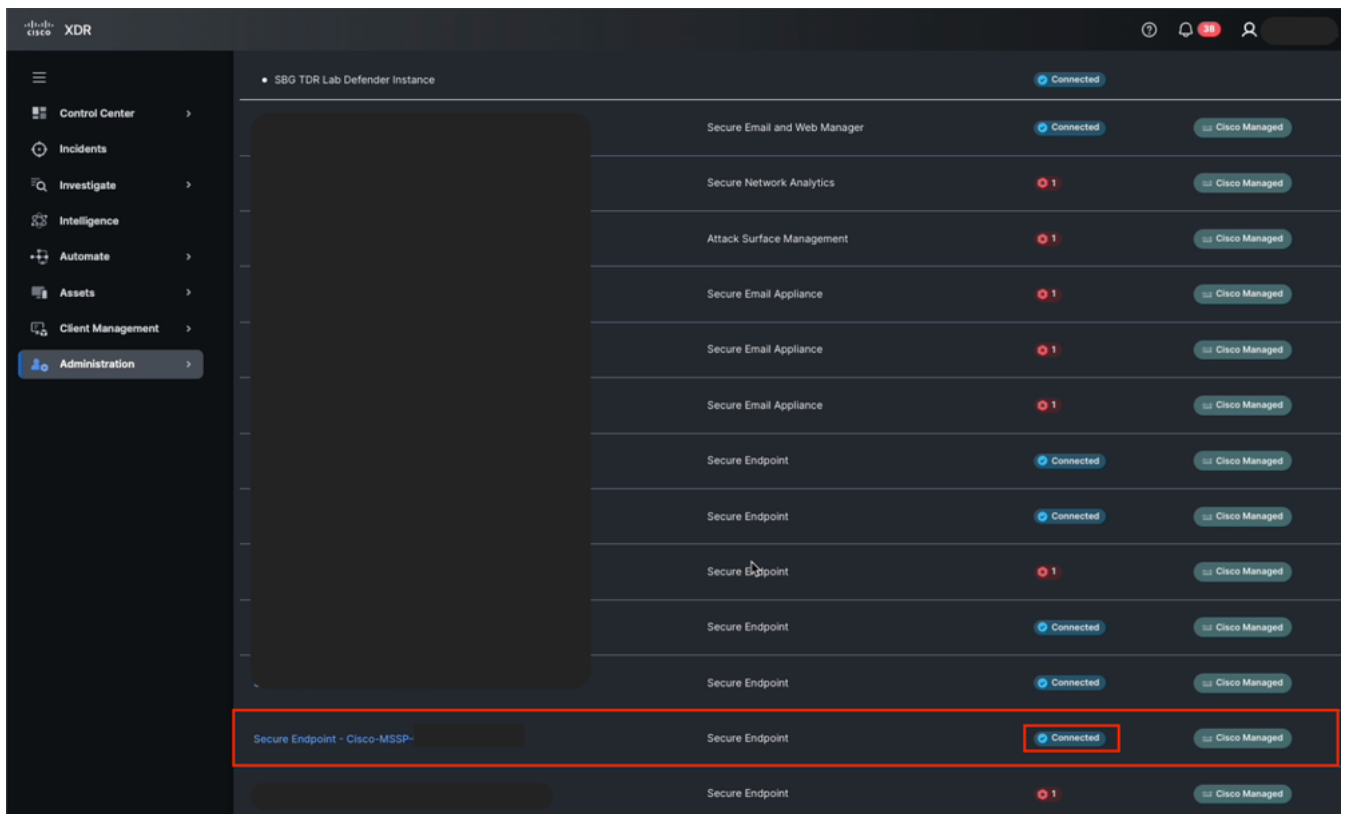
5. 如有必要，請儲存更改並分發策略。

驗證與思科安全終端的整合

步驟 2.1:驗證整合

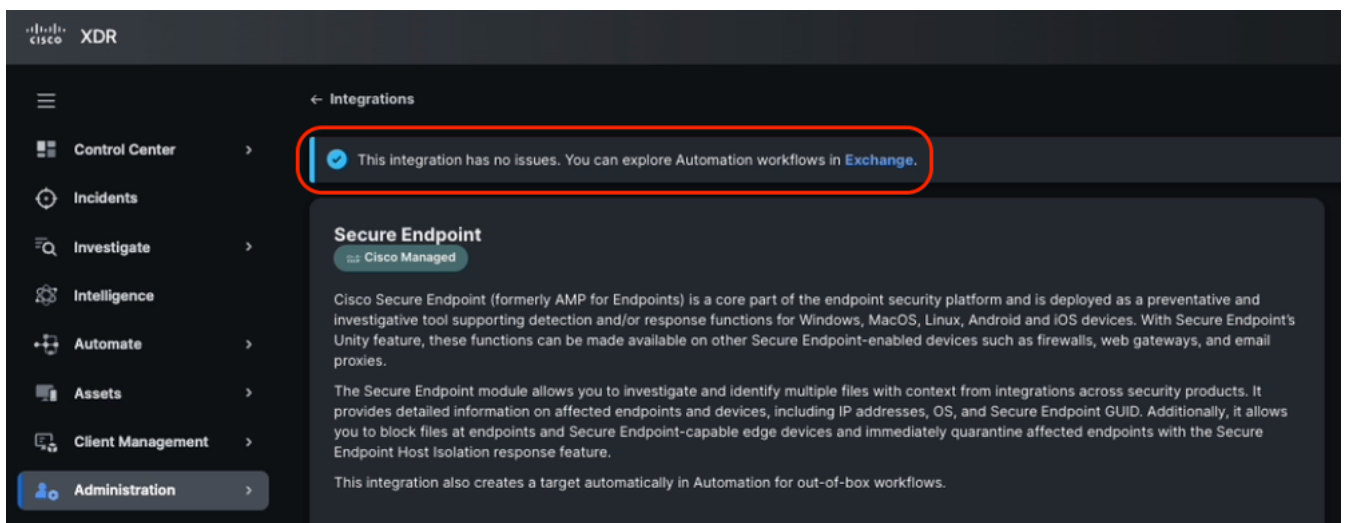
1. 登入Cisco XDR
2. 導航到管理>整合>我的整合部分。
3. 確保正確配置與思科安全終端的整合：

驗證已連線中的整合狀態。



來自Cisco XDR的安全端點整合狀態

確認API配置中沒有錯誤。



安全端點整合運行狀況檢查

從Cisco XDR Exchange安裝工作流

步驟 3.1: 安裝終端隔離工作流

