Configurar o fluxo de trabalho automatizado de isolamento de endpoint com o Cisco XDR

Contents

Introdução

Este documento descreve como criar um fluxo de trabalho de automação para isolar um endpoint para um novo incidente.

Pré-requisitos

Requisitos

Não existem requisitos específicos para este documento.

Componentes Utilizados

Este documento não se restringe a versões de software e hardware específicas.

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma

configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Configurar

Este guia detalha as etapas necessárias para configurar e ativar um fluxo de trabalho para isolar automaticamente um endpoint quando ocorrer um incidente. A integração é realizada com o Cisco Secure Endpoint e a funcionalidade de automação de fluxo de trabalho. As etapas são descritas a seguir.

Configuração inicial no Cisco Secure Endpoint

Passo 1.1: Ativar o recurso de isolamento na política

1. Faça login no portal Cisco Secure Endpoint.
2. Navegue até a seção Gerenciamento > Políticas.
3. Selecione a política que se aplica ao ponto de extremidade que você deseja isolar.
4. Verifique se a opção Isolamento de dispositivo está habilitada nas configurações de política.

   Permitir Isolamento de Ponto de Extremidade da Política de Ponto de Extremidade Segura

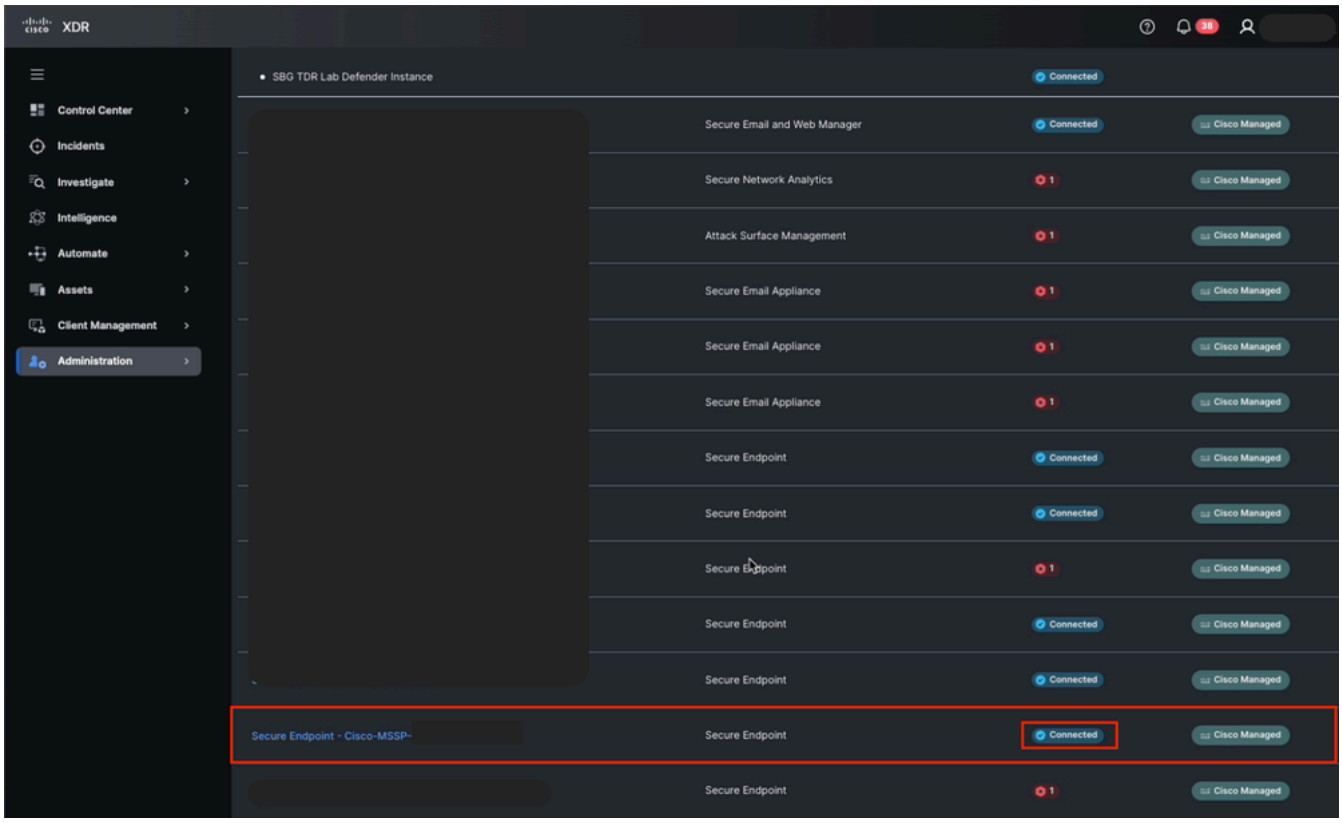
5. Salve as alterações e distribua a diretiva, se necessário.

