Configurar Fluxo de Trabalho Automatizado de Notificação por Email com XDR

Contents

Introdução

Este documento descreve como criar um fluxo de trabalho automatizado para enviar uma notificação por e-mail para um novo incidente.

Pré-requisitos

Requisitos

Não existem requisitos específicos para este documento.

Componentes Utilizados

Este documento não se restringe a versões de software e hardware específicas.

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Configurar

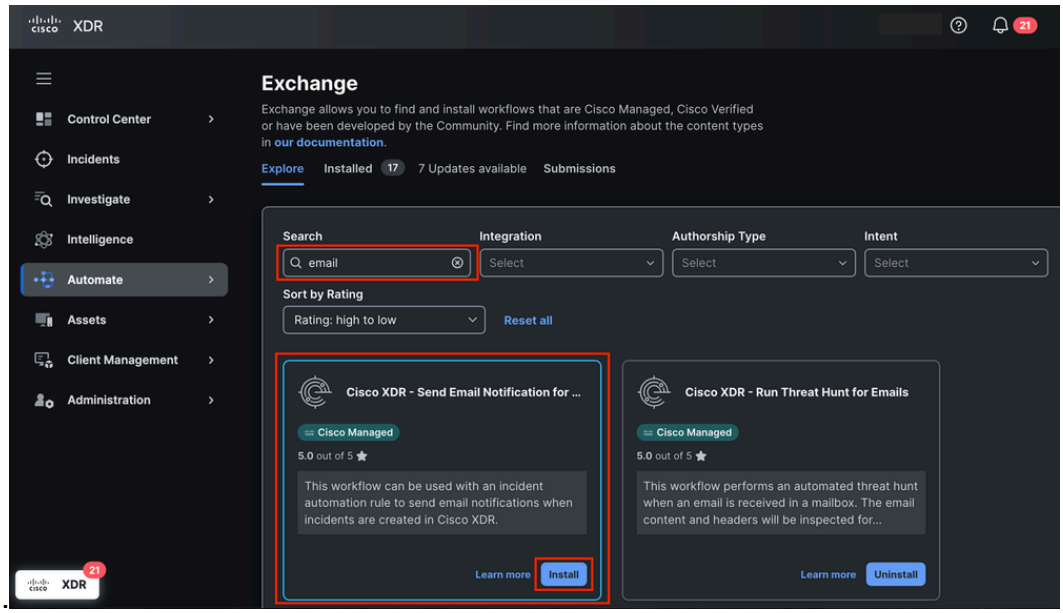
Este guia detalha as etapas necessárias para configurar e ativar um fluxo de trabalho para enviar automaticamente uma notificação por e-mail quando ocorrer um incidente. As etapas são

detalhadas a seguir.

Instalar o fluxo de trabalho do Cisco XDR Exchange

Etapa 1. Instalar o Fluxo de Trabalho de Isolamento de Ponto Final

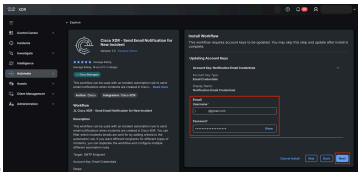
1. Faça login no Cisco XDR e navegue até Automate > Exchange.
2. Procure o fluxo de trabalho chamado Cisco XDR - Send Email Notification for New Incident e clique em Install.



