Configuración del flujo de trabajo automatizado de notificaciones por correo electrónico con XDR

Contenido

Introducción

Este documento describe cómo crear un flujo de trabajo automatizado para enviar una notificación por correo electrónico para un nuevo incidente.

Prerequisites

Requirements

No hay requisitos específicos para este documento.

Componentes Utilizados

Este documento no tiene restricciones específicas en cuanto a versiones de software y de hardware.

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Configurar

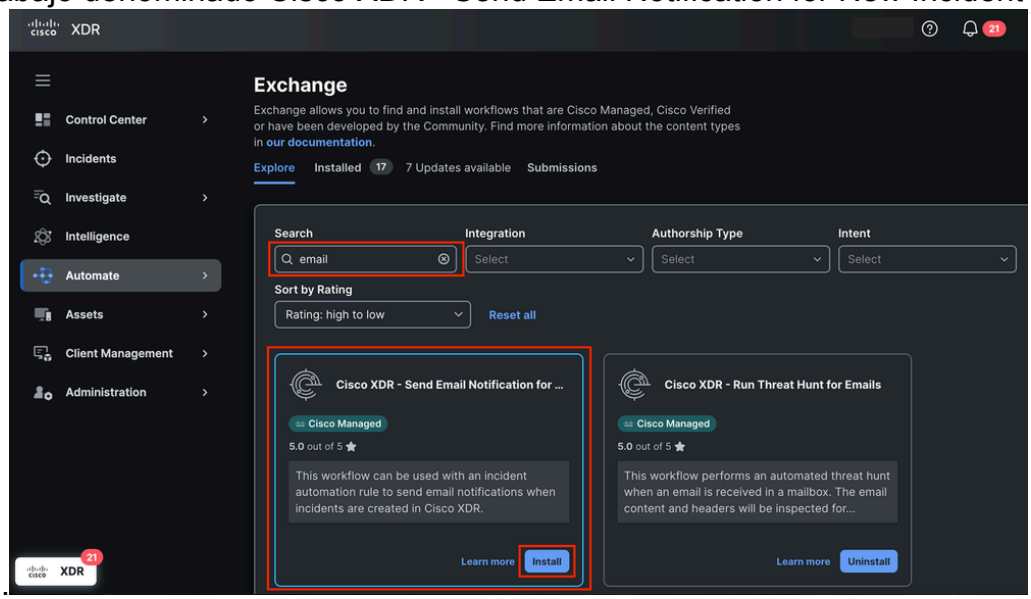
Esta guía detalla los pasos necesarios para configurar y activar un flujo de trabajo para enviar

automáticamente una notificación por correo electrónico cuando se produce un incidente. Los pasos se detallan a continuación.

Instalación del flujo de trabajo desde Cisco XDR Exchange

Paso 1. Instalación del flujo de trabajo de aislamiento de terminales

1. Inicie sesión en Cisco XDR y navegue hasta Automatizar > Exchange.
2. Busque el flujo de trabajo denominado Cisco XDR - Send Email Notification for New Incident y haga clic en Install.

