CHECK POINT

03 July 2026

PLAYBLOCKS

Administration Guide

Contents

1. Important Information

Latest Software

We recommend that you install the most recent software release to stay up-to-date with the latest functional improvements, stability fixes, security enhancements and protection against new and evolving attacks.

Certifications

For third party independent certification of Check Point products, see the Check Point Certifications page.

Check Point Playblocks Administration Guide

For more about this release, see the home page.

Latest Version of this Document in English

Open the latest version of this document in a Web browser.

Download the latest version of this document in PDF format.

Feedback

Check Point is engaged in a continuous effort to improve its documentation.

Feedback for Playblocks Administration Guide Please help us by sending your comments.

1.1. Revision History

This topic lists the revision history entries, including additions and updates made over time.

Date	Description
06 May 2026	Added Notify on Tunnel Up by SASE *(on page 44)*
12 February 2026	Added: • Appendix H - Webhooks and Authentications *(on page 304)* • Webhooks *(on page 199)* • Authentications *(on page)*
10 February 2026	Added Quantum Cloud Log Ingestion Health Monitor *(on page 65)*
05 February 2026	Added Notify on Tunnel Down by SASE *(on page 45)*
11 December 2025	Updated Check Point Firewall Enforcement *(on page 224)*

Date	Description
27 November 2025	Added: • Alert on Generative AI Risky Session *(on page 116)*. • **Allowed Identities** and **Untrusted Identities** lists. See Lists *(on page 220)*.
18 November 2025	Added AI Agent - Management health report *(on page 61)*.
07 October 2025	Added Notify on Failed GAIA Portal Login *(on page 73)*.
08 September 2025	Added Appendix G - Using Custom Automation Step Schemas *(on page 286)*.
18 August 2025	Added Credentials leakage detected by ERM triggering reset password *(on page 65)*.
18 July 2025	Added: • **Endpoint Security IOC Enforcement** in IOC Enforcement *(on page 252)*. • Block malicious file indicator identified by Threat Extraction Endpoint Security *(on page 47)* • Block malicious file indicator identified by Threat Emulation Endpoint Security *(on page 48)* • Block malicious file indicator identified by Anti-Bot Endpoint Security *(on page 49)* • Block malicious URL indicator identified by Anti-Bot Endpoint Security *(on page 50)* • Block malicious indicator identified by Zero Phishing Endpoint Security *(on page 53)* • Notify on URL Reputation Identification by SASE *(on page 43)* • Notify on Malicious File Detection by SASE *(on page 46)* • Notify on URL filtering blocked by SASE *(on page 42)* • Notify on Firewall Traffic Blocked by SASE *(on page 41)* • De-isolate potentially clean Microsoft Defender machine *(on page 72)* • Notify on AIOps alert *(on page 135)* • Spark Management event *(on page 114)*
14 July 2025	Added **Creating Automation by AI Copilot** in Customization in Playblocks *(on page 141)*.
05 June 2025	Added Overview *(on page 28)*.
07 May 2025	Added Customization in Playblocks *(on page 141)*.

Date	Description
22 April 2025	Updated: • Quarantine compromised Endpoint Security device (enforced by Firewall) *(on page 39)* • Quarantine potentially infected Endpoint Security device (enforced by Firewall) *(on page 40)* • Quarantine potentially infected CrowdStrike device (enforced by Firewall) *(on page 70)* • Isolate potentially infected CrowdStrike device (enforced by Endpoint) *(on page 59)* Added: • Isolate Endpoint device *(on page 91)* • Isolate compromised Endpoint Security device (enforced by Endpoint) *(on page 56)* • Isolate potentially Infected Endpoint Security device (enforced by Endpoint) *(on page 57)* • Quarantine potentially infected Microsoft Defender device (enforced by Firewall) *(on page 63)* • Isolate potentially infected Microsoft Defender device (enforced by Endpoint) *(on page 62)* • Quarantine potentially infected SentinelOne device (enforced by Firewall) *(on page 60)* • Isolate potentially infected SentinelOne device (enforced by Endpoint) *(on page 58)* • Add malicious file indicator Identified by SentinelOne to IOC feed *(on page 134)* • Add malicious file indicator Identified by Microsoft Defender to IOC feed *(on page 134)* • Add malicious file indicator Identified by CrowdStrike to IOC feed *(on page 133)*
01 April 2025	Added IOC Enforcement *(on page 252)*.
21 February 2025	Added: • SentinelOne *(on page 250)* • Appendix F - Creating a SentinelOne Service User *(on page 281)*
09 December 2024	Updated Supported Products *(on page 15)*.

Date	Description
05 November 2024	• Added new automations: ◦ Alert on MTA email bypass *(on page 79)* ◦ Block attacking IP with malicious reputation identified by WAF Application Security Application Security *(on page 38)* ◦ Alert if VPN Tunnel is down *(on page 87)* ◦ Notify on Management validations *(on page 80)* • Updated Block attackers upon IPS detection of popular attacks *(on page 35)*
12 September 2024	Added: • Automations: ◦ Quarantine potentially infected CrowdStrike device (enforced by Firewall) *(on page 70)* ◦ Isolate potentially infected CrowdStrike device (enforced by Endpoint) *(on page 59)* • Appendix E - Integrating CrowdStrike Falcon *(on page 278)* • CrowdStrike *(on page 247)*
09 September 2024	Added: • Automations: ◦ Reset User Password in Identity Provider *(on page 98)* ◦ Notify on degradation in Check Point Firewall Compliance status *(on page 76)* • Connectors: ◦ Okta *(on page 249)* ◦ Microsoft Entra ID *(on page 248)*
07 August 2024	Added note in Appendix C - Creating Workflow for Microsoft Teams Notification *(on page 271)*.
02 August 2024	Added Appendix C - Creating Workflow for Microsoft Teams Notification *(on page 271)*

Date	Description
01 July 2024	Updated: • Notify on failure of installation of blades updates on Check Point Firewalls *(on page 83)* • Notify on failure of Policy Installation on Check Point Firewall *(on page 75)* • Alert on licenses expiration on Quantum device *(on page 85)* • Alert on VPN certificates expiration on Check Point Firewall *(on page 86)* • Notify on repeated login failures to Management *(on page 81)* • Enforce Policy on newly discovered IoT Zone *(on page 93)* • IoT Device is at risk *(on page 94)* • Quarantine compromised Endpoint Security device (enforced by Firewall) *(on page 39)* • Quarantine potentially infected Endpoint Security device (enforced by Firewall) *(on page 40)* • Quarantine internal IP *(on page 92)* • Notify on high rate of blocked connections *(on page 82)* Added: • Notify on successful installation of blade updates on Check Point Firewalls *(on page 84)* • Notify on successful Policy Installation on Check Point Firewall *(on page 77)* • Alert on exploit attempt detected by Endpoint Security *(on page 121)* • Alert on ransomware attack detected by Endpoint Security *(on page 115)* • Alert on outdated Endpoint Security Behavioral Guard capability *(on page 124)* • Alert on malicious file detected by Endpoint Security *(on page 118)* • Alert on a phishing attempt detected by Endpoint Security *(on page 117)* • Alert on access to malicious site detected by Endpoint Security *(on page 119)* • Alert on password reuse attempt detected by Endpoint Security *(on page 120)* • Alert on the outdated Endpoint Security Static Analysis capability *(on page 122)* • Alert on the outdated Endpoint Security Offline Reputation capability *(on page 123)* • Alert on disconnected Endpoint Security clients *(on page 125)* • Alert on Endpoint Security Compliance warnings *(on page 126)* • Alert on device restrictions by Endpoint Security *(on page 127)* • Alert on outdated Endpoint Security Anti-Malware *(on page 128)* • Alert on Endpoint Security Anti-Malware license expiration *(on page 130)*

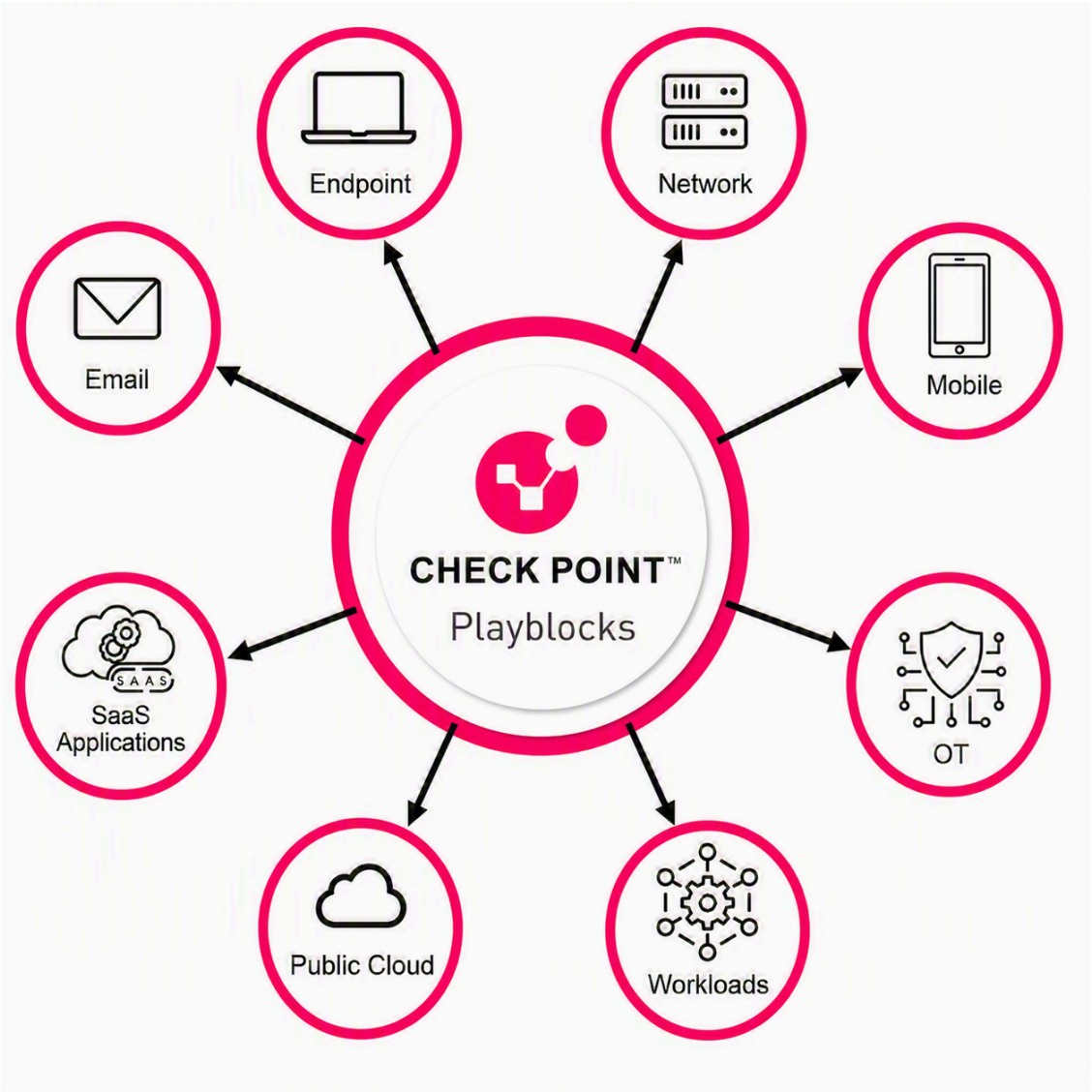
Date	Description
03 June 2024	Added Jira Ticketing *(on page 231)*.
15 March 2024	• Updated the procedure to attach a contract to the product in Accessing the Playblocks Administrator Portal *(on page 18)*. • Added Endpoint Security to the list of supported products. See: ◦ Introduction to Playblocks *(on page 14)* ◦ On-boarding Products *(on page 21)*
16 February 2024	• Added new automations: ◦ Notify on installation of blades updates on Quantum Gateways *(on page 83)* ◦ Alert on VPN certificates expiration on Quantum Gateway *(on page 86)* ◦ Alert if no communication with Quantum Gateway *(on page 88)* ◦ Notify on Endpoint Security client uninstall password change *(on page 95)* ◦ Notify on bulk uninstallation of Endpoint Security clients *(on page 96)* ◦ Stop and quarantine file via Microsoft Defender *(on page 110)* ◦ Scan machine via Microsoft Defender *(on page 108)* • Added Microsoft Defender *(on page 243)*
31 January 2024	Rebranded Horizon Playblocks to Playblocks.
09 January 2024	Added new automations: • Notify on repeated login failures to Management *(on page 81)* • Notify on high rate of blocked connections *(on page 82)* • Alert on licenses expiration on device *(on page 85)* • Open ticket and notify *(on page 113)*
04 January 2024	Added new automations: • Block malicious IOC identified by SASE *(on page 51)* • Block malicious indicator identified by Anti-Bot *(on page 52)* • Block malicious indicator identified by Anti-Virus *(on page 53)* • Block malicious indicator identified by Zero Phishing *(on page 55)* • Block malicious indicator identified by Email Security *(on page 54)*

Date	Description
20 January 2024	Updated: • Check Point Firewall Logs *(on page 223)* • Check Point Firewall Enforcement *(on page 224)*
29 November 2023	Added new automations: • Notify on Management High Availability Change-Over *(on page 81)* • Notify on Repeated Login Failures to Management *(on page 81)* • Scan Endpoint Security Device *(on page 102)*
08 November 2023	First release of this document.

2. Introduction to Playblocks

This topic introduces the automated response capabilities of PlayBlocks and its integration with collaborative tools. It provides an overview of how PlayBlocks helps protect organizations from cyber attacks.

Check Point Playblocks is an automated response solution that automatically takes preventive actions, including isolating hosts, initiating kill processes and notifying Administrators, against cyber attacks in your organization without manual intervention and shares the incident details through your preferred collaborative tools, such as Microsoft Teams, Slack and so on.



Related information
Benefits *(on page 14)*
Use Case *(on page 15)*
Supported Products *(on page 15)*

2.1. Benefits

This topic describes key benefits that improve automation, operational integration, and administrative actions for incident handling. It highlights efficiencies and streamlined communication across collaborative platforms.

- **Automation and Efficiency** - Playblocks minimizes the burden on the SOC teams, eliminates manual errors and increases the speed of incident handling.
- **Operational Integration** - Integration with collaborative tools such as Slack and ServiceNow ensures seamless communication and alignment between security teams.
- **Seamless Administrative Actions** - Administrators can efficiently trigger responsive actions through collaborative platforms such as Microsoft Teams and Slack, enhancing the ease of incident management.

2.2. Use Case

This topic describes a scenario where automated incident response is needed across multiple security products. It outlines desired preventive actions and communication flows.

You are subscribed to multiple Check Point products and you want an automatic incident response tool that integrates with these products to execute appropriate preventive measures. These include isolating affected devices, blocking suspicious connections, or triggering alerts to security teams without relying solely on manual intervention and communicating updates and details through collaborative tools.

2.3. Supported Products

This topic lists the products that can be used with PlayBlocks and their supported environments. It includes both on-premises and cloud-based product options.

You can use Playblocks with these products:

- Check Point Multi-Domain Security Management (MDS) Server and Single-Domain Security Management (SMC) Server with Security Gateway R81 and higher:
  - On-premises:
    - R81.20
    - R81.10 JHF Take 79 and higher
  - Smart-1 Cloud
- Check Point XDR integrated with these Check Point products:
  - Check Point Multi-Domain Security Management (MDS) Server and Single-Domain Security Management (SMC) Server
    - On-premises R81.10 Jumbo Hotfix Accumulator Take 93 and higher with Check Point Security Gateway R81 and higher.
    - Smart-1 Cloud with Check Point Security Gateway R81 and higher.
- Endpoint Security
- SASE
- IoT Security
- Quantum SD-WAN
- Events & AIOps
- External Risk Management
- IoC Management

- Okta
- Microsoft Entra ID
- Microsoft Defender
- CrowdStrike
- SentinelOne
- Spark Management
- ServiceNow
- Jira

2.4. How it Works

This topic describes how the automation process operates from detection through execution and administrator review. It outlines each step performed by the system and the administrator.

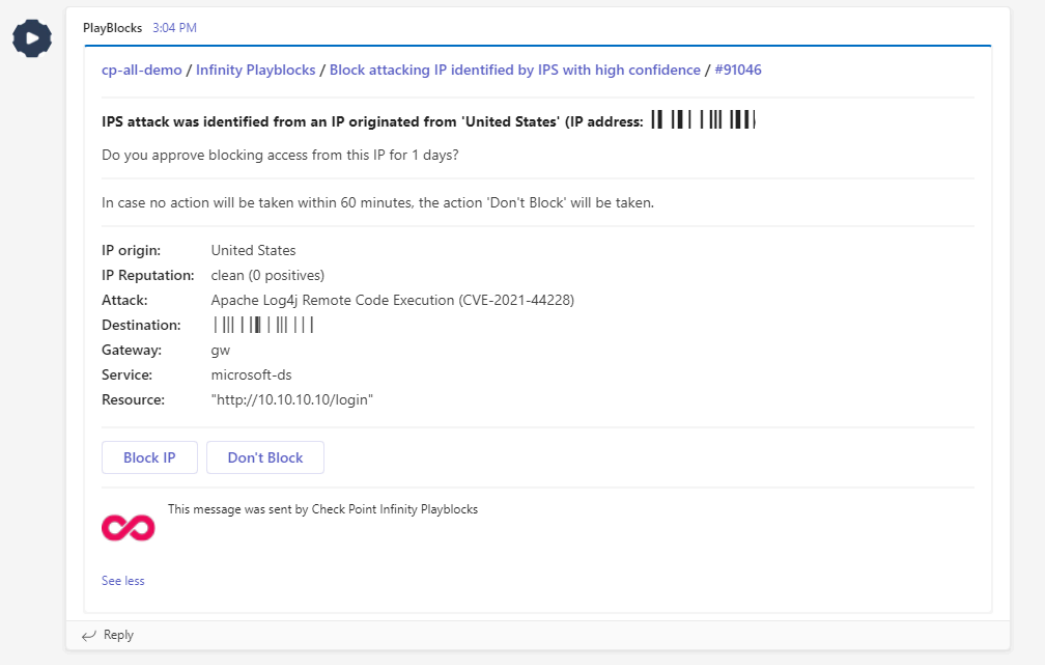
Procedure:

1. Playblocks either detects a malicious activity by analyzing the logs (On the Security Gateway or Multi-Domain Security Management or and Single-Domain Security Management) or receives the preventive or corrective action to be executed directly, for example, from XDR.
2. Automatically correlates the required action to a predefined automation.
3. Executes the automation.

> **Note:**
>
> You can disable automatic execution of an automation and configure Administrator approval for execution.

4. Sends a notification to the Administrator through the configured communication channel, such as Microsoft Teams.

   For example:



5. The Administrator reviews the notification and takes the required action:

   - Revert the execution.
   - Approve or block the execution if Administrator approval is enabled.

     See Approving, Rejecting or Reverting an Automation Execution.

3. Getting Started

This topic describes the initial steps required to begin working with PlayBlocks. It provides links to create an account, access the portal, license the product, and onboard services.

Procedure:

1. Create an Account in the Check Point Portal *(on page)*
2. Access the Playblocks Administrator Portal *(on page 18)*
3. License the product *(on page 20)*
4. On-boarding Products *(on page 21)*

3.1. Creating an Account in the Check Point Portal

This topic provides an overview of the Check Point Portal and points to additional documentation for creating an account.

Check Point Portal is a web-based interface that hosts the Check Point security SaaS services.

With Check Point Portal, you can manage and secure your IT infrastructures: networks, cloud, IoT, endpoints, and mobile devices.

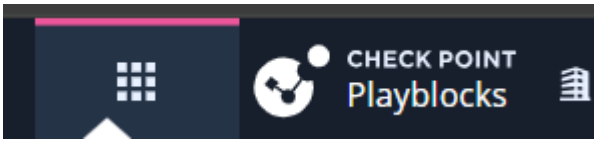
To create an Check Point Portal account, see the Check Point Portal Administration Guide.

3.2. Accessing the Playblocks Administrator Portal

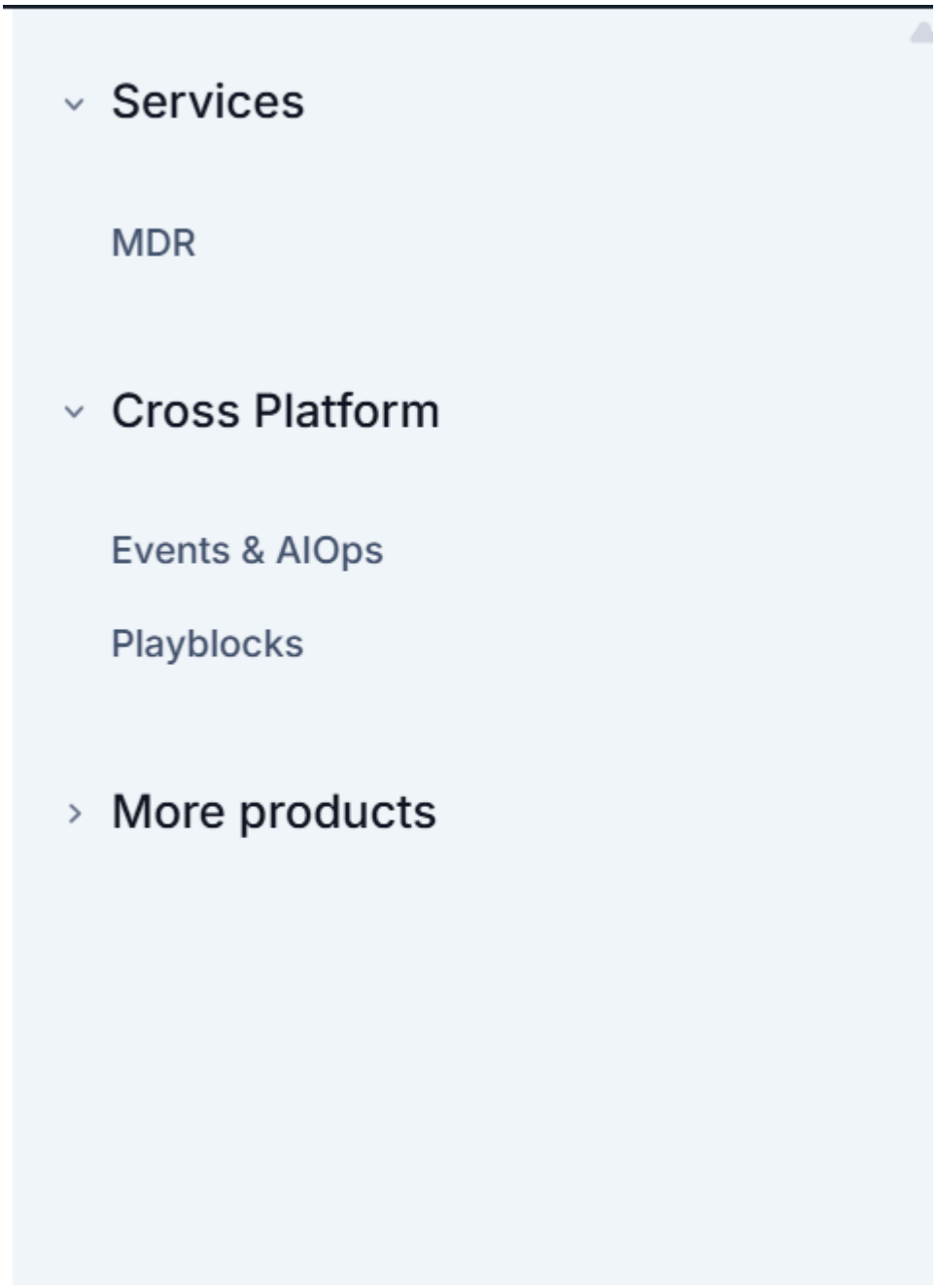
This task explains how to access the Playblocks Administrator Portal through the Check Point Portal. Follow the steps to sign in and open the Playblocks interface.

Procedure:

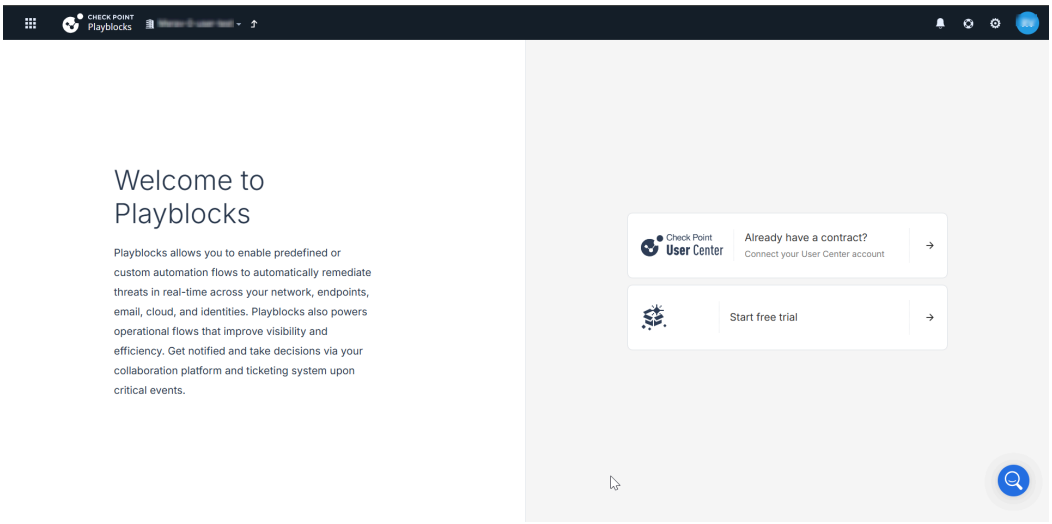
1. Sign in to Check Point Portal.
2. Click the **Menu** icon in the top left corner.



3. In the **Cross Platform** section, click **Playblocks**.

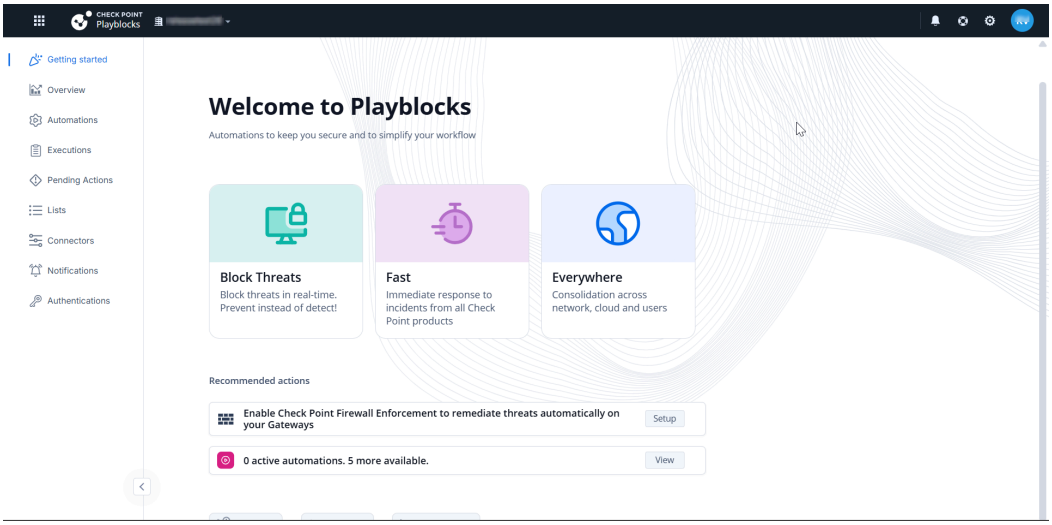


4. If you are accessing the portal for the first time, do one of these.



   - If you already have a Check Point contract, click **Already have a contract** to attach the contract to the product. For more information, see **Associated Accounts** in Check Point Portal.
   - If you want to trial the product, click **Start free trial**.

   If you have already attached the contract with the product, the **Overview** page appears.



5. Follow the **Recommended actions** to enable connectors *(on page 223)* and automations *(on page 29)*.

> **Note:**
>
> Check Point recommends that you run automations *(on page 29)* to test it before you enable it.

3.3. Licensing the Product

This topic explains how to obtain, purchase, and view license information for the product. It also describes where to manage contract details in the Check Point Portal.

You get a free 30-day trial when you create an account in the Check Point Portal.. Use your Check Point User Center account to purchase a license to continue to use the product after the trial period ends. For instructions, see sk22716.

After you create a User Center account, contact your Check Point sales representative to purchase a license.

If you have licensed the product, to view your current contract (license) information, go to the **Check Point Portal.** > **Global Settings** > **Contracts page**.

3.4. On-boarding Products

This topic lists products and describes their respective on-boarding processes. It summarizes how different product types are added or enabled.

Product Name	On-boarding Process
• Check Point Single-Domain Security Management (SMC) Server • Check Point Multi-Domain Security Management (MDS) Server	• On-premises ◦ R81.20 ◦ R81.10 JHF Take 79 or higher See On-boarding Check Point Security Gateways *(on page 224)*. • Smart-1 Cloud - Automatic if you subscribe to Playblocks.
XDR	Automatic if you subscribe to XDR.
IoT Security	Automatic if you subscribe to IoT Security.
Quantum SD-WAN	Enable the Handle SD-WAN Link Swap ISP Down *(on page 111)* automation.
Endpoint Security	Automatic if you subscribe to Endpoint Security.

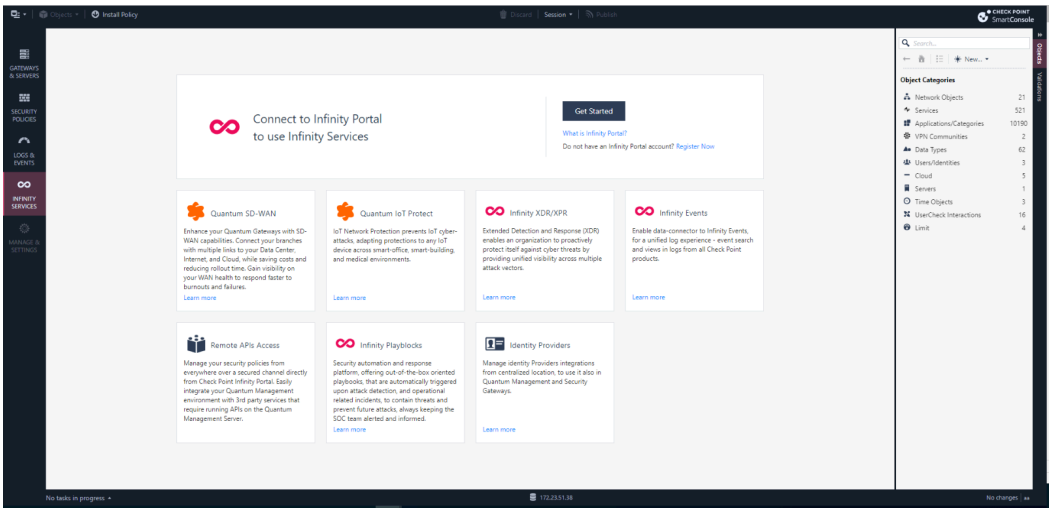
3.4.1. On-boarding the On-premises Check Point Security Management Server

This topic describes how to onboard an on-premises system to PlayBlocks. It provides step-by-step instructions to complete the onboarding workflow.

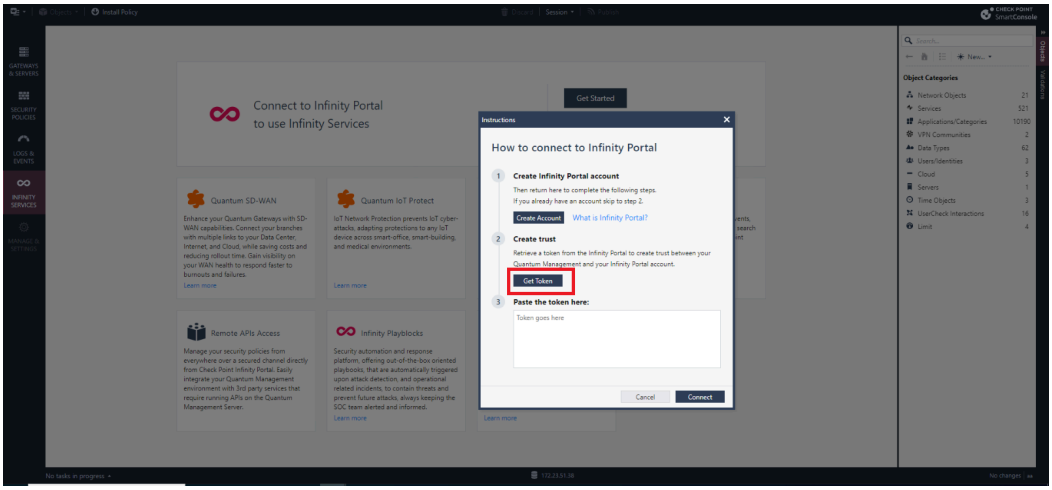
About this task:
To on-board the on-premises Check Point Security Management Server with Playblocks:

Procedure:

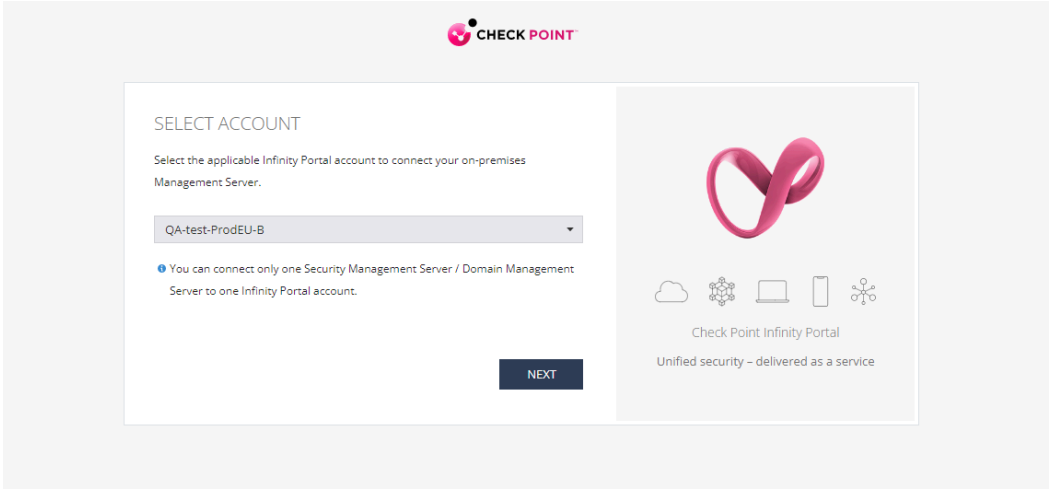
1. In the SmartConsole, navigate to the **Infinity Services** menu, and click **Get Started**.



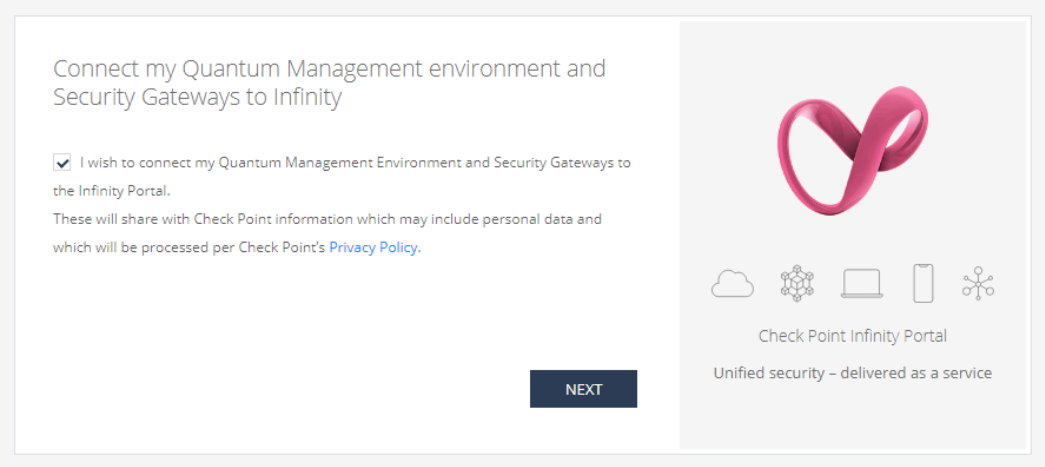
2. In the **Instructions** window, click **Get Token**.



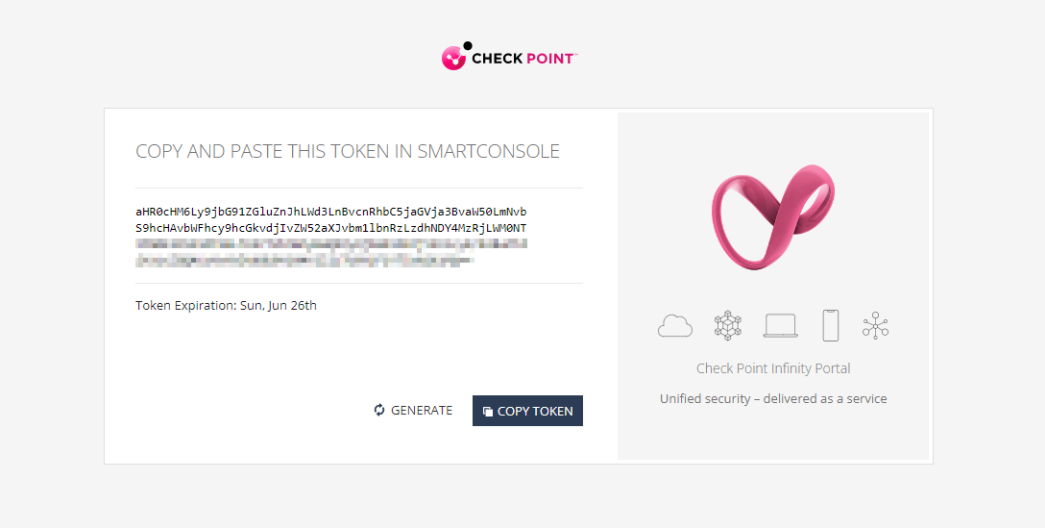
3. Select the registered account and click **Next**.



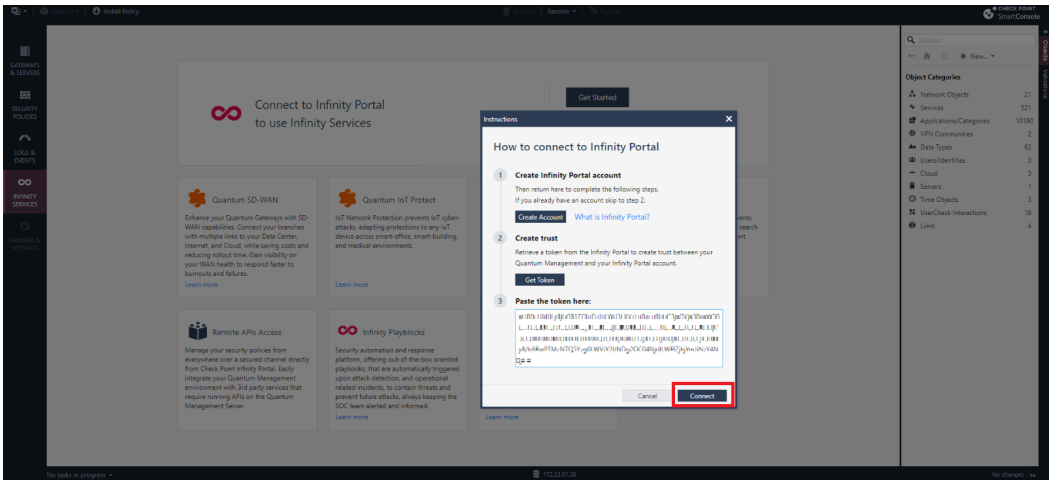
4. Accept the terms of service and click **Next**.



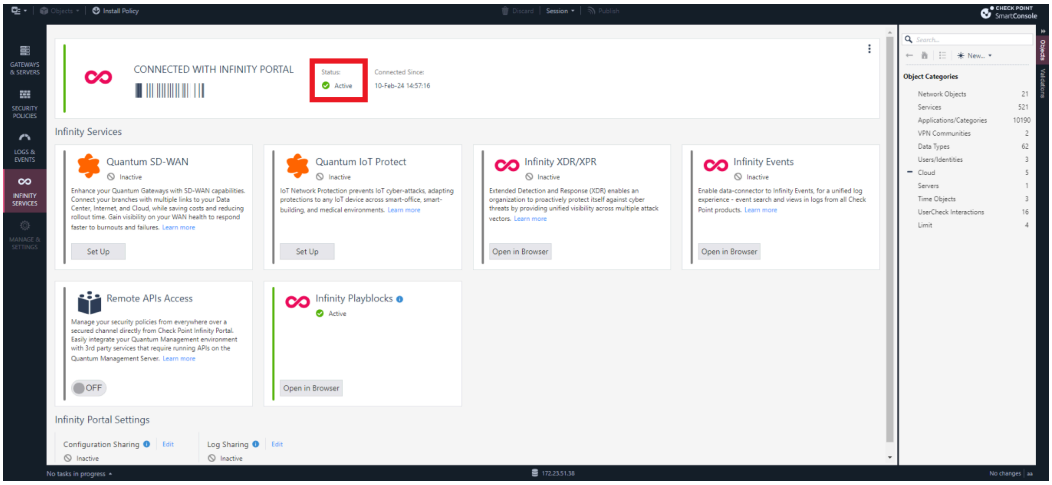
5. Click **Copy Token**.



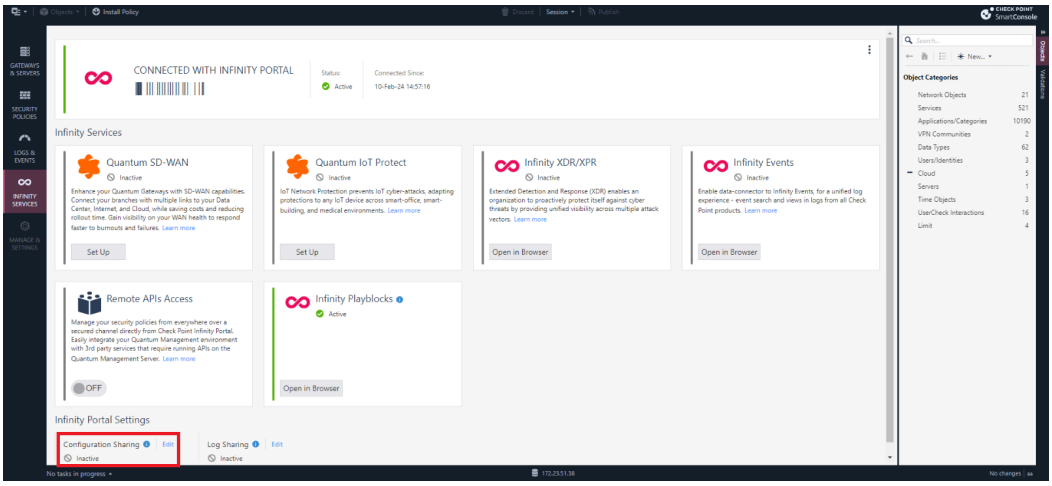
6. In the **Instructions** window, paste the token and click **Connect**.



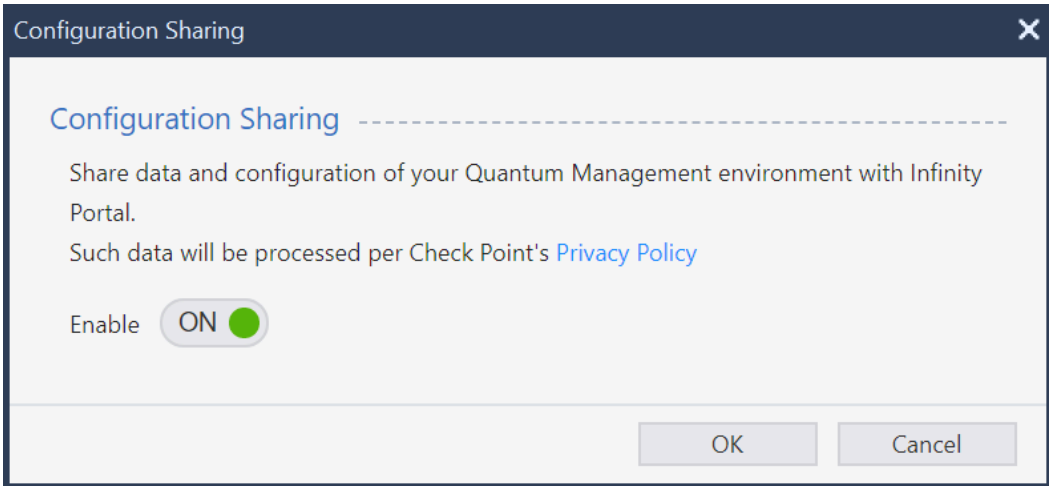
When the SmartConsole connects to the Check Point Portal, the **Connectivity Status** changes to **Active**.



7. Go to the **Data Sharing** section and click **Edit** for **Configuration Sharing**.



The **Configuration Sharing** pop-up appears.



8. Turn on the toggle button to enable and click **OK**.

   After the Configuration Sharing completes the initial synchronization, the status changes to **Active**.

> **Note:**
>
> If you want to view statistics in the Monitor *(on page 215)* page, then enable **Log Sharing**.

4. Video Tutorials

4.1. How to create a workflow to send Microsoft Teams notifications for actions taken by Playblocks

This topic provides a video tutorial showing how to create a workflow that sends Microsoft Teams notifications for actions taken by Playblocks. It summarizes the configuration process and connector setup.

https://embed.app.guidde.com/playbooks/qBUQP4eiXRAg9tmFLRZiGx

4.2. How to configure ServiceNow Ticketing connector

This topic explains how to configure the ServiceNow Ticketing connector in Playblocks. It provides the required steps and prerequisites for creating and preparing a ServiceNow account.

About this task:

How to configure ServiceNow Ticketing connector

https://embed.app.guidde.com/playbooks/rsKyMXKzGc5woqtkHKM83S

Procedure:

4.3. How to configure Jira Ticketing Connector

This topic describes how to configure the Jira Ticketing Connector in Playblocks. It provides the required steps to prepare Jira and enter configuration details.

About this task:

How to configure Jira Ticketing Connector

https://embed.app.guidde.com/playbooks/j1Sy8c5F5kvstDTWPuMf1A

Procedure:

1. Log into your Atlassian account and copy the endpoint URL of the Jira instance.
2. Click the profile icon and select **Manage account**.
3. Click the **Security** tab and then click **Create and manage API tokens**.
4. In the API tokens page, click **Create API token**.
5. In the **Label** field, enter a name for the token and click **Create**.
6. Click **Copy** to copy the token.

   Note:

   After this step, you cannot retrieve the token.

7. Access the Playblocks Administration portal and click **Connectors**.
8. Click **Jira Ticketing**.

9. Turn on the **Enable** toggle button and fill in these details:
    - **Name** - Enter a name for the Jira instance in Playblocks. This name will not be used outside of the Playblocks application.
    - **URL** - Enter the endpoint URL of the Jira instance that you copied.
    - **Username** - Enter the email address of a user as the username for this instance.
    - **Password** - Paste the API token that you created in the Atlassian account.
    - **Version** - Enter the API version of Jira. The default version is 2.
10. Click **Fetch**.

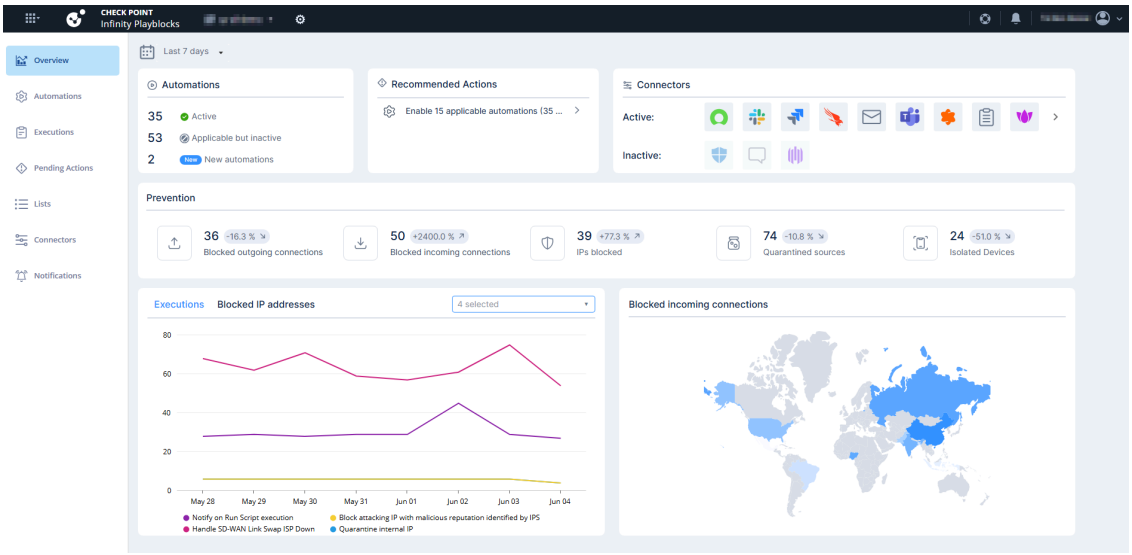
    After authentication, the predefined ticket types used for opening a ticket in Jira section appears.
11. Enter the required details and click **Save**.

5. Overview

This topic describes the Overview page, which displays key information and statistics about Playblocks. It explains how to access the Overview page and view its data.

In the **Overview** page, you can see important information and statistics that helps you get visibility on the prevention value that you get out of Playblocks. You can find details on top attacking countries, most frequently executed automations and important recommendations.

To view the **Overview** page, access **Playblocks** and click **Overview**.



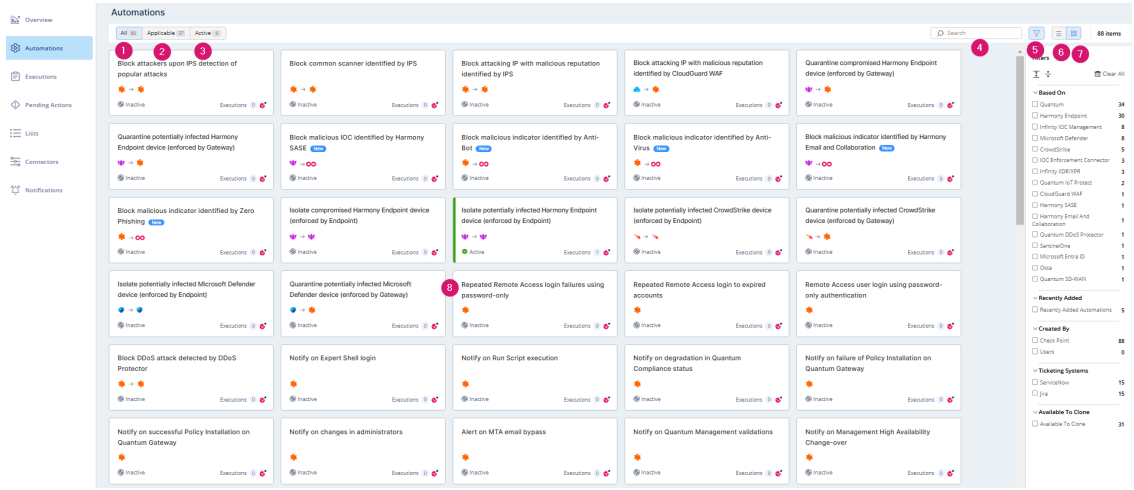
6. Automations

This topic describes the Automations page and its interface elements. It provides details about automation categories, views, filtering options, and automation card components.

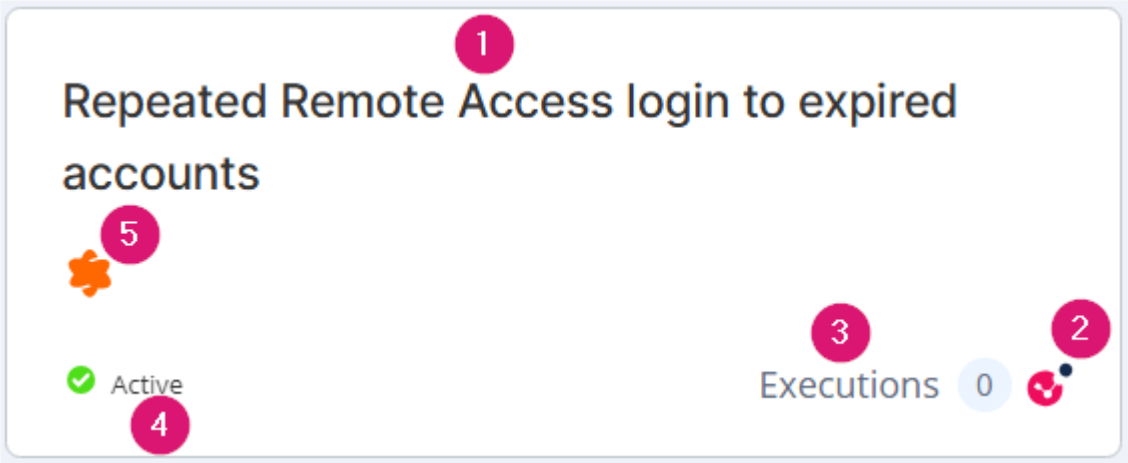
Automations are a set of predefined preventives or mitigative actions that Playblocks executes automatically. When a malicious activity is detected in a Check Point Security Gateway log or when the XDR recommends a preventive action on the Check Point Security Gateway, Playblocks automatically correlates this to a predefined automation and executes it.

You can customize automations according to your organization's needs. For information on how to customize automation, see Customization in Playblocks *(on page 141)*.

To view the **Automations** page, access **Playblocks** and click **Automations**.



Leg-end	Item	Description
1	All	Displays all automations supported by Playblocks.
2	Applic-able	Displays only the applicable automations based on your onboarded products.
3	Active	Shows all enabled *(on page 138)* automations.
4	Search	Search for an automation.
5	Filter	Filter the automations based on the source of the automation, recently added automations, created by ticketing systems, and available to clone.
6	List	Displays automations in a list view.
7	Card	Displays automation in a card view.

Leg-end	Item	Description
8	Au-toma-tions	Automation card.  **1** Click to view Automation Parameters and Flowchart *(on page 31)*. **2** Owner who created the automation. **3** Number of times the automation executed in the last seven days (default). **4** Automation status: • Inactive (not enabled) • Active (enabled *(on page 138)*) **5** Source of the automation: • Quantum: ◦ Check Point Security Gateway ◦ Check Point Security Management Server ◦ IoT Security ◦ Quantum SD-WAN • Endpoint Security • Infinity IOC Management • Okta • Microsoft Entra ID • Microsoft Defender

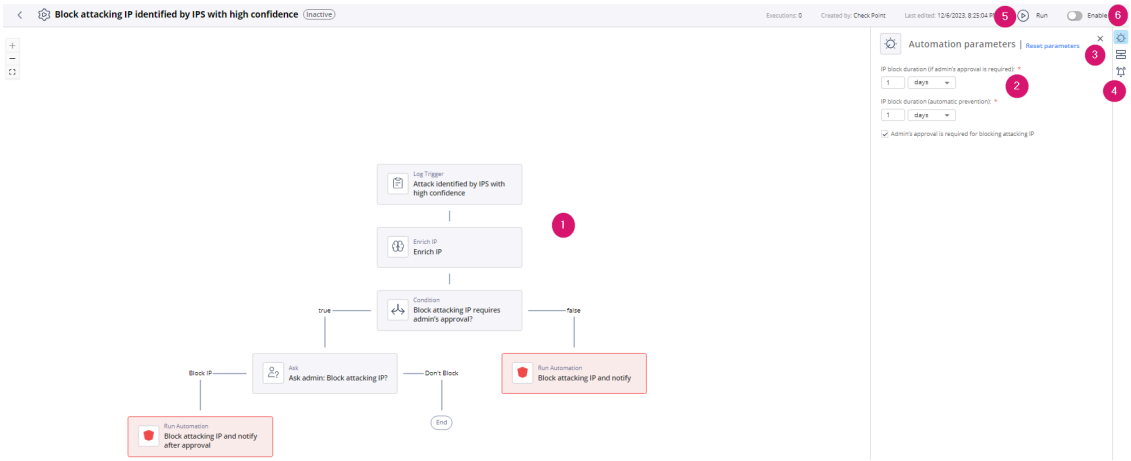
6.1. Automation Parameters and Flowchart

This topic describes the Automation Parameters and Flowchart page and outlines the items displayed in the interface. It also provides steps to access the automation details.

You can set parameters for automation, for example, the amount of time until expiration. The Automation Flowchart shows the steps in the automation.

To view the **Automation Parameters and Flowchart** page:

1. Access **Playblocks** and click **Automations**.
2. Click an automation card.



Item	Description
1	Flowchart (Read-only). Click a step to view the General, Branch Options and Example Output on the right side.
2	Automation Parameters. *(on page 136)*
3	Trigger: • General (Read-only). Shows parameters of the selected step. • Branch options (Read-only). Shows advanced options to handle errors in the selected step. • Example output (Read-only). Shows possible outputs for the selected step.
4	Edit the notification *(on page 257)* profile.
5	Run the automation. *(on page 136)*
6	Enable the automation. *(on page 138)*

6.2. Predefined Automations

This topic lists predefined automations available in the system. It provides links to automation actions triggered by various security detections and events.

Playblocks has these predefined automations:

6.2.1. Block attackers upon IPS detection of popular attacks

This topic describes automation that blocks attackers based on IPS-detected popular attacks and outlines supported products, parameters, triggers, and flow details.

The automation blocks attackers across the organization and is triggered by popular attacks that are detected by IPS. The notification includes information on the attack and the attacker. More parameters can be set using the automation parameters such as the block duration, whether the block is automatic or upon administrators approval, and more.

Supported Product

Check Point Security Management Server (Quantum)

Parameters

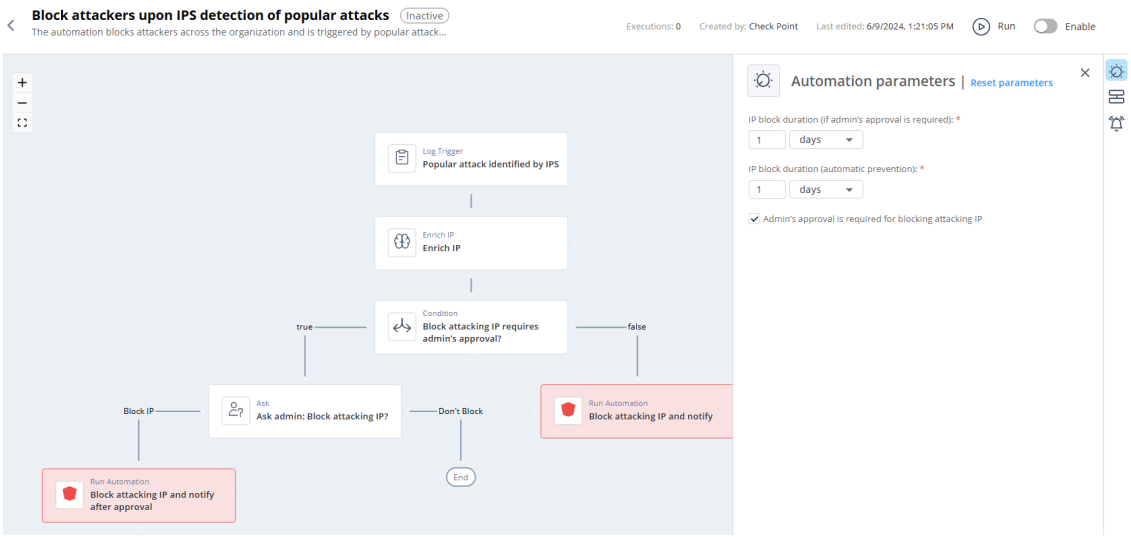
IP Block duration (if admin's approval is required)	Set the expiration period for the automation. This applies only if you have selected the **Admin's approval is required for blocking attacking IP** checkbox. After the expiration, Playblocks sends the notification for the Administrator's approval.
IP block duration (automatic prevention)	Set the expiration period for the automations that are executed automatically (without the Administrator's approval). The default duration is **1 day**.
Admin's approval is required for blocking attacking IP	Select the checkbox if you want Administrator's approval to execute the automation. Check Point recommends that you leave **Admin's approval is required for blocking attacking IP** checkbox unselected.

Trigger

Matching attacking IP address identified by IPS blade with high confidence.

To view the example of this log, click Run.

Flow



6.2.2. Block common scanner identified by IPS

This topic describes automation that blocks scanners detected by the IPS blade with high confidence and outlines its parameters, trigger, and flow.

The automation blocks scanners across the organization and is triggered by scans that are detected by IPS blade with very high confidence. The notification includes information on the scan and the scanner.

Supported Product

Check Point Security Management Server (Quantum)

Parameters

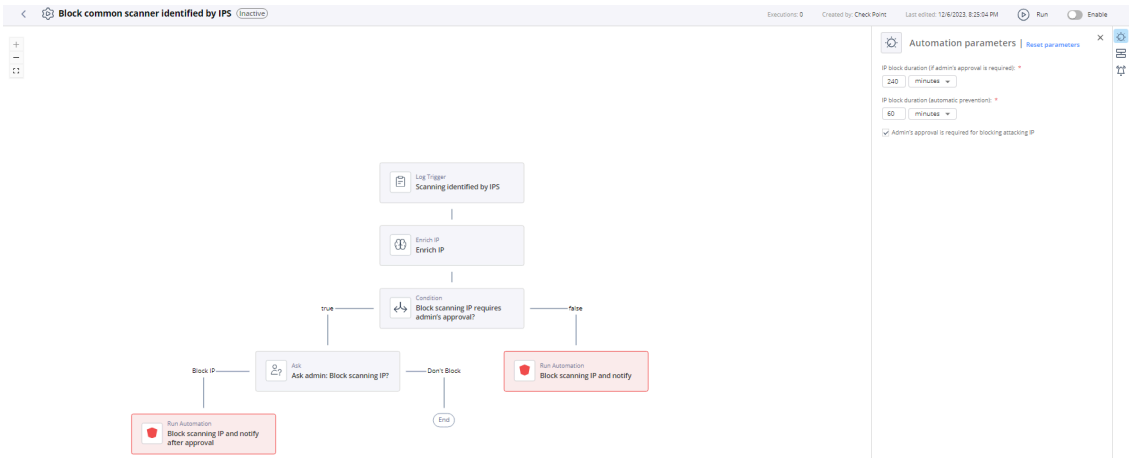
IP Block duration (if admin's approval is required)	Set the expiration period for the automation. This applies only if you have selected the **Admin's approval is required for blocking scanning IP** checkbox. After the expiration, Playblocks sends the notification for the Administrator's approval.
IP block duration (automatic prevention)	Set the expiration period for the automations that are executed automatically (without the Administrator's approval). The default duration is **1 day**.
Admin's approval is required for blocking scanning IP	Select the checkbox if you want Administrator's approval to execute the automation. Check Point recommends that you leave **Admin's approval is required for blocking scanning IP** checkbox unselected.

Trigger

Matching common scanner identified by IPS.

To view the example of this log, click Run.

Flow



6.2.3. Block attacking IP with malicious reputation identified by IPS

This topic describes the automation that blocks attackers flagged as malicious by IP reputation services and triggered by IPS-detected attacks. It also lists supported products, parameters, triggers, and workflow details.

Supported Product

Check Point Security Management Server (Quantum)

The automation blocks attackers across the organization that are flagged as malicious by IP reputation services and is triggered by attacks that are detected by IPS. The notification includes information on the attack and the attacker.

Parameters

IP Block duration (if admin's approval is required)	Set the expiration period for the automation. This applies only if you have selected the **Admin's approval is required for blocking attacking IP** checkbox. After the expiration, Playblocks sends the notification for the Administrator's approval.
IP block duration (automatic prevention)	Set the expiration period for the automations that are executed automatically (without the Administrator's approval). The default duration is **1 day**.
Admin's approval is required for blocking attacking IP	Select the checkbox if you want Administrator's approval to execute the automation. Check Point recommends that you leave **Admin's approval is required for blocking attacking IP** checkbox unselected.

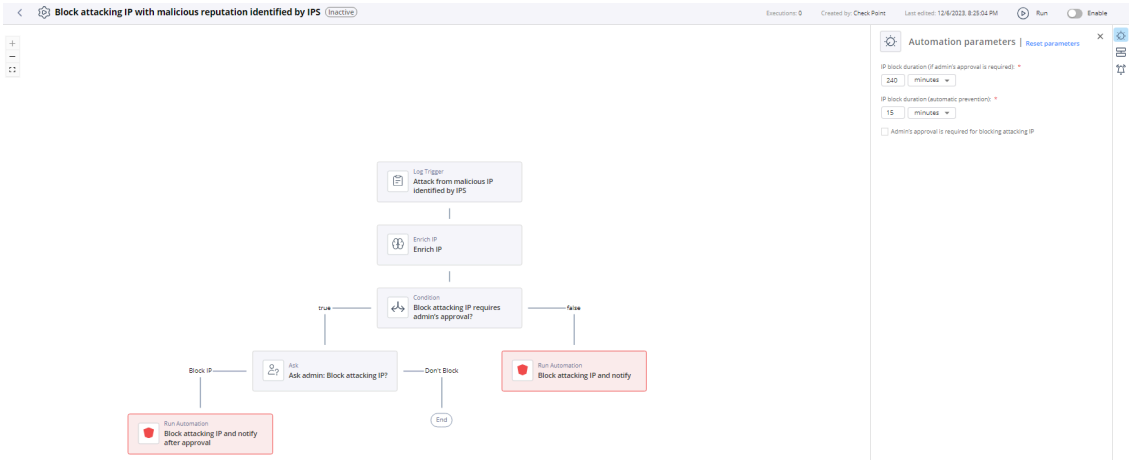
Trigger

Matching attacking IP with malicious reputation identified by IPS.

In this automation, the log is triggered not only by the log itself but also by verifying if the IP is flagged as malicious by IP reputation services.

To view the example of this log, click Run.

Flow



6.2.4. Block attacking IP with malicious reputation identified by WAF Application Security

This topic describes the automation that blocks attacking IP addresses identified with malicious reputation and outlines supported products, parameters, trigger details, and flow.

Supported Products

- WAF Application Security
- Check Point Security Management Server (Quantum)

Parameters

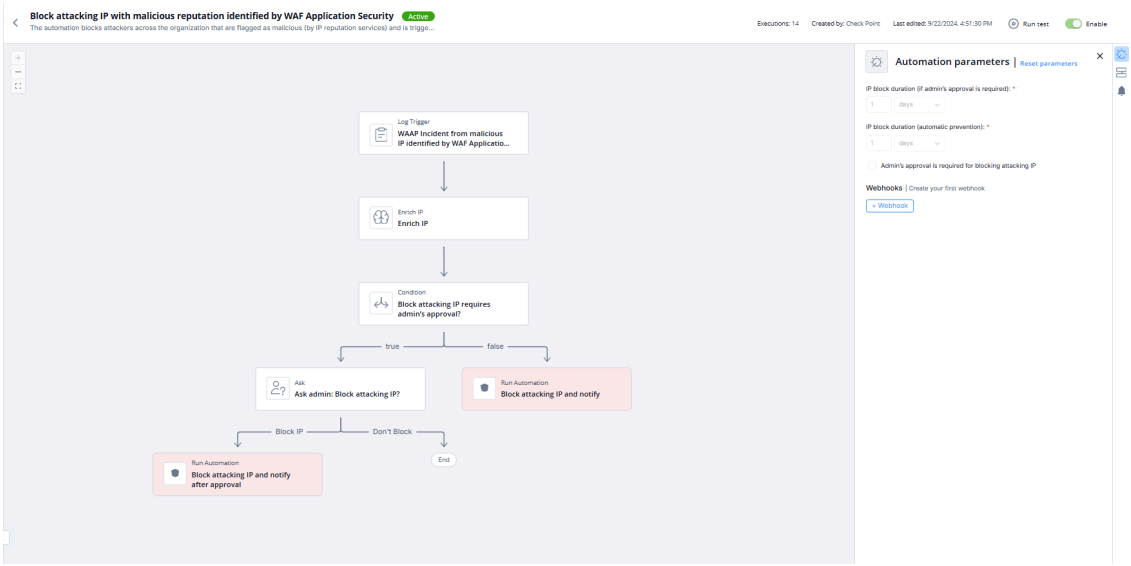
IP block duration (if admin's approval is required)	Set the expiration period for the automation. This applies only if you have selected the **Admin's approval is required for blocking attacking IP** checkbox. After the expiration, Playblocks sends the notification for the administrator's approval.
IP block duration (automatic prevention)	Set the expiration period for the automations that are executed automatically (without the administrator's approval). The default duration is **1 day**.
Admin's approval is required for blocking attacking IP	Select the checkbox if you want administrator's approval to execute the automation. Check Point recommends that you leave **Admin's approval is required for blocking attacking IP** checkbox unselected.

Trigger

Matching attacking IP with malicious reputation identified by WAF Application Security.

To view the example of this log, click Run.

Flow



6.2.5. Quarantine compromised Endpoint Security device (enforced by Firewall)

This topic describes settings and behavior for quarantining compromised Endpoint Security devices enforced by a Check Point Firewall. It includes supported products, parameters, trigger details, and flow information.

The automation blocks outgoing traffic from compromised devices (for example, ransomware), detected by Endpoint Security, to prevent lateral movement and communication with C&C (Command and Control).

Supported Product

- Check PointSecurity Management Server)
- Endpoint Security

Parameters

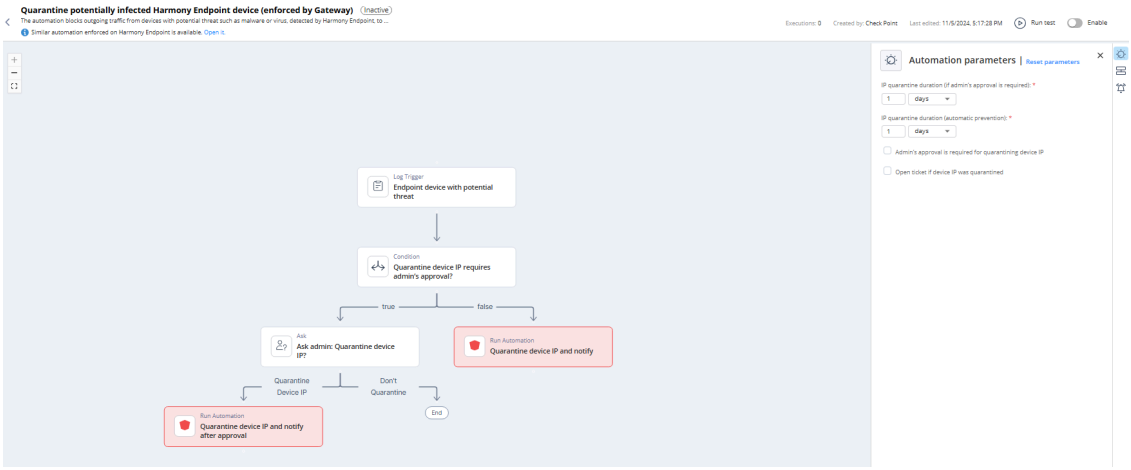
IP quarantine duration (if admin's approval is required)	Set the expiration period for the automation. This applies only if you have selected the **Admin's approval is required for quarantining device IP** checkbox. After the expiration, Playblocks sends the notification for the Administrator's approval.
IP quarantine duration (automatic prevention)	Set the expiration period for the automations that are executed automatically (without the Administrator's approval). The default duration is **1 day**.
Admin's approval is required for quarantining device IP	Select the checkbox if you want Administrator's approval to execute the automation. Check Point recommends that you leave **Admin's approval is required for quarantining device IP** checkbox unselected.
Open ticket if device IP was quarantined	Select the checkbox if you want to open a ticket when device IP was quarantined.

Trigger

Matching quarantine IP of compromised device identified by Endpoint.

To view the example of this log, click Run.

Flow



6.2.6. Quarantine potentially infected Endpoint Security device (enforced by Firewall)

This topic describes quarantining potentially infected Endpoint Security devices and provides details about supported products, parameters, triggers, and the automation flow. It explains configuration options and associated behaviors.

The automation blocks outgoing traffic from devices with potential threat such as malware or virus, detected by Endpoint Security, to prevent lateral movement or communication with C&C (Command and Control).

Supported Product

- Check Point Security Management Server
- Endpoint Security

Parameters

IP quarantine duration (if admin's approval is required)	Set the expiration period for the automation. This applies only if you have selected the **Admin's approval is required for quarantining device IP** checkbox. After the expiration, Playblocks sends the notification for the Administrator's approval.
IP quarantine duration (automatic prevention)	Set the expiration period for the automations that are executed automatically (without the Administrator's approval). The default duration is **1 day**.
Admin's approval is required for quarantining device IP	Select the checkbox if you want Administrator's approval to execute the automation. Check Point recommends that you leave **Admin's approval is required for quarantining device IP** checkbox unselected.

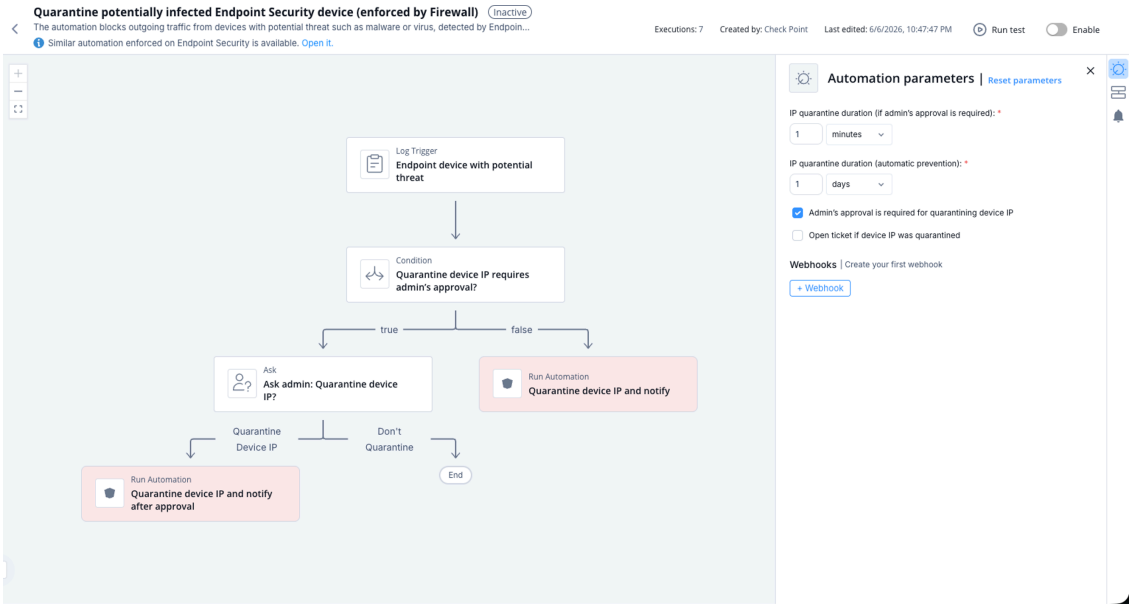
Open ticket if device IP was quarantined	Select the checkbox if you want to open a ticket when device IP was quarantined.

Trigger

Matching quarantine potentially infected Endpoint device.

To view the example of this log, click ../running-automation/running-the-automation.dita.

Flow



6.2.7. Notify on Firewall Traffic Blocked by Check Point SASE

This topic describes an automation that sends a notification when firewall traffic is blocked by Check Point SASE. It outlines supported product details, parameters, triggers, and flow.

This automation sends a notification when Firewall Traffic is blocked by Check Point SASE.

Supported Product

SASE

Parameters

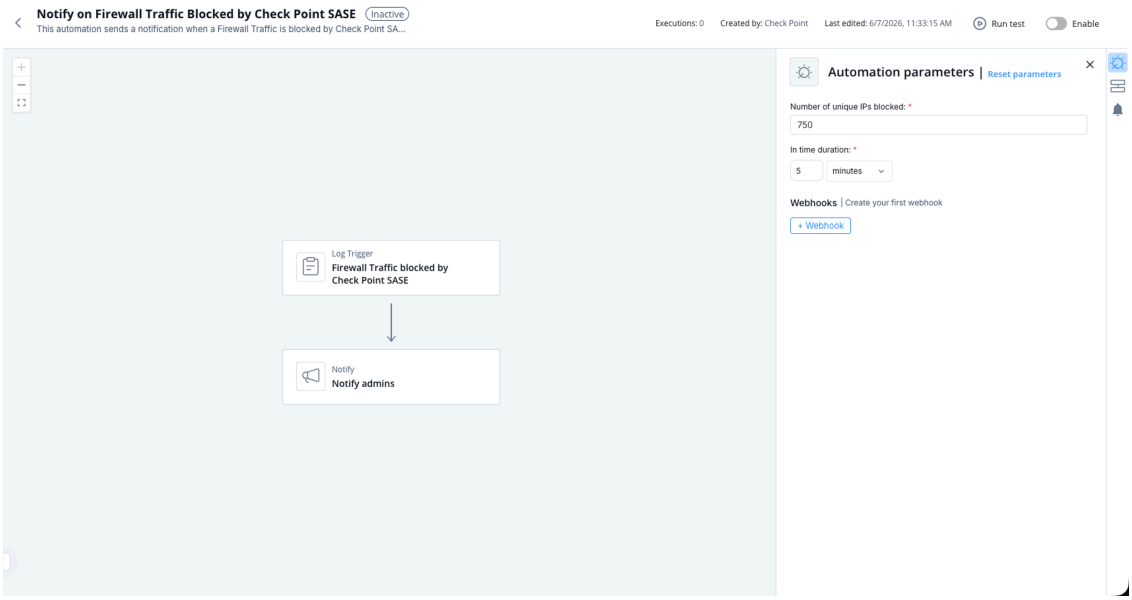
Number of unique IPs blocked	Set the minimum number of IPs blocked for the automation to be triggered.
In time duration	Set the time duration for the IPs blocked.

Trigger

When the number of unique IPs blocked in a time duration exceeds the values specified in the automation parameters.

To view the example of this log, click ../running-automation/running-the-automation.dita.

Flow



6.2.8. Notify on URL filtering blocked by Check Point SASE

This topic describes an automation that sends notifications when standard risk URL filtering events are blocked by Check Point SASE and explains its parameters and trigger conditions.

This automation sends a notification when a standard risk URL filtering is blocked by Check Point SASE.

Supported Product

SASE

Parameters

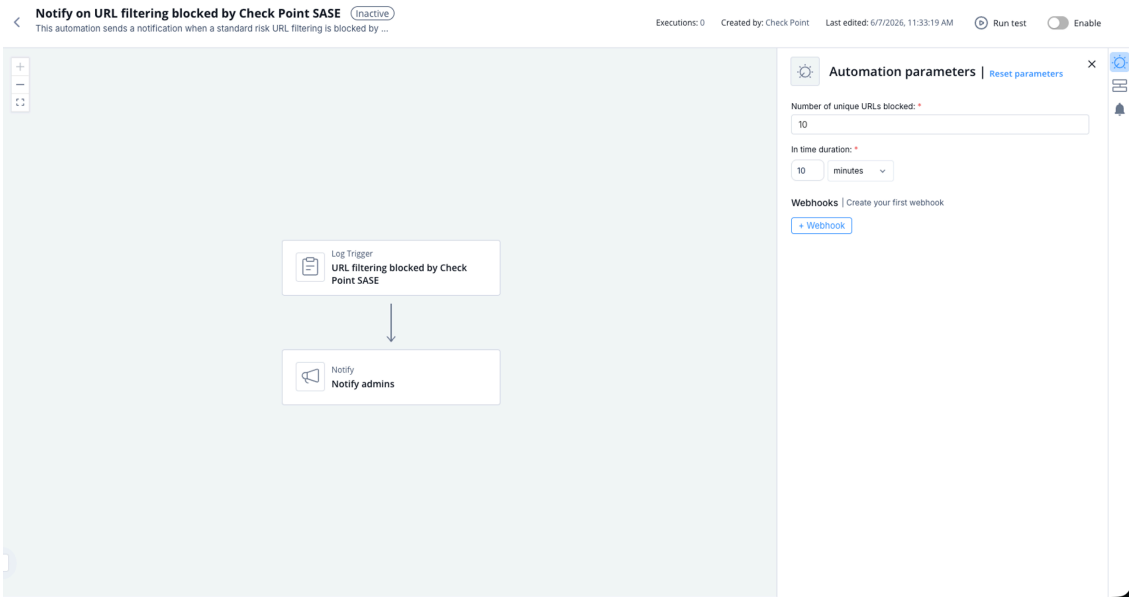
Number of unique URLs blocked	Set the minimum number of URLs blocked for the automation to be triggered.
In time duration	Set the time duration for the URLs blocked.

Trigger

When the number of unique URLs blocked in a time duration exceeds the values specified in the automation parameters.

To view the example of this log, click ../running-automation/running-the-automation.dita.

Flow



6.2.9. Notify on URL Reputation Identification by Check Point SASE

This topic describes the automation that sends notifications when a URL reputation is detected by Check Point SASE and outlines its parameters, trigger conditions, and workflow.

This automation sends an immediate notification when a URL Reputation is detected by SASE.

Supported Product

SASE

Parameters

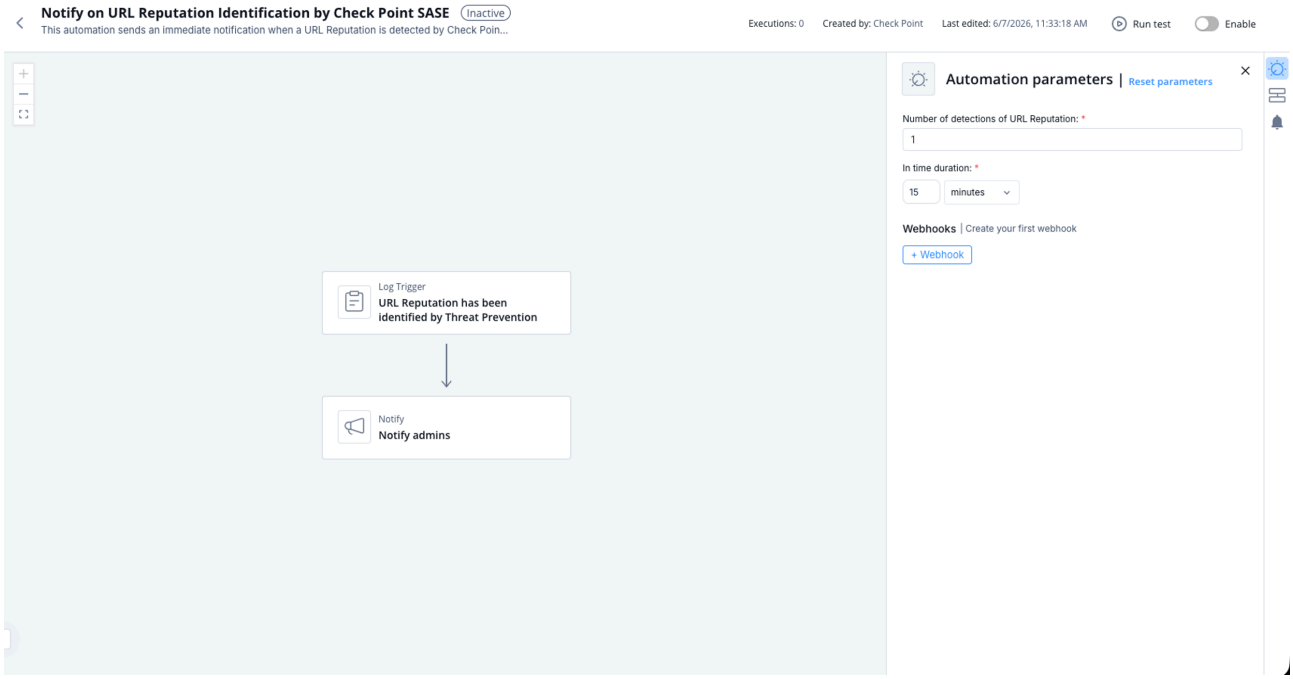
Number of detections of URL Reputation	Set the minimum number of detections for the automation to be triggered.
In time duration	Set the time duration for the URL reputations.

Trigger

When the number of detections of URL reputation in a time duration exceeds the values specified in the automation parameters.

To view the example of this log, click ../running-automation/running-the-automation.dita.

Flow



6.2.10. Notify on Tunnel Up by SASE

This topic describes an automation that notifies when a SASE tunnel is detected as up. It explains supported products, parameters, trigger conditions, and flow.

Check Point Playblocks Administration Guide

Notify on Tunnel Up by SASE

This automation notifies when a SASE Tunnel is detected as up. The notification includes information such as the tunnel name. Tunnels listed under **SASE Tunnels Excluded from Alerts** are not counted.

Supported Product

Check Point SASE

Parameters

Parameter	Description
Alert again after	Set the frequency to receive alerts again on the same Tunnel.

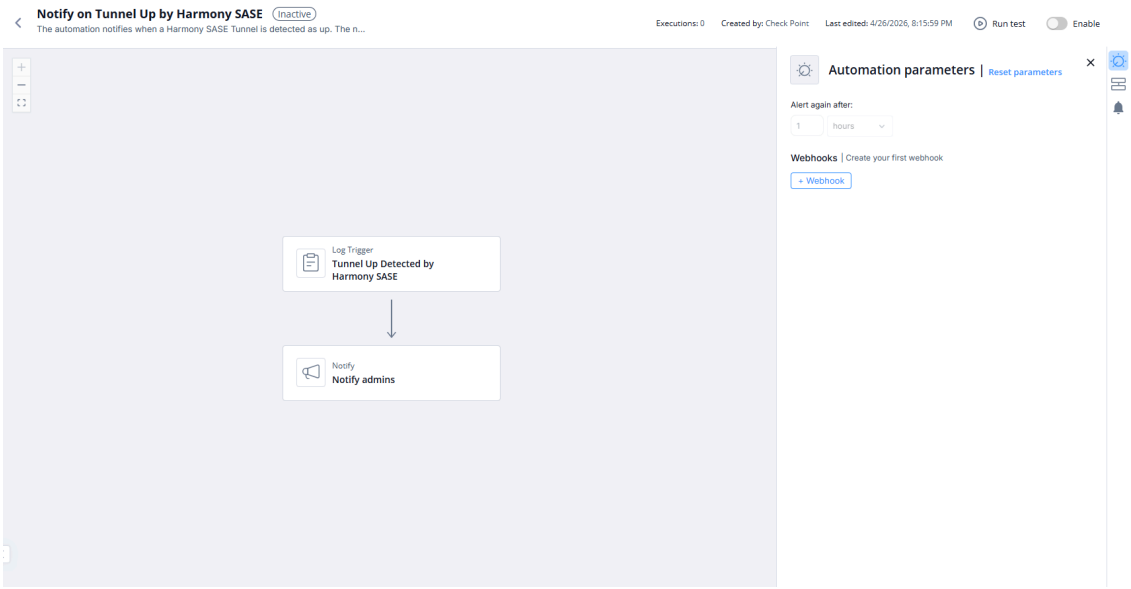
Trigger

The automation is triggered when a Check Point SASE tunnel is detected as up.

To view the example of this log, click Run *(on page 136)*.

Flow

Notify on Tunnel Up by Check Point SASE Automation Flowchart



6.2.11. Notify on Tunnel Down by Check Point SASE

This topic describes the automation that sends notifications when a Check Point SASE tunnel is detected as down and outlines its parameters, trigger, and flow.

This automation sends a notification when a Check Point SASE tunnel is detected as down. The notification includes the tunnel name. Tunnels listed under **SASE Tunnels Excluded from Alerts** are excluded from triggering the automation.

Supported Product

SASE

Parameters

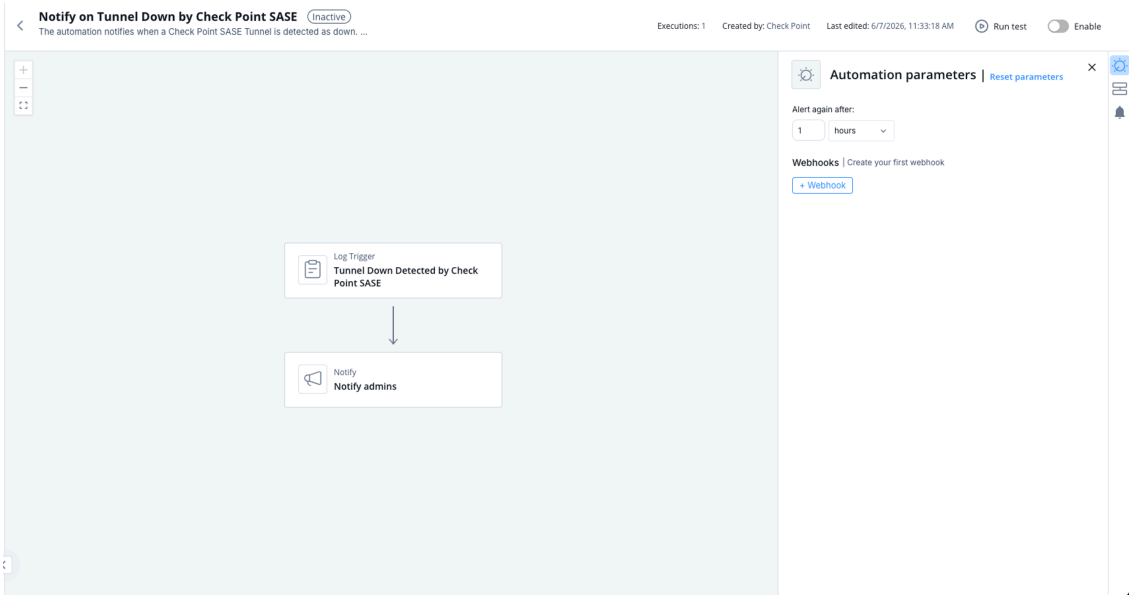
Alert again after	Set the time interval to send another alert for the same tunnel.

Trigger

When a Check Point SASE tunnel status is detected as down.

To view the example of this log, click Run.

Flow



6.2.12. Notify on Malicious File Detection by Check Point SASE

This topic describes an automation that sends notifications when a malicious file is detected by Check Point SASE Threat Prevention. It includes supported product details, configurable parameters, trigger conditions, and the automation flow.

This automation sends an immediate notification when a malicious file is detected by SASE Threat Prevention.

Supported Product

SASE

Parameters

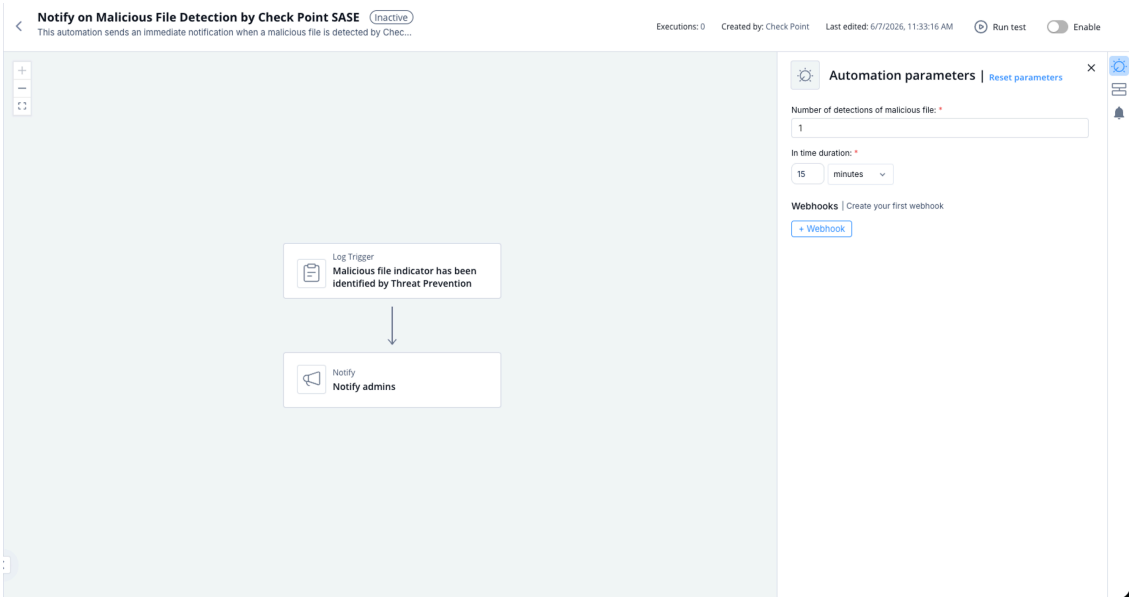
Number of detections of malicious file	Set the minimum number of detections for the automation to be triggered.
In time duration	Set the time duration for the malicious files.

Trigger

When the number of detections of malicious files in a time duration exceeds the values specified in the automation parameters.

To view the example of this log, click ../running-automation/running-the-automation.dita.

Flow



6.2.13. Block malicious file indicator identified by Threat Extraction Endpoint Security

This topic describes an automation that adds a malicious file indicator identified by Threat Extraction Endpoint Security to an IOC feed to enhance threat intelligence and response.

This automation adds the malicious file indicator identified by Threat Extraction Endpoint Security as an indicator to an IOC feed, updating threat intelligence and enhancing security response.

Supported Product

- Endpoint Security
- IoC Management

Parameters

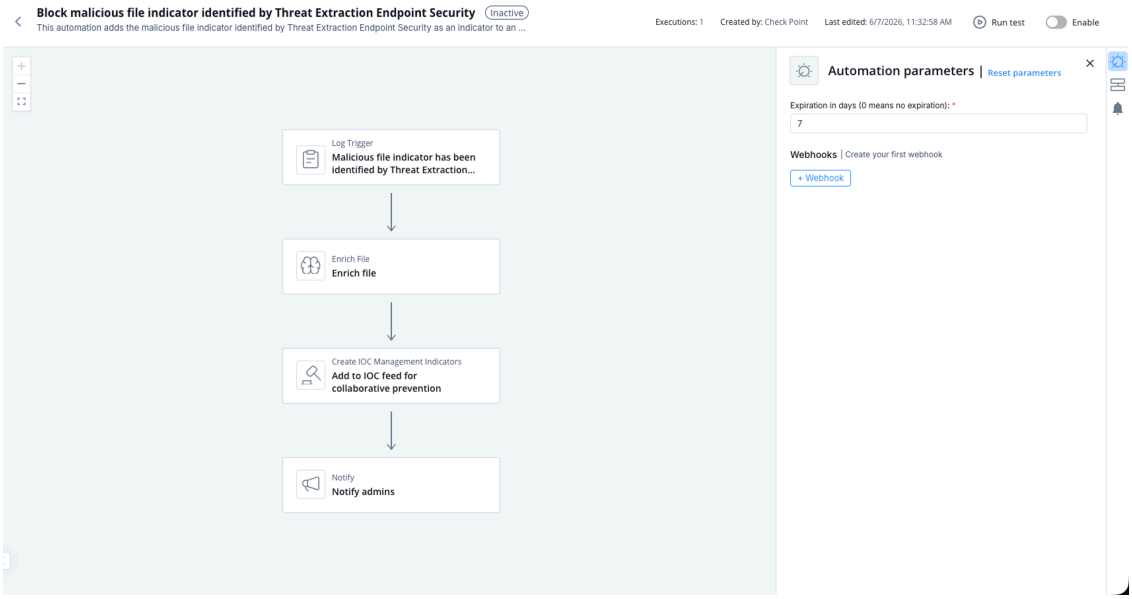
Expiration in days (0 means no expiration)	Set the expiration period for the automation.

Trigger

Matching malicious file indicator identified by Threat Extraction Endpoint Security with high confidence.

To view the example of this log, click ../running-automation/running-the-automation.dita.

Flow



6.2.14. Block malicious file indicator identified by Threat Emulation Endpoint Security

This topic describes the automation that adds a malicious file indicator identified by Threat Emulation Endpoint Security to an IOC feed for enhanced threat intelligence and response.

This automation adds the malicious file indicator identified by Threat Emulation Endpoint Security as an indicator to an IOC feed, updating threat intelligence and enhancing security response.

Supported Product

- Endpoint Security
- IoC Management

Parameters

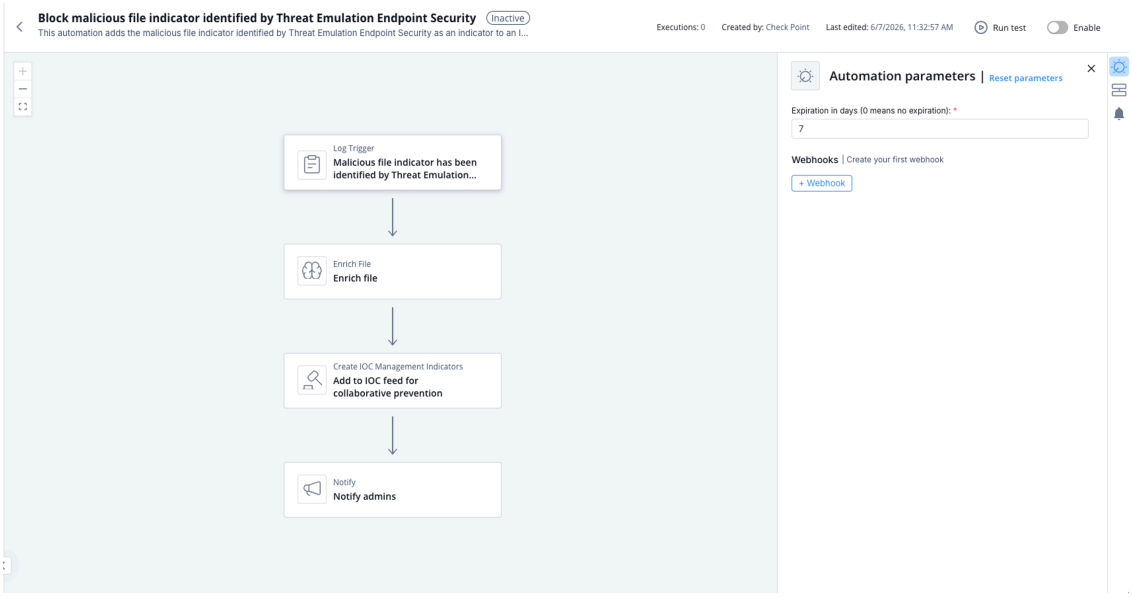
Expiration in days (0 means no expiration)	Set the expiration period for the automation.

Trigger

Matching malicious file indicator identified by Threat Emulation Endpoint Security with high confidence.

To view the example of this log, click ../running-automation/running-the-automation.dita.

Flow



6.2.15. Block malicious file indicator identified by Anti-Bot Endpoint Security

This topic describes an automation that adds malicious file indicators identified by Anti-Bot Endpoint Security to an IOC feed to enhance threat intelligence and security response. It outlines supported products, parameters, trigger conditions, and flow.

This automation adds the malicious file identified by Anti-Bot Endpoint Security as an indicator to an IOC feed, updating threat intelligence and enhancing security response.

Supported Product

- Endpoint Security
- IoC Management

Parameters

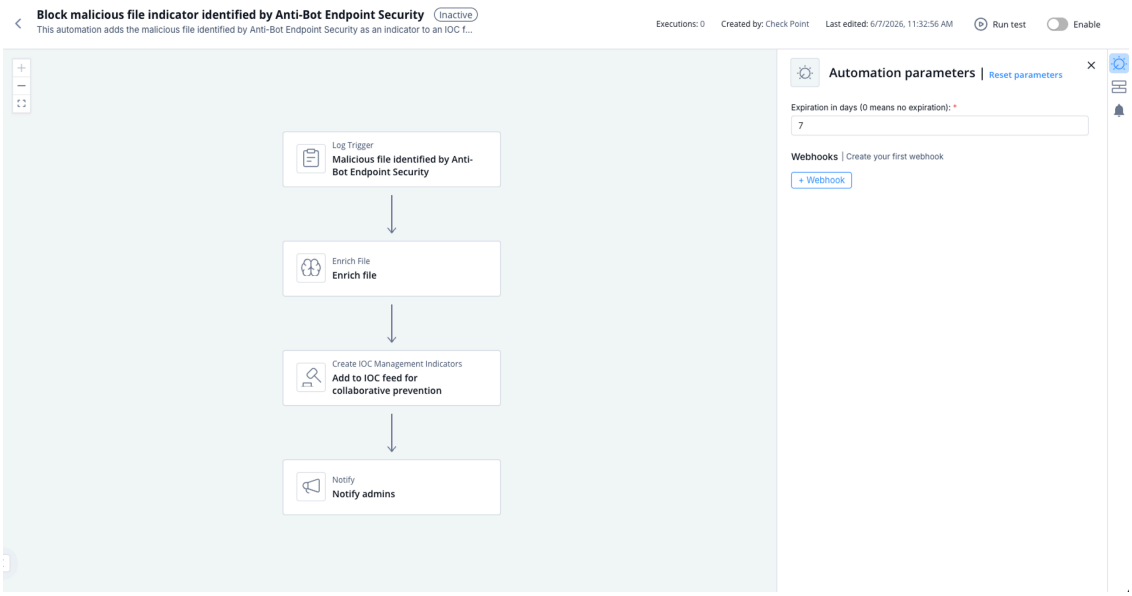
Expiration in days (0 means no expiration)	Set the expiration period for the automation.

Trigger

Matching malicious file indicator identified by Anti-Bot Endpoint Security with high confidence.

To view the example of this log, click ../running-automation/running-the-automation.dita.

Flow



6.2.16. Block malicious URL indicator identified by Anti-Bot Endpoint Security

This topic describes an automation that blocks malicious URL indicators identified by Anti-Bot Endpoint Security by adding them to an IOC feed to enhance threat intelligence and response.

This automation adds the malicious URL identified by Anti-Bot Endpoint Security as an indicator to an IOC feed, updating threat intelligence and enhancing security response.

