

使用Cisco XDR配置终端隔离自动化工作流程

目录

[简介](#)

[先决条件](#)

[要求](#)

[使用的组件](#)

[配置](#)

[思科安全终端中的初始配置](#)

[第 1.1 步：在策略中启用隔离功能](#)

[验证与思科安全终端的集成](#)

[第 2.1 步：验证集成](#)

[从Cisco XDR Exchange安装工作流](#)

[第 3.1 步：安装终端隔离工作流程](#)

[创建自动化规则](#)

[第 4.1 步：配置自动化规则](#)

[验证工作流程功能](#)

[第 5.1 步：验证工作流程执行](#)

[第 5.2 步：确认终端隔离](#)

[常见问题](#)

[未从思科安全终端启用隔离功能](#)

简介

本文档介绍如何创建自动化工作流程以隔离新事件的终端。

先决条件

要求

本文档没有任何特定的要求。

使用的组件

本文档不限于特定的软件和硬件版本。

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

配置

本指南详细介绍配置和激活工作流程以在发生事件时自动隔离端点所需的步骤。集成通过思科安全终端和 workflow 自动化功能执行。这些步骤概述如下。

思科安全终端中的初始配置

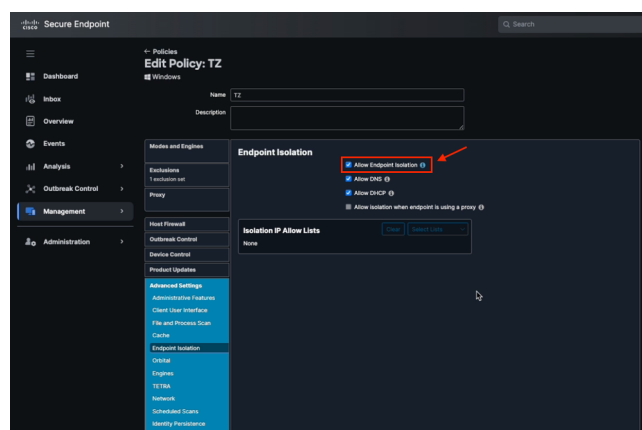
第 1.1 步：在策略中启用隔离功能

1. 登录思科安全终端门户。
2. 导航到管理>策略部分。
3. 选择应用于要隔离的终端的策略。

4. 确保已在策略设置中启用Device Isolation选项。

允许从安全端点策略隔离端点

5. 如有必要，请保存更改并分发策略。

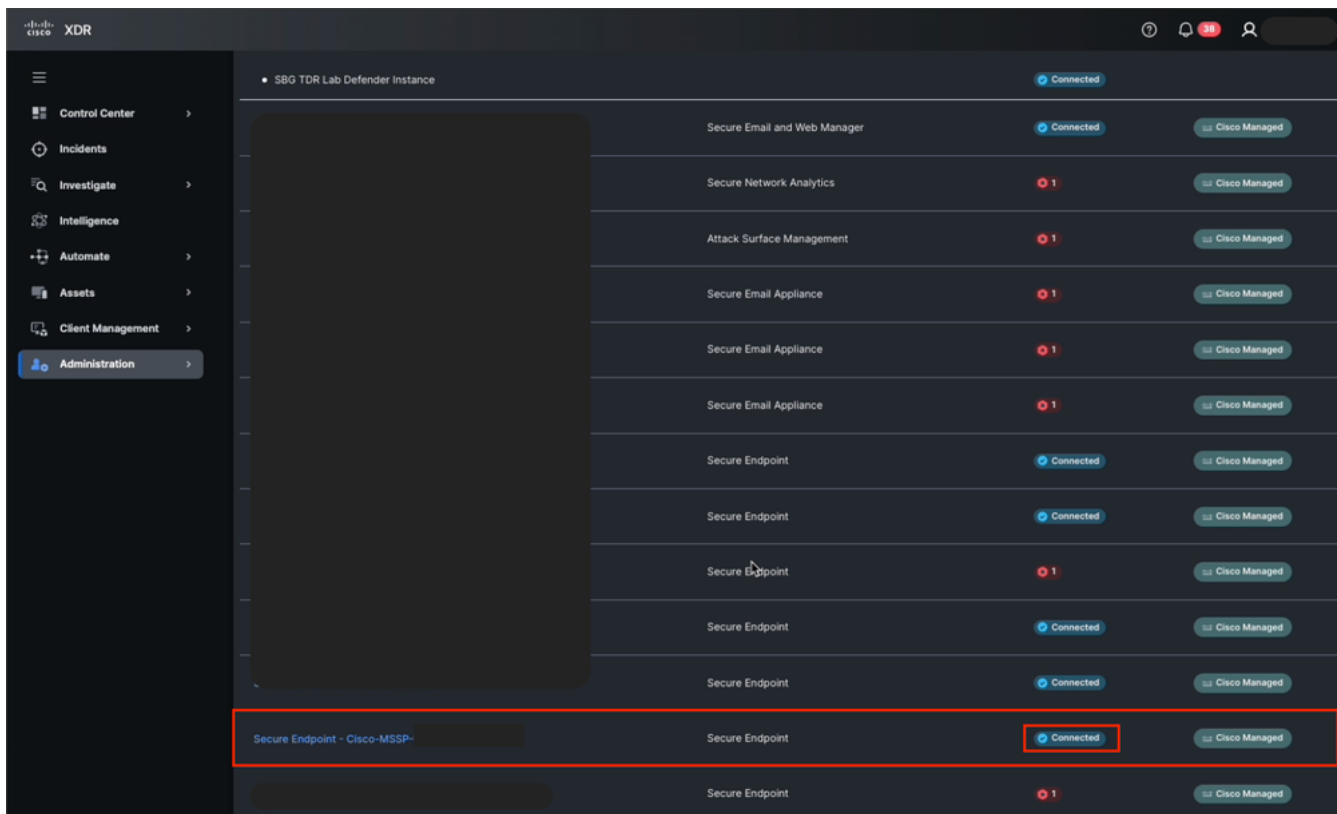


验证与思科安全终端的集成

第 2.1 步：验证集成

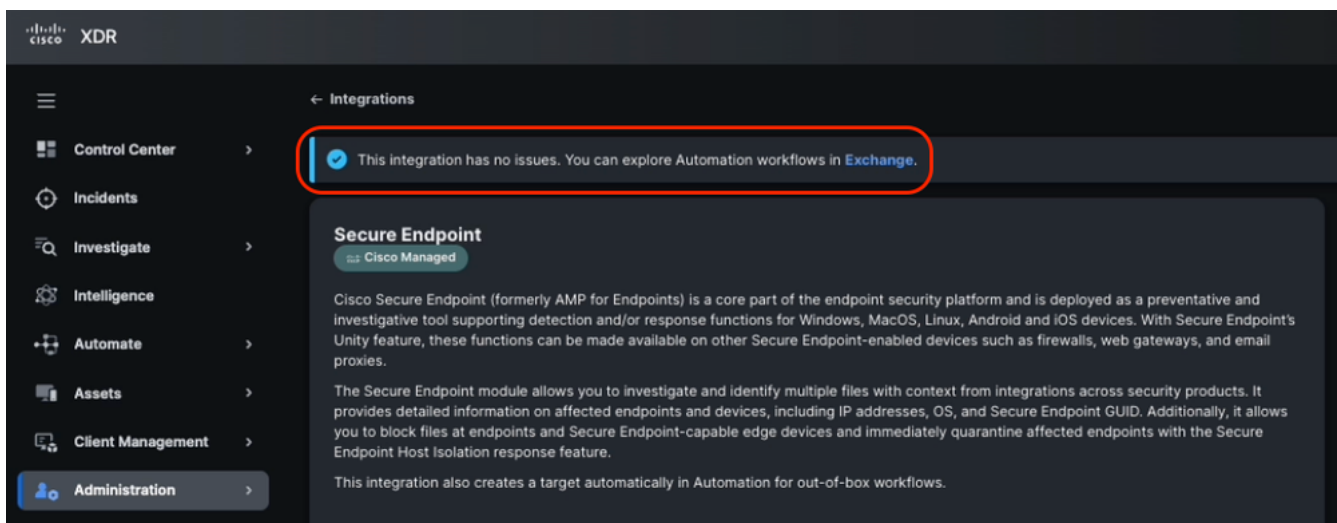
1. 登录到Cisco XDR。
2. 导航到管理>集成>我的集成部分。
3. 确保正确配置与思科安全终端的集成：

