Configurer le workflow automatisé de notification par e-mail avec XDR

Table des matières

Introduction

Ce document décrit comment créer un workflow automatisé pour envoyer une notification par e-mail pour un nouvel incident.

Conditions préalables

Exigences

Aucune exigence spécifique n'est associée à ce document.

Composants utilisés

Ce document n'est pas limité à des versions de matériel et de logiciel spécifiques.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

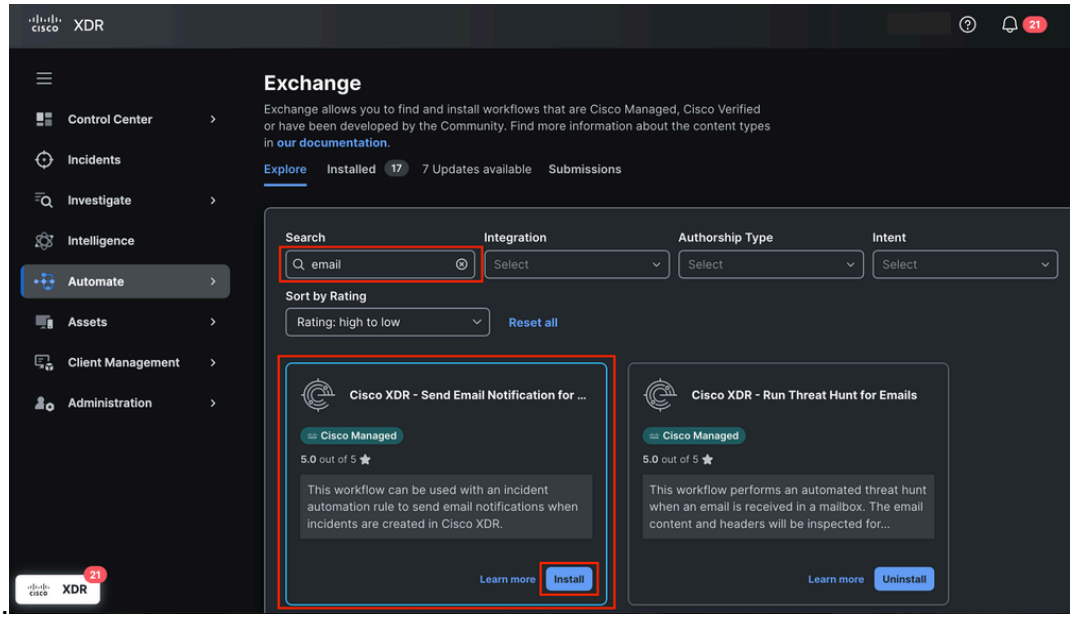
Configurer

Ce guide détaille les étapes nécessaires pour configurer et activer un flux de travail afin d'envoyer automatiquement une notification par e-mail lorsqu'un incident se produit. Les étapes sont détaillées comme suit.

Installer le workflow à partir de Cisco XDR Exchange

Étape 1. Installation du workflow d'isolation des terminaux

1. Connectez-vous à Cisco XDR et accédez à Automate > Exchange.
2. Recherchez le workflow nommé Cisco XDR - Send Email Notification for New Incident et cliquez sur Install.