Valide a integração com o Cisco Secure Endpoint

Passo 2.1: Verificar a integração

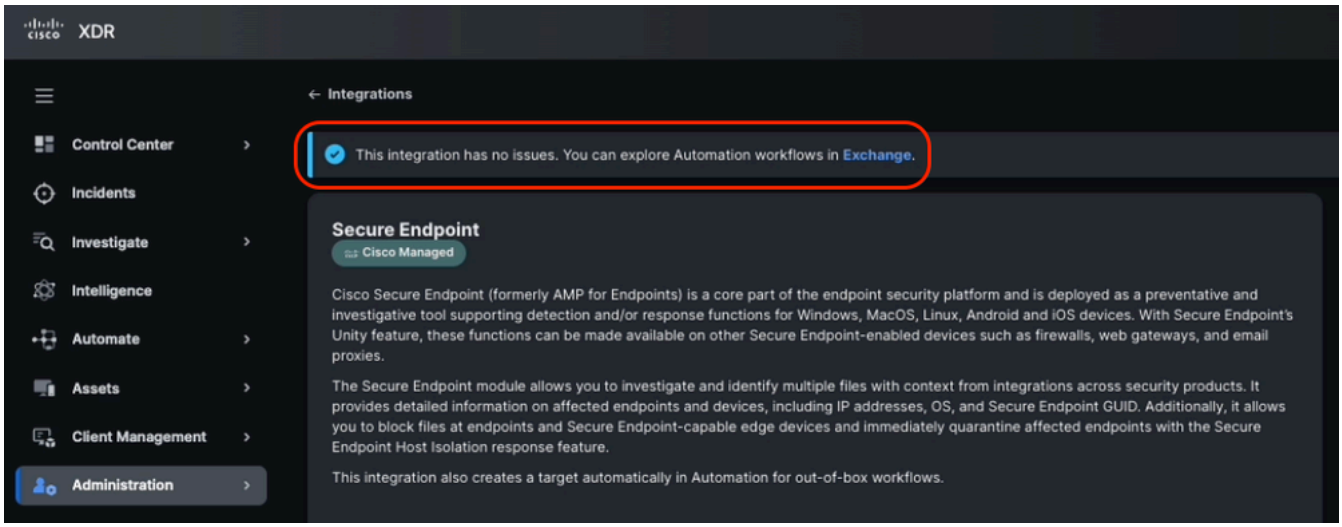
1. Faça login no Cisco XDR.
2. Navegue até a seção Administração > Integrações > Minhas integrações.
3. Verifique se a integração com o Cisco Secure Endpoint está configurada corretamente:

   Verifique o status da integração em Conectado.



Status de integração de endpoint seguro do Cisco XDR

Confirme se não há erros na configuração da API.

