Configure Email Notification Automated Workflow with XDR

Contents

Introduction

This document describes how to create an automated workflow to send an email notification for a new incident.

Prerequisites

Requirements

There are no specific requirements for this document.

Components Used

This document is not restricted to specific software and hardware versions.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

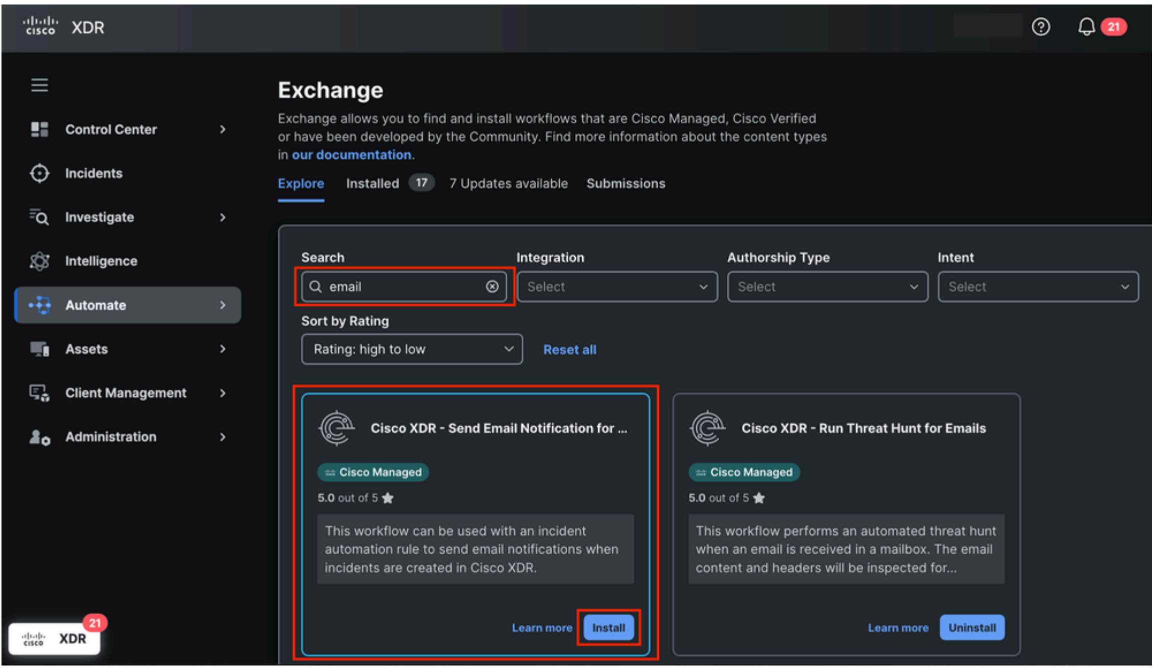
Configure

This guide details the steps necessary to configure and activate a workflow to automatically send an email notification when an incident occurs. The steps are detailed as follows.

Install the Workflow from Cisco XDR Exchange

Step 1. Install the Endpoint Isolation Workflow

1. Log in to Cisco XDR and navigate to **Automate** > **Exchange**.
2. Search for the workflow named **Cisco XDR - Send Email Notification for New Incident** and click **Install**.



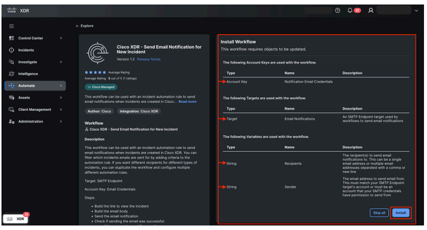
Exchange allows you to find and install workflows that are Cisco Managed, Cisco Verified or have been developed by the Community. Find more information about the content types in **our documentation**.

This workflow can be used with an incident automation rule to send email notifications when incidents are created in Cisco XDR.