Envoyer un workflow de notification par courrier électronique depuis Exchange

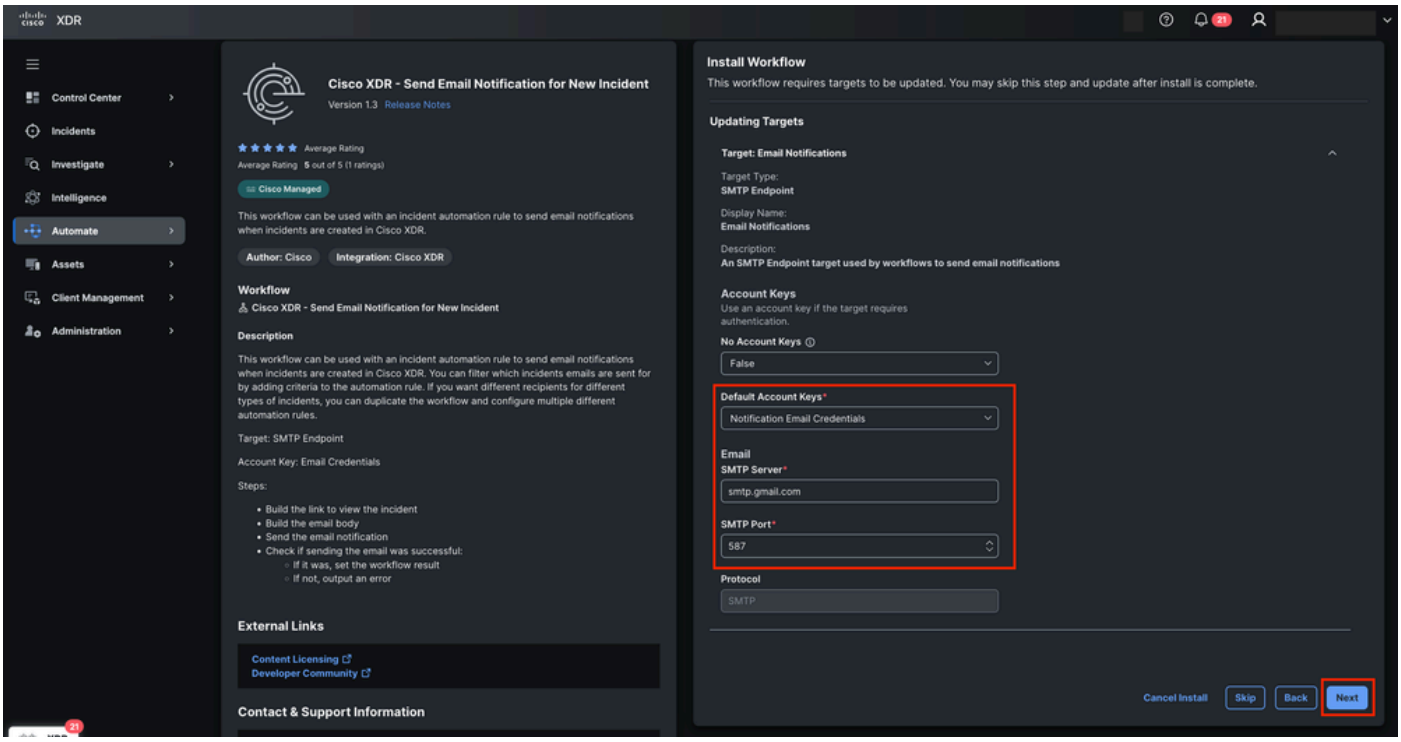
3. Vérifiez les informations nécessaires pour configurer correctement le workflow. 

Présentation du workflow Envoyer une notification par e-mail

4. Remplissez les clés de compteavec les informations d'identification de l'e-mail pour définir l'expéditeur. Le nom affiché est Notification Email Credentials et cliquez sur Suivant. 

