Geautomatiseerde workflow voor endpointisolatie configureren met Cisco XDR

Inhoud

Inleiding

In dit document wordt beschreven hoe u een automatiseringsworkflow kunt maken om een eindpunt voor een nieuw incident te isoleren.

Voorwaarden

Vereisten

Er zijn geen specifieke vereisten van toepassing op dit document.

Gebruikte componenten

Dit document is niet beperkt tot specifieke software- en hardware-versies.

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een

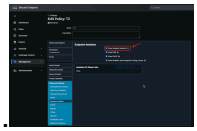
opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

Configureren

In deze handleiding worden de stappen beschreven die nodig zijn voor het configureren en activeren van een werkstroom om een eindpunt automatisch te isoleren wanneer zich een incident voordoet. De integratie wordt uitgevoerd met Cisco Secure Endpoint en de functionaliteit voor workflowautomatisering. De stappen worden als volgt beschreven.

Eerste configuratie in Cisco Secure Endpoint

Stap 1.1: Schakel de isolatiefunctie in het beleid in

1. Meld u aan bij het Cisco Secure Endpoint-portaal.
2. Navigeer naar de sectie Beheer > Beleid.
3. Selecteer het beleid dat geldt voor het eindpunt dat u wilt isoleren.
4. Controleer of de optie Apparaatisolatie is ingeschakeld in de beleidsinstellingen. 

   Endpoint-isolatie toestaan vanuit beveiligd eindpuntbeleid

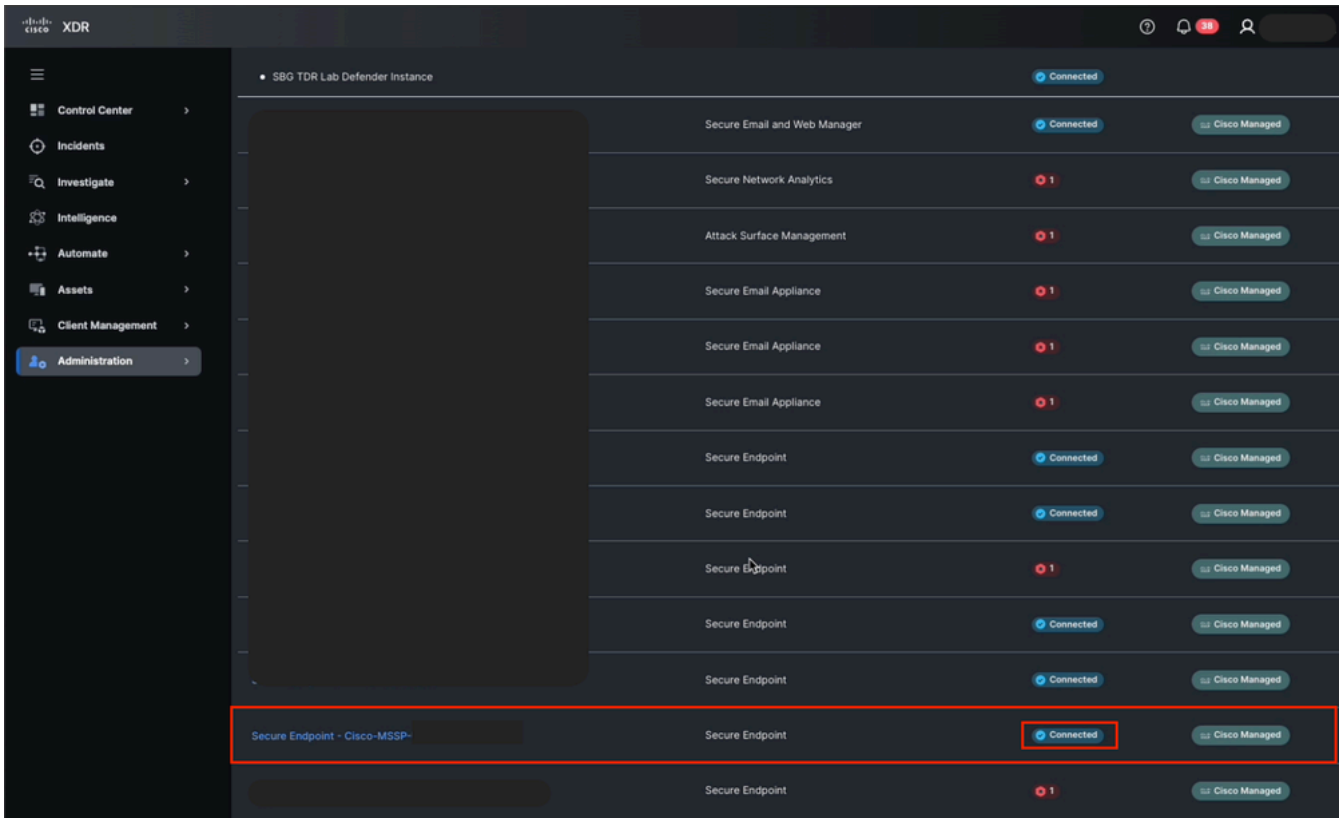
5. Sla de wijzigingen op en verspreid het beleid indien nodig.

