Configuration du workflow automatisé d'isolement des terminaux avec Cisco XDR

Table des matières

Introduction

Ce document décrit comment créer un workflow d'automatisation pour isoler un point de terminaison 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.

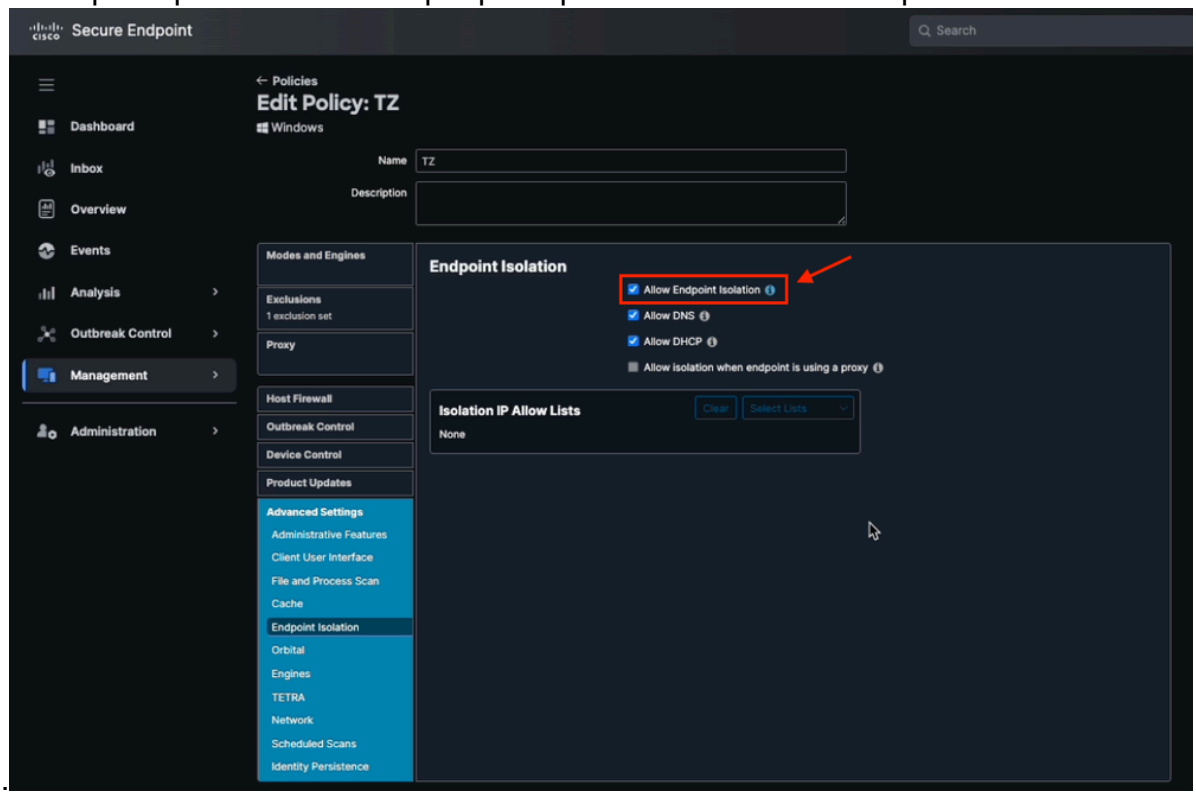
Configurer

Ce guide détaille les étapes nécessaires à la configuration et à l'activation d'un workflow pour isoler automatiquement un terminal en cas d'incident. L'intégration s'effectue avec Cisco Secure Endpoint et la fonctionnalité d'automatisation du workflow. Les étapes sont décrites comme suit.

Configuration initiale dans Cisco Secure Endpoint

Étape 1.1 : Activer la fonction d'isolation dans la stratégie

1. Connectez-vous au portail Cisco Secure Endpoint.
2. Accédez à la section Management > Policies.
3. Sélectionnez la stratégie qui s'applique au point de terminaison que vous souhaitez isoler.
4. Assurez-vous que l'option Isolation de périphérique est activée dans les paramètres de stratégie.