This workflow performs an automated threat hunt when an email is received in a mailbox. The email content and headers will be inspected for...

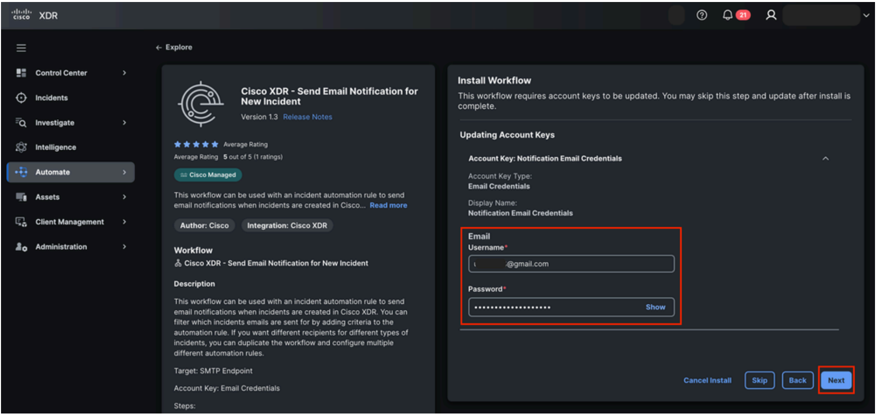
Send Email Notification Workflow from Exchange

3. Check the necessary information to configure the workflow correctly.



Send Email Notification Workflow Overview

4. Fill the **Account Keys**with the email credentials to set the sender. The Displayed name is Notification Email Credentials and Click **Next.**



Cisco XDR - Send Email Notification for New Incident

Version 1.3 Release Notes

Average Rating

Average Rating 5 out of 5 (1 ratings)

This workflow can be used with an incident automation rule to send email notifications when incidents are created in Cisco... Read more

Workflow

Cisco XDR - Send Email Notification for New Incident

Description

This workflow can be used with an incident automation rule to send email notifications when incidents are created in Cisco XDR. You can filter which incidents emails are sent for by adding criteria to the automation rule. If you want different recipients for different types of incidents, you can duplicate the workflow and configure multiple different automation rules.

Target: SMTP Endpoint

Account Key: Email Credentials

Steps:

Install Workflow

This workflow requires account keys to be updated. You may skip this step and update after install is complete.

