

# Release Notes

FortiNDR Cloud 2024



**FORTINET DOCUMENT LIBRARY**

<https://docs.fortinet.com>

**FORTINET VIDEO LIBRARY**

<https://video.fortinet.com>

**FORTINET BLOG**

<https://blog.fortinet.com>

**CUSTOMER SERVICE & SUPPORT**

<https://support.fortinet.com>

**FORTINET TRAINING & CERTIFICATION PROGRAM**

<https://www.fortinet.com/training-certification>

**FORTINET TRAINING INSTITUTE**

<https://training.fortinet.com>

**FORTIGUARD LABS**

<https://www.fortiguard.com>

**END USER LICENSE AGREEMENT**

<https://www.fortinet.com/doc/legal/EULA.pdf>

**FEEDBACK**

Email: [techdoc@fortinet.com](mailto:techdoc@fortinet.com)



February 27, 2025

FortiNDR Cloud 2024 Release Notes

78-242-1113279-20250227

# TABLE OF CONTENTS

<b>FortiNDR Cloud release notes</b> .....	<b>5</b>
<b>Version history</b> .....	<b>6</b>
11 December version 2024.11.0 .....	6
New functionality .....	7
Improved functionality .....	12
Other improvements / changes .....	13
05 November 2024 version 2024.10.0 .....	14
New terminology .....	14
New functionality .....	15
Improved functionality .....	16
Other improvements and updates .....	19
25 September 2024 version 2024.9.0 .....	20
New functionality .....	20
Improved functionality .....	21
09 September 2024 version 2024.8.1 .....	26
28 August 2024 version 2024.8.0 .....	26
New functionality .....	26
Improved functionality .....	29
Other improvements .....	34
31 July 2024 version 2024.7.0 .....	35
Improved functionality .....	35
Other improvements .....	38
26 June 2024 version 2024.6.0 .....	39
Improved functionality .....	39
Other improvements .....	43
29 May 2024 version 2024.5.0 .....	43
Improved functionality .....	44
Other improvements .....	45
15 May 2024 version 2024.4.1 .....	46
Improved functionality .....	46
01 May 2024 version 2024.4.0 .....	46
New functionality .....	47
Other improvements .....	49
10 April 2024 version 2024.3.1 .....	49
Improved functionality .....	49
27 March 2024 version 2024.3.0 .....	49
New Functionality .....	49
Improved Functionality .....	51
13 March 2024 version 2024.2.1 .....	53
Improved Functionality .....	54
29 February 2024 version 2024.2.0 .....	54
New Functionality .....	54
Improved Functionality .....	57
Status definitions .....	57

---

Discontinued Functionality .....	58
14 February 2024 version 2024.1.1 .....	59
31 January 2024 Version 2024.1.0 .....	59
Improved functionality .....	59
<b>New detection rules and observations .....</b>	<b>61</b>
2024.11.0 .....	61
2024.10.0 .....	61
2024.9.0 .....	61
2024.8.0 .....	62
2024.5.0 .....	62
2024.4.0 .....	63
2024.3.1 .....	63
2024.3.0 .....	63
2024.2.0 .....	64
<b>Resolved issues .....</b>	<b>65</b>
2024.11.0 .....	65
2024.10.0 .....	65
2024.9.0 .....	65
2024.8.1 .....	66
2024.8.0 .....	66
2024.7.0 .....	66
2024.6.0 .....	67
2024.5.0 .....	67
2024.4.1 .....	68
2024.4.0 .....	68
2024.3.1 .....	68
2024.3.0 .....	69
2024.2.1 .....	69
2024.2.0 .....	69
2024.1.1 .....	70
2024.1.0 .....	70

# FortiNDR Cloud release notes

This document provides information about FortiNDR Cloud releases.

FortiNDR Cloud is a SaaS network security monitoring platform designed to facilitate rapid detection, investigations, and threat hunting within your environment. FortiNDR Cloud is designed to be scalable and to remove the responsibilities of maintaining tooling from security analysts. For more information, see the [FortiNDR Cloud User Guide](#).

# Version history

Date	Version
11 December 2024	11 December version 2024.11.0 on page 6
05 November 2024	05 November 2024 version 2024.10.0 on page 14
25 September 2024	25 September 2024 version 2024.9.0 on page 20
09 September 2024	09 September 2024 version 2024.8.1 on page 26
28 August 2024	28 August 2024 version 2024.8.0 on page 26
31 July 2024	31 July 2024 version 2024.7.0 on page 35
26 June 2024	26 June 2024 version 2024.6.0 on page 39
29 May 2024	29 May 2024 version 2024.5.0 on page 43
15 May 2024	15 May 2024 version 2024.4.1 on page 46
01 May 2024	01 May 2024 version 2024.4.0 on page 46
10 April 2024	10 April 2024 version 2024.3.1 on page 49
27 March 2024	27 March 2024 version 2024.3.0 on page 49
13 March 2024	13 March 2024 version 2024.2.1 on page 53
29 February 2024	29 February 2024 version 2024.2.0 on page 54
14 February 2024	14 February 2024 version 2024.1.1 on page 59
31 January 2024	31 January 2024 Version 2024.1.0 on page 59

## 11 December version 2024.11.0

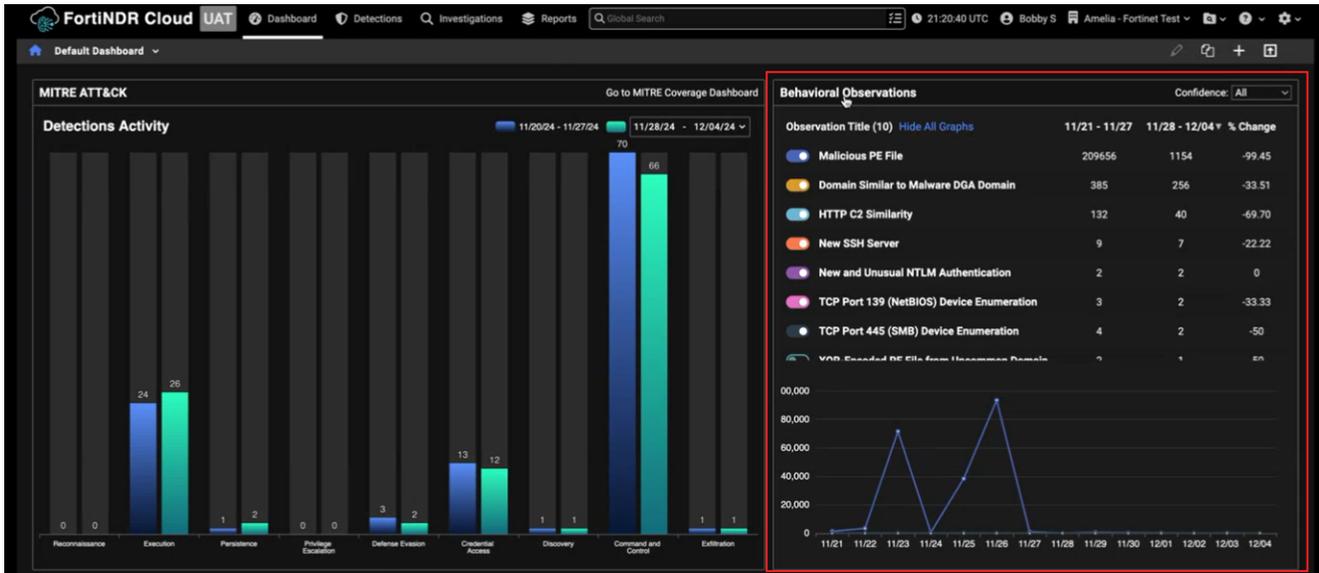
- New functionality
  - Dashboard
    - Behavioral Observations
  - Investigations
    - SNMP queries
- Improved functionality
  - Sensors
  - Tags
  - Reports
- Other improvements

## New functionality

### Dashboard

### Behavioral Observations

The *Observations* widget in the dashboard has been replaced with the *Behavioral Observations* widget.

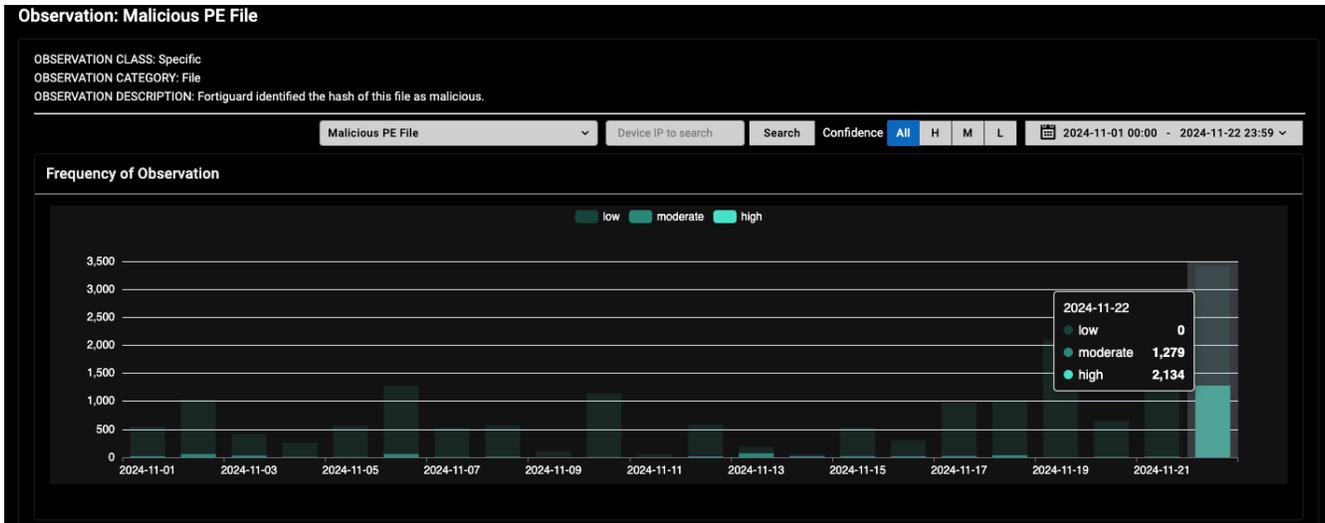


Click the widget title to open the *Behavioral Observations* list page. You can use the search field to find observations that contain instances of a specific IP address or text in the *Observation Title* and *Description* columns.

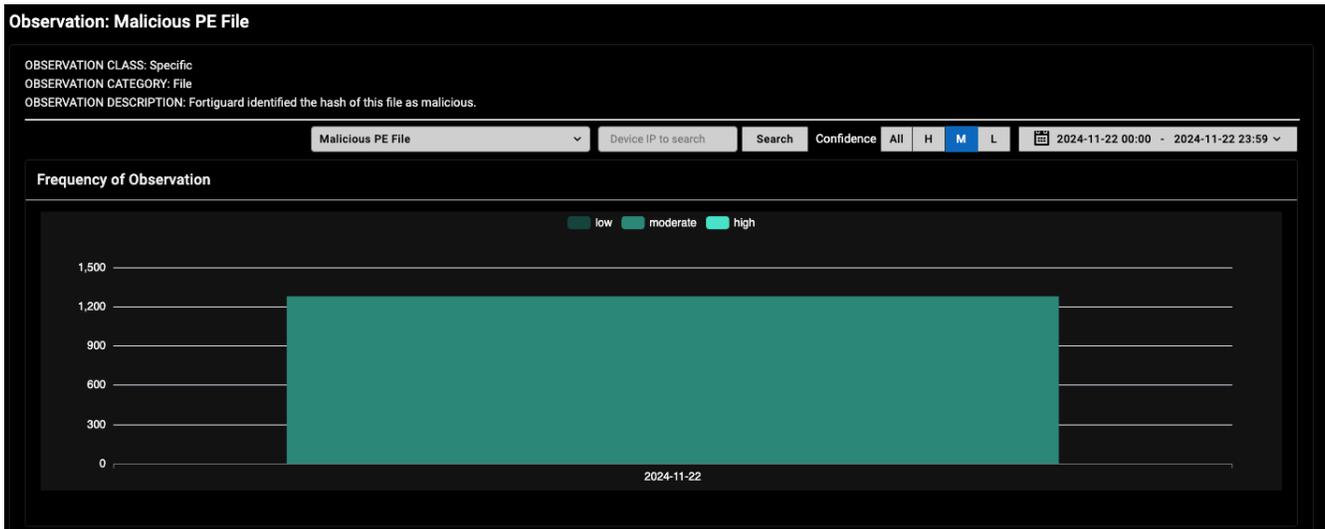
The screenshot shows the 'Behavioral Observations' list page. The table below contains the data displayed in the screenshot.

Observation Title	Confidence	Category	Class	Instances	First Seen	Last Seen	Description
Domain Similar to Malware DGA Domain	LOW	asset	specific	638	2024-11-21 01:29:51 Z	2024-12-04 20:35:03 Z	A domain was observed that is similar to what
Domain Similar to Malware DGA Domain	MOD	asset	specific	3	2024-11-22 03:01:44 Z	2024-12-04 14:32:24 Z	A domain was observed that is similar to what
High Count of Distinct Domain Names associated with Unusual Second-Level Domain	LOW	relationship	specific	1	2024-11-26 08:25:31 Z	2024-11-26 08:25:31 Z	A high count of distinct domain names associa
HTTP C2 Similarity	LOW	relationship	specific	159	2024-11-21 01:03:29 Z	2024-12-04 21:35:47 Z	HTTP connections were observed that resembl
HTTP C2 Similarity	MOD	relationship	specific	12	2024-11-22 05:45:09 Z	2024-12-02 17:00:26 Z	HTTP connections were observed that resembl
HTTP C2 Similarity	HIGH	relationship	specific	1	2024-11-24 05:30:05 Z	2024-11-24 05:30:05 Z	HTTP connections were observed that resembl
Malicious PE File	MOD	file	specific	12000	2024-11-21 07:36:22 Z	2024-12-03 21:01:07 Z	Fortiguard identified the hash of this file as mal
Malicious PE File	HIGH	file	specific	198810	2024-11-21 04:02:22 Z	2024-12-04 14:01:04 Z	Fortiguard identified the hash of this file as mal
New and Unusual NTLM Authentication	LOW	relationship	specific	4	2024-11-21 03:14:19 Z	2024-12-04 03:09:45 Z	Suspicious NTLM authentication was observed
New Internal Enumeration Source	LOW	relationship	specific	3	2024-11-26 01:32:52 Z	2024-11-26 01:32:52 Z	A new, internal device scanned and/or conduct
New SSH Server	HIGH	asset	newly observed	16	2024-11-21 15:39:02 Z	2024-11-28 17:13:53 Z	SSH server observed for the first time in the pa
TCP Port 139 (NetBIOS) Device Enumeration	LOW	relationship	specific	5	2024-11-24 22:14:43 Z	2024-12-01 12:53:05 Z	A single device contacted multiple hosts on TC
TCP Port 445 (SMB) Device Enumeration	LOW	relationship	specific	6	2024-11-24 22:15:09 Z	2024-12-01 12:53:29 Z	A single device contacted multiple hosts on TC
XOR-Encoded PE File from Uncommon Domain	MOD	file	specific	3	2024-11-21 20:50:56 Z	2024-11-29 18:49:29 Z	A single-byte XOR-encoded PE file was observe

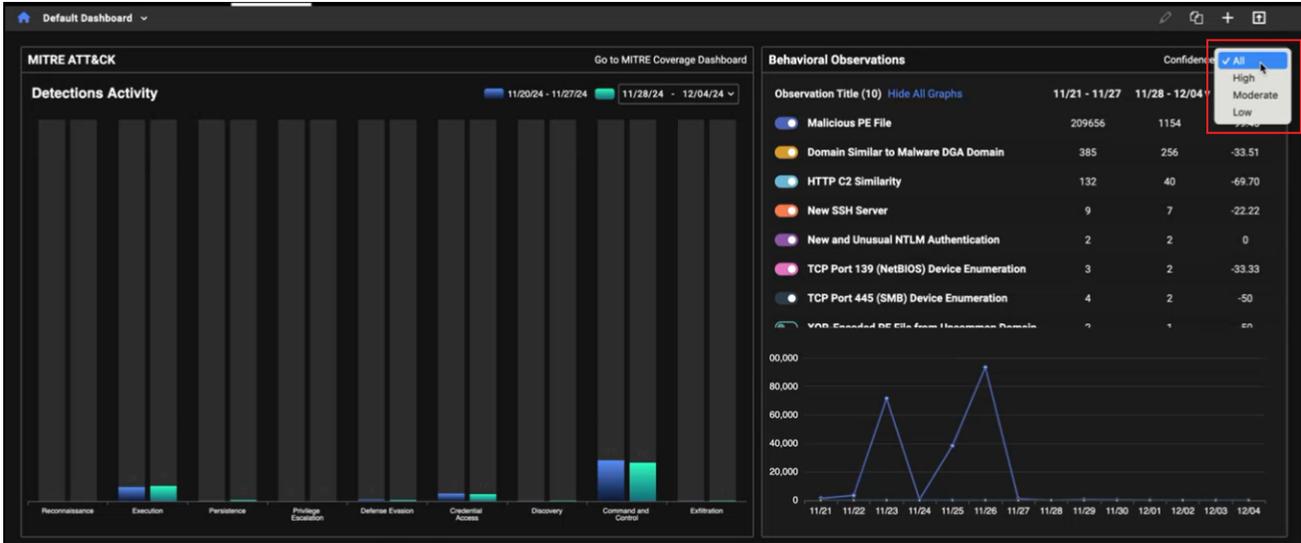
When you click an individual observation in the dashboard widget, it will open the *Observation Details* page.



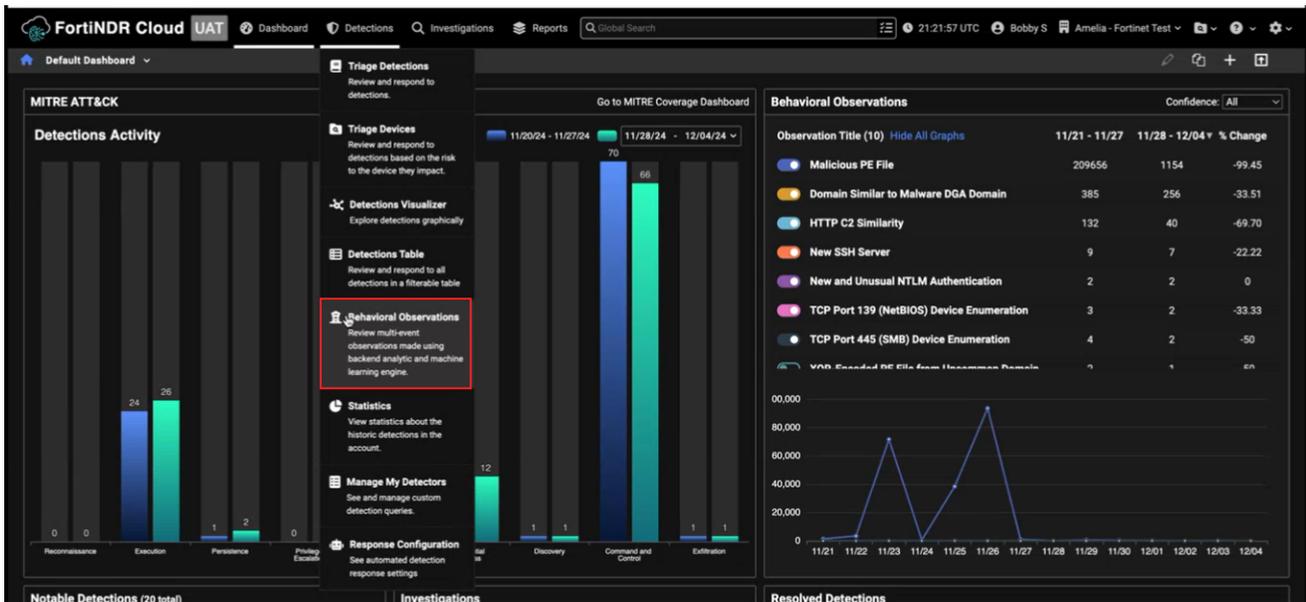
When you click on any part of the observation frequency chart, the time range and confidence filter for that part of the chart will be applied to the page.



You can filter the observations in the widget by confidence level. When you click an observation with that confidence level in the filter, the observations in the details page will reflect that confidence level.



*Behavioral Observations* have also been added to the *Detections* menu which takes you to the *Behavioral Observations* list page.



An *Observations* section was also added to the *Entity Panel*.

**FortiNDR Cloud UAT** Dashboard | Detections | Investigations | Reports | Global Search | 21:30:06 UTC | Bobby S | Amelia - Fortinet Test

**Behavioral Observations > HTTP C2 Similarity**

**Observation: HTTP C2 Similarity**

OBSERVATION CLASS: Specific  
OBSERVATION CATEGORY: Relationship  
OBSERVATION DESCRIPTION: HTTP connections were observed that resemble malware command & control (C2) traffic.

HTTP C2 Similarity | Device IP to search | Search | Confidence: All | H | M | L | 2024-11-21 00:00 - 2024-12-05 21:29

**Frequency of Observation**

low moderate high

**Observation Instances**

Showing most recent 159 out of 159 event(s) | Filter current observation results | Filter

Timeframe	Src	Dst	Confidence	Evidence Iq1	Host
2024-12-04 21:35:47 Z	10.10.1.117	application	Low	event_type = "http" AND src.ip = "10.10.1.117" ...	dl.mycommerce.com
2024-12-04 15:32:53 Z	10.10.1.111	log-pw	Low	event_type = "http" AND src.ip = "10.10.1.111" ...	www.aleov.com
2024-12-04 10:58:42 Z	10.10.1.110	eniron	Low	event_type = "http" AND src.ip = "10.10.1.110" ...	www.aleov.com
2024-12-03 23:34:03 Z	10.10.1.110	eniron	Low	event_type = "http" AND src.ip = "10.10.1.110" ...	bejnz.com
2024-12-03 18:30:58 Z	10.10.1.110	eniron	Low	event_type = "http" AND src.ip = "10.10.1.110" ...	bejnz.com
2024-12-03 16:15:09 Z	10.10.1.118	application	Low	event_type = "http" AND src.ip = "10.10.1.118" ...	dl.mycommerce.com
2024-12-03 13:43:31 Z	10.10.1.114	eniron	Low	event_type = "http" AND src.ip = "10.10.1.114" ...	dl.mycommerce.com
2024-12-03 11:22:10 Z	10.10.1.110	eniron	Low	event_type = "http" AND src.ip = "10.10.1.110" ...	dl.mycommerce.com
2024-12-03 10:54:34 Z	10.10.1.114	eniron	Low	event_type = "http" AND src.ip = "10.10.1.114" ...	dl.mycommerce.com
2024-12-03 08:38:56 Z	10.10.1.114	eniron	Low	event_type = "http" AND src.ip = "10.10.1.114" ...	bejnz.com
2024-12-02 19:55:16 Z	10.10.1.98	eniron	Low	event_type = "http" AND src.ip = "10.10.1.98" A...	systemexplorer.net
2024-12-02 16:47:27 Z	10.10.1.114	eniron	Low	event_type = "http" AND src.ip = "10.10.1.114" ...	www.aleov.com

**Summary**

Connections from 0 internal devices yesterday

First seen: 2023-05-08 17:46:29 UTC  
Last seen: 2024-12-05 21:23:11 UTC  
Risk score: 10.0  
Annotations:

application: dl | owner: owner

Add an Annotation | Modify Annotations

VirusTotal  
No VirusTotal Results Found

FortiManager

CrowdStrike Falcon  
Not installed on this Host

WHOIS >  
Updated: 1995-06-01 00:00:00 UTC

Filter Results by Date  
2024-11-21 - 2024-12-05

PDNS  
No PDNS Results Found

Detections  
No Detections Found

**Observations >**  
7 Observations

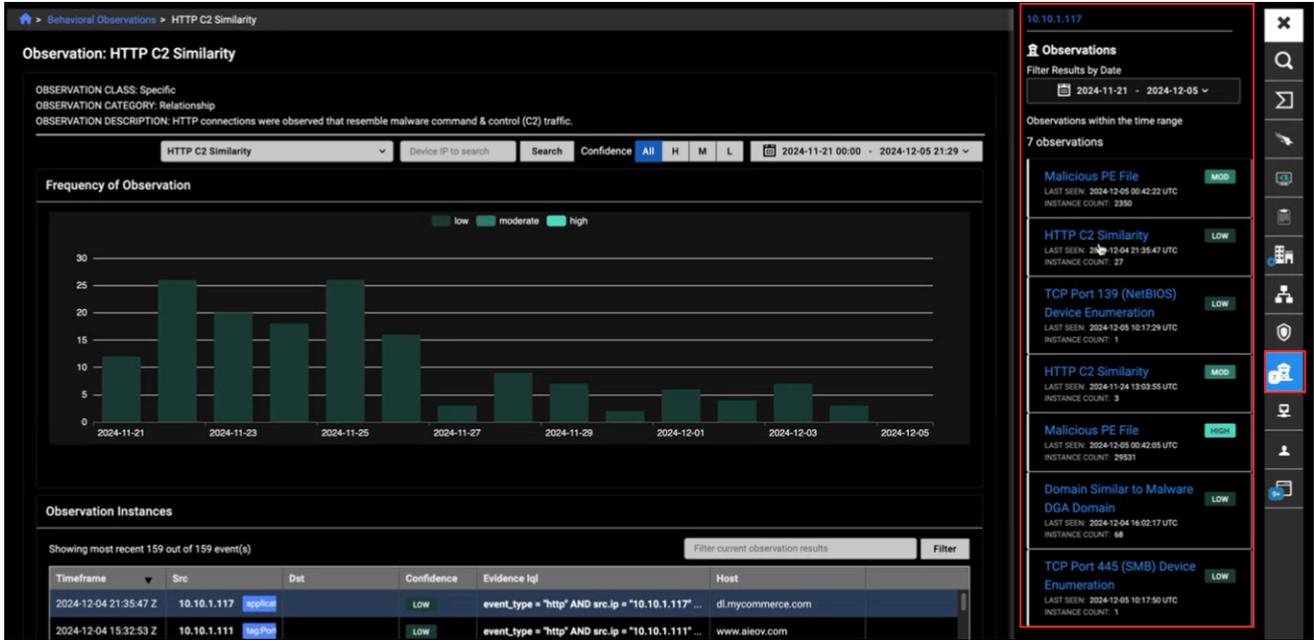
DHCP  
No DHCP Records Found

Accounts  
No Accounts Found

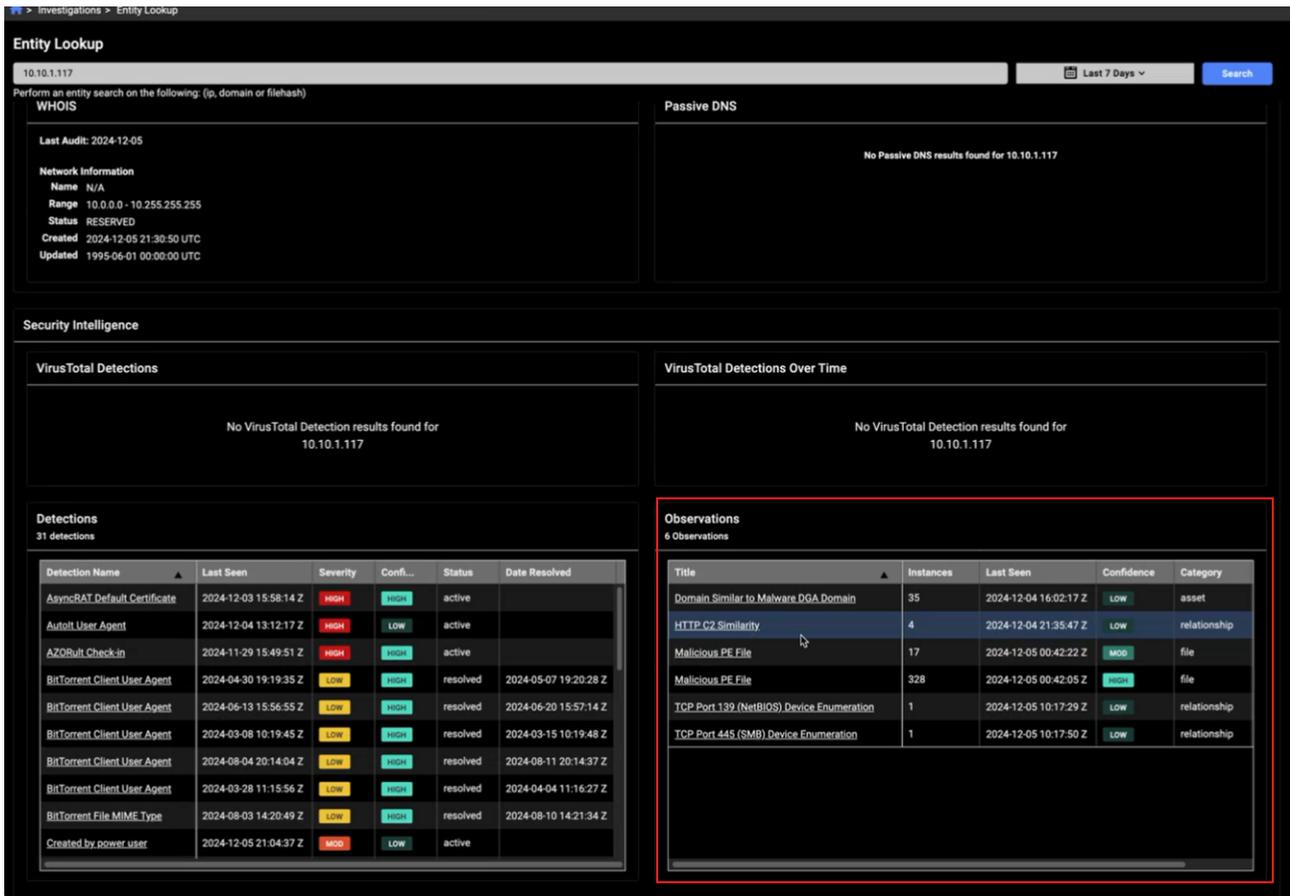
Software >  
133 Software Records

Search Events | Create PCAP

Click the link, or the *Observations* icon to view the observations in the panel. When you click on an observation in the list it will open the *Observation Details* page.