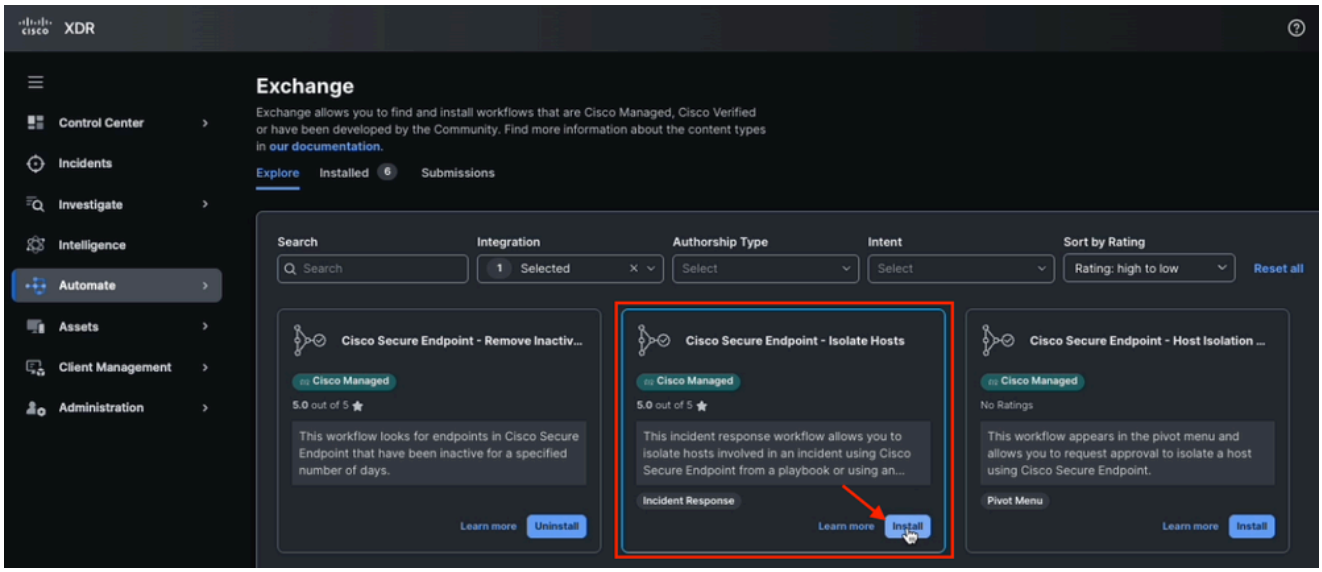


Verificação de integridade da integração do Secure Endpoint

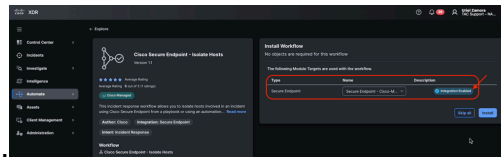
Instalar o fluxo de trabalho do Cisco XDR Exchange

Passo 3.1: Instalar o Fluxo de Trabalho de Isolamento de Ponto de Extremidade

1. Faça login no Cisco XDR e navegue até Automate > Exchange.
2. Procure o fluxo de trabalho chamado Cisco Secure Endpoint - Isolate Hosts e clique em Install.



Isolar Fluxo de Trabalho de Host do Exchange

3. Verifique se o destino está disponível antes da instalação. 

Destino do Módulo Habilitado no Fluxo de Trabalho

4. Instale o fluxo de trabalho em seu sistema de automação.

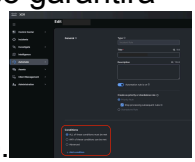
Criar uma Regra de Automação

Uma regra de automação é uma configuração que define quando um fluxo de trabalho deve ser executado, com base em eventos específicos ou em uma agenda predefinida. Essas regras podem incluir condições opcionais e, se essas condições forem atendidas, os fluxos de trabalho associados serão acionados automaticamente.

Passo 4.1: Configurar uma regra de automação

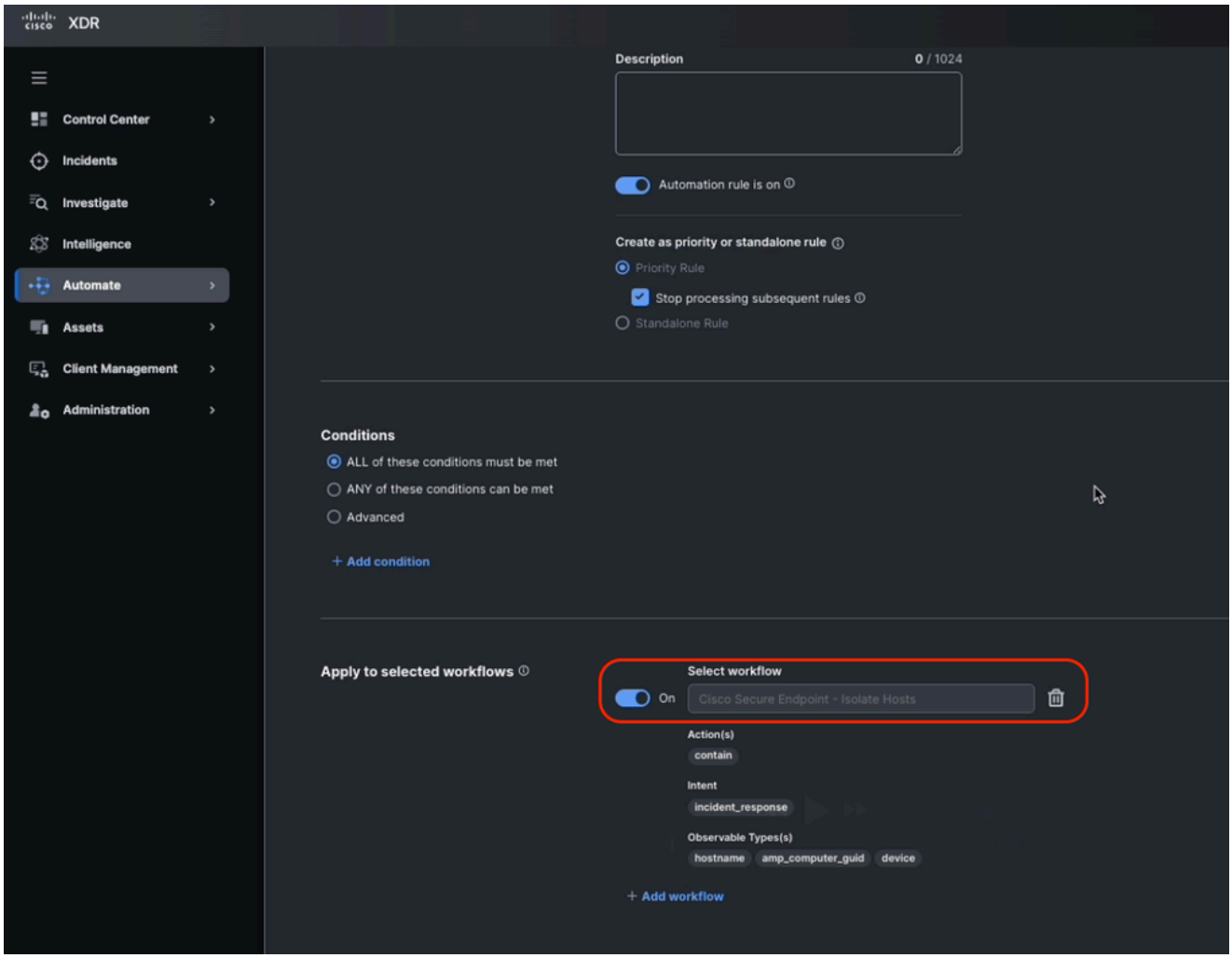
1. Navegue até a seção Automação > Triggers.
2. Crie uma nova regra. Clique em Adicionar regra de automação e atribua um nome. 