Supported Product

- Endpoint Security
- IoC Management

Parameters

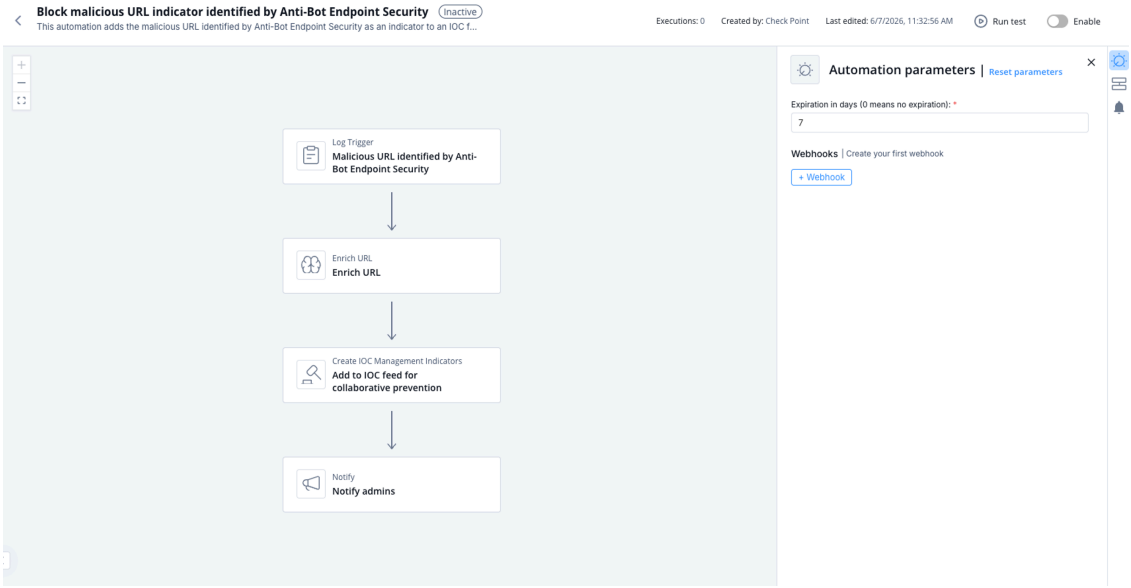
Expiration in days (0 means no expiration)	Set the expiration period for the automation.

Trigger

Matching malicious URL indicator identified by Anti-Bot Endpoint Security with high confidence.

To view the example of this log, click ../running-automation/running-the-automation.dita.

Flow



6.2.17. Block malicious IOC identified by SASE

This topic describes an automation that adds a malicious URL identified by SASE as an indicator to an IOC feed. It updates threat intelligence to enhance security response.

This automation adds the malicious URL identified by SASE Threat Prevention engines as an indicator to an IoC Feed, updating threat intelligence and enhancing security response.

Supported Product

- SASE
- IoC Management Management

Parameters

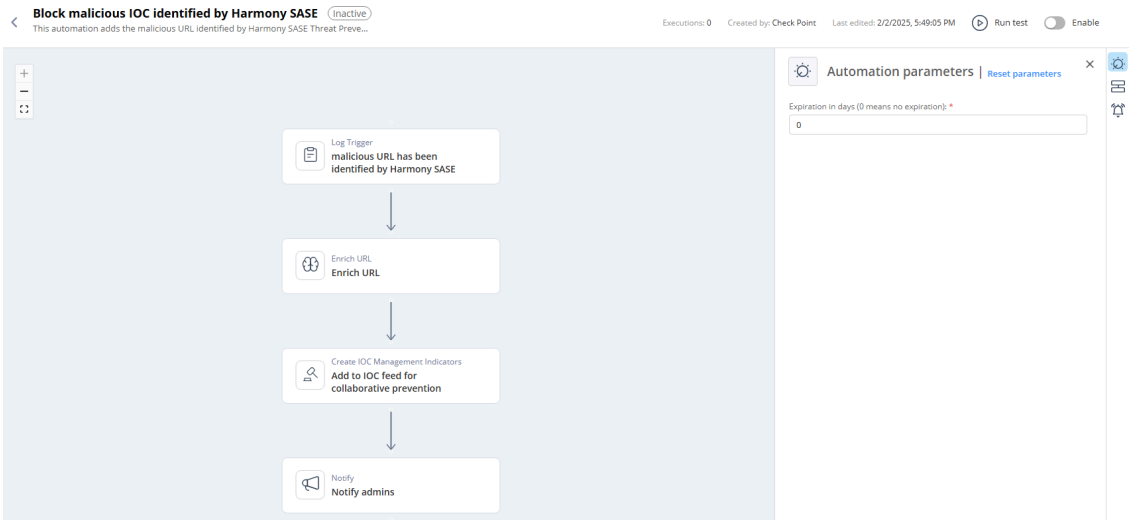
Expiration in days (0 means no expiration)	Set the expiration period for the automation

Trigger

Matching phishing URL identified by Anti-Bot blade with high confidence.

To view the example of this log, click Run.

Flow



6.2.18. Block malicious indicator identified by Anti-Bot

This topic describes an automation that adds a malicious URL identified by Anti-Bot to an IOC feed to enhance threat intelligence and security response.

Supported Product

- Check Point Security Management Server (Quantum)
- IoC Management Management

Parameters

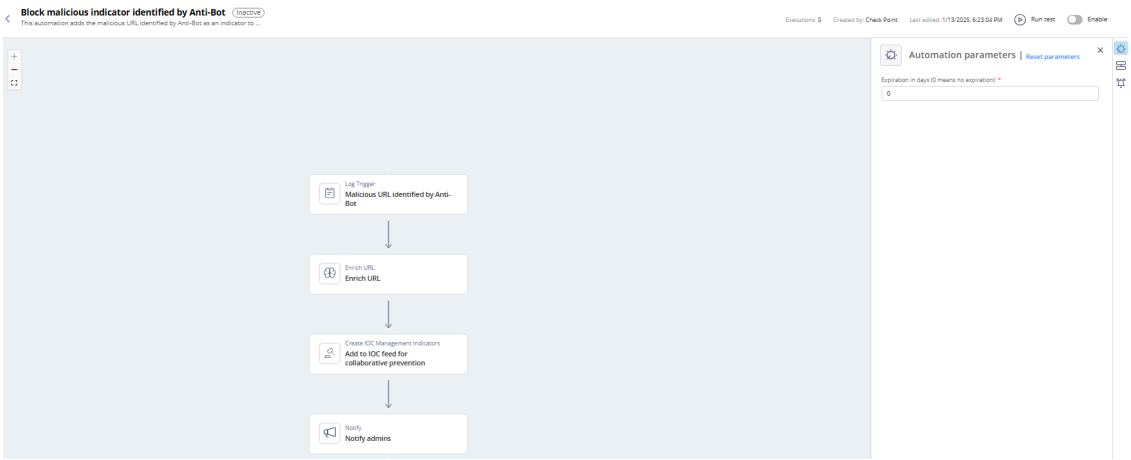
Expiration in days (0 means no expiration)	Set the expiration period for the automation

Trigger

Matching phishing URL identified by Anti-Bot blade with high confidence.

To view the example of this log, click Run.

Flow



6.2.19. Block malicious indicator identified by Anti-Virus

This topic describes how the automation blocks a malicious URL identified by Anti-Virus by adding it as an indicator to an IOC feed. It summarizes supported products, parameters, trigger conditions, and the automation flow.

Supported Product

- Check Point Security Management Server (Quantum)
- IoC Management Management

Parameters

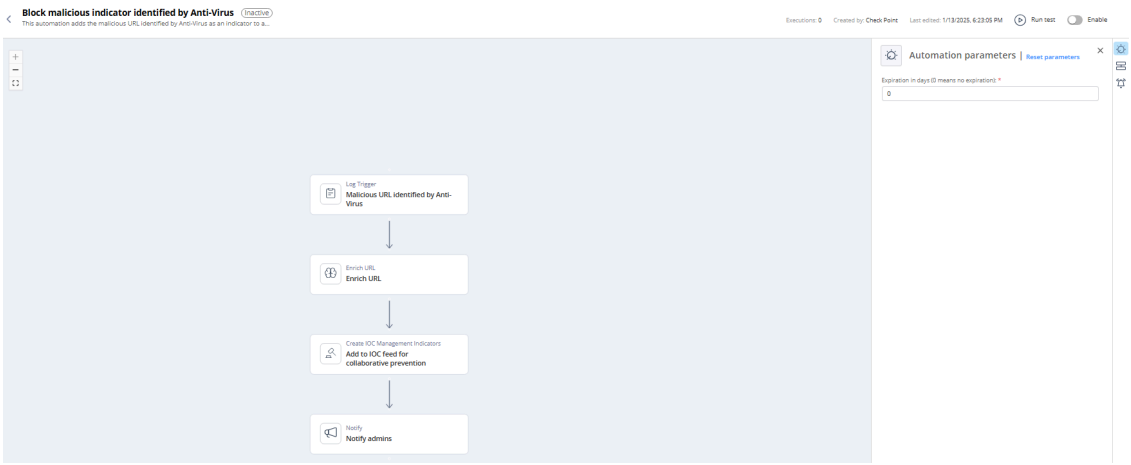
Expiration in days (0 means no expiration)	Set the expiration period for the automation

Trigger

Matching phishing URL identified by Anti-Virus blade with high confidence.

To view the example of this log, click Run.

Flow



6.2.20. Block malicious indicator identified by Zero Phishing Endpoint Security

This topic describes the automation that adds a malicious URL identified by Zero Phishing Endpoint Security to an IOC feed. It updates threat intelligence and enhances the security response.

This automation adds the malicious URL identified by Zero Phishing Endpoint Security as an indicator to an IOC feed, updating threat intelligence and enhancing security response.

Supported Product

- Endpoint Security
- IoC Management

Parameters

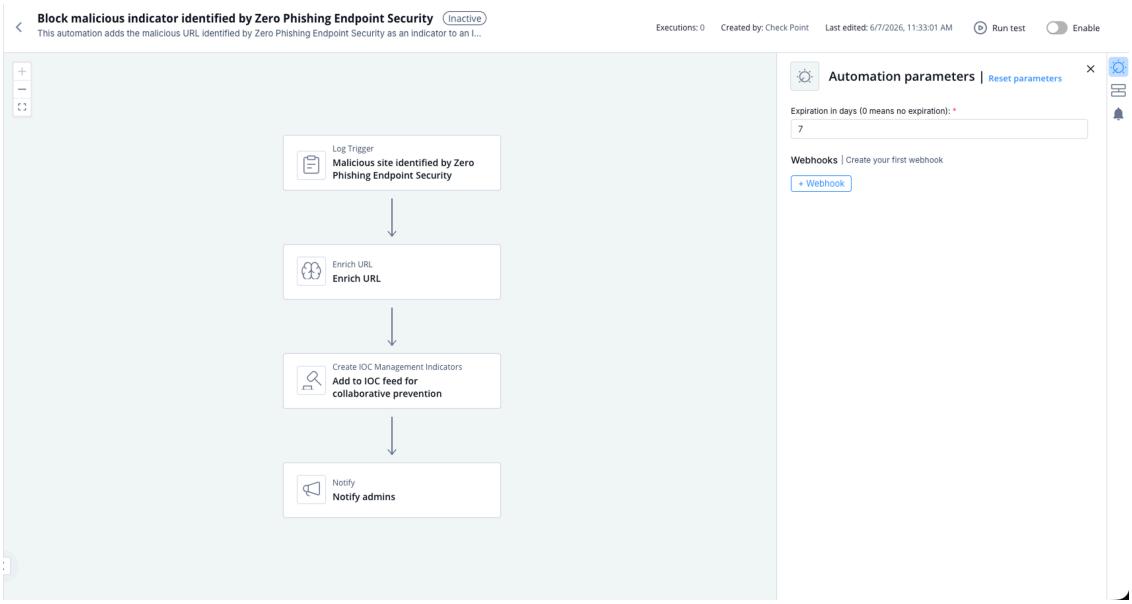
Expiration in days (0 means no expiration)	Set the expiration period for the automation.

Trigger

Matching malicious indicator identified by Zero Phishing Endpoint Security with high confidence.

To view the example of this log, click ../running-automation/running-the-automation.dita.

Flow



6.2.21. Block malicious indicator identified by Email Security

This topic describes an automation that adds a malicious URL identified by the Email Security blade as an indicator to an IOC feed. It helps update threat intelligence and enhance security response.

This automation adds the malicious URL identified by Email Security as an indicator to an IoC Feed, updating threat intelligence and enhancing security response.

Supported Product

- Email Security
- IoC Management Management

Parameters

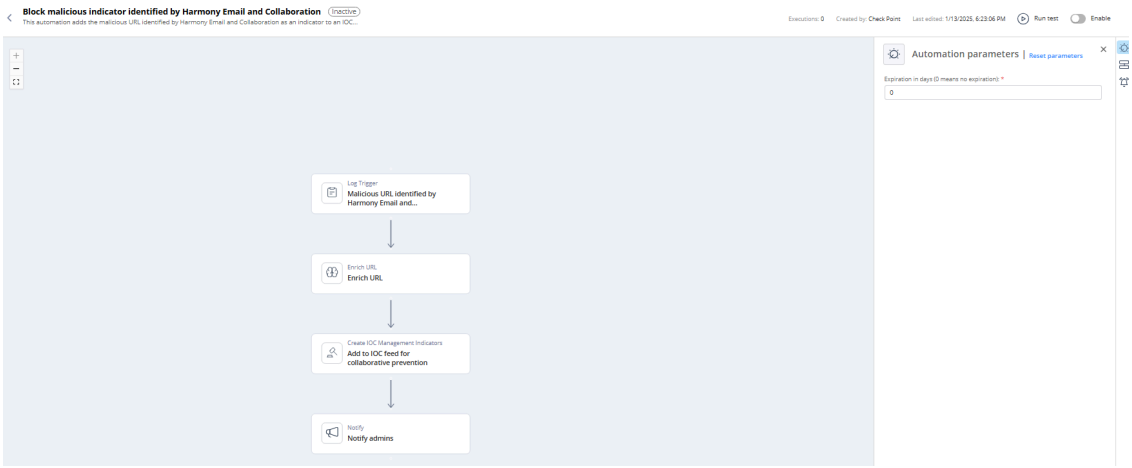
Expiration in days (0 means no expiration)	Set the expiration period for the automation

Trigger

Matching phishing URL identified by Email Security blade with high confidence.

To view the example of this log, click Run.

Flow



6.2.22. Block malicious indicator identified by Zero Phishing

This topic describes an automation that blocks a malicious URL identified by Zero Phishing by adding it as an indicator. It updates threat intelligence to enhance security response.

Supported Product

- Check Point Security Management Server (Quantum)
- IoC Management Management

Parameters

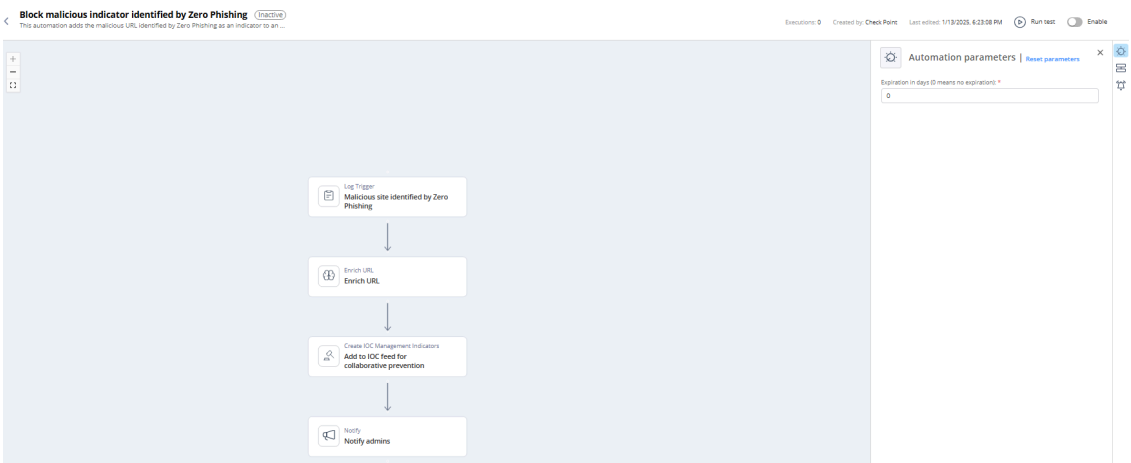
Expiration in days (0 means no expiration)	Set the expiration period for the automation

Trigger

Matching phishing URL identified by Zero Phishing blade with high confidence.

To view the example of this log, click Run.

Flow



6.2.23. Isolate compromised Endpoint Security device (enforced by Endpoint)

This topic describes the automation that isolates compromised Endpoint Security devices and details its supported product, parameters, trigger, and workflow.

The automation isolates compromised Endpoint Security devices (for example, following Ransomware), detected by Endpoint Security, to prevent the threat from spreading inside the organization. More parameters can be set using the automation parameters such as the isolation duration, whether the isolation is automatic or upon administrator approval, and so on.

Supported Product

Endpoint Security

Parameters

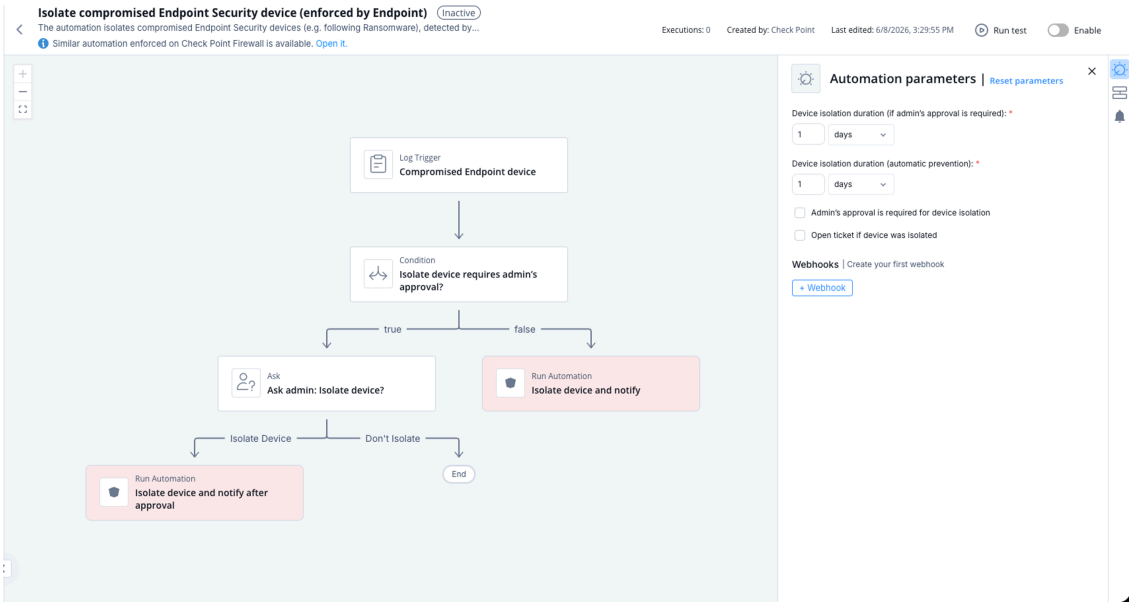
Device isolation duration (if admin's approval is required)	Set the expiration period for the automation. This applies only if you have selected the **Admin's approval is required for device isolation** checkbox. After the expiration, Playblocks sends the notification for the Administrator's approval.
Device isolation duration (automatic prevention)	Set the expiration period for the automations that are executed automatically (without the administrator's approval). The default duration is **1 day**.
Admin's approval is required for device isolation	Select the checkbox if you want administrator's approval to execute the automation. It is recommended that you leave the **Admin's approval is required for device isolation** checkbox unselected.
Open ticket if device was isolated	Select the checkbox if you want to open a ticket when device was isolated.

Trigger

Compromised Endpoint Security device.

To view the example of this log, click ../running-automation/running-the-automation.dita.

Flow



6.2.24. Isolate potentially Infected Endpoint Security device (enforced by Endpoint)

This topic describes the automation that isolates potentially infected Endpoint Security devices and lists its parameters, trigger conditions, and flow. It explains how the automation helps prevent threats from spreading inside an organization.

The automation isolates Endpoint Security devices with potential threat such as malware or virus, detected by Endpoint Security, to prevent the threat from spreading inside the organization. More parameters can be set using the automation parameters such as the isolation duration, whether the isolation is automatic or upon administrators approval, and so on.

Supported Product

Endpoint Security

Parameters

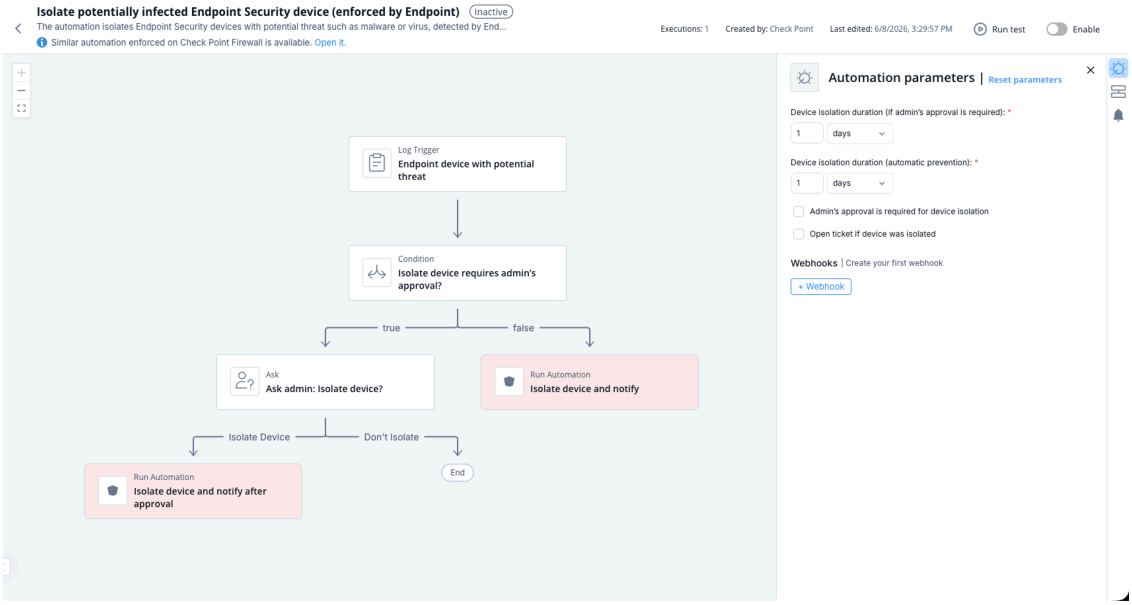
Device isolation duration (if admin's approval is required)	Set the expiration period for the automation. This applies only if you have selected the **Admin's approval is required for device isolation** checkbox. After the expiration, Playblocks sends the notification for the Administrator's approval.
Device isolation duration (automatic prevention)	Set the expiration period for the automations that are executed automatically (without the administrator's approval). The default duration is **1 day**.
Admin's approval is required for device isolation	Select the checkbox if you want administrator's approval to execute the automation. It is recommended that you leave the **Admin's approval is required for device isolation** checkbox unselected.
Open ticket if device was isolated	Select the checkbox if you want to open a ticket when device was isolated.

Trigger

Compromised Endpoint Security device.

To view the example of this log, click ../running-automation/running-the-automation.dita.

Flow



6.2.25. Isolate potentially infected SentinelOne device (enforced by Endpoint)

This topic describes automation settings for isolating SentinelOne devices with high-severity infections and details supported products, parameters, trigger conditions, and flow.

The automation isolates SentinelOne devices with high severity infection such as malware or virus, detected by SentinelOne, to prevent the threat from spreading inside the organization. Automation parameters can be set such as the isolation duration, whether the isolation is automatic or upon administrators approval, and so on.

Supported Product

SentinelOne

Parameters

Device isolation duration (if admin's approval is required)	Set the expiration period for the automation. This applies only if you have selected the **Admin's approval is required for device isolation** checkbox. After the expiration, Playblocks sends the notification for the Administrator's approval.
Device isolation duration (automatic prevention)	Set the expiration period for the automations that are executed automatically (without the administrator's approval). The default duration is **1 day**.
Admin's approval is required for device isolation	Select the checkbox if you want administrator's approval to execute the automation. It is recommended that you leave the **Admin's approval is required for device isolation** checkbox unselected.

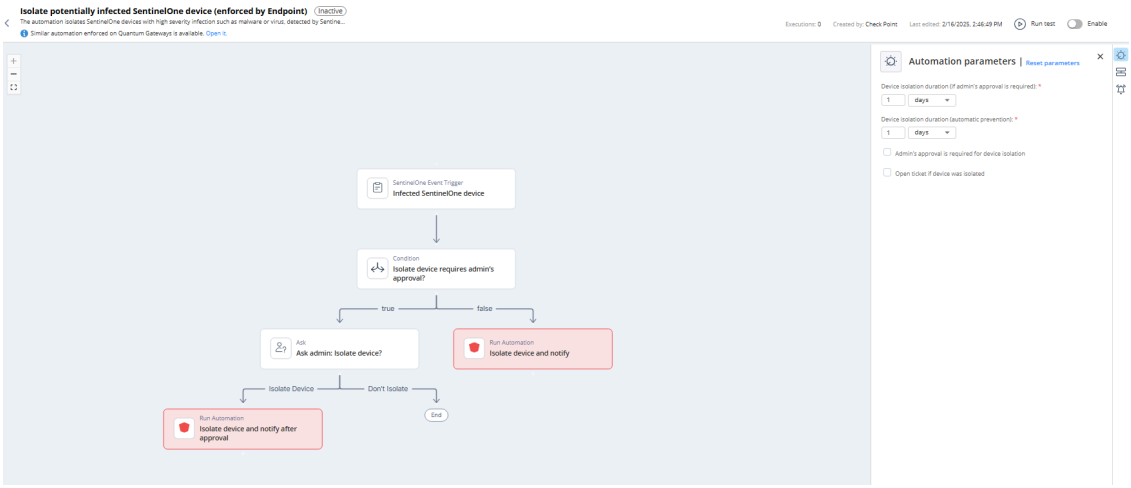
Open ticket if device was isolated	Select the checkbox if you want to open a ticket when device was isolated.

Trigger

Infected SentinelOne device.

To view the example of this log, click Run.

Flow



6.2.26. Isolate potentially infected CrowdStrike device (enforced by Endpoint)

This topic describes how the automation isolates CrowdStrike devices with high severity infections and lists its parameters, triggers, and operational flow.

Supported Product

CrowdStrike for Endpoint

Parameters

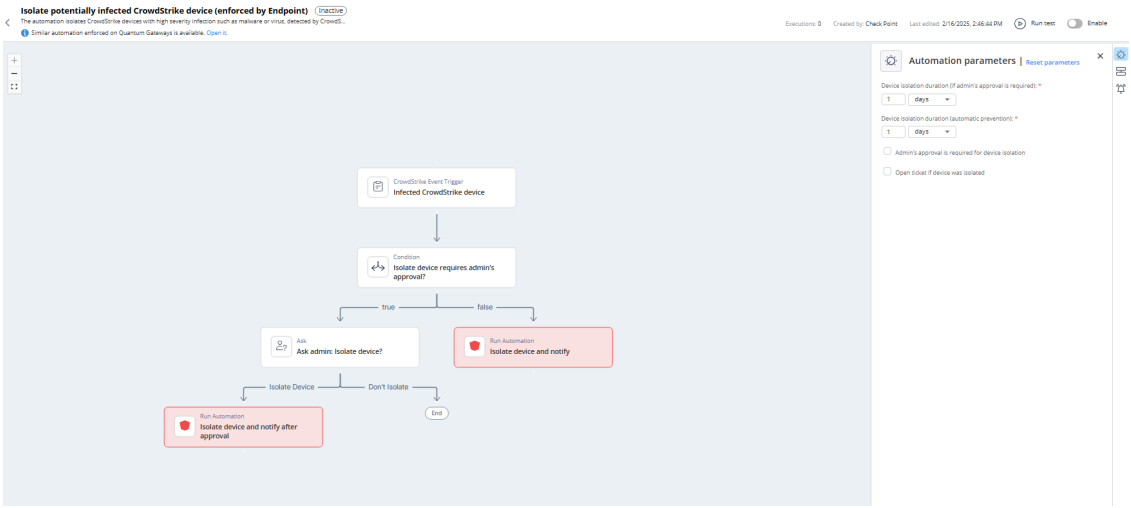
Device isolation duration (if admin's approval is required)	Set the expiration period for the automation. This applies only if you have selected the **Admin's approval is required for device isolation** checkbox. After the expiration, Playblocks sends the notification for the Administrator's approval.
Device isolation duration (automatic prevention)	Set the expiration period for the automations that are executed automatically (without the administrator's approval). The default duration is **1 day**.
Admin's approval is required for device isolation	Select the checkbox if you want Administrator's approval to execute the automation. Check Point recommends that you leave **Admin's approval is required for device isolation** checkbox unselected.
Open ticket if device was isolated	Select the checkbox if you want to open a ticket when device IP was quarantined.

Trigger

Infected CrowdStrike device.

To view the example of this log, click Run.

Flow



6.2.27. Quarantine potentially infected SentinelOne device (enforced by Firewall)

This topic describes quarantining SentinelOne devices with high-severity infections and lists supported products, parameters, triggers, and flow. It explains how automation settings control quarantine behavior.

The automation blocks outgoing traffic from devices with high severity infection such as malware or virus, detected by SentinelOne, to prevent the threat from spreading inside the organization. Automation parameters can be set such as the quarantine duration, whether the quarantine is automatic or upon admins' approval, and so on.

Supported Product

- Check Point Security Management Server
- SentinelOne

Parameters

IP quarantine duration (if admin's approval is required)	Set the expiration period for the automation. This applies only if you have selected the **Admin's approval is required for quarantining device IP** checkbox. After the expiration, Playblocks sends the notification for the Administrator's approval.
IP quarantine duration (automatic prevention)	Set the expiration period for the automations that are executed automatically (without the administrator's approval). The default duration is **1 day**.

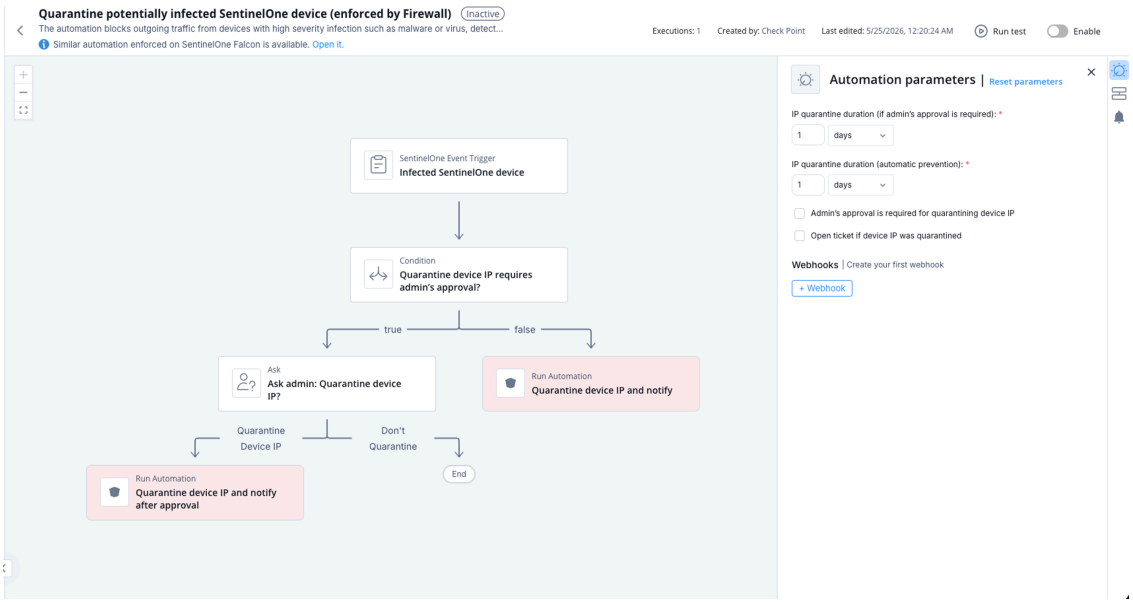
Admin's approval is required for quarantining device IP	Select the checkbox if you want administrator's approval to execute the automation. It is recommended that you leave the **Admin's approval is required for device IP** checkbox unselected.
Open ticket if device was isolated	Select the checkbox if you want to open a ticket when device was isolated.

Trigger

Infected SentinelOne devices.

To view the example of this log, click ../running-automation/running-the-automation.dita.

Flow



6.2.28. AI Agent - Management health report

This topic describes the AI-based automation that analyzes CPM Doctor reports and outlines supported products, parameters, triggers, and flow. It provides details for configuring ticketing options and scheduling.

The automation fetches the CPM Doctor report file using the run-script API from the management server, analyzes and enriches it with an AI agent, and sends a summary report.

Note:

- The automation is currently supported only on EU and US regions.
- The automation is not supported on Multi-Domain and Smart-1 Cloud.

Supported Product

Check Point Security Management Server

Parameters

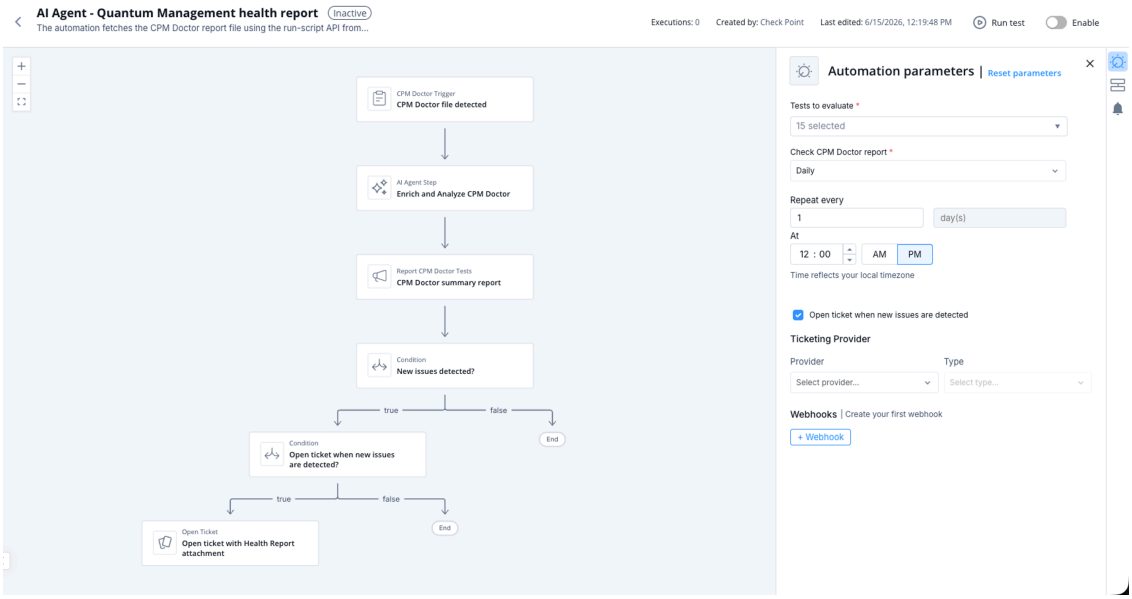
Tests to evaluate	Select the tests you want the AI agent to enrich. By default, all available tests are selected.
Check CPM doctor report	Set the schedule for when the automation should run. By default, it runs daily at 11:00 AM.
Ticketing Provider	Set the ticketing provider.
Open ticket when new issues are detected	Enable this option to automatically open tickets when new test failures are detected. Uncheck this box if you prefer to skip automatic ticket creation.

Trigger

Runs automatically based on the schedule defined in the **Check CPM Doctor Report** parameter.

To view the example of this log, click ../running-automation/running-the-automation.dita.

Flow



6.2.29. Isolate potentially infected Microsoft Defender device (enforced by Endpoint)

This topic describes the automation that isolates potentially infected Microsoft Defender devices and outlines supported products, parameters, trigger conditions, and flow information.

Supported Product

Microsoft Defender

Parameters

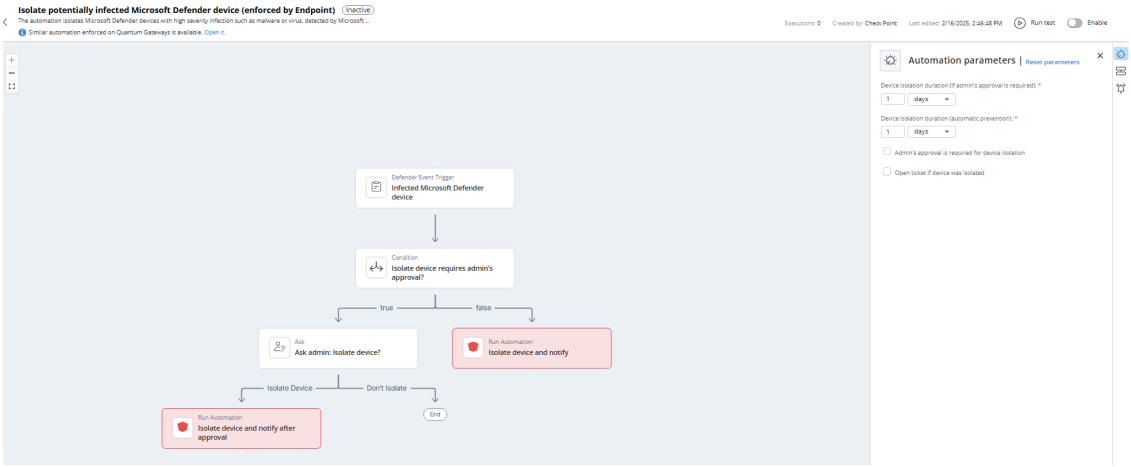
Device isolation duration (if admin's approval is required)	Set the expiration period for the automation. This applies only if you have selected the **Admin's approval is required for device isolation** checkbox. After the expiration, Playblocks sends the notification for the Administrator's approval.
Device isolation duration (automatic prevention)	Set the expiration period for the automations that are executed automatically (without the administrator's approval). The default duration is **1 day**.
Admin's approval is required for device isolation	Select the checkbox if you want administrator's approval to execute the automation. It is recommended that you leave the **Admin's approval is required for device isolation** checkbox unselected.
Open ticket if device was isolated	Select the checkbox if you want to open a ticket when device was isolated.

Trigger

Infected Microsoft Defender device.

To view the example of this log, click Run.

Flow



6.2.30. Quarantine potentially infected Microsoft Defender device (enforced by Firewall)

This topic describes how to quarantine potentially infected Microsoft Defender devices when enforcement is applied by the firewall. It includes supported products, parameters, trigger details, and automation flow.

The automation blocks outgoing traffic from devices with high severity infection such as malware or virus, detected by Microsoft Defender, to prevent the threat from spreading inside the organization. Automation parameters can be set such as the quarantine duration, whether the quarantine is automatic or upon administrators approval, and so on.

Supported Product

- Check Point Security Management Server
- Microsoft Defender

Parameters

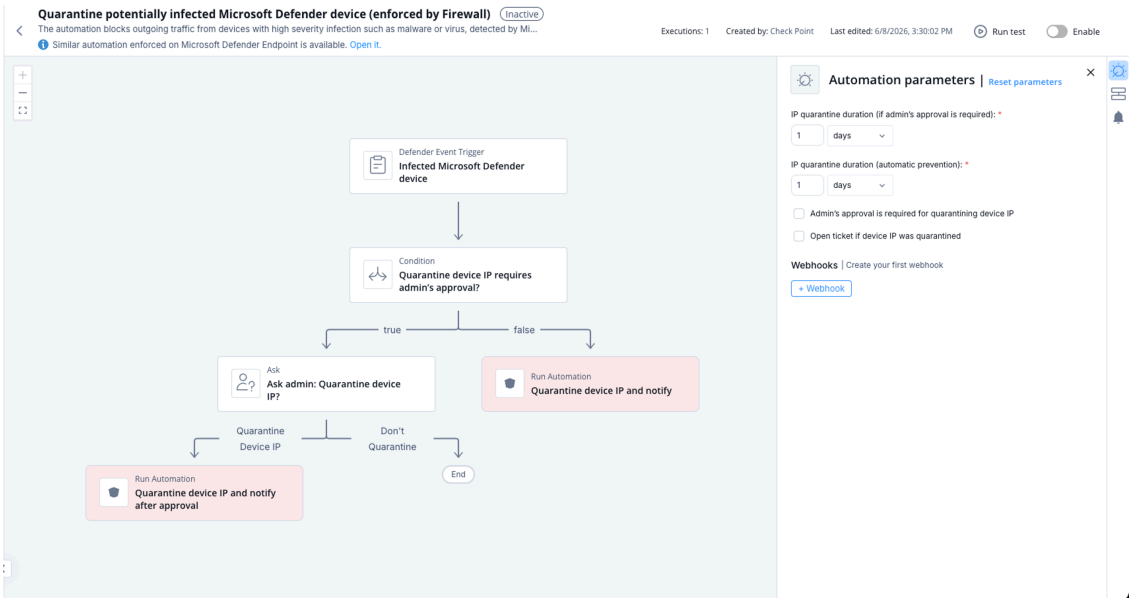
IP quarantine duration (if admin's approval is required)	Set the expiration period for the automation. This applies only if you have selected the **Admin's approval is required for quarantining device IP** checkbox. After the expiration, Playblocks sends the notification for the Administrator's approval.
IP quarantine duration (automatic prevention)	Set the expiration period for the automations that are executed automatically (without the administrator's approval). The default duration is **1 day**.
Admin's approval is required for quarantining device IP	Select the checkbox if you want administrator's approval to execute the automation. It is recommended that you leave the **Admin's approval is required for device IP** checkbox unselected.
Open ticket if device was isolated	Select the checkbox if you want to open a ticket when device was isolated.

Trigger

Triggering quarantine for devices identified as infected by Microsoft Defender.

To view the example of this log, click ../running-automation/running-the-automation.dita.

Flow



6.2.31. Credentials leakage detected by External Risk Management triggering reset password

This topic describes the automation that resets passwords when credentials leakage is detected by External Risk Management. It also lists supported products, parameters, trigger conditions, and the flow diagram.

The automation triggers passwords reset when credentials leakage is detected by External Risk Management, and closes the alert in External Risk Management.

Supported Product

- External Risk Management
- Microsoft Entra ID
- Okta

Parameters

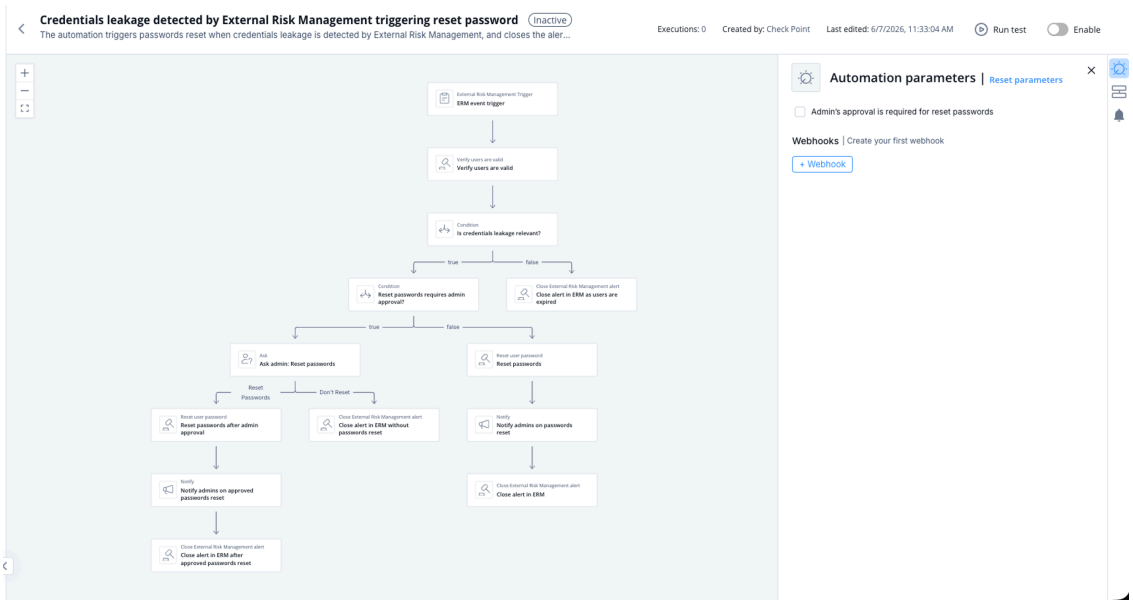
Admin's approval is required for reset passwords	Select the checkbox if you want administrator's approval to reset passwords.

Trigger

Credentials leakage is detected by External Risk Management.

To view the example of this log, click ../running-automation/running-the-automation.dita.

Flow



6.2.32. Check Point Firewall Cloud Log Ingestion Health Monitor

Describes the health monitor that evaluates cloud log ingestion status for Check Point Firewall Management Servers and notifies administrators about failures or successful ingestion events. Includes supported products, parameters, triggers, and the process flow.

Monitors cloud log ingestion for Check Point Firewall Management Servers configured with log sharing. The automation runs on a schedule and evaluates each Management Server individually. If no logs are received within the configured time frame, the automation notifies administrators and recommends reviewing the Log Sharing status. Optionally, the automation can also notify administrators when log ingestion is successful.

Supported Product

Check Point Security Management Server

Parameters

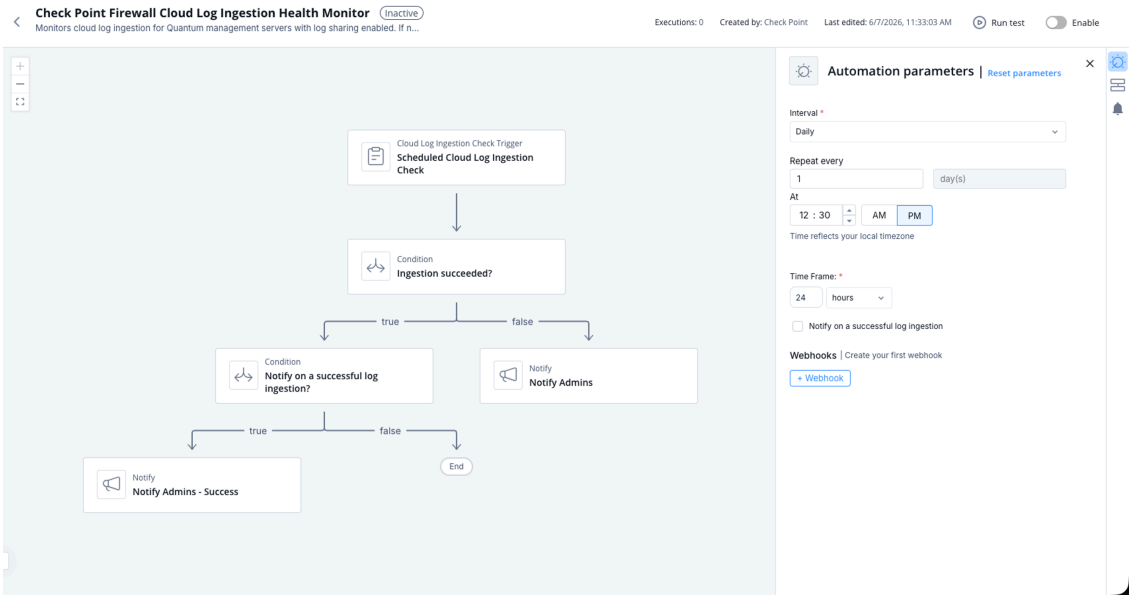
Interval	Defines how often the health monitor runs.
Time frame	Defines the period during which cloud log ingestion is evaluated. If no logs are detected during this period, the automation is triggered.
Notify on a successful log ingestion	When enabled, sends a notification when cloud logs are successfully received from the management server within the configured time frame.

Trigger

The automation runs on a user-defined schedule. On each run, it checks every Check Point Firewall Management Server with log sharing enabled.

- If no logs are received from a server within the configured time frame, a failure notification is sent.
- If logs are received and **Notify on a successful log ingestion** is enabled, a success notification is sent.

Flow



6.2.33. Repeated Remote Access login failures using password-only

This topic describes automation behavior for repeated Remote Access login failures using password-only authentication and the configurable parameters that control it.

The automation notifies on repeated Remote Access login failures using password-only authentication and blocks the source IP across all Quantum Gateways. The notification provides details about the users, the number of failures and more. Automation parameters can be set such as the threshold for login failures, the block duration, whether the block is automatic or upon administrators approval, and so on.

Supported Product

Check Point Security Management Server (Quantum)

Parameters

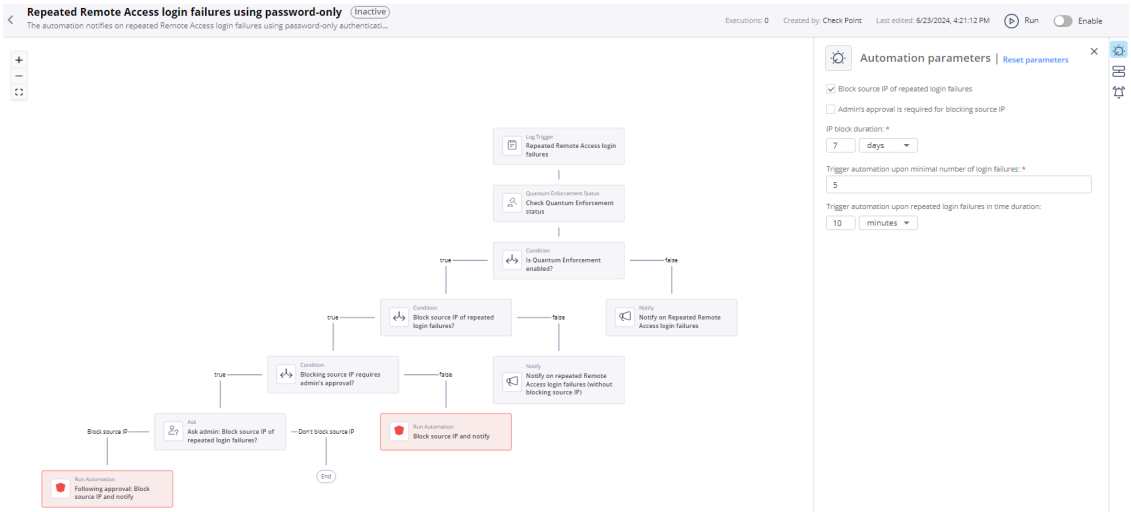
Block source IP of repeated login failures	Select the checkbox to block the source IP of repeated login failures.
Admin's approval is required for blocking source IP	Select the checkbox if admin's approval is required for blocking source IP
IP block duration	Set the IP block duration.
Trigger automation upon minimal number of login failures	Set the minimal number of login failures to trigger the automation.
Trigger automation upon repeated login failures in time duration	Set the time duration to count the login failures.

Trigger

When there are repeated Remote Access login failures using password only.

To view the example of this log, click Run.

Flow



6.2.34. Repeated Remote Access login to expired accounts

This topic describes notifications and blocking behavior for repeated Remote Access login attempts to expired accounts. It also lists supported products, parameters, trigger conditions, and the automation flow.

The automation notifies on login to expired accounts and blocks the source IP across all Quantum Gateways. The notification provides details about the users who failed to log in, the total number of failures within a specified time duration, and the source IP address. Parameters can be configured using the automation parameters such as the threshold for login failures, the block duration, whether the block is automatic or upon administrators approval, and so on.

Supported Product

Check Point Security Management Server (Quantum)

Parameters

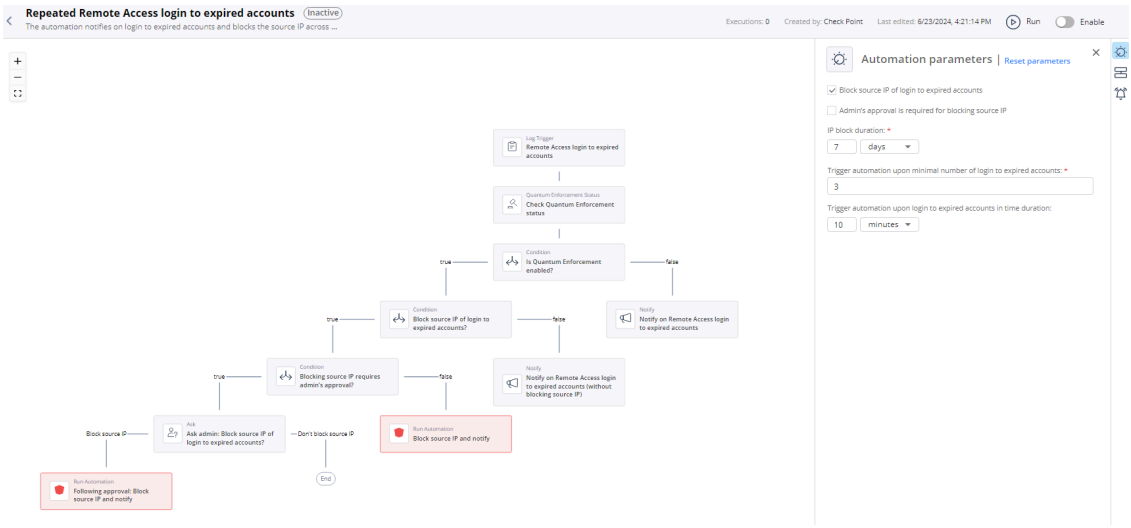
Block source IP of login to expired accounts	Select the checkbox to block the source IP of repeated login failures.
Admin's approval is required for blocking source IP	Select the checkbox if admin's approval is required for blocking source IP.
IP block duration	Set the IP block duration.
Trigger automation upon minimal number of login to expired accounts	Set the minimal number of login to expired accounts to trigger the automation.
Trigger automation upon login to expired accounts in time duration	Set the time duration to count the login to expired accounts.

Trigger

When there are repeated Remote Access login to expired accounts.

To view the example of this log, click Run.

Flow



6.2.35. Remote Access user login using password-only Authentication

This topic describes automation notifications triggered by Remote Access user logins that use password-only authentication. It outlines supported products, parameters, and the event flow.

Supported Product

Check Point Security Management Server (Quantum)

Parameters

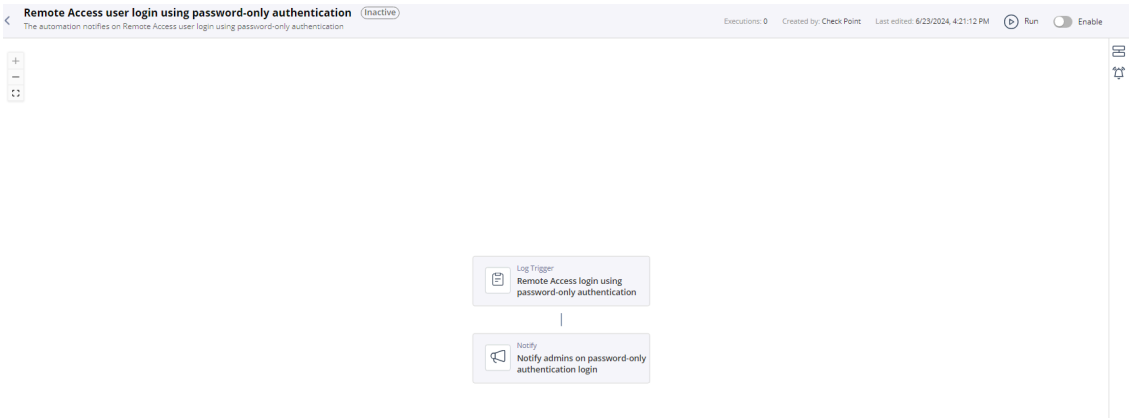
None

Trigger

When there is Remote Access user login with password-only.

To view the example of this log, click Run.

Flow



6.2.36. Block DDoS attack detected by DDoS Protector

This topic describes the automated blocking of attackers detected by DDoS Protector and outlines supported products, parameters, trigger conditions, and flow information. It includes details about configuration options and automation behavior.

Supported Product

- Check Point Security Management Server (Quantum)
- Check Point Quantum DDoS Protector

The automation blocks attackers across the organization and is triggered by attacks that are detected by DDoS Protector. The notification includes information on the attack and the attacker. More parameters can be set using the automation parameters such as the block duration, whether the block is automatic or upon administrator' approval, and so on.

Parameters

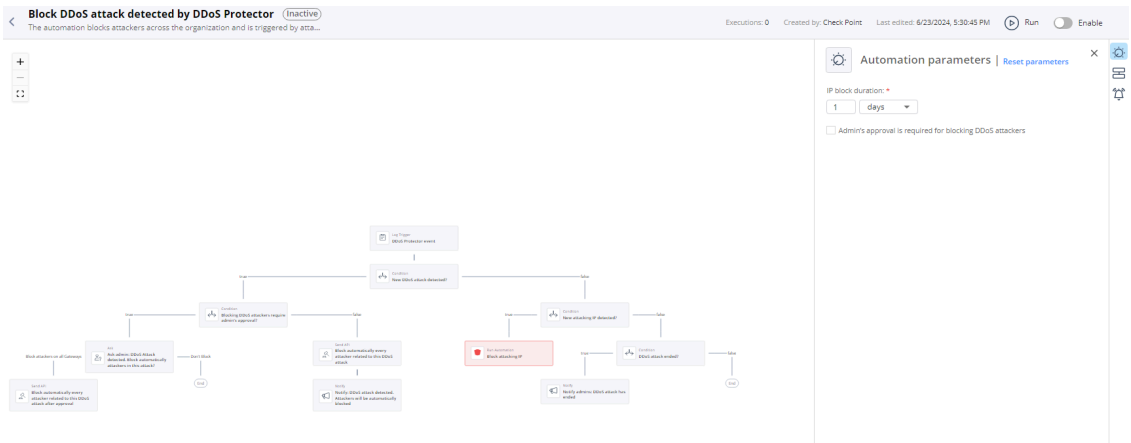
IP block duration	Select the expiration period for the blocked IPs. The default duration is 1 day.
Admin's approval is required for blocking DDoS attackers	Select the checkbox if you want administrator's approval to execute the automation. **Tip:** Check Point recommends that you leave **Admin's approval is required for blocking DDoS attackers** checkbox unselected.

Trigger

Attack identified by Quantum DDoS Protector.

To view the example of this log, click Run.

Flow



6.2.37. Quarantine potentially infected CrowdStrike device (enforced by Firewall)

This topic describes automation behavior that quarantines devices identified by CrowdStrike as potentially infected. It also details supported products, parameters, trigger conditions, and the process flow.

The automation blocks outgoing traffic from devices with potential threats, such as malware or viruses detected by CrowdStrike, to prevent lateral movement and communication with Command and Control (C&C).

Supported Product

- Check Point Security Management Server
- CrowdStrike for Endpoint

Parameters

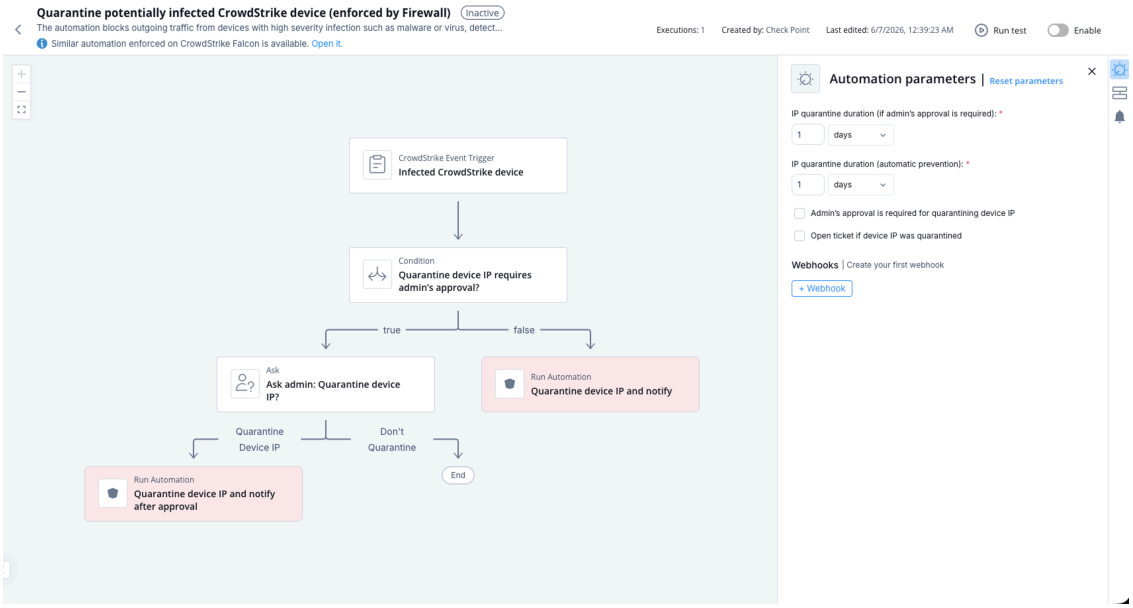
IP quarantine duration (if admin's approval is required)	Set the expiration period for the automation. **Note:** This applies only if you have selected the **Admin's approval is required for quarantining device IP** checkbox. After the expiration, Playblocks sends the notification for the Administrator's approval.
IP quarantine duration (automatic prevention)	Set the expiration period for the automations that are executed automatically (without the administrator's approval). The default duration is **1 day**.
Admin's approval is required for quarantining device IP	Select the checkbox if you want administrator's approval to execute the automation. **Tip:** Check Point recommends that you leave **Admin's approval is required for quarantining device IP** checkbox unselected.

Trigger

Triggering quarantine for devices identified as infected by CrowdStrike.

To view the example of this log, click ../running-automation/running-the-automation.dita.

Flow



6.2.38. De-isolate potentially clean Microsoft Defender machine

This topic describes the automation that removes isolation from a potentially clean Microsoft Defender machine upon administrator approval. It outlines supported products, parameters, trigger conditions, and flow details.

Supported Product

Microsoft Defender

Parameters

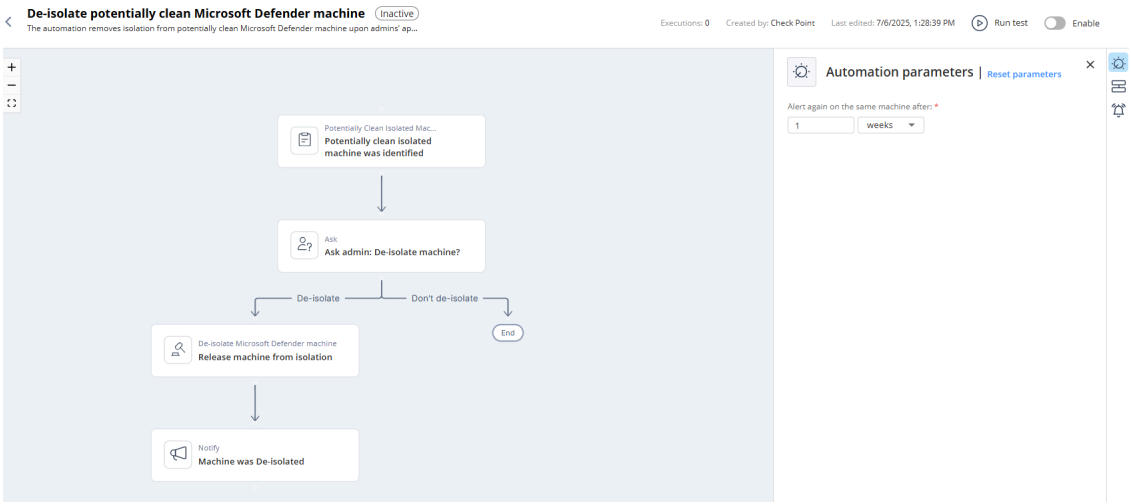
Alert again on the same machine after	Set the frequency to receive alerts again on the same machine.

Trigger

When a potentially **clean** isolated machine is detected.

To view the example of this log, click Run.

Flow



6.2.39. Notify on Failed GAIA Portal Login

This topic describes an automation that notifies when an administrator login to the GAIA Portal fails. It includes supported products, trigger conditions, and a flow diagram.

The automation notifies when an administrator login to the GAIA Portal fails. The notification includes details such as the administrator, the target device.

Supported Product

Check PointSecurity Management Server (Quantum)

Parameters

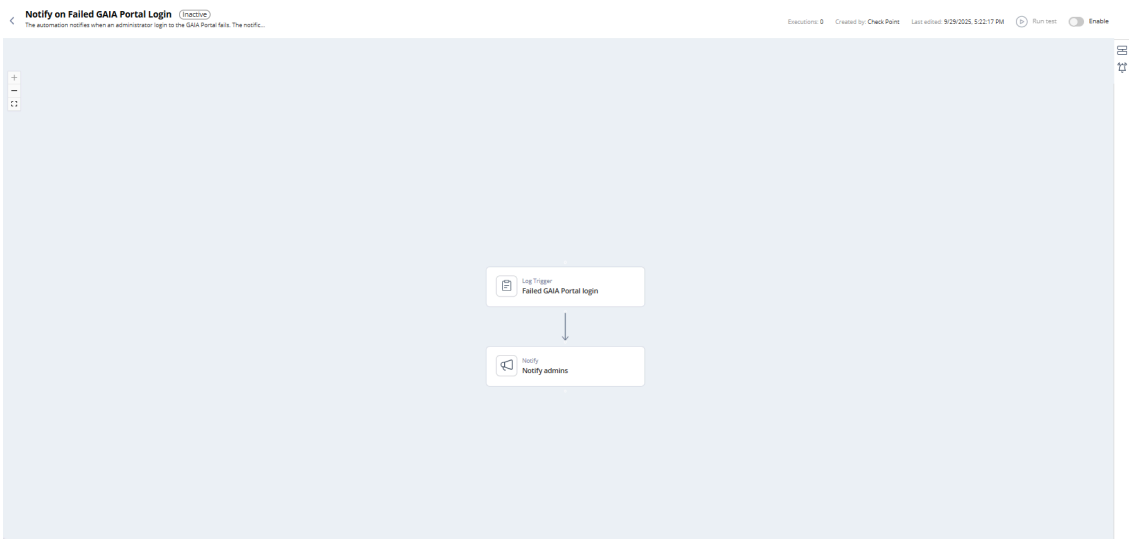
None

Trigger

When a failed administrator login attempt to the GAIA Portal occurs.

To view the example of this log, click Run.

Flow



6.2.40. Notify on Expert Shell Login

This topic describes the notification generated when an Expert Shell login occurs on Gaia or Embedded devices and lists supported product versions, parameters, triggers, and flow.

The automation notifies upon Expert Shell login to the Gaia or Gaia Embedded devices. The notification includes:

- **Machine**
- **Machine Type**
- **Client IP**
- **Administrator**

Supported Product

Check Point Security Management Server (Quantum)

- R81.20 JHF Take 24 and higher
- R81.10 with JHF Take 110 and higher

Parameters

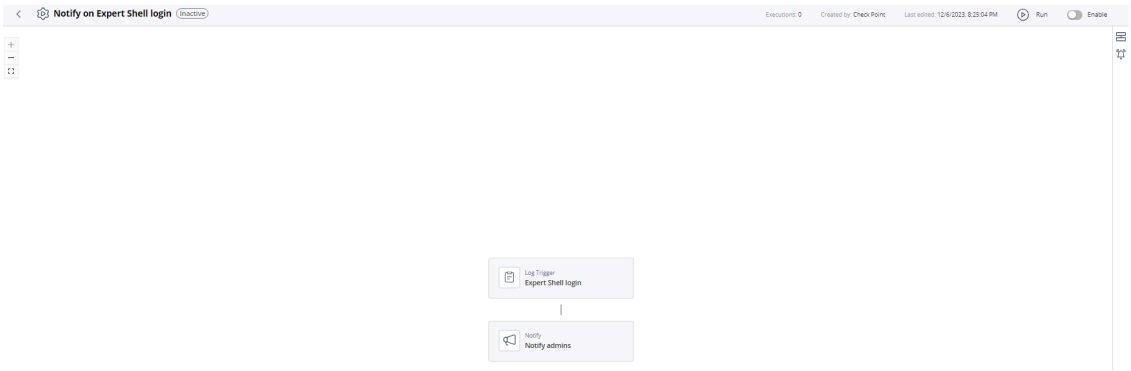
None

Trigger

When an expert Shell login occurs.

To view the example of this log, click Run.

Flow



6.2.41. Notify on Run Script execution

This topic describes the notification generated when scripts are executed on a Gaia device. It outlines the included notification details and related flow information.

The automation notifies upon running scripts on a Gaia device. The notification includes:

- **Device Name**
- **Executed from**
- **Subject**
- **Administrator**

Supported Product

Check Point Security Management Server (Quantum)

Parameters

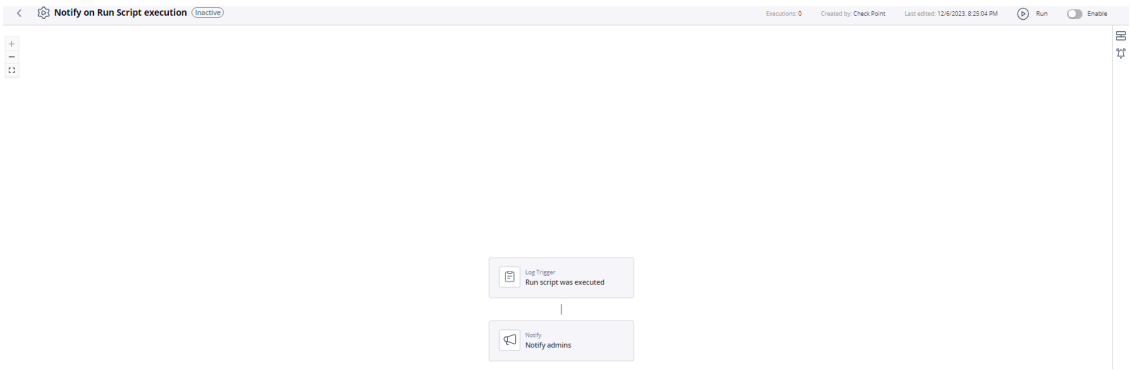
None

Trigger

When a script in run on a Gaia device.

To view the example of this log, click Run.

Flow



6.2.42. Notify on failure of Policy Installation on Check Point Firewall

This topic describes notification behavior when a policy installation on Check Point Firewall fails. It outlines supported products, trigger conditions, and the automation flow.

The automation notifies upon failure of policy installation on Check Point Firewall. The notification includes information on the Gateway, the policy, and the administrator.

Supported Product

Check Point Security Management Server

Parameters

None

Trigger

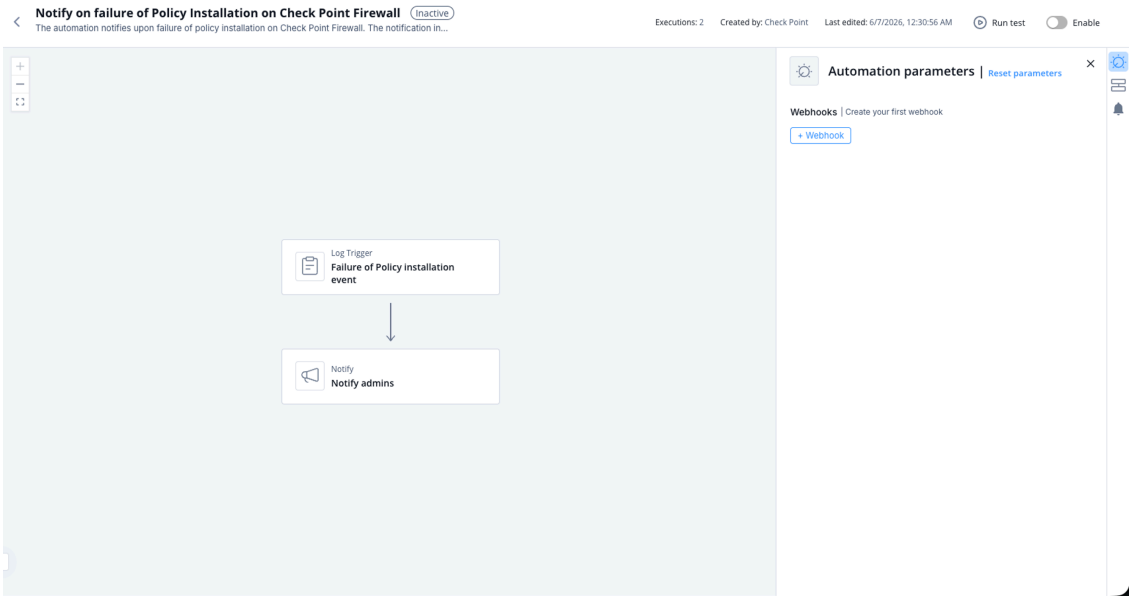
When a policy installation on Check Point Firewall failed.

To view the example of this log, click ../running-automation/running-the-automation.dita.

Note:

The automation is not triggered for QoS and Desktop Policy installation.

Flow



6.2.43. Notify on degradation in Check Point Firewall Compliance status

This topic describes automated notifications triggered by degradation in Check Point Firewall Compliance status and configurable parameters for reporting and ticket creation.

The automation notifies on degradation in Check Point Firewall Compliance status and sends a report that includes information on the changes in Best Practices and Regulations. The user can choose the least severe status change that will be included in the report using the automation parameter. The user can choose to open a ticket with the report link using the automation parameters.

Supported Product

Check Point Security Management Server

Parameters

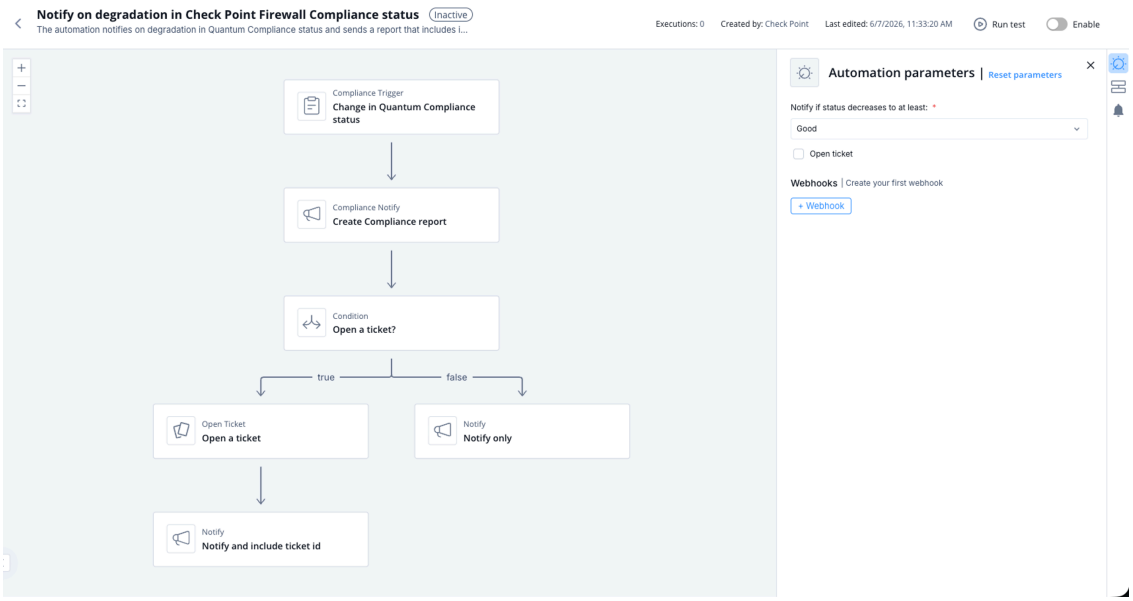
Notify if status decreases to at least	Set the least severe status change that will be included in the report.
Open Ticket	Select the checkbox if you want to open a ticket.
ServiceNow ticket type	Ticket type for ServiceNow connector.
Jira ticket type	Ticket type for Jira connector.

Trigger

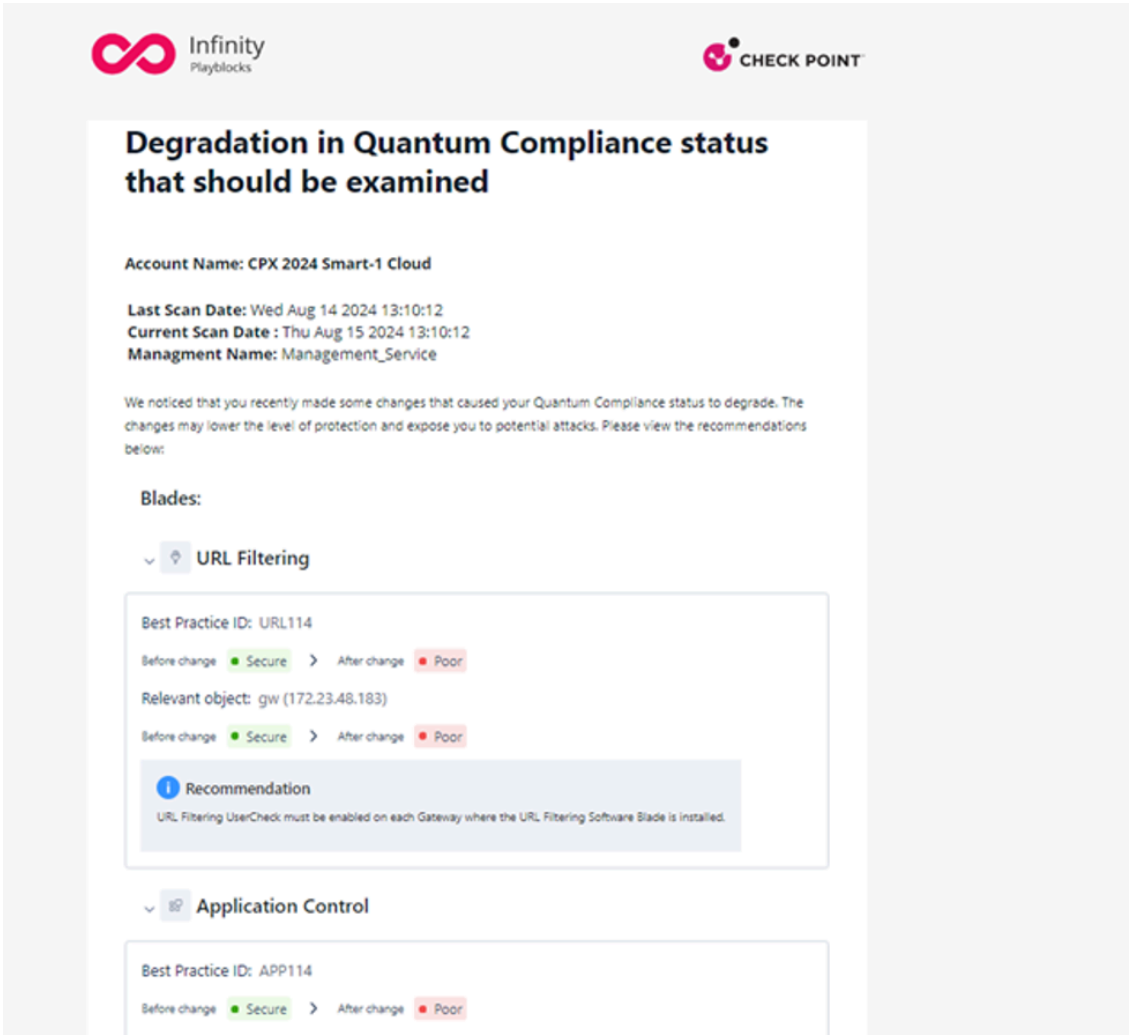
When there is a degradation in Check Point Firewall Compliance status.

To view the example of this log, click ../running-automation/running-the-automation.dita.

Flow



Example report:



6.2.44. Notify on successful Policy Installation on Check Point Firewall

This topic describes automated notifications triggered upon successful policy installation on Check Point Firewall. It outlines supported products, trigger conditions, and flow information.

The automation notifies upon successful policy installation on Check Point Firewall. The notification includes information on the Gateway, the policy, and the administrator.

Supported Product

Check Point Security Management Server

Parameters

None

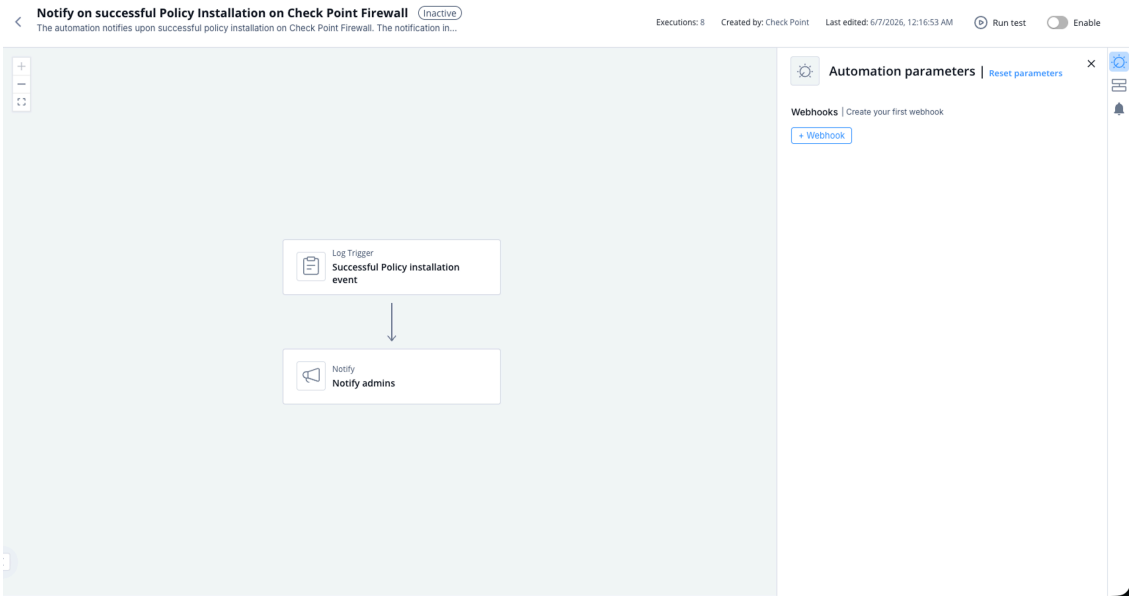
Trigger

When a policy installation on Check Point Firewall succeeded.

To view the example of this log, click ../running-automation/running-the-automation.dita.

> **Note:**
>
> The automation is not triggered for QoS and Desktop Policy installation.

Flow



6.2.45. Notify on changes in administrators

This topic describes an automation that notifies about changes in administrators and their permissions in the management server. It explains supported products, parameters, trigger conditions, and the automation flow.

The automation notifies upon changes in Administrators and their permissions in the Security Management Server. The notification includes the details of the changes, such as who performed the change, what were the changes and so on.

Supported Product

Check Point Security Management Server (Quantum)

Parameters

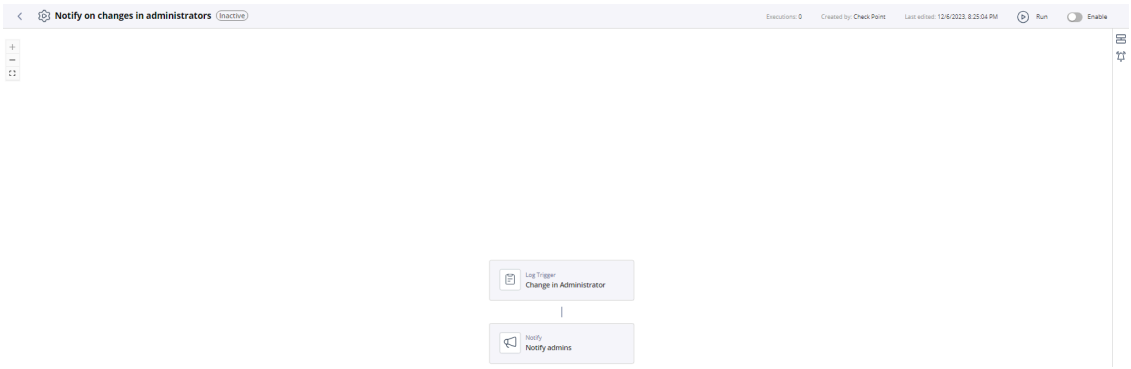
None

Trigger

When changes in administrators occur in the Security Management Server.

To view the example of this log, click Run.

Flow



6.2.46. Alert on MTA email bypass

This topic describes alerts generated when MTA email bypass is detected and the parameter controlling repeated notifications. It also provides product support information, trigger details, and flow visualization.

The automation alerts when MTA email bypass is detected. Automation parameter can be set to configure when to receive additional notification if the issue persists.

Supported Product

Check Point Security Management Server (Quantum)

Parameters

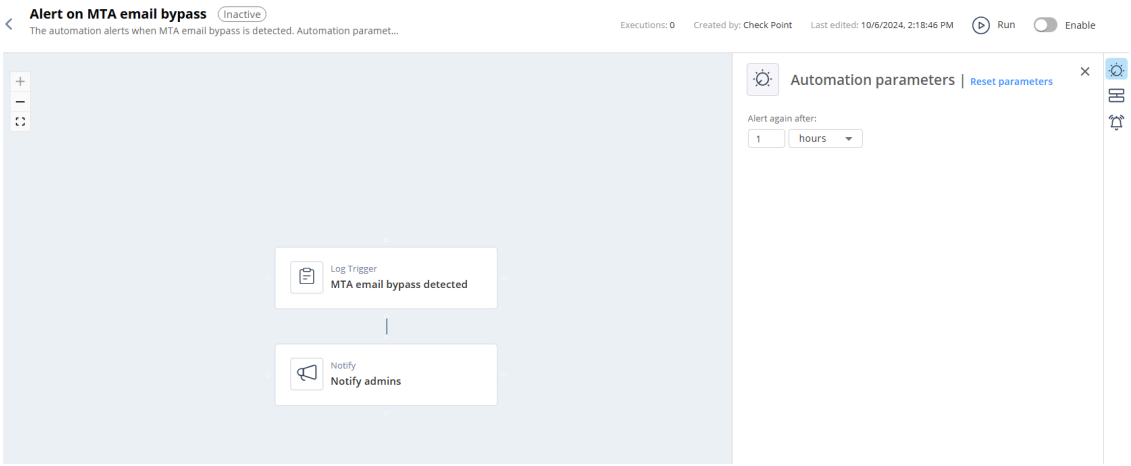
Alert again after	Set the frequency to receive alerts again on this automation.

Trigger

When MTA email bypass detected.

To view the example of this log, click Run.

Flow



6.2.47. Notify on Management validations

This topic describes notifications for validation errors or warnings on Management and outlines parameters, triggers, and flow.

The automation notifies of any validation errors or warnings on your Management.

Supported Product

Check Point Security Management Server

Parameters

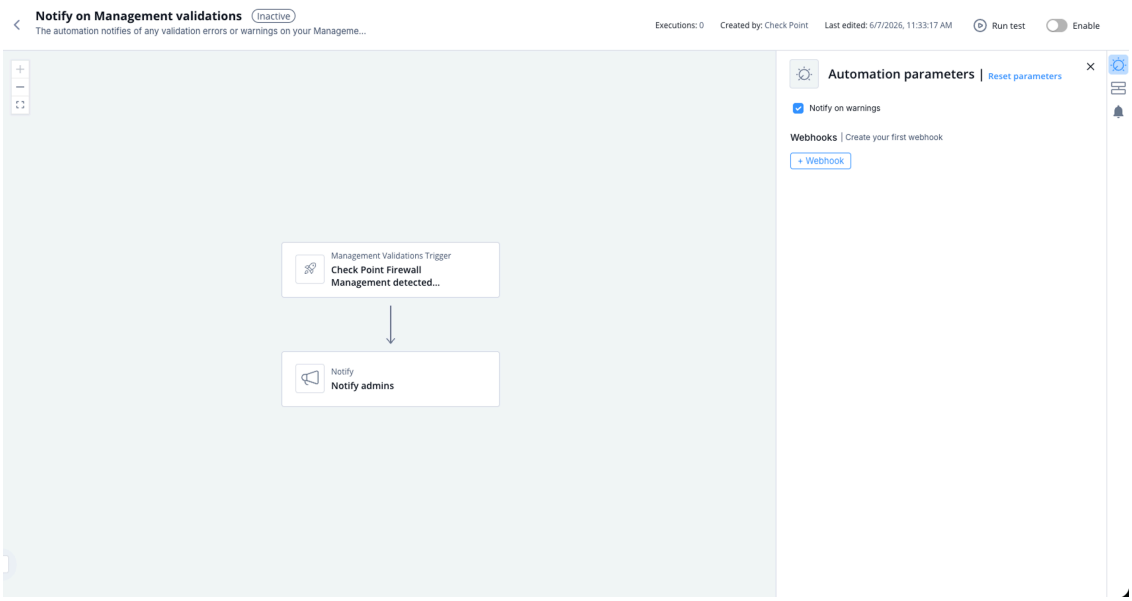
Notify on warnings	The checkbox is selected by default to notify on warnings as well.

Trigger

When errors are detected on your Management.

To view the example of this log, click ../running-automation/running-the-automation.dita.

Flow



6.2.48. Notify on Management High Availability Change-over

This topic describes automated notifications triggered by a change-over event in the management high availability environment. It outlines supported products, parameters, trigger conditions, and the automation flow.

The automation notifies upon change over in the Security Management Server High Availability. The notification includes details on the machine, the result (success or failure) and the administrator who ran it.

Supported Product

Check Point Security Management Server

Parameters

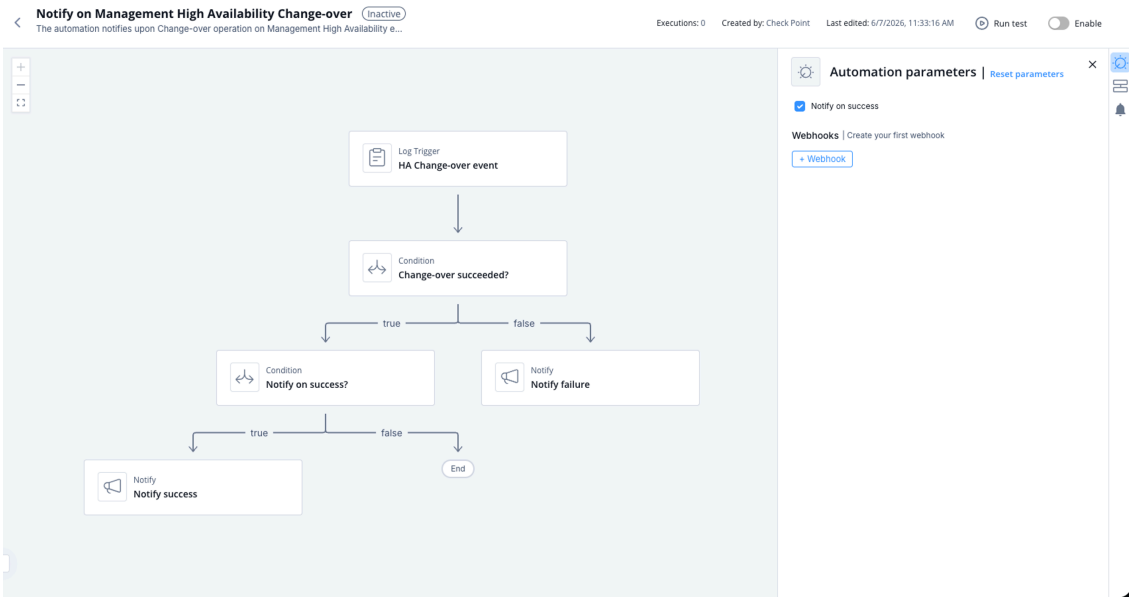
Notify on success	Select the checkbox to notify success of change over in the Security Management Server High Availability.

Trigger

When a changeover operation occurred in the Security Management Server High Availability.

To view the example of this log, click ../running-automation/running-the-automation.dita.

Flow



6.2.49. Notify on repeated login failures to Management

This topic describes the automated notification for repeated login failures to Management and the parameters that control its behavior.

This automation notifies you upon repeated login failures to Management. A parameter to count failures by user can be set using the automation parameters. The notification includes details on the number of failures in the time duration.

Supported Product

Check Point Security Management Server

Parameters

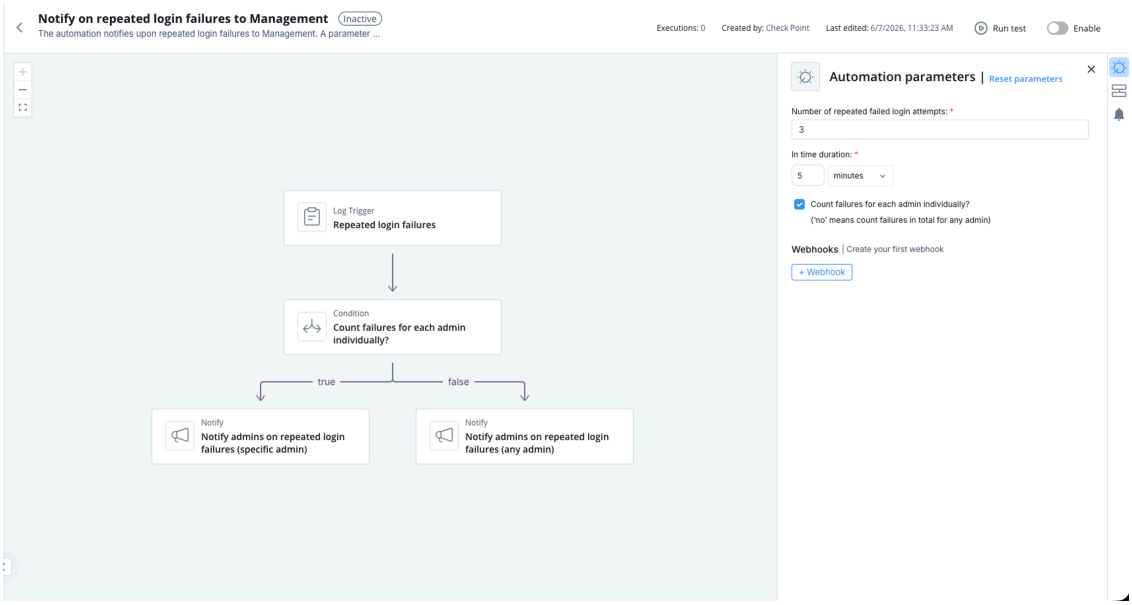
Number of repeated failed login attempts	Set the number of repeated failed login attempts before notify.
In time duration	Set the time duration for the repeated failed login attempts.
Count failures for each admin individually? ('no' means count failures in total for any admin)	Select the checkbox if you want to count failures by each admin individually.

Trigger

When the number of repeated failed login attempts reach to the number defined in the automation parameters.

To view the example of this log, click ../running-automation/running-the-automation.dita.

Flow



6.2.50. Notify on high rate of blocked connections

This topic describes how the automation notifies when a high number of blocked connections occur from the same origin machine. It also lists the parameters and trigger conditions for this notification.

Supported Product

Check Point Security Management Server (Quantum)

Note:

Make sure that you have enabled **Log Sharing** in On-boarding the On-premises Check Point Security Gateway *(on page 21)*.

Parameters

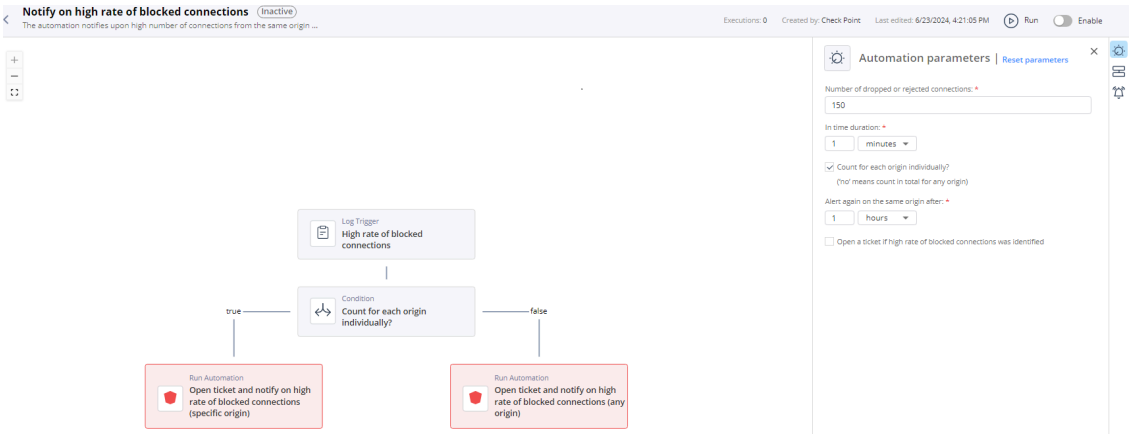
Number of dropped or rejected connections	Set the number of dropped or rejected connections after which the system notifies the Administrator.
In time duration	Set the time duration for the blocked connections.
Count for each origin individually? ('no' means count in total for any origin)	Select the checkbox if you want to count failures by each origin individually.
Open a ticket if high rate of blocked connections was identified	Select the checkbox if you want to open a ticket when high rate of blocked connections was identified.

Trigger

When the number of blocked connections match the specified value in the automation parameters.

To view the example of this log, click Run *(on page 136)*.

Flow



6.2.51. Notify on failure of installation blade updates on Check Point Firewalls

This topic describes notifications generated when blade update installations fail on Check Point Firewalls. It includes supported products, parameters, trigger conditions, and the automation flow.

The automation notifies on failure of installation blades updates on Check Point Firewalls, such as IPS update and Application Control update. The notification includes details of the blade, package version, product and the severity.

Supported Product

Check Point Security Management Server

Parameters

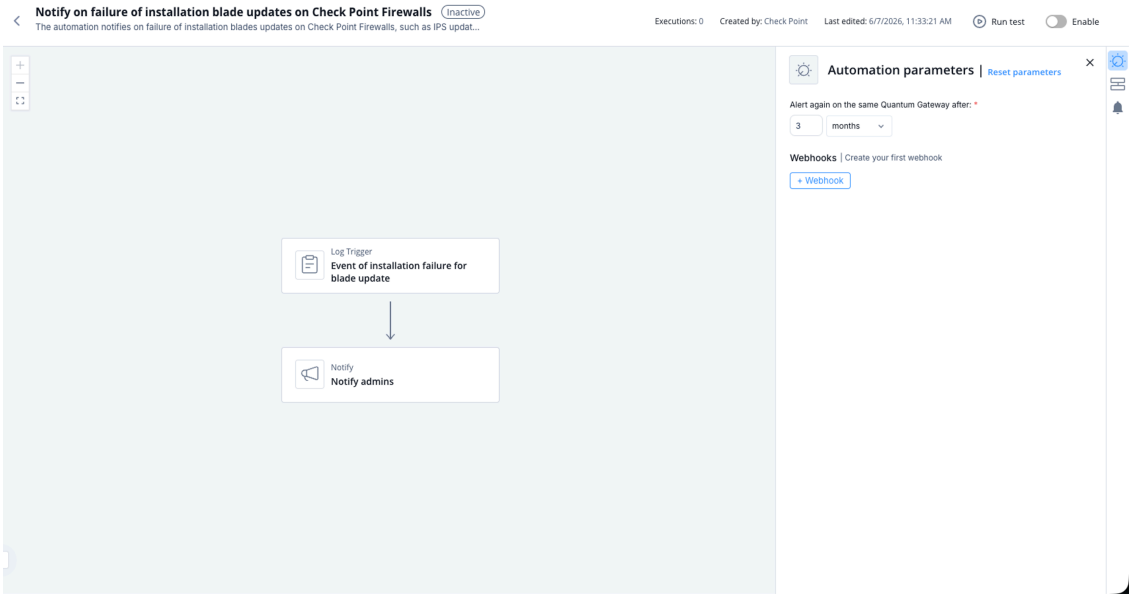
Alert again on the same Check Point Firewall after	Set the frequency to receive alerts again on the same Gateway.

Trigger

When installation of blade updates on Check Point Firewalls failed.

To view the example of this log, click ../running-automation/running-the-automation.dita.

Flow



6.2.52. Notify on successful installation of blade updates on Check Point Firewalls

This topic describes automation that notifies on successful installation of blade updates on Check Point Firewalls and provides details about related parameters and triggers. It also includes product support information and a flow diagram.

The automation notifies on successful installation blades updates on Check Point Firewalls, such as IPS update and Application Control update. The notification includes details of the blade, package version, product and the severity.

Supported Product

Check Point Security Management Server

Parameters

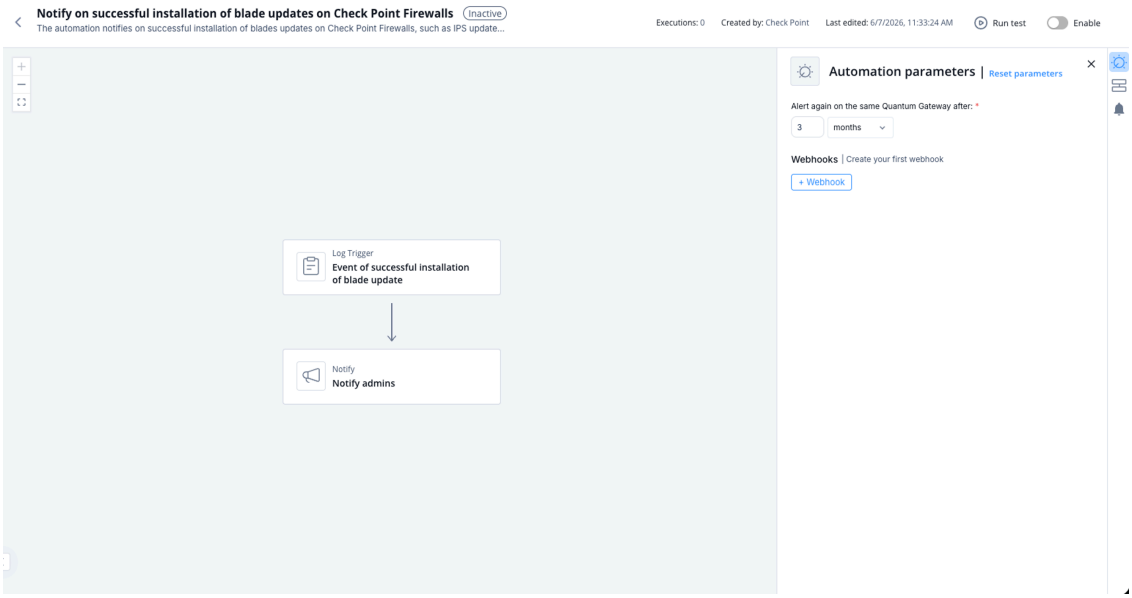
Alert again on the same Check Point Firewall after	Set the frequency to receive alerts again on the same Gateway.

Trigger

When installation of blade updates on Check Point Firewalls succeeded.

To view the example of this log, click ../running-automation/running-the-automation.dita.

Flow



6.2.53. Alert on licenses expiration on Check Point Firewall device

This topic describes automation behavior for notifying and opening tickets when licenses on Check Point Firewall devices are about to expire. It also lists the supported product, parameters, trigger, and flow of the automation.

The automation notifies upon licenses expiration on Check Point Firewall devices. The alert notifies and opens a ticket with the information of the device. Automation parameters can be set to configure the frequency of license expiration, time to alert before license is about to expire, and more.

Supported Product

Check Point Security Management Server

> **Note:**
>
> The automation is temporarily not supported with Multi-Domain Security Management.

