Workspace Security

26 March 2026

CHECK POINT XDR

Administration Guide

CHECK POINT™

Check Point Copyright Notice

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.

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.
Please help us by sending your comments.

Revision History

Date	Description
25 March 2026	Updated product name and product grouping to align with the new Check Point strategic pillars and portal navigation. No functional changes were made. Infinity XDR/XPR is now referred to as **Check Point XDR**.
22 January 2026	Added deprecation information in *"Microsoft Entra ID" on page 327*.
15 December 2025	Updated screenshots in *"Sending Microsoft Teams Notifications" on page 362*.
28 August 2025	Added options to display related assets and indicators in *"Notifications" on page 358*.
16 July 2025	Updated *"Introduction to Check Point XDR" on page 21*.
14 July 2025	Updated *"Licensing the Product" on page 42*.
11 July 2025	Updated **Threat Hunting** page as per the latest UI changes. See *"Threat Hunting" on page 165*.
01 July 2025	Added **Users - Organizational Units Tree Details**. See *"Users" on page 139*.
30 June 2025	Added **Intelligence Widget Card** information in Incidents page. See Intelligence Widget Card.
19 May 2025	Added *"Network Inventory" on page 346* in **Settings**.
5 May 2025	Updated **Reports**. Added: ■ *"XDR/XPR Predefined Activity Report" on page 354* ■ *"Weekly XDR/XPR Summary Email Settings" on page 357*
22 April 2025	Added **Groups** tab for **Assets**. See: ■ *"Devices - Group Details" on page 162* ■ *"Users - Group Details" on page 148*
21 April 2025	Renamed **Insights** page to **Alerts**. See *"Alerts" on page 121*.
25 March 2025	Updated *"Incidents - Affected Assets" on page 94*: Added details about tabs for each asset type.

Date	Description
12 March 2025	Updated *"XDR/XPR API - Operations related to incidents, alerts, actions and exceptions." on page 38*: Added prerequisite to create a new account API key for XDR in the Infinity Portal.
10 March 2025	Updated *"Notifications" on page 358*: ■ Added a checkbox to send notifications only for incidents that were not prevented. ■ Added **Content** section to include tenant name in email notifications.
29 January 2025	■ Added **Prevention** widget in the **Overview** page. See *"Overview" on page 50*. ■ Updated the **Incident** widget to show the number of indicators and artifacts as separate sections. See *"Incidents" on page 57*.
8 January 2025	Updated the description for **Add filter** option in **Incidents** page. See *"Incidents" on page 57*.
7 January 2025	■ Added *"Prevention Center" on page 127*. ■ Added **Asset incident priority** and **Top 5 assets by priority** widgets in the **Overview** page. See *"Overview" on page 50*. ■ Added information about **[Related Incidents]: Assignee** and **[Related Incidents]: Priority** filters in Assets. See *"Adding Filters" on page 156*.
19 December 2024	Added **Assets** tab. See: ■ *"Assets" on page 137* • *"Users" on page 139* • *"Devices" on page 152*
17 December 2024	Updated *"Intelligence" on page 210*: ■ Renamed **Sample attackers** tab to **Example reports**. ■ When analyzing a file, added the option to upload a password protected file. See *"Analyzing a File" on page 216*.
9 December 2024	Updated *"Log Processing" on page 333*: ■ Added **Daily Entitlement** value to the **Weekly log processing** widget. ■ Added a dotted line to show the entitlement in the **Processing by product** section.
25 November 2024	Added *"Processing Exception List" on page 337* in Log Processing.

Date	Description
11 November 2024	■ Added response integration configuration in *"Singularity Endpoint" on page 271*. ■ Added **Reset Password** prevention action for all identity providers integrated through Infinity Next. See **Supported Preventive Actions** section in *"Microsoft Entra ID" on page 327* and *"Okta" on page 328*.
05 November 2024	Added **Insights** page where you can view insights from all the incidents. See *"Alerts" on page 121*.
28 October 2024	Added: ■ Support for Mobile Security. See *"On-boarding Products" on page 45* and *"Incidents - Affected Assets" on page 94*. ■ Views in Threat Topology map. See *"Threat Topology Map" on page 172*.
04 October 2024	Added UAE to *"Supported Regions" on page 38*.
24 September 2024	■ Added video tutorial on how to manage an incident. See *"How to Address an Incident" on page 48*. ■ Updated the procedure to send Microsoft Teams notifications for an incident. See *"Sending Microsoft Teams Notifications" on page 362*.
10 September 2024	Added *"Log Processing" on page 333*.
28 August 2024	Added XDR integration with: ■ *"Microsoft Entra ID" on page 327* ■ *"Okta" on page 328*
02 August 2024	■ Added a table to show the type of integration for each supported product. See *"The table below shows the supported products, their log integration types, and whether they support response integration and IoC Management." on page 28*. ■ Added SK reference for the supported file types in Intelligence > *"Analyzing a File" on page 216*.
24 July 2024	Updated configuration information in *"Cisco Firepower Threat Defense" on page 311*

Date	Description
22 July 2024	Added: ■ *"AI Copilot" on page 372* ■ EPP response for CrowdStrike Falcon and Trend Vision One for Endpoint. See *Incidents - Overview* > *"Prevention" on page 70*.
18 July 2024	Added: ■ *"Threat Topology Map" on page 172* ■ *"Incidents - Attack Map" on page 85*
27 May 2024	■ Added XDR integration with SentinelOne. See *"Singularity Endpoint" on page 271*. ■ Added support for SentinelOne event logs. See *"Events" on page 201*.
24 May 2024	■ Added XDR integration with Palo Alto Networks Next Generation Firewall. See *"Palo Alto Networks Next Generation Firewall" on page 282*. ■ Added support for Microsoft 365 Defender for Endpoint and Palo Alto Networks Next Generation Firewall event logs. See *"Events" on page 201*. ■ Added export of Threat Hunting data to CSV file. See *"Threat Hunting" on page 165*.
22 May 2024	Added India to *"Supported Regions" on page 38*.
13 May 2024	Updated for the new left navigation pane.
30 April 2024	■ Added reference to sk182156 to on-board multi-domain servers for a single tenant in *"On-boarding Products" on page 45*. ■ Removed the appendix for on-boarding a Multi-Domain Security Management Server.
18 April 2024	Added: ■ *"Advanced Exclusions" on page 238*. ■ Description field for Shared Bookmarks in Threat Hunting. See *"Saving a Query as a Bookmark" on page 171*. ■ Support for logs from CrowdStrike Falcon, Trend Vision One for Endpoint and Cisco Firepower Threat Defense. See *"Events" on page 201*.
03 April 2024	Added support for Fortinet FortiGate Next Generation Firewall logs. See *"Events" on page 201*.

Date	Description
26 March 2024	Added these integrations: ■ *"CrowdStrike Falcon" on page 263* ■ *"Trend Vision One for Endpoint" on page 305* ■ *"Cisco Firepower Threat Defense" on page 311*
20 March 2024	Added *"Incident Timeline" on page 111*.
15 March 2024	Updated the procedure to attach a contract to the product in *"Accessing the XDR Administrator Portal" on page 39*.
08 February 2024	Updated *"API Support" on page 38* for Horizon to Infinity rebranding.
07 February 2024	Added **Fortinet FortiGate Next Generation Firewall** to the list of supported products in *"On-boarding Products" on page 45*.
02 February 2024	Updated **Getting Started** page. See *"Accessing the XDR Administrator Portal" on page 39*.
31 January 2024	Rebranded Horizon XDR/XPR to XDR.
18 January 2024	■ Added information about the *"Prevention" on page 70* widget in the Incidents Overview page. ■ Added Microsoft Entra ID (formerly Azure AD) to the list of supported products for Identity Service. See: • *"The table below shows the supported products, their log integration types, and whether they support response integration and IoC Management." on page 28*. • *"On-boarding Products" on page 45*.
04 January 2024	Added *"Fortinet FortiGate Next Generation Firewall" on page 249*.
27 December 2023	Added information about the new sample mode. See *"Accessing the XDR Administrator Portal" on page 39*.
13 December 2023	Added: ■ Trail request form. See *"Accessing the XDR Administrator Portal" on page 39*. ■ Identity Service. See *"The table below shows the supported products, their log integration types, and whether they support response integration and IoC Management." on page 28*.

Date	Description
06 December 2023	Updated *"Prevention" on page 70*.
06 December 2023	■ Added information about support for Microsoft Active Directory and Cloud Firewall. See *"The table below shows the supported products, their log integration types, and whether they support response integration and IoC Management." on page 28*. ■ Added *"Personalized News" on page 56*. ■ Added *"Incident Description" on page 67*.
22 November 2023	Added *"XDR/XPR Reports" on page 350*.
20 November 2023	Added information about the supported regions for XDR and Threat Hunting. See *"Supported Regions" on page 38* and *"Threat Hunting" on page 165*.
10 November 2023	Added information about how to migrate from the legacy IoC Management to the New IoC Management. See *"Migrating to the New IoC Management" on page 229*.
02 November 2023	■ Added the procedure to create exclusion for artifacts in: • *"Creating an Exclusion for Artifacts and Indicators from an Incident" on page 105*. • *"Exclusions" on page 236*. ■ Added information about the incidents prevented automatically by XDR. See *"Overview" on page 50*.
28 August 2023	Added information about how to integrate Microsoft 365 Defender for Endpoint with XDR. See *"Microsoft 365 Defender for Endpoint" on page 245*.
24 August 2023	Added information about *"Saving a Query as a Bookmark" on page 171* and *"Custom Rules" on page 233*.
11 July 2023	■ Added information about *"Audit Logs" on page 369*. ■ Updated information about the Connectivity widget on the *"Overview" on page 50*page.
01 June 2023	Added information about *"API Support" on page 38*.
15 March 2023	Updated *"Getting Started" on page 39*.
06 March 2023	Added the Take number for on-boarding Quantum Security Gateway on-premises R81.10.

Date	Description
24 February 2023	First release of this document.

Table of Contents

Introduction to Check Point XDR *21*

Definitions and Concepts *22*

Understanding Events, Alerts, and Incidents *22*

Components of an Incident *22*

Alert Processing *23*

Grouping *23*

Enrichment *23*

Validation *23*

Correlation *24*

Alert Action Status *24*

Incident Prevented Status *24*

Collaborative Enforcement *25*

IoCs *25*

IoC Management *25*

XDR Feed *25*

Policy Automation *26*

Product Integrations *26*

Check Point Products *26*

Identity Sources *27*

Third-Party Integrations *27*

Log Integration *27*

Response Integration *27*

IOC *28*

Key Application Components *29*

Integrations *29*

Incident Management *30*

Incident List *30*

Asset Incident Priority ... 30
Alert Table ... 31
Prevention Center ... 31
Assets ... 31
Threat Hunting ... 32
Events ... 32
Notifications ... 33
XDR Detections ... 33
The Power of AI in XDR ... 33
XDR Unique Detection Method ... 34
Detection Catalog ... 34
Licensing ... 36
Data Processing Entitlement ... 37
Connected Product Entitlement ... 37
License Expiration ... 37
Data Retention ... 38
Supported Regions ... 38
API Support ... 38
Getting Started ... **39**
Creating an Account in the Check Point Portal ... 39
Accessing the XDR Administrator Portal ... 39
Licensing the Product ... 42
Licensing Options ... 42
Data Retention ... 42
Getting Started with Licensing ... 43
Start a Free Trial ... 43
Activating a License ... 43
License Expiration Policy ... 44
On-boarding Products ... 45
Adding Users ... 47

How to Address an Incident ... *48*
Overview ... *50*
Connectivity ... *51*
Prevention ... *52*
Asset Incident Priority ... *53*
Top 5 Assets by Priority ... *54*
Incidents ... *55*
Incidents Over Time ... *55*
Personalized News ... *56*
Open Incidents by Assignee ... *56*
Incidents ... *57*
Incidents ... *57*
Top Banner ... *64*
Incidents - Overview ... *64*
Incident Summary ... *66*
Incident Description ... *67*
MITRE ... *68*
Assets and Indicators ... *68*
Managing Assets and Indicators ... *69*
Prevention ... *70*
Prevention ... *70*
Rejected & Expired ... *73*
Audit Log ... *74*
Insights Timeline ... *75*
Comments ... *76*
Adding a Comment ... *76*
Creating Advanced Exclusions from an Incident ... *76*
Attack graphs ... *85*
Incidents - Attack Map ... *85*
Reading an Attack Map ... *85*

Filtering an Attack Map ... 89
Incidents - Forensics Trees ... 93
Incidents - Affected Assets ... 94
Devices ... 94
Managing Affected Devices ... 96
Creating an Exclusion for Devices from an Incident ... 97
Users ... 97
Managing Affected Users ... 99
Mobile ... 99
Adding Filters ... 100
Incidents - Indicators & Artifacts ... 101
Managing Indicators and Artifacts ... 104
Creating an Exclusion for Artifacts and Indicators from an Incident ... 105
Adding or Editing an Indicator or Artifact in IoC Management ... 107
Removing an Indicator from IoC Management ... 109
Incidents - MITRE ... 110
Incident Timeline ... 111
Incidents - Insights & Forensics ... 113
Creating an Advanced Exclusion from an Insight ... 113
Incidents Executions ... 118
Alerts ... 121
Alerts Table ... 122
Statistics ... 124
Adding a New Filter ... 125
Prevention Center ... **127**
Prevention Status ... 128
Pending User Actions ... 128
Statistics ... 129
Details Table ... 130
Status ... 130

Prevention Actions Taken ... 131
Attacks Prevented by XDR/XPR ... 132
Executions ... 134
Assets ... **137**
Users ... 139
Users by Priority ... 139
Users by Related Devices Number ... 140
Users Table ... 141
Filtering the Users Page ... 142
Adding Filters ... 142
Filter In and Filter Out in Users Table ... 143
User Threat Hunting Details ... 144
User - Related Devices, Incidents, Identity Provider (IdP) Groups and Organizational Unit ... 144
User Details ... 145
Users - Device Details ... 146
Users - Incident Details ... 147
Users - Group Details ... 148
Users - Organizational Units Tree Details ... 150
Devices ... 152
Devices by Priority ... 152
Devices by Type ... 153
Devices Table ... 154
Filtering the Devices Page ... 155
Adding Filters ... 156
Filter In and Filter Out in Devices Table ... 157
Device Threat Hunting Details ... 158
Device - Related Users, Incidents and IdP Groups ... 158
Device Details ... 158
Devices - User Details ... 160

Devices - Incident Details ... 160
Devices - Group Details ... 162
Investigate ... **164**
Threat Hunting ... 165
Supported Regions ... 166
Supported Versions ... 166
Enabling Threat Hunting ... 166
Using Threat Hunting ... 167
Saving a Query as a Bookmark ... 171
Use Case - Maze Ransomware Threat Hunting ... 172
Threat Topology Map ... 172
Topology Map - Overview ... 174
Managing Views ... 176
Adding a New View ... 178
Editing a View ... 180
Cloning a View ... 181
Deleting a View ... 182
Internal IP Settings ... 183
Excluded Views ... 185
Reading the Threat Topology Map ... 188
Searching the Threat Topology Map ... 196
Filtering the Threat Topology Map ... 198
Events ... **201**
Supported Products ... 201
Statistics ... 203
Events Table ... 204
Managing the Events Table ... 205
Viewing Events for a Time Period ... 207
Searching for Events ... 207
Exporting Events ... 207

Card ... 209
Intelligence ... **210**
Viewing Intelligence for Indicators ... 210
Intelligence Dashboard ... 212
Indicator Information ... 212
Research ... 213
Check Point Traffic Analysis ... 215
Open Source Intelligence Tools ... 215
Exporting the Search Summary to a CSV ... 215
Copying and Removing an Indicator from the Search Summary ... 216
Analyzing a File ... 216
Investigating a File ... 218
IOC Management ... **219**
New IoC Management ... 219
Legacy IoC Management ... 219
IoC Management Overview ... 219
Working with IoC Management ... 219
Creating a New IoC ... 221
Adding IoCs by Uploading a CSV File ... 222
Editing and Deleting an IoC ... 223
Filtering IoCs ... 224
Exporting IoCs ... 224
Configuring IoC Management ... 224
Testing IoC Management ... 228
Migrating to the New IoC Management ... 229
Prerequisite ... 229
Changes to IoCs During Migration ... 229
Procedure ... 229
Policy ... **231**
Automations ... 232

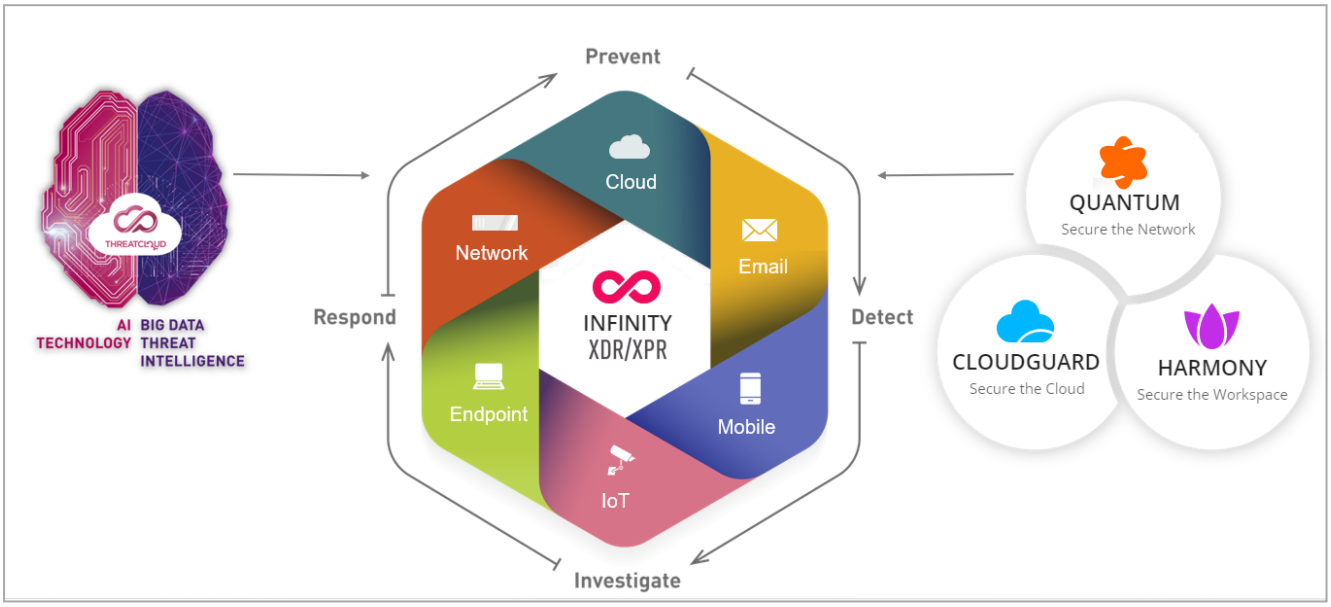
Custom Rules ... 233
Managing Custom Rules ... 234
Running a Custom Rule ... 235
Exclusions ... 236
Simple Exclusions ... 236
Advanced Exclusions ... 238
Reverting a Retroactive Exclusion ... 241
Editing an Exclusion ... 242
Exporting Exclusions ... 242
Settings ... ***243***
Integrations ... 244
Microsoft 365 Defender for Endpoint ... 245
Prerequisites ... 245
Integrating Microsoft 365 Defender for Endpoint ... 245
IOC Management ... 248
Deleting the Integration ... 248
Fortinet FortiGate Next Generation Firewall ... 249
Integrating FortiGate Next Generation Firewall ... 249
Disabling the Integration ... 256
Regenerating the Certificate ... 257
Deleting the Integration ... 258
Configuring IoCs ... 258
CrowdStrike Falcon ... 263
Integrating CrowdStrike Falcon ... 264
IOC Management ... 270
Deleting the Integration ... 270
Supported Preventive Actions ... 270
Singularity Endpoint ... 271
Integrating Singularity Endpoint ... 271
Regenerating the Certificate ... 278

Deleting the Integration ... 279
Supported Preventive Actions ... 280
Palo Alto Networks Next Generation Firewall ... 282
Integrating Palo Alto Networks Next Generation Firewall ... 282
Regenerating the Certificate ... 295
Configuring IoCs ... 297
Deleting the Integration ... 304
Trend Vision One for Endpoint ... 305
Integrating Trend Vision One for Endpoint ... 305
IOC Management ... 309
Deleting the Integration ... 309
Supported Preventive Actions ... 310
Cisco Firepower Threat Defense ... 311
Integrating Cisco Firepower ... 311
Regenerating the Certificate ... 320
Configuring IoCs ... 322
Deleting the Integration ... 325
Microsoft Entra ID ... 327
Okta ... 328
Integrating Okta ... 328
Deleting the Integration ... 330
Supported Preventive Actions ... 331
Log Processing ... 333
Weekly Log Processing ... 334
Top Weekly Usage by Products ... 334
Top Weekly Usage by Quantum Devices ... 334
Average Log Processing ... 335
Processing by Product ... 335
Assess Exceptions ... 336
Processing Exception List ... 337

Adding a Processing Exception ... 338
Managing the Processing Exception List ... 345
Network Inventory ... 346
Private Networks ... 346
Adding a new Private Network ... 346
Managing Private Networks ... 349
Reports ... 350
XDR/XPR Reports ... 350
XDR/XPR Configurable Activity Report ... 350
Generating an Activity Report ... 350
Scheduling an Activity Report ... 352
XDR/XPR Predefined Activity Report ... 354
Weekly XDR/XPR Summary Email Settings ... 357
Prerequisite ... 357
Notifications ... 358
Sending Email Notifications ... 361
Sending Slack Notifications ... 361
Sending Microsoft Teams Notifications ... 362
Testing Notifications ... 368
Audit Logs ... 369
Topology Map Excluded Views ... 371
AI Copilot ... 372
General Actions ... 372
Providing Feedback on the Response ... 374
Supported Capabilities for XDR ... 375
General Query ... 375
Sample Prompts ... 375
Incident Specific Query and Action ... 376
Sample Prompt for Queries on an Incident ... 376

Introduction to Check Point XDR

Check Point **XDR** (formerly Infinity XDR/XPR) is an Extended Detection Response (XDR) and Extended Prevention Response (XPR) tool that provides a unified view of all the security operations across onboarded products and helps you detect, respond to and prevent cyber attacks.



XDR provides a consolidated security view across all connected products. It provides a focused and prioritized set of incidents that require operator attention. The application provides recommendations for the actions to be taken to address the incident and options to automate enforcement across the monitored deployment.

The primary benefits of XDR are:

- **Operator efficiency** - Reduces operator workload by processing large numbers of events and alerts to create a small number of prioritized events for operator attention.
- **Unique Detections** - XDR has a view across the network and for extended periods of time. This allows it to leverage Artificial Intelligence (AI), Machine Learning (ML) and correlation to generate detections beyond those that are generated by each of the connected products. This includes the following detection types:
  - **Correlation** - Connection of multiple events across connected products to identify a security incident. As additional logs are connected or correlated together, events with lower severity may be seen within context of a higher priority incident.
  - **User Entity Behavioral Analytics (UEBA)** - Uses ML to build models of the usual activities on the deployment. These can be leveraged to detect and flag any activities that do not match this expected model.

- **Collaborative Enforcement** - Coordinates and automates response actions across all connected products. Feeds containing Indicators of Compromise (IoCs) are leveraged for this enforcement.

Definitions and Concepts

Understanding Events, Alerts, and Incidents

In the context of XDR, the terms events, alerts, and incidents represent three key types of messages that indicate different levels of activity and potential risk. Understanding the distinction between these categories is important to understanding the XDR functionality.

- **Events**

  Event are records of normal or noteworthy activity that occur within a system, network, or application. They are often automatically generated by devices or software. Examples of such events include login events, file access and network connections. While most events are benign, they provide the foundational data used to detect issues or anomalies. For example, while all users must login to gain access, a login performed from an unusual location or time may be considered potentially anomalous. Events are also referred to as **Logs**.

- **Alerts**

  Alerts are notifications generated when specific conditions or thresholds are met, typically defined by detection rules or AI-based analysis. An alert signifies something that may require attention, such as unusual network traffic, failed login attempts, or a critical system error. Not all alerts indicate a real problem, but they warrant investigation.

- **Incidents**
  Incidents are confirmed or suspected breaches, disruptions, or threats that negatively affect operations or security. An incident often originates from one or more alerts but involves a validated issue that needs containment, resolution, and possibly reporting. Some examples of incidents are data exfiltration attempts and brute force login attempts.

Incidents are the primary set of items to be handled by the administrator. Each incident can be managed from the XDR management interface during its lifecycle. This allows an incident to be assigned to a specific administrator, have comments added to provide additional data as investigation progress until finally get assigned one of the multiple closure statuses to reflect the final incident resolution.

Note - Within the scope of incidents, alerts are currently displayed as Insights. However the terms Alerts and Insights can be considered synonymously and will eventually be consolidated and displayed as Alerts.

Components of an Incident

The three primary components of an incident are:

- **Assets** - Valuable resources within an organization that need protection and may be targeted or impacted during a security incident. In the context of XDR, monitored assets are users and devices.
- **Artifacts** - Pieces of evidence of the entities associated with an event or alert that provide additional context. Examples of artifacts are files, processes, IP addresses and URLs.
- **Indicator** - A type of artifact that has been identified as a meaningful sign of potential malicious activity. While all indicators are artifacts, not all artifacts qualify as indicators, only those that are known or suspected to signal a security threat or compromise.

Administrator can reclassify items between the indicator and artifact categories.

Alert Processing

There are multiple steps performed during the processing of an alert:

- Grouping
- Enrichment
- Validation
- Correlation

These are described in the following sections.

Grouping

Alerts for which all the key data elements are the same, except for the time of the alert, are **grouped** together. It is possible to display such alerts as **grouped alerts**, that are displayed as a single record together with the time of the first alert in the group, in addition to the time of the most recent alert.

Enrichment

Enrichment is the process of adding contextual information and threat intelligence to security alerts to provide deeper insights about potential threats, such as adding geolocation data, common usage, reputation scores, or historical patterns.

Validation

There are multiple sources for alerts:

- Alerts generated by the connected products. These are sometimes referred to as **parity alerts**.
- Alerts generated by AI/ML algorithms and Advanced User Entity Behavioral Analytics (UEBA) detections.

In both cases, the alert goes through validation, which is the process of calculating a single score for the alert and its indicators, including the result of the different enrichment options. The validation workflow is used to confirm whether an alert represents a true security incident, a false positive, or something between that should continue to be monitored. It ensures the alert is legitimate, actionable, and prioritized correctly.

As a result of the validation process, each alert is assigned a verdict, along with a short textual justification. This verdict may determine whether the alert requires attention and will be included as part of an incident, or will continue to be monitored as additional events are received and correlated.

Correlation

Correlation refers to the process of connecting and analyzing alerts from multiple sources to identify threats that may not be evident from a single data point alone. Assets, Artifacts and Indicators are extracted when XDR process the Events and Alerts. These are the critical components that are leveraged in correlation across events from all the connected products by identifying the common components associated across the events and alerts. For example, cases where the same user or IP address is seen across multiple events. Correlated data is processed and, when sufficient correlating factors are identified, multiple events can be stitched together. These events are correlated into a single incident or attack, and may originate from the same product or across multiple products.

Alert Action Status

For every alert, it is determined whether the associated threat was only detected or fully blocked. This is reflected in the **Action** field associated with each alert as follows:

- **Detected** - The threat was detected.
- **Blocked** - Any impact from the threat was blocked.

Incident Prevented Status

The status of the incident is calculated from all the automatic actions done by XDR or the different products reporting to it, along with remaining actions that need to be done by the user or authorized by them.

This is reflected in the **Prevented Status** for each incident as follows:

- **Detected** - The threat was detected but was not fully prevented. Detected alerts are displayed in the user interface as having **Action Required** and are prioritized for operator attention.
- **Prevented** - The threat was blocked and addressed the identified source of the threat to prevent further alerts from the same source.

Collaborative Enforcement

A key capability of XDR is the ability for enforcement across all connected integrations. There are two key aspects of this capability:

- IoCs - Indicators of Compromise, together with related management and data.
- Policy Automation

IoCs

Indicators of Compromise (IoCs) are discrete data points such as an IP address, domain, URL, file hash, or malware signature, that is shared in real time or near real time to help organizations identify, detect, and defend against known threats.

Security vendors or communities often curate these IoCs to automatically update systems for proactive threat detection and response.

IoCs are the key component of the collaborative responses that can be performed across the managed network. Events that match on the IoC can be blocked across all connected products.

IoC Management

Customers who have access to XDR also have access to the **IoC Management** capabilities after they select the **IoC Management** option in the XDR menu.

The **IoC Management** is a centralized platform to manage Indicators of Compromise (IoCs) across products. It collects IoCs from various sources through feeds or inputs (manual or live) and also provides output feeds that can be consumed by security products.

You can define one or more IoC feeds. When there are multiple feeds defined, the administrator must assign priority between the various feeds. This allows for resolution of any conflicts in cases where the same IoC is included in multiple feeds. The feeds are evaluated in priority order, and the setting from the first feed containing the IoC is taken.

To enforce the IoCs on third-party systems, create the **Output (Blends)** within IoC Management, select the feeds to be included in the output and then copy the URL for this feed. This URL should then be integrated with every third-party product connected to XDR.

XDR Feed

In addition to any external inputs/feeds that are defined, there is an additional input/feed called **XDR Feed**, created automatically by default. This feed contains IoCs created from within XDR. These IoCs may be created either upon user request from the XDR user interface or automatically based on policy automation settings.

Policy Automation

In the **Automations** page, you can configure XDR to take prevention actions automatically when an incident is generated with a specified confidence and severity. Currently, the automatic response supports adding indicators to IoC Management.

The policy can be set to create the IoCs in **Disabled** state, to be subsequently manually reviewed and enabled. Alternatively, you can configure the IoCs to be enabled immediately upon creation.

Product Integrations

XDR gets a wider view and inputs across the monitored network through the supported product integrations. There are three types of supported product integrations:

- Check Point products
- Identity sources
- Third-party products

For each of these supported integration types, three integration aspects should be considered:

- Log integration
- Response integration
- IoCs integration

Response integration allows to perform the commands/responses on the integrated device using APIs.

Check Point Products

All supported Check Point products can be fully integrated, without additional configuration, in the following use cases:

- **Endpoint Security** - Uses the Endpoint Security cloud management (EPMaaS).

  When working with Endpoint Security, there are two data sources that will be seen in the application:

  - Endpoint Security - Endpoint Client
  - Endpoint Security Management - Endpoint Management

  This ensures there is full coverage for all events from Endpoint Security. There may be some duplicated events reported from both sources that will be correlated and, where applicable, included in the same incident.

- **Quantum Security Gateway/Cloud Firewall** - For Quantum Security Gateway, the **Sharing SmartConsole Configuration and Logs with Check Point Portal** option must be enabled to allow access by XDR.

  There are two data sources that may be seen for Quantum related events:

  - Quantum Gateway
  - Quantum Gateway Telemetry
- **Email Security** - All deployments.
- **Mobile Security** - All deployments. However, if you need to enable IoC support for a tenant, contact Mobile Security product team.

Identity Sources

Identity Sources provide enrichment of alerts providing asset related information. For example, in addition to IP information included, these will also be mapped to include the names of devices.

When working with Endpoint Security, you can define the Identity Connector on Endpoint Security to enrich the Endpoint logs sent for processing to XDR, with relevant identity information.

For Quantum Gateway, configure either Active Directory or Okta as an Identity Provider on the **Identity & Access** page in Check Point Portal. This allows enrichment of the logs from Quantum gateway and AI/ML analysis, detection of unusual user login activity and the creation of corresponding incidents.

Third-Party Integrations

Log Integration

Log integration for each third-party product is supported through one of the following integration methods:

- **Syslog** - Logs are pushed to XDR.
- **API** - Logs are pulled over the API interface.

In both cases, following successful integration, the logs from the product are stored in Check Point's cloud infrastructure and are visible as events.

To enable such integrations, you must do the necessary configurations to enable access to relevant data sources. This is typically done using a certificate (commonly used for syslog integrations) or authentication keys and similar settings (commonly used for API).

Response Integration

To enable XDR to issue responses for a specific third-party integration, you must configure an access token or similar credential that allows access to the relevant API.

If log integration is performed over API, additional configuration for response integration may not be necessary. However, if Syslog is used for event integration and API is used for integrating responses, each requires separate configuration.

IOC

To configure the IoC feed to take effect on the third-party device, the administrator must set up an output integration in the IoC Management. This setup defines the location and format of the URL to be configured for processing on the third-party management. Sometimes, multiple URLs may be required for integration if different types of indicators use different feeds.

The table below shows the supported products, their log integration types, and whether they support response integration and IoC Management.

Product Family	Product Name	Log Integration	Response Integration	IOC Management Support
Check Point	Quantum Security Gateway ■ R81.10 with the R81.10 Jumbo Hotfix Accumulator Take 93 and higher. ■ Smart-1 Cloud	Check Point cloud	Supported	Supported
	Cloud Firewall	Check Point cloud	Supported	Supported
	Endpoint Security (EPMaaS)	Check Point cloud	Supported	Supported
	Email Security	Check Point cloud	Not supported	Supported
	Mobile Security	Check Point cloud	Not supported	Can be enabled upon user request
Microsoft	Microsoft 365 Defender for Endpoint	API	Supported	Supported
Fortinet	FortiGate Next Generation Firewall	Syslog	Not supported	Supported

Product Family	Product Name	Log Integration	Response Integration	IOC Management Support
CrowdStrike	Falcon	API	Supported	Supported
SentinelOne	Singularity Endpoint	Syslog	Supported	Supported
Palo Alto Network	Palo Alto Networks Next Generation Firewall	Syslog	Not supported	Supported
Trend Micro	Trend Vision One	API	Supported	Supported
Cisco	Cisco Firepower	Syslog	Not supported	Supported
Okta	Okta	Infinity Identity Providers Integration	Supported	Not supported
Identity Service*	Identity Sources supported by the Check Point Security Gateway	Check Point cloud	Not supported	Not supported

**Tracks unusual user activities, such as repeated failed logins, logins after office hours, and so on. XDR correlates this activity to security events from other sources and generates an incident.*

Key Application Components

This section describes some of the key application components in XDR.

For all tables that contain data, you can filter the records displayed.

Integrations

From this page, you can view the status of the currently integrated products and integrate additional products by following the configuration guidelines.

The **Connectivity** widget in the **Overview** page reflects the status of integrated products and provides summary about the related events.

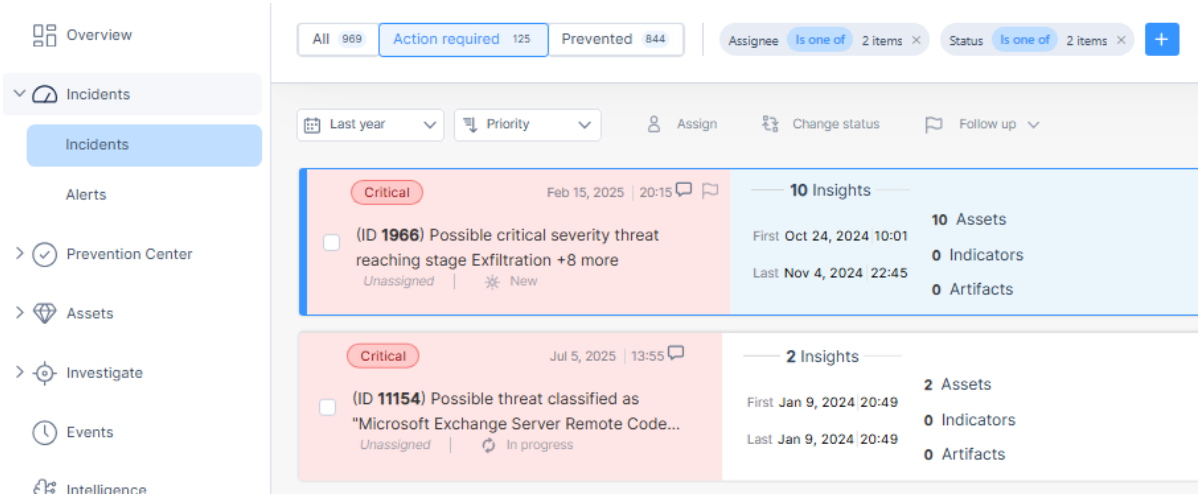
Incident Management

Incidents provide a summarized, prioritized and focused list of items to be handled by the security team. There are two primary workflows that the administrator can follow to review all items:

- Incident List
- Asset Incident Priority

Incident List

Provides a filtered list of all incidents. By default, the filter is set to show incidents that are new or in progress, assigned to the currently logged in administrator or those unassigned. The list is presented in descending order of priority to show those incidents that have **Action Required**.



The set of incidents are also displayed in the **Overview** page in the form of a Kanban board, where incidents are displayed in a table format with columns representing the different incident statuses.

Asset Incident Priority

A widget on the **Overview** page presents an asset-centric view. All incidents have a defined priority and can be associated with one or more assets. The incident priority of an asset is derived from the incidents it is associated with, according to the following criteria:

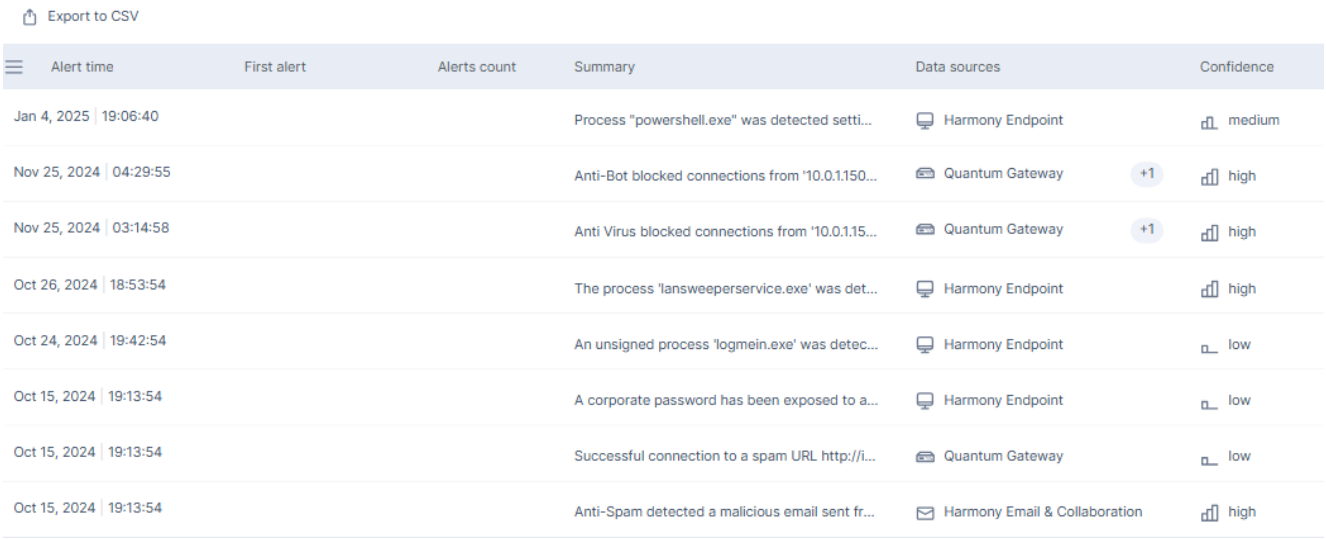
- Incidents that are not in **Closed** state and not marked as **Prevented** are considered to determine the Incident Priority. These are the incidents that require action by the user.
- Some incidents that impact a large number of assets are excluded from determining the Incident Priority. Such incidents are considered as **Filtered**. An example of a filtered incident is a port scan that can be associated with a large number of assets.

The Incident Priority is set to the highest priority of the incidents that meet the above criteria. For example, if there are one or more associated incident(s) with **Critical** priority, then the Incident Priority of the asset is set to **Critical**.

The display also includes the Asset Incident Priority based on **Unassigned** incidents only. This allows any new incidents to be assigned, after which the unassigned count will be reset back to 0.

Alert Table

The Incident list is the primary mechanism for handling issues detected by XDR. The **Alert** table provides additional visibility to all the alerts processed by XDR and their associated verdict and justification. It can be used to audit and provide visibility into the validation on alerts performed by XDR.



Prevention Center

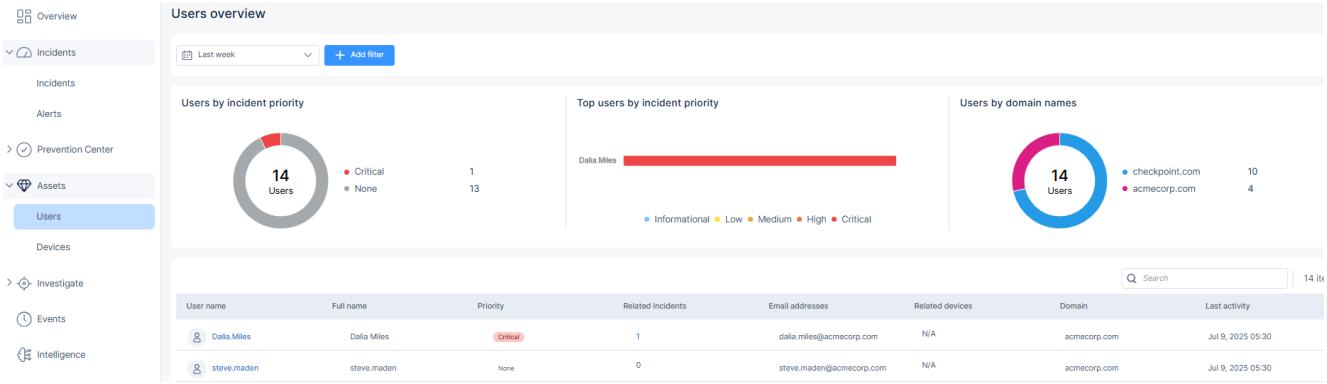
The **Prevention Center** provides a summary of prevention activities performed across all data processed in your account.

It consists of the following sections:

- **Prevention Status** - Shows the statistics of prevention actions in your account, that includes pending, active and expired actions.
- **Executions** - Provides visibility into how XDR processes alerts and executes actions in response to the alerts.

Assets

The **Assets** tables provide asset-centric view on Users and Devices protected by XDR.



For each asset, information is collected and displayed in one of the following categories:

- Asset operational configuration (such as Asset Name, Operating System and Version)
- Visibility into any associated Groups and Organization Units (OU)
- Incident Priority and Related Incidents
- Related Assets - There are interrelations between users and devices. For example, users access a network through one or more device. These relationships are displayed in the **Related Devices** / **Usernames** field.
- Activity Time - The **Last Activity** time is updated whenever data is received for an asset. When you select a time filter for asset display, filtering is done based on the **Last Activity** time of the assets.

Threat Hunting

Threat Hunting is an investigative tool which allows for advanced querying on all malicious and benign forensics events collected from the onboarded Endpoint Security and Quantum Gateway.

The information collected lets you to:

- Investigate the full scope of an attack.
- Discover stealth attack by observation of a suspicious activity.
- Remediate the attack before it causes further damage.
- Proactively hunt for advanced attacks by searching for anomalies, and using hunting leads and enrichment.

Events

A view of all the raw events processed on the tenant. This is the standard **Events** widget included in most of the applications in Check Point Portaland may include events from products that are not integrated with XDR.

Notifications

You can configure and enable notifications to be sent when new a new incident is created. The related configuration includes:

- Conditions for when a notification is to be sent.
- Notification contents.
- Recipients and channels on which the notification is to be sent.

Notifications can be sent by email, Slack and over Microsoft Teams. Notifications allow administrators to get initial details of new incidents without connecting to the application. Notification contents also include a URL to view the full incident details within the application.

XDR Detections

This section provides an overview of the XDR unique detection capabilities, explaining each detection category implemented in our security platform. XDR integrates multiple security layers to provide comprehensive threat detection, investigation, and response across endpoints, networks, cloud workloads, and applications.

The Power of AI in XDR

The XDR solution leverages cutting-edge artificial intelligence to transform security operations. Through multiple AI technologies working in concert, the platform delivers detections of the following types:

- **Autonomous Threat Detection** - AI algorithms continuously analyze vast amounts of data across all security layers to identify threats that would be impossible to detect with manual analysis or rule-based systems.
- **Predictive Threat Intelligence** - Machine learning models predict emerging threats based on subtle behavior patterns before traditional IoCs become visible.
- **Adaptive Security Posture** - The AI engine dynamically adjusts detection parameters as it learns your environment, becoming more accurate and effective over time.
- **Automated Contextual Analysis** - Advanced algorithmics and AI technologies automatically contextualize alerts, reducing the number of false alarms and providing security analysts with comprehensive attack narratives rather than isolated data points.
- **Cognitive Response Automation** - AI-driven decision-making enables intelligent, context-aware automated responses that adapt to the specific nature of each threat.

XDR Unique Detection Method

User and Entity Behavior Analytics (UEBA) is a cybersecurity technology that uses machine learning and advanced analytics to detect abnormal behavior by users and entities (such as devices or applications) that may indicate security threats, such as insider attacks, compromised accounts, or data exfiltration. It establishes baselines of normal activity and flags deviations for investigation. XDR leverages UEBA which enables detection of novel threats and sophisticated attacks that evade conventional defences.

By continuously learning and adapting to our environment, baseline analysis provides context-aware security that reduces false positives while improving detection of true threats. This capability is uniquely powerful within XDR due to its holistic visibility across multiple security layers and data sources.

Detection Catalog

This section provides details about the specific detection categories provided in XDR.

Category	Description
Anonymization and Proxy Services	Detects the use of anonymization tools, VPNs, or proxy services that may indicate attempts to hide malicious activity or evade geographic restrictions. These technologies can be used legitimately but also serve as methods for attackers to mask their origin.
Abnormal Application Data Usage	Identifies unusual patterns in how applications access, process, or transfer data. This includes detecting when applications exceed normal data processing thresholds or access sensitive data they typically do not interact with.
Authentication and Access Patterns	Monitors for unusual authentication flows or access patterns that deviate from established baselines, which could indicate account takeover or unauthorized access attempts.
Brute Force Detection	▪ **Failed Brute Force** - Identifies multiple failed authentication attempts followed by cessation, indicating an unsuccessful brute force attack. ▪ **Brute Force Guessing** - Detects ongoing systematic attempts to guess credentials or access codes, potentially using dictionary or algorithmic approaches.

Category	Description
Insider and Credential Attacks	▪ **Credentials Dumping** - Identifies attempts to extract credentials from memory, security databases, or credential stores. ▪ **Abnormal Failed/Successful Logins** - Detects login attempts that deviate from normal patterns, such as logins from unusual locations, devices, or times. ▪ **Credentials Theft/Abuse** - Recognizes when stolen credentials are being used or when legitimate credentials are being misused.
Command & Control Communication	Detects communication with known malicious infrastructure or unusual communication patterns that may indicate malware connecting to command-and-control servers through non-standard channels.
Network Traffic Patterns	Identifies anomalous network traffic that deviates from established baselines, including unusual protocols, timing patterns, or volumes.
Data Exfiltration	Detects unusual outbound data transfers that could indicate sensitive information being removed from the organization, including large data transfers or communications with suspicious destinations.
Vulnerability Sonar	Identifies reconnaissance activities from external sources attempting to discover vulnerabilities in internet-facing assets, and determine which systems were found vulnerable, which vulnerability was found and if there are undetected systems successfully accessed from the same scanner.
Initial Access	Detect techniques used by threat actors to gain their first foothold in a network, including exploitation of vulnerabilities in public-facing applications, drive-by downloads, or supply chain compromises, open ports and available services.
Internal Discovery and Information Collection	Monitors for systematic attempts to gather information about the internal environment such as Accounts & Groups, Local System Information, Network & Shares, Location, Security Products, Software and system configurations.
Lateral Movement	Detects attempts to move through the network after initial compromise, for example, Executable and File Transfer, unusual remote executions, unusual access or mounting of network shares.
Ransomware, Wiper, or Data Destruction	Detects behaviors that are associated with encrypting files for ransom, wiping data, or other destructive activities targeting information assets.

Category	Description
Security Control Evasion	Identifies techniques used to bypass security controls. Examples - Injection, File Format Tampering, Hidden Artifacts, Indirect Executions, Masquerading, Obfuscation, Script Execution.
Supply Chain Distortion	Identifies IoCs related to trusted software updates or third-party components.
Suspicious Executions	Monitors for unusual execution patterns, commonly used by attackers. Examples - Long Execution Chain, Execution During Remote Connection, Execution During Remote Connection, Unusual LOLBin Execution.
System Behavior	Monitors for changes to system configuration and behavior: ■ **Persistence** - Detects techniques used to maintain access across system restarts. ■ **Process/Library Execution Anomalies** - Identifies unusual process behavior or library usage. ■ **Unusual Configuration Changes** - Detects modifications to system configurations that may indicate compromise.
Security Product Tampering	Identifies attempts to disable or bypass security tools: ■ **Disable Tools** - Detects attempts to turn off security controls. ■ **Local Firewall** - Monitors for changes to firewall configurations. ■ **DNS Configuration** - Identifies suspicious DNS setting modifications.
Suspicious File Operation	Detects suspicious file characteristics or behaviors that may indicate malware.
Suspicious Trace Removal	Identifies attempts to clear logs, delete files, or otherwise remove evidence of compromise.
Time-Based Anomalies	Detects activities occurring at unusual times or with suspicious timing patterns.
Unsolicited External Access	Identifies unexpected inbound connections or data transfers from external sources.

Licensing

At least one valid license is required to entitle the XDR application to operate and perform processing. There are three different aspects of entitlement associated with a license:

- Data Processing Entitlement
- Connected Product Entitlement
- Expiry Date

Data Processing Entitlement

XDR performs extensive analysis and processing of all the data that it receives. Therefore, the entitlement to XDR processing is based on the total amount of data from all connected products that is analyzed and processed.

There are two types of licenses that can contribute to this entitlement:

- **License with a per-user Entitlement** - License is purchased for a specific number of users. Each user is assigned a data entitlement as defined in the product catalog. The total data entitlement of the license is calculated by multiplying the number of users and the per-user entitlement.
- **Volume Entitlement** - License that gives entitlement directly as a number of gigabytes (GB).

It is possible to have multiple active licenses, including a mix of both license types. The total data processing entitlement is the sum of the entitlements provided by all active licenses.

To track the current volume of data being processed, compared to the entitlement, go to **Settings** > **Log Processing**. The current volume of data being processed is calculated as the average volume of data processed daily, during the last seven days.

Connected Product Entitlement

There are two types of licenses in terms of connected product entitlement:

- **Endpoint Security only** - Licenses that are purchased together with Endpoint Security (HEP). With this license, XDR is operational as Endpoint Detection and Response (EDR).
- **All Products** - All products can be connected.

  There must be at least one active license for **All Products** to integrate additional products.

License Expiration

Each individual license has an expiry date. When this date is reached, the license expires and the corresponding entitlement associated with the license is no longer active. When all active licenses have expired, XDR enters a Grace Period before all processing of data is stopped. The current Grace Period after expiry of production licenses is 30 days but this duration is subject to change.

Data Retention

The raw events from all connected products, including third-party products, are retained for a default period of 3 months. To extend this duration to 6 or 12 months, you can purchase additional licenses as part of Events & AIOps - Logging & Analytics.

These retention periods also apply to any data derived or retrieved by XDR. This includes incidents and report files, such as forensic reports, that are retrieved from other systems and stored in XDR.

Supported Regions

XDR is supported only for the Check Point Portal tenants (accounts) residing in these regions:

- EU
- US
- India (AI Copilot and Playblocks are not available)
- UAE (AI Copilot and Playblocks are not available)

When leveraging XDR with other Check Point products, the region selected for XDR account creation must match the region to which the other products are sending data.

API Support

The following suites of APIs are available for interaction with XDR. They are available for use with a valid XDR license:

- **XDR/XPR API** - Operations related to incidents, alerts, actions and exceptions.

  See XDR/XPR API.

- **Threat Hunting API** - Retrieves Threat Hunting records.

  See TH API Docs.

- **Infinity Events API** - Retrieves raw Event logs as displayed in the **Events** tab.

  See Infinity Events API.

Getting Started

To get started with Check Point XDR (formerly Infinity XDR/XPR):

1. Create an Account in the Check Point Portal
2. Access the XDR Administrator Portal
3. License the product
4. On-board Applications
5. Add Users
6. Address an Incident

Creating an Account in the Check Point Portal

Check Point 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.

Accessing the XDR Administrator Portal

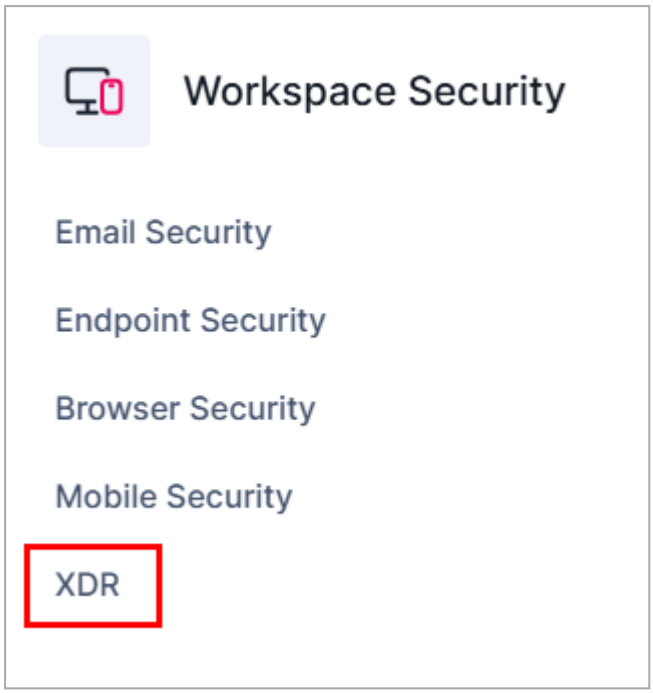
Notes:

- XDR is supported only for the Check Point Portal tenants (accounts) residing in these regions:
  - EU
  - US
  - India (AI Copilot and Playblocks are not available)
  - UAE (AI Copilot and Playblocks are not available)
- The recommended browser is Google Chrome.

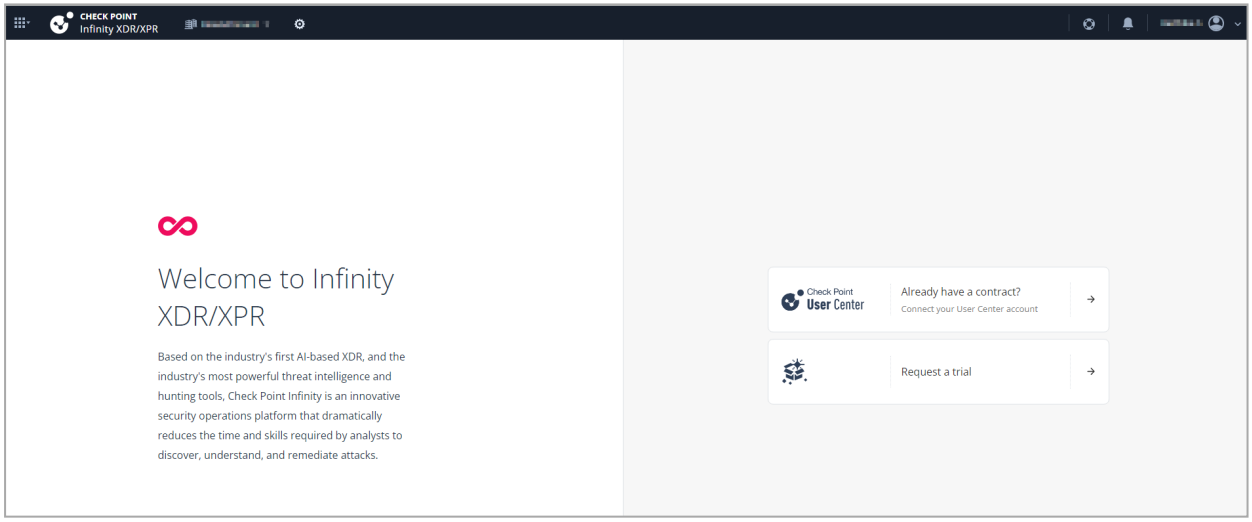
To access the XDR Administrator Portal (formerly Infinity XDR/XPR):

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

3. In the **Workspace Security** section, click **XDR**.



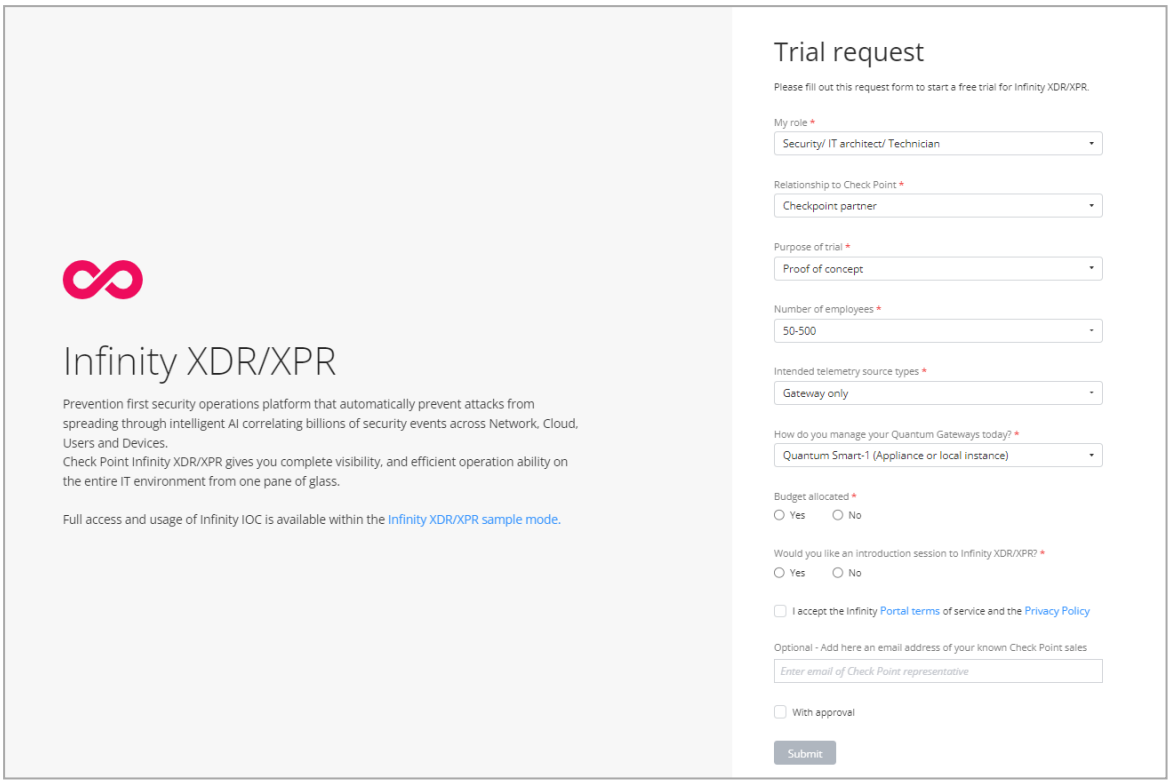
4. If you are accessing the portal for the first time, do one of these:



   - 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 the *Check Point Administration Guide*.

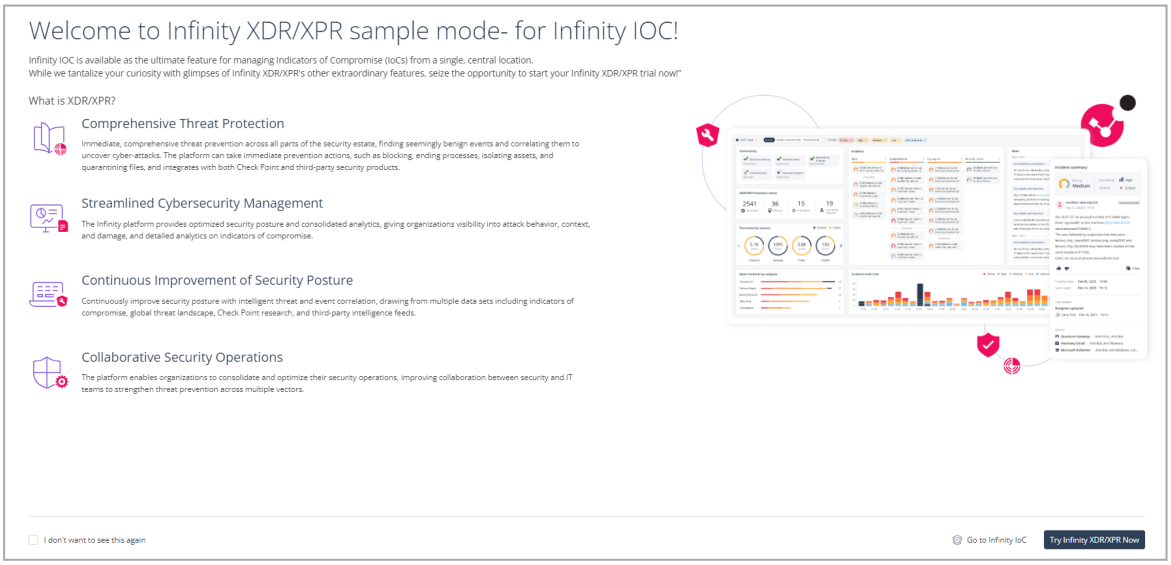
- If you want to trial the product, click **Request a trial**.

  Fill and submit the **Trial request** form. You will receive an email with the trial status and further instructions to proceed.

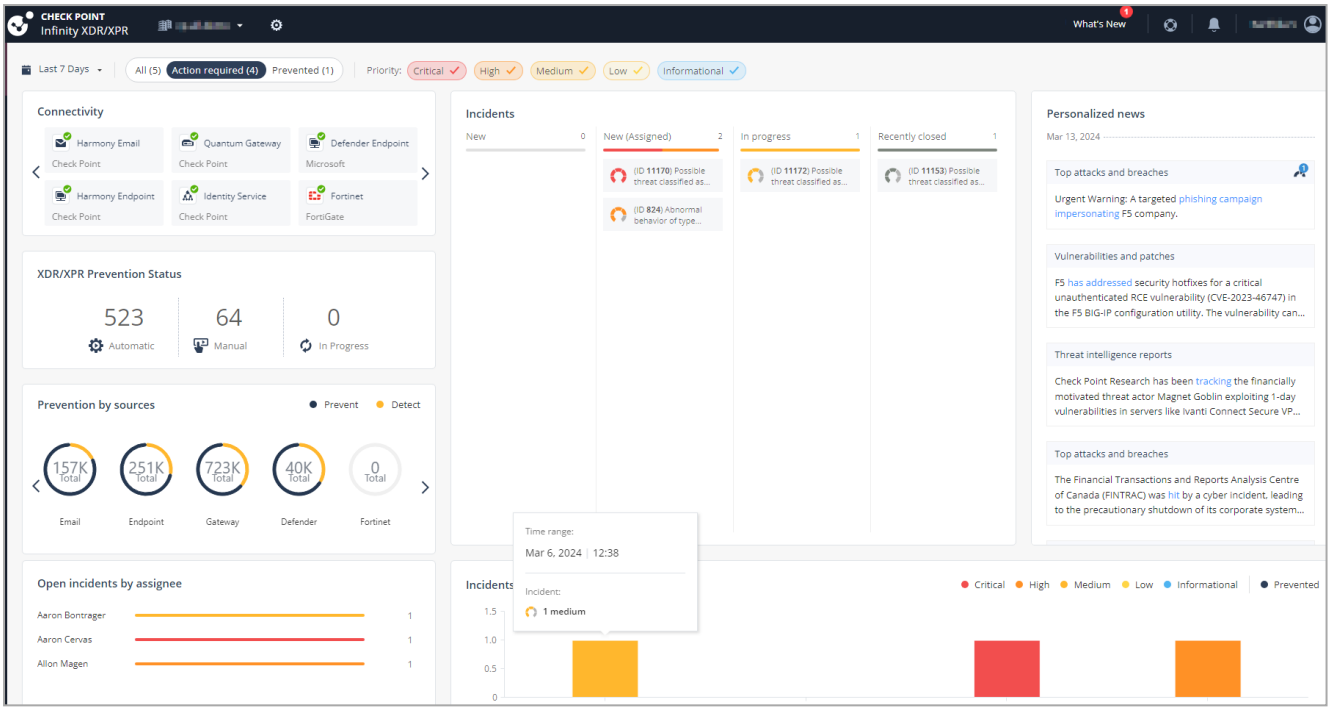


  Optionally, you can click **XDR sample mode** to experience the application with sample data before the trial.

  Click **Try XDR Now** to fill and submit the **Trial request** form.



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



Licensing the Product

Check Point XDR licenses include:

- Playblocks (All playbooks included)
- Events & AIOps
- AI Copilot
- IoC Management

Licensing Options

Check Point XDR offers flexible licensing options:

- **Full XDR** – All integrations included.
- **Infinity EDR** – XDR for Endpoint Security (Harmony Elite).
- **Managed XDR** – XDR bundled with Infinity Global Services (IGS).

Data Retention

- Standard - 90 days
- Optional upgrades - 6 months or 1 year

Getting Started with Licensing

Start a Free Trial

New accounts are eligible for a 30-day trial. During this period, you can connect your security solutions and evaluate the platform's capabilities.

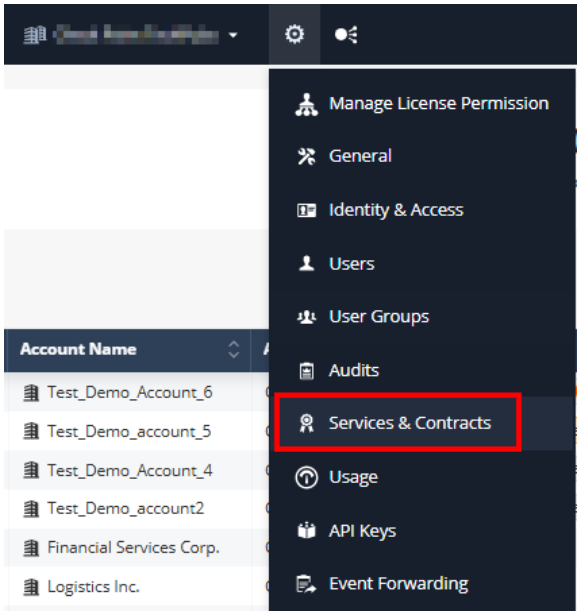
To purchase a license:

- Contact your Check Point representative or partner.
- For technical assistance, contact XDR sales team.

Activating a License

To activate a license:

1. Log in to the Check Point Portal.
2. Click the **Global Settings** icon next to the tenant's name.
3. Click **Services & Contracts**.



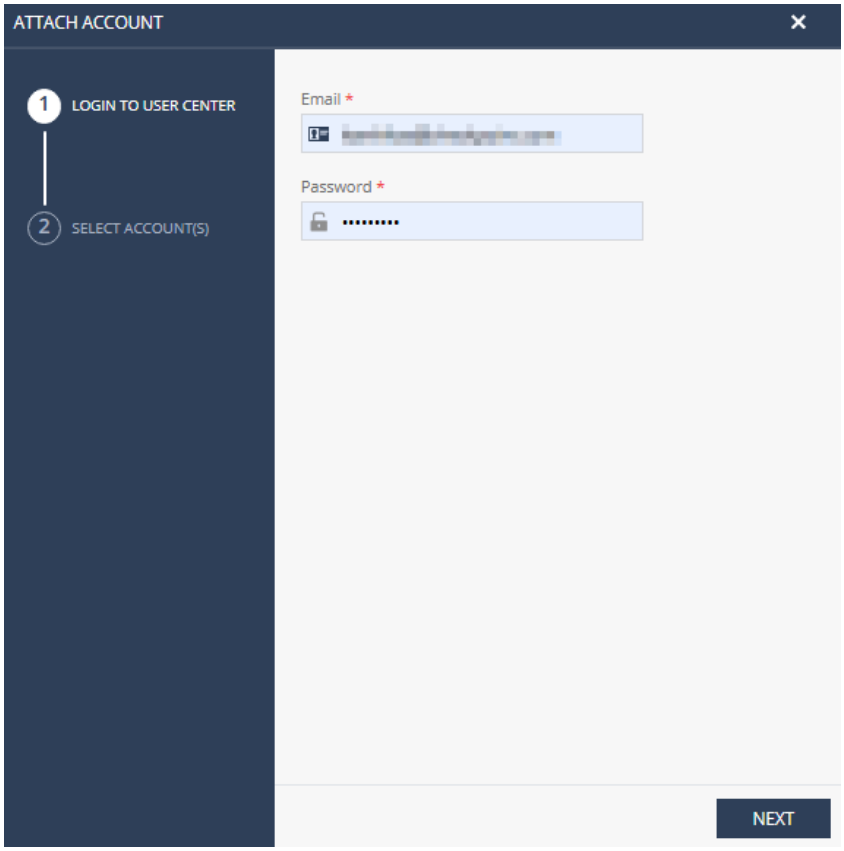
4. From the top-right, click **Associated Accounts/Manage Accounts**.

   The **Managed Accounts** window appears.

5. Click **Attach Account**.

   The **Attach Account** window appears.

6. Enter your User Center account credentials.



7. Click **Next**.
8. Select the license to apply.
9. Click **Finish**.

   Once the process is complete, the license is displayed in the **Services & Contracts** page. For more information, see sk182949.

Notes:

- If you already have a related account and want to add one more license, go to **Global Settings** > **Services & Contracts** > **Associated Accounts** and use the **sync** option to update the license. Once updated, the license status appears as **Active**.
- It may take up to 24 hours for the license status to update to **Active**.

License Expiration Policy

- After the license expires, XDR stops generating new security incidents.
- After a 60-day grace period, access to the application will be disabled.
- For license extensions or support, contact your partner or Check Point representative.
- For technical assistance, contact XDR sales team.

On-boarding Products

This table provides the on-boarding process for the supported products:

Product Family	Product Name	On-boarding Process
Check Point	Quantum Security Gateway	■ On-premises • For R81.10 with the R81.10 Jumbo Hotfix Accumulator Take 93 and higher, see **Sharing SmartConsole Configuration and Logs with Check Point Portal** > **To share your on-premises Management Server log information with the Check Point Portal** in the *R81.10 Security Management Administration Guide*. • For R81.20, see **Sharing SmartConsole Configuration and Logs with Check Point Portal** > **To share your on-premises Management Server log information with the Check Point Portal** in the *R81.20 Security Management Administration Guide*. • For R82, see **Connecting On-Premises Management Servers and Security Gateways to the Check Point Portal** in the *R82 Security Management Administration Guide*. **Note** - To on-board Multi-Domain Security Management Servers to a single tenant, see sk182156. ■ Smart-1 Cloud - Automatic if you subscribe to Hybrid Mesh Network Security Security Gateway.
	Cloud Firewall	Automatic if you subscribe to Cloud Firewall.
	Endpoint Security (EPMaaS)	Automatic if you subscribe to Endpoint Security. Ensure that you enable Threat Hunting in Endpoint Security. To enable, see *"Enabling Threat Hunting" on page 166*. **Note** - You can on-board only one account (tenant) of Endpoint Security.
	Email Security	Automatic if you subscribe to Email Security. **Note** - You can on-board only one account (tenant) of Email Security.

Product Family	Product Name	On-boarding Process
	Mobile Security	Automatic if you subscribe to Mobile Security. **Note** - You can on-board only one account (tenant) of Mobile Security.
Microsoft	Microsoft 365 Defender for Endpoint	See *"Microsoft 365 Defender for Endpoint" on page 245*.
Fortinet	FortiGate Next Generation Firewall	See *"Fortinet FortiGate Next Generation Firewall" on page 249*.
CrowdStrike	Falcon	See *"CrowdStrike Falcon" on page 263*.
SentinelOne	Singularity Endpoint	See *"Singularity Endpoint" on page 271*.
Palo Alto Network	Palo Alto Networks Next Generation Firewall	See *"Palo Alto Networks Next Generation Firewall" on page 282*.
Trend Micro	Trend Vision One	See *"Trend Vision One for Endpoint" on page 305*.
Cisco	Cisco Firepower	See *"Cisco Firepower Threat Defense" on page 311*.
Identity Service	Identity Sources supported by the Check Point Security Gateway	Enable Identity Awareness (IDA) blade on your Check Point Security Gateway. Refer to the Identity Awareness Administration Guide for your version > chapters **Configuring Identity Awareness** and **Identity Sources**.

After you successfully on-board, appears for the product in the **Connectivity** widget. If does not appear after 45 minutes of on-boarding, contact *Check Point Support*.

The connection timeout duration is 48 hours. If the product does not send events to XDR in 48 hours, the product becomes inactive and the icon changes to red.

Note - The connectivity status of Cloud Firewall is indicated by Quantum Gateway.

Adding Users

To address incidents, you must assign it to a Security Operations Center (SOC) analyst (assignee) in your organization. To assign, you must add SOC analysts as users with **Operator** service specific role in the XDR portal. The specific service roles are in addition to the global rules and do not override them. For more information, see Specific Service Rules in the *Harmony Endpoint EPMaaS Administration Guide*.

To access **Specific Service Roles**, go to **Global Settings** > **Users** > **New** > **Add User** and expand **Specific Service Roles**.

Role	Description
Admin	Full Read and Write access to all system aspects.
Operator	Full access to handle incidents, including taking prevention actions, and read-only access to the **Policy** menu. Typically, your SOC analyst.
Read-Only	Read-only access to the application.

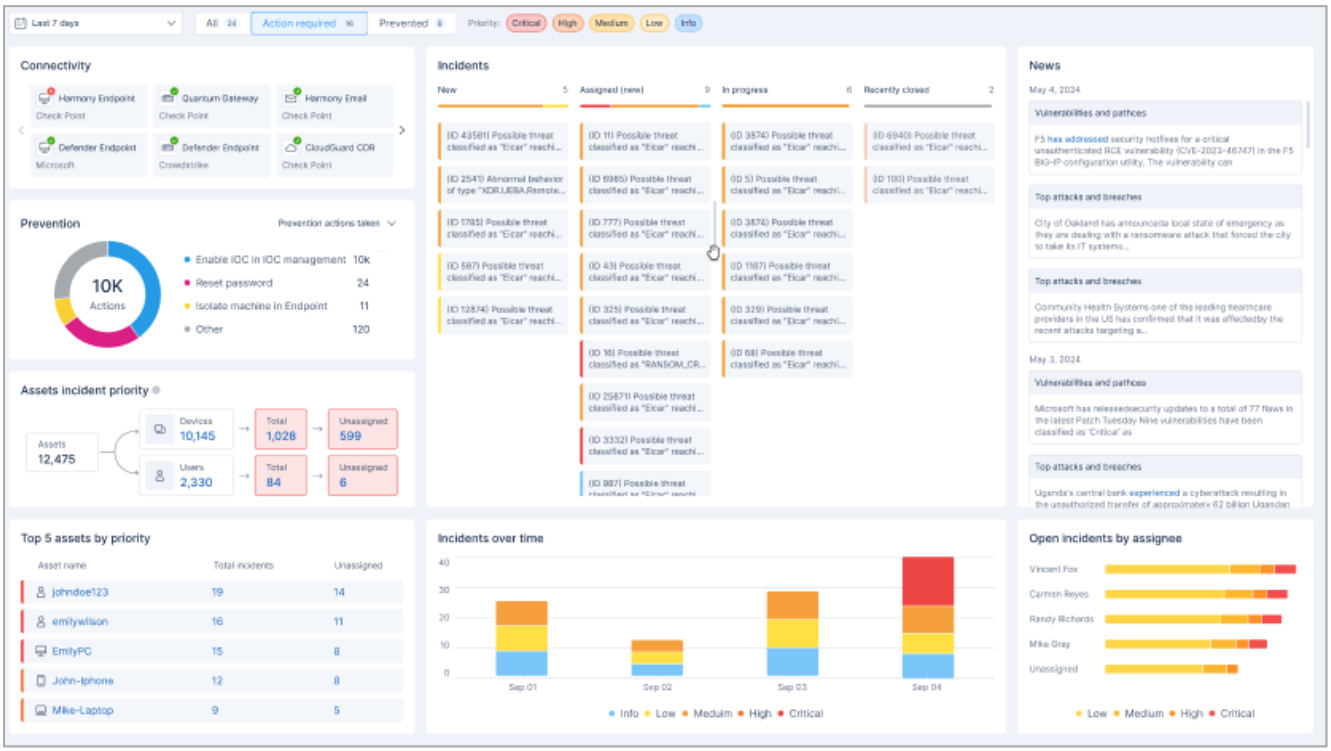
How to Address an Incident

Step	Owner	Action
1	XDR	XDR generates an incident.
2	Administrator	Assign the incident to a Security Operations Center (SOC) analyst.
3	SOC Analyst	In the *"Incidents" on page 57* page, review these information on the incident: ■ Description ■ Priority level ■ Sources ■ MITRE ATT&CK tactics involved. ■ Assets involved. ■ Identified Indicators of Compromise. ■ Prevention actions taken and recommended prevention actions. ■ Timeline of the incident
4	SOC Analyst	For further investigation on the incident: ■ See *"Incidents - Insights & Forensics" on page 113* to view insights and forensics (processes, files, URL, domains and Registry involved in the insight) related to the incident. ■ See *"Incidents - Affected Assets" on page 94* to view the assets involved in the incident. ■ See *"Incidents - Indicators & Artifacts" on page 101* to view the indicators and artifacts involved the incident. ■ See *"Incidents - Forensics Trees" on page 93* to view a graphical representation of the forensic report generated by Endpoint Security for each detection in an insight. ■ See *"Incidents - MITRE" on page 110* to know the MITRE ATT&CK tactics used in the incident.

Step	Owner	Action
5	SOC Analyst	To investigate the Indicator of Compromise involved in the incident and analyze a file, see *"Intelligence" on page 210*.
6	SOC Analyst	To investigate the logs further, see *"Threat Hunting" on page 165*.
7	SOC Analyst	Take the recommended prevention actions. See *"Prevention" on page 70*.

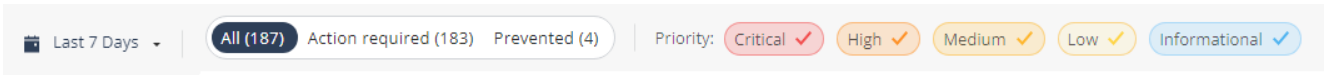
Overview

The **Overview** page shows a summary of the security operations of the on-boarded applications.



To view the **Overview** page, access Check Point XDR and click **Overview**.

By default, the **Overview** page shows the data (all priorities) from the last 7 days.



To filter the data by priority:

1. Select the time period. By default, it lists from the last 7 days.
2. To filter incidents that require action, click **Action required**.
3. To filter incidents prevented automatically by XDR, click **Prevented**.
4. To filter incidents of specific priority, select the required **Priority**. By default, all priority levels are selected.

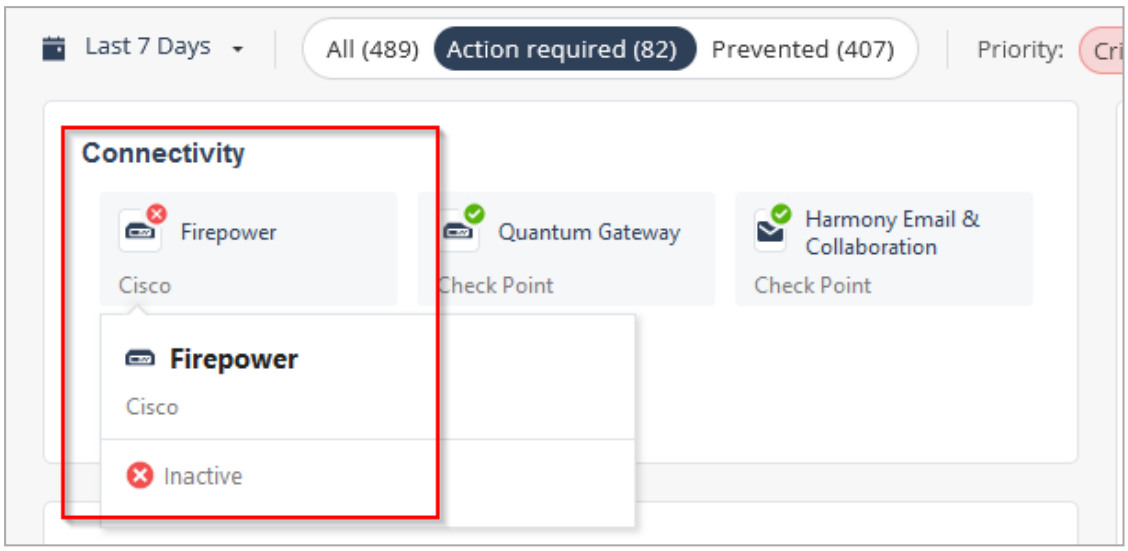
Connectivity

The **Connectivity** widget shows the connection status of the products connected to Check Point XDR. When you hover over the product name in the widget, you can view the following details:

- The connectivity status of the product.
- The number of events sent by the product.
- Time when the product sent the last event.

Notes:

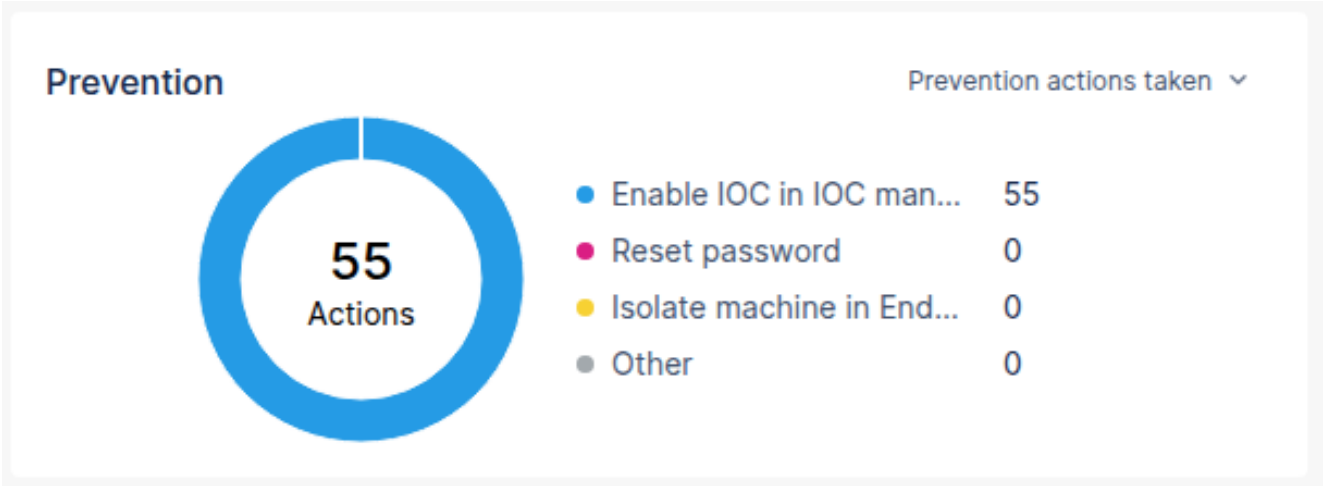
- The connection timeout duration is 48 hours. If the product does not send events to XDR in 48 hours, the product becomes inactive and the icon changes to red.



- The connectivity status of Cloud Firewall is indicated by Quantum Gateway.
- Certificate expiry status for the Fortinet FortiGate Next Generation Firewall integration is indicated by the icon.
  For example:

  To renew the certificate, see *"Fortinet FortiGate Next Generation Firewall" on page 249*.

Prevention

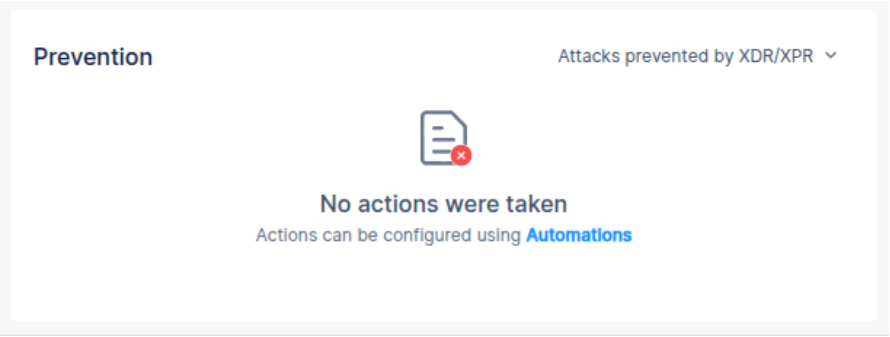


The **Prevention** widget shows statistics from the Prevention Center.

You can filter the widget by:

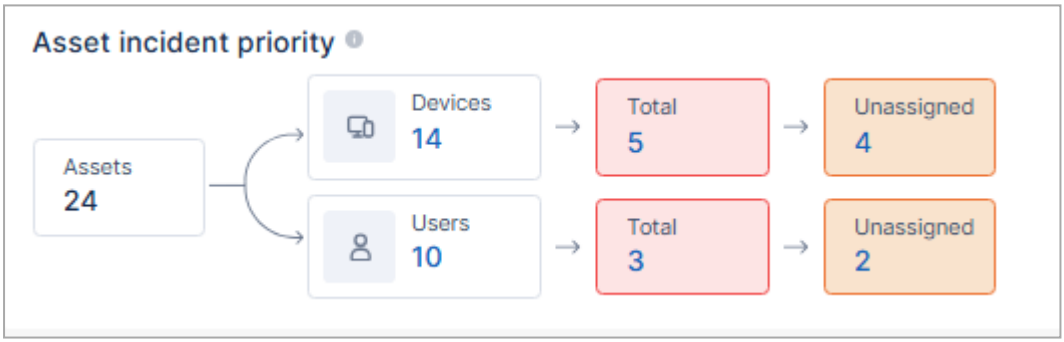
- **Prevention actions taken** (default)
- **Attacks prevented by XDR/XPR**

Note - If no data is available for the filtered option, the widget appears as:



To configure automatic prevention actions, click the **Automations** link. The *"Automations" on page 232* page appears.

Asset Incident Priority



The **Asset incident priority** widget shows:

Item	Description
Assets	Total number of assets (Devices + Users) in your account.
Devices	Number of Device assets in your account. To view the asset details, click the link. The *"Devices" on page 152* page appears.
Users	Number of User assets in your account. To view the asset details, click the link. The *"Users" on page 139* page appears.

Item	Description
Total	Total number of assets (Devices/Users) with incidents that are at **Critical** or **High** priority levels. Hover over the widget to view the count in each category. To view assets' details, click the link. The Devices/Users page appears filtered by **Incident Priority**.
Unassigned	Number of assets (Devices/Users) with unassigned incidents that are at **Critical** or **High** priority levels. Hover over the widget to view the count in each category. To view assets' details, click the link. The Devices/Users page appears filtered by **Incident Priority** and **Related Incidents** that are unassigned.

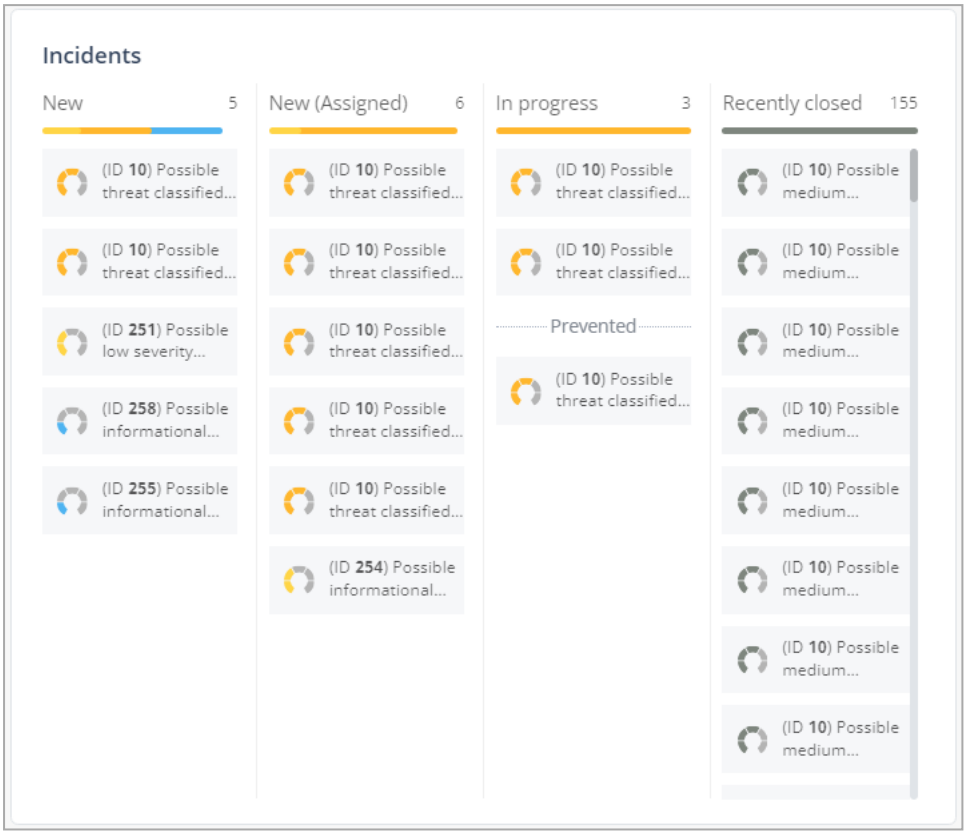
Top 5 Assets by Priority

The **Top 5 assets by priority** widget shows the top five assets based on the priority levels of their related incidents.

The table shows:

Item	Description
Asset name	Name of the asset. To view the details, click the asset name.
Total incidents	Total number of incidents related to the asset. To view the details, click the count. The *"Incidents" on page 57* page appears and lists all the related incidents.
Unassigned	Number of unassigned incidents related to the asset. To view the details, click the count. The *"Incidents" on page 57* page appears and lists the unassigned incidents.

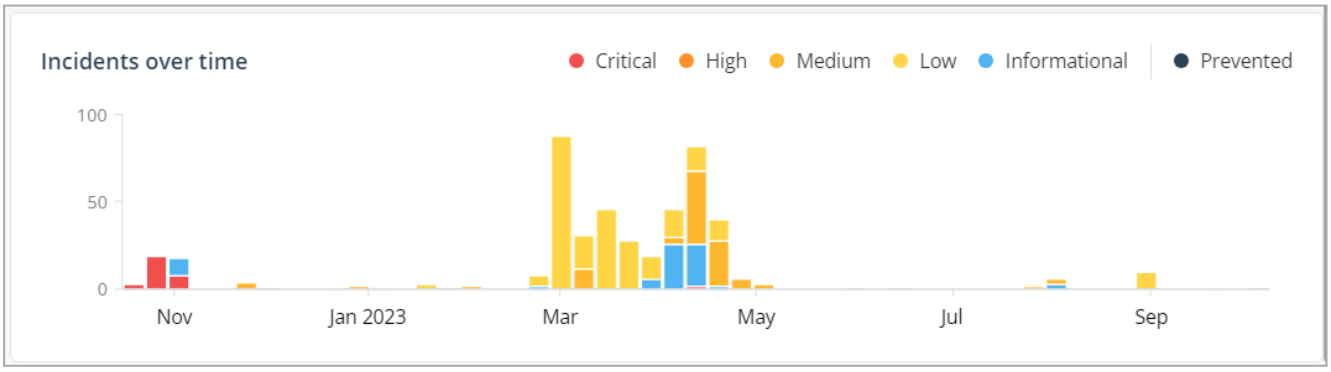
Incidents



The **Incidents** widget lists incidents by status. Hover over the incident for more information. Incidents are color-coded based on the priority levels.

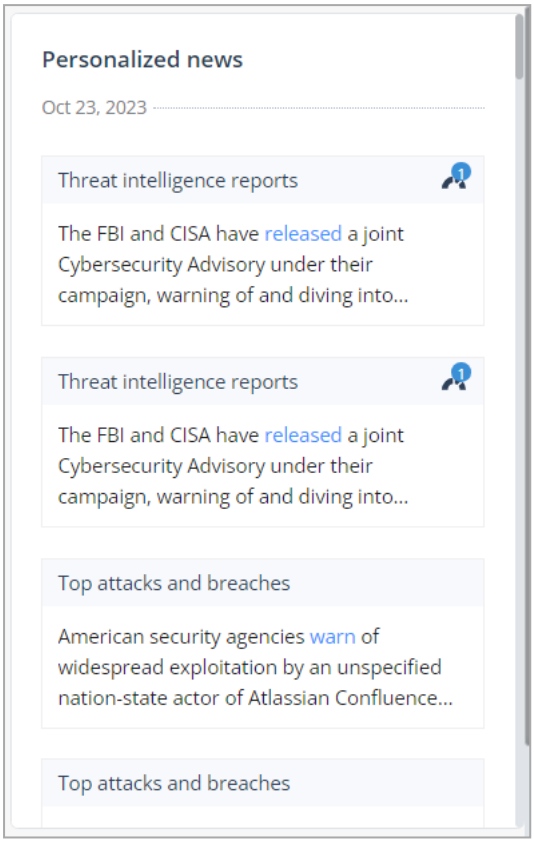
Under **Prevented**, the widget shows the incidents automatically prevented by XDR.

Incidents Over Time



The **Incidents over time** widget shows the timeline of incidents by priority. Incidents are color-coded based on the priority levels.

Personalized News



The **Personalized News** widget shows cyber security news curated by the Check Point research team.

- XDR analyzes the logs for the vulnerability described in the news article and creates incidents if necessary.
- News related to existing incidents are listed first at the top. To view the related incidents, click the icon. The system redirects to the *"Incidents" on page 57* page and shows the related incidents.

Open Incidents by Assignee

The **Open incidents by Assignee** widget lists the number of open incidents for each assignee. Incidents are color-coded based on the priority levels.

Incidents

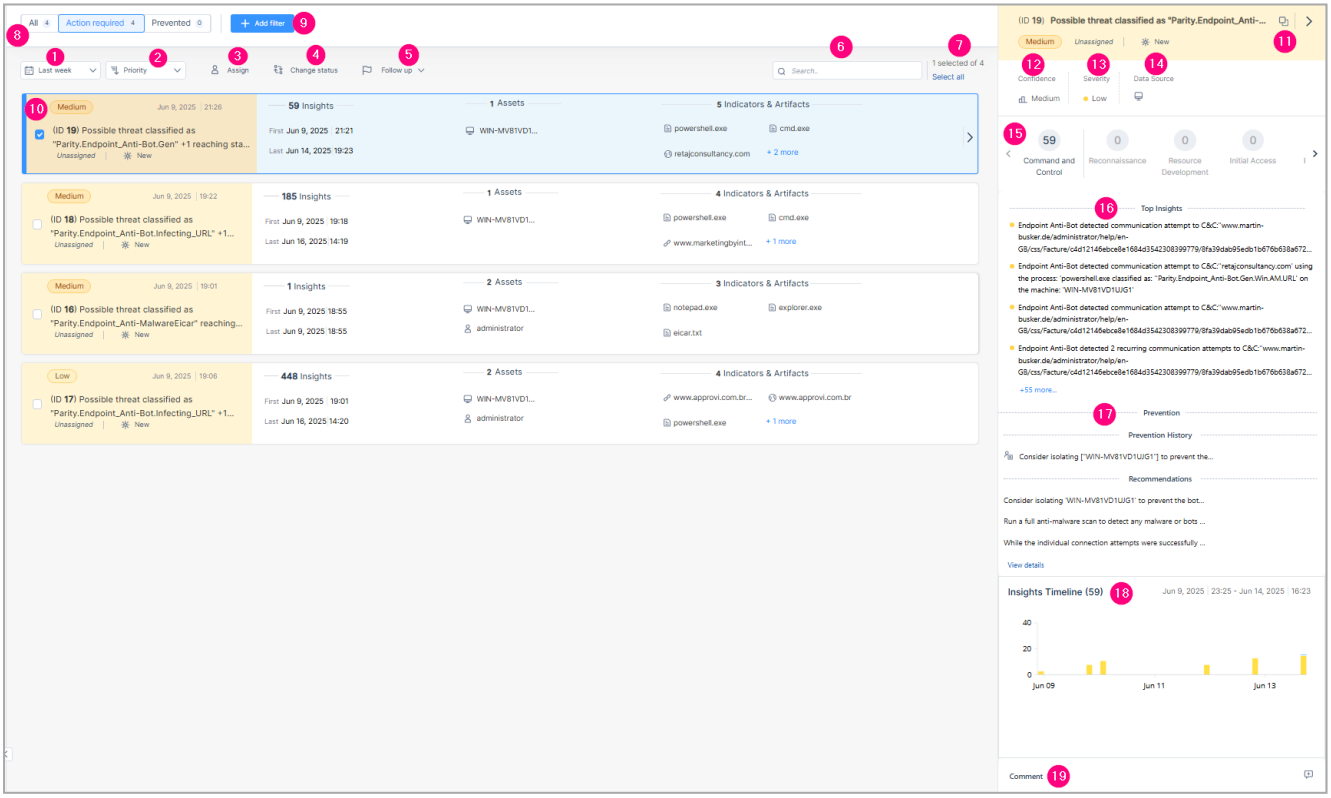
Incidents

An incident is a collection of events from one or more products that together represent an attack story. Check Point XDR (formerly Infinity XDR/XPR) utilizes ThreatCloud's Artificial Intelligence (AI) and applies Machine Learning (ML) models to correlate between the events from on-boarded products (both benign and security events) into unified incidents. The incident's priority level is calculated based on the artifacts of the incident, including the confidence and severity levels of the detection. Incidents are actionable with prevention steps that can be taken within the XDR application.

The **Incidents** page shows the list of incidents and its details that includes:

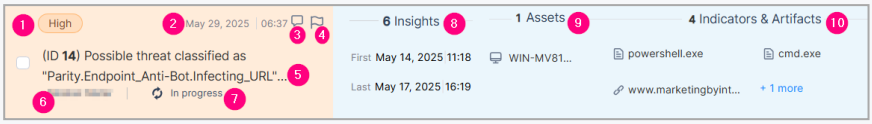
- Insights that triggered the incident and its timeline
- Impacted assets and users
- Indicators
- Prevention history and recommended prevention actions. You can automate some of these actions. For more information, see *"Automations" on page 232*.

To view the **Incidents** page, access Check Point XDR and click **Incidents** > **Incidents**.



Legend	Item	Description
1	Time span	Select the duration for which you want to view the incidents. ■ Last 24 hours ■ Last week ■ Last two weeks ■ Last month ■ Last year
2	Sort by	Select a criterion to sort the incidents. ■ Priority ■ Creation date ■ Last update ■ Severity
3	Assign	Assign a security expert to address the incident.
4	Change status	Change the status of the incident. ■ New ■ In Progress ■ Close - Handled ■ Close - False Positive ■ Close - Known Activity
5	Follow up	Indicates that the incident requires a follow-up. **Note** - XDR does not send automatic reminders for follow-up.
6	Search	Search for the an asset, incident or a user.
7	Select all	Select or clear all incidents.
8	Filters	Filter the incidents by: ■ All ■ Action required ■ Prevented

Legend	Item	Description
9	 Add filter	Allows you to filter the incident list. **To add a new filter:** 1. Click **+ Add Filter**. 2. Enter **Field**, **Operator** and **Value**. 3. Click **Save**. You can filter the incidents by: ■ Assignee ■ Confidence ■ Data Source ■ Incident Sequence ID ■ MITRE tactics ■ MITRE Techniques ■ News Articles ■ Prevented ■ Priority ■ Severity ■ Status

Legend	Item	Description
10	Incident	Shows incident details. 

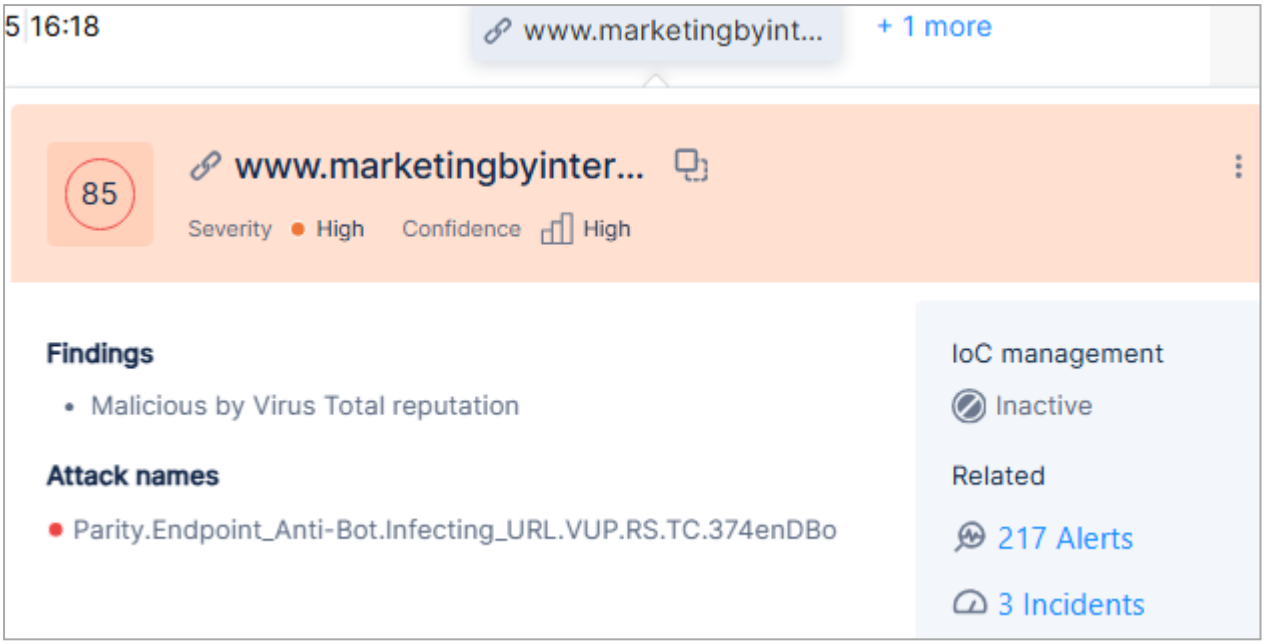
Legend	Description
1	Priority of the incident: ■ Critical ■ High ■ Medium ■ Low ■ Informational
2	Date and time when the incident was generated.
3	View the comments added related to the incident.
4	Add or remove the follow-up flag on the incident.
5	Incident ID and title. Click the title to open the *"Incidents - Overview" on page 64* page.
6	Security Operations Center (SOC) analyst assigned to the incident. Shows **Unassigned** if an incident is unassigned.
7	Status of the incident. Click to set the status. ■ New ■ In Progress ■ Close - Handled ■ Close - False Positive ■ Close - Known Activity

<table>
<tr><th>Legend</th><th>Item</th><th>Description</th></tr>
<tr><td></td><td></td><td>
<table>
<tr><th>Legend</th><th>Description</th></tr>
<tr><td>8</td><td>Number of insights involved in triggering the incident with date and time when the first and last insight was created. Click to view "Incidents - Insights & Forensics" on page 113 page.
An insight is anaggregation of one or more logs into valuable observations indicating the nature of the activity.</td></tr>
<tr><td>9</td><td>Number of assets involved in the incident.</td></tr>
<tr><td>10</td><td>Number of indicators and artifacts involved in the incident.
Hover over an indicator/artifact to view its Intelligence widget card. For more information, see "Intelligence Widget Card" on the next page.</td></tr>
</table>
</td></tr>
<tr><td>11</td><td>  </td><td>Opens the incident "Incidents - Overview" on page 64 page in a new tab.</td></tr>
<tr><td>12</td><td>Confidence</td><td>Confidence level of the detection:
High
Medium
Low</td></tr>
<tr><td>13</td><td>Severity</td><td>Priority of the incident:
Critical
High
Medium
Low
Informational</td></tr>
</table>

Legend	Item	Description
14	Source	The source of the events correlated into the incident. ■ Endpoint (Endpoint Security) ■ Gateway (Quantum Security Gateway and/or Cloud Firewall) ■ Email (Email Security) ■ Mobile (Mobile Security) ■ Defender (Microsoft Defender) ■ Identity Service
15	MITRE ATT&CK	MITRE ATT&CK tactics and techniques involved in the incident. The numbers represent the number of insights related to each tactic. Opens the *"Incidents - Insights & Forensics" on page 113* page that shows the related insights.
16	Top Insights	Top insights for the incident.
17	Prevention	Lists prevention actions taken and those that are recommended to be taken.
18	Insights Timeline	Shows the timeline of insights and the duration between the first and the last insight.
19	Comments	Shows the comments added for the incident. Click to add a comment.

Intelligence Widget Card

The **Intelligence widget** card displays the latest intelligence information about the indicator/artifact. The card's color reflects the severity level of the indicator/artifact.



The card displays these details:

- Indicator/artifact value
- XDR score which indicates the overall threat level
- Severity level
- Confidence level
- Findings - Findings from the XDR validation engines.
- Attack names - Name of attacks in which the indicator/artifact was involved.
- General information based on the indicator/artifact type and the third-party threat intelligence verdict.
- Status of the indicator in IOC Management.
- Related info:
  - Number of related alerts - Click the link to view the **Alerts** page filtered by the specific indicator.
  - Number of related incidents - Click the link to view the **Incidents** page filtered by the specific indicator.

Note - If the indicator/artifact information was updated after the incident was created, the card displays the message **Information updated since initial analysis** at the top right.

Click the ⋮ icon on the card to perform more actions on the indicator/artifact.

Top Banner

The top banner is displayed in these pages:

- *"Incidents - Overview" below*
- *"Incidents - Affected Assets" on page 94*
- *"Incidents - Indicators & Artifacts" on page 101*
- *"Incidents - MITRE" on page 110*
- *"Incidents - Insights & Forensics" on page 113*
- *"Incidents - Forensics Trees" on page 93*.

You can see the incident title, priority of the incident and allows you to add a comment and change incident status.

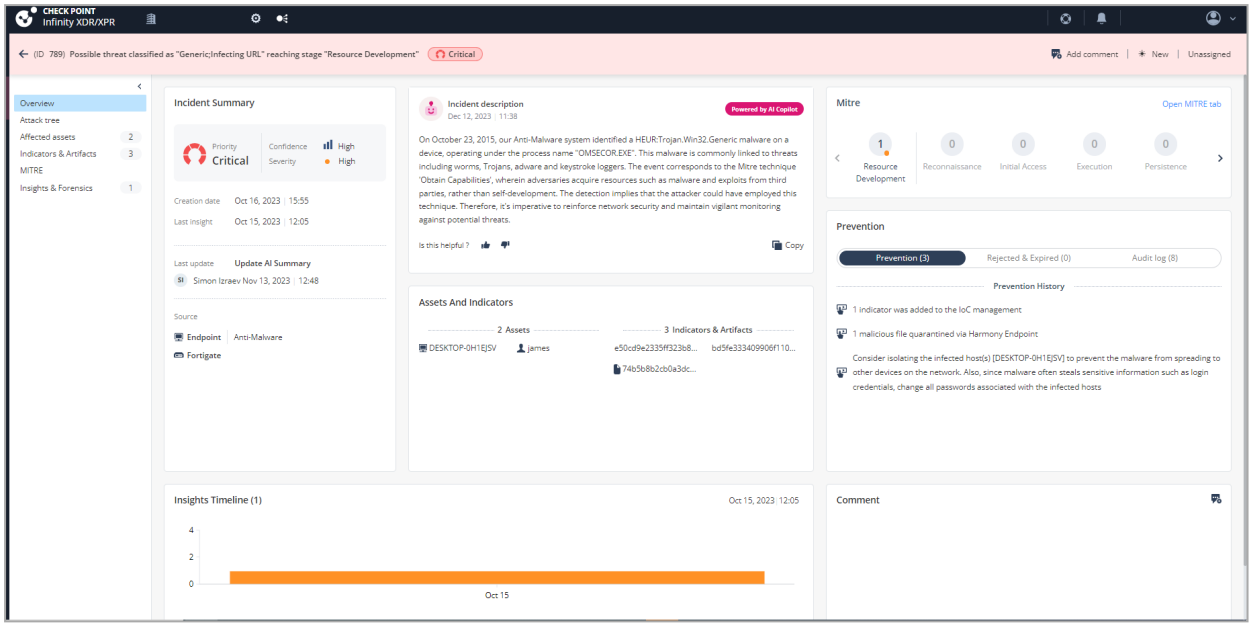
Incidents - Overview

The **Overview** page shows the details of the incident and allows you to perform these actions:

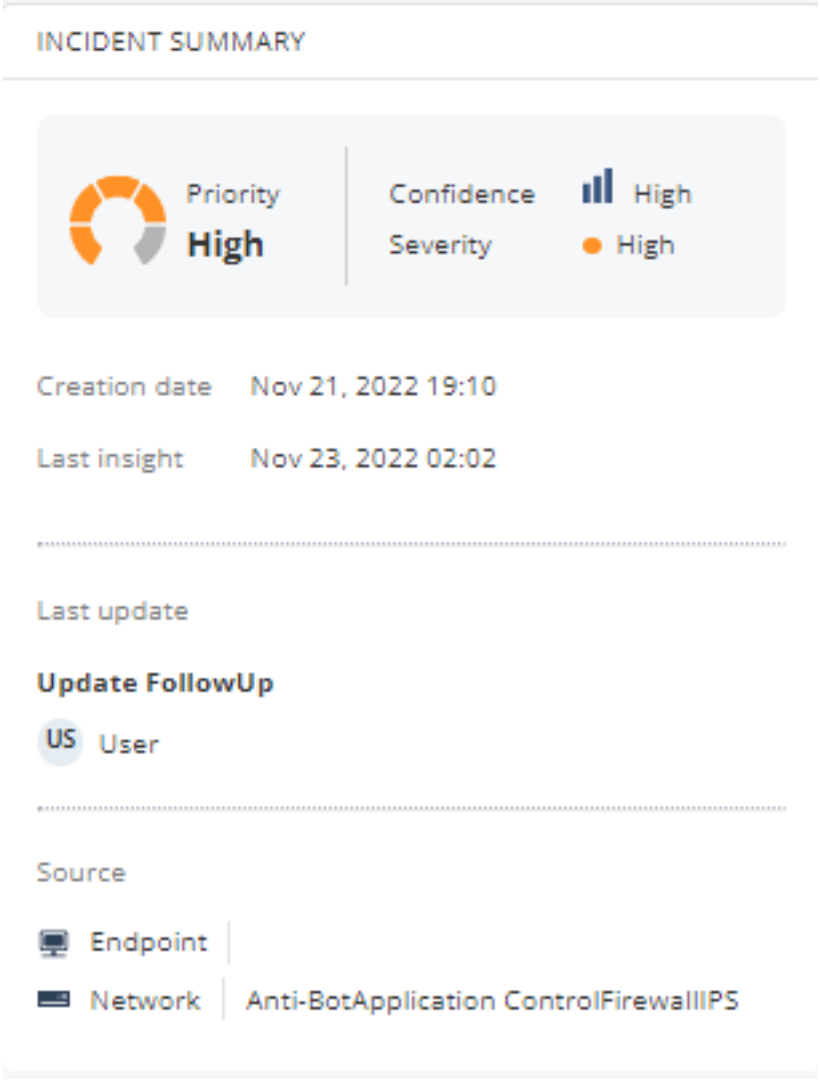
- *"Managing Assets and Indicators" on page 69*
  - Copying an asset, indicator or artifact name to the clipboard
  - Viewing forensic details related to the chosen asset
  - Viewing intelligence for asset, indicator or an artifact
  - Searching for an asset, indicator or an artifact in an incident
- Execute prevention actions. See *"Prevention" on page 70*
- *"Adding a Comment" on page 76*
- *"Creating Advanced Exclusions from an Incident" on page 76*

To view the **Overview** page:

1. Access XDR and click **Incidents** > **Incidents**.
2. Click the incident title or hover over the incident and click **>**.



Incident Summary

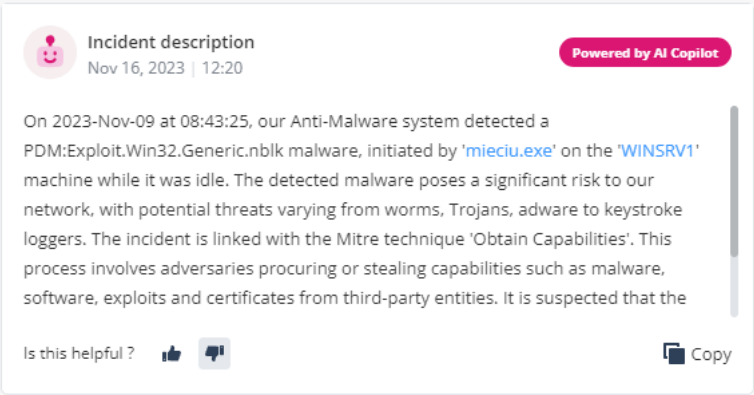


The **Incident Summary** widget shows:

- Priority of the incident:
  - Critical
  - High
  - Medium
  - Low
  - Informational
- Confidence level of the detection:

  - High
  - Medium
  - Low
- Severity of the incident:
  - Critical
  - High
  - Medium
  - Low
  - Informational
- Creation date - Date and time when incident was created.
- Last insight - Date and time when the last insight was added to the incident.
- Last update on the incident
- The source of the events correlated into the incident.
  - Endpoint (Endpoint Security)
  - Gateway (Quantum Security Gateway and/or Cloud Firewall)
  - Email (Email Security)
  - Mobile (Mobile Security)
  - Defender (Microsoft Defender)
  - Identity Service

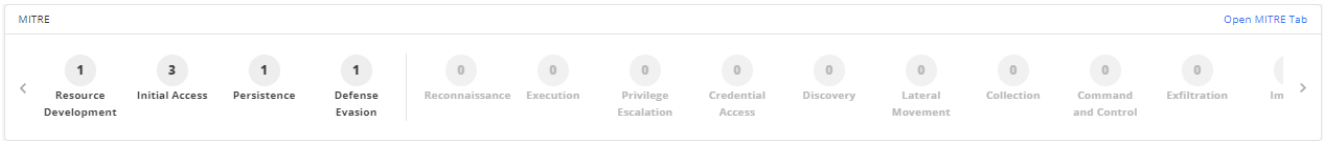
Incident Description



The **Incident Description** widget shows the AI generated description of the incident.

To provide feedback on the description, click or , enter a description and click **Save**.

MITRE



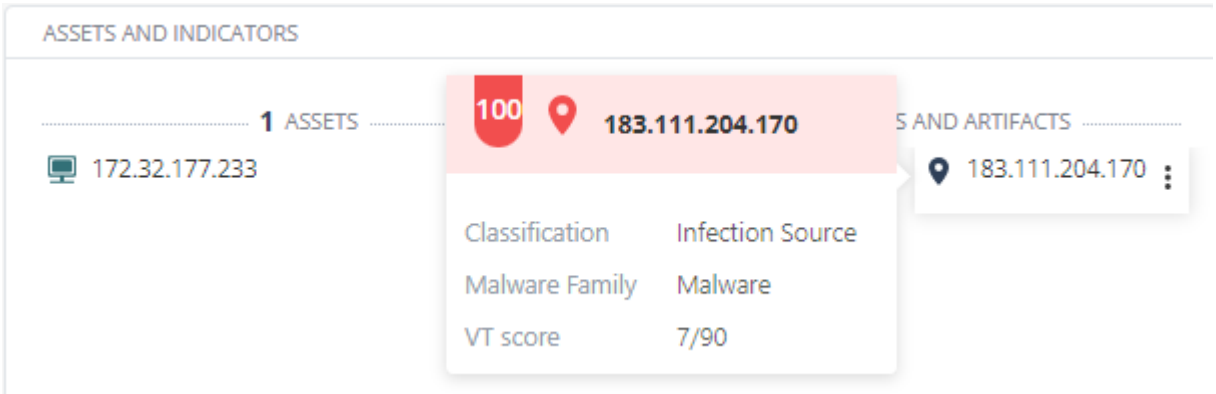
MITRE ATT&CK tactics and techniques involved in the incident. The numbers represent the number of insights related to each tactic.

Click **Open MITRE Tab** to open the *"Incidents - MITRE" on page 110* page.

Assets and Indicators

The **Assets and Indicators** widget shows:

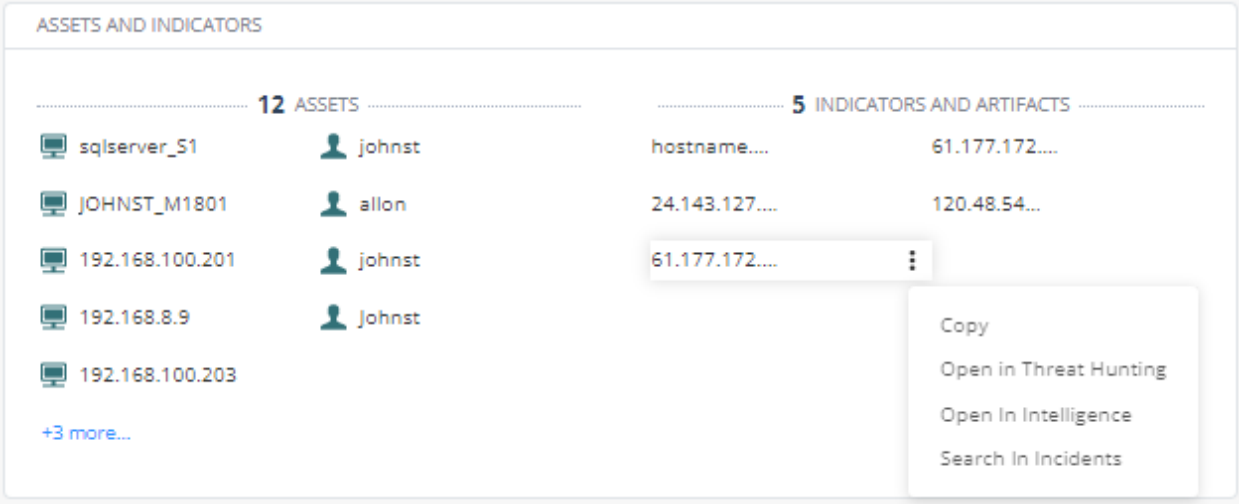
- Assets involved in the incident.
- Indicators and artifacts involved in the incident.



Hover over the indicator or artifact to view the risk level score (for example, 34), **Classification**, **Malware Family** and the **VT score**.

Managing Assets and Indicators

1. Click **Incidents**:
   a. Click the incident title.
   b. Hover over the incident and click **>**.
2. In the **Assets and Indicators** widget, hover over the asset, indicator or an artifact.



3. Hover over ⋮.
4. To copy an asset, indicator or artifact name to the clipboard, click **Copy**.

   XDR copies the name of the asset, indicator or the artifact to the clipboard.
5. To view forensic details related to the chosen asset, click **Open in Threat Hunting**.

   XDR opens the *"Threat Hunting" on page 165* page and shows the data for the asset, indicator or the artifact for the last seven days.