Updating Account Keys

Account Key: Notification Email Credentials

Account Key Type:
Email Credentials

Display Name:
Notification Email Credentials

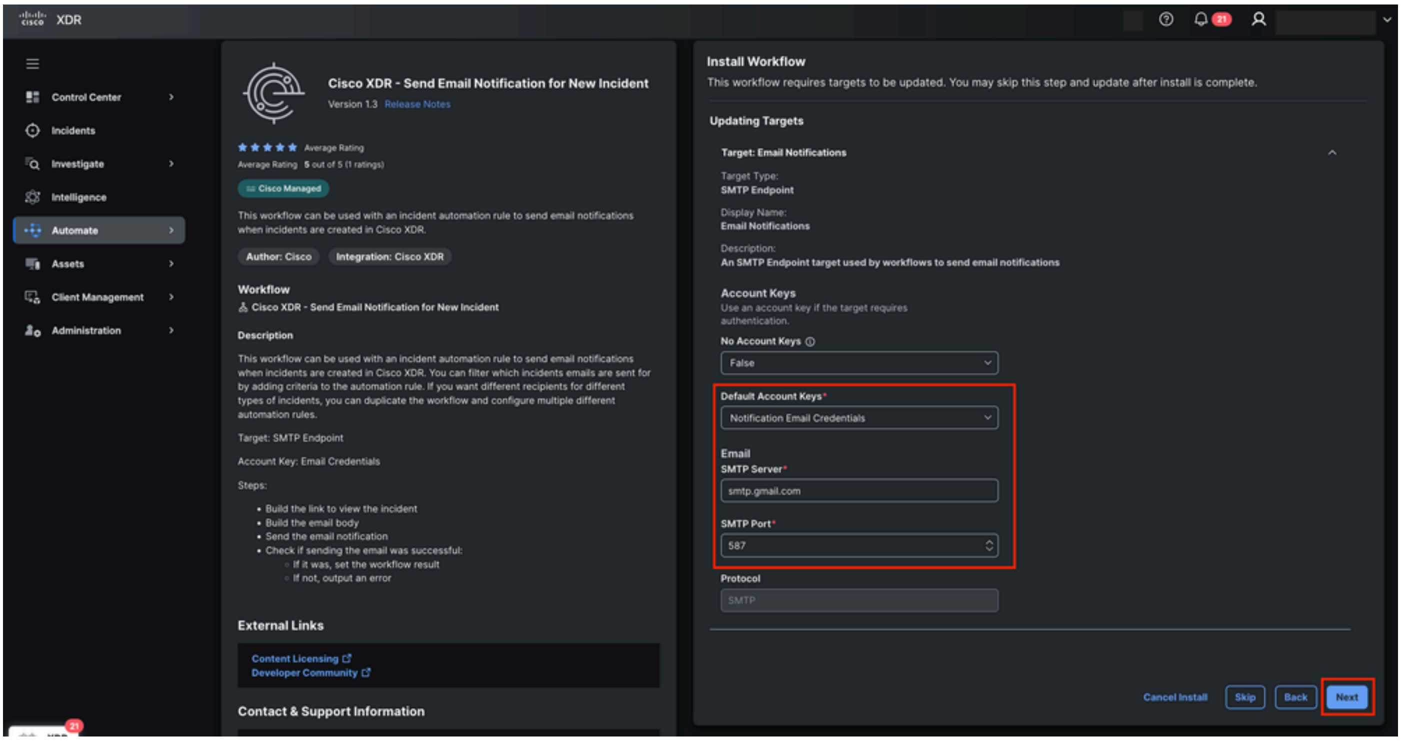
Email

Username*
[redacted]@gmail.com

Password*
••••••••••••••••••••

Account Keys for Workflow

5. Configure the target information with:
   - **Account Keys:** Notification Email Credentials
   - **Email**
     - **SMTP server:** smtp.gmail.com
     - **SMTP Port:** 587



Cisco XDR - Send Email Notification for New Incident

Version 1.3 Release Notes

★★★★★ Average Rating

Average Rating 5 out of 5 (1 ratings)

Cisco Managed

This workflow can be used with an incident automation rule to send email notifications when incidents are created in Cisco XDR.

Author: Cisco | Integration: Cisco XDR

Workflow

Cisco XDR - Send Email Notification for New Incident

Description

This workflow can be used with an incident automation rule to send email notifications when incidents are created in Cisco XDR. You can filter which incidents emails are sent for by adding criteria to the automation rule. If you want different recipients for different types of incidents, you can duplicate the workflow and configure multiple different automation rules.

Target: SMTP Endpoint

Account Key: Email Credentials

Steps:

- Build the link to view the incident
- Build the email body
- Send the email notification
- Check if sending the email was successful:
  - If it was, set the workflow result
  - If not, output an error

External Links

Content Licensing
Developer Community

Contact & Support Information

Install Workflow

This workflow requires targets to be updated. You may skip this step and update after install is complete.

Updating Targets

Target: Email Notifications

Target Type:
SMTP Endpoint

Display Name:
Email Notifications

Description:
An SMTP Endpoint target used by workflows to send email notifications

Account Keys

Use an account key if the target requires authentication.