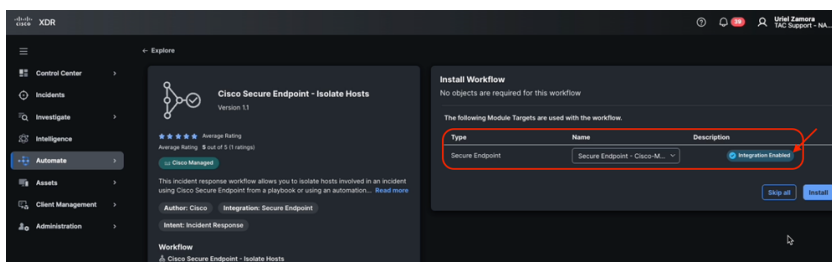
1. 登入到Cisco XDR並導航到自動> Exchange。
2. 搜尋名為Cisco Secure Endpoint - Isolate Hosts的工作流，然後按一下Install。

從Exchange隔離主機工作流



3. 在安裝之前，驗證目標是否可用。

從工作流中啟用模組目標



4.在自動化系統中安裝工作流。

建立自動化規則

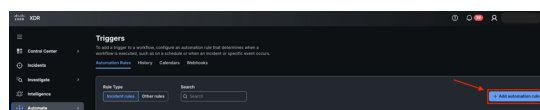
自動化規則是一種配置，它根據特定事件或預定義的時間表定義執行工作流的時間。這些規則可以包括可選條件，如果滿足這些條件，將自動觸發關聯的工作流程。