Autoriser l'isolement des terminaux depuis la stratégie Secure Endpoint

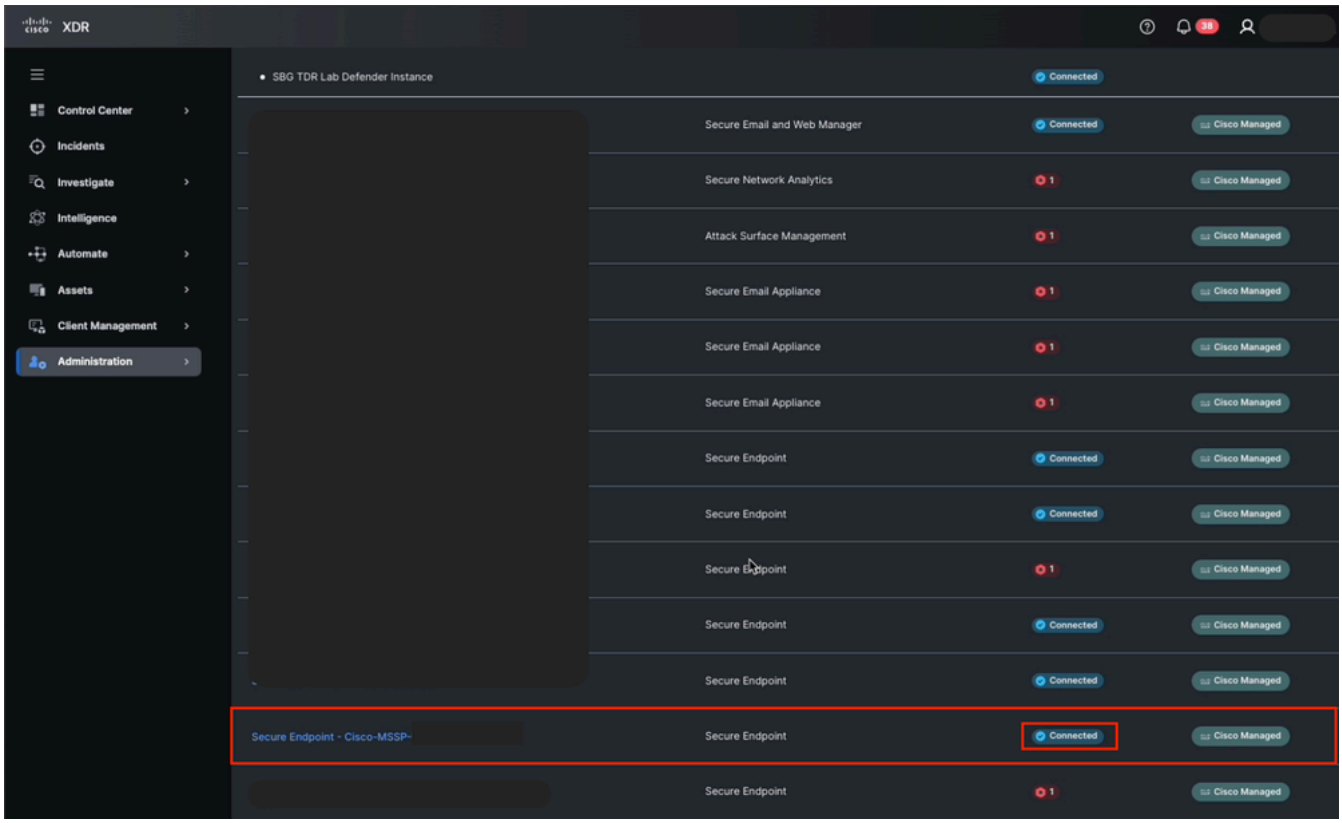
5. Enregistrez les modifications et distribuez la stratégie si nécessaire.

Validation de l'intégration avec Cisco Secure Endpoint

Étape 2.1 : Vérification de l'intégration

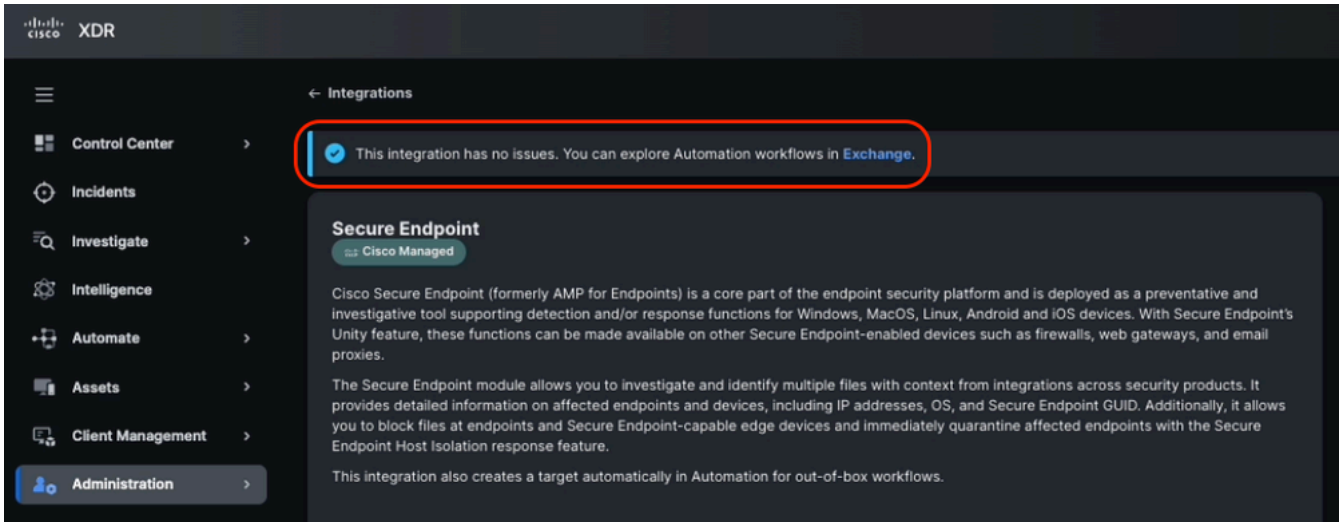
1. Connectez-vous à Cisco XDR.
2. Accédez à Administration > Integrations > My Integrations section.
3. Assurez-vous que l'intégration avec Cisco Secure Endpoint est correctement configurée :

