Configuración del flujo de trabajo automatizado de aislamiento de terminales con Cisco XDR

Contenido

Introducción

Este documento describe cómo crear un flujo de trabajo de automatización para aislar un terminal para un nuevo incidente.

conservado

Prerequisites

Requirements

No hay requisitos específicos para este documento.

Componentes Utilizados

Este documento no tiene restricciones específicas en cuanto a versiones de software y de hardware.

La información que contiene este documento se creó a partir de los dispositivos en un ambiente

de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

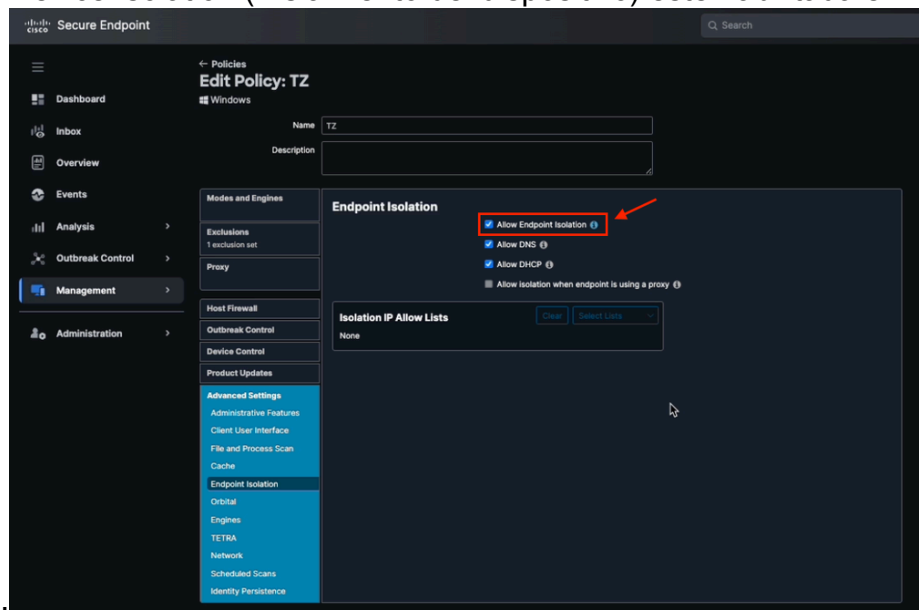
Configurar

Esta guía detalla los pasos necesarios para configurar y activar un flujo de trabajo para aislar automáticamente un terminal cuando se produce un incidente. La integración se realiza con Cisco Secure Endpoint y la funcionalidad de automatización del flujo de trabajo. Los pasos se describen a continuación.

Configuración inicial en Cisco Secure Endpoint

Paso 1.1: Activar la función de aislamiento en la política

1. Inicie sesión en el portal de Cisco Secure Endpoint.
2. Navegue hasta la sección Administración > Políticas.
3. Seleccione la política que se aplica al terminal que desea aislar.
4. Asegúrese de que la opción Device Isolation (Aislamiento del dispositivo) esté habilitada en la configuración de directiva.