步驟 4.1:配置自動化規則

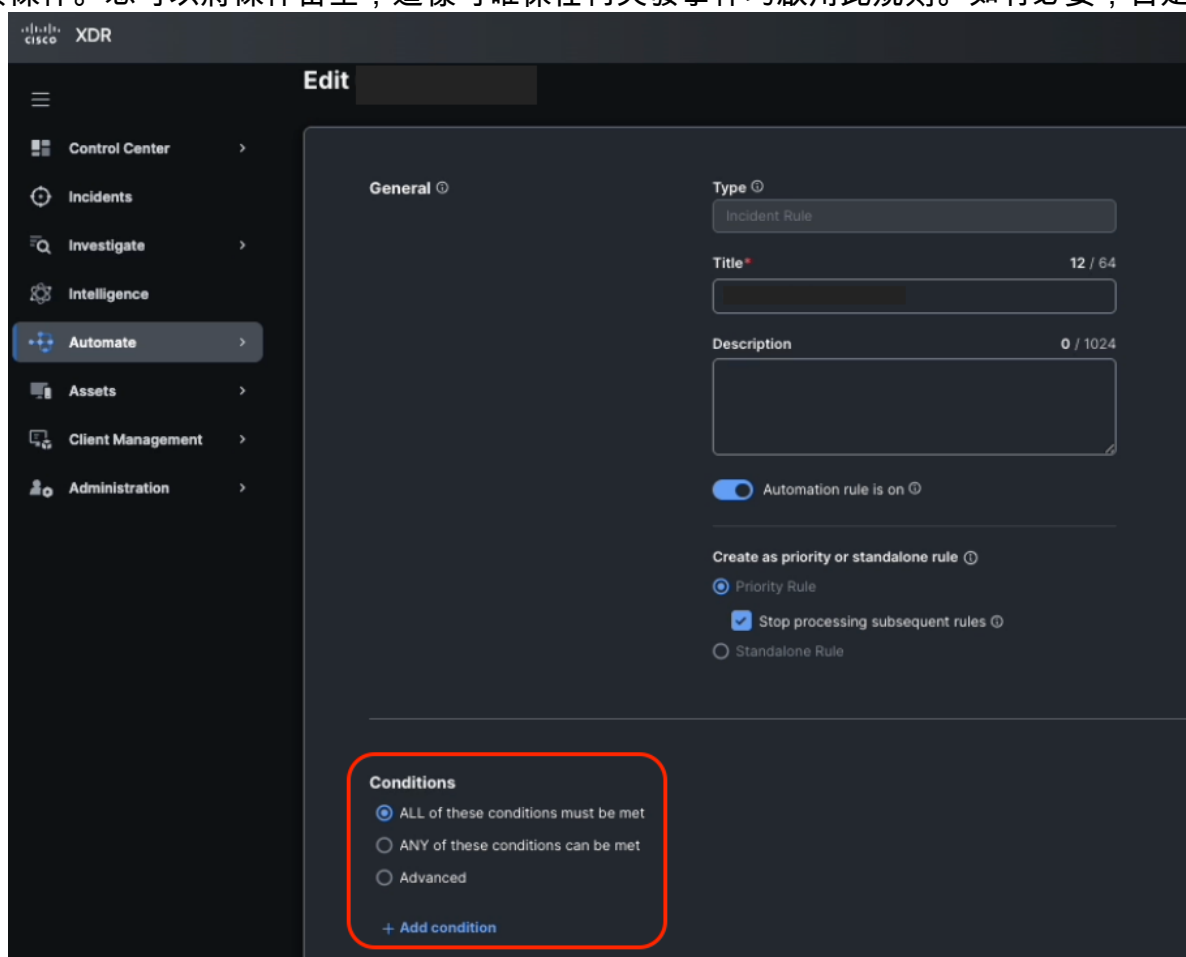
1. 導航到Automation > Triggers部分。

2. 建立新規則。按一下Add automation rule並分配名稱。

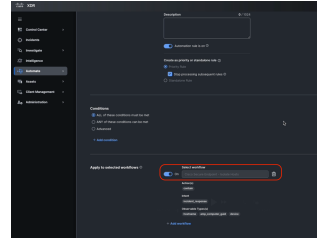
從觸發器新增自動化規則



3. 設定觸發條件。您可以將條件留空，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。