验证已连接中的集成状态。



来自思科XDR的安全终端集成状态

确认API配置中没有错误。



安全终端集成运行状况检查

从Cisco XDR Exchange安装 workflows

第 3.1 步：安装终端隔离工作流程

1. 登录到Cisco XDR并导航到自动> Exchange。

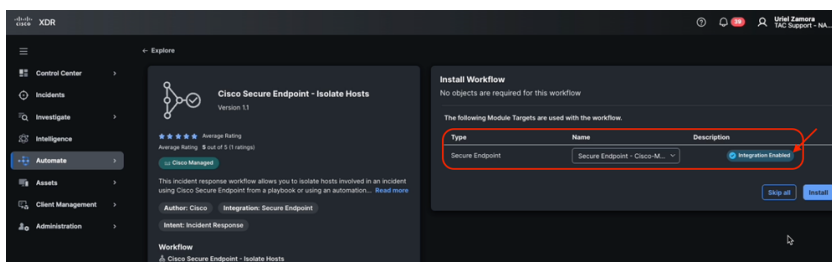
2. 搜索名为Cisco Secure Endpoint - Isolate Hosts的工作流程，然后单击Install。



从Exchange隔离主机 workflow

3. 在安装之前，验证目标是否可用。

从工作流程启用模块目标



4.在自动化系统中安装 workflow。

创建自动化规则

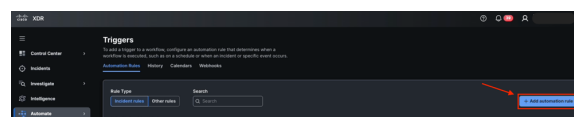
自动化规则是一种配置，它根据特定事件或预定义的计划定义应何时执行 workflow。这些规则可以包括可选条件，如果满足这些条件，将自动触发关联的工作流程。