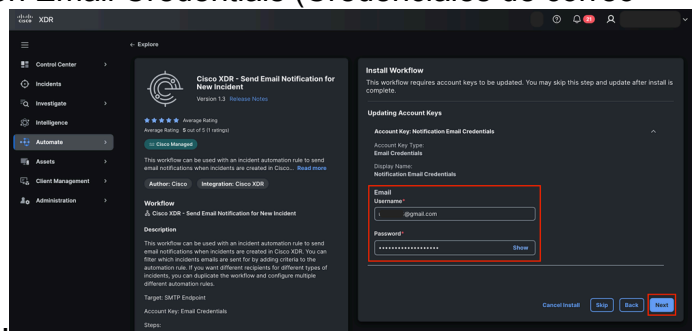


Enviar flujo de trabajo de notificación por correo electrónico desde Exchange

3. Compruebe la información necesaria para configurar el flujo de trabajo correctamente.

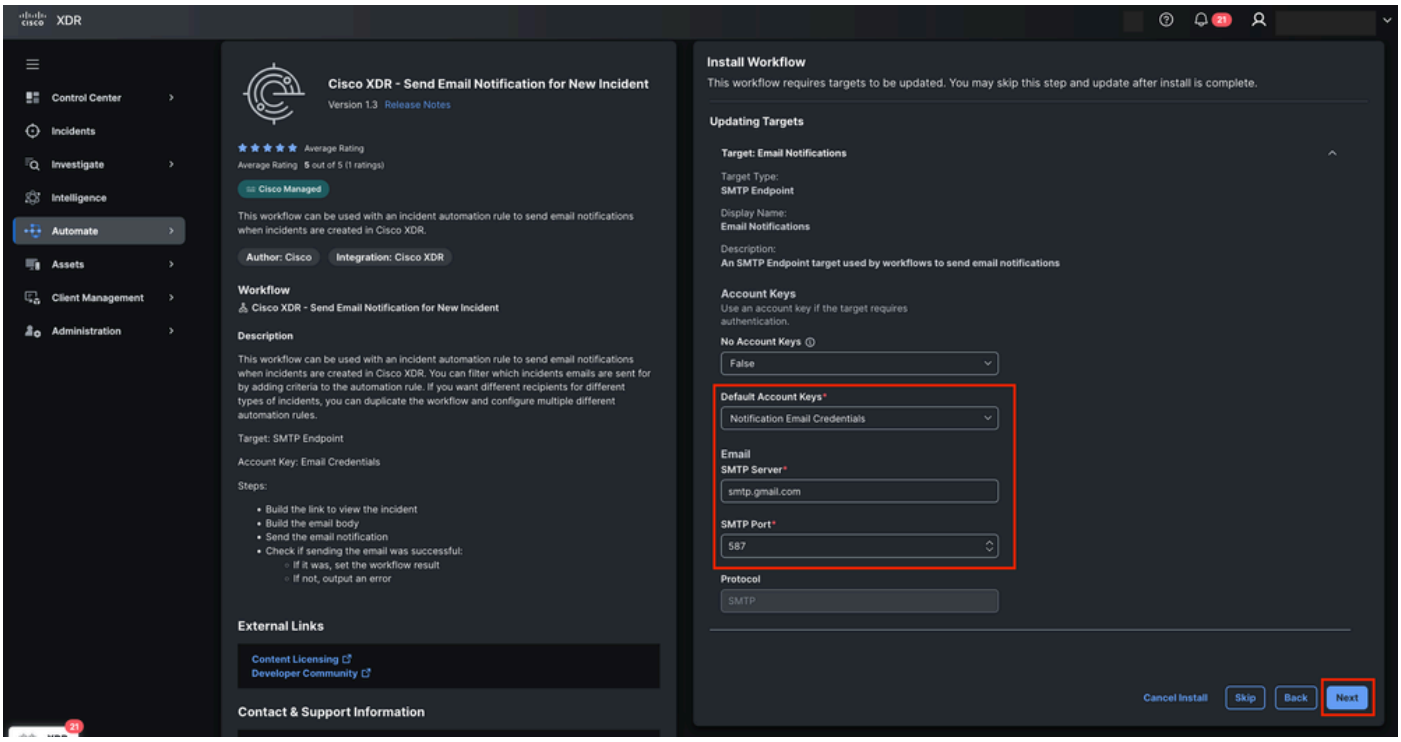
Enviar flujo de trabajo de notificación por correo electrónico

4. Rellene las claves de cuentacon las credenciales de correo electrónico para establecer el remitente. El nombre mostrado es Notification Email Credentials (Credenciales de correo electrónico de notificación) y Click Siguiente.



