Konfigurieren des automatisierten Workflows für E-Mail-Benachrichtigungen mit XDR

Inhalt

Einleitung

Dieses Dokument beschreibt die Erstellung eines automatisierten Workflows zum Senden einer E-Mail-Benachrichtigung für einen neuen Vorfall.

Voraussetzungen

Anforderungen

Es gibt keine spezifischen Anforderungen für dieses Dokument.

Verwendete Komponenten

Dieses Dokument ist nicht auf bestimmte Software- und Hardware-Versionen beschränkt.

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

Konfigurieren

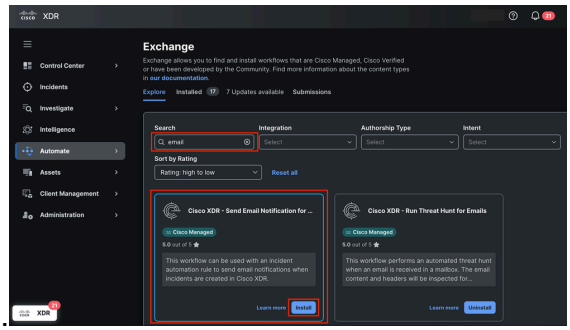
In diesem Leitfaden werden die erforderlichen Schritte zum Konfigurieren und Aktivieren eines Workflows beschrieben, mit dem bei einem Vorfall automatisch eine E-Mail-Benachrichtigung

gesendet wird. Die einzelnen Schritte werden wie folgt beschrieben.

Workflow aus Cisco XDR Exchange installieren

Schritt 1: Installieren des Workflows für die Endpunktisolierung

1. Melden Sie sich bei Cisco XDR an, und navigieren Sie zu Automate > Exchange.
2. Suchen Sie nach dem Workflow mit dem Namen Cisco XDR - Send Email Notification for New Incident, und klicken Sie auf Install (Installieren).

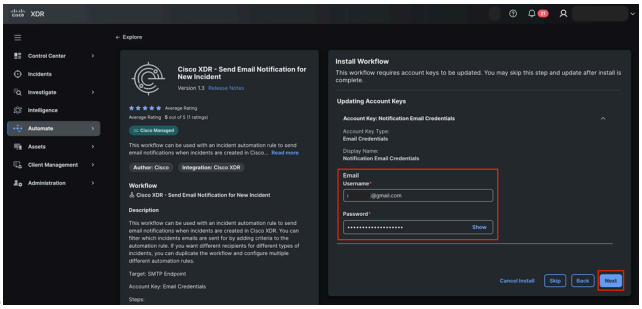


E-Mail-Benachrichtigungs-Workflow aus Exchange senden

3. Überprüfen Sie die erforderlichen Informationen, um den Workflow richtig zu konfigurieren.

