Automatische workflow voor e-mailmeldingen configureren met XDR

Inhoud

Inleiding

In dit document wordt beschreven hoe u een geautomatiseerde workflow kunt maken om een e-mailmelding te verzenden voor een nieuw incident.

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

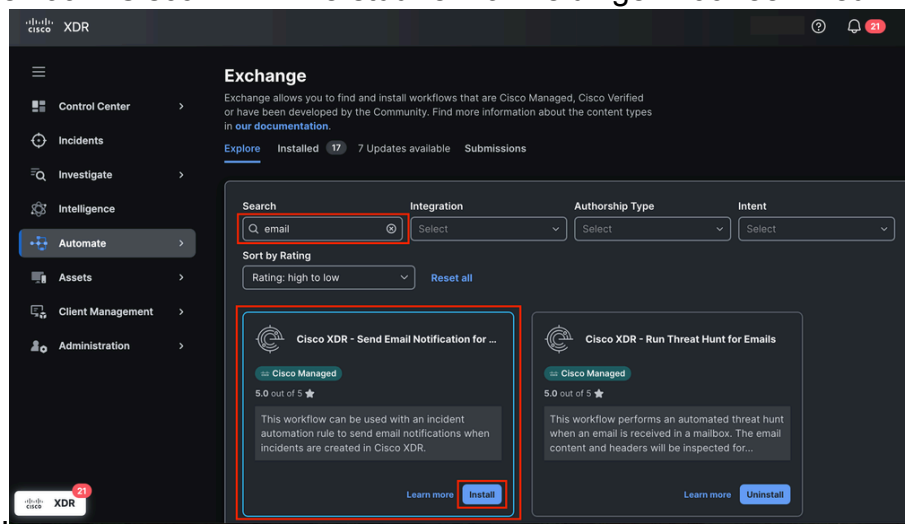
In deze handleiding worden de stappen beschreven die nodig zijn om een workflow te configureren en te activeren om automatisch een e-mailmelding te verzenden wanneer zich een

incident voordoet. De stappen worden als volgt beschreven.

Installeer de werkstroom van Cisco XDR Exchange

Stap 1. De workflow voor het isoleren van eindpunten installeren

1. Meld u aan bij Cisco XDR en navigeer naar Automate > Exchange.
2. Zoek naar de workflow met de naam Cisco XDR - Verstuur e-mailmeldingen voor een nieuw incident en klik op Installeren.

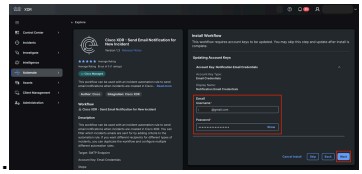


Werkstroom voor e-mailmeldingen verzenden vanuit Exchange

3. Controleer de benodigde informatie om de workflow correct te configureren.

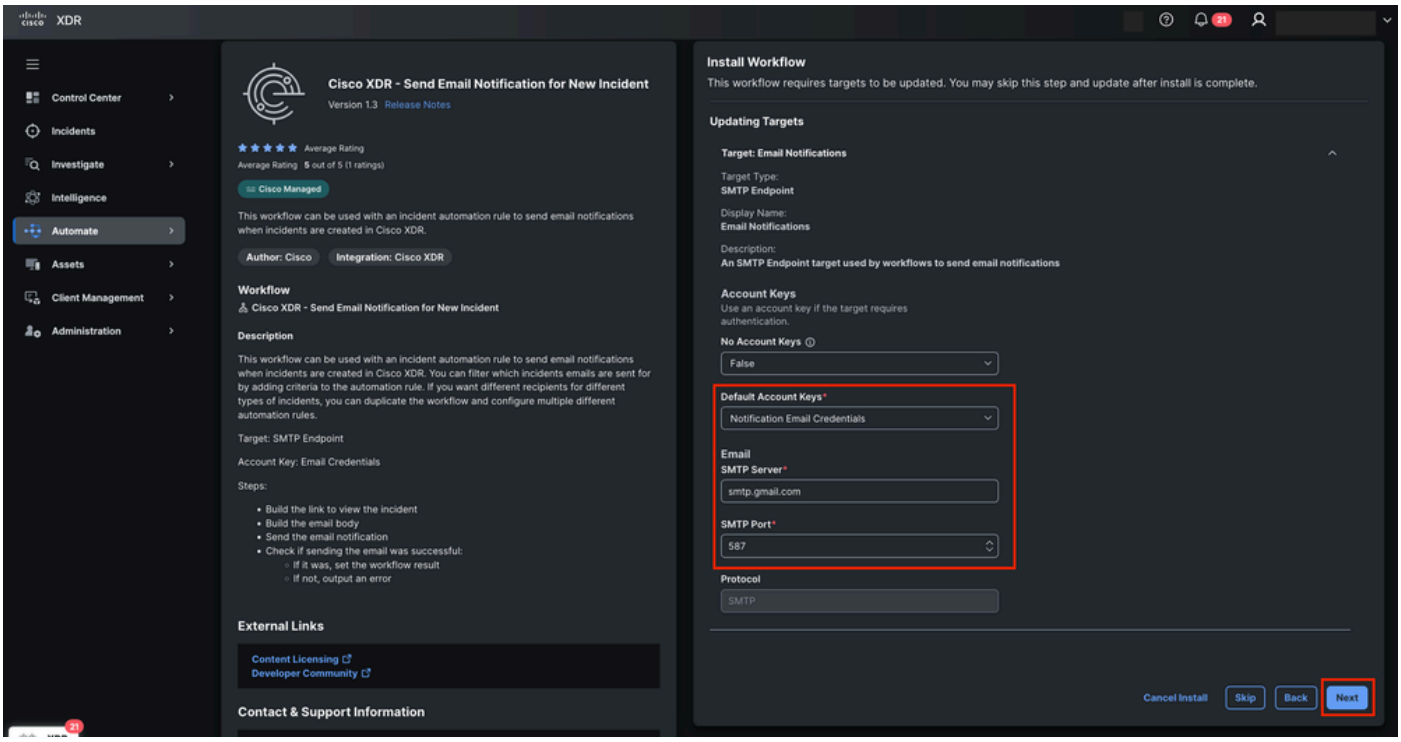
Overzicht van de werkstroom voor e-mailmeldingen verzenden