Enviar Fluxo de Trabalho de Notificação por Email do Exchange

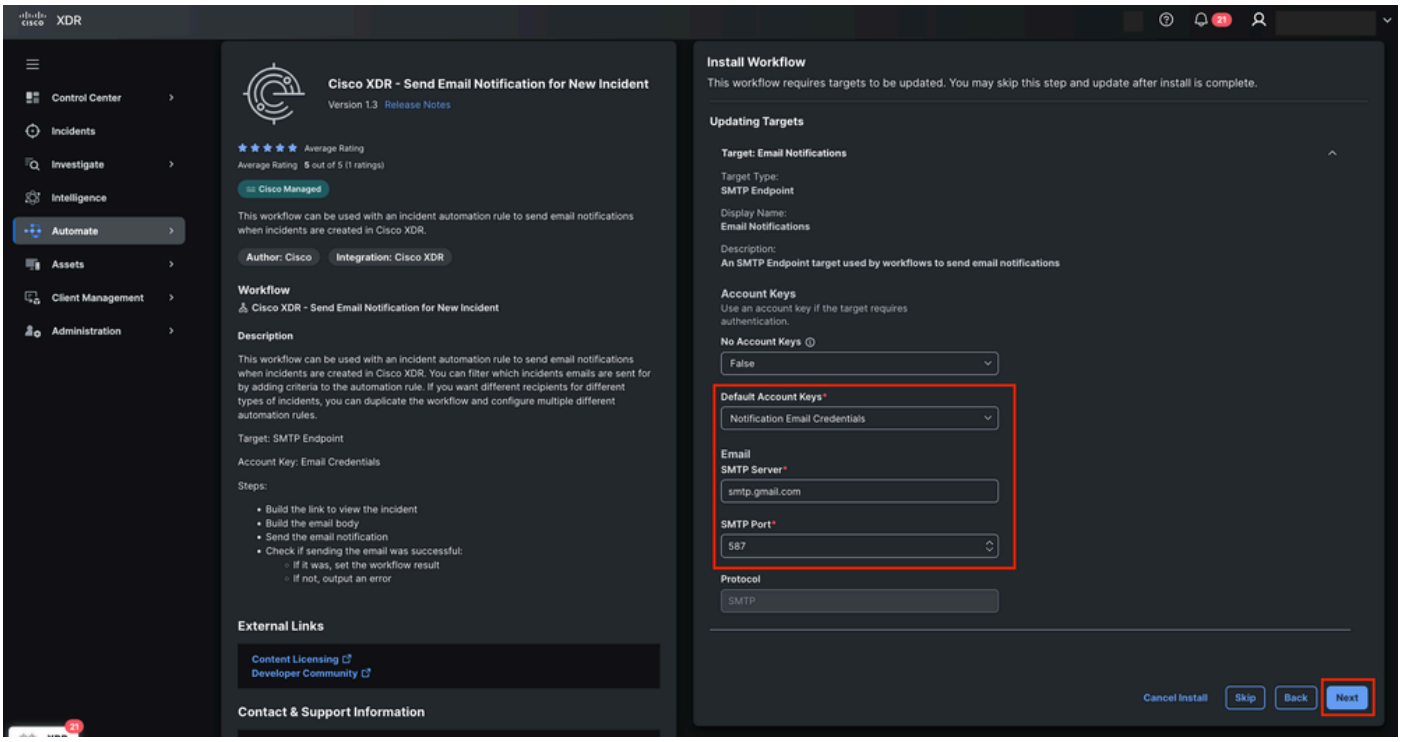
3. Verifique as informações necessárias para configurar o fluxo de trabalho corretamente. 

Visão Geral do Fluxo de Trabalho de Enviar Notificação por Email

4. Preencha as chaves da contacom as credenciais de email para definir o remetente. O nome exibido é Credenciais de e-mail de notificação e clique em Próximo. 