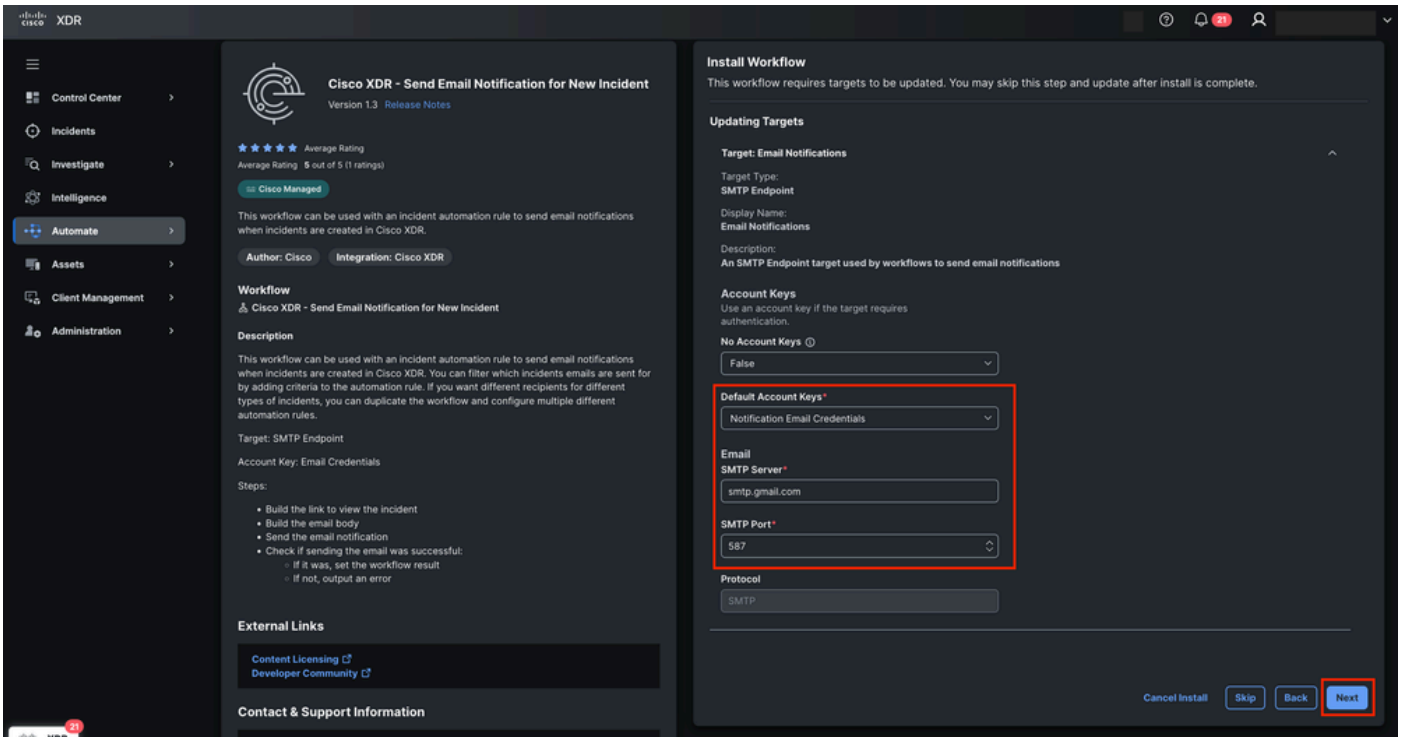
Übersicht über den E-Mail-Benachrichtigungsworkflow senden

4. Füllen Sie die Kontoschlüssel aus.mit den E-Mail-Anmeldeinformationen, um den Absender festzulegen. Der angezeigte Name lautet E-Mail-Anmeldeinformationen für Benachrichtigungen, und klicken Sie auf Weiter.