Permitir el aislamiento de terminales desde la política de terminales seguros

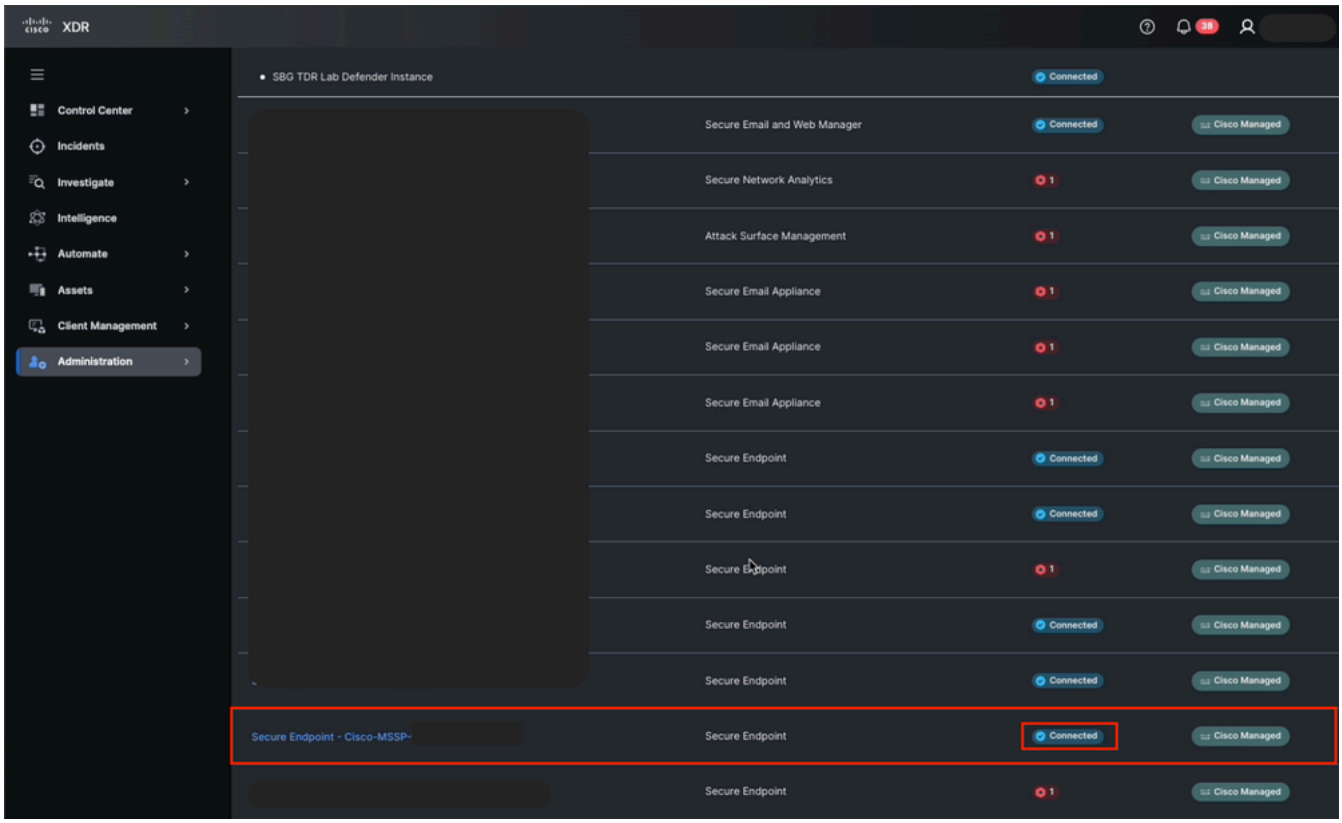
5. Guarde los cambios y distribuya la directiva si es necesario.

Validar la integración con Cisco Secure Endpoint

Paso 2.1: Verificar la integración

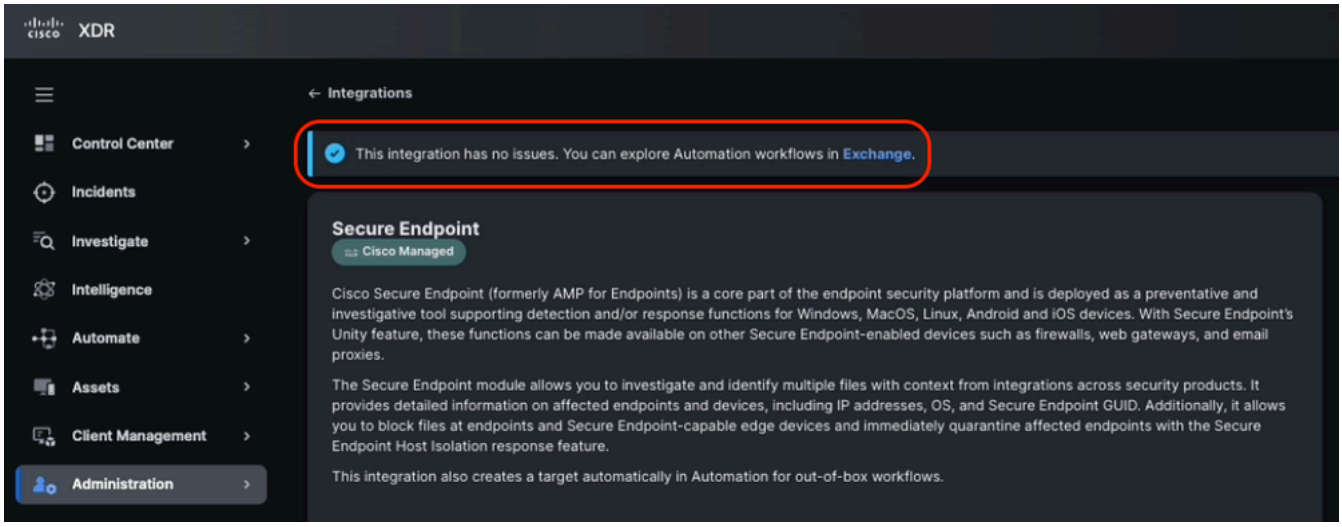
1. Inicie sesión en Cisco XDR.
2. Vaya a la sección Administración > Integraciones > Mis integraciones.
3. Asegúrese de que la integración con Cisco Secure Endpoint esté configurada correctamente:

Verifique el estado de integración en Conectado.



