XDRを使用した電子メール通知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電子メール通知を送信する自動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

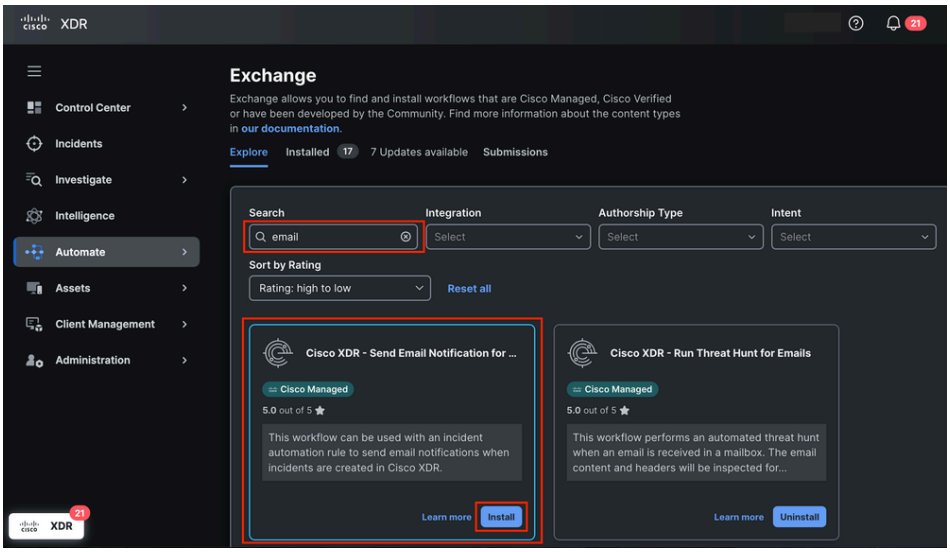
このガイドでは、インシデントが発生したときに電子メール通知を自動的に送信するワークフロ

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。手順の詳細は次のとおりです。

Cisco XDR Exchangeからのワークフローのインストール

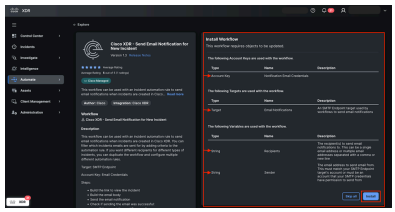
ステップ 1：エンドポイント分離ワークフローのインストール

1. Cisco XDRにログインし、Automate > Exchangeの順に選択します。
2. Cisco XDR - Send Email Notification for New Incident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。