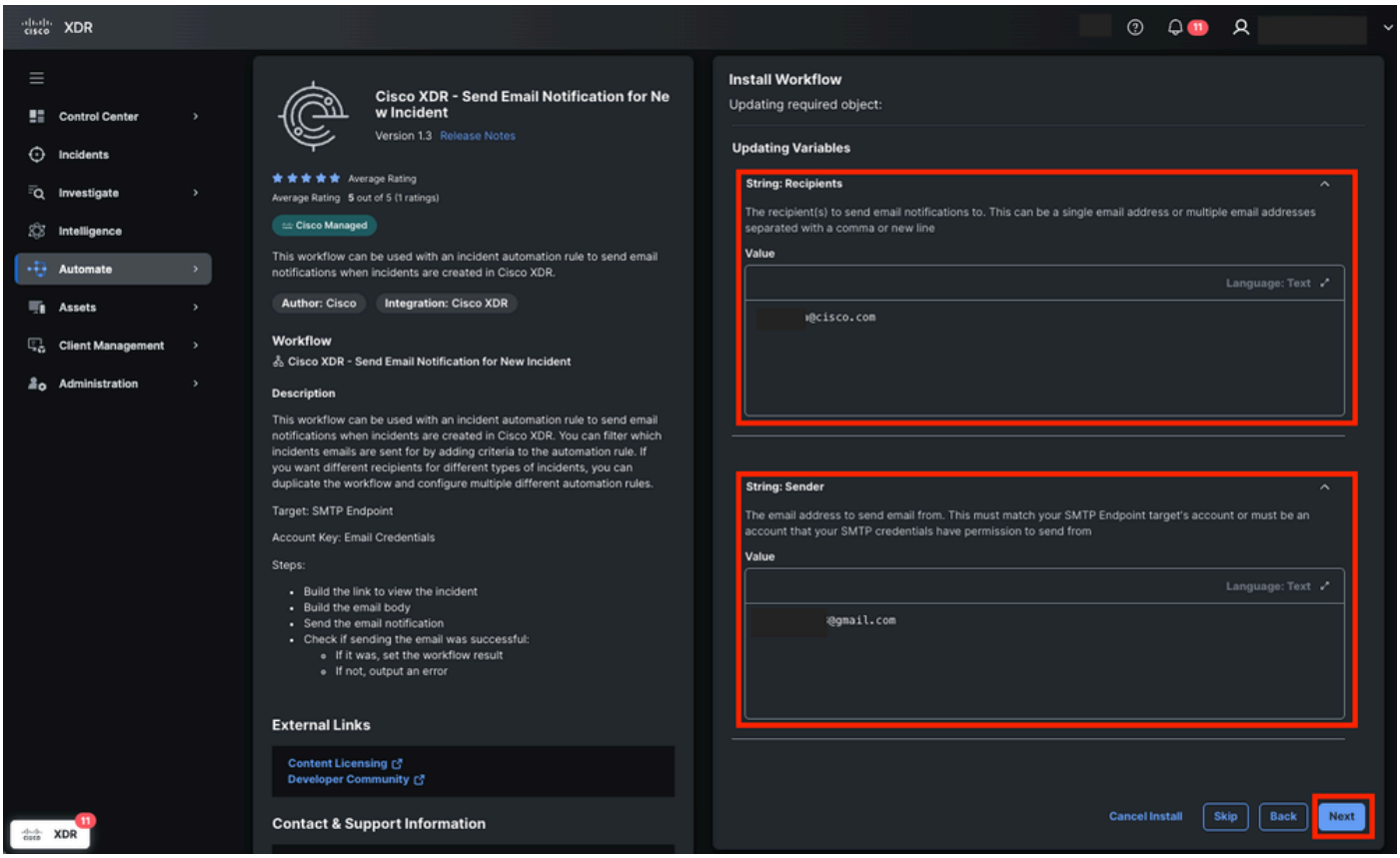
Clés de compte pour le workflow

5. Configurez les informations de la cible avec :
   - Clés de compte : Informations d'identification de notification
   - Courriel
     - Serveur SMTP : smtp.gmail.com
     - Port SMTP : 587



Configuration cible pour le workflow

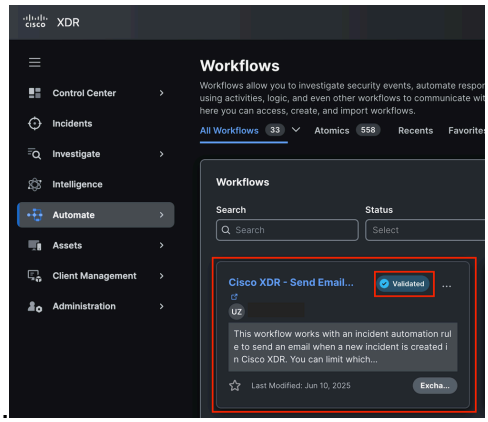
1. Cliquez sur Next (Suivant).
2. Mettez à jour la variable pour :
    - Destinataires
    - Expéditeur