Adicionar Regra de Automação de Gatilhos

3. Defina as condições de disparo. Você pode deixar as condições em branco, isso garantirá que qualquer incidente ative essa regra. Personalize a condição, se necessário. 

Condições da regra de automação

4. Na ação da regra, selecione o fluxo de trabalho Cisco Secure Endpoint - Isolate Hosts instalado anteriormente.

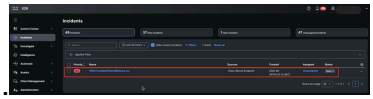


Atribuir a Regra de Automação ao Fluxo de Trabalho

5. Click Save.

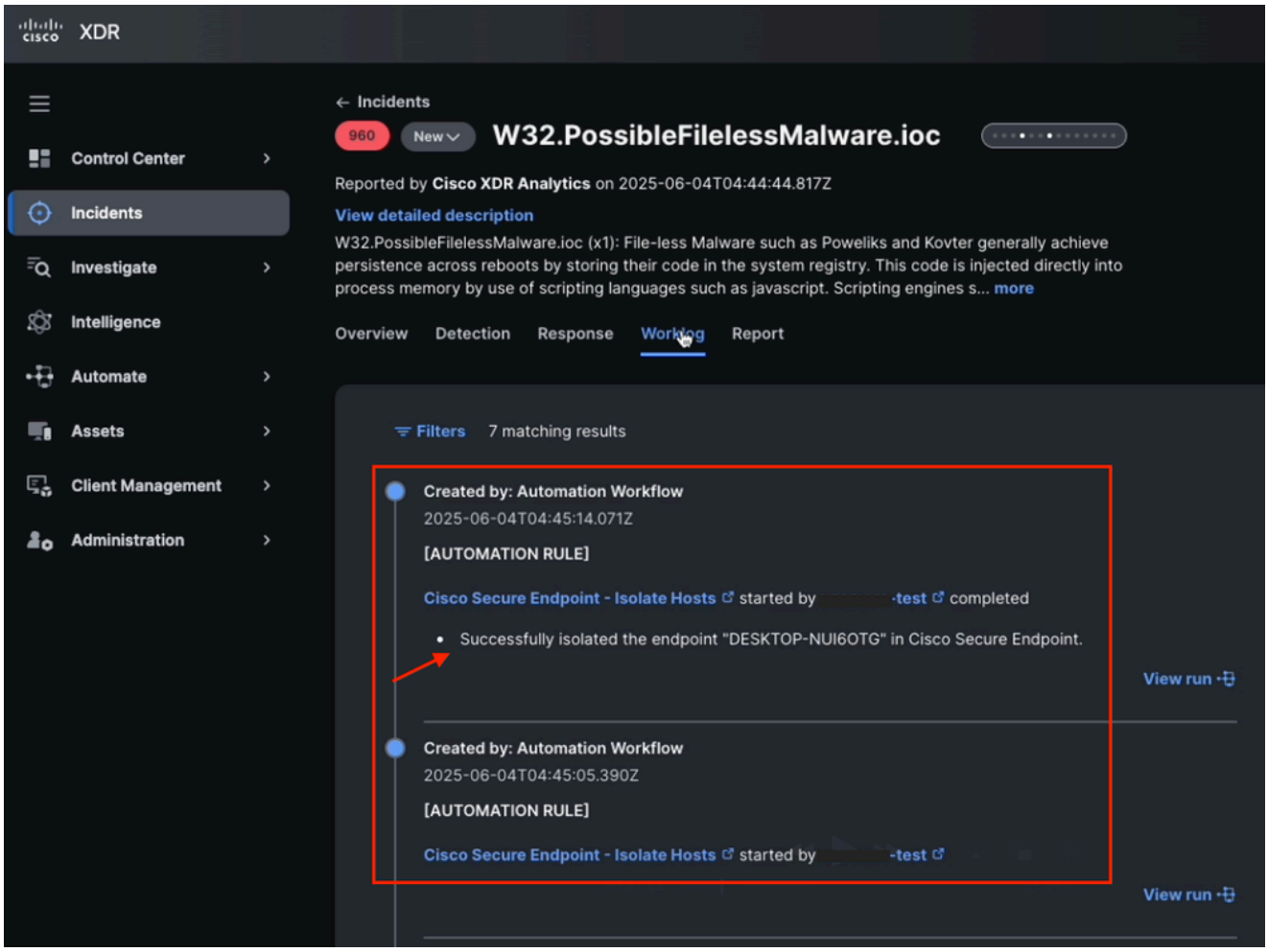
Validar Funcionalidade do Fluxo de Trabalho