Estado de integración de terminales seguros de Cisco XDR

Confirme que no haya errores en la configuración de la API.

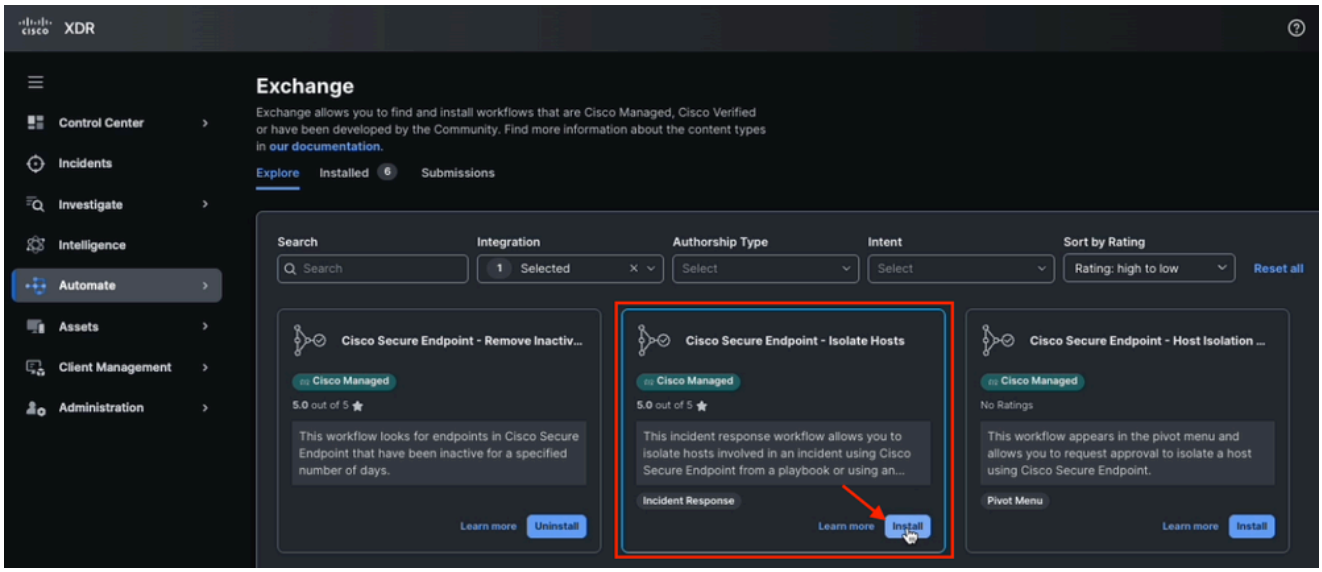


Comprobación del estado de integración de terminales seguros

Instalación del flujo de trabajo desde Cisco XDR Exchange

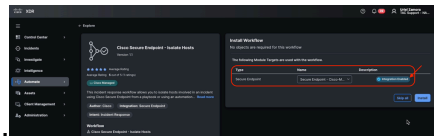
Paso 3.1: Instalación del flujo de trabajo de aislamiento de terminales

1. Inicie sesión en Cisco XDR y navegue hasta Automatizar > Exchange.
2. Busque el flujo de trabajo denominado Cisco Secure Endpoint - Isolate Hosts y haga clic en Install.