No Account Keys: False

Default Account Keys*: Notification Email Credentials

Email

SMTP Server*: smtp.gmail.com

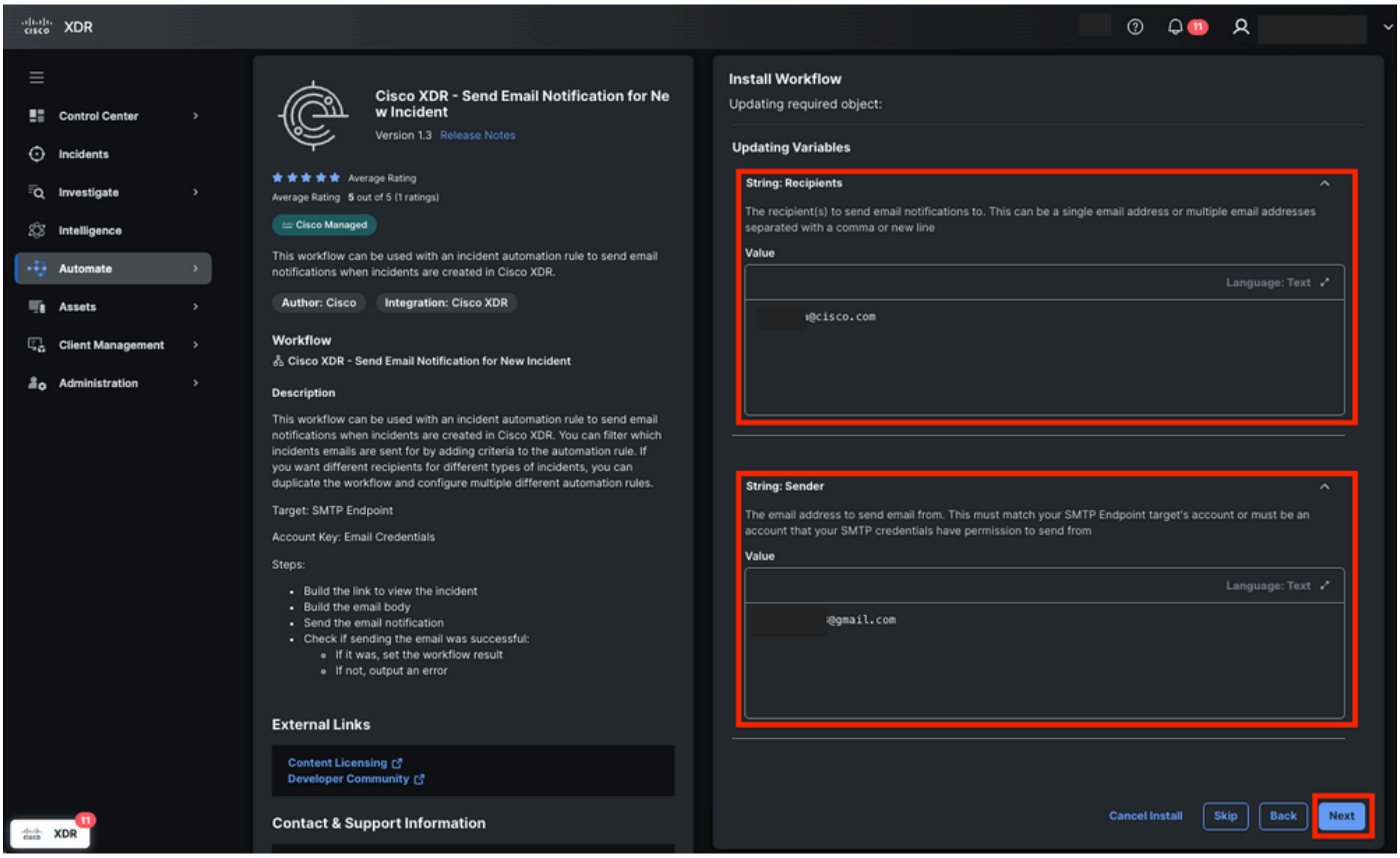
SMTP Port*: 587

Protocol: SMTP

Cancel Install | Skip | Back | Next

Target Configuration for Workflow

1. Click **Next.**
2. Update the variable for:
   - **Recipients**
   - **Sender**



Cisco XDR - Send Email Notification for New Incident

Version 1.3 Release Notes

★★★★★ Average Rating

Average Rating 5 out of 5 (1 ratings)

Cisco Managed

This workflow can be used with an incident automation rule to send email notifications when incidents are created in Cisco XDR.