   Note - This option is not available for Mobile assets.
6. To view intelligence for an indicator or artifact, click **Open in Intelligence**.

   XDR opens the Intelligence page and shows the available intelligence for the asset, indicator or the artifact.

   Note - This option is not available for Mobile assets.
7. To search for asset, indicator or artifact in incidents, click **Search in Incidents**.

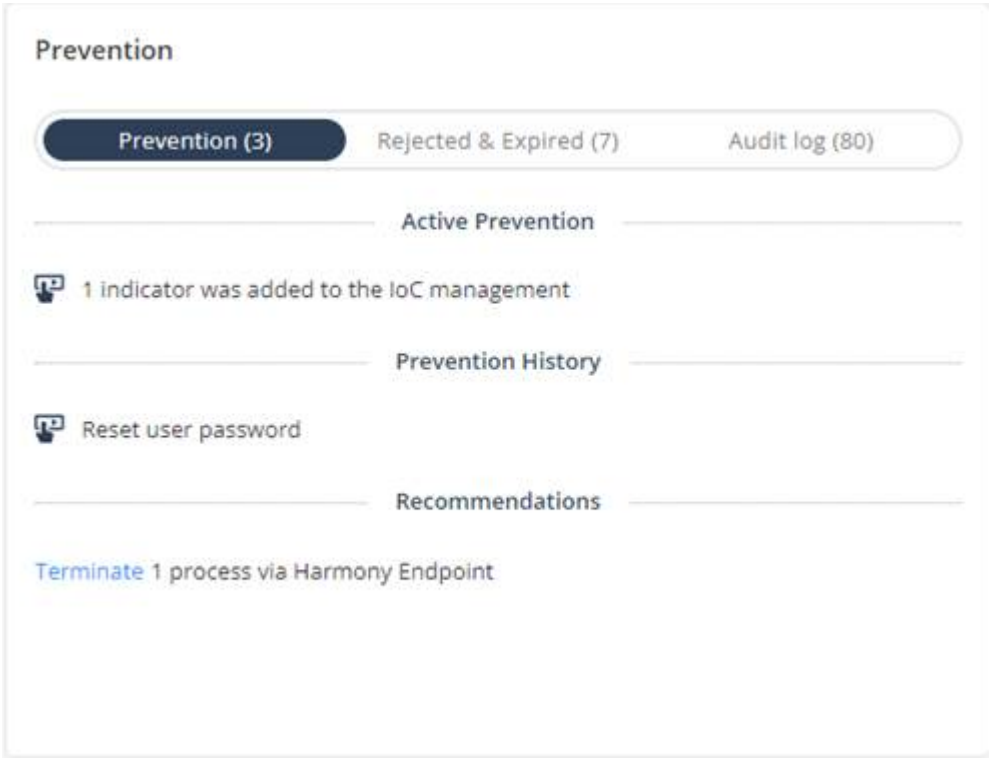
   XDR opens the *"Incidents" on page 57* page and shows the incidents with the searched asset, indicator or the artifact.

Note - This option is not available for Mobile assets.

Prevention

The **Prevention** widget shows preventive actions taken automatically or manually and that are recommended to remediate the incident:

Prevention



- **Active Prevention** - Preventive actions activated either manually or automatically. To revert the preventive action, click .

- **Prevention History** - Automatic ( ) and manual ( ) preventive actions taken.

Note - For more information on preventive actions that you can automate, see *"Automations" on page 232*.

- **Recommendations** - Preventive actions recommended by XDR to mitigate the incident. The available preventive actions include:
  - Enable IoCs in the IoC Management
  - Reset user password and revoke session in:
    - Okta
  - Isolate a machine in:
    - Endpoint Security
    - Microsoft 365 Defender for Endpoint
    - CrowdStrike Falcon
    - Trend Vision One for Endpoint
    - Singularity Endpoint
  - Quarantine a file in Endpoint Security and in Microsoft 365 Defender for Endpoint
  - Terminate a process in Endpoint Security.

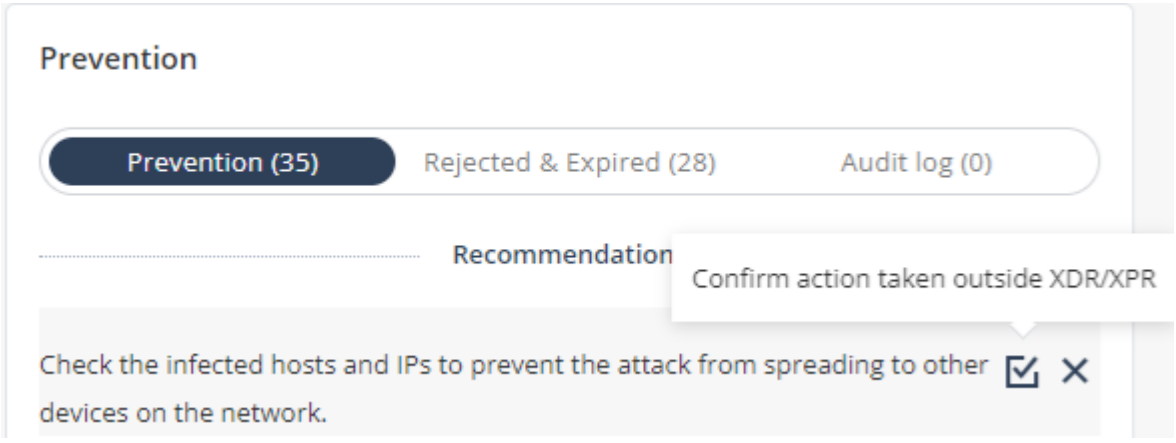
    For more information, see **Push Operations** in the *Endpoint Security EPMaaS Administration Guide*.
  - Isolate IP addresses (hosts) in the Quantum Security Gateway.

    This is implemented using Check Point Playblocks. For more information, see Infinity Playblocks Administration Guide.

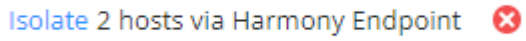
To enforce a preventive action, click the action. For example, click **Terminate**.

To reject a preventive action, click **X**. Rejected preventive actions are listed under *"Rejected & Expired" on page 73*.

A preventive action can also be an instruction that you should manually execute outside of XDR. After you execute the preventive action, click the checkbox across to indicate that the preventive action was executed.



A failed preventive action is indicated by .



To troubleshoot:

- For Endpoint Security, check whether the :
  - Endpoint Management Server is up and running.
  - Endpoint device is reachable.
- For Quantum Security Gateway, check whether the gateway is up and running.

Notes:

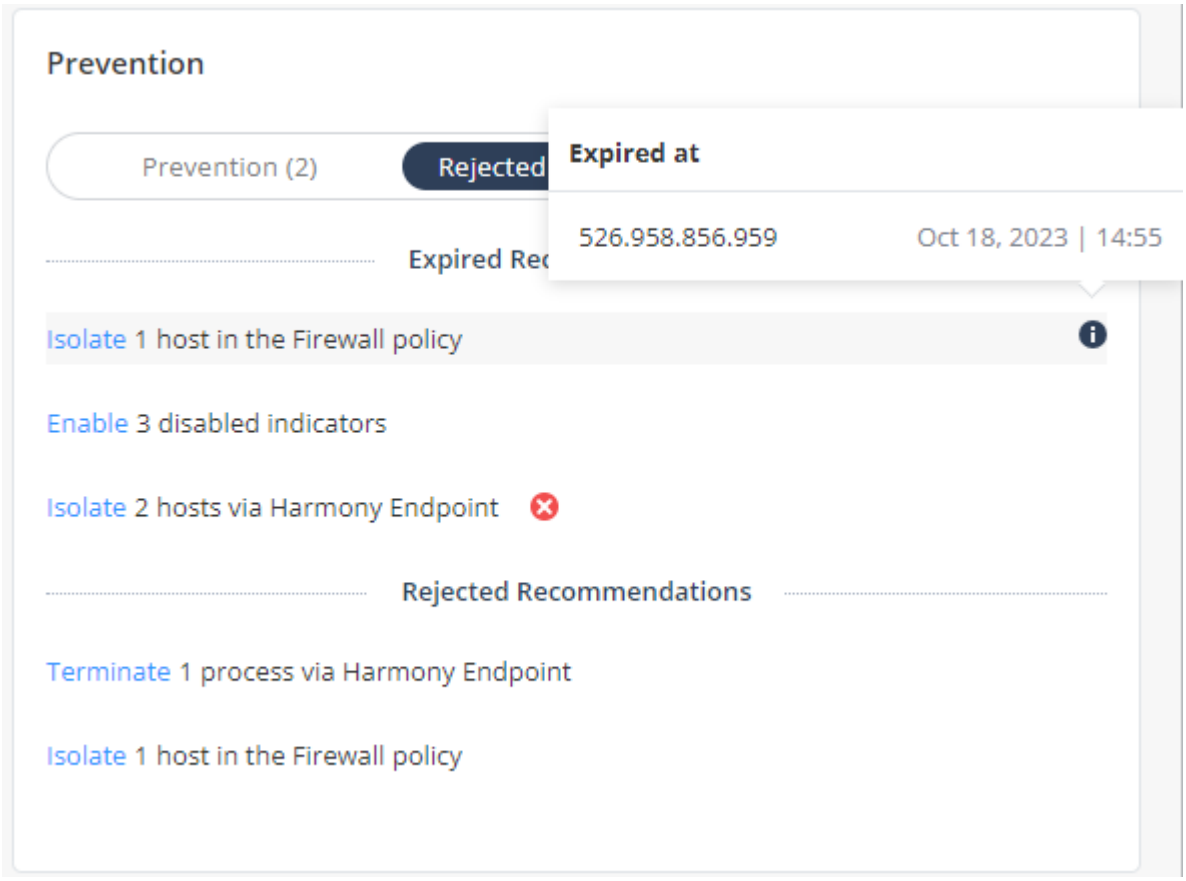
- Recommendations that are enforced will expire:

Preventive action	Expiry Duration
Related to IoC types **URL** and **File**	7 days
All other preventive actions	24 hours

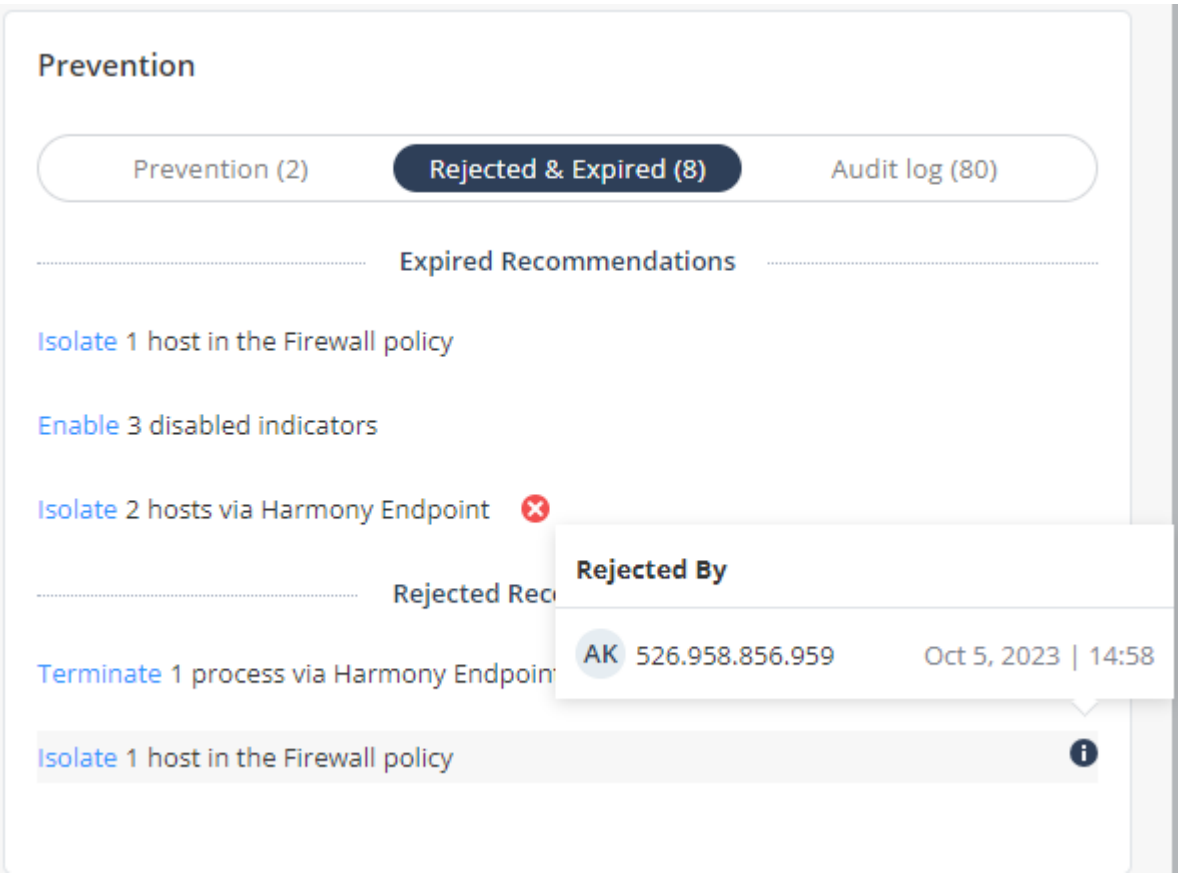
- Expired preventive actions are moved to the **Rejected & Expired** tab and are available for you to enforce the action.
- If the incident's reported activity continues and a new recommended preventive action is generated and if the same action already exists, then the expiry duration is extended by further 7 days or 24 hours based on the preventive action.

Rejected & Expired

- **Expired Recommendations** - Recommended preventive actions that are expired.



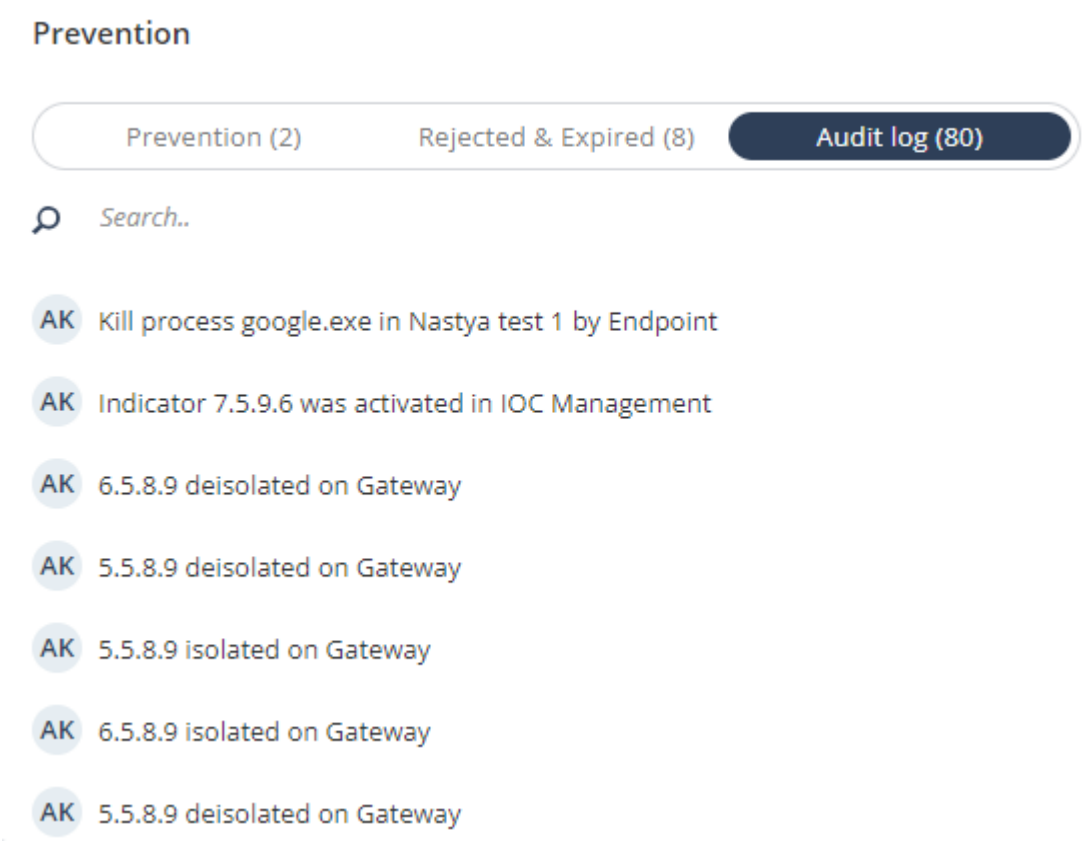
  - To know the expiration date and time, hover over the action.
  - To enforce the preventive action, click the action. For example, click **Isolate**. Enforced actions are moved either to the **Prevention**, **Active Prevention** or the **Prevention History** tab depending on the action type.
- **Rejected Recommendations** - Recommended preventive actions that are rejected by you.



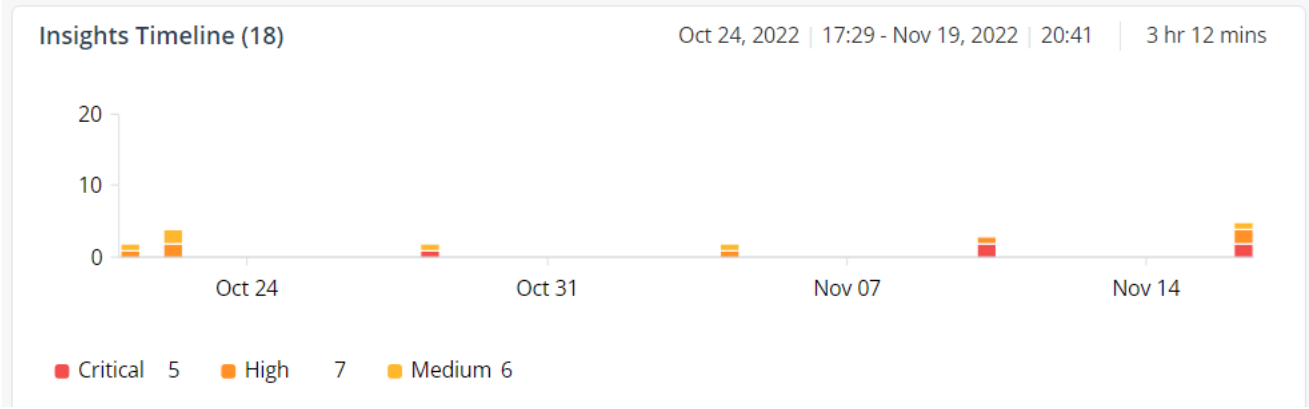
- To know the user that rejected the action, hover over the action.
- To enforce the preventive action, click the action. For example, click **Terminate**. Enforced actions are moved either to the **Prevention**, **Active Prevention** or the **Prevention History** tab depending on the action type.

Audit Log

Shows the audit log of all the activities related to preventive actions.



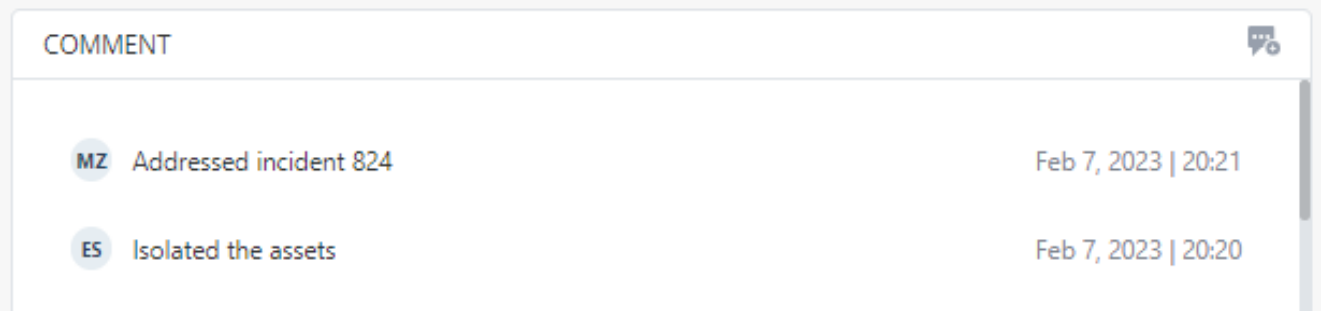
Insights Timeline



The **Insights Timeline** widget shows the:

- Timeline of insights color-coded according to their severity.
- Date and time when the first and last insight was created.
- Duration between the first and last insight.

Comments



The **Comments** widget shows the comments added by the SOC analysts to the incident.

Adding a Comment

1. Click **Incidents**:
   a. Click the incident title.
   b. Hover over the incident and click **>**.
2. In the **Comments** widget, click  .
3. Enter a comment (maximum 150 characters) and click **Save**.

Creating Advanced Exclusions from an Incident

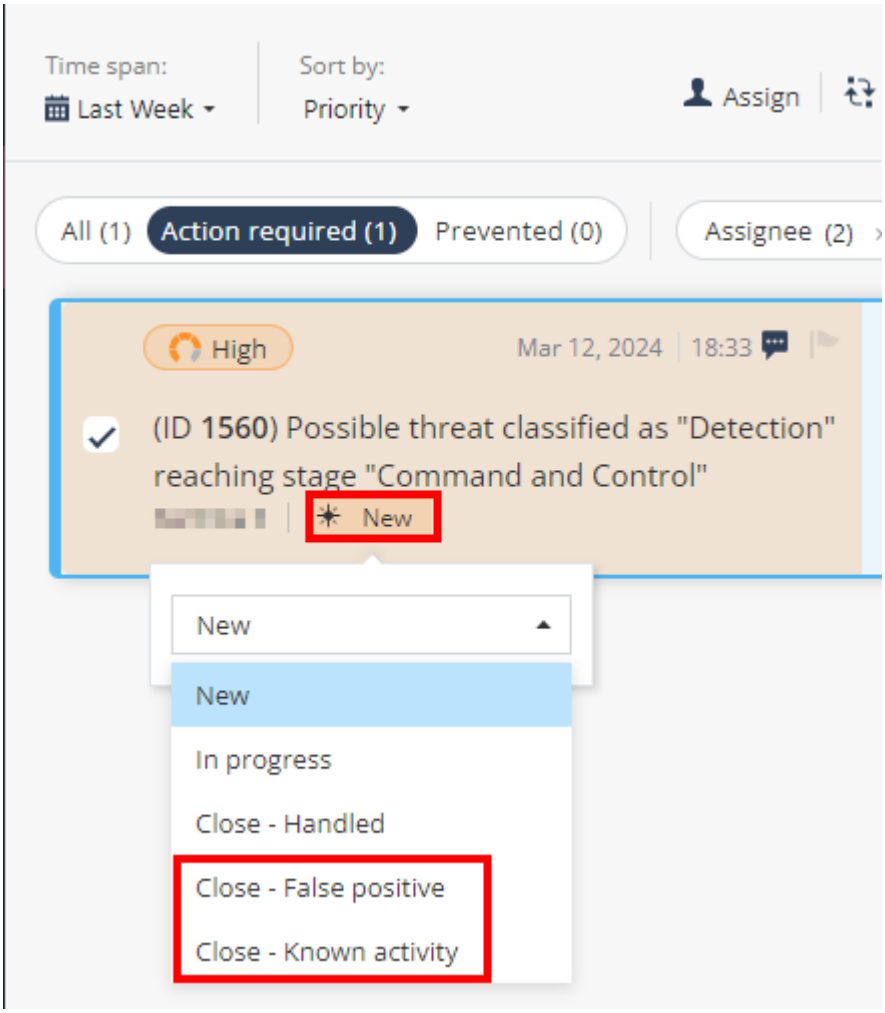
You can create advanced exclusions from incidents. XDR creates separate exclusions for each standalone insight.

Note - A standalone insight is a single, isolated security event detected only once by XDR.

To create an advanced exclusion for a standalone insight from an incident:

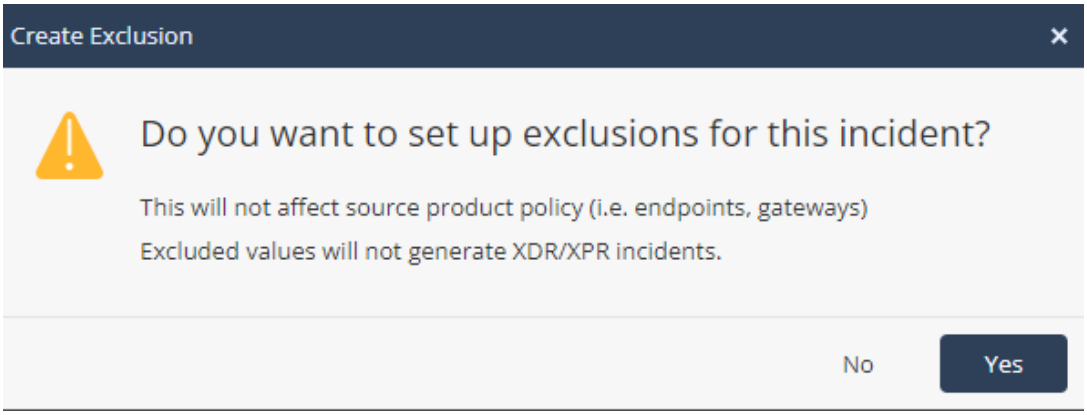
1. Go to **Incidents** page.
2. To create an advanced exclusion:

- When you close the incident:
  a. Select the incident you want to close and set the **Status** as one of these:
     - **Close - False positive**
     - **Close - Known Activity**



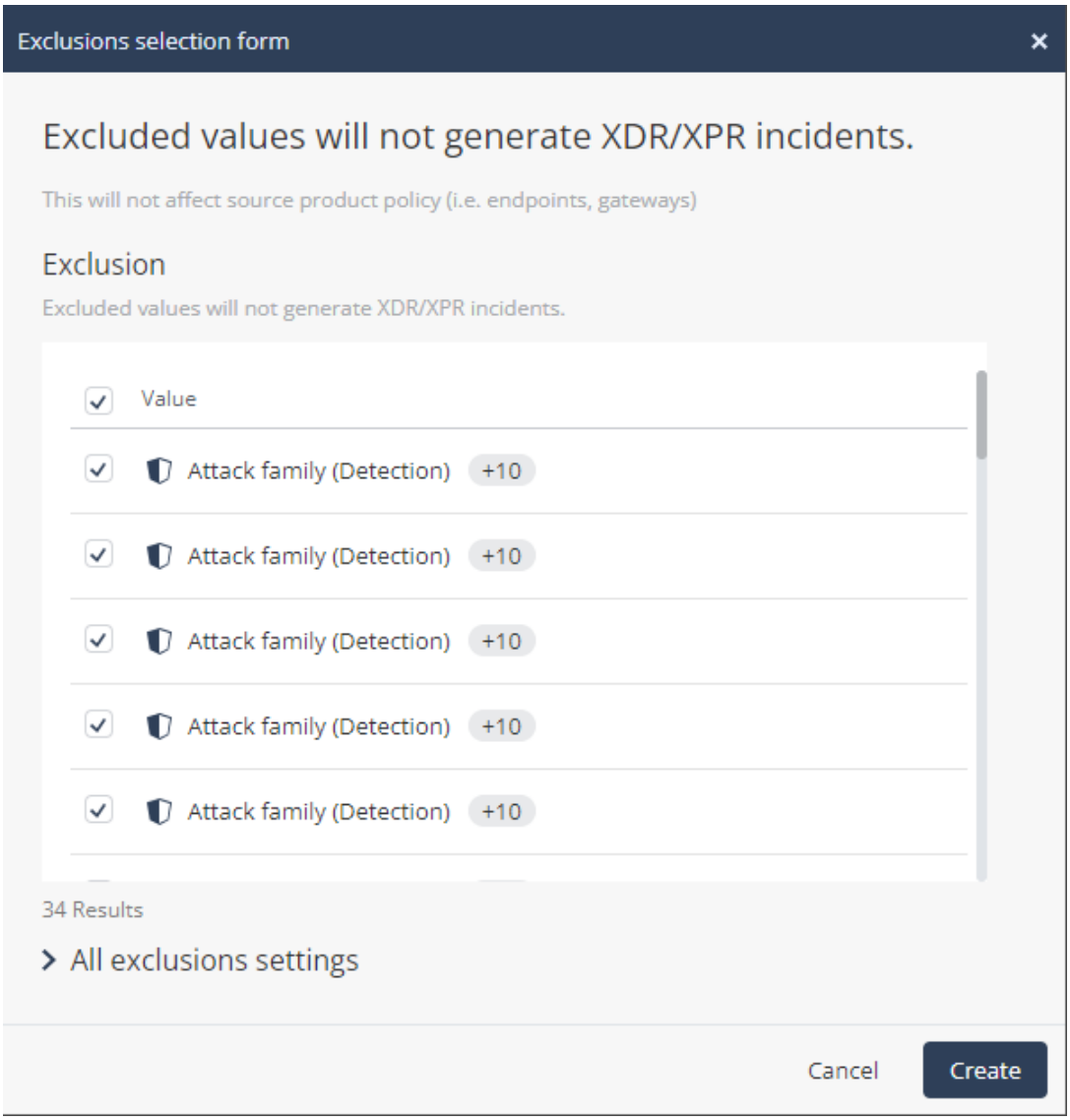
b. Add a comment and click **Save**.

The **Create Exclusion** pop-up window appears.

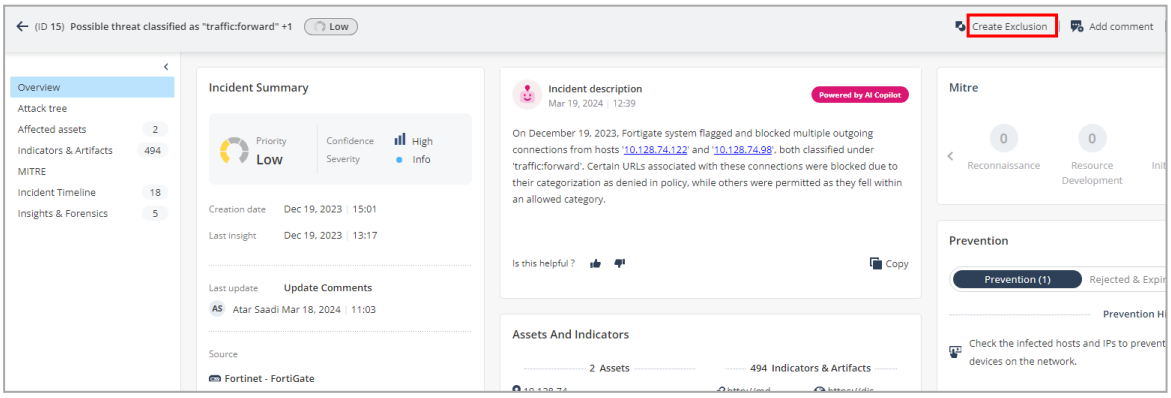


c. Click **Yes**.

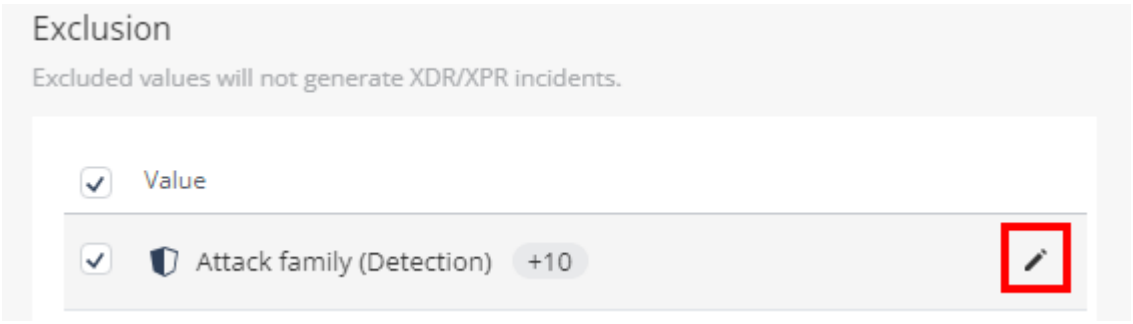
The **Exclusions selection form** window appears. It shows the fields of all the standalone insights for this incident. By default, all fields are selected.



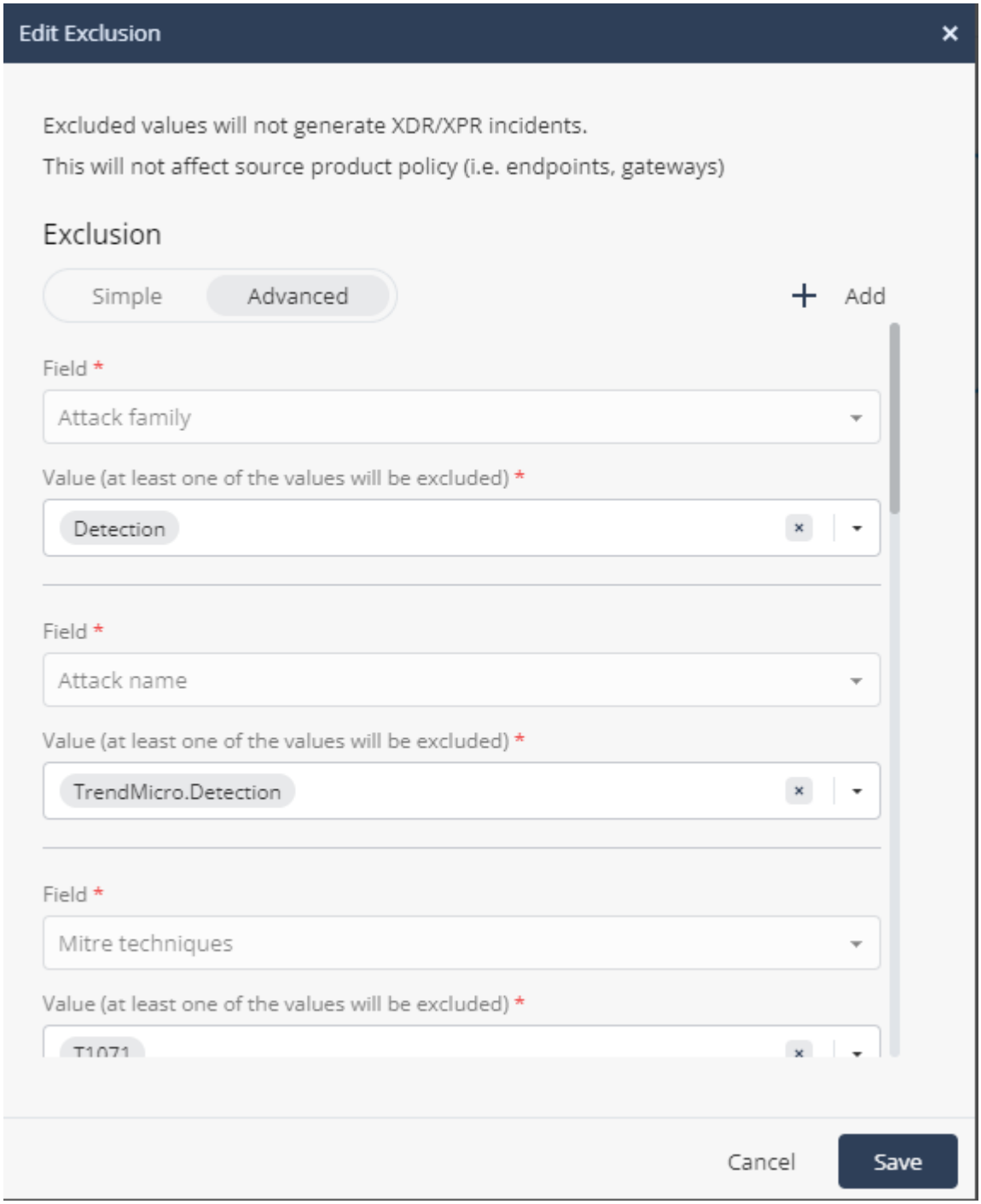
- From the **Overview** page, click **Create Exclusion**. The **Exclusions selection form** window appears.



3. In the **Exclusion** section, select the standalone insight fields to be excluded.
4. To edit a field, hover over it and click .



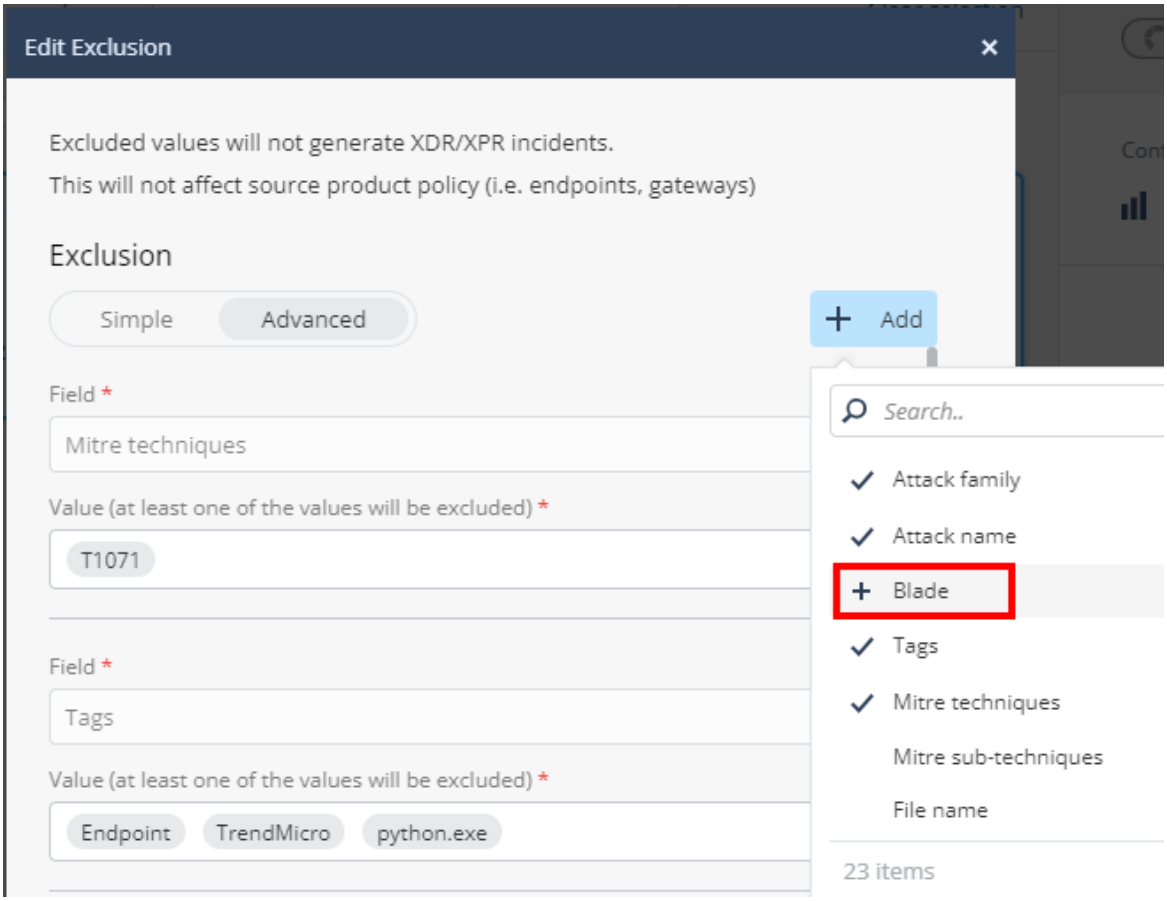
The **Edit Exclusion** window appears.



5. For each **Field**, edit the values as required. XDR applies this exclusion on insights that contain all the above fields and any of these values.

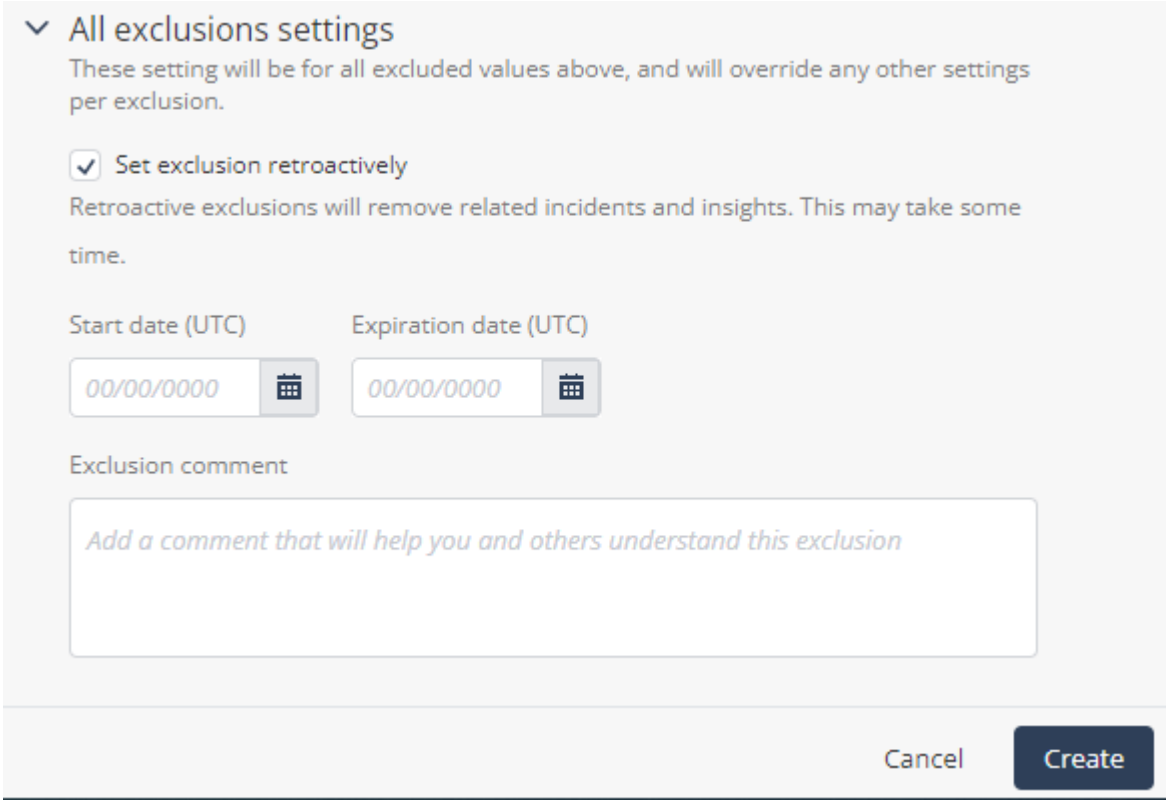
6. To add or remove a **Field**, click **+ Add**. The fields already selected are marked with ✓.

- To add, hover over the field name and click **+**.
- To remove a field, click the field name.



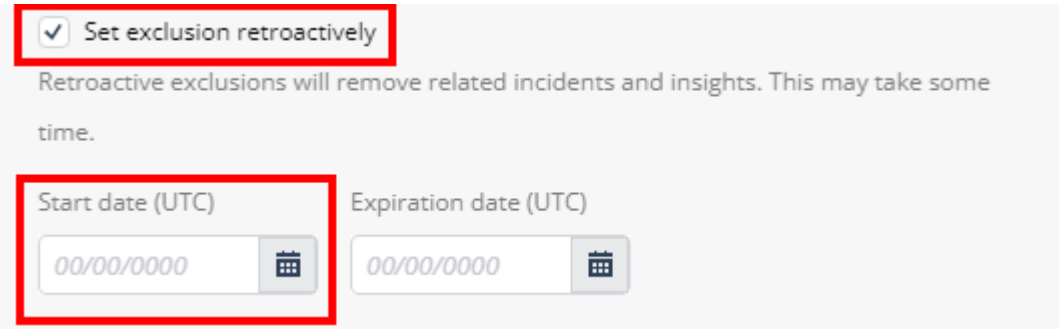
7. Click **Save**.
8. In the **All exclusion settings** section:

   Note - The values set in the **All exclusion settings** section is applied to all the above standalone insights' fields and overrides the values set for each insight field.



a. (Optional) To exclude the incidents already generated based on this insight:

   i. Select the **Set exclusion retroactively** checkbox.



   ii. In the **Start date (UTC)** field, select a date within the last 90 days. XDR excludes all the incidents that were generated from this date based on this insight. To revert the exclusion, see *"Reverting a Retroactive Exclusion" on page 241*.

b. (Optional) In the **Expiration date (UTC)** field, select an expiration date for the exclusion. After this date, XDR generates incidents for this insight. By default, there is no expiry date for an exclusion.

c. (Optional) In the **Exclusion comment** section, enter a description about the exclusion.

9. Click **Create**.

The exclusion is added to the **Exclusions** table in **Policy** > **Exclusions**. See *"Advanced Exclusions" on page 238*.

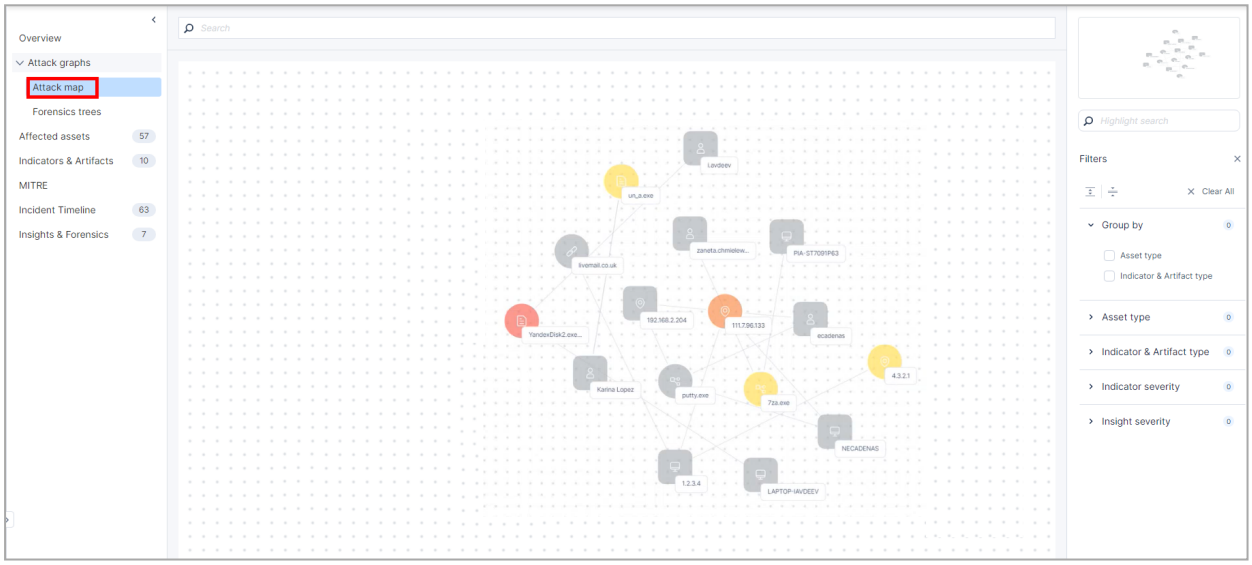
Attack graphs

Incidents - Attack Map

An **Attack map** shows the connections between assets and their associated artifacts and indicators in an incident.

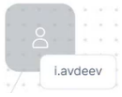
To view the Attack map of an incident:

1. Access the XDR Administrator Portal and click **Incidents** > **Incidents**.
2. Click the incident title or hover over the incident and click **>**.
3. Click **Attack graphs** > **Attack map**.



Reading an Attack Map

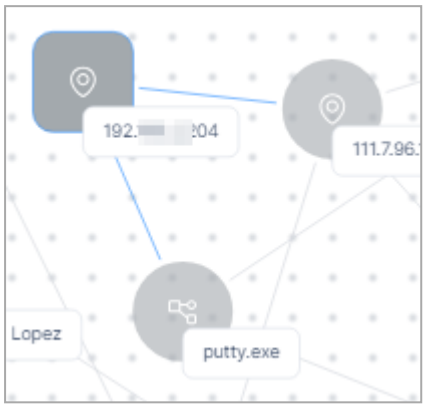
Legend

Item	Description
	Asset
	Artifact or Indicator **Note** - For artifacts, the color code indicates their severity.

To view the attack map of an asset:

1. Click the asset.

   The system highlights all the artifacts and indicators connected to the asset.

   You can drag and re-arrange the asset and the connected artifacts/indicators to view their connection in detail.

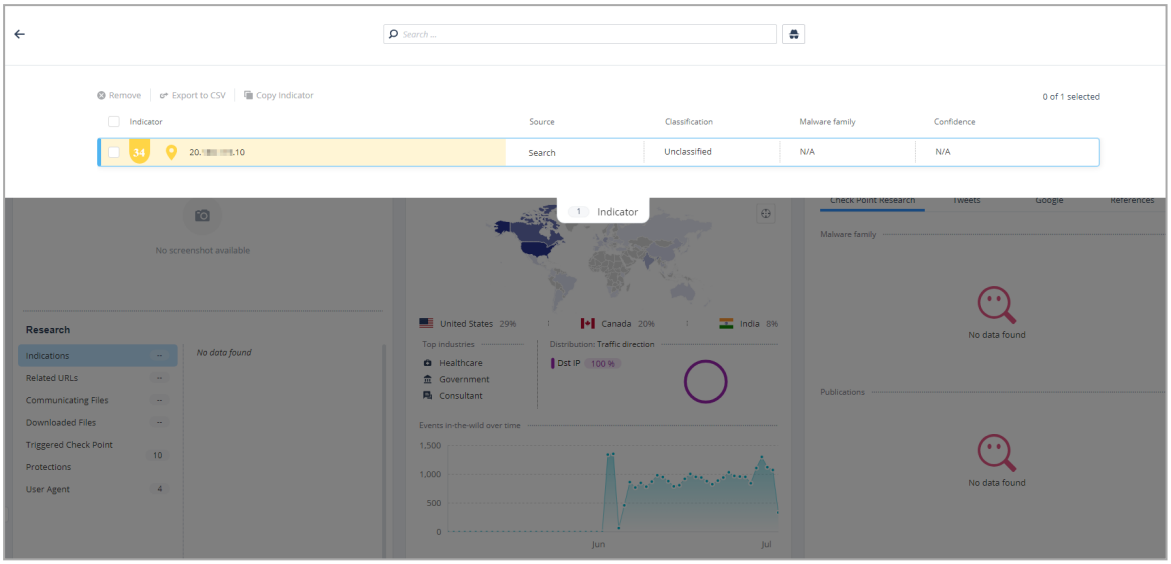
2. To view the artifact details, hover over it.

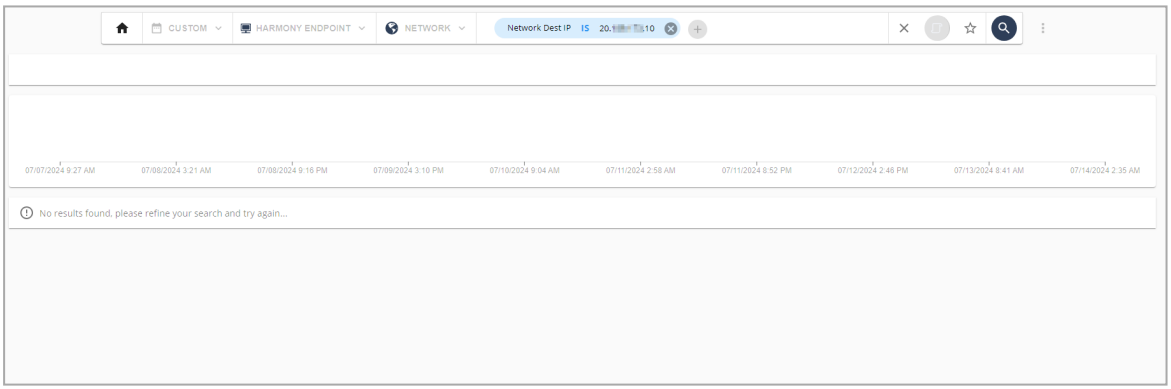
   The card shows:

   - Check Point reputation score of the artifact.
   - Threat classification of the artifact (when available)
   - Malware family of the artifact (when available)

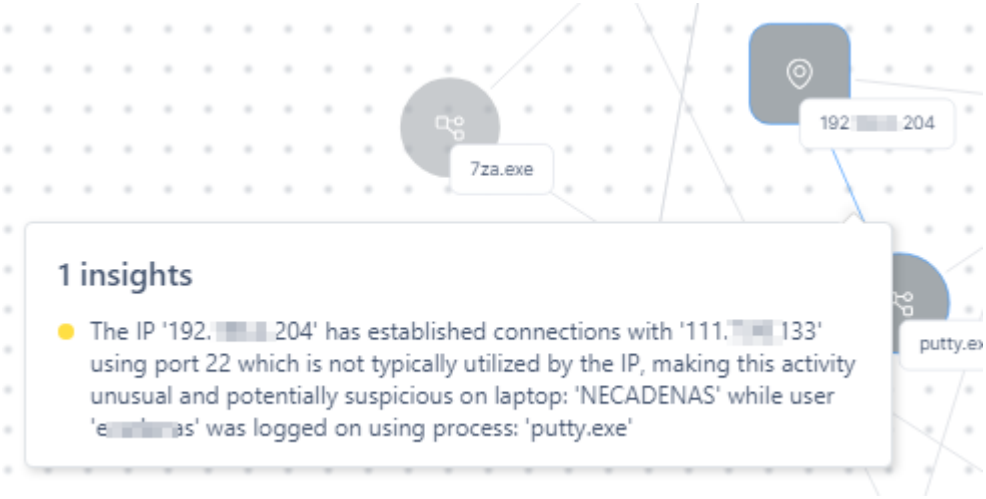
- To view the Intelligence information about the artifact, click **Intelligence**. The system opens the **Intelligence** page and shows the data filtered by the artifact's IP address.



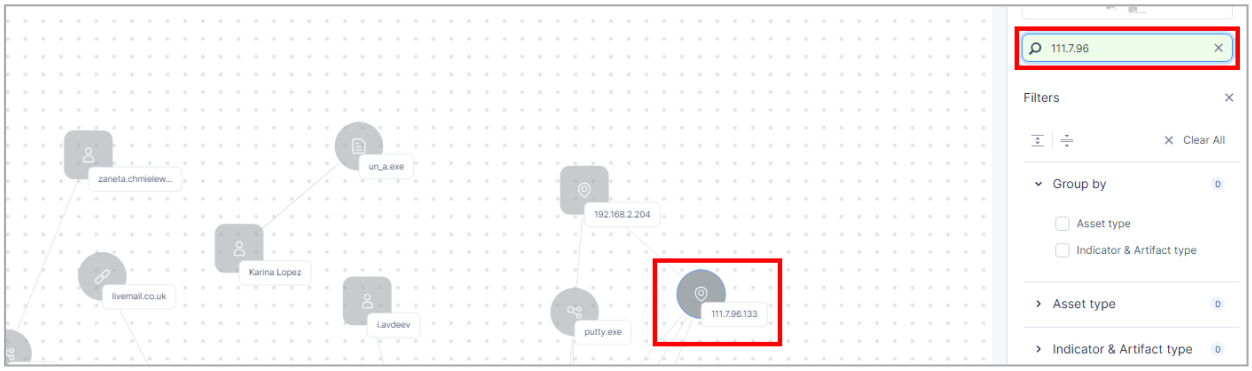
- To view the Threat Hunting information about the artifact, click **Threat hunting**. The system opens the **Threat Hunting** page and shows the data filtered by the artifact's IP address.



3. To view the insight summary of the connection, hover over the link.

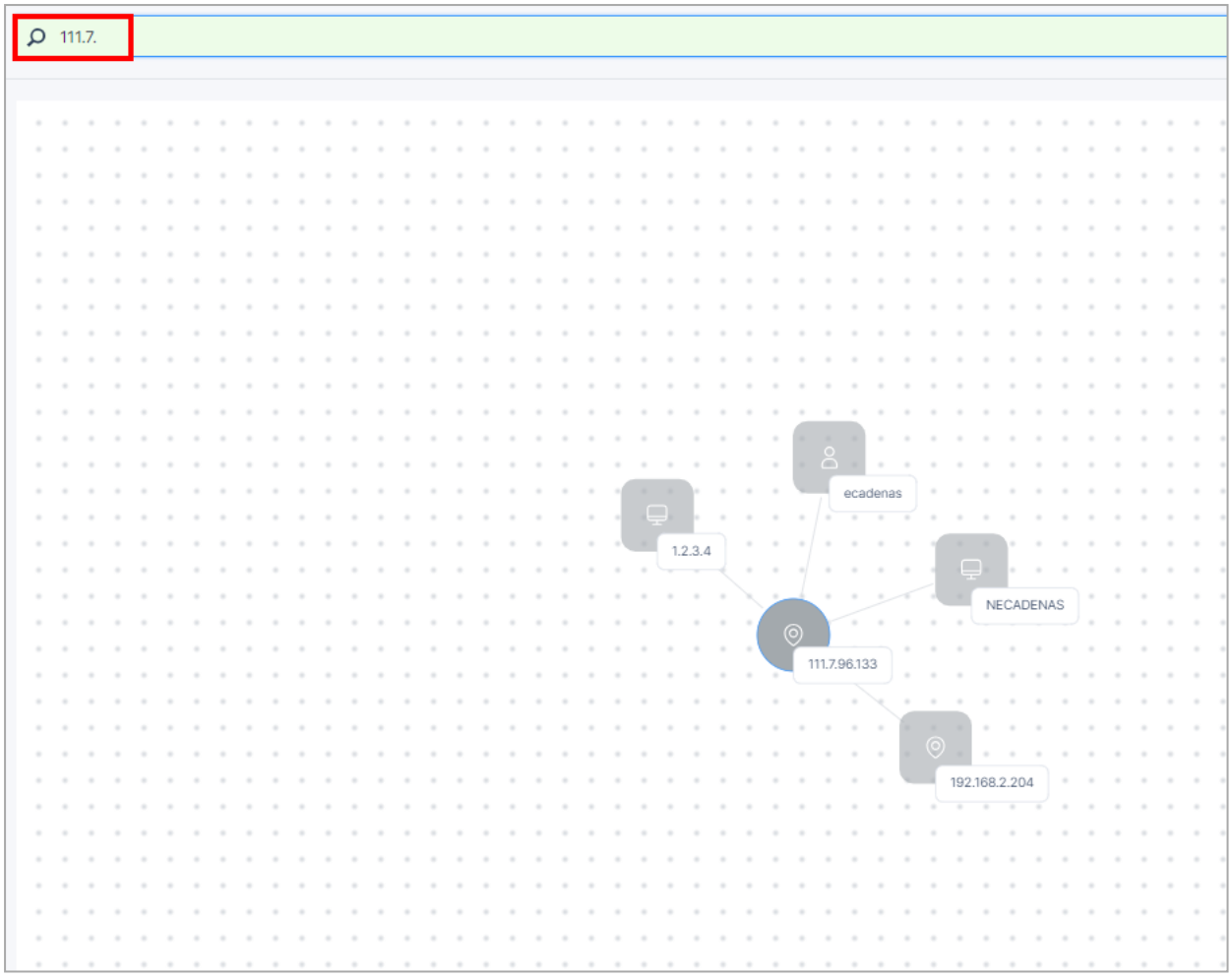


4. To find an asset, artifact or indicator on the attack map, on the right pane, in the **Highlight search** field, enter the value.

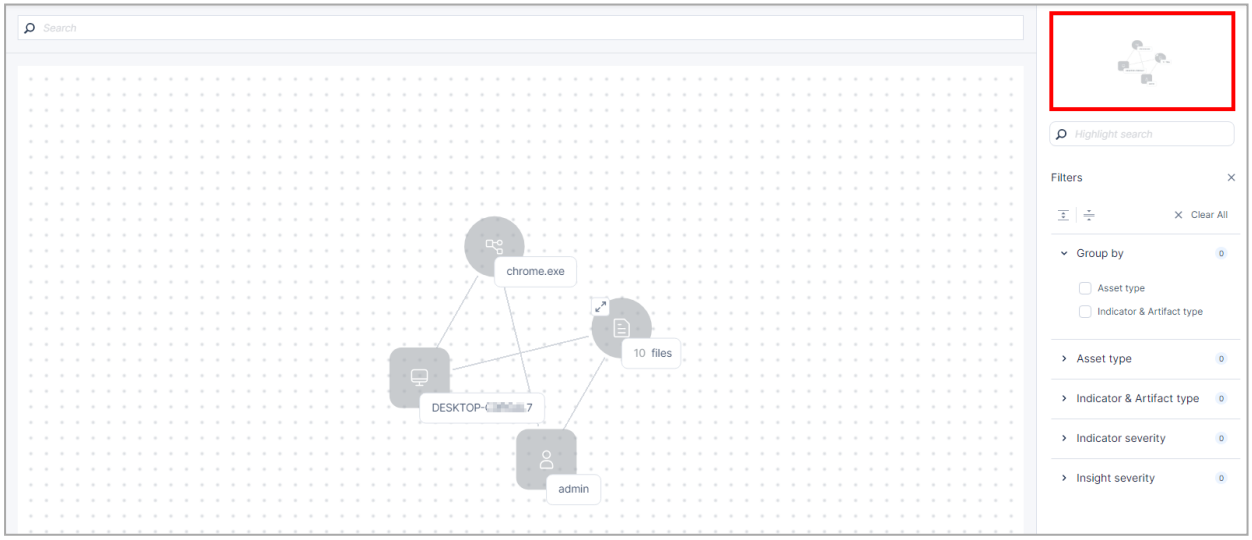


The system highlights the node on the map.

5. To search and view only the nodes connected to the searched value, enter the value in the **Search** field at the top.



6. To view a miniature version of the attack map, see the mini-map at the top-right corner.

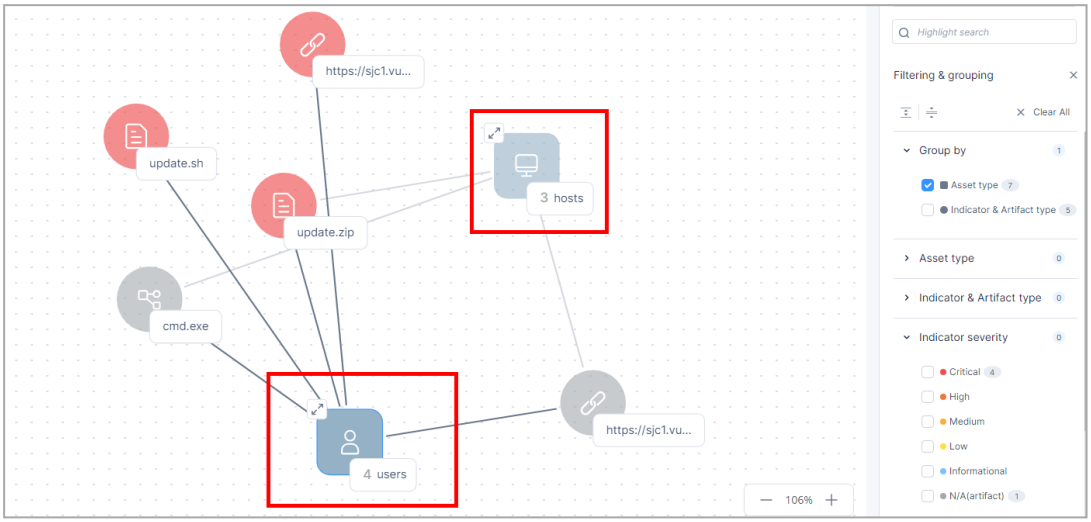


Filtering an Attack Map

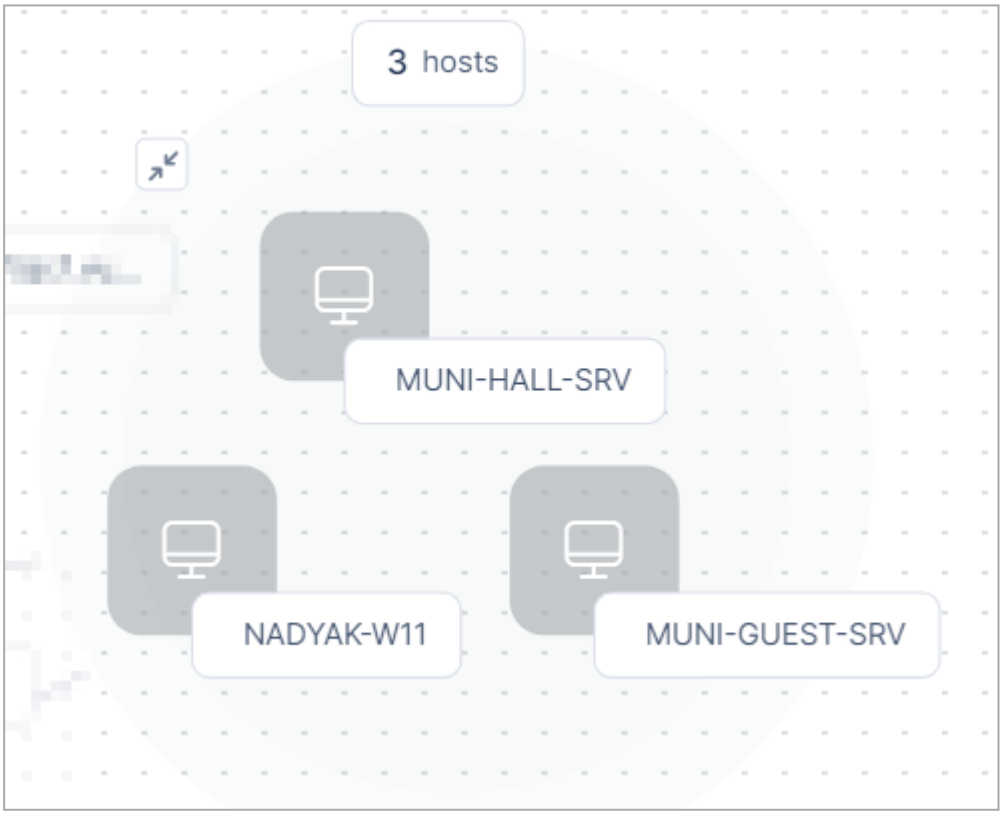
You can filter an Attack map by:

- Groups
  - **By Asset type**:
    a. In the **Group by** section, select the **Asset type** checkbox.

    The system shows the attack map grouped by asset type.



    b. To view the assets in a group, click the ⤢ icon or the grouped node.

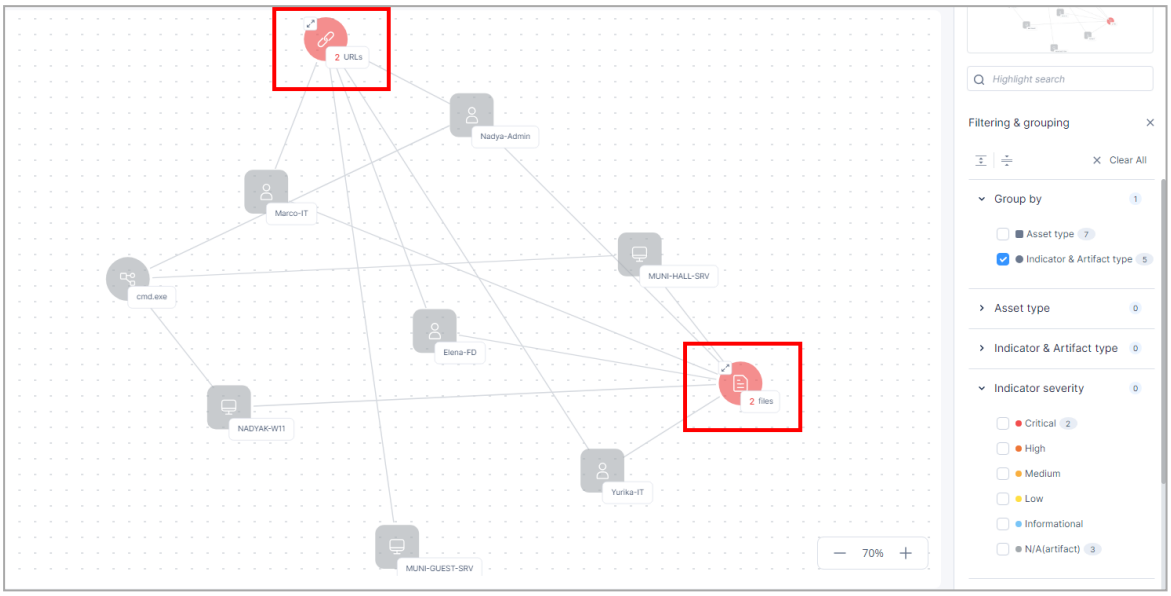


    c. To go back to the grouped view, click ⤡ or click anywhere within the group.

- **By Indicators and Artifacts type**:

  In the **Group by** section, select the **Indicator & Artifact type** checkbox.

  The system shows the attack map grouped by indicator/artifact type.



- Asset type
  - Machine
  - User
  - IP Address
- Indicator and Artifact type
  - Registry
  - Process
  - URL
  - IP Address
  - File
- Indicator severity
  - Critical
  - High
  - Medium
  - Low

    - Informational
    - N/A (artifact)
- Insight severity
    - Critical
    - High
    - Medium
    - Low
    - Informational

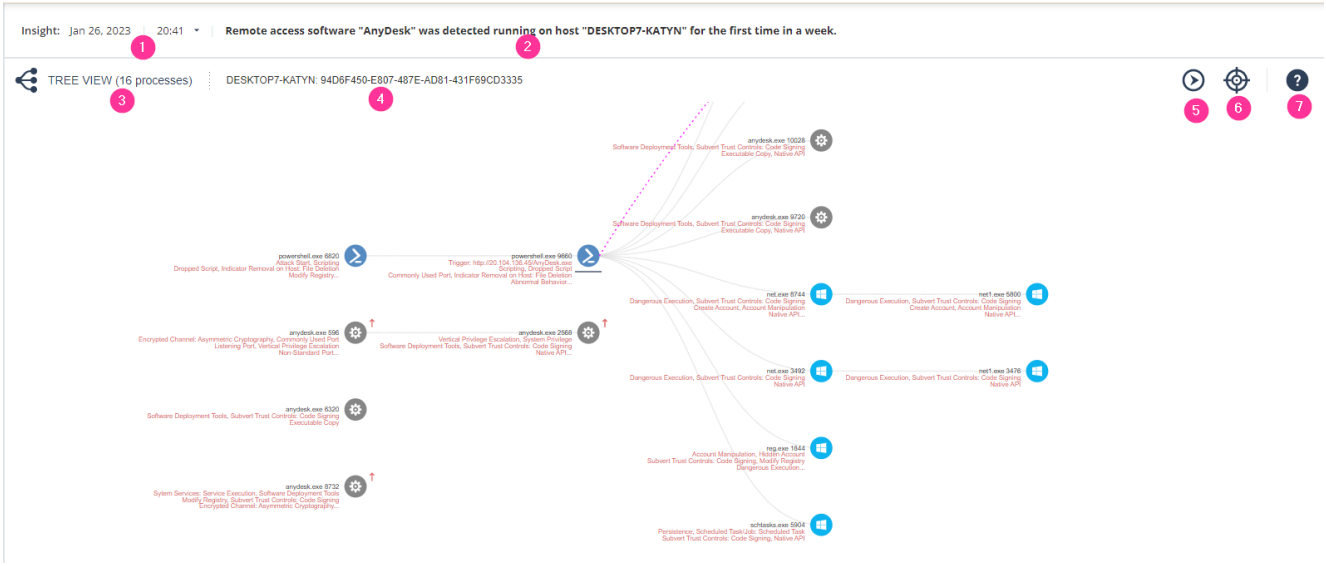
Incidents - Forensics Trees

The **Forensics trees** shows a graphical representation of the forensic report generated by Endpoint Security for each detection in an insight.

Note - An insight can contain zero or multiple forensic trees.

To view the **Forensics Tree** page:

1. Access XDR and click **Incidents** > **Incidents**.
2. Click the incident title or hover over the incident and click **>**.
3. Click **Attack graphs** > **Forensics trees**.



Legend	Description
1	Date and time when the insight was generated. Click to view the insights and forensics trees available for the incident. Click the forensics tree to view its graphical representation.
2	Insight summary.
3	Process involved in the insight.
4	Asset involved in the insight.
5	Goes to that start of the tree.
6	Goes through the processes in the tree.
7	Opens the graph legends.

Incidents - Affected Assets

The **Affected Assets** page displays the assets involved in the incident, with a separate tab for each of the asset types. The label on the tab indicates the number of assets in that type.

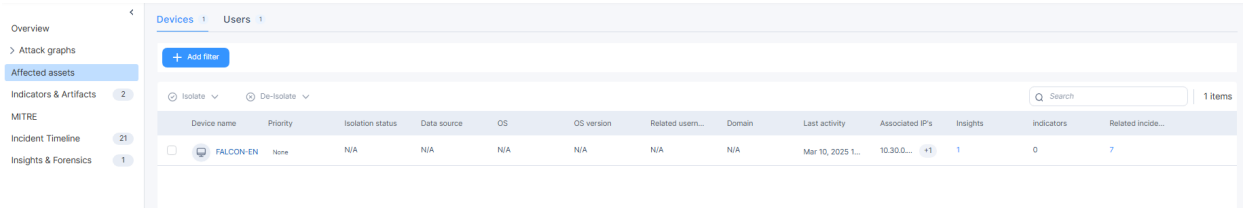
The asset types include:

- *"Devices" below*
- *"Users" on page 97*
- *"Mobile" on page 99*

Note - The tab for mobile assets is displayed only if there are mobile assets present in the incident.

To view the Affected Assets page:

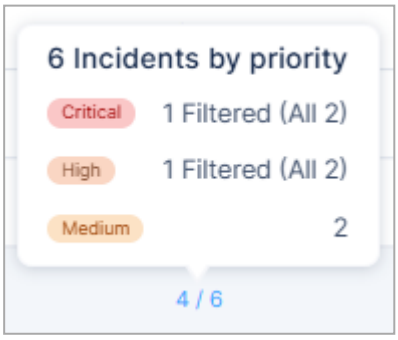
1. Access XDR and click **Incidents** > **Incidents**.
2. Click the incident title or hover over the incident and click **>**.
3. Click **Affected assets**.



Devices

The **Devices** tab displays information about the device assets involved in the incident.

Item	Description
Device name	Name of the device. ■ To view more information about the device, click the name. The *"Devices" on page 152* page appears. ■ For more actions, hover over the device name and click the ⋮ icon. You can: ○ Filter the table by including or excluding the device name. ○ View the device details in Threat Hunting.
Priority	Priority level of the associated incident. For more actions, hover over the priority and click the ⋮ icon. You can filter the table by including or excluding the specific priority level.

Item	Description
Isolation status	Isolation status of the device. Applies only to devices with Endpoint Security Security Client installed.
Data source	Security product that detected the device.
OS	Operating System on the device.
OS version	Operating System version.
Related usernames	Users who have used the device.
Domain	Domains accessed on the device.
Last activity	Time stamp of last activity on the device.
Associated IPs	IP addresses associated with the device.
Insights	Number of insights related to the incident in which the device is involved. Hover over the count to view the insights by severity. To view the insight details, click the count. The *"Incidents - Insights & Forensics" on page 113* page appears.
Indicators	Number of indicators related to the incident in which the device is involved.
Related incidents	Number of incidents in which the device is involved. Hover over the count to view the number of the filtered incidents (if applicable) and the total number of incidents. **Note** - Some incidents that impact a large number of assets are excluded from determining the Incident Priority. Such incidents are considered as **Filtered**.  To view the incidents details, click the count. The *"Incidents" on page 57* page appears.
Security agent	Security agent running on the device.

Managing Affected Devices

1. Click **Incidents**:
   - Click the incident title.
   - Hover over the incident and click **>**.
2. Click **Affected assets**.
3. Click the **Devices** tab.
4. To copy the device name, hover over at the end of the row, click ⋮ and then click **Copy asset name**.

   XDR copies the name of the device to the clipboard.
5. To view Threat Hunting for a device, hover over at the end of the row, click ⋮ and then click **Open in Threat Hunting**.

   XDR opens the *"Threat Hunting" on page 165* page searching for the chosen device in the logs from the past seven days.
6. To create an exclusion for the device, hover over at the end of the row, click ⋮ and then click **Create Exclusion**. For more information, see *"Creating an Exclusion for Devices from an Incident" on the next page*.
7. To search, in the **Search** field, enter the string. The table automatically filters and shows the content that matches with the string.
8. To isolate a device from the network, select the device and at the top of the page, click **Isolate** and then click **Isolate on Endpoint**. In the confirmation message appears, click **Yes**.

   XDR enforces isolation through Endpoint Security's **Isolate Computer** push operation.
9. To isolate a device of the type IP address on the Quantum Security Gateway, at the top of the page, click **Isolate** and then click **Isolate on Gateway**. In the confirmation message that appears, click **Yes**.
10. To de-isolate an isolated device from the network, select the device and at the top of the page, click **De-Isolate** and then click **De-Isolate on Endpoint**. In the confirmation message appears, click **Yes**.

    XDR enforces isolation through Endpoint Security's **Isolate Computer** push operation.
11. To view intelligence for an IP address, hover over at the end of the row, click ⋮ and then click **Open in Intelligence**.

    XDR opens the Intelligence page and shows the available intelligence for the IP address.

Note - This applies only to devices of type IP address.

12. To isolate an IP address on the Quantum Security Gateway, hover over at the end of the row, click ⋮ and then click **Isolate on GW**.

    A confirmation message appears. Click **Yes**.

    Notes:
    - This applies only to assets of type IP address.
    - This is implemented using Check Point Playblocks. For more information, see Infinity Playblocks Administration Guide.

Creating an Exclusion for Devices from an Incident

You can create exclusions for devices so that they do not create new incidents. For example, an asset that represents an approved network scanner.

Note - You can also create exclusions from the **Policy** menu. See *"Exclusions" on page 236*.

To create an exclusion for devices from an incident:

1. Click **Incidents**:
   - Click the incident title.
   - Hover over the incident and click **>**.
2. Click **Affected assets** and select the **Devices** tab.
3. In the table, at the end of the row, hover over ⋮ for the device, and click **Create Exclusion**.

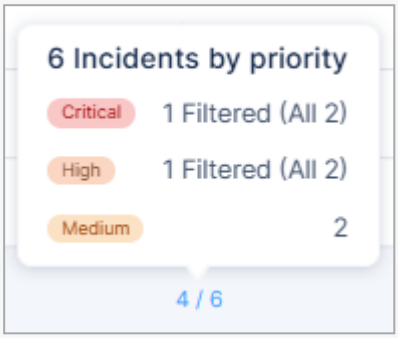
   The **New Exclusion** window appears.

   The **Field** and **Value** are pre-filled.
4. (Optional) In the **Expiration date (UTC)** field, set an expiration date for the exclusion. After the expiration date, the asset can create incidents.
5. (Optional) In the **Exclusion comment** field, enter a comment about the exclusion.
6. Click **Create**.

Users

The **Users** tab displays information about the user assets involved in the incident.

Item	Description
User name	Name of the user in the events and alerts processed by XDR. ■ To view more information about the user, click the name. The *"Users" on page 139* page appears. ■ For more actions, hover over the user name and click the ⋮ icon. You can: ◦ Filter the table by including or excluding the user name. ◦ View the user details in Threat Hunting.
Full name	Full name of the user.
Priority	Priority level of the associated incident. For more actions, hover over the priority and click the ⋮ icon. You can filter the table by including or excluding the specific priority level.
Email addresses	Email address(es) of the user.
Related devices	Devices used by the user.
Domain	Domain(s) accessed by the user.
Last activity	Time stamp of last activity by the user.
Insights	Number of insights related to the incident in which the user is involved. Hover over the count to view the insights by severity. To view the insight details, click the count. The *"Incidents - Insights & Forensics" on page 113* page appears.
Indicators	Number of indicators related to the incident in which the user is involved.

Item	Description
Related incidents	Number of incidents in which the user is involved. Hover over the count to view the number of the filtered incidents (if applicable) and the total number of incidents. **Note** - Some incidents that impact a large number of assets are excluded from determining the Incident Priority. Such incidents are considered as **Filtered**.  To view the incidents details, click the count. The *"Incidents" on page 57* page appears.

Managing Affected Users

1. Click **Incidents**:
   - Click the incident title.
   - Hover over the incident and click **>**.
2. Click **Affected assets**.
3. Click the **Users** tab.
4. To copy the username, hover over at the end of the row, click ⋮ and then click **Copy asset name**.

   XDR copies the username to the clipboard.
5. To view Threat Hunting for a user, hover over at the end of the row, click ⋮ and then click **Open in Threat Hunting**.

   XDR opens the *"Threat Hunting" on page 165* page searching for the chosen user in the logs from the past seven days.
6. To search, in the **Search** field, enter the string. The table automatically filters and shows the content that matches with the string.

Mobile

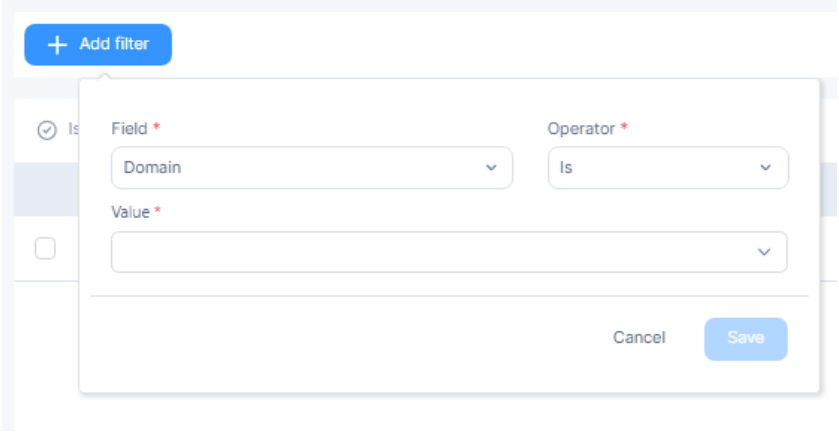
The **Mobile** tab displays information about the mobile device assets involved in the incident.

Item	Description
Status	Status of the mobile device.
Device model	Mobile device model.
Phone number	Phone number of the mobile device.
Email	Email address of the mobile device user.
Device type	Mobile device OS type: ■ iOS ■ Android
OS version	Operating system version on the device.
Name	Name of the mobile device.

Adding Filters

To add a new filter:

1. Click **+ Add Filter**.



2. Enter these details:
   a. **Field** - Select the device/user field.
   b. **Operator** - Select the operator to be applied.
   c. **Value** - Select the value of the device/user field.

3. Click **Save**.

   Note - You can add multiple filters.

   The system updates the table based on all the active filters.

Incidents - Indicators & Artifacts

The **Indicators & Artifacts** page shows the indicators and artifacts in the incident.

An artifact of an incident is a domain, URL, IP address or a file affected in the incident. An indicator is a malicious artifact. For example, an artifact is a legitimate file involved in an incident and an indicator is a malicious domain.

You can use the **Indicators & Artifacts** page to perform these actions:

- *"Managing Indicators and Artifacts" on page 104*
  - Copying an Indicator or an Artifact Value to Clipboard
  - Copying HASH of an Indicator to Clipboard
  - Viewing Intelligence for an Indicator or Artifact
  - Viewing Threat Hunting for an Indicator or Artifact
- *"Creating an Exclusion for Artifacts and Indicators from an Incident" on page 105*
- *"Adding or Editing an Indicator or Artifact in IoC Management" on page 107*
- *"Removing an Indicator from IoC Management" on page 109*

To view the **Indicators & Artifacts** page:

1. Access XDR and click **Incidents** > **Incidents**.
2. Click the incident title or hover over the incident and click **>**.
3. Click **Indicators & Artifacts**.

   To edit the columns in the table, click **Edit columns** and select the columns.

   To export the data to an excel in CSV format, click **Export All (CSV)**.

   To search, in the **Search** field, enter the string. The table automatically filters and shows the content that matches with the string.

The **Indicators & Artifacts** tab shows a list of all indicators and artifacts involved in the incident. The **Domains**, **URL**, **IP Address** and **Files** tabs offer a drill-down view into their respective type and their related information:

Column	Description	Indicators & Artifacts	Domains	URL	IP Address	Files
Type	Indicator or an artifact.	✓	✓	✓	✓	✓
Value	Value of the indicator or artifact.	✓	✓	✓	✓	✓
Status IOC Mgmt	Indicates whether the indicator was enabled or disabled in the IoC management.	✓	✓	✓	✓	✓
XDR Confidence	Confidence level of the indicator, calculated by XDR.	✓	✓	✓	✓	✓
XDR Severity	Severity level of the indicator, calculated by XDR.	✓	✓	✓	✓	✓
Classification	Threat classification of the indicator. For example, Malware or Benign.	✓	✓	✓	✓	✓
Malware Family	The malware family associated with the indicator. For example, Invader.	✓	✓	✓	✓	✓
VT Score	VirusTotal score reported by virustotal.com.	✓	✓	✓	✓	✓

Column	Description	Indicators & Artifacts	Domains	URL	IP Address	Files
Related Assets	Assets related to the indicator or artifact.	✓	✓	✓	✓	✓
Related Incidents	Incidents related to the indicator or artifact.	✓	✓	✓	✓	✓
Global Top country	Top country where the indicator was seen in the Check Point telemetry.	✓	✓	✓	✓	✓
Global Top industry	Top industry where the indicator was seen in the Check Point telemetry.	✓	✓	✓	✓	✓
Registrar name	Name of the registrar.	–	✓	✓	–	–
Country	Country where the IP address is registered.	–	–	–	✓	–
Owner	Organization to which the IP address is registered.	–	–	–	✓	–
IP abuse	Confidence of abuse reported by abuseipdb.com.	–	–	–	✓	–
File type	Type of file.	–	–	–	–	✓
File size	Size of the file.	–	–	–	–	✓

Column	Description	Indicators & Artifacts	Domains	URL	IP Address	Files
Signer	Authority that signed the certificate of the file.	⊖	⊖	⊖	⊖	✓
Additional file names	Other known names seen for the file's hash in the on-boarded product logs.	⊖	⊖	⊖	⊖	✓
File path	Path of the file.	⊖	⊖	⊖	⊖	✓
File origin	Source application of the file.	⊖	⊖	⊖	⊖	✓
Threat Emulation report	Download the Threat Emulation report for the file.	⊖	⊖	⊖	⊖	✓

Managing Indicators and Artifacts

Copying an Indicator or an Artifact Value to the clipboard:

1. Click **Incidents**:
   - Click the incident title.
   - Hover over the incident and click **>**.
2. Click **Indicators & Artifacts**.
3. At the end of the row, hover over ⋮.
4. To copy the indicator or artifact (of the type file) file name, click **Copy file name**.

   XDR copies the file name to the clipboard.
5. To copy the indicator or artifact value, click **Copy value**.

   XDR copies the value to the clipboard.
6. To copy the indicator or artifact (of the type file) file name, click **Copy HASH**.

XDR copies the HASH of the file to the clipboard.

7. To view the intelligence for indicators or artifacts, and click **Open in Intelligence** at the top of the table. You can select up to 20 indicators or artifacts.

   XDR opens the *"Intelligence" on page 210* page and shows the available intelligence for the indicator or artifact.

8. To view Threat Hunting for an indicator or artifact, click **Open in Threat Hunting**

   XDR opens the *"Threat Hunting" on page 165* page and shows the data for the indicator or artifact.

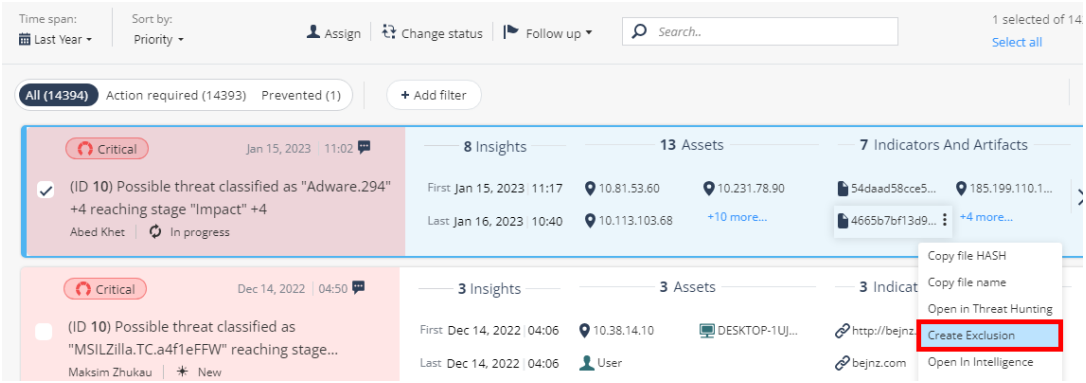
Creating an Exclusion for Artifacts and Indicators from an Incident

You can create exclusions for artifacts and indicators so that they are not added to the existing incidents and do not create new incidents.

Note - You can also create exclusions from the **Policy** menu. See *"Exclusions" on page 236*.

To create an exclusion for an indicator or artifact from an incident:

1. Go the **Incidents** page.
2. To create an exclusion:
   - From the **Incidents** main page:
     a. In the **Indicators and Artifacts** section, hover over the indicator or artifact and click ⋮.
     b. Click **Create Exclusion**.



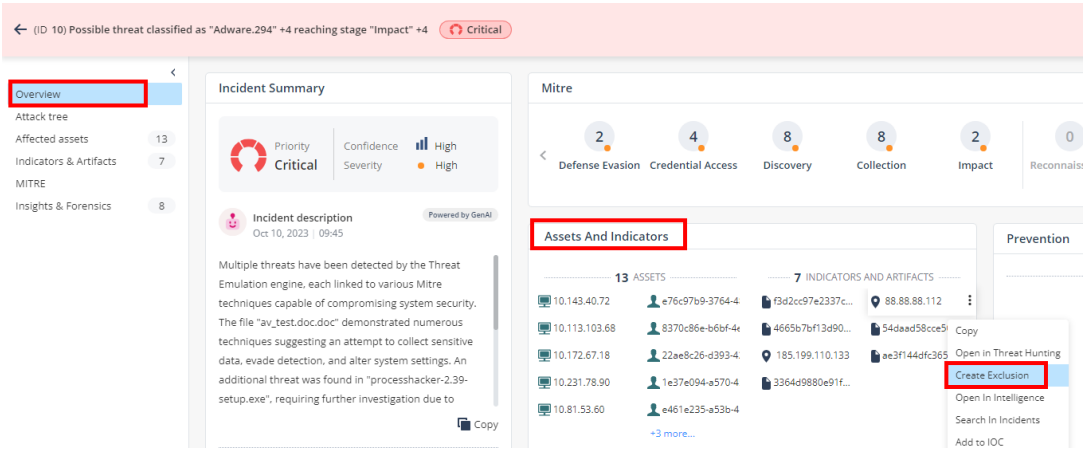
- From the incident **Overview** page:
  a. In the **Incidents** page, click the incident or hover over the incident and click **>**.

     The incident **Overview** page appears.

  b. Go to **Assets and Indicators** > **Indicators and Artifacts** section.

  c. Hover over the indicator or artifact and click ⋮ .

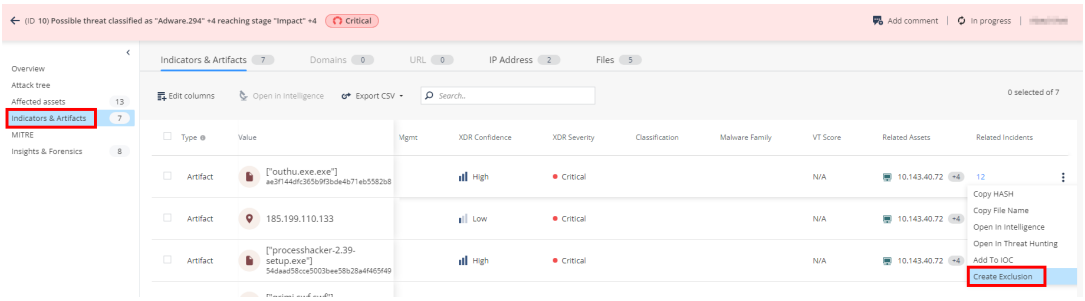
  d. Click **Create Exclusion**.



- From the incident **Indicators & Artifacts** page:
  a. In the **Incidents** page, click the incident or hover over the incident and click **>**.

  b. Go to **Indicators & Artifacts** tab.

  c. In the table, at the end of the row, hover over ⋮, and click **Create Exclusion**.

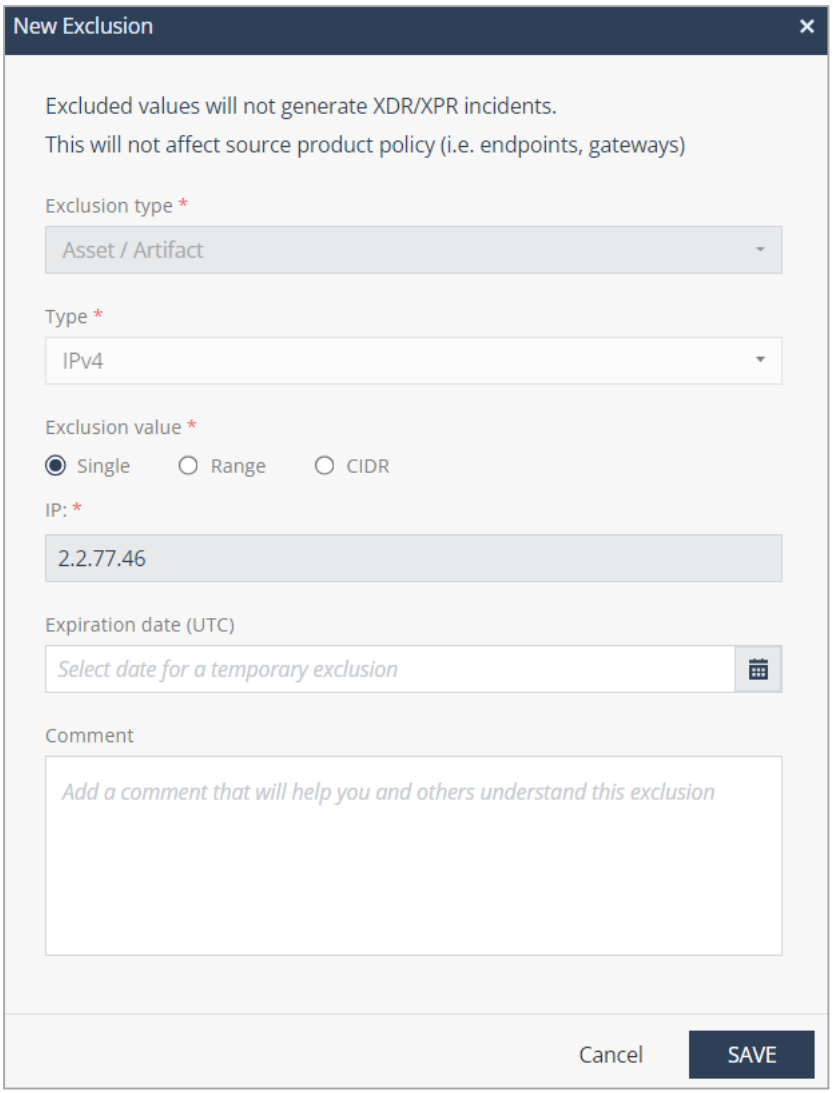


The **New Exclusion** window appears. The following fields are pre-filled:

- **Exclusion type** - Asset / Artifact
- **Type** - Type of the selected artifact.

  For example, IPV4, URL

- **Exclusion value** - Value of the selected artifact.



3. (Optional) Select an **Expiration date (UTC)** for the exclusion. After the expiration date, the artifact or indicator can create incidents.
4. (Optional) Enter **Comments**.
5. Click **Save**.

Adding or Editing an Indicator or Artifact in IoC Management

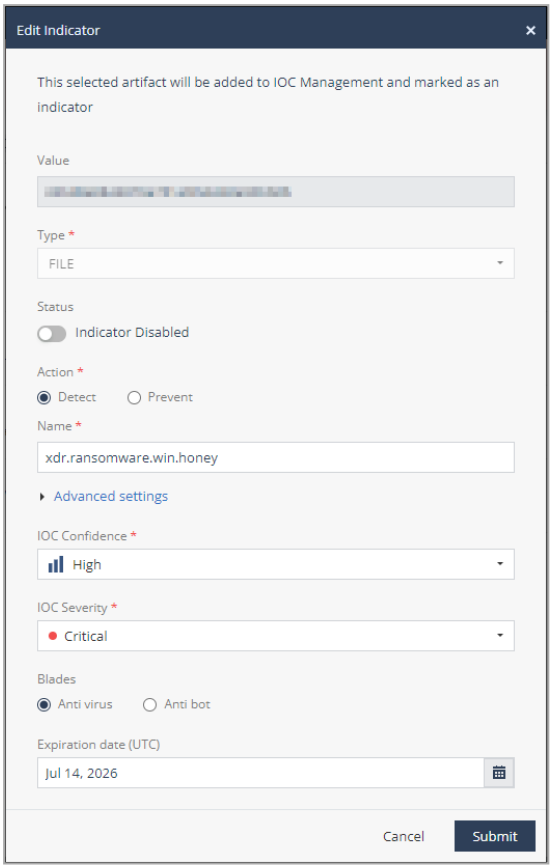
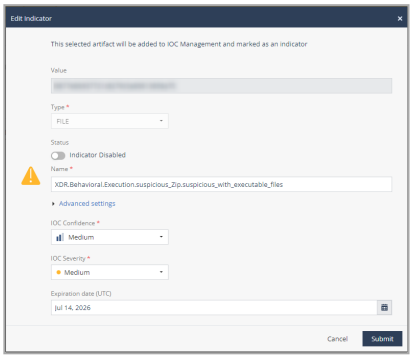
1. Click **Incidents**:
   - Click the incident title.
   - Hover over the incident and click **>**.
2. Click **Indicators & Artifacts**.

3. To add an artifact to IoC Management, in the table, at the end of the row, hover over ⋮, and click **Add to IoC Management**.

   Note - Adding an artifact to IoC Management changes its type from artifact to indicator.

4. To edit an indicator's setting in IoC Management, in the table, at the end of the row, hover over ⋮, and click **Edit in IoC Management**.

   The **Edit Indicator** pop-up appears.

If you are using the legacy IoC Management	If you are using the New IoC Management
■ XDR automatically populates **Status**, **Action** and **Name** fields.  ■ Expand **Advanced settings**, and enter: • **Confidence** • **Severity** • **Blade** • **Expiration date** - After the expiration date, the IoC is disabled automatically.	■ XDR automatically populates **Value**, **Type** and **Feed** fields.  ■ Enter **Confidence**, **Severity**, and **Expiration date**. **Note** - To migrate to the New IoC Management, see *"Migrating to the New IoC Management" on page 229*.

5. Click **Save**.

Removing an Indicator from IoC Management

1. Click **Incidents**:
   - Click the incident title.
   - Hover over the incident and click **>**.
2. Click **Indicators & Artifacts**.

3. To remove an indicator from IoC Management, in the table, at the end of the row, hover over ⋮, and click **Remove from IoC Management**.

   Note - If you remove an indicator from IoC Management, it changes its type from an indicator to an artifact.

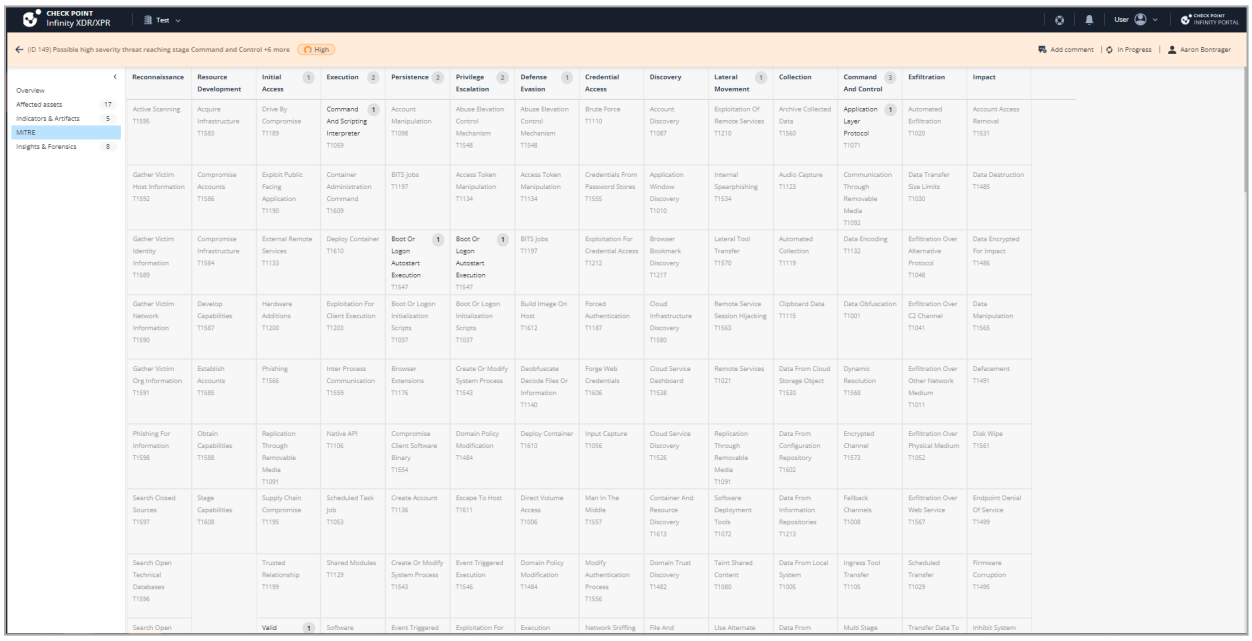
4. A confirmation message appears. click **Yes**.

Incidents - MITRE

The MITRE ATT&CK is a framework that breaks down the cyber attack lifecycle into its component stages and provides in-depth information about how each stage was accomplished.

To view the **MITRE** page:

1. Access XDR and click **Incidents** > **Incidents**.
2. Click the incident title or hover over the incident and click **>**.
3. Click **MITRE**.



MITRE ATT&CK organizes information into a hierarchy:

- Tactics: The column headers, represent adversaries' tactical goals in a cyber attack.
- Techniques: The cells under the tactic, represent the known methodologies available to achieve each tactic.

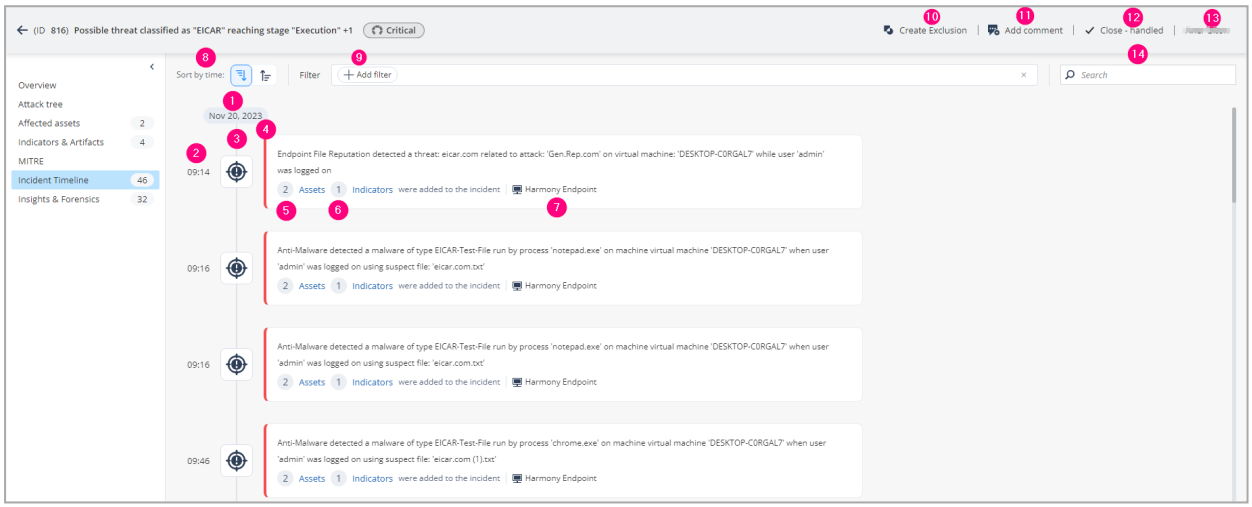
The number in a cell indicates the number of insights associated with the tactic or technique in the incident. Click the number to view the *"Incidents - Insights & Forensics" on page 113* page searching for the chosen tactic or technique.

Incident Timeline

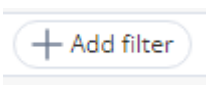
The **Incident Timeline** shows the timeline of all the events of an incident, starting from the time the incident was created.

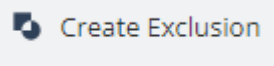
To view the **Incident Timeline** page:

1. Access XDR and click **Incidents** > **Incidents**.
2. Click the incident title or hover over the incident and click **>**.
3. Click **Incident Timeline**.



Legend	Item	Description
1	Date	Date of event.
2	Time	Time of event.

<table>
<tr><th>Legend</th><th>Item</th><th>Description</th></tr>
<tr><td>3</td><td>Event type</td><td>
<table>
<tr><th>Icon</th><th>Description</th></tr>
<tr><td>  </td><td>Action generated from an Insight by XDR.
To view the Insight details, hover over the action and click >. The Insights & Forensics page appears.</td></tr>
<tr><td>  </td><td>Automatic prevention action by XDR.
To view the Incident Overview page, hover over the action and click >.</td></tr>
<tr><td>  </td><td>Manual prevention action by the user or administrator. For example, adding an indicator to the IoC Management.
To view the Incident Overview page, hover over the action and click >.</td></tr>
<tr><td>  </td><td>User action. For example, user updated the incident status.</td></tr>
</table>
</td></tr>
<tr><td>4</td><td>Severity</td><td>Severity of the event. An event is color-coded based on its severity.</td></tr>
<tr><td>5</td><td>Assets
(Applies to Insight type only)</td><td>Number of assets involved in the incident.
To view the asset details, click the Assets link. The Affected assets page appears.</td></tr>
<tr><td>6</td><td>Indicators</td><td>Number of indicators created for the incident.
To view the indicator details, click the Indicators link. The Indicators & Artifacts page appears.</td></tr>
<tr><td>7</td><td>Source of the incident
(Applies to Insight type only)</td><td>N/A</td></tr>
<tr><td>8</td><td>Sort by time  </td><td>Sort events in the chronological or reverse-chronological order.</td></tr>
<tr><td>9</td><td> 
</td><td>Filter the timeline by:
■ Type
■ Severity
■ Data Sources</td></tr>
</table>

Legend	Item	Description
10		Create an exclusion for the incident. See *"Exclusions" on page 236*.
11		Add a comment on the incident.
12	Status	Status of the incident. ■ New ■ In Progress ■ Close - Handled ■ Close - False Positive ■ Close - Known Activity
13	Assignee name	Security expert to whom the incident is assigned.
14	Search	Enter free text to search in the timeline.

Incidents - Insights & Forensics

The **Insights & Forensics** page shows the details of insights and forensics (processes, files, URL, domains and Registry involved in the insight) related to the incident.

To view the **Insights & Forensics** page:

1. Access XDR and click **Incidents** > **Incidents**.
2. Click the incident title or hover over the incident and click **>**.
3. Click **Insights & Forensics**.

To edit the columns in the table, click **Edit columns** and select the columns.

To export the data to an excel in CSV format, click **Export All (CSV)**.

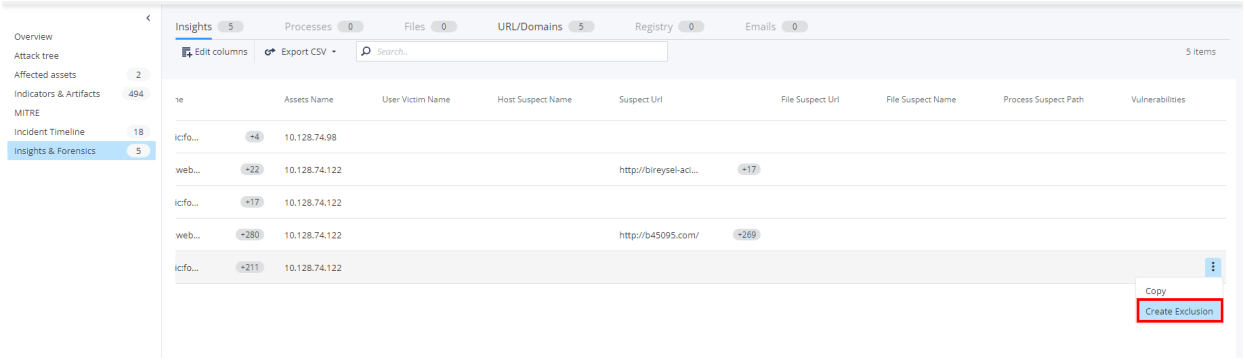
To search, in the **Search** field, enter the string. The table automatically filters and shows the content that matches with the string.

Creating an Advanced Exclusion from an Insight

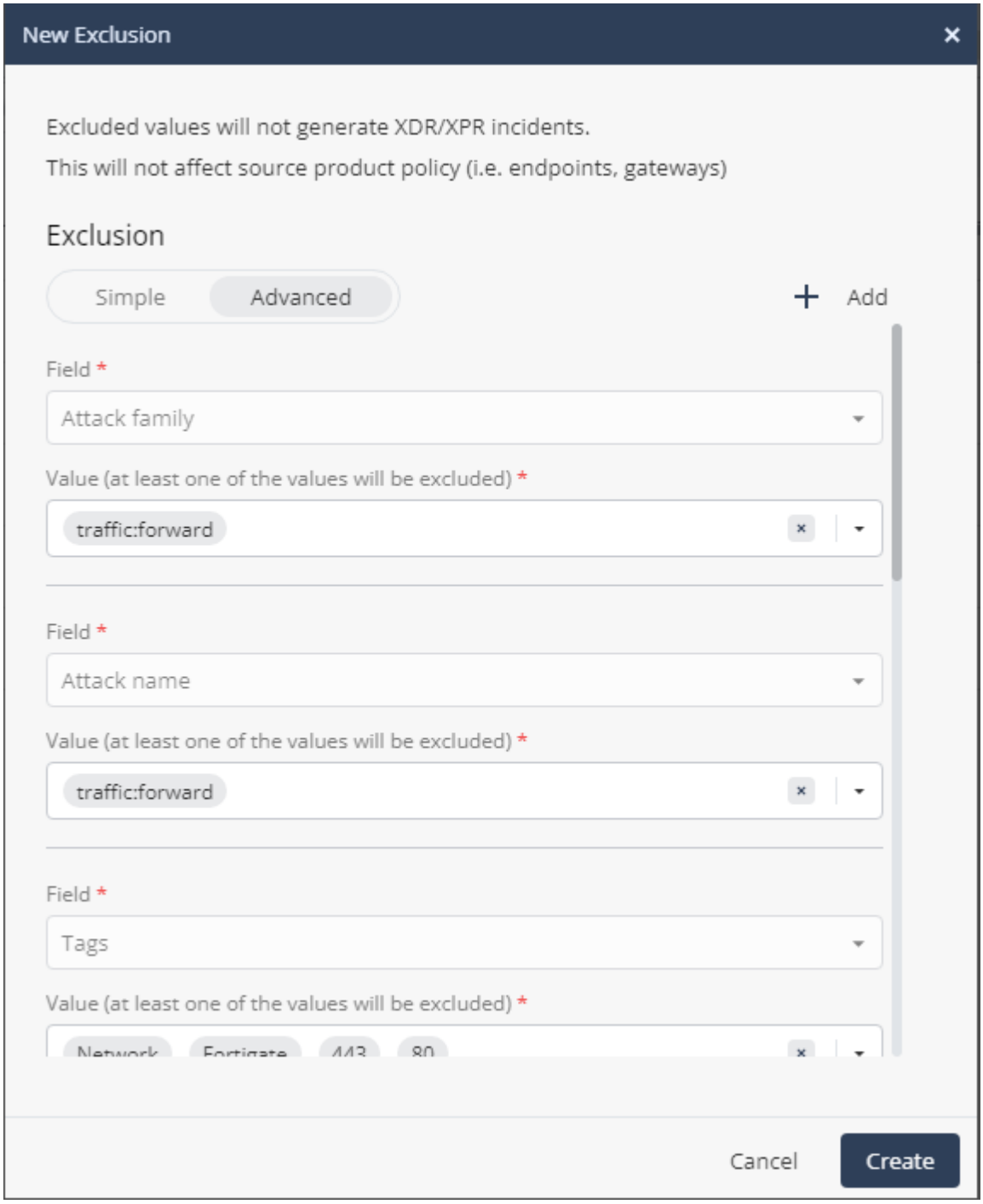
1. Access XDR and click **Incidents**:
   - Click the incident title.
   - Hover over the incident and click **>**.
2. Click **Insights & Forensics**.

   The **Insights & Forensics** page appears.

3. In the **Insights** table, hover over the insight for which you want to create the exclusion, click ⋮ and then click **Create Exclusion**.



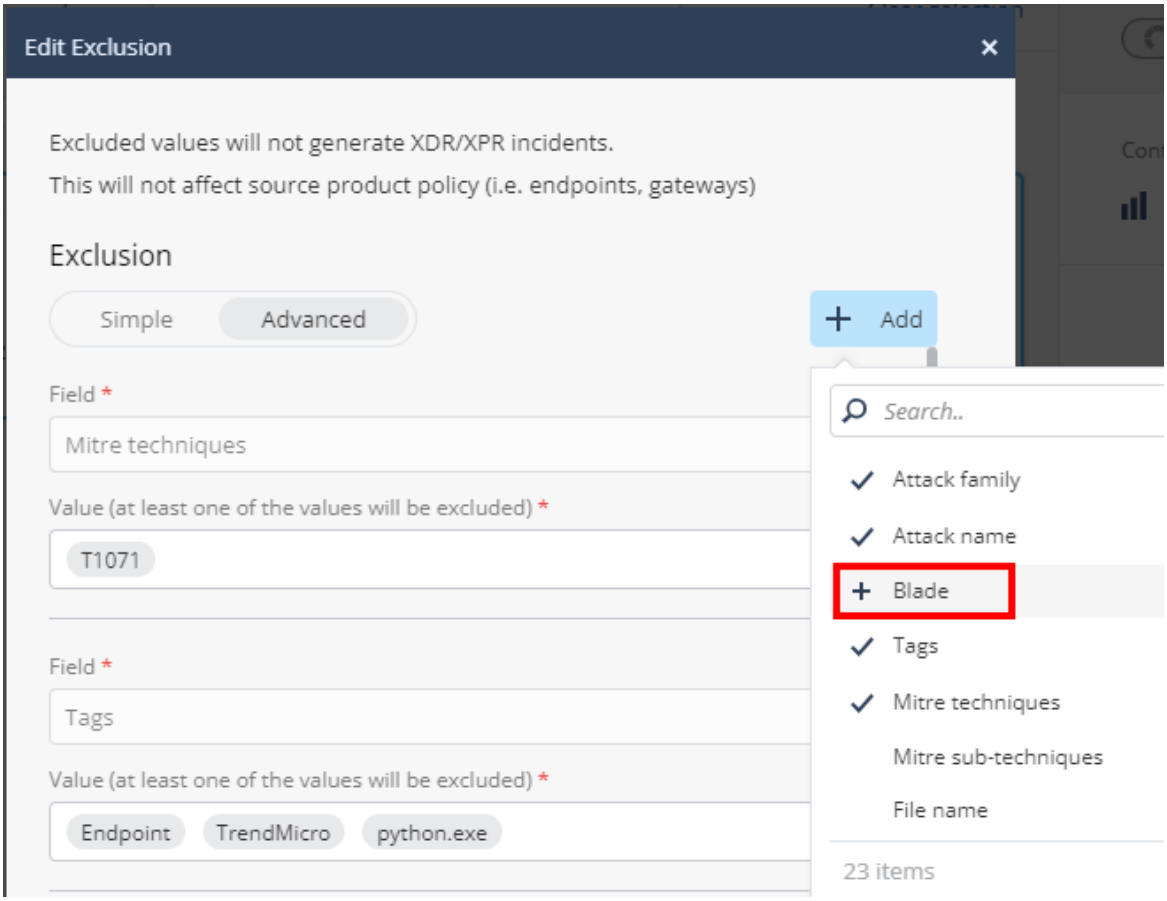
The **New Exclusion** window appears. The system automatically populates the field details of the insight.



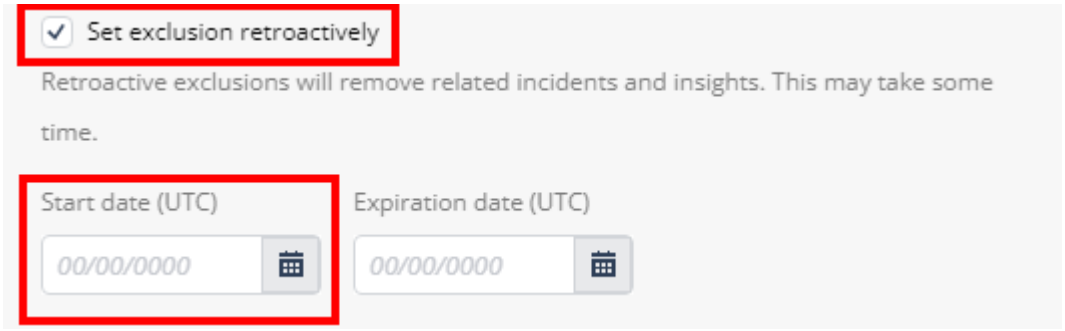
4. For each **Field**, edit the values as required. XDR applies this exclusion on insights that contain all the above fields and any of these values.

5. To add or remove a field, click **+ Add**. The fields already selected are marked with ✓.

- To add, hover over the field name and click **+**.
- To remove an already selected field, click the field name.



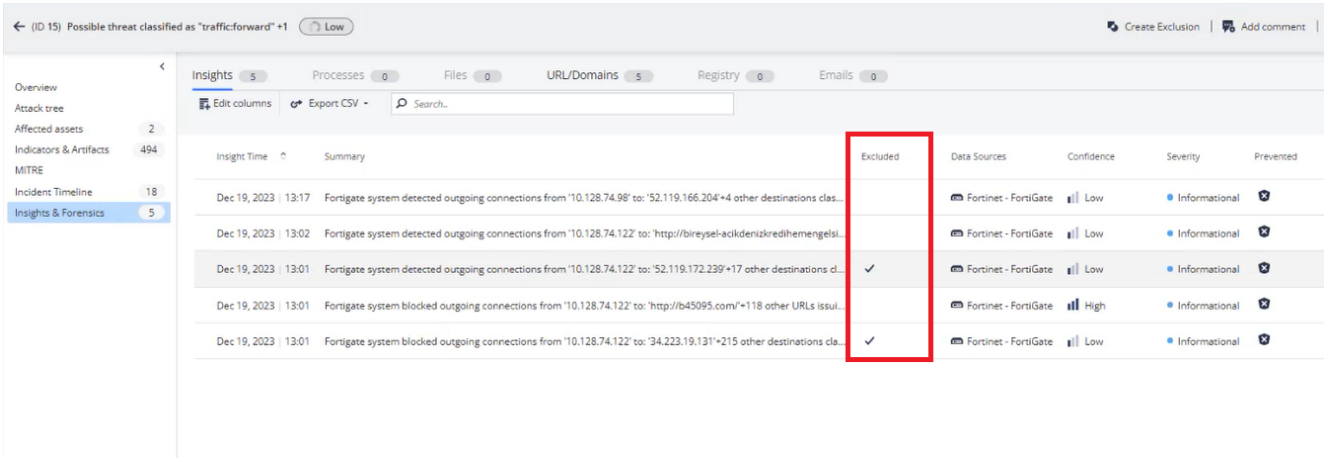
6. (Optional) To exclude the incidents already generated based on this insight:
   a. Select the **Set exclusion retroactively** checkbox.



   b. In the **Start date (UTC)** field, select a date within the last 90 days. XDR excludes all the incidents that were generated from this date based on this insight. To revert the exclusion, see *"Reverting a Retroactive Exclusion" on page 241*.
7. (Optional) In the **Expiration date (UTC)** field, select an expiration date for the exclusion. After this date, XDR generates incidents for this insight. By default, there is no expiry date for an exclusion.
8. (Optional) In the **Exclusion comment** section, enter a description about the exclusion.