Aislar flujo de trabajo de host de Exchange

3. Verifique que el destino esté disponible antes de la instalación.



Objetivo del módulo habilitado desde el flujo de trabajo

4. Instale el flujo de trabajo en su sistema de automatización.

Crear una regla de automatización

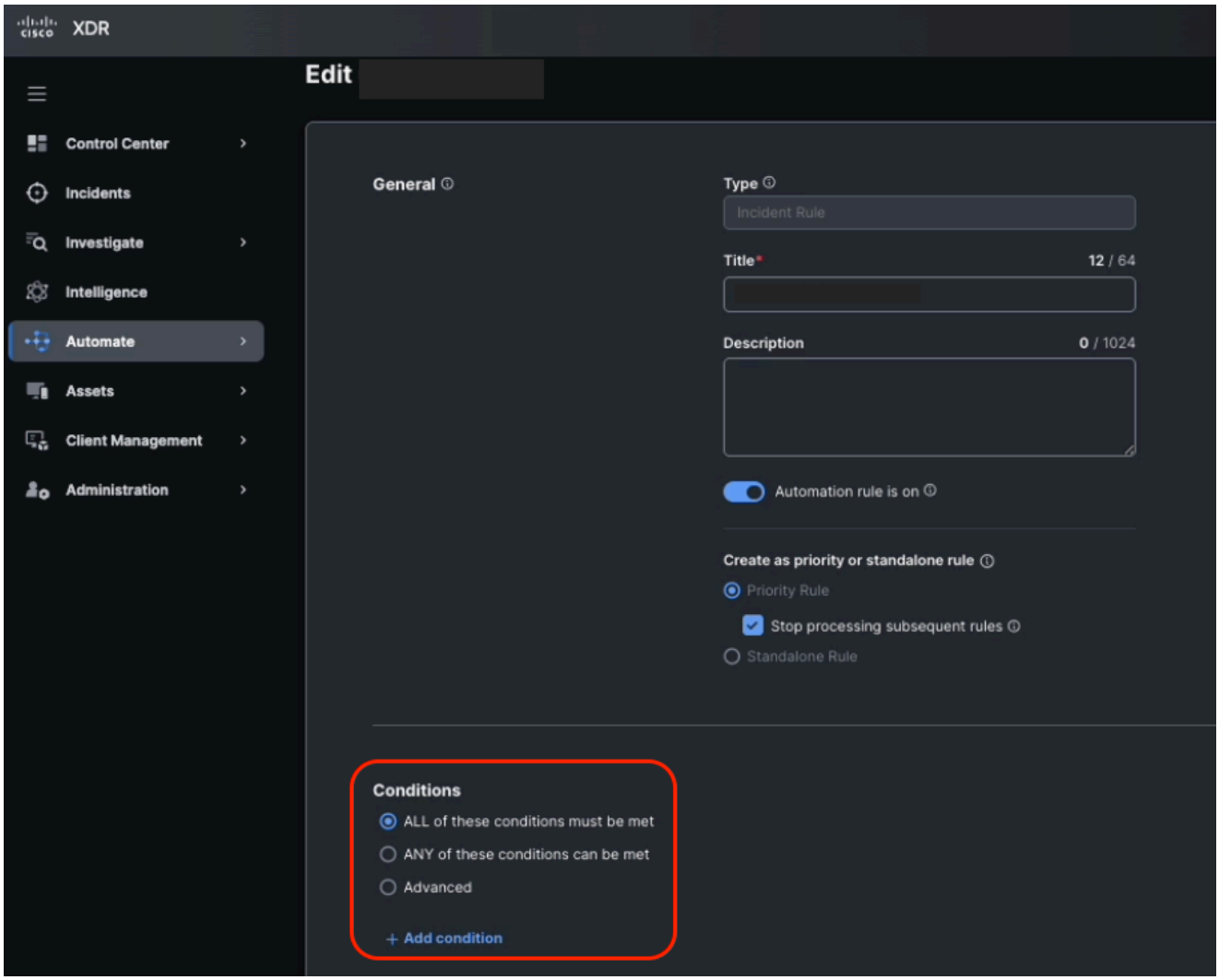
Una regla de automatización es una configuración que define cuándo debe ejecutarse un flujo de trabajo, basándose en eventos específicos o en una programación predefinida. Estas reglas pueden incluir condiciones opcionales y, si se cumplen dichas condiciones, los flujos de trabajo asociados se desencadenan automáticamente.

Paso 4.1: Configurar una regla de automatización

1. Vaya a la sección Automatización > Desencadenadores.
2. Cree una nueva regla. Haga clic en Agregar regla de automatización y asigne un nombre.

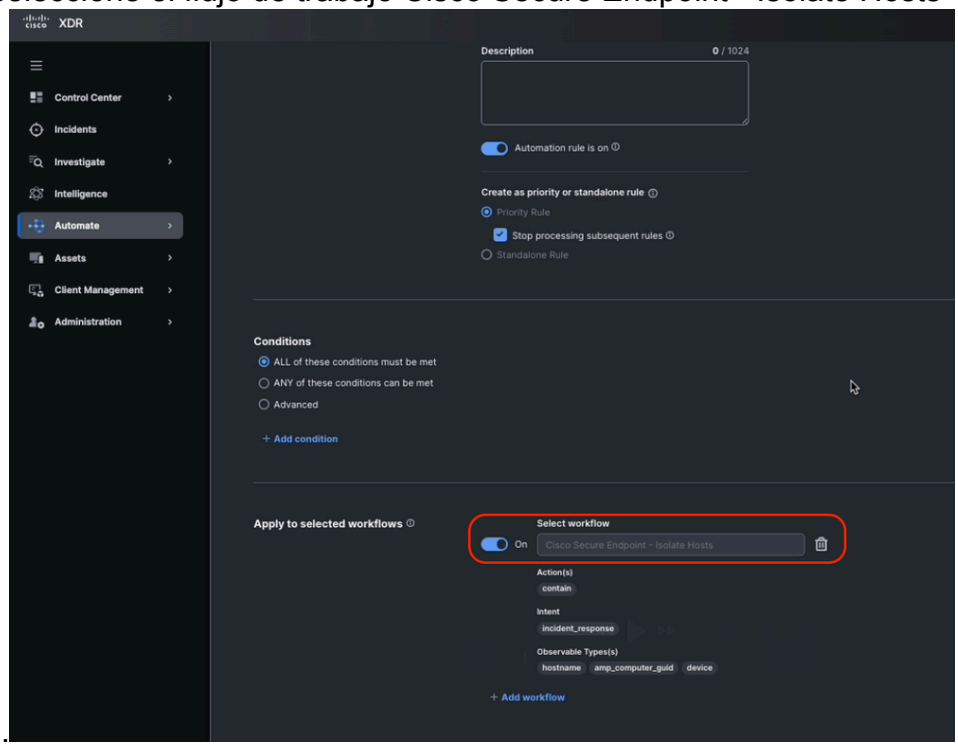
Agregar regla de automatización desde desencadenadores

