Cisco XDRによるエンドポイント分離自動ワークフローの設定

内容

はじめに

このドキュメントでは、新しいインシデントのエンドポイントを分離する自動化ワークフローを作成する方法について説明します。

前提条件

要件

このドキュメントに関する固有の要件はありません。

使用するコンポーネント

このドキュメントの内容は、特定のソフトウェアやハードウェアのバージョンに限定されるものではありません。

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このド

キュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

設定

このガイドでは、インシデントが発生したときにエンドポイントを自動的に分離するワークフローを設定およびアクティブ化するために必要な手順について詳しく説明します。統合は、Cisco Secure Endpointおよびワークフロー自動化機能を使用して実行されます。手順の概要は次のとおりです。

Cisco Secure Endpointの初期設定

ステップ1.1：ポリシーで隔離機能を有効にする

1. Cisco Secure Endpointポータルにログインします。
2. Management > Policiesの順に移動します。
3. 分離するエンドポイントに適用するポリシーを選択します。
4. ポリシー設定内でDevice Isolationオプションが有効になっていることを確認します。 

   セキュアエンドポイントポリシーからのエンドポイントの分離を許可

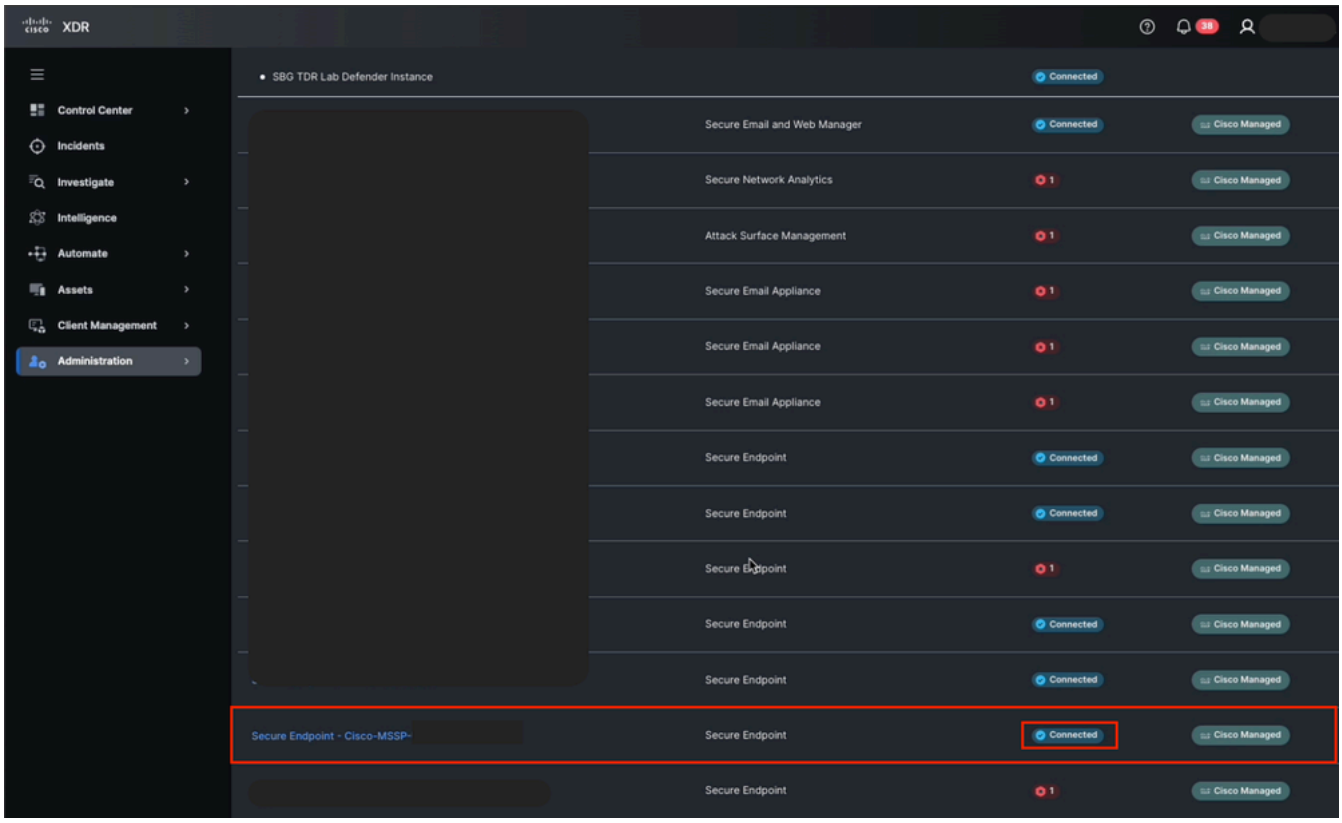
5. 必要に応じて、変更を保存し、ポリシーを配布します。

Cisco Secure Endpointとの統合の検証

ステップ2.1：統合の確認

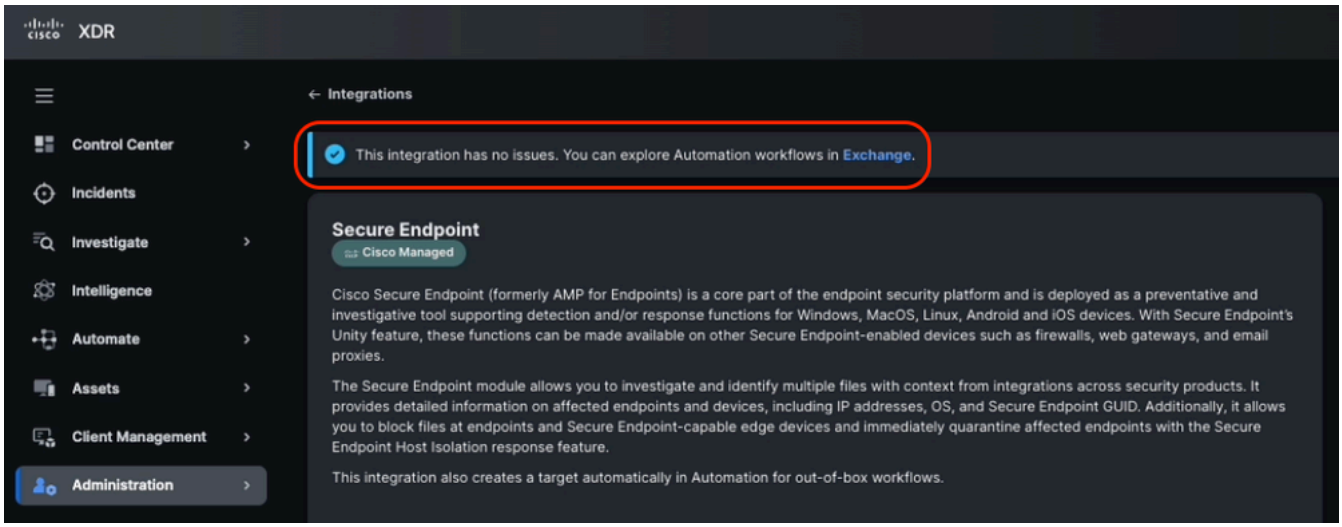
1. Cisco XDRにログインする
2. Administration > Integrations > My Integrationsの順に移動します。
3. Cisco Secure Endpointとの統合が正しく設定されていることを確認します。