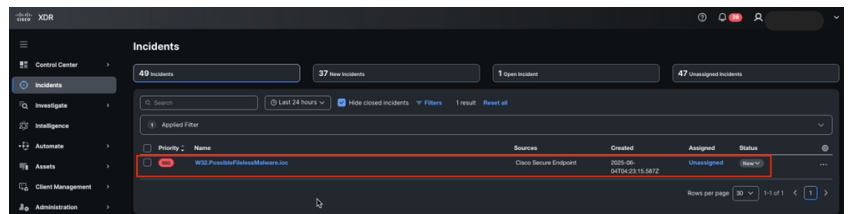
4. 在規則的操作中，選擇之前安裝的思科安全終端 — 隔離主機工作流程。

將自動化規則分配給 workflow

5. 按一下「Save」。

驗證 workflow 功能

步驟 5.1: 驗證 workflow 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

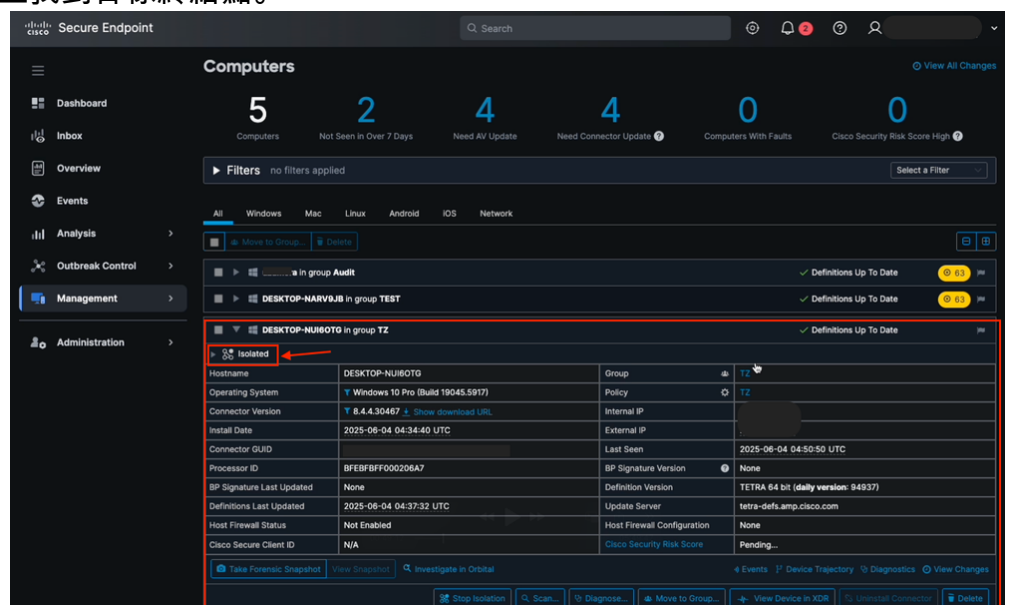
2. 建立突發事件後，請檢查Worklog頁籤（在突發事件中）以確認 workflow 是否成功執行。