Vérifiez l'état d'intégration dans Connected.



État de l'intégration des terminaux sécurisés de Cisco XDR

Vérifiez qu'il n'y a aucune erreur dans la configuration de l'API.

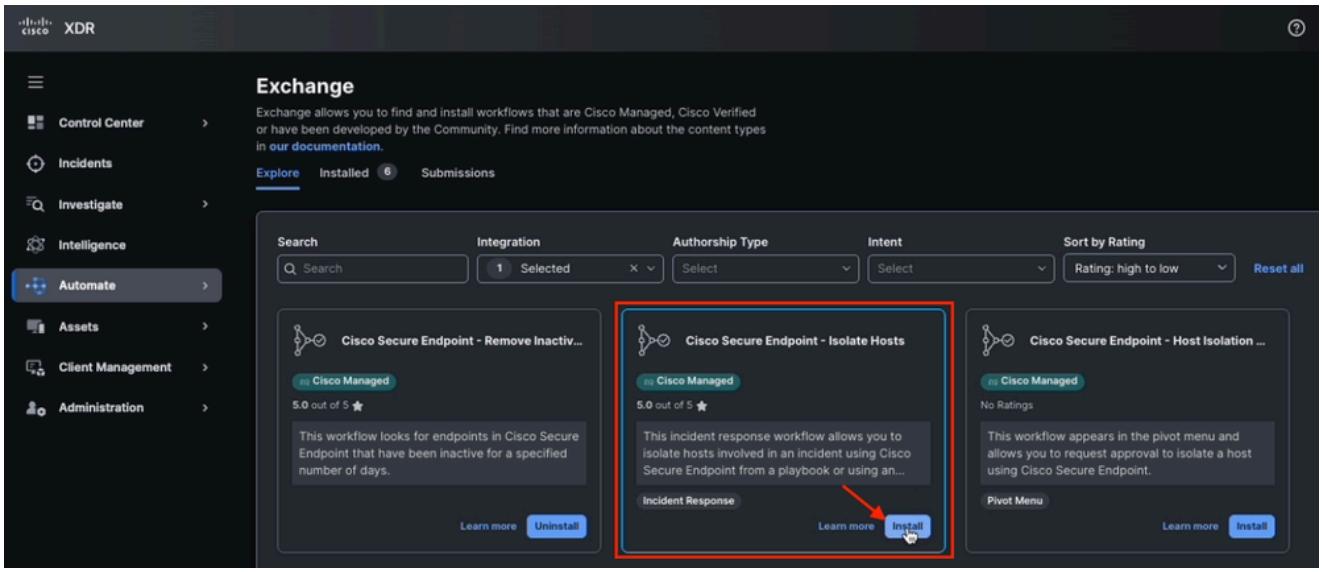


Vérification du fonctionnement de l'intégration Secure Endpoint

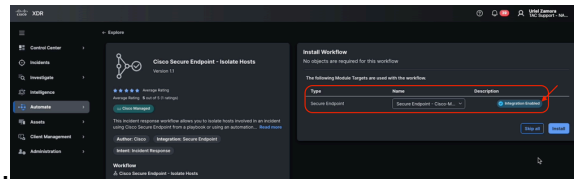
Installer le workflow à partir de Cisco XDR Exchange

Étape 3.1 : Installer le workflow d'isolation des terminaux

1. Connectez-vous à Cisco XDR et accédez à Automate > Exchange.
2. Recherchez le flux de travail intitulé Cisco Secure Endpoint - Isolate Hosts et cliquez sur Install.