De integratie valideren met Cisco Secure Endpoint

Stap 2.1: Controleer de integratie

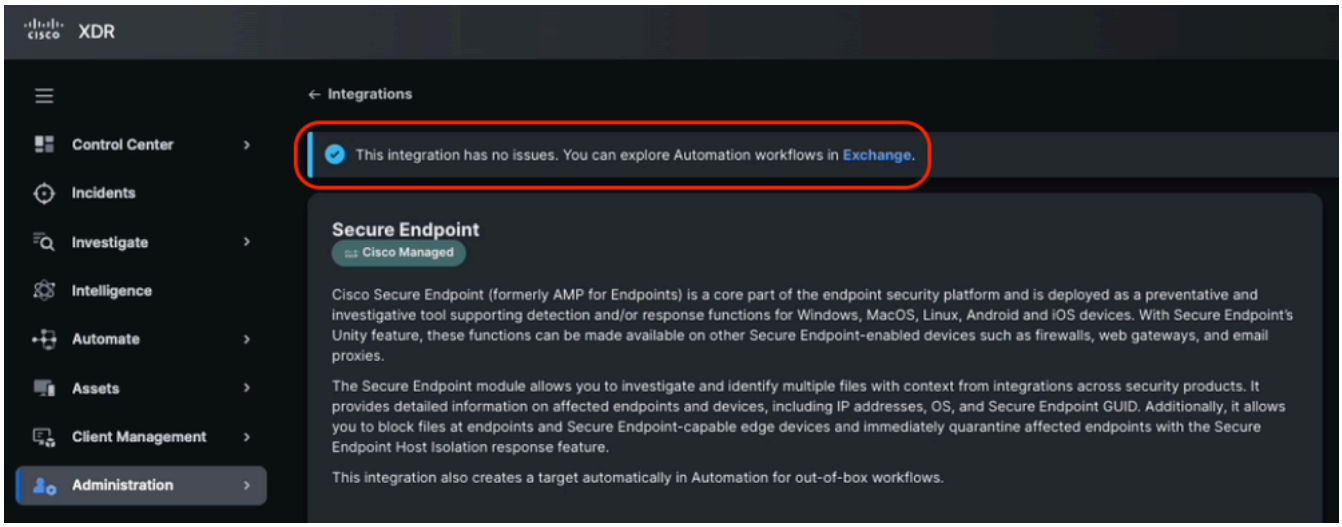
1. Meld u aan bij Cisco XDR
2. Navigeer naar Beheer > Integraties > Mijn integraties.
3. Zorg ervoor dat de integratie met Cisco Secure Endpoint correct is geconfigureerd:

   Controleer de integratiestatus in Connected.



Integratiestatus van beveiligd eindpunt van Cisco XDR

Bevestig dat er geen fouten zijn in de API-configuratie.

