Configurare il flusso di lavoro automatico di notifica e-mail con XDR

Sommario

Introduzione

In questo documento viene descritto come creare un flusso di lavoro automatico per inviare una notifica e-mail per un nuovo incidente.

Prerequisiti

Requisiti

Nessun requisito specifico previsto per questo documento.

Componenti usati

Il documento può essere consultato per tutte le versioni software o hardware.

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Configurazione

In questa guida vengono illustrati in dettaglio i passaggi necessari per configurare e attivare un flusso di lavoro per l'invio automatico di una notifica e-mail quando si verifica un evento imprevisto.

I passaggi sono descritti di seguito.

Installare il flusso di lavoro da Cisco XDR Exchange

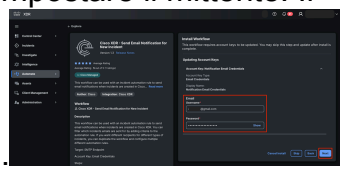
Passaggio 1. Installare il flusso di lavoro Isolamento endpoint

1. Accedere a Cisco XDR e selezionare Automate > Exchange.
2. Cercare il flusso di lavoro Cisco XDR - Send Email Notification for New Incident (Invia notifica tramite posta elettronica per nuovo incidente), quindi fare clic su Install (Installa). 

   Invia flusso di lavoro di notifica tramite posta elettronica da Exchange

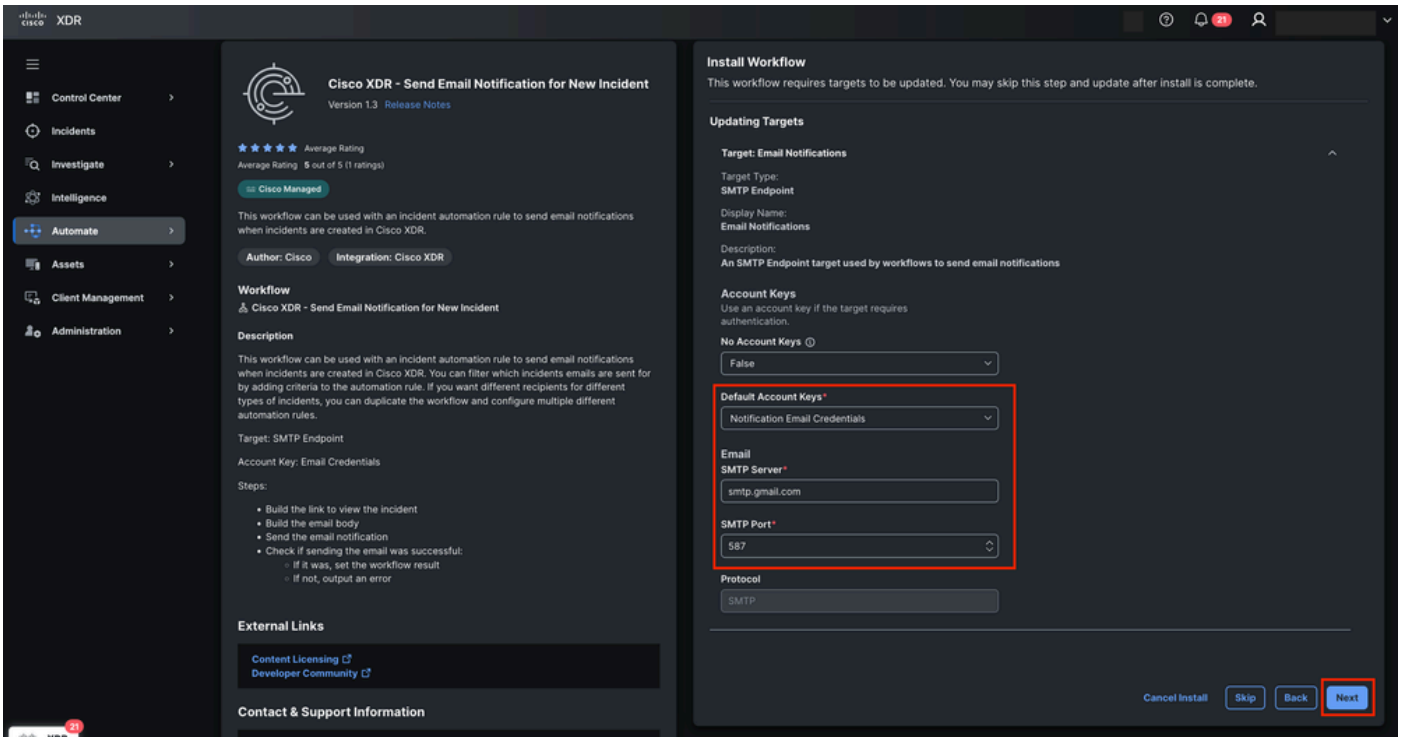
3. Controllare le informazioni necessarie per configurare correttamente il flusso di lavoro. 

   Panoramica sul flusso di lavoro Invia notifica tramite posta elettronica

4. Inserisci le chiavi del contocon le credenziali di posta elettronica per impostare il mittente. Il nome visualizzato è Credenziali e-mail di notifica e fare clic su Avanti. 