第 4.1 步：配置自动化规则

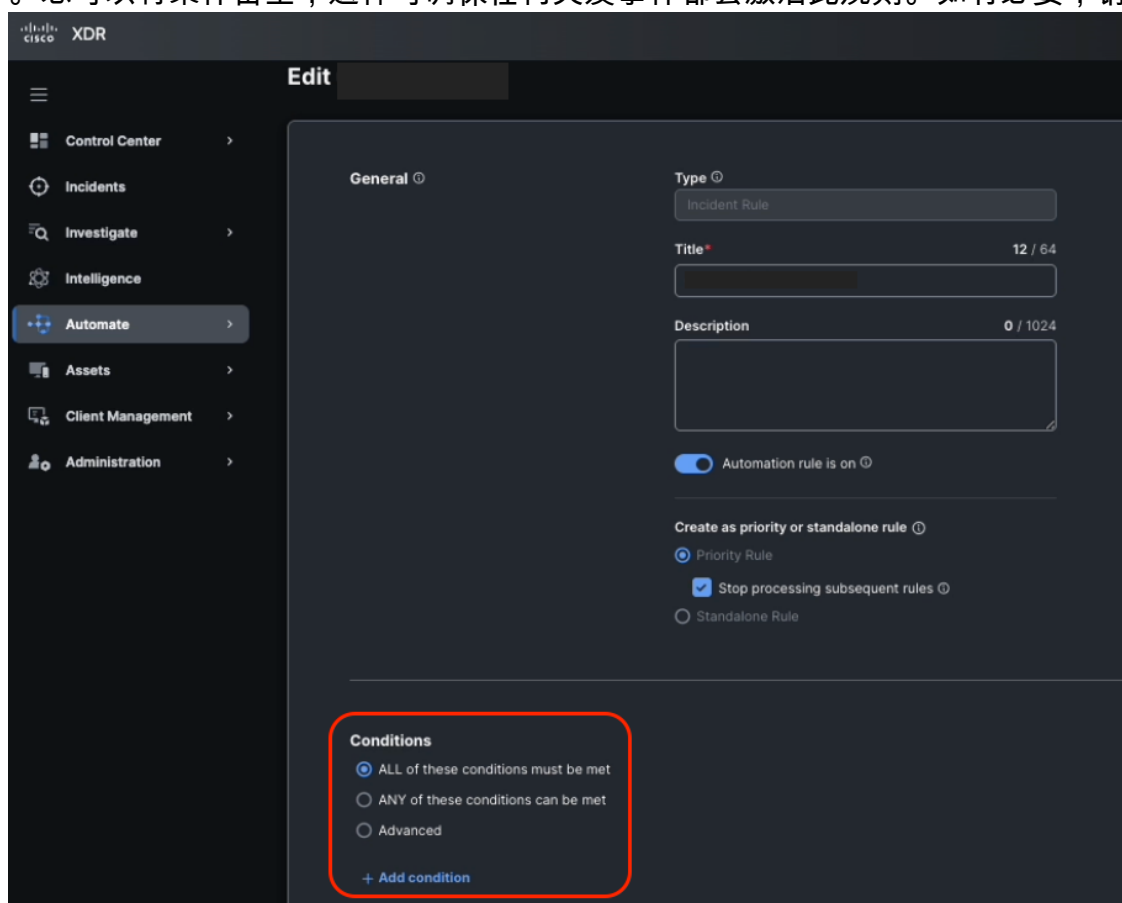
1. 导航到自动化>触发器部分。

2. 创建新规则。单击Add automation rule并分配名称。

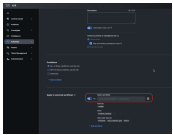
从触发器添加自动化规则



3. 设置触发条件。您可以将条件留空，这样可确保任何突发事件都会激活此规则。如有必要，请



自定义条件。



4. 在规则的操作中，选择之前安装的Cisco Secure Endpoint - Isolate Hosts工作流。

将自动化规则分配给工作流

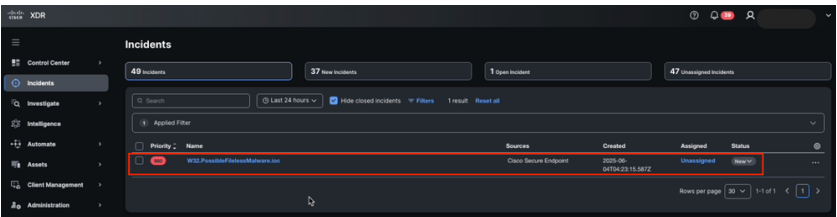
5. Click Save.