Isoler le workflow hôte d'Exchange

3. Vérifiez que la cible est disponible avant l'installation. 

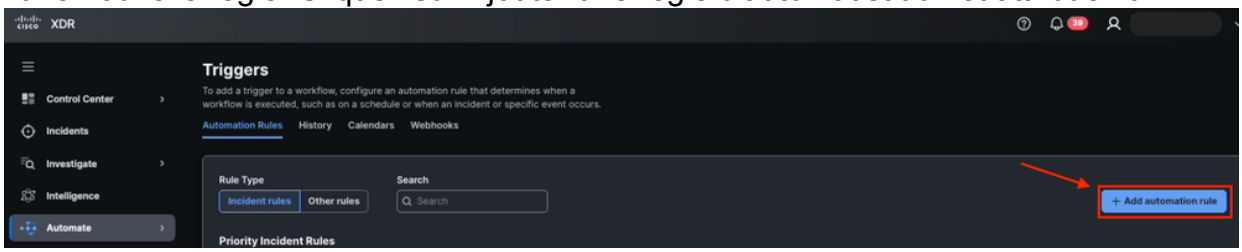
Cible de module activée à partir du workflow

4. Installez le workflow dans votre système d'automatisation.

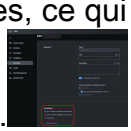
Créer une règle d'automatisation

Une règle d'automatisation est une configuration qui définit quand un workflow doit être exécuté, en fonction d'événements spécifiques ou d'un planning prédéfini. Ces règles peuvent inclure des conditions facultatives. Si ces conditions sont remplies, le ou les workflows associés sont déclenchés automatiquement.

Étape 4.1 : Configurer une règle d'automatisation

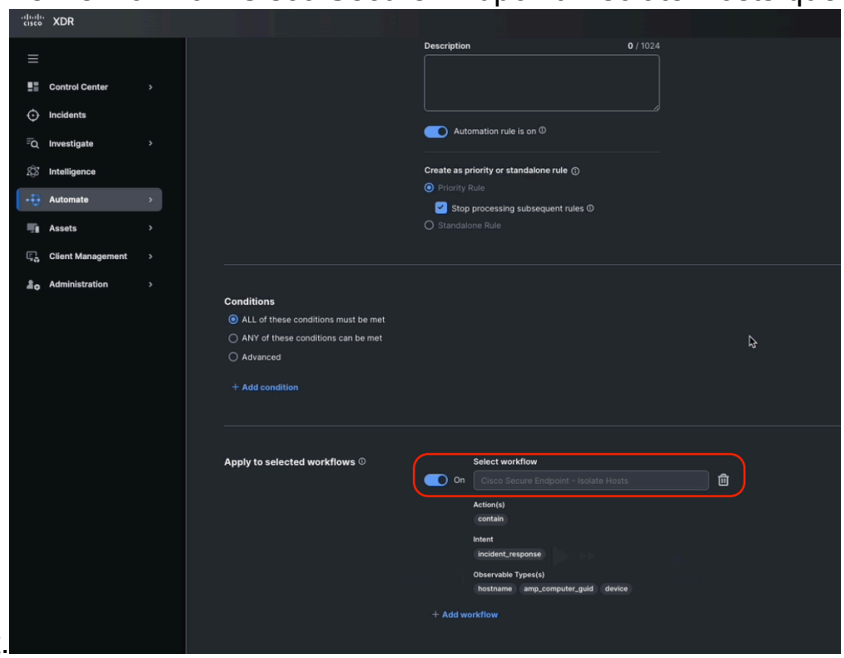
1. Accédez à la section Automatisation > Déclencheurs.
2. Créez une nouvelle règle. Cliquez sur Ajouter une règle d'automatisation et attribuez un nom. 

Ajouter une règle d'automatisation à partir des déclencheurs

3. Définissez les conditions de déclenchement. Vous pouvez laisser les conditions vides, ce qui garantit que tout incident active cette règle. Personnalisez la condition si nécessaire. 

Conditions des règles d'automatisation

4. Dans l'action de la règle, sélectionnez le workflow Cisco Secure Endpoint - Isolate Hosts que vous avez installé précédemment.