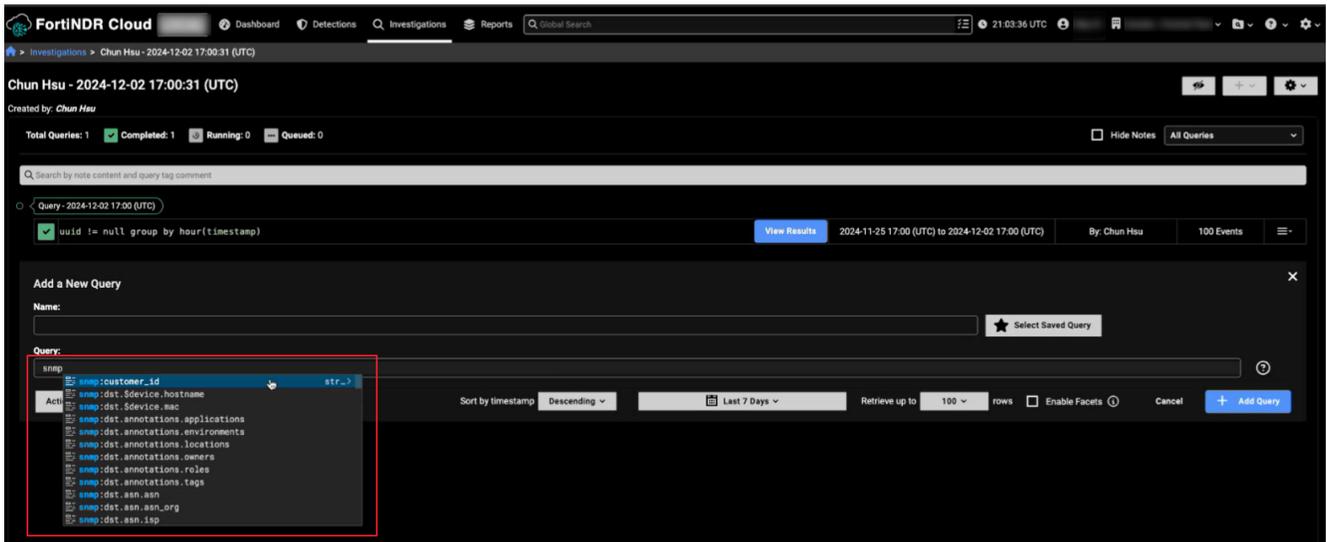
An *Observations* table was also added to the *Entity Lookup* page which shows the observations for the IP within the specified time range. When you click on the observation name in the table it will open the *Observation Details* page preserving the time range and confidence level.



## Investigations

### SNMP queries

FortiNDR Cloud now supports SNMP event queries.

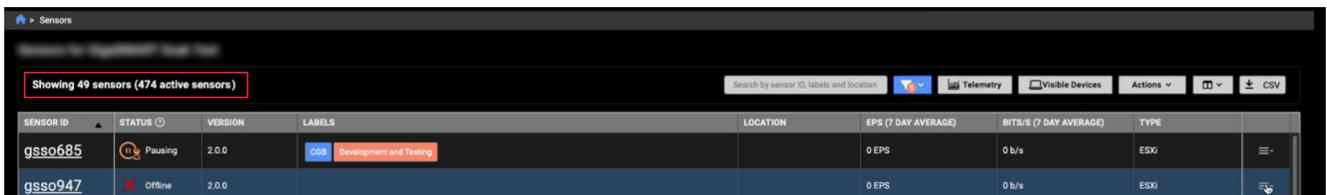


## Improved functionality

### Sensors

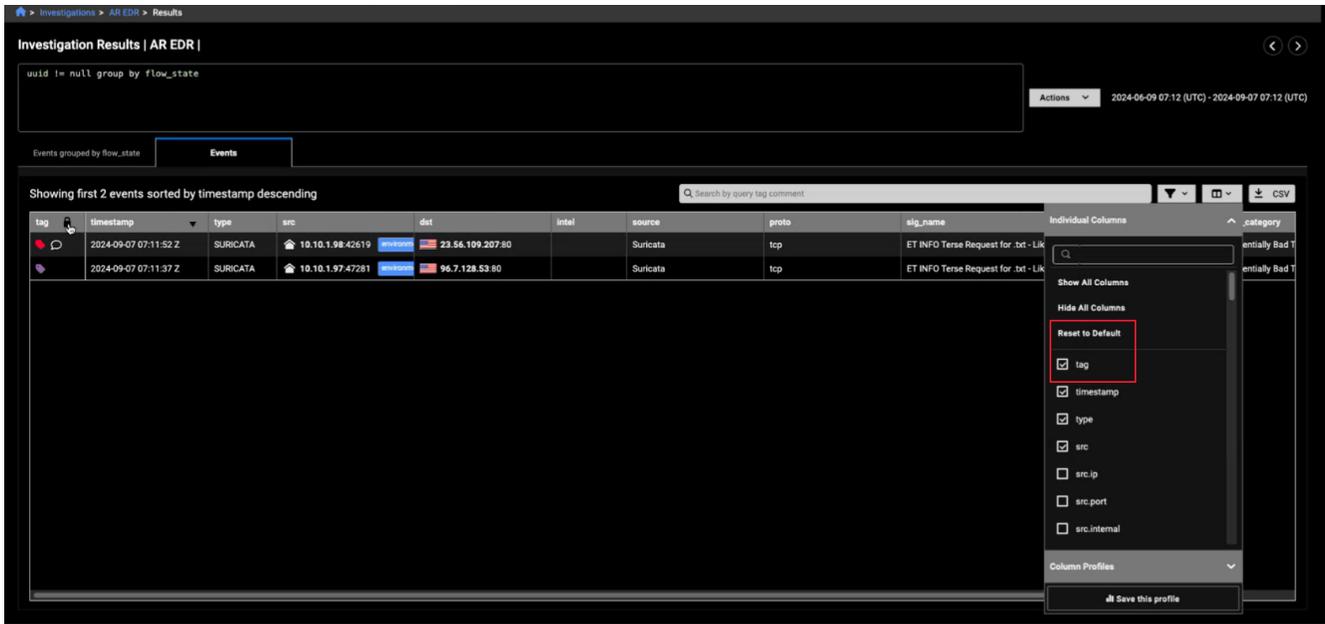
In sensors running version 2.0 or later, we have introduced a *Pausing* and *Resuming* state to indicate the sensor is in the process of being paused or resumed.

We have also added context to the number of sensors to indicate the number of sensors and the number of active sensors.



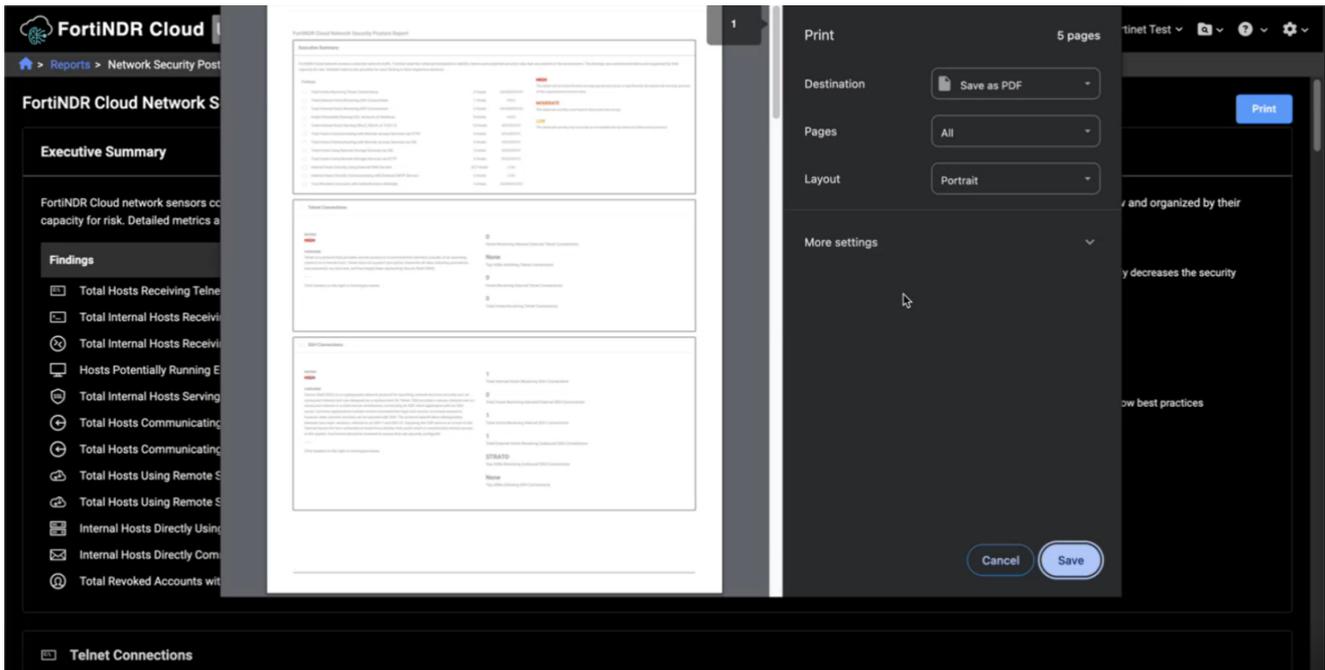
### Tags

We have improved the behavior of the *Tags* column in *Investigations* to make it is easier to find. To lock the *tag* column to the left side of the table, in the *Individual columns* filter under *Individual Columns*, select *Reset to Default* or *tag*. You can also lock the column by selecting *Default* under the *Column Profile* in the same menu.



## Reports

We have added a *Print* button and print dialog with preview for PDF reports.



## Other improvements / changes

- The *Default width* setting has been renamed *Header width* in the *Investigations* tab in the column headers.
- You can now sort all the columns in the *Annotations* table by clicking the column header.

- We redesigned the tooltip in the *Entity Lookup* to include a scroll bar to fit the page.

## 05 November 2024 version 2024.10.0

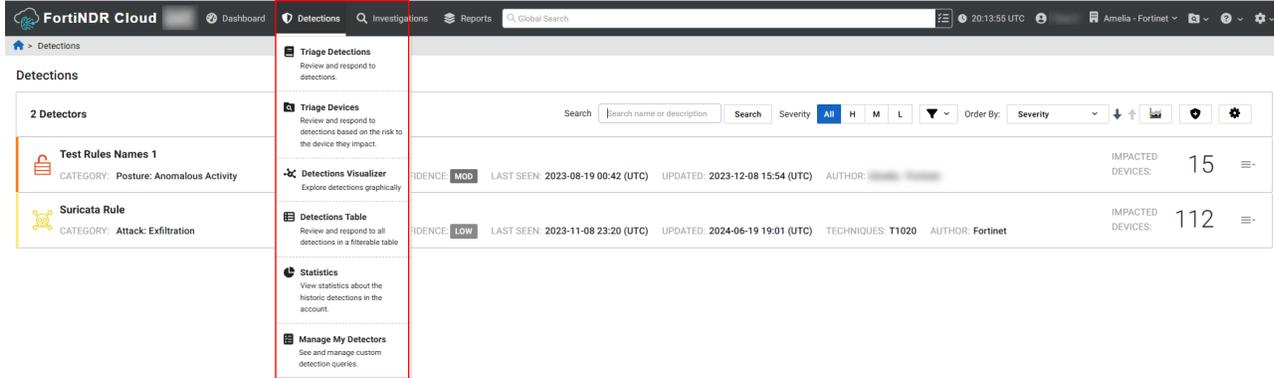
- New terminology
- New functionality
  - Login with FortiCloud
- Improved functionality
  - Sensors
  - Account Management
  - Detections
  - Global Search
- Other improvements and updates

### New terminology

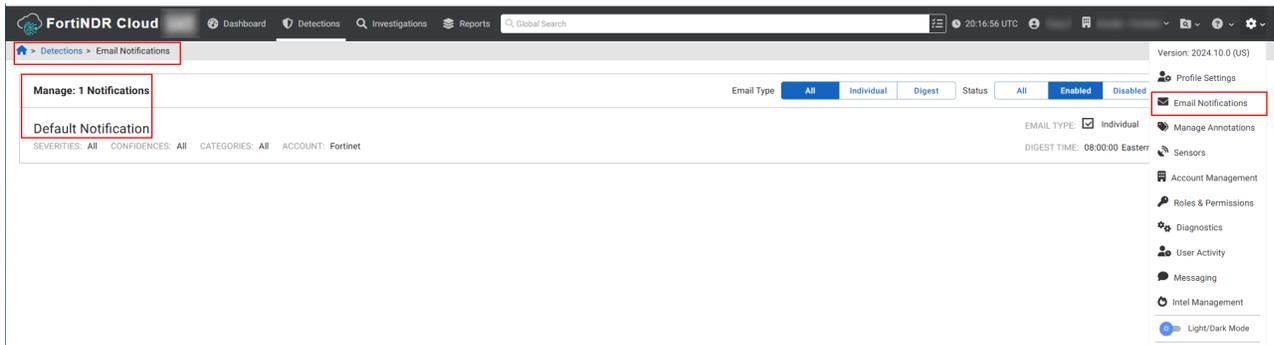
We have updated our terminology to be consistent with standard industry terms so that our documentation and user interface is more intuitive and accessible.

Please be aware we have changed the names of several modules in the portal:

- *Rules* are now referred to as *Detections* or *Detectors*.



- *Subscriptions* are now *Notifications*.



## Version history

- *Signatures* are now referred to as *Query* or *Queries*.

The screenshot shows the 'Test Rules Names 1' detection page. At the top right, it indicates 'SEVERITY: MOD' and 'CONFIDENCE: MOD'. On the right side, it shows 'DEVICES IMPACTED' with a monitor icon and the number '15'. The 'Description' section is titled 'Test rule'. Below this, there are buttons for 'Start Investigation' and 'View Related Investigations'. Further down, there are fields for 'RUNNING ACCOUNTS: Amella - Fortinet', 'AUTHOR: Amella - Fortinet', and 'IMPACTED DEVICE FIELDS: src ip and/or dst.ip'. At the bottom, there are tabs for 'Impacted Devices', 'Query' (highlighted with a red box), 'Events', 'Indicators', and 'Detections Graph'. There is also an 'Add a Custom Filter' button.

- *Playbooks* are now named *Guided Queries*.

The screenshot shows the 'Investigations' section of the FortiNDR Cloud interface. On the left, there is a search bar and a list of investigations. On the right, there is a table of investigations. The 'Guided Queries' option is highlighted with a red box. The table has columns for 'Name', 'Created by', 'Date Created', 'Date Updated', 'Activities', 'Queries', and 'Notes'. The 'Guided Queries' row shows 5 queries and 0 notes.

Name	Created by	Date Created	Date Updated	Activities	Queries	Notes
GigaSMART Soak Test - 2024-09-18 19:44:50 (UTC)		2024-09-18 19:44 (UTC)	2024-09-18 19:44 (UTC)		0	0
Fortinet - 2024-08-29 19:16:11 (UTC)		2024-08-29 19:16 (UTC)	2024-08-29 19:31 (UTC)		1	0
Fortinet - 2024-02-12 18:49:20 (UTC)		2024-02-12 18:49 (UTC)	2024-06-28 19:38 (UTC)		5	0
Fortinet - 2024-01-10 20:55 (UTC)		2024-01-10 20:55 (UTC)	2024-03-21 19:14 (UTC)		2	0

## New functionality

### Login with FortiCloud

You can now log into the FortiNDR Cloud portal using your FortiCloud account. You must have a valid FortiCloud account that matches an existing FortiNDR Cloud account to use this option.

The screenshot shows the login page for FortiNDR Cloud. It features a logo at the top, followed by the text 'Login to FortiNDR Cloud' and 'Enter your credentials below'. There are two input fields for credentials, a 'LOGIN' button, and a 'FORTICLOUD' button. The 'FORTICLOUD' button is highlighted with a red box.

## Improved functionality

### Sensors

We have also added a new *Decommission Pending* status to the *Sensors* page.

SENSOR ID	STATUS	VERSION	TYPE	LABELS	LOCATION	EPS (7 DAY AVERAGE)	BITS/S (7 DAY AVERAGE)
eng1	Offline	Unknown	Amazon EC2			0 EPS	0 b/s
eng2	Provisioning	Unknown				0 EPS	0 b/s
eng3	Provisioning	Unknown				0 EPS	0 b/s
eng4	Provisioning	Unknown				0 EPS	0 b/s
eng7	Decommission Pending	2.0.0	sensor			0 EPS	0 b/s
eng8	Provisioning	2.0.0	sensor			0 EPS	0 b/s

### Account Management

#### PCAP encryption keys

PCAP encryption keys are now validated in the *Account Management > Settings* page.

Fortinet Account Management > Settings

STATUS: **ENABLED** MFA REQUIRED: **DISABLED** CODE: SUBSCRIPTION SERIAL NUMBER: Unknown LAST LOGIN: 2024-11-01 20:26:59 UID: USERS: 68 SENSORS: 20

SAML SSO: SAML Single Sign-on (SSO) initial setup

PCAP ENCRYPTION KEYS: Settings for packet capture

Current key: ...SCAwEAAQ== (last 10 characters)

Set PCAP Encryption Key

RSA Key - 4096 bits or larger preferred

d&dliidi

Key has an invalid header or footer

Cancel Set Key

### Accounts

A *Last Login* filter has been added to the *Accounts* page. This feature is only applicable to users with access to multiple accounts. You can use this filter to view which accounts are in use to determine if an account should be deleted.

Account Management

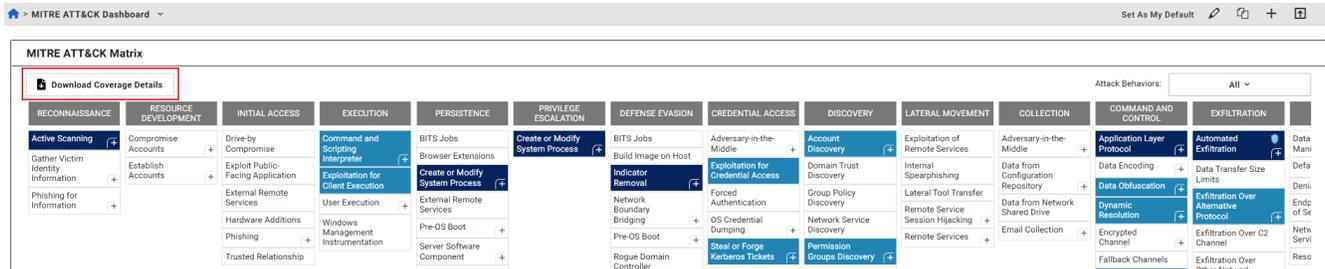
4 Accounts

Search: Search Accounts/Users

Order By: Last Login

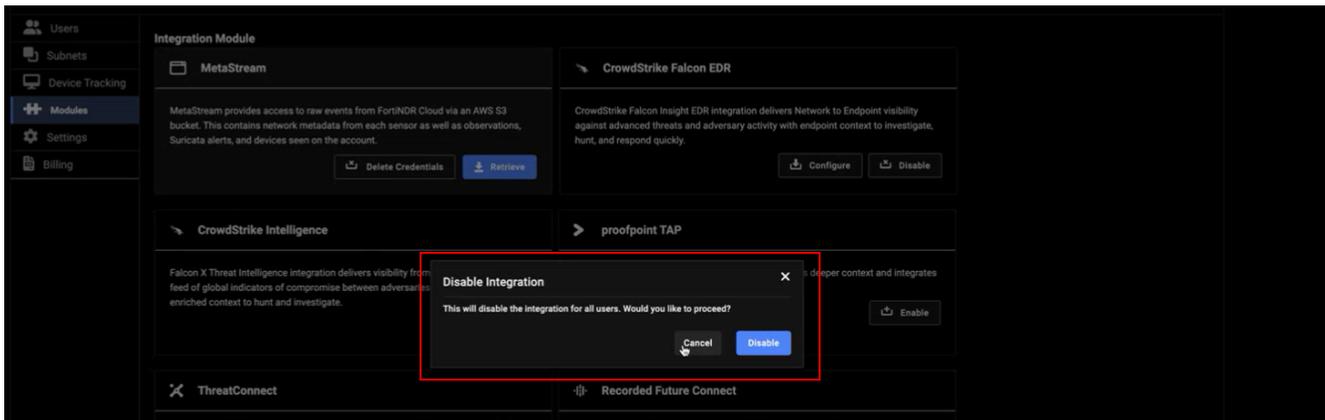
## MITRE ATT&CK Matrix

We have added a *Download Coverage Details* button to the *MITRE ATT&CK Matrix* dashboard. Click the button to download the coverage details as a CSV file which contains the *Date Updated*, *Name*, *Primary Attack ID*, *Secondary Attack ID* and *Description*.



## Modules

We have added a confirmation message when disabling an integration to prevent disabling an integration by accident.

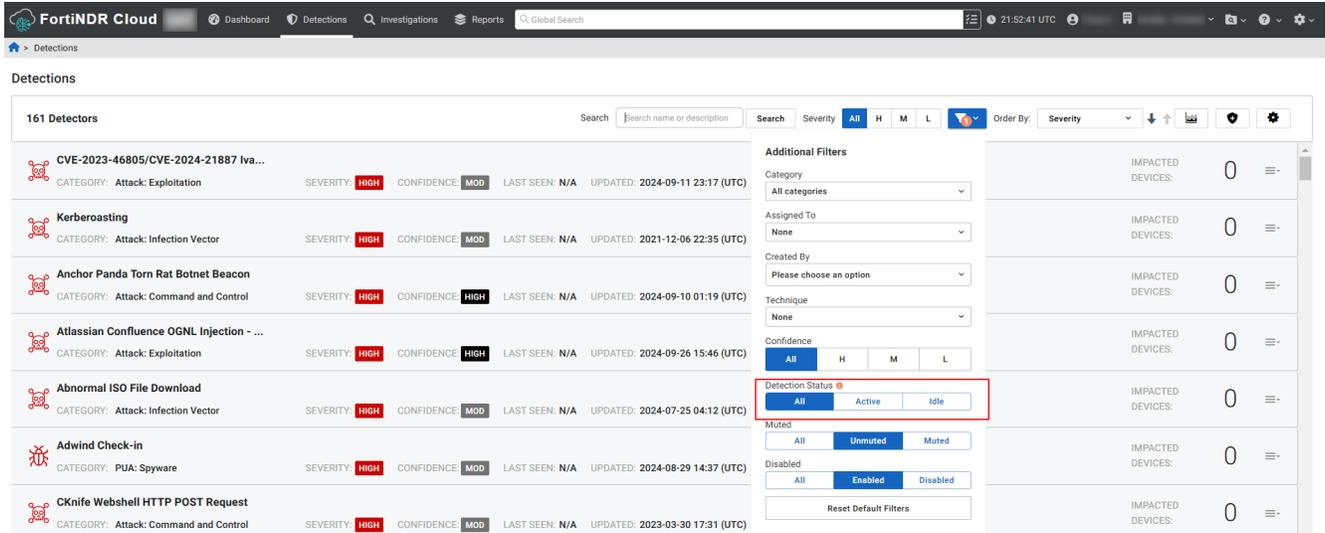


## Detections

### Triage detections

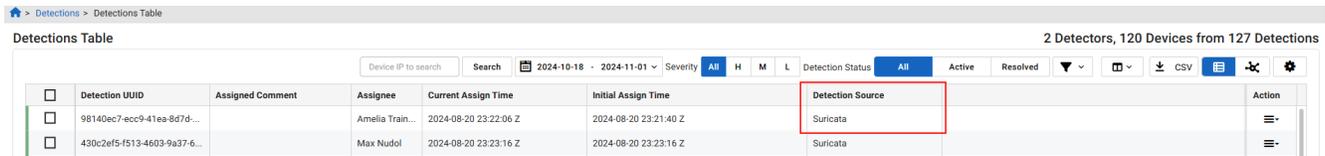
We have updated the *Detection Status* filter logic in the *Triage Detections* page:

- *All*: Returns all detections the user has access to regardless of whether or not it was triggered in the current account.
- *Idle*: Returns all detections that have been triggered in the current account but are not currently active.
- *Active*: Returns all active detections.

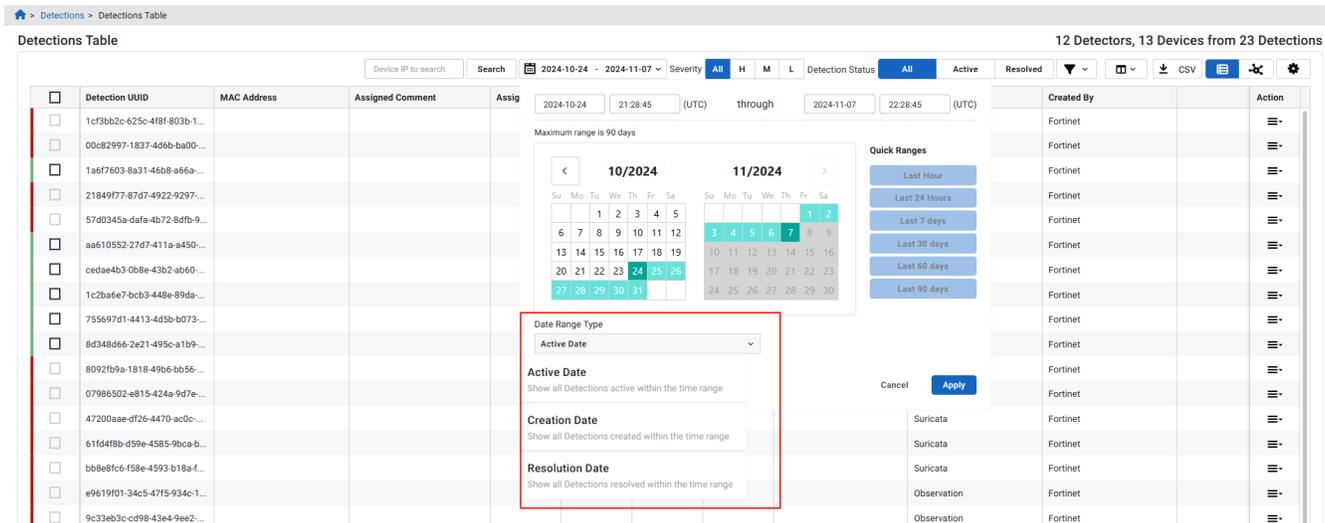


## Detections table

We have added a *Detection Source* column to the *Detections Table* which is determined by the detector's query. Note that *Suricata* and *Observation* are the only sources that are displayed at this time, otherwise the field is empty.



We have also added three new *Date Range Type* options (*Active Date*, *Creation Date*, and *Resolution Date*). The date displayed in the date picker will be displayed in the *Entity Panel*.



## Global Search

We have added a *Detections Coverage* section to the Global Search results which shows matches in the detector name, description or technique ID regardless of the detector status.