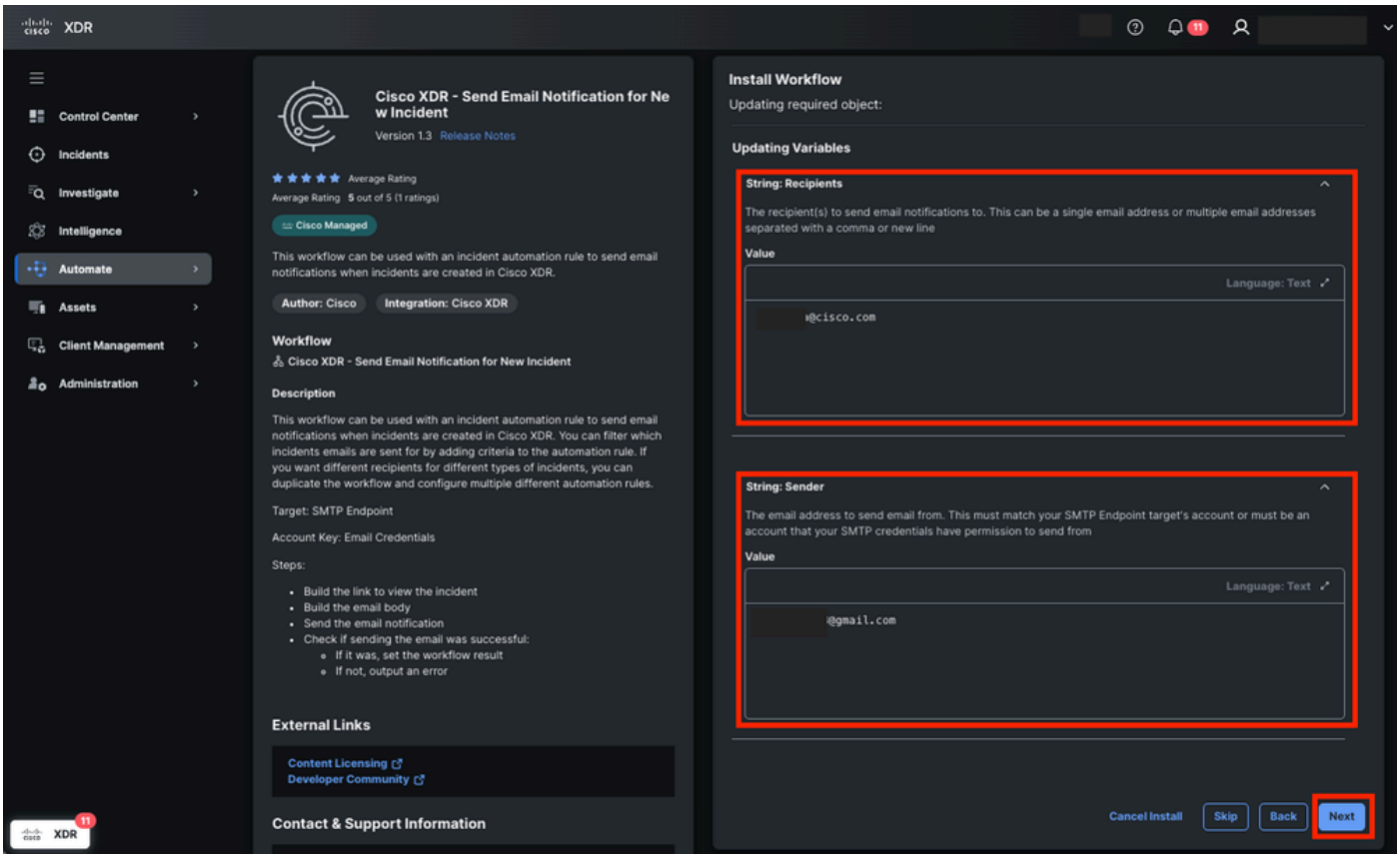
Kontoschlüssel für Workflow

5. Konfigurieren Sie die Zielinformationen wie folgt:
   - Kontoschlüssel: Benachrichtigungs-E-Mail-Anmeldeinformationen
   - E-Mail
     - SMTP-Server: smtp.gmail.com
     - SMTP-Port: 587



Zielkonfiguration für Workflow

1. Klicken Sie auf Next (Weiter).
2. Aktualisieren Sie die Variable für:
    - Empfänger
    - Absender



Variablen für Workflow zuweisen

8. Klicken Sie auf Weiter.

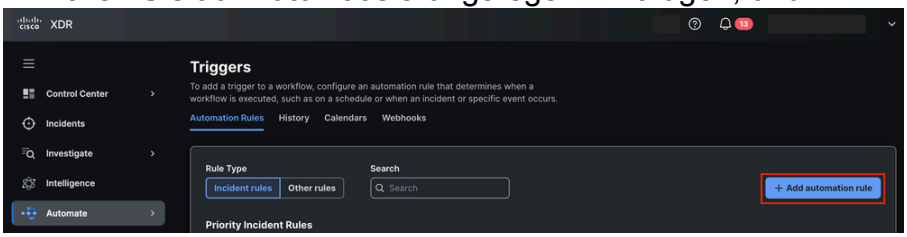
9. Navigieren Sie zu "Automatisieren" > "Workflows", um den Status Validiert zu überprüfen. 