「事件工作日志」頁籤資訊

步驟 5.2: 確認端點隔離

1. 登入到思科安全終端門戶。
2. 導航到管理>電腦部分並找到目標終結點。



3. 確認裝置狀態為隔離。

4. 如果端點未隔離，請檢視工作流日誌和配置以確定可能的問題。

常見問題

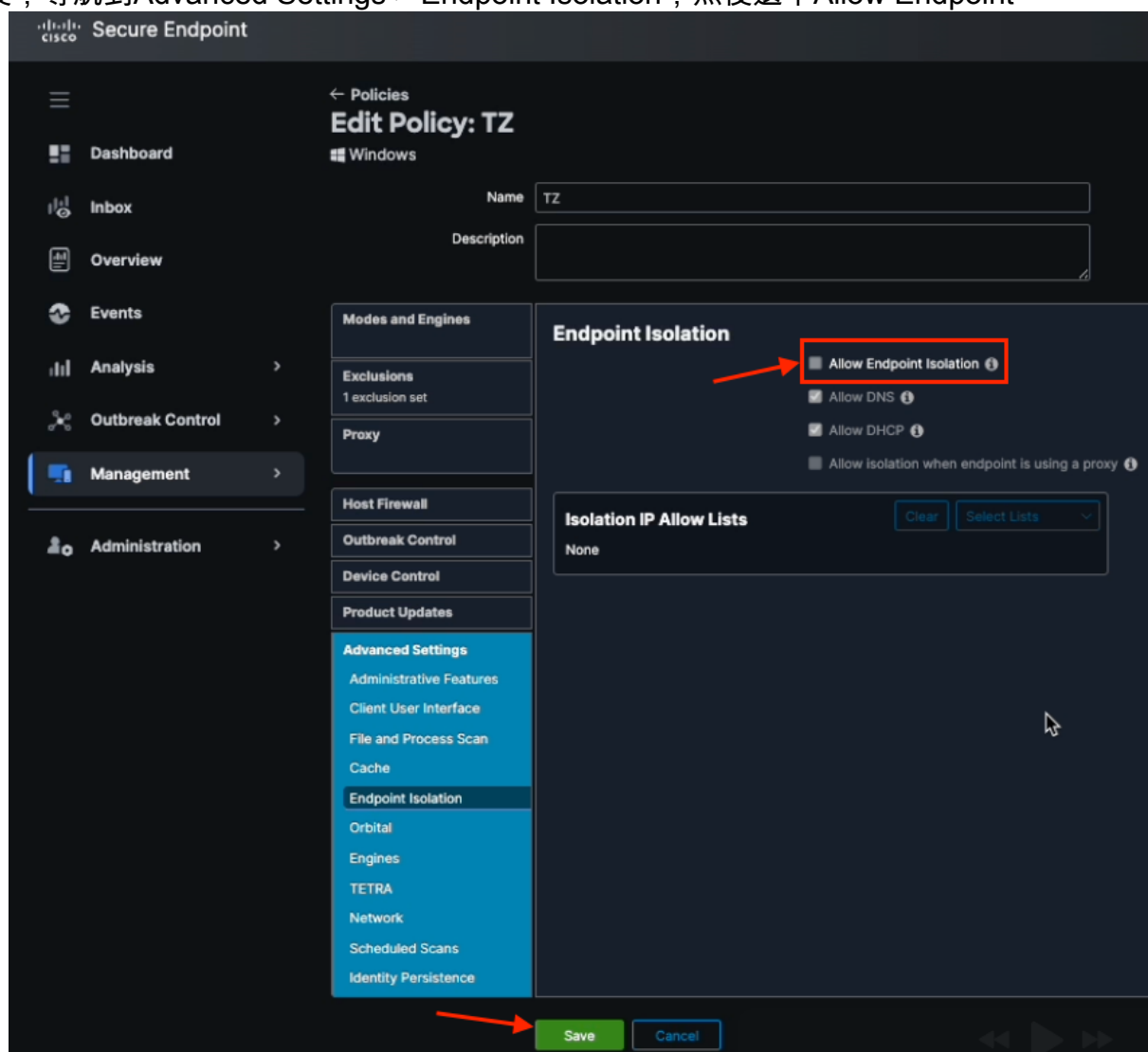
未從思科安全端點啟用隔離功能

1. 從Cisco XDR導航到Incidents，找到最後一個事件，然後導航到Worklog。