Affecter la règle d'automatisation au workflow

5. Cliquez sur Save.

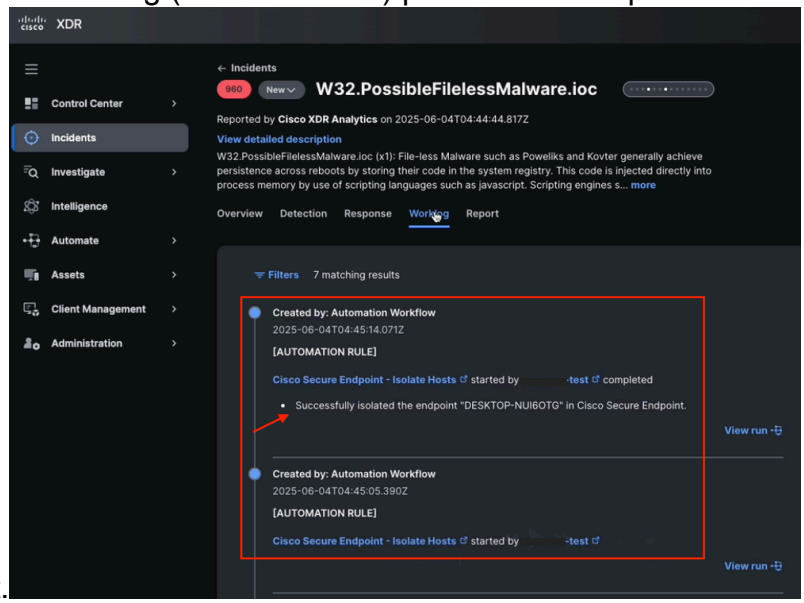
Valider la fonctionnalité de workflow

Étape 5.1 : Vérifier l'exécution du workflow

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

Nouvel incident détecté dans Cisco XDR

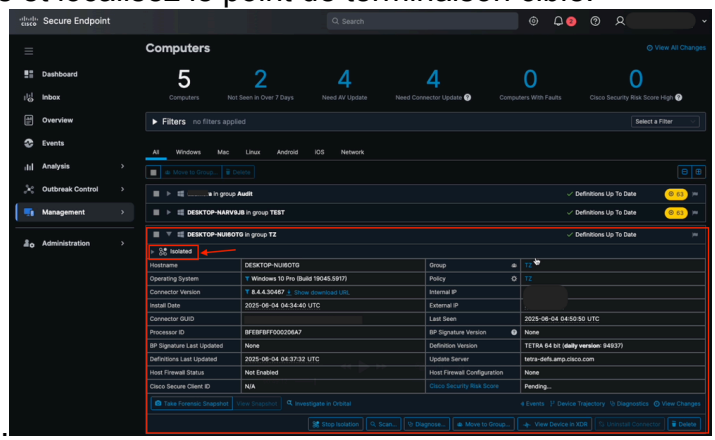
2. Une fois l'incident créé, vérifiez l'onglet Worklog (dans l'incident) pour confirmer que le workflow s'est exécuté correctement.



Onglet Journal des incidents - Informations

Étape 5.2 : Confirmer l'isolement des terminaux

1. Connectez-vous au portail Cisco Secure Endpoint.
2. Accédez à la section Gestion > Ordinateurs et localisez le point de terminaison cible.



3. Vérifiez que l'état du périphérique est Isolé.

État d'isolation des ordinateurs de terminaux sécurisés

4. Si le point d'extrémité n'est pas isolé, consultez les journaux de workflow et la configuration pour identifier les problèmes éventuels.

Problème courant

La fonction d'isolation n'est pas activée depuis Cisco Secure Endpoint

1. Dans Cisco XDR, accédez à Incidents, localisez le dernier incident et accédez à Worklog.

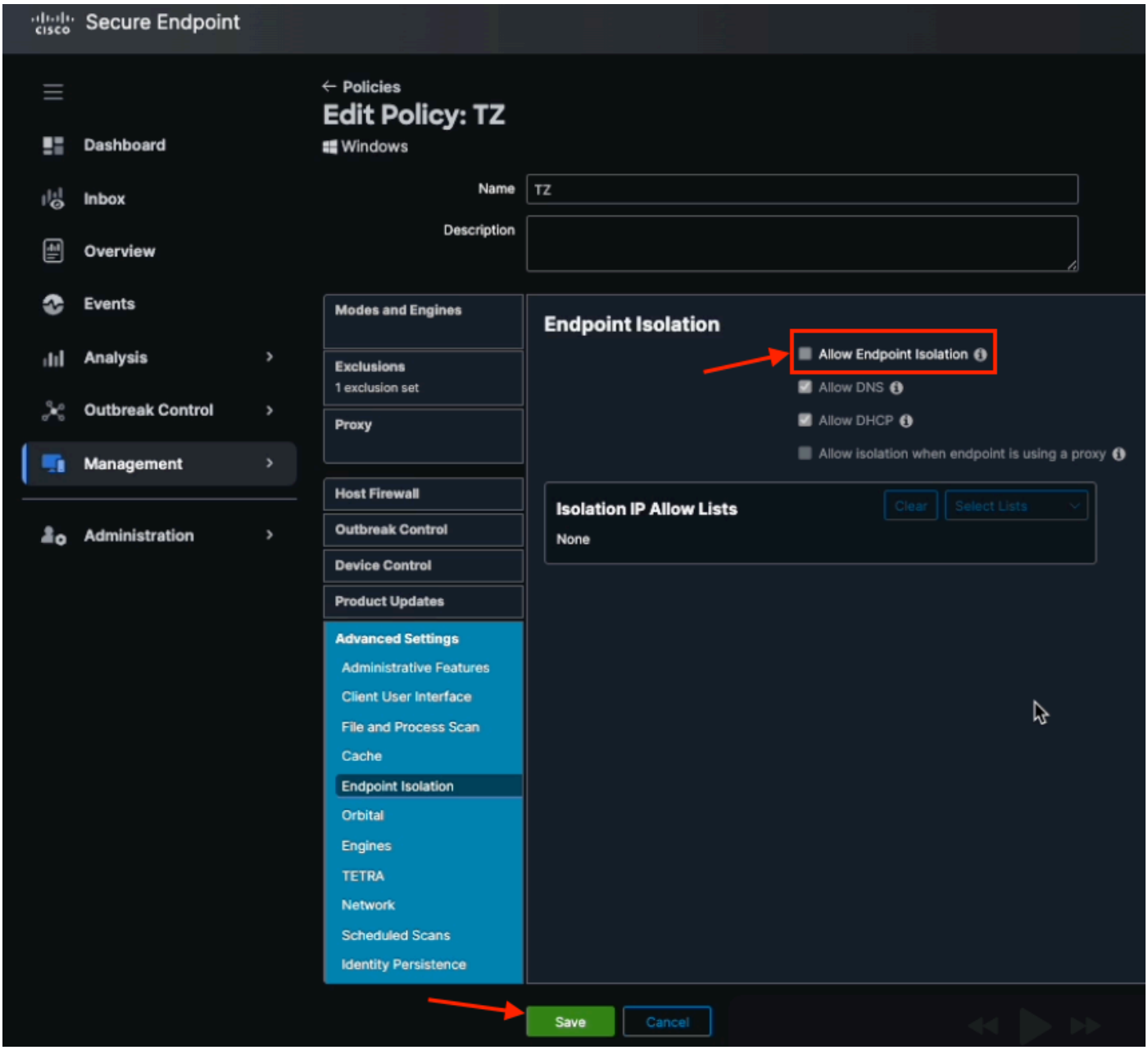
2. Vérifiez s'il y a une erreur associée après l'exécution du workflow d'automatisation.