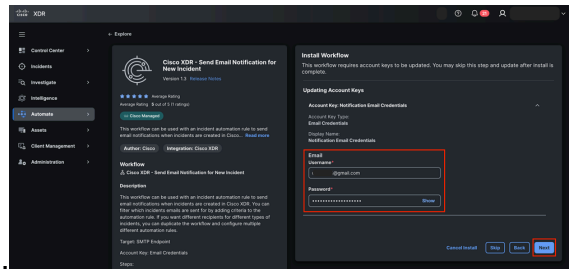
Exchangeからの電子メール通知ワークフローの送信

3. ワークフローを正しく設定するために必要な情報を確認します。



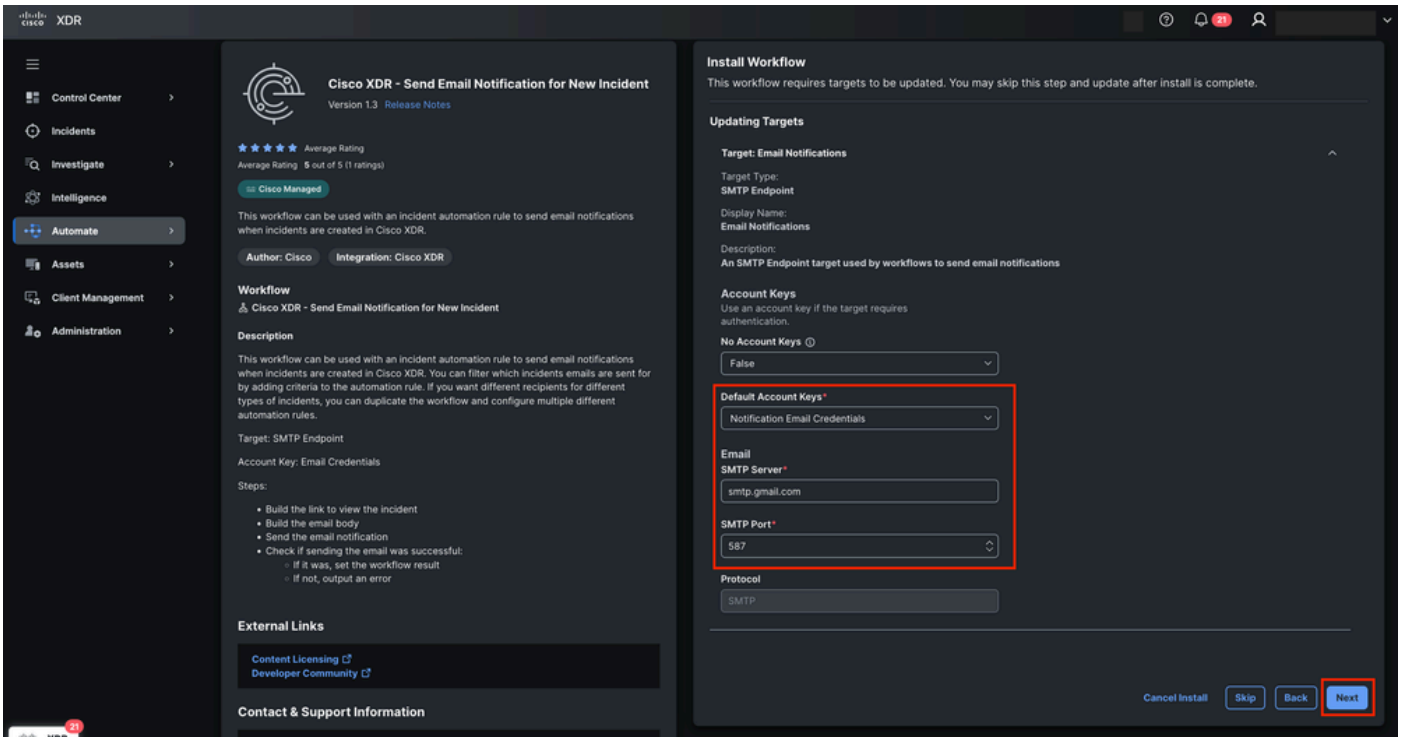
電子メール通知の送信ワークフローの概要

4. アカウントキーの入力電子メールのクレデンシャルを使用して、送信者を設定します。表示される名前はNotification Email Credentialsで、 次へ.