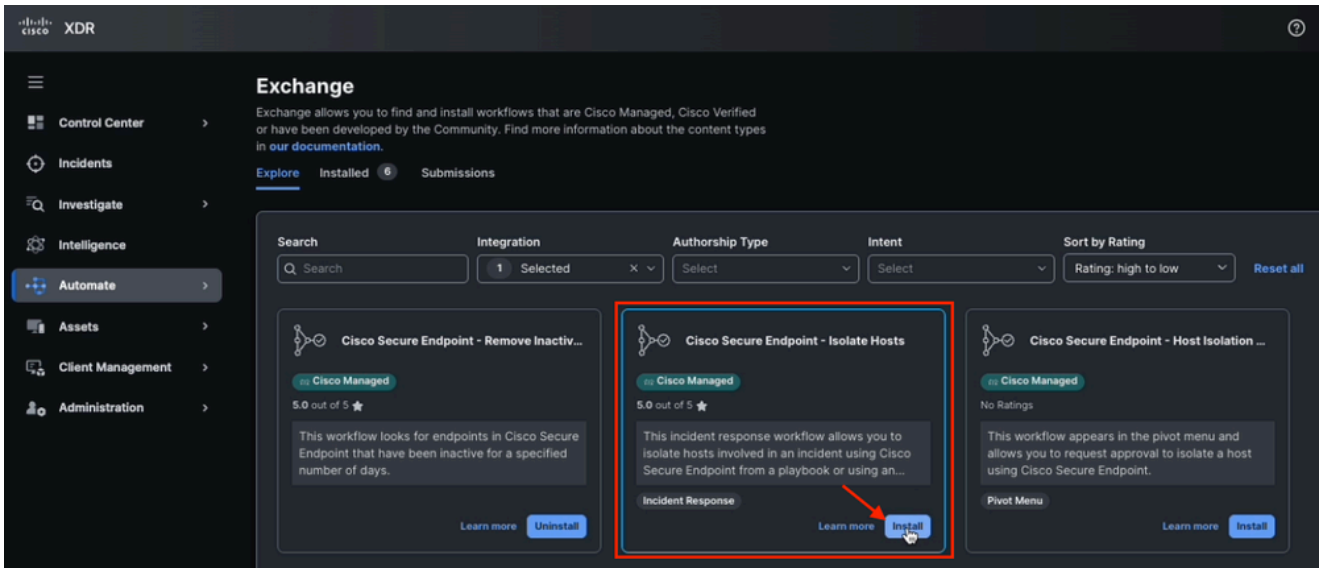


Beveiligde integratiecontrole van het eindpunt

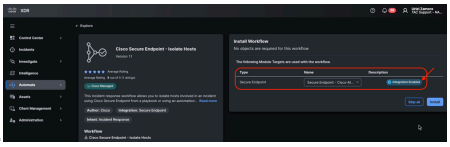
Installeer de werkstroom van Cisco XDR Exchange

Stap 3.1: Installeer de Endpoint Isolation Workflow

1. Meld u aan bij Cisco XDR en navigeer naar Automate > Exchange.
2. Zoek naar de workflow met de naam Cisco Secure Endpoint - Isolate Hosts en klik op Installeren.



Hostworkflow isoleren uit Exchange

3. Controleer of het doel beschikbaar is voordat u het installeert. 

Moduledoel ingeschakeld vanuit werkstroom

4. Installeer de workflow in uw automatiseringssysteem.

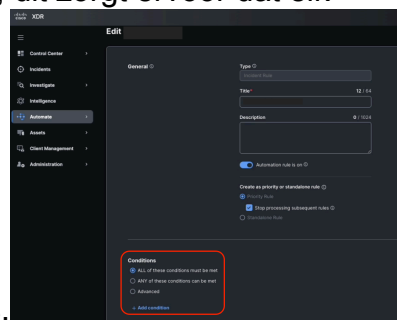
Een automatiseringsregel maken

Een automatiseringsregel is een configuratie die bepaalt wanneer een werkstroom moet worden uitgevoerd, op basis van specifieke gebeurtenissen of een vooraf gedefinieerd schema. Deze regels kunnen optionele voorwaarden bevatten en als aan die voorwaarden wordt voldaan, worden de bijbehorende workflow(s) automatisch geactiveerd.