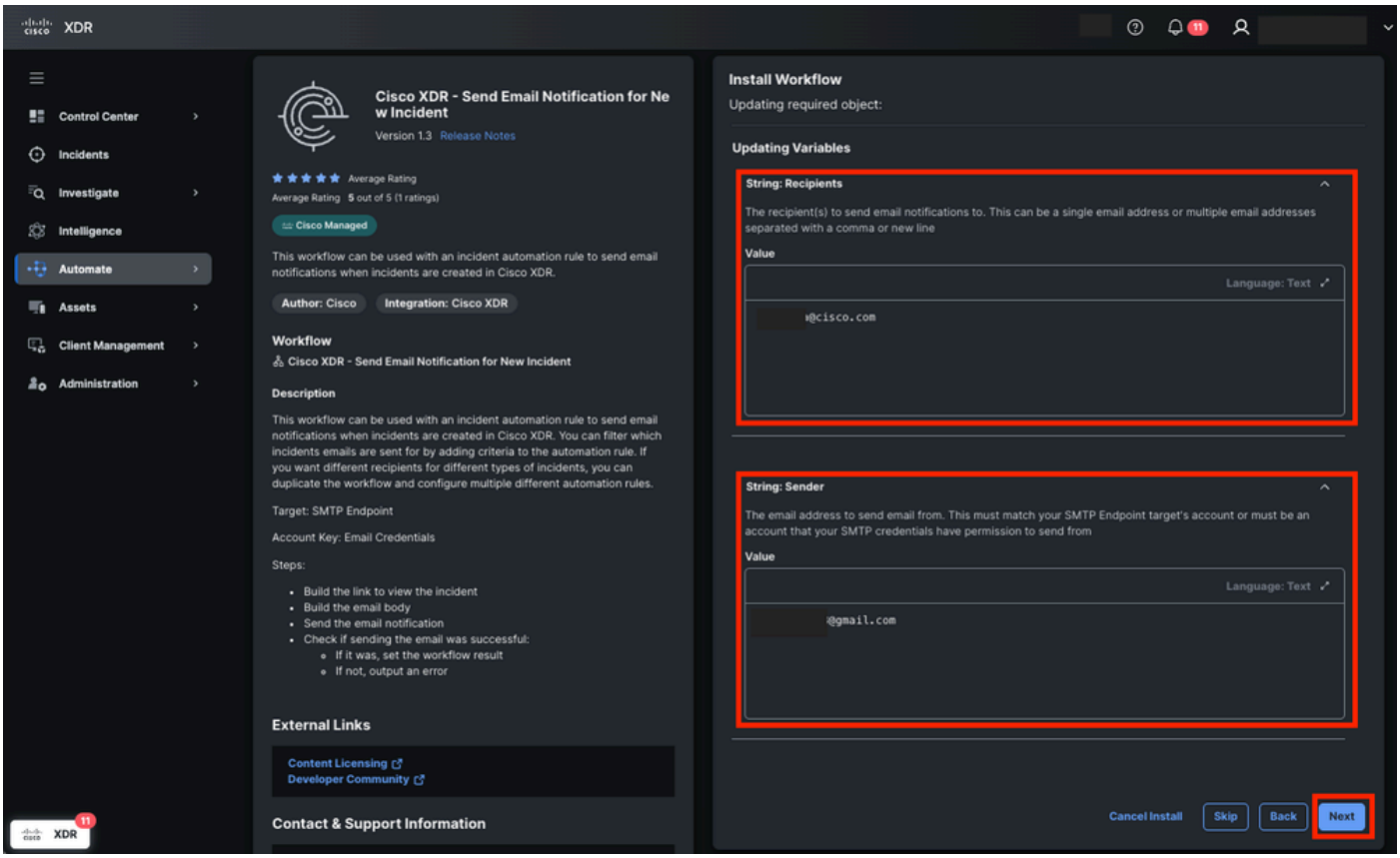
Chaves de Conta para Fluxo de Trabalho

5. Configure as informações de destino com:
   - Chaves de conta: Credenciais de e-mail de notificação
   - E-mail
     - Servidor SMTP: smtp.gmail.com
     - Porta SMTP: 587



Configuração de Destino para Fluxo de Trabalho

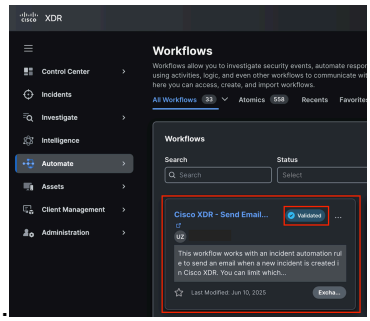
1. Clique em Next.
2. Atualizar a variável para:
    - Destinatários
    - Remetente