9. Click **Create**.

After the exclusion is created, the **Excluded** column in the **Insights** table is marked with ✓ for that insight.



The exclusion is added to the **Exclusions** table in **Policy** > **Exclusions**. See *"Advanced Exclusions" on page 238*.

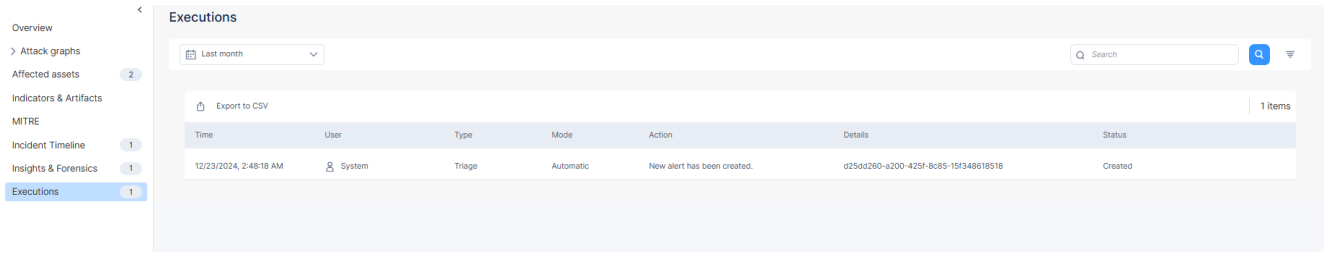
Incidents Executions

The **Executions** page shows the details of alert executions related to the incident.

For more information, see *Prevention Center* > *"Executions" on page 134*.

To view the Executions page:

1. Access XDR and click **Incidents** > **Incidents**.
2. Click the incident title or hover over the incident and click **>**.
3. Click **Executions**.

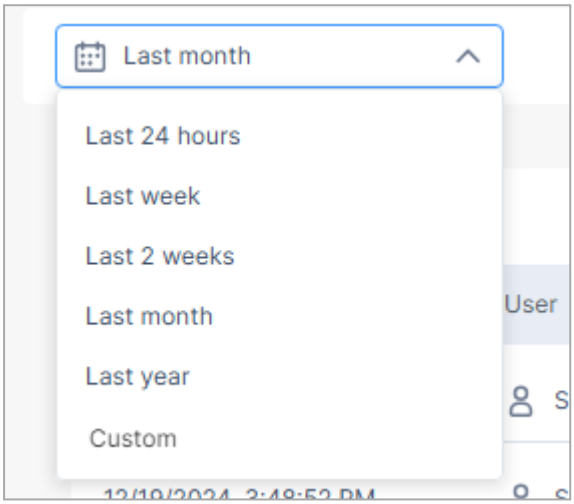


The **Executions** table shows:

Item	Description
Time	Date and time when the execution was performed.
User	User who performed the execution.
Type	Type of execution: ■ **Triage** - Involves handling of alerts, such as creating alerts or correlating them with existing incidents. ■ **Prevention** - Involves prevention actions taken by XDR in response to alerts, such as creating an IoC.
Mode	Mode of execution: ■ **Automatic** - Executed automatically by XDR. ■ **Manual** - Executed manually by user.
Action	Action taken on the alert.
Details	Details about the execution, such as Insight ID or indicator value.

Item	Description
Status	Status of the execution: ■ Created ■ Completed ■ Failed

To view the executions during a specific time period, select the required option from the list at the top.

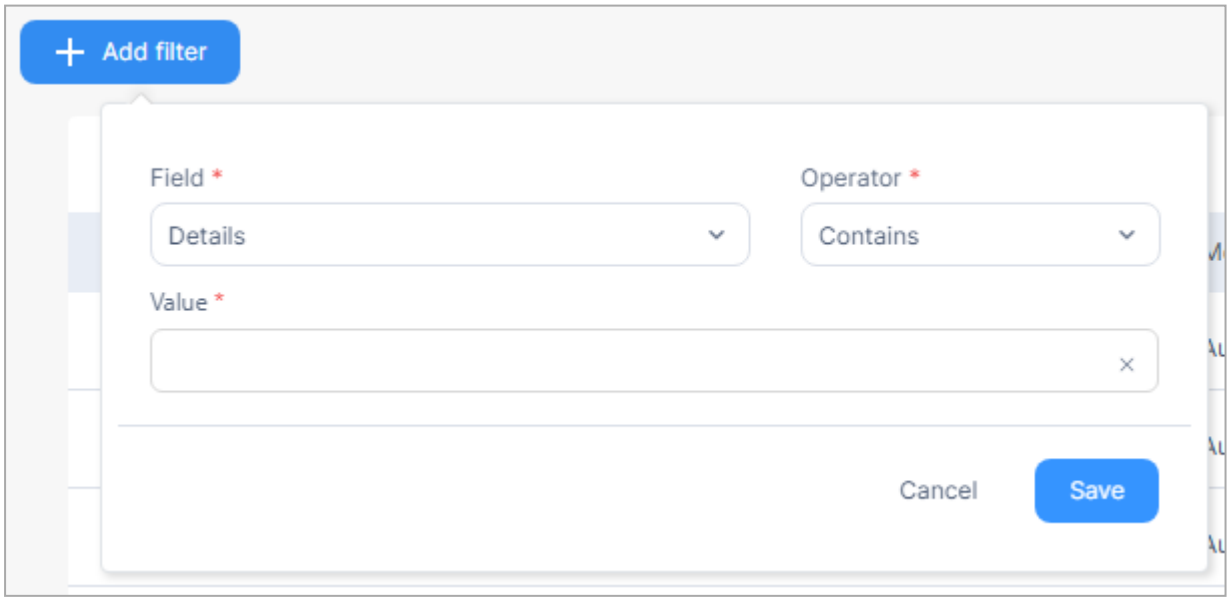


To export the Executions table data to a CSV file, click **Export to CSV**.

To search, in the **Search** field, enter the string and click the icon.

To filter the Executions table:

1. Click the icon and then click **Add filter**.

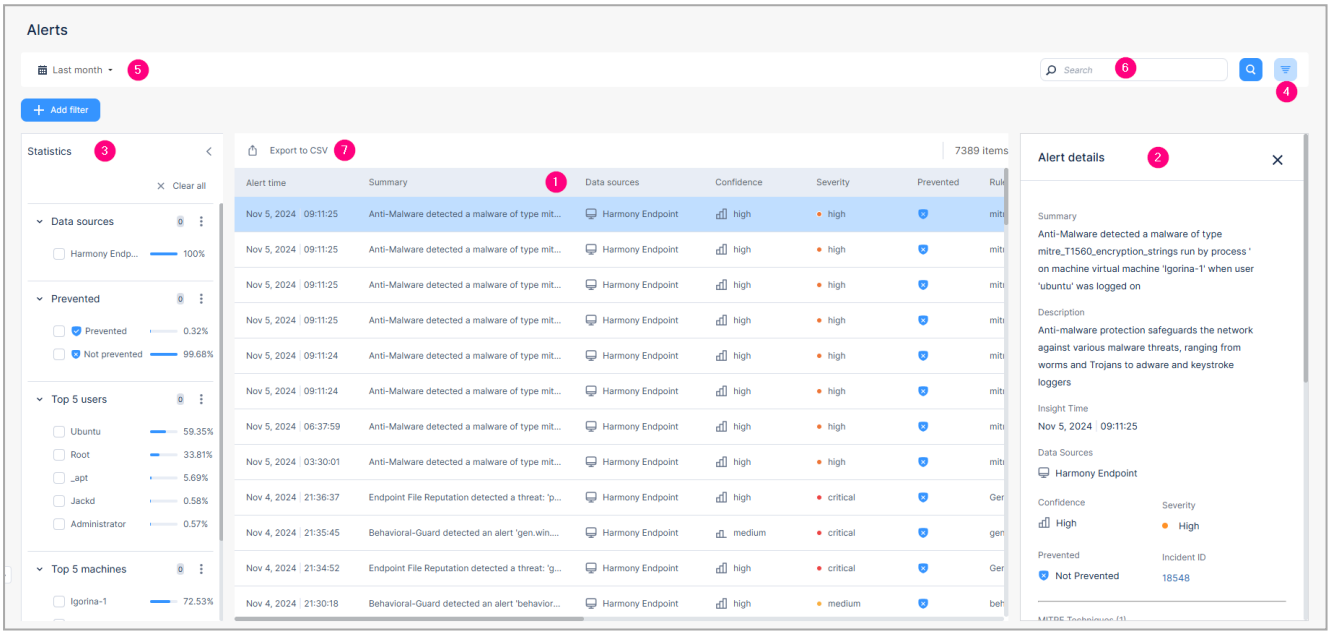


2. Enter the **Field**, **Operator** and **Value** and then click **Save**.

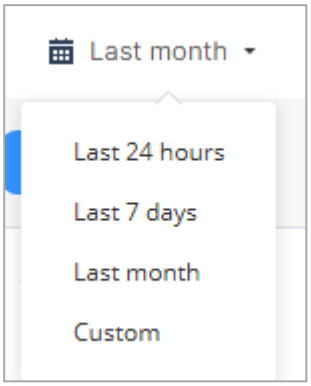
Alerts

Check Point XDR processes and triage all received alerts, and those that match one of the detection rules are considered as Alerts. The **Alerts** page provides you a summary of all alerts across the system. Extensive filtering capabilities on this page allows you to narrow the search within the Alerts table contents. You can also view additional details for an alert by selecting a record in the Alerts table.

To view the **Alerts** page, access the XDR Administrator Portal and click **Incidents** > **Alerts**.



Legend	Item	Description
1	Alerts table	Shows alerts from all the incidents. For more information, see *"Alerts Table" on the next page*.
2	Alert details	Shows additional information about the alert.
3	Statistics	Shows different filters that you can apply on the Alerts table. For more information, see *"Statistics" on page 124*.
4	Add filter icon	Adds a new filter to the Alerts table. For more information, see *"Adding a New Filter" on page 125*.

Legend	Item	Description
5	Time period	Shows the time period selected for the Alerts table. By default, the table shows the alerts generated in the previous month. To view alerts during a specific time period, select the required option from the list. 
6	Search	Enter the search text to search for any alert data.
7	Export to CSV	Click **Export to CSV** to export the Alerts table data to a CSV file. The system downloads a CSV file with the alerts data.

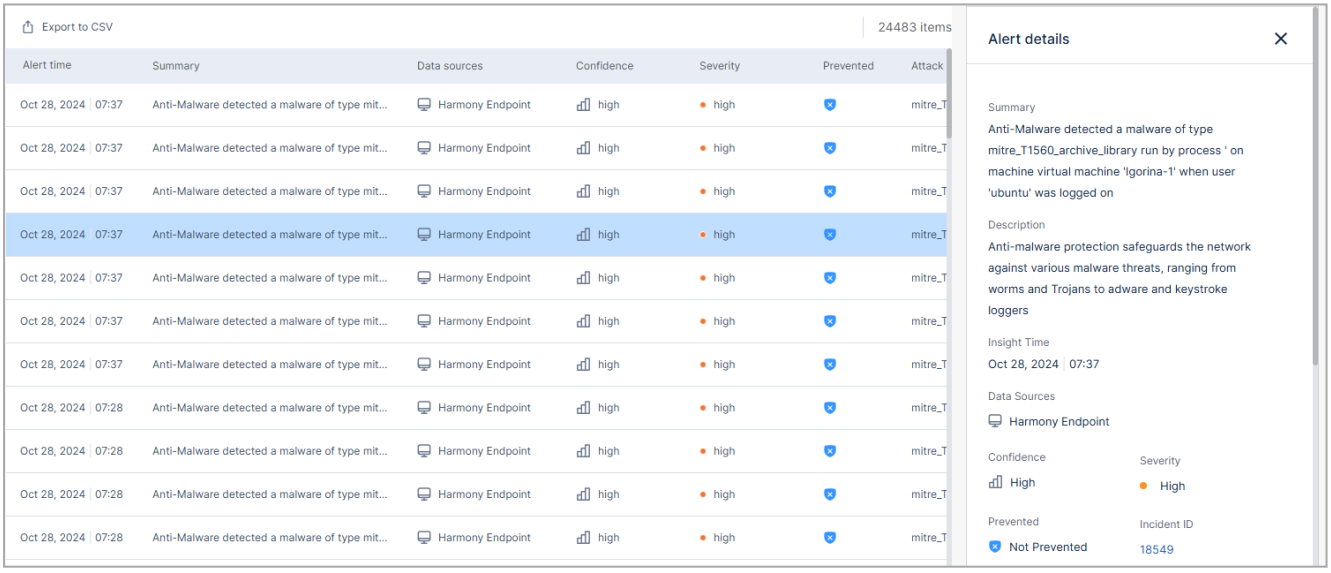
Alerts Table

The Alerts table shows:

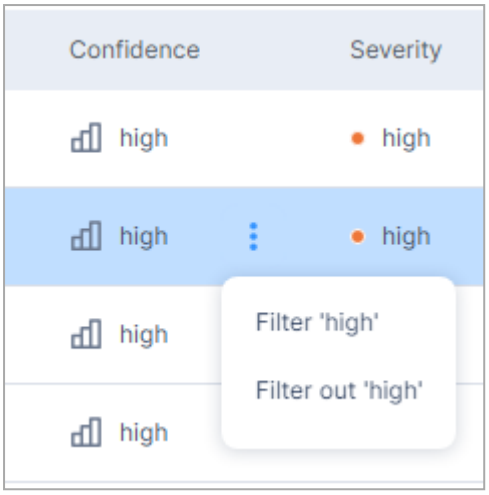
Column	Description
Alert time	Date and time when the alert was generated.
Summary	Summary of the alert.
Data sources	Application from which the alert was generated.
Confidence	Confidence level of alert detection.
Severity	Severity level of the alert.
Prevented	Shows whether the attack was prevented: ■ - Attack was prevented. ■ - Attack was not prevented.
Rule name	Name of the attack that generated the alert.
MITRE Techniques	MITRE ATT&CK technique used in the attack.

Column	Description
Indicators name	Name of the indicators related to the alert.
Asset name	Asset related to the alert.
Process name	Name of the process related to the alert.
Artifacts	Artifacts related to the alert.
Files	Files related to the alert.
Email subject	Subject(s) in the email that triggered the original detection.
Incident ID	ID of the incident related to the alert. To view the incident details, click the ID. The *"Incidents - Overview" on page 64* page appears.

To view details of a specific alert, click the alert row. The system shows the **Alert details** tab on the right side.



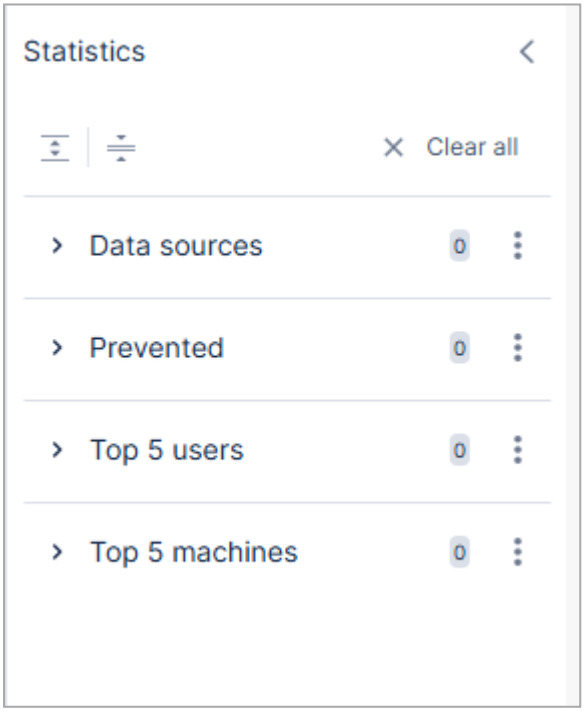
You can filter the Alerts table by either including (**Filter**) or excluding (**Filter out**) specific fields. To do that, hover over the field and click the ⋮ icon and then select the required option.



Statistics

The **Statistics** panel allows you to filter the Alerts table. By default, these primary filters are available:

- Data sources
- Prevented
- Top 5 users
- Top 5 machines



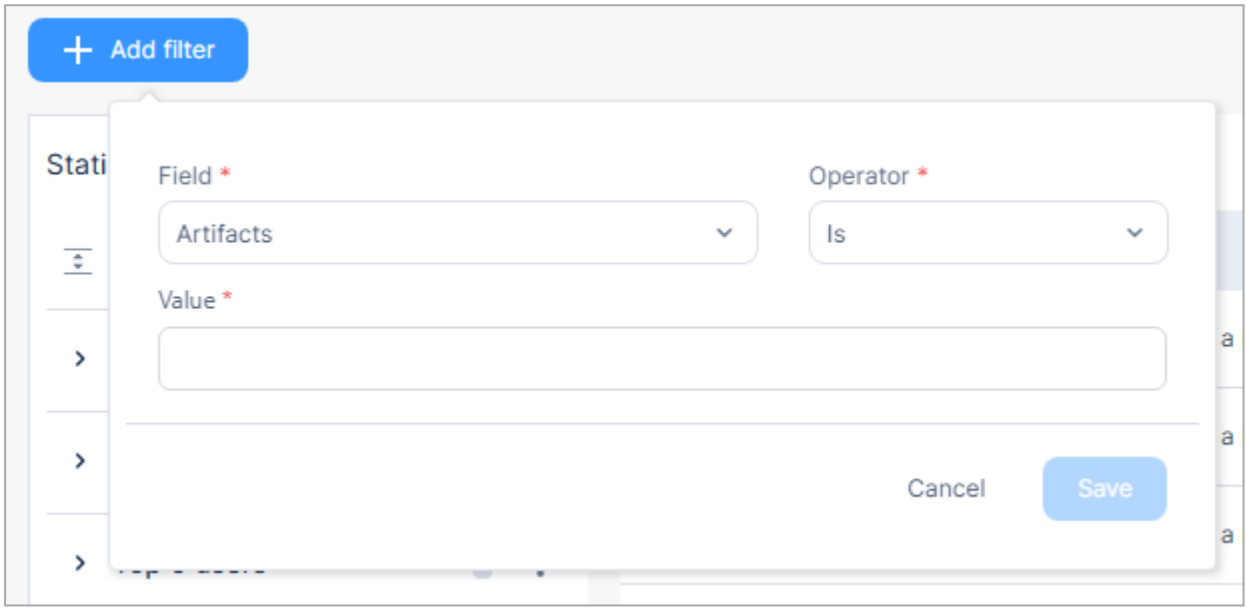
To apply these filters on the Alerts table data, expand the required filter and select the parameters.

Adding a New Filter

You can add new filters in addition to the primary filters.

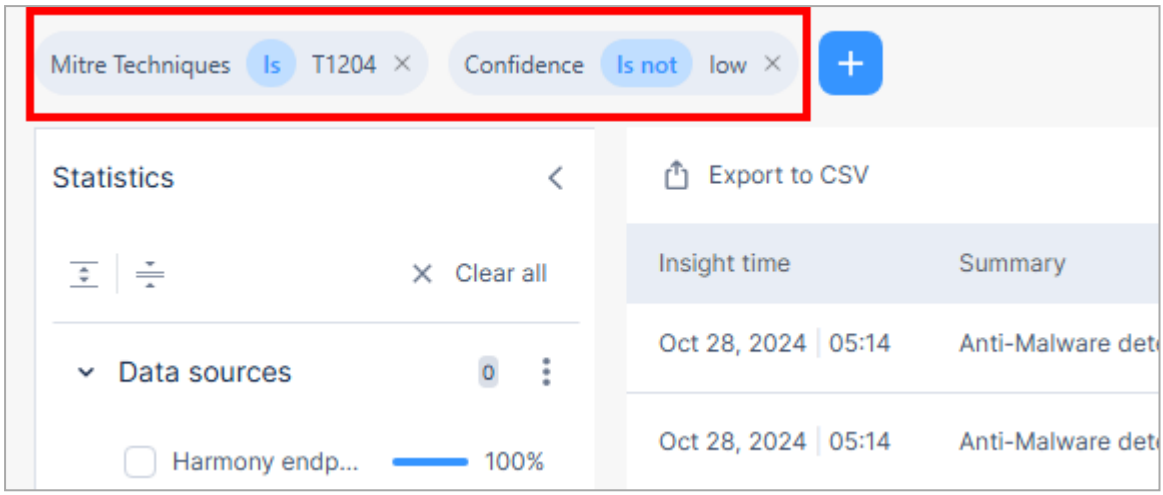
To add a new filter:

1. Click the icon at the top-right corner.
2. Click **Add filter** above the **Statistics** panel.



3. Enter these details:
   a. **Field** - Select the alert field.
   b. **Operator** - Select the operator to be applied.
   c. **Value** - Enter the value of the alert field.
4. Click **Save**.

The system adds the filter and applies it on the Alerts table.



Prevention Center

The **Prevention Center** provides a summary of prevention activities performed by Check Point XDR across all data processed in your account.

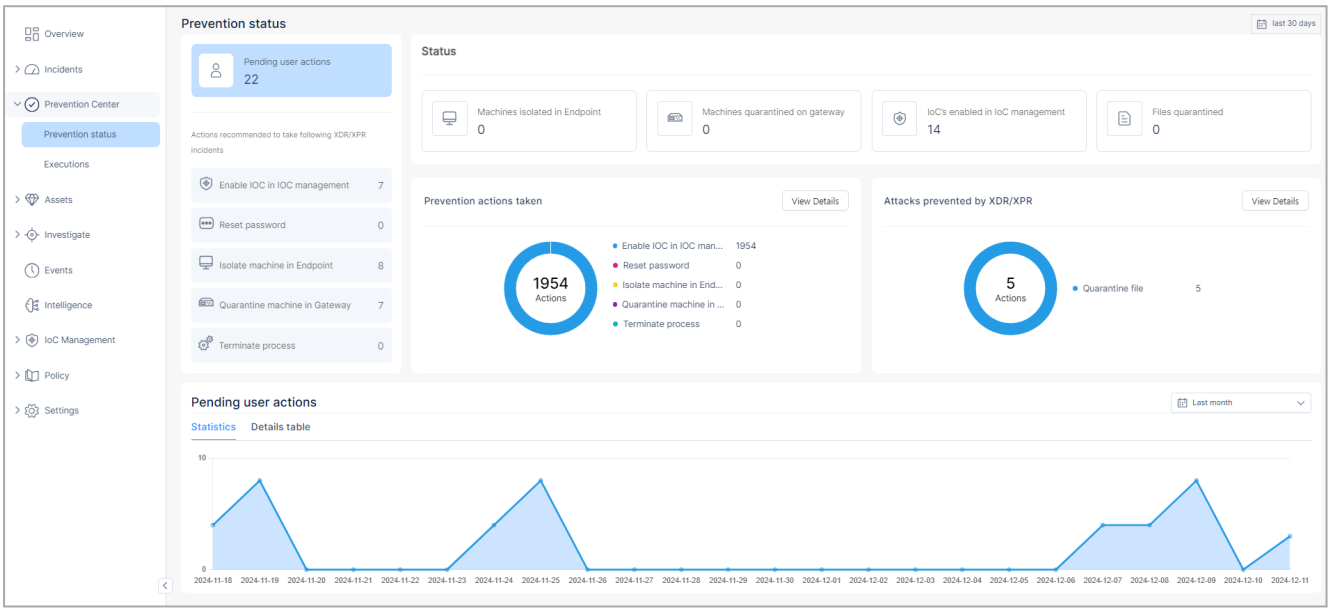
It consists of the following sections:

- **Prevention Status** - Shows the statistics of prevention actions in your account, that includes pending, active and expired actions. See *"Prevention Status" on page 128*.
- **Executions** - Provides visibility into how XDR processes alerts and executes actions in response to the alerts. See *"Executions" on page 134*.

Prevention Status

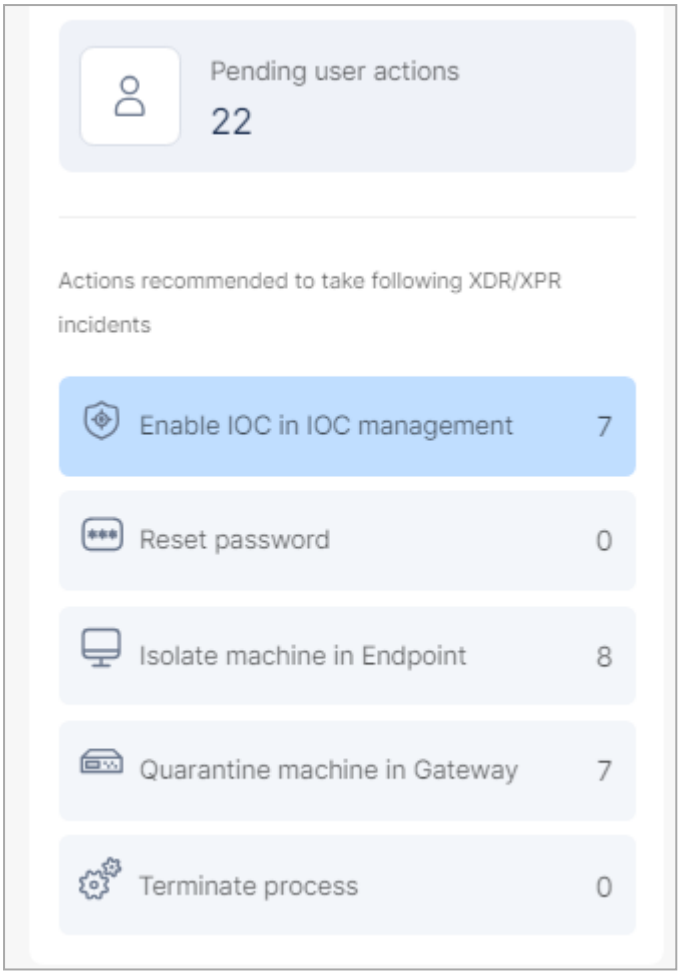
The **Prevention status** page provides a summary of pending prevention actions to be taken, actions that are currently active and historical actions that have already been taken over a specific time period.

To view the **Prevention status** page, access the XDR Administrator Portal and click **Prevention Center** > **Prevention status**. It shows the prevention status for the last 30 days.



Pending User Actions

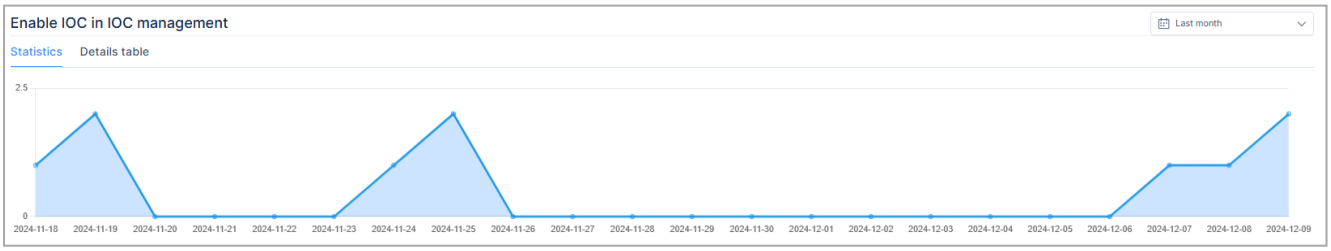
The **Pending user actions** widget shows the recommended prevention actions from all incidents in your account that require user action. The actions are categorized by their type (for example, **Enable IoC in IoC management** or **Reset password**).



To view the details of a pending action, click the relevant action type. The table that appears below the widget shows the statistics and details of the selected action.

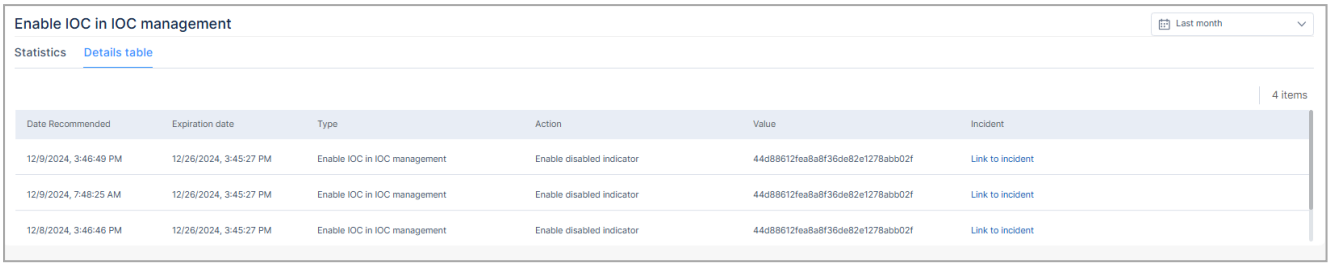
The example below shows the table displayed when you select the action **Enable IOC in IOC management**.

Statistics



The **Statistics** tab shows the number of recommended actions created in a specific time period. You can select the time period from the list at the top. By default, the system shows the statistics for the previous month.

Details Table

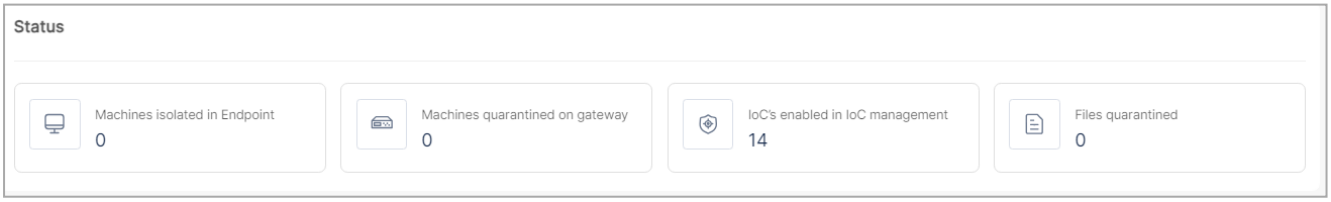


The **Details table** shows the details of the pending action.

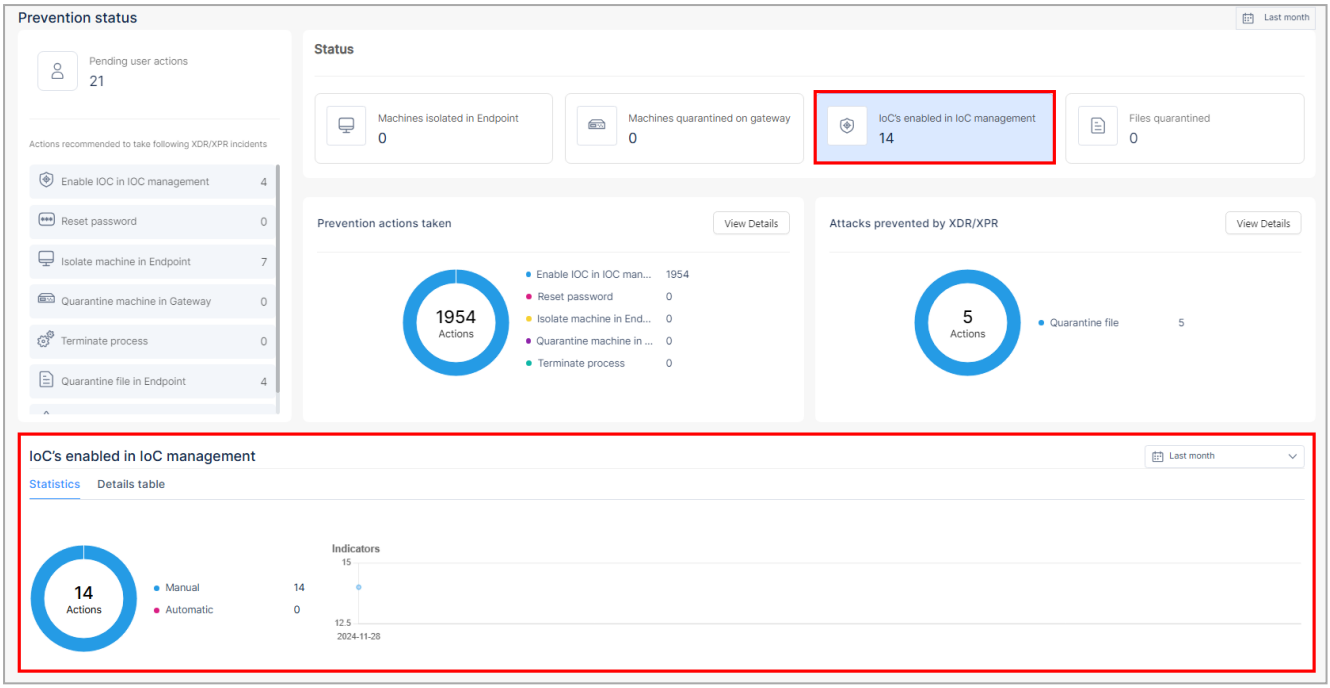
Item	Description
Date Recommended	Date and time when XDR recommended the prevention action.
Expiration date	Date and time when the prevention action expires.
Type	Type of the prevention action.
Action	Description of the prevention action.
Value	Indicator value/ machine name/ file name (Depends on the action type).
Incident	Link to the related incident. Click it to view the incident details.

Status

The **Status** widget shows the number of prevention actions taken that are currently active, categorized by action type. In the example below, the system has 14 IoCs currently enabled in IoC Management.



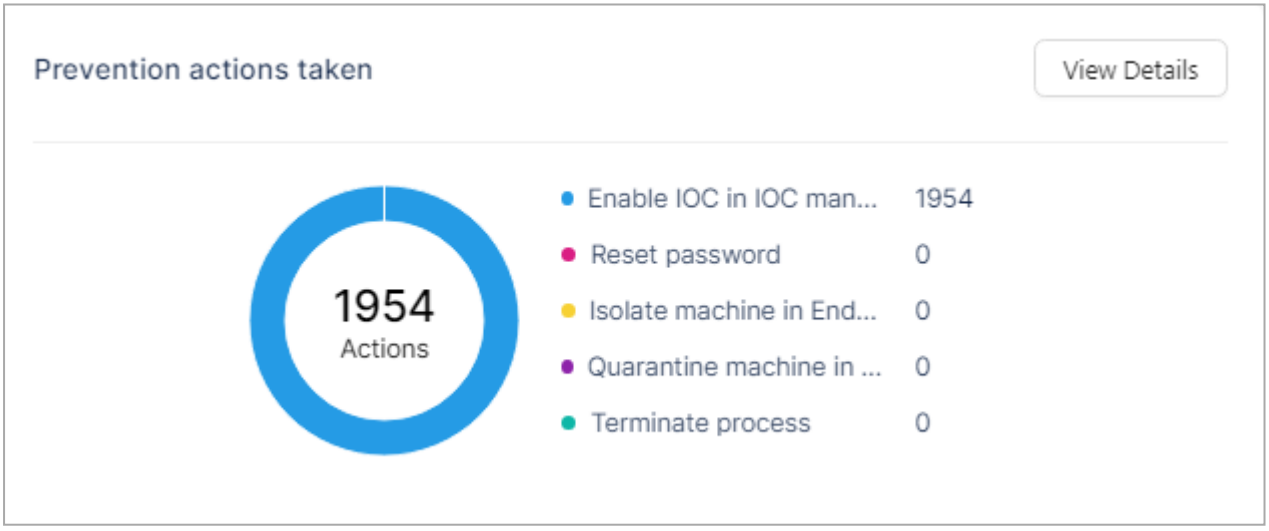
To view the details of an action, click the widget corresponding to the relevant action type (for example, **IoCs enable in IoC management**). The table that appears at the bottom shows the statistics and details of the selected action.



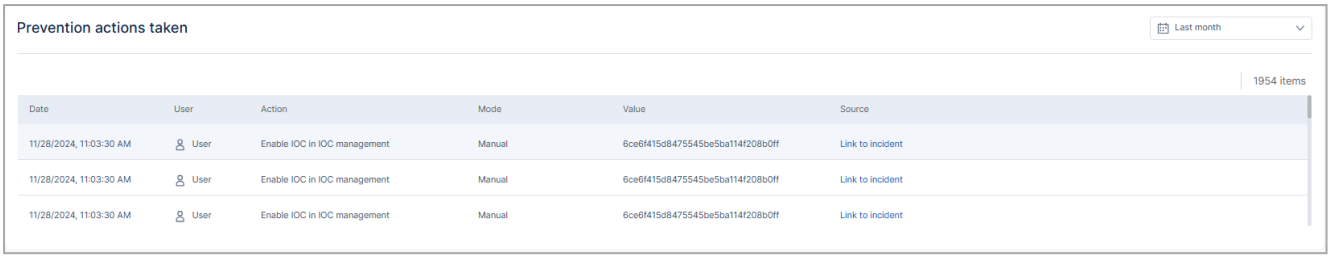
To view details of the selected action, click **Details table**.

Prevention Actions Taken

The **Prevention actions taken** widget shows the total number of prevention actions taken, including active ones, those that were deactivated by the user before they expired, and the expired ones.



To view the action details, click **View Details**. The **Prevention actions taken** table that appears below the widget provides information about all active and expired prevention actions.



The **Prevention actions taken** table shows:

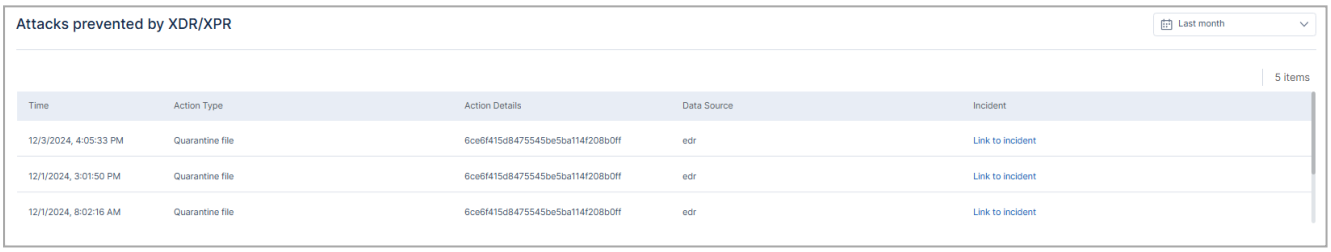
Item	Description
Date	Date and time when the prevention action was taken.
User	User who performed the action.
Action	Prevention action taken.
Mode	Mode of performing the prevention action: ■ **Automatic** - Performed automatically by XDR. See *"Automations" on page 232*. ■ **Manual** - Performed manually by the user.
Value	Indicator value/ machine name/ file name (Depends on the action type).
Source	Link to the related incident. Click it to view the incident details.

Attacks Prevented by XDR/XPR

The **Attacks prevented by XDR/XPR** widget shows the number of attacks blocked on different integrated products by performing the actions recommended by XDR. The widget categorizes the prevention actions by their type.

For example, Harmony Endpoint blocks an attack involving an indicator that was enabled based on a recommended action in XDR.

To view the attack details, click **View Details**. The **Attacks prevented by XDR/XPR** table that appears below the widget provides information about all the prevented attacks.



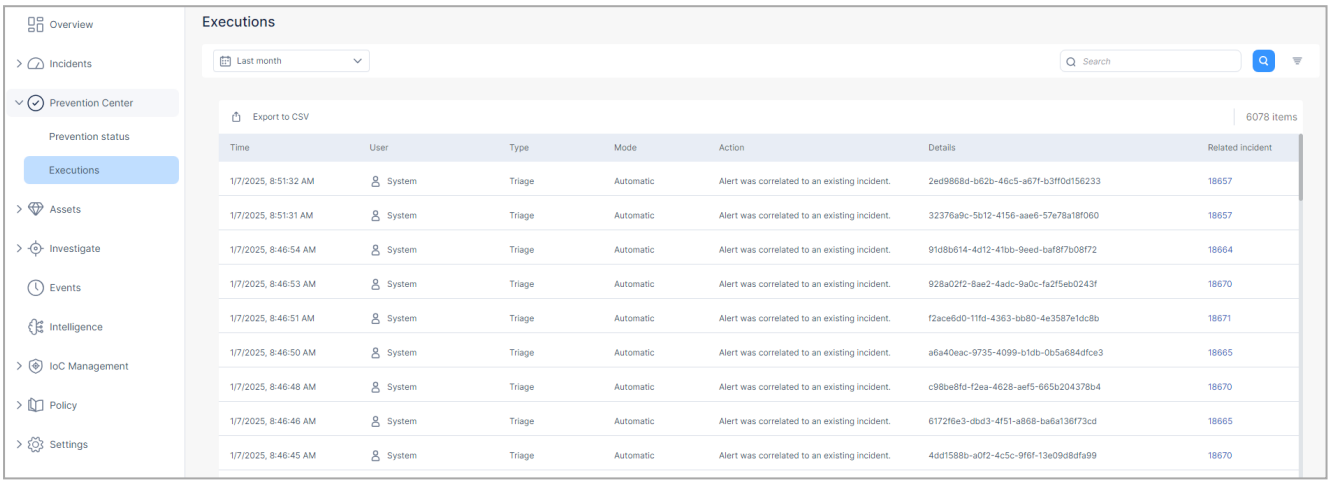
The **Attacks prevented by XDR/XPR** table shows:

Item	Description
Time	Date and time when the attack was prevented.
Action Type	Type of the prevention action taken.
Action Details	Indicator value/ machine name/ file name (Depends on the action type).
Data Source	Product that blocked the attack.
Incident	Link to the related incident. Click it to view the incident details.

Executions

The **Executions** page provides visibility into how Check Point XDR processes the alerts received in your account and the actions that it executes in response to the alerts.

To view the **Executions** page, access the XDR Administrator Portal and click **Prevention Center** > **Executions**. By default, it shows the executions from the previous month.

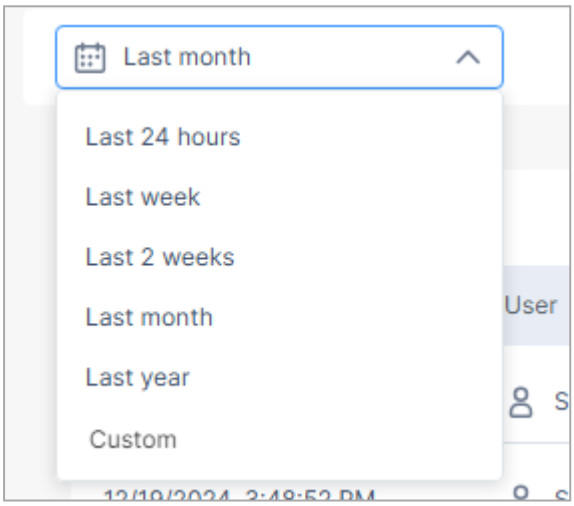


The **Executions** table shows:

Item	Description
Time	Date and time when the execution was performed.
User	User who performed the execution.
Type	Type of execution: ■ **Triage** - Involves handling of alerts, such as creating alerts or correlating them with existing incidents. ■ **Prevention** - Involves prevention actions taken by XDR in response to alerts, such as creating an IoC.
Mode	Mode of execution: ■ **Automatic** - Executed automatically by XDR. ■ **Manual** - Executed manually by user.
Action	Action taken on the alert.
Details	Details about the execution, such as Insight ID or indicator value.

Item	Description
Related incident	Incident related to the execution. Click the link to view the incident details. You can view the details in *"Incidents Executions" on page 118*.
Status	Status of the execution: ■ Created ■ Completed ■ Failed

To view the executions during a specific time period, select the required option from the list at the top.

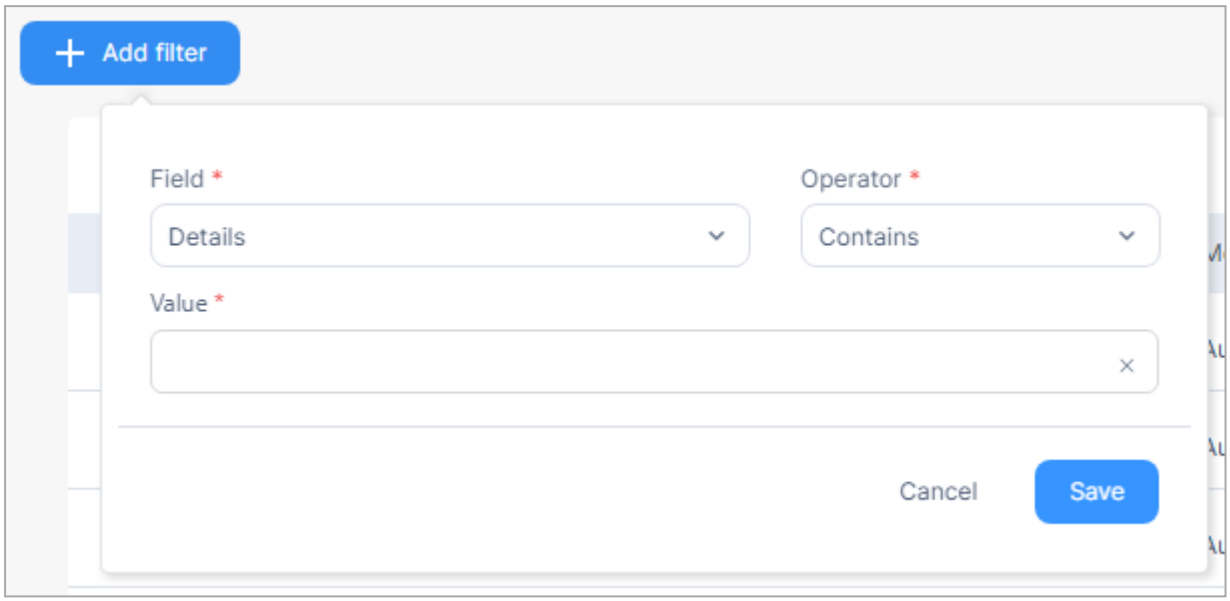


To export the Executions table data to a CSV file, click **Export to CSV**.

To search, in the **Search** field, enter the string and click the icon.

To filter the Executions table:

1. Click the icon and then click **Add filter**.



2. Enter the **Field**, **Operator** and **Value** and then click **Save**.

Assets

An **asset** refers to any resource within an organization's network that requires protection. The **Assets** tab provides visibility on the Usersand Devices assets protected by Check Point XDR. It serves as a starting point for investigating incidents, allowing you to examine individual users and devices and then pivot to related incidents for detailed analysis.

For each asset, information is collected and displayed in one of the following categories:

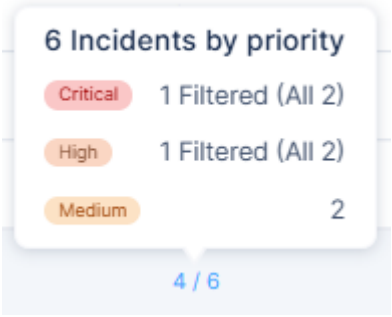
- Asset operational configuration (such as Asset Name, Operating System and Version)
- Incident Priority and Related Incidents

  In Check Point XDR, all incidents have a defined priority and can be associated with one or more assets. The incident priority of an asset is derived from the incidents it is associated with, according to the following criteria:

  - Incidents that are not in **Closed** state and not marked as **Prevented** are considered to determine the Incident Priority. These are the incidents that require action by the user.
  - Some incidents that impact a large number of assets are excluded from determining the Incident Priority. Such incidents are considered as **Filtered**.

  The Incident Priority is set to the highest priority of the incidents that meet the above criteria. For example, if there are one or more associated incident(s) with **Critical** priority, then the Incident Priority of the asset is set to **Critical**.

  In addition, the Related Incidents shows the total number of incidents related to the asset. The tool tip for the count shows the number of associated incidents in each priority category. If applicable, it also shows the number of the filtered incidents and the total number of incidents, as shown in the example below.



- Related Assets

  There are interrelations between users and devices. For example, users access a network through one or more device. These relationships are displayed in the **Related Devices** / **Usernames** field.

- Activity Time

When the system receives any data on an asset, it updates the **Last Activity** time for that asset. When you select a time filter for asset display, filtering is done based on the **Last Activity** time of the assets.

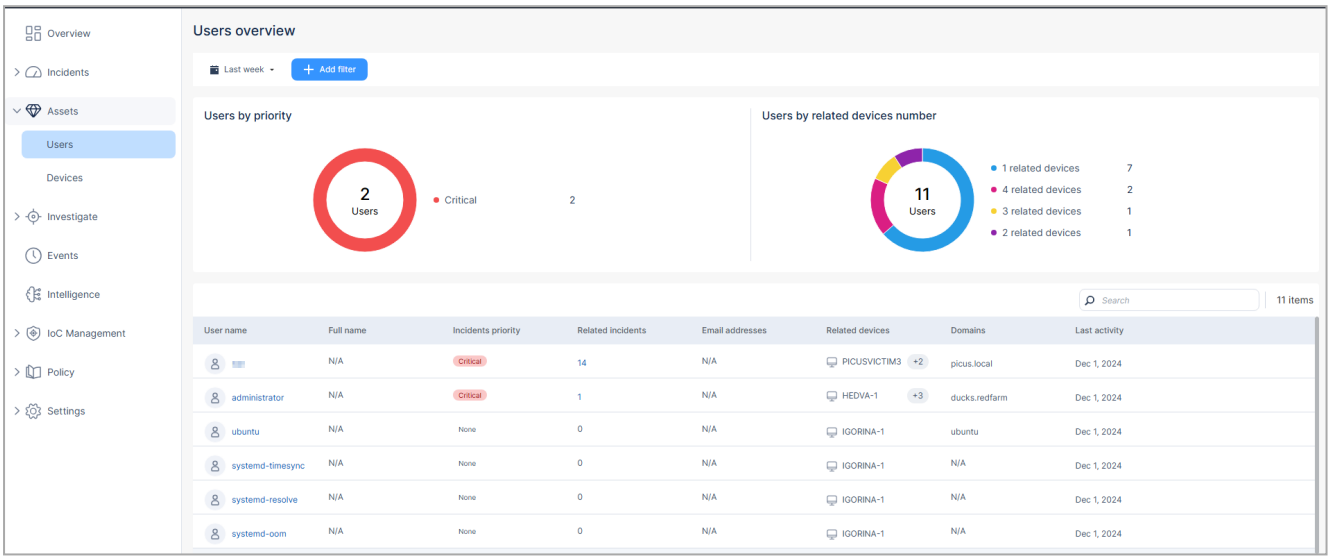
For example, if an asset has not communicated in the last week, it will not be displayed when the time filter is selected as **Last Week**. However, it will be displayed when the filter covers a period which is longer than a week.

- Identity Provider (IdP) groups in which the asset is a member.

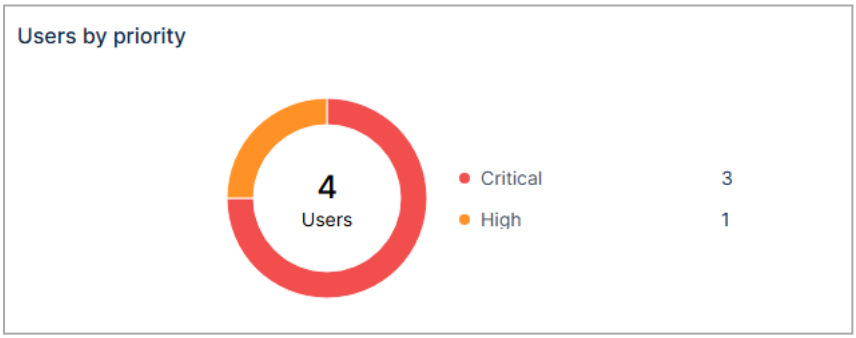
Users

The **Users** page shows information about the user assets in your account and the details of related devices, incidents and Identity Provider (IdP) groups.

To view the **Users** page, access the XDR Administrator Portal and click **Assets** > **Users**. By default, it shows details of users whose **Last activity** date is within the past seven days.

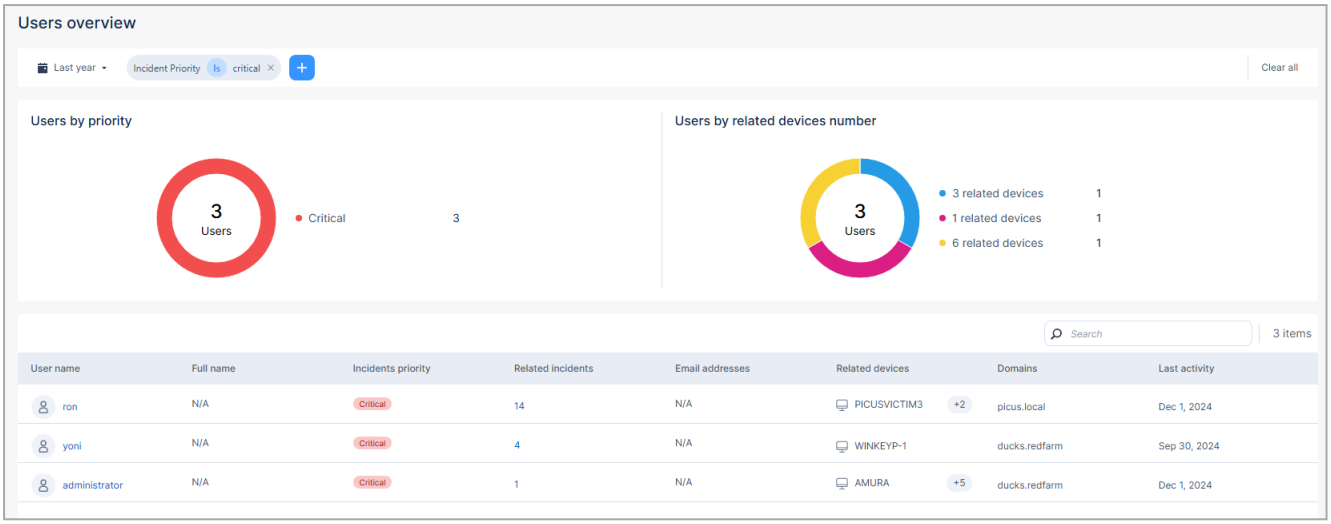


Users by Priority

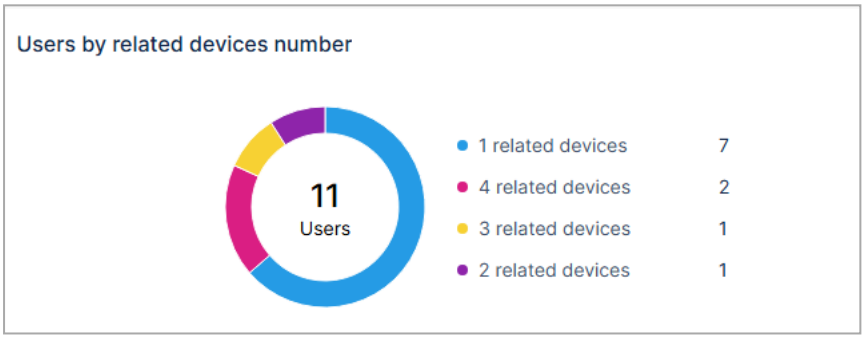


The **Users by priority** widget shows the number of users based on the priority level of the incidents they are involved in, within the selected time period.

To filter the **Users overview** page according to a specific priority level, click the relevant section on the pie chart. The system filters the page based on your selection and adds this filter to the Filter list.



Users by Related Devices Number

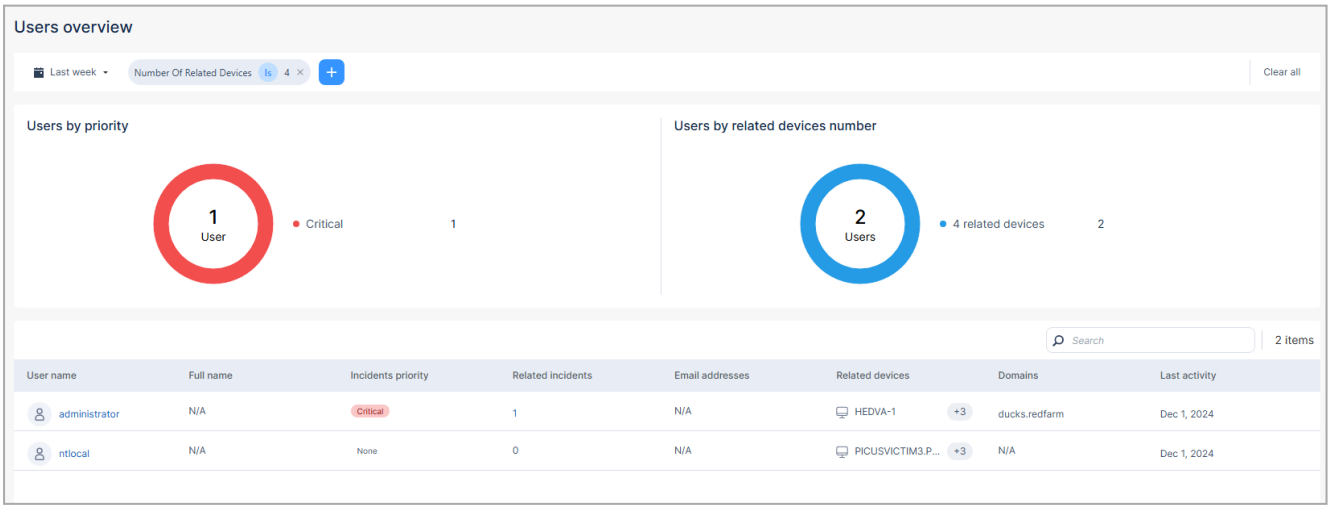


The **Users by related devices number** widget shows the total number of users and the statistics of related devices, within the selected time period.

To view information of users with a specific device count, click the relevant section on the pie chart. The system filters the page based on your selection and adds this filter to the Filter list.

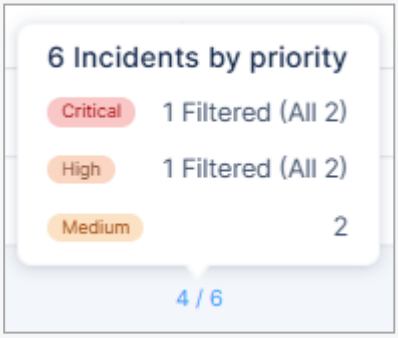
Example:

For the statistics displayed above, to view information about the two users with four related devices, click the pink section.



Users Table

The **Users** table is sorted by the priority of incidents related to the users. It shows:

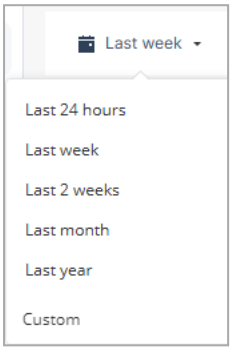
Item	Description
User name	Name of the user in the events and alerts processed by XDR.
Full name	Full name of the user.
Incidents priority	Highest priority level among all the related incidents.
Related incidents	Number of incidents in which the user is involved. Hover over the count to view the number of the filtered incidents (if applicable) and the total number of incidents. **Note** - Some incidents that impact a large number of assets are excluded from determining the Incident Priority. Such incidents are considered as **Filtered**.  To view the incidents details, click the count. The *"Incidents" on page 57* page appears.
Email addresses	Email address(es) of the user.
Related devices	Devices used by the user.
Domain	Domain(s) accessed by the user.
Last activity	Date of last activity by the user.

To sort the table, click the icon in the **Incidents priority** column.

To search for a specific user in the table, enter the user name in the **Search** field.

Filtering the Users Page

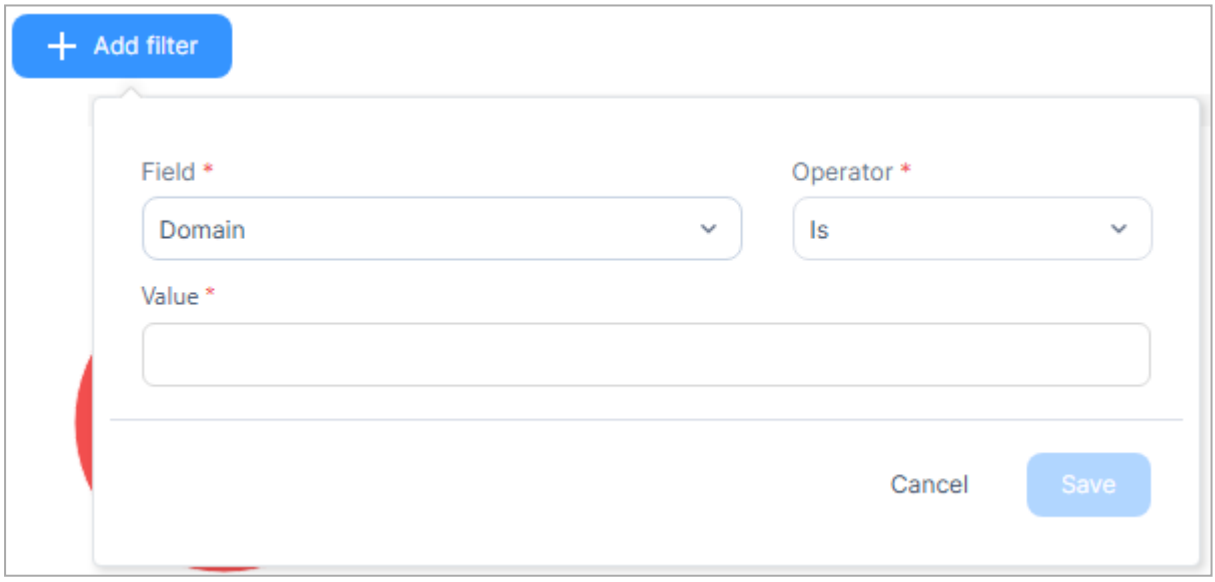
You can filter the information on the **Users overview** page for different time periods. The system shows information of users whose **Last activity** time is within the selected time period.



Adding Filters

To add a new filter:

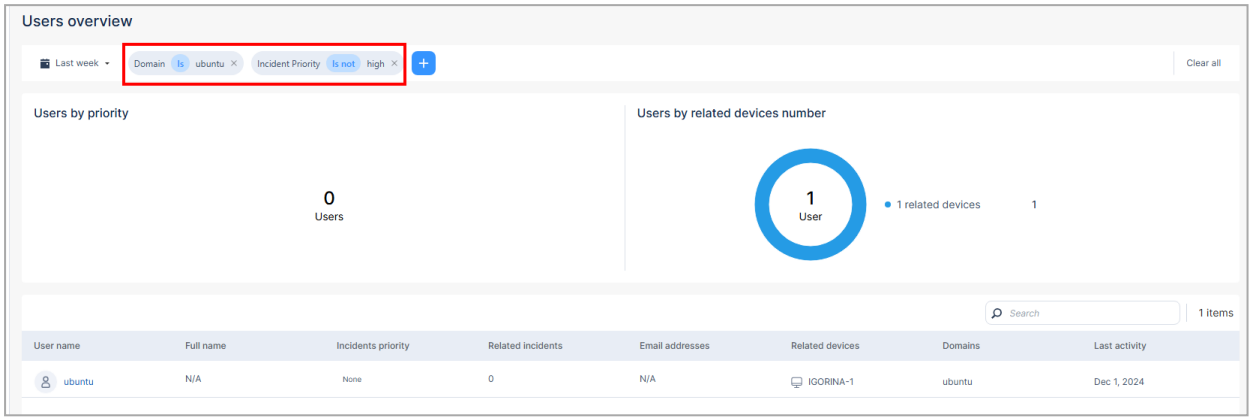
1. Click **+ Add Filter**.



2. Enter these details:
   a. **Field** - Select the user field.
   b. **Operator** - Select the operator to be applied.
   c. **Value** - Select the value of the user field.
3. Click **Save**.

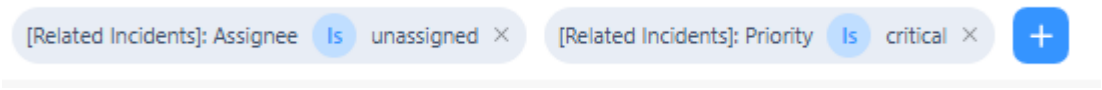
Note - You can add multiple filters.

The system updates the **Users overview** page based on all the active filters.



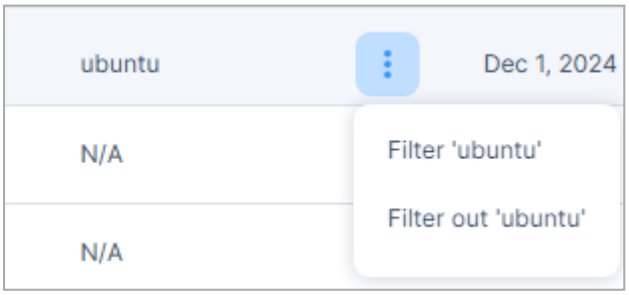
Note - You can define the filters below to specify the incidents to be considered to determine the **Incident priority** and **Related incidents**:

- **[Related Incidents]: Assignee** - Allows filtering to consider all incidents or only the unassigned ones. It helps you to prioritize incidents that have not yet been assigned to a team member, ensuring focus on new incidents.
- **[Related Incidents]: Priority** - Filters incidents with a specific priority level. It allows you to focus on incidents of a specific priority, for example, to consider only **High** priority incidents while ignoring other levels.



Filter In and Filter Out in Users Table

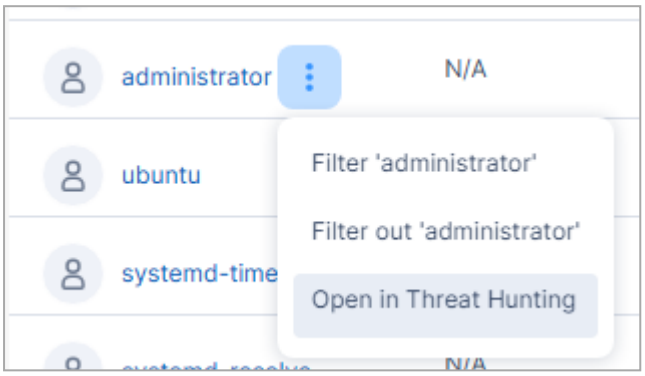
You can filter the **Users overview** page by either including (**Filter**) or excluding (**Filter out**) specific user fields in the Users table. To do that, hover over the field and click the ⋮ icon and then select the required option.



User Threat Hunting Details

To view the Threat Hunting details for the user:

1. Hover over the user name and click the ⋮ icon.
2. Click **Open in Threat Hunting**.

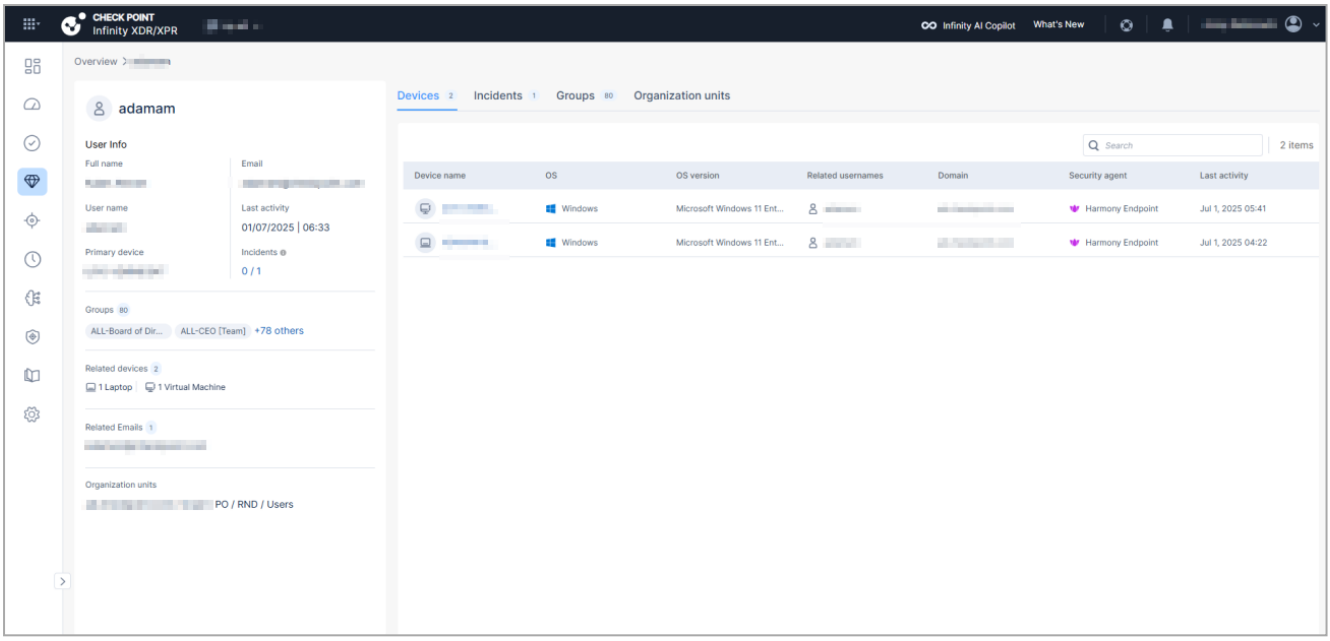


The Threat Hunting page appears and displays the Threat Hunting details for the user.

User - Related Devices, Incidents, Identity Provider (IdP) Groups and Organizational Unit

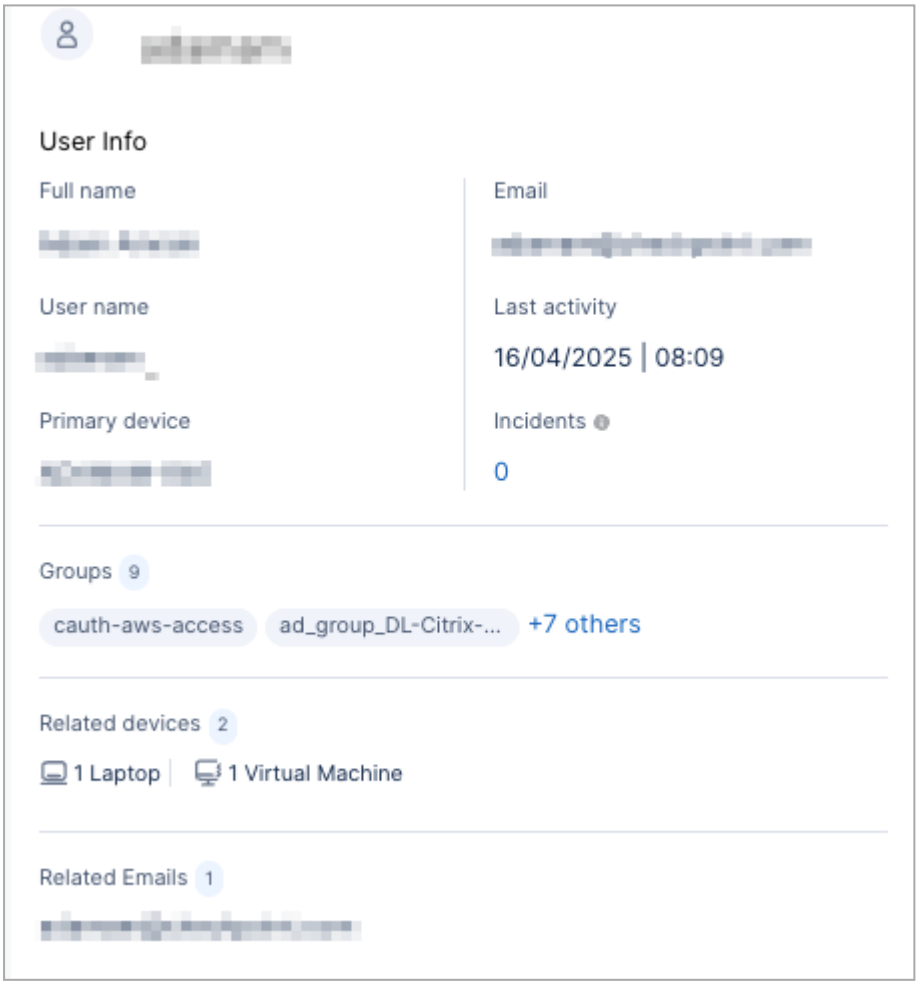
To view the devices, incidents and Identity Provider (IdP) groups related to a user, click the user name in **Users** table. The system shows:

- User information
- Devices used by the user
- Incidents in which the user was involved
- IdP groups in which the user is a member
- Organizational Unit (OU) hierarchy for assets



User Details

The **User Info** section displays the user details.

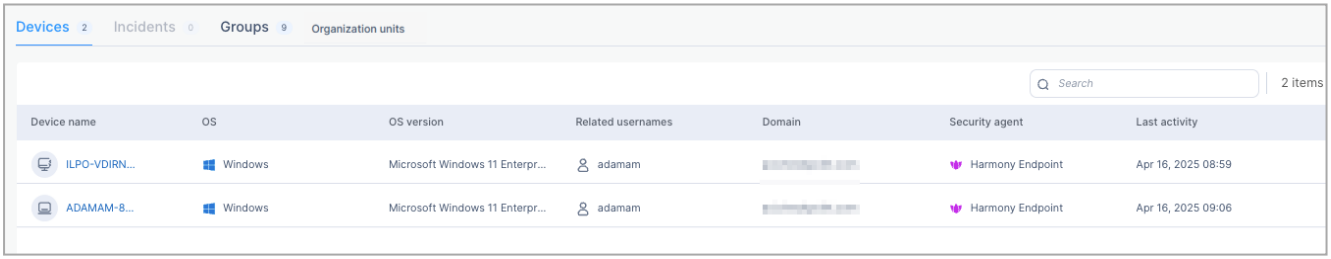


The **User Info** section shows:

Item	Description
Full name	Full name of the user.
Email	Email address of the user.
User name	Name of the user in the events and alerts processed by XDR.
Last activity	Date and time of last activity by the user.
Primary device	Main device the user uses.
Incidents	Number of incidents in which the user was involved during the past 30 days.
Groups	The Identity Provider (IdP) groups in which the user is a member.
Related devices	Devices the user has logged into.
Related Emails	Email addresses used by the user.

Users - Device Details

The **Devices** tab displays the devices used by the user.



The **Devices** table shows:

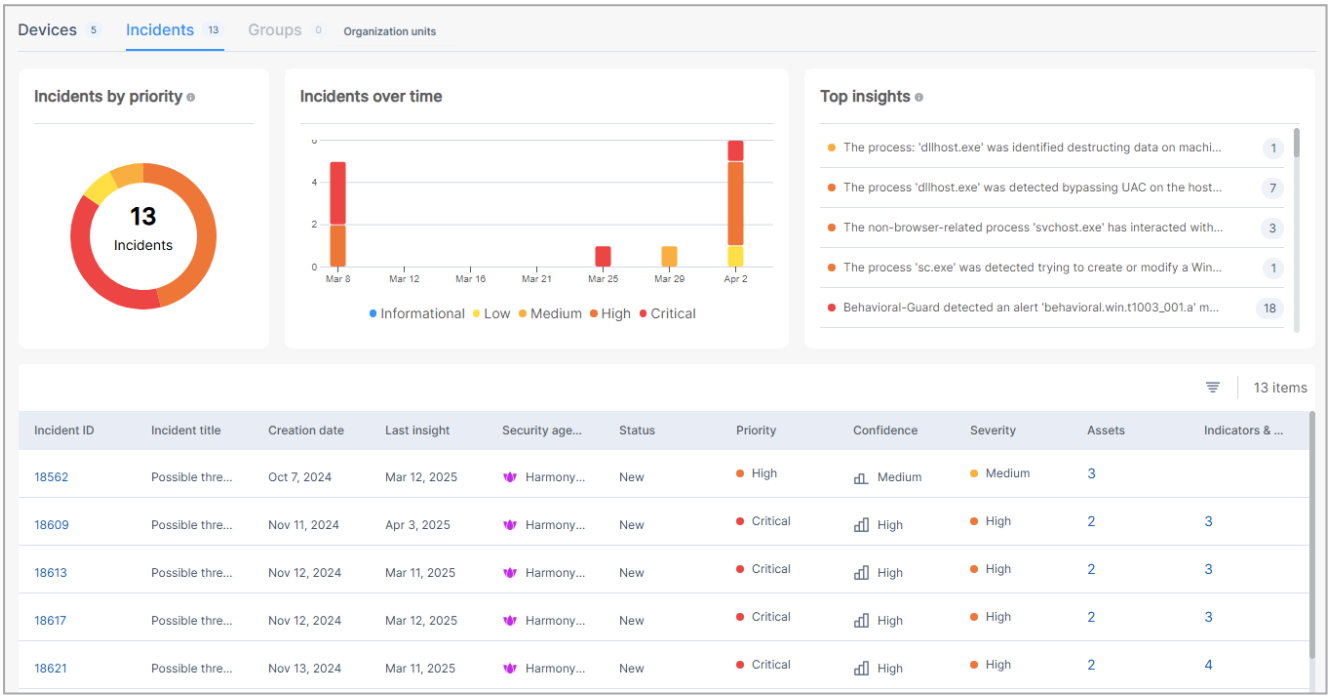
Item	Description
Device name	Name of the device.
OS	Operating System on the device.
OS version	Operating System version.
Related usernames	Users who have used the device.
Domain	Domains accessed on the device.
Security agent	Security agent running on the device.

Item	Description
Last activity	Date of last activity on the device.

To view more information about a device, click the device name.

Users - Incident Details

The **Incidents** tab displays the incidents in which the user was involved.



The **Incident** tab shows:

- **Incidents by priority** - Number of incidents in which the user was involved during the past 30 days, based on their priority.
- **Incidents over time** - Timeline of incidents during the past 30 days. Incidents are color-coded based on the priority levels.
- **Top insights** - Top insights in which the user was involved during the past 30 days.

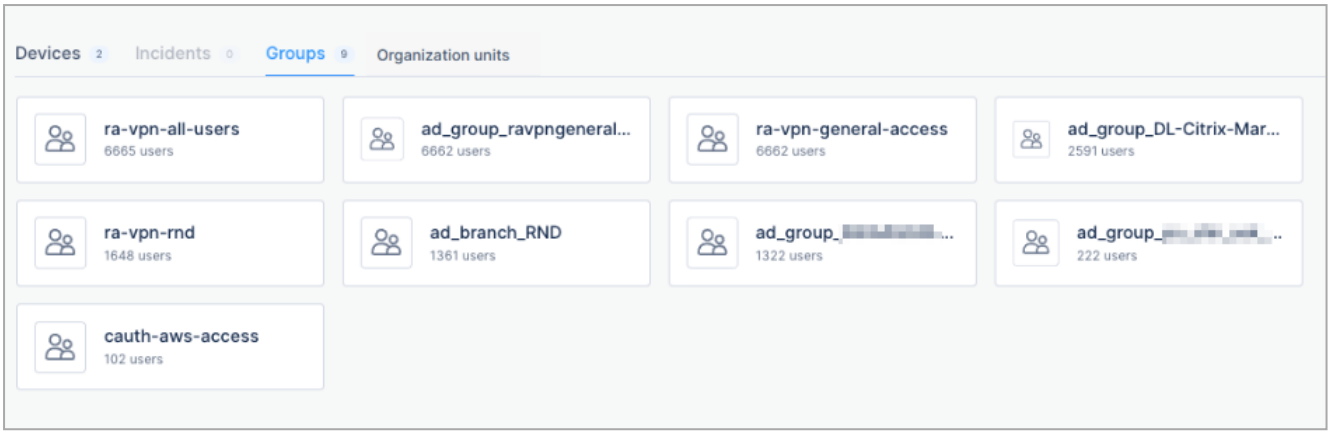
- **Incidents table**:

Item	Description
Incident ID	ID of the incident. To view more information about an incident, click the ID. The *"Incidents - Overview" on page 64* page appears.
Incident title	Title of the incident.
Creation date	Date on which the incident was generated.
Last insight	Date when the last insight was created for the incident.
Security agents	Security agent(s) running on the device
Status	Status of the incident.
Priority	Priority level of the incident.
Confidence	Confidence level of the security event detection.
Severity	Severity level of the incident.
Assets	Number of affected assets in the incident. To view the asset details, click the count link. The *"Incidents - Affected Assets" on page 94* page appears.
Indicators & Artifacts	Number of indicators and artifacts involved in the incident. To view more details on the indicators and artifacts, click the count link. The *"Incidents - Indicators & Artifacts" on page 101* page appears.

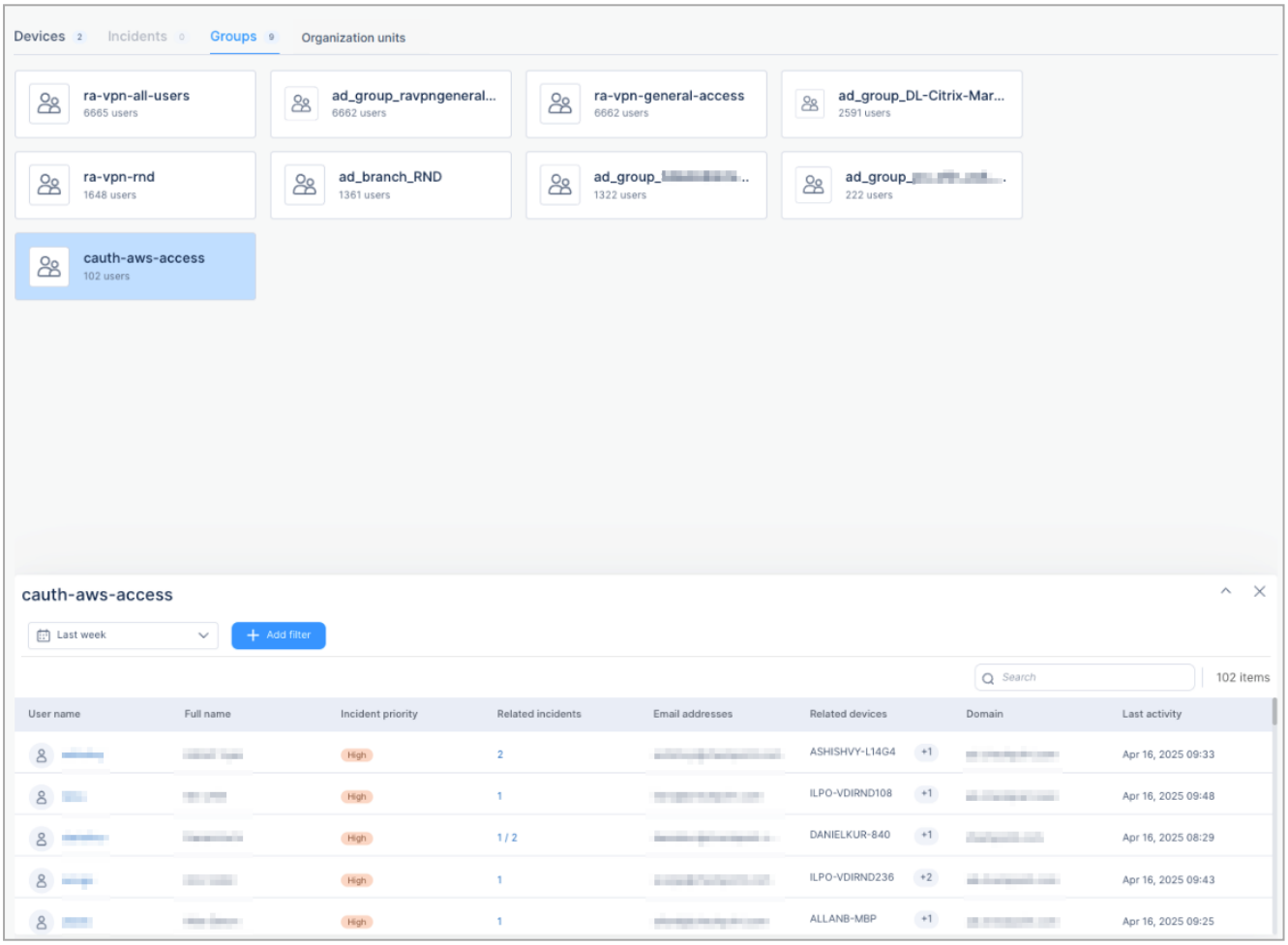
To filter the Incidents table, click the icon.

Users - Group Details

The **Groups** tab displays the Identity Provider (IdP) groups in which the user is a member. Each group card displays the number of users in that IdP group.



To view details of the users in an IdP group, click the group card. The system displays the Users table for that IdP group at the bottom of the page.

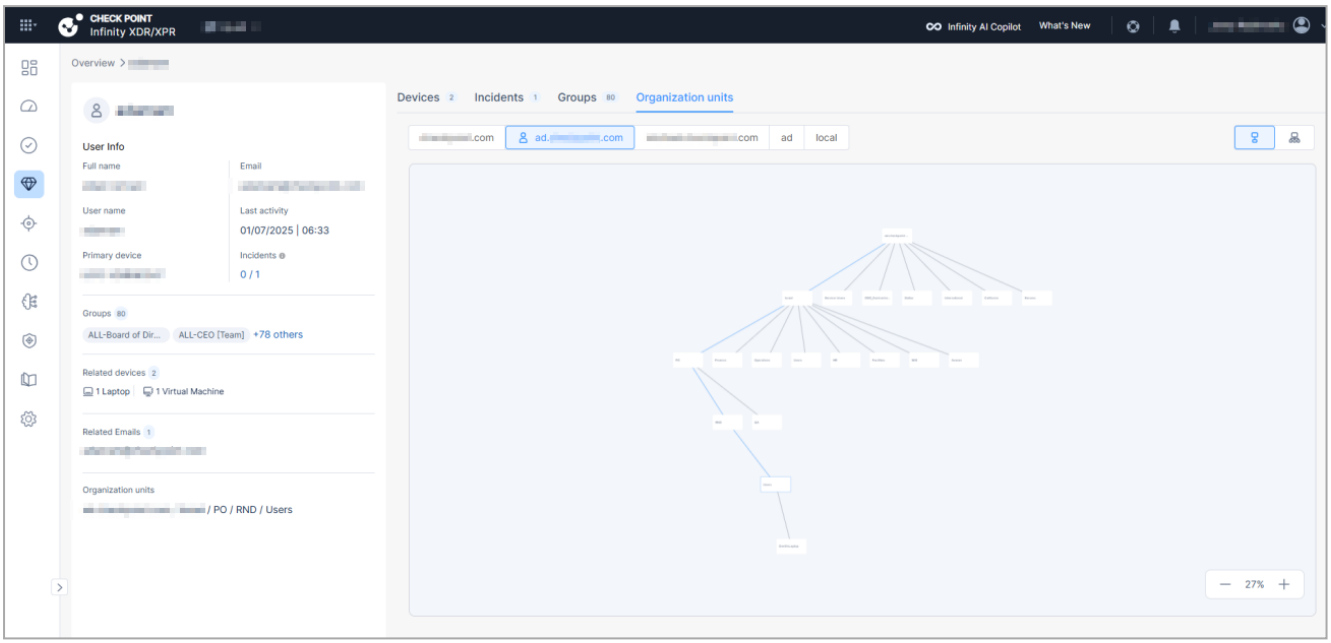


By default, it shows details of users whose **Last activity** date is within the past seven days.

To filter the Users table, see *"Filtering the Users Page" on page 142*.

Users - Organizational Units Tree Details

The **Organization Units** tab displays the full Organizational Unit (OU) hierarchy for assets in the platform.



The **Organizational units** tab shows:

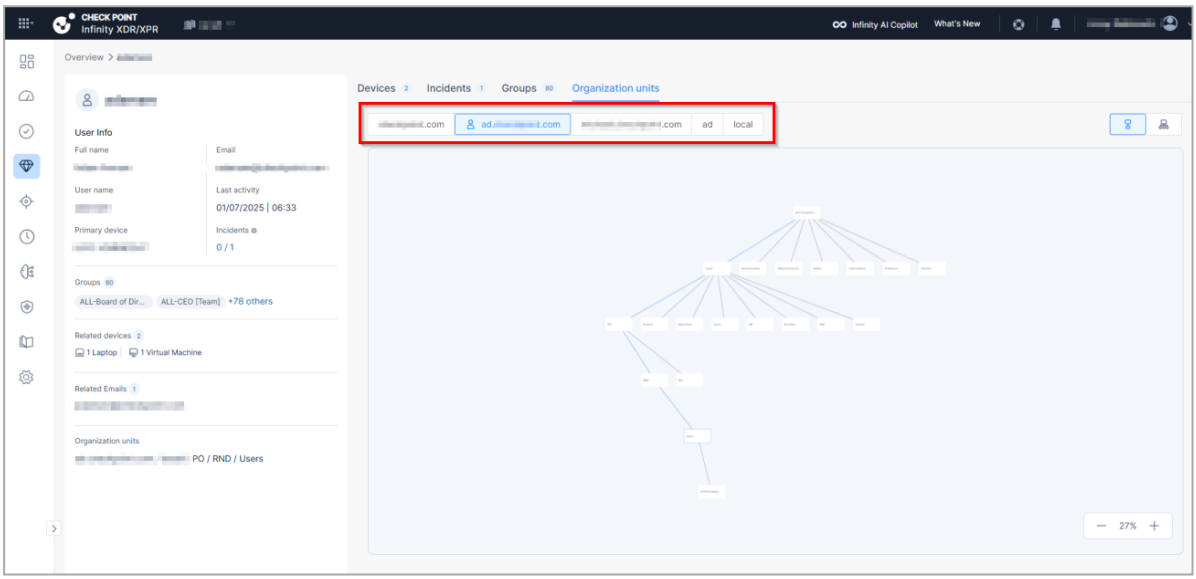
- A tree structure of OUs.
- Where the asset is located within your organization's structure.
- **User Info** section:

Item	Description
Full name	Full name of the user.
User name	Name of the user in the events and alerts processed by XDR.
Primary device	Main device the user uses.
Email	Email address of the user.
Last activity	Date and time of last activity by the user.
Incidents	Number of incidents in which the user was involved during the past 30 days.
Groups	The Identity Provider (IdP) groups in which the user is a member.
Related devices	Devices the user has logged into.

Item	Description
Related Emails	Email addresses used by the user.
Organization units	Displays the user's path in the organization's hierarchy, for example, `acme.com/Internationsal/India/NPO/Users`.

Notes:

- The OU tree is read-only.
- If there are multiple domains, by default, the system selects the OU linked to the asset.

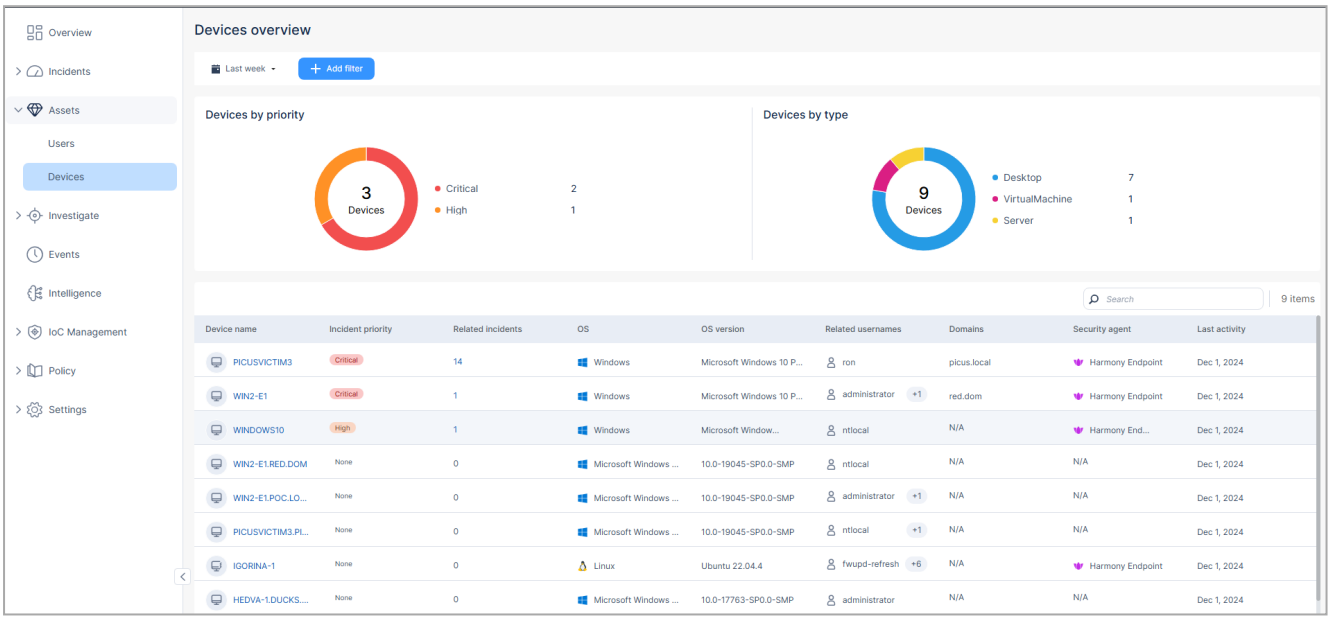


- The blue line highlights the full path from the root to the asset's organizational unit in the hierarchy.

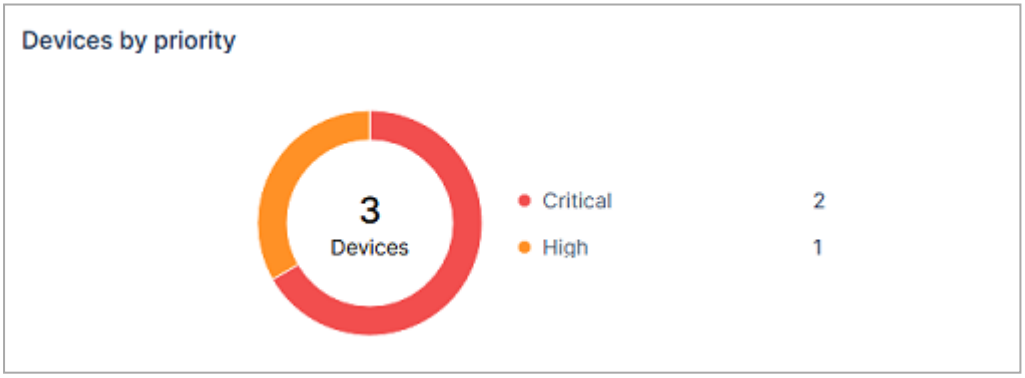
Devices

The **Devices** page shows information about the device assets in your account and the details of related users, incidents and Identity Provider (IdP) groups.

To view the **Devices** page, access the XDR Administrator Portal and click **Assets** > **Devices**. By default, it shows details of devices whose **Last activity** date is within the past seven days.

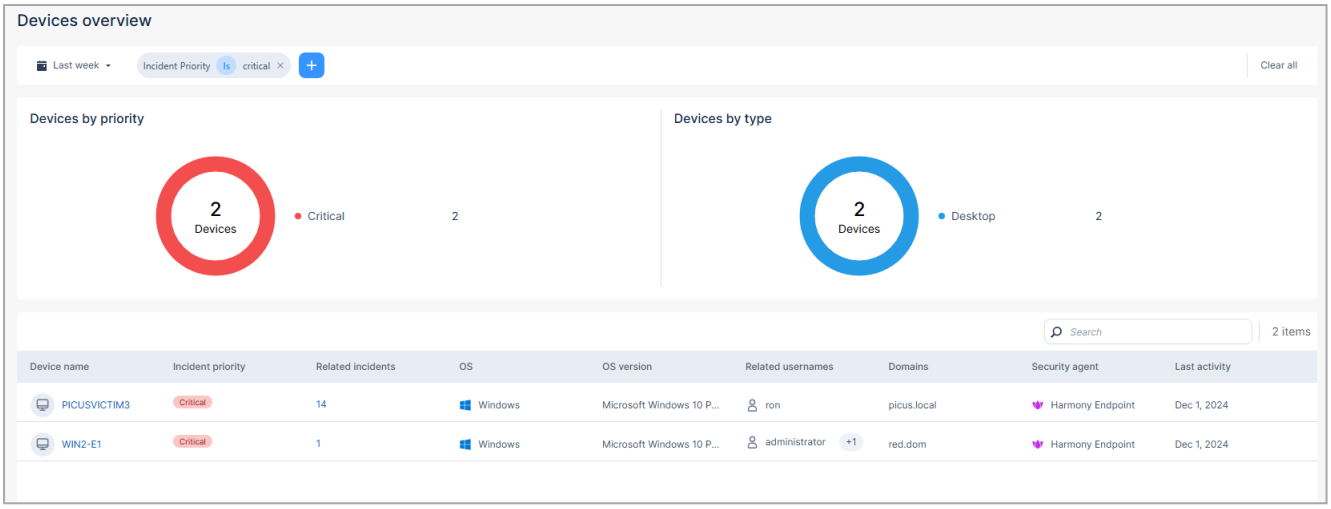


Devices by Priority

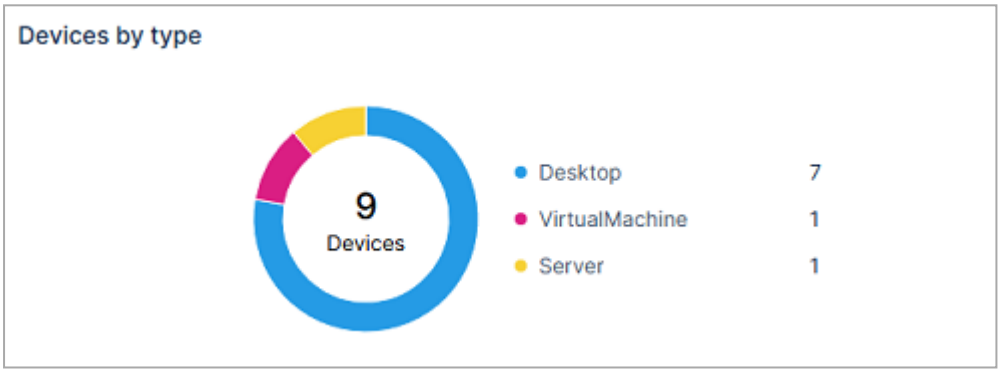


The **Devices by priority** widget shows the number of devices based on the priority level of the incidents they are involved in, within the selected time period.

To filter the **Devices overview** page according to a specific priority level, click the relevant section on the pie chart. The system filters the page based on your selection and adds this filter to the Filter list.



Devices by Type

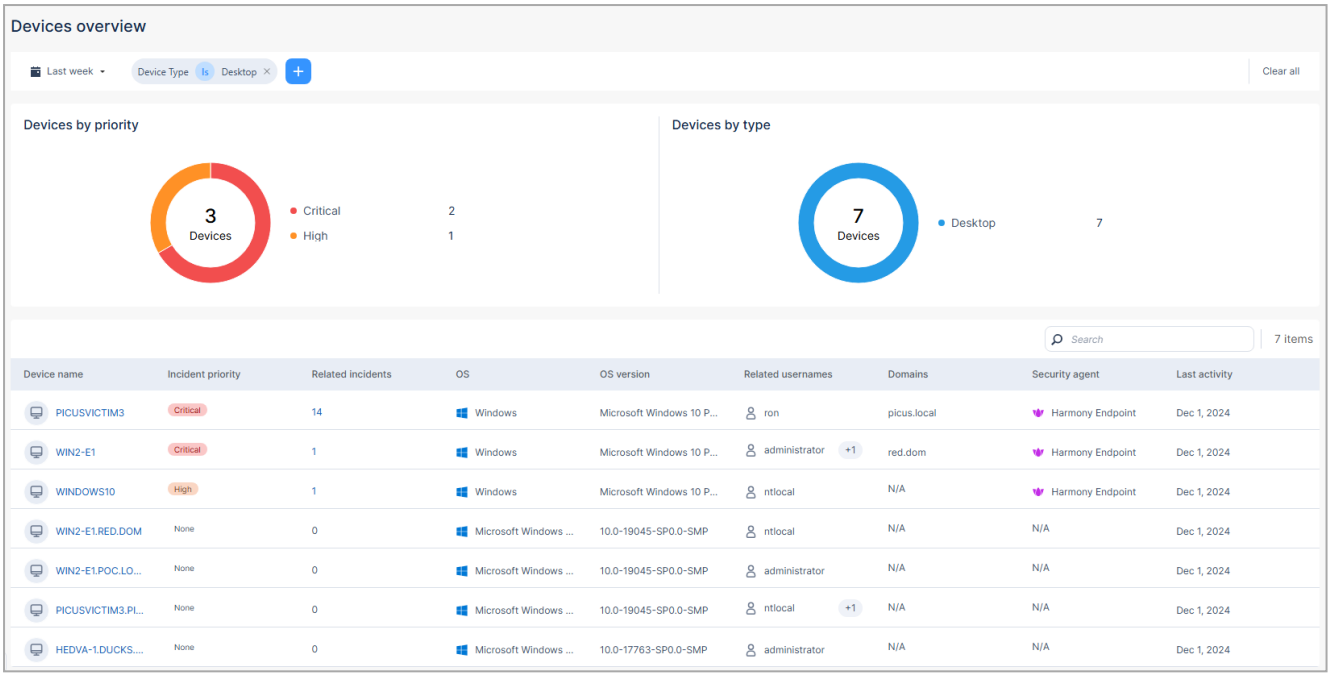


The **Devices by type** widget shows the total number of devices and the statistics of device types, within the selected time period.

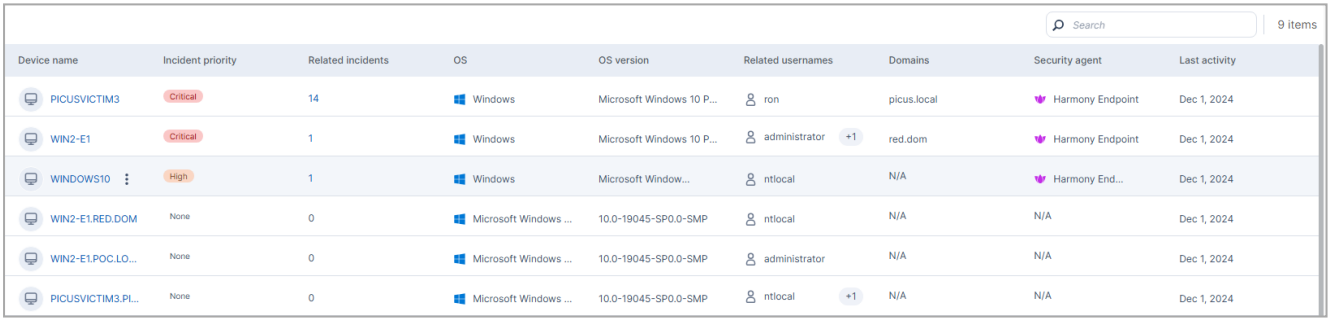
To view the information of devices in a specific device type, click the relevant section on the pie chart. The system filters the page based on your selection and adds this filter to the Filter list.

Example:

For the statistics displayed above, to view information about the seven desktop devices, click the blue section.

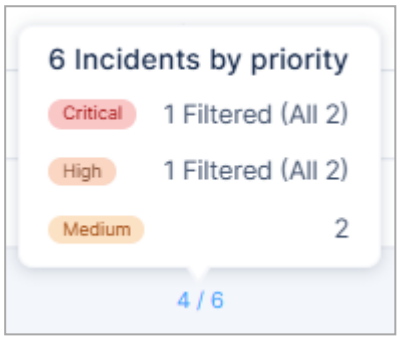


Devices Table



The **Devices** table is sorted by the priority of incidents related to the devices. It shows:

Item	Description
Device name	Name of the device.
Incidents priority	Highest priority level among all the related incidents.

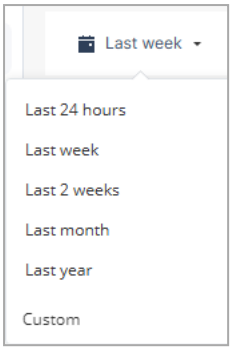
Item	Description
Related incidents	Number of incidents in which the device is involved. Hover over the count to view the number of the filtered incidents (if applicable) and the total number of incidents. **Note** - Some incidents that impact a large number of assets are excluded from determining the Incident Priority. Such incidents are considered as **Filtered**.  To view the incidents details, click the count. The *"Incidents" on page 57* page appears.
OS	Operating System on the device.
OS version	Operating System version.
Related usernames	Users who have used the device.
Domains	Domains accessed on the device.
Security agent	Security agent running on the device.
Last activity	Date of last activity on the device.

To sort the table, click the icon in the **Incidents priority** column.

To search for a specific device in the table, enter the device name in the **Search** field.

Filtering the Devices Page

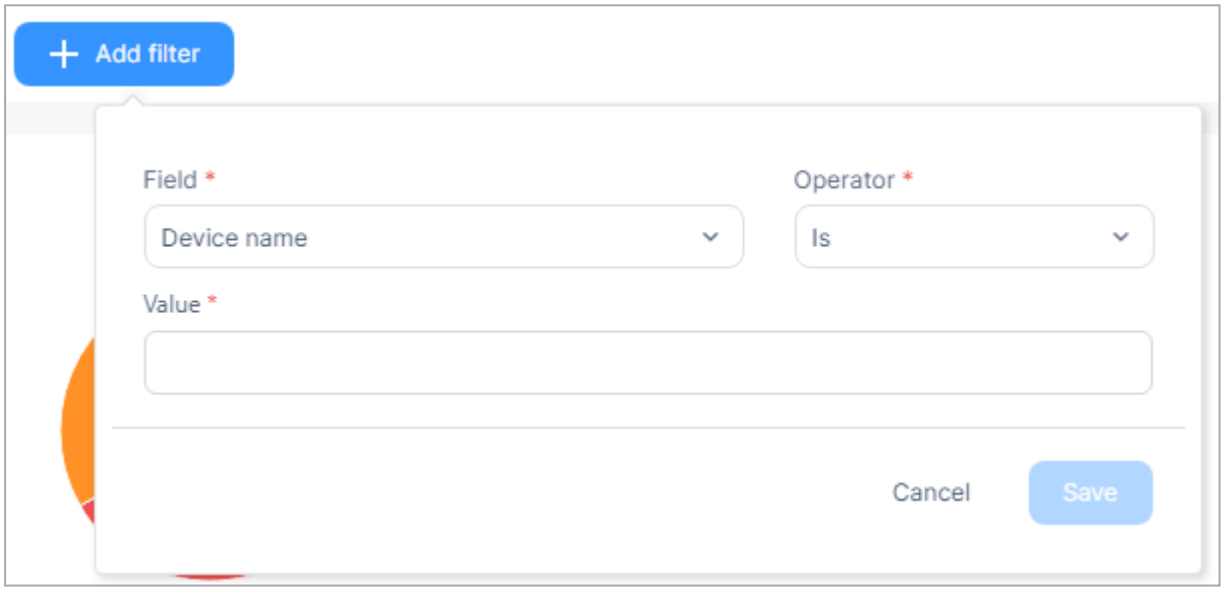
You can filter the information on the **Devices overview** page for different time periods. The system shows information of devices whose **Last activity** time is within the selected time period.



Adding Filters

To add a new filter:

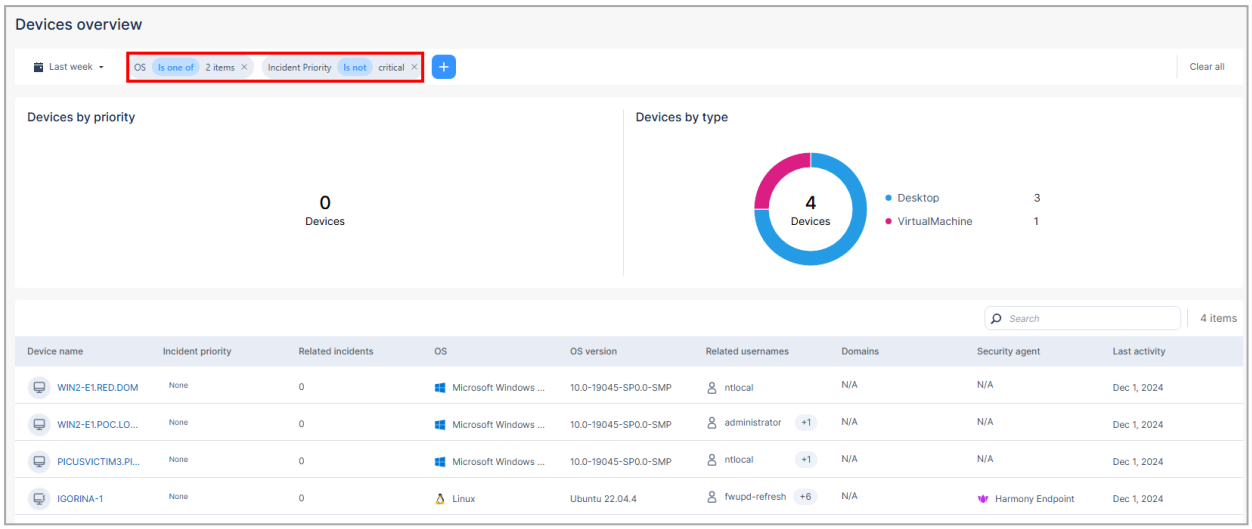
1. Click **+ Add Filter**.



2. Enter these details:
   a. **Field** - Select the device field.
   b. **Operator** - Select the operator to be applied.
   c. **Value** - Select the value of the device field.
3. Click **Save**.

Note - You can add multiple filters.

The system updates the **Devices overview** page based on all the active filters.

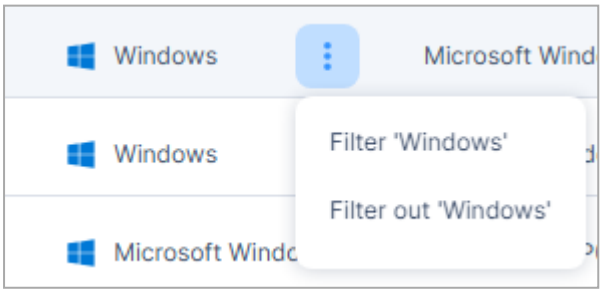


Note - You can define the filters below to specify the incidents to be considered to determine the **Incident priority** and **Related incidents**:

- **[Related Incidents]: Assignee** - Allows filtering to consider all incidents or only the unassigned ones. It helps you to prioritize incidents that have not yet been assigned to a team member, ensuring focus on new incidents.
- **[Related Incidents]: Priority** - Filters incidents with a specific priority level. It allows you to focus on incidents of a specific priority, for example, to consider only **High** priority incidents while ignoring other levels.

Filter In and Filter Out in Devices Table

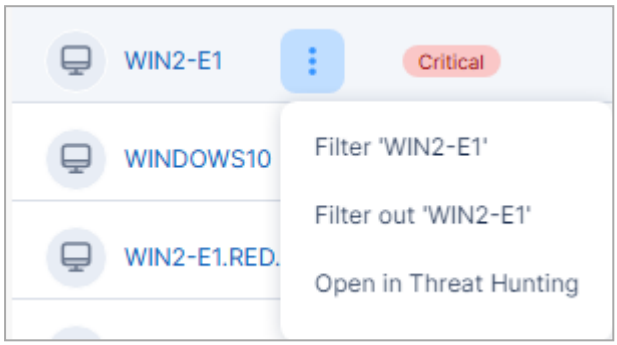
You can filter the **Devices overview** page by either including (**Filter**) or excluding (**Filter out**) specific device fields in the Devices table. To do that, hover over the field and click the ⋮ icon and then select the required option.



Device Threat Hunting Details

To view the Threat Hunting details for the device:

1. Hover over the device name and click the ⋮ icon.
2. Click **Open in Threat Hunting**.

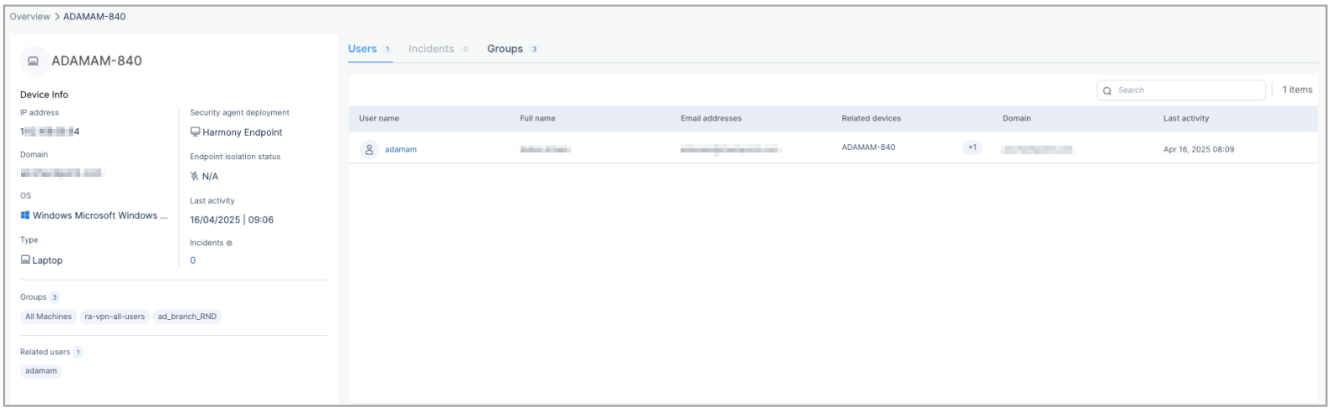


The Threat Hunting page appears and displays the Threat Hunting details for the device.

Device - Related Users, Incidents and IdP Groups

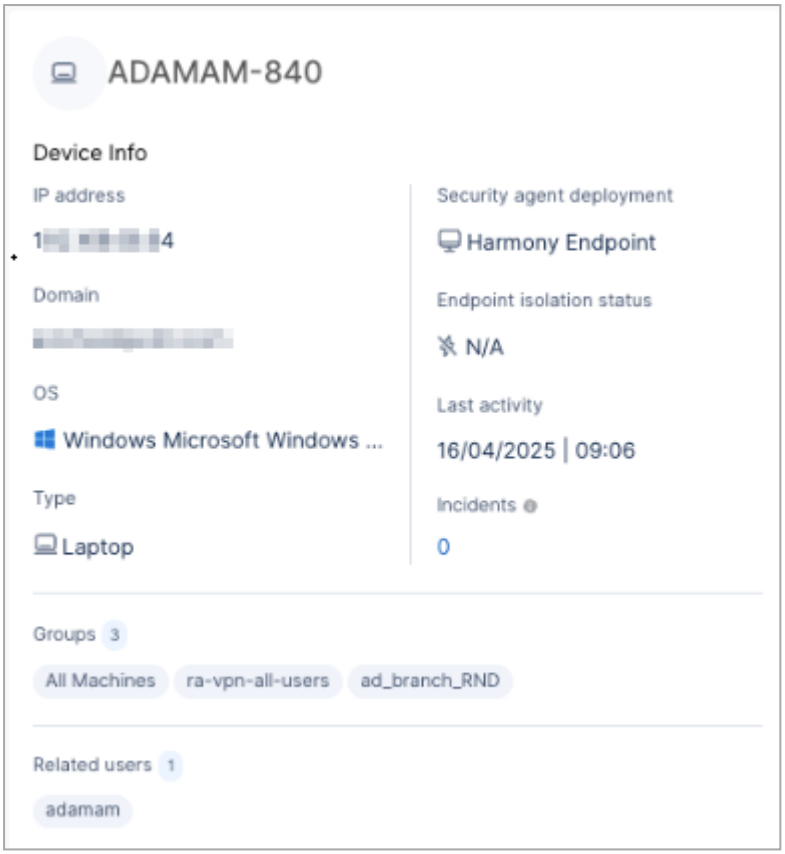
To view the users, incidents and Identity Provider (IdP) groups related to a device, click the device name in **Devices** table. The system shows:

- Device information
- Details of users who have used the device
- Incidents in which the device was involved
- IdP groups in which the device is a member



Device Details

The **Device Info** section displays the device information.



The **Device Info** section shows:

Item	Description
IP address	IP address of the device.
Domain	Domain accessed on the device.
OS	Operation System on the device.
Type	Type of the device.
Security agent deployment	Security agent running on the device.
Endpoint isolation status	Shows whether endpoint was isolated (disconnected from network).
Last activity	Date and time of last activity on the device.
Incidents	Number of incidents in which the device was involved during the past 30 days.
Groups	The Identity Provider (IdP) groups in which the device is a member.

Item	Description
Related users	Users who have used the device.

Devices - User Details

The **Users** tab displays the details of users who have used the device.

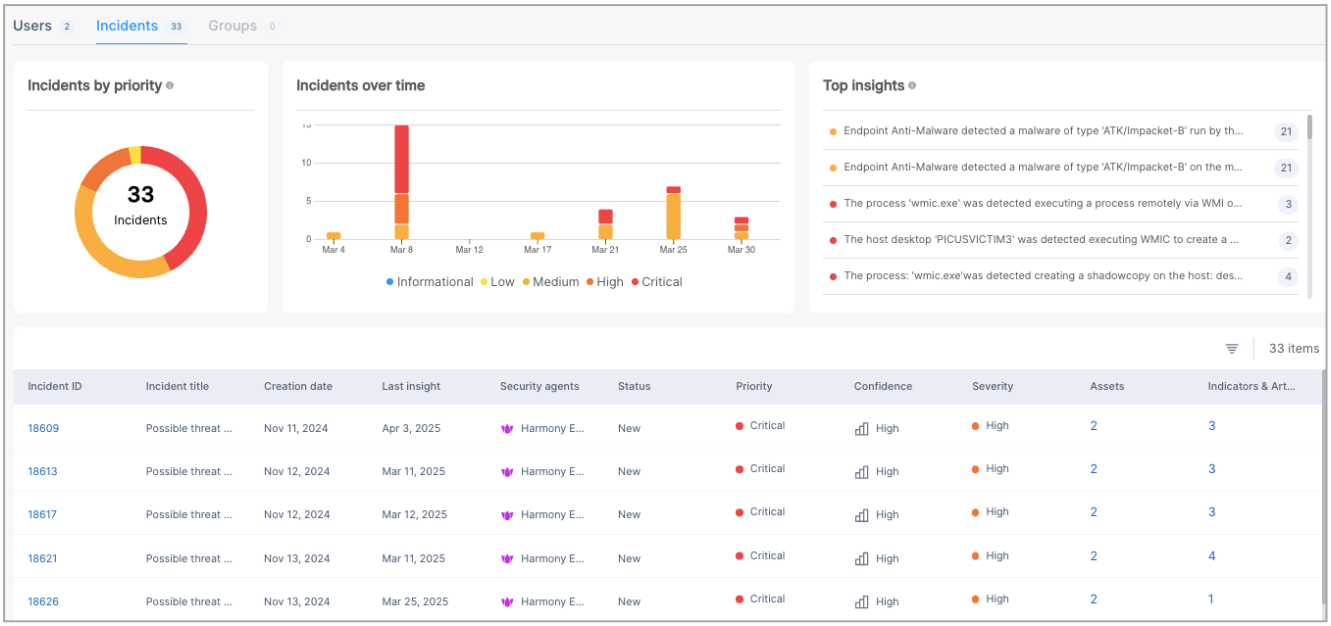
The **Users** table shows:

Item	Description
User name	Name of the user in the events and alerts processed by XDR.
Full name	Full name of the user.
Email addresses	Email address(es) of the user.
Related devices	Devices used by the user.
Domain	Domain(s) accessed by the user.
Last activity	Date of last activity by the user.