Par exemple, l'isolement de point de terminaison n'a pas permis d'isoler l'hôte car l'isolement de point de terminaison n'a pas été activé sur la stratégie de point de terminaison sécurisé.

Résultats du workflow d'automatisation du journal des incidents

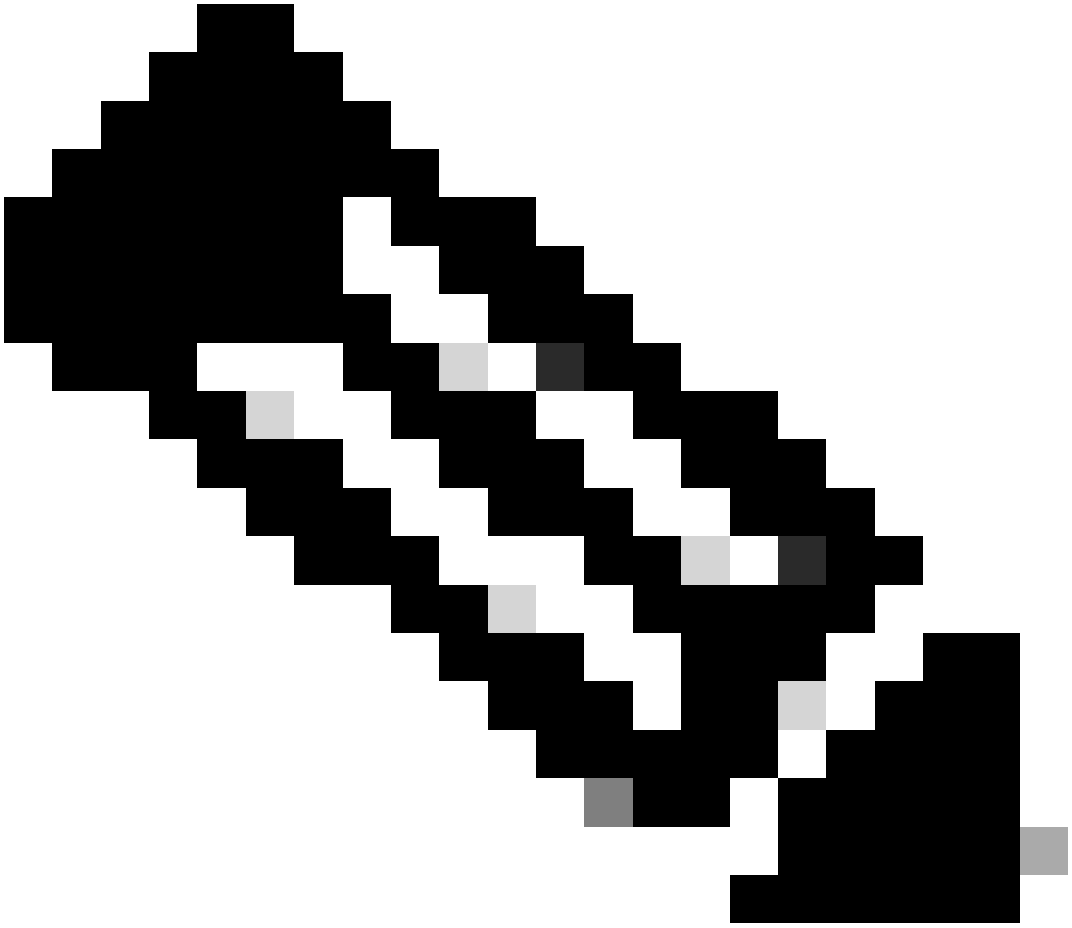
3. Dans Secure Endpoint, accédez à Management > Policies et sélectionnez la stratégie en question.