Atribuir Variáveis para Fluxo de Trabalho

8. Clique em Próximo.

9. Navegue até Automatizar > Workflows para verificar o status Validado.



Status Validado do Fluxo de Trabalho

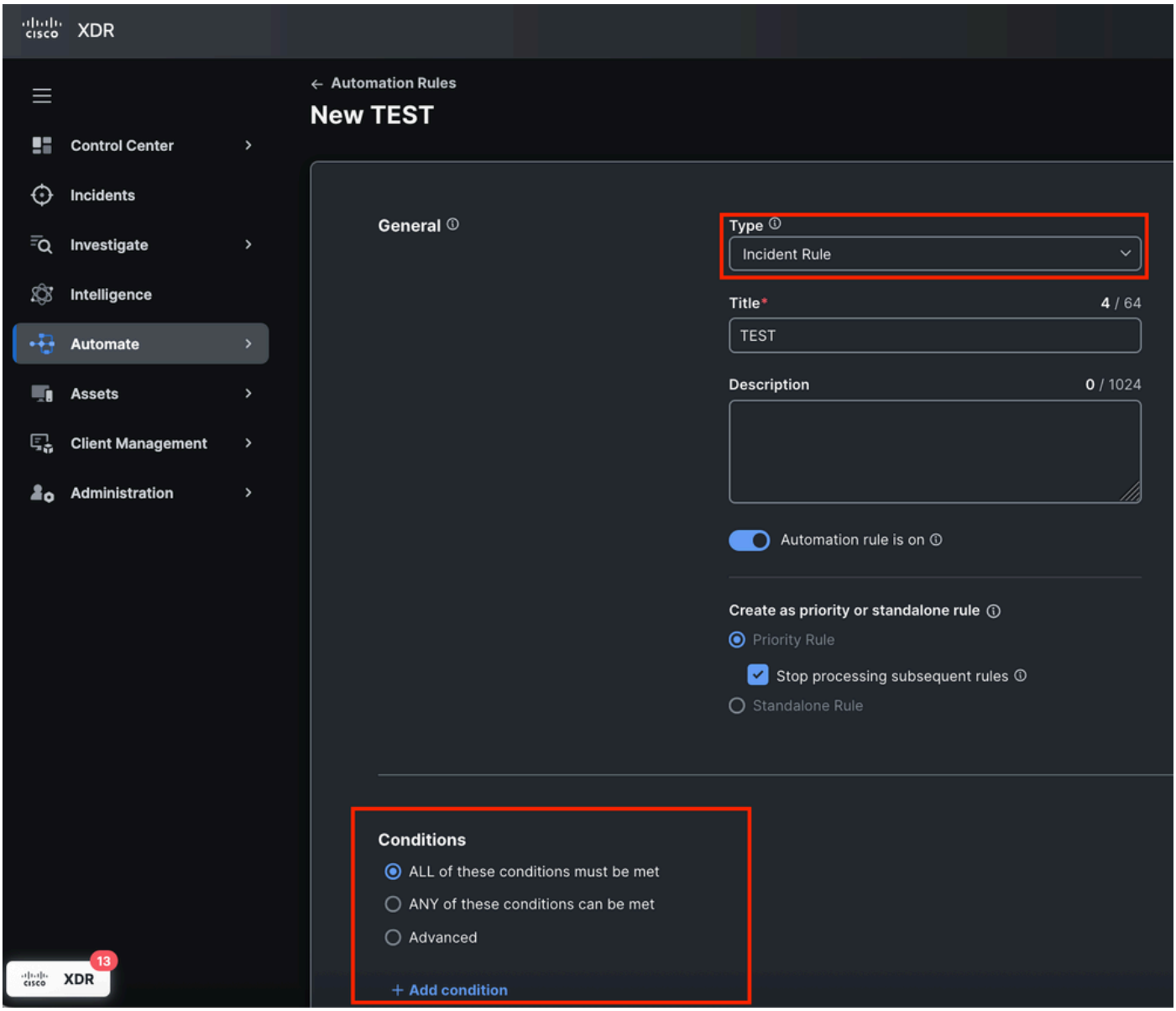
Criar uma Regra de Automação

Etapa 2. Configurar uma Regra de Automação

1. Navegue até a seção Automação > Triggers.
2. Crie uma nova regra. Clique em Adicionar regra de automação e atribua um nome. 