Stap 4.1: Automatiseringsregel configureren

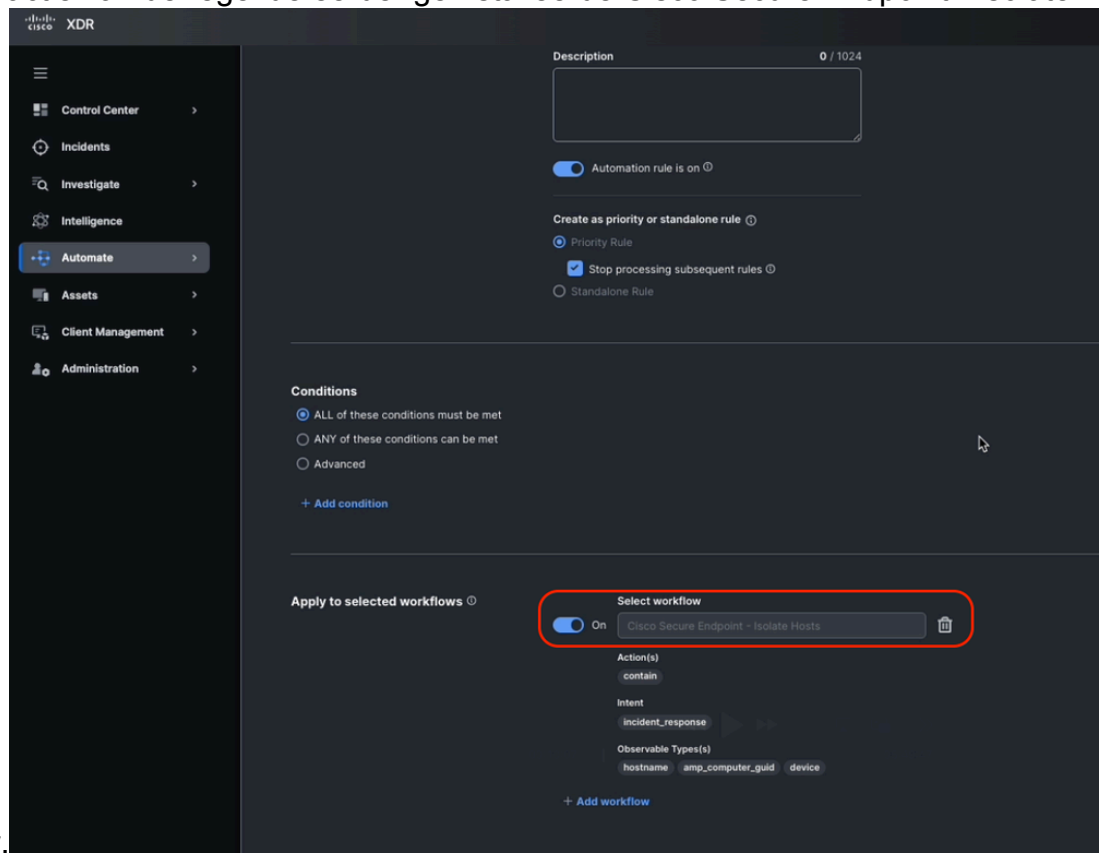
1. Navigeer naar de sectie Automation > Triggers.
2. Maak een nieuwe regel. Klik op Automatiseringsregel toevoegen en geef een naam op. 

Automatiseringsregel van triggers toevoegen

3. Stel de triggervoorwaarden in. U kunt de voorwaarden leeg laten, dit zorgt ervoor dat elk incident deze regel activeert. Pas de conditie aan als dat nodig is. 

Regelvoorwaarden voor automatisering

4. Selecteer in de actie van de regel de eerder geïnstalleerde Cisco Secure Endpoint - Isolate Hosts-workflow.



De automatiseringsregel toewijzen aan de werkstroom

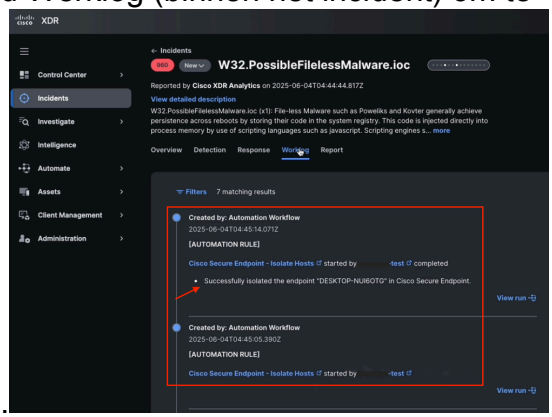
5. Klik op Save (Opslaan).

Werkstroomfunctionaliteit valideren

Stap 5.1: Controleren van de uitvoering van de workflow

1. Genereer of wacht op een incident dat voldoet aan de voorwaarden van de regel. 

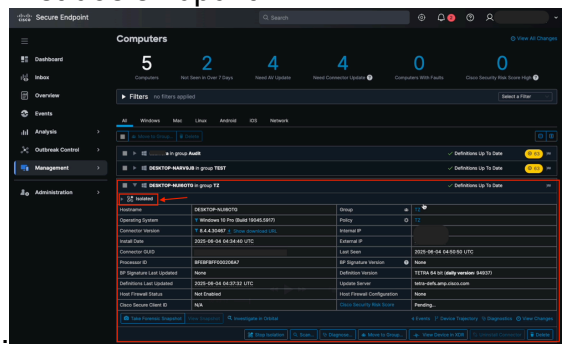
Nieuw incident in Cisco XDR gedetecteerd

2. Nadat het incident is gemaakt, controleert u het tabblad Werklog (binnen het incident) om te bevestigen dat de werkstroom succesvol is uitgevoerd. 