2. 運行自動化工作流後，檢查是否存在任何相關錯誤。

例如，由於未在安全端點策略上啟用端點隔離，因此端點隔離不允許隔離主機。

事件工作日誌中的自動化工作流結果

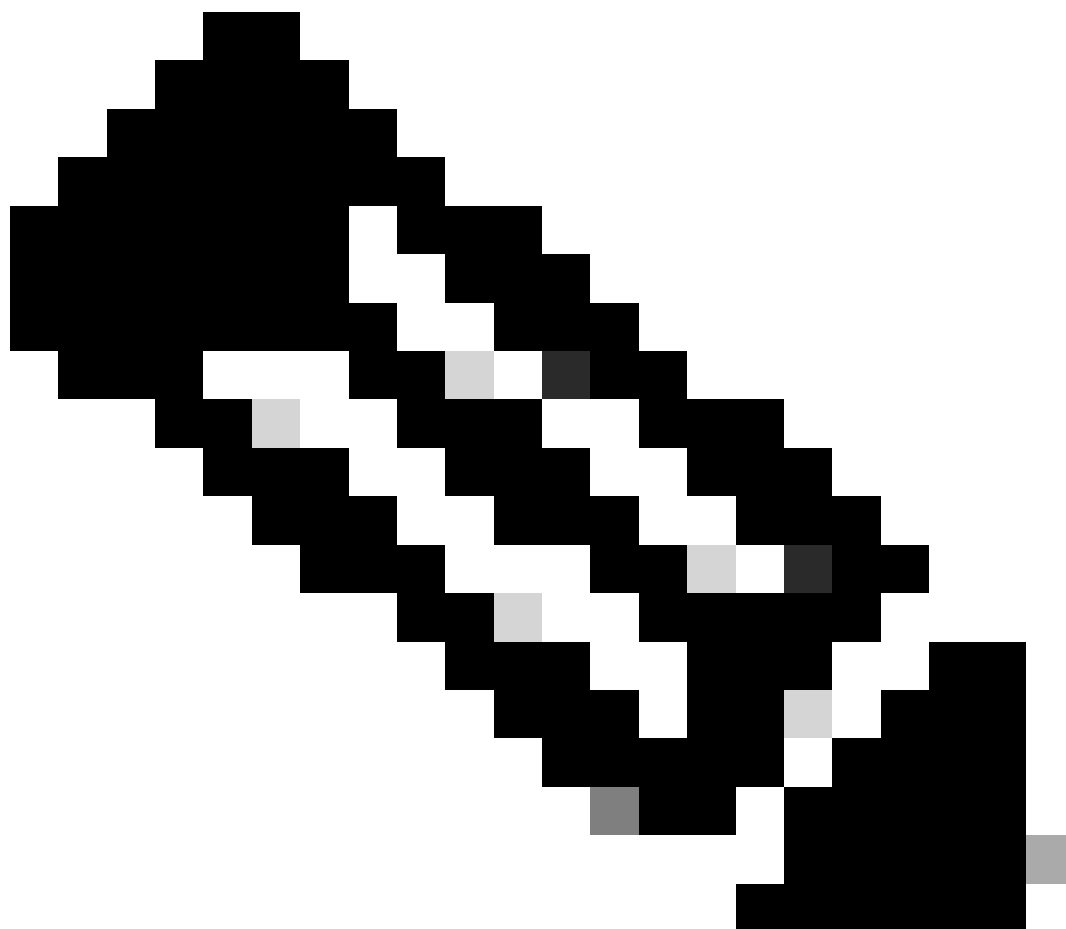
3. 從安全端點導航到管理>策略，選擇有問題的策略。
4. 進入策略後，導航到Advanced Settings > Endpoint Isolation，然後選中Allow Endpoint