**Detections** IP address, detection name, and detection description

Device IP	Lifetime Events	Indicators	Last Seen	Status	Resolved By	Resolution	Date Resolved	Detection Name	Detection Description
...	2 Events	0 Indicators	2022-10-25 ...	Active				Suricata Rule	
...	3 Events	0 Indicators	2022-08-02 ...	Active				Suricata Rule	
...	1 Event	0 Indicators	2022-08-11 ...	Active				Suricata Rule	
...	5 Events	0 Indicators	2022-07-05 ...	Active				Suricata Rule	
...	1 Event	0 Indicators	2022-07-28 ...	Active				Suricata Rule	

**Detections Coverage** Name, description, and Mitre Technique

**Suricata Rule**  
 CATEGORY: Attack: Exfiltration SEVERITY: **Low** CONFIDENCE: **Low** LAST SEEN: 2023-11-08 23:20 (UTC) UPDATED: 2024-06-19 19:01 (UTC) TECHNIQUES: T1020 AUTHOR: Fortinet IMPACTED DEVICES: 112 MUTED: 5

**Investigations** Name, description, and comments

Name	Description	Created by	Date Created	Date Updated	Activities	Queries	Notes
Suricata Rule, ... -2023-11-20 00:5...		Unknown User	2023-11-20 00:55 (UTC)	2023-11-20 00:55 (UTC)		1	0

**Detections** IP address, detection name, and detection description

Search string does not have any IP address or matched rules

**Detections Coverage** Name, description, and Mitre Technique

<b>Windows Banner String in ICMP Request</b> CATEGORY: Attack: Command and Control	SEVERITY: <b>HIGH</b> CONFIDENCE: <b>HIGH</b>	LAST SEEN: 2024-10-16 12:44 (UTC) UPDATED: 2021-12-06 22:34 (UTC)	TECHNIQUES: T1095	AUTHOR: Fortinet	IMPACTED DEVICES: 1	MUTED: 1
<b>Executable Retrieved with Minimal HTT...</b> CATEGORY: Attack: Installation	SEVERITY: <b>HIGH</b> CONFIDENCE: <b>Low</b>	LAST SEEN: 2024-11-04 17:08 (UTC) UPDATED: 2021-12-06 22:35 (UTC)	TECHNIQUES: T1105/T1059.001	AUTHOR: Fortinet	IMPACTED DEVICES: 8	MUTED: 1
<b>Cryptocurrency Mining Client Check-in</b> CATEGORY: PUA: Unauthorized Resource Use	SEVERITY: <b>MOD</b> CONFIDENCE: <b>MOD</b>	LAST SEEN: 2024-11-03 10:16 (UTC) UPDATED: 2021-12-06 22:33 (UTC)	TECHNIQUES: T1095	AUTHOR: Fortinet	IMPACTED DEVICES: 2	MUTED: 1
<b>HTML Application (HTA) Download</b> CATEGORY: Attack: Installation	SEVERITY: <b>MOD</b> CONFIDENCE: <b>MOD</b>	LAST SEEN: 2024-10-25 17:09 (UTC) UPDATED: 2021-12-06 22:34 (UTC)	TECHNIQUES: T1105/T1218.005	AUTHOR: Fortinet	IMPACTED DEVICES: 0	MUTED: 1
<b>Executable Binary or Script Downloade...</b> CATEGORY: Attack: Installation	SEVERITY: <b>MOD</b> CONFIDENCE: <b>MOD</b>	LAST SEEN: 2024-10-25 16:43 (UTC) UPDATED: 2021-12-06 22:35 (UTC)	TECHNIQUES: T1105	AUTHOR: Fortinet	IMPACTED DEVICES: 0	MUTED: 1

**Investigations** Name, description, and comments  
No investigations found.

**Private Search** Query contents or comments  
No queries found.

## Other improvements and updates

- The *Fit Width* options has been added to the following pages:
  - Triage Detections Detail
  - Triage Device

- Detection Table
- Sensors
- User List
- the Zscaler sensor download has been removed. Zscaler integration is now via cloud upload.

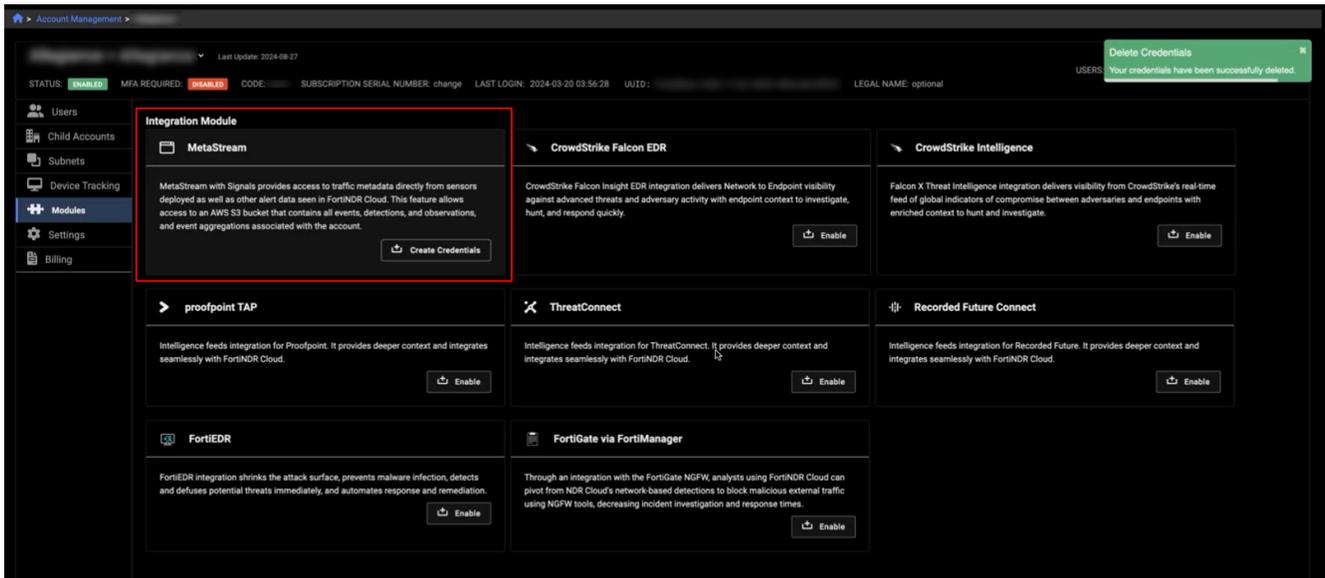
## 25 September 2024 version 2024.9.0

- New functionality
  - MetaStream Module
  - User activity timeout
- Improved functionality
  - Pivot to events
  - Sensor Telemetry
  - User Roles
  - Detection assignment
  - Manage Annotations

### New functionality

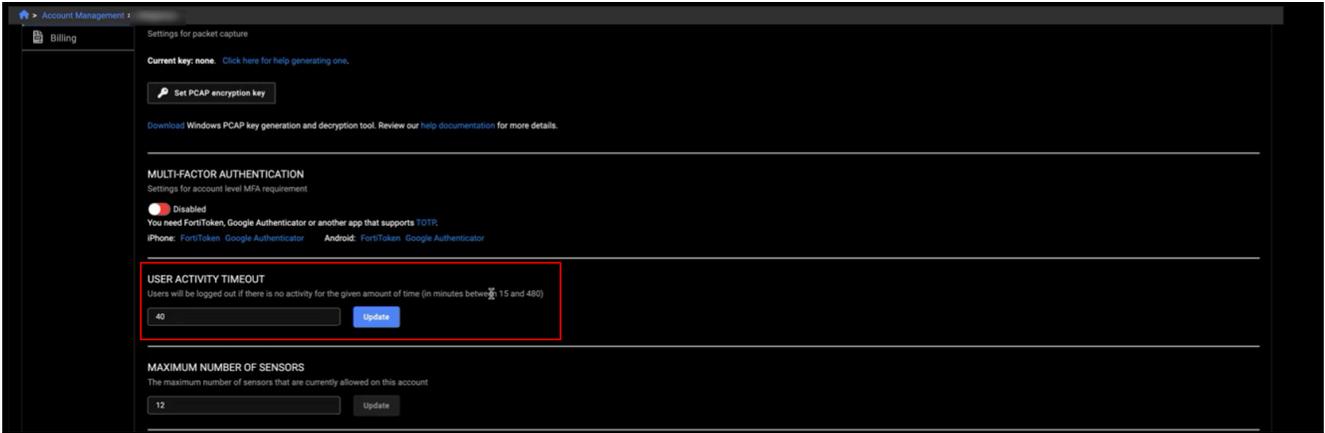
#### MetaStream Module

The *MetaStream* module is now included with all accounts. Going forward, Admins will only need to create, delete, recreate or retrieve a credential.



## User activity timeout

You can now set the amount of inactivity time before a user is automatically logged out of the portal. The new timeout time goes into effect the next time users log into the portal.



## Improved functionality

### Pivot to events

You can now click the tag icon to pivot directly to the *Events* table in an investigation. This saves time navigating to the investigation with the GUI. This function is available on all tags in the investigation tooltip, the investigation detail page, and tagged queries in the *Private Search* page.



The *Events* table will display the same number of events tagged in the investigation dialog.

Investigation Results | [redacted] - 2024-06-05 15:09:53 (UTC) |

src.ip != null group by src.ip

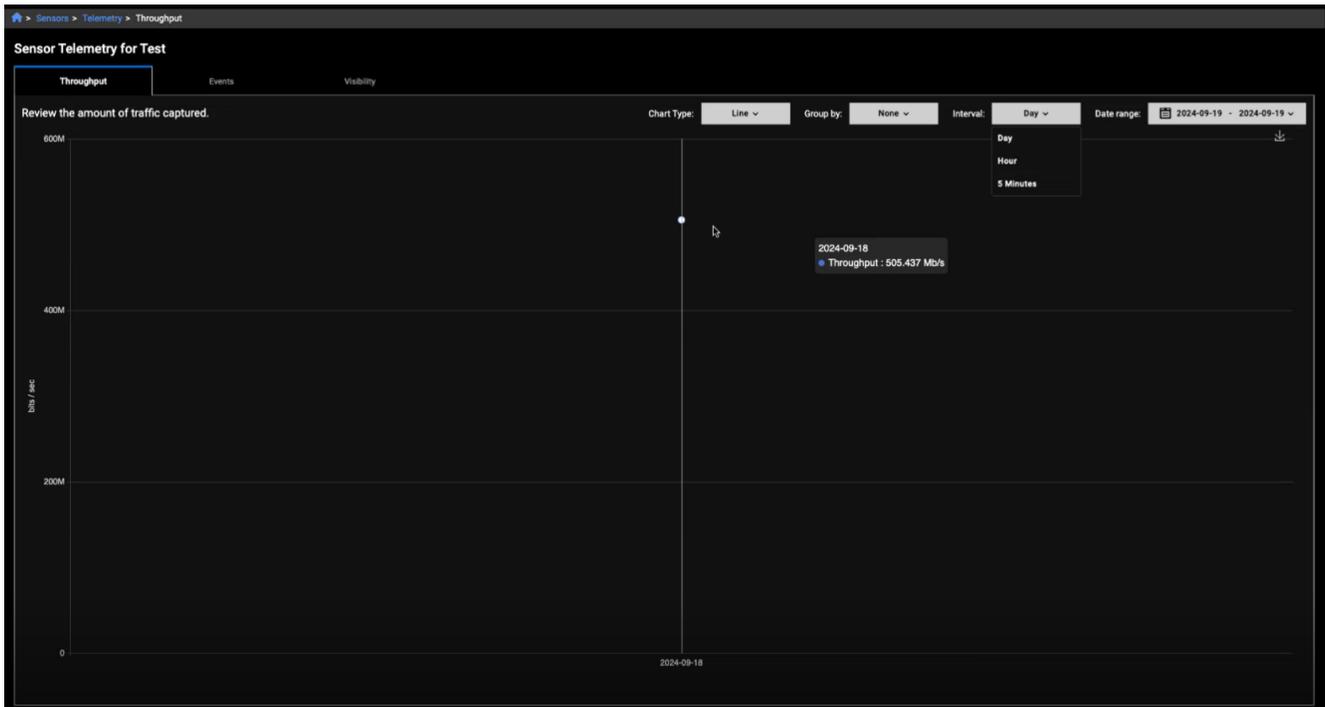
Events grouped by src.ip

Showing first 5 events sorted by timestamp descending

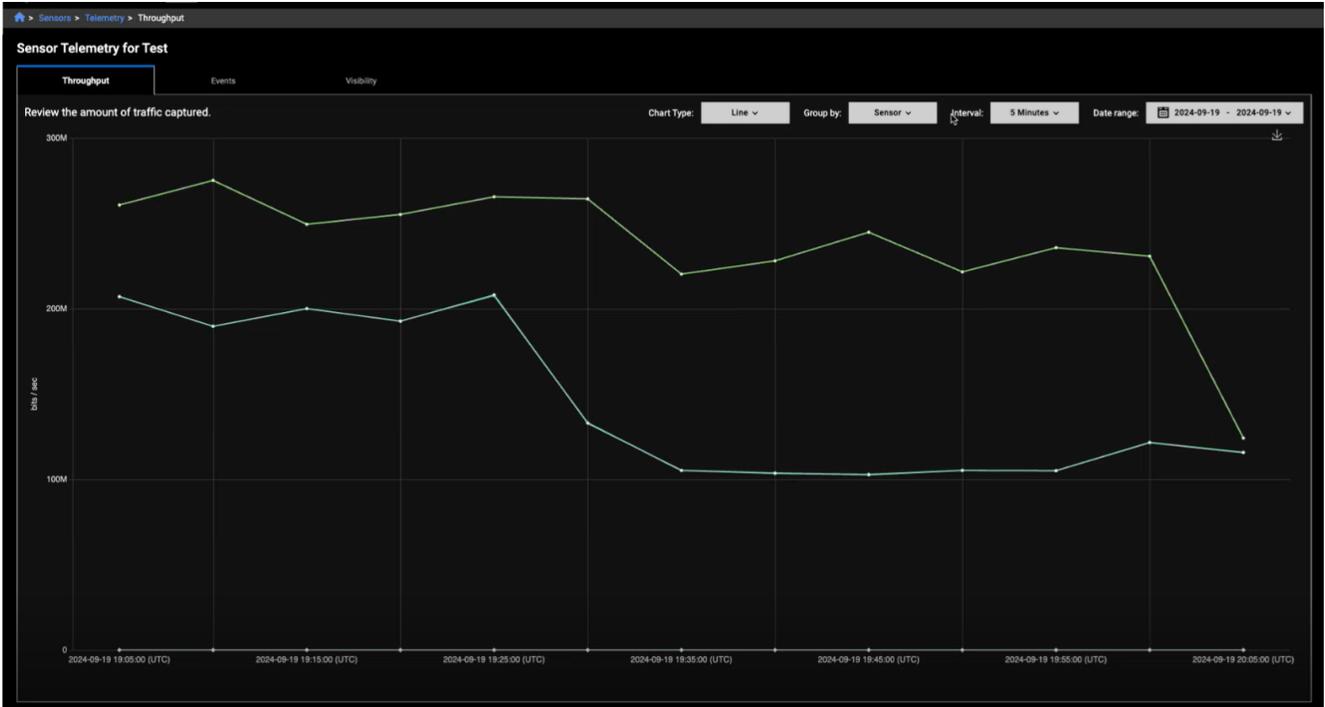
tag	timestamp	type	src	src.ip	src.port	src.internal	src.asn	src.asn.asn_org	src.asn.isp	src.asn.org	src.pkts	src.ip_byt...	src.geo.city	src.geo.country
[redacted]	2024-09-19 18:14:07 Z	SURICATA	10.10.1.97-33231	10.10.1.97	33231	True								
[redacted]	2024-09-19 18:14:02 Z	SURICATA	10.10.1.98-57458	10.10.1.98	57458	True								
[redacted]	2024-09-19 18:09:45 Z	FLOW	10.10.1.111-37372	10.10.1.111	37372	True					6	357 Bytes		
[redacted]	2024-09-19 18:09:45 Z	SURICATA	10.10.1.118-42803	10.10.1.118	42803	True								
[redacted]	2024-09-19 18:09:45 Z	SURICATA	10.10.1.118-42803	10.10.1.118	42803	True								

## Sensor Telemetry

You can now filter the sensor *Telemetry* data by *Day*, *Hour* and last *5 Minutes*.



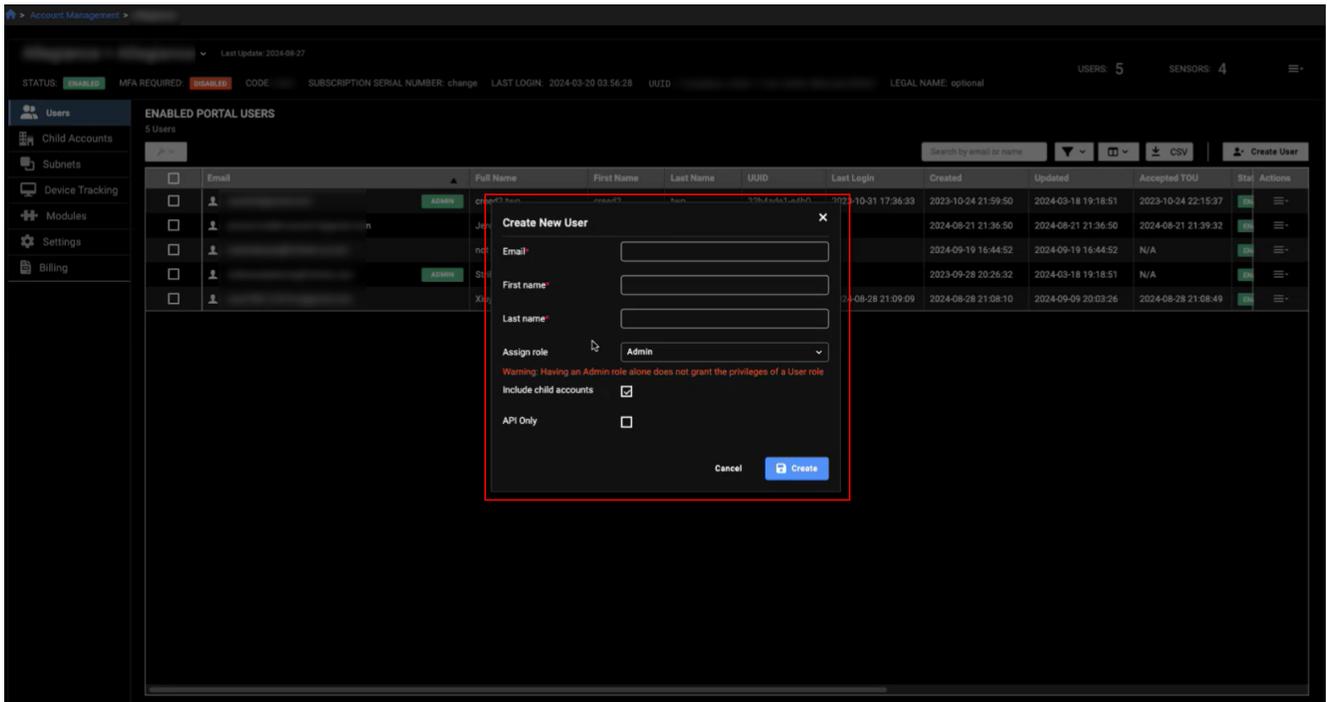
You can also group the page by *Sensor*.



## User Roles

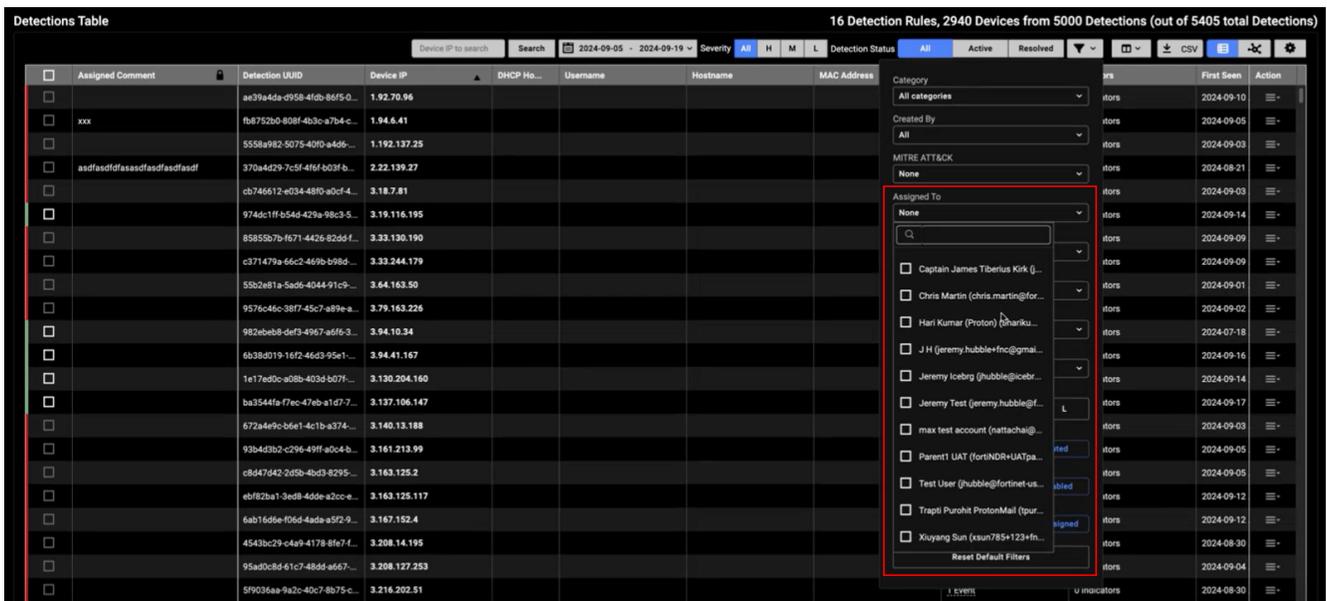
We have added a tooltip with a description of each role when you create a new user. The tooltip describes the privileges and limitations of each role and offers suggestions to make sure you are assigning the appropriate role to the user. For example, the new user may need both *Admin* and *User* roles to configure settings and perform queries. To view the description, hover over the name of the role in the dialog.

An auto-check is performed when you select the user role. A warning appears to remind you of the limitations of the role. If you choose to ignore the warning, it will not prevent you from creating the new user.



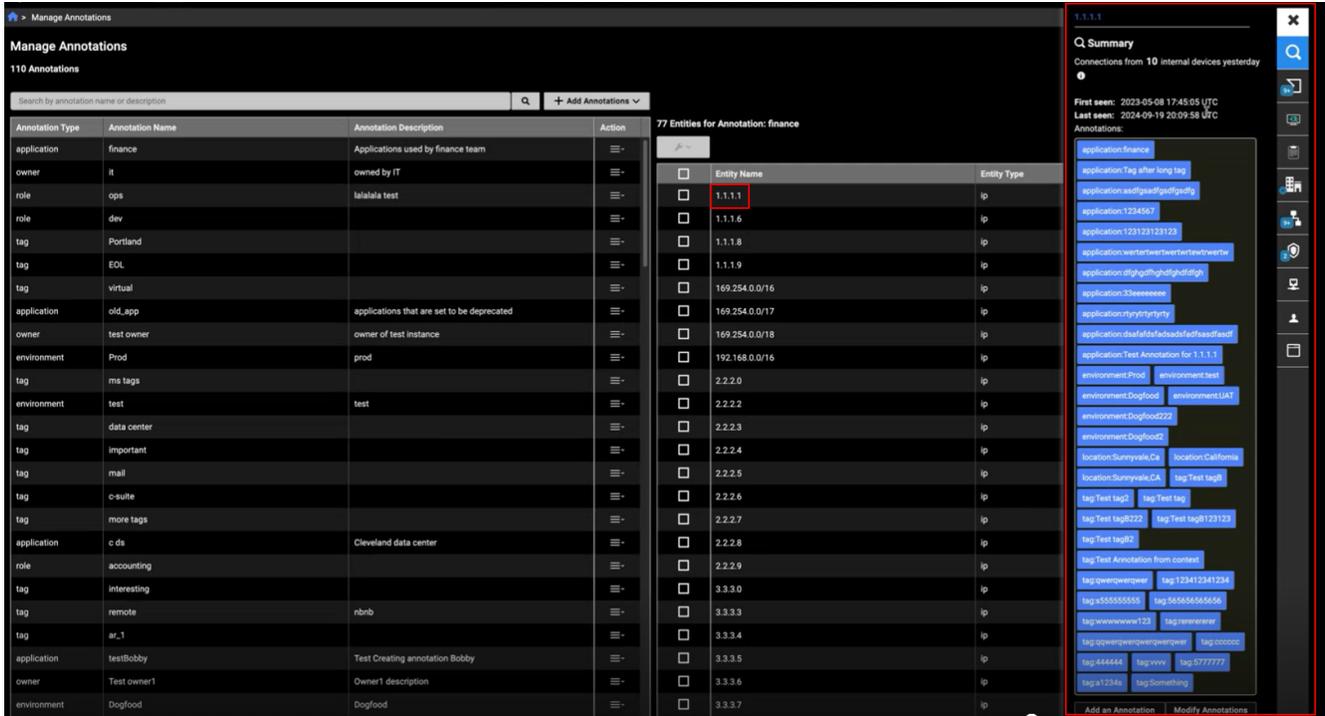
## Detection assignment

You can now assign a detection to any active user with any role in the current account. Previously you could only assign detections to active users created in the current account.

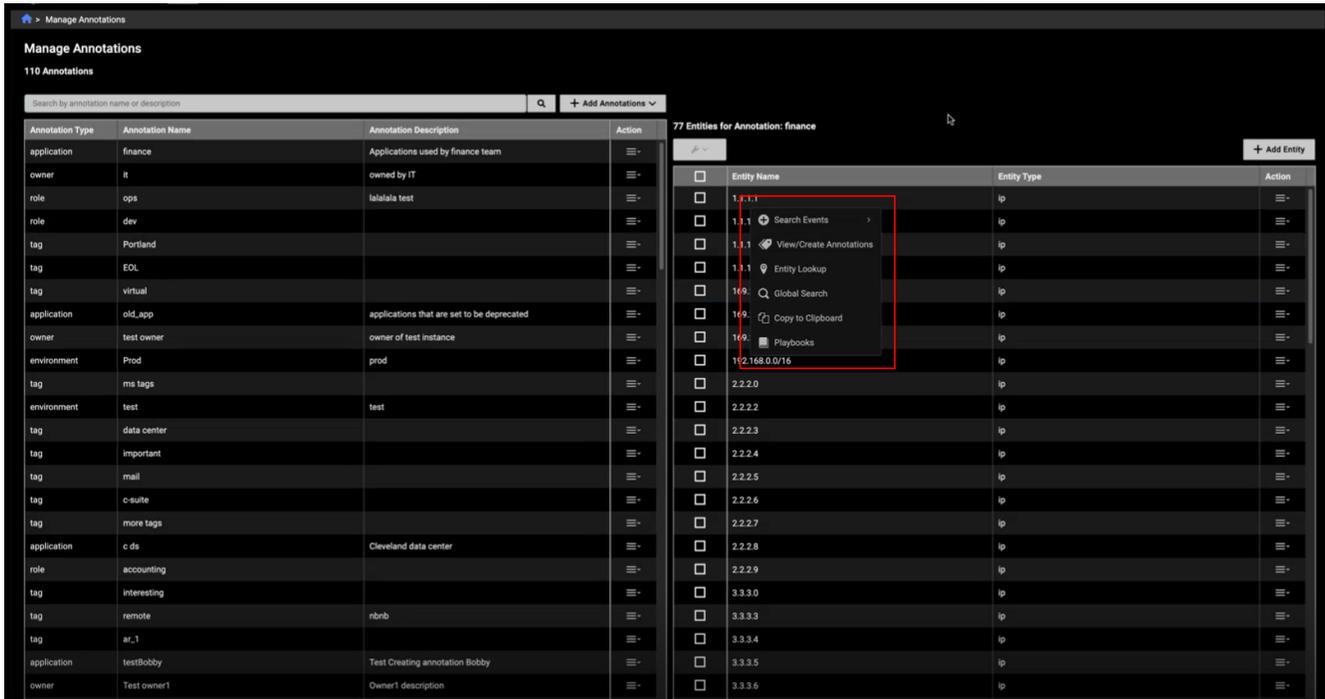


## Manage Annotations

You can now open the *Entity Panel* when you click the *Entity Name* in the *Manage Annotations* page when the entity is a valid IP, CIDR, domain, or URL.