Passo 5.1: Verificar Execução do Fluxo de Trabalho

1. Gerar ou aguardar um incidente que atenda às condições da regra. 

   Novo incidente detectado no Cisco XDR

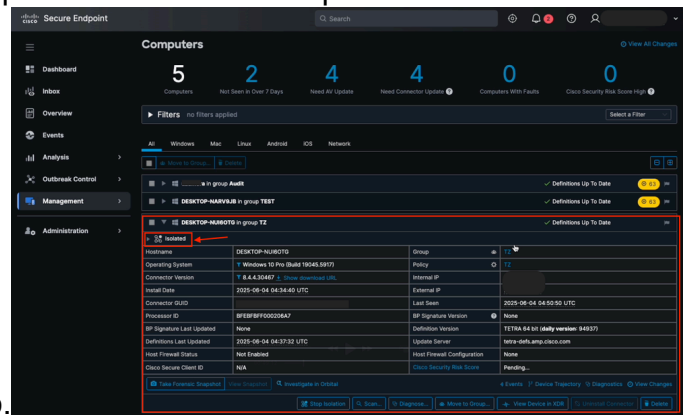
2. Depois que o incidente for criado, verifique a guia Log de Trabalho (no incidente) para confirmar se o fluxo de trabalho foi executado com êxito.



Informações da guia Registro de trabalho do incidente

Passo 5.2: Confirmar Isolamento de Ponto de Extremidade

1. Faça login no portal Cisco Secure Endpoint.
2. Navegue até a seção Gerenciamento > Computadores e localize o ponto final de destino.
3. Confirme se o status do dispositivo é Isolado.



Status de isolamento de computadores de endpoint seguros

4. Se o endpoint não estiver isolado, revise os logs e a configuração do fluxo de trabalho para identificar possíveis problemas.