Parameters

Attempt to check expiration of licenses on Check Point Firewall devices every	Set the frequency to check the expiration of licenses on Check Point Firewall devices.
Alert if licenses are about to expire	Select the checkbox if you want to receive alerts on licenses that are about to expire.
Alert if licenses are about to expire within	Set the duration. The systems alerts if the licenses are about to expire within the specified duration.
Alert again on the same Check Point Firewall device after	Set the frequency to receive alerts again on the same Check Point Firewall device.

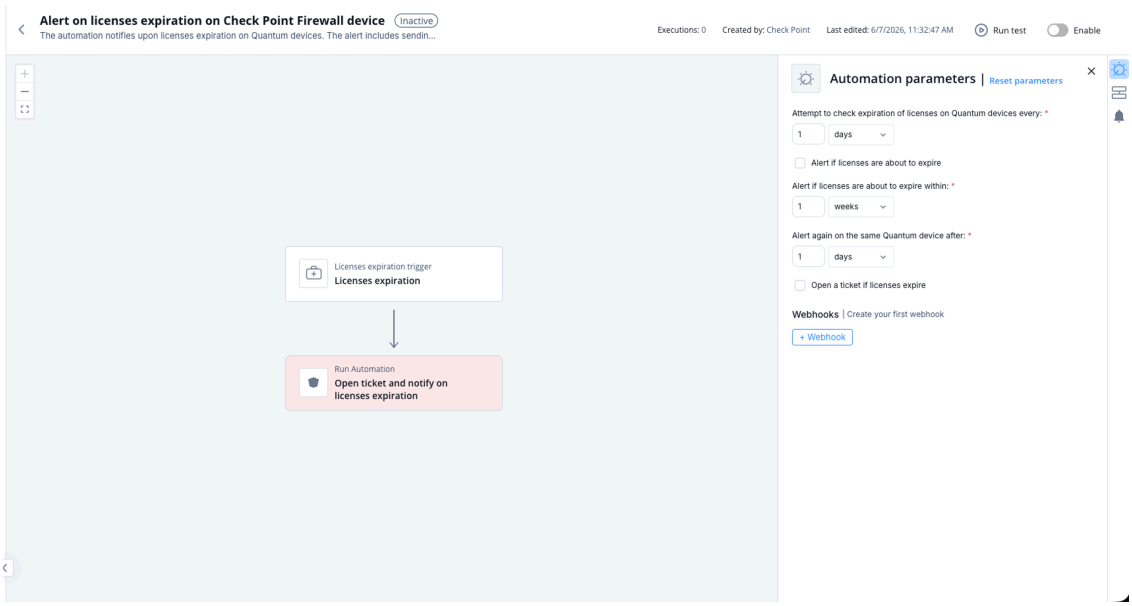
Open a ticket if licenses expire	Select the checkbox if you want to open a ticket when the automation is triggered.

Trigger

When licenses expire or about to expire on your Check Point Firewall devices.

To view the example of this log, click ../running-automation/running-the-automation.dita.

Flow



6.2.54. Alert on VPN certificates expiration on Check Point Firewall

This topic describes how automation alerts when VPN certificates expire on Check Point Firewalls and outlines the configurable parameters for expiration monitoring.

The automation notifies when VPN certificate expire on Check Point Firewalls. The alert notifies and opens a ticket with the information of the gateway. Automation parameters can be set to configure the frequency of VPN certificates expiration, time to alert before VPN certificates are about to be expired, and so on.

Supported Product

Check Point Security Management Server

Parameters

Attempt to check expiration of VPN certificates on Check Point Firewalls every	Set the frequency to check the expiration of VPN certificates on Check Point Firewalls.
Alert if VPN certificates are about to expire	Select the checkbox to receive alert when VPN certificates are about to expire.
Alert if VPN certificates are about to expire within	Set the time to receive alerts when VPN certificates are about to expire.

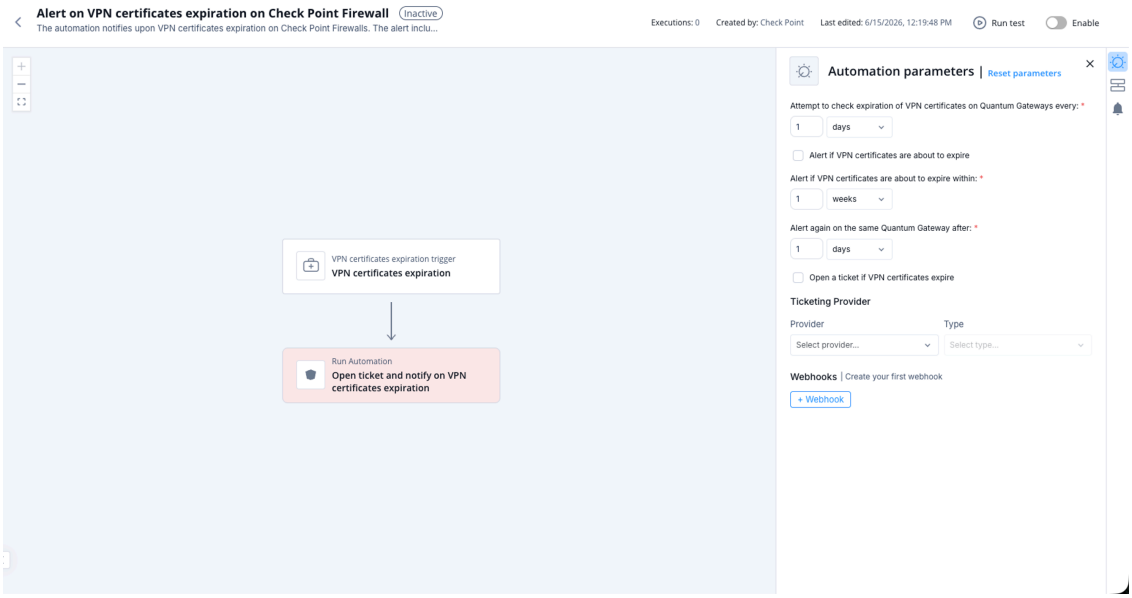
Alert again on the same Check Point Firewall after	Set the frequency to receive alerts again on the same Gateway.
Open a ticket if VPN certificates expired	Select the checkbox to open a ticket when automation is triggered.

Trigger

When VPN certificate expire or about to expire on Check Point Firewalls.

To view the example of this log, click ../running-automation/running-the-automation.dita.

Flow



6.2.55. Alert if VPN Tunnel is down

This topic describes an automation that sends an alert when a permanent VPN tunnel goes down. It explains supported products, configuration parameters, trigger conditions, and flow behavior.

The automation triggers an alert when a permanent VPN tunnel goes down.

The alert includes sending a notification and, optionally, opening a ticket containing information about the affected Gateway.

A parameter in the automation settings allows you to specify whether a ticket should be opened when an alert is triggered.

Supported Product

Check Point Security Management Server (Quantum)

Parameters

Open a ticket if VPN Tunnel is down	Select the checkbox if you want to open a ticket.

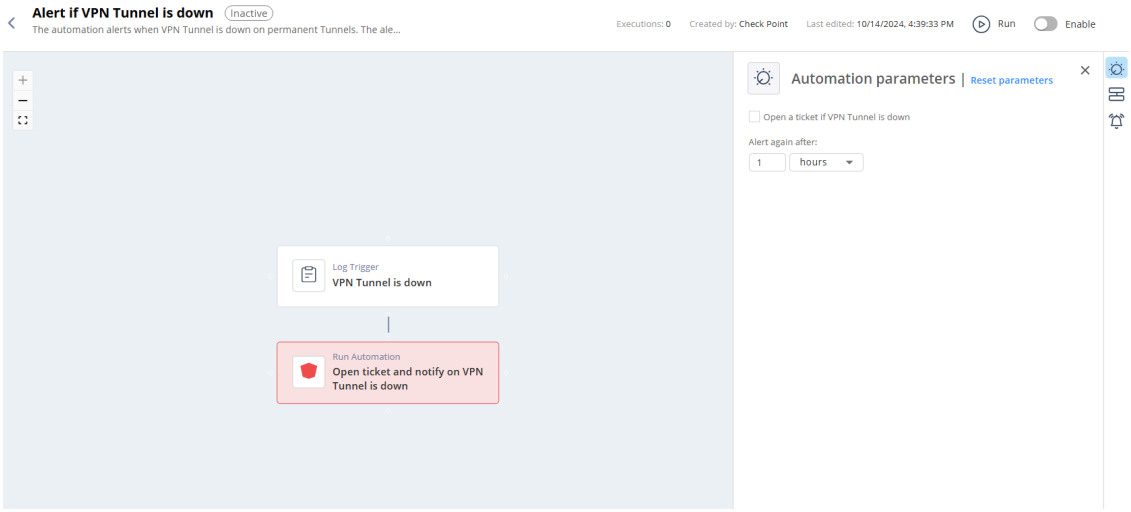
Alert again after	Set the frequency to receive alerts again on the same peer Gateway.

Trigger

When VPN Tunnel changes status to **DOWN**.

To view the example of this log, click Run.

Flow



6.2.56. Alert if no communication with Check Point Firewall

This topic describes the alert generated when Check Point Firewall Management cannot communicate with one or more Check Point Firewalls. It lists supported products, parameters, trigger conditions, and the automation flow.

The automation alerts when the Check Point Firewall Management is unable to communicate with one or more Check Point Firewalls. The alert notifies and opens a ticket with the information on the gateway. Automations parameters can be set to configure the frequency of testing the communication, number of failed attempts before creating the alert, and if a ticket has to be opened.

Supported Product

Check Point Security Management Server

Parameters

Attempt to communicate with Gateways every	Set the frequency to check communication with the Gateway.
Number of failed attempts to communicate with a Gateway before sending alert	Set the number of failed attempts to communicate with a Gateway before sending alert.
Alert again on the same Gateway after	Set the frequency to receive alerts again on the same Gateway.

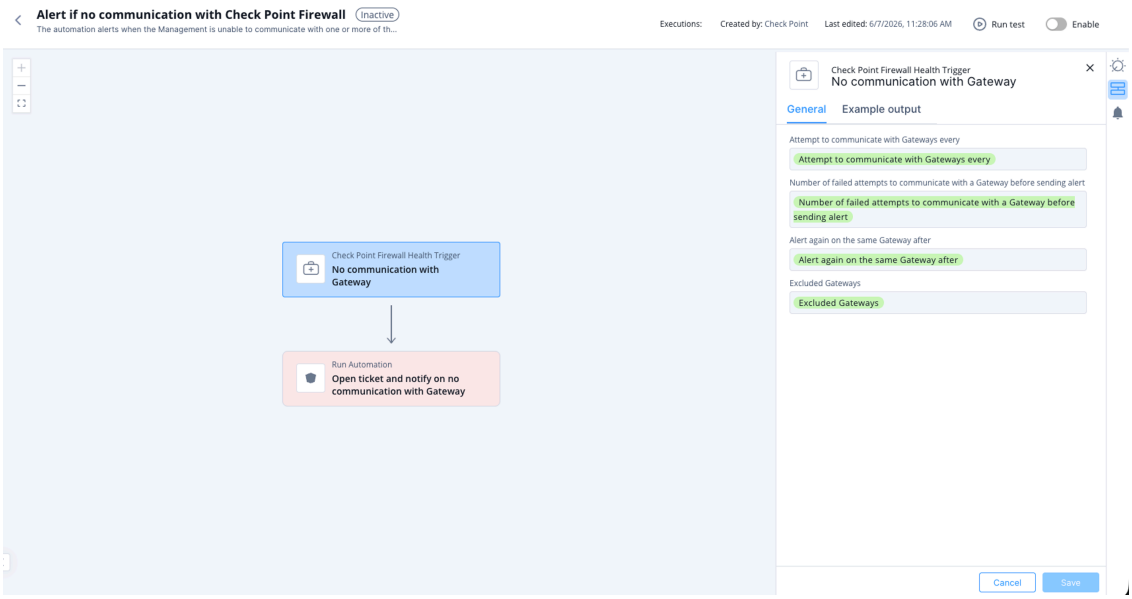
Open a ticket if no communication with Gateway	Select the checkbox if you want to open a ticket when the automation is triggered.
Exclude the following Gateways from testing communication	Select the gateway(s) checkbox(s) to exclude testing communication.

Trigger

When Check Point Firewall Management is unable to communicate with one or more Check Point Firewalls.

To view the example of this log, click ../running-automation/running-the-automation.dita.

Flow



6.2.57. Notify on non-compliant devices blocked by Identity and Trust

This topic describes an automation that sends notifications when non-compliant devices are blocked by the identity and trust system. It outlines supported products, triggers, and the flow.

This automation sends notifications when blocked devices are identified as non-compliant by Identity and Trust.

Supported Products

- Check Point Security Management Server (Quantum)
- Identity and Trust

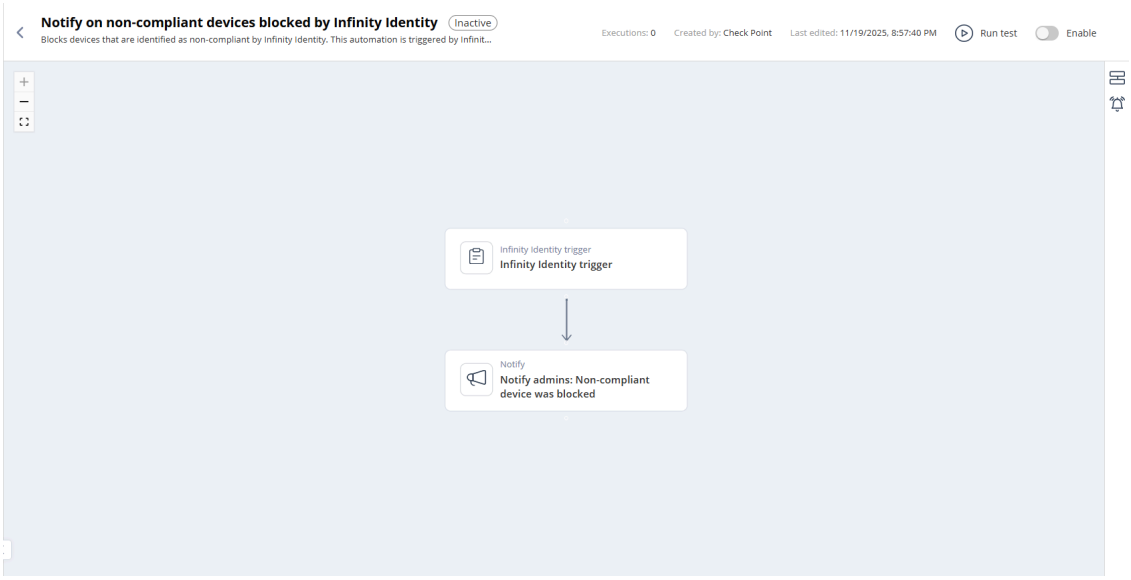
Parameters

None

Trigger

- A non-compliant device was blocked by Identity and Trust.
- To view the example of this log, click Run.

Flow



6.2.58. Block external IP

This topic describes the automation that blocks incoming access from external IP addresses and details supported products, parameters, triggers, and flow information.

Supported Product

Check Point Security Management Server (Quantum)

The automation blocks the incoming access from external IP on the Check Point Security Gateway across the organization.

Parameters

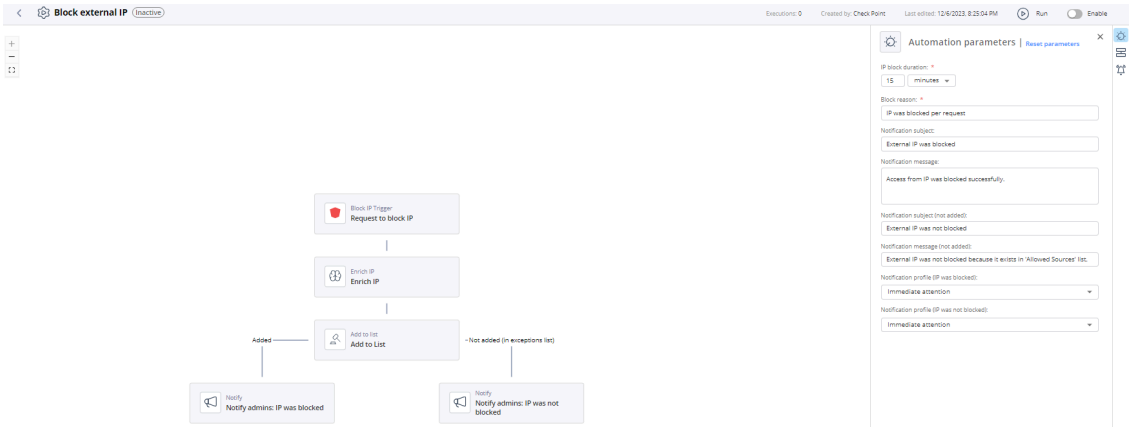
IP block duration	Set the expiration period for the automations that are executed automatically (without Administrator's approval).
Block reason	Enter the reason for blocking IP.
Notification subject	Enter a subject for a notification you receive through a configured communication tool.
Notification message	Enter the text for a notification you receive through a configured communication tool.
Notification subject (not added)	Enter the subject for the notification that is sent to the Administrator if the IP address is not quarantined as it is listed in the Allowed Sources List *(on page 220)*.
Notification message (not added)	Enter the message for the notification that is sent to the Administrator if the IP address is not quarantined as it is listed in the Allowed Sources List *(on page 220)*.
Notification profile (IP was blocked)	Select a notification profile to send notification to Administrator if the IP address is blocked. For more information, see Notifications *(on page 257)*.
Notification profile (IP was not blocked)	Select a notification profile to send notification to Administrator if the IP address is not blocked as it is in the Allowed Sources List *(on page 220)*. For more information, see Notifications *(on page 257)*.

Trigger

Matching block IP.

To view the example of this log, click Run.

Flow



6.2.59. Isolate endpoint device

This topic describes isolating an endpoint device through automated actions. It includes supported products, parameters, trigger details, and a flow diagram.

Supported Product

- Endpoint Security
- Microsoft Defender
- Crowdstrike
- SentinelOne

Parameters

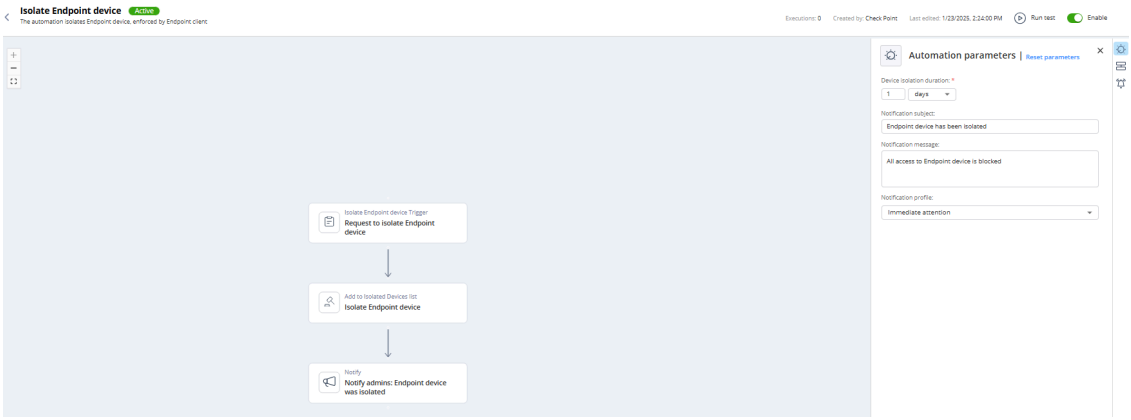
Device isolation duration (if admin's approval is required)	Set the expiration period for the automation. The default duration is **1 day**.
Notification subject	The subject of the notification you receive through a configured communication tool.
Notification message	The text of the notification you receive through a configured communication tool.
Notification profile	The notification profile sent to Administrator.

Trigger

Request to isolate Endpoint device.

To view the example of this log, click Run.

Flow



6.2.60. Quarantine internal IP

This topic describes how internal devices are quarantined by blocking their outgoing access across the organization. It explains the automation behavior applied on the security gateway.

The automation quarantines internal device by blocking outgoing access from it on the Quantum Gateways across the organization.

6.2.60.1. Supported Product

This topic lists the supported product details. It includes product keywords referencing Check Point Quantum family components.

Supported Product

Check Point Security Management Server (Quantum)

6.2.60.2. Parameters

This topic describes parameters related to IP blocking, notifications, and quarantine handling. It outlines configuration options for setting durations, messages, profiles, and automated actions.

IP block duration	Set the expiration period for the automations that are executed automatically (without Administrator's approval).
Block reason	Enter the reason for blocking IP.
Notification subject	Enter a subject for a notification you receive through a configured communication tool.
Notification message	Enter the text for a notification you receive through a configured communication tool.
Notification subject (not added)	Enter the subject for the notification that is sent to the Administrator if the IP address is not quarantined as it is listed in the Allowed Sources List *(on page 220)*.

Notification message (not added)	Enter the message for the notification that is sent to the Administrator if the IP address is not quarantined as it is listed in the Allowed Sources List *(on page 220)*.
Notification profile (Device IP was quarantine)	Select a notification profile to send notification to Administrator if the IP address is quarantined. For more information, see Notifications *(on page 257)*.
Notification profile (Device IP was not quarantine)	Select a notification profile to send notification to Administrator if the IP address is not quarantined as it is in the Allowed Sources List *(on page 220)*. For more information, see Notifications *(on page 257)*.
Open ticket if device IP was quarantined	Select the checkbox if you want to open a ticket when device IP was quarantined.

6.2.60.3. Trigger

Describes the trigger condition involving matching a quarantine IP and how to view an example log entry.

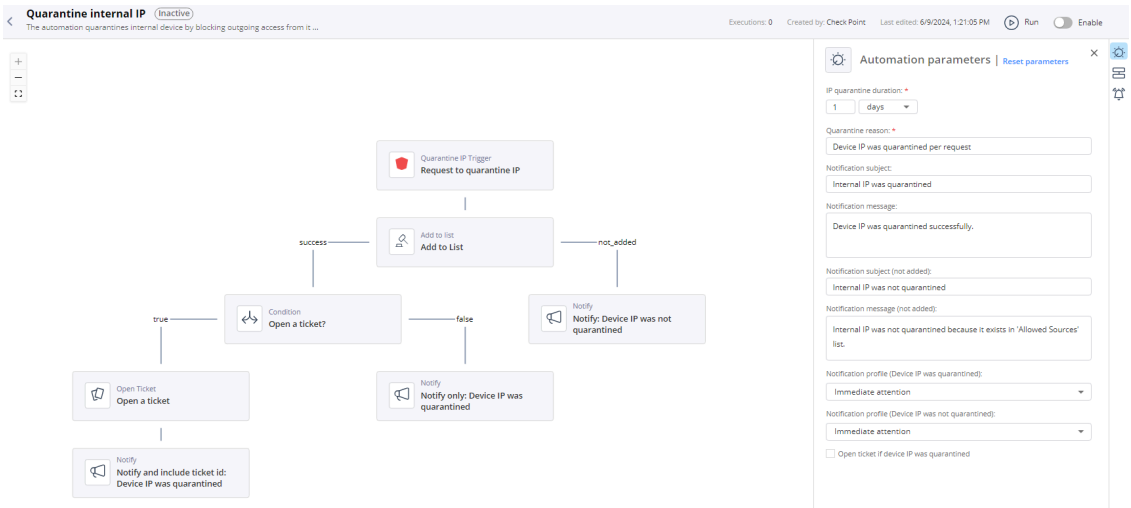
Trigger

Matching quarantine IP.

To view the example of this log, click Run.

6.2.60.4. Flow

This topic provides a visual representation of the flow using the provided diagram. It illustrates the process as depicted in the referenced image.



6.2.61. Enforce Policy on newly discovered IoT Zone

This topic describes the automation that enforces best practice policy on a newly discovered IoT zone. It outlines supported products, trigger conditions, and the automation flow.

Supported Product

IoT Security

Parameters

None

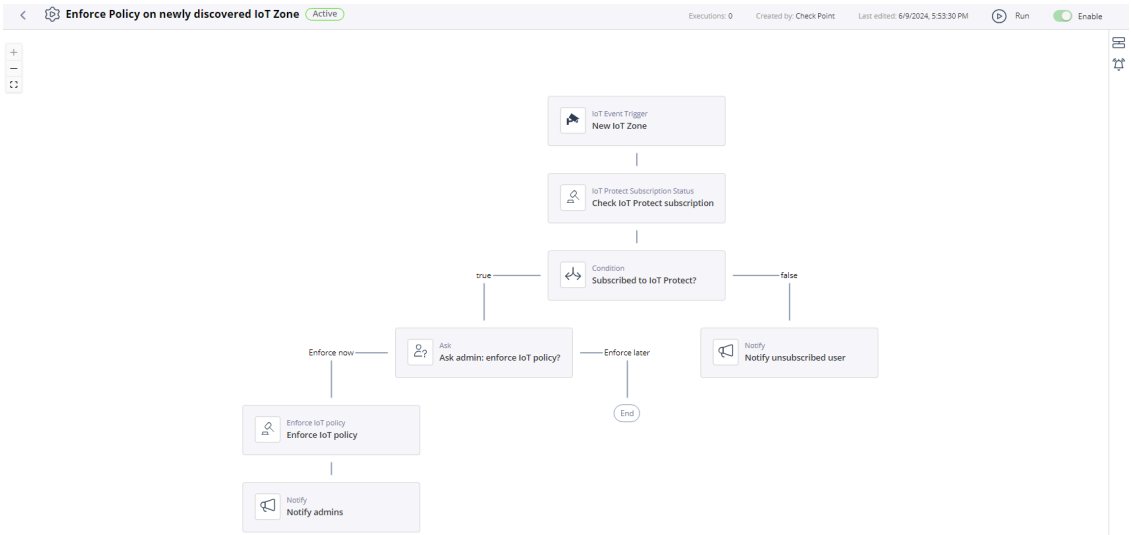
Trigger

Matching policy on newly discovered IoT zone.

This automation is automatically called by IoT Security.

To view the example of this log, click Run.

Flow



6.2.62. Device is at risk IoT

This topic describes notifications generated when an IoT device is at risk and the available administrative actions. It also outlines supported products, parameters, triggers, and flow information.

The automation notifies when an IoT device is at risk. As part of the notification, the admin can decide to change the enforce mode to Prevent and to enforce the policy.

Supported Product

IoT Security

Parameters

None

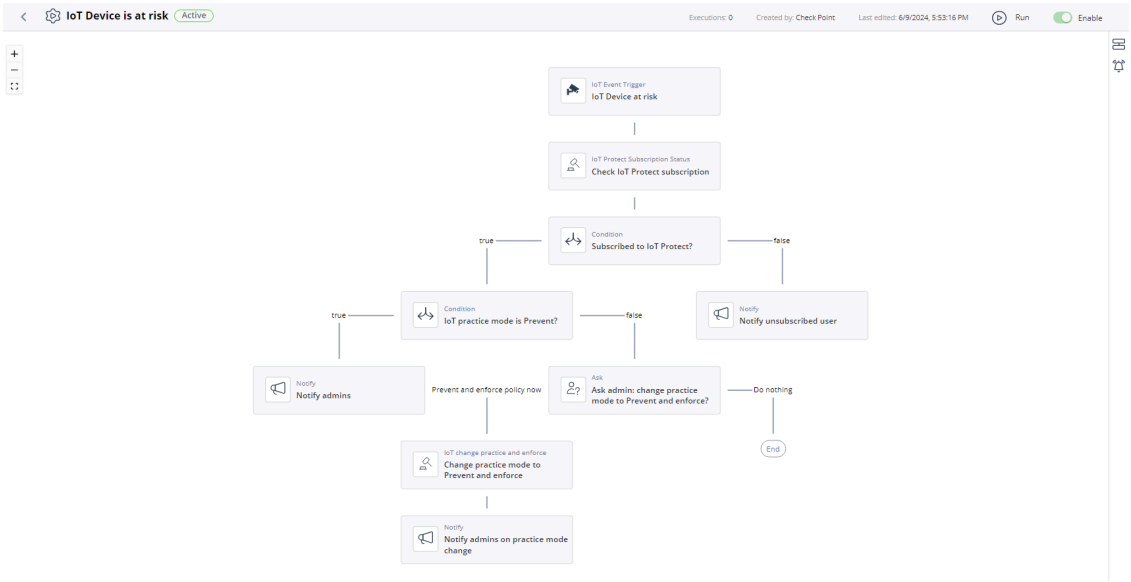
Trigger

Matching IoT device at risk.

This automation is automatically called by IoT Security.

To view the example of this log, click Run.

Flow



6.2.63. Notify on Endpoint Security client uninstall password change

This topic describes automation that notifies when the Endpoint Security client uninstall password changes. It includes supported product details, parameters, trigger conditions, and flow information.

The automation notifies upon changes to the Endpoint Security client uninstall password.

Supported Product

Endpoint Security

Parameters

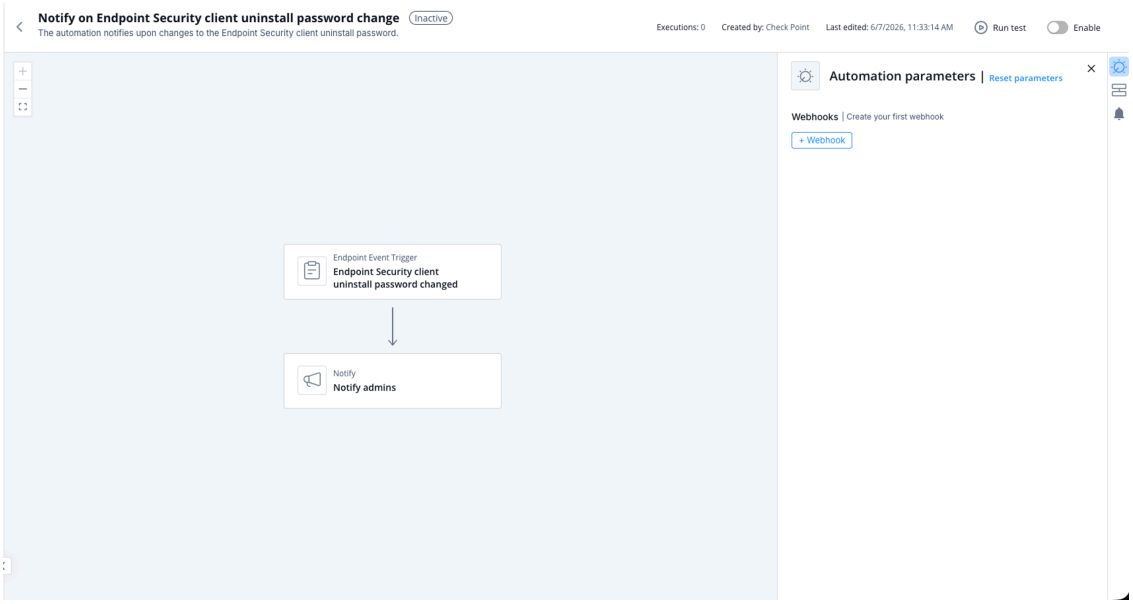
None

Trigger

When uninstall password change occurs.

To view the example of this log, click ../running-automation/running-the-automation.dita.

Flow



6.2.64. Notify on bulk uninstallation of Endpoint Security clients

This topic describes automation that notifies when multiple Endpoint Security clients are uninstalled within a defined time period. It also outlines supported products, parameters, trigger conditions, and flow information.

The automation notifies upon bulk uninstallation of Endpoint Security clients. The notification includes details on the number of uninstalled clients in the time duration.

Supported Product

Endpoint Security

Parameters

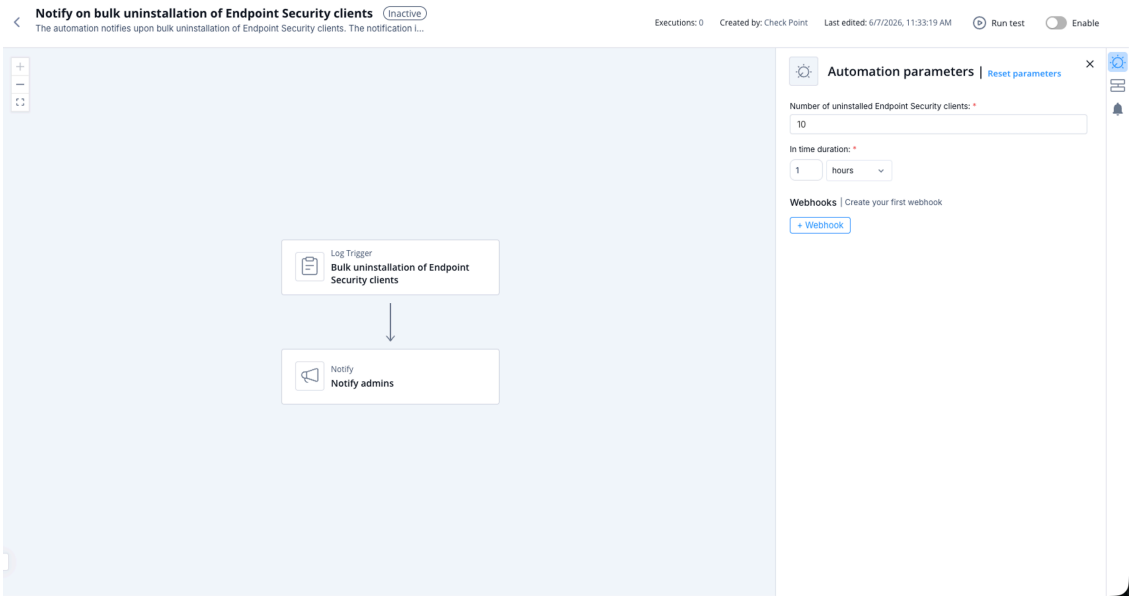
Number of uninstalled Endpoint Security clients	Set the number of uninstalled Endpoint Security clients.
In time duration	Set the time duration for the uninstalled Endpoint Security clients.

Trigger

When the number of uninstalled Endpoint Security clients match the specified value in the automation parameters.

To view the example of this log, click ../running-automation/running-the-automation.dita.

Flow



6.2.65. Notify on repeated login failures to user Windows device

This topic describes an automation that alerts on repeated login failures to a user's Windows device. It provides information about failure counting and details included in the notification.

The automation notifies upon repeated login failures to user Windows device. A parameter to count failures by user can be set using the automation parameters. The notification includes details on the number of failures in the time duration.

6.2.65.1. Supported Product

This topic describes the supported product referenced in the content. It provides a brief indication of the applicable product environment.

Endpoint Security

6.2.65.2. Parameters

This topic describes configurable parameters for handling repeated failed login attempts. It includes options for thresholds, time duration, and user-based counting.

Number of repeated failed login attempts	Set the number of repeated failed login attempts after which the system notifies the Administrator. The default value is **3**.
In time duration	Set the time duration for the repeated failed login attempts. The default duration is **5 minutes**.
Count failures for each user individually? **('no' means count failures in total for any user)**	Select the checkbox if you want to count failures by each user individually.

6.2.65.3. Trigger

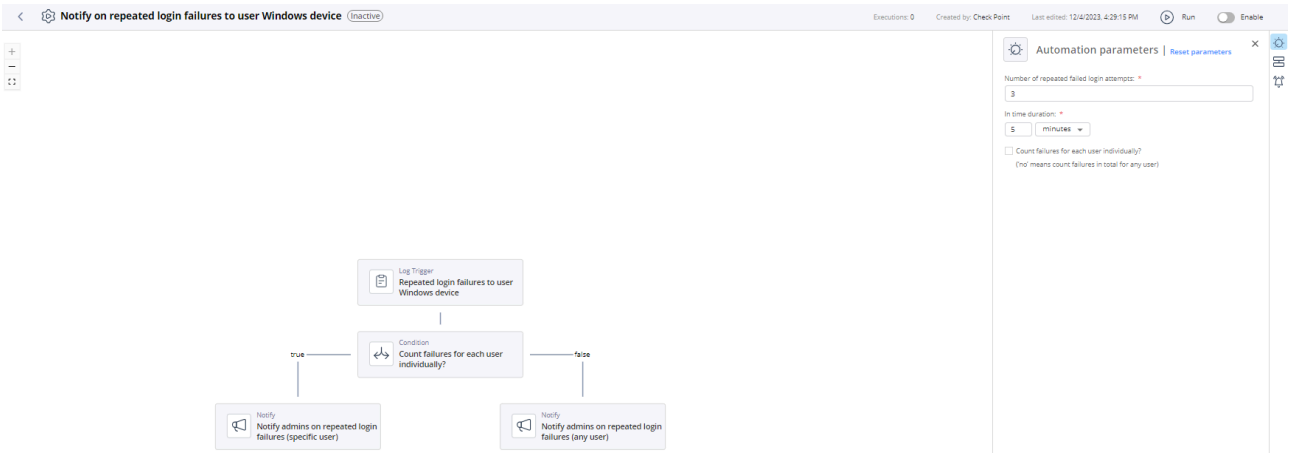
This topic describes the trigger conditions related to repeated failed login attempts. It also directs users to an example log entry.

When the number of repeated failed login attempts match the specified value in the automation parameters.

To view the example of this log, click Run.

6.2.65.4. Flow

This topic shows a flow diagram related to repeated login failure notifications for a Windows device. It provides a visual overview of the process.



6.2.66. Reset User Password in Identity Provider

This topic describes how the automation resets a user password in the identity provider linked to the account. It outlines supported products, parameters, triggers, and the automation flow.

The automation resets the password for the specific user in the relevant Identity Provider linked to the account.

> **Note:**
>
> This automation is also used by XDR.

Supported Product

Microsoft Entra ID, Okta

Parameters

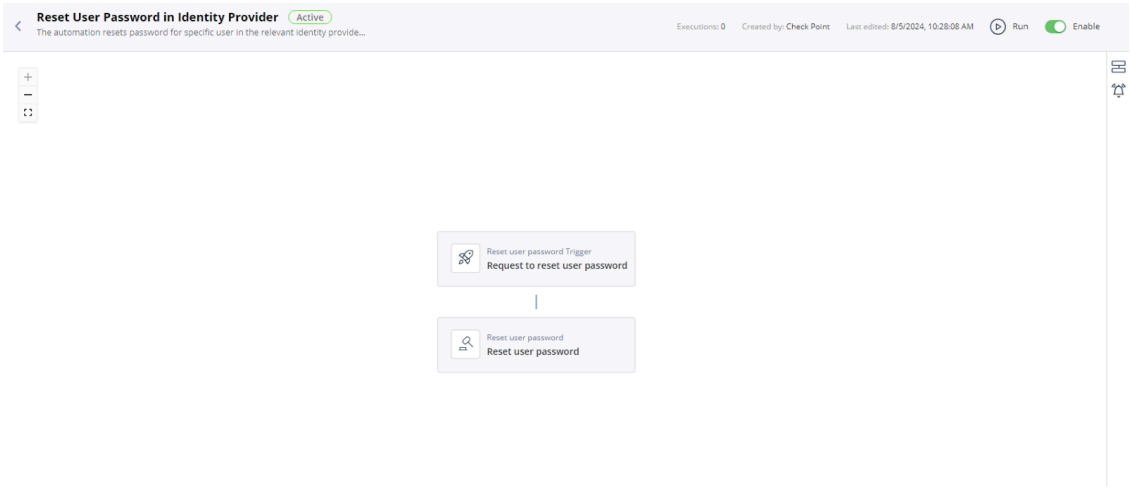
None

Trigger

The input includes **userEmail** of the user whose password needs to be reset.

To view the example of this log, click Run.

Flow



6.2.67. Delete file on Endpoint Security device

This topic describes the automation that deletes a file on a Endpoint Security device and outlines its parameters, triggers, and workflow.

The automation deletes file on Endpoint Security device.

Supported Product

Endpoint Security

Parameters

Comment	(Optional) Enter a comment or description.
Action will expire after	Set the expiration period for the automation.
Notification subject	Enter a subject for a notification you receive through a configured communication tool.
Notification message	Enter the text for a notification you receive through a configured communication tool.
Inform user (via UserCheck popup message)	Select the checkbox to get a popup message during the operation. Otherwise, the automation is executed silently.
Allow the user to postpone the operation	Select the checkbox to postpone the operation.

Trigger

The input includes the target, its type and the path of the file to delete.

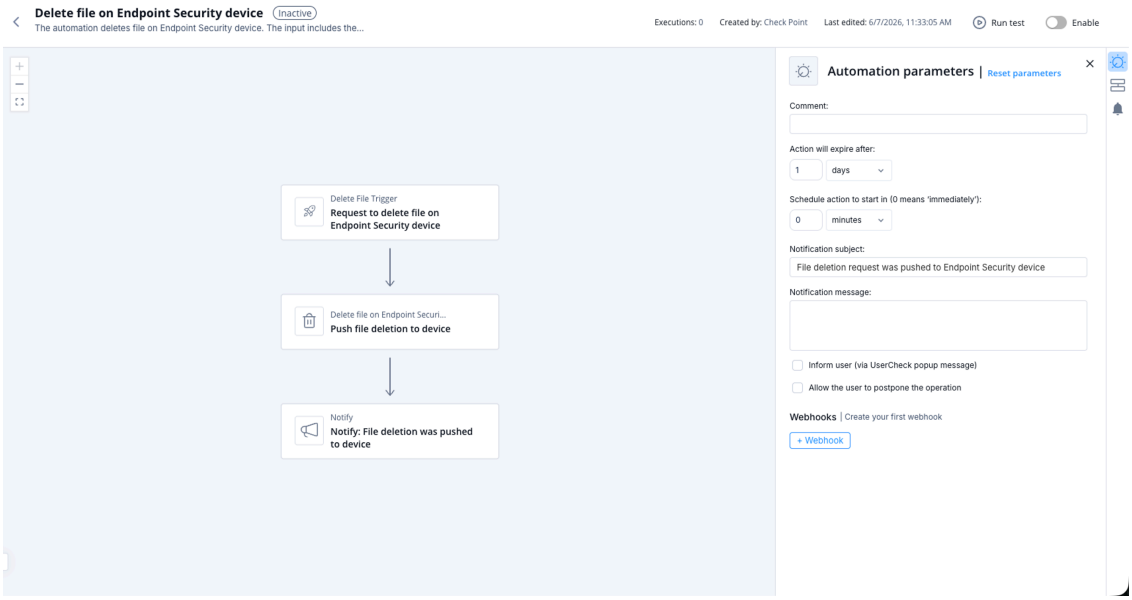
Supported types:

- `computerName`
- `computerIp`
- `computerId`

Matching deleted file on Endpoint Security device.

To view the example of this log, click ../running-automation/running-the-automation.dita.

Flow



6.2.68. Terminate process on Endpoint Security device

This topic describes the automation that terminates a process on a Endpoint Security device.

The automation terminates process on Endpoint Security device.

Supported Product

Endpoint Security

Parameters

Comment	(Optional) Enter a comment or description.
Action will expire after	Set the expiration period for the automation.
Notification subject	Enter a subject for a notification you receive through a configured communication tool.
Notification message	Enter the text for a notification you receive through a configured communication tool.
Inform user (via UserCheck popup message)	Select the checkbox to get a popup message during the operation. Otherwise, the automation is executed silently.

Allow the user to postpone the operation	Select the checkbox to postpone the operation.
Terminate all instances	Select the checkbox to terminate all instances.

Trigger

The input includes the target, its type and the process to terminate.

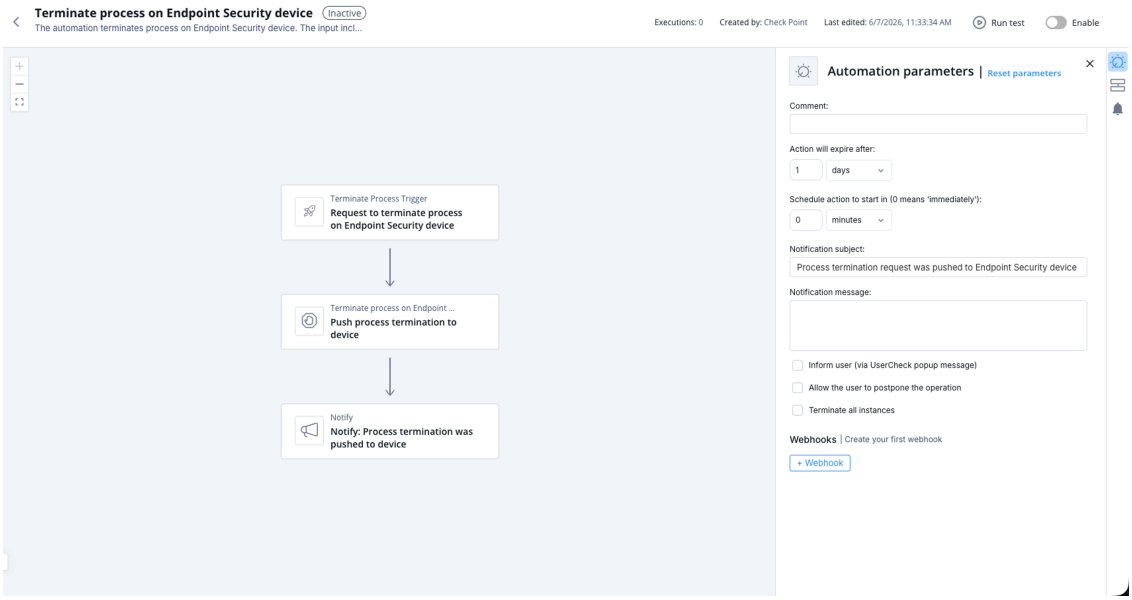
Supported types:

- `computerName`
- `computerIp`
- `computerId`

Matching terminate process on Endpoint Security device.

To view the example of this log, click ../running-automation/running-the-automation.dita.

Flow



6.2.68.1. Parameters

This topic describes parameters available for configuring automation behavior. It provides details for each option and its intended use.

Comment	(Optional) Enter a comment or description.
Action will expire after	Set the expiration period for the automation.
Notification subject	Enter a subject for a notification you receive through a configured communication tool.

Notification message	Enter the text for a notification you receive through a configured communication tool.
Inform user (via UserCheck popup message	Select the checkbox to get a popup message during the operation. Otherwise, the automation is executed silently.
Allow the user to postpone the operation	Select the checkbox to postpone the operation.
Terminate all instances	Select the checkbox to terminate all instances.

6.2.68.2. Trigger

This topic describes the inputs required for triggering a terminate process action and presents the flow of the operation. It outlines supported target types and the overall process.

The input includes the target, its type and the process to terminate.

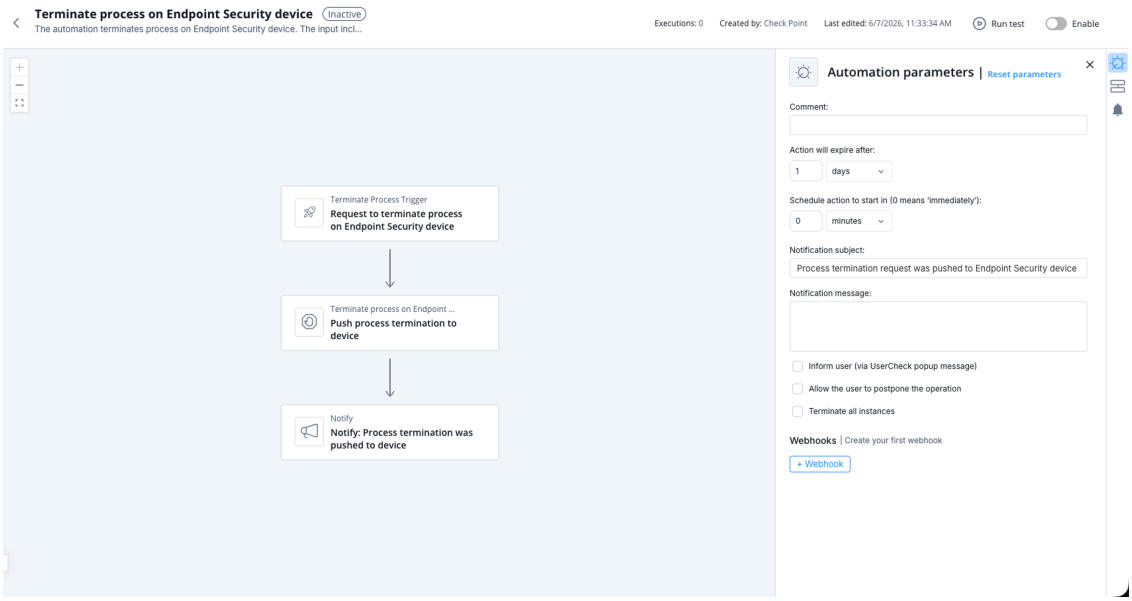
Supported types:

- `computerName`
- `computerIp`
- `omputerId`

Matching terminate process on Endpoint Security device.

To view the example of this log, click Run.

Flow



6.2.69. Scan Endpoint Security Device

This topic describes scanning a Endpoint Security device for malware. It provides information about supported product, parameters, trigger, and flow.

The automation scans for malwares on Endpoint Security device.

Supported Product

Endpoint Security

Parameters

Note:

You must specify at least one parameter to perform the scan.

Comment	(Optional) Enter a comment or description.
Action will expire after	Set the expiration period for the automation.
Schedule action to start in (0 means 'immediately')	Schedule when to start the operation.
Notification subject	Enter a subject for a notification you receive through a configured communication tool.
Notification message	Enter the text for a notification you receive through a configured communication tool.
Inform user (via UserCheck popup message)	Select the checkbox to get a popup message during the operation. Otherwise, the automation is executed silently.
Allow the user to postpone the operation	Select the checkbox to allow users to postpone the scan.
File size limit (0 means 'no limit')	Select the checkbox to set a limit to file size.
Scan operation system, processes and memory	Select the checkbox to scan operation system, processes and memory.
Scan local drives	Select the checkbox to scan local drives.
Scan CD-ROM	Select the checkbox to scan Compact Disc Read-Only Memory (CD-ROM).
Scan removable drives	Select the checkbox to scan removable drives.
Scan network drives	Select the checkbox to scan network drives.

Scan other drives	Select the checkbox to scan other drives.
Skip non executables	Select the checkbox to skip non executables.

Trigger

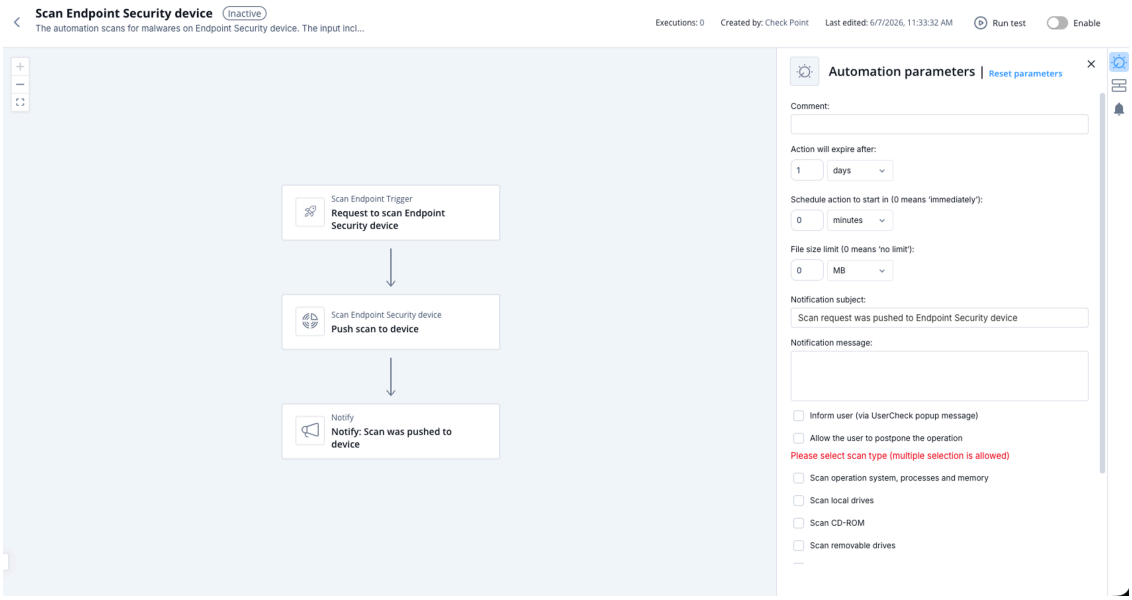
The input includes the target and its type.

Supported types:

- `computerName`
- `computerIp`
- `computerId`

To view the example of this log, click ../running-automation/running-the-automation.dita.

Flow



6.2.69.1. Parameters

This topic describes the parameters available for configuring a scan. It provides explanations for each option you can set.

Note:

You must specify at least one parameter to perform the scan.

Comment	(Optional) Enter a comment or description.
Action will expire after	Set the expiration period for the automation.

Schedule action to start in (0 means 'immediately')	Schedule when to start the operation.
Notification subject	Enter a subject for a notification you receive through a configured communication tool.
Notification message	Enter the text for a notification you receive through a configured communication tool.
Inform user (via UserCheck popup message)	Select the checkbox to get a popup message during the operation. Otherwise, the automation is executed silently.
Allow the user to postpone the operation	Select the checkbox to allow users to postpone the scan.
File size limit (0 means 'no limit')	Select the checkbox to set a limit to file size.
Scan operation system, processes and memory	Select the checkbox to scan operation system, processes and memory.
Scan local drives	Select the checkbox to scan local drives.
Scan CD-ROM	Select the checkbox to scan Compact Disc Read-Only Memory (CD-ROM).
Scan removable drives	Select the checkbox to scan removable drives.
Scan network drives	Select the checkbox to scan network drives.
Scan other drives	Select the checkbox to scan other drives.
Skip non executables	Select the checkbox to skip non executables.

6.2.69.2. Trigger

This topic describes the trigger input and the supported target types. It also provides a link to view an example log.

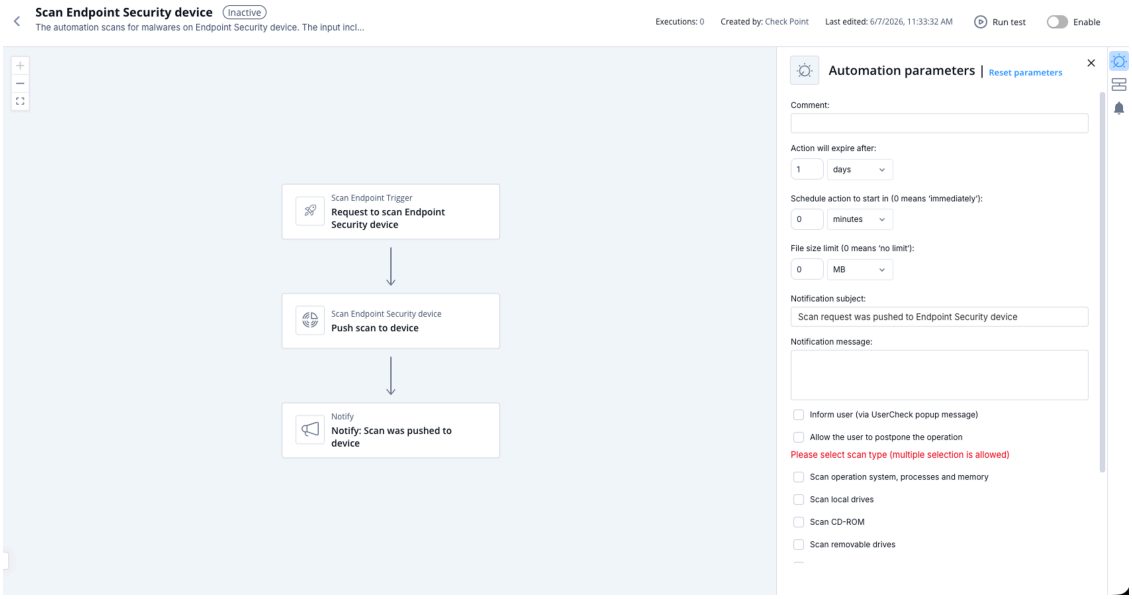
The input includes the target and its type.

Supported types:

- `computerName`
- `computerIp`
- `omputerId`

To view the example of this log, click Run.

6.2.69.3. Flow



6.2.70. IOC Management - New indicator

This topic describes the settings and parameters used to add a new indicator to an IOC feed. It also outlines the trigger behavior and provides a flow diagram.

The automation adds a new indicator to an IoC feed.

Supported Product

XDR IOC Management

Parameters

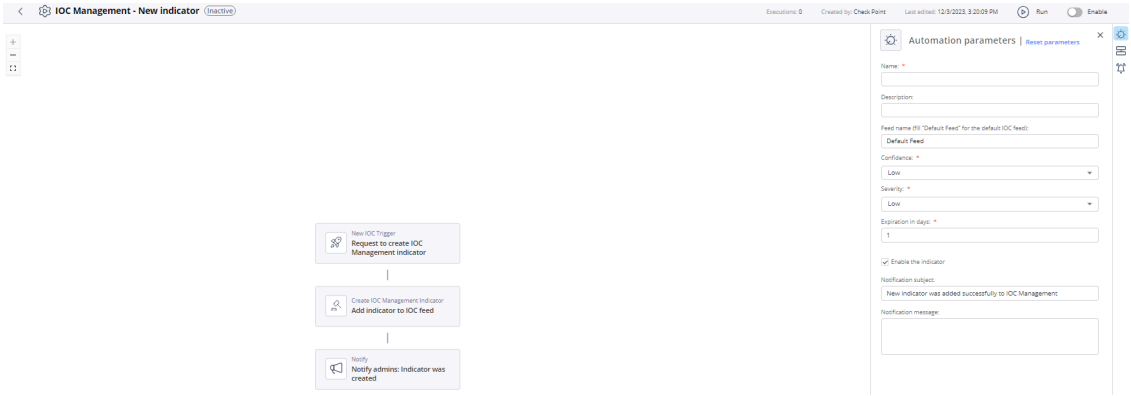
Name	Enter a name.
Description	(Optional) Enter a description for the IoC.
Feed name	Enter the feed name. Make sure the feed name already exists in IoC Management. The default is **Default Feed**.
Confidence	Select the confidence level of the IoC from the list. Default level is **Low**.
Severity	Select the severity level of the IoC from the list. Default level is **Low**.
Expiration in days	Set the expiration period for the automation.
Enable the indicator	Select the checkbox to enable the indicator.
Notification subject	Enter a subject for notification you receive through a configured communication tool.
Notification message	Enter the text for the notification you receive through a configured communication tool.

Trigger

Matching IOC management new indicator.

To view the example of this log, click Run.

Flow



6.2.71. IOC Management - Delete indicator

This topic describes how an automation deletes an existing indicator from an IOC feed and lists parameters, triggers, and flow information.

Supported Product

XDR IOC Management

Parameters

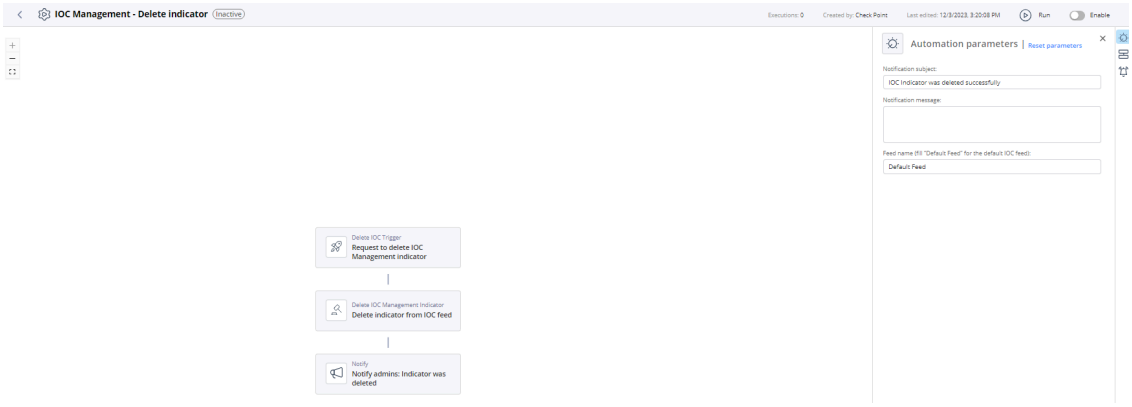
Notification subject	Enter a subject for notification you receive through a configured communication tool.
Notification message	Enter the text for the notification you receive through a configured communication tool.
Feed name	Enter a feed name. Default value is **Default Feed**.

Trigger

Matching IOC management delete indicator.

To view the example of this log, click Run.

Flow



The automation deletes an existing indicator from an IoC feed.

6.2.72. Stop and quarantine file via Microsoft Defender

This topic describes how the automation stops and quarantines a file on a Microsoft Defender machine and outlines the required parameters, trigger details, and flow.

The automation stops and quarantines a file on the Microsoft Defender machine.

Supported Product

Microsoft Defender for Endpoint

Parameters

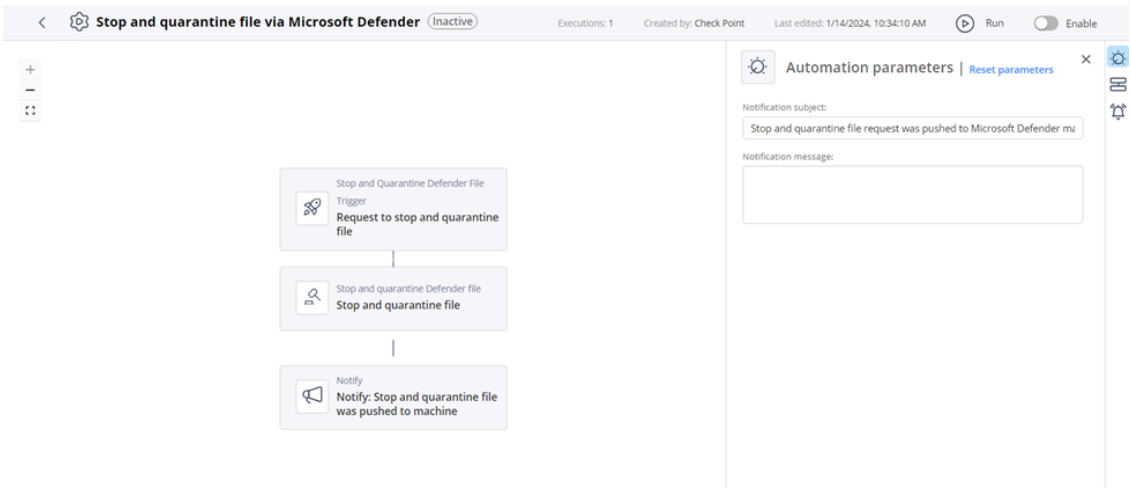
Notification subject	Enter a subject for a notification you receive through a configured communication tool.
Notification message	Enter the text for a notification you receive through a configured communication tool.

Trigger

The input includes machine ID of the Microsoft Defender machine, a comment, and sha1 of the file on the machine.

To view the example of this log, click Run.

Flow



6.2.73. Scan machine via Microsoft Defender

This topic describes how the automation scans a machine using Microsoft Defender and details supported products, parameters, triggers, and flow.

Supported Product

Microsoft Defender for Endpoint

Parameters

Notification subject	Enter a subject for a notification you receive through a configured communication tool.
Notification message	Enter the text for a notification you receive through a configured communication tool.

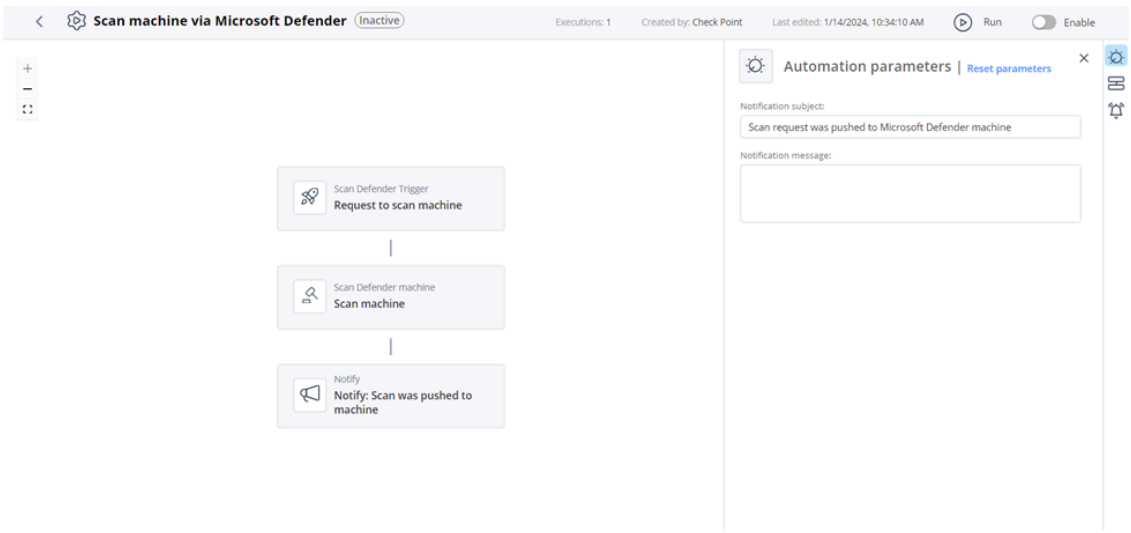
Trigger

The input includes machine ID of the Microsoft Defender machine, a comment, and the scan type. Scan type can be:

- **Full**
- **Quick**

To view the example of this log, click Run.

Flow



6.2.74. Isolate machine via Microsoft Defender (by XDR)

This topic describes the automation used to isolate a machine protected by Microsoft Defender. It outlines supported products, parameters, trigger conditions, and the automation flow.

Supported Product

XDR

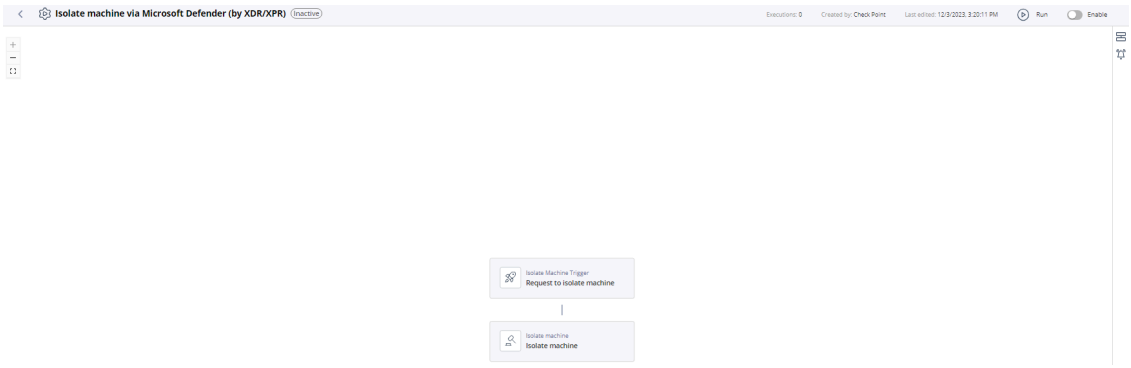
Parameters

None

Trigger

This automation is automatically called by XDR.

Flow



6.2.75. Release machine from isolation via Microsoft Defender (by XDR)

This topic describes an automation that releases a Microsoft Defender protected machine from isolation when triggered by XDR. It explains supported products, parameters, trigger behavior, and the automation flow.

The automation is used by XDR to release a machine that is protected by Microsoft Defender from isolation.

Supported Product

XDR

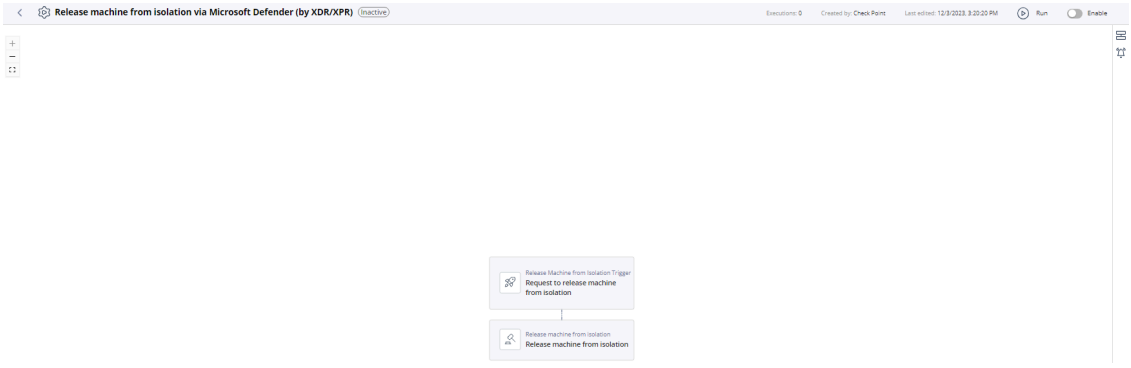
Parameters

None

Trigger

This automation is automatically called by XDR.

Flow



6.2.76. Stop and quarantine file via Microsoft Defender (by XDR)

This topic describes an automation that stops and quarantines a file on a machine protected by Microsoft Defender using XDR. It outlines supported products, parameters, trigger, and automation flow.

The automation is used by XDR to stop and quarantine a file on a machine that is protected by Microsoft Defender.

Supported Product

XDR

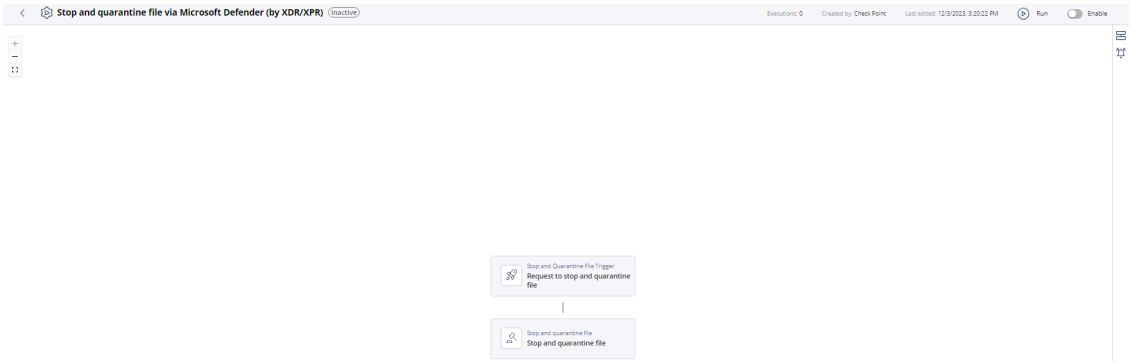
Parameters

None

Trigger

This automation is automatically called by XDR.

Flow



6.2.77. Handle SD-WAN Link Swap ISP Down

This topic describes the automation behavior when an SD-WAN link swap occurs due to an ISP outage and a critical ticket is generated for follow-up. It also summarizes supported products, parameters, trigger conditions, and workflow.

The automation alerts on SD-WAN link swap when the ISP is down. A critical ticket is opened for the user to follow up and take additional steps if necessary.

Supported Product

Quantum SD-WAN

Parameters

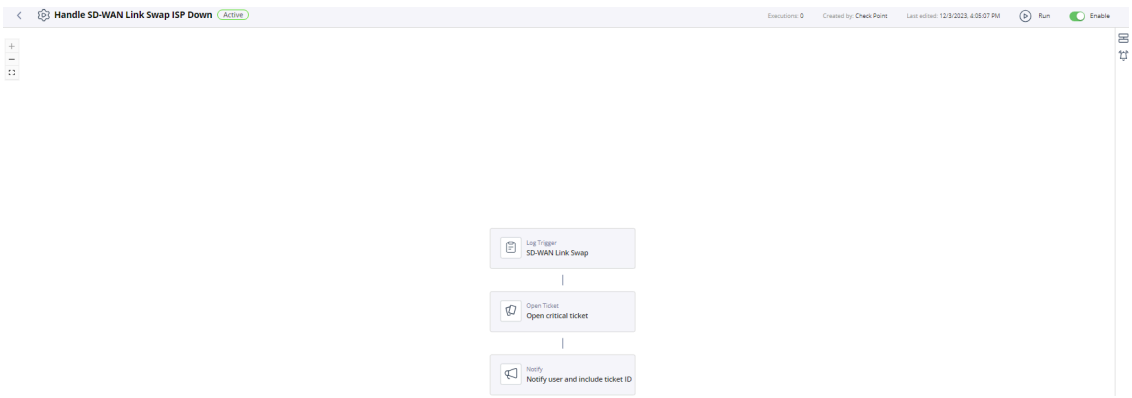
None

Trigger

The input for this automation is an SD-WAN event log that is identical to the following filter - appear in the **Log-Trigger** step.

To view the example of this log, click Run.

Flow



6.2.78. Open ticket

This topic describes how an automation creates a ticket in an enabled ticketing system based on a provided subject and description. It also lists supported products, parameters, trigger information, and flow details.

Supported Product

All

Parameters

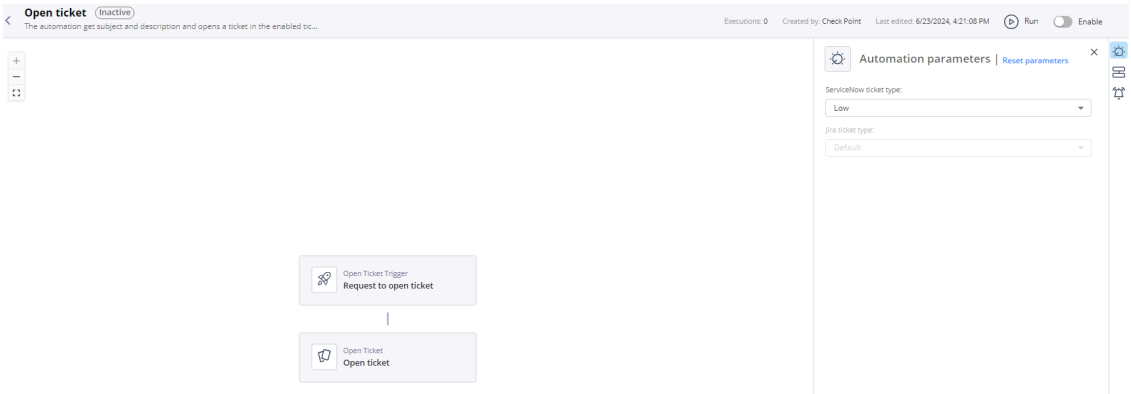
ServiceNow ticket type	Ticket type for ServiceNow connector.
Jira ticket type	Ticket type for Jira connector.

Trigger

Subject and Description for ticket.

To view the example of this log, click Run.

Flow



6.2.79. Close ticket

This topic describes the automation process that closes a ticket using a ticket number, close state, and close description. It also outlines supported products, parameters, triggers, and the automation flow.

The automation gets a ticket number, close state and close description and closes the ticket. The user can update additional fields as part of the close according to the ticketing system fields.

Supported Product

All

Parameters

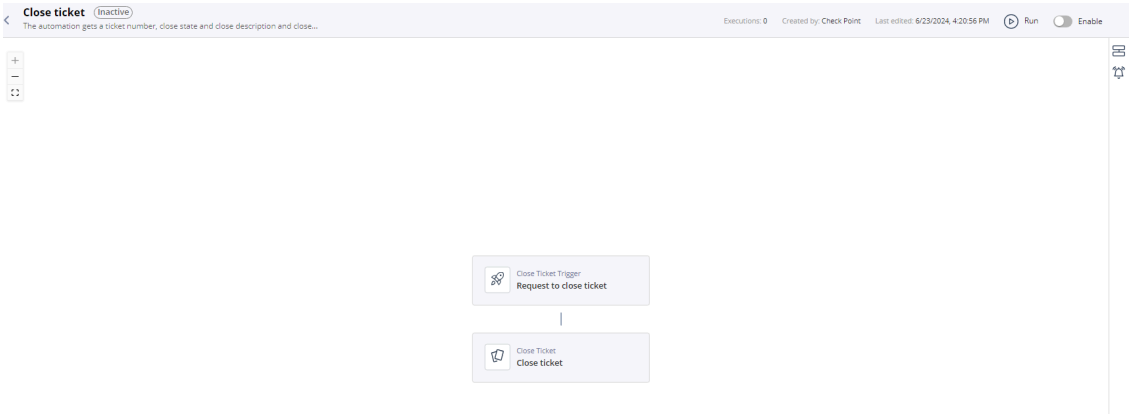
None

Trigger

Ticket number, close state and close description.

To view the example of this log, click Run.

Flow



6.2.80. Get ticket

This topic describes how the automation retrieves a ticket number and returns all available information about the ticket. It also lists supported products, parameters, triggers, and shows the process flow.

The automation gets a ticket number and returns all the information available about the ticket.

Supported Product

All

Parameters

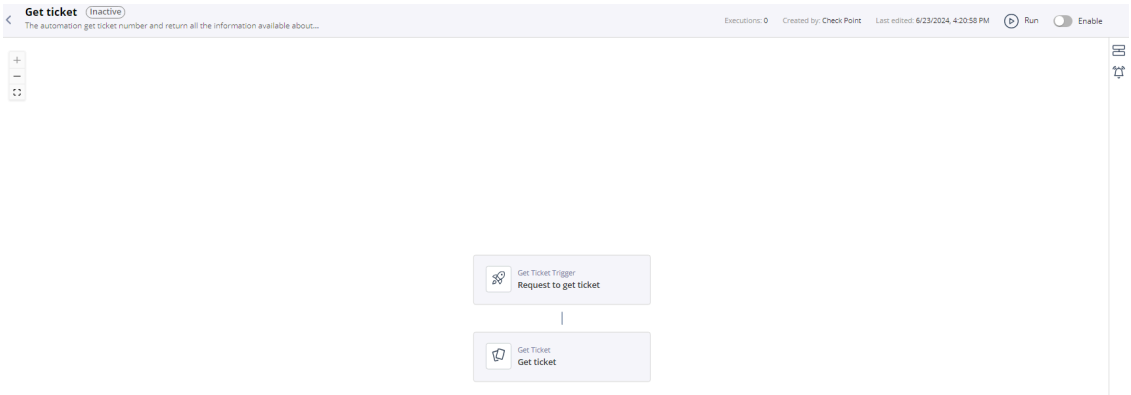
None

Trigger

Ticket number.

To view the example of this log, click Run.

Flow



6.2.81. Open ticket and notify

This topic describes how the automation opens a ticket and sends notifications when an event occurs. It also lists the configurable parameters and trigger behavior.

The automation opens a ticket (optional) and notifies on a given event.

Supported Product

None

Parameters

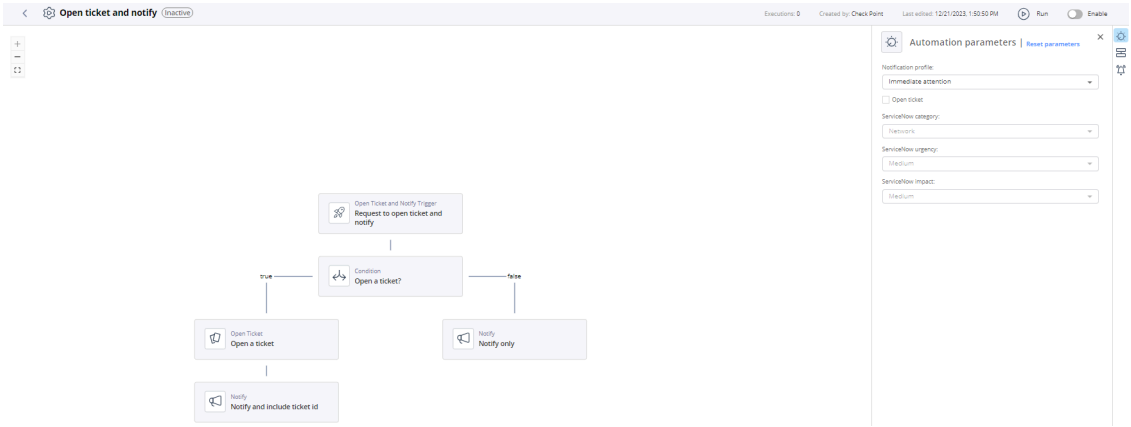
Notification profile	Select a notification profile to send the notification. For more information, see Notifications *(on page 257)*.
Open ticket	Select the checkbox if you want to open a ticket when the automation is triggered.
ServiceNow category	Select the category for the ticket in ServiceNow.
ServiceNow urgency	Select the urgency for the ticket in ServiceNow.
ServiceNow impact	Select the impact for the ticket in ServiceNow.

Trigger

When the automation is called.

To view the example of this log, click Run.

Flow



6.2.82. Spark Management event

This topic describes the automation used by Spark Management to handle detected events and shows the associated flow.

Supported Product

Spark Management

Parameters

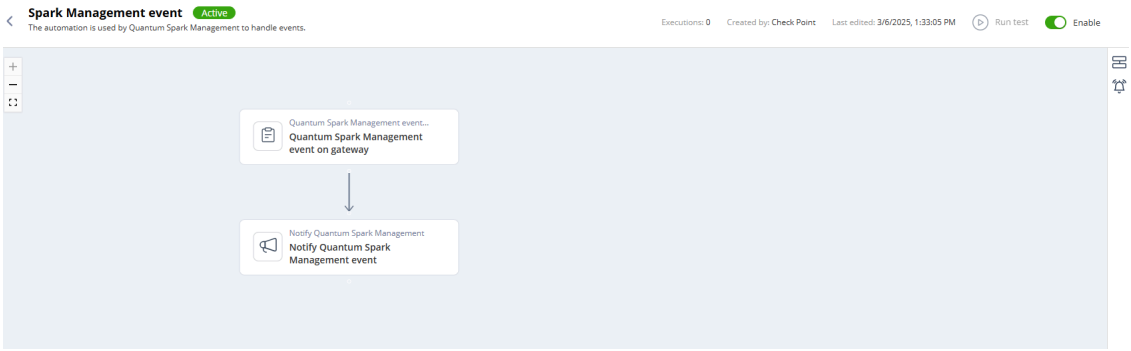
N/A

Trigger

When Spark Management event is detected on gateway.

To view the example of this log, click Run.

Flow



6.2.83. Alert on ransomware attack detected by Endpoint Security

This topic describes an automation that alerts when a ransomware attack is detected and outlines supported products, parameters, triggers, and workflow.

The automation notifies upon detection of ransomware attack. The notification includes information on the number of events and number of affected devices. Automation parameters can be set such as the affected devices threshold and total events threshold.

Supported Product

Endpoint Security

Parameters

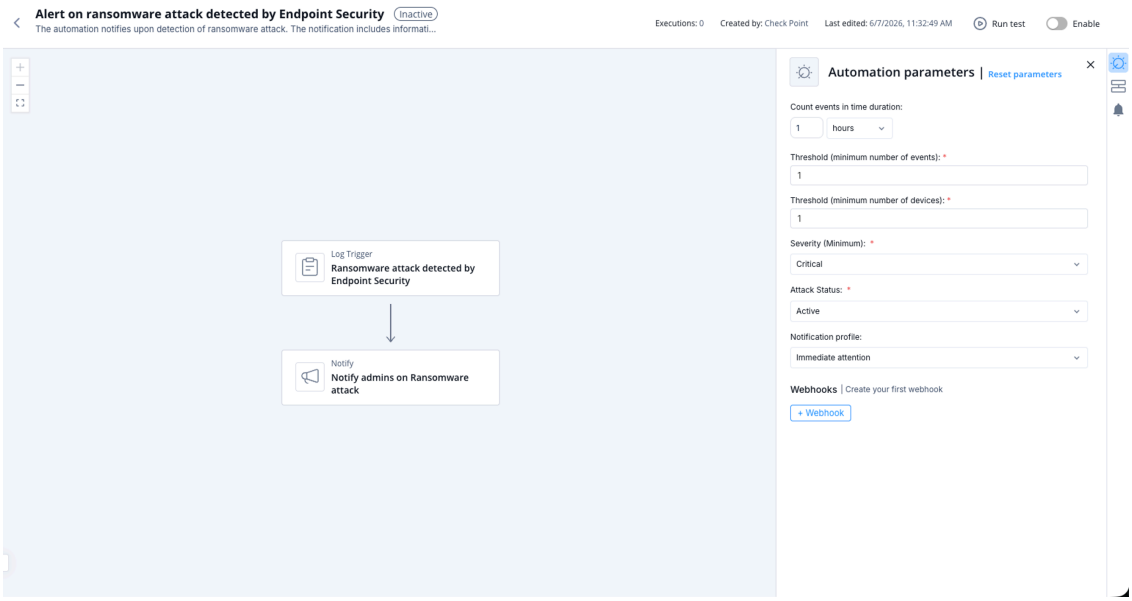
Count events in time duration	Set the duration of time in which to count the events.
Threshold (minimum number of events)	Set the minimum number of events for the automation to be triggered.
Threshold (minimum number of devices)	Set the minimum number of devices affected for the automation to be triggered.
Severity (Minimum)	Set the minimum severity.
Attack Status	Set the attack status.
Notification profile	Set the notification profile.

Trigger

When a ransomware attack is detected by Endpoint Security.

To view the example of this log, click ../running-automation/running-the-automation.dita.

Flow



6.2.84. Alert on Generative AI Risky Session

This topic describes notifications generated when a Generative AI risky session is detected and outlines the parameters, trigger conditions, and flow.

Supported Product

Check Point Infinity GenAI Protect

Parameters

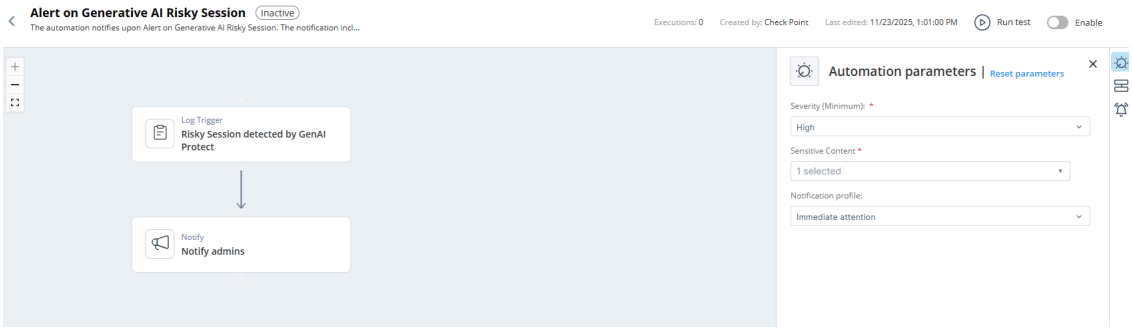
Severity (Minimum)	Set the minimum risk severity level that must be detected in a session for the automation to run. The automation triggers only when the session's risk severity is equal to or higher than the value you select.
Sensitive Content	Select the sensitive content types that should trigger the automation. The automation runs when the session includes any of the sensitive content categories you choose.
Notification profile	Select a notification profile to send the notification. For more information, see Notifications-s">Notifications *(on page 257)*.

Trigger

When an AI Risky Session is detected.

To view the example of this log, click Run *(on page 136)*.

Flow



6.2.85. Alert on a phishing attempt detected by Endpoint Security

This topic describes the alert generated when a phishing attempt is detected by Endpoint Security and lists its configurable parameters and trigger details.

The automation notifies upon detection of phishing attack. The notification includes information on the number of events and the affected devices. More parameters can be set using the automation parameters such as the affected devices threshold and total events threshold.

Supported Product

Endpoint Security

Parameters

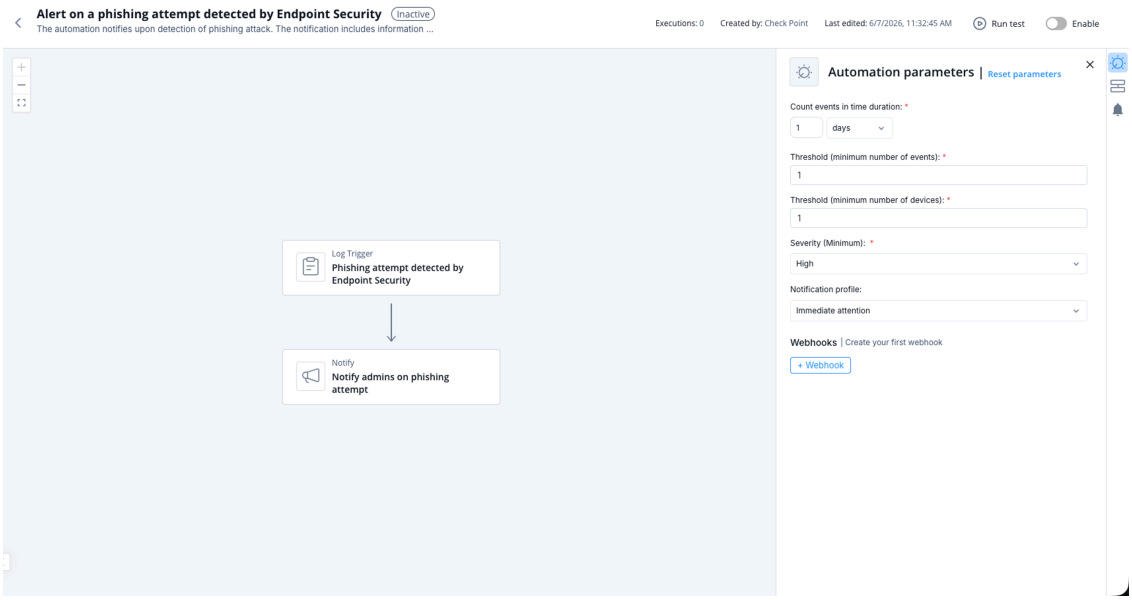
Count events in time duration	Set the duration of time in which to count the events.
Threshold (minimum number of events)	Set the minimum number of events for the automation to be triggered.
Threshold (minimum number of devices)	Set the minimum number of devices affected for the automation to be triggered.
Severity (Minimum)	Set the minimum severity.
Attack Status	Set the attack status.
Notification profile	Set the notification profile.

Trigger

When a phishing attempt is detected by Endpoint Security.

To view the example of this log, click ../running-automation/running-the-automation.dita.

Flow



6.2.86. Alert on malicious file detected by Endpoint Security

This topic describes the alert generated when a malicious file is detected by Endpoint Security and outlines its parameters, trigger, and flow. It provides information for configuring thresholds and notification settings.

The automation notifies upon detection of malicious file. The notification includes information on the number of events and number of affected devices. Automation parameters can be set such as the affected devices threshold and total events threshold.

Supported Product

Endpoint Security

Parameters

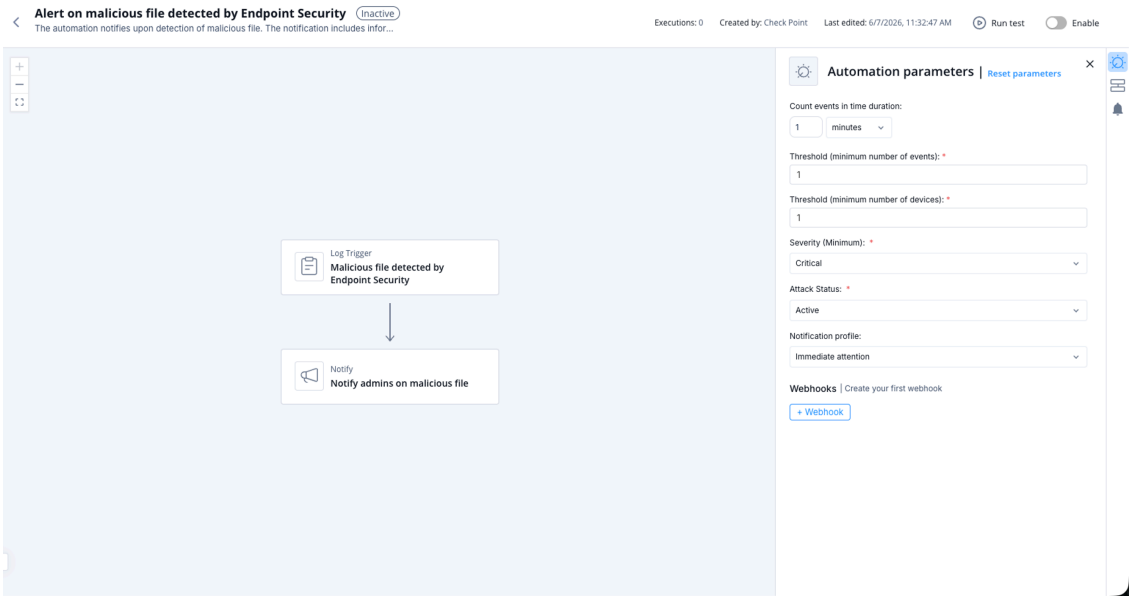
Count events in time duration	Set the duration of time in which to count the events.
Threshold (minimum number of events)	Set the minimum number of events for the automation to be triggered.
Threshold (minimum number of devices)	Set the minimum number of devices affected for the automation to be triggered.
Severity (Minimum)	Set the minimum severity.
Notification profile	Set the notification profile.

Trigger

When a malicious file is detected by Endpoint Security.

To view the example of this log, click ../running-automation/running-the-automation.dita.

Flow



6.2.87. Alert on access to malicious site detected by Endpoint Security

This topic describes the alert triggered when access to a malicious site is detected by Endpoint Security and outlines the available automation parameters. It also provides information about the trigger and flow of the automation.

The automation notifies upon detection of access to malicious sites. The notification includes information on the number of events and number of affected devices. Automation parameters can be set such as the affected devices threshold and total events threshold.

Supported Product

Endpoint Security

Parameters

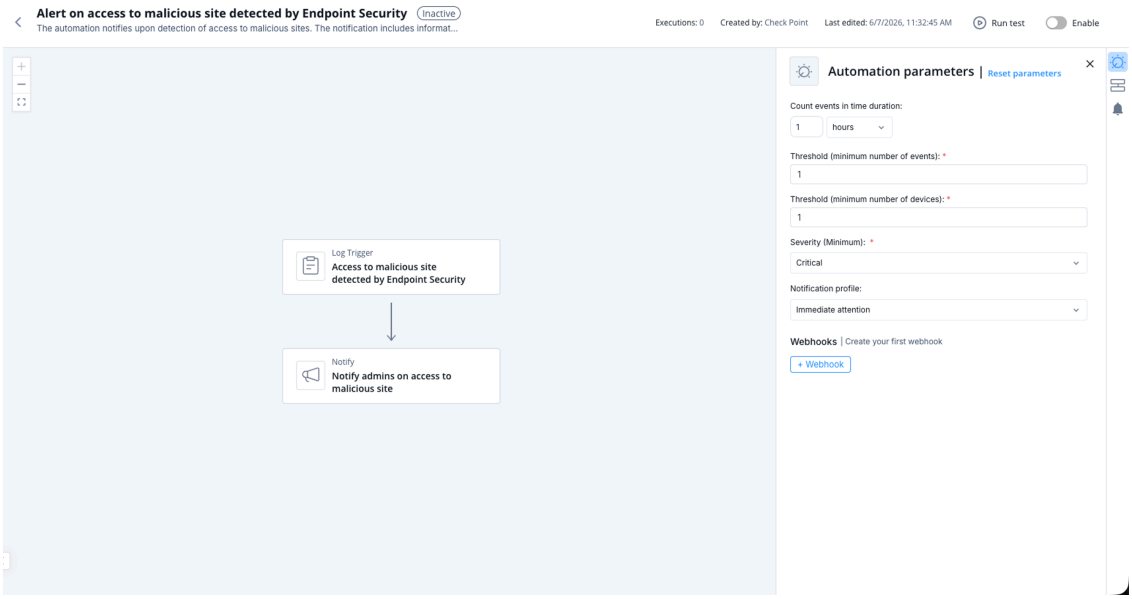
Count events in time duration	Set the duration of time in which to count the events.
Threshold (minimum number of events)	Set the minimum number of events for the automation to be triggered.
Threshold (minimum number of devices)	Set the minimum number of devices affected for the automation to be triggered.
Severity (Minimum)	Set the minimum severity.
Notification profile	Set the notification profile.

Trigger

When a malicious site is detected by Endpoint Security.

To view the example of this log, click ../running-automation/running-the-automation.dita.

Flow



6.2.88. Alert on password reuse attempt detected by Endpoint Security

This topic describes the alert triggered when a password reuse attempt is detected and explains the parameters and flow of the automation. It includes supported product information, trigger conditions, and configuration options.

The automation notifies upon the reuse of the password. The notification includes information on the number of events and number of affected devices. Automation parameters can be set such as the affected devices threshold and total events threshold.

Supported Product

Endpoint Security

Parameters

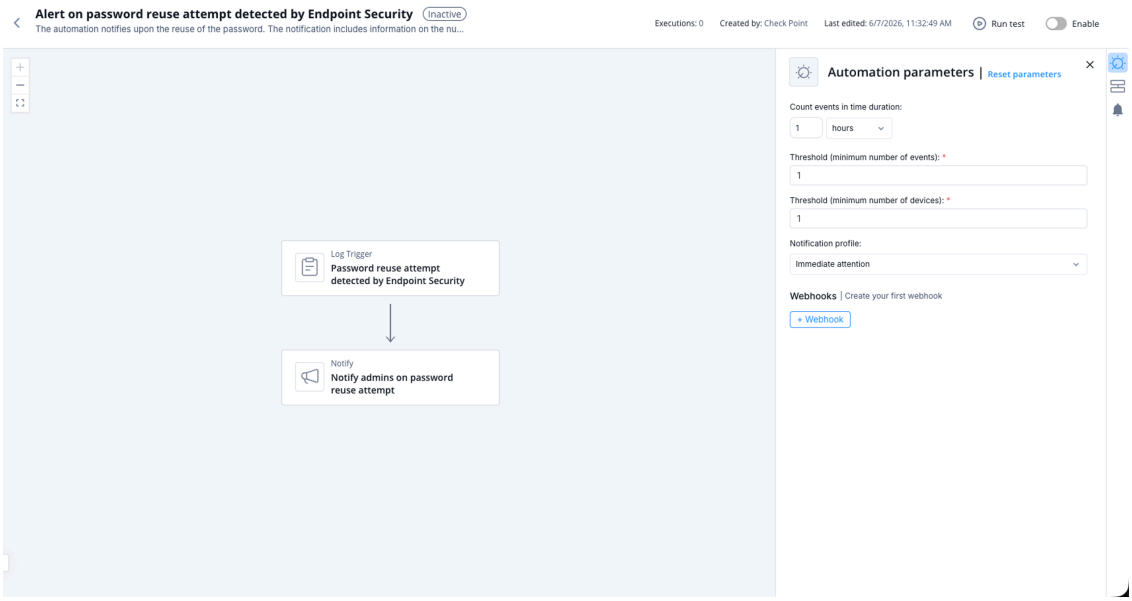
Count events in time duration	Set the duration of time in which to count the events.
Threshold (minimum number of events)	Set the minimum number of events for the automation to be triggered.
Threshold (minimum number of devices)	Set the minimum number of devices affected for the automation to be triggered.
Notification profile	Set the notification profile.

Trigger

When a password reuse is detected by Endpoint Security.

To view the example of this log, click ../running-automation/running-the-automation.dita.

Flow



6.2.89. Alert on exploit attempt detected by Endpoint Security

This topic describes alert behavior when an exploit attempt is detected and details the parameters, trigger conditions, and flow for the automation. It provides configuration information for thresholds, severity, and notification settings.

The automation notifies upon detection of exploit attack. The notification includes information on the number of events and number of affected devices. Automation parameters can be set such as the affected devices threshold and total events threshold.

Supported Product

Endpoint Security

Parameters

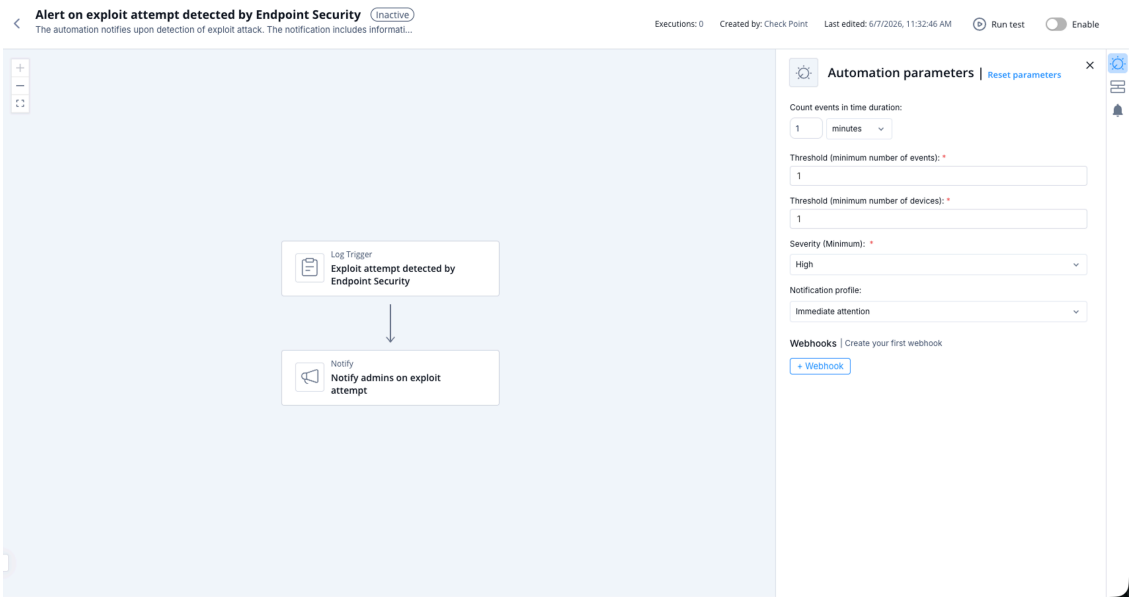
Count events in time duration	Set the duration of time in which to count the events.
Threshold (minimum number of events)	Set the minimum number of events for the automation to be triggered.
Threshold (minimum number of devices)	Set the minimum number of devices affected for the automation to be triggered.
Severity (Minimum)	Set the minimum severity.
Notification profile	Set the notification profile.

Trigger

When an exploit attempt is detected by Endpoint Security.

To view the example of this log, click ../running-automation/running-the-automation.dita.

Flow



6.2.90. Alert on the outdated Endpoint Security Static Analysis capability

This topic describes the alert generated when the Endpoint Security Static Analysis capability becomes outdated. It outlines the trigger, supported product, and flow of this automation.

The automation notifies if the Endpoint Security Static Analysis capability is outdated.