Connectedで統合ステータスを確認します。



Cisco XDRからのセキュアエンドポイント統合ステータス

API設定にエラーがないことを確認します。

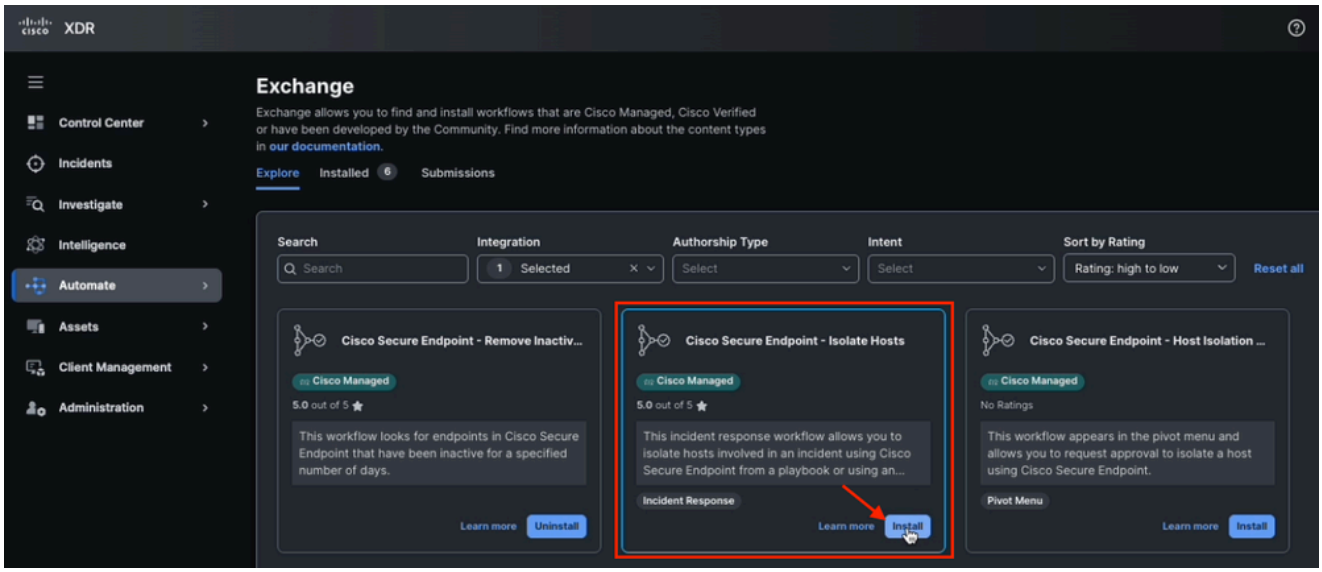


セキュアエンドポイント統合のヘルスチェック

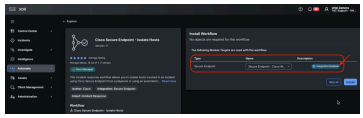
Cisco XDR Exchangeからのワークフローのインストール

ステップ3.1：エンドポイント分離ワークフローのインストール

1. Cisco XDRにログインし、Automate > Exchangeの順に選択します。
2. Cisco Secure Endpoint - Isolate Hostsという名前のワークフローを検索し、Installをクリックします。



Exchangeからのホストワークフローの分離

3. ターゲットがインストール前に使用可能であることを確認します。 

ワークフローから有効化されたモジュールターゲット

4. ワークフローをオートメーションシステムにインストールします。

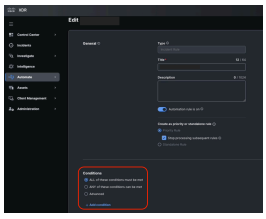
自動化ルールの作成

自動化ルールは、特定のイベントまたは定義済みのスケジュールに基づいて、ワークフローをいつ実行するかを定義する設定です。これらのルールにはオプションの条件を含めることができ、それらの条件が満たされると、関連するワークフローが自動的にトリガーされます。