Author: Cisco | Integration: Cisco XDR

Workflow

Cisco XDR - Send Email Notification for New Incident

Description

This workflow can be used with an incident automation rule to send email notifications when incidents are created in Cisco XDR. You can filter which incidents emails are sent for by adding criteria to the automation rule. If you want different recipients for different types of incidents, you can duplicate the workflow and configure multiple different automation rules.

Target: SMTP Endpoint

Account Key: Email Credentials

Steps:

- Build the link to view the incident
- Build the email body
- Send the email notification
- Check if sending the email was successful:
  - If it was, set the workflow result
  - If not, output an error

External Links

Content Licensing
Developer Community

Contact & Support Information

Install Workflow

Updating required object:

Updating Variables

String: Recipients

The recipient(s) to send email notifications to. This can be a single email address or multiple email addresses separated with a comma or new line

Value (Language: Text)

```
[redacted]@cisco.com
```

String: Sender

The email address to send email from. This must match your SMTP Endpoint target's account or must be an account that your SMTP credentials have permission to send from

Value (Language: Text)

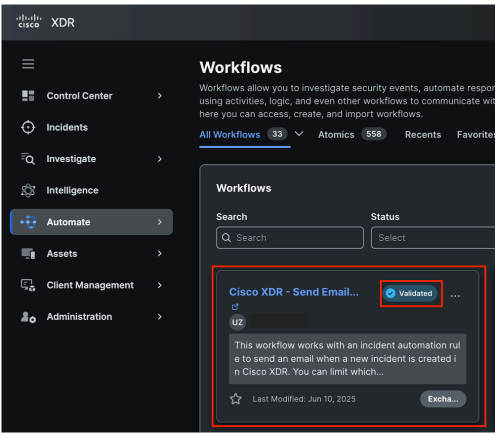
```
[redacted]@gmail.com
```

Cancel Install | Skip | Back | Next

Assign Variables for Workflow

8. Click **Next.**

9. Navigate to **Automate > Workflows** to check the **Validated** status.



Workflows allow you to investigate security events, automate respor using activities, logic, and even other workflows to communicate wit here you can access, create, and import workflows.

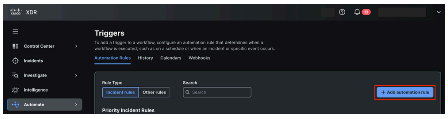
This workflow works with an incident automation rul e to send an email when a new incident is created i n Cisco XDR. You can limit which...