Supported Product

Endpoint Security

Parameters

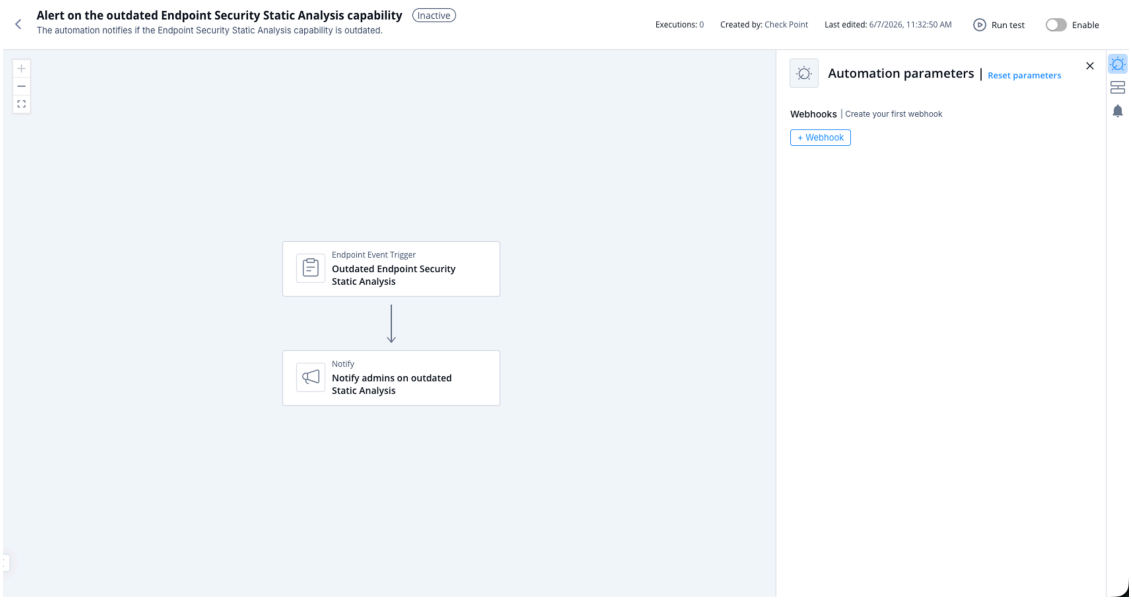
None

Trigger

When an outdated Endpoint Security Static Analysis capability is detected.

To view the example of this log, click ../running-automation/running-the-automation.dita.

Flow



6.2.91. Alert on the outdated Endpoint Security Offline Reputation capability

This topic describes an automation that notifies when the Endpoint Security Offline Reputation capability is outdated. It provides information about the supported product, trigger conditions, and flow.

The automation notifies if the Endpoint Security Offline Reputation capability is outdated.

Supported Product

Endpoint Security

Parameters

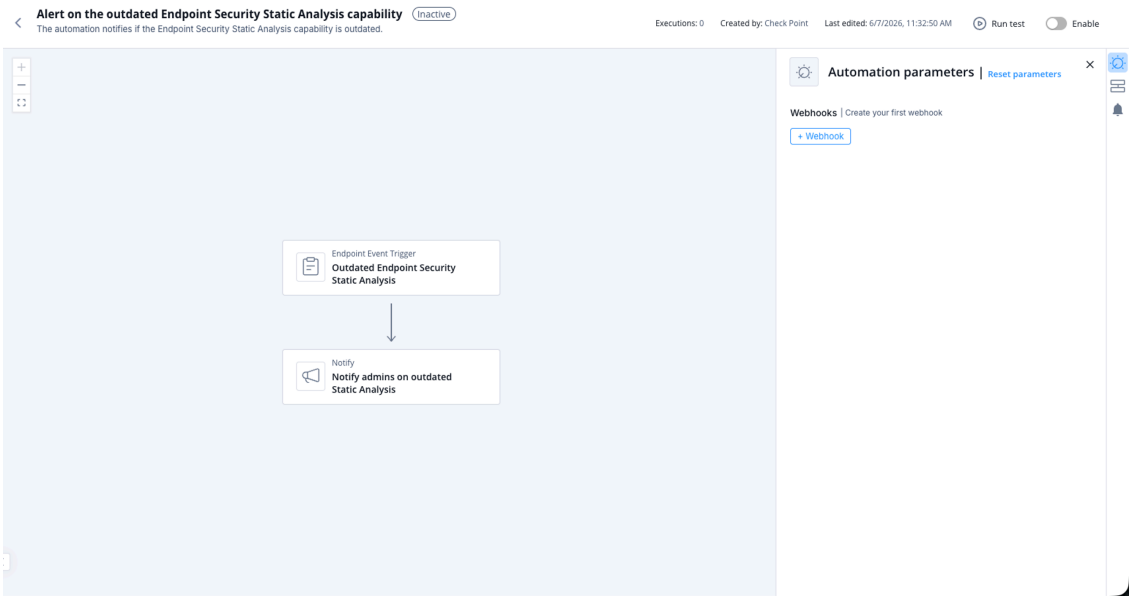
None

Trigger

When an outdated Endpoint Security Offline Reputation capability is detected.

To view the example of this log, click ../running-automation/running-the-automation.dita.

Flow



6.2.92. Alert on outdated Endpoint Security Behavioral Guard capability

This topic describes an automation alert that notifies when the Endpoint Security Behavioral Guard capability becomes outdated. It provides information about the trigger and flow of the alert.

The automation notifies if the Endpoint Security Behavioral Guard capability is outdated.

Supported Product

Endpoint Security

Parameters

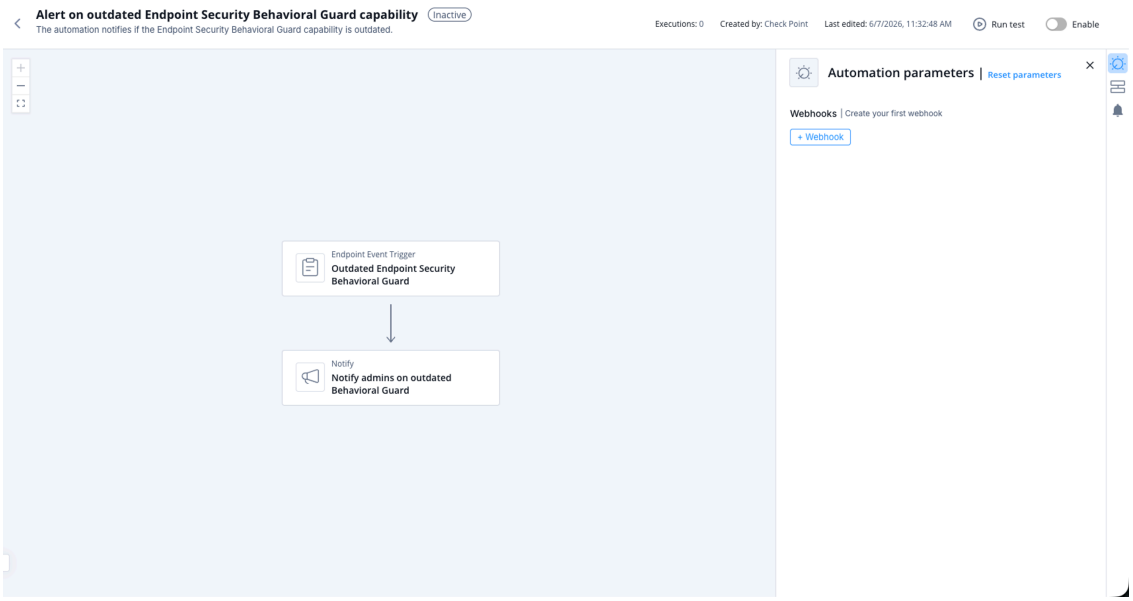
None

Trigger

When an outdated Endpoint Security Behavioral Guard capability is detected.

To view the example of this log, click ../running-automation/running-the-automation.dita.

Flow



6.2.93. Alert on disconnected Endpoint Security clients

This topic describes the automation that notifies when a Endpoint Security client becomes disconnected. It outlines the supported product, parameters, trigger, and flow.

The automation notifies if the Endpoint Security client is disconnected.

Supported Product

Endpoint Security

Parameters

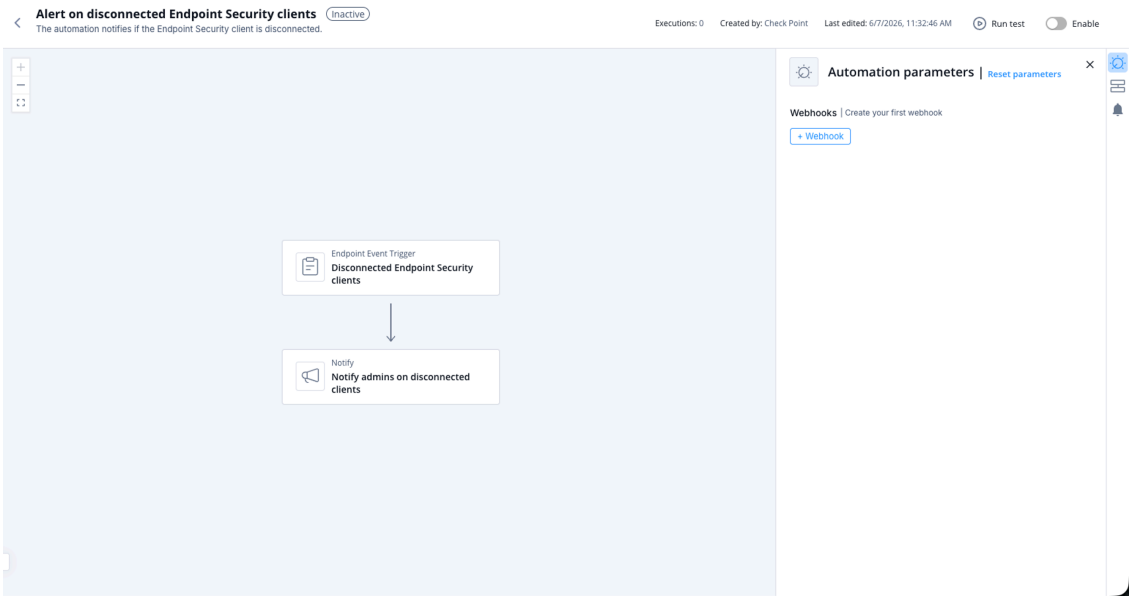
None

Trigger

When a disconnected Endpoint Security client is detected.

To view the example of this log, click ../running-automation/running-the-automation.dita.

Flow



6.2.94. Alert on Endpoint Security Compliance warnings

This topic describes how the automation notifies users when Endpoint Security compliance warnings are triggered. It also provides information about supported products, parameters, triggers, and flow.

The automation notifies upon triggered compliance warnings.

Supported Product

Endpoint Security

Parameters

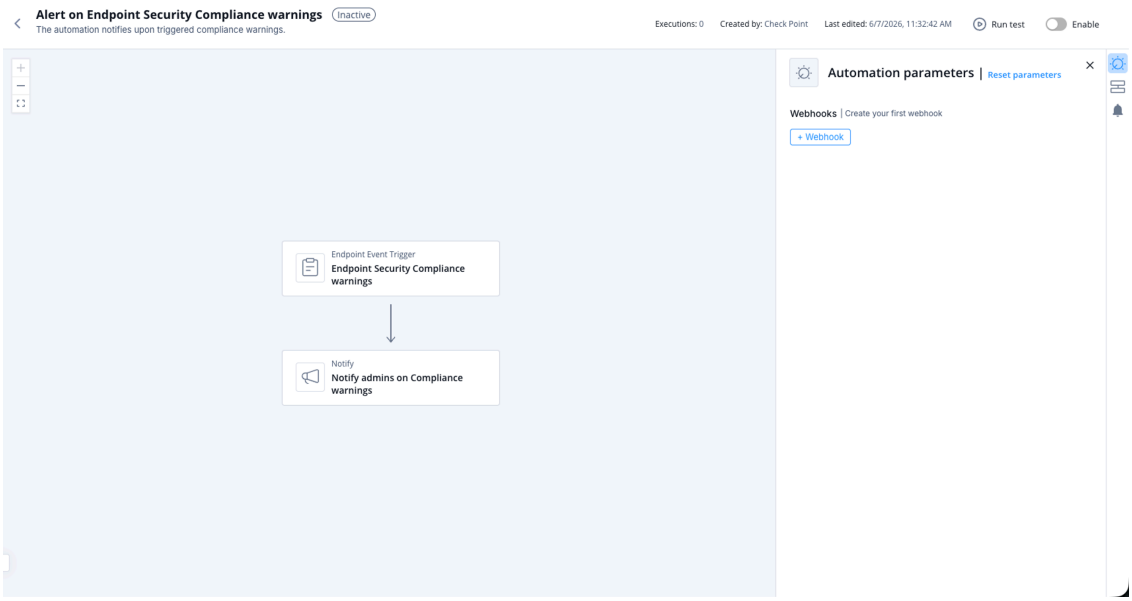
None

Trigger

When a Endpoint Security Compliance warning is detected.

To view the example of this log, click ../running-automation/running-the-automation.dita.

Flow



6.2.95. Alert on device restrictions by Endpoint Security

This topic describes notifications generated when device restrictions are initiated by the Endpoint Security compliance capability. It outlines supported products, parameters, triggers, and the process flow.

The automation notifies upon device restrictions initiated by the Endpoint Security Compliance capability.

Supported Product

Endpoint Security

Parameters

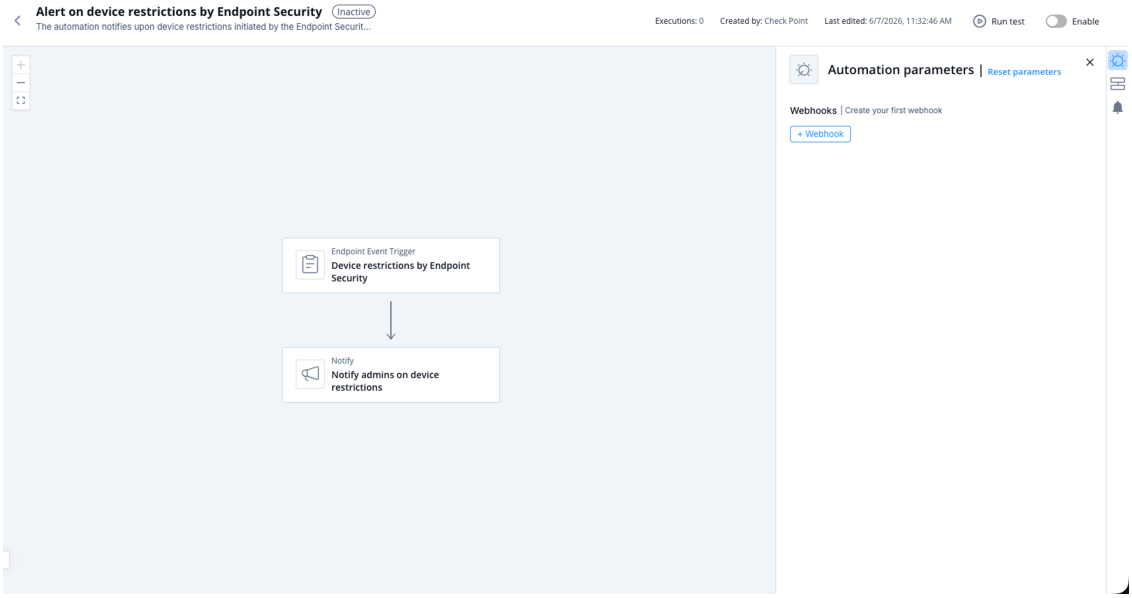
None

Trigger

When a device restriction by Endpoint Security is detected.

To view the example of this log, click ../running-automation/running-the-automation.dita.

Flow



6.2.96. Alert on outdated Endpoint Security Anti-Malware

This topic describes the alert generated when the Endpoint Security Anti-Malware capability is outdated. It also lists supported products, parameters, triggers, and flow information.

The automation notifies if the Endpoint Security Anti-Malware capability is outdated.

Supported Product

Endpoint Security

Parameters

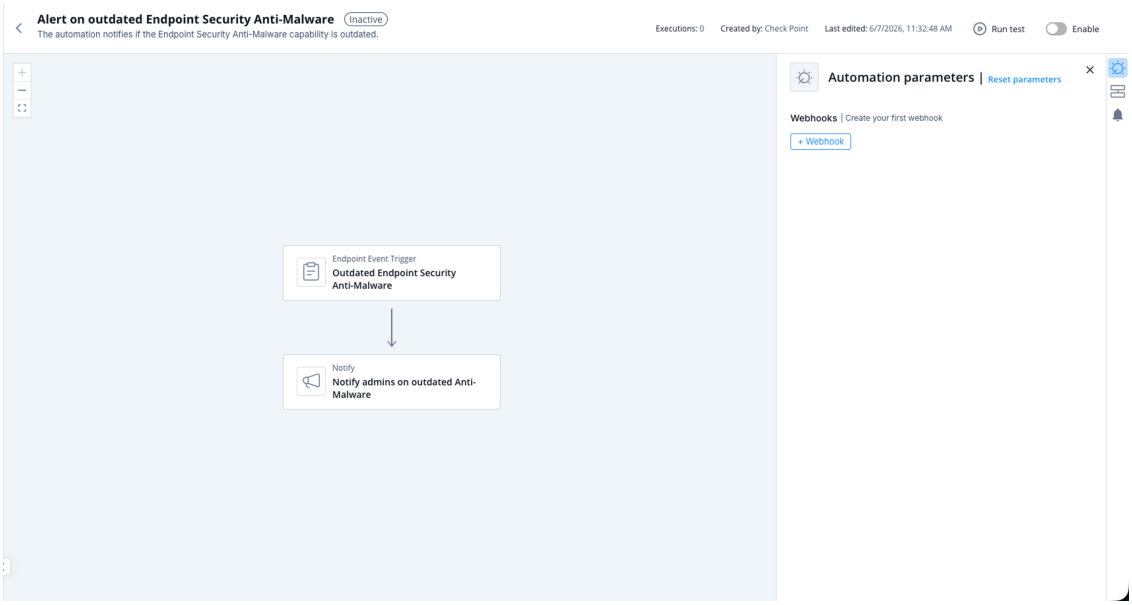
None

Trigger

When an outdated Endpoint Security Anti-Malware is detected.

To view the example of this log, click ../running-automation/running-the-automation.dita.

Flow



6.2.97. Alert if the device is not scanned by the Endpoint Security Anti-Malware capability

This topic describes an automation that alerts when a device has not been fully scanned by the Endpoint Security Anti-Malware capability. It outlines supported products, trigger conditions, and the flow of the automation.

The automation notifies if the device is not fully scanned by the Endpoint Security Anti-Malware.

Supported Product

Endpoint Security

Parameters

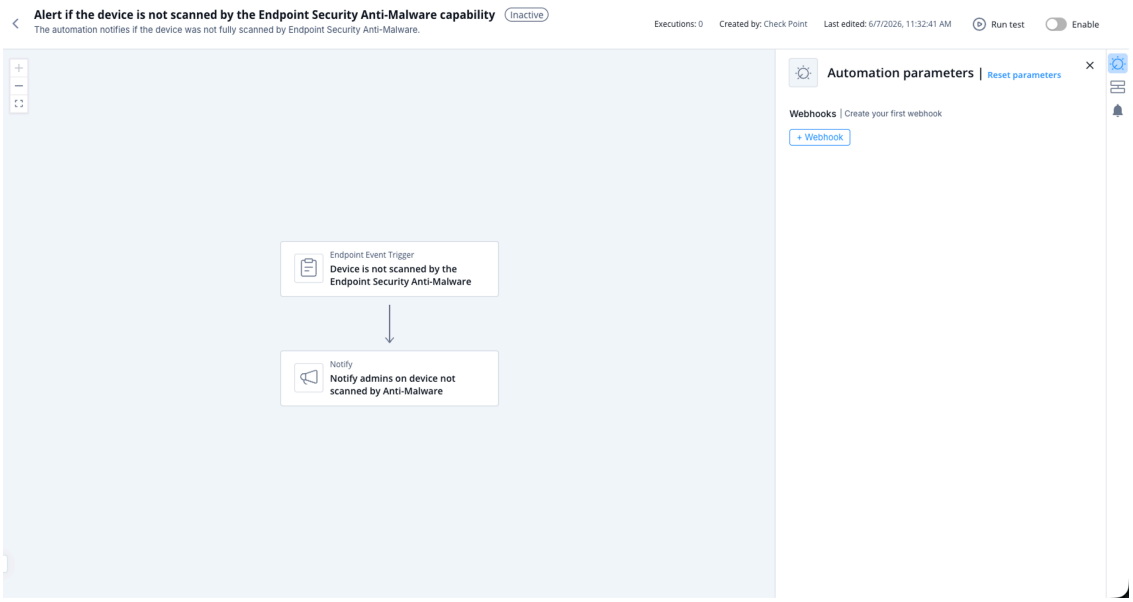
None

Trigger

When it was detected that the device was not scanned by the Endpoint Security Anti-Malware capability.

To view the example of this log, click ../running-automation/running-the-automation.dita.

Flow



6.2.98. Alert on Endpoint Security Anti-Malware license expiration

This topic describes the alert generated when the Endpoint Security Anti-Malware license expires and outlines its trigger and flow.

The automation notifies upon the Endpoint Security Anti-Malware license expiration.

Supported Product

Endpoint Security

Parameters

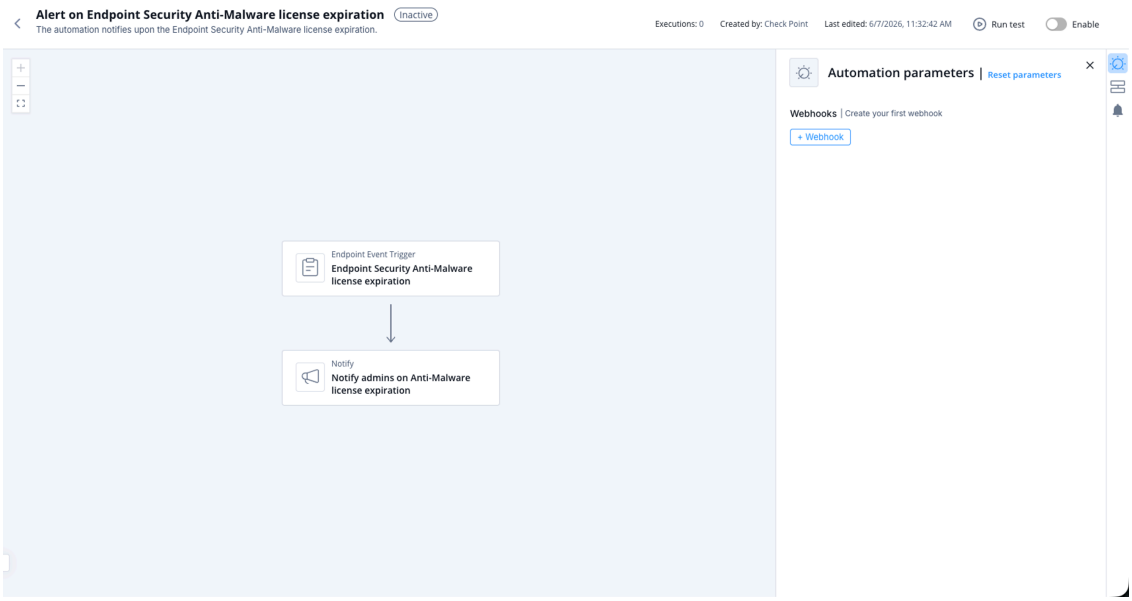
None

Trigger

When the Endpoint Security Anti-Malware license expiration is detected.

To view the example of this log, click ../running-automation/running-the-automation.dita.

Flow



6.2.99. Alert on Endpoint Security deployment failure

This topic describes the alert generated when a Endpoint Security Client deployment fails. It also outlines the supported product, trigger conditions, and flow overview.

The automation notifies if the Endpoint Security Client deployment failed on the device.

Supported Product

Endpoint Security

Parameters

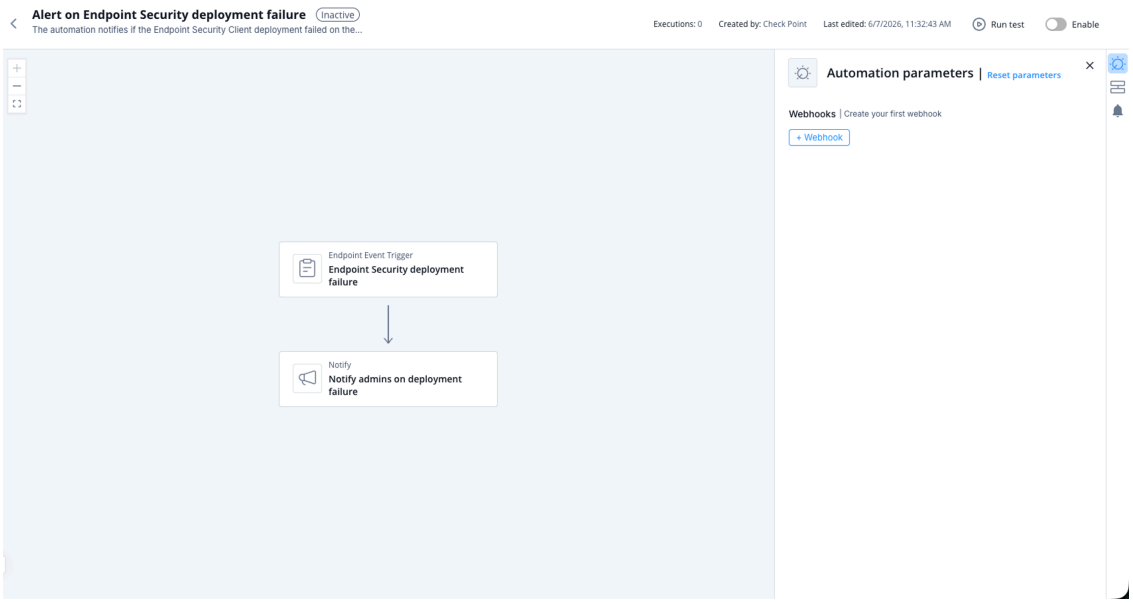
None

Trigger

When the Endpoint Security Client deployment failure is detected.

To view the example of this log, click ../running-automation/running-the-automation.dita.

Flow



6.2.100. Alert if Endpoint Security client capabilities stop running

This topic explains the alert that notifies when one or more Endpoint Security client capabilities stop running or fail to report their status.

The automation notifies if one or more capabilities on the Endpoint Security security client stops running or the client is unable to report the capability status.

Supported Product

Endpoint Security

Parameters

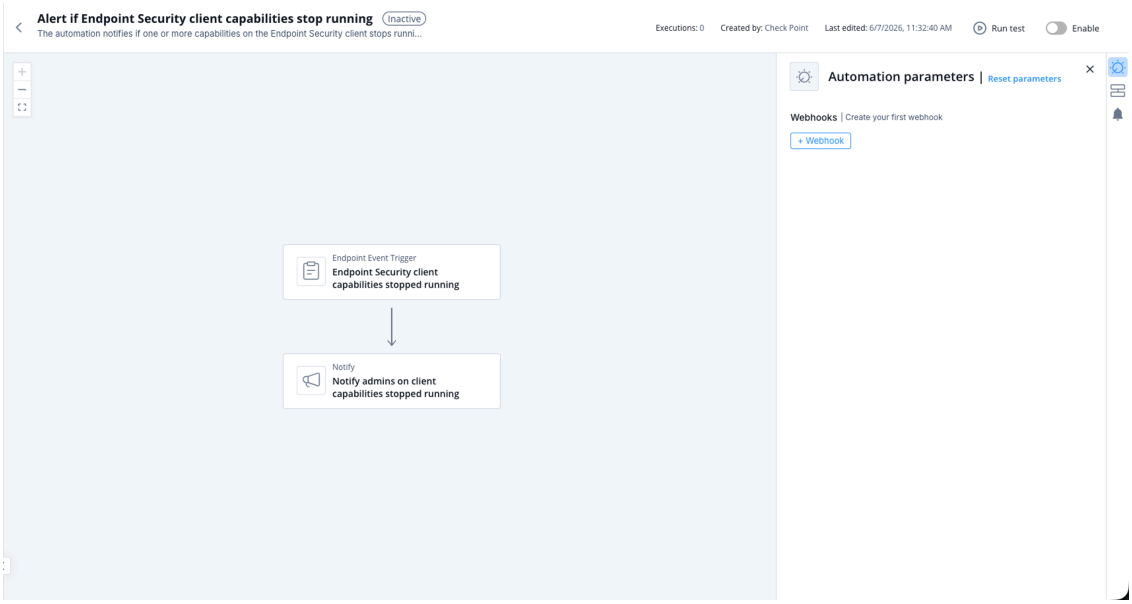
None

Trigger

When Endpoint Security capabilities stop running.

To view the example of this log, click ../running-automation/running-the-automation.dita.

Flow



6.2.101. Add malicious file indicator Identified by CrowdStrike to IOC feed

This topic describes an automation that adds SHA256 hashes of malicious files identified by CrowdStrike to an IOC feed. It helps enhance threat intelligence and security response.

Supported Product

- CrowdStrike
- IoC Management Management

Parameters

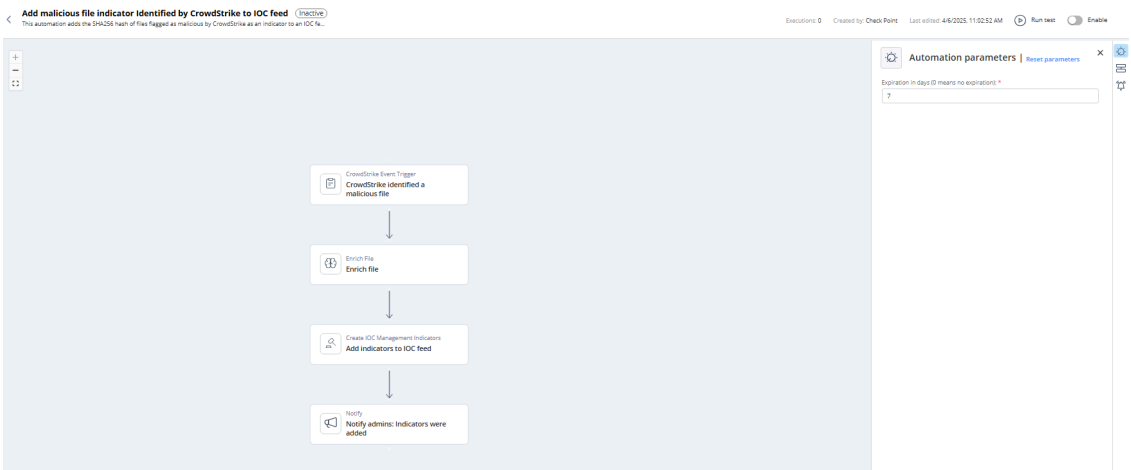
Expiration in days (0 means no expiration)	Set the expiration period for the automation.

Trigger

Malicious file identified by CrowdStrike.

To view the example of this log, click Run.

Flow



6.2.102. Add malicious file indicator Identified by SentinelOne to IOC feed

This topic describes an automation that adds SHA1 hashes of malicious files flagged by SentinelOne to an IOC feed. It updates threat intelligence and can help prevent malicious files from running on devices.

Supported Product

- SentinelOne
- IoC Management Management

Parameters

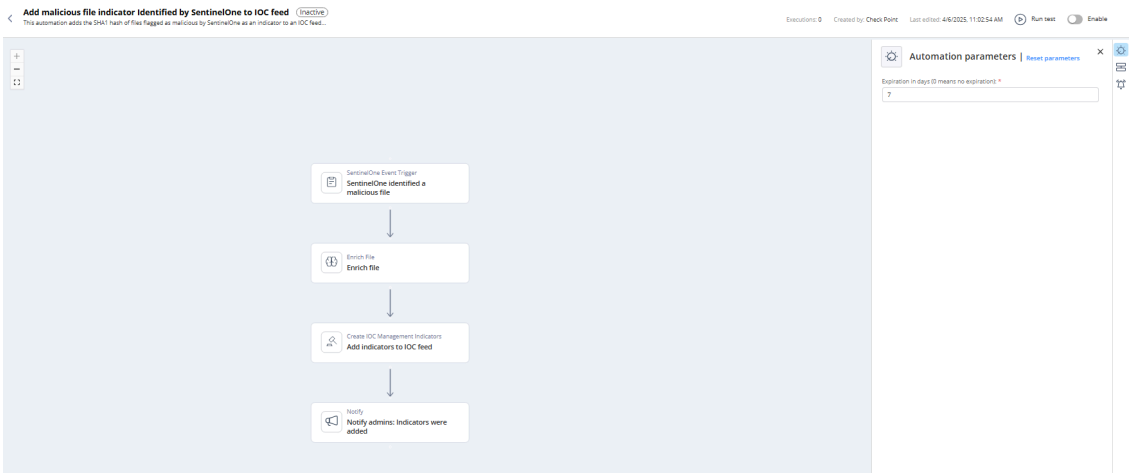
Expiration in days (0 means no expiration)	Set the expiration period for the automation.

Trigger

Infected SentinelOne devices.

To view the example of this log, click Run.

Flow



6.2.103. Add malicious file indicator Identified by Microsoft Defender to IOC feed

This topic describes an automation that adds SHA1 hashes of malicious files detected by Microsoft Defender into an IOC feed. It also adds the source URL to enhance threat intelligence and security response.

Supported Product

- Microsoft Defender
- IoC Management Management

Parameters

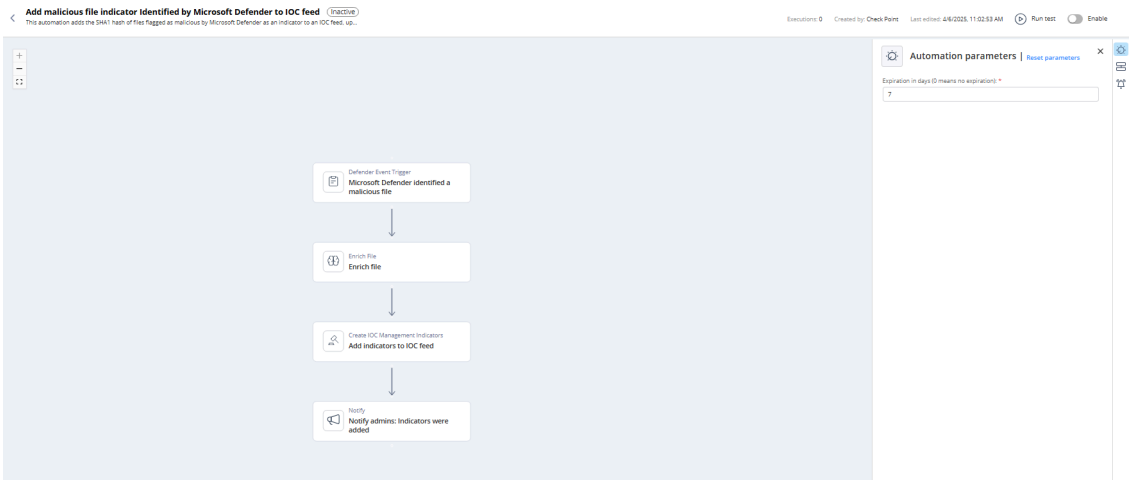
Expiration in days (0 means no expiration)	Set the expiration period for the automation.

Trigger

Infected Microsoft Defender device.

To view the example of this log, click Run.

Flow



6.2.104. Notify on Events & AIOps alert

This topic describes the automation that notifies when Events & AIOps alerts are detected. It outlines the trigger and shows the flow of the notification process.

The automation notifies on Events & AIOps alerts.

Supported Product

Events & AIOps

Parameters

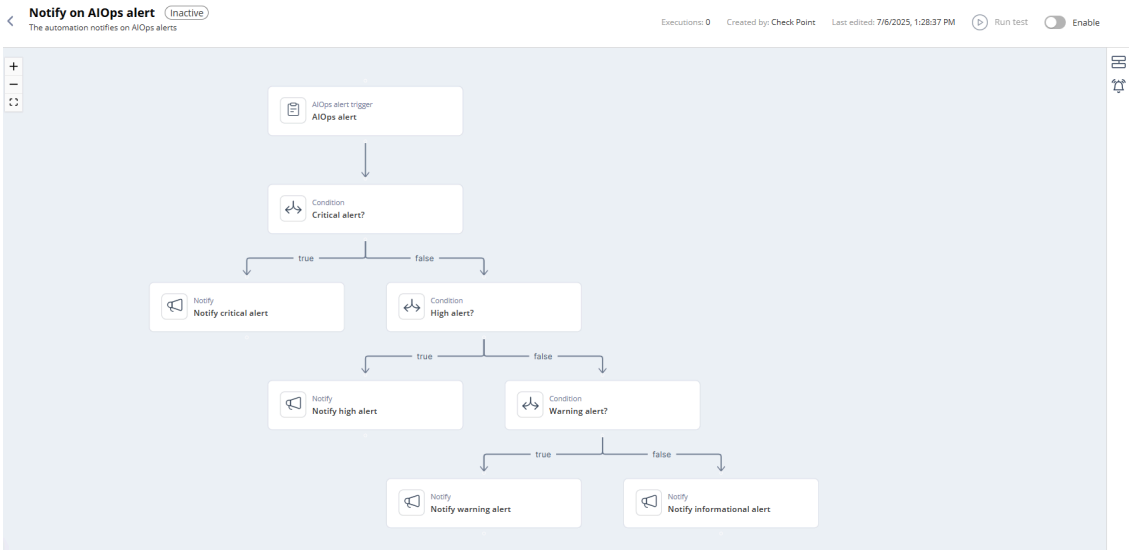
N/A

Trigger

When a critical Events & AIOps alert is detected.

To view the example of this log, click Run *(on page 136)*.

Flow



6.3. Configuring the Automation Parameters

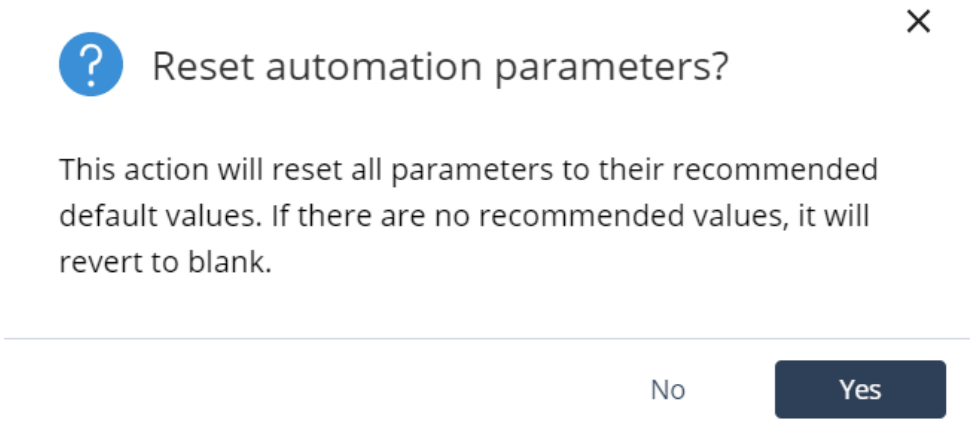
This topic describes how to configure automation parameters in Playblocks and how to reset them to default values.

Procedure:

1. Access **Playblocks** and click **Automations**.
2. Click the automation you want to configure.
3. Configure the parameters *(on page 31)*.
4. To reset parameters to default values.

    a. Click **Reset parameters**

    The **Reset automation parameters** pop-up window appears.



    b. Click **Yes**.

6.4. Running the Automation

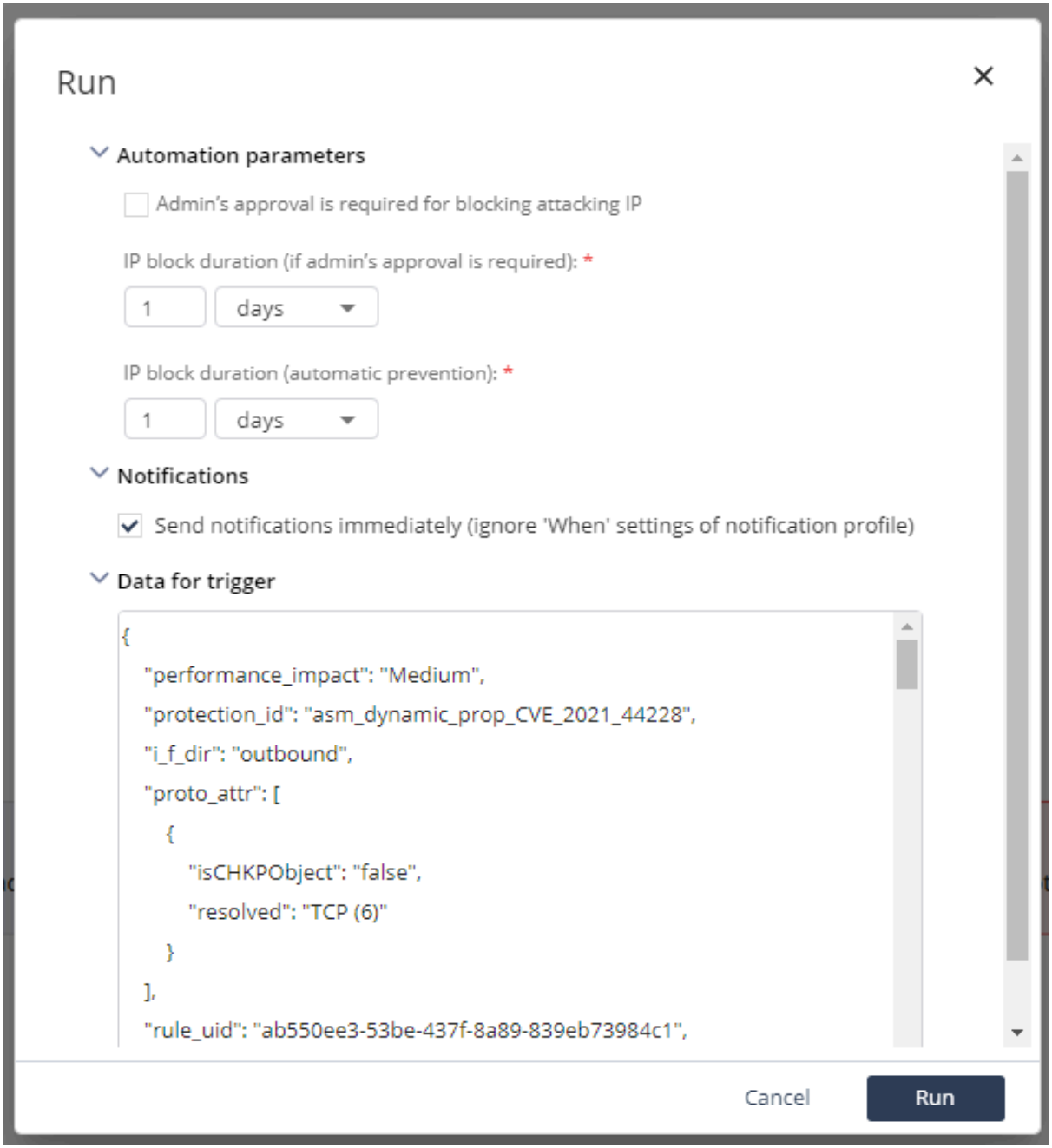
This topic describes how to manually run an automation for evaluation and verification purposes. It provides step-by-step instructions for accessing, configuring, and executing an automation.

About this task:
You can run (execute) the automation manually for evaluation purposes to test and verify the execution.

Procedure:

1. Access **Playblocks** and click **Automations**.
2. Select an automation.
3. Click **Run**.

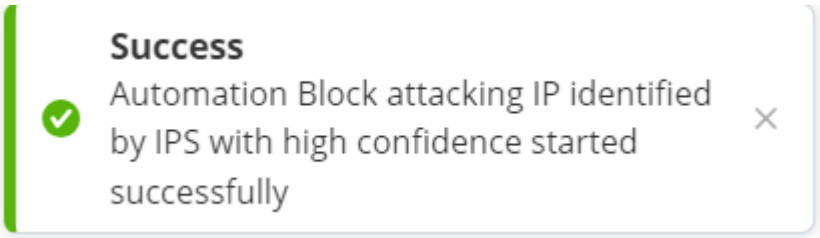
   The **Run** pop-up window appears.



4. Modify the parameters if required.
5. The **Data for trigger** shows the logs recorded after the execution.

   For example, you can edit the log to run the automation for a different IP address. To edit the IP address, go to `"src"` and change the IP address.

6. Click **Run**.
7. If the automation is executed successfully, a **Success** message appears in the top right corner.



6.5. Enabling the Automation

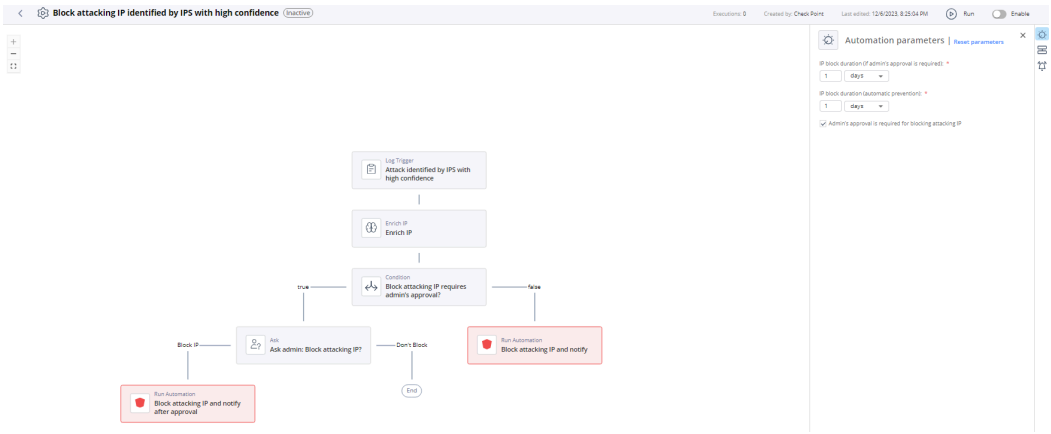
This topic describes how to enable an automation in Playblocks. Automations are enabled by default but can be manually activated.

About this task:
You must enable the automation to execute it. By default, all automations are enabled.

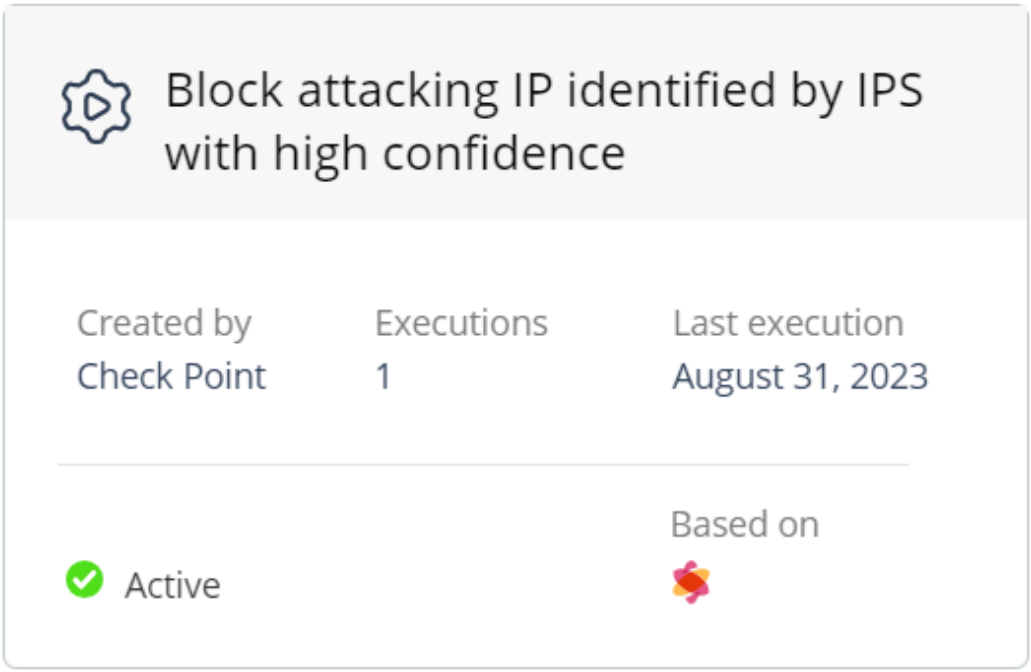
Procedure:

1. Access **Playblocks** and click **Automations**.
2. Select an automation.

3. Turn on the **Enable** toggle button in the upper right corner.



4. After the automation is enabled, the status in the automation card changes to **Active**.



6.6. Approving, Rejecting or Reverting an Automation Execution

This task explains how to approve, reject, or revert an automation execution through communication channels or the Pending Actions page.

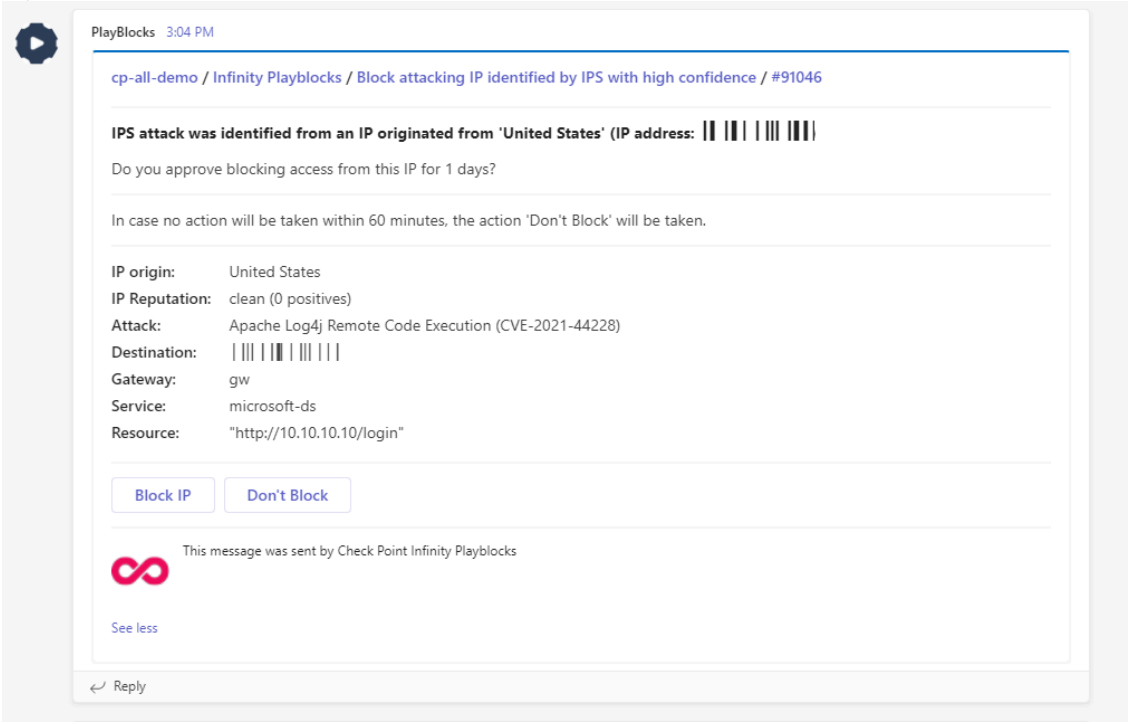
About this task:
If you selected the **Admin's approval is required** checkbox for the automation, then the Administrator's approval is required to approve or reject the execution of the automation. Otherwise, the Administrator can revert an automatically executed automation.

Procedure:

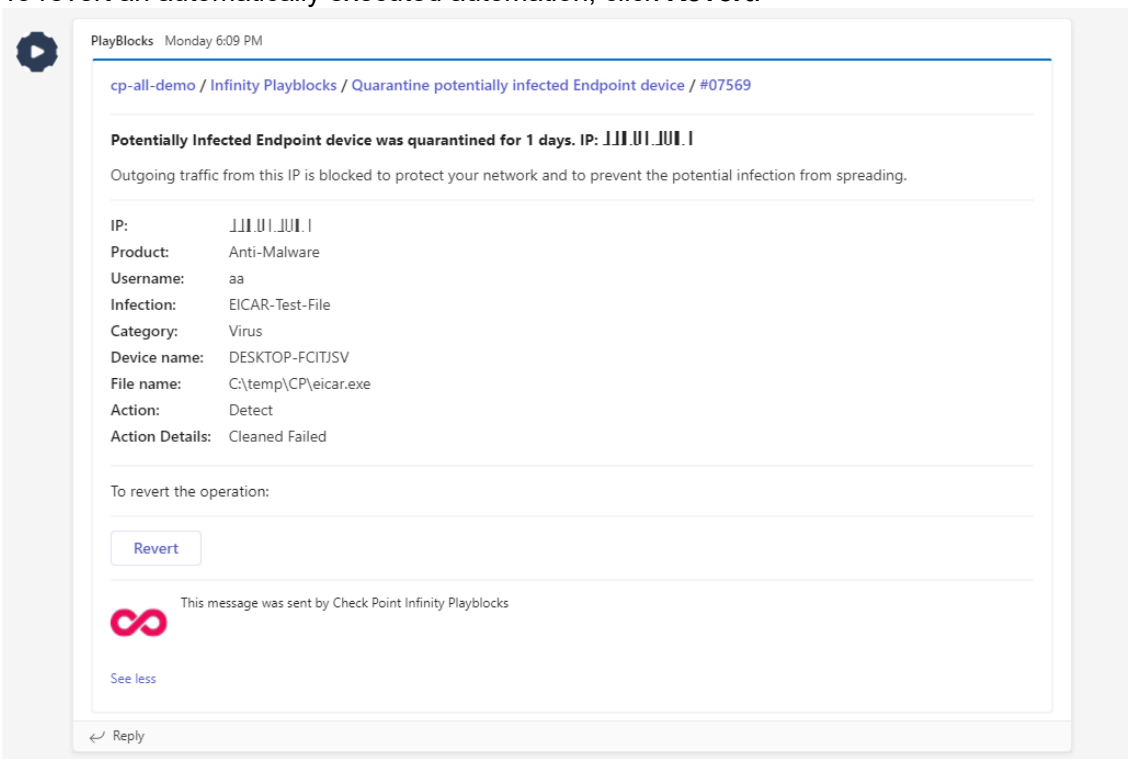
1. To approve, reject or revert an automation execution through a configured communication channel.

    a. Open the notification from the communication channel.

    b. Take the necessary action. For example, click **Block IP** to approve or click **Don't Block** to reject.



    c. To revert an automatically executed automation, click **Revert**.

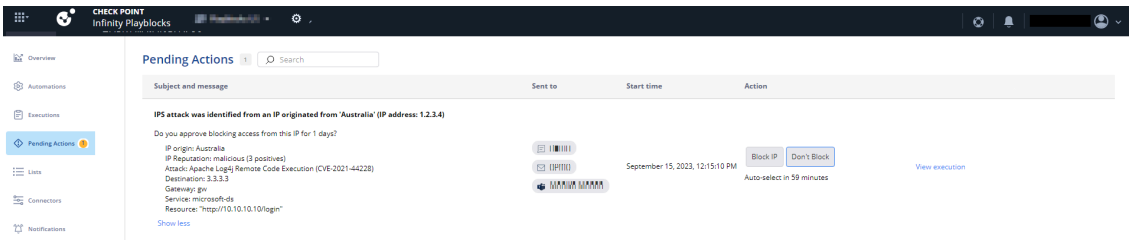


2. To approve or reject an automation execution through the **Pending Actions** page.

    a. Access **Playblocks** and click **Pending Actions**.

    b. Under **Action** column, for example, click **Block IP** to approve or click **Don't Block** to reject.

> **Note:**
>
> You cannot revert an action from the **Pending Actions** page. The Revert action is only possible through connectors such as Microsoft Teams, Outlook, and so on.



6.7. Customization in Playblocks

Playblocks provides flexible customization options to tailor automations according to your organization's needs.

Playblocks provides flexible customization options. These are the primary methods to create or customize automations:

- Creating Automation from Blank *(on page 142)*
- Log Trigger *(on page 143)*
- Schedule Trigger *(on page 147)*
- Managing Trigger *(on page 149)*
- Notifications *(on page 151)*
- Enrichments *(on page 157)*
- Conditions *(on page 159)*
- Actions *(on page 161)*
    - Run Automation *(on page 161)*
    - Add to List *(on page 164)*
    - Create IOC Management Indicators *(on page 165)*
    - API Request *(on page 166)*
    - Isolate Endpoint Device *(on page 177)*
    - Scan Endpoint Security Device *(on page 177)*
    - Terminate Process on Endpoint Security Device *(on page 180)*
    - Delete File on Endpoint Security Device *(on page 182)*
- Exporting/Importing Automation *(on page 184)*

- Cloning Existing Automation *(on page 186)*
- Creating Automation by AI Copilot *(on page)*
- Automation Capabilities *(on page 187)*
- Replace Trigger *(on page 189)*

6.7.1. Creating Automation from Blank

Creating an automation from blank allows you to build fully customized flows from scratch and tailor every step to your specific use case.

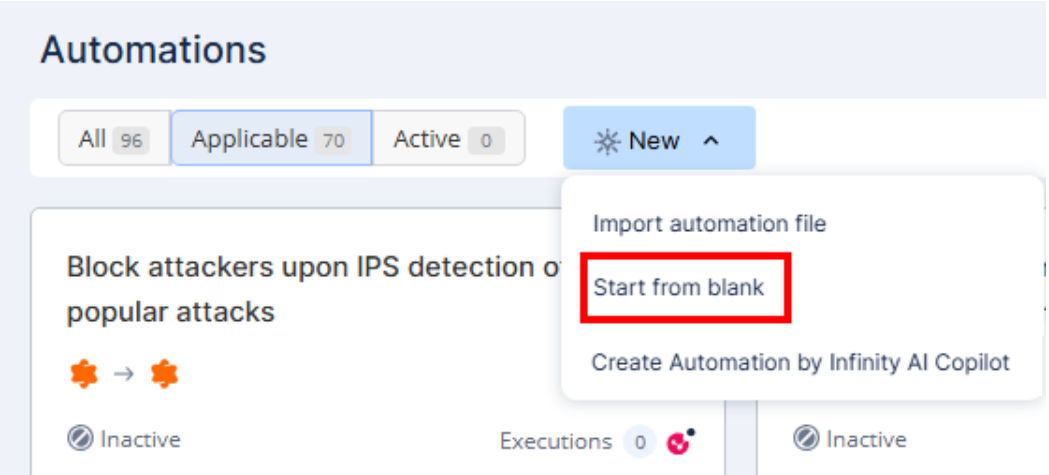
About this task:

Creating an automation from blank allows you to build fully customized flows from scratch, tailoring every step to your specific use case.

To create an automation from blank:

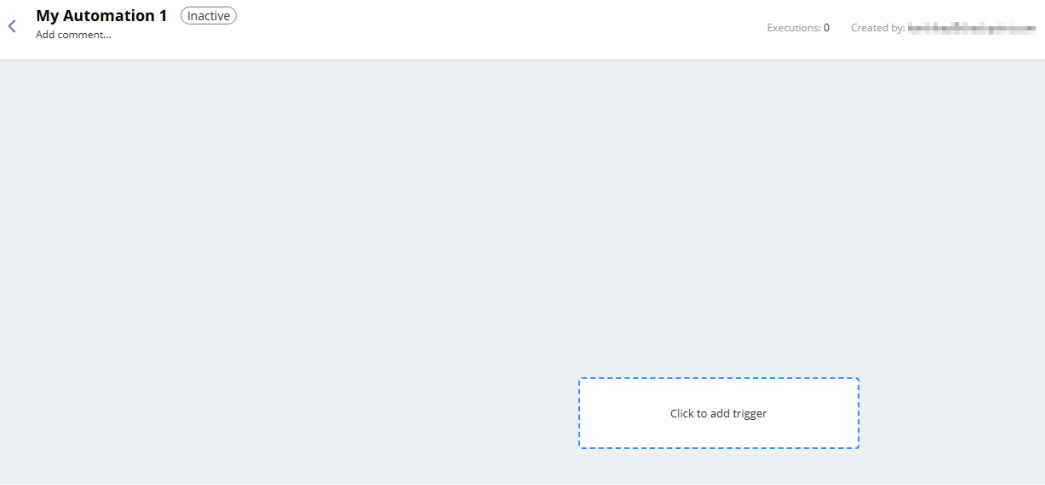
Procedure:

1. Access **Playblocks** and go to **Automations**.
2. Click **New** and select **Start from blank**.

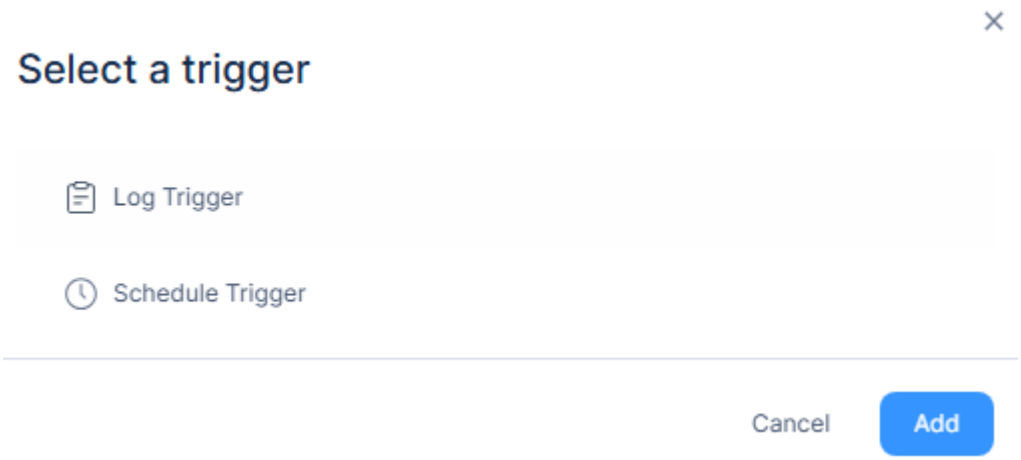


A new automation window appears.

3. Click the box to add a trigger.



4. Select a trigger:
   - **Log Trigger** - To monitor specific log types with optional filters and time intervals. See Log Trigger *(on page 143)*.
   - **Schedule Trigger** - To execute the automation at defined time intervals. See Schedule Trigger *(on page 147)*.



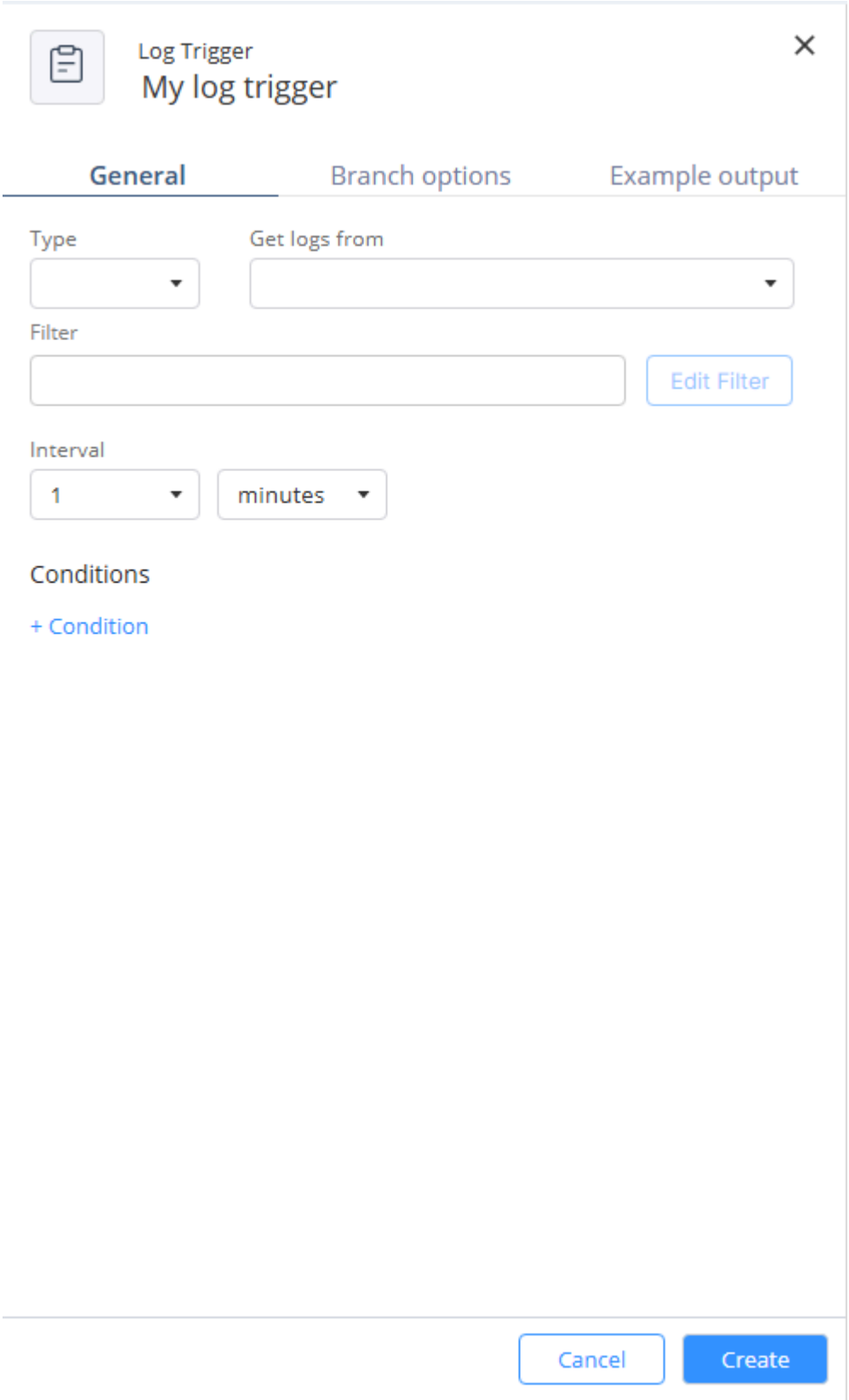
5. Click **Add**.

6.7.2. Log Trigger

Configure a Log Trigger to monitor logs, define conditions, and create example outputs for automation workflows.

About this task:

In the **Log Trigger** window:


Log Trigger
My log trigger
General
Branch options
Example output
Type
Get logs from
Filter
Edit Filter
Interval
1
minutes
Conditions
+ Condition
Cancel
Create

Procedure:

1. In the **General** tab:

   a. From the **Type** list, select the log type:

      - Logs
      - Audit

   Note:

   An additional option **Events** is available if you select **Quantum SD-WAN** as the source product.

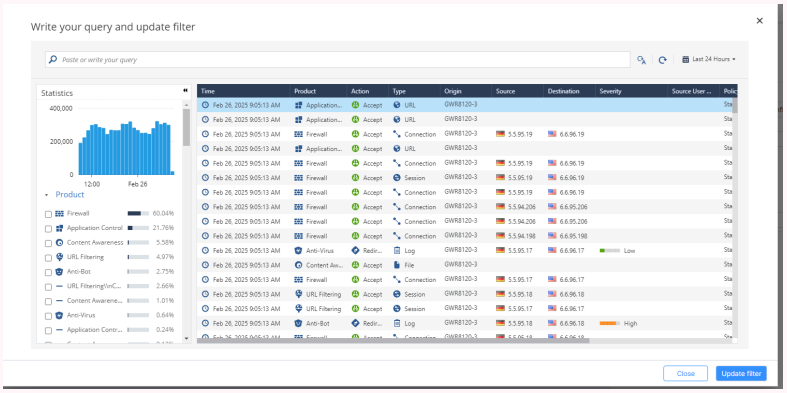
   b. From the **Get logs from** list, select the source product for the logs.

   Note:

   For **Quantum** products, there are two options:

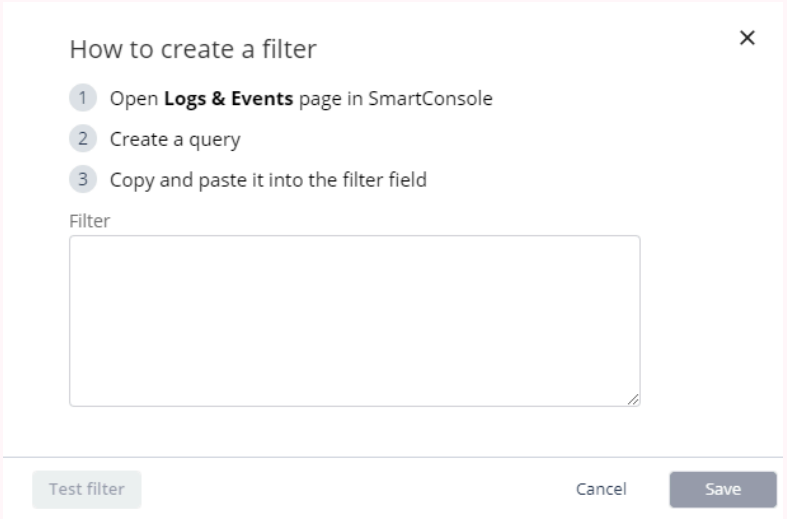
      i. Quantum Management (Check Point Portal)

      Opens the cloud logs view (requires Smart-1 Cloud or Log Sharing).



      ii. Quantum Management (Self-Hosted Log Server)

      Opens a manual input for filter text.



   Additional products that support filter editing via the cloud logs view are:

      - Endpoint Security
      - Email Security

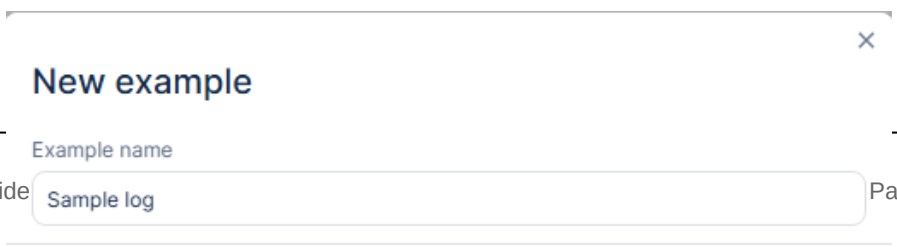
2. In the **Example output** tab:

◦ If logs matching your filter were found in the last 24 hours, the system displays an example log.

◦ Otherwise, you can manually define an example to enable use of log fields:

a. Click **New example**.

b. Enter a name and click **Create**.



3. Click **Create**.

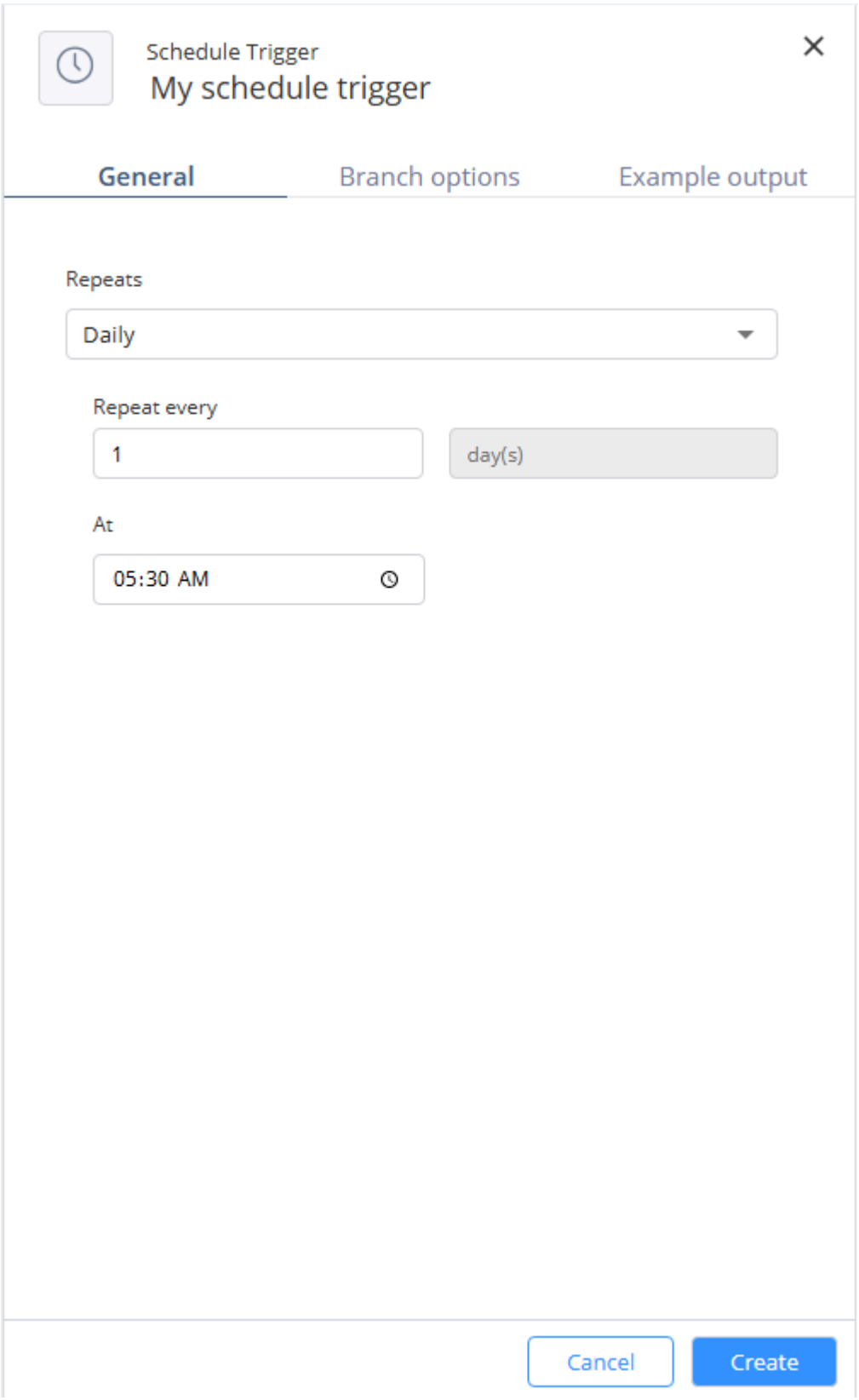
6.7.3. Schedule Trigger

Configure a schedule trigger to run automation at recurring intervals. The task explains how to select the repetition frequency and create the trigger.

About this task:

Schedule Trigger

In the **Schedule Trigger** window:


Schedule Trigger
My schedule trigger
General
Branch options
Example output
Repeats
Daily
Repeat every
1
day(s)
At
05:30 AM
Cancel
Create

Procedure:

1. In the **General** tab, from the **Repeats** list, select the frequency to repeat the trigger to run the automation:
    - **Monthly** - Runs the automation every X months, on specified days.
    - **Weekly** - Runs the automation on selected weekdays, at a specific time.
    - **Daily** - Runs the automation every X days, at a set time.
    - **Hourly** - Runs the automation every X hours.
2. Click **Create**.

6.7.4. Managing Trigger

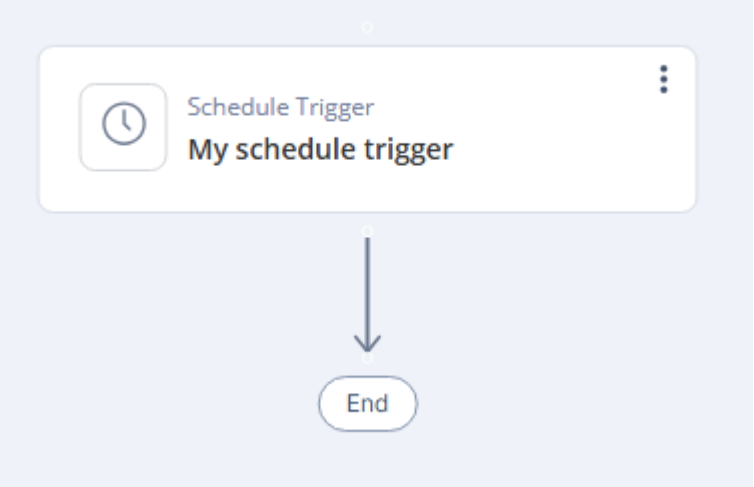
Learn how to manage a trigger by adding notifications, enrichments, conditions, or actions.

About this task:

Managing Trigger

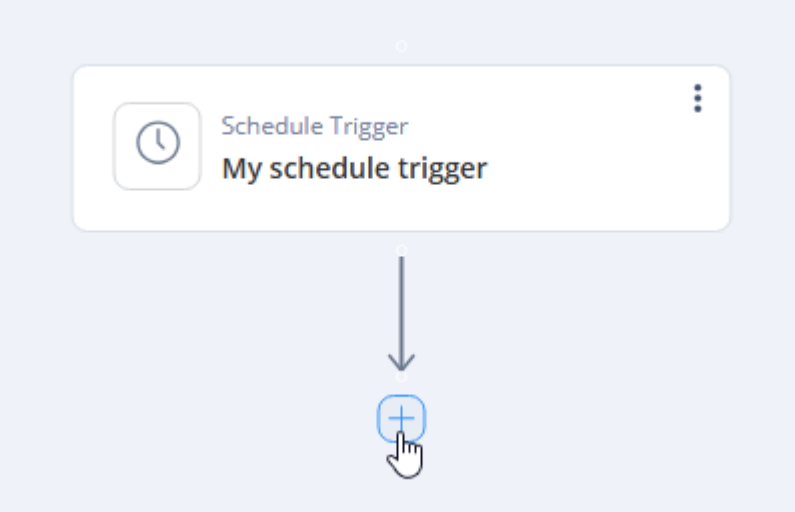
Procedure:

1. Hover over the **End** button in your trigger.

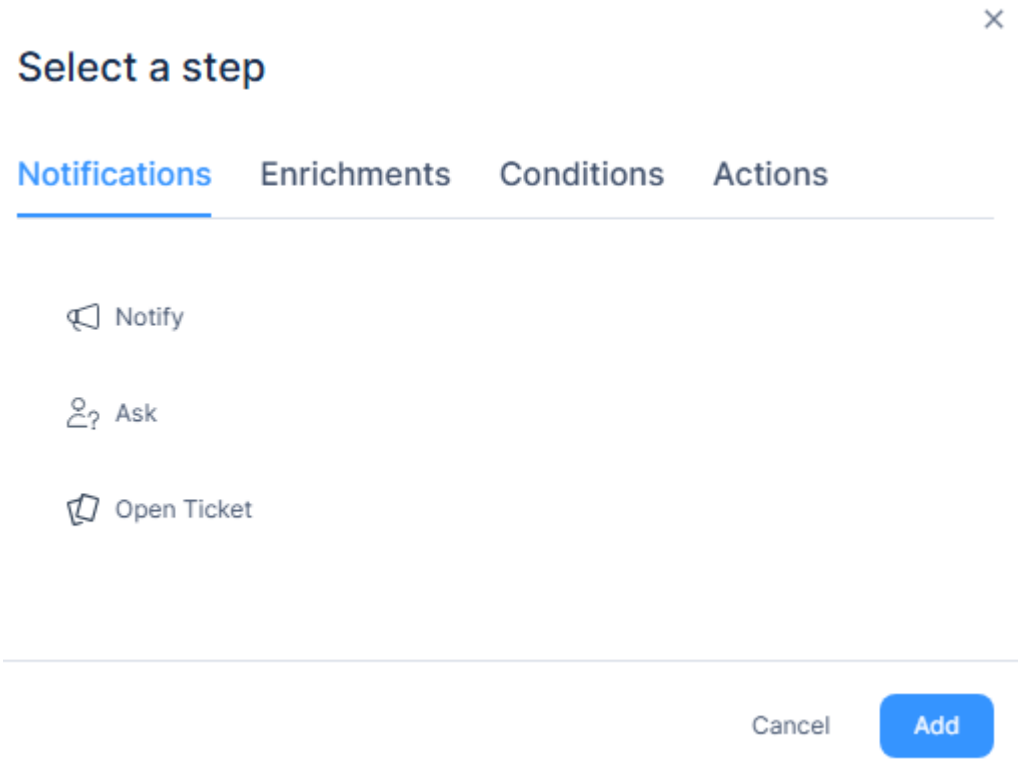


It changes to **+**.

2. Click **+**.



3. Select the required option:
    - Notifications *(on page 151)*
    - Enrichments *(on page 157)*
    - Conditions *(on page 159)*
    - Actions *(on page 161)*



6.7.5. Notifications

Configure notification actions including Notify, Ask, and Open Ticket options. This task explains how to create and customize notification messages and ticket actions.

About this task:

Notifications

In **Notifications**, select one of these:

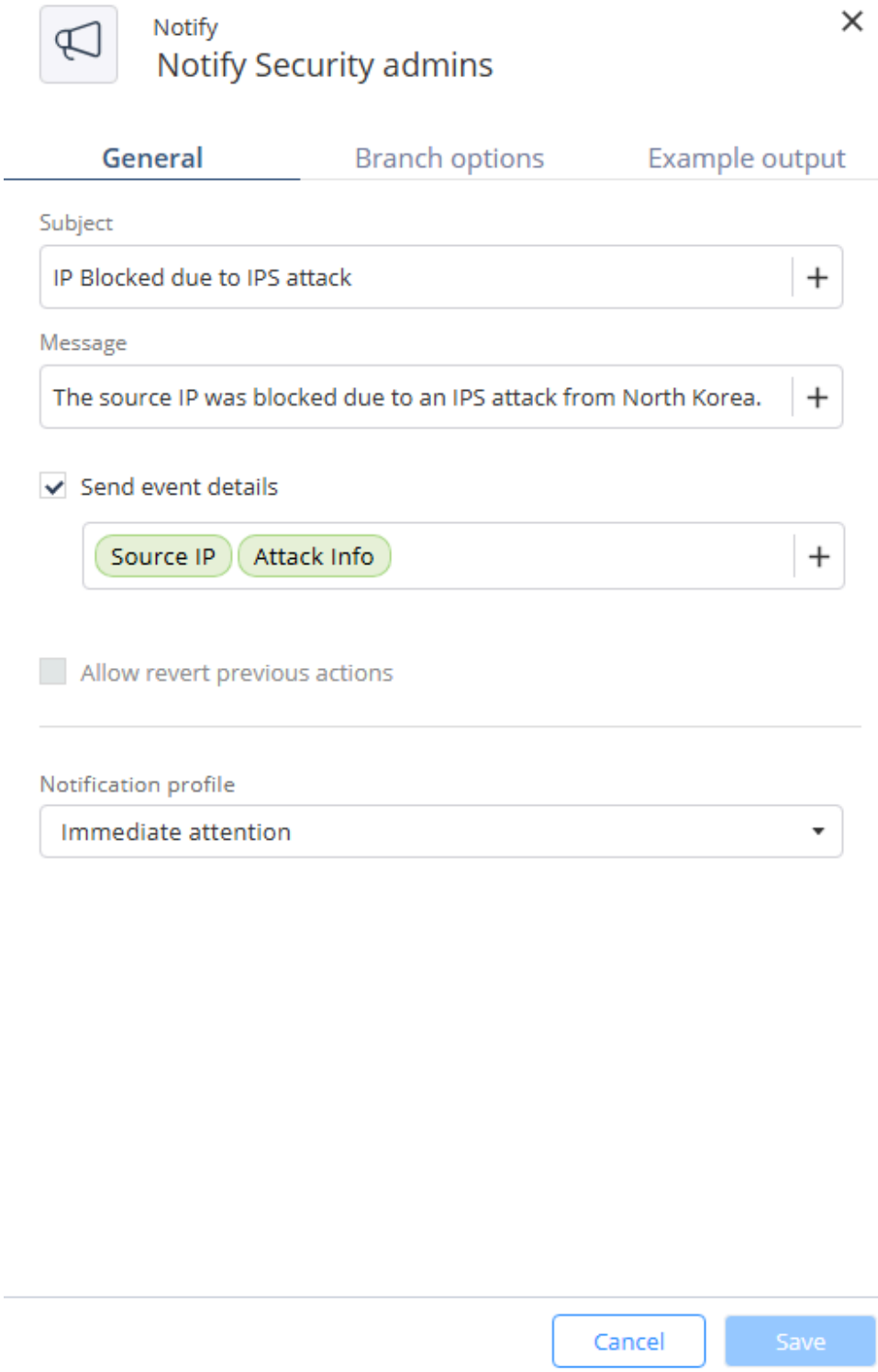
Procedure:

1. **Notify**

   a. To send a notification with customizable subject and message content, select **Notify**.

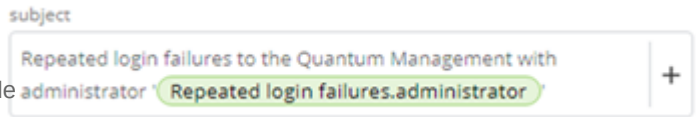
   b. Click **Add**.

   The **Notify** window appears.



   c. Enter these:

      i. **Subject** - Text combined and dynamic values from previous steps or automation parameters.

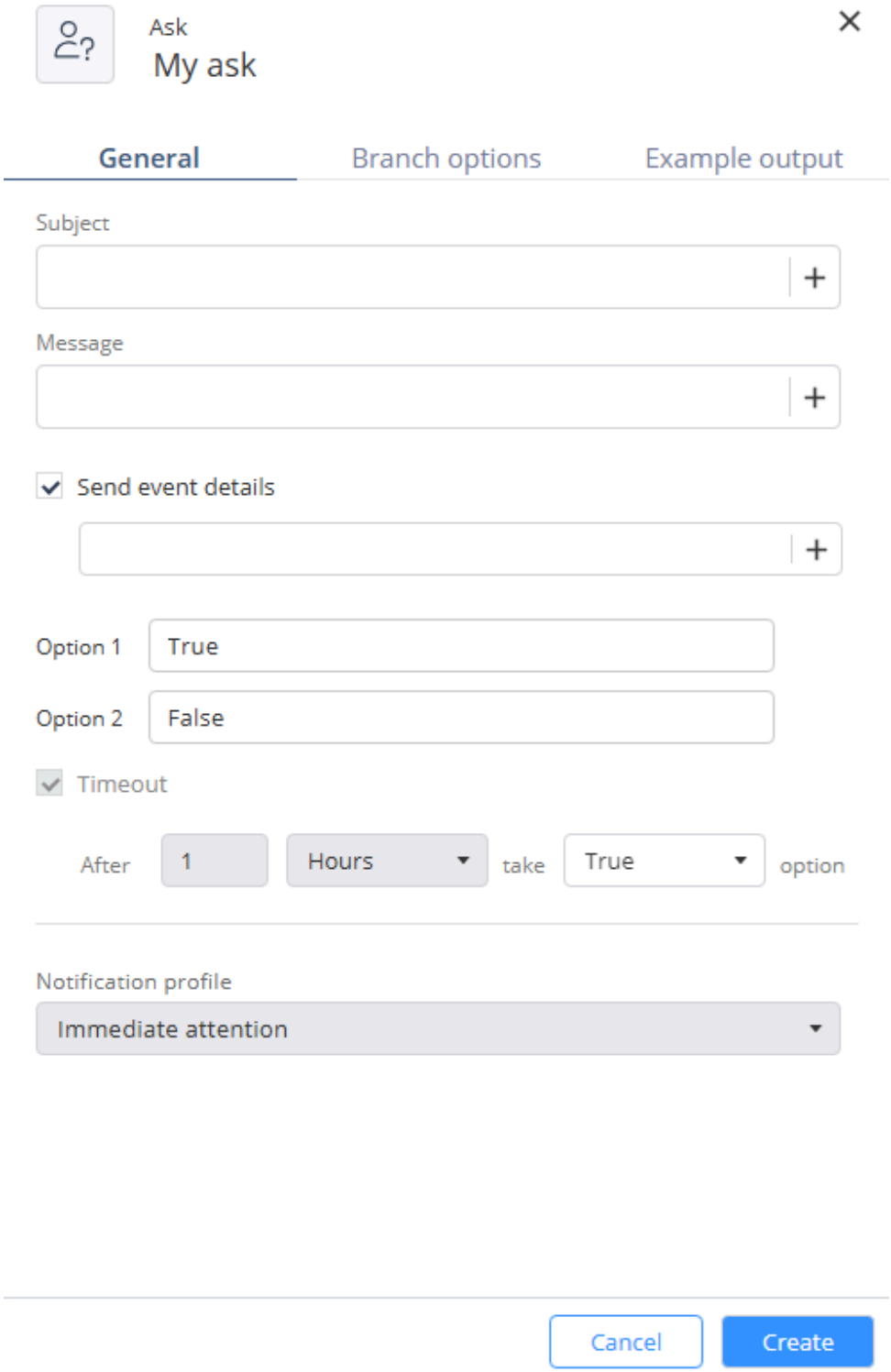


2. **Ask**

   a. To send a customizable message that prompts a user response, select **Ask**.

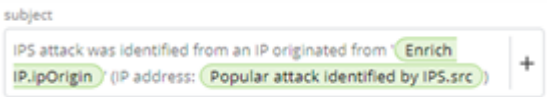
   b. Click **Add**.

   The **Ask** window appears.



   c. Enter these:

      i. **Subject** - Text combined and dynamic values from previous steps or automation parameters.



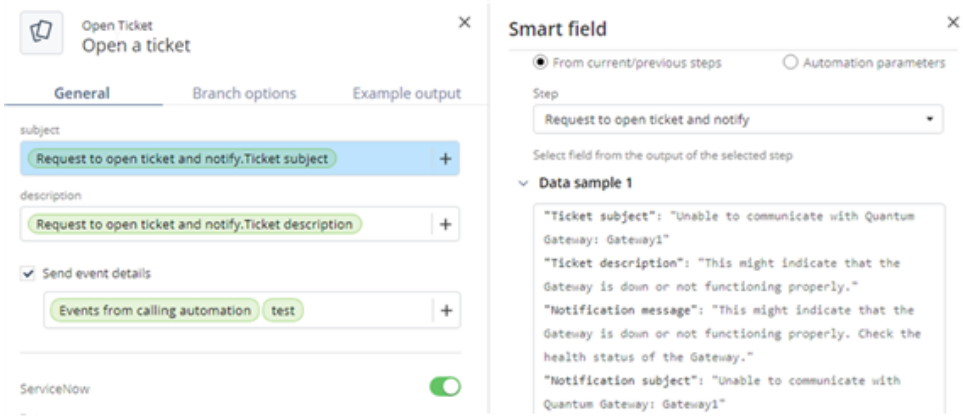
      ii. **Message** - Text combined and dynamic values from previous steps or automation

3. **Open Ticket**

    a. To create a ticket, select **Open Ticket**.

    b. Click **Add**.

    The **Open Ticket** window appears.



    c. Enter these:

        i. **Subject** - Configure the ticket subject, with the option to add fields from the outputs of the current or previous steps and from the automation parameters.

        ii. **Description** - Configure the ticket description, with the option to add fields from the outputs of the current or previous steps and from the automation parameters.

        iii. (Optional) **Send event details** - Choose whether to send event details, and select specific details from the outputs of the current or previous steps, or from the automation parameters.

    d. Click **Create**.

6.7.6. Alert Steps

Alert steps let an automation drive an incident through its full on-call lifecycle in PagerDuty and other alerting platforms behind the same vendor-neutral steps.

The Alert steps let an automation drive an incident through its full on-call lifecycle in PagerDuty (and, in the future, in other alerting platforms behind the same vendor-neutral steps). The Alert steps appear under the **Alerting** tab in the step picker and are available after you configure the PagerDuty connector.

There are five Alert steps:

1. Trigger Alert - Open a new incident.
2. Get Alert - Read the current state of an incident.
3. Acknowledge Alert - Pause escalation on an open incident.
4. Add Note to Alert - Attach a free-text note to an incident.
5. Resolve Alert - Close an incident.

Common Fields

Two fields appear across all five Alert steps and behave the same way.

Provider

Every Alert step has a **Provider** dropdown at the top of its side panel. The Provider field determines which alerting platform receives the request.

Alert ID

The Alert ID is a vendor-neutral identifier that ties Trigger, Acknowledge, Resolve, Get, and Add Note events to the same logical incident.

> **Note:**
>
> Alert IDs are capped at 255 characters.

6.7.6.1. Trigger Alert

The Trigger Alert step opens a new incident in PagerDuty. If an open incident with the same Alert ID already exists, PagerDuty returns the existing incident and does not create a duplicate.

Opens a new incident in PagerDuty. If an open incident with the same Alert ID already exists, PagerDuty returns the existing incident and does not create a duplicate. This makes Trigger Alert safe to call repeatedly for the same source event.

Fields

Provider	See the Common Fields section in Alert Steps.
Summary (required)	Short, one-line description of what happened. PagerDuty displays this as the incident title and across mobile push notifications.
Severity (required)	One of: • **Critical** - System-down, customer-impacting outages. • **Error** - Something broken that needs attention but is not catastrophic. • **Warning** - Degraded behavior worth investigating. • **Info** - Informational. Useful in dashboards but not necessarily paging. Severity determines the notification policy that PagerDuty uses to decide how aggressively to page.
Service (required)	The PagerDuty service that owns the new incident. The dropdown defaults to the service that you selected as the **Default service** on the PagerDuty connector, but you can override it per-step. The Service determines which escalation policy and on-call schedule fire.
Source (optional)	Free-text identifier of where the alert came from (a hostname, an IP, a Check Point Firewall name, an Endpoint device name, and so on). PagerDuty records this for context. It is not used for deduplication.
Alert ID (optional)	See the Common Fields section in Alert Steps.

Description (optional)	Long-form context for the incident. Up to 16,384 characters. PagerDuty forwards the text end-to-end and displays it in the incident body.

6.7.6.2. Get Alert

The Get Alert step reads the current state of an existing incident in PagerDuty.

Reads the current state of an existing incident. Useful when a later step needs to branch on the incident's status. For example, send a "still open" reminder only if the incident is still in the "triggered" state.

Fields

Provider	See the Common Fields section in Alert Steps.
Alert ID (required)	The Alert ID that an earlier Trigger Alert step returns, or a value that you tracked yourself.

6.7.6.3. Acknowledge Alert

The Acknowledge Alert step pauses escalation on an open incident in PagerDuty.

Pauses escalation on an open incident in PagerDuty. After acknowledge, PagerDuty stops paging the on-call rotation as long as the incident stays in the "acknowledged" state.

> **Note:**
>
> The step does not assign the incident to any specific user. PagerDuty records the "From" email that you configured on the PagerDuty connector as the acknowledging actor.

Fields

Provider	See the Common Fields section in Alert Steps.
Alert ID (required)	See the Common Fields section in Alert Steps.

6.7.6.4. Add Note to Alert

The Add Note to Alert step posts a free-text note to an existing incident in PagerDuty.

Posts a free-text note to an existing incident in PagerDuty. Notes appear under the incident's activity log alongside acknowledgments and status changes. Notes are visible to everyone with access to the incident.

Fields

Provider	See the Common Fields section in Alert Steps.
Alert ID (required)	See the Common Fields section in Alert Steps.

Note (required)	The text to post. Up to 16,384 characters.

6.7.6.5. Resolve Alert

The Resolve Alert step closes an incident in PagerDuty.

Closes an incident in PagerDuty. After resolve, PagerDuty stops all escalations and the incident moves to the "resolved" state.

> **Note:**
>
> Resolve is generally the last Alert step in an automation chain.

Fields

Provider	See the Common Fields section in Alert Steps.
Alert ID (required)	See the Common Fields section in Alert Steps.

6.7.7. Enrichments

Use enrichment steps to query the Reputation Service for IP addresses, URLs, or file hashes from previous step outputs. The enrichments provide threat intelligence data about the selected value.

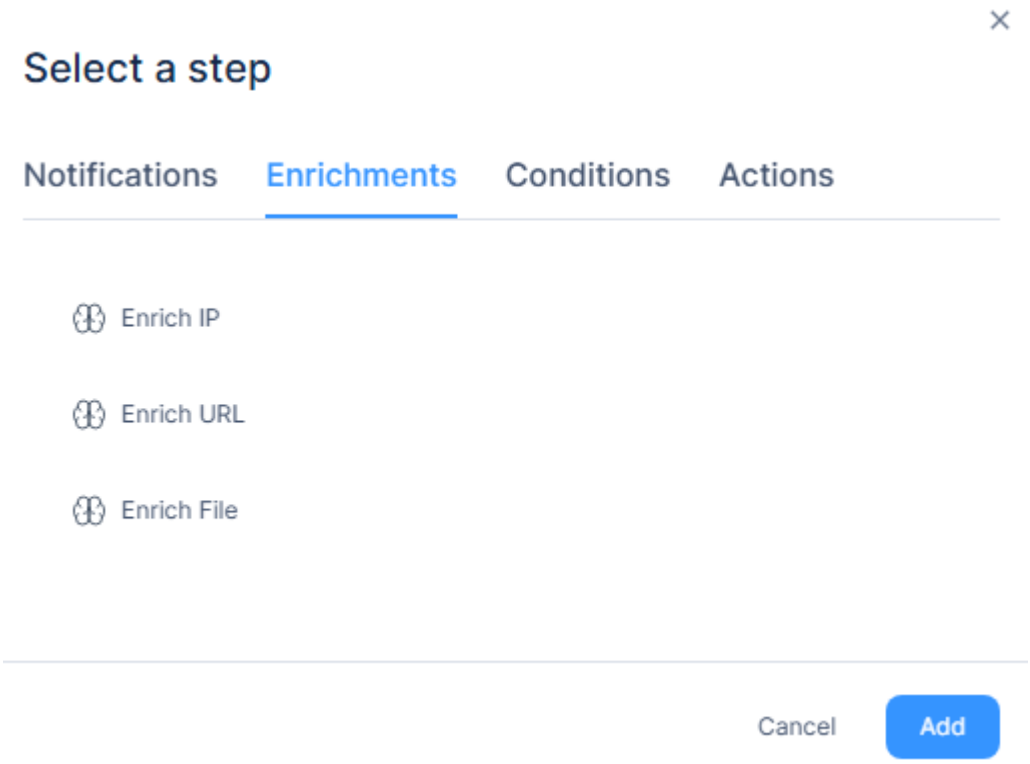
About this task:

Enrichments

Enrichment steps query Check Point Reputation Service to return relevant data for IP addresses, URLs, or file hashes from previous step outputs. Each enrichment provides threat intelligence about the value being checked.

Procedure:

In **Enrichments**, select one of these:

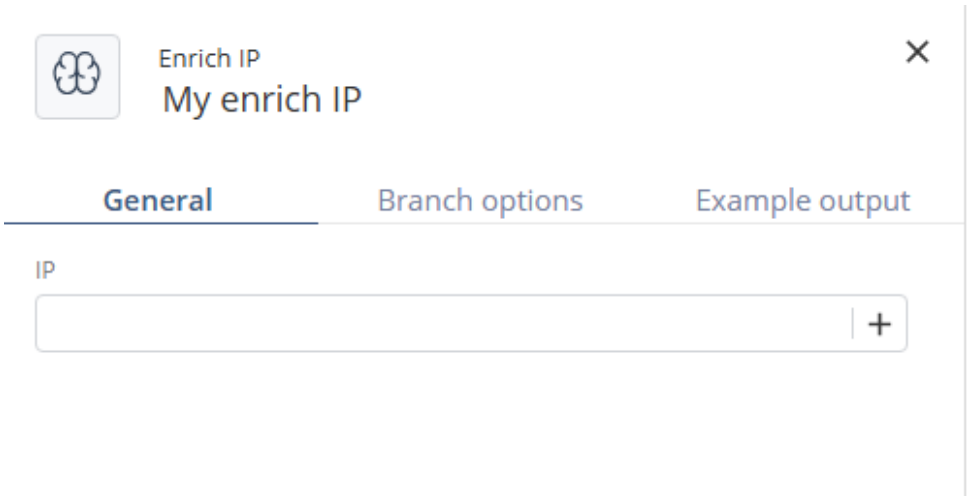


- **Enrich IP**

  a. To return data for an IP address, select **Enrich IP**.

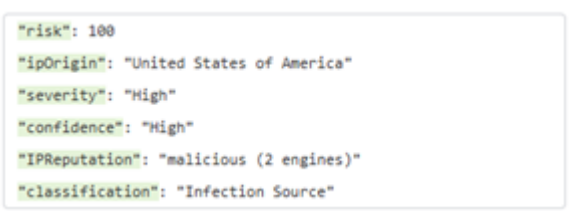
  b. Click **Add**.

  The **Enrich IP** window appears.



  c. Enter an IP address selected from previous steps outputs.

  The system returns the following information:



  d. Click **Create**.

- **Enrich URL**

6.7.8. Conditions

Use conditions to create branches in the automation flow based on logical evaluations. This task explains how to configure condition expressions and operations.

About this task:

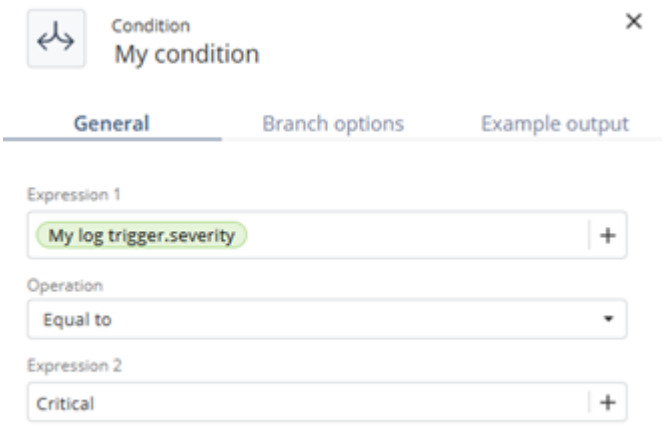
Conditions are used to create branches in the automation flow based on logical evaluations.

Conditions

Procedure:

1. In **Conditions** tab, select **Condition**.
2. Click **Add**.

   The **My Condition** window appears.



3. Specify these:

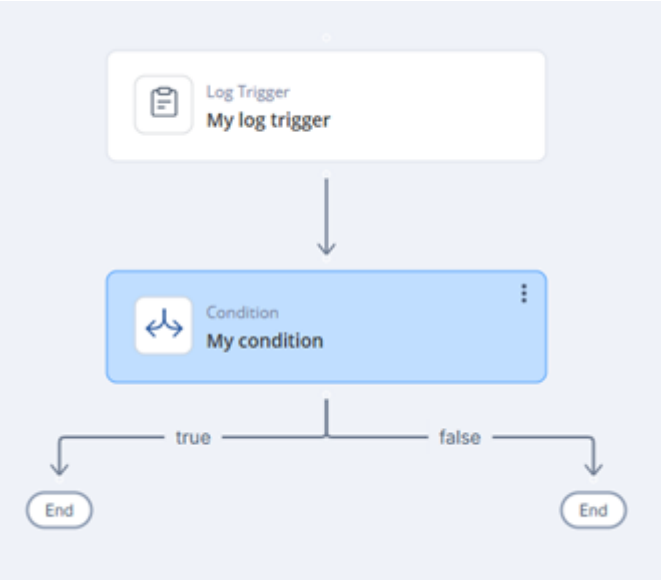
    a. Expression 1

    b. Operation:

        - Equal to
        - Not equal to
        - Greater than
        - Greater than or equal to
        - Less than
        - Less than or equal to

    c. Expression 2

    Both expressions can use static values or outputs from previous steps. Define what happens when the condition is met or not met.