You can also right-click the entity with a valid IP to *Search Events*, *View/Create Annotations*, perform an *Entity Lookup* and *Global Search*, or open a *Playbook*.



## 09 September 2024 version 2024.8.1

FortiNDR Cloud version 2024.8.1 includes bug fixes, but no new features. See, [Resolved issues on page 65](#).

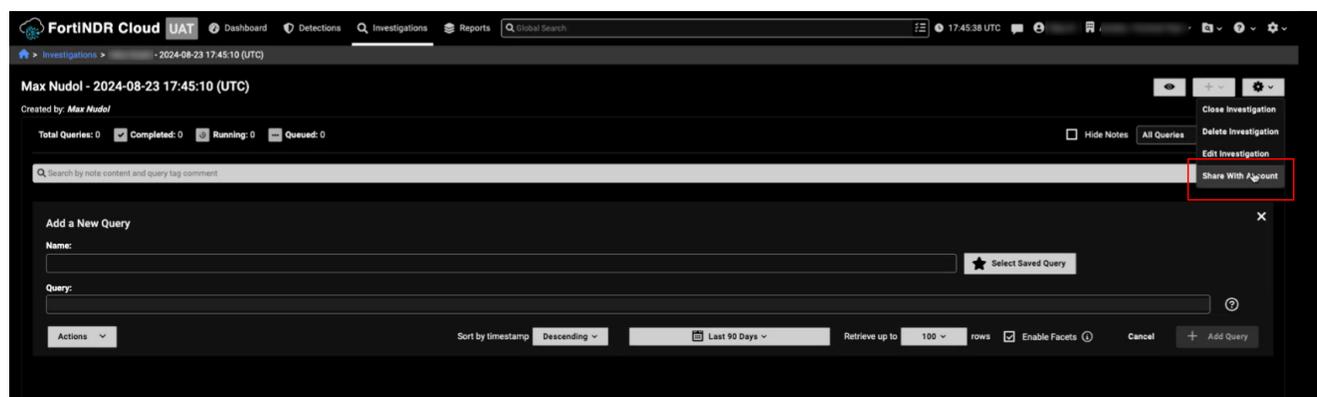
## 28 August 2024 version 2024.8.0

- New functionality on page 26
  - [Share investigations on page 26](#)
  - [Detection assignment on page 27](#)
- Improved functionality on page 29
  - [Account region on page 29](#)
  - [Events table on page 30](#)
  - [Observations widget on page 30](#)
  - [Manage Annotations on page 31](#)
  - [User management on page 32](#)
  - [Triage devices on page 33](#)
- Other improvements on page 34
  - [Detections table on page 34](#)
  - [Search Timeline on page 34](#)
  - [Integrations guides on page 34](#)

## New functionality

### Share investigations

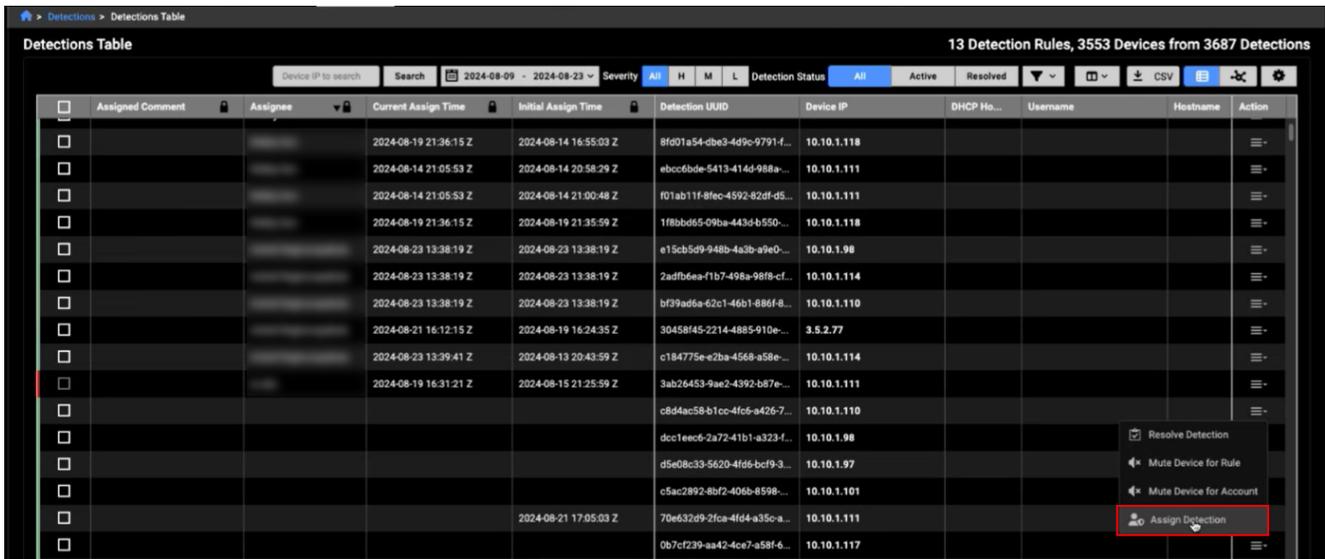
Users with multiple accounts can share investigations in their primary account with users in their secondary account. Sharing an investigation will allow all users with access to the secondary account to see and make changes to the investigation. Once the investigation is shared, it cannot be undone. For more information, see [Share investigations](#).



## Detection assignment

You can now assign active detections to a user from the *Detections Table*, *Triage Device*, and the *Triage Rules* page. For more information, see [Assigning detections](#).

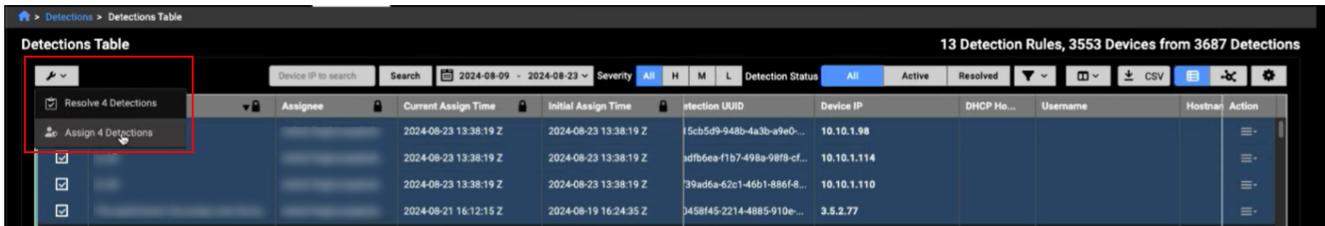
To assign a detection to a user from the *Detections Table*, click the actions menu and select *Assign Detection*.



The screenshot shows the 'Detections Table' interface. At the top, it displays '13 Detection Rules, 3553 Devices from 3687 Detections'. Below this is a search bar and filters for 'Severity' (All, H, M, L) and 'Detection Status' (All, Active, Resolved). The table has columns for 'Assigned Comment', 'Assignee', 'Current Assign Time', 'Initial Assign Time', 'Detection UUID', 'Device IP', 'DHCP Ho...', 'Username', 'Hostname', and 'Action'. The 'Action' column for the last row is highlighted with a red box, and a dropdown menu is open showing the 'Assign Detection' option.

Assigned Comment	Assignee	Current Assign Time	Initial Assign Time	Detection UUID	Device IP	DHCP Ho...	Username	Hostname	Action
		2024-08-19 21:36:15 Z	2024-08-14 16:55:03 Z	8fd01a54-dbe3-4d9c-9791-f...	10.10.1.118				⋮
		2024-08-14 21:05:53 Z	2024-08-14 20:58:29 Z	ebcc6bde-5413-414d-988a-...	10.10.1.111				⋮
		2024-08-14 21:05:53 Z	2024-08-14 21:00:48 Z	f01ab11f-8fec-4592-82df-d5...	10.10.1.111				⋮
		2024-08-19 21:36:15 Z	2024-08-19 21:35:59 Z	1f8bbd65-09ba-443d-b550-...	10.10.1.118				⋮
		2024-08-23 13:38:19 Z	2024-08-23 13:38:19 Z	e15cb5d9-948b-4a3b-a9e0-...	10.10.1.98				⋮
		2024-08-23 13:38:19 Z	2024-08-23 13:38:19 Z	2adfb6ea-f1b7-498a-98f8-cf...	10.10.1.114				⋮
		2024-08-23 13:38:19 Z	2024-08-23 13:38:19 Z	bf39ad6a-62c1-46b1-886f-8...	10.10.1.110				⋮
		2024-08-21 16:12:15 Z	2024-08-19 16:24:35 Z	30458f45-2214-4885-910e-...	3.5.2.77				⋮
		2024-08-23 13:39:41 Z	2024-08-13 20:43:59 Z	c184775e-e2ba-4568-a58e-...	10.10.1.114				⋮
		2024-08-19 16:31:21 Z	2024-08-15 21:25:59 Z	3ab26453-9ae2-4392-b87e-...	10.10.1.111				⋮
				c8d4ac58-b1cc-4fc6-a426-7...	10.10.1.110				⋮
				dcc1eec6-2a72-41b1-a323-f...	10.10.1.98				⋮
				d5e08c33-5620-4fd6-bcf9-3...	10.10.1.97				⋮
				c5ac2892-8bf2-406b-8598-...	10.10.1.101				⋮
			2024-08-21 17:05:03 Z	70e632d9-2fca-4fd4-a35c-a...	10.10.1.111				⋮
				0b7cf239-aa42-4ce7-a58f-6...	10.10.1.117				⋮

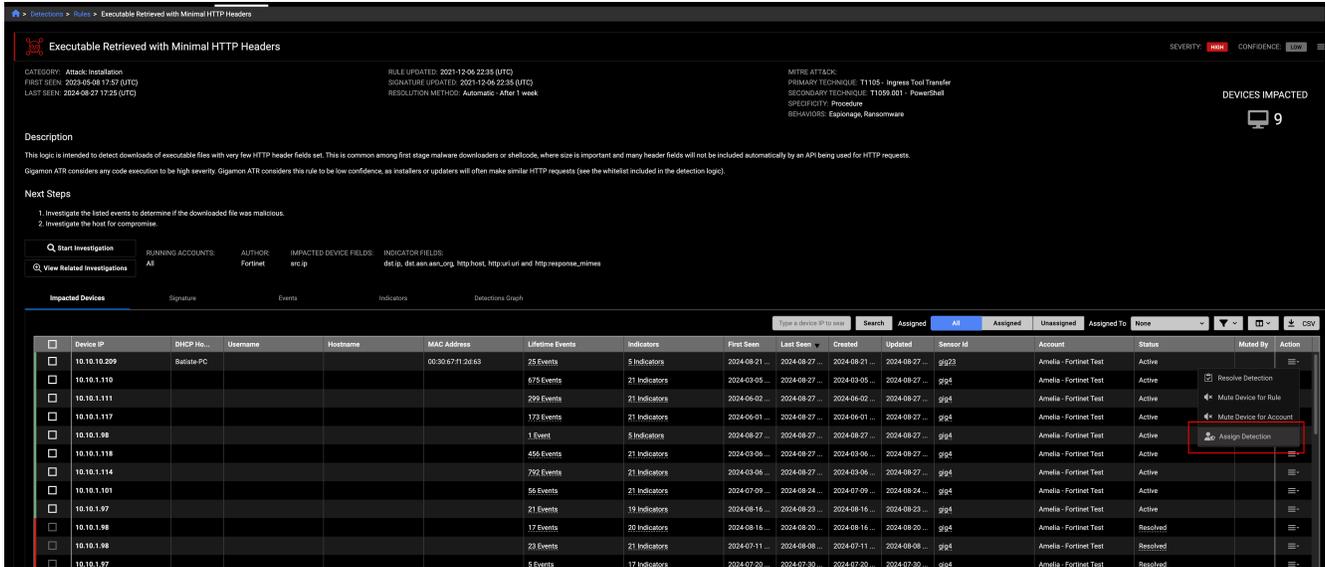
You can bulk assign and unassign detections from the tools menu at the top-left of the table.



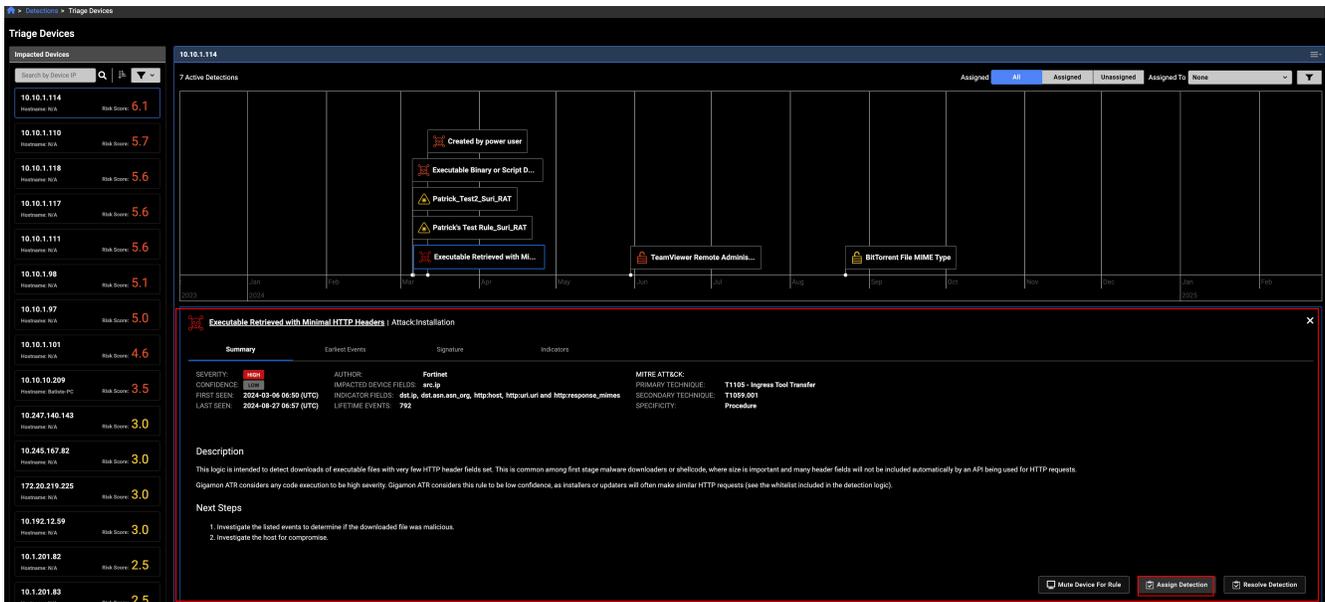
The screenshot shows the 'Detections Table' interface. At the top, it displays '13 Detection Rules, 3553 Devices from 3687 Detections'. Below this is a search bar and filters for 'Severity' (All, H, M, L) and 'Detection Status' (All, Active, Resolved). The table has columns for 'Assigned Comment', 'Assignee', 'Current Assign Time', 'Initial Assign Time', 'Detection UUID', 'Device IP', 'DHCP Ho...', 'Username', 'Hostname', and 'Action'. The tools menu at the top-left of the table is open, and the 'Assign 4 Detections' option is highlighted with a red box.

Assigned Comment	Assignee	Current Assign Time	Initial Assign Time	Detection UUID	Device IP	DHCP Ho...	Username	Hostname	Action
		2024-08-23 13:38:19 Z	2024-08-23 13:38:19 Z	5cb5d9-948b-4a3b-a9e0-...	10.10.1.98				⋮
		2024-08-23 13:38:19 Z	2024-08-23 13:38:19 Z	adfb6ea-f1b7-498a-98f8-cf...	10.10.1.114				⋮
		2024-08-23 13:38:19 Z	2024-08-23 13:38:19 Z	39ad6a-62c1-46b1-886f-8...	10.10.1.110				⋮
		2024-08-21 16:12:15 Z	2024-08-19 16:24:35 Z	458f45-2214-4885-910e-...	3.5.2.77				⋮

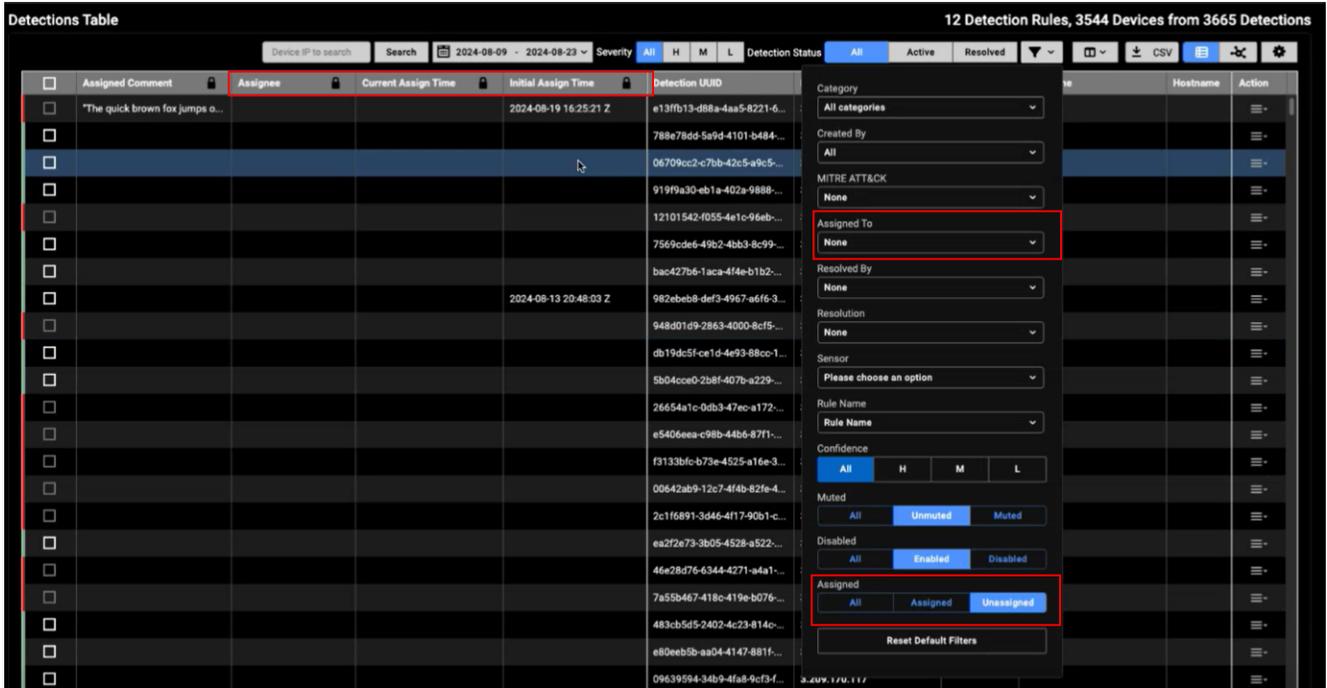
You can also assign a detection from the actions menu in the *Triage Rules* page.



Similarly, you can assign a detection from a rule in the events table in the *Triage Device* page. Select an impacted device, and then select a rule and click the *Assign Detection* button.



The following new columns were added to the *Detections Table* : *Assigned Comment*, *Assignee*, *Current Assign Time*, and *Initial Assign time*. An *Assigned / Unassigned* value was also added to the table filter. You can filter the table based on the user the detection was assigned to.



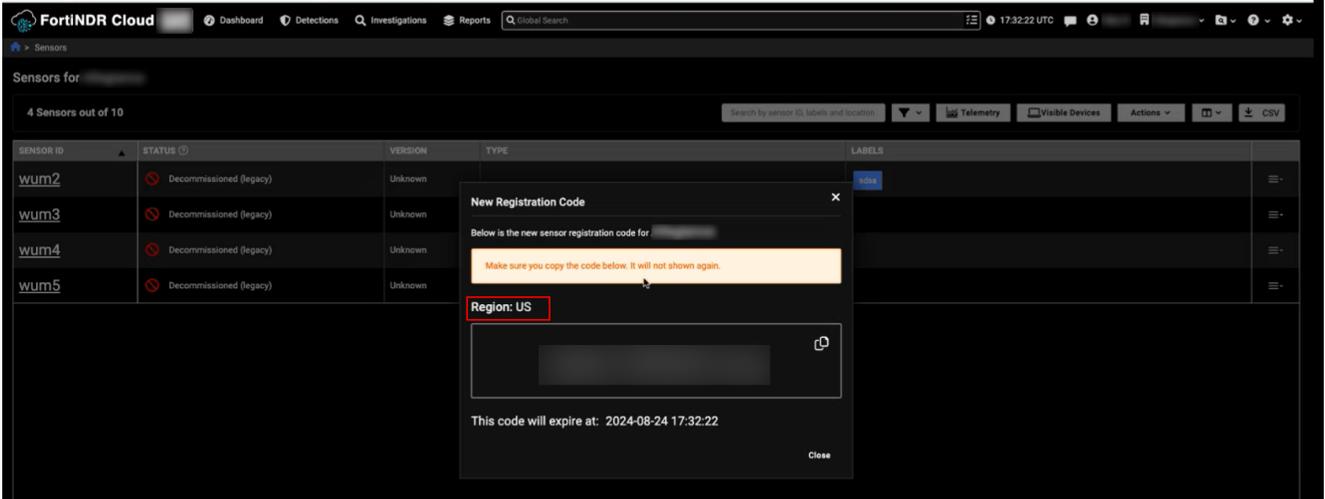
## Improved functionality

### Account region

The account region now appears at the top of the settings menu and sensor provisioning page.

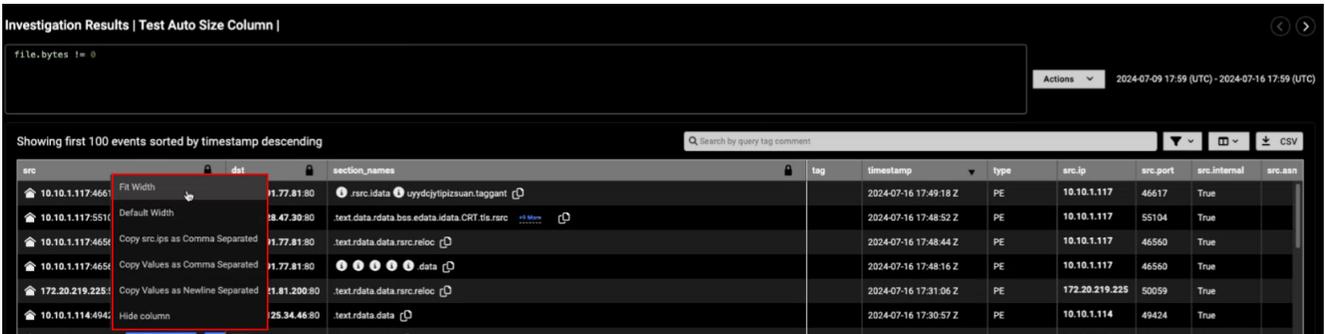


The region can be either *US* or *EU*.



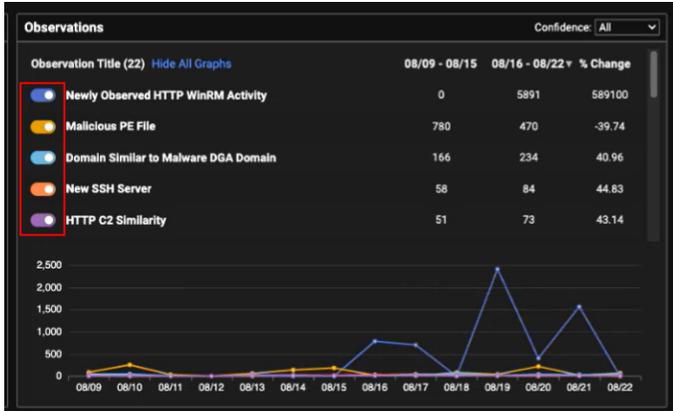
## Events table

When you show all columns in the *Events* table, you now have the option to quickly adjust the column width to the widest cell in the table. To adjust the column width, right-click the column header and select either *Fit Width* or *Default Width*.



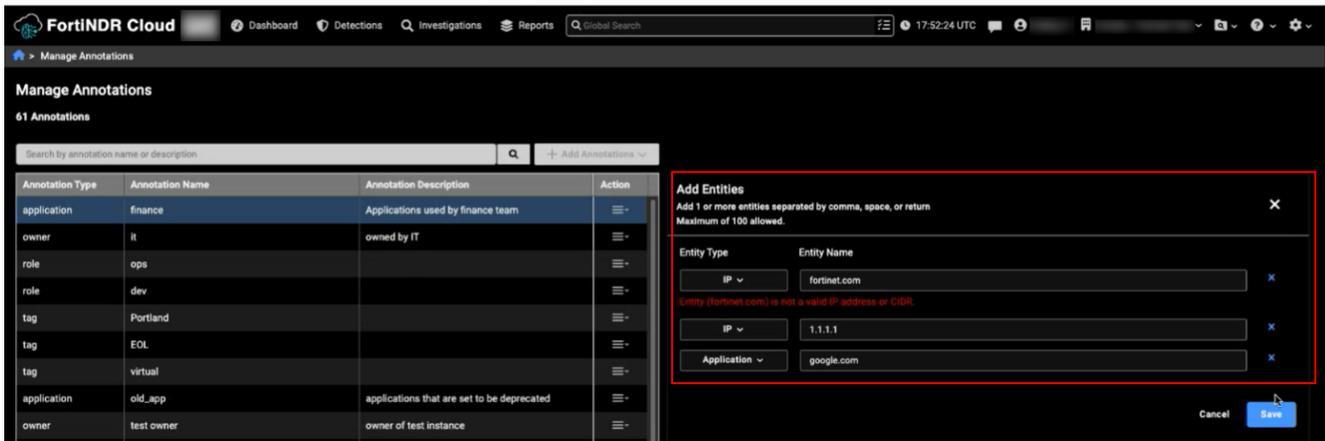
## Observations widget

The *Observations* widget in the default dashboard has been enhanced to make it easier to filter and view observations. The filter toggles have been enlarged to make them easier to see and click. The widget also displays all the observations. The total number of observations is displayed at the top of the widget and a scroll bar has been added to scroll through the list. You can also *Hide All Graphs* and toggle the graphs you want to see.

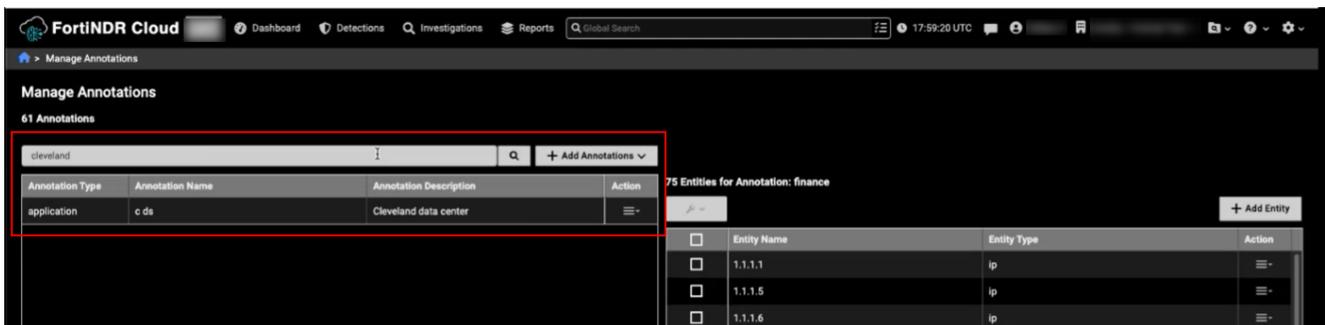


## Manage Annotations

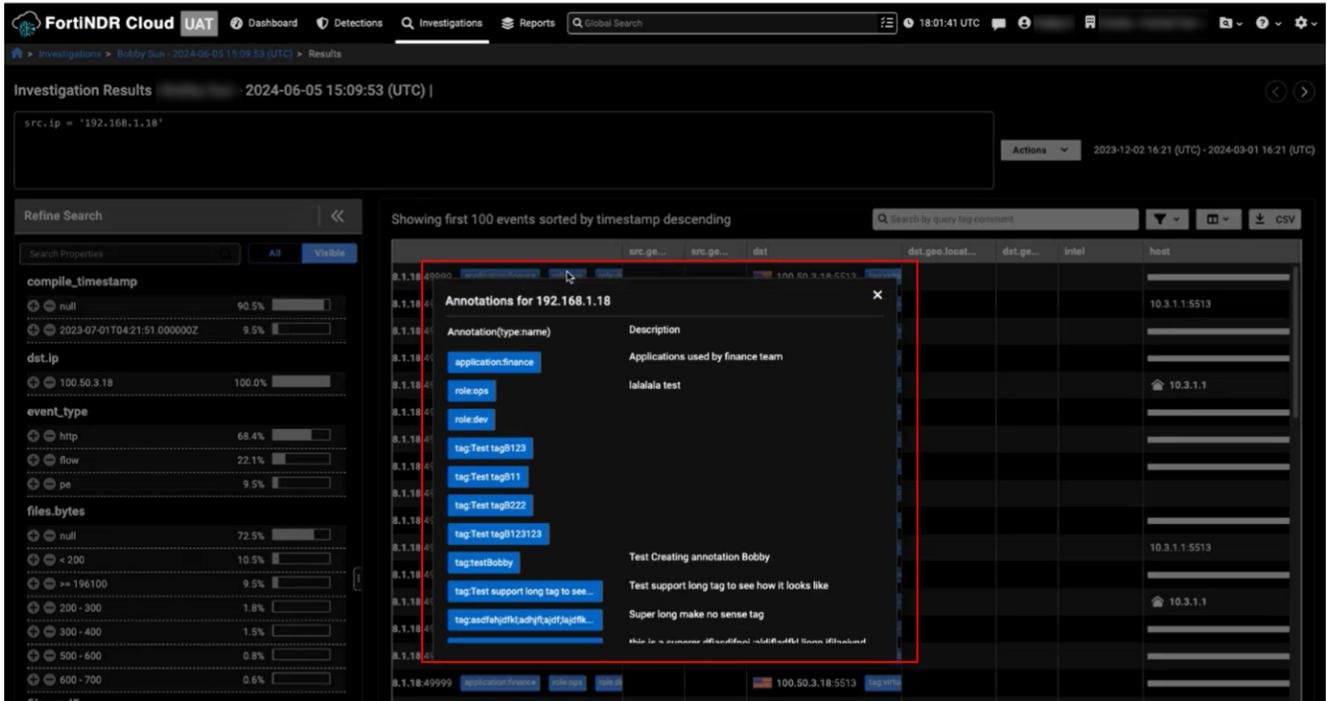
The tables in the *Manage Annotations* page have been enhanced. When you add entities, FortiNDR Cloud will validate the field when you click **Save**.