Informatie op het tabblad Werklog voor incidenten

Stap 5.2: Eindpuntisolatie bevestigen

1. Meld u aan bij het Cisco Secure Endpoint-portaal.
2. Navigeer naar de sectie Beheer > Computers en zoek het doeleindpunt.



3. Bevestig dat de status van het apparaat is geïsoleerd.

   Isolatiestatus van beveiligde eindpuntcomputers

4. Als het eindpunt niet geïsoleerd is, bekijkt u de werkstroomlogboeken en de configuratie om mogelijke problemen te identificeren.

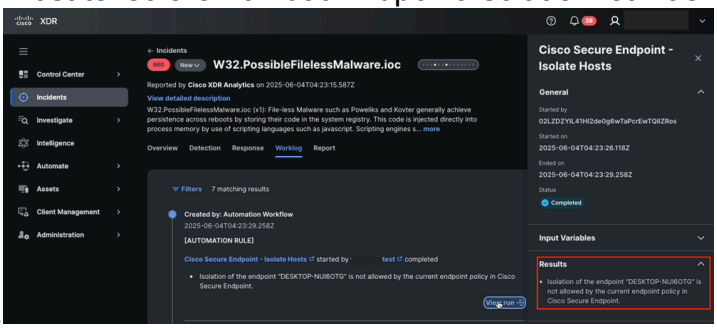
Gemeenschappelijke aangelegenheid

Isolatiefunctie is niet ingeschakeld vanuit Cisco Secure Endpoint

1. Navigeer vanuit Cisco XDR naar Incidenten, zoek het laatste incident en navigeer naar Werklog.

2. Controleer of er een gerelateerde fout is opgetreden na het uitvoeren van de automatiseringsworkflow.

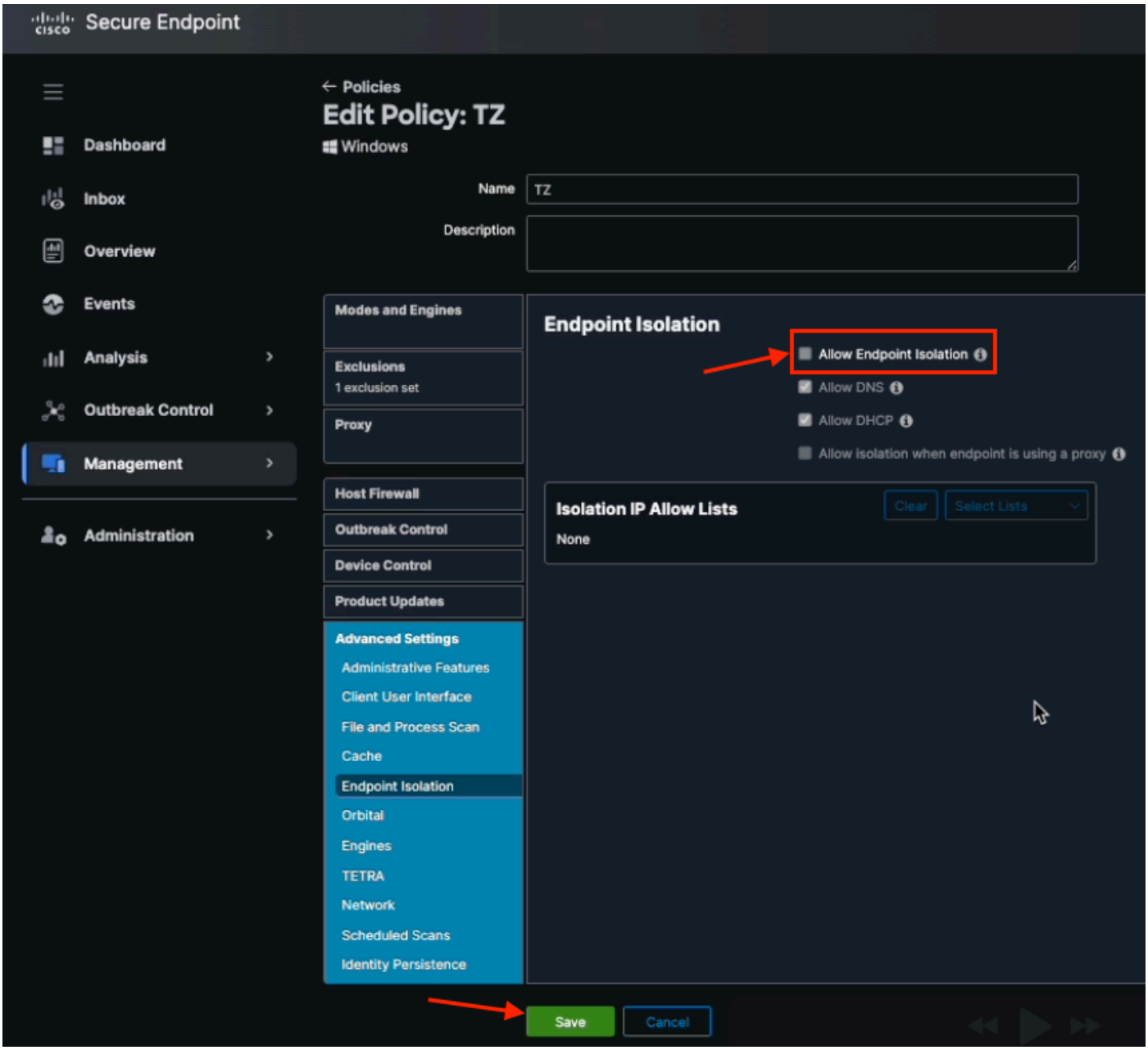
   Endpoint-isolatie liet bijvoorbeeld niet toe de host te isoleren omdat Endpoint-isolatie niet was ingeschakeld in het Secure Endpoint-beleid.