6.7.9. Actions

Action steps perform operational tasks such as running automations, managing indicators, and sending external API requests.

Actions

Action steps perform operations such as running predefined automations, adding indicators to lists, creating IoC Management indicators, or sending external API requests.

6.7.10. Run Automation

Run an automation action and configure automation parameters and inputs for supported automation types.

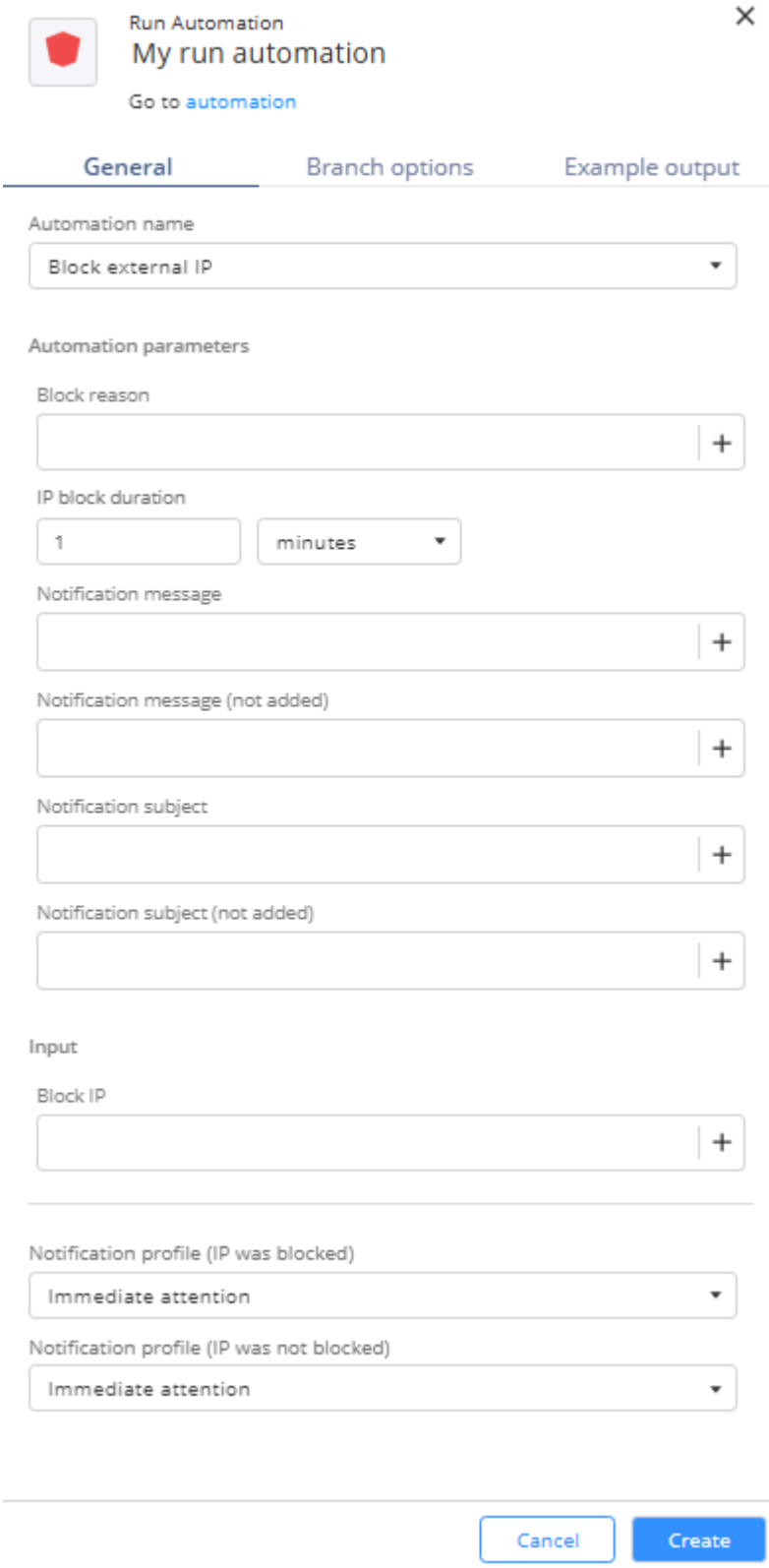
About this task:

Run Automation

Procedure:

1. In **Actions** tab, select **Run Automation**.
2. Click **Add**.

   The **Run Automation** window appears.



3. In the **General** tab, from the **Automation name** list, select one of these and specify the automation parameters and Input:
    - Block External IP:
        - Block reason
        - IP block duration
        - Notification message
        - Notification message (not added)
        - Notification subject
        - Notification subject (not added)
        - Block IP
        - Notification profile (IP was blocked)
        - Notification profile (IP was not blocked)
    - Quarantine Internal IP
        - Quarantine reason
        - IP quarantine duration
        - Notification message
        - Notification message (not added)
        - Notification subject
        - Notification subject (not added)
        - Open ticket if device IP was quarantined
        - Quarantine IP
        - Notification profile (Device IP was quarantined)
        - Notification profile (Device IP was not quarantined)
    - Open ticket and notify
        - Open ticket
        - ServiceNow ticket type
        - Jira ticket type
        - Notification subject
        - Notification message
        - Ticket subject
        - Ticket description
        - Notification profile
    - Isolate endpoint device
        - Device isolation duration
        - Notification subject

4. Click **Create**.

6.7.11. Add to List

Use the Add to List procedure to add IPs, URLs, domains, or hashes to a list with optional conditions and duration settings.

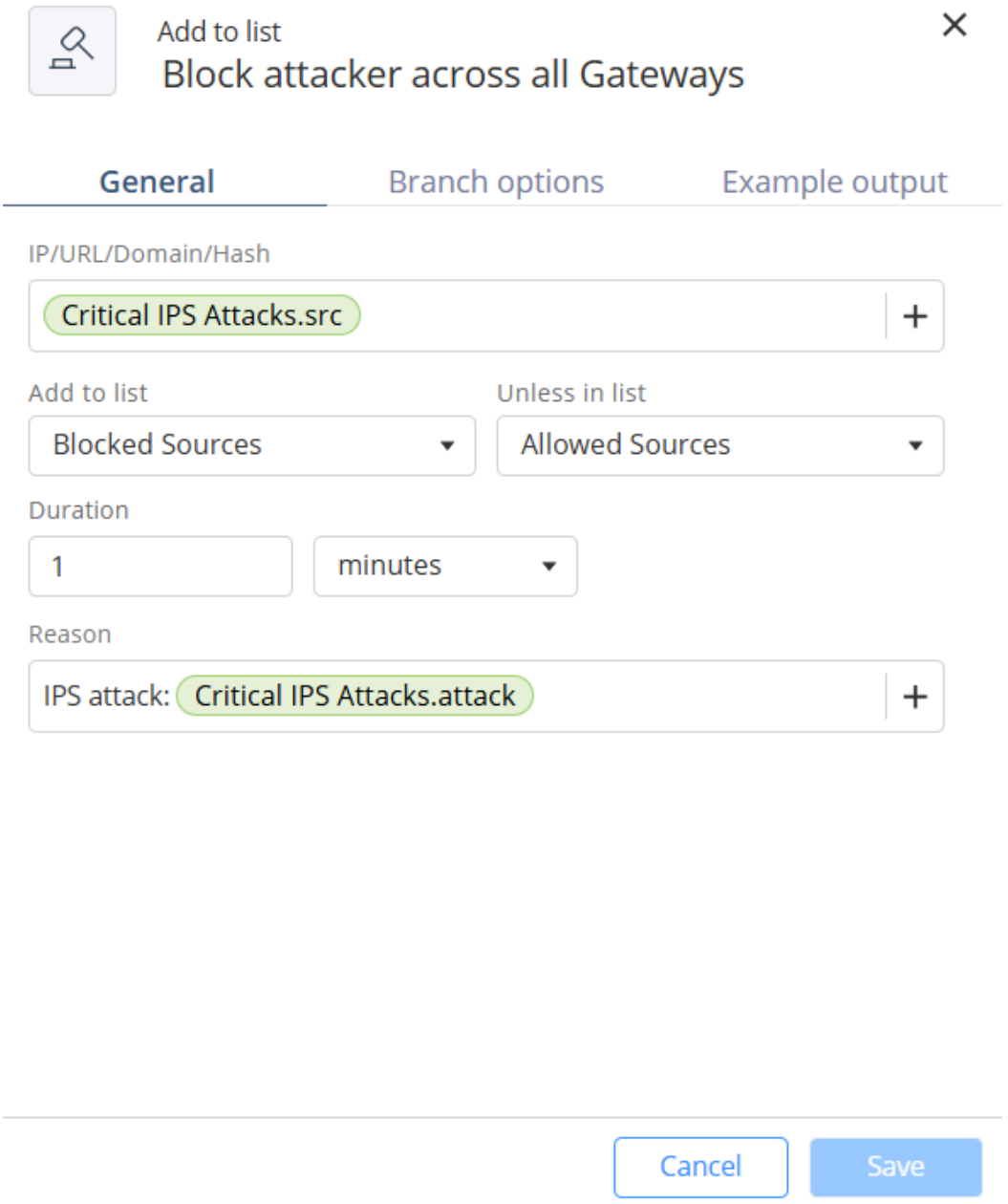
About this task:

Add to List

Procedure:

1. Select **Add to list** and then click **Add**.

   The **Add to list** window appears.



2. Specify these:
   a. IP/URL/Domain/Hash - A value of type IP, URL, Domain, or Hash from the outputs of previous steps.
   b. Add to list
   c. Unless in list
   d. Duration
   e. Reason

3. Click **Create**.

6.7.12. Create IoC Management Indicators

Create IoC Management indicators by specifying indicator values and expiration settings in the Create IoC Management Indicators window.

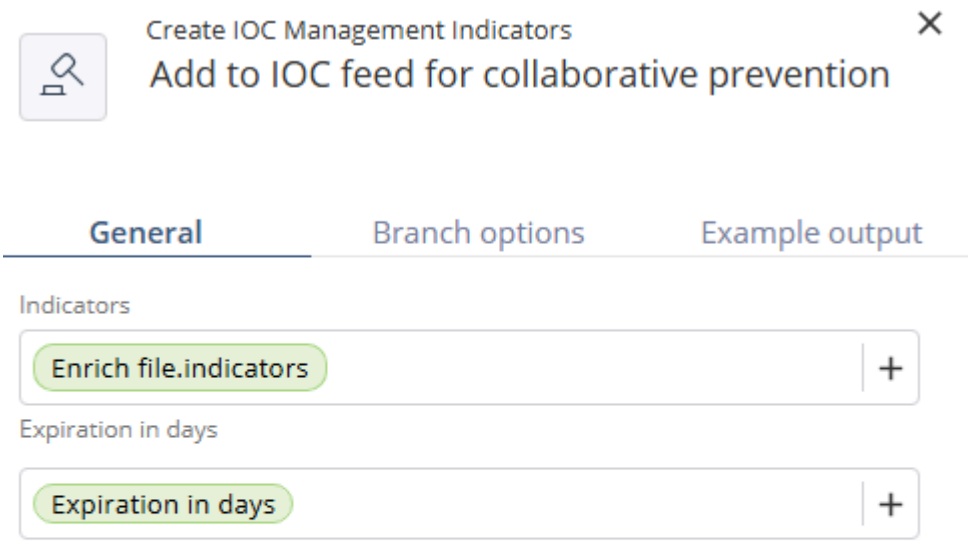
About this task:

Create IoC Management Indicators

Procedure:

1. Select **Create IoC Management Indicators** and then click **Add**.

   The **Create IoC Management Indicators** window appears.



2. Specify these:
   a. Indicators
   b. Expiration in days

3. Click **Create**.

6.7.13. API Request

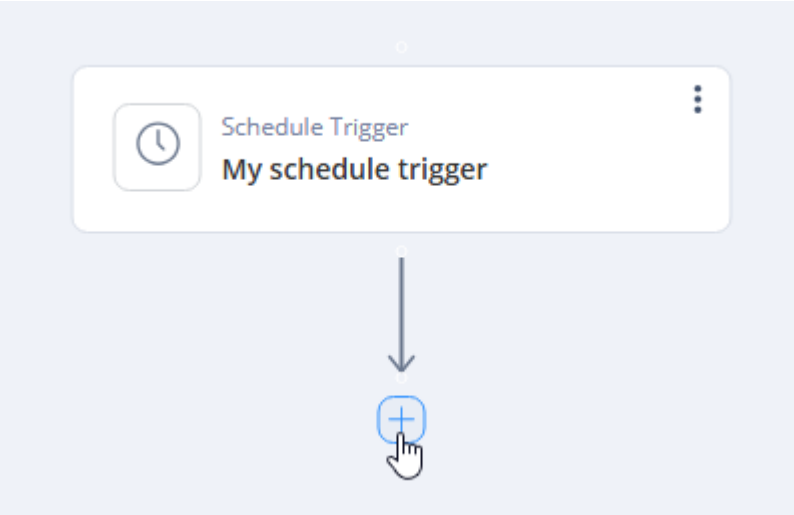
Configure an API Request action in an automation and define the example output structure for API responses.

About this task:

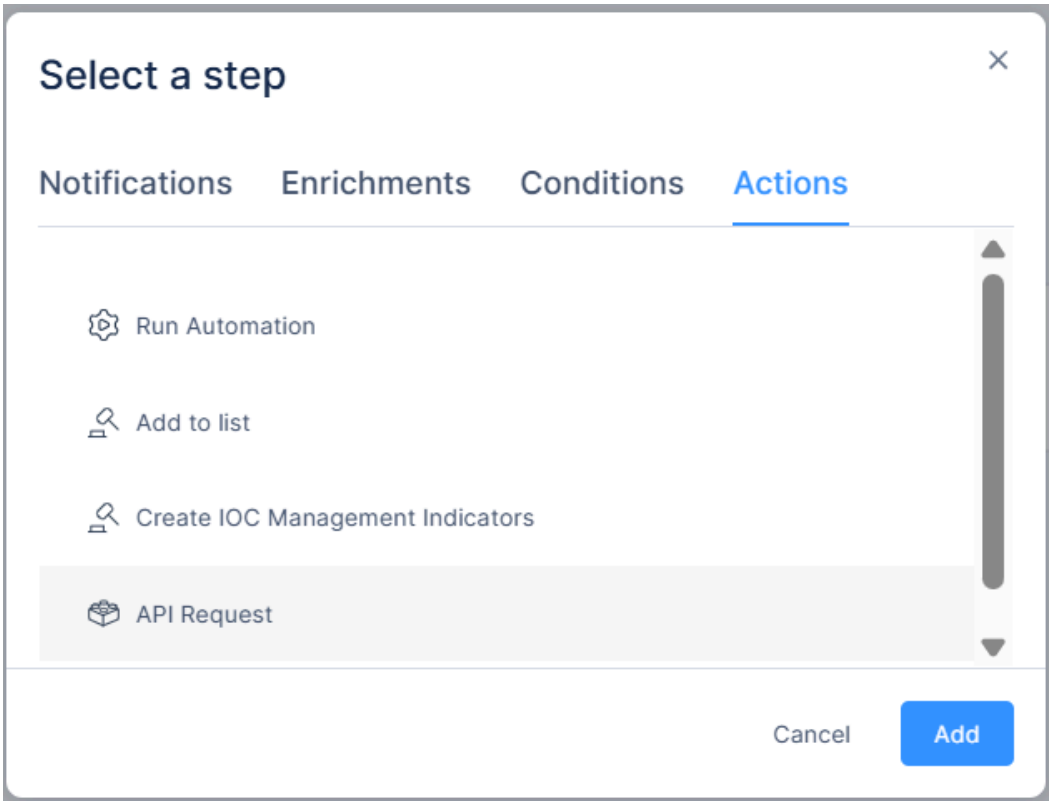
API Request

Procedure:

1. Access **Playblocks** and go to **Automations**.
2. Open your **Automation** and click **+**.

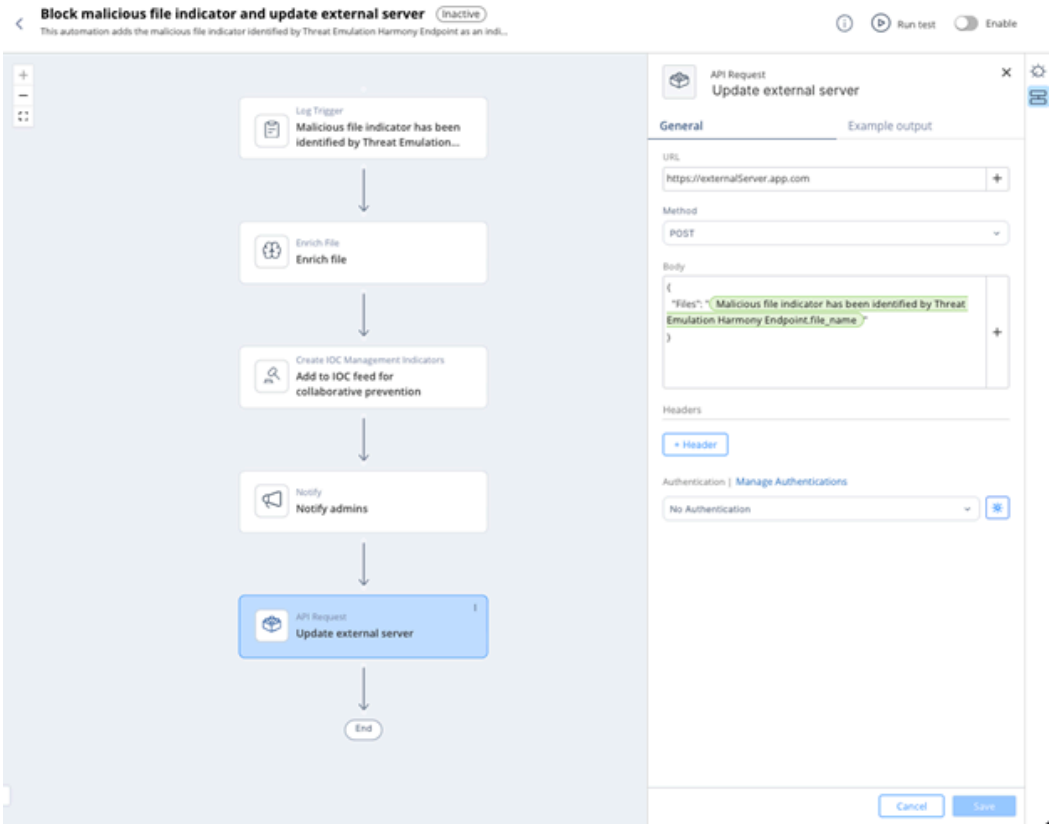


3. Select **Actions** > **API Request**.

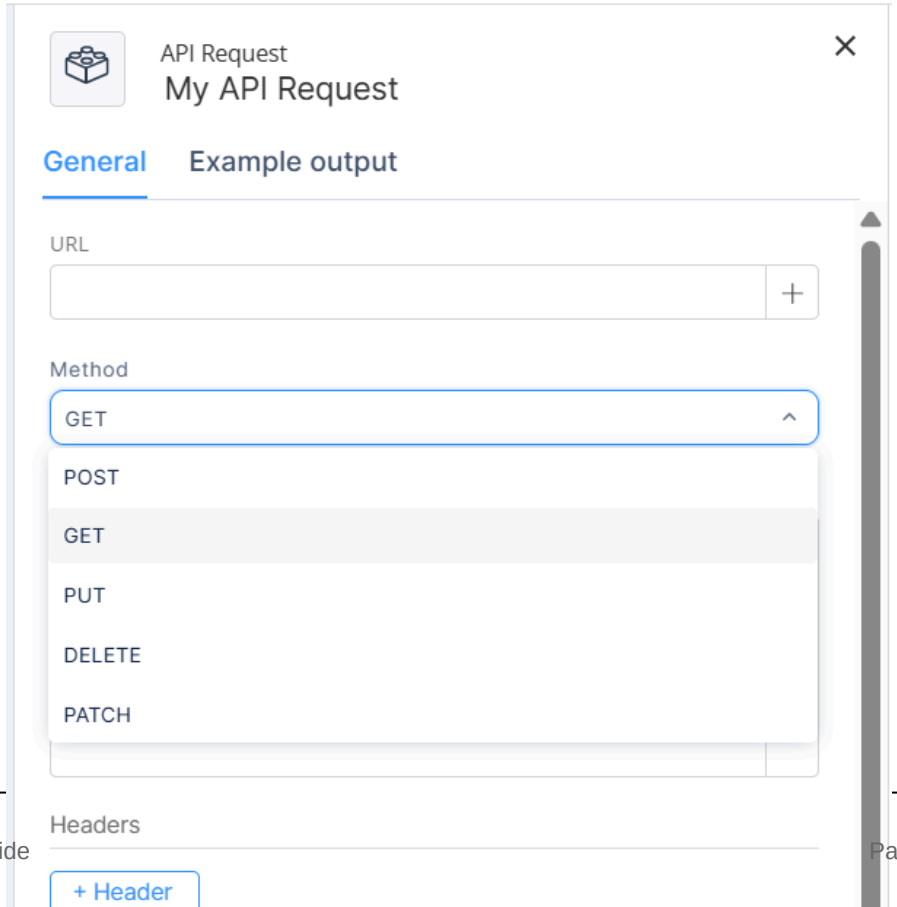


4. Click **Add**.

5. Fill these parameters.



- **URL**: The HTTPS endpoint for the request.
- **Method**: The HTTP method for the request. Supported methods:
  - POST
  - GET
  - PUT
  - DELETE
  - PATCH



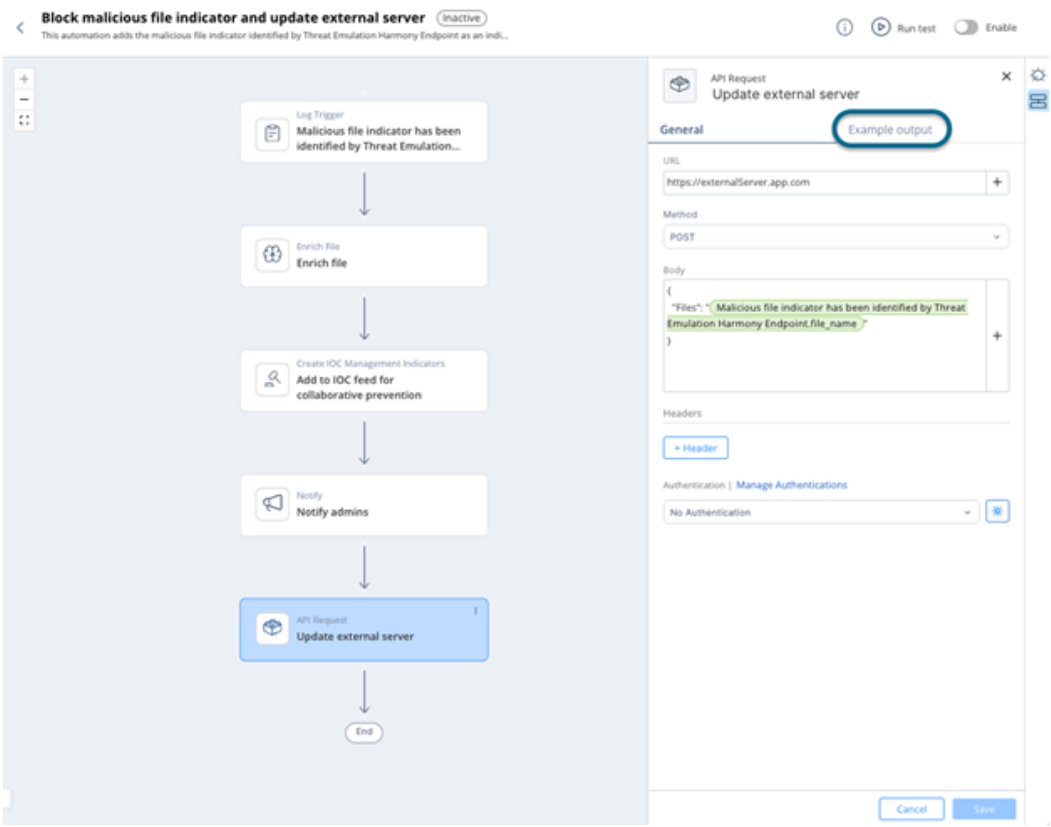
6. Define the example output for the API response.

   Example Output

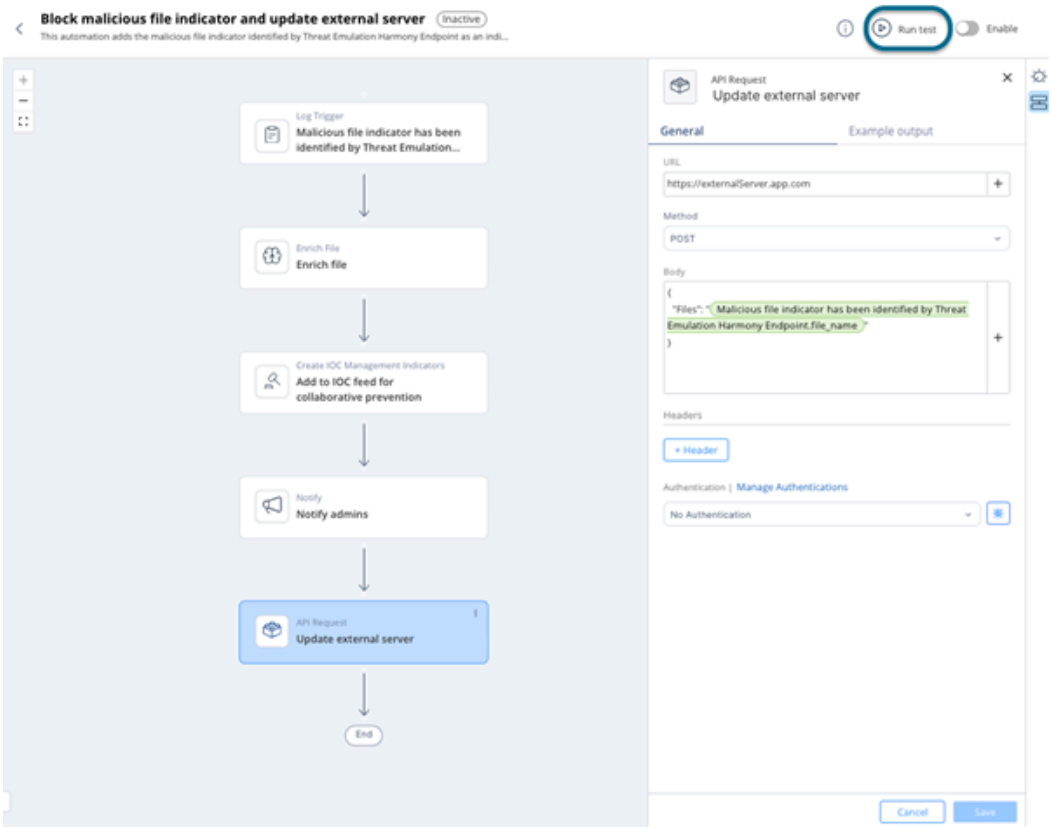
   The example output defines the required structure for the step's result, which is the response returned by the API request.

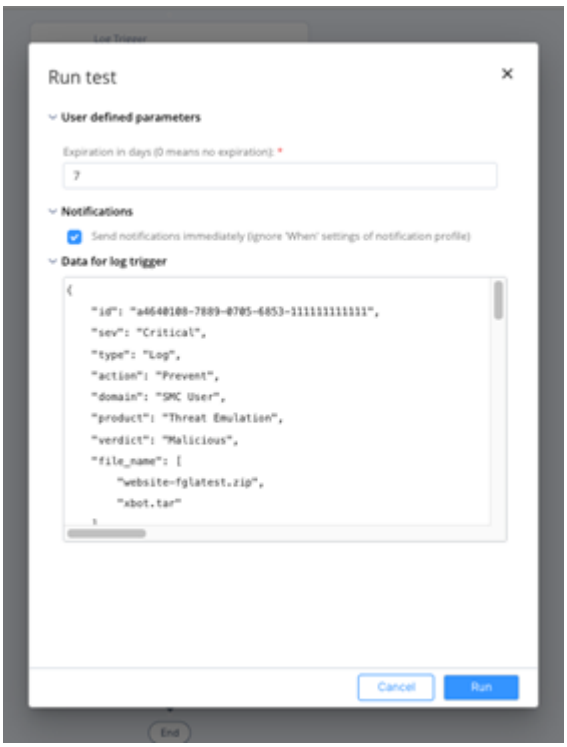
   Example output from the actual output of that step during execution:

7. Click **Example output**.



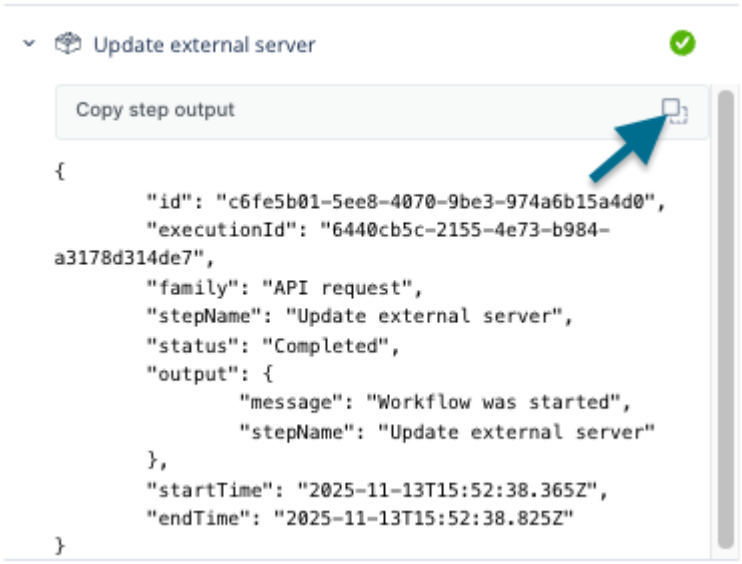
8. Run the automation manually using the **Run Test** button at the top of the automation page.





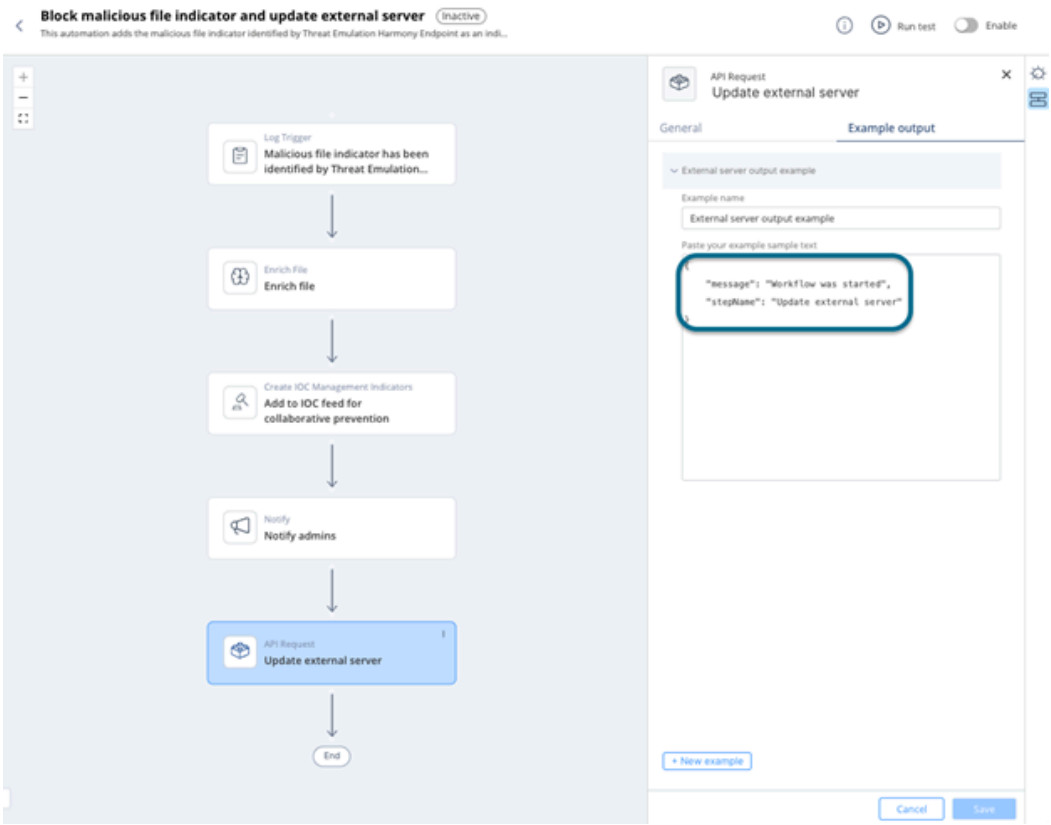
Run test popup appears

9. Copy the output of the API Request step.



Note: You can also copy this output from the **Executions** page.

10. Paste the output into the **Example Output**.



11. Click **Save**.

6.7.14. AI Request

Use the AI Request step to send a prompt to a connected AI provider and use the model's response in subsequent steps.

About this task:

Use the **AI Request** step to send a prompt to a connected AI provider and use the model's response in subsequent steps.

Before you add this step, connect at least one AI provider on the **Connectors** page. See ../ai-connectors/ai-connectors.dita.

To add an AI Request step:

Procedure:

1. Access **Playblocks** and go to **Automations**.
2. Open your automation and click **+** to add a new step.
3. Select **Actions** > **AI Request**.
4. Click **Add**.

   The **AI Request** window appears.

5. Enter these parameters:

    - **Provider** - The AI vendor to call. Only providers with a connected connector are selectable. Supported providers:

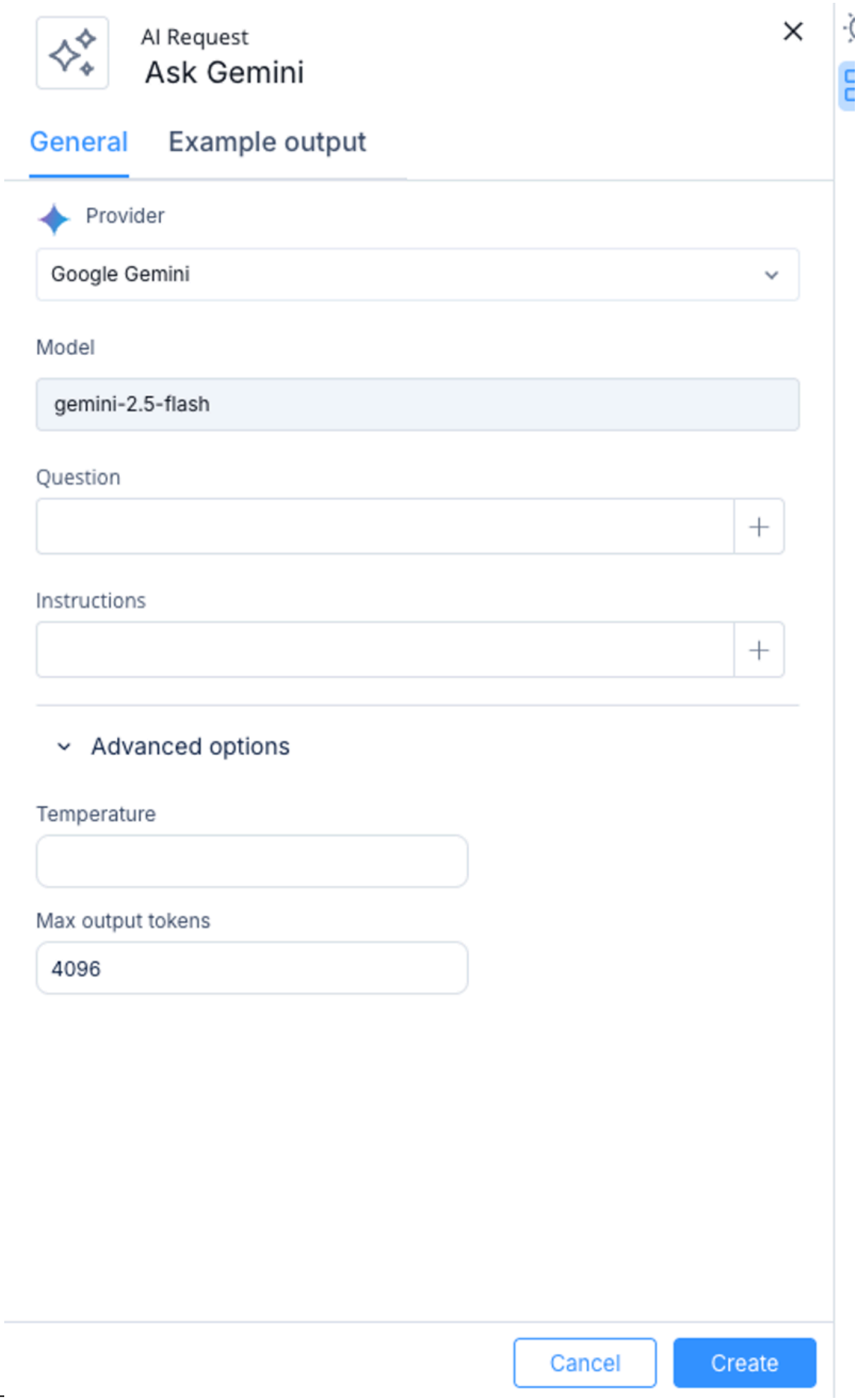
        - OpenAI
        - Google Gemini
        - Anthropic Claude

      If you do not connect a provider, an error directs you to the **Connectors** page.

    - **Model** - Read-only. Shows the model selected on the provider's connector. To change it, open the provider on the **Connectors** page and update the **Model** selection.
    - **Question** - The prompt to send to the model. Supports values from the outputs of previous steps.
    - **Instructions** - The system prompt that tells the model how to behave (role, format, constraints). Supports values from the outputs of previous steps.
    - **Advanced options** (optional):

        - **Temperature** - Controls response randomness. Value between 0 and 2. Lower values produce more deterministic output.
        - **Max output tokens** - Caps the response length. Integer between 1 and 128000.

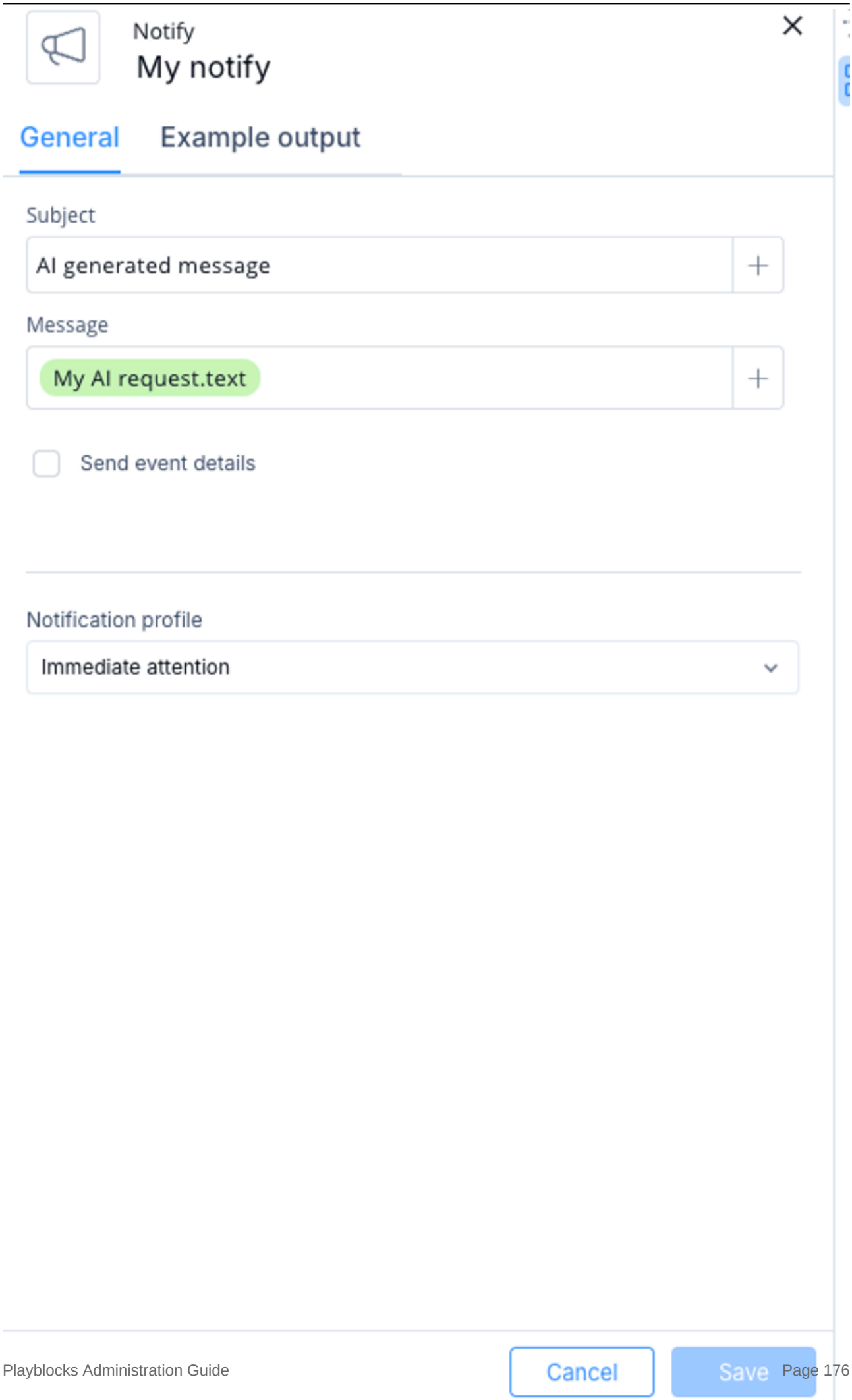
6. Click **Create**.



What to do next:

Using the Response

You can use the **AI Request** response in subsequent steps. In the smart-field selector, select the **AI Request** step as the source and select the output field (under **text** is the model response).


Notify
My notify
General
Example output
Subject
AI generated message
Message
My AI request.text
Send event details
Notification profile
Immediate attention
Cancel
Save

6.7.15. Isolate Endpoint Device

Configure and create an isolation action for an endpoint device. Specify the endpoint product, device details, isolation duration, and reason for isolation.

About this task:

Isolate Endpoint Device

Procedure:

1. Select Isolate Endpoint Device and then click Add.

   The **Isolate Endpoint Device** window appears.

2. Specify these:
   - **Type** - Select the endpoint product:
     - Endpoint Security
     - CrowdStrike
     - Microsoft Defender
     - SentinelOne
   - **Device Name** - Enter the device name, or select a value from previous step outputs or automation parameters.
   - **Duration** - Select how long the device remains isolated.
   - **Reason** - Enter the reason for isolating the device.
3. Click **Create**.

What to do next:

> **Note:**
>
> The selected endpoint product must be configured before the isolation action can run.

6.7.16. Scan Endpoint Security Device

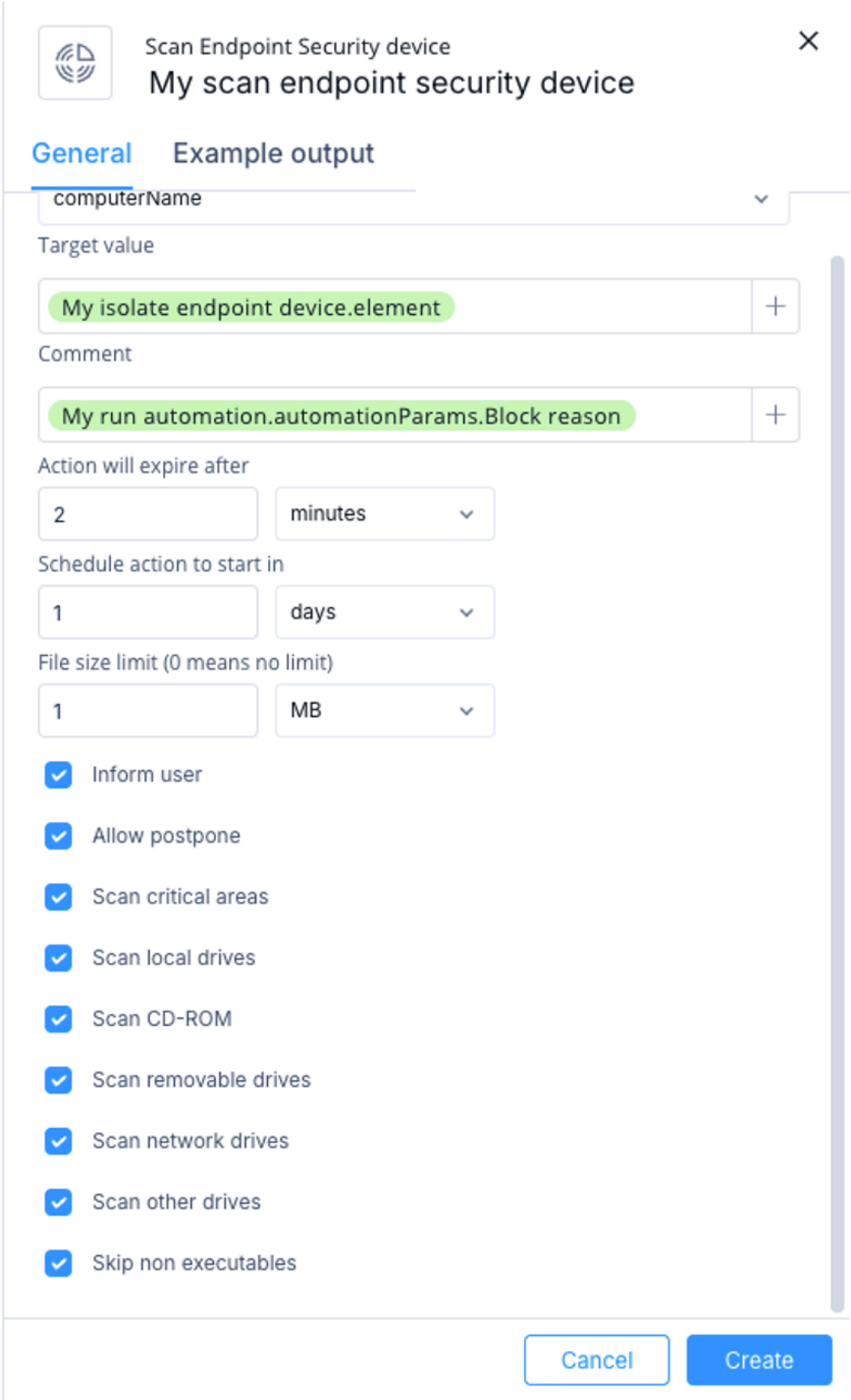
Scan an Endpoint Security device by configuring target identification, scan options, and scheduling parameters.

About this task:

This task describes how to configure a **Scan Endpoint Security Device** action to scan an endpoint device for threats.

Procedure:

1. Select **Scan Endpoint Security device** and then click **Add**.
   The **Scan Endpoint Security device** window appears.



2. Specify these:
    - **Target type** - Select how to identify the device:
        - computerName
        - computerId
        - computerIp
    - **Target value** - Enter the value that matches the selected target type, or select a value from previous step outputs or automation parameters.
    - **Comment** - Optional comment for the action.
    - **Action will expire after** - Select when the action expires.
    - **Schedule action to start in** - Select when to start the action. Use 0 to run immediately.
    - **File size limit** - Set the maximum file size to scan. Use 0 for no limit.
    - **Inform user** - Notify the endpoint user with a UserCheck popup message.
    - **Allow postpone** - Allow the endpoint user to postpone the operation.
    - **Scan critical areas** - Scan operating system, processes, and memory.
    - **Scan local drives**
    - **Scan CD-ROM**
    - **Scan removable drives**
    - **Scan network drives**
    - **Scan other drives**
    - **Skip non executables**

    Note:

    Select at least one scan area.

3. Click **Create**.

6.7.17. Terminate Process on Endpoint Security Device

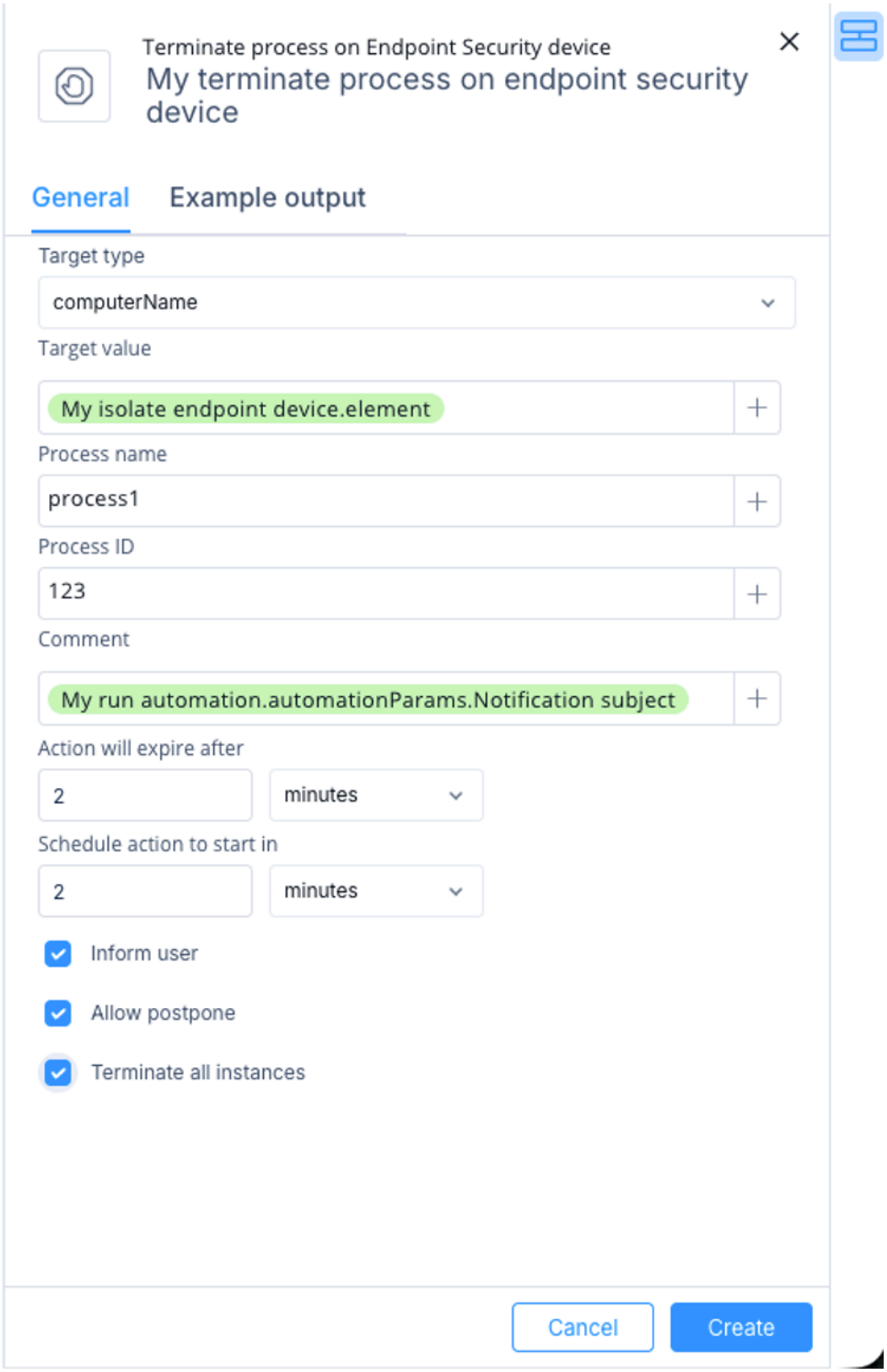
Terminate a process on an Endpoint Security device by configuring target details and action settings.

About this task:

This task describes how to configure a **Terminate process on Endpoint Security device** action to terminate a running process on an endpoint device.

Procedure:

1. Select **Terminate process on Endpoint Security device** and then click **Add**.
   The **Terminate process on Endpoint Security device** window appears.



2. Specify these:
    - **Target type** - Select how to identify the device:
        - computerName
        - computerId
        - computerIp
    - **Target value** - Enter the value that matches the selected target type, or select a value from previous step outputs or automation parameters.
    - **Process name** - Enter the process name to terminate.
    - **Process ID** - Optional process ID.
    - **Comment** - Optional comment for the action.
    - **Action will expire after** - Select when the action expires.
    - **Schedule action to start in** - Select when to start the action. Use 0 to run immediately.
    - **Inform user** - Notify the endpoint user with a UserCheck popup message.
    - **Allow postpone** - Allow the endpoint user to postpone the operation.
    - **Terminate all instances** - Terminate all matching process instances.
3. Click **Create**.

6.7.18. Delete File on Endpoint Security Device

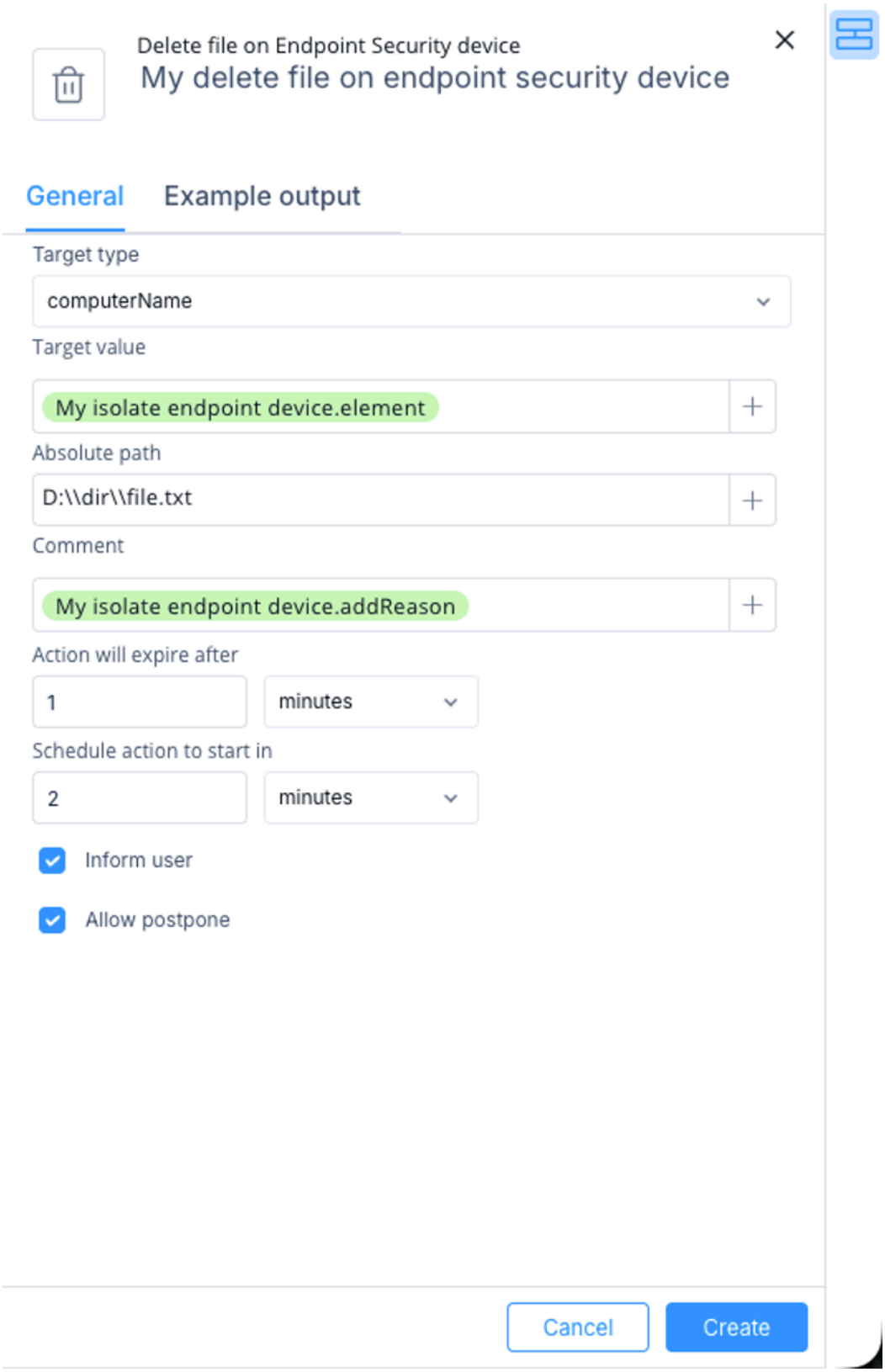
Delete a file on an Endpoint Security device by configuring the target device and file path settings. This task explains how to create the delete file action.

About this task:

This task describes how to configure a **Delete file on Endpoint Security device** action to remove a specific file from an endpoint device.

Procedure:

1. Select **Delete file on Endpoint Security device** and then click **Add**.
   The **Delete file on Endpoint Security device** window appears.



2. Specify these:
    - **Target type** - Select how to identify the device:
        - computerName
        - computerId
        - computerIp
    - **Target value** - Enter the value that matches the selected target type, or select a value from previous step outputs or automation parameters.
    - **Absolute path** - Enter the full path of the file to delete.
    - **Comment** - Optional comment for the action.
    - **Action will expire after** - Select when the action expires.
    - **Schedule action to start in** - Select when to start the action. Use 0 to run immediately.
    - **Inform user** - Notify the endpoint user with a UserCheck popup message.
    - **Allow postpone** - Allow the endpoint user to postpone the operation.
3. Click **Create**.

6.7.19. Exporting/Importing Automation

You can export and import an automation in JSON format. This task explains how to export an automation and import an automation file.

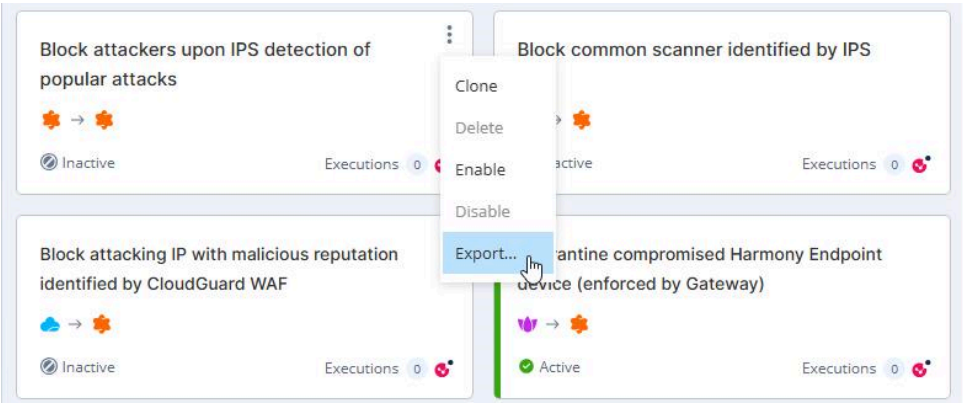
About this task:

You can export and import an automation in json format.

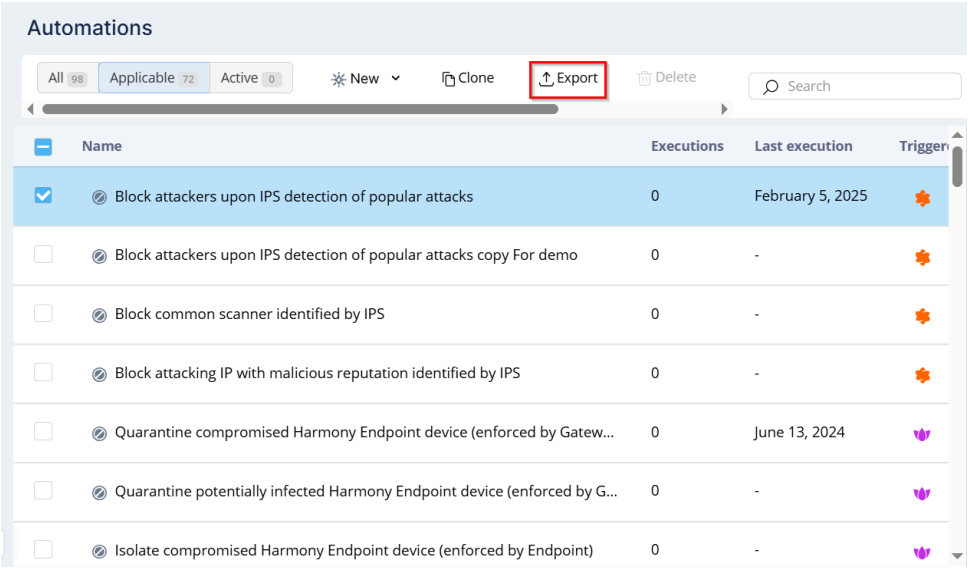
Procedure:

1. To export an automation:

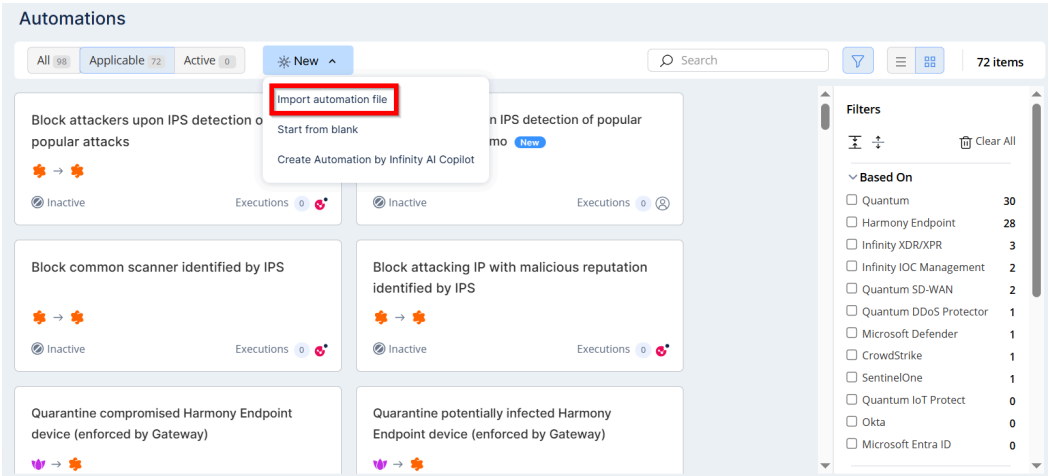
   - In the card view, click ⋮ in an automation card that you want to export and then click **Export**.



   - In the table view, select the automation that you want to export and then click **Export**.

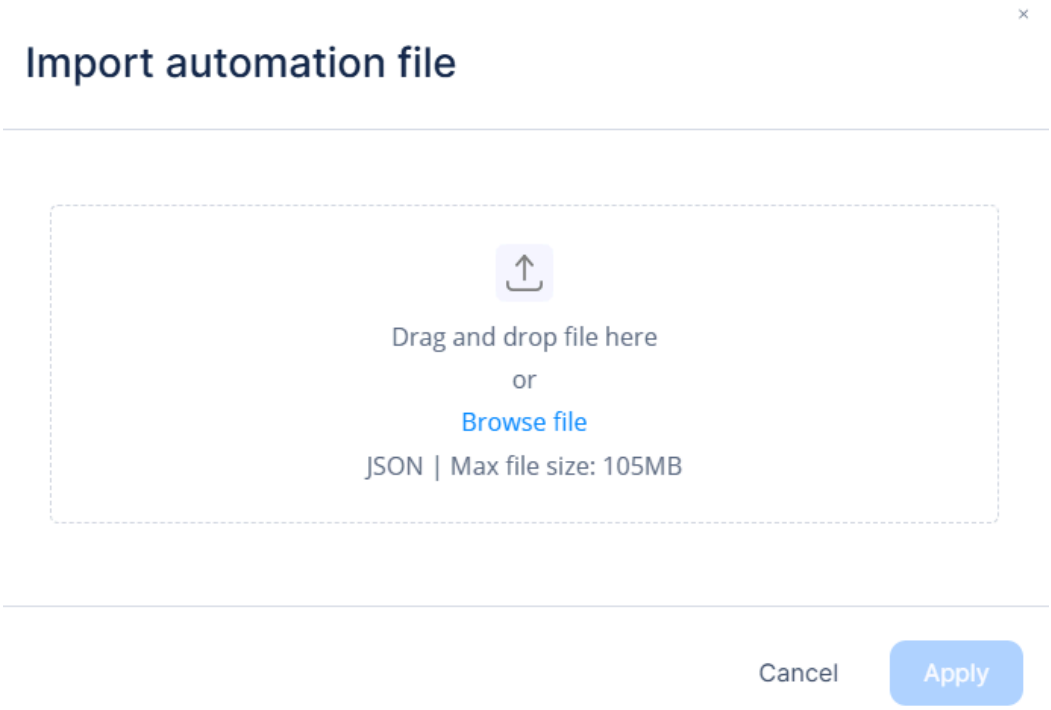


2. To import an automation, click **New**.



3. Select **Import automation file**.

   The **Import automation file** window appears.



4. Choose the *.json* file from your local drive.
5. Click **Apply**.

6.7.20. Cloning Existing Automation

You can clone an existing automation for editing and customization. This task explains how to clone an automation from the card view and table view.

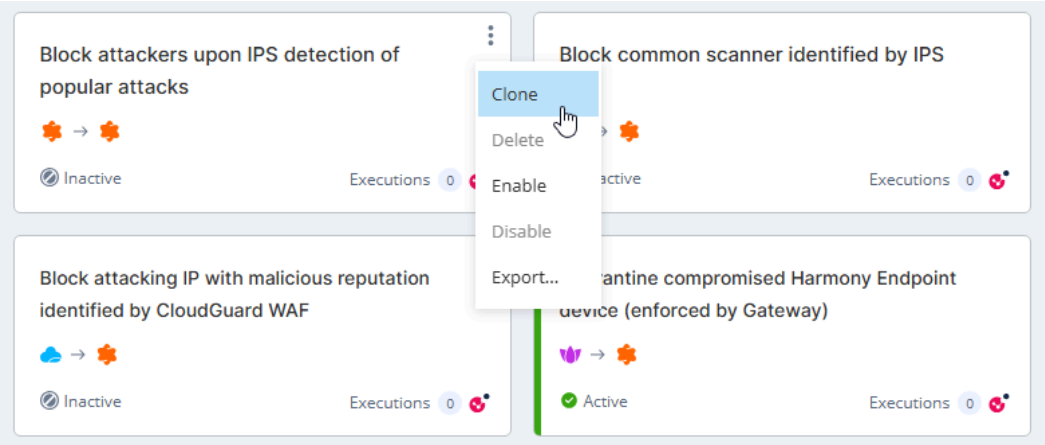
About this task:

You can clone an existing automation for editing and customization. To do that:

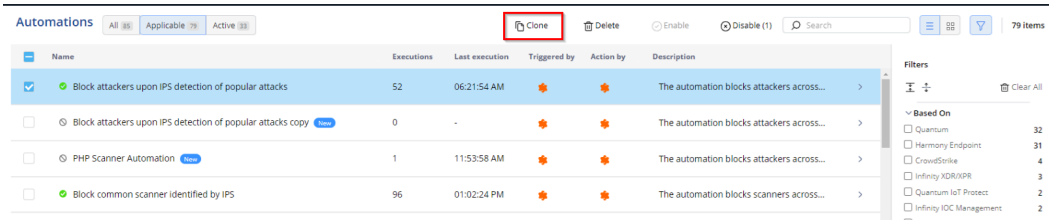
Cloning Existing Automation

Procedure:

1. In the card view, click ⋮ in an automation card that you want to clone and then click **Clone**.



2. In the table view, select the automation that you want to clone and then click **Clone**.



6.7.21. Automation Capabilities

This topic describes the different automation capability types, their use cases, abilities, and editing restrictions.

Automation Capabilities - Out-of-the-Box Automations

Use Case	Default automations provided by the system.
Abilities	• Update automation parameter values • Update notification profiles • Reset parameters
Editing Restrictions	• Cannot edit steps • Cannot change structure or metadata

Cloned Automations - Not Exported but Exportable

Use Case	Cloned from out-of-the-box automations without structural changes.

Abilities	• Update metadata and step content • Add/remove steps from the end of the graph • Reset parameters
Editing Restrictions	• Cannot change structure in the middle of the graph • Notification profile menu is unavailable

Fully Custom or Modified Automations - Exported and Exportable

Use Case	Cloned and modified, or created from blank, import, or AI.
Abilities	• Full metadata and step updates • Add/remove steps from the end of the graph
Editing Restrictions	• Cannot reset parameters • Notification profile menu is unavailable

Cloned Automations - Not Exported or Exportable

Use Case	Limited to 3 default automations: • Notify on high rate of blocked connections • Repeated Remote Access login to expired accounts • Repeated Remote Access login failures (password-only)
Abilities	• Update metadata • Update step content • Reset parameters
Editing Restrictions	• Cannot add/remove steps • Notification profile menu is unavailable

6.7.22. Replace Trigger

Replace Trigger allows you to change the current trigger type in your automation to a different one. This topic explains how to replace a trigger, configure the new trigger, and resolve validation errors.

About this task:

Replace

Replace Trigger allows you to change the current trigger type in your automation to a different one.

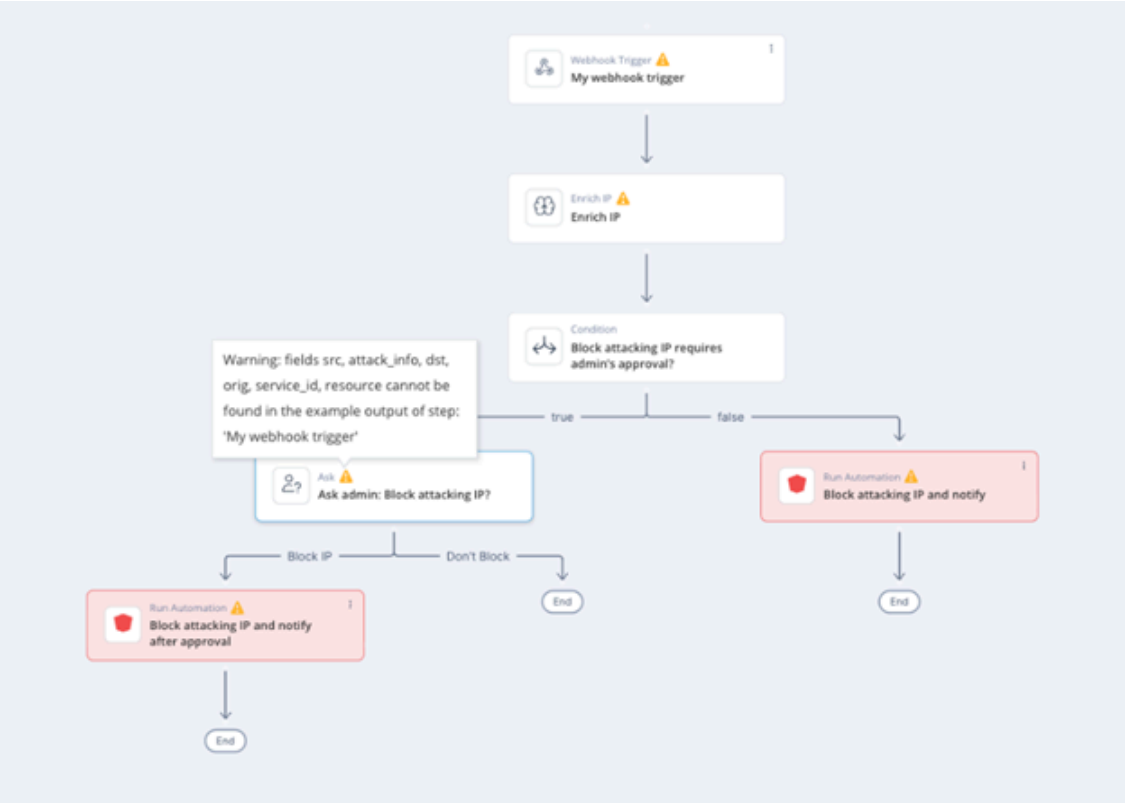
Choose trigger type:

- **Log Trigger** - Starts the automation when a specific log event occurs.
- **Webhook Trigger** - Starts the automation when data is sent to a webhook endpoint.
- **Scheduled Trigger** - Starts the automation based on a predefined schedule (for example, daily or hourly).

Configuring the New Trigger

- The system creates the new trigger immediately for a Webhook Trigger.
- For all other trigger types, enter the required parameters in the trigger window and click **Save**.

Note: When you replace a trigger, the **Example Output** associated with the previous trigger is removed. Any steps in the automation that rely on fields from that output displays validation errors.



Resolving Validation Errors

When you replace a trigger, steps that reference fields from the previous trigger may display validation errors. These errors occur because the referenced fields are not available in the new trigger's output example.

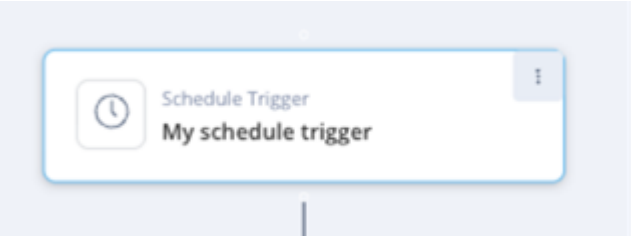
To resolve these errors:

Note: Notes -

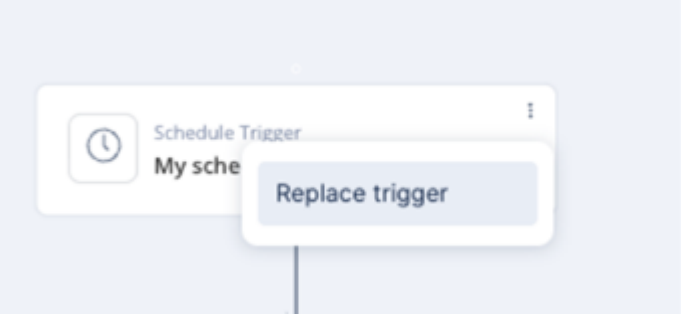
- All references in dependent steps must match the fields defined in the trigger's Example Output.
- You can either add old field names to the new example output or update the dependent steps to use the new field names.

Procedure:

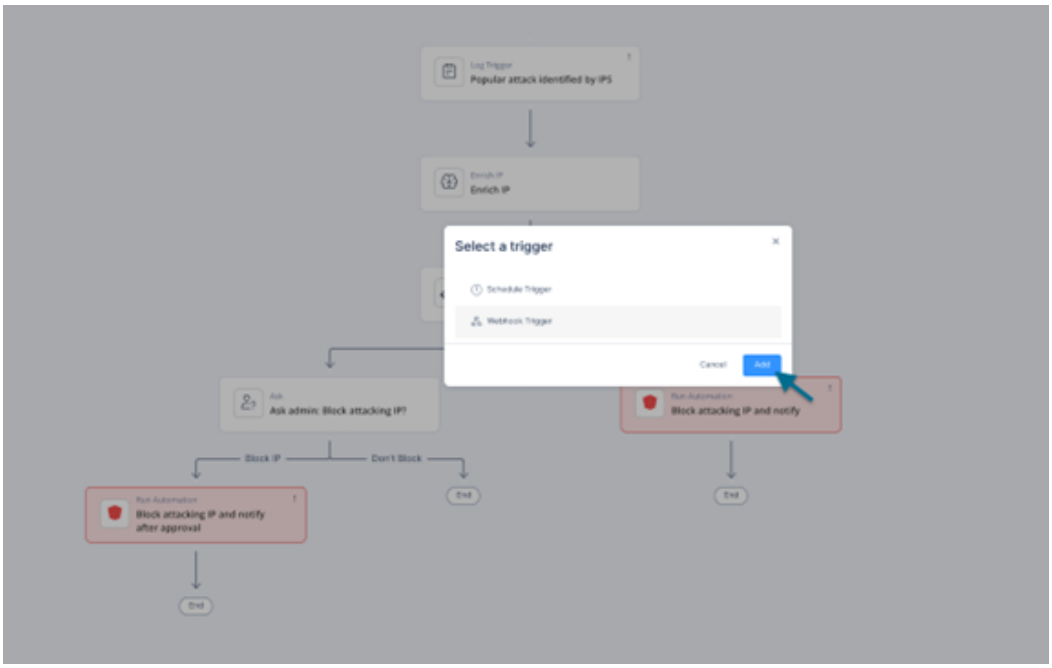
1. In the trigger step, click .



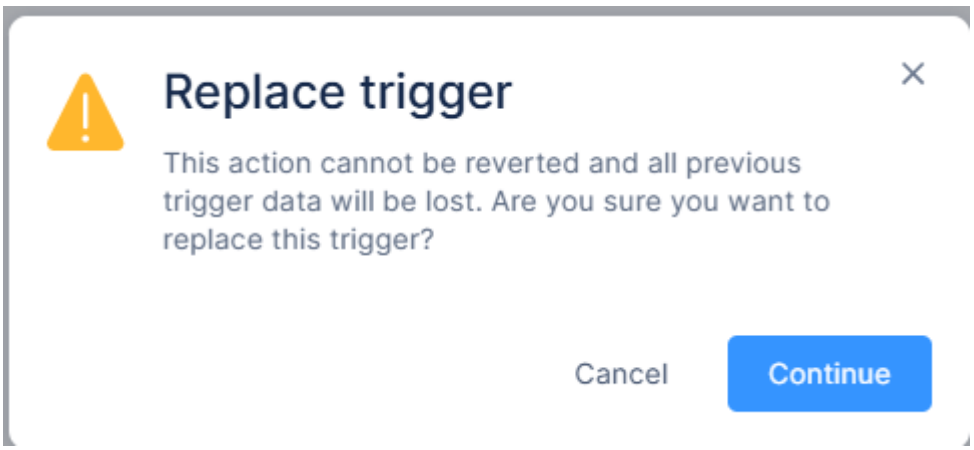
2. Click **Replace Trigger**.



3. Choose the new trigger type and click **Add**.



A warning message appears



Note: Replacing a trigger permanently deletes all previous trigger data. This action cannot be undone.

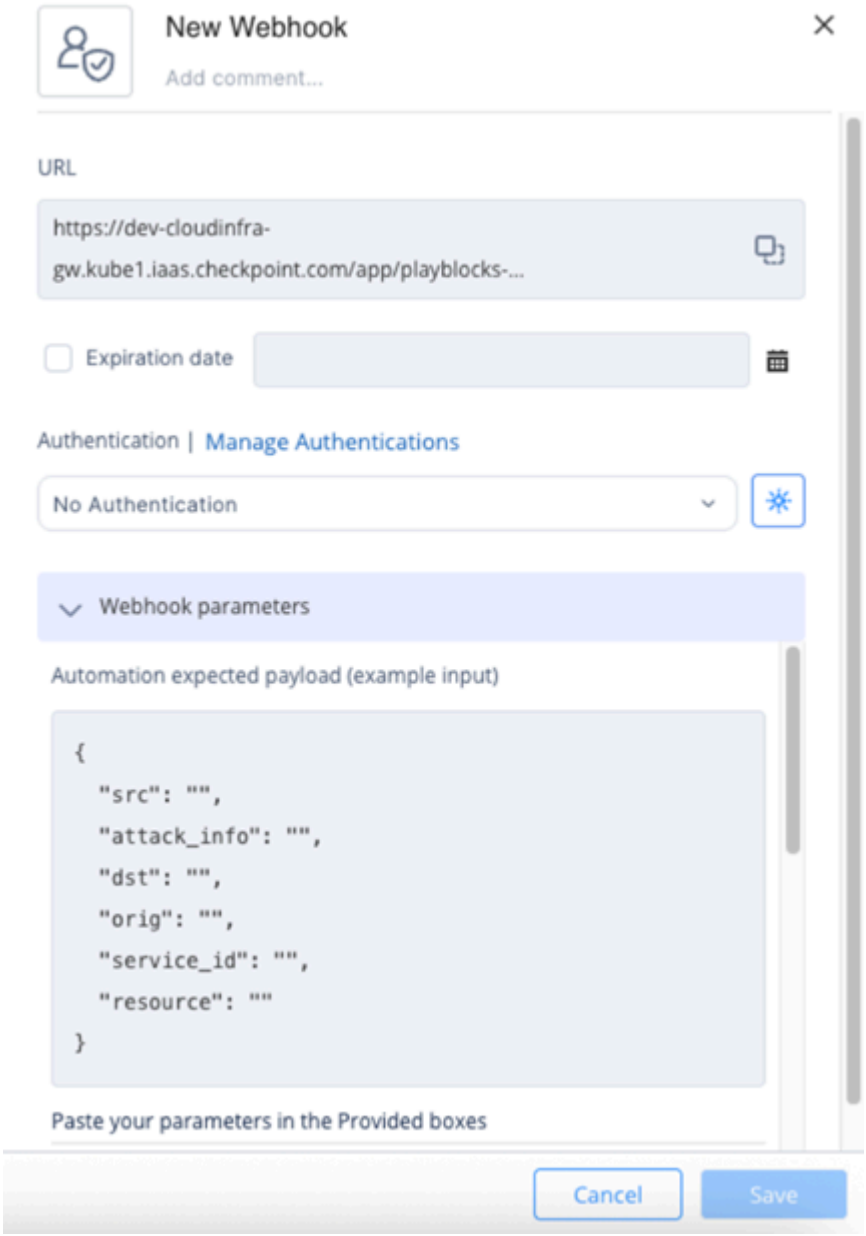
4. Click **Continue**.

5. Remove unused references
   a. Open the step that shows the validation error.
   b. Remove any references to fields from the previous trigger that are no longer required.
   c. Save the step.

6. Update output example and references
   a. Open the new trigger configuration.
   b. In the Example Output, add all required fields that are referenced by dependent steps.
   c. If the new trigger uses different field names, update the references in the dependent steps to match the new field names.
   d. Save the changes.

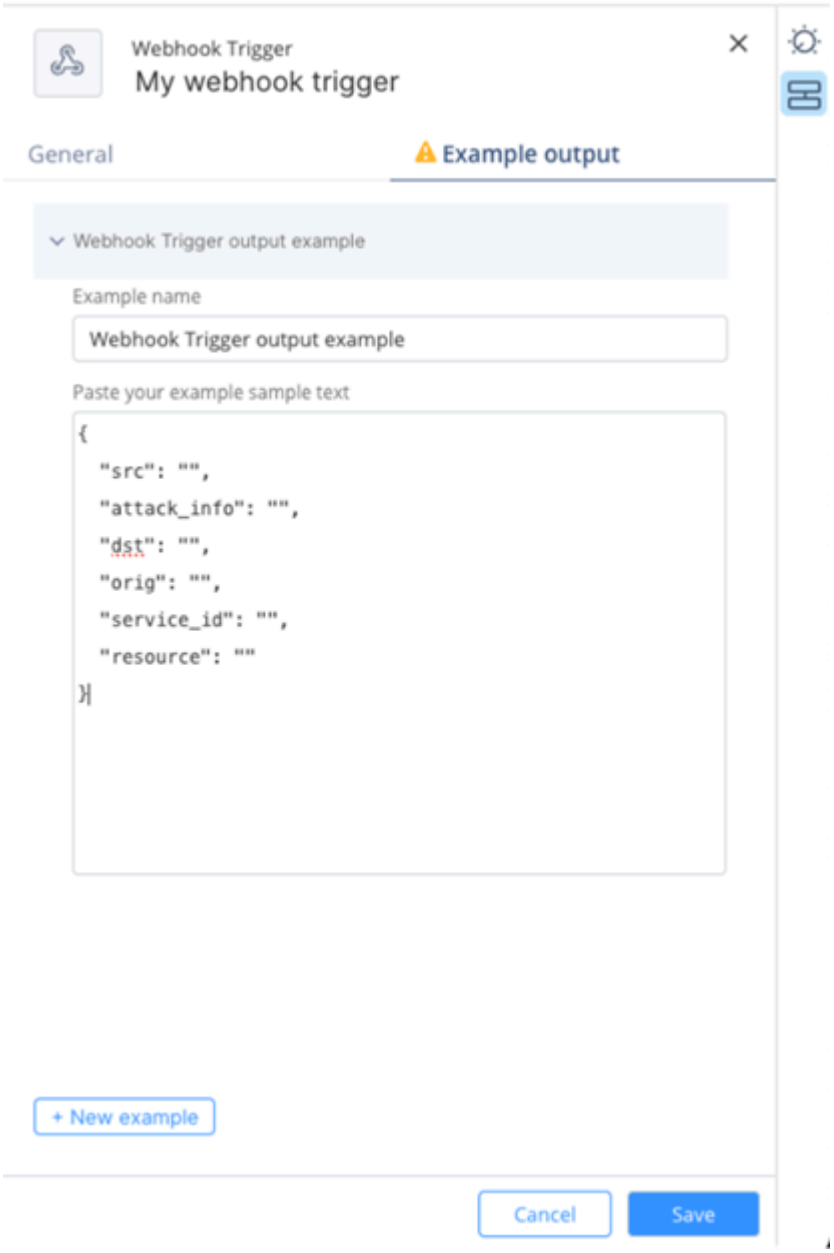
7. Create the webhook.

8. Open **Webhook Parameters** and review the **Automation Expected Payload**.



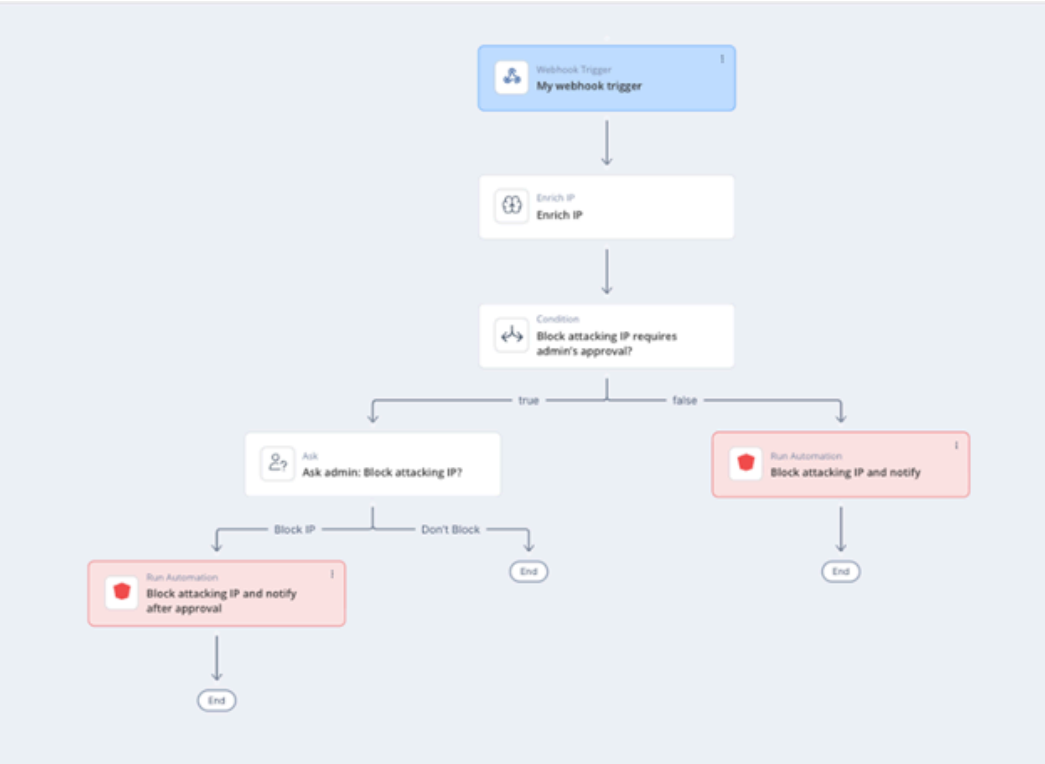
9. Use this payload as a guideline for the required fields.

10. Update the Example Output with all necessary fields.



11. Click **Save**.

    The system automatically resolves validation errors.



Note: The expected payload is only a structural guideline. It does not represent the actual payload your webhook sends.

6.7.23. Adding a Step to the Middle of an Automation

You can add new steps between existing steps in an automation to extend the flow without creating a new automation. When you add a Condition or Ask step, you must specify how the automation continues to the next step.

You can add new steps between existing steps in an automation.

Note:

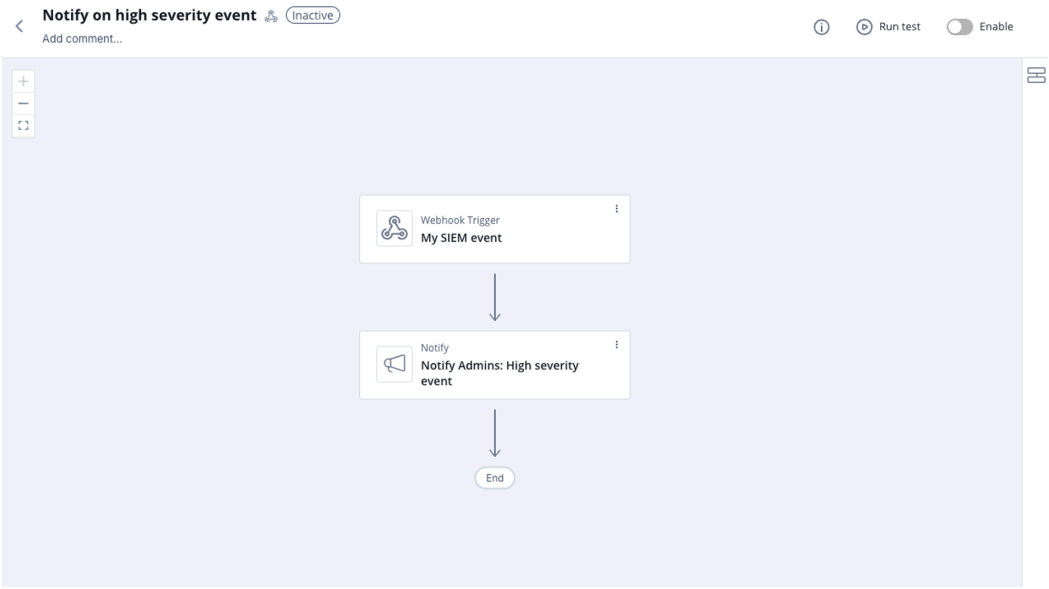
When you add a **Condition** or **Ask** step between existing steps, you must specify how the automation continues to the next step.

Adding a Condition Step Between Existing Steps

When you add a **Condition** step between two existing steps, you must select which branch the next step follows: **True** or **False**.

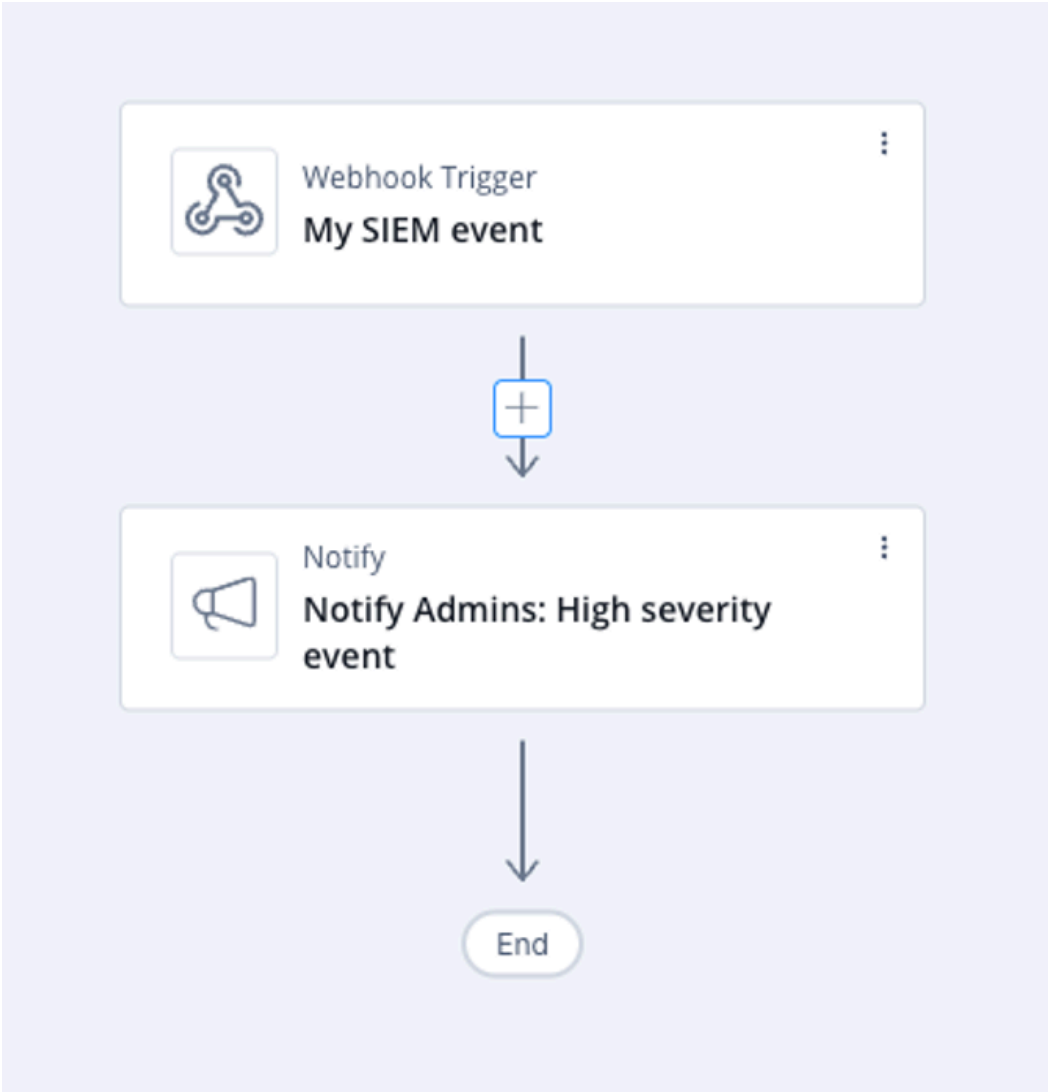
To add a Condition step between existing steps:

1. Access **Playblocks** and open the required automation.



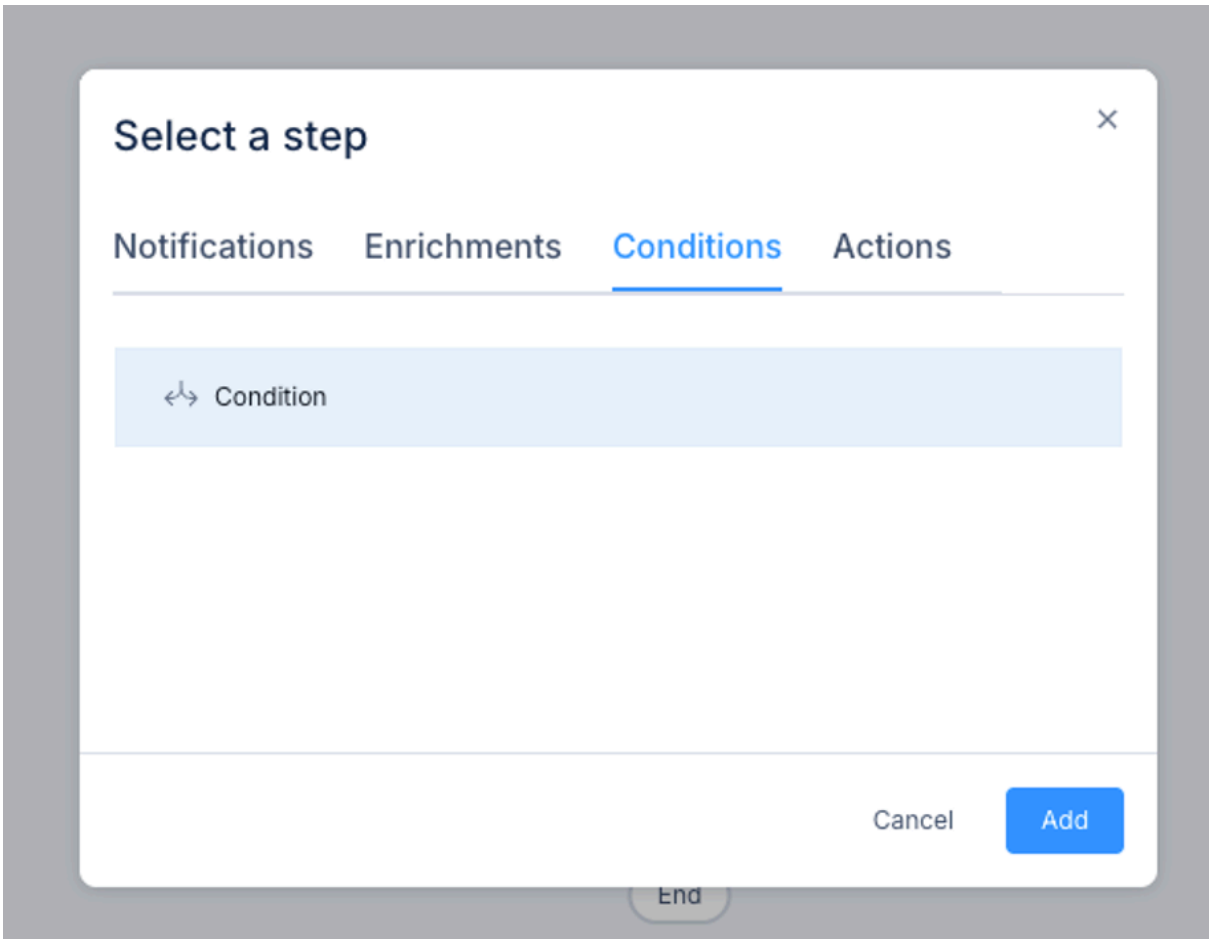
2. Move the cursor over the arrow between the two existing steps.

   The arrow changes to a **+** button.



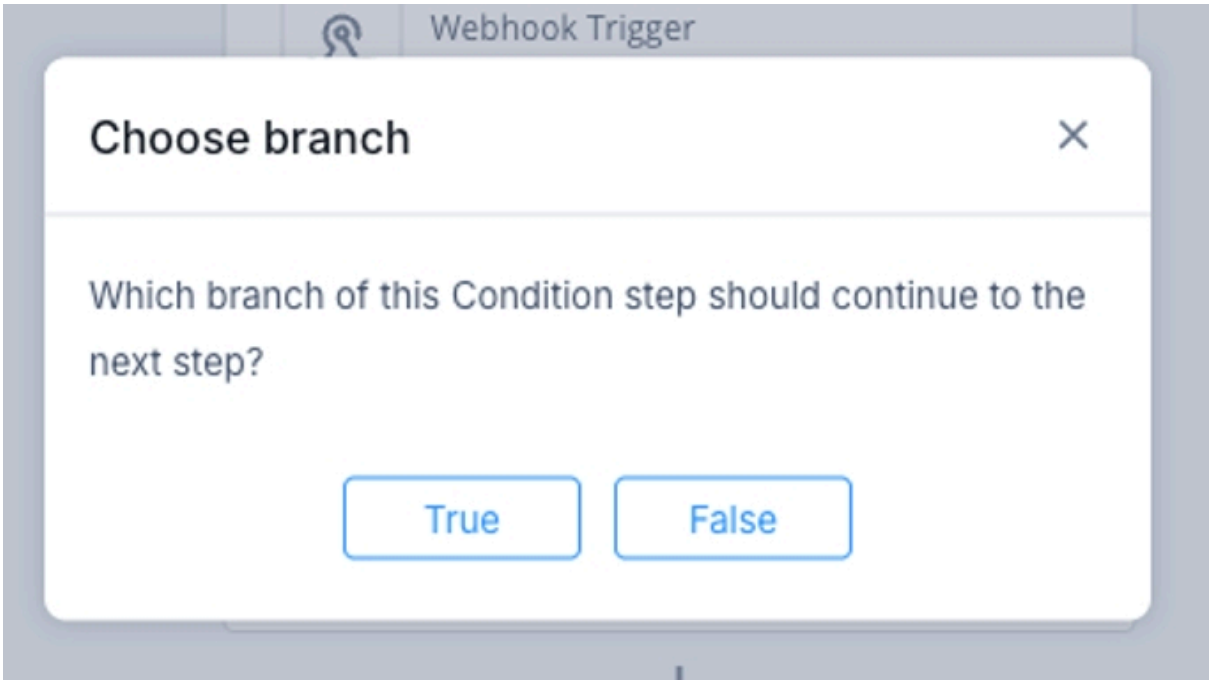
3. Click **+**.

   The **Select a step** window appears.



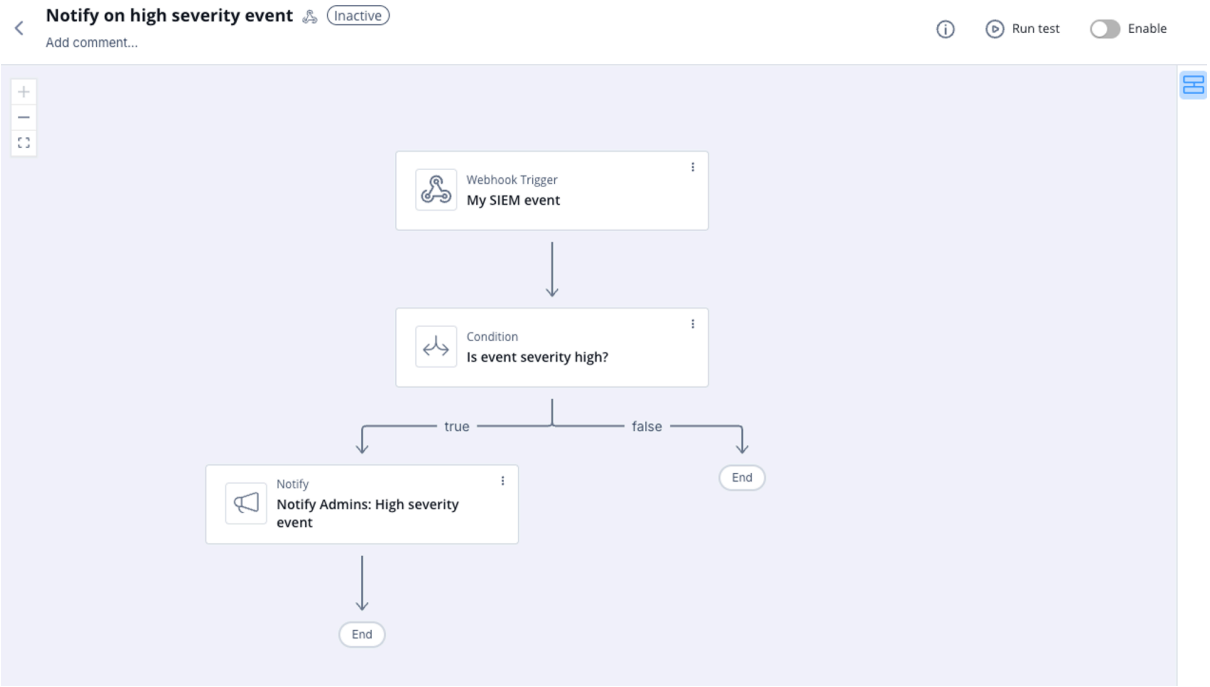
4. On the **Conditions** tab, select **Condition** and click **Add**.