3. Establezca las condiciones de activación. Puede dejar las condiciones en blanco para asegurarse de que cualquier incidente active esta regla. Personalice la condición si es necesario.



Condiciones de regla de automatización

4. En la acción de la regla, seleccione el flujo de trabajo Cisco Secure Endpoint - Isolate Hosts que instaló anteriormente.



Asignar la regla de automatización al flujo de trabajo

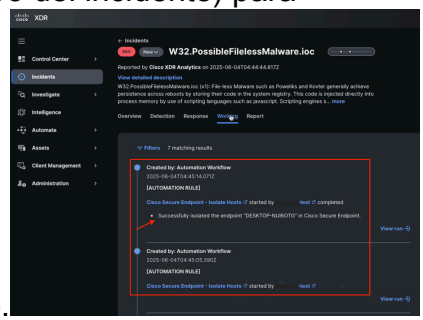
5. Click Save.

Validar funcionalidad de flujo de trabajo

Paso 5.1: Verificar ejecución del flujo de trabajo

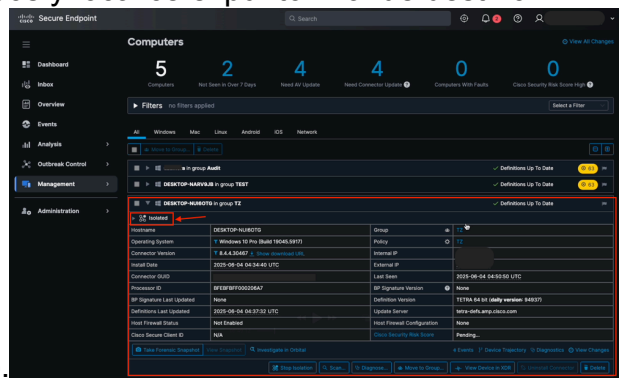
1. Generar o esperar un incidente que cumpla las condiciones de la regla. 

   Se ha detectado un nuevo incidente en Cisco XDR

2. Una vez creado el incidente, compruebe la ficha Worklog (dentro del incidente) para confirmar que el flujo de trabajo se ha ejecutado correctamente. 

   Información de la ficha Incident Worklog

Paso 5.2: Confirmar aislamiento de terminales

1. Inicie sesión en el portal de Cisco Secure Endpoint.
2. Navegue hasta la sección Administración > Equipos y localice el punto final de destino.
3. Confirme que el estado del dispositivo es Aislado. 

   Estado de aislamiento de equipos de terminales seguros

4. Si el terminal no está aislado, revise los registros y la configuración del flujo de trabajo para identificar posibles problemas.