Workflow Validated Status

Create an Automation Rule

Step 2. Configure an Automation Rule

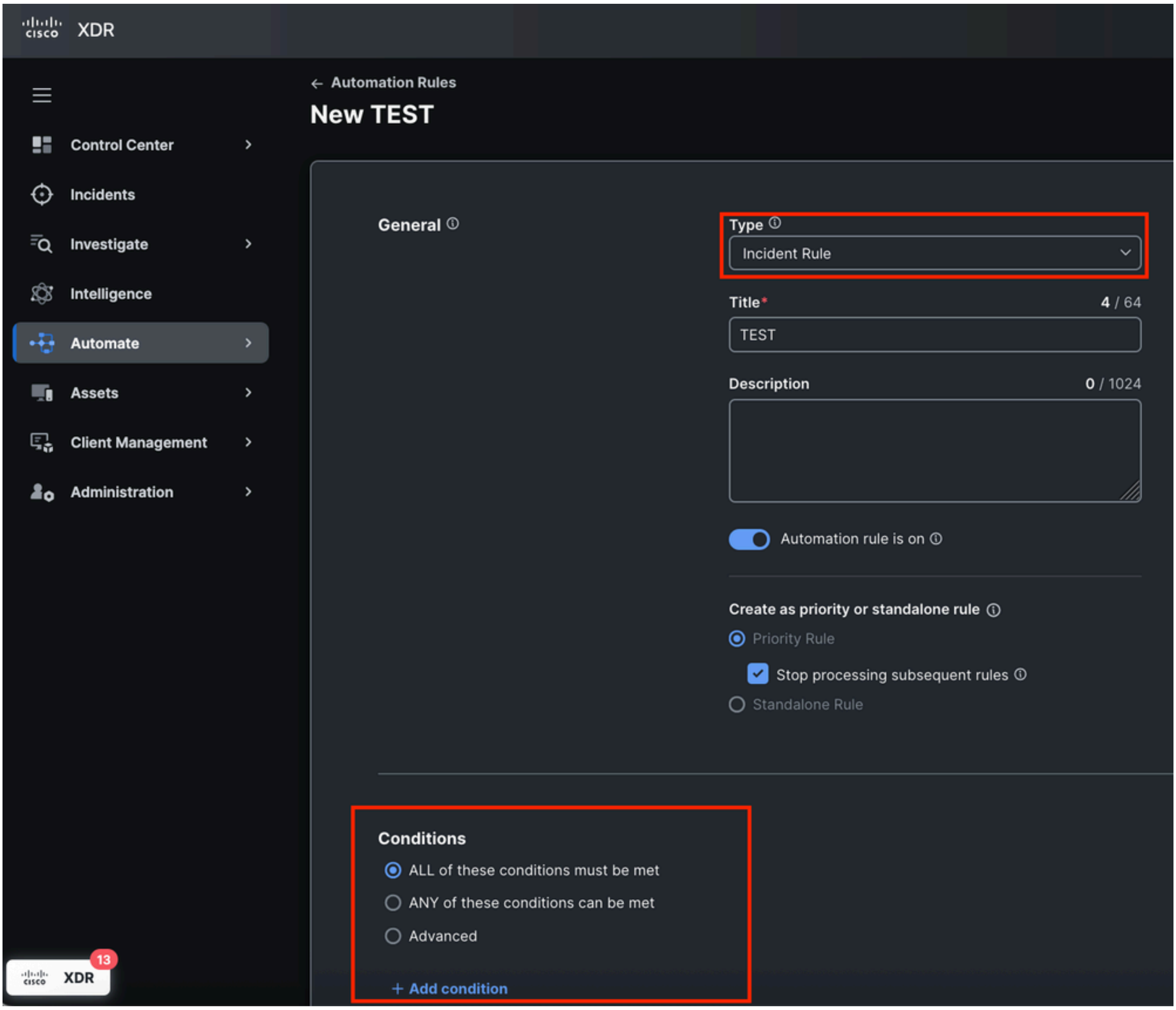
1. Navigate to the **Automation > Triggers** section.
2. Create a new **rule**. Click **Add automation rule** and assign a **name**.



To add a trigger to a workflow, configure an automation rule that determines when a workflow is executed, such as on a schedule or when an incident or specific event occurs.

Add Automation Rule from Triggers

3. Select **Incident Rule** type and define the trigger conditions. You can proceed without the need to add a rule condition, which ensures that any incident activates this rule. Customize the conditions if necessary.