Workflow-Validierungsstatus

Erstellen einer Automatisierungsregel

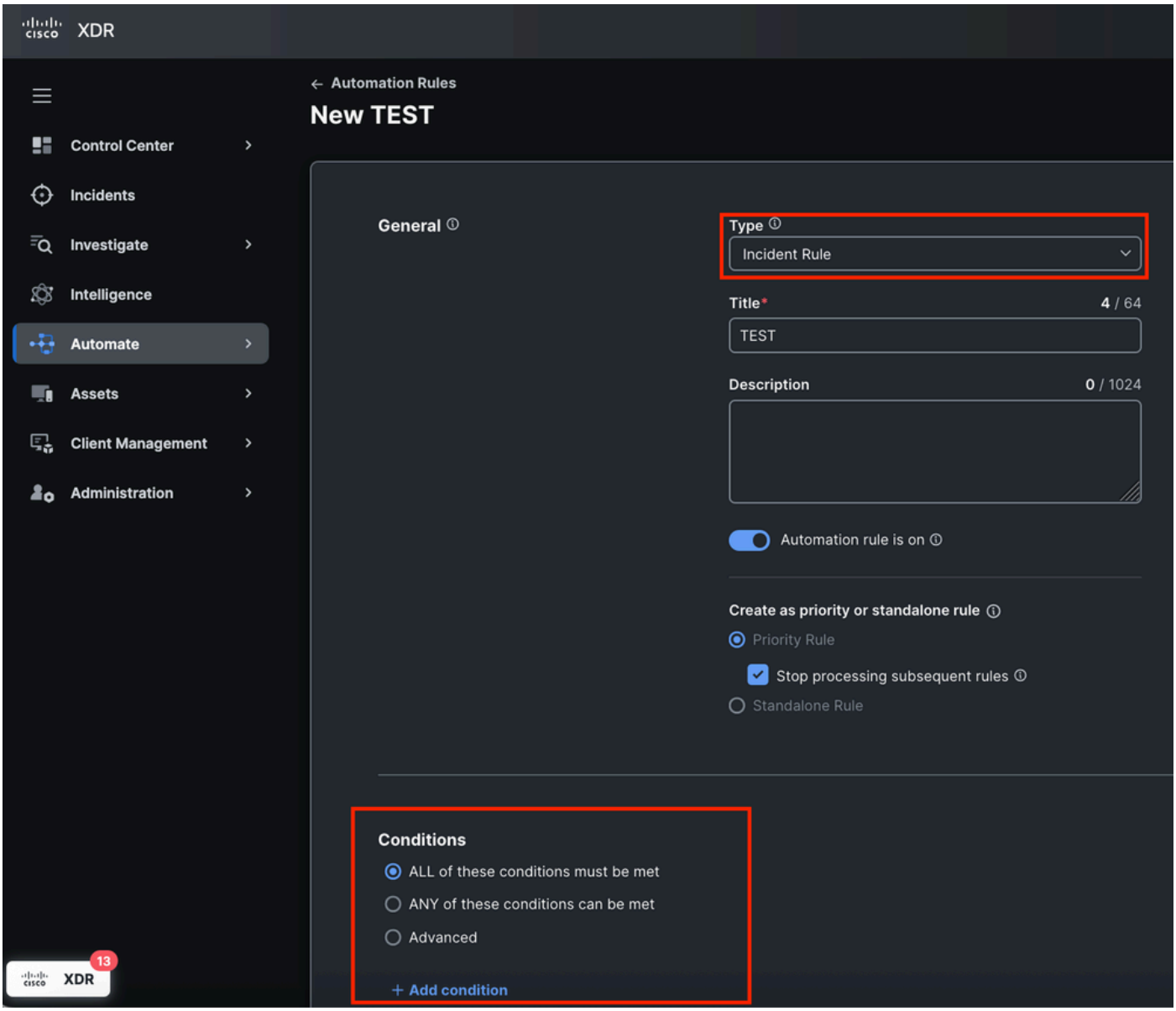
Schritt 2: Konfigurieren einer Automatisierungsregel

1. Navigieren Sie zum Abschnitt Automatisierung > Trigger.
2. Erstellen Sie eine neue Regel. Klicken Sie auf Automatisierungsregel hinzufügen, und weisen Sie einen Namen zu.



Automatisierungsregel aus Triggern hinzufügen

3. Wählen Sie den Typ der Vorfallregel, und definieren Sie die Auslösebedingungen. Sie können fortfahren, ohne eine Regelbedingung hinzufügen zu müssen, die sicherstellt, dass jeder Vorfall diese Regel aktiviert. Passen Sie ggf. die Bedingungen an.



Typ und Bedingungen der Automatisierungsregel

4. Wenden Sie die Automatisierungsregel auf den zuvor installierten Cisco XDR - Send Email Notification for New Incident workflow an. Legen Sie die Variablen Empfänger und Absender fest.

Automatisierungsregel auf Workflow anwenden und Variablen zuweisen

5. Speichern Sie die Regel.

Workflow-Funktionalität überprüfen

Schritt 3: Workflow-Ausführung überprüfen

1. Generieren Sie einen Vorfall, der die Bedingungen der Regel erfüllt, oder warten Sie diesen.

   Neuer Vorfall in Cisco XDR erkannt

2. Klicken Sie auf Incident und dann auf Incident-Details anzeigen.

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

Der Name des ersten Vorfalls wird auf Grundlage der ersten Erkennung generiert. Sie kann sich jedoch ändern, wenn zusätzliche Erkennungen auftreten oder neue Informationen den Vorfall bereichern.

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.