To view more information about a user, click the user name.

Devices - Incident Details

The **Incidents** tab displays the incidents in which the device was involved.



The **Incident** tab shows:

- **Incidents by priority** - Number of incidents in which the device was involved during the past 30 days, based on their priority.
- **Incidents over time** - Timeline of incidents during the past 30 days. Incidents are color-coded based on the priority levels.
- **Top insights** - Top insights in which the device was involved during the past 30 days.

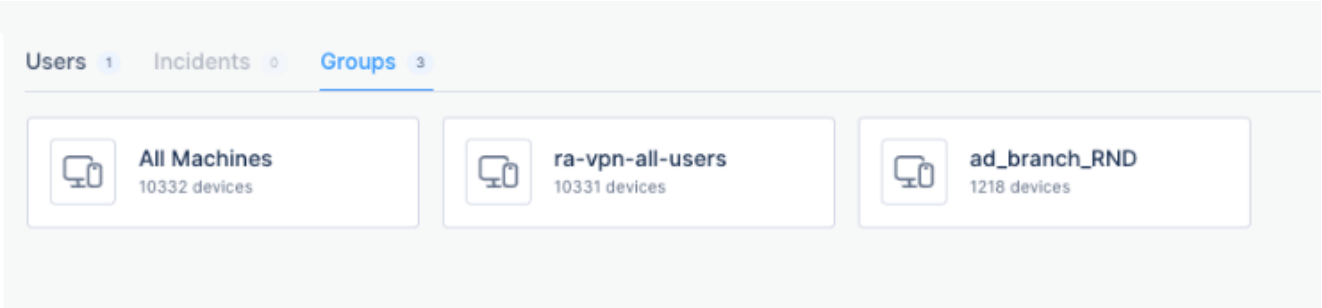
- **Incidents table**:

Item	Description
Incident ID	ID of the incident. To view more information about an incident, click the ID. The *"Incidents - Overview" on page 64* page appears.
Incident title	Title of the incident.
Creation date	Date on which the incident was generated.
Last insight	Date when the last insight was created for the incident.
Security agents	Security agent(s) running on the device
Status	Status of the incident.
Priority	Priority level of the incident.
Confidence	Confidence level of the security event detection.
Severity	Severity level of the incident.
Assets	Number of affected assets in the incident. To view the asset details, click the count link. The *"Incidents - Affected Assets" on page 94* page appears.
Indicators & Artifacts	Number of indicators and artifacts involved in the incident. To view more details on the indicators and artifacts, click the count link. The *"Incidents - Indicators & Artifacts" on page 101* page appears.

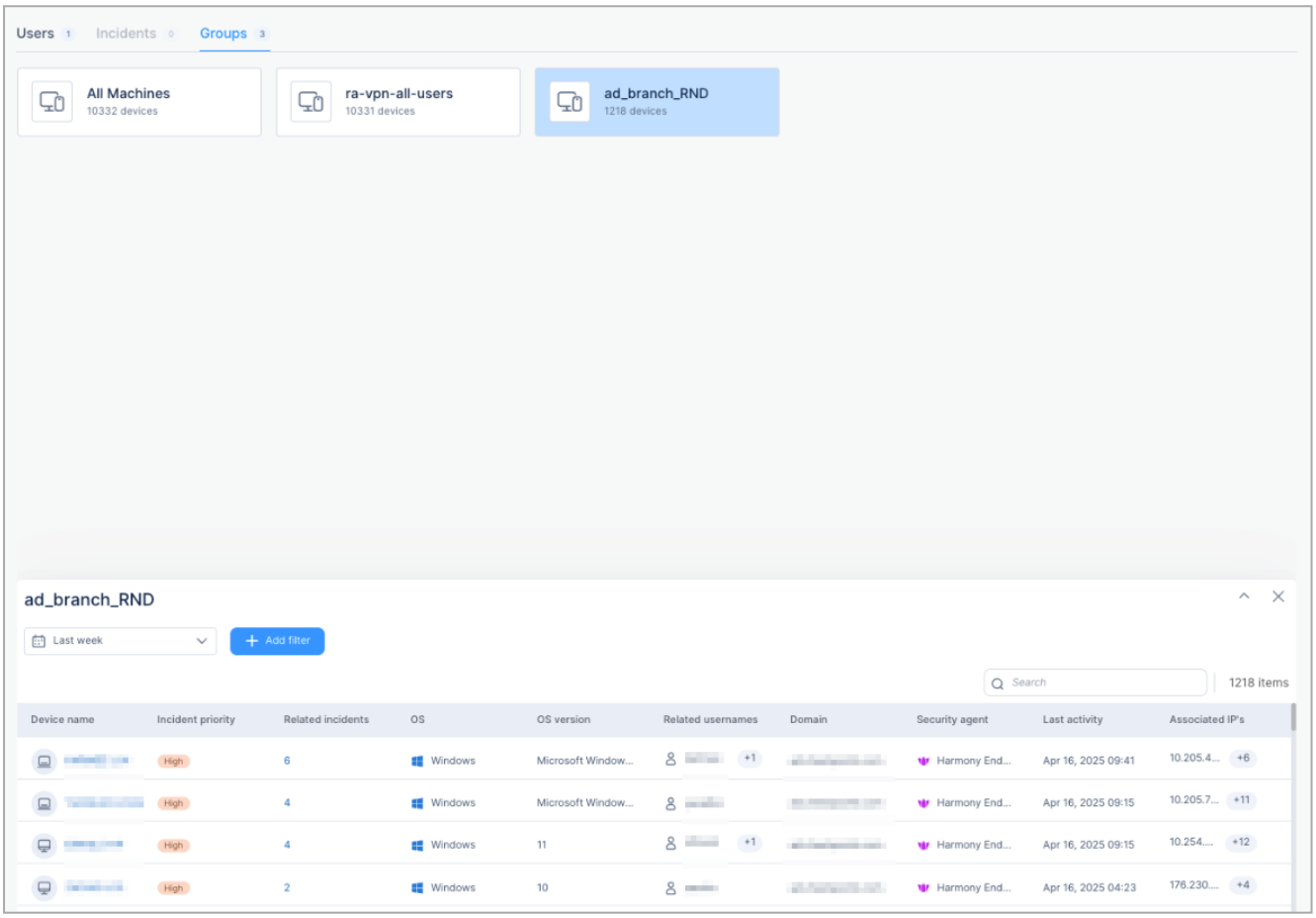
To filter the Incidents table, click the icon.

Devices - Group Details

The **Groups** tab displays the Identity Provider (IdP) groups in which the device is a member. Each group card displays the number of devices in that IdP group.



To view the details of devices in an IdP group, click the group card. The system displays the Devices table for that IdP group at the bottom of the page.



By default, it shows details of devices whose **Last activity** date is within the past seven days.

To filter the Devices table, see *"Filtering the Devices Page" on page 155*.

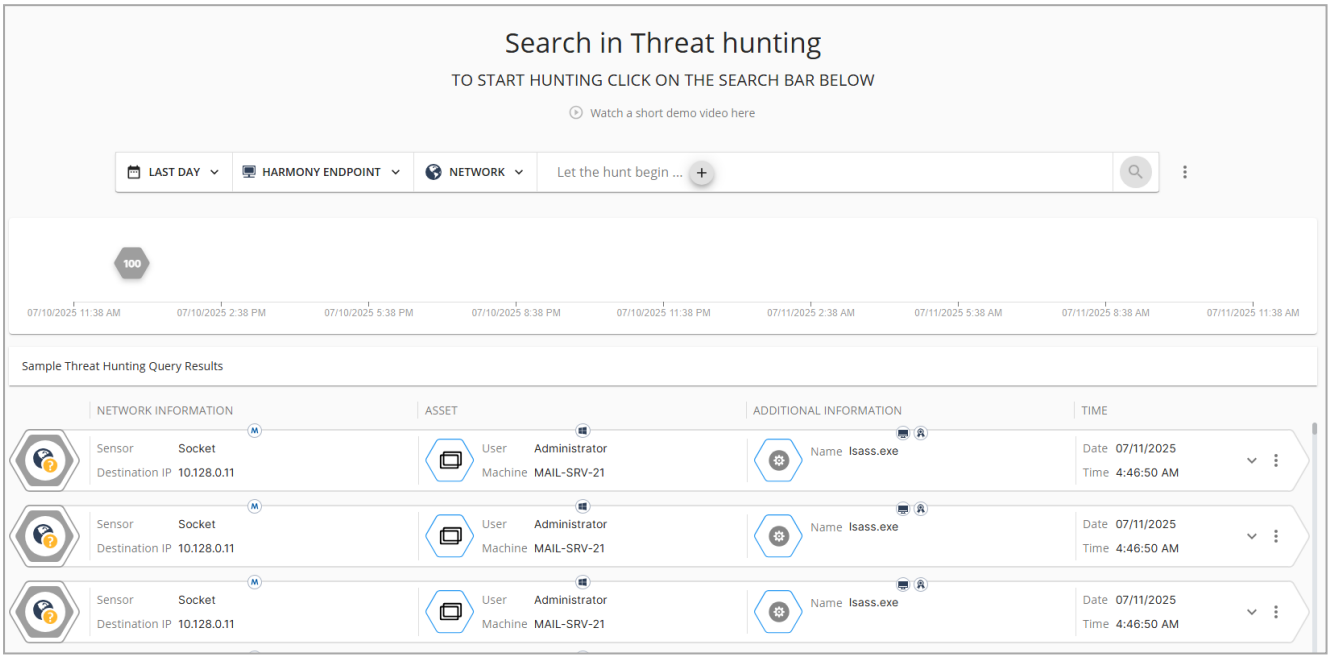
Investigate

In the **Investigate** section, you can view modes of incident investigation.

- *"Threat Hunting" on page 165*
- *"Threat Topology Map" on page 172*

Threat Hunting

Threat Hunting is an investigative tool which allows for advanced querying on all malicious and benign forensics events collected from the onboarded Endpoint Security and Quantum Security Gateway.



The information collected lets you to:

- Investigate the full scope of an attack.
- Discover stealth attack by observation of a suspicious activity.
- Remediate the attack before it causes further damage.
- Proactively hunt for advanced attacks by searching for anomalies, and using hunting leads and enrichment.

Threat Hunting supports:

- Data collection and enrichment - All events are collected through multiple sensors and sent to a unified repository and enhanced by ThreatCloud, MITRE mapping and alerts from all the prevention engines.
- Rich toolset for custom queries, drill down and pivoting to suspicious activity.
- Predefined queries and a MITRE dashboard which map all activity and allow a quick start to proactive hunting.
- Remediation actions per result or a bulk operation integrated in the Threat Hunting flow (such as file quarantine and kill process).

Supported Regions

Threat Hunting is supported only for the Check Point Portal tenants (accounts) residing in these regions:

- Australia
- EU
- India
- United Kingdom
- United Arab Emirates
- US

Supported Versions

- For Endpoint Security, Endpoint Security Client version E84.10 and higher.

Enabling Threat Hunting

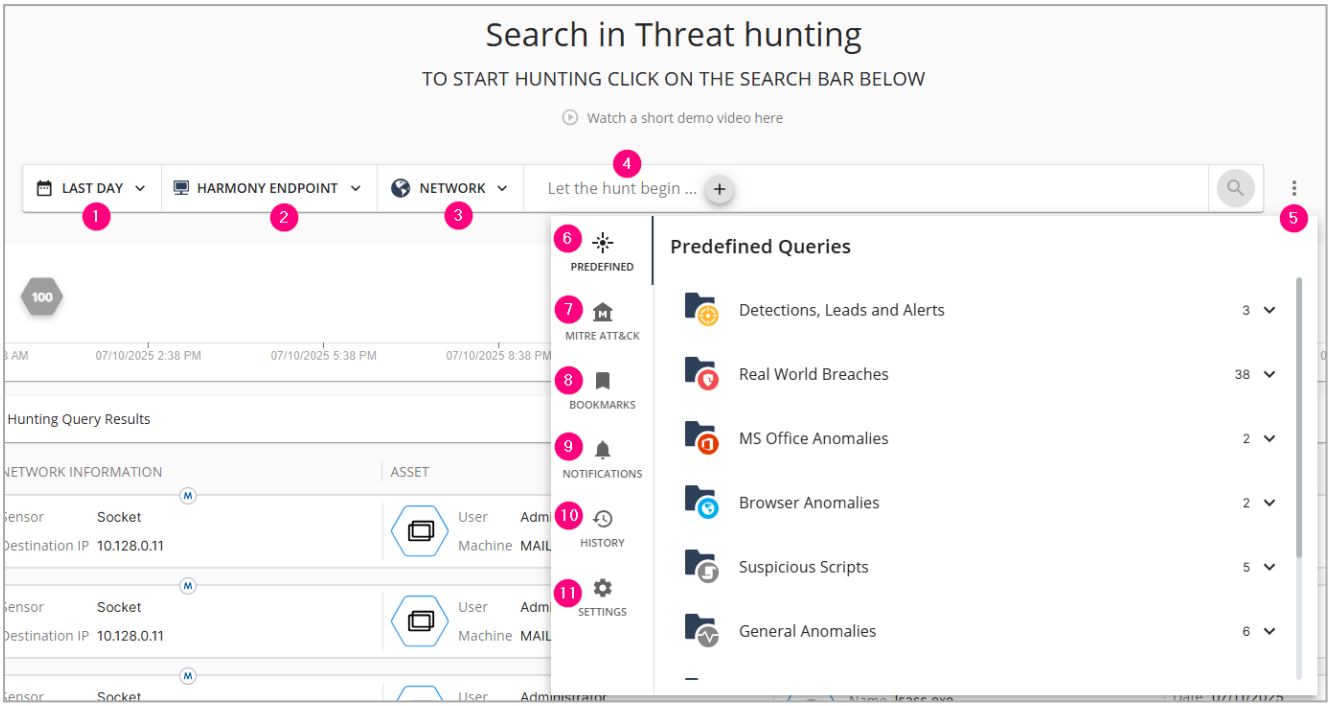
By default, Threat Hunting is disabled in Endpoint Security.

To enable Threat Hunting:

1. Go to **Policy** > **Policy Capabilities**.
2. Click the **Analysis & Remediation** tab.
3. From the **Enable Threat Hunting** list, select **On**.
4. Click **Save & Install**.
5. After the policy is pushed to the agents, wait a few minutes until data is sent by the agents.

   Then you can go to the **Threat Hunting** view to start searching through events.

Using Threat Hunting



Item	Description
1	**Last Day** - Time filter for the query. Users can choose between **Last Day**, **Last 2 Days**, **Last Week** and a **Custom** time period.
2	**Data Sources** - Filter events by onboarded products. By default, all the data sources are selected. To filter events, click **Data Sources** and select the required product(s).
3	**Process** - Refine your query results according to the activity type.
4	**Let the hunt begin** - Click **+** and define the values to search in the logs. You can add multiple values and fields at a time.
5	Menu for predefined queries.
6	**Predefined** - Check Point's predefined queries, divided by category. **Note - Leads** in **Detections, Leads and Alerts** are lead detections or signatures. If an incident is raised under this category, the term **Lead.** is prefixed to its protection name. For example, **Lead.Win.BrwsrPassThft.B**. It does **NOT** indicate an attack and we recommend that you ignore these incidents. This is used by Check Point to analyze if a protection has to be developed. For example, create a new signature.

Item	Description
7	**MITRE ATT&CK** - Shows the **MITRE ATT&CK** framework of tactics and techniques. Each technique includes one or more queries, pre-defined by *Check Point Research*.
8	**Bookmarks** - Shows the custom queries saved as bookmarks, either as global (available for all users in the account) or private (available only for the user). Users can also define email notifications for these saved queries, currently limited to 10. For more information, see *"Saving a Query as a Bookmark" on page 171*.
9	**Notifications** - Shows the list of recipients that receive email notifications if Threat Hunting events match the custom query. To add recipients, see Threat Hunting Email Notifications.
10	**History** - See all the queries that you used.
11	**Settings** - Change the UI look and feel.

To hunt for threats, you can use predefined queries or by proactively creating your own queries.

- To use predefined queries:

  1. Go to **Predefined Hunting Queries** or

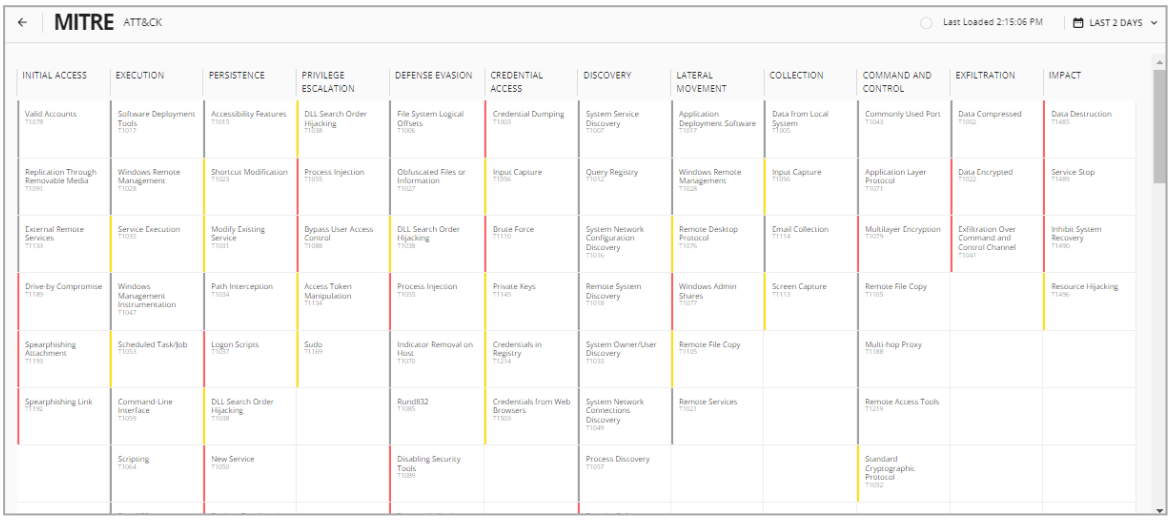
     Click the ⋮ icon next to the search box and select **Predefined**.

     You can quickly find all active attacks and browse through different malicious events detected by Endpoint clients.

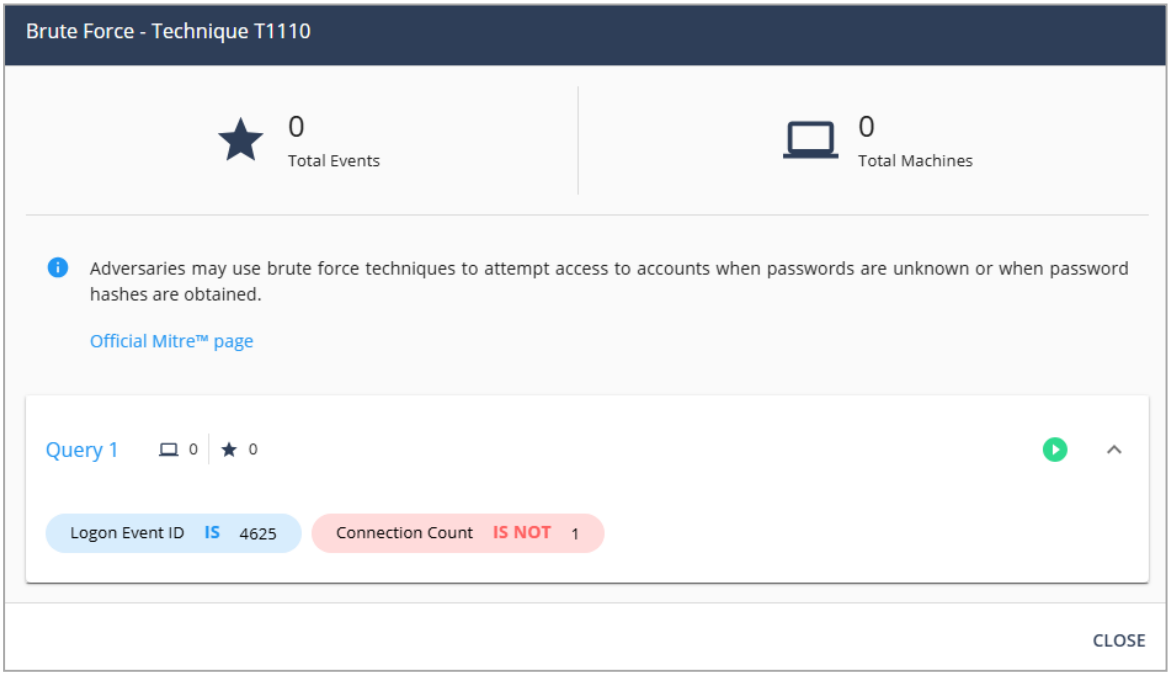
2. Click the ⋮ icon next to the search box and select **MITRE ATT&CK**.

   The **MITRE ATT&CK** dashboard provides real-time visibility on all the techniques observed by Endpoint Security across your endpoints. It maps all raw events to MITRE Tactics, Techniques, and Procedures (TTPs) regardless of status.

   The **MITRE ATT&CK** dashboard is divided into 12 categories and each category is a stage in an attack. Each category includes multiple attack techniques.

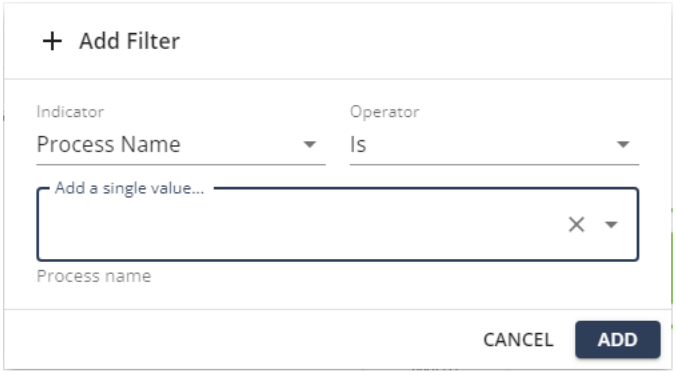


   When you click a technique, a window opens with an explanation about the technique and a list of predefined queries. Run a query to get a list of the events in which the specific technique implementation was used.



- To search for specific events by proactively creating your own queries:

1. Go to **Threat Hunting**.
2. Click the **+** sign next to **Let the hunt begin**.
3. From the **Indicator** list, select the filter.



4. From the **Operator** list, select the condition.
5. In the **Add a single value** field, enter a value for the indicator.
6. Click **Add**.

   It shows the search results in a timeline. The timeline provides behavioral insights that indicate anomalies or attacks.
7. To add another filter to the same query, repeat steps 2 to 6.

   Note - If you have multiple filters, the system applies the logical **AND** operator between the filters.
8. To filter events based on the timeline, click the required hexagon.

   It shows detailed information about the event, together with intelligent enrichment, such as attack classification, malware family and MITRE technique details.
9. To create a bookmark for a query, see *"Saving a Query as a Bookmark" on the next page*.
10. You can also filter the results by date and process.
11. To take remediation action for the filtered results, click **Actions** and choose any of these:
    - **Terminate Process**
    - **Quarantine File**
    - **Trigger Forensic Analysis**
    - **Isolate Machine**
12. To export the results to a CSV file, click **Actions** > **Export to CSV**.

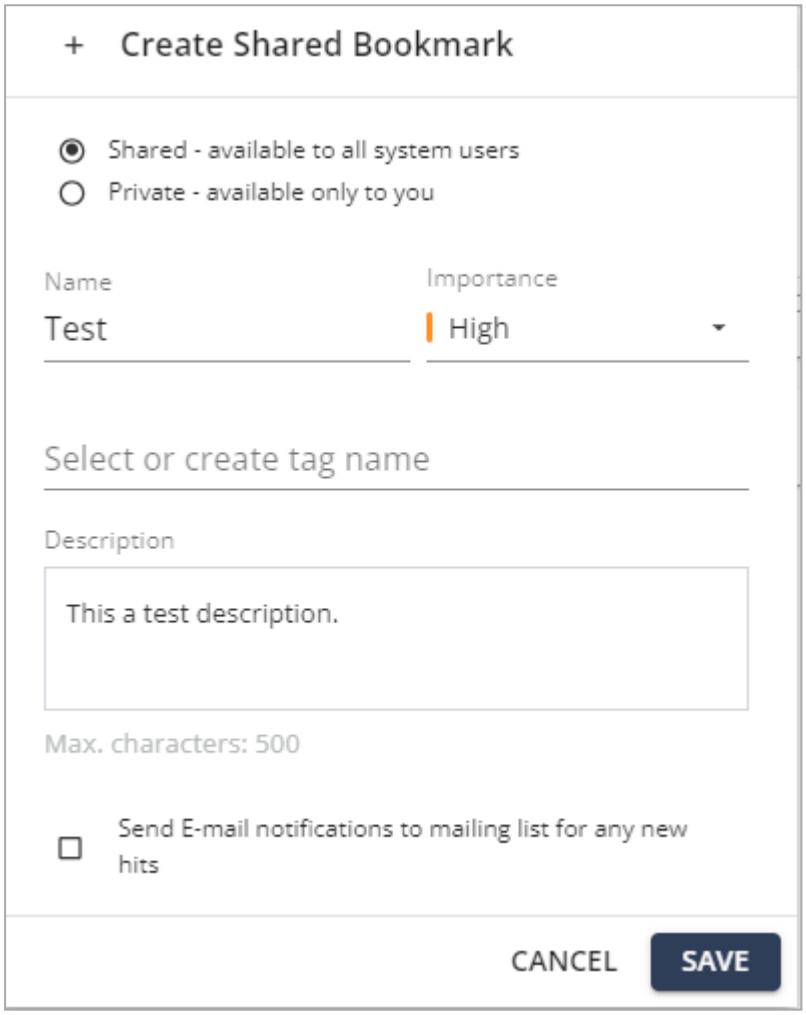
Saving a Query as a Bookmark

You can add filters to a query and save it as a bookmark. You can also send email notifications to users if Threat Hunting activity matches the query.

To save a query as a bookmark:

1. Create a query.
2. Click ☆ from the top right corner of the page.

   The **Create Shared/Private Bookmark** pop-up appears.



3. To make the bookmark public, select **Shared - available to all system users**.
4. To make the bookmark private, select **Private - available only to you**.
5. In the **Name** field, enter a query name.
6. From the **Importance** list, select an importance level for the query detection.

7. In the **Select or create tag name** field, enter the tag name or select the tag name if available.

   Tags create folders to store bookmarked queries.

8. In the **Description** field, enter a description for the bookmark.
9. To send email notifications if new activity matches the bookmarked query, select **Send E-mail notifications to mailing list for any new hits** checkbox.

   XDR sends email notifications to the recipients added to the **Threat Hunting Notifications** page.

10. Click **Save**.

To add recipients to Threat Hunting email notifications:

1. Go to **Threat Hunting**.
2. Click the ⋮ icon next to the search box and select **Notifications**.
3. From the **Recipients** list, select the users or enter the email address.

Use Case - Maze Ransomware Threat Hunting

You want to investigate the maze ransomware attack. You read about it in the internet and you are afraid it may already have infiltrated your organization.

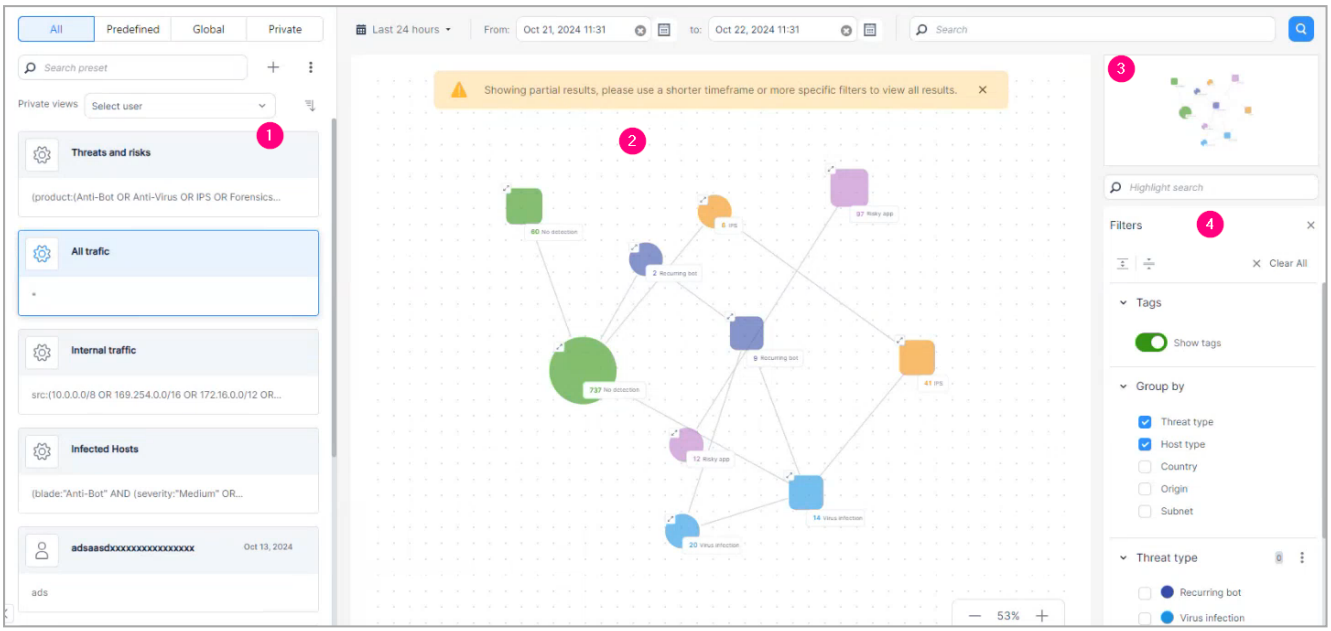
1. In the MITRE ATT&CK website: Search for Maze ransomware.
2. From the list of techniques that Maze ransomware uses, select the applicable technique. For example: Windows Management Instrumentation
3. From the Check Point Portal > **Threat Hunting**, click the ⋮ icon on the right side of the search box, and go to **MITRE ATT&CK**.
4. In the **MITRE ATT&CK** dashboard, search for the technique you copied from the Maze website.
5. Click the technique to see all the events in your organization in which this technique was used.

Threat Topology Map

Threat Topology Map is an investigative tool that allows the visualization of event data. The visualized event data resembles the data shown in the *"Events" on page 201* page. The data displayed on the topology map shows information on both the connections between hosts and any threats detected on the hosts.

To view the Threat Topology map, access the XDR Administrator Portal and click **Investigate > Threat topology map**.

By default, the page shows the Threat topology map for the last 24 hours.



Legend	Item	Description
1	Views	Shows filters with the predefined queries that are applied to the data before it is displayed on the topology map. For more information, see *"Managing Views" on page 176*.
2	Topology Map	Shows the connections between hosts and any threats detected on the hosts. For more information, see *"Reading the Threat Topology Map" on page 188*.
3	Mini map	A miniature overview of the Topology map.
4	Filters	Parameters that help to filter the Threat Topology map. For more information, see *"Filtering the Threat Topology Map" on page 198*.

Topology Map - Overview

The Threat Topology map shows the connections between hosts and any detected threats, providing an intuitive overview of your network's security status.

Views

A **View** is a filter with a predefined query that is applied to the data before it is displayed on the topology map. When a view is selected, the corresponding filter is applied, restricting the scope of data that will be displayed and can be searched on the map.

Internal IP Settings:

Internal IP settings contain a list of predefined IP address ranges in CIDR format, that are considered as internal. Admins can add their internal IP address ranges to this list. These are added to the **Internal traffic** predefined view, allowing a focused view of internal network traffic on the map. It also impacts the **Host type** displayed on the map. For more information, see *"Internal IP Settings" on page 183*.

Excluded Views:

Administrators can create **Excluded Views** to hide specific information on the topology map. You can either create a query to exclude certain data or define a range of IP addresses to be excluded on the topology map. For example, to avoid monitoring test devices on the topology map, you can create an excluded view for their IP address range.

Any data that matches an excluded view will not be shown on the map regardless of any View or Search definitions.

For more information, see *"Excluded Views" on page 185*.

Visualizing Connections

Lines show the connections between the hosts. You can hover a line to see the number of distinct connections made between the hosts. There are different representations for the **Host type**, depending on whether it is an internal or external host.

There are two options that control the set of events represented on the topology map:

- **Threats** (Default) - Only threat-related information is reported as **Alerts**
- **All** - All event records

Color Coding

Hosts are color-coded according to the **Threat type**, as shown in the legends on the right side. If a host has multiple threat types, the system displays the highest priority threat first and lists the other threat types in descending order of priority.

Filtering and Searching

You can configure the map's event data time frame, with optional search criteria for more specific data retrieval. For more information on the search query syntax, see *"Searching the Threat Topology Map" on page 196*.

If the data volume exceeds the display limit, the system shows a warning message and only partial results are displayed. In such cases, it is recommended to refine your search criteria or reduce the time frame to retrieve a more specific data set.

Hosts Grouping

Hosts can be grouped by **Threat type**, **Host type**, **Country**, **Origin**, and **Subnet** to reduce the number of data points on the map and to improve readability. By default, hosts are grouped by **Threat type** and **Host type**.

Hosts Tags and Details

You can configure tags for hosts and have it displayed on the map when you select the **Show tags** option.

You can also view the related details for any selected host. The details include:

- **Alerts** - Alerts detected that include the host.
- **Applications** - Logs related to Application control.
- **Matched Indicators** - Indicators that matched the host.

By leveraging these features, the Threat Topology map helps you effectively monitor and manage network security, ensuring a clear understanding of connections and potential threats.

Managing Views

View Categories

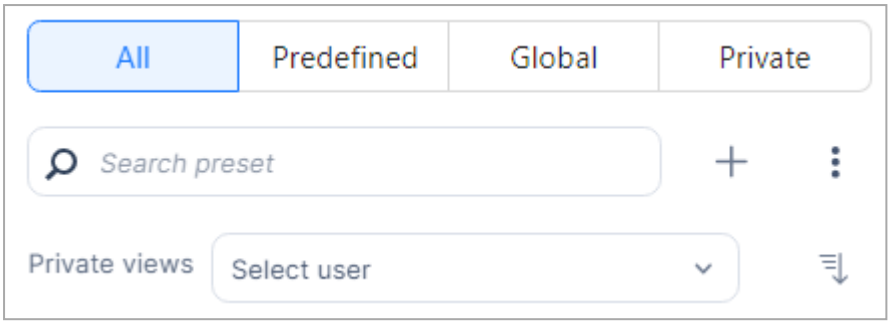
The different **View** categories are:

Icon	Category	Description
	Predefined	Views that are predefined by Check Point. These views cannot be modified or deleted by any user. Check Point provides these predefined Views: ■ Threats and risks ■ All traffic ■ Internal traffic ■ Infected Hosts
	Global	Views that can be used by all users. Only administrators can add/modify/delete these views.
	Private	These Views are specific to the user. Unlike predefined views, these views can be created, modified, or deleted by the user. Only the user and administrators have access to view private views.

Important - Your ability to manage Views depends on the permissions assigned to you in **Global Roles** or in **Specific Service Roles**:

Role	Description
Global Roles	
Admin	Full Read and Write access to all system aspects.
Specific Service Roles	
Admin	Full Read and Write access to all system aspects.
Operator	Full access to handle incidents, including taking prevention actions, and read-only access to the **Policy** menu. Typically, your SOC analyst.
Read-Only	Read-only access to the application.

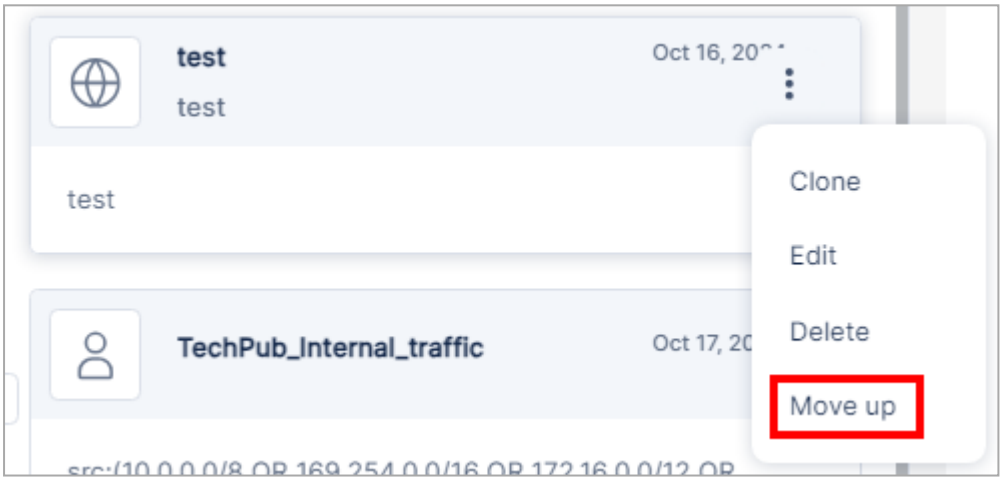
The **All** tab shows an ordered list of all the **Predefined**, **Global** and **Private** views. To sort the order of views, click the icon.



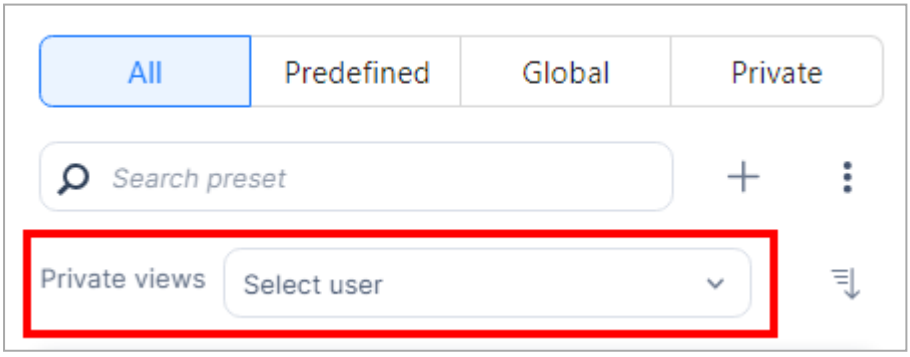
Changing the Order of Views

You can move **Global** and **Private** views up or down within the same view type to arrange them based on their importance.

Note - Admins can change the order of both **Global** and **Private** views.



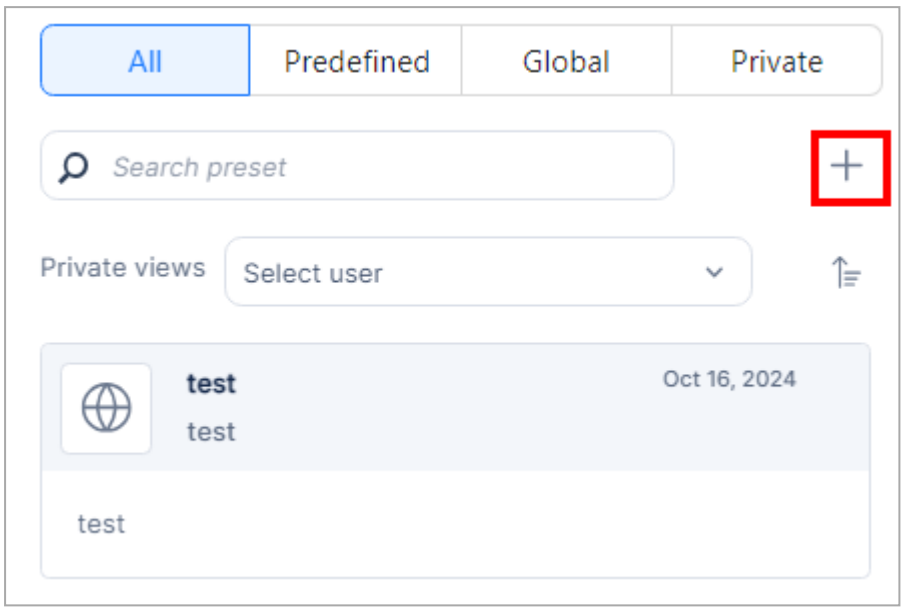
The **Private views** section is shown only for administrators to view the Private views created by other users.



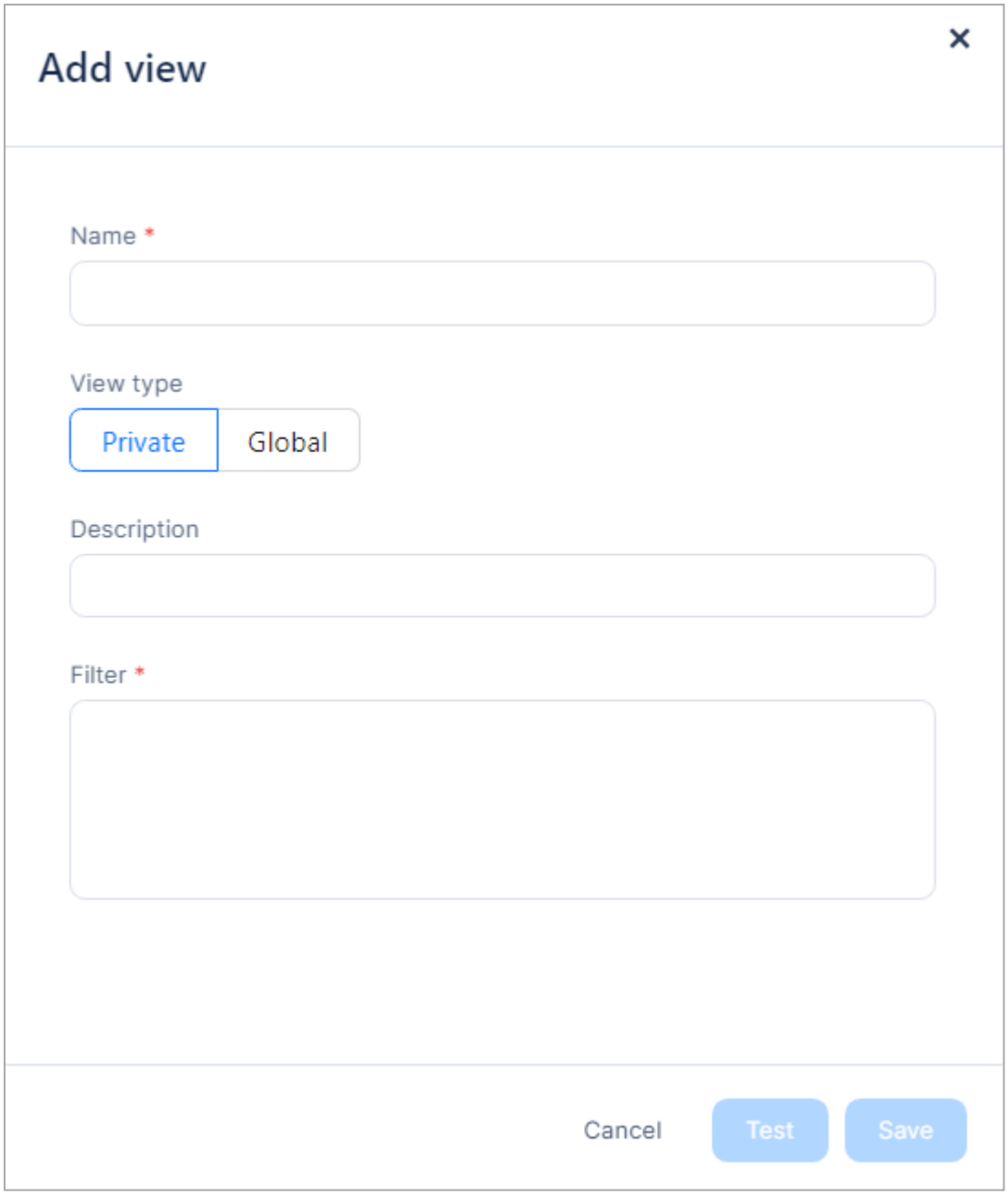
To search for a specific view or any fields in the view, enter the text in the **Search preset** field.

Adding a New View

1. In the **Views** section, click **+** at the top-right corner.



The **Add view** window appears.



2. In the **Name** field, enter a name for the view.
3. In the **View type** field, select the type of the view:
   - **Private**
   - **Global**

   Note - Admins can create both **Global** and **Private** views. **Operators** and **Read-Only** users can create only **Private** views.
4. (Optional) In the **Description** field, enter a description for the view.
5. In the **Filter** field, enter the filter query.
6. (Optional) To test the query, click **Test**.

The system shows a message indicating whether the query is valid and the number of matching records, if any.

7. Click **Save**.

Editing a View

Administrators can edit the details of existing views, including changing them from Global to Private and vice versa. However, all users can edit their own Private views.

The table below shows the edit permissions for different View categories and user roles:

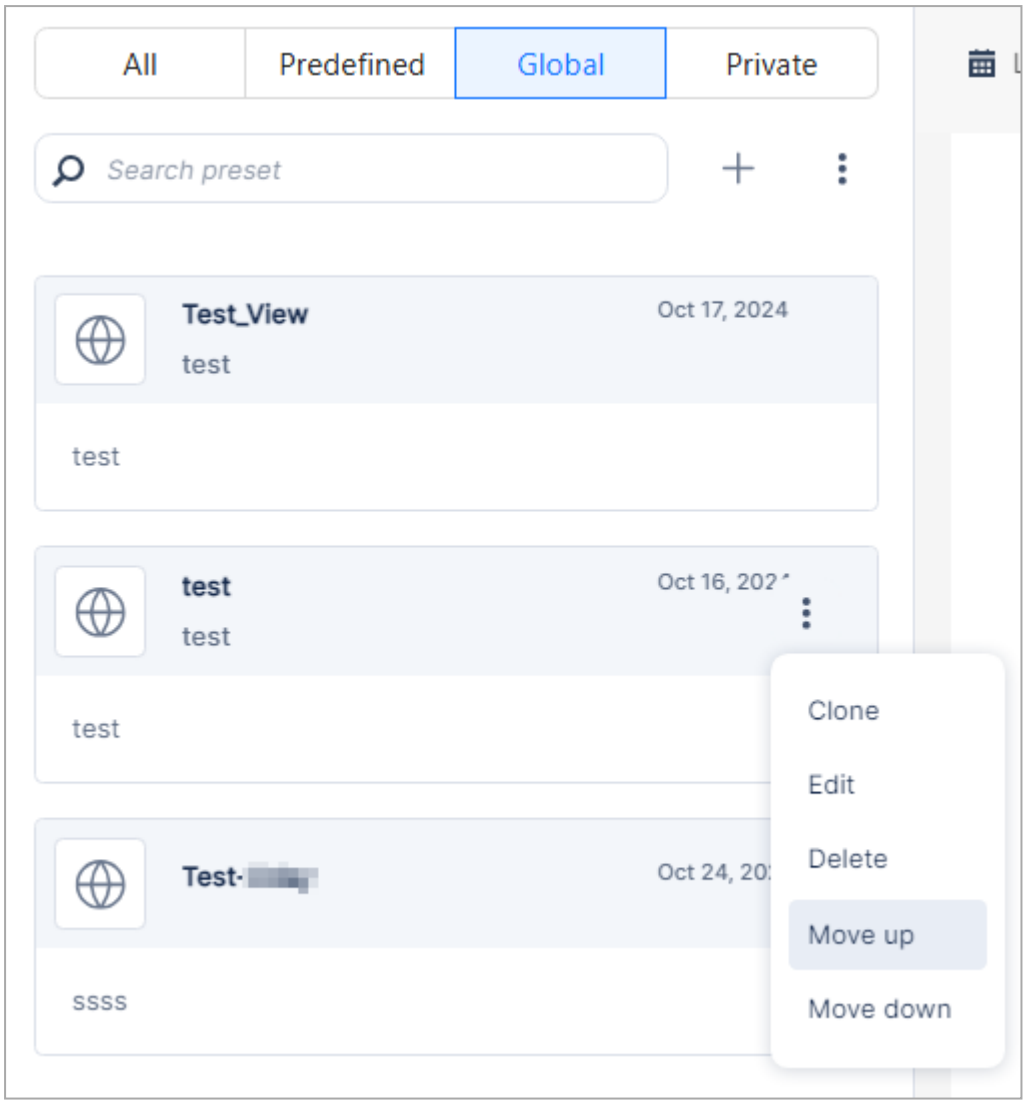
View Category	Edit Permission
Global	Only admins can edit.
Private	Only the user who created the view can edit.
Predefined	Editing is not permitted. However, you can clone it and save as either a Global (only for admins) or Private view. See *"Cloning a View" on the next page*.

To edit a View:

1. Hover over the view and click .
2. Click **Edit**.

   The **Edit view** window appears.
3. Make the necessary changes and click **Save**.
4. To move the order of a view up or down the list, click and then click **Move up** or **Move**

down.

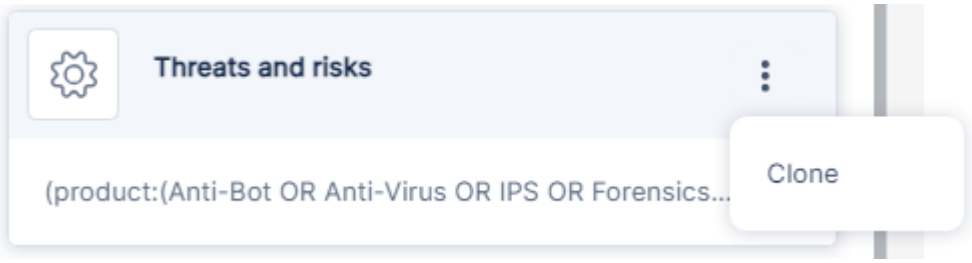


Cloning a View

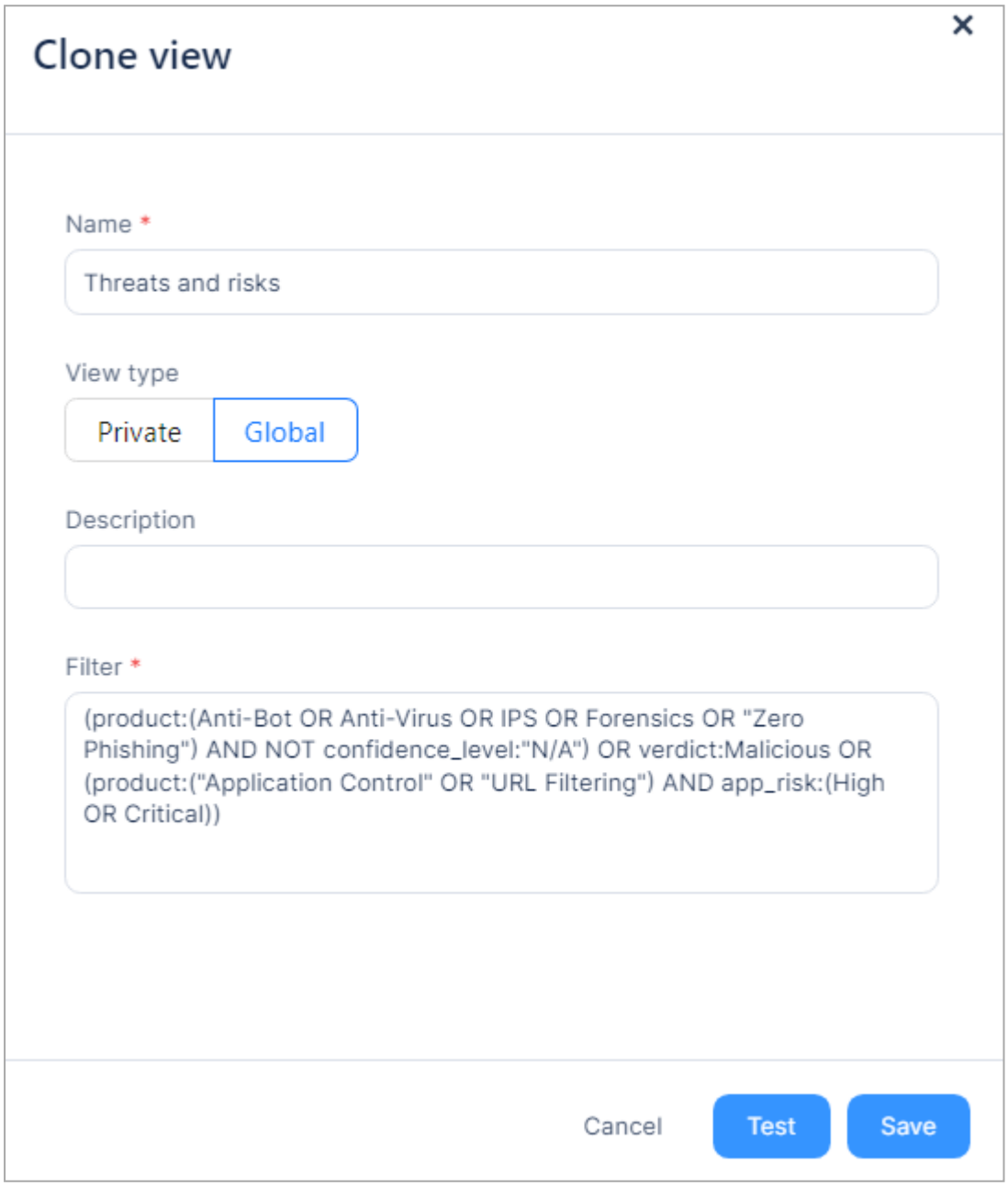
You can create a copy of an existing view, edit it and save it as a Global (only for admins) or Private view.

To clone a view:

1. Hover over the view and click ⋮.
2. Click **Clone**.



The **Clone view** window appears.



3. Make the necessary changes and click **Save**.

Deleting a View

The table below shows the delete permissions for different view categories and user roles:

View Category	Delete Permission
Global	Only admins can delete.
Private	Only the user who created the view can delete.
Predefined	Deleting is not permitted.

To delete a Global or Private view:

1. Hover over the view and click ⋮.
2. Click **Delete**.

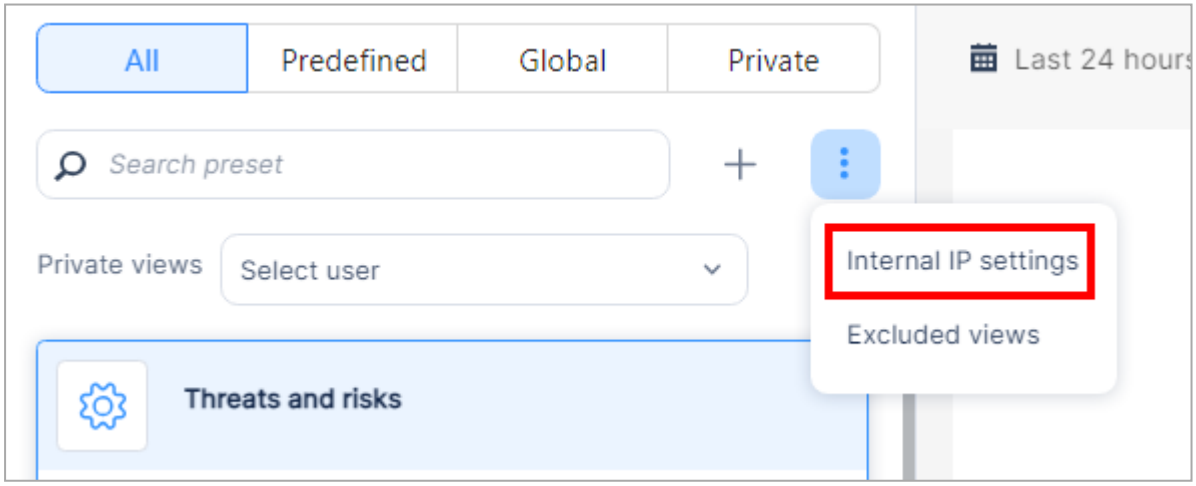
Internal IP Settings

Note - Only admins can add/modify/delete the internal IP settings.

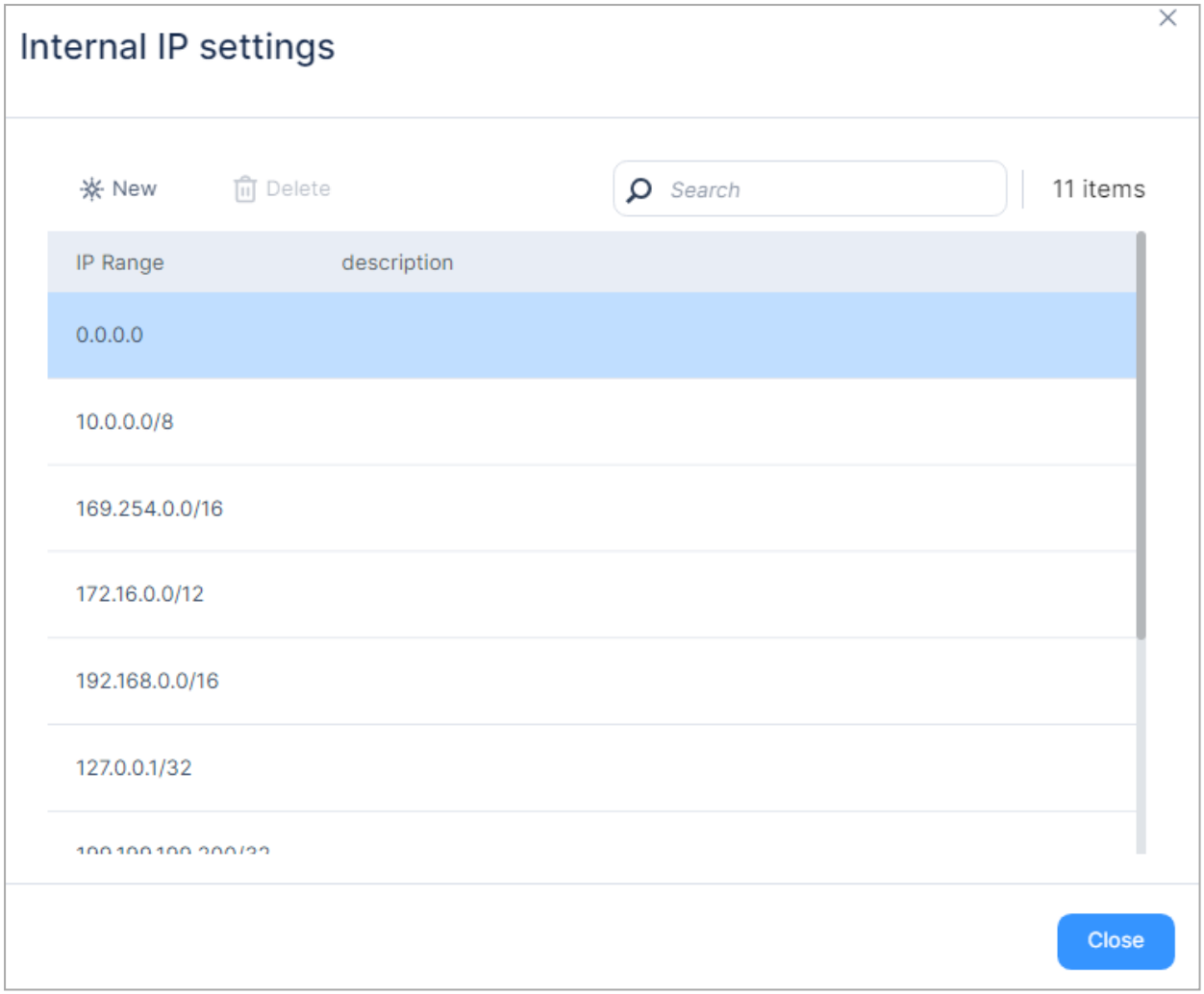
Internal IP settings contains a list of predefined internal IP address ranges in CIDR format. This list is added to the **Internal traffic** predefined view by default. You can add your internal IP ranges to this list.

To add an IP address range to the internal IP settings:

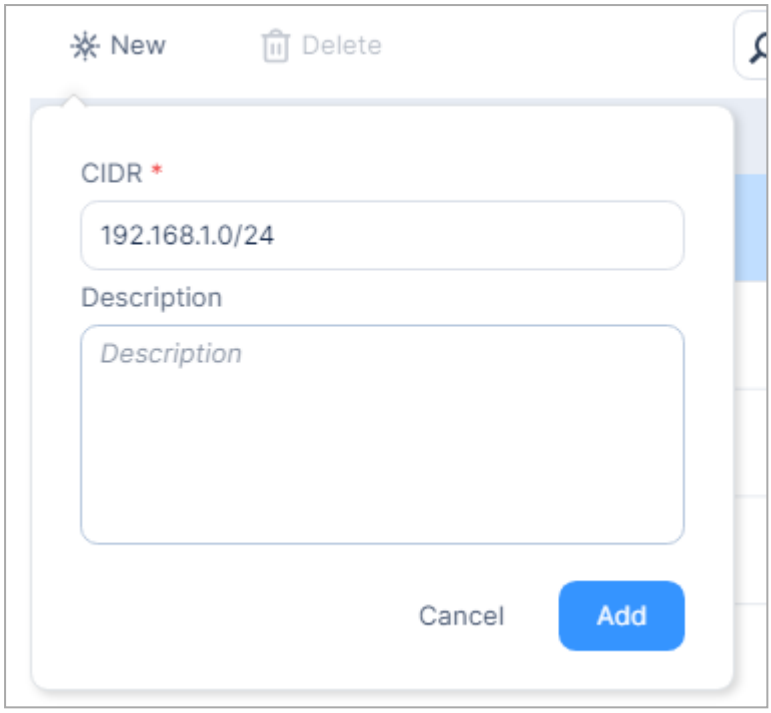
1. In the **Views** section, click ⋮ icon in the top-right corner, and then select **Internal IP settings**.



The **Internal IP settings** window appears.



2. Click **New**.
3. In the **CIDR** field, enter the IP address range in CIDR format (for example, 192.168.1.0/24).



Note - If the address range already exists in any of the predefined IP ranges, the system displays an error message.

4. (Optional) Add a description.
5. Click **Add**.

To delete an IP address from the internal IP settings:

Note - You can only delete the IP ranges created by you or other administrators. You cannot delete the predefined IP ranges.

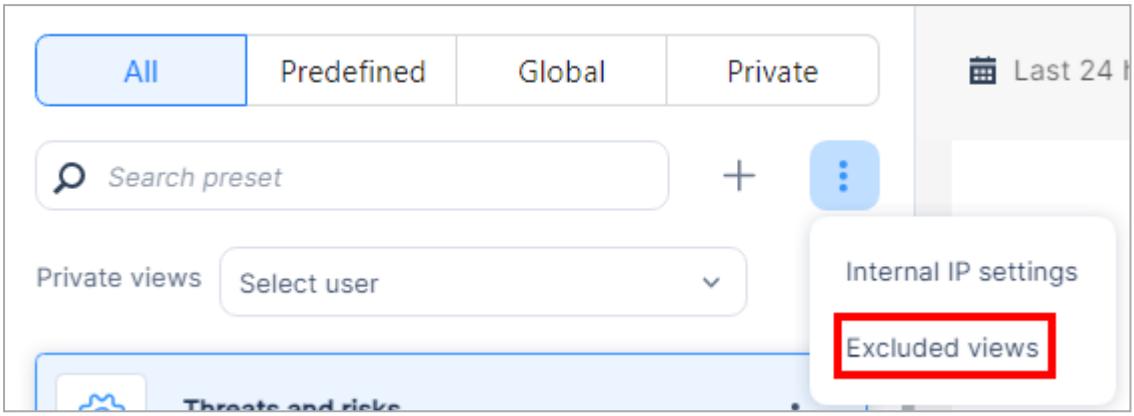
To delete, select the IP range in the **Internal IP settings** table and click **Delete**.

Excluded Views

Administrators can create **Excluded Views** to hide specific information on the topology map. You can either create a query to exclude certain data or define a range of IP addresses to be excluded on the topology map. For example, to avoid monitoring test devices on the topology map, you can create an excluded view for their IP address range.

Any data that matches an excluded view will not be shown on the map regardless of any View or Search definitions.

To view the excluded views for the topology map, in the **Views** section, click ⋮ icon in the top-right corner, and then select **Excluded views**.



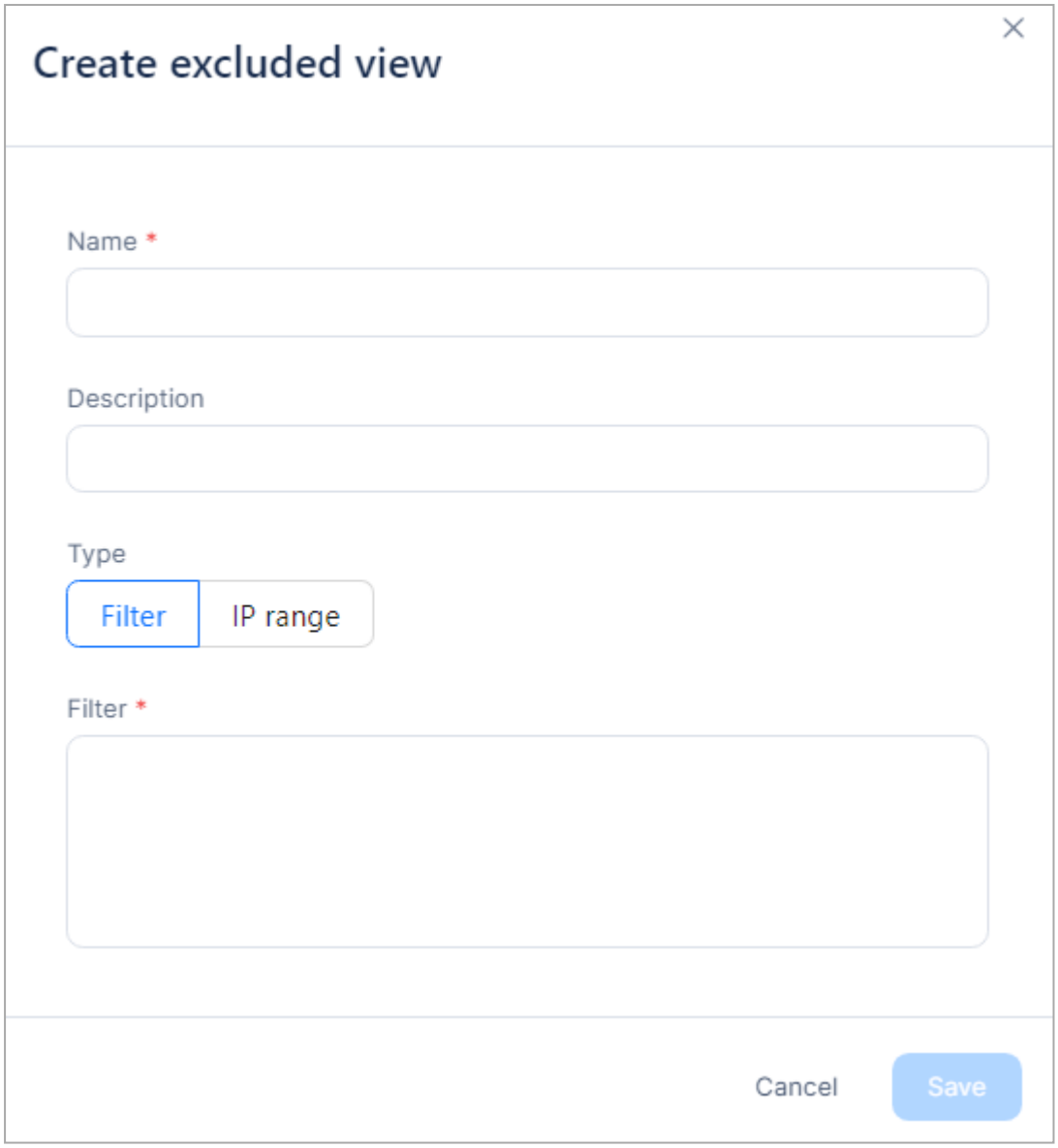
The **Topology map excluded views** page in the **Settings** tab appears.

To add a specific query (filter) or IP address as an exclusion for the topology map:

Note - Only admins can add/modify/delete Excluded views.

1. In the **Topology map excluded views** page, click **New**.

   The **Create excluded view** window appears.



2. Enter these:
    a. **Name** - Enter a name for the view.
    b. (Optional) **Description** - Enter a description about the exclusion.
    c. **Type** - Select one of these:
        - **Filter** - To add a filter query.
        - **IP range** - To add an IP range.
    d. **Filter** - Enter the filter query or the IP range in CIDR format.
3. Click **Save**.

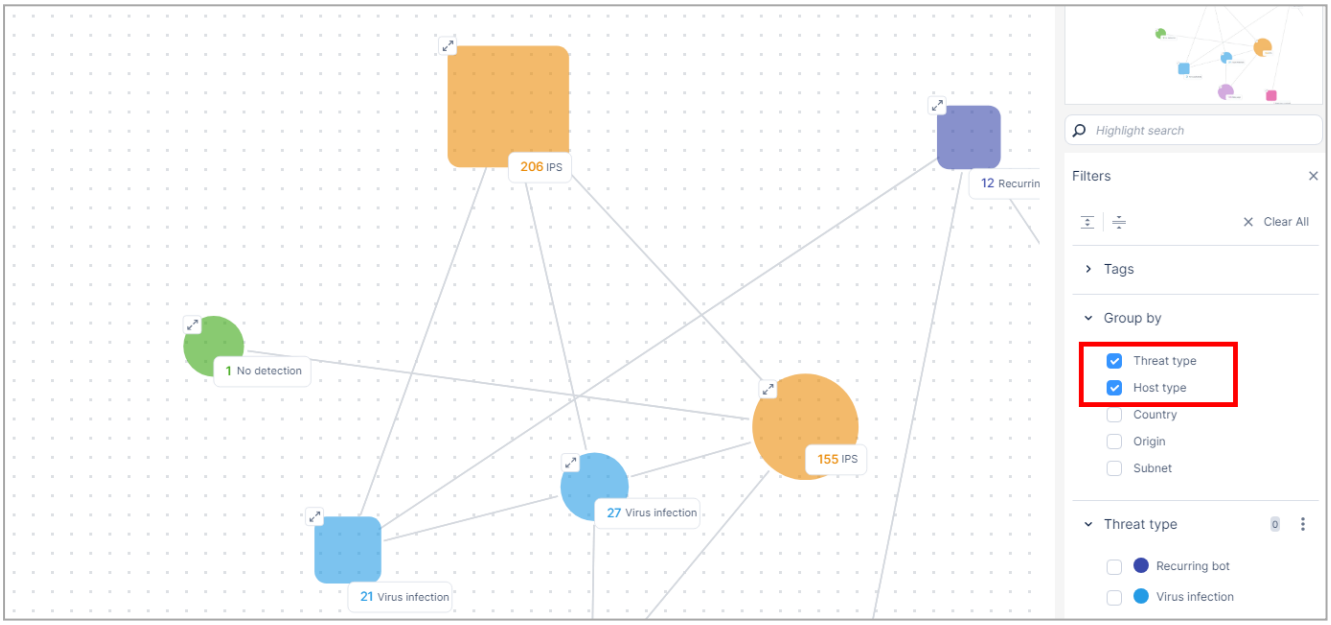
The system adds the view to the excluded views table and hides the corresponding data on the topology map.

Reading the Threat Topology Map

Legend

Item	Description
	Internal host. A computer in a private network, such as your organization's network.
	External host. A computer in a public network, such as the internet.

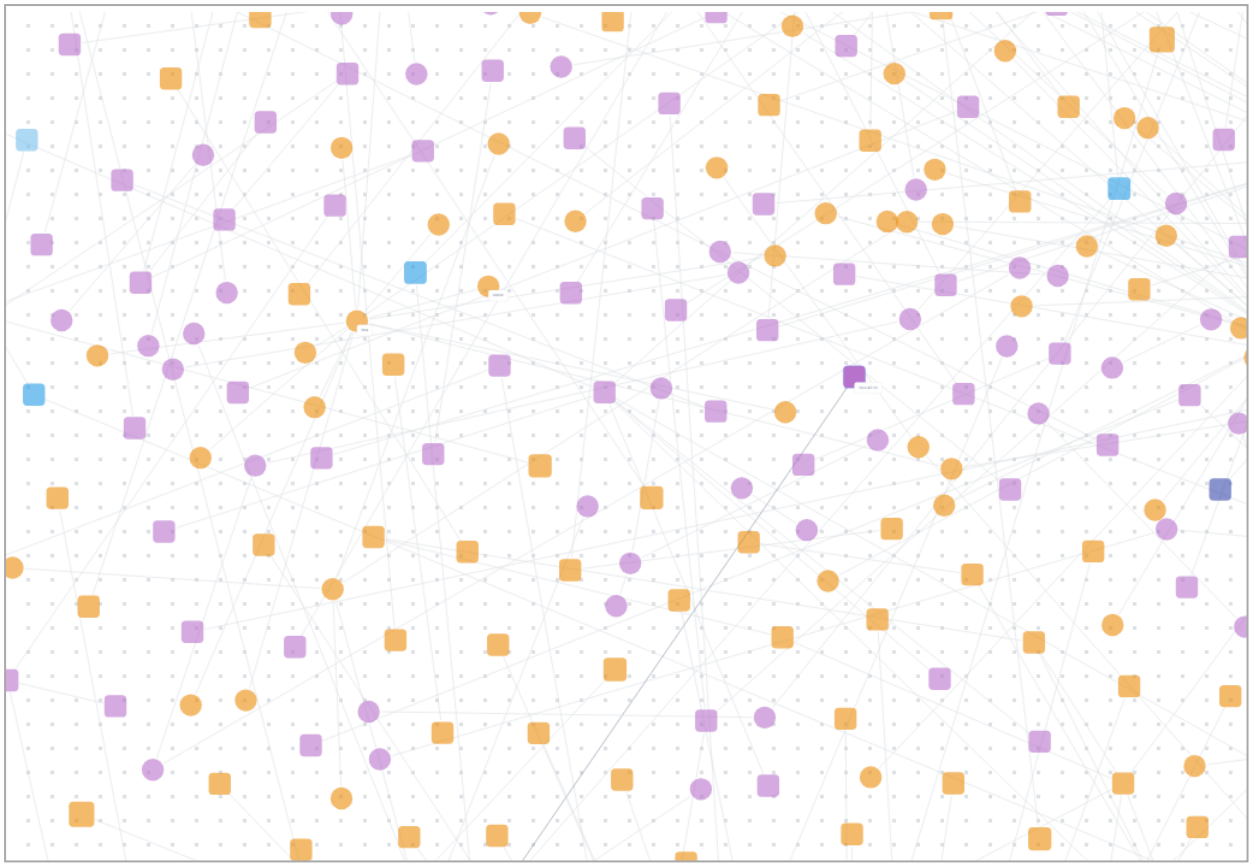
By default, the hosts are grouped by **Threat type** and **Host type**. For more information, see *"Filtering the Threat Topology Map" on page 198*.



To view the hosts on the Threat Topology map:

1. In the **Group by** section, clear the checkboxes for **Threat type** and **Host type**.

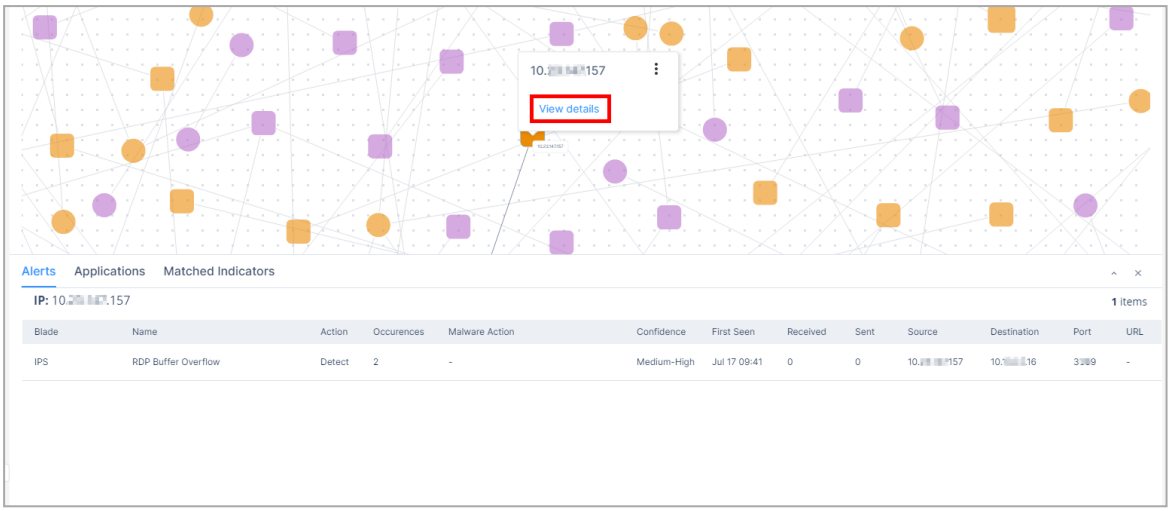
   The map shows all the hosts from the events in the selected time frame and search query.



You can drag and re-arrange the hosts to view the connection in detail.

2. To view the host details, hover over the host. The card shows:
   - IP address of the host.
   - Country where the host is located.
   - Username logged in to the host (when available)
   - Hostname (when available)
   - Tag name (when available)

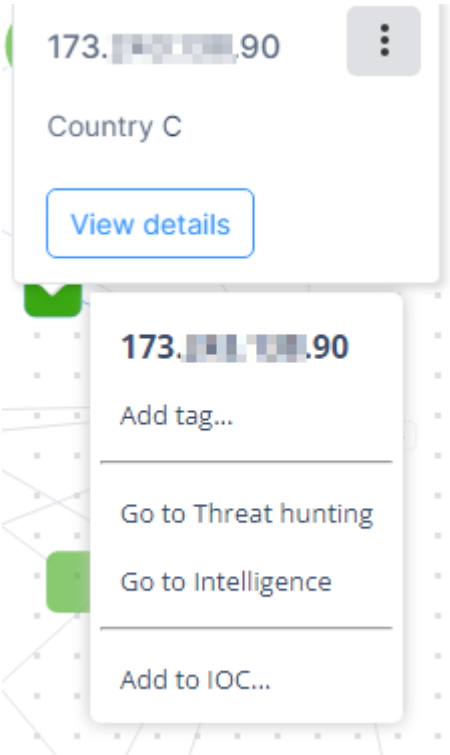
- To view more information about the host, click the host or click **View details**.



The system shows these details:

Item	Description
Alerts	Alerts detected that include the host.
Applications	Logs related to Application control.
Matched Indicators	Indicators that matched the host.

3. To perform actions on a host, right-click the host or hover over it and click ⋮.



Select the required action:

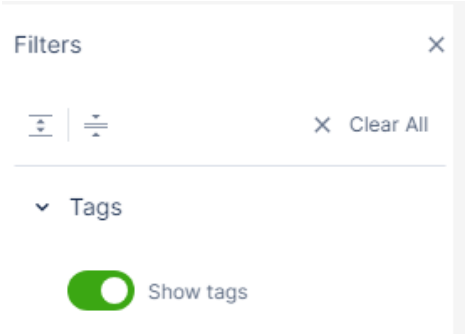
a. To easily identify the host on the map, add a tag:

   i. Click **Add tag**.

   ii. Enter a tag name and click **Save**.

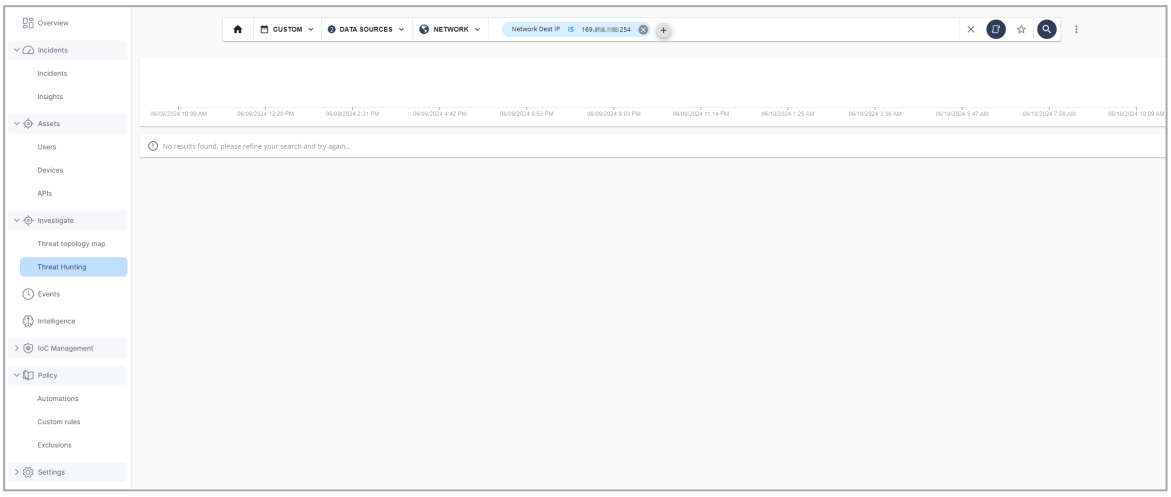
   The system displays the tag name on the host.

Note - To display the tag name on the map, go to **Filters** > **Tags** and enable the **Show tags** toggle button.



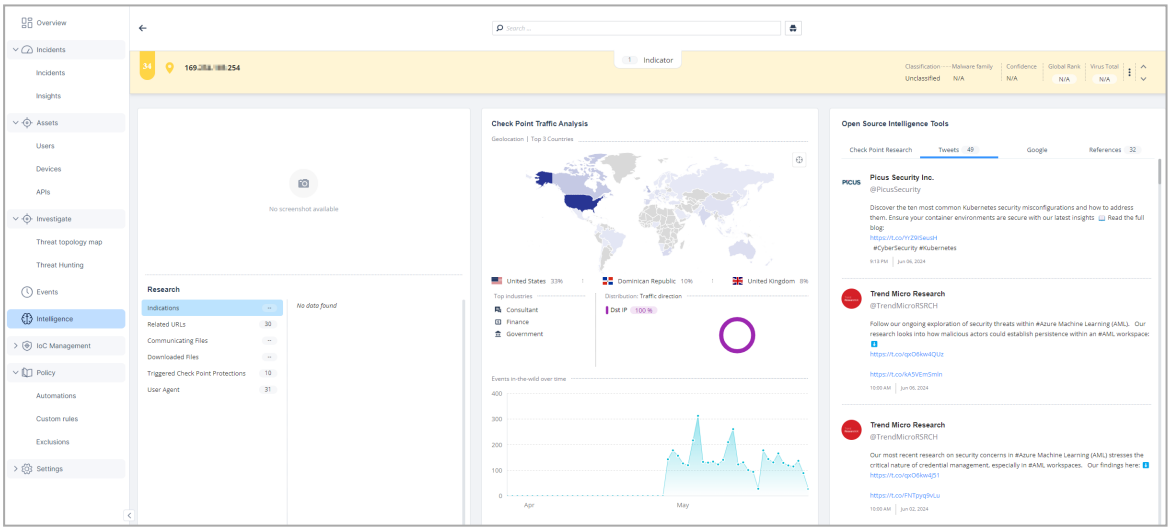
b. To view the Threat Hunting information about the host, click **Go to Threat hunting**.

The system opens the **Threat Hunting** page and shows the data filtered by the host IP address.



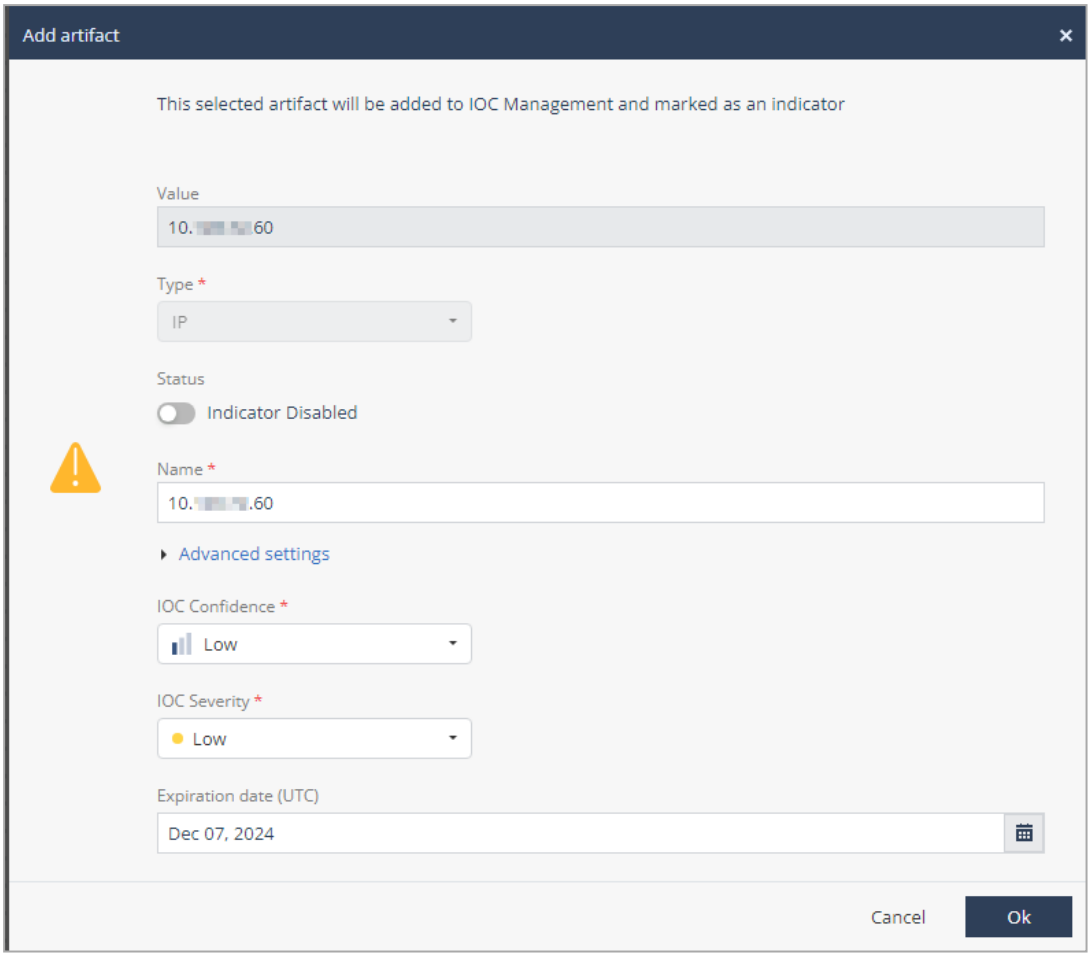
c. To view the Intelligence information about the host, click **Go to Intelligence**.

The system opens the **Intelligence** page and shows the data filtered by the host IP address.



d. To add the host as an indicator to IoC Management:

i. Click **Add to IOC**. The **Add artifact** window appears.

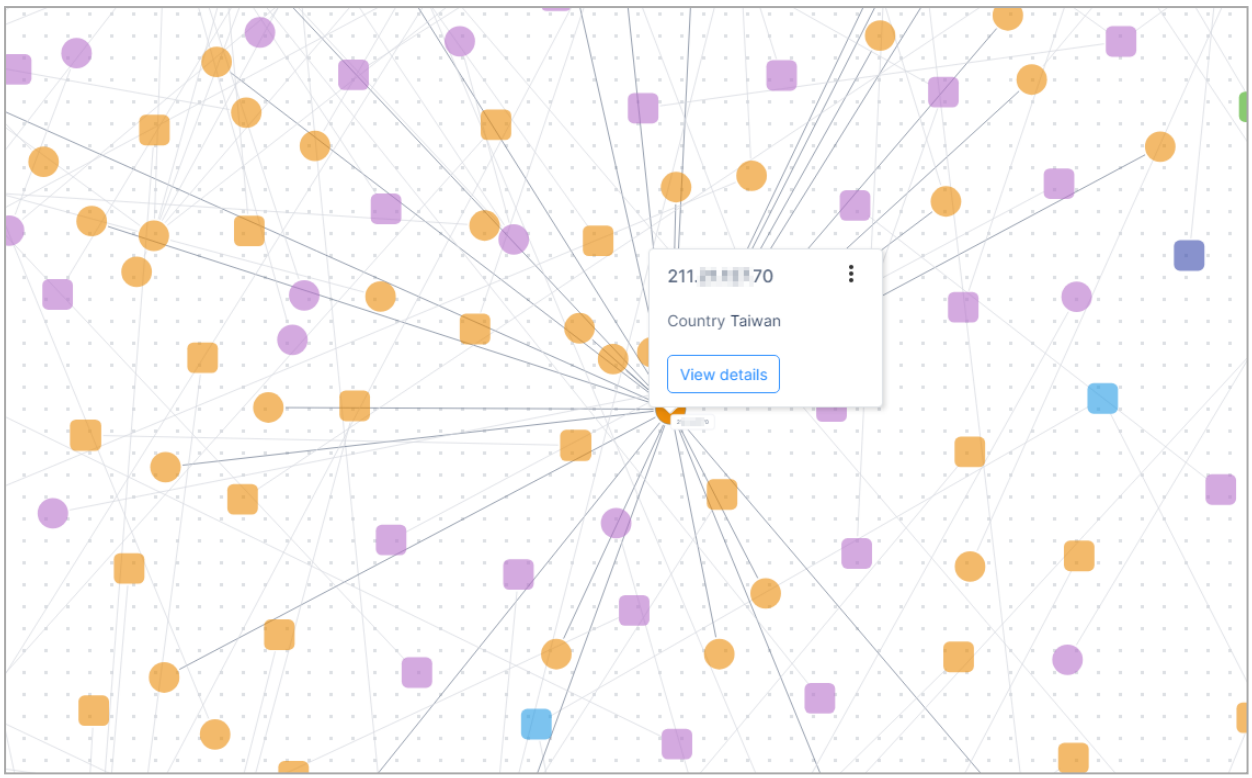


ii. Enter the required details and click **OK**.

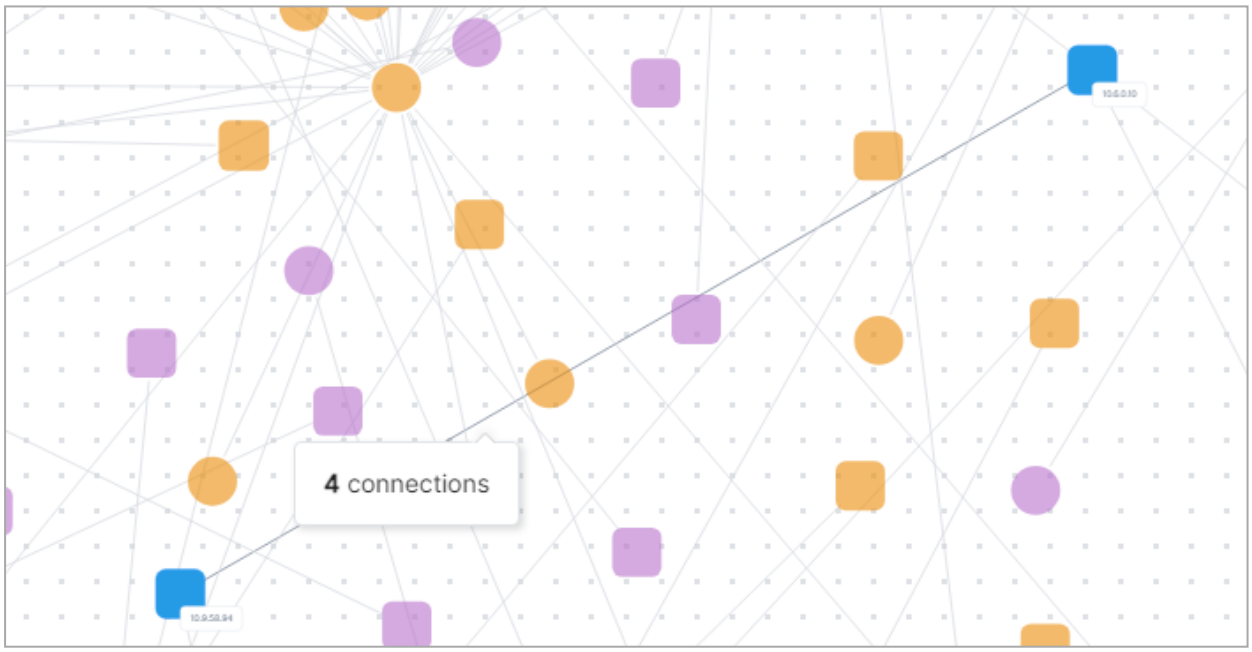
The system adds the host IP address as an indicator to IoC Management.

4. To view the connections of a host, hover over the host.

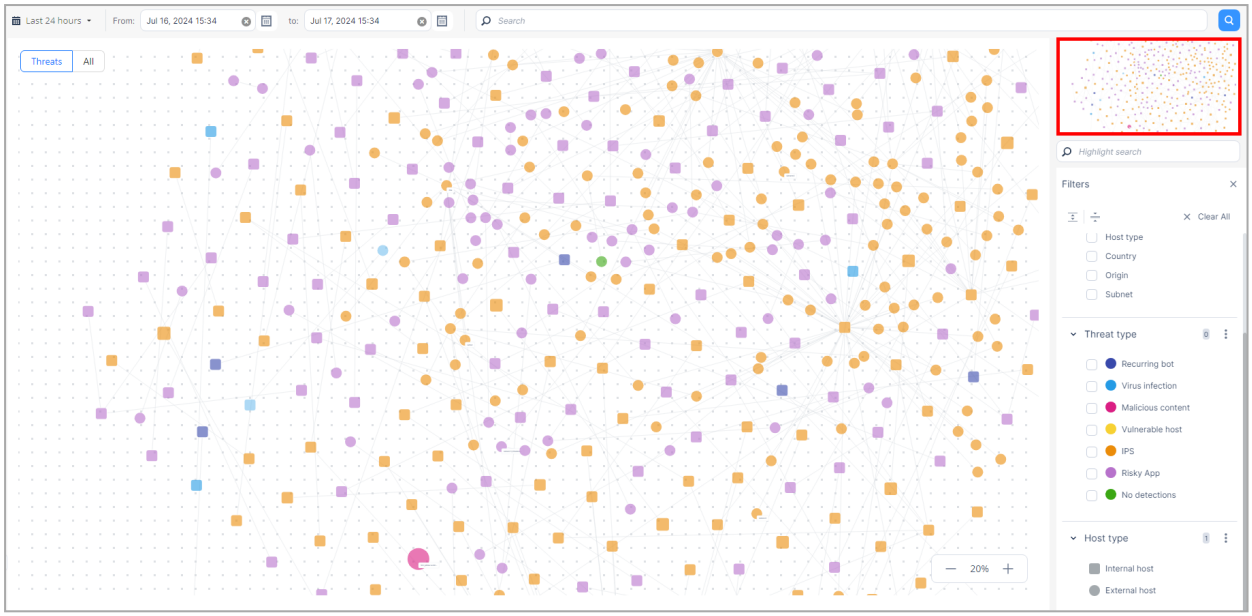
The system highlights all the connected nodes.



5. To view the number of the connections between two hosts, hover over their link.

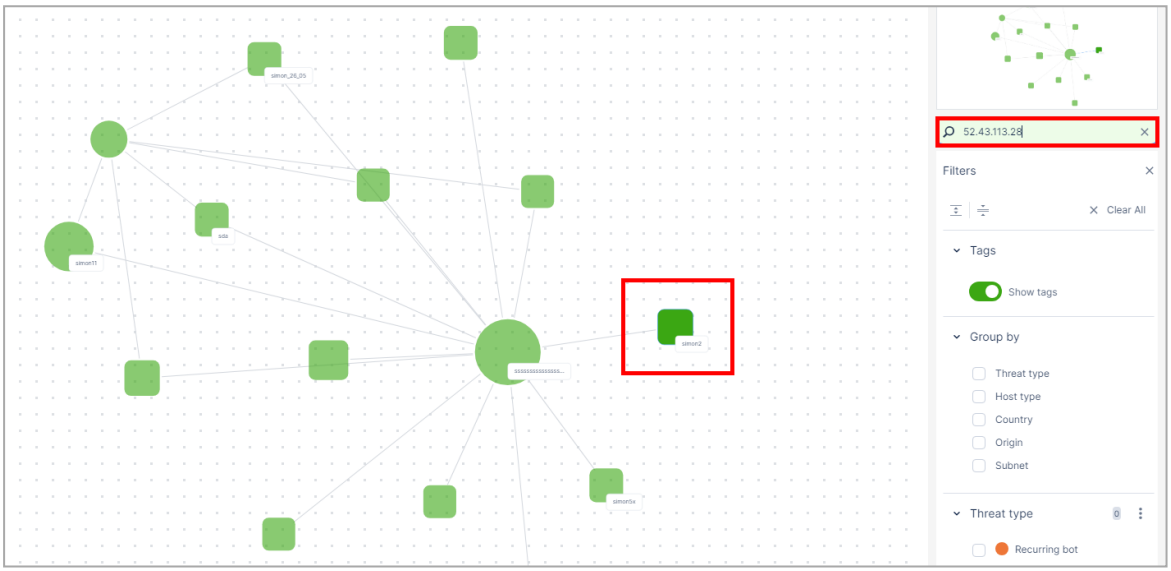


6. To zoom in or out, scroll the mouse wheel up/down or use the zoom-in/zoom-out buttons in the bottom-right corner.
7. To pan the map, click and hold anywhere outside the nodes and links and then move the mouse.
8. For an overview of the current Topology map, see the mini-map at the top-right corner.


Last 24 hours
From:
Jul 16, 2024 15:34
to:
Jul 17, 2024 15:34
Search
Threats
All
Highlight search
Filters
Clear All
Host type
Country
Origin
Subnet
Threat type
Recurring bot
Virus infection
Malicious content
Vulnerable host
IPS
Risky App
No detections
Host type
Internal host
External host
20%

Searching the Threat Topology Map

1. To find a host on the map, on the right pane, in the **Highlight search** field, enter any of these:
   - Host IP address
   - Tag name
   - Username
   - Hostname

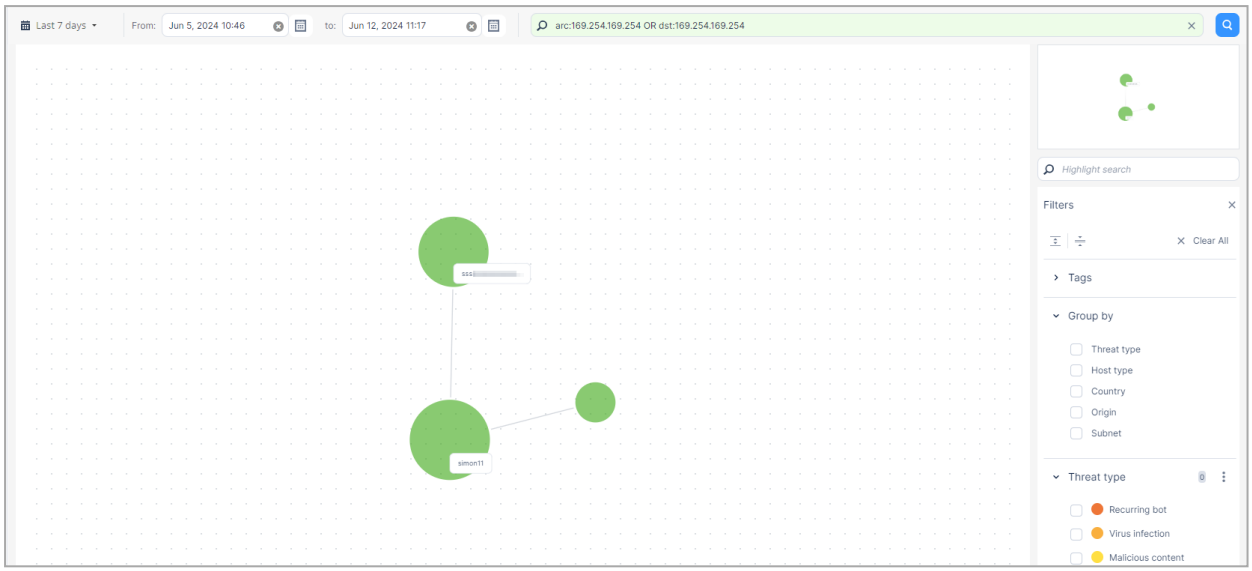
   The system highlights the node on the map.
2. To find hosts from events in a specific time period, select the time frame at the top and click icon.
3. To search for hosts with specific conditions, enter the query in the **Search** field and click icon.

   The basic query syntax is `[<Field>:] <Filter Criterion>`

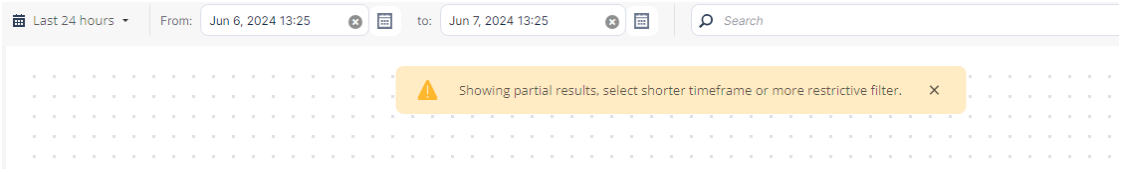
   To put together many criteria in one query, use Boolean operators:

   `[<Field>:] <Filter Criterion> {AND|OR|NOT} [<Field>:] <Filter`

```
Criterion> ...
```



Note - If the number of events in the selected time frame exceeds the allowed limit for display, the system shows only partial results and displays this banner.



For accurate search results, select a short time frame or enter a specific query in the **Search** field.

Filtering the Threat Topology Map

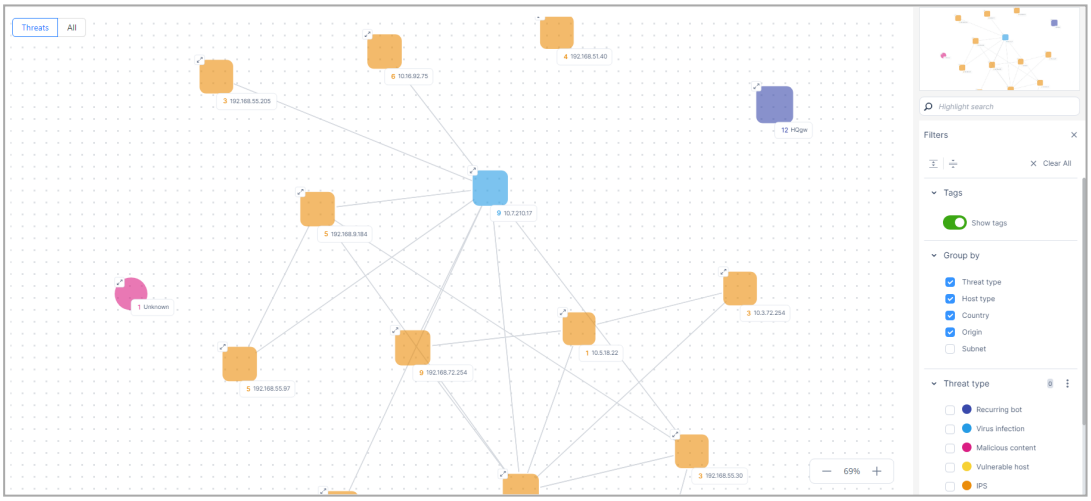
You can filter a Threat Topology map by:

- **Group by**

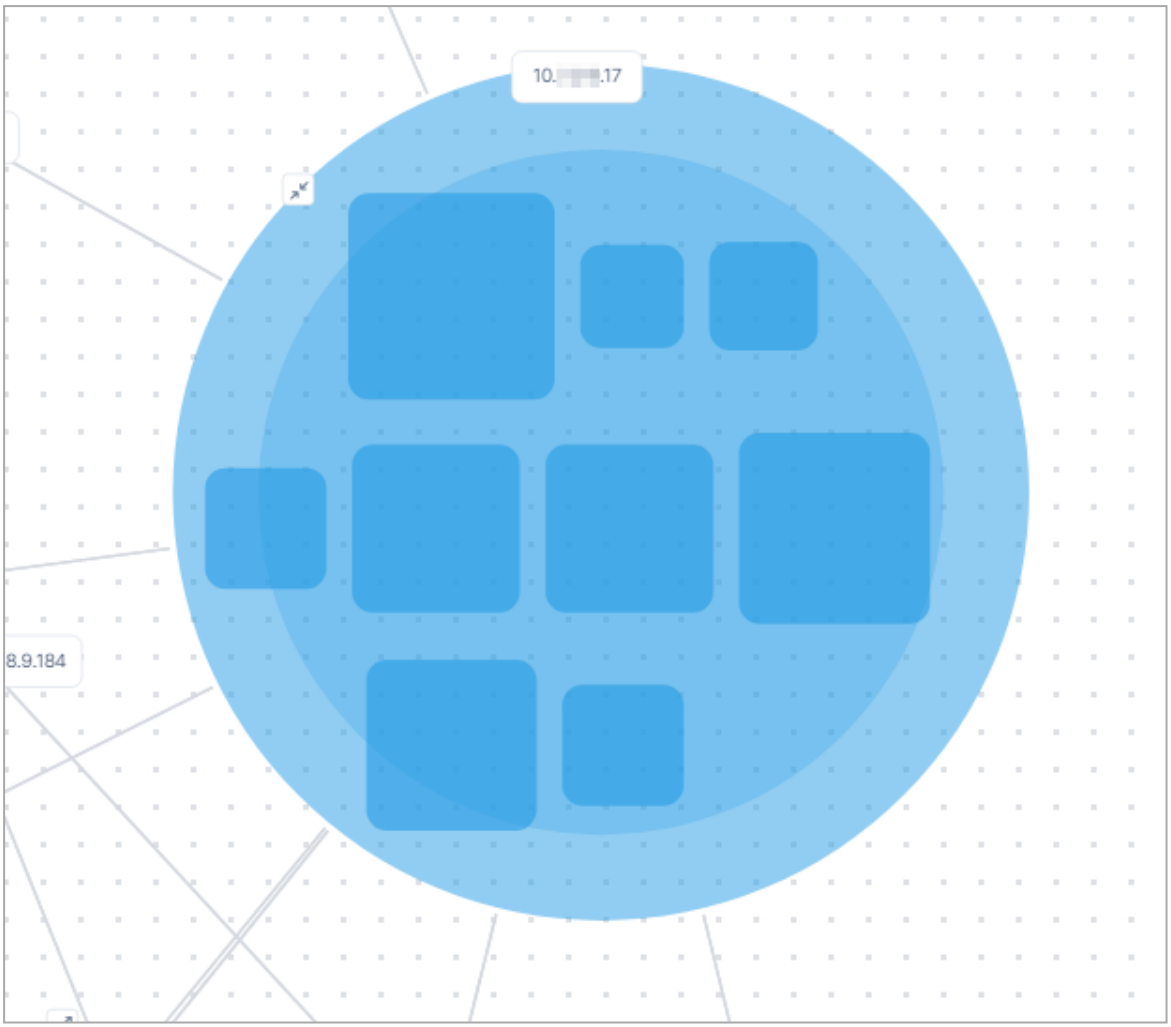
  a. Select the parameter(s) by which you want to group the hosts on the map:

  - Threat type
  - Host type
  - Country
  - Origin
  - Subnet
    - Subnet A
    - Subnet B
    - Subnet C

  The system shows the map grouped by the selected parameters.



b. To view the hosts in a group, click the icon or the grouped node.



c. To go back to the grouped view, click or click anywhere within the group.

- Threat type
  - Recurring bot
  - Virus infection
  - Malicious content
  - Vulnerable host
  - IPS
  - Risky App
  - No detections
- Host type

- Internal host
- External host

Events

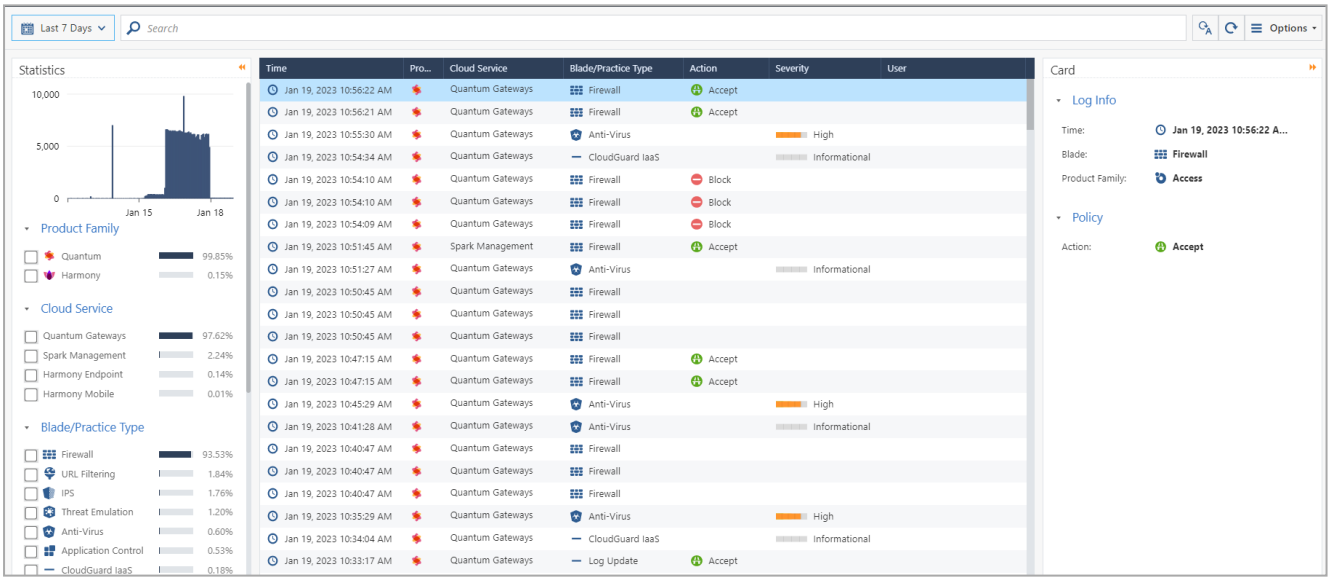
The **Events** page provides a unified interface to view security events of products supported by Events & AIOps. For more information, see *Events & AIOps Administration Guide*.

Note - Corrective action for an event must be taken in the product that generated the event. For example, if a benign URL is blocked, then access the product and correct the policy.

The **Events** page shows:

- *"Statistics" on page 203*
- *"Events Table" on page 204*
- *"Card" on page 209*

To view the **Events** page, access XDR and click **Events**.



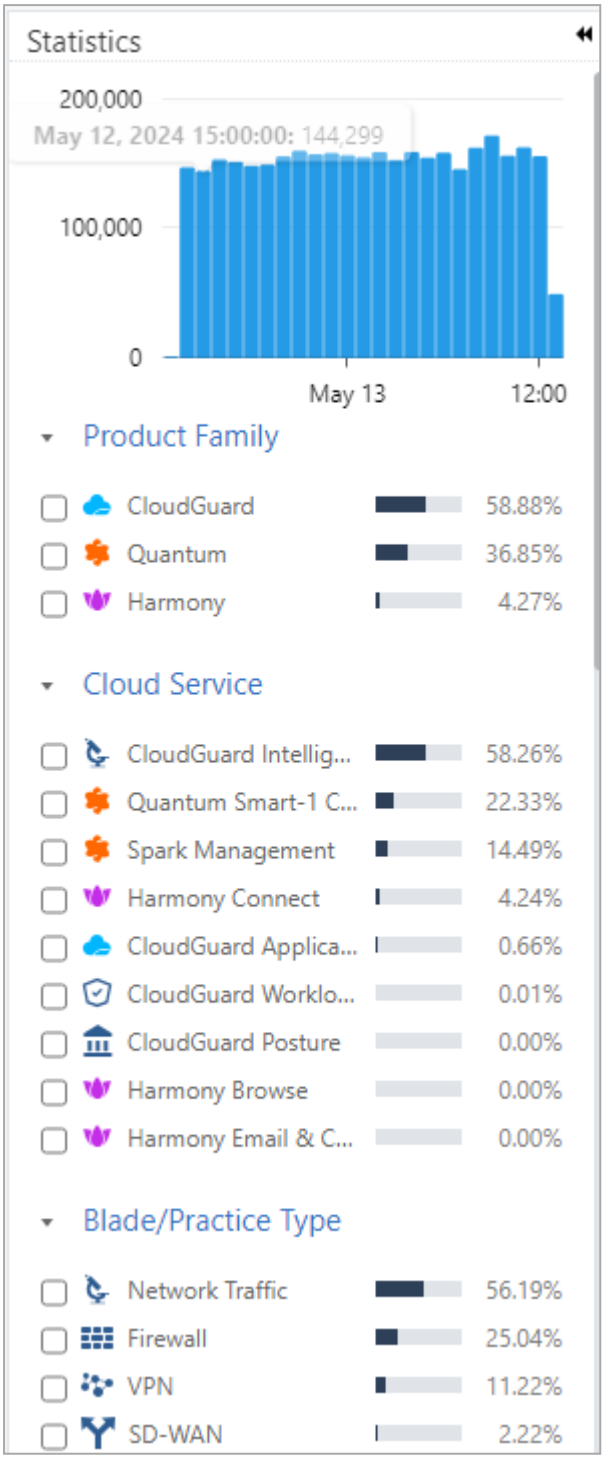
Note - The default log retention duration is 90 days. To extend the duration to 180 days or 365 days, contact *Check Point Support*.

Supported Products

- Quantum Self-Hosted Management
- Quantum Spark Management
- Smart-1 Cloud
- Endpoint Security
- Mobile Security

- Harmony Connect
- Browser Security
- Email Security
- SASE
- CloudGuard Posture
- CloudGuard WAF
- Fortinet FortiGate Next Generation Firewall
- CrowdStrike Falcon
- Trend Vision One for Endpoint
- Cisco Firepower Threat Defense
- Microsoft 365 Defender for Endpoint
- Palo Alto Networks Next Generation Firewall
- Singularity Endpoint

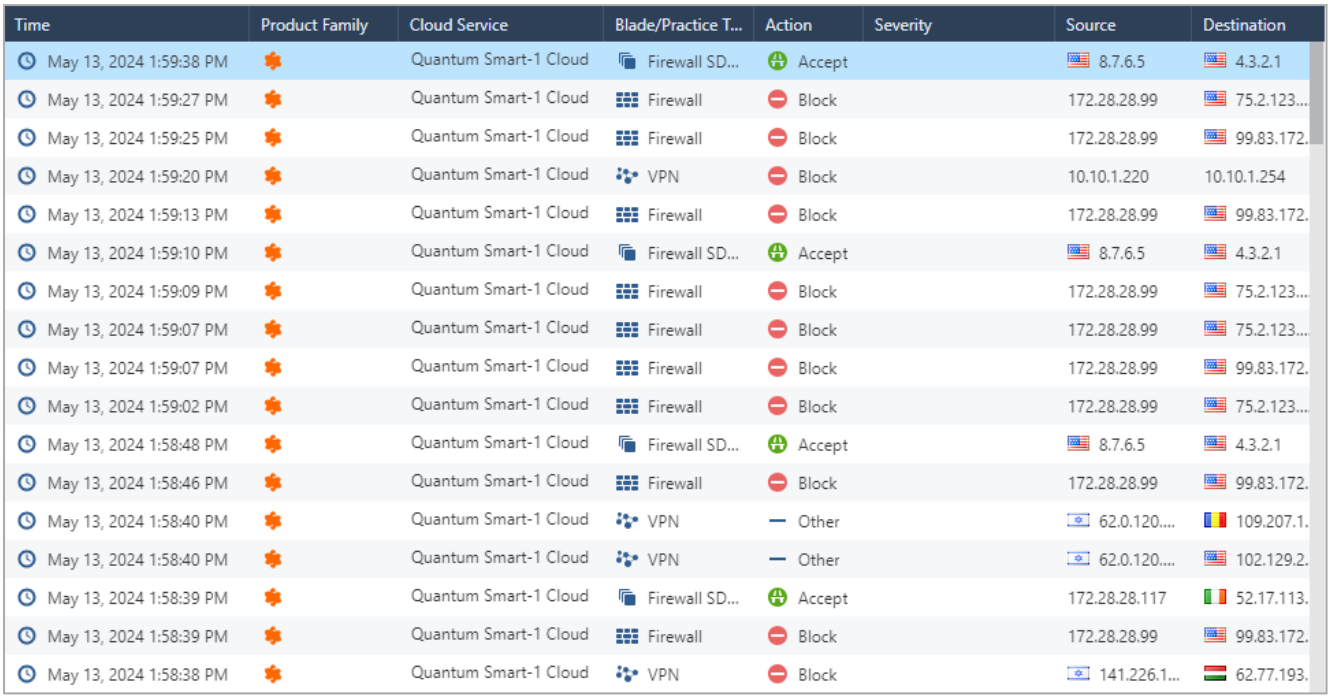
Statistics



On the **Statistics** pane, you can:

- See a bar graph of the number of events for the selected time frame.
- Filter the event data in *"Events Table" on the next page*. For example, you can filter the events data for a product family, a Blade/Practice Type and more.

Events Table



Time	Product Family	Cloud Service	Blade/Practice T...	Action	Severity	Source	Destination
May 13, 2024 1:59:38 PM		Quantum Smart-1 Cloud	Firewall SD...	Accept		8.7.6.5	4.3.2.1
May 13, 2024 1:59:27 PM		Quantum Smart-1 Cloud	Firewall	Block		172.28.28.99	75.2.123....
May 13, 2024 1:59:25 PM		Quantum Smart-1 Cloud	Firewall	Block		172.28.28.99	99.83.172.
May 13, 2024 1:59:20 PM		Quantum Smart-1 Cloud	VPN	Block		10.10.1.220	10.10.1.254
May 13, 2024 1:59:13 PM		Quantum Smart-1 Cloud	Firewall	Block		172.28.28.99	99.83.172.
May 13, 2024 1:59:10 PM		Quantum Smart-1 Cloud	Firewall SD...	Accept		8.7.6.5	4.3.2.1
May 13, 2024 1:59:09 PM		Quantum Smart-1 Cloud	Firewall	Block		172.28.28.99	75.2.123....
May 13, 2024 1:59:07 PM		Quantum Smart-1 Cloud	Firewall	Block		172.28.28.99	75.2.123....
May 13, 2024 1:59:07 PM		Quantum Smart-1 Cloud	Firewall	Block		172.28.28.99	99.83.172.
May 13, 2024 1:59:02 PM		Quantum Smart-1 Cloud	Firewall	Block		172.28.28.99	75.2.123....
May 13, 2024 1:58:48 PM		Quantum Smart-1 Cloud	Firewall SD...	Accept		8.7.6.5	4.3.2.1
May 13, 2024 1:58:46 PM		Quantum Smart-1 Cloud	Firewall	Block		172.28.28.99	99.83.172.
May 13, 2024 1:58:40 PM		Quantum Smart-1 Cloud	VPN	Other		62.0.120....	109.207.1.
May 13, 2024 1:58:40 PM		Quantum Smart-1 Cloud	VPN	Other		62.0.120....	102.129.2.
May 13, 2024 1:58:39 PM		Quantum Smart-1 Cloud	Firewall SD...	Accept		172.28.28.117	52.17.113.
May 13, 2024 1:58:39 PM		Quantum Smart-1 Cloud	Firewall	Block		172.28.28.99	99.83.172.
May 13, 2024 1:58:38 PM		Quantum Smart-1 Cloud	VPN	Block		141.226.1...	62.77.193.