The search function has also been improved to support searching any text in the *Annotation Name* and *Annotation Description* columns. In previous versions, search was limited to an exact match of the annotation name.

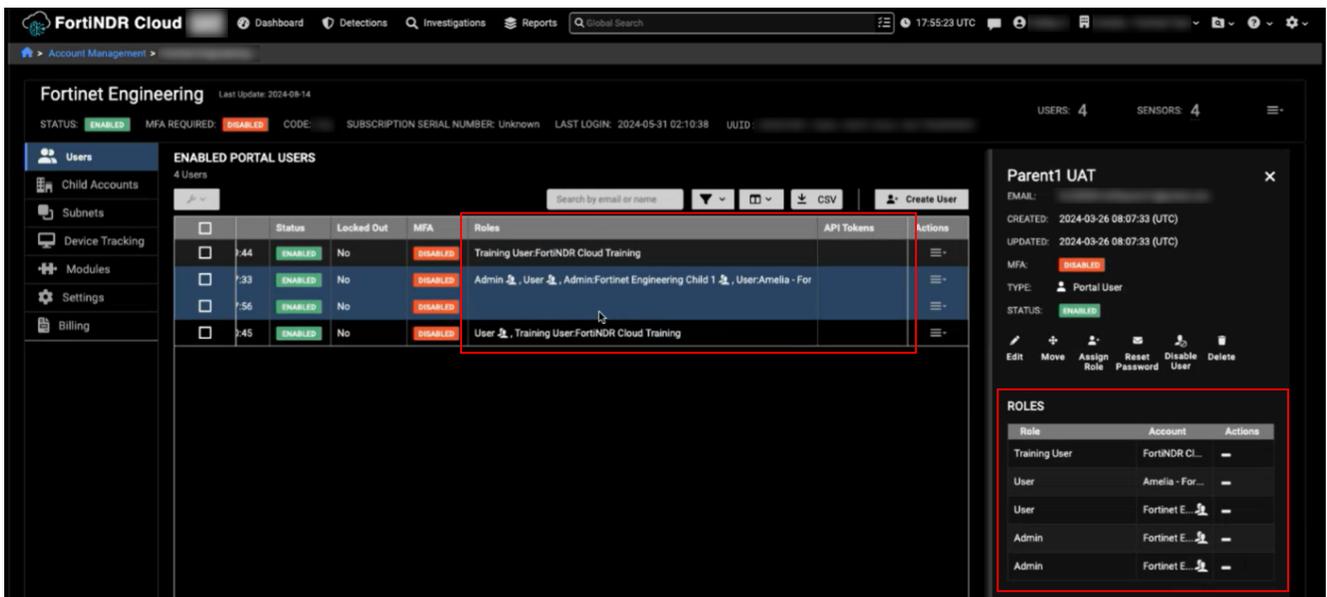


When you hover over an annotation in the Event table, it will show a tooltip with the annotation name and description. When you click the annotation, all the annotation details are displayed in a pop-up window.



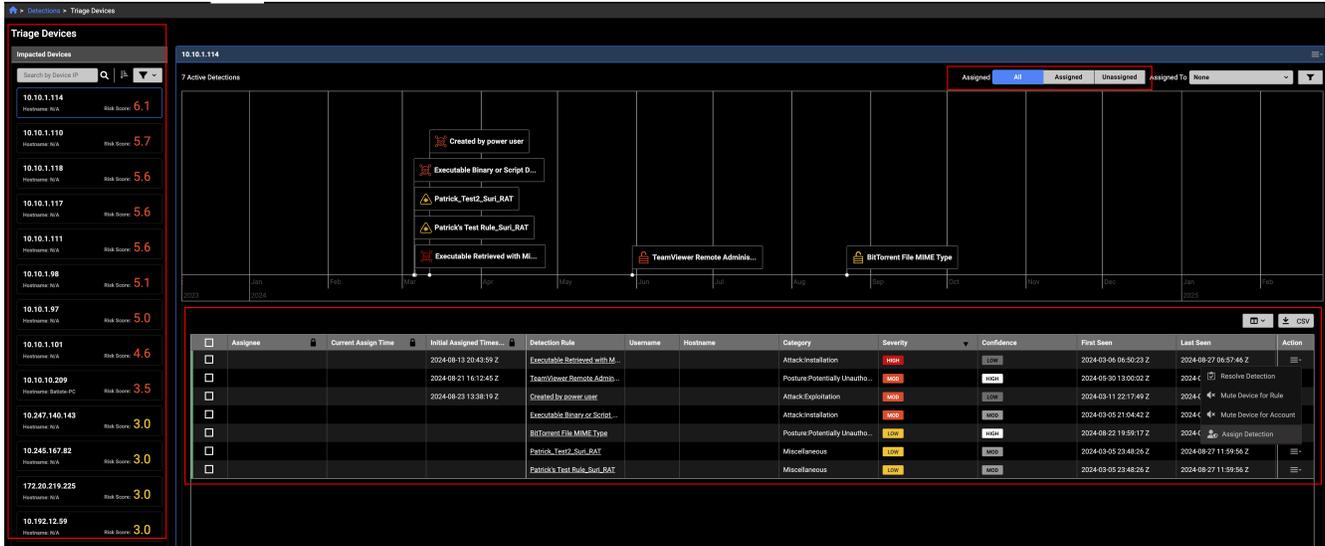
## User management

The Roles column in the Users page, now mirrors the roles and icons in the user details pane. When you download the table as a CSV file, the roles are assigned a column for each role.

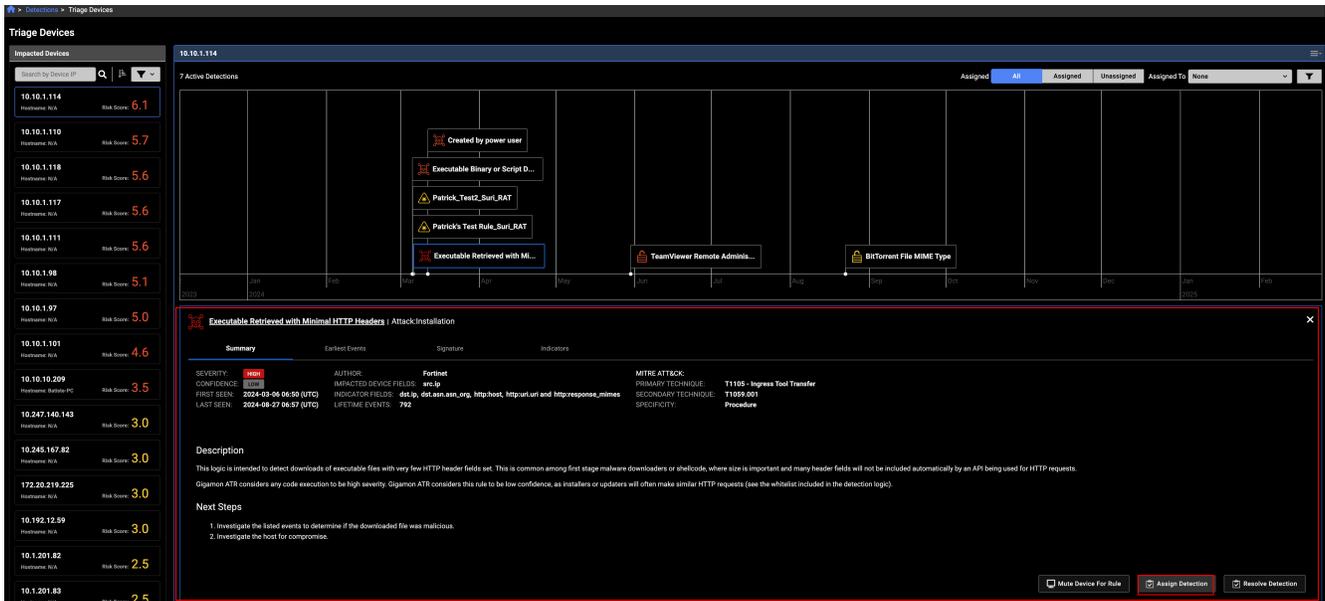


## Triage devices

The *Triage Devices* page has been improved, with a scrollable *Impacted Devices* panel at the left side of the page. The device detections table at the bottom of the page has also been replaced with a new scrollable table. All of the filters have been moved to the top of the page.



When you click the link in the *Detection Rule* column the rule details are displayed, and assign a detection. You can use the pane to assign a detection to a user.



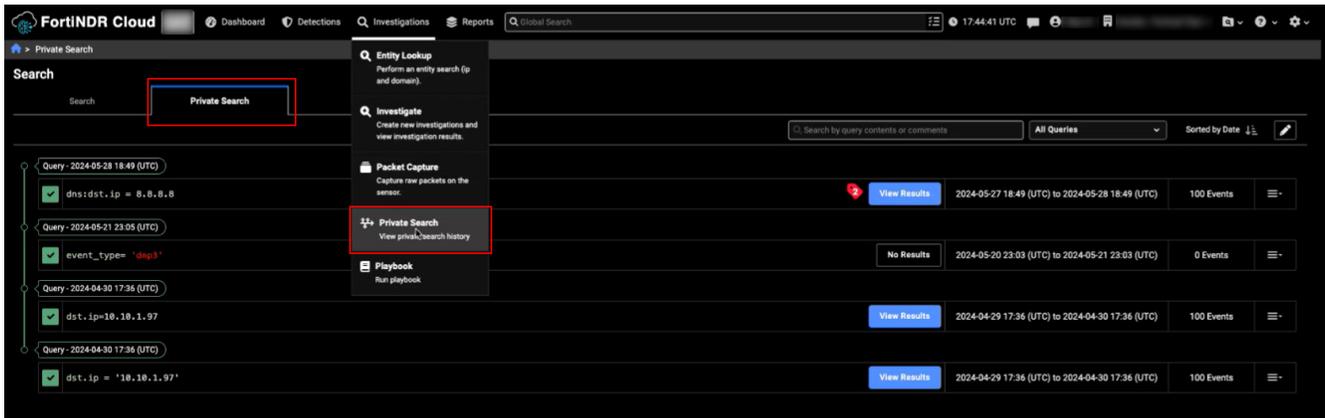
## Other improvements

### Detections table

The can now use any column header in the *Detections Table* to sort the detections. This enhancement is only available in the Detections Table.

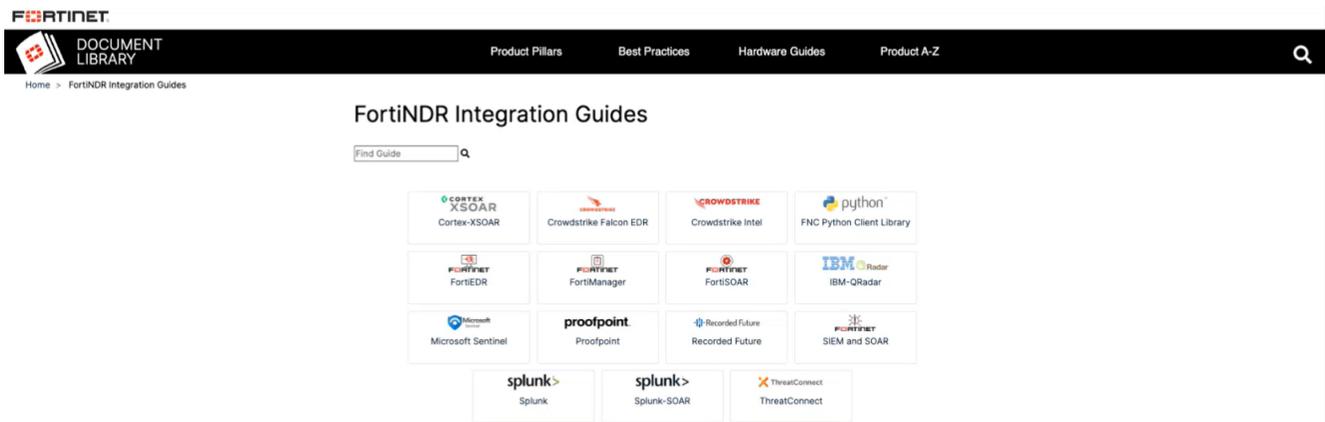
### Search Timeline

The *Search Timeline* feature has been renamed *Private Search*.

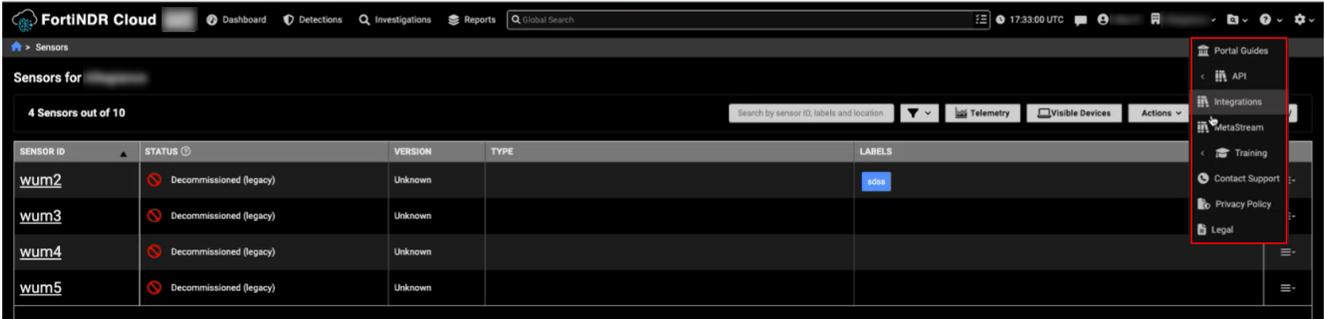


## Integrations guides

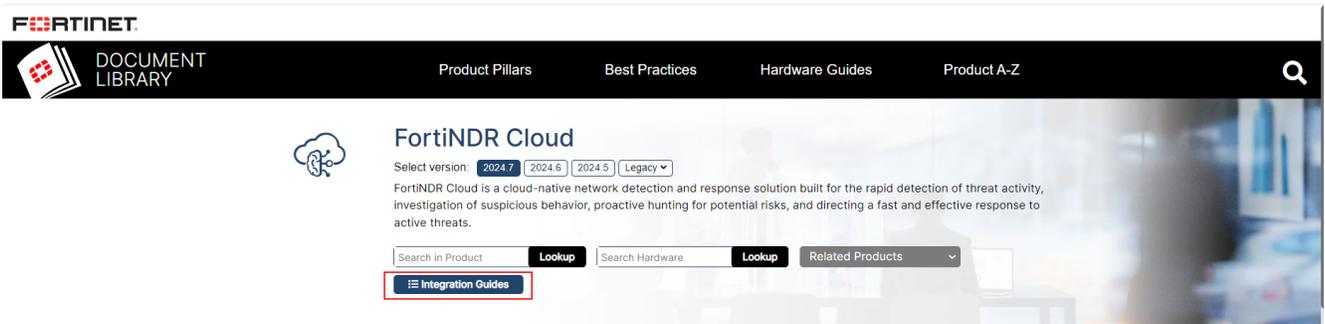
The integrations guides have been consolidated onto a dedicated page.



To access the page, in the Portal, click *Portal Guides > Integrations*.



You can also access the page by clicking the *Integration Guides* button in the [Fortinet Document Library](#).



## 31 July 2024 version 2024.7.0

- Improved functionality on page 35
  - Investigation tooltip on page 35
  - Sensors on page 36
  - Investigations on page 37
- Other improvements on page 38

## Improved functionality

### Investigation tooltip

An investigation tooltip has been added to the *Investigations* widget in the default dashboard, the *Investigations* page, and the search results in global search.

## Version history

The screenshot shows the FortiNDR Cloud interface. At the top, there's a navigation bar with 'Dashboard', 'Detections', 'Investigations', and 'Reports'. A search bar contains 'suricata rule'. Below the navigation bar, there's a 'Global Search' section. The main content area is divided into two sections: 'Detections' and 'Investigations'.

**Detections** (IP address, rule name, and rule description)

Device IP	Lifetime Events	Indicators	Last Seen	Status	Resolved By	Resolution	Date Resolved	Rule Name
...	2 Events	0 Indicators	2022-10-25 ...	Active				Suricata Rule
...	3 Events	0 Indicators	2022-08-02 ...	Active				Suricata Rule
...	1 Event	0 Indicators	2022-08-11 ...	Active				Suricata Rule
...	5 Events	0 Indicators	2022-07-05 ...	Active				Suricata Rule
...	1 Event	0 Indicators	2022-07-28 ...	Active				Suricata Rule

**Investigations** (Name, description, and comments)

Name	Description	Created by	Date Created	Date Updated	Activities	Queries	Notes
Suricata Rule	Fortinet	Unknown User	2023-11-20 00:55 (UTC)	2023-11-20 00:55 (UTC)		1	0

**Search Timeline** (Query contents or copy)

No queries found.

**Entity Lookup** (IPs and Domains found)

Search string does not have any IP or Domain

**Investigation Query** (Completed: 1, Running: 0, Queued: 0)

```
sig_id = 2018908 exclude source in ('Zscaler')
```

2023-11-13 00:46 (UTC) to 2023-11-20 00:55 (UTC)

No Events

You can also disable the investigation tooltip from the *Profile Settings* page.

The screenshot shows the 'My Profile' page in FortiNDR Cloud. It is divided into two main sections: 'User Information' and 'Account Information'.

**User Information**

- User Email: tcorreia@fortinet.com
- User Name: Tony Correia
- User UUID: 7bcb9e0f-b5f0-4e95-8198-2e7c093dc204
- User MFA: DISABLED
- Investigation Tooltip:  (disabled)

**Account Information**

- Account Name: Fortinet
- Account UUID: b1f533b5-6360-494a-9f8b-9d90f1ad0207
- Subscription Serial Number: Unknown

## Sensors

### Filter by sensor version

A new filter was added to the *Sensors* page allowing you to filter by the sensor version.

The screenshot shows the 'Sensors' page in FortiNDR Cloud. The page title is 'Sensors for Test' and it shows '4 Sensors out of 1000'. There's a search bar for 'Search by sensor ID, labels and location'. Below the search bar, there's a table of sensors with columns for 'SENSOR ID', 'STATUS', 'VERSION', 'LABELS', 'LOCATION', 'EPS (7 DAY AVERAGE)', 'TYPE', and 'PCAP'. A filter menu is open over the table, showing 'Additional Filters' with options for 'Status', 'Type', and 'Version'. The 'Version' filter is selected, and it shows a list of versions: '1.12.0', '1.11.0', '2.0.0', and 'Unknown'. The 'Unknown' version is checked.

## PCAP column

A sortable *PCAP* column was added to the *Sensors* page indicating if *Packet Capture* is enabled or disabled.

The screenshot shows the 'Sensors for Test' page in FortiNDR Cloud. A table lists 63 sensors out of 1000. The table has columns for Sensor ID, Status, Version, Labels, Location, EPS (7 Day Average), Bits/s (7 Day Average), Type, and a new PCAP column. The PCAP column contains 'DISABLED' for all sensors shown. A red box highlights the PCAP column header and its content in the first few rows.

SENSOR ID	STATUS	VERSION	LABELS	LOCATION	EPS (7 DAY AVERAGE)	BITS/S (7 DAY AVERAGE)	TYPE	PCAP
test16	Provisioning	Unknown	Lab, Sensor 16, Test, 8.0.1.0, 1.0	Seattle, WA	0 EPS	0 b/s		DISABLED
test19	Provisioning	Unknown	Test, Zoom	Seattle	0 EPS	0 b/s		DISABLED
test705	Online	1.12.0			0.1 EPS	11.663 Kb/s	ESXI	DISABLED
test822	Offline	1.12.0			0 EPS	0 b/s	Large (3rd Gen)	DISABLED
test823	Provisioning	1.11.0			0 EPS	0 b/s	QEMU/KVM	DISABLED
test824	Offline	1.12.0			0 EPS	0 b/s	Large (4th Gen)	DISABLED
test826	Online	Unknown			0.1 EPS	9.358 Kb/s	ESXI	DISABLED
test831	Offline	1.12.0			0 EPS	23.322 Kb/s	QEMU/KVM	DISABLED
test834	Offline	1.12.0			0 EPS	0 b/s	ESXI	DISABLED
test836	Offline	1.11.0			0 EPS	0 b/s	QEMU/KVM	DISABLED
test856	Offline	1.12.0			0 EPS	0 b/s	Azure/HyperV	DISABLED
test857	Offline	1.12.0			0 EPS	0 b/s	Azure/HyperV	DISABLED

## Sensor last update

A *Last Updated* field was added to the sensor detail page.

The screenshot shows the sensor detail page for 'test870'. The sensor is 'Offline'. The 'Connection Status' section shows 'Status: Offline', 'Serial Number: [redacted]', and 'Management IP: [redacted]'. A red box highlights the 'Last Updated' field, which displays '2024-04-30 20:31 (UTC)'. Below this are sections for 'Interfaces', 'Hardware', and 'Software'.

Interface	Speed
ens192 mgmt	0 b/s
ens224	0 b/s
ens256	0 b/s

Hardware	Software
Processor(s): Intel(R) Xeon(R) CPU E5-2670 0 @ 2.60GHz	Operating System: Debian GNU/Linux 12 (bookworm)
Number of Cores: 16	ZEEK Version: 5.0.10
Total Memory: 31.388 GB	Suricata Version: 6.0.16 RELEASE
Total Disk Space: 97.278 GB	Sensor Version: 2.0.0

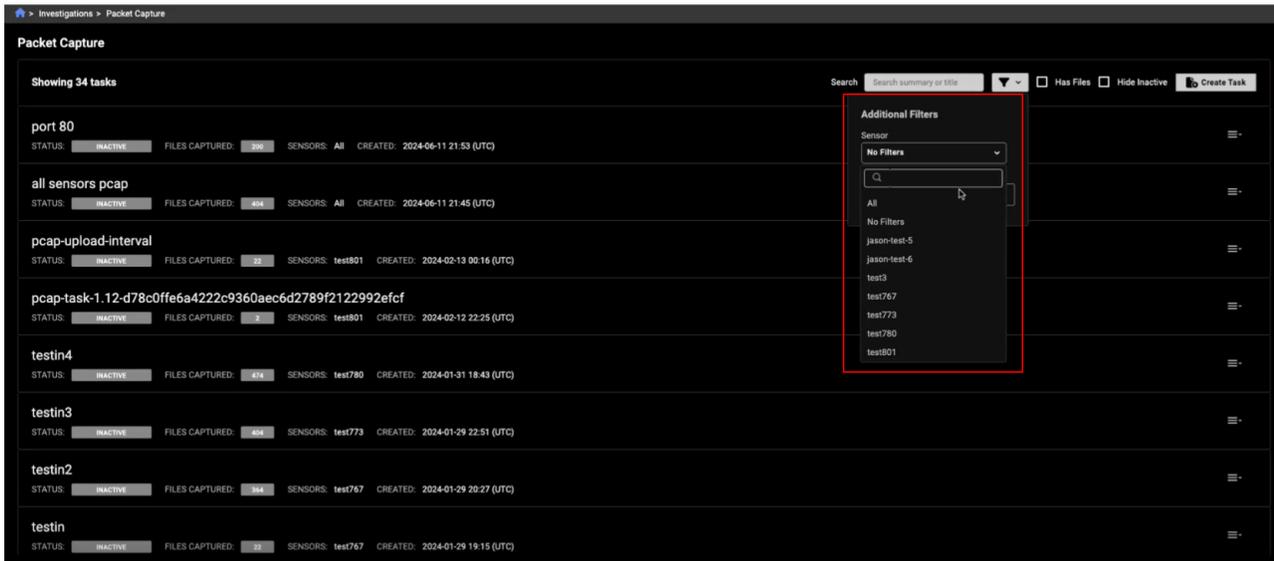
Timestamp	Action	User Account Name	User Name	Comment
2024-04-29 17:32:39.303000Z	Provision	Fortinet	Sensor Service	Sensor provisioned

## Investigations

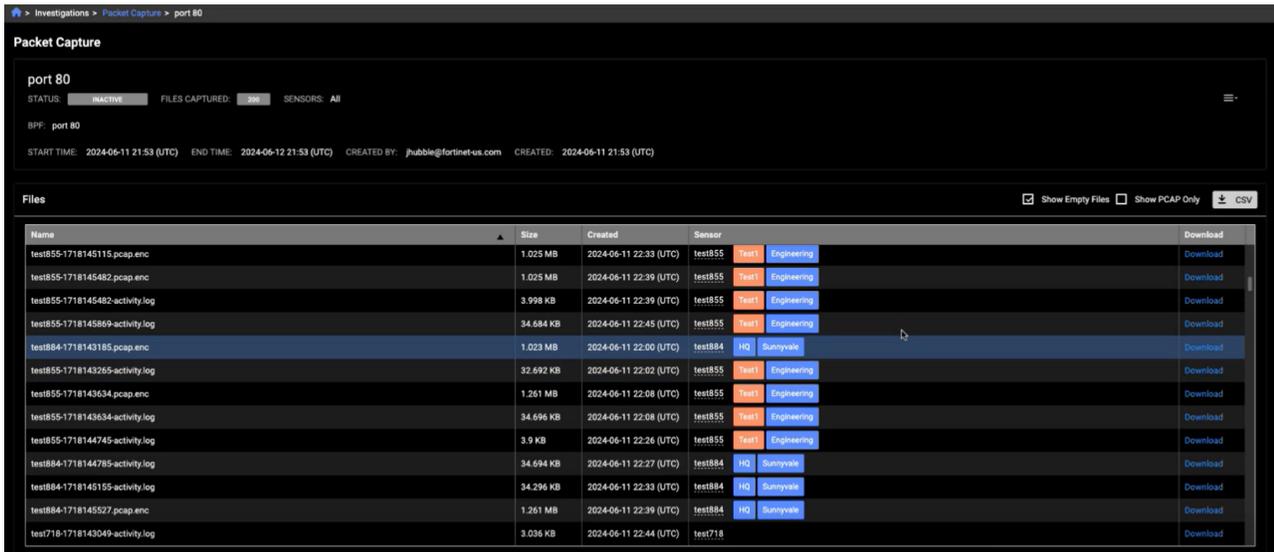
### Packet Capture page

The *Investigations > Packet Capture* page has been updated.

The sensor filter only shows the sensors that have PCAPs configured. That is, the PCAPs where that sensor is configured and any PCAP that has files from that sensor are shown. If there are any All PCAPs configured, *All* can be selected. By default, *No Filters* is selected.