验证 workflow 功能

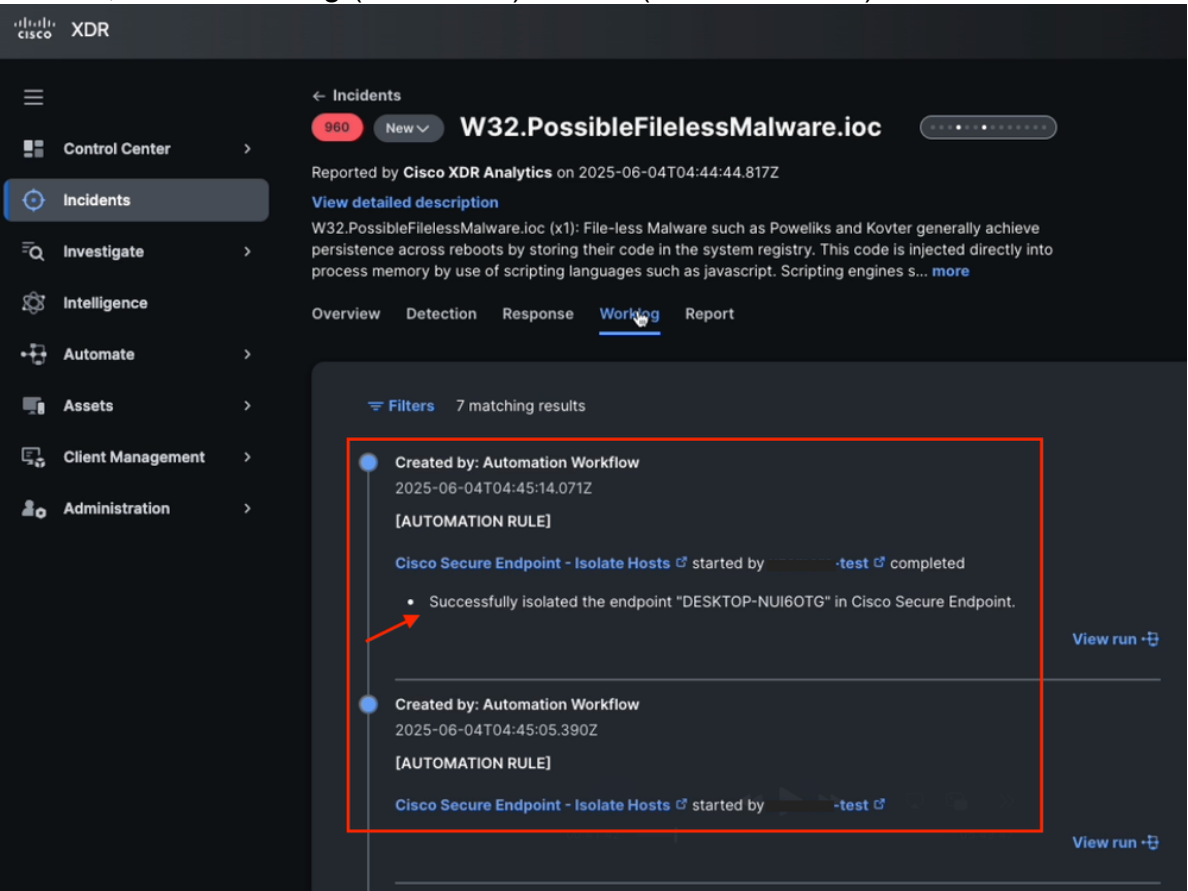
第 5.1 步：验证 workflow 执行

1. 生成或等待符合规则条件的事件。

检测到Cisco XDR中的新事件



2. 创建突发事件后，请选中Worklog（工作日志）选项卡（在突发事件内）以确认工作流是否成功执行。

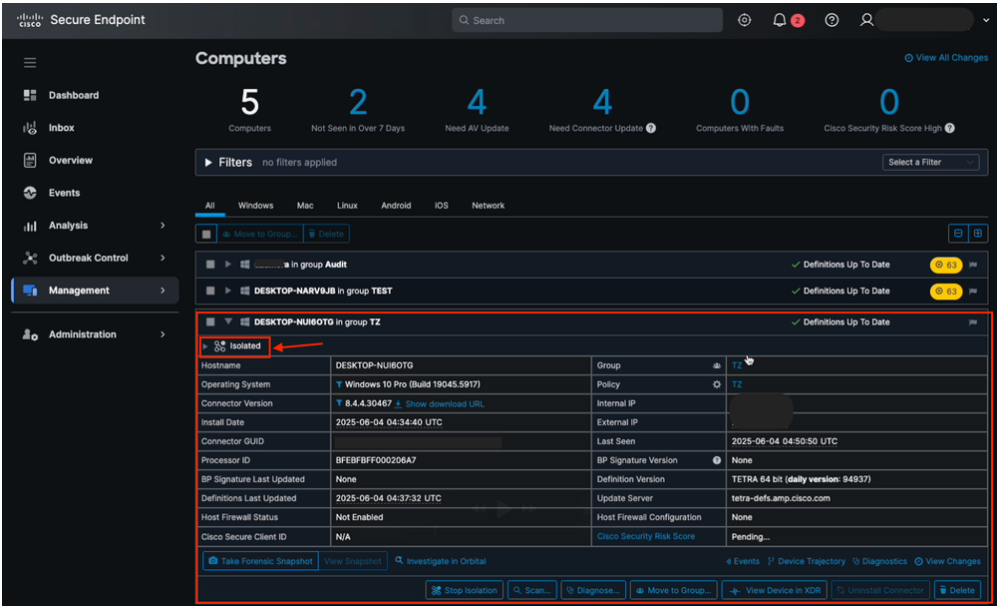


功执行。

事故工作日志选项卡信息

第 5.2 步：确认终端隔离

- 1. 登录思科安全终端门户。
- 2. 导航到管理>计算机部分并找到目标终端。



3. 确认设备状态为隔离。

从安全终端计算机隔离状态

4. 如果终端未隔离，请查看工作流程日志和配置以确定可能的问题。

常见问题

未从思科安全终端启用隔离功能

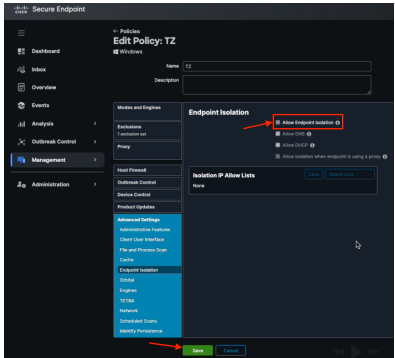
- 1.从Cisco XDR导航到Incidents，找到最后一个事件并导航到Worklog。
- 2.运行自动化工作流后，检查是否存在任何相关错误。