Problema común

La función de aislamiento no está habilitada desde Cisco Secure Endpoint

1. En Cisco XDR, desplácese hasta Incidentes, localice el último incidente y desplácese hasta Registro de trabajo.

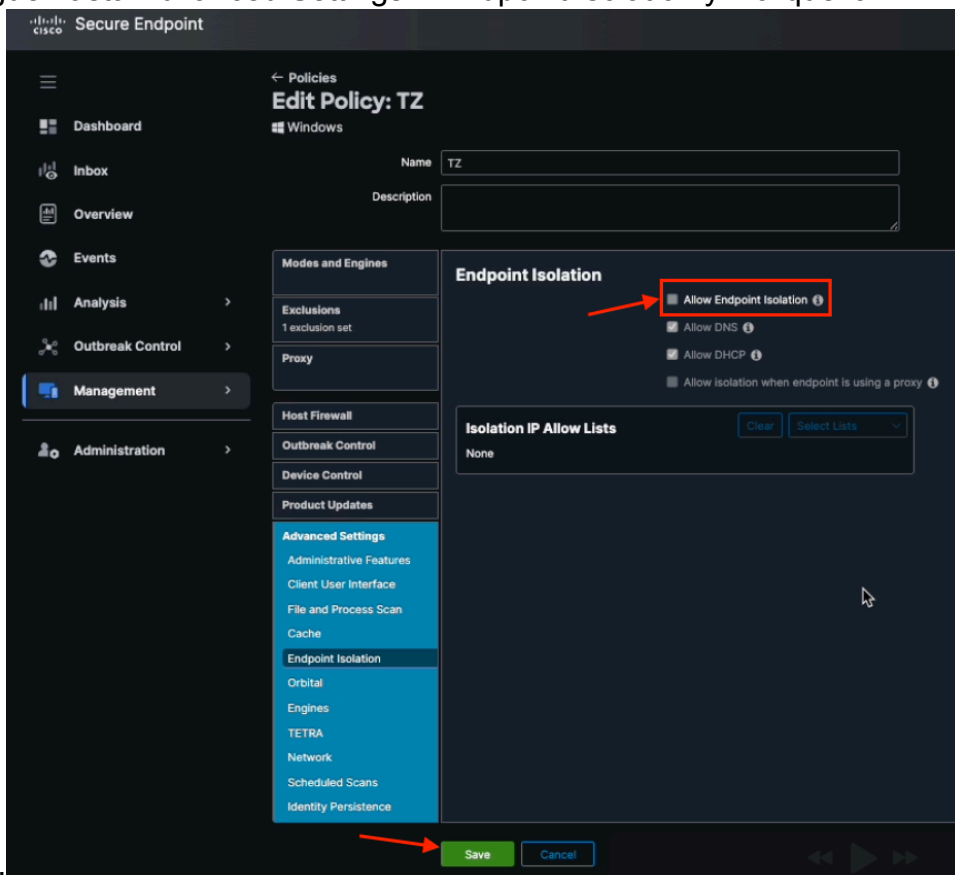
2. Compruebe si hay algún error relacionado después de ejecutar el flujo de trabajo de automatización.

Por ejemplo, el aislamiento de terminales no permitía aislar el host debido a que el aislamiento de terminales no estaba habilitado en la directiva de terminales seguros.

Resultados del flujo de trabajo de automatización del registro de incidentes

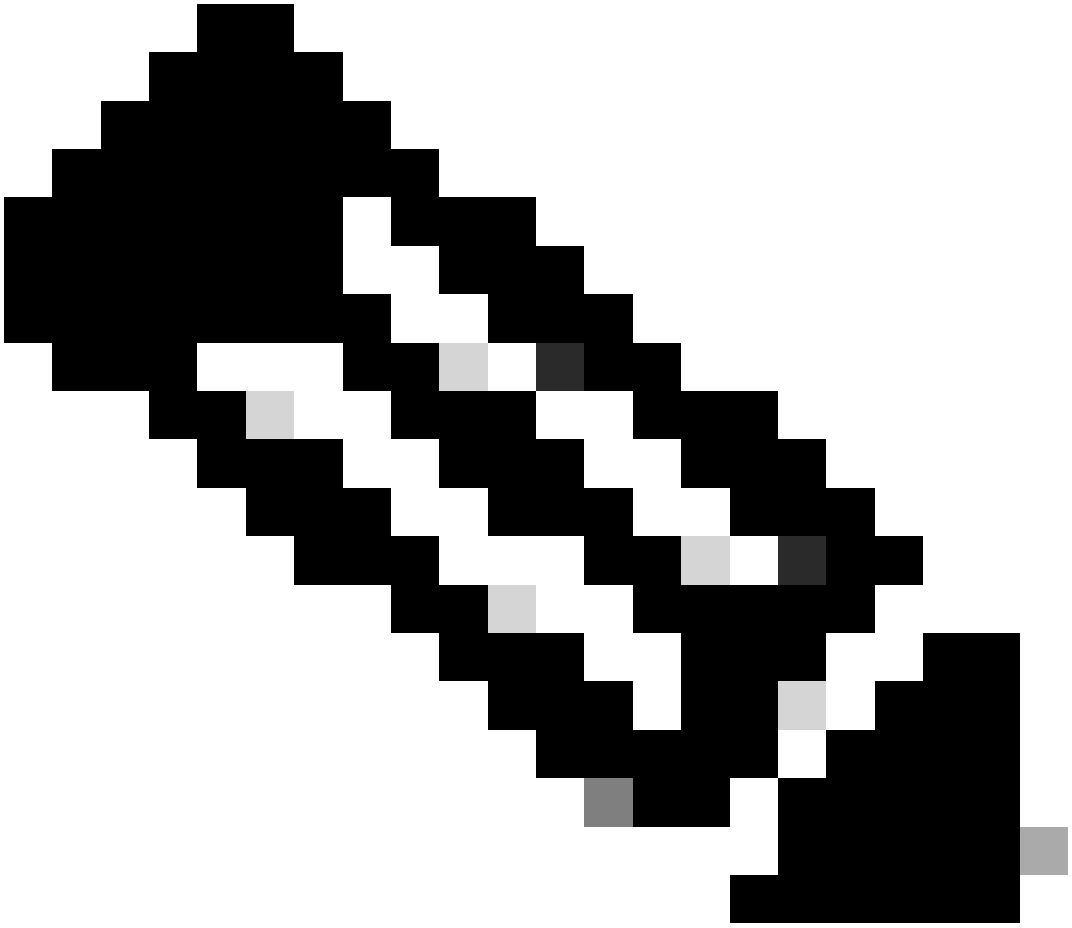
3. Desde Secure Endpoint, navegue hasta Management > Policies y seleccione la política en cuestión.