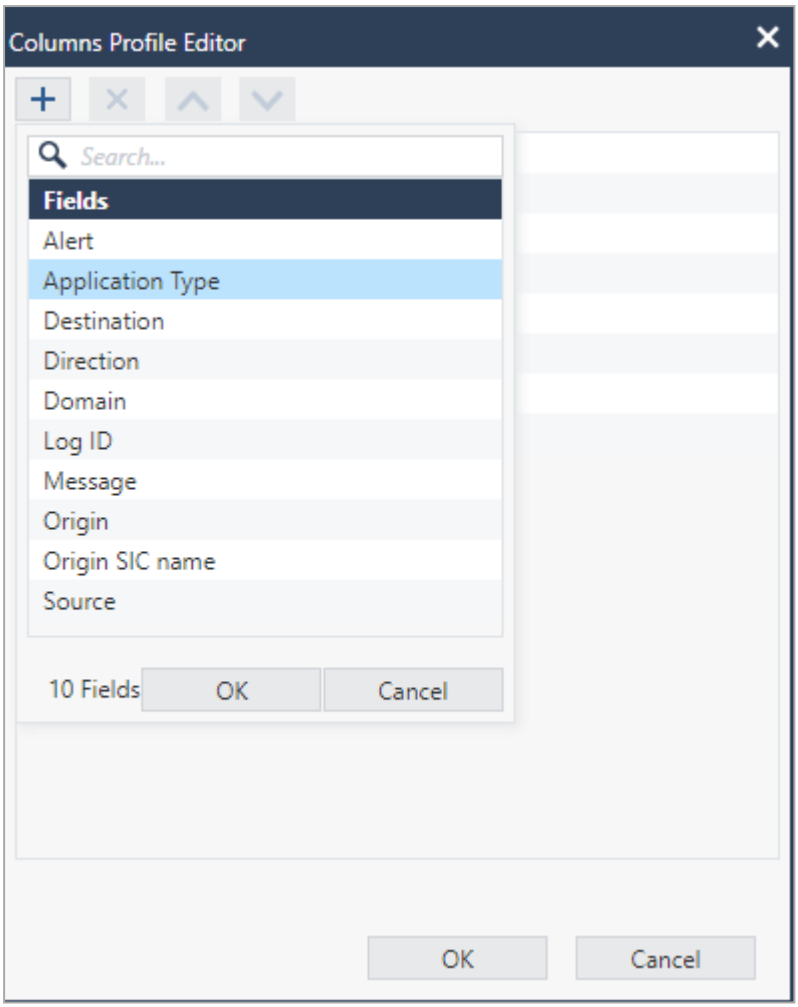
Field Name	Description
Default Fields	
Time	Time of the event.
Product Family	Check Point product family. For example, Quantum, Harmony or CloudGuard.
Cloud Service	The cloud service used by the Check Point product. For example, Quantum Gateways.
Blade/Practice Type	Software blade that triggered the event. For example, Firewall, VPN, Syslog.
Action	Action enforced on the event: ■ Accept ■ Block ■ Detect ■ Other

Field Name	Description
Severity	Severity of the event: ■ Critical ■ Informational ■ Low ■ Medium ■ High
User	User logged in at the time of the event.
Additional Fields	
Alert	Type of alert generated for the event. For example, spoof alert, mail.
Destination	Destination IP address.
Direction	Direction of the network traffic: ■ Inbound ■ Outbound
Domain	Domain name sent to DNS request.
Log ID	Unique identity for logs. Includes Type, Family, Product/Blade, Category.
Message	Message displayed for the security event. For example, *remote access client IP address and port were changed*.
Origin	Name of the first Security Gateway that reported this event.
Source	Source IP address.

Managing the Events Table

1. To view the details of a specific log, double-click the row.
2. To view the default columns, right-click the table header row and click **Default**.
3. To modify the table columns, right-click the table header row and click **Columns Profile Editor**.
4. To add a new column to the table:

a. Click **+**.



b. Select the column from the list and click **OK**.

The new column appears in the Events table and in the **Statistics** pane.

5. To remove a column from the table:

a. Select the column you want to delete and click **X**.

b. Click **OK**.

The selected column is deleted from the Events table and from the **Statistics** pane.

6. To sort the columns:

a. Select the column.

- To move the column higher in the order, click .
- To move the column lower in the order, click .

b. Click **OK**.

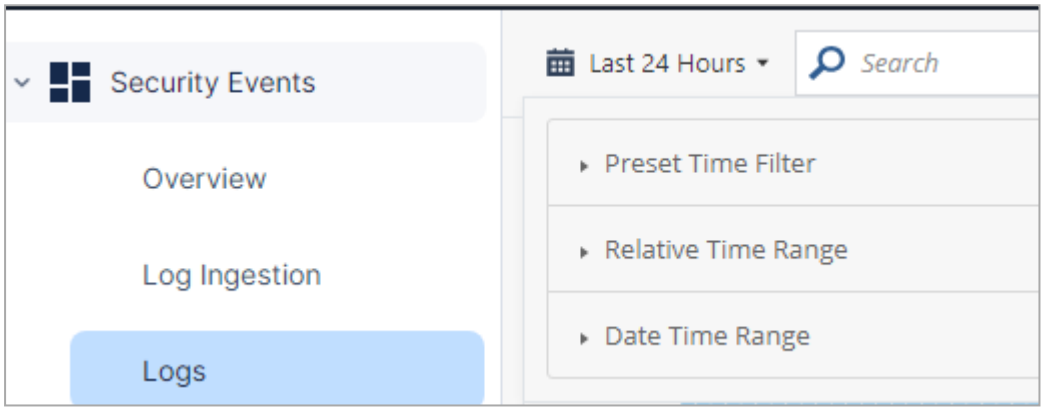
The column position is updated in the Events table and in the **Statistics** pane.

Viewing Events for a Time Period

By default, the Events table shows events for the last 7 days.

To view Events table for a specified period, use one of these to set the time range:

- Preset Time Filter
- Relative Time Range
- Date Time Range



Searching for Events

You can search for events using free text or a filter.

- To search using free text, in the **Search** field, enter the text and press **Enter**.

  For example, if you enter **Block**, the search results show all the blocked events.

- To search using a filter, click the **Search** field, select a filter and enter the text.

  For example, if the filter is **Blade/Practice Type** and text is **URL Filtering**, search as Blade/Practice Type:"URL Filtering".

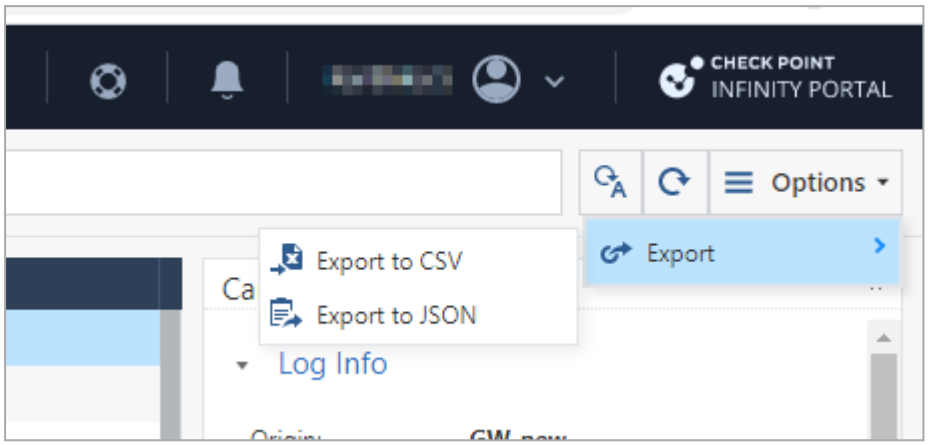
  The search results show all events with **Blade/Practice Type** as **URL Filtering**.

  Note - You can use logical operations AND, OR and NOT in the search. For example, **Block AND URL Filtering** shows the blocked events with **Blade/Practice Type** as **URL Filtering**.

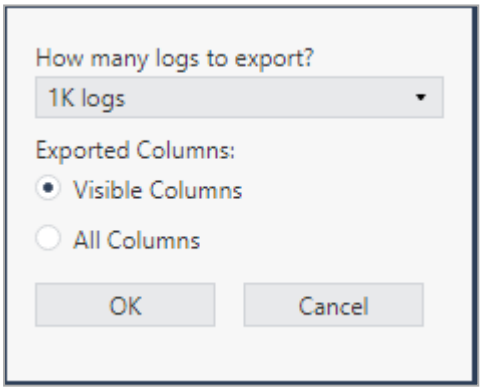
Exporting Events

You can export events from the Events table to a CSV file or to a JSON file.

1. In the **Events** window, click **Options** > **Export**.



2. Select one of these output file formats:
   - **Export to CSV**
   - **Export to JSON**
3. Enter the information for these fields:
   - In **How many logs to export** drop-down, select the number of logs you want to export.
   - In **Exported Columns**, select whether to export event data from **Visible Columns** or from **All Columns**.



4. Click **OK**.

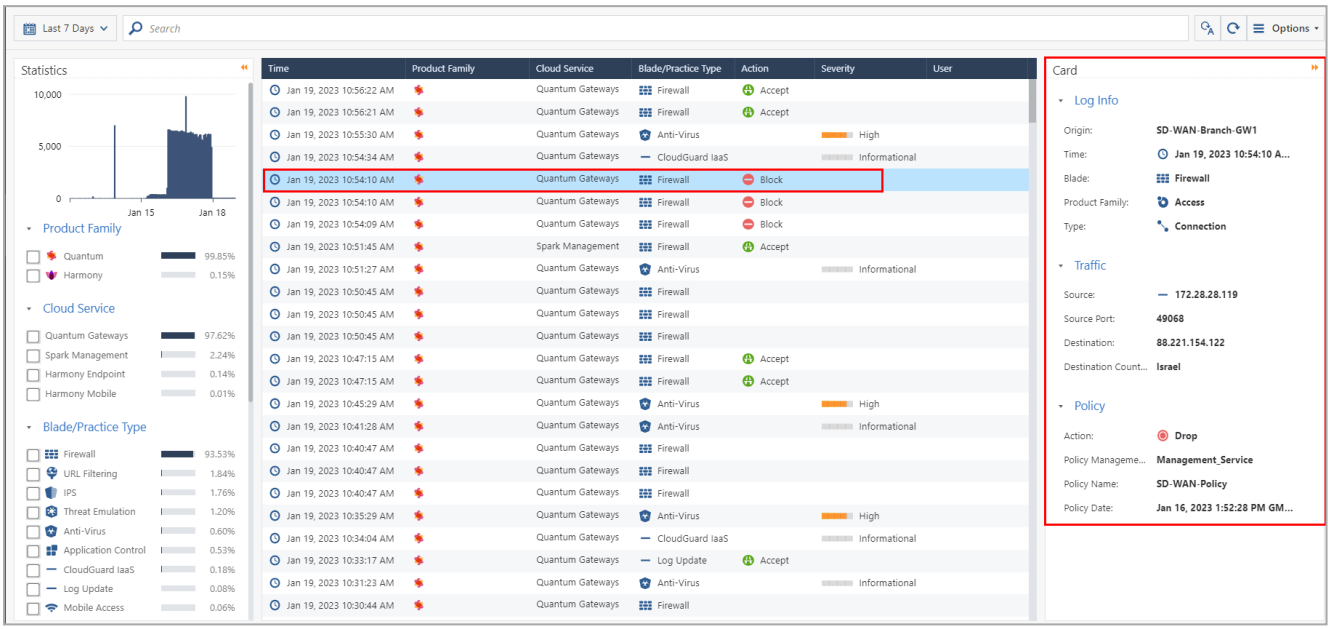
For CSV output, system generates an Excel sheet with the file name format: *Events_Logs_Date_Time.xls*.

For JSON output, system generates a json file with name format: *Events_Logs_Date_Time.json*.

Example, *Events_Logs_Oct_17_2022_01_48_24_PM*.

Card

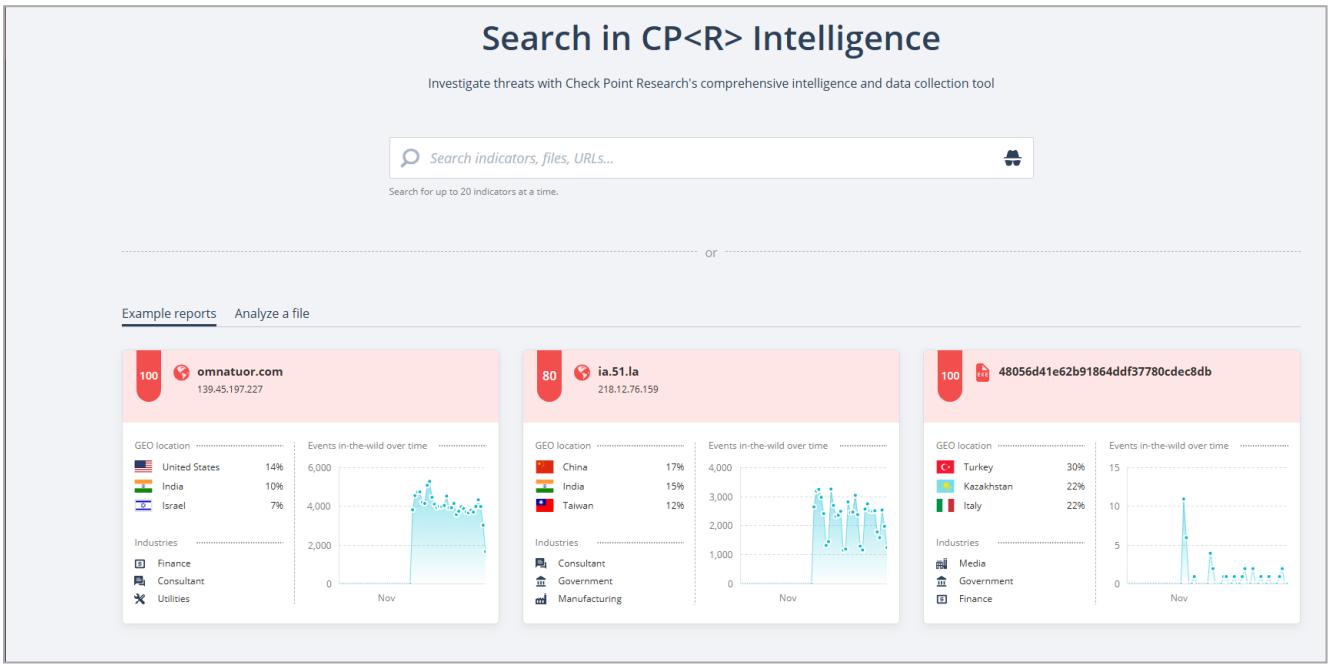
The **Card** pane shows the details for the event selected in the *"Events Table" on page 204*.



Intelligence

The **Intelligence** page shows the intelligence available for an indicator derived from internal (Check Point's ThreatCloud, Research and Threat Emulation services) and external sources (reliable closed and open third-party feeds). On this page, you can also upload a file to Check Point's Threat Emulation Sandbox for analysis.

To view the **Intelligence** page, access the XDR Administrator Portal and click **Intelligence**.



The **Example reports** tab shows examples of the available intelligence. Click the tiles to view the intelligence data.

You can use the **Intelligence** page to perform these actions:

- *"Viewing Intelligence for Indicators" below*.
- *"Analyzing a File" on page 216*.

Viewing Intelligence for Indicators

You can view the intelligence for a specific:

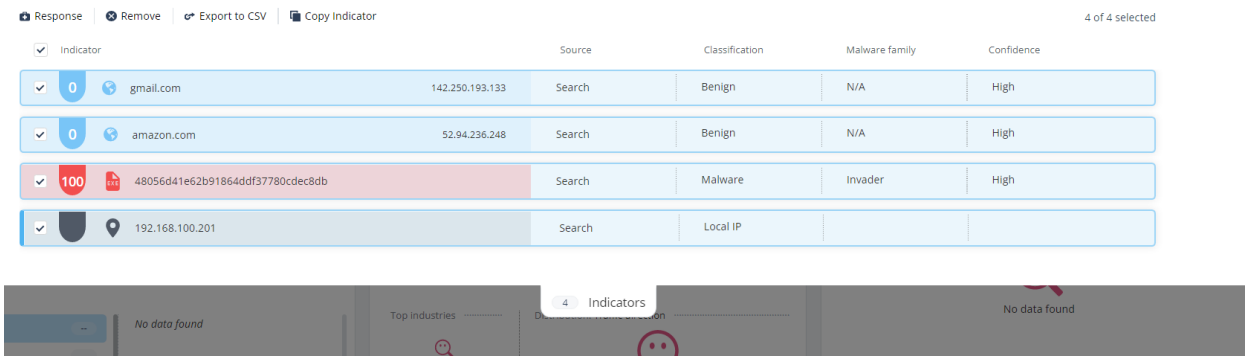
- URL
- Domain
- MD5, SHA1 or SHA256 hash of a file
- IP address

To view the intelligence for an indicator:

1. Click **Intelligence**.
2. Enter the indicator name(s) in the **Search** field and press **Enter**.

   Note - To search in Incognito mode, click the icon. This will disable actions that trigger activity on the searched websites.

   The search summary table is displayed. You can search for up to 20 indicators in a single search. The indicators can be of the same type or different types.



Item	Description
Risk	The indicator's risk level based on the Check Point reputation engine. The higher the risk, higher the degree of maliciousness. Value ranges from 1 to 100, where 100 indicates a higher risk level and/or level of maliciousness.
Indicator IP Address (For URLs and Domains)	IP address of the indicator.
File Type (For files)	Type of the file. For example, *.exe*, *.dll*.
Source	Indicates the source where you searched for the indicator. Examples - ■ If you searched the indicator from the **Search** field, then the **Source** is displayed as **Search**. ■ If you search for *amazon.com* and added an indicator from *Research > Communicating Files*, the **Source** is displayed as **amazon.com > Communicating Files**.

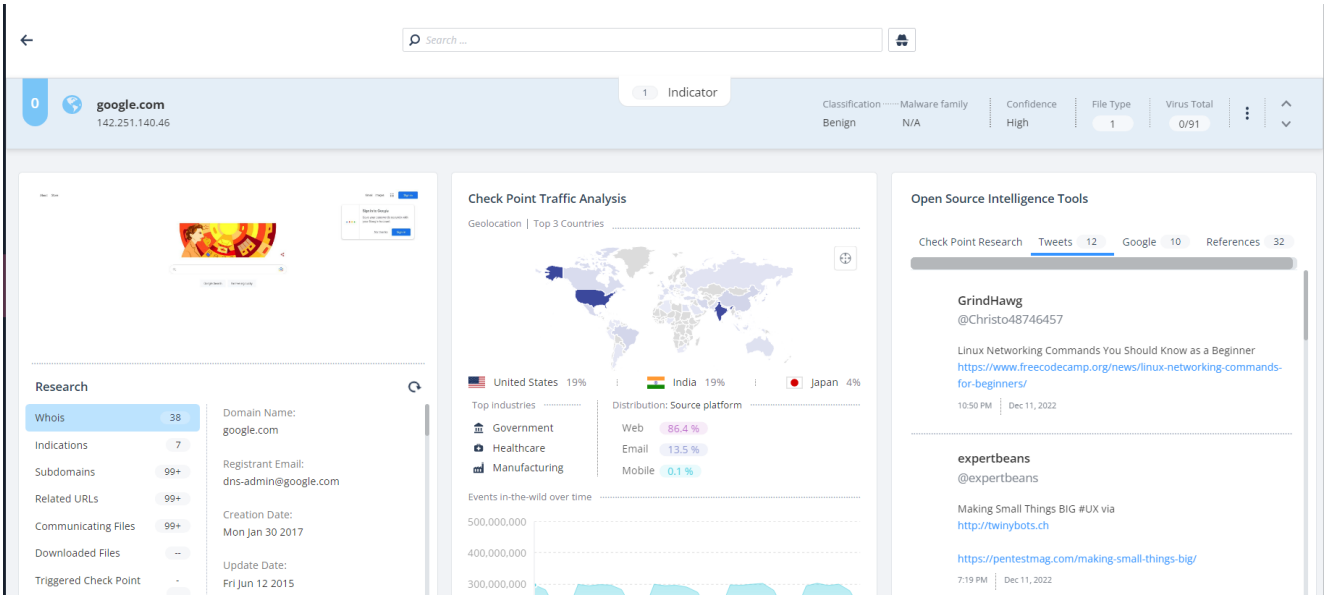
Item	Description
Classification	Threat classification determined by Check Point engines. For example, Malware or Benign.
Malware family	The malware family associated with the indicator, determined by Check Point engines. For example, Invader.
Confidence	The confidence level of the indicator's classification, determined by Check Point engines.

3. To view the Intelligence Dashboard for the indicator, click the indicator row.

Intelligence Dashboard

The Intelligence dashboard shows:

- *"Indicator Information" below*
- *"Research" on the next page*
- *"Check Point Traffic Analysis" on page 215*
- *"Open Source Intelligence Tools" on page 215*



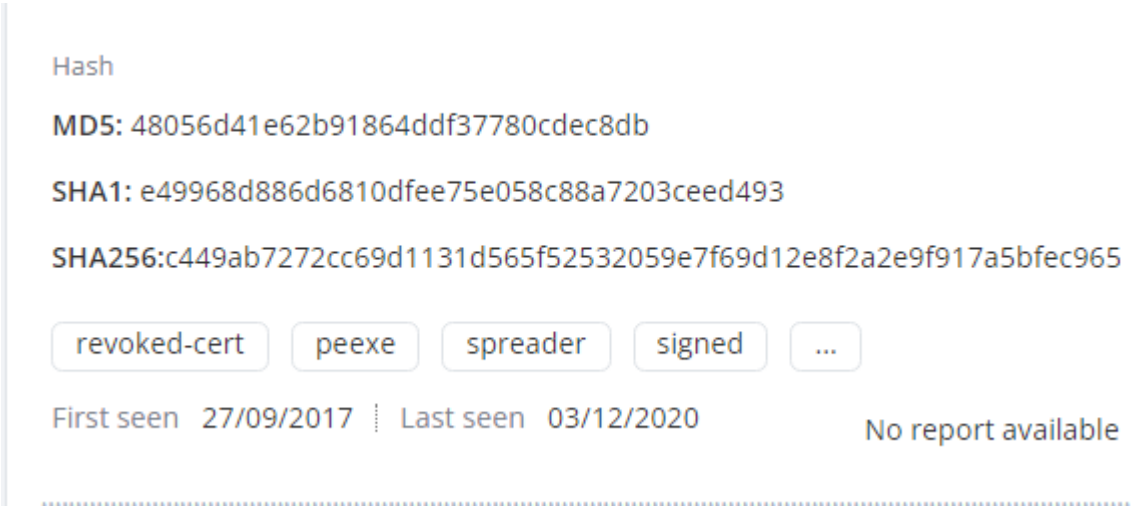
Indicator Information

The **Indicator Information** widget displays a high level overview of the analyzed indicator.

- For domains and URLs, this widget shows a live screenshot of the website.
- For files, the widget shows:

- File hash details - MD5, SHA1, and SHA256
- Tags - The file tags from VirusTotal. Indicates the different characteristics about the file.

  For example, the **signed** tag indicates that the file is signed by a valid authority.
- First seen - Date the file was first seen.
- Last seen - Date the file was last seen.
- Report - Check Point Threat Emulation Report (if available).



Research

The **Research** widget displays technical information about the indicator.

- For domain and URLs, the widget shows:

Item	Description
Whois data	Shows registered users or assignees of an Internet resource such as a domain name or IP address block.
Indications	Summarized reputation data on this domain.
Subdomains	Sub-domains for this domain.
Related URLs	URLs under this domain.
Communicating Files	Files that were seen communicating with the searched domain.
Downloaded Files	Files downloaded from this domain.
Triggered Check Point Protections	Check Point protections triggered by the domain in: • Anti-Virus • Anti-Bot • IPS
User Agent	The user agent used to contact this domain during a malicious event.

- For files, the widget shows:

Item	Description
File Names	The file names observed by Check Point for this file.
Network Activity	The network traffic the file created during Check Point Threat Emulation.
DNS Resolutions	DNS requests the file created during Check Point Threat Emulation.
Parent Process	The process that created the file.
Parent Archive	The hash of the available file archive.
Source URLs	URLs from which the file was downloaded.
Email Subjects	Email subjects that contains this file as an attachment.

Check Point Traffic Analysis

The **Check Point Traffic Analysis** widget shows a global view of the indicator's network traffic based on Check Point's global sensors. It gives a comparative view of the network traffic across different geographies. The widget shows:

Item	Description
Geolocation	The indicator's usage in different geographic locations. ■ Highlights the top 3 countries that have the highest number of hits for this indicator. ■ To view the hits in a region, hover your mouse over that region. ■ You can also zoom in and zoom out the map.
Top industries	Top 3 industries where this indicator was seen.
Distribution	Types of platforms that accessed the indicator. For example, Web, Email.
Events in-the-wild over time	The number of events over time for the indicator.

Open Source Intelligence Tools

The **Open Source Intelligence Tools** widget shows the indicator information from Open Source Intelligence (OSINT). The widget has these tabs:

Tab	Description
Check Point Research	Articles published by Check Point Research that mention this indicator and/or malware family.
Tweets	Any tweets that mention the indicator, based on Check Point Research's social media crawler.
Google	Google Search results for the indicator.
References	Web page links that contains the indicator.

Exporting the Search Summary to a CSV

1. Click **Intelligence**.
2. Enter the indicator name(s) in the **Search** field and press **Enter**.
3. In the Search Summary table, select the indicators you want to export.

By default, all the searched indicators are selected.

4. At the top, click **Export to CSV**.

   The system downloads a .csv file in the name format *Exported Summary Report Date Time*.

   For example, *Exported Summary Report 2022-12-08 12-33-37.csv*

Copying and Removing an Indicator from the Search Summary

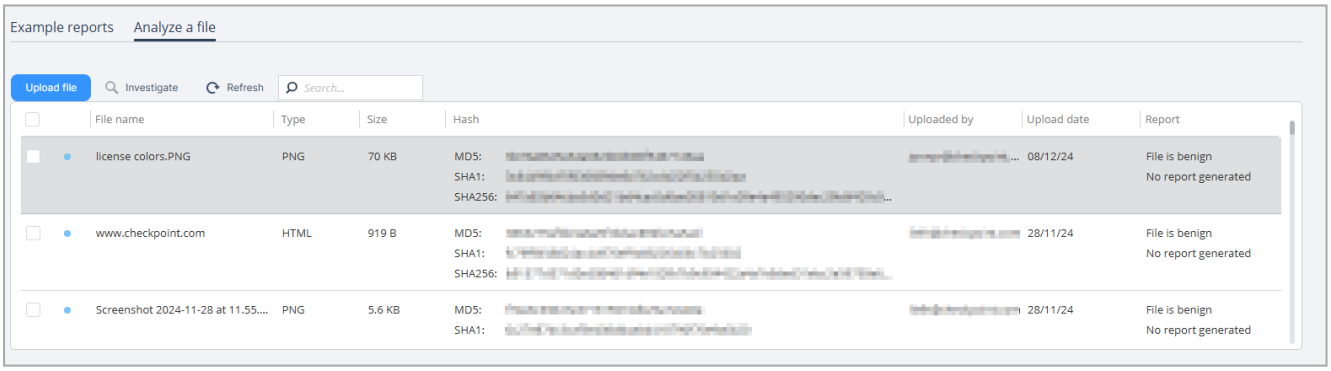
1. To copy an indicator, select the indicator in the Search Summary table and at the top, click **Copy Indicator**.

   You can copy the indicator name and search for the indicator in any external or internal resources, or share the indicator name with other applications.

2. To remove an indicator, select the indicator in the Search Summary table and at the top, click **Remove**.

Analyzing a File

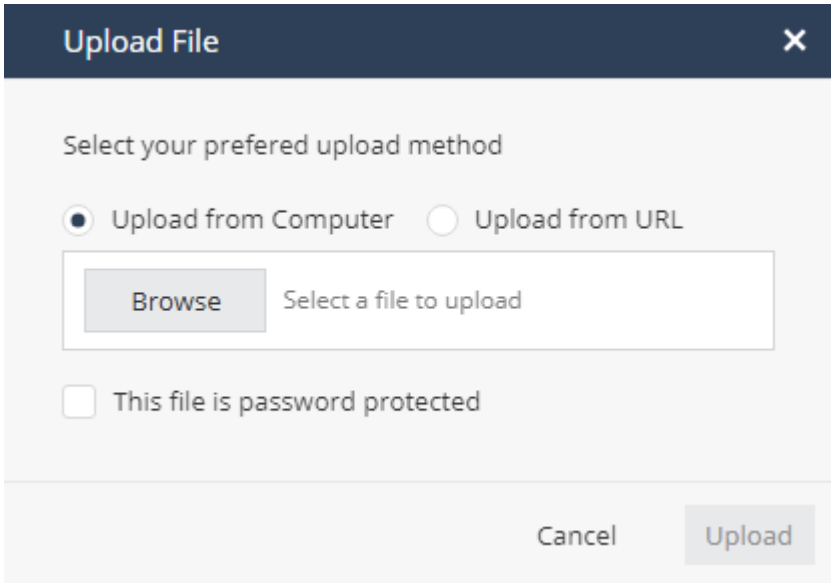
You can upload a file to Check Point's Threat Emulation Sandbox for analysis. For the supported file types, see sk106123.



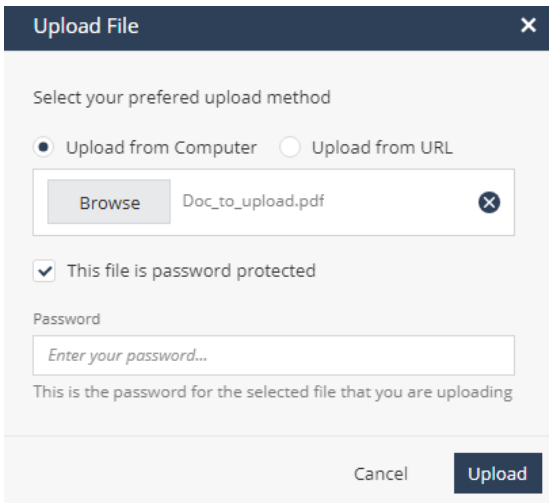
To analyze a file:

1. Go to **Intelligence** > **Analyze a file**.
2. Click **Upload file**.

   The **Upload File** window appears.



3. Do one of these:
   - To upload a file from your computer:
     a. Click **Upload from Computer** and then click **Browse**.
     b. In the Explorer window, select the file and click **Open**.
   - To upload the file from a URL:
     a. Click **Upload from URL**.
     b. Enter the URL of the file. For example, *https://databases.about.com/library/samples/address.xls*
4. If the file is protected with a password, select the **This file is password protected** checkbox and enter the password.



5. Click **Upload**.

   The file is added to the summary table.

6. To refresh the summary table, click **Refresh**.
7. To search for a file in the summary table, enter the file name in the **Search** field and press **Enter**.

   The summary table shows these file parameters:

Item	Description
File name	Name of the file.
Type	Type of the file. For example, EXE, DLL, CSV.
Size	File size.
Hash	File hash details: ■ MD5 ■ SHA1 ■ SHA256
Upload by	Email address of the user who uploaded the file.
Upload date	The date on which the file was uploaded.
Report	The verdict returned by Check Point Threat Emulation analysis. If the file was determined as malicious, the Threat Emulation report is available to download.

Investigating a File

You can view the intelligence information for a file and investigate it from the Intelligence dashboard.

To investigate about a file:

1. Go to **Intelligence** > **Analyze a file**.
2. Upload the file.
3. In the summary table, select the file to investigate. Click **Investigate**.

   The intelligence information for the file is displayed.

IOC Management

Check Point XDR supports two modes of IOC Management:

- *"New IoC Management" below*
- *"Legacy IoC Management" below*

New IoC Management

See *IoC Management Administration Guide*.

Legacy IoC Management

With **IoC Management**, you can view, create and edit Indicators of Compromise (IoCs) that apply to all the products on-boarded with XDR.

To view the **Legacy IoC Management** page, access XDR and go to **IoC Management** > **Legacy IoC Management**.

Note - The legacy IoC Management will be deprecated soon. We recommend that you migrate to the New IoC Management. For the procedure to migrate, see *"Migrating to the New IoC Management" on page 229*.

Note - For the tenants created from July 23, 2023 onwards, the Legacy IoC Management is disabled and only the *"New IoC Management" above* is supported.

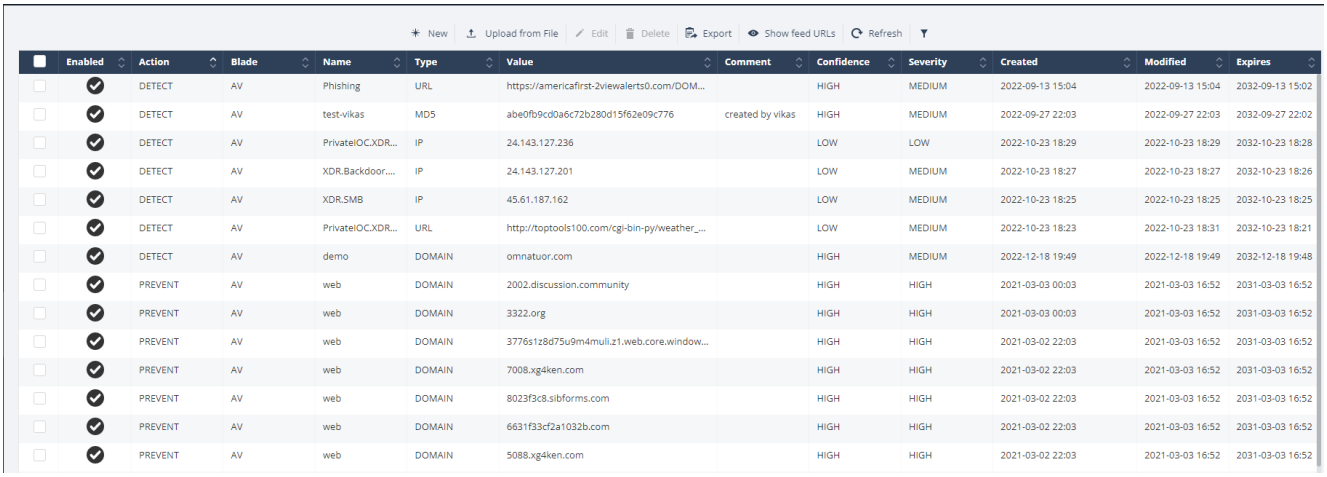
IoC Management Overview

During the XDR onboarding process, two separate feeds for *Detect* and *Prevent* actions are created. To configure these feeds on the Management Server, see *"Configuring IoC Management" on page 224*.

XDR IoC management requires no new rules or policy installation. IoC management works directly on the Security Gateway. After configuration, the Security Gateway continually fetches intelligence data stored in a *.cvs* file on the Check Point web server. You can use the CSV file link with other products that support intelligence feeds from external sources, such as cloud-based mail protection platforms.

Working with IoC Management

The IoC Management table shows only the latest 30 IoCs added to IoC Management. To view the all IoCs, click **Export** > **Export All**. See *"Exporting IoCs" on page 224*.



Enabled	Action	Blade	Name	Type	Value	Comment	Confidence	Severity	Created	Modified	Expires
✓	DETECT	AV	Phishing	URL	https://americafirst-2viewalerts0.com/DOM...		HIGH	MEDIUM	2022-09-13 15:04	2022-09-13 15:04	2032-09-13 15:02
✓	DETECT	AV	test-vikas	MD5	abe0fb9cd0a6c72b280d15f62e09c776	created by vikas	HIGH	MEDIUM	2022-09-27 22:03	2022-09-27 22:03	2032-09-27 22:02
✓	DETECT	AV	PrivateIOC.XDR...	IP	24.143.127.236		LOW	LOW	2022-10-23 18:29	2022-10-23 18:29	2032-10-23 18:28
✓	DETECT	AV	XDR.Backdoor....	IP	24.143.127.201		LOW	MEDIUM	2022-10-23 18:27	2022-10-23 18:27	2032-10-23 18:26
✓	DETECT	AV	XDR.SMB	IP	45.61.187.162		LOW	MEDIUM	2022-10-23 18:25	2022-10-23 18:25	2032-10-23 18:25
✓	DETECT	AV	PrivateIOC.XDR...	URL	http://toptools100.com/cgi-bin-py/weather_...		LOW	MEDIUM	2022-10-23 18:23	2022-10-23 18:31	2032-10-23 18:21
✓	DETECT	AV	demo	DOMAIN	omnatuor.com		HIGH	MEDIUM	2022-12-18 19:49	2022-12-18 19:49	2032-12-18 19:48
✓	PREVENT	AV	web	DOMAIN	2002.discussion.community		HIGH	HIGH	2021-03-03 00:03	2021-03-03 16:52	2031-03-03 16:52
✓	PREVENT	AV	web	DOMAIN	3322.org		HIGH	HIGH	2021-03-03 00:03	2021-03-03 16:52	2031-03-03 16:52
✓	PREVENT	AV	web	DOMAIN	3776s1z8d75u9m4muli.z1.web.core.window...		HIGH	HIGH	2021-03-02 22:03	2021-03-03 16:52	2031-03-03 16:52
✓	PREVENT	AV	web	DOMAIN	7008.xg4ken.com		HIGH	HIGH	2021-03-02 22:03	2021-03-03 16:52	2031-03-03 16:52
✓	PREVENT	AV	web	DOMAIN	8023f3c8.sibforms.com		HIGH	HIGH	2021-03-02 22:03	2021-03-03 16:52	2031-03-03 16:52
✓	PREVENT	AV	web	DOMAIN	6631f33cf2a1032b.com		HIGH	HIGH	2021-03-02 22:03	2021-03-03 16:52	2031-03-03 16:52
✓	PREVENT	AV	web	DOMAIN	5088.xg4ken.com		HIGH	HIGH	2021-03-02 22:03	2021-03-03 16:52	2031-03-03 16:52

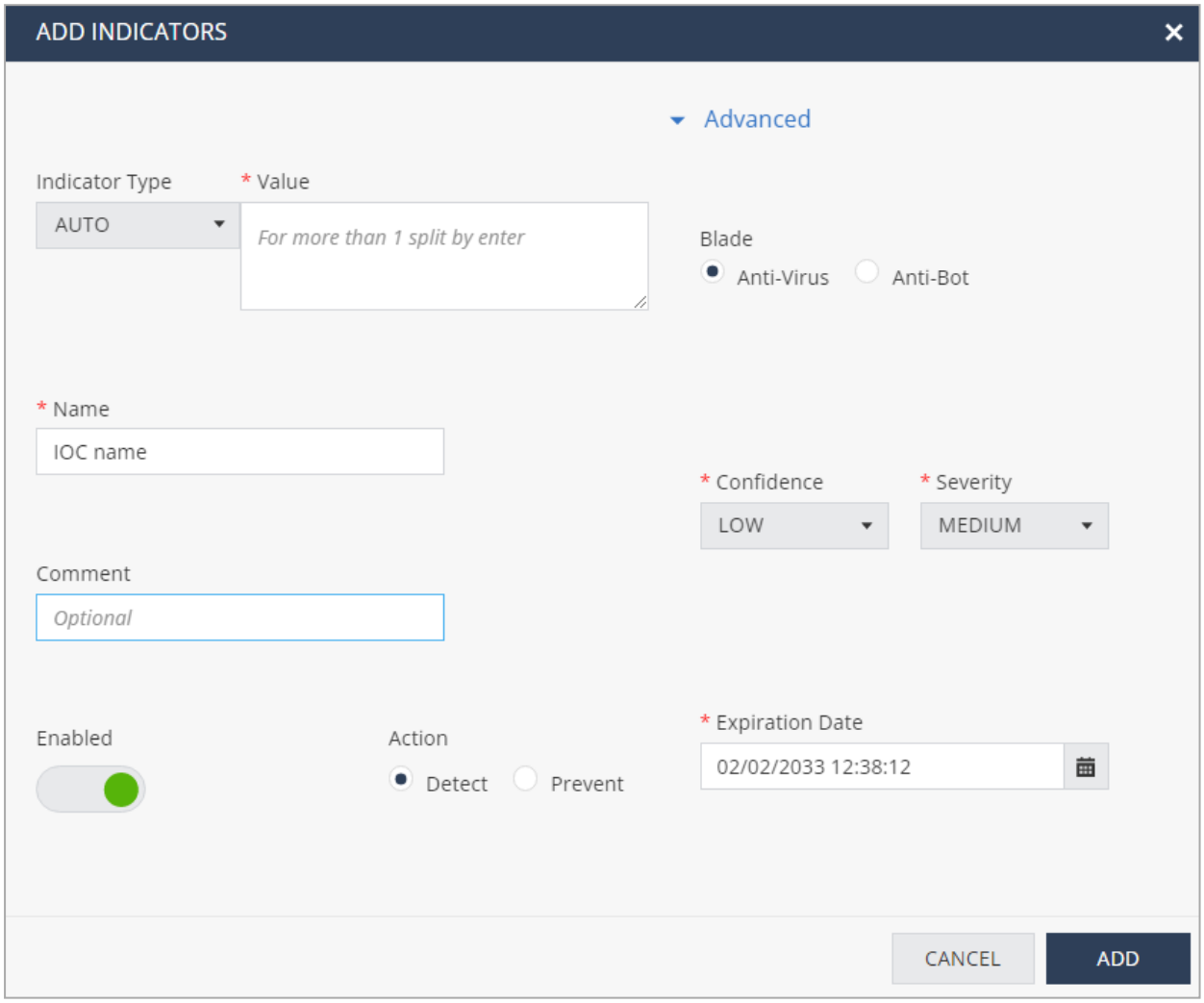
Item	Description
Enabled	Indicates whether the **Action** is enabled (enforced) on the IoC.
Action	The action enforced on the IoC: ■ Detect ■ Prevent
Blade	The software blade that the IoC triggers: ■ Anti-Bot(AB) ■ Anti-Virus(AV)
Name	Name of the IoC.
Type	IoC type: ■ Domain ■ IP address ■ URL ■ File - MD5, SHA1 or SHA256 hash key
Value	Value of the IoC.
Confidence	Confidence level of the IoC detection.
Severity	Severity of the IoC.
Created	Date and time on which the IoC was created.
Modified	Date and time on which the IoC was last modified.
Expires	Date and time when the IoC expires. After the IoC expires, it is deleted automatically.

Creating a New IoC

Note - You can also add IoCs to IoC Management from the **Incidents** tab. See *"Adding or Editing an Indicator or Artifact in IoC Management" on page 107*.

1. In the **Legacy IoC Management** menu bar, click **New**.

   The **Add Indicators** window appears.



2. Enter these:

   - **Indicator Type** - Select the IoC type.
   - **Value** - Enter the value of the IoC.
   - **Name** - Enter a name for the IoC.

- **(Optional) Comment**

  This name and comment appears in the log created when the relevant blade detects or prevents the IoC.

- Enable an **Action** - **Detect** or **Prevent**.

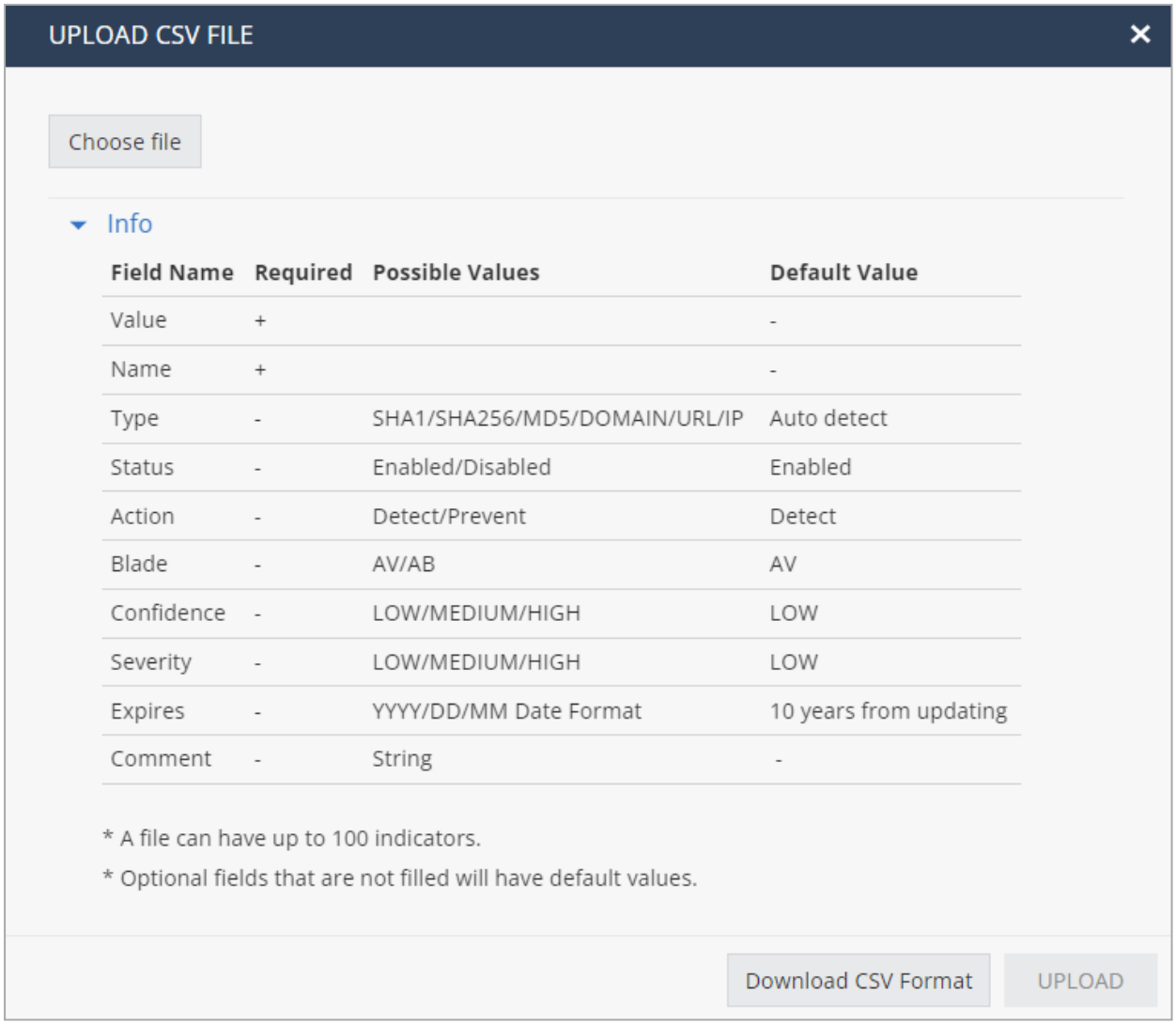
3. Click **Advanced**.
   - Select a **Blade** that the IoC triggers.
   - Select **Confidence** and **Severity** levels for the trigger.
   - Select an **Expiration Date**. After the expiration date, the IoC is deleted automatically.

     If the values for these fields are not defined, indicators are added with default values, as shown in the previous screen.
4. Click **Add**.

Adding IoCs by Uploading a CSV File

1. In the **Legacy IoC Management** menu bar, click **Upload from File**.

   The **Upload CSV File** window appears.



2. If you have the CSV file to upload:
   a. Click **Choose file**.
   b. Browse the select the file and click **Upload**.
3. If you do not know the format of the CSV file:
   a. Click **Info** > **Download CSV Format**.

      The system downloads **Upload_Format.xls**.
   b. Enter the IoC information in **Upload_Format.xls** and upload this file.

Editing and Deleting an IoC

1. To edit an IoC, select the IoC in the IoC Management table.
2. In the **Legacy IoC Management** menu bar, click **Edit**.

In the **Edit Indicators** window, enter the details and click **Update**.

3. To delete an IoC, select the IoC and click **Delete**.

Filtering IoCs

1. In the **Legacy IoC Management** menu bar, click  .

   The **Filter** pane appears.

2. Select the parameter to filter the IoCs.

   The IoC Management table refreshes and shows only the IoCs relevant to the applied filter.

Exporting IoCs

1. In the **Legacy IoC Management** menu bar, click **Export**.
2. Select one of these export options:
   - **Export All** - To export information of all the IoCs in the IoC Management table.
   - **Export Filtered** - To export information of the IoCs relevant to the applied filter.
   - **Export Selected** - To export information of only the selected IoCs in the IoC Management table.

   System downloads a CSV file with the IoC information.

Configuring IoC Management

After you successfully onboard to XDR:

1. In the **Legacy IoC Management** menu bar, click **Show feed URLs**.

   The **Feed URLS** window appears.

   When you onboard to XDR, two feeds in *.cvs* format are created for **Prevent** and **Detect** actions. To create these files again, click **Regenerate URLs**.

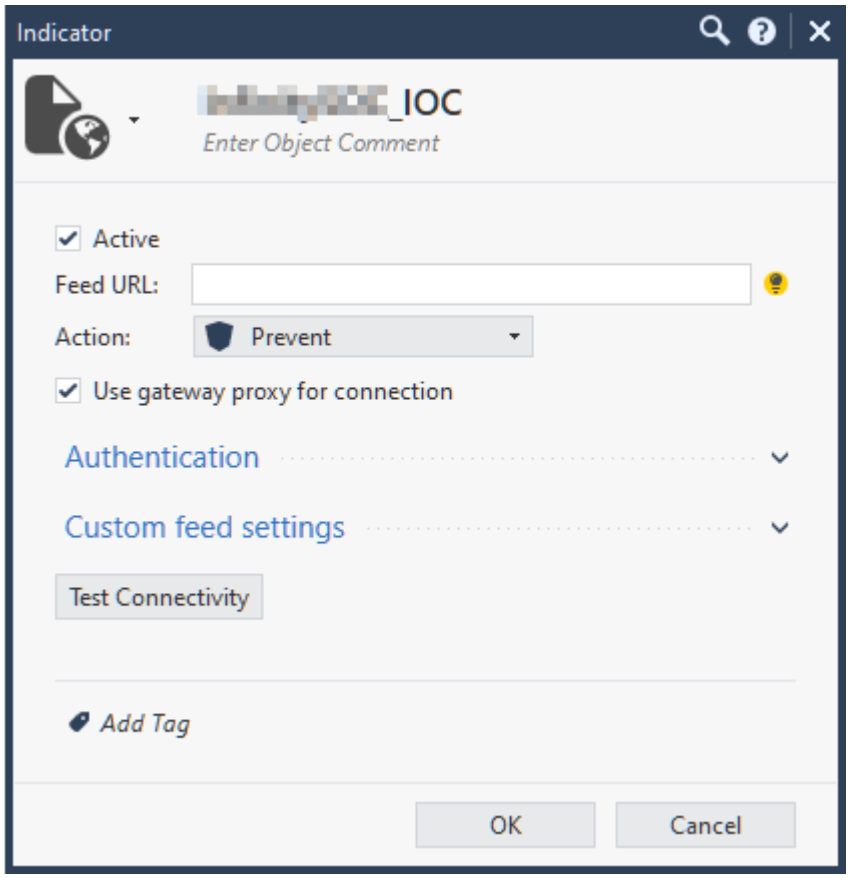
2. Copy the **Prevent URL** and the **Detect URL** to a text file.

   For example:

```
https://feeds.now.checkpoint.com/public_feeds/xxxxxxxxxx.csv

https://feeds.now.checkpoint.com/public_feeds/xxxxxxxxxx.csv
```

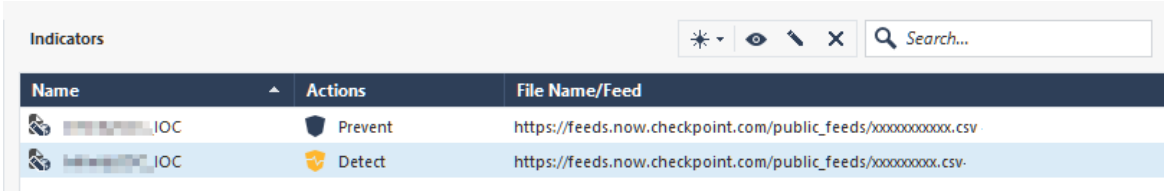
3. In SmartConsole:
   a. From the left navigation panel, click **Security Policies**.
   b. In the middle top pane, click **Threat Prevention** > **Indicators**.
   c. From the top toolbar, click **New** > **External IoC Feed**.

      The **Indicator** window appears.



   d. In **Feed URL**, enter the **Prevent URL** from step 2.
   e. In **Action**, select **Prevent** and click **OK**.
   f. Create a new **External IoC Feed** (Follow steps a to c).
   g. In **Feed URL**, enter the **Detect URL** from step 2.
   h. In **Action**, select **Detect** and click **OK**.

      You have now created IoC feeds for **Prevent** and **Detect** actions.



i. Install the Threat Prevention policy on this Security Gateway.

For more information, see Importing External Custom Intelligence Feeds in SmartConsole.

4. In **XDR**, go to **Legacy IoC Management** and click **Show Feed URLs**.

Copy the full Security Gateway commands for **Prevent** and **Detect**.

Example:

```
ioc_feeds add --feed_name InfinitySOCPrevent --transport https
--resource "https://feeds.now.checkpoint.com/public_
feeds/xxxxxxxxxx1.csv" --feed_action Prevent
```

```
ioc_feeds add --feed_name InfinitySOCDetect --transport https
--resource "https://feeds.now.checkpoint.com/public_
feeds/xxxxxxxxxx2.csv" --feed_action Detect
```

5. In SmartConsole:

a. From the left navigation panel, click **Gateways & Servers**.

b. Right-click the Security Gateway object and click **Actions** > **Open Shell**.

Alternatively, connect to the command line on the Security Gateway through a SSH client.

6. Run the commands you copied in step 4 from XDR:

Example:

```
ioc_feeds add --feed_name InfinitySOCPrevent --transport https
--resource "https://feeds.now.checkpoint.com/public_
feeds/xxxxxxxxxx1.csv" --feed_action Prevent
```

```
ioc_feeds add --feed_name InfinitySOCDetect --transport https
--resource "https://feeds.now.checkpoint.com/public_
feeds/xxxxxxxxxx2.csv" --feed_action Detect
```

7. Close the shell after the operation completes successfully.

Note - If you generate the URLs again, the old feeds are no longer accessible. You must update the feeds on the Security Gateway and the indicator URL in SmartConsole.

Testing IoC Management

As a simple test, block access to a website.

If the site is still accessible after you update the IoC feed:

1. Connect to the command line on the Security Gateway for each Cluster Member.
2. Log in to the Expert mode.
3. Fetch feeds in debug mode:

   ```
   $FWDIR/bin/ioc_feeder -d -f
   ```

4. Examine this configuration file:

   `$FWDIR/conf/ioc_feeder.conf`

   If the file is corrupt, delete the feed, make the required changes in the feed, and add the feed again.

5. Examine these files for errors:

   - `$FWDIR/log/ioc_feeder.elg`

     For example:

     ```
     Feed log External IOC - External Indicators processing
     failedInfinitySOCPrevent: Failed to fetch feed. Resource:
     https://feeds.now.checkpoint.com/public_
     feeds/PersonalFeed.csv, Reason: Peer certificate cannot
     be authenticated with given CA certificates
     ```

     ```
     InfinitySOCDetect: Failed to fetch feed. Resource:
     https://feeds.now.checkpoint.com/public_
     feeds/PersonalFeed.csv, Reason: Peer certificate cannot
     be authenticated with given CA
     certificateshttps://supportcenter.checkpoint.com/supportc
     enter/portal?eventSubmit_
     doGoviewsolutiondetails=&solutionid=sk132193
     ```

   - `$FWDIR/log/ext_ioc_push.elg`

Migrating to the New IoC Management

Prerequisite

You must have **Admin** role in **Global Roles** or **Specific Service Roles**.

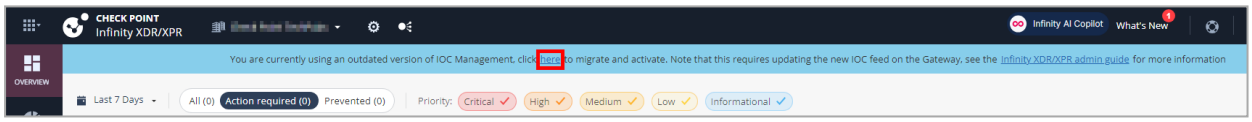
Changes to IoCs During Migration

- In the new IoC Management, enforcement of the IoC depends only on the Threat Prevention policy protection mode set in the related product. For more information, see *"New IoC Management" on page 219*.
- The legacy IoC Management is disabled.

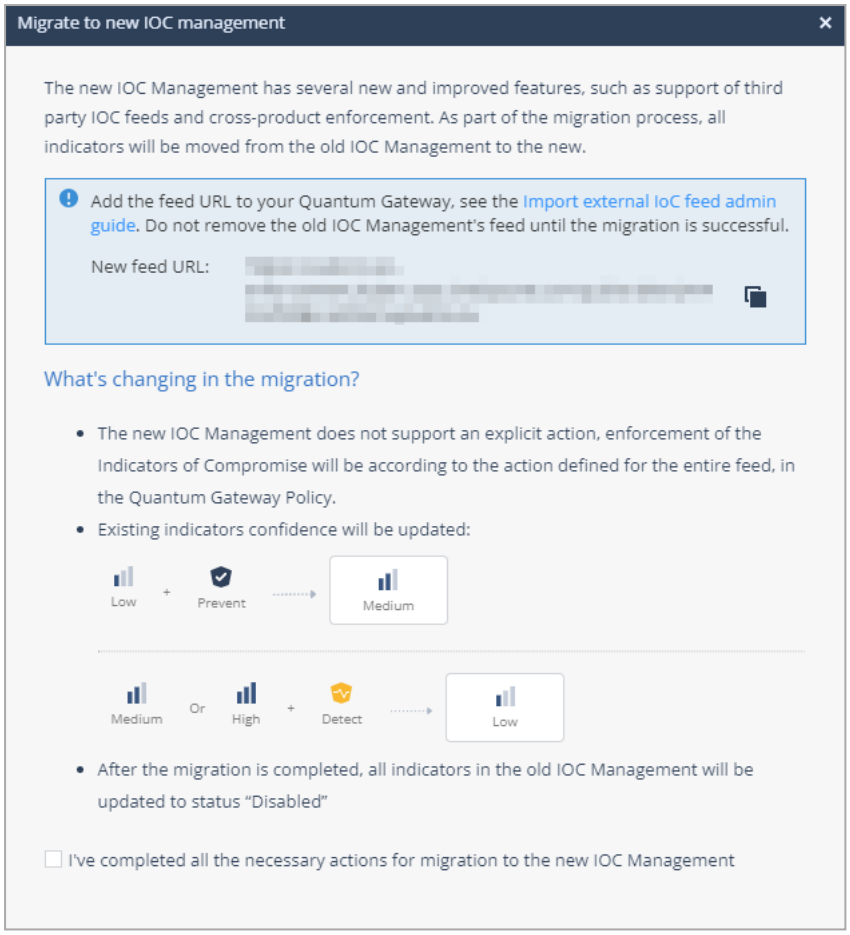
Procedure

To migrate to the New IoC Management:

1. On the **Overview** page, click the link in the banner at the top.



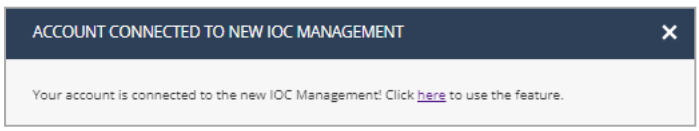
   The **Migrate to New IoC Management** pop-up window appears.



2. If you are using the Check Point Security Gateway as an enforcer, then click to copy the **New Feed URL** and add it as an IoC feed in the SmartConsole. For more information, see Importing External Custom Intelligence Feeds in SmartConsole.
3. Select the **I've completed all the necessary actions for migration to the new IoC Management** checkbox.
4. Click **Start Migration**.

   To view the progress of the migration, go to **Settings** > **Audit logs**.

   After the migration is successful, a confirmation message appears, and the legacy IoC Management and its IoCs are disabled.



   Now, your Check Point Portal tenant is configured to use the new IoC Management.
5. If you are using the Check Point Security Gateway and if you have performed step 2, then remove the old feed URLs.

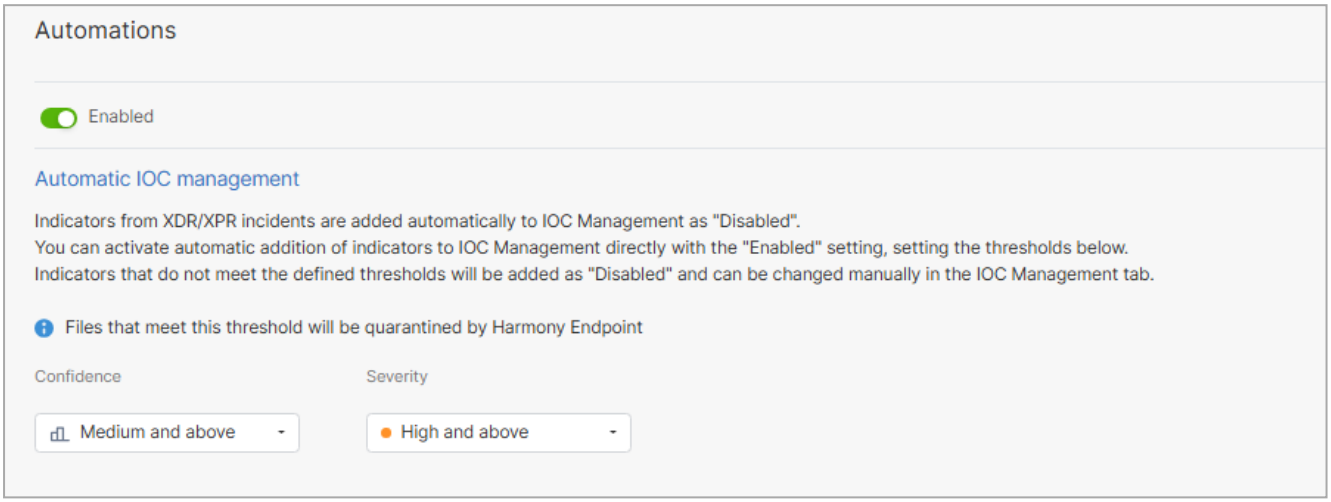
Policy

In the **Policy** section, you can:

- Configure automatic response when XDR detects an IoC with a specified severity. See *"Automations" on page 232*.
- Save queries as a rule to generate XDR incidents when a Threat Hunting event matches the rule. See *"Custom Rules" on page 233*.
- Configure exclusions for assets, artifacts and insights that are not malicious. See *"Exclusions" on page 236*.

Automations

In the **Automations** page, you can configure XDR to take prevention actions automatically when an incident is generated with a specified confidence and severity. Currently, the automatic response supports adding indicators to IoC Management.



For example, you can configure the automatic response that all IoCs with severity **High** and above must be added to IoC Management with the **Enabled** status.

Notes:

- By default, XDR automatically adds all the indicators to IoC Management with the **Disabled** status.
- For the tenants created from July 23, 2023 onwards, the *"Legacy IoC Management" on page 219* is disabled and only the *"New IoC Management" on page 219* is supported.

To configure an automatic response:

1. Go to **Policy** > **Automations**.
2. Enable the toggle button.
3. Select the required threshold (**Confidence** and **Severity** level).

Note - If the IoC is a file that matches the configured threshold, and if it is detected in a machine with Endpoint Security Security client installed, the file will be quarantined by Endpoint Security.

Custom Rules

Custom Rules allows you to save queries as a rule to generate XDR incidents when a Threat Hunting event matches the rule.

To create a custom rule:

1. Go to **Investigate** > **Threat Hunting**.
2. Run a query and click the  icon from the top right corner of the page.

3. In the **Rule name** field, enter a rule name.
4. In the **Attack name** field, enter a name. For example, Emotet.

   The system prefixes *XDR.CUSTOM* to the attack name, for example *XDR.CUSTOM.Emotet*. This is useful in finding insights and incidents generated by a custom rule.
5. From the **Confidence** field, select a confidence level for the detection.
6. From the **Severity** field, select a severity level for the incident.
7. In the **Description** field, enter a description for the rule.
8. (Optional) In the **Comment** field, enter comment, if any.
9. To generate incidents if the Threat Hunting events match the custom rule, toggle **Status** to **On**. Otherwise, the custom rule is only saved and does not generate incidents upon matching activity.
10. Click **Add**.

11. To view all custom rules created, go to **Policy** > **Custom Rules**.

Column Name	Description
Status	Indicates whether the custom rule is enabled or not.
Rule Name	Name of the rule.
Confidence	Confidence level of the detection.
Severity	Severity of the detection.
Attack Name	Name of the attack.
Description	Description of the rule.
Creator	Name of the person that created the rule.
Creation Date	Date and time when the rule was created.
Date Last Edited	Date on which the rule was last modified.
Comment	Comment about the rule.

To export the rules to an excel in CSV format, click **Export All (CSV)**.

Managing Custom Rules

To edit a custom rule:

1. Go to **Policy** > **Custom rules**.
2. Select the rule you want to edit and click **Edit in Threat Hunting**.

   The system redirects you to the **Threat Hunting** page that shows the custom rule and the query.
3. Edit the custom rule and click **Update**.

To delete a rule:

1. Select the rule you want to delete and click **Delete**.
2. Click **Yes** in the confirmation dialog.

Running a Custom Rule

To manually run the Custom Rule:

1. Go to **Policy** > **Custom rules**.
2. Select the rule and click **Run in Threat Hunting**.

   The system redirects you to the **Threat Hunting** page that shows the custom rule and the query.

Exclusions

Exclusions allow you to exclude assets, artifacts and insights from generating incidents.

Note - These exclusions affect only the creation of incidents in Check Point XDR and do not affect the policies of the on-boarded products.

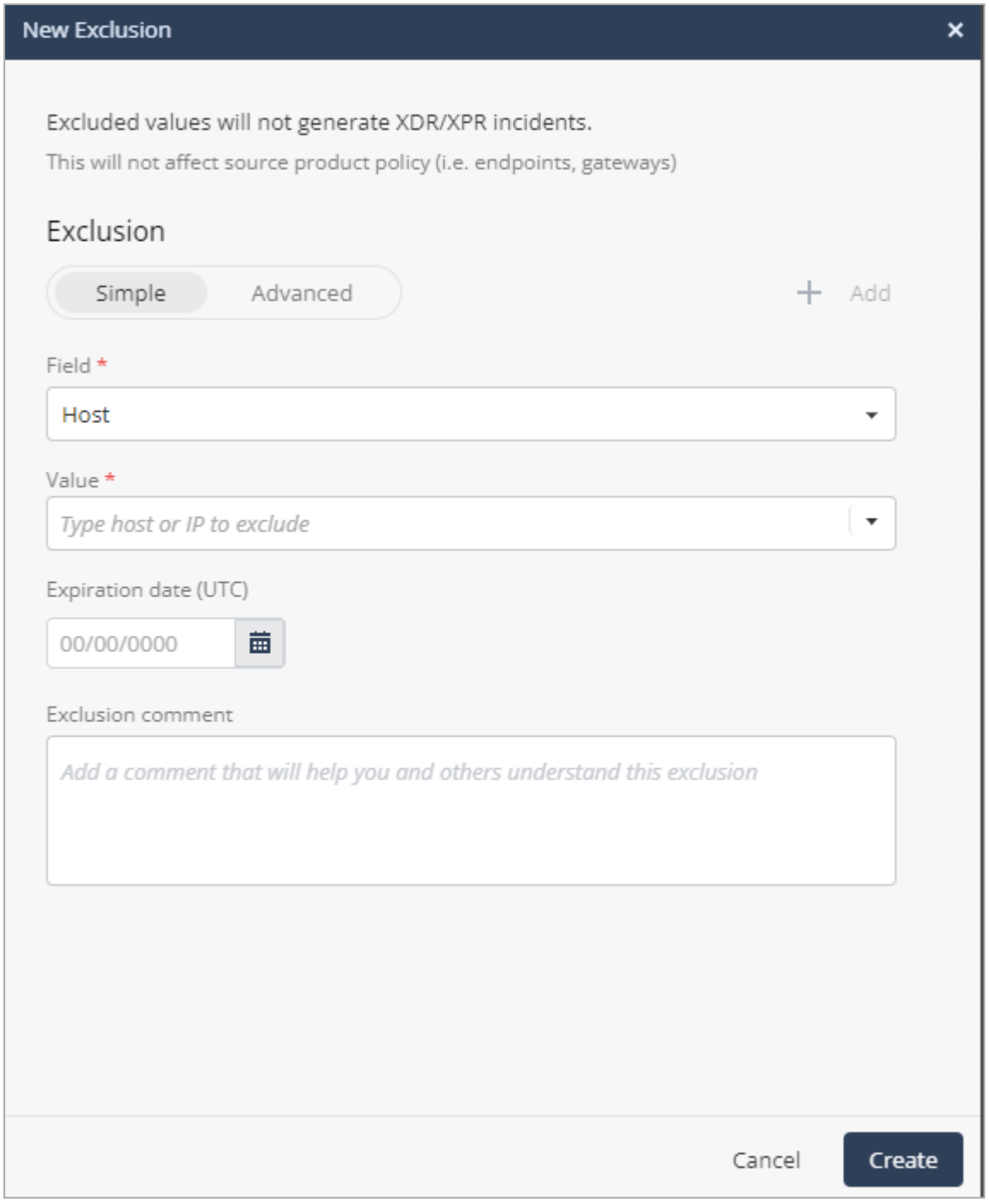
Simple Exclusions

Simple exclusions allow you to exclude assets and artifacts, so that XDR excludes them from both current and future incidents. For example, an asset that represents an approved network scanner.

To create a Simple exclusion for the XDR incidents:

1. Go to **Policy** > **Exclusions**.
2. Click **New**.

   The **New Exclusion** window appears. The **Simple** exclusion tab is displayed by default.



3. From the **Field** list, select the type of asset / artifact:
   - To add an exclusion for a machine:
     i. Select **Host**.
     ii. In the **Value** field, enter the host name or the IP address.
   - To add an exclusion for an email address, select **Email address** and enter the email address.

- To add an exclusion for a URL, select **URL**, and enter the URL.
- To add an exclusion for a file MD5 key, select **File MD5**, and enter the file MD5 key.
- To add an exclusion for IP address:
  i. Select **IPv4**.
  ii. In the **Value** section:
    - To add single IP address, select **Single** and enter the IP address.
    - To add a range of IP address, select **Range** and enter the **From** and **To** IP address.
    - To add the IP address in CIDR, select **CIDR** and enter the **Subnet** and **Prefix**.

4. (Optional) In the **Expiration date (UTC)** field, select an expiration date for the exclusion. After this date, XDR starts creating incidents for this asset/artifact. By default, there is no expiry date for an exclusion.
5. (Optional) In the **Exclusion comment** section, enter a description about the exclusion.
6. Click **Create**.

Advanced Exclusions

Advanced exclusions allow you to exclude insights so that XDR excludes them from generating future incidents. Optionally, you can also exclude insights generated in the past. If all the standalone insights of an incident are excluded, then the incident is also excluded.

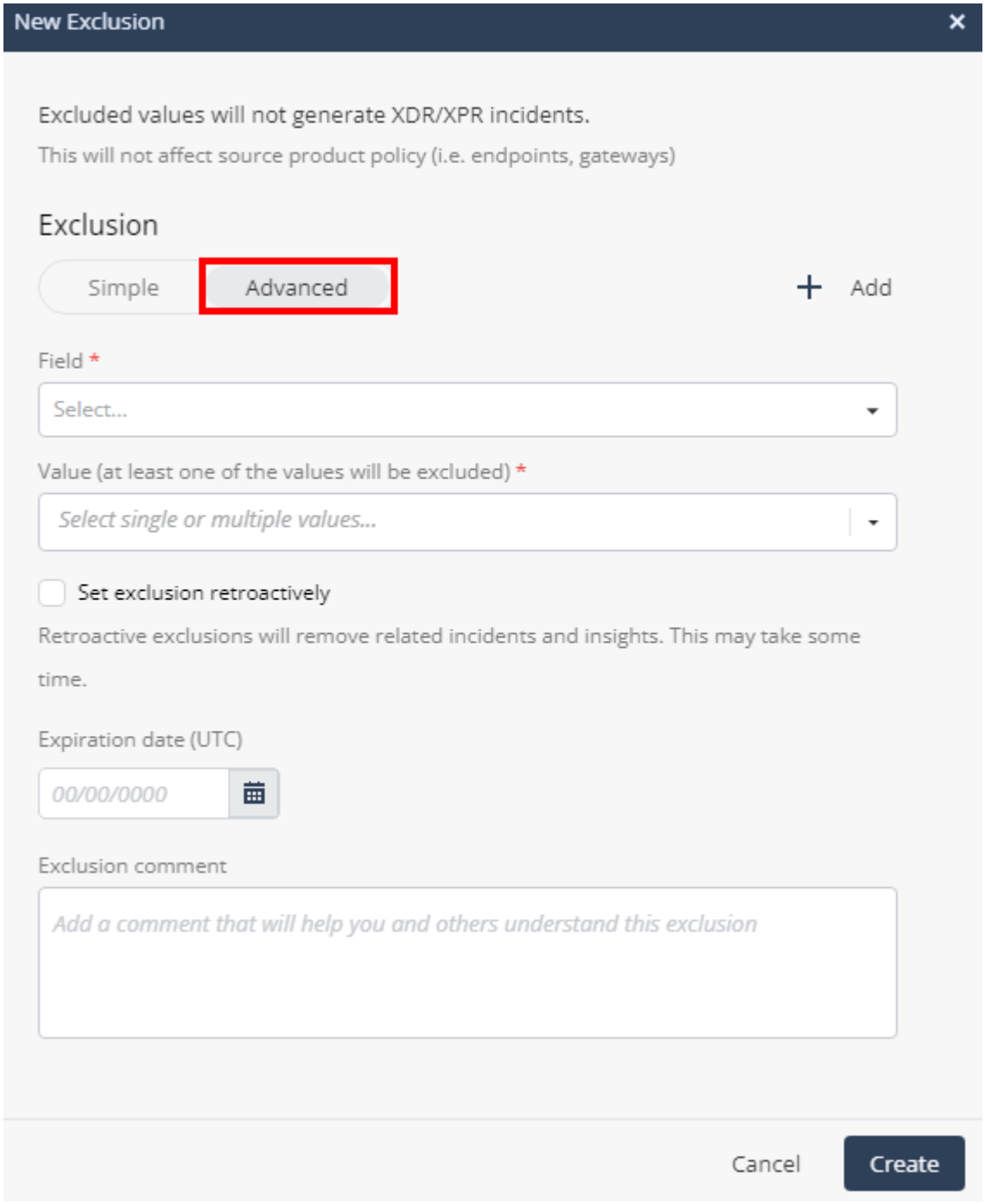
Note - You can also create Advanced Exclusions from the:

- **Overview** page. See *"Creating Advanced Exclusions from an Incident" on page 76*.
- **Insights & Forensics** page. See *"Creating an Advanced Exclusion from an Insight" on page 113*.

To create an Advanced Exclusion:

1. Go to **Policy** > **Exclusions**.
2. Click **New**.

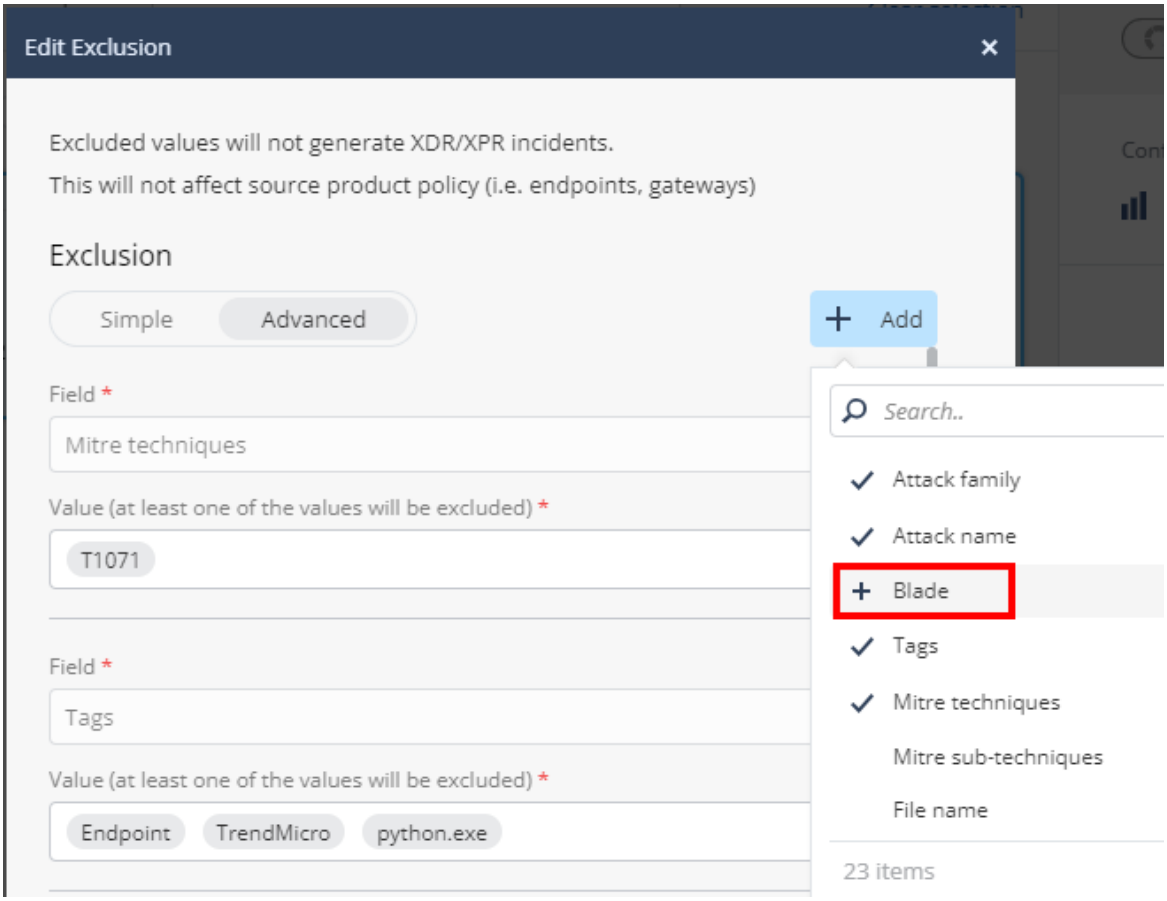
   The **New Exclusion** window appears.
3. Click the **Advanced** tab.



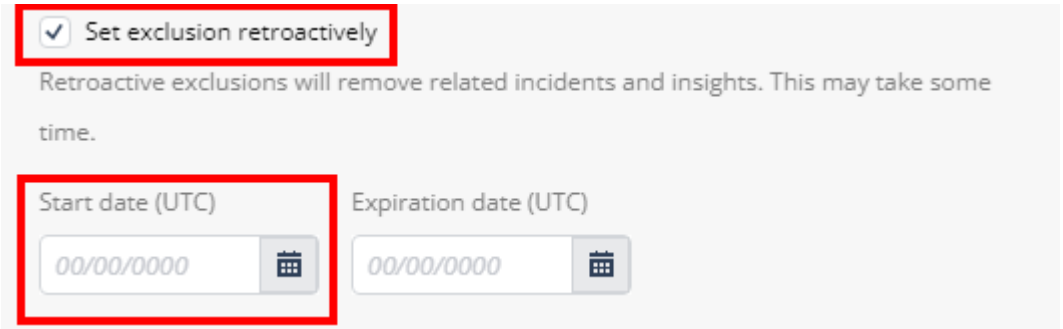
4. From the **Field** list, select the insight field(s) to be excluded. Fields are the column names in the **Insights & Forensics** page.

5. To add or remove a field, click **+ Add**. The fields already selected are marked with ✓.

- To add, hover over the field name and click **+**.
- To remove an already selected field, click the field name.



6. In the **Value** field, enter the field values to be excluded. XDR applies this exclusion on insights that contain all the above fields and any of these values.
7. Repeat steps 5 and 6 to add another field and value.
8. (Optional) To exclude the incidents already generated based on this insight:
   a. Select the **Set exclusion retroactively** checkbox.

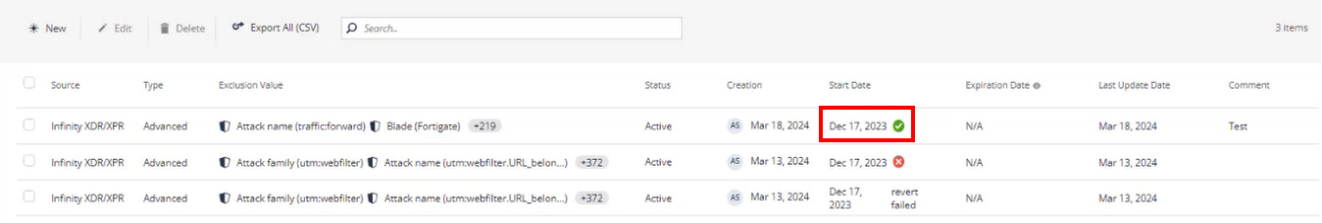


b. In the **Start date (UTC)** field, select a date within the last 90 days. XDR excludes all the incidents that were generated from this date based on this insight. To revert the exclusion, see *"Reverting a Retroactive Exclusion" below*.

9. (Optional) In the **Expiration date (UTC)** field, select an expiration date for the exclusion. After this date, XDR generates incidents for this insight. By default, there is no expiry date for an exclusion.
10. (Optional) In the **Exclusion comment** section, enter a description about the exclusion.
11. Click **Create**.

The exclusion is added to the **Exclusions** table.

in the **Start Date** column indicates that the system has successfully executed the retroactive exclusion. indicates that the system failed to execute the retroactive exclusion.

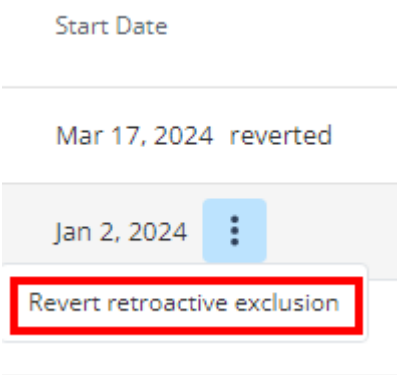


Reverting a Retroactive Exclusion

You can revert a retroactive exclusion to restore the incidents excluded by this exclusion.

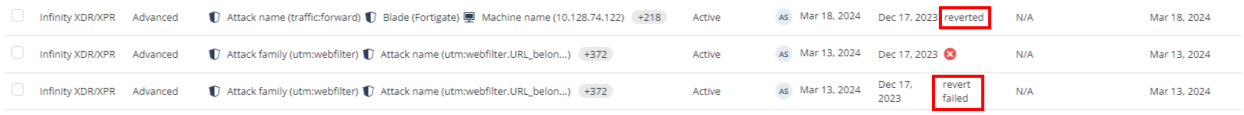
To revert a retroactive exclusion:

1. Go to **Policy** > **Exclusions**.
2. In the **Exclusions** table, for the exclusion you want to revert, hover over the **Start Date**, click and then click **Revert retroactive exclusion**.



If the revert is successful, *reverted* message appears in the **Start Date** column.

If revert fails, *revert failed* message appears.



Editing an Exclusion

To edit an exclusion:

1. Go to **Policy** > **Exclusions**.
2. Select the exclusion and click **Edit**.

   The **Edit Exclusion** window appears.
3. Make the necessary changes for the exclusion and click **Submit**.

Note - You cannot edit an exclusion for which retroactive or revert operation is in progress.

Exporting Exclusions

To export the exclusions:

1. Go to **Policy** > **Exclusions**.
2. Click **Export All (CSV)**.

The system downloads the report in the CSV format.

Settings

In the **Settings** section, you can:

- View the integrated third-party security products. See *"Integrations" on page 244*.
- View the volume of product logs processed by XDR and compare it with the actual entitlement. See *"Log Processing" on page 333*.
- View XDR activity report. See *"Reports" on page 350*.
- Send email, Slack and Microsoft Teams notifications when an incident with a specified priority is generated. See *"Notifications" on page 358*.
- View the record of activities in XDR. See *"Audit Logs" on page 369*.

Integrations

Check Point XDR (formerly Infinity XDR/XPR) allows you to integrate third-party security products for unified security coverage. It analyzes the security events from the third-party security products and generates incidents with an appropriate priority based on the severity and confidence level of the detection, and provides automatic mitigation to the incident.

Note - Check Point XDR fetches alerts from the third-party integration and creates incidents based on its detection rules. While alert details are the same in both systems, incident information may differ. For more information about the incident, refer to the third-party system.

Check Point XDR supports integrations with these third-party security products:

- *"Microsoft 365 Defender for Endpoint" on page 245*
- *"Fortinet FortiGate Next Generation Firewall" on page 249*
- *"CrowdStrike Falcon" on page 263*
- *"Singularity Endpoint" on page 271*
- *"Palo Alto Networks Next Generation Firewall" on page 282*
- *"Trend Vision One for Endpoint" on page 305*
- *"Cisco Firepower Threat Defense" on page 311*
- *"Okta" on page 328*

Microsoft 365 Defender for Endpoint

Microsoft 365 Defender for Endpoint is an enterprise endpoint security platform designed to help enterprise networks prevent, detect, investigate, and respond to advanced threats.

XDR analyzes the alerts generated in Microsoft 365 Defender for Endpoint and takes relevant corrective action, such as quarantine a file, terminate a process, or isolate a machine automatically through Check Point Playblocks.

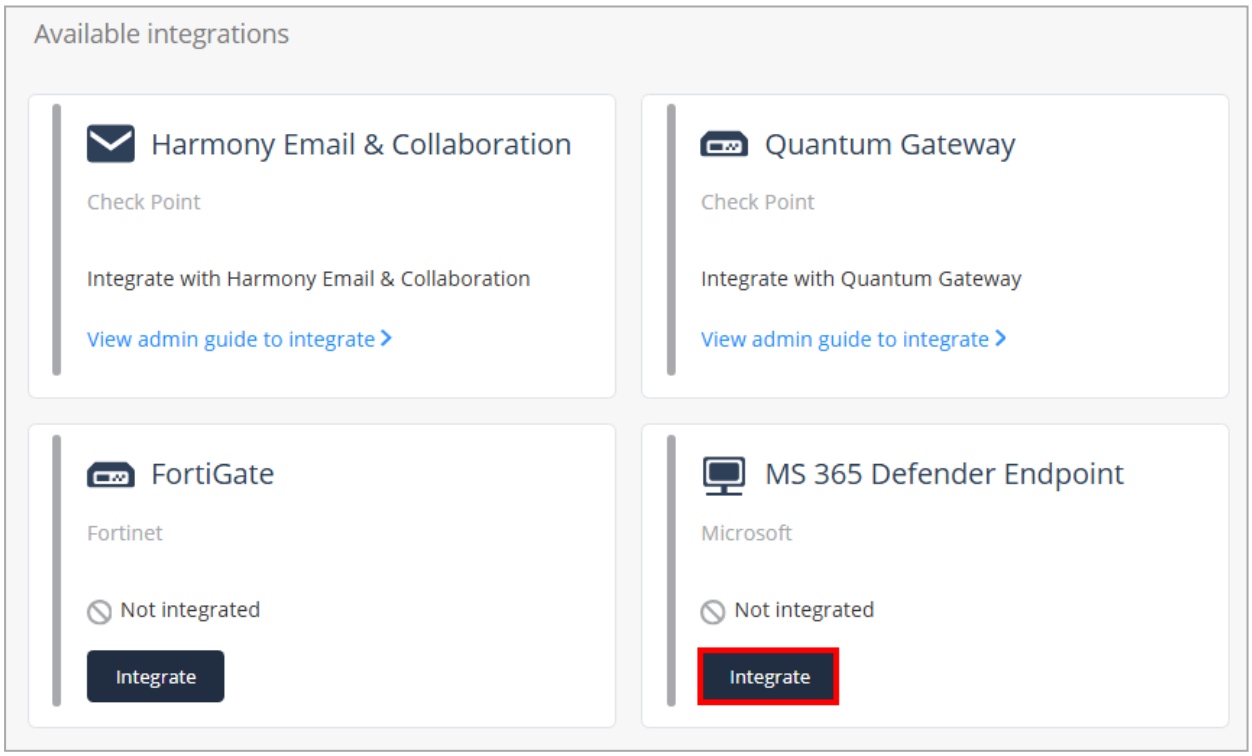
For more information on suggested preventive actions, see **Incidents Overview** > *"Prevention" on page 70*.

Prerequisites

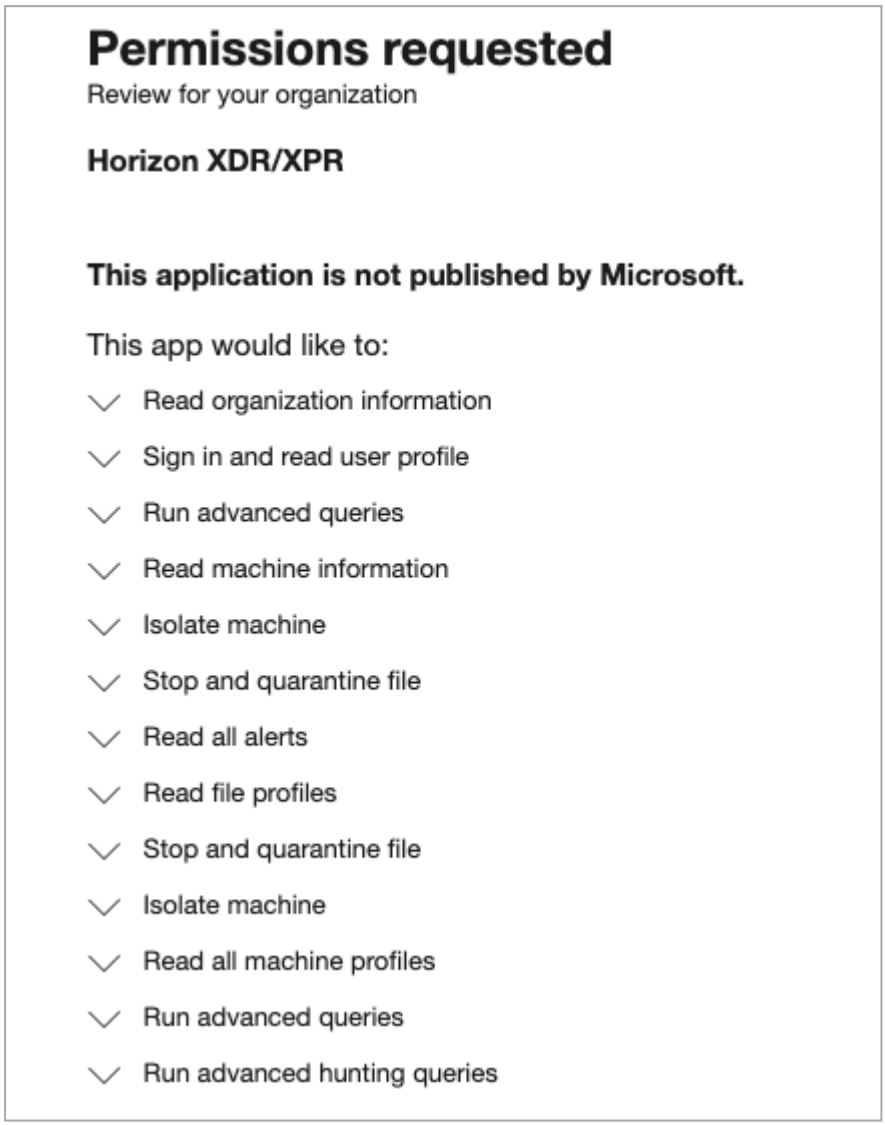
- Active subscription to Microsoft 365 Defender for Endpoint.
- Administrator privileges to add integration to Microsoft 365 Defender for Endpoint.

Integrating Microsoft 365 Defender for Endpoint

1. Log in to the XDR Administrator Portal.
2. Go to **Settings** > **Integrations**.
3. In the **Available integrations** section, in the **MS 365 Defender Endpoint** widget, click **Integrate**.



4. In the Microsoft authentication pop up, log in to the relevant user account with administrator credentials.
5. Accept the required permissions and click **OK**.

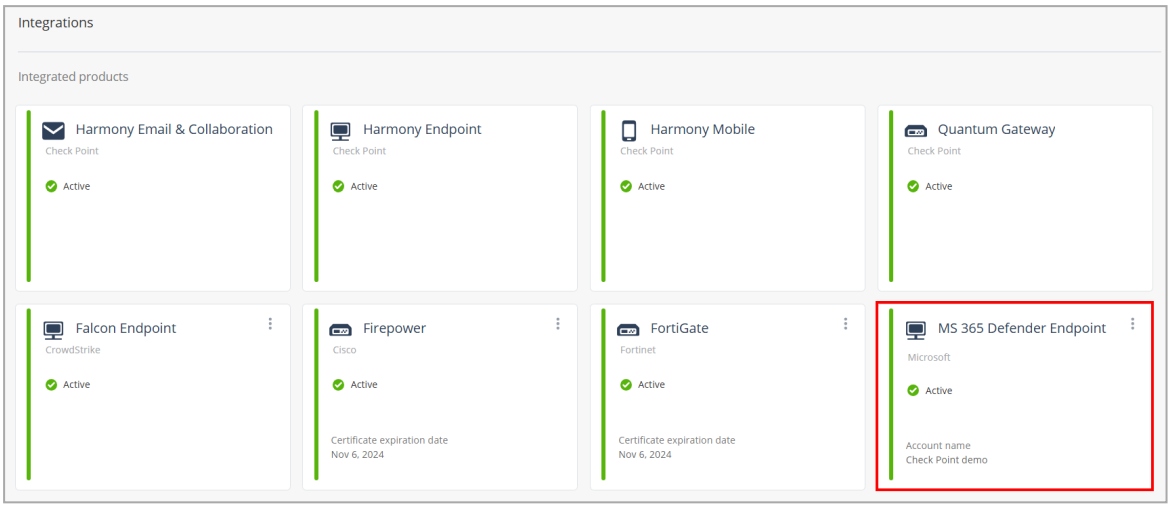


After successful authentication, XDR integrates successfully with Microsoft 365 Defender for Endpoint.

6. To check if the integration is successful, in the XDR Administrator Portal:

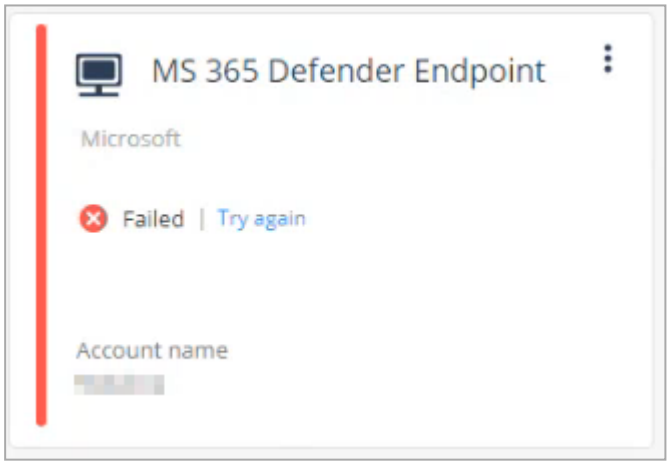
- Go to **Settings** > **Integrations**.

  In the **Integrated products** section, verify if **MS 365 Defender Endpoint** is listed as **Active**.

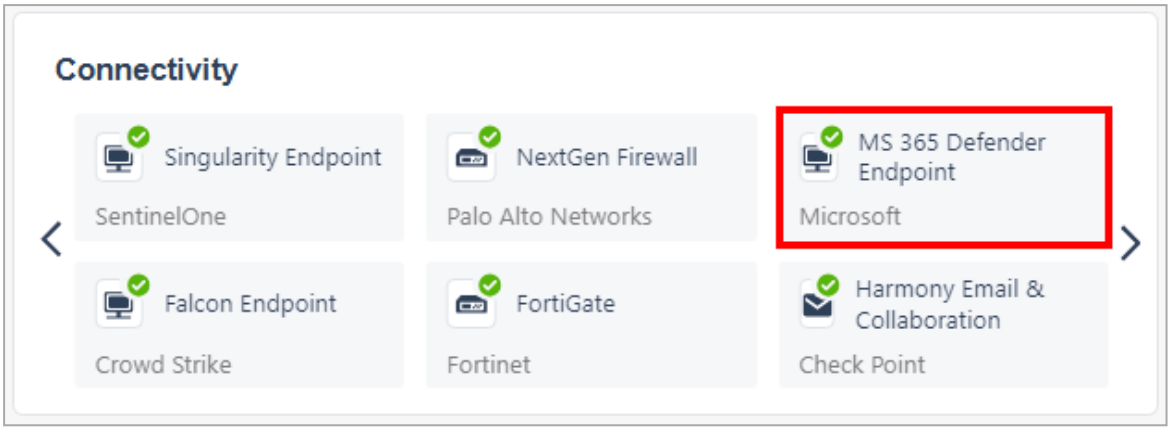


Notes -

- The widget will display **Inactive** status until XDR begins receiving logs from Microsoft 365 Defender for Endpoint.
- If the integration failed, the widget shows the status as **Failed**. For assistance, contact *Check Point Support*.



- Go to the **Overview** page and in the **Connectivity** widget, verify if **MS 365 Defender Endpoint** is listed as connected.



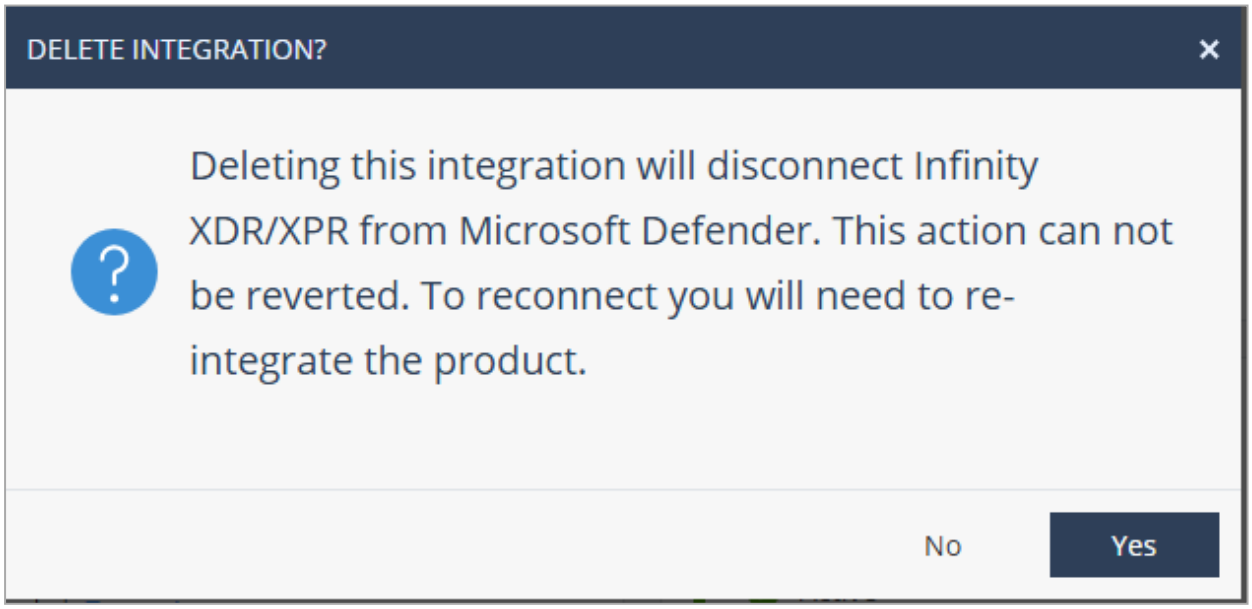
IOC Management

You can manage Indicators Of Compromise (IoCs) on Microsoft 365 Defender for Endpoint. You can import a list of IoCs to it in CSV format. For more information, see Microsoft Defender documentation.

Deleting the Integration

1. Go to **Settings** > **Integrations**.
2. In the **MS 365 Defender Endpoint** widget, click ⋮.
3. Click **Delete**.

   The **Delete Integration** window appears.



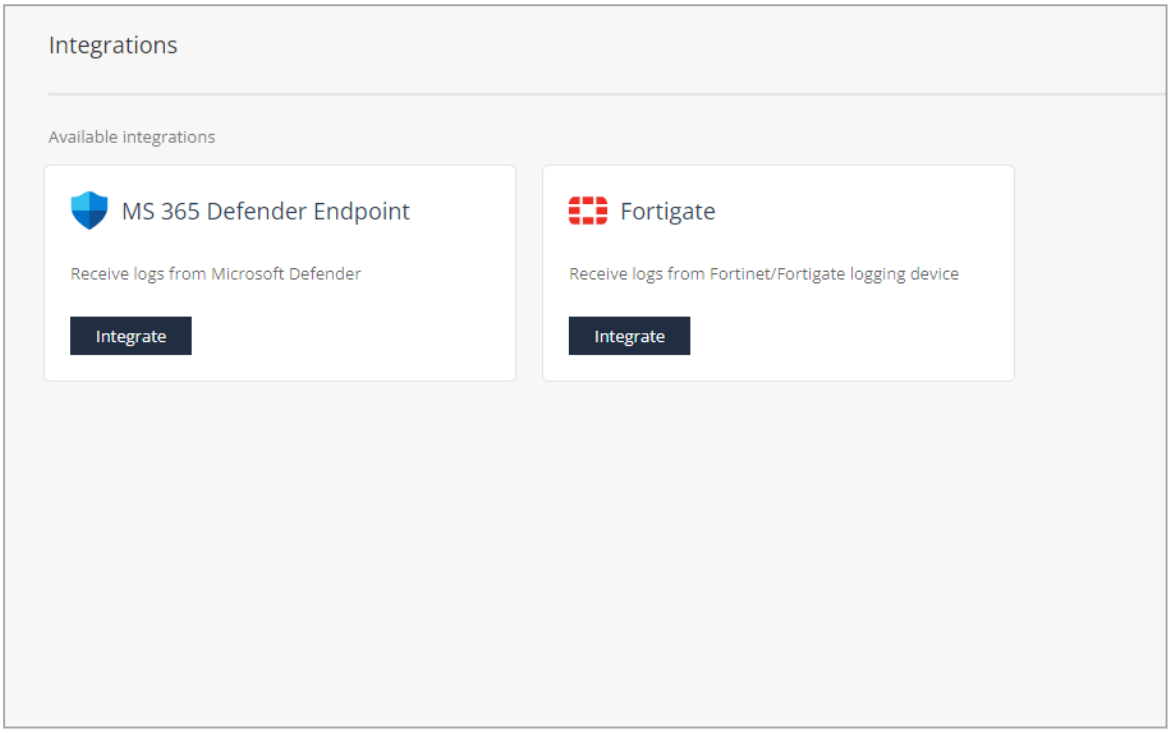
4. Click **Yes**.

Fortinet FortiGate Next Generation Firewall

Check Point XDR analyzes the syslogs from FortiGate Next Generation Firewall for malicious activity and enforces the preventive or corrective action through the firewall.

Integrating FortiGate Next Generation Firewall

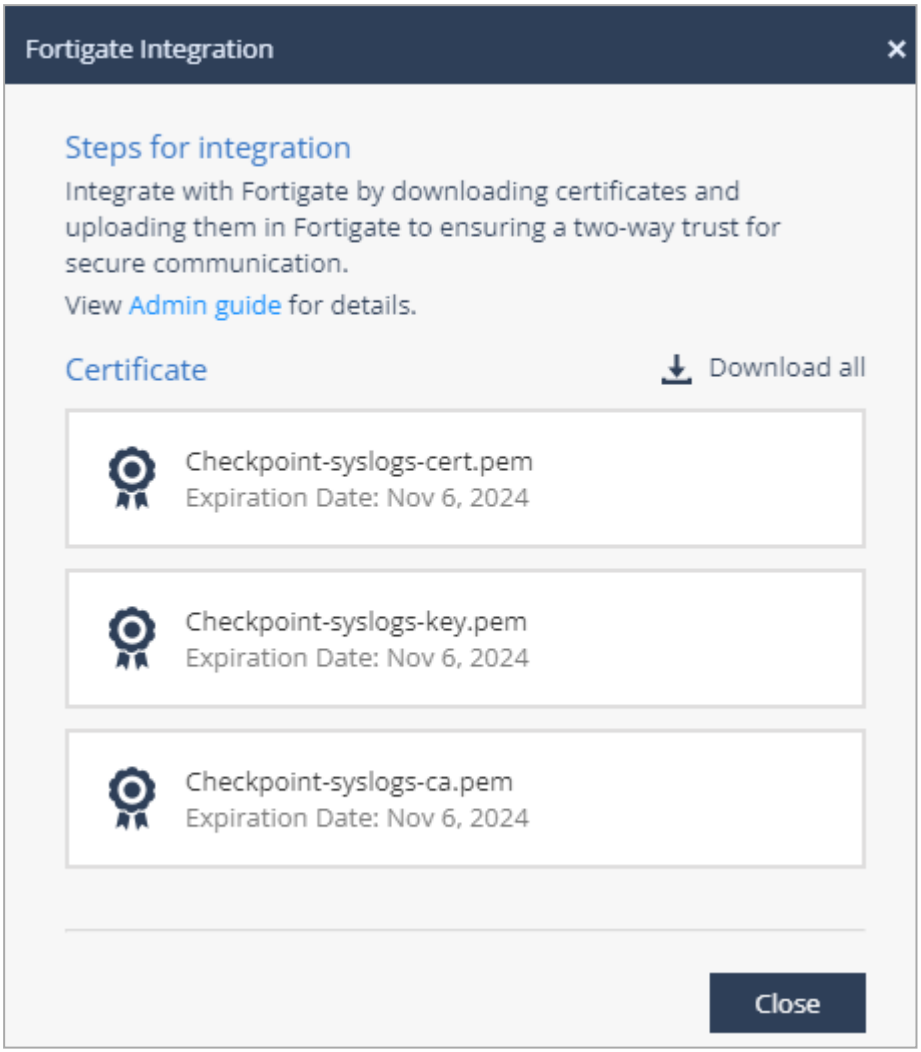
1. Log in to the XDR Administrator Portal:
    a. Go to **Settings** > **Integrations**.



    b. In the **Fortigate** widget, click **Integrate**.

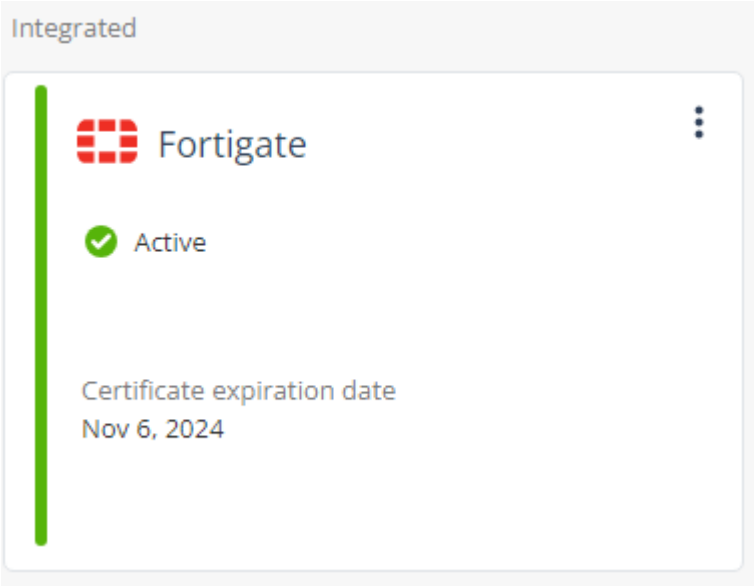
c. Click **Download all** to download the zip file that includes these certificates:

- *checkpoint-syslogs-cert.pem*
- *checkpoint-syslogs-key.pem*
- *checkpoint-syslogs-ca.pem*



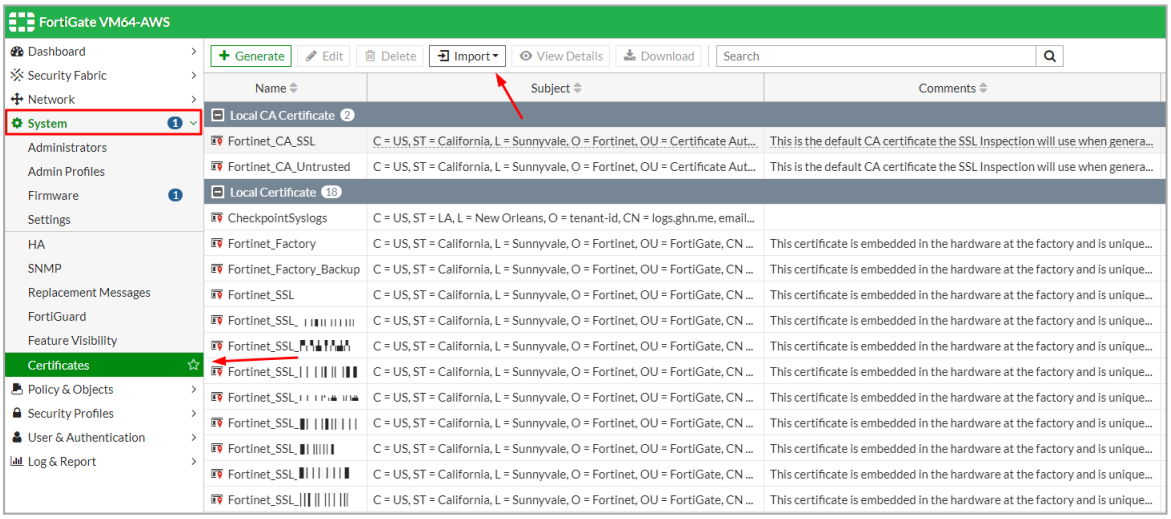
d. Click **Close**.

The **Fortigate** widget status changes to **Active**.

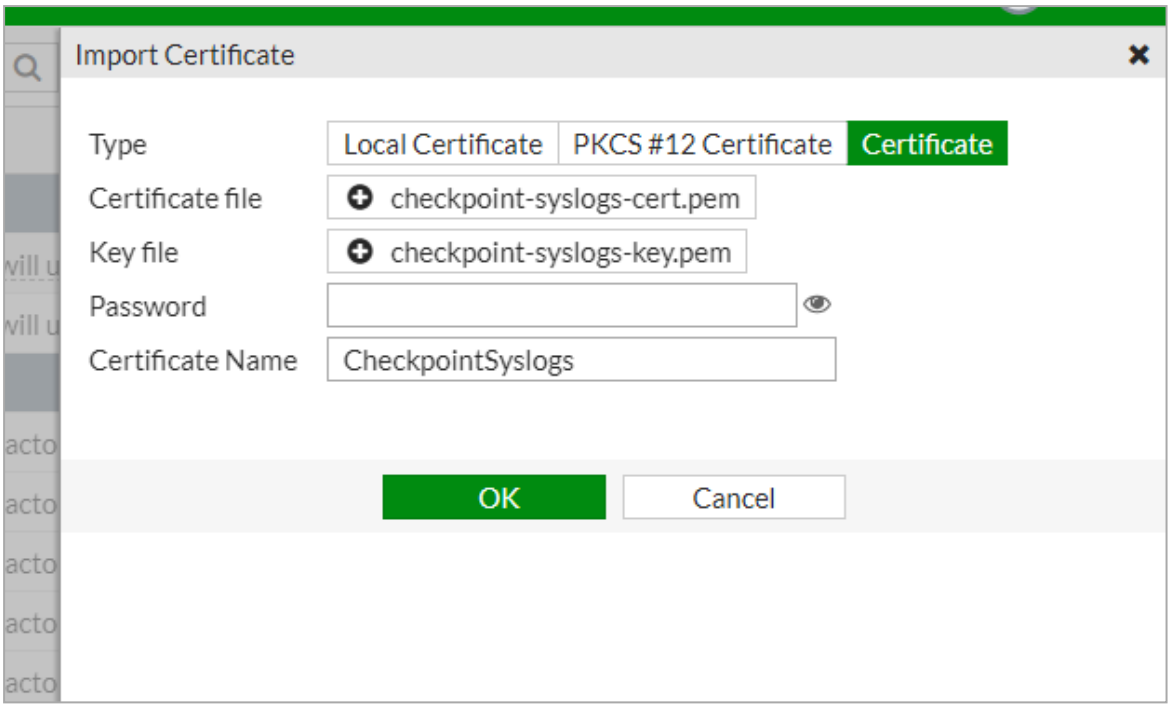


2. Log in to the FortiGate Next Generation Firewall Administrator Portal:

a. Go to **System** > **Certificates**.



b. From the **Import** list, select **Local Certificate**:



i. In the **Type** field, select **Certificate**.

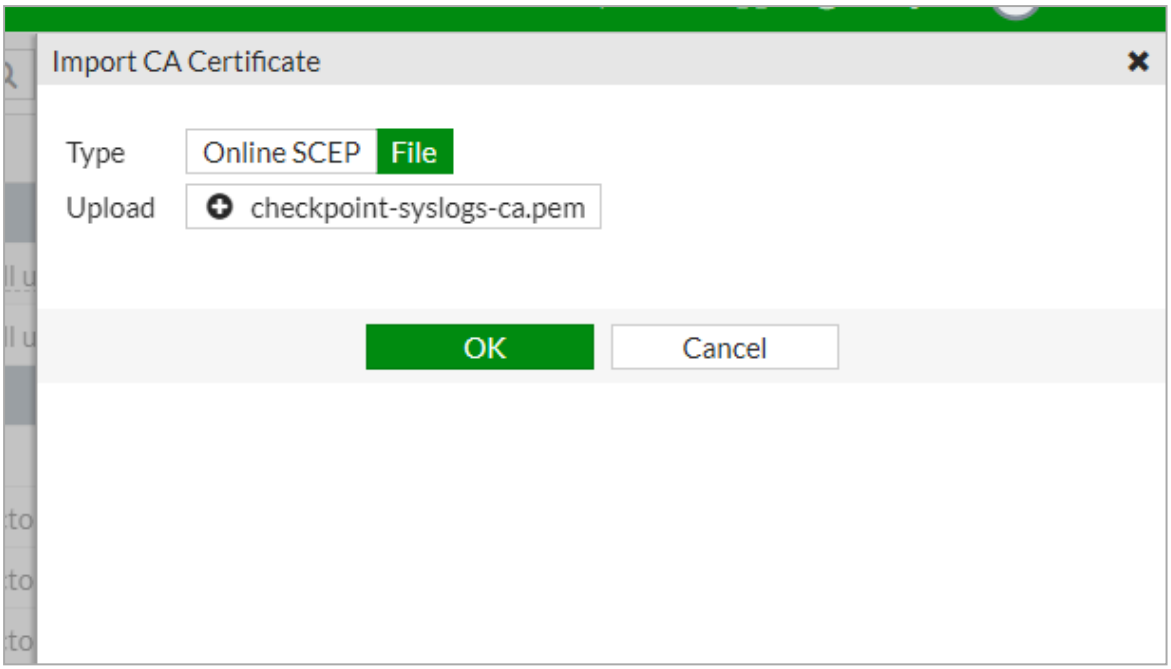
ii. In the **Certificate file** field, click ⊕ and upload the *checkpoint-syslogs-cert.pem* file.

iii. In the **Key file** field, click ⊕ and upload the *checkpoint-syslogs-key.pem* file.

iv. In the **Certificate Name** field, type `CheckpointSyslogs`.

v. Click **OK**.

c. From the **Import** list, select **CA Certificate**:



i. In the **Type** field, select **File**.

ii. In the **Upload** field, click ⊕ and upload the *checkpoint-syslogs-ca.pem* file.

iii. Click **OK**.

d. Click icon in the right top corner to open the CLI terminal and run:

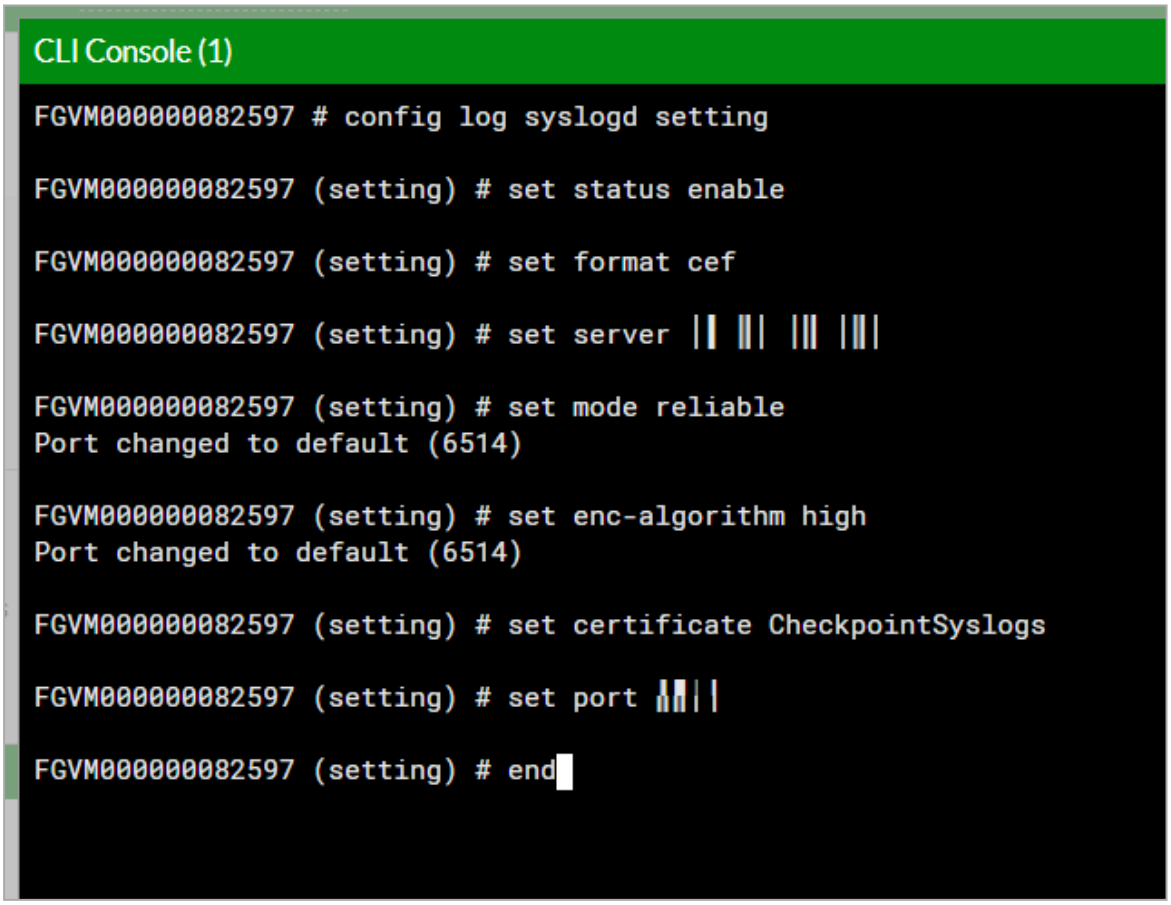
```
config log syslogd setting
```

Note - If you have used `syslogd` with another integration, use `syslogd2`, `syslogd3`, or `syslogd4`.