例如，由于未在安全终端策略上启用终端隔离，终端隔离不允许隔离主机。

事件工作日志中的自动化工作流程结果

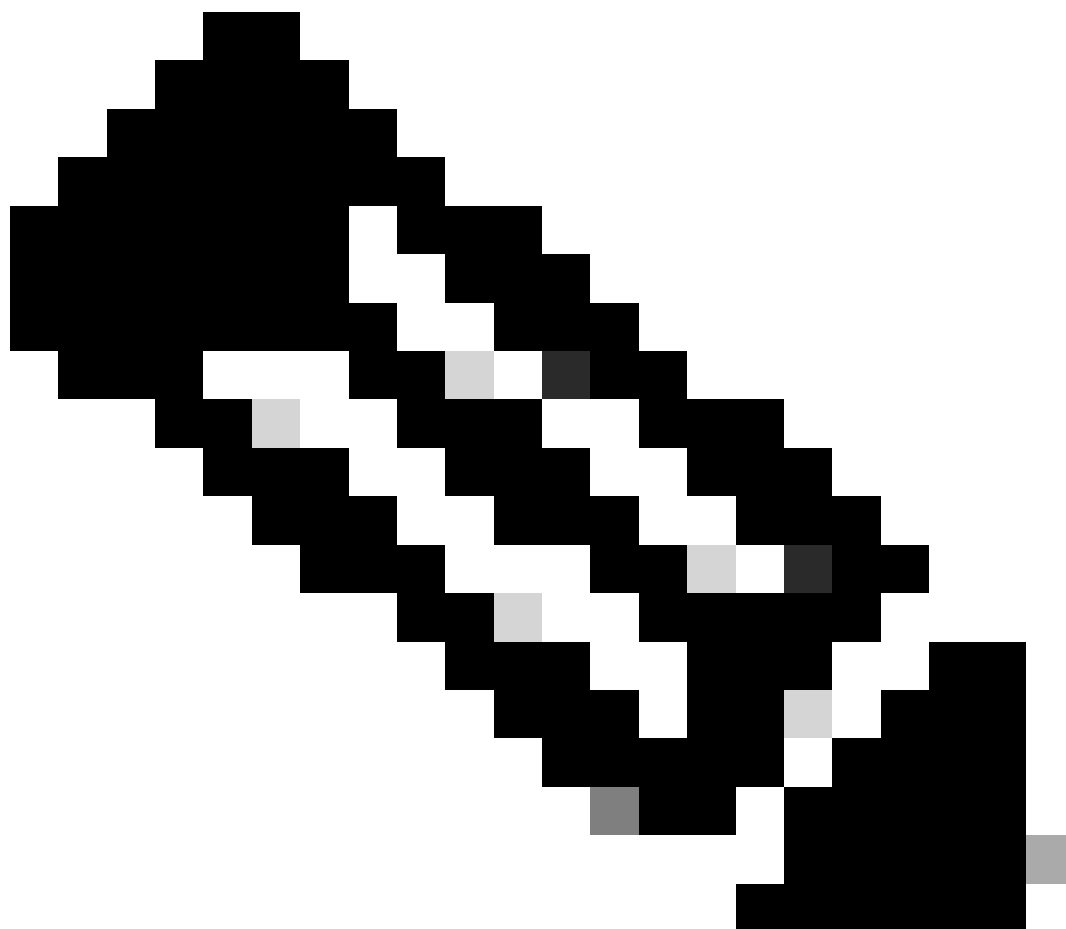
3.在安全终端中，导航到管理>策略，选择有问题的策略。



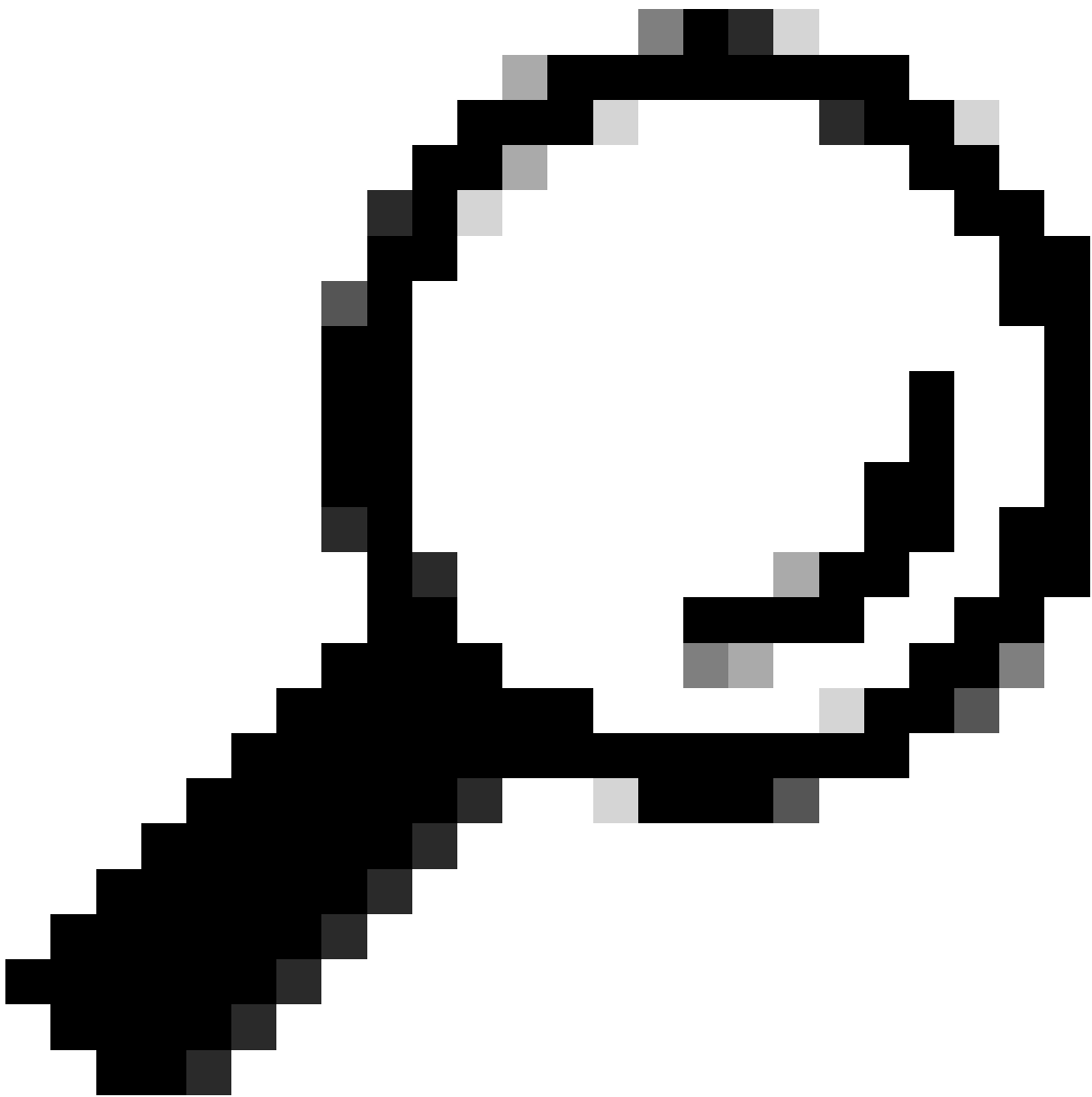