   The **Choose branch** window appears.



5. Select the branch that continues to the next step:
    - **True** - The next step runs when the condition is met.
    - **False** - The next step runs when the condition is not met.
6. Configure the condition expressions and operator. For more information, see Conditions.
7. Click **Create**.

   The **Condition** step appears between the existing steps with **true** and **false** branches.

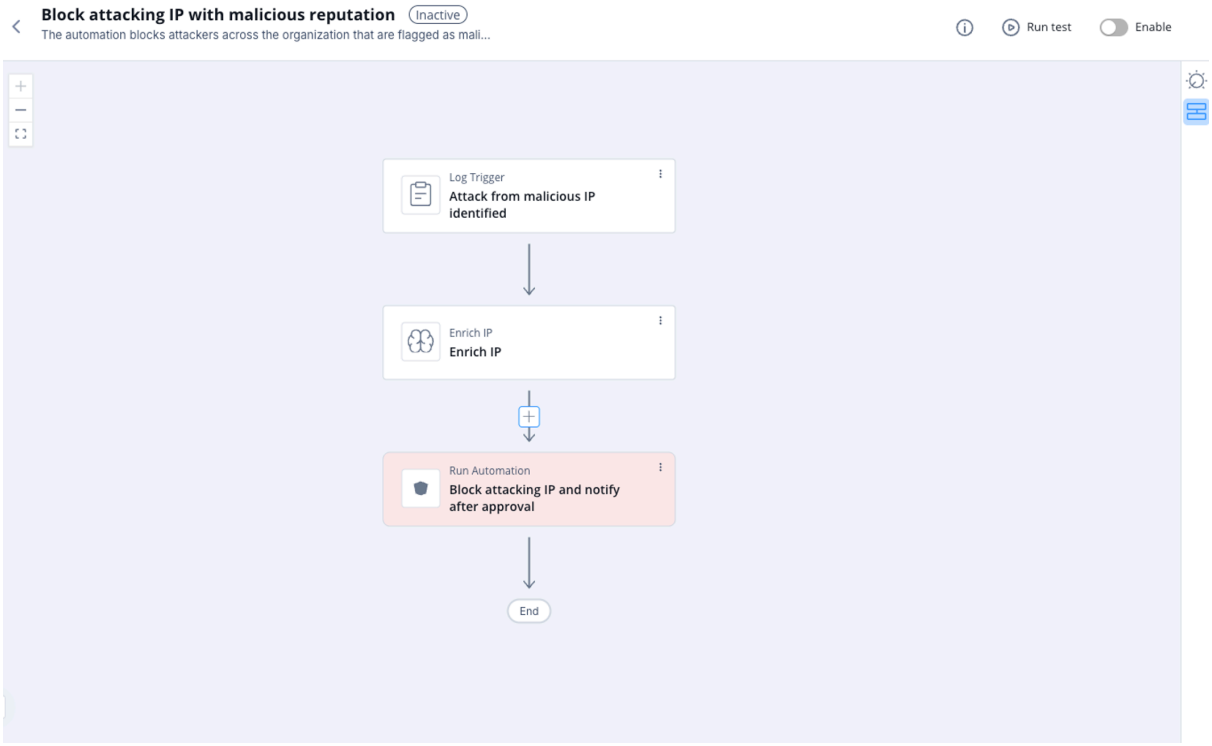


Adding an Ask Step Between Existing Steps

When you add an **Ask** step between existing steps, the next step is automatically added to the path of the first **Ask** option.

To add an Ask step between existing steps:

1. Access **Playblocks** and open the required automation.



2. Move the cursor over the arrow between the two existing steps.

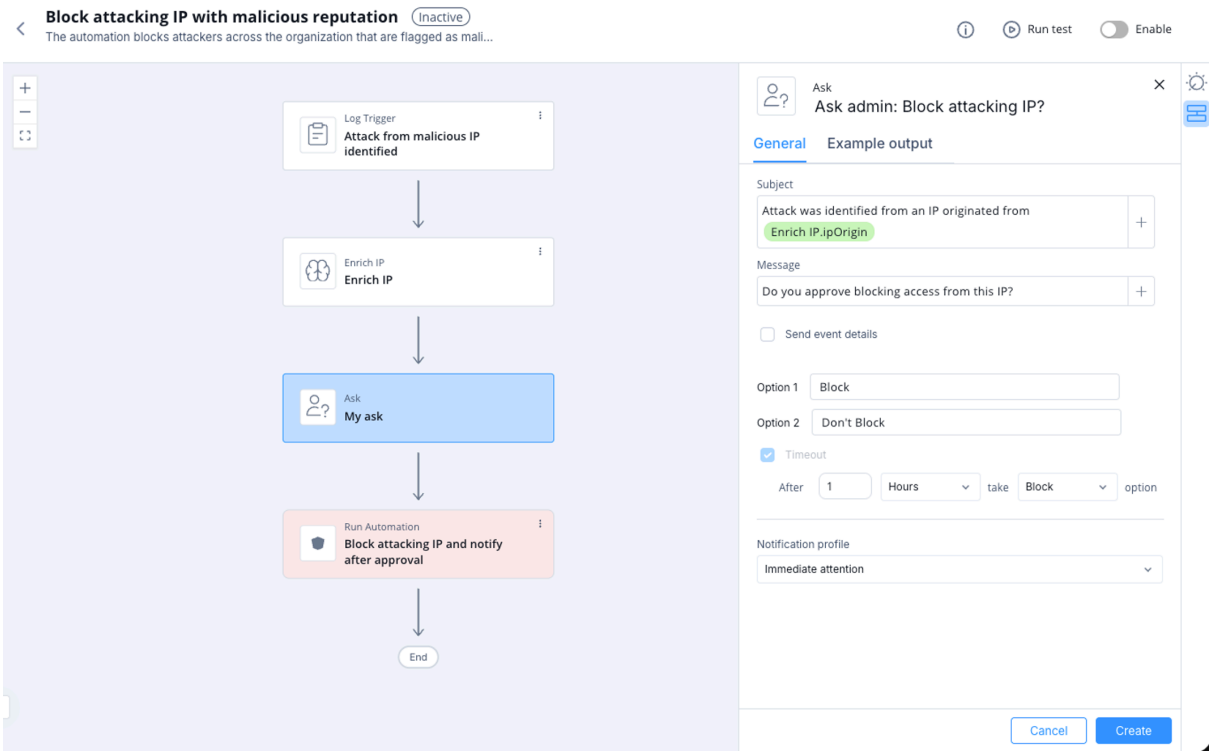
   The arrow changes to a **+** button.

3. Click **+**.

   The **Select a step** window appears.

4. On the **Notifications** tab, select **Ask** and click **Add**.

   The **Ask** window appears.



5. Specify these fields:

    a. In the **Subject** field, enter text combined with dynamic values from previous steps or automation parameters.

    b. In the **Message** field, enter text combined with dynamic values from previous steps or automation parameters.

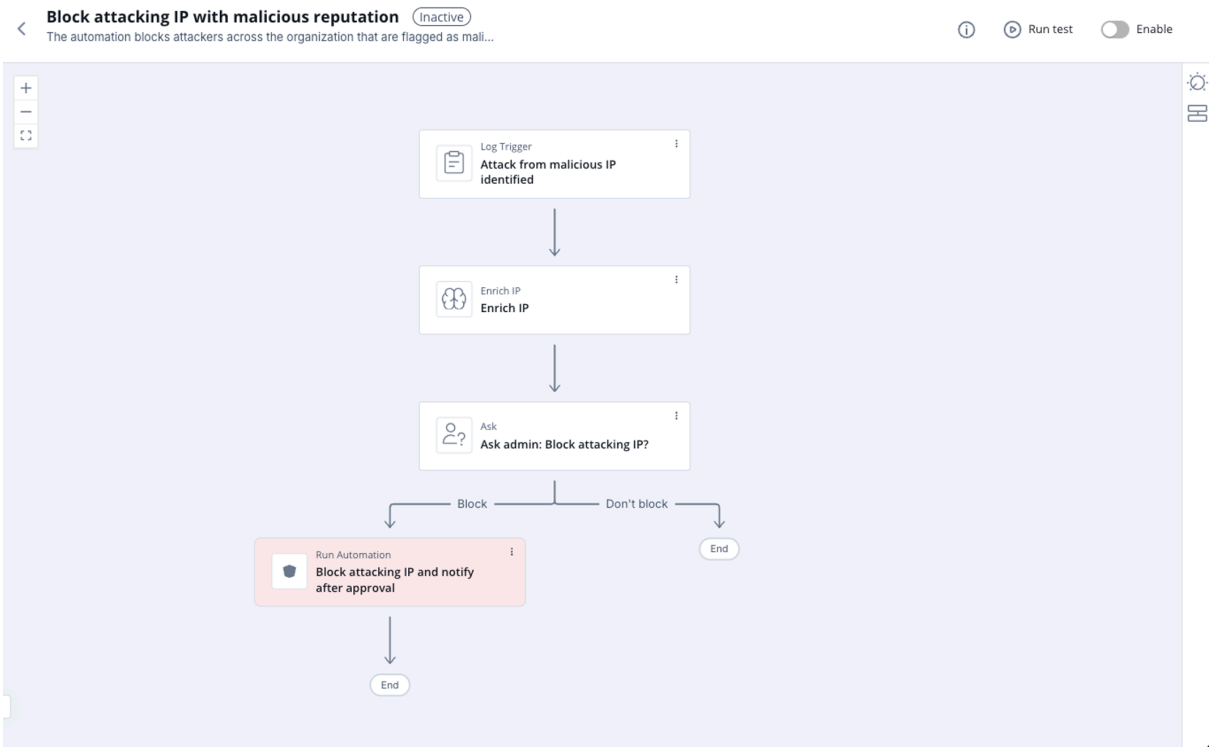
    c. (Optional) Select **Send event details** to include selected event data from the outputs of the current or previous steps, or from the automation parameters.

    d. Under **Options and Defaults**, define user response options and a default fallback in case of timeout.

    e. From the **Notification profile** list, select the notification profile of the step.

6. Click **Create**.

    The **Ask** step appears between the existing steps. The subsequent step automatically follows the path of the first **Ask** option.



6.8. Webhooks

This topic describes how webhooks enable third-party systems to trigger automations. It outlines common uses for out-of-the-box, custom, and cloned automations.

Webhooks allow third-party systems to trigger automations. You can use webhooks for:

- Out-of-the-box automations
- Custom automations
- Cloned automations

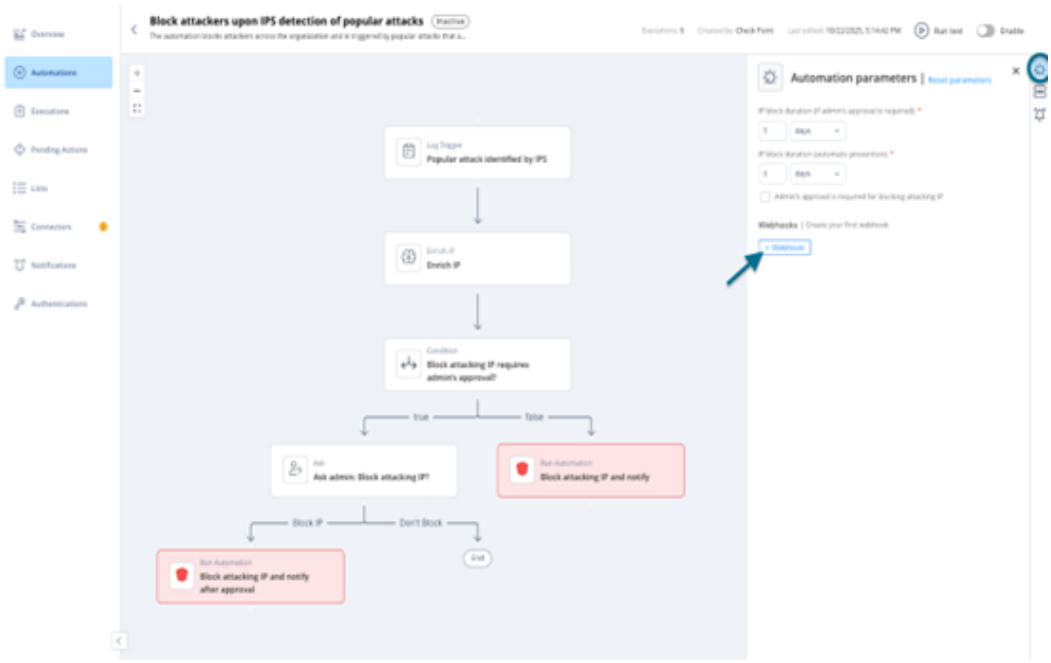
6.8.1. Triggering an Out-of-the-Box Automation Using Webhooks

This task explains how to trigger an automation using a webhook. It outlines the required steps to configure and create a webhook.

About this task:
To trigger an automation using a webhook:

Procedure:

1. In the Automation Parameters panel, click **+Webhook**.

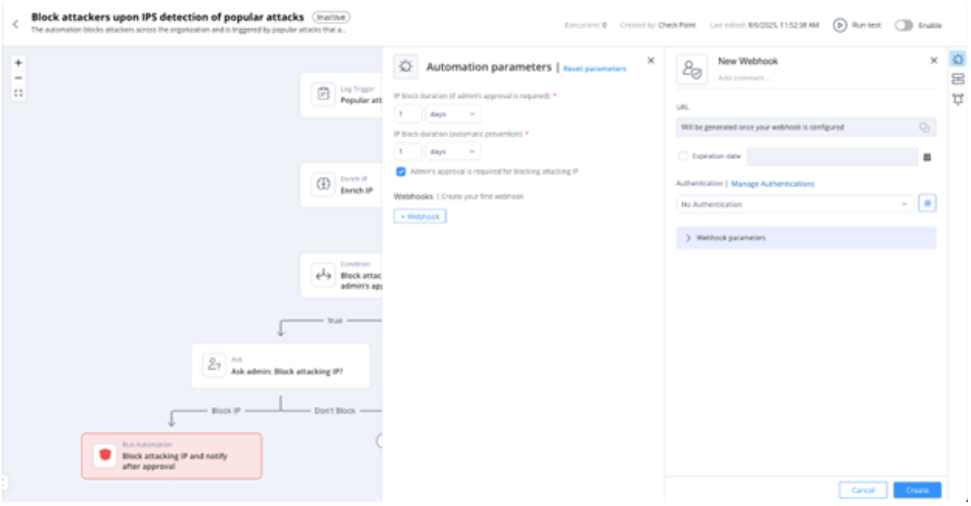


2. In the New Webhook window, enter the required details.

   a. **Name**

   b. (Optional) **Expiration date**

   c. (Optional) **Authentication**



3. Click **Create** to create the webhook.

What to do next:
For detailed configuration steps, see Creating a Webhook *(on page 206)*.

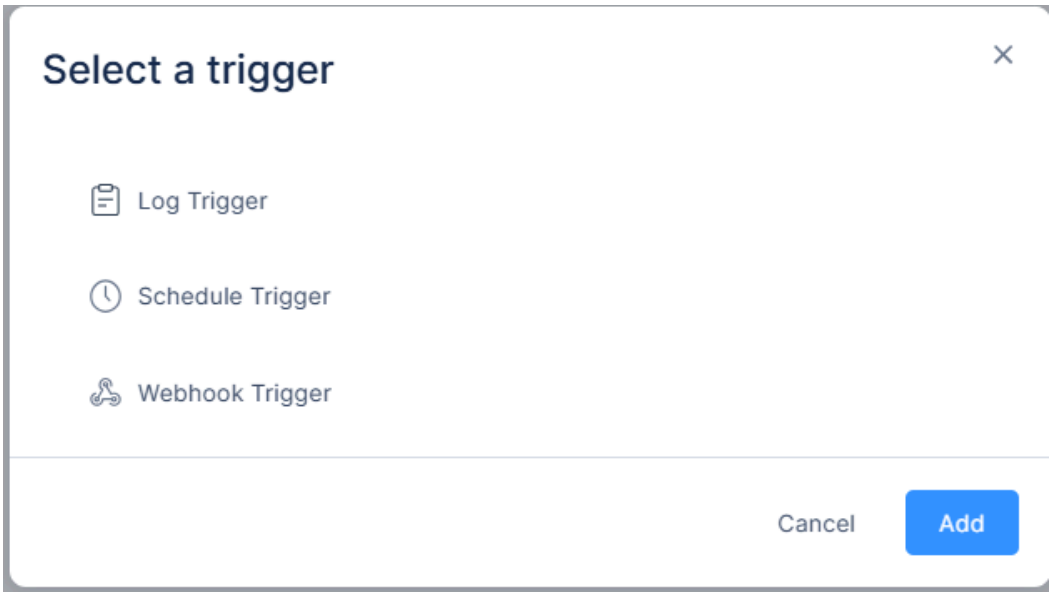
6.8.2. Triggering a Custom Automation Using Webhooks

This task describes how to trigger a custom automation using a webhook and configure its parameters. It guides users through adding a webhook trigger and defining the example output.

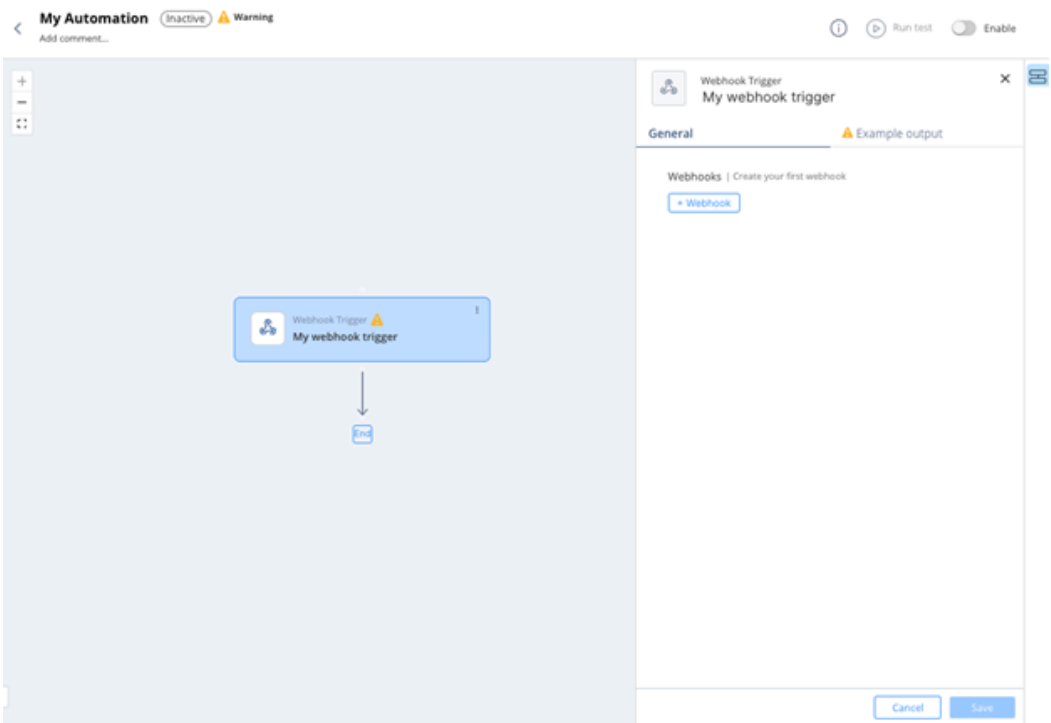
About this task:
To trigger a custom automation using a webhook:

Procedure:

1. Open a blank automation (create a new one or edit an existing blank automation).
2. Click **Click to add trigger**, select **Webhook Trigger** and click **Add**.

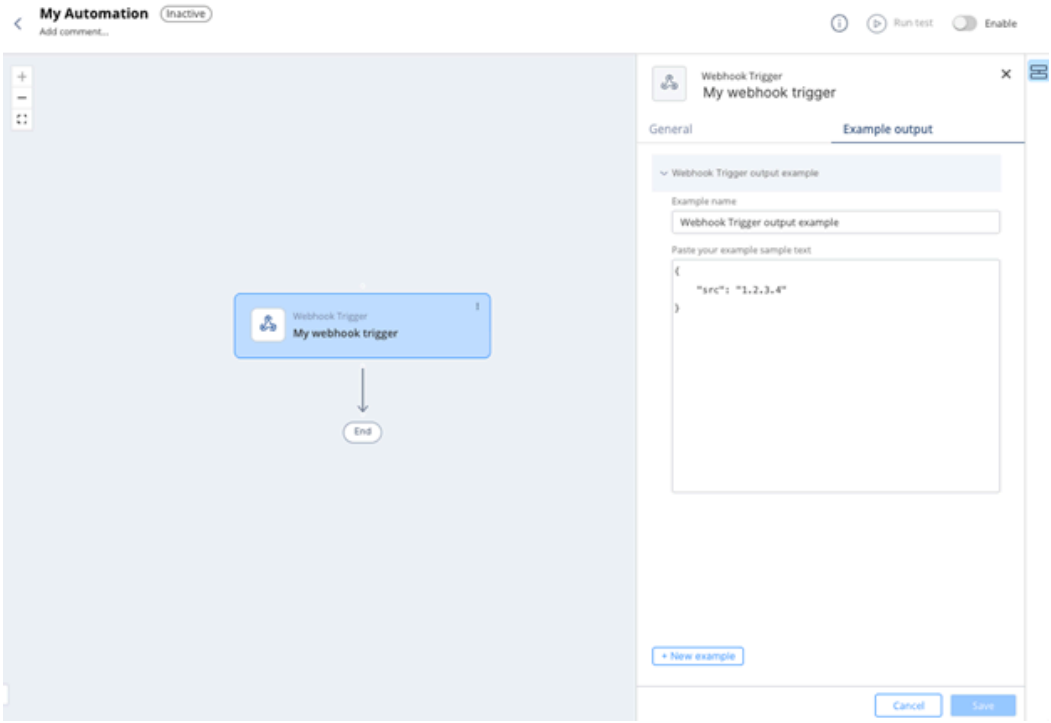


Webhook trigger is created.

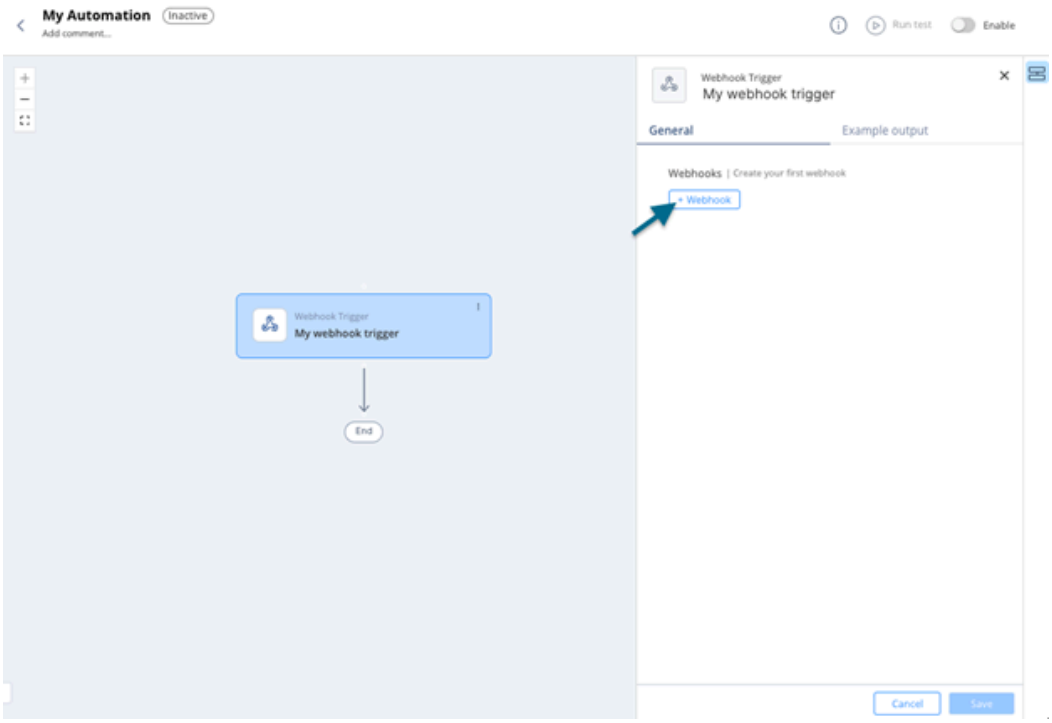


3. Configure the **Example Output** to define the expected webhook payload that third-party systems send to trigger the automation.

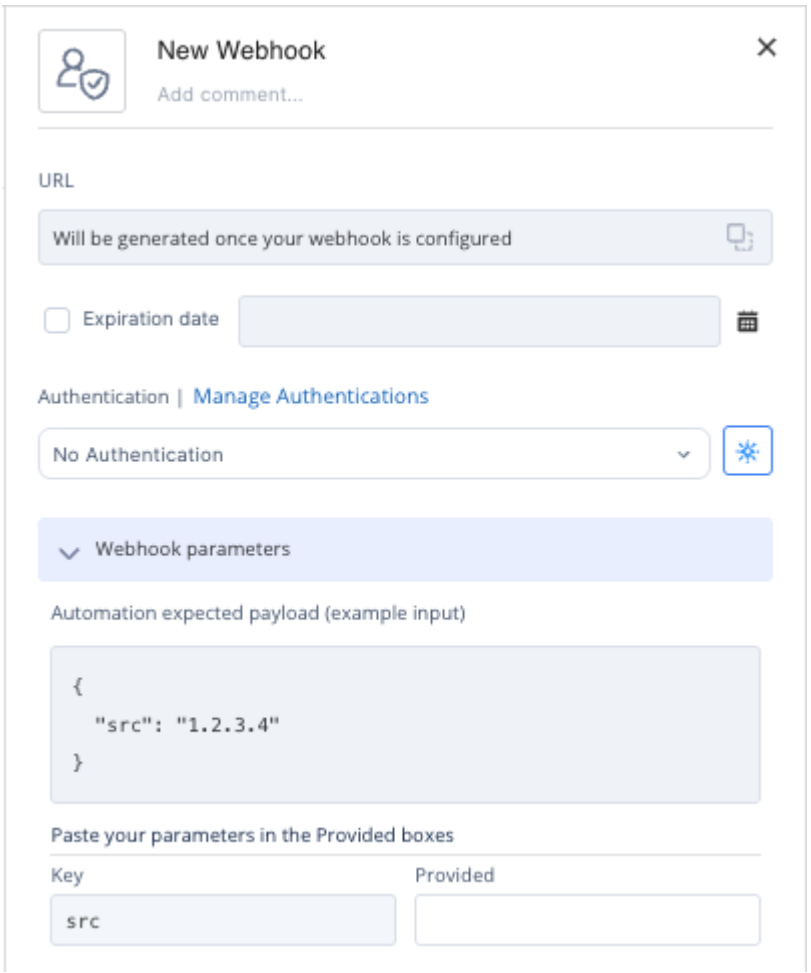
   The example shows the fields that the system passes to the subsequent steps.



4. In the **General** tab, click **+Webhook**.



5. After you use a field from the trigger's example output in a subsequent step, add field mapping to it under **Webhook Parameters**.



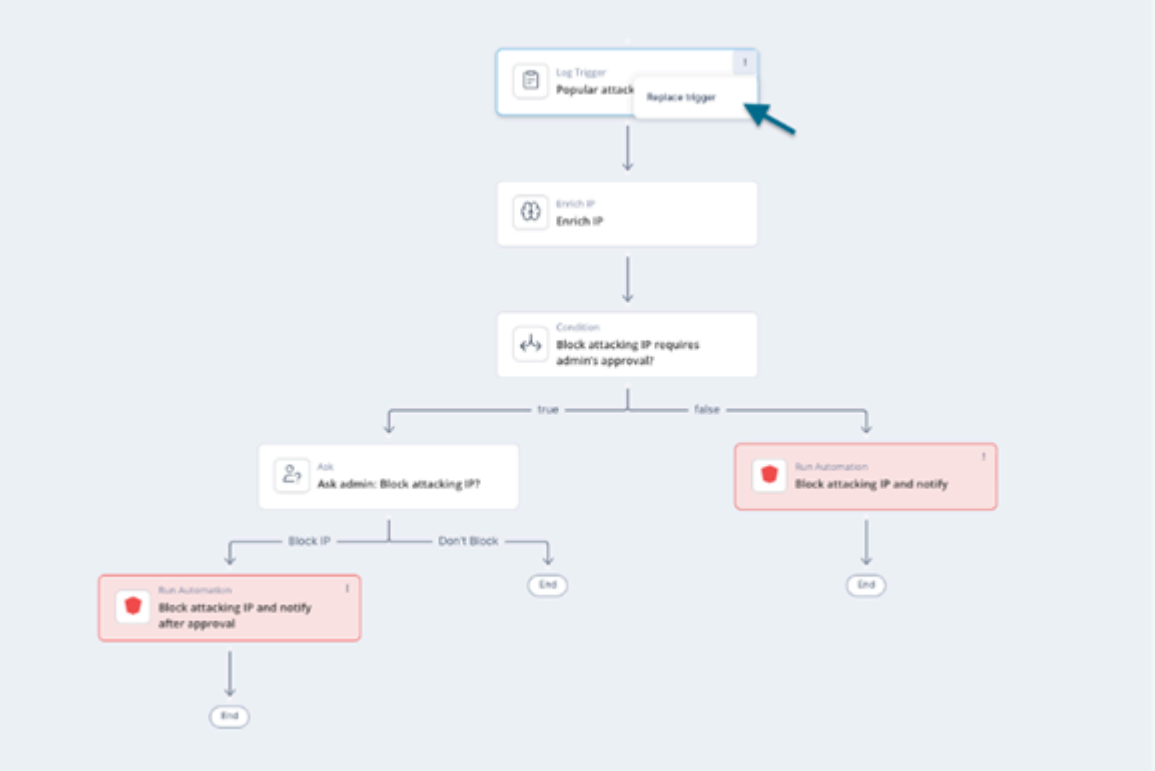
What to do next:
For more details, see Creating a Webhook *(on page 206)*.

6.8.3. Triggering a Cloned Automation Using Webhooks

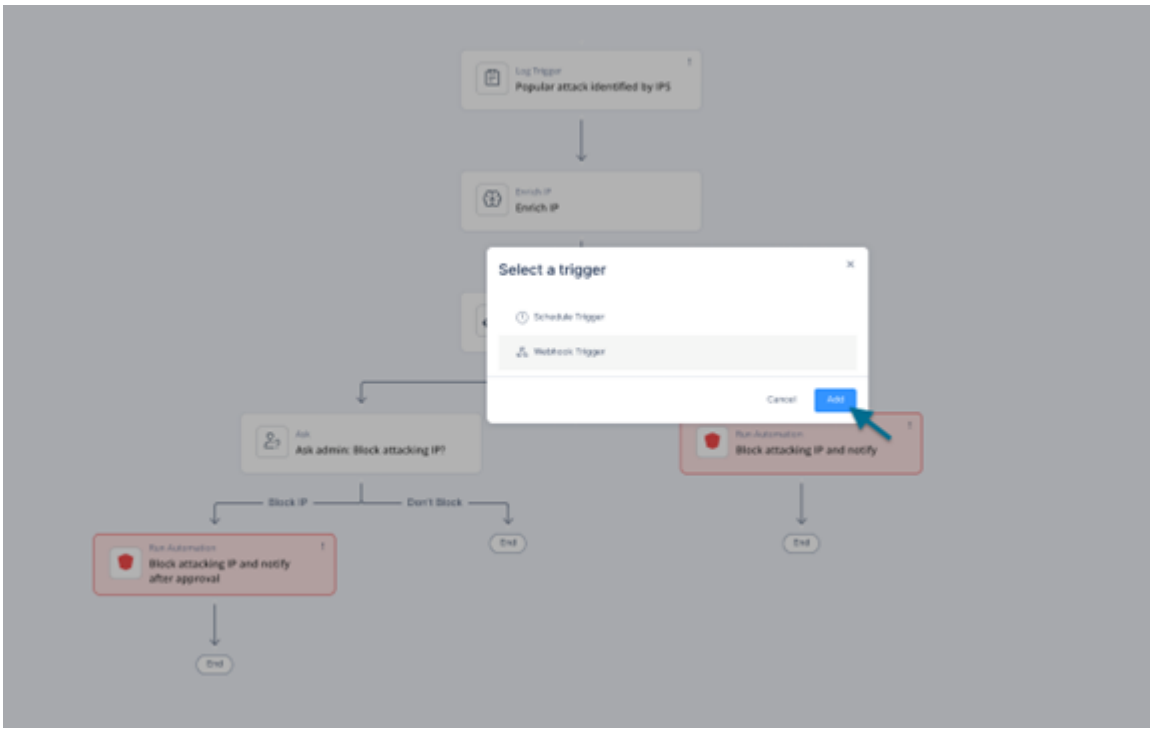
This task describes how to trigger a cloned automation using a webhook. It guides you through replacing the trigger and configuring webhook parameters.

Procedure:

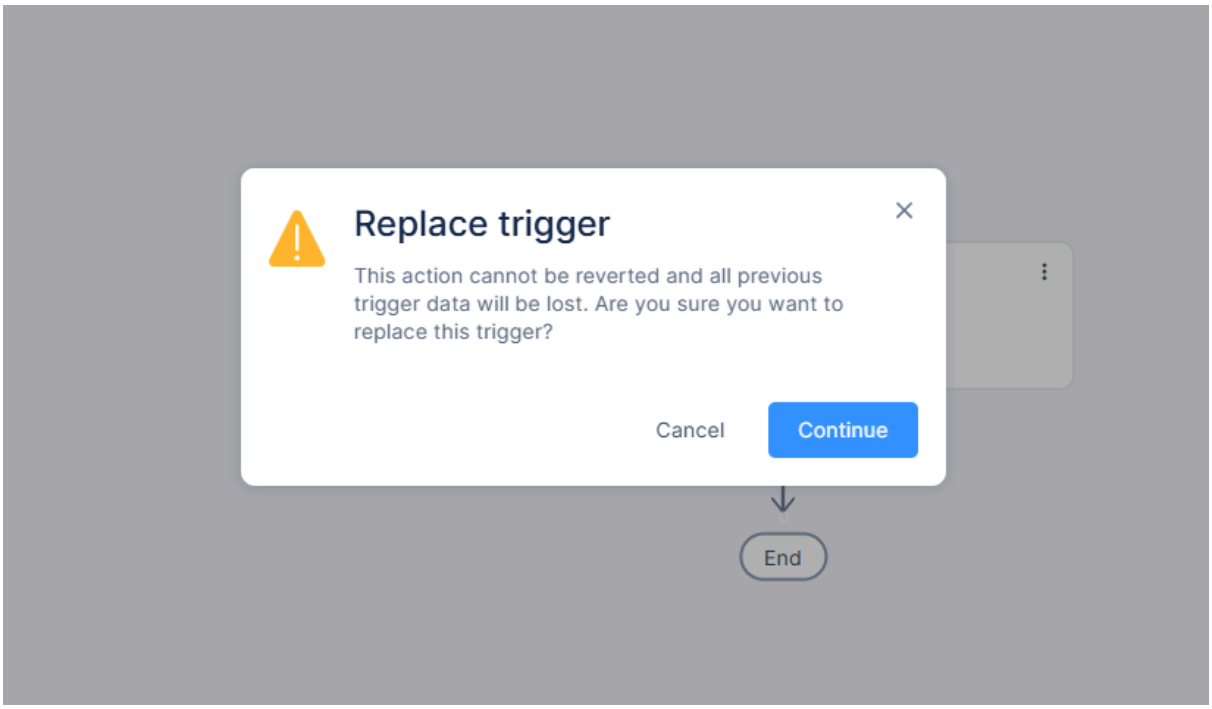
1. Open Automation, click ⋮ and select **Replace Trigger**.



2. Selected **Webhook Trigger**, click **Add**.



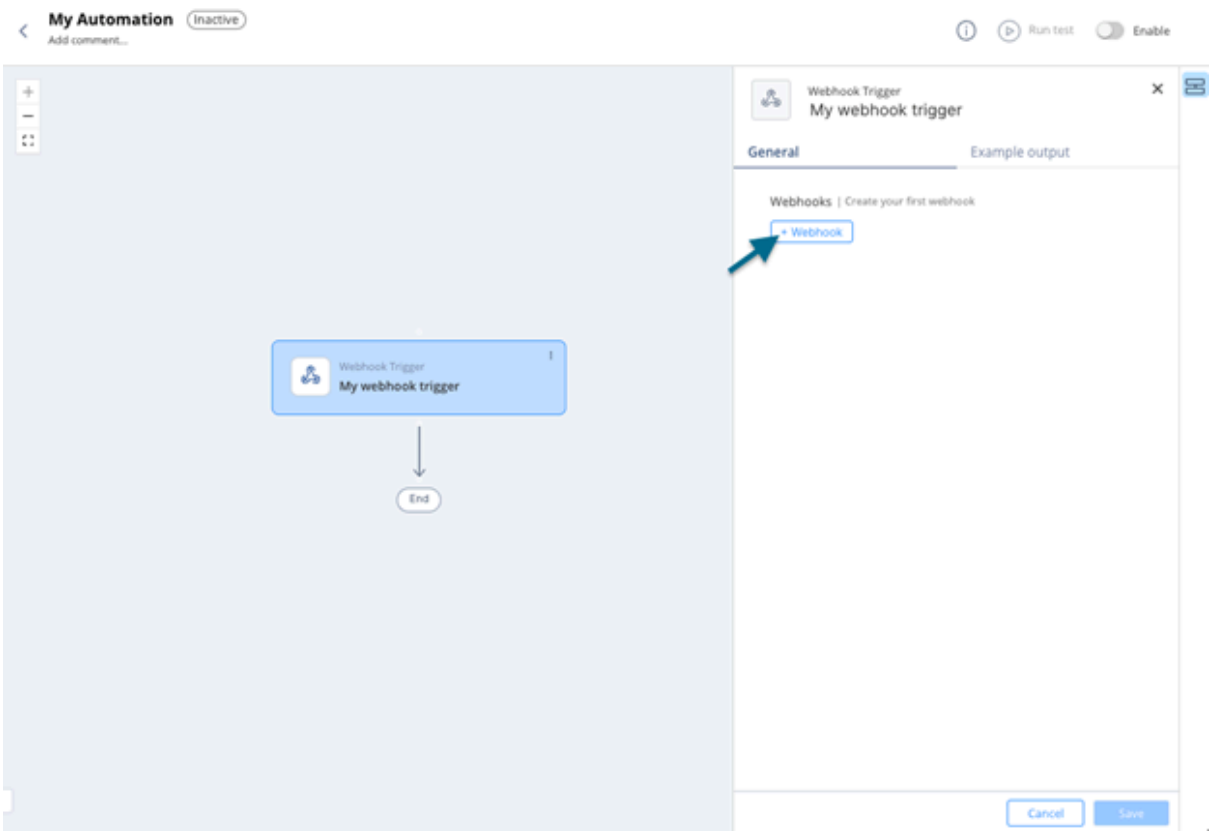
3. Click **Continue** to replace the trigger.



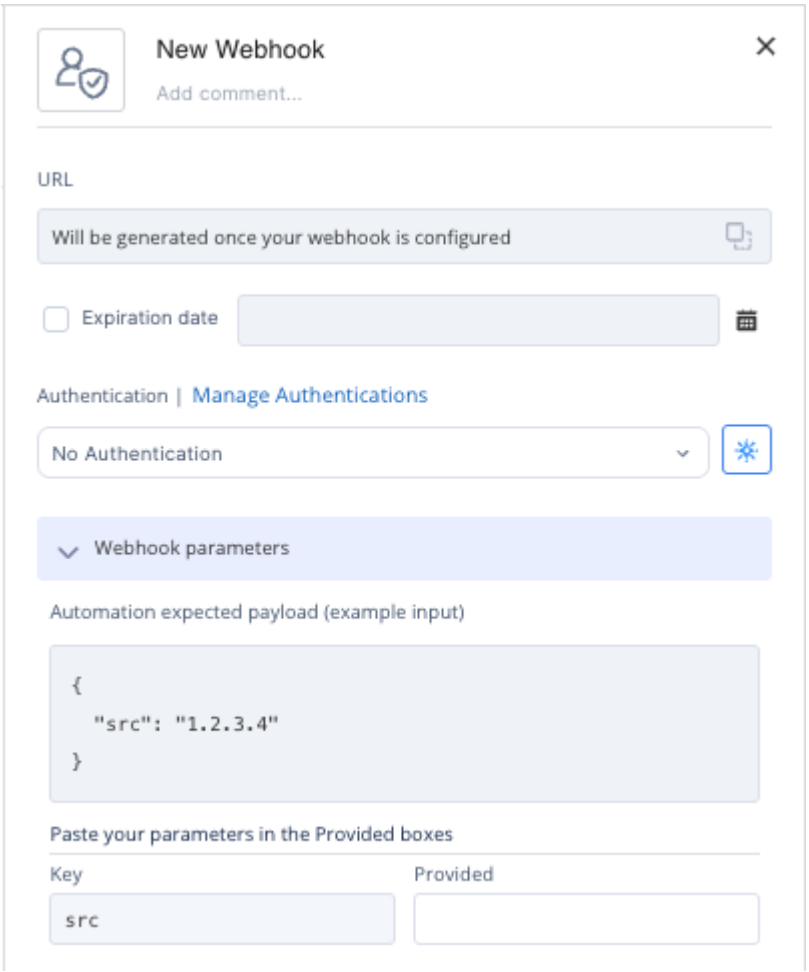
A warning message appears

Note - Replacing a trigger permanently deletes all previous trigger data. This action cannot be undone.

4. In the **General** tab, click **+Webhook**.



5. After you use a field from the trigger's example output in a subsequent step, you can add field mapping to it under **Webhook Parameters**.



6. Click **Create**.

Related information
Replace Trigger *(on page 141)*

6.8.4. Creating a Webhook

This topic describes how to create a webhook, configure its URL and expiration date, and optionally apply authentication. It also provides guidance on managing exposed or expired webhook URLs.

Webhook URL

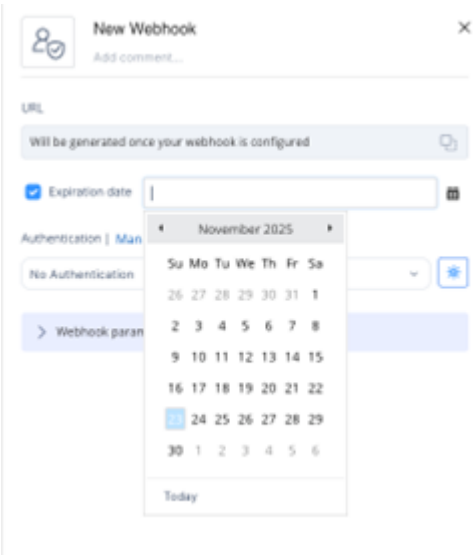
- Each webhook is assigned a unique URL when the webhook is created.
- Once generated, you can copy and use this URL in any service or application that needs to trigger the webhook.

  Notes -

  - The URL cannot be modified.
  - This URL is sensitive and should be protected. Do not share or expose it-anyone who has access to the URL can trigger the webhook.
- If the URL is exposed:
  - Clone the webhook.
  - Update any integrations to use the new webhook's URL.
  - Delete the old webhook.

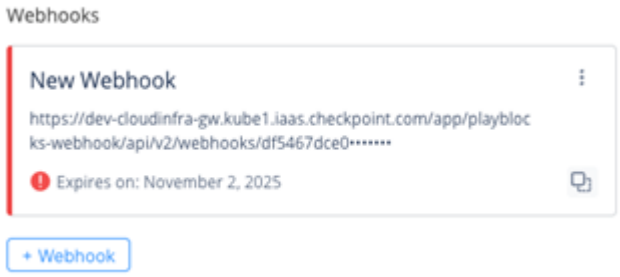
Expiration Date

- (Optional) Set an expiration date by selecting Expiration Date and choosing the desired date.



- Seven days before a webhook expires, and again on the expiration date, you receive a reminder email.

- In the portal, expired webhooks are marked in the automation webhooks list.



- If a webhook expires:
  - Clone the webhook.
  - Update any integrations to use the new webhook's URL.
  - Delete the old webhook.

Authentication

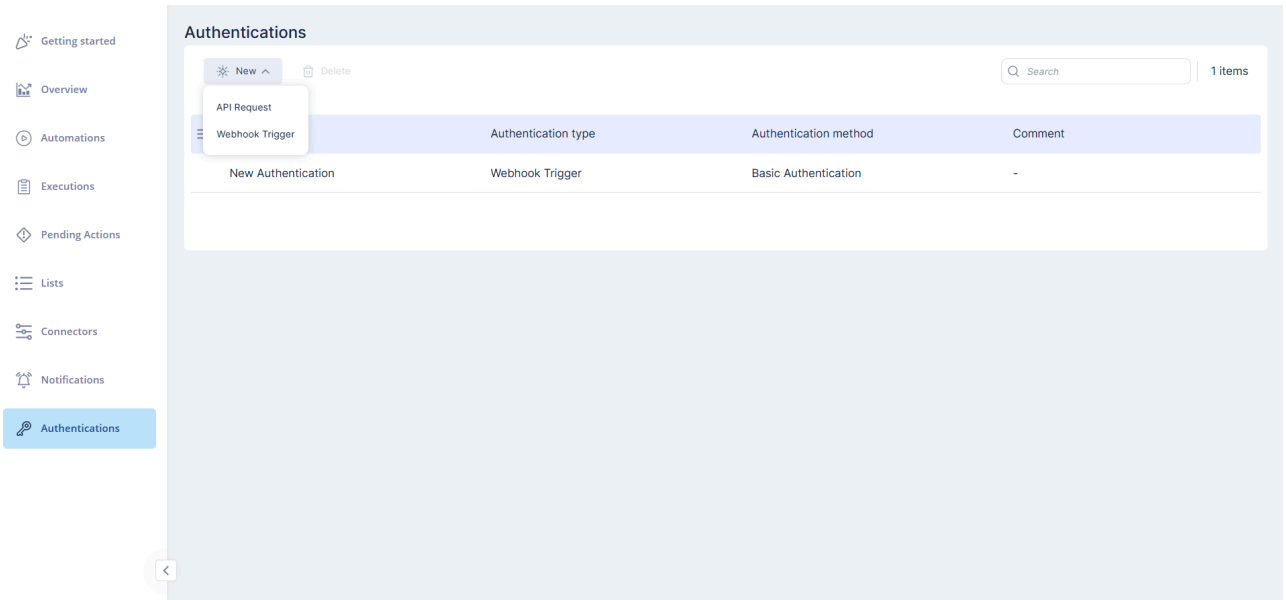
A webhook may include authentication. Supported types:

- **Basic Authentication** (username and password)
- **Custom Authentication** (custom key-value pair)

We recommend adding authentication for security. Even if someone obtains the webhook URL, they still need valid credentials.

Select an existing authentication from the drop-down list or create a new one.

Click Manage Authentications to open the Authentications page, where you can view details or edit existing authentication settings.



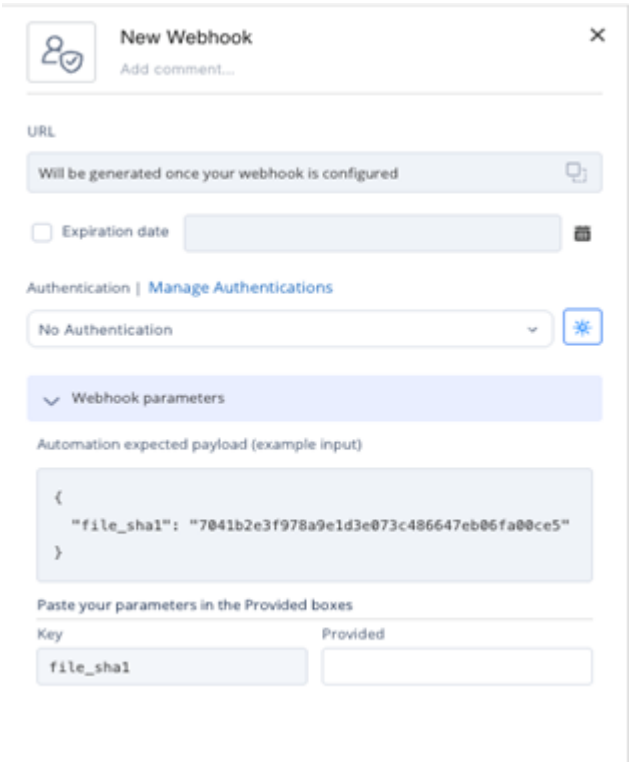
For more information, see Authentications *(on page)*.

6.8.5. Webhook Parameters - Mapping Webhook Payload Fields

This topic explains how to map incoming webhook payload fields to the expected structure using Webhook Parameters. It describes scenarios where field names or formats differ from the Example Output.

When configuring a webhook:

- The automation's trigger step may include an Example Output, which defines the expected data structure for subsequent steps.
- In rare cases, the webhook payload sent by the third-party system does not match the format expected by Playblocks.
- Use Webhook Parameters to map fields from the incoming webhook payload to the fields defined in the Example Output:



Note:

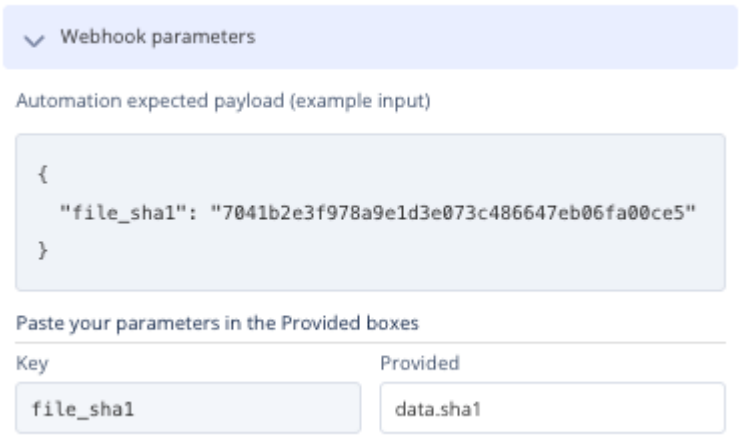
If mapping is not defined, the system assumes identical field names as shown in the example output.

- Mapping ensures that the automation receives the correct data in the correct format.

- Example Scenario
  - The Example Output includes a field named file_sha1.
  - A later step in the automation relies on this field.
  - The third-party system sends a payload in these format:

```
{
                "data": {
                "sha1": "7041b2e3f978a9e1d3e073c486647eb06fa00ce5"
                }
                }
```

- Since the incoming payload uses a different structure and field name, create a mapping so the automation receives the value in the expected file_sha1 field.
- Steps to Create a Mapping
  - Go to Webhook Parameters in the webhook configuration.
  - Map the incoming field (data.sha1) to the expected field (file_sha1).



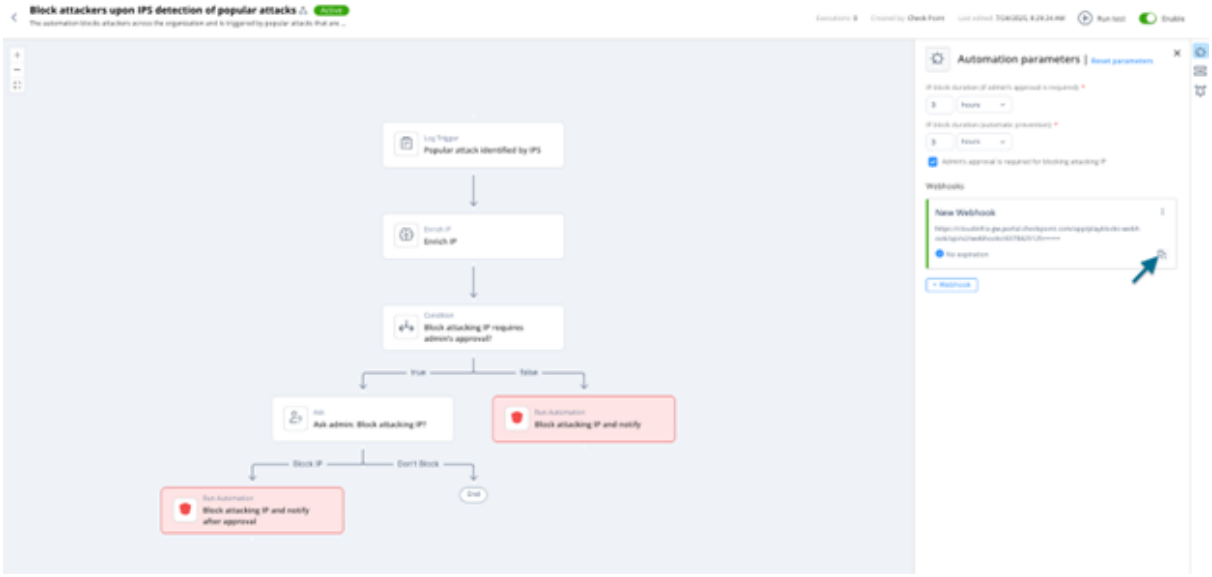
6.8.6. Using a Webhook

This topic describes how to use a webhook after it has been created. It provides step-by-step instructions for configuration and usage.

About this task:
Once the webhook is created, complete the following steps.

Procedure:

1. Enable the automation.
2. Copy the webhook URL from the webhook card.



> **Note:** The webhook URL is sensitive. Do not share or expose it. Anyone with access to the URL can trigger the webhook.

3. Use the URL as the POST request endpoint in the third-party system.
4. Configure these in the third-party system.
    a. Authentication (if defined)
    b. Webhook payload
5. Test the webhook by sending a sample payload from the third-party system to confirm the automation triggers correctly.

What to do next:

For Webhook Trigger step schema definitions, see Appendix G - Using Custom Automation Step Schemas *(on page 286)*.

For webhook REST APIs, see Appendix H - Webhooks and Authentications *(on page 304)*.

6.9. Authentications

6.9.1. Creating an Authentication

This task describes how to create a new authentication. It guides users through selecting authentication types and configuring related options.

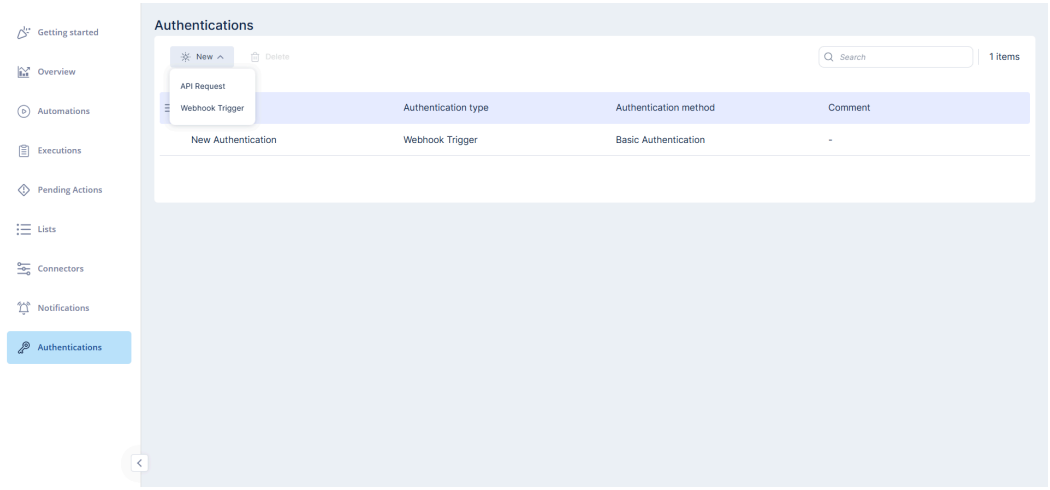
About this task:

Authentications are used to secure API requests and webhooks. You can view, create, edit, and delete authentications from the **Authentications** page.

To create a new authentication:

Procedure:

1. On the **Authentications** page, click **New**.
2. Select the authentication type.



   - API Request
   - Webhook Trigger
3. Enter the required details for the selected type.
4. Click **Save** to create the authentication.

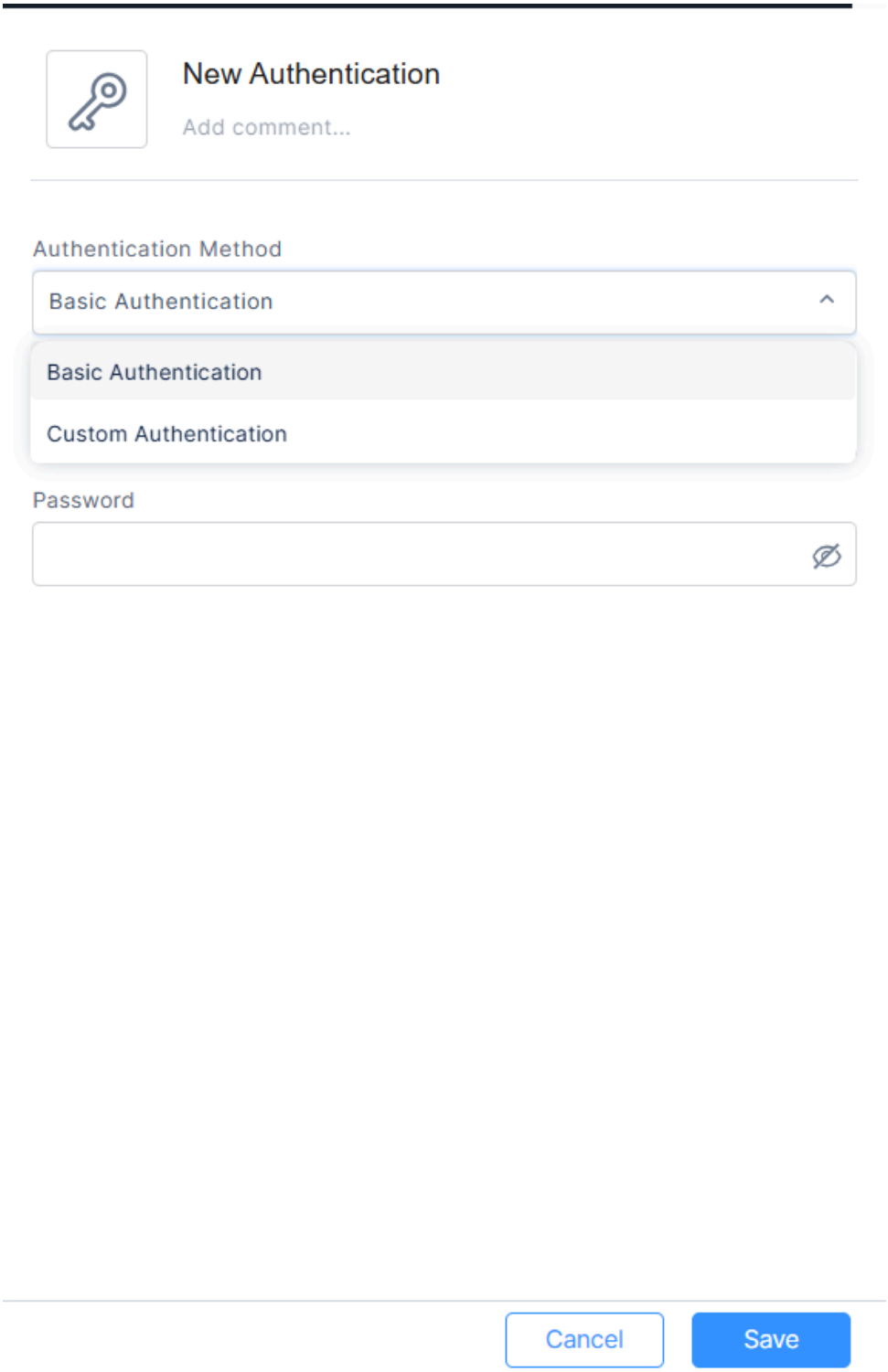
> **Note:**
>
> We recommend adding authentication for security. Even if someone obtains the webhook URL, they still need valid credentials.

5. You can also create other authentication types.
   - Webhook Trigger authentication directly from a webhook's configuration (see Creating a Webhook *(on page 206)*).
   - An API Request authentication from within the API Request step (see API Request *(on page 141)*).

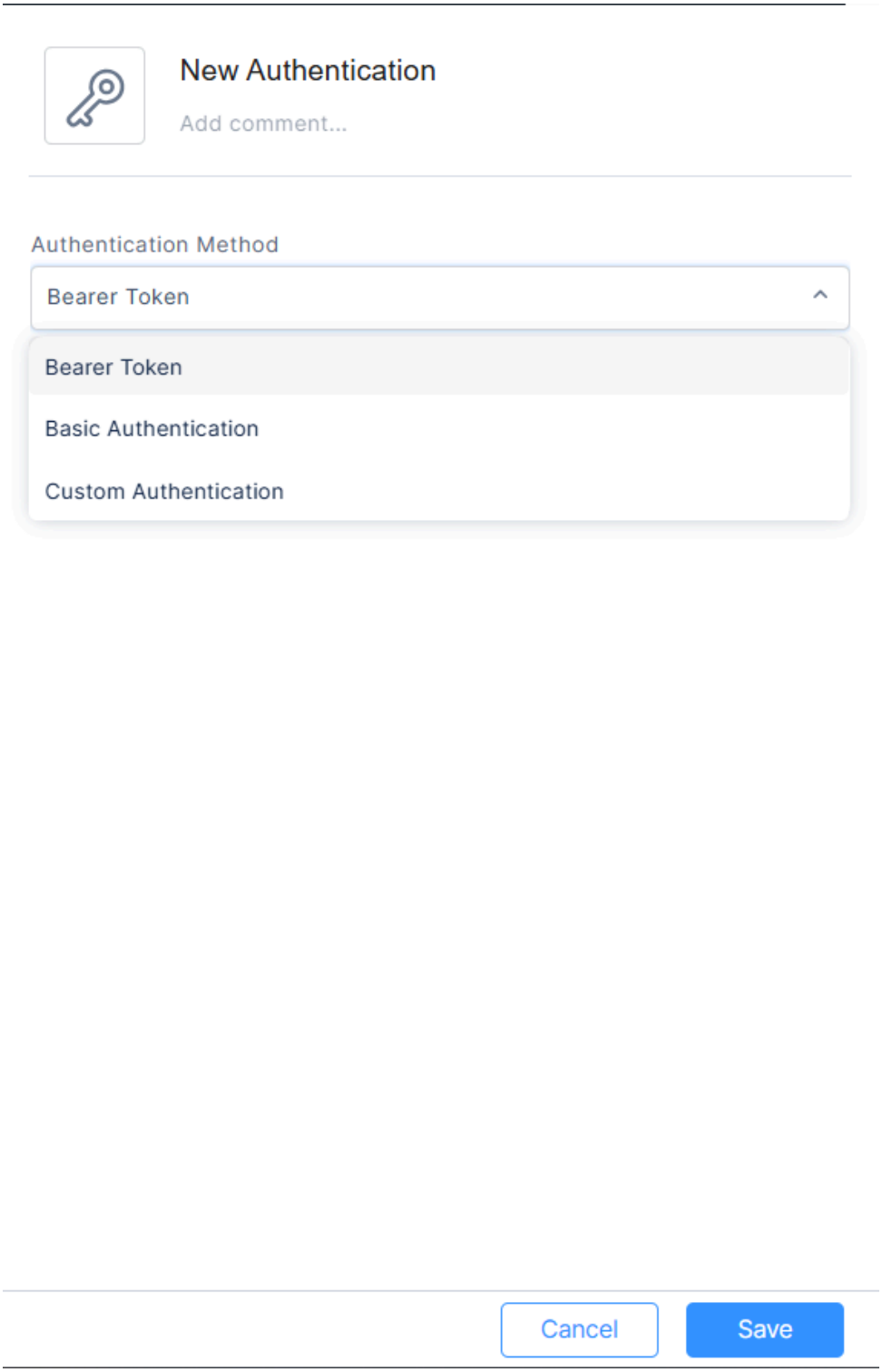
6.9.2. Supported Authentication Methods

This topic lists supported authentication methods for webhook triggers and API requests. It describes available basic, custom, and token-based authentication options.

- Webhook Trigger
  - **Basic Authentication** (username and password)
  - **Custom Authentication** (custom key-value pair)



- API Request
  - **Bearer Token**
  - **Basic Authentication** (username and password)
  - **Custom Authentication** (custom key-value pair)

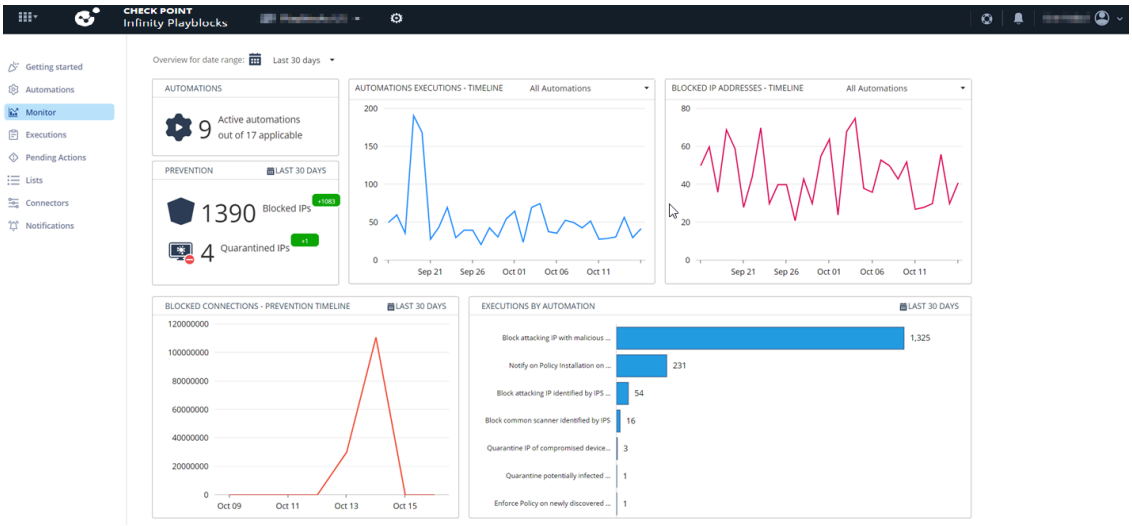


7. Monitor

This topic describes the Monitor page, which displays statistics and visual widgets showing automation activity and prevention data. It summarizes the available monitoring views and their functions.

The **Monitor** page shows statistics about the automations.

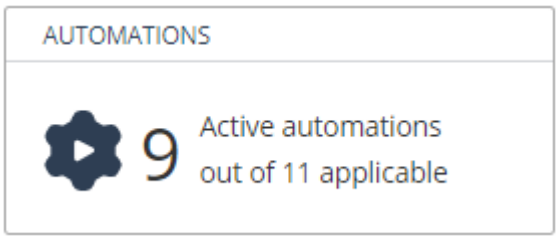
To view the **Monitor** page, access **Playblocks** and click **Monitor**.



Note:

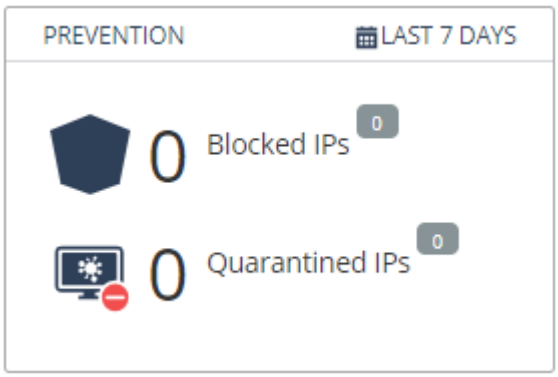
Make sure that you have enabled **Log Sharing** in On-boarding the On-premises Check Point Security Gateway *(on page 21)*.

Automations



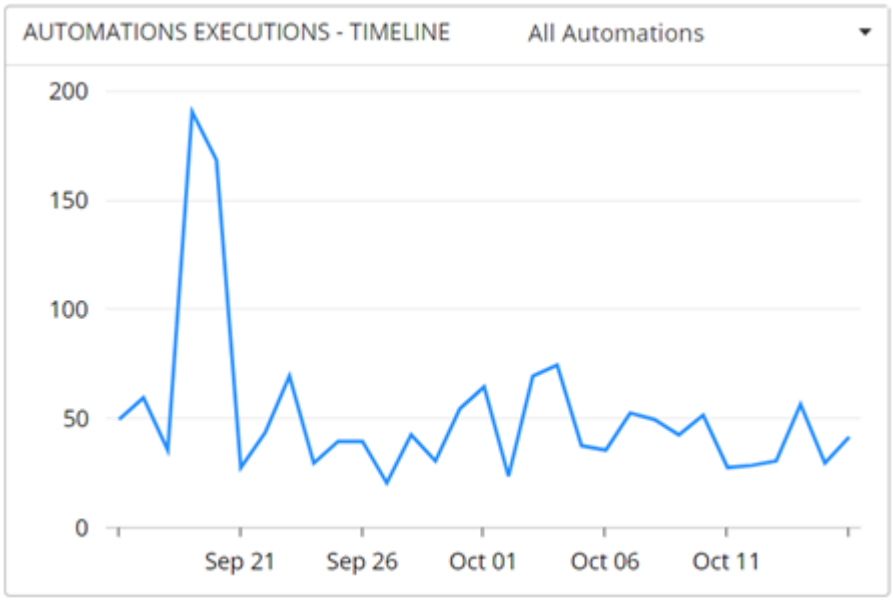
The **Automations** widget shows the active automations out of the available automations in Playblocks.

Prevention



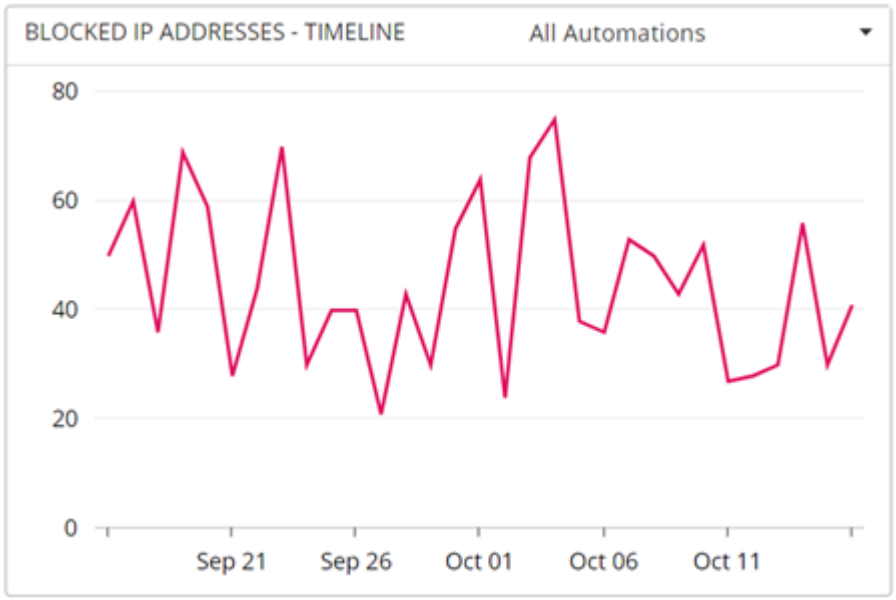
The **Prevention** widget shows the number of blocked and quarantined IP addresses. For more information, see Lists *(on page 220)*.

Automations Executions - Timeline



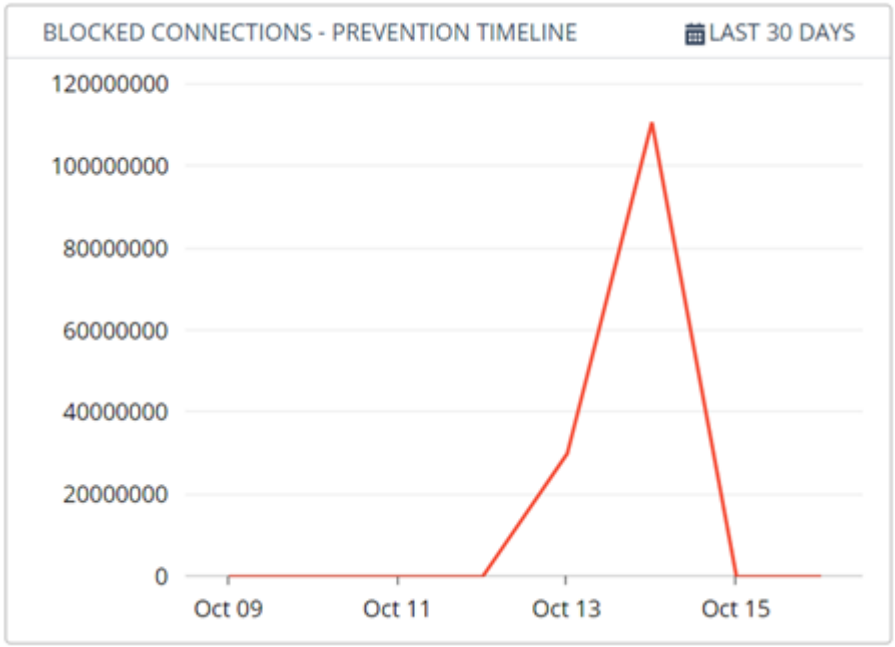
The **Automations Executions - Timeline** widget shows the line graph of the automation executioned over time.

Blocked IP Addresses - Timeline



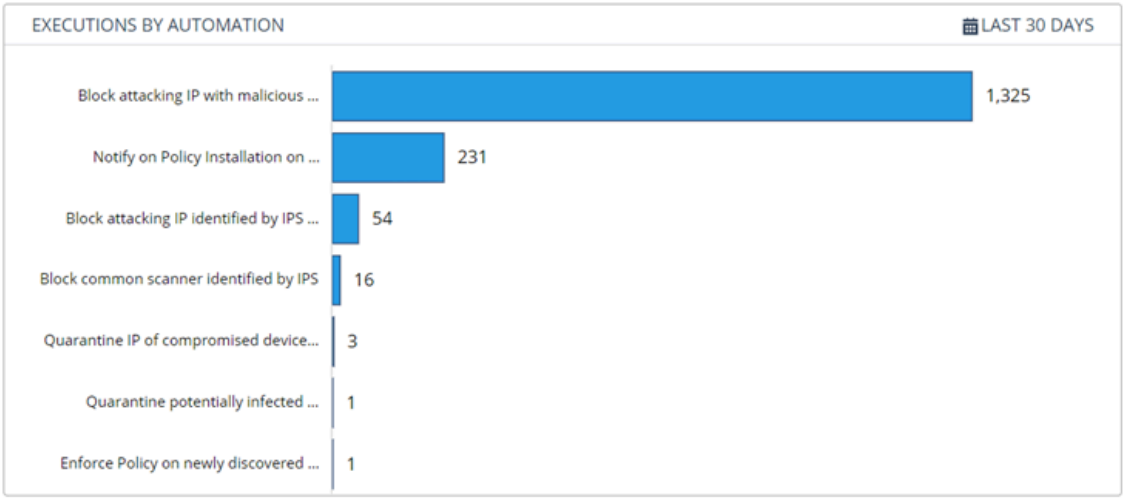
The **Blocked IP Addresses - Timeline** widget shows the line graph of blocked IP addresses over time.

Blocked Connections - Prevention Timeline



The **Blocked Connections - Prevention Timeline** widget shows the line graph of blocked connections over time.

Executions by Automation



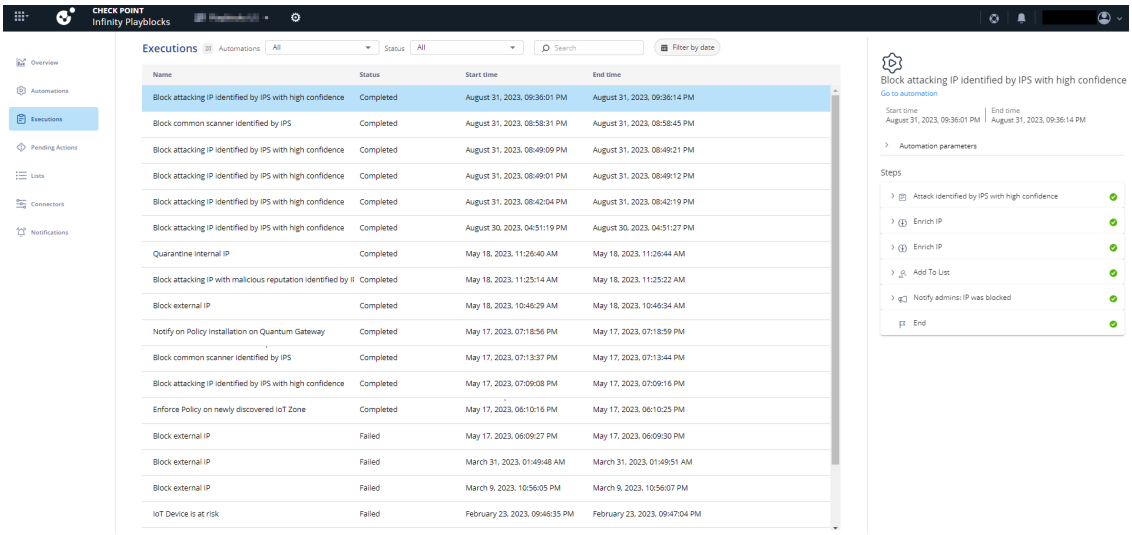
The **Executions by Automation** widget shows the total number of executions performed by each automation.

8. Executions

This topic describes the Executions page and how to access it. It provides an overview of the information shown for executed automations.

The **Executions** page shows a log of all the executed automations in your account. It also shows the parameters and all the steps in the output of an execution.

To view the **Execution** page, access **Playblocks** and click **Execution**.



Column	Description
Name	Execution name.
Status	Status of the execution: • In progress • In progress (pending action) • Completed • Failed
Start time	Date and time when the execution started.
End time	Date and time when the execution completed.

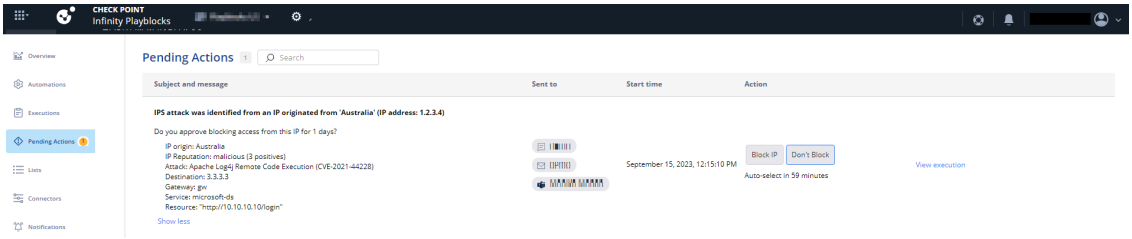
9. Pending Actions

This topic describes the Pending Actions page, which lists automation executions awaiting approval. It also explains how to access this page in Playblocks.

The **Pending Actions** page shows the list of executions awaiting approval from the Administrator. You can also reject or revert an automation.

An execution requires Administrator approval if you select the **Admin's approval is required** checkbox in the Automation Parameters *(on page 211)* page.

To view the **Pending Actions** page, access **Playblocks** and click **Pending Actions**.



Notification details

Column Name	Description
Subject and message	Brief description of the notification sent for the Administrator's approval.
Sent to	Notification recipients.
Start time	Date and time the notification was sent.
Action	Approve or reject the execution.

9.1. Approving, Rejecting or Reverting an Automation Execution

This topic describes how to approve, reject, or revert an automation execution. It provides the steps required to manage pending automation actions.

Procedure:

1. Access **Playblocks** and click **Pending Actions**.
2. Under **Action** column, for example, click **Block IP** to approve or click **Don't Block** to reject.

What to do next:

Note:

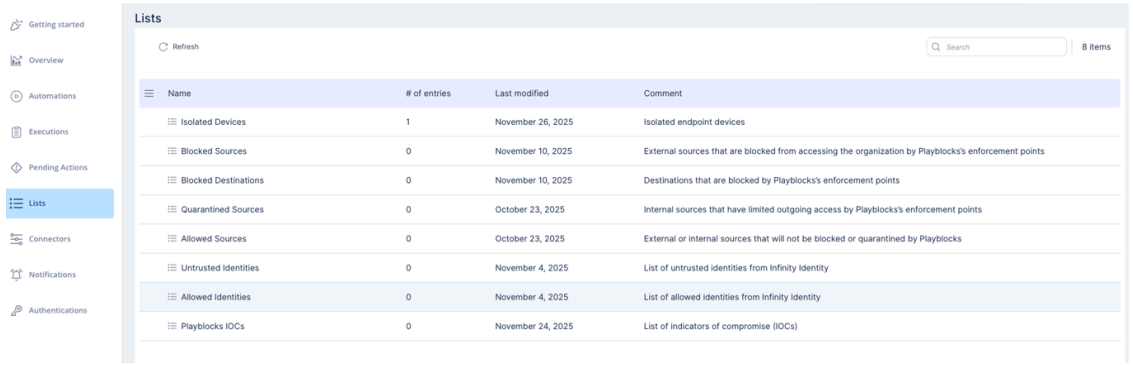
You cannot revert an action from the **Pending Actions** page. The Revert action is only possible through connectors such as Microsoft Teams, Outlook, and so on.

10. Lists

This topic describes the Lists page, which shows various types of destinations, sources, devices, and identities managed by the system. It explains the purpose of each list category.

The **Lists** page shows the list of Blocked Destinations (IP address/subnet), Allowed, Blocked and Quarantined Sources (IP address/subnet) that are either created manually or automatically by Playblocks due to an automation execution.

To view the **Lists** page, access **Playblocks** and click **Lists**.



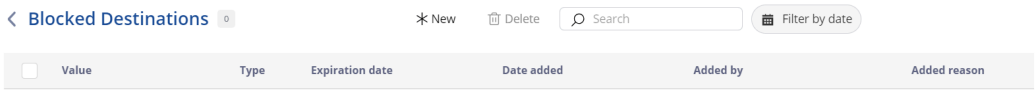
Name	Description
Blocked Destinations	Traffic sent from the organization to the destination IP address/subnet is blocked.
Allowed Sources	Traffic sent from the source IP addresses/subnets is not blocked or quarantined.
Quarantined Sources	Internal IP addresses/subnets are quarantined and cannot communicate with other resources within the organization.
Playblocks IoCs	List of indicators of compromise (IoCs).
Isolated Devices	Isolated Endpoint devices.
Blocked Sources	Traffic sent from these IP addresses/subnets to the organization is blocked.
Allowed Identities	List of allowed identities from Identity and Trust.
Untrusted Identities	List of untrusted identities from Identity and Trust.

10.1. Configuring Lists Manually

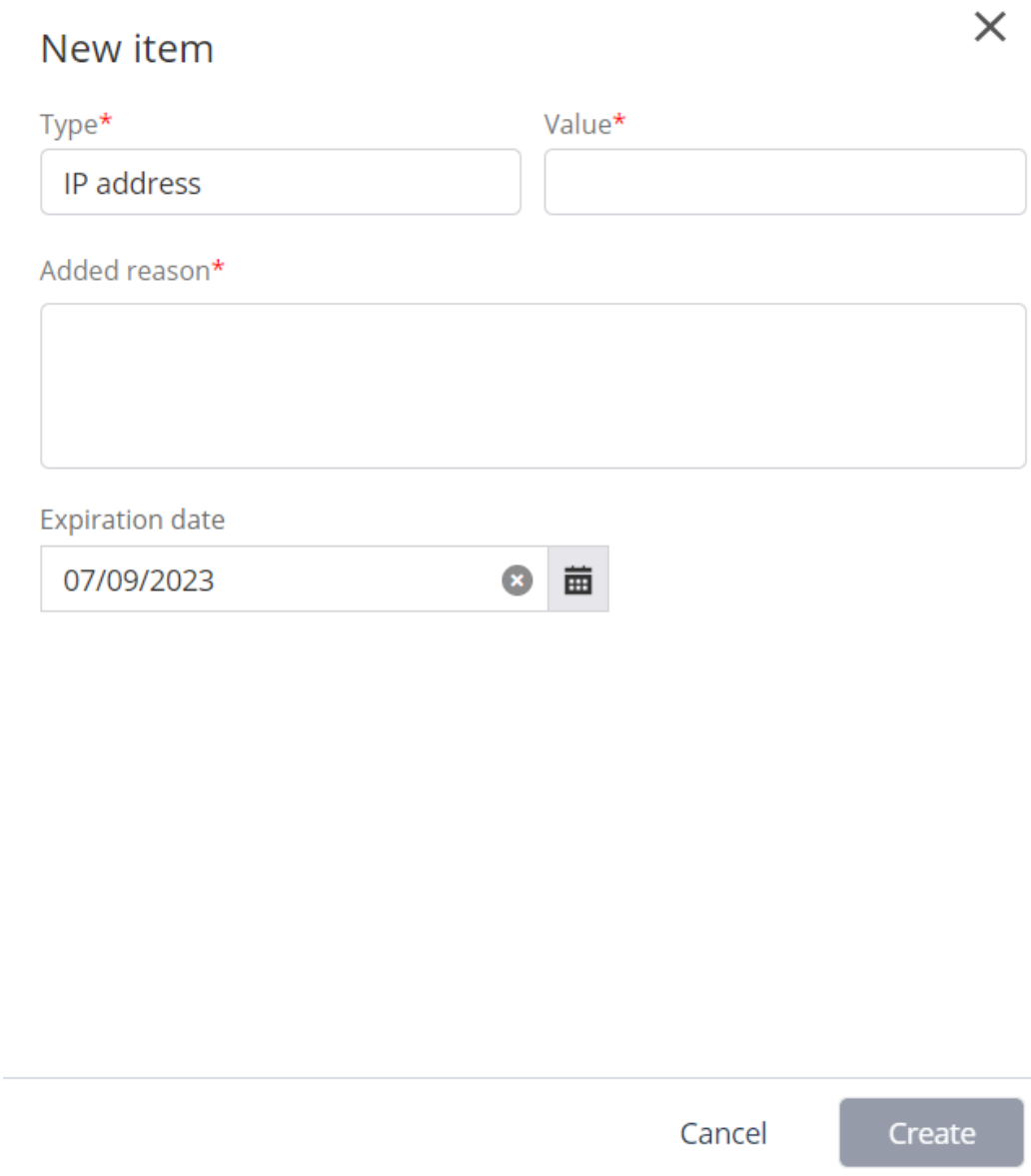
This task describes how to manually configure lists in Playblocks. It guides users through selecting list types, adding items, and managing entries.

Procedure:

1. Access **Playblocks** and click **Lists**.
2. Select a list.
    - **Blocked Destinations**
    - **Allowed Sources**
    - **Quarantined Sources**
    - **Playblocks IoCs**
    - **Isolated Devices**
    - **Blocked Sources**
    - **Allowed Identities**
    - **Untrusted Identities**
3. Click **New**.



4. Enter these.
    a. In the **Type** list, select **IP address**, **Subnet**, or **Range**.
    b. In the **Value** field, enter a value.
        - For example, for subnet, enter *10.10.11.0/24*.
        - For example, for IP range, enter *10.11.12.0-10.11.12.123*.
    c. In the **Added reason** field, enter the reason for adding.
    d. Set the **Expiration Date**.



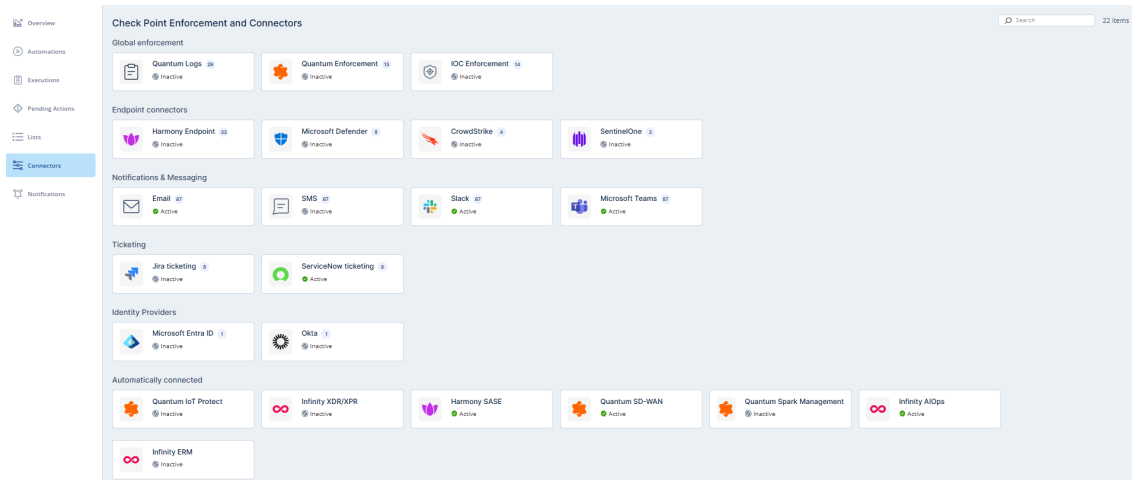
5. Click **Create**.
6. To delete, select the IP address and click **Delete**.

11. Connectors

This topic describes connectors used in Playblocks and explains how they support automatic incident response and collaboration. It also shows how to access the Connectors page and identifies automatically connected products.

Playblocks uses connectors to enforce automatic incident response actions and collaborative tools to communicate the details of the incident and the action taken.

To view the **Connectors** page, access **Playblocks** and click **Connectors**.



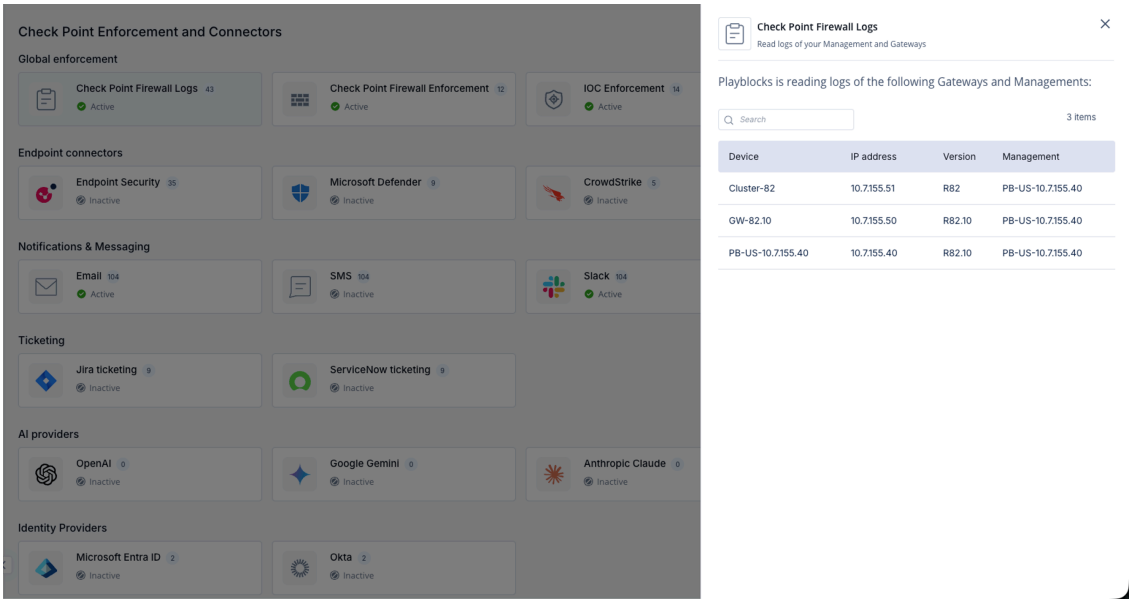
Automatically Connected

Automatically connected connectors indicate which products are connected to the user's portal. They cannot be edited.

11.1. Check Point Firewall Logs

This topic describes the Check Point Firewall Logs interface and the information it displays about connected management servers and firewalls.

Check Point Firewall Logs are relevant to Check Point Security Management Server and (S1C). It indicates Playblocks can access the logs of the Security Management Server and the Check Point Firewalls connected to (S1C) or on-premises Security Management Server. Check Point Firewall Logs shows the name, IP address, version, and the Management Server of the Check Point Firewalls and the Security Management Server.



11.2. Check Point Firewall Enforcement

This topic describes Check Point Firewall Enforcement and the related supported configurations and objects it adds to the management system. It also outlines prerequisites for on-premises onboarding.

With Check Point Firewall Enforcement, you can select the Check Point Firewalls and Managements through which you want to execute an automation. It lists the Check Point Firewall from both on-premises Security Management Server and (S1C).

For an on-premises Security Management Server, make sure that you have on-boarded the Check Point Firewall. See ../on-boarding-products/on-boarding-products.dita.

Note:

- Check Point Firewall R81 and higher is supported as the enforcer.
- VSX Check Point Firewalls/VSX Clusters are supported with Management on versions R81.20 and higher with Configuration Sharing Take 187. See https://support.checkpoint.com/results/sk/sk177205.
- Check Point Firewalls/Clusters managed with SmartProvisioning are not supported.

Playblocks adds these network objects to your Security Management Server:

- **Allowed Sources** - External or internal resources that are not blocked by Playblocks.
- **Blocked Sources** - External resources that are blocked from accessing the organization by Playblocks's enforcement points.
- **Blocked Destinations** - External or internal destinations that are blocked by Playblocks's enforcement points.
- **Quarantined Sources** - Internal resources that have limited outgoing access by Playblocks's enforcement points.

- **Playblocks DataCenter** - Generic Data Center that allows dynamic enforcement of Playblocks on Check Point Firewalls.
- **Playblocks Policy** - UserCheck Interaction. A block page appears in the browser in case the device is in quarantine. You can customize this page in SmartConsole.

It also creates a predefined Access Policy Layer called **Automated Remediation**. This layer is added all your security policies and installed on the selected Check Point Firewalls.

11.2.1. Identity and Trust Enforcement

This topic describes Identity and Trust Enforcement, its related network objects, and the procedures to enable and configure Check Point Firewall Enforcement. It provides step-by-step instructions for managing enforcement and automation settings.

About this task:

Identity and Trust Enforcement enables you to control and restrict access from non-compliant devices by leveraging real-time identity and compliance data.

Note:

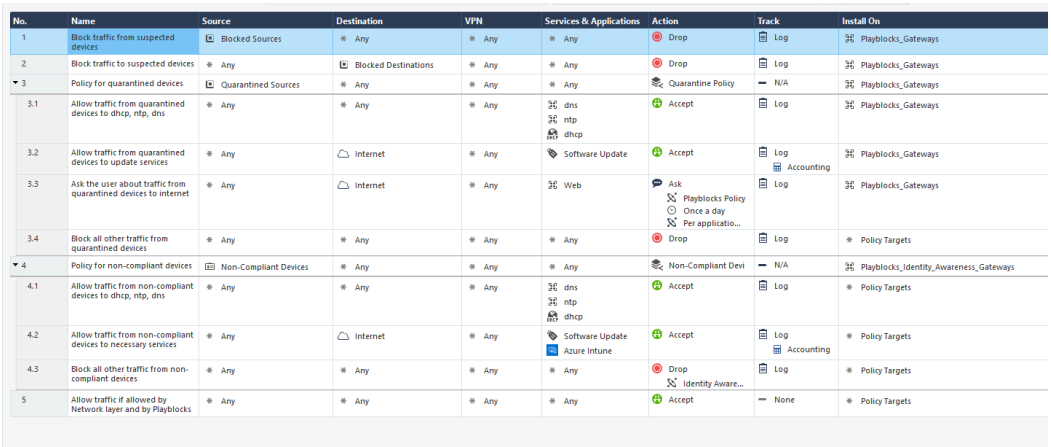
- Check Point Firewall R82 and higher is supported as the enforcer.
- Identity and Trust Enforcement is available only on Check Point Firewalls with the Identity Awareness blade.

Playblocks adds these network objects to your Security Management Server:

- **Not Compliant Devices Policy** - An access layer for controlling traffic from non-compliant devices.
- **Identity Awareness Policy** - UserCheck Interaction. A block page that appears in the browser for non-compliant devices.
- **Not Compliant Devices** - Access role based on the **Not_Compliant_Devices** identity tag which provides access to the list of non-compliant devices from Identity and Trust.

Note:

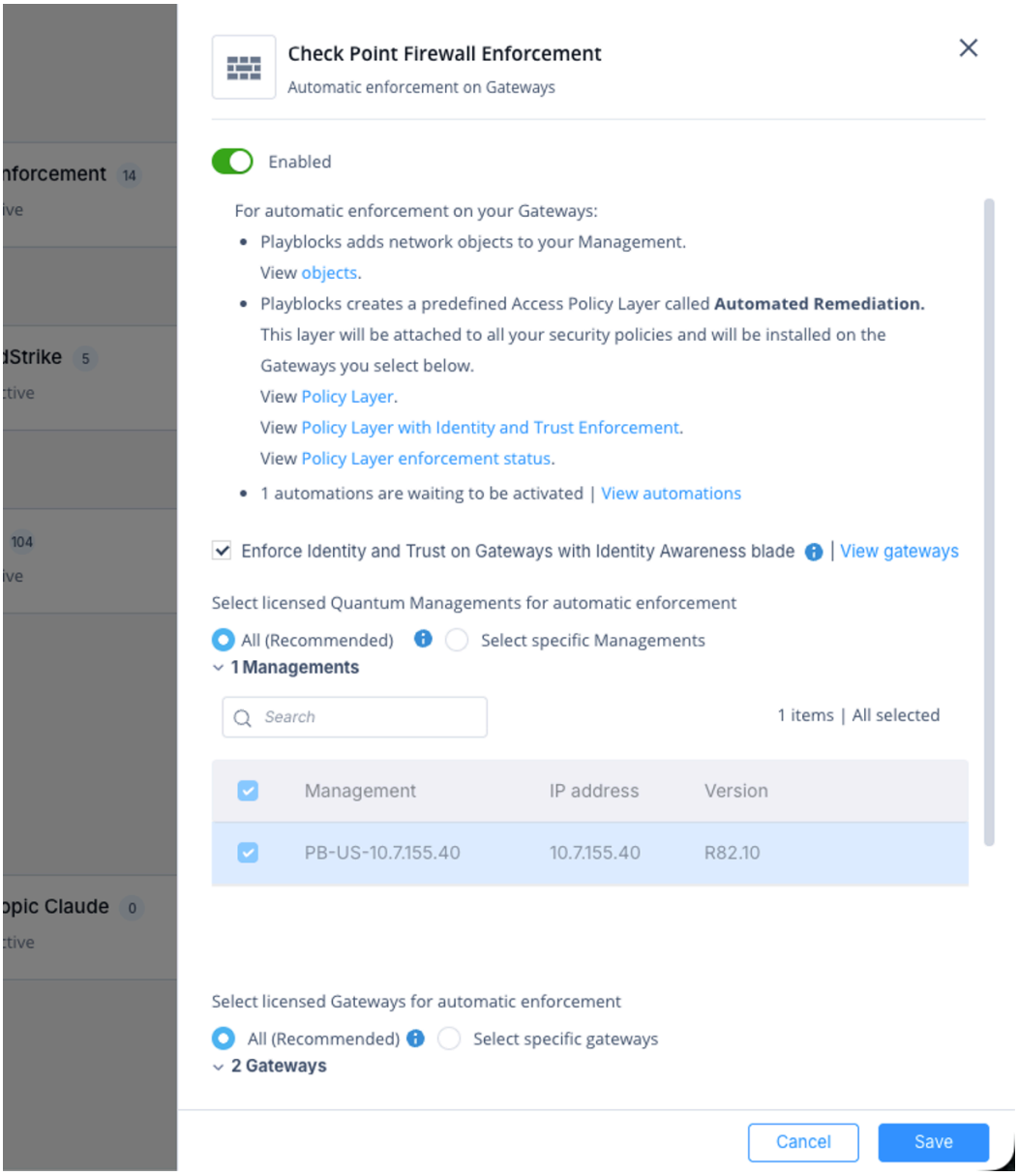
Not_Compliant_Devices is an identity tag used to identify non-compliant devices.



To enable Identity and Trust Enforcement:

Procedure:

1. Access **Playblocks** and click **Connectors**.
2. Select **Check Point Firewall Enforcement**.
3. Turn on the **Enabled** toggle button.