ステップ4.1：自動化ルールの設定

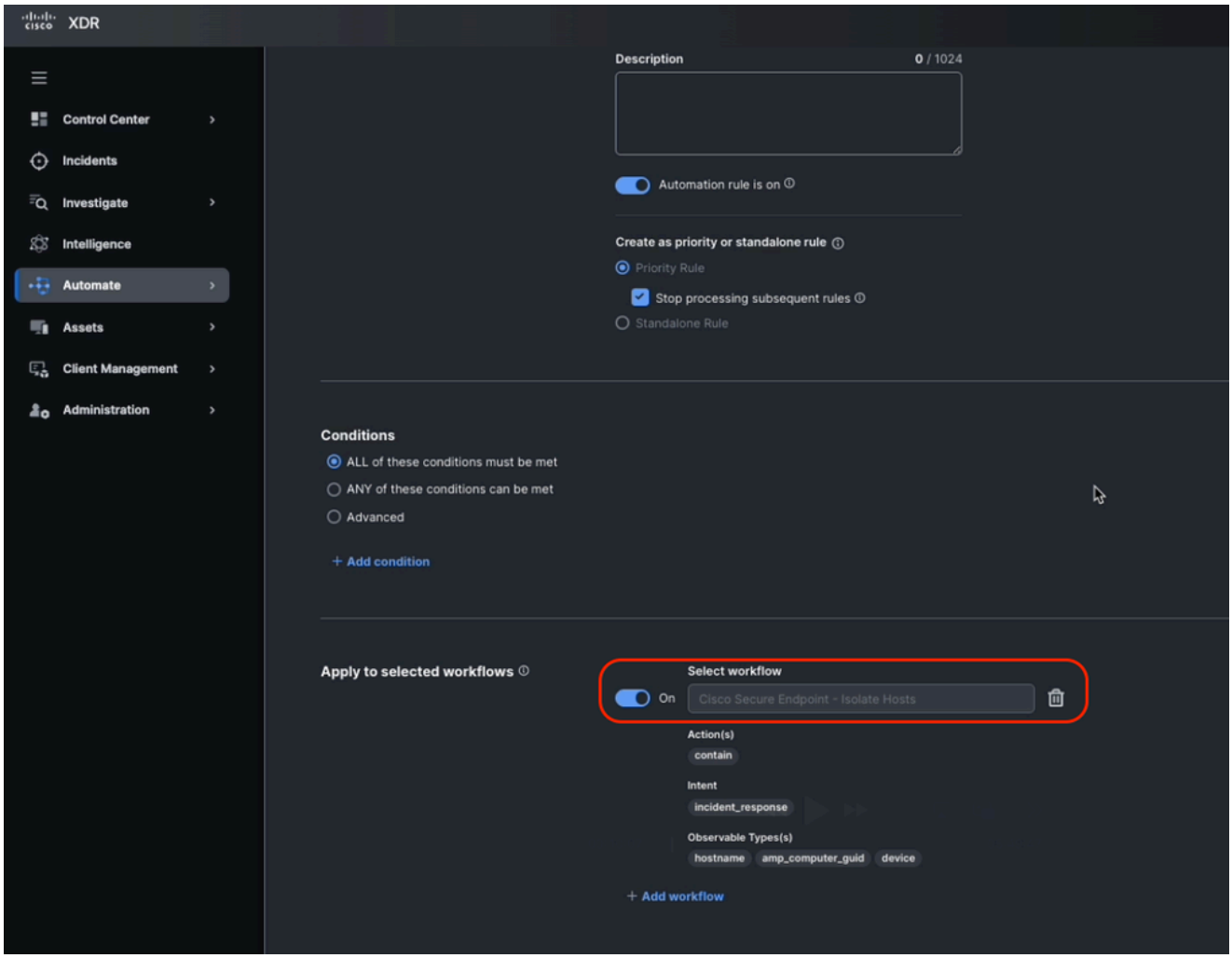
1. Automation > Triggersセクションに移動します。
2. 新しいルールを作成します。Add automation ruleをクリックして、名前を割り当てます。