4.进入策略后，导航到高级设置>端点隔离，然后选中允许端点隔离框。

“安全终端策略”中的“允许终端隔离”复选框

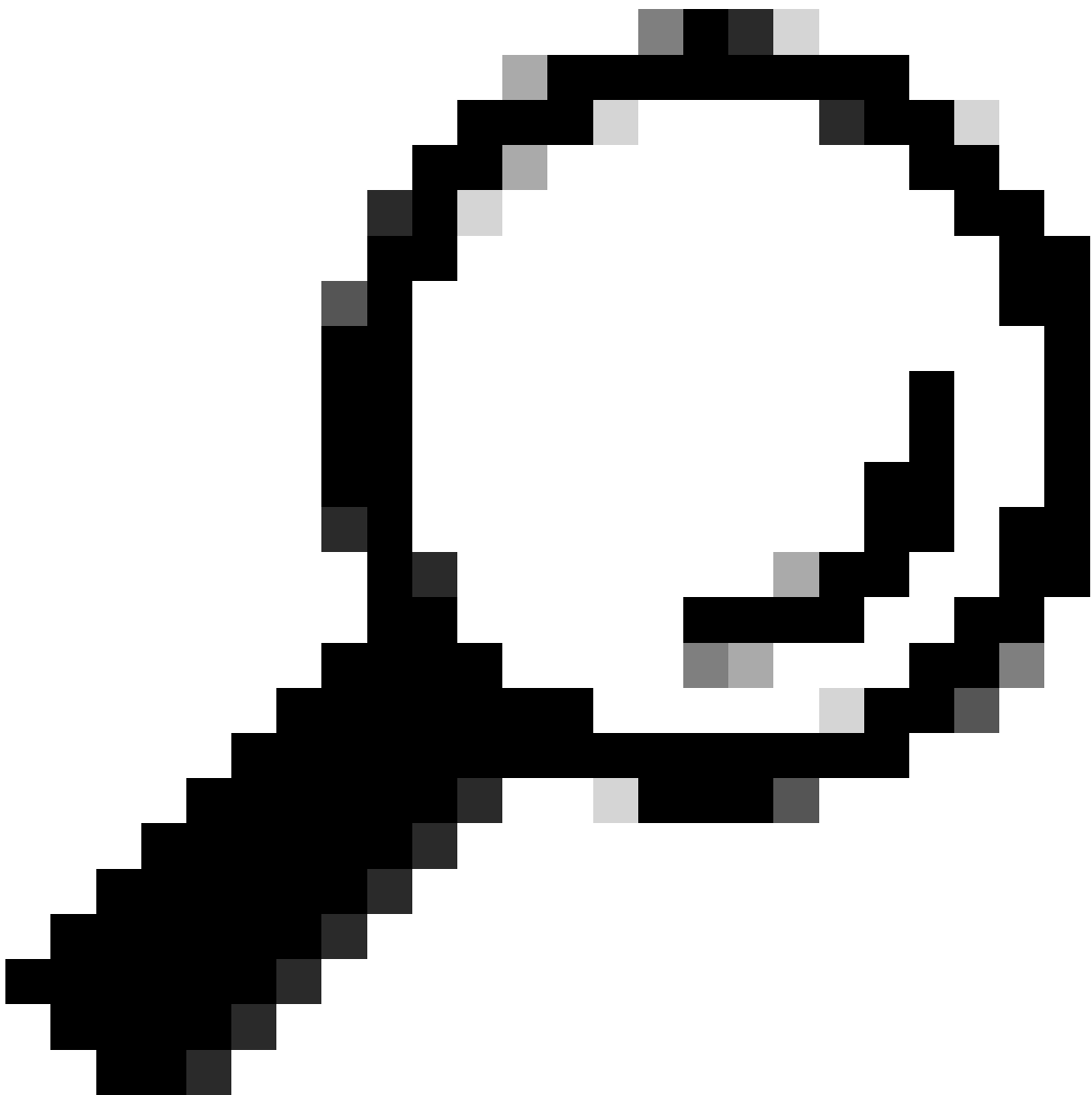
5.单击保存。



注意：确保您具有配置集成和工作流程所需的管理权限。



提示：在生产中部署自动化之前，请在受控环境中测试设置。



提示：记录对工作流或自动化规则所做的任何自定义调整。

完成这些步骤后，您可以成功配置并激活工作流，该工作流会在发生事故后自动隔离终端，并确保快速有效地响应安全威胁。

关于此翻译

思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。