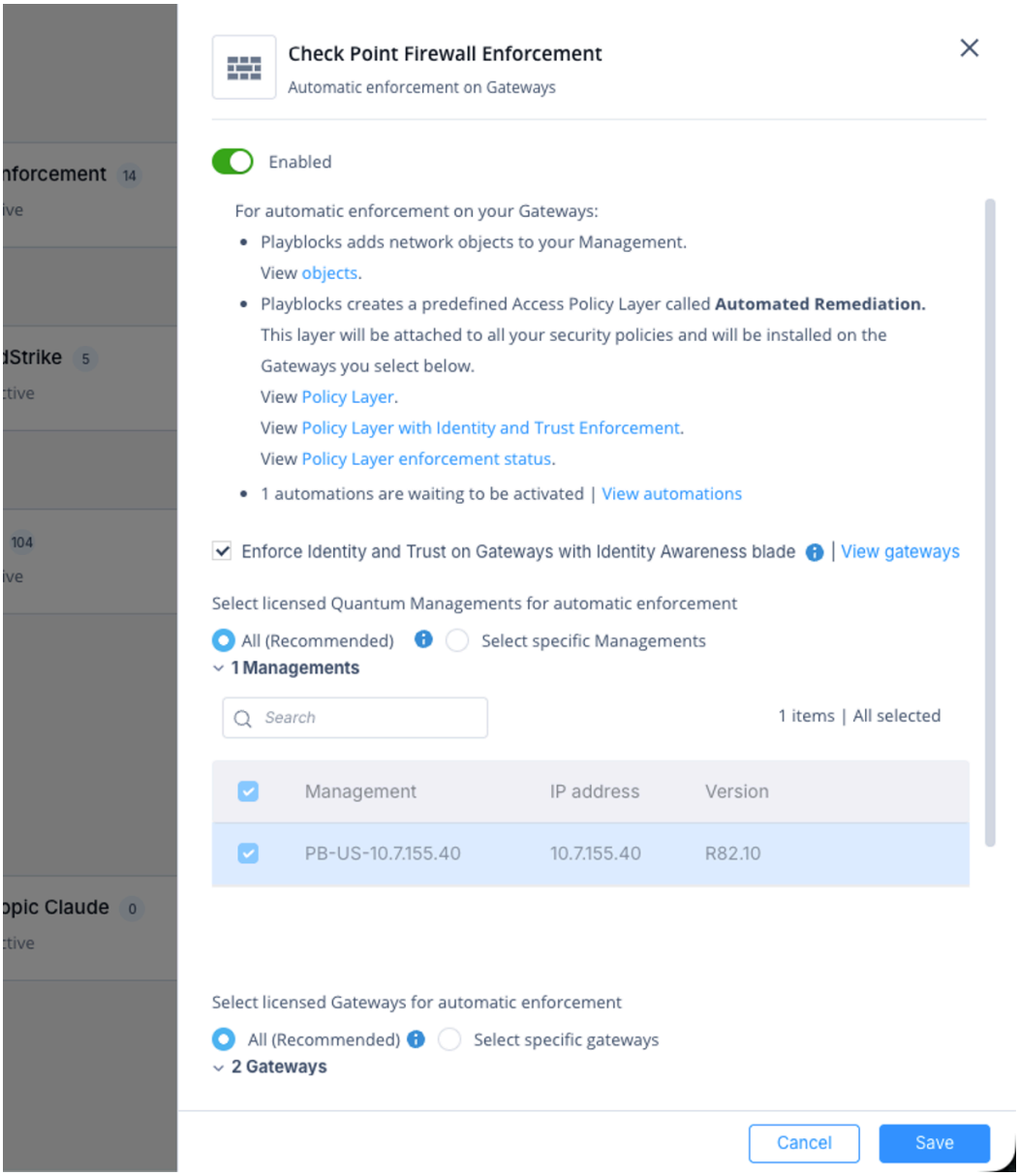
4. Select the **Enforce Identity and Trust on Gateways with Identity Awareness blade** checkbox.
5. Click **View Gateways** to see gateways applicable for the enforcement.
6. To execute the automation on all the Security Gateways, click **All (Recommended)**.

   In addition, this automatically executes the automation on a new Security Gateway with Identity Awareness blade detected by Playblocks.
7. To manually select the specific gateways, click **Select specific Managements**, and then select the gateways.
8. Click **Save**.

What to do next:

To select the Check Point Firewall Management to add to Check Point Firewall Enforcement:

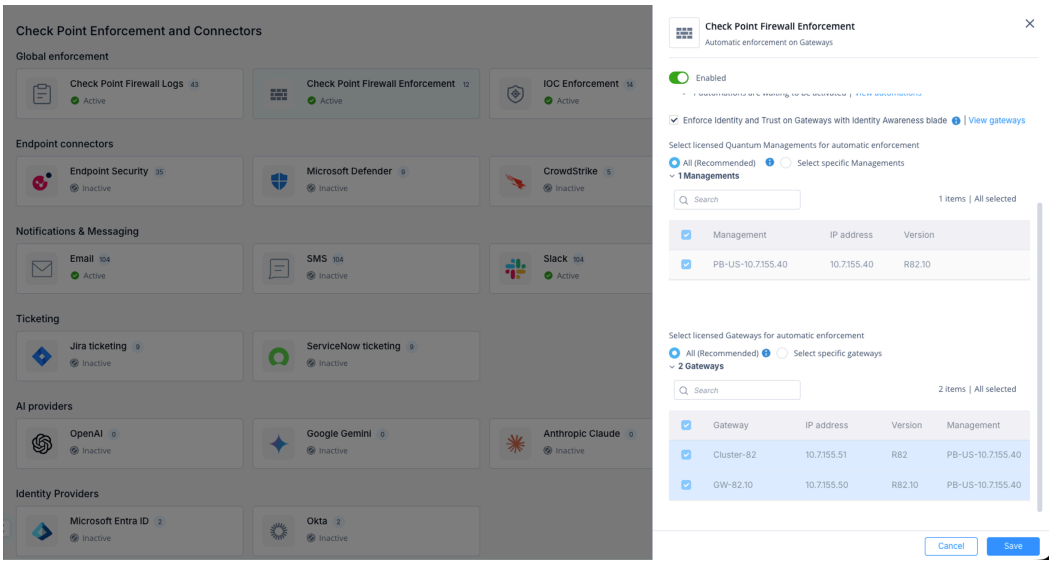
1. Access **Playblocks** and click **Connectors**.
2. Select **Check Point Firewall Enforcement**.



3. Turn on the **Enabled** toggle button.
4. To add all Check Point Firewall Managements to Check Point Firewall Enforcement, click **All (Recommended)**. In addition, this automatically enables Check Point Firewall Enforcement on additional management environments that connects to the Check Point Portal Managements.
5. To manually select the specific Check Point Firewall Managements, click **Select specific gateways** and then select the Check Point Firewall Managements.
6. Click **Save**.

To select the Check Point Firewalls to execute the automation:

1. Access **Playblocks** and click **Connectors**.
2. Select **Check Point Firewall Enforcement**.



3. Turn on the **Enabled** toggle button.
4. To execute the automation on all the Check Point Firewalls, click **All (Recommended)**. In addition, this automatically executes the automation on a new Check Point Firewall detected by Playblocks.
5. To manually select the specific Check Point Firewalls, click **Select specific gateways** and then select the firewall.
6. Click **Save**.

11.2.2. Check Point Firewalls and management Configuration Options

This topic describes configuration options for Check Point Firewall Managements and firewall capabilities. It outlines how management connections and configuration sharing affect enforcement behavior.

1. All Check Point Firewalls and All management Configuration
    - Connecting new Check Point Firewall Managements automatically enables Check Point Firewall Enforcement (if you enable Configuration Sharing).
    - The system adds new firewalls to the list of enforcing firewalls automatically.
2. Specific Check Point Firewalls Managements and All Check Point Firewalls Configuration
    - Connecting new Check Point Firewalls Managements do not automatically enable Check Point Firewall Enforcement.
    - You must enable Configuration Sharing and select the new Check Point Firewall Management in the Check Point Firewall Enforcement connector to activate Check Point Firewalls Enforcement.
    - The system adds new Check Point Firewalls connected to the selected Check Point Firewalls Managements to the list of enforcing Firewalls automatically.

3. Specific Check Point Firewalls Managements and Specific Check Point Firewalls Configuration
    - Connecting new Check Point Firewalls Managements do not automatically enable Check Point Firewall Enforcement.
    - You must enable Configuration Sharing and select the new Check Point Firewall Management in the Check Point Firewall Enforcement connector to enable Check Point Firewall Enforcement.
    - You must add new Firewalls to the list of enforcing Firewalls manually.
4. All Check Point Firewalls Managements and Specific Check Point Firewall Configuration
    - Connecting new Check Point Firewalls Managements automatically enables Check Point Firewalls Enforcement if you enable Configuration Sharing.
    - You must add new Firewalls to the list of enforcing Firewalls manually.

11.3. Email

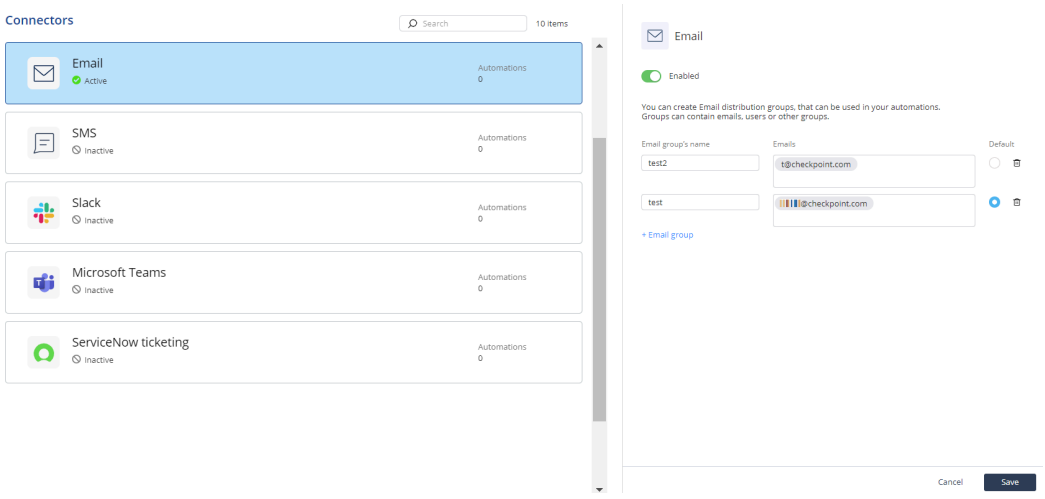
This topic describes how to configure an email connector for sending notifications. It guides you through defining groups, addresses, and default settings.

About this task:

You can specify recipients to receive email notification about the incident and responsive action taken.

Procedure:

1. Access **Playblocks** and click **Connectors**.
2. Select **Email**.



3. Turn on the **Enabled** toggle button.
4. In the **Email group's name** field, enter a name for the group.
5. In the **Emails** field, enter an email address.

   You can add multiple email addresses within a single group.
6. To add another group, click **Email group** and repeat step 4 and 5.

7. Click the **Default** option button to set one email address as the default.

> **Note:**
>
> To send notifications to multiple groups, see Notifications *(on page 257)*.

8. To delete a group, click the delete icon  .

> **Note:**
>
> Deleted groups are also removed from the Notification profile *(on page 257)*.

9. Click **Save**.

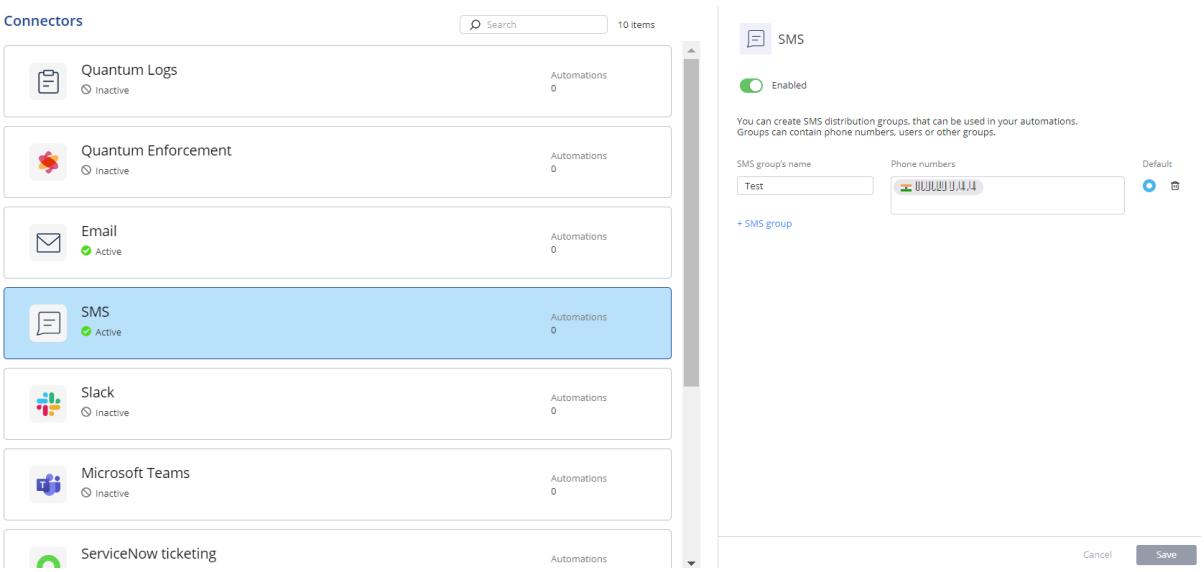
11.4. SMS

This topic explains how to configure an SMS connector to send incident notifications. It provides steps for adding groups, entering phone numbers, and managing defaults.

About this task:
You can specify the mobile phone numbers to receive an SMS with the details of the incident and responsive action taken.

Procedure:

1. Access **Playblocks** and click **Connectors**.
2. Select **SMS**.



3. Turn on the **Enabled** toggle button.
4. In the **SMS group's name** field, enter a name for the group.

5. In the **Phone numbers** field, enter a phone number.

   You can add multiple phone numbers within a single group.

6. To add another group, click **SMS group** and repeat step 4 and 5.

7. Click the **Default** option button to set one phone number as the default.

> **Note:**
>
> To send notifications to multiple groups, see Notifications *(on page 257)*.

8. To delete a group, click  .

> **Note:**
>
> Deleted groups are also removed from the Notification profile *(on page 257)*.

9. Click **Save**.

11.5. Jira Ticketing

This topic describes how to configure a Jira Ticketing connector in Playblocks. It provides step-by-step instructions for setting up access and ticket type parameters.

Before you begin:

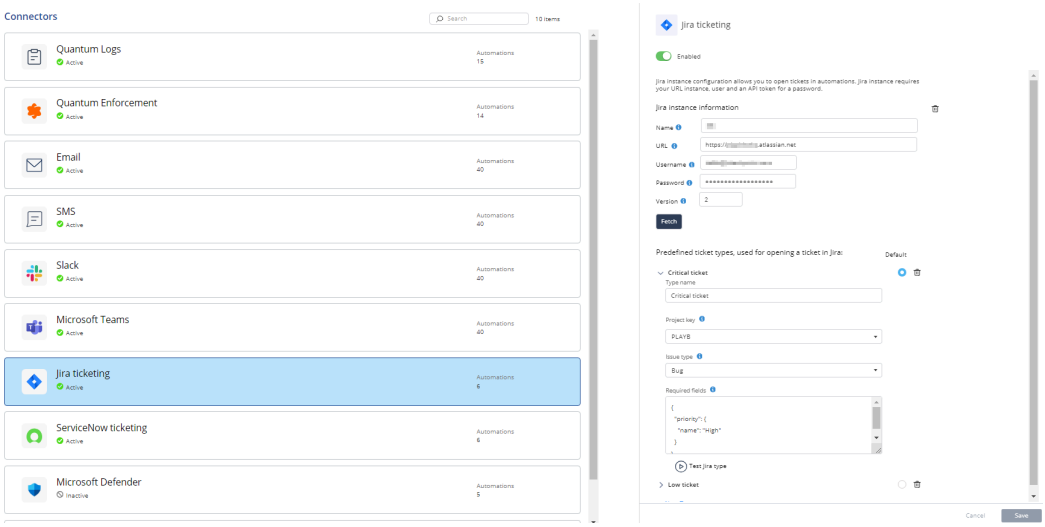
> **Note:**
>
> Before you configure the Jira Ticketing connector, you must create an API token. For more information, see Appendix D - Creating an API Token in Atlassian Account *(on page 275)*.

About this task:

Jira instance configuration allows you to open tickets, get information about tickets, and close tickets.

Procedure:

1. Access **Playblocks** and click **Connectors**.
2. Select **Jira ticketing**.



3. Turn on the **Enabled** toggle button.
4. In the **Name** field, enter a name for the Jira instance in Playblocks. This name will not be used outside of Playblocks application.
5. In the **URL** field, enter the endpoint URL of the Jira instance, for example, `https://<company_name>.atlassian.net`.
6. In the **Username** field, enter email address of a user as username for this instance, for example, `<user_name@domain.com>`.
7. In the **Password** field, enter the API token that you created in your Atlassian account.
8. In the **Version** field, enter the API version of Jira. Default is **2**.
9. Click **Fetch**.

   After authentication, the **Predefined ticket types, used for opening a ticket in jira** section appears.
10. In the **Type name** field, enter a name for the ticket type.
11. From the **Project key** list, select your project key.

    To find your project key:

    a. Log in to your Jira account.

    b. Go to **Projects** > **View all Projects**.

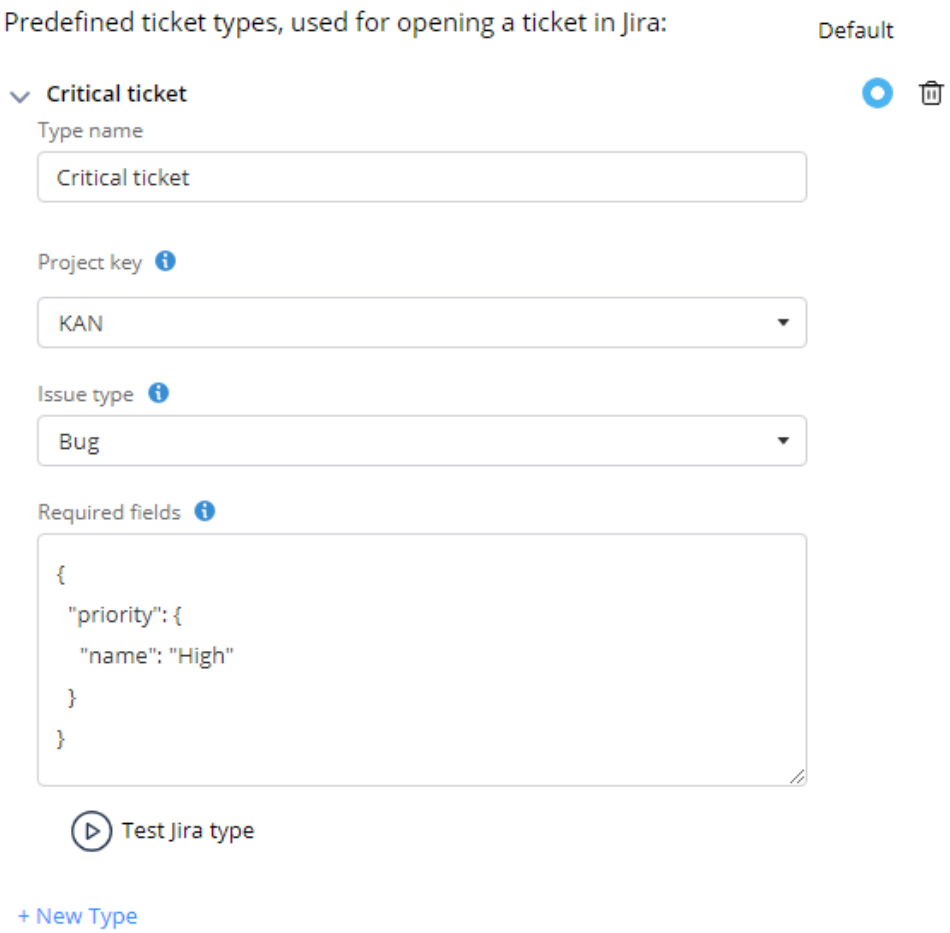
    c. Select the project for which you want to view the project key.

    d. Click **Project Settings**.

    e. Find your project key in the **Key** field.

12. From the **Issue type** list, select the issue.

    For example: Bug, Task, or Epic.



13. In the **Required fields** section, enter the fields required for the ticket type in JSON format.

    For example, if you want to add *priority* as a field for the ticket, then enter `{"priority":{"name":"High"}}`. For more information, see Jira Documentation.

14. To add more ticket types, click **New Type** and repeat steps 10 to 13.

15. Click **Save**.

11.6. Slack

This topic describes how to configure a Slack connector to receive incident details and responsive actions. It guides you through adding and managing Slack channels.

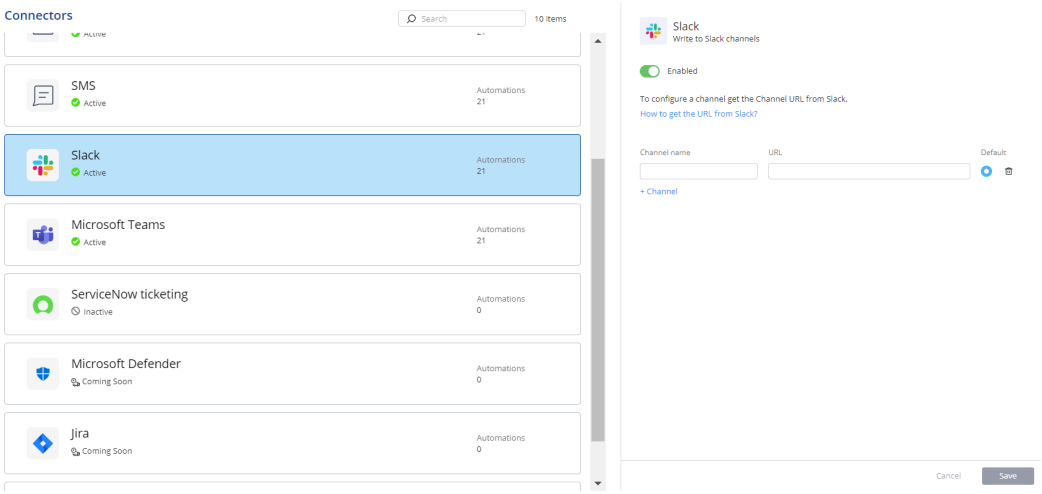
About this task:

You can receive details of the incident and responsive action taken through Slack.

> **Note:**
>
> Before you configure the Slack connector, create an incoming Webhook in your Slack channel. For more information, see Appendix B - Creating an Incoming Webhook in the Slack Channel *(on page 268)*.

Procedure:

1. Access **Playblocks** and click **Connectors**.
2. Select **Slack**.



3. Turn on the **Enabled** toggle button.
4. In the **Channel name** field, enter a channel name.
5. In the **URL** field, enter the Slack channel URL.
6. To add another channel, click **Channel** and repeat step 4 and 5.
7. Click the **Default** option button to set one channel as the default.

> **Note:**
>
> To send notifications to multiple channels, see Notifications *(on page 257)*.

8. To delete a channel, click  .

> **Note:**
>
> Deleted channels are also removed from the Notification profile *(on page 257)*.

9. Click **Save**.

11.7. Microsoft Teams

This topic describes how to configure a Microsoft Teams connector to receive notifications. It provides step-by-step instructions for adding and managing Teams channels.

About this task:

You can receive Microsoft Teams notifications of the incident and responsive action taken.

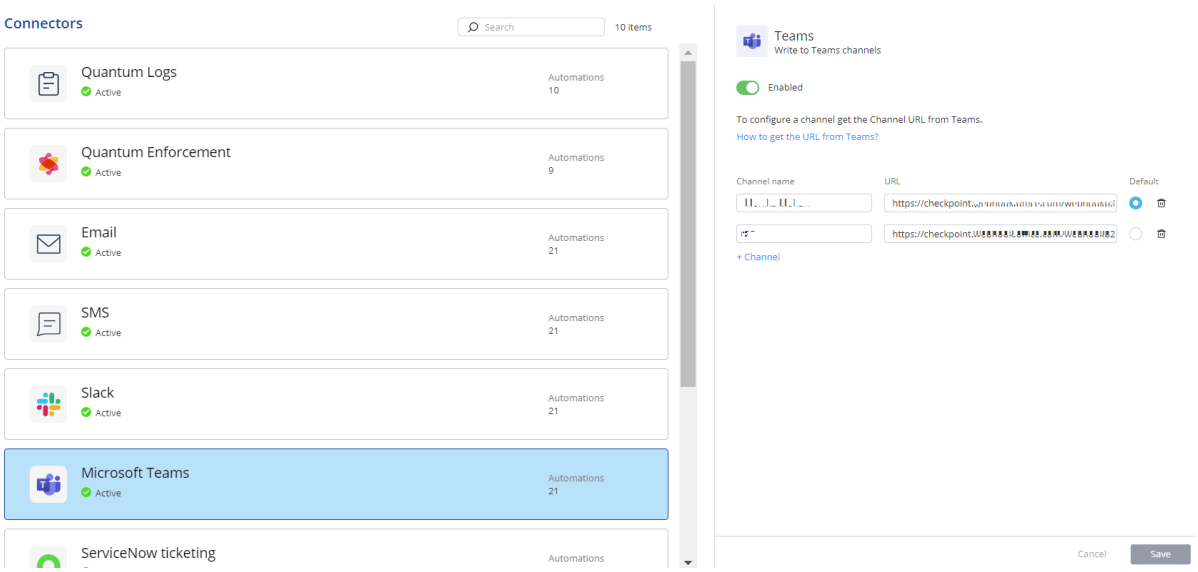
Note:

Before you configure the Microsoft Teams connector, create a workflow for Microsoft Teams Notification. For more information, see Appendix C - Creating Workflow for Microsoft Teams Notification *(on page 271)*

To configure a Microsoft Teams connector:

Procedure:

1. Access **Playblocks** and click **Connectors**.
2. Select **Microsoft Teams**.



3. Turn on the **Enabled** toggle button.
4. In the **Channel name** field, enter a channel name.
5. In the **URL** field, enter the Microsoft Teams channel URL.
6. To add another channel, click **Channel** and repeat step 4 and 5.
7. Click the **Default** option button to set one channel as the default.

Note:

To send notifications to multiple channels, see Notifications *(on page 257)*.

8. To delete a channel, click  .

> **Note:**
>
> Deleted channels are also removed from the Notification profile *(on page 257)*.

9. Click **Save**.

11.8. ServiceNow Ticketing

This topic describes how you can receive incident details and responsive actions through ServiceNow Ticketing. It also provides prerequisite information for configuring the ServiceNow Ticketing connector.

You can receive details of the incident and responsive action taken through ServiceNow Ticketing.

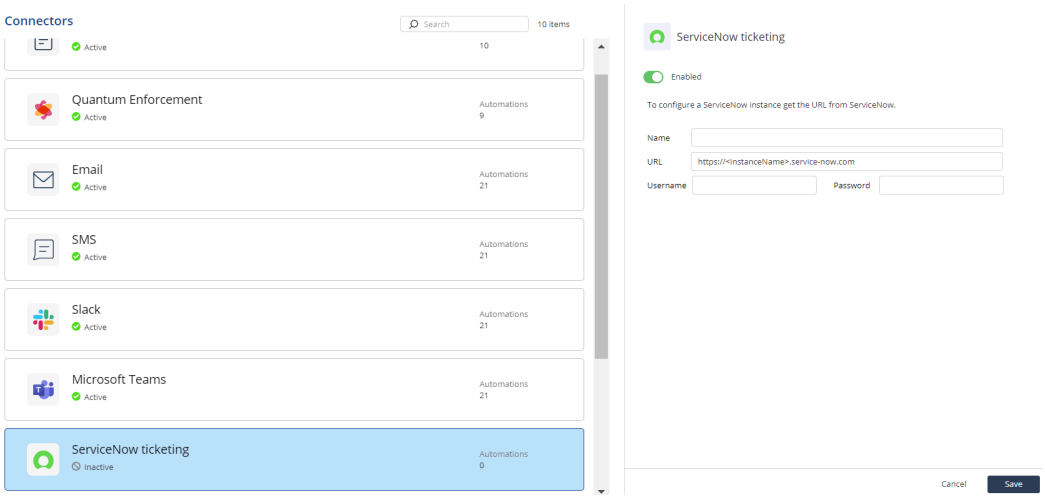
> **Important:**
>
> Before you configure the ServiceNow Ticketing connector, create a ServiceNow account for Playblocks. For more information, see Appendix A - Creating a User with Specific Roles in ServiceNow *(on page 266)*

11.8.1. Configure a ServiceNow Ticketing connector

This task describes how to configure the ServiceNow Ticketing connector in Playblocks. Follow the steps to enable and set up the connector.

Procedure:

1. Access **Playblocks** and click **Connectors**.
2. Select **ServiceNow ticketing**.



3. Turn on the **Enabled** toggle button.
4. In the **Name** field, enter a name.

5. In the **URL** field, enter your ServiceNow URL.
6. In the **Username** and **Password** field, enter the User ID and Password that you created for Playblocks in your ServiceNow account.
7. Click **Save**.

11.9. PagerDuty Alerting

Configure the PagerDuty connector to enable automations to open, acknowledge, and resolve incidents in PagerDuty as part of an automated response.

About this task:

The PagerDuty connector lets your automations open, acknowledge, and resolve incidents in PagerDuty as part of an automated response. PagerDuty is in the **Alerting** connector category — a category dedicated to incident-management platforms that own the on-call lifecycle (trigger → acknowledge → resolve) and escalation policies.

When the connector is configured, automations can use the **Trigger Alert**, **Get Alert**, **Acknowledge Alert**, **Add Note to Alert**, and **Resolve Alert** steps from the **Alerting** tab in the step picker. Each step's **Provider** field is set to PagerDuty.

> **Important:**
>
> **Before you begin:** You must generate a PagerDuty General Access Key (an account-wide REST API key) and have one PagerDuty user email address available to attribute incident actions to. See Appendix I - Creating a PagerDuty General Access Key *(on page 305)*.

To configure the PagerDuty connector:

Procedure:

1. In the Check Point Portal, go to **Playblocks** > **Connectors**.
2. In the **Alerting** section, click the **PagerDuty** card.
3. In the connector side panel, turn on the **Enable** toggle.
4. Under **Step 1 - Authenticate**, fill in these fields:
   - **API key** - Paste the PagerDuty General Access Key you created. See Appendix I - Creating a PagerDuty General Access Key *(on page 305)*.
   - **Email** - The email address of a real user in your PagerDuty organization. PagerDuty requires a "From" email header on every REST API request that creates or modifies an incident. Playblocks sends this address as the "From" header on every incident action. The email controls only the attribution that shows up in PagerDuty's audit log; it is unrelated to the authentication itself, which is handled entirely by the General Access Key.
   - **Service URL** - The PagerDuty REST API base URL. Defaults to `https://api.pagerduty.com`. EU tenants should override to `https://api.eu.pagerduty.com`. No other values are accepted.

5. Click **Save**.

   Playblocks validates the API key.

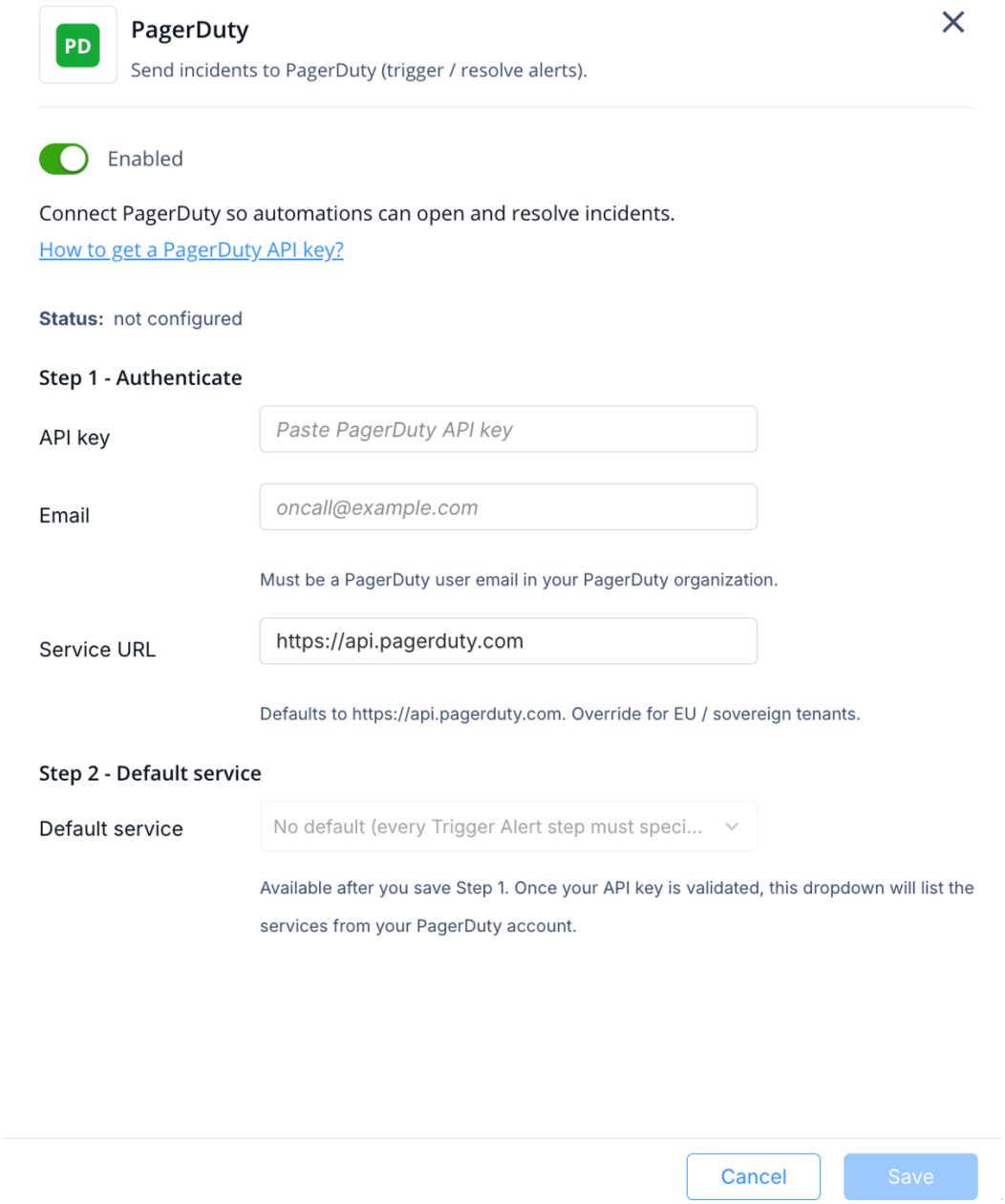
   - On success, the connector is marked **Connected**.
   - On failure, the side panel shows the error and the connector is left in an **Error** state. Fix the credentials and save again.

6. Under **Step 2 - Default service**, select the PagerDuty service that new incidents should be created in by default.

   The dropdown lists every active service in your PagerDuty account.

   > **Note:**
   >
   > The default service is used by the **Trigger Alert** step unless a specific service is chosen on the step itself.

7. Click **Save**.



11.10. AI Connectors

This topic describes how to connect an AI provider to Playblocks and how to use the AI Request step in custom automations.

About this task:

Overview

Playblocks supports three AI providers:

- **OpenAI** - ChatGPT models
- **Google Gemini**
- **Anthropic Claude**

Configure each provider on the **Connectors** page. After you connect a provider connector, custom automations can use it through the **AI Request** step to send prompts and receive AI-generated responses.

Connecting an AI Provider

You need an API key from the AI vendor (OpenAI, Google AI Studio, or Anthropic). Playblocks validates the key against the vendor's live API at save time and stores it encrypted.

To connect an AI provider:

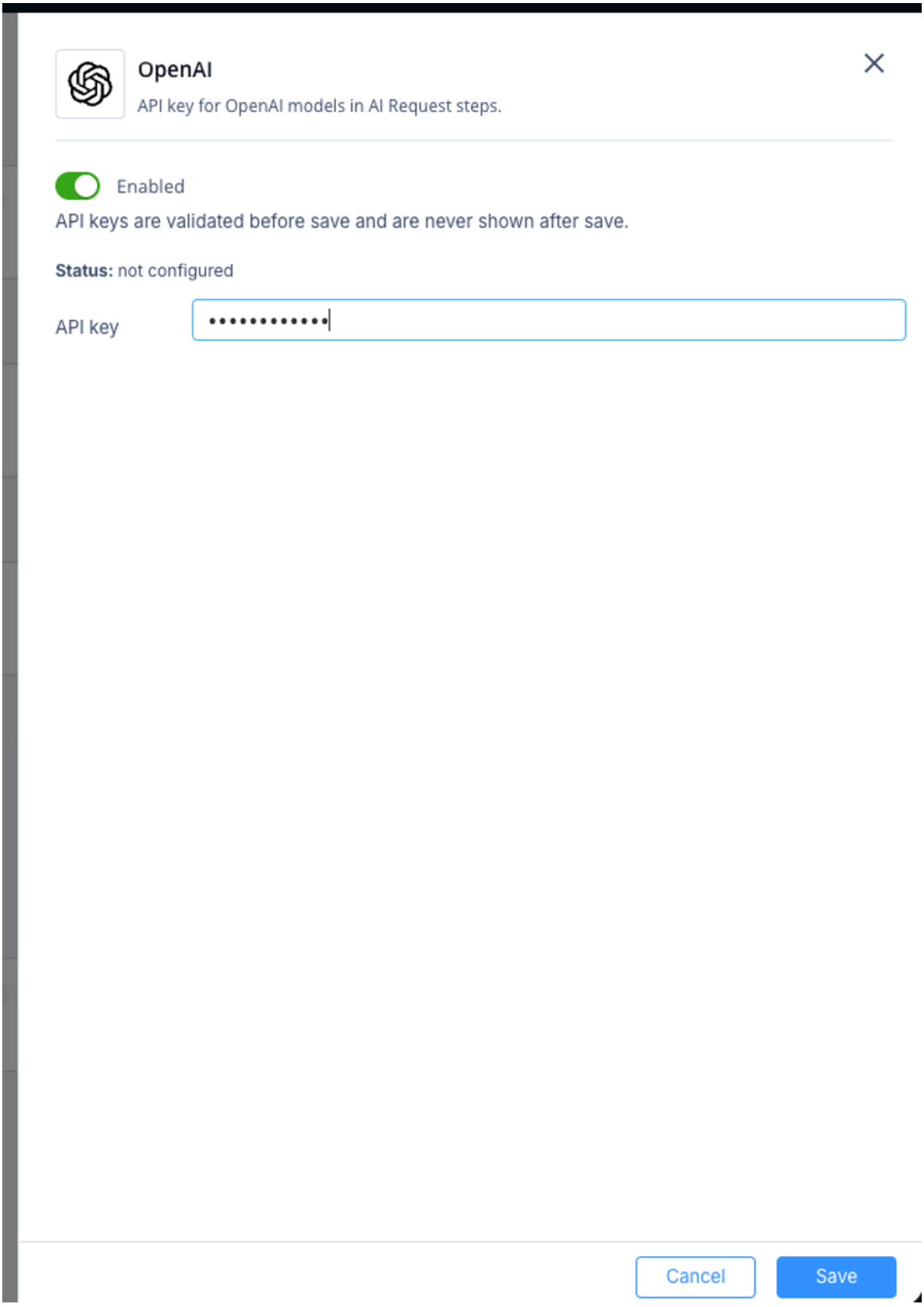
Procedure:

1. Open the **Connectors** page in the Playblocks portal.
2. Locate the provider you want to connect (**OpenAI**, **Google Gemini**, or **Anthropic Claude**) and open its side panel.
3. Turn on the **Enabled** toggle.
4. In the **API key** field, paste your API key.

5. Click **Save**.

   Playblocks validates the key.

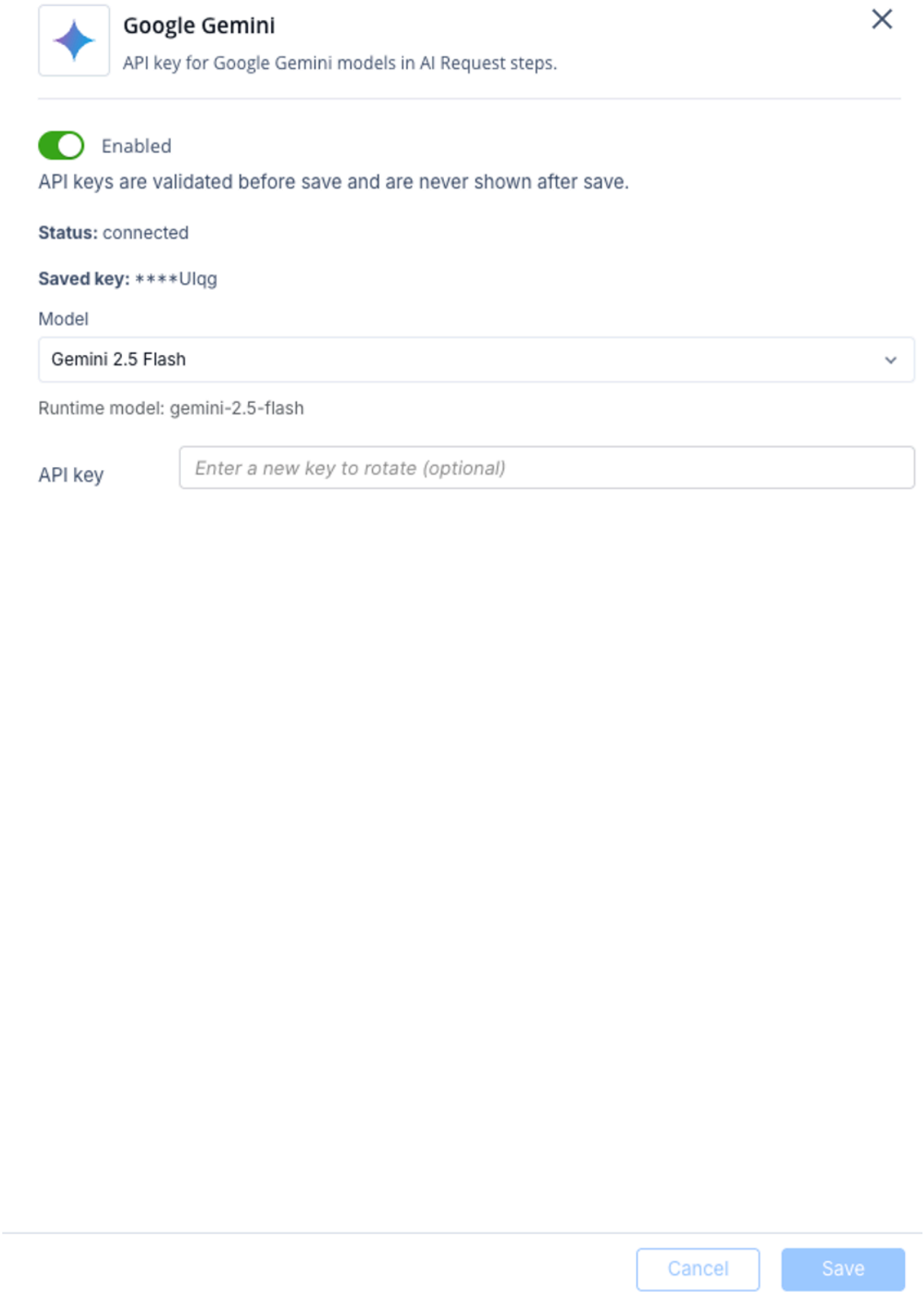
   On success, the connector status changes to **connected**. You can choose a model to use in Playblocks steps from the list of models the provider allows.



6. After the first successful save, from the dropdown, select a **Model**.

> **Note:**
>
> If you do not select a model, Playblocks falls back to the provider's default.

7. Click **Save** to persist the model selection.



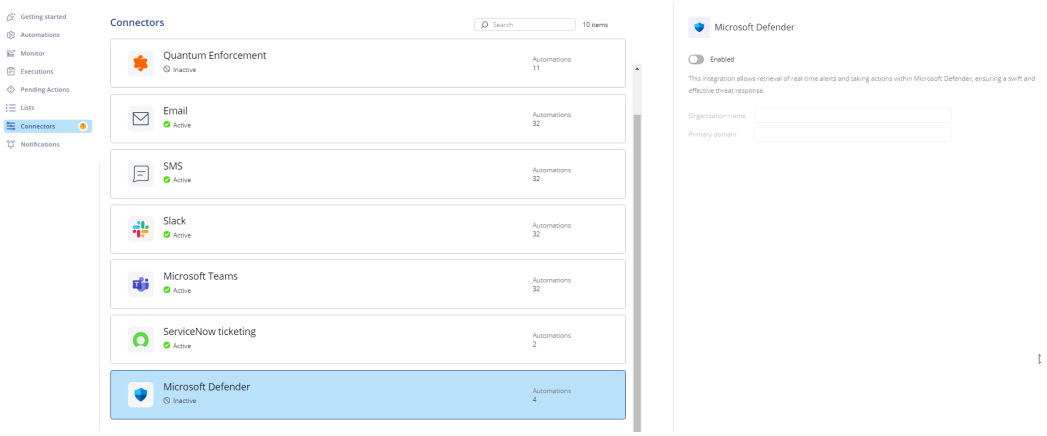
11.11. Microsoft Defender

This topic describes how to configure a Microsoft Defender connector in Playblocks. It provides the steps required to enable and authorize the connector.

About this task:
You can execute machine actions and read real-time alerts from the Microsoft Defender for Endpoint.

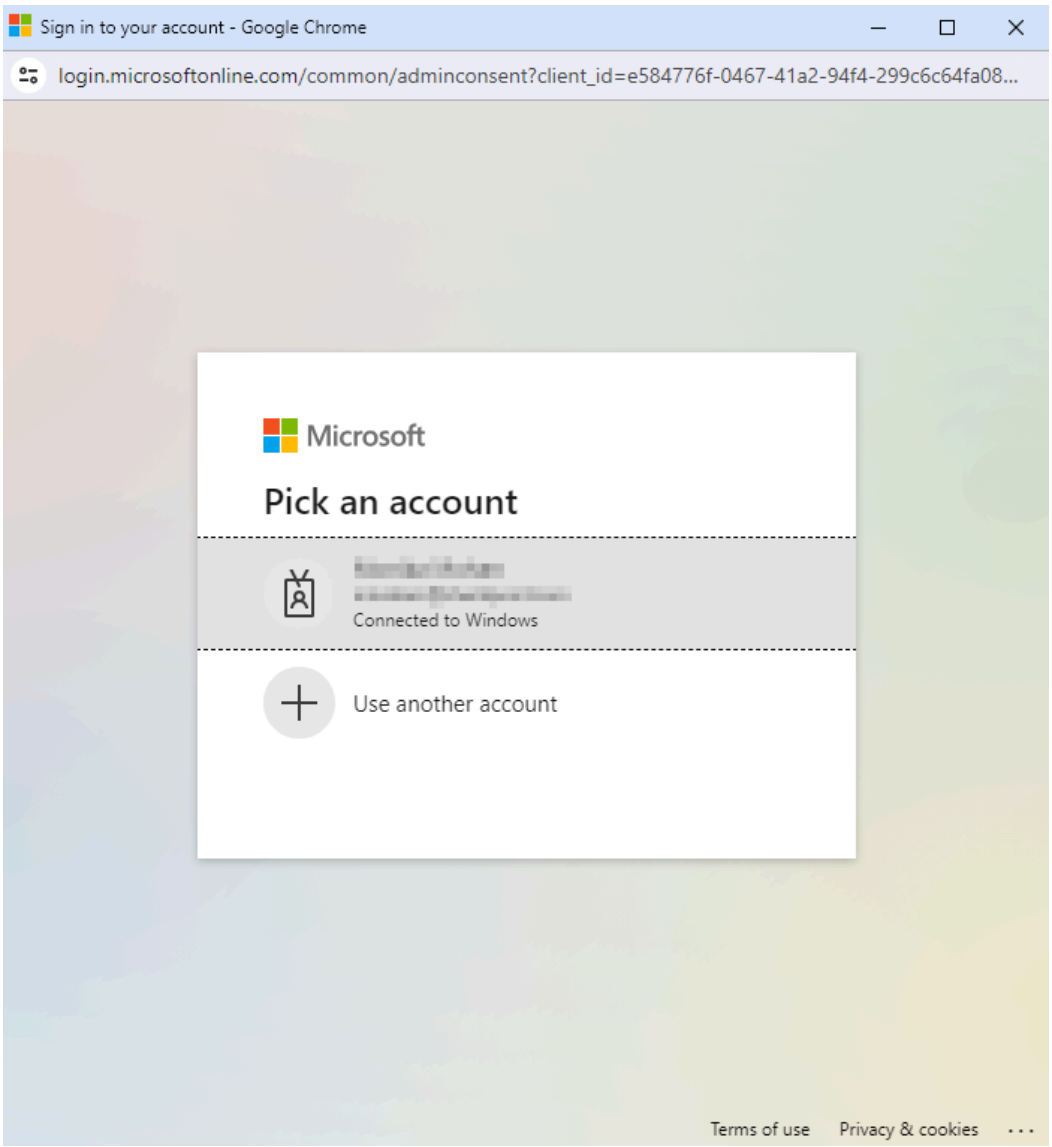
Procedure:

1. Access **Playblocks** and click **Connectors**.
2. Select **Microsoft Defender**.

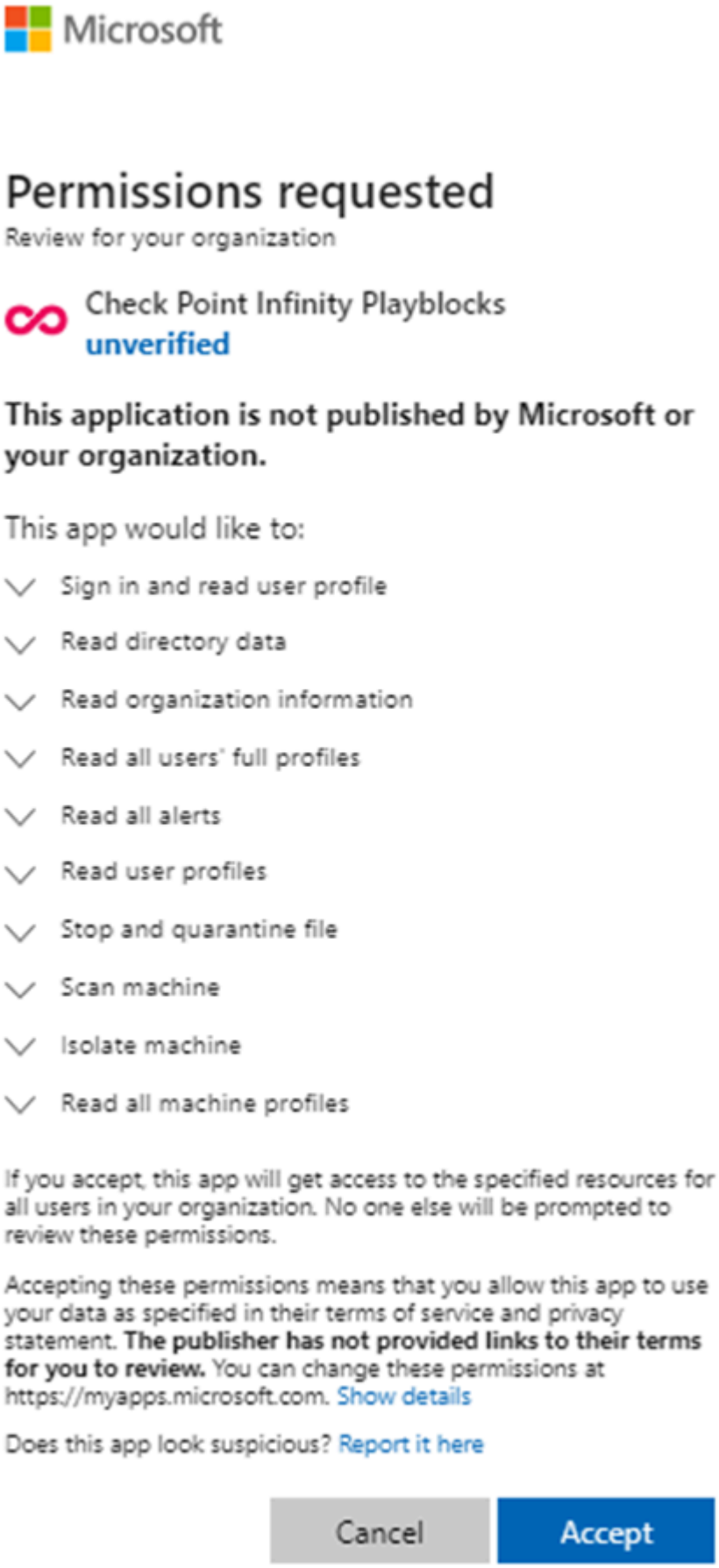


3. Turn on the **Enabled** toggle button.

   The **Sign in to your account** window appears.

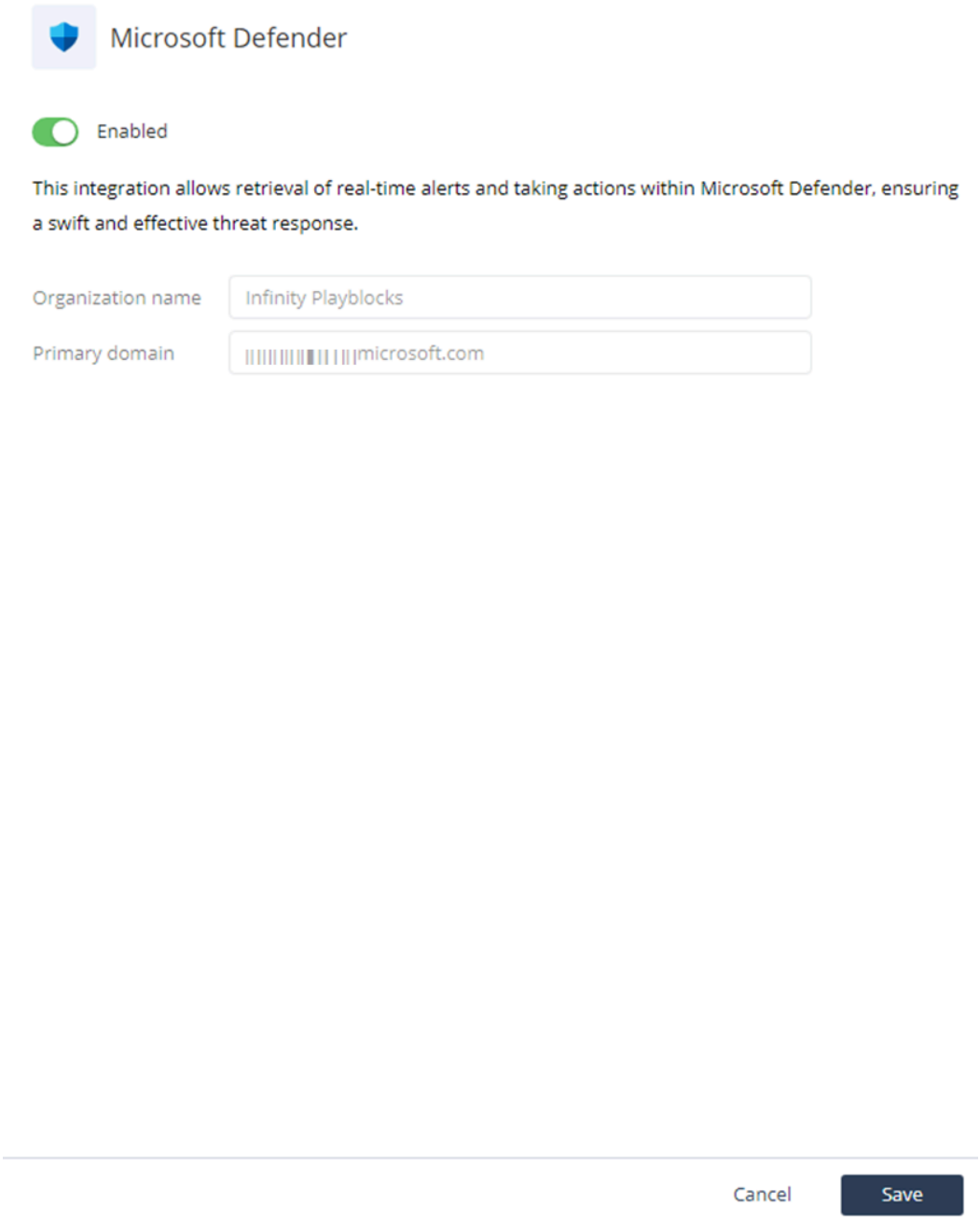


4. Select the account.



5. Click **Accept**.

   The system automatically populates **Organization name** and **Primary domain**.



6. Click **Save**.

11.12. CrowdStrike

This topic describes how to connect CrowdStrike Falcon with an Playblocks account. It provides steps to enable the connector and configure required credentials.

About this task:

The integration of Playblocks with CrowdStrike Falcon allows you to receive real-time alerts from CrowdStrike Falcon for Endpoint and take corrective actions through automations. These automated workflows enable faster responses and more efficient threat management.

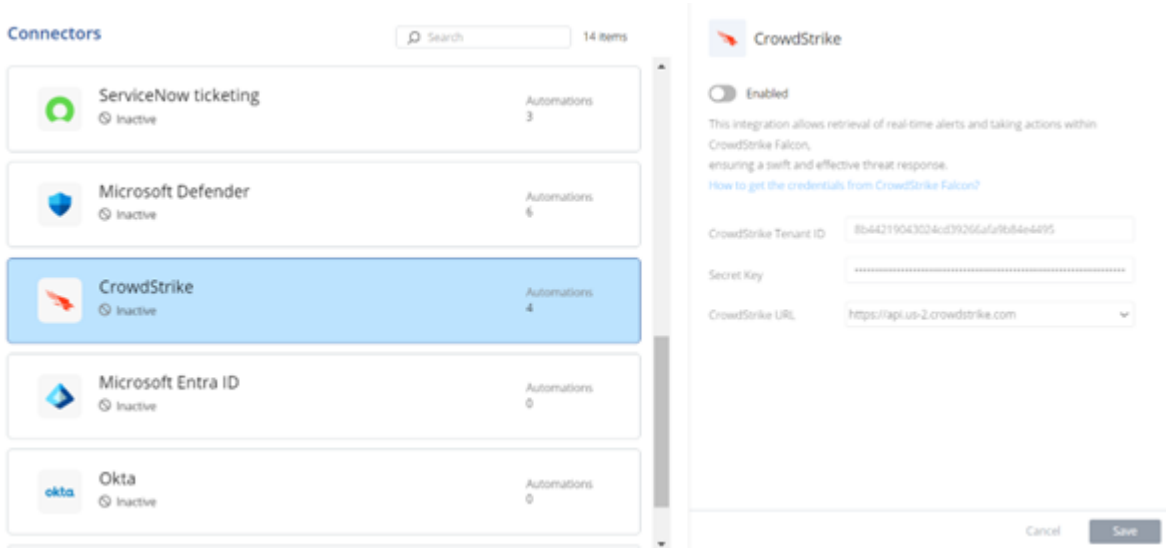
Note:

Before you configure the CrowdStrike connector, you must integrate the Playblocks and CrowdStrike Falcon. For more information, see Appendix E - Integrating CrowdStrike Falcon *(on page 278)*

To connect CrowdStrike Falcon with your Check Point Portal account:

Procedure:

1. Log in to Playblocks and click **Connectors**.
2. Select **CrowdStrike** and turn on the **Enabled** toggle button.



3. Enter these:
   - **Client ID**
   - **Secret Key**
   - **Base URL**
4. Click **Save**.

11.13. Microsoft Entra ID

This task describes how to connect Microsoft Entra ID with your Check Point Portal account. Follow the steps to configure and enable the connector.

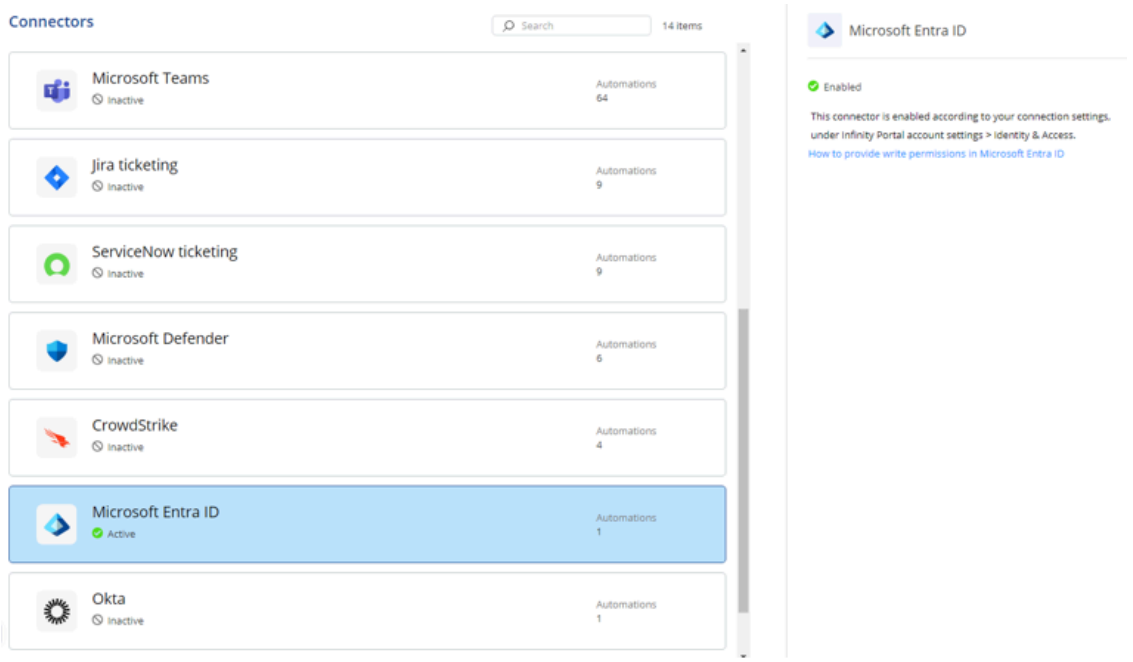
About this task:
To connect Microsoft Entra ID with your Check Point Portal account:

Procedure:

1. Sign in to Check Point Portal.
2. Go to **Account Settings** > **Identity & Access**.
3. Follow the instructions in the Check Point Portal Administration Guide.

Procedure result:

Once connected, the Microsoft Entra ID connector is automatically enabled.



11.13.1. Reset user password permissions

This topic describes how to provide write permissions required to reset a user password in Entra ID. It guides you through assigning the appropriate role to the application.

About this task:

To reset user password, you need to provide write permissions in Microsoft Entra ID. To do that:

Procedure:

1. Open the Microsoft Entra ID portal.
2. Go to the **Roles and administrators** tab.
3. Search for **User Administrator**.
4. Click **Add assignments**.
5. Search for the application created for Check Point and click **Add**.
6. Add the desired role to Check Point application.

   For information on the available roles, see Microsoft Entra ID documentation.

11.14. Okta

This topic describes how to connect Okta with your Check Point Portal account. It provides the required steps and connection behavior.

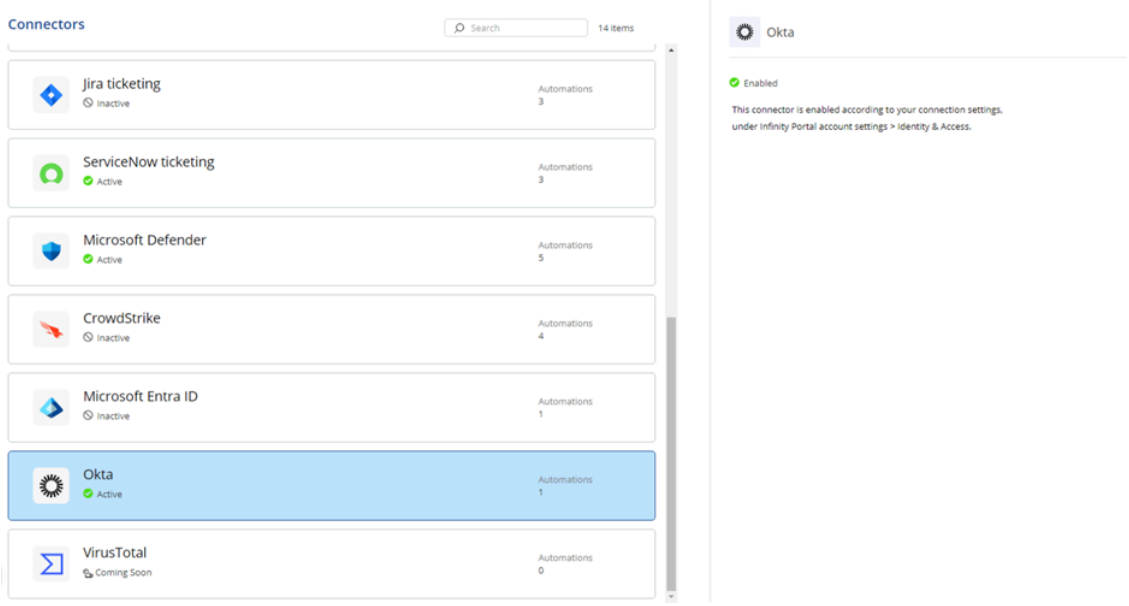
About this task:
To connect Okta with your Check Point Portal account:

Procedure:

1. Sign in to Check Point Check Point Portal.
2. Go to **Account Settings** > **Identity & Access**.
3. Follow the instructions in the Check Point Portal Administration Guide.

Procedure result:

Once connected, the Okta connector is automatically enabled.



11.15. SentinelOne

This topic describes the integration of playbook blocks with SentinelOne and explains how automated workflows help improve threat management. It also includes a note about required SentinelOne service user permissions.

The integration of Playblocks with SentinelOne allows you to receive real-time alerts from SentinelOne agents and take corrective actions through automations. These automated workflows enable faster responses and more efficient threat management.

Note:

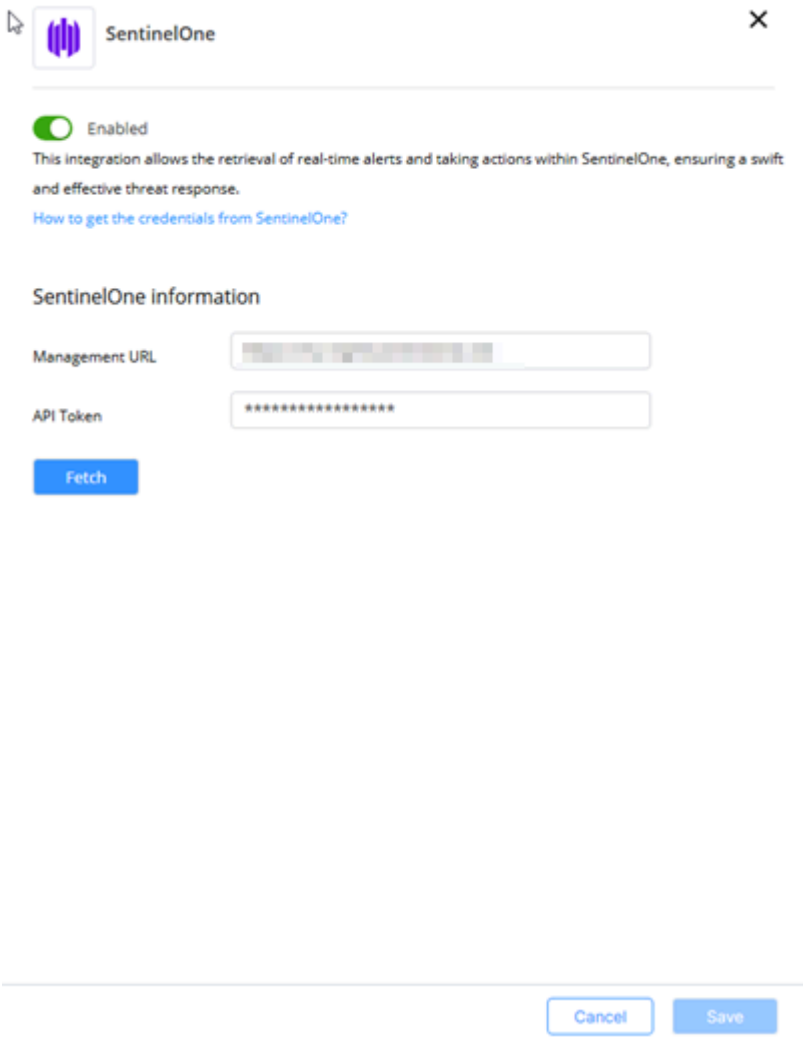
Before you configure the SentinelOne connector, create a SentinelOne service user with sufficient permissions. For more information, see Appendix F - Creating a SentinelOne Service User *(on page 281)*.

11.15.1. Configure a SentinelOne connector

This task describes how to configure a SentinelOne connector in Playblocks. Follow the steps to enable the connector and provide required credentials.

Procedure:

1. Access **Playblocks** and click **Connectors**.
2. Select **SentinelOne**.



3. Turn on the **Enable** toggle button.
4. In the **Management URL** field, enter your SentinelOne domain, for example, `https://my-mgmt.sentinelone.net`.
5. In the **API Token** field, enter the API token that you created in your SentinelOne account.

6. Click **Fetch**.

7. Click **Save**.

   The protected account that you chose is displayed.

11.16. IOC Enforcement

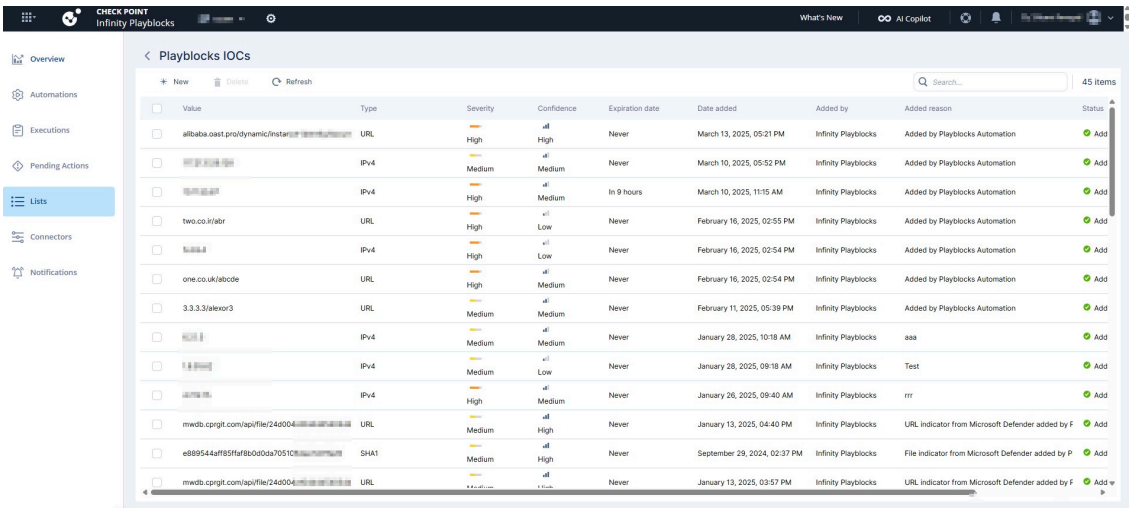
This topic describes IOC Enforcement and how it synchronizes indicators across connected security products. It explains how Playblocks IOCs are updated and distributed through the IOC Management platform.

The IOC Enforcement connector ensures seamless synchronization between Playblocks and all connected products enforcing IOC.

It automatically updates and distributes newly added IOC across the security products, enhancing protection through up-to-date threat intelligence.

With Check Point Firewall IOC Enforcement, you can select the Security managements you want to fetch the indicators from the output blend of the IOC Management platform. Each gateway connected to the management with anti-bot and anti-virus will start enforcing IOCs after installing the new Threat prevention policy.

When enabling IOC Enforcement, a new list **Playblocks IOCs** is added. This list sync with a new feed in the IoC Management platform called **Playblocks feed**. In this feed is be added every indicator that is found by Playblocks automations.



11.16.1. Configure an IOC Enforcement connector

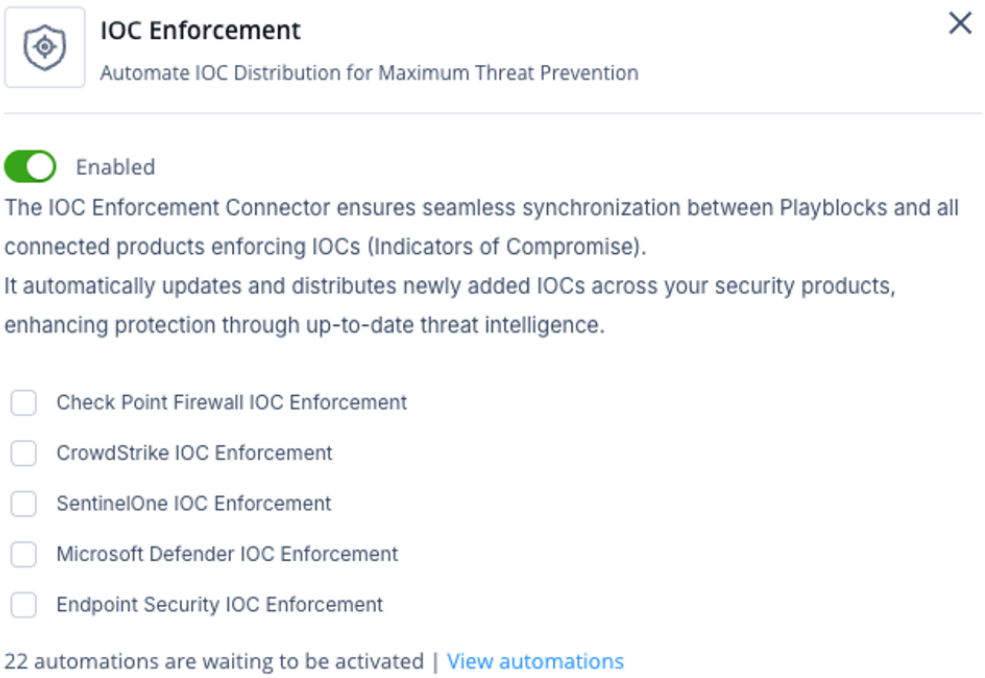
This topic describes how to configure IOC Enforcement connectors and enable integrations with supported security platforms. It provides step-by-step instructions for setup, validation, and enforcement options.

About this task:

To configure an IOC Enforcement connector, follow these steps.

Procedure:

1. Access **Playblocks** and click **Connectors**.
2. Select **IOC Enforcement**.



3. Turn on the **Enable** toggle button.

4. To enable Check Point Firewall IOC enforcement, select the **Check Point Firewall IOC Enforcement** checkbox.

   a. In the **Select Managements for automatic enforcement** section, select one of these:

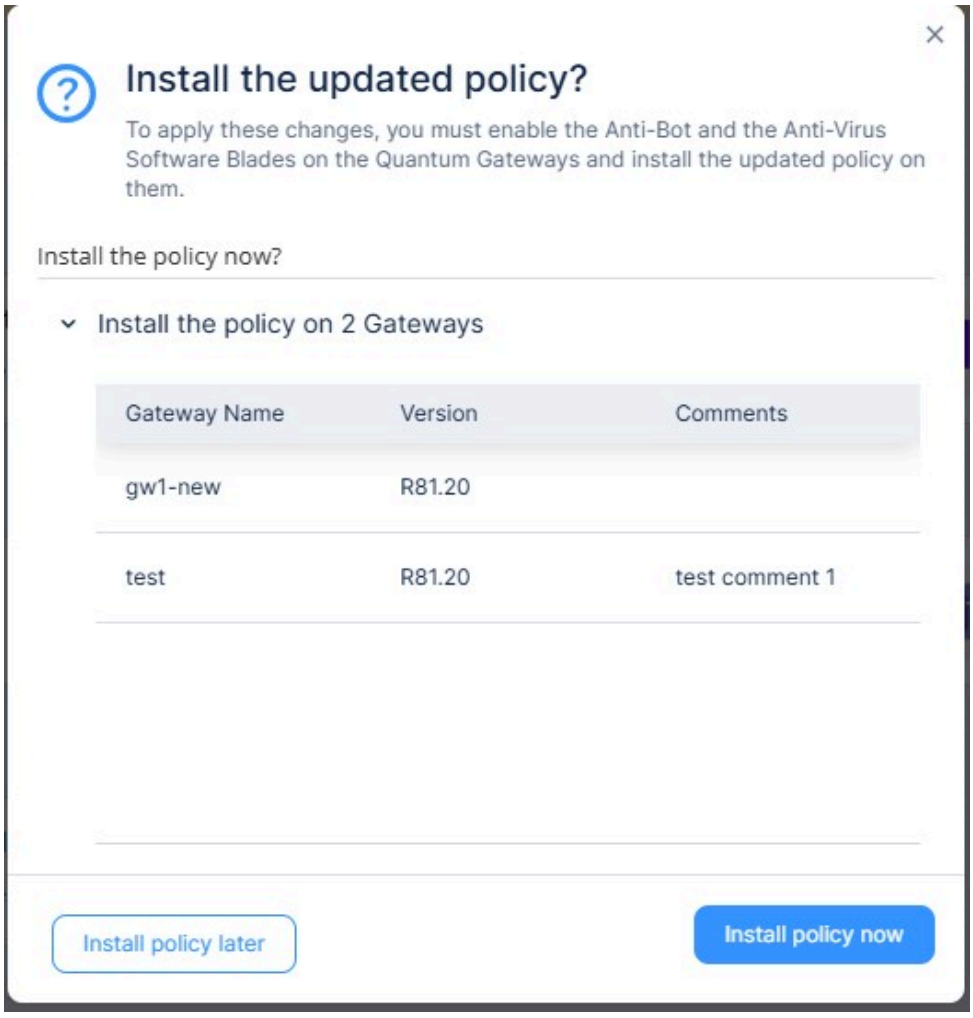
      - **All (Recommended)** - Automatically enables Check Point Firewall IOC Enforcement on all Managements connected to the Check Point Portal. This includes any current and future environment that connects to the Check Point Portal.
      - **Specific managements** - Manually choose which Managements to enable Check Point Firewall IOC Enforcement on. The system does not automatically add new managements that connect to the Check Point Portal.

   b. Search and select the relevant managements.

   c. Click **Save**.

      The **Install updated policy** window appears.

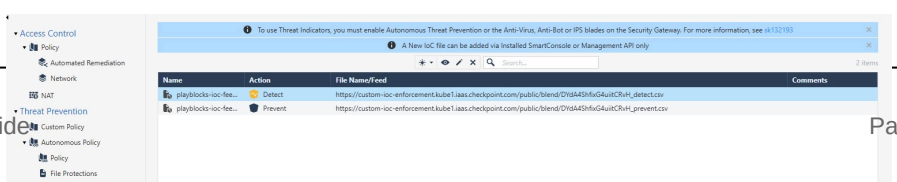
      You can see the relevant gateways connected to your management with Anti-Bot and Anti-Virus blades installed on them.



   d. To install the Threat Prevention policy, click **Install Policy**.

   e. To verify the changes:

      i. In the SmartConsole, navigate to **Security Policies** > **Custom Policy Tools** > **Indicators**.



5. To enable CrowdStrike IOC enforcement, select the **CrowdStrike IOC Enforcement** checkbox and click **Save**.

   Note:

   - Make sure the ../crowdstrike/crowdstrike.dita is enabled.
   - Disabling the CrowdStrike connector also disables IOC enforcement, removing all Playblocks added indicators from CrowdStrike.

   Now, all existing IOCs in the Playblocks feed are synced into CrowdStrike IOC, and any new indicators detected by automation are added.

   File hash indicators MD5 and SHA256 are added with the **Prevent** action and IP indicators are added with the **Detect** action, as CrowdStrike do not support IP prevention.

6. To enable SentinelOne IOC enforcement, select the **SentinelOne IOC Enforcement** checkbox and click **Save**.

   Note:

   - Make sure the Configure a SentinelOne connector *(on page 250)* is enabled.
   - Disabling the SentinelOne connector also disables IOC enforcement, removing all Playblocks added indicators from SentinelOne.

   Now, all existing IOCs in the Playblocks feed are synced into SentinelOne IOC, and any new indicators detected by automation are added.

   SentinelOne enforces expiration limits on indicators. It adjusts any indicator that exceeds these limits to expire according to these limitations:

   - IP: 30 days
   - URL and Domain: 180 days
   - Hash (SHA1, SHA256, MD5): 180 days

7. To enable Microsoft Defender IOC enforcement, select the **Microsoft Defender IOC Enforcement** checkbox and click **Save**.

   Note:

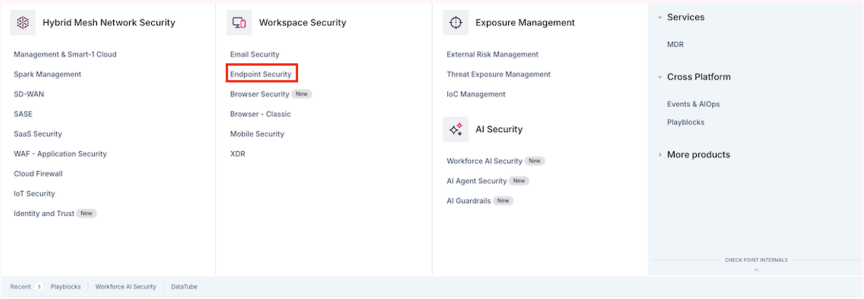
   - Make sure the Microsoft Defender *(on page 243)* is enabled.
   - Disabling the Microsoft Defender connector also disables IOC enforcement, removing all Playblocks added indicators from Microsoft Defender.

   Now, all existing IOCs in the Playblocks feed are synced into Microsoft Defender IOC, and any new indicators detected by automation are added.

8. To enable Endpoint Security IOC enforcement, select the **Endpoint Security IOC Enforcement** checkbox and click **Save**.

   Note:

   - Make sure the Endpoint Security service in the Check Point Portal is up and running.

   - Make sure the Endpoint Security connector is enabled.
   - If the Endpoint Security service is up but the connector is not enabled, contact https://www.checkpoint.com/support-services/contact-support/.
   - Endpoint Security do not expire IOCs automatically. However, Playblocks runs a sync at regular intervals to remove all expired indicators from Endpoint Security.
   - Endpoint Security supports MD5 and SHA1 file hash indicators, IPv4, HTTP URL, and domain indicators.

   Now, all existing IOCs in the Playblocks feed are synced into Endpoint Security IOC, and any new indicators detected by automation are added.

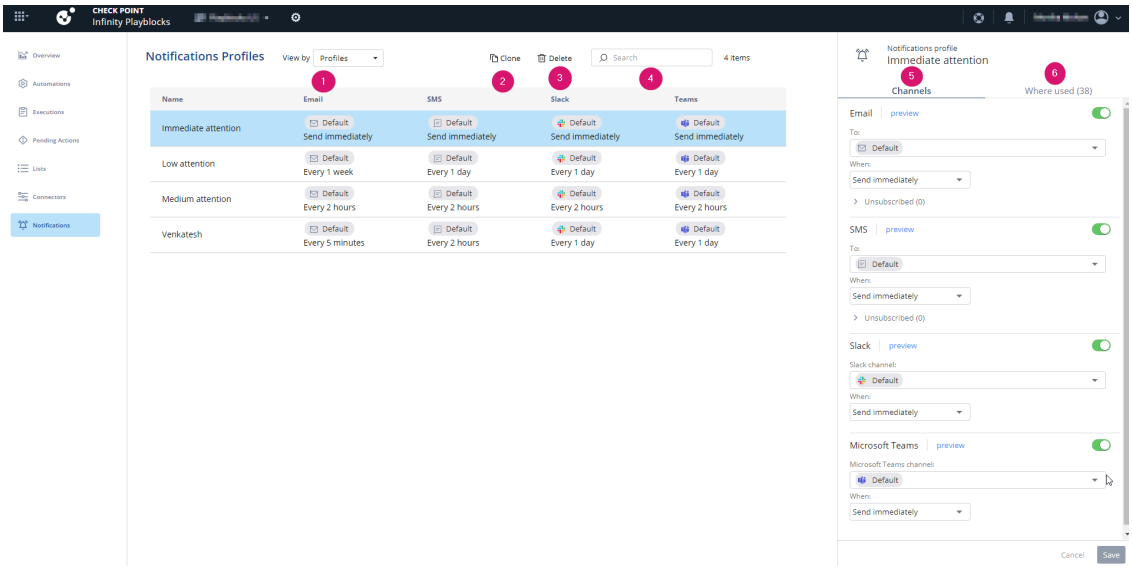
12. Notifications

The Notifications page provides options to manage who receives notifications and how they are delivered. It also displays legends describing available actions and views.

The **Notifications** page allows you to:

- Control who receives notifications and when (immediately, or with a scheduled report), according to your desired attention level for an event.
- View and manage the list of users in your account who have unsubscribed from notifications by Playblocks.

To view the **Notifications** page, access **Playblocks** and click **Notifications**.



Legend	Description
1	Select a view: • Profiles *(on page 258)* • Automations *(on page 261)*
2	Clone a notification profile to add a new profile *(on page 260)*.
3	Delete a notification profile *(on page 261)*.
4	Search for a specific notification profile.
5	Configure Channels *(on page 258)*.
6	Shows the automations where the notification profile is used.

12.1. View notifications by Profiles

This topic describes how notifications can be viewed according to predefined profiles. It outlines the default attention profiles available in the Profiles view.

In the **Profiles** view, you can view notification by profiles. The default profiles are:

- **Immediate attention** - Sends notification immediately.
- **Medium attention** - Sends notification every 2 hours.
- **Low attention** - Sends notifications every 1 day.

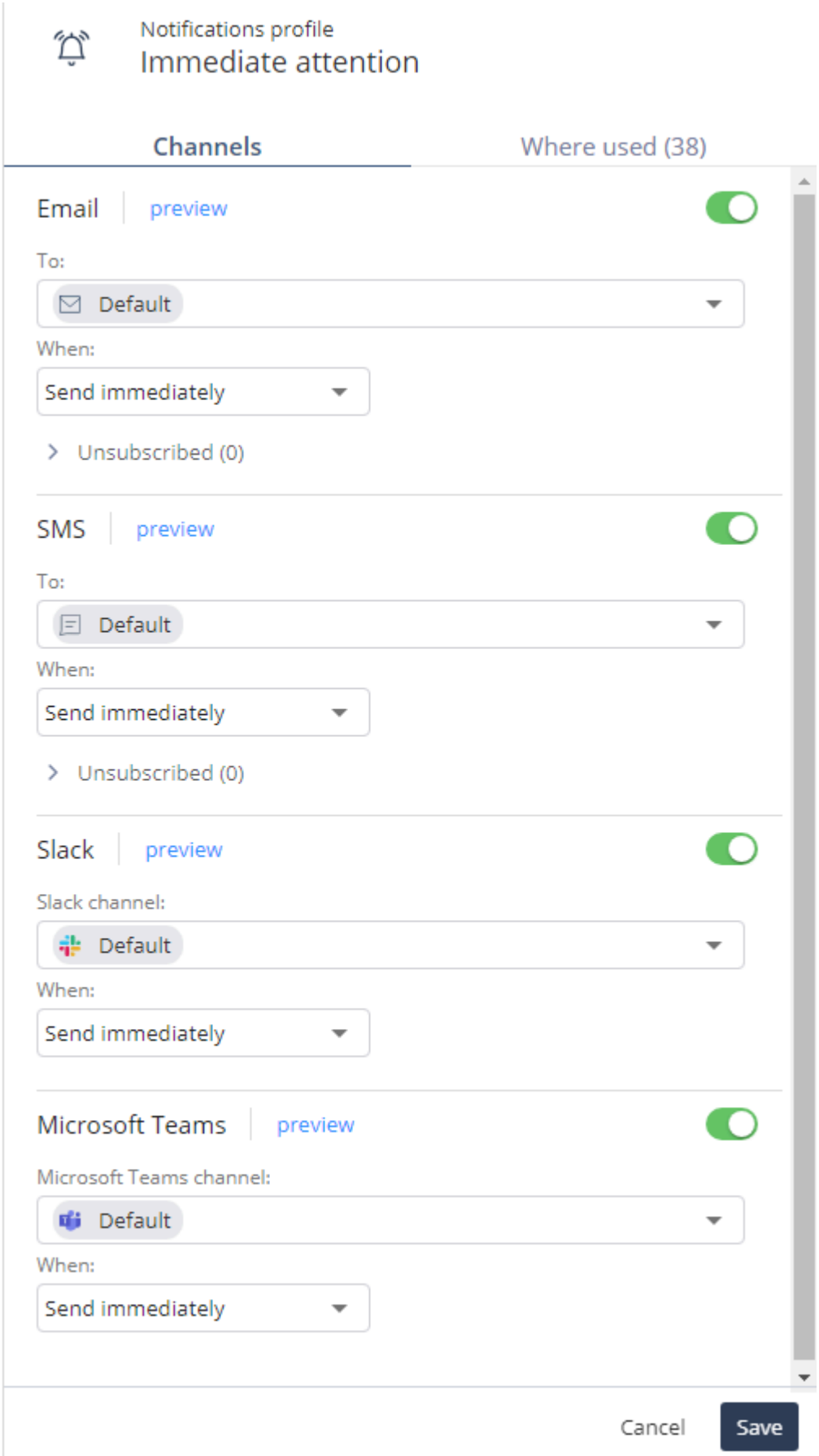
12.2. Configure a notification profile

This task explains how to configure a notification profile in Playblocks. It includes steps for selecting channels, managing recipients, and previewing notifications.

Procedure:

1. Access **Playblocks** and click **Notifications**.
2. Select a notifications profile.

3. Go to the **Channels** tab.



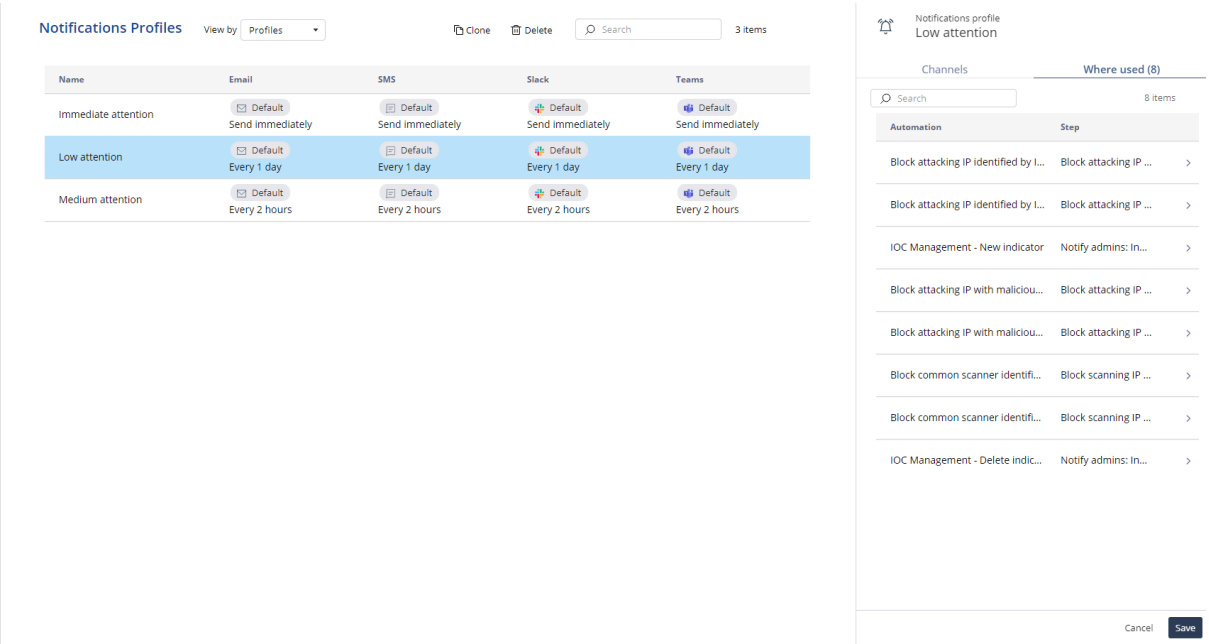
a. Turn on the toggle button for the connector you want to enable.

b. From the **To** list, select the user or user groups to send the notification.

To add or manage users and user groups, see these connectors pages:

- Email *(on page 229)*
- SMS *(on page 230)*

4. Click **Save**.
5. To know the automation and the step where the notification profile is used, click the **Where used** tab and click ›.



The system redirects to the Automation *(on page 29)* page.

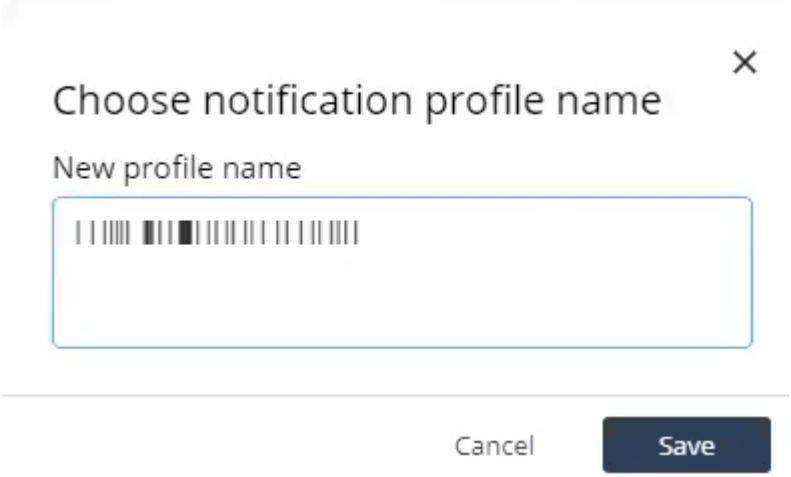
12.3. Cloning a Notification Profile

This task describes how to clone an existing notification profile. Follow the steps to duplicate a profile and prepare it for further configuration.

Procedure:

1. Access **Playblocks** and click **Notifications**.
2. Select the notification profile you want to clone.
3. Click **Clone**.

   The **Choose notification profile name** pop-up window appears.



4. In the **New profile name** field, enter a new profile name.

5. Click **Save**.
6. Configure channels in the profile. *(on page 258)*

12.4. Deleting a Notification Profile

This task describes how to delete an existing notification profile in Playblocks. Follow the steps to remove a profile that is no longer required.

Procedure:

1. Access **Playblocks** and click **Notifications**.
2. Select the notification profile you want to delete.
3. Click **Delete**.

What to do next:

Note:

You can delete a notification profile only if it is not used by any steps. If the notification profile is used by certain steps, you must update those steps to use a different notification profile.

12.5. View by Automations

This topic describes how to view notifications in the Automations view. It explains the purpose of the Automations interface.

In the **Automations** view, you can view the notifications by automations.

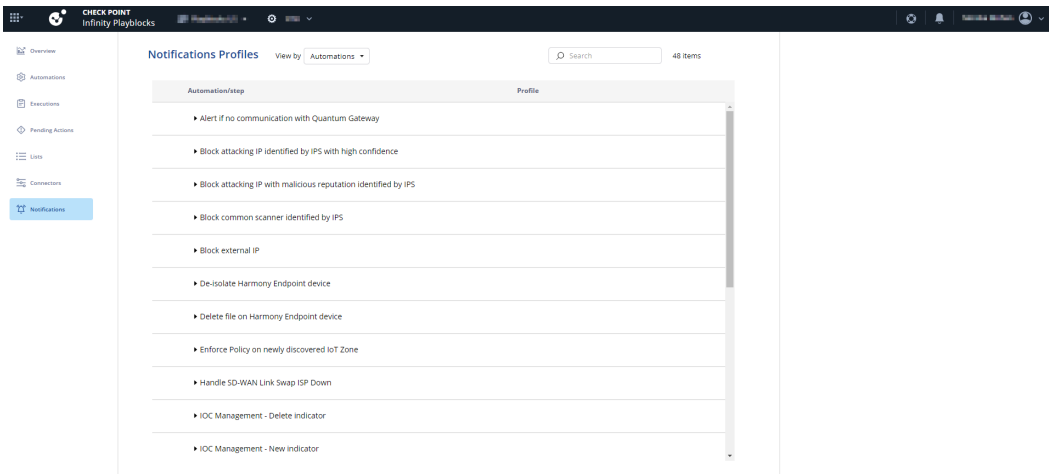
12.6. Configure a notification profile for an automation

This task describes how to configure a notification profile for an automation. It guides you through selecting automations, modifying profiles, and adjusting notification settings.

Procedure:

1. Access **Playblocks** and click **Notifications**.
2. In **View by** list, select **Automations**.

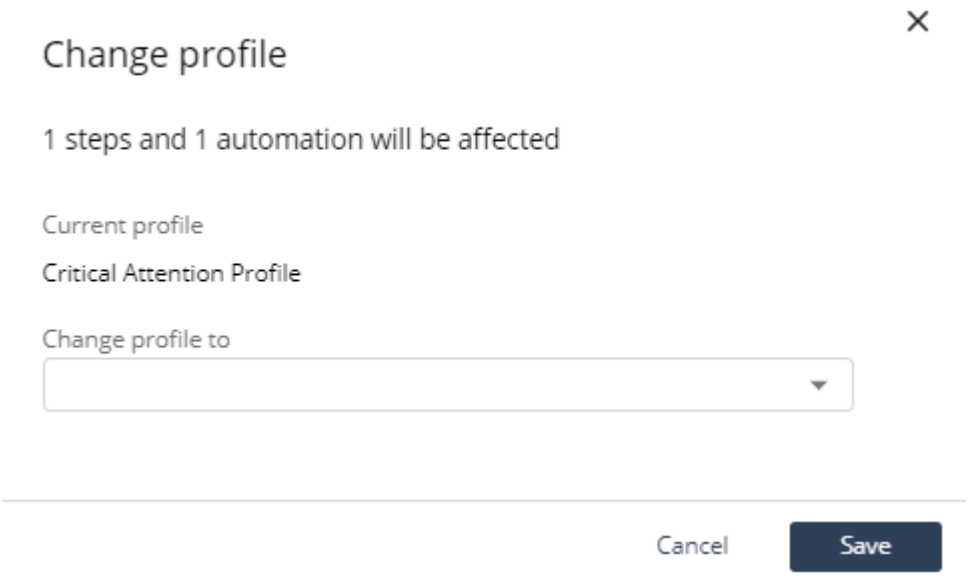
   The system displays the list of automations.



3. Expand the automation and select the checkbox for the automation step(s).

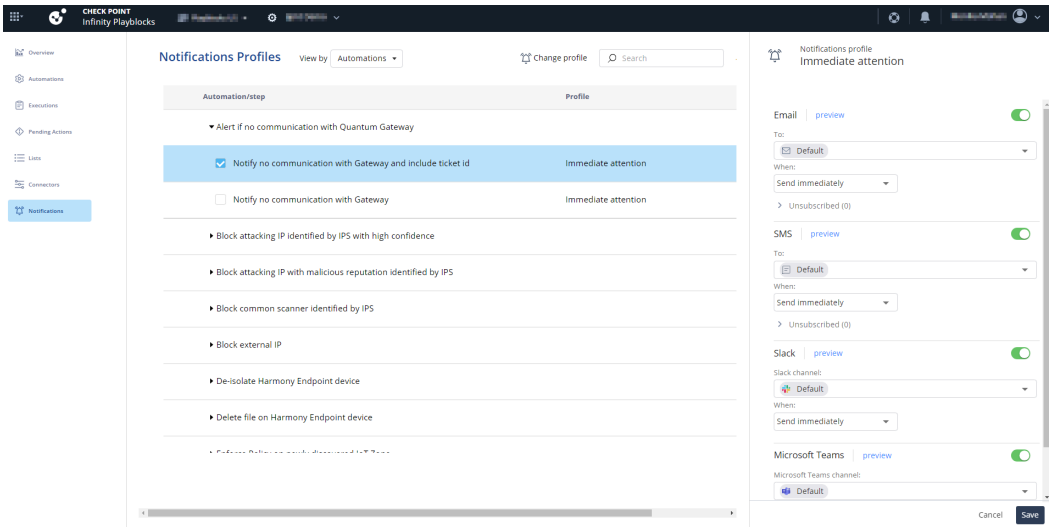
4. To change the profile, click **Change profile**.

   The **Change profile** window appears.



   a. From the **Change profile to** list, select the profile.
   b. Click **Save**.

5. To edit the notification profile for the automation step, select the automation step(s).



6. In the **Notifications profile** tab:

   a. Turn on the toggle button for the connector you want to enable.

   b. From the **To** list, select the user or user groups to send the notification.

      To add or manage users and user groups, see these connectors pages:

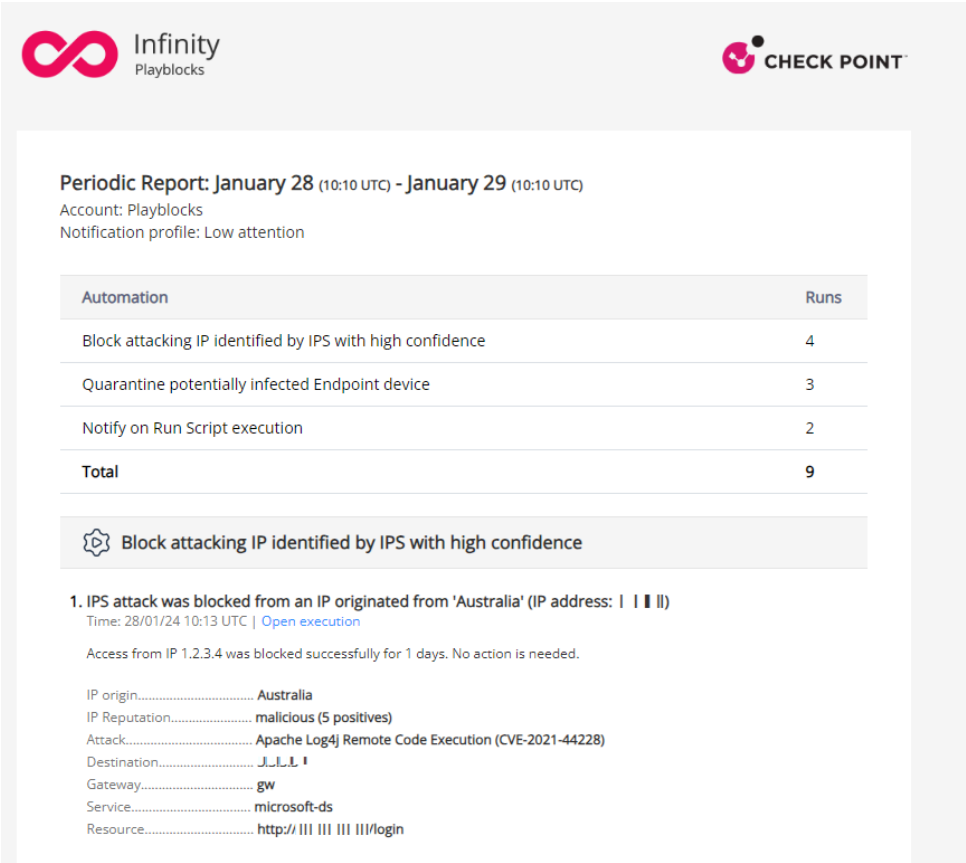
      - Email *(on page 229)*
      - SMS *(on page 230)*
      - Slack *(on page 233)*
      - Microsoft Teams *(on page 234)*

   c. From the **When** list, select the frequency to send the notification.

> **Note:**
>
> You cannot change **Send immediately** to any other frequency in the **Immediate attention** profile.

   d. To preview the notification, click **Preview**.

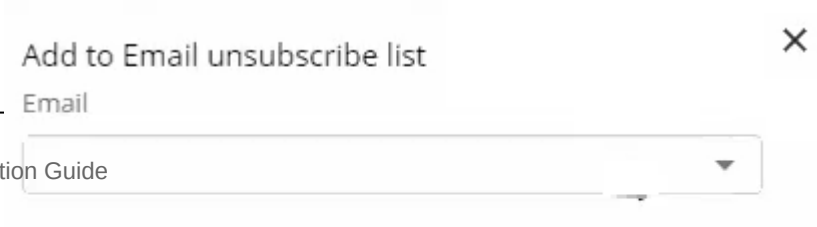
      The **Report Preview** window appears.



   e. To remove a user from the group, expand the **Unsubscribe** section.

   f. Click + .