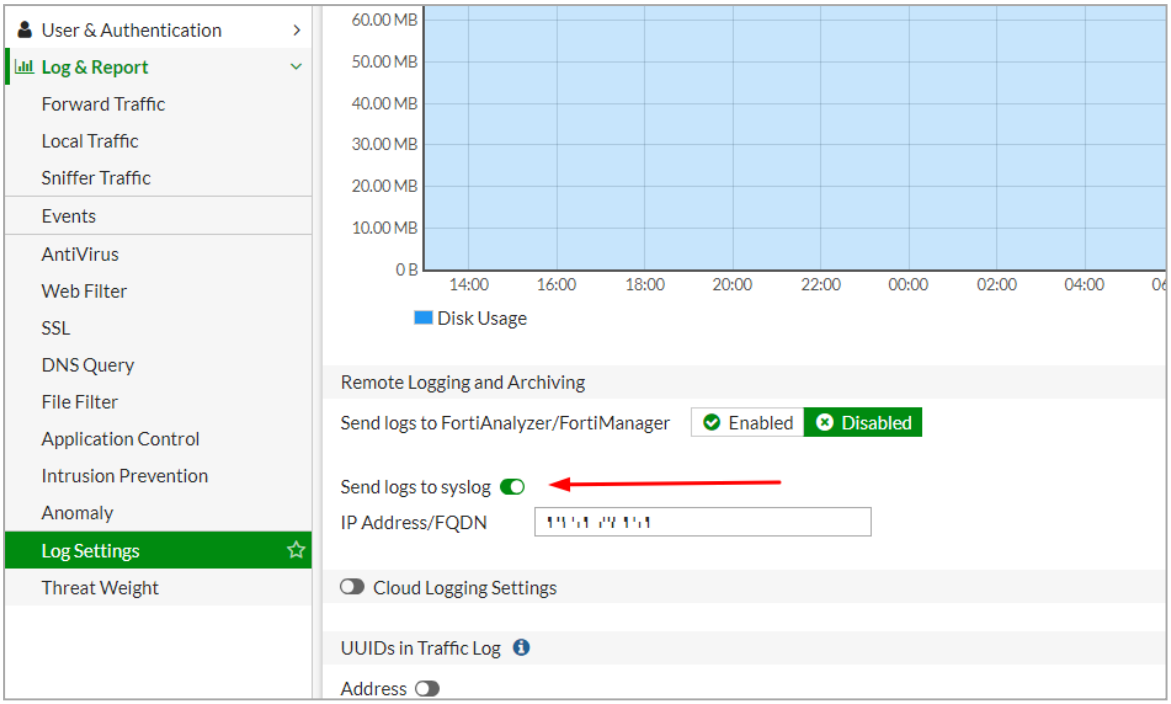
```
set status enable

set format cef

set server <Production server IP address of the region. For EU, it is 20.76.50.141. For US, it is 20.22.126.247. For UAE, it is 20.174.45.149>

set mode reliable

set enc-algorithm high

set certificate CheckpointSyslogs
```

Note - Make sure the certificate name matches the name entered in the **Certificate Name** field. See step 2.b.iv in Integrating the Fortinet FortiGate Next Generation Firewall.

```
set port 6514

end
```



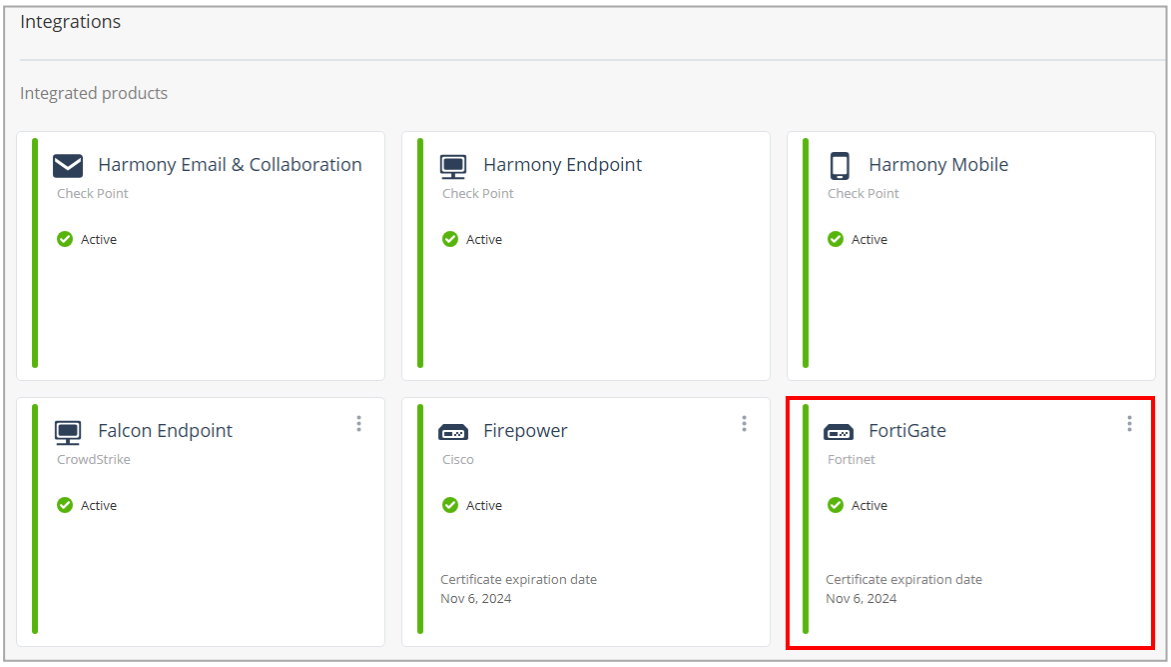
e. Go to **Log & Report** > **Log Settings** in the left pane and make sure the **Send logs to syslog** toggle button is turned on.



3. To check if the integration is successful, in the XDR Administrator Portal:

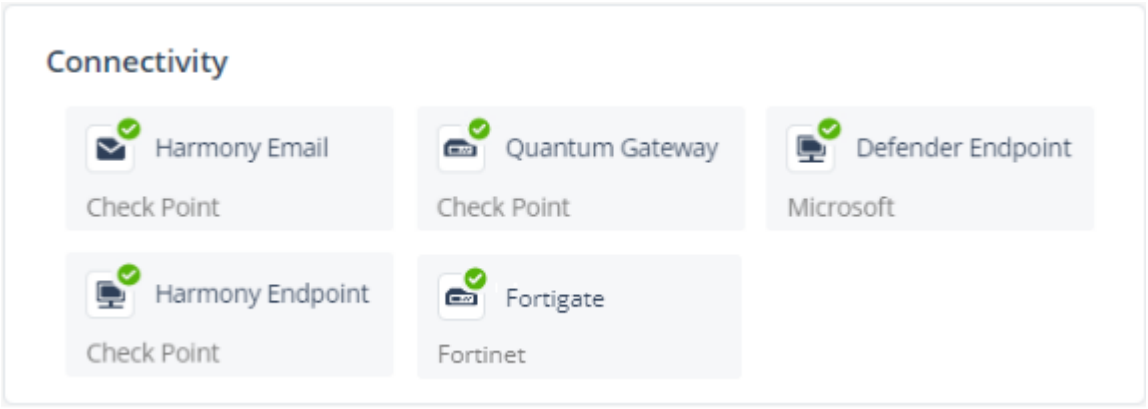
   - Go to **Settings** > **Integrations**.

     In the **Integrated products** section, verify if **FortiGate** is listed as **Active**.



Note - The widget will display **Inactive** status until XDR begins receiving logs from FortiGate Next Generation Firewall.

- Go to the **Overview** page and in the **Connectivity** widget, verify if **Fortigate** is listed as connected.



Disabling the Integration

You can disable the integration to stop XDR from reading the FortiGate Next Generation Firewall's syslogs.

1. Log in to the FortiGate Next Generation Firewall web portal and do one of these:
   - Click icon in the right top corner to open the CLI terminal and run:

     ```
     config log syslogd setting
     set status disable
     end
     ```

   - Go to **Log & Report** > **Log Settings** and turn off the **Send logs to syslog** toggle button.
2. To re-enable the integration:
   a. Log in to the FortiGate Next Generation Firewall web portal.
   b. Click icon in the right top corner to open the CLI terminal and run:

     ```
     config log syslogd setting
     set status enable
     set certificate CheckpointSyslogs
     end
     ```

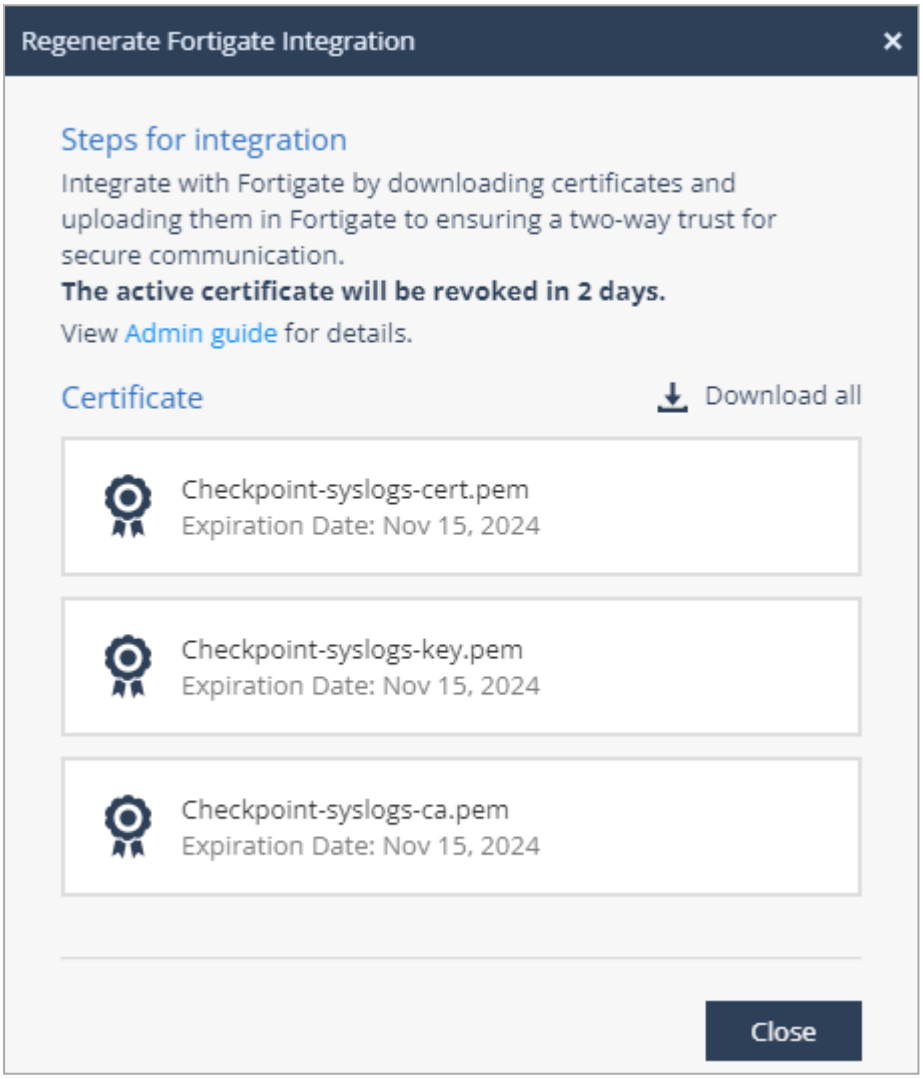
Note - Make sure you use the latest certificate name.

Regenerating the Certificate

If you revoke a certificate, you must regenerate and upload the certificate to the FortiGate Next Generation Firewall web portal within two days.

1. Log in to the XDR Administrator Portal:
   a. Go to **Settings** > **Integrations**.
   b. In the **Fortigate** widget, click ⋮.
   c. Click **Regenerate Certificate**.

      The **Regenerate Fortigate Integration** window appears.

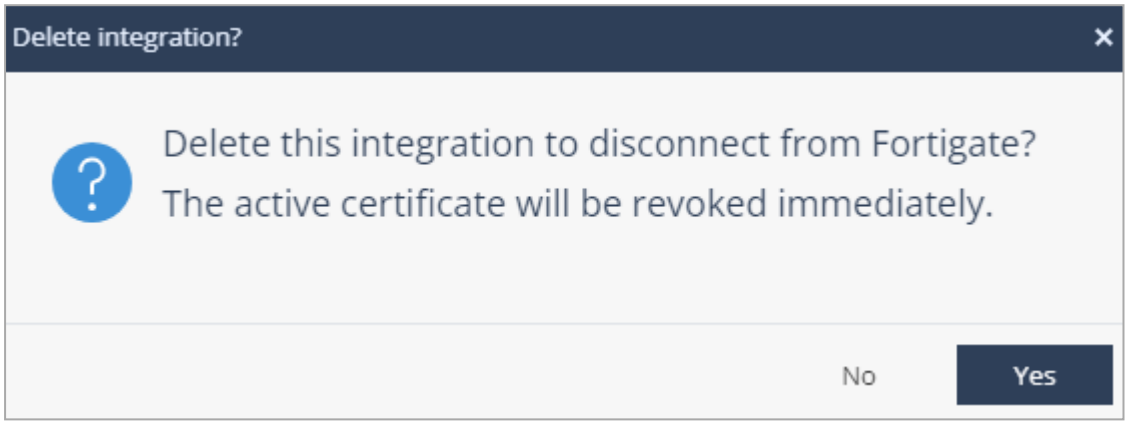


   d. Perform steps from 1.c until the end in *"Integrating FortiGate Next Generation Firewall" on page 249*.

Deleting the Integration

1. Go to **Settings** > **Integrations**.
2. In the **Fortigate** widget, click ⋮.
3. Click **Delete**.

   The **Delete Integration** window appears.



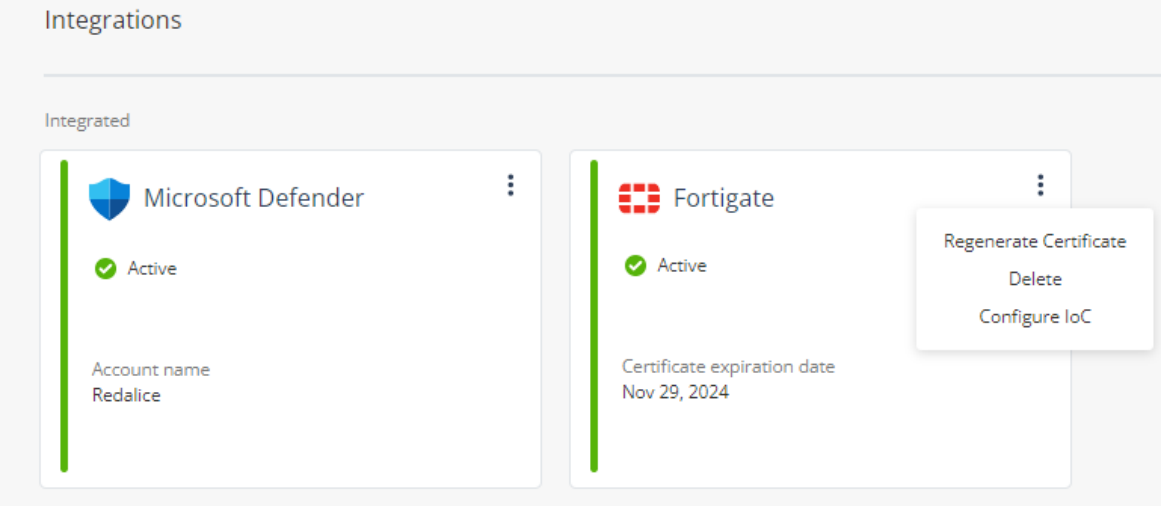
4. Click **Yes**.

Configuring IoCs

You can use the **Public Blend URL** in the IoC Management to enforce IoCs on the FortiGate Next Generation Firewall.

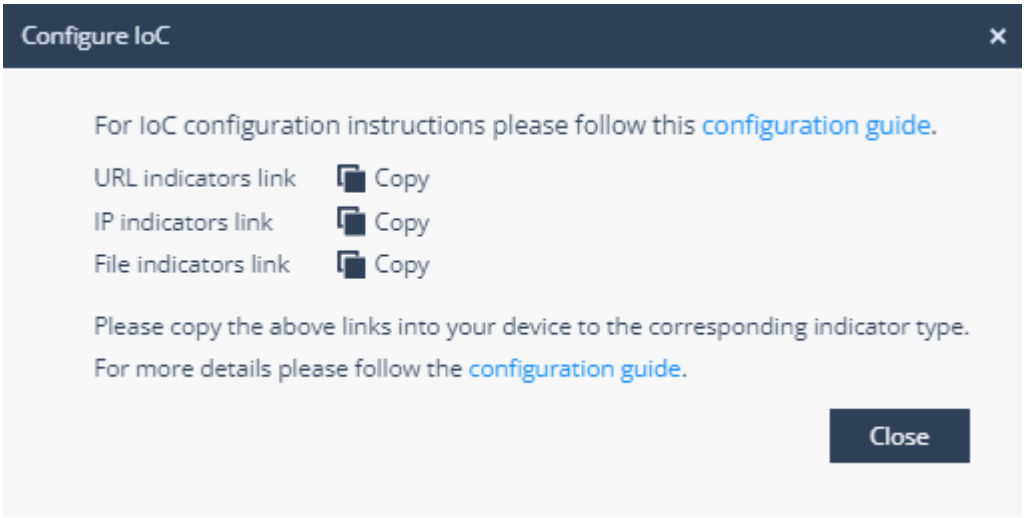
To configure IoCs:

1. Log in to the XDR Administrator Portal:
   a. Go to **Settings** > **Integrations**.
   b. In the **Fortigate** widget, click ⋮ and select **Configure IoC**.



   The **Configure IoC** window appears. It lists three indicator links generated automatically using the **All Indicators link** from the **Public Blend URL** in the IoC Management.

   c. Click ⧉ to copy the indicator link.

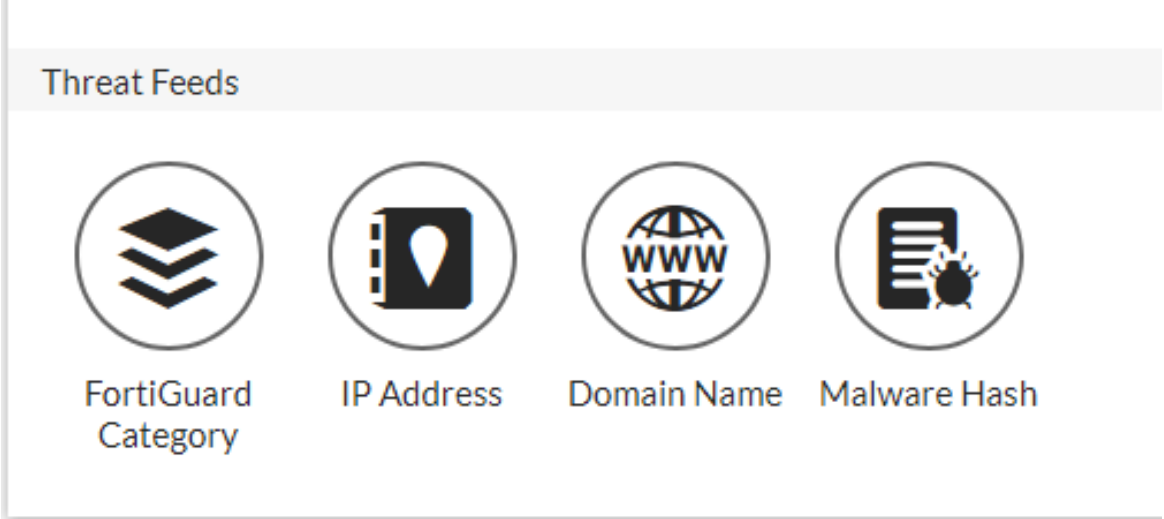


   d. Click **Close**.
2. Log in to the FortiGate Next Generation Firewall Admin Portal:

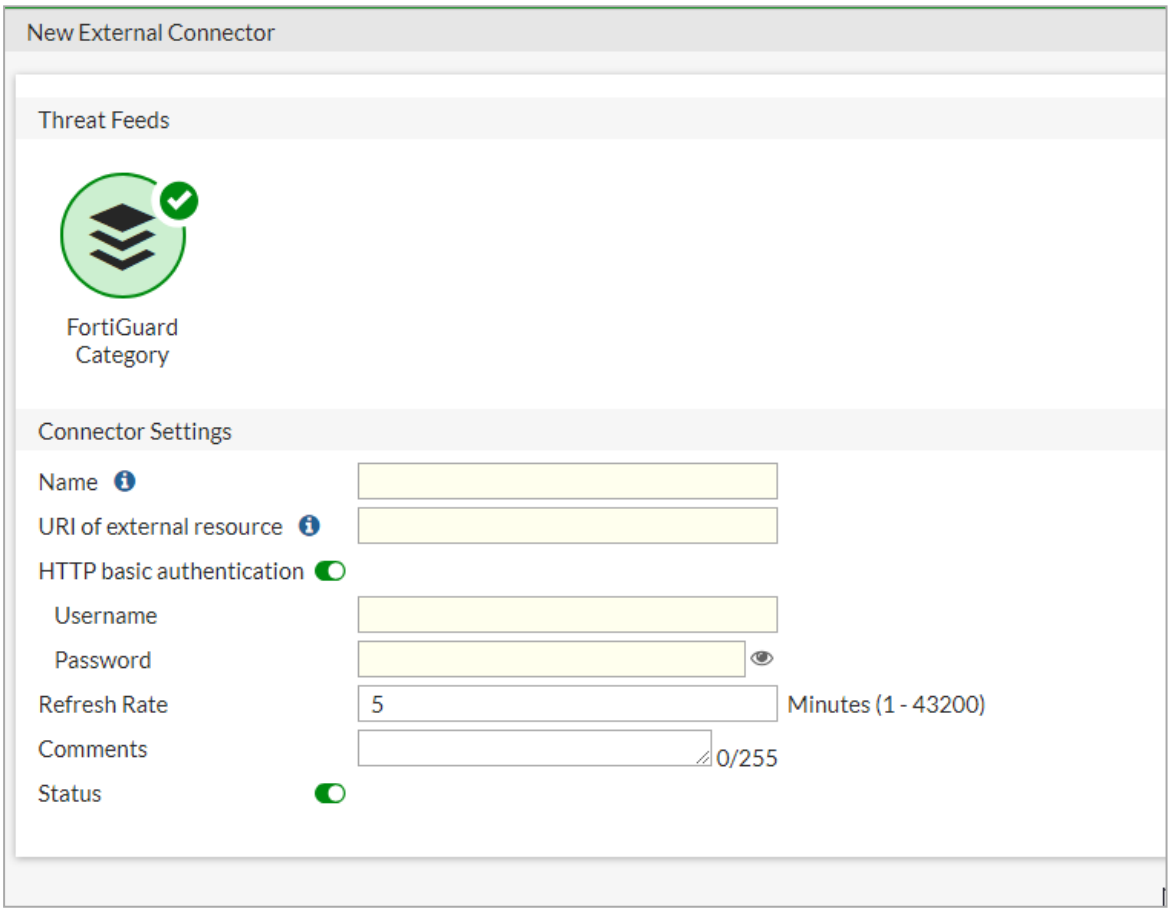
a. Go to **Security Fabric** > **External Connectors**.

b. Click **Create New**.

c. Scroll down and in the **Threat Feeds** section, select **FortiGuard Category**.



The **Connector Settings** window appears.



d. Do these:

   i. **Name** - Name of the threat feed.

   ii. **URI of external resources** - **URL indicators link** copied in the step **1.i**.

   iii. Turn off the **HTTP basic authentication** toggle button.

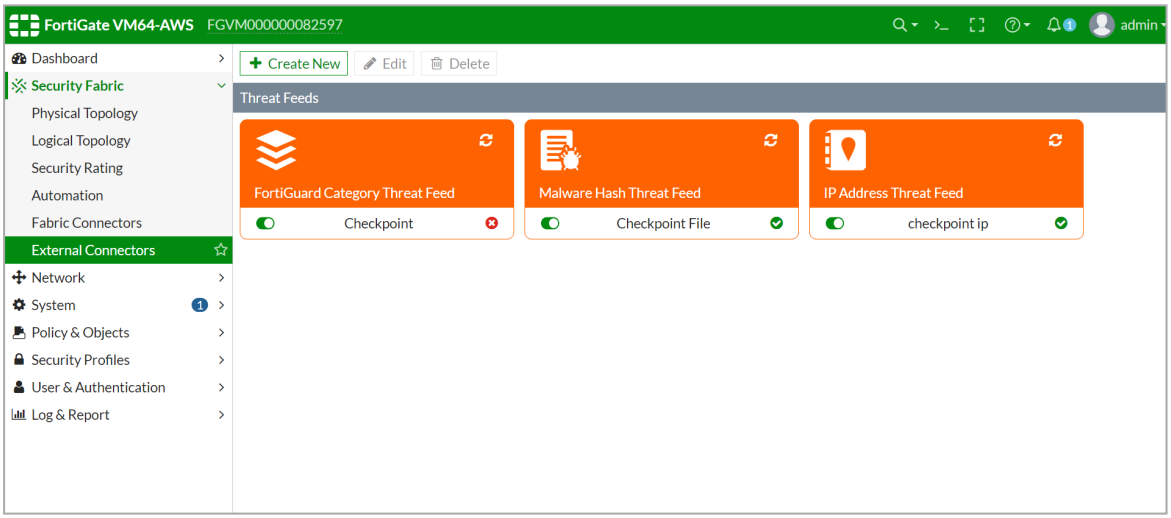
   iv. Turn on the **Status** toggle button.

   v. Click **OK**.

e. Repeat steps **2.b** through **2.d** with these details:

FortiGate Threat Feed	Configure IoC link (from step 1.i)
IP Address	IP indicators link
Malware Hash	File indicators link

The Threat Feeds widget appears in the **External Connectors** page.

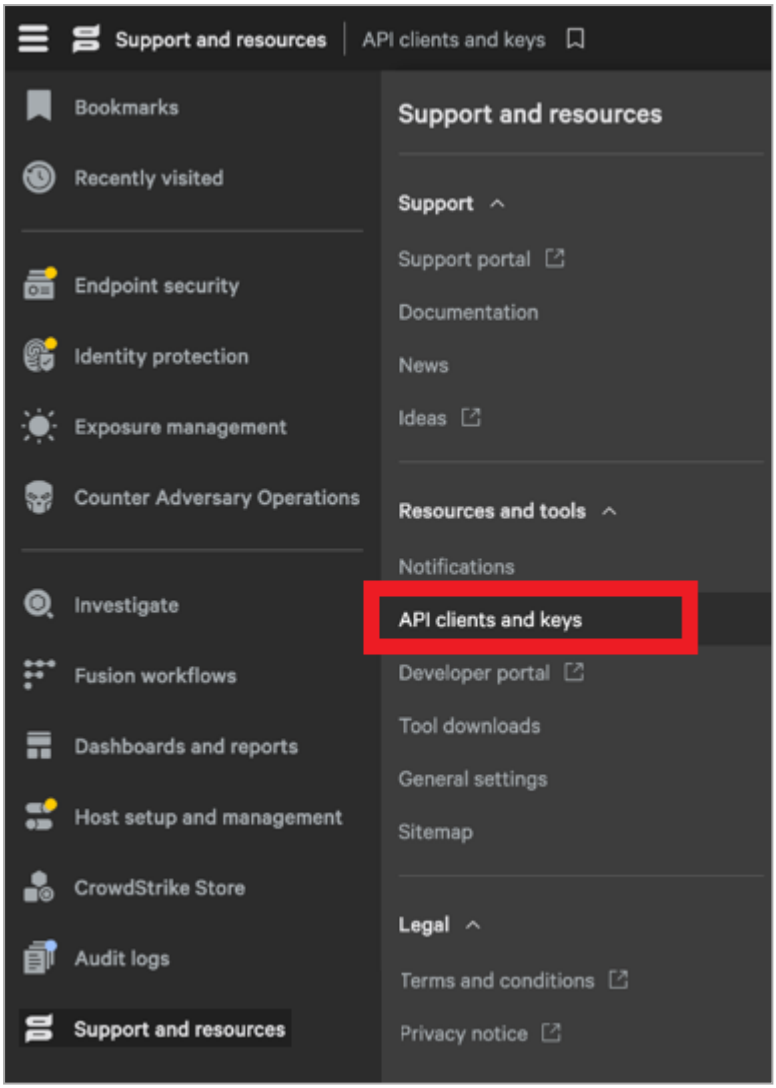


CrowdStrike Falcon

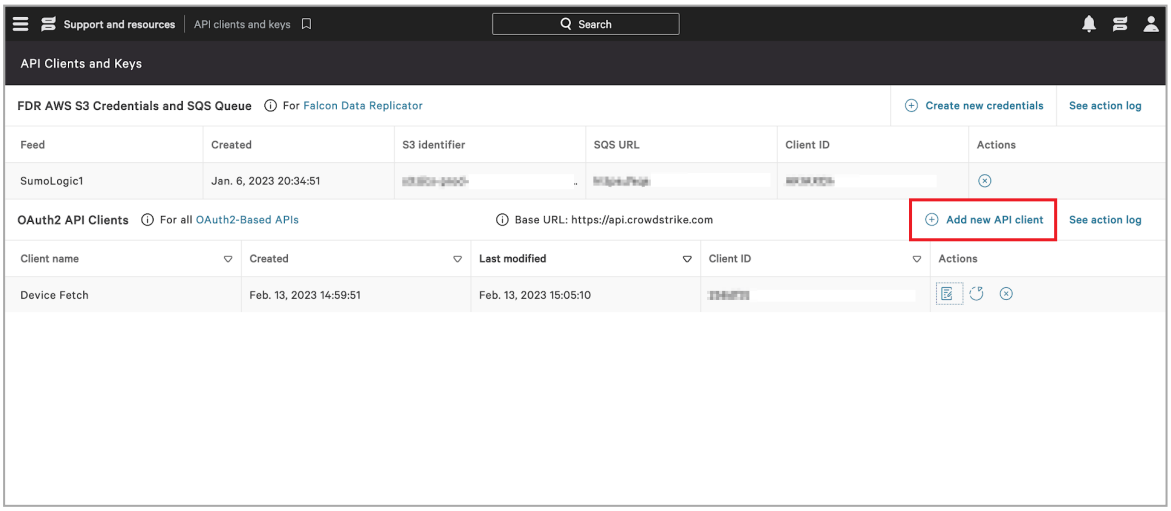
Check Point XDR analyzes the logs from CrowdStrike Falcon management portal for malicious activity, and suggests preventive actions, which you must manually enforce on the endpoint.

Integrating CrowdStrike Falcon

1. Log in to the CrowdStrike Falcon web portal:
   a. Go to **Support and resources** > **API clients and keys**.

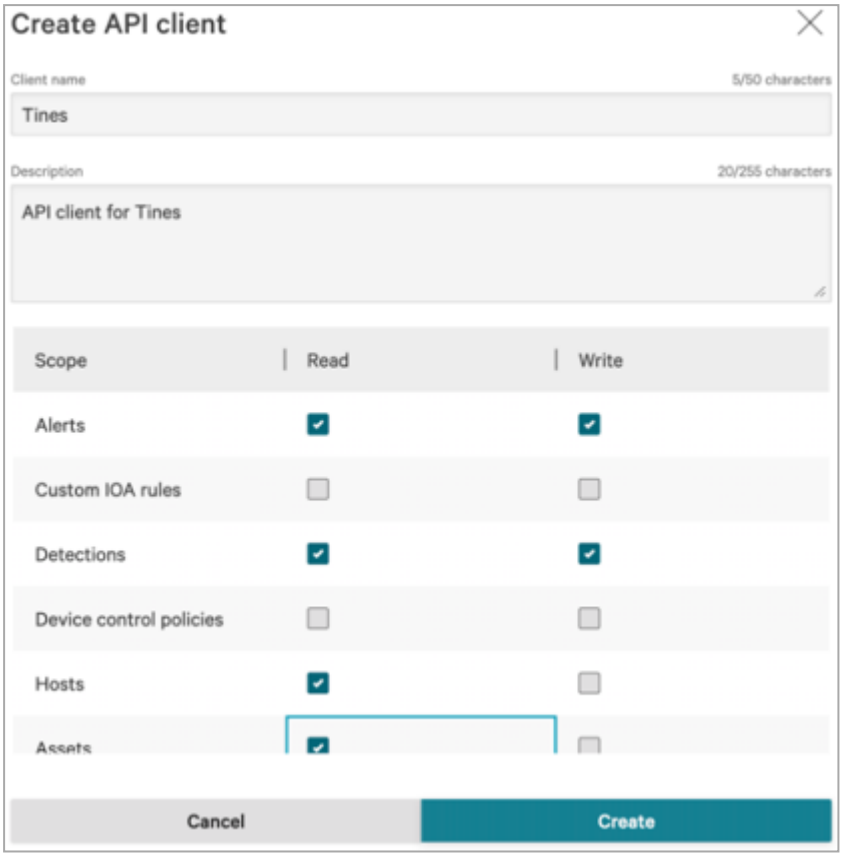


The **API Clients and Keys** window appears.



b. Click **Add new API client**.

The **Create API client** window appears.



c. Enter these:

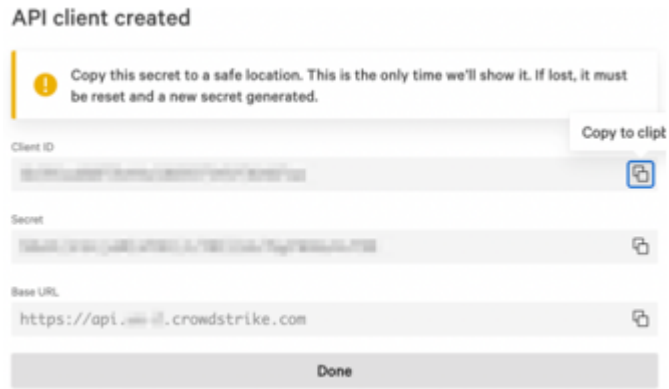
   i. **Client name**

   ii. **Description**

d. Select the relevant scopes checkbox(s).

e. Click **Create**.

The **API client created** window appears.



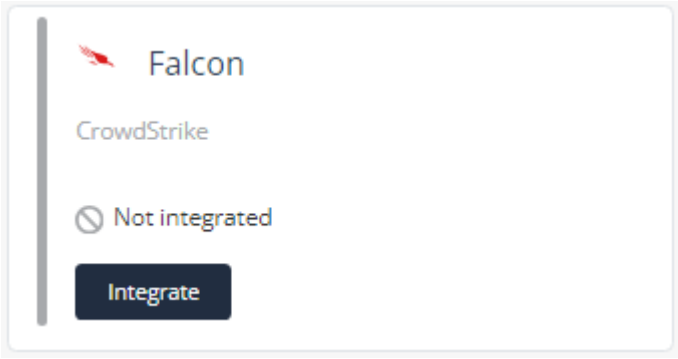
f. Click  to copy **Client ID**, **Secret Key** and **Base URL**.

g. Click **Done**.

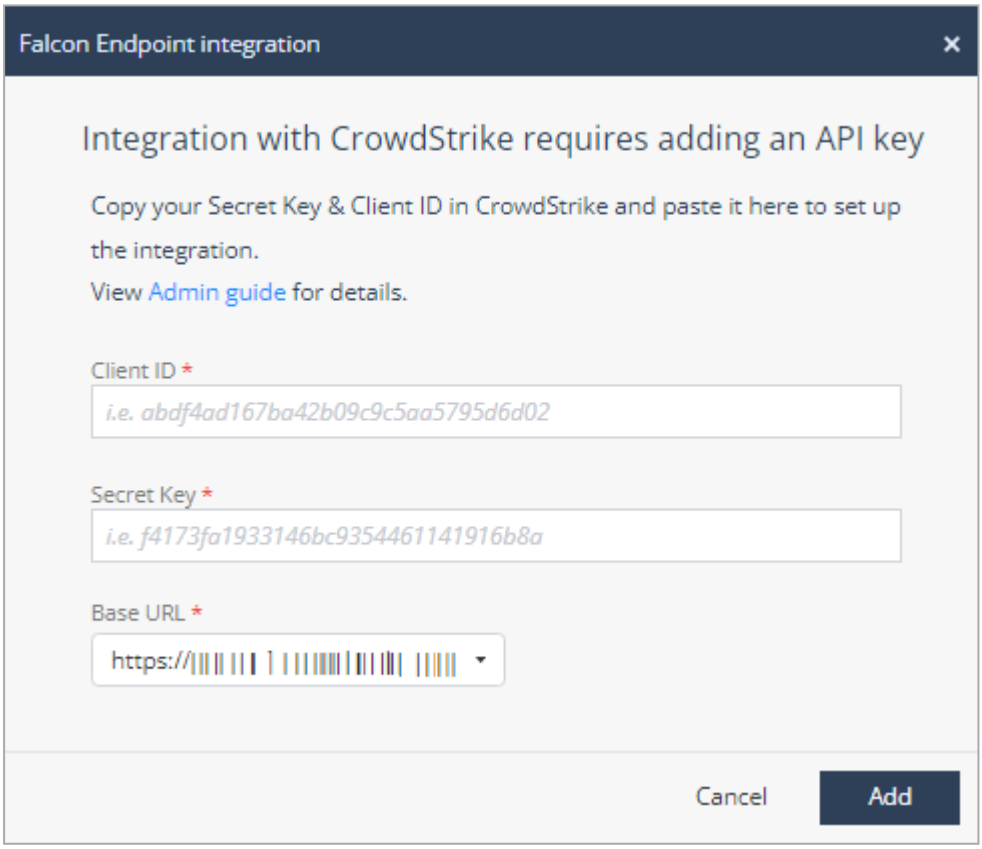
2. Log in to the XDR Administrator Portal:

   a. Go to **Settings** > **Integrations**.

   b. In the **Falcon** widget, click **Integrate**.



The **Falcon Endpoint integration** window appears.



c. Enter these:

   i. **Client ID**

   ii. **Secret Key**

   iii. **Base URL**

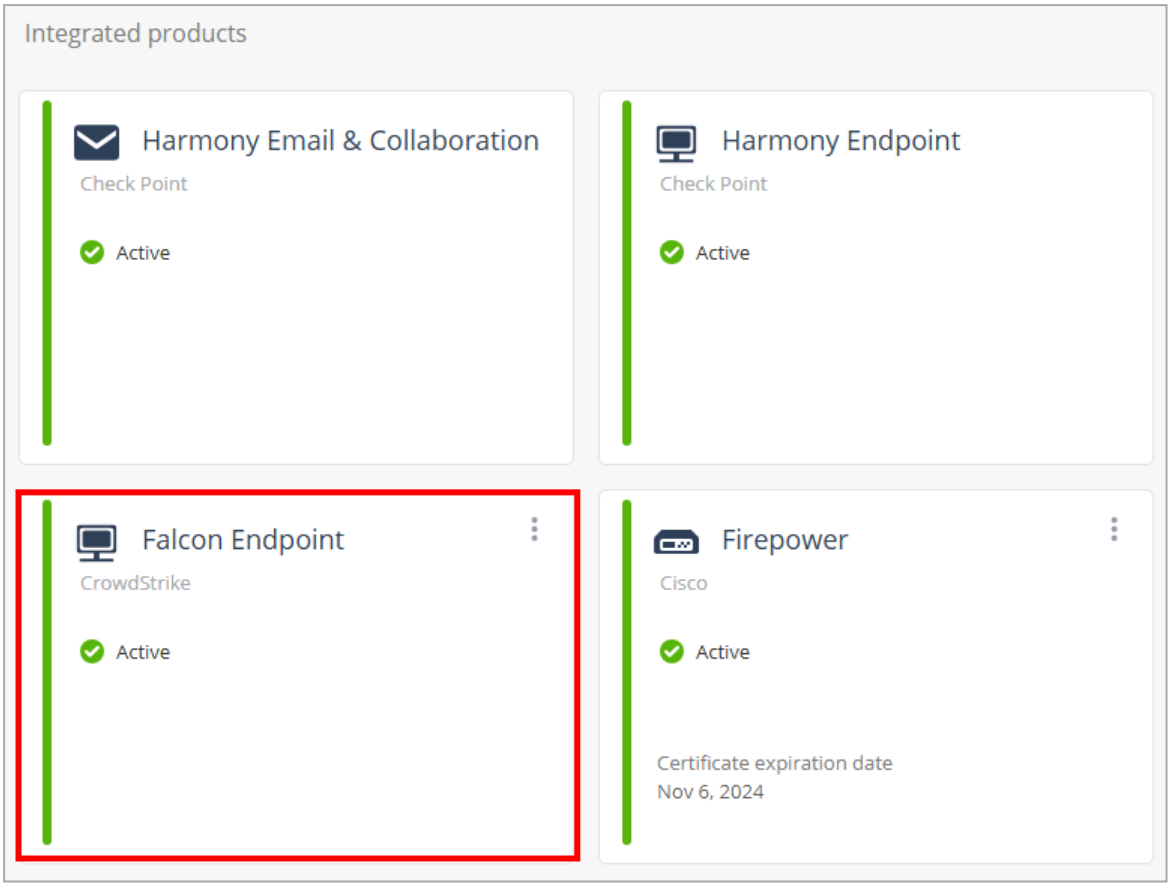
d. Click **Add**.

   The **Falcon** widget status changes to **Active**.

3. To check if the integration is successful, in the XDR Administrator Portal:

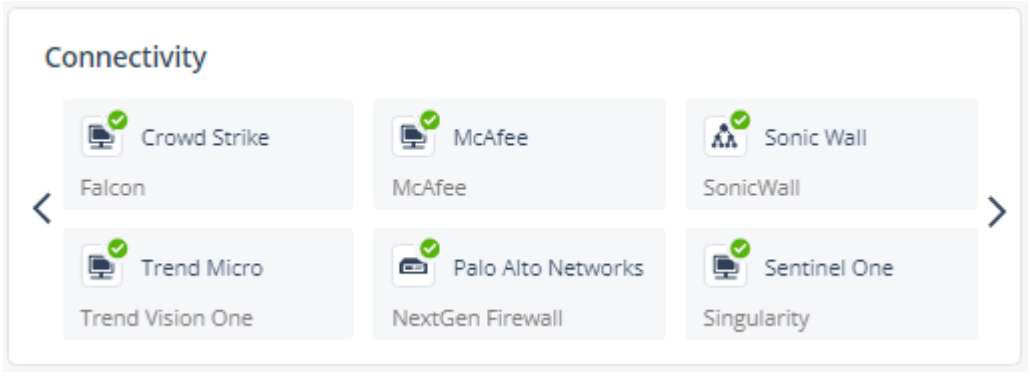
- Go to **Settings** > **Integrations**.

  In the **Integrated products** section, verify if **Falcon** is listed as **Active**.



Note - The widget will display **Inactive** status until XDR begins receiving logs from CrowdStrike Falcon.

- Go to the **Overview** page and in the **Connectivity** widget, verify if **Crowd Strike** is listed as connected.



Note - If the connectivity status is disconnected for more than 30 minutes, verify the **Client ID**, **Secret Key** and **Base URL**.

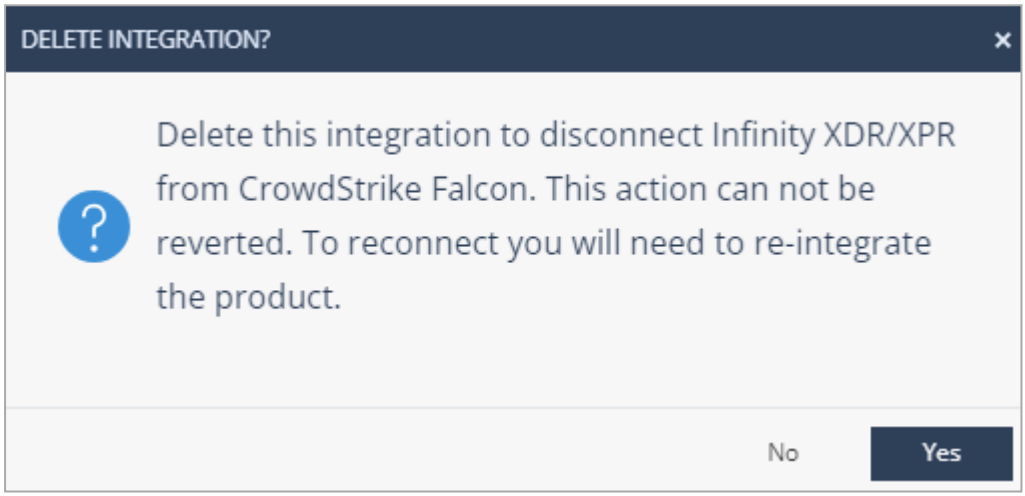
IOC Management

You can manage Indicators Of Compromise (IoCs) on CrowdStrike Falcon and you can import IoCs to it. For more information, see CrowdStrike documentation.

Deleting the Integration

1. Go to **Settings** > **Integrations**.
2. In the **Falcon** widget, click ⋮.
3. Click **Delete**.

   The **Delete Integration** window appears.



4. Click **Yes**.

Supported Preventive Actions

When XDR detects any malicious activity, it generates an incident and recommends preventive actions to mitigate it. The supported preventive action is to isolate a machine. For more information, see **Incidents Overview** > *"Prevention" on page 70*.

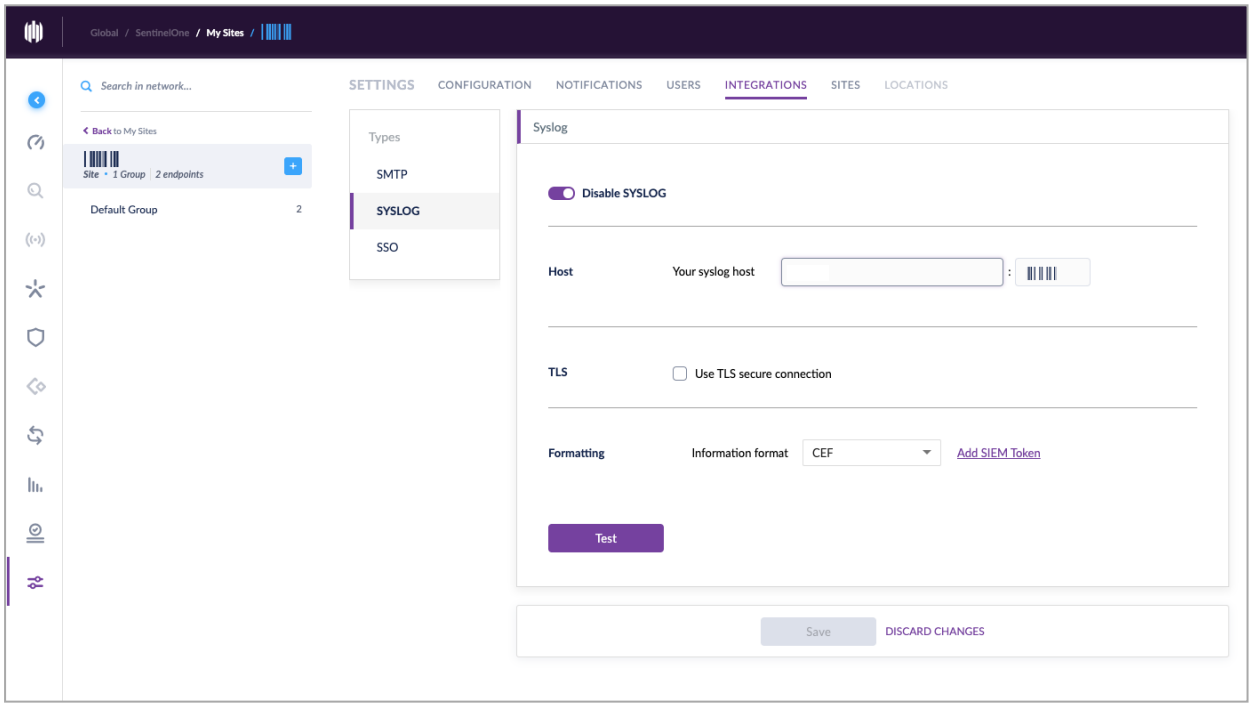
Singularity Endpoint

Check Point XDR analyzes the logs from Singularity Endpoint management portal for malicious activity, and recommends preventive actions to isolate affected endpoints.

Integrating Singularity Endpoint

To configure Singularity Endpoint to send logs to XDR:

1. Log in to the SentinelOne web portal.
2. Select your site.
3. In the left navigation pane, click .
4. Click the **Integrations** tab.



5. From the **Types** list, select **SYSLOG**.
6. Turn off the **Disable SYSLOG** toggle button to enable syslog.
7. In the **Host** field, enter your syslog server IP address and port:
   a. For EU region, enter **20.76.50.141** and port **6514**
   b. For US region, enter **20.22.126.247** and port **6514**
8. In the **TLS** field, select the **Use TLS secure connection** checkbox.
9. In the **Formatting** field, from the **Information format**list, select **CEF**.

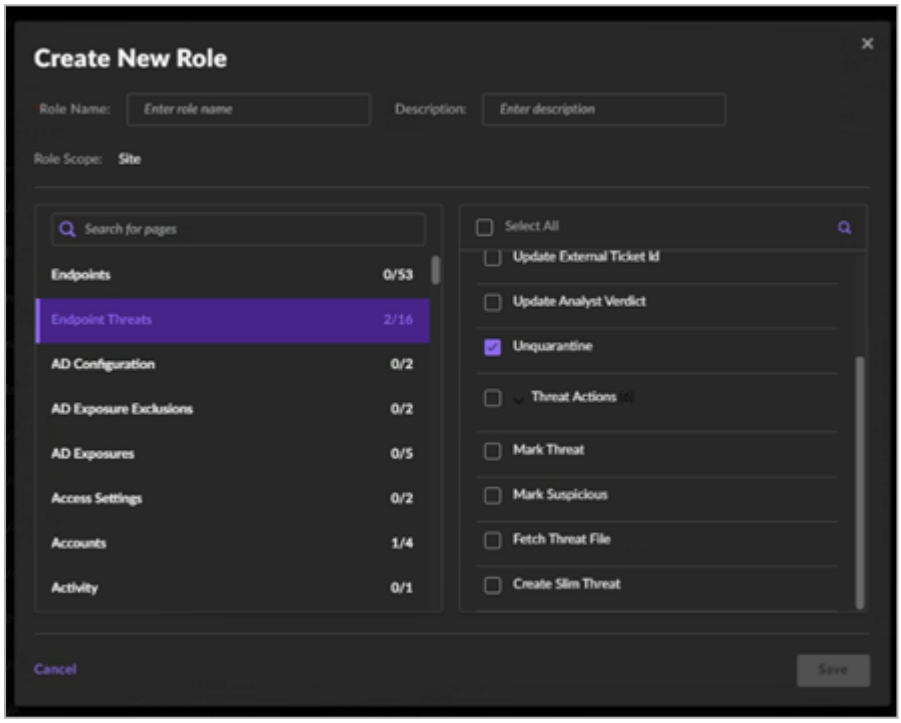
10. Click **Test**.
11. Click **Save**.

To receive response on Singularity Endpoint from XDR:

Note - This section is optional. Do these steps if you want to issue responses from XDR on Singularity Endpoint.

1. Log in to the SentinelOne web portal.
2. Go to **Settings** > **Users** and then click **Roles**.
3. Create a new role or use an existing one, such as *IR Team*.

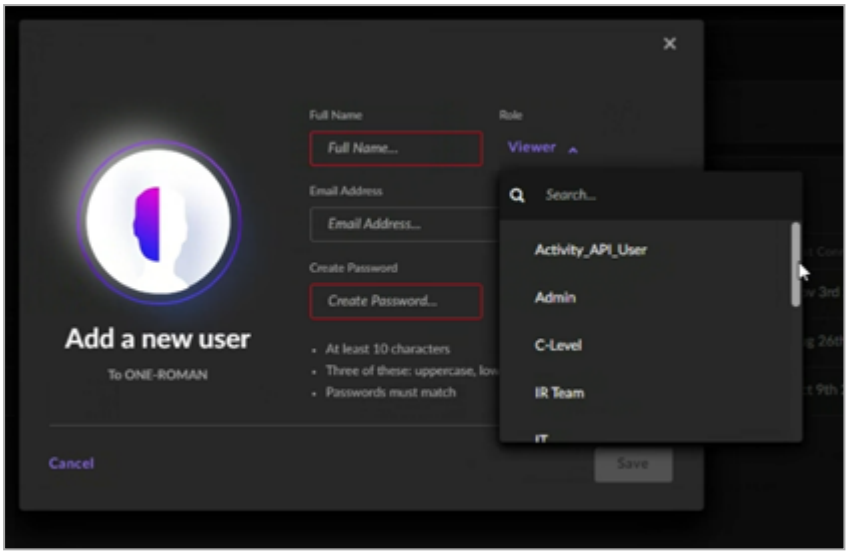
   If you are creating a new role, ensure that it includes permissions for **Endpoint Threats** and **Unquarantine**.



4. Create a Service User:

i. Go to **Service Users** and click **Create New User**.

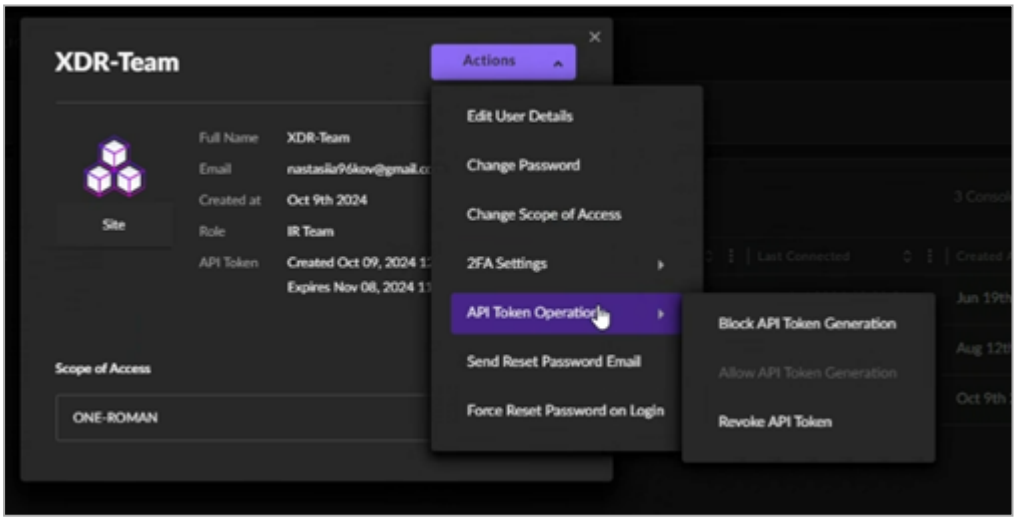
ii. Enter the user details and in the **Role** section, assign the new user to the *IR Team* role or the custom role created in the previous step.



5. Enable API Token Generation:

a. Open the user details.

b. From the **Actions** list, select **API Token Operations** > **Allow API Token Generation**.

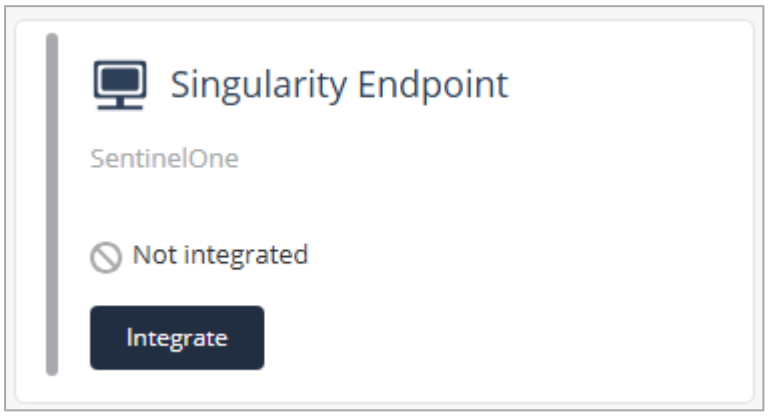


6. Generate the API token and copy it.

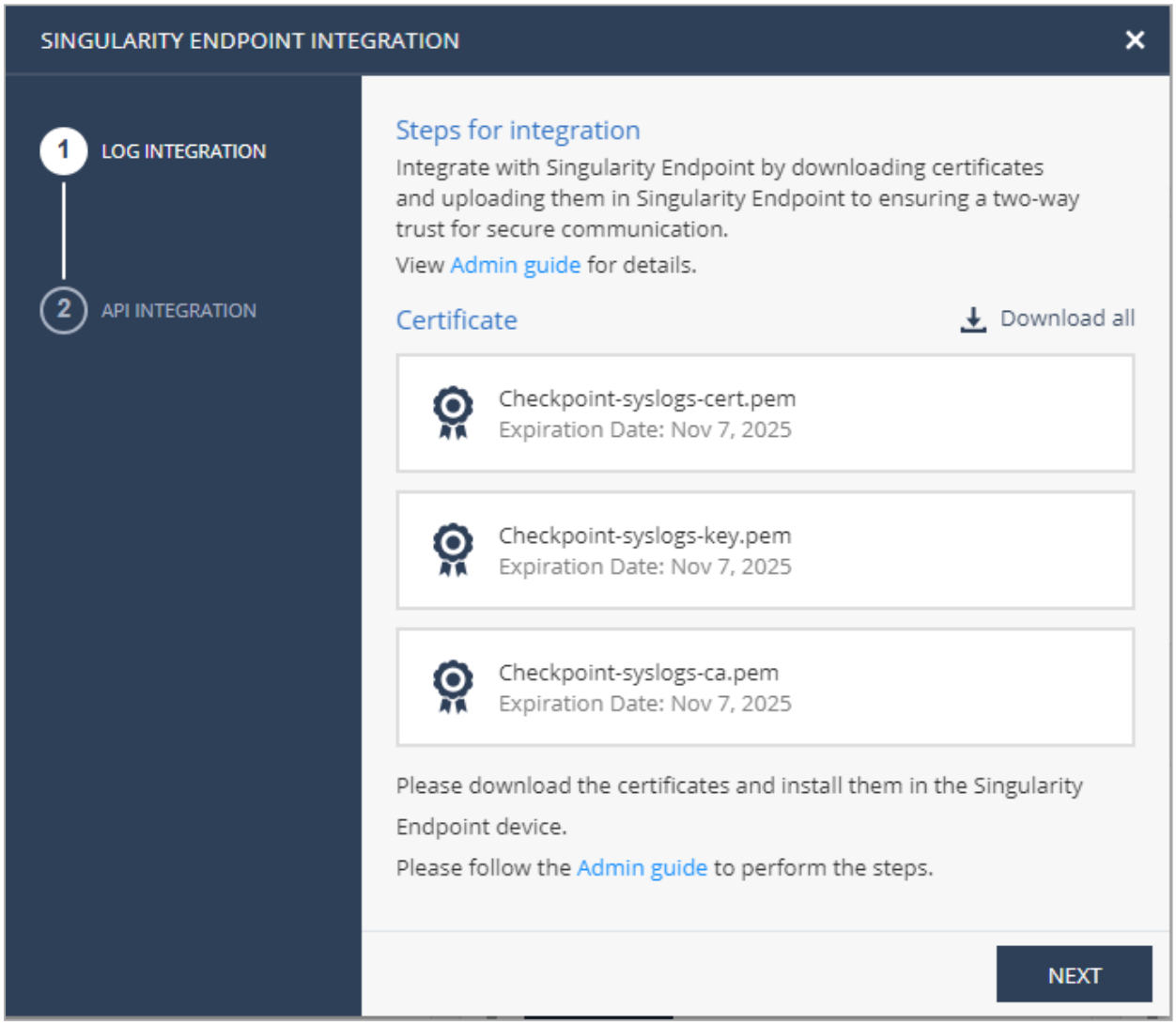
Important - The token is valid for 30 days. You must regenerate it after this period.

To integrate Singularity Endpoint in XDR Administrator Portal:

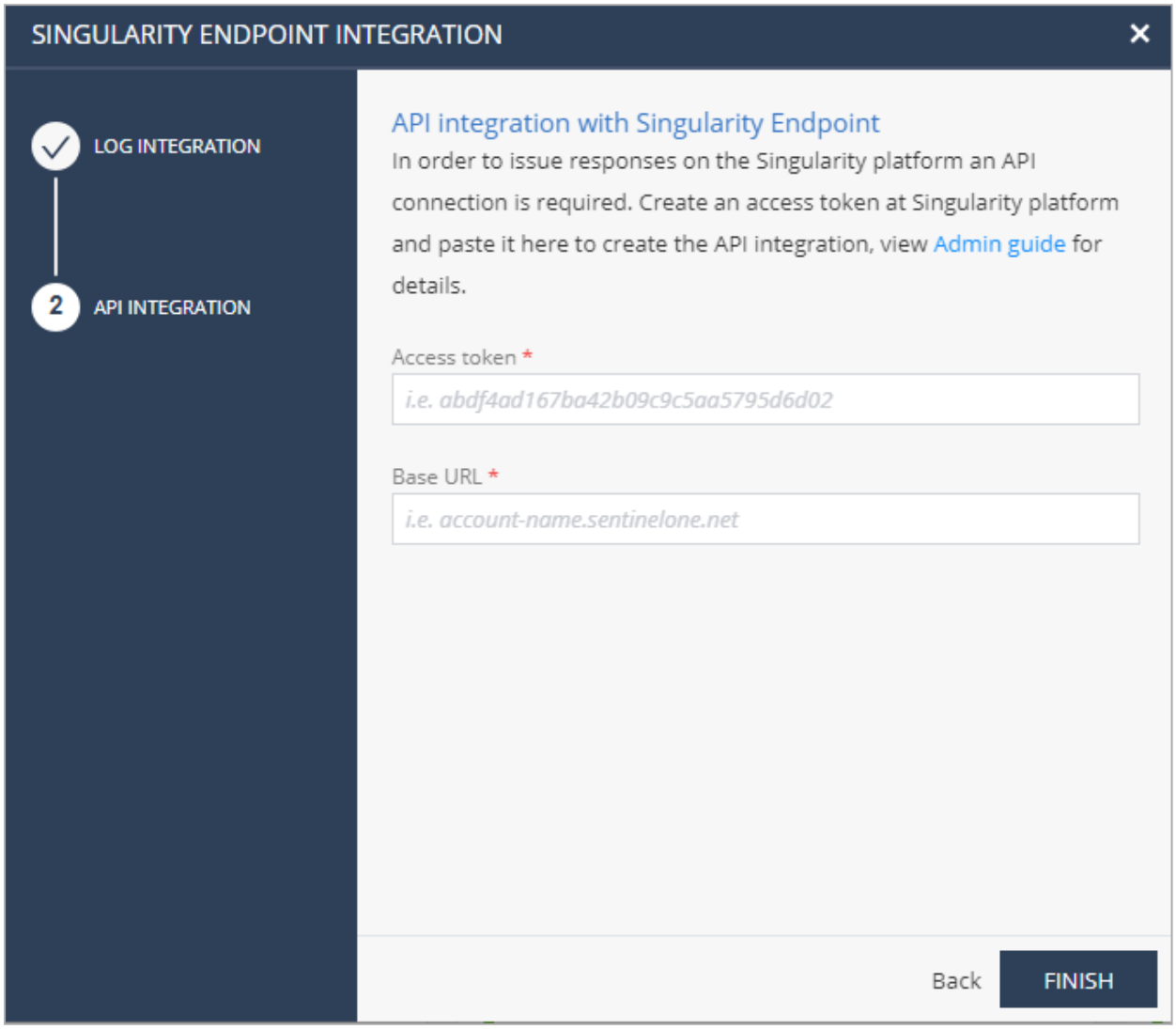
1. Log in to the XDR Administrator Portal and go to **Settings** > **Integrations**.
2. In the **Singularity Endpoint** widget, click **Integrate**.



The **Singularity Endpoint Integration** window appears.



3. In the **Log Integration** section, click **Download all** to download the zip file that includes these certificates:
   - *checkpoint-syslogs-cert.pem*
   - *checkpoint-syslogs-key.pem*
   - *checkpoint-syslogs-ca.pem*
4. Click **Next**.
5. (Optional) To issue responses on Singularity Endpoint, in the **API Integration** section:



   a. In the **Access token** field, enter the API token copied from the SentinelOne web portal.

b. In the **Base URL** field, enter the SentinelOne URL for your account, in this format:

account-name.sentinelone.net

where **account-name** is the name of your account in SentinelOne web portal.

6. Click **Finish**.

The widget shows **Inactive** status until XDR begins receiving logs from Singularity Endpoint.

After that, the status changes to **Active** or **Partially active**, depending on whether you have configured API integration.

7. To check if the integration is successful:

- In the **Integrated products** section:
  - If you have configured API integration, verify if **Singularity Endpoint** is listed as **Active**.

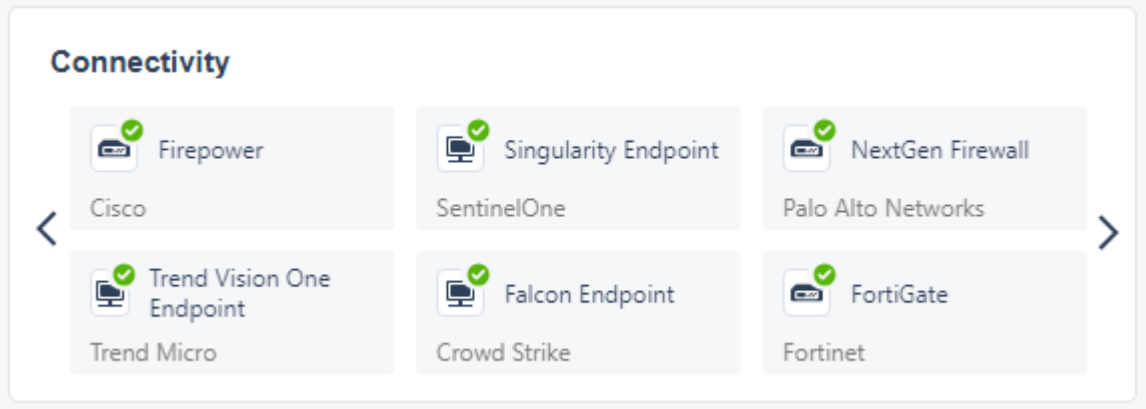
  - If you have not configured API integration, verify if **Singularity Endpoint** is listed as **Partially active**.

    To configure API integration, click the link in the tooltip or click ⋮ and then click **Edit API credentials**.

- If the access token expired, the integration status appears as **Partially active**.

  To make it active, you must generate a new API token in the SentinelOne web portal and then re-configure API integration.

- Go to the **Overview** page and in the **Connectivity** widget, verify if **Singularity Endpoint** is listed as connected.



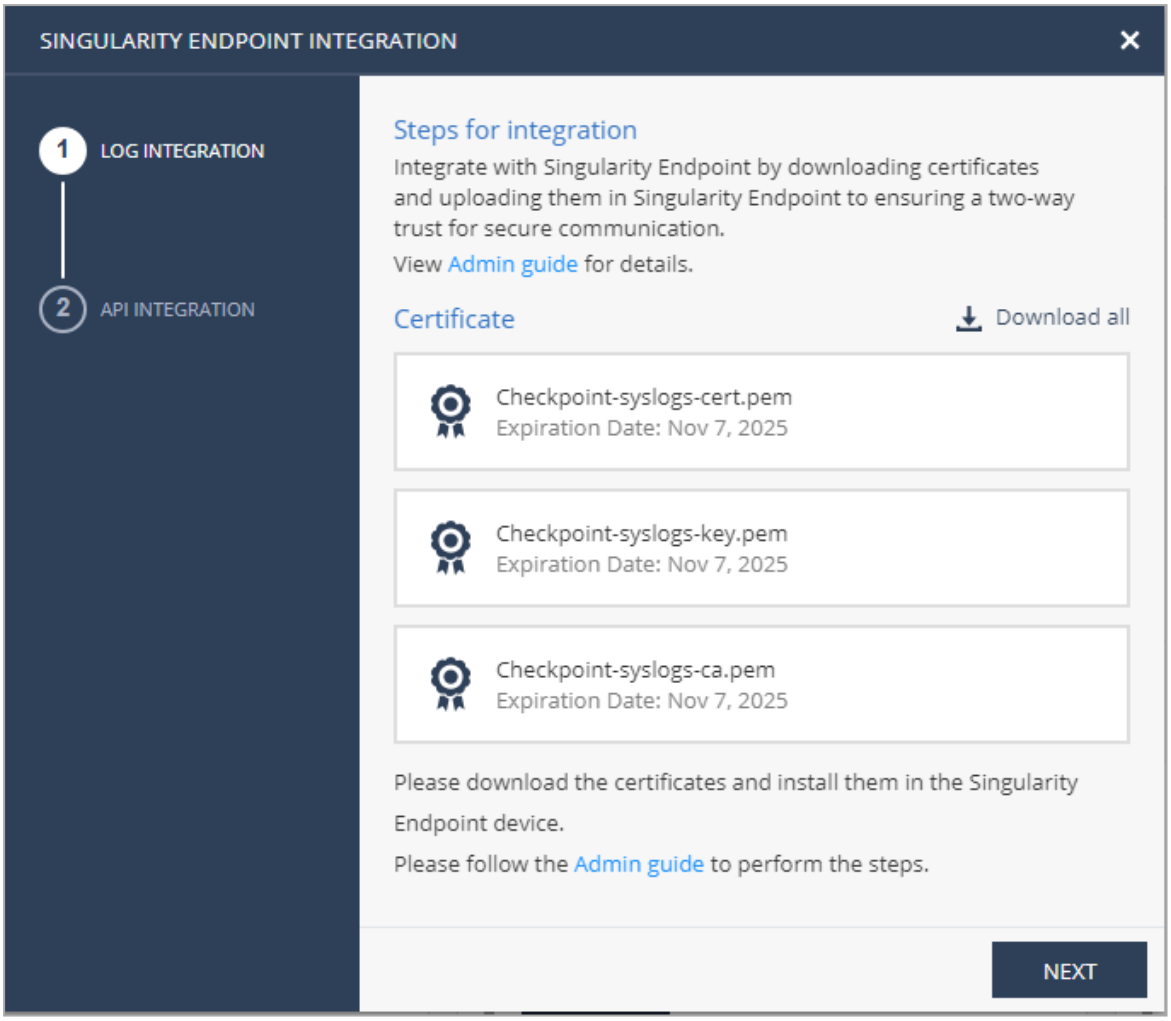
Regenerating the Certificate

If you revoke a certificate, you must regenerate and upload the certificate to the SentinelOne portal within two days.

1. Log in to the XDR Administrator Portal:
   a. Go to **Settings** > **Integrations**.
   b. In the **Singularity Endpoint** widget, click ⋮.

c. Click **Regenerate Certificate**.

The **Singularity Endpoint Integration** window appears.

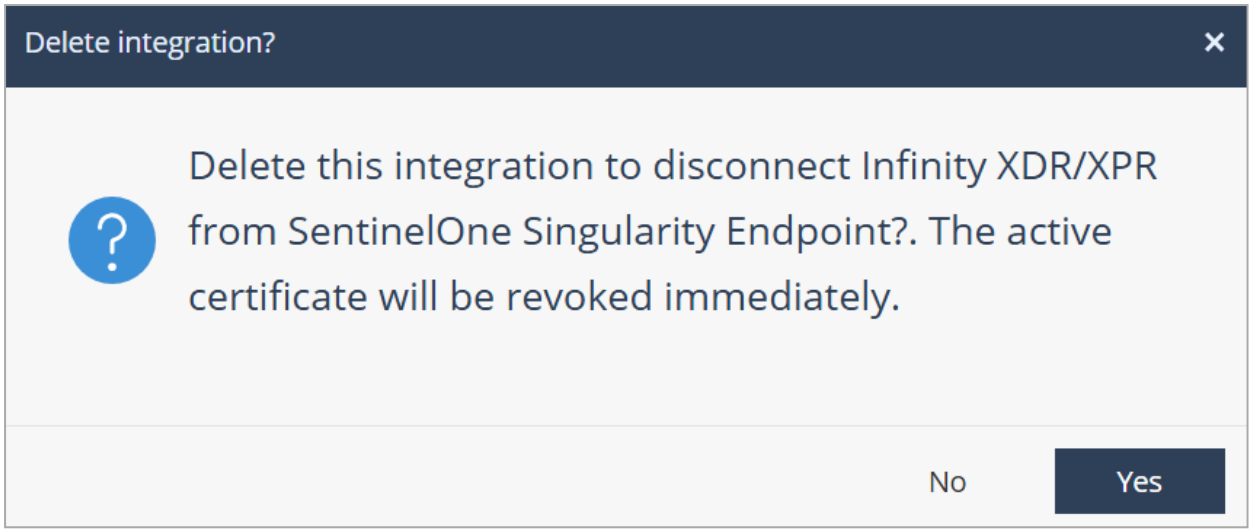


d. Perform steps 3 to 7 in Integrating SentinelOne with XDR.

Deleting the Integration

1. Go to **Settings** > **Integrations**.
2. In the **Singularity Endpoint** widget, click ⋮.
3. Click **Delete**.

   The **Delete Integration** window appears.



4. Click **Yes**.

Supported Preventive Actions

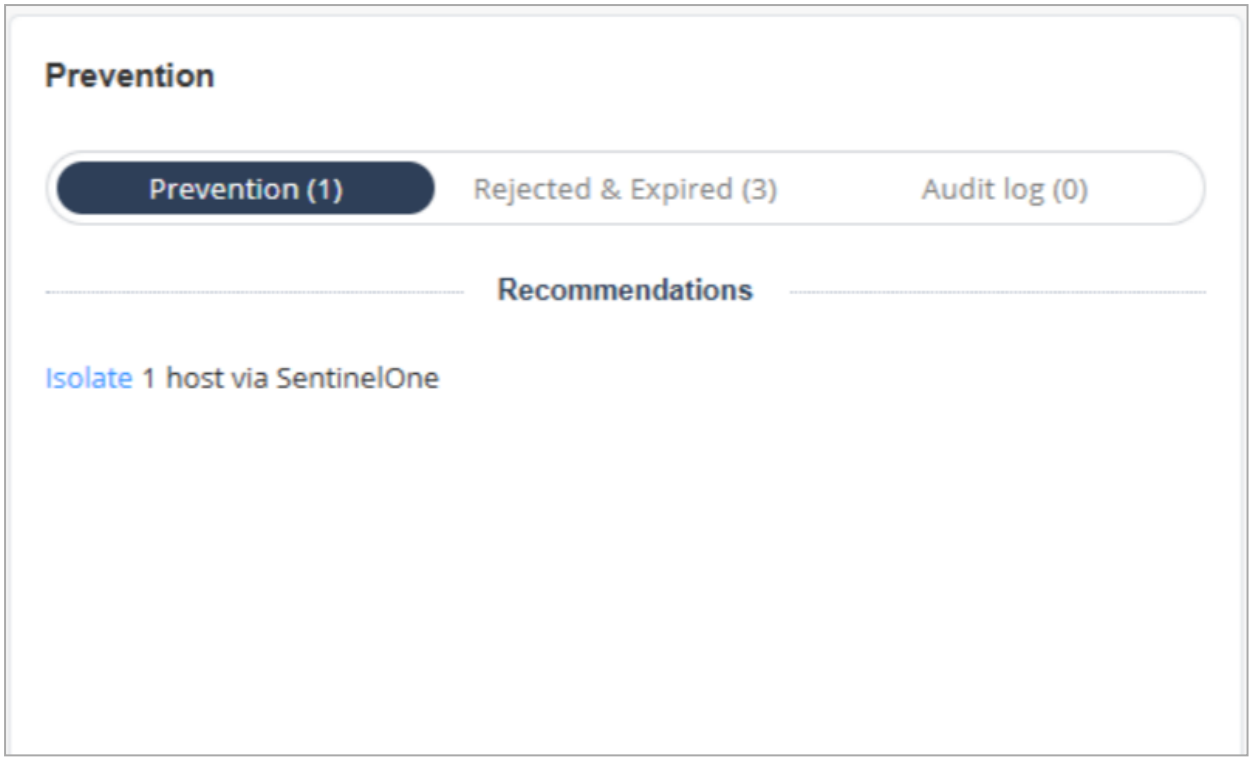
When XDR detects any malicious activity that involves SentinelOne Endpoint, it generates an incident and recommends preventive actions to mitigate it. The supported preventive action is to:

- Isolate potentially infected SentinelOne device (enforced by Endpoint)
- Quarantine potentially infected SentinelOne device (enforced by Gateway)
- Isolate Endpoint device
- Add malicious file indicator Identified by SentinelOne to IOC feed

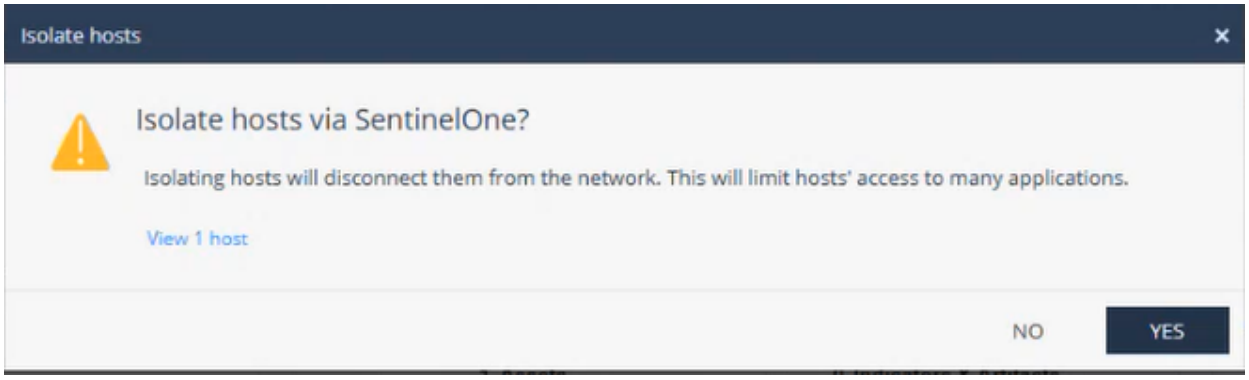
To view the recommended preventive actions for the incident:

1. Go to **Incidents** page and click the incident title or hover over the incident and click **>**.
2. In the incident **Overview** page, go to **Prevention** widget.

   The system shows the recommended preventive actions in the **Recommendations** section.
3. To isolate the host, click **Isolate**.



4. Click **Yes**.



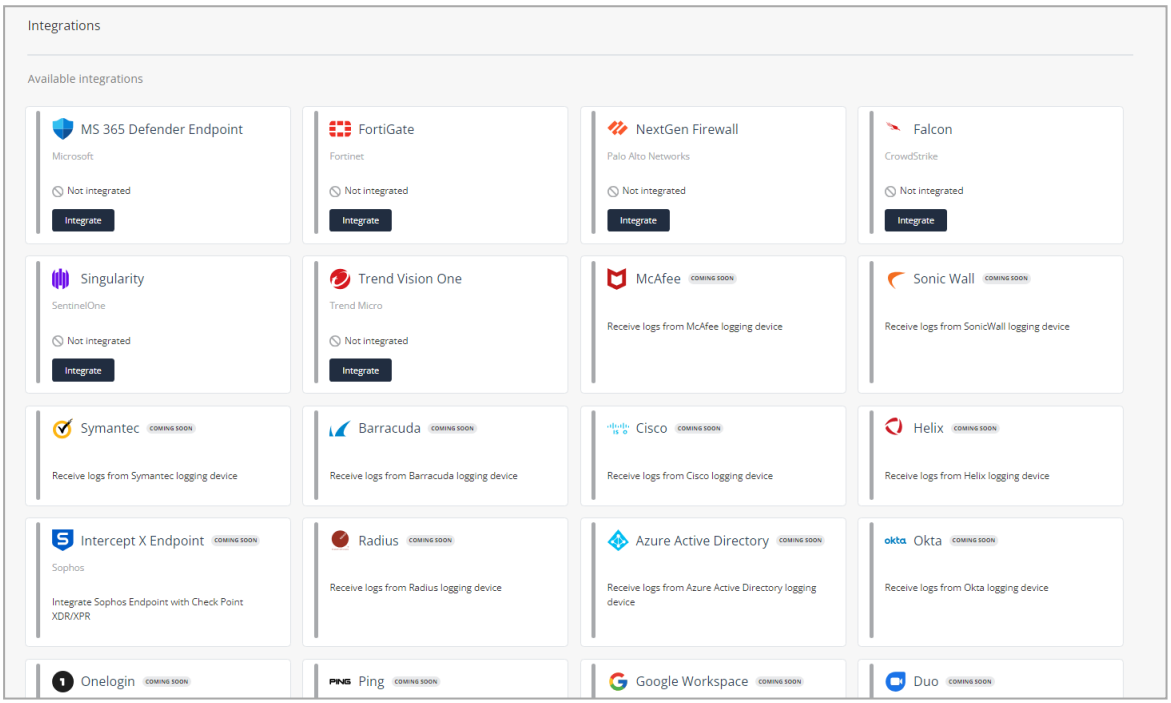
The host will be disconnected from the network.

Palo Alto Networks Next Generation Firewall

Check Point XDR analyzes the syslogs from Palo Alto Networks Next Generation Firewall for malicious activity, and suggests preventive actions, which you must manually enforce on the endpoint.

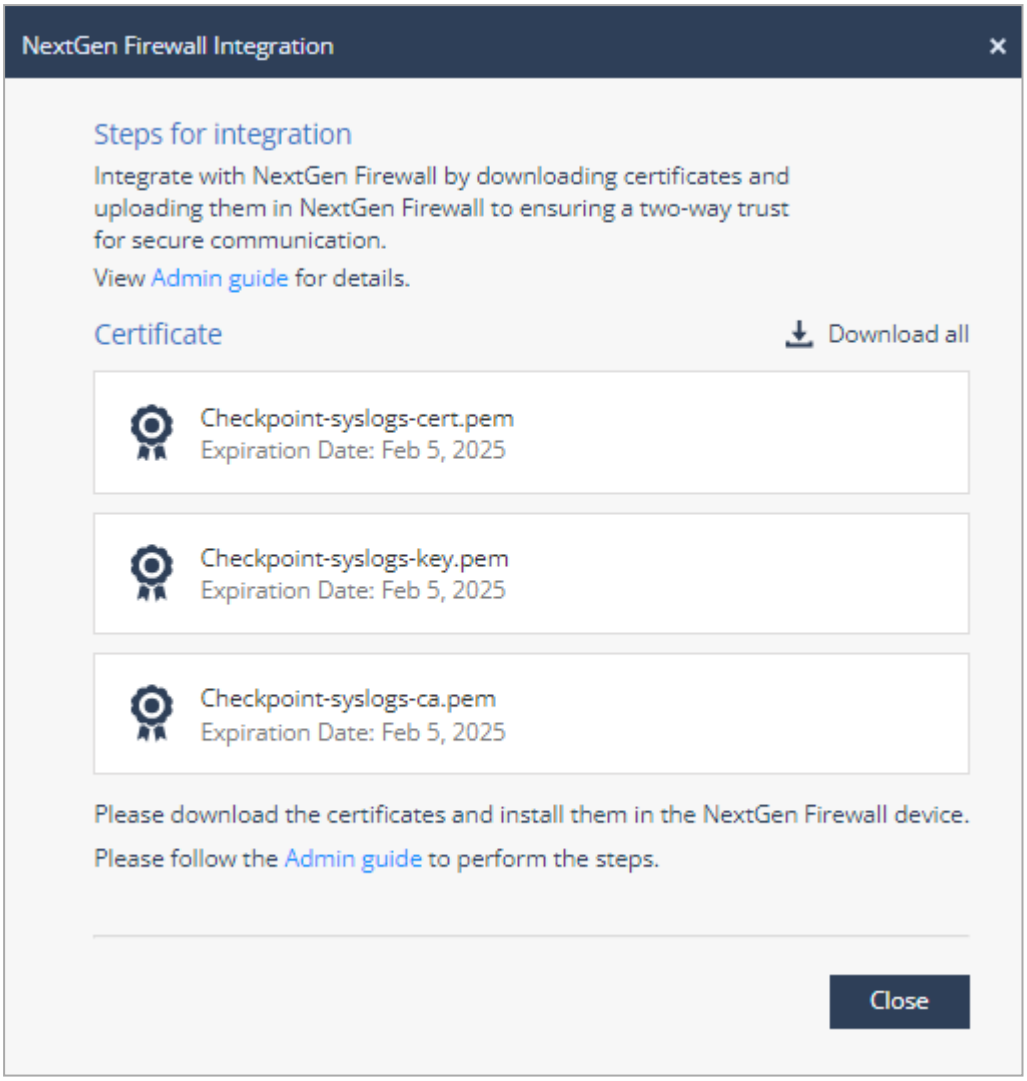
Integrating Palo Alto Networks Next Generation Firewall

1. Log in to the XDR Administrator Portal:
    a. Go to **Settings** > **Integrations**.



b. In the **NextGen Firewall** widget, click **Integrate**.

The **NextGen Firewall Integration** window appears.

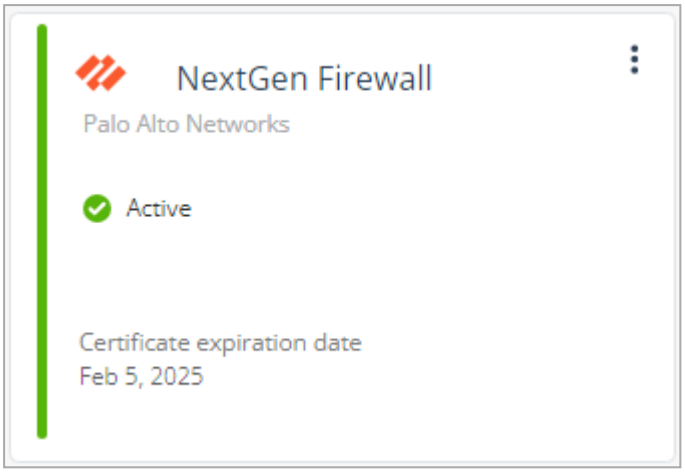


c. Click **Download all** to download the zip file that includes these certificates:

- *checkpoint-syslogs-cert.pem*
- *checkpoint-syslogs-key.pem*
- *checkpoint-syslogs-ca.pem*

d. Click **Close**.

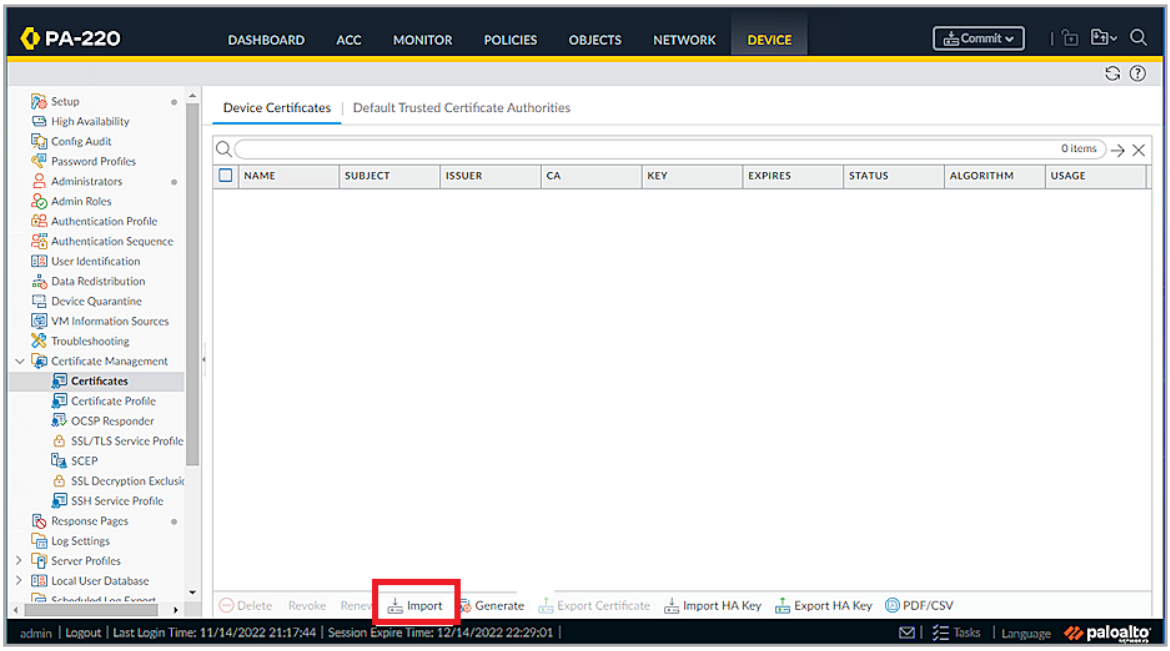
The **NextGen Firewall** widget status changes to **Active**.



2. Log in to the Palo Alto Networks Next Generation Firewall Administrator Portal:

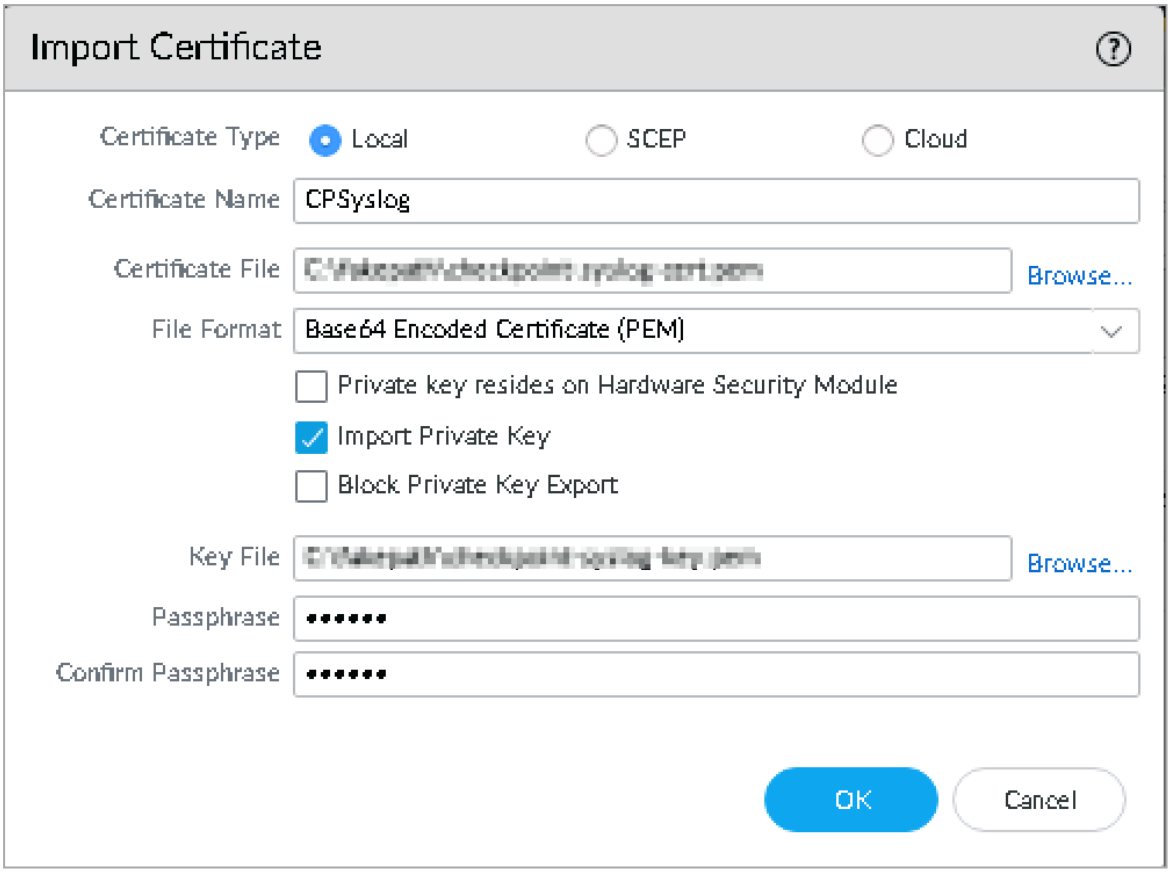
a. Go to **Device** > **Certificate Management** > **Certificates**.

b. Click **Import**.



c. From the **Import** list, select **Certificate**.

The **Import Certificate** window appears.



d. In the **Certificate Type** field, select **Local**.

e. In the **Certificate Name** field, enter **CPSyslog**.

f. In the **Certificate File** field, click **Browse** and upload the *checkpoint-syslogs-cert.pem* file.

g. From the **File Format** list, select **Base64 Encoded Certificate (PEM)**.

h. Select the **Import Private Key** checkbox.

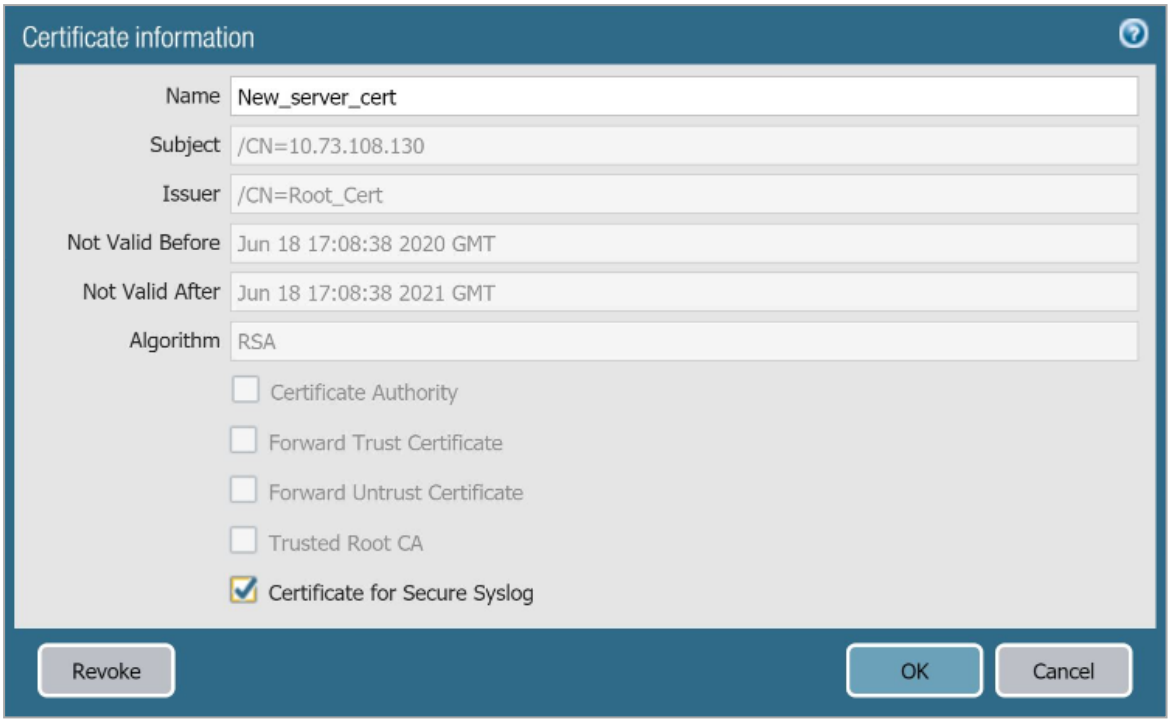
i. In the **Key File** field, click **Browse** and upload the *checkpoint-syslogs-key.pem* file.

j. In the **Passphrase** field, enter a password. The minimum supported character is six.

k. Click **OK**.

l. Click the certificate name.

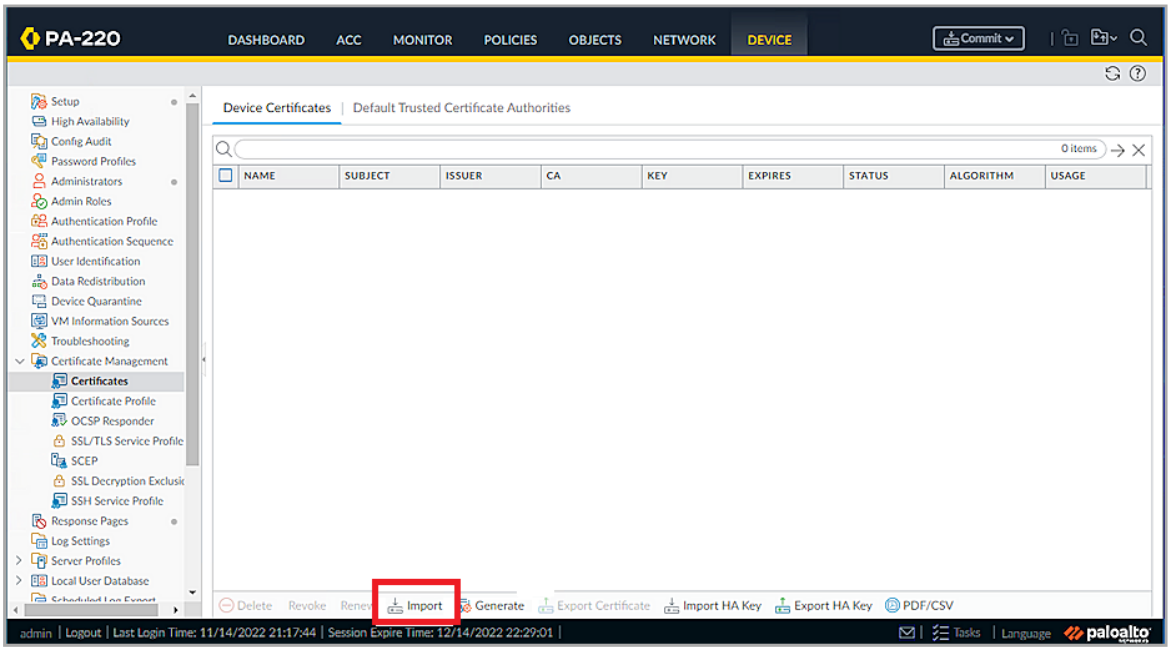
The **Certificate information** window appears.



m. Select the **Certificate for Secure Syslog** checkbox to use the certificate for SSL handshake.

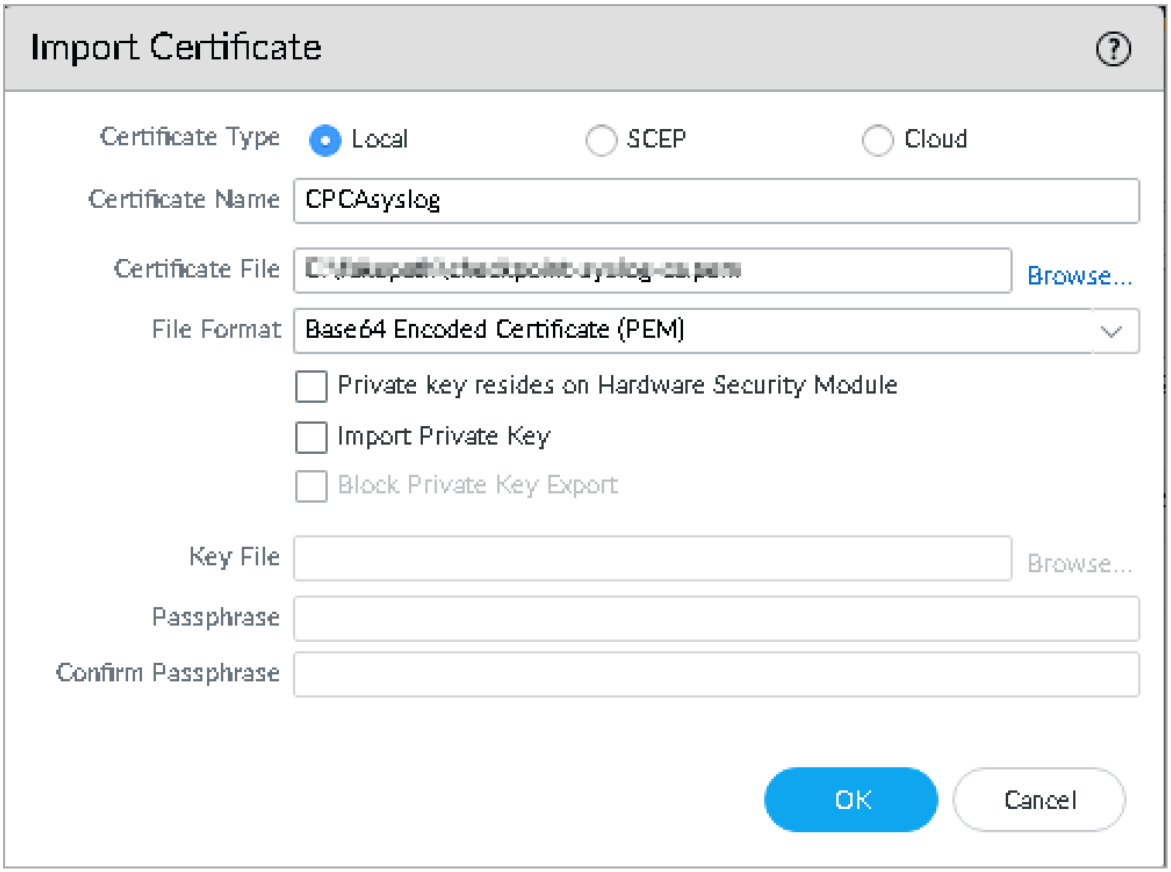
n. Click **OK**.

o. Click **Import**.



p. From the **Import** list, select **Certificate Authority (CA)**.

The **Import Certificate** window appears.



q. In the **Certificate Type** field, select **Local**.

r. In the **Certificate Name** field, enter **CPCASyslogs**.

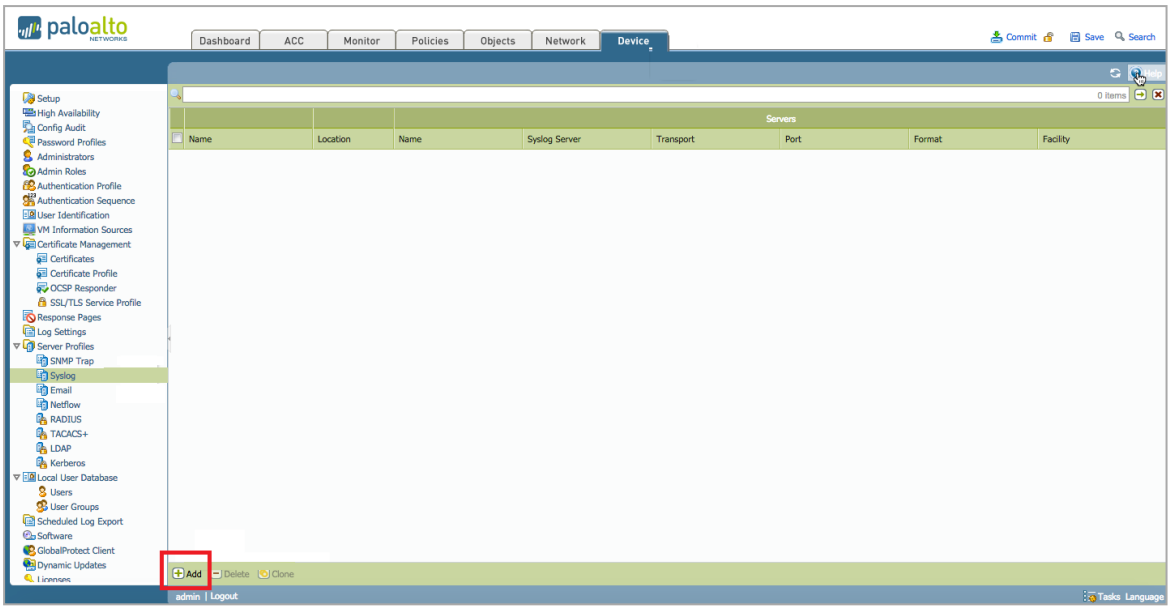
s. In the **Certificate File** field, click **Browse** and upload the *checkpoint-syslogs-ca.pem* file.

t. From the **File Format** list, select **Base64 Encoded Certificate (PEM)**.

u. Click **OK**.

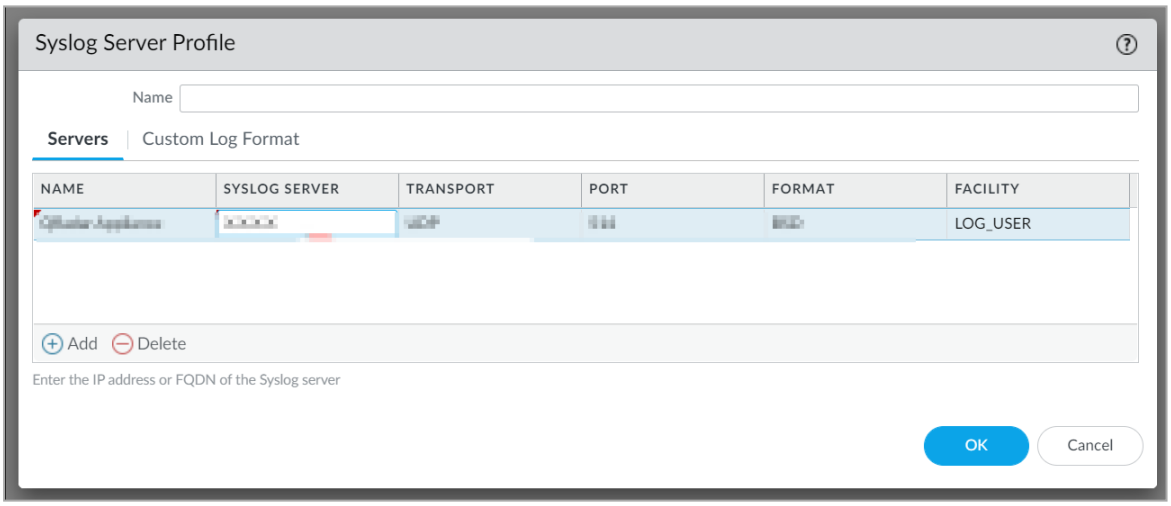
3. To configure syslog monitoring:

a. Go to **Device** > **Server Profiles** > **Syslog**.



b. Click **Add** to create a new profile.

The **Syslog Server Profile** window appears.



c. In the **Name** field, enter **XDRIntegration**.

d. Click the **Servers** tab:

   i. In the **Name** field, enter a name for the syslog server.

   ii. In the **Syslog Server** field, enter your production server IP address:

   - For EU region, enter **20.76.50.141**
   - For US region, enter **20.22.126.247**
   - For UAE region, enter **20.174.45.149**

   iii. From the **Transport** list, select **SSL**.

   iv. In the **Port** field, enter **6514**.

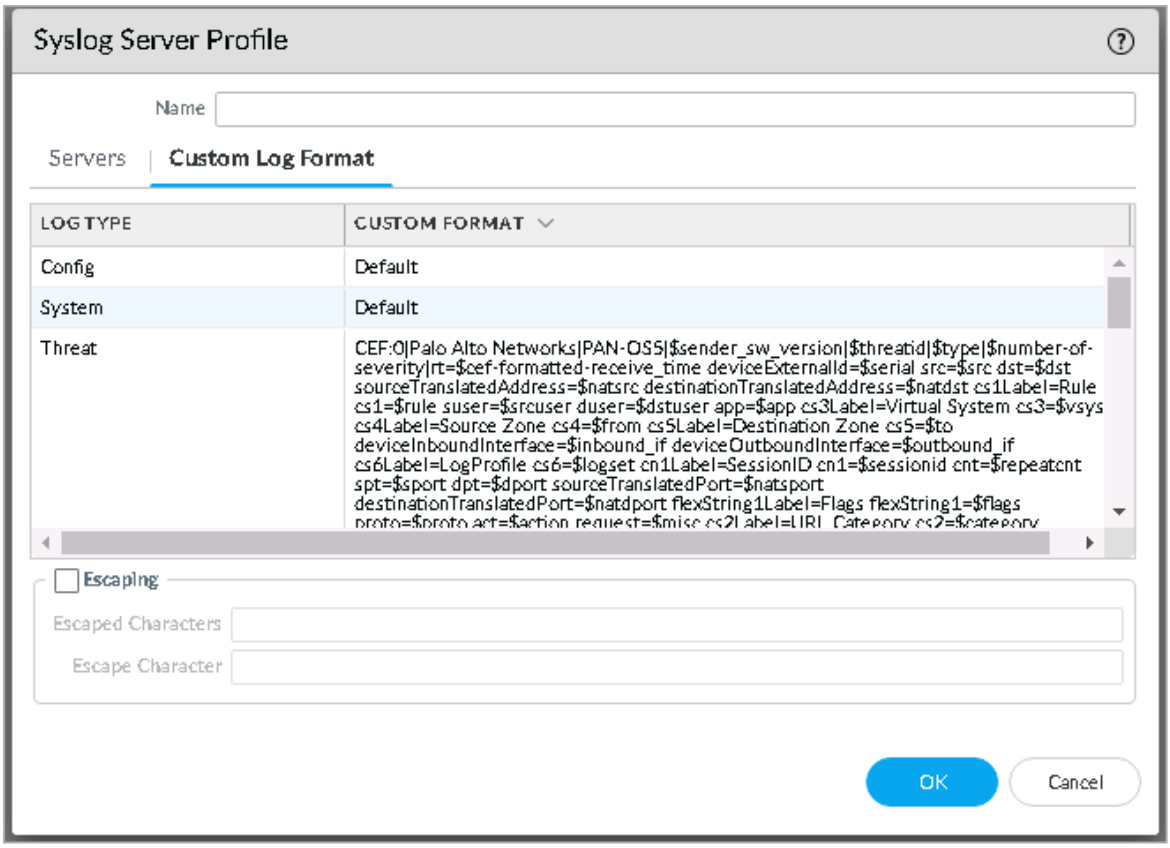
   v. From the **Format** list, select **BSD**.

   vi. From the **Facility** list, select **LOG_USER**.

e. To translate PAN log format to CEF log format, go to **Custom Log Format** and in the **Threat** field, paste this syntax:

```
CEF:0|Palo Alto Networks|PAN-OS5|$sender_sw_
version|$threatid|$type|$number-of-severity|rt=$cef-
formatted-receive_time deviceExternalId=$serial src=$src
dst=$dst sourceTranslatedAddress=$natsrc
destinationTranslatedAddress=$natdst cs1Label=Rule cs1=$rule
suser=$srcuser duser=$dstuser app=$app cs3Label=Virtual
System cs3=$vsys cs4Label=Source Zone cs4=$from
cs5Label=Destination Zone cs5=$to
deviceInboundInterface=$inbound_if
deviceOutboundInterface=$outbound_if cs6Label=LogProfile
cs6=$logset cn1Label=SessionID cn1=$sessionid cnt=$repeatcnt
spt=$sport dpt=$dport sourceTranslatedPort=$natsport
destinationTranslatedPort=$natdport flexString1Label=Flags
flexString1=$flags proto=$proto act=$action request=$misc
cs2Label=URL Category cs2=$category
flexString2Label=Direction flexString2=$direction
PanOSActionFlags=$actionflags externalId=$seqno cat=$subtype
fileId=$pcap_id PanOSDGl1=$dg_hier_level_1 PanOSDGl2=$dg_
hier_level_2 PanOSDGl3=$dg_hier_level_3 PanOSDGl4=$dg_hier_
level_4 PanOSVsysName=$vsys_name dvchost=$device_name
PanOSSrcUUID=$src_uuid PanOSDstUUID=$dst_uuid
PanOSTunnelID=$tunnelid PanOSMonitorTag=$monitortag
PanOSParentSessionID=$parent_session_id
PanOSParentStartTime=$parent_start_time
PanOSTunnelType=$tunnel PanOSThreatCategory=$thr_category
PanOSContentVer=$contentver PanOSAssocID=$assoc_id
PanOSPPID=$ppid PanOSHTTPHeader=$http_headers
PanOSURLCatList=$url_category_list PanOSRuleUUID=$rule_uuid
PanOSHTTP2Con=$http2_connection
PanDynamicUsrgrp=$dynusergroup_name PanXFFIP=$xff_ip
PanSrcDeviceCat=$src_category PanSrcDeviceProf=$src_profile
PanSrcDeviceModel=$src_model PanSrcDeviceVendor=$src_vendor
PanSrcDeviceOS=$src_osfamily PanSrcDeviceOSv=$src_osversion
PanSrcHostname=$src_host PanSrcMac=$src_mac
PanDstDeviceCat=$dst_category PanDstDeviceProf=$dst_profile
PanDstDeviceModel=$dst_model PanDstDeviceVendor=$dst_vendor
PanDstDeviceOS=$dst_osfamily PanDstDeviceOSv=$dst_osversion
PanDstHostname=$dst_host PanDstMac=$dst_mac
PanContainerName=$container_id PanPODNamespace=$pod_
namespace PanPODName=$pod_name PanSrcEDL=$src_edl
PanDstEDL=$dst_edl PanGPHostID=$hostid
PanEPSerial=$serialnumber PanDomainEDL=$domain_edl
PanSrcDAG=$src_dag PanDstDAG=$dst_dag
PanPartialHash=$partial_hash PanTimeHighRes=$high_res_
timestamp PanReasonFilteringAction=$reason
```

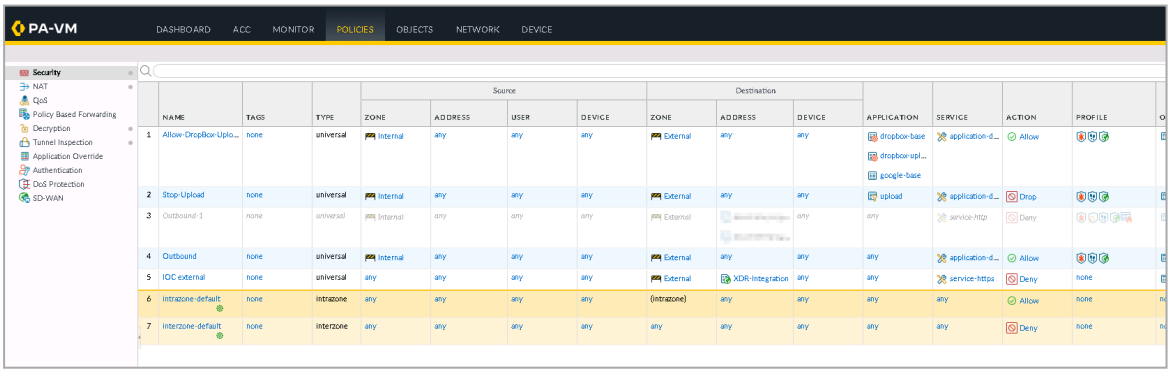
```
PanJustification=$justification PanASServiceType=$nssai_sst
```



f. Click **OK** to save the profile.

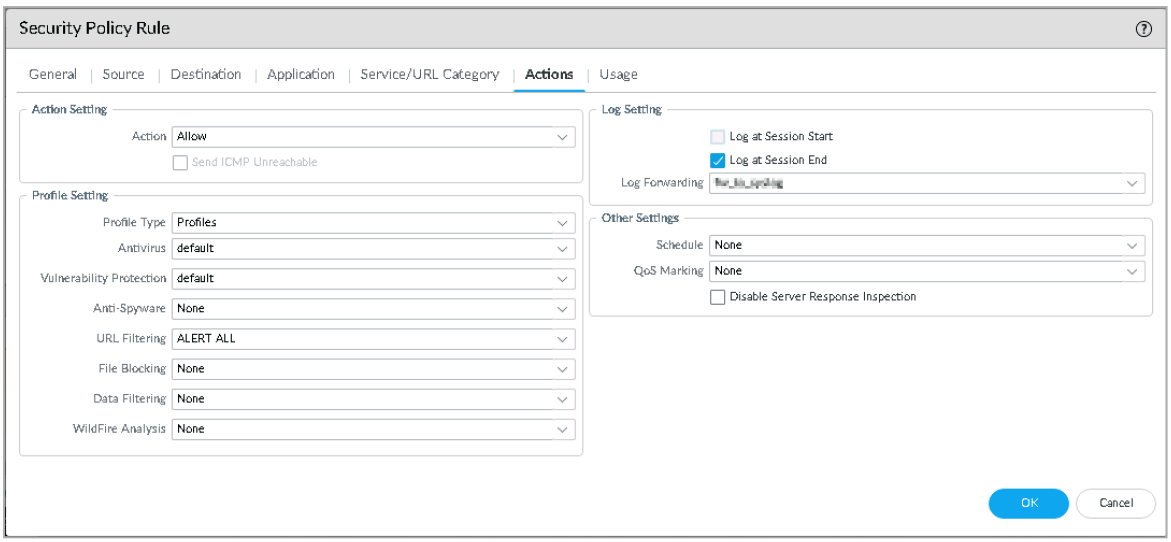
4. To configure security policy rule action as log forwarding:

   a. Go to **Policies** > **Security**.



b. Select a rule for which you want to enable log forwarding.

   The **Security Policy Rule** window appears.



c. Click **Actions**.

d. In the **Log Setting** section, select the **Log at Session End** checkbox.