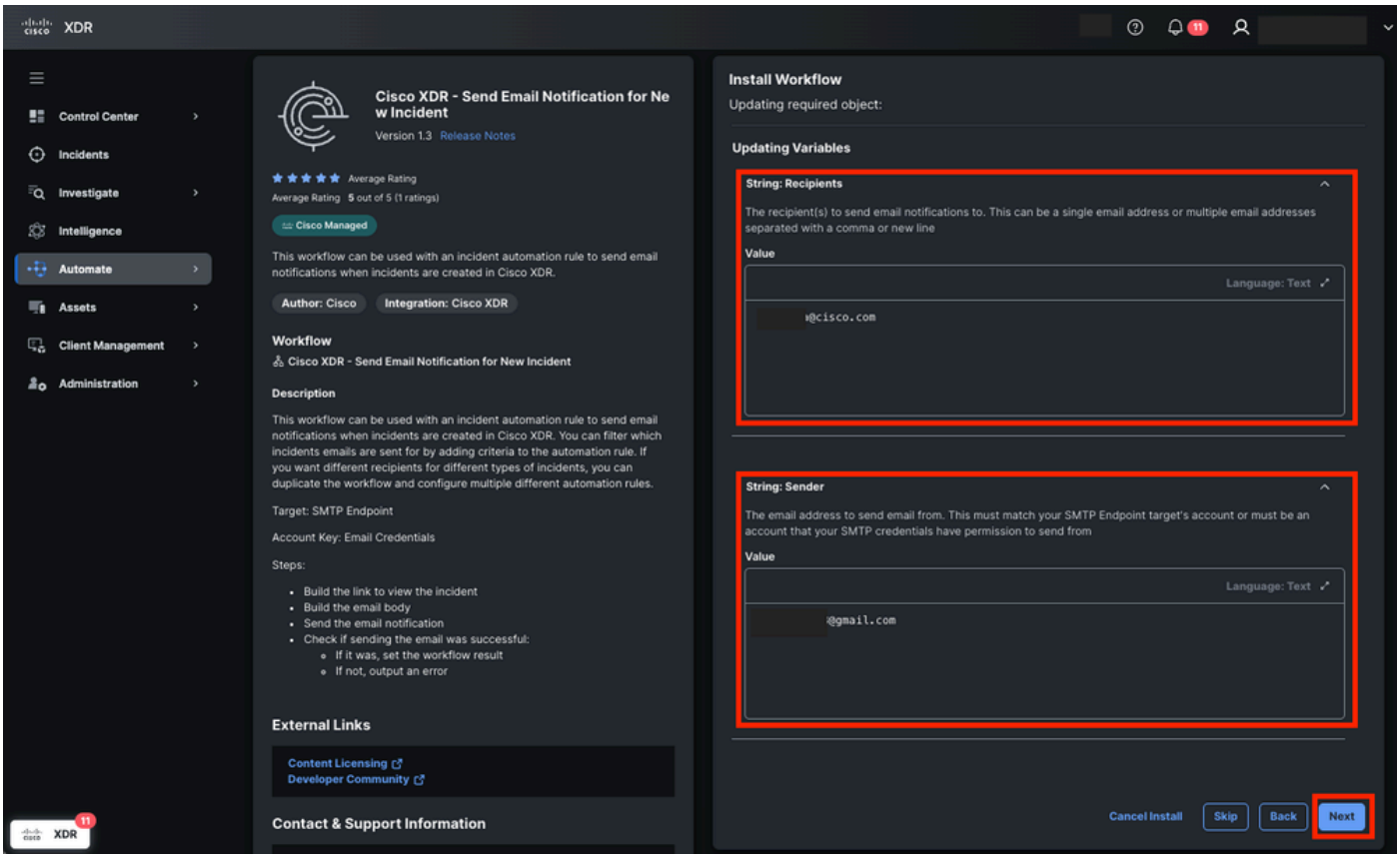
ワークフローのアカウントキー

5. ターゲット情報を次のように設定します。
   - アカウントキー：通知電子メール認証情報
   - Email
     - SMTPサーバ：smtp.gmail.com
     - SMTPポート：587