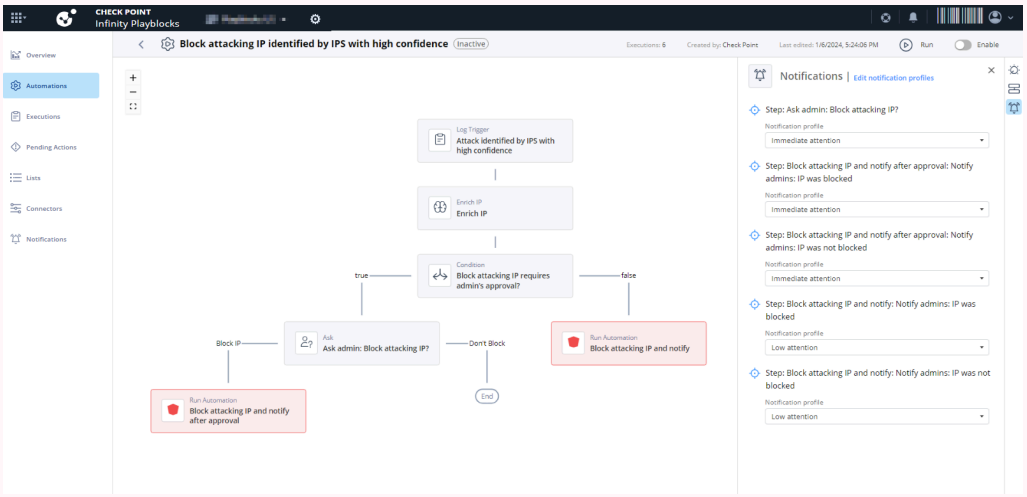
      The **Add to unsubscribe list** window appears.



What to do next:

Note:

You can also edit the notifications profile for each automation step in the **Automations** page. For more information, see Automation Parameters and Flowchart.



13. Appendix

This appendix provides links to supporting procedures for integrating various external services with Check Point Playblocks. It lists additional configuration resources for multiple platforms.

13.1. Appendix A - Creating a User with Specific Roles in ServiceNow

This task describes how to create a ServiceNow user and assign specific roles for use with Playblocks. It includes login steps, user creation, password setup, and role configuration.

About this task:

To create a user with specific roles in ServiceNow:

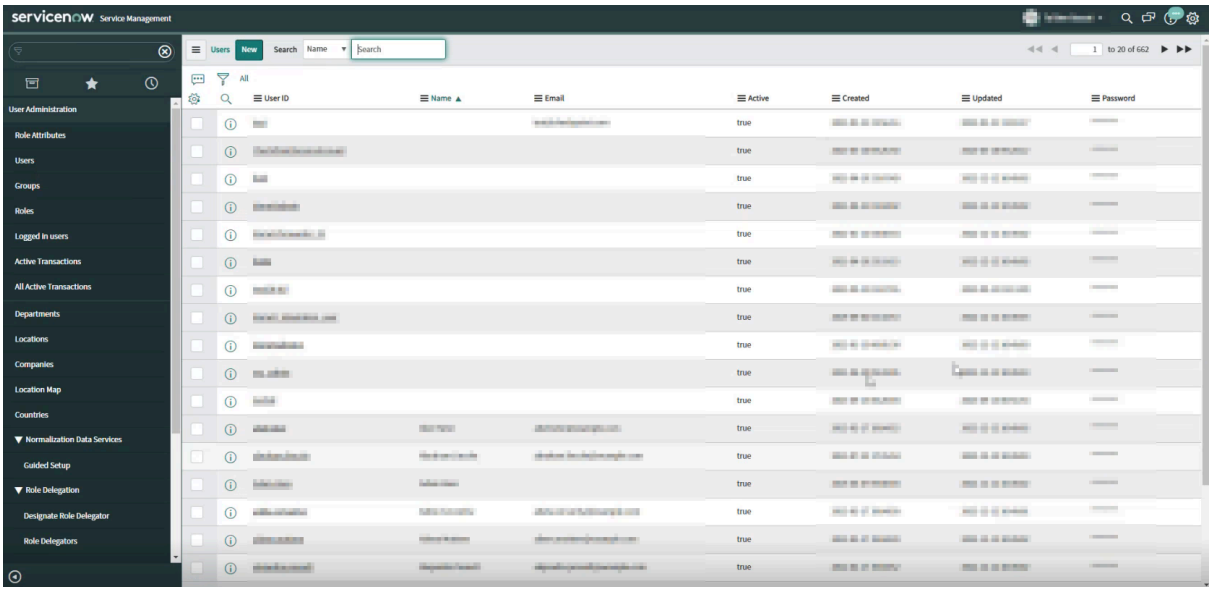
https://embed.app.guidde.com/playbooks/rsKyMXKzGc5woqtkHKM83S

Procedure:

1. Log in to your ServiceNow account.

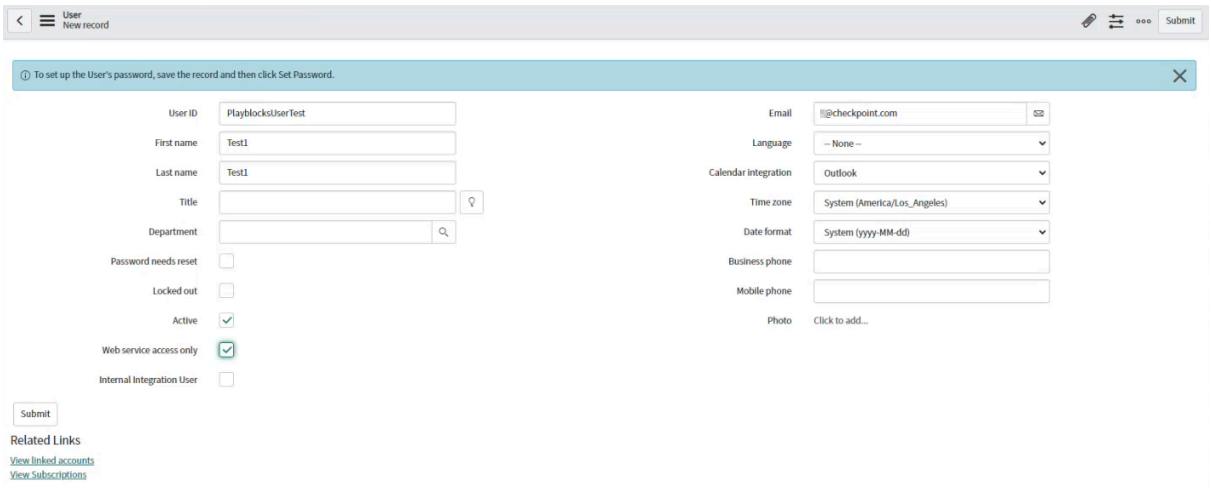
   https://<instance>.service-now.com

2. In the left pane, go to **User Administration** > **Users**.



3. Click **New**.

4. Enter the user details and select the **Active** and **Web service access only** checkboxes.



> **Note:**
>
> User ID is the Username specified when you configure the ServiceNow ticketing connector *(on page 236)*.

5. Click **Submit**.

   The system creates the user.

6. In the **Search** list, select **Name** and search for the user ID you created.
7. From the search results, click the user ID.
8. Click **Set Password**.

   The **Set Password** window appears.

9. Click **Generate**.

   The system generates a password.

10. To copy the password, click the copy icon.

    1ServiceNowCopyPassword.png

11. To save the password, click **Save Password**.

> **Note:**
>
> Make a note of this password. It is required to configure the ServiceNow ticketing connector. *(on page)*

12. To give permissions to the user:

    a. Go to the **Roles** tab at the bottom of the page.

    b. Click **Edit**.

    c. In the **Collection** search box, search for these roles and click the arrow.

    - `rest_api_explorer`
    - `snc_platform_rest_api_access`
    - `itil`

    The selected roles are added to the Role List.

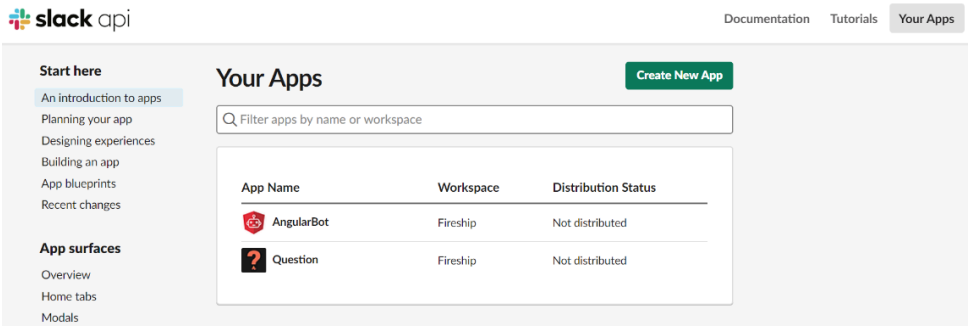
    d. Click **Save**.

13.2. Appendix B - Creating an Incoming Webhook in the Slack Channel

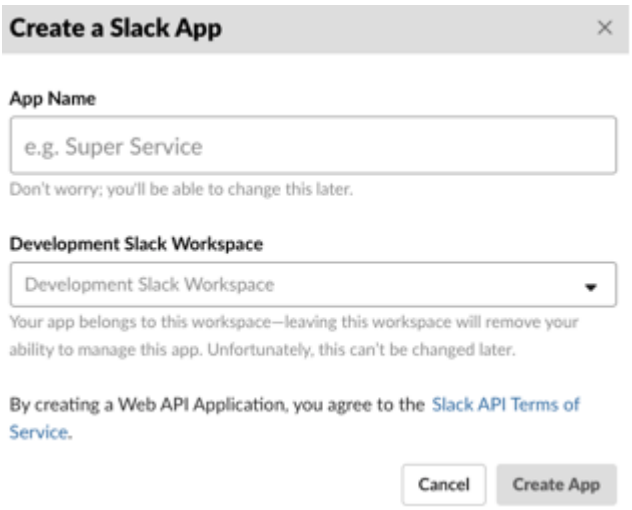
This task describes how to create an incoming webhook in a Slack channel. Follow the steps to configure a Slack application and obtain the webhook URL.

Procedure:

1. Go to https://api.slack.com/apps and sign in to your Slack account.
2. Create a Slack application.
    a. Go to **Your Apps** and click **Create New App**.



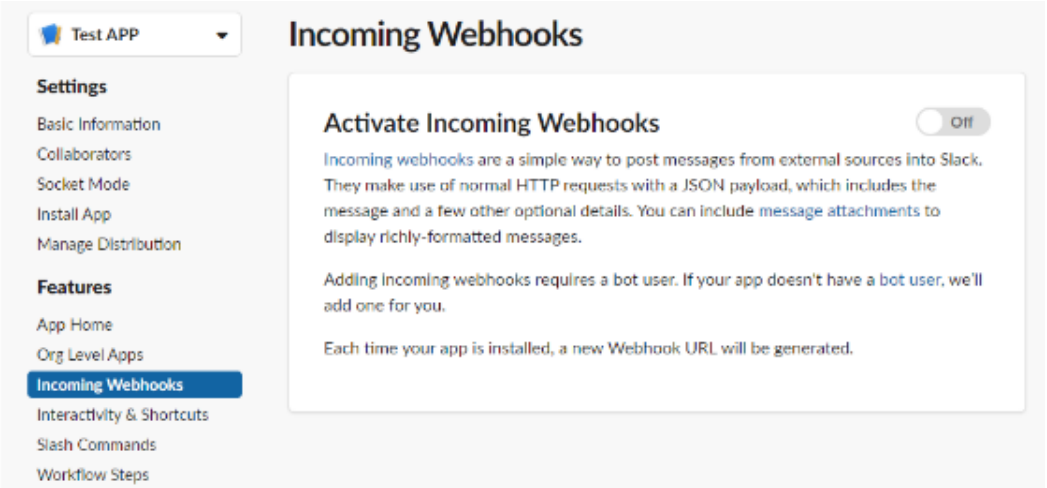
The **Create a Slack App** window appears.



    b. Enter a name for your application and select the workspace to connect the app.
    c. Click **Create App**.

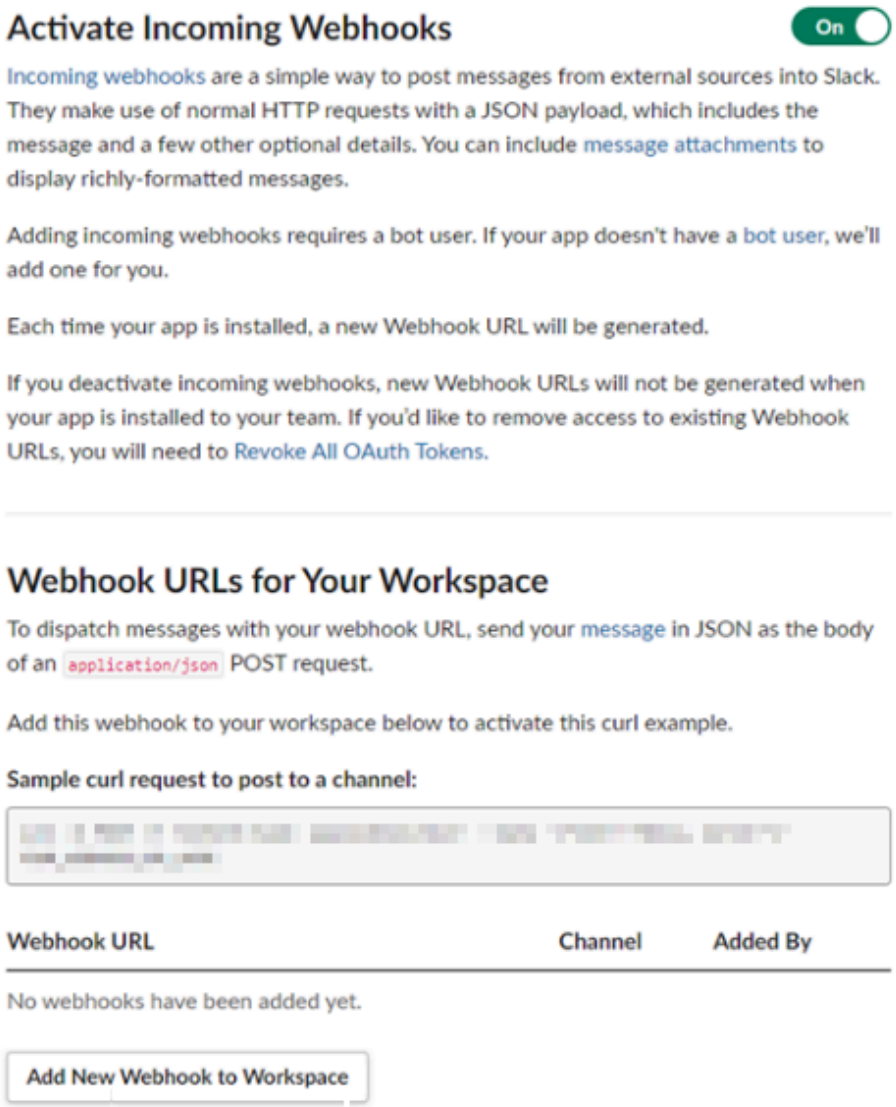
    You are redirected to the **Settings** page.

3. Go to **Features** > **Incoming Webhooks**.



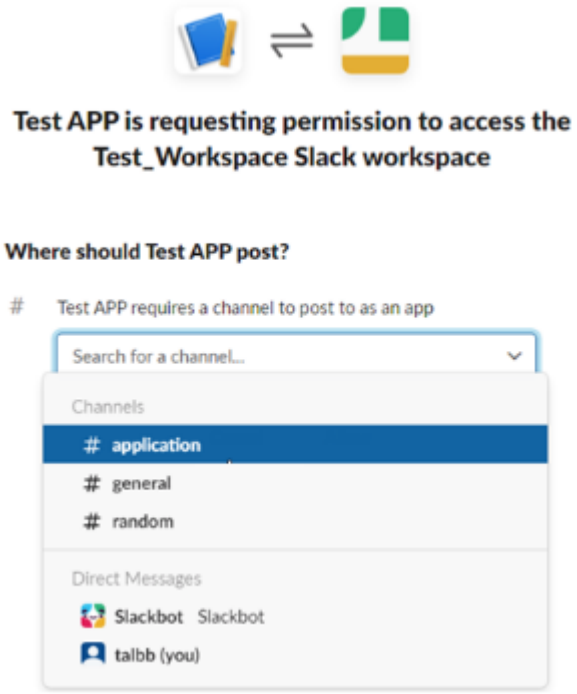
4. Turn on the **Active Incoming Webhooks** toggle button.

5. Click **Add New Webhook to Workspace**.

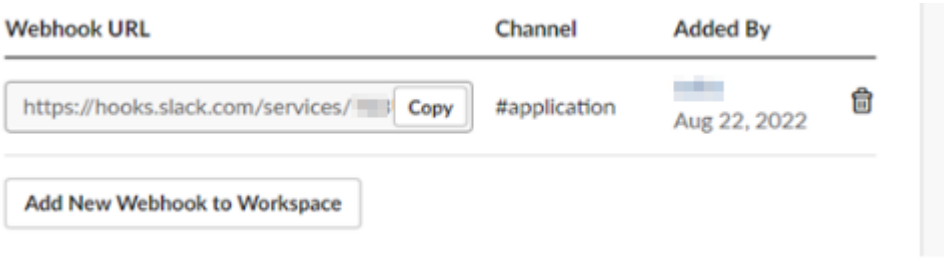


Choose the required channel from the options.

6. Select the channel from the list to which you want to add the webhook.



7. To copy the webhook URL, click **Copy**.



Note:

This URL is required to configure the Slack connector *(on page 233)*.

13.3. Appendix C - Creating Workflow for Microsoft Teams Notification

This task describes how to create a workflow for Microsoft Teams notifications using Microsoft Power Automate. Follow the steps to configure triggers and actions for Teams webhook requests.

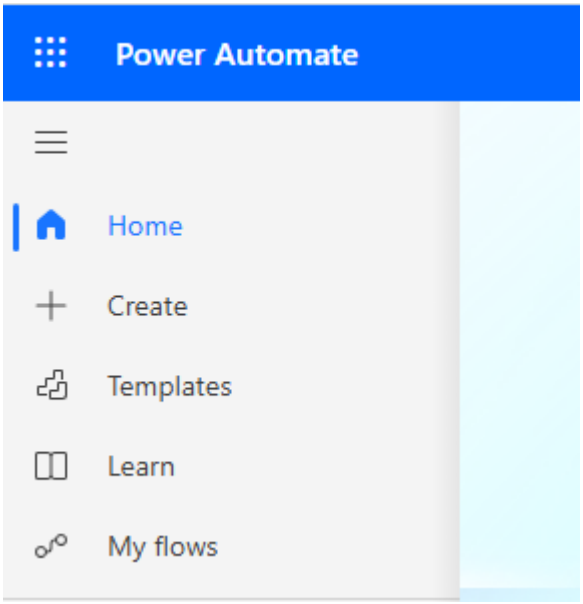
About this task:

Note:

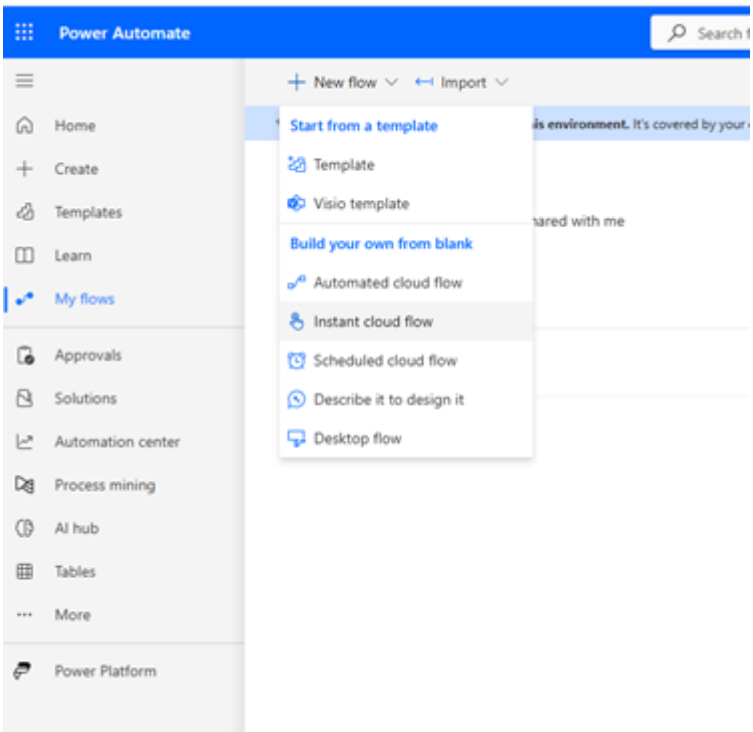
If you are using Microsoft Teams Classic, click on **Apps** in the sidebar, search for Workflows and then add Workflows. Click the **Post to a channel when a webhook request is received** workflow. Continue the instructions below from step **4**.

Procedure:

1. Go to Microsoft Power Automate.
2. In the left navigation pane, select **My Flows**.

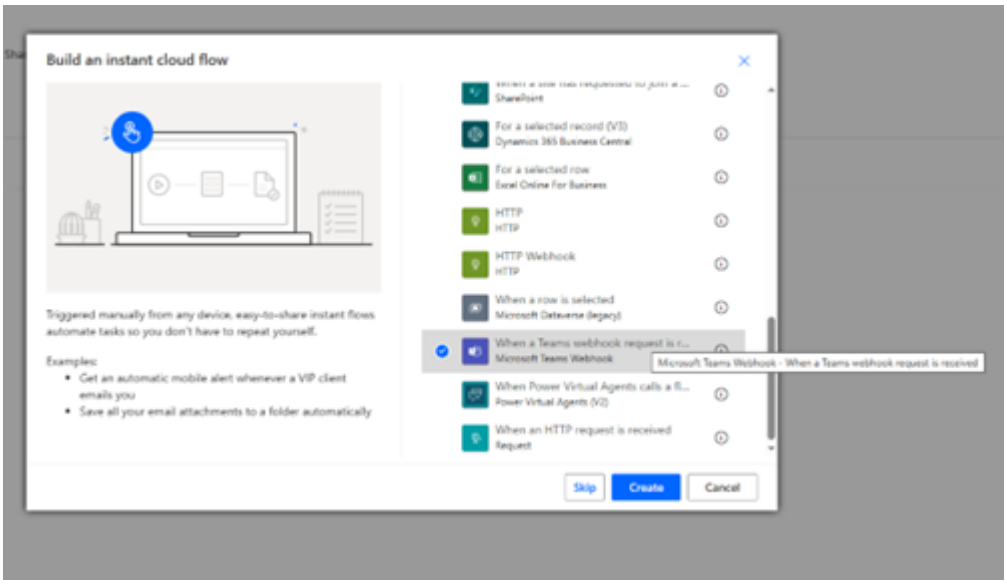


3. Under **New flow**, click **Instant cloud flow**.



4. Enter a name for the flow.

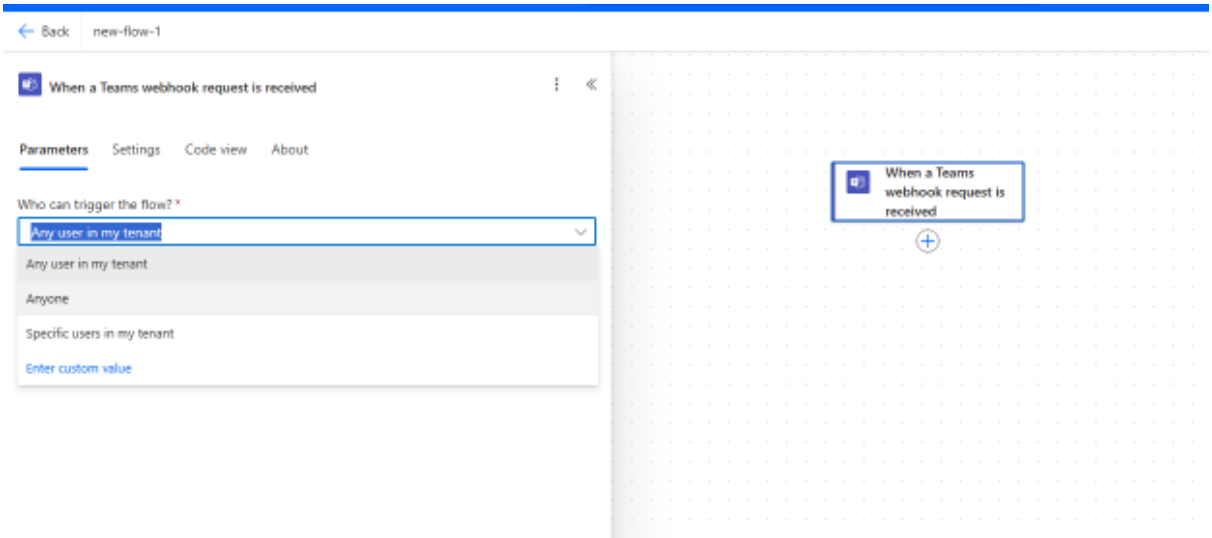
   Under Choose how to trigger this flow, select When a Teams webhook request is received.



5. Click **Create**.

6. Select **When a Teams webhook request is received** to open the side pane.

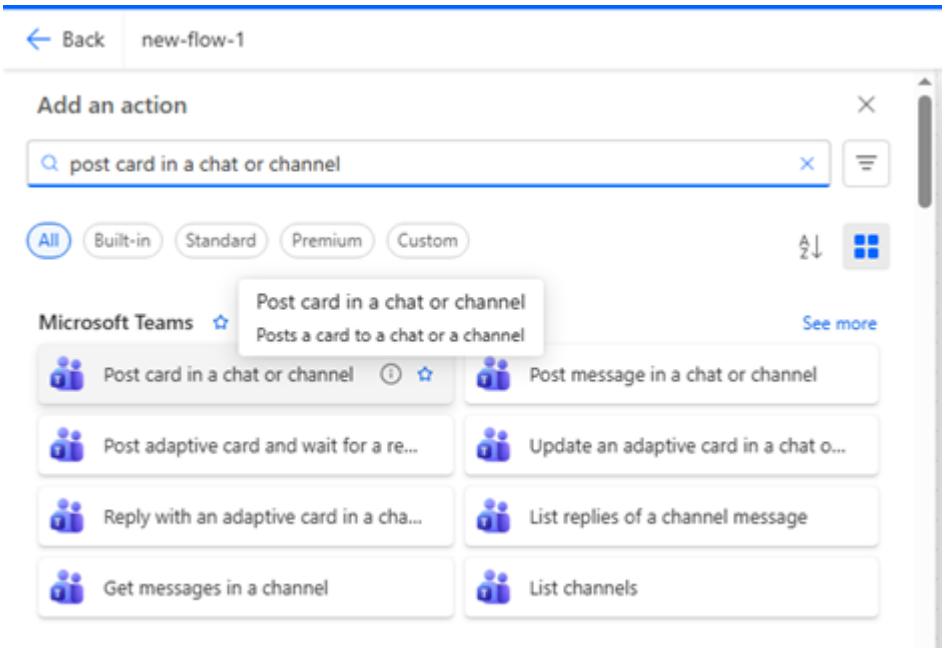
7. Under Parameters, from Who can trigger the flow?, select **Anyone**.



8. Close the side pane.

9. Click **+** below the trigger to add a new step.

10. Under **Add a new action**, select **Post card in a chat or channel**.

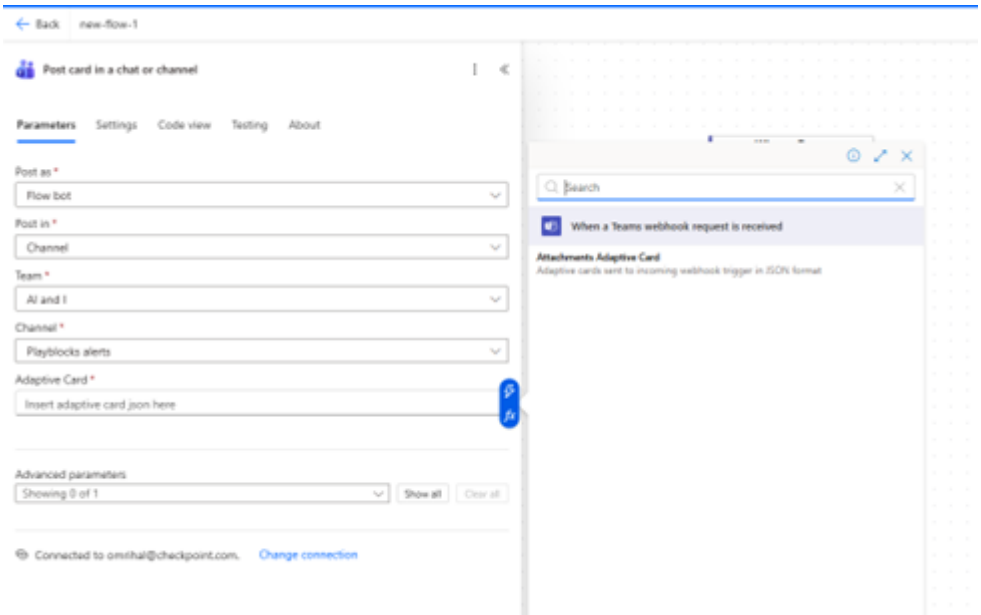


11. In the side pane, set these values.
    a. Post as: **Flow bot**
    b. Post in: **Channel**

12. From **Team**, select your team.

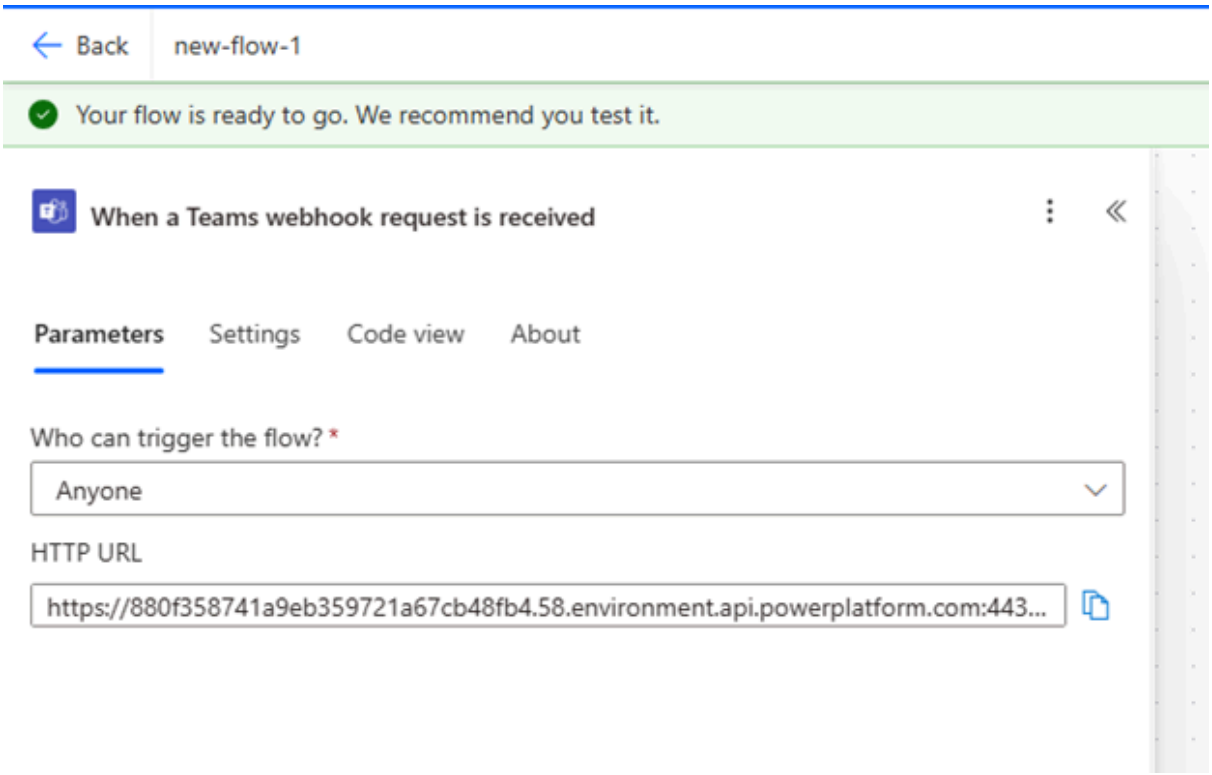
13. From Channel, select your channel.

14. In **Adaptive card**, click **Enter the data from previous step** (blue lightning icon), and then select **Attachment adaptive card**.



15. Click **Save**.

16. Select **When a Teams webhook request is received** to open the side pane again.
17. Under Parameters, copy the HTTP URL.



13.4. Appendix D - Creating an API Token in Atlassian Account

This task describes how to create an API token in an Atlassian account for Jira integration with Playblocks. It includes step-by-step instructions for generating and copying the token.

About this task:

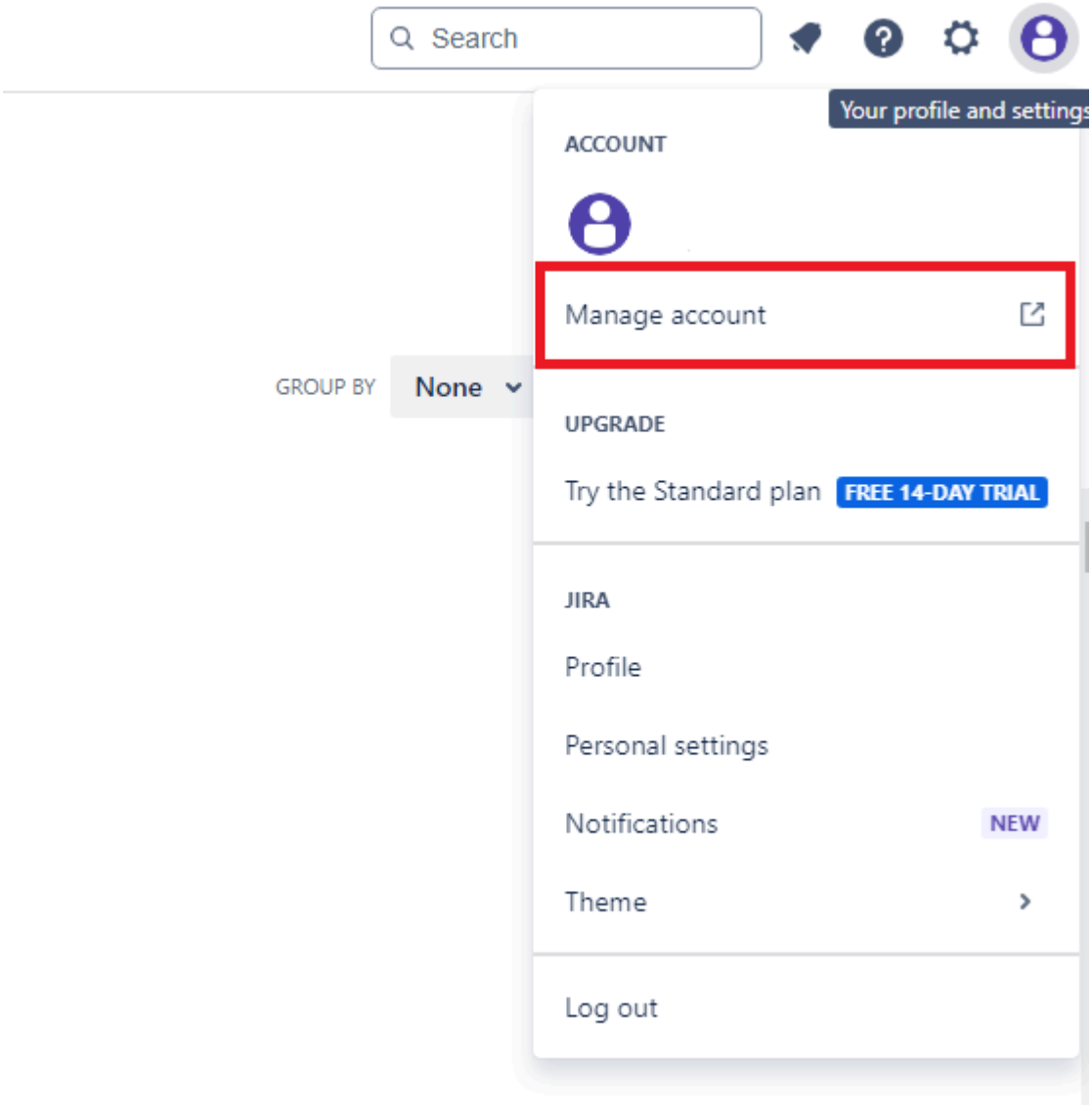
https://embed.app.guidde.com/playbooks/j1Sy8c5F5kvstDTWPuMf1A

Procedure:

1. Log in to your Atlassian account.

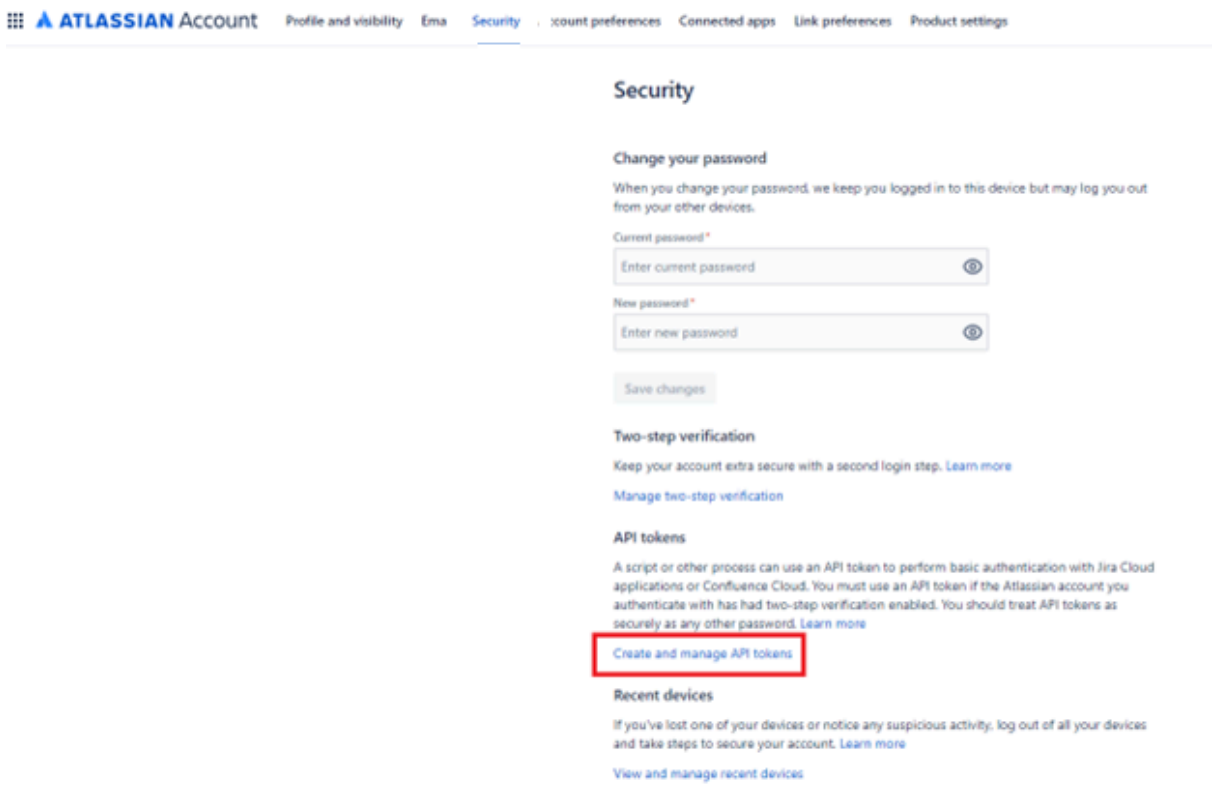
   https://instancename.atlassian.net

2. Click your profile icon at the top left corner and select **Manage account**.

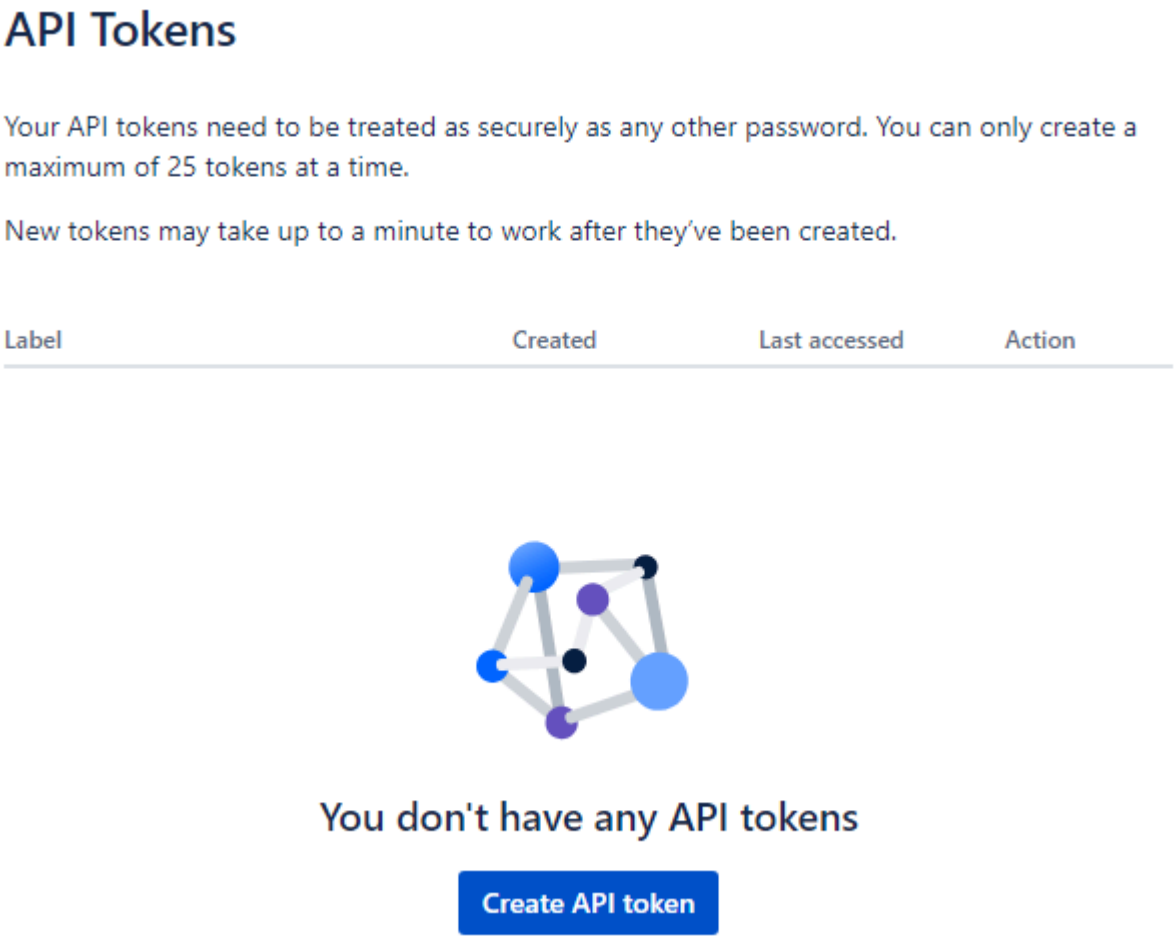


3. Click the **Security** tab.

4. In the **API tokens** section, click **Create and manage API tokens**.

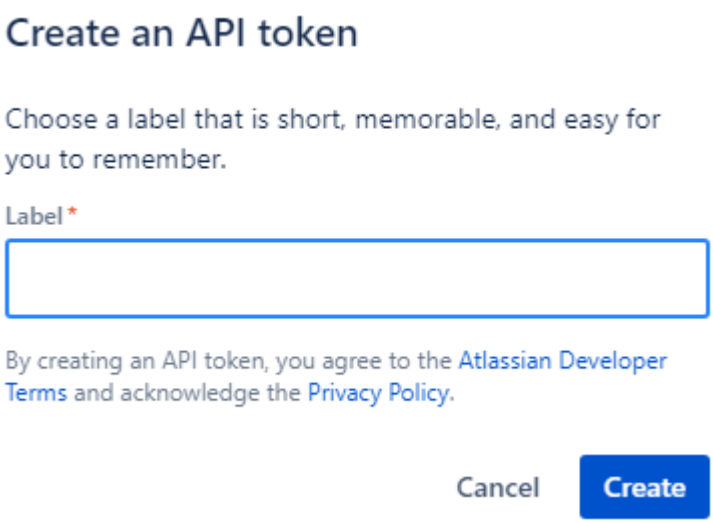


The **API Tokens** page appears.



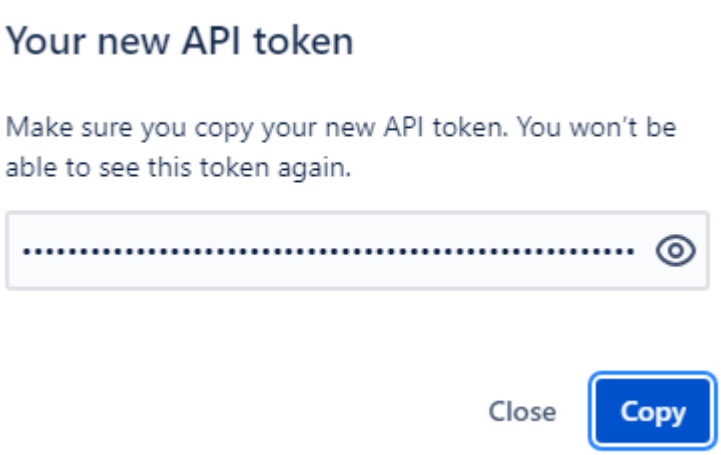
5. Click **Create API token**.

   The **Create an API token** window appears.



6. In the **Label** field, enter a name for the token.
7. Click **Create**.

   The **Your new API token** window appears.



8. Click **Copy**.

> **Note:**
>
> After this step, you cannot retrieve the token.
>
> API Token is the **Password** specified when you configure the Jira ticketing connector *(on page 231)*.

13.5. Appendix E - Integrating CrowdStrike Falcon

This topic describes how to integrate Check Point Playblocks with CrowdStrike Falcon to enable automated alert handling and response actions. It outlines the steps required to configure API access in the CrowdStrike Falcon portal.

About this task:

The integration of Playblocks with CrowdStrike Falcon allows you to receive real-time alerts and take corrective actions using automated workflows. These workflows improve response time and threat management efficiency.

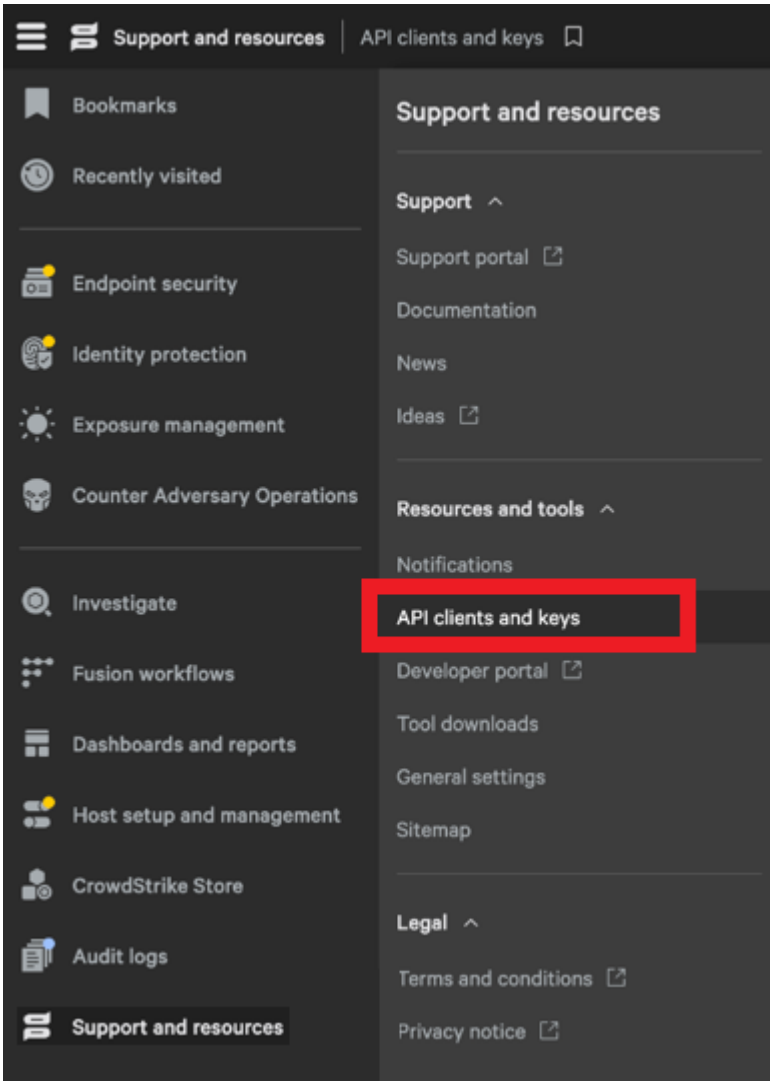
Note:

Make sure you have the necessary permissions to isolate (contain) and de-isolate devices.

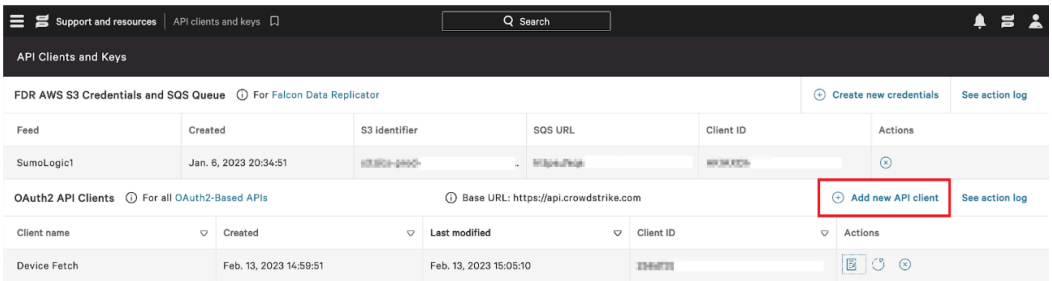
Procedure:

Log in to the CrowdStrike Falcon web portal.

a. Go to **Support and resources** > **API clients and keys**.

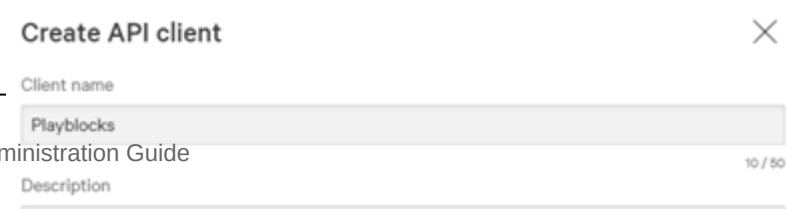


The **API Clients and Keys** window appears.



b. Click **Add new API client**.

The **Create API client** window appears.



13.6. Appendix F - Creating a SentinelOne Service User

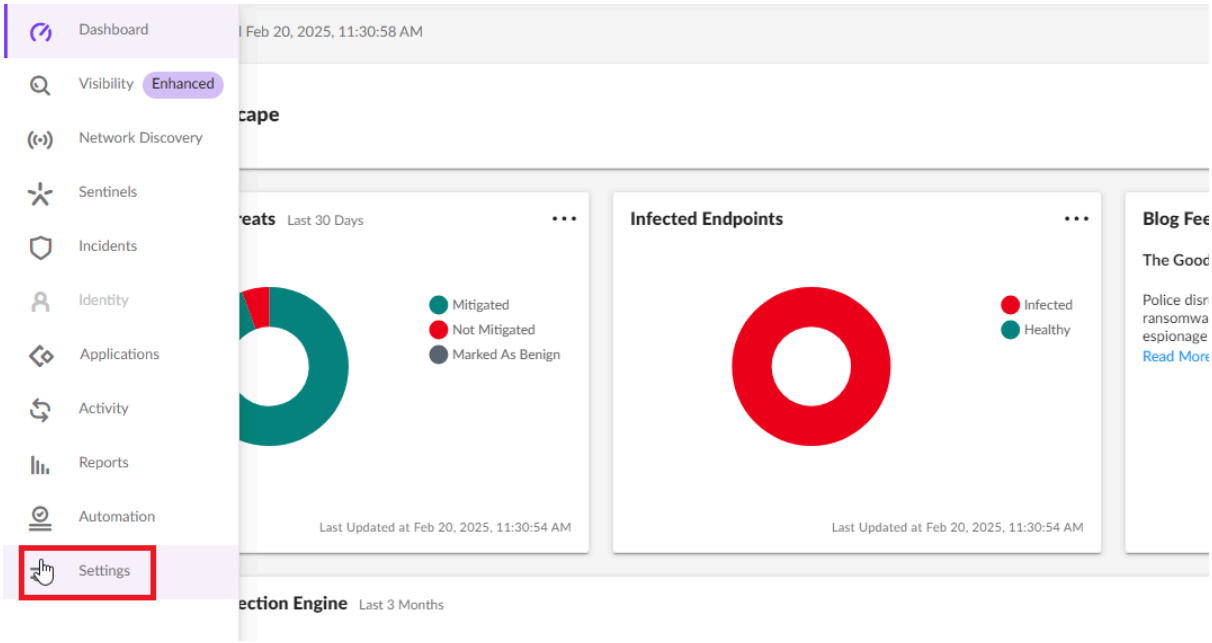
This task describes how to create a SentinelOne service user with specific role permissions. It guides you through configuring roles, permissions, and generating an API token.

Before you begin:

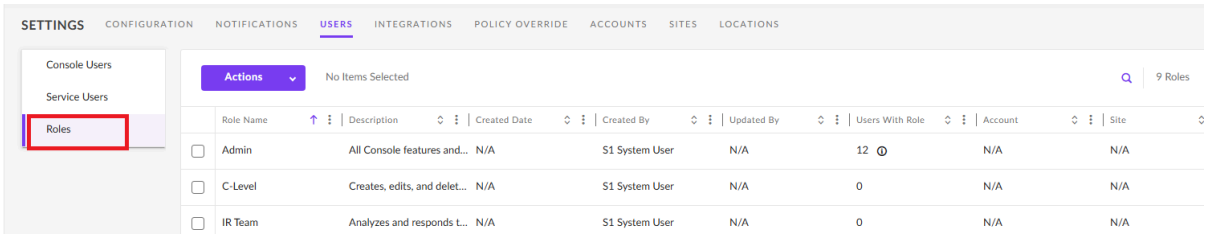
You must have access to the SentinelOne web portal with permissions to create roles and service users.

Procedure:

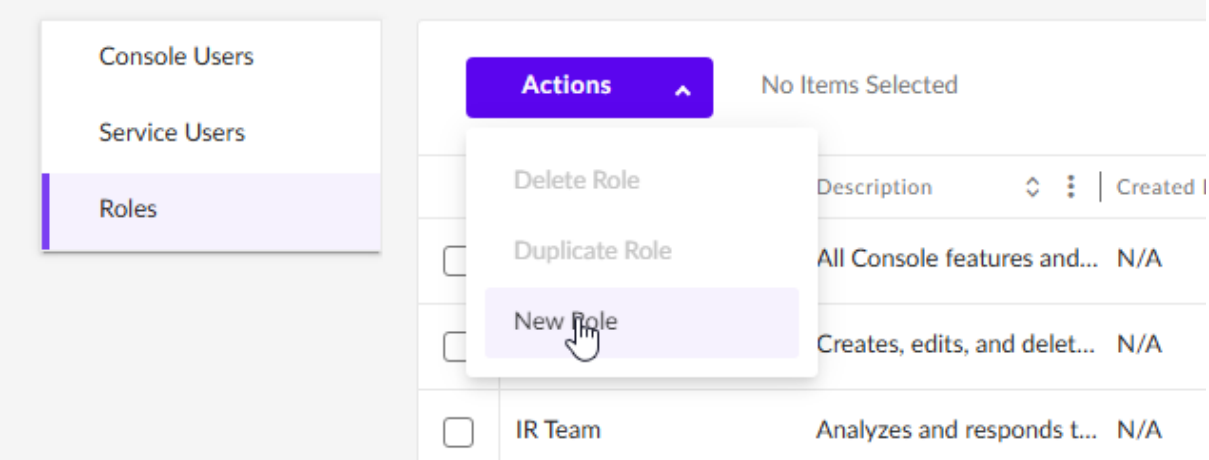
1. Log in to the SentinelOne web portal.
2. Click **Settings**.



3. Go to the **Users** tab and click **Roles**.



4. From the **Actions** list, select **New Role**.



The **New Role** window appears.

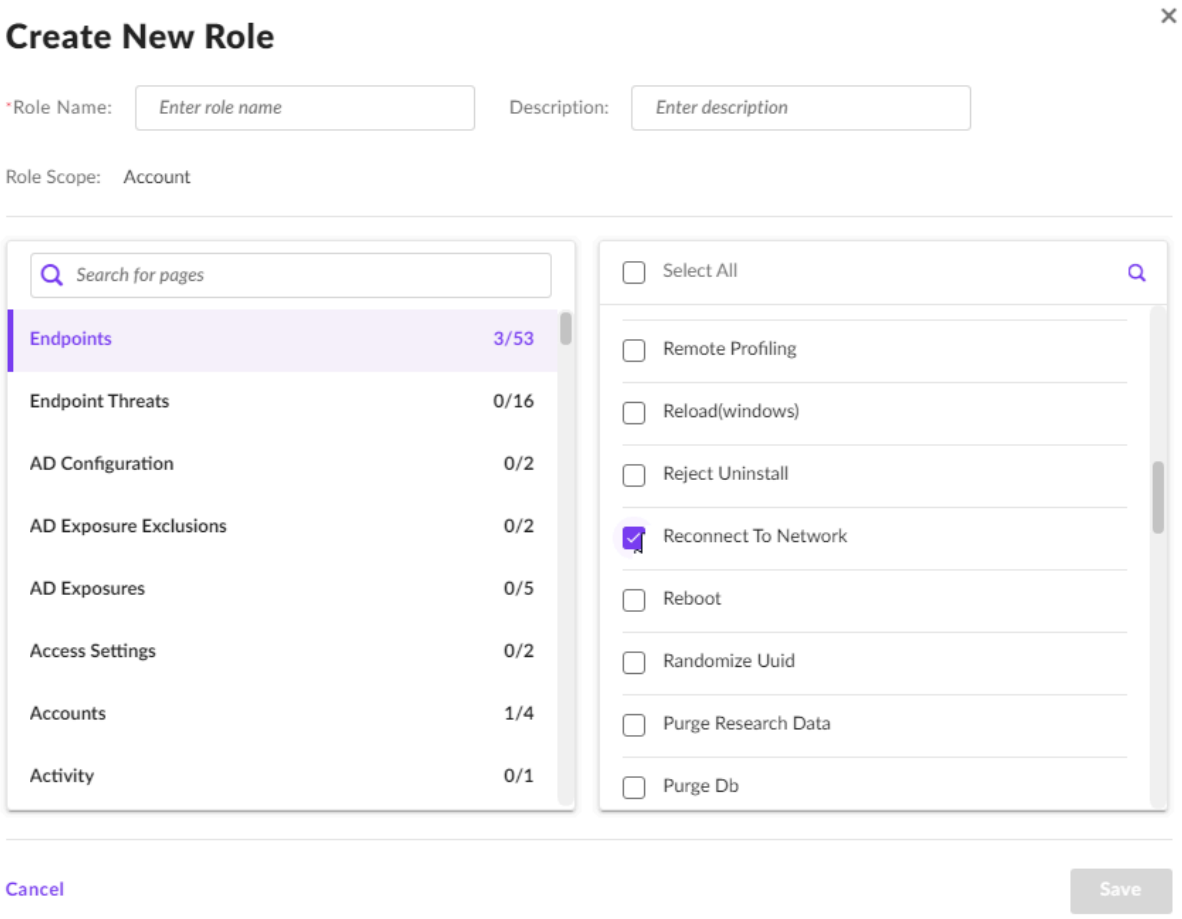
5. In the **Role Name** field, enter a name for the role.
6. In the **Description** field, enter the description.

7. In the search field, search and select these permissions and click **Save**.

   Permissions:

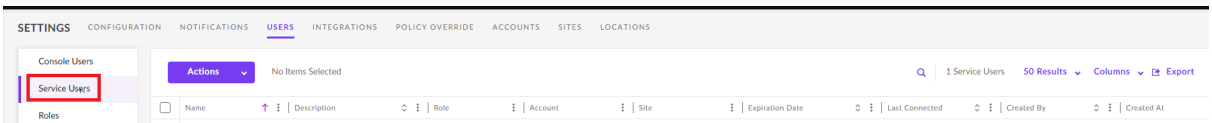
Page	Permission
Endpoints	Reconnect To Network
Endpoints	Disconnect From Network
Endpoint Threat	View
Threat Intelligence	Manage
Service Users	Create

   For example:

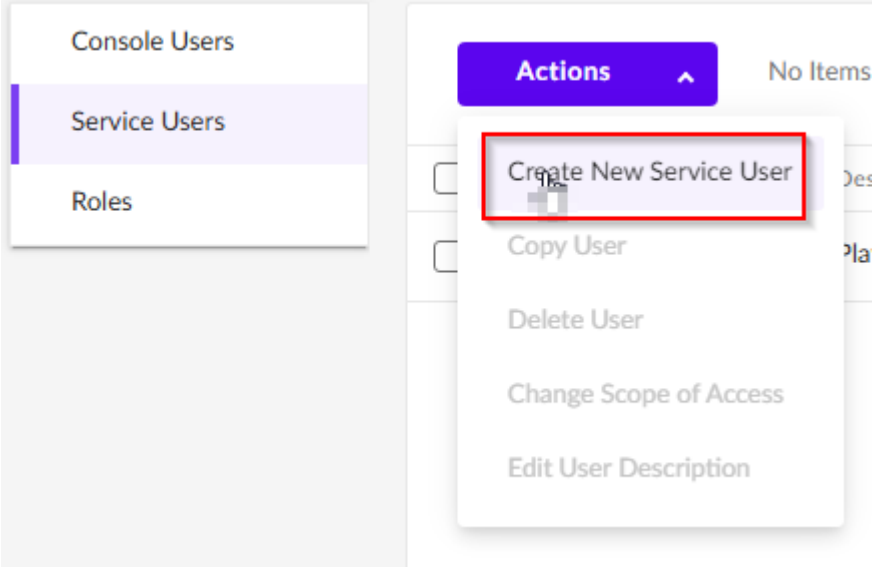


8. Click **Save** and verify that the roles are created.

9. Click **Service Users**.



10. From the **Actions** list, select **Create New Service User**.

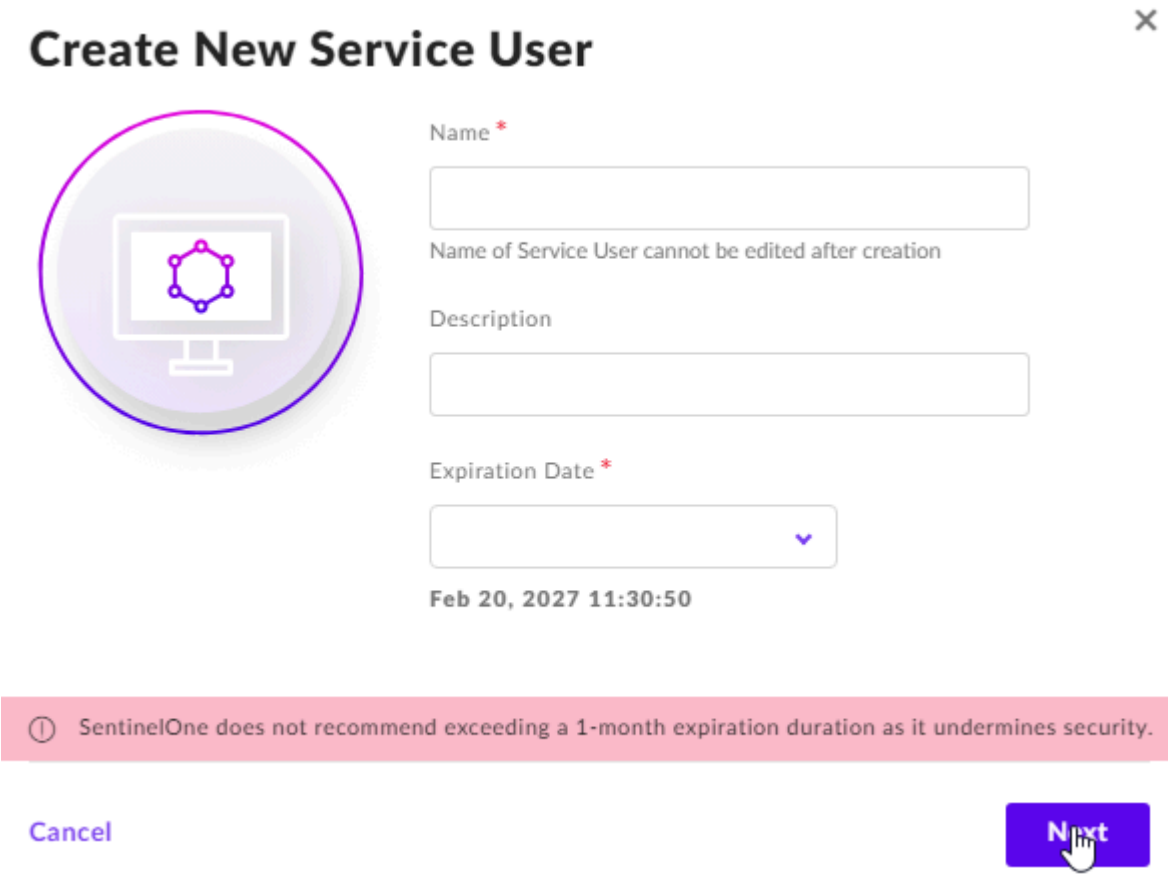


11. Specify these:

    a. **Name**

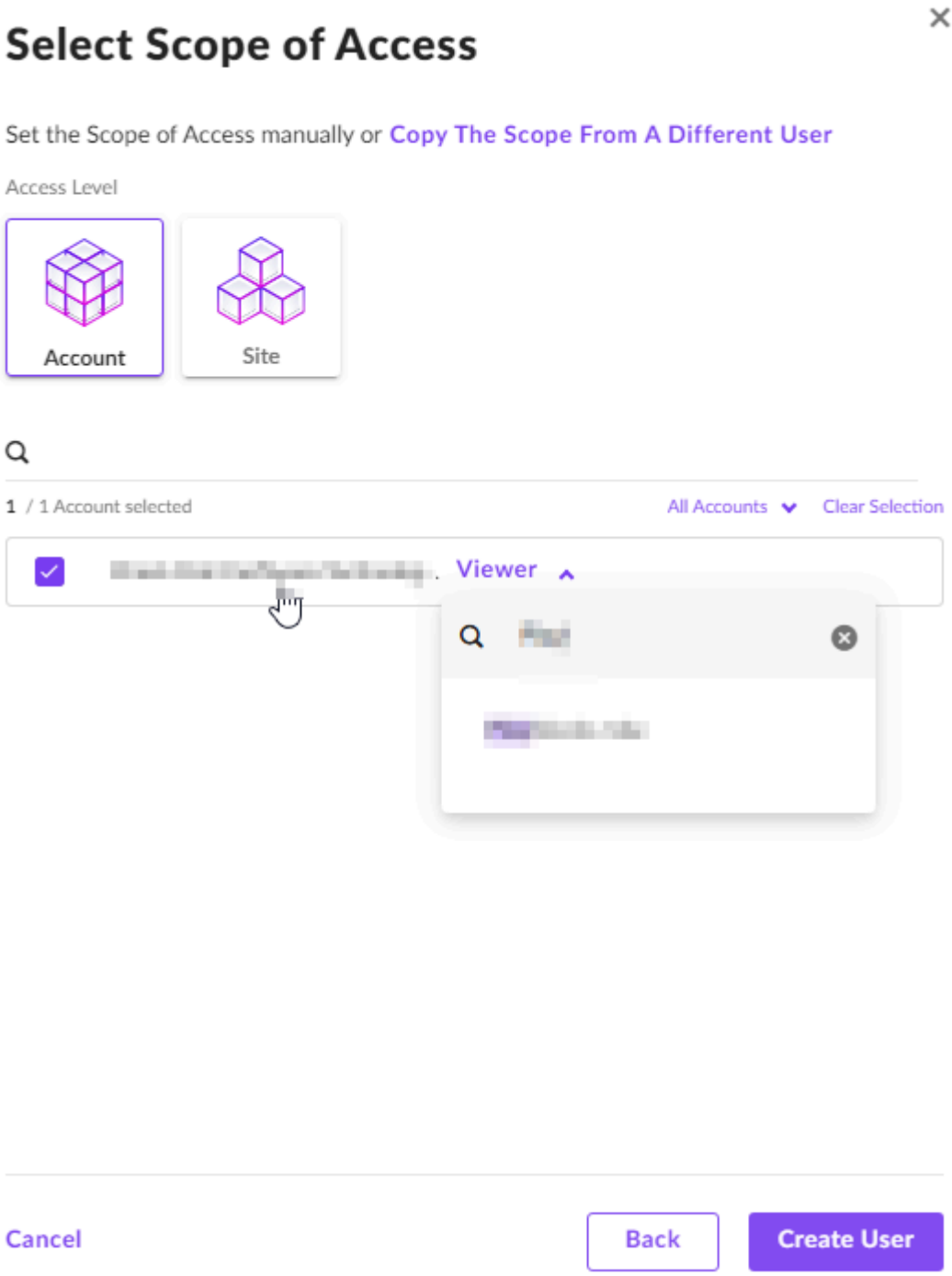
    b. **Description**

    c. **Expiration Date**



12. Click **Next**.

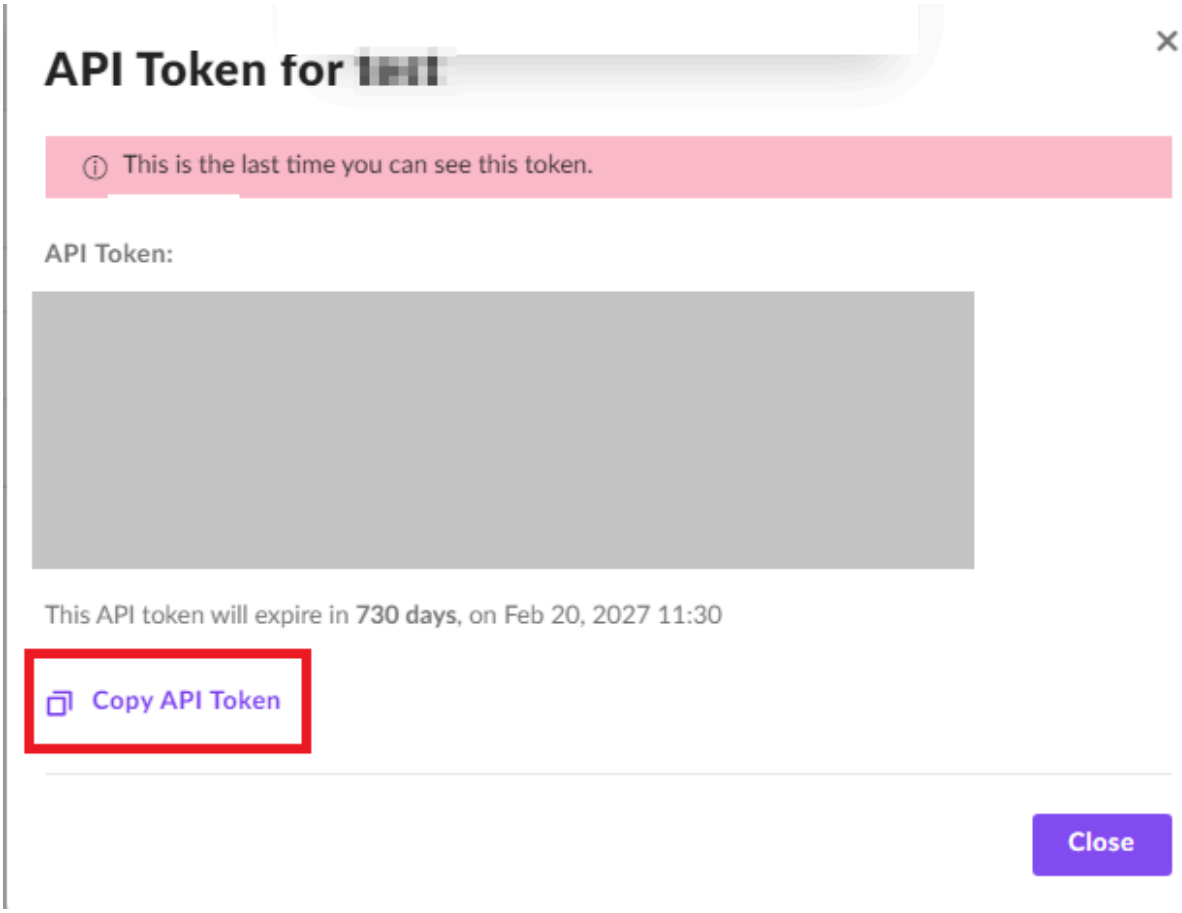
    The **Select Scope of Access** window appears.



13. In the **Access Level** section, select **Account**.
14. Search and select your account.
15. From the **Viewer** list, select the new role that you just created.

16. Click **Create User**.

    The **API Token** window appears.



17. To copy the API Token, click **Copy API Token**.

    Notes:

    - After this step, you cannot retrieve the token.
    - This API Token is required to Configure the SentinelOne connector *(on page 250)*.

18. Click **Close**.

13.7. Appendix G - Using Custom Automation Step Schemas

This topic describes parameter schemas for supported step types in custom automations and references the full Automations API documentation. It provides validation rules and dynamic reference details for automation steps.

This topic defines parameter schemas for all supported step types in Playblocks custom automations. Each step includes validation rules and dynamic reference capabilities for use with the Playblocks Automations API.

For the complete Playblocks Automations API, see the Swagger documentation.

13.7.1. Parameter References

This topic describes supported parameter reference types and how they enable dynamic retrieval of values from automation steps or parameters. It also outlines the characteristics of each reference type.

Supported Reference Types

Many parameters support Parameter References that allow you to dynamically reference values from previous steps or automation parameters:

- **Step References**: {{step['Step Name']['field_name']}} - References output from a previous step in the automation flow
- **Automation Parameter References**: {{automationParam['parameter_name']}} - References user-defined automation parameters that are passed when the automation is executed

Reference Types

- `ParamRef`:
  - Supports step outputs and Automation parameters.
  - Most flexible and used where dynamic behavior is expected.
- `AutoParamRef`:
  - Supports automation parameters only and step references not allowed.
  - Restricts to inputs provided by the user during automation execution.

13.7.2. Step Categories

This topic lists the available step categories used within automation workflows. It provides quick navigation to each category type.

1. Triggers *(on page 287)*
2. Notifications *(on page 292)*
3. Enrichments *(on page 295)*
4. Conditions *(on page 297)*
5. Actions *(on page 298)*
6. Create IOC Management Indicators *(on page 299)*
7. Run Automation *(on page 300)*

13.7.3. Triggers

This topic describes trigger types and their parameters for automation workflows. It includes log, schedule, and webhook triggers with detailed parameter schemas and examples.

Triggers

Trigger steps define how and when an automation starts.

Log Trigger

Monitors log sources and triggers automation when specified conditions are met.

Parameters Schema

```
{
  "filter": string (required),
  "interval": TimeInterval (required),
  "log_type": string (required),
  "source": string (required),
  "conditions": LogTriggerCondition[] (optional)
}
```

Parameters Detail

- **filter** (string, required): Log filter query using the log search syntax
- **interval** (TimeInterval, required): How frequently to check for new logs (minimum 15 seconds)

```
{
"value": number,
"unit": "seconds" | "minutes" | "hours" | "days"
}
```

- **log_type** (string, required): Type of logs to monitor
  - Valid values: "logs", "audit"
- **source** (string, required): Log source to monitor
  - Valid values: Quantum Management, Endpoint Security, Quantum SD-WAN, CloudGuard WAF, Email Security, SASE
- **conditions** (array, optional): Additional conditions to apply to the logs

Log Trigger Condition Types

- Check List

  Verify if field values exist in predefined lists.

```
{
  "type": "Check List",
  "parameters": {
    "value_to_check": string (optional),
    "lists": string[] (optional)
  }
}
```

  Parameter Details:

  - value_to_check (string, optional): The log field name whose value should be checked against the selected lists
  - lists (array, optional): Names of predefined lists to check against
    - Valid lists values: `Allowed Sources`, `Quarantined Sources`, `Blocked Sources`, `Blocked Destinations`, `Isolated Devices`, `Playblocks IOCs`

- value_to_check (string, optional): The log field name whose value should be checked against the selected lists
- lists (array, optional): Names of predefined lists to check against
  - Valid lists values: `Allowed Sources`, `Quarantined Sources`, `Blocked Sources`, `Blocked Destinations`, `Isolated Devices`, `Playblocks IOCs`
- Valid lists values: `Allowed Sources`, `Quarantined Sources`, `Blocked Sources`, `Blocked Destinations`, `Isolated Devices`, `Playblocks IOCs`
- Check Fields Values

  Match, contains, or exclude field values.

```
{
  "type": "Check Fields Values",
  "parameters": {
    "match_check": [{"field": string, "value": string}],
    "contains_match_check": [{"field": string, "value": string}],
    "not_match_check": [{"field": string, "value": string}]
  }
}
```

  Parameter Details:

  - **match_check** (string, optional): Array of field-value pairs that must match exactly. The log will only trigger if all specified fields have exactly the specified values.
  - **contains_match_check** (array, optional): Array of field-value pairs where the field must contain the specified value as a substring. Useful for partial text matching.
  - **not_match_check** (array, optional): Array of field-value pairs that must not match. The log will only trigger if none of the specified fields have the specified values.

- **match_check** (string, optional): Array of field-value pairs that must match exactly. The log will only trigger if all specified fields have exactly the specified values.
- **contains_match_check** (array, optional): Array of field-value pairs where the field must contain the specified value as a substring. Useful for partial text matching.
- **not_match_check** (array, optional): Array of field-value pairs that must not match. The log will only trigger if none of the specified fields have the specified values.
- Check Fields Exist

  Verify that specific fields exist in the log.

```
1
2 {
3  "type": "Check Fields Exist",
4  "parameters": {
5  "fields": string[]
6  }
7 }
8
```

  Parameter Details:

  fields (array, required): Array of log field names that must be present in the log entry. The condition will only be satisfied if all specified fields exist in the log, regardless of their values.

- Count Logs

  Count logs based on criteria.

```
1
2 {
3  "type": "Count Logs",
4  "parameters": {
5  "expression_1": {
6  "function": "CountDistinct" | "CountOccurrences",
7  "value": string | ParamRef
8  },
9  "operator": "Equal to" | "Not equal to" | "Greater than" | "Greater than or
   equal to" | "Less than" | "Less than o",
10  "expression_2": number | AutoParamRef,
11  "time_frame": TimeInterval | ParamRef,
12  "enrich_logs_with_fields": string[] | ParamRef (optional)
13  }
14 }
15
```

  Parameter Details:

  - **expression_1** (object, required): Defines what to count in the logs
    - function: `CountDistinct` counts unique values, `CountOccurrences` counts total occurrences
    - value: The log field name to count (example, `source_ip` to count unique IP addresses)
  - **operator** (string, required): Comparison operator for the count condition
  - **expression_2** (number/AutoParamRef, required): The threshold number to compare against
  - **time_frame** (TimeInterval/ParamRef, required): Time window for counting logs (for example, count logs in the last 5 minutes)
  - **enrich_logs_with_fields** (array, optional): Additional log fields to include in the trigger output for context

- **expression_1** (object, required): Defines what to count in the logs
  - function: `CountDistinct` counts unique values, `CountOccurrences` counts total occurrences
  - value: The log field name to count (example, `source_ip` to count unique IP addresses)
- function: `CountDistinct` counts unique values, `CountOccurrences` counts total occurrences
- value: The log field name to count (example, `source_ip` to count unique IP addresses)
- **operator** (string, required): Comparison operator for the count condition
- **expression_2** (number/AutoParamRef, required): The threshold number to compare against
- **time_frame** (TimeInterval/ParamRef, required): Time window for counting logs (for example, count logs in the last 5 minutes)

- **enrich_logs_with_fields** (array, optional): Additional log fields to include in the trigger output for context

- Alert Again

  Control re-alerting behavior.

```
1
2  {
3   "type": "Alert Again",
4   "parameters": {
5   "alert_again_time": TimeInterval | ParamRef,
6   "log_fields_for_key": string[] (optional),
7   "log_fields_for_value": string[] (optional)
8   }
9  }
10
```

  Parameter Details:

  - **alert_again_time** (TimeInterval/ParamRef, required): Time interval that must pass before the same alert can be triggered again
  - **log_fields_for_key** (array, optional): Log field names used to create a unique identifier (key)
  - **log_fields_for_value** (array, optional): Log field names used to create a unique identifier value

13.7.4. Notifications

This topic describes notification-related automation steps including Ask, Notify, and Open Ticket. It provides parameter schemas, detailed descriptions, and examples.

Notification steps handle user interaction and external communications.

Ask

Prompts users for input with predefined response options.

Ask - Parameters Schema

```
1  {
2          "subject": string (required),
3          "message": string (required),
4          "event_details": EventDetails (required),
5          "user_response_options": string[] (required),
6          "response_option_after_timeout": string (required),
7          "notification_profile": string | AutoParamRef (required)
8          }
```

Ask - Parameters Detail

- **subject** (string, required): Question or prompt title (max length is 300 characters)
- **message** (string, required): Detailed message or description (max length is 600 characters)

- **event_details** (object, required): Structured information to display to users in notifications and prompts. This allows you to present relevant context data in a formatted way, such as IP addresses, user names, timestamps, or any other relevant information from the automation flow.

```
{
            "enabled": boolean,
            "event_details_fields": [
            {
            "name": string,
            "value": string | number | ParamRef
            }
            ]
            }
```

- **user_response_options** (array, required): Exactly 2 unique response options
- **response_option_after_timeout** (string, required): Default response if user do not respond (must match one of the response options)
- **notification_profile** (string, required): Notification delivery method that determines how and to whom the notification is sent. This refers to predefined notification profiles configured in your Playblocks system, such as Immediate attention, Low attention, or custom profiles that specify recipients, delivery channels (such as email, SMS, and so on), and timing preferences.

Ask - Example

```
{
        "type": "Ask",
        "name": "Approve Action",
        "parameters": {
        "subject": "Suspicious activity detected",
        "message": "Should we block this IP address?",
        "event_details": {
        "enabled": true,
        "event_details_fields": [
        {
        "name": "IP Address",
        "value": "{{step['Log Trigger']['client_ip']}}"
        }
        ]
        },
        "user_response_options": ["Block", "Ignore"],
        "response_option_after_timeout": "Block",
        "notification_profile": "Immediate attention"
        }
        }
```

Notify

Sends notifications to users or teams.

Notify - Parameters Schema

```
{
        "subject": string | ParamRef (required),
        "message": string | ParamRef (optional),
        "event_details": EventDetails (required),
        "notification_profile": string | AutoParamRef (required)
        }
```

Notify - Parameters Detail

- **subject** (string/ParamRef, required): Notification subject/title (max length is 300 characters)
- **message** (string/ParamRef, optional): Notification body message (max length is 600 characters)
- **event_details** (object, required): Structured information to display to users in notifications and prompts. This allows you to present relevant context data in a formatted way, such as IP addresses, user names, timestamps, or any other relevant information from the automation flow.
- **notification_profile** (string, required): Notification delivery method that determines how and to whom the notification is sent. This refers to predefined notification profiles configured in your Playblocks system, such as "Immediate attention", "Low attention", or custom profiles that specify recipients, delivery channels (email, SMS, webhook), and timing preferences.

Notify - Example

```
{
        "type": "Notify",
        "name": "Notify admins",
        "parameters": {
        "subject": "Expert Shell login detected",
        "message": "Administrative access detected on critical system",
        "event_details": {
        "enabled": true,
        "event_details_fields": [
        {
        "name": "Administrator",
        "value": "{{step['Expert Shell login']['administrator']}}"
        },
        {
        "name": "Client IP",
        "value": "{{step['Expert Shell login']['client_ip']}}"
        }
        ]
        },
        "notification_profile": "Immediate attention"
        }
        }
```

Open Ticket

Creates tickets in external ticketing systems.

Open Ticket - Parameters Schema

```
{
        "subject": string | ParamRef (required),
        "description": string | ParamRef (required),
        "event_details": EventDetails (required),
        "ticket_types": TicketTypes (optional)
        }
```

Open Ticket - Parameters Detail

- **subject** (string/ParamRef, required): Ticket title/summary (max length is 300 characters)
- **description** (string/ParamRef, required): Ticket description/details (max length is 600 characters)

- **event_details** (object, required): Structured information to include with the ticket. This allows you to attach relevant context data to the ticket, such as affected systems, security indicators, timestamps, or any other information that will help ticket handlers understand and respond to the issue.
- **ticket_types** (object, optional): Ticket type per connector

```
{
            "jira": string | ParamRef (optional),
            "service_now": string | ParamRef (optional)
            }
```

  - Valid service_now values: `Low`, `Moderate`, `High`, `Critical`

Open Ticket - Example

```
{
        "type": "Open Ticket",
        "name": "Create Security Incident",
        "parameters": {
        "subject": "Security Alert: {{step['Log Trigger']['event_type']}}",
        "description": "Automated security incident created from Playblocks",
        "event_details": {
        "enabled": true,
        "event_details_fields": [
        {
        "name": "Source IP",
        "value": "{{step['Log Trigger']['source_ip']}}"
        },
        {
        "name": "Severity",
        "value": "High"
        }
        ]
        },
        "ticket_types": {
        "jira": "Default",
        "service_now": "Moderate"
        }
        }
        }
```

13.7.5. Enrichments

This topic describes enrichment steps that gather additional information about IPs, URLs, and files. It includes parameter schemas, details, and examples for each enrichment type.

Enrich IP

Enriches IP addresses with reputation and geo-location data.

Enrich IP - Parameters Schema

```
{
        "ip": string | ParamRef (required)
        }
```

Enrich IP - Parameters Detail

ip (string/ParamRef, required): IPv4 address to enrich (must be valid IPv4 format when not using parameter reference)

Enrich IP - Example

```
{
        "type": "Enrich IP",
        "name": "Enrich client IP",
        "parameters": {
        "ip": "{{step['Expert Shell login']['client_ip']}}"
        }
        }
```

Enrich URL

Enriches URLs with reputation and analysis data.

Enrich URL - Parameters Schema

```
{
        "url": string | string[] | ParamRef (required)
        }
```

Enrich URL - Parameters Detail

url (string/array/ParamRef, required): URL(s) to enrich (must be valid URL format when not using parameter reference)

Enrich URL - Example

```
{
        "type": "Enrich URL",
        "name": "Analyze suspicious URL",
        "parameters": {
        "url": "{{step['Log Trigger']['requested_url']}}"
        }
        }
```

Enrich File

Enriches file hashes with reputation and analysis data.

Enrich File - Parameters Schema

```
{
        "file_hash": string | ParamRef (required)
        }
```

Enrich File - Parameters Detail

file_hash (string/ParamRef, required): File hash to enrich (must be valid MD5, SHA-1, or SHA-256 hash when not using parameter reference)

Enrich File - Example

```
{
        "type": "Enrich File",
        "name": "Check file reputation",
        "parameters": {
        "file_hash": "{{step['Log Trigger']['file_hash']}}"
        }
        }
```

13.7.6. Conditions

This topic describes conditional logic steps used in automation flows and details their parameters and usage. It includes schema definitions, parameter descriptions, and example structures.

Conditions

Condition steps implement conditional logic in automation flows.

Condition

Evaluates conditions and determines the next step based on the result.

Parameters Schema

```
{
        "condition": Condition[] (required)
        }
```

Condition Object

```
{
        "expression_1": ParamRef (required),
        "operator": string (required),
        "expression_2": string | number | boolean (required)
        }
```

Parameters Detail

- **conditions**(array, required): Array of condition objects to evaluate
- **expression_1** (ParamRef, required): Parameter reference to evaluate (must be in format `{{step['Step Name']['field']}}`)
- **operator** (string, required): Comparison operator
    - Valid values: `Equal to`, `Not equal to`, `Greater than`, `Greater than or equal to`, `Less than`, `Less than or equal to`
- **expression_2** (string/number/boolean, required): Value to compare against

Example

```
{
        "type": "Condition",
        "name": "Check IP reputation",
        "parameters": {
        "conditions": [
        {
        "expression_1": "{{step['Enrich client IP']['reputation']}}",
        "operator": "Equal to",
        "expression_2": "Malicious"
        }
        ]
        }
        }
```

13.7.7. Actions

Describes actions, schemas, parameters, and examples for automation, list management, IOC creation, and running automation tasks. Provides detailed structures and valid input formats.

Actions

Action steps perform specific operations like blocking IPs, creating indicators, or running other automations.

Add to List

Adds elements (IPs, domains, ranges) to security lists on Quantum Gateway.

Parameters Schema

```
{
  "element": string | ParamRef (required),
  "list": string (required),
  "exceptions_list": string (optional),
  "duration": TimeInterval | ParamRef (required),
  "add_reason": string (required)
}
```

Parameters Detail

- **element** (string/ParamRef, required): IPv4 address to add to the list (must be valid IPv4 when not using parameter reference)
- **list** (string, required): Target list name
  - Valid values: `Allowed Sources`, `Quarantined Sources`, `Blocked Sources`, `Blocked Destinations`
- **exceptions_list** (string, optional): Exception list name (same valid values as list)
- **duration** (TimeInterval/ParamRef, required): How long to keep the element in the list
- **add_reason** (string, required): Reason for adding the element

API Request

This schema defines the parameter structure for the API Request step when creating or updating automations via API.

API Request Step Parameters Schema

```
{
  "url": string | ParamRef* (required),
  "method": "GET" | "POST" | "PUT" | "PATCH" | "DELETE" (required),
  "headers": object (optional),
  "body": object (optional),
  "authentication_id": string (optional)
}
```

- ParamRef is a reference to the Example Output of a previous step.

  Example: To reference the src field from a previous step with ID 0540c6d7-456c-411b-a87e-3576c304d80e, use:

  ```
  {{step[0540c6d7-456c-411b-a87e-3576c304d80e][src]}}
  ```

- `authentication_id` is the ID of a pre-defined authentication.

  For API details to retrieve authentications, see Appendix H - Webhooks and Authentications *(on page 304)*.

Step Schema Example

```
{
    "type": "API Request",
    "name": "My API Request",
    "parameters": {
        "url": "https://secure.myServerAPI/post",
        "method": "POST",
        "headers": {
            "x-Request-ID": 544
        },
        "body": {
            "Comment": "my post request"
        },
        "authentication_id": null,
    },
     "outputExample": {
          "my_post_request_output": {
              "name": " my_post_request_output",
              "output": {"success": true},
              "comment": ""
          }
      }
}
```

Create IOC Management Indicators

Creates multiple Indicators of Compromise (IOCs) in the threat intelligence system

Parameters Schema

```
{
  "indicators": IocIndicator[] | ParamRef (required),
  "expiration_in_days": number | ParamRef (required)
}
```

IoC Indicator Object

```
{
  "indicator_value": string | ParamRef (required),
  "indicator_type": string | ParamRef (required),
  "name": string | ParamRef (required),
  "description": string | ParamRef (optional),
  "confidence": "Low" | "Medium" | "High" (required),
  "severity": "Low" | "Medium" | "High" | "Critical" (required)
}
```

Parameters Detail

- **indicators** (array/ParamRef, required): Array of IOC indicator objects
- **expiration_in_days** (number/ParamRef, required): Days until indicators expire
- **indicator_type** valid values: `url`, `ip`, `domain`, `md5`, `sha256`, `sha1`, `ipv4`

Example

```
{
  "type": "Create IOC Management Indicators",
  "name": "Create threat indicators",
  "parameters": {
    "indicators": [
      {
        "indicator_value": "{{step['Log Trigger']['malicious_ip']}}",
        "indicator_type": "ip",
        "name": "Suspicious IP from logs",
        "description": "IP detected in security logs",
        "confidence": "High",
        "severity": "Medium"
      }
    ],
    "expiration_in_days": 30
  }
}
```

Run Automation

Executes predefined automation templates with custom parameters.

Parameters Schema

```
{
  "automation_name": string (required),
  "automation_params": object (required),
  "input": object (required),
  "event_details": EventDetails (optional)
}
```

Parameters Detail

- **automation_name** (string, required): Name of the automation to run
  - Valid values: `Block external IP`, `Quarantine internal IP`, `Open ticket and notify`, `Isolate Endpoint device`
- **automation_params**: Parameters specific to the chosen automation
- **input**: Input data specific to the chosen automation
- **event_details** (object, optional): Structured information to include with the automation execution. This allows you to pass additional context data that may be used by the target automation or included in its notifications.

Automation-Specific Schema

- Block external IP

```
{
  "automation_params": {
    "Block reason": string (required),
    "IP block duration": TimeInterval | ParamRef (required),
    "Notification message": string (required),
    "Notification message (not added)": string (required),
    "Notification profile (IP was blocked)": string (required),
    "Notification profile (IP was not blocked)": string (required),
    "Notification subject": string (required),
    "Notification subject (not added)": string (required)
  },
  "input": {
    "Block IP": string | ParamRef (required)
  }
}
```

- Quarantine internal IP

```
{
  "automation_params": {
    "Quarantine reason": string (required, max length: 300 characters),
    "IP quarantine duration": TimeInterval | ParamRef (required),
    "Notification message": string (required, max length: 600 characters),
    "Notification message (not added)": string (required, max length: 600 characters),
    "Notification profile (Device IP was quarantined)": string (required),
    "Notification profile (Device IP was not quarantined)": string (required),
    "Notification subject": string (required, max length: 300 characters),
    "Notification subject (not added)": string (required, max length: 300 characters),
    "Open ticket if device IP was quarantined": boolean | ParamRef (required)
  },
  "input": {
    "Quarantine IP": string | ParamRef (required)
  }
}
```

- Open ticket and notify

```
{
  "automation_params": {
    "Open ticket": boolean | ParamRef (required),
    "Notification profile": string (required),
    "ServiceNow ticket type": string (required),
    "Jira ticket type": string (required)
  },
  "input": {
    "Notification subject": string | ParamRef (required, max length: 300 characters),
    "Notification message": string | ParamRef (required, max length: 600 characters),
    "Ticket subject": string | ParamRef (required, max length: 300 characters),
    "Ticket description": string | ParamRef (required, max length: 600 characters)
  }
}
```

- Isolate Endpoint device

```
{
  "automation_params": {
    "Device isolation duration": TimeInterval | ParamRef (required),
    "Notification subject": string | ParamRef (required, max length: 300 characters),
    "Notification message": string (required, max length: 600 characters),
    "Open ticket if device was isolated": boolean | ParamRef (required),
    "Notification profile": string (required)
  },
  "input": {
    "type": "Endpoint Security" (required),
    "deviceName": string | ParamRef (required),
    "deviceIp": string | ParamRef (required),
    "machineId": string | ParamRef (required),
    "comment": string (required)
  }
}
```

Example

```
{
  "type": "Run Automation",
  "name": "Block external threat",
  "parameters": {
    "automation_name": "Block external IP",
    "automation_params": {
      "Block reason": "Automated blocking from threat detection",
      "IP block duration": {
        "value": 24,
        "unit": "hours"
      },
      "Notification message": "IP has been blocked due to suspicious activity",
      "Notification message (not added)": "IP could not be blocked",
      "Notification profile (IP was blocked)": "Immediate attention",
      "Notification profile (IP was not blocked)": "Immediate attention",
      "Notification subject": "External IP Blocked",
      "Notification subject (not added)": "External IP Block Failed"
    },
    "input": {
      "Block IP": "{{step['Log Trigger']['external_ip']}}"
```

```
21     }
22   }
23 }
```

13.7.8. Common Data Types

This topic describes common structured data types used for duration values and event detail definitions. It includes specifications for TimeInterval and EventDetails formats.

TimeInterval

Represents a duration with a numeric value and time unit.

```
1  {
2          "value": number (required),
3          "unit": "seconds" | "minutes" | "hours" | "days" (required)
4          }
```

EventDetails

Structured data for displaying information in notifications and tickets.

```
1  {
2          "enabled": boolean (required),
3          "event_details_fields": [
4          {
5          "name": string (required),
6          "value": string | number | ParamRef (required)
7          }
8          ] (required)
9          }
```

13.7.9. Parameter Behavior and Validation Notes

Describes rules for parameter behavior, validation requirements, optional fields, string length limits, and trigger output expectations in automation flows.

Parameter References

When referencing outputs from previous steps, the referenced step must come earlier in the automation flow.

Validation

- All parameter values are validated against their defined schema.
- Invalid input cause automation creation to fail.

Optional Parameters

- Parameters marked as optional can be omitted without error.
- Defaults may apply depending on the schema.

String Length Limits

Text fields may have maximum character limits, which vary by field type (for example, input field, name, ID).

Trigger Output Requirements

- Trigger steps (for example, Log Trigger, Schedule Trigger) must include an `output_example` field.
- This defines the data structure they provide to downstream steps.

13.8. Appendix H - Webhooks and Authentications

This topic introduces REST APIs related to webhooks and authentications used in Playblocks automations.

This topic provides REST APIs related to webhooks and authentications used in Playblocks automations.

Create Webhooks via API

This section describes how to create webhooks by using the API. It provides the method, URL, and request body structure with an example.

- Method: `POST`
- URL: https://cloudinfra-gw.portal.checkpoint.com/app/playblocks/api/v3/configuration/webhooks
- Request Body Schema:

```
{
            "name": string (required),
            "authenticationId": UUID (optional),
            "automationId": UUID (required),
            "expiration": Date (optional),
            "fieldsMapping": Object (optional)
            }
```

- Request Body Example:

```
{
            "name": "My webhook",
            "authenticationId": null,
            "automationId": "8fcec37b-0aa4-41f8-9a10-bed73f5a1360",
            "expiration": "2027-11-03T14:19:19.079Z",
            "fieldsMapping": {"src":"data.src"}
            }
```

View Required Fields for Trigger Output

To view the required fields in the automation trigger output (set mappings if required), use:

- Method: `GET`
- URL: /expectedTriggerOutput/{automationId}" scope="external">https://cloudinfra-gw.portal.checkpoint.com/app/playblocks/api/v3/configuration/automations/automation/expectedTriggerOutput/{automationId}

Response includes:

- `output`: Defines the expected trigger output structure.
- `fieldsInUse`: Lists the fields from the trigger output that are used in subsequent steps.

```
{
        "output": {
        "src": "1.2.3.4",
        "event_details": {"severity": "high"}
        },
        "fieldsInUse": ["src", "event_details.severity"]
        }
```

Retrieve your authentications via API

To retrieve your authentications, use these API:

- Method: `GET`
- URL: ations/automation/expectedTriggerOutput/{automationId}" scope="external">https://cloudinfra-gw.portal.checkpoint.com/app/playblocks/api/v3/configuration/automations/automation/expectedTriggerOutput/{automationId}
- Response structure:

```
{
            "success": true,
            "data": {
            "authentications": [
            {
            "id": "9824a0ee-eabe-48d6-aa14-43d4a1111111",
            "name": "My Authentication",
            "method": "Bearer Token",
            "type": "API Request",
            "parameters": {
            "token": <MY BEARER TOKEN>
            },
            "createdBy": "Playblocks System",
            "comment": "Create tickets permissions",
            "createdAt": "2025-08-27T14:29:32.975Z",
            "updatedAt": "2025-08-27T14:29:32.975Z"
            }
            ]
            }
            }
```

13.9. Appendix I - Creating a PagerDuty General Access Key

This appendix describes the one-time setup in PagerDuty that the PagerDuty Alerting connector requires.

About this task:

Playblocks uses two PagerDuty assets:

- **A General Access Key** - An account-wide REST API key that you generate under PagerDuty's **Integrations** > **API Access Keys**. The key authorizes Playblocks to read services and write to incidents on behalf of the entire PagerDuty account.
- **A PagerDuty user email address** - Appears as the "From" address on incidents that Playblocks creates and modifies. This is for audit attribution only. PagerDuty does not authenticate against this address.

Step 1 - Generate a General Access Key

To generate a General Access Key:

Procedure:

1. Sign in to PagerDuty as an account administrator.
2. Go to **Integrations** > **API Access Keys**.
3. Click **Create New API Key**.
4. Enter these details:
    - **Description** - For example, Playblocks. This helps you identify the key if you need to rotate or revoke it.
    - Make sure **Read-only access** is not selected.

    > **Note:**
    >
    > Playblocks needs write access to create and update incidents.

5. Click **Create Key**.
6. Copy the key immediately.

    > **Important:**
    >
    > The key appears only once. Store it securely because you cannot retrieve it later.

What to do next:

Step 2 - Identify the email to use as the "From" address

PagerDuty's REST API requires a "From" header that contains the email address of a real, valid user in the PagerDuty account whenever an incident is created or modified. The General Access Key authenticates the request. The "From" email tells PagerDuty which user to record in the incident's history.

Select the email of an existing PagerDuty user. For example, the on-call admin, a SOC manager, or a dedicated "Playblocks Automation" service user that you create.

> **Note:**
>
> The email must belong to a real PagerDuty user. PagerDuty rejects requests with an unknown email.

Step 3 - Identify the correct service URL

PagerDuty operates two regional REST endpoints:

- **United States (default):** `https://api.pagerduty.com`
- **European Union:** `https://api.eu.pagerduty.com`

If you are not sure which region hosts your PagerDuty account, sign in to PagerDuty and check the URL in your browser's address bar:

- EU tenants sign in through `*.eu.pagerduty.com`.
- US tenants sign in through `*.pagerduty.com`.

You now have:

- A PagerDuty General Access Key.
- A PagerDuty user email to use as the "From" address.
- The correct regional service URL.

Return to PagerDuty Alerting and continue with the **Configure the PagerDuty connector** procedure.

Index