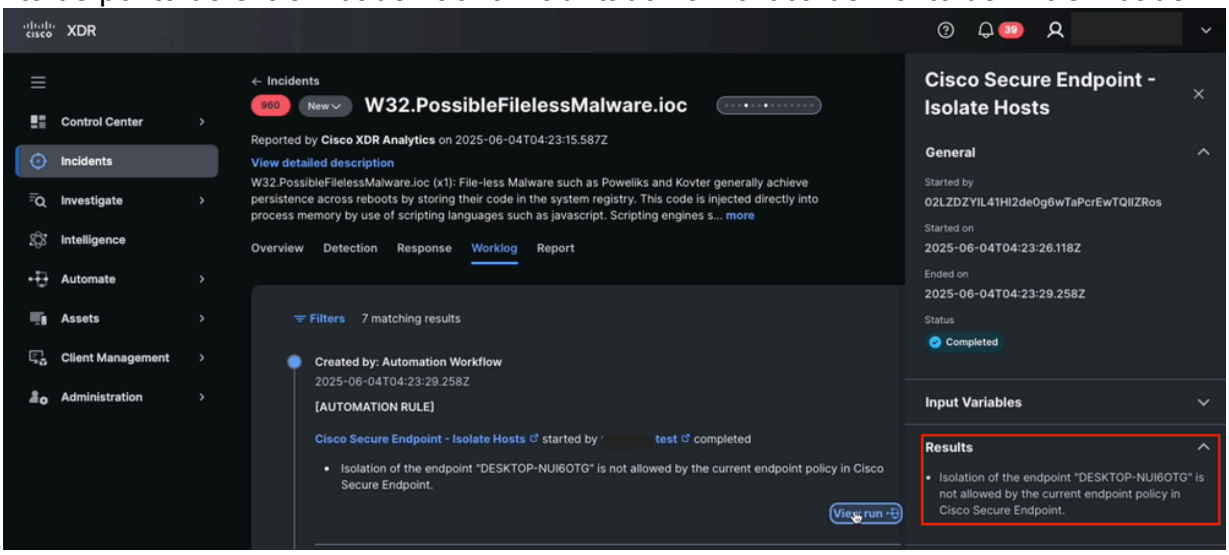
Problema comum

O recurso de isolamento não está habilitado no Cisco Secure Endpoint

1. No Cisco XDR, navegue até Incident, localize o último incidente e vá até Worklog.

2. Verifique se há algum erro relacionado após a execução do fluxo de trabalho de automação.

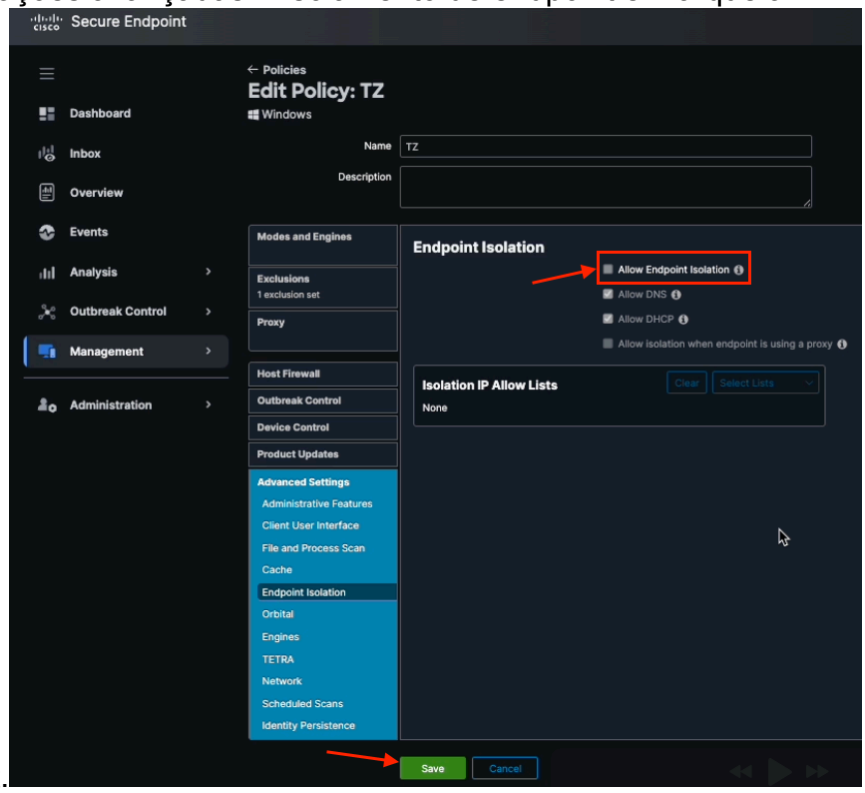
Por exemplo, o isolamento de ponto de extremidade não permitiu isolar o host porque o isolamento de ponto de extremidade não foi habilitado na Política de Ponto de Extremidade Seguro.



Resultados do Fluxo de Trabalho de Automação do Log de Trabalho de Incidentes

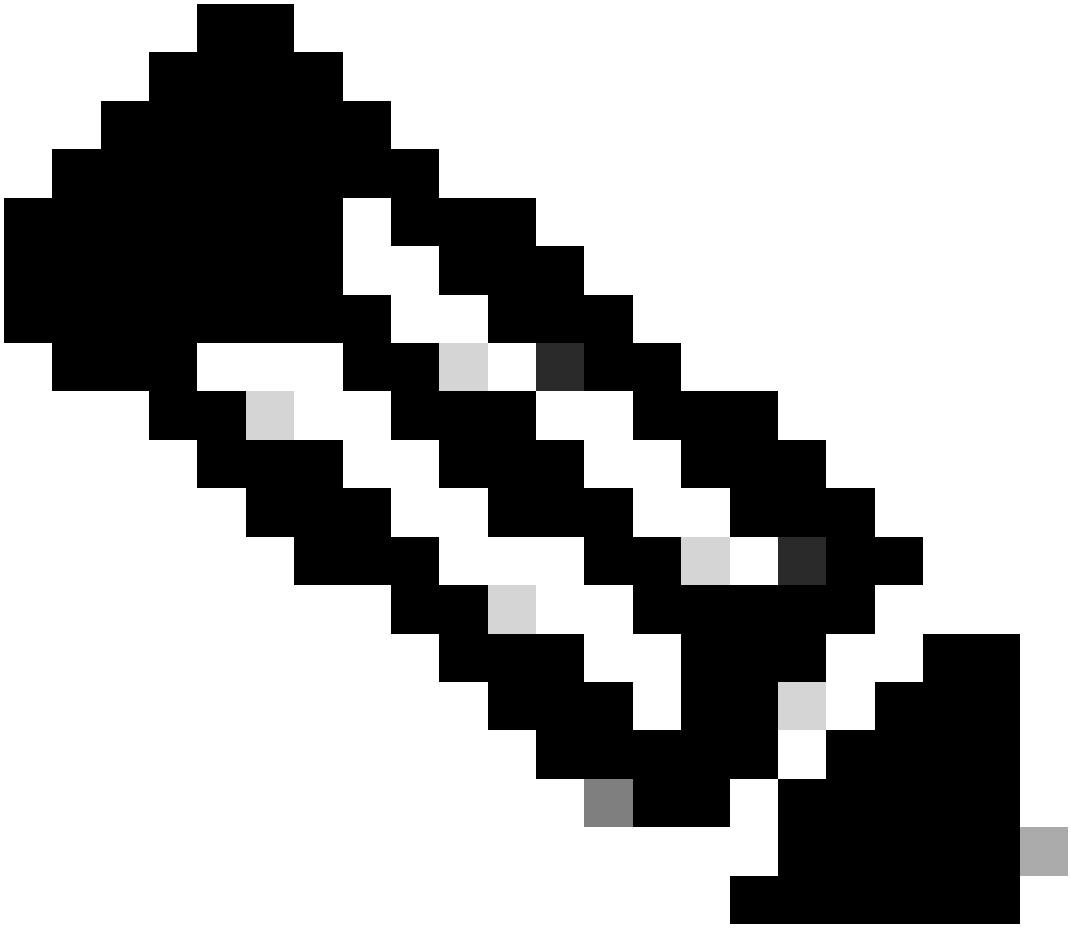
3. Em Ponto Final Seguro, navegue para Gerenciamento > Políticas e selecione a Política em questão.