4. Una vez en la política, navegue hasta Advanced Settings > Endpoint Isolation y marque la casilla Allow Endpoint Isolation.

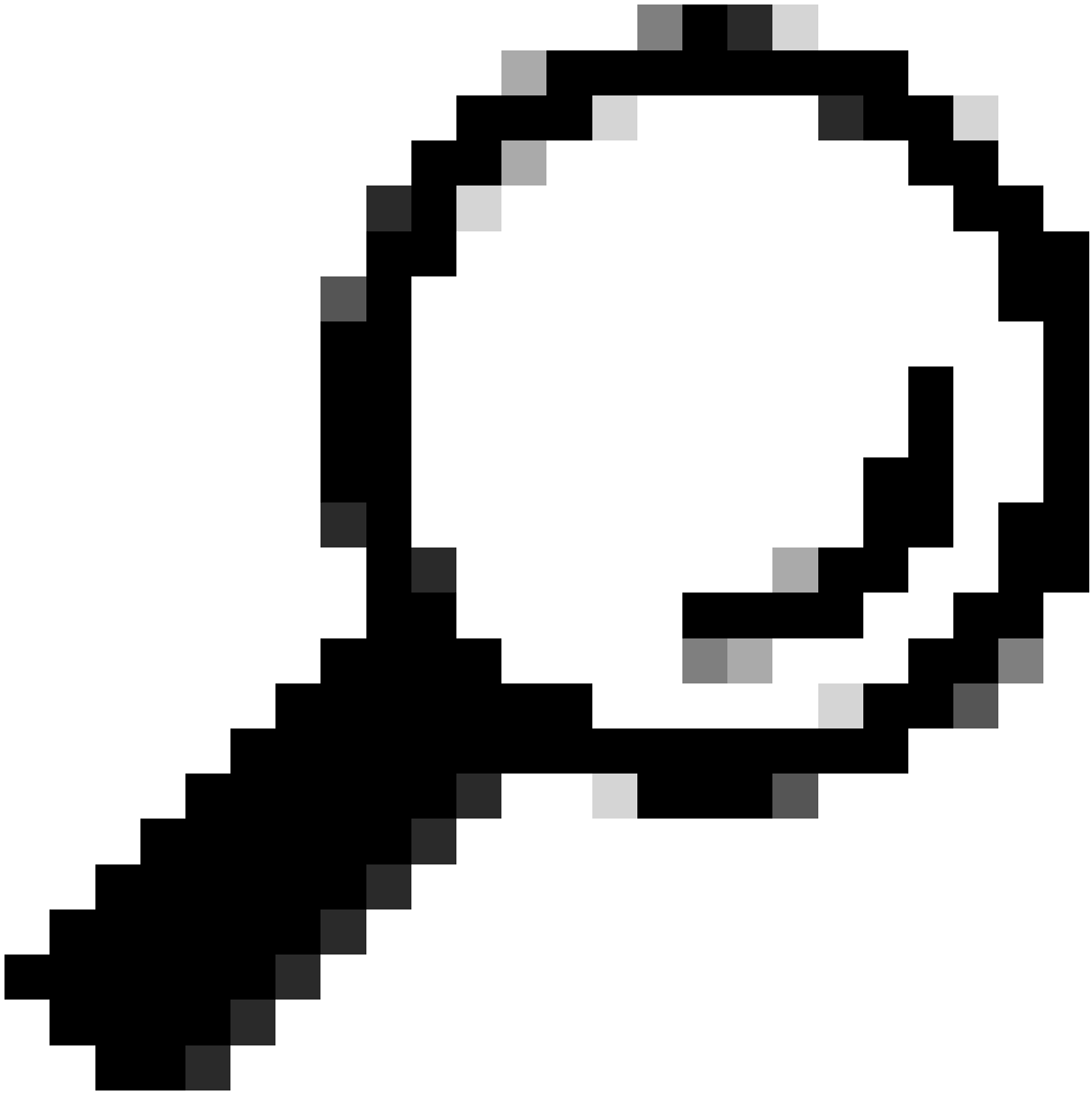


Casilla de verificación Permitir aislamiento de terminales en directiva de terminales seguros