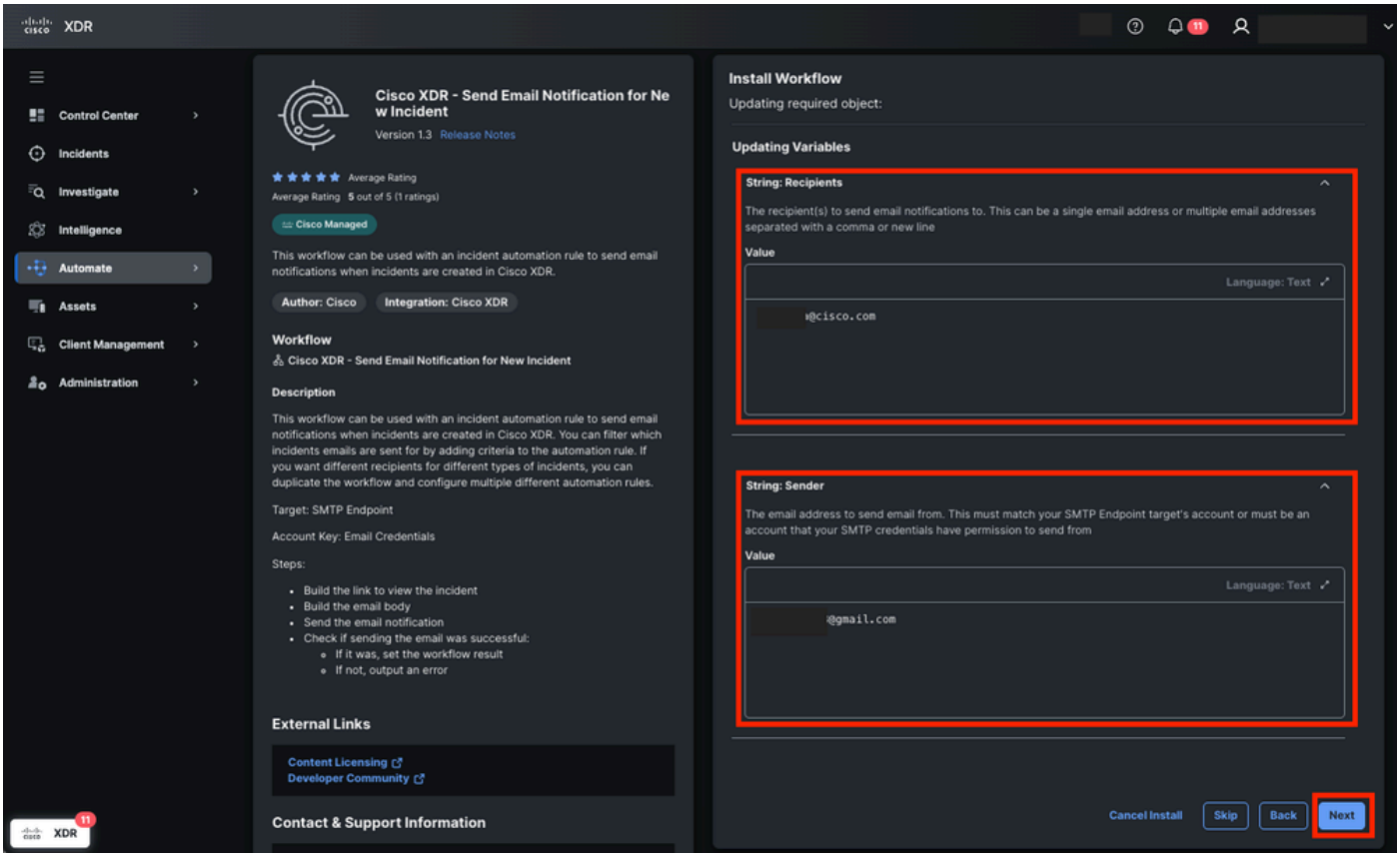
   Chiavi account per il flusso di lavoro

5. Configurare le informazioni sulla destinazione con:
   - Chiavi account: credenziali posta elettronica di notifica
   - Email
     - Server SMTP: smtp.gmail.com
     - Porta SMTP: 587



Configurazione di destinazione per il flusso di lavoro

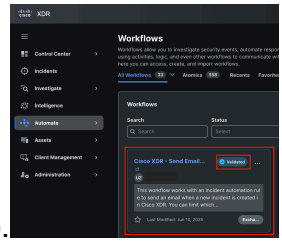
1. Fare clic su Next (Avanti).
2. Aggiorna la variabile per:
    - Destinatari
    - Mittente