In the *Files* section, a sortable *Sensor* column that lists the sensor IDs was added. The files table is also now scrollable, instead of paginated.



## Other improvements

### Metastream module

The *Metastream* module has been redesigned to align with the look and feel of the other integrations on the page. If there is an error while enabling the integration, an error will appear at the top of the page.

## Custom Dashboards

Custom dashboards now support default names, allowing users to add a dashboard without a unique name.

## GUI

- The *Copy* button has been updated and standardized across the portal.
- A link to the CSV guidelines document has been added on the *Manage Annotations* page.
- In *Reports > Network Security Posture Report*, you can now click an event to start an investigation.

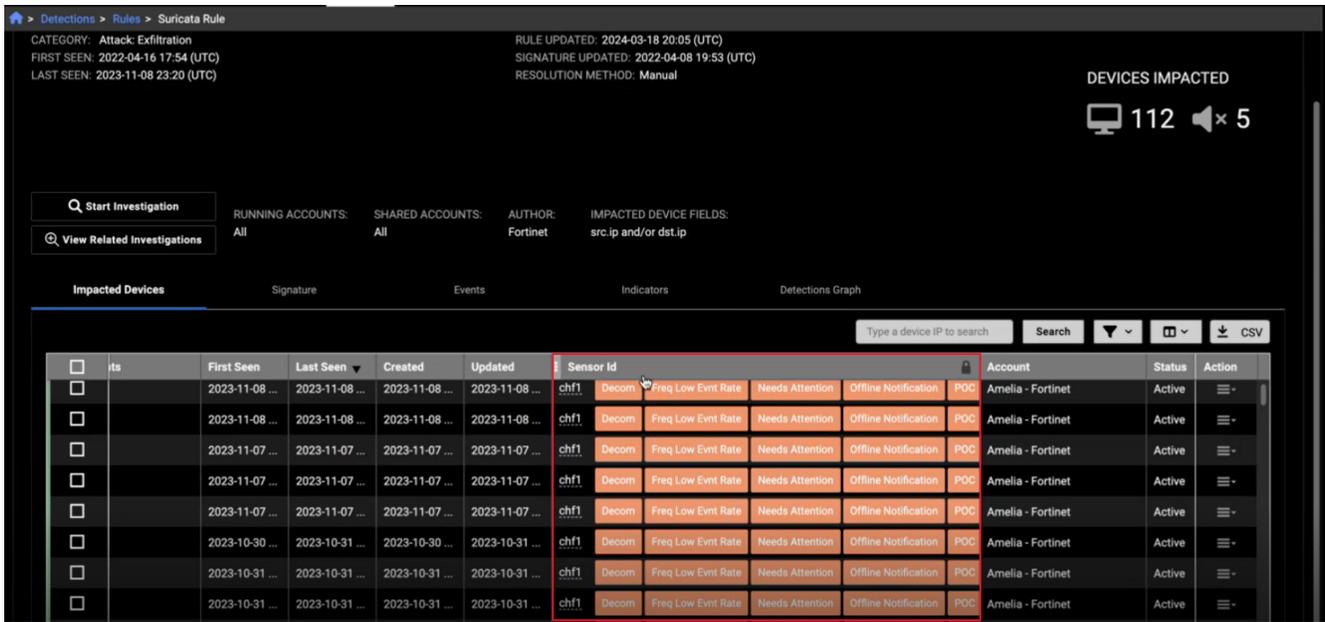
## 26 June 2024 version 2024.6.0

- Improved functionality on page 39
  - Sensors on page 39
  - Create new detections on page 40
  - API tokens on page 41
  - Default dashboard on page 42
    - MITRE ATT&CK widget on page 42
    - Observations widget on page 42
- Other improvements on page 43
  - Detections Rules tab on page 43
  - Packet Capture on page 43

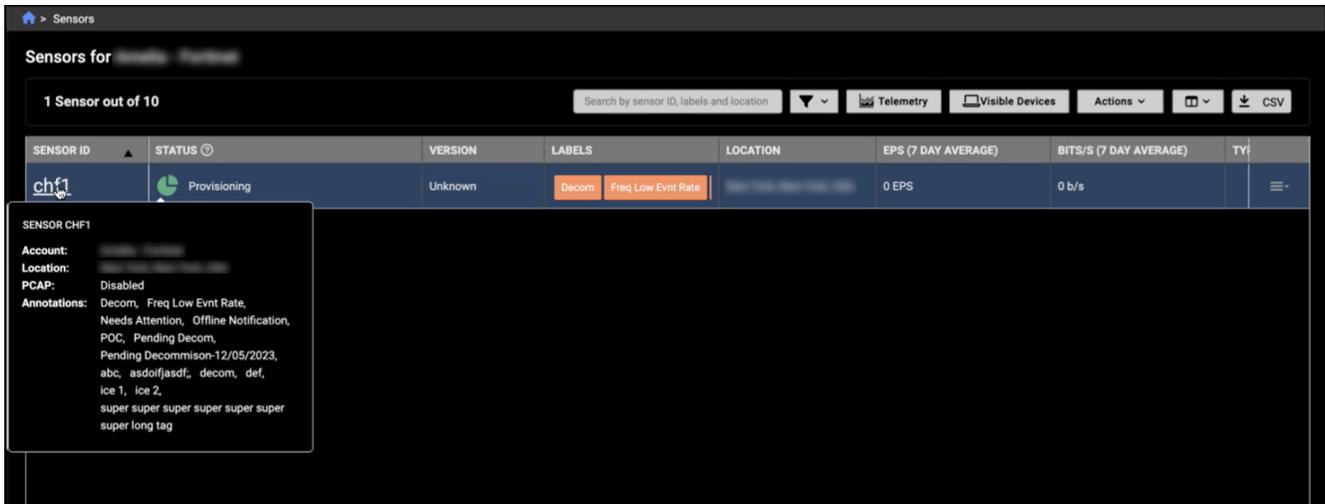
## Improved functionality

### Sensors

The *Sensor ID* column now displays all the tags within the column. You can also click the sensor ID to open the *Sensor Details* page. When you hover over the Sensor ID, a dialog displays all the annotations for the sensor. With the exception of the *Sensors* page, this change applies to all tables that have the *Sensor ID* column including *Search*, *Search Timeline* results page and the *Events* table.

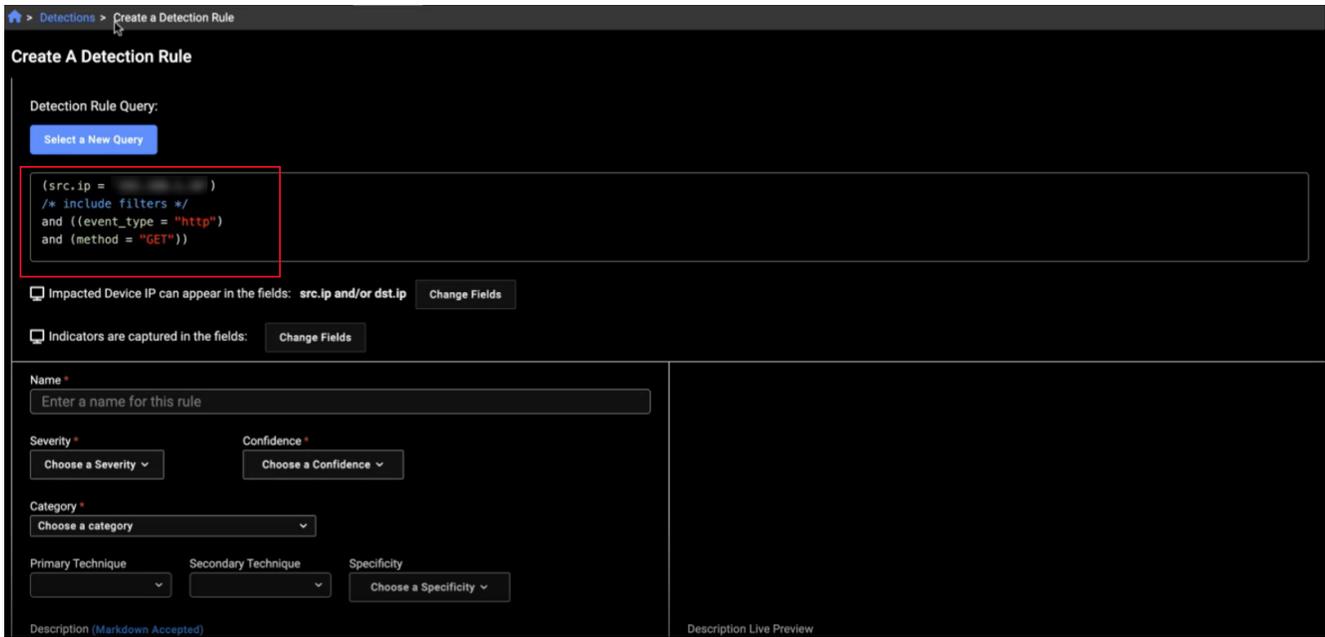


In the *Sensors* page, when you hover over the Sensor ID in the list, a dialog will display the sensor information.



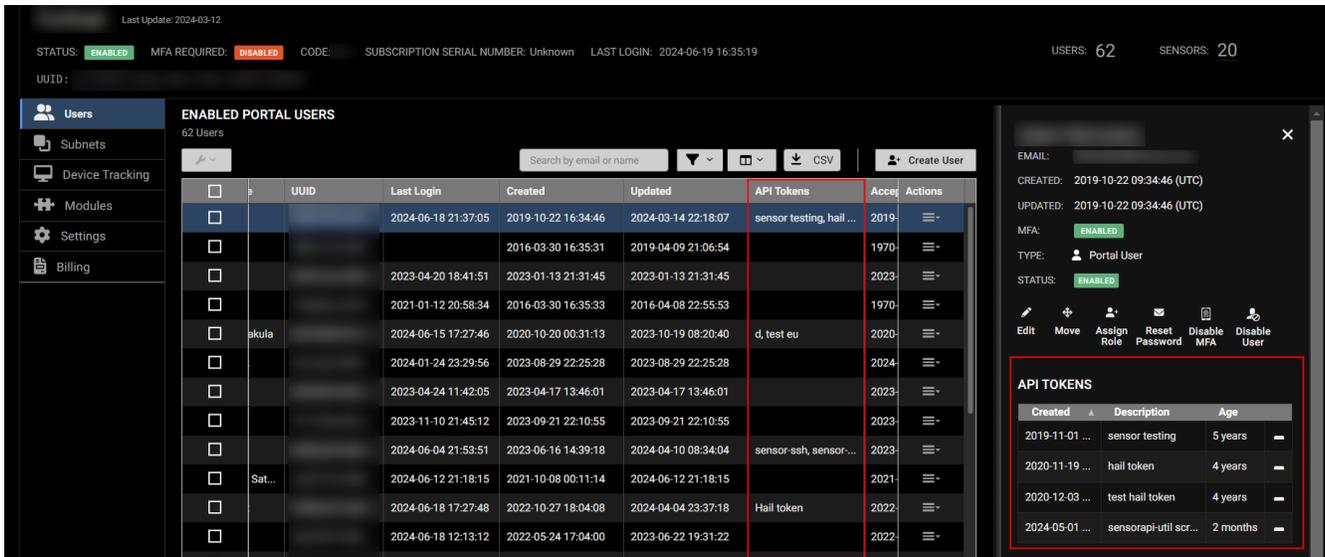
## Create new detections

The facet filters are now included in the query field when you create a new detection from the results in the *Search Timeline* page. To try this out, open the *Search Timeline* page and locate an entry with results. Click the actions menu and select *Create Detection*. The facet filters are displayed in the query field.

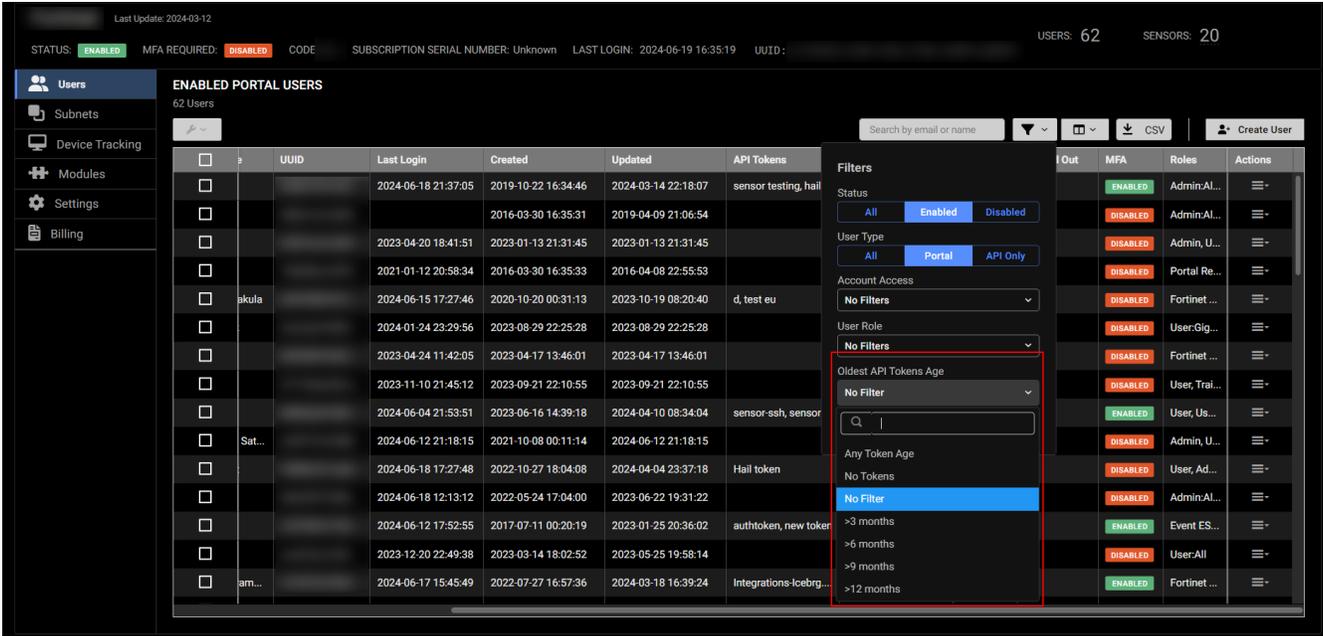


## API tokens

The term *Permanent Tokens* has been replaced with *API Tokens*. An *API Tokens* column was also added to the *Users* tab in the *Account Management* page.



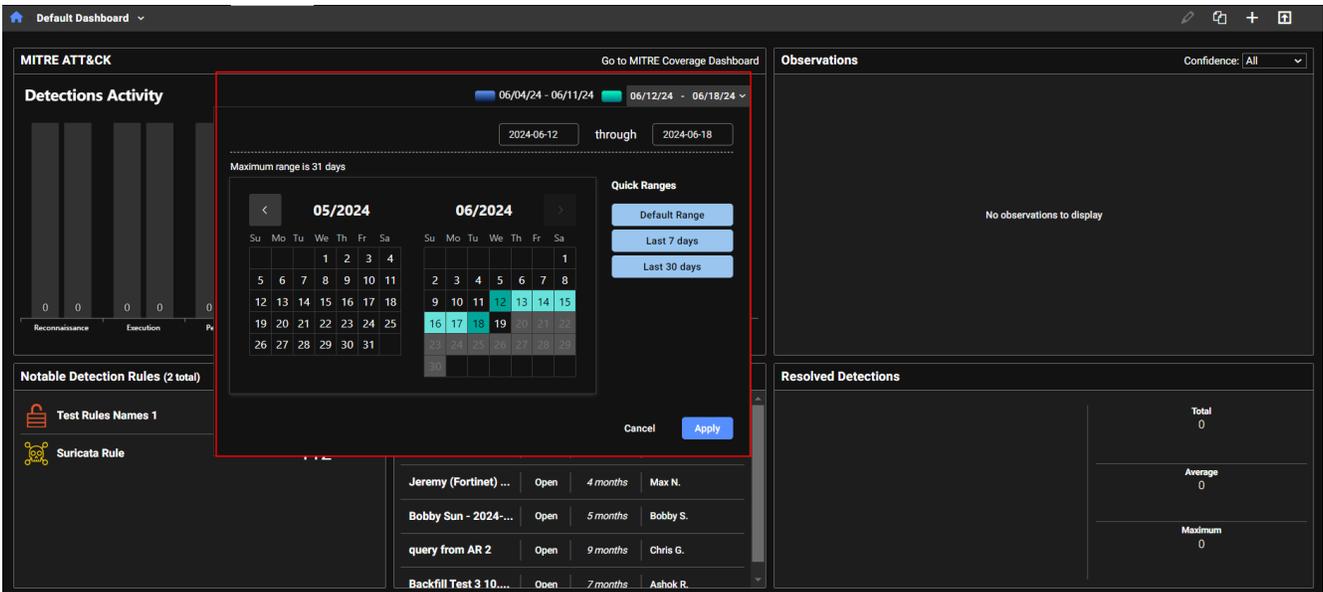
You can also use API tokens to filter the page.



## Default dashboard

### MITRE ATT&CK widget

A date-range picker was added to the *MITRE ATT&CK* widget in the default dashboard.



### Observations widget

You can now filter the graph in the widget by clicking an observation title in the graph's legend.



## Other improvements

### Detections Rules tab

The *Detections Rules* page no longer displays rules that have never been triggered when you filter the page by *All*. Pagination has also been removed from the page to make it easier to scroll through the results. This change also applies to the detail wheel.

### Packet Capture

We have removed the option to select the number of rows to view on the page. The page now shows all the tasks on a scrollable page.

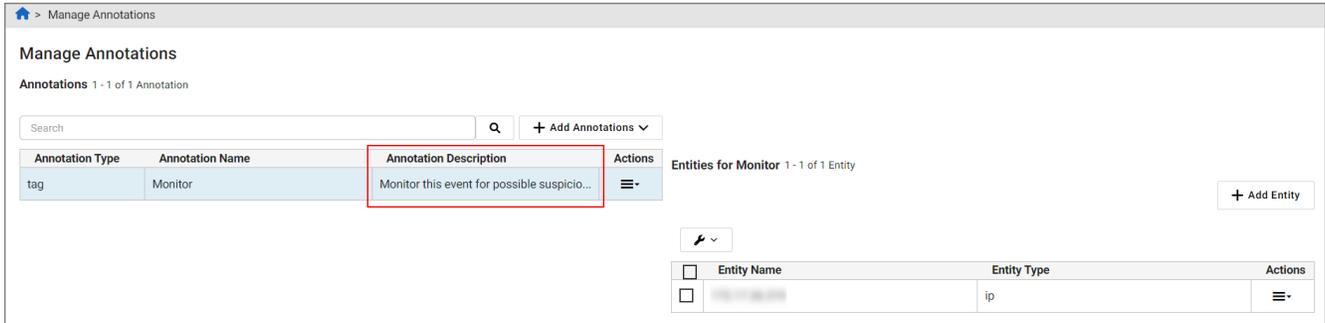
## 29 May 2024 version 2024.5.0

- Improved functionality on page 44
  - Manage annotations on page 44
  - Search timeline on page 44
  - Global Search on page 45
- Other improvements on page 45
  - Queries on page 45
  - Investigations on page 46

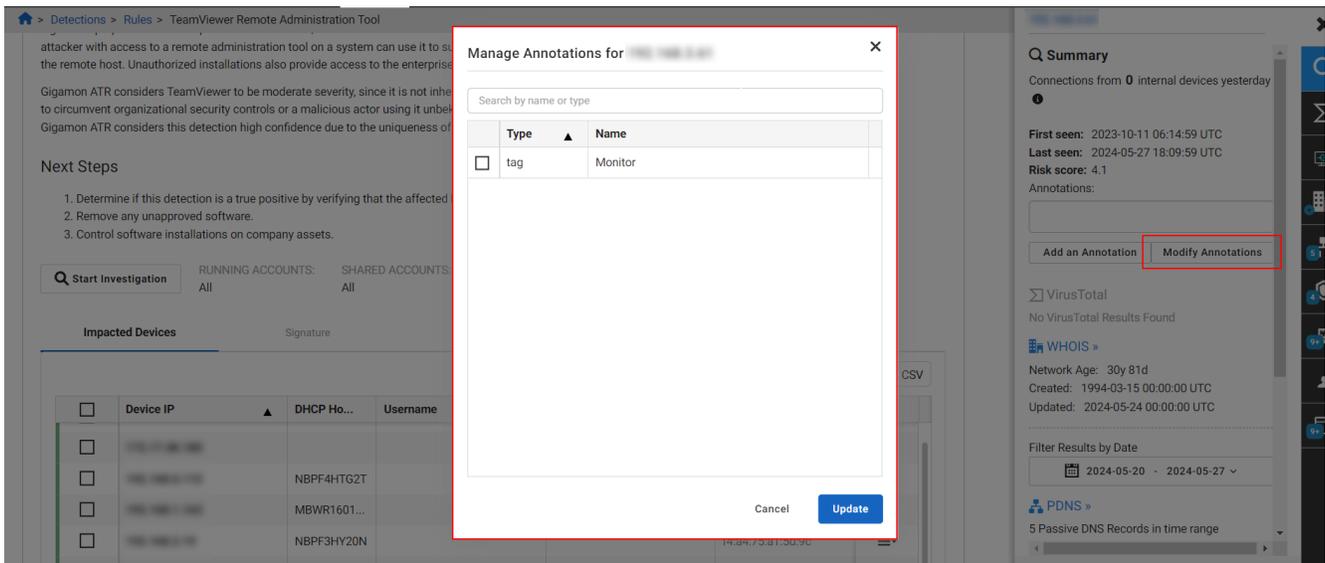
## Improved functionality

### Manage annotations

A new *Annotations Description* column was added to the *Manage Annotations* page.

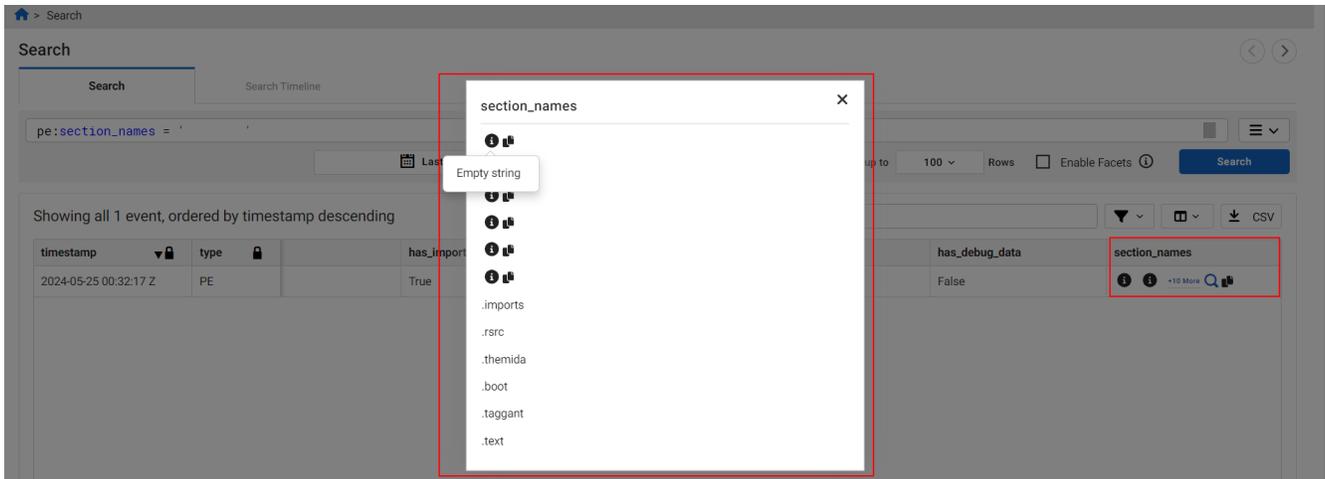


In the *Entity Panel*, the *Manage Annotations* button has been renamed *Modify Annotations* and the GUI was improved so you can search for and quickly add or remove annotations.



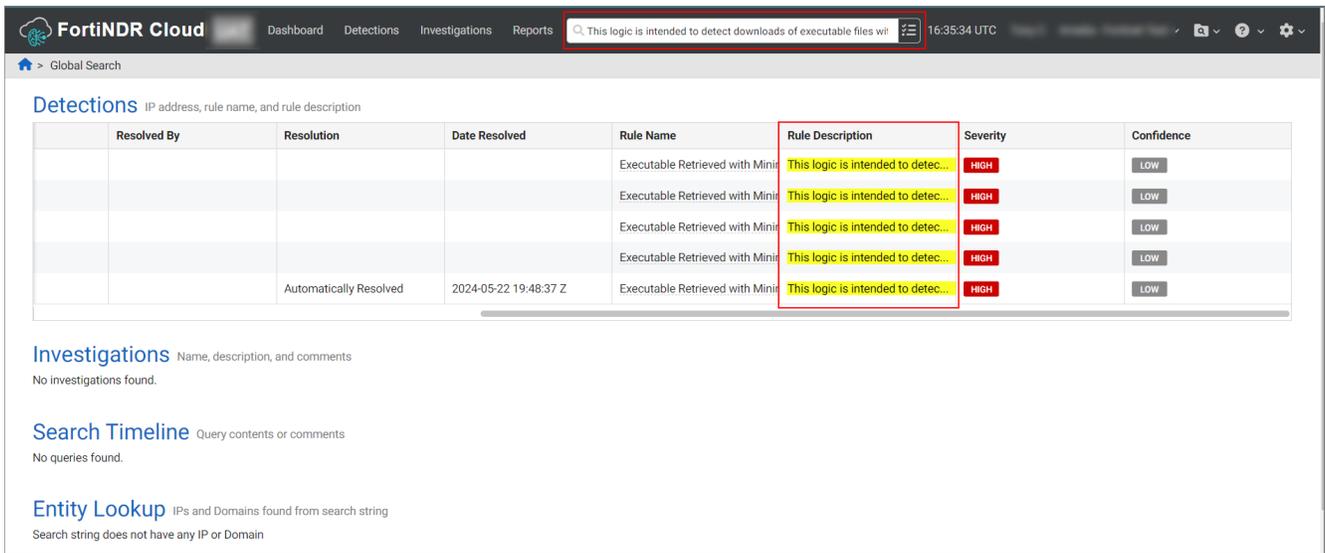
### Search timeline

New icons have been added to the *section\_names* column to add explanation and functionality to the data. Hover over the information icon to view the number of empty strings and spaces. Use the copy icon to copy the information. You can also click the link to view the values and icons in a dialog box.



## Global Search

Global search now supports search Rule descriptions. Copy and paste text from Rule description into the search field. Search results will be highlighted in the *Rule Description* column of the in the *Detections* section. A highlight was also added to the *Device IP* column when you search by IP.



## Other improvements

### Queries

- The dashboard and report queries have been improved to make them faster.
- You can now query *dnp3*, *dnp3\_control*, and *dnp3\_object* event types in an investigation.

## Investigations

The *src* column in the *Events* tab now displays the annotation names (as opposed to the number of annotations).

## 15 May 2024 version 2024.4.1

- Improved functionality on page 46
  - Navigation improvements on page 46

## Improved functionality

### Navigation improvements

You can now pivot to the *Sensor Details* page from the *Sensor ID* column in the *Rules Details*. Go to *Detections > Triage Rules* and open a rule. Click a sensor in the *Sensor ID* column. If the sensor is available, the *Sensor Details* page opens.

The screenshot shows the 'Rules Details' page for a rule named 'Test rule'. The page includes a breadcrumb trail 'Detections > Rules > Test rule'. Key information includes:
 

- CATEGORY:** Posture: Anomalous Activity
- FIRST SEEN:** 2023-05-03 17:39 (UTC)
- LAST SEEN:** 2023-08-19 00:42 (UTC)
- RULE UPDATED:** 2023-12-08 15:54 (UTC)
- SIGNATURE UPDATED:** 2023-11-28 17:25 (UTC)
- RESOLUTION METHOD:** Manual

 On the right, it indicates 'DEVICES IMPACTED' with a monitor icon and the number '15'. Below this, there are buttons for 'Start Investigation' and 'View Related Investigations'. Further down, there are fields for 'RUNNING ACCOUNTS', 'AUTHOR', and 'IMPACTED DEVICE FIELDS: src.ip and/or dst.ip'. At the bottom, there is a tabbed interface with 'Impacted Devices' selected. The table below shows a list of impacted devices with columns for 'Sensor Id', 'Account', 'Status', 'Muted By', and 'Date Muted'. The 'Sensor Id' column contains 'chf1' and 'chf10', with 'chf1' highlighted in a red box. The 'Status' column shows 'Active' for both. The 'Action' column contains menu icons.

	een	Last Seen ▼	Created	Updated	Sensor Id	Account	Status	Muted By	Date Muted	Action
<input type="checkbox"/>	8-19 ...	2023-08-19 ...	2023-08-19 ...	2023-08-19 ...	chf1	[Redacted]	Active			⋮
<input type="checkbox"/>	5-16 ...	2023-06-08 ...	2023-05-16 ...	2023-06-08 ...	chf10	[Redacted]	Active			⋮

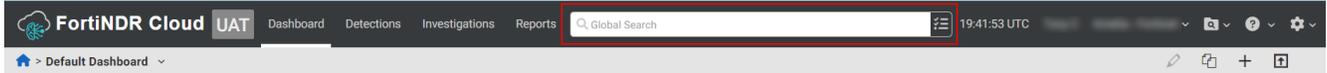
## 01 May 2024 version 2024.4.0

- New functionality on page 47
  - Global search on page 47
  - Sensor lookup on page 48
  - Modbus events on page 48
- Other improvements on page 49

## New functionality

### Global search

A new Global Search function was added to the navigation banner allowing you to search FortiNDR Cloud with a text string, IP address or domain. You can enter multiple IPs and domains separated by a comma or space.