   Werkstroomresultaten voor automatisering van incidentwerklog

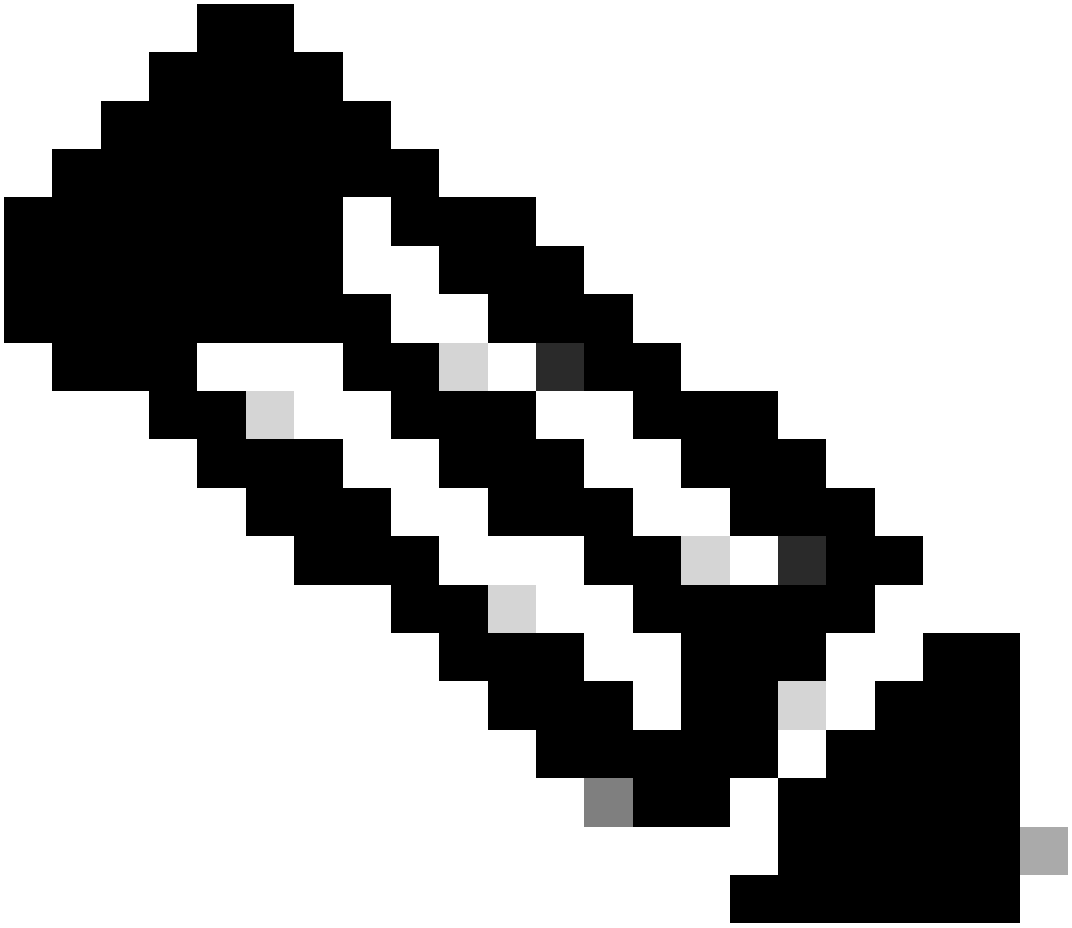
3. Navigeer vanuit Veilig Eindpunt naar Beheer > Beleid om het betreffende Beleid te selecteren.