← Automation Rules

New TEST

General

Type: Incident Rule

Title*: TEST (4 / 64)

Description: (0 / 1024)

Automation rule is on

Create as priority or standalone rule

● Priority Rule

☑ Stop processing subsequent rules

○ Standalone Rule

Conditions

● ALL of these conditions must be met

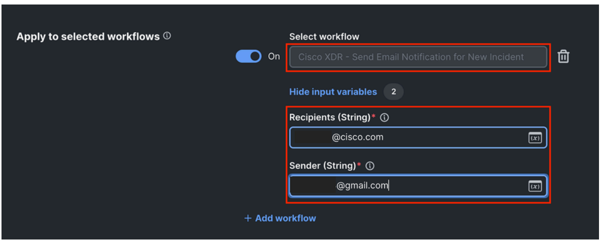
○ ANY of these conditions can be met

○ Advanced

+ Add condition

Automation Rule Type and Conditions

4. Apply the Automation Rule to the **Cisco XDR - Send Email Notification for New Incident** workflow you installed earlier. Set the **Recipients** and **Sender** variables.



Apply to selected workflows

On

Select workflow: Cisco XDR - Send Email Notification for New Incident

Hide input variables 2

Recipients (String)*: [redacted]@cisco.com

Sender (String)*: [redacted]@gmail.com

+ Add workflow

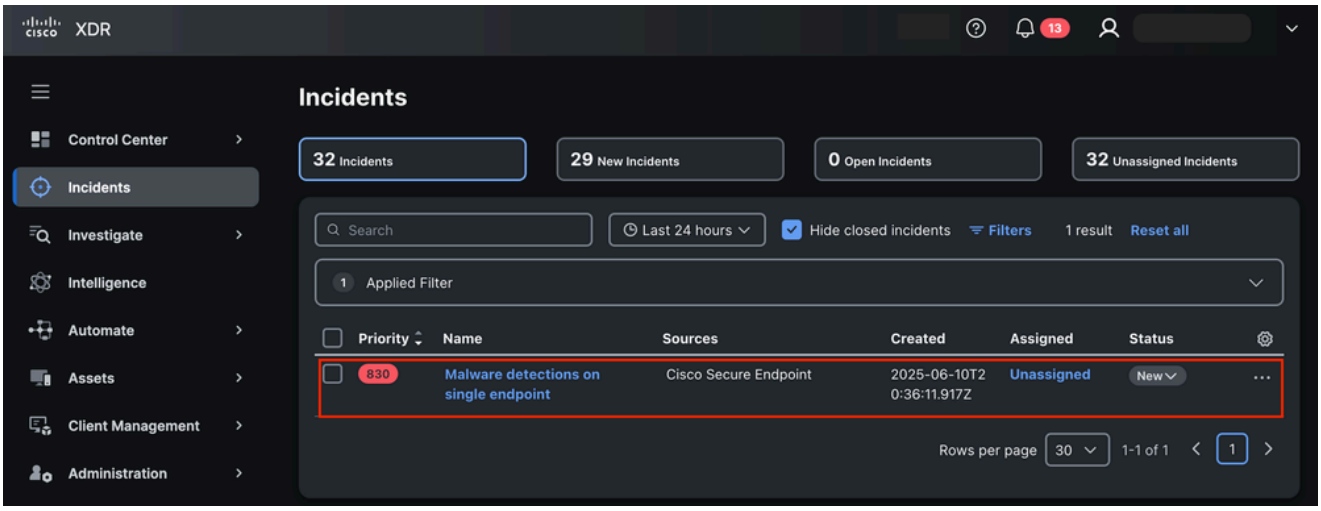
Apply the Automation Rule to the Workflow and Assign Variables