4. Na política, navegue para Configurações avançadas > Isolamento de endpoint e marque a caixa Permitir isolamento de endpoint.

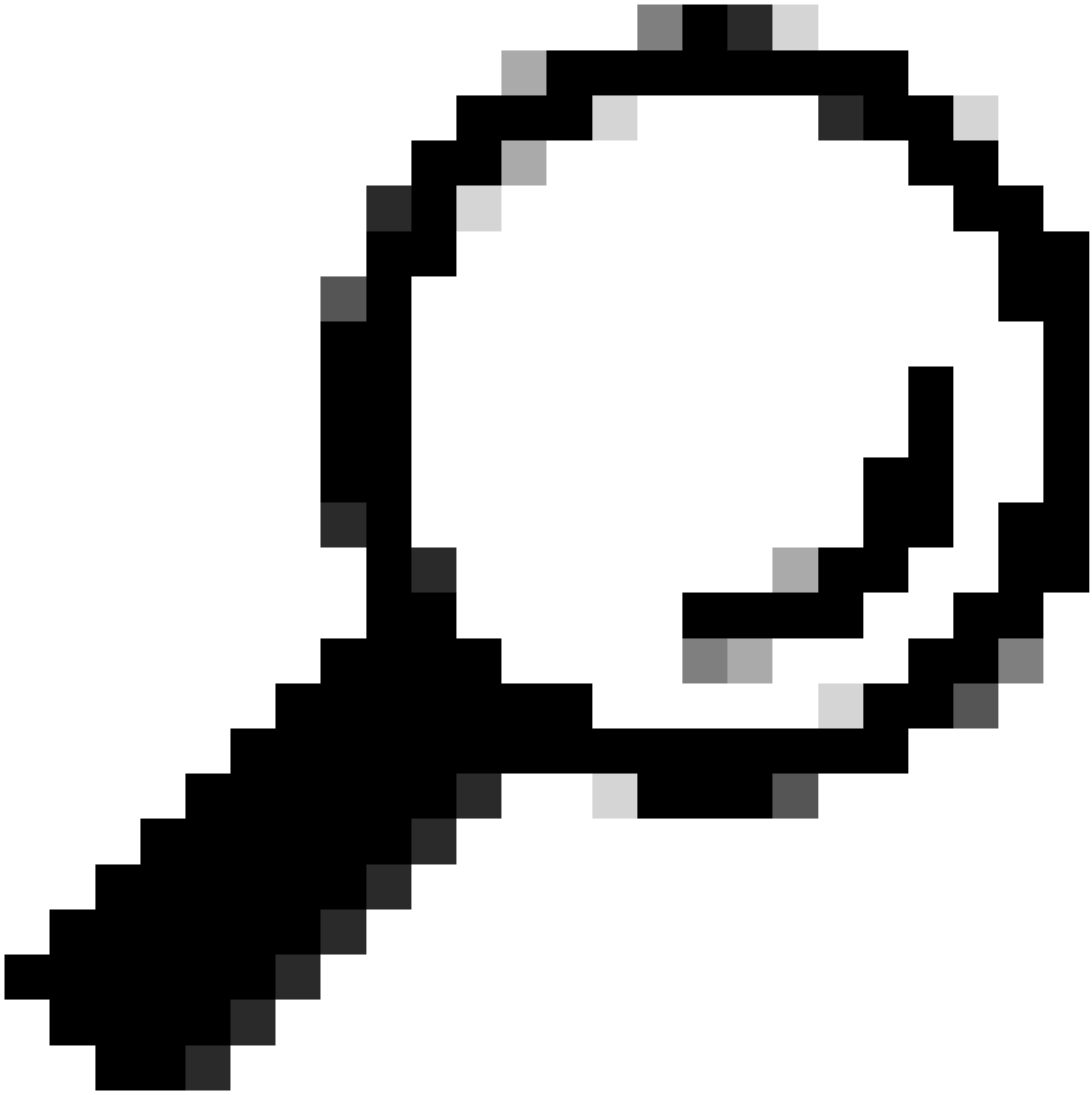


Caixa de Seleção Permitir Isolamento de Ponto de Extremidade na Política de Ponto de Extremidade Segura