The search results are organized by *Detections*, *Investigations*, *Search Timeline* and *Entity Lookup*. Global Search does not support searching Rules at this time.

**Detections** IP address  
No detections found for the IP

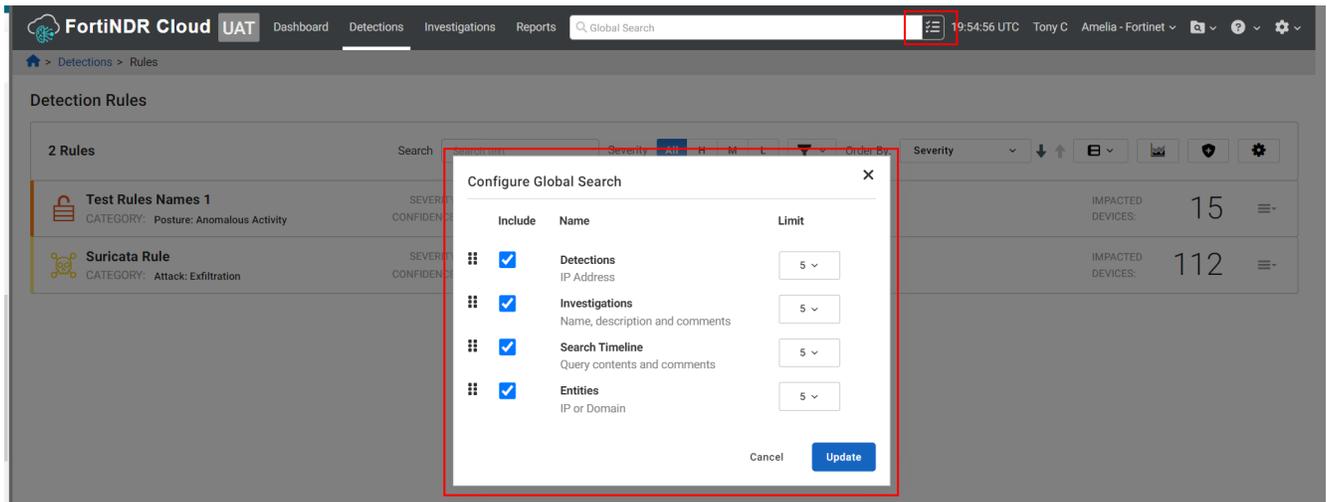
**Investigations** Name, description and comments  
No investigations found.

**Search Timeline** Query contents or comments  
No queries found.

**Entity Lookup** IPs and Domains found from search string

Entity	Type	Count	First Seen	Last Seen
8.8.8.8	IP	25662	2023-05-08 17:44 (UTC)	2024-04-30 16:59 (UTC)
1.1.1.1	IP	3133413	2023-05-08 17:45 (UTC)	2024-04-30 17:01 (UTC)

You can configure how the results are displayed by clicking the menu next to the search field. You can show or hide a category, limit the number of results, or arrange the order they appear in the page.



You can also access Global Search when you right-click a *scr* IP.

## Version history

Showing all 100 events, ordered by timestamp descending

timestamp	type	src	src.ip	src.port	src.internal	src.asn	src.asn.asn_org	src.asn.isp
2023-06-08 22:09:54 Z	FLOW	10.81.1.252	10.81.1.252	56399	True			
2023-06-08 22:09:54 Z	FLOW			56186	True			
2023-06-08 22:09:54 Z	FLOW			59162	True			
2023-06-08 22:09:54 Z	FLOW			59190	True			
2023-06-08 22:09:54 Z	FLOW			59174	True			
2023-06-08 22:09:54 Z	FLOW			56112	True			
2023-06-08 22:09:54 Z	FLOW			35764	True			
2023-06-08 22:09:54 Z	FLOW			57332	True			
2023-06-08 22:09:54 Z	FLOW			44103	True			
2023-06-08 22:09:54 Z	FLOW			43196	True			

## Sensor lookup

A new search function was added to the *Sensors* page allowing you to search the page by *Sensor ID*, *Labels* and *Location*.

Sensors for *Amelia Fortinet*

1 Sensor

Search by sensor ID, labels and location.

SENSOR ID	STATUS	VERSION	LABELS	LOCATION	EPS (7 DAY AVERAGE)	BITS/S (7 DAY AVERAGE)	TYPE
	Provisioning	Unknown	D F N O P P P a a d d i l	New York, New York, USA	0 EPS	0 b/s	

## Modbus events

You can now query Modbus events in an investigation.

Total Queries: 1  Completed: 1  Running: 0  Queued: 0

Search by note content and query tag comment

Query - 20: `modbus:dst.annotations.roles` string

ip  `modbus:dst.annotations.tags`

`modbus:dst.asn.asn`

`modbus:dst.asn.asn_org`

`modbus:dst.asn.isp`

`modbus:dst.asn.org`

Add a Note

Name: `modbus:dst.geo.city`

`modbus:dst.geo.country`

`modbus:dst.geo.subdivision`

`modbus:dst.internal`

Query: `modbus:dst.ip`

`modbus`

Actions Sort by timestamp Descending Last 7 Days Retrieve up to 100 rows Enable Facets Cancel Add Query

## Other improvements

- You can now open and close the date picker by clicking the date-range button. The date picker is responsive so the dates are visible regardless of its position on the screen.
- The subscription serial number is displayed in the *My Profile* page. If the serial number is not displayed, you will see a tooltip informing you the SN is available from your account representative. You can also update the serial number in the *Update account* dialog.
- A banner is displayed when your account is set to expire in less than 90 days.

## 10 April 2024 version 2024.3.1

- Improved functionality on page 49
  - Detections table on page 49

### Improved functionality

#### Detections table

A new *Created by* column was added to the *Detections table*.

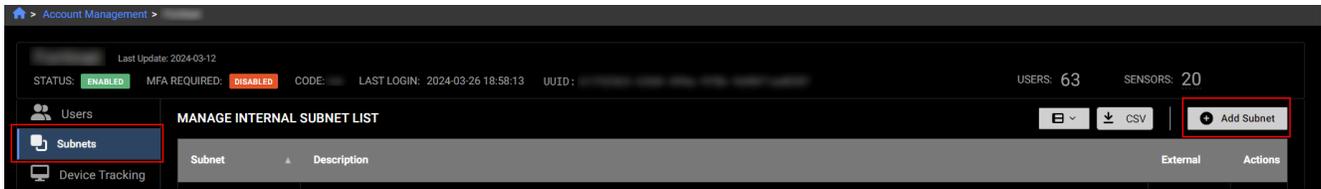
## 27 March 2024 version 2024.3.0

- New Functionality on page 49
  - Edit subnets on page 49
  - Mandatory SSO on page 50
- Improved Functionality on page 51
  - User management on page 51
  - Run a private query on page 52
  - Export sensor information on page 53

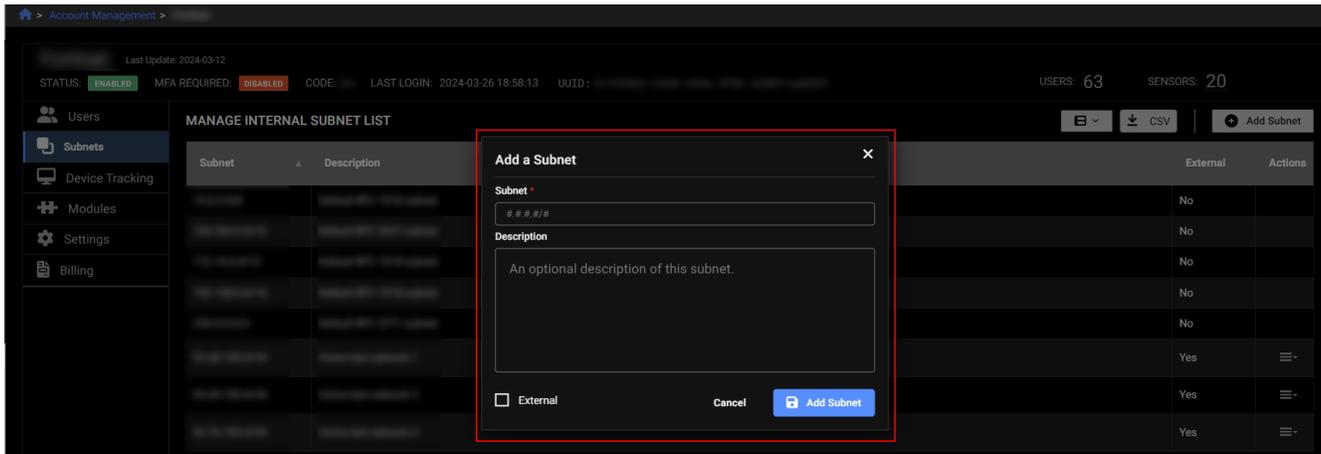
### New Functionality

#### Edit subnets

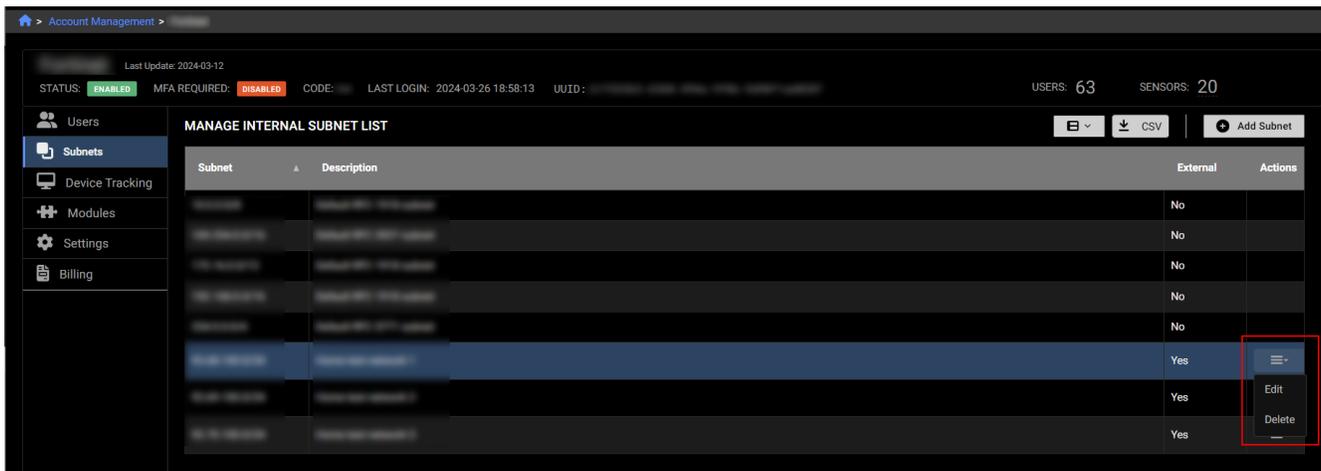
You now have the ability to add and edit subnets. Go to *Account Management > Subnets* and click *Add Subnet*.



Configure the subnet and click *Add Subnet*.



After the subnet is added, you can edit or delete the subnet from the menu in the *Actions* column.

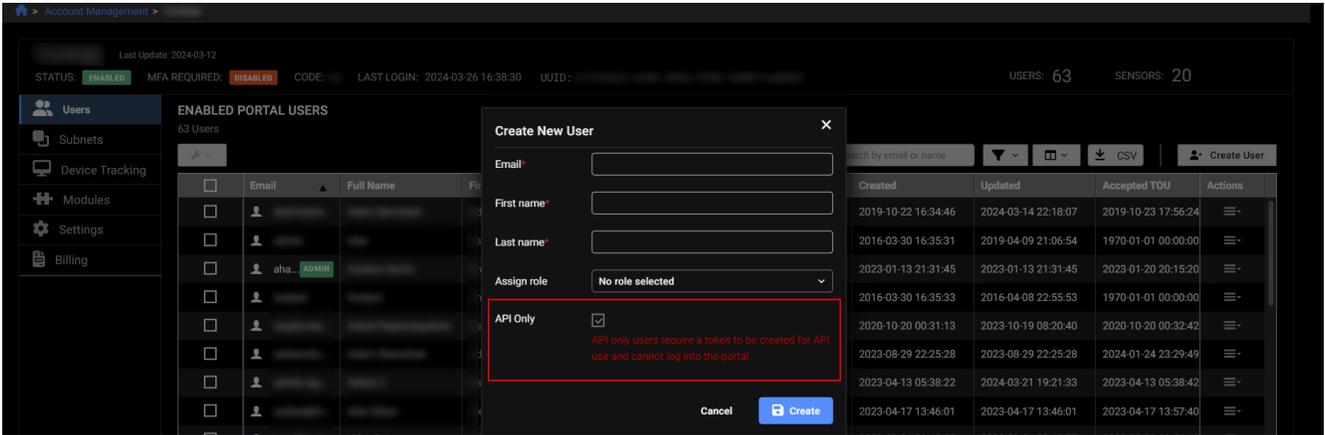


## Mandatory SSO

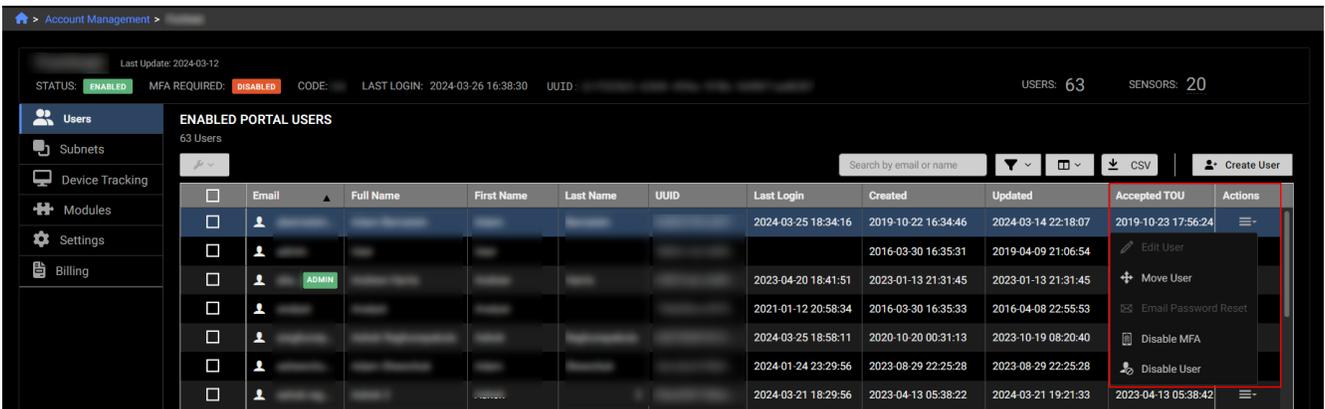
You can now require all users to log in with SSO. Go to *Account Management > Settings*. When SAML SSO is enabled the *Require SSO Logging disable login with username/password* option is displayed. For more information, see [Settings \(Account Management\) > SAML SSO > Mandatory SSO](#) in the FortiNDR Cloud User Guide.



When mandatory SSO is enabled, *API Only* is selected by default when you create a new user.



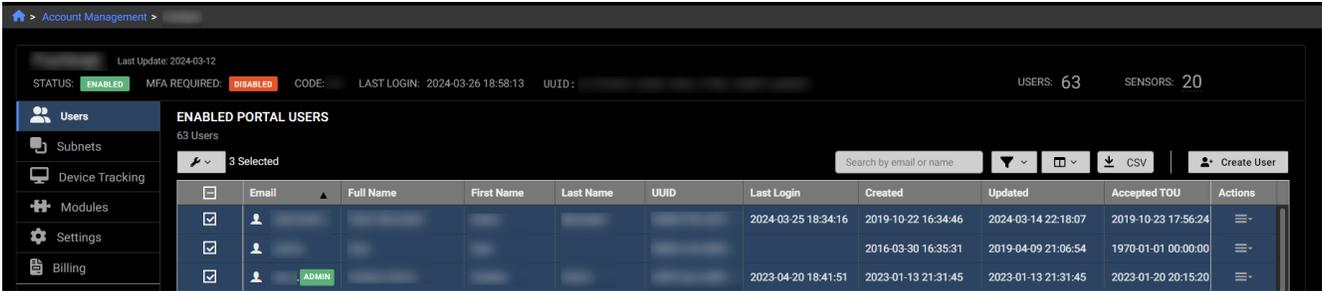
The *Edit User* and *Email Password Reset* options are also disabled in the *Users* page and the user details pane when mandatory SSO is enabled.



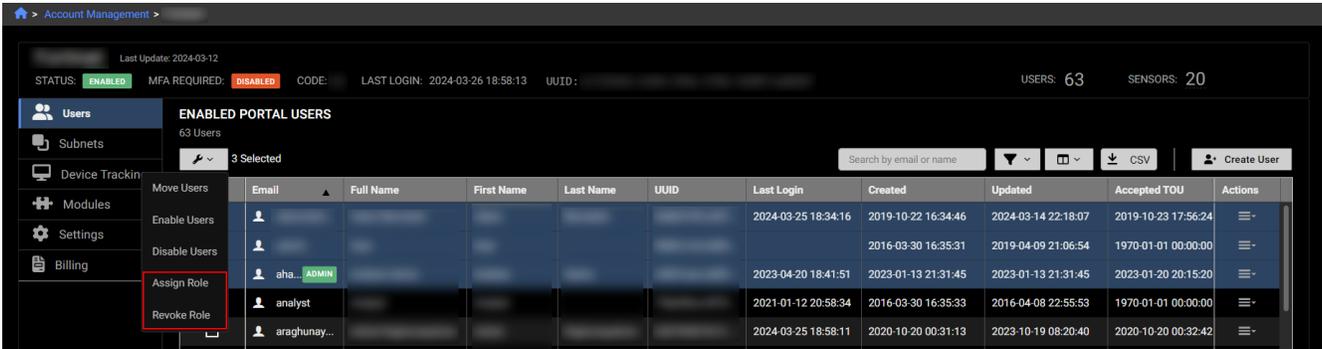
## Improved Functionality

### User management

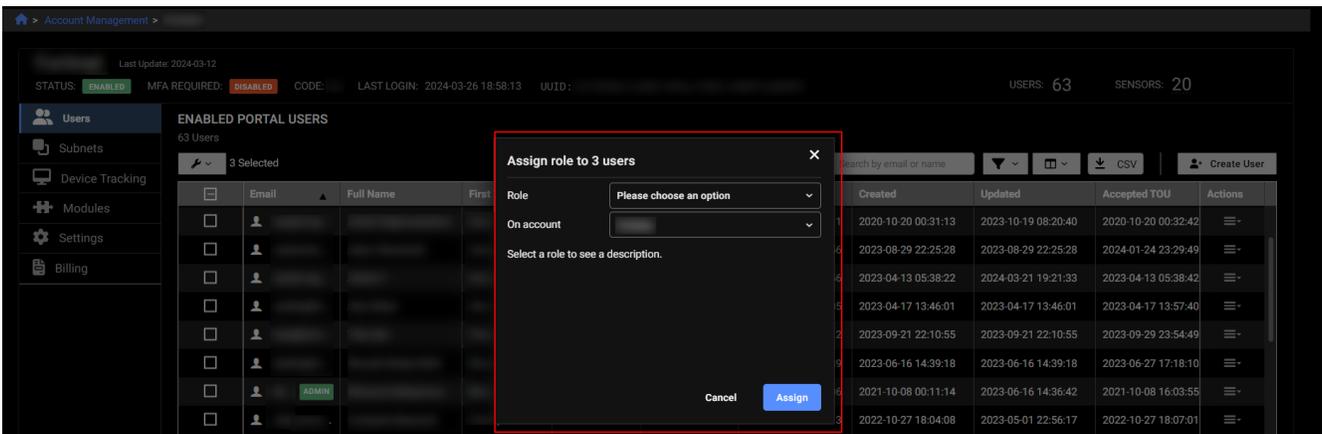
You can now assign or remove roles in bulk from the *User Management* page. Go to *Account Management > Users* and select the users you want to assign roles to.



Click the tool icon and select *Assign Role* or *Revoke Role*.

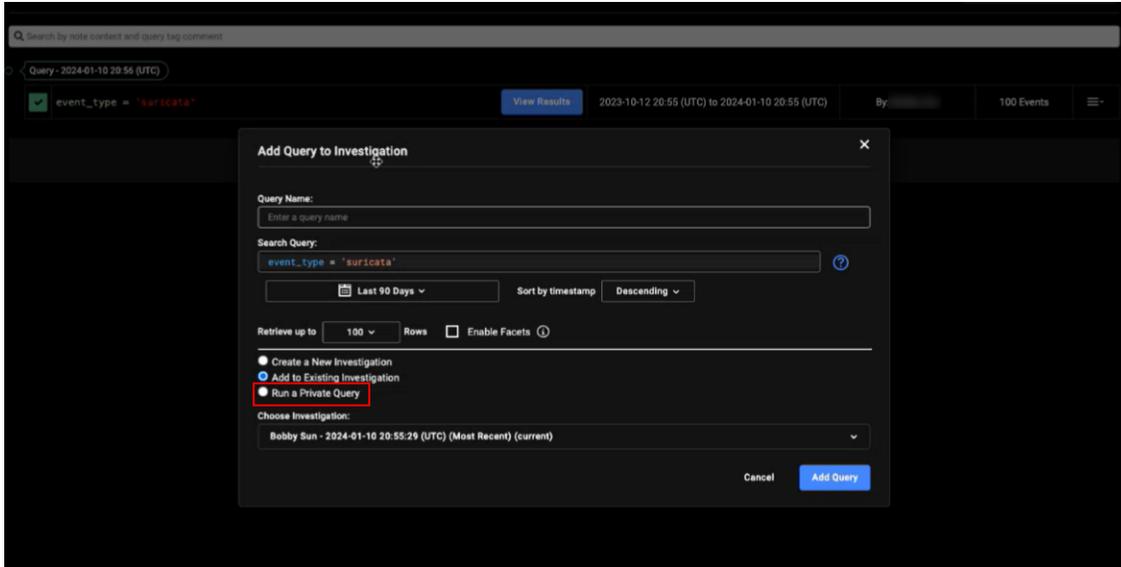


Select an option from the list and the click *Assign* or *Remove*. If the user has access to more than one account, you will see an *On Account* dropdown.



## Run a private query

You can now add a query to an adhoc search. When you clone a query you will see a new *Run a Private Query* option at the bottom of the dialog. This option is available anywhere the *Add query to Investigation* dialog appears. For information, see [Adding queries to an investigation](#).



## Export sensor information

The *Management IP* column was added to the Sensor CSV export. If there is no Management IP to display the cell is blank.

	processor_name	status.processor_core_count	status.suricata_version	status.bro_version	status.updated	status.type	interfaces	admin	prov_status	type	events	throughput	throughput_raw	management_ip
2		0			2024-02-26T19:09:10.283Z				decommissioned		0	0	0	
3	Keon(R) CPU E5-2630 v3 @ 2.40GHz	16	4.0.0-dev (rev 49)	4.1.1-0516	2024-01-22T12:45:39.430Z	ESXI			decommissioned	ESXI	0	0	0	
4		0			2024-02-28T00:25:38.280Z				decommissioned		0	0	0	
5		0			2024-02-28T00:29:37.268Z				decommissioned		0	0	0	
6		0			2024-02-28T00:37:49.477Z				decommissioned		0	0	0	
7		0			2022-11-23T22:14:50.373Z				provisioning		0	0	0	
8		0			2022-12-01T19:52:28.084Z				provisioning		0	0	0	
9	Keon(R) CPU E5-2630 v3 @ 2.40GHz	16	4.0.0-dev (rev 49)	4.1.1-0516	2022-12-02T16:56:18.365Z	ESXI			provisioning	ESXI	0	0	0	
10		0			2022-12-09T19:23:05.988Z				provisioning		0	0	0	
11		0			2022-12-12T22:06:51.496Z				provisioning		0	0	0	
12		0			2022-12-12T23:39:54.758Z				provisioning		0	0	0	
13		0			2022-12-13T00:38:45.045Z				provisioning		0	0	0	

## 13 March 2024 version 2024.2.1

- Improved Functionality
  - Sensors

## Improved Functionality

### Sensors

- A link to the [Sensors](#) topic in the *FortiNDR Cloud User Guide* was added to the *Status* column header in the *Sensors* page. This topic contains a description of each status.
- The *Sensor History* table in the *Sensor* detail page is hidden when there are no records to display.

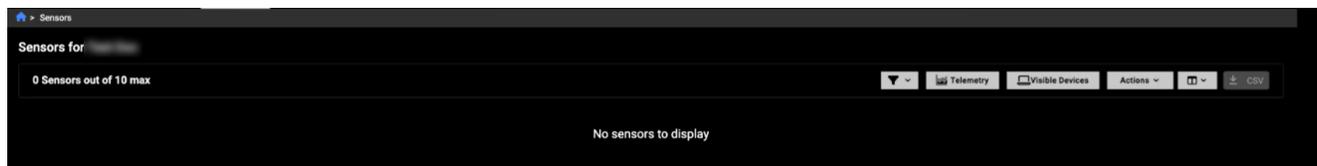
## 29 February 2024 version 2024.2.0

- New Functionality
  - [Sensors page](#)
  - [Sensor history](#)
  - [FortiGate integration](#)
- Improved Functionality
  - [Status definitions](#)
  - [Other improvements](#)
- Discontinued Functionality
  - [Enabled column](#)

## New Functionality

### Sensors page

The *Sensors* page now displays a *No sensors to display* message when there are no sensors.



A new *Decommissioned* status was added. You can use this status to filter the page. The *Decommissioned (legacy)* status indicates a sensor that was previously disabled.



In previous versions of FortiNDR Cloud a sensor with a status of *Disabled* could come back online and send data. A sensor with a status of *Decommissioned* will not send data.

---

Sensors for GigaSMART Soak Test

12 Sensors out of 500 max

SENSOR ID	STATUS	VERSION	LABELS	DAY AVERAGE	BITS/S (7 DAY AVERAGE)	TYPE
gssso591	online	Unknown			1.283 Mb/s	ESXi
gssso619	online	Unknown			0 b/s	Zscaler
gssso620	online	Unknown			0 b/s	Zscaler
gssso621	online	Unknown			0 b/s	Zscaler
gssso622	online	Unknown			0 b/s	Zscaler
gssso685	online	1.12.0	ESX		1.283 Mb/s	ESXi
gssso840	online	1.11.0			1.532 Mb/s	ESXi
gssso865	online	1.12.0			12.049 Kb/s	Large (4th Gen)
gssso920	online	Unknown			9.096 Kb/s	ESXi
gssso932	online	1.12.0		0 EPS	1.879 Kb/s	ESXi
gssso935	online	1.12.0		0 EPS	1.713 Kb/s	ESXi
gssso936	online	1.12.0		0 EPS	414.318 Kb/s	Small (4th Gen)

Additional Filters

- Status: Online
- All
- No Filters
- Decommissioned
- Decommissioned (auto)
- Decommissioned (legacy)
- Offline
- Online
- Provisioning
- Shutdown

## Sensor history

A new *Sensor History* table was added to the *Sensors* details page. This table shows the actions performed, the user who performed them as well as any comments from the user. The table is sorted in descending order by timestamp. A message appears if there is no history to display.