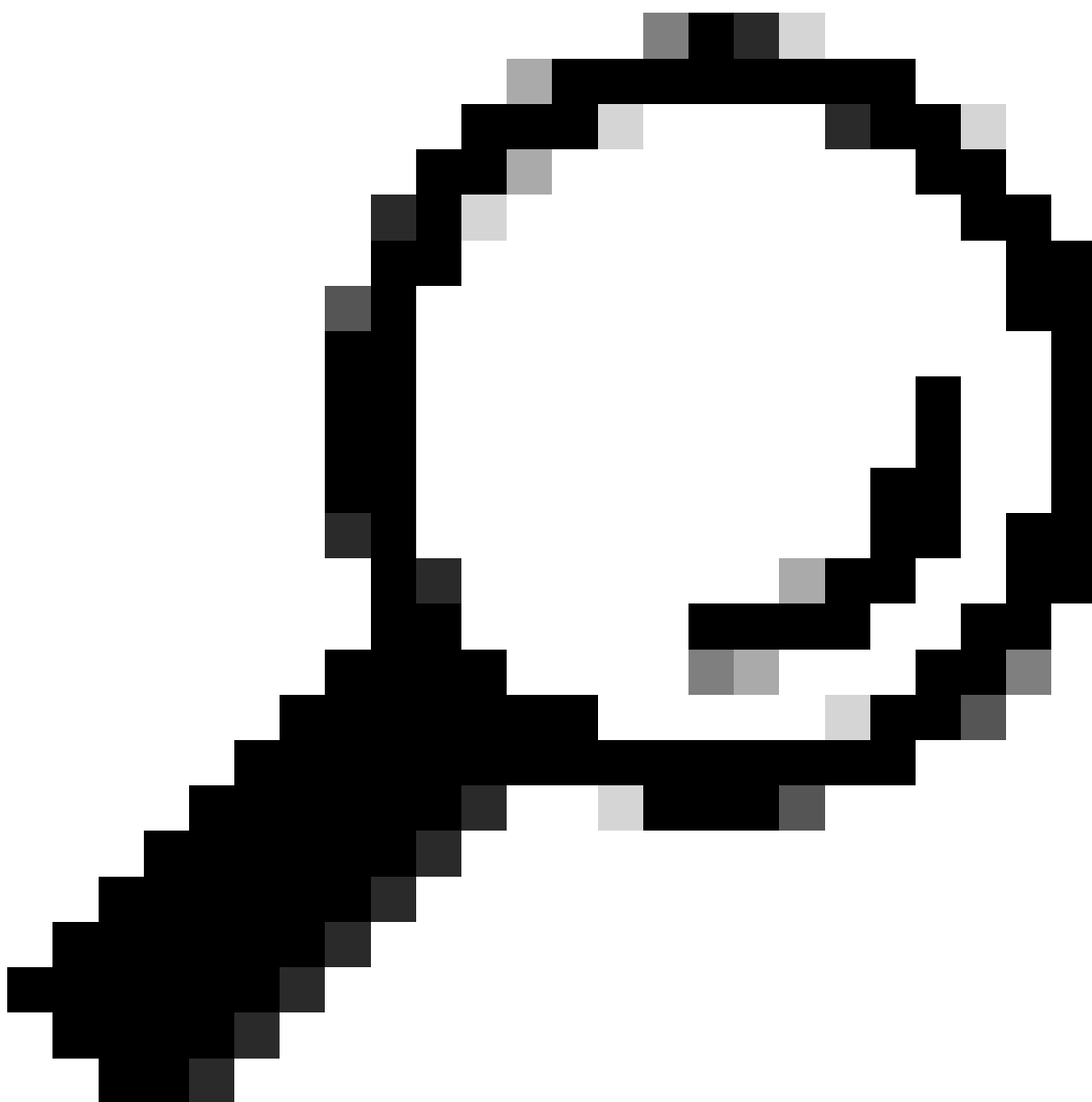
Isolation框。

安全端點策略中的「允許端點隔離」覈取方塊

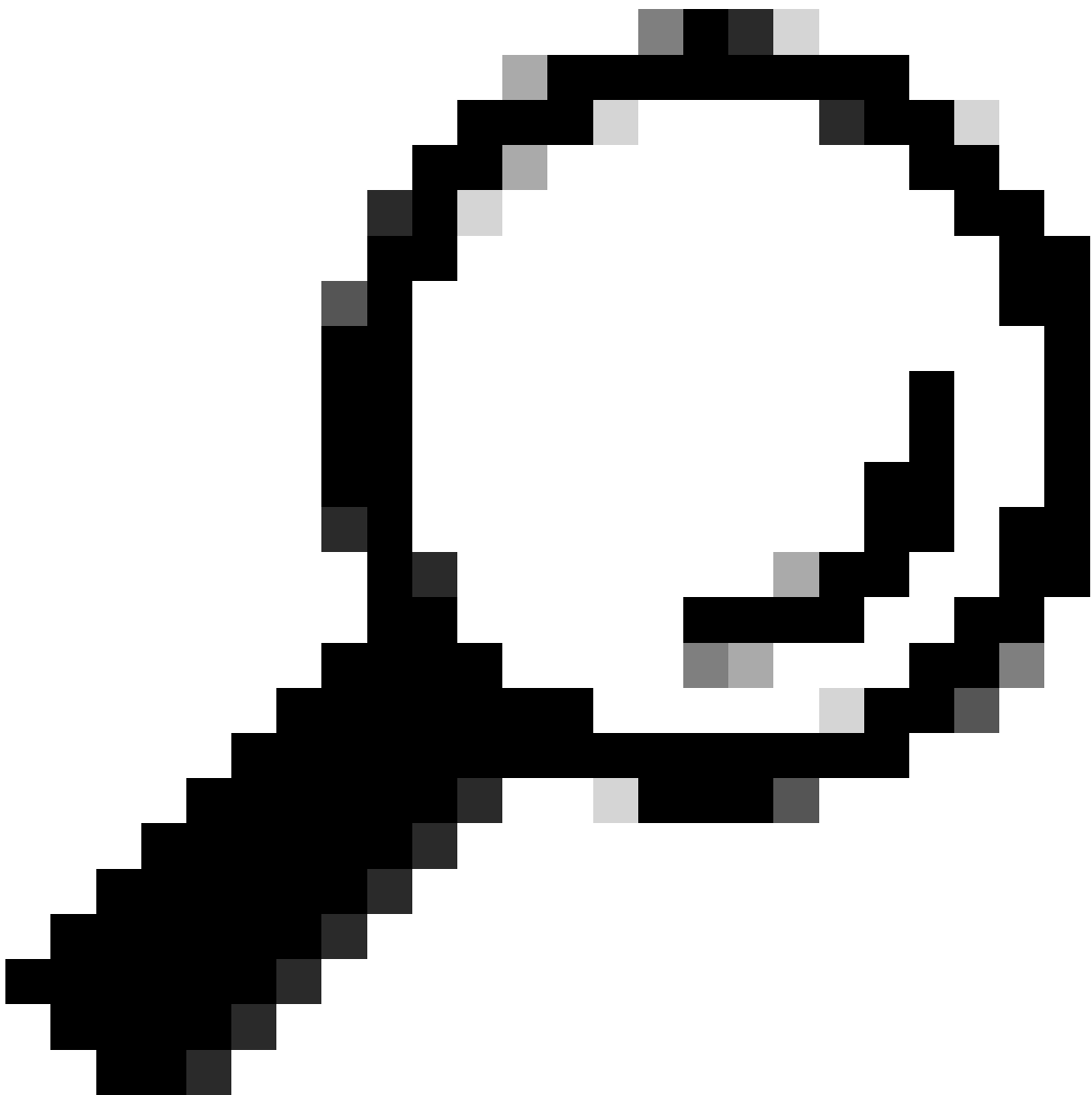
5.按一下儲存。



注意：確保您擁有配置整合和工作流程所需的管理許可權。



提示：在生產中部署自動化之前，在受控環境中測試設定。



提示：記錄對工作流或自動化規則所做的任何自定義調整。

完成這些步驟後，您可以成功配置並啟用工作流，該工作流在建立事件後自動隔離終端，並確保快速有效地響應安全威脅。

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）。