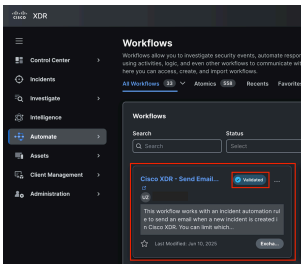
ワークフローのターゲット構成

1. [Next] をクリックします。
2. 次の変数を更新します。
    - 受信者
    - 送信者



ワークフローの変数の割り当て

8. 「次へ」をクリックします。



9. Automate > Workflowsの順に移動し、Validatedステータスを確認します。

ワークフローの検証ステータス

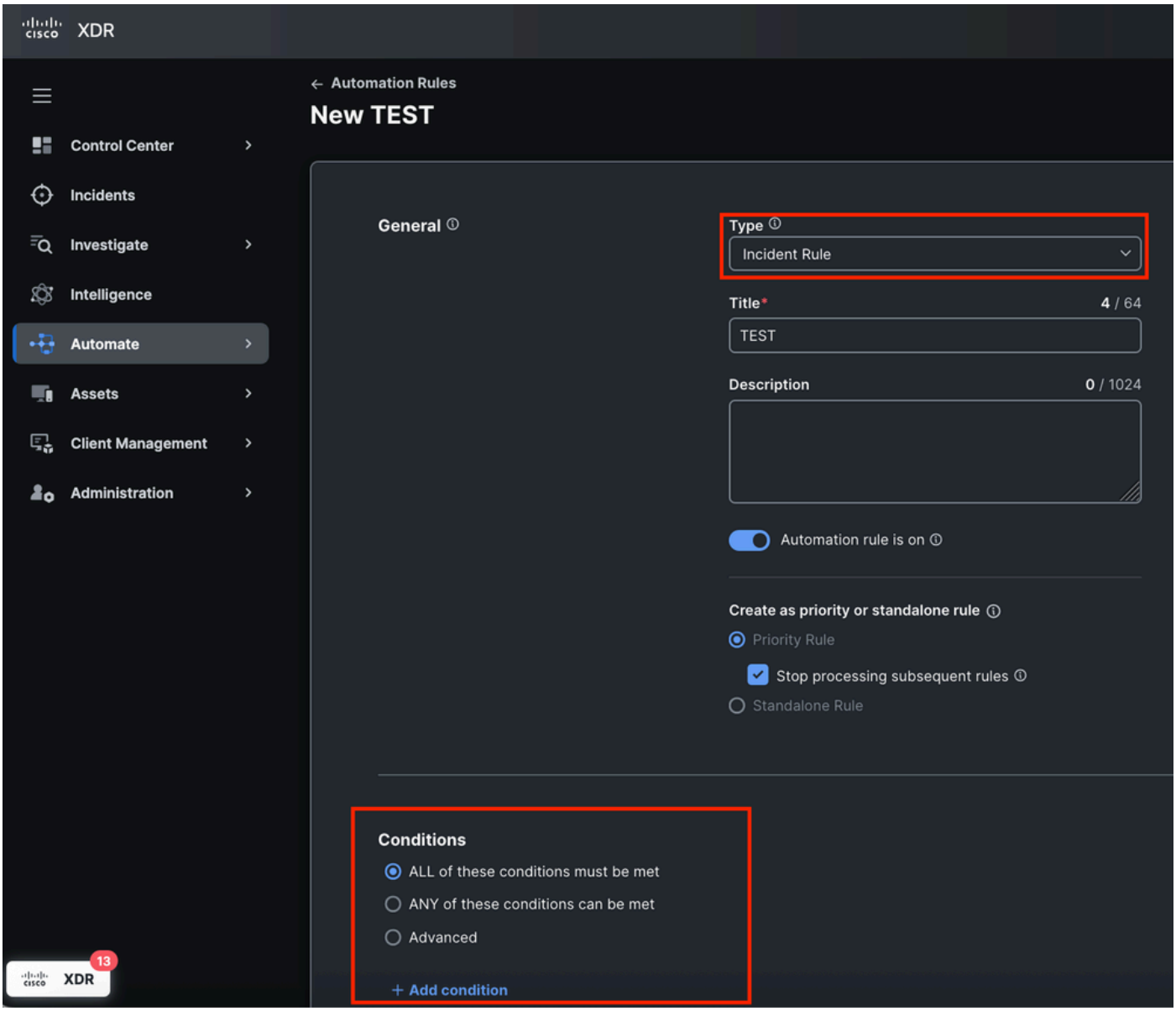
自動化ルールの作成

ステップ 2：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。

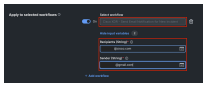
   トリガーからの自動化ルールの追加

3. インシデントルールタイプを選択し、トリガー条件を定義します。ルール条件を追加しなくても続行できます。これにより、インシデントがこのルールをアクティブ化できます。必要に応じて条件をカスタマイズします。



自動化ルールのタイプと条件

4. 自動化ルールを先ほどインストールした「Cisco XDR - Send Email Notification for New Incident」ワークフローに適用します。Recipients変数とSender変数を設定します。



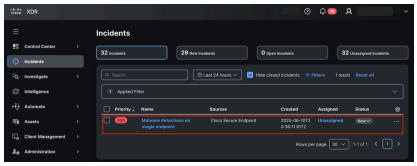
ワークフローへの自動化ルールの適用と変数の割り当て

5. ルールを保存します。

ワークフロー機能の検証

ステップ 3：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。



2. Incidentをクリックし、次にView Incident Detailをクリックします。

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

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。