トリガーからの自動化ルールの追加

3. トリガー条件を設定します。条件を空白のままにしておくと、インシデントによってこのルールがアクティブになります。必要に応じて条件をカスタマイズします。 

自動化ルールの条件

4. ルールのアクションで、以前にインストールしたCisco Secure Endpoint - Isolate Hostsワークフローを選択します。



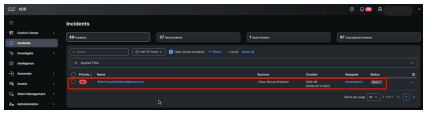
ワークフローへの自動化ルールの割り当て

5. [Save] をクリックします。

ワークフロー機能の検証

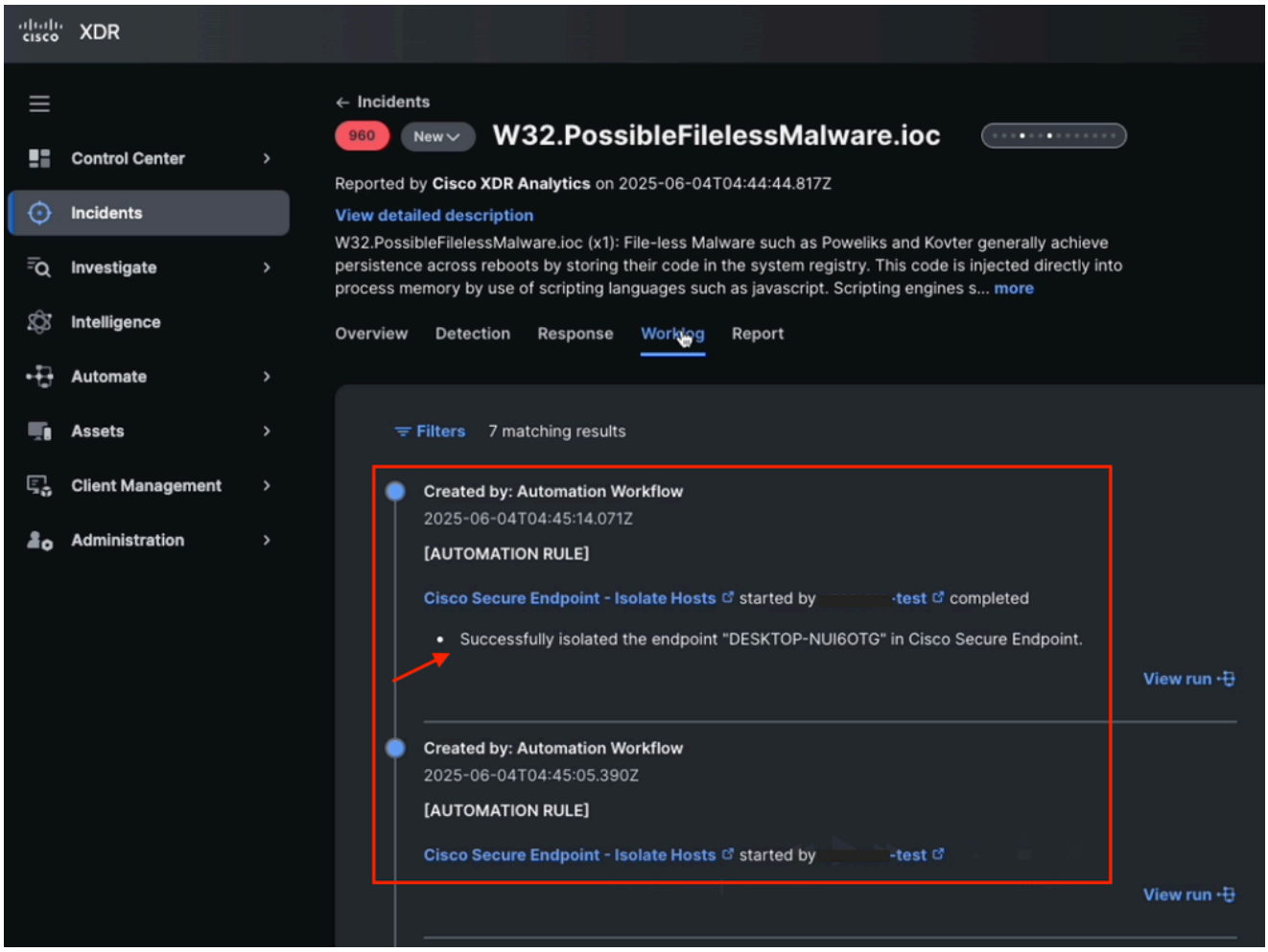
ステップ5.1：ワークフロー実行の確認

1. ルールの条件を満たすインシデントを生成または待機します。



Cisco XDRの新しいインシデントの検出

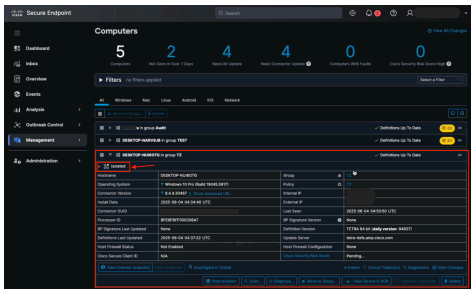
2. インシデントが作成されたら、（インシデント内の）Worklogタブを確認して、ワークフローが正常に実行されたことを確認します。