4. Vul de accountsleutels inmet de e-mailreferenties om de afzender in te stellen. De weergegeven naam is Bericht e-mailreferenties en klik op Volgende.



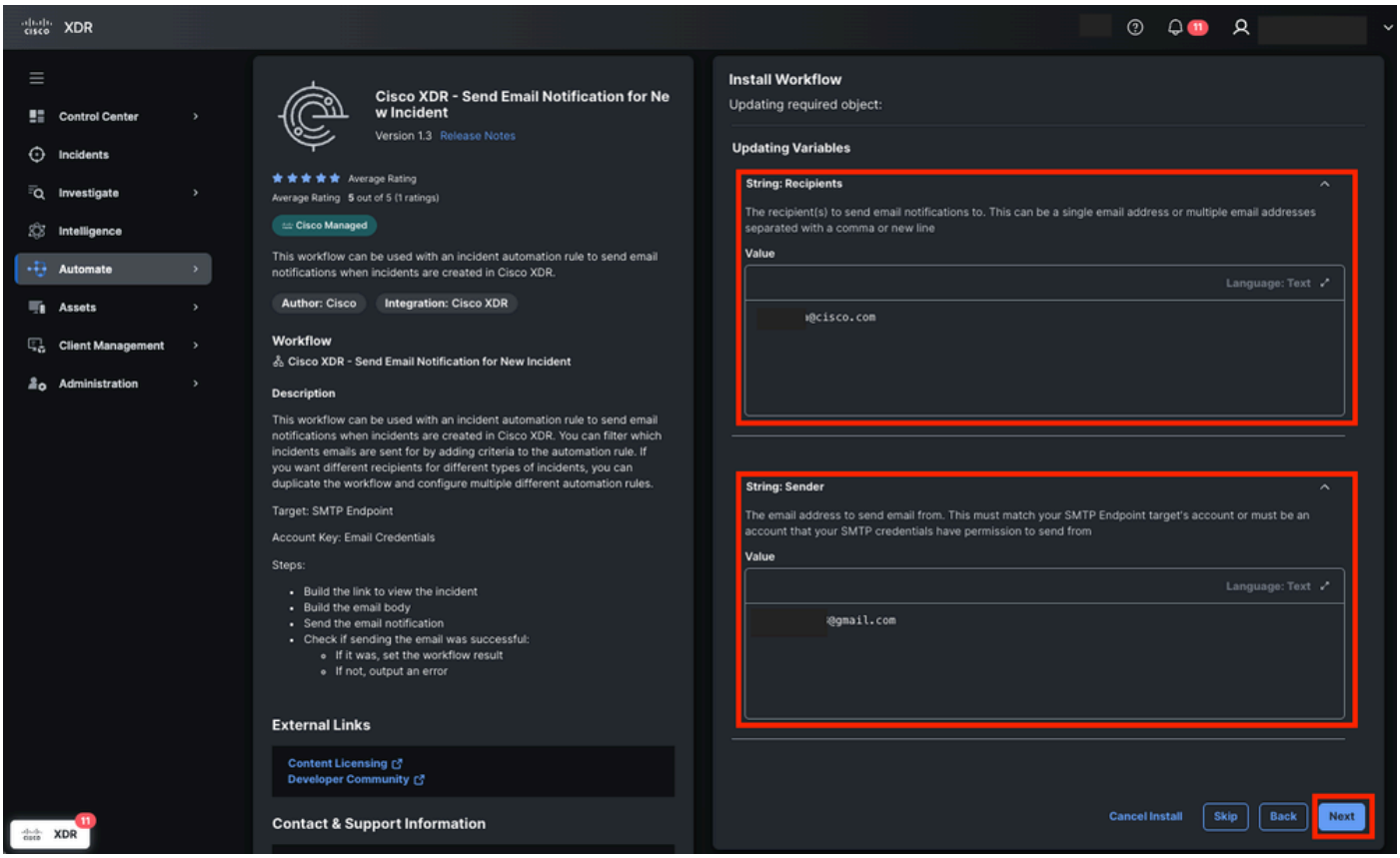
Accountsleutels voor workflow

5. Configureer de doelinformatie met:
    - Accountsleutels: aanmeldingsgegevens e-mail
    - Email
        - SMTP-server: smtp.gmail.com
        - SMTP-poort: 587