Affecter des variables au workflow

8. Cliquez sur Suivant.

9. Accédez à Automate > Workflows pour vérifier le statut Validé.

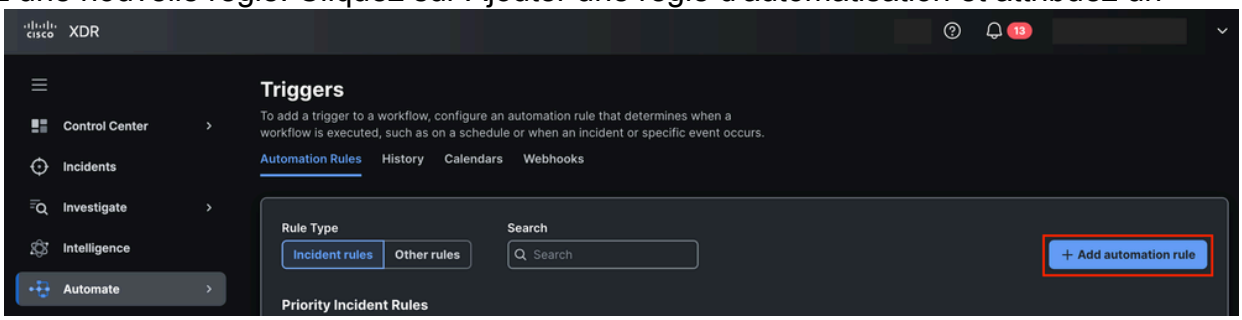


Statut validé du workflow

Créer une règle d'automatisation

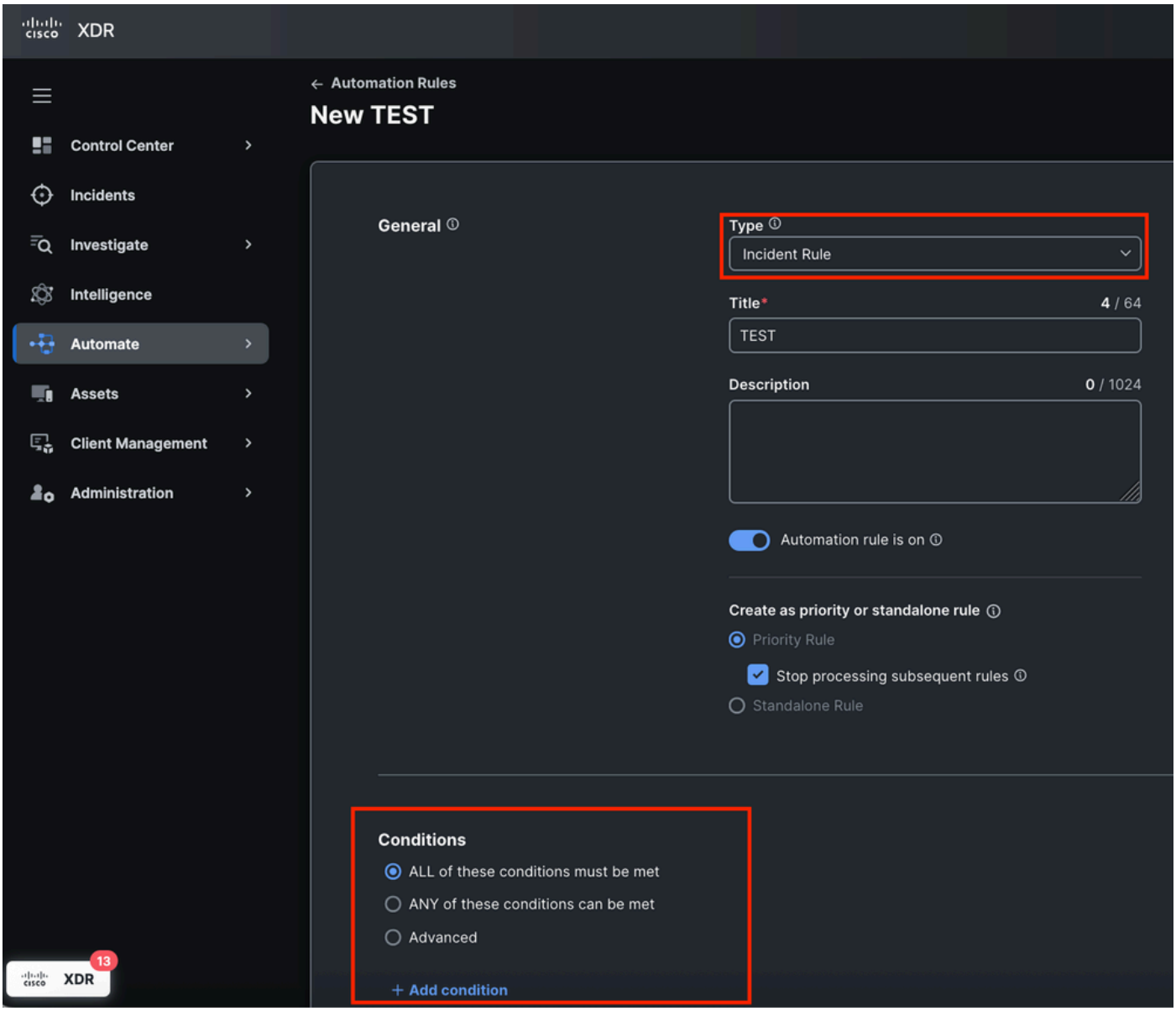
Étape 2 : configuration d’une règle d’automatisation