「インシデント・ワークログ」タブの情報

ステップ5.2：エンドポイントの分離の確認

1. Cisco Secure Endpointポータルにログインします。
2. Managment > Computersセクションに移動し、ターゲットエンドポイントを見つけます。



3. デバイスのステータスがIsolatedであることを確認します。

セキュアエンドポイントコンピュータからの隔離状態

4. エンドポイントが分離されていない場合は、ワークフローのログと設定を確認して、考えられる問題を特定します。

一般的な問題

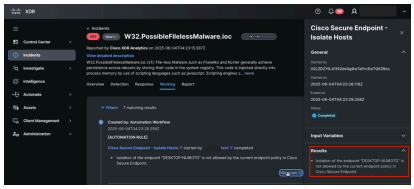
Cisco Secure Endpointで分離機能が有効になっていない

1. Cisco XDRから、Incidentsに移動し、最後のインシデントを見つけて、Worklogに移動します

。

2. 自動化ワークフローの実行後に関連するエラーが発生していないか確認します。

たとえば、セキュアエンドポイントポリシーでエンドポイントの分離が有効になっていない

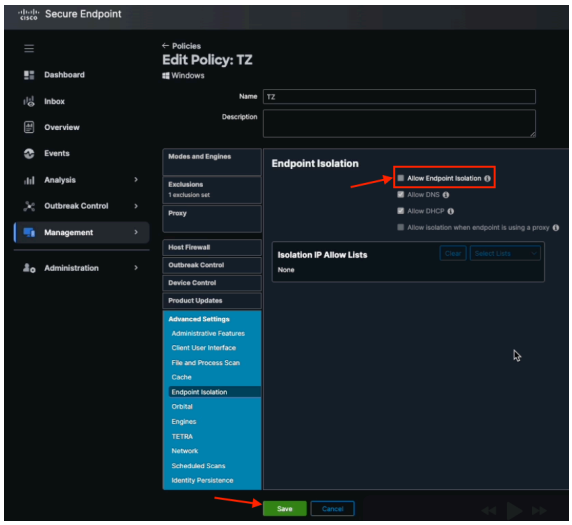


ため、エンドポイントの分離でホストを分離できませんでした。

インシデントワークログからの自動化ワークフローの結果

3. Secure Endpointから、Management > Policiesの順に移動し、該当するポリシーを選択します。

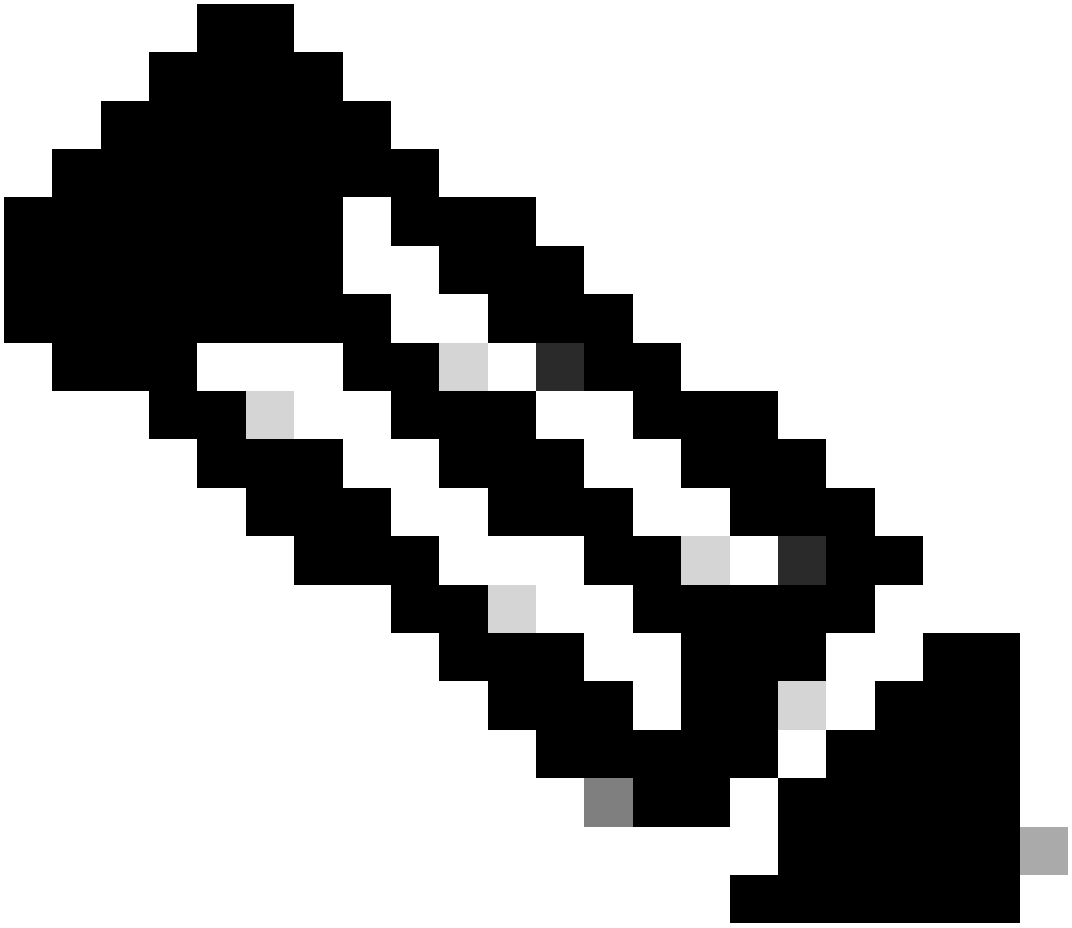
4. ポリシーが表示されたら、Advanced Settings > Ednpoint Isolationの順に移動し、Allow