Assegna variabili per flusso di lavoro

8. Fare clic su Avanti.

9. Passare a Automatizza > Flussi di lavoro per controllare lo stato Convalidato.



Stato convalida flusso di lavoro

Creare una regola di automazione

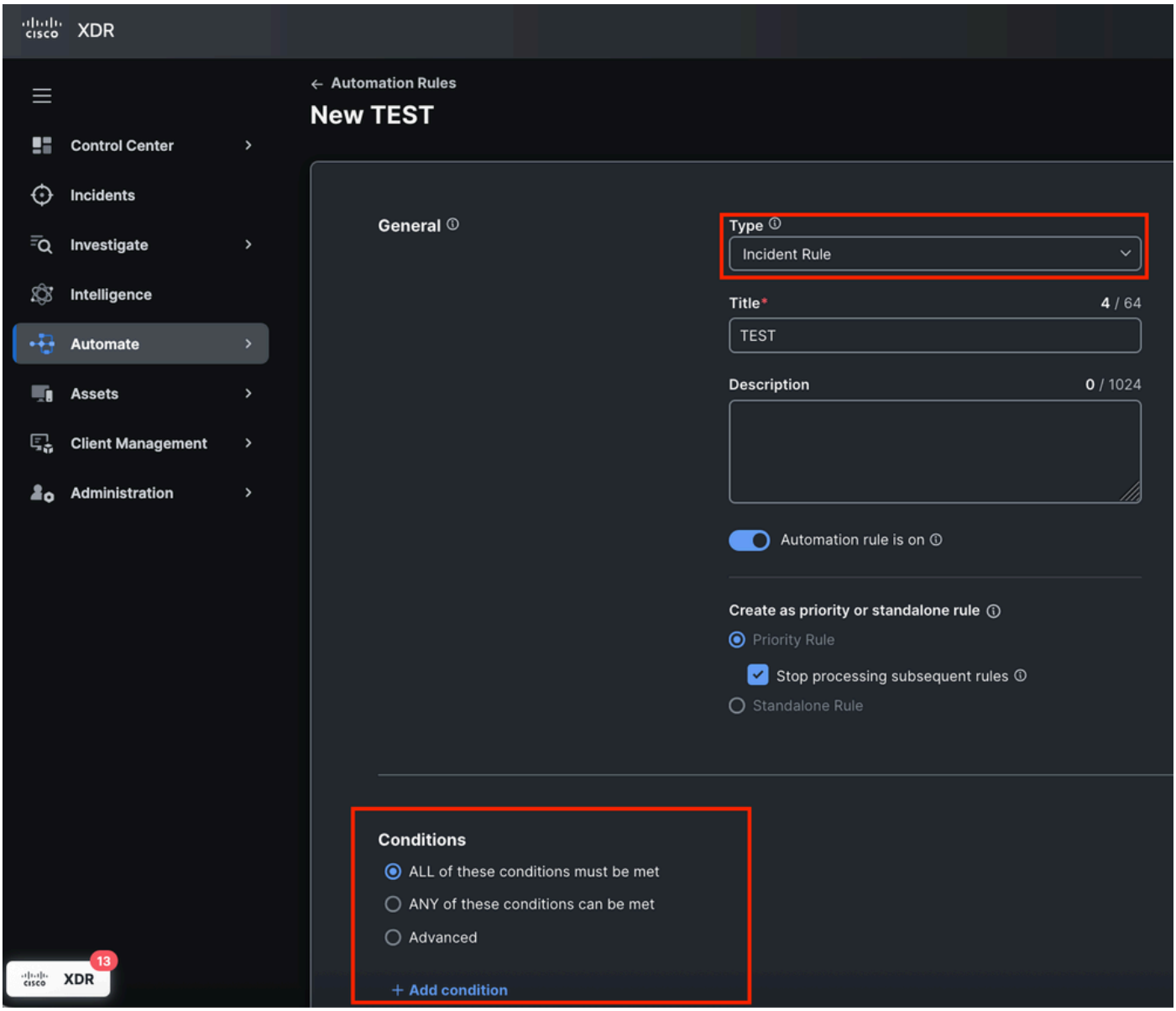
Passaggio 2. Configurare una regola di automazione

1. Passare alla sezione Automazione > Trigger.
2. Crea una nuova regola. Fare clic su Aggiungi regola di automazione e assegnare un nome.

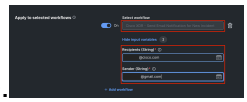
Aggiungi regola di automazione da trigger

3. Selezionare il tipo di regola di incidente e definire le condizioni di attivazione. È possibile

procedere senza la necessità di aggiungere una condizione della regola, che assicura che qualsiasi evento imprevisto attivi questa regola. Se necessario, personalizzare le condizioni.



Tipo di regola e condizioni di automazione

4. Applicare la regola di automazione al flusso di lavoro Cisco XDR - Send Email Notification for New Incident installato in precedenza. Impostare le variabili Destinatari e Mittente. 

Applica la regola di automazione al flusso di lavoro e assegna variabili

5. Salvare la regola.

Convalida funzionalità flusso di lavoro

Passaggio 3. Verifica dell'esecuzione del flusso di lavoro

1. Generare o attendere un evento imprevisto che soddisfi le condizioni della regola. 

2. Fare clic su Incidente e quindi su Visualizza dettagli incidente.

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

il nome iniziale dell'incidente è generato in base al primo rilevamento; tuttavia, può cambiare se si verificano ulteriori rilevamenti o se nuove informazioni arricchiscono l'incidente.

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).