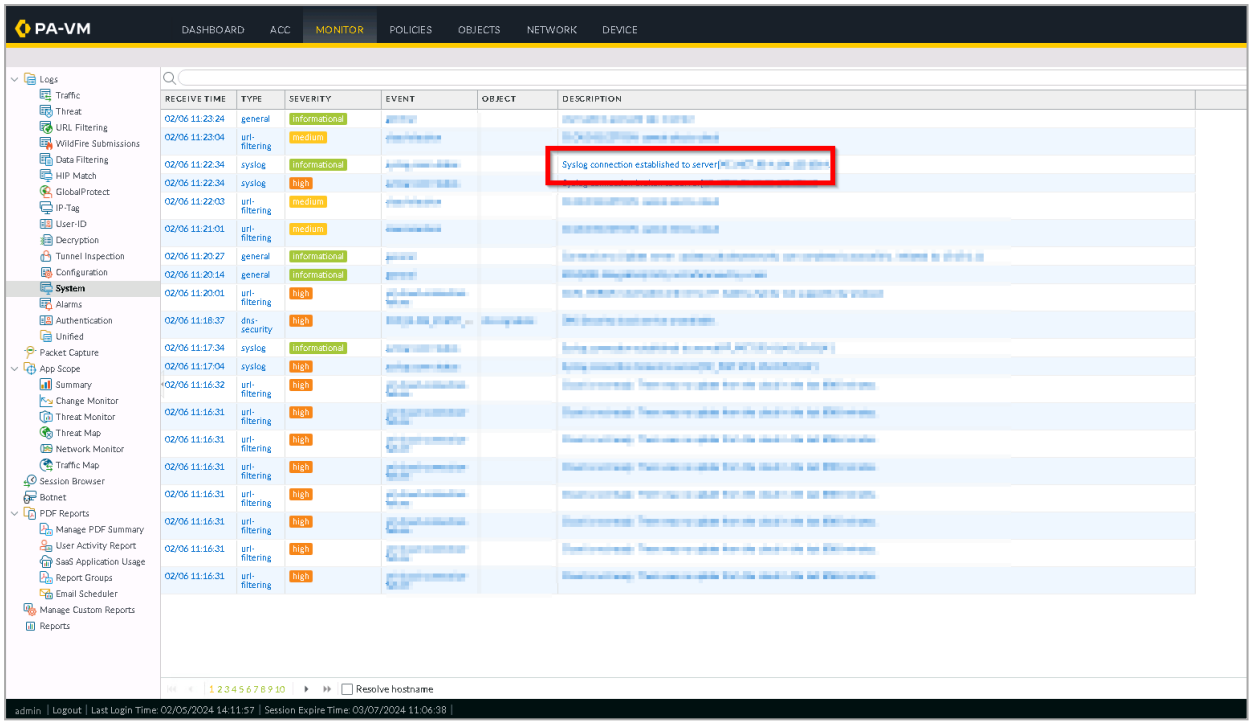
e. From the **Log Forwarding** list, select **XDRIntegration** syslog profile to which the logs to be forwarded.

f. Click **OK**.

5. To verify log forwarding:

   a. Go to **Monitor** > **Logs** > **System**.

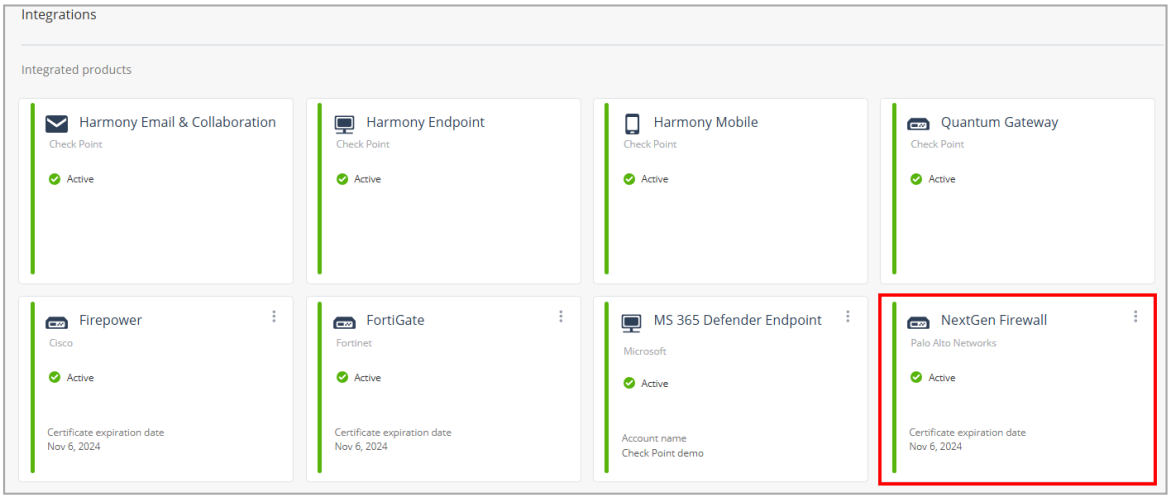
   b. Make sure the `Syslog connection established to server <IP Address>` message is displayed and error messages are not listed.



6. To check if the integration is successful, in the XDR Administrator Portal:

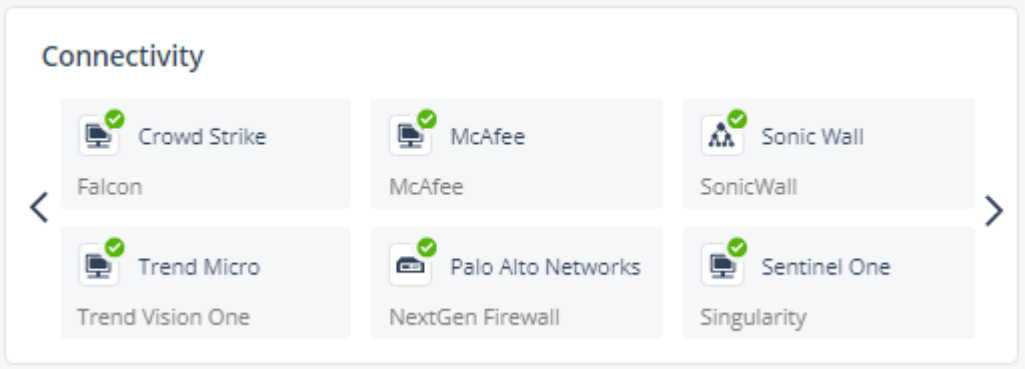
   - Go to **Settings** > **Integrations**.

     In the **Integrated products** section, verify if **NextGen Firewall** is listed as **Active**.



Note - The widget will display **Inactive** status until XDR begins receiving logs from Palo Alto Networks Next Generation Firewall.

- Go to the **Overview** page and in the **Connectivity** widget, verify if **Palo Alto Networks**is listed as connected.

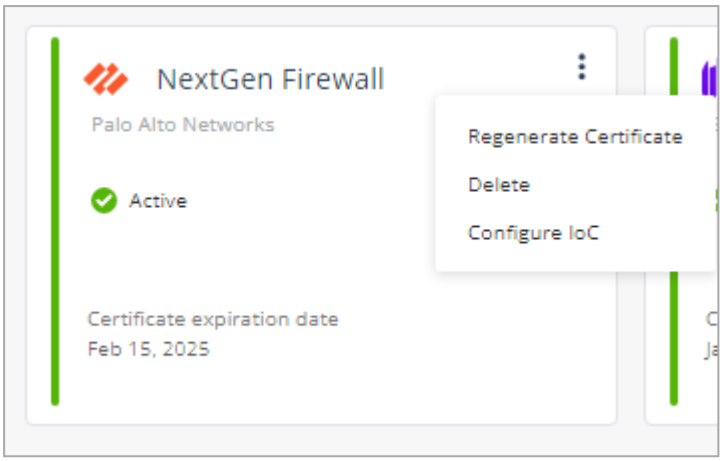


Regenerating the Certificate

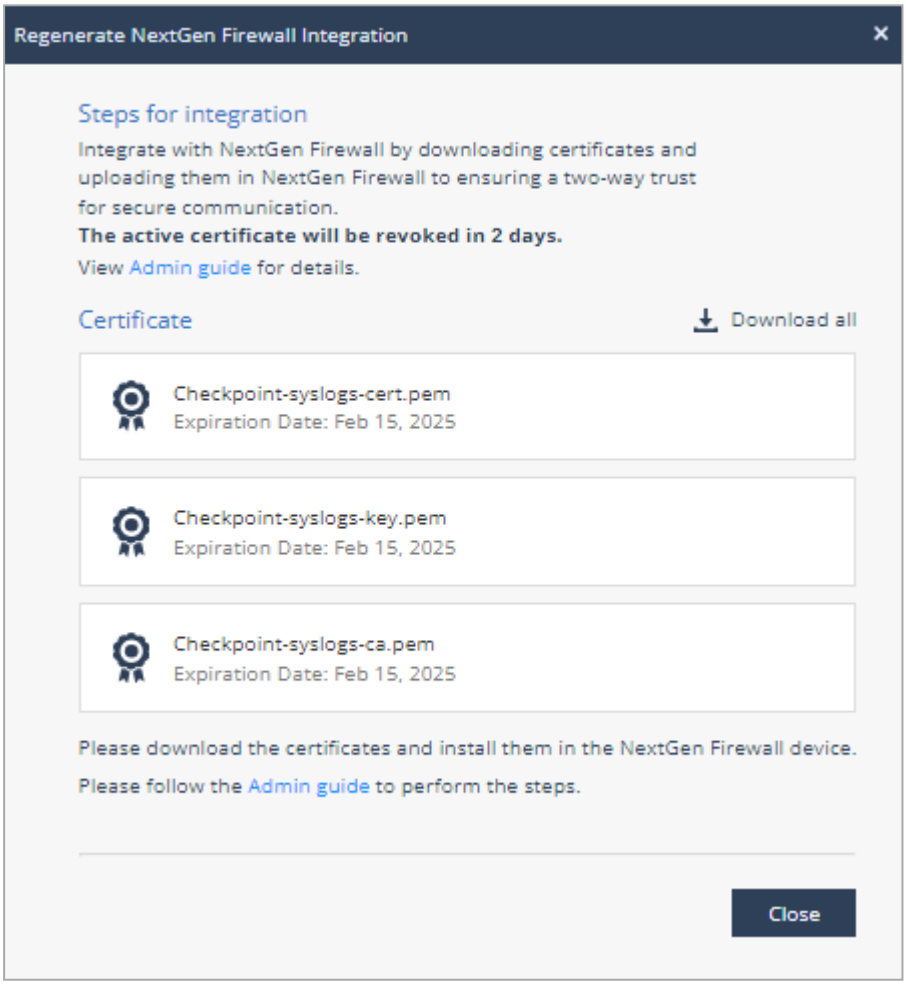
If you revoke a certificate, you must regenerate and upload the certificate to the Palo Alto Networks Next Generation Firewall portal within two days.

1. Log in to the XDR Administrator Portal:
   a. Go to **Settings** > **Integrations**.
   b. In the **NextGen Firewall** widget, click ⋮.

c. Click **Regenerate Certificate**.



The **Regenerate NextGen Firewall Integration** window appears.



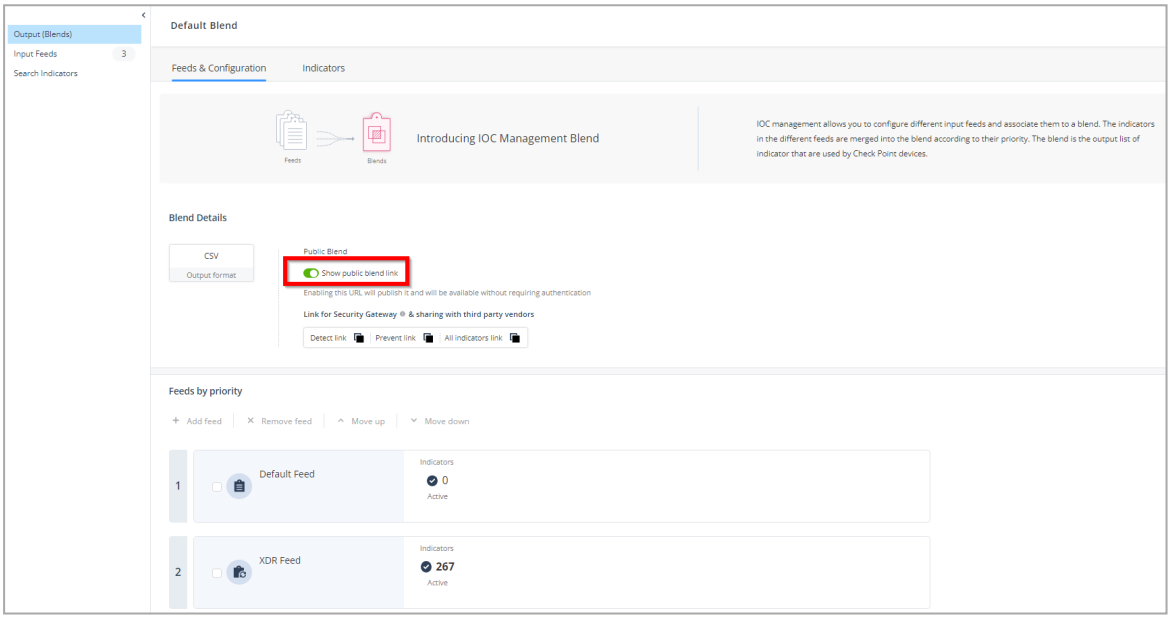
d. Perform steps from 1.c until the end in *"Integrating Palo Alto Networks Next Generation Firewall" on page 282*.

Configuring IoCs

You can use the **Public Blend URL** in the IoC Management to enforce IoCs on the Palo Alto Networks Next Generation Firewall.

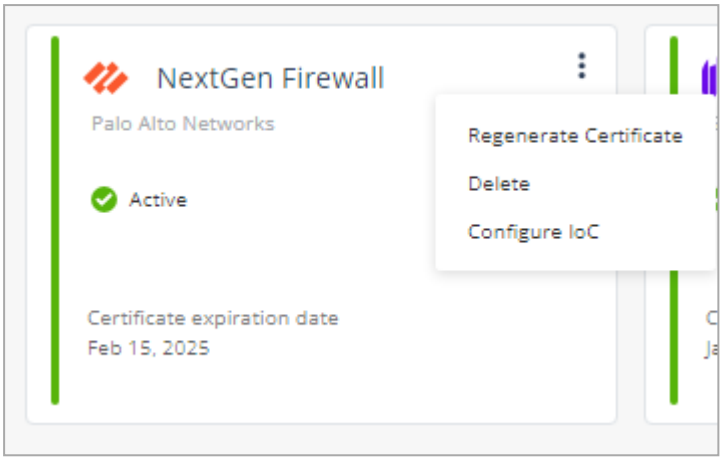
To configure IoCs:

1. Log in to the XDR Administrator Portal:
   a. Go to **New IOC Management** > **Output (Blends)** > **Feeds & Configuration**.
   b. Turn on the **Show public blend link** toggle button.



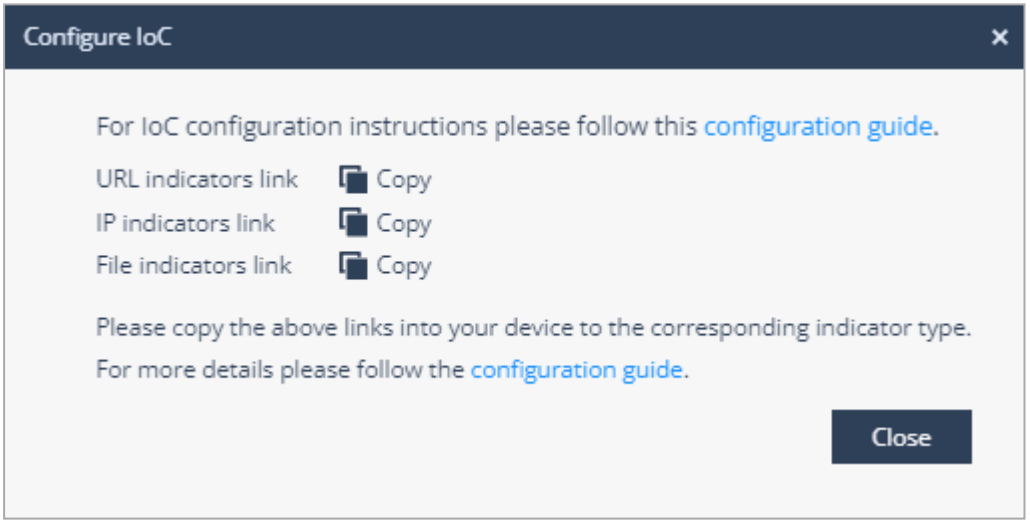
   c. Go to **Settings** > **Integrations**.

d. In the **NextGen Firewall** widget, click ⋮ and select **Configure IoC**.



The **Configure IoC** window appears. It lists three indicator links generated automatically using the **All Indicators link** from the **Public Blend URL** in the IoC Management.

e. Click ⧉ to copy the indicators link.



Note - The Palo Alto Networks Next Generation Firewall do not support the **File indicators link**.

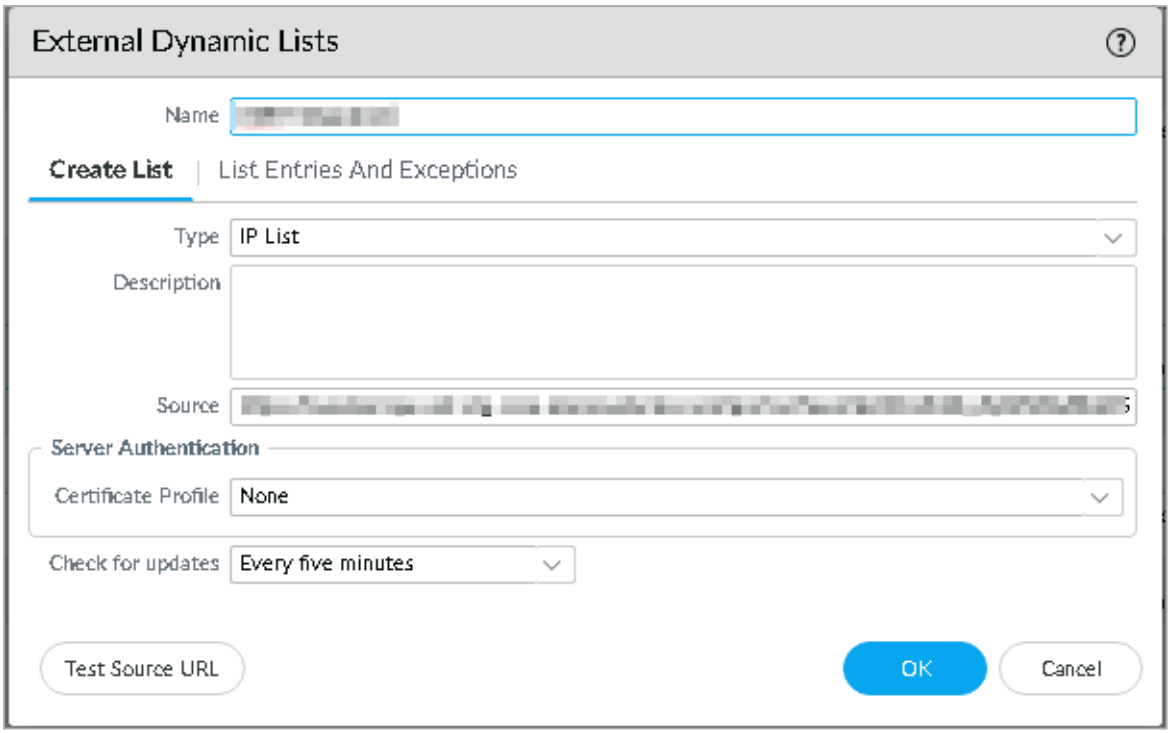
f. Click **Close**.

2. Log in to the Palo Alto Networks Next Generation Firewall Administrator Portal:

a. Go to **Objects** > **External Dynamic Lists**.

b. Click **Add**.

The **External Dynamic Lists** window appears.



c. In the **Name** field, enter the name of the External Dynamic List.

d. Click the **Create List** tab.

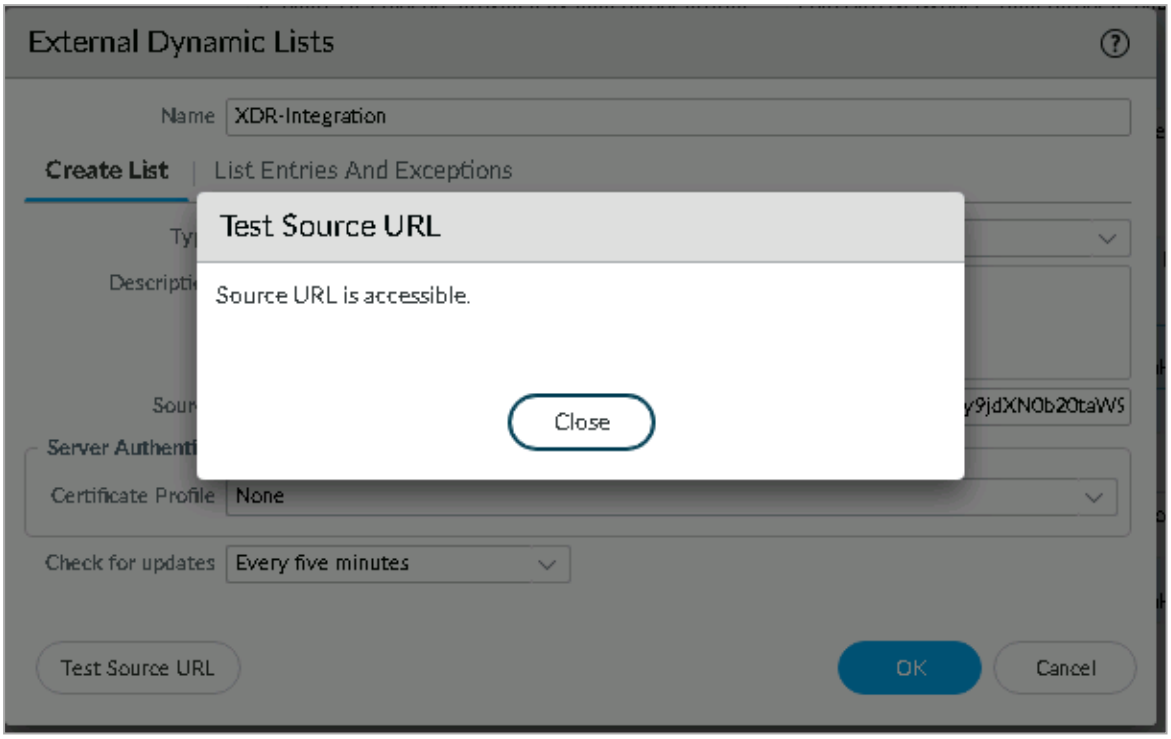
e. From the **Type** list, select **IP List**.

f. In the **Source** field, paste the **IP indicators link** copied in the step 1.e.

g. To check if the source url is accessible, click **Test Source URL**.

If the source url is accessible, the **Test Source URL** window appears with a message:

Source URL is accessible



h. Click **Close**.

i. Click **OK**.

j. Repeat steps **2.b** through **2.i** with this detail:

Type	Source
URL List	**URL indicators link** (Configure IoC link from step 1.e)

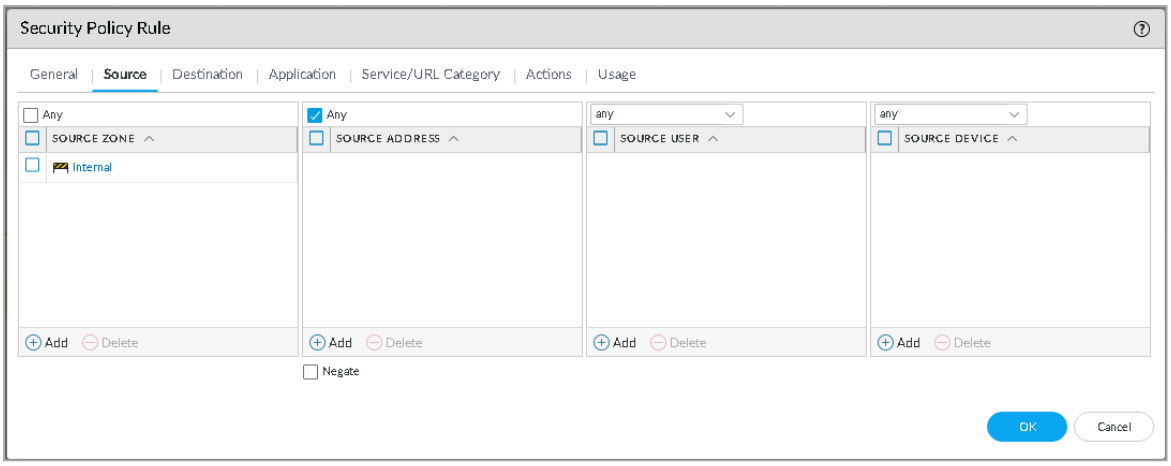
k. Click **Commit** at the top right corner to commit your changes.

3. To create a security policy with External Dynamic List (EDL):

a. Go to **Policies** > **Security**.

b. Click **Add**.

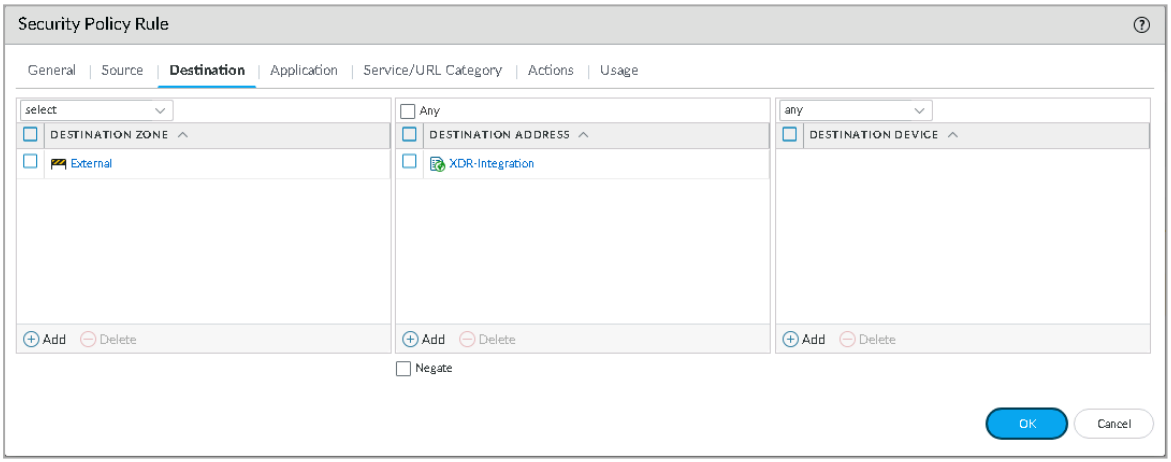
c. Click the **Source** tab.



d. In the **Source Zone** column, click **Add** and from the list, select a source zone.

e. In the **Source Address** column, select the **Any** checkbox.

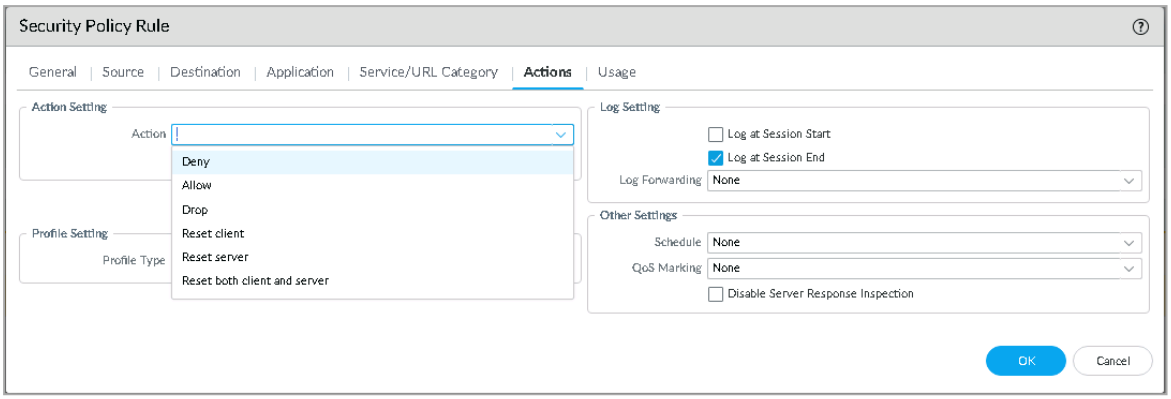
f. Click the **Destination** tab.



g. In the **Destination Zone** column, click **Add** and from the list, select **External**.

h. In the **Destination Address** column, click **Add** and from the list, select your External Dynamic List name.

i. Click the **Actions** tab.



j. In the **Action Setting** section, from the **Action** list, select one of these:

- **Allow**
- **Deny**
- **Drop**
- **Reset client**
- **Reset server**
- **Reset both client and server**

k. Click **OK**.

The newly added EDL appears in the policy table.

l. Click **Commit** at the top right corner to save your changes.

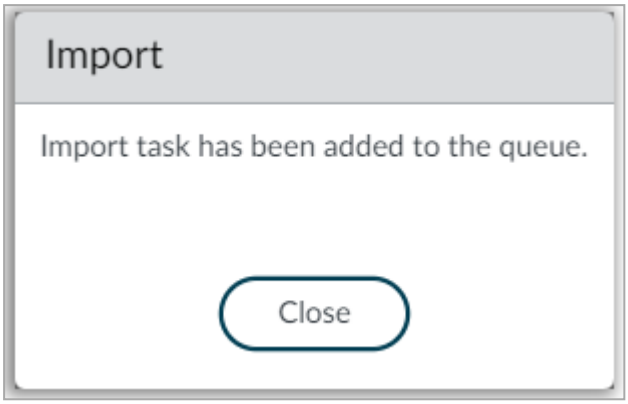
4. To verify the IP addresses that are newly created in EDL:

a. Go to **Objects** > **External Dynamic Lists**.

b. Select your EDL.

c. Click **Import Now** at the bottom.

The **Import** window appears.

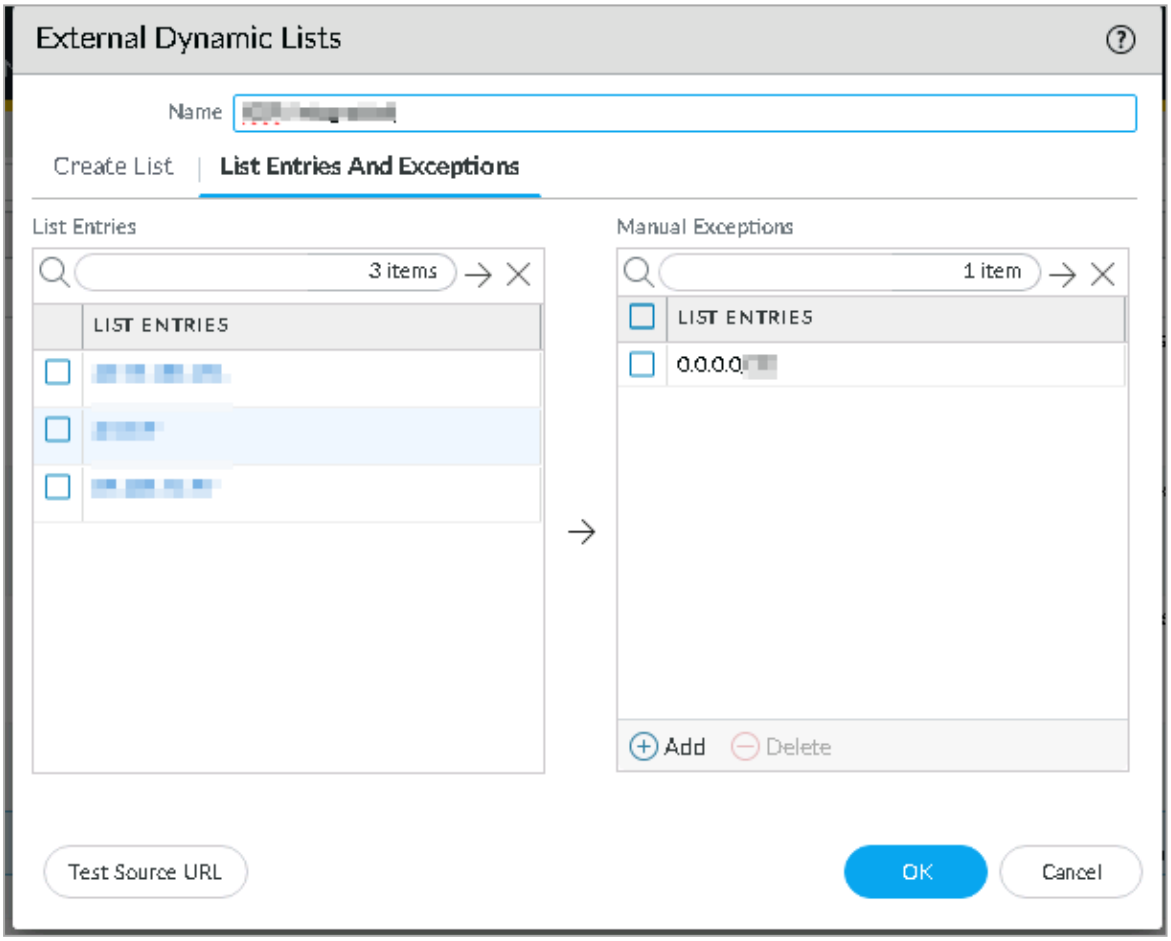


d. Click **Close**.

e. Click **Commit** at the top right corner to save your changes.

f. To check the available IP addresses on the XDR external feed, select your EDL.

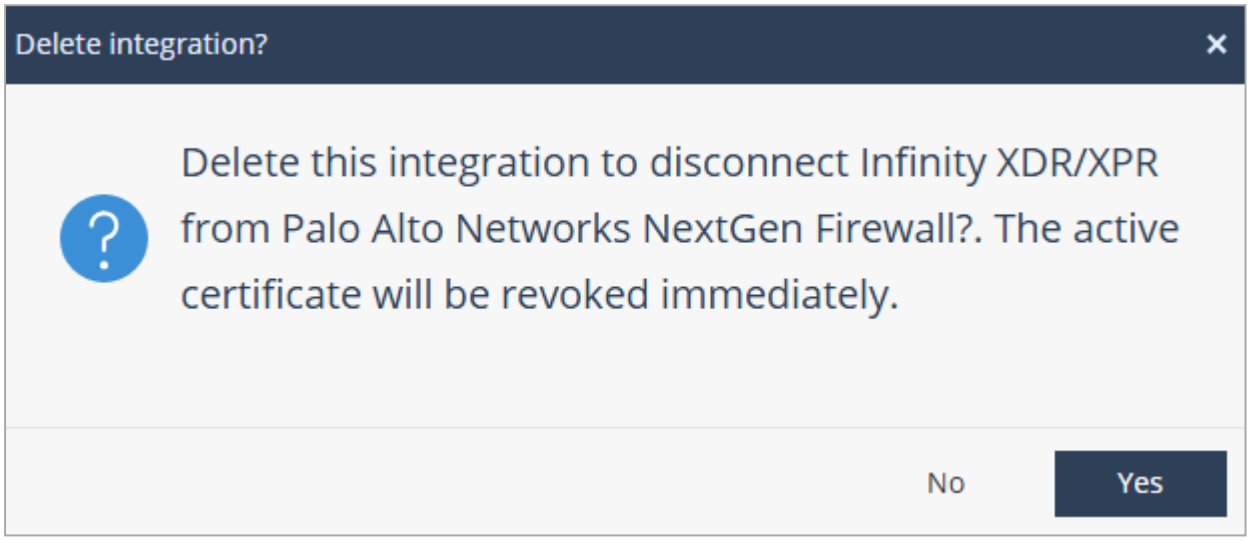
g. Click the **List Entries and Exceptions** tab.



Deleting the Integration

1. Go to **Settings** > **Integrations**.
2. In the **NextGen Firewall** widget, click ⋮.
3. Click **Delete**.

   The **Delete Integration** window appears.



4. Click **Yes**.

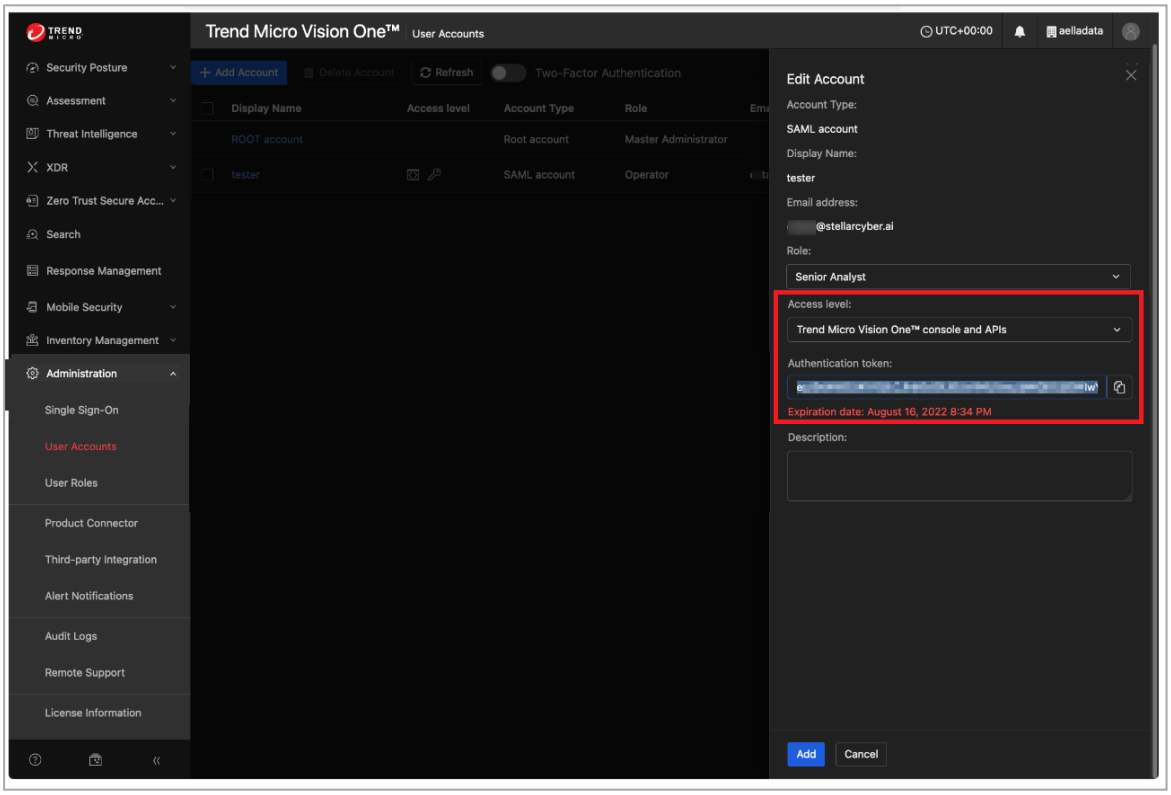
Trend Vision One for Endpoint

Check Point XDR analyzes the alerts generated in Trend Vision One for malicious activity, and suggests preventive actions, which you must manually enforce on the endpoint.

Integrating Trend Vision One for Endpoint

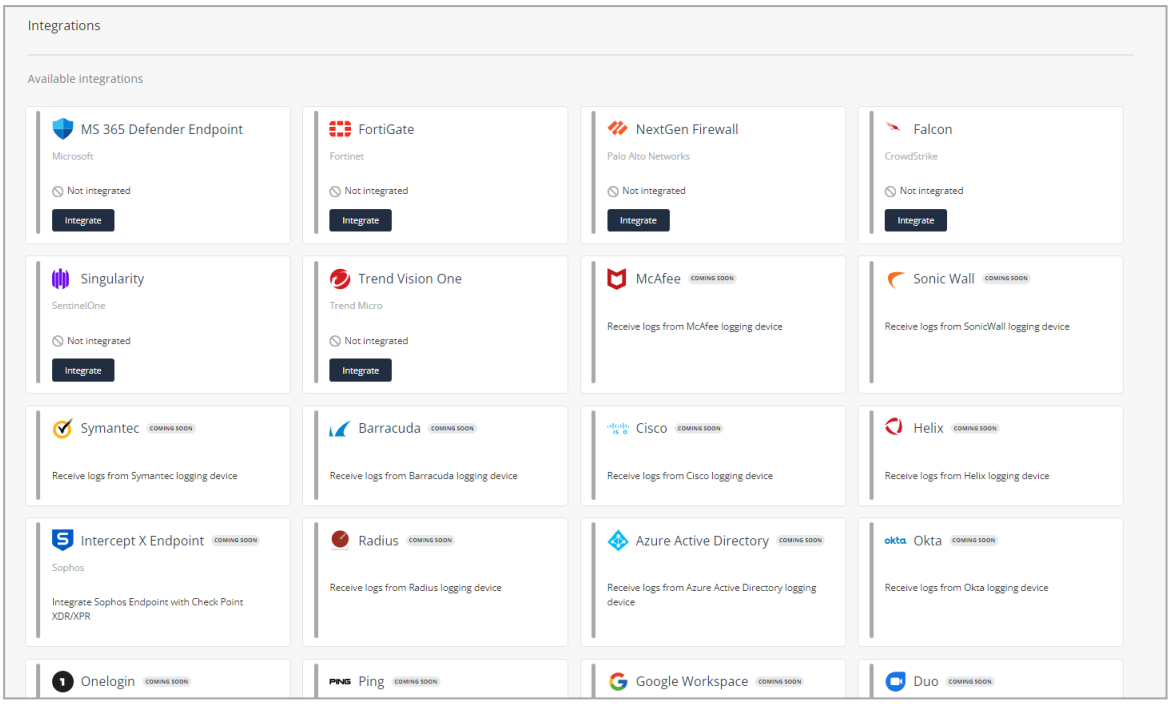
1. Log in to your Trend Micro Vision One portal:
   a. Go to **Administration** > **User Accounts**.
   b. Select the account that is associated with your XDR Administrator Portal.

      The **Edit Account** window appears.
   c. Make sure that the **Access level** is set to **Trend Micro Vision One™ console and APIs**.



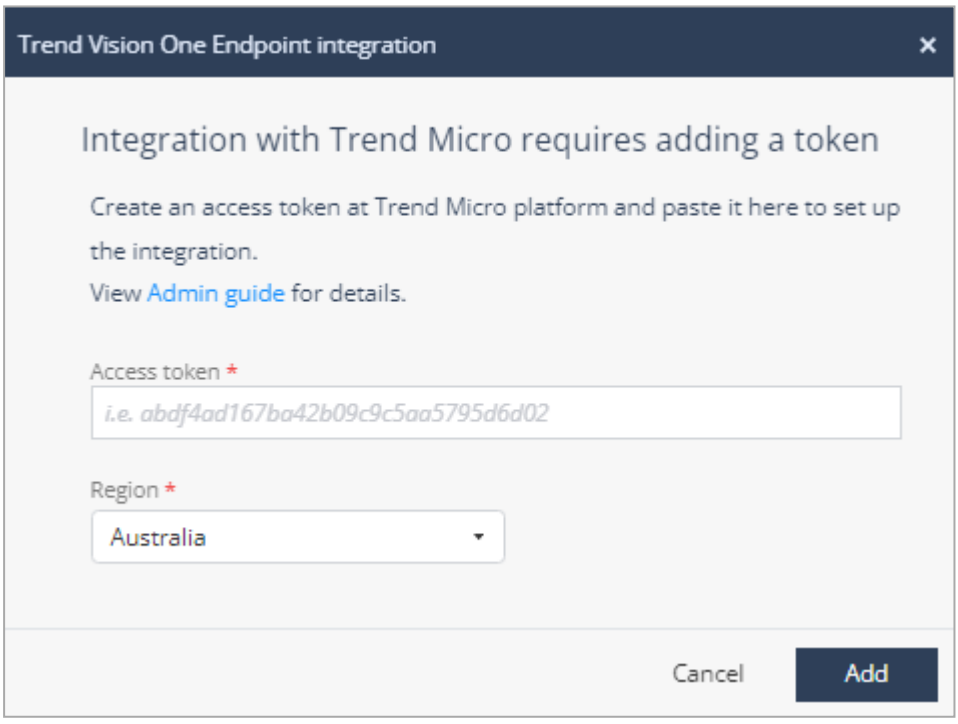
   d. In the **Authentication token** field, click to copy the token. If the API token is missing, click **Generate new authentication token** to generate the token and then click .
   e. Click **Add**.
2. Log in to the XDR Administrator Portal:

a. Go to **Settings** > **Integrations**.



b. In the **Trend Vision One** widget, click **Integrate**.

The **Trend Vision One Endpoint integration** window appears.

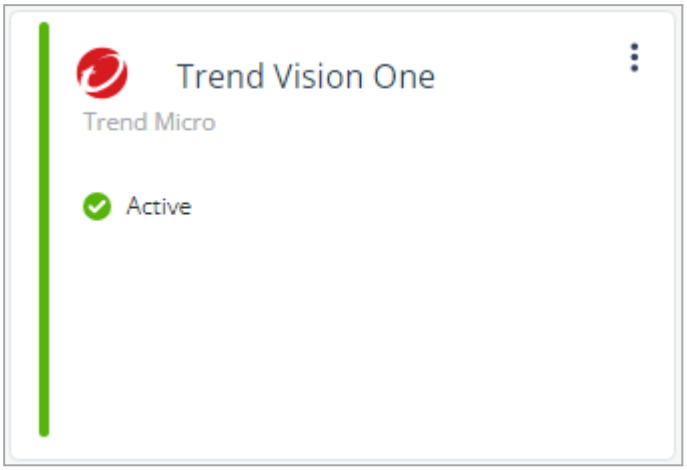


c. In the **Access token** field, paste the authentication token copied in step 1.d.

d. From the **Region** list, select your region.

e. Click **Add**.

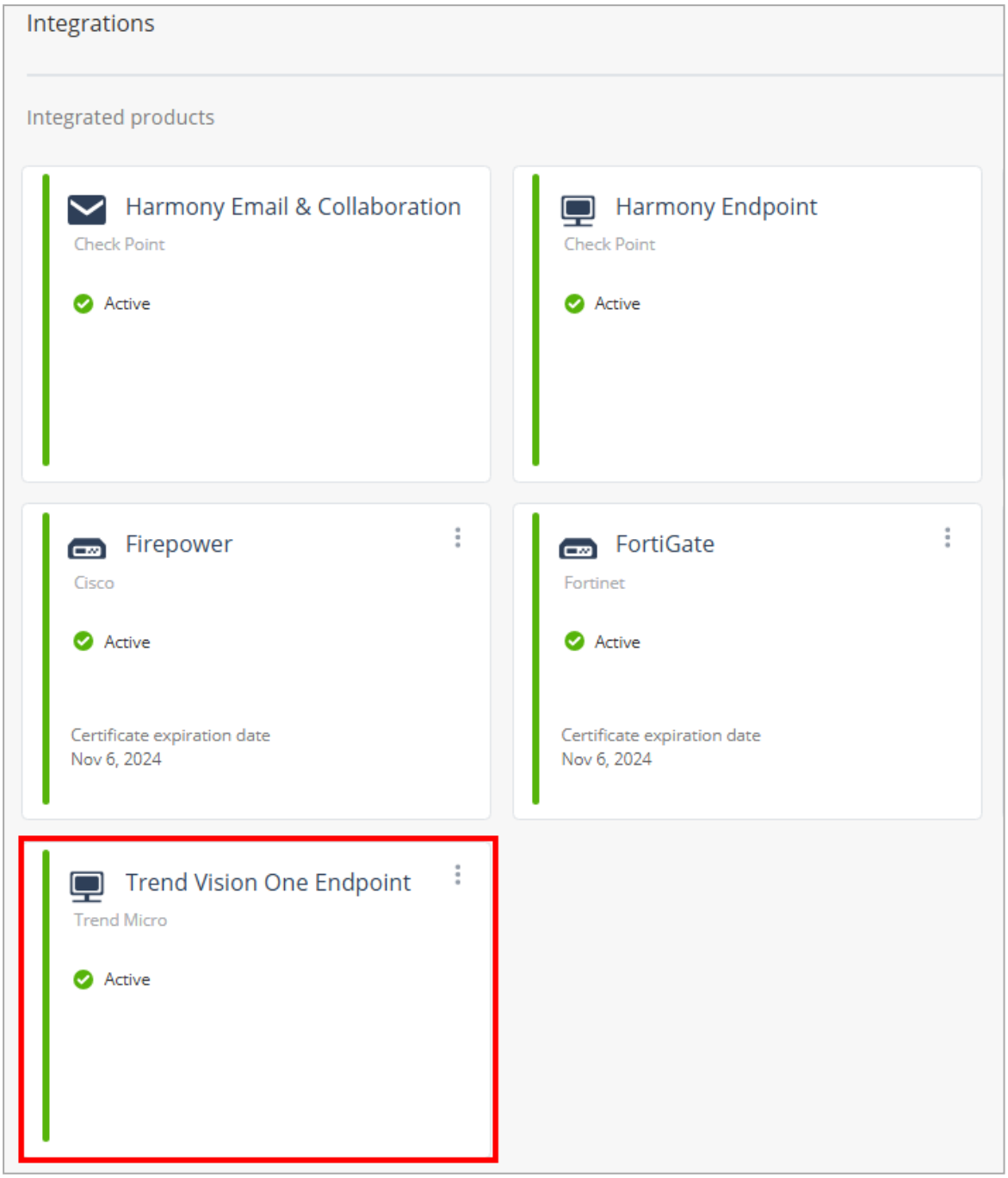
The **Trend Vision One** widget status changes to **Active**.



3. To check if the integration is successful, in the XDR Administrator Portal:

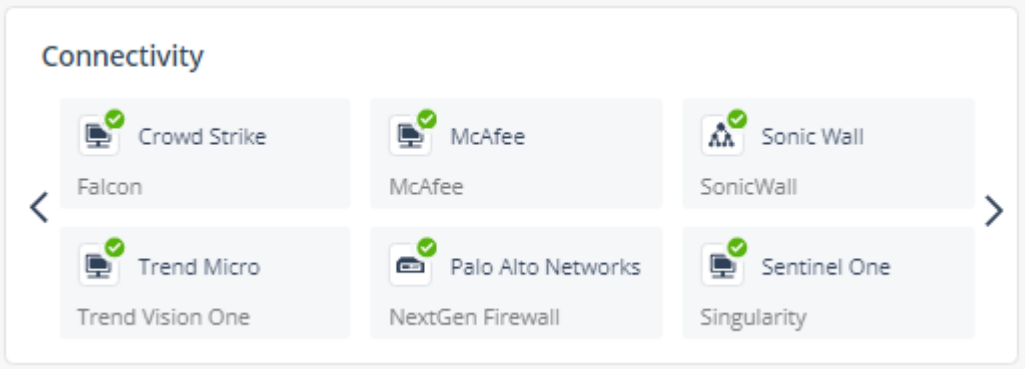
- Go to **Settings** > **Integrations**.

  In the **Integrated products** section, verify if **Trend Vision One Endpoint** is listed as **Active**.



Note - The widget will display **Inactive** status until XDR begins receiving logs from Trend Vision One Endpoint.

- Go to the **Overview** page and in the **Connectivity** widget, verify if **Trend Micro** is listed as connected.



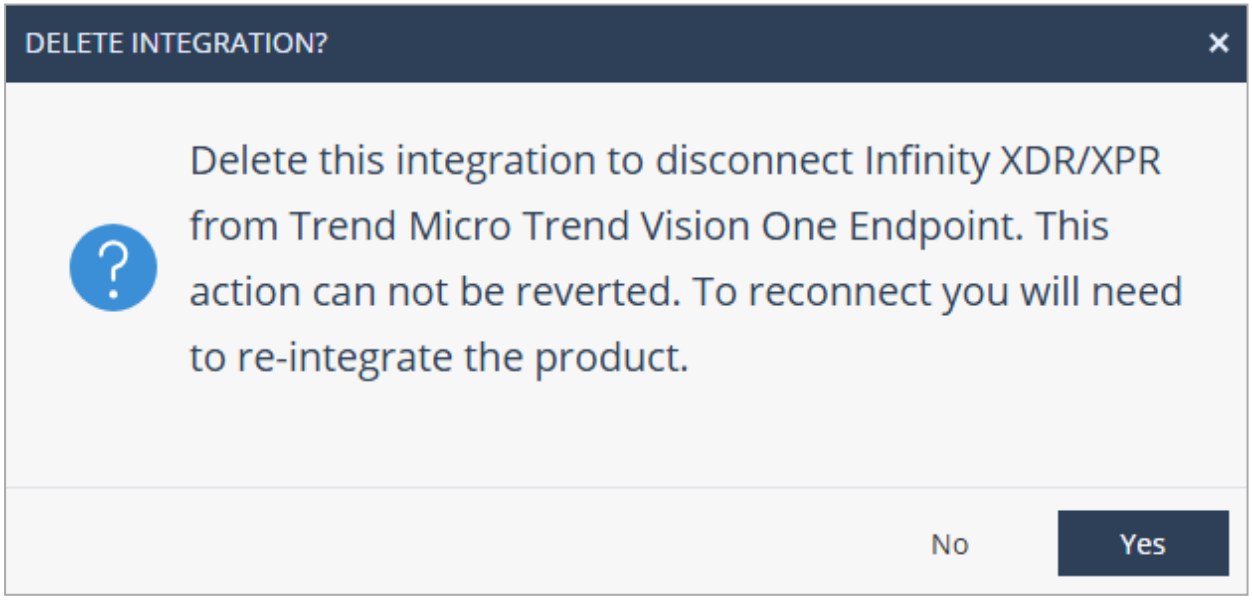
IOC Management

You can manage Indicators Of Compromise (IoCs) on Trend Vision One for Endpoint. You can import IoCs to it through different methods including CSV, OpenIOC, and STIX files. For more information, see Trend Micro documentation.

Deleting the Integration

1. Go to **Settings** > **Integrations**.
2. In the **Trend Vision One** widget, click ⋮.
3. Click **Delete**.

   The **Delete Integration** window appears.



4. Click **Yes**.

Supported Preventive Actions

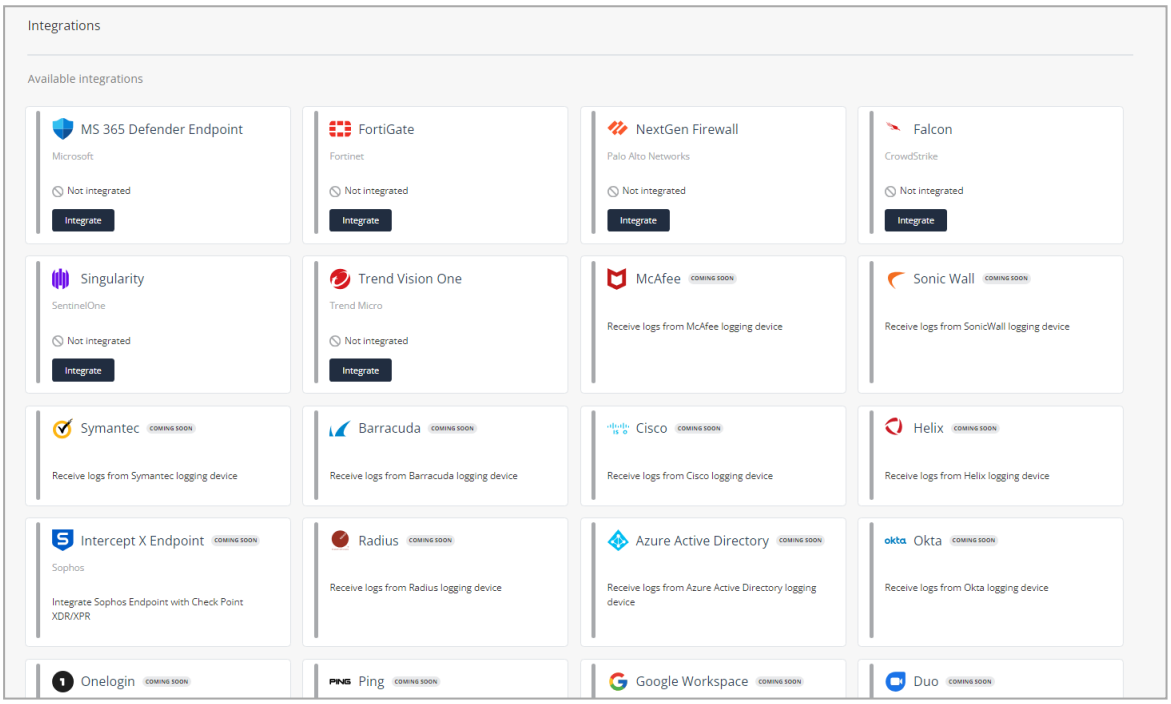
When XDR detects any malicious activity, it generates an incident and recommends preventive actions to mitigate it.The supported preventive action is to isolate a machine. For more information, see **Incidents Overview** > *"Prevention" on page 70*.

Cisco Firepower Threat Defense

Check Point XDR supports integration with Cisco Firepower Threat Defense (FTD) firewall by using syslog-ng (Log Management Solution) to collect its syslogs. XDR analyzes the syslogs for malicious activity and suggests preventive actions, which you must manually enforce on the firewall.

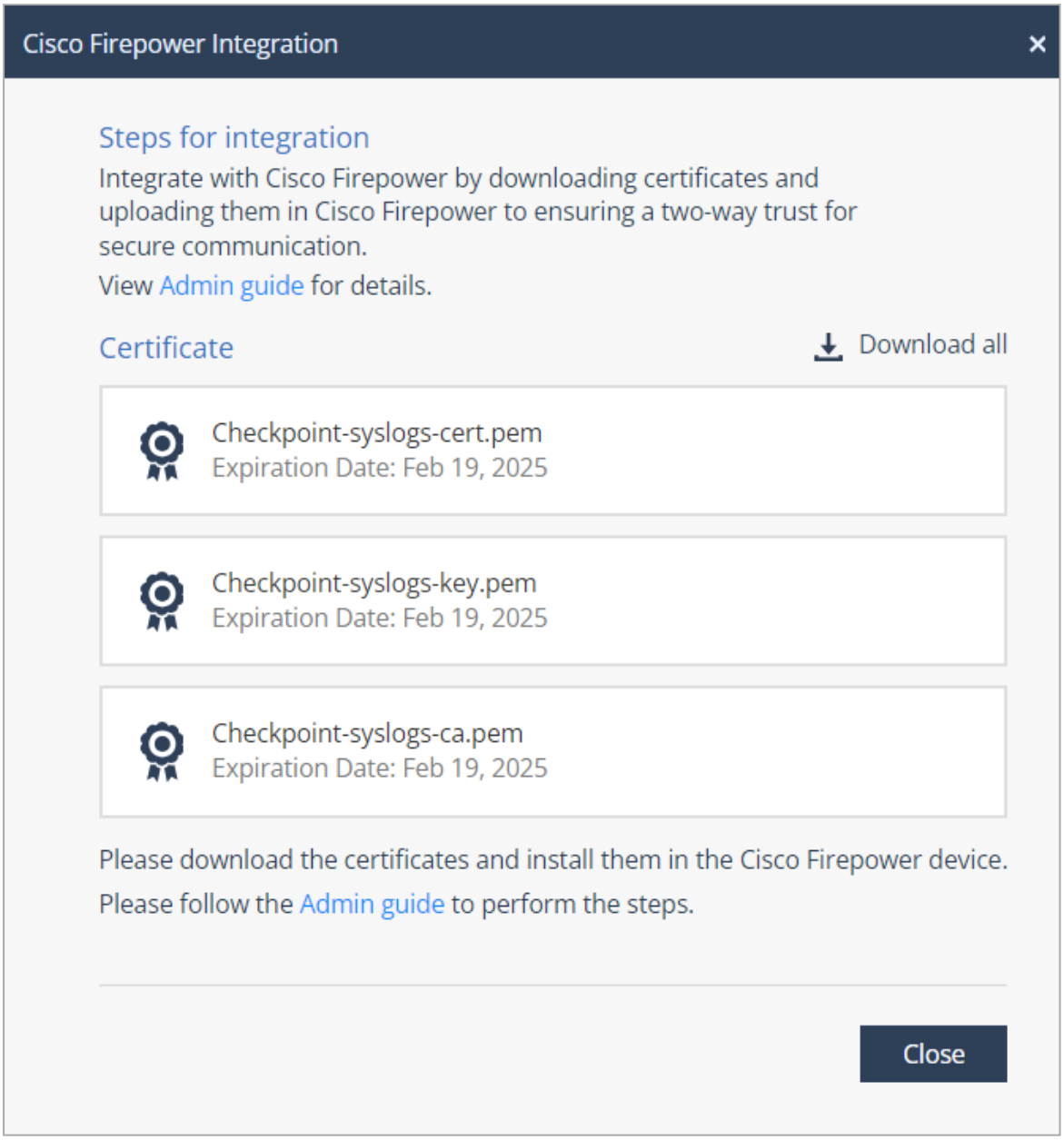
Integrating Cisco Firepower

1. Log in to the XDR Administrator Portal:
    a. Go to **Settings** > **Integrations**.



b. In the **Cisco** widget, click **Integrate**.

The **Cisco Firepower Integration** window appears.



c. Click **Download all** to download the zip file that includes these certificates:

- *checkpoint-syslogs-cert.pem*
- *checkpoint-syslogs-key.pem*
- *checkpoint-syslogs-ca.pem*

d. Click **Close**.

The **Cisco Firepower** widget status changes to **Active**.

2. To install syslog-ng on your internal machine:

a. Depending on the Operating System, use the appropriate package manager to install syslog-ng. For Ubuntu or Debian systems:

i. To update the list of available packages, run:

```
sudo apt-get update
```

ii. To install syslog-ng and any of its subpackage, run:

```
sudo apt-get install syslog-ng
```

b. To create a directory to store your TLS certificates, run:

```
sudo mkdir -p /etc/syslog-ng/cer
```

c. Unzip the zip file downloaded in step **1.c** and copy the *.pem* files to `/etc/syslog-ng/cer` in your internal machine.

Note - You can use Secure Copy Protocol (SCP) or any secure method to transfer these files.

d. To set permissions for certificate files to ensure that they are secure and accessible only by syslog-ng, run:

```
sudo chmod 600 /etc/syslog-ng/cer/*
```

e. Navigate to `/etc/syslog-ng/syslog-ng.conf`, open the **syslog-ng.conf** file in a text editor and paste this configuration:

```
@version:XXX
source s_cisco {
network(
transport("udp")
port(514)
);
};

log {
source(s_cisco);
destination(d_remote_syslog);
};

destination d_remote_syslog {
syslog(
"20.4.164.135" transport("tls")
port(6514)
tls(
key-file("/etc/syslog-ng/cer/checkpoint-syslogs-key.pem")
cert-file("/etc/syslog-ng/cer/checkpoint-syslogs-cert.pem")
ca-file("/etc/syslog-ng/cer/checkpoint-syslogs-ca.pem")
peer-verify("required-trusted")
)
);
};
```

To find the current version, run `syslog-ng --version` and search for the current version installed on your machine. Note that this is tested and working on v4.3.

f. Replace the IP address **20.4.164.135** with the appropriate IP address for your region:

Region	IP Address
EU	20.76.50.141
US	20.22.126.247
India	4.187.145.23
UAE	20.174.45.149

g. Save the changes and exit the text editor.

h. Restart the syslog-ng service to apply the changes:

```
sudo systemctl restart syslog-ng
```

i. To check the syslog-ng service status, run this:

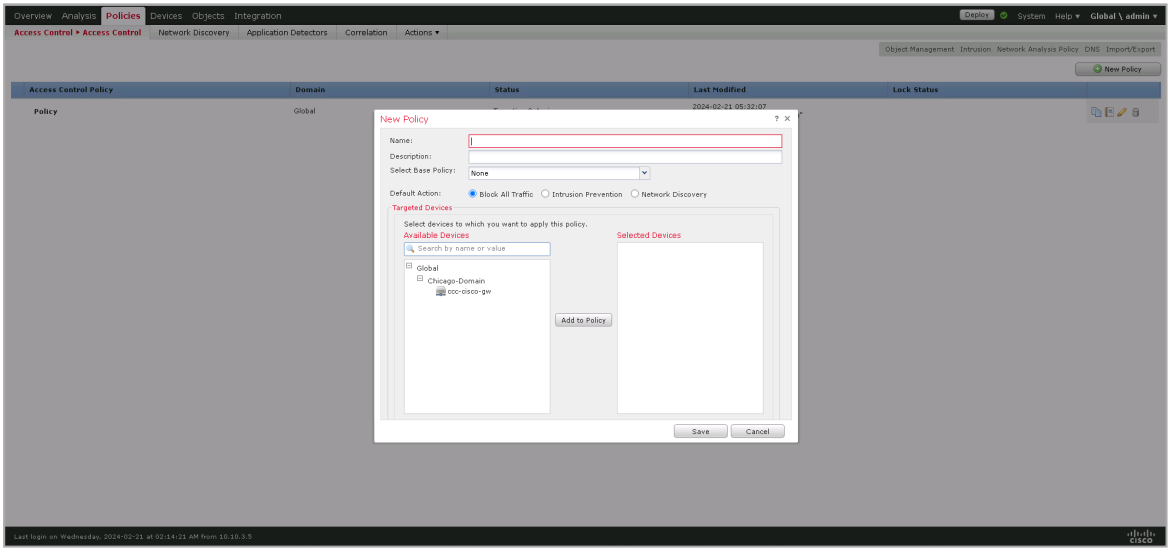
```
sudo systemctl status syslog-ng
```

3. Log in to your Cisco Firepower Management Center (FMC) portal:

a. Go to **Devices** > **Platform Settings**.

b. To create a new Firepower Threat Defense (FTD) policy, click **New Policy** and select the **Threat Defense Settings** device type. If you already have a policy, in the policy table, scroll to the end of the row and click  to edit the policy.

The **New Policy** window appears.



c. Enter **Name** and **Description**.

d. In the **Targeted Devices** section, in the **Available Devices** search field, search for the FTD appliance to which you want to apply this policy.

e. Click **Add to Policy**.

f. Click **Save**.

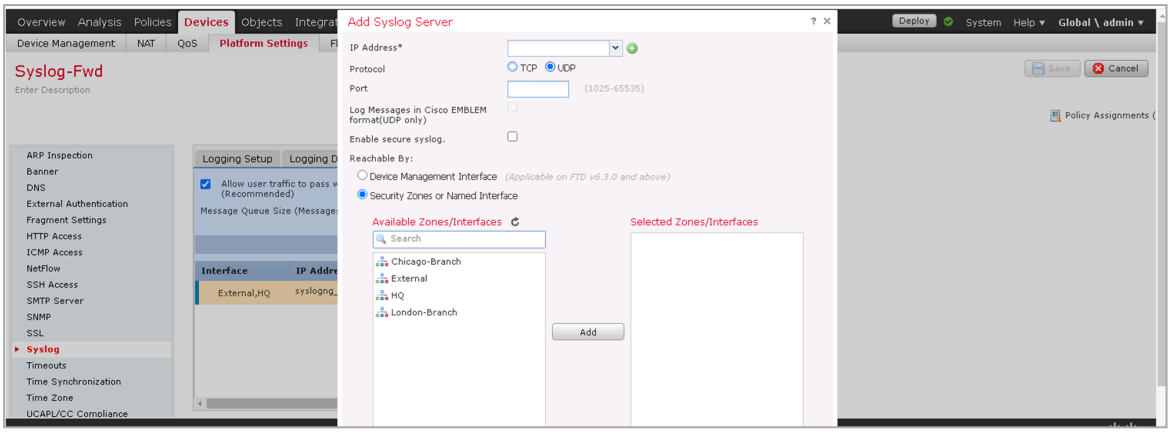
The system creates the policy.

g. Click  .

h. Go to **Syslog** and click the **Syslog Servers** tab.

i. To add remote syslog servers, click **Add**.

The **Add Syslog Server** window appears.



j. From the **IP Address** list, select the network object that has the syslog-ng server installed in step **2.a**. If you have not created a network object, click  to create a new object.

k. In the **Protocol** field, select **UDP**.

l. In the **Port** field, enter **514**.

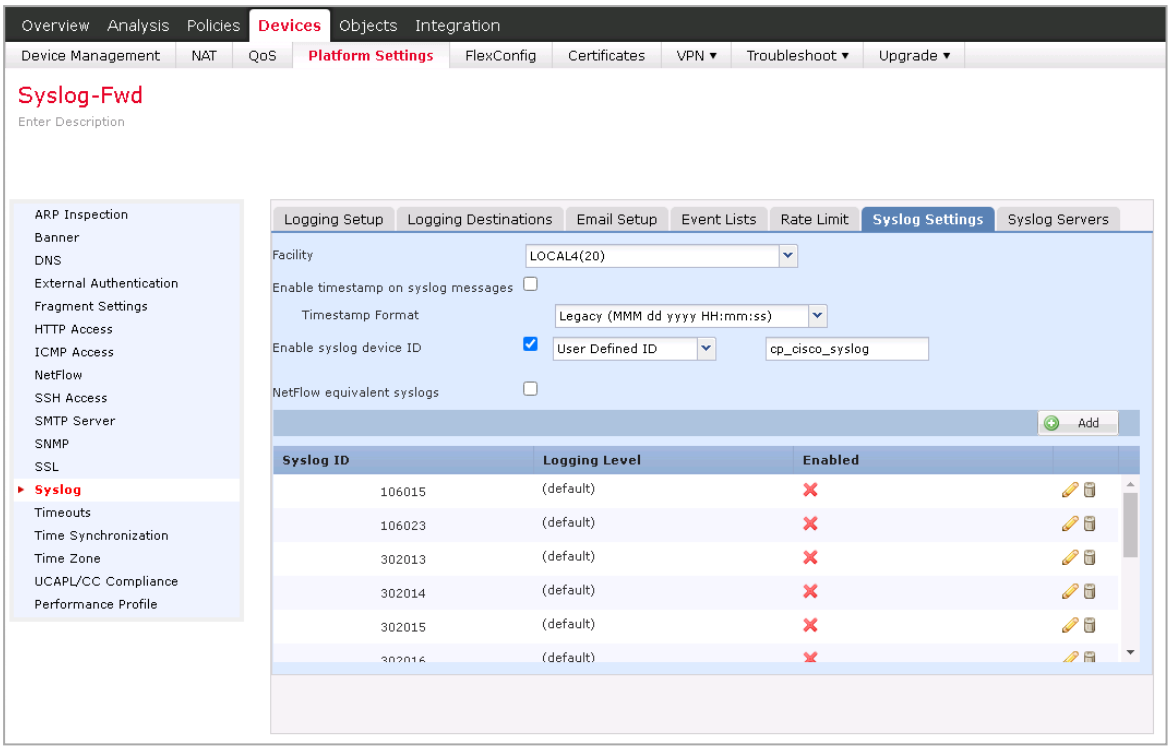
m. Make sure that the **Enable secure syslog** checkbox is not selected.

n. In the **Available Zones/Interfaces** search field, search for the security zones over which the syslog server is reachable.

o. Click **Add** and then click **OK**.

p. Click the **Syslog Settings** tab.

q. Select the **Enable syslog device ID** checkbox.

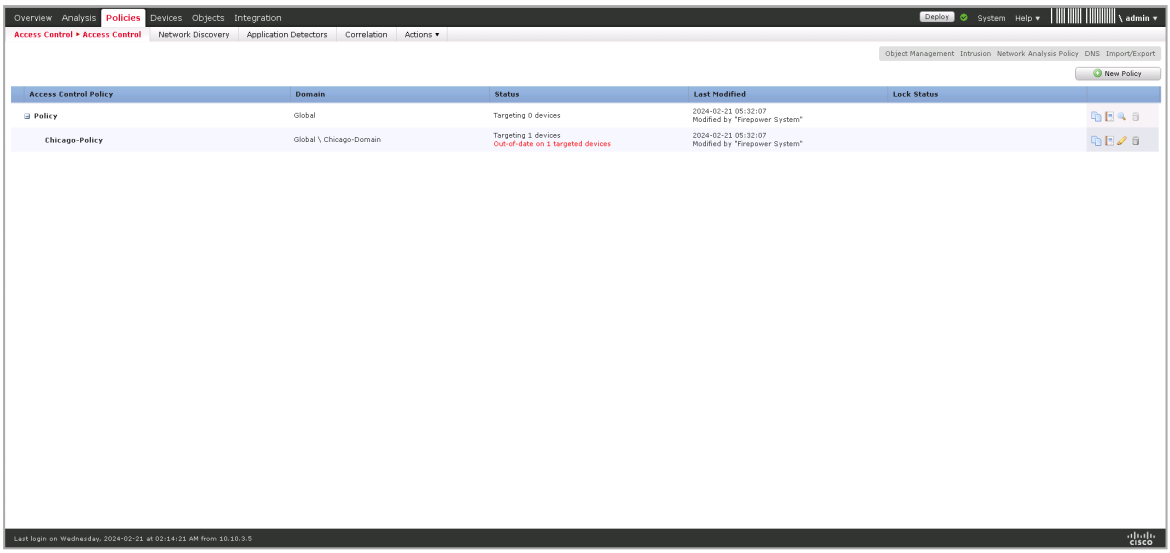


r. From the list, select **User Defined ID** and enter **cp_cisco_syslog**.

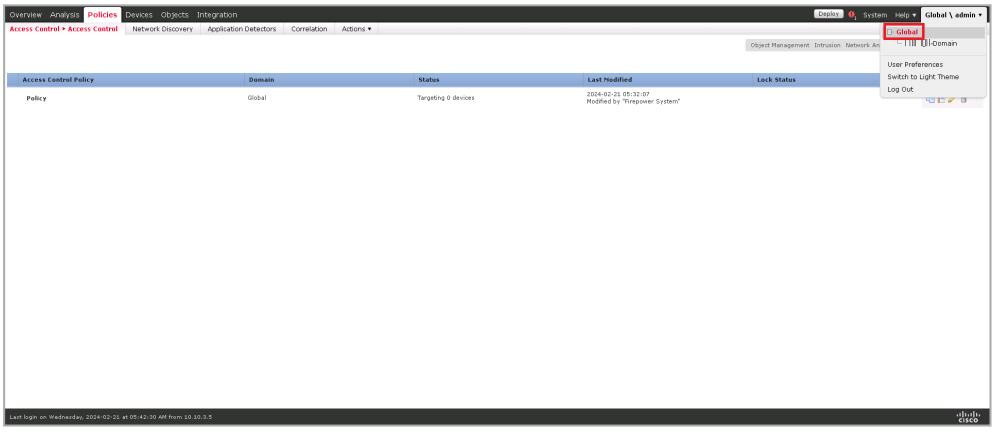
s. Click **Save** to save the configuration.

t. Click **Save** and then click **Deploy** to start deployment of the platform setting.

u. Go to **Policies** > **Access Control** > **Access Control**.

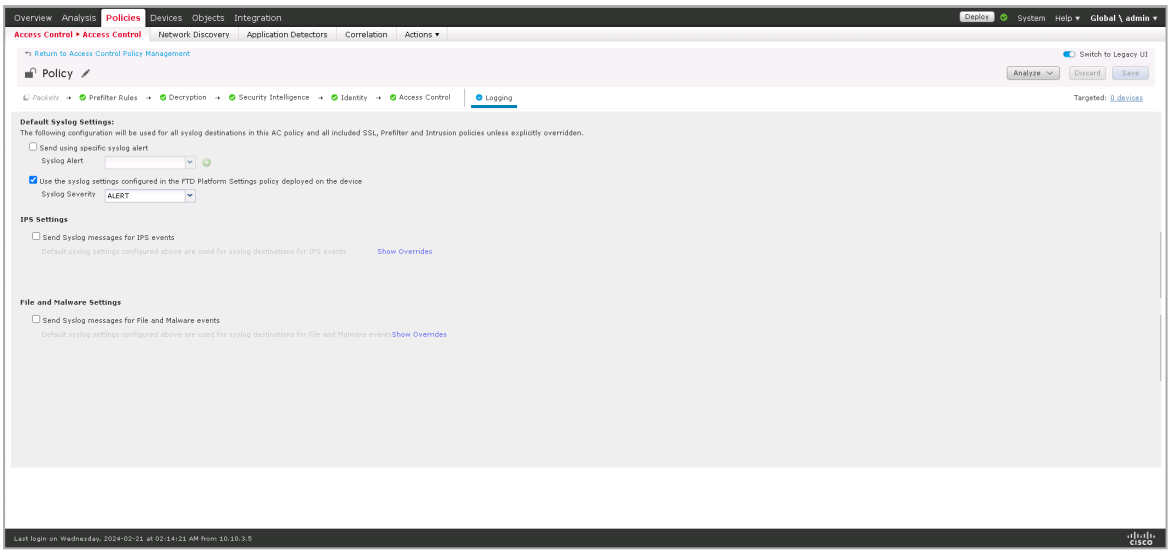


Note - Make sure that you have logged in under **Global** configurations.



v. In the policy table, scroll to the end of the row and click  .

w. Click the **Logging** tab.



Note - Make sure that:

- Cisco Firepower logs include the `SrcIP` and `DstIP` fields.
- Source IP and destination IP are not the same.

x. Select the **Use the syslog settings configured in the FTD Platform Settings policy deployed on the device Syslog Severity** checkbox.

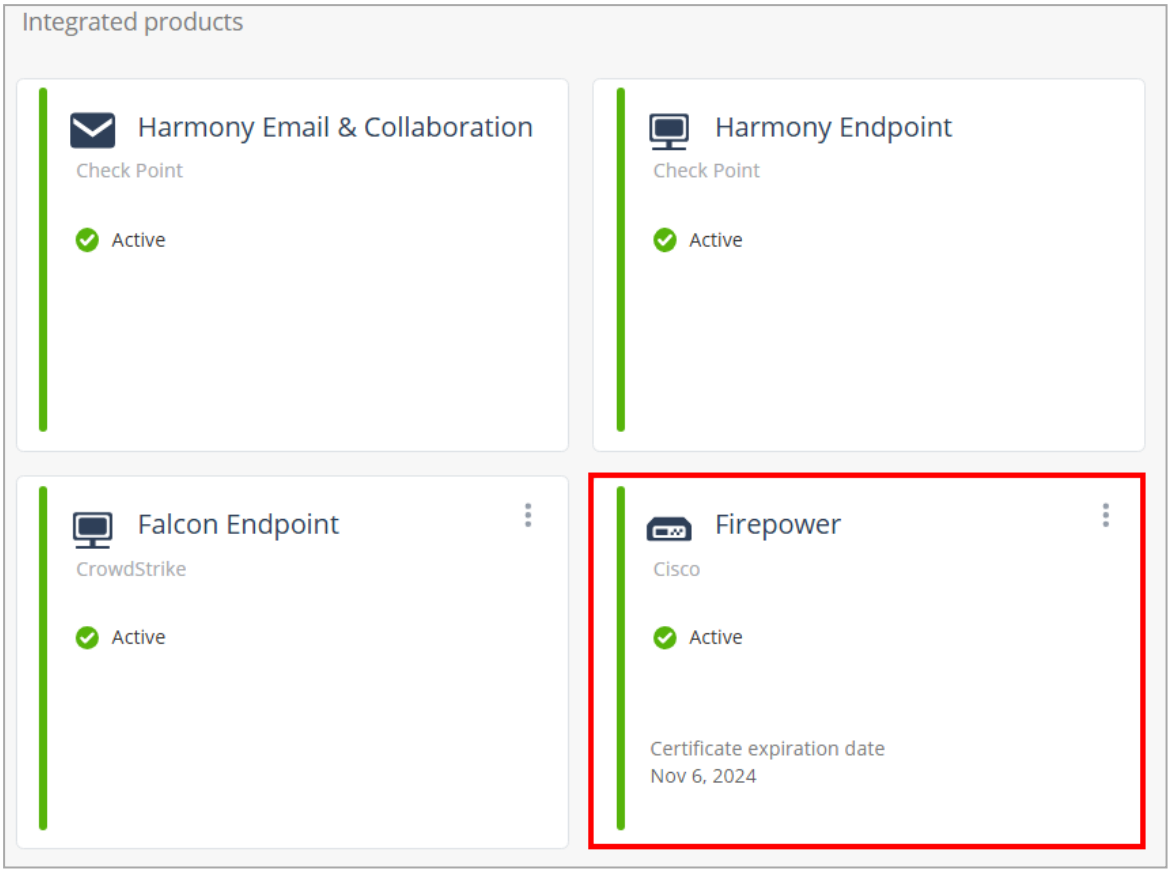
y. From the list, select **ALERT**.

z. Click **Save** and then click **Deploy**.

4. To check if the integration is successful, in the XDR Administrator Portal:

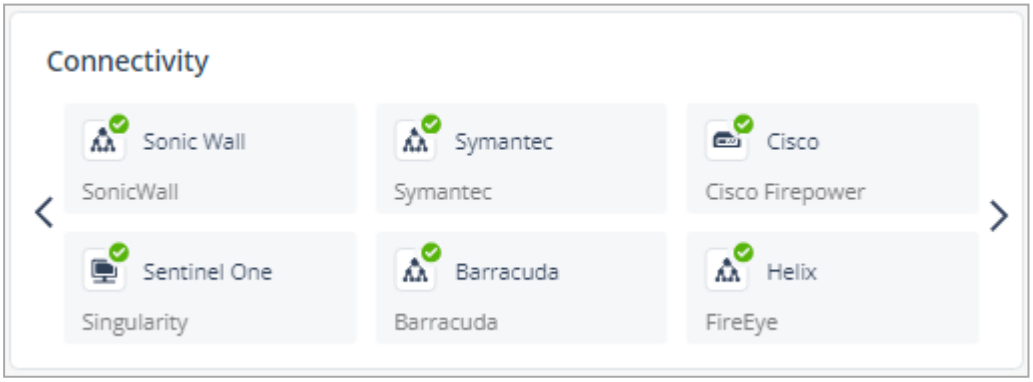
- Go to **Settings** > **Integrations**.

  In the **Integrated products** section, verify if Cisco is listed as **Active**.



Note - The widget will display **Inactive** status until XDR begins receiving logs from Cisco Firepower.

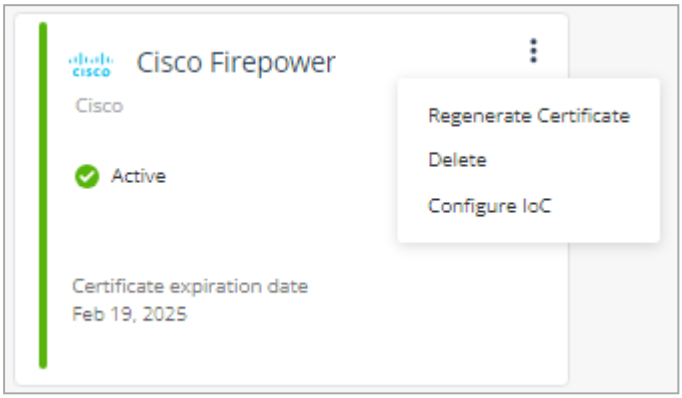
- Go to the **Overview** page and in the **Connectivity** widget, verify if **Cisco** is listed as connected.



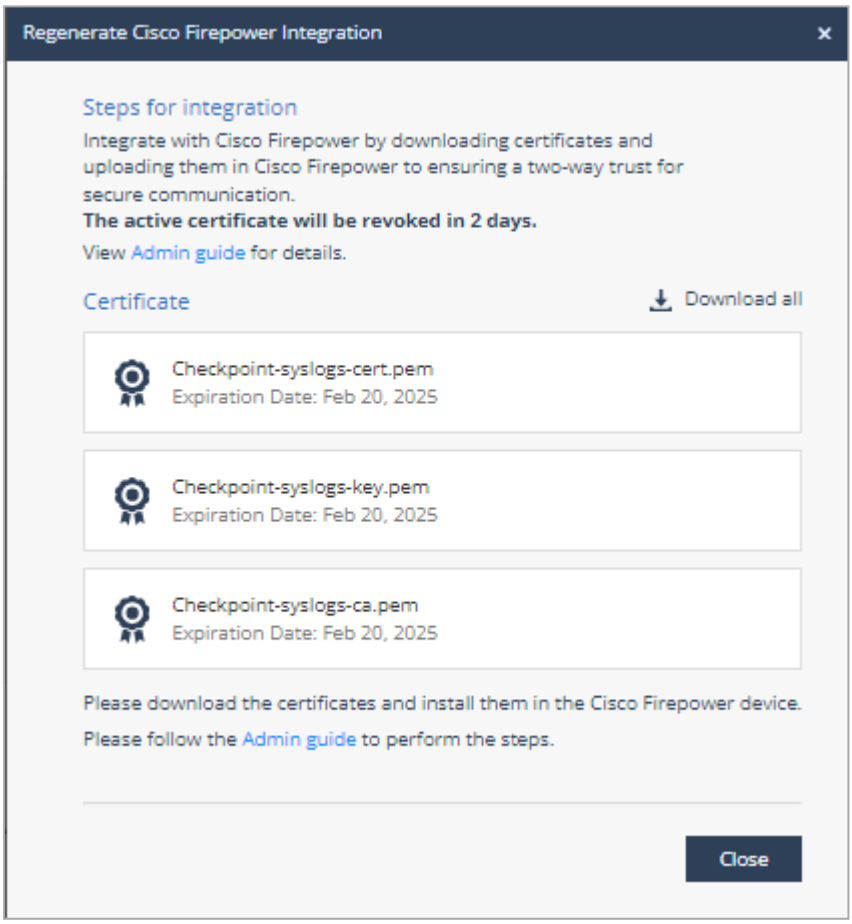
Regenerating the Certificate

If you revoke a certificate, you must regenerate and upload the certificate to the Cisco Firepower Management Center portal within two days.

1. Log in to the XDR Administrator Portal:
   a. Go to **Settings** > **Integrations**.
   b. In the **Cisco Firepower** widget, click ⋮.
   c. Click **Regenerate Certificate**.



The **Regenerate Cisco Firepower Integration** window appears.



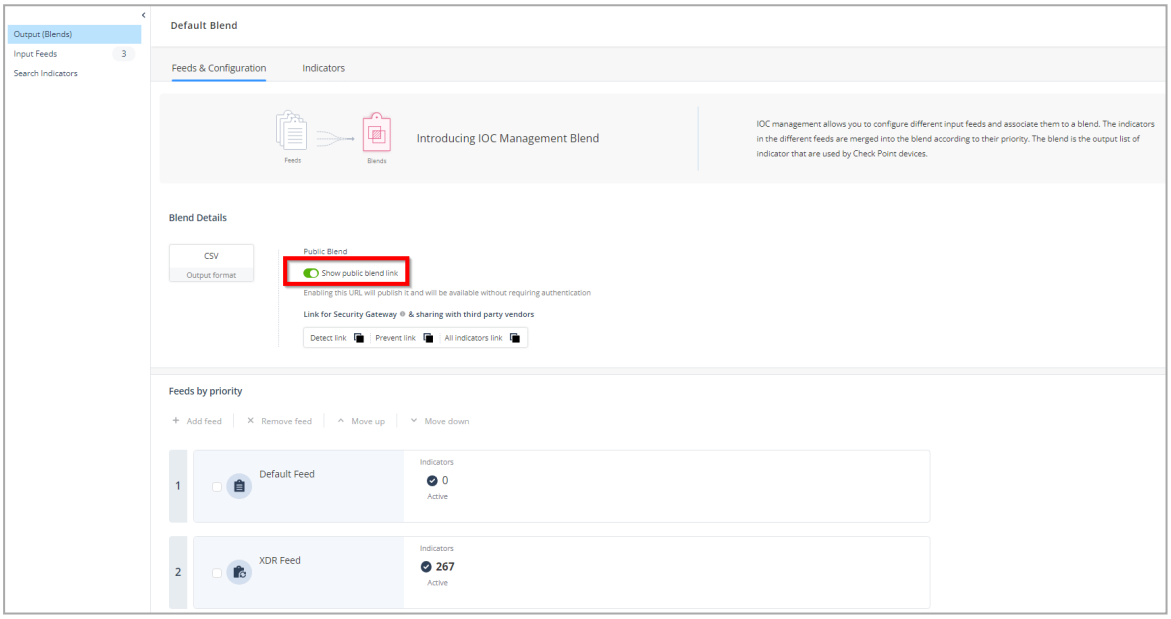
   d. Perform steps from **1.c** until the end in Integrating the Cisco Firepower.

Configuring IoCs

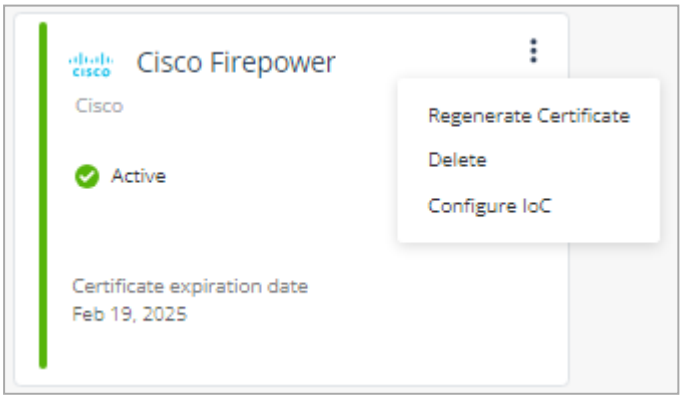
You can use the **Public Blend URL** in the IoC Management to enforce IoCs on the Cisco Firepower Management Center.

To configure IoCs:

1. Log in to the XDR Administrator Portal:
   a. Go to **New IOC Management** > **Output (Blends)** > **Feeds & Configuration**.
   b. Turn on the **Show public blend link** toggle button.

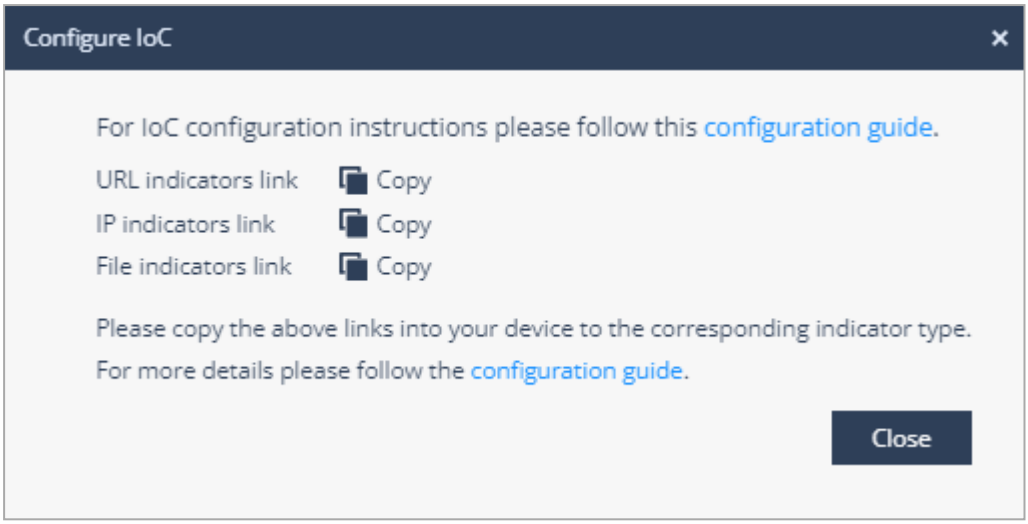


   c. Go to **Settings** > **Integrations**.
   d. In the **Cisco Firepower** widget, click ⋮ and select **Configure IoC**.



The **Configure IoC** window appears. It lists three indicator links generated automatically using the **All Indicators link** from the **Public Blend URL** in the IoC Management.

e. Click  to copy the indicators link.

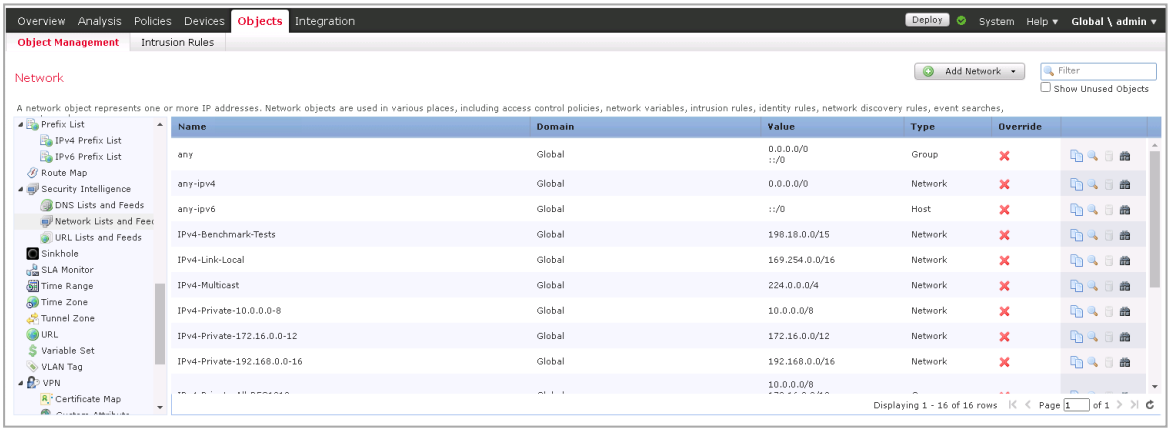


f. Click **Close**.

2. Log in to the Firepower Management Center (FMC) portal:

   a. Go to **Objects** > **Object Management** > **Security Intelligence**.

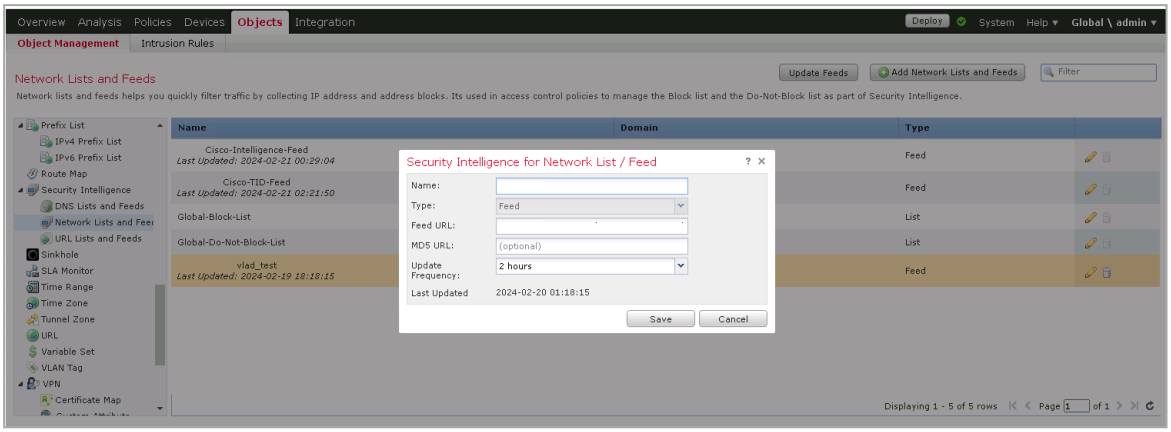
   b. Select **Network Lists and Feeds**.



The **Network Lists and Feeds** window appears.

c. Click **Add Network Lists and Feeds**.

The **Security Intelligence for Network List / Feed** window appears.



d. In the **Name** field, enter a name for the feed

e. In the **Feed URL** field, paste the **IP indicators link** copied in the step **1.e**

f. From the **Update Frequency** list, select **2 hours**.

g. Click **Save**.

h. Click **Save** and then click **Deploy**.

i. Repeat steps **2.b** through **2.e** with this detail:

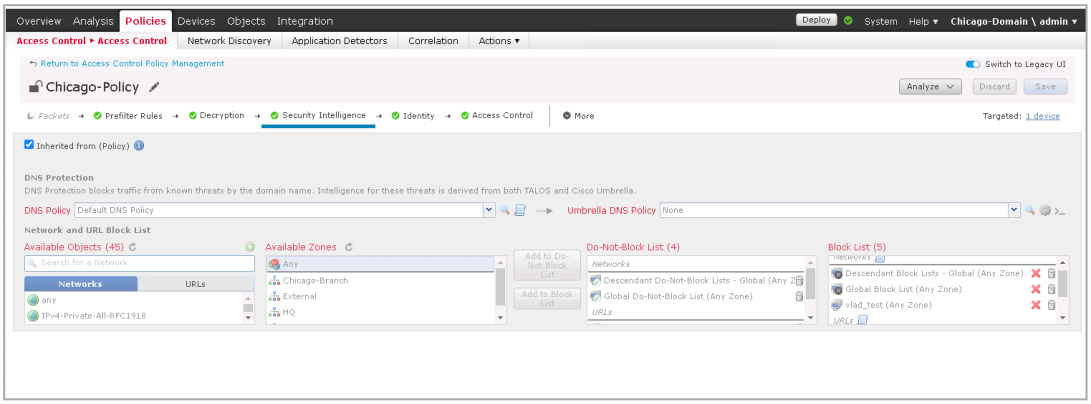
Security Intelligence	Feed URL
URL Lists and Feeds	**URL indicators link** (Configure IoC link from step 1.e)

j. Once the feed is configured and validated, deploy it on your FTD devices:

   i. Go to **Policies** > **Access Control Policies**.

   ii. Select the policy to which you want to add the feed.

   iii. Click **Security Intelligence**.



   iv. From the **Available Objects** search field, search and select your newly created feed.

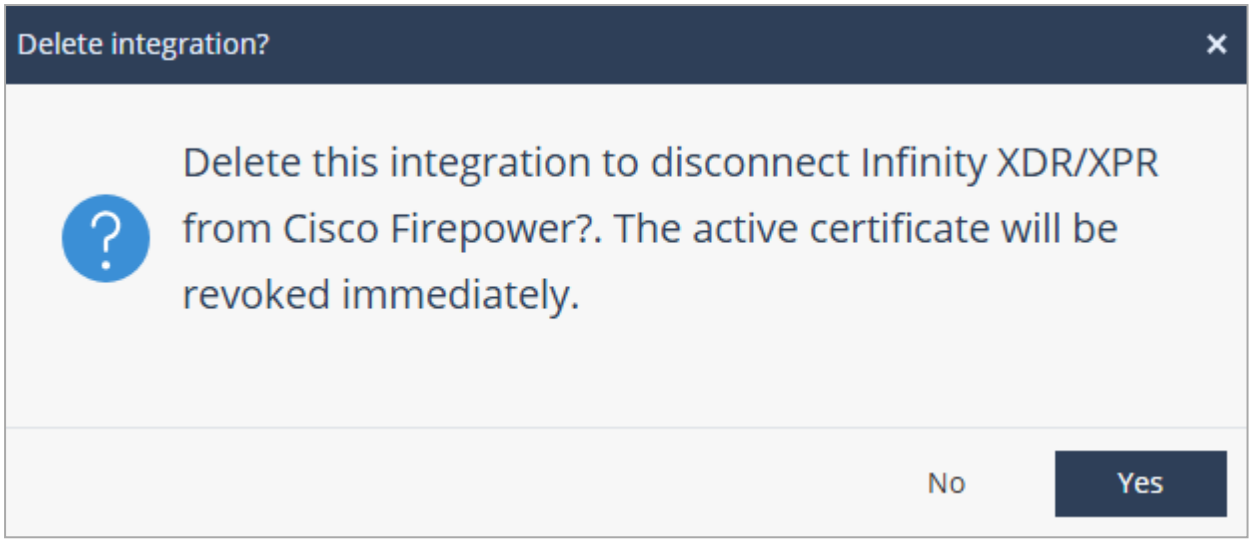
   v. Click **Save**.

   vi. Click **Save** and then click **Deploy**.

Deleting the Integration

1. Go to **Settings** > **Integrations**.
2. In the **Cisco Firepower** widget, click ⋮.
3. Click **Delete**.

   The **Delete Integration** window appears.


Delete integration?
Delete this integration to disconnect Infinity XDR/XPR from Cisco Firepower?. The active certificate will be revoked immediately.
No
Yes

4. Click **Yes**.

Microsoft Entra ID

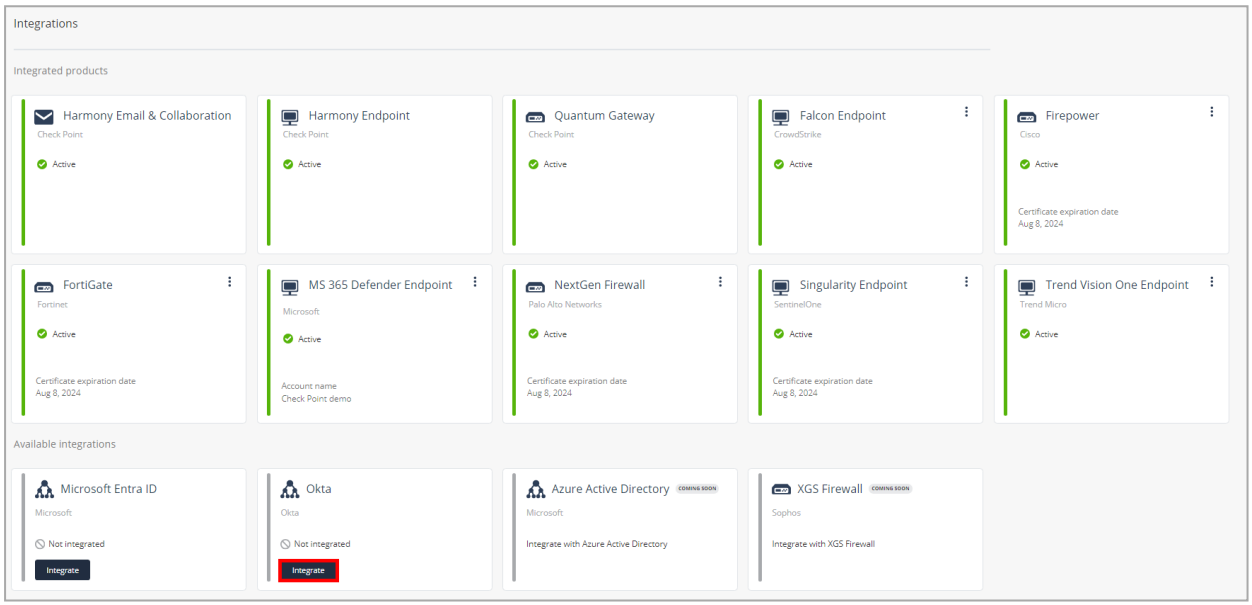
Microsoft Entra ID integration has been deprecated and is no longer supported in Check Point XDR.

Okta

Check Point XDR analyzes the Check Point Identity Next logs from Okta for malicious or abnormal activity, generates an incident and suggests preventive actions.

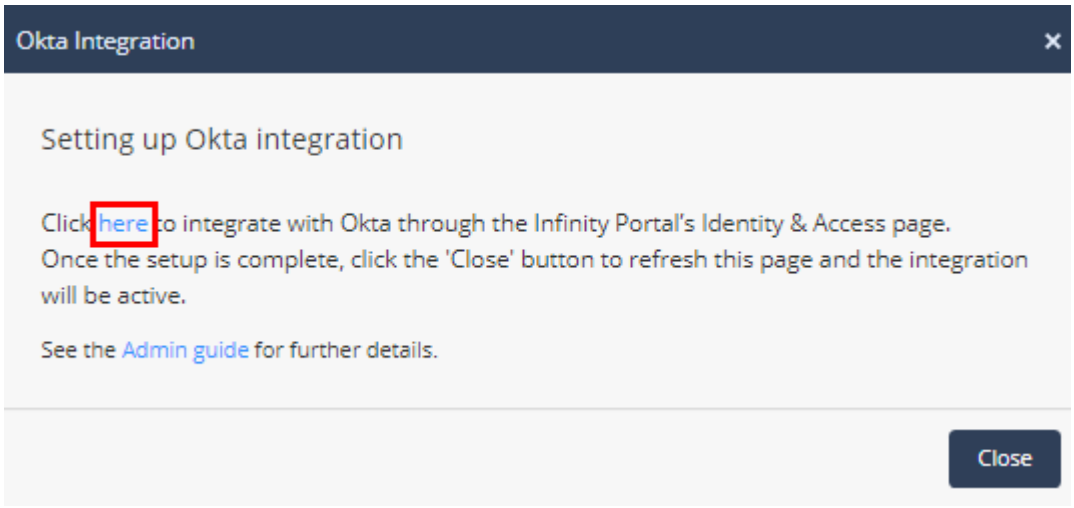
Integrating Okta

1. Access the XDR Administrator Portal:
2. Go to **Settings** > **Integrations**.
3. In the **Available integrations** section, in the **Okta** widget, click **Integrate**.

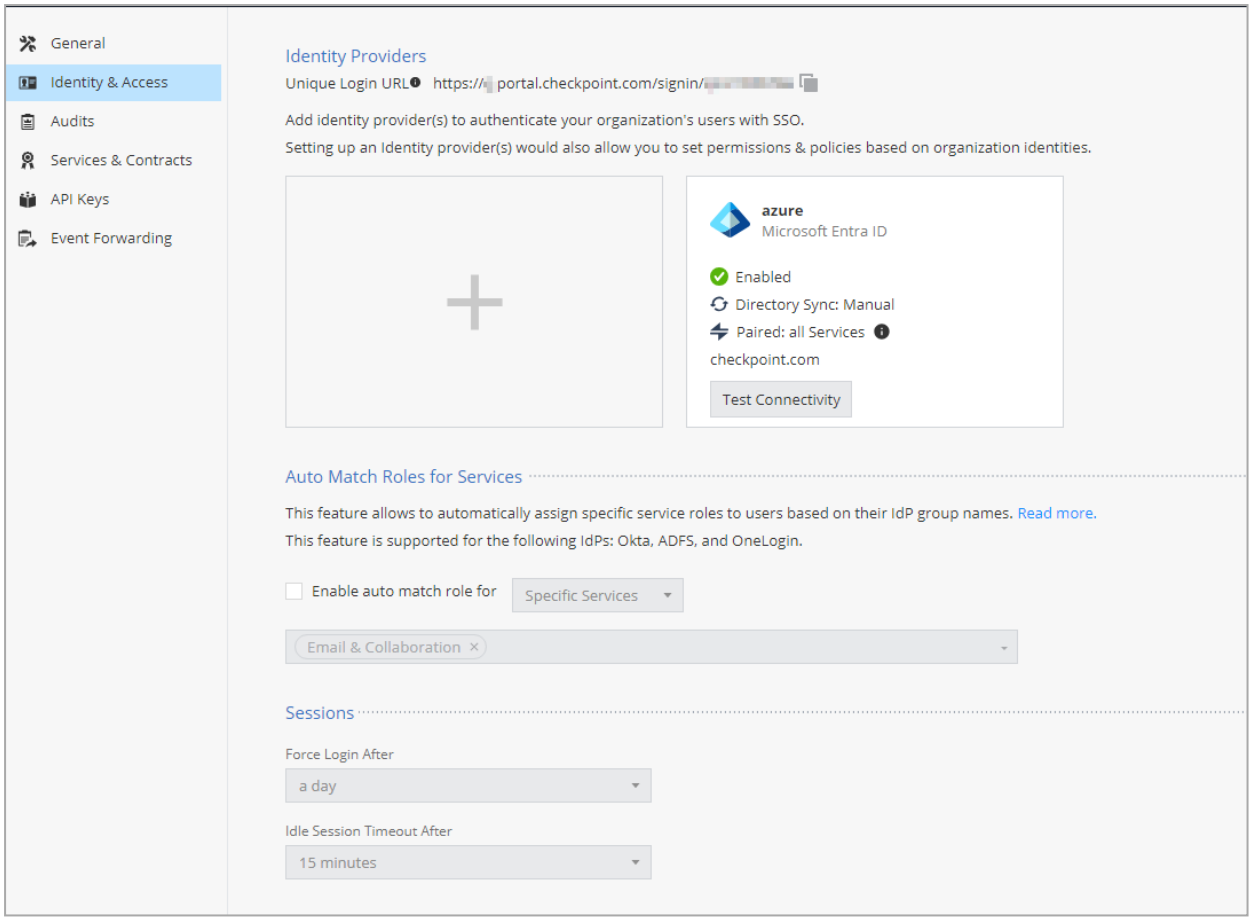


The **Okta Integration** window appears.

4. Click the link to integrate Okta with Check Point Check Point Portal.



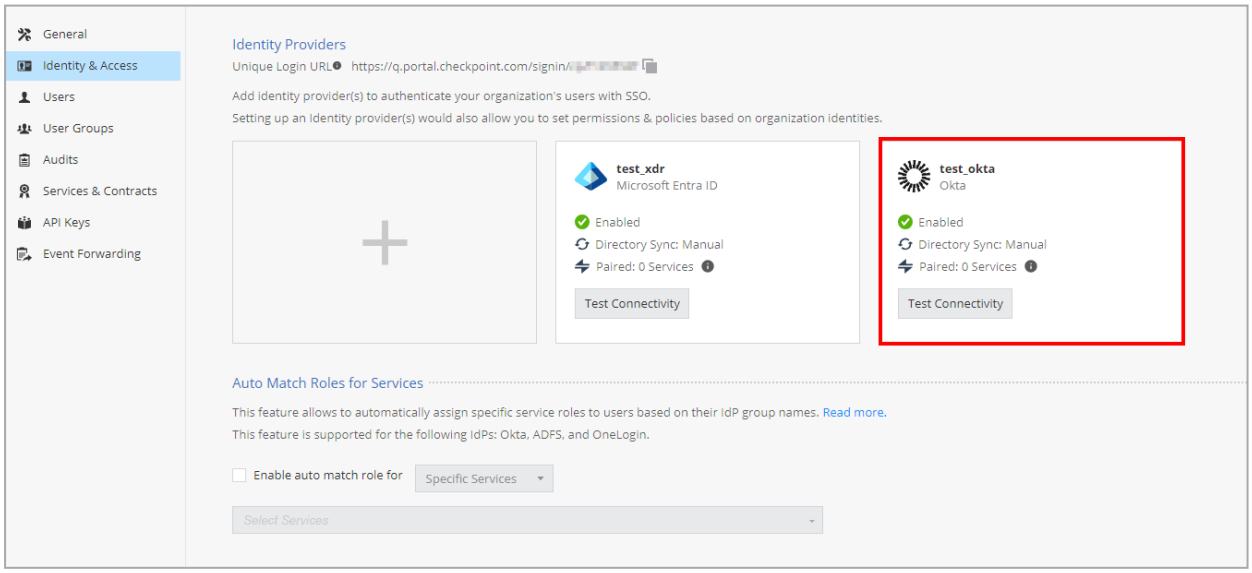
The **Identity & Access** page in the Check Point Portal appears.



5. Set up the Okta integration with Check Point Portal. For instructions, see SSO authentication with Okta.

   After the integration is completed, permissions to reset passwords are granted by default.

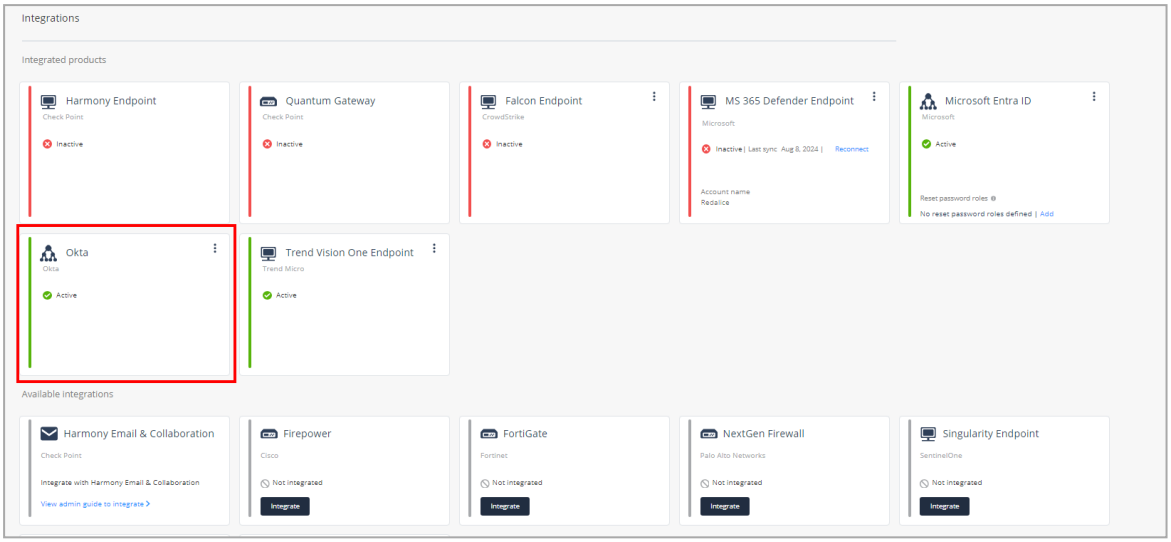
   The system displays the Okta integration card in the **Identity & Access** page.



6. To check if the integration is successful, in the XDR Administrator Portal:

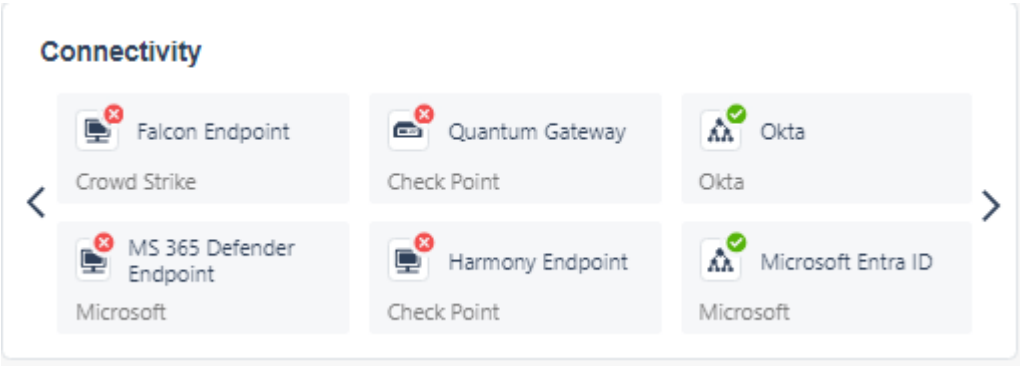
- Go to **Settings** > **Integrations**.

  In the **Integrated products** section, verify if Okta is listed as **Active**.



Note - The widget will display **Inactive** status until XDR begins receiving logs from Okta.

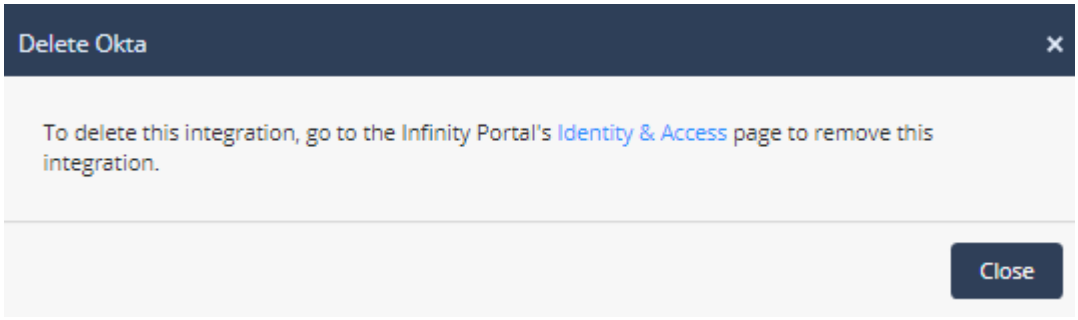
- Go to the **Overview** page and in the **Connectivity** widget, verify if Okta is listed as connected.



Deleting the Integration

1. Go to **Settings** > **Integrations**.
2. In the **Okta** widget, click the ⋮ icon and then click **Delete integration**.

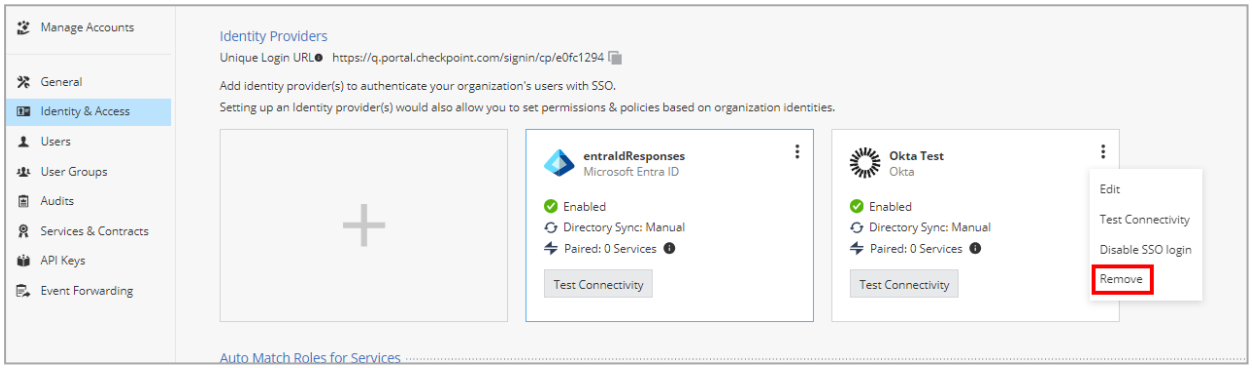
   The **Delete Okta** window appears.



3. Click the **Identity & Access** link.

   The **Identity & Access** page appears.

4. On the Okta integration card, click the ⋮ icon and then click **Remove**.



Supported Preventive Actions

When XDR detects malicious activity that involves Okta IDP, it generates an incident and recommends preventive actions to mitigate it.

The supported preventive actions include resetting the user's Okta password and revoking the session through Okta.

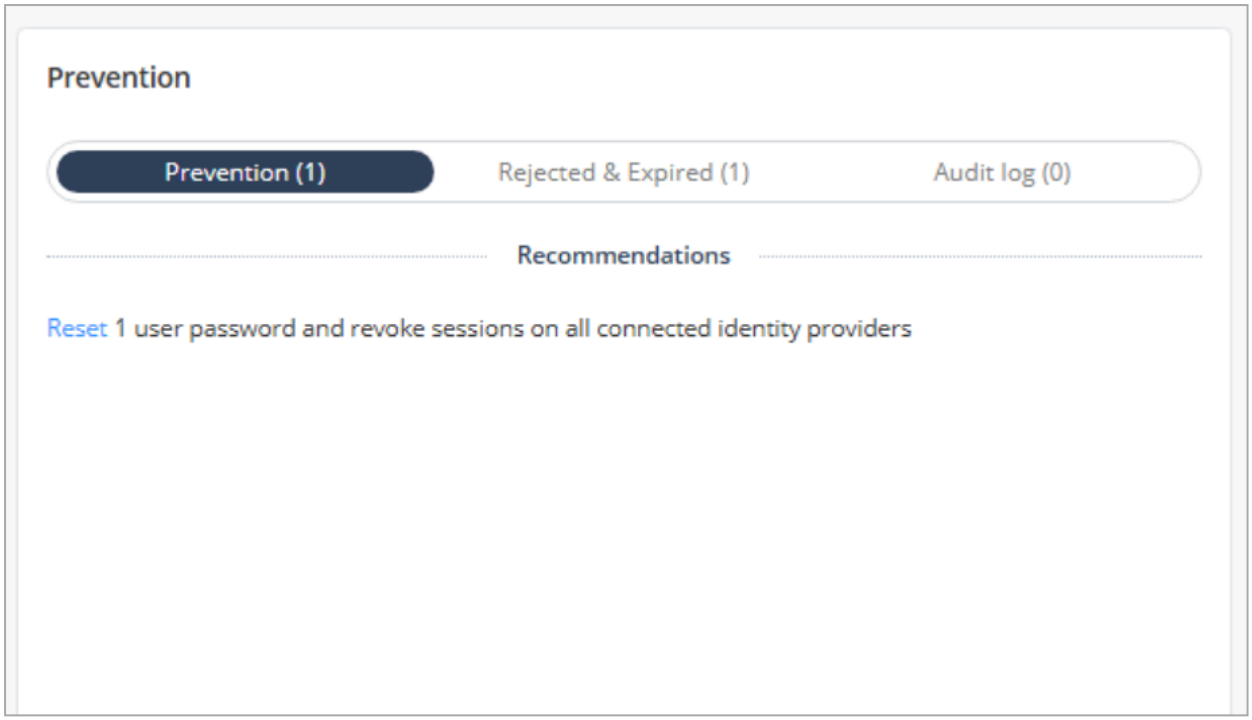
Important - You cannot revert the reset password action.