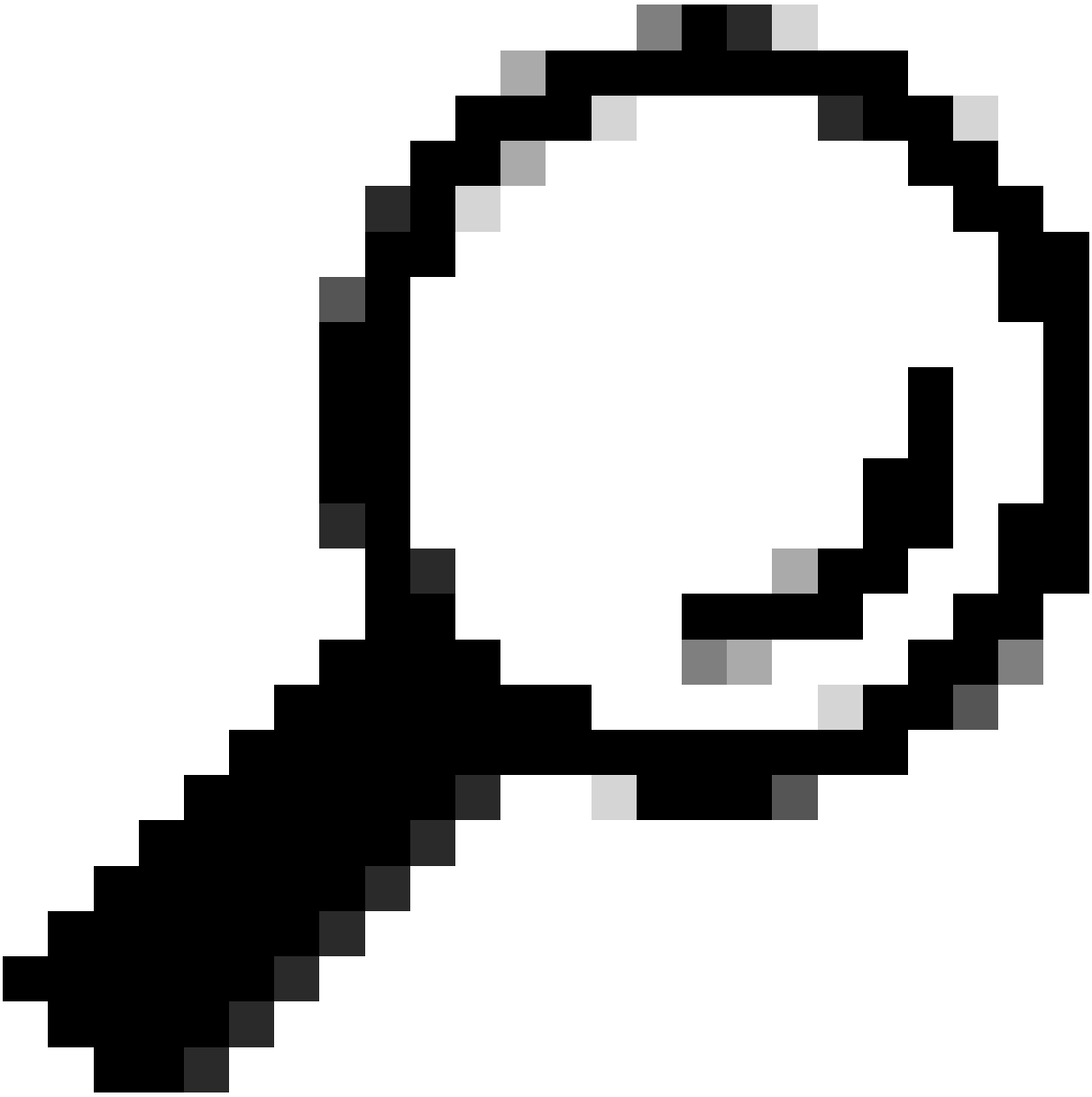
5. Clique em Salvar.



Observação: verifique se você tem as permissões administrativas necessárias para configurar a integração e o fluxo de trabalho.



Tip: Teste a configuração em um ambiente controlado antes de implantar a automação na produção.



Tip: Documente todos os ajustes personalizados feitos na regra de automação ou fluxo de trabalho.

Depois que essas etapas são executadas, você configura e ativa com êxito um fluxo de trabalho que isola automaticamente um endpoint após a criação de um incidente e garante uma resposta rápida e eficaz às ameaças à segurança.

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.