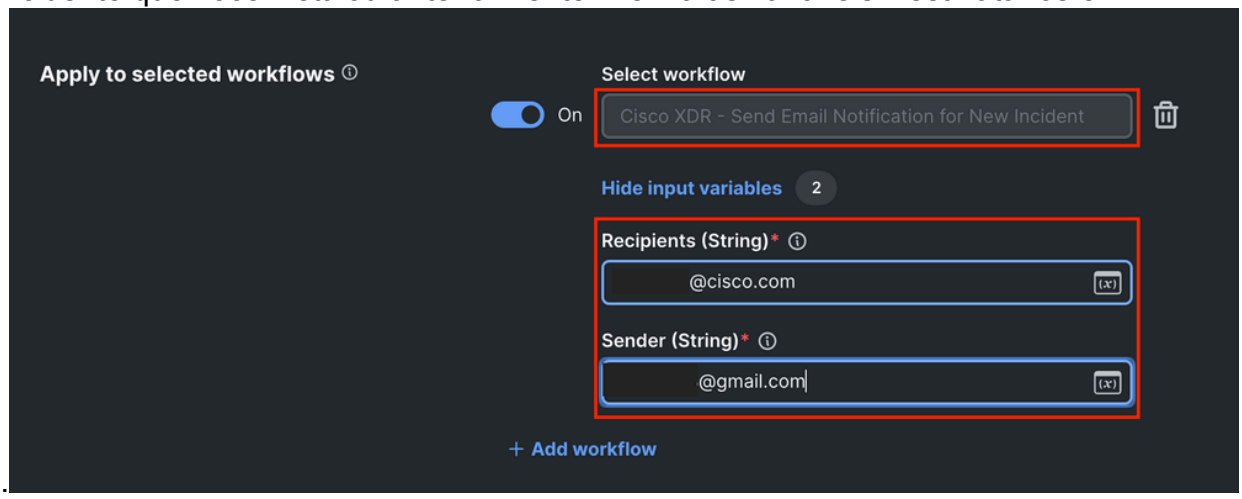
   Adicionar Regra de Automação de Gatilhos

3. Selecione o tipo Regra de incidente e defina as condições do acionador. Você pode continuar sem a necessidade de adicionar uma condição de regra, o que garante que qualquer incidente ative essa regra. Personalize as condições, se necessário.



Tipo e condições da regra de automação

4. Aplique a regra de automação ao fluxo de trabalho Cisco XDR - Enviar notificação por e-mail para novo incidente que você instalou anteriormente. Defina as variáveis Destinatários e Remetente.

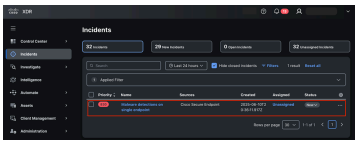


Aplicar a Regra de Automação ao Workflow e Atribuir Variáveis

5. Salve a regra.

Validar Funcionalidade do Fluxo de Trabalho

Etapa 3. Verificar a Execução do Workflow



1. Gerar ou aguardar um incidente que atenda às condições da regra.

   Novo incidente detectado no Cisco XDR

2. Clique em Incidente e em Exibir detalhes do 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

: O nome inicial do incidente é gerado com base na primeira detecção; no entanto, ela pode mudar se ocorrerem detecções adicionais ou se novas informações enriquecerem o incidente.

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.