1. Accédez à la section Automatisation > Déclencheurs.
2. Créez une nouvelle règle. Cliquez sur Ajouter une règle d'automatisation et attribuez un nom.



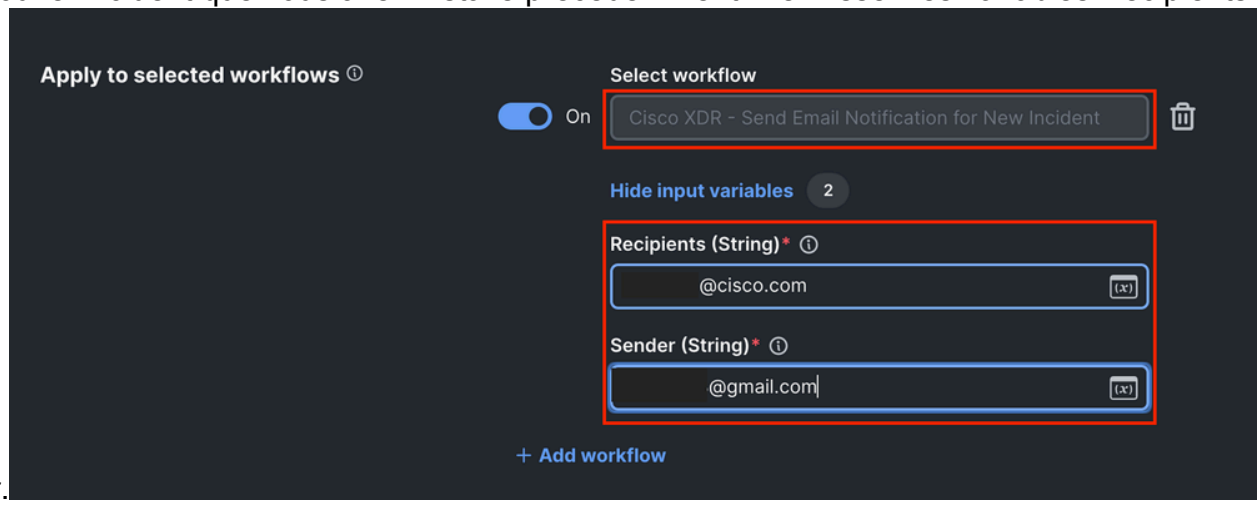
Ajouter une règle d'automatisation à partir des déclencheurs

3. Sélectionnez le type de règle d'incident et définissez les conditions de déclenchement. Vous pouvez continuer sans avoir à ajouter de condition de règle, ce qui garantit que tout incident active cette règle. Personnalisez les conditions si nécessaire.



Type et conditions de règle d'automatisation

4. Appliquez la règle d'automatisation au workflow Cisco XDR - Envoyer une notification par e-mail pour un nouvel incident que vous avez installé précédemment. Définissez les variables Recipients et Sender.

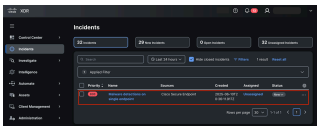


Appliquer la règle d'automatisation au workflow et affecter des variables

5. Enregistrez la règle.

Valider la fonctionnalité de workflow

Étape 3. Vérification de l'exécution du workflow



1. Générer ou attendre un incident qui répond aux conditions de la règle.

   Nouvel incident détecté dans Cisco XDR

2. Cliquez sur Incident, puis sur Afficher les détails de l'incident.

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

Le nom initial de l'incident est généré en fonction de la première détection ; toutefois, elle peut changer si des détections supplémentaires se produisent ou si de nouvelles informations enrichissent l'incident.

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.