4. Une fois dans la stratégie, naviguez vers Advanced Settings > Endpoint Isolation et cochez la case Allow Endpoint Isolation.

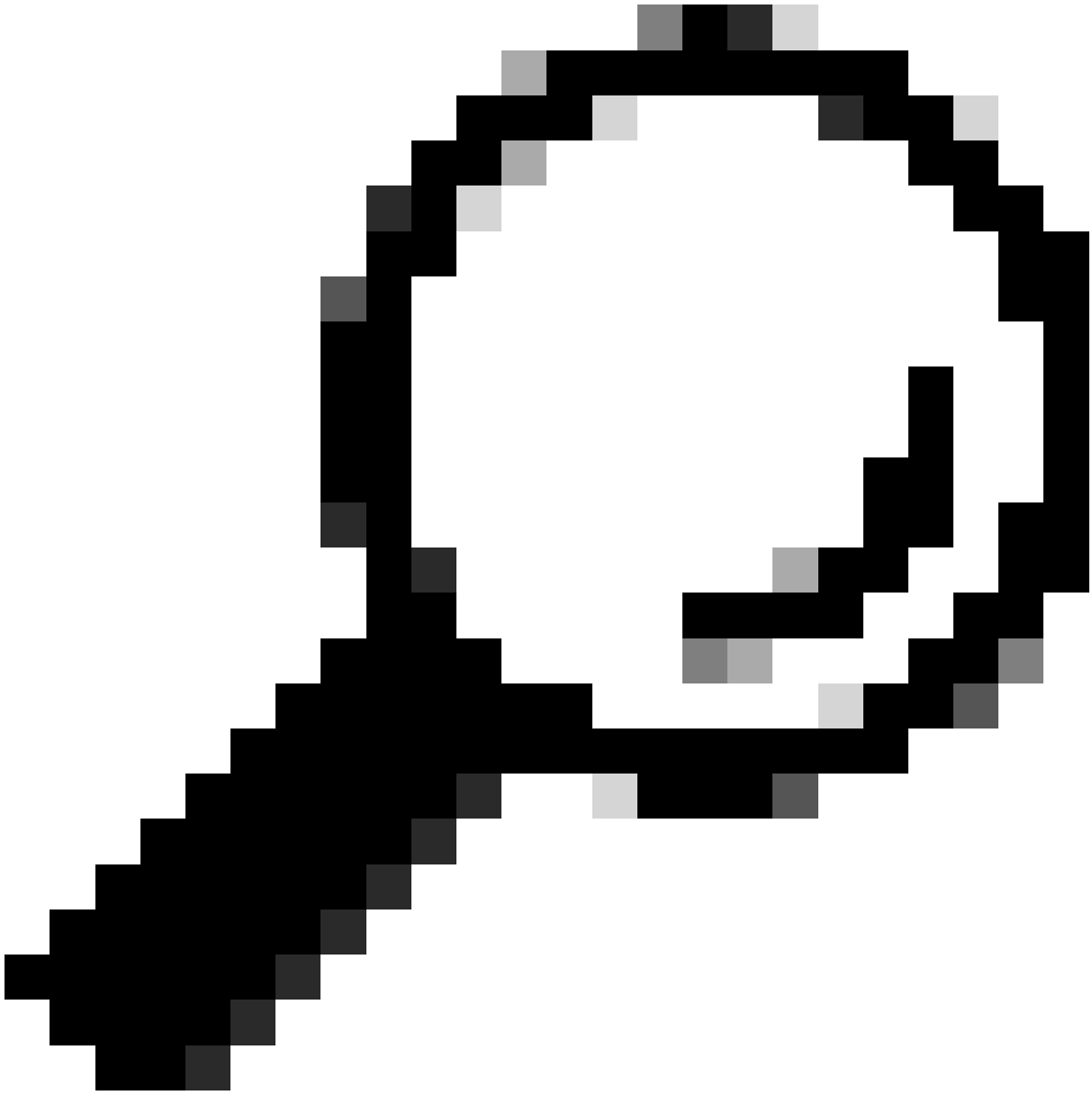


Case à cocher Autoriser l'isolation des points de terminaison dans la stratégie Secure Endpoint