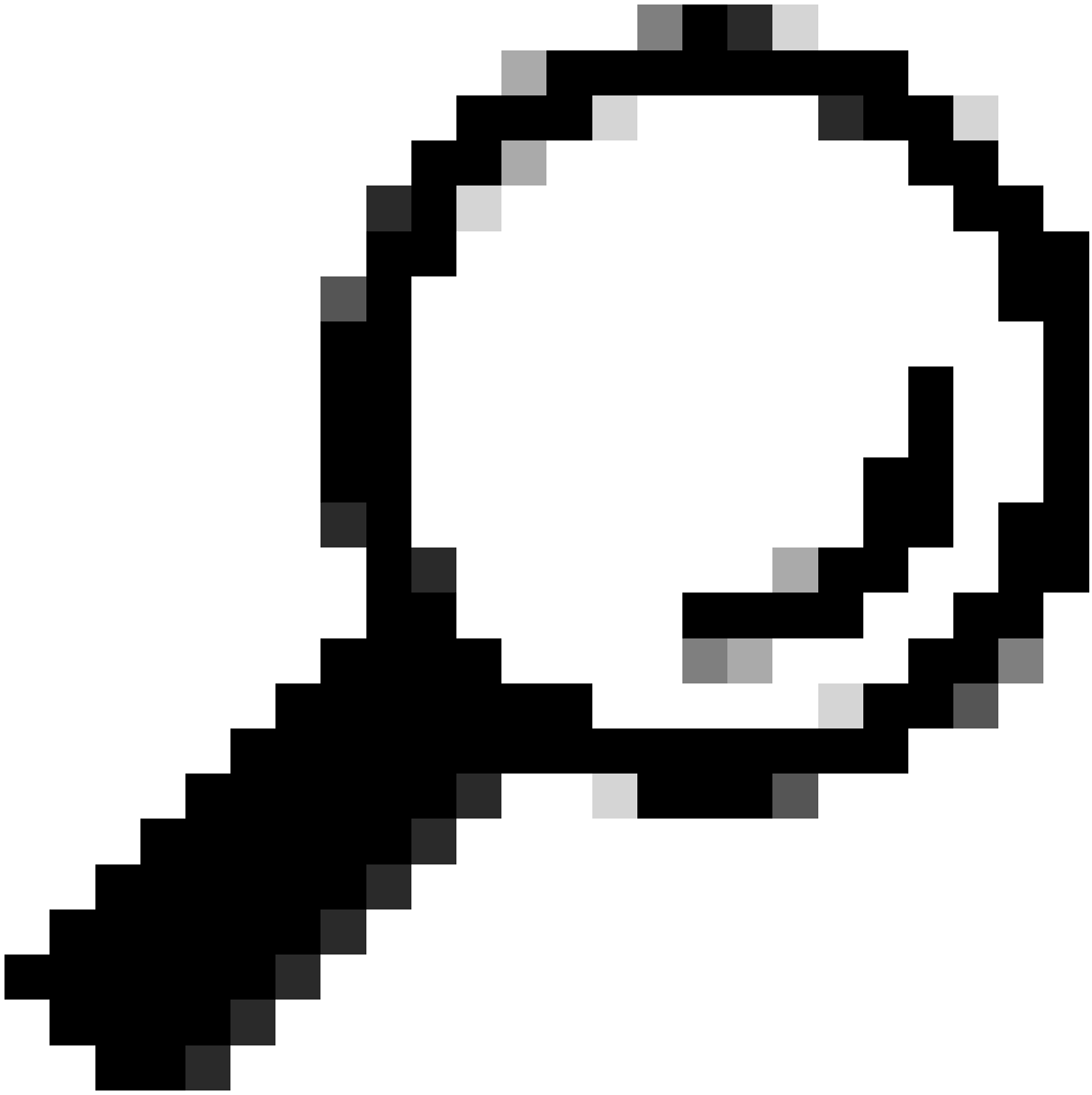
Ednpoint Isolationボックスにチェックマークを入れます。

セキュアエンドポイントポリシーでエンドポイントの分離を許可するチェックボックス

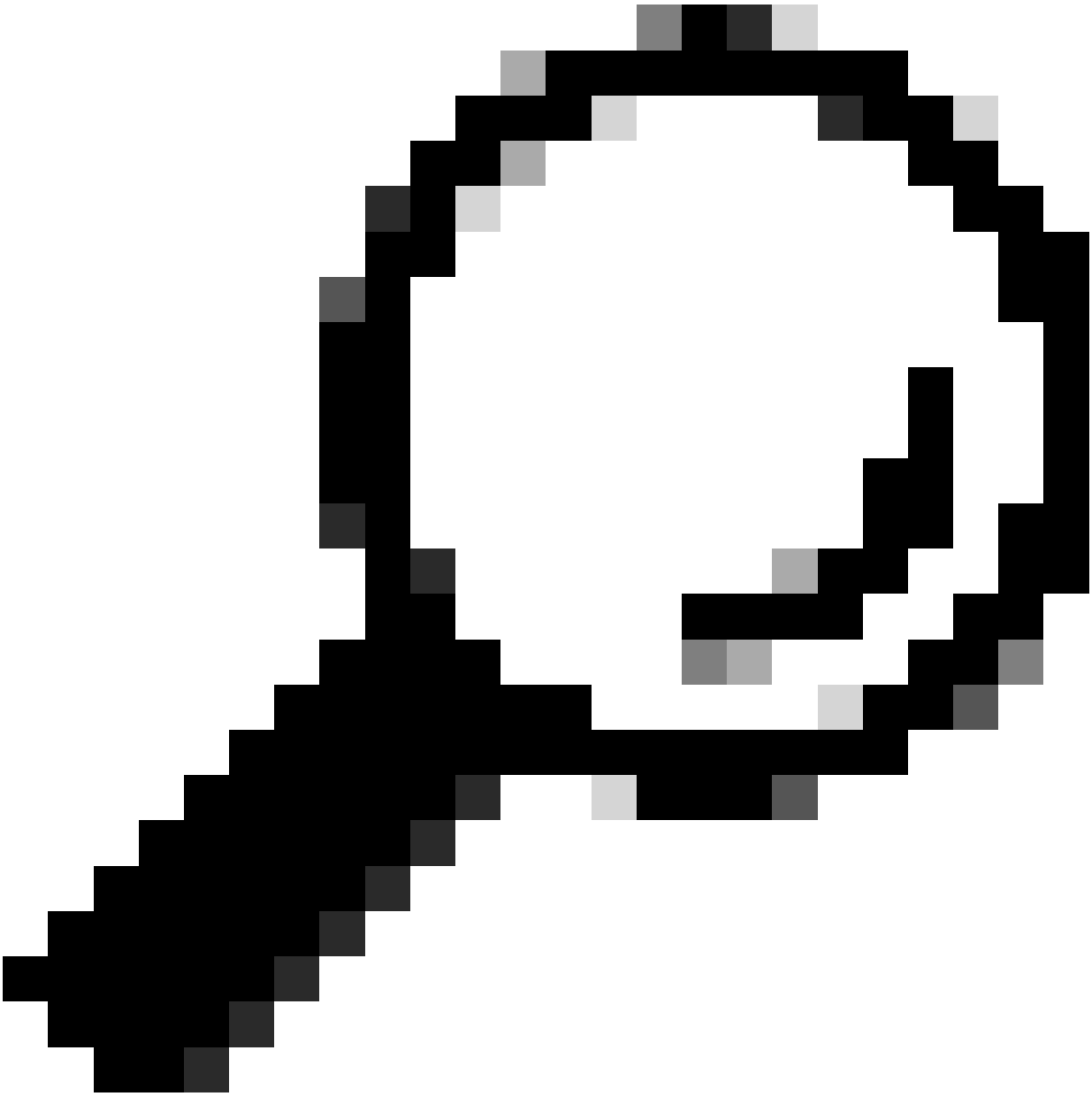
5. 「保存」をクリックします。



注：統合とワークフローを設定するために必要な管理者権限があることを確認してください。



ヒント：自動化を実稼働環境に導入する前に、制御された環境でセットアップをテストします。



ヒント：ワークフローまたは自動化ルールに対するカスタム調整を文書化します。

これらの手順を実行すると、インシデントの作成後にエンドポイントを自動的に分離するワークフローを正しく設定してアクティブ化し、セキュリティの脅威に対する迅速で効果的な対応を確保できます。

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。