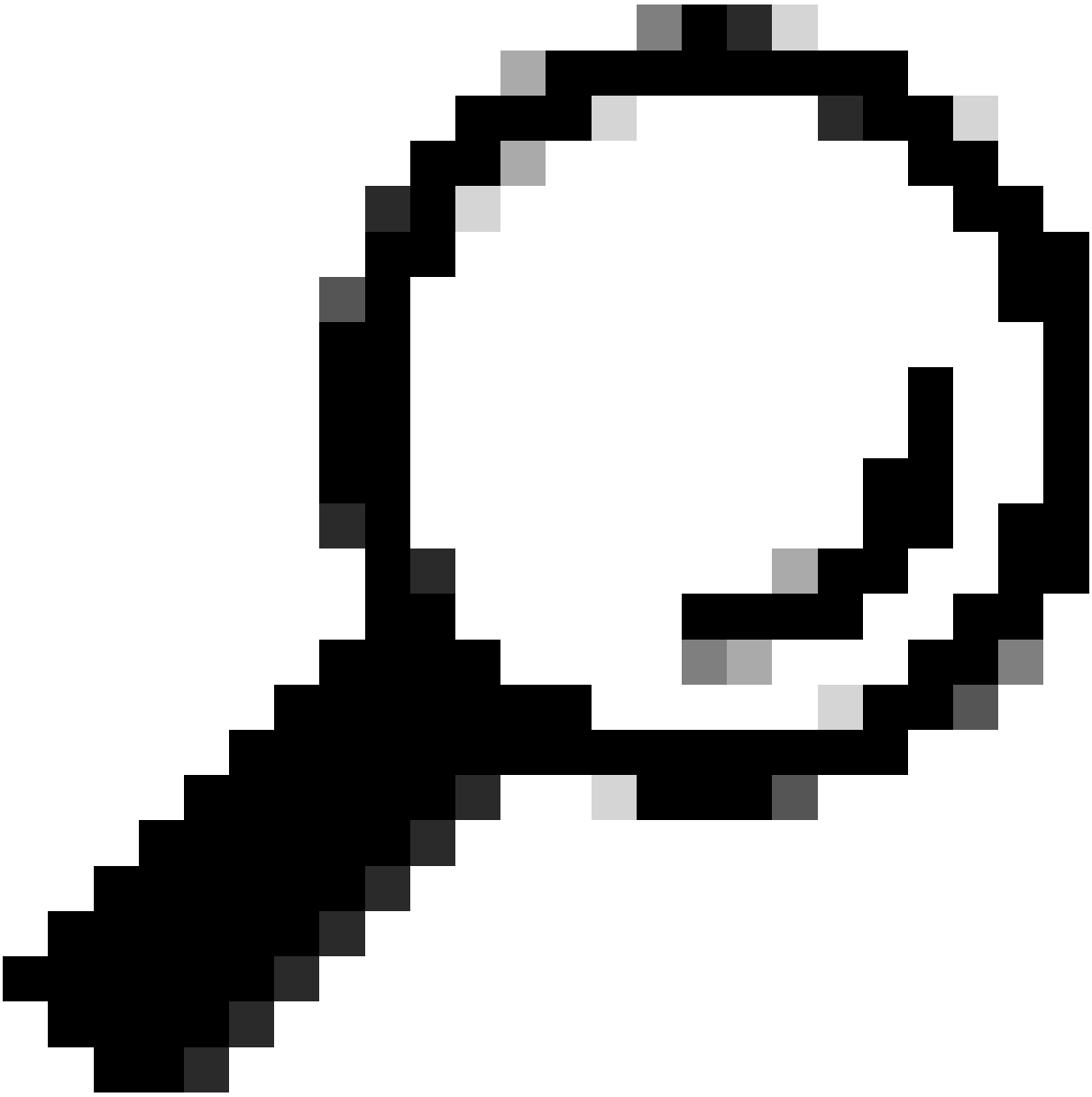
5. Haga clic en Guardar.



Nota: asegúrese de que dispone de los permisos administrativos necesarios para configurar la integración y el flujo de trabajo.



Consejo: Pruebe la configuración en un entorno controlado antes de implementar la automatización en producción.



Consejo: Documentar los ajustes personalizados realizados en el flujo de trabajo o la regla de automatización.

Una vez realizados estos pasos, se configura y activa correctamente un flujo de trabajo que aísla automáticamente un terminal después de crear un incidente y garantiza una respuesta rápida y eficaz a las amenazas de seguridad.

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).