Management IP: [redacted]

Interfaces

- ens192: 0 b/s
- ens224: 0 b/s

Hardware

- Processor(s): Intel(R) Xeon(R) CPU E5-2630 v3 @ 2.40GHz
- Number of Cores: 8
- Total Memory: 15.638 GB
- Total Disk Space: 67.944 GB

Software

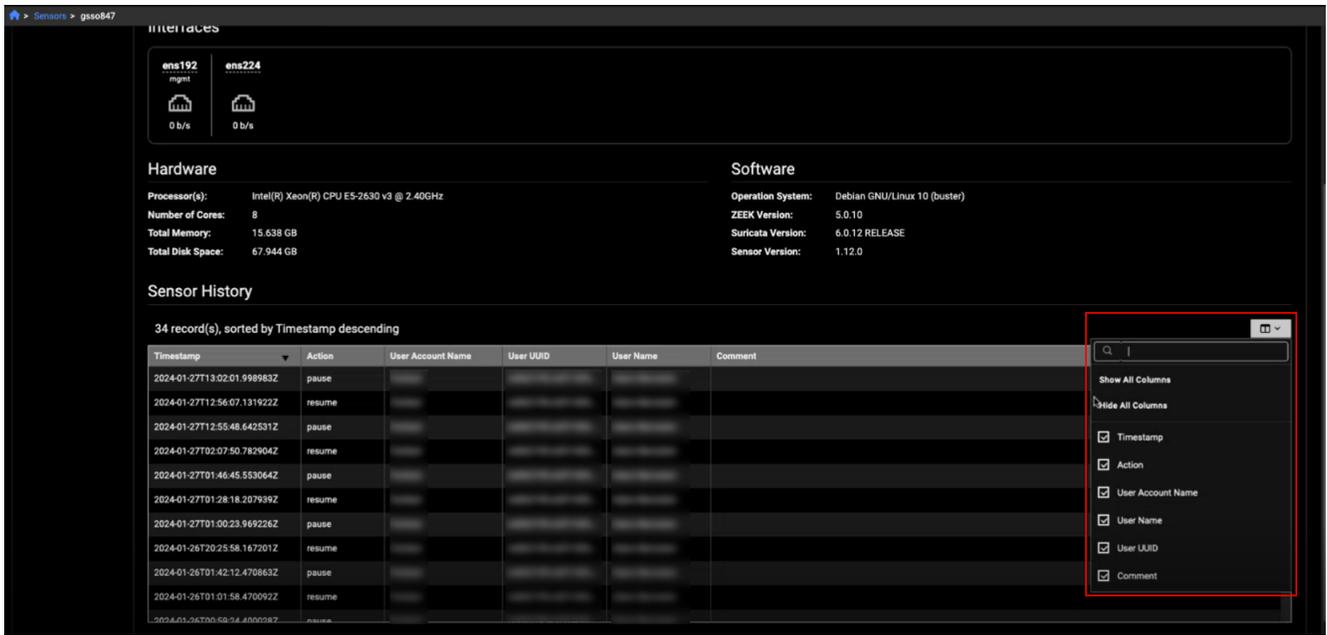
- Operation System: Debian GNU/Linux 10 (buster)
- ZEEK Version: 5.0.10
- Suricata Version: 6.0.12.RELEASE
- Sensor Version: 1.12.0

Sensor History

34 record(s), sorted by Timestamp descending

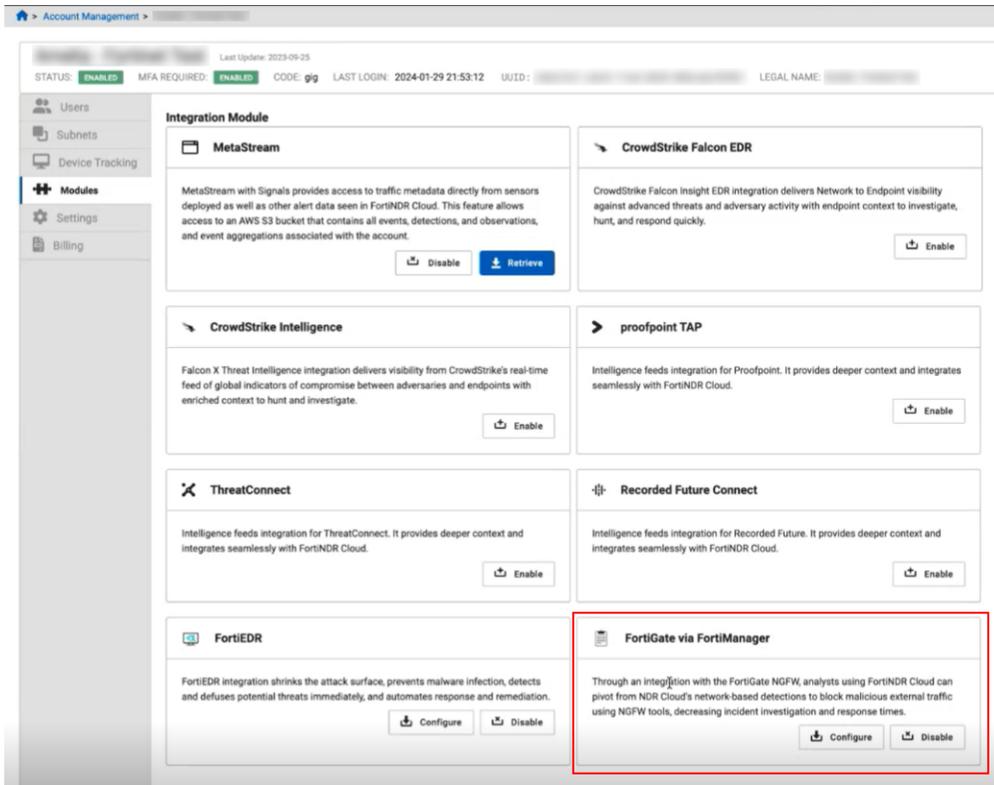
Timestamp	Action	User Account Name	User UUID	User Name	Comment
2024-01-27T13:02:01.998983Z	pause				
2024-01-27T12:56:07.131922Z	resume				
2024-01-27T12:55:48.642531Z	pause				
2024-01-27T02:07:50.782904Z	resume				
2024-01-27T01:46:45.553064Z	pause				
2024-01-27T01:28:18.207939Z	resume				
2024-01-27T01:00:23.969226Z	pause				
2024-01-26T20:25:58.167201Z	resume				
2024-01-26T01:42:12.470863Z	pause				

The table supports filtering. However, you cannot sort the *Timestamp* column in ascending order and you cannot fix the columns.

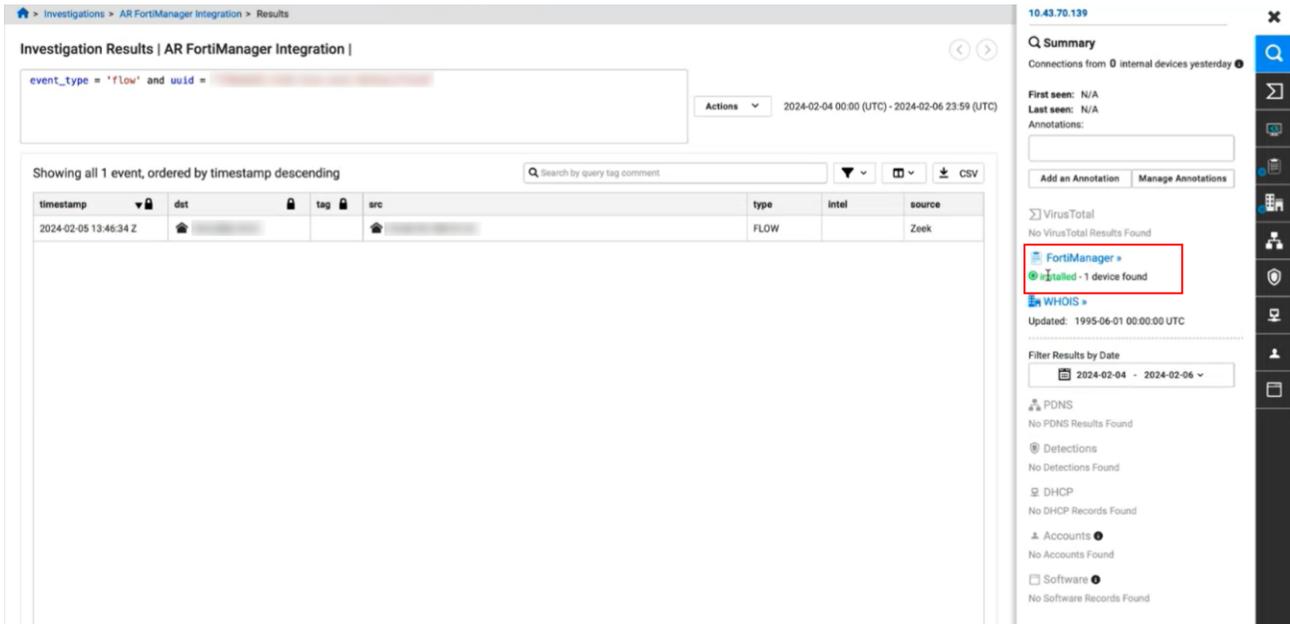


## FortiGate integration

A new FortiGate via FortiManager module was added to the *Modules* page. To add the integration, click the *Configure* button and then enter your username, password and URL.



You can view the data collected by the integration and perform FortiGate actions in the *Entity Panel* when you click on an IP in the portal.



## Improved Functionality

### Status definitions

You can now click the help icon to view a status definition. The link redirects you to the [Sensors](#) topic in the *User Guide*.



### Other improvements

- The *Entity Panel* remains open when you perform an action such as creating a filter.
- The Status definitions have been added to the User Guide. See the [Sensors](#) topic in the *User Guide*.

## Discontinued Functionality

### Enabled column

The *Enabled* column has been removed from the *Sensors* page.

The screenshot shows a table titled "Sensors for GigaSMART Soak Test" with 401 sensors out of a 500 max. The table has the following columns: SENSOR ID, STATUS, VERSION, LABELS, LOCATION, EPS (7 DAY AVERAGE), BITS/S (7 DAY AVERAGE), and TYPE. The first row shows sensor gssso333 with status "offline" and location "Tracy, CA". Other sensors are in "provisioning" status. The LABELS column contains buttons like "Exclude from monitoring", "status", "test", and "test test".

SENSOR ID	STATUS	VERSION	LABELS	LOCATION	EPS (7 DAY AVERAGE)	BITS/S (7 DAY AVERAGE)	TYPE
gssso333	offline	version2	Exclude from monitoring status test test test	Tracy, CA	0 EPS	0 b/s	QEMU/KVM
gssso355	provisioning	Unknown			0 EPS	0 b/s	
gssso368	provisioning	Unknown			0 EPS	0 b/s	
gssso378	provisioning	Unknown			0 EPS	0 b/s	
gssso388	provisioning	Unknown			0 EPS	0 b/s	
gssso406	provisioning	Unknown			0 EPS	0 b/s	
gssso442	provisioning	Unknown			0 EPS	0 b/s	
gssso444	provisioning	Unknown			0 EPS	0 b/s	ESXi
gssso453	provisioning	Unknown			0 EPS	0 b/s	
gssso458	provisioning	Unknown			0 EPS	0 b/s	
gssso461	provisioning	Unknown			0 EPS	0 b/s	
gssso467	provisioning	Unknown			0 EPS	0 b/s	
gssso468	provisioning	Unknown			0 EPS	0 b/s	

By default, the table is filtered by any status that is not *Decommissioned*. The default status filter (any status other than *decommissioned*) is the equivalent of the previous *Enabled* value.

The screenshot shows the same table as above, but with the "Additional Filters" dropdown menu open. The menu is titled "Additional Filters" and has a "Status" filter section. The status options are: Offline, Online, Provisioning, Shutdown, All, No Filters, Decommissioned, Decommissioned (auto), Decommissioned (legacy), Offline, Online, Provisioning, and Shutdown. The "Offline", "Provisioning", and "Shutdown" options are checked.

SENSOR ID	STATUS	VERSION	LABELS	LOCATION	EPS (7 DAY AVERAGE)	BITS/S (7 DAY AVERAGE)	TYPE
gssso333	offline	version2	Exclude from monitoring status test test test	Tracy, CA	0 EPS	0 b/s	QEMU/KVM
gssso355	provisioning	Unknown			0 EPS	0 b/s	
gssso368	provisioning	Unknown			0 EPS	0 b/s	
gssso378	provisioning	Unknown			0 EPS	0 b/s	
gssso388	provisioning	Unknown			0 EPS	0 b/s	
gssso406	provisioning	Unknown			0 EPS	0 b/s	
gssso442	provisioning	Unknown			0 EPS	0 b/s	
gssso444	provisioning	Unknown			0 EPS	0 b/s	ESXi
gssso453	provisioning	Unknown			0 EPS	0 b/s	
gssso458	provisioning	Unknown			0 EPS	0 b/s	
gssso461	provisioning	Unknown			0 EPS	0 b/s	
gssso467	provisioning	Unknown			0 EPS	0 b/s	
gssso468	provisioning	Unknown			0 EPS	0 b/s	

## 14 February 2024 version 2024.1.1

FortiNDR Cloud includes bug fixes, but no new features. See [Resolved issues on page 65](#).

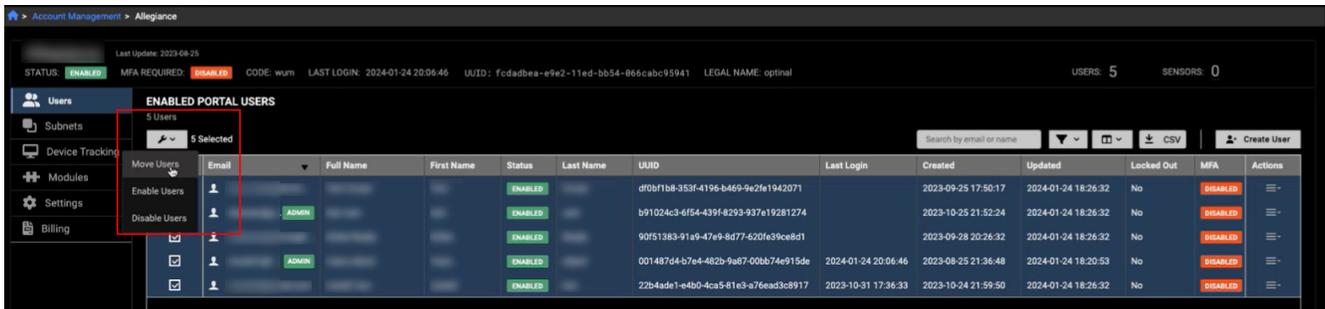
## 31 January 2024 Version 2024.1.0

- Improved functionality
  - Account management
  - Sensor table
  - Password enforcement

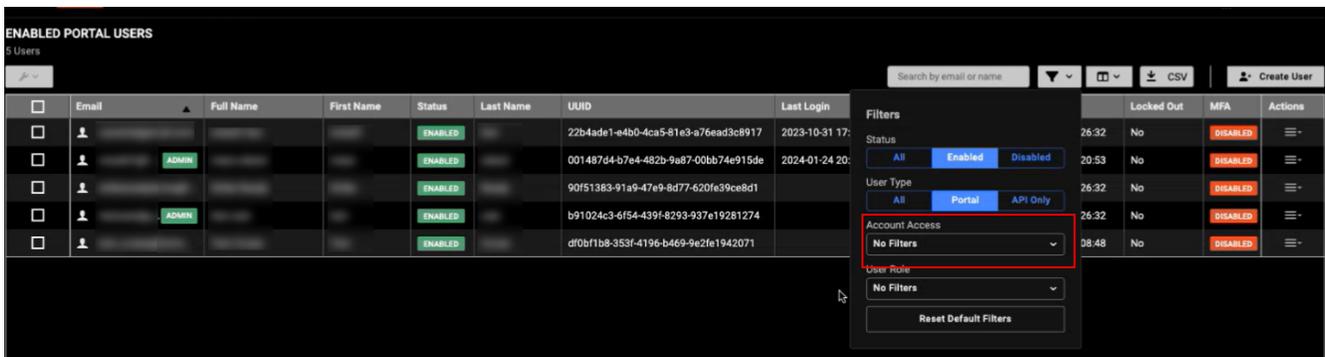
### Improved functionality

#### Account management

You are now able to move, enable, and disable multiple users at once in *the Account Management > Users* page. Simply select the users (or select all) and choose a bulk action from the menu. When you click *Confirm*, the bulk action status dialog appears as well as a message with the results. If you attempt to perform a bulk action on your own user account, the action will fail.



You are also able to filter users by account access.



## Sensor table

The sensor table has been updated to behave like the other tables in FortiNDR Cloud. The *Location* column now displays an empty cell when the location is unknown. The *7 Day Average Throughput* column has been split into two columns: *EPS (7 Day average)* and *BITS/S (7 Day average)*. This allows you to sort each column individually.



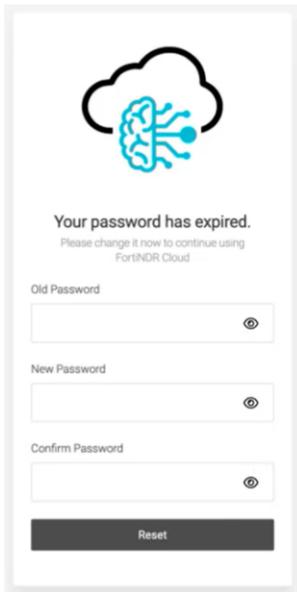
SENSOR ID	LS	LOCATION	EPS (7 DAY AVERAGE)	BITS/S (7 DAY AVERAGE)	TYPE	ENA
gssso305	side from monitoring Test zone	Tracy, ca	0 EPS	0 b/s	UNDEFINED	On
gssso333	side from monitoring Test Test		0 EPS	0 b/s	QEMU/KVM	On

## Password enforcement

The application will notify you when your password is about to expire. You can click the link in the dialog to open the reset password page. After you change a password, it will expire in 180 days. Passwords must be at least eight characters long.



If you attempt to log in after your password has expired, you will be prompted to create a new password.



Your password has expired.  
Please change it now to continue using FortiNDR Cloud

Old Password

New Password

Confirm Password

Reset

## New detection rules and observations

This page lists the new detections rules and observations in FortiNDR Cloud. New rules are created every month; however, it possible that a rule is created in a category that already exists.

### 2024.11.0

Primary ATT&CK Name	ATR Category
<b>Application Layer Protocol</b>	Attack:Command and Control > HTTP(S) Beaconing
<b>Exploit Public-Facing Application</b>	Attack:Exploitation > Exploit Public-facing Application

### 2024.10.0

Primary ATT&CK Name	ATR Category
<b>Application Layer Protocol</b>	Attack:Command and Control > Connectivity Check
<b>DNS</b>	Attack:Command and Control > DNS Tunneling
<b>Ingress Tool Transfer</b>	Attack:Installation > Remote File Copy from External
<b>LLMNR/NBT-NS Poisoning and SMB Relay</b>	Posture:Anomalous Activity
<b>Remote Access Software</b>	Posture:Potentially Unauthorized Software or Device > Remote Admin Tools
<b>Symmetric Cryptography</b>	Attack:Command and Control > Other Protocol

### 2024.9.0

Primary ATT&CK Name	ATR Category
<b>Abuse Elevation Control Mechanism</b>	Attack:Exploitation
<b>Application Layer Protocol</b>	Attack:Command and Control > Web Shell
<b>Exploit Public-Facing Application</b>	Attack:Exploitation > Exploit Public-facing Application

Primary ATT&CK Name	ATR Category
<b>Non-Application Layer Protocol</b>	Attack:Command and Control > Custom Protocol
<b>Web Protocols</b>	Attack:Command and Control > HTTP(S) Beaconing

## 2024.8.0

Primary ATT&CK Name	ATR Category
<b>Application Layer Protocol</b>	Attack:Command and Control > Other Protocol
<b>Domain Account</b>	Attack:Discovery > Remote System Scanning
<b>Domain Controller Authentication</b>	Attack:Miscellaneous
<b>Exploit Public-Facing Application</b>	Attack:Exploitation > Exploit Public-facing Application
<b>Exploitation for Client Execution</b>	Attack:Exploitation
<b>Exploitation for Privilege Escalation</b>	Attack:Miscellaneous
<b>Network Denial of Service</b>	Attack:Impact > Network DoS
<b>Non-Application Layer Protocol</b>	Attack:Command and Control > Custom Protocol

## 2024.5.0

Primary ATT&CK Name	ATR Category
<b>Exploit Public-Facing Application</b>	Attack: Command and Control > Other Protocol
<b>Non-Application Layer Protocol</b>	Attack:Command and Control > Other Protocol

## 2024.4.0

Primary ATT&CK Name	ATR Category
Network Denial of Service	Attack: Impact > Network DoS
Exploit Public-Facing Application	Attack: Exploitation > Exploit Public-facing Application
Network Denial of Service	Attack: Impact > Network DoS
Network Denial of Service	Posture: Anomalous Activity
Network Denial of Service	Attack: Impact > Service DoS
Network Denial of Service	Attack: Impact > Network DoS

## 2024.3.1

Primary ATT&CK Name	ATR Category
Application Layer Protocol	PUA:Adware
Command and Scripting Interpreter	Attack:Exploitation > Exploit Public-facing Application
Exfiltration Over Web Service	Attack:Exfiltration > C2 Server Upload
Exploit Public-Facing Application	Attack:Exploitation > Exploit Public-facing Application
Non-Application Layer Protocol	Attack:Command and Control > Custom Protocol
Web Protocols	Attack:Command and Control > HTTP(S) Beaconing

## 2024.3.0

Primary ATT&CK Name	ATR Category
Exploit Public-Facing Application	Attack:Exploitation > Exploit Public-facing Application
Non-Application Layer Protocol	Posture:Potentially Unauthorized Software or Device

## 2024.2.0

Primary ATT&CK Name	ATR Category
Web Protocols	Attack:Command and Control > Web Shell
Ingress Tool Transfer	Attack:Installation > Remote File Copy from External
Domain Groups	Attack:Discovery > Network Directory Scanning
LLMNR/NBT-NS Poisoning and SMB Relay	Attack:Infection Vector > LLMNR/NBT-NS Poisoning
Exploitation for Client Execution	Attack:Exploitation
Lateral Tool Transfer	Attack:Installation > Remote File Copy from External
Application Layer Protocol	PUA:Spyware

## Resolved issues

The following issues have been fixed in version 2024. To inquire about a particular bug, please contact [Customer Service & Support](#).

### 2024.11.0

Description
Fixed the CSV download of users in Account Management to honor the Account Access filter.
Resolved a UUID issue when updating an account.

### 2024.10.0

Description
Fixed the CSV download of users in Account Management to honor the Account Access filter.
Resolved a UUID issue when updating an account.
Fixed the resizing in the Event Type field.
Resolved issues affecting PCAP tasks.
Fixed a CrowdStrike containment issue.

### 2024.9.0

Description
Fixed an issue where clicking Resolve deselected the items in a bulk action.
Sharing investigations in the EU portal no longer fails.
The legend in the detections Visualizer no longer overlaps with the data.

## 2024.8.1

### Description

Three vulnerability bugs have been resolved.

Resolved an issue where the buttons on the Investigation Detail page were missing for some users.

Resolved an issue where certain columns were empty when viewing a query grouped by result.

## 2024.8.0

### Description

Fixed a performance issue with the Search field in the Detection Triage Rules Page.

Fixed the Roles & Permissions page to display properly in Firefox.

The Notable Detection Rules widget is displayed when there are no rules as designed.

Fixed inconsistencies between menu names and the breadcrumb.

Resolved an issue where the Entity Panel was not loading the Summary panel.

Fixed the columns and rows to fit the Files dialog.

Fixed inconsistent title case for the Source Device list.

## 2024.7.0

### Description

Fixed the MetaStream module.

No feedback was provided when a password reset failed.

The All Accounts option was sometimes missing in the Run on Accounts dialog.

Resolved a bug in the Default Dashboard. The Go back to dashboard link works as designed.

The sensor status updated timestamp is now visible on the sensor detail page.

Dashboards can be saved.

The count of visible devices had significant variations.

Fixed the security posture report query.

Fixed the New X.509 Certificates From VPS dashboard query.

### Description

Fixed the DCE/RPC Over Time dashboard query.

The correct IQL and Druid queries are used for the security report query Total Internal Hosts Serving TLSv1.1

## 2024.6.0

### Description

Resolved an issue in the Detections List where the Resolution filter was missing Automatically Resolved.

Auto-closing characters in the IQL editor no longer disables the Search button.

Users can no longer disable themselves via the user details pane or with bulk actions.

The icons in the Entity Panel are no longer obscured by the scroll bar when viewed in Safari.

Disabled accounts no longer appear in the account list when you assign a role, move a user, or perform bulk actions.

Resolved an issue in Reports where users could not select dates older than the supported backlog.

The undo function has been fixed in the Add Query field in Investigations.

Fixed an error in the Hosts Potentially Running EOL Versions of Windows query.

The security posture report shows the correct IQL version of Total Hosts Using Remote Storage Services via SSL and Total Hosts Using Remote Storage Services via HTTP.

Resolved an issue with the Users list where API users could not be deleted.

Fixed a malformed URL and error message when logging in and out of FortiNDR Cloud from the Rules details page.

## 2024.5.0

### Description

Account Management no longer displays two copies of an API token.

Fixed the example CSV file in the Manage Annotations page.

Fixed the All option in the Account dropdown menu.

Fixed the delete function in Modify Annotations in the Entity Panel.

## 2024.4.1

### Description

The detection counts in the Mitre Attack dashboard widget match the Detections Table as intended.

When a user clicks a link in an email, they no longer land on the Dashboard after they log into the portal.

When searching the Detections Table with the device IP, the search box displays the IP after the page is refreshed.

Modifying the search in adhoc search results no longer clears the IQL query box.

The items in the notifications dropdown no longer blink.

## 2024.4.0

### Description

Fixed the formatting in the Sensor detail page.

Clicking the Filehash indicators opens the Entity Panel as expected.

The Lifetime Events column in the Detections List no longer displays a Null value.

Fixed the Create button when creating a token.

Resolved an error message issue when resetting the password.

Resolved a navigation issue when creating a playbook.

Fixed the scroll bars in playbooks with a large number of queries.

## 2024.3.1

### Description

Fixed the Isolate Device feature in the FortiEDR integration.

The filters in the Sensors list no longer persist when you pivot to an account that does not have any sensors.

Fixed a styling issue in Account Management that caused errors to overlap with the page content.

Resolved an error handling issue in the FortiManager integration configuration.

## 2024.3.0

### Description

Power users can see the labels in the Sensors column in all accounts without Read/Write permissions.

Fixed a date picker issue where the start/end date does not update after resolving an error.

An SSO Account error page no longer appears when a page is refreshed.

Resolved an issue where all accounts displayed telemetry data in the Sensor page.

## 2024.2.1

### Description

Refreshing the Account Management page no longer generates an error screen.

Resolved an issue where Observations dashboard was not recovering from a previous failed query.

The Account Management detail page no longer shows the wrong permissions.

Resolved all permission issues (such as Edit and Disable) in the Child Account tab in the Account Detail page.

Fixed issues with Admin permissions in the Subnet tab.

Fixed the permission in Settings tab.

Fixed the Admin permissions in the Device Tracking tab.

The Decommissioned status the sensor's details page now matches the status in the Sensors page .

## 2024.2.0

### Description

Users with multiple accounts will see the Edit button for the accounts with Admin permissions.

Clicking an IP in the src column that has multiple annotations no longer opens the Entity Panel.

The error message styling has been improved to make it easier to read.

The Rule Name filter in the Detections table no longer disappears when the dropdown is closed.

## 2024.1.1

### Description

GUI: Bulk Move is no longer available to Admins with one account .

GUI: Sensors list page no longer displays the Edit button to users with only a user role in an account.

GUI: The BITS/S (7 DAY AVERAGE) column on the Sensors list page no longer displays undefined/s units.

A scroll bar was added to the Update Account Dialog in the Parent Account dropdown.

Detections table does not show error if there are a large number of active rules.

Detail View: Resolved an issue where the description header was missing when switching pages in the Details view.

Resolved an issues where the investigation was not selected when clicking Add to existing investigation.

## 2024.1.0

### Description

Account Management: The Account Management breadcrumb no longer appears as plain text when the user has multiple admin roles.

Refreshing the Edit Rule page no longer takes you to the Rule Details page.

Resolved an issue where clicking the title in a Dashboard widget did not launch the Add query to Investigation dialog.

Investigations: When a user switches accounts after copying a URL in the Investigations page, the URL will redirect back to the correct account as expected.

Sensors : Telemetry now displays the correct units in the Sensors page.



[www.fortinet.com](http://www.fortinet.com)

Copyright© 2025 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's Chief Legal Officer, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.