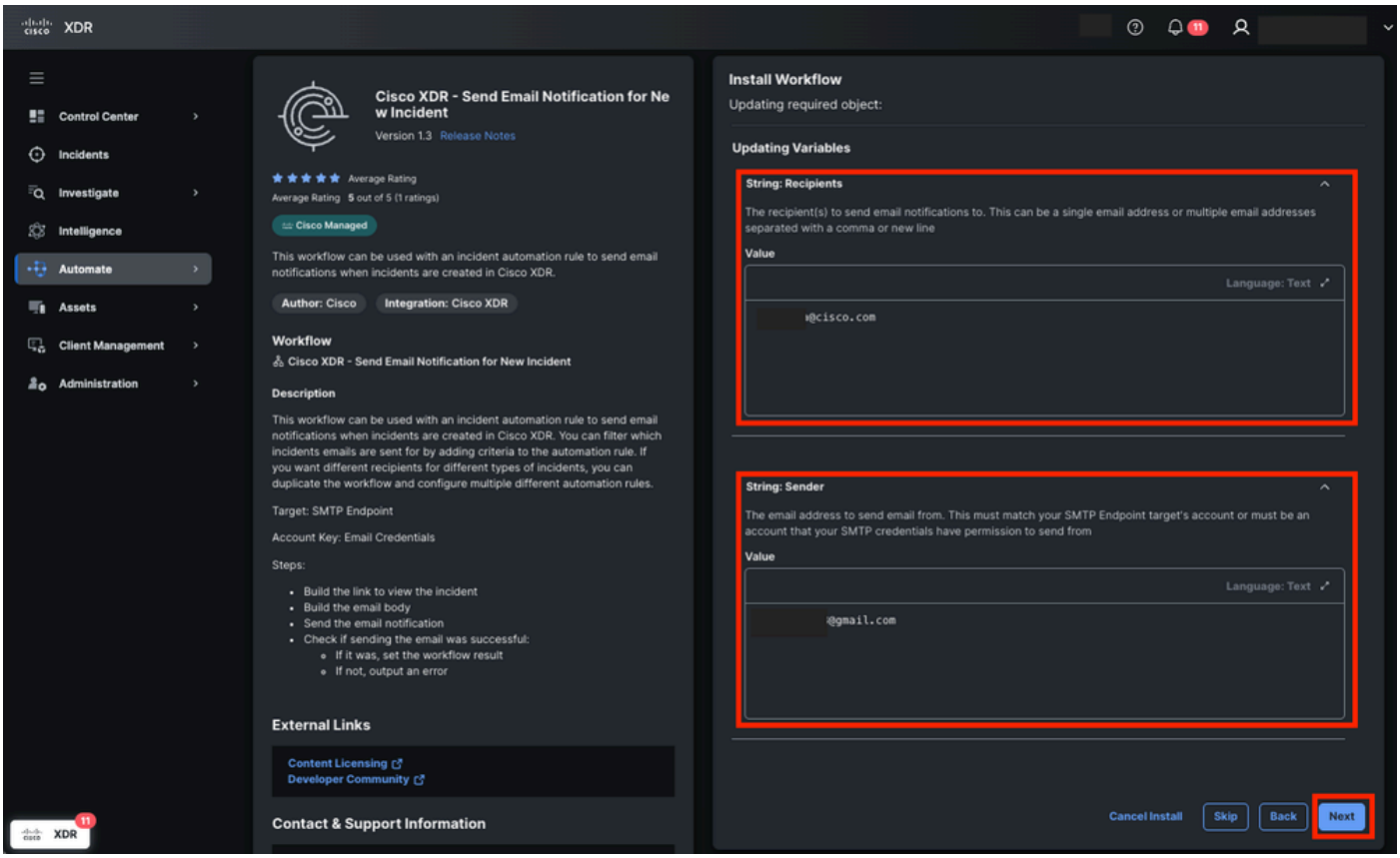
Claves de cuenta para flujo de trabajo

5. Configure la información de destino con:
   - Claves de cuenta: credenciales de correo electrónico de notificación
   - Correo electrónico
     - Servidor SMTP: smtp.gmail.com
     - Puerto SMTP: 587



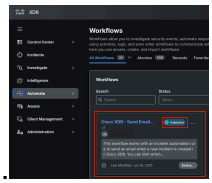
Configuración de destino para flujo de trabajo