5. Save the **rule**.

Validate Workflow Functionality

Step 3. Verify Workflow Execution

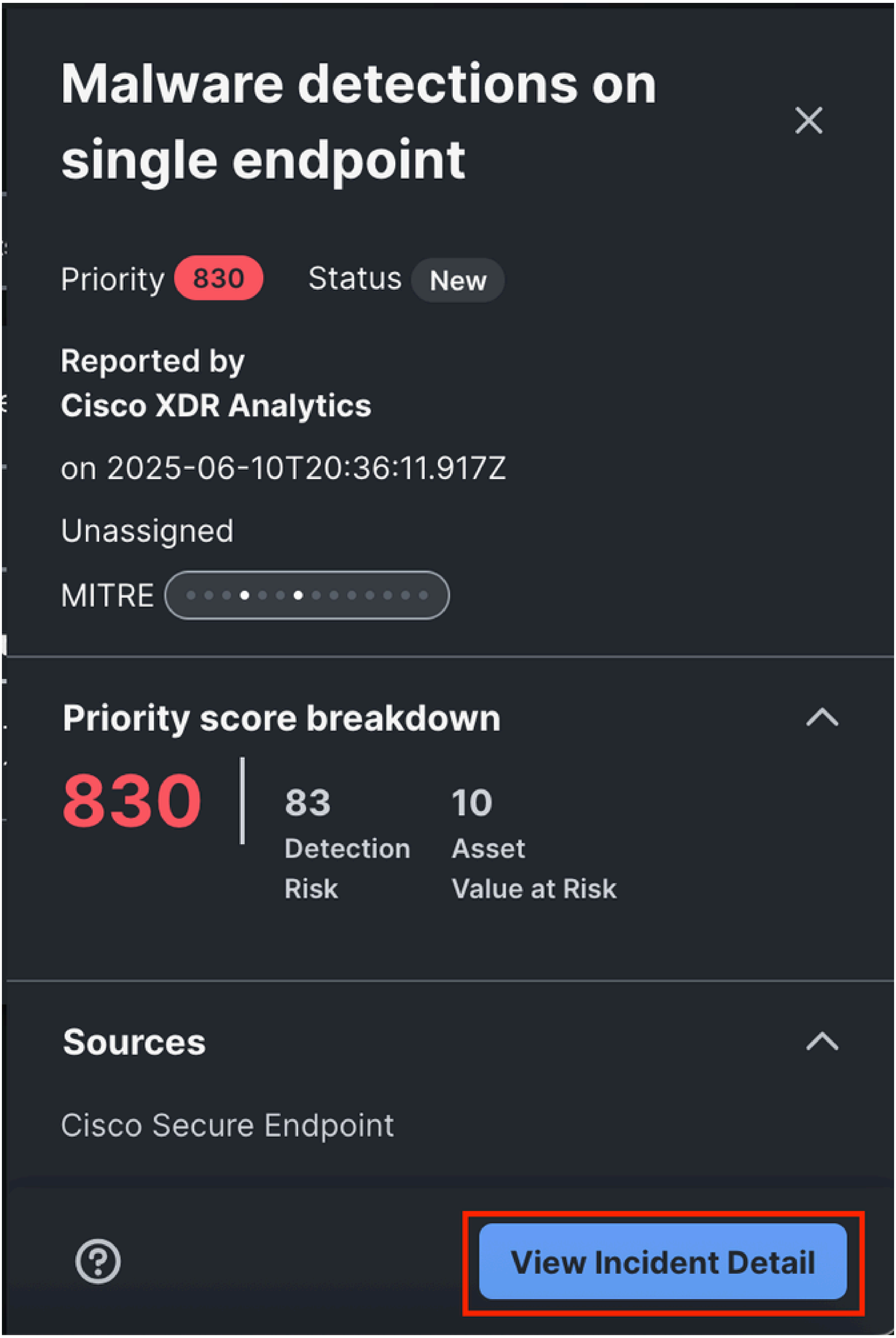
1. Generate or wait for an incident that meets the conditions of the rule.



Priority	Name	Sources	Created	Assigned	Status
830	Malware detections on single endpoint	Cisco Secure Endpoint	2025-06-10T20:36:11.917Z	Unassigned	New

New Incident in Cisco XDR Detected

2. Click **Incident** and then **View Incident Detail.**



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 Detection Risk | 10 Asset Value at Risk

Sources

Cisco Secure Endpoint

: The initial incident name is generated based on the first detection; however, it can change if additional detections occur or new information enriches the incident.