To view the recommended preventive actions for the incident:

1. Go to **Incidents** page and click the incident title or hover over the incident and click **>**.
2. In the incident **Overview** page, go to **Prevention** widget.

   The system shows the recommended preventive actions in the **Recommendations** section.

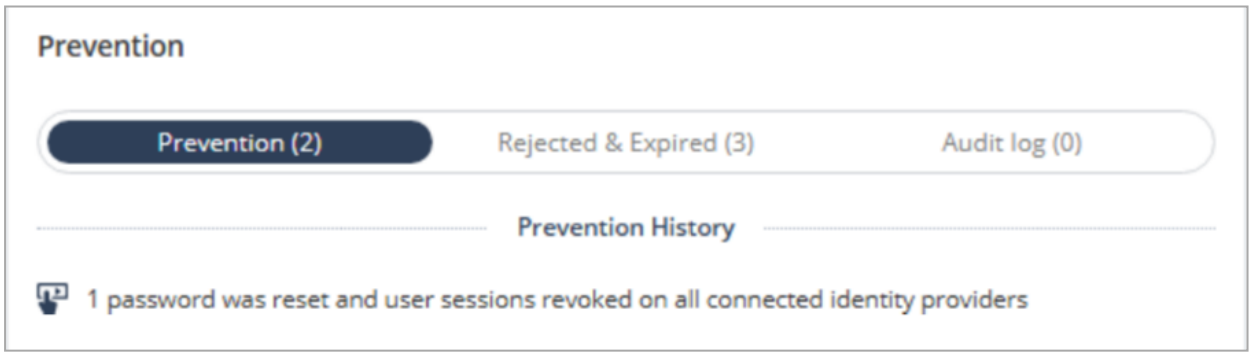
3. To reset the user password, click **Reset**.



Note - To ensure security, XDR resets password for all the connected identity providers integrated through Identity Next.

Once the password is reset, the end-user receives an email notification to reset the Okta password.

4. To view the preventive action taken, see the **Prevention History** section.



For more information, see **IncidentsOverview** > *"Prevention" on page 70*.

Log Processing

The Check Point XDR license provides an entitlement for analyzing and processing data from your subscribed products, based on data volume in gigabytes (GB). The **Log processing** page shows the currently processed data volume and this information is used to compare the data utilization to the entitlement.

You can also define Processing Exceptions, that exclude the data from selected products or Quantum devices from being processed by XDR. The system will not generate any incidents based on the data from the excluded items. These exceptions reduce the processed data volume. The log processing data volume displayed is the volume after considering the active processing exceptions during the display period.

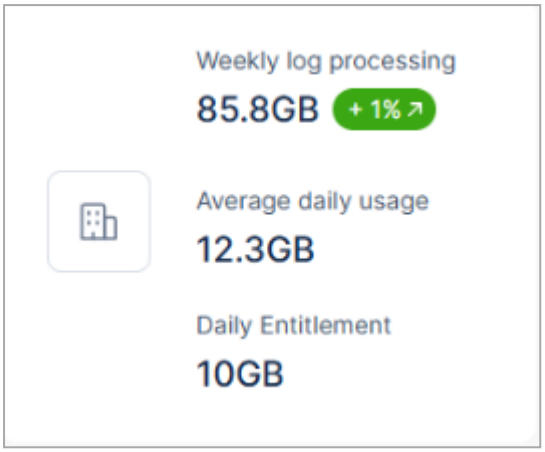
The **Log processing** page:

- Shows the total volume of logs processed in the designated time interval assuming the currently active processing exceptions. It also calculates the average data utilization to compare with the actual entitlement.
- Compares the data utilization across the different product types and Quantum devices that provide data.
- Allows you to assess potential changes to data utilization when specific products or Quantum devices are excluded from being processed by XDR, to optimize your data usage. After assessment, you can exclude their data from processing.

Note - The **Log processing** page displays the calculated data utilization with a two-day time delay.

To view the **Log processing** page, access the XDR Administrator Portal and go to **Settings** > **Log processing**.

Weekly Log Processing

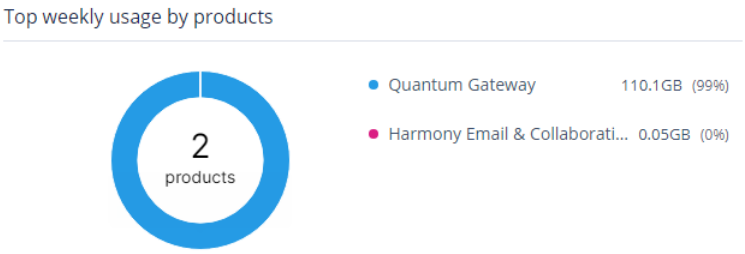


The **Weekly log processing** widget shows:

- **Weekly log processing** - Volume of logs processed in the previous week and comparison with the usage from the week before.
- **Average daily usage** - Average volume of logs processed in a day.
- **Daily Entitlement** - The maximum volume of logs entitled to be processed in a day.

Note - Average daily utilization from the previous week is used to ensure that both weekdays and weekends are included.

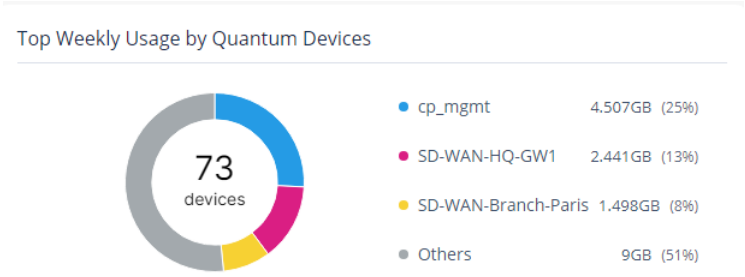
Top Weekly Usage by Products



The **Top weekly usage by products** widget shows the data utilized by products in the previous week. The system shows the top three product names and the rest are shown as **Others**.

Top Weekly Usage by Quantum Devices

Note - The widget shows data only if you have subscribed to Quantum Gateway.



The **Top Weekly Usage by Quantum Devices** widget shows the data utilized by Quantum devices in the previous week. The system shows the top three device names and the rest are shown as **Others**.

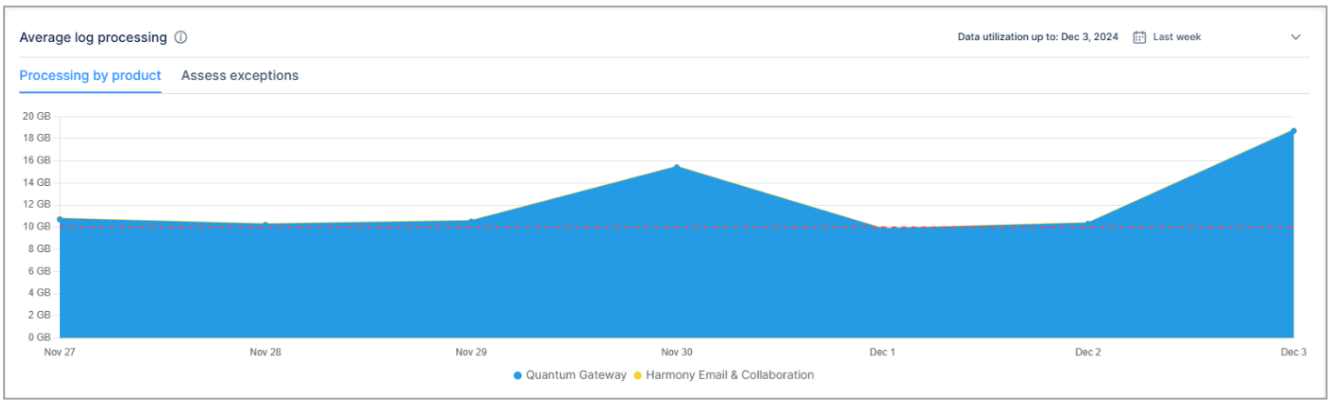
Average Log Processing

Processing by Product

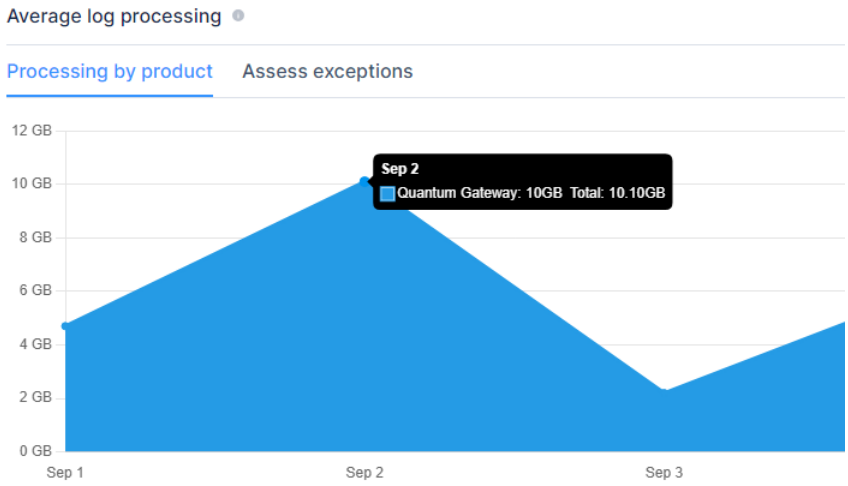
The **Processing by product** section shows the data processed by each product over a specific time period and the entitled volume of data that can be processed. The red dotted line represents the entitlement, allowing you to compare current usage to the entitlement.

Note - Currently, XDR does not enforce the entitlement limit and continues processing data even when the limit is reached.

By default, it shows the data usage in the previous week. You can select the required time period from the top right corner.



To view the data usage on a specific date, hover over the date.



Assess Exceptions

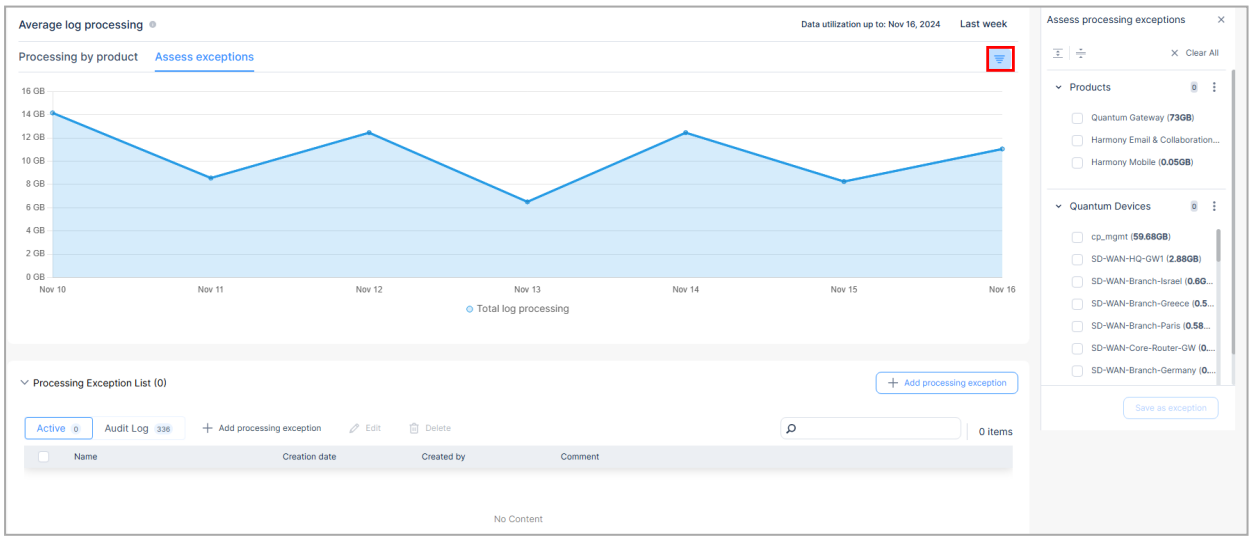
The **Assess exceptions** section shows the total data volume processed by all the products. Additionally, you can assess the data usage after excluding specific products or Quantum devices from being processed by XDR. After assessment, you can exclude their data from processing.

When assessing the processing exceptions, the system always shows the data from the previous week. This ensures that the data from the most recent week is used to determine the current data utilization.

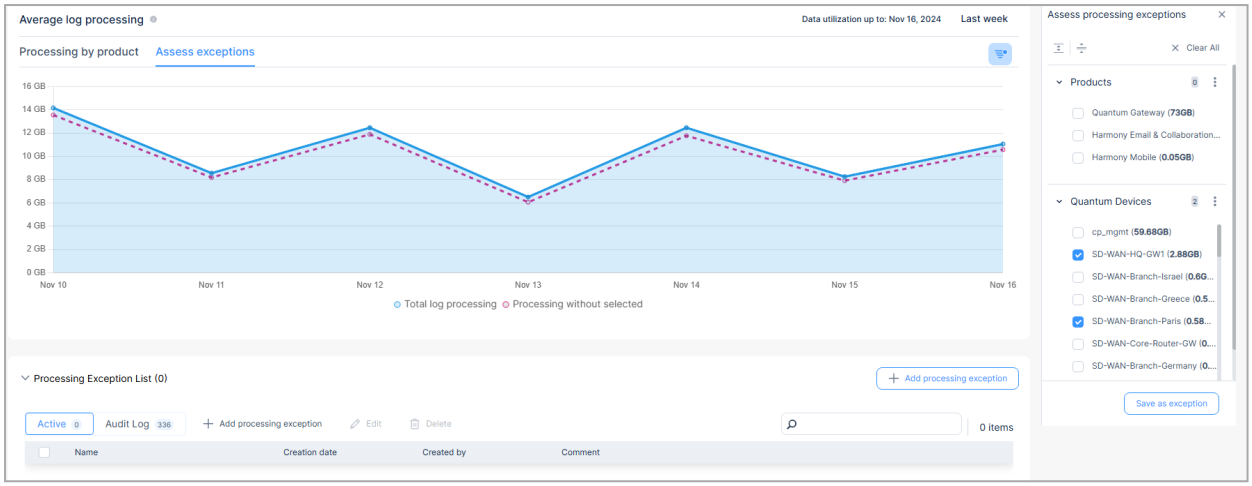
To assess the data utilization after excluding a product or Quantum device:

1. Click the icon.

   The **Assess processing exceptions** window appears.



2. Select the product(s) or the Quantum device(s) you want to exclude.

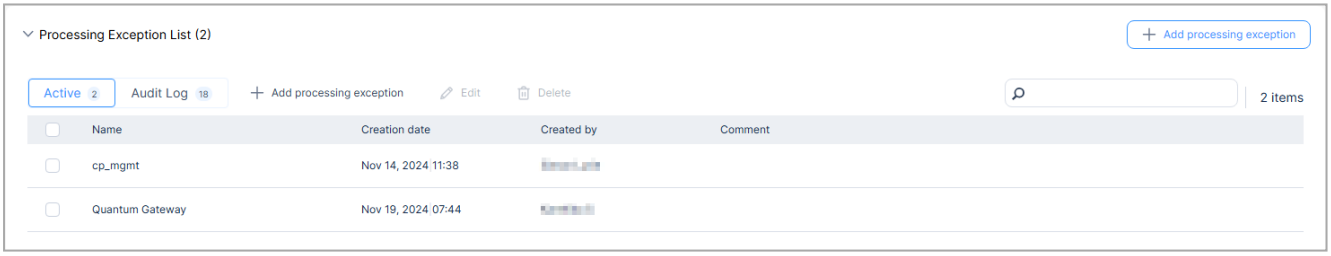


The system shows the total volume of data usage and the reduced data usage after exclusion as dotted lines.

3. To add the selected products or Quantum devices to the Processing Exception list, see adding to processing exception list.

Processing Exception List

After you assess the data usage by excluding specific product(s) or Quantum device(s), you can exclude their data from being processed by XDR. The **Processing Exception List** section shows the list of products and Quantum devices that are excluded from processing.



The **Active** tab shows the exceptions that are currently active.

The **Audit Log** tab shows the history of exceptions that were previously defined but are no longer active. This is important data to review because while the exceptions were active, no incidents would have been created based on the excluded items.

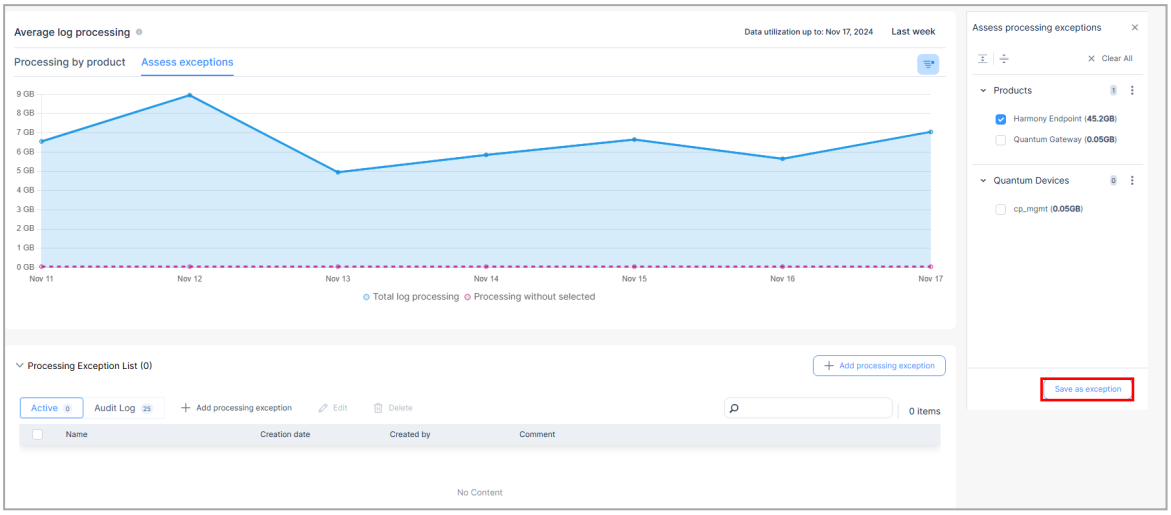
Note - The **Log processing** page shows information based on the active exceptions.

Adding a Processing Exception

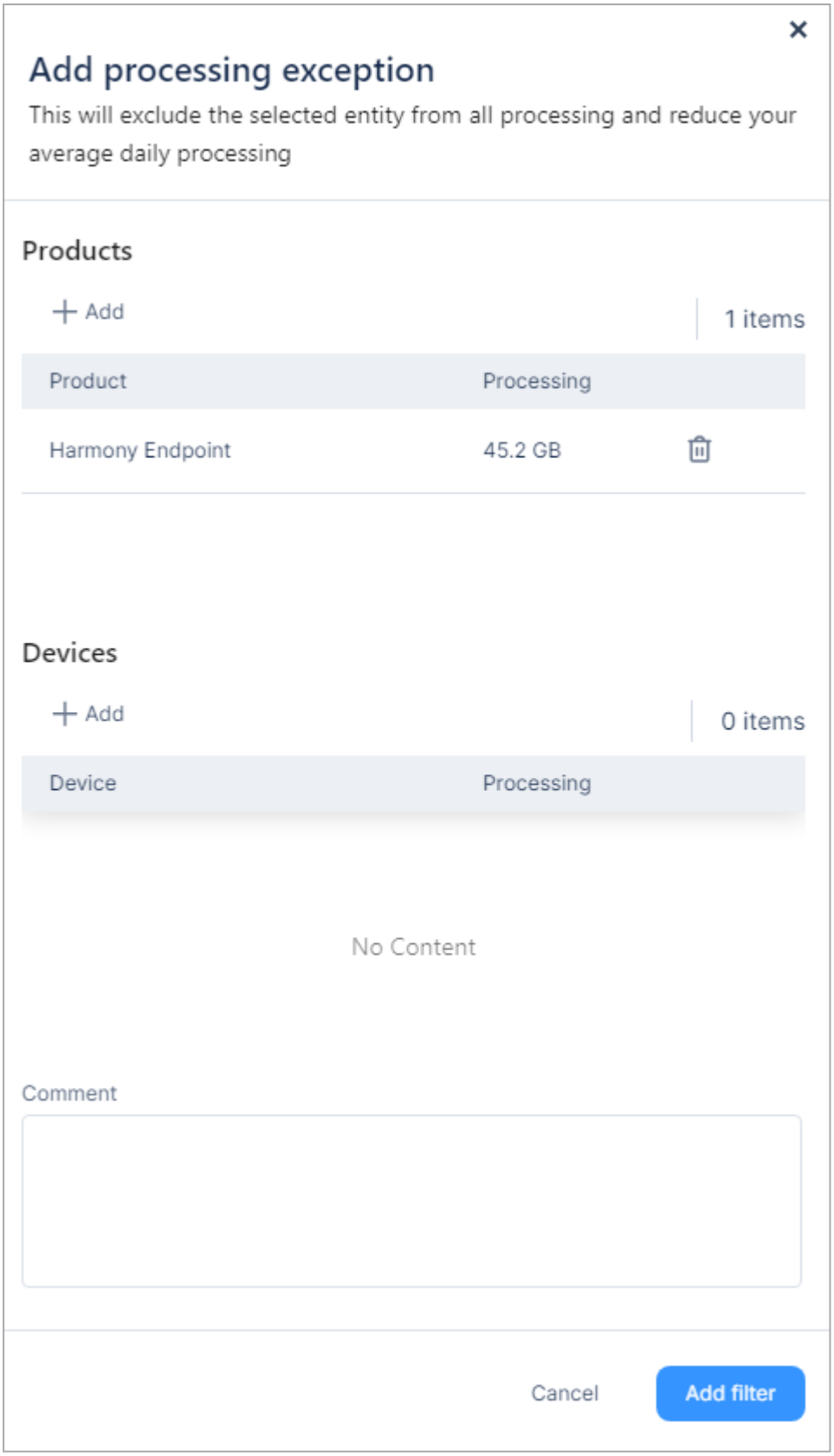
To add products or Quantum devices to the Processing Exception list:

1. To assess the data usage and then add to the exception list:

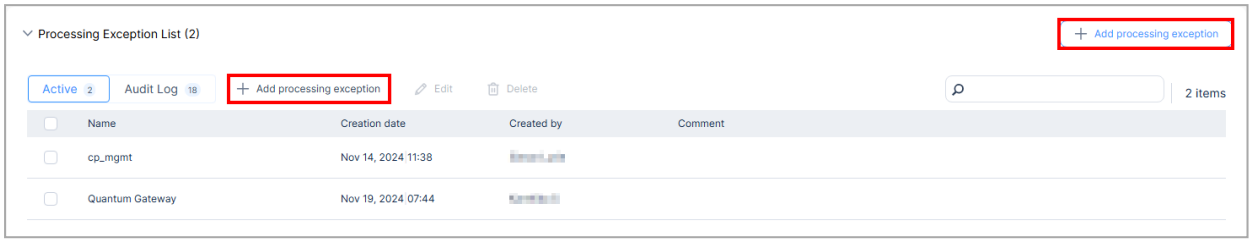
a. In the **Assess processing exceptions** panel, select the required products/devices and click **Save as exception**.



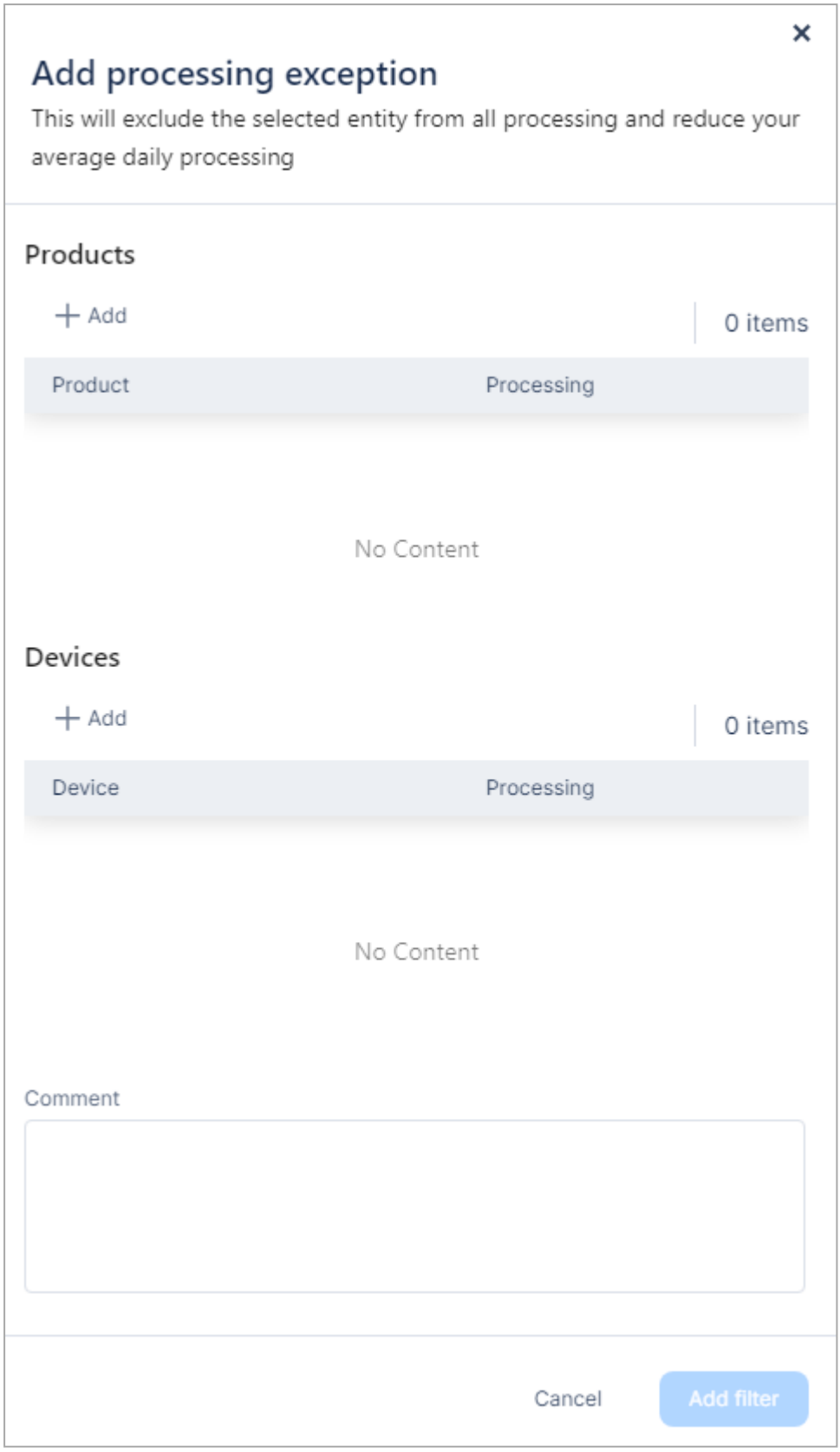
The **Add processing exception** window appears and shows the assessed product/device and its data usage.


Add processing exception
This will exclude the selected entity from all processing and reduce your average daily processing
Products
Add
1 items
Product
Processing
Harmony Endpoint
45.2 GB
Devices
Add
0 items
Device
Processing
No Content
Comment
Cancel
Add filter

2. To directly add products or Quantum devices to the Processing Exception list, in the **Processing Exception List** section, click **+ Add processing exception** on the right-side or above the table.



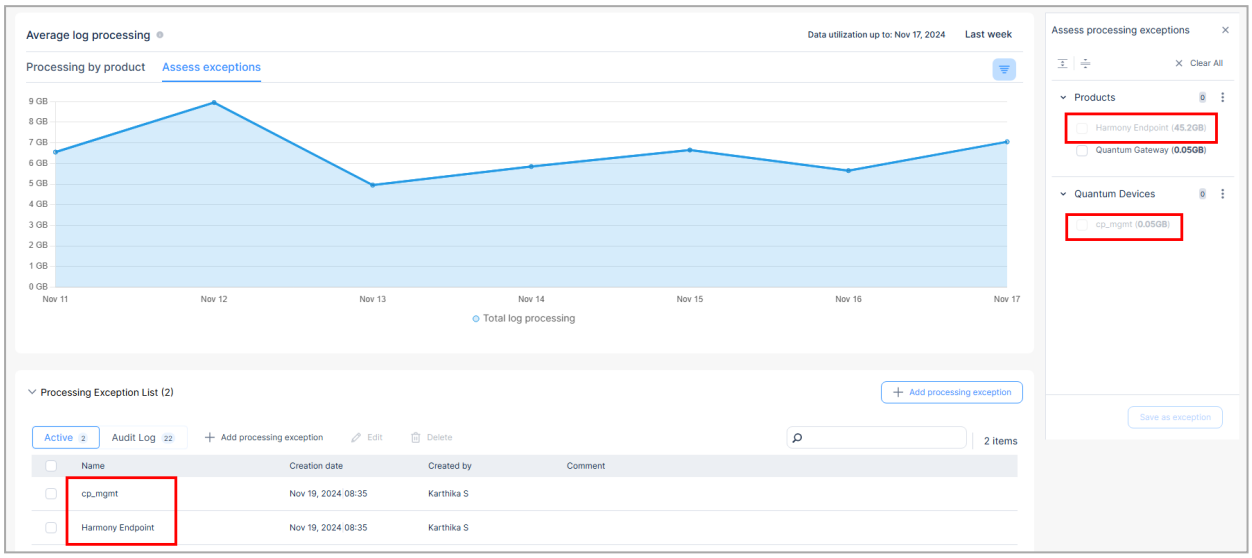
The **Add processing exception** window appears.



3. To add a product, in the **Products** section, click **+Add**and select the product(s).
4. To add a Quantum device, in the **Devices** section, click **+Add**and select the device(s).
5. (Optional) Add a comment.

6. Click **Add filter**.

   The system adds the selected products and Quantum devices to the active Processing Exception list, so that XDR no longer process their data. These products/devices will appear grayed out in the **Assess processing exceptions** panel.



Managing the Processing Exception List

1. To edit an active exception:
   a. In the **Processing Exception List** section, select the product/device and then click **Edit**.
   b. Make the necessary changes and click **Save**.
2. To delete active exception(s):
   a. In the **Processing Exception List** section, select the products/devices and then click **Delete**.
   b. In the confirmation box, click **Save**.

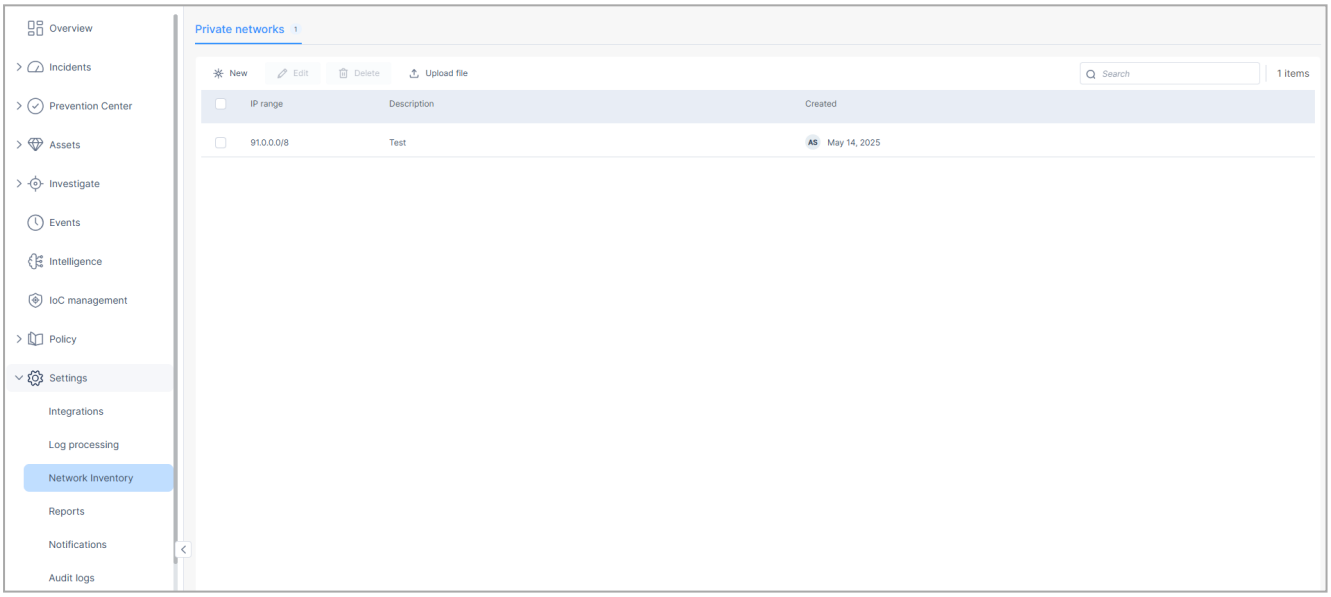
Network Inventory

The **Network Inventory** page allows you to add details about your organization's internal networks. This information helps Check Point XDR to:

- Identify trusted internal traffic and distinguish it from external or suspicious activity.
- Make more informed decisions when analyzing events.

Events involving internal networks could appear in incidents; however, the system classify them as artifacts rather than Indicators of Compromise (IoCs). This distinction ensures that internal artifacts do not trigger automatic blocking actions via IOC management, helping to avoid disruptions caused by blocking trusted internal resources.

To view the **Network Inventory** page, access the XDR Administrator Portal and go to **Settings** > **Network Inventory**.



Note - You can also access the **Network Inventory** page from **Settings** > **Getting Started**.

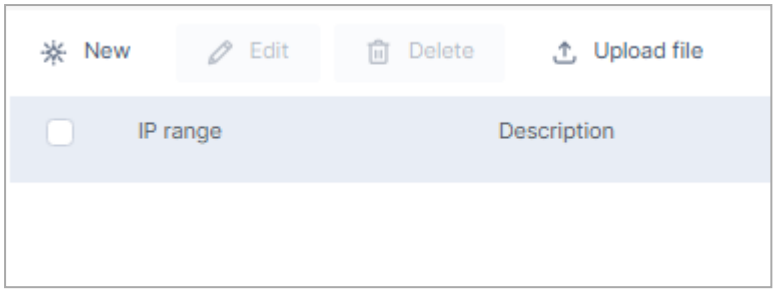
Private Networks

The **Private networks** tab displays the details of internal IP addresses or IP ranges (CIDR) used within your organization.

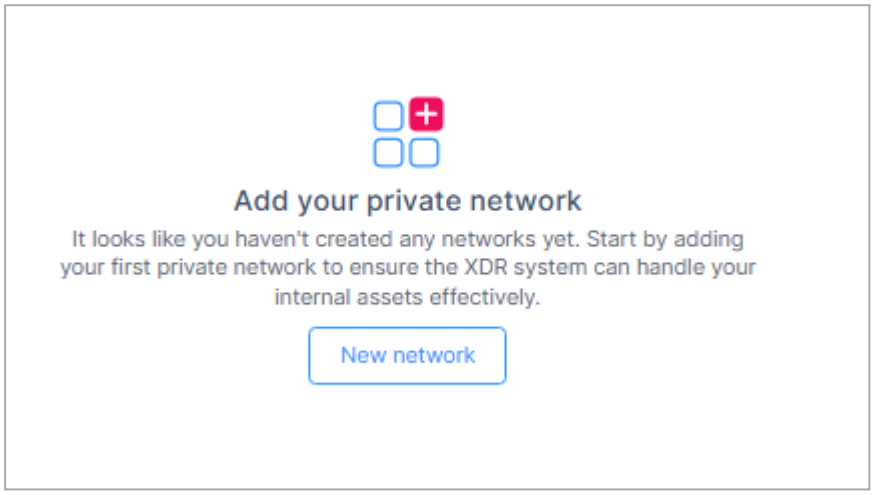
Adding a new Private Network

To add IP addresses or a network range (CIDR) manually:

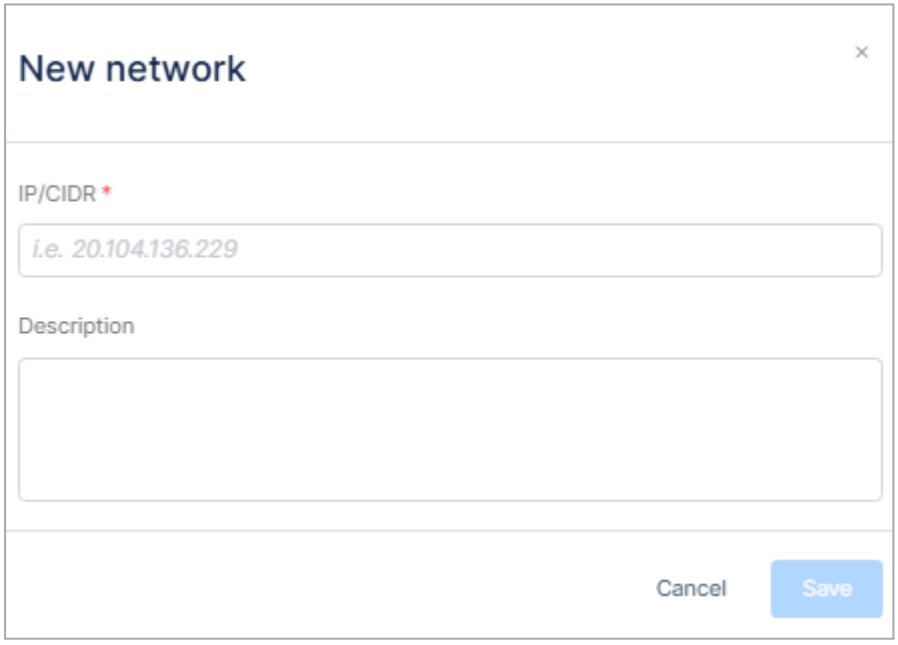
1. Go to **Settings** > **Network Inventory**.
2. Click **New**.



Note - If you have not added any network, you can click **New network**.



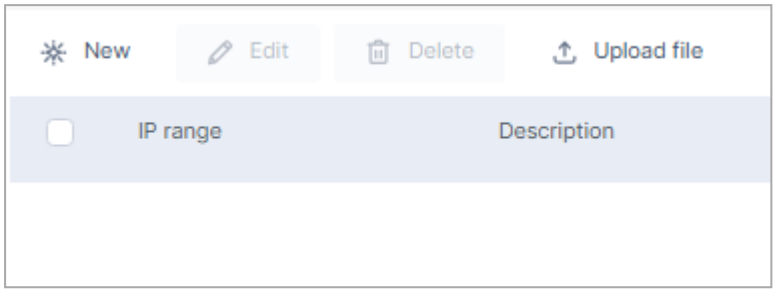
The **New network** window appears.



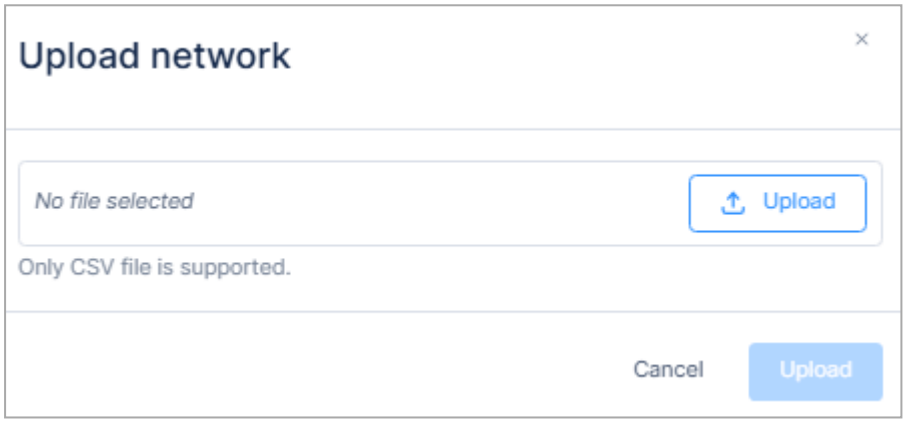
3. In the **IP/CIDR** field, enter a single IP address (example, 192.168.1.10) or a network range in CIDR notation (example, 192.168.1.0/24) corresponding to your internal network.
4. (Optional) Enter a description for the network for easy identification.
5. Click **Save**.

To add a list of IP addresses or a network range (CIDR) from a CSV file:

1. Click **Upload file**.



The **Upload network** window appears.

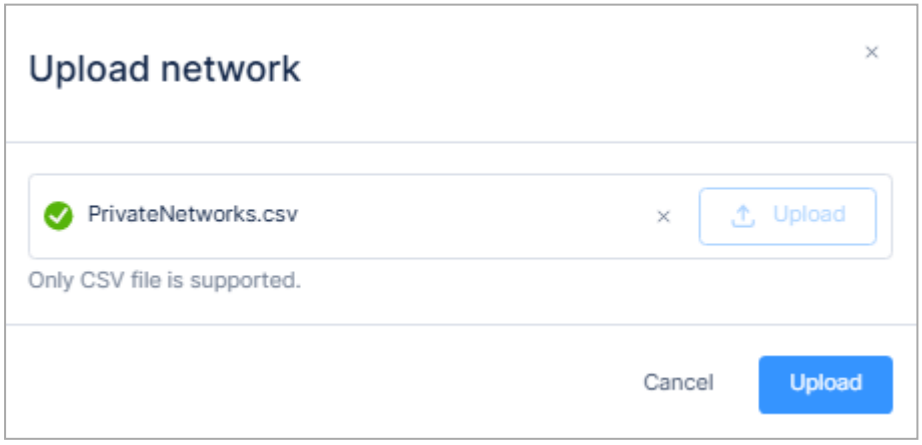


2. Click **Upload** and select the CSV file that contains the list of IP addresses and/or ranges.

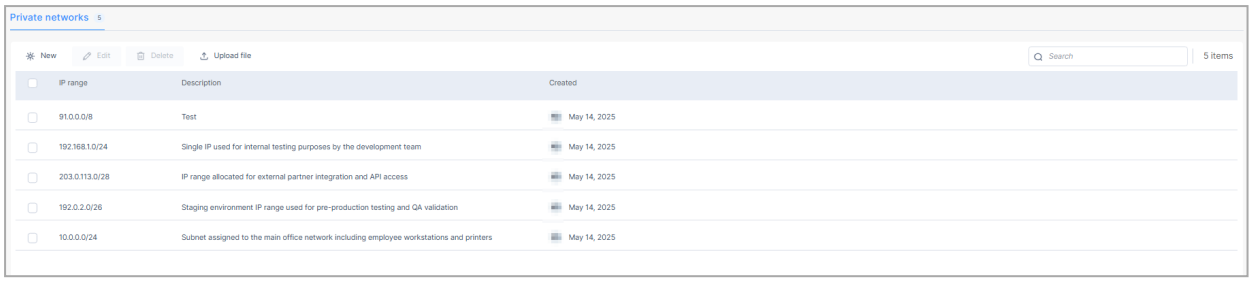
Important -

- The CSV file must contain two columns: one for the **IP address** or **CIDR**, and one for a description (can be empty or up to 200 characters).
- The file must **not include** a header row. Otherwise, the system displays an error.

3. Click **Upload**.



The system adds the IP addresses from the CSV file to the **Private networks** table.



The **Private networks** table shows:

Item	Description
IP range	IP address or CIDR of the private network.
Description	Description of the private network.
Created	Shows the user who added the network and the date of creation.

You can search for an IP address, range, or creator by entering the relevant text in the **Search** box above the table.

Managing Private Networks

1. To edit the details of a network:
    a. Select the network in the table and click **Edit**.
    b. Make the necessary changes and click **Save**.
2. To delete a network:
    a. Select the network in the table and click **Delete**.
    b. Click **Yes** in the confirmation box.

Reports

XDR/XPR Reports

XDR/XPR Configurable Activity Report

Configurable Activity Report is the XDR activity report for a specific time period.

It contains information about:

- Connected products
- Prevention statistics
- Incidents
- Exclusions
- Intelligence

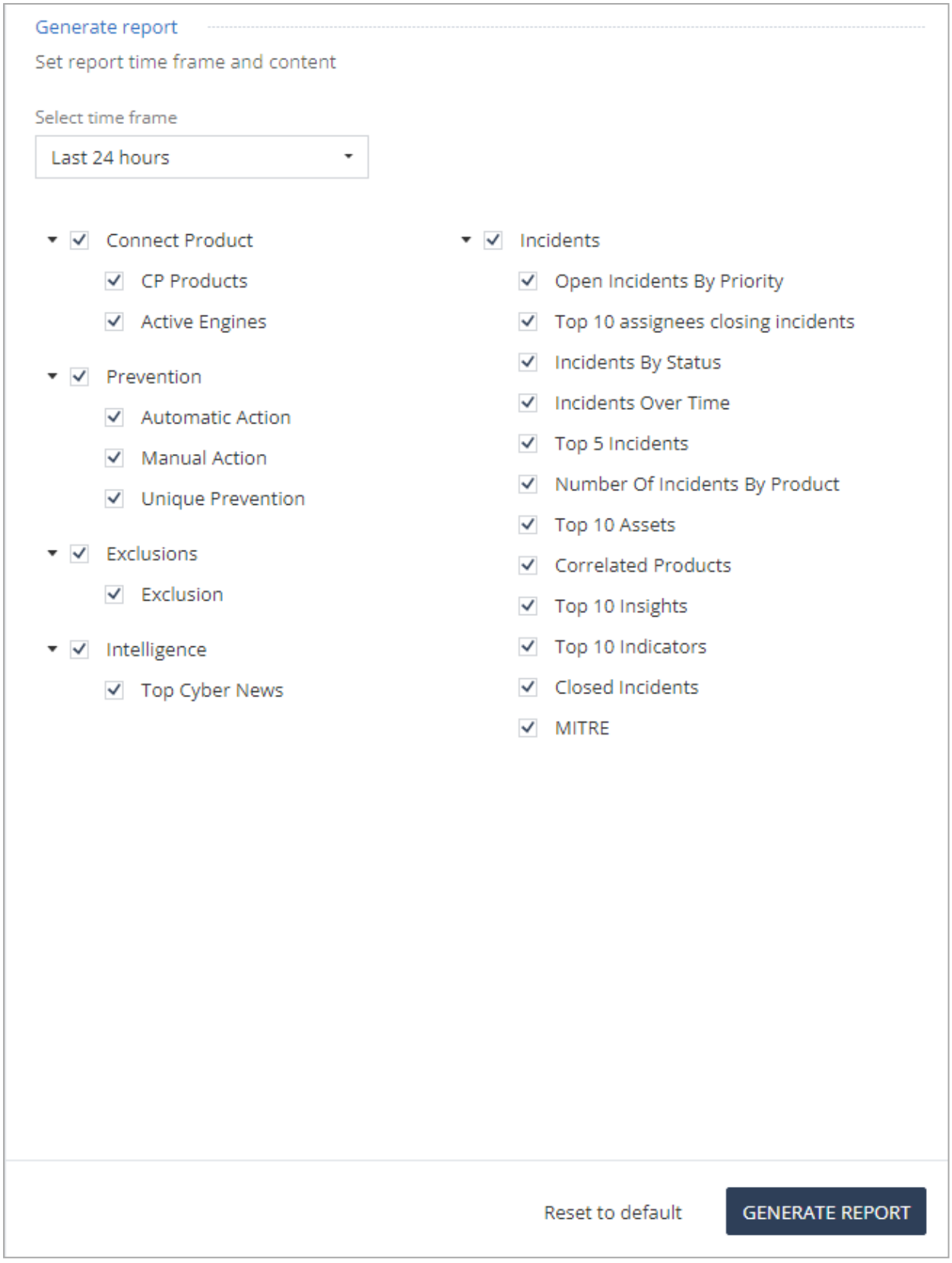
You can configure the report content, download the report on-demand or schedule it daily, weekly and monthly, and email it to recipients.

Generating an Activity Report

To generate an activity report:

1. Log in to the XDR Administrator Portal.
2. Go to **Settings** > **Reports**.
3. Click **Generate Report**.

   The **Generate report** window appears.



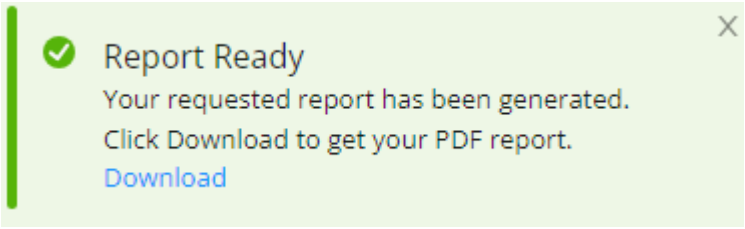
a. Select the time frame for the report.

b. Select the content for the report.

c. To reset the content to the default values, click **Reset to default**.

d. Click **Generate Report**.

When the report is ready, a pop-window appears.

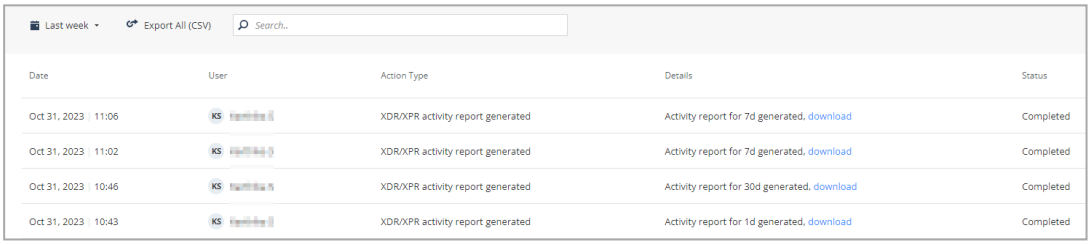


e. Click **Download**.The system downloads the report in the PDF format.

f. (Optional) To view and download previous reports:

i. Click **Go to view history**.

The **Audit logs** page appears.



ii. For the report you want to download, click **download**.

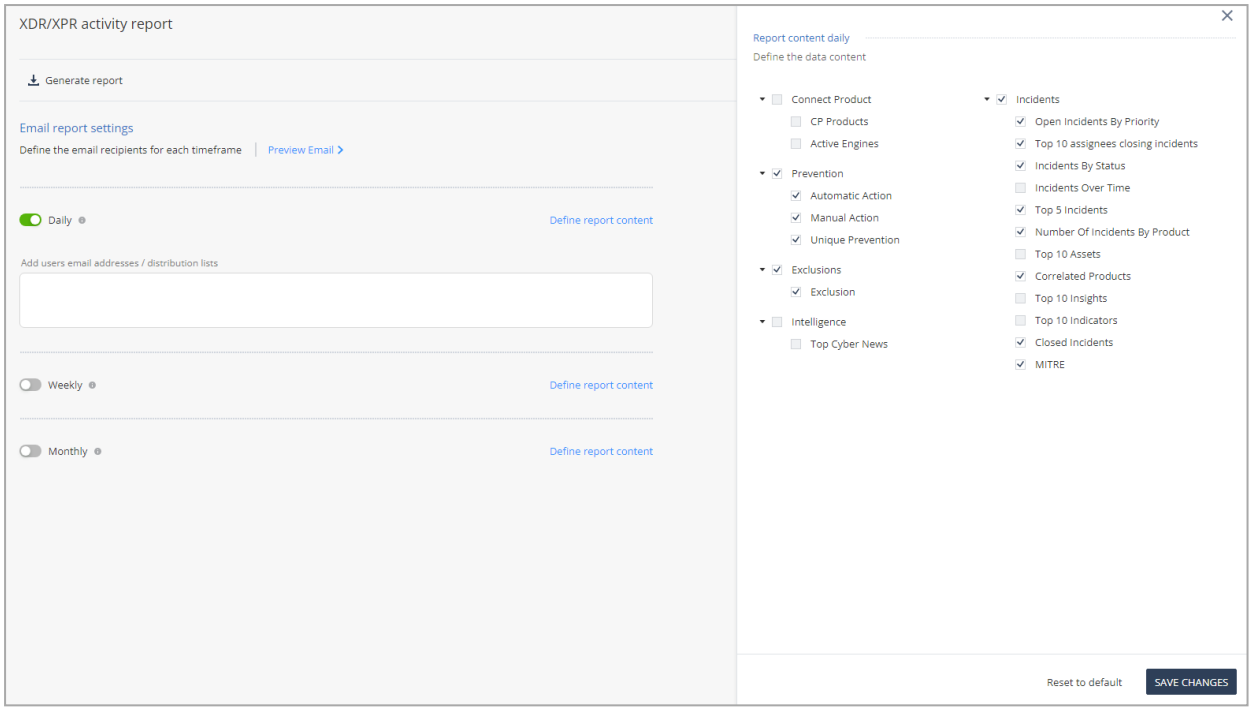
Scheduling an Activity Report

To schedule an activity report:

In the **Email report settings** section:

1. To preview the email content, click **Preview Email**.
2. Select the frequency to send the report.
   - **Daily** - The report is sent every day at 00:00 hours.
   - **Weekly** - The report is sent on every Monday at 00:00 hours.
   - **Monthly** - The report is sent on 1st of every month at 00:00 hours.
3. To define the report content, click **Define report content**.

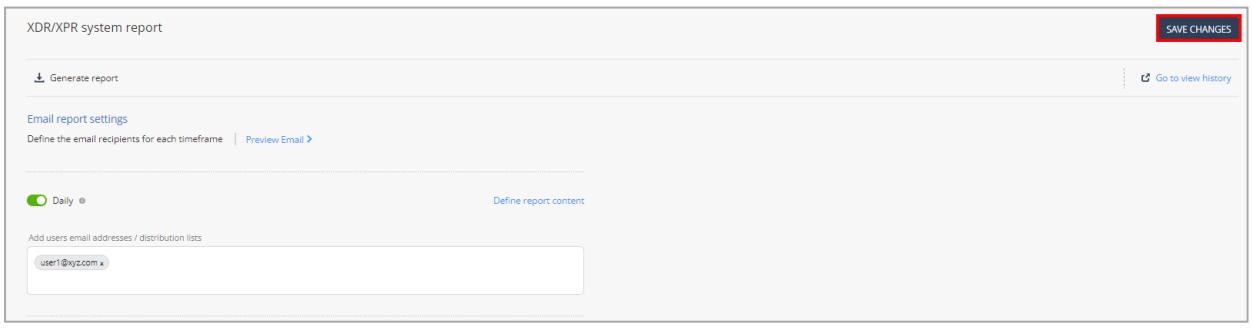
   The **Report content** window appears.



4. Select the content for the report.

   Note - The report content differs depending on the frequency selected to send the report.

5. To reset the content to the default values, click **Reset to default**.
6. Click **Save Changes**.
7. Enter the email addresses.
8. Click **Save Changes**.

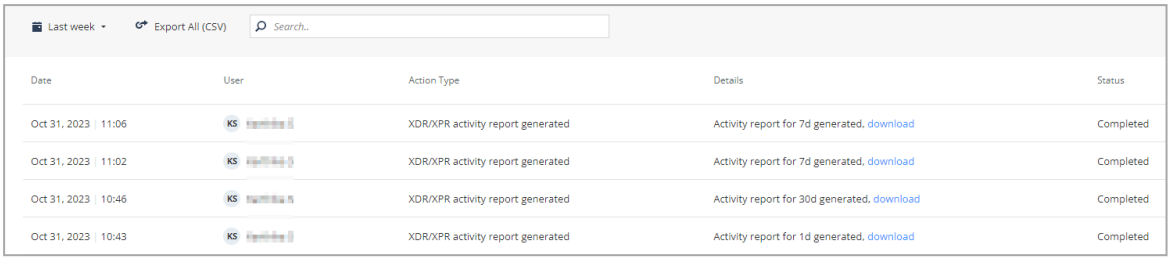


   The system sends the report in PDF format to the recipients.

9. (Optional) To view and download previous reports:

i. Click **Go to view history**.

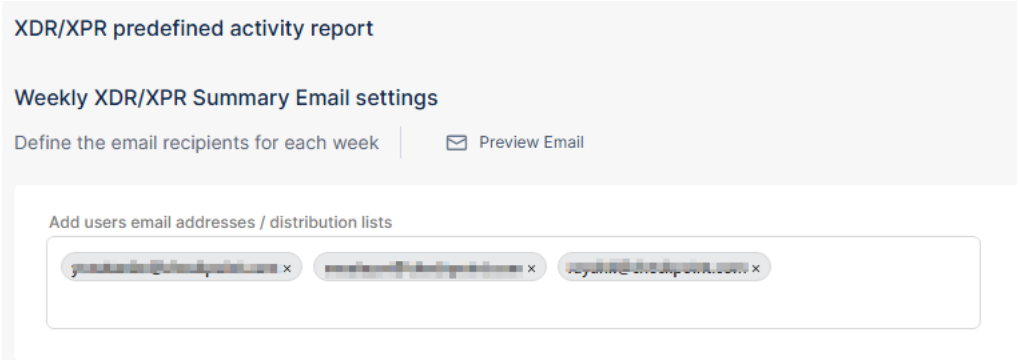
The **Audit logs** page appears.



ii. For the report you want to download, click **download**.

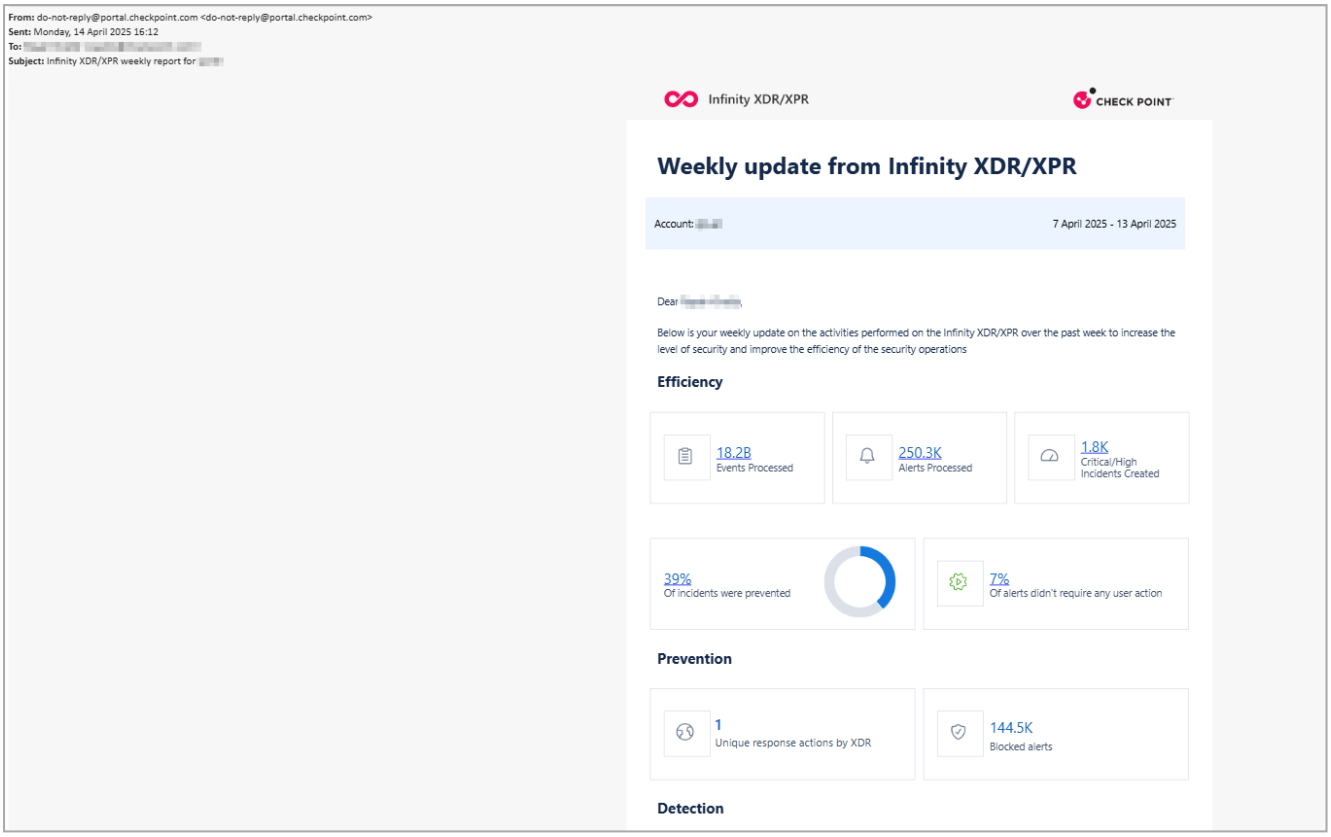
XDR/XPR Predefined Activity Report

The **XDR/XPR predefined activity report** provides a summary of key events and updates in XDR over the past seven days. You can configure the report to be sent automatically to specific users every week. To configure the email settings, see *"Weekly XDR/XPR Summary Email Settings" on page 357*.



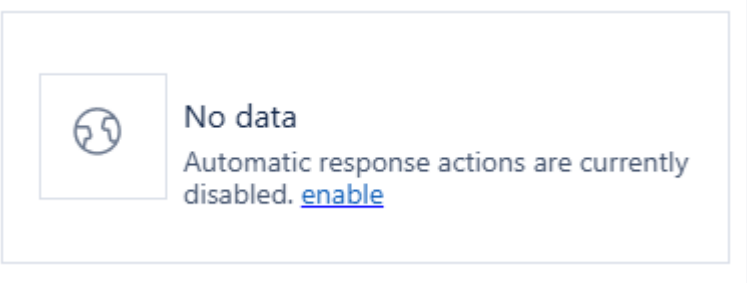
The system sends the weekly report email every **Monday**.

Sample weekly report:



The table below describes the contents of the weekly report:

Item	Description
Efficiency	
Events Processed	Total number of events processed by XDR in the report time frame. To view events details, click the count link. The Events page appears.
Alerts Processed	Total number of alerts processed by XDR in the report time frame. To view alerts details, click the count link. The Alerts page appears.
Critical/High Incidents Created	Total number of incidents with **Critical** and **High** severity levels created by XDR in the report time frame. To view incidents details, click the count link. The Incidents page appears, filtered by **Critical** and **High** priority levels.
Incidents prevented	Percentage of incidents prevented by XDR in the report time frame. To view incidents details, click the count link. The Incidents page appears, filtered by **Prevented** incidents.
Alerts do not require any user action	Percentage of alerts during the report time frame that required no user action. To view alerts details, click the percentage link. The Alerts page appears, filtered by **No Action Required** verdict.

Item	Description
Prevention	
Unique response actions by XDR	Total number of prevention actions taken by XDR in the report time frame (for example, add an indicator to IoC Management). To view actions details, click the count link. The Prevention Status page appears. **Note** - This section displays data only if automatic response is enabled. Otherwise, the report displays **No data**.  To enable automatic response, click the **enable** link. The Automations page appears.
Blocked alerts	Total number of alerts automatically blocked by XDR in the report time frame.
Detection	
Alerts detected using XDR's AI models	▪ Total number of alerts detected by XDR's AI model in the report time frame. To view alerts details, click the link. The Alerts page appears, displaying the alerts generated only by XDR, excluding the alerts from connected components. ▪ The graph shows the statistics of detection in the report time frame.

Unsubscribing from weekly report email

To unsubscribe, click the unsubscribe link in the email.

The system displays a message if you have successfully unsubscribed.

Note - If any error occurs, the system displays **Unsubscribe error**.

Weekly XDR/XPR Summary Email Settings

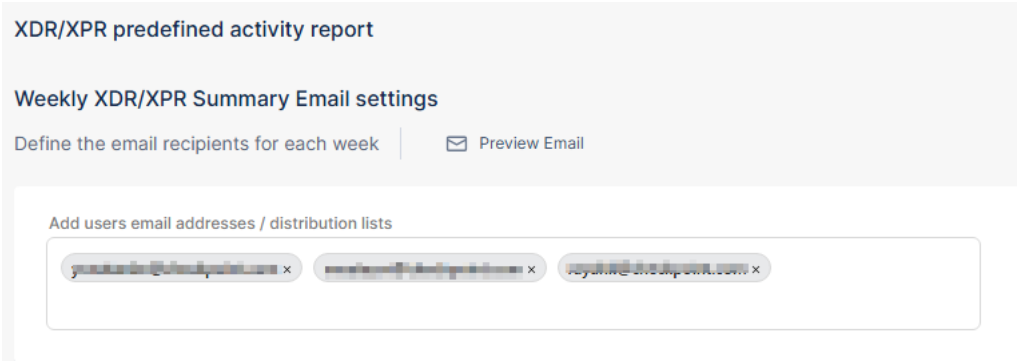
Prerequisite

To configure the weekly XDR/XPR summary email settings, you must have **Admin** role in **Global Roles** or **Specific Service Roles**.

To configure the weekly XDR/XPR summary email settings:

1. Go to **Settings** > **Reports**.
2. To add email recipients for the weekly report, in the **Weekly XDR/XPR Summary Email settings** section, enter the email address of users or the required distribution list.

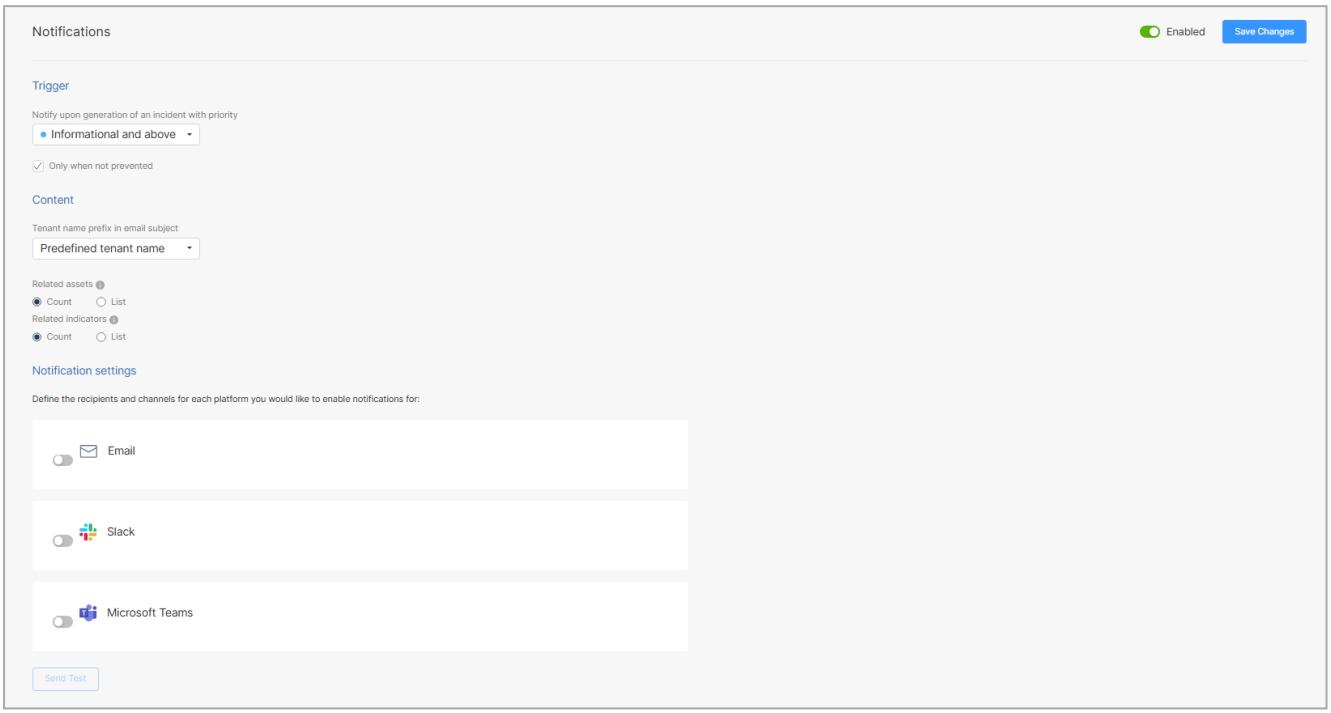
   Note - If a user unsubscribes from the weekly updates via the link in the email, the system automatically removes the user's email address from this list.



3. (Optional) To preview the email template, click **Preview Email**.
4. Click **Save Changes.**

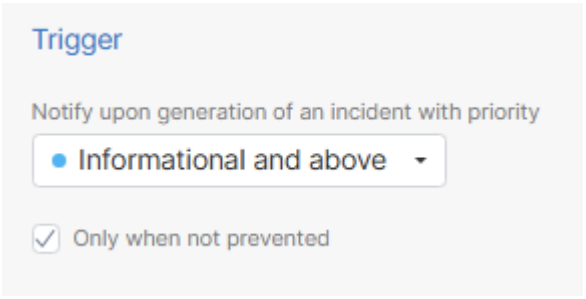
Notifications

You can send email, Slack and Microsoft Teams notifications when the system generates an incident with a specified priority.



To send notifications for XDR incidents:

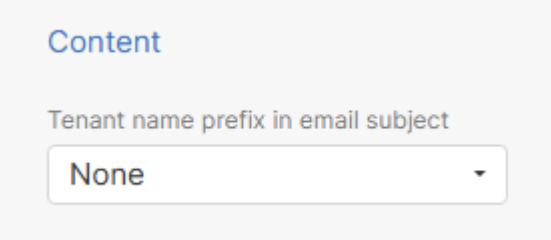
1. Log in to the XDR Administrator Portal.
2. Go to **Settings** > **Notifications**.
3. Enable the toggle button.
4. In the **Trigger** section:



   a. Select the priority level to trigger notifications. The system sends a notification when a generated incident matches the selected priority level.

b. To send notifications only for incidents that were not prevented, select the **Only when not prevented** checkbox. If not selected, the system sends notifications for all incidents that match the selected priority level.

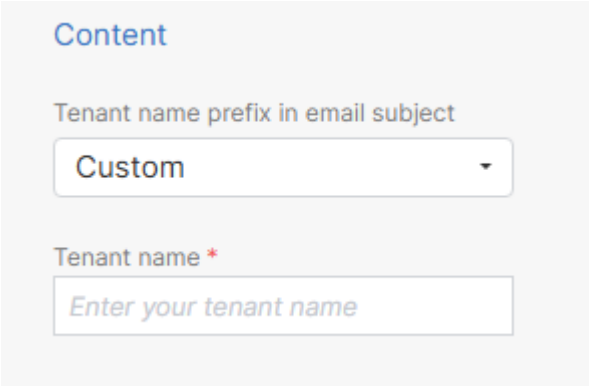
5. In the **Content** section, choose if you want to include tenant name in email notifications.



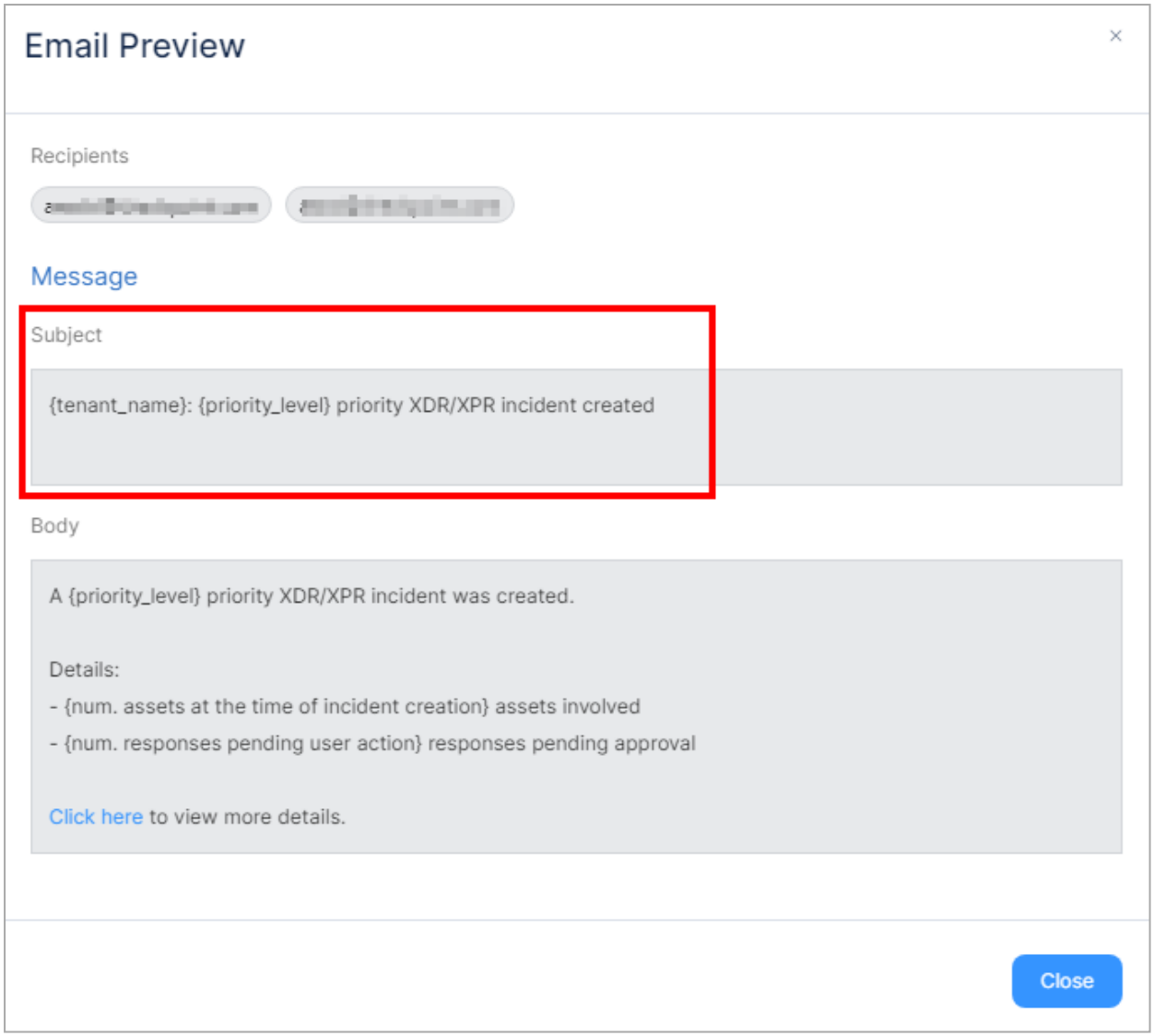
Select one of these:

- **None** - No prefix is added.
- **Predefined tenant name** - Adds the Check Point Portal tenant name as a prefix.
- **Custom** - Adds a custom tenant name as a prefix.

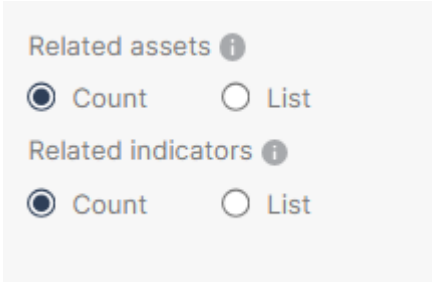
  Enter a name in the **Tenant name** field.



The tenant name appears as a prefix in the email Subject. Adding the tenant name helps to easily identify the account associated with the generated incident.



6. Select these:
   - **Related assets** - Choose whether to include the number of related assets or list their names (up to 5) in the notification.
   - **Related indicators** - Choose whether to include the number of related indicators or list their names (up to 5) in the notification.



7. Click **Save Changes**.

Sending Email Notifications

1. Enable the **Email** toggle button.
2. Enter the email addresses of users and/or distribution lists.
3. To view how the email subject and body appears, click **Preview Email**.
4. Click **Save Changes**.

Sending Slack Notifications

1. Enable the **Slack** toggle button.
2. Click **Edit**.

   Slack Channels pop-up appears.
3. Enter the **Channel name** and its **URL**.

   To add multiple channels, click **Add Channel** and enter the **Channel name** and its **URL**.
4. Click **Save**.
5. To view how the Slack notification appears, click **Preview Message**.
6. Click **Save Changes**.

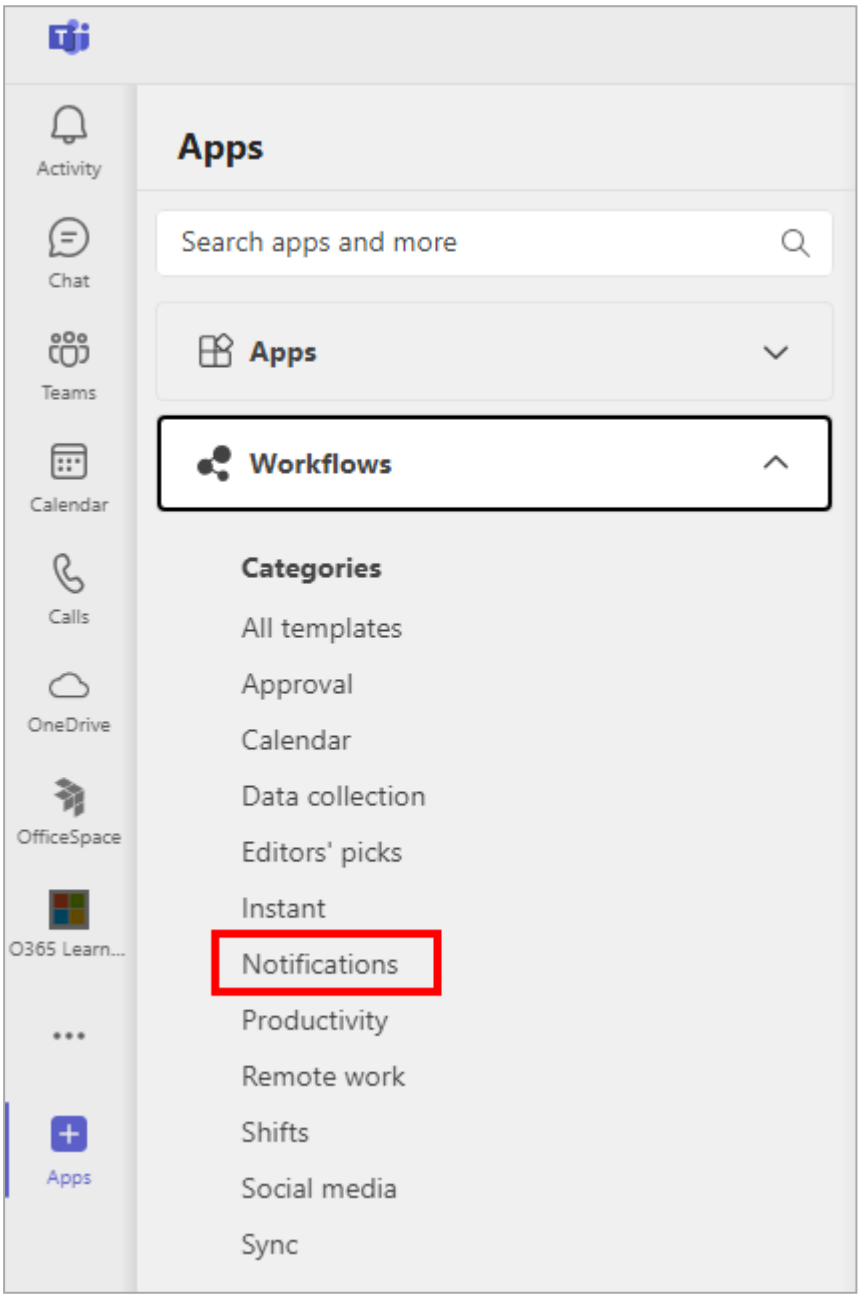
Sending Microsoft Teams Notifications

1. Create a workflow in Microsoft Teams:

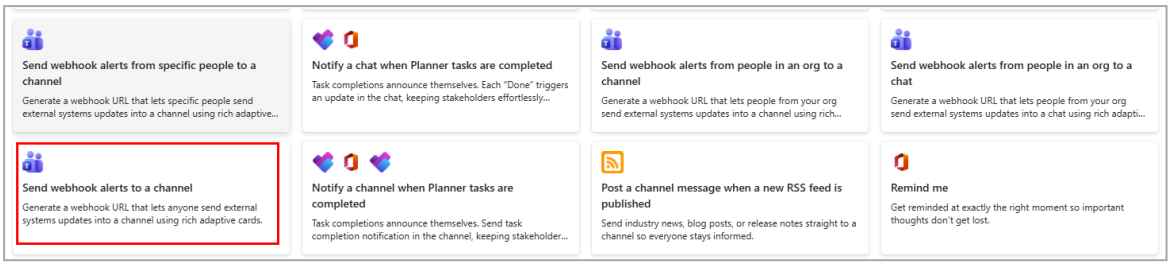
   Note - As a prerequisite, create a team and channel in Microsoft Teams to receive notifications.

   a. Open Microsoft Teams and click **+ Apps**.

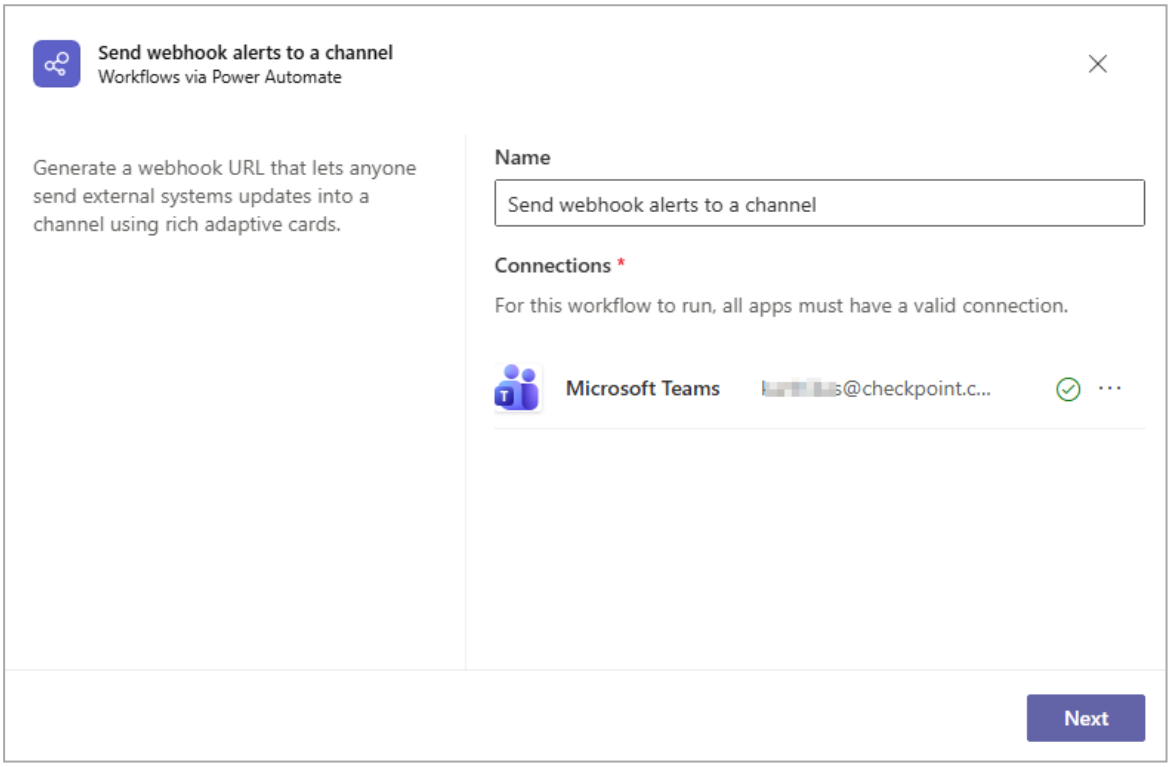
   b. Expand **Workflows** and click **Notifications**.



c. Select the **Send webhook alerts to a channel** workflow.



The workflow window appears.

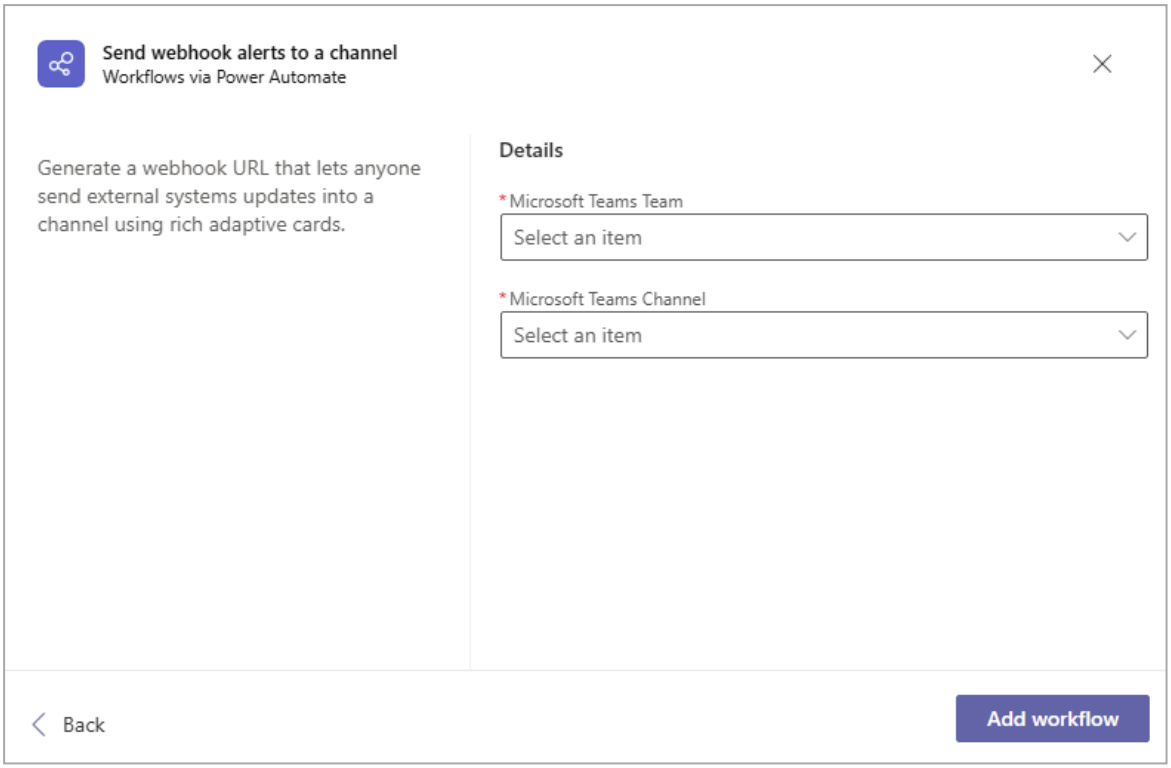


d. In the **Name** field, enter a name for your workflow.

e. Click ··· and select your Microsoft Teams account.

f. Click **Next**.

The workflow **Details** window appears.



g. From the **Microsoft Teams Team** list, select your team.

h. From the **Microsoft Teams Channel** list, select your channel.

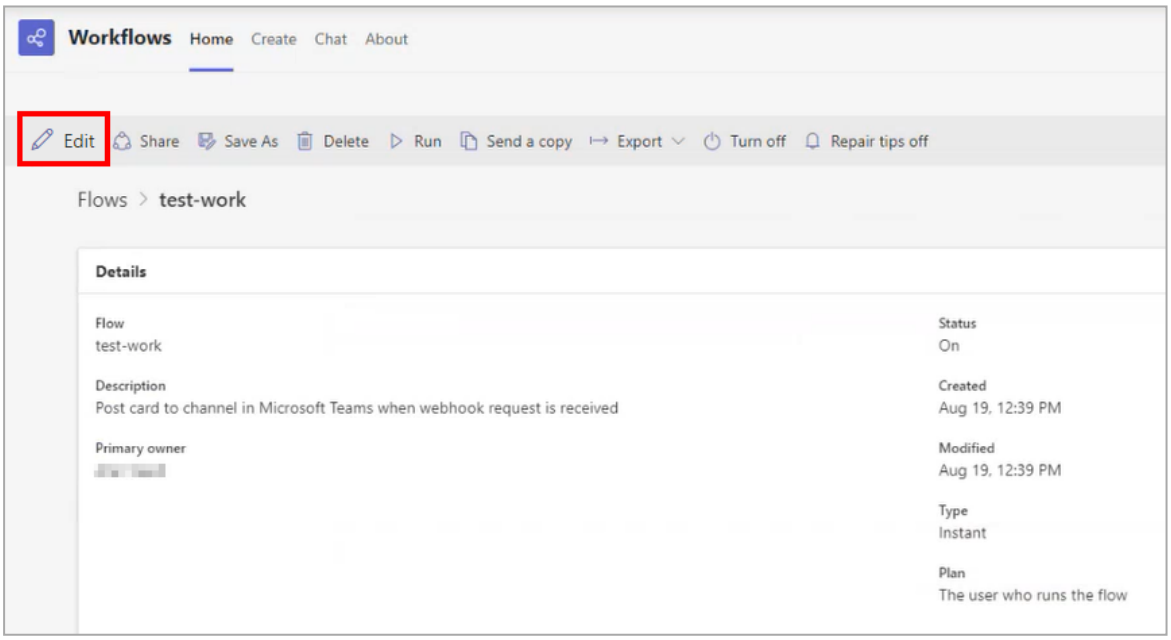
i. Click **Add workflow**.

The system creates the workflow.

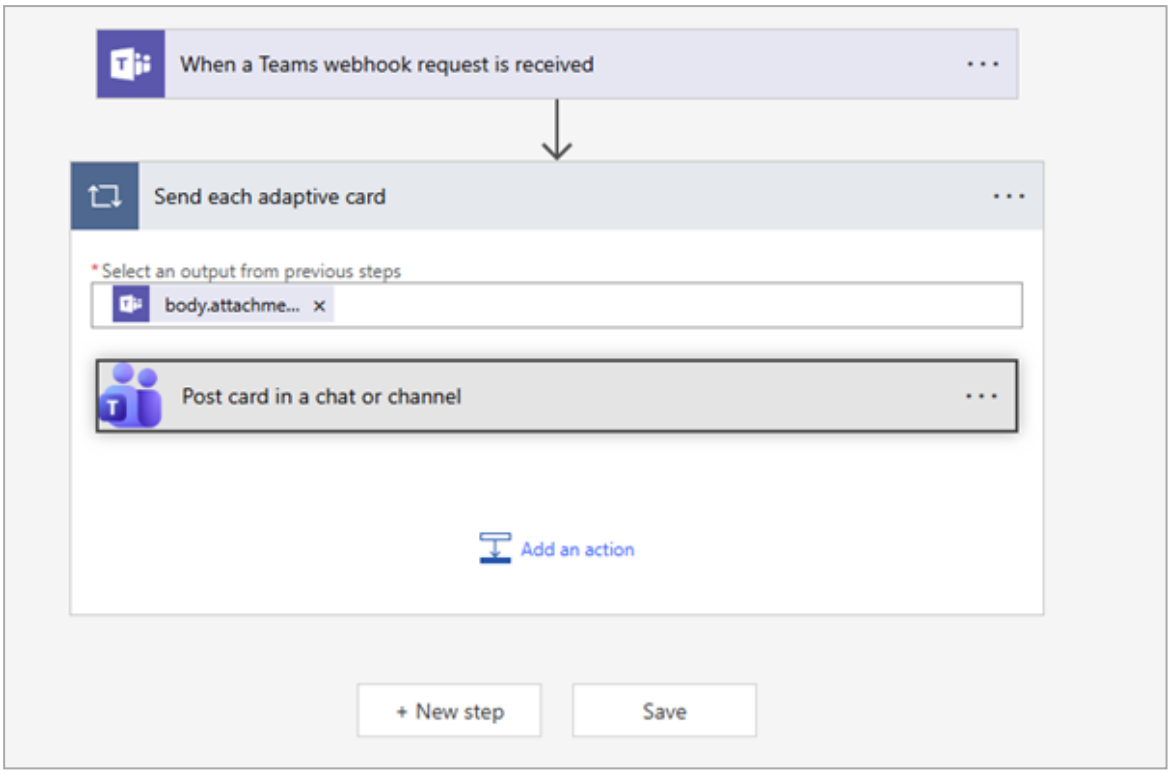
j. Copy the workflow link and click **Manage your workflow**.

The **Home** tab in the **Workflows**page appears.

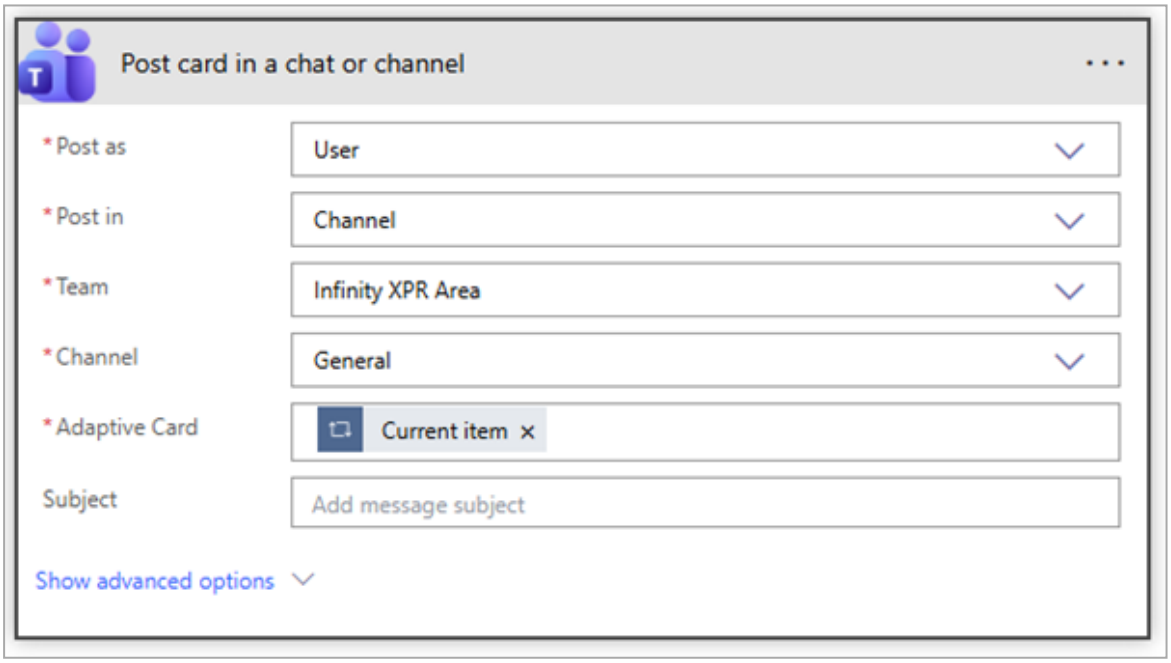
k. Click **Edit**.



l. Click **Send each adaptive card** > **Post card in a chat or channel**.



m. From the **Post as** list, select **User**.

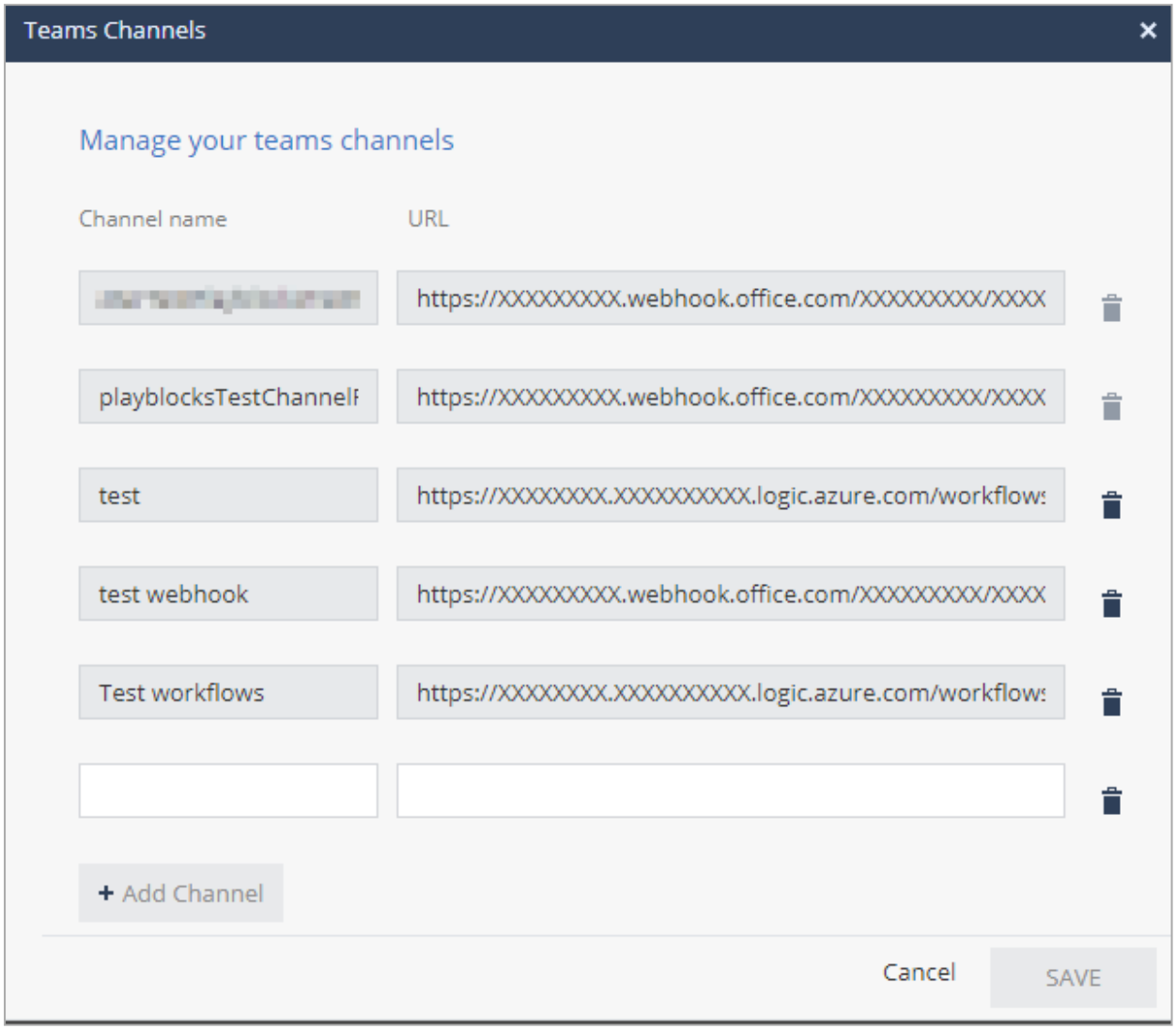


n. In the **Adaptive Card** field, select **Current item**.

o. Click **Save**.

2. In the XDR Administrator Portal, go to **Settings** > **Notifications** and enable the **Microsoft Teams** toggle button.
3. Click **Edit**.

   Teams Channels window appears.



4. Enter the **Channel name** and in the **URL** field, paste the workflow URL copied in step 1.j.
5. Click **Save**.
6. To view how the Microsoft Teams notification appears, click **Preview message**.
7. Click **Save Changes**.

Testing Notifications

To test the configured email, Slack, and Microsoft Teams notifications:

1. Click **Settings** > **Notifications**.
2. Click **Send Test**.
3. In the **Test Platforms** section, select the platforms you need to test (Email, Slack, Teams).
4. In the **Test** section, select the users.
   - To send the notifications to all the configured email addresses or channels, click **All recipients**.
   - To send the notifications to specific users or channels, click **Specific** and enter the required **Recipients**.
5. Click **Send**.

Audit Logs

The **Audit logs** page allows you to view the activities in Check Point XDR.

Note - Only high level activities that affect Check Point product security are shown. Changes in incident management (such as assignee, status and comments) are not shown.

To view the **Audit logs**, go to **Settings** > **Audit logs**.

XDR creates **Audit logs** only for these activities:

- Incident status (Created/Closed)
- IoC Management (Added/Edited/Deleted)
- Notifications
  - Policy changes (Enabled/Updated/Disabled)
  - Notifications sent
- Manual or automatic action taken
  - Isolate host on endpoint or gateway
  - Kill process on Endpoint
  - Quarantine file on Endpoint
- Automatic response (Enabled/Updated/Disabled)
- Exclusions (Created/Updated/Deleted)

To search for a specific activity, enter the name in the **Search** field.

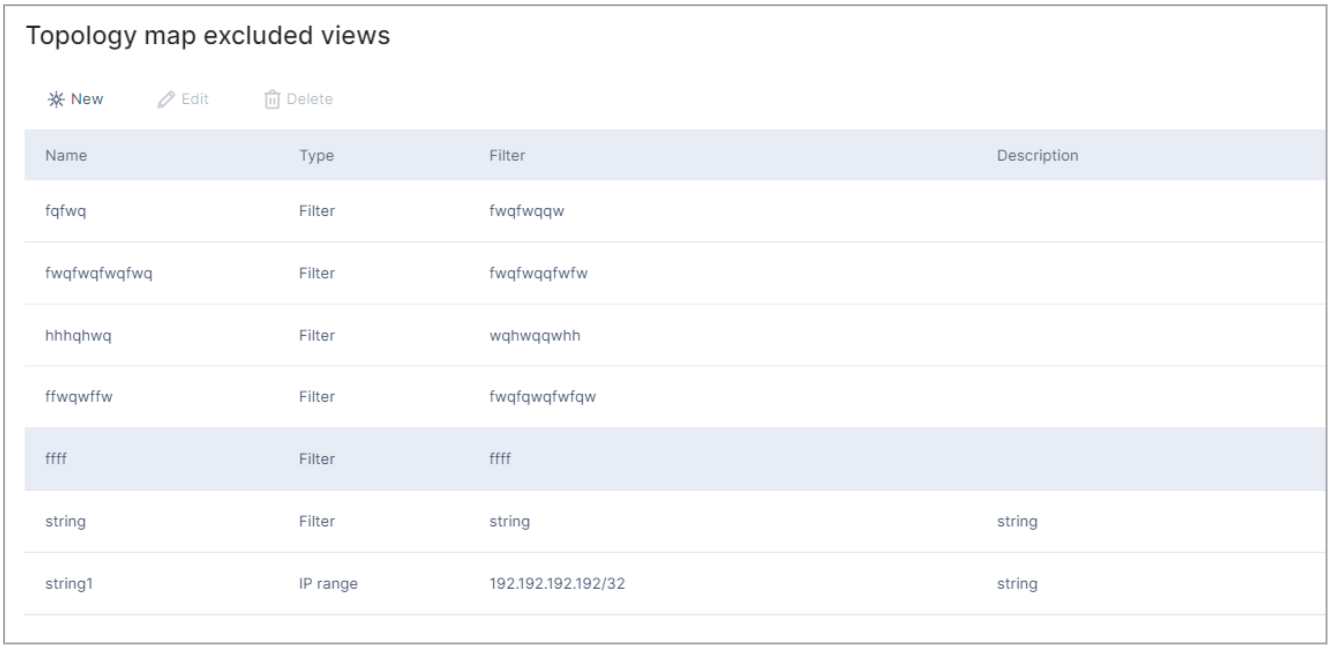
To export the data to an excel in CSV format, click **Export all (CSV)**.

Column Name	Description
Date	Date and time the activity was started.
User	Name of the user who initiated the activity. **System** indicates that the activity was performed by XDR.
Action Type	Type of activity performed.
Details	Details of the activity. For activities on incidents, it shows a link to the relevant incident.

Column Name	Description
Status	Status of the activity. ■ In progress ■ Completed ■ Failed

Topology Map Excluded Views

In this section, administrators can create **Excluded Views** to hide specific information on the Threat Topology map. Any data that matches an excluded view will not be shown on the map regardless of any View or Search definitions.



For more information, see *"Excluded Views" on page 185* in Threat Topology map.

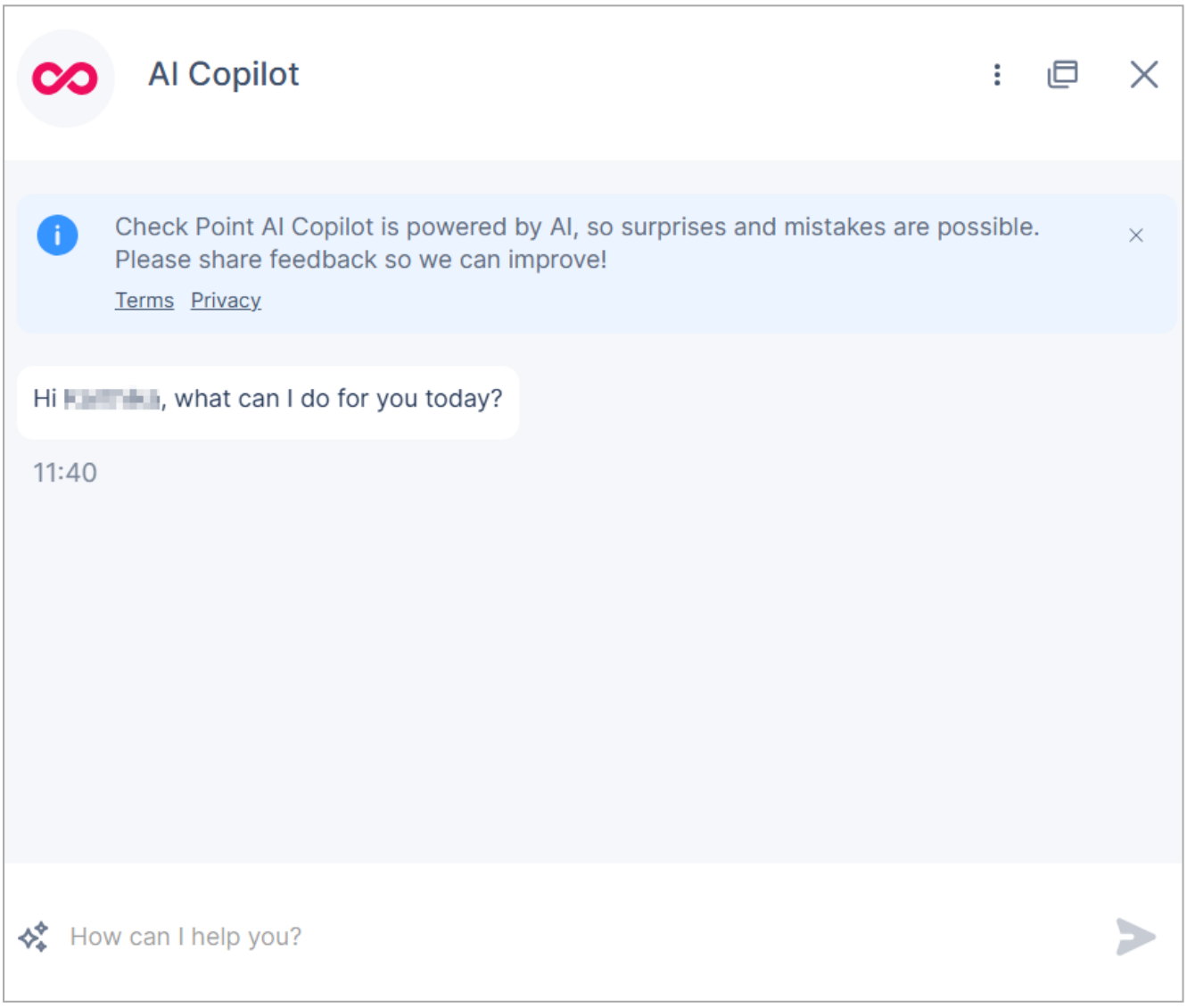
AI Copilot

AI Copilot is Check Point's GenAI assistant, that boosts security effectiveness of administrators and SOC analysts.

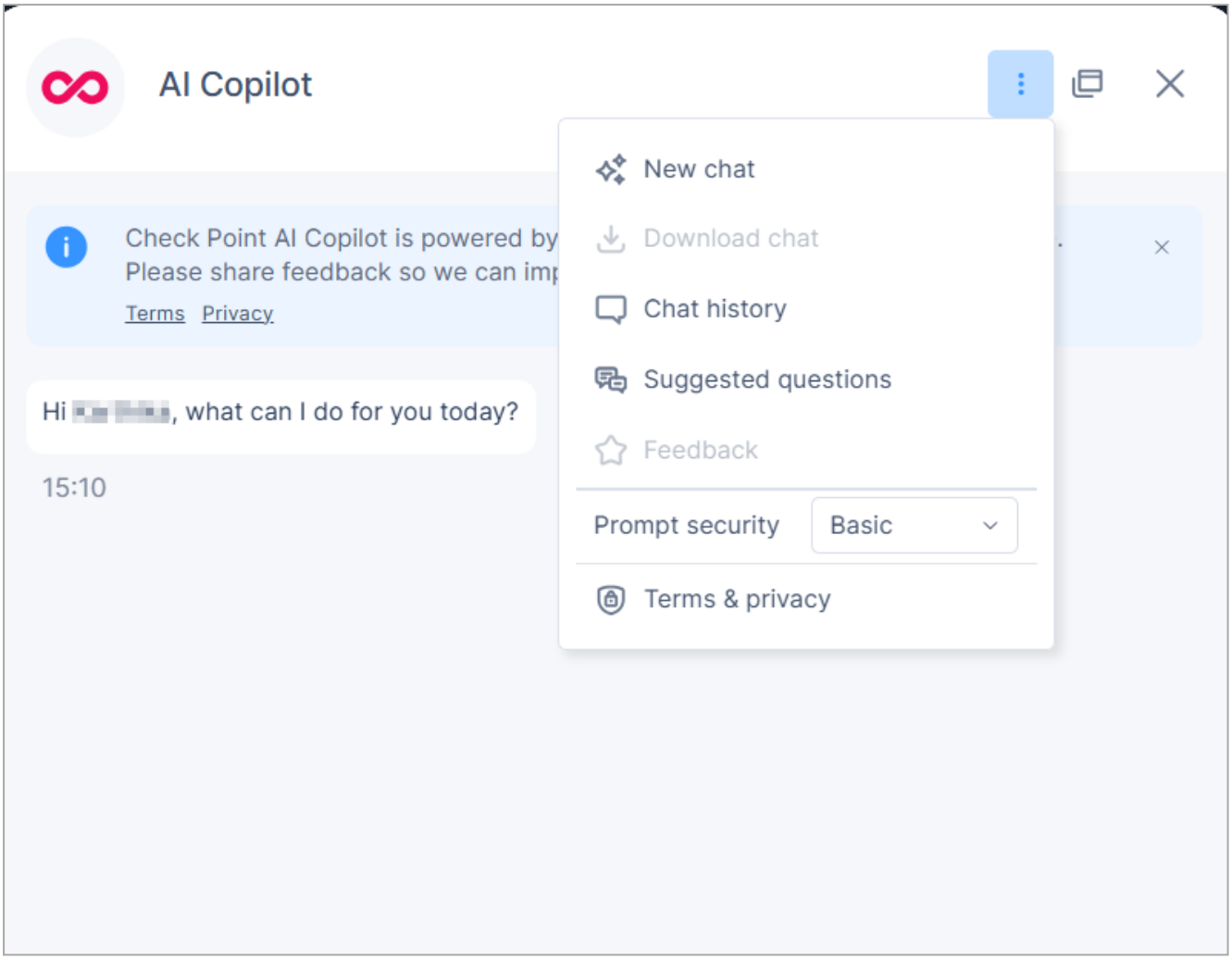
To access AI Copilot, click **AI Copilot** from the top banner, which opens the Copilot's chat window.

General Actions

To perform the general actions, access AI Copilot from the top banner.



Click ⋮ in the Copilot's chat window to perform these actions:



Action	Description
New chat	Starts a new chat.
Chat history	View chat history by month.

<table>
<tr><th>Action</th><th>Description</th></tr>
<tr><td>Prompt security</td><td>Scans the user prompt and response for protection, such as Data Loss Protection (DLP), Advanced Context Check (out-of-context and inappropriate text), and Jailbreak Check (prompts that try to bypass the AI engine security to obtain confidentially sensitive information in response).
It supports three modes:
<table>
<tr><th colspan="2">Mode</th><th>Data Loss Protection (DLP)</th><th>Advanced Context Check</th><th>Jailbreak Check</th></tr>
<tr><td>Basic</td><td>User Prompt</td><td>✓</td><td>–</td><td></td></tr>
<tr><td></td><td>Response</td><td>–</td><td></td><td></td></tr>
<tr><td>Optimized</td><td>User Prompt</td><td>✓</td><td>–</td><td>✓</td></tr>
<tr><td></td><td>Response</td><td>–</td><td>–</td><td>✓</td></tr>
<tr><td>Strict</td><td>User Prompt</td><td>✓</td><td>✓</td><td>✓</td></tr>
<tr><td></td><td>Response</td><td>–</td><td>✓</td><td>✓</td></tr>
</table>
</td></tr>
</table>

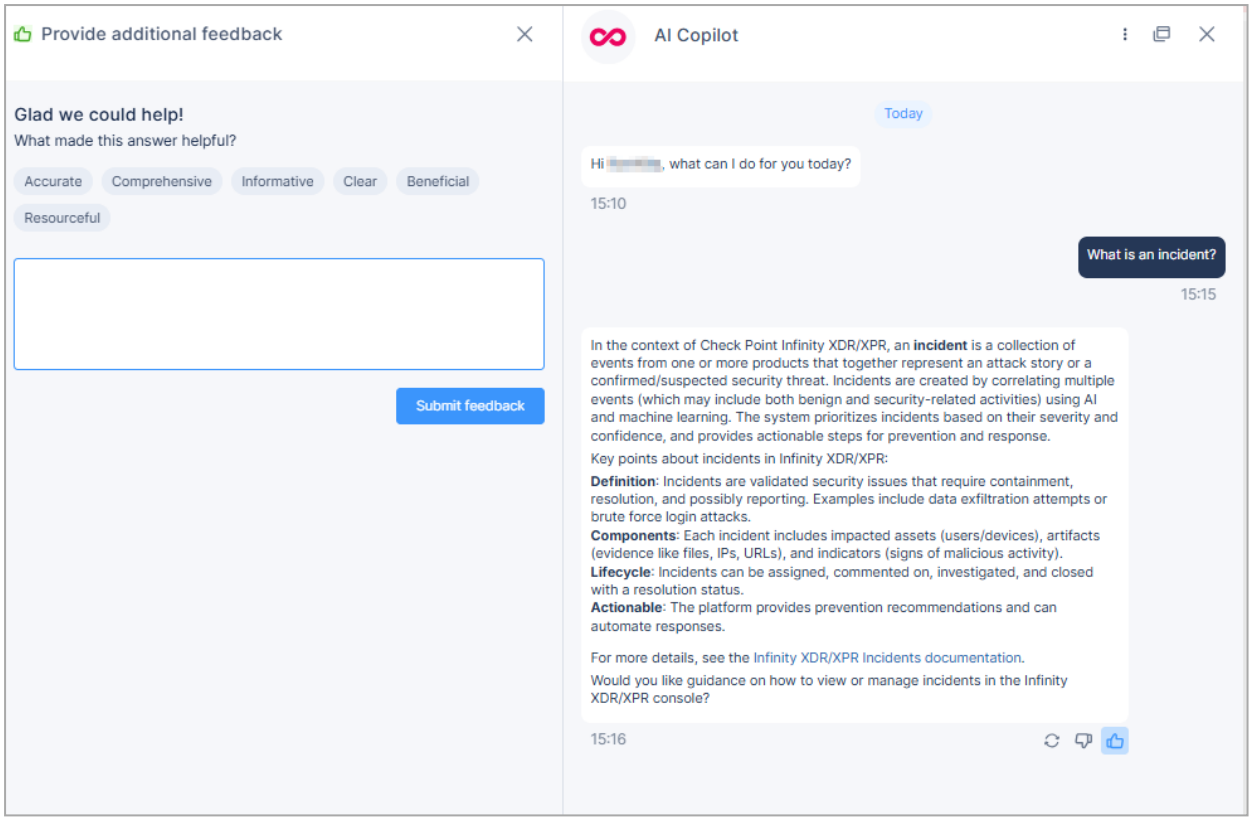
Providing Feedback on the Response

You can provide feedback on the copilot's responses. This feedback is monitored by Check Point for continuous improvement of the Copilot's responses.

To provide feedback:

1. After you get a response, click one of these:
   - If the response needs improvement, click .
   - If you like the response, click .

   The **Provide additional feedback** window appears.



2. Enter your feedback and click **Submit feedback**.

Supported Capabilities for XDR

With the AI Copilot, you can ask questions about XDR, Check Point documentation, MITRE ATT&CK framework and general cyber security terms, and take actions. Write actions are currently not supported.

General Query

You can ask the Copilot general questions about XDR and Check Point documentation.

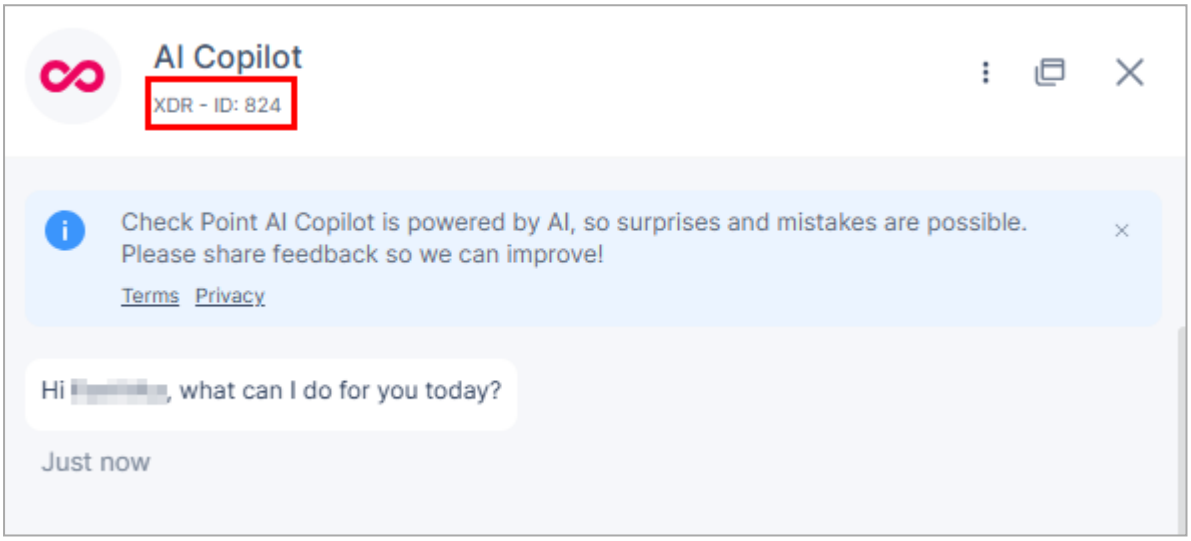
Sample Prompts

- How should I investigate this incident?
- What is Phishing?
- How to add an IOC to IOC management?
- What is Threat Hunting?
- What is lateral movement?
- What is Emotet?
- How to integrate MS Defender with XDR?

- Show the top IP addresses the machine <machine name> communicated with since the start of the year?
- What is T1053? Was it seen exploited in my environment?
- What was the RCA of this incident?

Incident Specific Query and Action

When in a specific incident, you can ask the copilot questions about that incident and its details, from all the tabs (for example, **Insights & Forensics**, **Affected assets** and so on) within the incident. The system opens the AI Copilot for the specific incident.



Sample Prompt for Queries on an Incident

- Can you summarize this incident?
- What immediate actions are recommended?
- Which assets were affected?
- What are the key IOCs identified?