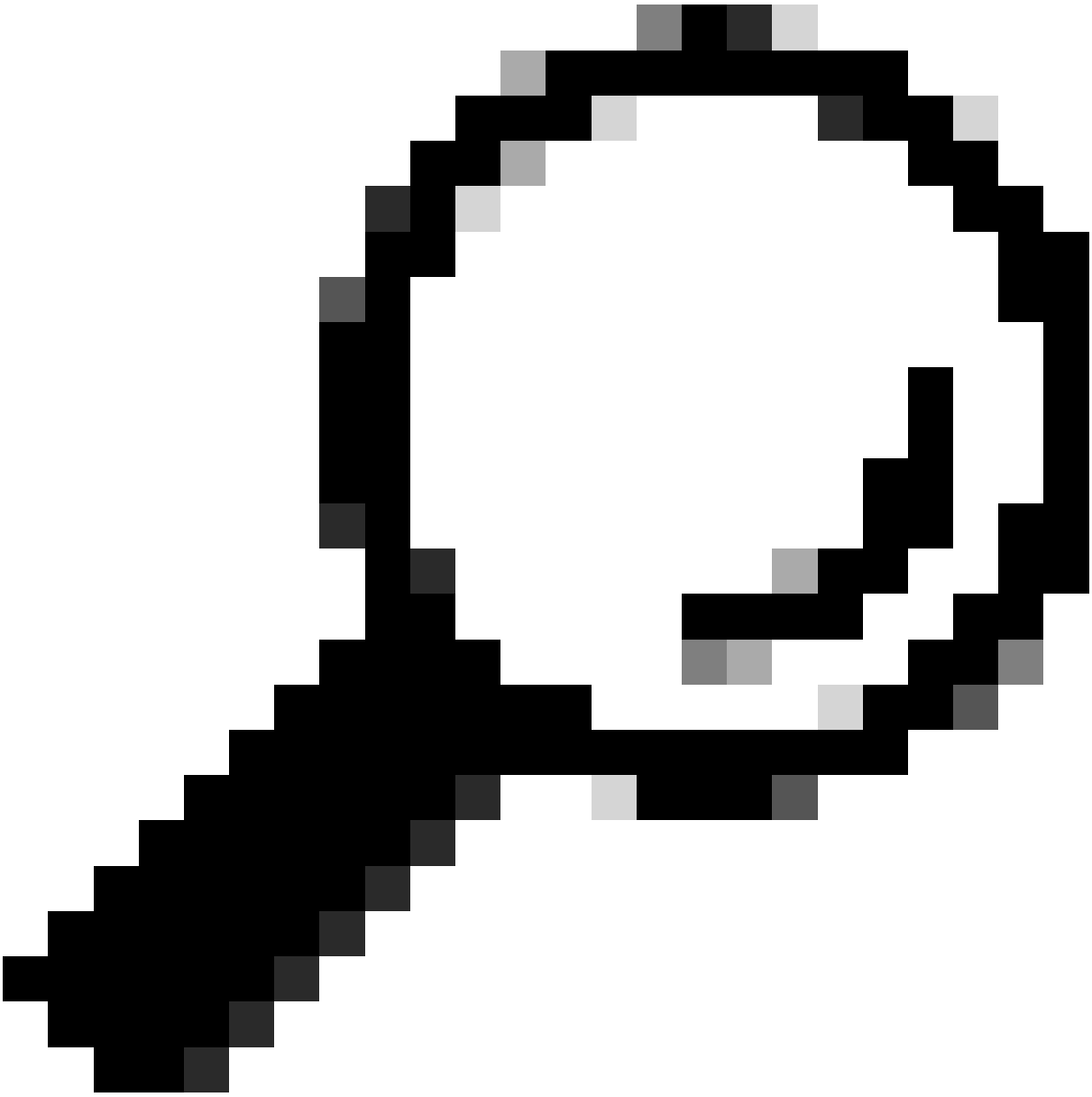
5. Cliquez sur Enregistrer.



Remarque : assurez-vous que vous disposez des autorisations administratives nécessaires pour configurer l'intégration et le workflow.



Conseil : Testez la configuration dans un environnement contrôlé avant de déployer l'automatisation en production.



Conseil : Documentez tous les ajustements personnalisés apportés au workflow ou à la règle d'automatisation.

Une fois ces étapes effectuées, vous configurez et activez avec succès un workflow qui isole automatiquement un terminal après la création d'un incident et garantit une réponse rapide et efficace aux menaces de sécurité.

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.