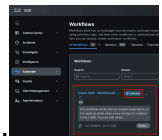
Doelconfiguratie voor workflow

1. Klik op Next (Volgende).
2. Werk de variabele bij voor:
    - Ontvangers
    - afzender



Variabelen toewijzen voor werkstroom

8. Klik op Volgende.

9. Navigeer naar Automatisch > Werkstromen om de gevalideerde status te controleren. 

Werkstroom gevalideerde status

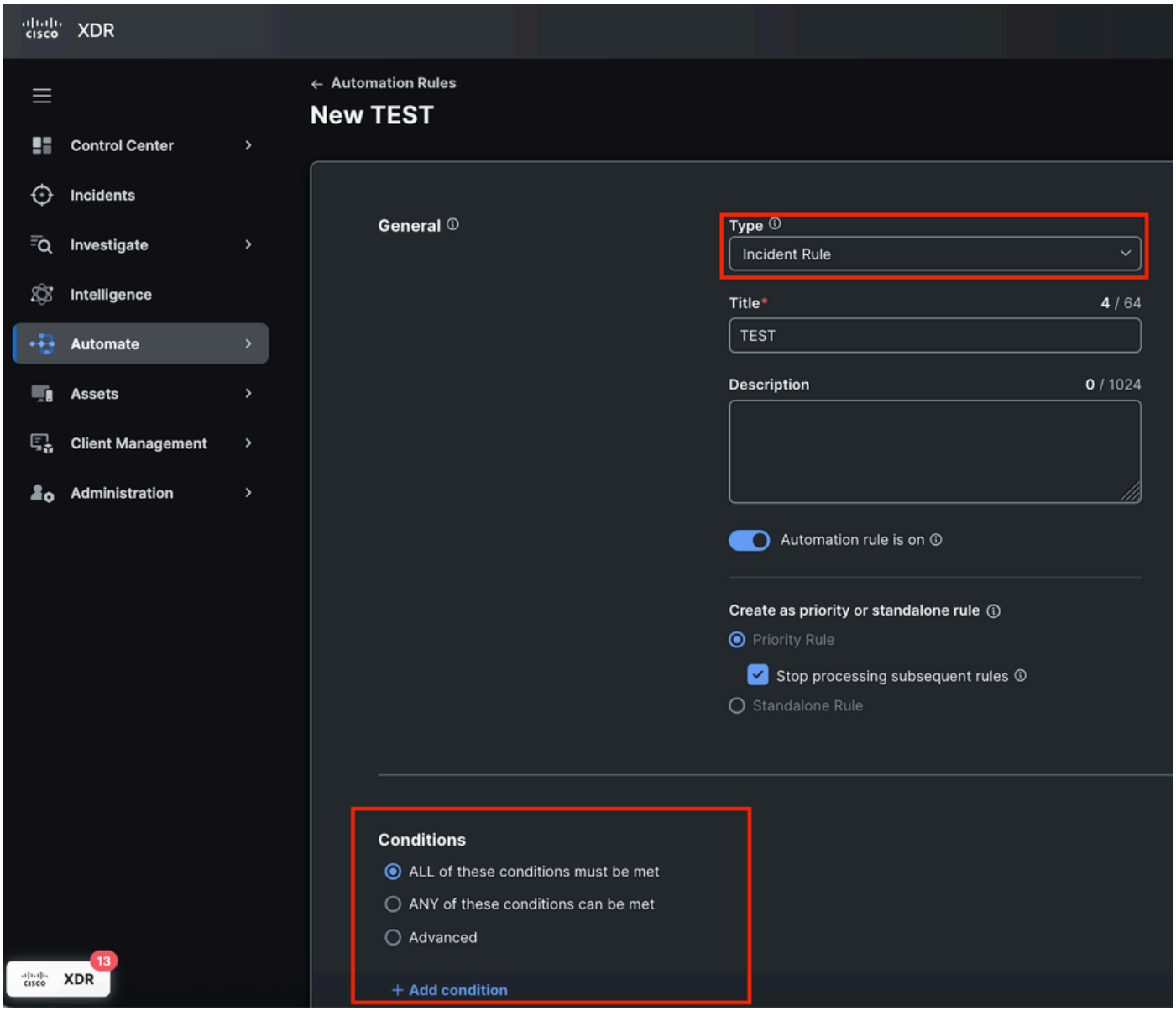
Een automatiseringsregel maken

Stap 2. Automatiseringsregel configureren

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

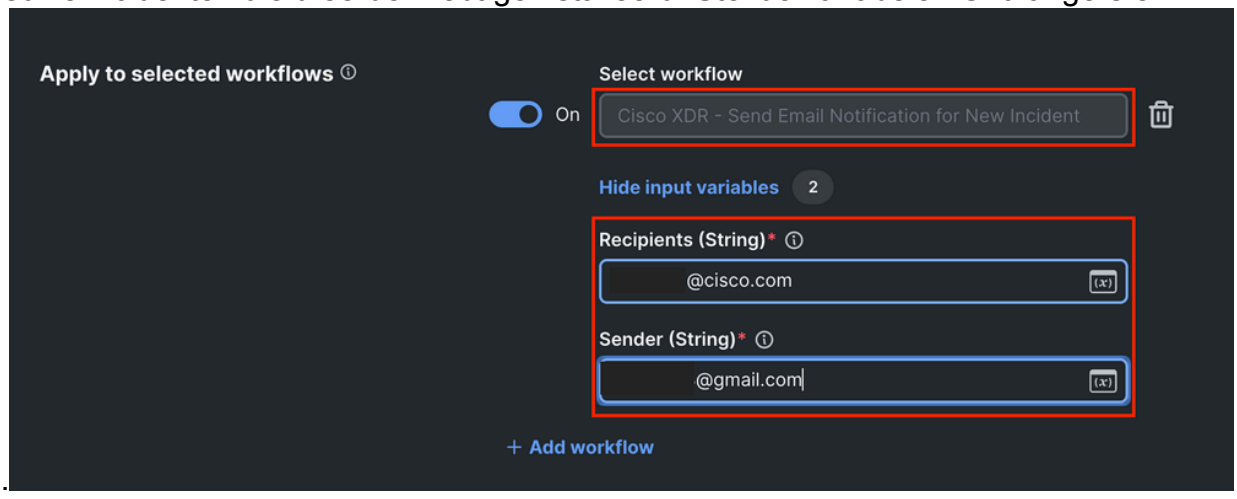
   Automatiseringsregel van triggers toevoegen

3. Selecteer het type Incidentregel en definieer de triggervoorwaarden. U kunt doorgaan zonder dat u een regelvoorwaarde hoeft toe te voegen, waardoor deze regel bij elk incident wordt geactiveerd. Pas indien nodig de voorwaarden aan.



Type en voorwaarden automatiseringsregel

4. Pas de automatiseringsregel toe op de Cisco XDR - E-mailmeldingen verzenden voor de workflow Nieuwe incidenten die u eerder hebt geïnstalleerd. Stel de variabelen Ontvangers en Afzender in.



De automatiseringsregel toepassen op de werkstroom en variabelen toewijzen

5. Sla de regel op.

Werkstroomfunctionaliteit valideren

Stap 3. Controleren van de uitvoering van de werkstroom

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

   Nieuw incident in Cisco XDR gedetecteerd

2. Klik op Incident en vervolgens op Incident Details bekijken.

Malware detections on single endpoint

Priority 830 Status New

Reported by
Cisco XDR Analytics

on 2025-06-10T20:36:11.917Z

Unassigned

MITRE

Priority score breakdown

830

83	10
Detection Risk	Asset Value at Risk

Sources

Cisco Secure Endpoint

View Incident Detail

: de naam van het eerste incident wordt gegenereerd op basis van de eerste detectie. Deze naam kan echter worden gewijzigd als er extra detecties worden uitgevoerd of nieuwe informatie het incident verrijkt.

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.