1. Haga clic en Next (Siguiente).
2. Actualice la variable para:
    - Destinatarios
    - Remitente



Asignar variables para flujo de trabajo

8. Haga clic en Siguiente.

9. Acceda a Automatización > Flujos de Trabajo para comprobar el estado Validado. 

Estado de flujo de trabajo validado

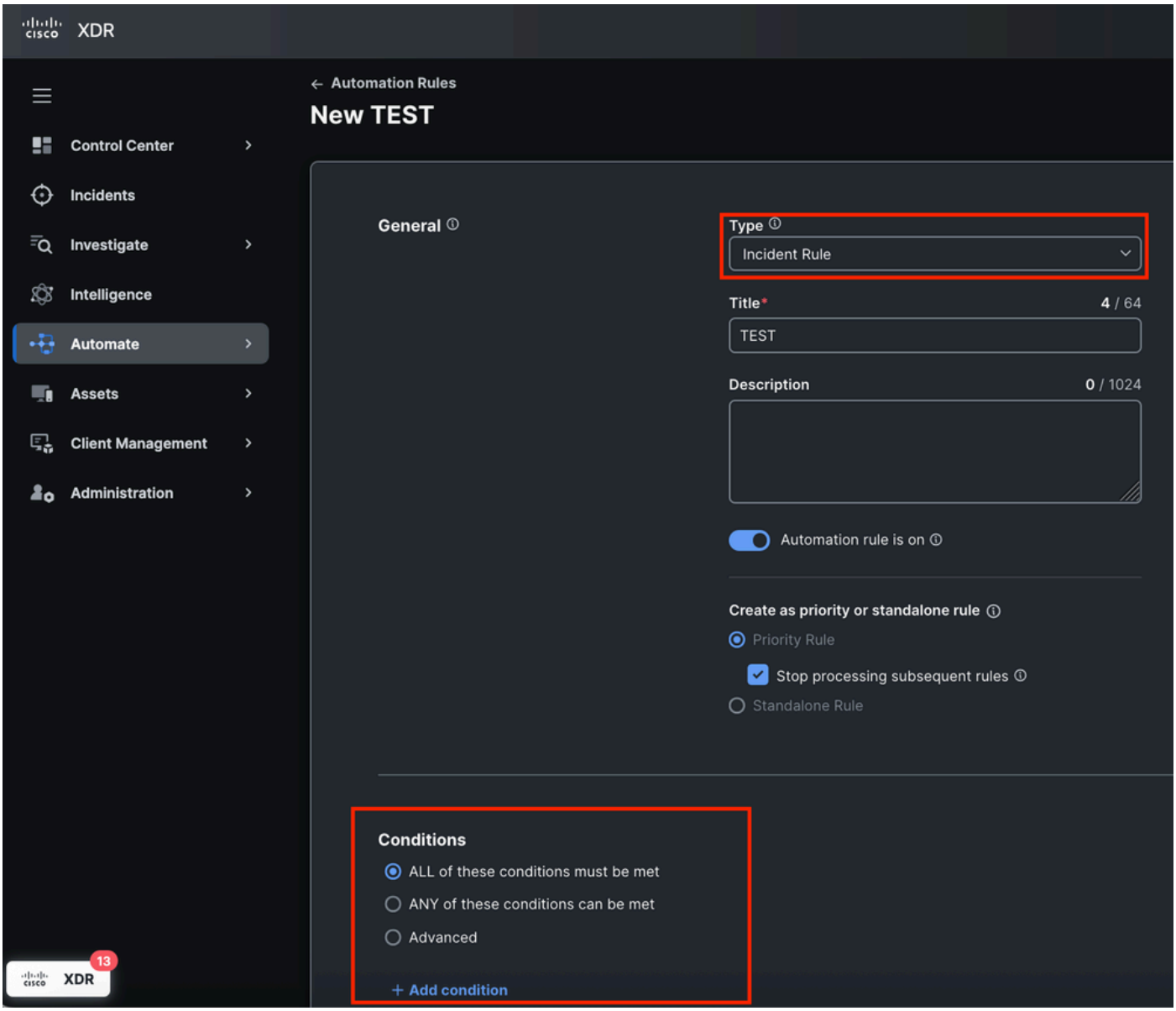
Crear una regla de automatización

Paso 2. Configuración de una regla de automatización

1. Vaya a la sección Automatización > Desencadenadores.
2. Cree una nueva regla. Haga clic en Agregar regla de automatización y asigne un nombre. [redacted]

   Agregar regla de automatización desde desencadenadores

3. Seleccione Incident Rule y defina las condiciones del disparador. Puede continuar sin necesidad de agregar una condición de regla, lo que garantiza que cualquier incidente active esta regla. Personalice las condiciones si es necesario.



Tipo y condiciones de regla de automatización

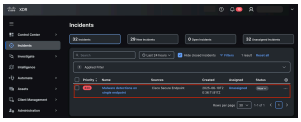
4. Aplique la regla de automatización al flujo de trabajo Cisco XDR - Send Email Notification for New Incident que instaló anteriormente. Establezca las variables Recipients y Sender. 

Aplicar la regla de automatización al flujo de trabajo y asignar variables

5. Guarde la regla.

Validar funcionalidad de flujo de trabajo

Paso 3. Verificar la ejecución del flujo de trabajo

1. Generar o esperar un incidente que cumpla las condiciones de la regla. 

   Se ha detectado un nuevo incidente en Cisco XDR

2. Haga clic en Incidente y luego en Ver detalles del 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

El nombre del incidente inicial se genera en función de la primera detección; sin embargo, puede cambiar si se producen detecciones adicionales o si la nueva información enriquece el incidente.

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).