4. Navigeer in het beleid naar Geavanceerde instellingen > Endpoint Isolation en vink het vakje Endpoint Isolation toestaan aan.

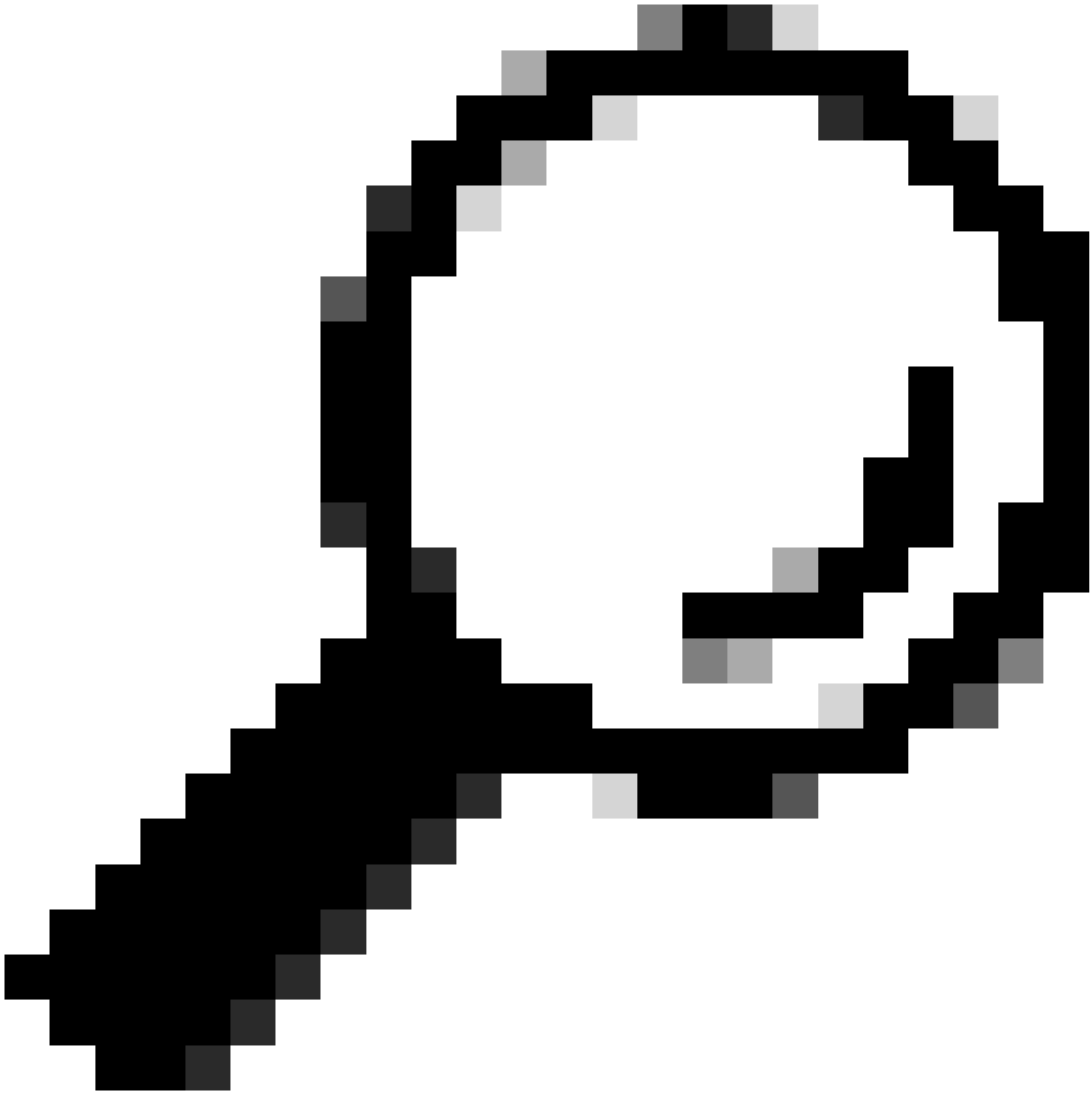


Selectievakje Eindpuntisolatie toestaan in Veilig eindpuntbeleid

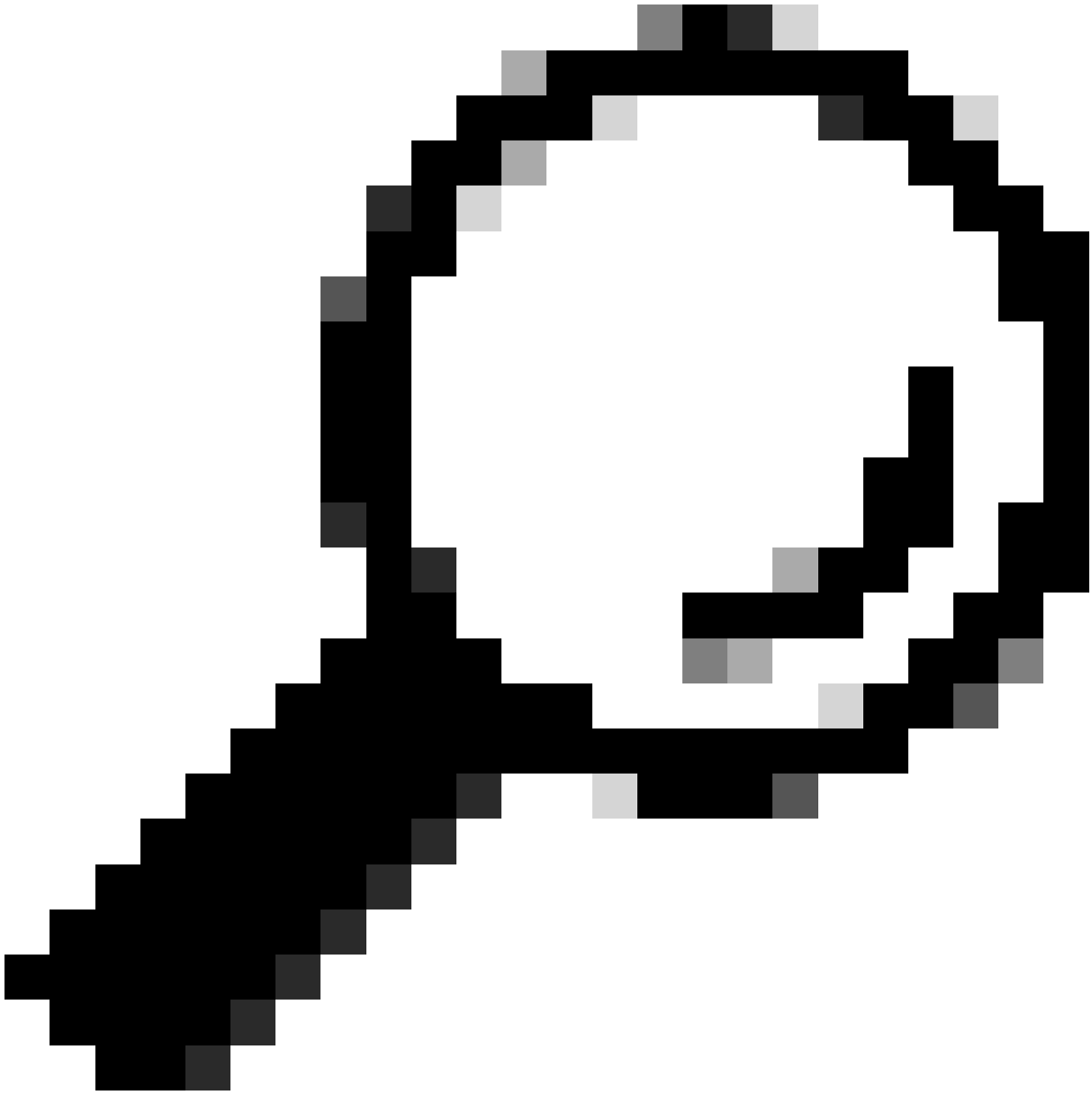
5. Klik op Opslaan.



Opmerking: Zorg ervoor dat u over de nodige beheerdersrechten beschikt om de integratie en workflow te configureren.



Tip: Test de installatie in een gecontroleerde omgeving voordat u de automatisering in productie implementeert.



Tip: Documenteer aangepaste aanpassingen die zijn gemaakt in de werkstroom- of automatiseringsregel.

Zodra deze stappen zijn voltooid, configureert en activeert u met succes een workflow die automatisch een eindpunt isoleert nadat een incident is gemaakt en zorgt voor een snelle en effectieve reactie op beveiligingsbedreigingen.

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.